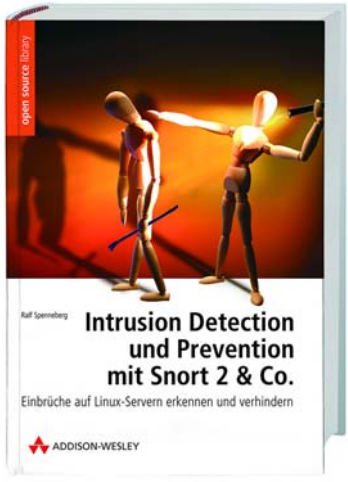
Linux-Firewalls mit iptables & Co.

open source library

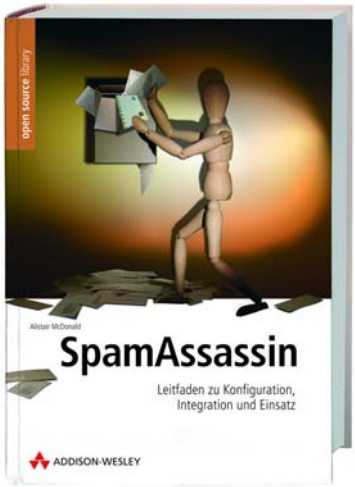
Open Source Software wird gegenüber kommerziellen Lösungen immer wichtiger. Addison-Wesley trägt dieser Entwicklung Rechnung mit den Büchern der **Open Source Library**. Administratoren, Entwickler und User erhalten hier professionelles Know-how, um freie Software effizient einzusetzen. Behandelt werden sowohl Themen wie Betriebssysteme, Netzwerke und Sicherheit als auch Programmierung.

Eine Auswahl aus unserem Programm:



Dieses Buch zeigt, wie mit den Bordmitteln jeder Linux-Distribution – z. B. Snort 2.0 – auf einem Linux-Server ein professionelles System zur Einbruchserkennung und -Verhinderung aufgesetzt wird. Der Autor erläutert die Anwendung von IDS auf komplexe Netzwerke, beschreibt die Arbeit mit den wichtigsten Tools (Tripwire und Snort) zur System- und Netzwerküberwachung, schildert ausführlich die Analyse der gewonnenen Daten sowie ihre Interpretation und gibt Richtlinien für die Prävention und die richtige Reaktion im Ernstfall. Er beschreibt außerdem die technischen und formalen Voraussetzungen für den Einsatz eines IDS, zeigt Grenzen auf und warnt vor juristischen Fallstricken.

Ralf Spenneberg
Intrusion Detection und Prevention mit Snort 2 & Co
ISBN-13: 978-3-8273-2134-3
ISBN-10: 3-8273-2134-4
840 Seiten
Euro 59,95 (D), 61,70 (A)



Dieses Buch beschreibt fokussiert und übersichtlich, wie SpamAssassin auf- und eingesetzt wird, um Spam erfolgreich abzuwehren. Der Autor schafft mit der Beschreibung verschiedener Abwehr-Verfahren zunächst die theoretischen Grundlagen, bevor er detailliert deren Umsetzung mit SpamAssassin beschreibt. Von der Zusammenarbeit mit verschiedenen Mailservern wie sendmail, qmail, postfix und exim über die dynamische Optimierung der Filter bis hin zu Performancefragen werden alle Aspekte der SpamAssassin-Praxis behandelt.

Alistair McDonald
SpamAssassin
ISBN-13: 978-3-8273-2205-0
ISBN-10: 3-8273-2205-7
288 Seiten
Euro 39,95 (D), 41,10 (A)

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

Umwelthinweis:
Dieses Produkt wurde auf chlorfrei gebleichtem Papier gedruckt.

10 9 8 7 6 5 4 3 2 1

08 07 06

ISBN-13: 978-3-8273-2136-7
ISBN-10: 3-8273-2136-0

ein Imprint der Pearson Education Deutschland GmbH,
Martin-Kollar-Straße 10–12, D-81829 München/Germany

Einbandgestaltung: Marco Lindenbeck, webwo GmbH (mlindenbeck@webwo.de)
Lektorat: Boris Karnikowski, bkarnikowski@pearson.de
Korrektorat: Friederike Daenecke, Zülpich
Fachkorrektorat: Wilhelm Dolle, Berlin
Herstellung: Monika Weiher, mweiher@pearson.de
Satz: LE-TEX Jelonek, Schmidt & Vöckler GbR, Leipzig
Druck und Verarbeitung: Kösel, Krugzell (www.KoeselBuch.de)
Printed in Germany

Für Claudia

Ich Dich auch ;-)

Inhaltsübersicht

Inhaltsverzeichnis

Vorwort

Dieses Buch widmet sich dem Paketfilter *Netfilter/Iptables* der Linux-Kernel 2.4 und 2.6. Obwohl bereits einiges an Literatur zu diesem Thema existiert, hat mir persönlich kein Buch richtig gut gefallen. Daher habe ich bereits seit einigen Jahren überlegt, ein eigenes Buch zu diesem Thema zu schreiben, das auch die fortgeschrittenen Themen und neue Eigenschaften behandelt, die in den letzten Jahren hinzugekommen sind.

Während ich an diesem Buch geschrieben habe, hat das Netfilter-Team (das das Framework im Kernel entwickelt, das mit Iptables gesteuert wird) große Teile, die im Kernel verborgen sind, ausgetauscht. Das hat zu einem Wettlauf zwischen mir und den Release-Zyklen der Kernel geführt. Natürlich wollte ich diese Funktionen auch in dieses Buch einarbeiten. Da ich selbst noch nicht sämtliche Auswirkungen auf alle Bereiche absehen kann und sich einige auch noch im Fluss befinden, habe ich diese Neuerungen in ein eigenes Kapitel (siehe Kapitel 27) verschoben. Jedoch wird der typische Endanwender diese Modifikationen entweder gar nicht wahrnehmen oder aber in einigen Bereichen auch begrüßen.

Ansonsten habe ich versucht, sowohl den Einsteiger zu berücksichtigen und ihn in einzelnen Kapiteln behutsam mit der Materie des Paketfilters vertraut zu machen als auch dem fortgeschrittenen Benutzer die Mittel an die Hand zu geben, die er für eine mächtige Firewall benötigt.

Ich hoffe, dass es mir mit diesem Buch gelungen ist, Ihren Geschmack zu treffen und Ihnen wertvolle Informationen zu liefern. Nach meinen Büchern »VPN mit Linux (ISBN 3-8273-2114-X)« und »Intrusion Detection und Prevention mit Snort 2 & Co. (ISBN 3-8273-2134-4)« rundet dieses Buch das Thema Netzwerksicherheit mit Open Source ab.

Sollten Sie Fragen oder Kritik zu diesem Buch haben, zusätzliche Ideen haben oder Informationen vermissen, würde ich mich über Ihre E-Mail an *ralf@spenneberg.net* freuen.

Ich wünsche Ihnen viel Spaß beim Lesen und viel Erfolg bei der Konfiguration und Administration Ihrer Linux-Firewall.

Einleitung

Angesichts täglicher Meldungen über neue Viren, Hackerangriffe und Sicherheitslücken ist eine Firewall ein wesentlicher Bestandteil eines sicheren Netzwerks. Eine Firewall ist besonders wichtig, wenn Sie Ihr Netzwerk mit anderen unbekannten und nicht vertrauten Netzwerken wie dem Internet verbinden. Dann sollten Sie diese Verbindung mit einer Firewall überwachen. Die Firewall beschränkt den Netzwerkverkehr auf den von Ihnen gewünschten Verkehr und weist alle anderen Anfragen ab. Natürlich müssen Sie sicherstellen, dass es keine Möglichkeit gibt, die Firewall mit Hilfe eines Modems oder anderer Hilfsmittel zu umgehen, denn dann ist die Firewall fast nichts mehr wert. Es bleibt Ihnen dann nur noch der Wert der Hardware.

Aber selbst wenn Sie Ihr Netzwerk nicht mit einem anderen Netz verbinden oder hierzu eine kommerzielle Firewall verwenden, kann es sinnvoll sein, über interne Linux-Firewalls nachzudenken. Kennen Sie Ihre Benutzer und Anwender wirklich? Vertrauen Sie ihnen? Gibt es in Ihrem Netz Systeme, die Sie schützen möchten oder müssen? Dann ist es sinnvoll, auch innerhalb eines Netzes mit Firewalls den Schutz dieser Systeme zu implementieren.

Dieses Buch hilft Ihnen dabei, diese Funktionen mit Hilfe von Linux und Iptables zu realisieren.

Das Buch beginnt mit den Firewall-Grundlagen. Hier lernen Sie wichtige Begriffe, Architekturen und die Unterschiede der verschiedenen Firewall-Technologien kennen. Außerdem erhalten Sie einen kurzen Überblick, wie Firewalls entstanden sind.

Der zweite Teil beschäftigt sich mit einer Einführung in Iptables und zeigt Ihnen, wie Sie eine einfache Firewall auf einem Gateway mit Iptables realisieren. Außerdem erfahren Sie in diesem Kapitel, wie Sie eine Linux-Distribution härten und wie Ihnen Intrusion-Detection-Systeme helfen können, Angriffe zu erkennen, die Ihre Firewall nicht abgewehrt hat.

Der dritte Teil beschäftigt sich mit typischen Firewall-Architekturen und stellt Ihnen eine lokale Firewall und eine Firewall mit DMZ inklusive der Realisierung und möglicher Probleme vor.

Im vierten Teil werden verschiedene zusätzliche Werkzeuge vorgestellt, die Sie benötigen oder verwenden können, um erfolgreich eine Firewall aufzubauen und zu warten. Dies sind Protokollserver, Zeitserver, Protokollanalysewerkzeuge, Oberflächen für die Administration, eine Betrachtung der von den Distributionen mitgelieferten Werkzeuge und Werkzeuge für den Test Ihrer Firewall.

Der fünfte Teil ist für die fortgeschrittenen Anwender gedacht und beginnt mit einer kompletten Referenz aller Iptables-Funktionen (Tests und Ziele), den in Patch-O-Matic verfügbaren zusätzlichen Funktionen, einer Beschreibung des Connection-Tracking-Mechanismus und dessen Tuning und der Beschreibung der NAT-, Mangle- und Raw-Tabellen. Weiterhin finden Sie hier die Erklärung der Variablen im `/proc`-Verzeichnis. Sie lernen, wie Sie in Datenbanken protokollieren, IP-Adressen mit `ipset` gruppieren, hochverfügbare Firewalls aufbauen und welche Funktionen in der nächsten Zukunft in Iptables zu erwarten sind.

Der sechste Teil ist komplett transparenten Firewalls gewidmet. Dies sind Firewalls, die auf der IP-Ebene unsichtbar sind und wie auf einer Bridge arbeiten.

Der siebte Teil beschäftigt sich mit den Besonderheiten einzelner Protokolle und zeigt Ihnen, wie Sie DHCP, IPv6 oder IPsec filtern. Diese Kapitel sollten alle Fragen rund um eine Iptables-Firewall beantworten.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

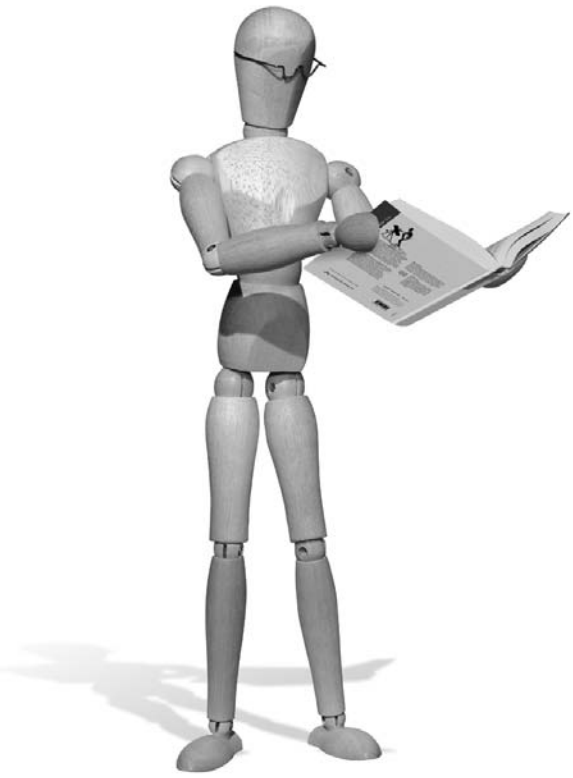
ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Teil I

Firewall-Grundlagen



1 Firewall-Geschichte

Ich persönlich empfinde es immer als hilfreich, die geschichtliche Entwicklung der eingesetzten Produkte und Technologien zu kennen, um diese besser bewerten und einschätzen zu können. Dieses Kapitel versucht, skizzenhaft die Entwicklung der Firewalls aufzuzeigen.

1.1 Der Anfang des Internets

Das Internet begann als eine Reihe von Notizen von J.C.R. Licklider am MIT, in denen er 1962 ein »Galactic Network« beschreibt. Ein Jahr früher veröffentlichte Leonard Kleinrock (ebenfalls am MIT) eine erste Arbeit über paketvermittelnde Netzwerke. Aus diesen Ideen entstand 1965 das erste Wide-Area-Network (WAN), in dem Lawrence G. Roberts gemeinsam mit Thomas Merrill den TX-2 Computer des Lincoln Labs in Massachusetts mit dem Q-32-Computer des SDC in Kalifornien verband. 1966 ging Roberts dann zur Defense Advanced Research Projects Agency (DARPA), um dort ein Konzept für ein Computer-Netzwerk zu entwickeln. Angeblich versprach Charlie Hertzfeld (Direktor der DARPA) dem IPTO-Direktor Bob Taylor eine Million Dollar für die erfolgreiche Implementierung eines verteilten Kommunikationsnetzwerks. Die Entwicklung des ARPANET begann. Im Dezember 1970 wurde das erste Netzwerkprotokoll für das ARPANET offiziell verabschiedet: das Network Control Protocol (NCP). Die Entwicklung der Anwendungen konnte beginnen. 1972 wurde als erste Applikation E-Mail vorgestellt.

Das NCP-Protokoll erlaubte zwar die Kommunikation in dem Netz. Je größer das ARPANET wurde, desto deutlicher wurden jedoch seine Schwächen. So wurde die Entwicklung der Internetprotokollfamilie TCP/IP begonnen. TCP/IP wurde 1980 vom Department of Defense bereits als Standard anerkannt und 1982 in einem RFC beschrieben. Am 1.1.1983 wurde das ARPANET auf TCP/IP umgestellt. In den folgenden Jahren wuchs das ARPANET. Weitere Netzwerke wurden aufgebaut: BITNET, USENET, MFENET, HEPNET, SPAN, CSNET. Im kommerziellen Bereich entstanden XNS (Xerox), IBM SNA und das DECNET. Speziell für den akademischen Bereich wurde das NSFNET gestartet. Dieses wuchs in nur 8 Jahren von einem Backbone mit 6 Knoten (56 kBit/s) zu 21 Knoten mit bis zu 45 Mbit/s. Das Internet wuchs in dieser Zeit zu einer Zahl von 50.000 Netzen weltweit.

Dennoch handelte es sich beim Internet lange Zeit um eine heile Welt. Jeder kannte und vertraute jedem anderen Teilnehmer, und unter dem Aspekt Sicherheit betrachtete man lediglich die Gefahr eines Paketverlustes und entwickelte Methoden und

Protokolle, um den Verlust von Paketen zu verhindern und die Verfügbarkeit der Dienste und der Kommunikation zu garantieren.

1.2 Der Morris-Wurm

Im November 1988 löste der Morris-Wurm von Robert Tappan Morris eine Epidemie im Internet aus. Dieser Wurm drang über Sicherheitslücken in den Unix-Betriebssystemen ein und nutzte Sendmail, Finger und die R-Dienste für seine Verbreitung aus. Die verwendeten Sicherheitslücken werden in der Bugtraq-Datenbank unter den Nummern 1 und 2 geführt (*http://www.securityfocus.com/bid/1*). Während seiner Verbreitung infizierte dieser Wurm mit 6000 Rechnern etwa 10% des damaligen Internets. Robert Morris wurde am 26. Juli 1989 als Freisetzer des Wurms identifiziert und am 22. Januar 1990 zu 400 Stunden gemeinnütziger Arbeit und 10.400 Dollar Geldstrafe verurteilt. Interessanterweise war sein Vater, Robert Morris Senior, zu diesem Zeitpunkt Chef-Wissenschaftler der National Security Agency (NSA).

Als direkte Reaktion auf den Wurm wurde noch im November 1988 das Computer Emergency Report Team Coordination Center (CERT/CC) von der Defense Advanced Research Projects Agency (DARPA) gegründet.

Des Weiteren begannen die Unternehmen, über einen Schutz ihrer Netzwerke vor dem Internet nachzudenken. Bis zu diesem Zeitpunkt gab es keine Firewalls, kein NAT und auch keinen anderweitigen Schutz.

1.3 Die erste Firewall

Recht früh wurden bereits Router als Sicherheitssysteme für die Abschottung eines Netzes von den anderen Netzen eingesetzt. Zu Beginn nutzte man diese Router, um zu verhindern, dass Netzwerk-Fehlkonfigurationen Broadcast-Stürme auslösten, die sämtliche Netze in Mitleidenschaft zogen[1].

Die ersten richtigen Firewalls wurden relativ gleichzeitig bei DEC und AT&T entwickelt. Bei DEC betrieb zunächst Brian Reid und dann Paul Vixie ein System mit dem Namen `gatekeeper.dec.com`. Für den Zugriff auf das Internet mussten die Anwender sich auf diesem System anmelden (telnet und ftp) und konnten dann von diesem System auf Systeme im Internet zugreifen.

Gleichzeitig arbeitete Marcus J. Ranum für Frederick Avolio in einer anderen Abteilung bei DEC. Sie verfügten über eine Internetverbindung mit 9600 Baud und benötigten eine ähnliche Sicherheitsstruktur. Marcus Ranum wollte jedoch den Anwendern keine Konten auf dem System für eine Anmeldung zur Verfügung stellen

[1] Ein Broadcast-Paket wird von jedem Rechner entgegengenommen. Viele der ersten Protokolle verwendeten Broadcast-Pakete für die Kommunikation. Ein Router leitet Broadcast-Pakete nicht weiter. So sind die Rechner hinter dem Router nicht von einem Broadcast-Paket betroffen. Ansonsten kann in einem großen Netzwerk der Broadcast-Verkehr einen großen Teil der Netzwerkkapazität belegen.

und schrieb daher den ersten FTP-Proxy für seinen Gatekeeper. Kurze Zeit später (1991) wurde diese Firewall bereits als erste kommerzielle Firewall DEC-SEAL (Securing External Access Link) an einen großen Chemie-Konzern verkauft und dort im Juni 1991 auf mehreren Systemen eingerichtet. Ein Firewall-System bestand aus einem Gatekeeper, der als einziges System auf das Internet zugreifen durfte, und einem Gate, das den Zugriff des internen Netzes auf den Gatekeeper als Paketfilter überwachte. Der Gatekeeper verfügte über eine gewisse Anzahl von Proxys, die den Zugriff per telnet, ftp, E-Mail, News, Whois und X erlaubten. Die DEC SEAL wurde schließlich zur AltaVista Firewall weiterentwickelt.

Frederick Avolio und Marcus Ranum wechselten zu Trusted Information Systems (TIS) und programmierten dort das TIS Firewall-Toolkit (TIS FWTK, *http://www.fwtk.org/*). Nach dem Kauf von TIS durch NAI 1998 wurde diese Firewall als Gauntlet kommerziell vermarktet.

Gleichzeitig wurde bei AT&T von William R. Cheswick und Steven M. Bellovin in den Bell Laboratories eine Firewall entwickelt, die nicht über einzelne Proxys für jedes Protokoll verfügte, sondern als Curcuit-Relay-Proxy ausgelegt war. Dies war der Vorgänger des SOCKS-Protokolls und des SOCKS-Proxy. Kommerziell wurde diese Firewall als Raptor Eagle kurze Zeit später verkauft.

Die ersten Firewalls waren also immer Systeme, die für die Funktion auf Proxys zurückgriffen. Auch heute gibt es noch viele Firewall-Systeme, die für die Realisierung Proxys einsetzen. Bei einigen Protokollen ist dies auch sinnvoll, um eine Filterung von Viren oder unerwünschten Inhalten durchzuführen.

Im Jahr 1994 betrat Check Point den Markt der Firewalls und bot von Anfang an einen Paketfilter mit einer grafischen, leicht zu administrierenden Oberfläche an. Gleichzeitig war dieser Paketfilter in der Lage, den Zustand der TCP-Verbindungen zu überwachen und Verbindungen nur in bestimmten Richtungen zu erlauben.

1.4 Firewalls heute

Heute bestehen Firewall-Systeme meist aus einer Kombination aus Paketfilter und Proxy. Während einige Protokolle auf Grund ihrer Natur nicht mit einem Proxy gefiltert werden können (z.B. IPsec), ist es bei anderen Protokollen zum Schutz der eigenen Infrastruktur zwingend erforderlich, Proxys einzusetzen. Ein Paketfilter kann keinen Virus oder andere bösartige Inhalte in E-Mails oder in Webseiten erkennen und entfernen.

Dennoch gibt es auch häufig Szenarien, bei denen dieses gar nicht gewünscht wird oder eine Proxy-Firewall nicht den Datendurchsatz bewältigen könnte. Hier werden dann reine Paketfilter eingesetzt.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

2 Firewall-Technologien

Es gibt viele verschiedene Technologien, die beim Aufbau einer Firewall eingesetzt werden können. Dieses Kapitel stellt die wichtigsten vor und beschreibt ihre Funktionsweise sowie ihre Vor- und Nachteile.

2.1 Paketfilter

Der Paketfilter ist die einfachste Technologie für die Implementierung einer Firewall. Die erste Implementierung geht auf Jeffrey C. Mogul im Jahr 1989 zurück (Simple and flexible datagram access controls for Unix-based gateways: *ftp://ftp.digital.com/pub/Digital/WRL/research-reports/WRL-TR-89.4.pdf*). Mogul stellte auf der USENIX Summer Conference im März 1989 mit dem Programm `screend` einen ersten Paketfilter vor. Der `screend` ist ein Userspace-Programm, das die Entscheidung trifft, ob ein Paket passieren darf oder nicht.

Im Grunde ist ein Paketfilter ein intelligenter Router. Während ein normaler Router lediglich entscheidet, wohin ein Paket geschickt wird, analysiert ein Paketfilter zusätzlich das Paket und bestimmt, ob ein Paket überhaupt weitergesendet werden darf oder ob es verworfen werden muss.

Da diese beiden Aufgaben eng miteinander verwandt sind, werden seit damals fast alle Router mit zusätzlichen Paketfilterfunktionalitäten ausgestattet. Auch die meisten Netzwerkbetriebssysteme verfügen seit Jahren über derartige Paketfilter.

Die meisten Paketfilter sind IP-Paketfilter. Das bedeutet, sie beschränken ihre Betrachtung auf IP-Pakete. Dort analysieren sie den IP-Header. Die meisten Paketfilter können zusätzlich im Falle eines UDP-, TCP- oder ICMP-Paketes auch deren Header analysieren. Hierzu nutzen die Paketfilter üblicherweise ein Regelwerk, das sie Regel für Regel bei jedem Paket testen. Trifft eine Regel zu, so wird die mit der Regel verbundene Aktion ausgeführt. Die üblicherweise unterstützten Aktionen sind das Annehmen und Routen des Pakets, das Verwerfen des Pakets und das Ablehnen des Pakets (Senden einer Fehlermeldung an den Absender).

Ein klassischer zustandsloser Paketfilter kann nicht erkennen, ob ein Paket zu einer aufgebauten Verbindung gehört oder nicht. Jedes Paket wird einzeln für sich betrachtet und analysiert. Der Zusammenhang, in dem das Paket auftritt, ist belanglos. Der Administrator eines Paketfilters muss daher sowohl die Pakete des Clients als auch die Pakete des potenziellen Servers in seinem Regelwerk berücksichtigen.

2.2 Zustandsorientierte Paketfilter

Die ersten zustandsorientierten kommerziellen Paketfilter wurden 1993 verfügbar. Das bekannteste, heute noch im Einsatz befindliche Produkt ist die Check Point Firewall-1. Dieses Produkt besaß eine einfache Verbindungstabelle, in der sich die Firewall sämtliche Verbindungen merkte, die von innen aufgebaut worden waren, und automatisch sämtliche Antworten zuließ.

Die erste frei verfügbare Variante eines zustandsorientierten Paketfilters war IP-Filter (IPF) 3.0 (1996) von Darren Reed. Ebenfalls 1996 erschien mit der SF Firewall (*http://www.ifi.unizh.ch/ikm/SINUS/sf-doc/impl.htm*) eine erste Implementierung für Linux. Diese wurde in den weiteren Jahren zur Sinus Firewall mit grafischer Oberfläche weiterentwickelt.

Heute besitzt Linux mit Iptables/Netfilter einen der mächtigsten zustandsorientierten Paketfilter, die verfügbar sind.

Allen zustandsorientierten Paketfiltern ist gemeinsam, dass sie sich in einer Tabelle die aufgebauten und von dem Regelsatz erlaubten Verbindungen merken und alle weiteren Pakete dieser Verbindungen mehr oder weniger automatisch erkennen und zulassen. Die explizite Erkennung dieser Pakete durch einzelne Regeln ist nicht erforderlich. Dies vereinfacht zum einen die Definition und die Wartung der Regeln erheblich, denn die Zahl der Regeln schrumpft mindestens um die Hälfte. Zum anderen erhöht es auch sehr stark die Sicherheit der Firewall. Es ist nun nicht erforderlich, grundsätzlich jedes mögliche Antwortpaket eines jeden möglichen Kommunikationspartners durchzulassen. Die zustandsorientierte Firewall beschränkt dies auf die Pakete, die sie als Teil der Verbindung tatsächlich erkennt.

Eine Weiterentwicklung ist die Inspection- oder auch Deep-Inspection-Firewall. Hierbei handelt es sich um Systeme, die die Pakete noch genauer analysieren und – besonders als Deep-Inspection-Systeme – eine Kombination aus Paketfilter und Intrusion-Detection-System oder Virenscanner darstellen. Hierzu prüfen die Systeme, ob über die Verbindung ein Angriff oder ein Virus übertragen wird. Auf Grund der Natur eines Paketfilters und der hohen Anforderung an die Geschwindigkeit, sind die Deep-Inspection-Systeme jedoch meist nicht so gut wie eine Kombination aus einem reinen Paketfilter und einem Virusscanner oder einem IDS.

Dennoch haben sich die Paketfilter in vielen Bereichen gegenüber den Proxys durchgesetzt, da die Implementierung preiswert und einfach möglich ist, der Paketfilter auch im Bereich der Gigabit-Netzwerke eine leistungsgerechte Filterung durchführen kann und als zustandsorientierter Paketfilter mit Inspection oder sogar Deep-Inspection-Analyse für viele Anwendungsfälle ausreichend Sicherheit bietet.

2.3 Curcuit Relay

Das Curcuit Relay ist ein Proxy auf der Transport-Schicht, der das verwendete Applikationsprotokoll nicht versteht, sondern die Daten auf der Transport-Schicht austauscht. Dieses Prinzip wurde 1996 in dem SOCKS-Protokoll weiterentwickelt und

verbessert. Das SOCKSv5-Protokoll wurde in dem RFC 1928 definiert und festgelegt. Heute sind noch zwei Versionen des Protokolls im Einsatz: SOCKSv4 und SOCKSv5. SOCKSv5 unterstützt auch Applikationen, die das UDP-Protokoll nutzen.

Der besondere Pluspunkt für den Einsatz des SOCKS-Proxys ist die einfache Implementierung. Wenn der Quelltext einer Applikation verfügbar ist, kann diese sehr einfach mit der Fähigkeit ausgestattet werden, den SOCKS-Proxy zu nutzen. Der einfache Socket-Aufruf muss lediglich durch den SOCKS-Socket-Aufruf ersetzt werden. Viele kommerzielle Programme, wie der Microsoft Internet Explorer, enthalten bereits die hierfür notwendige Logik.

2.4 Application-Level-Gateway (Proxy)

Dies ist die klassische Firewall-Technologie, wie sie von Marcus Ranum (siehe Kapitel 1) in der ersten Firewall implementiert wurde. Hierbei handelt es sich um Proxys, die auf der Schicht des Applikationsprotokolls arbeiten. Daher benötigt ein derartiges Gateway für jedes Applikationsprotokoll einen eigenen Proxy. Diese Application-Level-Gateways können daher meist nur eine beschränkte Anzahl von Protokollen filtern. Obwohl Sie dies als einen Nachteil dieser Technologie ansehen können, bietet diese Technologie auch Vorteile. Die Application-Level-Gateways implementieren das Applikationsprotokoll und können daher auch die korrekte Verwendung prüfen. Speziell bei komplizierten und gefährlichen Protokollen wie FTP oder HTTP können diese Proxys durch selektive Unterstützung des Protokolls die gefährlichen Befehle herausfiltern und deren Verwendung unterbinden. Ein reiner Paketfilter kann dies nicht. Hier sind zusätzliche Funktionen in Form eines Inspection- oder Deep-Inspection-Paketfilters erforderlich. Während jedoch das Application-Level-Gateway nur die erlaubten Funktionen implementiert (Positiv-Liste) und alle weiteren Verwendungen des Protokolls automatisch unterbindet, muss ein Deep-Inspection-Paketfilter die bösartige Verwendung des Protokolls erkennen und verhindern (Negativ-Liste). Der Deep-Inspection-Paketfilter kann daher nur bekannte Angriffe erkennen und verhindern, während ein Application-Level-Gateway weiter reichende Sicherheit bietet.

Dennoch haben sich in den letzten Jahren die Paketfilter in vielen Bereichen durchgesetzt. Dies hängt mit den vielen verschiedenen, teilweise sehr komplizierten modernen Protokollen zusammen. Für jedes dieser Protokolle ist ein eigener Proxy erforderlich. Deren Implementierung ist häufig so aufwendig und kompliziert, dass sie entweder gar nicht vorgenommen wird oder der Proxy anschließend selbst zu einem Sicherheitsrisiko wird, da die Implementierung Fehler aufweist.

2.5 Network Address Translation

Die Network Address Translation (NAT) wurde zunächst als Antwort auf die beschränkte Anzahl von IP-Adressen im Internet entwickelt. Mit Hilfe von NAT können viele Rechner über dieselbe IP-Adresse auf Dienste im Internet zugreifen. Hier-

für wird NAT üblicherweise auf einem Router oder der Firewall implementiert. Die IP-Adresse aller in das Internet ausgehenden Pakete wird dann von dem Router oder der Firewall durch die IP-Adresse des Routers/der Firewall selbst ersetzt. Dabei verwendet der Router/die Firewall für jede Verbindung einen eindeutigen ungenutzten lokalen Port. Die Information über die Verbindung und die verwendeten IP-Adressen und Ports speichert das Gerät in einer Tabelle ab. Sobald ein Antwortpaket das Gerät erreicht, liest das Gerät das echte Ziel aus der Tabelle ab und leitet das Paket an den entsprechenden Rechner weiter. Nach Beendigung der Verbindung oder nach Ablauf eines Zeitgebers wird die Verbindung aus der Tabelle entfernt. Dies ist ein Source-NAT, bei dem die Quelle der Verbindung *genattet*, also die Quelladresse ausgetauscht, wird.

Das Source-NAT wird häufig als Sicherheitsfunktion eingesetzt, da es auch wirksam den Zugriff auf Systeme hinter dem Router/der Firewall unterbindet. Da deren IP-Adresse unbekannt ist, ist kein Zugriff möglich, außer es existiert ein entsprechender Eintrag in der NAT-Tabelle, der Pakete, die von außen auf einer bestimmten IP/Port-Kombination ankommen, nach innen zu einem System weiterleitet. Dies ist das Destination-NAT. Dabei wird die Zieladresse einer Verbindung ausgetauscht.

Grundsätzlich ist ein Destination-NAT unter Sicherheitsaspekten kritischer zu betrachten, da es durch die Firewall den Zugriff auf interne Systeme erlaubt. Bei dem Einsatz des Destination-NAT sollte daher das interne System, auf das der Zugriff freigegeben wird, zusätzlich isoliert sein. Dies erfolgt in den meisten Umgebungen durch die Platzierung dieser Systeme in einer DMZ (siehe Abschnitt 3.2).

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

3 Firewall-Architekturen

Eine Firewall ist nicht ein einzelnes Gerät oder eine Gruppe von Geräten, sondern ein Konzept. Für die Implementierung eines Firewall-Konzepts haben sich in den vergangenen Jahren verschiedene Architekturen durchgesetzt. Diese Architekturen möchte ich Ihnen in diesem Kapitel vorstellen. Jede Architektur hat ihre Daseinsberechtigung. Es gibt keine absolut richtige Architektur. Wie bei allen anderen Betrachtungen sollten Sie immer Aufwand und Nutzen abwägen. Speziell bei der Wahl der Architektur müssen Sie den Aufwand in Form der benötigten Hardware analysieren.

Verabschieden Sie sich von dem Gedanken, eine absolut sichere Firewall aufzubauen, wenn Sie nicht das Netzwerkkabel durchschneiden wollen. Eine 100%ig sichere Firewall gibt es nicht. Daher muss Ihre Architektur mögliche Fehler in Ihrer Konfiguration und der Implementierung durch den Hersteller möglichst lange überleben, um Ihnen die Gelegenheit für eine Reaktion auf einen erfolgreichen Angriff auf Ihre Firewall einzuräumen. Ihre Firewall-Architektur sollte keinen Single-Point-of-Failure besitzen. Das ist ein Punkt, bei dessen Ausfall die Sicherheit komplett kompromittiert ist.

3.1 Screening-Router

Die erste Implementierung des Screening-Routers war der `screend` von Jeffrey Mogul. Ein Screening-Router ist im Grunde nichts anderes als ein einfacher Paketfilter, wie er in diesem Buch beschrieben wird. Als Architektur basiert die Firewall lediglich auf diesem Screening-Router und verwendet keine andere zusätzliche Struktur. Abbildung 3.1 zeigt die Architektur.

Der Screening-Router erlaubt üblicherweise nur Verbindungen von innen nach außen. Eine Verbindungsaufnahme von außen nach innen wird von dem Screening-Router unterbunden.

In vielen Umgebungen, bei denen nur der Zugriff von innen nach außen erlaubt werden soll, ist ein Screening-Router ausreichend, um die Sicherheit eines Netzes zu gewährleisten. Dies hängt sicherlich auch stark davon ab, ob auch interne Dienste angeboten werden sollen. Dann ist in vielen Fällen ein Screening-Router nicht ausreichend, und Sie sollten sich Gedanken über die Verwendung einer demilitarisierten Zone machen (siehe Abschnitt 3.2).

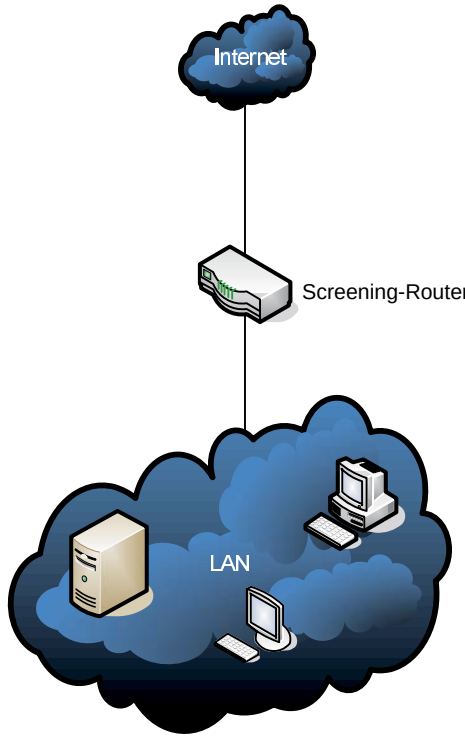


Abbildung 3.1: Ein Screening-Router schützt das interne Netz.

Ein nicht zu unterschätzender Nachteil eines einzelnen Screening-Routers ist bei einem Fehler in der Implementierung oder einem erfolgreichen Angriff das offene Netz. Wenn Ihre Firewall-Architektur nur aus einer Komponente besteht, kann ein Angreifer durch die Überwindung dieser Komponente kompletten Zugriff auf Ihr Netzwerk erhalten. Um dieses zu verhindern, sollten Sie eine mehrstufige Firewall-Architektur wie die Multiple DMZ wählen (siehe Abschnitt 3.3).

3.2 DMZ

Sobald Sie Dienste anbieten möchten, die von anderen Anwendern im Internet oder von einem nicht vertrauenswürdigen Netz genutzt werden sollen, sollten Sie sich für die Implementierung Ihres Firewall-Konzepts mit der DMZ-Architektur beschäftigen. Hierbei handelt es sich um eine demilitarisierte Zone (häufig auch entmilitarisierte Zone genannt). Dies ist ein besonderes ausgelagertes Netz, in dem Sie die Systeme positionieren, auf die ein Zugriff aus dem Internet erforderlich ist. Auch ein Proxy wird üblicherweise in dieser DMZ aufgestellt. Ein zusätzlicher Screening-Router steuert den Paketfluss, so dass aus dem internen Netz nur ein Zugriff auf die Systeme der DMZ möglich ist (siehe Abbildung 3.2).

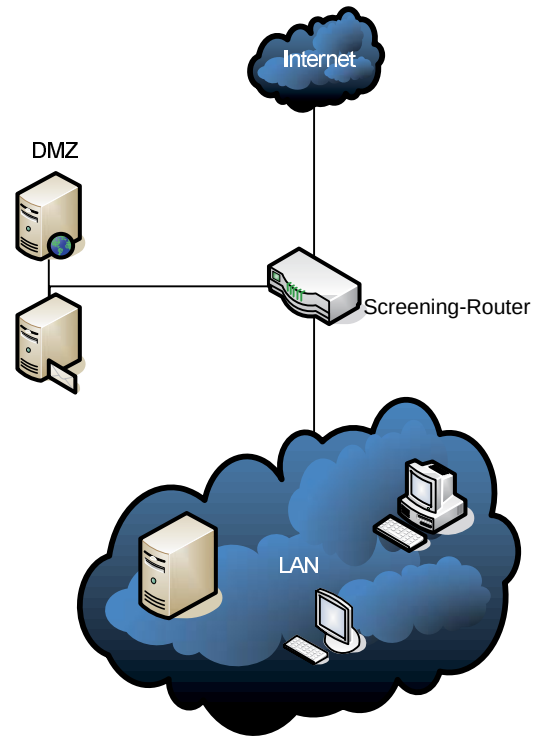


Abbildung 3.2: Die DMZ wird am einfachsten durch ein drittes Bein am Screening-Router realisiert. Der Screening-Router regelt den Paketfluss.

Ein direkter Zugriff auf das Internet wird so unterbunden[1]. Die Proxys greifen dann auf die Dienste im Internet zu und dienen dem internen Netz beim Zugriff auf das Internet als Mittelsmann. Alle Dienste, die Sie dem Internet anbieten möchten, wie zum Beispiel ein Web- und ein -Server, werden ebenfalls von Systemen in der DMZ implementiert. Da Sie diese Dienste anbieten möchten, können Sie diese Systeme nicht so schützen wie die internen Systeme, auf die kein Zugriff erlaubt wird. Bei einem erfolgreichen Angriff und Einbruch in diese weniger geschützten Systeme, sind die internen Systeme aber immer noch durch den Screening-Router geschützt, der hoffentlich nicht jeden Zugriff aus der DMZ in das interne Netz erlaubt.

Diese Kombination aus Proxys und Paketfilter erhöht die Sicherheit der geschützten Systeme. Selbst wenn Sie keine Proxys einsetzen, erhöht die Auslagerung der angebotenen Dienste aus dem internen Netz die Sicherheit desselben, da nun bei einem Angriff kein direkter Zugriff auf die weiteren Rechner des internen Netzes möglich ist.

[1] Da einige Protokolle nicht von Proxys unterstützt werden, ist für diese Protokolle häufig noch ein direkter Zugriff auf das Internet notwendig, wenn diese Protokolle genutzt werden sollen.

Dennoch basiert die Sicherheit der Architektur auf einem Single-Point-of-Failure, dem Screening-Router. Wenn der Administrator oder der Programmierer bei der Einrichtung oder Entwicklung des Screening-Routers einen Fehler macht, der erfolgreich von einem Angreifer ausgenutzt werden kann, ist der Angreifer in der Lage, auf das interne Netz zuzugreifen, da nur der Screening-Router dieses Netz schützt. Wenn dies nicht akzeptabel ist, können Sie die DMZ durch zwei Paketfilter realisieren: einen externen und einen internen Paketfilter. Der interne Paketfilter regelt den Verkehr zwischen der DMZ und dem internen Netz. Der externe Paketfilter regelt den Verkehr zwischen der DMZ und dem Rest. Dies ähnelt der multiplen DMZ (nächster Abschnitt).

3.3 Multiple DMZ

Den Begriff der multiplen DMZ verwende ich, um eine mehrstufige Firewall zu beschreiben, die über mehrere DMZs verfügt. Abbildung 3.3 zeigt das Prinzip.

Bei der multiplen DMZ existiert kein Single-Point-of-Failure. Die in Abbildung 3.3 dargestellte Architektur wird durch zwei Screening-Router realisiert, die keine direkte Verbindung besitzen. Anstatt die beiden Screening-Router direkt miteinander zu verbinden, verfügen die Application-Level-Gateways über zwei Netzwerkkarten und stehen mit jeweils einem Bein in der inneren und der äußeren DMZ. Kann der Angreifer den äußeren Screening-Router überwinden, so ist das interne Netz immer noch durch die Application-Level-Gateways und den inneren Screening-Router geschützt. Selbst wenn der Angreifer direkt ein Application-Level-Gateway angreifen könnte, wird das interne Netz immer noch von dem inneren Screening-Router geschützt. Die angebotenen Dienste besitzen nur eine Netzwerkkarte und befinden sich in der äußeren DMZ. Falls diese Dienste auf interne Datenbanken zugreifen müssen, ist der Zugriff nur über die Application-Level-Gateways möglich, oder diese Systeme benötigen für diesen Zugriff ein weiteres Bein in der inneren DMZ.

Der schiere Hardware-Aufwand und der damit einhergehende Administrationsaufwand lassen diese Lösung natürlich nur für Netze mit einem hohen Schutzbedürfnis adäquat erscheinen. Natürlich sind auch zahlreiche Variationen der Architektur denkbar.

Der Vorteil dieser Architektur ist das Fehlen des Single-Point-of-Failure. Sie haben hoffentlich beim erfolgreichen Angriff auf die Firewall genügend Zeit, mit entsprechenden Maßnahmen (Unterbrechung der Netzwerkverbindung) zu reagieren.

3.4 Wahl der Architektur

Die Wahl der richtigen Architektur ist nicht einfach. Wie schon erwähnt: eine 100%ig sichere Firewall gibt es nicht. Diese mag in Hochglanzprospekten der Hersteller existieren. In der Realität habe ich sie noch nie gefunden. Falls Sie einen Hersteller finden, der Ihnen diese verspricht, fragen Sie ihn, warum er Ihnen dann auch noch ein IDS und einen Virenscanner verkaufen möchte.

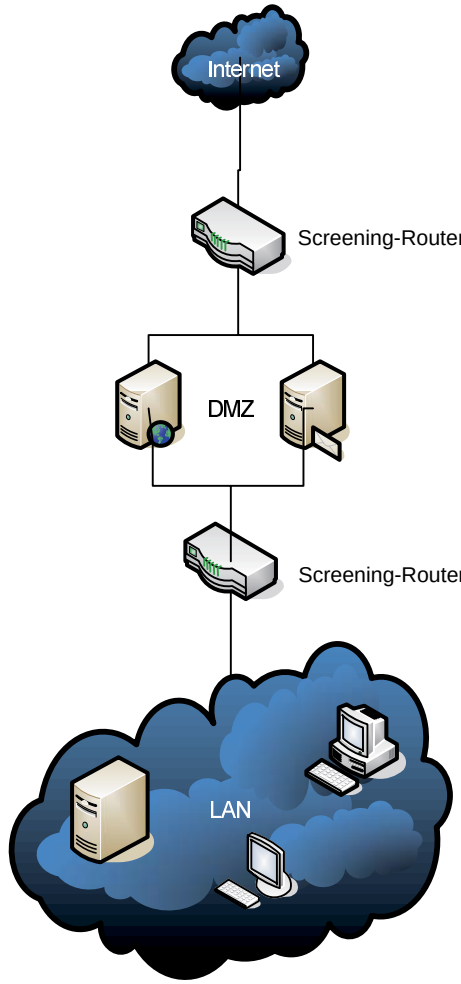


Abbildung 3.3: Bei einer multiplen DMZ gibt es keinen Single-Point-of-Failure.

Die Wahl der Architektur ist entscheidend für die Standhaftigkeit der Firewall. Vergleichen Sie Ihr Netzwerk mit einer Stadt aus dem Mittelalter. Im Mittelalter war jede Stadt in Bezug auf ihren Schutz auf sich allein gestellt. Es gab keine Polizeigewalt, die den Austausch von Waren und das Reisen zwischen den Städten überwachte. Vielmehr regierten außerhalb der Städte meistens Raubritter und Diebe. Es herrschte Anarchie, wie es heute in vielen Bereichen des Internets der Fall ist. Sobald Sie Ihr Netz mit dem Internet verbinden, sind Sie daher bezüglich der Sicherheit Ihres Netzes auch auf sich allein gestellt. Sie müssen sich, wie die Städte im Mittelalter, gegen jeden nur möglichen Angriff verteidigen. Im Mittelalter bauten die Stadtbewohner daher Burgmauern und zogen Gräben. Meist wurde nicht nur eine Mauer oder ein Graben gezogen, damit die Verteidiger ausreichend Zeit für

die Vorbereitung der Verteidigung erhielten. Musste der Angreifer nur eine Mauer überwinden, benötigte er nur genügend lange Leitern, um den Angriff erfolgreich durchzuführen. Gute Verteidigungsanlagen verfügten über mehrere Mauern und Gräben und deren Kombination, so dass die Mauer zwar mit einer Leiter überwunden werden konnte, aber der Angreifer für den Graben Boote benötigte und die Leitern nicht einsetzen konnte. Die Verteidiger hatten in der Zeit die Gelegenheit, ihr Öl zum Sieden zu bringen, um es über die Angreifer zu gießen.

Nutzen auch Sie daher in Ihrer Firewall-Architektur unterschiedliche Technologien zur Verteidigung, und bauen Sie mehrere Schutzwälle auf. Auch heute zeigt sich wie im Mittelalter, dass Angreifer häufig auch nur die schlecht geschützten Ziele angreifen. Diese werden auch als »low hanging fruits« (niedrig hängende Früchte) bezeichnet.

Gegen derartige Angriffe sind Sie mit einer mehrstufigen Firewall durch die Abschreckung gut geschützt. Falls ein Angreifer Sie tatsächlich gezielt angreift, bietet ein mehrstufiges System Ihnen hoffentlich die notwendige Zeit zur Vorbereitung der Verteidigung, bevor der Angreifer in Ihr Netz gelangt.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

4 Bedrohungen bei der Vernetzung von Systemen

Solange die Rechner nicht vernetzt waren, war die Welt noch in Ordnung. Angriffe beschränkten sich auf physikalische Zugänge. Solange die Systeme für Unbefugte unzugänglich aufgestellt wurden, war ihre Sicherheit gewährleistet. Die physikalische Sicherheit des Rechnergehäuses und des Serverraums garantierte auch die Sicherheit der vorhandenen Daten. Sobald jedoch die Rechner eine größere Verbreitung fanden und Massenspeicher in Form von Disketten zum Austausch von Daten eingesetzt wurden, tauchte eine neue Bedrohung in Form von Viren auf. Der erste funktionsfähige Virus wurde von Dr. Fred Cohen in seiner Doktorarbeit 1983 beschrieben[1]. Die tatsächliche Verbreitung begann mit der Verbreitung des IBM PCs und dem zunehmenden Informationsaustausch per Diskette und per Modem.

Durch die Vernetzung haben die Bedrohungen stark zugenommen. Der Angriff ist immer, zu jeder Zeit und von überall fast anonym durchführbar. Um sich für die Verteidigung zu rüsten, ist es wichtig, die Bedrohungen zu kennen und zu verstehen.

4.1 Angreifer und Motivation

Zunächst sollten Sie sich einige Gedanken über den potenziellen Angreifer und seine Motivation machen. Hieraus ergeben sich anschließend direkt Schlussfolgerungen zum erforderlichen Aufwand für die Sicherheit.

Die meisten Administratoren denken bei einem Angreifer zunächst an den klassischen Hacker. In den seltensten Fällen ist dieser jedoch für den Angriff verantwortlich.

4.1.1 Der klassische Hacker

Der klassische Hacker interessiert sich meist aus Neugierde für die interne Funktion eines Programms oder eines Betriebssystems. Der Hacker unterscheidet sich von dem Cracker, der – mit ähnlichem Wissen ausgestattet – versucht, in fremde

[1] Allerdings existierten auch schon früher Programme, die viele Anzeichen eines Virus aufwiesen. Diese Arbeit analysierte aber erstmalig wissenschaftlich das Phänomen.

Systeme einzudringen und dort Schaden anzurichten. Der Hacker verfügt über sehr spezialisiertes Wissen über die verwendeten Programmiersprachen und Algorithmen. Er analysiert die Softwarefunktionen und findet dabei Programmier-, Logik- oder Designfehler. Anschließend versucht er, diese Fehler auszunutzen, um das Programm zu anderen Zwecken zu gebrauchen. Ist er erfolgreich, so hat er einen so genannten *Exploit* gefunden. Seine Motivation ist meist Neugierde, Wissensdrang, Weiterbildung und »weil es möglich ist«.

Der klassische Hacker ist normalerweise nicht daran interessiert, tatsächlich in fremde Systeme einzudringen. Er veröffentlicht meist die für den Angriff erforderlichen Informationen (teilweise gegen Bezahlung).

Der Chaos Computer Club hat auf seiner Webpage (*http://www.ccc.de/hacker ethics*) eine Hacker-Ethik veröffentlicht, mit der sich wahrscheinlich die meisten Hacker identifizieren können.

4.1.2 Script-Kiddies

Der Begriff Script-Kiddie bezeichnet Angreifer, die nicht selbst in der Lage sind, eine Sicherheitslücke zu finden, zu analysieren und einen Exploit zu entwickeln. Diese Angreifer sind darauf angewiesen, dass ein anderer Hacker einen Exploit entwickelt, den sie anschließend verwenden. Häufig wird dazu der Exploit in ein Skript eingebunden. Dieses Skript wird anschließend genutzt, um eine Vielzahl von Systemen anzugreifen und dort einzubrechen.

Die Tatsache, dass von Kiddies gesprochen wird, hat keinen Bezug auf das Alter der Personen. Script-Kiddies gibt es in jedem Alter. Es soll eher abfällig zum Ausdruck bringen, dass das Script-Kiddie nicht erfahren genug ist, den Exploit selbst zu entwickeln.

Script-Kiddies werden meist durch Neugierde und die Suche nach Anerkennung in Hacker- und Möchtegern-Hackerkreisen motiviert. Hier versucht ein Script-Kiddie dadurch auf sich aufmerksam zu machen, dass er in besonders viele Systeme eingedrungen ist.

4.1.3 Insider

Eine zweite sehr gefährliche Gruppe von potenziellen Angreifern ist der Insider. Hier handelt es sich zum Beispiel um entlassene Mitarbeiter, die über internes Wissen verfügen, oder aber auch um enttäuschte Mitarbeiter, die Rache üben möchten. Des Weiteren kann es sich um Zulieferer, Berater oder andere handeln. Diese Personen sind deshalb so besonders gefährlich, da sie über interne Informationen verfügen, die anderen Angreifern nicht zugänglich sind. Dadurch können sie unter Umständen Sicherheitsvorkehrungen umgehen oder besser angreifen. Meist müssen diese Personen sich keine Gedanken um die Firewall machen, da sie über Zugänge verfügen, die nicht von der Firewall überwacht werden. Dabei kann es sich um den lokalen Zugang im Netz oder um VPN-Zugänge handeln.

Auch wenn diese Gruppe häufig nicht über so hohes technisches Wissen in Bezug auf Sicherheitslücken wie ein Hacker verfügt, ist ihre kriminelle Energie meist höher einzustufen.

4.1.4 Mitbewerber

Auch Mitbewerber gehören zu den potenziellen Angreifern. Dabei reichen teilweise sicherlich auch Denial-of-Service-Angriffe aus, um einen wirtschaftlichen Vorteil zu erhalten. Stellen Sie sich vor, Sie suchen einen neuen Partner für das Outsourcing Ihrer E-Mail-Kommunikation inklusive Spam- und Virenschutz. In der heißen Phase der Verhandlung mit zwei potenziellen Partnern ist eines der beiden Unternehmen per E-Mail nicht mehr erreichbar. Welchem der beiden potenziellen Partnern vertrauen Sie mehr? Unternehmen A, das gerade unter einem Denial-of-Service-Angriff (DoS) leidet, oder Unternehmen B, das diesen DoS durchführt oder in Auftrag gegeben hat?

Natürlich sind Ihre Mitbewerber aber auch an Ihren Daten interessiert. Wenn sich also die Gelegenheit ergibt, Zugang zu Ihrer Datenbank zu erhalten, den E-Mail-Verkehr mit Ihren Kunden mitzulesen oder Zugang zu neuen Produktentwicklungen zu erhalten, sind Ihre Mitbewerber sicherlich sehr interessiert.

Ihre Mitbewerber haben meist auch die finanziellen Möglichkeiten, hochqualifizierte Angreifer (Industriespione) zu bezahlen. So können Ihre Mitbewerber selbst dann zur Gefahr werden, wenn sie selbst über kein entsprechendes Wissen verfügen.

4.1.5 Geheimdienste

Die Geheimdienste waren schon immer an allen Informationen interessiert. Sie hören die Kommunikation zwischen Regierungen, aber auch zwischen Unternehmen ab. Häufig betreiben sie auch Wirtschaftsspionage mit nationalem Interesse, um Unternehmen aus dem eigenen Land einen Wettbewerbsvorteil zu verschaffen. Die Nachrichtendienste verfügen meist über ausreichend finanzielle Mittel, die erforderlichen Kenntnisse sowie die notwendigen Netzwerke und Computer, um Angriffe und Einbrüche durchzuführen. Sie sind auch in der Lage, schwach verschlüsselte Informationen sehr einfach und schnell zu entschlüsseln.

Schließlich besitzen sie häufig auch die Möglichkeit, sich physikalischen Zugang zu bestimmten Informationen zu verschaffen, wenn ein Computerangriff nicht erfolgreich ist. Häufig ist ein physikalischer Einbruch sogar einfacher.

4.1.6 Terroristen und organisierte Kriminalität

Auch Terroristen und das organisierte Verbrechen erkennen im Internet immer mehr ein Potenzial für ihre Geschäfte – sowohl, um eigene Geschäfte über das Internet abzuwickeln, als auch, um durch Angriffe und Einbrüche an sensitive Daten heranzukommen.

So sind die Phishing-Angriffe der Jahre 2004 und 2005 sicherlich noch nicht vorbei. Beim Phishing versuchen organisierte Banden gezielt an Login-Informationen zu gelangen. Auch der Versand von Spam ist immer mehr ein Geschäft von wenigen organisierten Banden. Dabei werden kompromittierte Rechner unwissender Anwender genutzt, um in großer Zahl E-Mails zu versenden, die den Empfänger zum Kauf von Viagra bewegen sollen.

2004 wurde auch bekannt, dass ein Erpresserring versucht hat, Online-Wettbüros mit DoS-Angriffen zu erpressen. Der Erpresserring verfügte angeblich über Kontakte zur russischen Mafia (siehe c't 14/2004 und *http://www.heise.de/ct/04/14/048/default.shtml* und *http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/49292*).

Viele Angriffe sind auch politisch motiviert. So wurden nach dem 11. September 2001 besonders viele Angriffe auf muslimische Websites unternommen.

Derartige Angriffe werden sicherlich in nächster Zukunft stark weiter zunehmen und weitere Medien entdecken. Ich selbst befürchte schon für das Medium VoIP ähnliche Entwicklungen, wie wir sie im Moment bei E-Mail mit Spam erleben. Der Begriff für VoIP-Spam ist bereits gefunden worden. Diese Form wird als SPIT (Spam via Internet-Telefonie) bezeichnet.

4.2 Tendenzen und Entwicklungen

Wenn man nun die potenziellen Angreifer, ihr Know-how und ihre kriminelle Energie betrachtet, kann man recht einfach die Grafik 4.1 erzeugen. Diese Grafik zeigt, dass das größte GefahrenPotenzial von den Geheimdiensten und den Industriespionen ausgeht, die von Mitbewerbern angeheuert werden.

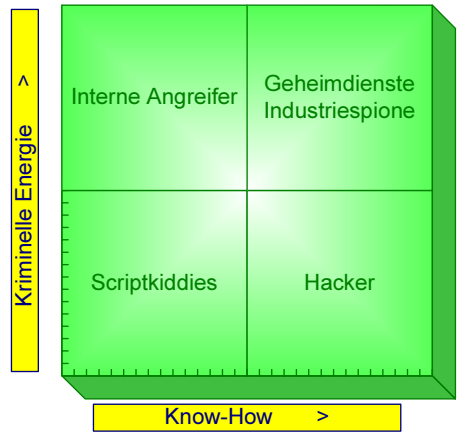


Abbildung 4.1: Das Risiko eines erfolgreichen Angriffs steigt mit steigender krimineller Energie und steigendem Know-how.

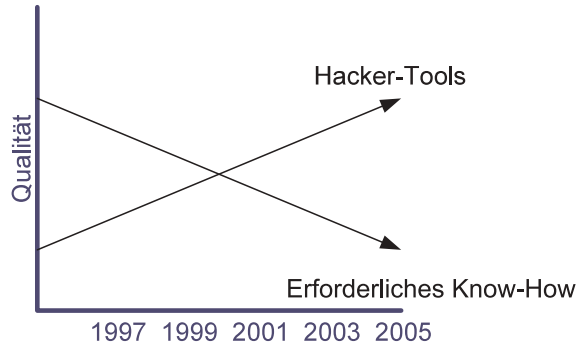


Abbildung 4.2: Die Qualität der Angriffswerkzeuge nimmt seit einigen Jahren stark zu. Das notwendige Know-how sinkt daher stetig.

Allerdings sollten Sie auch die Insider nicht aus den Augen verlieren. Ihre hohe kriminelle Energie macht sie besonders gefährlich. Die Script-Kiddies sind meist zu vernachlässigen. Sie führen keine gezielten Angriffe auf Sie durch, sondern suchen meist allgemein nach verwundbaren Systemen. Sie suchen die niedriger hängenden Früchte, die leicht zu erreichen und anzugreifen sind. Ein gezielter Angriff gegen Ihre Systeme durch Script-Kiddies ist unwahrscheinlich, wenn Sie Ihre Hausaufgaben gemacht haben, Ihre erreichbaren Systeme ordentlich gepatcht sind und Sie über eine Firewall verfügen. Dann zählen Sie nicht zu den niedrig hängenden Früchten. Dennoch müssen Sie möglicherweise mit gezielten Angriffen durch Mitbewerber, Industriespione etc. rechnen. Hier kommt erschwerend hinzu, dass in den letzten Jahren die Angriffswerkzeuge immer besser geworden sind und das erforderliche Know-how des Durchschnittseindringlings entsprechend abgenommen hat (siehe Abbildung 4.2)

4.3 Schutzziele

In diesem Abschnitt möchte ich ganz allgemein die zu schützenden Ziele beschreiben. Im Grunde gibt es vier Ziele beim Schutz von Netzen, Rechnern und Daten:

- Integrität
- Vertraulichkeit
- Authentizität
- Verfügbarkeit

Datenintegrität bedeutet, dass eine Änderung der Daten durch Unbefugte nicht unbemerkt bleibt. Die Integrität von Daten wird üblicherweise durch kryptographische Prüfsummen erreicht.

Die Vertraulichkeit der Daten wird meist mit Hilfe von eingeschränkten Leserechten und zusätzlicher Verschlüsselung erreicht. Nur autorisierte Personen erhalten den

Schlüssel für die Entschlüsselung. Das Abhören einer Kommunikation oder das Ausspähen von Daten wird so unmöglich.

Die Authentizität stellt sicher, dass die Daten aus der richtigen Quelle stammen. In einer Kommunikationsbeziehung wird dies durch Authentifizierungen und digitale Signaturen erreicht.

Die Verfügbarkeit von Daten wird häufig vernachlässigt. Dieses Ziel verlangt, dass die gewünschten Daten jederzeit verfügbar sind. Hier werden häufig technische Hilfsmittel, wie Backups, unterbrechungsfreie Stromversorgungen, Cluster etc. genutzt, um die Verfügbarkeit zu sichern.

Sie mögen sich fragen, was diese Ziele nun mit einer Firewall zu tun haben. Eine Firewall ist auch ein Werkzeug, um diese Sicherheitsziele zu erreichen. Sie sichert die Integrität der lokal gespeicherten Daten, indem sie nichtautorisierte Kommunikationsanfragen, zum Beispiel an den Datenbankserver, ablehnt. Sie stellt die Vertraulichkeit von Daten sicher, indem sie verhindert, dass bestimmte Kommunikationsverbindungen von und nach außen aufgebaut werden können. Die Authentizität kann eine Firewall nur begrenzt prüfen. Sie schützt aber vor einfachen Spoofing-Angriffen. Schließlich kann sie auch die Verfügbarkeit der Daten durch die Abwehr eines Denial-of-Service-Angriffs garantieren oder selbst hochverfügbar die Internetanbindung sicherstellen.

In größeren Unternehmen gibt es neben diesen sehr technischen Zielen auch formale Ziele. Hierzu gehören zum Beispiel die Nachvollziehbarkeit der Datenverarbeitung. Jeder Vorgang, zum Beispiel in einer Bank, muss nachvollziehbar sein. Auch die Revisionssicherheit spielt hier häufig eine große Rolle. Die Revisionssicherheit verlangt zusätzliche Protokolle, Erhebungen, Inventuren und spezielle Formen der Datenspeicherung und -haltung. Schließlich spielen auch gesetzliche Rahmenbedingungen eine große Rolle. Das können einfache Gesetze sein, wie zum Beispiel der Datenschutz personenbezogener Daten, aber auch sehr komplexe gesetzliche Rahmenbedingungen, wie Basel-2 und der Sarbanes-Oxley-Act. Da viele Unternehmen heute global arbeiten, unterliegen sie auch international gültigen Gesetzen.

Auch bei der Einhaltung und Erfüllung dieser Rahmenbedingungen kann eine Firewall eine wichtige Aufgabe spielen. Gerade die Protokollierung durch eine Firewall wird hier häufig betroffen sein. Während der Datenschutz das Protokollieren personenbezogener Daten hier kritisch sehen wird, werden andere Personen in den Protokollen wertvolle Hilfsmittel zur Revisionssicherheit und Sicherstellung der Nachvollziehbarkeit sehen.

Falls Sie nicht eine Firewall für ein Unternehmen der Fortune500 aufbauen wollen, sind diese letzten Überlegungen möglicherweise für Sie uninteressant. Dennoch sollten Sie zum Beispiel den Datenschutz nicht aus dem Blickfeld verlieren. Hier müssen Sie sich bei einer Firewall möglicherweise ausführlich Gedanken machen.

4.4 Angriffsmethoden

Die meisten Angriffe lassen sich in wenigen Gruppen kategorisieren. Im Folgenden stelle ich Ihnen die wichtigsten Kategorien vor.

Hinweis

Ich konzentriere mich im Weiteren auf die sehr technische Seite der möglichen Angriffe über ein Netzwerk. Daneben gibt es natürlich auch noch:

- **Social Engineering**. Hier versucht der Angreifer, durch soziale Kompetenz vertrauliche Informationen, wie zum Beispiel Kennwörter, zu erhalten. Hierzu täuscht er einen legitimen Benutzer, einen Administrator oder andere vertrauenswürdige Personen vor. Kevin Mitnick hat ein sehr eindrucksvolles Buch zu diesem Thema geschrieben (The Art of Deception, Kevin Mitnick, 2003).
- **War Dialing**. Anstatt den direkten Zugang durch eine Firewall zu suchen, bemüht sich der Angreifer, alternative Zugänge über unbewachte Modem- oder ISDN-Zugänge zu finden. Hierfür verwendet er Software, die jede erdenkliche Telefonnummer eines Unternehmens anwählt und die Antwort testet.

Zunächst gibt es die große Menge der Denial-of-Service-Angriffe. Hier versucht der Angreifer nicht, die Kontrolle über das System zu erhalten, sondern die Funktion des Systems zu stören. Beim Spoofing täuscht der Angreifer eine falsche Identität als Client oder Server vor. Beim Hijacking versucht ein Angreifer, eine aufgebaute Verbindung zu kapern. Ein Bufferoverflow kann auch einen Denial-of-Service auslösen. Jedoch versucht der Angreifer, wenn möglich mit einem Bufferoverflow die Kontrolle über das System zu übernehmen. Der Bufferoverflow wird durch Programmierfehler in den betroffenen Applikationen möglich. Der Formatstring-Angriff ist dem Bufferoverflow sehr ähnlich und erlaubt den Angreifer ebenfalls häufig die Übernahme der Kontrolle. Bei der Race-Condition handelt es sich um einen Fehler in der Programmlogik. Hierbei konkurrieren zwei Prozesse um eine Ressource. Wenn der Programmierer die Ressource nicht richtig vor dem Zugriff des zweiten Prozesses geschützt hat, kann der Angreifer dies ausnutzen. Die SQL-Injektion ist ein typischer Angriff auf Webserver mit dynamischen datenbankgestützten Webseiten. Hier versucht der Angreifer, die von der Webapplikation verwendeten SQL-Abfragen zu modifizieren. So kann er auf Daten zugreifen, die die Webapplikation normalerweise nicht ausgeben würde, oder sogar die Daten in der Datenbank modifizieren.

Im Folgenden werden die verschiedenen Angriffsmethoden ausführlicher dargestellt. Ich werde Ihnen dann auch verschiedene Möglichkeiten der Abwehr nennen.

4.4.1 Denial-of-Service (DoS)

Bei einem Denial-of-Service stört der Angreifer die Funktion eines Dienstes so, dass ein legitimer Nutzer nicht mehr auf diesen Dienst zugreifen kann. Im einfachsten Fall verübt bereits eine Putzfrau, die mit ihrem Staubsauger das Kabel eines Servers aus der Steckdose zieht, bereits unwissentlich einen DoS.

Es gibt viele verschiedene Möglichkeiten, einen DoS durchzuführen. Diese entsprechen den verschiedenen Schichten, auf denen die Kommunikation erfolgt.

- Der Angreifer kann versuchen, die Netzwerkbandbreite des Servers komplett auszulasten, so dass weiterer Verkehr nur sehr langsam transportiert wird. Dieser Angriff erfolgt also auf der physikalischen Schicht und ist durch deren Bandbreite begrenzt. Es ist heute sehr schwierig geworden, diesen Angriff durchzuführen, da die Bandbreiten in den letzten Jahren stark zugenommen haben. Der Angreifer benötigt enorme Ressourcen, um sein Ziel zu erreichen.

  Allerdings ist es mit so genannten Bot-Netzen sehr wohl möglich, den nötigen Netzwerkverkehr zu generieren. Bot-Netze sind trojanisierte Rechner (meist Microsoft Windows), die zu Tausenden in einem Netz zusammengeschlossen wurden und gemeinsam von dem Angreifer gesteuert werden. Ein Bot-Netz wird häufig für den Versand von Spam-E-Mails verwendet.

  Ein Schutz vor diesem Angriff ist nur mit Unterstützung des Providers möglich, der den Verkehr vielleicht vorher filtern kann. Werden jedoch die Absenderadressen der Pakete gefälscht und diese Pakete von vielen verschiedenen Systemen verschickt, ist das sehr schwer.

- Der nächste mögliche DoS-Angriff greift den TCP-Stack des Servers an und führt einen SYN-Flood durch. Der Angreifer generiert viele TCP-SYN-Pakete. Hierbei handelt es sich um Pakete, die einen Verbindungsaufbau anzeigen. Der Server antwortet auf dieses Paket mit einem SYN/ACK-Paket. Damit sich der Server später an diesen Verbindungsaufbau erinnern kann, speichert er die Verbindungsinformationen in einer Tabelle ab, in der alle schwebenden Verbindungen vorgehalten werden (Pending Connections). Sobald das dritte Paket, das TCP-ACK-Paket des Clients, erhalten wird, erhält die Verbindung den Status einer aufgebauten Verbindung und wird aus der Pending-Connections-Tabelle gelöscht und in der Tabelle der aufgebauten Verbindungen (Established Connections) eingetragen.

  Bei einem SYN-Flood überflutet der Angreifer den Server mit einer Vielzahl von TCP-SYN-Paketen. Hierbei fälscht der Angreifer zufällig die Absenderadresse der Pakete. Sinnvoll sind hier Absenderadressen von nicht existenten Rechnern. Der Server wird auf alle TCP-SYN-Pakete mit einem TCP-SYN/ACK-Paket antworten und diese Verbindungen in die Pending-Connections-Tabelle eintragen. Diese Tabelle weist jedoch (ähnlich allen anderen Tabellen in Computern) nur eine begrenzte Größe auf. Sendet der Angreifer mehr Pakete, als Verbindungen in dieser Tabelle gespeichert werden können, so muss der Server Verbindungen aus dieser Tabelle löschen.

Erfolgt gleichzeitig zum SYN-Flood ein korrekter Verbindungsaufbau durch einen echten Client, so kann der Server nicht zwischen dieser Verbindung und den Verbindungen des Angreifers unterscheiden. Sendet der Angreifer die TCP-SYN-Pakete so schnell, dass der Server auch die echte Verbindung aus der Tabelle der Pending Connections entfernen muss, bevor das dritte Paket des TCP-Handshakes vom Client empfangen wird, so wird der Server dieses Paket zurückweisen, da er keine Informationen über die Verbindung mehr besitzt. Die Verbindung wird abgebrochen und der Dienst steht nicht mehr zur Verfügung.

Viele TCP-Implementierungen brechen ab 100 TCP-SYN-Paketen pro Sekunde zusammen. Linux bietet die SYN-Cookies . Diese erlauben immer noch einen Verbindungsaufbau bei einem SYN-Flood mit bis zu 100.000 SYN-Paketen pro Sekunde. Hierbei wird die Tabelle der Pending Connections ignoriert und lediglich auf Basis der Sequenznummer über einen Verbindungsaufbau entschieden. Die Funktionsweise wird in Kapitel 23 beschrieben.

4.4.2 Spoofing

Spoofing bezeichnet Angriffe, bei denen der Angreifer bestimmte Informationen fälscht. Meist erfolgt dies, um die Identität eines anderen Rechners anzunehmen. Drei verschiedene Arten des Spoofings werden heute durchgeführt. Hierbei handelt es sich um:

- **IP-Spoofing.** Bei dem IP-Spoofing verändert der Angreifer den IP-Header seiner Pakete. Meist fälscht er seine Absender-IP-Adresse. Hiermit kann er die Identität eines anderen Rechners annehmen. Dies erfolgt, um entweder seine Spuren zu verwischen oder um Vertrauensstellungen zwischen gewissen Rechnern auszunutzen.
- **ARP-Spoofing.** Dies wird besonders von Angreifern in geswitchten Netzen eingesetzt, um trotz des Einsatzes eines Switches weiterhin sämtliche ausgetauschten Pakete zu protokollieren. Hierbei werden ARP-Antworten gefälscht. Außerdem wird es für ein TCP-Session-Hijacking verwendet (s.u.).
- **DNS-Spoofing.** Hierbei fälscht ein Angreifer die Zuordnung eines DNS-Namens zu einer IP-Adresse, indem er die Antwort eines DNS-Servers fälscht.

IP-Spoofing

Dies ist die älteste Variante des Spoofings. Hierbei täuscht der Angreifer eine andere IP-Adresse als Absender vor. Dies wird zum Beispiel beim SYN-Flood verwendet, um die eigenen Spuren zu verwischen.

Das IP-Spoofing kann jedoch auch für einen direkten Angriff genutzt werden. Bei dem SMURF-Angriff sendet der Angreifer ein ICMP-Echo-Request-Paket an die Broadcast-Adresse eines Netzwerks. Sämtliche Unix-Rechner dieses Netzwerks reagieren mit einem ICMP-Echo-Reply-Paket. Der Angreifer erhält hiermit also eine Multiplikation seiner Pakete. Fälscht der Angreifer nun die Absenderadresse so, dass sie die IP-Adresse des anzugreifenden Rechners darstellt, antworten alle Unix-

Rechner bei einem Broadcast-Ping an diesen Rechner. Erfolgt dies häufig genug, so besteht die Möglichkeit, die Netzwerkverbindung des angegriffenen Rechners zu überlasten. Jedoch ist die Antwort auf ein Broadcast-Echo-Request-Paket nur eine Eigenschaft von Unix-Systemen, die heute meist von dem Hersteller oder dem Administrator abgestellt wird.

Schließlich kann das IP-Spoofing auch verwendet werden, um Vertrauensstellungen zwischen Rechnern auszunutzen. Das UDP-Protokoll bietet keinen Schutz vor gespooften Paketen, da es nicht verbindungsorientiert arbeitet. Bei einer TCP-Verbindung genügt nicht das Fälschen der IP-Adresse. Der Angreifer muss darüber hinaus auch die Sequenz- und Acknowledgement-Nummern spoofen.

Erlaubt zum Beispiel ein Syslogd-Server die Protokollierung von Meldungen mit dem UDP-Protokoll nur bestimmten IP-Adressen, so genügt es in diesem Fall, wenn der Angreifer die IP-Adresse entsprechend fälscht. Das Paket wird dann akzeptiert und die Meldung dementsprechend protokolliert, als käme sie von dem korrekten Rechner.

Ein Schutz vor IP-Spoofing ist nur auf einer Firewall möglich. Hierbei sollten Sie darauf achten, dass die Firewall keine unzulässigen IP-Adressen akzeptiert. Wenn in Ihrer DMZ Adressen aus dem Netzwerk 192.168.0.0/24 verwendet werden, dann dürfen Anfragen aus diesem physikalischen Netz keine andere Absenderadresse verwenden.

ARP-Spoofing

Beim ARP-Spoofing verfolgt der Angreifer entweder das Ziel, ein TCP-Session-Hijacking durchzuführen (s.u.) oder in einer Umgebung, die durch einen Switch kontrolliert wird, dennoch einen Netzwerksniffer einzusetzen.

Der zweite Angriff soll hier ein wenig ausführlicher betrachtet werden.

Wenn zwei Netzwerkgeräte sich mit dem IP-Protokoll unterhalten möchten, so benötigen sie in einem Ethernet-Netzwerk für die eigentliche Kommunikation zunächst auch noch die Ethernet-MAC-Adressen. Hierfür ist das ARP-Protokoll zuständig. Der Rechner, der ein IP-Paket an die IP-Adresse des Zielsystems senden möchte, sendet zunächst einen ARP-Request, um die dazugehörige MAC-Adresse zu ermitteln. Anschließend sendet er das IP-Paket an die IP-Adresse des Zielsystems und den Ethernet-Rahmen an die MAC-Adresse des Zielsystems.

Wird aus Geschwindigkeitsgründen in diesem Netzwerk ein Switch eingesetzt, so wird dieser zunächst den ARP-Request, da dieser an die Broadcast-Ethernet-Adresse gerichtet ist, an alle angeschlossenen Geräte weiterleiten. Der anschließend versandte Ethernet-Rahmen mit IP-Paket wird jedoch vom Switch nur an das tatsächliche Ziel versandt. Um dies zu ermöglichen, besitzt der Switch eine Liste, in die MAC-Adressen der angeschlossenen Geräte abgespeichert werden.

Bei dem ARP-Spoofing-Angriff (Abbildung 4.3) fälscht der Angreifer (Laptop) den ARP-Reply.

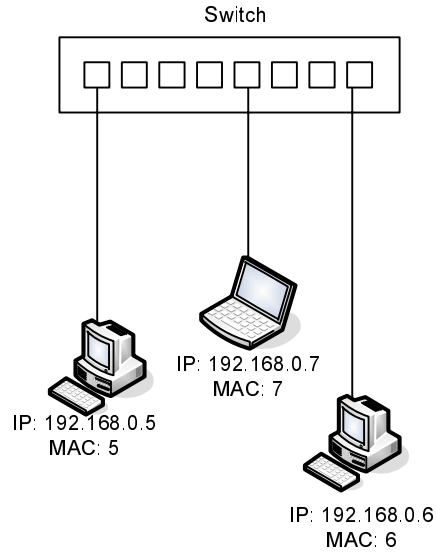


Abbildung 4.3: ARP-Spoofing bei einem Switch.

1. Der Rechner 192.168.0.5 möchte ein Paket an den Rechner 192.168.0.6 senden. Er sendet einen ARP-Request: Welche MAC-Adresse hat der Rechner 192.168.0.6?

2. Der Angreifer beantwortet diese Anfrage nun. Hierzu fälscht er die Antwort, indem er Folgendes sendet: Der Rechner mit der IP-Adresse 192.168.0.6 besitzt die MAC-Adresse **7**.

3. Der Rechner 192.168.0.5 sendet nun sein IP-Paket an: Ziel-IP: 192.168.0.6; Ziel-MAC: 7. Der Switch ist nicht in der Lage, die IP-Adressen zu lesen. Er arbeitet lediglich auf der Ebene der MAC-Adressen. Er schlägt in seiner Tabelle nach und stellt fest, dass das Netzwerkgerät mit der MAC-Adresse **7** an Port 4 angeschlossen ist, und leitet das Paket an diesen Port weiter.

4. Der Angreifer muss auf seinem Rechner eine Routing-Software aktivieren. Der Rechner des Angreifers erhält nun das Paket und verarbeitet es, da es an die MAC-Adresse seiner Netzwerkkarte gerichtet ist. Es ist jedoch nicht an seine IP-Adresse gerichtet. Dies ist typisch für einen Router. Wurde das Routing aktiviert, so leitet dieser Rechner das Paket nun an die IP-Adresse 192.168.0.6 und die MAC-Adresse 6 weiter. Als Absender trägt er die IP-Adresse 192.168.0.5 und seine eigene MAC-Adresse 7 ein. Der Switch wird dieses Paket nun beim richtigen Empfänger zustellen. Dieser wird das Paket verarbeiten und umgekehrt antworten.

Es existieren fertige Werkzeuge, die in der Lage sind, unter Linux ein ARP-Spoofing durchzuführen. Ein Schutz vor ARP-Spoofing ist nur durch die folgenden Maßnahmen erreichbar:

- **Statische ARP-Tabellen.** Die Pflege dieser Tabellen ist aber sehr aufwendig. Sie können unter Linux einen statischen Eintrag mit dem Befehl `arp -s "ip" "mac"` erzeugen.
- **ARPwatch.** Der ARPwatch-Daemon ist in den meisten Linux-Distributionen enthalten und ist eine Art ARP-Intrusion-Detection-System. Er überwacht alle ARP-Pakete und meldet Änderungen und damit auch Angriffe.
- **Port-Security.** Viele professionelle Switches sind verwaltbar und bieten die Möglichkeit, die Anzahl der an einem Port erlaubten MAC-Adressen zu beschränken. Bei Überschreitung schaltet der Switch den Port ab.

DNS-Spoofing

Das DNS-Spoofing führt einen Angriff auf DNS-Ebene durch, der dem Angriff auf ARP-Ebene gleicht. Ein Beispiel wird in der Abbildung 4.4 dargestellt.

Beim DNS-Spoofing sind die folgenden Schritte erforderlich:

1. Der Client 192.168.0.5 möchte eine Netzwerkverbindung mit dem Rechner *www.sparkasse.de* aufbauen. Hierzu benötigt er zunächst die IP-Adresse dieses Rechners. Um diese zu ermitteln, kontaktiert er seinen DNS-Server und fragt ihn nach der IP-Adresse von *www.sparkasse.de*.
2. Da für diese DNS-Anfrage üblicherweise zunächst das UDP-Protokoll eingesetzt wird, existiert kein Schutz gegen gespoofte Pakete. Der Angreifer antwortet an der Stelle des echten DNS-Servers (schneller als der echte DNS-Server) und teilt dem Client mit, dass der Rechner *www.sparkasse.de* die IP-Adresse 192.168.0.7 aufweist.

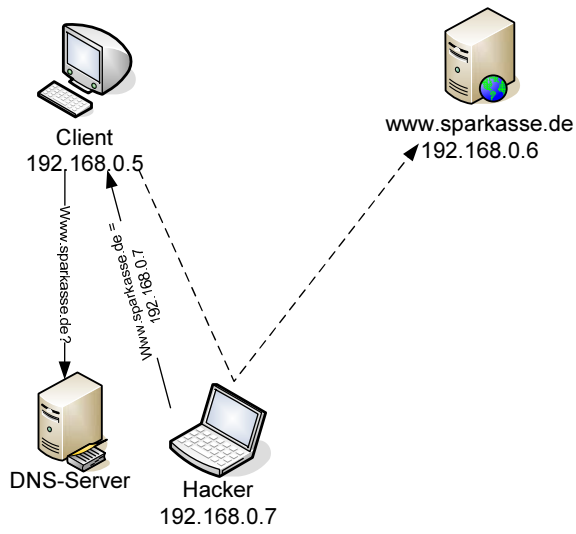


Abbildung 4.4: DNS-Spoofing

3. Der Client wird sich nun mit diesem Rechner verbinden und in Wirklichkeit den Rechner *www.sparkasse.de* erwarten. Damit der Client diese Illusion erhält, richtet der Angreifer auf dem Rechner einen Proxy ein, der sämtliche Anfragen an den echten Rechner weiterleitet und die Anworten an den Client übermittelt.

4. Dieser Angriff ist leicht durch die Verwendung von SSL zu vereiteln. Dazu ist aber zusätzlich erforderlich, dass der Client das SSL-Protokoll auch korrekt einsetzt und die Authentifizierung des Servers überprüft.

Es existieren fertige Werkzeuge, die in der Lage sind, unter Linux ein DNS-Spoofing durchzuführen. Auch existieren Werkzeuge, die dann als SSL-Proxy versuchen, eine SSL-Verbindung zu unterwandern. Wenn der Client die SSL-Zertifikate nicht richtig prüft, kann ein Angreifer so eine Verbindung abhören.

Gespoofter Portscan

Normalerweise ist ein gespoofter Portscan nicht möglich. Bei einem Portscan versucht der Angreifer, Daten über das untersuchte System zu ermitteln. Spooft er jedoch seine Absenderadresse, so erhält er nie das Ergebnis seines Scans.

Verschiedene Werkzeuge wie zum Beispiel Nmap (*http://www.nmap.org*) versuchen das Problem zu lösen, indem sie jedes Paket in einem Scan mehrfach senden. Alle zusätzlichen Pakete weisen eine gefälschte Absenderadresse (so genannte Decoys) auf. Dies erschwert eine Analyse und Bestimmung des Ursprungs des Portscans sehr oder macht diese Bestimmung sogar unmöglich.

Jedoch gibt es auch die Möglichkeit, einen echten gespooften Portscan durchzuführen. Hierzu ist ein dritter Rechner erforderlich. Dieser Rechner sollte gleichzeitig keine aktiven Netzwerkverbindungen besitzen. Daher wird er als *Silent Host* bezeichnet. Abbildung 4.5 demonstriert die Vorgehensweise.

Der Angreifer sucht zunächst einen so genannten *Silent Host*. Dies ist ein Rechner, der gleichzeitig keine anderen Netzwerkverbindungen unterhält. Hierbei kann es

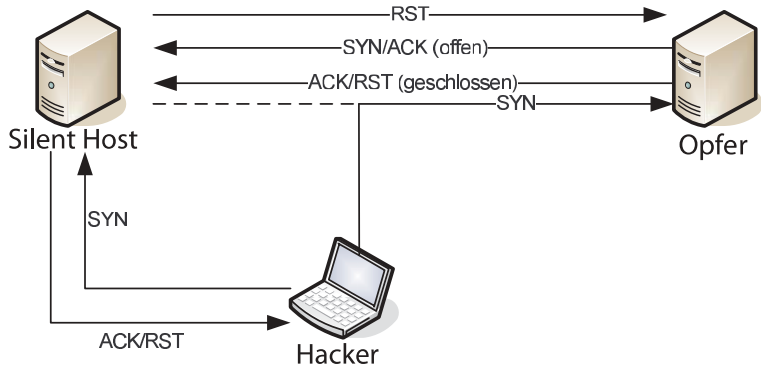


Abbildung 4.5: Gespoofter Portscan

sich zum Beispiel um einen Windows 98-Rechner einer asiatischen Universität handeln. Er beginnt nun, TCP-SYN-Pakete in regelmäßigen Abständen (1/Sekunde) an einen geschlossenen Port zu senden. Er erhält für jedes Paket ein TCP-RST/ACK-Paket zurück. Diese Pakete weisen eine steigende IP-Identifikationsnummer auf (Abbildung C.2 auf Seite 601). Wenn der Rechner gleichzeitig keine weiteren Pakete versendet, so wird diese Nummer immer um 1 inkrementiert. (Achtung: Windows vertauscht die beiden Bytes der Identifikationsnummer. Unter Linux erscheint damit der Inkrementierungsschritt als 256.)

Nun beginnt der Angreifer mit dem Portscan. Er sendet mehrere TCP-SYN-Pakete in den gleichen regelmäßigen Abständen an das Opfer. Hierbei fälscht er die Absenderadresse so, dass das Opfer seine Antworten an den *Silent Host* sendet. Es existieren nun zwei Möglichkeiten: Der Port ist offen, oder der Port ist geschlossen.

1. **Offen:** Wenn der Port auf dem Opfer offen ist, so antwortet das Opfer mit einem TCP-SYN/ACK-Paket an den *Silent Host*. Dieser kann dieses Paket nicht zuordnen und sendet ein TCP-RST-Paket an das Opfer. Damit ist die Verbindung für alle beendet.

2. **Geschlossen:** Wenn der Port auf dem Opfer geschlossen ist, so antwortet das Opfer mit einem TCP-RST/ACK-Paket an den *Silent Host*. Dieser reagiert auf das Paket nicht mit einem weiteren Paket.

Da der *Silent Host*, wenn der Port auf dem Opfer offen war, nun weitere Pakete in regelmäßigen Abständen an das Opfer versendet, wird die IP-Identifikationsnummer der Pakete, die vom *Silent Host* an den Angreifer gesendet werden, immer um 2 inkrementiert. Dies ist ein Zeichen, dass der Port offen war. Ändert sich dies nicht, so war der Port geschlossen.

Das Opfer vermutet, dass es vom *Silent Host* gescannt wird. Wenn der *Silent Host* nicht durch eine Firewall überwacht wird, so kann die Herkunft des Portscans nicht festgestellt werden.

Nmap kann diesen Scan seit einigen Versionen auch durchführen. Hier heißt der Scan »Idle-Scan« und der Silent-Host wird als »Zombie« bezeichnet. Sie benötigen also nicht unbedingt `hping`, wenn Sie bereits Nmap installiert haben.

Vor diesem Scan können Sie sich nicht schützen. Sie sollten lediglich bei der Analyse der Protokolle Ihrer Firewall darauf achten, dass fast alle Informationen in den Protokollen falsch sein können.

4.4.3 Session Hijacking

Der Mitnick-Angriff hat die Verwundbarkeit des TCP-Protokolls vorgeführt, wenn die initialen Sequenznummern vorhergesagt werden können. Aber selbst wenn das nicht der Fall ist, ist ein Übernehmen der Verbindung durch einen Angreifer (Session Hijacking) möglich. Hierzu ist es jedoch erforderlich, dass der Angreifer in

der Lage ist, die Verbindung zu beobachten. Er kann dann die verwendeten TCP-Sequenznummern direkt von den ausgetauschten Paketen ablesen.

Durch eine sinnvolle Konstruktion von gespooften Paketen ist es dann möglich, eigene Daten in diese Verbindung zu injizieren. Dieser Angriff war in der Vergangenheit sehr kompliziert und schwer durchzuführen. Seit einigen Jahren existieren jedoch mehrere Werkzeuge, die dies stark vereinfachen. Die bekanntesten Werkzeuge sind `juggernaut` und `hunt`.

Im Folgenden soll schematisch die Funktionsweise von `hunt` erläutert werden.

1. Wenn `hunt` eine laufende Verbindung beobachtet, so ist es in der Lage, diese Verbindung zu übernehmen. Das Programm `hunt` ist hierbei für Rlogin- und Telnet-Verbindungen optimiert. Der Angriff erfolgt, in dem `hunt` sowohl den Client als auch den Server davor überzeugt, dass sie die Pakete an andere MAC-Adressen versenden müssen (ARP-Spoofing). Anschließend senden sowohl Client als auch Server weiterhin korrekte TCP/IP-Pakete. Diese werden jedoch nicht mehr von der Gegenseite gesehen, da sie an falsche und unter Umständen nicht existente MAC-Adressen gerichtet sind. `hunt` sieht jedoch weiterhin diese Pakete und ist in der Lage, die wichtigen Informationen zwischen Client und Server auszutauschen.

2. Nun kann `hunt` weitere Informationen in den Fluss dieser Verbindung injizieren. Da `hunt` die TCP-Pakete sieht, kann `hunt` die erforderlichen Sequenznummern berechnen.

3. Der Server wird den Empfang der zusätzlichen Daten bestätigen. Da er jedoch das ACK-Paket an die korrekte IP-Adresse des Clients sendet, aber die falsche MAC-Adresse nutzt, sieht der Client diese Bestätigung nicht und sendet keine Fehlermeldung an den Server. `hunt` ist weiterhin in der Lage, weitere Daten mit der Vertrauensstellung des Clients an den Server zu senden.

4. Nachdem die Injektion erfolgt ist, bestehen zwei grundsätzliche Möglichkeiten. `hunt` ist in der Lage, die Verbindung mit einem RST-Paket abzubrechen. `hunt` ist aber auch in der Lage, die Verbindung zu resynchronisieren. Hierbei werden einige Daten an den Client und den Server gesendet. Außerdem ist es erforderlich, dass der Benutzer auf dem Client weitere Daten eingibt. Dann kann eine Resynchronisation erfolgreich sein. Der Client hat den Eindruck, dass die Netzwerkverbindung lediglich vorübergehend ausgefallen ist.

Das Werkzeug `hunt` ist auf der Homepage von Pavel Krauz erhältlich (*http://lin.fsid.cvut.cz/~kra/index.html*). Leider funktioniert diese URL aktuell nicht. Sie können das Werkzeug aber alternativ von *http://packetstorm.linuxsecurity.com/sniffers/hunt/* herunterladen.

Die TCP/IP-Protokolle bieten keinen Schutz vor diesen Angriffen. Ein Schutz ist hier nur durch eine zusätzliche Signatur der Pakete, durch höhere Protokolle oder

ein VPN möglich. Leider bietet TCP/IP keine Möglichkeit, die Authentizität eines Pakets zu überprüfen. Viele Applikationen wie Telnet führen die Authentifizierung aber nur zu Beginn durch. Anschließend gilt die Verbindung als authentifiziert. Ein Angreifer kann die Verbindung übernehmen und ist dann ebenfalls authentifiziert.

4.4.4 Bufferoverflow

Ein Bufferoverflow ist das Ergebnis eines Programmierfehlers. Nicht jeder Programmierfehler führt zu einem Bufferoverflow, und nicht jeder mögliche Bufferoverflow kann von einem Angreifer ausgenutzt werden. Um den Bufferoverflow zu verstehen, müssen Sie sich in die Rolle eines Programmierers hineinversetzen.

In vielen Programmen kommen einzelne Aufgaben wiederkehrend vor. Diese Aufgaben werden dann gern in einem Unterprogramm realisiert, das von verschiedenen Stellen des Hauptprogramms aufgerufen werden kann. Damit das Unterprogramm später weiß, wohin es im Hauptprogramm zurückspringen muss, sichert der Prozessor vor dem Aufruf des Unterprogramms den aktuellen Stand des Befehlszeigers (Instruction Pointer, IP) auf dem Stapel (Stack). Der Stapel ist eine dynamische Struktur, auf der ein Programm vorübergehend Daten ablegen kann. Jedes Programm besitzt einen eigenen Stapel. Ein Stapel erlaubt lediglich das Lesen und Schreiben der Daten auf dem höchsten Punkt. Dieser wird mit dem Stapelzeiger (Stackpointer) referenziert (siehe Abbildung 4.6). Benötigt nun das Unterprogramm vorübergehend Speicherplatz für eine Variable, so fordert es diesen Puffer (Buffer) auf dem Stapel an. Der Stapelzeiger wird um die entsprechende Anzahl Bytes verschoben und als Referenz an das Unterprogramm zurückgegeben (siehe Abbildung 4.7). Das bedeutet, das Unterprogramm kann nun Daten auf dem Stapel ablegen, wobei es beim Stapelzeiger beginnt und dann rückwärts geht.

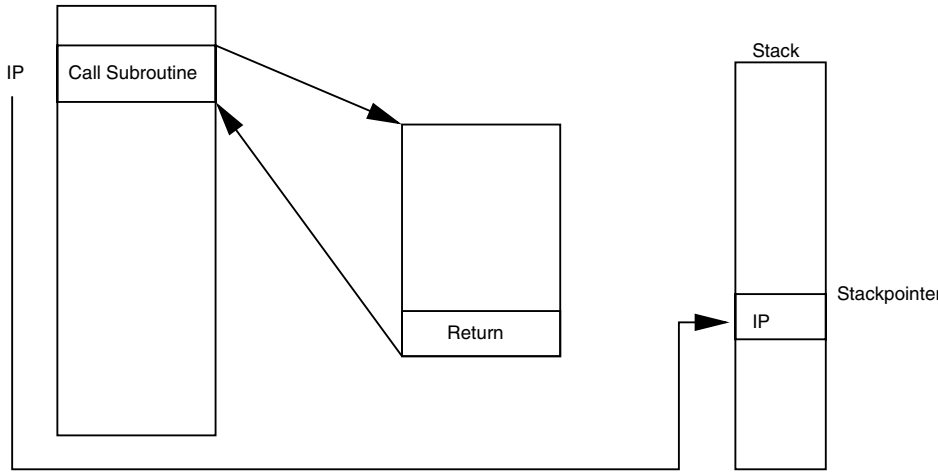


Abbildung 4.6: Funktionsweise eines Bufferoverflows

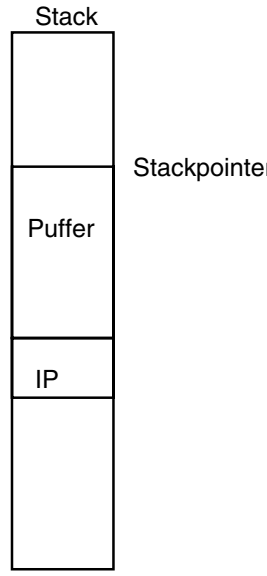


Abbildung 4.7: Pufferreservierung auf dem Stapel

Stellen wir uns vor, das Programm erwartet die Eingabe des Geburtsdatums des Benutzers. So genügen sicherlich 32 Bytes, um diese Eingabe entgegenzunehmen. Diese 32 Bytes werden nun auf dem Stapel reserviert. Aus irgendeinem Grund (Unwissenheit, Bösartigkeit) gibt der Benutzer jedoch 100 Zeichen ein. Überprüft der Programmierer vor der Kopie der Zeichenkette in den dynamisch allozierten Datenbereich auf dem Stapel ihre Länge nicht, so werden alle 100 Bytes auf den Stapel kopiert. Dadurch werden auch Bereiche überschrieben, die andere gültige Daten enthielten. Es kommt zu einem Überlaufen (Overflow) des originalen Puffers (siehe Abbildung 4.8). Hierbei können auch zum Beispiel Rücksprungadressen der Unterprogramme überschrieben werden.

Es gibt einige Programmiersprachen, die dem Programmierer diese Arbeit (das so genannte Boundary Checking) abnehmen, jedoch gehören die Programmiersprachen Assembler und C nicht dazu. In C werden die meisten Anwendungen für Unix- und auch für Windows-Betriebssysteme programmiert.

Handelt es sich um willkürliche Daten, so stürzt das Programm ab und es kommt zum Segmentation Fault (Linux) oder zu einer allgemeinen Schutzverletzung (General Protection Fault, Windows). Der Prozessor erkennt, dass es sich um eine unerlaubte Rücksprungadresse handelt. Ein Zugriff auf den Speicher an der Zieladresse ist dem Programm nicht erlaubt. Das Programm wird von dem Prozessor beendet (stürzt ab) und steht nicht mehr zur Verfügung. Dies ist ein Denial-of-Service.

Unter Umständen besteht jedoch auch die Möglichkeit, den Ort einer Rücksprungadresse auf dem Stack vorherzusagen und so zu überschreiben, dass ein geziel-

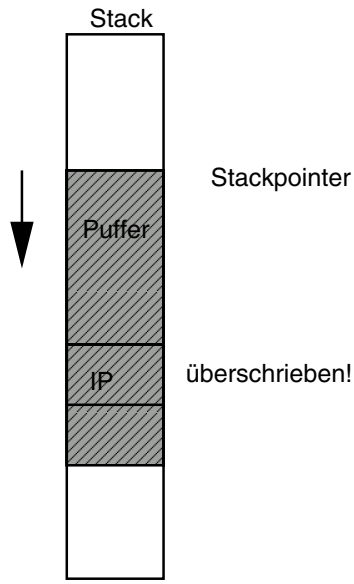


Abbildung 4.8: Überlaufen des Puffers

ter Rücksprung auf Code erfolgt, der sich im Vorfeld in den eingegebenen Daten befand. Dann wird in dem Benutzerkontext des missbrauchten Programms der gerade eingegebene Code ausgeführt. Üblicherweise handelt es sich hierbei um den Aufruf einer Unix-Shell. Daher bezeichnet man diesen von dem Einbrecher verwendeten Code auch häufig als Shell-Code. Dies ist unter Unix besonders brisant, da viele Netzwerkdienste über Rootprivilegien verfügen und Eingaben aus ungewisser Quelle entgegennehmen. Weisen diese Dienste derartige Mängel auf, so können sie ausgenutzt werden, um Rootprivilegien auf dem entsprechenden Rechner zu erlangen. In diesem Fall spricht man von Root Exploits.

Viele der ersten geschriebenen Bufferoverflows sind leicht an dem so genannten NOP Sled zu erkennen. Ein gezielter Rücksprung, wie gerade beschrieben, ist meist nicht möglich. Der Angreifer kann nur selten genau den Zustand des Stacks vorhersagen. Daher kann er auch nicht die Rücksprungadresse berechnen. Nun versieht er seinen Code zu Beginn mit bis zu mehreren hundert NOP-Befehlen. Ein NOP ist ein No-Operation-Befehl. Dieser Befehl hat, wenn er von dem Prozessor ausgeführt wird, keine Funktion, außer den Instruction-Pointer weiterzubewegen. Ist der Code für den Bufferoverflow derartig angepasst, so muss die Rücksprungadresse nur noch ungefähr in den Bereich der NOP-Befehle zeigen. Dies bezeichnet man als NOP-Schlitten (Sled), da der Befehlszeiger wie auf einem Schlitten über die NOPs zum Bufferoverflow rutscht und schließlich diesen Code ausführt.

Der injizierte Code wird als Shell-Code bezeichnet. Dieser Name leitet sich aus der Tatsache ab, dass klassische Bufferoverflows versuchen, eine Shell zu starten und so Kommandozeilenzugriff auf dem angegriffenen System zu erhalten.

Es gibt verschiedene Möglichkeiten, sich vor Bufferoverflows zu schützen. Der älteste Schutz erreicht dies, indem der gesamte Stapel für das Programm als nichtausführbar gekennzeichnet wird.

Achtung

Machen Sie nicht den Fehler anzunehmen, dass Sie mit dieser Methode aus dem Schneider sind. Erstens stürzt das Programm weiterhin ab. Der Prozessor erkennt lediglich, dass unerlaubter Code angesprungen werden soll. Außerdem gibt es auch Heap-Overflows. Hier hilft die Methode nicht.

Bei älteren Prozessoren der i386-Architektur ist dies nur mit Tricks möglich. Aktuelle Prozessoren unterstützen diese Funktion in Hardware. Bei dem Athlon64 existiert das No-eXecute-Bit (NX), das von AMD als Enhanced-Virus-Protection Technologie vermarktet wird. Intel hat bei den Itanium- und den neuesten Pentium 4- und M-Modellen das eXecute-Disable-Bit (XD) eingeführt. PowerPC, SPARC und Alpha-Prozessoren verfügen über diese Funktion schon länger.

Achtung

Wichtig zu wissen beim NX- und XD-Bit ist, dass diese Bits nicht automatisch aktiviert werden. Sie müssen ein Betriebssystem einsetzen, das diese Bits auch nutzt (zum Beispiel RHEL4 und Fedora Core mit ExecShield).

Es existieren noch drei weitere Varianten, um sich vor den Gefahren des Bufferoverflows zu schützen. Der modifizierte GNU-C-Compiler Stackguard implementierte als Erster den Schutz mit dem so genannten Canary (Kanarienvogel). Hierbei erzeugt der Compiler modifizierten Code, der vor jedem Sprung in ein Unterprogramm eine Zufallszahl auf dem Stapel abspeichert. Vor jedem Rücksprung überprüft das Programm, ob die Zufallszahl modifiziert wurde. Ist dies der Fall, wird ein Bufferoverflow angenommen und die Ausführung abgebrochen. Ansonsten fährt das Programm fort. Diese Vorgehensweise ist von IBM in ProPolice weiterentwickelt worden. ProPolice gibt es für einige Linux-Distributionen und OpenBSD.

Red Hat hat mit den Position-Independent-Executables (PIE) einen Schritt in eine andere Richtung gemacht. Auch hier wurde der GNU-C-Compiler so modifiziert, dass der entstehende Programmcode beliebig im Speicher arrangiert werden kann. Ein modifizierter Kernel (ExecShield-Patch) kann nun bei jedem Aufruf das Programm und alle Daten inklusive des Stapels zufällig an einer anderen Position abspeichern. Der Angreifer hat nun das Problem, dass er die Rücksprungadressen nicht mehr vorhersagen kann. Stellen Sie sich vor, Sie wären in einem Raum mit

fünfhundert Türen. Eine ist offen. Sie haben nur einen Versuch. Es ist einfach die richtige Tür zu finden, wenn sie immer an derselben Stelle ist und Sie dies vorher in einem anderen Raum üben können. Wenn die richtige Tür aber jedes Mal eine andere ist, ist dies vielfach schwerer.

Ihre letzte Schutzmöglichkeit vor Bufferoverflows ist der Austausch zentraler C-Funktionen. Die meisten Bufferoverflows nutzen spezielle C-Funktionen aus (z.B. `strcpy`). Die Libsafe-Bibliothek bietet Ihnen die Möglichkeit, diese Funktionen gegen sichere Varianten auszutauschen. Die neuen C-Funktionen überprüfen vor jedem Aufruf die Größe des zur Verfügung stehenden Puffers. Libsafe können Sie auf *http://www.research.avayalabs.com/project/libsafe/* herunterladen. Da Libsafe in Kombination mit dem Prelude-IDS (*http://www.prelude-ids.org*) als Intrusion-Detection-System eingesetzt werden kann, finden Sie in meinem Buch »Intrusion Detection und Prevention mit Snort 2 & Co.« weitere Hinweise zur Installation.

Achtung

Eine Firewall kann nicht vor einem Bufferoverflow schützen.

4.4.5 Formatstring-Angriffe

Bei den Formatstring-Angriffen handelt es sich um eine noch rechte junge Gruppe von Angriffen. Der Formatstring-Angriff wurde zum ersten Mal im Juni 2000 für einen Angriff auf den WU-Ftpd-Server verwendet. Ähnlich wie der Bufferoverflow betrifft dieses Problem Programme, die in C geschrieben wurden. Die Programmiersprache C kennt verschiedene Funktionen, die formatierte Textausgaben erlauben: `printf`, `scanf` etc. Diese Funktionen nehmen einen Formatstring und mehrere Werte entgegen und geben die Werte formatiert aus.

```
printf("%s", buffer)
```

Leider geben nicht alle Programmierer immer den Formatstring an, sondern sparen sich die Mühe und schreiben `printf(buffer)`. Wenn nun der Inhalt des Puffers von dem Angreifer eingegeben wurde, kann er auch Formatstrings angeben. Die Formatstrings und der Puffer werden immer über den Stapel an die Funktion übergeben. Die `printf`-Funktion interpretiert dann die Formatstrings des Angreifers. Es gibt Formatstrings, mit denen der Angreifer sowohl Daten von dem Stapel lesen kann (zum Beispiel `%s` und `%x`) als auch Werte schreiben kann (`%n`). So kann der Angreifer zunächst den Ort der richtigen Rücksprungadresse eines Unterprogramms ermitteln und anschließend überschreiben. Die Auswirkung ähnelt also einem Bufferoverflow. Ein Formatstring-Angriff kann also auch verwendet werden, um die Kontrolle über einen Dienst oder ein System zu erlangen. Dabei besteht mit dem

Formatstring %n die Möglichkeit, an beliebigen Adressen den Inhalt zu modifizieren. Der so von dem Angreifer injizierte Code muss also nicht auf dem Stapel liegen. Die Schutzmechanismen, die einen Überlauf erkennen (Stackguard, ProPolice) oder den Stapel als nicht-ausführbar deklarieren, können uns daher nicht vor Formatstring-Angriffen wirksam schützen. Lediglich die Randomisierung der Adressen (Exec-Shield mit PIE, PaX etc.) bietet hier einen gewissen Schutz.

Achtung

Eine Firewall bietet auch hier keinen Schutz!

4.4.6 Race-Condition

Eine Race-Condition entsteht, wenn zwei Prozesse gleichzeitig auf eine Ressource zugreifen, dieser Zugriff nicht geordnet erfolgt und der Ausgang von der Reihenfolge des Zugriffs abhängig ist. Diesen langen komplizierten Satz möchte ich anhand eines einfachen Beispiels erläutern.

Stellen Sie sich vor, Sie haben bei einer Bank ein Konto. Das Konto weist ein Guthaben von 500,00 EUR auf. Sie tätigen eine Überweisung und spenden 250,00 EUR für die Free-Software-Foundation-Europe (FSFE). Gleichzeitig geht Ihr Gehalt von Ihrem Arbeitgeber ein (2.500,00 EUR). Wenn diese beiden Vorgänge nun nicht geordnet durchgeführt werden, kann Folgendes passieren:

1. Für die Spendenüberweisung wird das Guthaben gelesen. Guthaben = 500,00 EUR.

2. Für die Gehaltsüberweisung wird das Guthaben gelesen. Guthaben = 500,00 EUR.

3. Das Gehalt wird addiert, und die Summe wird als neues Guthaben geführt. Guthaben = 500,00 EUR + 2.500,00 EUR = 3.000 EUR.

   Diese Summe wird als Guthaben gespeichert.

4. Für die Überweisung wird von dem Guthaben (500,00 EUR, es wurde ja früher gelesen) 250,00 EUR abgezogen. Guthaben = 500,00 EUR – 250,00 EUR = 250,00 EUR.

   Diese Summe wird nun als neues Guthaben gespeichert. Die 2.500,00 EUR sind verloren.

Natürlich hätte es auch genau andersherum passieren können. Dann hätten Sie trotz der Überweisung von 250,00 EUR an die FSFE anschließend immer noch 3.000,00 EUR besessen.

Eine Race-Condition führt also zu inkonsistenten Daten. Teilweise kann ein Angreifer diese aber auch ausnutzen, um erweiterte Rechte zu erlangen. Meist erfordert das Ausnutzen einer Race-Condition bereits Zugang zu einem System. Race-Conditions, die aus der Ferne über Netzwerkdienste ausgenutzt werden können, sind sehr selten.

Im Folgenden möchte ich Ihnen zwei typische Race-Conditions vorstellen: `/tmp`-Race-Conditions und die `ptrace`-Race-Condition.

Race-Conditions bei der Behandlung von temporären Dateien

Häufig treten bei der Behandlung von temporären Dateien Race-Conditions auf. Dies hängt damit zusammen, dass bei einem mehrfachen Zugriff auf temporäre Dateien über den Dateinamen das Programm nicht garantieren kann, dass es sich immer um dieselbe Datei handelt.

Stellen Sie sich vor, dass Sie ein Skript entwickeln möchten, das bei allen Systemkonten die Shell auf `/bin/false` ändern sollte. Ein Systemkonto benötigt keine Möglichkeit der interaktiven Anmeldung auf einem Linux-System. Ihr Skript könnte folgendermaßen aussehen:

Listing 4.1: Ein per Race-Condition verwundbares Skript

```
#!/bin/sh

TEMP=/tmp/mytemp

rm -f $TEMP

cat /etc/passwd | while read zeile
do
  echo $zeile | awk -F':' \
        '{if ((>0) && (<500)) print $1":"$2":"$3":"$4":"$5":"$6":/bin/false";
          else print $0}'
done >> $TEMP

mv $TEMP /etc/passwd
chmod 644 /etc/passwd
```

Dieses Skript löscht zunächst die temporäre Datei, da es anschließend eine Zeile an die neue Datei anhängen möchte (`done >> $TEMP`). Dann liest es die Datei `/etc/passwd` und ersetzt bei allen Konten mit den Nummern 1-499 die Shell in der Spalte 7 durch

`/bin/false`. Anschließend benennt das Skript die Datei in `/etc/passwd` um und setzt die Rechte entsprechend.

Wo ist hier die Race-Condition? Stellen Sie sich vor, der Angreifer wüsste, dass Sie dieses Skript als *root* starten. Er könnte versuchen, ein eigenes Skript gleichzeitig laufen zu lassen.

Listing 4.2: Der Exploit

```
#!/bin/sh

TEMP=/tmp/mytemp

touch $TEMP

while test -f $TEMP
do
  NOP=0 # do nothing
done
echo "toor::0:0:toor owns your machine:/:/bin/sh" > $TEMP
```

Dieses Skript legt die temporäre Datei mit dem bekannten Namen an. Anschließend prüft das Skript, ob die Datei noch existiert oder bereits von dem verwundbaren Skript gelöscht wurde. Sobald das erkannt wurde, bricht die Schleife ab und das Skript schreibt die angegebene Zeile in die Datei `/tmp/mytemp`, bevor das verwundbare Programm seine Daten an diese Datei anhängt.

Tipp

Wenn Sie dieses Problem nachstellen möchten, dann sollten Sie, damit es nicht von Ihrem Glück abhängt, in dem verwundbaren Programm die Zeitspanne des möglichen Exploits vergrößern. Fügen Sie einfach ein `sleep 1` nach dem `rm`-Befehl ein.

Um sich vor diesen Race-Conditions bei der Verwendung von temporären Dateien zu schützen, ist es wichtig, dass der Name der temporären Datei möglichst nicht vorhersagbar ist. Viele Programme hängen daher ihre PID (Prozess-ID) an den Dateinamen an. Jedoch ist auch diese PID auf vielen Linux/Unix-Systemen in gewissen Bereichen vorhersagbar. Die beste Lösung ist die Verwendung von benutzerspezifischen temporären Verzeichnissen, in denen andere Benutzer keine Dateien erzeugen können, oder der Befehl `mktemp`, der eine temporäre Datei nach dem Muster `/tmp/tmp.XXXXXXXXXX` erzeugt. Hiermit sind 26^{10} verschiedene Dateinamen möglich. Eine Vorhersage durch den Angreifer ist unmöglich.

Achtung

Bei der Beschreibung des Angriffs sollte Ihnen deutlich geworden sein, dass eine Firewall keinerlei Schutz bietet. Hier kann aber ein MAC-System wie SELinux durchaus Abhilfe schaffen.

Die ptrace-Race-Condition

Hierbei handelt es sich um eine Race-Condition im Linux-Kernel, die im Januar 2003 entdeckt wurde. Diese Sicherheitslücke war nur lokal ausnutzbar. Dennoch wurde sie in vielen Angriffen genutzt, denn es gab gleichzeitig auch Sicherheitslücken in weiteren Netzwerkdiensten wie dem Apache-Webserver. Die Angreifer konnten über den Netzwerkdienst Kommandozeilenzugriff auf das Zielsystem erhalten. Da die meisten Netzwerkdienste aber nicht über root-Privilegien verfügen, musste der Angreifer anschließend nach einer weiteren Sicherheitslücke suchen, um eine Privilege-Escalation, eine Erweiterung seiner Privilegien, durchzuführen. Dafür wurde dann die `ptrace`-Race-Condition genutzt. Linux-Kernel < 2.2.25/2.4.20 weisen diese Sicherheitslücke auf.

Der Fehler tritt auf, wenn ein Prozess eine Funktion nutzen möchte, die über ein noch nicht geladenes Kernelmodul realisiert wird. Dies ist zum Beispiel häufig beim Öffnen eines Netzwerk-Sockets für eine untypische Protokoll-Familie (PF_IPX, PF_X25, PF_AX25, PF_APPLETALK etc.) der Fall. Um die Protokoll-Familie zu unterstützen, muss der Kernel ein Modul nachladen. Hierzu erzeugt der Kernel automatisch von dem anfordernden Prozess einen Kindprozess. Anschließend stellt der Kernel die User-ID des Kindprozesses auf 0 und lädt mit dem Befehl `modprobe` das Modul. Da der Kindprozess in dem Kontext des ursprünglichen Benutzers gestartet wird, kann dieser auf den Prozess Einfluss nehmen, bevor der Kernel die root-Privilegien überträgt. Hier ist die Race-Condition.

Wie nutzt man dies nun aus? Der Kernel bietet mit der `ptrace`-Funktion die Möglichkeit, Prozesse zu beobachten, Breakpoints einzufügen und den Code zu modifizieren. Diese Funktion wird von Debuggern zur Fehlersuche verwendet. Kann der Angreifer mit dieser Funktion sich an den Kindprozess binden, bevor der Kernel die root-Privilegien überträgt, so kann er anschließend einen Prozess mit root-Privilegien steuern, den Code modifizieren und so jede beliebige Tätigkeit auf dem System ausüben. Er hat die komplette Kontrolle über das System übernommen.

Ich hoffe, Sie haben erkannt, dass die Race-Condition weniger ein technischer Programmierfehler als viel mehr ein Fehler im logischen Design einer Applikation ist. Häufig sind es Seiteneffekte, die eine Race-Condition ermöglichen. Eine Verteidigung mit einer Firewall ist nicht möglich. Hier helfen nur Mandatory-Access-Control-Systeme wie SELinux, LIDS oder grsecurity. Wenn diese Systeme auch die

Race-Condition selbst nicht verhindern können, wenden sie jedoch weiteren Schaden von dem System ab.

4.4.7 SQL-Injektion

Die SQL-Injektion wird hier als ein Paradebeispiel eines Angriffs über einen Webserver beschrieben. Erwartungsgemäß erfolgen heute die meisten Angriffe über das Netzwerk entweder über das HTTP/HTTPS- oder das SMTP-Protokoll. Dies sind in vielen Fällen noch die einzigen Wege in das Netzwerk eines Unternehmens. Jeder andere Zugriff wird heute meist von Firewalls unterbunden. Mögliche Fernzugriffe werden über sichere VPN-Lösungen implementiert. Der Angreifer kann, vorausgesetzt Sie haben Ihre Hausaufgaben als Firewall-Administrator gemacht, nur auf den Webserver und den Mailserver des Unternehmens zugreifen. Allerdings bestehen die meisten Websites heute aus dynamischen Seiten, die von einer Web-Applikation erzeugt werden. Diese Web-Applikation greift hierzu auf eine Datenbank im Hintergrund zu. Über diesen Zugriff erhält die Web-Applikation eines Internet-Shops zum Beispiel Informationen über den Preis und die Verfügbarkeit eines Artikels. Diese Datenbank befindet sich meist in dem internen Netz des Unternehmens (siehe Abbildung 4.9). Der Webserver, der sich in der DMZ befindet, benötigt daher Zugriff auf diese Datenbank. Ein Angreifer, der diese Logik ausnutzen kann, erhält so unter Umständen Zugriff auf interne Systeme!

Bei der SQL-Injektion versucht der Angreifer herauszufinden, wie eine Web-Applikation die von ihm eingegebenen Daten verwendet. Wenn die Applikation

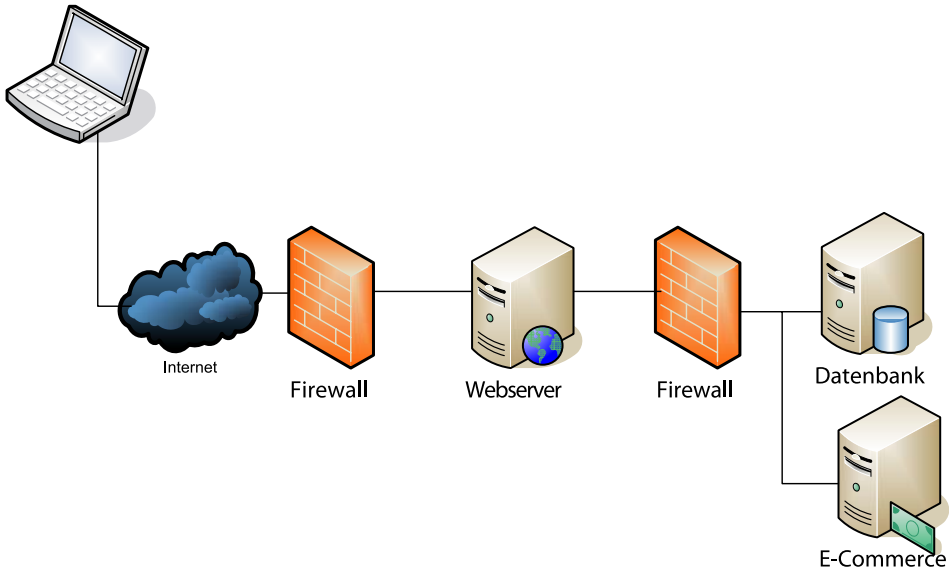


Abbildung 4.9: Die Web-Applikation auf einem Webserver greift meist durch die Firewall auf die interne Datenbank zu.

Abbildung 4.10: Viele Applikationen sind durch eine Login-Seite geschützt.

zum Beispiel über eine Login-Seite verfügt (Abbildung 4.10), dann besteht die Möglichkeit, dass die Applikation zur Überprüfung der Daten folgende Anfrage an die Datenbank stellt:

```
SELECT name FROM users WHERE name="$name« AND password="$pass«
```

Wenn der Angreifer als Namen `Bob` und als Kennwort `password` eingibt, wird der folgende SQL-Befehl ausgeführt:

```
SELECT name FROM users WHERE name="Bob" AND password="password"
```

Existiert der Benutzer und ist das Kennwort korrekt, so liefert diese Anweisung den Namen des angemeldeten Benutzers. Vielleicht kennt der Angreifer den Namen, aber nicht das Kennwort eines Benutzers. Dann kann er folgende Eingabe versuchen:

```
name=Bob
pass="weissnicht" OR "1"="1"
```

Wird dies nun in der SQL-Anweisung eingesetzt, ergibt sich die folgende Anweisung:

```
SELECT name FROM users WHERE name="Bob" AND
  password="weissnicht" OR "1"="1"
```

Da der Ausdruck 1=1 immer stimmt, ist die Anmeldung unabhängig von dem eingegebenen Kennwort gültig, da die Select-Anweisung ein Ergebnis liefert.

Diese Sicherheitslücke ist möglich, da der Programmierer die eingegebenen Daten nicht vor der Verwendung prüft. Es handelt sich um eine fehlende Eingabevalidierung ähnlich dem Bufferoverflow oder dem Formatstring-Angriff. Die Web-Applikation muss sämtliche Eingaben auf ihre Gültigkeit prüfen, bevor diese an die

Datenbank weitergereicht werden. In diesem Beispiel wäre es zum Beispiel sinnvoll, beim Benutzernamen zu prüfen, ob außer den Zeichen A-Z,a-z weitere nichterlaubte Zeichen in dem Namen oder außer A-Z,a-z,0-9 weitere Zeichen in dem Kennwort vorkommen. Diese Aufgabe kann jedoch nur von der Web-Applikation selbst erledigt werden. Nur der Programmierer der Web-Applikation kann die gültigen Zeichen einer Eingabe festlegen. Eine Firewall ist hier überfordert.

4.4.8 Welchen Schutz bietet eine Firewall?

Ich habe Ihnen auf den letzten Seiten verschiedene Bedrohungsszenarien bei der Anbindung Ihrer Rechner an das Internet vorgestellt. Bei fast allen Angriffen habe ich Sie darauf hingewiesen, dass sie von einer Firewall nur in geringem Maße oder gar nicht abgewehrt werden können.

Warum sollen Sie dann überhaupt den Aufwand einer Firewall betreiben?

Ohne Firewall wird alles noch schlimmer! Überlegen Sie sich, welche Dienste Sie in Ihrem Netz und auf Ihren Rechnern betreiben. Sicherlich möchten Sie nicht, dass jeder im Internet auf diese Dienste zugreifen kann. Wahrscheinlich ist es auch nicht in Ihrem Sinne, dass jeder Benutzer auf jeden Dienst im Internet zugreifen kann. Hier bietet die Firewall Schutz. Natürlich erkennt die Firewall keinen Bufferoverflow- oder Formatstring-Angriff. Ohne Firewall kann ein Angreifer mit diesen Methoden alle Ihre Systeme angreifen. Wenn Sie eine Firewall besitzen, ist dieser Angriff nur auf den Systemen möglich, auf die die Firewall den Zugriff erlaubt.

Eine Firewall bietet Schutz nach dem Prinzip »Single-Point-of-Defense«. Anstatt jeden Rechner einzeln zu verteidigen und die Dienste in allen Punkten auf Sicherheitslücken zu prüfen, regelt die Firewall, wer auf welche Dienste zugreifen darf. Natürlich sind diese Dienste dann immer noch besonders gefährdet. Diese Dienste können immer noch mit einem Bufferoverflow-Angriff getroffen werden. Die tatsächliche Zahl der verwundbaren Systeme und Dienste haben Sie aber durch den Einsatz einer Firewall reduziert.

Eine Firewall hilft auch bei der Schadensbegrenzung nach einem erfolgreichen Angriff, denn Angriffe erfolgen nur selten blind. Der Angreifer will nach dem Bufferoverflow auf der Kommandozeile des Zielsystems arbeiten, seine Privilegien erweitern und weiteren Schaden anrichten. Hierfür benötigt er Netzwerkverbindungen, Werkzeuge und die Möglichkeit, weitere Systeme zu kontaktieren.

Betrachten Sie noch einmal die Abbildung 4.9. Wenn die Firewall Verbindungen des Webservers in das Internet unterbindet, kann ein Angreifer keine weiteren Werkzeuge nachladen. Auch der Start einer Remote-Shell, die eine neue Netzwerkverbindung aufbaut, ist nicht ohne weiteres möglich. Erlaubt die Firewall zusätzlich nur den Zugriff auf den Port des Datenbankservers in dem internen Netz, sind die weiteren Rechner vor dem Zugriff des Angreifers geschützt. Der Angreifer muss jetzt erst eine Sicherheitslücke in dem Datenbankserver finden, um diesen angreifen zu können.

Daher ist eine Firewall sehr wohl sinnvoll. Die Firewall schützt aber nicht vor allen Gefahren und Bedrohungen aus dem Internet. Sie müssen diese Bedrohungen kennen, um zusätzliche Maßnahmen zu implementieren, die Systeme regelmäßig zu patchen und so Sicherheit aufrechtzuerhalten.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Teil II

Firewalls mit Iptables – Einführung

5 Eine einfache Firewall mit Iptables

Dieses Kapitel spricht in erster Linie den Linux-Benutzer an, der sich noch nie ernsthaft mit den Linux-Paketfilterfunktionen beschäftigt hat. Es beginnt direkt mit praktischen Beispielen, aber erklärt auch sämtliche nötigen Grundlagen, ohne zu tief zu gehen. Nach diesem Kapitel können Sie bereits eine einfache simple Linux-Paketfilter-Firewall entwickeln und einsetzen. Spätere Kapitel beschreiben dann weitergehende Funktionen.

5.1 Netfilter und Iptables

Wenn Sie sich das erste Mal mit den Linux-Paketfilterfunktionen beschäftigen, werden Sie zwangsläufig auf die Begriffe *Netfilter* und *Iptables* treffen. Viele Anwender kennen den Unterschied nicht und nutzen diese Begriffe daher als Synonym. In Wirklichkeit sollten Sie diese Begriffe unterscheiden, daher beginnen wir zunächst mit einer Begriffsdefinition:

- **Netfilter**: Netfilter bietet Ankerpunkte (Hooks) im Netzwerkstapel von Linux an. Hier können sich dann weitere Kernelmodule anmelden. Sobald ein Paket an diesem Ankerpunkt vorbeikommt, wird das entsprechende Modul aufgerufen. Es handelt sich also um eine ganz allgemeine Struktur, die Filterfunktionen anbietet.
- **Iptables**: Iptables erlaubt die Definition von Regeln in Tabellen (Tables). Jede Tabelle besteht aus mehreren Ketten. Diese Ketten werden von Iptables an die verschiedenen Hooks von Netfilter gebunden. Es nutzt also die von Netfilter zur Verfügung gestellte Struktur.

Für die gesamte Funktionalität des Linux-Paketfilters ist zusätzlich auch noch das Connection-Tracking- und das NAT-Subsystem erforderlich (s.u.).

Als Anwender werden Sie sich nie mit Netfilter beschäftigen müssen. Alle für Sie interessanten Funktionen werden Sie mit dem `iptables`-Befehl konfigurieren können.

5.2 Der Iptables-Befehl und die Filter-Tabelle

Wenn Sie bereits einige Erfahrungen mit dem Einsatz des `iptables`-Befehls gemacht haben, können Sie diesen Abschnitt überspringen. Vielleicht lesen Sie ihn aber doch. Es könnte sich der eine oder andere interessante Hinweis finden lassen.

Iptables verwaltet seine Regeln in mindestens drei Tabellen: `filter`, `mangle` und `nat`. Hier wird zunächst nur die `filter`-Tabelle besprochen. Die anderen Tabellen werden in weiteren Abschnitten (5.7, 5.8) erörtert.

Die `filter`-Tabelle ist für die Filterung der Pakete verantwortlich. Das heißt, hier entscheidet der Linux-Kernel, ob ein Paket erlaubt, abgelehnt oder verworfen wird. Da dies die wesentliche Funktion einer Firewall darstellt, werden wir uns zunächst hiermit beschäftigen.

In der `filter`-Tabelle unterscheidet der Linux-Kernel drei Ketten: `INPUT`, `OUTPUT` und `FORWARD` (siehe Abbildung 5.1). Diese drei Ketten haben genau definierte Aufgaben. Alle Pakete, die an den Rechner selbst gerichtet sind, durchlaufen die `INPUT`-Kette. Alle Pakete, die der Rechner selbst erzeugt, werden vor dem Verlassen des Rechners durch die `OUTPUT`-Kette gefiltert. Die `FORWARD`-Kette kümmert sich schließlich um die Pakete, die der Rechner lediglich weiterleiten soll. Hierbei handelt es sich also um Pakete, die an die Firewall als Gateway zur Weiterleitung geschickt werden.

Achtung

Diese Aufgabenteilung unter den Ketten ist bei Iptables neu. Wenn Sie sich bereits mit dem Paketfilter `ipchains` beschäftigt haben, kennen Sie von dort noch eine andere Nutzung dieser Ketten.

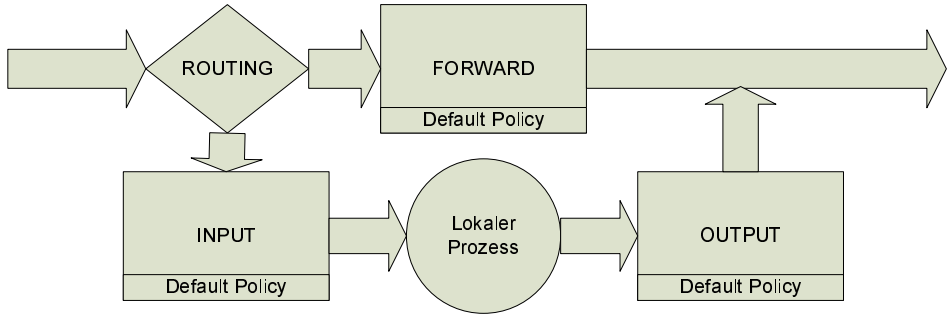


Abbildung 5.1: Die Filtertabelle besteht aus drei Ketten.

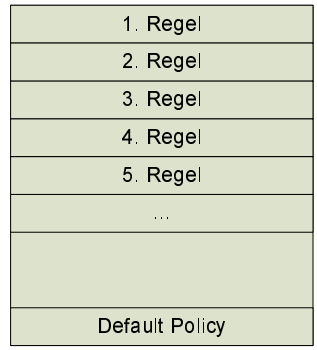


Abbildung 5.2: Die Regeln in einer Kette werden der Reihe nach abgearbeitet. Trifft keine Regel auf das Paket zu, gilt die Default-Policy.

Jede dieser Ketten besteht nun aus einer Liste von Regeln, die für jedes Paket nacheinander abgearbeitet werden (Abbildung 5.2). Sobald eine Regel auf das Paket zutrifft, wird die mit der Regel verbundene Aktion ausgeführt und mit wenigen Ausnahmen die Abarbeitung weiterer Regeln abgebrochen. Trifft keine Regel aus der Liste zu, so wird die *Default Policy* der Kette aktiv. Diese Default-Regel trifft auf alle Pakete zu, die nach Abarbeitung aller Regeln noch in der Kette verblieben sind.

Da diese Einführung bisher recht theoretisch und abstrakt war, macht es Sinn, dies gleich in die Praxis umzusetzen. Im Folgenden setze ich voraus, dass Sie über einen Rechner mit einer aktuellen Linux-Distribution Ihrer Wahl verfügen und als *root* angemeldet sind.

Prüfen Sie bitte zunächst Ihre Installation, indem Sie folgenden Befehl eingeben:[1]

```
[root@bibo root]# iptables -V
iptables v1.2.9
```

Wenn der Befehl auf Ihrem System die Fehlermeldung »-bash: Iptables: command not found« ausgibt, dann prüfen Sie bitte, ob Sie das entsprechende Paket noch installieren müssen. Gibt der Befehl so wie oben eine Versionsnummer aus, können Sie direkt fortfahren. Die Version selbst ist im Moment noch unerheblich.

Als Erstes sollten Sie sich eventuell bereits vorhandene Regeln anzeigen lassen:

```
[root@bibo root]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
```

[1] Wundern Sie sich bitte nicht über die Namen meiner Rechner. Alle meine Systeme haben Namen aus der Sesamstraße als Rechnernamen. Neben Kermit, Oskar und Grobi gibt es auch einen Bibo.

```
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Werden bei dieser Ausgabe bereits Regeln angezeigt, sollten Sie für die Dauer dieses Kapitels die Regeln deaktivieren. Wenn Sie diese Regeln nicht selbst gesetzt haben, ist hierfür wahrscheinlich Ihre Distribution verantwortlich. Auf einer Red Hat Linux-basierten Distribution (auch Fedora Core) können Sie mit folgendem Befehl die eingebaute Firewall abschalten:

```
[root@bibo root]# service iptables stop
Firewall-Regeln löschen:                                   [  OK  ]
Setze Chains auf Policy ACCEPT: filter                     [  OK  ]
iptables-Module beenden:                                   [  OK  ]
```

Auf einer SUSE-Distribution geben Sie bitte folgenden Befehl ein:

```
rcSUSEfirwall2 stop
```

Auf einem Gentoo-System sollte schließlich dieser Befehl die Firewall abschalten:

```
/etc/init.d/firewall stop
```

Es ist sicherlich nicht möglich, hier alle Eventualitäten und Distributionen zu berücksichtigen. Wenn die oben aufgeführten Befehle auf Ihren Systemen nicht funktionieren, lesen Sie bitte in der Dokumentation Ihrer Distribution nach.

Nun können Sie erste Regeln erzeugen. Dies erfolgt zunächst direkt auf der Kommandozeile mit dem Befehl `iptables`. Um direkt einen Effekt erkennen zu können, sollten Sie der Einfachheit halber auf einer grafischen Oberfläche arbeiten und dort zwei Fenster öffnen. In dem einen Fenster rufen Sie den `ping`-Befehl auf: `ping 127.0.0.1` (Abbildung 5.3). In dem anderen Fenster arbeiten Sie mit dem `iptables`-Befehl.

Beobachten Sie die Ausgabe des Ping, wenn Sie den folgenden Befehl absetzen:

```
[root@bibo root]# iptables -A INPUT -p icmp -j DROP
```

Der Ping sollte nun unbeantwortet bleiben. Dieser Befehl hängt eine Regel an die INPUT-Kette an (`-A; --append`). Diese Regel prüft in der INPUT-Kette, ob ein Paket das Protokoll ICMP (`-p; --protocol`) verwendet. Dieses Protokoll wird zum Beispiel von dem Ping genutzt. Ist das der Fall, wird das Paket verworfen (`-j; --jump, DROP`). Alle auf dem Rechner ankommenden Ping-Pakete werden also nun von der eingebauten Firewall verworfen. Alle weiteren Pakete können die Firewall weiterhin passieren.

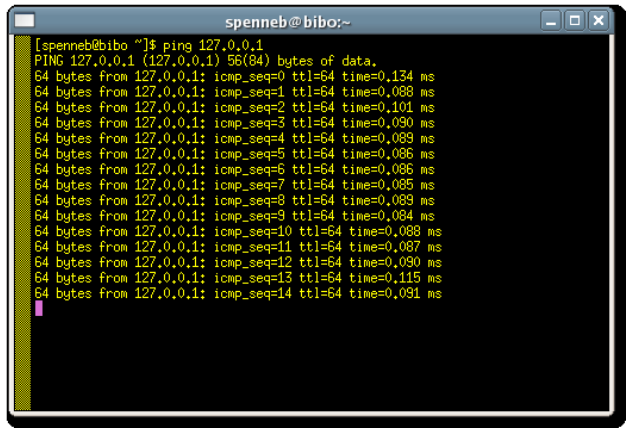


Abbildung 5.3: Der Ping-Befehl kann die Erreichbarkeit eines Rechners prüfen.

Achtung

Ein DROP verwirft die betroffenen Pakete, ohne den Absender davon zu unterrichten. Der Absender erhält keine Antwort und auch keine Fehlermeldung. Er wird es je nach Protokoll und Anwendung ein weiteres Mal versuchen. Nach mehreren Fehlversuchen wird der Absender üblicherweise den Verbindungaufbau mit einem Timeout abbrechen. Möchten Sie direkt dem Absender eine Fehlermeldung senden, um diesen Vorgang abzukürzen, können Sie das Ziel REJECT nutzen. Das REJECT-Ziel verwirft das Paket und sendet eine Fehlermeldung an den Absender, so dass dieser es nicht erneut versucht.

```
[root@bibo root]# iptables -A INPUT -p icmp -j REJECT
```

Sie können sich die Regeln mit `iptables -L` wieder ansehen. Mehr Information erhalten Sie aber mit folgendem Befehl:

```
[root@bibo root]# iptables -vnL --line-numbers
Chain INPUT (policy ACCEPT 142K packets, 209M bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        2   168 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 112K packets, 6371K bytes)
num   pkts bytes target     prot opt in     out     source               destination
```

Hier sehen Sie die ausführliche (`-v; --verbose`) Liste der Regeln (`-L; --list`) in numerischer Form (`-n; --numeric`) mit Zeilennummern (`--line-numbers`). Zunächst sehen Sie wieder jede Kette mit ihrer Default-Policy in Klammern. Hinter der Default-Policy sehen Sie, wie viele Pakete bereits von dieser Default-Policy bearbeitet wurden und wie viele Bytes das sind. Anschließend werden bei jeder Kette die Regeln aufgezählt.

In der ersten Spalte wird die Nummer der Regel angezeigt. Diese Nummer kann später verwendet werden, um diese Regel zu löschen. In der zweiten und dritten Spalte wird wieder die Anzahl der Pakete und die Anzahl der Bytes angegeben, auf die diese Regel zutraf. Hiermit können Sie auch Ihren Netzwerkverkehr auswerten[2]. Dann sehen Sie das IP-Protokoll (icmp) und mögliche Optionen. Die nächsten beiden Spalten geben die Netzwerkkarte an, die das Paket verwenden muss, damit diese Regel zutrifft. Es ist möglich, bei der Erzeugung einer Regel sowohl die Netzwerkkarte anzugeben, über die das Paket den Rechner erreichen muss (`-i; --in-interface`), als auch die Netzwerkkarte, über die es den Rechner verlassen muss (`-o; --out-interface`). In unserer Regel haben wir keine Netzwerkkarte angegeben, daher befinden sich hier Sternchen als Wildcard für alle verfügbaren Karten. Nun folgen noch die Quelladresse (`-s; --src; --source`) und die Zieladresse (`-d; --dst; --destination`) des zu filternden Pakets. Auch hier haben wir keine Angabe gemacht, daher hat Iptables hier 0.0.0.0/0 eingetragen. Dies entspricht einem Netzwerk mit allen möglichen IP-Adressen.

Exkurs: CIDR-Notation

Mit der Einführung des Subnetting löste man sich von den starren Netzwerkklassen A, B und C. Um die Netzmasken einfacher zu schreiben, wurde die Classless Internet Domain Routing-(CIDR-) Notation eingeführt. Anstelle von 255.255.255.0 nutzt diese Notation /24. Für die Umwandlung der Netzmaske in die CIDR-Notation stellen Sie sich die Netzmaske binär vor:

```
255.255.255.0 = 11111111.11111111.11111111.00000000
```

Nun zählen Sie die Einsen in der Netzmaske von links ab. Es handelt sich um drei mal acht Einsen, also 24 Einsen. Diese werden nun als CIDR-Notation nach dem Schrägstrich geschrieben. Im Folgenden finden Sie die üblichen Netzmasken in CIDR-Notation:

```
/0.0.0.0         = /0
/255.0.0.0       = /8
/255.255.0.0     = /16
/255.255.255.0   = /24
/255.255.255.255 = /32
```

[2] Sie können auch Regeln erzeugen, die kein Ziel haben. Diese Regeln zählen nur die betroffenen Pakete!

Wenn Sie den Iptables-Befehl mehrfach wiederholen, fügen Sie mehrere Regeln in der INPUT-Kette hinzu:

```
[root@bibo root]# iptables -A INPUT -p icmp -j DROP
[root@bibo root]# iptables -A INPUT -p icmp -j DROP
[root@bibo root]# iptables -A INPUT -p icmp -j DROP
[root@bibo root]# iptables -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere
DROP       icmp --  anywhere             anywhere
DROP       icmp --  anywhere             anywhere
DROP       icmp --  anywhere             anywhere
```

Jede Regel wird »unten« an der Kette angehängt. Wenn Sie nur eine Kette anzeigen möchten, können Sie, wie hier gezeigt, auch den Namen der Kette beim Kommando `iptables -L` mit angeben.

Um einzelne Regeln wieder zu löschen, können Sie die Option `-D` beziehungsweise `--delete` verwenden. Um die Regel Nummer Eins zu löschen, verwenden Sie:

```
[root@bibo root]# iptables -D INPUT 1
```

Existiert keine Regel mit dieser Nummer, erhalten Sie folgende Fehlermeldung:

```
[root@bibo root]# iptables -D INPUT 5
iptables: Index of deletion too big
```

Alle weiteren Regeln rücken automatisch nach dem Löschen auf. Löschen Sie die Regel Eins, so wird die Regel Zwei zu Eins, Drei zu Zwei usw.

Möchten Sie alle Regeln löschen, können Sie den Befehl `iptables -F` verwenden. Dieser Befehl löscht alle Regeln in allen Ketten der Filtertabelle. Möchten Sie nur sämtliche Regeln der INPUT-Kette löschen, verwenden Sie:

```
[root@bibo root]# iptables -F INPUT
[root@bibo root]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Nun sind Sie wieder da, wo wir angefangen haben. Sämtliche Ketten sind leer. Die Default-Policies sind auf ACCEPT gestellt.

Nun bauen wir die Regeln anders auf. Während bis jetzt alles erlaubt war und nur das ICMP-Protokoll mit einer spezifischen Regel verboten wurde, möchten wir nun alles verbieten und nur ausgewählte Protokolle erlauben. Hierzu setzen Sie zunächst die Default-Policy in der INPUT-Kette auf DROP.

Achtung

Stellen Sie sicher, dass Sie *lokal* angemeldet sind. Wenn Sie in diesem Moment über das Netzwerk arbeiten, wird der folgende Befehl Ihre Verbindung unterbrechen!

Dies erledigen Sie mit folgendem Befehl:

```
[root@bibo root]# iptables -P INPUT DROP
```

Nun sollte Ihr Rechner keine Pakete mehr entgegennehmen[3]. Der Ping sollte auch nicht mehr möglich sein. Auch eine Secure Shell-Verbindung von außen sollte keine Antwort liefern. Um nun ausgewählte Protokolle wieder nutzen zu können, müssen Sie diese durch einzelne Regeln erlauben.

Erlauben Sie als Erstes wieder den Ping, indem Sie spezifisch das Protokoll ICMP akzeptieren:

```
[root@bibo root]# iptables -A INPUT -p icmp -j ACCEPT
```

Wenn Sie auf Ihrem System einen SSH-Server betreiben, können Sie auch die SSH-Verbindungsaufnahmen wieder gestatten. Benutzen Sie dazu bitte folgenden Befehl:

```
[root@bibo root]# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
[root@bibo root]# iptables -vnL
Chain INPUT (policy DROP 51 packets, 5528 bytes)
 pkts bytes target     prot opt in     out     source               destination
    4   372 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
   15  8121 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0     tcp dpt:22

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 398K packets, 23M bytes)
 pkts bytes target     prot opt in     out     source
```

[3] Wenn Sie auf Ihrem Rechner nun auch keine neuen Fenster mehr öffnen können, dann liegt das am lokalen Netzwerkverkehr, der für die grafische Oberfläche benötigt wird. Solange noch Fenster geöffnet sind, sollten Sie in diesen aber ohne Probleme weiterarbeiten können.

Dieser Befehl fügt eine Regel in der INPUT-Kette hinzu, die alle Pakete akzeptiert, die das TCP-Protokoll verwenden (`-p tcp`) und an den Port 22 gerichtet sind (`--dport`; `--destination-port 22`)[4]. Dies setzt natürlich einen laufenden SSH-Server auf Ihrer Maschine voraus.

Um nun den Originalzustand wiederherzustellen, genügt es nicht, den Befehl `iptables -F` aufzurufen. Dieser Befehl löscht zwar sämtliche Regeln in den Ketten, verändert aber nicht die Default-Policies! Da die Default-Policy in Ihrer INPUT-Kette aber immer noch auf DROP gestellt ist, werden weiterhin alle Pakete verworfen. Sie müssen zusätzlich noch den folgenden Befehl eingeben:

```
[root@bibo root]# iptables -P INPUT ACCEPT
```

Damit setzen Sie die Default-Policy wieder auf den ursprünglichen Wert. Jetzt werden wieder alle Pakete in der INPUT-Kette akzeptiert.

5.3 Ihr erstes Firewall-Skript

Nachdem Sie in dem letzten Abschnitt ein wenig mit dem `iptables`-Befehl herumgespielt haben, sollen Sie nun Ihr erstes Firewall-Skript entwickeln. Dieses Skript soll die Regeln für ein Firewall-Gateway nach Abbildung 5.4 implementieren. Das Skript soll sämtliche Verbindung von innen nach außen zulassen, aber keine Verbindung von außen nach innen. Hierzu benötigen Sie zwei Rechner. Einer dieser beiden Rechner sollte über zwei Netzwerkkarten verfügen und mit dem Internet verbunden sein. Der andere Rechner sollte eine Netzwerkkarte besitzen und die zweite Karte des ersten Rechners erreichen können.

Achtung

Im Weiteren benutze ich die Worte »innen« und »außen«, um jeweils das innere, von der Firewall geschützte Netz und das äußere Internet zu bezeichnen.

[4] Falls Sie dies nun mit `ssh localhost` testen wollen, wird das noch nicht funktionieren. Sie benötigen hier noch zusätzlich die Regel:

```
[root@bibo root]# Iptables -A INPUT -p tcp --sport 22 -j ACCEPT
```

Dies ist erforderlich, da auch der Client von der Firewall betroffen ist. Wenn Sie Ihren SSH-Client auf einer zweiten Maschine aufrufen, ist das nicht der Fall.

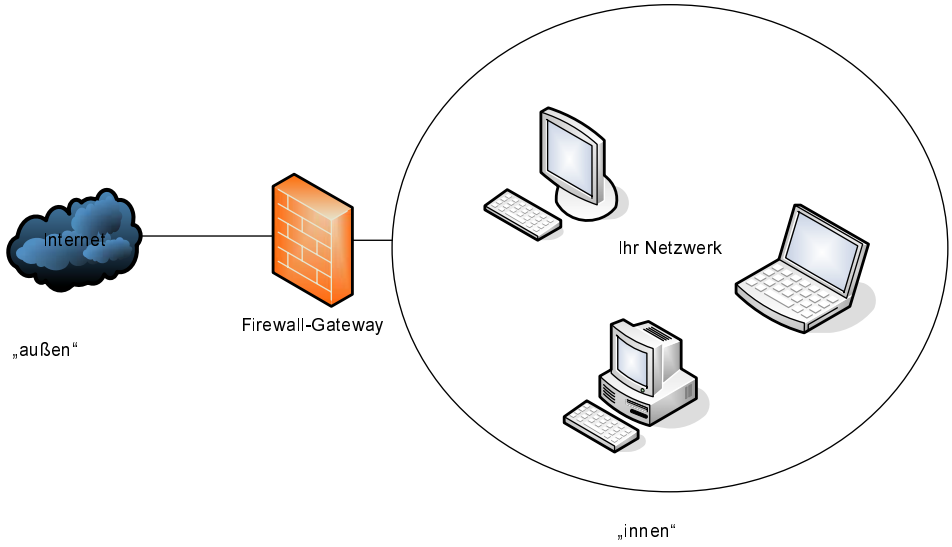


Abbildung 5.4: Das Firewall-Gateway schützt Ihr internes Netz vor den Zugriffen aus dem Internet.

Hinweis: User-Mode-Linux

Falls Sie nicht über zwei Rechner verfügen, können Sie an dieser Stelle auch einen Rechner (den Client) virtuell betreiben. Hierzu befindet sich auf der CD ein kompletter virtueller Rechner, den Sie direkt von der CD aus starten können. Gehen Sie hierzu in das Verzeichnis `/virtualclient`. Für RPM-basierte Distributionen müssen Sie noch das beigelegte `user_mode_linux-<version>.i386.rpm` installieren. Unter Debian müssen Sie das `uml-utilities`-Paket installieren.

Nun rufen Sie das Skript `./start_client` auf. Es bootet dann eine virtuelle Linux-Maschine. Diese wird anschließend die Aufgabe des Clients aus Abbildung 5.4 übernehmen. Die IP-Adressen sind schon entsprechend eingestellt. Lediglich die Namen der Netzwerkkarten werden sich noch ändern. Dies wird noch an der entsprechenden Stelle beschrieben.

Die Rechner sollten über folgende IP-Adressen verfügen:

- **Externe Karte der Firewall**: Beliebige IP-Adresse außer 10.x.x.x
- **Interne Karte der Firewall**: IP-Adresse 10.0.0.1, Netzmaske 255.0.0.0
- **Karte des Clients**: IP-Adresse 10.0.0.100, Netzmaske 255.0.0.0, Gateway 10.0.0.1

Diese IP-Adressen sind beim User-Mode-Linux-Client bereits voreingestellt. Wenn Sie alles richtig konfiguriert haben, sollten Sie in der Lage sein, von dem

Firewall-System Ihren Client anzupingen (`ping 10.0.0.100`) und umgekehrt (`ping 10.0.0.1`).

Funktioniert so weit alles, beginnen Sie mit Ihrem Firewall-Skript. Warum sollten Sie ein Skript schreiben?

- Nun, Änderungen sind in einem Skript mit einem Editor möglich.
- Sie können sämtliche Regeln in dem Skript aufnehmen und dann auf einmal ausführen.
- Nach einem Reboot vergisst der Linux-Rechner alle Regeln. Mit einem Skript können Sie diese wieder laden.
- In einem Skript können Sie Kommentare einfügen, die später (auch nach einem Jahr) erläutern, warum Sie diese oder jene Regel für besonders wichtig hielten.
- Außerdem können Sie in einem Skript Variablen nutzen und so die Wartung des Skripts stark vereinfachen.

Ein ordentliches Shell-Skript sollte immer mit etwa folgenden Zeilen beginnen:

```
#!/bin/sh
#
# Autor  : Ralf Spenneberg
# Version: 0.1
# Datum  : 17. Dez 2004
#
# Dieses Skript lädt die Regeln für die Firewall
```

Die erste Zeile ist zwingend erforderlich. Durch diese Zeile erkennt das Betriebssystem, mit welchem Interpreter das Skript ausgeführt werden muss. Unter Linux gibt es viele Skriptsprachen. Jede besitzt ihren eigenen Interpreter. Da diese nicht kompatibel sind, sollten Sie den zu wählenden Interpreter in der ersten Zeile mit »#!« angeben. Diese Zeichenfolge wird auch als »She-Bang« bezeichnet. Die anderen Angaben können Sie entsprechend Ihren Wünschen anpassen. Für die dauerhafte Pflege Ihrer Skripte beschäftigen Sie sich am besten mit einem Revision-Control-System (RCS). Es gibt RCS und CVS. RCS ist auf fast jedem Linux-System vorhanden und verfügt über eine einleitende Manpage (`rcsintro(1)`).

Zunächst sollte Ihr Skript sicherstellen, dass der Befehl `iptables` immer gefunden wird. Da sich möglicherweise auch der Pfad in einer zukünftigen Distributionsversion ändern kann, sollten Sie hierfür eine Variable verwenden. Fügen Sie die folgende Zeile zu Ihrem Skript hinzu, und Sie können den Pfad dann bei Bedarf anpassen:

```
IPTABLES="/sbin/iptables"
```

Nun sollten Sie alle Ketten zunächst durch das Skript sperren lassen. Dazu setzen Sie die Default-Policies in allen Ketten auf DROP:

```
#!/bin/sh
#
# Autor  : Ralf Spenneberg
# Version: 0.1
# Datum  : 17. Dez 2004
#
# Dieses Skript lädt die Regeln für die Firewall

IPTABLES="/sbin/iptables"

# Verwerfe erstmal alles, indem
# die Default-Policy auf DROP gesetzt wird
$IPTABLES -P INPUT  DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP
```

Der Zugriff auf die Variable erfolgt durch Voranstellen des Dollarzeichens. Bei der Zuweisung des Wertes ist es wichtig, dass um das Gleichheitszeichen keine Leerzeichen vorkommen.

Nun müssen die Regeln hinzugefügt werden. Diese sollen nur Verbindungen von innen nach außen zulassen. Für die Firewall handelt es sich um weitergeleitete Pakete. Daher müssen diese in der FORWARD-Kette gesetzt werden. Die Regeln müssen die Richtung unterscheiden können. Diese Unterscheidung ist am einfachsten über die Netzwerkkarten möglich. Sinnvollerweise erzeugen Sie sich für die Namen Ihrer Netzwerkkarten auch wieder Variablen. Vielleicht ändert sich mal eine Netzwerkkarte. Dann können Sie durch eine Modifikation Ihres Skripts dieses an die neue Situation anpassen.

```
INTDEV="eth0"
EXTDEV="eth1"
```

Achtung

Wenn Sie User-Mode-Linux einsetzen, ist die interne Netzwerkkarte `tap0`. Das bedeutet, Sie müssen die Zeile wie folgt abändern:

```
INTDEV="tap0"
```

Diese Variablen fügen Sie sinnvollerweise am Anfang direkt hinter der Iptables-Variable ein. Um nun die Verbindung von innen zu erlauben, fügen Sie die folgenden Regeln am Ende Ihres Skripts an:

```
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Die erste Regel prüft, ob ein Paket über die interne Netzwerkkarte die Firewall erreicht (`-i $INTDEV`) und über die externe Netzwerkkarte die Firewall verlässt (`-o $EXTDEV`)[5]. Zusätzlich prüft die Regel den Zustand des Pakets. Hierzu pflegt das Linux-System eine Tabelle, in der jede erlaubte Verbindung eingetragen wird. Ein Paket besitzt den Zustand NEW, wenn es zu keiner bisher eingetragenen Verbindung passt. Es besitzt den Zustand ESTABLISHED, wenn es bereits eine Verbindung in der Tabelle gibt, der dieses Paket zugeordnet werden kann. Der Zustand RELATED wird verwendet, wenn das Paket nicht Teil der Verbindung ist, sondern in einer anderen Beziehung zu dieser Verbindung steht. Hierbei kann es sich zum Beispiel um eine ICMP-Fehlermeldung handeln. Eine ausführlichere Erklärung der Verbindungsüberwachung (engl. Connection Tracking) gibt es im Abschnitt 5.5 und in Kapitel 19. Die erste Regel akzeptiert so jedes Paket, das eine neue Verbindung aufbauen möchte und von innen nach außen geschickt wird. Gleichzeitig wird diese Verbindung dann in der Tabelle eingetragen.

Die zweite Regel prüft dann lediglich, ob ein Paket den Zustand ESTABLISHED oder RELATED aufweist. Alle diese Pakete werden von der zweiten Regel akzeptiert. So ist ein Verbindungsaufbau nur von innen nach außen möglich.

Warum ist das sicher? Wenn nun ein Paket von außen eine neue Verbindung aufbauen wollte, würde es von der Firewall nicht akzeptiert werden. Dieses Paket besitzt den Zustand NEW. In der ersten Regel werden zwar solche Pakete akzeptiert, aber dieses Paket würde nicht die Bedingung erfüllen, über die interne Netzwerkkarte die Firewall erreicht zu haben. Damit ein Paket von außen zugelassen wird, ist erst ein Paket von innen erforderlich, das dieses Paket anfordert und die Verbindung in der Zustandstabelle einträgt. Sobald dies erfolgt ist, erhalten alle weiteren Pakete der Verbindung den Zustand ESTABLISHED und werden von der zweiten Regel unabhängig von ihrer Richtung akzeptiert.

Achtung

Warum werden die Regeln in der FORWARD-Kette hinzugefügt? Wieso nicht in der INPUT- oder OUTPUT-Kette? Wenn Sie sich nochmal die Abbildung 5.1 auf Seite 82 ansehen, wird Ihnen auffallen, dass die Pakete, die durch das Gateway durchgeroutet werden, nur von der FORWARD-Kette bearbeitet werden. Die INPUT- und die OUTPUT-Kette sind hier gar nicht beteiligt. Diese Ketten werden nur aktiv, wenn das Gateway selbst Kommunikationspartner wäre. Dies wird in Kapitel 8 genauer besprochen!

[5] Noch sicherer können Sie die Regel definieren, wenn Sie auch noch prüfen, ob die Absender-Adresse des Pakets aus Ihrem Netzwerk stammt. Hierzu können Sie eine Variable `INTNET=10.0.0.0/8` anlegen und diese zusätzlich mit der Option `-s $INTNET` der Regel hinzufügen.

Damit ist das Skript aber noch nicht ganz fertig. Zwei wesentliche Punkte fehlen noch, damit es funktioniert:

1. **Forwarding**: Selbst wenn die Firewall momentan von innen Pakete für die Weiterleitung nach außen erhält, wird sie diese im Moment noch nicht weiterleiten.
2. **Masquerading**: Selbst wenn die Weiterleitung aktiviert wurde und ein interner Client Netzwerkpakete nach außen sendet, werden die Systeme außerhalb der Firewall nicht wissen, wohin sie antworten sollen, da den Systemen die IP-Adresse und das Netzwerk des Clients unbekannt ist. Die IP-Adresse der Firewall ist bekannt. Daher kann die Firewall dieses Problem beheben, in dem sie eine Network Address Translation durchführt. Hierbei wird die originale Absenderadresse des Clients durch die Adresse der Firewall ausgetauscht. Dies wird auch als Masquerading bezeichnet.

Zunächst soll das Forwarding aktiviert werden. Derartige Funktionen werden bei Linux über das virtuelle `/proc`-Dateisystem angeschaltet. Dieses Dateisystem erlaubt die Konfiguration des Linux-Kernels zur Laufzeit. Für das Forwarding ist die Datei `/proc/sys/net/ipv4/ip_forward` zuständig. Enthält diese Datei eine 0, so ist das Forwarding nicht aktiv. Bei einer 1 leitet der Linux-Kernel zwischen allen Netzwerkkarten die Pakete als Router weiter.

Es gibt grundsätzlich zwei Möglichkeiten, um nun das Forwarding einzuschalten:

- Sie verwenden den `/bin/echo`-Befehl. Mit diesem Befehl können Sie in der Datei folgendermaßen eine 1 speichern:

```
ECHO="/bin/echo"
$ECHO "1" > /proc/sys/net/ipv4/ip_forward
```

- Die zweite Möglichkeit ist der Befehl `sysctl`. Dieser Befehl kann die Werte im `/proc`-Dateisystem lesen und setzen. Die folgenden Zeilen erreichen dasselbe wie der Echo-Befehl weiter oben.

```
SYSCTL="/bin/sysctl"
$SYSCTL -w net.ipv4.ip_forward=1
```

Für welchen Befehl Sie sich hier entscheiden, bleibt Ihnen überlassen. Weitere Informationen über den Befehl `sysctl` und das `/proc`-Dateisystem erhalten Sie im Kapitel 23.

Network Address Translation (NAT) und die NAT-Tabelle werden im Abschnitt 5.7 ausführlich besprochen. Hier soll nur die erforderliche Regel vorgestellt und erklärt werden. Damit das Masquerading, das eine spezielle Form des NAT ist, funktioniert, benötigen Sie die folgende Regel:

```
$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -j MASQUERADE
```

Das Masquerading erfolgt in der POSTROUTING-Kette der NAT-Tabelle. Diese Kette ist die letzte Kette, die ein Paket durchläuft, das den Rechner verlässt. In

dieser Kette tauscht diese Regel die Absenderadresse jedes Pakets gegen die Absenderadresse der Firewall aus und merkt sich die Originaladresse. So kann die Firewall bei einem Antwortpaket die originale Adresse wieder einsetzen. Dieser Vorgang soll nur für Pakete aktiviert werden, die die Firewall nach außen verlassen (`-o $EXTDEV`). Die NAT-Tabelle enthält auch noch die Ketten PREROUTING und OUTPUT. Diese Ketten und die weiteren Funktionen der NAT-Tabelle werden im Abschnitt 5.7 besprochen.

Sinnvoll sind in dem Skript zu Beginn nun noch einige Befehle, die möglicherweise vorhandene Regeln aufräumen und entfernen, ehe neue Regeln hinzugefügt werden. Dies kann mit den folgenden beiden Zeilen erreicht werden:

```
$IPTABLES -F
$IPTABLES -t nat -F
```

Das komplette Skript sieht nun wie folgt aus:

Listing 5.1: Das erste Firewall-Skript erlaubt nur Verbindungen von innen.

```
#!/bin/sh
#
# Autor  : Ralf Spenneberg
# Version: 0.1
# Datum  : 17. Dez 2004
#
# Dieses Skript lädt die Regeln für die Firewall

INTDEV="eth1"
# Achtung: Bei Einsatz von User-Mode-Linux lautet diese Variable
# INTDEV="tap0"

EXTDEV="eth0"

# Definiere einige Befehle
ECHO="/bin/echo"
SYSCTL="/bin/sysctl"
IPTABLES="/sbin/iptables"

# Verwerfe erstmal alles
$IPTABLES -P INPUT  DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP

# Leere die Ketten
$IPTABLES -F
```

```
# Die NAT-Tabelle muss extra geleert werden
$IPTABLES -t nat -F


# Akzeptiere Verbindungsaufbauten von innen
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -m state --state NEW -j ACCEPT

# Akzeptiere alle Pakete, die Teil einer aufgebauten Verbindung sind
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# Maskiere alle Pakete bei der Weiterleitung nach außen
$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -j MASQUERADE

# Aktiviere das Forwarding
$ECHO "1" > /proc/sys/net/ipv4/ip_forward

# Alternativ:
# $SYSCTL -w net.ipv4.ip_forward=1
```

Achtung

Möglicherweise verhält sich Ihre Firewall anders, als Sie es erwarten würden. Es kann sein, dass bei einem Zugriff auf einen E-Mail- oder FTP-Server scheinbar die Verbindung erst verzögert zustande kommt. Schuld daran ist die Tatsache, dass Sie alle Verbindungen, die von außen aufgebaut werden, ohne Fehlermeldung verwerfen. Leider bauen gerade Unix-E-Mail-Server und FTP-Server bei einem Verbindungsaufbau Ihrerseits eine Verbindung zu Ihnen auf dem Port 113/tcp auf. Hier horcht bei Unix-Systemen normalerweise der identd. Der E-Mailserver und der FTP-Server fragen diesen Dienst, welcher Benutzer die ursprüngliche Verbindung aufgebaut hat. Da dieser Verbindungsversuch verworfen wird, wiederholen Sie den Versuch mehrfach. Solange müssen Sie mit Ihrer Verbindung warten. Am einfachsten lösen Sie das Problem, indem Sie Verbindungen auf dem Port 113/tcp nicht verwerfen, sondern mit einer Fehlermeldung ablehnen:

```
$IPTABLES -A INPUT -i $EXTDEV -p tcp --dport 113 -j REJECT
```

Nun ist es an der Zeit, dieses Skript zu testen, falls Sie es nicht schon vorher getan haben. Hierfür speichern Sie dieses Skript unter dem Namen `firewall` ab und machen es anschließend ausführbar: `chmod 755 firewall`. Leider schleichen sich bei der Eingabe häufig Tippfehler ein, die nur schwer gefunden werden können, da die Fehlermeldungen der Shell nicht besonders aussagekräftig sind – so zum Beispiel:

```
[root@bibo root]# ./firewall
iptables: No chain/target/match by that name
```

Erfreulicherweise bietet die BASH-Shell eine Option, mit der die Zeile, auf der sich der Fehler eingeschlichen hat, leicht ermittelt werden kann. Die Option `-x` gibt jede Zeile vor der Ausführung auf dem Bildschirm aus. Sie müssen also nur die Fehlermeldung wiederfinden und die Zeile davor genau analysieren:

```
... gekürzt ...
+ /sbin/iptables -P INPUT DROP
+ /sbin/iptables -P OUTPUT DROP
+ /sbin/iptables -P FORWARD DROP
+ /sbin/iptables -A FORWARD -i eth0 -o eth1 -m state --state NEW -j ACCEPT
+ /sbin/iptables -A FORARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables: No chain/target/match by that name
+ /sbin/iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
... gekürzt ...
```

Hier kann sehr schnell der Übeltäter erkannt werden. Es handelt sich um einen Tippfehler in dem Namen der FORWARD-Kette. Anstelle von FORWARD wurde FORARD verwendet.

Herzlichen Glückwunsch, wenn keine Fehler auftreten. Sie sollten jetzt schon über einen funktionsfähigen Firewall-Regelsatz verfügen. Dieser erlaubt im Moment der Firewall selbst keinerlei Teilnahme am Netzwerkverkehr. Die Firewall kann also zum Beispiel nicht pingen und keinen Ping beantworten. Jedoch sollte ein Client durch die Firewall auf andere Rechner zugreifen können. Versuchen Sie doch einfach mal Ihr Glück mit einem Ping vom Client ins Internet. Wenn es nicht funktioniert, finden Sie am Ende dieses Abschnitts einige weitere Hinweise zur Fehlersuche.

Hinweis: Warum kann die Firewall nicht pingen?

Die INPUT- und die OUTPUT-Kette enthalten keine Regeln. Da die Default-Policies dieser Ketten auf DROP gesetzt sind, werden in diesen Ketten daher keine Pakete akzeptiert, sondern sämtliche Pakete verworfen. Sowohl die Pakete, die von außen an die Firewall selbst gerichtet sind, als auch die Pakete, die die Firewall versenden möchte, sind davon betroffen. Nur in der FORWARD-Kette akzeptiert die Firewall Netzwerkpakete. Daher ist ein Ping durch die Firewall möglich! Im Kapitel 8 werden die INPUT- und die OUTPUT-Kette genauer betrachtet. Dort lernen Sie, wie Sie auch hier sinnvoll filtern. Wenn Sie dieses Verhalten für den Moment abstellen wollen, ändern Sie in Ihrem Skript die Default-Policy der INPUT- und der OUTPUT-Kette auf ACCEPT. Dann schützt sich die Firewall aber selbst nicht mehr!

Da Sie gerade in Übung sind, was das Schreiben von Firewall-Skripten betrifft, sollten Sie sich auch ein Skript erzeugen, das die Firewall wieder beendet. Hierzu können Sie das folgende Skript verwenden:

Listing 5.2: Dieses Skript (firewall_stop) entfernt alle Regeln und setzt die Default-Policies wieder auf ACCEPT zurück.

```
#!/bin/sh
#
# Autor  : Ralf Spenneberg
# Version: 0.1
# Datum  : 17. Dez 2004
#
# Dieses Skript löscht die Regeln für die Firewall

ECHO="/bin/echo"
IPTABLES="/sbin/iptables"

# Lösche alle vorhandenen Regeln
$IPTABLES -F
$IPTABLES -t nat -F

# Stelle die Default-Policies wieder her
$IPTABLES -P INPUT  ACCEPT
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -P FORWARD ACCEPT

# Deaktiviere das Forwarding
$ECHO "0" > /proc/sys/net/ipv4/ip_forward
```

Mit diesem Skript können Sie Ihre Firewall immer wieder zu Testzwecken beenden.

5.3.1 Fehlersuche

Ich hoffe, dass die meisten Leser mit dem Nachvollziehen des Kapitels keine Probleme[6] haben werden, da gerade die ersten Versuche häufig darüber entscheiden, ob man von einem System begeistert ist oder nicht. Daher habe ich mich bemüht, jeden Schritt genau zu erklären und an alle Eventualitäten zu denken. Dennoch kann es zu weiteren Fehlern kommen, die ich hier versuche zu erklären. Prüfen Sie aber bitte als Erstes Ihr Skript auf syntaktische Richtigkeit. Sobald beim Aufruf Ihres Firewall-Skripts eine Fehlermeldung ausgegeben wird, kann es nicht funktionieren! Suchen Sie den Fehler, und beheben Sie ihn, wie oben erläutert.

[6] Die Beispiele wurden auf den handelsüblichen Distributionen und Kerneln getestet. Wenn Sie einen selbstgebauten Kernel und/oder Iptables-Befehl verwenden, kann ich nicht dafür garantieren. Dann sollten Sie aber über die Erfahrung verfügen, diesbezügliche Fehler selbst zu lösen.

Wenn Ihr Skript erfolgreich lädt, Sie aber dennoch keinen Rechner außerhalb Ihrer Firewall erreichen können, gehen Sie bitte bei der Fehlersuche folgendermaßen vor:

1. Beenden Sie Ihre Firewall mit dem `firewall_stop`-Skript.

2. Prüfen Sie nun, ob Sie von Ihrem Client aus Ihre Firewall erreichen können: `ping 10.0.0.1`. Klappt das nicht, überprüfen Sie die Netzwerkverbindung. Ansonsten fahren Sie in der Fehlersuche fort.

3. Prüfen Sie nun, ob Sie von der Firewall einen Rechner außerhalb erreichen können. Klappt dies nicht, überprüfen Sie bitte die Netzwerkverbindung Ihrer Firewall.

4. Prüfen Sie nun die Routing-Konfiguration des Clients. Ist die interne IP-Adresse der Firewall das Standard-Gateway des Clients? Dies können Sie mit dem Befehl `/sbin/route` erledigen:

```
[root@bibo root]# /sbin/route
Kernel IP Routentabelle
Ziel            Router          Genmask         Flags Metric Ref    Use Iface
10.0.0.1        *               255.255.255.255 UH    0      0        0 eth0
192.168.0.0     *               255.255.255.0   U     0      0        0 eth1
default         192.168.0.254   0.0.0.0         UG    0      0        0 eth1
```

   Hier ist hat das Default-Gateway die IP-Adresse 192.168.0.254. Sie können mit `route del default` vorübergehend das Default-Gateway entfernen und mit `route add default gw <ip-adresse>` neu setzen.

5. Wenn Sie DNS-Namen verwenden möchten, prüfen Sie bitte, ob der Client die richtigen DNS-Server kennt. Wenn Sie keinen direkten Zugriff auf das Internet haben, können die DNS-Server speziell des User-Mode-Linux-Clients falsch eingerichtet sein. Die DNS-Server werden in der Datei `/etc/resolv.conf` gepflegt. Tragen Sie hier die DNS-Server ein, deren Funktion Sie sicher kennen.

6. Aktivieren Sie testweise auf der Firewall das Forwarding und das Masquerading:

```
[root@bibo root]# iptables -t nat -A POSTROUTING -o $EXTDEV -j MASQUERADE
[root@bibo root]# echo "1" > /proc/sys/net/ipv4/ip_forward
```

   Ersetzen Sie hierbei `$EXTDEV` durch den Namen Ihrer externen Netzwerkkarte. Prüfen Sie anschließend, ob Sie nun von Ihrem Client aus den zuvor getesteten Rechner außerhalb Ihrer Firewall erreichen können.

7. Starten Sie nun Ihr Firewall-Skript erneut. Prüfen Sie, ob Sie immer noch den Rechner erreichen können.

5.4 Einbindung in den Boot-Prozess

Im letzten Abschnitt haben Sie erfolgreich Ihr erstes Firewall-Skript geschrieben. Vielleicht ist Ihnen bereits aufgefallen, dass nach einem Neustart des Systems alle Regeln, die durch das Skript gesetzt wurden, wieder verloren sind. Für eine richtige Firewall ist es daher erforderlich, dass bei jedem Neustart diese Regeln neu geladen werden. Bei den meisten Linux-Distributionen kümmert sich der SysV-Init-Prozess um den Bootvorgang, die Initialisierung des Systems und das Starten der Dienste.

Welcher Dienst beim Bootvorgang des Rechners gestartet wird, hängt von dem Betriebszustand des Rechners ab. Dieser Betriebszustand wird als Runlevel bezeichnet. Die meisten modernen Linux-Distributionen unterscheiden die folgenden Runlevel.

Runlevel	Bedeutung
0	Halt-Zustand
1	Single-User
2	Multi-User ohne Netzwerkfunktionen
3	Multi-User mit allen Netzwerkdiensten
4	Vorkonfiguriert wie 3, aber ohne Verwendung
5	Multi-User wie 3, aber mit grafischer Oberfläche
6	Reboot
7-9	Nicht konfiguriert

Tabelle 5.1: Runlevel und ihre Bedeutung

In welchem Zustand sich Ihr System befindet, können Sie mit dem Befehl `runlevel` oder `who -r` ermitteln:

```
[root@bibo root]# runlevel
N 5
[root@bibo root]# who -r
         Runlevel 5   Dec 20 06:37                   last=S
```

Beide Befehle sind sich einig, dass sich mein System im Moment in Runlevel 5 befindet. Welcher Runlevel beim nächsten Reboot automatisch von dem System gewählt wird, können Sie in der Datei `/etc/inittab` festlegen:

Listing 5.3: Der Default-Runlevel wird in der Datei /etc/inittab definiert:

```
#
# inittab       This file describes how the INIT process should set up
#               the system in a certain run-level.
#
# Author:       Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
#               Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
```

```
# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:5:initdefault:
... gekürzt ...
```

Bei einer Firewall ist es sinnvoll, dafür zu sorgen, dass die Regeln beim Bootvorgang unabhängig von dem gewählten Runlevel geladen werden. Daher sollten Sie Ihr Skript in den Bootvorgang des Runlevels 3, 4 und 5 einbinden. In den Runleveln 1 und 2 stehen normalerweise keine Netzwerkdienste zur Verfügung, daher ist die Einbindung hier nicht zwingend erforderlich. Allerdings kann es auch nicht schaden. Daher können Sie auch in diesen Runleveln Ihr Skript einbinden.

Die Einbindung erfolgt über Verknüpfungen in den Verzeichnissen `/etc/rcX.d`. Die Anleitung für die Einbindung in aller Kürze:

1. Kopieren Sie Ihr Skript in das Verzeichnis `/etc/init.d/`:

   ```
   cp firewall /etc/init.d/MyFirewall
   ```

2. Machen Sie das Skript ausführbar: `chmod 755 /etc/init.d/MyFirewall`

3. Gehen Sie in das Verzeichnis `/etc/rc.d/rc3.d/`, und erzeugen Sie einen Startlink:

   ```
   [root@bibo root]# cd /etc/rc.d/rc3.d/
   [root@bibo rc3.d]# ln -s /etc/init.d/MyFirewall S05MyFirewall
   ```

4. Wiederholen Sie den letzten Schritt für die Verzeichnisse mit den Nummern 4 und 5. Wenn Sie möchten, können Sie dies auch für die Verzeichnisse 1 und 2 durchführen.

Diese vier Schritte genügen üblicherweise für die Einbindung des Skripts. Wenn Sie nun Ihren Rechner neu starten, sollte Ihr Skript automatisch geladen werden.

Möglicherweise fragen Sie sich nun, warum ich die Nummer 05 für die Verknüpfung `S05MyFirewall` gewählt habe. Die S-Nummer definiert die Reihenfolge der zu startenden Dienste. Die K-Nummer definiert die Reihenfolge, in der die Dienste beendet werden. Dies ist erforderlich, da es durchaus Abhängigkeiten unter den Diensten gibt. So ist zum Beispiel der Start des Netzwerks erforderlich, bevor ein Netzwerkdienst gestartet werden kann.

Im Falle der Firewall-Regeln sollten diese geladen werden, bevor das Netzwerk gestartet wurde und die Netzwerkkarten initialisiert wurden. Dies erfolgt bei Red Hat an der Position 10. Dadurch sind die Regeln schon aktiv, wenn die Netzwerkkarten aktiviert werden. So entsteht keine Lücke, die ein Angreifer ausnutzen könnte.

Tipp

Erfreulicherweise erlaubt der `iptables`-Befehl das Laden der Regeln für Netzwerkkarten und IP-Adressen, die noch nicht existieren!

Die hier vorgenommene Einbindung ist sicherlich nicht distributionskonform. Das werden Sie daran erkennen, dass Sie diesen Dienst mit den Werkzeugen Ihrer Distribution nun nicht konfigurieren können. In dem Handbuch Ihrer Distribution werden Sie weitere Hinweise dazu finden, wie Sie das Skript distributionskonform einbinden, so dass Sie es auch mit den Werkzeugen Ihrer Distribution verwalten können.

Damit Ihnen nun die distributionseigene Firewall die Arbeit nicht wieder zunichte macht, sollte diese deaktiviert werden. Auf einer Red Hat-basierten Linux-Distribution erreichen Sie das mit dem Befehl:

```
[root@bibo /]# chkconfig iptables off
```

Bei SUSE verwenden Sie YaST und deaktivieren die Firewall.

Nun sollten Sie Ihren Rechner neu starten und prüfen, ob anschließend auch Ihre Firewall-Regeln so geladen wurden, wie Sie sie eingestellt haben.

5.5 Connection Tracking und Netzwerkverbindungen

Die wesentliche Eigenschaft, die Iptables von älteren Paketfiltern unterscheidet, ist die Verbindungsüberwachung. Während ein einfacher Paketfilter wirklich nur Pakete analysieren und filtern kann, ist Iptables in der Lage, Verbindungen zu filtern. Dies erreicht Iptables, indem es eine Liste der bekannten Verbindungen pflegt und so Pakete zuordnen kann. Um dies besser zu verstehen, beschreibe ich zunächst kurz die Funktionsweise eines einfachen Paketfilters wie ipchains. Die Entwicklung der notwendigen Regeln soll sowohl anhand einer TCP- als auch einer UDP-Verbindung durchgesprochen werden. Den Abschluss machen ICMP-Pakete. Im Anschluss erläutere ich die Verbindungsüberwachung (Connection Tracking) durch Iptables. Dann sollte Ihnen deutlich werden, dass dieses Connection Tracking den Aufbau wesentlich sicherer Firewalls ermöglicht. Gleichzeitig wird das Regelwerk einfacher und übersichtlicher.

5.5.1 Der zustandslose Paketfilter IPchains

Wenn Sie bereits mit dem Paketfilter IPchains des Linux-Kernels 2.2 Erfahrungen gesammelt haben, wird Ihnen sicherlich dieses Kapitel bekannt vorkommen. Bitte

überspringen Sie es dennoch nicht, denn viele Iptables-Anwender haben bis heute nicht den wesentlichen Funktionsunterschied zwischen IPchains und Iptables richtig verstanden.

IPchains ist ein klassischer Paketfilter, der in der Lage ist, die Protokoll-Header eines Pakets zu analysieren und anschließend das Paket zu akzeptieren oder zu verwerfen. Dabei muss IPchains sich jedes Paket einzeln ansehen und ist als Paketfilter nicht in der Lage, Abhängigkeiten der Pakete zu erkennen. Im Folgenden sollen Beispielregeln für typische Netzwerkverbindungen in IPchains entwickelt werden. Sie müssen die IPchains-Syntax hierfür nicht erlernen. Ich werde sie an der entsprechenden Stelle ausführlich erläutern. Sie ähnelt auch stark der Iptables-Syntax. Ich möchte Sie lediglich auf einige Sicherheitsprobleme im Zusammenhang mit Paketfiltern hinweisen.

5.5.2 IPchains und UDP

Beginnen wir mit einer typischen UDP-Verbindung. Die DNS-Namensauflösung ist ein typische UDP-Verbindung und sicherlich für einen Großteil des UDP-Verkehrs im Internet verantwortlich. Hier fragt ein DNS-Client einen DNS-Server nach der IP-Adresse für einen DNS-Namen oder umgekehrt.

Die Anfrage ist schematisch in Abbildung 5.5 dargestellt, und ein TCPDump-Mitschnitt ist in Listing 5.4 zu sehen.

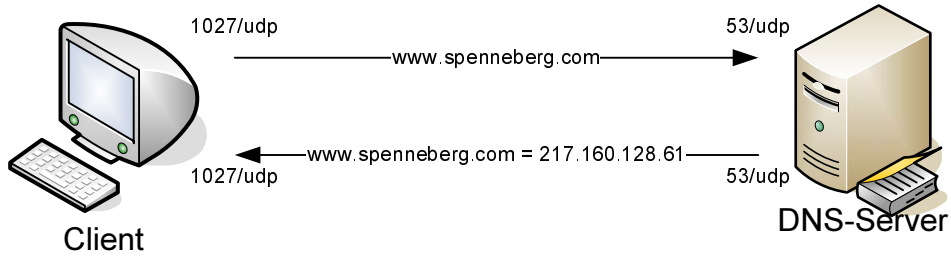


Abbildung 5.5: Der DNS-Client fragt den DNS-Server mit dem UDP-Protokoll auf Port 53 nach der IP-Adresse für www.spenneberg.com.

Listing 5.4: TCPDump-Mitschnitt der DNS-Anfrage »www.spenneberg.com«

```
[root@bibo tmp]# tcpdump -nvv port 53
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes

17:33:50.850459 IP (tos 0x0, ttl  64, id 0, offset 0, flags [DF], proto 17, length: 64)
192.168.0.112.35785 > 128.176.0.12.domain: [udp sum ok]  52380+ A? www.spenneberg.com. (36)

17:33:50.891933 IP (tos 0x0, ttl  48, id 51717, offset 0, flags [none], proto 17,
length: 176) 128.176.0.12.domain > 192.168.0.112.35785:  52380 q: A? www.spenneberg.com.
2/2/2 www.spenneberg.com. CNAME spenneberg.com., spenneberg.com.[|domain]
```

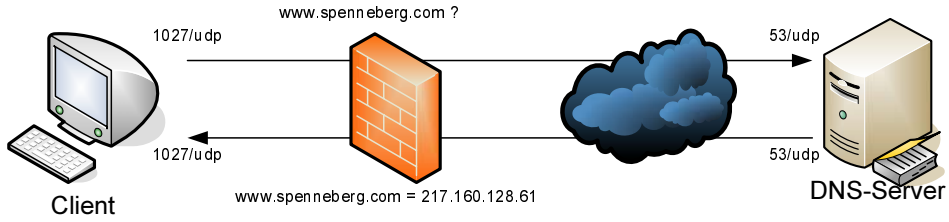


Abbildung 5.6: Der Client wird nun durch einen Paketfilter geschützt.

Hier schickt der Client 192.168.0.112 von Port 35785 ein UDP-Paket an den Server 128.176.0.12 auf dem Port 53 (domain). Der Server antwortet unter Verwendung derselben IP-Adressen und Ports. Diese Informationen können nun verwendet werden, um die Paketfilterregeln zu entwickeln.

Stellen Sie sich vor, zwischen dem Client und dem Server befindet sich ein Paketfilter, der genau diese Art von Anfragen erlauben soll (Abbildung 5.6). Dabei sei aber nicht bekannt, bei welchem DNS-Server der Client die Frage stellt. Das bedeutet, dass der Paketfilter zwei Regeln benötigt:

1. Eine Regel muss das Paket von dem Client zum Server erlauben. Die IP-Adresse des Servers ist nicht bekannt. Lediglich das Protokoll (UDP) und der Port (53) stehen fest. Vom Client ist die IP-Adresse oder der Adressbereich bekannt.

2. Die zweite Regel muss das Antwortpaket des Servers an den Client erlauben. IPchains verfügt jedoch über kein Gedächtnis. Es ist nicht in der Lage, sich zu merken, dass ein Client ein Paket an einen DNS-Server rausgeschickt hat. Daher muss diese Regel jedes theoretisch mögliche Antwortpaket akzeptieren. Da der Client aber ein Paket an jeden möglichen DNS-Server geschickt haben kann, muss diese Regel Antwortpakete von jedem theoretisch möglichen DNS-Server im Internet erlauben. Sie kann diese Pakete nur anhand des verwendeten Protokolls (UDP) und Ports (53) erkennen.

Die Regel Eins würde in IPchains-Syntax folgendermaßen lauten:

```
CLIENTS=192.168.0.0/24
ipchains -A forward -p udp -s $CLIENTS -d any/0 53 -j ACCEPT
```

Diese Regel akzeptiert (`-j ACCEPT`) UDP-Pakete (`-p udp`) mit einer Absenderadresse aus dem Netzwerk 192.168.0.0/24 (`-s`) und einer beliebigen Zieladresse (`-d`) auf dem Port 53. So kann die Anfrage nach außen zum DNS-Server gelangen. Nun muss auch die Antwort akzeptiert werden. Regel Zwei sieht folgendermaßen aus:

```
ipchains -A forward -p udp -s any/0 53 -d $CLIENTS -j ACCEPT
```

Was leisten diese Regeln nicht? Diese Regeln können nicht verhindern, dass ein Angreifer UDP-Pakete mit dem Absenderport 53 von außen nach innen schickt. Dabei

beschränken diese Regeln nicht den Zielport auf dem Client. Dies ist auch nicht möglich, da dieser Port nicht bekannt ist. Jeder Client kann einen fast beliebigen Port für seine Anfrage wählen. Bei jeder Anfrage wird er diesen auch neu wählen. Daher muss die Firewall Antworten auf jedem beliebigen Port erlauben.

Dies ist nicht ganz richtig, werden einige Leser jetzt bemerken. Und richtig, unter Unix-ähnlichen Systemen darf ein Client nur einen nicht-privilegierten Port verwenden. Dies sind die Ports 1024 bis 65535. Meist verwendet der Client nur einen bestimmten Bereich, zum Beispiel würde ein Linux 2.6-Kernel einen Port-Bereich von 32768-61000 nutzen. Die meisten anderen Systeme halten sich auch an diese Konvention. Bei einem einfachen Paketfilter nutzt man diese Tatsache aus, um die Regeln noch sicherer zu machen:

Listing 5.5: Der Client verwendet einen unprivilegierten Port für den Verbindungsaufbau.

```
CLIENTS=192.168.0.0/24
ipchains -A forward -p udp -s $CLIENTS 1024:65535 -d any/0 53 -j ACCEPT
ipchains -A forward -p udp -s any/0 53 -d $CLIENTS 1024:65535 -j ACCEPT
```

Dennoch kann die zweite Regel einen Angreifer nicht daran hindern, UDP-Pakete durch die Firewall an einen beliebigen Client auf einen unprivilegierten Port zu schicken. Diese Regel muss jedes scheinbar sinnvolle Paket durchlassen. Da es durchaus einige UDP-Dienste gibt, die einen derartigen Port verwenden, ist es möglich, durch diese Firewall eine UDP-Verbindung von außen nach innen aufzubauen, vorausgesetzt, ich verwende als Client den Port 53/udp. Gute IPchains-Paketfilterkonfigurationen schließen diese Ports wieder aus.

Tipp

Wie beeinflusse ich bei einem Angriff den Client-Port? Es gibt viele Möglichkeiten, dies zu tun. Wenn Sie aber nur schnell für einen Scan einer Firewall den Client-Port einstellen möchten, bieten die modernen Scan-Werkzeuge dies bereits an. So können Sie beim bekannten Werkzeug `nmap` (siehe Abschnitt 15.2) mit der Option `--source-port` den Client-Port einstellen. Der Befehl `nmap -sU --source-port 53 <client>` würde den Client scannen, vorausgesetzt, es wird nicht gleichzeitig NAT eingesetzt.

5.5.3 IPchains und TCP

Nachdem wir eine typische UDP-Verbindung betrachtet haben, soll nun eine TCP-Verbindung analysiert werden. Hier werden wir uns zwei verschiedene Applikationsprotokolle anschauen. Zunächst wird das HTTP-Protokoll betrachtet und anschließend das FTP-Protokoll. Wenn Sie sich hier wundern sollten, warum ich zwei Protokolle betrachte, werden Sie sich nach der Erklärung des FTP-Protokolls wahrscheinlich noch mehr wundern.

Das TCP-Transport-Protokoll ist komplizierter als das UDP-Protokoll. Es garantiert im Gegensatz zum UDP-Protokoll die Übertragung der Informationen in der richtigen Reihenfolge.

Tipp: TCP und UDP

Wenn sie nach dem Unterschied zwischen TCP und UDP gefragt werden, antworten die meisten Netzwerkadministratoren, TCP sei verbindungsorientiert und UDP verbindungslos. Fragt man genauer nach, was dies denn bedeute, stehen viele Administratoren bereits auf dem Schlauch. Sie haben es zwar alle in der Vergangenheit gelernt, aber im Laufe der Jahre wieder vergessen.

Ich möchte hier kurz erläutern, was für mich der wesentliche Unterschied zwischen diesen beiden Protokollen ist. Eine ausführlichere Betrachtung finden Sie in Abschnitt 19.4.8. Das TCP-Protokoll garantiert im Gegensatz zum UDP-Protokoll den Transport der Daten. Das bedeutet, die Applikation kann dem Protokoll vertrauen, dass alle Daten übertragen werden oder eine Fehlermeldung generiert wird. Geht ein Paket auf dem Weg verloren, so erkennt das TCP-Protokoll dies und sendet selbstständig das Paket neu. Außerdem garantiert TCP, dass die Applikation auf der Empfängerseite die Daten in derselben Reihenfolge erhält, in der sie losgeschickt wurden, selbst wenn die Pakete in unterschiedlicher Reihenfolge ankommen. UDP leistet diese Garantien nicht. Hier muss sich die Applikation im Zweifelsfall darum kümmern.

Um dies zu tun, versieht TCP jedes übertragene Byte mit einer Nummer. Dies ist die Sequenznummer. Diese Nummer bestätigt der Empfänger (Bestätigungsnummer/Acknowledgement-Nummer). Anhand der Nummer kann der Empfänger die Daten in der richtigen Reihenfolge zusammenbauen und erkennen, ob noch Daten fehlen.

Aus Sicherheitsgründen darf eine TCP-Verbindung nicht mit der Nummer 0 beginnend die Daten nummerieren. Damit nun dennoch beide Seiten erkennen können, wo die Übertragung anfängt, welche Daten übertragen wurden und welche noch fehlen, müssen sich die beiden Kommunikationspartner zu Beginn auf die verwendeten Sequenznummern einigen. Dies erfolgt im TCP-Handshake. Im ersten TCP-SYN-Paket überträgt der Client seine initiale Sequenznummer an den Server zur Synchronisation. Dieser bestätigt diese (ACK)in seinem ersten Paket und überträgt seine initiale Sequenznummer ebenfalls zur Synchronisation (SYN). Diese wird im dritten Paket nun vom Client bestätigt, und der TCP-Handshake ist erfolgreich durchgeführt worden.

TCP wird immer dann von Applikationen eingesetzt, wenn größere Datenmengen transportiert werden müssen. UDP ist ein typisches Protokoll, wenn die Datenmengen sehr klein sind, so dass sie in ein Paket passen oder die Daten zeitkritisch übertragen werden müssen. Genügt ein Paket für den Transport, so ist die Reihenfolge der Ankunft unerheblich. Ob das Paket angekommen ist, kann der Client an der fehlenden Antwort des Servers erkennen. Sind die Daten zeitkritisch, so schadet die Verzögerung durch die erneute Sendung der Daten möglicherweise mehr, als wenn diese Daten übersprungen werden. Schließlich ist es in bestimmten Umgebungen sehr unwahrscheinlich, dass Daten verloren gehen oder die Reihenfolge durcheinander gerät. Im lokalen LAN wird daher häufig tFTP für den Datentransport mit Routern eingesetzt. Dieses sehr einfache Protokoll verwendet ebenfalls UDP.

Das TCP-Protokoll benötigt einen TCP-Handshake für den Aufbau einer Verbindung. Ansonsten unterscheidet es sich aus Sicht eines Paketfilters nicht von dem UDP-Protokoll (Abschnitt 5.7).

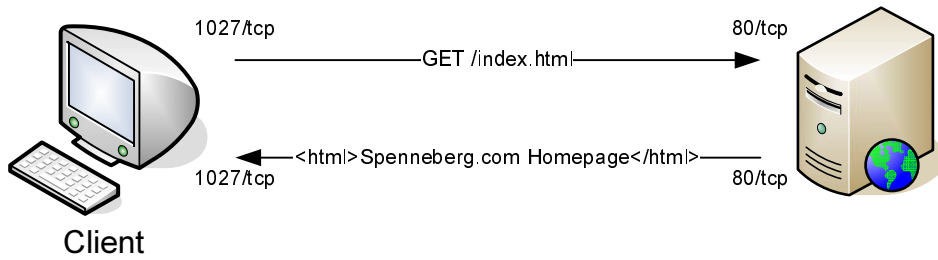


Abbildung 5.7: Der Webbrowser fragt den Webserver mit dem TCP-Protokoll auf Port 80 nach einer Webseite.

Listing 5.6: TCPDump-Mitschnitt der Web-Anfrage

```
[root@bibo root]# tcpdump -ni eth1 host www.nohup.info and port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
12:57:44.543981 IP 192.168.0.112.39305 > 217.160.128.61.http: S 795473263:795473
263(0) win 5840 <mss 1460,sackOK,timestamp 24325838 0,nop,wscale 7>
12:57:44.568941 IP 217.160.128.61.http > 192.168.0.112.39305: S 3041076941:30410
76941(0) ack 795473264 win 5792 <mss 1452,sackOK,timestamp 53796879 24325838,nop,wscale 0>
12:57:44.568972 IP 192.168.0.112.39305 > 217.160.128.61.http: . ack 1 win 46 <no
p,nop,timestamp 24325863 53796879>
12:57:44.570825 IP 192.168.0.112.39305 > 217.160.128.61.http: P 1:130(129) ack 1
 win 46 <nop,nop,timestamp 24325865 53796879>
12:57:44.600939 IP 217.160.128.61.http > 192.168.0.112.39305: . ack 130 win 6432
```

```
 <nop,nop,timestamp 53796882 24325865>
... gekürzt ...
12:57:45.627324 IP 192.168.0.112.39306 > 217.160.128.61.http: . ack 15511 win 29
5 <nop,nop,timestamp 24326922 53796983>
12:57:45.628648 IP 217.160.128.61.http > 192.168.0.112.39306: F 15511:15511(0) a
ck 140 win 6432 <nop,nop,timestamp 53796983 24326882>
12:57:45.629519 IP 192.168.0.112.39306 > 217.160.128.61.http: F 140:140(0) ack 1
5512 win 295 <nop,nop,timestamp 24326924 53796983>
12:57:45.658078 IP 217.160.128.61.http > 192.168.0.112.39306: . ack 141 win 6432
 <nop,nop,timestamp 53796988 24326924>
```

Die Regeln für diese TCP-Verbindung sind zunächst den UDP-Regeln sehr ähnlich. Lediglich der Zielport auf dem Server und das Protokoll sind angepasst worden.

```
CLIENTS=192.168.0.0/24
ipchains -A forward -p tcp -s $CLIENTS 1024:65535 -d any/0 80 -j ACCEPT
ipchains -A forward -p tcp -s any/0 80 -d $CLIENTS 1024:65535 -j ACCEPT
```

Einfache Paketfilter wie IPchains können aber bei einer TCP-Verbindung auch noch das erste Paket erkennen. Dieses Paket zeichnet sich dadurch aus, dass von allen TCP-Flags (siehe Abschnitt 19.4.8) nur das SYN-Flag für die Sequenznummersynchronisation gesetzt ist. Das erste Antwortpaket des Servers enthält bereits zusätzlich das ACK-Bit gesetzt. Da diese Pakete nur von dem Client zum Server und nicht in umgekehrter Richtung transportiert werden dürfen, kann dies in den Regeln berücksichtigt werden. IPchains bietet hierfür die Option `-y,--syn`. Diese Option erkennt das erste SYN-Paket. Als Negation `! --syn` erkennt diese Option alle Pakete außer dem ersten SYN-Paket. Die Regeln lassen sich also folgendermaßen ändern:

```
CLIENTS=192.168.0.0/24
ipchains -A forward -p tcp -s $CLIENTS 1024:65535 -d any/0 80 -j ACCEPT
ipchains -A forward -p tcp -s any/0 80 -d $CLIENTS 1024:65535 ! --syn -j ACCEPT
```

Damit wird der Empfang eines SYN-Pakets von außen nach innen nicht erlaubt. Dennoch ist es möglich, dass ein Angreifer aus einer Verbindung herausgelöste TCP-ACK- oder TCP-FIN-Pakete senden kann. Hiermit kann er zwar keine Verbindung aufbauen, aber dennoch möglicherweise wertvolle Informationen sammeln (siehe Abschnitt 15.2).

Bei einer FTP-Verbindung wird die Konfiguration der Firewall komplizierter und unsicherer. Das FTP-Protokoll verwendet mehrere TCP-Verbindungen, um die Informationen zu übertragen (siehe auch Abschnitt 32.10). Zunächst baut der Client ausgehend von einem unprivilegierten Port eine TCP-Verbindung zum Port 21 auf. Dies ist die Steuerungsverbindung (Control Connection). Diese Verbindung wird genutzt, um die Anmeldeinformationen und alle Befehle zu übertragen. Sobald aber der Server Daten zum Client übertragen muss, wird eine zusätzliche Datenverbindung geöffnet.

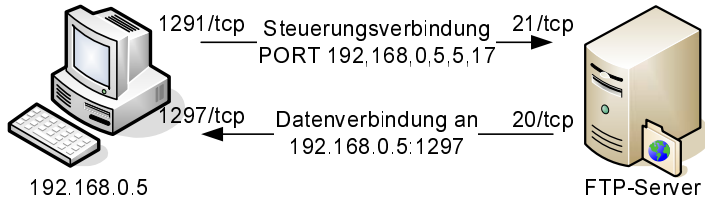


Abbildung 5.8: Bei dem aktiven FTP baut der Server eine TCP-Verbindung zum Client auf.

Für diese Datenverbindung gibt es zwei Möglichkeiten. Im klassischen Fall des aktiven FTPs wird diese Verbindung von dem Server von Port 20 zu einem unprivilegierten Port des Clients aufgebaut (siehe Abbildung 5.8). Im Fall des passiven FTPs wird die Verbindung von dem Client ausgehend von einem beliebigen unprivilegierten Port zu einem – vom Server vorher bestimmten – unprivilegierten Port des Servers aufgebaut.

Aktives FTP durch einen IPchains-Paketfilter zu erlauben, heißt Türen und Tore öffnen. Der IPchains-Paketfilter muss den Aufbau einer TCP-Verbindung von außen erlauben. Die einzigen Einschränkungen betreffen den Quellport (20) und den Zielport (1024-65535). Da dies inakzeptabel ist, wird aktives FTP von Administratoren, die Paketfilter wie IPchains einsetzen, meist nicht erlaubt.

Passives FTP ist nicht ganz so kritisch, da die Verbindungen von innen aufgebaut werden. Jedoch kann der Firewall-Administrator nicht das Ziel der Verbindung beschränken. Der Client kann eine Verbindung zu einem beliebigen unprivilegierten Port im Internet aufbauen. Filesharing-Börsen wie KaZaa nutzen auch derartige Verbindungen!

Wieso ist die Filterung so problematisch? Wenn der Paketfilter in der Lage wäre, einen Zusammenhang zwischen den Client- und den Serverpaketen und der Steuerungsverbindung und der Datenverbindung aufzubauen, würden viele Probleme entfallen!

5.5.4 IPchains und ICMP

Schließlich gibt es noch ein drittes sehr wichtiges Protokoll, das ein Paketfilter betrachten kann: das Internet Control Message Protocol (ICMP). Dieses Protokoll wird zum einen von dem Ping-Befehl verwendet und ist zum anderen für die Übertragung von Fehlerzuständen im Internet verantwortlich. Dieses Protokoll kennt keine Ports wie TCP oder UDP, sondern nur Typen und Codes.

Betrachten wir zunächst den Ping-Befehl. Dieser sendet, wie eine Client-Applikation, ein ICMP-Echo-Request-Paket an einen entfernten Rechner. Dieser Rechner antwortet, wie ein Server, mit einem ICMP-Echo-Reply-Paket.

```
[root@bibo root]# tcpdump -ni eth1 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
14:09:36.849952 IP 192.168.0.112 > 217.160.128.61: icmp 64: echo request seq 0
14:09:36.875897 IP 217.160.128.61 > 192.168.0.112: icmp 64: echo reply seq 0
```

Damit ein Client pingen kann, muss die Firewall dies erlauben. Hierzu muss sie die Echo-Request-Pakete nach außen und die Echo-Reply-Pakete nach innen passieren lassen.

ICMP wird aber auch verwendet, um Fehlermeldungen zu verschicken. Hierbei handelt es sich zum Beispiel um Fehlermeldungen, die anzeigen, dass das Ziel nicht erreichbar ist. Ist das Ziel nicht erreichbar, kann das Paket nicht zugestellt werden und wird verworfen. Mit dieser Fehlermeldung erhält der Absender die entsprechende Information. Diese Fehlermeldungen werden als Destination-Unreachable bezeichnet. Eine Filterung der Fehlermeldungen ist nur in Abhängigkeit des Typs und Codes möglich. Eine Prüfung, ob diese Fehlermeldung sich auf eine gültige Verbindung bezieht, kann von IPchains nicht durchgeführt werden!

5.5.5 IPchains und Masquerading

Einige erfahrene IPchains-Firewall-Administratoren werden bei den letzten Beispielen bereits innerlich auf die Masquerading-Funktion von IPchains hingewiesen haben. Hierbei handelt es sich um eine Art Network Address Translation, die in der Lage ist, den Zustand von Verbindungen zu überwachen und nur die Pakete durchzulassen, die Teil einer bestimmten Verbindung sind.

Das ist natürlich richtig. Wenn IPchains mit NAT eingesetzt wurde, konnte so die Sicherheit stark erhöht werden. Sobald aber auf NAT verzichtet wurde, tauchten die oben erwähnten Probleme auf. Der Firewall-Administrator konnte diese Funktion auch nicht für die eigentliche Filterung der Pakete einsetzen, sondern musste auf die Intelligenz des Masquerading-Codes vertrauen.

5.5.6 Iptables und Conntrack

Mit Iptables können Sie die oben aufgeführten IPchains-Regelsätze eins zu eins umsetzen und genau dieselben Sicherheitsprobleme erzeugen, die ich oben erläutert habe. Sie müssen lediglich die angepasste Syntax bei Iptables gegenüber IPchains beachten. Sie können aber auch durch Nutzung des Connection Tracking (es wird auch State Machine genannt) wesentlich intelligenter und sicherer filtern. Dieser Abschnitt zeigt Ihnen, wie das geht und welche Möglichkeiten sich Ihnen eröffnen. Im Kapitel 19 finden Sie weitere Hinweise zum Tuning der Verbindungsüberwachung.

Iptables verfügt über eine Verbindungsüberwachung, die Sie für die Filterung von Verbindungen einsetzen können. Während ein normaler Paketfilter Pakete filtert, kann Iptables beim Einsatz der Verbindungsüberwachung Verbindungen filtern! Sie akzeptieren ein Paket einer Netzwerkverbindung, und automatisch werden alle weiteren Pakete, die Teil dieser Verbindung sind, auch akzeptiert! Dabei erkennt das System automatisch und fehlerfrei alle weiteren Pakete, auch die Antwortpakete des Servers.

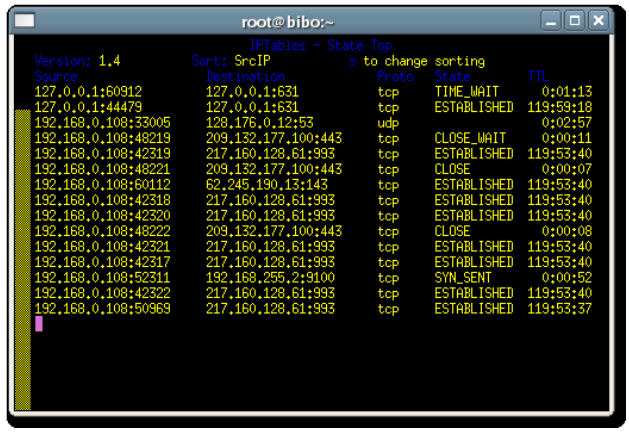


Abbildung 5.9: Der Befehl iptstate zeigt die Verbindung ähnlich dem Befehl top an.

Wie funktioniert das? Das Conntrack-System des Linux-Kernels pflegt intern eine Tabelle aller bekannten Verbindungen. Dieses Conntrack-System kann sowohl als Modul geladen werden als auch fest im Linux-Kernel einkompiliert sein. Allerdings ermöglicht das Laden des Conntrack-Systems zusätzliches Tuning über Optionen (siehe Kapitel 19). Sie laden das Modul mit dem Befehl `modprobe ip_conntrack`[7].

Sobald nun ein neues Paket den Rechner erreicht, klassifiziert das Conntrack-System dieses Paket als NEW, ESTABLISHED, RELATED oder INVALID[8]. Diese Klassifizierung erfolgt übrigens in der PREROUTING-Kette der NAT-Tabelle (siehe Kapitel 20) für Pakete, die von außen kommen, und in der OUTPUT-Kette der NAT-Tabelle für lokal generierte Pakete. Hierzu betrachtet das Conntrack-System das Paket und vergleicht es mit den bereits in der Verbindungstabelle befindlichen Verbindungen. Den aktuellen Stand der Liste können Sie sich mit dem Befehl `cat /proc/net/ip_conntrack` anzeigen lassen. Falls sich bereits Verbindungen in dieser Tabelle befinden, werden sie der folgenden ähneln.

Listing 5.7: Eine TCP-Verbindung in /proc/net/ipconntrack

```
tcp      6 431995 ESTABLISHED src=192.168.0.112 dst=205.156.51.200 sport=36188 dport=80
  src=205.156.51.200 dst=192.168.0.112 sport=80 dport=36188 [ASSURED] use=1
```

Eine aufbereitete Darstellung (Abbildung 5.9) der Tabelle kann mit dem Befehl `iptstate` angezeigt werden (siehe auch Abschnitt 12.2).

[7] Sobald Sie das Conntrack-System laden, werden alle Pakete von dem Conntrack-System automatisch defragmentiert. Während Sie die Defragmentierung bis zum Linux-Kernel 2.2 ein- und abschalten konnten, ist dies nun nicht mehr möglich (siehe auch Abschnitt 16.1.6).

[8] Wenn der Kernel die Unterstützung für die Raw-Tabelle besitzt, ist auch noch der Zustand `UNTRACKED` verfügbar.

Das Conntrack-System vergleicht nun das Transportprotokoll (TCP, UDP, ICMP etc.), die IP-Adressen und, wenn wie bei TCP und UDP vorhanden, die Ports der Einträge mit dem Paket. Das Paket erhält dann einen der folgenden vier Zustände:

- **NEW**. Das Paket erhält den Zustand neu, wenn ein Paket mit dieser Kombination aus Protokoll, IP-Adressen und Ports in der Tabelle noch nicht existiert. Diese neue Verbindung wird aber nicht automatisch in der Tabelle eingetragen.
- **ESTABLISHED**. Das Paket erhält den Zustand ESTABLISHED, wenn es mit seinem Protokoll, den IP-Adressen und den Ports genau auf eine Verbindung in der Tabelle passt. Dabei ist es einerlei, in welcher Richtung das Paket transportiert wird. Handelt es sich um das erste derartige Paket, wird gleichzeitig der Zustand der Verbindung in der Tabelle aktualisiert, so dass diese Verbindung nun den Zustand `[ASSURED]` hat.
- **RELATED**. Das Paket erhält den Zustand RELATED, wenn es in einer besonderen Beziehung zu einer bereits in der Tabelle vorhandenen Verbindung steht. Hierbei handelt es sich typischerweise um ICMP-Fehlermeldungen, die sich auf eine aufgebaute Verbindung beziehen. Diese können nicht den Zustand ESTABLISHED erhalten, da sie bereits ein anderes Protokoll (ICMP) verwenden als die in der Tabelle eingetragene Verbindung. Das Conntrack-System kann jedoch erkennen, auf welche Verbindung sich eine ICMP-Fehlermeldung bezieht. Existiert diese Verbindung in der Tabelle, bekommt das Paket der ICMP-Fehlermeldung den Zustand RELATED. Außerdem werden auch FTP-Datenverbindungen unter Umständen als RELATED angesehen (siehe unten).
- **INVALID**. Dass ein Paket den Zustand INVALID erhält, kann zwei Ursachen haben. Entweder verfügt das System nicht über ausreichend Ressourcen, um den Zustand zu ermitteln und zu speichern, oder es handelt sich um eine ICMP-Fehlermeldung, die sich auf eine nicht existente Verbindung bezieht.

Achtung: Maximale Anzahl der Verbindungen in der Tabelle

Die Größe der Tabelle zur Verbindungsüberwachung ist natürlich begrenzt. Allerdings können Sie die Größe dieser Tabelle, wie auch viele andere Parameter des Connection Tracking, anpassen und tunen. Dies wird aber in einem eigenen Kapitel (siehe Kapitel 19) beschrieben.

Mit Hilfe dieses Systems ist es nun möglich, komplett auf die löchrigen Regeln zu verzichten, die mögliche Antwortpakete für aufgebaute Verbindungen zulassen. Um dies zu verdeutlichen, sollen die oben aufgeführten Beispiele nun mit Iptables und Conntrack nachvollzogen werden.

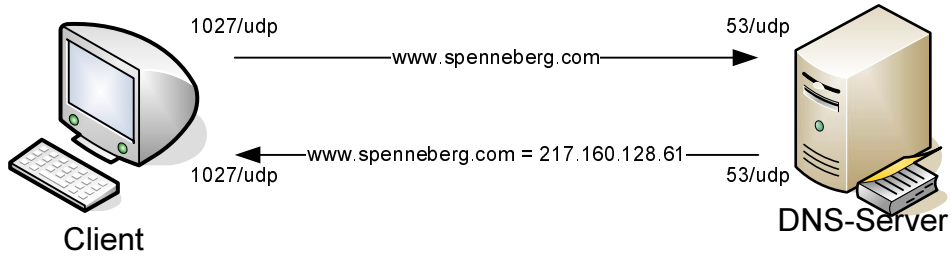


Abbildung 5.10: Der DNS-Client fragt den DNS-Server mit dem UDP-Protokoll auf Port 53 nach der IP-Adresse für www.spenneberg.com.

Conntrack und UDP

Wir beginnen wieder mit dem Beispiel einer DNS-Verbindung (Abbildung 5.10). Hier sendet der Client ein Paket an den DNS-Server und der DNS-Server, antwortet mit einem Paket.

Wenn Sie einem Client durch Ihren Paketfilter den Zugriff auf einen beliebigen DNS-Server erlauben möchten, benötigen Sie folgende Regel:

Listing 5.8: Der Client baut mit seiner DNS-Anfrage eine neue UDP-Verbindung auf.

```
CLIENTS=192.168.0.0/24
iptables -A FORWARD -s $CLIENTS -p udp --dport 53 -m state --state NEW -j ACCEPT
```

Diese Regel erlaubt (`-j ACCEPT`) es einem Client (`-s $CLIENTS`), ein UDP Paket (`-p udp`) an den Zielport 53 (`--dport 53`) zu schicken, wenn die Zustandsmaschine (`-m state`) dieses Paket als neu kategorisiert (`--state NEW`). Zusätzlich merkt sich die Zustandsmaschine diese Verbindung nun in ihrer Tabelle. Um die Antwort des DNS-Servers auch zu erlauben, benötigen Sie die folgende Regel:

Listing 5.9: Akzeptiere alle weiteren Pakete in der Verbindung

```
iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT
```

Diese Regel prüft, ob es sich beim Paket um ein Paket einer Verbindung handelt, die bereits erlaubt und aufgebaut wurde (`--state ESTABLISHED`). Ist dies der Fall, wird auch dieses Paket akzeptiert (`-j ACCEPT`). Es ist hier nicht nötig, erneut den Port zu testen. Verwendet das Paket einen anderen Port als 53/udp, dann gehört es nicht zu der aufgebauten Verbindung und wird daher verworfen.

Wie stellt sich das in der Verbindungstabelle dar? Nachdem das erste Paket von dem Client durch die Firewall an den Server geschickt wurde, wird die Zustandsmaschine folgenden Eintrag in der Zustandstabelle protokollieren:

```
udp      17 28 src=10.0.2.100 dst=5.255.255.254 sport=1024 dport=53 [UNREPLIED]
  src=5.255.255.254 dst=10.0.2.100 sport=53 dport=1024 use=1 mark=0
```

Die Angabe [UNREPLIED] zeigt an, dass die Zustandsmaschine noch keine Antwort für dieses Paket verarbeitet hat. Die weiteren Angaben des Eintrags sind das Protokoll (udp) und die Protokollnummer (17). Anschließend wird die Verweildauer des Eintrags in der Tabelle in Sekunden (28) angegeben. Nun kommen die Absender- und die Zieladresse sowie der Absender- und der Zielport. Eine genauere Erklärung der Angaben finden Sie in Kapitel 19.

Sobald nun von dem Server eine Antwort geschickt wird, ändert sich der Zustand in der Tabelle:

Listing 5.10: Die Einträge der Zustandstabelle können über die Datei /proc/net/ip_conntrack betrachtet werden.

```
udp      17 20 src=10.0.2.100 dst=5.255.255.254 sport=1024 dport=53 src=5.255.255.254
  dst=10.0.2.100 sport=53 dport=1024 use=1 mark=0
```

Nun ist der Status [UNREPLIED] nicht mehr vorhanden. Die Zustandsmaschine hat für diese Verbindung Pakete in beiden Richtungen gesehen und zugelassen.

Ein aufmerksamer Leser mag sich nun fragen, wie lange die UDP-Verbindung in der Tabelle verbleibt. Da das UDP-Protokoll keinen Verbindungsabbau kennt, kann die Zustandsmaschine dies nur über Zeitgeber lösen. Ein Standardkernel erlaubt eine UDP-Verbindung im Zustand UNREPLIED für 30 Sekunden in der Tabelle. Sobald die Zustandsmaschine Antwortpakete verarbeitet hat, bleibt die Verbindung für 180 Sekunden in der Zustandstabelle. Jedes weitere Paket dieser Verbindung setzt diese Zähler wieder auf ihre Ausgangswerte zurück.

Conntrack und TCP

Bei dem TCP-Protokoll wollen wir auch zunächst wieder eine HTTP-Verbindung betrachten. In Abbildung 5.11 ist noch einmal die HTTP-Verbindung schematisch gezeigt.

Wenn Sie nun einem Client durch Ihren Paketfilter den Zugriff auf einen beliebigen Webserver im internen Netz erlauben möchten, können Sie die Regeln, die wir für

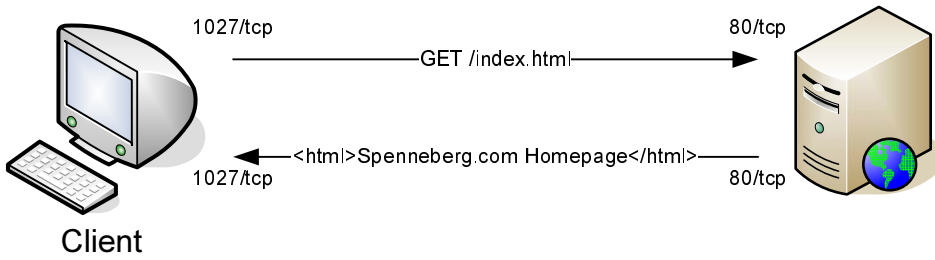


Abbildung 5.11: Der Webbrowser fragt den Webserver mit dem TCP-Protokoll auf Port 80 nach einer Webseite.

den DNS-Server aufgestellt haben, fast unverändert übernehmen. Zunächst benötigen Sie auch eine Regel, die den Aufbau der Verbindung von innen nach außen erlaubt:

```
CLIENTS=192.168.0.0/24
iptables -A FORWARD -s $CLIENTS -p tcp --dport 80 -m state --state NEW -j ACCEPT
```

Diese Regel erlaubt es dem ersten Paket einer jeden HTTP-Verbindung, von innen nach außen zu gelangen. Dieses erste Paket wird von der Zustandsmaschine als NEW kategorisiert[9].

Damit alle weiteren Pakete der Verbindung zugelassen werden, ist eine zweite Regel erforderlich:

```
iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT
```

Aufmerksame Leser werden feststellen, dass sich diese Regel nicht von der entsprechenden Regel für die UDP-Verbindungen unterscheidet. Sobald nun ein Paket von dieser Regel bearbeitet wird, das zu einer Verbindung gehört, die sich bereits in der Zustandstabelle befindet, wird das Paket akzeptiert. Es genügt als eine einzige Regel, um alle weiteren Pakete aufgebauter Verbindungen zu akzeptieren! Während Sie bei IPchains jeweils Regeln für die Rückrichtungen brauchten, genügt hier eine universelle Regel! Die Anzahl der Regeln ist daher bei Iptables wesentlich kleiner.

Auch die TCP-Verbindungen werden in der Zustandstabelle gepflegt und können über die Datei `/proc/net/ip_conntrack` betrachtet werden. Allerdings besitzen diese Einträge auch weitere Zustände, die daher hier kurz vorgestellt werden sollen. Insgesamt kennt die Zustandsmaschine acht verschiedene Zustände einer TCP-Verbindung, die hier aber nicht alle gezeigt werden können. Sie finden weitere Informationen im Kapitel 19.

Sobald der Client sein erstes Paket schickt, befindet sich in der Zustandstabelle folgender Eintrag:

```
tcp      6 115 SYN_SENT src=10.0.2.100 dst=5.255.255.254 sport=1024 dport=80 [UNREPLIED]
  src=5.255.255.254 dst=10.0.2.100 sport=80 dport=1024 use=1 mark=0
```

Normalerweise sehen Sie diesen Eintrag gar nicht, da der Server sofort antwortet! Hier hat die Verbindung aber noch den Zustand [UNREPLIED]. Zusätzlich sehen Sie den Zustand SYN_SENT. Dies ist eine zusätzliche Information über die Verbindung.

Sobald der TCP-Handshake komplett vollzogen wurde, wechselt die Verbindung ihren Zustand:

[9] Die Zustandsmaschine macht hier aber noch zusätzliche Einschränkungen: Damit ein TCP-Paket den Zustand NEW haben kann, muss es sich um ein Paket handeln, das entweder nur das TCP-SYN-Flag oder das TCP-ACK-Flag oder kein Flag gesetzt hat. Die Zustand der TCP-Flags URG und PSH ist hierbei unerheblich.

```
tcp      6 431996 ESTABLISHED src=10.0.2.100 dst=5.255.255.254 sport=1024 dport=80
  src=5.255.255.254 dst=10.0.2.100 sport=80 dport=1024 [ASSURED] use=1 mark=0
```

Da nun Pakete in beiden Richtungen gesehen wurden, erhält die Verbindung den Zustand [ASSURED] und zusätzlich die Information ESTABLISHED.

Sobald ein Client nun ein TCP-FIN-Paket für den Abbau der Verbindung schickt, wechselt wieder der Zustand:

```
tcp      6 119 FIN_WAIT src=10.0.2.100 dst=5.255.255.254 sport=1024 dport=80
  src=5.255.255.254 dst=10.0.2.100 sport=80 dport=1024 [ASSURED] use=1 mark=0
```

Die Verbindung bleibt [ASSURED], hat aber nun zusätzlich den Zustand FIN_WAIT. Sobald nun auch die Gegenseite ihr FIN gesendet hat, wechselt die Verbindung abermals den Zustand:

```
tcp      6 119 TIME_WAIT src=10.0.2.100 dst=5.255.255.254 sport=1024 dport=80
  src=5.255.255.254 dst=10.0.2.100 sport=80 dport=1024 [ASSURED] use=1 mark=0
```

Diese verschiedenen Zustände sind wichtig, da die Zustandsmaschine diesen verschiedenen Zuständen unterschiedliche Verweildauern in der Zustandstabelle einräumt. So hat der Zustand SYN_SENT zum Beispiel eine Verweildauer von 2 Minuten in der Zustandstabelle. Das bedeutet, dass innerhalb von 2 Minuten das nächste Paket der Verbindung die Firewall erreichen muss, damit die Verbindung nicht aus der Tabelle entfernt wird. Der Zustand ESTABLISHED hat eine Verweildauer von 5 Tagen! Je nach verwendetem Kernel können Sie diese Zeiten anpassen. Die weiteren Zeiten und ihre Anpassung werden im Kapitel 19 erklärt.

Erinnern Sie sich noch an das FTP-Protokoll und die Probleme, dieses Protokoll mit IPchains zu filtern? Nun, die Zustandsmaschine bietet auch hier eine geniale Lösung an. Bei dem FTP-Protokoll handeln der Client und der Server dynamische Ports für den Transport der Daten aus. Diese Ports können daher nicht von vornherein in den Regeln berücksichtigt werden. Jedoch werden diese Informationen ja in dem Moment, in dem sie benötigt werden, live übertragen. Die Zustandsmaschine besitzt speziellen Code, der diese Informationen auslesen und verwerten kann. Dies ist das `ip_conntrack_ftp`-Kernelmodul. Dieser Code kann als Modul (empfehlenswert) oder fest in den Kernel eingebaut werden. Sobald dieses Modul geladen wurde (oder fest eingebaut wurde), ist es aktiv. Es überwacht dann alle Pakete, die an den Port 21 (FTP) gehen, und analysiert diese. Sobald eine Datenverbindung über die Steuerungsverbindung angekündigt wird, extrahiert es die Daten und trägt die resultierende zu erwartende Datenverbindung in der Zustandstabelle ein. Alle Pakete, die anschließend auf diese Verbindung passen, erhalten den Zustand RELATED. Wenn Sie also FTP-Verbindungen (aktiv wie passiv) sicher durch Ihre Firewall erlauben wollen, genügen die folgenden Befehle:

```
modprobe ip_conntrack_ftp
iptables -A FORWARD -s $CLIENTS -p tcp --dport 21 -m state --state NEW -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Die erste Zeile lädt das Modul zur Erkennung der Datenverbindungen[10]. Die zweite Zeile erlaubt den Aufbau der FTP-Steuerungsverbindung. Die dritte Zeile schließlich erlaubt alle Pakete, die zur FTP-Steuerungsverbindung gehören, und alle von der Zustandsmaschine erkannten FTP-Datenverbindungen. So können Sie sicher FTP-Verkehr filtern!

Conntrack und ICMP

Kommen wir nun zum dritten sehr wichtigen Protokoll bei der Definition von Firewall-Regeln, dem ICMP-Protokoll. Wie bereits gesagt, wird dieses Protokoll sowohl für die Meldung von Übertragungsfehlern als auch für den Ping-Befehl genutzt.

Beginnen wir mit dem Ping-Befehl. Erfreulicherweise betrachtet die Zustandsmaschine die Pakete, die von dem Ping-Befehl erzeugt werden, wie die Pakete, die zwischen einem Client und einem Server ausgetauscht werden. Eine Ping-Anfrage (ICMP-Echo-Request) baut eine Verbindung auf und erhält den Zustand NEW. Eine Ping-Antwort (ICMP-Echo-Reply) wird von der Zustandsmaschine als ESTABLISHED eingeordnet und entfernt auch sofort die Verbindung wieder aus der Tabelle. Das bedeutet, dass für jedes ausgesandte Echo-Request-Paket nur ein, und zwar das richtige Echo-Reply-Paket zugelassen wird. Die Zuordnung der einzelnen Pakete erfolgt über die ICMP-Sequenznummer.

Ausgehend von unserem Firewall-Szenario benötigen Sie die folgende Regel, um nun das Echo-Request-Paket zuzulassen:

```
CLIENTS=192.168.0.0/24
iptables -A FORWARD -s $CLIENTS -p icmp --icmp-type echo-request -m state
  --state NEW -j ACCEPT
```

Diese Regel lässt ein neues Paket (`-m state --state NEW`) eines Clients (`-s $CLIENTS`) zu (`-j ACCEPT`), wenn es das Protokoll ICMP (`-p icmp`) und den ICMP-Typ Echo-Request (`--icmp-type echo-request`) verwendet.

Nun benötigen Sie noch eine Regel, die die Antwortpakete erlaubt. Hier genügt wieder die bereits oben vorgestellte allgemeine Regel, die alle Pakete mit dem Zustand ESTABLISHED erlaubt:

```
iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT
```

[10] Wenn Sie einen ungewöhnlichen FTP-Server verwenden, der nicht auf dem Port 21, sondern auf einem anderen Port Verbindungen entgegennimmt, wird das Modul die Verbindung nicht erkennen. Hierfür können Sie beim Laden des Moduls eine Liste von bis zu 8 Ports angeben (mit dem Parameter `ports`), die das Modul betrachten soll. Dies ist nicht möglich, wenn der Code fest in den Kernel integriert wurde!

Wie sieht das nun in der Zustandstabelle aus? Nachdem die Firewall das ICMP-Echo-Request-Paket gesehen und verarbeitet hat, können Sie den folgenden Eintrag in der Zustandstabelle beobachten:

```
icmp     1 29 src=10.0.2.100 dst=5.255.255.254 type=8 code=0 id=31489 [UNREPLIED]
  src=5.255.255.254 dst=10.0.2.100 type=0 code=0 id=31489 use=1 mark=0
```

In den meisten Fällen werden Sie diesen Eintrag nie sehen, da er direkt gelöscht wird, sobald die Zustandsmaschine das ICMP-Echo-Reply-Paket sieht. So können Sie Ping-Pakete zustandsorientiert filtern. Sie müssen nicht grundsätzlich alle Reply-Pakete durchlassen wie bei IPchains.

Die Verbindung verbleibt übrigens im Zustand UNREPLIED für maximal 30 Sekunden in der Verbindungstabelle.

Wie behandelt die Zustandsmaschine nun ICMP-Fehlermeldungen? Erfreulicherweise erkennt die Zustandsmaschine die Fehlermeldungen und kann diese den Verbindungen in der Zustandstabelle zuordnen. Dabei erkennt sie, ob sich die Fehlermeldung auf eine der Verbindungen in der Tabelle bezieht oder nicht. Ist das der Fall, so erhält das Paket den Zustand RELATED. Ist das nicht der Fall, so ist das Paket INVALID. So können Sie alle Fehlermeldungen sicher mit einer Regel filtern:

```
iptables -A FORWARD -m state --state RELATED -j ACCEPT
```

Diese Regel akzeptiert auch FTP-Datenverbindungen vom Zustand RELATED. Wenn Sie das nicht möchten, können Sie das auch für ICMP-Pakete einschränken:

```
iptables -A FORWARD -p icmp -m state --state RELATED -j ACCEPT
```

Sobald die Zustandsmaschine übrigens eine Fehlermeldung erkennt und zuordnen kann, führt dies auch zur Entfernung der betroffenen Verbindung aus der Zustandstabelle!

Conntrack und alle weiteren generischen Protokolle

Alle weiteren IP-Protokolle, wie IGMP, GRE, ESP und so weiter, können auch von Conntrack überwacht werden[11]. Ansonsten erfolgt die Filterung der generischen Protokolle ähnlich dem UDP-Protokoll. Das erste Paket erhält den Status NEW, während alle weiteren Pakete den Status ESTABLISHED erhalten. Um zum Beispiel das ESP-Protokoll zustandsorientiert zu filtern, verwenden Sie die folgenden Regeln:

```
CLIENTS=192.168.0.0/24
iptables -A FORWARD -s $CLIENTS -p 50 -m state --state NEW -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT
```

[11] Da jedoch diese Protokolle weder über Ports noch über ICMP-IDs verfügen, ist Conntrack nicht in der Lage, gleichzeitig mehrere derartige Verbindungen zu überwachen. Für das PPTP-Protokoll gibt es hier einen besonderen Patch, der dies doch wieder ermöglicht.

Das ESP-Protokoll ist das IP-Protokoll 50 (siehe `/etc/protocols`). Die erste Iptables-Regel akzeptiert jedes neue Paket eines Clients. Die zweite Regel akzeptiert alle Pakete, die zu dieser aufgebauten Verbindung gehören.

Achtung

Die zustandsorientierte Filterung dieser Protokolle ist nicht einfach, da Conntrack keine Informationen über den tatsächlichen Zustand der Verbindung extrahieren kann. Alle Pakete werden gleichwertig behandelt. Zur Überwachung des Zustands der Verbindung werden lediglich Zeitgeber eingesetzt, die entscheiden, ob eine Verbindung beendet wurde oder nicht (siehe Kapitel 19). Dies führt häufig zu Problemen. Daher sollten Sie überlegen, ob Sie diese Protokolle besser zustandslos filtern. Dies ist mit den folgenden zwei Zeilen möglich:

```
CLIENTS=192.168.0.0/24
iptables -A FORWARD -s $CLIENTS -p 50 -j ACCEPT
iptables -A FORWARD -d $CLIENTS -p 50 -j ACCEPT
```

5.6 Filter-Regeln

Sie haben bereits in den Abschnitten 5.2 und 5.3 erste Filterregeln erzeugt. Dieses Thema soll in diesem Abschnitt vertieft werden. Während Sie im Abschnitt 5.2 nur einzelne Regeln zum Test der Funktionalität erzeugt haben, ist im Abschnitt 5.3 bereits ein funktionsfähiges Firewall-Skript entstanden. Dieses wies jedoch lediglich Regeln auf, die Verbindungen durch die Firewall von innen nach außen erlaubten. Hier wurden dann aber alle denkbaren Verbindungen zugelassen. Weitere Verbindungen auf dem Gateway direkt wurden von dem Skript nicht geduldet. Für den ersten Start ist dies meist ausreichend, anschließend aber häufig vollkommen indiskutabel.

Was fehlt? Nun in vielen Fällen sind zusätzliche Verbindungen erwünscht, die von der Firewall abgehen oder auf der Firewall ankommen, da aus Budget-Gründen auf der Firewall zusätzlich zum Beispiel ein Squid-Proxy oder ein Postfix-Mailserver installiert werden sollen. Außerdem ist es für viele Firmen indiskutabel, alle Verbindungen von innen nach außen zu erlauben. Meist existiert bereits in den Firmen eine Benutzerrichtlinie, die genau festlegt, welche Dienste die Benutzer beim Zugriff auf das Internet nutzen dürfen und zu welchem Zweck. Es ist dann sinnvoll, bei der Definition der Regeln nur diese Dienste zu erlauben, um so die Benutzer vor sich selbst zu schützen.

Im Folgenden sollen diese Regeln vorgestellt und das Skript aus Abschnitt 5.3 entsprechend angepasst werden.

Zunächst wollen wir die Regeln betrachten, die notwendig sind, um Dienste direkt auf der Firewall anzusprechen. Da die Firewall aber nicht ganz ohne Schutz geöffnet

werden soll, ist es sinnvoll, diesen Zugriff nur auf wenige Dienste zu beschränken. Ein typischer Dienst, der häufig gewünscht wird, ist der Secure-Shell-Dienst (sshd), mit dem eine Fernadministration der Firewall möglich ist. Wenn Sie von innen auf diesen Dienst zugreifen möchten, benötigen Sie folgende Regel:

Listing 5.11: Erlaube den Aufbau einer SSH-Verbindung von innen.

```
$IPTABLES -A INPUT -s $CLIENTS -i $INTDEV -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

Diese Regel wird an die INPUT-Kette angehängt. Diese Kette analysiert sämtliche Pakete, die von außen an die Firewall gesendet werden. Zur Erläuterung sind in Abbildung 5.12 noch einmal die Ketten der Filter-Tabelle dargestellt.

Wenn Sie diese Abbildung betrachten, werden Sie erkennen, dass sämtliche Pakete, die die Firewall von außen erreichen und an die Firewall gerichtet sind und nicht weitergeleitet werden, von der INPUT-Kette verarbeitet werden. Unsere neue Regel akzeptiert in der INPUT-Kette alle Pakete, die eine neue TCP-Verbindung (`-p tcp`) auf dem Port 22 (`--dport 22`) öffnen.

Nun müssen Sie auch die Antworten der Firewall an den SSH-Client zulassen. Hierzu ist eine entsprechende Regel in der OUTPUT-Kette erforderlich. Diese Kette analysiert alle Pakete, die auf der Firewall erzeugt werden und diese verlassen, also auch die Antwortpakete des Secure-Shell-Servers.

```
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Diese Aufgabe kann sehr leicht der Zustandskontrolle übertragen werden. Diese Regel akzeptiert in der OUTPUT-Kette alle Pakete, die zu erlaubten aufgebauten Verbindungen gehören oder wie eine Fehlermeldung sich auf diese beziehen. Eine erneute Prüfung des Ports ist hier nicht erforderlich, denn nur Verbindungen, die wir vorher erlaubt haben, werden in die Verbindungstabelle aufgenommen.

Damit ist das Regelwerk aber noch nicht ganz komplett. Auch der SSH-Client wird weitere Pakete schicken, die nun nicht mehr den Zustand NEW, sondern den Zustand ESTABLISHED oder im Falle einer Fehlermeldung RELATED haben können.

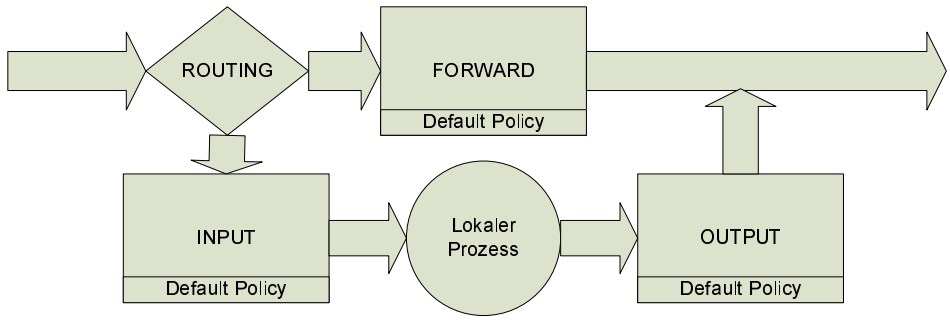


Abbildung 5.12: Die Filtertabelle besteht aus drei Ketten.

Um auch diese Pakete auf der Firewall zu erlauben, ist es erforderlich, dass auch in der INPUT-Kette diese Pakete erlaubt werden:

```
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Nach diesem Muster können Sie nun weitere Dienste hinzufügen. Möchten Sie zum Beispiel auch von außen auf den SSH-Server zugreifen, genügt nun die folgende zusätzliche Regel:

Listing 5.12: Erlaube den Zugriff mit SSH von außen.

```
$IPTABLES -A INPUT -i $EXTDEV -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

Möchten Sie einen Webserver auf der Firewall betreiben, der von außen erreichbar sein soll, so genügt nun die folgende Regel:

Listing 5.13: Erlaube den Zugriff mit SSH von außen.

```
$IPTABLES -A INPUT -i $EXTDEV -p tcp --dport 80 -m state --state NEW -j ACCEPT
```

Achtung

Ich halte es nicht für eine gute Idee, auf der Firewall gleichzeitig auch noch weitere Dienste, wie SSH und HTTP, anzubieten. Dennoch weiß ich, dass es in vielen Umgebungen zwingend erforderlich ist, da das Budget für dedizierte Systeme häufig fehlt. Dennoch sollten Sie auf einer Firewall nur die nötigen Dienste installieren und betreiben. Falls aus Kostengründen dies nicht möglich ist, sollten Sie mindestens über eine Virtualisierung nachdenken.

Auf der anderen Seite können Sie natürlich auf jedem Linux-Server so eine lokale Firewall installieren und nutzen! Dies wird aber noch im Kapitel 8 genauer besprochen.

5.7 Die NAT-Tabelle und -Regeln

Jetzt sehen wir uns die NAT-Tabelle an. In den letzten Abschnitten haben Sie bereits einige NAT-Regeln aufgesetzt. Dabei handelte es sich um Regeln, die die Absenderadresse von Paketen maskieren konnten. In diesem Abschnitt will ich nun alle Möglichkeiten der NAT-Tabelle vorstellen und kurz erläutern. Ausführlichere technische Hinweise finden Sie im Kapitel 20.

Die NAT-Tabelle hat insgesamt drei Ketten: OUTPUT, PREROUTING und POSTROUTING. Diese drei Ketten sind komplett eigenständige Ketten und sind nicht identisch mit gleichnamigen Ketten der anderen Tabellen. Die Abbildung 5.13 zeigt, wie sich die Tabellen in die Filtertabelle einbinden.

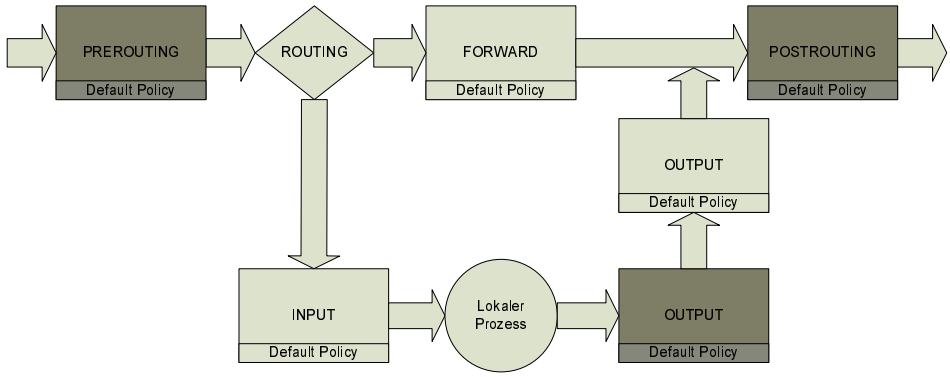


Abbildung 5.13: Die NAT-Tabelle besteht aus drei Ketten.

Bei der Network Address Translation ändert das System die Addressierung eines Pakets. Es gibt grundsätzlich zwei verschiedene Arten der Network Address Translation (NAT):

- Source-NAT: Hier wird die Absender-Adresse geändert.
- Destination-NAT: Hier wird die Zieladresse geändert.

Ein Source-NAT ist nur in der POSTROUTING-Kette der NAT-Tabelle erlaubt. Ein Destination-NAT ist nur in der PREROUTING- und der OUTPUT-Kette erlaubt. Wenn Sie sich die Abbildung 5.13 kurz anschauen, wird Ihnen auch sofort der Sinn klar.

Bei dem Source-NAT ändert die Firewall die Absenderadresse. Da das in der POSTROUTING-Kette erfolgt, ist sichergestellt, dass die Filterregeln in der FORWARD- und der OUTPUT-Kette das Paket vor der Adressänderung analysieren. Ihre Filterregeln betrachten also das originale Paket mit der »echten« Absenderadresse.

Bei dem Destination-NAT ändert die Firewall die Zieladresse. Dies passiert in der PREROUTING- oder der OUTPUT-Kette der NAT-Tabelle und damit vor der Analyse durch die entsprechenden Filterketten. Bei diesem NAT wird die scheinbare Zieladresse durch eine neue tatsächliche Zieladresse ausgetauscht. Die Filtertabelle betrachtet nun also wieder das Paket mit der »echten« Zieladresse!

Im Folgenden betrachten wir zunächst das Source-NAT und dann das Destination-NAT ein wenig genauer. Dabei werden Sie für beide Fälle auch ein paar Beispielregeln kennen lernen und in Ihrem Skript einbauen.

5.7.1 Source-NAT

Das Source-NAT ändert die Absender-Adresse eines Pakets. Dies ist häufig bei der Anbindung von Netzwerken an das Internet erforderlich. Lokale Netzwerke werden üblicherweise unter Zuhilfenahme von so genannten privaten IP-Adressen

aufgebaut. Hierbei handelt es sich um spezielle IP-Adressen, die im Internet nicht verwendet werden.

Exkurs: Private IP-Adressen nach RFC 1918

Bei dem Aufbau eines Netzes ist es zwingend erforderlich, dass die verwendeten IP-Adressen nicht doppelt verwendet werden, sondern eindeutig sind. Dies gilt auch, wenn mehrere Netze miteinander verbunden werden. Sobald Sie ein Netz mit dem Internet verbinden, müssen Sie auch hier die Eindeutigkeit der verwendeten IP-Adressen sicherstellen. Das bedeutet für Sie, dass Sie garantieren müssen, dass die von Ihnen verwendeten IP-Adressen nicht im Internet genutzt werden! Das ist unmöglich, solange Sie nicht wissen, dass bestimmte IP-Adressen im Internet »verboten« sind. Hierzu wurde der RFC1918[12] geschaffen. Dieser RFC (Address Allocation for Private Internets) beschreibt die privaten IP-Adressen.

Die folgenden IP-Adressen werden als private IP-Adressen reserviert:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Sobald Sie Ihre eigenen Netze mit diesen IP-Adressen aufbauen, erzeugen Sie bei einer Anbindung an das Internet keinen IP-Adresskonflikt. Für kleine Netze ist der Bereich 192.168.0.0/24 üblich.

Wenn Sie jedoch private IP-Adressen für den Aufbau Ihres Netzes verwenden und nun das Netz mit dem Internet verbinden, haben Sie wieder ein Problem. Es kann zwar nun nicht mehr zum Adresskonflikt kommen, jedoch werden Sie auch keine Antwort erhalten. Betrachten Sie die Abbildung 5.14.

Der Client sendet das Paket mit seiner privaten Absenderadresse über seinen Router in das Internet, wo es den Webserver erreicht. Der Webserver beantwortet das Paket und schickt sein Antwortpaket an die private Adresse des Clients. Da diese Adressen jedoch im Internet verboten sind, wissen die Internet-Router nicht, wohin sie dieses Antwortpaket weiterleiten sollen. Das Paket wird mit der Fehlermeldung »Ziel nicht erreichbar« (Destination unreachable) verworfen.

Für diesen Zweck wurde nun das Source-NAT entwickelt. Dabei kann der Router des Clients dessen private IP-Adresse gegen eine offizielle IP-Adresse austauschen, deren Ort im Internet bekannt ist (siehe Abbildung 5.15). Damit die Antworten auch beim Router wieder ankommen, verwendet man hier die offizielle Internet-Adresse des Routers selbst. Grundsätzlich wäre es auch möglich, hier irgendeine andere Adresse einzutragen, jedoch würden die Antwortpakete des Webservers nicht beim Router landen und damit nie den Client erreichen.

[12] Sie können die RFCs im Internet auf der Webseite *http://www.rfc-editor.org* nachlesen.

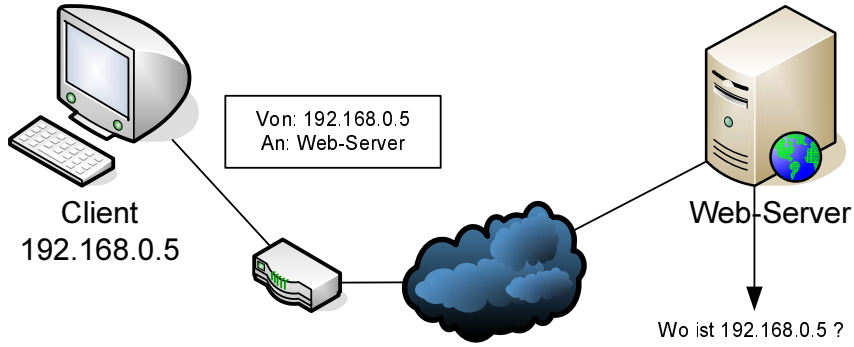


Abbildung 5.14: Ein Rechner im Internet kann auf einen Verbindungsaufbau mit privater IP-Adresse nicht reagieren.

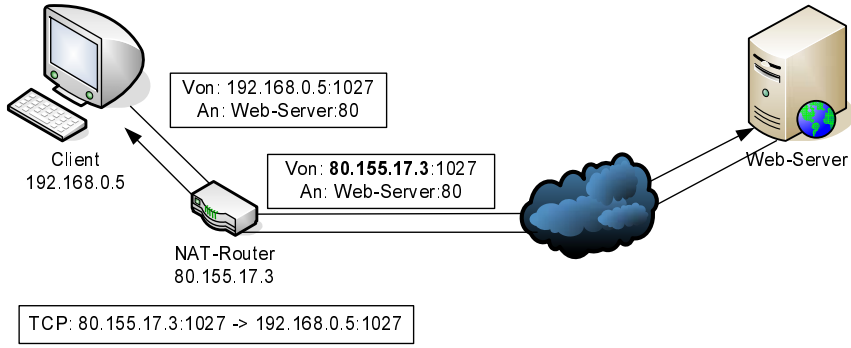


Abbildung 5.15: Bei dem Source-NAT tauscht der Router die private IP-Adresse des Clients gegen seine eigene offizielle IP-Adresse aus und merkt sich diese Tatsache in einer Tabelle.

Der Router merkt sich die Verbindungen, die von ihm genattet wurden, damit er alle weiteren Pakete der Verbindungen identisch natten kann und auch die Antworten aus dem Internet wieder an die richtigen Clients nach innen weitersenden kann. Iptables benötigt hierfür das `ip_conntrack`-Modul, das auch für die Zustandsüberwachung verantwortlich ist.

Tipp

Sobald Sie nur eine offizielle IP-Adresse für das Source-NAT von mehreren Clients verwenden, handelt es sich eigentlich nicht mehr um ein NAT (Network Address Translation), sondern um ein NAPT (Network Address and Port Translation). Dies wollen wir hier aber nicht genauer besprechen. Sie finden hierfür eine ausführliche Erklärung im Kapitel 20.

Um nun ein Source-NAT zu realisieren, gibt es beim Befehl `iptables` das Ziel `SNAT`. Hiermit können Sie ein Source-NAT durchführen:

```
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 3.0.0.1
```

Diese NAT-Regel sorgt nun dafür, dass sämtliche Verbindungen auf die Absenderadresse 3.0.0.1 genattet werden. Das bedeutet, dass in allen Paketen die Absenderadresse entsprechend ausgetauscht wird. Die Antwortpakete werden übrigens dann auch automatisch wieder an die Clients passend zurückgeschickt. Das heißt, das NAT wird für die Antwortpakete automatisch rückgängig gemacht. Sie benötigen hier keine zusätzliche Regel!

Sobald Sie Änderungen an einer der Ketten der NAT-Tabelle vornehmen wollen oder diese nur anzeigen wollen, ist es wichtig, dass Sie die NAT-Tabelle spezifisch definieren:

```
iptables -t nat -L   # Zeigt den Inhalt der NAT-Tabelle
iptables -L          # Zeigt nur den Inhalt der Filter-Tabelle (default)
```

Mit der Option `--to-source` können Sie auch einen IP-Adressbereich oder sogar mehrere Adressen durch Wiederholung der Option angeben:

```
--to-source 192.168.0.1-192.168.0.5
--to-source 192.168.0.1 --to-source 192.168.0.3
```

Diese IP-Adressen werden dann immer abwechselnd verwendet.

In vielen Fällen ist das Ziel `SNAT` jedoch nicht einsetzbar. Vielleicht haben Sie zu Hause einen eigenen Internetzugang. Wahrscheinlich handelt es sich hierbei um einen ISDN- oder ADSL-Zugang. Bei den meisten derartigen Zugängen erhalten Sie für die Dauer Ihrer Onlinezeit eine zufällige IP-Adresse zugewiesen, die Sie für diese Zeit nutzen dürfen. Betreiben Sie nun einen Router und dahinter ein Netz mit privaten IP-Adressen, ist der Aufwand groß. Sie müssten immer Ihr Skript ändern und die IP-Adresse, auf die Ihre Pakete genattet werden sollen, an die aktuell zugewiesene Adresse anpassen.

Hierfür wurde ein zusätzliches Ziel geschaffen: `MASQUERADE`. Wenn Sie dieses Ziel anstelle von `SNAT` einsetzen, müssen Sie nicht mehr die IP-Adresse angeben. Iptables wird nun selbst die aktuelle externe IP-Adresse ermitteln und verwenden. Wenn sich die IP-Adresse ändert, so verwendet Iptables automatisch anschließend die richtige IP-Adresse!

Damit wird der Aufbau einer typischen NAT-Regel viel einfacher:

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Diese Regel kennen Sie schon aus Ihrem ersten Skript aus dem letzten Abschnitt.

5.7.2 Destination-NAT

Das Destination-NAT ist seltener anzutreffen, aber mindestens genauso interessant wie das Source-NAT. Während ein Source-NAT heute allgemein üblich und allen Administratoren bekannt ist, sind das Destination-NAT und die damit verbundenen Möglichkeiten häufig unbekannt. Das Destination-NAT wird häufig auch als Port-Forwarding bezeichnet.

Bei einem Destination-NAT wird die Zieladresse eines Pakets modifiziert. Damit können Sie ein Paket, das eigentlich an die Firewall gerichtet war, auf einen anderen Rechner weiterleiten. Abbildung 5.16 verdeutlicht die Möglichkeiten.

So können Sie zum Beispiel sämtliche Anfragen auf dem TCP-Port 80 Ihrer Firewall nach innen auf einen Webserver weiterleiten. Der Client im Internet merkt nicht, dass er in Wirklichkeit nicht mit der Firewall, sondern mit dem privaten Webserver spricht. So können Sie Dienste, die Sie nicht direkt auf der Firewall anbieten wollen, dennoch von außen erreichbar anbieten!

Die Regel für dieses Beispiel sähe folgendermaßen aus:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.0.2
```

Natürlich ist es möglich, einen anderen Port auf einen anderen Rechner weiterzuleiten. Möchten Sie zum Beispiel SMTP-Verbindungen auf Ihren internen E-Mailserver weiterleiten, können Sie die folgende Regel hinzufügen:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 25 -j DNAT --to-destination 192.168.0.3
```

Sie können ein Destination-NAT in der PREROUTING- und in der OUTPUT-Kette durchführen. In der PREROUTING-Kette betrifft das DNAT sämtliche Pakete, die den Rechner von außen erreichen und entweder an ihn lokal gerichtet sind oder

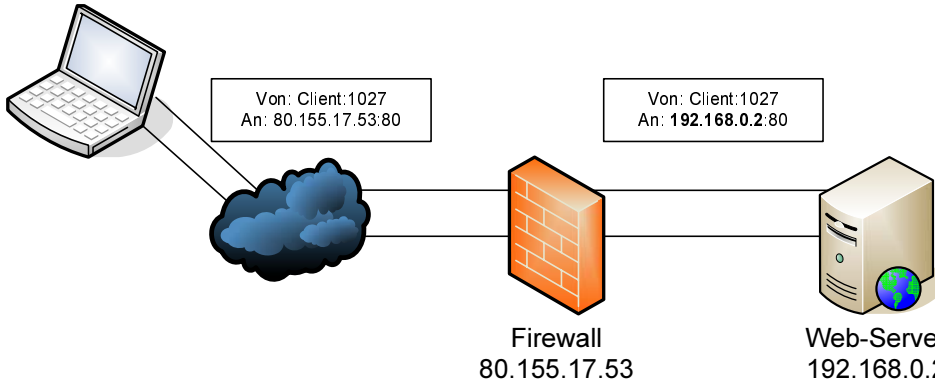


Abbildung 5.16: Bei dem DNAT können Anfragen von außen auf interne Systeme mit privaten Adressen weitergeleitet werden.

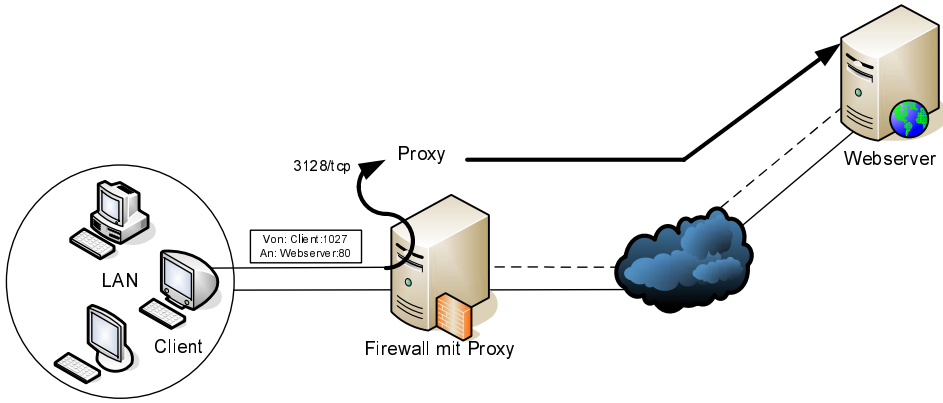


Abbildung 5.17: Das REDIRECT-Ziel leitet die Pakete auf einen anderen lokalen Port um.

weitergeleitet werden müssen. In der OUTPUT-Kette betrifft das DNAT nur die lokal erzeugten Pakete.

Zusätzlich zum Ziel `DNAT` gibt es noch ein weiteres Ziel: `REDIRECT`. Dieses Ziel erlaubt es, Pakete, die normalerweise an ein anderes beliebiges Ziel gerichtet sind, auf einen lokalen Port umzulenken (Abbildung 5.17). Hiermit ist es möglich, einen transparenten Proxy aufzubauen. Mehr Informationen über einen transparenten Proxy erhalten Sie im Abschnitt 20.9.

5.7.3 NAT-Beispiel

Da sehr viele Erstanwender mit der Implementierung ihrer NAT-Regeln auf Probleme stoßen, folgt nun ein kleines Beispiel. Stellen Sie sich vor, Sie hätten eine Internetanbindung mit einer statischen IP-Adresse, die Ihnen von Ihrem Provider fest zugeteilt worden ist. Nun möchten Sie sowohl auf das Internet und dessen Dienste zugreifen können als auch selbst Dienste anbieten. Da Sie aber die Dienste nicht auf der Firewall installieren wollen, haben Sie sich folgendes Setup (Abbildung 5.18) ausgedacht: Ihre Firewall ist mit dem Internet verbunden. Die Dienste installieren Sie auf dedizierten Rechnern in Ihrem internen Netz. In dem DNS für Ihre Domäne tragen Sie für `www.meine-domaene.de` die offizielle IP-Adresse Ihrer Firewall ein. Das Gleiche machen Sie für den Mail-Exchanger (MX)[13] Ihrer Domäne.

Im Folgenden sollen nun die NAT-Regeln definiert werden. Natürlich benötigen Sie zusätzlich auch noch Firewall-Regeln. Obwohl Sie diese nun selbst erzeugen können sollten, werden wir diese auch noch betrachten.

Zunächst soll sichergestellt werden, dass die Clients im internen Netz das Internet erreichen können. Hierzu definieren Sie eine Regel, die sämtliche Pakete nattet:

[13] Der Mail-Exchanger definiert, welcher Rechner für eine Domäne die E-Mails annimmt. Sie können im DNS mehrere Mail-Exchanger (MX) mit unterschiedlicher Priorität zur Lastverteilung und Ausfallsicherheit angeben.

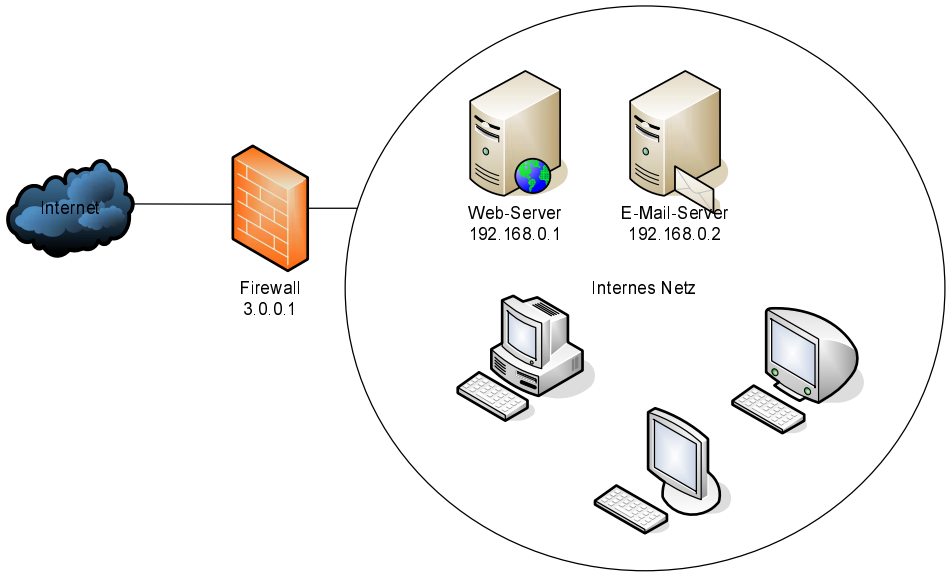


Abbildung 5.18: In dem internen Netz befinden sich ein Webserver und ein E-Mailserver, die aus dem Internet erreicht werden sollen.

```
EXTDEV=eth0
INTDEV=eth1
EXTIP=3.0.0.1

$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -j SNAT --to-source $EXTIP
```

Nun möchten Sie noch erreichen, dass Verbindungen, die von außen Ihre Firewall auf dem TCP-Port 80 und 25 erreichen, an Ihren Webserver bzw. Ihren E-Mail-Server weitergeleitet werden.

```
WEBSERVER=192.168.0.1
EMAILSERVER=192.168.0.2

$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tcp --dport 80 -j DNAT↵
  --to-destination $WEBSERVER
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tcp --dport 25 -j DNAT↵
  --to-destination $EMAILSERVER
```

Diese Regeln reichen für das NAT bereits vollkommen aus. Nun benötigen Sie noch einige Firewall-Regeln, die zunächst die Verbindungen von innen nach außen für Ihre Clients beim Zugriff auf das Internet zulassen:

```
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Zusätzlich benötigen Sie noch Regeln, die die Web- und die E-Mail-Verbindungen nach innen auf Ihren Web- und Ihren E-Mail-Server erlauben:

```
$IPTABLES -A FORWARD -i $EXTDEV -o $INTDEV -p tcp --dport 80 -d $WEBSERVER -m state ↵
  --state NEW -j ACCEPT
$IPTABLES -A FORWARD -i $EXTDEV -o $INTDEV -p tcp --dport 25 -d $EMAILSERVER -m state ↵
  --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Die erste Regel erlaubt neue Pakete (`-m state --state NEW`) von außen (`-i $EXTDEV`) nach innen (`-o $INTDEV`), wenn sie an den Webserver (`-d $WEBSERVER`) auf dem TCP-Port 80 gerichtet sind (`-p tcp --dport 80`). Die zweite Regel wiederholt dies für den E-Mailserver. Die dritte Regel erlaubt sämtliche weiteren Pakete dieser Verbindungen. Diese dritte Regel hatten wir aber bereits weiter oben definiert. Daher brauchen wir diese hier nicht erneut anzugeben!

Ein komplettes Skript würde also folgendermaßen aussehen:

```
#!/bin/sh
#
# Autor  : Ralf Spenneberg
# Version: 0.1
# Datum  : 17. Dez 2004
#
# Dieses Skript lädt die Regeln für die Firewall.
# Außerdem erlaubt es den Zugriff von außen auf einen internen Web-
# und E-Mail-Server

INTDEV="eth1"
# Achtung: Bei Einsatz von User-Mode-Linux lautet diese Variable
# INTDEV="tap0"

EXTDEV="eth0"

EXTIP=3.0.0.1
WEBSERVER=192.168.0.1
EMAILSERVER=192.168.0.2


# Definiere einige Befehle
ECHO="/bin/echo"
SYSCTL="/bin/sysctl"
IPTABLES="/sbin/iptables"

# Leere die Ketten
$IPTABLES -F
```

```
# Die NAT-Tabelle muss extra geleert werden
$IPTABLES -t nat -F


# Verwerfe erstmal alles
$IPTABLES -P INPUT  DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP

# Akzeptiere Verbindungsaufbauten von innen
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -m state --state NEW -j ACCEPT

# Akzeptiere alle Pakete, die Teil einer aufgebauten Verbindung sind
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# Akzeptiere Verbindungen für den Web- und E-Mail-Server
$IPTABLES -A FORWARD -i $EXTDEV -o $INTDEV -p tcp --dport 80 -d $WEBSERVER -m state ↵
  --state NEW -j ACCEPT
$IPTABLES -A FORWARD -i $EXTDEV -o $INTDEV -p tcp --dport 25 -d $EMAILSERVER -m state ↵
  --state NEW -j ACCEPT

# Setze NAT-Regeln

# Natte den Zugriff nach außen
$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -j SNAT --to-source $EXTIP

# Wenn Sie die IP-Adressen nicht kennen, können Sie auch diese Zeile
# nutzen:
# $IPTABLES -t nat -A POSTROUTING -o $EXTDEV -j MASQUERADE

# Natte den Zugriff von außen auf den Web- und E-Mail-Server
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tcp --dport 80 -j DNAT ↵
  --to-destination $WEBSERVER
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tcp --dport 25 -j DNAT ↵
  --to-destination $EMAILSERVER


# Aktiviere das Forwarding
$ECHO "1" > /proc/sys/net/ipv4/ip_forward

# Alternativ:
# $SYSCTL -w net.ipv4.ip_forward=1
```

5.8 Die Mangle-Tabelle

Die Mangle-Tabelle führt ein Schattendasein bei Iptables. Sie bietet nicht besonders viele Funktionen. Dabei verfügt sie über die meisten Ketten: INPUT, OUTPUT, FORWARD, PREROUTING und POSTROUTING (Abbildung 5.19)[14]. In der Mangle-Tabelle können Sie Pakete modifizieren. Leider bietet Iptables nur einige wenige Möglichkeiten für diese Modifikationen.

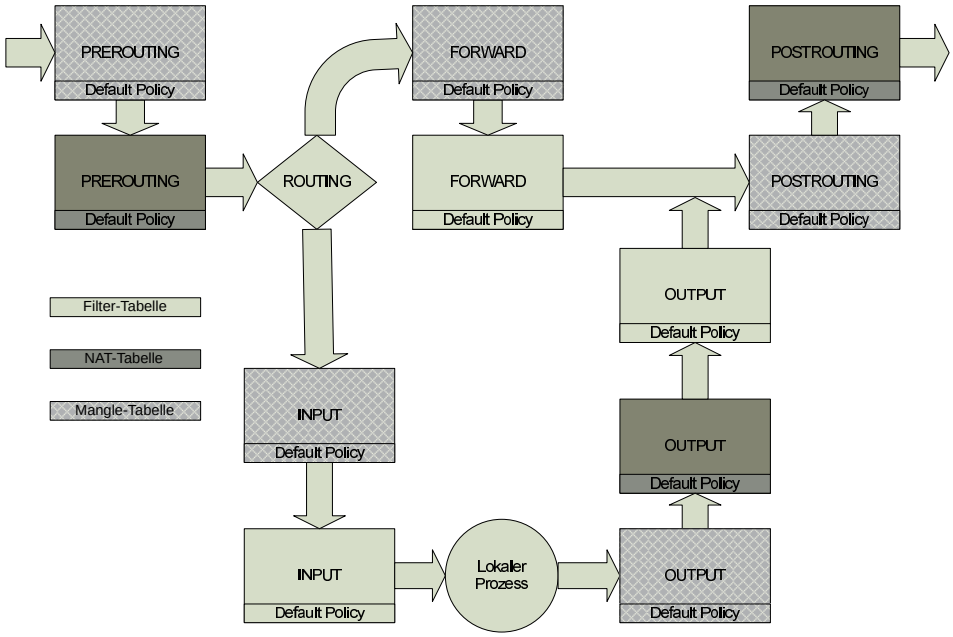


Abbildung 5.19: In der Mangle-Tabelle können Sie ein Paket modifizieren.

Bevor wir uns über die verschiedenen Möglichkeiten einen Überblick verschaffen, betrachten Sie bitte die Abbildung 5.19. Ihnen sollte auffallen, dass jedes Paket zuerst die entsprechende Mangle-Kette durchläuft, bevor die NAT- und Filter-Ketten durchlaufen werden. Dadurch können Sie in der Mangle-Tabelle ein Paket modifizieren und diese Modifikation in einer der Filter-Ketten zum Beispiel prüfen.

Welche Möglichkeiten gibt es nun in der Mangle-Tabelle? Die meisten Distributionen bieten folgende Ziele für die Mangle-Tabelle an:

- `DSCP`: Dieses Ziel erlaubt es, die Diffserv-Codepoints (DSCP) in dem TOS-Feld des IP-Pakets zu ändern. Diffserv-Codepoints werden für die Realisierung von Quality-of-Service verwendet. Weitere Informationen finden Sie im Abschnitt 21.2.3.

[14] Wenn Sie noch einen alten Kernel < 2.4.18 einsetzen sollten, verfügt Ihr Kernel in der Mangle-Tabelle nur über eine PREROUTING- und eine OUTPUT-Kette.

- ECN: Hiermit können Sie die ECN-Bits aus dem TCP-Header entfernen. ECN ist eine Art Stauvermeidung für das Internet. Leider nutzen nur sehr wenige Betriebssysteme bisher diese Funktion, und viele Firewalls verwerfen derartig markierte Pakete. Weitere Informationen finden Sie im Abschnitt 21.2.3.
- MARK: Hiermit können Sie Pakete mit einer Zahl markieren. Diese Markierung verändert das Paket nicht, sondern klebt wie ein Aufkleber an dem Paket, so lange, wie es sich auf der Firewall befindet. Sobald das Paket die Firewall verlässt, wird die Markierung entfernt. Diese Funktion kann zum Beispiel für die Filterung von IPsec-VPN-Verkehr genutzt werden (siehe Kapitel 33). Weitere Informationen über dieses Ziel finden Sie in Abschnitt 21.2.7.
- ROUTE: Dieses Ziel kann die Routenentscheidung des Kernels überschreiben. Damit können Sie ein Paket über eine andere Route senden und sogar eine Kopie eines Pakets erzeugen, die an ein anderes Ziel geroutet wird. Weitere Informationen über dieses Ziel finden Sie im Abschnitt 21.2.8.
- TOS: Dieses Ziel kann das Type-of-Service-Feld im IP-Header setzen. Weitere Informationen über dieses Ziel finden Sie im Abschnitt 21.2.9.
- TTL: Hiermit können Sie den TTL-Wert eines Pakets verändern. So können Sie den TTL-Wert sowohl herauf- als auch herabsetzen. Es existieren kaum sinnvolle Anwendungen hierfür. Weitere Informationen finden Sie im Abschnitt 21.2.10.
- CLASSIFY: Der Linux-Kernel erlaubt die Klassifizierung von Paketen in unterschiedliche Quality-of-Service-Klassen. Dieses Ziel erlaubt die Einsortierung der Pakete mit Firewall-Regeln. Weitere Informationen finden Sie im Abschnitt 21.2.1.

Ob Ihr Kernel alle diese Ziele unterstützt, können Sie leicht selbst herausbekommen. Schauen Sie einfach in das Verzeichnis */lib/modules/<Kernel-Version>/kernel/net/ipv4/netfilter*. Befindet sich dort die Datei *ipt_TTL.ko*, so unterstützt der Kernel das Ziel. Achten Sie auf die Groß- und Kleinschreibung.

Eine weitere Erklärung der Ziele und Ihrer Möglichkeiten mit Beispielregeln finden Sie in Kapitel 21.

5.9 Die Raw-Tabelle

Die Raw-Tabelle besitzt zwei Ketten: PREROUTING und OUTPUT. Sie steht auf alten Kerneln nicht zur Verfügung. Jedes Paket durchläuft diese Ketten als Erstes. Wenn das Paket von außen kommt, durchläuft es die Raw-PREROUTING-Kette. Wenn das Paket lokal erzeugt wurde, durchläuft es die Raw-OUTPUT-Kette (siehe Abbildung 5.20). Da zu diesem Zeitpunkt ip_conntrack noch nicht die Pakete analysiert hat[15], können Sie hier mit dem Ziel NOTRACK Pakete von der Überwachung ausschließen. Das bedeutet dann aber auch gleichzeitig, dass diese Pakete nicht mehr genattet werden können.

[15] Das passiert in der NAT-Tabelle.

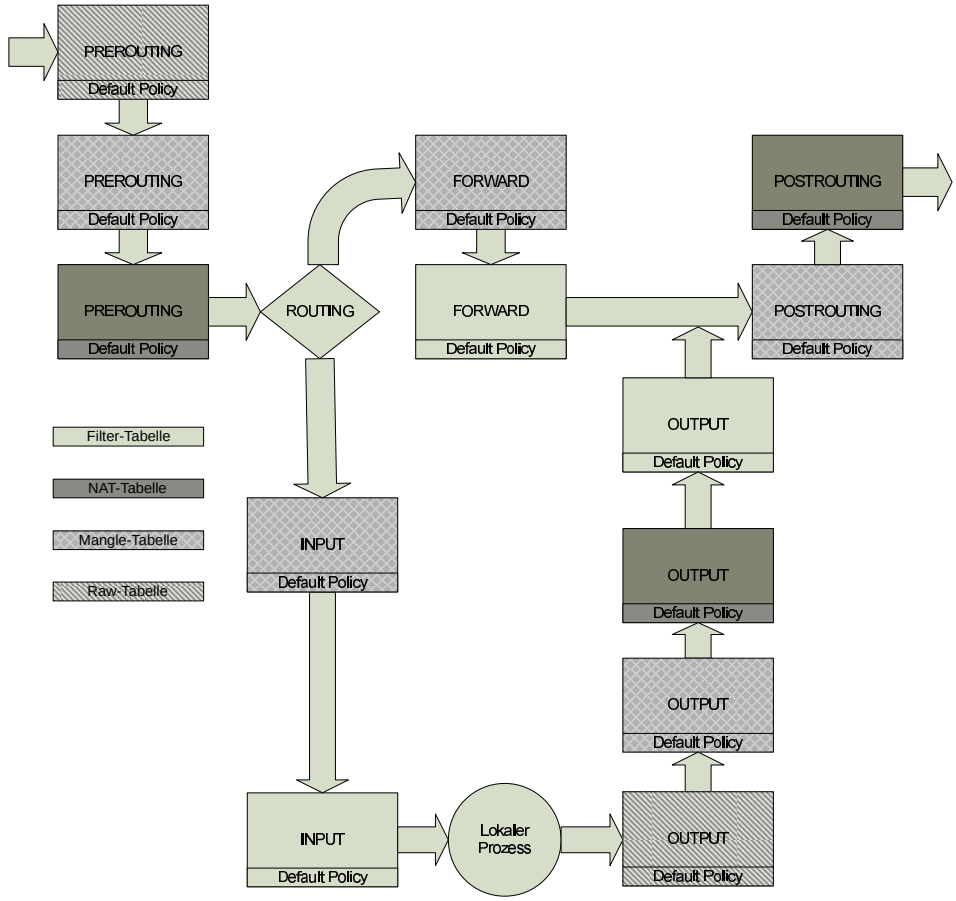


Abbildung 5.20: Die Raw-Tabelle wird vor jeder anderen Tabelle durchlaufen. Sie steht nicht auf allen Kerneln zur Verfügung.

Als zweites Ziel dieser Tabelle existiert TRACE. Dieses Ziel erlaubt es, bestimmte Pakete bei ihrem Durchlauf durch Ihr Regelwerk zu verfolgen. Ein Paket, das mit dem TRACE-Ziel markiert wurde, wird anschließend von jeder Regel, die auf das Paket zutrifft, protokolliert:

```
TRACE: tablename/chainname/rulenum packet
```

Weitere Informationen über die Raw-Tabelle finden Sie im Kapitel 22.

5.10 Einstellungen des Kernels

Zusätzlich zu den Firewall-Regeln gibt es auch noch eine ganze Reihe von Kerneleinstellungen, die eine zusätzliche Sicherheit für Ihr System schaffen können. Hierbei handelt es sich um Einstellungen, die Sie in dem Verzeichnis */proc/sys/net/ipv4*

verändern können, wodurch Sie so zur Laufzeit das Verhalten des Kernels modifizieren.

Eine erste Einstellung haben Sie bereits kennen gelernt: `ip_forward`. Hiermit können Sie entscheiden, ob Ihr System Pakete zwischen den Netzwerkkarten weiterleiten soll oder nicht. Ist der Wert in dieser Datei eine 0, so werden die Pakete nicht weitergeleitet. Ist der Wert 1, so findet eine Weiterleitung statt.

Sie haben bereits zwei Varianten kennen gelernt, wie Sie diesen Wert einstellen können:

1. `echo 1 > /proc/sys/net/ipv4/ip_forward`
2. `sysctl -w net.ipv4.ip_forward=1`

Wenn Sie bereits die erste Syntax kennen, können Sie sehr leicht die Syntax des `sysctl`-Kommandos ableiten. Entfernen Sie einfach den Pfad `/proc/sys/`, und ersetzen Sie anschließend alle Schrägstriche durch einen Punkt[16]. Mit dieser Syntax können Sie die zu setzenden Variablen auch in der Datei `/etc/sysctl.conf` eintragen. Diese Datei steht auf fast allen aktuellen Distributionen zur Verfügung und wird üblicherweise nach dem Booten und nach jedem Neustart des Netzwerks gelesen.

Weitere wichtige Kernelparameter sind:

- `ip_echo_ignore_broadcasts`: Klassischerweise reagiert jeder Unix/Linux-Rechner auf einen Broadcast-Ping. Hierbei handelt es sich um eine Ping-Anfrage, die an die Broadcast-Adresse eines Netzes gesendet wurde (z.B. mit `ping -b 192.168.0.255`). Dies kann jedoch für eine Denial-of-Service-Attacke genutzt werden. Der Angreifer braucht nur ein Ping-Paket mit gefälschter Absenderadresse loszuschicken, und sämtliche Unix/Linux-Systeme in dem Zielnetz antworten. So kommt es zu einer Vervielfältigung des Pakets, die zum DoS auf die Netzwerkleitung führen kann. Dieser Angriff ist als SMURF-Angriff bekannt. Die Netze, die eine Vervielfältigung erlauben, sind so genannte Amplifier-(Verstärker-)Netze. Eine Übersicht über derartige Netze gibt die Smurf-Amplifier-Registry (*http://www.powertech.no/smurf/*). Damit die Gefahr durch eine fehlerhafte Konfiguration des Netzes gar nicht erst entsteht, wird allgemein empfohlen, diese Funktion des Linux-Systems abzuschalten:

  ```
  sysctl -w net.ipv4.ip_echo_ignore_broadcasts=1
  ```

  Viele Distributionen haben diese Einstellung bereits zum Default gemacht.

- `ip_default_ttl`: Mit diesem Wert können Sie den TTL-Wert einstellen, den sämtliche Pakete erhalten sollen, die von Ihrem Rechner erzeugt werden. Typisch für Linux ist 64. Andere Betriebssysteme verwenden andere (z.B. 255) Werte. Daher kann eine grobe Erkennung des Betriebssystems über diesen Wert erfolgen. Eine Änderung ist nicht sinnvoll.

[16] Der letzte Schritt ist nicht zwingend erforderlich. Es funktioniert auch:

```
sysctl -w net/ipv4/ip_forward=1
```

- `tcp_ecn`. Hiermit stellen Sie ein, ob Sie die Explicit Congestion Notification (ECN)[17] wünschen. Dabei handelt es sich um eine neue Methode, mit der zwei kommunizierende Systeme im Internet eine "Verstopfung" frühzeitig erkennen können und durch präventive Verlangsamung der Pakete diese zu umgehen versuchen. Leider gibt es viele Firewalls, die Pakete verwerfen, die die ECN-Bits tragen. Daher ist es im Moment nicht sinnvoll, dies grundsätzlich einzuschalten. Wenn Sie ECN einschalten, können Sie es mit Hilfe von Firewall-Regeln in der Mangle-Tabelle für bestimmte Ziele auch wieder abschalten (siehe Abschnitt 21.2.4).

- `tcp_syncookies`: Der TCP/IP-Stack der meisten Betriebssysteme (auch Linux) ist durch einen SYN-Flood-DoS verwundbar. Hierbei handelt es sich um sehr viele TCP-SYN-Pakete, die der Angreifer mit gefälschter Adresse an den Rechner schickt. Der angegriffene Rechner kann zwischen den gefälschten TCP-SYN-Paketen und regulären Paketen nicht unterscheiden und muss auf alle diese Pakete reagieren und sich die Informationen des Verbindungsaufbaus merken. Dies kann bei genügend gefälschten Paketen zu einem Überlauf der hierfür verwendeten Tabelle führen. Die TCP-Syncookies schaffen diese Tabelle ab und speichern die notwendigen Daten in der Verbindung selbst[18]. Ein Einschalten dieser Funktion hilft natürlich nur auf dem angegriffenen Server selbst. Auf einem Paketfilter hat das keine Auswirkungen auf die durchgeleiteten Verbindungen[19].

- `conf/<interface>/accept_source_route`: Diese Funktion sollte auf jedem System abgeschaltet sein. Bei eingeschaltetem Zustand besteht die Gefahr, dass ein Angreifer Pakete nach seinem Willen routen kann. Als Source-Routing bezeichnet man nämlich die Funktion, dass der Absender den Weg des Pakets über IP-Optionen beeinflussen kann.

- `conf/<interface>/rp_filter`: Dies ist ein in dem Kernel eingebauter Anti-Spoofing-Schutz. Sie können diesen Schutz anschalten (1) und abschalten (0). Der Linux-Kernel betrachtet bei eingeschaltetem Anti-Spoofing-Schutz jedes Paket und prüft, ob ein potenzielles Antwortpaket den umgekehrten Weg nehmen würde. Diese Reverse-Path-Filterung ist in dem RFC 1812 beschrieben.

- `conf/<interface>/log_martians`: Diese Protokollfunktion protokolliert alle unmöglichen Pakete über den zentralen Syslog-Daemon. Dazu gehören zum Beispiel die Pakete, die von `rp_filter` und `accept_source_route` verworfen wurden.

- `conf/<interface>/forwarding`: Hiermit können Sie für jedes Interface einzeln die Forwarding-Funktion konfigurieren. Wenn Sie das Forwarding für den gesamten Rechner einschalten (`ip_forward`), wird dieser Parameter bei jeder Netzwerk-

[17] Weitere Informationen erhalten Sie hier: *http://www.icir.org/floyd/ecn.html*

[18] Für die Interessierten: Die Daten werden in der Sequenznummer verschlüsselt hinterlegt. Weitere Informationen über Syn-Cookies finden Sie unter: *http://www.heise.de/security/artikel/43066/2* und *http://cr.yp.to/syncookies.html*.

[19] OpenBSD kann als SYN-Proxy sogar als Paketfilter vor einem SYN-Flood schützen. Allerdings werden hier keine SYN-Cookies verwendet. OpenBSD verwirft zufällig Verbindungen, sobald die Tabelle sich füllt.

karte ebenfalls eingeschaltet. Schalten Sie ihn für eine bestimmte Netzwerkkarte wieder ab, so leitet die entsprechende Netzwerkkarte Pakete nicht mehr weiter.

Alle Parameter hier aufzuzählen, würde den Rahmen an dieser Stelle sprengen. Sie finden weitere wichtige Parameter und ihre Erläuterung im Kapitel 23.

Für Sie zunächst sinnvolle zusätzliche Parameter sind:

```
sysctl -w net.ipv4.conf.all.rp_filter=1
sysctl -w net.ipv4.conf.all.accept_source_route=0
```

5.11 Protokollierung

Die Protokollierung ist ein sehr wichtiger Vorgang bei einer Firewall. Jeder Firewall-Administrator sollte wissen, was auf seiner Firewall vorgeht. Dafür ist eine Protokollierung der abgelehnten Verbindungen zwingend erforderlich. Vielleicht ist auch eine Protokollierung der erlaubten Verbindungen in bestimmten Umgebungen wünschenswert.

In diesem Abschnitt werden wir die einfache Protokollierung mit Iptables kennen lernen. Werkzeuge zur Auswertung werden in einem späteren Kapitel (siehe Kapitel 12) vorgestellt. Auch eine weitere fortgeschrittene Protokollalternative (ULOG) wird in einem späteren Abschnitt besprochen (siehe Abschnitt 24.1).

Für die Protokollierung mit Iptables gibt es ein einfaches Ziel, das in der Firewall-Regel angegeben wird: `LOG`. Eine Protokollregel sieht dann zum Beispiel so aus:

```
# Die nächste Regel protokolliert alle Verbindungsaufnahmen von außen
iptables -A FORWARD -i $EXTDEV -m state --state NEW -j LOG
```

Während alle anderen Ziele, die Sie bisher kennen gelernt haben (DROP, REJECT, ACCEPT), direkt über das Schicksal des Pakets entschieden und eine weitere Abarbeitung der Regeln in der Kette nicht erfolgte, ist das bei LOG nicht so. Wenn ein Paket protokolliert wurde, wird die weitere Abarbeitung der Regeln in der Kette nicht abgebrochen, da über sein Schicksal noch nicht entschieden worden ist.

Möchten Sie also ein Telnet-Paket protokollieren und anschließend verwerfen, so benötigen Sie zwei Regeln:

```
$IPTABLES -A FORWARD -p tcp --dport 23 -j LOG
$IPTABLES -A FORWARD -p tcp --dport 23 -j DROP
```

Achtung

Achten Sie darauf, dass Sie nicht die Reihenfolge durcheinander bringen. Dann würde nämlich das Paket zuerst verworfen werden, die Abarbeitung der weiteren Regeln würde nicht erfolgen, und die LOG-Regel würde nie ausgeführt werden!

Genauso können Sie ein Paket protokollieren und akzeptieren. Möchten Sie alle neuen Telnet-Verbindungen erlauben, aber auch protokollieren, können Sie die folgenden Regeln verwenden:

```
$IPTABLES -A FORWARD -p tcp --dport 23 -m state --state NEW -j LOG
$IPTABLES -A FORWARD -p tcp --dport 23 -m state --state NEW -j ACCEPT
```

Wie sehen nun die protokollierten Pakete aus? Das Protokollformat ist zunächst ein wenig gewöhnungsbedürftig, enthält aber alle wichtigen Informationen:

```
Jul 14 18:41:45 bibo kernel: IN= OUT=eth0 SRC=192.168.255.100 DST=209.132.177.100 LEN=453
  TOS=0x00 PREC=0x00 TTL=64 ID=33418 DF PROTO=TCP SPT=35379 DPT=443 WINDOW=2068 RES=0x00
  ACK PSH URGP=0
```

Dies ist ein typisches TCP-Paket, das so vom Syslog-Daemon protokolliert wurde. In welcher Datei die Protokollmeldungen auftauchen, hängt von Ihrer Syslog-Konfiguration ab.

Exkurs: Syslog-Daemon-Konfiguration

Bei der Konfiguration des Syslog-Daemons sollten Sie zunächst prüfen, welche Variante Ihr aktuelles Linux-System nutzt. Allgemein werden im Moment vor allem zwei alternative Syslog-Daemons eingesetzt:

- Der von dem BSD-Syslogd abgeleitete Syslog-Daemon wird in der Datei `/etc/syslog.conf` konfiguriert, und der laufende Prozess heißt `syslogd`.
- Der Syslog-ng ist ein moderner Syslog-Daemon, der viele Erweiterungen gegenüber dem BSD-Syslog erfahren hat. Seine Konfigurationsdatei ist die `/etc/syslog-ng.conf`, und der Prozess heißt auch entsprechend. Während im Folgenden kurz der BSD-Syslogd angesprochen wird, wird dieser Daemon in einem eigenen späteren Abschnitt besprochen (Abschnitt 10.3).

Hier wollen wir uns kurz auf den BSD-Syslog beschränken. Schauen Sie in die Datei `/etc/syslog.conf`, und suchen Sie nach einem nicht auskommentierten Eintrag `kernel.<irgendwas>` oder `*.<irgendwas>`. In der rechten Spalte finden Sie dann den Namen der Datei, in der alle Meldungen des Kernels bzw. aller Protokollquellen mit mindestens der Priorität <irgendwas> protokolliert werden. In dieser Datei finden Sie dann auch die Firewall-Protokolle.

Betrachten wir den Protokolleintrag der Reihe nach. Zunächst schreibt der Protokolldienst das aktuelle Datum und die Uhrzeit: `Jul 14 18:41:45`.

Achtung

Der Unix-Protokolldienst schreibt keine Jahreszahlen! Wenn Sie die Protokolle länger aufbewahren wollen, müssen Sie selbst sich das Jahr merken (z.B. in dem Namen der Protokolldatei).

Anschließend schreibt der Protokolldienst den Namen des Rechners, der den Eintrag erzeugt hat: `bibo`. Dies ist wichtig, da der Protokolldienst grundsätzlich netzwerkfähig ist und Sie die Protokolle auf einem Protokollserver zusammenfassen können. Damit Sie später wissen, welche Einträge von welchem Server kommen, wird auch der Name protokolliert.

Es folgt die Quelle der Meldung: `kernel:`. An dieser Stelle finden Sie auch mail, cron, news etc.

Nun folgt die eigentliche Meldung. Sie beginnt mit der Information, über welche Netzwerkkarte das protokollierte Paket den Rechner erreicht hat und verlassen wird: `IN= OUT=eth0`. Hier handelt es sich um ein lokal erzeugtes Paket, das den Rechner über eth0 verlässt.

Anschließend werden die Absender und Ziel-IP-Adresse protokolliert: `SRC=192.168.255.100 DST=209.132.177.100`. Handelt es sich um ein ankommendes Paket, sehen Sie zuvor auch noch den Ethernet-Header des Pakets: `MAC=00:0f:1f:1c:bd:15:00:12:17:dd:dd:07:08:00`. Dieser Ethernet-Header enthält in den ersten sechs Bytes die Quell-MAC-Adresse (00:0f:1f:1c:bd:15), dann die Ziel-MAC-Adresse (00:12:17:dd:dd:07) und schließlich noch die Information, dass sich in dem Ethernet-Paket ein IP-Paket befindet (08:00).

Auf die Adressen folgen die weiteren Informationen aus dem IP-Header des Pakets: die Länge in Bytes (`LEN=40`), der Inhalt des TOS- und PREC-Feldes (`TOS=0x00 PREC=0x00`, siehe Abschnitt 21.2.9), der TTL-Wert (`TTL=64`) und die Fragmentierungsidentifikationsnummer (`ID=33418`). Wenn das DF-Bit gesetzt ist, erscheint im Protokoll ein `DF`. Als Letztes folgt das Transportprotokoll (`PROTO=TCP`).

Bei einem TCP-Paket folgen nun der Quell- und Zielport (`SPT=35379 DPT=443`), die Größe des TCP-Windows (`WINDOW=2068`), der Zustand der reservierten Bits im TCP-Header (`RES=0x00`) und die weiteren Flags des TCP-Headers (`ACK PSH`). Falls ein URG-Flag gesetzt ist, muss auch der Urgent-Pointer gesetzt sein: `URGP=0`.

Anhand des Quell- und Zielports können Sie ableiten, um welche Art von Verbindung es sich wahrscheinlich handelt. Hier finden Sie einen Zielport 443. Es wird sich daher um eine HTTPS-Verbindung (SSL-verschlüsselte HTTP-Verbindung) handeln.

Das LOG-Ziel verfügt über einige Optionen, die sein Verhalten noch verändern können.

- `--log-level <level>`: Hiermit können Sie die Priorität der Meldungen anpassen und damit diese Meldungen durch eine Anpassung der `/etc/syslog.conf` in unterschiedlichen Dateien protokollieren.
- `--log-prefix <prefix>`: Sie können eine Zeichenkette von bis zu 29 Buchstaben angeben, die jeder Protokollmeldung vorangestellt wird. Damit können Sie anschließend sehr leicht (zum Beispiel mit `grep`) in Ihren Protokollen nach bestimmten Meldungen suchen.

```
$IPTABLES -A FORWARD -p tcp --dport 23 -m state --state NEW -j LOG↵
  --log-prefix "Neue-Telnet-Verbindung"
```

- `--log-tcp-sequence`: Dies protokolliert bei jedem Paket auch die verwendeten Sequenznummern. Sind die Sequenznummern und der Mechanismus ihrer Erzeugung bekannt, ist es möglich, einen Man-in-the-Middle-Angriff auf die Verbindung durchzuführen. Bei einer Protokollierung sollten Sie daher sicherstellen, dass zumindest keine normalen Benutzer die Protokolle lesen dürfen.
- `--log-tcp-options`, `--log-ip-options`: Hiermit werden mögliche zusätzliche Optionen des TCP-Headers (z.B. MSS) und des IP-Headers (z.B. Source-Routing) protokolliert.
- `--log-uid`: Diese Option ist nur in der OUTPUT-Kette sinnvoll. Sie protokolliert bei lokal erzeugten Paketen zusätzlich die UID des Users, dessen Prozess das Paket erzeugt hat.

Achtung

Achten Sie darauf, dass Sie vorsichtig mit der Protokollierung umgehen. Eine unachtsam gesetzte Protokollregel kann schnell mehrere 100 MByte an Protokollen pro Tag erzeugen! Der Analyse der Protokolle ist ein eigenes Kapitel (Kapitel 12) gewidmet.

5.12 Test der Firewall

Dies ist häufig eines der schwierigsten Kapitel für den Einsteiger. Wie testet man eine Firewall? Wie testet man, ob die Firewall sicher ist, aber dennoch die notwendigen Zugriffe erlaubt?

Zunächst sollten Sie prüfen, ob das von Ihnen geschriebene Skript syntaktisch korrekt ist. Wenn beim Aufruf Ihres Skripts bereits Fehlermeldungen erscheinen, sollten Sie diese Fehler suchen und entfernen. Anschließend können Sie die Funktion testen.

Besonders schön ist es natürlich, wenn Sie eine möglichst reale Testumgebung für Ihre Versuche haben. Das kann auch eine virtuelle Testumgebung mit User-Mode-Linux sein.

Dann sollten Sie zunächst prüfen, ob alle Dienste so funktionieren, wie Sie es wünschen. Dies können Sie relativ einfach und effektiv mit den realen Programmen durchführen. Wenn diese Ihnen nicht zur Verfügung stehen, können Sie mit dem Werkzeug `nmap` zumindestens prüfen, ob die benötigten Verbindungen aufgebaut werden können. Hierzu starten Sie Nmap mit der Option `-sT`. Dies führt einen TCP-Connect-Scan durch. Das bedeutet, Nmap baut tatsächlich die TCP-Verbindung so auf, wie es der Client auch machen würde.

```
# nmap -sT <ziel>
```

Funktionieren alle Dienste entsprechend Ihren Wünschen, können Sie nun prüfen, ob alle unerwünschten Zugriffe korrekt abgelehnt und bei entsprechender Konfiguration auch protokolliert werden.

Hierzu müssen Sie vor allem von außen auch den Zugriff testen. Falls Sie keine Testumgebung zur Verfügung haben und einen Test auf dem System in seiner Live-Umgebung durchführen müssen, müssen Sie den Scan aus dem Internet durchführen. Hierzu können Sie zum Beispiel einen zweiten Rechner nutzen, der sich über ISDN oder Modem eingewählt hat. Vielleicht verfügen Sie auch über einen Bekannten, der einen Internetzugang besitzt und den Scan durchführen kann. Trifft das alles nicht zu, so gibt es im Internet Dienstleister, die Ihnen anbieten, Sie zu scannen. Ein kostenloser Anbieter eines derartigen Dienstes ist der Heise Verlag. Unter *http://www.heise.de/security/dienste/itssecure/* bietet der Verlag einen einfachen Portscan an. In einer weiteren Stufe wird ein kostenpflichtiger (aktuell EUR 89,00) Intensivcheck angeboten.

Beachten Sie bitte, dass ein Scan wesentlich länger dauert, wenn Ihre Firewall die unerwünschten Pakete verwirft (DROP) und nicht ablehnt (REJECT). Am Ende eines Scans erhalten Sie von Nmap eine Ausgabe, die der folgenden ähnelt:

```
[root@bibo ~]# nmap -sT www.nohup.info

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-07-14 20:06 CEST
Interesting ports on mail.spenneberg.net (217.160.128.61):
(The 1618 ports scanned but not shown below are in state: closed)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    open     smtp
53/tcp    open     domain
80/tcp    open     http
140/tcp   filtered emfis-data
161/tcp   filtered snmp
168/tcp   filtered rsvd
225/tcp   filtered unknown
237/tcp   filtered unknown
258/tcp   filtered Fw1-mc-gui
271/tcp   filtered unknown
310/tcp   filtered bhmds
```

```
331/tcp   filtered unknown
366/tcp   filtered odmr
379/tcp   filtered is99c
423/tcp   filtered opc-job-start
443/tcp   open     https
536/tcp   filtered opalis-rdv
567/tcp   filtered banyan-rpc
641/tcp   filtered unknown
722/tcp   filtered unknown
734/tcp   filtered unknown
743/tcp   filtered unknown
814/tcp   filtered unknown
819/tcp   filtered unknown
843/tcp   filtered unknown
852/tcp   filtered unknown
877/tcp   filtered unknown
891/tcp   filtered unknown
950/tcp   filtered oftep-rpc
993/tcp   open     imaps
1367/tcp  filtered dcs
1449/tcp  filtered peport
1482/tcp  filtered miteksys-lm
1720/tcp  filtered H.323/Q.931
2003/tcp  filtered cfingerd
2004/tcp  filtered mailbox
2201/tcp  filtered ats
2604/tcp  filtered ospfd
5490/tcp  filtered connect-proxy
5555/tcp  filtered freeciv
6007/tcp  filtered X11:7
8888/tcp  filtered sun-answerbook
9152/tcp  filtered ms-sql2000
18185/tcp filtered opsec_omi

Nmap finished: 1 IP address (1 host up) scanned in 24.558 seconds
```

Hier können Sie erkennen, dass sehr viele Ports von einer Firewall gefiltert werden, aber doch einige wenige Ports offen sind: 22, 25, 53, 80, 443 und 993. Auf dem System laufen anscheined ein SSH-Daemon (22) und ein DNS-Server (53). Außerdem findet sich ein Webserver, der sowohl HTTP (80) als auch HTTPS-Verbindungen (443) entgegennimmt, und ein E-Mail-Server, der SMTP- (25) und SSL-verschlüsselte IMAP-Verbindungen (993) entgegennimmt. Alle hier nicht aufgeführten Ports werden nicht gefiltert, sind aber dennoch geschlossen, da auf dem Zielsystem kein Dienst installiert wurde.

Weitere Hinweise zur Anwendung von Nmap und weitere Werkzeuge zum Test Ihrer Firewall werden im Kapitel 15 beschrieben.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

6 Härtung eines Linux-Systems

Wenn Sie eine Linux-Distribution als Firewall-System nutzen wollen, sollte diese gehärtet sein. Die üblichen Distributionen (SUSE Linux, SUSE Linux OSS, Fedora Core und Debian) sind noch nicht an die besonderen Anforderungen einer Firewall angepasst. Wenn Sie eine für diesen speziellen Zweck vorbereitete Distribution nutzen, haben die Hersteller meist bereits eine gute Vorarbeit geleistet. Dennoch kann es nicht schaden, wenn Sie trotzdem noch einmal einen Blick auf die Härtung werfen.

Was ist Härtung? Eine gute Frage. Es gibt keine allgemeine Antwort. Kein RFC oder Standard definiert die Härtung eines Betriebssystems. Im Folgenden gebe ich Ihnen meine Vorstellung von der Härtung eines Betriebssystems wieder.

Da die Härtung eines Betriebssystems keine einfache Aufgabe ist, schnell wichtige Punkte vergessen werden und häufig ähnliche Systeme anschließend unterschiedlich konfiguriert wurden, stelle ich Ihnen anschließend im Kapitel Bastille-Linux vor. Bastille-Linux ist ein Werkzeug für die wichtigsten Linux-Distributionen (und auch Mac OS X und HP-UX), das Sie bei dieser Arbeit menügeführt unterstützt. Selbst wenn Sie es nicht für diesen Zweck einsetzen möchten, können Sie es sehr gut als Assessment-Werkzeug verwenden, um Ihre manuelle Konfiguration zu prüfen.

6.1 Warum sollte eine Firewall gehärtet werden?

Um zu klären, warum eine Firewall gehärtet werden sollte, sollten wir uns zunächst ansehen, was Härtung bedeutet. Wenn Sie eine aktuelle Linux-Distribution durch bloßes Anwählen der Default-Einstellungen installieren, so installieren Sie zahllose, für eine Firewall überflüssige Softwarepakete. Diese Softwarepakete sind häufig nicht nur überflüssig, sondern können auch Sicherheitslücken enthalten. Wenn die Distribution nach einem Neustart auch einige dieser überflüssigen Netzwerkdienste aktiviert, so dass sie von außen erreichbar sind, könnten diese Dienste auch über das Netz angreifbar sein.

Natürlich installieren Sie Ihre Firewall-Regeln so, dass ein Zugriff auf die Dienste gar nicht erst möglich ist. Aber vielleicht unterläuft Ihnen bei der Konfiguration ein Fehler? Um derartige Probleme von vornherein zu umgehen, sollten Sie diese Dienste deaktivieren und besser gar nicht installieren. Auch sollten alle überflüs-

sigen Benutzerkonten von dem System entfernt werden. Der Bootvorgang sollte auf Möglichkeiten zur Kompromittierung des Systems überprüft werden, und die Rechte der Verzeichnisse und der ausführbaren Befehle (besonders die SetUID- und SetGID-Rechte) sollten überprüft und angepasst werden.

6.2 Installation des Linux-Systems

Ich möchte Ihnen hier nicht eine Empfehlung für eine Linux-Distribution aussprechen, denn ich denke, dass es nicht *die beste* Distribution gibt. Sicherlich gibt es Unterschiede im Design und in der Anwendung, und es mag subjektive Gründe geben, warum Sie und ich die eine oder andere Distribution vorziehen. Allerdings können Sie jede Distribution für eine Firewall einsetzen. Es ist nicht erforderlich, eine spezielle Distribution wie Fli4L[1] oder IPCop[2] zu nutzen. Wenn Sie diese Distributionen nicht kennen, sind sie sicherlich einen Blick wert. Ob es allerdings Sinn macht, beim Aufbau einer Firewall eine neue Distribution zu lernen, möchte ich bezweifeln. Verwenden Sie die Distribution, die Sie am besten kennen und konfigurieren können. Lediglich wenn Sie vor unüberwindbare Probleme stoßen, die der Distribution zuzuschreiben sind, würde ich Ihnen raten, eine andere Distribution zu testen.

Dennoch gibt es einige allgemeine Hinweise für die Installation des Systems.

Zunächst sollten Sie sich Gedanken über die Ausfallsicherheit des Systems machen. Die Firewall stellt Ihre Internetverbindung dar. Wenn diese ausfällt, kann das verheerende Konsequenzen für Ihr Geschäftsmodell haben, wenn Ihre gesamte Kommunikation (E-Mail, VoIP etc.) auf dem Internet basiert. Falls es sich lediglich um eine Firewall für private Zwecke handelt, ist das sicherlich nicht so tragisch, aber auch hier kann ein Ausfall des Internets unerwünscht sein.

Wählen Sie also eine möglichst robuste Hardware. Wenn das System ununterbrochen laufen soll, achten Sie besonders auf die Luftzufuhr und Kühlung. Wählen Sie lieber einen stromsparenden Prozessor, der auch weniger Abwärme erzeugt als die neueste Heizplatte. Ein reiner Paketfilter benötigt nicht einen Pentium 4 mit 3 GHz. Wenn Sie auch noch andere Funktionen (z.B. VPN oder Proxy) auf demselben System betreiben möchten, sieht das natürlich anders aus. Aber meist reicht auch hier noch ein einfacher stromsparender Prozessor.

Investieren Sie Ihr Geld lieber in zwei Festplatten und wenn möglich in ein Mainboard mit redundanter Stromversorgung über zwei Netzteile. Falls es Ihr Budget hergibt, ist auch ein Hardware-Raid-Controller sinnvoll. Achten Sie aber darauf, dass der Controller auch von Linux unterstützt wird. Ein Festplattenspiegel mit Raid 1 reicht vollkommen aus. Ein Raid 5 ist nicht erforderlich.

Selbst wenn Sie nicht das Geld für einen Raid-Controller ausgeben möchten, empfehle ich den Einsatz von zwei Festplatten mit einem Software-Raid 1. In einem

[1] *http://www.fli4l.de*
[2] *http://www.ipcop.org*

Fehlerfall ist die Wiederherstellung zwar etwas aufwendiger, jedoch verlieren Sie nicht Ihre Daten. Die meisten großen Distributionen können bereits bei der Installation ein Software-Raid einrichten und installieren. Ansonsten finden Sie in dem Linux Software-Raid-Howto (*http://www.tldp.org/HOWTO/Software-RAID-HOWTO.html*) entsprechende Hinweise für die Einrichtung.

Der wesentliche Vorteil bei einem Raid-System ist die Tatsache, dass das System auch bei Ausfall einer Festplatte weiterarbeitet. Aus demselben Grund empfehle ich auch die Verwendung redundanter Netzteile. Die Netzteile und die Festplatten sind am häufigsten für den Ausfall eines Systems verantwortlich. Sind beide redundant vorhanden, arbeitet das System trotz Ausfall einer Komponente weiter.

Wenn Sie das ganze Firewall-System redundant implementieren möchten, sollten Sie das Kapitel über den HA-Firewall-Cluster (Kapitel 26) lesen. Dort wird die Konfiguration eines Firewall-Clusters auf der Basis von Linux beschrieben.

Sobald Sie die Hardware ausgewählt und angeschafft haben, müssen Sie sich mit der Installation beschäftigen. Hier sind zunächst die Partitionierung und die Paketauswahl wichtig. Bei der Partitionierung sollten Sie bedenken, dass die spätere Firewall nur einen geringen Platz für die binären Pakete benötigt. Jedoch werden die Systeme Protokolldateien erzeugen, die schnell sehr groß werden können. Dies sollten Sie in der Partionierung berücksichtigen. Folgendes Schema hat sich bewährt:

- `/boot` 128M. So haben Sie immer ausreichend Platz für Kernel-Updates.
- `/usr` 1G. Sie installieren nur wenige Pakete.
- `/` 512M. Die Konfigurationsdateien (`/etc/`) und Geräte (`/dev`) benötigen nicht viel Speicher.
- `/tmp` 256M. Der temporäre Speicher sollte auf einer eigenen Partition liegen, so dass er nicht die Root-Partition füllen kann.
- `/var` Rest. Hier liegen die Protokolldateien. Dieses Verzeichnis wird bei der Verwendung der Firewall wachsen. Eventuell ist es sinnvoll, das Verzeichnis `/var/log` auch noch auf eine eigene Partition auszulagern.

Bei der Paketauswahl sollten Sie dann eine Minimalinstallation wählen. Sollte der oben angegebene Platz nicht ausreichen, müssen Sie die eine oder andere Partitionsgröße anpassen. Allerdings kenne ich keine Distribution, bei der das aktuell der Fall wäre.

Nach der Installation sollten Sie sich für den unwahrscheinlichen Fall, dass beide Festplatten ausfallen, mit einer Disaster-Recovery-Lösung wappnen. Dies ist umso wichtiger, wenn Sie nur eine Festplatte verwenden. Zwei Disaster-Recovery-Lösungen sind mir bekannt und werden von mir verwendet:

- Mondo-Rescue: *http://www.mondorescue.org/*
- Mkcdrec: *http://mkcdrec.ota.be/*

Beide Programme analysieren das System und erzeugen ein oder mehrere bootfähige CD-Images, die für die Wiederherstellung des Systems genutzt werden kön-

nen. Dabei wird das System nicht blockweise kopiert, sondern die Programme analysieren die Partitionierung und Formatierung, sichern alle Dateien und können diese dann auf einer neuen, mindestens gleich großen Festplatte wiederherstellen. Beide Systeme können mit Software-Raid- und Logical-Volume-Manager-Partitionen (LVM) umgehen.

Es empfiehlt sich, eine der beiden Lösungen zu installieren und zu testen. Später sollten Sie dann nach jeder wesentlichen Änderung des Systems oder vielleicht monatlich ein neues Disaster-Recovery-Image erzeugen. Achten Sie darauf, dass die Protokolle nicht gesichert werden. Dies bläht die Images nur unnötig auf.

6.3 Updates

Wenn Sie Ihr Linux-System mit Hilfe von CDs installieren, dann sind die darauf enthaltenen Dateien sicherlich bei der Installation zumindest teilweise veraltet. Bei vielen Paketen wurden Fehler gefunden, und bei einigen Paketen sind die Fehler möglicherweise sogar sicherheitsrelevant. Sie sollten daher, direkt anschließend an die Installation, die neuesten Updates installieren. Sehr einfach ist das, wenn Ihre Distribution dafür einen Mechanismus anbietet. Dies ist unter anderem bei Debian, SUSE, RedHat und Fedora Core der Fall. Die Anwendung dieser Mechanismen wird weiter unten erläutert.

Sie sollten sich auch überlegen, ob Sie diesen Update-Mechanismus automatisch einbinden wollen. Für mich persönlich habe ich auf vielen Systemen diese Entscheidung getroffen. So werden auf meinen Systemen die Updates stündlich geprüft und eingespielt. Manch einer mag nun die Nase rümpfen. Was passiert, wenn das Update fehlschlägt? Nun, ich habe für mich eine Risikoabwägung durchgeführt. Was passiert, wenn eine Sicherheitslücke bekannt wird und ich nicht rechtzeitig das Update durchführe? Der Schaden ist ungemein größer, als wenn automatisch ein Update durchgeführt wird, dieses fehlschlägt und der Dienst anschließend für einige Zeit nicht zur Verfügung steht. Er kann zumindest nicht mehr angegriffen werden.

Außerdem sollten Sie sich überlegen, wie Sie vorgehen, wenn Sie selbst manuell das Paket aktualisieren. Wahrscheinlich werden Sie das Update von Ihrer Distribution installieren. Im Grunde führen Sie dieselben Schritte durch, nur manuell und später. Das Update kann genauso fehlschlagen. Sie müssen das System genauso reparieren.

Ich persönlich habe erst ein einziges Mal eine schlechte Erfahrung mit der automatischen Aktualisierung der Pakete gemacht. Dabei handelte es sich um das `bind`-Paket der RHEL-3 Distribution. Nachdem das Update eingespielt wurde, wurde der Nameserver gestoppt, aber nicht wieder gestartet. Da es sich um einen primären Nameserver handelte, für den es noch weitere sekundäre Nameserver gab, fiel dies nicht sofort auf. Erst nach zwei Wochen, als die sekundären Nameserver aufgrund des fehlenden primären Nameservers ihre Arbeit einstellten, funktionierte die Namensauflösung nicht mehr.

Wenn Sie wie ich nachts schlafen, ab und zu in den Urlaub fahren und nicht 24 Stunden am Tag ein Support-Team beschäftigen möchten, kann ich Ihnen nur empfehlen, eine automatische Aktualisierung der kritischen Systeme einzurichten.

6.3.1 Debian-Updates

Auf einem Debian-System ist ein Update einfach durchzuführen. Hierzu rufen Sie nacheinander die folgenden Befehle auf:

```
/usr/bin/apt-get update -q -y
/usr/bin/apt-get upgrade -q -y
```

Der erste Befehl aktualisiert die lokal vorgehaltenen Paketlisten der verfügbaren Programmpakete. Der zweite Befehl aktualisiert die Pakete anhand dieser Liste. Die Option `-q` unterdrückt die Ausgabe von unnötigen Informationen (quiet), und die Option `-y` beantwortet automatisch alle möglichen Fragen mit Ja (yes).

6.3.2 SUSE-Updates

Bei SUSE kann das YaST-Online-Update (YOU, Abbildung 6.1) über das Werkzeug YaST konfiguriert werden. Hierzu müssen Sie aber auch sicherstellen, dass das Online-Update-Paket installiert wurde. Bei dem Einsatz eines SUSE-Linux-Enterprise-Servers (SLES) benötigen Sie für das Online-Update auch noch ein Kennwort.

6.3.3 Red Hat-Updates

Bei den kommerziellen Red Hat Enterprise Linux-(RHEL-)Systemen erfolgt das Update der Pakete mit dem Kommando `up2date`. Dieses Kommando besitzt eine grafische Oberfläche. Jedoch können Sie diese auch mit der Option `-nox` deaktivieren. Um dieses Werkzeug nutzen zu können, benötigen Sie ähnlich wie beim SLES ein Red Hat Network-(RHN-)Login und einen Wartungsvertrag.

6.3.4 Fedora Core-Updates

Bei der freien Fedora Core-Distribution ist ein Update der Pakete sehr einfach mit dem Befehl `yum` möglich. Ein `yum update` aktualisiert das System mit den aktuellen Paketen. Die Option `-y` beantwortet auch hier alle Fragen mit Ja.

6.4 Deaktivieren überflüssiger Dienste

Sobald Sie die Installation des Systems abgeschlossen und eventuelle Updates eingespielt haben, sollten Sie überflüssige Dienste deaktivieren.

Wie finden Sie nun diese Dienste? Im Grunde gibt es drei verschiedene Varianten, wie auf einem typischen Linux-System ein Dienst automatisch gestartet wird.

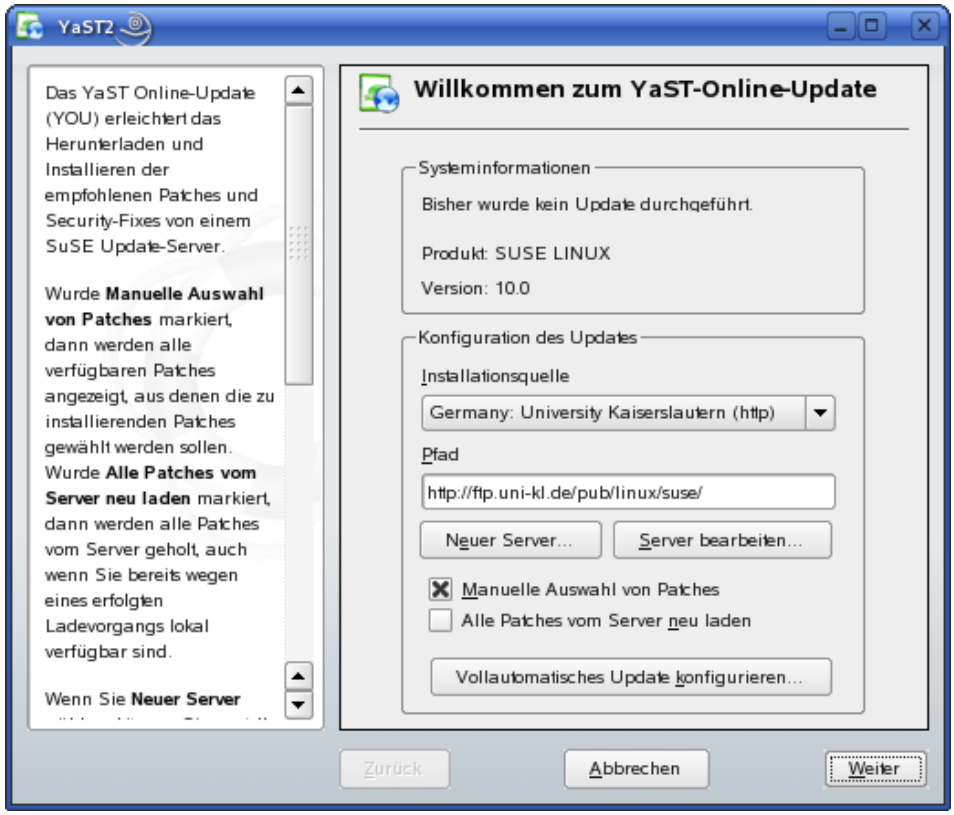


Abbildung 6.1: YaST ermöglicht das Online-Update.

- Startskripten. Viele Linux-Distributionen nutzen SysVInit-Skripten, um die Dienste zu starten. Einige, vor allem kleinere Distributionen nutzen ein einziges Startskript.
- Internet-Super-Server. Der Internet-Super-Server `inetd` oder `xinetd` startet Netzwerkdienste bei Bedarf.
- Cron-Daemon. Der Cron-Daemon startet automatisch Programme zu bestimmten Zeiten.

Die Konfiguration dieser Varianten wird weiter unten erläutert.

Woran erkennen Sie nun einen überflüssigen Dienst? Ich hoffe, dass Sie das bei vielen Diensten selbst erkennen können, da Sie wissen, was der Dienst treibt. Falls das nicht der Fall ist, sollten Sie versuchen, es herauszufinden. Hilfreich sind hier die Manpage, die Dokumentation des Pakets[3] und natürlich Google. Falls Ihnen diese Informationen nicht weiterhelfen, können Sie versuchen, zum Test den Dienst zu

[3] Mit dem Befehl `rpm -qif /etc/init.d/<dienst>` zeigen Sie die Informationen über das RPM-Paket des Dienstes an.

deaktivieren. Falls bei einem Reboot keine Fehlermeldung auftritt und alle wichtigen Funktionen zur Verfügung stehen, war der Dienst nicht erforderlich.

6.4.1 Startskripten

Die meisten Distributionen nutzen SysVInit-Startskripten. Diese Skripten befinden sich in dem Verzeichnis `/etc/init.d`. Ob ein Dienst gestartet wird oder nicht, wird über Verknüpfungen in den Verzeichnissen `/etc/rc.d/rc[0-6].d` konfiguriert. Anstatt diese Verknüpfungen jedoch von Hand zu modifizieren, sollten Sie den Befehl `chkconfig` verwenden, der auf den meisten Distributionen vorhanden ist. Falls dieser Befehl bei Ihnen nicht existiert, lesen Sie bitte in der Dokumentation der Distribution nach.

Mit dem Befehl `chkconfig --list` können Sie den aktuellen Zustand der Startskripten anzeigen.

```
# chkconfig --list postfix
postfix         0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

`chkconfig <dienst> off` schaltet den entsprechenden Dienst ab.

Alternativ zu den SysVInit-Skripten gibt es vor allem auf kleinen Distributionen ein einzelnes Startskript, das die Dienste startet. Hier müssen Sie in die Datei schauen und die entsprechenden Zeilen durch Kommentieren deaktivieren. Teilweise (z.B. OpenWRT) existiert auch ein Verzeichnis `/etc/init.d`, und jedes Skript in diesem Verzeichnis wird automatisch aufgerufen. Um einen Dienst zu deaktivieren, genügt es dann meist, die Ausführrechte von der Datei zu entfernen.

Achtung

Änderungen in den Startskripten machen sich erst bei einem Neustart oder dem Wechsel des Runlevels bemerkbar.

6.4.2 Internet-Super-Server

Fast jede Linux-Distribution verfügt über den Internet-Super-Server `inetd` oder `xinetd`. Wird dieser Dienst über ein Startskript gestartet, so startet er bei Bedarf, entsprechend seiner Konfiguration, weitere Dienste. Das bedeutet, dass Sie den Telnet-Server in der Ausgabe von `ps -ef` nicht sehen, obwohl er verfügbar ist. Er wird erst bei Bedarf von dem `(x)inetd` gestartet.

Der Inetd verfügt über eine Konfigurationsdatei `/etc/inetd.conf`, in der pro Zeile ein Dienst konfiguriert wird. Sie schalten die entsprechenden Dienste durch Auskommentieren der Zeile ab.

Bei dem Xinetd werden die Dienste meist über einzelne Dateien im Verzeichnis `/etc/xinetd.d` gesteuert. Diese Dateien enthalten eine Zeile `enable=` oder `disable=`. Durch Setzen des ensprechenden Wertes (`enable=no` bzw. `disable=yes`) deaktivieren Sie den Dienst.

Achtung

Natürlich müssen Sie nach einer Modifikation der Konfiguration den Internet-Super-Server neu starten.

6.4.3 Cron-Daemon

Schließlich können Programme auch automatisch von dem Cron-Daemon gestartet werden. Der Cron-Daemon wird über Cron-Tabellen konfiguriert. Auf den meisten Linux-Systemen existieren zwei Arten von Cron-Tabellen.

Jeder Benutzer kann eine persönliche Cron-Tabelle anlegen, wenn ihm dies über die Dateien `/etc/cron.allow` oder `/etc/cron.deny` erlaubt wird. Existiert die erste Datei, so dürfen nur die dort aufgeführten Benutzer eine Cron-Tabelle anlegen. Existiert die zweite Datei, so dürfen alle Benutzer, außer den dort aufgeführten, eine Cron-Tabelle anlegen. Diese Cron-Tabelle wird mit dem Befehl `crontab -e` angelegt und editiert. Mit dem Befehl `crontab -l` zeigen Sie Ihre eigene Cron-Tabelle an, und mit `crontab -r` löschen Sie diese.

Die Syntax dieser Datei ist recht einfach. Es handelt sich um eine Tabelle mit sechs Spalten. Die ersten fünf Spalten enthalten die Definition eines Zeitpunkts: Minuten, Stunden, Tag, Monat und Wochentag. Dabei wird der Wochentag ebenfalls mit einer Ziffer angegeben (0,7 = Sonntag). Der Cron-Daemon vergleicht jede Minute die aktuelle Systemzeit mit der eingetragenen Zeit und führt bei Übereinstimmung den Befehl in der sechsten Spalte aus. Betrachten Sie folgendes Beispiel:

```
0      5    *    *    *   /bin/test.sh
*/30  7-18  *    *   1-5  /bin/getmail.sh
```

Das Skript `/bin/test.sh` wird um 5:00 Uhr an jedem Tag (*), in jedem Monat (*) und unabhängig vom Wochentag (*) ausgeführt. Das Skript `/bin/getmail.sh` wird von 7:00 Uhr bis 18:30 alle 30 Minuten (wenn die Division ohne Rest aufgeht) von Montag (1) bis Freitag (5) unabhängig vom Datum ausgeführt.

Zusätzlich zu den Cron-Tabellen der Benutzer existiert auf einem modernen Linux-System auch eine System-Cron-Tabelle `/etc/crontab`. Diese Cron-Tabelle gleicht stark den Tabellen der Benutzer, weist jedoch eine zusätzliche Spalte zwischen der fünften und sechsten Spalte auf. Hier kann der Benutzer angegeben werden, in dessen Kontext der Cron-Daemon den Befehl in der nun siebten Spalte aufrufen soll.

```
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

Die obigen Zeilen stammen von einer Fedora Core Linux-Distribution. Der hier von dem Cron-Daemon aufgerufene Befehl ist `run-parts`. Diesem Befehl werden in Abhängigkeit von der Zeit unterschiedliche Verzeichnisse als Argument übergeben. Der Befehl durchsucht das angegebene Verzeichnis und ruft alle Befehle in diesem Verzeichnis auf. So wird immer eine Minute nach der vollen Stunde jede ausführbare Datei in dem Verzeichnis `/etc/cron.hourly` aufgerufen. Ähnlich wird immer Sonntag (0) um 4:22 das Verzeichnis `/etc/cron.weekly` abgearbeitet.

Um zu erkennen, welche Programme aufgerufen werden, sollten Sie daher die Verzeichnisse analysieren und überflüssige Programme entfernen oder ihnen das Ausführrecht entziehen. Dieses Verhalten ist eigentlich bei allen Linux-Distributionen ähnlich.

Achtung

Änderungen an den Cron-Tabellen der Benutzer sind sofort aktiv. Ein Neustart des Cron-Daemons ist nur bei einer Modifikation der Datei `/etc/crontab` erforderlich. Auch Änderungen in den Verzeichnissen `/etc/cron.*` erfordern keinen Neustart.

6.5 Entfernen überflüssiger Software

Nachdem Sie überflüssige Dienste deaktiviert haben, können Sie nun die entsprechenden Pakete und vielleicht auch noch weitere Pakete entfernen. Das Entfernen von überflüssigen Paketen ist unter Linux seit der Einführung der Paketverwaltungssysteme recht einfach geworden, da diese die Abhängigkeiten überwachen und im Zweifelsfall die Deinstallation verhindern. Beginnen Sie am einfachsten damit, dass Sie alle Pakete auflisten. Dies geht auf einer RPM-basierten Distribution recht einfach mit `rpm -qa`. Auf einer Debian-Distribution zeigt der Befehl `dpkg -l` die installierten Pakete an. Untersuchen Sie die Liste, und versuchen Sie, Pakete zu deinstallieren, die Sie nicht benötigen. Sobald das Paket noch von weiteren Paketen benötigt wird, wird die Paketverwaltung Ihnen einen Abhängigkeitskonflikt anzeigen. Entscheiden Sie dann, ob Sie diese Pakete auch deinstallieren wollen.

Tipp

Wenn Sie diese Entscheidungen mangels Erfahrung noch nicht treffen können oder wollen, stellen Sie zumindest sicher, dass Sie möglicherweise vorhandene C-Compiler von dem System entfernen. In der Vergangenheit sind bereits mehrfach Würmer aufgetreten, die nach einem Einbruch auf einem System zunächst sich selbst übersetzt haben. Fehlt der C-Compiler, ist die Verbreitung eines solchen Wurms gestoppt.

6.6 Sicherheit auf Dateisystemebene

Die meisten Linux-Distributionen sind nicht speziell auf Firewall-Zwecke ausgerichtet. Ihre Zielsetzung ist eher ein Multifunktionssystem. Es soll möglichst einfach sein, sowohl Netzwerkdienste anzubieten als auch als normaler Benutzer über die grafische Oberfläche eine DVD abzuspielen und zu brennen. Hierfür müssen diese Systeme viele Tricks anwenden, damit das auch so unproblematisch funktioniert, wie es der Anwender möchte. So hat normalerweise ein einfacher Benutzer nicht das Recht, auf das CD- oder DVD-Laufwerk zuzugreifen, und er besitzt dort schon gar keine Schreibrechte. Auch ein einfaches Ping darf der normale Benutzer nicht starten. Diese und viele weitere Aktionen dürfen nur von dem privilegierten Benutzer *root* durchgeführt werden. Damit dennoch ein Benutzer den Befehl benutzen darf, wird entweder der Benutzer für die Ausführung des Befehls mit *root*-Privilegien ausgestattet oder die Rechte der Ressource, auf die der Benutzer zugreifen möchte, werden entsprechend angepasst.

Die grundsätzliche Problematik ist schon sehr alt. Wie soll zum Beispiel ein Benutzer sein Kennwort ändern, wenn er keine Schreibrechte an der Datei `/etc/passwd` oder `/etc/shadow` hat? Daher wurde sehr früh in der Geschichte von Unix (1971) bereits ein Mechanismus geschaffen, der es erlaubt, für die Ausführung eines Befehls dem Prozess erweiterte Privilegien zu übertragen. Das SetUID- und das SetGID-Recht waren geboren. Verfügt ein Befehl über diese Rechte, so werden für die Ausführung des Befehls die Rechte des Eigentümers (SetUID) oder der Gruppe (SetGID) auf den Prozess übertragen. Sie erkennen diese Rechte an einem kleinen `s`.

```
-r-s--x--x  1 root root 18840  7. Mär 2005  /usr/bin/passwd
-r-xr-sr-x  1 root tty   9752 27. Apr 17:42 /usr/bin/wall
```

Wenn ein Benutzer den Befehl `/usr/bin/passwd` aufruft, erbt er für die Ausführung die Rechte des Eigentümers *root*. Bei Aufruf des Befehls `/usr/bin/wall` erbt er die Rechte der Gruppe *tty*. Es ist dann Aufgabe der Befehle zu prüfen, dass der Anwender auch tatsächlich nur den vorgesehenen Vorgang durchführt und die Rechte nicht missbraucht. Leider wiesen die Befehle in der Vergangenheit immer wieder Fehler auf, so dass für die Zukunft weitere Fehler nicht ausgeschlossen werden können.

Daher sollten Sie sich fragen, ob auf Ihrer Firewall überhaupt normale unprivilegierte Benutzer arbeiten sollen. Wenn Sie beim Aufruf der Befehle bereits *root* sind

oder die Rechte immer über `sudo` (siehe unten) erhalten, ist es nicht nötig, dass diese Rechte gesetzt sind.

Diese Rechte haben den zusätzlichen Nachteil, dass Sie jedem Benutzer, auch einem Systembenutzer wie *nobody*, für die Ausführung die Privilegien übertragen. Sie sollten daher diese Rechte entfernen. Um das System nach derartigen Befehlen abzusuchen, können Sie die folgenden Befehle verwenden:

```
# find / -perm +4000 -ls
# find / -perm +2000 -ls
```

Sie können die Rechte mit `chmod u-s <datei>` und `chmod g-s <datei>` entfernen. Prüfen Sie auch hier anschließend mit einem Neustart, ob das System noch so arbeitet, wie Sie es sich vorstellen.

Tipp: Sudo

Sinnvollerweise legen Sie auf der Firewall lediglich für jeden Firewall-Administrator ein Benutzerkonto an, das Sie mit individuellen Kennwörtern versehen. Die Administration des Systems kann dann mit dem Befehl `sudo` erfolgen. Mit diesem Befehl können Sie einem bestimmten Benutzer bei der Ausführung eines bestimmten Befehls erweiterte Privilegien zuweisen. Bei der ersten Ausführung verlangt der Befehl zusätzlich noch die Authentifizierung des Benutzers, die Sie aber auch abschalten können.

Sie konfigurieren den Befehl `sudo` in der Datei `/etc/sudoers`. Diese Datei sollten Sie jedoch nicht direkt, sondern mit dem Befehl `visudo` editieren. Dieser Befehl prüft die Syntax und warnt Sie vor dem Abspeichern bei Fehlern in der Datei.

Um nun eine Gruppe von Administratoren mit *root*-Privilegien auszustatten, können Sie die folgenden Zeilen verwenden:

```
User_Alias ADMIN = spenneb, oliver
ADMIN ALL=(root) ALL
```

Die erste Zeile definiert einen Alias `ADMIN` für die Benutzer *spenneb* und *oliver*. Die zweite Zeile erlaubt diesen Benutzern, auf allen Rechnern als *root* jeden Befehl auszuführen. Die Einschränkung der Rechner ermöglicht es Ihnen, eine zentrale Datei zu erzeugen und für mehrere Systeme zu verwenden und zu verteilen. Dann können Sie hier den Rechnernamen angeben, für den diese Zeile gelten soll.

Die Benutzer *spenneb* und *oliver* benötigen nun nicht mehr das *root*-Kennwort. Sie können selbst jeden Befehl ausführen. Bei der ersten Verwendung und nach Ablauf von 5 Minuten müssen Sie sich mit Ihrem eigenen Kennwort authentifizieren.

Jeder Zugriff wird außerdem protokolliert:

```
Sep 11 15:16:59 bibo sudo:  spenneb : TTY=pts/2 ; PWD=/buch/fw_buch/buch ;
  USER=root ; COMMAND=/usr/bin/tail /var/log/messages
```

6.7 Sicherheit beim Bootvorgang

Damit Ihre Bemühungen, das System zu sichern, nicht vergebens sind, sollten Sie auch den Bootvorgang des Systems in Ihre Betrachtungen mit einbeziehen.

Zunächst sollten Sie sorgfältig den Aufstellungsort für das System wählen. Achten Sie darauf, dass kein Unbefugter physikalischen Zugang zu dem System erhält. Wählen Sie also nicht die Besenkammer am Ende des Flurs, sondern einen Raum, den Sie abschließen können.

Zusätzlich sollten Sie darauf achten, dass die Bootreihenfolge im BIOS es nicht ermöglicht, das System von Diskette, CD oder USB-Stick zu booten. Sichern Sie das BIOS gegen unbefugte Änderungen mit einem Kennwort.

Achten Sie auch darauf, dass der Boot-Manager mit einem Kennwort gegen unbefugte Änderungen geschützt ist. Erfreulicherweise bieten moderne Distributionen Ihnen dies direkt bei der Installation an. Falls dies nicht der Fall ist, fügen Sie ein Kennwort zur Konfiguration hinzu.

Bei dem Boot-Manager Lilo können Sie einfach zwei Zeilen an den Anfang der Datei `/etc/lilo.conf` anfügen:

```
password=geheimes_Kennwort
restricted
```

Leider müssen Sie das Kennwort in Klartext angeben. Sie sollten daher darauf achten, dass keiner außer *root* diese Datei lesen darf. Der Parameter `restricted` sorgt dafür, dass lediglich Modifikationen des Bootvorgangs ein Kennwort verlangen. Nach der Modifikation der Datei müssen Sie Lilo neu installieren. Rufen Sie hierzu `lilo -v` auf.

Bei dem Boot-Manager Grub können Sie mit dem Befehl `grub-md5-crypt` ein Kennwort verschlüsseln und in der Grub-Konfigurationsdatei mit dem Parameter `password --md5 $1$...` angeben. Anschließend ist für jede Modifikation des Bootverhaltens das Kennwort anzugeben.

Auf Red Hat- und Fedora Core Linux-Distributionen existiert zusätzlich noch die Möglichkeit, während des Startens der Dienste diese interaktiv zu bestätigen. Dazu müssen Sie, während der Init-Prozess startet, `I` eingeben. Sie sollten auch diese Möglichkeit abschalten, damit niemand beim Boot einen Dienst überspringen kann. Setzen Sie hierzu in der Datei `/etc/sysconfig/init` die Variable `Prompt=no`.

Nun sollte keine unbefugte Modifikation des Bootvorgangs mehr möglich sein.

6.8 Bastille-Linux

Die von mir bisher beschriebenen Schritte zur Härtung können nur einen allgemeinen Weg aufzeigen. Je nachdem, welche Distribution Sie verwenden, sind vielleicht noch weitergehende Schritte erforderlich, oder Sie können den einen oder anderen Schritt überspringen. Es ist in jedem Fall ein großer Aufwand, alle Schritte richtig und in der richtigen Reihenfolge reproduzierbar und dokumentiert durchzuführen. Bastille-Linux hilft Ihnen dabei.

Bastille-Linux ist ein Härtungswerkzeug für Linux- und Unix-Systeme. Es unterstützt RedHat Linux, RedHat Enterprise Linux, Fedora Core, SUSE, Mandrake, Gentoo, Debian, HP-UX und MacOS X. Sie können mit diesem Werkzeug einfach, reproduzier- und automatisierbar Dienste und Systemeinstellungen konfigurieren. Es schaltet unnötige Dienste ab und kann sogar Dienste in einem Chroot laufen lassen.

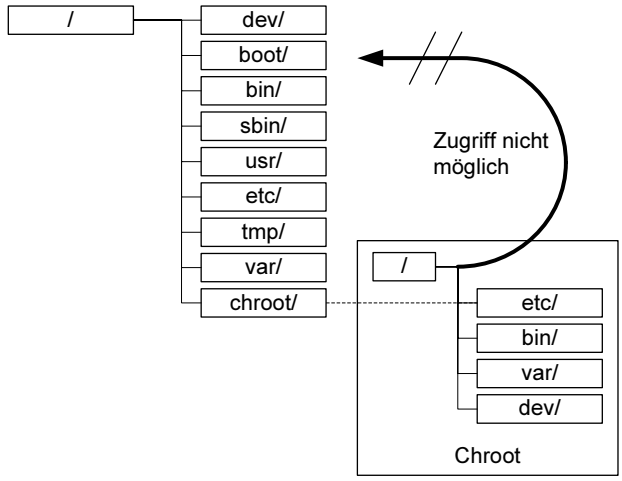


Abbildung 6.2: Nach einem Chroot kann ein Prozess auf Dateien außerhalb des Chroot nicht mehr zugreifen.

Tipp: Chroot

Ein Chroot stellt eine zusätzliche Sicherheitsfunktion dar. Dabei wechselt ein Prozess beim Start sein Root-Verzeichnis (siehe Abbildung 6.2). Anschließend kann der Prozess auf Dateien außerhalb des eigenen Root-Verzeichnisses nicht mehr zugreifen. Ein Angreifer hat so nach einem Einbruch über diesen Prozess keinen Zugriff auf Dateien des restlichen Systems.

Leider ist die Konfiguration eines derartigen Chroot sehr aufwendig, da alle Dateien, die der Prozess während seiner Ausführung

benötigt, in diesem Chroot-Verzeichnis physikalisch vorhanden sein müssen. Eine symbolische Verknüpfung reicht hier nicht aus. So benötigen viele Dienste Zugriff auf weitere Bibliotheken und Dateien wie `/etc/passwd`, `/etc/resolv.conf`, `/etc/hosts` etc. Die Administration eines Chroot ist daher recht umständlich, aber bei einigen Diensten den Aufwand wert. Dienste, die von Haus aus ein Chroot unterstützen, sind zum Beispiel der Bind-Nameserver und Snort. Weitere Dienste können mit dem Kommandozeilenbefehl `chroot` in einem Chroot-Verzeichnis gestartet werden.

Leider ist ein Chroot auf einem Linux-System nicht so effektiv wie auf einigen anderen Unix-Plattformen. Sobald ein Prozess in dem Chroot-Verzeichnis Privilegien des Benutzers *root* benötigt, besteht die Gefahr, dass ein Angreifer aus dem Chroot-Verzeichnis ausbrechen kann. Ein Chroot schützt nicht vor *root*! Stellen Sie daher sicher, dass alle Prozesse nach dem Wechsel in das Chroot auch ihre Benutzeridentität wechseln.

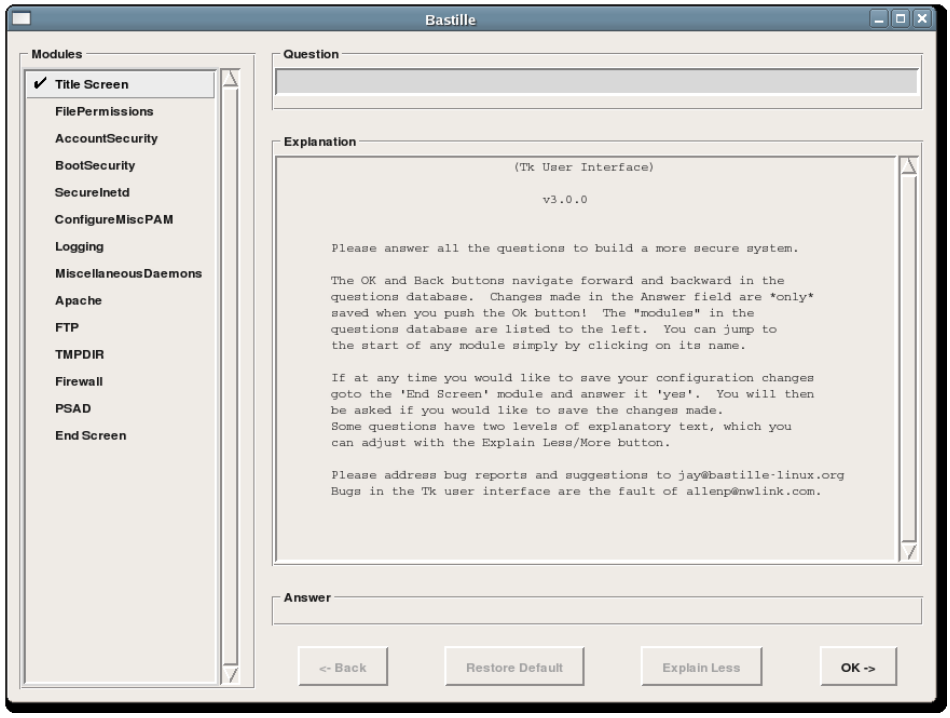


Abbildung 6.3: Die grafische Oberfläche kann mit der Maus bedient werden (bastille -x).

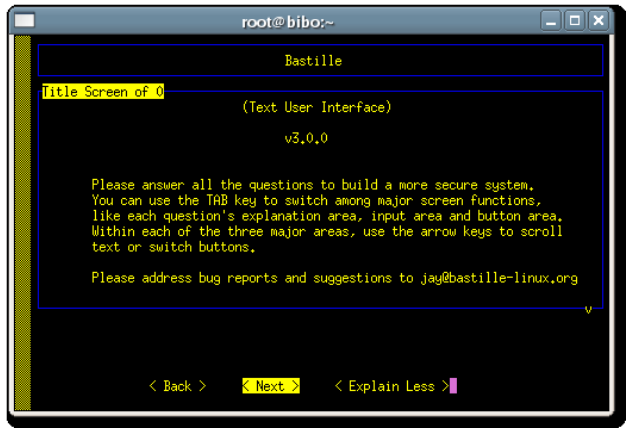


Abbildung 6.4: Firewall-Systeme verfügen meist nicht über eine grafische Oberfläche. Hier können Sie Bastille im Text-Modus einsetzen (bastille -c).

Sie können Bastille-Linux in zwei verschiedenen Varianten verwenden: interaktiv und nicht-interaktiv. Im interaktiven Modus können Sie zwischen einer grafischen Perl/TK- (Abbildung 6.3) und einer textbasierten Perl/Curses-Oberfläche (Abbildung 6.4) wählen. Wenn Sie es interaktiv einsetzen, wird Ihnen Bastille-Linux die verschiedenen Optionen erklären, und Sie entscheiden, ob und wie die Probleme abgestellt werden. Der nicht-interaktive Modus bietet sich für die automatische Vervielfältigung einer Sicherheitsrichtlinie auf vielen Systemen an. Sie stellen so die Nachvollziehbarkeit der Systemhärtung sicher.

Ich werde Ihnen nun kurz eine Führung durch die verschiedenen Funktionen von Bastille-Linux 3.0.X geben.

Bastille-Linux beginnt mit der Härtung der Dateirechte. Zunächst werden die Rechte wichtiger Befehle der Systemadministration so modifiziert, dass ein normaler Benutzer keinen Zugriff erhält (Abbildung 6.5).

Anschließend können Sie entscheiden, ob die Befehle `at`, `ping`, `traceroute`, `mount` etc. über die SetUID-Rechte verfügen sollen oder nicht. Damit Bastille-Linux die Sicherheit erhöht, müssen Sie auf diesen Bildschirmen jeweils `Yes` anwählen.

Im Bereich *AccountSecurity* können Sie wählen, ob die R-Werkzeuge, die eine Klartextanmeldung ohne Kennwort, basierend auf der IP-Adresse, erlauben, deaktiviert werden sollen. Zusätzlich bietet Bastille-Linux die Implementierung von Richtlinien, die das Alter von Kennwörtern überprüfen, das Setzen einer Umask und das Ablehnen des *root*-Logins. Achten Sie darauf, dass Bastille-Linux einige Fragen bereits per Default mit `Yes` beantwortet!

Bei der Betrachtung der *Boot-Security* kann Bastille-Linux den Reboot per Ctrl-Alt-Delete abstellen und den Single-User-Modus mit einem Kennwort schützen, falls dies noch nicht der Fall sein sollte.

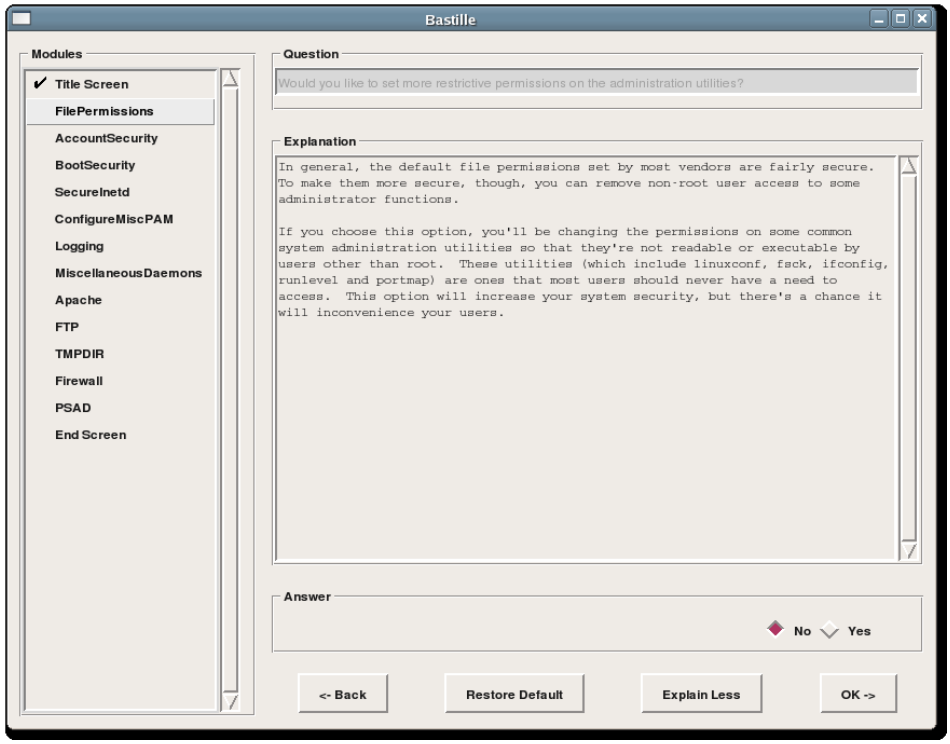


Abbildung 6.5: Bastille entfernt bei Sysadmin-Befehlen die Lese- und Ausführrechte für unprivilegierte Benutzer.

Tipp

Falls Sie beim Aufruf von Bastille-Linux weniger oder darüber hinausgehende Fragen gestellt bekommen sollten, hängt dies wahrscheinlich mit Ihrer Linux-Distribution zusammen. Bastille-Linux analysiert das System und stellt die Fragen entsprechend.

Bei der Konfiguration des `inetd` bietet Bastille-Linux zunächst die Sicherung der Dienste mit TCP-Wrappers über einen Default-Eintrag in der Datei `/etc/hosts.deny` (siehe Abbildung 6.6) und die Konfiguration von Standard-Bannern für die typischen Dienste Telnet, FTP etc.

Der nächste Bildschirm bietet die Konfiguration der Pluggable Authentication Modules (PAM) an. Hier können Sie zum Beispiel den Konsolenzugriff auf eine bestimmte Liste von Konten beschränken. Alle weiteren Konten dürfen sich nicht auf der Konsole anmelden.

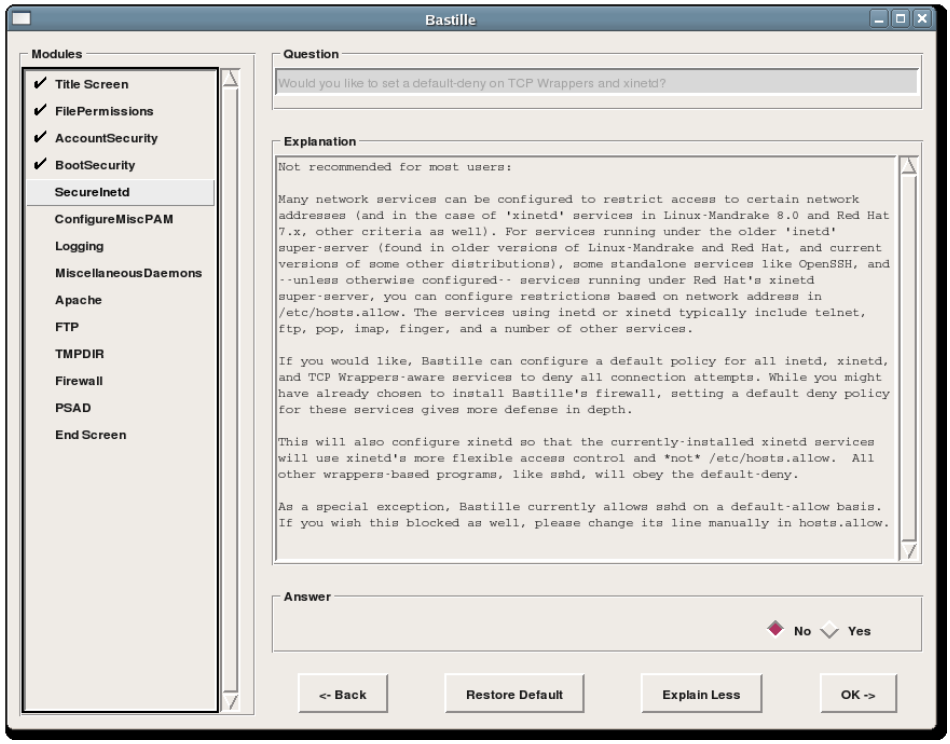


Abbildung 6.6: Viele Netzwerkdienste nutzen TCP-Wrappers als Zugangskontrolle. Bastille-Linux kann den Zugriff auf diese Dienste mit einem Default-Eintrag ähnlich einer Firewall beschränken.

Der nächste Punkt, *Logging*, erlaubt die Aktivierung des Process-Accounting. Hiermit überwacht und protokolliert der Linux-Kernel jeden aufgerufenen Befehl. Achtung, die Protokolle wachsen sehr schnell auf einem normalen System. Für eine Firewall kann dies aber durchaus sinnvoll sein. Denken Sie jedoch daran, dass auch die von Cron aufgerufenen Befehle protokolliert werden.

Im Bereich *Miscellaneous Daemons* können Sie Dienste wie NFS und Samba deaktivieren, die Unterstützung für den HP Office Jet (HPOJ) abschalten und ISDN deaktivieren. Dienste wie Apache und FTP werden gesondert behandelt.

Bei der Konfiguration des Apache können Sie diesen zunächst nur auf dem lokalen Rechner (localhost) anbieten, auf eine spezielle IP-Adresse binden und zum Beispiel die Verwendung von symbolischen Verknüpfungen abschalten.

Die FTP-Server-Konfiguration durch Bastille-Linux kann sowohl den WU-ftpd als auch den heute üblicheren Vsftpd konfigurieren und gegen Angriffe sichern.

Unter dem Punkt *TMPDIR* bietet Bastille-Linux eine sehr interessante Möglichkeit zur Erzeugung temporärer sicherer `/tmp`-Verzeichnisse. Diese werden für jeden Be-

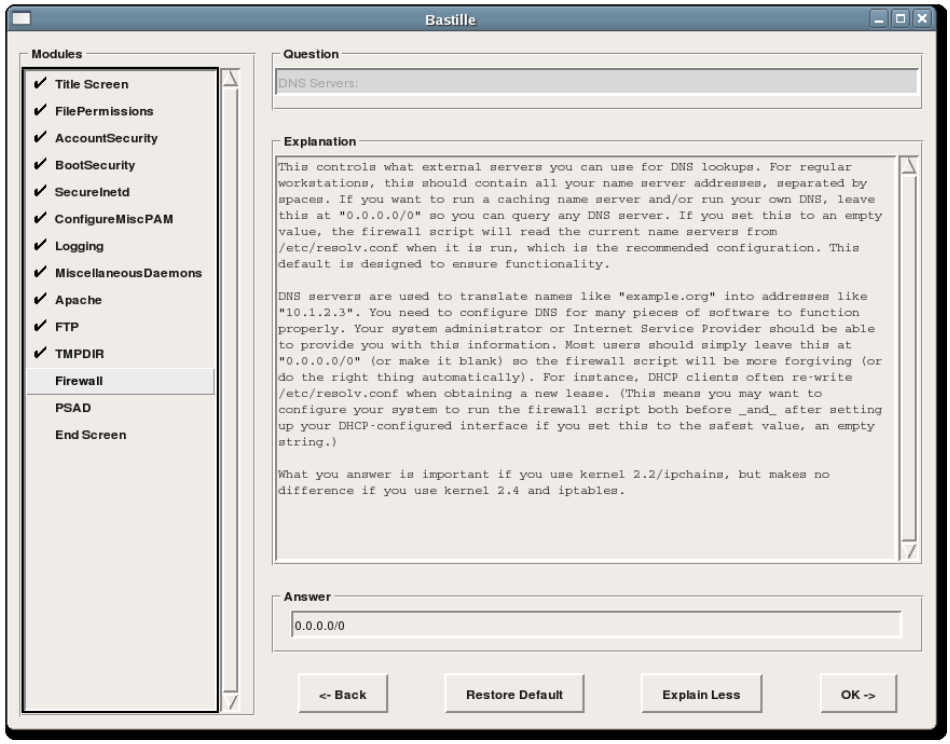


Abbildung 6.7: Bastille-Linux kann sogar nach Beantwortung einiger Fragen ein Firewall-Skript erzeugen.

nutzer automatisch bei seiner Anmeldung erzeugt. So verfügt jeder Benutzer über ein eigenes temporäres Verzeichnis. Viele Angriffe, die dieses Verzeichnis und seine allgemeine Verfügbarkeit ausnutzen, sind so nicht möglich.

Im Grunde versucht Bastille-Linux sogar, dieses Buch zu ersetzen, in dem es die Möglichkeit einer skriptgesteuerten Erzeugung einer Firewall-Konfiguration ermöglicht. Hierzu müssen Sie in mehreren Bildschirmen Fragen zu Ihren genutzten Diensten (z.B. DNS, siehe Abbildung 6.7) beantworten, und Bastille-Linux generiert am Ende ein fertiges Firewall-Skript.

Natürlich ermöglicht es Ihnen Bastille-Linux nicht, sämtliche Feinheiten des Iptables-Befehls auszuschöpfen, jedoch stellt das Skript auch einen guten Start für die Eigenentwicklung dar. Vielleicht finden Sie in diesem Skript einige gute Ideen, die Sie übernehmen wollen.

Als letzten Punkt bietet Bastille-Linux noch die Konfiguration des Port Scan Attack Detector (psad, *http://www.cipherdyne.org/psad/*) an. Dieses Werkzeug analysiert Netfilter-Protokolle und ermittelt mögliche Portscans und Angriffe. Dieses Werkzeug wird auch im Kapitel 12 besprochen. Daher möchte ich für weitere Informationen auf dieses Kapitel verweisen.

Eine besonders nette Funktion von Bastille-Linux ist die Tatsache, dass Sie alle Änderungen wieder rückgängig machen oder auf einer anderen Maschine klonen können. Dies ist möglich, da die interaktive Oberfläche lediglich eine Konfigurationsdatei erzeugt, aber diese noch nicht aktiviert. Diese Aktivierung erfolgt anschließend und kann auch auf einem anderen System durchgeführt werden. Diese Konfigurationsdatei befindet sich anschließend in dem Verzeichnis `/etc/Bastille`. In dieser Datei befinden sich die Fragen und die von Ihnen gegebenen Antworten.

```
# Q:  Are you finished making changes to your Bastille configuration?
.End_Screen="Y"
# Q:  Would you like to enforce password aging? [Y]
AccountSecurity.passwdage="Y"
# Q:  Should Bastille disable clear-text r-protocols that use IP-based authentication? [Y]
AccountSecurity.protectrhost="Y"
# Q:  Should we disallow root login on tty's 1-6? [N]
AccountSecurity.rootttylogins="N"
# Q:  What umask would you like to set for users on the system? [077]
AccountSecurity.umask="077"
# Q:  Do you want to set the default umask? [Y]
AccountSecurity.umaskyn="Y"

... gekürzt ...
```

Bastille-Linux kann Sie so sehr mächtig und leicht reproduzier- und dokumentierbar bei der Härtung Ihrer Linux-Systeme unterstützen. Sicherlich ist die Härtung eines Systems eine Aufgabe, die Sie nicht auf jedem System durchführen werden. Es empfiehlt sich jedoch für alle exponierten Systeme in der DMZ und Firewalls.

6.9 Mandatory-Access-Control-Systeme (MAC)

Leider unterstützt ein klassisches Linux-System nur ein sehr einfaches Rechte-Modell. So können der Benutzer *root* und der Eigentümer einer Datei die Rechte dieser Datei modifizieren. Dabei können die Rechte für den Eigentümer, eine Gruppe und alle weiteren Benutzer definiert werden. Mit modernen Dateisystemen können auch die POSIX-ACLs verwendet werden (siehe Tipp). Dann ist es möglich, auch mehreren Benutzern unterschiedliche Rechte zuzuweisen.

Auch beim Einsatz der POSIX-ACLs haben Sie lediglich die Rechte `r`, `w` und `x`. Sie können also lediglich die Rechte für das Lesen, Schreiben und Ausführen verwalten. Weitergehende Rechte existieren nicht.

Wünschenswert wäre die Möglichkeit, die Privilegien des Benutzers *root* einzelnen normalen Benutzern für bestimmte Aufgaben zukommen zu lassen. Obwohl dies seit Jahren mit dem Capability-System möglich ist, existierte bis zur Einführung von SELinux keine sinnvolle Administrationsoberfläche, die zum festen Bestandteil von Linux geworden ist. Alle anderen verschiedenen Ansätze (LIDS, grsecurity, RSBAC etc.) sind nur als Patch verfügbar. Diese Systeme werden häufig auch als

Mandatory-Access-Control-Systeme (MAC) bezeichnet. Dies setzt sie von dem klassischen Unix als Discretionary-Access-Control-System (DAC) ab. Unix ist ein DAC-System, da hier der Eigentümer einer Datei ihre Rechte definiert (die Rechte werden entsprechend der Diskretion des Eigentümers definiert). Der Eigentümer kann hierbei auch leicht Fehler machen. Bei einem MAC-System werden die Rechte zentral für alle Dateien verwaltet. Selbst wenn der Eigentümer *root* fälschlicherweise einem anderen Benutzer Leserecht an der Datei `/etc/shadow` zuweisen würde, könnte das MAC-System, das von einem über *root* stehenden Superuser verwaltet wird, diesen Zugriff noch verhindern.

Alle MAC-Systeme verfügen über einen derartigen von *root* unterschiedlichen Superuser. Häufig wird hierfür ein weiteres Kennwort verlangt. Teilweise ist zur Laufzeit keine Modifikation des MAC-Systems möglich.

Alle MAC-Systeme für Linux stellen nur zusätzliche Systeme dar. Das bedeutet, dass beim Zugriff auf eine Datei sowohl das DAC- als auch das MAC-System den Zugriff erlauben müssen.

Derartige Systeme können stark die Sicherheit des Betriebssystems erhöhen. Leider ist eine komplette Besprechung dieser Systeme im Rahmen dieses Buches nicht möglich und sinnvoll. Das Linux Intrusion Detection System (LIDS) wurde aber von mir bereits in dem Buch »Intrusion Detection und Prevention mit Snort 2 & Co.« ausführlich behandelt.

Tipp

Verwenden Sie einfach eine Distribution, die bereits ein derartiges MAC-System vorkonfiguriert mitbringt. Aktuell sind das zum Beispiel Fedora Core 3 und 4, RHEL 4 und Gentoo.

Tipp: POSIX-ACLs

Die klassischen Unix- und Linux-Dateisysteme erlauben es nur, die Rechte für den Eigentümer, eine Gruppe und den Rest (others) zu verwalten. Eine weitere Abstufung ist nicht möglich. Es kann nicht eine Gruppe mit Leserechten und eine weitere Gruppe mit Schreibrechten ausgestattet werden. Viele andere Betriebssysteme bieten diese Möglichkeit. Für Unix wurden die POSIX-ACLs geschaffen, um dieses Problem zu beheben. Alle aktuellen Linux-Dateisysteme unterstützen inzwischen auch diese erweiterten ACLs.

Um die ACLs zu nutzen, müssen Sie das Dateisystem mit der Option `acl` mounten. Hierzu tragen Sie die Option in der Datei `/etc/fstab` in der entsprechenden Spalte ein oder geben sie beim

Mount-Vorgang auf der Kommandozeile ein. Um das Dateisystem `/home` mit ACL-Optionen neu zu mounten, verwenden Sie den folgenden Befehl:

```
mount -o remount,acl /home
```

Nun können Sie für Dateien erweiterte ACLs definieren. Hierfür gibt es die Befehle `setfacl` und `getfacl`. Leider unterstützen die Befehle `ls` und `chmod` die ACLs nicht.

```
# ls -l datei
-rw-r--r--  1 root root 0 19. Sep 18:17 datei
# setfacl -m u:test:rw datei
# ls -l datei
-rw-rw-r--+ 1 root root 0 19. Sep 18:17 datei
# getfacl datei
# file: datei
# owner: root
# group: root
user::rw-
user:test:rw-
group::r--
mask::rw-
other::r--

# setfacl -m u:test:rwx datei
# setfacl -m m::rx datei
# ls -l datei
-rw-r-xr--+ 1 root root 0 19. Sep 18:17 datei
# getfacl datei
# file: datei
# owner: root
# group: root
user::rw-
user:test:rwx                                   #effective:r-x
group::r--
mask::r-x
other::r--
```

Sobald Sie eine ACL einer Datei hinzugefügt haben, zeigt der Befehl `ls` bei den Rechten ein `+` an. Dieses zeigt Ihnen, dass weitere ACLs verborgen sind. Außerdem wird an der Stelle, an der üblicherweise die Gruppenrechte angezeigt werden, nun die Maske angezeigt. Diese Maske definiert die maximalen Rechte, die mit den ACLs

vergeben werden können. Alle über die Maske per ACL hinausgehenden Rechte werden automatisch nicht aktiv.

Wenn Sie ACLs einsetzen, sollten Sie darauf achten, dass das Dateisystem immer mit der Option `acl` gemountet wird. Ansonsten sind die ACLs nicht aktiv. Außerdem sollten Sie Ihre Backup-Programme überprüfen. Viele Backup-Programme können nicht mit ACLs umgehen. So sichert `tar` die ACLs nicht! Anstelle von `tar` können Sie aber `star` verwenden.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

7 Intrusion-Detection- und -Prevention-Systeme

Ist Ihre Firewall sicher? Natürlich haben Sie bereits einige Erfahrung in der Konfiguration von Firewalls oder werden dieses Buch aufmerksam lesen, aber sind Sie sicher, dass Sie keinen Fehler machen?

Vielleicht kommt ein potenzieller Angriff auch gar nicht von außen, so dass die Firewall ihn nicht abwehren kann. Viele Angriffe werden von innen ausgeführt. Diese Angriffe müssen die externe Firewall nicht mehr passieren und können daher weder abgewehrt oder protokolliert werden!

Hier helfen Intrusion-Detection- und -Prevention-Systeme. Während ein Intrusion-Detection-System (IDS) keine zusätzliche Sicherheit schafft, sondern nur nach einem Angriff diesen meldet, wehrt ein Intrusion-Prevention-System (IPS) diesen Angriff direkt bei der Erkennung ab. Im Folgenden werde ich Ihnen eine kurze Einführung in die verschiedenen Technologien geben. Weitere Informationen finden Sie in meinem Buch »Intrusion Detection und Prevention mit Snort 2 & Co.« das ebenfalls im Addison-Wesley Verlag erschienen ist.

7.1 Intrusion-Detection-Systeme

Die Intrusion Detection versucht, Einbrüche und Missbrauch zu erkennen und zu melden. Hierzu versuchen die verschiedenen Systeme, sowohl das Netzwerk als auch die Rechner auf Anzeichen eines Angriffs, Einbruchs oder Missbrauchs zu analysieren und im Zweifel einen Alarm auszulösen. Achtung: Die Intrusion Detection verhindert nicht den Einbruch. Sie ist mit einem Feuermelder in einem Haus vergleichbar. Wenn keine Reaktion auf den Feueralarm erfolgt, wird das Haus trotz des Alarms niederbrennen. Für ein erfolgreiches Intrusion-Detection-Konzept ist es erforderlich, dass die Meldungen analysiert und anschließend Reaktionen eingeleitet werden.

Die Intrusion-Detection-Systeme werden allgemein in zwei Gruppen eingeteilt:

- Netzwerkbasierte IDS (NIDS)
- Hostbasierte IDS (HIDS)

Die NIDS beziehen ihre Daten aus dem Netzwerk. Sie analysieren jedes Paket und jede Netzwerkverbindung auf ihre Gültigkeit, auf Angriffsmuster und auf das Vorhandensein von Signaturen bekannter Angriffe. NIDS kämpfen heute vor allem mit zwei Problemen.

1. Die LANs werden immer schneller und transportieren immer mehr Daten. Für die Realisierung dieser LANs wird daher meist eine Paket-Switching-Technologie eingesetzt, die es nicht mehr jedem Rechner im Netzwerk erlaubt, den gesamten Verkehr zu beobachten. Daher müssen NIDS über spezielle Network-Taps oder Spanning-Ports angeschlossen werden. Gleichzeitig sollen die NIDS aber mehrere Systeme, meist ganze Netze, überwachen. Das bedeutet, dass die NIDS heute mit 1-Gbit/s- oder 10-Gbit/s-Verkehr umgehen müssen. Die Anforderungen an die Hardware sind enorm. Meist kann übliche Hardware diese Anforderungen nicht erfüllen und spezielle prozessorunterstützte Netzwerkkarten sind erforderlich.

2. Die wesentlichen Funktionen des NIDS werden immer noch signaturbasiert erreicht. Auch wenn die Signaturen der modernen IDS wie Snort wesentlich besser geworden sind, besteht dennoch die Problematik, dass meist nur für bekannte Angriffe Signaturen existieren. Eine komplette Überprüfung sämtlicher Applikationsprotokolle ist häufig zu aufwändig.

Bei den HIDS gibt es wesentlich mehr Variabilität. Es existieren viele verschiedene Technologien, die ihre Daten von einem Host beziehen und auf unterschiedlichste Weise versuchen, einen Einbruch zu erkennen. Die bekanntesten sind Werkzeuge wie Tripwire, Aide oder Samhain. Hierbei handelt es sich um File Integrity Verifier (auch als System Integrity Assessment bezeichnet). Diese analysieren ein System und melden Änderungen der überwachten Dateien. Sie müssen dann entscheiden, ob die Modifikation der Datei erlaubt war oder ob dies auf eine nicht autorisierte Handlung hinweist. Nachdem Tripwire lange Zeit die am häufigsten eingesetzte Applikation war, kann Samhain seit einigen Jahren eine steigende Zahl an Benutzern vorweisen. Sehr intelligente Funktionen machen es möglich, mit Samhain mehrere Systeme gleichzeitig zentral zu überwachen. Dies ist mit der Open-Source-Variante von Tripwire nicht möglich.

Andere HIDS überwachen die Anzahl der Prozesse, die angemeldeten Benutzer oder den Speicherverbrauch und melden hier ungewöhnliche Zustände. Systeme wie Logwatch oder Logsurfer analysieren die Protokolldateien und erkennen unbekannte Meldungen, die sie anschließend melden. Der Administrator muss nun wieder entscheiden, ob die Meldung harmlos ist oder auf einen Einbruch hinweist.

Da das Thema dieses Buches der Aufbau von Firewalls ist und von mir zum Thema Intrusion Detection bereits ein Buch im Addison-Wesley Verlag (»Intrusion Detection und Prevention mit Snort 2 & Co.«, ISBN 3-8273-2134-4) erschienen ist, möchte ich für weitere Informationen auf diesen Titel verweisen.

Achtung

Bei allem Hype um Intrusion-Detection-Systeme sollten Sie nie vergessen, dass ein Intrusion-Detection-System nie gute Systemadministration, gutes Patchmanagement und eine gute Firewall ersetzen kann. Außerdem vereinfacht ein IDS nicht die weitere Administration, sondern erhöht den Aufwand, da die Meldungen des IDS analysiert und ausgewertet werden müssen. Denken Sie an den Feuermelder, den niemand hört!

7.2 Intrusion-Prevention-Systeme

Im Juni 2003 erklärte die Beratungsfirma Gartner, dass IDS bis zum Jahr 2005 überflüssig werden würden. Dies führte zu viel Verwirrung bei den führenden Anbietern von IDS und ihren potenziellen Kunden. Gartners Schlüsselaussage war, dass Firmen in Zukunft mehr Geld in ihre Firewalls investieren würden, um Angriffe abzuwehren, anstatt in IDS, um die erfolgreichen Einbrüche zu melden.

Diese Aussage weist eine gewisse Logik auf. Jedoch existierten kaum Firewalls, die die Angriffe abwehren können, die ein Intrusion-Detection-System erkennen kann. Die Hersteller von IDS sahen hier ein neues Geschäftsfeld. Die Intrusion Prevention war geboren.

Ein Network-Intrusion-Prevention-System (NIPS) ist die aktive und intelligente Kombination aus Firewall und IDS. Dabei wird der Verkehr von der Firewall gefiltert, und bestimmte Protokolle werden zusätzlich von dem IDS analysiert. Sobald das IDS einen Angriff erkennt, erlaubt die Firewall nicht die Weiterleitung des Netzwerkpakets. Jeder namhafte Hersteller hat seit einigen Jahren NIPS-Produkte in seinem Portfolio.

Genauso haben die Anbieter von HIDS die Entwicklung von Host-Intrusion-Prevention-Systemen begonnen. Diese erkennen zum Beispiel den Versuch einer Dateimodifikation und verhindern diesen direkt. Zusätzlich kann der betroffene Benutzer gleichzeitig abgemeldet werden, können erneute Anmeldungen unterbunden werden oder ähnliche Maßnahmen von dem HIPS eingeleitet werden.

Ein HIPS kann Prozesse beenden oder dafür sorgen, dass ein Prozess immer läuft. Sobald ein bestimmter Prozess versucht, andere unautorisierte Prozesse zu starten (zum Beispiel eine Shell), kann der Prozessaufruf unterbunden werden oder sogar der Elternprozess beendet werden.

Die größte Schwäche dieser IPS sind falsch-positive Angriffserkennungen. Während dies bei einem IDS ärgerlich ist und mit Fine-Tuning recht gut in den Griff zu bekommen ist, ist dies bei einem IPS unverzeihlich. Die Netzwerkverbindung oder der Zugriff auf eine Datei werden effektiv unterbunden. Falls gerade wichtige, nicht wiederherstellbare Daten transportiert oder gespeichert werden sollen, kann ein IPS hohe Verluste erzeugen.

Wenn die Intrusion-Prevention-Systeme in Zukunft zielsicherer werden und die Gefahr falsch-positiver Erkennung zurückgeht, stellen sie eine sinnvolle Ergänzung einer Firewall dar. Wenn Sie heute bereits mit derartigen Systemen experimentieren möchten, empfehle ich Ihnen mein Buch »Intrusion Detection und Prevention mit Snort 2 & Co.« aus dem Addison-Wesley Verlag.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

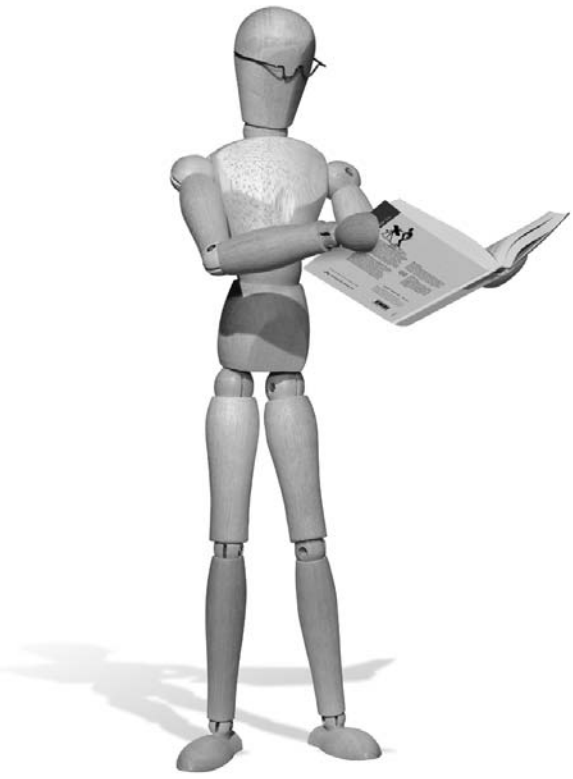
ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Teil III

Typische Firewall-Konfigurationen



8 Eine lokale Firewall

Im letzten Kapitel haben wir uns mit einer typischen Firewall beschäftigt. Dabei handelte es sich um einen Router, der sämtliche Pakete, die durch ihn weitergeleitet wurden, gefiltert hat. Viele Anwender vergessen jedoch, dass die kompletten Firewall-Funktionalitäten auch auf jedem anderen Linux-System vorhanden sind. Sie können die Firewall-Funktionen also auch lokal nutzen, um Ihr System vor den Zugriffen anderer Benutzer im lokalen Netz zu schützen. Das ist insbesondere interessant, wenn es sich beim Rechner um einen Standalone-Rechner handelt. Das kann zum Beispiel ein Root-Server bei einem Provider sein oder ein DNS-Server, der relativ ungeschützt in einer demilitarisierten Zone (DMZ) steht.

Dieses Kapitel zeigt Ihnen, wie Sie die Firewall einrichten, so dass Ihre lokalen Dienste geschützt werden.

8.1 Wieso eine lokale Firewall?

Wieso sollten Sie eine lokale Firewall einrichten, wenn Sie doch schon Ihr Netzwerk mit einer Firewall gesichert haben? Wie bereits in der Einführung erwähnt, können Sie bei einigen Rechnern (z.B. Root-Servern) gar keinen Einfluss auf die zentrale Firewall des Netzes nehmen. Auch Systeme in einer DMZ sind meist nicht ganz so gut geschützt. Zumindest untereinander werden sie häufig nicht noch einmal von einer Firewall getrennt. Auch wenn Sie über eine zentrale Firewall verfügen, möchten Sie vielleicht spezielle Rechner (z.B. Datenbankserver) zusätzlich vor den anderen Rechnern durch eine Firewall schützen. Im Zeitalter der Viren und Trojaner kann dies die Rettung für derartige Systeme darstellen.

Im Windows-Desktop-Bereich haben sich lokale Firewalls seit einiger Zeit etabliert. Obwohl man unterschiedlicher Meinung über diese Firewall-Systeme sein kann (siehe den Exkurs Windows-Desktop-Firewalls), haben diese Systeme einige nicht zu unterschätzende Vorteile.

Exkurs: Windows-Desktop-Firewalls

Die ersten Windows-Desktop-Firewalls erschienen für Windows 9x und ME. Während diese Systeme eine scheinbare Sicherheit vorgaukelten, konnten sie diese in Wirklichkeit nicht bieten. Da diese Windows-Betriebssysteme nicht das Benutzer/Rechte-Konzept kennen, gibt es auf diesen Betriebsystemen keine Möglichkeit, den Firewall-Prozess besonders zu schützen. Sobald der Benutzer

ein Programm aufruft, kann dieses Programm mit den Rechten des Benutzers die Firewall beenden, entfernen und umkonfigurieren. Einen Schutz können diese Programme also erst bieten, sobald der normale Benutzer keinerlei Zugriff mehr auf die Administration der Firewall hat. Dies ist erst ab Windows NT möglich. Hier kann eine Firewall mit Administratorrechten installiert und konfiguriert werden. Solange anschließend der Benutzer nicht mit Administratorrechten arbeitet, kann so verhindert werden, dass der Benutzer oder ein von ihm aufgerufenes Programm die Firewall abschaltet.

Dennoch stehe ich weiterhin derartigen Systemen auf dem Windows-Desktop kritisch gegenüber. Sie kennen das Phänomen vielleicht auch: Sie haben einen Bekannten, der einen Windows-Desktop benutzt und seit einer Woche eine derartige Firewall installiert hat. Anschließend fragt er Sie bei jedem Treffen (denn Sie haben ja Ahnung von Rechnern), warum er denn so häufig angegriffen werde, ob die Angriffe gefährlich seien und dass er ja früher vollkommen ungeschützt gewesen sei. Möglicherweise ist der Bekannte aber auch so verängstigt, dass er den Rechner gar nicht mehr verwendet.

Viele Desktop-Firewall-Produkte erzeugen jedes Mal ein Popup-Fenster, sobald ein beliebiger Zugriff auf den Rechner erfolgt. Bei einem Portscan öffnen manche Firewalls schneller die Popup-Fenster, als der Anwender sie schließen kann. Während ein derartiger Portscan vollkommen ungefährlich ist, suggeriert die Firewall einen gefährlichen Angriff. Denken Sie daran: Wo kein Dienst angeboten wird, kann ein Angreifer auch in keinen Dienst einbrechen[1].

Eine sehr schöne Funktion einer derartigen Desktop-Firewall ist jedoch die Möglichkeit nachzuvollziehen, ob und welche Software gerade einen Zugriff auf das Internet durchführt. So können Sie mit einer Desktop-Firewall bei entsprechendem Wissen recht einfach Spyware und Trojaner erkennen.

Meiner Meinung nach ist der wichtigste Vorteil einer lokalen Firewall die Möglichkeit zu entscheiden, welcher Prozess eine Kommunikation mit dem Netzwerk führen darf. Da die Firewall auf demselben System installiert ist, auf dem auch der Prozess läuft, kann Iptables diesen Zusammenhang nutzen, um Pakete zu erlauben. So können Sie zum Beispiel auf einem DNS-Server nur dem Prozess `named` die Erlaubnis geben, Pakete zu versenden.

[1] Wir vernachlässigen hier einmal die Gefahr eines Einbruchs in den Kernel des Betriebssystems selbst.

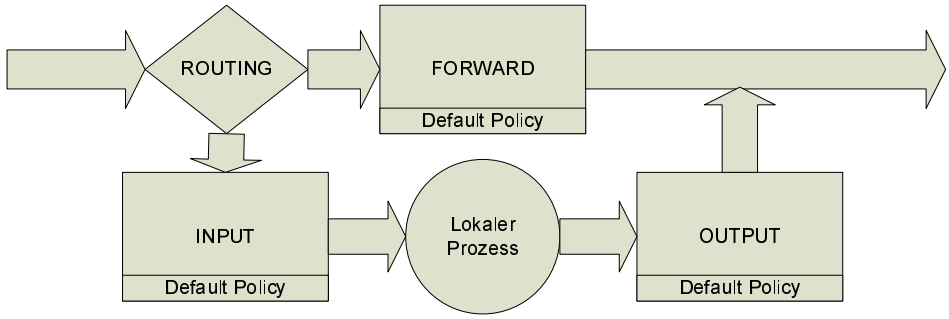


Abbildung 8.1: Für die Filterung der lokalen Pakete sind die INPUT- und OUTPUT-Ketten zuständig.

8.2 Die Ketten

Während auf einer Firewall, die als Router fungiert, vor allem die FORWARD-Kette der Filtertabelle betrachtet werden muss, sind für eine lokale Firewall die Ketten INPUT und OUTPUT der Filtertabelle interessant (siehe Abbildung 8.1).

Jedes Paket von außen wird in der INPUT-Kette gefiltert. Jedes Paket, das auf dem System erzeugt wird und den Rechner verlässt, wird in der OUTPUT-Kette gefiltert.

Wenn Sie möchten, dass ein System nur Verbindungen nach außen öffnen darf, dass aber keine Verbindungen von außen aufgebaut werden dürfen, können Sie folgende Regeln verwenden:

Listing 8.1: Diese lokale Firewall erlaubt alle ausgehenden Verbindungen.

```
# (1) Verwerfe alle nicht explizit akzeptierten Pakete
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP

# (2) Lösche alle Regeln in den INPUT- und OUTPUT-Ketten
$IPTABLES -F INPUT
$IPTABLES -F OUTPUT

# (3) Erlaube neue Verbindungsaufbauten nach außen
$IPTABLES -A OUTPUT -m state --state NEW -j ACCEPT

# (4) Erlaube Antwortpakete und Fehlermeldungen für aufgebaute Verbindungen
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# (5) Erlaube aufgebaute Verbindungen nach außen
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Die Regeln haben die folgende Aufgabe:

1. Zunächst werden die Grundregeln (Policies) der Ketten INPUT und OUTPUT auf DROP gesetzt. Damit wird jedes Paket, das nicht explizit durch eine Regel akzeptiert wird, verworfen.
2. Dies löscht alle vorhandenen Regeln in den Ketten INPUT und OUTPUT. Damit ist sichergestellt, dass die anschließend eingefügten Regeln die einzigen Regeln in diesen Ketten sind.
3. Diese Regel erlaubt Pakete in der OUTPUT-Kette, wenn sie eine neue Verbindung aufbauen. Das bedeutet, dass eine derartige Verbindung noch nicht in der Zustandstabelle enthalten sein darf. Damit wird also das erste Paket einer jeden Verbindung erlaubt.
4. Mit dieser Regel werden die Antwortpakete (`ESTABLISHED`) anderer Rechner akzeptiert, wenn in der Verbindungstabelle (Connection Tracking-Table, `/proc/net/ip_conntrack`) eine passende Verbindung gefunden wird. Außerdem akzeptiert diese Regel Fehlermeldungen, wenn sie eine der Verbindungen in der Verbindungstabelle betreffen (`RELATED`).
5. Diese letzte Regel wird gern vergessen. Jedoch funktioniert ohne sie nichts. Diese Regel akzeptiert alle weiteren lokal erzeugten Pakete, die zu einer aufgebauten Verbindung gehören. Die Regel Drei erlaubt nur das eine Paket zum Verbindungsaufbau. Alle weiteren Pakete werden von der Regel Drei nicht mehr akzeptiert, da nun die Verbindung bekannt ist und die Pakete nicht mehr den Status `NEW` aufweisen. Alle weiteren lokal erzeugten Pakete einer Verbindung besitzen den Status `ESTABLISHED`. Mit den `RELATED`-Paketen werden auch Fehlermeldungen akzeptiert, die sich auf diese Verbindungen beziehen. Wenn diese Regel fehlt, erfolgt ein Verbindungsaufbau, der angesprochene Rechner antwortet, und die Antwort erreicht auch den lokalen Prozess, aber jedes weitere Paket des lokalen Prozesses wird verworfen.

Natürlich können Sie auch den Zugriff auf bestimmte Dienste einschränken. Dabei sollten Sie aber nicht vergessen, dass Ihr System für seine Funktion bestimmte Dienste grundsätzlich benötigen kann. Hierbei handelt es sich zum Beispiel um DHCP, DNS oder NTP. Wenn Ihre Firewall diese Dienste dann nicht erlaubt, ist ein einwandfreies Arbeiten des Systems nicht möglich. Die Funktion dieser Dienste und Ihre Filterung mit Iptables wird in einem eigenen Kapitel (siehe Kapitel 32) behandelt. Hier soll nur exemplarisch der Aufbau eines derartigen Regelwerks besprochen werden.

Stellen Sie sich vor, Sie möchten auf Ihrem Client lediglich zwei Dienste nutzen: DNS für die Namensauflösung und HTTP zum Surfen im Internet. Ihre lokale Firewall soll daher nur den Zugriff auf diese beiden Dienste erlauben. Sie könnten hierfür folgende Regeln nutzen:

Listing 8.2: Diese lokale Firewall erlaubt nur den Zugriff auf DNS und HTTP.

```
# (1) Verwerfe alle nicht explizit akzeptierten Pakete
$IPTABLES -P INPUT DROP
```

```
$IPTABLES -P OUTPUT DROP

# (2) Lösche alle Regeln in den INPUT- und OUTPUT-Ketten
$IPTABLES -F INPUT
$IPTABLES -F OUTPUT

# (3a) Erlaube neue DNS-Anfragen
$IPTABLES -A OUTPUT -p udp --dport 53 -m state --state NEW -j ACCEPT
$IPTABLES -A OUTPUT -p tcp --dport 53 -m state --state NEW -j ACCEPT

# (3b) Erlaube neue HTTP-Verbindungen
$IPTABLES -A OUTPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT

# (4) Erlaube Antwortpakete und Fehlermeldungen für aufgebaute Verbindungen
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# (5) Erlaube aufgebaute Verbindungen nach außen
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Zunächst ist der Aufbau der Regeln wieder identisch mit dem ersten Ansatz. Die Regeln unterscheiden sich nur in dem Punkt 3. Während wir in dem ersten Ansatz (Listing 8.1) jede neue ausgehende Verbindung erlaubt haben, werden hier die möglichen Verbindungen stark eingeschränkt. Zunächst erlaubt der Punkt 3a die DNS-Anfrage. Hier müssen Sie die DNS-Anfrage sowohl mit dem UDP- als auch mit dem TCP-Protokoll erlauben. DNS ist ein wenig ungewöhnlich. Es stellt zunächst immer die Anfrage in UDP. Können jedoch mit UDP nicht alle Daten übertragen werden, stellt der Client die Anfrage erneut mit TCP. Weitere Informationen finden Sie im Abschnitt 32.2. Der Punkt 3b erlaubt dann neue HTTP-Verbindungen. Da die Pakete mit dem Zustand neu in der OUTPUT-Kette akzeptiert werden, ist nicht der Aufbau neuer Verbindungen von außen möglich. Der Rest der Regeln gleicht wieder dem ersten Ansatz.

Achtung

Wenn Sie derart eine lokale Firewall aufsetzen, sollten Sie nie vergessen, dass auch lokale Prozesse untereinander über ein lokales Netz kommunizieren. Sobald die lokalen Prozesse Internet-Sockets[2] und nicht Unix-Sockets nutzen, werden hierbei auch Pakete erzeugt, die in der OUTPUT- und INPUT-Kette gefiltert werden. Wenn Sie nicht spezielle Regeln vorsehen, die diese Pakete akzeptieren, unterbinden Sie die lokale Kommunikation. Viele Dienste funktionieren dann nicht mehr!

[2] Ein Unix-Socket ist eine lokale Datei im Verzeichnisbaum, die für die Kommunikation genutzt wird. Ein Beispiel ist `/dev/log`. Netzwerkverbindungen nutzen Internet-Sockets. Diese können auch von lokalen Prozessen für die lokale Kommunikation genutzt werden. Wenn Sie den Befehl `telnet localhost` aufrufen, kommunizieren Sie über einen derartigen Internet-Socket.

Dieser Regelsatz genügt jedoch meist nicht. Häufig existieren lokal genutzte Dienste wie eine grafische Oberfläche, die ebenfalls Netzwerkfunktionen nutzt. Damit diese Dienste auch weiterhin funktionieren, müssen Sie sicherstellen, dass deren Netzwerkpakete von Ihrer Firewall nicht verworfen werden. Die Firewall akzeptiert im Moment aber nur DNS- und HTTP-Verbindungen. Am einfachsten fügen Sie zu Beginn folgende Regeln grundsätzlich Ihren Firewall-Skripten hinzu:

```
# Akzeptiere den lokalen Verkehr
$IPTABLES -A INPUT -i lo -j ACCEPT
$IPTABLES -A OUTPUT -o lo -j ACCEPT
```

Diese Regeln akzeptieren den gesamten Verkehr, der über das Loopback-Device `lo` abgewickelt wird. Dies ist ein virtuelles Interface, das den gesamten lokalen Verkehr transportiert. Von außen ist kein Zugriff auf dieses Interface möglich. Daher stellt eine Akzeptanz des gesamten Verkehrs auf diesem Interface normalerweise auch kein Sicherheitsproblem dar.

Hinweis

Wenn auf Ihrem System mehrere Benutzer arbeiten, deren Netzwerkverkehr auch untereinander überwacht werden soll, dürfen Sie natürlich nicht den Verkehr blind akzeptieren. Dieses Szenario ist aber recht selten. Wenn Sie in Ihrer Firewall dieses Szenario implementieren wollen, lesen Sie bitte noch den nächsten Abschnitt über den Owner-Match. Dieser wird Ihnen die Arbeit erheblich vereinfachen.

Sie sollten nun bereits die Mächtigkeit der lokalen Firewall erkannt haben. Noch wichtiger wird die lokale Firewall, wenn Sie auf einem ansonsten ungeschützten System die Dienste schützen möchten. Auch hier können Sie eine lokale Firewall nutzen. Nur werden hier die neuen Verbindungen von außen aufgebaut. Sie können aber entscheiden, mit welchem Protokoll auf welchen Port Sie die Verbindung erlauben. Wenn Sie zum Beispiel einen Root-Server betreiben und sich auf diesem System sowohl ein Webserver als auch ein SSH-Server befinden, können Sie die folgenden Regeln nutzen:

Listing 8.3: Die lokale Firewall schützt einen Root-Server.

```
# (1) Verwerfe alle nicht explizit akzeptierten Pakete
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP

# (2) Lösche alle Regeln in den INPUT- und OUTPUT-Ketten
$IPTABLES -F INPUT
$IPTABLES -F OUTPUT

# (3) Akzeptiere den lokalen Verkehr
```

```
$IPTABLES -A INPUT -i lo -j ACCEPT
$IPTABLES -A OUTPUT -o lo -j ACCEPT

# (4a) Erlaube neue SSH-Verbindungen von außen
$IPTABLES -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT

# (4b) Erlaube neue HTTP-Verbindungen von außen
$IPTABLES -A INPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT

# (5) Erlaube Antwortpakete und Fehlermeldungen für aufgebaute Verbindungen
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# (6) Erlaube aufgebaute Verbindungen nach außen
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Den Großteil der Regeln kennen Sie bereits. Die meisten Regeln wurden nicht verändert. Hier nochmal ihre Funktion in aller Kürze:

1. Hier werden die Grundregeln für die Ketten INPUT und OUTPUT auf DROP gesetzt.
2. Hier werden alle möglicherweise vorhandenen Regeln in den Ketten INPUT und OUTPUT gelöscht.
3. Diese Regeln akzeptieren den gesamten lokalen Verkehr auf dem Loopback-Interface.
4. Die Punkte 4a und 4b erlauben schließlich neue SSH- und HTTP-Verbindungen von außen.
5. Diese Regel erlaubt alle Pakete ab dem zweiten Paket in einer aufgebauten Verbindung von außen.
6. Diese Regel schließlich erlaubt es, dass der lokale Rechner auf die von außen aufgebauten Verbindungen reagieren darf.

Mit einem derartigen Firewall-Skript können Sie sicherstellen, dass von außen nur die von Ihnen gewünschten Dienste auf dem System genutzt werden dürfen, unabhängig von den installierten und gestarteten Diensten. Die lokale Nutzung der installierten Dienste ist davon aber nicht betroffen.

Wenn Sie zusätzlich den Zugriff einschränken möchten und immer von einer bestimmten IP-Adresse auf den SSH-Server zugreifen, können Sie dies durch eine einfache Änderung der Regel 4a erreichen:

```
REMOTE_ACCESS=3.0.0.1

# (4a) Erlaube neue SSH-Verbindungen von außen
$IPTABLES -A INPUT -p tcp -s $REMOTE_ACCESS --dport 22 -m state --state NEW -j ACCEPT
```

Mit der Option `-s` definieren Sie, dass nur neue SSH-Verbindungen von dieser Source-IP-Adresse akzeptiert werden!

8.3 Der Owner-Match

Sie haben jetzt bereits sehr mächtige lokale Firewalls aufgebaut, die nur den Zugriff auf bestimmte Dienste zugelassen haben. Sie können diese weiter verbessern, indem Sie den Owner-Match einsetzen. Hierbei handelt es sich um eine Iptables-Option, die Sie in der OUTPUT-Kette nutzen können. Diese Option erlaubt es festzustellen, welcher Benutzer oder welche Gruppe ein Paket erzeugt hat. Dies ist jedoch nur in der OUTPUT-Kette möglich, da Iptables diese Funktion natürlich nur für lokal erzeugte Pakete anbieten kann. Zusätzlich kann diese Option auch die Prozessnummer oder die Sitzungsnummer zur Auswahl verwenden. Neue Versionen von Iptables können auch den Kommandonamen verwenden!

Die genaue Syntax des Owner-Match können Sie im Abschnitt 16.23 nachlesen. Hier werden Sie einige Beispielregeln sehen.

Ein einfaches erstes Beispiel wird Ihnen die Möglichkeiten des Owner-Matches verdeutlichen. Stellen Sie sich vor, Sie betreiben einen Terminalserver, auf dem mehrere Benutzer gleichzeitig arbeiten dürfen. Einige Benutzer haben das Recht, auf das Internet zuzugreifen, während anderen Benutzern dieser Zugriff verwehrt werden soll. Mit den normalen Mitteln können Sie dies nicht implementieren, da alle Benutzer dieselbe Source-IP-Adresse nutzen. Der Owner-Match macht es nun doch möglich. Sie können neue Verbindungen eines Benutzers zulassen und einen anderen Benutzer ablehnen:

```
# Benutzer Ralf hat die UID 500
$IPTABLES -A OUTPUT -m owner --uid-owner 500 -m state --state NEW -j ACCEPT

# Benutzer Otto hat die UID 501
$IPTABLES -A OUTPUT -m owner --uid-owner 501 -m state --state NEW -j REJECT
```

Wenn Sie darauf achten, dass Sie ansonsten alle ESTABLISHED- und RELATED-Pakete in der INPUT- und OUTPUT-Kette akzeptieren, wird nun der Benutzer Ralf auf das Internet zugreifen dürfen, während der Benutzer Otto das nicht darf. Dabei können Sie dem Benutzer Ralf auch nur bestimmte Befehle erlauben. Wenn der Benutzer Ralf nur Verbindungen mit dem Kommando `ssh` aufbauen darf, können Sie folgende Zeile verwenden:

```
# Benutzer Ralf hat die UID 500 und darf ssh benutzen
$IPTABLES -A OUTPUT -m owner --uid-owner 500 --cmd-owner ssh -m state --state NEW -j ACCEPT
```

Achtung

Allerdings müssen Sie diese Funktion mit Vorsicht genießen. Der Anwender kann sehr einfach versuchen, diese Funktion zu unterlaufen, da er einen beliebigen Befehl in sein Heimatverzeichnis unter dem Namen `ssh` kopieren und dort aufrufen kann.

Diese Funktion können Sie auch verwenden, um einen Server zusätzlich zu sichern. Wenn Sie zum Beispiel einen kombinierten Mail- und Webserver betreiben, so können Sie sicherstellen, dass lediglich der Mailserver Verbindungen nach außen aufbauen darf und der Webserver nur Verbindungen entgegennimmt. Sollte es einem Angreifer gelingen, in den Webserver-Prozess einzubrechen, so verfügt er nicht über die Möglichkeit, zusätzliche Angriffswerkzeuge aus dem Internet nachzuladen.

Listing 8.4: Nur der E-Mail-Server darf eine Verbindung nach außen aufbauen. Dem Webserver ist dies untersagt.

```
# Der Webserver hat die UID 48 (apache)
# Der E-Mail-Server hat die UID 89 (postfix)

# Der E-Mail-Server baut (mindestens) DNS- und SMTP-Verbindungen auf
$IPTABLES -A OUTPUT -m owner --uid-owner 89 -p udp --dport 53 -m state --state NEW -j ACCEPT
$IPTABLES -A OUTPUT -m owner --uid-owner 89 -p tcp -m multiport --dport 25,53 -m state↵
  --state NEW -j ACCEPT

# Der Webserver darf keine Verbindung aufbauen
$IPTABLES -A OUTPUT -m owner --uid-owner 48 -m state --state NEW -j REJECT
```

Die in diesem Regelsatz verwendete Option `multiport` erlaubt die gleichzeitige Angabe von bis zu 15 UDP- oder TCP-Ports. So können mehrere Regeln zu einer zusammengefasst werden und kann die Lesbarkeit erhöht werden. Weitere Hinweise zu `multiport` finden Sie im Abschnitt 16.22.

Zum Abschluss möchte ich Ihnen noch ein komplettes Beispielskript für einen Root-Server vorschlagen. Sie können es entsprechend Ihren Wünschen natürlich anpassen:

Listing 8.5: Dieses Firewall-Skript schützt einen typischen Root-Server.

```
#
#
# Firewall-Skript für einen Root-Server
# (c) Ralf Spenneberg 15. Juni 2005
#
```

```
# Dieser Root-Server bietet die folgende Dienste
# HTTP   Port 80/tcp
# HTTPS  Port 443/tcp
# SMTP   Port 25/tcp
# IMAPS  Port 995/tcp
# DNS    Port 53/tcp und 53/udp
#
# Dieser Root-Server benötigt Zugriff auf
# DNS    Port 53/tcp und 53/udp
# NTP    Port 123/udp (Zeitsynchronisation)
# SMTP   Port 25/tcp  (zum Verschicken von E-Mail)
#
# Jeder lokale Dienst nutzt den lokalen DNS-Server zur Namensauflösung
# Keiner der Dienste versucht eigenständig, einen anderen DNS-Server zu erreichen

# Definiere Variablen
IPTABLES=/sbin/iptables
ECHO=/bin/echo
SYSCTL=/sbin/sysctl

$ECHO "Starte Firewall"

$ECHO "Setze Kernelparameter"
$SYSCTL -w net.ipv4.tcp_syncookies=1
$SYSCTL -w net.ipv4.icmp_echo_ignore_broadcasts=1

$ECHO "Setze Regeln"
# Setze die Default-Policy auf DROP
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP

# Akzeptiere Verkehr auf der Loopback-Schnittstelle
$IPTABLES -A INPUT -i lo -j ACCEPT
$IPTABLES -A OUTPUT -o lo -j ACCEPT

# Akzeptiere eingehende Verbindungen für SMTP, DNS, HTTP, HTTPS und IMAPS
$IPTABLES -A INPUT -p tcp -m multiport --dport 25,53,80,443,995 -m state↵
  --state NEW -j ACCEPT
$IPTABLES -A INPUT -p udp --dport 53 -m state --state NEW -j ACCEPT

# Ausgehende Verbindungen

# Der DNS-Server baut Verbindungen als Benutzer named auf
UID=$(id -u named)
```

```
$IPTABLES -A OUTPUT -p udp --dport 53 --m owner --uid-owner $UID -m state↵
  --state NEW -j ACCEPT
$IPTABLES -A OUTPUT -p tcp --dport 53 --m owner --uid-owner $UID -m state↵
  --state NEW -j ACCEPT

# Der NTP-Server baut Verbindungen als Benutzer ntp auf
UID=$(id -u ntp)
$IPTABLES -A OUTPUT -p udp --dport 123 --m owner --uid-owner $UID -m state↵
  --state NEW -j ACCEPT

# Der SMTP-Server baut Verbindungen als Benutzer postfix auf
UID=$(id -u postfix)
$IPTABLES -A OUTPUT -p tcp --dport 25 --m owner --uid-owner $UID -m state↵
  --state NEW -j ACCEPT

# Alle bereits aufgebauten Verbindungen sollen erlaubt werden
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

$ECHO "Firewall erfolgreich gestartet"
```

Tipp

Wenn Sie das Skript auf mehreren Rechnern einsetzen wollen, kann es sein, dass der Benutzer `postfix` auf diesen Systemen eine unterschiedliche UID aufweist. Der Befehl `id -u postfix` ermittelt die aktuelle UID. So können Sie das Skript leichter auf weitere Systeme übertragen.

Dieses Skript sollte Ihnen genug Material für erste Experimente mit einer lokalen Firewall geben. Weitere Anregungen und Hinweise erhalten Sie in den fortgeschrittenen Kapiteln.

8.4 Kombination mit Gateway-Regeln

Sie werden nur in wenigen Umgebungen den idealen Fall antreffen, dass eine Firewall keinerlei eigene Dienste anbieten wird. In vielen Fällen wird mindestens noch ein SSH-Daemon für die Administration auf dem System installiert sein. In einigen Konstellationen wird sich auf der Firewall auch ein VPN-Produkt befinden, das einen VPN-Zugang in das interne Netz ermöglicht. Daher müssen Sie häufig auf einer klassischen Firewall, die als Gateway zwei Netze verbindet und den Verkehr kontrolliert, auch zusätzliche Regeln für die Filterung des lokalen Verkehrs vorsehen. Diese Regeln unterscheiden sich kaum von den bisher betrachteten Regeln,

jedoch sollten Sie zusätzlich die Tatsache berücksichtigen, dass die Firewall über mehrere Netzwerkkarten verfügt, die Sie beim Aufsetzen Ihrer Regeln berücksichtigen können und sollten.

Beginnen wir mit dem einfachen Fall, dass Sie auf Ihrer Firewall, die bereits mit einem kompletten Regelsatz ausgestattet ist (siehe Abschnitt 5.14), nun auch noch einen SSH-Server installieren und auf diesen von innen zugreifen möchten. Dies ist sehr einfach durch das Hinzufügen der folgenden Regeln an das Ende des vorhandenen Skripts möglich:

Listing 8.6: Ein Zugriff auf den SSH-Server soll von innen erlaubt werden.

```
# Erlaube SSH-Zugriff von innen
$IPTABLES -A INPUT -i $INTDEV -p tcp --dport 22 -m state --state NEW -j ACCEPT

# Erlaube alle bereits aufgebauten Verbindungen in der INPUT- und OUTPUT-Kette
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Diese Regeln nutzen die Variable `$INTDEV`, die Sie hoffentlich bereits in Ihrem Firewall-Skript definiert haben. Der Wert dieser Variablen entspricht der internen Netzwerkkarte. So können Sie sehr einfach nur SSH-Verbindungen von innen zulassen. Wenn Sie den Zugriff weiter einschränken möchten und zum Beispiel nur bestimmte Administrationsrechner von innen zugreifen lassen möchten, können Sie die folgenden Regeln verwenden:

```
# Adminrechner, Liste durch Leerzeichen getrennt
ADMIN="192.168.0.5 192.168.0.8 192.168.0.17"

# Erlaube den Adminrechnern SSH-Zugriff von innen
for PC in $ADMIN
do
  $IPTABLES -A INPUT -s $PC -i $INTDEV -p tcp --dport 22 -m state --state NEW -j ACCEPT
done
```

Exkurs: For-Schleife

Jede Shell bietet Ihnen Möglichkeiten der Prozesssteuerung und auch eine For-Schleife. Die For-Schleife der Bourne-Shell (und damit auch der Bash- und Korn-Shell) erlaubt dabei die Angabe einer Werteliste, die anschließend durchlaufen wird. Damit Sie einen Eindruck von der Funktion der For-Schleife erhalten, können Sie den folgenden Befehl auf der Kommandozeile aufrufen:

```
[spenneb@bibo ~]$ for i in eins zwei drei vier; do echo $i; done
eins
```

```
zwei
drei
vier
```

So können Sie sehr einfach einen Befehl wiederholt mit unterschiedlichen Werten aufrufen. In dem Iptables-Listing oben wird der Iptables-Befehl mehrfach mit unterschiedlichen Source-Adressen aufgerufen. So wird für jede Source-Adresse eine Regel hinzugefügt, die eine SSH-Verbindung erlaubt.

Tipp

Anstelle einer For-Schleife können Sie auch IP-Sets verwenden. Dies ist eine Weiterentwicklung des ehemaligen IP-Pools. Damit können Sie mehrere IP-Adressen in einer Regel verwenden. Leider unterstützen noch nicht alle Distributionen automatisch diese Funktion, und Sie müssen den Kernel und den Iptables-Befehl patchen. Weitere Informationen über diese Funktion finden Sie im Kapitel 25.

Möchten Sie entsprechend den SSH-Zugriff von außen erlauben, so ersetzen Sie in der Regel `-i $INTDEV` durch `-i $EXTDEV`.

Häufig wünschen die Administratoren und damit vielleicht auch Sie, Verbindungen von der Firewall in das Internet aufbauen zu können. Zumindest soll es möglich sein, von der Firewall zu Testzwecken mit dem Ping-Befehl die Konnektivität testen zu können. Das können Sie ganz einfach erreichen, in dem Sie die folgende Zeile hinzufügen:

```
# Erlaube Ping in das Internet
$IPTABLES -A OUTPUT -o $EXTDEV -p icmp --icmp-type echo-request -m state ↵
  --state NEW -j ACCEPT
```

Möchten Sie, dass die Firewall auch angepingt (echo-request) werden kann, um die Erreichbarkeit der Firewall sowohl von innen als auch von außen testen zu können, benötigen Sie noch die folgende Zeile:

```
# Erlaube, dass die Firewall per Ping getestet werden kann
$IPTABLES -A INPUT -p icmp --icmp-type echo-request -m state --state NEW -j ACCEPT
```

Alle diese Regeln benötigen natürlich für eine korrekte Funktion zusätzliche Regeln in der INPUT- und OUTPUT-Kette, die ESTABLISHED- und RELATED-Pakete akzeptieren.

Nun sollten Sie über das Rüstzeug verfügen, um ein Standalone-Linux-System mit einer Firewall zu schützen. Außerdem können Sie ein Firewall-Gateway so konfigurieren, dass Sie lokale Dienste auf der Firewall nutzen können und diese Firewall selbst auf weitere Dienste zugreifen darf.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

9 Aufbau einer DMZ

Eine demilitarisierte Zone (DMZ) ist ein eigenes Netzwerk, in das bestimmte Rechner ausgelagert werden, die einen unbeschränkteren Zugriff auf das Internet benötigen oder vom Internet erreicht werden sollen (z.B. Webserver). Dieser Aufbau einer demilitarisierten Zone bietet viele Vorteile. Wenn ein Angreifer erfolgreich in einen dieser Rechner einbrechen sollte, so hat er noch keinen Zugriff auf das immer noch geschützte interne LAN. Befände sich der Webserver nicht in der DMZ, sondern direkt im internen LAN, hätte der Angreifer Zugriff auf alle Systeme!

Dieses Kapitel beschreibt den Aufbau einer DMZ, zeigt unterschiedliche Architekturen und beispielhaft den Aufbau der Firewall-Skripten, um diese zu implementieren.

9.1 DMZ-Architekturen

Bereits im Kapitel 3, »Firewall-Architekturen« haben wir verschiedene Möglichkeiten angesprochen, eine DMZ zu implementieren. Dabei wurden auch Vor- und Nachteile der verschiedenen Varianten erörtert. Im Folgenden soll die Implementierung einer DMZ als drittes Bein eines Paketfilters (Abbildung 3.2) und als Netz zwischen zwei Paketfiltern (Abbildung 3.3) exemplarisch durchgespielt werden. Während die Implementierung als drittes Bein einen relativ geringen Hardwareaufwand bedeutet, benötigt die Variante mit zwei Paketfiltern mindestens ein System als Paketfilter mehr. Dies bedeutet Geld-, Platz- und Kühlaufwand.

In der DMZ der Beispielfirma *Nohup.info* soll jeweils ein Web-, ein E-Mail, ein cachender DNS- und ein Proxy-Server betrieben werden. Diese Systeme erhalten private IP-Adressen aus dem Bereich 192.168.255.0/24. Dabei soll aus dem Internet ein Zugriff auf den Web- und den E-Mail-Server möglich sein. Aus dem internen Netz ist ein Zugriff auf den Proxy- und den E-Mail-Server notwendig. Der Zugriff auf den Webserver wird über den Proxy-Server realisiert. Ein direkter Zugriff auf das Internet ist nicht vorgesehen. Der Paketfilter erhält als externe IP-Adresse eine feste statische IP-Adresse 3.0.0.1. Alle Dienste werden im Internet unter dieser IP-Adresse angebunden. Das bedeutet, dass ein DNS-Server bei der Frage nach der Adresse `www.nohup.info` die IP-Adresse 3.0.0.1 zurückliefert.

9.2 Dreibeiniger Paketfilter mit DMZ

Die Variante des dreibeinigen Paketfilters zur Implementierung einer demilitarisierten Zone ist die einfachste Variante einer DMZ. Der Hardwareaufwand ist gering, denn Sie benötigen hierfür nur eine zusätzliche Netzwerkkarte in Ihrem Paketfilter. Auch der weitere technische Aufwand in Bezug auf Platz und Kühlung ist eher zu vernachlässigen, da Sie ja sowieso bereits ein System als Paketfilter einsetzen.

Falls Sie bereits ein Firewall-Skript für einen Paketfilter besitzen und dieses um die Funktionen für eine DMZ erweitern wollen, ist auch dies recht einfach machbar. In diesem Kapitel werden wir jedoch ein neues Skript entwickeln. Sie können die hier vorgestellten Vorschläge aber auch in jedes andere Skript übernehmen.

Zunächst sollten Sie die Netzwerkkarten zuordnen und in Ihrem Skript Variablen definieren, denen Sie die entsprechenden Werte zuweisen. Zusätzlich zu der Variable `INTDEV` und `EXTDEV` werden wir noch eine Variable `DMZDEV` verwenden. Dieser Variablen weisen Sie zunächst den Namen der Netzwerkkarte zu, über die die DMZ angebunden wird.

Listing 9.1: Eine dreibeinige Firewall mit DMZ-Anschluss

```
#!/bin/sh
#
# Autor  : Ralf Spenneberg
# Version: 0.1
# Datum  : 17. Dez 2004
#
# Dieses Skript lädt die Regeln für die Firewall

INTDEV="eth1"
# Achtung: Bei Einsatz von User-Mode-Linux lautet diese Variable
# INTDEV="tap0"

EXTDEV="eth0"

DMZDEV="eth2"

IPTABLES=/sbin/iptables
SYSCTL=/sbin/sysctl
```

Nun sollten Sie für die verschiedenen Dienste und Systeme Variablen definieren. Das erleichtert später die Wartung. Vielleicht installieren Sie zunächst nur ein System in der DMZ, das sowohl einen Web-, einen E-Mail- als auch einen Proxy-Server beherbergt. Später möchten Sie vielleicht den E-Mail-Server auf einem eigenen System betreiben. Wenn Sie zu Beginn darauf geachtet haben, für alle Systeme Variablen zu verwenden, müssen Sie diese anschließend nur entsprechend anpassen und Ihr Skript neu starten.

```
MAIL=192.168.255.2
WEB=192.168.255.3
DNS=192.168.255.4
PROXY=192.168.255.5
EXTERN=3.0.0.1
```

Tipp

Auch wenn in unserem Skript für den DNS-Server eine eigene IP-Adresse vorgesehen wurde, ist es natürlich nicht erforderlich, diesen auf eigener dedizierter Hardware zu installieren. Wenn Sie den DNS-Server auf derselben Hardware wie den Proxy-Server installieren wollen, verwenden Sie einfach für beide Variablen dieselbe IP-Adresse!

Nun sollten Sie, bevor Sie irgendwelche Regeln hinzufügen, einen sauberen Grundzustand erzeugen.

```
# Setze Default-Regeln
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP

# Lösche die Filter-Tabelle
$IPTABLES -F

# Lösche die NAT-Tabelle
$IPTABLES -t nat -F
```

Beginnen wir nun mit den NAT-Regeln. Insgesamt müssen wir die folgenden NAT-Regeln konfigurieren:

1. Der Proxy muss auf das Internet zugreifen können.
2. Der cachende DNS-Server muss auf das Internet zugreifen können.
3. Der -Server muss auf das Internet zugreifen können.
4. Das Internet muss auf den Webserver zugreifen können.
5. Das Internet muss auf den E-Mail-Server zugreifen können.

Diese Anforderungen können mit den folgenden vier Regeln umgesetzt werden:

```
# (1) Proxy-Zugriff
$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -s $PROXY -j SNAT --to-source $EXTERN
```

```
# (2) DNS-Zugriff
$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -s $DNS -j SNAT --to-source $EXTERN

# (3) Mailserver-Zugriff nach außen
$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -s $MAIL -j SNAT --to-source $EXTERN

# (4) Webserver-Zugriff von außen
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tcp -d $EXTERN -m multiport --dport 80,443 ↵
  -j DNAT --to-destination $WEB

# (5) Mailserver-Zugriff von außen
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tcp -d $EXTERN --dport 25 -j DNAT ↵
  --to-destination $MAIL
```

Die Regeln Eins bis Drei führen eine Network Address Translation (NAT) der Absenderadresse durch. Dabei wird die originale Absenderadresse des Proxy oder des Mailservers bei einem Verbindungsaufbau nach außen durch die Adresse der Firewall ersetzt. Die Regeln vier und fünf sorgen dafür, dass bei Verbindungen von außen, die auf den Ports 25, 80 und 443 aufgebaut werden, Pakete entsprechend auf den E-Mail- und Webserver in die DMZ weitergeleitet werden. Dies erfolgt durch einen Austausch der Ziel-IP-Adresse in der NAT-PREROUTING-Kette. Die Portnummer wird dabei nicht modifiziert. Da aber die Weiterleitung (Forwarding) in Abhängigkeit der Portnummer erfolgen soll, muss zusätzlich auch das Protokoll TCP angegeben werden.

Tipp

Wenn Sie aus bestimmten Gründen den Webserver in der DMZ auf einem anderen Port betreiben möchten, so wäre es auch möglich, die Portnummer zu modifizieren:

```
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tcp -d $EXTERN ↵
  --dport 80 -j DNAT --to-destination $WEB:8080
```

Die NAT-Regeln sind jedoch lediglich für die Adressumsetzung beim Zugriff aus dem Internet und in das Internet verantwortlich. Weitere Firewall-Regeln sind für die Funktion der Firewall erforderlich. Diese Regeln müssen nun auch den gewünschten Verkehr erlauben.

Wir benötigen zunächst eine Regel, die sämtliche aufgebauten Verbindungen und deren Fehlermeldungen akzeptiert:

```
# Akzeptiere alle aufgebauten Verbindungen
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Tipp

Denken Sie daran: Die Zustandsüberwachung der Iptables-Firewall macht es möglich, dass Sie immer nur die Verbindungsaufbauten filtern und anschließend alle ermaßen aufgebauten Verbindungen über eine einzige Regel akzeptieren. Nur Verbindungen, die Sie vorher explizit erlaubt haben (im Status NEW), werden von dieser Regel zugelassen. Der Aufbau der Regeln wird so wesentlich einfacher und übersichtlicher.

Nun benötigen wir eine Regel, um von innen auf den Proxy und den Mailserver zuzugreifen. Der Port eines Proxys ist nicht so festgelegt wie zum Beispiel der Port beim Zugriff auf einen Web- oder E-Mail-Server. Hier werden vollkommen unterschiedliche Portnummern verwendet. Der Squid-Proxy-Server verwendet zum Beispiel die Portnummer 3128/tcp als Standardport. Es ist sinnvoll, auch hierfür eine Variable zu Beginn des Skripts zu definieren: `PROXYPORT=3128`. Dann können Sie diese Variable in Ihren Regeln nutzen und müssen bei einer Änderung nur zu Beginn des Skripts Änderungen vornehmen.

```
# Erlaube den Zugriff auf den Proxy
$IPTABLES -A FORWARD -i $INTDEV -o $DMZDEV -d $PROXY -p tcp --dport $PROXYPORT -m state ↵
  --state NEW -j ACCEPT

# Erlaube den Zugriff auf den E-Mail-Server
$IPTABLES -A FORWARD -i $INTDEV -o $DMZDEV -d $MAIL -p tcp --dport 25 -m state ↵
  --state NEW -j ACCEPT
```

Tipp

Wenn der E-Mail-Server in der DMZ auch Dienste zum Abholen der E-Mail bereitstellt, müssen Sie die letzte Regel so erweitern, dass auch diese Funktion unterstützt wird. Das *Post Office Protocol* (POP-3) verwendet den Port 110, und das Internet Message Access Protocol (IMAP) verwendet den Port 143. Sinnvoller ist es aber, diese Dienste auf einem eigenen E-Mail-Server in dem internen Netz anzubieten und den E-Mail-Server in der DMZ nur als Relay zu nutzen. Dann können Sie natürlich auch den Zugriff auf den E-Mail-Server in der DMZ auf den internen E-Mail-Server beschränken, denn alle internen Anwender benutzen für ihren E-Mail-Zugriff nur den internen E-Mail-Server.

```
MAILINTERN=192.168.0.100
# Erlaube den Zugriff auf den E-Mail-Server
$IPTABLES -A FORWARD -i $INTDEV -o $DMZDEV -s $MAILINTERN -d $MAIL -p tcp ↵
  --dport 25 -m state --state NEW -j ACCEPT
```

Sobald eine E-Mail in das Internet gesendet werden muss, sendet der interne E-Mail-Server diese E-Mail an den E-Mail-Server in der DMZ, der sie in das Internet weiterleitet. Eingehende E-Mails nehmen den entgegengesetzten Weg. Der Aufbau eines derartigen E-Mail-Relays mit Postfix ist in dem Anhang Postfix-Mail-Relay (siehe Anhang A) erläutert.

Für diesen Rückweg ist dann natürlich auch noch eine weitere Regel erforderlich, die den Transport aus der DMZ in das interne Netz erlaubt:

```
# Erlaube den Transport von E-Mail aus der DMZ in das interne Netz
$IPTABLES -A FORWARD -i $DMZDEV -o $INTDEV -d $MAILINTERN -s $MAIL ↲
  -p tcp --dport 25 -m state --state NEW -j ACCEPT
```

Des Weiteren benötigen natürlich der E-Mail-Server, der DNS-Server und der Proxy einen Zugriff auf das Internet. Wenn kein eigener cachender DNS-Server in der DMZ betrieben werden soll, benötigen diese Systeme natürlich auch einen Zugriff auf einen DNS-Server in dem Internet.

```
# Erlaube dem DNS-Server einen Zugriff auf Nameserver im Internet
$IPTABLES -A FORWARD -i $DMZDEV -o $EXTDEV -s $DNS -p tcp --dport 53 -m state ↲
  --state NEW -j ACCEPT
$IPTABLES -A FORWARD -i $DMZDEV -o $EXTDEV -s $DNS -p udp --dport 53 -m state ↲
  --state NEW -j ACCEPT

# Erlaube dem Proxy Zugriff auf das Internet
$IPTABLES -A FORWARD -i $DMZDEV -o $EXTDEV -s $PROXY -p tcp -m multiport --dport 21,80,443 ↲
  -m state --state NEW -j ACCEPT

# Erlaube dem E-Mail-Server Zugriff auf das Internet
$IPTABLES -A FORWARD -i $DMZDEV -o $EXTDEV -s $MAIL -p tcp --dport 25 -m state --state NEW ↲
  -j ACCEPT
```

Wenn die Benutzer über den Proxy sowohl auf FTP-, HTTP- und HTTPS-Server zugreifen sollen, muss der Proxy auch auf entsprechende Ports zugreifen dürfen.

Achtung

Das FTP-Protokoll ist ein sehr kompliziertes Protokoll. Daher wird es in einem eigenen Abschnitt genauer betrachtet (siehe Abschnitt 32.10). Dieses Protokoll verwendet eine Steuerungsverbindung, die üblicherweise auf dem TCP-Port 21 terminiert wird, und zusätzlich für jede zu übertragende Datei eine eigene Datenverbindung, deren Ports dynamisch ausgehandelt werden. Da es sehr schwer ist, statische Regeln für derartig dynamisch ausgehandelte und damit

unbekannte Ports zu definieren, gibt es die Stateful-Inspection. Diese kann den Inhalt der Steuerungsverbindung mitlesen und die dynamisch ausgehandelten Ports erkennen. So können dann automatisch die ausgehandelten Datenverbindungen erlaubt werden. Sie müssen in Ihrem Skript dann nur noch die Steuerungsverbindung erlauben.

Damit das funktioniert, müssen Sie noch das Kernelmodul `ip_conntrack_ftp` laden:

```
MODPROBE=/sbin/modprobe
$MODPROBE ip_conntrack_ftp
```

Wenn Sie auf Ihrer Firewall auch NAT verwenden, ist zusätzlich auch noch das weitere Kernel-Modul `ip_nat_ftp` erforderlich:

```
$MODPROBE ip_nat_ftp
```

Diese Zeilen fügen Sie am besten zu Beginn Ihres Skripts ein. Alle beobachteten Datenverbindungen werden dann auch mit dem Zustand `RELATED` versehen. Da Sie derartige Pakete in der `FORWARD`-Kette bereits akzeptieren, werden diese Verbindungen erlaubt. Weitere Informationen über das FTP-Protokoll und die Kernelmodule erhalten Sie in Abschnitt 32.10.

Nun fehlt noch der Zugriff aus dem Internet auf den Webserver und den E-Mail-Server. Diese Zugriffe sind jetzt sehr einfach zu konfigurieren und erfolgen analog den bereits definierten Regeln. Der Zugriff erfolgt von außen auf die Systeme in der DMZ. Ein NAT wurde bereits konfiguriert. Es bleiben die folgenden Firewall-Regeln:

```
# Erlaube dem Internet den Zugriff auf den E-Mail-Server
$IPTABLES -A FORWARD -i $EXTDEV -o $DMZDEV -d $MAIL -p tcp --dport 25 -m state ↵
  --state NEW -j ACCEPT

# Erlaube dem Internet den Zugriff auf den Webserver
$IPTABLES -A FORWARD -i $EXTDEV -o $DMZDEV -d $WEB -p tcp -m multiport --dport 80,443 ↵
  -m state --state NEW -j ACCEPT
```

Grundsätzlich sollte nun die komplette Funktionalität des Skripts bereits gewährleistet sein. Sinnvollerweise werden jedoch noch ein paar Protokollregeln und Ausnahmen hinzugefügt.

Als Erstes sollten Sie sicherstellen, dass Anfragen auf dem Port 113/tcdp (identd) abgelehnt und nicht verworfen werden. Ansonsten kann es zu Verzögerungen beim Aufbau von FTP- und SMTP-Verbindungen kommen.

```
$IPTABLES -A INPUT -p tcp --dport 113 -j REJECT
```

Damit Ihre internen Benutzer auch nicht auf einen Timeout warten müssen, wenn die Benutzer ein nicht erlaubtes Protokoll verwenden möchten, macht es Sinn, Anfragen von innen, die abgelehnt werden sollen, nicht zu verwerfen, sondern zu protokollieren und abzulehnen. So behalten Sie immer den Überblick darüber, was Ihre Benutzer gerade treiben. Achten Sie jedoch auf die Datenschutzrichtlinien in Ihrem Unternehmen und die gesetzlichen Rahmenbedingungen.

```
$IPTABLES -A FORWARD -i $INTDEV -j LOG --log-prefix "Unerlaubt von innen: "
$IPTABLES -A FORWARD -i $INTDEV -j REJECT
$IPTABLES -A INPUT -i $INTDEV -j LOG --log-prefix "Unerlaubt von innen: "
$IPTABLES -A INPUT -i $INTDEV -j REJECT
```

Da Sie diese Regeln an das Ende der Kette hängen, werden sie nur die Pakete betreffen, die nicht im Vorfeld der Kette von Ihren Regeln akzeptiert wurden.

Möglicherweise möchten Sie eine entsprechende Regel auch für Verbindungen von außen aufsetzen. Je nach Ihrer Internetanbindung möchte ich jedoch von einer derartigen grundsätzlichen Regel abraten, da Sie wahrscheinlich nicht die Zeit haben werden, Protokolle mit mehreren zehntausend Einträgen pro Tag zu analysieren. Sehr aufschlussreich ist aber noch eine derartige Regel für Verbindungen aus der DMZ, die Sie nicht explizit in Ihren Regeln erlaubt haben. Damit sind Sie in der Lage, sehr früh Probleme in Ihrem Regelwerk oder auf Ihren Systemen in der DMZ zu erkennen.

```
$IPTABLES -A FORWARD -i $DMZDEV -j LOG --log-prefix "Unerlaubt aus der DMZ: "
$IPTABLES -A FORWARD -i $DMZDEV -j REJECT
$IPTABLES -A INPUT -i $DMZDEV -j LOG --log-prefix "Unerlaubt aus der DMZ: "
$IPTABLES -A INPUT -i $DMZDEV -j REJECT
```

Diese Regeln können ein Intrusion-Detection-System sehr gut komplettieren und bei der Analyse eines Angriffs oder Einbruchs sinnvolle zusätzliche Informationen bieten.

Damit sollte das Skript schließlich fertig sein. Sicherlich haben Sie noch Ideen und Wünsche, wie Sie das Skript erweitern können. Vielleicht haben Sie auch eine vierbeinige Firewall mit zwei DMZ. Dieses Skript sollten Ihnen dann aber eine gute Ausgangsposition für eigene Anpassungen geben. Im Folgenden ist das komplette Skript noch einmal zur Referenz abgedruckt.

Listing 9.2: Eine dreibeinige Firewall mit DMZ

```
#!/bin/sh
#
# Autor  : Ralf Spenneberg
# Version: 0.1
# Datum  : 17. Dez 2004
#
# Dieses Skript lädt die Regeln für die Firewall
INTDEV="eth1"
```

```
# Achtung: Bei Einsatz von User-Mode-Linux lautet diese Variable
# INTDEV="tap0"

EXTDEV="eth0"

DMZDEV="eth2"

IPTABLES=/sbin/iptables
SYSCTL=/sbin/sysctl
MODPROBE=/sbin/modprobe

MAIL=192.168.255.2
WEB=192.168.255.3
DNS=192.168.255.4
PROXY=192.168.255.5
PROXYPORT=3128
EXTERN=3.0.0.1

# Lade die Kernelmodule für die Stateful-Inspection des FTP-Protokolls
$MODPROBE ip_conntrack_ftp
$MODPROBE ip_nat_ftp

# Setze Default-Regeln
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP

# Lösche die Filter-Tabelle
$IPTABLES -F

# Lösche die NAT-Tabelle
$IPTABLES -t nat -F

## NAT-Regeln ##
# (1) Proxy-Zugriff
$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -s $PROXY -j SNAT --to-source $EXTERN
# (2) DNS-Zugriff
$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -s $DNS -j SNAT --to-source $EXTERN

# (3) Mailserver-Zugriff nach außen
$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -s $MAIL -j SNAT --to-source $EXTERN

# (4) Webserver-Zugriff von außen
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tcp -d $EXTERN -m multiport --dport 80,443
  -j DNAT --to-destination $WEB
```

```
# (5) Mailserver-Zugriff von außen
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tcp -d $EXTERN --dport 25 -j DNAT
  --to-destination $MAIL

## Firewall-Regeln
# Akzeptiere alle aufgebauten Verbindungen
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# Erlaube den Zugriff auf den Proxy
$IPTABLES -A FORWARD -i $INTDEV -o $DMZDEV -d $PROXY -p tcp --dport $PROXYPORT
  -m state --state NEW -j ACCEPT

# Erlaube den Zugriff auf den E-Mail-Server
$IPTABLES -A FORWARD -i $INTDEV -o $DMZDEV -d $MAIL -p tcp --dport 25 -m state
  --state NEW -j ACCEPT

### Bei Verwendung eines internen E-Mail-Servers:
# MAILINTERN=192.168.0.100
# Erlaube den Zugriff auf den E-Mail-Server
# $IPTABLES -A FORWARD -i $INTDEV -o $DMZDEV -s $MAILINTERN -d $MAIL -p tcp --dport 25
  -m state --state NEW -j ACCEPT
# Erlaube den Transport von E-Mail aus der DMZ in das interne Netz
# $IPTABLES -A FORWARD -i $DMZDEV -o $INTDEV -d $MAILINTERN -s $MAIL -p tcp --dport 25
  -m state --state NEW -j ACCEPT
###

# Erlaube dem DNS-Server einen Zugriff auf Nameserver im Internet
$IPTABLES -A FORWARD -i $DMZDEV -o $EXTDEV -s $DNS -p tcp --dport 53 -m state --state NEW
  -j ACCEPT
$IPTABLES -A FORWARD -i $DMZDEV -o $EXTDEV -s $DNS -p udp --dport 53 -m state --state NEW
  -j ACCEPT

# Erlaube dem Proxy den Zugriff auf das Internet
$IPTABLES -A FORWARD -i $DMZDEV -o $EXTDEV -s $PROXY -p tcp -m multiport --dport 21,80,443
  -m state --state NEW -j ACCEPT

# Erlaube dem E-Mail-Server den Zugriff auf das Internet
$IPTABLES -A FORWARD -i $DMZDEV -o $EXTDEV -s $MAIL -p tcp --dport 25 -m state --state NEW
  -j ACCEPT

# Erlaube dem Internet den Zugriff auf den E-Mail-Server
$IPTABLES -A FORWARD -i $EXTDEV -o $DMZDEV -d $MAIL -p tcp --dport 25 -m state --state NEW
  -j ACCEPT
```

```
# Erlaube dem Internet den Zugriff auf den Webserver
$IPTABLES -A FORWARD -i $EXTDEV -o $DMZDEV -d $WEB -p tcp -m multiport --dport 80,443
  -m state --state NEW -j ACCEPT

# Lehne Identd-Anfragen ab
$IPTABLES -A INPUT -p tcp --dport 113 -j REJECT

# Protokolliere alle anderen Anfragen von innen
$IPTABLES -A FORWARD -i $INTDEV -j LOG --log-prefix "Unerlaubt von innen: "
$IPTABLES -A FORWARD -i $INTDEV -j REJECT
$IPTABLES -A INPUT -i $INTDEV -j LOG --log-prefix "Unerlaubt von innen: "
$IPTABLES -A INPUT -i $INTDEV -j REJECT

$IPTABLES -A FORWARD -i $DMZDEV -j LOG --log-prefix "Unerlaubt aus der DMZ: "
$IPTABLES -A FORWARD -i $DMZDEV -j REJECT
$IPTABLES -A INPUT -i $DMZDEV -j LOG --log-prefix "Unerlaubt aus der DMZ: "
$IPTABLES -A INPUT -i $DMZDEV -j REJECT
```

In seiner jetzigen Form ist das Skript bereits durchaus lang und wahrscheinlich im ersten Moment auch für den einen oder anderen Administrator durchaus unübersichtlich. Im nächsten Abschnitt werden Sie sehen, wie diese Skripten lesbarer und wartbarer gestaltet werden können. Wir werden das Skript in Bezug auf seine Lesbarkeit und die Geschwindigkeit der Verarbeitung optimieren.

9.3 Optimierung mit benutzerdefinierten Ketten

Im letzten Abschnitt haben wir bereits ein recht umfangreiches Skript für eine dreibeinige Firewall mit DMZ entwickelt. Dieses Skript war bereits fast 100 Zeilen lang. Da das Skript für fast jede veränderliche Information (wie IP-Adressen) Variablen nutzt, ist eine weitere Wartung recht einfach. Dennoch ist es durchaus schwierig, einen Überblick zu behalten und den genauen Paketfluss nachzuvollziehen. Einfacher kann das geschehen, wenn Sie sich Ihre eigenen Ketten für jede Funktion erzeugen. Iptables bietet, wie früher schon Ipchains, die Möglichkeit, neue Ketten mit einem eigenen Namen zu definieren und diese dann mit Regeln zu füllen.

Diese benutzerdefinierte Kette weist mehrere Vorteile auf:

- Sie können durch eine sinnvolle Strukturierung der Regeln und anschließend durch eine entsprechende Auswahl der Ketten die Gesamtzahl der auszuwertenden Regeln pro Paket senken und damit die Abarbeitung der Regeln pro Paket stark beschleunigen. Stellen Sie sich vor, Ihre Firewall verfügte über 100 Regeln. Davon beträfen jeweils 50 Regeln TCP- und UDP-Pakete. Im besten Fall trifft die erste Regel bereits auf das aktuell betrachtete Paket zu, im schlechtesten Fall aber erst die Regel 100. Dabei müssten Sie bei einem TCP-Paket die UDP-Regeln gar nicht betrachten und umgekehrt. Also erzeugen Sie sich zwei neue

Ketten: `mein_udp` und `mein_tcp`. Anschließend verschieben Sie alle TCP-Regeln in die Kette `mein_tcp` und alle UDP-Regeln in die Kette `mein_udp`. Nun müssen Sie nur noch in der originalen Kette prüfen, ob es sich um ein TCP-Paket handelt. Dann springen Sie in die Kette `mein_tcp`. In dem anderen Fall springen Sie in die Kette `mein_udp`. Nun wird Ihr Paket im besten Fall von der Regel Zwei bereits akzeptiert (die erste Regel prüft ja, ob es ein TCP- oder UDP-Paket ist). Im schlechtesten Fall müssen aber nur 51 Regeln abgearbeitet werden. Die Gesamtzahl der pro Paket auszuwertenden Regeln sinkt also drastisch. Dies können Sie möglicherweise durch eine weitere Aufteilung weiter senken.

- Die benutzerdefinierten Ketten erlauben Ihnen auch eine Optimierung der Lesbarkeit. Sie können zum Beispiel drei Ketten erzeugen: `mein_extern`, `mein_dmz` und `mein_intern`. Sobald ein Paket aus dem entsprechenden Netz kommt, springen Sie in die jeweilige Kette. Dies erlaubt Ihnen eine logische Gruppierung der Regeln. Wenn Sie wissen möchten, was die DMZ verlassen darf, so müssen Sie nur noch in eine Kette schauen.
- Schließlich ist es auch in bestimmten Umgebungen mit benutzerdefinierten Ketten leichter möglich, Veränderungen an den Firewall-Regeln vorzunehmen. Vor einigen Jahren wurde ich gebeten, eine Firewall für ein größeres IT-Schulungsunternehmen aufzusetzen. Diese Firewall sollte neben dem Netz für die Personalverwaltung, den Vertrieb und dem Labornetz auch die Netze der einzelnen Schulungsräume untereinander und im Zugriff auf das Internet kontrollieren und regeln. Aufgrund der verschiedenen Themen, die in dem Unternehmen geschult wurden, waren häufig Änderungen an den Firewall-Regeln erforderlich. Die Administration sollte jedoch von Personen durchgeführt werden, die über keinerlei oder nur geringe Kenntnisse verfügten. Daher implementierte ich für jeden Schulungsraum eine eigene benutzerdefinierte Kette, in der die Regeln für den Zugriff der Rechner dieses Raumes auf das Internet definiert wurden. Zusätzlich schrieb ich ein einfaches Skript, das den Benutzer nach der Raumnummer fragte und anschließend fünf vordefinierte Firewall-Regelsätze anbot. Nach der Auswahl löschte das Skript nur die Regeln in der benutzerdefinierten Kette dieses Raumes und fügte die neuen Regeln ein. Dadurch war sichergestellt, dass alle weiteren Räume und auch die weiteren Netze zur Verwaltung der Firma ungestört weiterarbeiten konnten. Dieser Vorgang wäre ohne benutzerdefinierte Ketten ungleich komplizierter gewesen, denn ein kompletter Neustart des Firewall-Skripts kam nicht in Frage.

Bevor wir uns aber mit einer praktischen Implementierung beschäftigen, wollen wir zunächst schauen, wie die benutzerdefinierten Ketten arbeiten. Wenn Sie die Beispiele nachstellen wollen, sollten Sie zunächst sämtliche auf Ihrem System geladenen Firewall-Regeln löschen und die Default-Policies der Ketten auf ACCEPT setzen. Auf einem Fedora/RedHat-System kann das zum Beispiel recht komfortabel mit dem Befehl `service Iptables stop` erfolgen. Ansonsten können Sie ein Skript wie in Listing 5.2 auf Seite 98 verwenden. Im Anhang finden Sie noch ein ausführliches Skript, das tatsächlich alle Ketten löscht und den Urzustand wiederherstellt (siehe Abschnitt B.1).

Hinweis

Dieses Skript zum Stopp der Firewall ist auch auf der CD in dem Ordner *Beispielskripte* enthalten.

Sie können eine neue benutzerdefinierte Kette mit dem Befehl `iptables` erzeugen. Hierzu verwenden Sie einfach:

```
[root@bibo ~]# iptables -N meinekette
[root@bibo ~]# iptables -vnL
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 93 packets, 58921 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 92 packets, 7147 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain meinekette (0 references)
 pkts bytes target     prot opt in     out     source               destination
```

Sie sehen am unteren Ende der Ausgabe des Befehls `iptables -vnL` Ihre neue Kette. Sofort fällt auf, dass diese Kette scheinbar keine Policy hat. Anstelle der Policy wird hier die Anzahl der Referenzen angegeben. Damit Sie erkennen, was eine Referenz ist, erzeugen wir nun eine Regel, die die Kette nutzt:

```
[root@bibo ~]# iptables -A INPUT -j meinekette
[root@bibo ~]# iptables -vnL
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 654 packets, 243K bytes)
 pkts bytes target     prot opt in     out     source               destination
  299 38464 meinekette  all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT 649 packets, 60506 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain meinekette (1 references)
 pkts bytes target     prot opt in     out     source               destination
```

In der Kette INPUT ist nun eine Regel vorhanden, die auf die Kette `meinekette` verweist. Dadurch wird die Kette `meinekette` in einer weiteren Kette referenziert. Dies wird in dem Referenzzähler in der Kette `meinekette` angezeigt.

Solange die Kette `meinekette` noch irgendwo referenziert wird, können Sie diese nicht entfernen. Die benutzerdefinierte Kette können Sie genauso entfernen, wie Sie diese auch erzeugen. Hierfür verwenden Sie lediglich die Option `-X`.

```
[root@bibo ~]# iptables -X meinekette
iptables: Too many links
```

Hier werden Sie darauf hingewiesen, dass noch eine Verknüpfung mit dieser Kette existiert. Diese müssen Sie zuerst löschen. Es gibt keine Suchfunktion für diese Referenz. Sie können sich nur durch den `grep`-Befehl unterstützen lassen.

Nun fügen wir der Kette `meinekette` zunächst eine Regel hinzu:

```
[root@bibo ~]# iptables -A meinekette -j DROP
```

Dann löschen wir die Referenz:

```
[root@bibo ~]# iptables -F INPUT
[root@bibo ~]# iptables -vnL
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 1427 packets, 612K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 1455 packets, 135K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain meinekette (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

Wenn Sie nun versuchen, die Kette zu löschen, wird der Versuch wieder fehlschlagen, da die Kette noch nicht leer ist. Erst nach dem Flush der Kette kann die benutzerdefinierte Kette gelöscht werden.

```
[root@bibo ~]# iptables -X meinekette
iptables: Directory not empty
[root@bibo ~]# iptables -F meinekette
[root@bibo ~]# iptables -X meinekette
```

Damit ist schon fast alles zur Administration der benutzerdefinierten Ketten gesagt. Es bleibt der Verweis auf die Möglichkeit, dass Sie eine benutzerdefinierte Kette umbenennen können. Hierzu gibt es den folgenden Befehl:

```
[root@bibo ~]# iptables -E meinekette neuername
```

Eine Frage ist aber dennoch offen: Was passiert am Ende der benutzerdefinierten Kette, wenn es keine Standardrichtlinien (Policy) gibt? Antwort: Die benutzerdefinierte Kette arbeitet ähnlich einem Unterprogramm. Nach ihrer Abarbeitung springt sie in die aufrufende Kette zurück, die weiter abgearbeitet wird. Wenn Sie dieses Verhalten verhindern möchten, müssen Sie am Ende der benutzerdefinierten Kette eine eigene Regel vorsehen, die alle nicht von expliziten Regeln betrachteten Pakete betrifft. Das könnte zum Beispiel der folgende Iptables-Befehl erreichen:

```
[root@bibo ~]# iptables -A meinekette -j DROP
```

Diese Regel würde alle weiteren Pakete in dieser Kette verwerfen. Ein Rücksprung in die aufrufende Kette würde nicht mehr erfolgen, da für alle Pakete in dieser Kette eine Entscheidung getroffen wurde. Ob Sie die restlichen Pakete verwerfen (`DROP`), ablehnen (`REJECT`) oder akzeptieren (`ACCEPT`) hängt sicherlich von der Logik Ihrer Firewall ab.

Genauso kann es jedoch sein, dass Sie bei bestimmten Paketen einen sofortigen Rücksprung in die aufrufende Kette veranlassen möchten. Auch dies ist möglich. Hierfür gibt es das Ziel `RETURN`. Damit können Sie die benutzerdefinierte Kette sofort verlassen und in der aufrufenden Kette die weiteren Regeln betrachten.

```
[root@bibo ~]# iptables -A meinekette -j RETURN
```

9.3.1 Anwendung der benutzerdefinierten Ketten

Nun wollen wir die benutzerdefinierten Ketten nutzen, um das Skript der dreibeinigen Firewall übersichtlicher und wartbarer zu gestalten. Wenn Sie das entsprechende Kapitel nicht gelesen haben, möchte ich Ihnen nun ans Herz legen, es kurz querzulesen, so dass Sie den Sinn des folgenden Skripts und des Umbaus kennen.

Zunächst sollten wir uns überlegen, welche Ketten wir benutzerdefiniert anlegen möchten. Es gibt grundsätzlich mehrere konzeptionelle Möglichkeiten:

1. Wir erzeugen für jedes Netz eine Kette. In dieser Kette wird definiert, welche Verbindungen das Netz aufbauen darf. Dies trennt die Regeln also entsprechend der Herkunft der Verbindungen auf. Die drei Ketten heißen dann: `DMZ`, `LAN` und `INTERNET`.

2. Wir erzeugen für jedes IP-Protokoll eine Kette. So gibt es drei Ketten: `TCP`, `UDP` und `ICMP`. Dies kann in bestimmten Umgebungen von Vorteil sein. Hier ist es das sicher nicht.

3. Wir erzeugen für jeden Informationsfluss eine Kette. Das bedeutet, dass wir eine Kette für den Zugriff auf unseren Webserver erzeugen, eine Kette für den E-Mail-Verkehr und eine Kette für den Proxy. Sobald wir Änderungen an der Art und Weise der E-Mail-Zustellung vornehmen wollen, müssen wir nur in der entsprechenden Kette die Änderungen vornehmen.

Achtung

Es ist nicht möglich, eine Kette `icmp` zu erzeugen und zu benutzen, da dieses Schlüsselwort bereits belegt ist. Sie können diese Namenskonflikte sehr einfach vermeiden, indem Sie Großbuchstaben für Ihre Ketten verwenden oder jeder Kette einen Buchstaben voranstellen.

Welche der drei Konzepte Sie für Ihre zukünftigen Firewalls verwenden, möchte ich Ihnen überlassen. Ich wähle für die weitere Erläuterung den Fall Eins, bei dem drei Ketten (`DMZ`, `LAN` und `INTERNET`) erzeugt werden.

Das Skript 9.2 kann nun umgeschrieben werden. Dabei werden die ersten Zeilen inklusive der NAT-Regeln unverändert übernommen und anschließend die benutzerdefinierten Ketten erzeugt.

```
#!/bin/sh
#
# Autor  : Ralf Spenneberg
# Version: 0.1
# Datum  : 17. Dez 2004
#
# Dieses Skript lädt die Regeln für die Firewall

INTDEV="eth1"
# Achtung: Bei Einsatz von User-Mode-Linux lautet diese Variable
# INTDEV="tap0"

EXTDEV="eth0"

DMZDEV="eth2"

IPTABLES=/sbin/iptables
SYSCTL=/sbin/sysctl
MODPROBE=/sbin/modprobe

MAIL=192.168.255.2
WEB=192.168.255.3
DNS=192.168.255.4
PROXY=192.168.255.5
PROXYPORT=3128
EXTERN=3.0.0.1

# Lade die Kernelmodule für die Stateful-Inspection des FTP-Protokolls
$MODPROBE ip_conntrack_ftp
```

```
$MODPROBE ip_nat_ftp

# Setze Default-Regeln
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP

# Lösche die Filter-Tabelle
$IPTABLES -F

# Lösche die NAT-Tabelle
$IPTABLES -t nat -F

## NAT-Regeln ##
# (1) Proxy-Zugriff
$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -s $PROXY -j SNAT --to-source $EXTERN
# (2) DNS-Zugriff
$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -s $DNS -j SNAT --to-source $EXTERN

# (3) Mailserver-Zugriff nach außen
$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -s $MAIL -j SNAT --to-source $EXTERN

# (4) Webserver-Zugriff von außen
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tcp -d $EXTERN -m multiport --dport 80,443 ↵
  -j DNAT --to-destination $WEB

# (5) Mailserver-Zugriff von außen
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tcp -d $EXTERN --dport 25 -j DNAT ↵
  --to-destination $MAIL

# Erzeuge benutzerdefinierte Ketten
$IPTABLES -N DMZ
$IPTABLES -N LAN
$IPTABLES -N INTERNET

## Firewall-Regeln
# Akzeptiere alle aufgebauten Verbindungen
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Nun können die Regeln auf die Ketten verteilt werden und die Ketten angesprungen werden.

```
#######################################################
#
# Zugriff aus dem LAN
#
```

```
# Erlaube den Zugriff auf den Proxy
$IPTABLES -A LAN -o $DMZDEV -d $PROXY -p tcp --dport $PROXYPORT -m state --state NEW ↵
  -j ACCEPT

# Erlaube den Zugriff auf den E-Mail-Server
$IPTABLES -A LAN -o $DMZDEV -d $MAIL -p tcp --dport 25 -m state --state NEW -j ACCEPT

### Bei Verwendung eines internen E-Mail-Servers:
# MAILINTERN=192.168.0.100
# Erlaube den Zugriff auf den E-Mail-Server
# $IPTABLES -A LAN -o $DMZDEV -s $MAILINTERN -d $MAIL -p tcp --dport 25 -m state ↵
  --state NEW -j ACCEPT

# Protokolliere alle anderen Anfragen von innen
$IPTABLES -A LAN -j LOG --log-prefix "Unerlaubt von innen: "
$IPTABLES -A LAN -j REJECT

#########################################################
#
# Zugriff aus der DMZ
#
# Erlaube den Transport von E-Mail aus der DMZ in das interne Netz
# $IPTABLES -A DMZ -o $INTDEV -d $MAILINTERN -s $MAIL -p tcp --dport 25 -m state ↵
  --state NEW -j ACCEPT
###

# Erlaube dem DNS-Server einen Zugriff auf Nameserver im Internet
$IPTABLES -A DMZ -o $EXTDEV -s $DNS -p tcp --dport 53 -m state --state NEW -j ACCEPT
$IPTABLES -A DMZ -o $EXTDEV -s $DNS -p udp --dport 53 -m state --state NEW -j ACCEPT

# Erlaube dem Proxy den Zugriff auf das Internet
$IPTABLES -A DMZ -o $EXTDEV -s $PROXY -p tcp -m multiport --dport 21,80,443 -m state ↵
  --state NEW -j ACCEPT

# Erlaube dem E-Mail-Server den Zugriff auf das Internet
$IPTABLES -A DMZ -o $EXTDEV -s $MAIL -p tcp --dport 25 -m state --state NEW -j ACCEPT

# Protokolliere alle anderen Zugriffe aus der DMZ
$IPTABLES -A DMZ -j LOG --log-prefix "Unerlaubt aus der DMZ: "
$IPTABLES -A DMZ -j REJECT

#########################################
#
# Zugriff aus dem Internet
#
```

```
# Erlaube dem Internet den Zugriff auf den E-Mail-Server
$IPTABLES -A INTERNET -o $DMZDEV -d $MAIL -p tcp --dport 25 -m state --state NEW -j ACCEPT

# Erlaube dem Internet den Zugriff auf den Webserver
$IPTABLES -A INTERNET -o $DMZDEV -d $WEB -p tcp -m multiport --dport 80,443 -m state ↵
  --state NEW -j ACCEPT

# Rufe die Ketten auf

# FORWARD
$IPTABLES -A FORWARD -i $INTDEV -j LAN
$IPTABLES -A FORWARD -i $DMZDEV -j DMZ
$IPTABLES -A FORWARD -i $EXTDEV -j INTERNET

# INPUT
$IPTABLES -A INPUT -p tcp --dport 113 -j REJECT
$IPTABLES -A INPUT -i $INTDEV -j LAN
$IPTABLES -A INPUT -i $DMZDEV -j DMZ
```

Wenn Sie sich nun Ihre `FORWARD`-Kette ansehen, werden Sie feststellen, dass diese sehr übersichtlich geworden ist. Es sind nur noch 4 Regeln vorhanden:

```
[root@bibo ~]# iptables -vnL FORWARD
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0 ↵
                                                                  state RELATED,ESTABLISHED
    0     0 LAN        all  --  eth1   *       0.0.0.0/0            0.0.0.0/0
    0     0 DMZ        all  --  eth2   *       0.0.0.0/0            0.0.0.0/0
    0     0 INTERNET   all  --  eth0   *       0.0.0.0/0            0.0.0.0/0
```

Sie können sehr leicht feststellen, welchen Weg ein neues Verbindungsaufbaupaket durch Ihr Regelwerk nimmt. Denken Sie daran, dass alle Pakete, die zu aufgebauten Verbindungen gehören, bereits von der ersten Regel in dieser Kette akzeptiert werden. Alle Verbindungsaufbauten werden entsprechend der Netzwerkkarte, über die diese Pakete eingehen, auf die verschiedenen Ketten verteilt. Erreicht das Paket über die Netzwerkkarte `eth2` das System, so wird es an die Kette `DMZ` übergeben, die das Paket prüft, gegebenenfalls akzeptiert oder protokolliert und verwirft.

Falls Sie nun die genauen Regeln betrachten möchten, die das Paket dann prüfen, so genügt es, die Kette `DMZ` anzuzeigen.

```
[root@bibo ~]# iptables -vnL DMZ
Chain DMZ (2 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  *      eth0    192.168.255.4        0.0.0.0/0 ↵
                                                                     tcp dpt:53 state NEW
```

```
0     0 ACCEPT     udp  --  *      eth0    192.168.255.4       0.0.0.0/0 ↵
                                                                udp dpt:53 state NEW
0     0 ACCEPT     tcp  --  *      eth0    192.168.255.5       0.0.0.0/0 ↵
                                                        multiport dports 21,80,443 state NEW
0     0 ACCEPT     tcp  --  *      eth0    192.168.255.2       0.0.0.0/0 ↵
                                                                tcp dpt:25 state NEW
0     0 LOG        all  --  *      *       0.0.0.0/0           0.0.0.0/0 ↵
                                         LOG flags 0 level 4 prefix 'Unerlaubt aus der DMZ: '
0     0 REJECT     all  --  *      *       0.0.0.0/0           0.0.0.0/0 ↵
                                                        reject-with icmp-port-unreachable
```

Der Vorteil der benutzerdefinierten Ketten in puncto Lesbarkeit sollte Ihnen nun klar geworden sein. Gleichzeitig haben wir aber auch etwas für die Optimierung der Geschwindigkeit getan. Ein Paket, das eine neue Verbindung aus dem Internet zu dem Webserver starten möchte, hätte beim alten Firewall-Skript von 10 Regeln betrachtet werden müssen, bevor es akzeptiert worden wäre. Dies kostet Zeit. Nun handelt es sich lediglich um vier Regeln in der `FORWARD`-Kette und dann um zwei Regeln in der Kette `INTERNET`. Insgesamt sind es also nur sechs Regeln. Bei einer derart geringen Regelzahl ist der Vorteil nur minimal, und häufig ist nicht das Firewall-System das Nadelöhr beim Pakettransport, sondern die Bandbreiten der beteiligten Netzwerkverbindungen. Stellen Sie sich aber eine Firewall mit mehreren hundert Regeln vor, die mit Gigabit-Geschwindigkeit die Pakete verarbeiten soll. Hier kann die Firewall sehr wohl ein Nadelöhr darstellen.

Hinweis

Natürlich ist streng genommen nicht die Anzahl der Regeln, sondern die Anzahl der durchzuführenden Prüfungen interessant. Die meisten Regeln prüfen nicht nur eine Eigenschaft des Pakets, sondern meist gleich mehrere. Diese Prüfungen dauern leider nicht alle gleich lang, so dass objektive Berechnungen nicht möglich sind. Die Anzahl der Prüfungen erlaubt jedoch eine grobe Abschätzung des Aufwands.

9.4 DMZ mit zwei Paketfiltern

Eine dreibeinige Firewall mit DMZ bietet bereits einen recht ordentlichen Schutz. Jedoch besteht immer die Gefahr, dass ein Angreifer auf dem System einen Konfigurationsfehler oder einen Bug in der verwendeten Software (zum Beispiel in dem Linux-Kernel) findet. Erlangt der Angreifer so die Kontrolle über das System, kann er von einer dreibeinigen Firewall aus jedes System in der DMZ, aber auch jedes System in dem internen LAN erreichen. Bei den Systemen in der DMZ muss ein möglicher Angriff mit anschließendem Einbruch immer als Risiko akzeptiert werden muss, da die Systeme im (eingeschränkten) Zugriff des Internets stehen. Dies soll die Firewall für die internen Systeme im LAN gerade verhindern. Sie können

dazu eine zweistufige Firewall mit zwei Paketfiltern einsetzen. Fällt der erste Paketfilter in die Hände des Angreifers, so schützt der zweite Paketfilter noch das interne LAN.

Natürlich besteht die Gefahr, dass der Angreifer auch in den zweiten Paketfilter eindringt. Als Firewall-Administrator hofft man jedoch, dass dies so viel Zeit kostet, dass man Gegenmaßnahmen einleiten kann. Das kann zum Beispiel eine Unterbrechung der Netzwerkverbindung sein. Häufig wird aus diesem Grund auch empfohlen, zwei unterschiedliche Produkte als Paketfilter einzusetzen[1]. So kann ein Angreifer nicht denselben Softwarefehler für den Einbruch in beiden Paketfiltern nutzen, sondern muss nach neuen Lücken suchen. Auch Konfigurationsfehler treten selten auf beiden Systemen gleich auf. Dies erhöht also die Schwierigkeit für den Angreifer. Da dies jedoch ein Iptables-Buch ist, möchte ich mich hier darauf beschränken, die Empfehlung zu erwähnen und es Ihnen zu überlassen, ob Sie dieser Empfehlung folgen und welches zusätzliche Produkt Sie auswählen.

Die Implementierung der zweistufigen Firewall erfolgt wie in Abbildung 9.1.

Wie bereits zu Beginn des Kapitels erwähnt wurde (siehe Abschnitt 9.1), befinden sich in der DMZ der Beispielfirma *Nohup.info* jeweils ein Web-, ein E-Mail-, ein cachender DNS- und ein Proxy-Server. Diese Systeme erhalten private IP-Adressen aus dem Bereich 192.168.255.0/24. Dabei soll aus dem Internet ein Zugriff auf den Web- und den E-Mail-Server möglich sein. Aus dem internen Netz ist ein Zugriff auf den Proxy- und den E-Mail-Server notwendig. Der Zugriff auf den Webserver wird über den Proxy-Server realisiert. Ein direkter Zugriff auf das Internet ist nicht vorgesehen. Der äußere Paketfilter erhält als externe IP-Adresse eine feste statische IP-Adresse 3.0.0.1. Alle Dienste werden im Internet unter dieser IP-Adresse angebunden. Das bedeutet, dass ein DNS-Server bei der Frage nach der Adresse `www.nohup.info` die IP-Adresse 3.0.0.1 zurückliefert.

Teilen wir nun die Implementierung auf. Zunächst besprechen wir die Regeln für den äußeren Paketfilter, anschließend für den inneren Paketfilter.

Tipp

Wenn Sie den Hardwareaufwand für zwei Paketfilter scheuen und Ihr System über mindestens drei Netzwerkkarten verfügt, können Sie die beiden Paketfilter auch als virtuelle Systeme auf der Hardware laufen lassen. Hierfür können Sie VMware[2], User-Mode-Linux[3] oder Xen[4] verwenden. Alle diese Systeme sind in der Lage, die Hardware zu virtualisieren und voneinander getrennte Linux-Systeme auf derselben Hardware zu ermöglichen. Die Sicherheit ist sicherlich nicht so hoch wie bei zwei physikalisch getrennten Systemen, aber besser als bei einer dreibeinigen Firewall.

[1] Das BSI (Bundesamt für Sicherheit in der Informationstechnik) spricht zum Beispiel diese Empfehlung aus.

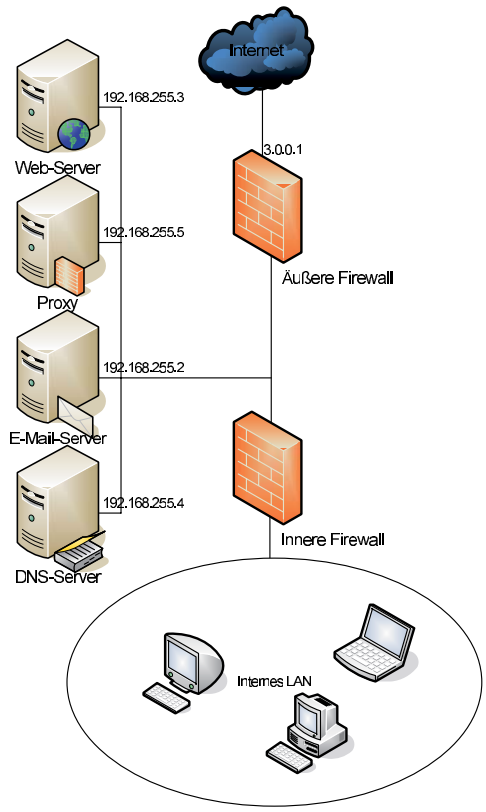


Abbildung 9.1: Eine zweistufige Firewall schützt die DMZ.

9.4.1 Der äußere Paketfilter

Der äußere Paketfilter muss den Zugriff des Internets auf den Webserver und den E-Mail-Server in der DMZ erlauben. Außerdem muss er dem Proxy, dem DNS-Server und dem E-Mail-Server den Zugriff auf die Ressourcen des Internets ermöglichen.

Das Skript beginnt wieder mit der üblichen Definition der Variablen. Die zwei vorhandenen Netzwerkkarten erhalten die Variablennamen `$EXTDEV` und `$DMZDEV`. Ansonsten kann der Skriptkopf des Skripts für die dreibeinige Firewall unverändert übernommen werden.

[2] Ein kommerzielles System zur Virtualisierung: *http://www.vmware.com*.

[3] Ein Linux-Kernel, der auf einem bestehenden Linux-System ein weiteres System booten kann: *http://user-mode-linux.sf.net*.

[4] Xen erlaubt eine komplette Virtualisierung eines Systems. Es ist nicht mehr möglich, zwischen einem Host und einem Gastsystem zu unterscheiden. Es ist mit der S/390-Großrechner-Technik und dem VMware-Produkt ESX-Server vergleichbar: *http://www.cl.cam.ac.uk/Research/SRG/netos/xen/*.

```
#!/bin/sh
#
# Autor  : Ralf Spenneberg
# Version: 0.1
# Datum  : 17. Dez 2004
#
# Dieses Skript lädt die Regeln für die Firewall

EXTDEV="eth0"

DMZDEV="eth1"

IPTABLES=/sbin/iptables
SYSCTL=/sbin/sysctl
MODPROBE=/sbin/modprobe

MAIL=192.168.255.2
WEB=192.168.255.3
DNS=192.168.255.4
PROXY=192.168.255.5
EXTERN=3.0.0.1

# Lade die Kernelmodule für die Stateful-Inspection des FTP-Protokolls
$MODPROBE ip_conntrack_ftp
$MODPROBE ip_nat_ftp

# Setze Default-Regeln
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP

# Lösche die Filter-Tabelle
$IPTABLES -F

# Lösche die NAT-Tabelle
$IPTABLES -t nat -F
```

Die äußere Firewall ist auch für ein NAT der Adressen zum Internet hin zuständig. Hier können die NAT-Regeln aus dem Skript für die dreibeinige Firewall unverändert übernommen werden:

```
## NAT-Regeln ##
# (1) Proxy-Zugriff
$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -s $PROXY -j SNAT --to-source $EXTERN

# (2) DNS-Zugriff
```

```
$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -s $DNS -j SNAT --to-source $EXTERN

# (3) Mailserver-Zugriff nach außen
$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -s $MAIL -j SNAT --to-source $EXTERN

# (4) Webserver-Zugriff von außen
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tcp -d $EXTERN -m multiport --dport 80,443 ↲
  -j DNAT --to-destination $WEB

# (5) Mailserver-Zugriff von außen
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tcp -d $EXTERN --dport 25 -j DNAT ↲
  --to-destination $MAIL
```

Diese Regeln sorgen dafür, dass bei einem Zugriff auf das Internet die Quell-IP-Adressen des DNS-, E-Mail- und Proxy-Servers genattet werden. Auch bei einem Zugriff aus dem Internet auf den E-Mail- und den Webserver wird der Zugriff genattet.

Es fehlen nun noch die Filterregeln. Auch diese können fast unverändert übernommen werden.

```
# Erlaube dem DNS-Server einen Zugriff auf Nameserver im Internet
$IPTABLES -A FORWARD -i $DMZDEV -o $EXTDEV -s $DNS -p tcp --dport 53 -m state ↲
  --state NEW -j ACCEPT
$IPTABLES -A FORWARD -i $DMZDEV -o $EXTDEV -s $DNS -p udp --dport 53 -m state ↲
  --state NEW -j ACCEPT

# Erlaube dem Proxy den Zugriff auf das Internet
$IPTABLES -A FORWARD -i $DMZDEV -o $EXTDEV -s $PROXY -p tcp -m multiport --dport 21,80,443 ↲
  -m state --state NEW -j ACCEPT

# Erlaube dem E-Mail-Server den Zugriff auf das Internet
$IPTABLES -A FORWARD -i $DMZDEV -o $EXTDEV -s $MAIL -p tcp --dport 25 -m state --state NEW ↲
  -j ACCEPT

# Erlaube dem Internet den Zugriff auf den E-Mail-Server
$IPTABLES -A FORWARD -i $EXTDEV -o $DMZDEV -d $MAIL -p tcp --dport 25 -m state --state NEW ↲
  -j ACCEPT

# Erlaube dem Internet den Zugriff auf den Webserver
$IPTABLES -A FORWARD -i $EXTDEV -o $DMZDEV -d $WEB -p tcp -m multiport --dport 80,443 ↲
  -m state --state NEW -j ACCEPT

# Lehne Identd-Anfragen ab
$IPTABLES -A INPUT -p tcp --dport 113 -j REJECT

$IPTABLES -A FORWARD -i $DMZDEV -j LOG --log-prefix "Unerlaubt aus der DMZ: "
```

```
$IPTABLES -A FORWARD -i $DMZDEV -j REJECT
$IPTABLES -A INPUT -i $DMZDEV -j LOG --log-prefix "Unerlaubt aus der DMZ: "
$IPTABLES -A INPUT -i $DMZDEV -j REJECT
```

Dieses Skript genügt für die Konfiguration des äußeren Paketfilters. Ein direkter Zugriff von dem inneren Paketfilter wird nicht erlaubt. So ist der äußere Paketfilter auch vor Angriffen von innen geschützt. Wenn Sie einen zusätzlichen Administrationszugang wünschen, so können Sie zum Beispiel einen Zugang per SSH erlauben:

```
$IPTABLES -A INPUT -i $DMZDEV -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
$IPTABLES -A OUTPUT -O $DMZDEV -m state --state ESTABLISHED -j ACCEPT
```

Natürlich könnten Sie auch diesen Zugang auf eine bestimmte IP-Adresse begrenzen. Dann ist es aber sinnvoll, für diese Adresse auch eine Variable, z.B. `ADMIN`, zu verwenden.

9.4.2 Der innere Paketfilter

Die Aufgabe des inneren Paketfilters ist es, den Zugriff des internen LANs auf die Systeme in der DMZ zu regeln. Je nach der gewählten E-Mail-Struktur muss er auch eine Verbindung des DMZ-E-Mail-Servers in das LAN ermöglichen.

Ich beschränke mich nun auf die Darstellung des kompletten Skripts und einige wenige Erklärungen. Die einzelnen Regeln wurden in den vorangegangenen Kapiteln bereits ausreichend erläutert. Die Netzwerkkarten in diesem Skript heißen `DMZDEV` und `INTDEV`. Das folgende Skript implementiert den inneren Paketfilter:

```
#!/bin/sh
#
# Autor  : Ralf Spenneberg
# Version: 0.1
# Datum  : 17. Dez 2004
#
# Dieses Skript lädt die Regeln für den inneren Paketfilter

INTDEV="eth1"

DMZDEV="eth2"

IPTABLES=/sbin/iptables
SYSCTL=/sbin/sysctl
MODPROBE=/sbin/modprobe

MAIL=192.168.255.2
PROXY=192.168.255.5
PROXYPORT=3128
```

```
# Setze Default-Regeln
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP

# Lösche die Filter-Tabelle
$IPTABLES -F

## Firewall-Regeln
# Akzeptiere alle aufgebauten Verbindungen
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

#####################################################
#
# Zugriff aus dem LAN
#
# Erlaube den Zugriff auf den Proxy
$IPTABLES -A FORWARD -i $INTDEV -o $DMZDEV -d $PROXY -p tcp --dport $PROXYPORT -m state --
state NEW -j ACCEPT

# Erlaube den Zugriff auf den E-Mail-Server
$IPTABLES -A FORWARD -i $INTDEV -o $DMZDEV -d $MAIL -p tcp --dport 25 -m state --state NEW -
j ACCEPT

### Bei Verwendung eines internen E-Mail-Servers:
# MAILINTERN=192.168.0.100
# Erlaube den Zugriff auf den E-Mail-Server
# $IPTABLES -A FORWARD -i $INTDEV -o $DMZDEV -s $MAILINTERN -d $MAIL -p tcp --dport 25 -
m state --state NEW -j ACCEPT

# Protokolliere alle anderen Anfragen von innen
$IPTABLES -A FORWARD -i $INTDEV -j LOG --log-prefix "Unerlaubt von innen: "
$IPTABLES -A FORWARD -i $INTDEV -j REJECT

#####################################################
#
# Zugriff aus der DMZ
#
# Erlaube den Transport von E-Mail aus der DMZ in das interne Netz
# $IPTABLES -A FORWARD -i $DMZDEV -o $INTDEV -d $MAILINTERN -s $MAIL -p tcp --dport 25 -
m state --state NEW -j ACCEPT
###

# Protokolliere alle anderen Zugriffe aus der DMZ
```

```
$IPTABLES -A FORWARD -i $DMZDEV -j LOG --log-prefix "Unerlaubt aus der DMZ: "
$IPTABLES -A FORWARD -i $DMZDEV -j REJECT
```

Dieser Paketfilter führt kein NAT durch, da kein Zugriff auf das Internet erfolgt. Dafür muss dann natürlich sichergestellt sein, dass die beteiligten Systeme über entsprechende Einträge in ihren Routingtabellen verfügen. Bei den Systemen im LAN ist dies recht einfach. Bei ihnen wird als Default-Gateway der Paketfilter eingetragen. Bei den Systemen in der DMZ ist es erforderlich, als Default-Gateway den äußeren Paketfilter einzutragen. Lediglich für die Verbindung zum internen LAN ist eine zusätzliche Route auf diesen Systemen erforderlich. Hier muss als Gateway der interne Paketfilter eingetragen werden.

Ich hoffe, dass ich Ihnen mit diesen Skripten ein paar Beispiele geliefert habe, die Sie nun bei der Erstellung Ihrer eigenen Skripten unterstützen. Natürlich handelt es sich hier nur um grobe Gerüste, die häufig um spezielle Anpassungen erweitert werden müssen. Diese hängen aber immer sehr von der Umgebung ab und werden daher hier nicht näher besprochen. Wenn Sie hierzu Hilfe benötigen, so schauen Sie in den Kapiteln zur fortgeschrittenen Konfiguration der Firewall nach. Dort werden dann die einzelnen Protokolle betrachtet und Beispielregeln für deren Filterung gezeigt. Auch fortgeschrittene Fähigkeiten des Iptables-Befehls werden dort besprochen. Ich bin mir sicher, dass Sie dort auch Anhaltspunkte für Ihr Problem finden werden.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

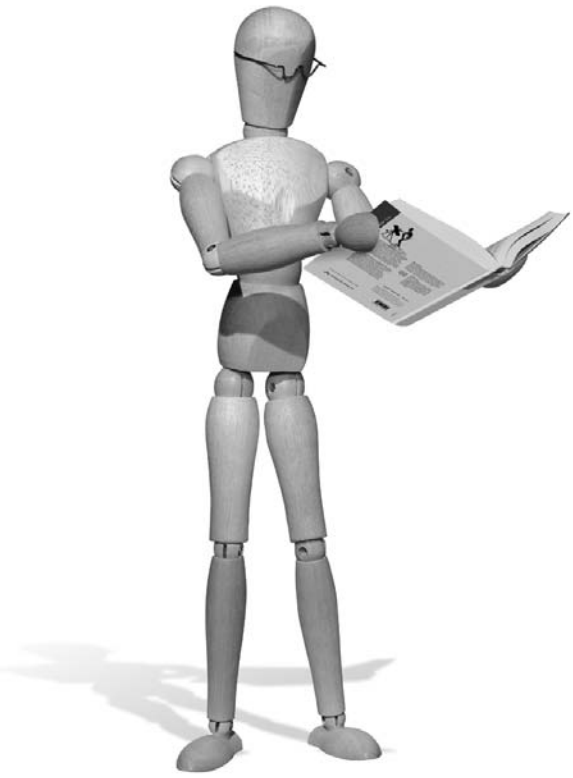
ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Teil IV

Werkzeuge



10 Zentrale Protokollserver

Sobald viele Unix- oder Linux-Rechner überwacht werden müssen, stellen die meisten Administratoren fest, dass eine manuelle Überwachung der Protokolle auf jedem einzelnen Rechner sehr mühsam und fehlerträchtig ist. Daher werden häufig zentrale Protokollserver für die Sammlung der Daten eingesetzt.

Es gibt aber noch einen weiteren, unter Sicherheitsaspekten wichtigeren Grund, für eine zentrale Protokollierung. Wenn tatsächlich ein Einbrecher in der Lage war, in Ihren Rechner einzudringen, so wird er zunächst versuchen, die Spuren, die der Einbruch hinterlassen hat, zu entfernen. Dies betrifft häufig auch entsprechende Einträge in den Protokollen. Werden diese Protokolle lediglich lokal und unverschlüsselt gespeichert, so hat er ein leichtes Spiel.

Protokolliert jedoch der Rechner seine Meldungen nicht nur lokal, sondern über das Netzwerk auch zentral auf einem Protokollserver, so kann der Einbrecher zwar die Spuren in den lokalen Protokolldateien entfernen, nicht jedoch die Meldungen auf dem zentralen Protokollserver löschen. Hierzu müsste er erst in den Protokollserver einbrechen.

Für die Auswertung der Protokolle ist es sehr wichtig, dass die überwachten Rechner eine gemeinsame Zeitbasis verwenden. Ansonsten besteht die Gefahr, dass bei einem Angriff die Meldungen der unterschiedlichen Rechner nicht miteinander korreliert werden können. Die Meldung eines Angriffs durch einen Snort-Sensor und die Modifikation von Dateien und die Installation eines Rootkits auf einem anderen Rechner können nicht in einen kausalen Zusammenhang gestellt werden, wenn nicht die Zeiten der Meldungen bzw. Modifikationen vergleichbar sind. Achten Sie daher darauf, dass Ihre Systeme über eine Zeitsynchronisation verfügen!

10.1 Einrichtung eines zentralen Protokollservers

Die meisten Linux-Distributionen verwenden für die Systemprotokollierung eine Kombination aus zwei Diensten: Syslogd und Klogd. Syslogd ist der zentrale Protokolldienst unter Linux. Dieser Protokolldienst nimmt die Meldungen von verschiedenen anderen Systemen entgegen. Hierbei handelt es sich unter anderen um *Crond*, *E-Mail*, *News*, *Login*, *Lpd* etc. Der Syslogd ist typischerweise nicht zuständig für Dienste wie zum Beispiel einen Apache-Webserver, einen Squid-Proxy oder Samba. Der Klogd nimmt vom Kernel die Meldungen entgegen und leitet sie üblicherweise an den Syslogd weiter. Damit werden auch Meldungen des Linux-Kernels durch den Syslogd protokolliert.

Im Folgenden möchte ich kurz die wesentlichen Möglichkeiten der Konfiguration des Syslogd und des Klogd beschreiben. Anschließend werde ich zwei weitere Syslogd-Daemons beschreiben, die ersatzweise eingesetzt werden können. Der modulare Syslogd ist im Gegensatz zum Syslog-ng nicht Bestandteil einer aktuellen Distribution und muss daher manuell installiert werden. Sowohl der modulare Syslogd als auch Syslog-ng verfügen jedoch über einige Eigenschaften, die ihren Einsatz auf sicherheitsrelevanten Systemen rechtfertigen.

Der BSD-Syslogd verfügt über lediglich eine Konfigurationsdatei. Dies ist die Datei `/etc/syslog.conf`. Sie enthält Informationen darüber, welche Meldungen wo zu protokollieren sind. Hierzu wird die folgende Syntax verwendet:

```
facility.priority            location
```

Der Standard-BSD-Syslogd, der in den meisten aktuellen Linux-Distributionen eingesetzt wird, ist in der Lage, die folgenden *Facilities* zu unterscheiden:

- `auth`
- `authpriv`
- `cron`
- `daemon`
- `kern`
- `lpr`
- `mail`
- `mark` (lediglich für interne Verwendung)
- `news`
- `security` (identisch mit `auth`, sollte jedoch nicht mehr eingesetzt werden)
- `syslog`
- `user`
- `uucp`
- `local0` bis `local7`

Als `priority` werden die folgenden Werte unterstützt:

- `debug`
- `info`
- `notice`
- `warning` und `warn` (obsolet)
- `err`, `error` (obsolet)
- `crit`
- `alert`
- `emerg`, `panic` (obsolet)

Bei einer Angabe wie zum Beispiel `cron.info` werden nun alle Meldungen von `cron` mit der Wertigkeit `info` und höher von dieser Regel protokolliert. Möchten Sie spezifisch nur die Meldungen mit der Wertigkeit `info` protokollieren, so können Sie dies mit der Angabe `cron.=info` erreichen. Außerdem ist die Negation möglich: `cron.!=info`. Zusätzlich besteht die Möglichkeit, sowohl für die Facility als auch für die Priority den Stern (*) als Wildcard zu verwenden.

Leider besteht beim Standard-BSD-Syslog nicht die Möglichkeit, in Abhängigkeit von einem Muster, zum Beispiel einem regulären Ausdruck, die Protokollierung zu konfigurieren.

Nachdem Sie die zu protokollierenden Meldungen in der linken Spalte der Datei `/etc/syslog.conf` ausgewählt haben, müssen Sie den Ort der Protokollierung definieren. Hier stehen ebenfalls mehrere Möglichkeiten zur Verfügung:

- Normale Datei, z.B. `/var/log/messages`
- Named Pipe, z.B. `|/var/log/my_fifo`. Diese Named Pipe muss zuvor mit dem Befehl `mkfifo` erzeugt werden. Hiermit besteht die Möglichkeit, die Informationen ähnlich einer normalen Pipe an einen anderen Prozess weiterzuleiten.
- Terminal bzw. Konsole, z.B. `/dev/tty10`
- Zentraler Protokollserver, z.B. `@logserver.example.com`
- Benutzer, z.B. `root`. Diese Personen erhalten die Meldungen auf ihrem Terminal, falls sie angemeldet sind. Es wird keine E-Mail versandt!
- Alle angemeldeten Benutzer `*`.

Ein paar Beispiele verdeutlichen dies:

```
# Kritische Kernelmeldungen auf der 10. virtuellen Konsole
kern.crit                                               /dev/tty10
# Notfälle direkt an root
kern.emerg                                              root
# Authentifizierungsvorgänge in einer geschützten Datei und zusätzlich
# zentral
authpriv.*                /var/log/secure
authpriv.*                                              @remotesyslog
# E-Mail getrennt
mail.*                /var/log/maillog
# Alles andere in einer Datei
*.info;mail.none;authpriv.none                  /var/log/messages
```

Der Syslog erhält üblicherweise die zu protokollierenden Meldungen über den Unix-Socket `/dev/log`. Dieser Socket wird vom Syslog beim Start erzeugt. Dies genügt in den meisten Fällen, da sämtliche lokalen Anwendungen auf diesen Socket zugreifen können. Bei einer Anwendung, die sich in einer Chroot-Umgebung befindet, besteht jedoch das Problem, dass ein derartiger Zugriff auf `/dev/log` nicht möglich ist. Der Syslogd muss dann bei seinem Start einen zusätzlichen Unix-Socket

in der Chroot-Umgebung erzeugen. Dies kann mit der Option `-a socket` erfolgen. Hiermit können bis zu 19 weitere Sockets definiert werden.

Mithilfe dieser Unix-Sockets ist jedoch der Syslogd nicht in der Lage, Meldungen über das Netzwerk entgegenzunehmen. Hierzu muss zusätzlich ein Internet-Socket geöffnet werden. Die Protokollierung über das Netzwerk erfolgt beim Standard-BSD-Syslogd an den UDP-Port 514. Die Konfiguration dieser Portnummer erfolgt beim Syslogd in der Datei `/etc/services`. Diese Datei enthält hierzu üblicherweise folgenden Eintrag:

```
syslog          514/udp
```

Leider erfolgt die Protokollierung nur mit UDP. Daher kann der Syslog nicht sicherstellen, dass sämtliche Meldungen tatsächlich den Empfänger erreichen. Einzelne Pakete können zum Beispiel aufgrund einer falsch konfigurierten Firewall oder einer Überlastung des Netzwerks verloren gehen. Auch bietet UDP kein Schutz vor Spoofing.

Damit der Syslogd nun diesen Port öffnet und Meldungen über diesen Internet-Socket annimmt, müssen Sie ihn mit der Option `-r` starten. Dann nimmt er jede Meldung, die an diesen Socket gesendet wird, an und protokolliert sie entsprechend seiner eigenen Konfigurationsdatei `/etc/syslog.conf`. Es besteht leider nicht die Möglichkeit, im Syslogd die Clients, die die Meldungen senden, zu authentifizieren oder aufgrund ihrer IP-Adresse einzuschränken. Dies kann lediglich durch das Setzen intelligenter Paketfilterregeln (Iptables) geschehen. Ein Angreifer könnte daher den Protokollserver mit Meldungen (auch mit gefälschten Absenderadressen[1]) bombardieren und so die Protokolle mit unsinnigen Meldungen füllen.

Der Klogd besitzt keine eigene Konfigurationsdatei. Die Meldungen des Kernels werden vom Klogd an den Syslogd weitergeleitet, der sie aufgrund seiner Konfigurationsdatei protokolliert. Der Klogd verfügt jedoch über eine interessante Startoption: `-c X`. Diese Option erlaubt die Definition einer Priority X. Kernel-Meldungen, die mindestens diese Wertigkeit aufweisen, werden direkt vom Klogd auf der Konsole protokolliert. Dies ist jedoch den Geschwindigkeitsbeschränkungen der Konsole unterworfen. Die Konsole wird als serielles Terminal mit einer üblichen Geschwindigkeit von 38.400 Baud emuliert. Bei dem Überschreiten der Geschwindigkeit kann es zum Verlust von Meldungen kommen.

Die unterschiedlichen Distributionen verwalten die Startoptionen des Klogd und des Syslogd an unterschiedlichen Positionen. Red Hat verwendet die Datei `/etc/sysconfig/syslog`. SUSE verwendet in Abhängigkeit von der Version entweder die Datei `/etc/rc.config` oder eine Datei im Verzeichnis `/etc/sysconfig`.

Der Standard-BSD-Syslogd ist also bereits in der Lage, seine Meldungen über das Netzwerk auf einem zentralen Logserver zu protokollieren. Leider weist er weder Mustererkennung mit regulären Ausdrücken noch Authentifizierung oder Ver-

[1] Dann hilft auch Iptables nicht mehr.

schlüsselung auf. Daher handelt es sich hierbei nicht um einen idealen Protokolldienst für sicherheitsrelevante Umgebungen.

Tipp

Wenn Sie eine Protokollmeldung aus einem Skript erzeugen wollen, können Sie einfach den Befehl `logger` verwenden. Dieser Befehl schreibt die Meldung über den Syslog-Socket `/dev/log` in die Protokolle.

10.2 Modular Syslog

Der modulare Syslog `msyslog` von der Firma Core Security Technologies (ehemals Core SDI, *http://www.corest.com*) ist ein Ersatz für den Standard-BSD-Syslog und den Klogd unter Linux, die von den meisten Linux-Distributionen eingesetzt werden. Der Msyslogd ist komplett rückwärtskompatibel zum Standard-BSD-Syslog und unterstützt zusätzlich folgende Funktionen:

- Annahme von Meldungen
  - Kernel-Meldungen über das BSD-Kernel-Interface und das Linux-`/proc/kmsg`-Interface.
  - Systemmeldungen über das Unix-Socket-Interface `/dev/log`
  - Meldungen über eine TCP- oder eine UDP-Verbindung auf einem beliebigen Port
  - Meldungen aus einer beliebigen Datei oder Named Pipe
- Ausgabe von Meldungen
  - kompatibel zum klassischen BSD-Syslogd
  - Mit einem kryptographischen Hash
  - Auf einem anderen Rechner mit TCP oder UDP
  - In Abhängigkeit von einem regulären Ausdruck
  - In einer MySQL- oder PostgreSQL-Datenbank
- Wenn der modulare Syslog die Protokolle kryptographisch mit einem PEO-Hash sichert, können Sie mit dem Werkzeug `peochk` die Integrität der Protokolle testen. Mit dem PEO-Hash werden die Log-Meldungen kryptographisch miteinander verkettet, so dass Sie später die Modifikation oder Löschung von Protokollmeldungen erkennen können. Genauere Informationen über das Protokoll finden Sie in *http://www2.corest.com/files/files/11/PEO.pdf*.

Der Secure Syslogd ist eine Vorgängerversion des Modular Syslogd und wurde auch von Core Security Technologies erzeugt. Er wies auch alle diese Fähigkeiten auf.

10.2.1 Installation des Msyslogd

Der modulare Syslogd `msyslogd` kann entweder von der Homepage von Core Security Technologies heruntergeladen werden (*http://www.corest.com*) oder von der Sourceforge-Projektseite (*http://sourceforge.net/projects/msyslog/*). Der modulare Syslogd wird unter der BSD-Lizenz vertrieben. Es handelt sich also um freie Open Source-Software, die sowohl zu privaten als auch zu kommerziellen Zwecken im Rahmen der Lizenz eingesetzt werden darf. Auf der Sourceforge-Projektseite werden üblicherweise sowohl das Quelltextpaket als auch RPM-Pakete angeboten. Die RPM-Pakete sind an die Distribution von Red Hat Linux angepasst. Nach einer leichten Anpassung des im Paket enthaltenen Start-Skripts `/etc/rc.d/init.d/msyslogd` können Sie das RPM-Paket jedoch auch auf SUSE Linux-Distributionen einsetzen. Für die Debian-Distribution existiert ebenfalls ein Paket. Eine Übersetzung des Quelltextarchivs sollte daher in den seltensten Fällen nötig sein. Falls doch, so genügt meistens ein Aufruf von

```
# ./configure
# make
# make install
```

Achtung

Die RPM-Pakete installieren den *msyslogd* unter dem Namen `msyslogd`. Dieser greift jedoch trotzdem auf die Datei `/etc/syslog.conf` zu. Die Manpages wurden jedoch ebenfalls in den RPM-Paketen umbenannt: `msyslogd.8` und `msyslog.conf.5`. Das Quelltextarchiv installiert den *msyslogd* als `syslogd`! Die ganze mitgelieferte Dokumentation geht davon aus, dass der *msyslogd* unter letzterem Namen zu finden ist. Im Weiteren wird in diesem Buch aber davon ausgegangen, dass das RPM-Paket installiert wurde und der Befehl `msyslogd` lautet.

10.2.2 Konfiguration von *msyslogd*

Bei der Konfiguration des `msyslogd` möchte ich Sie zunächst auf die hohe Kompatibilität zum Standard-BSD-Syslog hinweisen. Das wird im nächsten Abschnitt noch genauer betrachtet.

Der wesentliche Unterschied bei der Verwendung des `msyslogd` besteht in seinem Aufruf. Aufgrund seines modularen Aufbaus müssen Sie beim Start alle benötigten Eingabe-Module benennen. Der `msyslogd` verfügt über die folgenden Eingabe-Module: `bsd`, `doors`, `linux`, `streams`, `tcp`, `udp` und `unix`. Des Weiteren besitzt er folgende Ausgabe-Module: `classic`, `mysql`, `peo`, `pgsql`, `regex`, `tcp` und `udp`.

Kompatibel zum Standard-BSD-Syslogd

Ein großer Vorteil des `msyslogd` ist die Tatsache, dass dieser Syslogd abwärtskompatibel zum BSD-Syslogd ist. Der `msyslogd` verhält sich genau so, wie es von einem

Syslogd erwartet wird. Sie können einfach den BSD-Syslogd durch diesen ersetzen und die vorhandene Konfigurationsdatei ohne Änderung nutzen.

Der Prozess liest automatisch seine Konfigurationsdatei `/etc/syslog.conf` ein, liest die Kernel-Meldungen von `/proc/kmsg` und öffnet den Socket `/dev/log`.

Der `msyslogd` interpretiert die Konfigurationsdatei `/etc/syslog.conf` genauso wie der BSD- Syslogd. Leider existieren noch einige Fehler in der Implementation der Kompatibilität. Die entsprechenden Voraussetzungen sind jedoch sehr selten gegeben. Lesen Sie die Manpage (`msyslog.conf.5`) für weitere Informationen.

Die Kompatibilität mit den BSD-Syslogd-Funktionen wird vom `%classic`-Modul bereitgestellt. Sobald Sie die Funktionalität des `msyslgod` ausreichend getestet haben, sollten Sie die Konfigurationsdatei an die neue Syntax anpassen, so dass Sie anschließend auch die neuen Fähigkeiten (siehe den nächsten Abschnitt) nutzen können. Dazu ist an den entsprechenden Stellen ein Aufruf des `%classic`-Moduls erforderlich. Im nächsten Listing wird die klassische Konfiguration aus dem Listing 10.1 mit Modulen gezeigt.

```
# Kritische Kernelmeldungen auf der 10. virtuellen Konsole
kern.crit                                %classic   /dev/tty10
# Notfälle direkt an root
kern.emerg                               %classic   root
# Authentifizierungsvorgänge in einer geschützten Datei und zusätzlich
# zentral
authpriv.*                               %classic   /var/log/secure
authpriv.*                               %classic   @remotesyslog
# E-Mail getrennt
mail.*                                   %classic   /var/log/maillog
# Alles andere in einer Datei
*.info;mail.none;authpriv.none           %classic   /var/log/messages
```

Um auch den Aufruf des `msyslogd` an seine neuen Fähigkeiten anzupassen, sollten die Eingabe-Module `linux` (für das Kernel-Interface */proc/kmsg*) und `unix` (für die Bereitstellung des */dev/log*-Sockets) geladen werden. Wird der BSD-Syslogd auf Ihrem System bisher so aufgerufen:

```
syslogd -m 0
```

dann sollten Sie diesen Aufruf zusätzlich um die entsprechenden Module erweitern:

```
msyslogd -m 0 -i linux -i unix
```

Bei der Verwendung des RPM-Pakets befindet sich automatisch auf Ihrem System ein Startskript `/etc/rc.d/init.d/msyslog`, das die Startoptionen aus der Datei `/etc/sysconfig/msyslog` liest. Diese Datei enthält folgende Optionen:

```
CONFIG="" # example: "-f /etc/syslog.conf"
```

```
DEBUG="" # example: "-d 20"
MARK="" # example: "-m 20"
IM_BSD="" # example: "-i bsd"
IM_DOORS="" # example: "-i doors"
IM_LINUX="-i linux" # example: "-i linux"
IM_STREAMS="" # example: "-i streams"
IM_TCP="" # example: "-i tcp accepted.host.com 514"
IM_UDP="" # example: "-i udp:514"
IM_Unix="-i unix" # example: "-i unix"
# Look in the im_*.8 man pages for more details on these options
```

Hier sind bereits standardmäßig die beiden Module eingetragen. Daher genügt es, lediglich den klassischen `syslog`-Dienst zu deaktivieren und den `msyslog` zu aktivieren. Dies erfolgt bei den meisten Linux-Distributionen recht einfach mit:

```
# chkconfig --del syslog
# chkconfig --add msyslog
# chkconfig msyslog on
```

Nutzung der neuen Fähigkeiten

Wenn Sie den Standard-BSD-Syslog durch den modularen Syslog austauschen, so ergeben sich noch keine Vorteile. Sie müssen die zusätzlichen Funktionen des modularen Syslog aktivieren, damit sie genutzt werden können. Hierzu sind Anpassungen der Konfigurationsdatei `/etc/syslog.conf` und des Starts des `msyslogd` erforderlich. Zunächst werde ich die unterschiedlichen Optionen beim Aufruf erläutern, bevor ich die Anpassung der Konfigurationsdatei beschreiben werde. Abschließen werde ich die Betrachtung mit der Integritätsüberprüfung der Protokolldateien mit dem `peochk`-Befehl.

Beim Aufruf des `msyslogd` können Sie die folgenden Optionen angeben:

- `-d level`. Debugging-Level
- `-f file`. Konfigurationsdatei (Default: `/etc/syslog.conf`)
- `-m interval`. Intervall in Minuten zwischen *–MARK–* Meldungen (Default: 20, 0 schaltet ab). Diese sehr nützliche Funktion schreibt auch dann eine Meldung in die Protokolldatei, wenn es nichts zu protokollieren gibt. Damit können Sie überprüfen, ob Ihr Protokollserver tatsächlich läuft.
- `-u`. Annahme von Meldungen über den UDP-Port (ähnlich `-r` bei BSD Syslogd)
- `-i module`. Auswahl der Eingabe-Module

Hierbei stehen nun folgende Eingabe-Module zur Verfügung:

- `bsd`. Kernel-Meldungen eines BSD-Systems
- `doors [pfad]`. Eingabe-Modul für Doors Inter Process Call-(IPC-)Meldungen (Solaris)

- `streams [pfad]`. Eingabe-Modul für Streams Inter Process Call-(IPC-)Meldungen
- `tcp`. Eingabe-Modul für Meldungen über TCP-Verbindungen

  `udp`. Eingabe-Modul für Meldungen über UDP-Verbindungen
  - `-h host`. Nimmt auf der Adresse Anfragen an
  - `-p port`. TCP-Port, der geöffnet wird
  - `-a`. Extrahiert den Rechnernamen (FQDN)
  - `-q`. Extrahiert den Rechnernamen (nicht FQDN)

  `file`. Liest aus einer Datei oder Pipe
- – `-f datei`. Liest aus der angegebenen Datei
  - `-p pipe`. Liest aus der angegebenen Pipe
  - `-n Name`. Legt den Namen fest
- `unix [pfad]`. Liest aus einem Unix-Socket (Default: `/dev/log`)
- `linux`. Liest die Linux-Kernel-Meldungen
  - `-c level`. Setzt den Log-Level für die Konsole
  - `-C level`. Definiert den Log-Level eines laufenden *msyslog* neu und beendet sich
  - `-k ksyms`. Kernel-Symboltabelle (Default: `/proc/ksyms`)
  - `-s`. Verwendet das Syscall-Interface (Default: `/proc/kmsg`)
  - `-x`. Keine Übersetzung der Kernel-Symbole

Um nun den *msyslogd* auf einem lokalen Rechner als Protokolldienst einzusetzen, genügt meist die Angabe von:

```
msyslogd -i unix -i linux
```

Haben Sie eine Anwendung, zum Beispiel einen DNS-Server, in einem chroot-Verzeichnis installiert, so benötigt dieser Dienst einen Unix-Socket zur Protokollierung. Er ist nicht in der Lage, aus seinem chroot-Verzeichnis auf den Unix-Socket `/dev/log` zuzugreifen. Dann starten Sie den `msyslogd` mit:

```
msyslogd -i unix -i 'unix /chroot_dns/dev/log' -i linux
```

Der `msyslogd` wird dann beim Start den zusätzlichen Unix-Socket anlegen.

Wenn Sie den `msyslogd` als netzwerkfähigen Logserver starten möchten, so nutzen Sie folgende Startzeile:

```
msyslogd -i unix -i linux -i 'tcp -p 8000'
```

Hierbei müssen Sie jedoch beachten, dass die Übertragung mit UDP wie auch mit TCP unverschlüsselt und nicht authentifiziert erfolgt. Zur Sicherheit können Sie zusätzlich *stunnel* einsetzen.

```
msyslogd -i unix -i linux -i 'tcp -h localhost -p 8001'
stunnel -d 8000 -r localhost:8001
```

Weitere Informationen über *stunnel* finden Sie auf der Stunnel-Homepage *http://www.stunnel.org*.

Bei der Anpassung der Konfigurationsdatei `/etc/syslog.conf` an die neuen Fähigkeiten ist sicherlich die Signatur der Protokolle mit dem PEO-Protokoll die wichtigste Funktion. Wir werden zunächst jedoch die weiteren Ausgabe-Module betrachten und zum Schluss die Signatur besprechen.

Zur Kompatibilität mit dem Standard-BSD-Syslog verfügt der *msyslogd* über das Modul `%classic`. Dieses Modul verfügt über die identischen Fähigkeiten. Es erlaubt die Protokollierung in einer Datei bei Angabe eines Dateinamens (`%classic /var/log/messages`). Die Protokollierung auf den Terminals sämtlicher angemeldeter Benutzer erfolgt mit `%classic *`, und über eine kommaseparierte Liste können bestimmte Benutzer ausgewählt werden (z.B. `%classic xapfel,ybirne,zorange`). Eine Protokollierung über das Netz auf einem anderen syslog-Server erfolgt mit der Angabe von `%classic @logserver.example.net`.

Zusätzlich ist der *msyslogd* in der Lage, auf einem beliebigen UDP- oder TCP-Port die Protokollierung durchzuführen. Im Zusammenhang mit der Protokollierung über TCP bietet sich die Verschlüsselung mit *stunnel* an (s.o.). Das Modul `%udp` unterstützt hierbei die Angabe des Rechners (`-h`) und des Ports (`-p`). Zusätzlich kann mit der Option `-a` definiert werden, ob der eigene Rechnername in der Meldung übertragen wird. Beispiel:

```
kern.info    %udp -a -h logserver.example.net -p 514
```

Das Modul `%tcp` unterstützt zusätzlich zu diesen die weiteren Optionen `-m` und `-s`. Hiermit ist es möglich, eine maximale Zeit für Verbindungswiederholungen in Sekunden zu definieren und einen Puffer für die Aufnahme der noch nicht gesandten Meldungen zu generieren.

```
# TCP-Verbindung zu logserver, Retry 30 Sekunden, Puffer 16384 Bytes
kern.info    %tcp -a -h logserver.example.net -p 8000 -m 30 -s 16384
```

Bei der Wahl zwischen UDP und TCP ist zu berücksichtigen, dass UDP-Pakete verloren werden können. Allerdings erzeugt TCP einen zusätzlichen Overhead, der auch zu einer Überlastung bei vielen Log-Quellen führen kann. Dennoch bieten weitere Werkzeuge (z.B. stunnel) die Möglichkeit, TCP-Verbindungen mit SSL zu verschlüsseln. Dies ist bei UDP nicht möglich.

Ein weiteres sehr interessantes Ausgabe-Modul ist `%regex`. Hiermit können Sie die Sortierung der Meldungen in Abhängigkeit von einem regulären Ausdruck steuern.

Der normale BSD-Syslog erlaubt lediglich eine Verwaltung der Protokollmeldungen über die Angabe der *facility* und der *priority*. Eine feinere Verwaltung der Meldungen und ihre Aufteilung auf unterschiedliche Protokolldateien ist nicht möglich.

Der *msyslogd* ermöglicht mit dem Modul `%regex` die Verwendung von regulären Ausdrücken als Filter. Diese können getrennt auf die Nachricht (`-m`), den Rechnernamen (`-h`), das Datum (`-d`) und die Uhrzeit (`-t`) angewendet werden. Sie können auch den regulären Ausdruck mit `-v` invertieren (ähnlich `grep`).

Möchten Sie, dass auf einem zentralen Protokollserver die Protokolle für die verschiedenen Protokollclients (client1 und client2) in unterschiedlichen Dateien abgelegt werden, so können Sie das durch folgende Einträge erreichen:

```
*.*          %regex -h 'client1' %classic /var/log/client1.messages
*.*          %regex -h 'client2' %classic /var/log/client2.messages
```

Alle Meldungen, die im Host-Anteil nun den Namen *client1* tragen, werden mit dem `%classic`-Modul in der Protokolldatei `/var/log/client1.messages` abgespeichert.

Das Modul `%regex` erlaubt so eine sehr feinfühlige Verteilung der Meldungen auf unterschiedliche Protokolldateien und -server.

Zwei weitere Module, die die Auswertung der Protokollmeldungen vereinfachen können, sind `%pgsql` und `%mysql`. Hiermit können Sie die Syslog-Meldungen direkt in einer Datenbank protokollieren. Dies erlaubt später eine einfache Suche und Korrelation der Daten. Zusätzlich können Sie mit anderen Systemen recht einfach eine Auswertung der Daten (z.B. Apache/PHP-gestützt) vornehmen. Im Folgenden soll kurz die Konfiguration der Protokollierung in einer MySQL-Datenbank beschrieben werden.

Um die Protokollierung des `msyslogd` in einer Datenbank zu ermöglichen, ist es zunächst erforderlich, den MySQL-Datenbankserver und -client zu installieren. Dies erfolgt am einfachsten mit den Werkzeugen der Distribution. Nach der Installation und dem Start des MySQL-Datenbankservers müssen Sie das Kennwort des Datenbankadministrators root ändern. Dies erfolgt mit dem Befehl `mysqladmin`. Ein Beispielaufruf ist im Folgenden abgedruckt:

```
# mysqladmin -u root password "n3u3sk3nnw0rt"
```

Nun sollte die Datenbank für die Protokollierung durch *msyslogd* angelegt werden. Dies erfolgt mit den Befehlen:

```
# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12 to server version: 3.23.49

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> CREATE DATABASE syslog;
Query OK, 1 row affected (0.01 sec)

mysql> use syslog;
```

```
Database changed
mysql>  CREATE TABLE syslogTB (
    -> facility char(10),
    -> priority char(10),
    -> date date,
    -> time time,
    -> host varchar(128),
    -> message text,
    -> seq int unsigned auto_increment primary key
    -> );
Query OK, 0 rows affected (0.00 sec)
mysql> GRANT INSERT ON syslog.* TO msyslogd IDENTIFIED BY 'kennwort';
Query OK, 0 rows affected (0.00 sec)

mysql> quit;
Bye
```

Nun kann `msyslogd` in diese Datenbank protokollieren. Hierzu müssen Sie ihm nur noch mitteilen, wie die Datenbank heißt und wie er sich verbinden muss.

```
*.* %mysql -s host:port -u msyslogd -p kennwort -d syslog \
                      -t syslogTB -F -P
```

Die beiden Module `%mysql` und `%pgsql` benötigen identische Datenbankschemata und unterstützen auch die gleichen Optionen. Diese Optionen haben hierbei die folgende Bedeutung:

- `-s host:port`. MySQL-Server. Der Port ist optional.
- `-u user`. MySQL-Benutzer. Dieser Benutzer muss das Recht haben, Einträge hinzuzufügen.
- `-p password`. Klartextkennwort. Achtung: Diese Datei sollte anschließend nicht für alle Benutzer lesbar sein!
- `-d database`. Name der Datenbank
- `-t table`. Name der Tabelle in der Datenbank
- `-D`. Verzögerte Einfügungen (*Nur MySQL*: Hierbei erhält der Client sofort eine Bestätigung. Der tatsächliche Insert erfolgt verzögert. Dies beschleunigt die Zusammenarbeit mit MySQL!)
- `-F`. Trage `facility` in einer eigenen Spalte ein
- `-P`. Trage `priority` in einer eigenen Spalte ein

Das interessanteste Modul beim Einsatz des `msyslogd` ist jedoch sicherlich das Modul `%peo`. Dieses PEO-Modul verkettet die einzelnen Meldungen in einer Protokolldatei miteinander. Eine Modifikation der Protokolle wird daher später auffallen. Hierzu kann das Modul die Hash-Algorithmen MD5, SHA-1 (Default) oder RIPEMD160 einsetzen.

Um diese Verkettung durchzuführen, verknüpft das Modul einen Schlüssel mit der ersten Meldung. Das Ergebnis wird wieder als Schlüssel für die nächste Meldung abgelegt. Bei der Überprüfung der Protokolldatei wird dieser Vorgang wiederholt. Damit Sie die Überprüfung durchführen können, speichern Sie den initialen Schlüssel an einem sicheren Ort. Die Konfiguration des Moduls `%peo` bietet drei Optionen:

- `-k key`. Schlüssel, der für die Verknüpfung der nächsten Meldung verwendet wird
- `-l`. Line Corruption Mode. Dieser Modus erlaubt es, die Zeile zu erkennen, auf der die erste Modifikation erfolgte. Hierzu wird eine zweite Datei angelegt. Diese Datei trägt denselben Namen wie die Schlüsseldatei mit der zusätzlichen Endung `.mac`.
- `-m hash`. Hash-Methode. Möglich sind `md5`, `sha1` und `rmd160`. Default ist `sha1`.

Eine Beispielkonfiguration des Moduls `%peo` könnte bei Ihnen so aussehen:

```
*.*     %peo -l -k /var/ssyslog/.var.log.messages.key  %classic /var/log/messages
```

Damit diese Verkettung erfolgen kann, ist jedoch ein Initialisierungsvektor erforderlich. Sie erzeugen den initialen Schlüssel mit dem Befehl `peochk`.

Um den initialen Schlüssel zu generieren, geben Sie folgenden Befehl ein:

```
# mkdir /var/ssyslog
# peochk -g -f /var/ssyslog/.var.log.messages.key -i messages.key0
```

Der Befehl `peochk` generiert nun einen Schlüssel und legt diesen in Binärformat in der Datei `/var/ssyslog/.var.log.messages.key` ab. In ASCII-Format wird der Schlüssel in der Datei `messages.key0` erzeugt. Diese ASCII-Datei sollten Sie kopieren oder ausdrucken und vom Rechner entfernen.

Anschließend müssen Sie die Protokolldatei rotieren, denn das Modul `%peo` funktioniert nur, wenn es mit einer leeren (aber vorhandenen) Protokolldatei beginnt.

Die Integrität der Protokolldatei testen Sie ebenfalls mit dem `peochk`-Werkzeug. Hierzu müssen Sie zunächst die Datei `messages.key0` zur Verfügung stellen. Dies kann zum Beispiel mit einer Diskette erfolgen. Auf dem Rechner sollte die Datei gelöscht werden und nicht ständig zur Verfügung stehen!

```
# peochk -f /var/log/messages -i messages.key0 -k /var/ssyslog/.var.log.messages.key
(0) /var/log/messages file is ok
```

Der Befehl `peochk` unterstützt noch einige weitere Optionen. Die Erläuterung dieser Optionen finden Sie in der Manpage. Hier erwähnen möchte ich nur die Option `-q` für quiet. Beim Aufruf mit dieser Option gibt der Befehl eine 0 aus, wenn die Datei nicht verändert wurde. Ansonsten gibt der Befehl eine 1 und die Nummer der Zeile (-l) aus, auf der die Korruption auftritt. Damit bietet sich diese Option für den Aufruf in Skripten an.

10.3 Syslog-ng

Der Syslog-ng (*http://www.balabit.com/products/syslog_ng/*) ist eine weitere Alternative zu dem BSD-Syslog. Der Syslog-ng wird von der ungarischen Firma Balabit für ihr Firewall-Produkt Zorp entwickelt. Der Syslog-ng ist Open Source und wird unter der GPL-Lizenz vertrieben. Wenn Sie den Syslog-ng einsetzen möchten, müssen Sie sich von dem üblichen Format der Syslog-Konfiguration verabschieden. Der Syslog-ng verwendet ein eigenes, vollkommen anderes Format. Dafür gewinnen Sie aber auch einige sehr mächtige Vorteile gegenüber dem BSD-Syslog:

- Bessere Filterfunktionen inklusive regulären Ausdrücken
- Transport der Meldungen per UDP oder TCP
- Protokollierung in einer MySQL- oder PostgreSQL-Datenbank
- Die Unterstützung langer Rechnernamen erlaubt eine einfachere Zuordnung der Meldungen
- Saubere und klare Konfigurationsdatei

Die Installation des Syslog-ng ist recht einfach, da es für fast jede Distribution bereits fertige binäre Pakete gibt.

Tipp

Besonders einfach ist für Sie die Installation und Konfiguration des Syslog-ng, wenn Sie eine SUSE-Distribution einsetzen. SUSE unterstützt direkt über YaST die Installation und auch die Konfiguration von Syslog-ng. Sie brauchen nichts weiter zu tun, als den Syslog-ng in YaST auszuwählen.

Ab Fedora Core 4 unterstützt auch Red Hat den Syslog-ng. Für die kommerziellen RHEL-Versionen finden Sie auf der Syslog-ng Homepage binäre Pakete. Wenn Sie dennoch Syslog-ng aus seinen Quellen übersetzen möchten, können Sie das einfach mit den folgenden Befehlen erreichen:

```
$ ./configure
$ make
$ sudo make install
```

Um den Syslog-ng komfortabel über ein Init-Skript zu starten, können Sie eines der mitgelieferten Init-Skripten aus dem Verzeichnis `./contrib` verwenden.

Achtung

Für die Übersetzung benötigen Sie zusätzlich das libol-Paket. Dieses Paket erhalten Sie auf *http://www.balabit.com/downloads/libol/0.3/*. Übersetzen und installieren Sie dieses Paket zuerst!

Außerdem gibt es teilweise Probleme mit der Flex-Version. Ab Version 2.5.4 schlägt die Kompilierung teilweise fehl. Die Syslog-ng-FAQ gibt hier weitere Hinweise (*http://www.campin.net/syslog-ng/faq.html*).

Tipp

Bei der Konfiguration des Syslog-ng-Quelltext-Pakets können Sie einige optionale Funktionen aktivieren. Hierbei handelt es sich sowohl um Unterstützung für Sun Solaris-Betriebssysteme (`--enable-sun-streams` und `--enable-sun-door`) als auch um die Unterstützung für TCPwrapper (`--enable-tcp-wrapper`) und Source-Spoofing (`--enable-spoof-source`).

Nun müssen Sie noch den Syslog-ng konfigurieren. Der Syslog-ng verfolgt in seiner Konfigurationsdatei eine andere Philosophie als der BSD-Syslog und der modulare Syslog. Sie definieren zunächst die Quelle (Source) einer Meldung. Eine typische Quelle ist:

```
source src { unix-stream("/dev/log"); };
```

Anschließend definieren Sie einen oder mehrere Filter und dann die möglichen Ziele:

```
filter mail { facility("mail") and level ("info"); };
destination mail_file { file("/var/log/mail"); };
```

Wenn Sie Quellen, Filter und Ziele definiert haben, können Sie einen Protokollpfad (log path) definieren. Dieser Protokollpfad beschreibt, dass Meldungen aus einer bestimmten Quelle, auf die ein bestimmter Filter zutrifft, in einem bestimmten Ziel protokolliert werden sollen:

```
log { source(src);
      filter(mail);
      destination(mail_file); };
```

Da das Syslog-ng-Handbuch sehr ausführlich ist, werde ich mich hier nur auf die Beschreibung einiger spezieller Punkte beschränken. Zunächst möchte ich Ihnen eine typische Syslog-ng-Konfigurationsdatei für ein Linux-System vorstellen und erklären:

```
######
# options

options {
        # disable the chained hostname format in logs
        # (default is enabled)
        chain_hostnames(no);

        # enable fully qualified hostnames
        # (default is disabled)
use_fqdn(yes);

        # keep the original hostname
# (default disabled)
keep_hostname(yes);

        # which time to log: original (default) or received
#use_time_recvd(no);

        # the time to wait before a died connection is re-established
        # (default is 60)
        time_reopen(10);

        # the time to wait before an idle destination file is closed
        # (default is 60)
        time_reap(360);

        # the number of lines buffered before written to file
        # you might want to increase this if your disk isn't catching with
        # all the log messages you get or if you want less disk activity
        # (say on a laptop)
        # (default is 0)
        #sync(0);

        # the number of lines fitting in the output queue
        log_fifo_size(2048);

        # enable or disable directory creation for destination files
        create_dirs(yes);

        # default owner, group, and permissions for log files
        # (defaults are 0, 0, 0600)
        #owner(root);
        #group(root);
        #perm(0600);
```

```
        # default owner, group, and permissions for created directories
        # (defaults are 0, 0, 0700)
        #dir_owner(root);
        #dir_group(root);
        dir_perm(0700);

        # enable or disable DNS usage
        # syslog-ng blocks on DNS queries, so enabling DNS may lead to
        # a Denial of Service attack
        # (default is yes)
        use_dns(no);

        # maximum length of message in bytes
        # this is only limited by the program listening on the /dev/log Unix
        # socket, glibc can handle arbitrary length log messages, but -- for
        # example -- syslogd accepts only 1024 bytes
        # (default is 2048)
        #log_msg_size(2048);
};



# sources

source s_local {
        # message generated by Syslog-NG
        internal();
        # standard Linux log source (this is the default place for the syslog()
        # function to send logs to)
        unix-stream("/dev/log");
        # messages from the kernel
        file("/proc/kmsg" log_prefix("kernel: "));
};

source s_external {
        # tcp socket
        tcp ( ip(0.0.0.0) port(5140) keep-alive(yes));
};

# destinations

# some standard log files
destination df_auth { file("/var/log/auth.log"); };
destination df_syslog { file("/var/log/syslog"); };
```

```
destination df_cron { file("/var/log/cron.log"); };
destination df_daemon { file("/var/log/daemon.log"); };
destination df_kern { file("/var/log/kern.log"); };
destination df_mail { file("/var/log/mail.log"); };
destination df_user { file("/var/log/user.log"); };


destination df_messages { file("/var/log/messages"); };

# consoles
# this will send messages to everyone logged in
destination du_all { usertty("*"); };

# all messages from external
destination d_external { file("/var/log/external"); };

######
# filters

# all messages from the auth and authpriv facilities
filter f_auth { facility(auth, authpriv); };

# all messages except from the auth and authpriv facilities
filter f_syslog { not facility(auth, authpriv); };

# respectively: messages from the cron, daemon, kern, lpr, mail, news, user,
# and uucp facilities
filter f_cron { facility(cron); };
filter f_daemon { facility(daemon); };
filter f_kern { facility(kern); };
filter f_mail { facility(mail); };
filter f_user { facility(user); };


filter f_at_least_info { level(info..emerg); };

# all messages of info, notice, or warn priority not coming form the auth,
# authpriv, cron, daemon, mail, and news facilities
filter f_messages {
        level(info,notice,warn)
            and not facility(auth,authpriv,cron,daemon,mail,news);
};

# messages with priority emerg
filter f_emerg { level(emerg); };
```

```
######
# logs
# order matters if you use "flags(final);" to mark the end of processing in a
# "log" statement

log {
        source(s_local);
        filter(f_auth);
        destination(df_auth);
};

log {
        source(s_local);
        filter(f_syslog);
        destination(df_syslog);
};

log {
        source(s_local);
        filter(f_cron);
        destination(df_cron);
};

log {
        source(s_local);
        filter(f_daemon);
        destination(df_daemon);
};

log {
        source(s_local);
        filter(f_kern);
        destination(df_kern);
};


log {
        source(s_local);
        filter(f_mail);
filter(f_atleast_info);
        destination(df_mail);
};
```

```
log {
        source(s_local);
        filter(f_user);
        destination(df_user);
};

log {
        source(s_local);
        filter(f_messages);
        destination(df_messages);
};

log {
        source(s_local);
        filter(f_emerg);
        destination(du_all);
};

log {
        source(s_external);
        destination(d_external);
};
```

Sie beginnen mit der Konfiguration der Optionen des Syslog-ng. Einige Optionen sind beispielhaft aufgeführt. In dem Syslog-ng-Handbuch finden Sie alle unterstützten Optionen. Interessant auf einem Syslog-ng-Logserver, der auch von außen Meldungen entgegennimmt, ist die Option `keep_hostname`. Damit protokolliert der Syslog-ng den originalen Hostnamen des Rechners, der die Meldung gesendet hat, anstelle seines eigenen. Die Option `use_fqdn` protokolliert dann auch den vollqualifizierten Hostnamen, so dass die Rechner leichter auseinander gehalten werden können.

Anschließend definieren Sie die Protokollquellen. Hier wurde eine Quelle für lokale Meldungen (`s_local`) und eine Quelle für Meldungen, die über TCP transportiert werden, definiert. Der Syslog-ng öffnet nun einen TCP-Socket auf dem Port 5140 und nimmt hier Protokollmeldungen von außen entgegen. Wenn Sie den Syslog-ng mit der Option `--enable-tcp-wrapper` übersetzt haben, können Sie in den Dateien `/etc/hosts.allow` und `/etc/hosts.deny` festlegen, welche Rechner Protokollmeldungen zustellen dürfen. Damit zum Beispiel nur das lokale Netzwerk 192.168.0.0/24 auf den Syslog-ng-Server zugreifen darf, verwenden Sie folgende Zeile in der Datei `/etc/hosts.deny`:

```
syslog-ng: ALL EXCEPT 192.168.0.0/255.255.255.0
```

Nach den Quellen definieren Sie die Filter und die Ziele, wo die Protokollmeldungen gespeichert werden sollen. Hier wurden nur eine kleine Menge von typischen

Filtern und Zielen definiert. Sämtliche über das Netzwerk empfangenen Nachrichten werden komplett in einer eigenen Datei abgelegt. Die lokalen Meldungen werden wie üblich auf verschiedene Dateien aufgeteilt.

Der Syslog-ng kann auch eine Protokollierung direkt in einer Datenbank vornehmen. Hierzu unterstützt der Syslog-ng die MySQL- und die PostgreSQL-Datenbank. Damit Sie die Meldungen anschließend komfortabel betrachten können, existieren verschiedene in PHP geschriebene Oberflächen für die Verwaltung der Meldungen. Ich möchte Ihnen hier nur eine Oberfläche vorstellen:

- php-syslog-ng: *http://www.phpwizardry.com/php-syslog-ng.php*. Dies ist die aktive Weiterentwicklung des originalen php-syslog-ng von dieser Seite: *http://www.vermeer.org/projects/php-syslog-ng*. Es bietet einen sehr mächtigen Zugriff auf die in der MySQL-Datenbank gespeicherten Daten (siehe Abbildung 10.1).

Um diese Funktion zu nutzen, müssen Sie zunächst den Syslog-ng so konfigurieren, dass er seine Meldungen in die Datenbank schreibt. Hierzu benötigen Sie zunächst ein Ziel (Destination), das die Meldungen in die Datenbank schreibt:

```
# pipe messages to /var/log/mysql.pipe to be processed by mysql
destination d_mysql {
       pipe("/var/log/mysql.pipe"
       template("INSERT INTO logs
       (host, facility, priority, level, tag, datetime, program, msg)
       VALUES
       ( '$HOST', '$FACILITY', '$PRIORITY', '$LEVEL', '$TAG',
       '$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC','$PROGRAM', '$MSG' );\n")
       template-escape(yes));
};
```

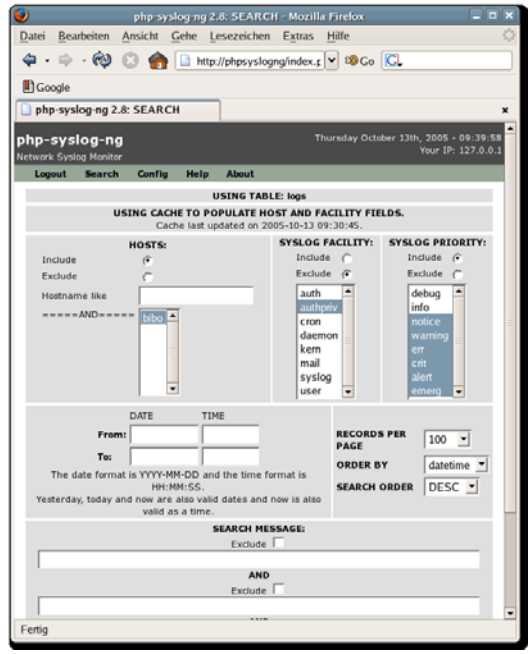
Tipp

Bevor Sie diese Zeilen abtippen, möchte ich Sie darauf hinweisen, dass sich in dem Unterverzeichnis `./scripts` in dem Paket phpsyslogng eine Beispielkonfiguration in der Datei `./scripts/syslog.conf` befindet.

Dieses Ziel schreibt nun die Meldungen in eine Datei `/var/log/mysql.pipe`. Dabei handelt es sich jedoch nicht um eine normale Datei, sondern um eine Pipe. Diese müssen Sie manuell anlegen:

```
$ sudo mkfifo /var/log/mysql.pipe
```

Eine derartige Named-Pipe ähnelt der Pipe (|) auf der Kommandozeile. Ein Prozess schreibt in die Pipe, während ein anderer Prozess die Daten in derselben Reihenfolge ausliest. Da die Daten bereits in der SQL-Sprache in die Pipe geschrieben



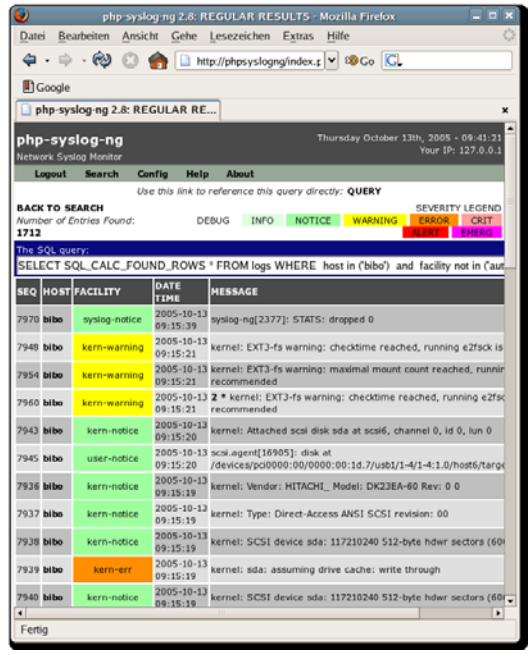


Abbildung 10.1: Mit dem PHP-Frontend php-syslog-ng können Sie komfortabel nach Meldungen suchen und sie betrachten.

werden, benötigen Sie jetzt nur noch ein Programm, das die Daten aus der Pipe ausliest und in die Datenbank schreibt. Das Datenbank-Managementsystem (DBMS) MySQL selbst kann dies nicht. Hierfür genügt aber das folgende einfache Skript `syslog2mysql.sh`:

```
#!/bin/bash

if [ ! -e /var/log/mysql.pipe ]
then
        mkfifo /var/log/mysql.pipe
fi
while [ -e /var/log/mysql.pipe ]
do
        mysql -u syslogfeeder --password=PW_HERE syslog < /var/log/mysql.pipe >/dev/null
done
```

Dieses Skript wird ebenfalls mit phpsyslogng als `./scripts/syslog2mysql.sh` mitgeliefert. Damit dieses Skript jedes Mal nach einem Neustart automatisch aufgerufen wird, kann es sehr einfach über den Cron-Daemon eingebunden werden. Wenn Sie den Vixie-Crond auf Ihrem Linux-System verwenden, so besitzt dieser seit über 10 Jahren die Möglichkeit, jedes Mal nach einem Reboot des Systems einen Befehl zu starten. Tragen Sie einfach folgende Zeile in der Daei `/etc/crontab` ein:

```
@reboot root /usr/local/bin/syslog2mysql.sh >> /var/log/syslog2mysql 2>&1
```

Jetzt müssen Sie noch die Datenbank anlegen. Starten Sie Ihr MySQL-DBMS. Für die Erzeugung der Datenbank enthält die aktuelle Version des phpsyslogng-Pakets in dem Unterverzeichnis `./scripts` eine Datei `scripts/dbsetup.sql`. Sie müssen diese Datei nur in Bezug auf die zu verwendenen Kennwörter anpassen und können dann das Skript aufrufen:

```
$ mysql -u root -p < scripts/dbsetup.sql
```

Nun müssen Sie nur noch im Syslog-ng die Meldungen auswählen, die in der Datenbank protokolliert werden sollen. Hierzu fügen Sie einen Protokollpfad in der Konfigurationsdatei des Syslog-ng hinzu. Am einfachsten ist der folgende Protokollpfad ohne Filter:

```
log { source(src); destination(d_mysql); };
```

Damit Sie später auch der Menge der Protokolleinträge in der Datenbank Herr werden, hat Claus Lund, der Entwickler von phpsyslogng ein Rotationsskript (`./scripts/logrotate.php`) geschrieben, das täglich die Log-Tabelle in der Datenbank umbenennt und eine neue Tabelle beginnt. Dieses Skript müssen Sie in Bezug auf den Installationsort von phpsyslogng anpassen:

```
$APP_ROOT = '/var/www/phpsyslogng';
```

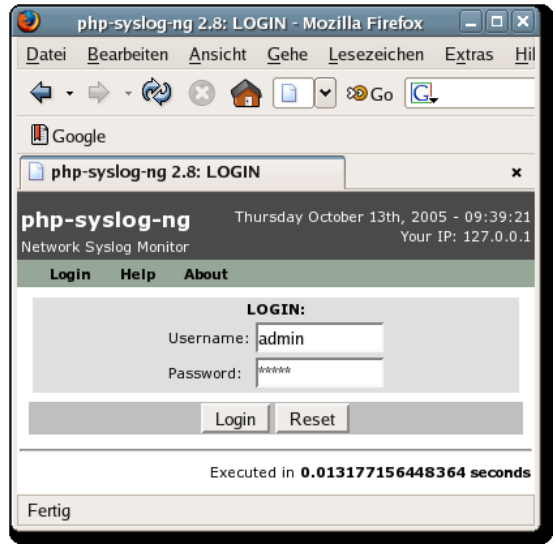


Abbildung 10.2: Bei dem ersten Login melden Sie sich mit admin/admin an.

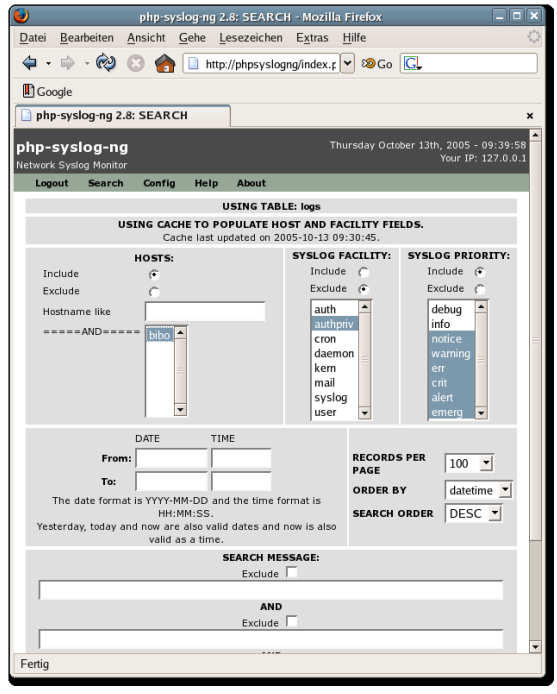


Abbildung 10.3: Eine mächtige Suchmaske erlaubt Ihnen das Eingrenzen der gewünschten Meldungen.

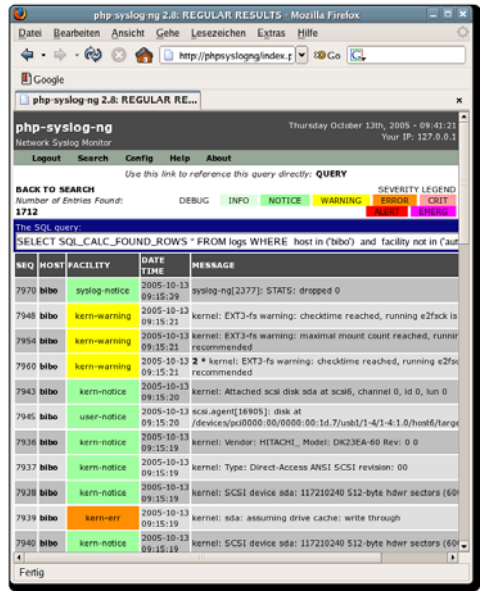


Abbildung 10.4: Die Ergebnisse werden in Farbe dargestellt.

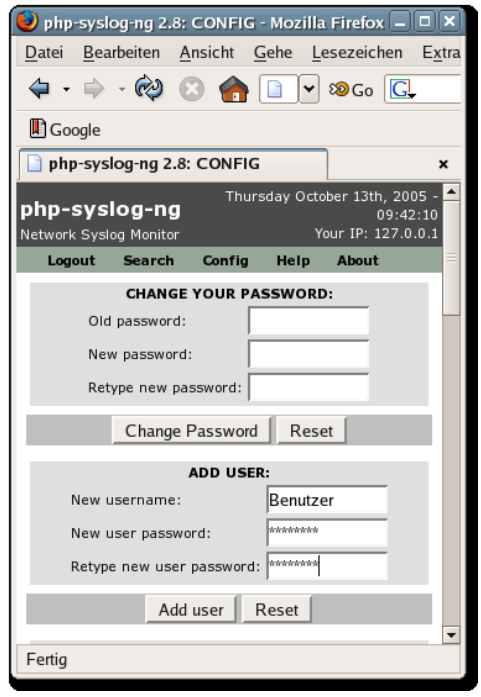


Abbildung 10.5: Für die tägliche Arbeit können Sie auch zusätzliche Benutzer anlegen.

Zusätzlich empfehle ich auch noch folgendes Skript, das ein Backup der Datenbank durchführt:

```
#!/bin/bash
# make sure you have directory /var/log/backup created with mask 600
/usr/bin/mysqlhotcopy --user=syslogadmin --password=g3h31m --allowold syslog
/var/log/backup
```

Diese Skripten können Sie ebenfalls über den Cron-Daemon aufrufen. Fügen Sie dazu folgende Zeilen Ihrer Cron-Tabelle `/etc/crontab` hinzu:

```
@daily   root /usr/local/bin/mysql-backup.sh >> /var/log/syslog2mysql 2>&1
```

Da sämtliche Skripten das Kennwort für den Zugriff auf die Datenbank enthalten, sollten Sie die Rechte so setzen, dass nur root diese Skripten lesen und verwenden darf!

Die restliche Konfiguration von phpsyslogng ist recht einfach. Beginnen Sie damit, dass Sie den phpsyslogng-Quelltextbaum in das DocumentRoot-Verzeichnis Ihres Webservers kopieren. Vielleicht legen Sie auch ein neues Verzeichnis an und erzeugen in dem Apache einen VirtualHost für dieses Verzeichnis. Anschließend müssen Sie lediglich die Datei `./config/config.php` anpassen. Hier sollten Sie darauf achten, dass Sie sämtliche Kennwörter wieder richtig anpassen. Haben Sie alles richtig gemacht, können Sie sich bereits mit einem Browser verbinden und sehen die Login-Seite von phpsyslogng (Abbildung 10.2).

Bei dem Login können Sie sich mit `Admin/Admin` anmelden. Anschließend können Sie in der Datenbank suchen (Abbildung 10.3), die Ergebnisse betrachten (Abbildung 10.4) und weitere Benutzer anlegen (Abbildung 10.5).

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

11 Zentrale Zeitsynchronisation

Wenn Sie Ihre Firewall-Protokolle später auswerten möchten und vielleicht auch noch mit Protokollen Ihres Webservers und Ihres Intrusion-Detection-Systems korrelieren möchten, ist es wichtig, dass die Protokolle über eine einheitliche Zeitbasis verfügen. Um dies zu erreichen, führt kein Weg an einem zentralen Zeitserver vorbei, der die Systeme mit der korrekten Uhrzeit versorgt. Dieses Kapitel zeigt Ihnen, wie Sie einen Zeitserver aufsetzen und Ihre Systeme damit synchronisieren.

11.1 Das Zeitsynchronisationsprotokoll NTP

Viele Systemadministratoren verschwenden keinen Gedanken an zentrale Zeitsynchronisation. Dabei ist die zentrale Zeitsynchronisation sämtlicher Netzwerkkomponenten im Falle eines sicherheitsrelevanten Ereignisses (Incident) von größter Bedeutung. Wie wollen Sie die Protokolle auswerten, wenn die Zeiten in den Protokollen des angegriffenen Webservers, der Datenbank, der Firewall und den Intrusion-Detection-Systems nicht zusammenpassen? Wollen Sie raten, was zuerst passiert ist? Auch die normale Auswertung von Protokollen ist bei nicht synchroner Zeit schwierig. Wie möchten Sie die Laufzeit einer E-Mail über zwei oder drei Mail-Relays ermitteln, wenn alle Systeme eine unterschiedliche Zeitbasis verwenden?

Um dieses Problem zu lösen, ist bereits vor langer Zeit das Network Time Protocol (NTP) geschaffen worden. Aktuell ist die Version 4 des Protokolls, das mit der Version 3 (RFC 1305) und den Versionen 1 (RFC1059) und 2 (RFC1119) kompatibel ist. Die wesentliche Neuerung des Protokolls Version 4 ist die Unterstützung von asymmetrischer Kryptographie und IPv6. Die Version 4 ist bisher nicht in einem RFC beschrieben worden. Es existiert lediglich ein Draft (*http://tools.ietf.org/wg/ntp/draft-ietf-ntp-ntpv4-proto/draft-ietf-ntp-ntpv4-proto-00.txt*), der das Protokoll beschreibt. Alternativ zu dem NTP-Protokoll existiert auch das Simple-Network-Time-Protocol (SNTP), das dem NTP-Protokoll ähnlich ist, aber weniger Funktionen besitzt und einfacher zu implementieren ist.

Das NTP-Protokoll verwendet zum Transport der Informationen den UDP-Port 123. Ungewöhnlicherweise verwendet das Protokoll diesen Port sowohl als Client wie auch als Server. Die Zeitinformationen können per Unicast, Multicast und Broadcast verteilt werden. Leider bietet das UDP-Protokoll keinerlei Schutz vor Spoofing oder Modifikation der transportierten Informationen. Hierfür kann ab der Version 4 die asymmetrische Kryptographie zum Schutz der Integrität und Authentizität eingesetzt werden.

Das NTP-Protokoll wird beim Zugriff eines NTP-Clients auf einen NTP-Server eingesetzt. Als NTP-Server kann jedes System eingesetzt werden, das über eine genaue Zeit verfügt. Die Zeitquelle kann eine DCF-77-Uhr sein, wie zum Beispiel die Expert Mouseclock von GUDE ANALOG- und DIGITALSYSTEME GmbH (*http://www.gude.info*). Alternativ können Sie auch eine GPS-Maus nutzen. Achten Sie nur darauf, dass das Produkt über Linux-Unterstützung verfügt. Natürlich können Sie auch einen oder mehrere andere NTP-Server als Zeitquelle nutzen. Eine Liste von öffentlich frei verfügbaren NTP-Servern finden Sie auf *http://www.pool.ntp.org/* und *http://ntp.isc.org/bin/view/Servers/WebHome*. Die Server werden in Stratum 1,2,3- etc. Server eingeteilt. Ein Stratum-1-Server ist direkt mit einer Hochpräzisionszeitquelle (z.B. Atomuhr) verbunden. Ein Stratum-3-Server synchronisiert sich mit einem Stratum-2-Server, der sich wieder mit einem Stratum-1-Server synchronisiert. Je weiter weg sich ein Server von einem Stratum-1-Server befindet, desto ungenauer ist seine Zeit. Wenn Sie selbst einen Server mit DCF-77-Uhr aufsetzen, ist dies ein Stratum-1-Server. Alle Systeme, die diesen Rechner zur Synchronisation verwenden, sind Stratum-2-Systeme.

Wenn Sie für die Synchronisation Ihres NTP-Servers weitere NTP-Server im Internet verwenden, achten Sie bitte darauf, dass Sie mehrere global verteilte Systeme verwenden. Ansonsten besteht die Gefahr, dass beim Ausfall eines Systems oder bei einer falschen Uhrzeit auf diesem System Ihre Zeitsynchronisation in Mitleidenschaft gezogen wird. Alle Systeme können mehrere Zeitserver zur Synchronisation einsetzen!

11.2 Der ntpd-Zeitserver

Die am häufigsten eingesetzte Software für den Aufbau eines Zeitservers auf der Basis von Linux ist der `ntpd` (früher `xntpd`). Er ist in den meisten Distributionen enthalten und wird von dem Internet Software Consortium entwickelt und gepflegt (*http://ntp.isc.org*). Eine weitere Möglichkeit für den Aufbau eines NTP-Servers ist die Software `openntp` von dem OpenBSD-Projekt (*http://www.openntpd.org*). Dieser Zeitserver ist wesentlich einfacher in seinen Funktionen und in vielen Konfigurationseinstellungen kompatibel. Er unterstützt bisher jedoch nicht NTP Version 4 und damit auch keine Authentifizierung.

Da der `ntpd` in allen aktuellen Distributionen enthalten ist, spare ich mir hier die Beschreibung der Installation aus den Quellen. Sie finden eine Installationsanleitung in dem Quellpaket, falls Sie tatsächlich das Paket manuell installieren möchten. Ansonsten stellen Sie bitte sicher, dass das `ntp`-Paket Ihrer Distribution installiert ist.

Zunächst betrachten wir die Konfiguration des NTP-Servers als Client und anschließend als Server.

11.2.1 Der Client

Das `ntp`-Paket enthält zwei Möglichkeiten, um ein System als Client mit einem Zeitserver zu synchronisieren. Der Kommandozeilenbefehl `ntpdate` führt eine einmalige

Synchronisierung durch. Der Server `ntpd` kann auch als Client eine ständige Synchronisierung des Clients mit einem NTP-Server ermöglichen. Sinnvoll ist daher der Einsatz des `ntpd` als Client, um die ständige Synchronisierung zu gewährleisten. Der `ntpdate`-Befehl wird jedoch in zukünftigen Versionen der Software entfernt werden, da er bereits jetzt durch den Aufruf `ntpd -q` ersetzt werden kann.

Hinweis

Wenn die Zeit des Clients um mehr als 1000 Sekunden von der Zeit des Servers abweicht, weigert sich der `ntpd`, die Zeit zu synchronisieren. Daher wird häufig der Befehl `ntpdate` vor dem Start des `ntpd` aufgerufen. Wenn Sie diesen Befehl durch `ntpd -q` ersetzen möchten, müssen Sie hier zusätzlich `-g` angeben. Diese Option schaltet die 1000-Sekunden-Prüfung ab.

Die Konfiguration des `ntpd` als Client ist sehr einfach. Erzeugen Sie lediglich die folgende Konfigurationsdatei `/etc/ntp.conf`:

```
# Erlaube per Default niemandem die Modifikation, die Abfrage oder
# das Monitoring des Zeitservers
restrict default ignore

# Erlaube alle Funktionen über das Loopback-Interface
restrict 127.0.0.1

# Lokale Drift-Datei, muss schreibbar sein.
driftfile /var/lib/ntp/drift


# Expert Mouseclock
# Generiere Link: ln -s /dev/ttyS0 /dev/refclock-0
# server 127.127.8.0 mode 5

# Server im Internet
server 0.pool.ntp.org
server 1.pool.ntp.org
server 2.pool.ntp.org

# Lokale Uhr
server  127.127.1.0     # local clock
fudge   127.127.1.0 stratum 10
```

Ausgestattet mit dieser Konfigurationsdatei, können Sie Ihren NTP-Server bereits probehalber starten. Natürlich sollten Sie die eingetragenen Server im Internet prüfen und bei Bedarf durch andere ersetzen. Um den NTP-Server probehalber zu starten, geben Sie auf der Kommandozeile zunächst den Befehl `ntpd -q -g` ein. Dies

führt eine einmalige Synchronisation durch. Dieser Vorgang kann einige Sekunden dauern:

```
# ntpd -q -g
ntpd: time set -6.640906s
```

Anschließend geben Sie das Kommando `ntpd` auf der Kommandozeile ein. Es sollte sich scheinbar sofort beenden. Prüfen Sie, ob der Ntpd richtig im Hintergrund läuft, indem Sie sich die laufenden Prozesse anzeigen lassen.

Sie können die Funktion des Ntpd nun mit dem Befehl `ntpdc` auf dem lokalen System überprüfen.

```
# ntpdc
ntpdc> peers
     remote           local      st poll reach  delay   offset    disp
==============================================================================
=216.154.195.60  192.168.255.100  3   64    3 0.15869  0.003562 1.98438
=LOCAL(0)        127.0.0.1       10   64    3 0.00000  0.000000 1.98436
=gatekeeper.no-s 192.168.255.100  1   64    3 0.23141  0.000760 1.98444
=frigg.interstro 192.168.255.100  3   64    3 0.07040  0.001728 1.98438
ntpdc>
```

Der Befehl `ntpdc` erlaubt die komplette Administration des Ntpd-Servers. Sie können Server hinzufügen und entfernen, den aktuellen Zustand betrachten, Rechte ändern etc. Die Manpage gibt Ihnen weitere Auskünfte. Der Befehl `peers` ist der häufigste Befehl, den Sie wahrscheinlich brauchen. Sie können diesen Befehl auch direkt mit `ntpdc -p` aufrufen. Dieser Befehl zeigt Ihnen die aktuellen Peers des Servers und ihre Zustände an. Die erste Spalte gibt Ihnen Auskunft über den Zustand des Peers:

- `+`: Symmetrisch aktiv. Der Rechner sendet regelmäßig Nachrichten an die Adresse und zeigt seine Synchronisationsfähigkeit.
- `-`: Symmetrisch passiv. Der Rechner empfängt symmetrisch aktive Nachrichten.
- `=`: Der Peer wird im Clientmode abgefragt.
- `^`: Broadcasts werden an die Adresse versandt.
- `~`: Broadcasts werden von dieser Adresse empfangen.
- `*`: Mit diesem Server erfolgt aktuell die Synchronisation.

Sobald Sie ein `*` in der ersten Spalte erkennen können, erfolgt eine aktive Zeitsynchronisation mit dem entsprechenden System.

```
# ntpdc -p
     remote           local      st poll reach  delay   offset    disp
==============================================================================
*216.154.195.60  192.168.255.100  3   64   37 0.15869  0.003562 0.66310
=LOCAL(0)        127.0.0.1       10   64   37 0.00000  0.000000 0.66202
```

```
=gatekeeper.no-s 192.168.255.100  1   64   37 0.23141  0.000760 0.66327
=frigg.interstro 192.168.255.100  3   64   37 0.07040  0.001728 0.66351
```

Sobald der NTP-Server als Client zu Ihrer Zufriedenheit läuft, können Sie ihn mit `kill` beenden und über die Startskripten Ihrer Distribution starten. Prüfen Sie bitte, ob der Server anschließend auch tatsächlich läuft. Viele Distributionen verwenden einen eigenen Benutzer für den Betrieb des NTP-Servers und starten ihn in einem Chroot (siehe »Sicherheit«, 11.3). Dabei kann es zu Rechteproblemen kommen. Prüfen Sie die Protokolle Ihrer Distribution, um mögliche Fehlermeldungen zu finden.

11.2.2 Der Server

Die bisher erstellte Konfigurationsdatei erlaubt den Betrieb eines NTP-Servers als Client. Dieser Client wird sich nun ständig mit den verfügbaren Zeitquellen synchronisieren. Häufig möchten Sie aber auch einen eigenen Zeitserver betreiben, so dass sich weitere Clients mit diesem Zeitserver synchronisieren können.

Die bisherige Konfiguration erlaubt es keinem Client, Synchronisationsanfragen an diesen Server zu schicken, und der Server versendet auch keine Broadcast-Pakete. Die Verwendung des Broadcast- oder Multicast-Transports kann ich auch nur empfehlen, wenn Sie gleichzeitig eine Authentifizierung aktivieren (siehe Abschnitt 11.3). Die Gefahr eines gespooften NTP-Angriffs ist ansonsten zu hoch.

Um einen Broadcast-Server zu konfigurieren, müssen Sie die Konfigurationsdatei nur um eine Zeile ergänzen:

```
broadcast 192.168.0.255
```

Wenn ein Client diesen Broadcast-Server nutzen soll, tragen Sie auf dem Client die folgenden beiden Zeilen ein:

```
broadcastclient
broadcastdelay  0.008
```

Um Unicast-Clients zu unterstützen, fügen Sie eine zusätzliche Zeile mit dem `restrict`-Parameter in der Konfigurationsdatei hinzu. Achten Sie darauf, dass Sie bei der Angabe den Clients nur die Abfrage der Synchronisationsinformationen erlauben.

```
restrict 192.168.0.0 mask 255.255.255.0 nomodify notrap
```

Nun dürfen Clients in dem Netzwerk 192.168.0.0/24 diesen NTP-Server als Zeitserver zur Synchronisation nutzen.

11.3 Sicherheit

In einem Firewall-Buch muss beim Einsatz von NTP auch über die Sicherheit des Protokolls, der Server und des Clients gesprochen werden. Dabei müssen zwei Aspekte betrachtet werden:

- Der NTP-Server verwendet den Port 123/udp. Dies ist ein privilegierter Port (< 1224), und er steht daher nur dem Benutzer root zur Verfügung. Der NTP-Server muss daher mit root-Rechten gestartet werden!
- Das NTP-Protokoll nutzt das UDP-Protokoll für den Transport der Informationen. Dieses Protokoll bietet keinen Schutz der Integrität und Authentizität. Ein Spoofing-Angriff ist leicht möglich.

Um die Sicherheit des Servers auf Port 123 zu erhöhen, ist der `ntpd` in der Lage, nach seinem Start die root-Privilegien abzugeben und in ein Chroot-Verzeichnis zu wechseln. Hiermit reduzieren Sie mögliche Gefahren bei einem Angriff auf den Dienst enorm.

Damit der `ntpd` nach dem Start die root-Privilegien abgibt, müssen Sie beim Start mit der Option `-u ntp:ntp` einen unprivilegierten Benutzer und eine unprivilegierte Gruppe übergeben. Sobald sich der NTP-Server an den Port 123/udp gebunden hat, wird er seinen Benutzerkontext entsprechend ändern.

Damit der NTP-Server in einem Chroot-Verzeichnis arbeitet, müssen Sie das Verzeichnis vorbereiten. Hierzu müssen Sie alle Dateien, die der `ntpd` für seine Funktion benötigt, in das Verzeichnis kopieren. Hierbei handelt es sich mindestens um die Datei `ntp.conf` und die Drift-Datei. In Abhängigkeit der Konfiguration sind auch noch die Verzeichnisse `/var/run`, `/var/log` und das `/dev`-Verzeichnis mit lokalen Zeitquellen erforderlich.

Anschließend starten Sie den NTP-Server mit der Option `-T /var/chroot-dir`. Diese Funktion erhöht die Sicherheit nur, wenn der Prozess auch die root-Privilegien abgibt!

Zum Schutz vor direkten Angriffen auf das Protokoll wie Spoofing unterstützt der NTP-Server in der Version 4 des NTP-Protokolls kryptographische Methoden. Um diese zu nutzen, müssen Sie zunächst Schlüssel erzeugen.

Am einfachsten ist die Authentifizierung mit symmetrischen Schlüsseln. Daher soll diese Authentifizierung hier zuerst besprochen werden.

11.3.1 Symmetrische Authentifizierung

Bei der symmetrischen Authentifizierung verfügen beide Authentifizierungspartner über identische Schlüssel. Dies ist sowohl ein Vorteil, denn die Verteilung ist sehr einfach, aber auch gleichzeitig ein Nachteil, da der Schlüssel vertraulich transportiert und gespeichert werden muss und der Austausch mit Dritten problematisch sein kann.

Es gibt vier verschiedene Arten von Schlüsseln:

1. `A`: Einen ASCII-Schlüssel aus maximal 8 Zeichen
2. `M`: Einen ASCII-Schlüssel mit maximal 31 Zeichen
3. `S`: Einen 64-Bit-Wert mit dem niedrigstwertigsten Bit pro Byte als Parität (DES)
4. `N`: Einen 64-Bit-Wert mit dem höchstwertigsten Bit pro Byte als Parität

Die Schlüssel `A` und `M` sind am einfachsten zu handhaben. Diese Schlüssel müssen nun in der Datei `/etc/ntp/keys` abgespeichert werden:

```
1 A ABCDEFGH
2 M qwertzuiopasdfghjklyxcvbnmqwer
```

Jeder Schlüssel in dieser Datei erhält eine Nummer und einen Typ. Über die Nummer des Schlüssels werden diese nun in der Konfigurationsdatei referenziert. Damit ein Client einen Schlüssel für die Verbindung zu einem Server nutzt, muss er zunächst dem Schlüssel vertrauen (trust) und wissen, welchen Schlüssel er für welchen Server verwenden soll:

```
trustedkey 1 2
server 192.168.0.5 key 1
server 192.168.0.7 key 2
```

Der Server benötigt identische Schlüssel und muss ebenfalls den Schlüsseln vertrauen. Wenn Sie die Zeit per Broadcast verteilen möchten, müssen Sie auf dem Server den Schlüssel in der `broadcast`-Zeile definieren und ebenfalls auf dem Client und dem Server den Schlüsseln vertrauen:

```
trustedkey 1 2
broadcast 192.168.0.255 key 1
```

Auf dem Client genügen dann die folgenden Zeilen:

```
broadcastclient
trustedkey 1 2
keys /etc/ntp/keys
```

11.3.2 Asymmetrische Authentifizierung

Die asymmetrische Authentifizierung ist in vielen Umgebungen die bessere Lösung. Sie müssen nun nur die öffentlichen Schlüssel (Public Keys) sämtlicher Systeme untereinander austauschen. So ist es auch einfach möglich, zu dritten Instanzen sichere Verbindungen aufzubauen.

Die asymmetrische Authentifizierung wird beim `ntpd` als *Autokey* bezeichnet. Bei der Konfiguration wird zwischen Broadcast- und Multicast-Autokey und Unicast-Autokey unterschieden. Während das Unicast-Autokey-Verfahren auf dem Client konfiguriert wird, wird das Broadcast- und Multicast-Autokey-Verfahren auf dem Server konfiguriert.

Für das Broadcast-Autokey-Verfahren tragen Sie auf dem Server folgende Zeile ein:

```
broadcast 192.168.0.255 autokey
```

Bei dem Unicast-Autokey-Verfahren tragen Sie auf dem Client folgende Zeile ein:

```
server 192.168.0.5 autokey
```

Zusätzlich benötigen beide Systeme noch die folgenden Zeilen:

```
crypto pw (client|server)password
keysdir /etc/ntp
```

Dann müssen Sie noch die Schlüssel erzeugen und verteilen. Autokey unterstützt drei verschiedene Identitätsschemata: IFF, GQ und MV.

- **IFF.** Bei dem IFF-Identitätsschema werden für jeden Server spezifische Schlüssel erzeugt. Sie müssen diesen Schlüssel für jeden Client exportieren. Dabei kann der Schlüssel wieder mit einem Client-Passwort verschlüsselt transportiert werden.

  Um die IFF-Parameter zu erzeugen, verwenden Sie:
  ```
  cd /etc/ntp
  ntp-keygen -T -I -p serverpassword
  ```

- **GQ.** Bei dem GQ-Identitätsschema wird ein Schlüssel erzeugt, der von allen Systemen in der Gruppe genutzt wird. Die Erzeugung erfolgt mit:
  ```
  cd /etc/ntp
  ntp-keygen -T -G -p serverpassword
  ```

- **MV.** Bei dem MV-Schema erzeugen Sie einen Schlüssel für den Server und N-1 Schlüssel für die Clients.
  ```
  cd /etc/ntp
  ntp-keygen -V N -p serverpassword.
  ```

Für die Erzeugung der Parameter werden ein Server Key und ein Zertifikat erzeugt. Diese sind nur für ein Jahr gültig und müssen anschließend neu erzeugt werden. Dies erfolgt mit `cd /etc/ntp; ntp-keygen -T -q serverpassword`.

Auf dem Client müssen Sie zunächst auch einen Schlüssel und ein Zertifikat erzeugen. Anschließend müssen Sie die entsprechenden Schlüssel der Server nun auch auf dem Client importieren und installieren. Um den Schlüssel und das Zertifikat für den Client zu erzeugen, verwenden Sie:

```
cd /etc/ntp
ntp-keygen -H -p clientpassword
```

- **IFF.** Bei den IFF-Gruppenschlüsseln müssen Sie diese auf den Servern zunächst exportieren. Dazu verwenden Sie den folgenden Befehl:
  ```
  ntp-keygen -e -q serverpassword -p clientpassword
  ```

Diesen so mit dem Client-Password verschlüsselten Schlüssel können Sie nun per E-Mail verschicken oder per Diskette auf den Client transportieren. Speichern Sie den Schlüssel auf dem Client in dem Verzeichnis `/etc/ntp` ab, und erzeugen Sie einen symbolischen Link:

```
cd /etc/ntp
ln -s ntpkey_IFFkey_server.3301264563 ntpkey_iff_server
```

- **GQ.** Kopieren Sie den GQ-Gruppen-Schlüssel sicher auf den Client, und erzeugen Sie ebenfalls eine Verknüpfung.

```
d /etc/ntp
ln -s ntpkey_GQpar_server.3301145293 ntpkey_gq_server
```

- **MV.** Kopieren Sie den auf dem Server erzeugten Client-MV-Schlüssel auf den Client, und erzeugen Sie ebenfalls die Verknüpfung.

```
cd /etc/ntp
ln -s ntpkey_MVkey1_server.3301144193 ntpkey_mv_server
```

Nach einem Neustart der `ntpd`-Daemons auf den Servern und Clients sollten Sie mit dem Kommando `ntpq -p` den Zustand der Synchronisation beobachten.

Mit `ntpq -c` erhalten Sie Informationen über die Authentifizierung:

```
# ntpq -c
nd assID status  conf reach auth condition  last_event cnt
===========================================================
  1 26132  f694   yes   yes   ok   sys.peer   reachable  9
```

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

12 Protokollanalyse

Wenn Sie eine Firewall betreiben, wollen Sie auch wissen, was passiert. Die Protokollanalyse ist eine der wichtigsten Aufgaben des Firewall-Administrators. Daher sollten Sie sich nur mit den besten Werkzeugen zufrieden geben. Leider ist die eierlegende Wollmilchsau in diesem Bereich noch nicht erfunden oder programmiert worden. Dieses Kapitel zeigt Ihnen die Werkzeuge, die ich in meiner Arbeit schätzen gelernt habe, und einige weitere, die ich sehr interessant finde.

12.1 Fwlogwatch

Fwlogwatch ist ein Echtzeit-Protokoll-Analysator speziell für Firewall-Protokolle. Fwlogwatch wird von Boris Wesslowski unter der GPL-Lizenz vertrieben (*http://fwlogwatch.inside-security.de/*). Firewall-Protokolle weisen häufig eine sehr spezielle Syntax auf. Auch wenn Sie ein Linux-Guru sind, gestaltet sich die Erstellung von Zusammenfassungen und speziellen Alarmmeldungen mit Linux-Hausmitteln wie `grep` und `awk` unter Umständen recht kompliziert. Mit Fwlogwatch sind Sie in der Lage, verschiedenste Protokollformate zu analysieren: Linux ipchains, Linux/Iptables, Solaris/BSD/Irix/HP-UX ipfilter, Cisco IOS, Cisco PIX, Windows XP Firewall und Snort IDS. Ich werde mich in diesem Buch aus nahe liegenden Gründen auf Iptables beschränken. Darüber hinaus können Sie mit diesem Werkzeug (gzip-)komprimierte Protokolldateien lesen, direkt Namensauflösungen durchführen und Berichte und Meldungen in Text und HTML-Format erstellen. Diese Berichte können automatisch oder interaktiv erstellt werden. Für die Überwachung eines laufenden Fwlogwatch-Dienstes existiert ein Web-Interface. Die Konfiguration können Sie ab der Version 0.9 webbasiert über ein PHP-Skript (`fwlogwatch.php`) durchführen, das in dem `contrib/`-Verzeichnis mitgeliefert wird.

12.1.1 Installation von Fwlogwatch

Fwlogwatch installieren Sie üblicherweise auf der Firewall. Wenn Sie aus Sicherheitsgründen die Installation auf einem anderen System durchführen möchten, müssen Sie entweder die Protokolle manuell kopieren, oder Sie richten eine zentrale Protokollierung über das Netzwerk ein. Dies ist recht einfach und wird im Kapitel 10 beschrieben.

Fwlogwatch ist meines Wissens nur in der Debian-Distribution fest enthalten. Die Benutzer anderer Distributionen müssen Fwlogwatch von der Homepage

http://fwlogwatch.inside-security.de/ laden. Dort finden Sie aber sowohl RPM-Pakete als auch Quelltextarchive. Das zum Zeitpunkt der Drucklegung dort vorgehaltene binäre RPM-Paket ist unter Red Hat 8.0 übersetzt worden. Ich verwende daher immer das Source-RPM-Paket und übersetze es für die entsprechende Distribution neu:

```
# rpmbuild --rebuild fwlogwatch-<version>.src.rpm
```

Anschließend können Sie das erzeugte Paket installieren. Diese Vorgehensweise funktioniert auch auf SUSE- und SUSE-Linux-OSS-Systemen.

Achtung

Da Sie für die Übersetzung einen Compiler und viele weitere Werkzeuge wie `make` und `patch` benötigen, sollten Sie das Paket auf einem anderen System übersetzen und anschließend auf die Firewall kopieren und dort installieren.

Damit Fwlogwatch automatisch als Dienst startet, rufen Sie den `chkconfig`-Befehl auf.

```
# chkconfig --add fwlogwatch
```

Bei älteren SUSE-Distributionen sollten Sie von Hand die Verknüpfungen für den gewünschten Runlevel überprüfen und bei Bedarf einrichten:

```
# ln -s /etc/rc.d/init.d/fwlogwatch /etc/rc.d/rc3.d/S90fwlogwatch
# ln -s /etc/rc.d/init.d/fwlogwatch /etc/rc.d/rc3.d/K10fwlogwatch
```

Wenn Sie Fwlogwatch direkt aus den Quellen übersetzen möchten, müssen Sie zunächst das Paket von der Homepage laden, auspacken und mit `make; sudo make install` übersetzen. Mit dem Befehl `sudo make install-config` installieren Sie eine Beispielkonfigurationsdatei und ein Template in */etc*.

12.1.2 Konfiguration von Fwlogwatch

Fwlogwatch unterstützt drei verschiedene Modi: Zusammenfassung (Summary), Meldung (Report) und Echtzeitantwort (Realtime Response). Der Modus Zusammenfassung erlaubt es, aus einem Firewall-Protokoll mit mehreren tausend Einträgen in wenigen Sekunden einen Bericht zu erzeugen, in dem die Ereignisse zusammengefasst werden. Eine typische Zusammenfassung sieht folgendermaßen aus:

```
fwlogwatch-Zusammenfassung
Generiert Mit Mai 29 10:01:08 CEST 2002 von root.
18184 von 18362 Einträgen in der Datei "/home/xxx_firewall/messages.2" sind Paketfiltereinträge, 139 sind eindeutig.
```

```
Erster Paketfiltereintrag: Mai 12 13:21:27, letzter: Mai 17 13:44:10.
Alle Einträge wurden vom diesem Rechner geloggt: "fwsteinfurt".
Alle Einträge haben das selbe Ziel: "-".
Mai 17 13:56:24 03:04:25:40 - eth1 3001 udp Pakete (187968 Bytes) von
 192.168.222.200 (-) bis 111.112.222.222 (-) Port 53
Mai 17 13:56:37 03:04:25:44 - eth1 2991 udp Pakete (187172 Bytes) von
 192.168.222.200 (-) bis 192.33.4.12 (c.root-servers.net) Port 53
Mai 17 13:56:33 03:04:25:50 - eth1 2983 udp Pakete (186434 Bytes) von
 192.168.222.200 (-) bis 192.112.36.4 (G.ROOT-SERVERS.NET) Port 53
Mai 17 13:56:37 03:04:25:44 - eth1 2976 udp Pakete (185906 Bytes) von
 192.168.222.200 (-) bis 192.5.5.241 (f.root-servers.net) Port 53
Mai 17 13:56:29 03:04:25:49 - eth1 2353 udp Pakete (142615 Bytes) von
 192.168.222.200 (-) bis 192.36.148.17 (i.root-servers.net) Port 53
Mai 17 11:14:21 03:20:24:24 AntiSpoofing:  eth4 866 icmp Pakete (48496 Bytes)
 von xxx.yyy.200.249 (-) bis 192.168.201.5 (-) Port 0
```

Hinweis

Die deutsche Variante der Zusammenfassung gibt leider als Übersetzung des englischen *to* das deutsche Wort *bis* anstatt sinnvollerweise *nach* an.

Sie können das verbessern, indem Sie in der Datei `po/de.po` im Fwlogwatch-Quelltext in Zeile 793 die folgende Ersetzung durchführen:

```
#: ../output.c:262
#, c-format
msgid " to %s"
msgstr " nach %s"
```

Mit dieser Zusammenfassung können Sie den Zustand der Firewall in den letzten Stunden überblicken. Sie erkennen leichter, welche Rechner die Richtlinien verletzen, als es die manuelle Analyse der Protokolldatei ermöglicht.

Im interaktiven Meldungsmodus ist Fwlogwatch in der Lage, automatisch E-Mails zu generieren, die an ein CERT oder an die verantwortlichen Administratoren der »angreifenden« Rechner gesendet werden. Diese Funktion sollte zur Vermeidung von Spam daher mit Vorsicht eingesetzt werden!

```
----------------------------------------------------------------------
From: root@kermit.spenneberg.de
To: [Insert address of abuse contact or CERT here]
Subject: Ereignisbericht 20020514-192.168.222.200

Dear Madam or Sir,
```

```
we would like to bring to your attention that [your organization's
networks] have been subject to heavy scans from a/several host/s in
your domain:


Angreifende IP-Adresse:    192.168.222.200
Ziel-IP-Adresse:           111.112.222.222
Anzahl der geloggten Versuche: 3001
Verfolgungsnummer:         20020514-192.168.222.200


Please take the appropriate steps to stop these scans.
In case you need more information we would be glad to provide you
with the appropriate log file excerpts as far as they are available.


Thank you.
Yours sincerely
[Your signature]
---------------------------------------------------------------------
```

Hinweis

Leider besteht hier das Problem, dass die sinnvollerweise in Englisch gehaltene E-Mail mit deutschen Informationen gefüllt wird, wenn Fwlogwatch in einer deutschen Umgebung verwendet wird. Dieses Problem (und auch das oben angesprochene) lässt sich vermeiden, wenn vor dem Aufruf die entsprechende Umgebungsvariable für das Locale modifiziert wird:

```
LANG="en_US" fwlogwatch -i 1000
```

Allerdings werden dann auch die Zusammenfassungen nicht mehr übersetzt. Natürlich können Sie die Umgebungsvariable `LANG` immer nur für den jeweiligen Lauf anpassen.

Schließlich unterstützt Fwlogwatch auch einen Echtzeit-Modus. Hier überwachen Sie mit Fwlogwatch in Echtzeit die Protokolldatei. Fwlogwatch kann Benachrichtigungen z.B. per E-Mail oder WinPopUp versenden, und Sie erhalten über den Fwlogwatch-Webserver immer den aktuellen Stand Ihrer Firewall angezeigt. Auch diese Funktion sollte zum Schutz vor Belästigungen mit Vorsicht eingesetzt werden!

Um diese Funktionen anzubieten, besitzt fwlogwatch zwei Konfigurationsdateien: `fwlogwatch.config` und `fwlogwatch.template`. Die Datei `fwlogwatch.template` stellt ein Template für die im interaktiven Meldungsmodus zu versendende E-Mail dar.

Die beiden mitgelieferten Dateien sind sehr gut dokumentiert und relativ selbsterklärend. Im Folgenden möchte ich Ihnen nur kurz die wichtigsten Optionen der verschiedenen Modi erklären. Die meisten Optionen können sowohl auf der Kommandozeile als auch in der Konfigurationsdatei definiert werden.

Allgemeine Optionen

Zunächst stehen Ihnen einige Funktionen in allen Modi zur Verfügung. Sinnvollerweise geben Sie die Parameter in der Konfigurationsdatei an. Mit den angegebenen Kommandozeilenoptionen können Sie aber auch die Funktion auf der Kommandozeile nutzen.

- `include_file`. Hiermit können Sie weitere Konfigurationsdateien einlesen. Damit lässt sich die Konfigurationsdatei aufsplitten.
- `verbose = <yes|no>, -v`. Diese Option ist nur auf der Kommandozeile sinnvoll. Die Angabe von zwei `-v` verstärkt die Wirkung.
- `resolve_hosts = <yes|no>, -n`. Hiermit schalten Sie die Namensauflösung an. Denken Sie daran, dass diese Namensauflösung Zeit kostet, Ihre Internetverbindung belastet und möglicherweise auch zu Einträgen in den Protokollen führt.
- `resolve_services = <yes|no>, -N`. Lesen Sie lieber Portnummern oder -namen?
- `input = <datei>, -f`. Hier geben Sie die zu verarbeitenden Protokolldateien an. Ab der Version 0.9.1 können Sie mehrere Dateien auf einzelnen Zeilen angeben. Ist die Datei mit `gzip` komprimiert worden (`.gz`), kann Fwlogwatch sie dekomprimieren. Bei Verwendung des Echtzeitmodus müssen Sie die Datei mit ihrem absoluten Pfad angeben. Der Einfachheit halber geben Sie die Datei immer mit ihrem absoluten Pfad an.
- `parser = infcpewls, -P`. Hier wählen Sie das Protokollformat. Fwlogwatch kann viele Formate lesen. Das Netfilter/Iptables-Format wählen Sie mit `parser = n`.
- `src_ip = on, -S; dst_ip = on , -D; protocol = on, -p; src_port = on, -s; dst_port = on, -d; tcp_opts = on, -y` Fwlogwatch sortiert und aggregiert die Einträge in der Protokolldatei. Sie können die Kriterien in der Konfigurationsdatei bestimmen.
- `exclude_src_host =, exclude_src_port =, exclude_dst_host =, exclude_dst_port =, include_src_host =, include_src_port =, include_dst_host =, include_dst_port =, -E` Hiermit können Sie bestimmte Rechner und Ports von der Analyse durch Fwlogwatch ausnehmen. Dies ist zum Beispiel sinnvoll, wenn Sie einen bestimmten Rechner für Nmap-Audit-Scans (15.2) verwenden. Sie können auch auf der Kommandozeile die zu ignorierenden Rechner angeben. Die Kommandozeilenoption `-E` verwendet `e` für exclude und `i` für include. Die Buchstaben `hpcb` stehen für host, port, chain und branch. In den ersteren beiden Fällen wird mit den Buchstaben `s` oder `d` noch source oder destination angegeben. Beispiel: `-Eehs127.0.0.1`.

  Ab der Version 1.0 können Sie hier auch die CIDR-Notation verwenden (Beispiel: `192.168.1.0/25`)

- `exclude_chain`, `exclude_branch`, ... , `-E`. Hiermit können Sie ganze Ketten oder Aktionen in der Fwlogwatch-Auswertung ignorieren. Das Format der Kommandozeilenoption `-E` wurde bereits bei der letzten Option erklärt. Beispiel: `-EecOUTPUT`.
- `sort_order = [cteznpbSsDd][ad]`, `-O`. Auch die Sortierung der Protokolleinträge in der Auswertung können Sie bestimmen. Der erste Buchstabe definiert das Sortierkriterium: `c` count, `t` Startzeit, `e` Endzeit, `z` Dauer, `n` Zielname, `p` Protokoll, `b` Anzahl Bytes, `S` Source, `s` Sourceport, `D` Ziel, `d` Zielport. Der zweite Buchstabe definiert die Sortierrichtung: aufsteigend (`a`, ascending) oder abfallend (`d`, descending). Es können mehrere Sortierungen angegeben werden, die in der angegebenen Reihenfolge genutzt werden. Default ist `tacd`.

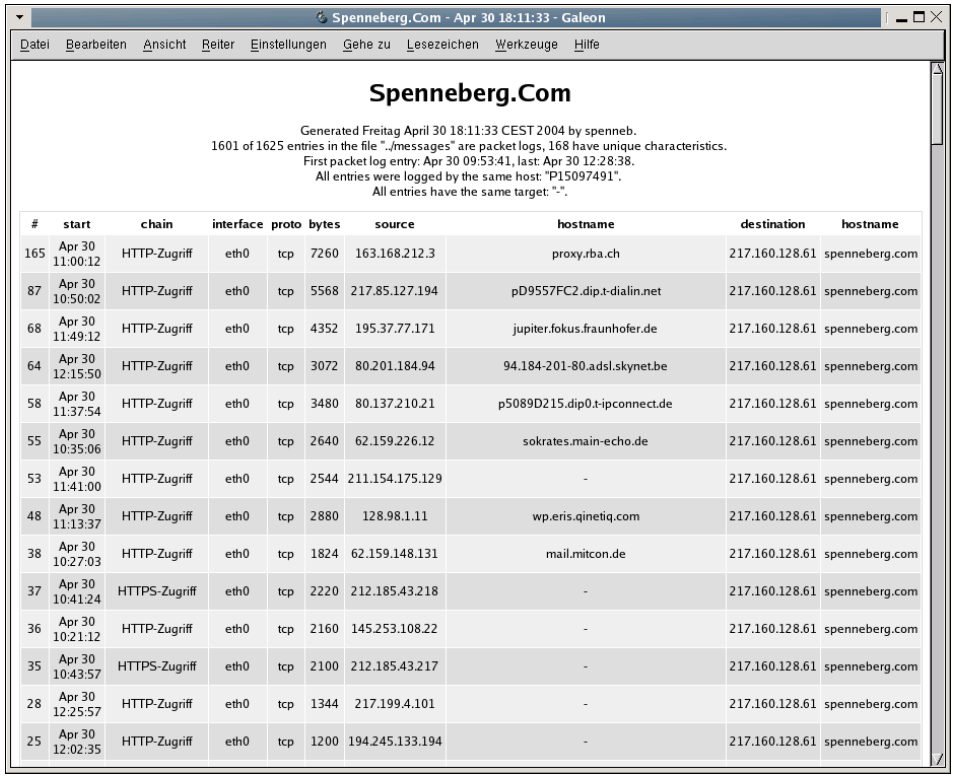
Weitere Optionen erlauben ab der Version 0.9.3 die Anpassung der Ausgabe an die eigenen Wünsche:

- `title =` Hiermit kann der Titel für die Ausgabe definiert werden. Default ist »fwlogwatch summary« im Zusammenfassungsmodus oder »fwlogwatch status« im Echtzeitmodus.
- `stylesheet =` Diese Option erlaubt die Angabe eines alternativen Stylesheets. Im Echtzeitmodus muss dies ein externer URL sein, der mit `http://` beginnt.
- `textcolor =`, `bgcolor =`, `rowcolor1 =`, `rowcolor2 =` Wenn die Farben zusätzlich angepasst werden sollen, können Sie das mit diesen Optionen durchführen.

Fwlogwatch-Zusammenfassung

Im Zusammenfassungsmodus können Sie folgende weitere Optionen nutzen:

- `data_amount`, `-b`. Hiermit erhalten Sie bei jedem Angriff die Summe der Pakete.
- `start_times = yes`, `-t`; `end_times = yes`, `-e`. Dies zeigt Ihnen den Start und das Ende des Angriffs an.
- `duration = yes`, `-z`. Dauer eines Angriffs.
- `html = yes`, `-w`. Erzeugt eine HTML-Ausgabe (siehe Abbildung 12.1, ab der Version 1.0 in XHTML 1.1).
- `output = <datei>`, `-o`. Fwlogwatch schreibt die Ausgabe in eine Datei.
- `recent = <zeitraum>[mhdwy]`, `-l` Wenn Sie sich nur für die letzte Woche interessieren, können Sie als Zeitraum `recent=w` verwenden.
- `at_least = <anzahl>`, `-m` Versteckt Einträge, die nur selten vorkommen.
- `maximum = <anzahl>`, `-M` Hiermit kann die Anzahl der Einträge in dem Bericht beschränkt werden.
- `whois_lookup = no`, `-W` Diese Option weist *Fwlogwatch* an, Informationen über die Source-IP-Adressen in der Whois-Datenbank zu ermitteln. Diese Option sollte nur mit Vorsicht eingesetzt werden, da sie sehr langsam ist und die Whois-Datenbanken stark belastet.



#	start	chain	interface	proto	bytes	source	hostname	destination	hostname
165	Apr 30 11:00:12	HTTP-Zugriff	eth0	tcp	7260	163.168.212.3	proxy.rba.ch	217.160.128.61	spenneberg.com
87	Apr 30 10:50:02	HTTP-Zugriff	eth0	tcp	5568	217.85.127.194	pD9557FC2.dip.t-dialin.net	217.160.128.61	spenneberg.com
68	Apr 30 11:49:12	HTTP-Zugriff	eth0	tcp	4352	195.37.77.171	jupiter.fokus.fraunhofer.de	217.160.128.61	spenneberg.com
64	Apr 30 12:15:50	HTTP-Zugriff	eth0	tcp	3072	80.201.184.94	94.184-201-80.adsl.skynet.be	217.160.128.61	spenneberg.com
58	Apr 30 11:37:54	HTTP-Zugriff	eth0	tcp	3480	80.137.210.21	p5089D215.dip0.t-ipconnect.de	217.160.128.61	spenneberg.com
55	Apr 30 10:35:06	HTTP-Zugriff	eth0	tcp	2640	62.159.226.12	sokrates.main-echo.de	217.160.128.61	spenneberg.com
53	Apr 30 11:41:00	HTTP-Zugriff	eth0	tcp	2544	211.154.175.129	-	217.160.128.61	spenneberg.com
48	Apr 30 11:13:37	HTTP-Zugriff	eth0	tcp	2880	128.98.1.11	wp.eris.qinetiq.com	217.160.128.61	spenneberg.com
38	Apr 30 10:27:03	HTTP-Zugriff	eth0	tcp	1824	62.159.148.131	mail.mitcon.de	217.160.128.61	spenneberg.com
37	Apr 30 10:41:24	HTTPS-Zugriff	eth0	tcp	2220	212.185.43.218	-	217.160.128.61	spenneberg.com
36	Apr 30 10:21:12	HTTP-Zugriff	eth0	tcp	2160	145.253.108.22	-	217.160.128.61	spenneberg.com
35	Apr 30 10:43:57	HTTPS-Zugriff	eth0	tcp	2100	212.185.43.217	-	217.160.128.61	spenneberg.com
28	Apr 30 12:25:57	HTTP-Zugriff	eth0	tcp	1344	217.199.4.101	-	217.160.128.61	spenneberg.com
25	Apr 30 12:02:35	HTTP-Zugriff	eth0	tcp	1200	194.245.133.194	-	217.160.128.61	spenneberg.com

Abbildung 12.1: Fwlogwatch kann im Zusammmenfassungsmodus auch eine HTML-Seite erzeugen.

Wenn Sie anfangen, mit dem Zusammenfassungsmodus zu experimentieren, können Sie zu Beginn die folgende Konfigurationsdatei verwenden und dann an die eigenen Bedürfnisse anpassen:

```
resolve_hosts = yes
parser = n
src_ip = on
dst_ip = on
data_amount = yes
duration = yes
protocol = on
dst_port = on
sort_order = tacd
```

Fwlogwatch-Meldung

In bestimmten Umgebungen kann es sinnvoll sein, direkt bei der Analyse der Protokolle gewisse Ereignisse zu melden. Im Meldungsmodus besteht die Möglichkeit,

eine E-Mail für jedes Angriffsereignis zu versenden. Diese Meldung kann an ein CERT oder an die verantwortlichen Administratoren des angreifenden Rechners gesendet werden. Die Meldung erfolgt nicht in Echtzeit, sondern zeitversetzt bei der Analyse der Protokolle mit Fwlogwatch.

Achtung

Natürlich sollten Sie mit dieser Funktion sehr vorsichtig sein. E-Mail-Adressen können gefälscht werden. Der scheinbare Angriff kann harmlos sein. Sie können sich lächerlich machen. Prüfen Sie daher genau die Ereignisse, bevor Sie eine E-Mail versenden.

Für die Konfiguration des E-Mail-Versands stehen Ihnen die folgenden Funktionen zur Verfügung:

- `interactive = <anzahl>, -i`. Dies aktiviert den Meldungsmodus. Für alle Angriffe mit mehr Paketen als der angegebenen Anzahl werden Meldungen erzeugt.
- `sender = <email>, -F`. Die E-Mail-Adresse des Absenders. Hier sollten Sie Ihre E-Mail-Adresse oder ein Funktionskonto (z.B. `firewall-admin@spenneberg.net`), das Sie verwenden, eintragen.
- `recipient = <email>, -T`. E-Mail-Adresse des Empfängers. Dies kann Ihr internes CERT sein. Senden Sie bitte nicht ohne Aufforderung an ein externes CERT.
- `cc = <email>, -C`. Carbon Copy. Die E-Mail wird zusätzlich an diese Adresse gesendet. Diese Funktion ermöglicht es Ihnen, einfach jede E-Mail zu archivieren oder an mehrere CERTs zu versenden.
- `template = <datei>, -I`. Template für die E-Mail (Default: `/etc/fwlogwatch.template`). Diese Datei können Sie frei nach Ihren Wünschen anpassen.

Damit Sie direkt loslegen können, habe ich hier eine einfache Beispielkonfiguration für Sie:

```
# Meldungsmodus
interactive = 3000
parser = n
sender = ralf@spenneberg.de
recipient = incident@firma.de
cc = incident@spenneberg.de
template = /etc/fwlogwatch.incident
```

Echtzeit

Im Echtzeitmodus ist Fwlogwatch in der Lage, Echtzeitbenachrichtigungen zu versenden und sogar aktiv zu reagieren. Hierzu konfigurieren Sie zwei mitgelieferte Skripten, die Sie zuvor anpassen können. Das erste Skript, `fwlw_notify`, versendet

Echtzeit-Alarmierungen per E-Mail oder Windows-Nachrichtendienst. Das zweite Skript, `fwlw_respond`, kann Firewall-Regeln mit `iptables` hinzufügen, um weitere Angriffe des Hosts zu verhindern. Den Einsatz des zweiten Skripts sollten Sie abwägen, da ansonsten ein Angreifer einen Denial-of-Service-Angriff auf Ihre Firewall durchführen kann. Hierzu würde es genügen, wenn der Angreifer die IP-Adressen der DNS-Root-Server oder einiger wichtiger Webserver fälschen würde. *Fwlogwatch* würde bei Verwendung des Skripts `fwlw_respond` diese IP-Adressen sperren und Ihnen keine Kommunikation mit den Systemen, deren IP-Adressen im Angriff gefälscht wurden, erlauben.

- `realtime_response = yes, -R`. Diese Option schaltet den Echtzeitmodus an.
- `ipchains_check = no`. Diese Option überprüft die Korrektheit der `ipchains`-Regeln beim Start. Beim Einsatz von `iptables` ist diese Funktion obsolet.
- `pidfile = <datei>`. Hiermit schreibt *Fwlogwatch* seine PID in die angegebene Datei. Damit ist es einfacher, einem laufenden Fwlogwatch-Prozess Signale zu senden.
- `run_as = `. Diese Option weist *Fwlogwatch* an, seinen Benutzerkontext zu ändern. Dabei wird der `fwlogwatch`-Befehl zunächst als `root` gestartet. So kann der Prozess sowohl auf die Protokolldatei als auch auf den privilegierten Port für den Webserver zugreifen. Anschließend werden diese `root`-Privilegien abgegeben.
- `alert_threshold = <anzahl>, -a`. Beim Überschreiten dieses Schwellenwertes löst Fwlogwatch Alarm aus (Default 5).
- `recent = , -l`. Lebensdauer der Ereignisse. Nach Ablauf vergisst Fwlogwatch die Ereignisse (siehe Zusammenfassungsmodus).
- `notify = yes, -A`. Führt das Notify-Skript aus.
- `respond = yes, -B`. Führt das Respond-Skript aus.
- `notification_script = <datei>; response_script = <datei>`. Name des entsprechenden Skripts (`fwlw_(notify|respond)`). In den mitgelieferten Skripten (`contrib/`) befinden sich weitere Beispiele und Kommentare.
- `known_host = <ip-address>, -k`. Die hier in CIDR-Notation (192.168.0.0/24) angegebenen Rechner oder Netzwerke lösen keine Warnmeldung aus.

Im Echtzeitmodus kann ein Webserver in *Fwlogwatch* aktiviert werden. Damit überwachen Sie den Echtzeitmodus. Hierfür stehen die folgenden Optionen zur Verfügung:

- `server_status = yes, -X`. Damit aktivieren Sie den Webserver.
- `bind_to = <ip-address>`. Hiermit kann die IP-Adresse angegeben werden, auf der anschließend der Webserver seine Dienste anbieten soll (Default: 127.0.0.1).
- `listen_port = <port>`. Diese Angabe definiert den TCP-Port, der verwendet wird.
- `listen_to = <ip-address>`. Lediglich die angegebene IP-Adresse darf sich mit dem Webserver verbinden.
- `status_user = <user>, status_password = <crypt>`. Fwlogwatch verlangt von dem Benutzer bei der Anmeldung eine Authentifizierung. Diese wird mit diesen

Angaben definiert. Das angegebene Kennwort muss verschlüsselt angegeben werden. Fwlogwatch verwendet wie die klassischen Unix-Systeme die `crypt`-Verschlüsselung. Sie können das Kennwort sehr leicht mit dem Befehl `htpasswd -nb <user kennwort>` erzeugen. Dieser Befehl ist üblicherweise in den Linux Apache-Paketen enthalten.

- `refresh = <Sekunden>`. Schließlich können Sie einen automatischen Refresh der Webseite mit dieser Option konfigurieren.

Eine Beispielkonfiguration mit der Konfiguration des Webservers für die Überwachung kann folgendermaßen aussehen:

```
realtime_response = yes
parser = n
run_as = fwloguser
alert_threshold = 5
notify = yes
notification_script = /usr/local/sbin/fwlw_notify
server_status = yes
bind_to = 192.168.0.1
listen_port = 8888
status_user = ralf
status_password = gie0lzYkkk9sQ
refresh = 10
```

Ein Screenshot der Web-Überwachung im Echtzeitmodus ist in Abbildung 12.1 zu sehen. Ab der Version 1.0 kann über das Web-Interface auch eine Konfiguration von Fwlogwatch erfolgen (Abbildung 12.3).

Achtung

Wenn Sie Fwlogwatch im Echtzeitmodus als Daemon einsetzen und ein anderes Werkzeug die Protokolldatei rotiert, verliert Fwlogwatch den Zugang zu den Protokollen. Sie müssen, damit Fwlogwatch nun die neue Datei liest, Fwlogwatch ein Signal schicken. Ein einfaches SIGHUP reicht jedoch nicht aus. Hier liest Fwlogwatch nur seine Konfigurationsdatei neu. Sie müssen ein SIGUSR1 an den Prozess schicken:

```
kill -USR1 $(cat /var/run/fwlogwatch-pid)
```

Weitere Web-Funktionen

Fwlogwatch weist noch einige weitere Funktionen auf, mit denen Sie komfortabel über ein Web-Interface Berichte erzeugen können. So enthält das `contrib/`-Verzeichnis der *Fwlogwatch*-Distribution zwei CGI-Programme und ein PHP-Programm. Diese können Sie nach Anpassung auf einem Webserver installieren und weitere Berichte erzeugen.

Abbildung 12.2: Im Echtzeitmodus kann Fwlogwatch seinen Status über ein Web-Interface anzeigen.

Das `fwlogsummary.cgi`-Skript erzeugt insgesamt 8 verschiedene HTML-Berichte, die anschließend mit einem Webbrowser betrachtet werden können. Hierzu ist es erforderlich, dass der Webserver das CGI-Skript und den Befehl `fwlogwatch` ausführen darf und Leserechte an der Protokolldatei hat. Es ist aber auch möglich, das Skript zu bestimmten Uhrzeiten automatisch über *Cron* aufzurufen. Die so erzeugten Berichte werden nach verschiedenen Aspekten sortiert und auf dem Webserver abgelegt. Sie erhalten so sehr einfach acht verschiedene Berichte der letzten Stunde, die die Einträge sortiert nach der Absender-Adresse, Zieladresse, Ports etc. aufführen. Die Erstellung all dieser Berichte dauert eine gewisse Zeit. Daher empfiehlt sich der Aufruf per Cron-Daemon.

Das zweite CGI-Skript `fwlogsummary_small.cgi` erzeugt lediglich einen Bericht, der die letzte Stunde zusammenfasst. Hiermit können Sie bei einer Alarmierung sehr schnell einen Überblick über den Zustand der Firewall erhalten.

Das PHP-Skript erlaubt schließlich online die Auswahl der Optionen für die Anzeige des Berichts. Dabei können fast alle Möglichkeiten von Fwlogwatch ausgereizt werden. Abbildung 12.4 zeigt die möglichen Optionen.

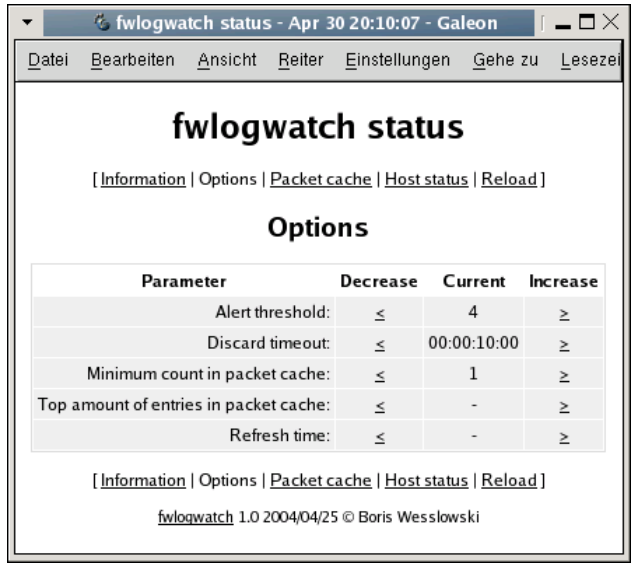


Abbildung 12.3: Das Web-Interface erlaubt auch eine Konfiguration von Fwlogwatch.

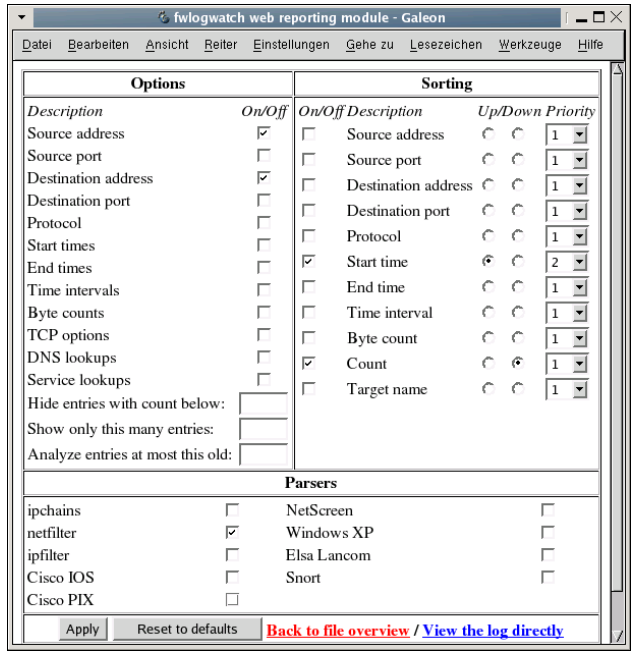


Abbildung 12.4: Mit dem PHP-Skript wählen Sie komfortabel die Optionen für die Erzeugung des Berichts.

12.2 IP Tables State (IPTState)

Der Befehl IPTState (*http://www.phildev.net/iptstate/index.html*) ist sehr hilfreich bei der täglichen Administration und Wartung einer Iptables-Firewall. Er ist mit dem Befehl `top` vergleichbar, der die Prozesse in einer sortierten Liste darstellt. Allerdings sollten Sie diesen Befehl nicht ununterbrochen auf Ihrer Firewall laufen lassen, da dies das System stark belastet. Um jedoch die aktuellen Verbindungen leicht lesbar anzuzeigen und zu sortieren, ist der Befehl sehr gut geeignet.

Um den Befehl zu installieren, benötigen Sie auf Ihrer Firewall lediglich das Ncurses-Paket. Dieses ist bei den meisten Distributionen enthalten und auch schon installiert. Sie können IPTState nicht auf einem anderen System als der Firewall installieren, da IPTState den aktuellen Zustand der Firewall direkt aus der Datei `/proc/net/ip_conntrack` liest.

IPTState ist bereits bei vielen Distributionen enthalten. Bevor Sie das Paket manuell installieren, sollten Sie prüfen, ob Ihre Distribution das Paket bereits mitliefert.

Laden Sie zur Installation das Paket von der Homepage herunter, und entpacken Sie es an geeigneter Stelle. Anschließend wechseln Sie in das Verzeichnis und rufen `make; make install` auf. Tritt hierbei ein Fehler auf, prüfen Sie bitte, ob das `ncurses-devel`-Paket Ihrer Distribution installiert ist.

```
$ cd /usr/local/src
$ tar xjf iptstate-<version>tar.bz2
$ cd iptstate-<version>
$ make
$ sudo make install
```

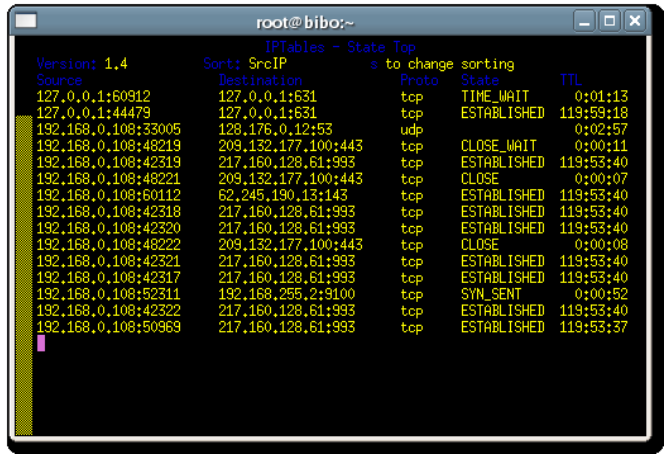


Abbildung 12.5: Der Befehl iptstate zeigt die aktuellen Verbindungen der Firewall an.

Nun sollten Sie bereits mit `man iptstate` die Handbuchseite des Befehls anzeigen können. Mit `iptstate` starten Sie bereits den Befehl, der Ihnen die Verbindungen über Ihre Firewall anzeigt.

Bei dem Aufruf des Programms können Sie über Kommandozeilenoptionen die Sortierreihenfolge und Filterfunktionen definieren. So erlaubt die Option `-b` die Sortierung der Verbindungen nach der Zieladresse (`-bd`), nach dem Protokoll (`-bp`), nach dem Zustand (`-bs`) oder nach ihrer Lebensdauer (`-bt`). Leider lassen sich diese nicht miteinander kombinieren. Mit den Optionen `-S` und `-D` können Sie nur die Verbindungen mit einer bestimmten Absender- oder Ziel-IP-Adresse anzeigen lassen. Die Option `-f` zeigt alle Loopback-Verbindungen nicht an. Die Option `-l` führt für jede Adresse eine Namensauflösung durch. Dabei werden die Namen der Clients von rechts abgeschnitten, da die meisten Clients aus Ihrer eigenen Domäne kommen werden, und die Namen der Server werden von links abgeschnitten, da Sie wahrscheinlich am meisten an den Domänen interessiert sind. Wenn Sie die Namensauflösung nutzen, ist die gleichzeitige Angabe von `-L` sinnvoll. Hiermit werden alle DNS-Verbindungen zur Namensauflösung in der Anzeige unterdrückt.

Sobald Sie sich in dem interaktiven Modus befinden, können Sie

- mit der Leertaste einen sofortigen Refresh der Anzeige auslösen,
- mit `r` rückwärts sortieren,
- mit `l` die DNS-Auflösung an- und abschalten,
- mit `n` die Anzeige der DNS-Verbindung an- und abschalten,
- mit `s` die Sortierung nach der nächsten Spalte durchführen
- und mit `q` den Befehl beenden.

Häufig benötigen Sie jedoch keine sich immer neu aktualisierende Anzeige, sondern möchten nur den aktuellen Zustand der Firewall in einer leicht lesbaren Liste anzeigen. Hierfür bietet IPTState die Option `-s`. Dies ist der Single-Run-Modus. Das Werkzeug gibt den aktuellen Zustand aus und beendet sich. Sie können die Ausgabe leicht mit `grep` und `awk` weiterbearbeiten oder auch per E-Mail verschicken.

```
# iptstate -s
IP Tables State Top -- Sort by: SrcIP
Source               Destination          Proto   State        TTL
192.168.255.100:52661 217.160.128.61:993    tcp     ESTABLISHED  119:54:02
192.168.255.100:52662 217.160.128.61:993    tcp     ESTABLISHED  119:54:02
192.168.255.100:35957 209.132.177.100:443   tcp     CLOSE          0:00:05
192.168.255.100:35956 209.132.177.100:443   tcp     CLOSE          0:00:04
192.168.255.100:52668 217.160.128.61:993    tcp     ESTABLISHED  119:54:01
192.168.255.100:50090 213.30.31.52:80       tcp     TIME_WAIT      0:00:52
192.168.255.100:56979 217.160.128.61:993    tcp     ESTABLISHED  119:54:02
192.168.255.100:59425 193.201.52.189:80     tcp     SYN_SENT       0:00:39
192.168.255.100:52667 217.160.128.61:993    tcp     ESTABLISHED  119:54:01
192.168.255.100:56978 217.160.128.61:993    tcp     ESTABLISHED  119:54:01
192.168.255.100:38752 192.168.255.1:53      udp                    0:00:04
```

```
192.168.255.100:38759 192.168.255.1:53      udp                    0:00:04
192.168.255.100:38760 192.168.255.1:53      udp                    0:02:53
192.168.255.100:52666 217.160.128.61:993    tcp     ESTABLISHED  119:54:01
192.168.255.100:42223 213.30.31.52:80       tcp     TIME_WAIT      0:01:52
192.168.255.125:1069  192.168.255.100:139   tcp     ESTABLISHED  119:56:57
```

Die hohen Werte in der Spalte TTL sind auf die hohen Verweildauern von TCP-Verbindungen in der Zustandstabelle zurückzuführen. Aufgebaute TCP-Verbindungen verbleiben für 5 Tage in der Tabelle, während UDP-Verbindungen lediglich 180 Sekunden lang dort gespeichert werden.

12.3 Webfwlog Firewall Log Analyzer

Der Webfwlog Firewall Log Analyzer bietet Ihnen eine webbasierte Firewall-Protokollanalyse und Berichtserzeugung. Sie benötigen für den Einsatz einen Webserver mit mindestens PHP 4.1, eine MySQL- oder PostgreSQL-Datenbank und einen Webbrowser. Damit Webfwlog die Protokolle analysieren kann, benötigt er Lesezugriff auf die Protokolle der Firewall.

Tipp

Webfwlog ist eines der wenigen Werkzeuge, die auch Protokolle aus einer Datenbank lesen können. Wenn Sie das `ULOG`-Target (siehe Abschnitt 24.1) einsetzen, können Sie damit die Protokollmeldungen in eine MySQL-Datenbank schreiben, die Sie mit diesem Werkzeug analysieren können!

Die aktuelle Version 0.91 von Webfwlog wurde am 23. April 2005 veröffentlicht und ist unter *http://www.webfwlog.net/* sowohl als RPM als auch als Quelltext verfügbar. Sie können daher auf einer RPM-basierten Distribution die Installation sehr einfach vornehmen. Falls für Ihre Distribution kein binäres RPM verfügbar ist, empfehle ich, dies selbst zu bauen:

```
rpmbuild --rebuild webfwlog-<version>.src.rpm
```

Falls Sie keine RPM-basierte Distribution einsetzen oder der Bau des RPMs fehlschlägt, können Sie Webfwlog auch leicht aus dem Quelltext übersetzen. Hierbei sollten Sie die folgenden Optionen beim Aufruf von `./configure` angeben:

- `--sysconfdir=/etc`. In diesem Verzeichnis wird die Konfigurationsdatei `webfwlog.conf` gesucht.
- `--with-html-doc-root=/var/www/html`. Dies ist das DocumentRoot des Apache Webservers.
- `--enable-syslog`. Hiermit aktivieren Sie den Syslog-Parser. Wenn Sie ULOG verwenden, benötigen Sie diesen nicht.

- `--enable-mysql|--enable-pgsql`. Dies aktiviert die Unterstützung für die entsprechende Datenbank. Die Client-Bibliotheken für die Datenbank müssen auf dem System installiert sein. Sie benötigen die Datenbankunterstützung auch, wenn Sie den Syslog-Parser verwenden.

Dann können Sie die Übersetzung starten:

```
$ ./configure --sysconfdir=/etc --with-html-doc-root=/var/www/webfwlog --with-mysql
$ make
$ sudo make install
```

Wenn Sie nicht den Syslog-Parser verwenden, wundern Sie sich bitte nicht, dass beim `make`-Kommando nichts passiert. Eine Übersetzung ist nur nötig, wenn der Parser aktiviert wird. Dennoch ist der Aufruf des `./configure`-Skripts erforderlich.

Tipp

Wenn Sie eine neue Version installieren, überprüft das Installationsskript, ob bereits eine Konfigurationsdatei `/etc/webfwlog.conf` vorhanden ist, und überschreibt diese nicht. Ein Upgrade ist also mit `make install` möglich.

Nun müssen Sie noch die Datenbank für Webfwlog anpassen. Hierfür gibt es in den Verzeichnissen `./mysql/` bzw. `./pgsql/` jeweils ein Setup-Skript. Wechseln Sie einfach in das vorgesehene Verzeichnis, und rufen Sie `./setup` auf. Dieses Skript fragt nach den notwendigen Informationen und erzeugt ein MySQL-Skript, mit dem Sie die notwendige Datenbank erzeugen können.

Anschließend müssen Sie nur noch die Konfigurationsdatei `/etc/webfwlog.conf` und bei Bedarf die Konfigurationsdatei `/etc/ulogd.conf` anpassen.

Hinweis

Bei mir hat das Installationsskript teilweise bei der Erzeugung der Datenbank einen kleinen Fehler gemacht und die Rechte für die Datenbank nicht richtig gesetzt. Dies lässt sich leicht anschließend mit folgendem Befehl korrigieren:

```
# mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 83 to server version: 4.1.12

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> grant all on webfwlog.* to webfwlog@localhost identified by
  'kennwort';
```

```
Query OK, 0 rows affected (0.03 sec)

mysql> Bye
```

Wenn Sie bei der Erzeugung des Datenbankskripts die Beispielskripten ausgewählt haben, können Sie direkt Webfwlog verwenden. Bei dem Zugriff auf Webfwlog bietet Ihnen die Weboberfläche direkt einige Beispielberichte an (Abbildung 12.6).

Natürlich können Sie auch Ihre eigenen Berichte erzeugen. Hier stehen Ihnen sehr viele verschiedene Kriterien für die Erzeugung des Berichts zur Verfügung (Abbildung 12.7).

12.4 Scanulog und ulog-acctd

Der `ulog-acctd`-Daemon (*http://alioth.debian.org/projects/pkg-ulog-acctd/*) erzeugt Protokolldateien für Accounting-Zwecke. Hierzu nimmt er über das ULOG-Target IP-Pakete entgegen und schreibt das Protokoll, die Absender- und Zieladresse, die Ports, die Größe und die beteiligten Netzwerkkarten in diese Protokolldatei. Dabei können Sie das Format der Ausgabe frei anpassen, so dass Sie theoretisch auch direkt in eine SQL-Datenbank protokollieren können. Der `ulog-acctd`-Daemon ist in diesem Fall eine Alternative zu dem Ulogd-Daemon von Harald Welte (siehe Abschnitt 24.1).

Die Installation des Daemons ist sehr einfach. Sie erfolgt einfach mit `make`. Anschließend müssen Sie manuell die ausführbare Datei `ulog-acctd` in ein entsprechendes Verzeichnis kopieren. Zusätzliche Startskripten sind nicht vorhanden. Ich empfehle daher den Start über Ihr Firewall-Skript.

```
ulog -c /etc/ulog-acctd.conf
```

Damit Sie nun auswertbare Protokolldateien erhalten, müssen Sie in Ihren Regeln die zu protokollierenden Pakete an das ULOG-Target senden:

```
iptables -A FORWARD -j ULOG --ulog-nlgroup 1 --ulog-cprange 60 --ulog-qthreshold
  50 --ulog-prefix "FORWARD"
```

Der `ulog-acctd`-Daemon verfügt über eine Konfigurationsdatei `/etc/ulog-acctd.conf`. Diese Datei enhält die folgenden Angaben:

```
# Die ulog-nlgroup:
multicast groups=1

accounting file=/var/log/ulog-acctd/account.log
dump file=/var/log/ulog-acctd/dump
debug file=/var/log/ulog-acctd/debug.log
debug = syscall, misc, statistics, error, asdf, error-packet
accounting format="%h\t%t\t%p\t%s\t%S\t%d\t%D\t%P\t%b\t\"%i\"\t\"%o\"\t\"%f\"\n"
```

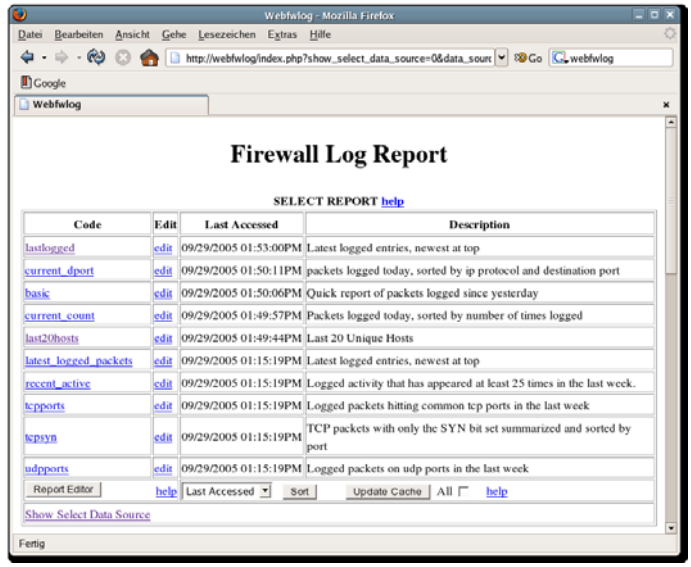


Abbildung 12.6: Webfwlog besitzt einige vorgefertigte Berichte.

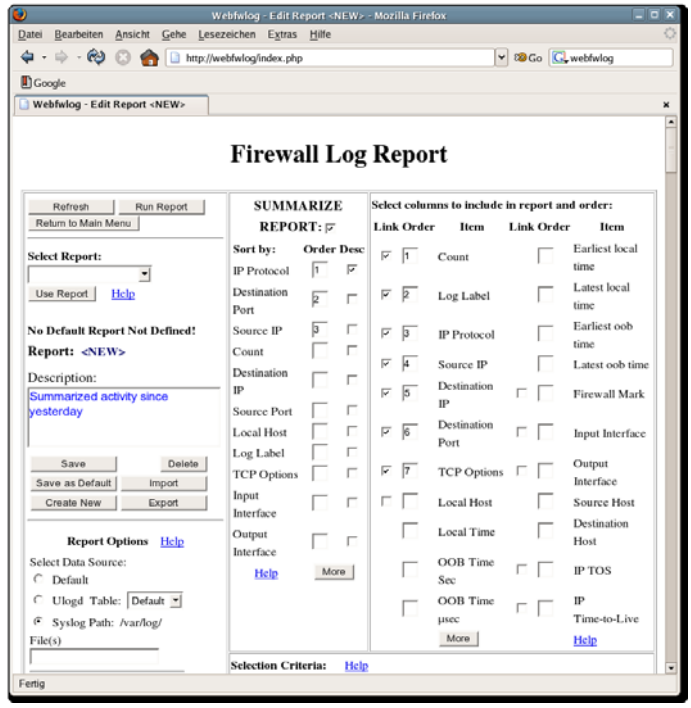


Abbildung 12.7: Webfwlog bietet Ihnen alle Freiheiten zur Erzeugung des Berichts.

```
empty interface="-"
empty prefix="-"

flush=30
fdelay=0
```

In der mitgelieferten Datei werden die einzelnen Parameter ausführlich erklärt, so dass ich mir das hier spare. Wichtig ist der Parameter `multicast groups`. Der Wert muss mit dem Wert `ulog-nlgroup` in der Iptables-Regel übereinstimmen.

Tipp

In dem `./contrib`-Verzeichnis finden Sie noch ein Skript `pg_load.php`, das die ulog-acctd-Daten in eine PostgreSQL-Datenbank lädt, und ein weiteres Skript, das die Daten für MRTG (Multi-Router-Traffic-Grapher, *http://www.mrtg.org*) entsprechend aufbereitet.

Da die Protokolle von `ulog-acctd` an sich nicht besonders aussagekräftig sind, können Sie mit `scanulog` grafische Auswertungen der Protokolle erzeugen. Hierfür installieren Sie Scanulog von der Homepage *http://www.aitrob.de/scanulog.html* mit `./configure; make` und passen die Konfiguration von `ulog-acctd` und `scanulog` an.

Das Ausgabeformat von `ulog-acctd` muss das folgende spezielle Format haben:

```
accounting format="%h\t%t\t%p\t%s\t%S\t%d\t%D\t%P\t%b\t\"%i\"\t\"%o\"\t\"%f\"\n"
```

Dies ist das Default-Format. Die Konfiguration von Scanulog erfolgt in einer Datei mit beliebigem Namen.

```
LogfilePath /var/log/ulog-acctd/account.log
OutputPath /var/www/traffic/
Bzip2Path /usr/bin/bzip2
CreateBzip2 true
LocalNet 192.168.0.0
LocalNetMask 24
```

Bei dem Aufruf von Scanulog sollten Sie den `ulog-acctd`-Server vorübergehend anhalten und erst im Anschluss weiterlaufen lassen:

```
#!/bin/bash

kill -TSTP $(cat /var/run/ulog-acctd.pid)
/usr/local/scanulog/scanulog /usr/local/scanulog/config
kill -CONT $(cat /var/run/ulog-acctd.pid)
```

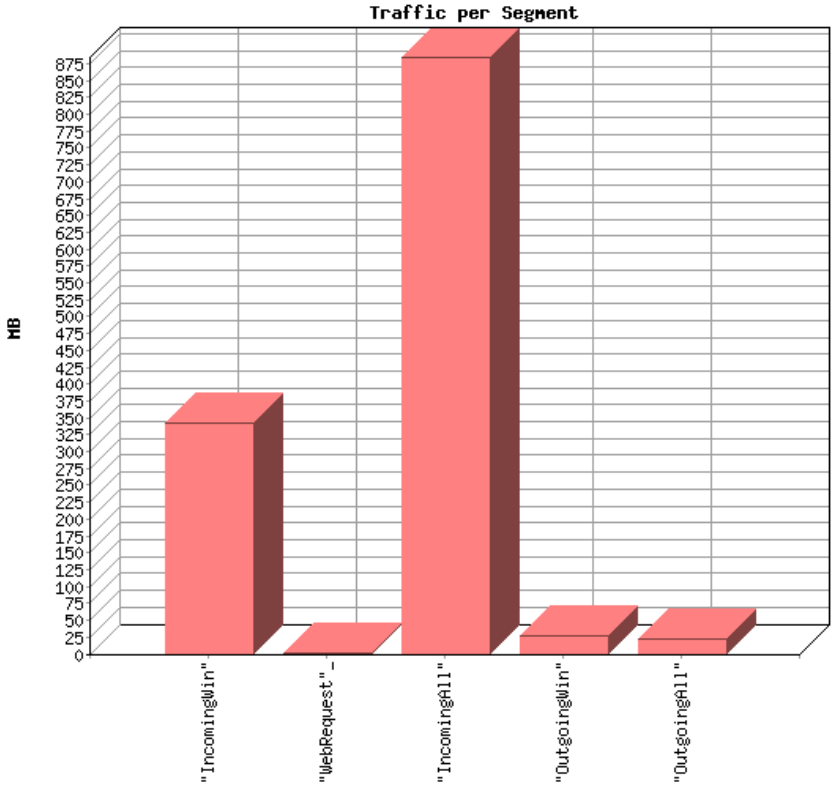


Abbildung 12.8: Scanulog erzeugt aus den Daten grafische Darstellungen.

Dies können Sie auch über einen Cronjob in regelmäßigen Abständen aufrufen. Anschließend können Sie über einen Webserver die Dateien in dem Verzeichnis `/var/www/traffic` betrachten (siehe Abbildung 12.8).

12.5 Nulog

Nulog (*http://www.inl.fr/Nulog.html*) ist ein Frontend für das Ulogd-Mysql-Plugin. Mit Nulog (ehemals ulog-php) können Sie webbasiert die Protokolle analysieren, die von Ulogd geschrieben werden. Nulog wird für die NuFW, eine authentifizierende Firewall für Linux, geschrieben. Allerdings können Sie Nulog auch auf jeder normalen Iptables-Firewall einsetzen, die den Ulogd-Daemon nutzt. Es handelt sich bei Nulog um eine Reihe von PHP-Skripten, die auf die Mysql-Datenbank zugreifen. Diese Datenbank wird von Ulogd (siehe Abschnitt 24.3) oder Specter (siehe Abschnitt 24.4) mit Werten gefüllt.

Mit Hilfe von Nulog können Sie diese Daten dann mit einem Browser analysieren (Abbildung 12.9).

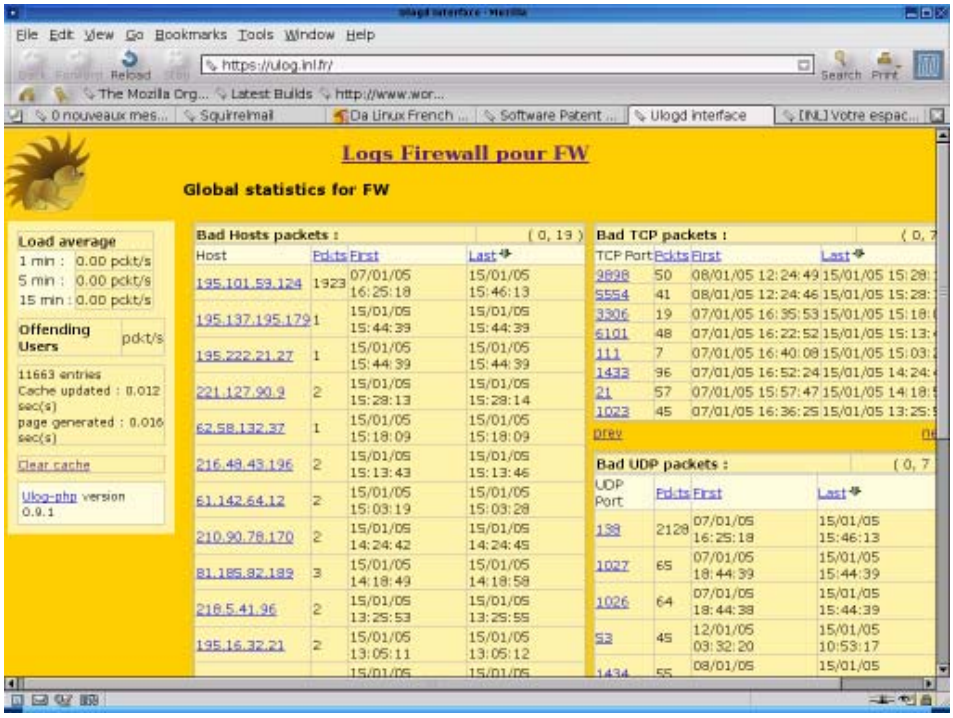


Abbildung 12.9: Nulog bietet die Analyse über einen Webserver.

12.6 EpyLog Log Analyzer

Der EpyLog Log Analyzer (*http://linux.duke.edu/projects/epylog/*) ist ein recht neuer Syslog-Parser, der die Protokolldateien liest, verarbeitet und einen leicht lesbaren HTML-Bericht erzeugt. Dieser Bericht wird dann per E-Mail versandt. EpyLog wurde für Umgebungen mit vielen Log-Servern geschrieben, die über den Syslog oder den Syslog-ng auf einen zentralen Logserver protokollieren (siehe Kapitel 10). Dort verarbeitet es dann die Protokolle. Es ähnelt in seiner Funktion damit dem Paket Logwatch (*http://www.logwatch.org*).

Da EpyLog über ein spezielles Firewall-Prozessierungsmodul verfügt, möchte ich es in diesem Kapitel erwähnen.

Die Installation von EpyLog ist sehr einfach. Für viele Distributionen existieren fertige Pakete. Bei Fedora Core ist es im Extras-Kanal enthalten. EpyLog ist in Python geschrieben und verlangt lediglich als Voraussetzung Python-2.2 oder neuer und die `libxml2-python`.

EpyLog wird üblicherweise täglich aufgerufen und erzeugt einen Bericht der letzten 24 Stunden. Dabei können Sie das Erscheinungsbild des Berichts und den E-Mail-Versand in der Konfigurationsdatei `/etc/epylog/epylog.conf` anpassen. Meist

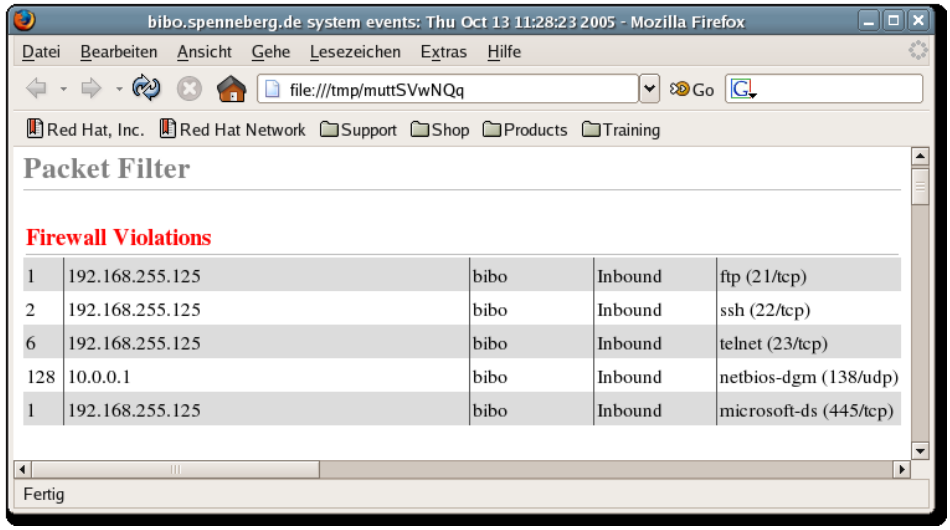


Abbildung 12.10: EpyLog erzeugt einen HTML-Bericht, in dem die Firewall-Meldungen zusammengefasst werden.

sind jedoch die Default-Einstellungen bereits ausreichend. Bei seinem Aufruf erzeugt dann EpyLog einen Bericht, der auch die Protokollmeldungen der Firewall beinhaltet. Hier soll nur kurz ein Auszug eines Berichts zur Demonstration gezeigt werden (Abbildung 12.10).

EpyLog kann so die Echtzeit-Protokollanalyse durch die Erzeugung von Berichten unterstützen, die auch andere Meldungen erfassen.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

13 Administrationsoberflächen

In diesem Kapitel möchte ich Ihnen einige Administrationsoberflächen vorstellen, die mir besonders gut gefallen haben oder die gewisse Probleme besonders intelligent lösen. Es kann sich dabei nur um eine subjektive Auswahl der allgemein zur Verfügung stehenden Oberflächen handeln. Wenn Ihr favorisiertes Werkzeug nicht dabei ist, verzeihen Sie es mir hoffentlich. Wenn Sie der Meinung sind, dass es auf jeden Fall dazugehört, schreiben Sie mir eine E-Mail. Vielleicht kenne ich es einfach noch nicht.

Da die grafischen Werkzeuge am einfachsten durch die Darstellung der Screenshots beschrieben werden können, befinden sich in diesem Kapitel mehr Bilder als im gesamten restlichen Buch zusammen.

13.1 Firewall Builder

Eine der fortgeschrittensten grafischen Oberflächen für die Konfiguration einer Linux-Firewall mit Iptables ist sicherlich der Firewall Builder (*http://www.fwbuilder.org*). Seine grafische Erscheinung (siehe Abbildung 13.1) ist einem kommerziellen Firewall-Produkt nachempfunden worden und hat einige sehr interessante Eigenschaften:

- Abstraktion von Rechnern und Netzen in Objekten
- Echtes Drag-and-Drop von Objekten
- Speicherung in XML-Format
- Erzeugung der Konfiguration auf einer Workstation und automatische Übertragung der Firewall-Konfiguration mit SCP auf die Firewall
- Template für die einfache Erzeugung einer neuen Firewall-Konfiguration
- Unterstützung einer Bridge-Firewall
- Ein Handbuch mit mehr als 100 Seiten

Firewall Builder unterstützt aktuell die Erzeugung von Firewall-Konfigurationen für Iptables, IP-Filter (FreeBSD, OpenBSD und Solaris) und OpenBSD PF. Ein zusätzliches kommerzielles Modul erlaubt auch die Generierung von Cisco PIX-Firewall-Konfigurationen. Sie können Firewall Builder unter Linux, FreeBSD, MacOS X und Windows XP einsetzen. Für die letzteren beiden Betriebssysteme können Sie die binären Pakete von *http://www.netcitadel.com/* herunterladen. Diese sind für 30 Tage

Abbildung 13.1: Beim Start von Firewall Builder können Sie wählen, ob Sie ein neues Projekt beginnen möchten.

ohne Einschränkung nutzbar. Anschließend müssen Sie für $ 49,95 eine Lizenz kaufen. Die Lizenz für das Firewall Builder-Modul für die Cisco PIX kostet $ 500,00. Dieses Modul ist aber auch in den ersten 30 Tagen ohne Lizenz nutzbar. Für alle weiteren unterstützten Betriebssysteme und Zielplattformen ist Firewall Builder unter der GPL freigegeben.

Für die einfache Installation finden Sie auf der Homepage RPM-Pakete für Fedora Core-, Red Hat-, SUSE-, Devillinux-, FloppyFW- und Mandrake-Distributionen. Bei der Debian-Distribution kann Firewall Builder einfach mit dem apt-get-Werkzeug nachinstalliert werden, da es Bestandteil der Stable-Distribution ist. Die Installation aus den Quellarchiven werde ich daher hier nicht beschreiben.

Für eine funktionsfähige Installation müssen Sie die folgenden drei Pakete installieren:

1. libfwbuilder
2. fwbuilder
3. fwbuilder-ipt

Sobald Sie diese Pakete installiert haben, können Sie Firewall Builder starten. Hierzu rufen Sie einfach den Befehl `fwbuilder` auf. Anschließend werden Sie von einem Popup-Fenster gefragt, ob Sie ein neues Projekt beginnen möchten oder ein existierendes Projekt öffnen möchten (Abbildung 13.1).

Wählen Sie hier `Create new project file`, und geben Sie für das Projekt einen Dateinamen im nächsten Dialog an. Dann können Sie durch Anwählen von `Weiter›` zum nächsten Dialog gelangen (Abbildung 13.2).

Hier können Sie Firewall Builder anweisen, die verschiedenen Versionen und Ihre Änderungen an der Konfiguration mit einem Versionskontrollsystem zu überwachen. Damit können Sie später immer wieder zu alten Versionen Ihrer Konfiguration zurückkehren.

Sobald Sie auch diesen Dialog bestätigt haben, befinden Sie sich in der Hauptansicht der Applikation (Abbildung 13.3).

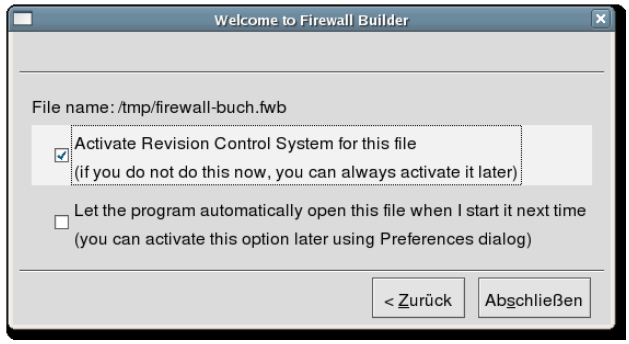


Abbildung 13.2: Firewall Builder kann direkt Ihre Firewall-Konfiguration mit einem Versionskontrollsystem überwachen.

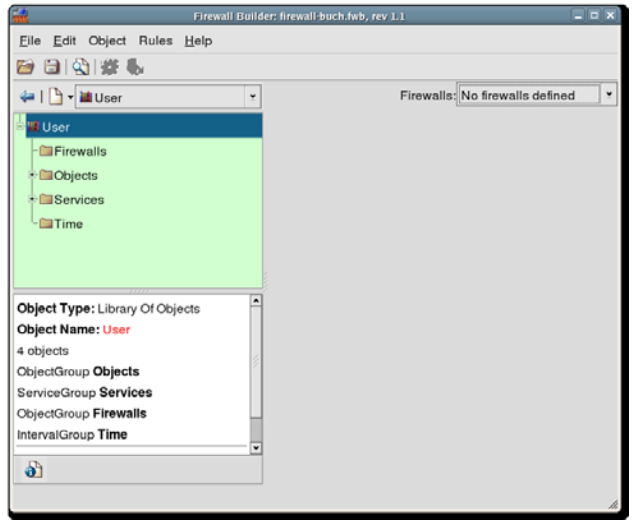


Abbildung 13.3: Bei dem Start ist die Oberfläche von Firewall Builder zunächst leer.

Sie beginnen die Konfiguration mit dem Erzeugen einer neuen Firewall. Hierzu klicken Sie entweder mit der rechten Maustaste auf den Firewall-Ordner in der linken Spalte, oder Sie klicken mit der linken Maustaste auf das `New Object`-Icon neben der Bibliotheksauswahl und wählen `New Firewall`. Dann müssen Sie einen Namen für die Firewall vergeben und das Zielbetriebssystem auswählen. Die Verwendung von Templates erleichtert Ihnen die weitere Konfiguration der Firewall.

Nun können Sie ein vorkonfiguriertes Template für die weitere Anpassung auswählen. Insgesamt gibt es sechs verschiedene Templates:

Abbildung 13.4: Firewall Builder unterstützt auch FreeBSD, Solaris, MacOS X und andere.

- `fw template 1`: Eine Firewall mit zwei Netzwerkkarten. Die externe Netzwerkkarte hat eine dynamische Adresse. Der Zugriff von innen nach außen ist nicht eingeschränkt.
- `fw template 2`: Dieses Template entspricht dem `fw template 1`. Zusätzlich bietet die Firewall DHCP- und DNS-Dienste für das interne Netz an.
- `fw template 3`: Diese Firewall besitzt drei Netzwerkkarten. An der `eth2` ist die DMZ angeschlossen.
- `host fw template 1`: Dieses Template schützt einen einzelnen Rechner. Lediglich SSH-Zugriff ist erlaubt.
- `linksys firewall`: Dieses Template ist für die Linux-Firmware von Sveasoft (*http://www.sveasoft.com*) vorbereitet. Die Netzwerkkarte `br0` ist die innere, und `vlan1` ist die äußere Netzwerkkarte.
- `web server`: Dieses Template schützt einen Webserver. Es erlaubt den Zugriff auf den Port 80 und 443.

Wählen Sie das Template, das Ihrer Konstellation am nächsten kommt. Für dieses Beispiel habe ich das `fw template 2` gewählt (Abbildung 13.5).

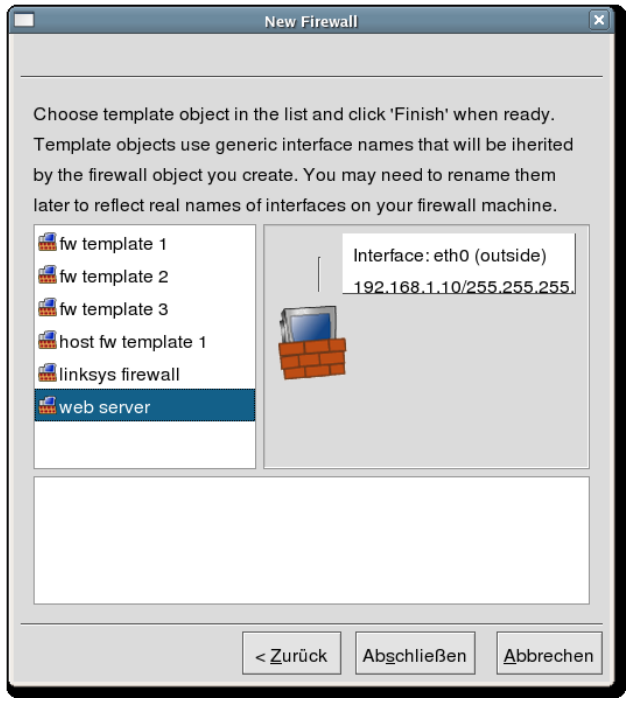


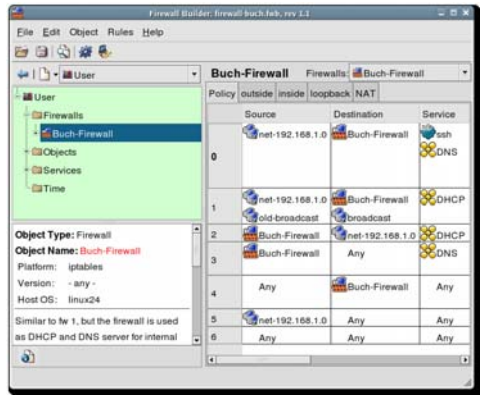
Abbildung 13.5: Mit den Templates können Sie sich viel Arbeit sparen.

Nun werden Sie zwei Fenster sehen. Im Hauptfenster (Abbildung 13.6) finden Sie bereits einige Regeln. In dem Fenster *Firewall* können Sie weitere Einstellungen vornehmen.

Interessant in dem letzteren Fenster sind die Einstellungen der Iptables-Version und weitere Einstellungen zum Betriebssystem und zur Firewall. Nach Anwahl der `Host OS Settings ...` können Sie den Kernel über das `/proc`-Interface konfigurieren (Abbildung 13.7).

Bei den `Firewall Settings ...` können Sie einstellen, wie die Firewall-Regeln aufgebaut werden sollen. Sie können Einfluss auf die Erzeugung der Regeln, die Installation des Skripts und die Protokollierung nehmen. Dazu können Sie zum Beispiel entscheiden, ob die Firewall auf einer Bridge installiert wird, wie die Pakete abgelehnt werden sollen und ob bei einem Neustart der Firewall alte Verbindungen weiter erlaubt sein sollen (Abbildung 13.8).

Um nun zum Beispiel die Regel Nummer 5 zu ändern und den Zugriff nur auf einen bestimmten Dienst zu erlauben, wählen Sie zunächst eine andere Bibliothek aus. Klicken Sie oben links `User` an, und wählen Sie die `Standard`-Bibliothek aus. Dort wählen Sie den Ordner `Services-TCP`. Dort wählen Sie dann den Dienst `http` aus und ziehen ihn in der Regel 5 in die Spalte Service und lassen ihn los (Abbildung 13.9).



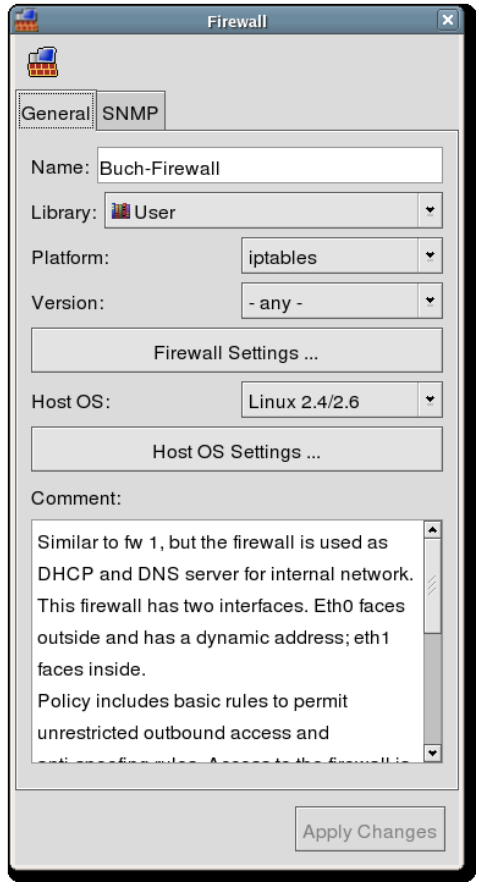


Abbildung 13.6: Nach Auswahl des Templates sind viele Einstellungen bereits vorgenommen worden.

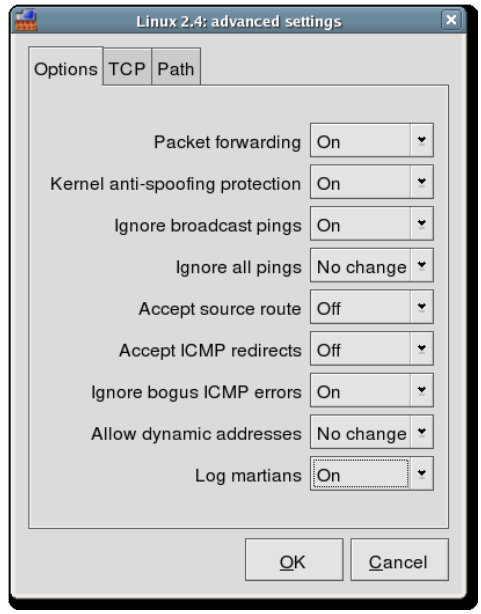


Abbildung 13.7: Firewall Builder bietet Ihnen auch die Konfiguration der Einstellungen im /proc-Verzeichnis.

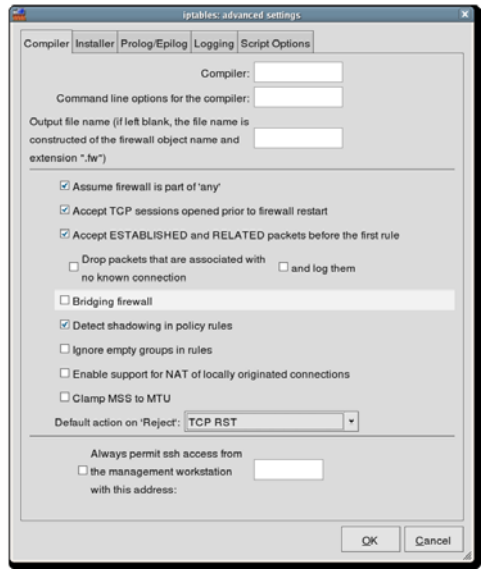


Abbildung 13.8: Firewall Builder erlaubt den Zugriff auf jede Einstellung.

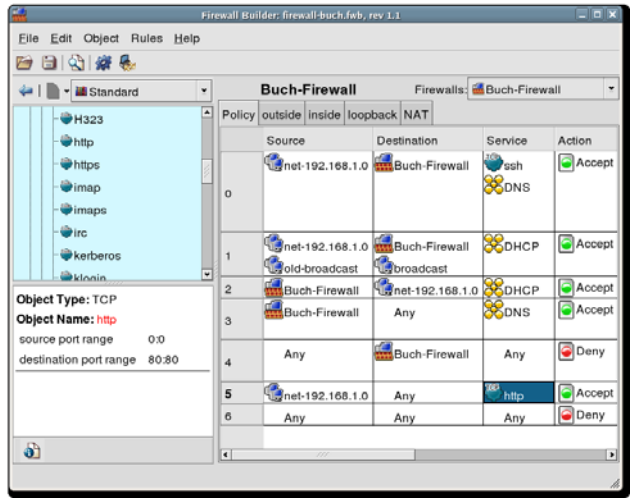


Abbildung 13.9: Sie können per Drag-and-Drop einen Dienst einer Regel hinzufügen.

Um nun eine Regel hinzuzufügen, wählen Sie aus dem Menü `Rules/Add Rule Below`. Ziehen Sie nun aus der Standard-Bibliothek den UDP-Dienst `domain` in die Spalte `Service` der neuen Regel. Nach einem Rechtsklick auf das `Deny` in der Spalte `Action` wählen Sie als neue Action `Accept`. Um nun auch das Netz als Source zu definieren, wählen Sie das Netz in einer anderen Zeile aus, kopieren es und fügen es mit `Paste` als Source in dieser Regel wieder ein (Abbildung 13.10).

Tipp

Sie können auch Netzwerkobjekte und Ports in Gruppen zusammenfassen. Diese Administration der Gruppen kann mit Drag-and-Drop erfolgen. So können Sie die beiden Regeln für den Zugriff auf HTTP und DNS auch zusammenfassen.

Auch die Reihenfolge der Regeln können Sie einfach ändern. Dazu aktivieren Sie die Regel mit der rechten Maustaste und wählen `Move`.

Kontrollieren Sie auch die NAT-Regeln der Firewall auf der entsprechenden Registerkarte (Abbildung 13.11).

Sobald Sie mit Ihren Regeln zufrieden sind, können Sie die Regeln in die Iptables-Sprache übersetzen lassen. Hierzu wählen Sie `Rules-Compile` (Abbildung 13.12).

Wenn Sie die Regeln nicht auf dem Zielsystem erzeugt haben, können Sie diese mit Firewall Builder auch dort installieren. Hierzu wählen Sie `Rules/Install`. In dem

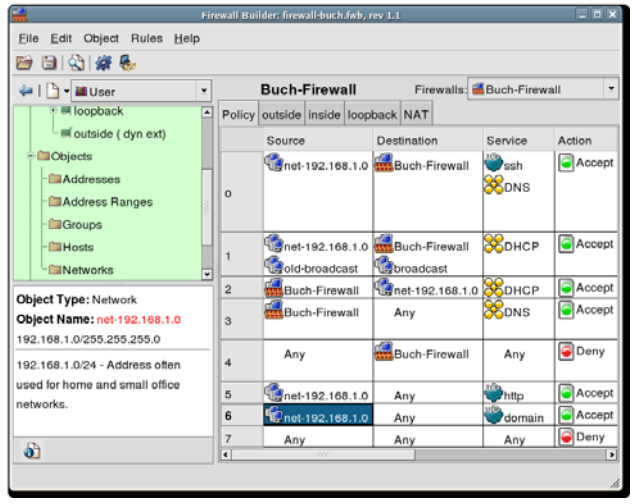


Abbildung 13.10: Sie können auch sehr einfach eine Regel hinzufügen.

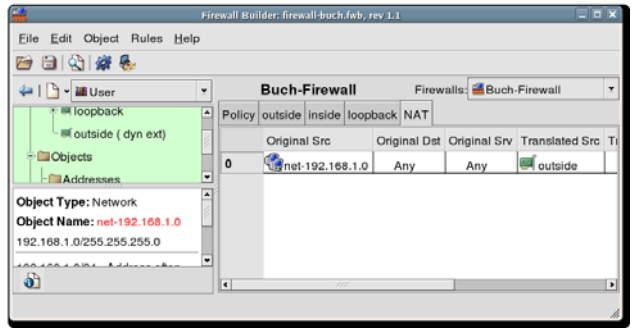


Abbildung 13.11: Auch die NAT-Regeln passen Sie mit dem Firewall Builder an.

nächsten Dialog können Sie den Benutzer und das Kennwort für die Installation angeben. Firewall Builder wird nun mit Secure-Copy die Iptables-Regeln auf dem Zielsystem installieren (Abbildung 13.13).

Firewall Builder bietet weitere sehr mächtige Funktionen, die ich hier nicht aufzählen möchte, da der User's Guide sehr ausführlich auf über 110 Seiten die verschiedenen Möglichkeiten darstellt. Ich hoffe, dass ich Ihnen einen einfachen und schnellen Einstieg ermöglicht habe.

Firewall Builder ist ein sehr gutes Werkzeug für die Konfiguration einer durchschnittlichen Firewall. Bei komplizierten Setups ziehe ich persönlich immer noch ein Skript vor, da das Regelwerk in Firewall Builder schnell unübersichtlich werden kann. In einem Skript haben Sie die Möglichkeit, selbst Variablen zu definieren und benutzerdefinierte Ketten zu generieren und so Ihre Regeln logisch zu gruppieren.

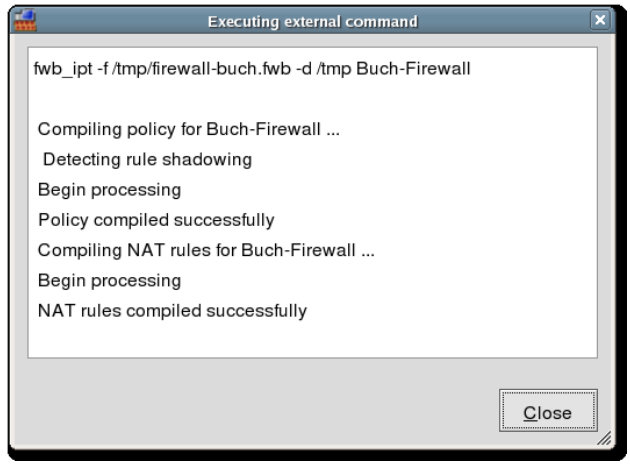


Abbildung 13.12: Sie können die Übersetzung in die Iptables-Regeln beobachten.

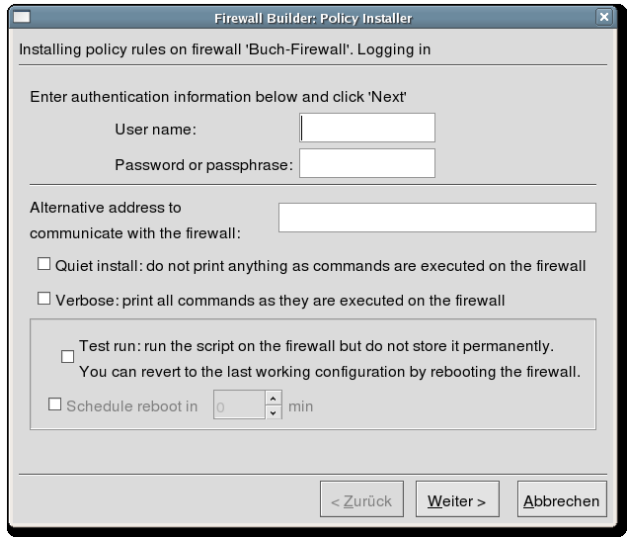


Abbildung 13.13: Firewall Builder kann auch die Regeln auf dem Zielsystem installieren.

Firewall Builder nutzt ebenfalls benutzerdefinierte Ketten, Sie können die Verwendung jedoch nicht steuern. Der Firewall Builder erzeugt für jede kompliziertere grafische Regel eine derartige benutzerdefinierte Kette. Dennoch eignet sich das Werkzeug für mittlere Regelsätze sehr gut, da Sie zusätzliche Kommentare vergeben können und die Verwendung der grafischen Objekte das Fehlen von Variablen mehr als aufwiegt.

13.2 Firestarter

Der Firestarter (*http://www.fs-security.com*) verfolgt eine etwas andere Philosophie als der Firewall Builder. Während der Firewall Builder Ihnen sämtliche Freiheiten bei der Definition Ihrer Firewall lässt und lediglich die Iptables-Details vor Ihnen versteckt, versucht der Firestarter eine möglichst einfache Schnittstelle für die Installation und Konfiguration einer Firewall zu sein. Er ist mit einer Personal-Desktop-Firewall vergleichbar, wie sie auf einigen kommerziellen Betriebssystemen zur Verfügung steht.

Der Firestarter besitzt eine einfache, aber sehr ansprechende grafische Oberfläche (siehe Abbildung 13.14), mit der Sie die Firewall an- oder abschalten, aktuelle Regelverstöße anzeigen und Rechner sperren oder freischalten können.

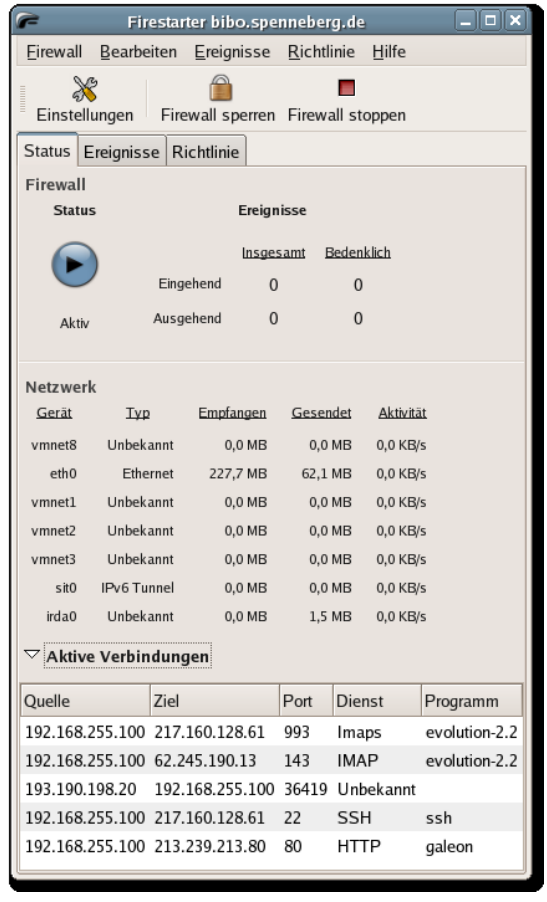


Abbildung 13.14: Der Firestarter ist eine Personal-Desktop-Firewall.

Auch Firestarter verfügt über ein sehr ausführliches Handbuch, so dass ich mich hier auf einige wenige Hinweise beschränken möchte.

Direkt nach dem Start heißt ein Firewall-Assistent Sie herzlich willkommen. Für viele Anwender erfreulich, erkennt Firestarter die konfigurierte Sprache und unterstützt dann auch Deutsch (Abbildung 13.15).

Auf den nächsten Bildschirmen wählen Sie zunächst die Netzwerkkarte aus, die mit dem Internet verbunden ist. Dabei können Sie auch die Unterstützung einer dynamischen IP-Adresse auf dieser Netzwerkkarte aktivieren. Anschließend werden Sie gefragt, ob Sie die Internet-Verbindung mit anderen Benutzern teilen möchten. Wenn Ihr System über zwei Netzwerkkarten verfügt und über eine Netzwerkkarte mit dem Internet und über die andere Netzwerkkarte mit einem lokalen Netz verbunden ist, können Sie hier für das lokale Netz die Internetverbindung freischalten. Eine besondere Funktion von Firestarter ist die Möglichkeit, hier direkt einen DHCP-Server für das interne Netz zu aktivieren (Abbildung 13.16). Dafür muss jedoch auf Ihrem System ein DHCP-Server installiert sein.

Abbildung 13.15: Der Firestarter unterstützt auch die deutsche Sprache.

Abbildung 13.16: Firestarter kann auch als Firewall für ein Netzwerk eingesetzt werden.

Auf dem letzten Bildschirm bleibt Ihnen nun nur noch der Start der Firewall. Achtung, falls Sie mit dem Firewall-Rechner gerade über das Netzwerk verbunden sind und Firestarter über das Netzwerk gestartet haben, sollten Sie die Firewall noch nicht starten, sondern erst eine Richtlinie erzeugen, die diesen Zugriff erlaubt.

Jetzt befinden Sie sich in dem Hauptfenster von Firestarter. Sie können nun die Firewall starten oder stoppen, die Einstellungen überprüfen, Ereignisse beobachten und Richtlinien hinzufügen (Abbildung 13.17).

Abbildung 13.17: Sie können auch Richtlinien hinzufügen.

Abbildung 13.18: Auf der Status-Seite erhalten Sie einen Überblick über eingehende und ausgehende Ereignisse.

Sobald Regelverletzungen stattfinden, erkennen Sie dies auf der Statusseite. Dort werden die Ereignisse gezählt (Abbildung 13.18). Wenn Sie dann auf die Registerkarte `Ereignisse` wechseln, können Sie die Regelverletzungen tatsächlich studieren.

Durch einen Rechtsklick auf eines der Ereignisse können Sie wählen, ob Sie alle weiteren Verbindungen von diesem Rechner ablehnen oder akzeptieren möchten, diesen Dienst freischalten möchten oder grundsätzlich diese Ereignisse nicht mehr protokollieren möchten.

Wenn Sie das Firestarter-Paket als RPM- oder Debian-Paket installiert haben, läuft die Firewall sogar nach einem Neustart des Systems. Um dies zu erreichen, wurde Firestarter als Systemdienst eingebunden und wird über ein Init-Skript automatisch bei einem Neustart ebenfalls gestartet. Die grafische Oberfläche benötigen Sie dann nur für die Konfiguration und Überwachung. Wenn Ihre Firewall über keinen X-Server verfügt, können Sie das grafische Werkzeug auch über das Netzwerk aufrufen!

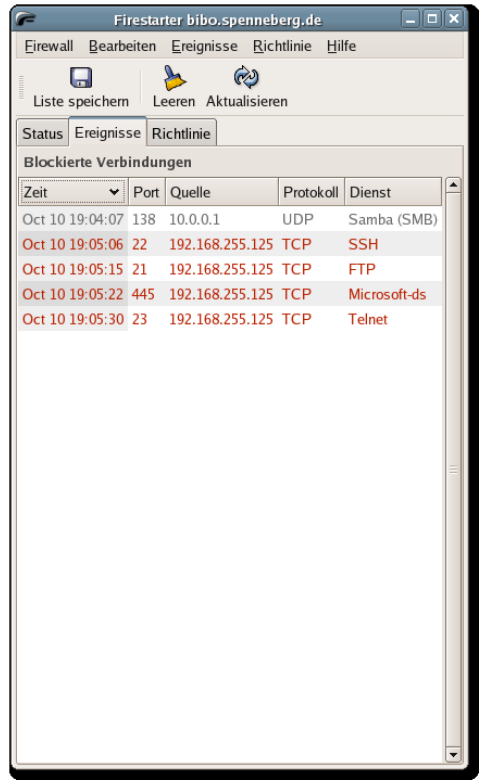


Abbildung 13.19: Die Ereignisse im Detail zeigt Firestarter nach Auswahl der Registerkarte an.

Um Firestarter zu installieren, gibt es mehrere Möglichkeiten. Am einfachsten installieren Sie Firestarter als RPM- oder Debian-Paket. Auf der Firestarter-Homepage finden Sie Pakete für alle aktuellen Distributionen inklusive Ubuntu und Gentoo.

Für kleine Installationen sind die Möglichkeiten, die Firestarter Ihnen bietet, häufig vollkommen ausreichend. Die Konfiguration komplizierter Regelsätze ist mit Firestarter nicht möglich, da Sie nicht selbst die Iptables-Regeln modifizieren oder anpassen können.

13.3 Shorewall (Shoreline Firewall)

Die Shoreline Firewall ist eine sehr komplexe Firewall, die Ihre Konfiguration aus Skripten liest und mit dem Iptables-Befehl in Firewall-Regeln umsetzt. Ihre Anwendung wird nicht durch eine grafische Oberfläche unterstützt. Es gibt jedoch für Webmin (*http://www.webmin.com*) ein leider veraltetes Shorewall-Modul. Dennoch verwenden viele Anwender gern Shorewall, da es sehr flexibel den Aufbau von komplizierten Firewalls auf der Distribution ihrer Wahl ermöglicht.

Shorewall wird im Moment im Wesentlichen von einem einzigen Entwickler gepflegt: Tom Eastep. Daher sollten Sie sich natürlich speziell bei einer Firewall überlegen, ob Sie sich auf die Leistung eines einzigen Entwicklers verlassen möchten. Sollte der Entwickler seine Arbeit einstellen, wissen Sie nicht, ob das Projekt weiter gepflegt wird.

Exkurs

Am 22. Mai 2005 hat Tom Eastep seinen Rückzug von dem Projekt bekannt gegeben. Im Wesentlichen waren persönliche Gründe und Überlastung der Grund dafür:

Zitat:

```
Since I began developing Shorewall:

a) I have gained over 60 pounds in weight.
b) My lawn and landscaping have become an embarrassment in the neighborhood.
c) I have begun exhibiting addictive behavior toward Linux and Shorewall.
d) I have developed sleep disorders (I use a breathing aid at night)
e) I dislike my life.
```

Anscheinend hat sich Tom jedoch entschieden, Shorewall weiterzupflegen, denn seit Anfang Oktober gibt es sogar eine Shorewall 3.0 Beta.

Die Installation von Shorewall ist sehr einfach, da Sie auf der Homepage *http://www.shorewall.net* Pakete für sämtliche aktuelle Distributionen finden. Teilweise ist Shorewall bereits in den Distributionen integriert.

13.3.1 Das Shorewall-Konzept

Die gesamte Konfiguration befindet sich in dem Verzeichnis `/etc/shorewall`. Die wichtigste Datei ist die Datei `zones`, in der die Firewall-Zonen definiert werden. Eine typische `zones`-Datei hat den folgenden Inhalt:

```
#ZONE   DISPLAY         COMMENTS
net     Internet        The big bad Internet
loc     Local           Local Network
dmz     DMZ             Demilitarized zone.
```

Diese Firewall verfügt über drei Netzwerkkarten. Per Default gibt es immer noch zusätzlich eine weitere Zone für die Firewall selbst: `fw`. Die zweite Datei, die Sie betrachten sollten, ist die Datei `policy`. Hier definieren Sie die Default-Policies für den Verkehr von einer in die andere Zone. Es gibt sechs verschiedene Policies, die Sie definieren können: `ACCEPT`, `DROP`, `REJECT`, `QUEUE`, `CONTINUE` oder `NONE`. Eine typische `policy`-Datei sieht so aus:

```
#SOURCE  DEST   POLICY       LOG            LIMIT:BURST
#                            LEVEL
loc      net    ACCEPT
net      all    DROP         info

# THE FOLLOWING POLICY MUST BE LAST
#
all      all    REJECT       info
```

Über den Log-Level definieren Sie, ob und wie die zutreffenden Pakete protokolliert werden sollen. Falls Sie den Ulog-Daemon einsetzen möchten, geben Sie hier `ULOG` an. In der letzten Spalte können Sie die maximale Rate der TCP-Verbindungen und den erlaubten Burst angeben (siehe Abschnitt 16.19).

Die Ausnahmen dieser Default-Policies werden dann in der Datei `rules` definiert. Sie müssen hier nur Regeln definieren, die den Verbindungsaufbau erlauben oder ablehnen. Die Shorewall kümmert sich dann selbst um alle weiteren Pakete, die zu der aufgebauten Verbindung gehören (State: ESTABLISHED) oder mit ihr verwandt sind (State: RELATED). Um zum Beispiel aus dem internen Netz mit der Secure Shell auf die Firewall zuzugreifen und die Firewall per https Updates aus dem Internet (z.B. Red Hat Network) downloaden zu lassen, müssen Sie die folgende Regel in der Datei `rules` einfügen:

```
#ACTION SOURCE  DEST PROTO   DEST    SOURCE   ORIGINAL  RATE   USER/
#                            PORT    PORT(S)  DEST      LIMIT  GROUP
ACCEPT  loc     fw   tcp     22
ACCEPT  fw      net  tcp     53
ACCEPT  fw      net  udp     53
ACCEPT  fw      net  tcp     443
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Tipp

Wenn es Sie stört, dass Sie zwei Zeilen für den DNS-Verkehr in der Datei `rules` definieren müssen, können Sie auch das mächtige Action-Konzept von Shorewall nutzen. Die Actions können Sie selbst definieren, aber Shorewall verfügt auch bereits über eine Reihe von vorkonfigurierten Actions in `/usr/share/shorewall/`. Die Action `AllowDNS` wurde so definiert:

```
#
# Shorewall version 2.4 - AllowDNS Action
#
# /usr/share/shorewall/action.AllowDNS
#
#       This action accepts DNS traffic.
#
```

```
###############################################################################
#TARGET SOURCE  DEST    PROTO   DEST    SOURCE  ORIGINAL      RATE    USER/
#                              PORT    PORT(S) DEST          LIMIT   GROUP
ACCEPT  -       -       udp     53
ACCEPT  -       -       tcp     53
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Das bedeutet, dass Sie auch folgende Einstellung in der Datei `rules` nutzen können, die das gleiche Ergebnis erzeugt:

```
#ACTION  SOURCE  DEST PROTO   DEST    SOURCE   ORIGINAL  RATE   USER/
#                           PORT    PORT(S)  DEST      LIMIT  GROUP
ACCEPT   loc     fw   tcp     22
AllowDNS fw      net
ACCEPT   fw      net  tcp     443
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Genauso können Sie auch die erste Zeile durch eine `AllowSSH`-Zeile ersetzen, da auch für SSH eine vorkonfigurierte Action vorhanden ist.

Nun müssen Sie noch die Zonen den verschiedenen Netzwerkkarten zuordnen. Dies erfolgt in der Datei `interfaces`.

```
#ZONE      INTERFACE     BROADCAST     OPTIONS
net        eth0          detect        dhcp,routefilter,norfc1918
loc        eth1          detect
dmz        eth2          detect
```

Schließlich fehlt noch die Definition des NAT. Hierzu verwendet Shorewall die Datei `masq`. Um einfach ein Masquerading zu definieren, tragen Sie hier die folgende Zeile ein:

```
#INTERFACE SUBNET    ADDRESS         PROTO   PORT(S) IPSEC
eth0       eth1
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

Diese Zeile maskiert jede über `eth0` ausgehende Verbindung aus dem Subnetz, das über die Netzwerkkarte `eth1` angebunden ist. Alternativ können Sie für `eth1` auch das Subnetz in Form von `192.168.0.0/24` angeben.

Nun müssen Sie nur noch Shorewall starten. Seit der Version 1.3.9 wird Shorewall automatisch zum Boot-Zeitpunkt des Rechners über ein Init-Skript gestartet. Ob dies bei Ihnen auch der Fall ist, können Sie mit dem Befehl `chkconfig` überprüfen.

```
#  chkconfig shorewall --list
shorewall       0:Aus   1:Aus   2:Ein   3:Ein   4:Ein   5:Ein   6:Aus
```

Damit jedoch nicht eine fehlerhafte oder fehlende Konfiguration den Zugriff auf den Rechner verhindert, ist der tatsächliche Start noch deaktiviert. Bei den aktuellen Distributionen wird der Start über die Datei `/etc/shorewall/shorewall.conf` gesteuert. Diese Datei enthält zu Beginn die Variable `STARTUP_ENABLED=No`. Setzen Sie diese Variable auf `Yes`, und Sie können Shorewall starten. Hierfür verwenden Sie den Befehl `shorewall`. Dieser Befehl hat die folgenden Optionen:

- `help`: Zeigt die Hilfe an.
- `start`: Dies startet die Shorewall.
- `stop`: Dies stoppt die Shorewall. Dabei werden das Forwarding und das Routing deaktiviert. Wenn Sie diesen Befehl aus der Ferne durchführen, sollte Ihre IP-Adresse in der Datei `routestopped` enthalten sein, damit die Shorewall anschließend noch die Kommunikation mit Ihrer IP-Adresse erlaubt.
- `clear`: Entfernt sämtliche Shorewall-Regeln und -Policies. Der Rechner ist anschließend von außen erreichbar.
- `restart`: Führt einen Neustart der Shorewall durch.
- `save`: Speichert die aktuelle Konfiguration in einer Backup-Datei für eine spätere Wiederherstellung ab.
- `restore`: Stellt die Konfiguration wieder her.
- `forget`: Entfernt die Backup-Datei.
- `check`: Prüft die Konfiguration.
- `try <Conf> [<timeout>]`: Führt einen Neustart der Shorewall mit dem angegebenen Konfigurationsverzeichnis durch. Allerdings wird, sobald ein Fehler auftritt, erneut ein Neustart mit der Default-Konfiguration in `/etc/shorewall` durchgeführt. Wenn Sie einen Timeout angeben, dann wird der Neustart immer nach Ablauf des Timeouts durchgeführt. Damit können Sie auch aus der Ferne eine neue Konfiguration testen, ohne befürchten zu müssen, sich dauerhaft auszuschließen.

Shorewall unterstützt die Verwendung von alternativen Konfigurationsverzeichnissen. Um diese mächtige Funktion zu nutzen, erzeugen Sie einfach ein neues Verzeichnis `/etc/test` und kopieren die Dateien, die Sie ändern möchten, in dieses Verzeichnis. Nach ihrer Modifikation können Sie zunächst die Konfiguration auf ihre syntaktische Korrektheit prüfen: `shorewall check /etc/test`. In dem Verzeichnis `/etc/test` fehlende Dateien werden automatisch aus dem Verzeichnis `/etc/shorewall` geladen. Nachdem Sie alle Fehler korrigiert haben, können Sie mit `shorewall try /etc/test 30` die neue Konfiguration prüfen. Sollten Sie sich bei diesem Vorgang selbst ausgeschlossen haben, müssen Sie nur 30 Sekunden warten. Dann wird die Shorewall sich selbst wieder zurücksetzen! Ist alles zu Ihrer Zufriedenheit, so kopieren Sie die modifizierten Dateien in das Verzeichnis `/etc/shorewall`, und die Firewall wird nun nach einem Neustart die aktuelle Konfiguration verwenden.

13.3.2 Die Shorewall-Dateien

Dieses Kapitel soll Ihnen kurz einen Eindruck von den von Shorewall verwendeten Dateien und ihren Funktionen vermitteln. Diese Information wird sicherlich nicht ausreichen, damit Sie die Dateien in Ihrer ganzen Fülle verstehen und administrieren können – dafür ist das Shorewall-Handbuch da –, aber Sie erhalten so einen Überblick über die Möglichkeiten.

accounting

In dieser Datei können Sie Accounting-Regeln angeben. Dies sind Zählregeln, die lediglich bestimmte Pakete zählen, um zum Beispiel den Anteil des HTTP-Verkehrs oder die Anzahl der SMTP-Verbindungen zu zählen.

actions

Hier können Sie Ihre eigenen Actions definieren. Actions sind eine Art Makro, mit der Sie komplizierte Regelsätze vereinfachen können. Beispiele für vordefinierte Shorewall-Actions finden Sie in `/usr/share/shorewall/`.

blacklist

Sie können in der Datei `interfaces` bei den verschiedenen Netzwerkkarten die Option `blacklist` mit angeben. Dann wird diese Datei für die entsprechende Netzwerkkarte ausgewertet. Jede IP-, Netz- oder MAC-Adresse in dieser Datei wird dann automatisch entsprechend der Variablen `BLACKLIST_DISPOSITION` und `BLACKLIST_LOGLEVEL` in der Datei `shorewall.conf` abgewiesen.

continue

In dieser Datei können Sie Befehle eintragen, die nach dem Aufruf des Befehls `shorewall clear` aufgerufen werden sollen. Damit können Sie zum Beispiel nach dem Löschen sämtlicher Regeln doch wieder bestimmte Grundregeln für die Grundsicherheit des Systems aktivieren.

ecn

Die Explicit Congestion Notification (ECN) ist eine sehr nützliche Methode, die eine Verstopfung der Netzwerkverbindung frühzeitig erkennen und verhindern kann. Da ECN jedoch bisher reservierte Bits in den IP- und TCP-Headern benutzt, blockieren viele ältere und kommerzielle Firewalls die Pakete, die ECN nutzen. Wenn Sie dennoch ECN nutzen wollen, können Sie in dieser Datei die Rechner angeben, für die die Shorewall ECN deaktivieren soll.

hosts

In einigen Konstellationen ist es sinnvoll, die Rechner, die über ein und dieselbe Netzwerkkarte mit der Shorewall verbunden sind, in unterschiedliche Zonen ein-

zuteilen. Damit können Sie noch feiner die Regeln für die einzelnen Rechner konfigurieren und zum Beispiel eine Zone `dmzdns` und eine Zone `dmzproxy` definieren. Die Zonen müssen Sie zunächst in der Datei `zones` angeben. Dann ordnen Sie nicht den Zonen in der Datei `interfaces` Netzwerkkarten zu, sondern geben in dieser Datei Subnetze und Rechner an.

init, initdone, start, started, stop und stopped

Hier können Sie Befehle definieren, die vor dem Start von `shorewall start` (`init`) oder nach der Initialisierung des Befehls und vor dem Hinzufügen der Regeln (`initdone`) ausgeführt werden sollen.

Die Dateien `start` und `started` werden nach dem Start der Shorewall ausgeführt. Dabei wird die Datei `started` erst nach dem vollständigen Start der Shorewall aufgerufen (siehe Dokumentation).

Die Datei `stop` wird zu Beginn des Befehls `shorewall stop` ausgeführt, und die Datei `stopped` wird anschließend ausgeführt.

Über diese Dateien können Sie die Shorewall mit eigenen Skripten beliebig erweitern.

interfaces

In dieser Datei ordnen Sie die Zonen verschiedenen Netzwerkkarten zu.

ipsec

In dieser Datei können Sie Regeln für IPsec-Verbindungen hinterlegen. Grundsätzlich können Sie hier zum Beispiel Regeln für die Maximum Segment Size (MSS) setzen. Wenn Sie zusätzliche Regeln setzen möchten, die den IPsec-Verkehr erlauben oder verbieten, müssen Ihr Kernel und Ihr Iptables-Befehl über den Policy-Match (siehe Kapitel 33) verfügen.

maclist

Mit dieser Datei können Sie Regeln definieren, die nur bestimmten MAC-Adressen die Kommunikation erlauben. Damit können Sie einen MAC-Filter erzeugen, wie er häufig auch für WLAN-Anwendungen verwendet wird.

masq

In dieser Datei definieren Sie das Masquerading und Source-NAT. Dabei haben Sie alle Freiheiten, die der Iptables-Befehl Ihnen auch gibt.

modules

Diese Datei lädt alle zum Start der Shorewall benötigten Module.

nat

Mit dieser Datei können Sie 1:1-NAT-Regeln definieren. Achten Sie darauf, dass Sie bei der Shorewall auch ProxyARP verwenden können. In einigen Fällen ist ProxyARP vorzuziehen. Auch ein einfaches Port-Forwarding wird nicht in dieser Datei, sondern in der Datei `rules` definiert.

netmap

Mit dieser Datei können Sie das Iptables-`NETMAP`-Target (siehe Abschnitt 20.5) nutzen. Dieses ermöglicht es Ihnen, sehr einfach jede IP-Adresse aus einem Netz einer IP-Adresse aus einem anderen Netz zuzuordnen.

params

Hier können Sie Variablen definieren, die Sie an anderen Stellen und in anderen Dateien wiederverwenden. Dazu definieren und nutzen Sie die Variablen in einfacher Bourne-Shell-Syntax.

policy

Diese Datei definiert die Default-Policies für die Verbindungen zwischen den verschiedenen Zonen. Alle Ausnahmen dieser Default-Policies werden dann in der Datei `rules` definiert.

providers

Hier können Sie zusätzliche Routing-Tabellen definieren. Dazu verwendet die Shorewall die Advanced-Routing-Funktionen des Kernels. Damit können Sie zum Beispiel Szenarien abdecken, bei denen Sie mehrere Verbindungen zum Internet besitzen und diese gleichzeitig nutzen möchten.

proxyarp

In dieser Datei können Sie Proxy-ARP definieren (siehe auch Kapitel 29).

routes

In dieser Datei können Sie Firewall-Regeln definieren, die dazu führen, dass einzelne Verbindungen anders geroutet werden. Ihr Kernel und Ihr Iptables-Befehl müssen dafür das `ROUTE`-Target (siehe Abschnitt 18.4.3) unterstützen.

routestopped

Wenn Sie die Shorewall stoppen, ist keine Kommunikation mehr möglich. Wenn Sie dennoch, zum Beispiel auf einer Bridge, die Kommunikation erlauben möchten, können Sie in dieser Datei Regeln angeben, die bei einer gestoppten Firewall dennoch Verbindungen akzeptieren.

rules

Diese Datei enthält den eigentlichen Kern des Shorewall-Regelwerkes. Hier definieren Sie Ihre Firewall-Regeln in der abstrakten Shorewall-Syntax. Dabei können Sie auch selbst definierte Actions aus der Datei `action` verwenden.

shorewall.conf

Diese Datei steuert zentral das Verhalten der Shorewall. Hier können Sie zum Beispiel konfigurieren, ob die Shorewall überhaupt startet!

tcrules

Häufig soll eine Firewall auch direkt die zur Verfügung stehende Bandbreite der Internetverbindung regulieren. Dazu unterstützt Shorewall die Quality-of-Service-Funktionen des Linux-Kernels. Hier können Sie Regeln definieren, die Pakete oder Verbindungen markieren und klassifizieren (siehe auch Abschnitt 21.2.1).

tos

Wenn Ihre Infrastruktur noch die Type-of-Service-Bits (TOS) in dem IP-Header unterstützt und Sie diese nutzen möchten, um bestimmte Verbindungen zu priorisieren, können Sie in dieser Datei Regeln definieren, die die TOS-Bits entsprechend setzen (siehe auch Abschnitt 21.2.9).

tunnels

Eine Firewall ist häufig auch der Endpunkt von VPN-Tunneln. Diese Tunnel können Sie in dieser Datei definieren. Die Shorewall wird dann diese Tunnel erlauben. Natürlich müssen Sie zusätzlich zum Beispiel Racoon oder OpenVPN konfigurieren, damit die Tunnel auch aufgebaut werden.

zones

In dieser Datei definieren Sie die Zonen, die von der Firewall überwacht werden sollen. Für die Anzeige können Sie hier jeder Zone einen aussagekräftigen Namen zuweisen.

13.3.3 Weitere Shorewall-Eigenschaften

Die Shorewall unterstützt im Weiteren folgende Funktionen, auf die ich im Rahmen dieses Buches nicht eingehen kann. Diese Funktionen werden aber in der mitgelieferten Dokumentation ausführlich beschrieben und mit Beispielen dokumentiert:

- Tunnel
  - IPv6- in IPv4-Tunnel
  - PPTP-Tunnel
  - IPv4- in IPv4-Tunnel

  - IPsec-Tunnel mit dem Linux-Kernel 2.4 und 2.6
  - OpenVPN-Tunnel
- Bandbreitenbegrenzung
- Firewall im Bridge-Modus
- Mehrere Internetzugänge
- Blacklisting von IP-Adressen

Wenn Sie eine mächtige und flexible Oberfläche suchen, die aber ohne Maus zu bedienen ist, einfach aus der Ferne gewartet werden kann und ein einfaches Backup ermöglicht, ist die Shorewall ein interessanter Kandidat.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

14 Distributionswerkzeuge

Viele Distributionen enthalten auch Werkzeuge für die Verwaltung von Firewalls. In diesem Kapitel werde ich diese Werkzeuge und einige spezielle Firewall-Distributionen vorstellen und deren Besonderheiten erläutern.

14.1 Fedora Core 4

Der Hersteller Red Hat vernachlässigt die Firewall-Funktion bisher am meisten. Nachdem lange Zeit mit `lokkit` nur ein Curses-basiertes Werkzeug (Abbildung 14.1) zur Verfügung stand, gibt es in den aktuellen Distributionen mit `system-config-securitylevel`[1] ein einfaches grafisches Werkzeug. Dieses Werkzeug bietet aber immer noch keine besondere Intelligenz oder Komfortabilität (Abbildung 14.2).

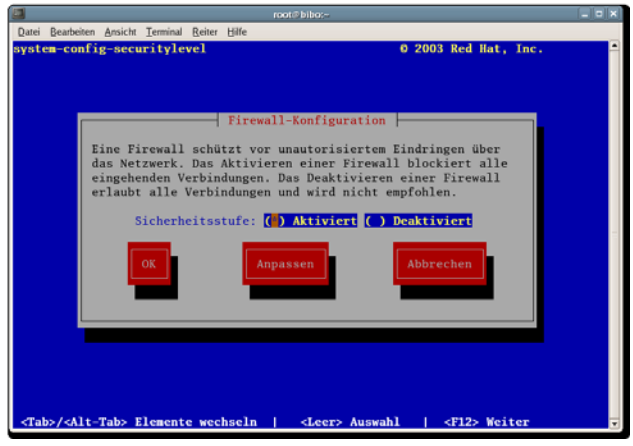


Abbildung 14.1: Das Werkzeug lokkit ist weder schön noch komfortabel. Es ist heute ein textbasiertes Interface des Befehls system-config-securitylevel.

Die Anwendung dieser Werkzeuge für die Konfiguration einer Firewall kann ich nicht empfehlen. In der Fedora Core 4-Distribution befinden sich keine weiteren Werkzeuge zur Pflege und Wartung einer Firewall (von `vi` mal abgesehen). Aller-

[1] Bei älteren Distributionen heißt dieses Werkzeug `redhat-config-securitylevel`.

Abbildung 14.2: Der grafische Befehl system-config-securitylevel erlaubt neben der Firewall auch die Konfiguration von SELinux.

dings befinden sich in dem von Freiwilligen gepflegten und von RedHat geförderten Fedora Core Extras Kanal die folgenden Pakete:

- Firewall Builder (siehe Abschnitt 13.1) und
- Shorewall (siehe Abschnitt 13.3).

Diese können Sie daher recht einfach auf einer Fedora Core-Distribution nutzen. Da ich diese Werkzeuge aber an anderer Stelle in diesem Buch behandele, möchte ich Sie auf die entsprechenden Kapitel verweisen.

14.2 SUSE Linux OSS 10

SUSE liefert seit der Version 8.0 die SUSEfirewall2 aus. Dabei handelt es sich im Wesentlichen um eine Konfigurationsdatei `/etc/sysconfig/SUSEfirewall2` und um eine Reihe von Bash-Skripten, die diese Konfigurationsdatei lesen und in Regeln umsetzen. Die SUSEfirewall2 unterstützt eine Firewall mit drei Zonen: *Innen*, *Außen* und *Entmilitarisiert (DMZ)*. Die Konfiguration kann sowohl über die Konfigurationsdatei direkt als auch über YaST erfolgen. Ich werde hier die Konfiguration mit dem grafischen Werkzeug YaST der Version SUSE Linux OSS 10 erläutern. Dabei werde ich aber auch jeweils die entsprechenden Variablen in der Konfigurationsdatei ansprechen, die von YaST beim entsprechenden Dialog geändert werden.

Da die gesamte Konfigurationsdatei inklusive der Kommentare fast 1000 Zeilen lang ist, werde ich mich hier auf die wesentlichen Punkte beschränken. Auf *http://susefaq.sourceforge.net/articles/firewall/fw_manual.html* finden Sie den Versuch einer Dokumentation der SUSEfirewall2 in einem 110 Seiten starken PDF-Dokument.

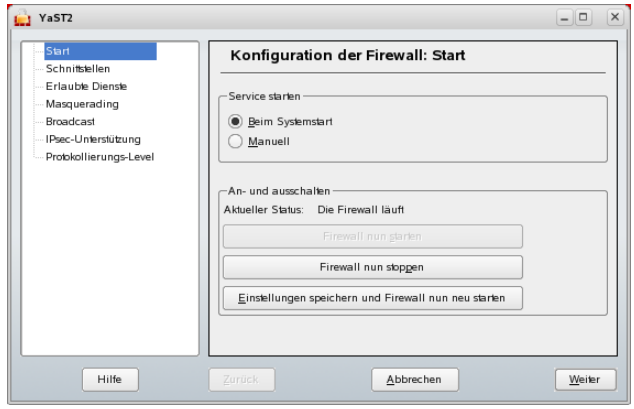


Abbildung 14.3: Sie können mit diesem Dialog die Firewall stoppen oder neu starten.

Sie starten zunächst YaST und wählen dort das Menü `Sicherheit` aus. Dort finden Sie ein Modul `Firewall`. Nach dem Anklicken öffnet sich das YaST2-Firewall-Modul (Abbildung 14.3). Dort können Sie auswählen, ob die SUSEfirewall2 automatisch bei jedem Systemstart oder nur auf manuelle Aufforderung gestartet werden soll. Außerdem erkennen Sie, ob aktuell die Firewall aktiv ist oder nicht.

Ein Neustart der Firewall kann übrigens auch auf der Kommandozeile erfolgen. Hierfür rufen Sie einfach `rcSUSEfirewall2 restart` auf.

Bevor Sie die Firewall konfigurieren können, müssen Sie die Netzwerkkarten festlegen. Hierfür wählen Sie im linken Baum den Punkt `Schnittstellen` aus (Abbildung 14.4). Hier legen Sie fest, welche Karte mit welcher Zone verbunden ist. Die SUSEfirewall2 unterscheidet drei Zonen:

- Interne Zone. Diese darf ungehindert auf die externe Zone zugreifen.
- Externe Zone. Diese Zone hat keinerlei Rechte, außer wenn ein Forwarding definiert ist (siehe weiter unten).
- Entmilitarisierte Zone. Der Zugriff auf die externe Zone ist erlaubt. Ein Zugriff aus der externen Zone in die entmilitarisierte Zone ist nach Konfiguration auch erlaubt.

Wenn Sie die Einstellungen in der Konfigurationsdatei nachvollziehen möchten oder manuell durchführen wollen, müssen Sie die folgenden Variablen editieren:

```
FW_DEV_EXT="any eth-id-00:0c:29:50:05:b0"
FW_DEV_INT="eth-id-00:0c:29:50:05:a6"
FW_DEV_DMZ="eth-id-00:0c:29:50:05:9c"
```

Lassen Sie sich nicht von den ungewöhnlichen Bezeichnungen der Netzwerkkarten irritieren. SUSE verwendet statt `eth0` die Bezeichnung `eth-id-<MAC-Adresse>`.

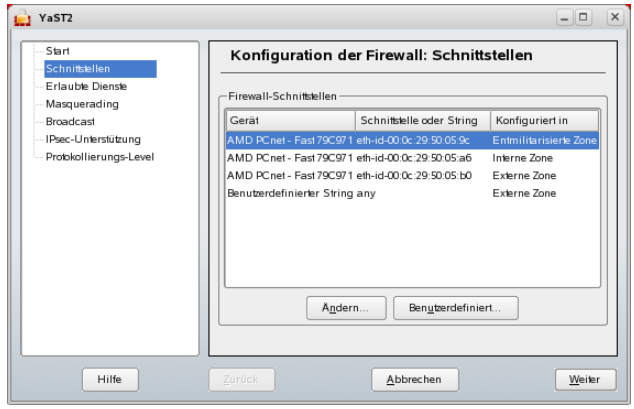


Abbildung 14.4: Weisen Sie jeder Netzwerkkarte die richtige Zone zu.

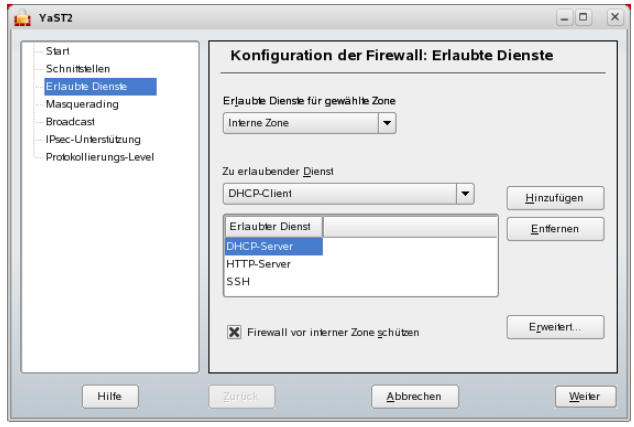


Abbildung 14.5: Um auf einen Dienst der Firewall zuzugreifen, müssen Sie diese freischalten.

Sie sollten jede Netzwerkkarte einer Zone zuordnen. Wenn Sie dies für eine Netzwerkkarte versäumen, darf diese keine Pakete versenden oder empfangen.

Nun müssen Sie im nächsten Dialog (Abbildung 14.5) die erlaubten Dienste definieren. Es handelt sich hierbei um Dienste auf der Firewall, auf die Sie aus den verschiedenen Zonen zugreifen. Es handelt sich nicht um einen Zugriff auf einen Dienst hinter der Firewall!

Wählen Sie nun jede Zone aus, und konfigurieren Sie die Dienste, auf die ein Zugriff erlaubt sein soll. Bei der internen Zone handelt es sich um einen Sonderfall. Da dies eine vertraute (Trusted) Zone ist, darf diese zunächst auf alle Dienste der Firewall zugreifen. Es ist jedoch sinnvoll, die Firewall auch vor der internen Zone zu schützen und nur bestimmte Dienste freizuschalten.

Auch diese Einstellungen können Sie in der Konfigurationsdatei wiederfinden oder direkt dort vornehmen. Dazu müssen Sie die folgenden Variablen editieren:

```
FW_PROTECT_FROM_INT="yes"
FW_SERVICES_EXT_TCP=""
FW_SERVICES_EXT_UDP="ipsec-nat-t isakmp"
FW_SERVICES_EXT_IP="esp"
FW_SERVICES_EXT_RPC=""
FW_SERVICES_DMZ_TCP=""
FW_SERVICES_DMZ_UDP=""
FW_SERVICES_DMZ_IP=""
FW_SERVICES_DMZ_RPC=""
FW_SERVICES_INT_TCP="http ssh"
FW_SERVICES_INT_UDP="bootps"
FW_SERVICES_INT_IP=""
FW_SERVICES_INT_RPC=""
```

Die hier aufgeführte Variable `FW_SERVICES_EXT_UDP="ipsec-nat-t isakmp"` wird an mehreren Stellen von YaST verändert. Die hier eingefügten Werte `"ipsec-nat-t isakmp"` werden von dem IPsec-Dialog gesetzt, wenn die IPsec-Unterstützung aktiv ist.

Der nächste Dialog beschreibt das `Masquerading` oder auch NAT. Zunächst aktivieren Sie hier grundsätzlich das Masquerading auf der externen Netzwerkkarte (Abbildung 14.6).

Die folgenden Variablen in der Konfigurationsdatei reflektieren Ihre Einstellungen:

```
FW_ROUTE="yes"
FW_MASQUERADE="yes"
FW_MASQ_DEV="$FW_DEV_EXT"
FW_MASQ_NETS="0/0"
```

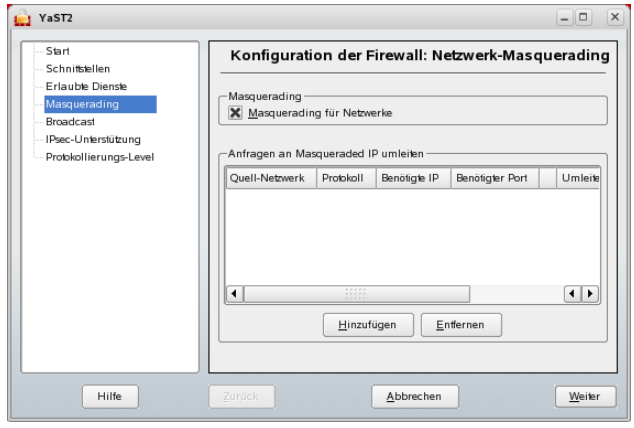


Abbildung 14.6: YaST erlaubt Ihnen sehr einfach, das Masquerading einzuschalten.

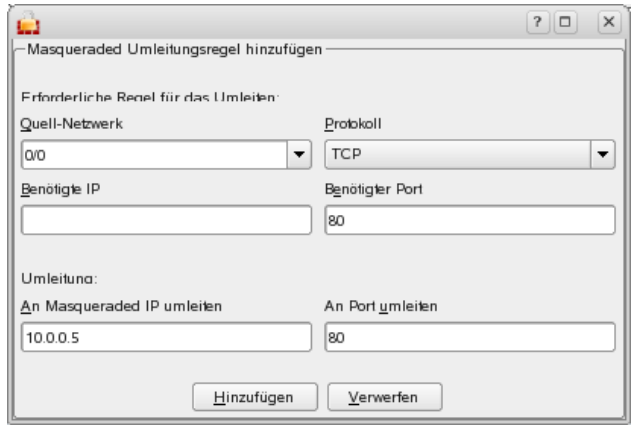


Abbildung 14.7: Auch ein Port- oder IP-Forwarding kann leicht eingerichtet werden.

Über denselben Dialog können Sie auch Weiterleitungen von Verbindungen nach innen definieren. Wählen Sie dazu in diesem Dialog lediglich `Hinzufügen`, und Sie erhalten einen neuen Dialog (Abbildung 14.7), in dem Sie die weiterzuleitende Verbindung eingeben.

Wenn Sie die Einstellung manuell vornehmen möchten, verwenden Sie die folgenden Variablen:

```
FW_FORWARD_MASQ="0/0,10.0.0.5,tcp,80"
```

Die Weiterleitung von Broadcast-IP-Paketen wird in dem nächsten Dialog (Abbildung 14.8) konfiguriert. Hier können Sie einstellen, welche IP-Broadcast-Pakete die Firewall erlaubt. Diese Broadcast-Pakete werden zum Beispiel von DHCP-Clients oder dem NETBIOS-Protokoll verwendet.

Diese Einstellungen können Sie auch manuell in den folgenden Variablen durchführen:

```
FW_ALLOW_FW_BROADCAST_EXT="no"
FW_ALLOW_FW_BROADCAST_INT="bootps"
FW_ALLOW_FW_BROADCAST_DMZ="no"
FW_IGNORE_FW_BROADCAST_EXT="no"
FW_IGNORE_FW_BROADCAST_INT="no"
FW_IGNORE_FW_BROADCAST_DMZ="no"
```

Wenn Sie bei einem der Dialoge eine Hilfe benötigen, können Sie jederzeit unten links in dem Dialog `Hilfe` anklicken. Sie kehren anschließend durch Anklicken von `Baum` zur Baumansicht zurück.

Die SUSEfirewall2 unterstützt auch die Filterung von IPsec-Verkehr. Sie können einfach durch Auswahl der IPsec-Option Ihre Firewall mit entsprechenden Regeln ausstatten, die den Zugriff per IPsec erlauben (Abbildung 14.9).

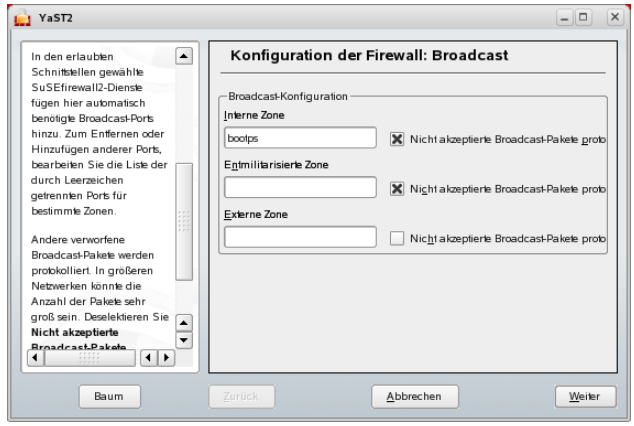


Abbildung 14.8: Normalerweise möchten Sie auf Ihrer Firewall sämtliche Broadcast-Pakete verwerfen. Ausnahme ist vielleicht ein DHCP-Server.

Abbildung 14.9: Die Aktivierung der IPsec-Unterstützung erfolgt nur durch das Setzen eines Hakens.

In der Konfigurationsdatei macht sich das durch die folgenden Variablen bemerkbar:

```
FW_SERVICES_EXT_UDP="ipsec-nat-t isakmp"
FW_SERVICES_EXT_IP="esp"
```

Als letzter Dialog wird von YaST der Protokollierungs-Level angeboten (Abbildung 14.10). Hier können Sie auswählen, welche Pakete eine Protokollierung erzeugen sollen. Um die Menge der Protokolle in einem erträglichen Rahmen zu halten, ist es sinnvoll, nur kritische Pakete zu protokollieren.

Die SUSEfirewall2 unterscheidet akzeptierte und verworfene kritische Pakete. Kritische verworfene Pakete sind gespoofte Pakete, TCP-Verbindungsanfragen und bestimmte ICMP-Pakete. Kritische akzeptierte Pakete sind TCP-Verbindungsaufbauten, RPC-Verbindungsanfragen und Zugriff auf hohe Ports. Die entsprechenden Variablen in der Konfigurationsdatei sind:

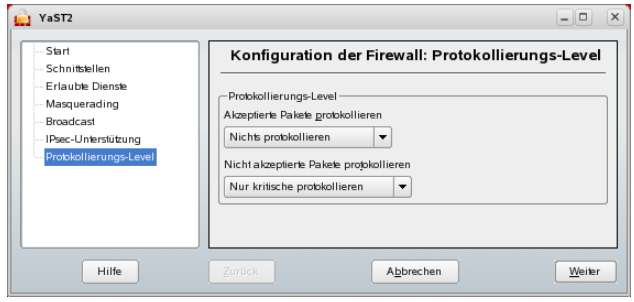


Abbildung 14.10: Wählen Sie nur kritische Pakete für die Protokollierung aus, sonst erkennen Sie anschließend den Wald vor lauter Bäumen nicht mehr.

```
FW_LOG_DROP_CRIT="yes"
FW_LOG_DROP_ALL="no"
FW_LOG_ACCEPT_CRIT="no"
FW_LOG_ACCEPT_ALL="no"
```

Weitere Einstellungen erlaubt Ihnen YaST nicht. Wenn Sie nun auf `Weiter` klicken, fasst YaST Ihre Firewall-Konfiguration noch einmal zusammen (Abbildung 14.11). Sie sollten hier noch einmal alle Einstellungen auf ihre Korrektheit kontrollieren. Durch Anwählen von `Übernehmen` werden diese Einstellungen jetzt in die Konfigurationsdatei geschrieben und wird die Firewall mit diesen Einstellungen neu gestartet (Abbildung 14.12).

Die SUSEfirewall2 bietet wesentlich mehr Funktionen, als YaST Ihnen zur Konfiguration anbietet. Viele Optionen, die YaST setzt, bietet es Ihnen gar nicht zur Auswahl an, sondern diese werden grundsätzlich vorausgesetzt. Natürlich können Sie aber auch auf YaST verzichten und die Datei manuell editieren. Insgesamt

Abbildung 14.11: YaST zeigt die Firewall-Konfiguration noch einmal in der Übersicht an.

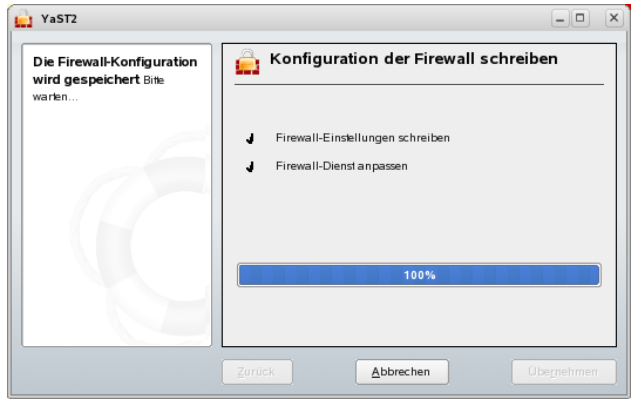


Abbildung 14.12: Nun wird die Konfiguration aktiviert. Hoffentlich haben Sie sämtliche Fehler korrigiert.

enthält die Datei bei SUSE Linux OSS 10.0 57 verschiedene Variablen, deren Namen relativ selbsterklärend sind und die durch zusätzliche Kommentare in der Datei erläutert werden. Hilfreich bei der manuellen Anpassung ist auch die erwähnte SUSEfirewall2-Dokumentation. Natürlich können Sie auch die SUSEfirewall2 abschalten. Eine Deinstallation ist nicht möglich. Aber setzen Sie einfach den Start-Modus auf manuell. Dann wird das System die Firewall nicht mehr starten, und Sie können eine alternative Oberfläche, z.B. Shorewall, verwenden.

Zum Abschluss finden Sie hier alle Variablen der SUSEfirewall2 als Referenz:

```
FW_DEV_EXT="any eth-id-00:0c:29:50:05:b0"
FW_DEV_INT="eth-id-00:0c:29:50:05:a6"
FW_DEV_DMZ="eth-id-00:0c:29:50:05:9c"
FW_ROUTE="yes"
FW_MASQUERADE="yes"
FW_MASQ_DEV="$FW_DEV_EXT"
FW_MASQ_NETS="0/0"
FW_PROTECT_FROM_INT="yes"
FW_SERVICES_EXT_TCP=""
FW_SERVICES_EXT_UDP="ipsec-nat-t isakmp"
FW_SERVICES_EXT_IP="esp"
FW_SERVICES_EXT_RPC=""
FW_SERVICES_DMZ_TCP=""
FW_SERVICES_DMZ_UDP=""
FW_SERVICES_DMZ_IP=""
FW_SERVICES_DMZ_RPC=""
FW_SERVICES_INT_TCP="http ssh"
FW_SERVICES_INT_UDP="bootps"
FW_SERVICES_INT_IP=""
```

```
FW_SERVICES_INT_RPC=""
FW_SERVICES_DROP_EXT=""
FW_SERVICES_REJECT_EXT="0/0,tcp,113"
FW_SERVICES_ACCEPT_EXT=""
FW_TRUSTED_NETS=""
FW_ALLOW_INCOMING_HIGHPORTS_TCP=""
FW_ALLOW_INCOMING_HIGHPORTS_UDP=""
FW_FORWARD=""
FW_FORWARD_MASQ="0/0,10.0.0.5,tcp,80"
FW_REDIRECT=""
FW_LOG_DROP_CRIT="yes"
FW_LOG_DROP_ALL="no"
FW_LOG_ACCEPT_CRIT="no"
FW_LOG_ACCEPT_ALL="no"
FW_LOG_LIMIT=""
FW_LOG=""
FW_KERNEL_SECURITY="yes"
FW_STOP_KEEP_ROUTING_STATE="no"
FW_ALLOW_PING_FW="yes"
FW_ALLOW_PING_DMZ="no"
FW_ALLOW_PING_EXT="no"
FW_ALLOW_FW_SOURCEQUENCH=""
FW_ALLOW_FW_BROADCAST_EXT="no"
FW_ALLOW_FW_BROADCAST_INT="bootps"
FW_ALLOW_FW_BROADCAST_DMZ="no"
FW_IGNORE_FW_BROADCAST_EXT="no"
FW_IGNORE_FW_BROADCAST_INT="no"
FW_IGNORE_FW_BROADCAST_DMZ="no"
FW_ALLOW_CLASS_ROUTING=""
FW_CUSTOMRULES=""
FW_REJECT=""
FW_HTB_TUNE_DEV=""
FW_IPv6=""
FW_IPv6_REJECT_OUTGOING=""
FW_IPSEC_TRUST="no"
FW_ZONES=""
FW_USE_IPTABLES_BATCH=""
FW_LOAD_MODULES=""
```

14.3 Debian

Die Debian-Distribution stellt sicherlich eine Ausnahme dar. Es gibt kein von der Distribution entwickeltes Firewall-Konfigurationswerkzeug, das diese Distribution auszeichnet, jedoch enthält die Distribution eine Vielzahl dieser Werkzeuge von an-

deren Autoren. So finden Sie Shorewall, Firewall Builder und Firestarter in der Distribution. Teilweise befinden sich die Pakete in dem Testing- oder Unstable Branch.

14.4 IPCop

IPCop ist eine reine GPL-Firewall-Distribution (*http://www.ipcop.org*). Die aktuelle Version ist die Version 1.4.8. Sie können diese Distribution als 43-MByte-ISO-Image von der Homepage herunterladen, auf eine CD brennen und anschließend zur Installation nutzen. Für die Installation von IPCop benötigen Sie einen beliebigen Intel-Rechner mit mindestens einem Intel 386-Prozessor, 32 MByte RAM und 300 MByte Festplatte. In den meisten Fällen werden Sie sicherlich mehr zur Verfügung haben. Ein Diskettenlaufwerk und ein CD-ROM-Laufwerk sind nicht erforderlich, aber nützlich. Nach der Installation benötigen Sie auch keinen Monitor und keine Tastatur mehr.

14.4.1 Das IPCop-Konzept

Die IPCop-Firewall dient, wie jede andere Firewall auch, als Wächter zwischen mehreren Netzwerken. Um diese Funktion leicht verständlich zu visualisieren, benennt IPCop die verschiedenen Netzwerkkarten der Firewall mit unterschiedlichen Farben:

- **Rot**: Die rote Netzwerkkarte verbindet die IPCop-Firewall mit dem Internet oder einem ähnlich unsicheren Netz.
- **Grün**: An der grünen Netzwerkkarte wird das von der Firewall geschützte Netz angeschlossen.
- **Blau**: Das blaue Netz ist für drahtlose Netze reserviert. Der Zugriff von dem blauen Netz auf das grüne Netz wird streng kontrolliert. Die Verwendung der blauen Netzwerkkarte ist optional.
- **Orange**: Das orange Netz ist die DMZ. Der Zugriff aus diesem Netz in das blaue oder grüne Netz wird streng kontrolliert.

Diese Farben sind bei der Konfiguration und der späteren Administration der IPCop-Firewall sehr wichtig. Die Farben vereinfachen aber auch die Konfiguration und die Kommunikation.

Sie sollten sich bereits vor der Installation der IPCop-Firewall Gedanken über die in dem grünen Netz verwendeten IP-Adressen und speziell über die IP-Adresse der grünen Netzwerkkarte der IPCop-Firewall machen.

Die IPCop-Firewall unterstützt noch folgende bemerkenswerte Eigenschaften:

- Eingebauter Update-Mechanismus mit Protokoll der installierten Updates. Nur signierte Updates werden von IPCop entgegengenommen.
- Grafische Status-Seiten mit Anzeige des Netzwerkdurchsatzes und der Prozessorauslastung

- Zusätzliche Netzwerkdienste: Proxy, DHCP-Server und NTP-Zeitserver
- Bandbreitenkontrolle. Die Bandbreitenkontrolle kann sehr einfach konfiguriert werden, ohne dass man die Einzelheiten des TCP-Protokolls kennen muss.
- Intrusion Detection mit Snort
- Grafische Administration der Firewall. Jedoch können Sie leider nicht den Zugriff von innen auf das Internet einschränken. Sie haben mit diesem Interface lediglich die Möglichkeit, den Zugriff von außen nach innen zu erlauben.
- Komplette VPN-Unterstützung für IPsec-Verbindungen mit Preshared-Keys und Zertifikaten
- Ausführliche Protokolle

Wenn Sie eine einfache Lösung für die Verwaltung einer Firewall suchen, die auch von Nicht-Linux-Administratoren verwaltet werden kann, ist IPCop durchaus ein vielversprechender Kandidat.

14.4.2 IPCop-Installation

Die Installation von IPCop ist recht einfach, wenn Sie bereits andere Linux-Distributionen installiert haben. Besonders, wenn Sie schon Debian oder Red Hat Linux text-basiert installiert haben, werden die Fragen bei der Installation Sie vor keine größeren Probleme stellen.

Achtung

Eine Dual-Boot-Installation ist bei IPCop nicht möglich. IPCop verwendet die gesamte Festplatte! Der erste Bildschirm nach dem Boot von der CD-ROM weist Sie darauf hin.

Wenn Sie IPCop testweise in VMware installieren möchten, wählen Sie bitte eine virtuelle IDE-Festplatte in VMWare aus. Die virtuelle SCSI-Festplatte wird teilweise nicht erkannt.

Nun können Sie zunächst die Sprache auswählen. IPCop unterstützt auch die deutsche Sprache. Nach einigen weiteren Bildschirmen werden die Pakete installiert, und Sie werden gefragt, ob Sie eine Diskette mit dem Backup einer alten IPCop-Installation besitzen. Diese können Sie hier wieder einspielen (Abbildung 14.13).

Auf dem nächsten Bildschirm werden Sie aufgefordert, das Netzwerk zu konfigurieren. IPCop unterscheidet das grüne, das blaue, das orange und das rote Netzwerk. Hier müssen Sie die grüne Netzwerkkarte konfigurieren (Abbildung 14.14). Wählen Sie die `Automatische Erkennung`. Anschließend müssen Sie die IP-Adresse für die grüne Netzwerkkarte eingeben. Wenn Ihr grünes Netzwerk die IP-Adressen 192.168.15.0/24 verwendet, werden Sie der IPCop-Firewall wahrscheinlich entweder die IP-Adresse 192.168.15.1 oder 192.168.15.254 zuweisen.

Abbildung 14.13: IPCop unterstützt auch die Wiederherstellung mit einer Backup-Diskette.

Abbildung 14.14: Achten Sie bei der Wahl der grünen Netzwerkkarte darauf, dass Sie die richtige auswählen.

Sobald Sie die IP-Adresse für die grüne Netzwerkkarte bestätigt haben, wird der Boot-Manager Grub installiert, und die Installation ist abgeschlossen. Entfernen Sie nun alle Disketten und CD-ROMs aus den Laufwerken, und bestätigen Sie mit `Ok`.

IPCop wird nun das Setup-Programm für die weitere Konfiguration aufrufen. Als Tastatur-Layout wählen Sie für eine deutsche Tastatur bitte `de-latin1-nodeadkeys`. Die Zeitzone für Deutschland ist `Europe/Berlin`. Als Rechnernamen können Sie die Voreinstellung `ipcop` beibehalten oder auch einen eigenen Namen nach Ihren Wünschen wählen. Anschließend wählen Sie einen geeigneten Domänen-Namen. Wenn Sie sich mit einer ISDN-Karte einwählen, müssen Sie das Protokoll (DSS1), die ISDN-Karte und mögliche zusätzliche Modulparameter für den Treiber und Ihre lokale Telefonnummer eingeben. Anschließend aktivieren Sie das ISDN. Wenn Sie keine ISDN-Karte verwenden, können Sie einfach den Bildschirm mit `ISDN Deaktivieren` bestätigen.

Wenn Sie keine ISDN-Karte verwenden oder zusätzlich eine DMZ oder ein drahtloses Netz verwenden möchten, müssen Sie auf dem nächsten Bildschirm die Netzwerkkonfiguration ändern. Ist Ihre IPCop-Firewall zum Beispiel mit einer Netzwerkkarte über DSL mit dem Internet verbunden, wählen Sie GREEN + RED. Verfügen Sie zusätzlich über eine DMZ, wählen Sie GREEN + ORANGE + RED und so weiter (Abbildung 14.15).

Anschließend müssen Sie den verschiedenen Farben Netzwerkkarten und IP-Adressen zuweisen. Die grüne Netzwerkkarte besitzt bereits eine IP-Adresse. Die orange und die blaue Netzwerkkarte erhält jeweils statische IP-Adressen. Bei der roten Netzwerkkarte können Sie zwischen einer statischen und einer dynamischen IP-Adresse wählen (Abbildung 14.16).

Wenn Sie für die rote Netzwerkkarte eine statische IP-Adresse ausgewählt haben, können Sie auch noch zwei DNS-Server und das Gateway angeben.

Abbildung 14.15: IPCop weist den Firewall-Zonen Farben zu. Wählen Sie die für Sie richtige Farbkombination aus.

Abbildung 14.16: IPCop unterstützt die Internetanbindung mit PPTP, PPPOE, DHCP und statischer IP-Adresse.

Achtung

Die angegebenen DNS-Server und das Gateway haben Vorrang vor den Angaben, die Ihr Provider Ihnen bei z.B. PPPOE mitteilt. Stellen Sie sicher, dass Sie bei einer dynamischen IP-Adresse hier keine Daten eingeben!

Nun sind Sie fast fertig. Auf dem nächsten Bildschirm gibt Ihnen IPCop die Möglichkeit, einen DHCP-Server auf der IPCop-Firewall für Ihre Clients im grünen Netz zu betreiben. Wenn Sie diese Funktion wünschen, aktivieren Sie den DHCP-Server und geben einen sinnvollen DHCP-Bereich vor (Abbildung 14.17).

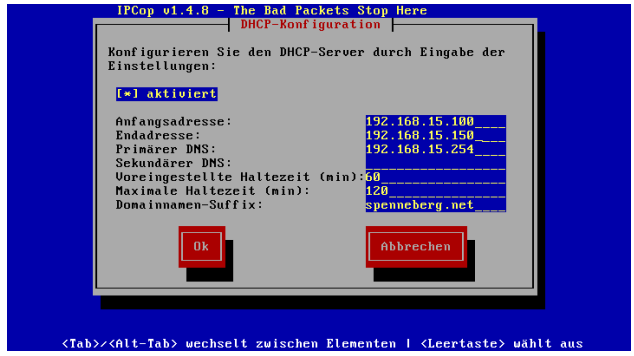


Abbildung 14.17: IPCop kann selbst als DHCP-Server für das grüne Netz arbeiten.

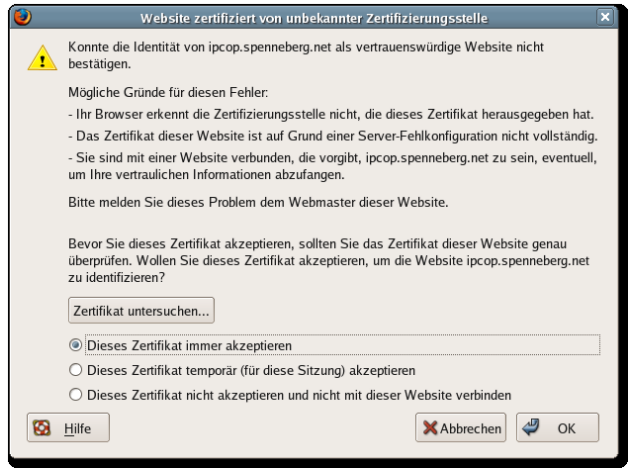


Abbildung 14.18: Bei der ersten Verbindung müssen Sie das Zertifikat akzeptieren.

Abbildung 14.19: Ein Aufruf der Konfigurationswerkzeuge ist auf der Konsole mit dem Befehl setup möglich.

Nun müssen Sie nur noch das Kennwort für den Benutzer root und für den IPCop-Administrator eingeben, und die Installation ist abgeschlossen.

Nach einem Reboot können Sie sich mit dem Web-Interface verbinden.

Tipp

Wenn Sie zu einem späteren Zeitpunkt feststellen, dass Sie die Konfiguration der letzten Schritte ändern müssen, dann können Sie das nicht über das Web-Interface erledigen. Sie müssen sich auf dem IPCop-System lokal anmelden und können dort das Kommando `setup` aufrufen. Dieses Kommando präsentiert Ihnen ein Menü (Abbildung 14.19), in dem Sie die Werkzeuge auswählen können, die Sie für die Änderung benötigen.

14.4.3 IPCop-Web-Interface

Das Web-Interface von IPCop ist über die IP-Adresse der grünen Netzwerkkarte erreichbar. Geben Sie einfach eine der beiden folgenden URLs in Ihrem Browser ein:

- *http://192.168.15.254:81/* oder
- *https://192.168.15.254:445/*

Ab der Version 1.4.0 ist die Verbindung nur noch verschlüsselt erlaubt. Daher werden Sie bei der Eingabe der ersten URL automatisch auf die zweite URL umgeleitet. Achten Sie bei den URLs auf die ungewöhnlichen Port-Nummern. Wenn Sie in Ihrer `/etc/hosts`-Datei den folgenden Eintrag vornehmen, können Sie auch anstelle der IP-Adresse den Rechnernamen `ipcop` verwenden:

```
192.168.15.254   ipcop.spenneberg.net ipcop
```

Bei der ersten Verbindung mit IPCop wird sich Ihr Browser über das Zertifikat des IPCop-Webservers beschweren. Die Meldung wird ähnlich aussehen wie in Abbildung 14.18. Wenn Sie sicher sind, dass sich in diesem Moment kein Bösewicht in Ihre Verbindung eingeklinkt hat, sollten Sie das Zertifikat dauerhaft akzeptieren. Bei dem Internet Explorer müssen Sie `View Certificate` und dann `Install Certificate` anwählen. Bei dem Firefox genügt es, wie in der Abbildung 14.18 den Punkt `Dieses Zertifikat immer akzeptieren` auszuwählen.

Falls Sie sich nicht sicher sind, dass das Zertifikat tatsächlich von Ihrer IPCop-Installation stammt, können Sie das überprüfen, wenn Sie sich auf Ihrem IPCop-System anmelden können. Geben Sie auf der Kommandozeile folgenden Befehl ein:

```
# openssl x509 -noout -fingerprint -in /etc/httpd/server.crt
MD5 Fingerprint=7D:94:26:27:D1:A3:59:59:A4:64:33:43:D7:FD:7E:59
```

Vergleichen Sie diesen Fingerprint mit dem von dem Browser angezeigten Fingerprint (bei Firefox wählen Sie `Zertifikat untersuchen`; Abbildung 14.20).

Wenn Sie sich über die IP-Adresse mit Ihrer IPCop-Installation verbinden, wird Ihnen anschließend noch eine zweite Warnung (Abbildung 14.21) angezeigt. Die

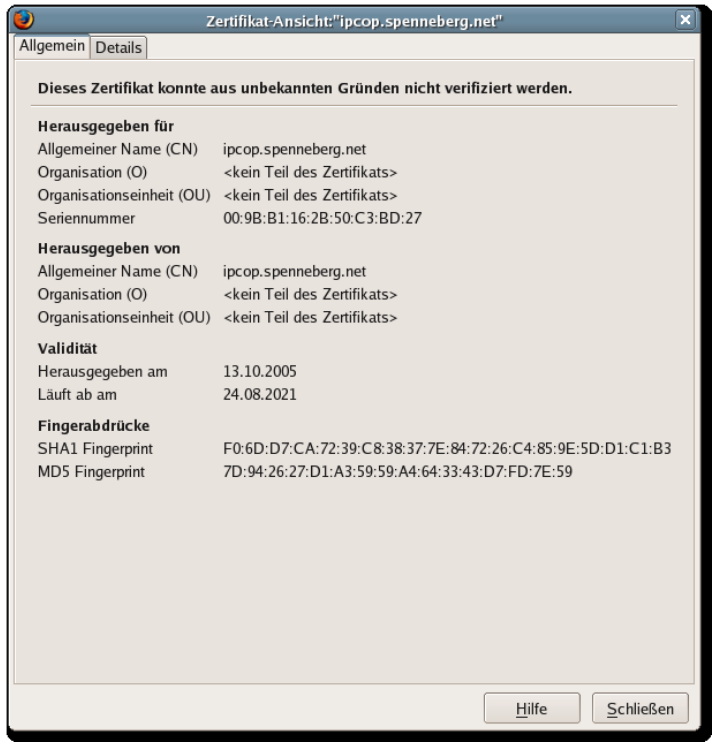


Abbildung 14.20: Überprüfen Sie im Zweifelsfall die Fingerabdrücke des Zertifikats.

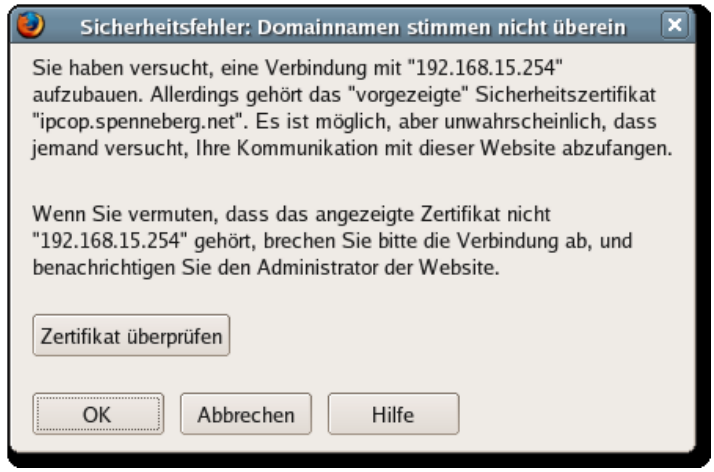


Abbildung 14.21: Firefox beschwert sich, da das Zertifikat für ipcop.spenneberg.net ausgestellt ist, die Verbindung jedoch mit 192.168.15.254 aufgebaut wird.

können Sie ignorieren. Um in Zukunft diese Warnung nicht mehr angezeigt zu bekommen, sollten Sie Ihre Datei `/etc/hosts` entsprechend anpassen. Diese Datei existiert auch auf einem Windows-System in `system32/drivers/etc/` und wird auch dort benutzt.

Nun sind Sie mit dem Web-Interface verbunden und können die IPCop-Firewall administrieren. Hoffentlich haben Sie bei der Konfiguration alles richtig gemacht. Wenn die IPCop-Firewall bereits an dem Internet angeschlossen ist, begrüßt Sie die Firewall mit der Meldung, dass die Firewall verbunden sei und ob Updates verfügbar sind. Wenn dies der Fall ist, sollten Sie zunächst diese Updates installieren. Wechseln Sie hierzu auf die Seite *Updates* in der Registerkarte *System*. Dazu werden Sie aufgefordert, sich als Benutzer *admin* anzumelden und Ihr Kennwort einzugeben. Das Update wird Ihnen dann beschrieben, und Sie finden dort einen Download-Link (*Info*), mit dem Sie zunächst das Update herunterladen und dann auf die IPCop-Firewall hochladen können (Abbildung 14.22).

Die Updates sind zum Schutz vor Trojanern mit GnuPG signiert. Nur korrekt signierte Updates werden von Ihrer IPCop-Firewall akzeptiert. Damit sind Sie sicher, dass nicht ein Angreifer Ihnen ein fehlerhaftes Update unterschiebt.

Auf der Registerkarte `Status` finden Sie die folgenden Informationen:

- `System-Status`. Hier finden Sie Informationen über die laufenden Dienste, den freien Speicherplatz und die Prozesse.
- `Netzwerk-Status`. Diese Seite zeigt Ihnen an, wie Ihre Netzwerkkarten, Routen und Internetverbindung konfiguriert sind.
- `System-Diagramme`. Hier finden Sie grafische Darstellungen der CPU-, Speicher- und Swap-Nutzung Ihrer Firewall.

Abbildung 14.22: IPCop hat einen eingebauten Update-Mechanismus. So sind Sie vor bekannten Sicherheitslücken geschützt.

- `Netzwerk-Diagramme`. Diese Seite zeigt die Auslastung der Netzwerkdiagramme grafisch an.
- `Verbindungen`. Hier werden Ihnen die aktuellen Netzwerkverbindungen angezeigt. Im Grunde handelt es sich um eine Darstellung der Datei `/proc/net/ip_conntrack`.

Auf der Registerkarte `Netzwerk` können Sie besondere Einstellungen für spezielle Modems und DSL-Geräte vornehmen. Einige dieser Geräte benötigen eine spezielle Firmware für ihre Funktion, die von IPCop in dem Gerät installiert werden muss. Hier konfigurieren Sie diese Funktionen.

Die Registerkarte `Dienste` erlaubt Ihnen die Konfiguration eines Proxys, eines DHCP-Servers, eines dynamischen DNS-Clients, die Bearbeitung der lokalen Hosts-Datei, den Einsatz eines NTP-Zeitservers, die Konfiguration der Bandbreitenregelung und die Aktivierung des Snort-Intrusion-Detection-Systems. Dabei unterstützt IPCop sogar bereits die neuen VRT-Regelsätze von Snort und erlaubt Ihnen die Eingabe des Lizenzschlüssels (Abbildung 14.23).

Auf der Registerkarte `Firewall` können Sie lediglich Verbindungen von außen nach innen konfigurieren. Normalerweise sind diese Verbindungen nicht erlaubt. Sie können aber von außen Port-Weiterleitungen nach innen konfigurieren. Sie kön-

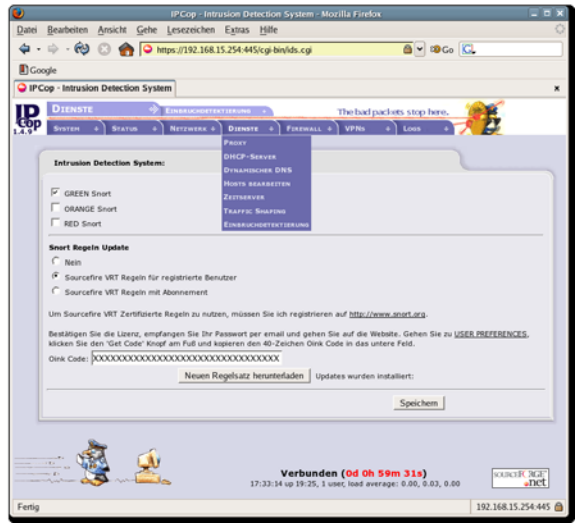


Abbildung 14.23: IPCop unterstützt bereits die VRT-Snort-Regelsätze.

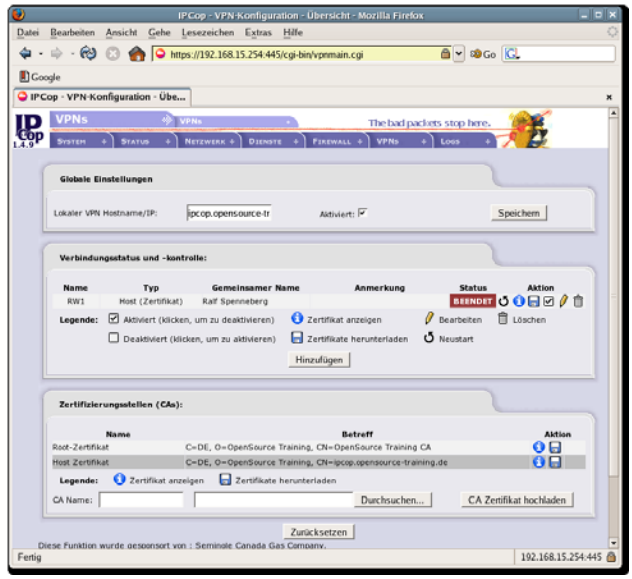


Abbildung 14.24: IPCop übernimmt die komplette Verwaltung der VPNs.

nen den externen Zugang zur IPCop-Administrationsoberfläche von außen freigeben und DMZ-Schlupflöcher (aus der DMZ in das grüne Netz) konfigurieren. Die Verbindungen aus dem grünen und dem blauen Netz in das Internet sind immer erlaubt und können nicht eingeschränkt werden!

Auf der Registerkarte VPN können Sie sehr einfach ein VPN konfigurieren. Hierzu können Sie zunächst eine Zertifikatsautorität erzeugen oder die Zertifikate einer externen CA hochladen. Anschließend erzeugen Sie Verbindungen und können den Status der Verbindung beobachten (Abbildung 14.24).

Bevor ich das Buch mit Screenshots zu sehr aufblähe, beende ich hier die Beschreibung von IPCop, da es auf der IPCop-Homepage auch eine sehr gute 60 Seiten starke Administrationsanleitung gibt. Ich denke, Sie haben die wesentlichen Möglichkeiten von IPCop kennen gelernt und finden sich auf dem Web-Interface von IPCop auch selbst recht schnell zurecht.

14.5 Smoothwall

Die Smoothwall (*http://www.smoothwall.org*) ist eine direkte Alternative zu IPCop. Die aktuelle Version, Smoothwall Express 3.0, wird wie IPCop unter der GPL-Lizenz als ISO-Image vertrieben und ist etwa 46 MByte groß. Die Dokumentation bei Smoothwall ist genauso ausführlich wie bei IPCop. Es gibt ebenfalls einen Quickstart-Guide, einen Installations-Guide und einen Administrations-Guide. Alle Handbücher sind im PDF-Format verfügbar und können von der Homepage heruntergeladen werden.

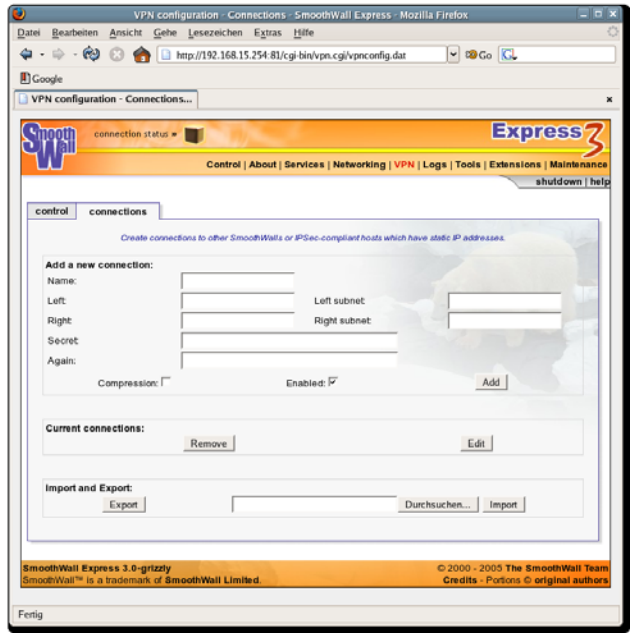


Abbildung 14.25: Das Web-Interface kann auch VPN-Verbindungen konfigurieren.

14.5.1 Smoothwall-Installation

Die Installation von Smoothwall ist ähnlich unproblematisch wie bei IPCop. Genauso wie IPCop beansprucht Smoothwall die gesamte Festplatte. Eine Dual-Boot-Installation ist nicht möglich. Ansonsten erfolgt die Installation mit ein oder zwei Ausnahmen identisch zu der IPCop-Installation. Dies ist nicht verwunderlich, da die IPCop-Firewall auf der Basis der GPL-Version von Smoothwall entwickelt wurde.

14.5.2 Smoothwall-Web-Interface

Obwohl das Web-Interface ein wenig anders gestaltet ist als bei IPCop, bietet es mehr oder weniger die gleichen Funktionen (Abbildung 14.25).

Ich nehme hier von einer genauen Beschreibung der Oberfläche Abstand und möchte nur auf einige Unterschiede zu IPCop hinweisen. Smoothwall Express 3.0 unterstützt wie IPCop einen Proxy, einen Dynamic-DNS-Client, Snort als IDS, einen DHCP- und einen NTP-Server. Jedoch kann Smoothwall im Gegensatz zu IPCop für Snort nicht automatisch neue Regelsätze von der Snort-Homepage laden. Die VPN-Funktionalität ist auch nicht so ausgereift wie bei IPCop. Smoothwall unterstützt hier keine Zertifikate zur Authentifizierung in dem VPN. Ansonsten sind Smoothwall und IPCop gleichermaßen für den Einsatz als Firewall-Distribution geeignet.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

15 Testmethoden und -werkzeuge

Wer eine Firewall aufsetzt, sollte diese auch testen. Syntaktische Fehler in Ihrem Firewall-Skript erkennen Sie direkt beim Aufruf. Logische Fehler sind wesentlich schwerer zu erkennen. Nur der Test zeigt Ihnen, ob Sie einen logischen Fehler in Ihrem Regelwerk übersehen haben.

Die Werkzeuge, die ich in diesem Kapitel vorstelle, eignen sich auch zum Test und Audit fremder Firewall-Systeme und Sicherheitsstrukturen. Daher gehe ich auch ein wenig ausführlicher auf Funktionen ein, die hier sinnvoll sind.

Achtung

Denken Sie jedoch bitte daran, dass niemand gern gescannt wird. Sie sollten sich vorher immer die schriftliche Erlaubnis einholen oder von der betroffenen Person dazu aufgefordert worden sein. Die Anwendung von Nessus kann im Gegensatz zu der von Nmap meiner Einschätzung nach sogar strafrechtliche Konsequenzen nach sich ziehen.

15.1 Test der Regeln

Sobald Sie Ihr Firewall-Skript fertig gestellt haben, sollten Sie es auf syntaktische Fehler testen. Die beste Möglichkeit hierzu ist der Aufruf des Shell-Skripts. Die Shell wird Syntaxfehler auf der Konsole melden. Leider schleichen sich auch immer logische Fehler in einem Firewall-Skript ein. Obwohl Sie glauben, alle Regeln richtig definiert zu haben, entspricht das Ergebnis nicht Ihren Vorstellungen. Dann müssen Sie nach dem Fehler suchen und diesen beheben.

Am einfachsten beginnen Sie mit den Diensten, deren Nutzung das Firewall-Skript erlauben soll. Prüfen Sie, ob die gewünschten Funktionen zur Verfügung stehen. Falls dies nicht der Fall ist, analysieren Sie den Netzwerkverkehr und vergleichen Sie diesen mit Ihren Regeln. Für die Analyse des Netzwerkverkehrs eignen sich unter Linux die Befehle `tcpdump` und `ethereal`. Tcpdump ist ein einfacher Kommandozeilenbefehl, der die Netzwerkpakete anzeigen kann. Dabei kann Tcpdump auch die Pakete sehen, die später von den Regeln verworfen werden. Die Ausgabe von Tcpdump ist in Abbildung 15.1 zu sehen.

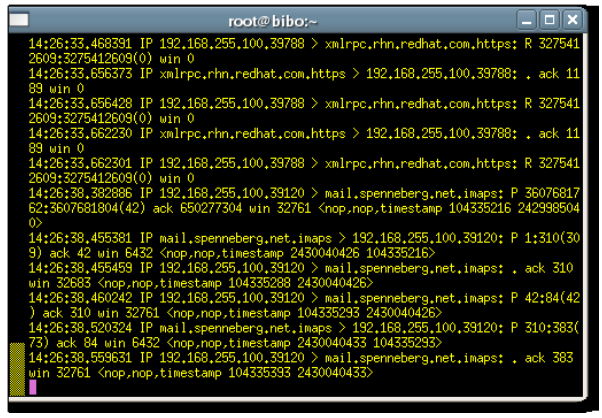


Abbildung 15.1: Tcpdump zeigt die Netzwerkpakete auf der Konsole an.

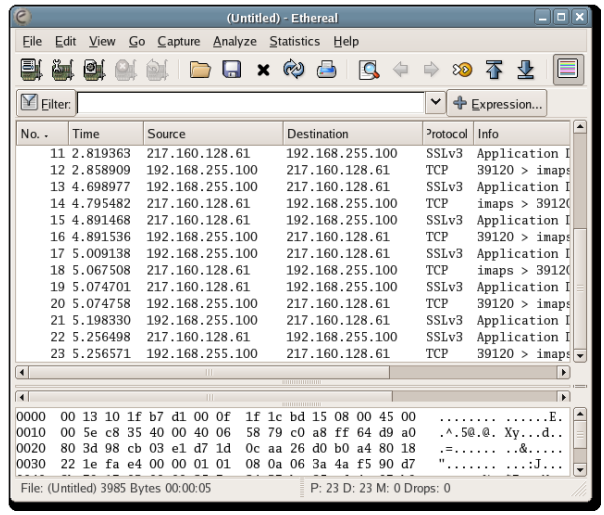


Abbildung 15.2: Ethereal browst die Netzwerkpakete grafisch.

Ethereal ist ein grafisches Werkzeug, das im Gegensatz zum spartanischen Tcpdump, die Daten ausführlicher aufbereitet (siehe Abbildung 15.2).

Falls Sie so immer noch nicht erkennen können, warum Ihr Firewall-Skript den speziellen Dienst unterbindet, fügen Sie zusätzliche Log-Regeln ein. Sorgen Sie dafür, dass in jeder Filter-Kette, bevor die Pakete verworfen werden, alle Pakete protokolliert werden.

Im Folgenden möchte ich Ihnen anhand eines Beispiels die Vorgehensweise zeigen. Schauen Sie sich das folgende Skript an, das von unserem hypothetischen Firewall-Administrator geschrieben wurde. Die Anforderung an die Firewall war:

- Erlaube keinen Zugriff von außen in das geschützte Netz.
- Erlaube aus dem geschützten Netz den HTTP- und HTTPS-Zugriff auf beliebige Webserver.

Der Firewall-Administrator erzeugte aus dieser Anforderung das folgende Skript:

```
#!/bin/sh

# Firewall-Skript
# Lehnt jeden Zugriff von außen ab
# Erlaubt HTTP und HTTPS

# Netzwerkkarten
INTDEV=eth0
EXTDEV=eth1

IPTABLES=/sbin/iptables

SERVICE="80,443"

$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP

$IPTABLES -A FORWARD -p tcp -i $INDEV -o $EXTDEV -m multiport \
  --dport $SERVICE -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Dieses Skript hat drei Schönheitsfehler, die wir nun suchen wollen. Zunächst startet der Administrator dieses Skript. Bei dem Start bekommt er direkt eine Fehlermeldung angezeigt:

```
# sh fw_skript
Warning: wierd character in interface ‘-o’ (No aliases, :, ! or *).
Bad argument ‘eth1’
Try ‘iptables -h’ or ’iptables --help’ for more information.
```

Leider zeigt die Fehlermeldung nicht, wo in dem Skript der Fehler aufgetreten ist. Bei diesem kurzen Skript ist es sicherlich leicht für Sie, den Fehler zu finden. Bei einem Skript von 200 oder 300 Regeln ist es ungemein schwerer, die Zeile mit dem Fehler zu entdecken.

Die Bash-Shell bietet hierfür die Option `-x`. Dann zeigt die Shell jede Zeile inklusive der ersetzten Variablen vor der Ausführung:

```
# sh -x fw_skript
+ INTDEV=eth0
```

```
+ EXTDEV=eth1
+ IPTABLES=/sbin/iptables
+ SERVICE=80,443
+ /sbin/iptables -P INPUT DROP
+ /sbin/iptables -P OUTPUT DROP
+ /sbin/iptables -P FORWARD DROP
+ /sbin/iptables -A FORWARD -p tcp -i -o eth1 -m multiport --dport 80,443 -m state
  --state NEW -j ACCEPT
Warning: wierd character in interface '-o' (No aliases, :, ! or *).
Bad argument 'eth1'
Try 'iptables -h' or 'iptables --help' for more information.
+ /sbin/iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Nun fällt auf, dass in der fett hervorgehobenen Zeile die Angabe der Netzwerkkarte für die Option `-i` fehlt. Scheinbar wurde die Variable nicht initialisiert, oder es gibt einen Tippfehler. Sie werden den Tippfehler sicherlich schon gefunden haben. Die Variable wurde mit dem Namen `INTDEV` initialisiert, und in dieser Zeile wurde die nicht definierte Variable `INDEV` verwendet. Nach der Korrektur läuft das Skript fehlerfrei. Allerdings stellt der Administrator bei mehrmaligen Aufrufen des Skripts fest, dass die neuen Regeln immer an die Ketten angehängt werden. Die Ketten werden nie gelöscht. Er fügt zusätzlich zu Beginn eine Zeile ein, die die Ketten zunächst löscht.

```
$IPTABLES -F
```

Dennoch ist es nicht möglich, die Firewall wie gewünscht zu nutzen. Zur Fehlersuche zeigt der Administrator nach dem Versuch, auf die Seite *http://www.spenneberg.com* zuzugreifen, die Regeln an:

```
# iptables -vnL FORWARD
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
                                                                   state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  eth1   eth0    0.0.0.0/0            0.0.0.0/0
                                                                 multiport dports 80,443 state NEW
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
                                                                   state RELATED,ESTABLISHED
```

Erstaunlicherweise haben alle Zähler der Regeln den Wert 0. Der Administrator startet nun auf der Firewall `tcpdump` auf der internen Netzwerkkarte, um den Verkehr zu beobachten:

```
# tcpdump -ni eth1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vmnet2, link-type EN10MB (Ethernet), capture size 96 bytes
```

```
10:53:43.766500 IP 10.0.1.128.32769 > 128.176.0.12.domain:  35667+ A? www.spenneberg.com.
                                                                                (36)
10:53:48.270266 arp who-has 10.0.1.1 tell 10.0.1.128
10:53:48.270286 arp reply 10.0.1.1 is-at 00:50:56:c0:00:02
10:53:48.270823 IP 10.0.1.128.32769 > 128.176.0.12.domain:  35667+ A? www.spenneberg.com.
                                                                                (36)
```

Eigentlich sollte diese Information dem Administrator für die Fehlersuche bereits ausreichen. Der Client versucht, einen Nameserver zu erreichen, um den Namen `www.spenneberg.com` aufzulösen, und erhält keine Antwort. Anscheinend erlaubt der Regelsatz keinen DNS-Verkehr.

Der Administrator möchte es aber genau wissen und fügt manuell eine LOG-Regel an die Kette an:

```
# iptables -A FORWARD -j LOG --log-prefix "FORWARD: "
# iptables -vnL FORWARD
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  vmnet2 eth0    0.0.0.0/0            0.0.0.0/0
                                                                multiport dports 80,443 state NEW
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
                                                                   state RELATED,ESTABLISHED
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0

                                                    LOG flags 0 level 4 prefix 'FORWARD: '
```

Nun versucht er erneut, auf die Webseite zuzugreifen, und beobachtet die Protokolle. Dort findet er folgende Einträge:

```
Jul 23 11:00:24 bibo kernel: FORWARD: IN=eth1 OUT=eth0 SRC=10.0.1.128 DST=128.176.0.12
  LEN=64 TOS=0x00 PREC=0x00 TTL=63 ID=0 DF PROTO=UDP SPT=32769 DPT=53 LEN=44
Jul 23 11:00:29 bibo kernel: FORWARD: IN=eth1 OUT=eth0 SRC=10.0.1.128 DST=128.176.0.12
  LEN=64 TOS=0x00 PREC=0x00 TTL=63 ID=1 DF PROTO=UDP SPT=32769 DPT=53 LEN=44
```

Diese Meldungen zeigen ihm nun eindeutig, dass die DNS-Anfragen an den UDP-Port 53 nicht von der Firewall erlaubt werden. Nach der Kontrolle seines Skripts stellt er fest, dass er folgende Regel vergessen hat:

```
$IPTABLES -A FORWARD -p udp -i $INTDEV -o $EXTDEV --dport 53 \
  -m state --state NEW -j ACCEPT
```

Er korrigiert sein Skript und startet es erneut. Ein weiterer Versuch scheitert immer noch. Er kontrolliert wieder den Netzwerkverkehr mit `tcpdump` auf der internen Netzwerkkarte der Firewall. Wieder sieht er nur die DNS-Anfragen, aber keine Antworten. Er aktiviert wieder manuell die Log-Regel und beobachtet die Protokolle. Hier tauchen nun keine Meldungen auf. Er zeigt die Regeln der FORWARD-Kette

an und wundert sich, dass keine der Regeln einschließlich der Default-Policy ein Paket gezählt hat. So findet er schließlich den letzten Fehler. Die Weiterleitung (das Forwarding) der Pakete ist auf der Firewall noch nicht aktiviert. Da ein Forwarding nicht erlaubt ist, tauchen die Pakete nicht in der `FORWARD`-Kette auf. Der Administrator erweitert sein Skript um eine der beiden folgenden Zeilen:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
sysctl -w net.ipv4.ip_forward=1
```

Nach einem Neustart des Skripts funktioniert auch der Zugriff auf das Internet. Das Skript erlaubt den gewünschten Zugriff. Nun muss der Administrator noch prüfen, ob auch der unerwünschte Zugriff unterbunden wird. Anstatt jeden einzelnen Dienst manuell zu testen, verwendet er `nmap`, das ich im nächsten Abschnitt genauer erläutere.

15.2 Nmap

Nmap, der »Network Mapper«, ist ein Open-Source-Werkzeug, das Sie bei der Analyse von Netzwerken und bei Sicherheitsaudits unterstützen kann. Es scannt große Netzwerke, wie auch einzelne Rechner, sehr schnell und kann sogar in vielen Fällen das Betriebssystem und die Laufzeit des Rechners ermitteln. In den Händen eines kundigen Anwenders, der Sie nach diesem Kapitel beginnen zu sein, erlaubt Nmap mächtige Prüfungen. Sie können feststellen, ob die Firewall stateful ist, welchen Patchlevel das Betriebssystem hat, welcher Dienst mit welcher Versionsnummer eingesetzt wird und ob ein Spoofen von TCP-Verbindungen möglich ist. Dabei sind die verschiedenen Funktionen von Nmap so gut dokumentiert, dass Sie nach dieser Einführung weitere Funktionen selbst sehr leicht erlernen können.

15.2.1 Nmap-Installation

Nmap ist bei den meisten Linux-Distributionen fester Bestandteil. Daher ist eine zusätzliche Installation aus den Quellen nicht zwingend erforderlich. Dennoch möchte ich im Weiteren kurz die Installation von Nmap beschreiben, da Sie nur so die aktuellste Version erhalten.

Tipp

Nmap wird regelmäßig aktualisiert. Nmap erhält neue Funktionen, und die Fingerprint-Datenbank wird regelmäßig erweitert. Es ist daher sinnvoll, immer die neueste Version von Nmap einzusetzen. Hierfür ist nicht unbedingt die Installation aus den Quellen erforderlich, da Sie auf der Nmap-Homepage auch RPM-Pakete der neuesten stabilen Version finden (*http://www.insecure.org/nmap/nmap_download.html*). Dort finden Sie auch Nmap in einer Version für Microsoft Windows! Allerdings gibt es bei einigen Windows-Versionen Probleme zwischen Nmap und der Windows-Firewall. Hier sollten Sie die Nmap-Dokumentation lesen.

Um Nmap aus den Quellen zu installieren, laden Sie zunächst die aktuelle Version von der Homepage *http://www.insecure.org/nmap/nmap_download.html* und entpacken diese in einem geeigneten Verzeichnis.

```
# cd /tmp
# wget http://download.insecure.org/nmap/dist/nmap-<version>.tar.bz2
# cd /usr/local/src
# tar xjf /tmp/nmap-<version>.tar.bz2
# cd nmap-<version>
```

Erfreulicherweise bringen die aktuellen Versionen von Nmap alle wesentlichen benötigten Bibliotheken wie libpcre, libpcap und libnet bereits mit. Eine zusätzliche Installation dieser Bibliotheken ist nicht erforderlich.

Die Übersetzung erfolgt mit dem üblichen Dreisatz:

```
# ./configure
# make
# sudo make install
```

Wenn Sie Nmap in einem anderen Verzeichnis als `/usr/local` installieren möchten, können Sie das Verzeichnis beim `./configure --prefix <dir>`-Aufruf mit angeben.

Bei der Installation werden zwei Befehle installiert:

- `nmap`: Hiermit können Sie auf der Kommandozeile einen Scan starten (siehe Abbildung 15.3).
- `nmapfe`: Dieses grafische Werkzeug erlaubt Ihnen die Konfiguration und den Start des Scans mit der Maus (siehe Abbildung 15.4). Dieses Werkzeug kann auch mit dem Befehl `xnmap` gestartet werden.

Das grafische Nmap-Frontend `nmapfe` ist sehr gut geeignet, um einen ersten Einstieg in die Verwendung von Nmap zu erhalten. Auch wenn ich eigentlich kein großer Freund von grafischen Oberflächen bin und der Kommandozeilenbefehl mehr Funktionen aufweist, besitzt die grafische Oberfläche die nette Eigenschaft, immer das entsprechende Nmap-Kommando anzuzeigen, das ausgeführt wird. Außerdem hilft die farbige Ausgabe bei der optischen Aufnahme der Informationen.

15.2.2 Einfache Scans

Nmap unterstützt eine Vielzahl von Netzwerk- und Rechnerscans. Am häufigsten wird Nmap eingesetzt, um festzustellen, welche Ports auf einem anderen Rechner geöffnet sind und ob diese Ports von einer Firewall geschützt werden. In diesem Abschnitt wollen wir uns mit dieser Form der Scans beschäftigen. Die fortgeschrittenen Scans werden Sie in dem nächsten Abschnitt kennen lernen.

Nmap kann sowohl einen TCP-Port-Scan als auch einen UDP-Port-Scan durchführen. Selbst beim TCP-Port-Scan gibt es verschiedene Varianten, wie dieser Port-Scan durchgeführt werden kann. Am einfachsten ist der TCP-Connect-Scan.

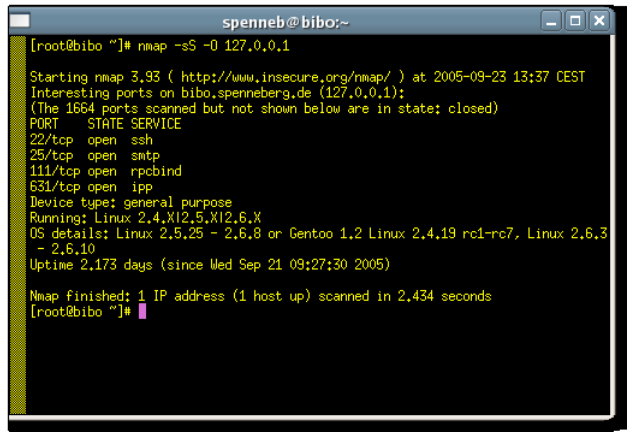


Abbildung 15.3: Alle Funktionen von Nmap stehen nur auf der Kommandozeile zur Verfügung.

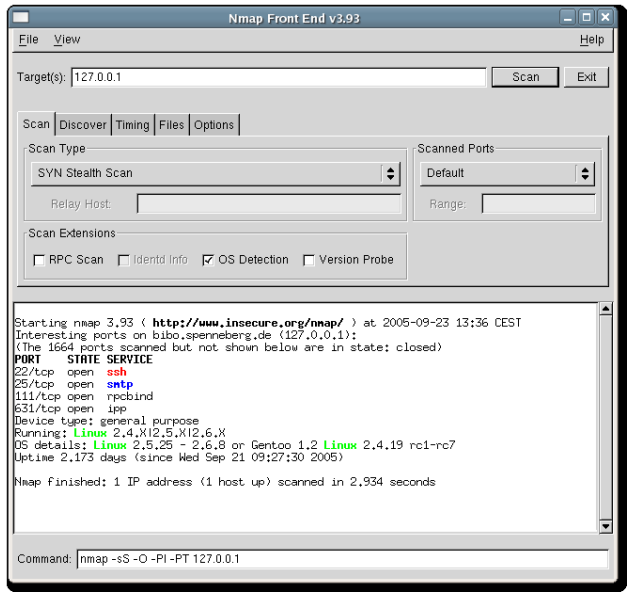


Abbildung 15.4: Die grafische Oberfläche erleichtert den Einstieg, aber bietet nur einen Teil der Funktionen.

TCP-Connect-Scan

Bei dem TCP-Connect-Scan (`nmap -sT`) versucht Nmap, zu jedem Port des Zielrechners eine vollständige TCP-Verbindung aufzubauen. Dabei wird ein kompletter TCP-Handshake durchlaufen. Dieser Scan liefert Ihnen das sicherste Ergebnis, da

hier die Verbindung tatsächlich so aufgebaut wird, wie auch ein Client sie aufbauen würde. Dies ist auch der einzige TCP-Scan, den Nmap ohne root-Privilegien durchführen kann, da dieser Scan ohne Umgehung des TCP/IP-Stapels durchgeführt werden kann.

```
# nmap -sT www.spenneberg.com
Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2005-09-23 15:04 CEST
Interesting ports on mail.spenneberg.net (217.160.128.61):
(The 1661 ports scanned but not shown below are in state: closed)
PORT    STATE    SERVICE
21/tcp  open     ftp
22/tcp  open     ssh
23/tcp  filtered telnet
25/tcp  open     smtp
53/tcp  open     domain
80/tcp  open     http
443/tcp open     https
993/tcp open     imaps

Nmap finished: 1 IP address (1 host up) scanned in 23.218 seconds
```

Nmap erkennt mit diesem Scan offene, geschlossene und von einer Firewall gefilterte Ports. Bei einem offenen Port kann Nmap die TCP-Verbindung aufbauen. Bei einem geschlossenen Port erhält Nmap beim Aufbau ein TCP-RST-Paket als Antwort, und bei einem von einer Firewall gefilterten Port erhält Nmap keine Antwort. Leider führt dieser Port-Scan zu Protokolleinträgen auf dem Zielsystem. Im Folgenden ist das Protokoll des Postfix-Mailservers während des Scans zu sehen:

```
Sep 23 15:07:17 mail postfix/smtpd[9259]: connect from p508F484E.dip.t-dialin.net
                                                                    [80.143.72.78]
Sep 23 15:07:17 mail postfix/smtpd[9259]: lost connection after CONNECT from p508F484E.
                                                        dip.t-dialin.net[80.143.72.78]
Sep 23 15:07:17 mail postfix/smtpd[9259]: disconnect from p508F484E.dip.t-dialin.net
                                                                    [80.143.72.78]
```

Um nun mit Nmap Ihre Firewall-Regeln zu prüfen, sollten Sie mit Nmap Ihre Firewall scannen und das Ergebnis mit Ihren Regeln vergleichen. Falls sich hinter der Firewall weitere nicht genattete Systeme befinden, sollten Sie auch versuchen, diese IP-Adressen zu scannen.

Tipp

Sobald eine Firewall im Spiel ist, können mindestens zwei verschiedene Phänomene auftreten:

Nmap bricht die Abarbeitung direkt ab. Dazu kommt es, da Nmap vor Beginn des Scans versucht, den Rechner zu pingen. Wenn dies nicht erfolgreich ist, vermutet Nmap, dass der Rechner nicht online ist, und bricht des Scan ab. Durch die Angabe von `-P0` (Pee Null) überspringen Sie den Ping. Zusätzlich kann es zu erhöhten Laufzeiten bei Nmap kommen. Eine Firewall verwirft möglicherweise die Pakete, die Nmap verschickt, und antwortet nicht darauf. Zur Sicherheit muss Nmap aber eine gewisse Zeit (Default 10 Sekunden) auf eine mögliche Antwort warten! Sie können die Nmap-Wartezeit mit der Option `--max_rtt_timeout` anpassen. Die Zeit geben Sie dabei in Millisekunden an. Um eine Sekunde als Timeout zu verwenden, nutzen Sie: `nmap -sT --max_rtt_timeout 1000 www.spenneberg.com`.

Außerdem beantworten einige Firewalls den TCP-Scan nicht mit TCP-RST-Paketen, sondern mit ICMP-Fehlermeldungen. So reagiert die Fedora Core 3-Standard-Firewall auf einen SYN-Scan mit ICMP-Host-Prohibited-Fehlermeldungen. Da diese Meldungen zusätzlich in ihrer Geschwindigkeit beschränkt werden, dauert der Scan mehrere Stunden. Die Verwendung der Option `-v` bei Nmap zeigt Ihnen, dass Nmap noch arbeitet, obwohl Sie keine Ausgaben sehen.

TCP-SYN-Scan

Eine Alternative zu dem Connect-Scan ist der SYN-Scan. Dieser Scan wird häufig auch als Half-Open-Scan bezeichnet, da er den TCP-Handshake nur zur Hälfte durchführt. Bei diesem Scan sendet Nmap ein SYN-Paket an den Port auf dem Server. Wenn Nmap ein TCP-ACK-Paket als Antwort eines offenen Ports erhält, sendet Nmap direkt im Anschluss ein TCP-RST-Paket, um die Verbindung bereits wieder zu beenden (siehe Abbildung 15.5).

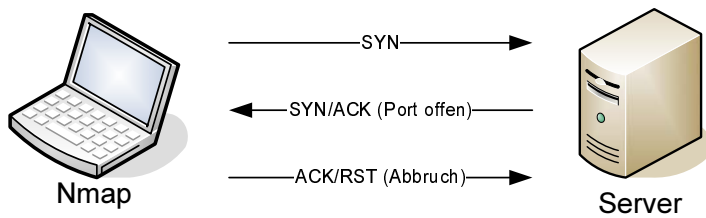


Abbildung 15.5: Nmap bricht beim SYN-Scan die Verbindung ab, bevor es zur Protokollierung auf dem Zielsystem kommt.

Einen geschlossenen Port erkennt Nmap an einer Fehlermeldung. Jedoch erkennt Nmap in diesem Modus, ob es sich um ein TCP-RST-Paket oder eine ICMP-Port-Unreachable-Meldung handelt. Während Nmap im Connect-Scan diesen Unterschied nicht erkennen kann, interpretiert es ein TCP-RST-Paket als geschlossenen Port, während es eine ICMP-Port-Unreachable-Meldung richtig als Ablehnung durch eine Firewall erkennt. Sobald Nmap eine ICMP-Port-Unreachable-Meldung oder keine Antwort erhält, zeigt es den Port als gefiltert an. Der folgende Scan ist auf derselben Maschine durchgeführt worden wie oben:

```
# nmap -sS www.spenneberg.com

Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2005-09-23 15:24 CEST
Interesting ports on mail.spenneberg.net (217.160.128.61):
(The 1657 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   filtered telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   open     http
110/tcp  filtered pop3
143/tcp  filtered imap
443/tcp  open     https
993/tcp  open     imaps
3306/tcp filtered mysql

Nmap finished: 1 IP address (1 host up) scanned in 10.177 seconds
```

Sie können erkennen, dass Nmap nun die Ports 110, 143 und 3306 zusätzlich als gefiltert anzeigt. Bei dem Connect-Scan wurden diese Ports als geschlossen interpretiert.

Wie Sie sehen, ist der SYN-Scan genauer als der Connect-Scan. Sie sollten daher Ihre Firewall und alle weiteren Systeme erneut mit dem SYN-Scan unter die Lupe nehmen. Falls Sie einen Port entdecken, der von der Firewall nicht geschützt wird, müssen Sie Ihr Firewall-Skript entsprechend anpassen.

Betriebssystem-Bestimmung

Sie möchten wissen, welches Betriebssystem auf einem entfernten System installiert ist? Nun, fragen Sie Nmap. Nmap kann mit Hilfe des TCP/IP-Stack-Fingerprinting sehr gut entscheiden, welches Betriebssystem sich auf der fraglichen Maschine befindet. Heute ist dies häufig eine der wenigen sicheren Methoden, das Betriebssystem zu ermitteln. Sicherlich sollten Sie zuvor prüfen, ob ein Banner-Grabbing Ihnen nicht einfacher und leichter diese Informationen zur Verfügung stellt:

```
# telnet www.spenneberg.com
Trying 217.160.128.61...
Connected to www.spenneberg.com (217.160.128.61).
Escape character is '^]'.
Fedora Core release 4 (Stentz)
Kernel 2.6.12-1.1398_FC4 on an i686
login:
```

Viele Administratoren ändern heute aber die Ausgabe der verschiedenen Dienste, so dass eine so ausführliche Ausgabe nur noch selten zu sehen ist. Dann hilft `nmap -O`:

```
# nmap -O www.spenneberg.com

Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2005-09-24 06:03 CEST
Interesting ports on mail.spenneberg.net (217.160.128.61):
(The 1657 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE
21/tcp   open     ftp
....
993/tcp  open     imaps
3306/tcp filtered mysql
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20
Uptime 282.906 days (since Wed Dec 15 07:19:50 2004)

Nmap finished: 1 IP address (1 host up) scanned in 17.989 seconds
```

Wie macht Nmap das? Nun, es verschickt verschiedene manuell erzeugte Pakete und beobachtet, wie das Zielsystem reagiert. Hierbei kommt es zu ganz charakteristischen Unterschieden. Zwar existieren Standards, die die TCP/IP-Protokolle beschreiben. Allerdings werden diese Standards von unterschiedlichen Programmierern unterschiedlich verstanden und interpretiert. Einige TCP/IP-Stacks enthalten auch einfach Fehler in der Behandlung von Paketen und verletzen den Standard. Anschließend vergleicht Nmap die gewonnenen Daten mit den Informationen in einer Datenbank und kann so das Betriebssystem bestimmen.

Hinweis

Nmap muss nicht immer das Betriebssystem richtig bestimmen können. Teilweise, besonders bei neuen Betriebssystemen, kann Nmap in seiner Datenbank kein passendes Betriebssystem finden. Dann können Sie, falls Sie wissen, um welches Betriebssystem es sich handelt, diese Informationen an den Programmierer von Nmap weitergeben!

Der Operatingsystem-Scan (-O) kann nur von root verwendet werden, da zur Erzeugung der Pakete besondere Privilegien erforderlich sind. Außerdem muss das Zielsystem über mindestens einen offenen und einen geschlossenen Port verfügen. Nmap scannt zu Beginn alle Ports und wählt dann jeweils einen aus. Wenn Sie bereits einen offenen und einen geschlossenen Port kennen, können Sie diese auch beim Aufruf angeben und Nmap so einen kompletten Portscan ersparen:

```
# nmap -O -p25,26 www.spenneberg.com
Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2005-09-24 06:24 CEST
Interesting ports on mail.spenneberg.net (217.160.128.61):
PORT   STATE  SERVICE
25/tcp open   smtp
26/tcp closed unknown
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20
Uptime 282.920 days (since Wed Dec 15 07:19:50 2004)

Nmap finished: 1 IP address (1 host up) scanned in 2.716 seconds
```

Hinweis

Sie können Nmap auch ein anderes Betriebssystem vorgaukeln. Für Linux existiert der IP-Personality Patch (*http://ippersonality.sf.net*). Dieser Patch für den Kernel 2.4 erlaubt es Ihnen, die Funktionen Ihres TCP/IP-Stacks so zu modifizieren, dass er einem anderen Stack (zum Beispiel AmigaOS oder HP Laserjet 4) entspricht.

Wenn Sie die Bestimmung des Betriebssystems betrachten, werden Sie feststellen, dass Nmap sogar die Uptime des gescannten Rechners ermitteln kann. Dies kann für einen potenziellen Angreifer eine sehr interessante Information sein. Ein Microsoft Windows NT-System, das seit über einem Jahr nicht neu gebootet wurde, kann kaum in der Zeit gepatcht worden sein. Nach dem Einspielen eines Patches oder Servicepacks, ja sogar nach dem Ändern einer IP-Adresse, ist ein Reboot erforderlich. Nmap verwendet für diese Technik die TCP-Timestamps aus dem RFC1323. Diese Technik wurde von den Nmap-Entwicklern von der Webpage *http://uptime.netcraft.com* übernommen.

Tipp

Wenn Sie den Timestamp-Scan Ihrer Systeme unterbinden möchten, können Sie unter Linux die Timestamps sehr leicht abschalten:

```
sysctl -w net.ipv4.tcp_timestamps=0
```

Wenn Sie möchten, dass diese Einstellung nach jedem Reboot aktiv ist, tragen Sie die Zeile `net.ipv4.tcp_timestamps=0` in der Datei `/etc/sysctl.conf` Ihrer Distribution ein.

UDP-Scan

Viele Administratoren verwenden lediglich die TCP-Scans von Nmap. Dabei kann Nmap noch viele weitere Scans durchführen. Der interessanteste Scan ist der UDP-Scan. Es gibt viele Dienste, die über einen UDP-Port erreichbar sind. Im Gegensatz zu TCP besteht bei UDP sehr leicht die Möglichkeit, gespoofte Pakete zu senden.

Hinweis

Natürlich ist es auch ein Leichtes, ein gespooftes TCP-Paket zu senden. Jedoch müssen Sie erst einen kompletten TCP-Handshake durchlaufen, bevor der Dienst Daten entgegennimmt. Das ist bei UDP anders. Sie versenden ein gespooftes UDP-Paket, und die Daten werden direkt an den Dienst weitergereicht. Handelt es sich um einen verwundbaren UDP-Dienst, so können Sie möglicherweise mit einem Paket bereits den kompletten Angriff durchführen. Eine sehr eindrucksvolle Demonstration war der SQL-Slammer-Wurm, der die Microsoft-SQL-Engine auf dem Port 1434/udp mit einem 376 Byte großen Paket angriff und die Kontrolle übernahm (*http://www.cert.org/advisories/CA-2003-04.html*).

Leider steht der UDP-Scan (`-sU`) nur dem Benutzer root zur Verfügung. Außerdem kann es beim UDP-Scan zu sehr langen Nmap-Laufzeiten kommen, wenn eine Firewall den Zugriff auf die Ports unterdrückt. Hier hilft auch die Option `--max_rtt_timeout`.

Um nun einen UDP-Scan durchzuführen, verwenden Sie den folgenden Befehl:

```
nmap -sU www.spenneberg.com
```

Hier kommt es im Zusammenhang mit Firewalls immer wieder zu Verwirrungen. Wenn eine Firewall mit einer DROP-Regel den Zugriff auf einen UDP-Port verwehrt, wird Nmap diesen Port als offen kennzeichnen. Um dies zu verstehen, müssen Sie wissen, wie Nmap UDP-Ports scannt. Hierzu sendet es ein UDP-Paket an den fraglichen Port des Zielrechners. Erhält Nmap ein ICMP-Port-Unreachable zurück, ist der Port geschlossen. Sobald Nmap aber ein UDP-Paket oder keine Antwort

zurückerhält, muss Nmap den Port als offen deklarieren. Die Tatsache, dass Nmap keine Antwort erhält, kann auch in einer fehlerhaften Anfrage an einen laufenden Dienst begründet sein. Wundern Sie sich also nicht, wenn Nmap offene UDP-Ports auf Ihrem System nennt.

15.2.3 Fortgeschrittene Anwendung

(TCP/Ping)-Sweeps

Bevor Sie mit der Überprüfung Ihrer Firewall-Regeln oder einer Analyse eines Netzwerks beginnen, sollten Sie ermitteln, welche Rechner überhaupt sichtbar sind. Vielleicht haben Sie von Ihrem Provider ein Klasse-C-Netzwerk zugeordnet bekommen. Diese IP-Adressen nutzen Sie nun in Ihrer Firewall und Ihrer DMZ. Natürlich kennen Sie diese IP-Adressen, aber Sie möchten prüfen, welche Rechner von außen ermittelt werden können. Hierfür eignen sich die Sweep-Scans. Diese fegen (sweep) durch ein Netzwerk und probieren dabei jede IP-Adresse aus.

Der einfachste Sweep-Scan ist der Ping-SweepSweep. Hier sendet Nmap an jede IP-Adresse eines Netzwerks ein Echo-Request-Paket und wartet auf die Echo-Reply-Antwort. Da einige Systeme Ping-Pakete blockieren, sendet Nmap zusätzlich auch ein TCP-ACK-Paket an den Port 80/tcp des Zielsystems. Wenn das Zielsystem erreichbar ist, antwortet es mit einem TCP-RST.

```
# nmap -sP 192.168.0.0/24

Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2005-09-24 07:08 CEST
Host 192.168.0.1 appears to be up.
MAC Address: 00:00:B4:B0:12:10 (Edimax Computer Company)
Host 192.168.0.108 appears to be up.
Host 192.168.0.254 appears to be up.
MAC Address: 00:50:18:1B:BC:A0 (AMIT)
Nmap finished: 256 IP addresses (3 hosts up) scanned in 6.364 seconds
```

Sobald sich jedoch eine Firewall zwischen Ihnen und dem Zielnetzwerk befindet, besteht die Gefahr, dass dieser Scan nicht funktioniert, da die Firewall Ping-Pakete unterbindet und ein TCP-ACK-Paket von einer zustandsorientierten (stateful) Firewall nur akzeptiert wird, wenn vorher eine TCP-Verbindung aufgebaut wurde.

Für diese Zwecke können Sie mit der Option `-P` die für den »Ping« zu verwendenen Pakete angeben!

- `-P0`: Kein Ping. Dies ist sinnvoll, wenn Sie wissen, dass ein Rechner online ist und Sie direkt einen Portscan starten möchten.
- `-PA25,80`: Sendet TCP-ACK-Pakete an die Ports 25 und 80. Wenn das System erreichbar ist, sendet es ein TCP-RST-Paket als Antwort. Eine zustandsorientierte Firewall erlaubt das TCP-ACK-Paket nicht.
- `-PS25,80`: Diese Option sendet ein SYN-Paket an den angegebenen Port. Damit besteht häufig die Möglichkeit, durch eine zustandsorientierte Firewall hindurch

einen Rechner zu erreichen. Die Firewall öffnet häufig die Ports 25 und 80, um SMTP- und HTTP-Verkehr zu erlauben. Weitere gute Ports zum Test sind 21 (FTP), 22 (SSH) und 443 (HTTPS).

- `-PU54,222`: Hiermit können Sie UDP-Pakete für den Ping nutzen. Wenn der Port geschlossen ist und der Rechner erreichbar ist, erwartet der Scan ein ICMP-Port-Unreachable. Bei einem offenen Port erhält man häufig keine Antwort, da der Dienst die Anfrage nicht versteht. Daher sollten Sie Ports verwenden, die üblicherweise geschlossen sind (z.B. 54 und 222).
- `-PE`: Wenn Sie diese Option verwenden, führt Nmap einen echten Ping-Scan durch. Damit können auch Broadcast-Adressen in dem Zielnetzwerk gefunden werden. Viele Systeme (vor allem Unix, kein Windows) reagieren auf einen Broadcast-Ping mit einer Antwort. Diese Broadcast-Adressen können dann für Denial-of-Service-Angriffe à la SMURF (*http://www.cert.org/advisories/CA-1998-01.html*) missbraucht werden.
- `-PP`: Diese Option verwendet ICMP-Timestamp-Request-Pakete für den Scan. Einige Systeme antworten auf diesen Scan mit einem ICMP-Timestamp-Reply. Daher kann dieser Scan anstelle eines Ping genutzt werden. Linux-Systeme ignorieren diese Anfrage.
- `-PM`: Diese Option verwendet einen ICMP-Netmask-Request für den Scan.
- `-PB`: Diese Option verwendet die Default-Nmap-Ping-Kombination aus einem Echo-Request- und einem TCP-ACK-Paket (siehe oben).

Wenn Sie durch eine zustandsorientierte Firewall die sich dahinter befindlichen Systeme auskundschaften möchten, ist es am einfachsten, die Option `-PS` zu verwenden. Allerdings sollten Sie sich Gedanken über die zu testenden Ports machen. Sinnvoll sind 22 (SSH), 21 (FTP), 25 (SMTP), 80 (HTTP), 110 (POP3), 143 (IMAP) und 443 (HTTPS). Damit erreichen Sie auch Systeme durch eine Firewall, die den Port 80 nur bei einer Verbindung zum Webserver erlaubt, aber nicht bei einer Verbindung zu einem Mailserver (siehe Abbildung 15.6).

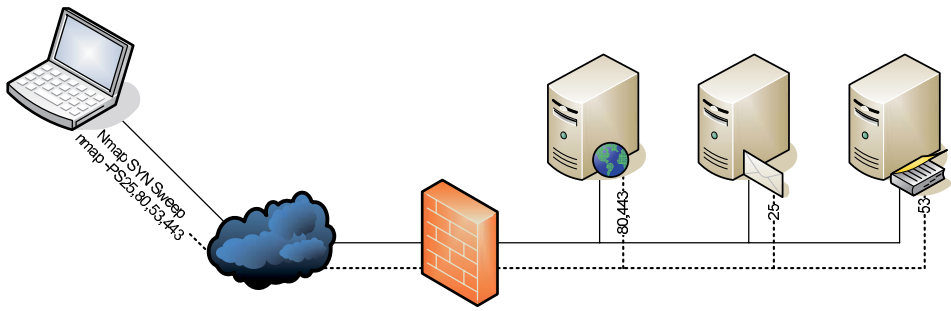


Abbildung 15.6: Nmap kann durch eine zustandsorientierte Firewall die in der DMZ stehenden Rechner ermitteln.

Protokoll-Scan

Sehr interessant ist häufig auch der Protokoll-Scan (`-sO`). Er kann sehr viel über ein System aussagen. Hier führt Nmap einen Scan der möglichen IP-Protokolle (`/etc/protocols`) durch. Bei einem normalen System sieht man üblicherweise nur die Protokolle ICMP, TCP und UDP:

```
# nmap -sO www.spenneberg.com

Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2005-09-24 16:01 CEST
Interesting protocols on mail.spenneberg.net (217.160.128.61):
(The 253 protocols scanned but not shown below are in state: open|filtered)
PROTOCOL STATE    SERVICE
1        open     icmp
6        open     tcp
17       filtered udp

Nmap finished: 1 IP address (1 host up) scanned in 6.099 seconds
```

Sobald das System aber auch über IPv6-Funktionalität verfügt, taucht mindestens auch dieses Protokoll in der Liste auf:

```
# nmap -sO localhost

Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2005-09-24 16:04 CEST
Interesting protocols on bibo.spenneberg.de (127.0.0.1):
(The 250 protocols scanned but not shown below are in state: closed)
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open          tcp
17       open          udp
41       open|filtered ipv6
```

Sehr interessant ist ein Protokoll-Scan eines VPN-Gateways. Dann tauchen zusätzlich in der Liste die Protokolle ESP und AH auf. Diese IPsec-Protokolle tauchen auch auf einem Linux-System erst auf, wenn die VPN-Funktionalität tatsächlich genutzt wird. So können Sie also mögliche VPN-Zugangssysteme erkennen.

```
# nmap -sO schulung.spenneberg.net
Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2005-09-24 16:08 CEST
Interesting protocols on schulung.spenneberg.net (x.y.z.a):
(The 248 protocols scanned but not shown below are in state: closed)
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open          tcp
```

```
17      open          udp
41      open|filtered ipv6
50      open|filtered esp
51      open|filtered ah
```

So können Sie auch prüfen, ob Ihre Firewall die entsprechenden IP-Protokolle richtig filtert.

Weitere Stealth-Scans

Wenn der Port-Scan möglichst unentdeckt bleiben soll oder Sie die Protokollierung Ihrer Firewall, die Auswertung der Protokolle oder Ihr Intrusion-Detection-System testen wollen, dann sollten Sie auch die Stealth-Scans von Nmap kennen. Diese Scans sollen unbemerkt von einem Administrator durchgeführt werden können. Allerdings erkennen viele IDS mindestes den Xmas- und den Null-Scan. Nmap bezeichnet drei Scans als Stealth-Scan:

- `-sF`: Der TCP-FIN-Scan sendet ein Paket, in dem nur das TCP-FIN-Flag gesetzt ist.
- `-sX`: Der Xmas-Scan sendet ein Paket, in dem das TCP-FIN, -URG und -PSH-Flag gesetzt sind. Im Gegensatz zur weitläufigen Meinung sind hier nicht alle Flags gesetzt, sondern nur sehr viele. Daher kommt auch der Name: Alle Flags brennen wie die Kerzen an einem Christbaum zu Weihnachten (Xmas).
- `-sN`: Der Null-Scan sendet ein Paket, in dem kein TCP-Flag gesetzt ist.

Bei allen diesen Scans muss das Zielsystem laut RFC793 bei einem offenen Port das Paket ignorieren. Ein geschlossener Port muss ein TCP-RST-Paket als Antwort generieren. Sie können mit diesen Scans also erkennen, ob ein Port geschlossen ist. Leider können Sie nicht sicher sagen, ob ein Port tatsächlich offen ist, da auch eine Firewall das Paket verworfen haben kann, so dass es nicht zur Antwort kam! Nmap listet daher die Ports als `open|filtered` auf:

```
# nmap -sF www.spenneberg.com

Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2005-09-24 16:35 CEST
Interesting ports on mail.spenneberg.net (217.160.128.61):
(The 1657 ports scanned but not shown below are in state: closed)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
110/tcp  filtered      pop3
143/tcp  filtered      imap
443/tcp  open|filtered https
```

```
993/tcp  open|filtered imaps
3306/tcp filtered      mysql
```

Dass in dem obigen Fall doch einige Ports als definitiv gefiltert angezeigt wurden, hängt mit den Firewall-Regeln zusammen. Diese Ports werden von der Firewall mit einem ICMP-Port-Unreachable abgelehnt. Da das echte Zielsystem ein TCP-RST-Paket erzeugen würde, muss die ICMP-Nachricht von einer Firewall stammen. Der Port wird also gefiltert.

Für mich zählt der TCP-ACK-Scan (`-sA`) auch zu den Stealth-Scans, denn ein IDS protokolliert üblicherweise den Scan nicht, und Sie können mit ihm feststellen, ob ein Port tatsächlich offen ist oder von einer Firewall gefiltert wurde:

```
# nmap -sA www.spenneberg.com

Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2005-09-24 16:38 CEST
Interesting ports on mail.spenneberg.net (217.160.128.61):
(The 1664 ports scanned but not shown below are in state: UNfiltered)
PORT     STATE    SERVICE
23/tcp   filtered telnet
110/tcp  filtered pop3
143/tcp  filtered imap
3306/tcp filtered mysql
```

Dieser Scan sendet ein TCP-ACK-Paket an den entsprechenden Port. Wird der entsprechende Port gefiltert, erwarten wir keine Antwort. Wird der entsprechende Port aber nicht gefiltert, erwarten wir in jedem Fall (Port offen oder geschlossen) immer ein TCP-RST-Paket als Antwort. Nmap zeigt nun, dass die Ports 23, 110, 143 und 3306 tatsächlich gefiltert werden. Das bedeutet in Kombination mit dem TCP-FIN-Scan, dass die Ports 21, 25, 53, 80, 443 und 993 offen sein müssen. Sie können also, ohne einen TCP-SYN-Scan einzusetzen, ermitteln, ob ein Port offen oder geschlossen ist oder durch eine Firewall gefiltert wird.

Hinweis

Dies funktioniert nur richtig bei einer zustandslosen Firewall wie `ipchains`. Eine richtig konfigurierte zustandsorientierte Firewall wird die TCP-ACK- und TCP-FIN-Pakete immer filtern und nicht passieren lassen. Nur eine zustandslose Firewall muss diese Pakete für offene Ports passieren lassen, da sie nicht erkennen kann, ob die Pakete zu aufgebauten Verbindungen gehören.

Decoy-Scan

Der Decoy-Scan ist sicherlich auch eher ein Scan für den Test eines Intrusion-Detection-Systems als für den Test einer Firewall. Aber er kann eingesetzt werden, um die Analyse der Firewall-Protokolle zu testen. Hierbei handelt es sich um eine

Ergänzung eines normalen Scans. Der Decoy-Scan kann mit allen Scans, außer dem RPC-Scan, eingesetzt werden. Dabei definieren Sie mit der Option `-D` mehrere IP-Adressen, die Nmap als Decoy (Tarnung) verwenden soll. An beliebiger Stelle in der komma-separierten Liste fügen Sie `ME` als Platzhalter für die eigene IP-Adresse ein. Nmap führt dann entsprechend viele Scans durch und fälscht dabei die Absenderadressen in den verschiedenen Scans. Wenn das gescannte System diese Scans protokolliert, hat es den Anschein, als ob das System gleichzeitig von verschiedensten Orten gescannt wird. Das Opfer kann kaum ermitteln, welche Ihre IP-Adresse ist, und den Scan daher nicht zurückverfolgen. Sie müssen Ihre Adresse natürlich angeben, denn sonst erhält Nmap keine Rückmeldung und kann Ihnen nicht das Ergebnis anzeigen. Versäumen Sie die Angabe der Position mit `ME`, wählt Nmap zufällig eine Position in der IP-Adressliste.

Banner-Grabbing

Sicherlich ist es ganz interessant, welche Ports auf einem System geöffnet sind. Die Tatsache, dass der Port 25/tcp offen ist, sagt bereits eine ganze Menge über das System aus. Es empfängt E-Mail, wahrscheinlich versendet es sie auch. Möglicherweise ist es ein Relay, das die E-Mail weiter nach innen versendet. Wahrscheinlich kann das System auch eine DNS-Auflösung durchführen. Um aber zu erkennen, ob sich dahinter eine echte Sicherheitslücke befindet, benötigen Sie mehr Informationen, und auch der potenzielle Angreifer, der durch Ihre Firewall auf Ihren Mailserver zugreift, wird versuchen, mehr Informationen zu erhalten. Am einfachsten erhält er die Informationen, indem er sich mit dem Port verbindet und versucht, den Dienst zur Ausgabe seines Banners zu überreden. Bei einem Mailserver erhalten Sie die Informationen automatisch, bei einem Webserver müssen Sie tatsächlich zunächst nach Informationen fragen, bevor Sie sein »Banner« erhalten. Nmap kann diese Aufgabe für Sie übernehmen. Nmap nennt diesen Scan den Version-Detection-Scan (`-sV`). Nmap ist häufig in der Lage, das Applikationsprotokoll (ftp, ssh, telnet etc.), den Namen der Applikation (Apache, Solaris telnetd etc.), dessen Version und sogar weitere Details zu ermitteln. Verlangt der Dienst eine Verbindung über die Secure Socket Layer (SSL), so nutzt Nmap auch OpenSSL, falls die Unterstützung bei der Übersetzung aktiviert wurde.

```
# nmap -sV www.spenneberg.com

Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2005-09-24 17:12 CEST
Interesting ports on mail.spenneberg.net (217.160.128.61):
(The 1657 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE  VERSION
21/tcp   open     ftp      vsFTPd 1.2.1
22/tcp   open     ssh      OpenSSH 3.6.1p2 (protocol 1.99)
23/tcp   filtered telnet
25/tcp   open     smtp     Postfix smtpd
53/tcp   open     domain   ISC Bind 9.2.4
80/tcp   open     http     Apache httpd 2.0.46 ((Red Hat))
```

```
110/tcp  filtered pop3
143/tcp  filtered imap
443/tcp  open     ssl/http Apache httpd 2.0.46 ((Red Hat))
993/tcp  open     ssl/imap Dovecot imapd
3306/tcp filtered mysql
Service Info: Host:  mail.spenneberg.net; OS: Unix

Nmap finished: 1 IP address (1 host up) scanned in 40.872 seconds
```

Wenn Sie Ihre Systeme prüfen, sollten Sie bei einer Ausgabe wie der obigen überlegen, ob Sie die Banner der Dienste nicht anpassen wollen, so dass die Ausgabe weniger Informationen enthält. Mindestens die Angabe der Versionsnummern sollte bei den Diensten, bei denen es möglich ist, unterbunden werden. Ein Beispiel hierfür ist der Dovecot-`imapd` oder der Postfix-`smtpd` in dem obigen Beispiel.

Idle-Scan

Der Idle-Scan wurde zuerst im Dezember 1998 von dem Hacker Antirez für sein Werkzeug `hping2` (*http://www.hping.org*) entwickelt. Hierbei führen Sie einen Portscan mit gespoofter Absenderadresse durch. Eigentlich ist das nicht möglich, denn für einen Portscan benötigen Sie ja eine Rückmeldung von dem Zielsystem, um zu unterscheiden, ob der Port offen oder geschlossen ist. Bei diesem Scan fälschen Sie jedoch Ihre Absenderadresse, so dass diese Antwort an ein anderes System geschickt wird. Bei dem Decoy-Scan konnte das funktionieren, da auch noch ein Scan mit der eigenen Adresse zusätzlich zu den gefälschten Adressen erfolgte. Das ist hier nicht der Fall.

Wie funktioniert das? Betrachten Sie die Abbildung 15.7. Dort sehen Sie ein Opfer (rechts), den Rechner des Angreifers (unten) und einen weiteren Rechner (links). Dieser weitere Rechner ist der *Zombie* oder *Silent Host*. In dem Scan verwendet der Angreifer dessen IP-Adresse als Absender-IP-Adresse.

Der Angreifer sendet nun mehrere TCP-SYN-Pakete an einen Port (1). Ist der Port offen, so sendet das Opfer ein TCP-SYN-ACK-Paket an den Zombie (2a). Ist der Port geschlossen, so sendet das Opfer ein TCP-RST-Paket an den Zombie (2b). Wie reagiert nun der Zombie? Auf das TCP-RST-Paket (2b) erfolgt keine Reaktion (3b). Auf das TCP-SYN-ACK-Paket (2a) reagiert der Zombie aber mit einem TCP-RST-Paket, da er die Verbindung nicht kennt (3a). Also, halten wir fest: Ist der Port auf dem Opfer offen, versendet der Zombie ein Paket. Ist der Port geschlossen, ist das nicht der Fall. Der Angreifer muss nun also herausfinden, ob der Zombie ein Paket versendet. Daraus kann er schließen, ob der Port offen oder geschlossen ist.

Hierzu nutzt der Angreifer das IP-Identifikationsfeld im IP-Header der Pakete. Dieses Feld wird von fast allen Betriebssystemen gesetzt, aber nur ausgewertet, wenn Pakete fragmentiert werden. Dann erkennt der Empfänger der Fragmente zusammengehörige Fragmente an der identischen Nummer in diesem Feld. Es gibt keinen weiteren regulären Nutzen für dieses Feld. Die meisten TCP/IP-Stacks zählen da-

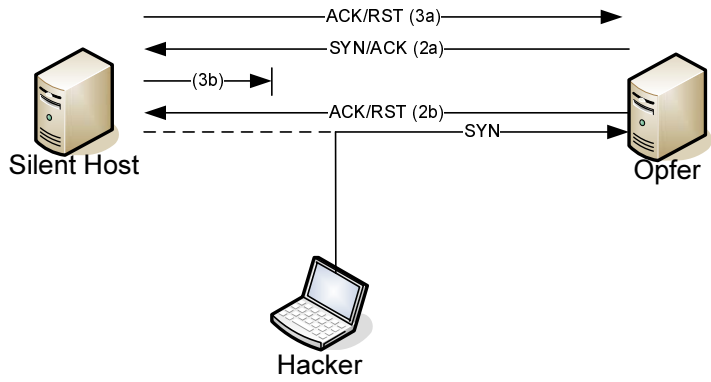


Abbildung 15.7: Bei dem Idlescan nutzt der Angreifer einen dritten Rechner in dem Scan.

her diese Nummer einfach hoch. Jedes Paket, das sie versenden, erhält eine um eins hochgezählte Nummer. Sobald sie bei 65535 angekommen sind, fangen sie wieder bei null an.

Hinweis

Die Linux-Kernel 2.4 und 2.6 setzen dieses Feld auf null, sobald die Path Maximum Transmission Unit Discovery (PMTU-Discovery) eingeschaltet ist. Da nun kein Paket mehr fragmentiert werden darf, wird dieses Feld nicht benötigt.

OpenBSD erzeugt zufällige Nummern in diesem Feld. Fragmente können dann immer noch an der gleichen Nummer erkannt werden.

Der Angreifer sucht nun als Zombie einen Rechner, der so die Identifikationsnummer hochzählt. Eine weitere Bedingung für dieses System ist seine Leblosigkeit. Das System sollte keinen weiteren Netzwerkverkehr erzeugen. Es sollte online sein, aber tot (Zombie, Silent Host).

Nun beginnt der Angreifer, diesem Rechner einmal pro Sekunde ein TCP-SYN-Paket auf einem geschlossenen Port zu senden. Der Zombie reagiert einmal pro Sekunde mit einem TCP-RST-Paket. Die Identifikationsnummer in den Paketen wird immer um 1 hochgezählt (4a, Abbildung 15.8). Gleichzeitig führt er den gespooften Portscan einmal pro Sekunde auf sein Opfer aus. Ist der Port offen, so muss der Zombie einmal pro Sekunde ein weiteres Paket versenden. Die Identfikationsnummer in dem TCP-SYN-Scan (4b) wird nun immer um zwei hochgezählt. War der Port geschlossen, so ändert sich an der Differenz zweier Identifikationsnummern nichts.

Während dieser Scan mit dem originalen Werkzeug `hping` durchaus umständlich war, ist dies mit Nmap sehr einfach. Sie geben lediglich mit der Option `-sI <zombie`

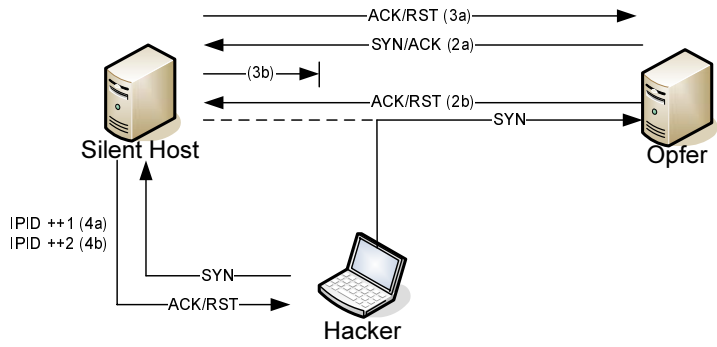


Abbildung 15.8: Bei dem Idlescan hängt die Identifikationsnummer der Pakete des Zombies von dem Zustand des Ports auf dem Opfer ab.

`host[:probeport]>` den Zombie-Rechner und optional einen Port an. Den Rest erledigt Nmap automatisch.

Achtung

Denken Sie daran, mit der Option `-P0` den Ping vor dem Scan abzuschalten. Dieser Ping wird sonst mit Ihrer echten IP-Adresse durchgeführt!

Achtung

Die Version 3.93 von Nmap hat einen Fehler in dem Idlescan, der zu einem Abbruch des Programms führt. Auf der Mailingliste wurde ein Patch veröffentlicht, der das Problem behebt (*http://seclists.org/lists/nmap-dev/2005/Jul-Sep/0197.html*).

Modifikation des Client-Ports, Spoofing, Time-Tuning und Fragmentierung

Häufig werden Sie einen Port-Scan einer Firewall durchführen, bei dem Sie anschließend das Gefühl haben, dass alles in Ordnung sei. Kein Port ist offen. Dennoch finden Sie anschließend Hinweise, dass ein Angreifer doch durch die Firewall gekommen ist, oder bei einem Penetrationstest findet eine andere Person doch Lücken in Ihrer Firewall. Wie kann das sein?

Die Probleme, die ich hier beschreibe, betreffen Sie nicht, wenn Sie Ihre Regeln so entwickelt und aufgesetzt haben, wie in diesem Buch beschrieben wird. Sie können aber davon betroffen sein, wenn Sie noch `ipchains` als Firewall einsetzen oder Ihre `iptables`-Regeln nicht das Connection Tracking nutzen.

Bei `ipchains`-Regelwerken finden Sie häufig die folgenden Regeln:

```
# DNS
ipchains -A forward -s $INTNETZ -p udp --destination-port 53 -j ACCEPT
ipchains -A forward -d $INTNETZ -p udp --source-port 53 -j ACCEPT

# Aktives FTP
ipchains -A forward -d $INTNETZ -p tcp --source-port 20 -j ACCEPT
ipchains -A forward -s $INTNETZ -p tcp --destination-port 20 -j ACCEPT
```

Die ersten beiden Regeln erlauben UDP-Pakete an den Port 53 im Internet und den Rückweg. Damit sollen DNS-Anfragen ermöglicht werden. Die nächsten beiden Regeln erlauben Verbindungen von dem Port 20/tcp in das interne Netz. Hiermit werden aktive FTP-Verbindungen erlaubt.

Achtung

Leider gibt es beim Einsatz von `ipchains` keine wesentlich bessere Alternative für die DNS-Regeln. Die Regeln für das aktive FTP sind aber grob fahrlässig. Bei Verwendung von `ipchains` müssen Sie aktives FTP verbieten. Dies öffnet zu viele Sicherheitslücken. Nutzen Sie stattdessen passives FTP. Bei richtiger Anwendung von `iptables` besteht hier aber keinerlei Sicherheitsproblem.

Diese Regeln erlauben Pakete von außen in das interne Netz `$INTNETZ`. Sie müssen nur als Absender den richtigen Port verwenden! Bei Nmap können Sie den Source-Port mit der Option `--source_port` angeben. Sinnvoll sind hier die Ports 53/udp, 20/tcp und 53/tcp. Bei dem oben angegebenen Regelwerk könnten Sie damit jeden Rechner hinter der Firewall scannen!

Auch ein Spoofing des Scans wie beim Idle-Scan kann Ihnen mehr Informationen liefern, als Sie normalerweise erhalten würden. Viele Regelsätze erlauben nur bestimmten Rechnern, durch die Firewall auf interne Rechner zuzugreifen. Wenn Sie derartige Vertrauensverhältnisse vermuten oder in Ihrer eigenen Firewall testen möchten, können Sie den Idle-Scan hierfür verwenden! Geben Sie als Zombie einfach den »vertrauten« Rechner an. Der Scan muss natürlich durchgeführt werden, wenn der Zombie keinen weiteren Netzwerkverkehr erzeugt (nachts).

Zwei weitere Optionen in Nmap versuchen, den Scan vor möglichen Erkennungssystemen zu verstecken. Die Option `-f` fragmentiert die Pakete vor dem Versand in kleine Fragmente. Viele Firewalls defragmentieren diese zwar vor ihrer Analyse, aber häufig übersehen gerade einfache Firewalls und IDS die Fragmente und beachten sie nicht.

Achtung

Wenn Sie Linux als scannendes Betriebssystem einsetzen, müssen Sie darauf achten, dass auf Ihrem System keine `iptables`-Firewall mit Connection Tracking aktiv ist. Diese Firewall defragmentiert auch die ausgehenden Pakete! Sie können dann keine fragmentierten Pakete versenden.

Einen versteckten Port-Scan können Sie häufig auch durchführen, indem Sie das Timing des Port-Scans verändern. Hierzu bietet Nmap die Option `-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane>`, mit der Sie sehr einfach das Timing einstellen können. Viele IDS erkennen einen Port-Scan nur an einer bestimmten Häufigkeit und Geschwindigkeit. Natürlich können Sie bei Nmap auch die Zeiten einzeln einstellen. Die Manpage gibt Ihnen hier weitere Informationen.

Ausgabeformate

Wenn Sie häufiger derartige Scans durchführen, werden Sie auch unterschiedliche Ausgabeformate testen wollen. Nmap kann zunächst die Ausgabe mit `-oN` (Normal), `-oG` (Grepable), `-oX` (XML), `-oA` (Alle: NGX) und `-oS` (Skript-Kiddie-Sprache) in einer Datei protokollieren. Sie können sogar einen abgebrochenen Scan, der mit `-oN` oder `-oG` protokolliert wurde, mit `--resume` wieder aufnehmen.

Um die XML-Ausgabe später darstellen zu können, liefert Nmap auch ein XSL-Stylesheet mit (siehe Abbildung 15.9).

15.3 Nmap-Hilfswerkzeuge

Nmap ist ein sehr gutes Werkzeug, um Audits durchzuführen. Sie erkennen neue Systeme in Ihrem Netzwerk. Sobald ein neuer Port und damit ein neuer Dienst auftaucht, zeigt Ihnen Nmap diese Information an. Wenn Sie aber schon Nmap für 20 oder sogar 200 Rechner gestartet haben, werden Sie wissen, dass die Ausgabe von Nmap nicht gerade die manuelle Verarbeitung erleichtert. Speziell bei einem wiederholenden Einsatz von Nmap ist das maschinelle Verarbeiten und Vergleichen eine Arbeitsersparnis. Ich werde Ihnen im Weiteren einige Werkzeuge vorstellen, die mir dabei das Leben vereinfachen. Es gibt sicherlich noch weitere, vielleicht auch bessere Werkzeuge. Ich würde mich freuen, wenn Sie mir eine E-Mail schreiben würden, sollten Sie ein derartiges Werkzeug kennen.

15.3.1 Nmap-Audit

Dieses Perl-Skript (*http://heavyk.org/nmap-audit/*) vereinfacht den Nmap-Lauf in einem großen Netzwerk. Es startet mehrere Nmap-Prozesse gleichzeitig, scannt dabei

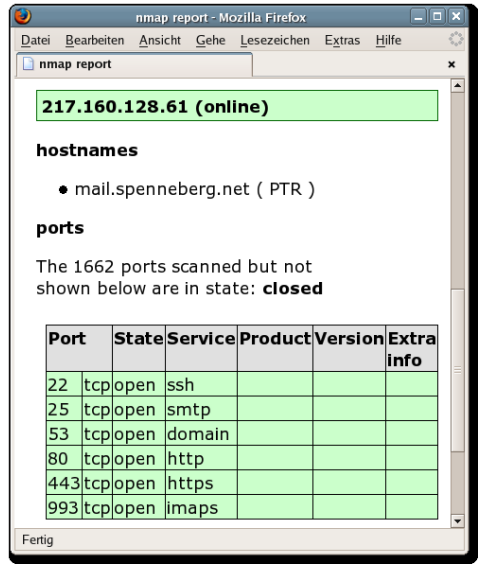


Abbildung 15.9: Nmap kann seine Ergebnisse in XML formatieren. Dieses können Sie zum Beispiel in Firefox anzeigen.

ein ganzes Netzwerk, ignoriert bei bestimmten Betriebssystemen konfigurierbare Ports und gibt das Ergebnis in einer übersichtlichen Ausgabe aus.

Um Nmap-Audit zu installieren, benötigen Sie Perl und das Perl-MIME-Lite-Modul. Falls dieses Modul nicht in Ihrer Distribution enthalten ist, können Sie es von CPAN (*http://cpan.uwinnipeg.ca/cpan/authors/id/Y/YV/YVES/MIME-Lite-3.01.tar.gz*) nachinstallieren. Anschließend laden Sie Nmap-Audit von der Homepage, entpacken es und installieren es mit den folgenden Befehlen:

```
# perl Makefile.PL
# make
# sudo make install
```

Nun müssen Sie noch eine Konfigurationsdatei erzeugen. Ohne Konfigurationsdatei kann Nmap-Audit nicht gestartet werden. Die Manpage `nmap-audit(1)` enthält ein ausführliches Beispiel, so dass ich hier nur eine kurze Version abbilde.

```
## IP-Adressen, die gescannt werden sollen
ips = 192.168.0.0/24

## E-Mail für Bericht
email-to = ralf@spenneberg.net
email-subject = Host Vulnerability Scanning Results
email-from = nmap-audit@spenneberg.net
```

```
## Gleichzeitige Nmap-Prozesse
max-threads = 20

## Detailgrad
detail = low

## Nmap-Scan
nmap = nmap -sS -v -O -T Polite -p 1-1024        # TCP scan

## Sicherungsverzeichnis
dir-name = /tmp/nmap

group windows
 os = Windows
 ignore = open        135        loc-srv            tcp
 ignore = open        135        loc-srv            udp
 ignore = open        137        netbios-ssn    udp            # wins
 ignore = open        138        netbios-ssn    udp            # netbios datagrams
 ignore = open        139        netbios-ssn    tcp            # netbios datagrams
 ignore = open        445        microsoft-ds   udp
 ignore = open        445        microsoft-ds   tcp
end group windows

group linux
 os = Linux Kernel 2.4.0 - 2.5.20
 ignore = open        22         ssh            tcp            # SSH
end group unix

group all
 hostname = *
 ignore = filtered    *        *        *
 ignore = closed      *        *        *
end group all
```

Diese Konfigurationsdatei teilt Nmap-Audit mit, welche IP-Adresse in dem Scan zu untersuchen sind. Anschließend sendet Nmap-Audit den Bericht an die angegebene Adresse. Sie geben auch den genauen Nmap-Befehl an, der von Nmap-Audit für jeden Rechner aufgerufen werden soll. Um die Ausgabe um die bekannten Ports zu reduzieren, können Sie für bestimmte Gruppen von Betriebssystemen die zu ignorierenden Ports angeben. Diese Ports tauchen dann in der Ausgabe nicht auf.

15.3.2 NDiff

NDiff ist ein Werkzeug, um die Unterschiede in zwei zeitlich versetzten Scans zu ermitteln. Obwohl Ndiff (*http://www.vinecorp.com/ndiff/download*) bereits stark in die Jahre gekommen ist (die letzte Version ist von 2001), liefert es immer noch wertvolle

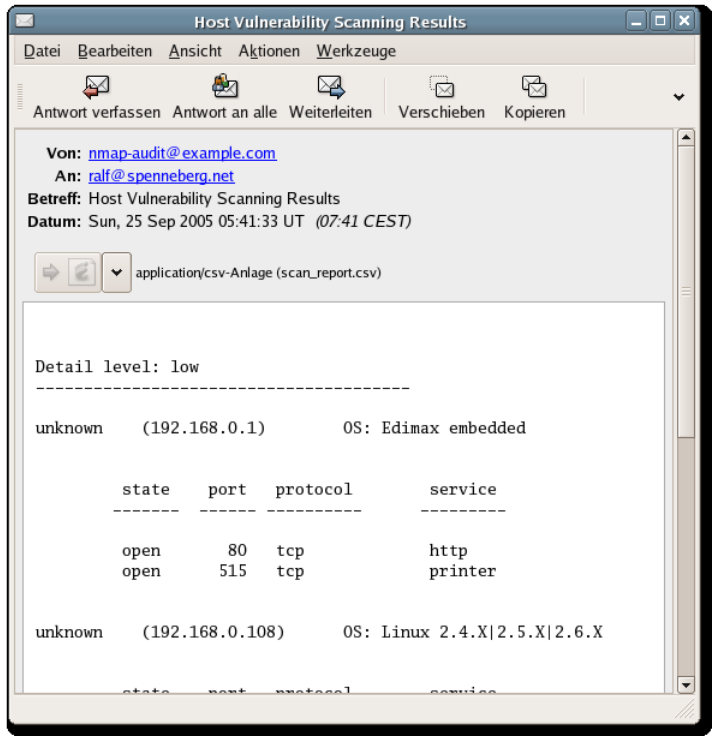


Abbildung 15.10: Nmap-Audit sendet seinen Bericht als E-Mail mit angehängter CSV-Datei.

Informationen. Ndiff enthält Werkzeuge zur Erzeugung von Baselines, erlaubt den täglichen vergleichenden Aufruf von Nmap und stellt die Ergebnisse in einer übersichtlichen Tabelle dar. Die Installation von NDiff erfolgt wie bei einem typischen Perl-Modul.

```
# tar xzf NDiff-<version>.tar.gz
# cd NDiff-<version>
# perl Makefile.PL
# make
# sudo make install
# man NDiff_Quickstart
```

Die Manpage enthält sehr viele Beispiele, so dass ich hier nur erste Hinweise zur Anwendung geben möchte. Um zwei Nmap-Läufe miteinander zu vergleichen, erzeugen Sie zunächst zwei maschinenlesbare Nmap-Protokolle, die Sie anschließend vergleichen.

```
# nmap -m /tmp/ersterlauf.nmap www.spenneberg.com
# nmap -m /tmp/zweiterlauf.nmap www.spenneberg.com
```

```
# ndiff -b /tmp/ersterlauf.nmap -o /tmp/zweiterlauf.nmap
-------------------------------------------------------
ndiff run So Sep 25 07:36:14 CEST 2005

command line: -b second -o first
baseline: ersterlauf.nmap
observed: zweiterlauf.nmap
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
new hosts:


- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
missing hosts:


- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
changed hosts:

217.160.128.61
     23/tcp    filtered -> open    telnet
    110/tcp    filtered -> open    pop3

-------------------------------------------------------
```

Wenn zwischen den beiden Läufen sich etwas geändert hat, dann wird Nmap das anzeigen.

15.3.3 Nmap-Parser

Seit einiger Zeit bietet Nmap die Ausgabe der Berichte in XML an. Diese Sprache bietet sich besonders zur Weiterverarbeitung durch Programme an. Nmap-Parser (*http://npx.sourceforge.net/*) ist eine Perl-Bibliothek, mit der Sie das XML-Format in Ihren Programmen parsen können. Dieses Werkzeug wird im Gegensatz zu den bisher vorgestellten Werkzeugen noch aktiv weiterentwickelt.

Nmap-Parser enthält auch zwei Perl-Beispielprogramme in dem Verzeichnis `./tools/`, die diese Bibliothek nutzen:

- `scan.pl`: Ein Perl-Skript, das einen Rechner scannt und die Ausgabe komprimierter als Nmap aufarbeitet.

```
Scan Host
-------------------------------------------------
[>] 192.168.7.52
      [+] Status: (UP)
      [+] Hostname(s) :
             test.spenneberg.com
      [+] Operation System(s) :
```

```
        Linux Kernel 2.4.0 - 2.5.20
[+] TCP Ports : (service) [version]
        22     ssh                 OpenSSH 3.5p1
        25     smtp
        443    https
[+] UDP Ports :
        111    rpcbind
```

- `nmap2sqlite.pl`: Dieses Programm nimmt die XML-Ausgabe von Nmap und speichert sie in einer SQLite DB. Dazu braucht dieses Skript eine Tabelle mit dem folgenden Schema:

```
ip              TEXT       PRIMARY  KEY NOT NULL,
mac             TEXT,
status          TEXT       DEFAULT  'down',
hostname        TEXT,
open_ports      TEXT       DEFAULT  'none',
filtered_ports  TEXT       DEFAULT  'none',
osname          TEXT,
osfamily        TEXT,
osgen           TEXT,
last_scanned    TIMESTAMP  DEFAULT  CURRENT_TIMESTAMP,
UNIQUE (ip))
```

  Das Skript kann sehr einfach für andere Datenbanken angepasst werden.

Auf der Homepage finden Sie in der Rubrik *Articles* weitere Hinweise und Beispielskripten.

15.3.4 nmaplr

Wenn Sie die XML-Ausgabe häufiger nutzen, werden Sie `nmaplr.pm` (*http://triple.aeoth.net/nmaplr/*) schätzen lernen. Dieses kleine Werkzeug nimmt einen Nmap-XML-Bericht und erzeugt daraus einen leicht lesbaren Bericht. So können Sie Ihre Ausgaben immer in XML schreiben lassen, müssen aber nicht auf lesbare Berichte verzichten.

Das Werkzeug nmaplr wird als Perl-Modul `nmaplr.pm` geliefert. Dadurch kann es nicht direkt eingesetzt werden. Die Dokumentation, die Sie mit `perldoc nmaplr.pm` erhalten, demonstriert Ihnen, wie Sie dieses Perl-Modul einsetzen können. Im Wesentlichen müssen Sie ein kleines Perl-Skript schreiben:

```
use nmaplr;

my $nlr = nmaplr->new(
log    => "nmap-report.xml",
report => "nmap-report.txt"
);
```

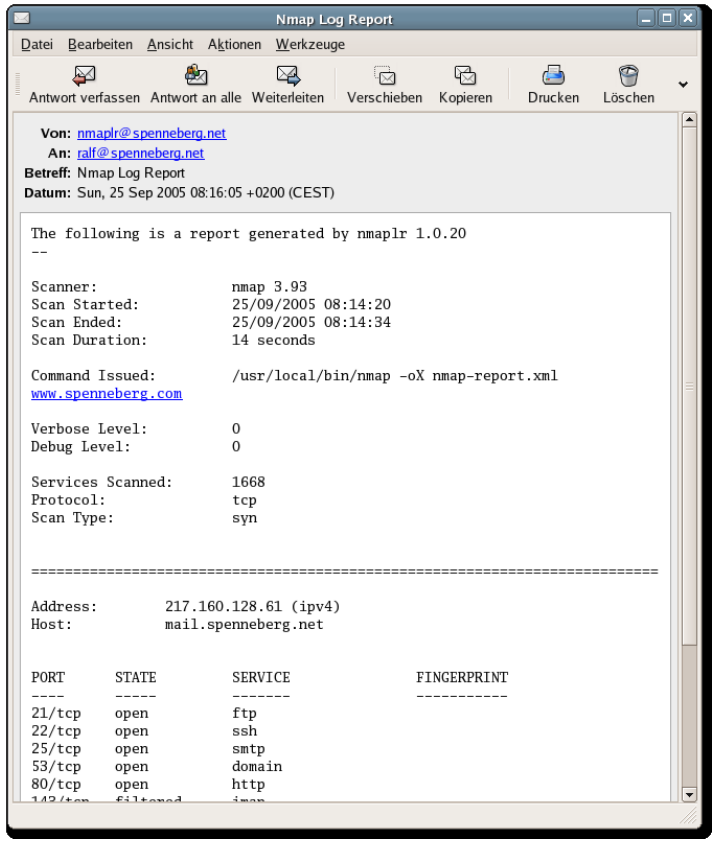


Abbildung 15.11: Nmaplr wandelt einen XML-Bericht in einen lesbaren Text um.

```
$nlr->createReport();

$nlr->sendMail(
  server => "localhost",
  from   => "nmaplr@spenneberg.net",
  to     => "ralf@spenneberg.net"
);
```

Nmaplr erzeugt dann die in der Abbildung 15.11 dargestellte E-Mail.

15.3.5 Fe3d

Fe3d (*http://projects.icapsid.net/fe3d/*) ist ein grafisches Visualisierungswerkzeug, das ein Nmap-XML-Protokoll in einem dreidimensionalen Raum darstellt. Dies erlaubt in einigen Fällen eine bessere Visualisierung der Daten und ihrer Zusammenhänge.

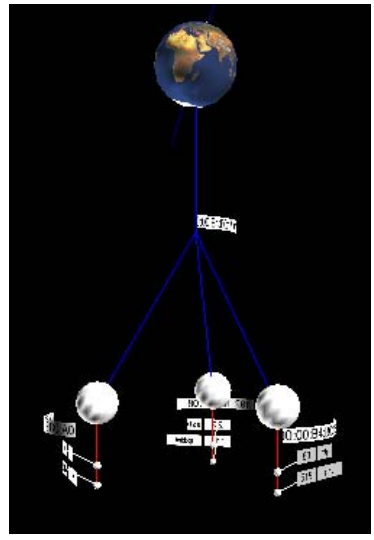


Abbildung 15.12: Fe3d kann die XML-Protokolldateien von Nmap dreidimensional und drehbar visualisieren.

Fe3d läuft unter Win32, IRIX, MacOS X und Linux. Der Entwickler stellt für Win32-Systeme fertige binäre Pakete zur Verfügung. Für die Installation unter MacOS X, IRIX oder Linux müssen Sie das Paket selbst installieren.

Für die Installation benötigen Sie die LibSDL-Bibliothek (*http://www.libsdl.org*), die LibSDL_TTF-Bibliothek (*http://www.libsdl.org/projects/SDL_ttf*), die LibPNG-Bibliothek (*http://www.libpng.org*) und den Xerces XML-Parser (*http://xml.apache.org/xerces-c/*). Viele dieser Pakete sind möglicherweise in Ihrer Distribution enthalten. Prüfen Sie das, bevor Sie die Pakete umständlich manuell installieren. Denken Sie auch daran, die entsprechenden Devel-Versionen der Pakete zu installieren. Dann können Sie Fe3d mit den Befehlen `./configure; make; sudo make install` installieren.

Anschließend können Sie mit `fe3d nmap.xml` die XML-Datei visualisieren. Abbildung 15.12 zeigt einen Screenshot unter Windows XP.

15.4 Nessus

Nessus (*http://www.nessus.org*) ist ein Open-Source-Vulnerability-Scanner. Eine komplette Vorstellung von Nessus würde den Rahmen dieses Buches sprengen, und es gibt auch bereits andere Bücher, die sich nur mit Nessus beschäftigen. Nessus ist ein hervorragendes Werkzeug, um einen Audit eines Netzwerks durchzuführen. Dies gilt umso mehr, da Nessus sehr ausführliche Berichte verfasst, aus denen hervorgeht, welche Sicherheitslücke gefunden wurde, wie diese zu bewerten ist und wie Sie sich dagegen schützen können. Allerdings ist Nessus immer nur so gut, wie die Person, die es bedient, und die Plugins, die es verwendet.

Hinweis: Nessus-Lizenz

Während Nessus selbst unter einer Open-Source-Lizenz steht, hat sich die Lizenz für die Plugins vor einiger Zeit geändert. Die Plugins, die von der Nessus-Entwicklerfirma Tenable Network Security veröffentlicht werden, sind unter zwei verschiedenen Lizenzen verfügbar. Die nicht-kommerzielle Lizenz erlaubt den Audit eigener Systeme und die Verwendung der Plugins zu diesem Zweck. Die kommerzielle Lizenz erlaubt darüber hinaus den Audit fremder Kundensysteme. Auf der Nessus-Homepage finden Sie weitere Informationen über die Lizenz (*http://www.nessus.org/plugins/*).

Während ich an diesem Buch gearbeitet habe, hat die Firma Tenable Network Security eine weitere Änderung der Lizenz bekannt gegeben. Nessus in der Version 3 wird nicht mehr unter der GPL-Lizenz, aber immer noch kostenfrei vertrieben werden! Allerdings haben sich eine ganze Reihe von Projekten die Weiterführung von Nessus unter GPL auf die Fahne geschrieben. Deren Erfolg muss abgewartet werden.

Nessus verfügt über sehr viele interessante Eigenschaften, die es für den Einsatz als Auditwerkzeug sehr wertvoll machen. Ich werde die wichtigsten im Folgenden aufzählen.

- Intelligenter Scan: Nessus erkennt Netzwerkdienste auch auf unüblichen Ports.
- Modulare Architektur: Der Client kann auf einem beliebigen Windows- oder Linux-System genutzt werden. Lediglich ein Linux-System für den Server ist erforderlich.
- Plugin-Architektur: Jede Sicherheitslücke wird durch ein externes Plugin realisiert. Neue Tests können so einfach über den Import neuer Plugins hinzugefügt werden. Dies können Sie sehr einfach über den Befehl `nessus-update-plugins` automatisieren. Die Plugins werden in NASL (Nessus Attack Scripting Language) geschrieben. Jedes offizielle Plugin referenziert CVE, CERT, Bugtraq etc.
- Berichte: Nessus erzeugt sehr ausführliche Berichte. Die Berichte können in HTML, XML oder sogar LaTeX exportiert werden.
- SSL-Unterstützung: Nessus kann auch über die Secure Socket Layer geschützte Dienste testen. Hierzu kann Nessus auch ein Clientzertifikat zugewiesen werden.
- Scanstufen: Nessus kann in unterschiedlichen Angriffsstärken gestartet werden. Während es per Default keinen Schaden auf dem Zielsystem anrichtet, können Sie Nessus auch so konfigurieren, dass es zu einem Einbruch oder Denial-of-Service auf dem Zielsystem kommen kann.
- Zusätzliche Software: Nessus kann weitere externe Software nutzen. So erkennt Nessus die Installation von Nmap, Nikto und Hydra und kann diese

Werkzeuge für den Scan nutzen. Nikto (*http://www.cirt.net/code/nikto.shtml*) ist ein Scanner für Webserver, während Hydra (*http://thc.org/thc-hydra/*) ein Brute-Force-Angriffswerkzeug für kennwortgeschützte Dienste ist.

- Lokale Checks: Nessus kann ab der Version 2.1 auch lokale Sicherheitsprüfungen auf den Systemen durchführen. Hierfür meldet sich Nessus über die Secure Shell (SSH) auf den Systemen an und führt dort die Überprüfungen lokal durch. Im Moment handelt es sich bei den Überprüfungen um die Analyse des Patchlevels für einige spezielle Betriebssysteme. Die aktuelle Liste der unterstützten Systeme finden Sie auf der Homepage.

Tipp

Wenn Sie Nessus zunächst nur einfach kennen lernen möchten, können Sie sich vom BSI die BSI Nessus-Live-CD BOSS (BSI OSS Security Suite) herunterladen. Diese enthält ein Knoppix mit vorbereitetem und modifiziertem Nessus. Sie finden weitere Informationen auf der BSI-Homepage (*http://www.bsi.de/produkte/boss/*).

Wenn Sie Nessus testen möchten, sollten Sie nicht das Nessus Ihrer Distribution verwenden. Die Entwicklung an Nessus schreitet zu schnell voran, als dass eine Distribution hiermit Schritt halten könnte. Laden Sie stattdessen Nessus von der Homepage als kompletten Installer: *http://www.nessus.org/download/*. Die Installation erfolgt dann ganz einfach mit dem Aufruf `sh nessus-installer-<version>.sh`. Der Installer prüft die Umgebung und weist Sie auf fehlende Software-Pakete hin. Nachdem Sie diese Pakete nachinstalliert haben, fragt der Installer Sie nach dem Installationsort und beginnt mit der Übersetzung und Installation. Anschließend erzeugen Sie

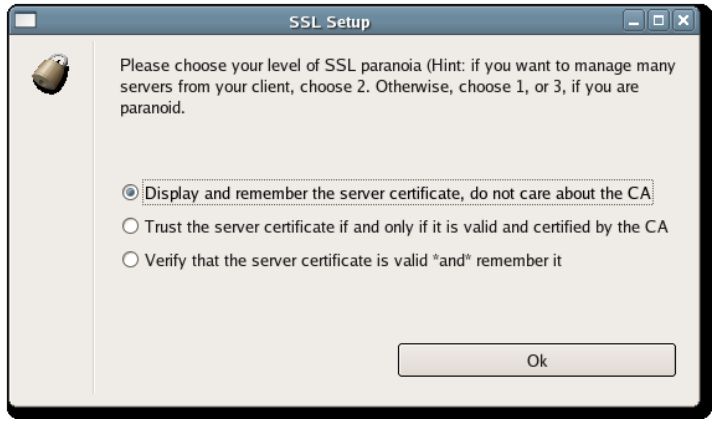


Abbildung 15.13: Die Verbindung zum Nessus-Server wird mit SSL geschützt. Bei der ersten Verbindung müssen Sie dem Zertifikat vertrauen.

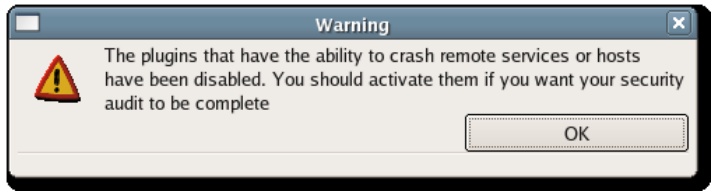


Abbildung 15.14: Nessus deaktiviert die gefährlichen Plugins per Default.

für den Nessus-Server mit dem Befehl `nessus-mkcert` ein Zertifikat. Die Kommunikation mit dem Nessus-Server `nessusd` wird mit SSL geschützt. Sie können für einen ersten Test die Default-Werte für die Zertifikatserzeugung übernehmen. Nun legen Sie mit `nessus-adduser` einen Benutzer an. Bei der Erzeugung des ersten Benutzers können Sie die Default-Werte übernehmen. Wählen Sie als Login einen beliebigen Namen (am einfachsten Ihren Linux-Login). Bei der *Authentification* wählen Sie `pass`. Wenn Sie nach den Regeln für den Benutzer gefragt werden, geben Sie direkt Strg-D ein. Damit beschränken Sie den Benutzer nicht. Als Kennwort geben Sie ein beliebiges Kennwort an. Jetzt können Sie den Nessus-Server `nessusd -D` starten. Der erste Start dauert ein wenig länger, da zunächst die Plugin-Datenbank initialisiert wird. Anschließend sollten Sie mit `nessus-update-plugins` prüfen, ob bereits neue Plugins veröffentlicht worden sind. Den Nessus-Client starten Sie mit `nessus`. Bei dem Start des Clients müssen Sie sich mit Ihrem Benutzernamen und dem gewählten Kennwort anmelden. Bei der ersten Anmeldung fragt der Client Sie, ob er dem Zertifikat des Nessus-Servers vertrauen soll (Abbildung 15.13). Wenn Sie sicher sind, dass kein Mann-in-der-Mitte-Angriff auf die Verbindung möglich ist, oder nachdem Sie das Zertifikat kontrolliert haben, wählen Sie `OK` und können den Server benutzen.

Per Default sind die gefährlichen Plugins direkt nach der Anmeldung deaktiviert (Abbildung 15.14).

Natürlich können Sie die Plugins einzeln an- und abschalten. Die grafische Oberfläche erleichtert die Wahl der Plugins mit Hilfe von Filtern, die Sie verwenden können, um nur die Plugins eines bestimmten Autors oder mit einem bestimmten Begriff in der Beschreibung oder im Namen anzuzeigen.

Haben Sie die Plugins für den Scan ausgewählt, können Sie auf der Registerkarte `Credentials` Login-Informationen für die lokalen Checks angeben. Nessus wird diese Informationen nutzen, um sich per SSH auf dem Zielsystem anzumelden. Die Registerkarte `Scan Options` bietet die Möglichkeit, den vorhergehenden Portscan zu optimieren und anstelle des eingebauten Scanners Nmap zu verwenden.

Auf der Registerkarte `Target` geben Sie das zu scannende Ziel ein. Hier können Sie sowohl IP-Adressen als auch Netze mit Netzmaske als auch DNS-Namen eingeben.

Die Registerkarte `Preferences` gibt Ihnen schließlich Konfigurationsmöglichkeiten für jeden Aspekt von Nessus inklusive der IDS-Evasion, Web-Traversal-Angriffen,

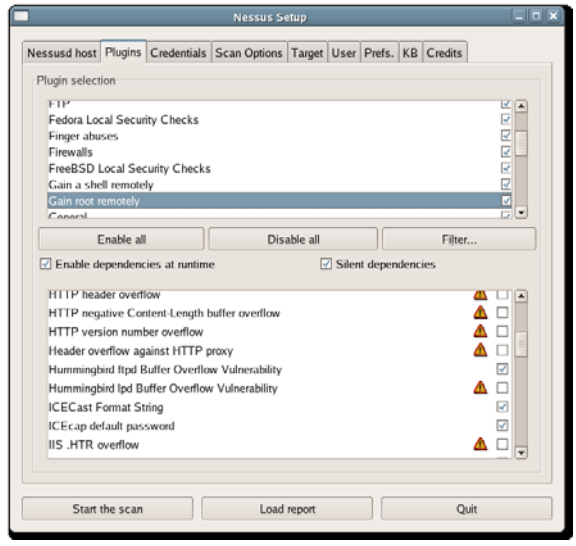


Abbildung 15.15: Sie können die Plugins bei Bedarf wieder aktivieren. Gefährliche Plugins tragen einen Warnhinweis mit Ausrufezeichen.

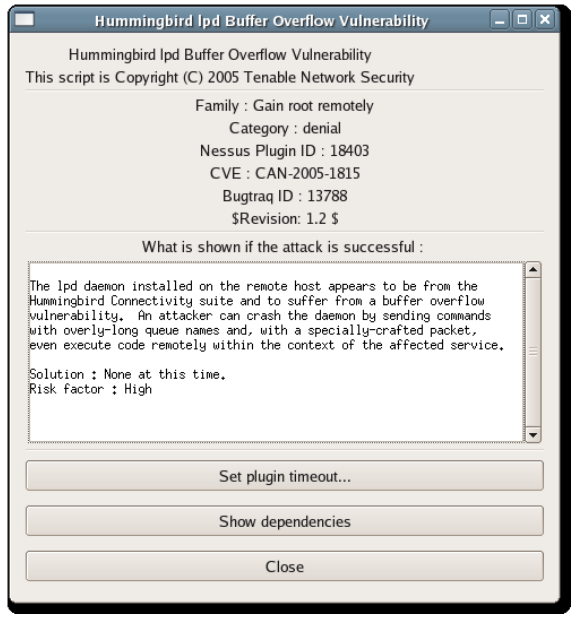


Abbildung 15.16: Durch Anklicken eines Plugins erhalten Sie weitere Informationen über das Plugin und seine Hintergründe und können es teilweise auch konfigurieren.

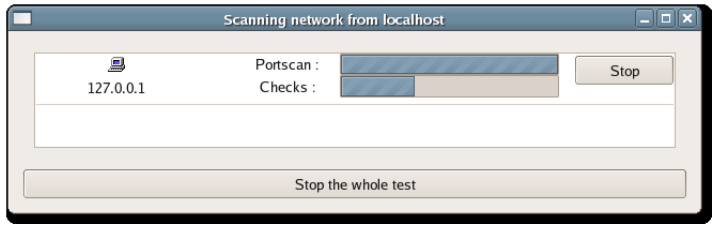


Abbildung 15.17: Während des Scans zeigt Nessus den Fortschritt an.

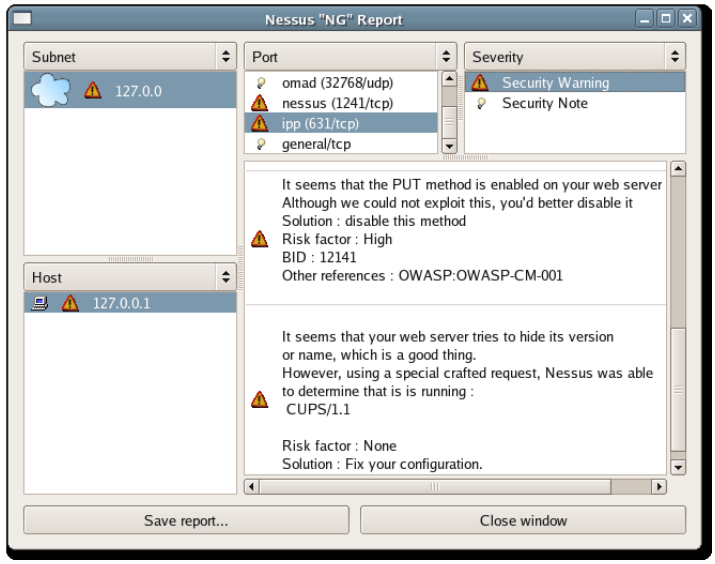


Abbildung 15.18: Nessus erzeugt einen ausführlichen Bericht mit den gefundenen Problemen.

Web-Mirroring etc. Für den ersten Scan sollten Sie diese Parameter nicht modifizieren.

Sehr interessant ist auch die Registerkarte KB. Hier verbirgt sich die Möglichkeit, das Ergebnis eines Scans in einer Datenbank (Knowledge Base) zu speichern. Spätere Scans können dann in Abhängigkeit von der Datenbank durchgeführt werden!

Haben Sie alles konfiguriert, starten Sie den Scan (Abbildung 15.17). Dieser Scan dauert nun je nach der Netzgeschwindigkeit, der ausgewählten Plugins und möglicher Firewalls wenige Minuten oder sogar Stunden.

Sobald Nessus mit dem Scan fertig ist, zeigt es in einem grafischen Browser den Bericht an. In der Abbildung 15.18 wurde nicht viel Erwähnenswertes gefunden. Dennoch sollten Sie in der Abbildung erkennen, dass Nessus die gefundenen Probleme beschreibt, Lösungen vorschlägt, Risikoabschätzungen abgibt und Referenzen

aufzählt. Sie können den Bericht nun als NBE, XML, HTML mit Grafiken und LaTeX abspeichern. Wenn Sie den Bericht in dem NBE-Format abspeichern, können Sie ihn später wieder in Nessus laden und auch in anderen Formaten sichern. Daher sollten Sie immer auch dieses Format wählen!

Ich hoffe, Sie haben mit dieser kurzen Einführung in Nessus einen ersten Einblick erhalten. Wenn Sie weitere Informationen über Nessus wünschen, finden Sie auf der Nessus-Homepage einige Artikel. Zusätzlich möchte ich Ihnen das englische Buch »Nessus Network Auditing« aus dem Syngress Verlag empfehlen. Es wurde von dem Nessus-Entwickler Renaud Deraison geschrieben.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

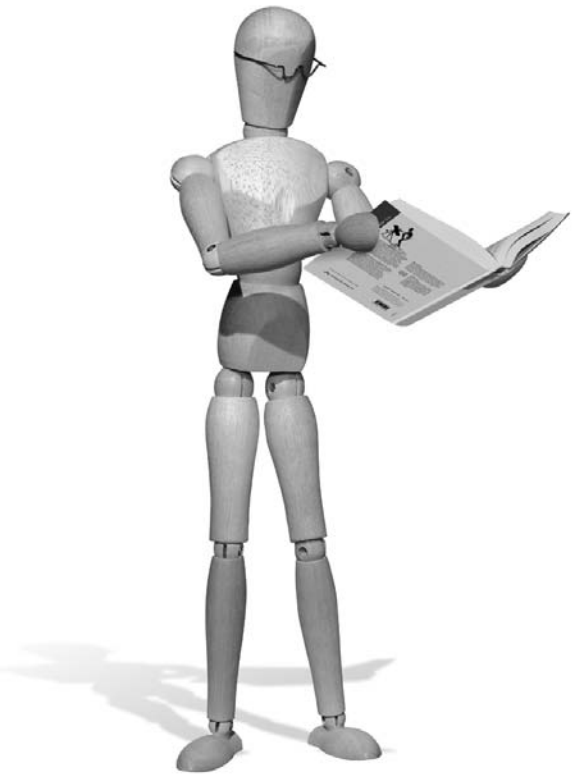
ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Teil V

Fortgeschrittene Konfiguration



16 Die Iptables-Standardtests

Dieses Kapitel führt alle Paketprüfungen auf, die in dem Linux-Kernel 2.6.14 und Iptables enthalten sind. Alle weiteren Paketprüfungen, die über Patch-O-Matic zur Verfügung gestellt werden, werden im Kapitel 18 besprochen.

Im Folgenden werden die verschiedenen Tests alphabetisch aufgeführt.

16.1 Eingebaute Tests

Iptables verfügt über eingebaute Tests und Erweiterungen. Während die Erweiterungen über Kernelmodule realisiert werden und immer mit der Option `-m <extension>` in jeder Regel aktiviert werden müssen, stehen die eingebauten Tests immer zur Verfügung. Die folgenden eingebauten Tests können Sie immer verwenden.

16.1.1 -p, –protocol

Dieser Test prüft das in dem Paket verwendete IP-Protokoll. Hier können Sie den Namen des Protokolls (`tcp`, `udp`, etc.) oder die Protokollnummer verwenden. Die Definition der Protokollnamen erfolgt in der Datei `/etc/protocols`. Wenn Sie den Test negieren möchten, können Sie das Ausrufezeichen dem Protokoll voranstellen: `--protocol ! tcp`.

16.1.2 -s, –source

Dieser Test prüft die Quell-IP-Adresse des Pakets. Dies kann eine IP-Adresse, ein Netzwerk oder ein DNS-Name sein. Bei der Angabe des Netzwerks können Sie die Netzmaske ausschreiben (`255.255.255.0`) oder die CIDR--Notation (`/24`) verwenden. Wenn Sie einen DNS-Namen verwenden, wird Iptables den DNS-Namen in dem Moment, in dem Sie die Regel hinzufügen, auflösen und anstelle des DNS-Namens die aufgelöste IP-Adresse nutzen. Dynamische DNS-Namen, deren IP-Adresse sich ändert, werden nicht unterstützt.

16.1.3 -d, –destination

Hiermit prüfen Sie die Ziel-IP-Adresse. Im Weiteren gelten die Beschränkungen wie bei der Quell-IP-Adresse.

16.1.4 -i, –in-interface

Hiermit können Sie prüfen, über welche Netzwerkkarte das Paket Ihren Rechner erreicht hat. Diesen Test können Sie nur in den `PREROUTING-`, `INPUT-` und `FORWARD-`Ketten benutzen. Die Verwendung in den `OUTPUT-` oder `POSTROUTING`-Ketten ist nicht erlaubt.

Die Netzwerkkarte muss in dem Moment, in dem Sie die Regel hinzufügen, noch nicht existieren. Wenn Sie mehrere Netzwerkkarten in einer Regel testen möchten, können Sie das `+` als Wildcard nutzen. Ein `eth+` trifft dann auf alle Ethernet-Netzwerkkarten zu.

16.1.5 -o, –out-interface

Hiermit können Sie prüfen, über welche Netzwerkkarte ein Paket den Rechner verlässt. Diesen Test dürfen Sie nur in den `FORWARD-`, `OUTPUT-` und `POSTROUTING`-Ketten verwenden. Ansonsten gelten die gleichen Einschränkungen wie oben.

16.1.6 -f, –fragment

Hiermit prüfen Sie, ob es sich bei einem fragmentierten Paket um das zweite oder ein weiteres Fragment handelt. Da Iptables ab dem zweiten Fragment keinen Zugriff mehr auf die Informationen des Transport-Protokolls hat, können Sie hiermit diese Fragmente herausfiltern und bei Bedarf zulassen.

Achtung

Da sich fragmentierte Pakete nur schlecht filtern lassen, sollten grundsätzlich alle Pakete vor der Filterung defragmentiert werden. Während Sie auf alten Linux-Kerneln dies speziell anschalten müssen, ist diese Funktion auf dem Linux-Kernel 2.4. und 2.6 automatisch aktiv, sobald Sie Connection Tracking nutzen. Sobald das Kernelmodul `ip_conntrack` geladen wurde, werden alle Pakete defragmentiert!

16.2 TCP-Tests

Wenn es sich beim Paket um ein TCP-Paket handelt und Sie dies mit der Option `-p tcp` in der Regel prüfen, können Sie weitere Prüfungen des TCP-Headers vornehmen. Dabei können Sie die Ports, die TCP-Flags und die TCP-Optionen prüfen.

16.2.1 sourceport

Mit der Option `--sourceport` (oder auch `--sport`) können Sie den Quellport prüfen. Hier können Sie einen Port oder einen Portbereich (`lt;port>:<port>`) angeben. Mehrere verschiedene Ports können Sie nicht angeben. Hierfür benötigen Sie den `multiport`-Test.

16.2.2 destinationport

Mit der Option `--destinationport` (oder auch `--dport`) können Sie den Zielport prüfen. Hier können Sie einen Port oder einen Portbereich (`lt;port>:<port>`) angeben. Mehrere verschiedene Ports können Sie nicht angeben. Hierfür benötigen Sie den `multiport`-Test.

16.2.3 tcp-flags

Mit dieser Option können Sie jedes TCP-Flag prüfen. Ingesamt gibt es sechs verschiedene: `SYN`, `ACK`, `FIN`, `RST`, `URG` und `PSH`. Dieser Test unterstützt auch noch `NONE` und `ALL`. Um die Flags zu testen, müssen Sie zunächst eine Maske mit den Flags definieren, die Sie prüfen möchten, und geben dann, durch ein Leerzeichen getrennt, die Flags an, die gesetzt sein müssen. Wenn Sie zum Beispiel prüfen möchtem, ob das SYN-Flag gesetzt ist, aber das RST- und ACK-Flag nicht gesetzt sind, verwenden Sie: `--tcp-flags SYN,ACK,RST SYN`. Dieser Test betrachtet alle drei Flags (`SYN`, `ACK` und `RST`). Aber nur `SYN` darf gesetzt sein. Der Zustand der anderen Flags ist unerheblich.

Tipp

Das Netzwerk-Scan-Werkzeug hping2 (*http://www.hping.org*) verwendet per Default TCP-Pakete, in denen kein einziges Flag gesetzt ist. Wenn Sie diese Pakete erkennen möchten, können Sie den folgenden Test nutzen:

```
$IPTABLES -A INPUT -p tcp --tcp-flags ALL NONE -j LOG \
  --log-prefix "Hping2 Scan:"
```

16.2.4 syn

Dieser Test (`--syn`) ist eine Kurzform für `--tcp-flags SYN,ACK,RST SYN` und prüft, ob ein Paket das erste SYN-Paket in einer Verbindung ist. Wenn Sie diesen Test negieren möchten, setzen Sie ein Ausrufezeichen vor ihn.

16.2.5 tcp-options

Das TCP-Protokoll unterstützt verschiedene Optionen, die das Verhalten des TCP-Protokolls beeinflussen. Eine dieser Optionen ist zum Beispiel die Maximum Segment Size (MSS, siehe Abschnitt 16.31). Mit diesem Test können Sie prüfen, ob eine bestimmte Option gesetzt ist.

16.3 UDP-Tests

Das UDP-Protokoll verfügt nicht über so viele Informationen wie das TCP-Protokoll. Daher können Sie hier nur die Ports testen.

16.3.1 sourceport

Mit der Option `--sourceport` (oder auch `--sport`) können Sie den Quellport prüfen. Hier können Sie einen Port oder einen Portbereich (`lt;port>:<port>`) angeben. Mehrere verschiedene Ports können Sie nicht angeben. Hierfür benötigen Sie den `multiport`-Test.

16.3.2 destinationport

Mit der Option `--destinationport` (oder auch `--dport`) können Sie den Zielport prüfen. Hier können Sie einen Port oder einen Portbereich (`lt;port>:<port>`) angeben. Mehrere verschiedene Ports können Sie nicht angeben. Hierfür benötigen Sie den `multiport`-Test.

16.4 ICMP-Tests

Das ICMP-Protokoll besitzt keine Ports. Bei ICMP werden die verschiedenen Nachrichten durch Typ und Code unterschieden. Damit auch Sie prüfen können, um was für eine ICMP-Nachricht es sich handelt, unterstützt Iptables für ICMP-Pakete den Test `--icmp-type`. Die verschiedenen ICMP-Typen, die Sie testen können, zeigt der Iptables-Befehl an:

```
$ iptables -p icmp -h
...
ICMP v1.3.0 options:
 --icmp-type [!] typename       match icmp type
                                (or numeric type or type/code)

Valid ICMP Types:
any
echo-reply (pong)
destination-unreachable
   network-unreachable
   host-unreachable
   protocol-unreachable
   port-unreachable
   fragmentation-needed
   source-route-failed
   network-unknown
   host-unknown
   network-prohibited
   host-prohibited
   TOS-network-unreachable
   TOS-host-unreachable
   communication-prohibited
```

```
   host-precedence-violation
   precedence-cutoff
source-quench
redirect
   network-redirect
   host-redirect
   TOS-network-redirect
   TOS-host-redirect
echo-request (ping)
router-advertisement
router-solicitation
time-exceeded (ttl-exceeded)
   ttl-zero-during-transit
   ttl-zero-during-reassembly
parameter-problem
   ip-header-bad
   required-option-missing
timestamp-request
timestamp-reply
address-mask-request
address-mask-reply
```

Die Filterung des ICMP-Protokolls wird ausführlich im Kapitel 34 besprochen.

16.5 addrtype

Der Routing-Code des Linux-Kernels kategorisiert jede IP-Adresse im Netzwerkstack. Dieser Test kann diese Kategorien testen und entsprechend Pakete verwerfen oder protokollieren. Die folgenden Kategorien werden von Linux unterstützt: `UNSPEC`, `UNICAST`, `LOCAL`, `BROADCAST`, `ANYCAST`, `MULTICAST`, `BLACKHOLE`, `UNREACHABLE`, `PROHIBIT`, `THROW`, `NAT` und `XRESOLVE`. Leider existiert kaum Dokumentation, in der die Kategorien erläutert werden.

Sie können sowohl die Quell-IP-Adresse als auch die Ziel-IP-Adresse testen:

```
-m addrtype --src-type <type>
-m addrtype --dst-type <type>
```

Ich kenne keine sinnvolle Verwendung für diesen Test.

16.6 ah

Mit diesem Test können Sie die Security-Parameter-Indices (SPI) des IPsec-AH-Protokolls testen. Da der Security-Parameter-Index üblicherweise dynamisch von dem IKE-Daemon ausgehandelt wird, ist eine statische Prüfung nicht besonders

sinnvoll, außer Sie verwenden manuell definierte IPsec-AH-Verbindungen (z.B. mit `setkey`).

```
-m ah --ahspi [!] <spi>[:<spi>]
```

16.7 comment

Dies ist kein wirklicher Test, da Sie hiermit keine Eigenschaft des Pakets prüfen können. Vielmehr können Sie einen Kommentar zu einer Regel hinzufügen. Damit können Sie nun die Regeln selbst dokumentieren, so dass bei einer späteren Auflistung der Regeln mit `iptables -vnL` die Kommentare angezeigt werden. Der Kommentar darf maximal 256 Zeichen lang sein.

```
-m comment --comment "Kommentar"
```

16.8 connbytes

Mit diesem Test können Sie prüfen, wie viele Pakete oder Bytes in einer Verbindung bereits übertragen wurden. So können Sie langlebige Downloads mit einer geringeren Priorität versehen, so dass sie den restlichen Verkehr nicht negativ beeinflussen. Sie können mit diesem Test die übertragenen Pakete oder Bytes in einer oder beiden Richtungen analysieren. Außerdem können Sie die durchschnittliche Paketgröße testen.

Dieser Test verfügt über drei zusätzliche Optionen:

- `[!] --connbytes <from>:[<to>]`: Hiermit prüfen Sie, ob die übertragenen Daten sich zwischen `from` und `to` befinden. Wenn Sie `to` nicht angeben, ist die obere Grenze nicht gesetzt.
- `--connbytes-dir [original|reply|both]`: Hiermit geben Sie die zu überwachenden Richtungen an.
- `--connbytes-mode [packets|bytes|avgpkt]`: Hiermit wählen Sie den Modus aus. Entweder zählt Connbytes die übertragenen Pakete oder Bytes, oder Connbytes ermittelt die durchschnittliche Paketgröße.

```
-m connbytes --connbytes 100000: --connbytes-dir both --connbytes-mode bytes
```

Tipp

Da die Zähler 64-Bit-Zähler sind, ist ein Überlauf der Zähler sehr unwahrscheinlich. Sie können hiermit sehr langlebige Verbindungen überwachen.

16.9 connmark

Verbindungen, die Sie in der NAT-Tabelle mit dem Target `CONNMARK` markiert haben, können Sie hiermit testen. Dazu können Sie entweder exakt die Markierung angeben oder auch zusätzlich noch eine Maske definieren. Diese Maske wird vor dem Test mit der Markierung der Verbindung Und-verknüpft.

```
-m connmark --mark <markierung>[/<maske>]
```

16.10 conntrack

Dieses Modul gibt Ihnen erweiterten Zugriff auf die internen Werte der Connection Tracking-Tabelle. Hiermit können Sie diese Werte in Regeln ausnutzen. Sie können auf diese Weise prüfen, welchen Zustand (INVALID RELATED, NEW, SNAT, DNAT, UNTRACKED), welche originale und welche genattete Adresse die dazugehörige Verbindung in der Zustandstabelle aufweist.

Da mir keine sinnvolle Anwendung bekannt ist, verweise ich den interessierten Leser auf die `iptables(8)`-Manpage.

16.11 dccp

Das Datagram Congestion Control Protocol (DCCP) ist ein nachrichtenorientiertes Transport-Protokoll. Es implementiert wie TCP einen Datenfluss, aber bietet keine Übertragungssicherheit. DCCP befindet sich aktuell in der Entwicklung und wird meines Wissens noch nicht produktiv eingesetzt.

Mit diesem Test können Sie das DCCP-Protokoll testen. Der Test unterstützt die folgenden Optionen:

- `--source-port`: Prüft den Quellport.
- `--destination-port`: Prüft den Zielport.
- `--dccp-types`: DCCP unterstützt die folgenden Pakettypen: `REQUEST`, `RESPONSE`, `DATA`, `ACK`, `DATAACK`, `CLOSEREQ`, `CLOSE`, `RESET`, `SYNC`, `SYNCACK` und `INVALID`.
- `--dccp-option`: Hiermit können Sie prüfen, ob eine numerische DCCP-Option gesetzt ist.

16.12 dscp

Das 6 Bit lange DiffServ-Code-Point-(DSCP-)Feld befindet sich in dem TOS-Feld des IP-Headers. DSCP hat TOS in den aktuellen IP-Protokoll-Standards abgelöst.

Sie können entweder den Wert numerisch oder durch Angabe der DSCP-Klasse testen:

```
-m dscp --dscp <nummer>
-m dscp --dscp-class <klasse>
```

16.13 ecn

Mit diesem Test können Sie prüfen, ob die Explicit Congestion Notification-(ECN-) Bits in dem Paket gesetzt sind. Mit den folgenden Optionen können Sie die einzelnen Bits testen:

- `-m ecn --ecn-tcp-cwr`: Ist das Congestion-Window-Received-Bit gesetzt?
- `-m ecn --ecn-tcp-ece`: Ist das ECN-Echo-Bit gesetzt?
- `-m ecn --ip-ect <nummer>`: Ist ein ECN-Capabable-Transport-Bit gesetzt?

Weitere Informationen über ECN und die verwendeten Bits im IP- und TCP-Header finden Sie auf *http://www.icir.org/floyd/ecn.html*. Eine sinnvolle Anwendung ist mir unbekannt, da Sie die ECN-Bits entfernen können, ohne vorher ihr Vorhandensein zu prüfen.

16.14 esp

Hiermit können Sie ähnlich dem `ah`-Test die Security-Parameter-Indices des IPsec-ESP-Protokolls testen. Da auch diese dynamisch ausgehandelt werden, ist die Anwendung nicht sinnvoll.

```
-m esp --espspi [!] <spi>[:<spi>]
```

16.15 hashlimit

Dieser sehr interessante Test ähnelt dem `limit`-Test. Wenn Sie den `limit`-Test noch nicht kennen, lesen Sie erst dort nach, und kehren Sie anschließend hierher zurück.

Der `hashlimit`-Test ermöglicht Ihnen im Gegensatz zum allgemeinen Limit-Test die Definition von Grenzwerten in Abhängigkeit von der Ziel/Quell-IP-Adresse und des -Ports.

Der Test besitzt eigene Zähler für jede IP-Adresse und/oder jeden Port und nicht nur einen Zähler für die gesamte Regel.

Der Test unterstützt die folgenden Optionen:

- `--hashlimit <rate>`: siehe `limit`.
- `--hashlimit-burst <burst>`: siehe `limit`.
- `--hashlimit-mode destip|srcip|dstport|srcport`: Hashlimit-Modus.
- `--hashlimit-name <name>`: Dies erzeugt einen Eintrag in `/proc/net/ipt_hashlimit/<name>` für diese Regel.
- `--hashlimit-htable-size <num>`: Größe der Hash-Tabelle in Buckets.
- `--hashlimit-htable-max <max>`: Maximale Anzahl der Einträge in der Hash-Tabelle.

- `--hashlimit-htable-gcinterval <intvl>`: Garbage Collector Interval (ms).
- `--hashlimit-htable-expire <ttl>`: Lebensdauer (ms) der Einträge in der Hash-Tabelle.

Mit diesem Test lassen sich zum Beispiel die SSH-Brute-Force-Angriffe des letzten Jahres hervorragend abwehren:

```
$IPTABLES -A INPUT -m tcp -p tcp --dport 22 \
  -m hashlimit --hashlimit 1/min --hashlimit-mode srcip
  --hashlimit-name ssh -m state --state NEW -j ACCEPT
```

Diese Regel akzeptiert nur eine SSH-Verbindungsanfrage pro Minute und pro Quell-IP-Adresse. Allerdings kann natürlich ein Angreifer auch einen DoS ausführen, falls er die IP-Adresse erraten kann, von der aus Sie sich mit dem System verbinden möchten. Er spooft dann einfach Ihre IP-Adresse und führt häufige Verbindungsaufbauten durch!

Achtung

Die Manpage des Iptables-Kommandos hat hier in einigen Versionen einen Fehler und behauptet, dieser Test könnte nur die Ziel-IP-Adresse mit einer Beschränkung belegen. Testen Sie Ihren Kernel mit:

```
$ iptables -m hashlimit -h
hashlimit v1.3.0 options:
--hashlimit <avg>               max average match rate
                                [Packets per second unless followed by
                                /sec /minute /hour /day postfixes]
--hashlimit-mode <mode>         mode is a comma-separated list of
                                        dstip,srcip,dstport,srcport
--hashlimit-name <name>         name for /proc/net/ipt_hashlimit/
[--hashlimit-burst <num>]       number to match in a burst, default 5
[--hashlimit-htable-size <num>] number of hashtable buckets
[--hashlimit-htable-max <num>]  number of hashtable entries
[--hashlimit-htable-gcinterval] interval between garbage collection runs
[--hashlimit-htable-expire]     after which time are idle entries expired?
```

16.16 helper

Dieser Test prüft, ob ein Paket durch ein bestimmtes Conntrack-Helfermodul erkannt wurde. Hierzu geben Sie lediglich den Namen des Helfermoduls an. Um alle FTP-Pakete (Control- und Data-Connection) zu erkennen, können Sie folgenden Ausdruck verwenden: `-m helper --helper ftp`. Wenn Sie von den Default-Ports abgewichen sind, können Sie den Port mit angeben: `-m helper --helper ftp-2121`. Andere Helfermodule arbeiten genauso.

Damit können Sie zum Beispiel RELATED-Pakete nur akzeptieren, wenn es sich gleichzeitig um Pakete einer FTP-Verbindung handelt. ICMP-Fehlermeldungen oder IRC-Datenverbindungen werden von der folgenden Regel nicht akzeptiert:

```
$IPTABLES -A FORWARD -m state --state RELATED -m helper --helper ftp -j ACCEPT
```

16.17 iprange

In vielen Fällen möchte man prüfen, ob eine IP-Adresse sich innerhalb eines bestimmten Bereichs befindet. Jedoch kann in vielen Fällen nicht ein Netzwerk mit Subnetzmaske verwendet werden, da der Bereich nicht auf Netzwerkgrenzen beginnt und endet. Dann können Sie diesen Test verwenden. Sie können die Quell- und Ziel-IP-Adresse prüfen:

```
-m iprange [!] --src-range <ip>-<ip>
-m iprange [!] --dst-range <ip>-<ip>
```

Wenn Ihr DHCP-Server zum Beispiel im Bereich von 192.168.0.100-150 dynamische IP-Adressen verteilt und Sie Regeln für die dynamischen Clients definieren möchten, können Sie folgenden Ausdruck verwenden: `-m iprange --src-range 192.168.0.100-192.168.0.150`.

16.18 length

Dieser Test prüft einfach die Länge eines Pakets. Sie können einen spezifischen Wert oder einen Bereich angeben:

```
-m length --length <länge>[:<länge>]
```

Damit ist es zum Beispiel möglich, ungewöhnlich große Ping-Pakete zu erkennen, die auf einen versteckten Kommunikationskanal hinweisen:

```
$IPTABLES -A FORWARD -p icmp --icmp-type echo-request -m length --length
  100:1500 -j LOG --log-prefix "Unusual Ping Size: "
```

16.19 limit

Dies ist der klassische Limit-Test des Iptables-Kommandos. Dieser Test ist in modernen Linux-Kerneln durch den `hashlimit`-Test im Wesentlichen abgelöst worden. Eine Regel, die diesen Test verwendet, trifft so lange zu, bis das Limit für die Regel erreicht wurde. Dabei besitzt die Regel nur einen einzigen Zähler, der unabhängig von den verwendeten IP-Adressen und -Ports die Ereignisse zählt. Hashlimit kann hier für jede IP-Adresse und jeden Port eigene Zähler verwalten. Dieser Test verfügt über zwei Optionen:

- `--limit <rate>`: Dies ist die maximale Paketrate. Sie können die Einheit in `/second`, `/minute`, `/hour` oder `/day` angeben. Default ist `3/hour`.

- `--limit-burst <rate>`: Hiermit können Sie einen initialen Schwellenwert definieren, der erst erreicht werden muss, bevor das Limit greift. Der Default-Wert ist 5.

Dieser Test eignet sich speziell für die Beschränkung der Protokollierung einzelner Pakete.

```
$IPTABLES -A FORWARD -p icmp --icmp-type echo-request \
  -m limit --limit 1/minute  -j LOG --log-prefix "Ping-Paket: "
```

16.20 mac

Mit diesem Test können Sie die Quell-MAC-Adresse testen. So können Sie sich vor ARP-Spoofing schützen, da Sie nur Pakete annehmen, die von einer bestimmten Quell-IP- und -MAC-Adresse stammen.

```
-m mac --mac-source <XX:XX:XX:XX:XX:XX>
```

Tipp

Wenn Sie diese Überprüfung für viele Systeme durchführen möchten, sollten Sie sich den `ipset`-Befehl mit der `macipmap` genauer ansehen (siehe Kapitel 25).

16.21 mark

Sie können in der Mangle-Tabelle Pakete mit dem `MARK`-Target markieren. Diese Firewall-Markierung können Sie mit diesem Test prüfen. Hierzu können Sie die Markierung genau angeben oder zusätzlich auch noch eine Maske definieren, die vor der Überprüfung mit der Markierung der Pakete Und-verknüpft wird.

```
-m mark --mark <markierung>[/<maske>]
```

Achtung

Die Paket-Markierung ist nur auf dem lokalen System gültig. Sobald das Paket das System verlässt, ist die Markierung verloren.

16.22 multiport

Diese Option erlaubt es Ihnen, mehrere Quell- oder Zielports in einer Regel anzugeben. Normalerweise erlaubt Iptables nur die Angabe eines Ports oder eines Port-Bereichs. Aktuelle Kernel (≥ 2.6.11) können bei dieser Option auch Port-Bereiche verwenden. Insgesamt dürfen Sie 15 Ports angeben. Ein Port-Bereich zählt als zwei Ports.

- `--source-ports [!] <port>[,<port>[,<port>:<port>]]`
- `--destination-ports [!] <port>[,<port>[,<port>:<port>]]`
- `--ports [!] <port>[,<port>[,<port>:<port>]]`

Mit diesem Test können Sie mehrere Regeln in einer zusammenfassen:

```
$IPTABLES -A FORWARD -p tcp -m multiport \
  --destination-ports 21,22,25,80,443 -j ACCEPT
```

16.23 owner

Dieser Test kann nur in der OUTPUT-Kette angewendet werden, da der Linux-Kernel nur den Erzeuger lokaler Pakete ermitteln kann. Mit diesem Test können Sie prüfen, welcher Benutzer (`--uid-owner <uid>`), welche Gruppe (`--gid-owner <gid>`), welcher Prozess (`--pid-owner <pid>`), welche Sitzung (`--sid-owner <sid>`) oder welches Kommando (`--cmd-owner <cmd>`) ein Paket erzeugt hat. Leider funktionieren die letzten drei Funktionen aktuell nicht auf Mehrprozessorsystemen.

Damit können Sie aber dem Webserver verbieten, selbst Verbindungen aufzubauen:

```
$IPTABLES -A OUTPUT -m owner --cmd-owner httpd -j REJECT
```

16.24 physdev

Diese Option wird beim Linux-Kernel 2.6 verwendet, um die in einer Bridge verwendeten Netzwerkkarten zu erkennen und in einer Regel zu testen. Die genaue Verwendung dieses Tests wird daher in dem entsprechenden Kapitel erläutert und soll hier nicht wiederholt werden (siehe Kapitel 30).

16.25 pkttype

Dieser Test prüft den Pakettyp der Schicht 2. Sie können damit prüfen, ob es sich um ein `unicast`-, `broadcast`- oder ein `multicast`-Paket handelt.

Mit diesem Test können Sie alle lokalen Broadcast-Pakete einfach auf Ihrer Firewall verwerfen.

```
$IPTABLES -A INPUT -m pkttype --pkt-type broadcast -j DROP
```

16.26 realm

Dynamische Routing-Protokolle wie das Border-Gateway-Protokoll (BGP) verwenden Routing Realms für die Konfiguration. Dieser Test kann prüfen, ob das Paket zu einem bestimmten Realm gehört. Wenn Sie auf Ihrem System kein BGP einsetzen, benötigen Sie diesen Test nicht.

```
-m realm --realm [!] <realm>[<maske>]
```

16.27 recent

Dieser Test erlaubt es Ihnen, dynamisch eine Liste der gerade aktiven Quell-IP-Adressen zu erzeugen und in Ihren Regeln zu testen. Der Test hat die folgenden Optionen:

- `--name <name>`: Sie können verschiedene Listen für unterschiedliche Zwecke anlegen. Wenn Sie den Namen nicht angeben, wird die `DEFAULT`-Liste verwendet.
- `[!] --set`: Dies fügt die IP-Adresse zur Liste hinzu. Falls die IP-Adresse bereits in der Liste enthalten ist, wird der Eintrag aktualisiert. Dieser Test ist immer wahr, außer Sie geben das Ausrufezeichen an.
- `[!] --rcheck`: Dies prüft, ob die aktuelle IP-Adresse in der Liste enthalten ist.
- `[!] --update`: Identisch mit `--rcheck`, jedoch wird zusätzlich der Eintrag aktualisiert.
- `[!] --remove`: Hiermit entfernen Sie eine IP-Adresse aus der Liste. Falls die IP-Adresse nicht in der Liste vorhanden ist, trifft die Regel nicht zu.
- `[!] --seconds <sekunden>`: Diese Option können Sie gemeinsam mit `--rcheck` oder `--update` verwenden. Diese Optionen treffen dann nur zu, wenn die IP-Adresse innerhalb der angegebenen Zeitdauer gesehen wurde.
- `[!] --hitcount <treffer>`: Diese Option kann gemeinsam mit `--rcheck` und `--update` verwendet werden und prüft, ob die IP-Adresse bereits so häufig gesehen wurde. Mit `--seconds` können Sie zusätzlich den Zeitraum einschränken.
- `--rttl`: Hiermit prüfen Sie, ob der TTL-Wert des aktuellen Pakets identisch mit dem Paket ist, das mit `--set` hinzugefügt wurde.

Das Modul legt in `/proc/net/ipt_recent/<name>` Dateien an, die auch direkt gelesen und geschrieben werden können. Um eine IP-Adresse hinzuzufügen, können Sie diese in die Datei schreiben:

```
echo <ip> > /proc/net/ipt_recent/<name>
```

Genauso können Sie auch eine IP-Adresse entfernen:

```
echo -<ip> > /proc/net/ipt_recent/<name>
```

Um die gesamte Liste zu löschen, schreiben Sie das Wort `clear` in die entsprechende Datei.

Das Modul `ipt_recent` unterstützt beim Laden auch noch einige Optionen. Die Klammern geben die Default-Werte an:

- `ip_list_tot`: Anzahl der IP-Adressen pro Liste (100).
- `ip_pkt_list_tot`: Anzahl der Pakete pro IP-Adresse (20).
- `ip_list_hash_size`: Größe der Hash-Tabelle (0, Berechnung in Abhängigkeit von der `ip_list_tot`).
- `ip_list_perms`: Rechte der Dateien in `/proc/net/ipt_recent/*` (0644).
- `debug`: Debug-Informationen (0).

Um diese Optionen zu setzen, müssen Sie das Modul laden, bevor Sie in Ihren Regeln den Test verwenden:

```
# modprobe ipt_recent ip_list_tot=200
```

Dieses Modul können Sie nun einsetzen, um sich in Ihren Regeln spezifische IP-Adressen zu merken und zusätzliche Regeln auf diese IP-Adressen anzuwenden.

Um zum Beispiel Brute-Force-SSH-Angriffe abzuwehren, könnten Sie anstelle des `hashlimit`-Tests auch die folgenden beiden Regeln verwenden:

```
iptables -I INPUT -p tcp --dport 22 -m state --state NEW \
  -m recent --name SSH --set

iptables -I INPUT -p tcp --dport 22 -m state --state NEW \
-m recent --name SSH --update --seconds 60 --hitcount 4 -j DROP
```

Die erste Regel fügt jede neue Quell-IP-Adresse, die eine SSH-Verbindung öffnet, der Liste `SSH` hinzu. Die zweite Regel prüft, ob von einer IP-Adresse innerhalb der letzten 60 Sekunden 4 Verbindungsanfragen erhalten wurden, und verwirft alle weiteren Anfragen. Sie können diese Regeln einsetzen, wenn der `hashlimit`-Test auf Ihrem Kernel nicht zur Verfügung steht.

16.28 sctp

Das Stream Control Transmission Protocol (SCTP, RFC 2960) ist ein Protokoll, das ähnlich wie TCP die Datenübertragung garantiert und verlorene oder beschädigte Pakete automatisch erneut sendet. Im Gegensatz zu TCP unterstützt SCTP mehrere Streams in einer Verbindung und Multihoming. Multihoming bedeutet, dass ein Kommunikationsendpunkt unter verschiedenen IP-Adressen erreicht werden kann.

SCTP wird aktuell von MPI-Parallel-Programmen und Telephonie-Software genutzt.

Mit diesem Test können Sie die Eigenschaften des Protokolls testen. Hierzu haben Sie die folgenden Optionen:

- `--source-port [!] <port>[:<port>]`

- `--destination-port [!] <port>[:<port>]`
- `--chunk-types [!] all|any|only <chunktype>[:<flags>]`

16.29 state

Dieser Test ermittelt den Zustand der Verbindung, zu der dieses Paket gehört. Die folgenden Zustände sind möglich:

- `NEW`: Das Paket gehört zu einer neuen Verbindung.
- `ESTABLISHED`: Das Paket gehört zu einer aufgebauten Verbindung.
- `RELATED`: Das Paket bezieht sich auf eine aufgebaute Verbindung (z.B. ICMP-Fehlernachricht).
- `INVALID`: Der Zustand des Pakets kann nicht ermittelt werden (z.B. ICMP-Fehlernachricht, die sich nicht auf eine bekannte Verbindung bezieht).

Wenn Ihr Kernel über die Raw-Tabelle verfügt, existiert zusätzlich noch der Zustand `UNTRACKED`. Der Zustand dieser Verbindung wird von dem Kernel nicht überwacht. Weitere Informationen finden Sie in Abschnitt 5.5 und in Kapitel 19.

16.30 string

Ab dem Kernel 2.6.14 ist der `string`-Test im Linux-Kernel fest verfügbar. Leider ist der entsprechende Code weder im aktuellen `iptables`-Kommando (1.3.3) noch im Patch-O-Matic verfügbar.

Ich gehe jedoch davon aus, dass zukünftige Versionen diesen Code enthalten werden. Ich vermute, dass die folgende Syntax verwendet werden wird:

- `--from <offset>`: Suche ab diesem Offset im Paket.
- `--to <offset>`: Suche bis zu diesem Offset im Paket.
- `--algo <algorithmus>`: Der Kernel 2.6.14 unterstützt im Moment drei verschiedene Algorithmen: Boyer-Moore (BM), Knuth-Morris-Pratt (KMP) und Finite-State-Machine (FSM).
- `--string <muster>`: Suche diese Zeichenkette.

16.31 tcpmss

Hiermit können Sie prüfen, ob in dem Paket eine Maximum Segment Size (MSS) gesetzt wurde. Dieser Test ist nur bei TCP-Paketen erlaubt. Sie können exakt einen Wert oder einen Bereich prüfen.

```
-m tcpmss [!] --mss <wert>[:<wert>]
```

Dieser Test ist nicht besonders hilfreich. Ich empfehle, bei Problemen mit der MSS grundsätzlich in allen Paketen die MSS zu ändern. Hierzu können Sie das `MSS`-Target einsetzen (siehe Abschnitt 17.21).

16.32 tos

Dieser Test ermöglicht die Prüfung des Type-of-Service-Wertes eines Pakets. Meines Erachtens gibt es keine wirklich sinnvolle Anwendung.

```
-m tos --tos <tos>
```

Sie können die folgenden Werte testen:

```
$ iptables -m tos -h
TOS match v1.3.0 options:
[!] --tos value                 Match Type of Service field from one of the
                                following numeric or descriptive values:
                                     Minimize-Delay 16 (0x10)
                                     Maximize-Throughput 8 (0x08)
                                     Maximize-Reliability 4 (0x04)
                                     Minimize-Cost 2 (0x02)
                                     Normal-Service 0 (0x00)
```

16.33 ttl

Mit dem `ttl`-Test können Sie den TTL-Wert eines Pakets prüfen. Sie können den genauen Wert testen oder prüfen, ob der Wert größer oder kleiner einem Vergleichswert ist. Hiermit können Sie zum Beispiel Windows-Systeme im lokalen Netz von Linux-Systemen unterscheiden, da Windows-Systeme eine andere initiale TTL verwenden. Es gibt aber bessere Methoden (z.B. `osf` in Patch-O-Matic, siehe Abschnitt 18.3.8).

```
-m ttl --ttl-eq <ttl>  # gleich
-m ttl --ttl-gt <ttl>  # größer
-m ttl --ttl-lt <ttl>  # kleiner
```

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

17 Alle Standardziele

Dieses Kapitel führt alle Ziele (Aktionen, Targets) auf, die in dem Linux-Kernel 2.6.14 enthalten sind. Alle weiteren Ziele, die über Patch-O-Matic zur Verfügung gestellt werden, werden im Kapitel besprochen (siehe Kapitel 18).

Im Folgenden werden die verschiedenen Ziele alphabetisch aufgeführt. Da einzelne Ziele nur in bestimmten Tabellen und Ketten erlaubt sind, wurden sie bereits in vielen Fällen in den entsprechenden Kapiteln erläutert. Hier wird dann nur auf das Kapitel verwiesen.

17.1 ACCEPT

Dieses Ziel akzeptiert ein Paket. Das bedeutet, das Paket durchläuft die Kette erfolgreich.

17.2 CLASSIFY

Dieses Ziel ist nur in der Mangle-Tabelle erlaubt und wird daher dort besprochen (siehe Abschnitt 21.2.1).

17.3 CLUSTERIP

Dies ist ein neues experimentelles Ziel der aktuellen Linux 2.6-Kernel. Mit diesem Ziel können Sie einen Cluster mit Lastverteilung und Hochverfügbarkeit ohne Loadbalancer aufbauen. Dies ist kein Firewall-Cluster, sondern kann zum Beispiel als Web- oder E-Mail-Server genutzt werden.

Hierzu benötigen Sie einen Switch, der Multicast-Linklayer-Adressen unterstützt und Pakete an diese Adressen an mehrere Ports versenden kann. Die meisten professionellen Switches unterstützen diese Funktion. Möglicherweise müssen Sie die Funktion aktivieren.

Das `CLUSTERIP`-Target sorgt dann dafür, dass ARP-Anfragen auf die Cluster-IP-Adresse mit einer Cluster-MAC-Adresse beantwortet werden. Diese MAC-Adresse ist eine Multicast-MAC-Adresse. Multicast-MAC-Adressen beginnen mit `01:00:5e:xx:xx:xx`. Anschließend werden die Anfragen an den Cluster an diese MAC-Adresse gesendet. Der Switch wird die Pakete an alle Ports senden, auf denen die

MAC-Adresse registriert ist. Die Nodes verwenden intern eine Markierung der Verbindungen, um zu erkennen, welche Verbindungen sie akzeptieren und welche Verbindungen sie ignorieren müssen. Hierzu muss jeder Node wissen, wie viele Nodes es insgesamt in dem Cluster gibt und welche Nummer er selbst besitzt.

Sie müssen auf jedem Node lediglich eine Regel für das `CLUSTERIP`-Target aufrufen:

```
# Node 1
iptables -A INPUT -d 192.168.0.200 -j CLUSTERIP --new \
  --hashmode sourceip --clustermac 01:00:5e:11:11:11
  --total-nodes 2 --local-node 1

# Node 2
iptables -A INPUT -d 192.168.0.200 -j CLUSTERIP --new \
  --hashmode sourceip --clustermac 01:00:5e:11:11:11
  --total-nodes 2 --local-node 2
```

Bei der Definition einer neuen Cluster-IP-Adresse müssen Sie in der ersten Regel immer die Option `--new` verwenden. Mit der Option `--hashmode` wählen Sie den Verteilungsmechanismus aus. Zur Verfügung steht `sourceip`, bei dem die Verbindungen in Abhängigkeit von der Quell-IP-Adresse verteilt werden. Verbindungen von derselben IP-Adresse landen bei demselben Node. Außerdem gibt es `sourceip-sourceport` und `sourceip-sourceport-destport`, die zusätzlich noch die Ports in die Verteilung mit einbeziehen. Die Option `--clustermac` definiert die identische Multicast-MAC-Adresse auf allen Nodes. Iptables kümmert sich dann selbst um die ARP-Antworten. Sie müssen keine darüber hinausgehende Konfiguration der MAC-Adresse vornehmen. Die Optionen `--total-nodes` und `--local-node` definieren schließlich die Anzahl der Nodes im Cluster und die Nummer des lokalen Nodes. Bei Bedarf können Sie mit `--hash-init` auch noch eine Zahl für die Initialisierung der Hash-Tabelle angeben.

Wichtig ist, dass Sie auf beiden Nodes die identische Cluster-IP-Adresse und Cluster-MAC-Adresse verwenden. Eine darüber hinausgehende Konfiguration der Netzwerkkarten ist nicht erforderlich.

Sobald die Regeln aktiviert wurden, finden Sie in `/proc/net/ipt_CLUSTERIP/192.168.0.200` eine Datei, die die Nummer des Nodes enthalten sollte.

Damit ist die Lastverteilung bereits implementiert. Um zusätzlich auch eine Hochverfügbarkeit zu erreichen, benötigen Sie zusätzlich eine Software, die die Gesundheit der Nodes in dem Cluster überwacht (z.B. Heartbeat, *http://www.linux-ha.org*). Diese muss beim Ausfall eines Nodes auf dem jeweils anderen Node nur einen Befehl ausführen. Bei Ausfall des Nodes 1 muss auf Node 2 der folgende Befehl gestartet werden:

```
echo "+1" > /proc/net/ipt_CLUSTERIP/192.168.0.200
```

Damit erhält der Node 2 die Information, auch die Verbindungen für Node 1 zu übernehmen. Dies funktioniert jedoch nur für neue Verbindungen. Bereits aufgebaute Verbindungen gehen verloren.

Achtung

CLUSTERIP ist ein sehr junges und noch experimentelles Target. Daher müssen Sie darauf achten, dass Sie möglichst aktuelle Kernel und den aktuellen Iptables-Code einsetzen. In den letzten Monaten sind hier noch einige Korrekturen und Änderungen vorgenommen worden.

17.4 CONNMARK

Dieses Ziel ist nur in der NAT- und in der Mangle-Tabelle erlaubt und wird daher am entsprechenden Ort besprochen (siehe Abschnitt 20.12 und Abschnitt 21.2.2).

17.5 DNAT

Dieses Ziel ist nur in der PREROUTING- und OUTPUT-Kette der NAT-Tabelle erlaubt und wird daher am entsprechenden Ort besprochen (siehe Abschnitt 20.8).

17.6 DROP

Dieses Ziel verwirft ein Paket. Das Paket wird aus der Kette entfernt. Es erfolgt keine Protokollierung oder Benachrichtigung des Absenders.

17.7 DSCP

Dieses Ziel ist nur in der Mangle-Tabelle erlaubt und wird daher im zugehörigen Kapitel besprochen (siehe Abschnitt 21.2.3).

17.8 ECN

Dieses Ziel ist nur in der Mangle-Tabelle erlaubt und wird daher im zugehörigen Kapitel besprochen (siehe Abschnitt 21.2.4).

17.9 LOG

Hiermit können Sie eine Regel erzeugen, die eine Protokollierung über den Syslog auslöst. Dieses Target unterscheidet sich von den meisten anderen Targets dadurch, dass es nicht das Schicksal des Pakets entscheidet. Daher werden die Pakete, auf die das LOG-Target angewendet wird, von den weiteren Regeln in der Kette analysiert.

Für eine aussagekräftige Protokollierung unterstützt dieses Target die folgenden Optionen:

- `--log-level <level>`: Hiermit definieren Sie die Priorität der Meldung (`debug`, `info`, `notice`, `warning`, `error`, `crit`, `alert`, `emerg`).
- `--log-prefix "Zeichenkette"`: Hiermit können Sie bis zu 29 Zeichen angeben, die der Meldung vorangestellt werden. Dies erleichtert später die Suche mit `grep` oder die Protokollierung mit dem Syslog-ng oder ähnlichen Syslog-Daemonen.
- `--log-tcp-sequence`: Dies protokolliert die TCP-Sequenznummern.
- `--log-tcp-options`: Dies protokolliert verwendete TCP-Optionen.
- `--log-ip-options`: Dies protokolliert verwendete IP-Optionen.
- `--log-uid`: Dies protokolliert bei lokal erzeugten Paketen den Benutzer, der das Paket erzeugt hat.

Tipp

Wenn Sie ein Paket protokollieren und verwerfen möchten, benötigen Sie zwei identische Regeln. Die erste Regel testet das Paket und protokolliert es. Die zweite Regel testet das Paket auf die identische Weise und verwirft es. Um hier den zusätzlichen Aufwand des doppelten Tests zu sparen, erzeugen Sie sich einfach eine benutzerdefinierte Kette `LOGDROP`:

```
$IPTABLES -N LOGDROP
$IPTABLES -A LOGDROP -j LOG --log-prefix "Log-and-Drop: "
$IPTABLES -A LOGDROP -j DROP
```

Wenn Sie nun ein Paket protokollieren und verwerfen möchten, verwenden Sie das Target `-j LOGDROP`.

17.10 MARK

Dieses Ziel ist nur in der Mangle-Tabelle erlaubt und wird daher im entsprechenden Kapitel besprochen (siehe Abschnitt 21.2.7).

17.11 MASQUERADE

Dieses Ziel ist nur in der `POSTROUTING`-Kette der NAT-Tabelle erlaubt und wird daher im entsprechenden Kapitel besprochen (siehe Abschnitt 20.4).

17.12 NETMAP

Dieses Ziel ist nur in der NAT-Tabelle erlaubt und wird daher im entsprechenden Kapitel besprochen (siehe Abschnitt 20.5).

17.13 NFQUEUE

Ab dem Kernel 2.6.14 können Sie anstelle des `QUEUE`-Targets auch das `NFQUEUE`-Target verwenden. Hiermit können Sie Pakete an unterschiedliche Userspace-Programme übergeben, da Sie bei diesem Target die Queue über eine 16-Bit-Zahl auswählen können.

17.14 NOTRACK

Dieses Ziel ist nur in der Raw-Tabelle erlaubt und wird daher im entsprechenden Kapitel besprochen (siehe Kapitel 22).

17.15 QUEUE

Hiermit können Sie ein Paket an ein Userspace-Programm senden. Dieses kann das Paket analysieren, verwerfen oder für die weitere Bearbeitung zurückgeben. Ein Programm, das diese Funktion nutzen kann, ist Snort-Inline (*http://snort-inline.sourceforge.net*).

17.16 REDIRECT

Dieses Ziel ist nur in der `PREROUTING`-Kette der NAT-Tabelle erlaubt und wird daher im entsprechenden Kapitel besprochen (siehe Abschnitt 20.9).

17.17 REJECT

Das `REJECT`-Target verwirft das Paket wie das `DROP`-Target. Es sendet jedoch eine Fehlermeldung an den Absender des Pakets. Dieses Target ist nur gültig in den `INPUT`-, `FORWARD`- und `OUTPUT`-Ketten. Sie können die zu verwendene Fehlermeldung mit der Option `--reject-with` angeben. Sie können die folgenden Fehlermeldungen benutzen:

- `icmp-net-unreachable`
- `icmp-host-unreachable`
- `icmp-port-unreachable` (Default)
- `icmp-proto-unreachable`
- `icmp-net-prohibited`
- `icmp-host-prohibited`
- `icmp-admin-prohibited` (Der Kernel muss dies unterstützen.)
- `tcp-reset` (Die Ablehnung muss sich auf eine TCP-Verbindung beziehen.)

```
$IPTABLES -A INPUT -p tcp --dport 113 -j REJECT --reject-with tcp-reset
```

17.18 RETURN

Dieses Ziel beendet die aktuelle benutzerdefinierte Kette und kehrt mit dem Paket zur aufrufenden Kette zurück, wo die restlichen Regeln abgearbeitet werden. Handelt es sich um eine eingebaute Kette, so wird bei einem `RETURN` die Default-Policy der Kette für das Paket ausgewertet.

17.19 SAME

Dieses Ziel ist nur in der NAT-Tabelle erlaubt und wird daher im zugehörigen Kapitel besprochen (siehe Abschnitt 20.7).

17.20 SNAT

Dieses Ziel ist nur in der `POSTROUTING`-Kette der NAT-Tabelle erlaubt und wird daher im zugehörigen Kapitel besprochen (siehe Abschnitt 20.6).

17.21 TCPMSS

Dieses Target ist eine der wichtigsten Funktionen von Iptables für alle Anwender von ADSL-Leitungen. Hiermit können Sie die Maximum Segment Size für TCP-Verbindungen setzen oder ändern.

Exkurs: Was ist die MSS und wofür brauche ich sie bei DSL?

DSL-Verbindungen werden üblicherweise mit dem PPPoE- oder PPTP-Protokoll realisiert. Als physikalisches Medium wird hierfür Ethernet eingesetzt. Jedes Medium besitzt eine Maximum Transmission Unit (MTU). Dies ist die maximale Größe der Pakete, die über das Medium transportiert werden können. Bei Ethernet ist dies 1500 Bytes. Wenn Sie nun das PPP-over-Ethernet-Protokoll (PPPoE) verwenden, so benötigt das PPP-Protokoll selbst 8 Bytes für seinen PPP-Header. Es bleiben 1492 Bytes für die transportierten Informationen. Also beträgt die MTU von PPPoE 1492 Bytes. Dass das darunter liegende Ethernet eine MTU von 1500 Bytes besitzt, ist für den Datentransport unerheblich, da wir für den Transport ja PPPoE und nicht direkt Ethernet verwenden.

Betrachten Sie nun Abbildung 17.1. Dort sehen Sie ein Netzwerk, das mit dem Internet über DSL mit dem Protokoll PPPoE verbunden ist. Im Internet befindet sich ein Webserver, der durch eine Firewall geschützt wird.

Ein Client in dem Netzwerk möchte nun auf den Webserver zugreifen. Der Client baut die Verbindung auf und fordert ein Bild in der Größe von 800 Bytes von dem Webserver an. Dies erzeugt keinerlei

Probleme, da das resultierende Paket nur wenig größer wird als 800 Bytes und von PPPoE mit einer MTU von 1492 Bytes ohne Probleme transportiert werden kann.

Sobald wir jedoch von dem Webserver ein Bild oder eine andere Datei von mehr als 1500 Bytes anfordern, kann ein Problem auftreten. Der Webserver baut die IP-Pakete entsprechend der MTU seiner eigenen Netzwerkkarte. Setzen wir voraus, dass der Webserver über Ethernet angebunden ist, beträgt diese 1500 Bytes. Der Webserver baut daher wenigstens ein Paket von 1500 Bytes. Ist die Datei sehr groß, können es auch mehrere Pakete sein. Dies sendet er durch seine Firewall an den DSL-Router auf der Seite des Providers. Dieser muss nun das Paket in PPPoE einpacken und über DSL versenden. Das Paket ist aber mit 1500 Bytes 8 Bytes zu groß. Die MTU von PPPoE beträgt ja nur 1492.

Alle modernen Betriebssysteme nutzen die Path MTU Discovery, bei der sie in allen Paketen das DF-Bit im IP-Header setzen. Dieses Don't-Fragment-Bit verbietet einem Router die Fragmentierung eines zu großen Pakets. Er muss das Paket verwerfen und eine Fehlermeldung (ICMP Destination Unreachable Fragmentation Needed) zurücksenden. Die Fehlermeldung enthält auch die maximal erlaubte Größe des Pakets. Dann kann der Absender das Paket erneut mit der richtigen Größe versenden.

Stellen Sie sich vor, die Firewall, die den Webserver schützt, lässt dieses Paket nicht durch. Die Fehlermeldung erreicht den Webserver nicht. Das originale Paket hat den Client aber auch nicht erreicht. Da der Webserver keine Bestätigung über den Empfang des Pakets erhält, wird er es nach einiger Zeit unverändert neu versenden. Das Paket wird wieder verworfen und die Firewall verwirft die Fehlermeldung. Die Verbindung hängt!

Mit einem Trick können Sie das verhindern. Das TCP-Protokoll bietet Ihnen die Möglichkeit, bei der Verbindungsaufnahme Ihre Maximum Segment Size zu veröffentlichen. Die MSS ist in etwa die MTU für TCP. Wenn Sie eine MSS von 1400 an den Kommunikationspartner senden, wird dieser nie mehr als 1400 Bytes in einem TCP-Paket versenden. Das resultierende IP-Paket erhält zusätzlich nur noch den TCP-Header und den IP-Header. Beide betragen im Normalfall jeweils 20 Bytes. Das IP-Paket wird dann nicht größer als 1440 Bytes.

Damit vergeuden Sie jedoch ein paar Bytes. Wir müssen ja nur sicherstellen, dass 1492 Bytes nicht überschritten werden. Also subtrahieren Sie zweimal 20 Bytes für den IP- und den TCP-Header und erhalten 1452 Bytes. Wenn Sie dafür sorgen, dass die MSS immer auf 1452 Bytes in allen TCP-Verbindungen gesetzt wird, haben Sie das Problem behoben.

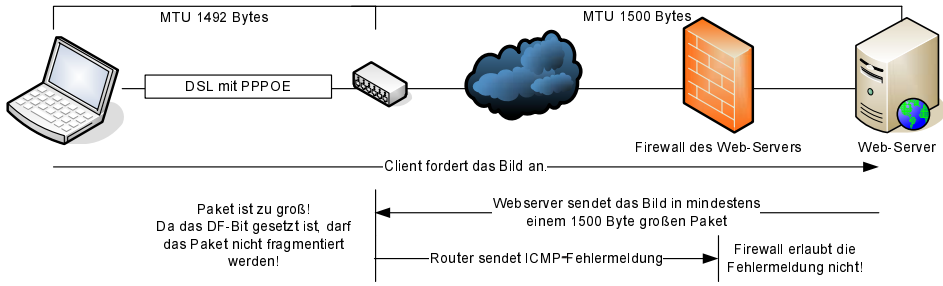


Abbildung 17.1: Bei dem Einsatz von DSL können Probleme mit der MTU auftreten.

Hinweis

Für andere Tunnel (IPsec, PPTP etc.) müssen Sie möglicherweise mit anderen Werten experimentieren. Ich habe auch schon PPPoE-Tunnel erlebt, die geringere Werte verlangt haben. Dort wurde zusätzlich noch ein weiteres Protokoll eingesetzt.

Die MSS kann nur in SYN-Paketen gesetzt werden. Sie haben zwei Möglichkeiten für das Setzen. Entweder Sie errechnen selbst die optimale MSS und verwenden die Option `--set-mss <mss>`, oder Sie überlassen die Rechnerei dem Kernel. Mit der Option `--clamp-mss-to-mtu` subtrahiert der Kernel selbstständig 40 Bytes von der Path-MTU und setzt die entsprechende MSS.

```
iptables -A FORWARD -p tcp --tcp-flags SYN,RST SYN \
 -j TCPMSS --clamp-mss-to-mtu
```

17.22 TOS

Dieses Ziel ist nur in der Mangle-Tabelle erlaubt und wird daher im entsprechenden Kapitel besprochen (siehe Abschnitt 21.2.9).

17.23 TTL

Dieses Ziel ist nur in der Mangle-Tabelle erlaubt und wird daher im entsprechenden Kapitel besprochen (siehe Abschnitt 21.2.10).

17.24 ULOG

Dieses Ziel wird im Kapitel 24, Fortgeschrittene Protokollierung, besprochen.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

18 Patch-O-Matic

Der Netfilter/Iptables-Code befindet sich in konstanter Entwicklung. Die von den Distributoren verteilten Kernel und die auf *http://www.kernel.org* zur Verfügung gestellten Kernel enthalten nicht alle verfügbaren Funktionen. Einige Funktionen sind sehr nützlich, einige sind interessant, einige unsinnig und viele fehlerhaft. Dennoch sollten Sie sich die in Patch-O-Matic zusätzlich zur Verfügung gestellten Funktionen ansehen, da sie teilweise einige Probleme sehr elegant lösen können und morgen vielleicht auch im Standard-Kernel enthalten sind.

18.1 Was ist Patch-O-Matic?

Bei dem Patch-O-Matic-Paket handelt es sich um ein Patch-Paket, das seit der Iptables-Version 1.2.7 in einem eigenen Paket vertrieben wird. Dieses Paket heißt `patch-o-matic-ng` oder kurz `p-o-m`. Dieses Paket enthält Patches vom Netfilter-Team und unabhängigen Entwicklern, die noch nicht Teil des Linux-Kernels und des Iptables-Befehls sind.

Patch-O-Matic enthält viele sehr interessante Funktionen, die teilweise auch von den Distributoren in ihren Kerneln integriert werden. Diese Funktionen sind aber entweder noch nicht ausreichend getestet, nicht ausreichend stabil oder nicht gut genug dokumentiert, so dass sie noch nicht in den Standard-Kernel aufgenommen wurden. Viele der Patches reifen aber in Patch-O-Matic und werden zu einem späteren Zeitpunkt tatsächlich Teil des Linux-Kernels. Der TCP-Window-Tracking-Patch von Jozsef Kadlecsik ist ein Beispiel für einen derartigen Patch. Nach vielen anfänglichen Problemen ist dieser Patch aus Patch-O-Matic seit der Version 2.6.9 in dem Linux-Kernel enthalten.

18.2 Wie bekomme ich Patch-O-Matic, und wie wende ich es an?

Früher war Patch-O-Matic Teil des Iptables-Befehls. Dann wurde es als eigenständiges Paket von dem Netfilter-Team in regelmäßigen Abständen veröffentlicht. Seit dem 30. Januar 2005 erhalten Sie nur noch tägliche Snapshots des Patch-O-Matic-Subversion-Servers zum Download. Entweder Sie checken den Quelltext aus dem Subversion-Server aus, oder Sie laden einen derartigen Snapshot herunter. Die Snapshots finden Sie täglich aktualisiert auf *http://ftp.netfilter.org/pub/patch-o-matic-ng/snapshot/*.

Wenn Sie den Quelltext aus dem Subversion-Server auschecken möchten, können Sie die folgenden Befehle nutzen:

```
$ svn co https://svn.netfilter.org/netfilter/trunk/patch-o-matic-ng
...
A  patch-o-matic-ng/pom2patch/pom2patch
Ausgecheckt, Revision 4354.
```

Wenn Sie später prüfen möchten, ob Updates verfügbar sind, wechseln Sie einfach in das entsprechende Verzeichnis und geben Sie folgenden Befehl ein:

```
$ svn update
Revision 4354.
```

Falls Änderungen erfolgt sind, wird Ihr Quelltext-Baum aktualisiert.

Um nun Patch-O-Matic anwenden zu können, benötigen Sie sowohl den Quelltext-Baum eines Linux-Kernels als auch des Iptables-Befehls. Patch-O-Matic muss viele Patches in beiden Software-Paketen durchführen. Den Linux-Kernel erhalten Sie auf *http://www.kernel.org*, und den Iptables-Quelltext erhalten Sie auf *http://www.Iptables.org*. Wenn Sie diese ausgepackt haben, können Sie Patch-O-Matic anwenden. Hierfür gibt es mehrere Möglichkeiten:

- `./runme pending`: Dieses Kommando wendet alle zum aktuellen Zeitpunkt bekannten Bugfixes auf den Kernel und den Iptables-Befehl an. Neue Funktionen werden nur hinzugefügt, wenn sie auch auf die Aufnahme in den Kernel warten.
- `./runme base`: Viele Patches sind zueinander inkompatibel. Dieser Befehl erlaubt Ihnen nur die Anwendung kompatibler Patches. Anschließend funktioniert noch alles.
- `./runme extra`: Hier müssen Sie wissen, was Sie tun. Dieser Befehl bietet Ihnen alle Patches an. Wenn Ihr Auto anschließend einen Kolbenfresser bekommt, ist das Ihre Schuld.
- `./runme obsolete`: Hiermit können Sie alte und überflüssige Patches anwenden. Warum sollten Sie das tun wollen?

Hinweis

Die Distributoren unter den Lesern werden diese Vorgehensweise nicht besonders mögen. Wenn Sie ein Kernel- oder Iptables-Paket bauen und einen bestimmten Patch hinzufügen möchten, bevorzugen Sie genau das, einen Patch, und nicht einen `runme`-Befehl. Hierfür gibt es den Befehl `pom2patch`. Dieser Befehl erzeugt aus Patch-O-Matic den entsprechenden Patch, den Sie mit dem `patch`-Kommando anwenden können.

Damit der Befehl `runme` die Patches auch anwenden kann, sollten Sie ihm mitteilen, wo sich der Kernel- und der Iptables-Quelltext befindet. Geben Sie beim Aufruf einfach den Ort mit den folgenden Variablen an:

```
$ KERNEL_DIR=/usr/local/src/linux-2.6.13 \
> IPTABLES_DIR=/usr/local/src/iptables-1.3.3 \
> ./runme pending
Loading patchlet definitions..................................................... done


Welcome to Patch-o-matic ($Revision: 4088 $)!

Kernel:   2.6.13, /usr/local/src/linux-2.6.13/
Iptables: 1.3.3, /usr/local/src/iptables-1.3.3/
Each patch is a new feature: many have minimal impact, some do not.
Almost every one has bugs, so don't apply what you don't need!
-------------------------------------------------------
Already applied:

Testing comment... not applied
The comment patch:
   Author: Brad Fisher <brad@info-link.net>
   Status: Part of 2.6.x mainline

This option adds CONFIG_IP_NF_MATCH_COMMENT, which supplies a comment
match module.  This match allows you to add comments (up to 256 characters)
to any rule.

Supported options:
--comment COMMENT

Example:
  -A INPUT -s 192.168.0.0/16 -m comment --comment "A privatized IP block"

-------------------------------------------------------------------
Do you want to apply this patch [N/y/t/f/a/r/b/w/q/?] y

Excellent! Source trees are ready for compilation.

Recompile the kernel image (if there are non-modular netfilter modules).
Recompile the netfilter kernel modules.
Recompile the iptables binaries.
```

Am Ende jedes Patches können Sie entscheiden, ob dieser Patch zur Anwendung kommen soll oder nicht. Sie haben folgende Möglichkeiten zur Auswahl:

- `n`: No. Dies ist auch der Default, daher können Sie auch Return drücken.
- `y`: Yes. Es wird zunächst geprüft, ob der Patch anwendbar ist, und dann wird er ausgeführt. Wenn beim Test ein Fehler auftritt, wird der Patch nicht angewendet.

- t: Test. Es wird geprüft, ob der Patch anwendbar ist.
- f: Force. Der Patch wird angewendet, obwohl dabei Fehler auftreten.
- a: Restart in apply mode. Patch-O-Matic wird neu gestartet, um Patches anzuwenden.
- r: Restart in reverse mode. Patch-O-Matic wird neu gestartet, um Patches zu entfernen.
- b: Back. Einen Patch zurück.
- w: Walk. Einen Patch vorwärts.
- q: Quit. Patch-O-Matic verlassen.
- ?: Hiermit zeigt Patch-O-Matic eine Hilfe an.

Sie werden nun Patch für Patch gefragt, ob Sie den Patch anwenden möchten. Wenn Sie alle Patches durchgearbeitet haben (oben war es nur ein einziger), werden Sie aufgefordert, nun Ihren Kernel und Iptables zu übersetzen und zu installieren.

18.3 Base-Patches

Ich werde hier die Base-Patches in Patch-O-Matic vom Oktober 2005 behandeln. Wenn Sie dieses Buch lesen, hat es hier sicherlich schon Veränderungen gegeben. Vielleicht sind einige hinzugekommen und einige in den Kernel übernommen worden. Die wichtigen Patches sollen aber ein wenig ausführlicher zur Sprache kommen.

18.3.1 IPV4OPTSSTRIP

Dieser Patch fügt ein Mangle-Target IPV4OPTSSTRIP hinzu, das sämtliche IP-Optionen von einem Paket entfernen kann. Typische IP-Optionen sind zum Beispiel Source-Routing. Das Target verfügt über keine weiteren Optionen und kann daher sehr einfach eingesetzt werden:

```
# iptables -t mangle -A PREROUTING -j IPV4OPTSSTRIP
# iptables -t mangle -nL
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
IPV4OPTSSTRIP  all  --  0.0.0.0/0            0.0.0.0/0
```

18.3.2 connlimit

Dieser Patch fügt einen Test hinzu, mit dem Sie die Anzahl der Verbindungen zu einem Server pro Client oder Client-Netzwerk beschränken können. Der Test verfügt über zwei Optionen:

- --connlimit-above <Limit>. Hiermit geben Sie die maximale Anzahl der Verbindungen an.

- `--connlimit-mask <Maske>`. Hiermit beschränken Sie die Anzahl der Verbindungen nicht pro Client, sondern pro Netzwerk.

```
# Maximal 25 HTTP-Verbindungen pro Client
iptables -A FORWARD -p tcp --syn --dport 80 -m connlimit --connlimit-above 25 -j REJECT

# Maximal 100 HTTP-Verbindungen pro /24 Netzwerk
iptables -A FORWARD -p tcp --syn --dport 80 -m connlimit --connlimit-above 100 \
        --connlimit-mask 24 -j REJECT
```

18.3.3 expire

Dieser Patch gibt Ihnen die Möglichkeit, Ihren Regeln eine Lebensdauer zu geben. Sobald die angegebene Zeit abgelaufen ist, wird die Regel aus dem Regelwerk entfernt. Dies ist zum Beispiel interessant, um für einen kurzen Zeitraum einen bestimmten Zugang freizuschalten. Sie müssen nicht selbst daran denken, die Regel zu entfernen oder einen Cron-Job zu erzeugen. Der Kernel kümmert sich selbst darum.

```
iptables -A INPUT -p tcp --dport 22 -m expire --expiration +5 -j ACCEPT
```

18.3.4 NETMAP

Wenn Sie komplette Netzwerke natten möchten, ist dieser Patch möglicherweise etwas für Sie. Dieser Patch fügt ein NAT-Target hinzu, mit dem Sie sehr einfach 1:1 NAT für komplette Netzwerke implementieren können. Anstatt für jeden Rechner eine eigene Regel zu erzeugen, nutzen Sie nun eine Regel für das ganze Netz. Das `NETMAP`-Target kann sowohl als SNAT-Target in der POSTROUTING-Kette als auch als DNAT-Target in der PREROUTING-Kette angewendet werden. In dem folgenden Beispiel wird jeder IP-Adresse aus dem 1.2.3.0/24-Netz die entsprechende IP-Adresse aus dem 5.6.7.0/24-Netz zugewiesen. Das heißt, 1.2.3.10 wird 5.6.7.10, und 1.2.3.128 wird 5.6.7.128.

```
iptables -t nat -A PREROUTING -d 1.2.3.0/24 -j NETMAP --to 5.6.7.0/24
```

18.3.5 fuzzy

Dieser Patch implementiert einen Test, der die übertragenen Pakete/Sekunde mit einem Fuzzy Logic Controller prüft. Dabei ist der Test dem Limit-Test ähnlich, jedoch etwas ungenauer und somit toleranter gegenüber plötzlichen Abweichungen nach oben und unten. Er kann somit besser zur Bekämpfung von Denial-of-Service-Angriffen eingesetzt werden. Der Patch bietet die folgenden Optionen:

- `--lower-limit <packets/second>`
- `--upper-limit <packets/second>`

18.3.6 ipv4options

Dieser Patch fügt einen Test hinzu, mit dem Sie prüfen können, ob IP-Optionen in dem IPv4-Header gesetzt sind. Sie können im Einzelnen die folgenden IPv4-Optionen testen:

- `--ssrr`. Strict Source Routing.
- `--lsrr`. Loose Source Routing.
- `--no-srr`. Kein Source Routing.
- `--rr`. Record Route.
- `--ts`. Time Stamp.
- `--ra`. Router Alert.
- `--any-opt`. Mindestens eine beliebige Option.

Damit können Sie zum Beispiel Source-Routing-Pakete verwerfen:

```
iptables -t mangle -A PREROUTING -m ipv4options --ssrr -j DROP
iptables -t mangle -A PREROUTING -m ipv4options --lsrr -j DROP
```

18.3.7 nth

Dieser Patch erlaubt es Ihnen, jeweils das n-te Paket zu testen. Dabei können Sie bis zu 16 verschiedene voneinander unabhängige Zähler einsetzen. Dieser Test verfügt über einige zusätzliche Optionen:

- `--every <Nth>`. Jedes n-te Paket wird von dieser Regel ausgewertet.
- `--counter <Zahl>`. Dabei können Sie einen bestimmten Zähler (0-15) wählen. Default ist 0.
- `--start <Zahl>`. Der Zähler kann mit einer Zahl kleiner N initialisiert werden.
- `--packet <Zahl>`. Hiermit können Sie angeben, was mit jedem Paket passiert. Wenn Sie zum Beispiel `--every 2` verwenden, gibt es zwei Gruppen von Paketen, je nachdem, ob Sie bei 0 oder bei 1 anfangen zu zählen. Sie können nun zwei Regeln definieren, einmal mit `--packet 0` und einmal mit `--packet 1`, die jeweils auf diese Gruppen zutreffen.

```
iptables -t nat -A POSTROUTING -o eth0 -m nth --counter 1 \
     --every 2 --packet 0 -j SNAT --to-source 10.0.0.5
iptables -t nat -A POSTROUTING -o eth0 -m nth --counter 1 \
     --every 2 --packet 1 -j SNAT --to-source 10.0.0.6
```

18.3.8 osf

OpenBSD hat es vorgemacht, und nun ist es auch unter Linux möglich: passives Betriebssystem-Fingerprinting in den Firewall-Regeln. Sie können mit diesem Patch

Regeln aufsetzen, die nur für bestimmte Betriebssysteme gelten. Einigen Linux-Fanatikern mag die folgende Regel gefallen:

```
iptables -A FORWARD -p tcp -m osf --genre Windows -j REJECT
```

Dieser TCP-Patch kennt die Optionen:

- `--genre <os>`
- `--log <0|1>`. Wenn Sie diese Option angeben, protokolliert die Regel das Betriebssystem, wenn es nicht mit dem in der Regel angegebenen übereinstimmt. Ist der Wert `1`, so wird nur das erste nicht übereinstimmende Betriebssystem protokolliert:

  ```
  ipt_osf:  Windows  [2000:SP3:Windows XP Pro SP1, 2000 SP3]:
       11.22.33.55:4024 -> 11.22.33.44:139
  ```

- `--smart`. OSF verwendet den TTL-Wert nur, wenn das lokale Netzwerk der Ausgangsort des Pakets ist.
- `--netlink`. Hiermit kann die Protokollierung über Nlogd erfolgen.

Die notwendigen Fingerprints können Sie von *http://www.openbsd.org/cgi-bin/cvsweb/src/etc/pf.os* herunterladen. Diese Fingerprints müssen dann über das Proc-Dateisystem in den Kernel geladen werden (`/proc/sys/net/ipv4/osf`).

18.3.9 psd

Dieser Patch implementiert einen Portscan-Detektor in dem Linux-Kernel. Der Algorithmus wurde von Solar Designer's Portscan-Detektor `scanlogd` (*http://www.openwall.com*) übernommen. Ich selbst halte die Anwendung für recht kritisch, denn eine Reaktion auf einen falschen Portscan kann von einem Angreifer für einen Denial-of-Service genutzt werden. Die Erkennung durch die aktuellen Portscan-Detektoren zum Beispiel in Snort ist auch wesentlich genauer. Dennoch möchte ich kurz die Optionen aufführen und erklären.

- `--psd-weight-threshold <threshold>`. Ab diesem Schwellenwert wird ein Portscan gemeldet.
- `--psd-delay-threshold <threshold>`. Pakete, deren Abstand geringer ist als die hier angegebene Zeitspanne in Hundertstel-Sekunden, werden als Portscan-Sequenz erkannt. Dabei müssen die Pakete von der identischen Quell-IP-Adresse stammen und unterschiedliche Zielports aufweisen.
- `--psd-lo-ports-weight <weight>`. Wenn die erkannten Portscan-Pakete an einen niedrigen Port (<=1024) gerichtet sind, werden die Pakete mit diesem Gewicht addiert.
- `--psd-hi-ports-weight <weight>`. Pakete an einen hohen Port werden mit diesem Gewicht addiert.

Sobald die Summe der erkannten und gewichteten Pakete den Schwellenwert überschreitet, wird ein Portscan erkannt.

18.3.10 quota

Mit diesem Patch können Sie Netzwerkquoten vergeben. Dazu definieren Sie eine Quote mit der Option `--quota <bytes>`. Jedes Paket verringert die Quote. Nach Ablauf der Quote werden keine weiteren Pakete mehr akzeptiert. Aktuelle Versionen sollten auch, entgegen der Dokumentation, auf SMP-Systemen einsetzbar sein.

18.3.11 random

Dieser Patch trifft zufällig auf Pakete zu. Sie können mit der Option `--average <Prozent>` die Wahrscheinlichkeit des Zutreffens variieren (Default: 50%). Dieser Patch ist besonders geeignet, um Fehler durch fehlerhafte Netzwerkhardware zu simulieren.

18.3.12 set

Dies ist der Nachfolger des obsoleten `pool`-Patches. Sie benötigen für die Anwendung zusätzlich den `ipset`-Befehl, den Sie ebenfalls auf der Netfilter-Homepage finden (*http://ipset.netfilter.org*). Dieser Patch erlaubt es Ihnen, Gruppen von IP-Adressen zu definieren und diese in einer Regel zu testen. Die IP-Adressen können auch von Iptables-Regeln dynamisch zu diesen Gruppen hinzugefügt werden. Dieser Patch ist so interessant und wichtig, dass er in einem eigenen Kapitel besprochen wird (Kapitel 25).

18.3.13 time

Mit diesem Patch können Sie Regeln definieren, die nur zu bestimmten Zeiten aktiv sind. Anstatt die Regelsätze per Cron austauschen zu lassen, können Sie die Uhrzeiten direkt in den Regeln hinterlegen. Zusätzlich erlaubt der Test folgende Optionen:

- `--timestart HH:MM`
- `--timestop HH:MM`
- `--days Mon,Tue,Wed,Thu,Fri,Sat,Sun`
- `--datestart YYYY[:MM[:DD[:hh[:mm[:ss]]]]]`
- `--datestop YYYY[:MM[:DD[:hh[:mm[:ss]]]]]`

Als Zeitbasis wird die lokale Uhrzeit verwendet.

18.3.14 u32

Wenn Sie immer schon mal etwas in einem Paket testen wollten, aber bisher nicht der Test dafür in Netfilter enthalten war, ist dies der Test für Sie. Hiermit können Sie ein beliebiges Bit an einer beliebigen Stelle in einem IP-Paket prüfen.

Hierzu stellt das Modul den Test `--u32` zur Verfügung. Diese Option erlaubt Ihnen die Beschreibung des Pakets in einer sehr mächtigen Sprache. Die Syntax wird im Kernel-Quelltext wie folgt angegeben:

```
--u32 tests
tests := location = value |  tests && location = value
value := range | value , range
range := number | number : number
location := number | location operator number
operator := & | << | >> | @
```

Hinweis

Es gibt ein paar Beschränkungen bei der Anwendug dieses Moduls:

- Sie dürfen nur maximal 10 `=` (Gleichheitszeichen) und damit 9 `&&` als Argument verwenden.
- Pro Wert (`value`) dürfen Sie nur maximal 10 Bereiche (`range`) verwenden.
- Pro Ort (`location`) dürfen Sie ebenfalls nur maximal 10 Nummern (`number`) angeben.

Es werden immer 4 Bytes von dem angegebenen Ort gelesen. Zunächst ein einfaches Beispiel. Im IP-Header befindet sich das Längenfeld in den Bytes 2 und 3 des Headers. Um nun die ersten 4 Bytes des Pakets zu lesen, verwenden Sie als Ortsangabe 0. Da Sie sich jedoch nur für die Bytes 2 und 3 interessieren, wird dieses Ergebnis mit 0x0000FFFF Und-verknüpft. Damit fallen die beiden Bytes 0 und 1 weg: `0&0xFFFF`. Wenn Sie prüfen möchten, ob die Länge des Pakets kleiner als 512 Bytes ist, so können Sie dann den folgenden Test verwenden: `0&0xFFFF=0x0:0x200`. Die Angabe `0x0:0x200` prüft, ob der Wert innerhalb dieses Bereichs (0x200=512) liegt.

Ein weiteres kompliziertes Beispiel prüft, ob das Byte 0-3 in den TCP-Daten den Wert 25 oder 50 hat. Der komplette Test lautet: `6&0xFF=6 && 0>>22&0x3C@12>>26&0x3C@0=25,50`. Schauen wir uns ihn der Reihe nach an. Zunächst ermitteln wir, ob es sich überhaupt um ein TCP-Paket handelt. Dies erkennen wir im IP-Header an dem Next-Protocol-Feld. Dieses Feld ist das Byte 9 im Header. Wir lesen ab dem Byte 6 die Länge von 4 Bytes und Und-verknüpfen dies mit 0xFF. Ist der Wert 6, handelt es sich um ein TCP-Paket, und wir machen weiter in dem Test.

Hinweis

Nun müssen wir eigentlich prüfen, ob es sich um ein IP-Fragment handelt. Da aber Iptables meist unter Einsatz der Connection Tracking-Funktion verwendet wird, sind die Pakete in den Tabellen Mangle, NAT und Filter bereits defragmentiert. Fragmente treffen wir hier nicht mehr an. Sie könnten aber diesen Test einfügen: `4&0x3FFF=0`. Er liest ab dem Byte 4 die Länge von 4 Bytes und extrahiert die letzten 6 Bits von Byte 6 und das komplette Byte 7. Hier werden das MF-Bit und der Fragment-Offset gespeichert. Sind diese 0, so handelt es sich um ein komplettes Paket. Möchten Sie das

erste Fragment genauso prüfen wie ein komplettes Paket, müssen Sie einfach nur die letzten 5 Bits des Byte 6 analysieren: `4&0x1FFF=0`. Im ersten Fragment ist das MF schon gesetzt, aber der Offset noch null.

Um die gesuchten Bytes in den TCP-Daten zu finden, müssen Sie nun die Länge des IP-Headers und die Länge des TCP-Headers ermitteln und entsprechend im Paket weiterspringen. Leider wird die Länge im IP-Header in 4-Byte-Worten angegeben. Das bedeutet, dass Sie diese Zahl noch mit 4 multiplizieren müssen. Die Länge wird in den letzten 4 Bits des ersten Bytes gespeichert. Dazu liest der Test `0>>22&0x3c@` die Bytes 0-3 und verschiebt diese um 22 Bits nach rechts. Es bleiben 10 Bits. Wäre die Verschiebung um 24 Bits erfolgt, so wäre nur das erste Byte übrig geblieben. Da wir um 2 Bits weniger schieben, wird dieses Byte aber automatisch mit 2^2=4 multipliziert. Jetzt muss der Test nur noch die restlichen gesetzten Bits entfernen. Hierfür führt er eine Und-Verknüpfung mit 0x3c (0000111100) durch. Stellen Sie sich vor, der IP-Header hätte seine Standardlänge von 20 Bytes. Dann befindet sich bei einem IPv4-Paket im ersten Byte die Zahl 0x45, binär: 01000101. Nach der Verschiebung bleiben 10 Bits: 01000101yy. Der Wert der Bits yy ist unbekannt. Nun führen Sie eine Und-Verknüpfung mit 0x3c (0000111100) durch und es bleibt: 0000010100 = 0x14 = 20. Das @ im Test definiert diese Zahl als neuen Offset für den nächsten Test. Dieser funktioniert analog `12>>26&0x3C@`. Die Länge des TCP-Headers wird wieder in 4-Byte-Worten in der linken Hälfte des Bytes 12 im TCP-Header angegeben. Sie lesen also ab Byte 12 die Länge von 4 Bytes und verschieben nun um 26 Bits nach rechts. Dadurch bleiben 6 Bits übrig. Die 4 höchstwertigen Bits sind automatisch mit 4 multipliziert worden. Nun setzen Sie die beiden niedrigwertigen Bits auf null, indem Sie eine Und-Verknüpfung mit 0x3c durchführen. Dies können Sie wieder als neuen Offset verwenden. Jetzt liest der Test ab diesem Offset wieder 4 Bytes und prüft, ob deren Inhalt entweder 25 oder 50 ist (`0=25,50`).

Wie Sie sehen, können Sie mit diesem Test alle nur denkbar möglichen Tests durchführen. Um dies auf ganze Verbindungen anzuwenden, wäre es zum Beispiel möglich, in Abhängigkeit von diesem Test eine Verbindung zu markieren, um sie anschließend anders zu behandeln.

18.4 Extra-Patches

Ich werde hier die zusätzlichen Extra-Patches in Patch-O-Matic vom Oktober 2005 behandeln. Wenn Sie dieses Buch lesen, hat es hier sicherlich schon Veränderungen gegeben. Vielleicht sind einige hinzugekommen und einige in die Base-Patches oder den Kernel übernommen worden. Die wichtigen Patches sollen aber ein wenig ausführlicher zu Sprache kommen.

Achtung

Viele der Patches im Extra-Bereich sind nicht mit den aktuellsten Kernel lauffähig. Sie müssen im Grunde jeden einzelnen testen.

18.4.1 ACCOUNT

Dieser Patch fügt ein sehr schnelles Accounting-System dem Kernel hinzu. Hierfür benötigen Sie zusätzlich doch die `libipt_ACCOUNT`-Bibliothek, mit der Sie die Informationen anschließend auslesen können. In dem Paket ist auch das `ipaccount`-Werkzeug enthalten, mit dem Sie die Zahlen auf der Kommandozeile auswerten können.

Der Patch fügt ein `ACCOUNT`-Target dem Kernel hinzu. Dieses Target kennt zwei Optionen:

- `--addr <network/mask>`: Für dieses Netzwerk wird die Zählung durchgeführt.
- `--tname <name>`: Hier werden die Zahlen gespeichert.

Weitere Informationen über den Patch und die zugehörigen Pakete erhalten Sie auf *http://www.intra2net.com/opensource/ipt_acount*.

18.4.2 IPMARK

Die Firewall-Markierung ist eine häufige Methode, um Pakete verschiedenen Quality-of-Service-Queues zuzuordnen. Bei einem Service-Provider ist es häufig erforderlich, jedem Client eine eigene Queue zuzuordnen, in der dessen Verkehr reglementiert wird. Handelt es sich um viele Clients, ist das sehr aufwendig, da Sie für jede IP-Adresse eine eigene Regel definieren müssen. Dieses Target erleichtert die Definition ungemein, da es die Markierung direkt aus der IP-Adresse erzeugen kann. Statt 50 Regeln für 50 Clients genügt dann häufig eine einzige Regel.

Das `IPMARK`-Target unterstützt in der Mangle-Tabelle noch die folgenden Optionen:

- `--addr src|dst`. Diese Option definiert, ob die Quell- oder die Ziel-IP-Adresse für die Erzeugung der Markierung genutzt wird.
- `--and-mask <mask>`. Vor Erzeugung der Markierung kann die IP-Adresse mit dieser Maske Und-verknüpft werden.
- `--or-mask <mask>`. Zusätzlich kann die IP-Adresse mit dieser Maske Oder-verknüpft werden. Es wird immer zuerst die Und- und dann die Oder-Verknüpfung durchgeführt.

Wenn Sie zum Beispiel ein Client-Netzwerk mit den IP-Adressen 192.168.0.0/24 verwenden und für jeden Client eine eigene Markierung zwischen 0 und 255 setzen möchten, können Sie die folgende Zeile verwenden:

```
iptables -t mangle -A PREROUTING -i eth1 -j IPMARK --addr=src
   --and-mask=0xff
```

18.4.3 ROUTE

Auch bei diesem Patch handelt es sich um einen Patch, der umständliche Konfigurationen, die über eine Firewall-Markierung eine andere Routing-Tabelle auswählen, überflüssig macht. Sie können mit diesem Patch direkt in der Mangle-Tabelle die Route eines Pakets ändern.

Dieser Patch unterstützt die folgenden Optionen:

- `-oif <ethX>`. Das Paket verlässt das System über diese Netzwerkkarte.
- `--iif <ethX>`. Das Paket kommt scheinbar über diese Netzwerkkarte an der Firewall an.
- `--gw <ip-address>`. Das Paket wird über diesen Router weitergeleitet.
- `--continue`. Normalerweise werden die weiteren Regeln nach dem `ROUTE`-Target nicht mehr betrachtet. Hiermit wird dieses Verhalten umgedreht und werden weitere Regeln ausgewertet.
- `--tee`. In diesem Fall wird eine Kopie des Pakets entsprechend der Regel geroutet. Das originale Paket wird aber den Regeln unverändert unterworfen.

Achtung

Die drei Optionen `--tee`, `--continue` und `--iif` können nicht gleichzeitig in derselben Regel auftauchen!

Um zum Beispiel den gesamten ausgehenden SMTP-Verkehr über ein anderes Gateway zu routen, können Sie den folgenden Befehl verwenden:

```
iptables -t mangle -A POSTROUTING -p tcp --dport 25 -j ROUTE --gw 1.2.3.4
```

18.4.4 TARPIT

Dieser Patch erzeugt ein neues Target `TARPIT`, das ähnlich wie LaBreas Tarpit eingesetzt werden kann. Dies ist zum Beispiel sinnvoll, um Würmer in ihrer Ausbreitung zu verlangsamen oder einen Port-Scanner zu verwirren. Dieses Target akzeptiert TCP-Verbindungen, indem es einen kompletten TCP-Handshake durchführt. Anschließend wird von Tarpit für die Verbindung ein TCP-Window von null übermittelt. Das weist den Client an, die Datenübertragung einzustellen. Der Client wird anschließend in regelmäßigen Abständen fragen, ob er fortfahren kann. Tarpit wird dies und auch einen Verbindungabbau ablehnen. Der Client muss auf den Timeout der Verbindung warten.

Tipp

Wenn Sie TARPIT verwenden, sollten Sie alle Verbindungen, die Sie später mit TARPIT verzögern möchten, bereits in der raw-Table aus dem Connection Tracking entfernen. Ansonsten speichert der Kernel unnützerweise in seiner Zustandstabelle die Verbindung ab und überwacht sie. Die Manpage gibt hier ein gutes Beispiel.

18.4.5 TRACE

Für die Fehlersuche in Ihren Regelsätzen ist das TRACE-Target eine interessante Funktion. Hiermit können Sie in der Raw-Tabelle ein Paket für den Trace auswählen. Anschließend protokolliert das System bei jeder auf dieses Paket zutreffenden Regel die Tabelle, die Kette und die Regelnummer. Die raw-Tabelle muss zur Verfügung stehen, um dieses Target zu verwenden.

18.4.6 XOR

Mit diesem Patch wird ein neues Target XOR für die Mangle-Tabelle eingeführt, mit dem Sie eine einfache XOR-»Verschlüsselung« durchführen können.

Hierzu akzeptiert dieses Target zwei Optionen:

- `--key <string>`
- `--block-size <blockgröße>`

18.4.7 account

Dieser Patch ähnelt dem ACCOUNT-Patch. Während Letzterer ein Target hinzufügt, implementiert dieser Patch einen Pakettest. Die Erweiterung account erlaubt die folgenden zusätzlichen Optionen:

- `--aname <name>`. Name des Zählers.
- `--aaddr <net/mask>`. Adresse, für die das Accounting durchgeführt werden soll.
- `--ashort`. Das Accounting implementiert getrennte Zähler für jedes Protokoll (TCP, UDP, ICMP und Other). Mit diesem Schalter werden alle Protokolle gemeinsam in einem Zähler geführt.

Die Zähler können anschließend über das Sysctl-Interface unter `/proc/net/ipt_account/<name>` ausgelesen und auch mit Startwerten gesetzt werden.

Weitere Informationen über den Patch erhalten Sie auf *http://www.barbara.eu.org/~quaker/ipt_account/*.

18.4.8 condition

Mit diesem Patch für den 2.4.x-Kernel können Sie selbst Variablen in dem Verzeichnis `/proc/net/ipt_condition` erzeugen und diese in Regeln auswerten:

```
echo 1 > /proc/net/ipt_condition/web_ok

iptables -A INPUT -p tcp -m condition --condition web_ok --dport 80 -j ACCEPT
```

18.4.9 connrate

Mit diesem Patch fügen Sie zu Ihrem Kernel einen Test hinzu, der die Datenrate der Verbindungen überwacht und es Ihnen erlaubt, Verbindungen anhand dieser Datenrate zu identifizieren. Dazu definieren Sie eine Unter- und eine Obergrenze, und dieser Test wird auf alle Verbindungen innerhalb dieses Bereichs zutreffen. Sie können die Raten nach Anwendung dieses Patches auch in der Datei `/proc/net/ip_conntrack` nachvollziehen.

Eine sinnvolle Anwendung ist zum Beispiel die Reklassifizierung von Verbindungen, die besonders viele Daten übertragen.

18.4.10 geoip

Mit diesem Patch können Sie IP-Adressen in Abhängigkeit des Ortes prüfen. Hierfür benötigen Sie die GeoIP-Datenbank. Diese Datenbank enthält Informationen, wo auf der Welt welche IP-Adressen verwendet werden. Diese Informationen können Sie nutzen, um zu testen, woher und wohin ein Paket transportiert wird:

```
iptables -A FORWARD -m geoip --source-country DE,US -j ACCEPT
```

Weitere Informationen über die Anwendung erhalten Sie auf *http://people.netfilter.org/peejix/geoip/howto/geoip-HOWTO.html*.

18.4.11 goto

Ein häufiges Problem bei der Anwendung von benutzerdefinierten Ketten ist die Tatsache, dass nach deren Abarbeitung ein Rücksprung in die aufrufende Kette erfolgt. Wenn Sie das nicht möchten, müssen Sie explizit an das Ende der benutzerdefinierten Kette eine Catch-All-Regel anfügen. Mit diesem Patch können Sie statt eines Jumps nun ein Goto durchführen. Auf diesen erfolgt kein Rücksprung! Wenn Sie eine benutzerdefinierte Kette abarbeiten, wird am Ende kein Rücksprung durchgeführt!

18.4.12 h323-conntrack-nat

Wenn Sie die H.323-Protokolle verwenden (z.B. Microsoft Netmeeting oder Gnomemeeting), dann wollen Sie wahrscheinlich auf Ihrer Firewall auch diesen Patch verwenden. Hiermit können Sie die sehr komplizierten Protokolle, bei denen

viele dynamische Ports ausgehandelt werden, recht einfach filtern und natten. Allerdings unterstützt dieser Patch kein H.245-Tunneling und kein H.225-RAS. Für eine minimale Netmeeting-Funktion genügt üblicherweise nach dem Laden der neuen Module die Berücksichtigung des Ports 1720/tcp.

18.4.13 ip_queue_vwmark

Mit diesem Patch können Sie die Firewall-Markierung eines Pakets in Userspace modifizieren. Hierzu wird das Paket über das QUEUE-Interface an einen Prozess im Userspace gegeben, der das Paket prüfen und markieren kann. Diese Funktionalität wird von der NuFW (*http://www.nufw.org*) genutzt, die spezielle Paketfilterregeln für einzelne Benutzer an- und abschalten kann.

18.4.14 ipp2p

Hiermit können Sie Peer-to-Peer-Verkehr testen. Die Funktion ist in Abschnitt 32.7 erläutert.

18.4.15 policy und IPsec-Patches

Es gibt eine Reihe von Patches in Patch-O-Matic, die den IPsec-Verkehr betreffen. Diese werden in dem entsprechenden Kapitel (siehe Kapitel 33) besprochen.

18.4.16 mms-conntrack-nat

Dieser Patch fügt Helfermodule hinzu, die das crosoft-Streaming-Media-Protokoll analysieren und neu ausgehandelte Verbindungen der Verbindungstabelle als Expectation mit dem Zustand RELATED hinzufügen.

Nach dem Laden der entsprechenden Module ist es ausreichend, den Port 1755 sowohl für TCP als auch für UDP zu öffnen.

18.4.17 mport

Für alte Kernel < 2.6.11 fügt dieser Patch die Möglichkeit hinzu, bei der Benutzung von `-m multiport` nicht nur einzelne Ports, sondern auch Port-Bereiche zu verwenden:

```
iptables -A FORWARD -p tcp -m mport --ports 21:23,80 -j ACCEPT
```

Ab dem Kernel 2.6.11 ist diese Funktion in `multiport` enthalten.

18.4.18 owner-socketlookup

Mit diesem Patch können Sie den `owner`-Match auch in der INPUT-Kette verwenden. Sie können prüfen, welcher Benutzer das Paket entgegennehmen wird.

18.4.19 pptp-conntrack-nat

Mit diesem Patch ist es möglich, Point-to-Point-Protokoll-Verkehr sicher zu filtern und zu natten. Das PPTP-Protokoll verwendet ähnlich dem FTP-Protokoll ausgehandelte Verbindungen. Die Steuerungsverbindung verwendet immer den Port 1723/tcp. Über diese Verbindung handeln Client und Server einen GRE-Tunnel aus. Mit diesem Patch können Sie den GRE-Tunnel automatisch mit dem Zustand RELATED akzeptieren. Netfilter erkennt dann selbstständig über ein Helfermodul den richtigen GRE-Tunnel. Außerdem können Sie auch das GRE-Protokoll natten. Dies ist schwierig, da GRE nicht über Ports verfügt und dadurch die Zuordnung mehrerer GRE-Tunnel zu verschiedenen Clients problematisch ist.

Nach Anwendung sind die folgenden zusätzlichen Module verfügbar, die Sie für die Funktion laden müssen:

```
ip_conntrack_proto_gre
ip_conntrack_pptp
ip_nat_proto_gre
ip_nat_pptp
```

Dann können Sie mit den folgenden Regeln PPTP zulassen:

```
iptables  -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -p tcp --dport 1723 -m state --state NEW -j ACCEPT
```

18.4.20 quake3-conntrack-nat

Dieser Patch funktioniert ähnlich dem PPTP-Patch. Auch dieser Patch fügt zwei neue Helfermodule (für Conntrack und NAT) hinzu und erlaubt dann automatisch die Akzeptanz der ausgehandelten Quake3-Verbindungen. Für die Funktion müssen Sie anschließend nur den Zugriff auf den Port 27950/udp erlauben.

18.4.21 rpc

Dieser Patch fügt sowohl Helfermodule als auch Tests hinzu, mit denen Sie Unix-RPC-Verbindungen (UDP und TCP) sicher filtern können. Allerdings sollten Sie grundsätzlich kein RPC über das Internet einsetzen. Der Patch kann dennoch Sinn machen, wenn Sie in Ihrem lokalen Netz NFS oder NIS einsetzen und Ihre Server mit einer Firewall schützen möchten.

18.4.22 rsh

Dieser Patch fügt Helfermodule für das RSH-Protokoll hinzu. Die Remote Shell erlaubt die Arbeit auf einem anderen System ähnlich Telnet und der Secure Shell. Allerdings ist RSH nicht verschlüsselt. Einige Anwendungen benötigen es jedoch (z.B. Legato NetWorker Backup).

18.4.23 sip

Dieser Patch fügt Helfermodule für das SIP-Protokoll hinzu (siehe Abschnitt 32.22).

18.4.24 talk-conntrack-nat

Dieser Patch fügt Helfermodule für das Talk- (517/udp) und NTalk/Ntalk2-Protokoll hinzu. Damit können Talk-Verbindungen in beiden Richtungen auch durch Firewalls und NAT aufgebaut werden.

18.4.25 tproxy

Dieser Patch implementiert eine sehr interessante Funktion: einen transparenten Proxy. Ein echter transparenter Proxy ist ein Proxy, der sowohl für den Client als auch den Server unsichtbar ist. Viele Implementierungen bezeichnen bereits eine Firewall als transparenten Proxy, wenn sie lediglich für den Client unsichtbar ist. Dies genügt jedoch manchmal nicht, da die Adresse des echten Clients für den Server verloren geht. Stellen Sie sich eine Firewall vor, die einen Webserver mittels eines transparenten Proxys schützen möchte. Da der Proxy nur für den Client und nicht für den Webserver unsichtbar ist, werden Sie bei der Auswertung der Protokolle des Webservers nur Zugriffe Ihres Proxys erkennen. Bei einem echt transparenten Proxy, wie Sie ihn mit diesem Patch implementieren können, ist das nicht der Fall. Die Verbindung des Proxys mit dem Server wird mit der originalen IP-Adresse des Clients wieder aufgebaut. Die Informationen für die NAT-Zuordnungen werden in einer eigenen Tabelle `tproxy` abgespeichert. Sie wählen die Verbindungen, die der transparente Proxy übernehmen soll, mit dem `TPROXY`-Target aus.

18.4.26 unclean

Der `unclean`-Test prüft viele verschiedene Eigenschaften eines IP-Pakets und entscheidet, ob dieses Paket den Regeln und Standards entspricht oder irgendwelche Regeln missachtet. Da in der Vergangenheit beim 2.4-Kernel größere Probleme auftraten, bei denen korrekte Pakete verworfen wurden, ist dieser Test nun nicht mehr Bestandteil des Standard-Kernels, sondern Teil von Patch-O-Matic. Wenn Sie den Patch angewendet haben, können Sie fehlerhafte Pakete ganz einfach verwerfen:

```
iptables -t FORWARD -m unclean -j DROP
```

Im Einzelnen führt dieses Modul die folgenden Tests durch:

- ICMP-spezifisch:
  - Ist der Header komplett?
  - Enthält das ICMP-Fehler-Paket das Paket, das den Fehler auslöste?
  - Verwendet das ICMP-Paket einen ungültigen ICMP-Code?
  - Ist das ICMP-Paket zu groß?
  - Bezieht sich die Parameter-Problem-Fehlermeldung tatsächlich auf den IP-Header des auslösenden Fehlerpakets?

  - Wurde die Source-Quench- oder Time-Exceeded-Fehlermeldung von einem Router gesendet? Router verwenden diese Fehlermeldungen nicht mehr!

  UDP-spezifisch:

- – Stimmt die Länge des Pakets?
  - Zielport 0 ist nicht erlaubt.
- TCP-spezifisch:
  - Ist das Paket kleiner als die Mindestgröße des TCP-Headers?
  - Wenn es sich um einen in einer ICMP-Fehlermeldung eingebetteten TCP-Header handelt, müssen die Ports vorhanden sein.
  - Port 0 ist nicht erlaubt.
  - Sind die reservierten Bits im TCP-Header tatsächlich ungenutzt? Dieser Test kennt bereits die ECN-Bits und berücksichtigt sie.
  - Werden nur erlaubte TCP-Flag-Kombinationen verwendet? Die erlaubten Kombinationen sind: SYN, SYN/ACK, RST, RST/ACK, RST/ACK/PSK, FIN/ACK, ACK, ACK/PSH, ACK/URG, ACK/URG/PSH, FIN/ACK/PSH, FIN/ACK/URG und FIN/ACK/URG/PSH.
  - Werden die TCP-Optionen in der richtigen Reihenfolge und Länge angegeben?

  Allgemeine Prüfungen:

- – Stimmt die Länge des IP-Pakets?
  - Weisen die Fragmente die richtige Länge auf, und bestehen sie aus Vielfachen von 8 Byte?
  - Ist die Länge der zusammengesetzten Fragmente länger als 64 kByte (Ping of Death)?
  - Werden die Fragment-Flags in ungültiger Kombination genutzt, oder ist die Länge eines Fragments null?
  - Ist das erste Fragment mindestens 128 Bytes lang (AX25)?
  - Ist das Next-Protocol-Feld gesetzt?

Alle diese Tests manuell (zum Beispiel mit dem `u32`-Test) zu implementieren, ist sehr aufwendig und verbraucht auch extrem viel Prozessorzeit. Hier ist `unclean` wesentlich einfacher in der Anwendung. Sie sollten die Pakete, die von diesem Test erkannt werden, mindestens protokollieren, vielleicht auch verwerfen.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

19 Connection Tracking

Das Connection Tracking ist eine wesentliche Funktion der Iptables/Netfilter-Firewall. Deshalb gebührt dieser Funktion auch ein eigenes Kapitel. Da diese Funktionalität aber für viele andere Funktionen (zustandsorientiertes Filtern, Network Address Translation) benötigt wird, wurden in den entsprechenden Kapiteln bereits ausführlich verschiedene Aspekte betrachtet. Hier soll es daher nur um die fortgeschrittene Konfiguration des Connection Tracking gehen.

19.1 Connection Tracking – Überblick

Das Connection Tracking ist verantwortlich für die Überwachung der Netzwerkverbindungen durch die Iptables-Firewall. Das Connection Tracking kann TCP-, UDP-, ICMP- und alle anderen Protokolle überwachen. Hierzu erkennt das Connection Tracking, aus welcher Richtung das erste Paket kommt. Dieses Paket erhält den virtuellen Zustand `NEW`. Wenn das Paket von den Firewall-Regeln akzeptiert wird, wird die Verbindung auch in der Zustandstabelle eingetragen. Das zweite Paket muss aus der anderen Richtung kommen. Nur dann erhalten das zweite Paket und die Verbindung in der Zustandstabelle den virtuellen Zustand `ESTABLISHED`. Alle weiteren Pakete erhalten unabhängig von ihrer Richtung den Zustand `ESTABLISHED`. Diese Funktion kann genutzt werden, um Verbindungen nur in bestimmten Richtungen zu erlauben.

Das Connection Tracking unterscheidet insgesamt 5 verschiedene Zustände:

- `NEW`: Ein Paket ist neu, wenn die dazugehörige Verbindung noch nicht in der Verbindungstabelle existiert und das Paket bestimmte andere Eigenschaften hat, die für ein neues Paket verlangt werden. Diese Eigenschaften sind von dem Protokoll abhängig und werden weiter unten besprochen.
- `ESTABLISHED`: Ein Paket hat den Zustand `ESTABLISHED`, wenn die Verbindung bereits in der Verbindungstabelle existiert und mindestens ein Antwortpaket bereits von dem Connection Tracking gesehen wurde oder dieses Paket das erste Antwortpaket ist.
- `RELATED`: Ein Paket ist mit einer Verbindung verwandt, wenn es, obwohl es ein anderes Protokoll, eine andere IP-Adresse und andere Ports verwendet, sich auf eine Verbindung bezieht, die den Zustand `ESTABLISHED` hat. Dies können ICMP-Fehlermeldungen sein oder Verbindungen, die von einem Connection Tracking-Helfermodul hinzugefügt wurden. Auf modernen Kerneln werden die letzten

Verbindungen in einer eigenen Verbindungstabelle `/proc/net/ip_conntrack_expect` verwaltet.

- `INVALID`: Falls ein Paket zu keiner der in der Verbindungstabelle aufgeführten Verbindungen passt, aber dennoch nicht die Anforderungen für eine neue Verbindung beim verwendeten Protokoll erfüllt, ist es ungültig. Dies können zum Beispiel ICMP-Fehlermeldungen sein, die sich auf eine in der Verbindungstabelle nicht vorhandene Verbindung beziehen.
- `UNTRACKED`: Wenn Ihr Kernel über die `raw`-Tabelle verfügt, kennt das Connection Tracking auch den Zustand `UNTRACKED`. Das bedeutet, dass diese Verbindung nicht von dem Connection Tracking überwacht wird und daher auch nicht in der Verbindungstabelle auftaucht.

Da die verschiedenen Protokolle unterschiedliche Arten der Verbindung unterstützen und diese unterschiedlich auf- und abbauen, unterscheidet das Connection Tracking im Linux-Kernel auch diese Protokolle in der Behandlung.

19.1.1 Das TCP-Connection Tracking

Bei dem TCP-Connection Tracking gibt es zwei Varianten. Dieser Abschnitt bespricht die alte Version, die bis Kernel 2.6.8 einschließlich genutzt wurde. Die neue Variante wird im Abschnitt TCP-Window-Tracking (siehe Abschnitt 19.3) besprochen.

Das alte TCP-Window-Tracking erkennt eine neue Verbindung daran, dass die verwendeten IP-Adressen und Ports des Pakets mit keiner der in der Verbindungstabelle eingetragenen Verbindungen übereinstimmen. Zusätzlich muss das Paket mit dem Zustand `NEW` entweder ein `SYN`-, ein `ACK`- oder ein Null-Paket sein. Ein Null-Paket hat kein TCP-Flag gesetzt.

Damit die Verbindung anschließend in den Zustand `ESTABLISHED` versetzt wird, muss auf ein `SYN`-Paket immer ein `SYN/ACK`-Paket aus der entgegengesetzten Richtung folgen. Wurde die Verbindung mit einem `ACK`-Paket im Zustand `NEW` begonnen, so befindet sich die Verbindung anschließend direkt in dem Zustand `ESTABLISHED`, ohne dass ein Antwort-Paket erforderlich ist. Dies erlaubt die Wiederaufnahme von Verbindungen nach einem Reboot der Firewall oder nach einem Failover in einem Firewall-Cluster. Weitere Informationen hierzu finden Sie im Abschnitt 26.3, »Hochverfügbarkeit bei zustandsorientierten Firewalls«.

Die aufgebaute Verbindung verbleibt für bis zu 5 Tage in der Verbindungstabelle, wenn keine weiteren Pakete von dem Connection Tracking erkannt werden. Jedes weitere Paket setzt die Lebensdauer des Eintrags in der Tabelle wieder auf 5 Tage zurück. Sobald das Connection Tracking ein TCP-`RST`-Paket oder ein TCP-`FIN`-Paket erkennt, wird die Verbindung auch aus der Zustandstabelle entfernt. Um diese verschiedenen Zustände sauber trennen zu können, verwaltet das Connection Tracking intern die Zustände viel detaillierter und versieht die einzelnen Zwischenzustände auch mit unterschiedlichen Timeouts. Diese verschiedenen Zwischenzustände werden im Abschnitt 19.4.14, »TCP-Zustände«, besprochen.

19.1.2 Das UDP-Connection Tracking

Das Protokoll UDP unterscheidet sich von dem Protokoll TCP dadurch, dass dieses Protokoll keine Verbindungen kennt. Daher gibt es auch keine Signalisierung eines Verbindungsaufbaus oder -abbaus in dem UDP-Protokoll. Die Überwachung der Verbindung kann nur durch reine Beobachtung der Pakete und Verwendung von Timeouts erfolgen.

Das Connection Tracking erkennt eine neue Verbindung daran, dass das Paket IP-Adressen und Portnummern verwendet, die zu keiner in der Tabelle gespeicherten UDP-Verbindungen passen. Ist das der Fall, erhält das Paket den Zustand `NEW` und die Verbindung wird, wenn die Regeln es erlauben, als neue Verbindung in die Tabelle eingetragen.

Da es durchaus Applikationen gibt, die über UDP lediglich Informationen versenden und nie eine Antwort erhalten, muss das Connection Tracking die Verbindung selbstständig nach einiger Zeit wieder entfernen. Eine Verbindung, für die das Connection Tracking keine Antwort-Pakete aus der entgegengesetzten Richtung gesehen hat, wird automatisch nach 30 Sekunden aus der Tabelle entfernt. Kommt das Antwort-Paket erst nach 31 Sekunden, so kommt es zu spät und wird nicht mehr als `ESTABLISHED` erkannt.

Erhält das Connection Tracking innerhalb der 30 Sekunden ein Antwort-Paket, so wird die Lebensdauer für die Verbindung in der Tabelle auf 180 Sekunden heraufgesetzt. Solange nun alle 180 Sekunden ein weiteres Paket mit identischen IP-Adressen und Portnummern ausgetauscht wird, verbleibt die Verbindung in der Tabelle. Ist das nicht der Fall, wird die Verbindung nach 180 Sekunden aus der Zustandstabelle entfernt.

19.1.3 Das ICMP-Connection Tracking

Auch beim ICMP-Protokoll gibt es ähnlich wie beim UDP-Protokoll keine echten Verbindungen. Jedoch ist zum Beispiel der Ping mit den Nachrichten Echo-Request und Echo-Reply einer Verbindung ähnlich. Das Connection Tracking behandelt daher alle ICMP-Request- und -Reply-Pakete auch entsprechend. Sobald das Connection Tracking ein Request-Paket erkennt, trägt es dieses mit seinen IP-Adressen, seiner Identifikations- und Sequenznummer in der Verbindungstabelle ein. Das Request-Paket erhält den Zustand `NEW` zugewiesen. Die Identifikationsnummer erlaubt es, die Request-Pakete verschiedener Ping-Befehle auseinander zu halten. Die Sequenznummer ermöglicht es, die Reply-Pakete den entsprechenden Request-Paketen zuzuordnen. Das Connection Tracking richtet in der Verbindungstabelle für jedes eindeutige Request-Paket eine Verbindung ein. Sobald nun das Connection Tracking ein Reply-Paket erkennt, prüft es die IP-Adressen, die Identifikationsnummer und die Sequenznummer und vergleicht diese mit den Verbindungen in der Tabelle. Stimmen diese mit einer Verbindung überein, so erhält das Paket den Zustand `ESTABLISHED` und die Verbindung wird aus der Tabelle entfernt, denn pro Echo-Request-Paket ist nur ein Reply-Paket erlaubt. Stimmen die Daten nicht mit einer bekannten Verbindung überein, so erhält das Reply-Paket den Zustand `INVALID`.

Damit die Verbindungen nicht unendlich lange in der Tabelle verbleiben, wenn kein Reply-Paket gesendet wird, erhalten diese Verbindungen eine Lebensdauer von 30 Sekunden. Das Reply-Paket muss innerhalb dieser 30 Sekunden erkannt werden, sonst entfernt das Connection Tracking die Verbindung aus der Tabelle.

Das ICMP-Protokoll wird aber auch dafür verwendet, um Fehler in TCP- und UDP-Verbindungen anzuzeigen. Diese Fehlermeldungen können von IP-Adressen versendet werden, die mit der eigentlichen Verbindung nichts zu tun haben (z.B. Router). Das Connection Tracking erkennt die Verbindung, auf die sich die ICMP-Fehlermeldung bezieht, an dem Inhalt des ICMP-Pakets. Eine ICMP-Fehlermeldung muss immer den kompletten IP-Header und die ersten 64 Bit der IP-Daten enthalten. Bei TCP- oder UDP-Paketen befinden sich hier die Ports. Diese Header werden von dem Connection Tracking ausgewertet. Existiert eine Verbindung in der Tabelle, auf die diese Informationen passen, so erhält das Paket den Zustand `RELATED` und die Verbindung, auf die sich die Fehlermeldung bezieht, wird aus der Tabelle entfernt.

19.1.4 Das Connection Tracking für alle weiteren Protokolle

Für alle weiteren Protokolle kennt das Connection Tracking mit einigen wenigen Ausnahmen (z.B. GRE bei Anwendung der PPTP-Patches) keine besonderen Regelungen. Sie werden alle gleich behandelt. Ein neues Paket erkennt das Connection Tracking an der Tatsache, dass sich in der Tabelle noch keine Verbindung befindet, die die gleichen IP-Adressen und das gleiche Protokoll verwendet. Sobald sich eine derartige Verbindung in der Tabelle befindet, werden alle weiteren Pakete, die identische IP-Adressen und dasselbe Protokoll verwenden, mit dem Zustand `ESTABLISHED` versehen. Die Verbindung bekommt ab dem ersten Paket die Lebensdauer von 600 Sekunden zugewiesen. Das bedeutet, dass entweder innerhalb von 600 Sekunden ein weiteres Paket dieser Verbindung erkannt werden muss oder die Verbindung aus der Tabelle entfernt wird. Jedes weitere Paket setzt die Lebensdauer wieder auf 600 Sekunden zurück.

19.2 Das ip_conntrack-Kernelmodul

Das `ip_conntrack`-Kernelmodul unterstützt beim Laden die Definition des Parameters `hashsize`. Um diesen Parameter zu verstehen, müssen wir uns zunächst mit der Verbindungstabelle beschäftigen. Die Verbindungstabelle wird als Hash-Tabelle angelegt, damit der Kernel schnell in der Tabelle suchen kann. Während Sie die Größe der Verbindungstabelle während der Verwendung der Tabelle ändern können, ist die Größe des Hashes fix und wird bei der Erzeugung der Verbindungstabelle festgelegt. Anschließend kann die Größe des Hashs nicht geändert werden.

Auf einem normalen Linux-System berechnet der Kernel die Größe der Verbindungstabelle und des Hashs aus der Arbeitsspeichergröße. Auf der Intel 32-Bit-Architektur wird die Größe der Verbindungstabelle wie folgt berechnet:

```
CONNTRACK_MAX = RAM / 16384
```

Auf einem 512-MByte-Rechner hat die Verbindungstabelle also eine Größe von maximal 32.768 Verbindungen. Diese Größe sinkt unabhängig von der Speichergröße nie unter 128, und auch auf Systemen mit mehr als 1 GByte Speicher beträgt dieser Wert maximal immer 65.536. Ist dieser Wert erreicht, werden weitere Verbindungen nicht mehr von der Firewall akzeptiert. Sie können diesen Wert aber manuell in der Variablen `ip_conntrack_max` setzen:

```
echo 128000 > /proc/sys/net/ipv4/ip_conntrack_max
```

Bei einigen Kernel müssen Sie alternativ auf diese Datei zugreifen:

```
echo 128000 > /proc/sys/net/ipv4/netfilter/ip_conntrack_max
```

Den aktuellen Wert können Sie hier auch auslesen.

Die Größe des Hashs (`hashsize`) wird ebenfalls von dem Kernel berechnet und beträgt auf der Intel 32-Bit-Architektur HASHSIZE=CONNTRACK_MAX / 8. Diese Berechnung wird nur einmal beim Laden des Moduls durchgeführt, da anschließend die Hashsize nicht mehr geändert werden kann. Wenn Sie anschließend aber den Wert CONNTRACK_MAX erhöhen, ist die Größe des Hashs nicht mehr optimal, und die Suche nach einer Verbindung in der Tabelle durch den Kernel dauert unnötig lange.

Um dies zu verhindern, sollten Sie vor dem Laden des Kernelmoduls bereits entscheiden, wie viele Verbindungen Ihre Verbindungstabelle später unterstützen soll. Berechnen Sie nun den passenden Wert für die Hashsize, indem Sie die maximale Anzahl der Verbindungen durch 8 teilen. Bei einem Kernel älter als 2.4.21 sollten Sie auf Grund des verwendeten Hash-Algorithmus möglichst eine Primzahl benutzen. Bei jüngeren Kerneln sollte es sich bei der Zahl um eine Potenz von 2 handeln. Wählen Sie die geeignete Zahl aus, und laden Sie das Modul `ip_conntrack` manuell, bevor Ihre Regeln es benötigen:

```
modprobe ip_conntrack hashsize=16384
```

Auslesen können Sie den Hashsize-Wert entweder aus den Kernelmeldungen beim Laden des Moduls oder, wenn Ihr Kernel es unterstützt, über die Variable `/proc/sys/net/ipv4/netfilter/ip_conntrack_buckets`.

Tipp

Falls Sie das Modul `ip_conntrack` fest in den Kernel einkompiliert haben, können Sie auch die Option `ip_conntrack.hashsize=16384` als Boot-Option dem Kernel übergeben.

19.3 TCP-Window-Tracking

Lange Zeit warfen Anwender und Hersteller kommerzieller Paketfilter dem Linux-Paketfilter vor, dass die Zustandsüberwachung speziell des TCP-Protokolls nicht ausreichend sei, da sie die TCP-Sequenznummern nicht überwachen würde. Um dies zu ermöglichen, schrieb Jozsef Kadlecsik bereits im August 2000 den TCP-Window-Tracking-Patch. Ursprünglich war dieser Patch recht kritisch in der Anwendung, da er das exakte Verhalten des TCP-Protokolls entsprechend des TCP-Standards nachbildete und viele Clients sich nicht zu 100 Prozent an diesen Standard halten. Der Patch wurde in den nächsten Jahren stark verbessert und vor allem um die Funktion erweitert, die Timeout-Werte für die verschiedenen Protokolle über das `/proc`-Verzeichnis einstellen zu können. Mit dem Kernel 2.6.9 wurde der Patch als fester Bestandteil in den Kernel übernommen. Für ältere Versionen steht der Patch noch auf der Netfilter-Homepage zur Verfügung.

Achtung

Mit dem TCP-Window-Tracking werden TCP-Null-Pakete nicht mehr als neue Pakete akzeptiert!

Das TCP-Window-Tracking analysiert die von den Kommunikationspartnern angegebenen TCP-Windows und die Sequenznummern der Pakete. Alle Pakete, die eine Sequenznummer verwenden, die nicht in die aktuellen TCP-Windows passt, werden von dem Connection Tracking als `INVALID` gekennzeichnet.

Tipp

Die Funktionsweise des Patches basiert auf dem Artikel von Guido van Rooij »Real Stateful TCP Packet Filtering in IP-Filter« (*http://www.iae.nl/users/guido/papers/tcp_filtering.ps.gz*). Der Artikel beschreibt diese Funktionalität in dem IP-Filter für BSD und Solaris. Wenn Sie sich für den Hintergrund interessieren, ist dies eine sehr ausführliche Quelle der angestellten Überlegungen.

19.4 /proc-Variablen

Der TCP-Window-Tracking-Patch fügt in seiner aktuellen Version ein neues Unterverzeichnis `netfilter` dem Verzeichnis `/proc/sys/net/ipv4/` hinzu. Da das Connection Tracking das Protokoll IPv6 noch nicht unterstützt, gibt es in dem Verzeichnis `/proc/sys/net/ipv6` kein entsprechendes Verzeichnis.

Achtung

Denken Sie daran, dass nach einem Neustart des Systems diese Werte wieder auf Ihre Default-Werte zurückgesetzt werden. Es ist sinnvoll, zu Beginn Ihres Firewall-Skripts die Werte manuell zu setzen, die Sie verwenden möchten.

Dieses Verzeichnis enthält die folgenden neuen Variablen:

19.4.1 ip_conntrack_buckets

In dieser Variablen können Sie die Hashsize der Verbindungstabelle auslesen (siehe Abschnitt 19.2).

19.4.2 ip_conntrack_count

Diese Variable zeigt die Anzahl der aktuell in der Verbindungstabelle vorgehaltenen Verbindungen an.

19.4.3 ip_conntrack_generic_timeout

Diese Variable definiert das Timeout der Verbindungen, die nicht das TCP-, UDP- oder ICMP-Protokoll verwenden.

Default: 600 Sekunden.

19.4.4 ip_conntrack_icmp_timeout

Diese Variable definiert das Timeout von ICMP-Verbindungen wie Echo-Request/Echo-Reply.

Default: 30 Sekunden.

19.4.5 ip_conntrack_log_invalid

Mit diesem Parameter können Sie die Protokollierung ungültiger Pakete für ein bestimmtes Protokoll anschalten. Hierzu müssen Sie die Nummer des Protokolls in diese Variable schreiben (TCP=6, siehe `/etc/protocols`). Um diese Funktion abzustellen, nutzen Sie das Protokoll 255.

Default: 0.

19.4.6 ip_conntrack_max

Diese Variable definiert die Größe Ihrer Verbindungstabelle. Mehr Verbindungen kann das Connection Tracking nicht überwachen. Sie können diesen Wert online ändern. Jedoch sollten Sie dann auch die Hashsize anpassen und den Abschnitt über das `ip_conntrack`-Kernelmodul (siehe Abschnitt 19.2) lesen.

19.4.7 ip_conntrack_tcp_be_liberal

Hiermit schalten Sie die Überwachung der Sequenznummern und der TCP-Windows für alle Pakete außer `RST`-Paketen ab. Wenn Sie Netzwerkgeräte verwenden, die sich nicht ganz an den TCP-Standard halten, kann dies notwendig sein.

Default: 0.

19.4.8 ip_conntrack_tcp_loose

Wie bereits mehrfach erwähnt wurde, akzeptiert der Linux-Kernel auch ein `ACK`-Paket als ein neues Paket. Das können Sie mit dieser Variable abschalten. Setzen Sie dazu diese Variable einfach auf 0. Wenn Sie das Verhalten wünschen, können Sie hier angeben, wie viele Pakete in beide Richtungen geflossen sein müssen, bevor das TCP-Window-Tracking aktiv werden darf.

Default: 3.

19.4.9 ip_conntrack_tcp_max_retrans

Dieser Wert definiert die maximale Anzahl von wiederholten TCP-Paketen ohne Bestätigung des Empfängers. Sobald dieser Wert erreicht wurde, fängt der `ip_conntrack_timeout_max_retrans` an zu zählen.

Default: 3.

19.4.10 ip_conntrack_tcp_timeout_close

Diese Variable definiert, wie lange eine Verbindung in dem Zustand CLOSE verbleibt (siehe Abschnitt 19.4.14).

Default: 10 Sekunden.

19.4.11 ip_conntrack_tcp_timeout_close_wait

Diese Variable definiert, wie lange eine Verbindung in dem Zustand CLOSE_WAIT verbleibt (siehe Abschnitt 19.4.14).

Default: 60 Sekunden.

19.4.12 ip_conntrack_tcp_timeout_established

Diese Variable definiert, wie lange eine Verbindung in dem Zustand ESTABLISHED verbleibt (siehe Abschnitt 19.4.14).

Default: 432000 Sekunden; das entspricht 5 Tagen.

19.4.13 ip_conntrack_tcp_timeout_fin_wait

Diese Variable definiert, wie lange eine Verbindung in dem Zustand FIN_WAIT verbleibt (siehe Abschnitt 19.4.14).

Default: 120 Sekunden.

ip_conntrack_tcp_timeout_last_ack

Diese Variable definiert, wie lange eine Verbindung in dem Zustand LAST_ACK verbleibt (siehe Abschnitt 19.4.14).

Default: 30 Sekunden.

ip_conntrack_tcp_timeout_max_retrans

Der Timeout für die Verbindung in der Verbindungstabelle, wenn nur Paketwiederholungen ohne Bestätigung des Empfängers beobachtet wurden.

Default: 300 Sekunden.

ip_conntrack_tcp_timeout_syn_recv

Diese Variable definiert, wie lange eine Verbindung in dem Zustand SYN_RECV verbleibt (siehe Abschnitt 19.4.14).

Default: 60 Sekunden.

ip_conntrack_tcp_timeout_syn_sent

Diese Variable definiert, wie lange eine Verbindung in dem Zustand SYN_SENT verbleibt (siehe Abschnitt 19.4.14).

Default: 120 Sekunden.

ip_conntrack_tcp_timeout_time_wait

Diese Variable definiert, wie lange eine Verbindung in dem Zustand TIME_WAIT verbleibt (siehe Abschnitt 19.4.14).

Default: 120 Sekunden.

ip_conntrack_udp_timeout

Hiermit definieren Sie den Timeout einer UDP-Verbindung, für die noch nicht Pakete in beiden Richtungen erkannt wurden.

Default: 30 Sekunden.

ip_conntrack_udp_timeout_stream

Hiermit definieren Sie den Timeout einer UDP-Verbindung, für die bereits Pakete in beiden Richtungen erkannt wurden.

Default: 180 Sekunden.

19.4.14 TCP-Zustände

Das Connection Tracking unterscheidet für TCP-Verbindungen die folgenden Zustände:

1. SYN-SENT: Ein erstes `SYN`-Paket wurde erkannt.
2. SYN-RECV: Das `SYN/ACK`-Paket wurde erkannt. Dies ist das zweite Paket des TCP-Handshakes.
3. ESTABLISHED: Das dritte Paket des TCP-Handshakes, das erste `ACK`-Paket, wurde erkannt.
4. FIN_WAIT: Das erste `FIN`-PAKET wurde erkannt. Die Verbindung wurde abgebaut.
5. CLOSE_WAIT: Das zweite `FIN`-Paket wurde erkannt.
6. LAST_ACK: Das letzte `ACK`-Paket als Antwort auf das zweite `FIN`-Paket wurde erkannt.
7. TIME_WAIT: Nach Ablauf des Zustands LAST_ACK wechselt die Verbindung in den Zustand TIME_WAIT, um Pakete, die während der Übertragung in eine falsche Reihenfolge gebracht wurden, noch zu akzeptieren.
8. CLOSE: Nach dem Ablauf des Zustands TIME_WAIT wechselt die Verbindung in den Zustand CLOSE, um sicherzustellen, dass es nicht zum Konflikt mit neuen Verbindungen kommen kann.

Der Übergang der verschiedenen Zustände wird durch das entsprechende Paket ausgelöst. Lediglich die letzten Übergänge von LAST_ACK nach CLOSE erfolgen durch den Ablauf des Timeouts. Kommt es vorher zum Ablauf eines anderen Timeouts, wird die Verbindung aus der Tabelle entfernt!

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

20 Die NAT-Tabelle

Mit Iptables können Sie auch eine Network Address Translation durchführen. Hierfür verfügt der Kernel über eine eigene NAT-Tabelle, in der sich drei Ketten mit unterschiedlichen Aufgaben befinden: `PREROUTING`, `OUTPUT` und `POSTROUTING`.

20.1 Die NAT-Tabelle und ihre Ketten

Die NAT-Tabelle verfügt über drei Ketten: `PREROUTING`, `OUTPUT` und `POSTROUTING` (Abbildung 20.1). Jede dieser drei Ketten hat eine besondere Aufgabe bei der Network Address Translation. Diese Aufgabe wurde bereits in Abschnitt 5.7 besprochen. Ich möchte sie hier aber kurz wiederholen.

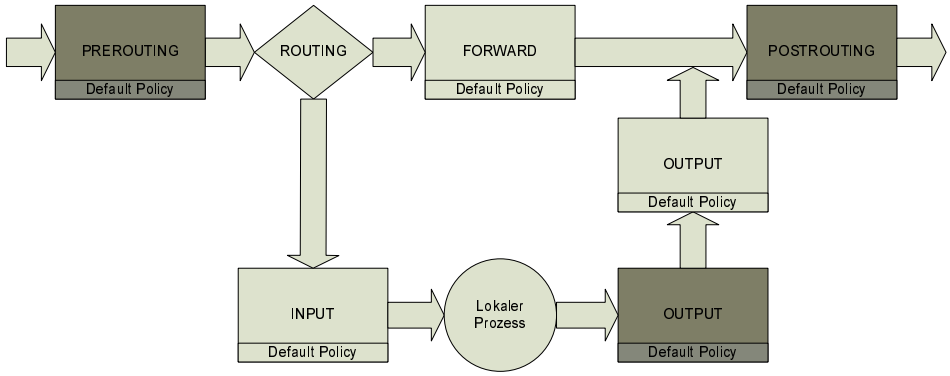


Abbildung 20.1: Die NAT-Tabelle hat drei Ketten.

Um die Tabelle anzuzeigen oder die enthaltenen Ketten zu modifizieren, müssen Sie immer beim Iptables-Befehl die Tabelle spezifisch angeben:

```
# iptables -vnL -t nat
Chain OUTPUT (policy ACCEPT 1937 packets, 94415 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 1934 packets, 94214 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

```
Chain PREROUTING (policy ACCEPT 27 packets, 3364 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Bei der Network Address Translation ändert das System die Adressierung eines Pakets. Es gibt grundsätzlich zwei verschiedene Arten der Network Address Translation (NAT):

- Source-NAT: Hier wird die Absenderadresse geändert.
- Destination-NAT: Hier wird die Zieladresse geändert.

Ein Source-NAT ist nur in der `POSTROUTING`-Kette der NAT-Tabelle erlaubt. Ein Destination-NAT ist nur in der `PREROUTING`- und der `OUTPUT`-Kette erlaubt. Entsprechend der Abbildung 20.1 wird auch sofort der Sinn klar.

Bei dem Source-NAT ändert die Firewall die Absenderadresse. Da das in der `POSTROUTING`-Kette erfolgt, ist sichergestellt, dass die Filterregeln in der `FORWARD`- und der `OUTPUT`-Kette das Paket vor der Adressänderung analysieren. Ihre Filterregeln betrachten also das originale Paket mit der »echten« Absenderadresse.

Bei dem Destination-NAT ändert die Firewall die Zieladresse. Dies passiert in der `PREROUTING`- oder der `OUTPUT`-Kette der NAT-Tabelle und damit vor der Analyse durch die entsprechenden Filterketten. Bei diesem NAT wird die scheinbare Zieladresse durch eine neue tatsächliche Zieladresse ausgetauscht. Die Filtertabelle betrachtet nun also wieder das Paket mit der »echten« Zieladresse!

Achtung

Die NAT-Ketten arbeiten anders als die Ketten der anderen Tabellen. Während die Ketten der anderen Tabellen jedes Paket einer Verbindung sehen und analysieren, ist das bei den NAT-Ketten nicht der Fall. Lediglich das erste Paket einer Verbindung wird von den NAT-Ketten und ihren Regeln analysiert. Wurde die Verbindung von dem Connection Tracking erkannt, die durchzuführende Adressumsetzung ermittelt und die Verbindung in die Tabelle aufgenommen, durchlaufen die weiteren Pakete der Verbindung die Tabelle nicht mehr. Die Tabelle ist daher auch ein sehr schlechter Ort für die Filterung oder die Zählung von Paketen.

Die in der NAT-Tabelle verfügbaren Ziele hängen von der Art des NAT ab. Für ein Source-NAT können Sie die folgenden Ziele verwenden: `MASQUERADE`, `NETMAP`, `SAME` und `SNAT`. Bei dem Destination-NAT stehen die folgenden Ziele zur Verfügung: `BALANCE`, `DNAT`, `NETMAP`, `REDIRECT`, `SAME` und `TPROXY`. Die Ziele `NETMAP` und `SAME` können sowohl für ein Source-NAT als auch für ein Destination-NAT eingesetzt werden.

Zusätzlich kann in der NAT-Tabelle auch das `CONNMARK`-Target eingesetzt werden.

Tipp

Linux ist beim NAT in beiden Richtungen sehr intelligent. Sie müssen mit Ihren Regeln immer nur das NAT in der Richtung des Verbindungsaufbaus definieren. Die Rückrichtung wird dann automatisch vom Kernel richtig gemacht. Bei einem SNAT müssen Sie also nur eine Regel definieren, die die Absenderadresse austauscht. Dass bei den Antwortpaketen der Verbindung dann die Zieladresse ausgetauscht werden muss, damit das Paket den Client erreicht, weiß das System dann automatisch. Bei dem DNAT ist es genauso. Sie müssen lediglich eine Regel definieren, mit der das Ziel ausgetauscht wird. Bei den Antwortpaketen wird dann automatisch der Absender wiederhergestellt.

20.2 Source-NAT

Das Source-NAT ändert die Absenderadresse eines Pakets. Das bedeutet, dass das Paket anschließend eine andere Absenderadresse besitzt. Dies ist häufig bei der Anbindung von Netzwerken an das Internet erforderlich. Lokale Netzwerke werden üblicherweise unter Zuhilfenahme von so genannten privaten IP-Adressen aufgebaut. Diese Adressen werden in dem RFC 1918 definiert. Es handelt sich um die folgenden Adressbereiche:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Sobald Sie Ihre eigenen Netze mit diesen IP-Adressen aufbauen, erzeugen Sie bei einer Anbindung an das Internet keinen IP-Adresskonflikt, da diese nicht im Internet genutzt werden. Für kleine Netze ist der Bereich 192.168.0.0/24 üblich.

Wenn Sie Ihr Netzwerk mit diesen privaten IP-Adressen aufbauen, müssen Sie jedoch am Übergang in das Internet die IP-Adressen umsetzen (Network Address Translation). Tun Sie das nicht, erhalten Sie auf Ihre Anfragen keine Antwort, denn der Client sendet das Paket mit seiner privaten Absenderadresse über seinen Router in das Internet, wo es zum Beispiel einen Webserver erreicht. Der Webserver beantwortet das Paket und schickt sein Antwortpaket an die private Adresse des Clients. Da diese Adressen jedoch im Internet verboten sind, verfügen die Internet-Router auch nicht über die notwendigen Routen. Das Paket wird mit der Fehlermeldung »Ziel nicht erreichbar« (Destination unreachable) verworfen.

Tipp

Unter Umständen können Sie dennoch derartige Pakete über das Internet routen. Das IP-Protokoll erlaubt ein Source Routing. Dabei definiert der Absender die Router, über die das Paket sein Ziel erreicht. Selbst wenn der Router nicht über eine Route verfügt, kann er so das Paket weitersenden. Viele Router unterbinden aber heute das Source-Routing, da es als Sicherheitslücke angesehen wird.

Für diesen Zweck wurde nun das Source-NAT entwickelt. Dabei kann der Router des Clients dessen private IP-Adresse gegen eine offizielle IP-Adresse, deren Ort im Internet bekannt ist, austauschen. Damit die Antworten auch beim Router wieder ankommen, verwendet man hier die offizielle Internet-Adresse des Routers selbst. Grundsätzlich wäre es auch möglich, hier irgendeine andere Adresse einzutragen, jedoch würden die Antwortpakete des Webservers nicht beim Router landen und damit nie den Client erreichen.

Sobald Sie nur eine offizielle IP-Adresse für das Source-NAT von mehreren Clients verwenden, handelt es sich eigentlich nicht mehr um ein NAT (Network Address Translation), sondern um ein NAPT (Network Address and Port Translation).

Bei dem NAPT wird nicht nur die Quell-IP-Adresse, sondern auch der Quellport geändert. Dies ist notwendig, da bei einem SNAT sich die Firewall auch für die Antwortpakete den Rückweg merken muss. Dies erfolgt über den Source-Port. Die Firewall weist jeder genatteten Verbindung eine eindeutige Kombination aus Source-IP-Adresse und -Port zu. Wenn zwei Clients identische Source-Ports verwenden, versucht die Firewall bei der ersten Verbindung den Source-Port beizubehalten. Die Firewall speichert diese Information in ihrer Verbindungstabelle. Bei der zweiten Verbindung verändert die Firewall nicht nur die IP-Adresse, sondern auch den Quellport, um die Antwortpakete den richtigen Clients wieder zuordnen zu können.

Bei der Wahl der Ports behandelt Iptables die Portbereiche unterschiedlich. Zunächst versucht der Kernel, immer den Quellport beizubehalten. Ist jedoch der Port bereits belegt, so versucht der Kernel, Ports < 512 auf andere Ports < 512 zu natten. Ports zwischen 512 und 1023 werden auf Ports wieder in diesem Bereich genattet. Hohe Ports werden durch andere hohe Ports ausgetauscht. Das können Sie durch spezifische Angaben der Ports teilweise modifizieren.

Hinweis

Dies ist übrigens auch der Grund, warum IPsec-Protokolle und GRE-Protokolle so schwer mit SNAT zu behandeln sind. Diese Protokolle besitzen keine Ports. Bei dem NAT von zwei Verbindungen fehlt der Quellport als Differenzierungskriterium für die Antworten.

20.3 Destination-NAT

Das Destination-NAT ist seltener anzutreffen, aber mindestens genauso interessant wie das Source-NAT. Während ein Source-NAT heute allgemein üblich und allen Administratoren bekannt ist, sind das Destination-NAT und die damit verbundenen Möglichkeiten häufig unbekannt. Das Destination-NAT wird häufig auch als Port-Forwarding bezeichnet.

Bei einem Destination-NAT wird die Zieladresse eines Pakets modifiziert. Damit können Sie ein Paket, das eigentlich an die Firewall gerichtet war, auf einen anderen Rechner weiterleiten. So können Sie zum Beispiel sämtliche Anfragen auf dem TCP-Port 80 Ihrer Firewall nach innen auf einen Webserver weiterleiten. Der Client im Internet merkt nicht, dass er in Wirklichkeit nicht mit der Firewall, sondern mit dem privaten Webserver spricht. So können Sie Dienste, die Sie nicht direkt auf der Firewall anbieten wollen, dennoch von außen erreichbar anbieten!

Sie können ein Destination-NAT in der `PREROUTING`- und in der `OUTPUT`-Kette durchführen. In der `PREROUTING`-Kette betrifft das DNAT sämtliche Pakete, die den Rechner von außen erreichen und entweder an ihn lokal gerichtet sind oder weitergeleitet werden müssen. In der `OUTPUT`-Kette betrifft das DNAT nur die lokal erzeugten Pakete.

20.4 MASQUERADE

Häufig möchten Sie ein SNAT durchführen, aber kennen beim Schreiben des Firewall-Skripts noch nicht die IP-Adresse, die Sie später verwenden möchten, da diese sich vielleicht auch dynamisch ändert. Das ist zum Beispiel bei den meisten Internet Service Providern (ISPs) der Fall, die Ihnen die Einwahl per ISDN oder ADSL erlauben. Die IP-Adresse, die der ISP Ihnen zuweist, ändert sich von Einwahl zu Einwahl. Viele Provider führen auch nach einer bestimmten Zeit eine Zwangstrennung durch, um Sie so zu einer neuen Einwahl und einer neuen IP-Adresse zu zwingen. Da Sie jedoch beim Target `SNAT` die IP-Adresse fest definieren müssen, ist dieses Target für diese Zwecke nicht geeignet. Hier können Sie das Target `MASQUERADE` verwenden. Dieses Target verwendet für das SNAT immer die gerade auf der entsprechenden Schnittstelle aktive Adresse. Dazu prüft das `MASQUERADE`-Target, über welche Netzwerkkarte das Paket den Rechner verlässt, und verwendet deren Adresse für das NAT.

Hinweis

Wenn Sie die Netzwerkkarte herunterfahren, werden automatisch alle Verbindungen verworfen, die über diese Netzwerkkarte maskiert wurden. Das ist sinnvoll, da bei einer neuen Einwahl eine neue IP-Adresse zu verwenden ist. Daher sollten Sie, wenn Sie eine statische IP-Adresse verwenden, immer `SNAT` dem `MASQUERADE` vorziehen, auch wenn die Regel ein wenig umständlicher in der Definition ist.

Das MASQUERADE-Target hat eine einzige Option, mit der Sie die zu verwendenden Ports für das NAPT vorgeben können. Dann weicht der Kernel von seiner üblichen Portwahl (siehe oben) ab und verwendet nur Ports in dem vorgegebenen Bereich (`--to-ports port[-port]`). Dann müssen Sie in der Regel aber auch das Protokoll spezifizieren, auf das sich der Portbereich bezieht (z.B. `-p tcp`). Natürlich kann keine weitere Verbindung maskiert werden, sobald die Ports aufgebraucht wurden.

Das MASQUERADE-Target kann nur in der POSTROUTING-Kette verwendet werden.

20.5 NETMAP

Dieses Target aus dem Patch-O-Matic erleichtert Ihnen das NAT von ganzen Netzwerken 1:1. Stellen Sie sich vor, dass Sie für den Zugriff auf ein anderes Netzwerk (zum Beispiel auch das Internet) jede IP-Adresse in Ihrem Netz durch genau eine IP-Adresse aus einem anderen Netz austauschen möchten. Wenn Sie dies statisch und nachvollziehbar mit dem SNAT-Target lösen möchten, benötigen Sie so viele Regeln, wie Sie IP-Adressen verwenden möchten. Dies können Sie mit dem NETMAP-Target vereinfachen.

Stellen Sie sich vor, dass Sie zwei Netze zusammenlegen möchten. Ihr Netz verwendet die IP-Adressen 192.168.0.0/24. Das entfernte Netz verwendet die IP-Adressen 172.16.0.0/16. Grundsätzlich besteht hier kein Problem, da unterschiedliche Adressbereiche verwendet werden. Nun kennt das entfernte Netz allerdings bereits ein weiteres Netz, in dem dieselben IP-Adressen verwendet werden (Abbildung 20.2). Für den Zugriff müssen Sie daher Ihre IP-Adressen durch andere austauschen. Dies ist mit der folgenden Zeile sehr einfach möglich:

```
iptables -t nat -A POSTROUTING -d 172.16.0.0/16 -j NETMAP --to 172.17.0.0/24
```

Nun wird bei jedem Zugriff aus Ihrem Netz die Absenderadresse durch eine Adresse aus dem Bereich 172.17.0.0/24 ersetzt. Das entfernte Netz benötigt natürlich eine Route in das 172.17.0.0/24-Netz. Genauso kann aber auch ein Zugriff aus dem entfernten Netz auf Ihr Netz erfolgen. Hierfür benötigen Sie dann ein NETMAP als Destination-NAT in der PREROUTING-Kette.

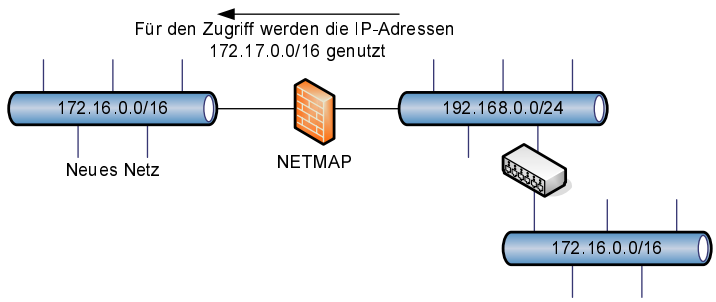


Abbildung 20.2: NETMAP kann Adresskonflikte lösen.

Sie definieren dies genauso einfach:

```
iptables -t nat -A PREROUTING -d 172.17.0.0/24 -j NETMAP --to 192.168.0.0/24
```

Dieses Target wird auch in dem Patch-O-Matic-Kapitel besprochen (siehe Abschnitt 18.3.4).

20.6 SNAT

Dieses Target ist das klassische Source-NAT-Target. Hiermit können Sie die Absender-IP-Adresse durch eine andere ersetzen. Als Ersatz können Sie auch einen Bereich von IP-Adressen angeben. Wenn Sie mehrere IP-Adressen zur Auswahl angeben, führt das `SNAT`-Target ein simples Round-Robin durch.

Um die IP-Adressen anzugeben, verwenden Sie die Option `--to-source <ip>`. Sie können auch einen Bereich angeben: `--to-source <ip-ip>`. Um Tipp-Arbeit zu sparen, können Sie die Option auch mit `--to` abkürzen.

Tipp

Bis Kernel-Version 2.6.10 des Iptables-Befehls können Sie auch die Option mehrfach verwenden, um nicht zusammenhängende IP-Adressen für das `SNAT` zu definieren.

Optional können Sie auch noch einen Port-Bereich angeben und damit den Kernel anweisen, beim Source-NAT nur Ports aus diesem Bereich zu verwenden.

Tipp

Die Verwendung von mehreren IP-Adressen zum Source-NAT ist in Umgebungen mit besonders vielen gleichzeitigen Verbindungen sinnvoll. Da der Kernel den Port als Unterscheidungskriterium zwischen den verschiedenen genatteten Verbindungen verwendet und maximal nur 65.536 Ports zur Verfügung stehen, können maximal pro IP-Adresse gleichzeitig nur diese Anzahl an Verbindungen genattet werden. Bei zwei IP-Adressen verdoppelt sich die Anzahl der möglichen Verbindungen bereits.

20.7 SAME

Dieses Target ähnelt dem `SNAT`- und dem `DNAT`-Target. Wenn Sie jedoch bei diesen Targets einen Bereich von IP-Adressen für das NAT angeben, führen die Targets ein Round-Robin durch. Das bedeutet, dass neue Verbindungen nacheinander jeweils

eine andere IP-Adresse erhalten und dass, sobald alle IP-Adressen aufgebraucht wurden, wieder von vorne begonnen wird. Dieses Verfahren ist jedoch für einige Anwendungen kritisch. Diese Anwendungen verlangen, dass jede Verbindung eines Clients auf dieselbe IP-Adresse genattet wird.

Dies können Sie mit dem `SAME`-Target erreichen. Sie können dieses Target sowohl in der `PREROUTING`- als auch in der `POSTROUTING`-Kette anwenden, je nachdem, ob Sie ein Destination- oder ein Source-NAT machen möchten. Die Verwendung ist sehr einfach. Zwei Beispiele:

```
iptables -t nat -A POSTROUTING -j SAME --to 1.1.1.1-1.1.1.5 --nodst
iptables -t nat -A PREROUTING -j SAME --to 1.1.1.1-1.1.1.5
```

Wird das Target `SAME` in der `POSTROUTING`-Kette für das Source-NAT eingesetzt, so wählt der Kernel nur dann dieselbe IP-Adresse, wenn der Client auch auf denselben Server zugreift. Für den Zugriff auf einen anderen Server darf der Kernel eine andere IP-Adresse wählen. Die Option `--nodst` sorgt bei der Wahl dafür, dass die Ziel-IP-Adresse unberücksichtigt bleibt. Der Client erhält beim Source-NAT für alle Zugriffe auf alle Server immer dieselbe IP-Adresse.

20.8 DNAT

Dies ist das klassische Destination-NAT-Target. Hiermit können Sie die Ziel-IP-Adresse eines Pakets und auch den Zielport des Pakets ändern. Diese Funktion wird häufig für ein Port-Forwarding in ein anderes Netzwerk (zum Beispiel eine DMZ) verwendet. Dieses Target ist nur gültig in der `PREROUTING`- und in der `OUTPUT`-Kette der NAT-Tabelle.

Die neue Ziel-IP-Adresse geben Sie mit der Option `--to-destination ip` an. Sie können genauso wie bei `SNAT` auch einen Bereich angeben (`--to-destination ip-ip`) und die Option auch einfach als `--to` abkürzen. Bis Kernel-Version 2.6.10 können Sie die Option auch mehrfach angeben.

Wenn Sie keinen Port oder Port-Bereich angeben, wird beim Destination-NAT der Port nie modifiziert. Sie können aber auch einen Port oder Port-Bereich definieren, der für das NAT verwendet wird. Dann müssen Sie aber ebenfalls das Protokoll angeben:

```
iptables -A PREROUTING -p tcp --dport 8080 -j DNAT --to 172.16.0.5:3128
```

Wenn Sie einen Bereich von IP-Adressen definieren, führt auch `DNAT` wie `SNAT` ein Round-Robin durch.

20.9 REDIRECT

Dieses Target führt ein spezielles Destination-NAT durch. Daher ist es auch nur in der `PREROUTING`- und `OUTPUT`-Kette erlaubt. Es leitet die Pakete an eine lokale IP-Adresse

um. Dabei verwendet das Target die lokale IP-Adresse der Netzwerkkarte, über die das Paket die Firewall erreicht hat. Lokal erzeugte Pakete werden an 127.0.0.1 umgeleitet. Diese Funktion kann für einen semi-transparenten Proxy verwendet werden. Der Client versucht, auf einen Server im Internet zuzugreifen. Die Firewall fängt die Verbindung ab und leitet sie an einen lokalen Proxy weiter, der an Stelle des Clients die Verbindung aufbaut. Der Client bemerkt die Umleitung nicht. Es handelt sich jedoch nur um einen semi-transparenten Proxy, da der Proxy die Verbindung zum Server nicht mit der IP-Adresse des Clients, sondern mit seiner eigenen IP-Adresse aufbaut. Um alle HTTP-Anfragen an einen transparenten Squid-Proxy weiterzuleiten, können Sie die folgende Iptables-Befehlszeile verwenden:

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth0 -j REDIRECT --to-ports 3128
```

Wenn Sie beim `REDIRECT`-Target keinen Port angeben, wird der Port nicht modifiziert.

Sie können Squid als semi-transparenten Proxy einsetzen. Hierfür müssen Sie bei Squid die folgenden Parameter in der Konfigurationsdatei setzen:

```
http_port 3128
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

20.10 TPROXY

Dieses Target (siehe auch Abschnitt 18.4.25) erlaubt den Aufbau echt transparenter Proxys. Dabei kann der Proxy die Verbindung zum echten Server mit der Absender-IP-Adresse des echten Clients aufbauen. Dieses Target aus dem Patch-O-Matic benötigt daher auch noch zusätzliche Tabellen, in denen es seine Informationen speichert, und angepasste Proxys wie bei der ZORP-Firewall, die von der Firma Balabit entwickelt wird (*http://www.balabit.com*). Diese Firma hat auch die Entwicklung des `TPROXY`-Targets vorangetrieben.

20.11 NAT-Helfermodule

Viele Protokolle sind so kompliziert, dass ein bloßer Austausch der Absender- oder Ziel-IP-Adresse für die Funktion des Protokolls nicht ausreicht. Zum einen kann es sich dabei um Protokolle wie FTP handeln, die weitere Verbindungen dynamisch öffnen und schließen. Weitere Protokolle, die dieses tun, sind: Point-to-Point Tunneling Protocol (PPTP), Internet Relay Chat (IRC), Advanced Maryland Automatic Network Disc Archiver (Amanda), Trivial FTP (TFTP), DirectX8, CuSeeMe, H.323, Microsoft Streaming Media Services (MMS) etc.

Weitere Probleme können auftreten, wenn die IP-Adresse zwar im IP-Header vom NAT getauscht wird, aber zusätzlich noch in dem Paket auftaucht. Auch hier gibt es

einige Protokolle, bei denen das der Fall ist. Ein klassischer Vertreter ist das Simple Network Management Protocol (SNMP).

Damit diese Protokolle richtig gehandhabt werden, müssen Sie zusätzliche Kernelmodule laden, die nicht nur die IP-Header der Pakete betrachten, sondern auch den Inhalt analysieren und dort vorhandene IP-Adressen austauschen beziehungsweise dynamisch ausgehandelte neue Verbindungen erkennen und als erwartete Verbindung (Expectation) in die Tabelle eintragen. Diese können Sie dann mit dem Zustand `RELATED` erlauben.

Das Laden dieser Module ist sehr einfach und erfolgt sinnvollerweise zu Beginn Ihres Firewall-Skripts:

```
modprobe ip_nat_ftp
```

Wenn die Module Abhängigkeiten besitzen, erkennt der `modprobe`-Befehl diese und lädt automatisch auch die weiteren benötigten Module. Bei einigen Modulen können Sie zum Lade-Zeitpunkt weitere Optionen angeben, mit denen Sie das Verhalten modifizieren können (zum Beispiel FTP, siehe Abschnitt 32.10). Die Informationen über die möglichen Optionen erhalten Sie am einfachsten mit dem `modinfo`-Befehl.

20.12 CONNMARK-Target

Mit diesem Ziel können Sie Verbindungen markieren. Dieses Ziel unterstützt in der NAT-Tabelle die beiden folgenden Optionen:

- `--set-mark <markierung>[/<maske>]`: Hiermit setzen Sie die Markierung. Wenn Sie eine Maske angeben, werden nur diese Bits modifiziert.
- `--save-mark [--mask <maske>]`: Hiermit übertragen Sie eine Paketmarkierung (siehe Abschnitt 21.2.7) auf die Verbindung. Diese können Sie in der Mangle-Tabelle mit dem `CONNMARK`-Ziel wiederherstellen.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

21 Die Mangle-Tabelle

Die Mangle-Tabelle ist der Ort, wo Sie spezielle Paket-Modifikationen vornehmen können. Sie können hier die Type-of-Service-Bits ändern, Pakete markieren oder das ECN-Bit abschalten.

21.1 Die Ketten der Mangle-Tabelle

Je nach Ihrem Kernel weist die Mangle-Tabelle zwei oder fünf Ketten auf. Bis einschließlich 2.4.17 gab es nur die beiden Ketten PREROUTING und OUTPUT in der Mangle-Tabelle. Anschließend kamen auch noch die Ketten INPUT, FORWARD und POSTROUTING hinzu. Diese Ketten werden immer vor ihren entsprechenden Brüdern in den Tabellen NAT und Filter durchlaufen. Das bedeutet, dass Sie die Pakete modifizieren können, bevor die NAT-Regeln und die Filter-Regeln das Paket verarbeiten.

21.2 Aktionen der Mangle-Tabelle

Es gibt einige Aktionen (Targets), die nur in der Mangle-Tabelle erlaubt sind. Hierbei handelt es sich um: `CLASSIFY`, `CONNMARK`, `DSCP`, `ECN`, `IPMARK`, `IPV4OPTSSTRIP`, `MARK`, `ROUTE`, `TOS`, `TTL` und `XOR`. Dabei ist das Target `CONNMARK` ein Sonderfall, da es sowohl in der NAT- als auch in der Mangle-Tabelle mit unterschiedlichen Optionen genutzt werden kann.

Diese Targets möchte ich nun in diesem Kapitel vorstellen. Natürlich können Sie auch `ACCEPT`, `DROP`, `REJECT` etc. in der Mangle-Tabelle nutzen. Diese Targets habe ich aber bereits an anderer Stelle vorgestellt.

21.2.1 CLASSIFY

Linux unterstützt Class-based Queueing (CBQ). Mit diesem Ziel können Sie direkt ohne Firewall-Markierung ein Paket einer bestimmten Klasse zuweisen. Hierzu geben Sie mit der zusätzlichen Option `--set-class` die Major:Minor-Klasse an:

```
$IPTABLES -t mangle -A POSTROUTING -p tcp --dport 22 \
  -j CLASSIFY --set-class 1:10
```

Sie müssen mit dem Kommando `tc` natürlich auch eine entsprechende Klasse angelegt haben.

21.2.2 CONNMARK

Mit diesem Target können Sie eine Verbindung markieren. Dies ist nicht dasselbe wie die Markierung eines Pakets mit dem `MARK`-Target (siehe Abschnitt 21.2.7). Wenn Sie dennoch die Markierung auf das Paket übertragen möchten, können Sie das mit der Option `--restore-mark` des `CONNMARK`-Targets erreichen. Diese Option dürfen Sie nur in der Mangle-Tabelle verwenden.

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j CONNMARK --set-mark 80
iptables -t mangle -A FORWARD -m connmark --mark 80 -j CONNMARK --restore-mark
```

21.2.3 DSCP

Mit diesem Target können Sie die Diffserv-Class-Point-Bits im ToS-Header eines IP-Pakets setzen. Dieses DSCP-Feld wird in RFC 2474 beschrieben. Diese Werte werden häufig von Routern und Switches verwendet, um die Priorität von Paketen festzulegen.

Hierfür stehen Ihnen zwei Optionen zur Verfügung:

- `--set-dscp <wert>`. Hiermit können Sie das DSCP-Feld mit einem numerischen Wert füllen.
- `--set-dscp-class <klasse>`. Hiermit können Sie eine DiffServ-Klasse auswählen.

21.2.4 ECN

Die Explicit Congestion Notification ist eine neue Methode, die in dem RFC 3168 beschrieben wurde. Hiermit können zwei Kommunikationspartner, wenn beide ECN unterstützen, Verstopfungen der Verbindung vor deren Auftreten erkennen und durch eine Reduktion der Sendeleistung reagieren. So ist die Wahrscheinlichkeit sehr groß, dass die Verstopfung erst gar nicht auftritt.

Leider verwerfen viele alte und auch noch einige moderne Firewalls Pakete, die ECN verwenden, da die hier verwendeten Bits im IP- und TCP-Header bis zur Definition des RFC 3168 reserviert waren und lediglich von Werkzeugen wie Nmap verwendet wurden.

Wenn Sie dennoch ECN verwenden möchten, stellen Sie wahrscheinlich fest, dass die Kommunikation mit einigen Zielen nicht funktioniert. Dann können Sie für diese Ziele die ECN-Bits entfernen lassen:

```
iptables -t mangle -A PREROUTING -p tcp -d $ECN_BLACKHOLE -j ECN --ecn-tcp-remove
```

21.2.5 IPMARK

Dieses Target aus dem Patch-O-Matic erlaubt es, automatisch Pakete entsprechend ihrer IP-Adresse zu markieren. Dieses Target darf in der Mangle-Tabelle in den PREROUTING-, FORWARD- und POSTROUTING-Ketten angewendet werden. Da es bereits in Abschnitt 18.4.2 besprochen wurde, verweise ich an dieser Stelle darauf.

21.2.6 IPV4OPTSSTRIP

Mit diesem Target aus dem Patch-O-Matic können Sie sämtliche IP-Optionen eines Pakets entfernen. Es erlaubt Ihnen nicht, zwischen den verschiedenen IP-Optionen zu unterscheiden. Daher ist die Anwendung sehr einfach:

```
iptables -t mangle -A PREROUTING -j IPV4OPTSSTRIP
```

21.2.7 MARK

Hiermit können Sie eine Netfilter-Markierung des Pakets vornehmen. Diese Firewall-Markierung können Sie später mit dem Test `-m mark --mark` wieder prüfen oder auch in Zusammenhang mit dem iproute2-Paket nutzen. Um zum Beispiel für bestimmte Pakete eine andere Routing-Tabelle zu nutzen, können Sie die folgenden Befehle nutzen:

```
iptables -t mangle -A PREROUTING -p tcp --dport 25 -j MARK --set-mark 25
ip route add table 25 default via 192.168.0.5
ip rule add fwmark 25 table 25
```

Hiermit markieren Sie alle TCP-Pakete an den Port 25 mit der entsprechenden Markierung. Anschließend erzeugen Sie eine zusätzliche Routing-Tabelle mit der Nummer 25, in der Sie ein weiteres Default-Gateway eintragen. Damit diese Routing-Tabelle auch genutzt wird, definieren Sie eine Regel, die alle Pakete mit der Markierung 25 über diese Tabelle routet.

21.2.8 ROUTE

Mit dem `ROUTE`-Target aus dem Patch-O-Matic können Sie die beim `MARK`-Target beschriebene Problemstellung leichter lösen, da Sie ohne zusätzliche Routing-Tabelle und Regel direkt in der Firewall-Regel ein neues Gateway für die Pakete angeben können. Die Verwendung dieses Targets wird in Abschnitt 18.4.3 genauer beschrieben.

21.2.9 TOS

Hiermit können Sie die Type-of-Service-Bits im IP-Header modifizieren. Einige Betriebssysteme, wie Linux, werten diese Bits aus. Hierfür verwenden Sie `-j TOS --set-tos <wert>`. Die zur Verfügung stehendenden Werte zeigt Ihnen der Befehl `iptables -j TOS -h` an:

```
TOS target v1.3.0 options:
  --set-tos value                 Set Type of Service field to one of the
                                  following numeric or descriptive values:
                                   Minimize-Delay 16 (0x10)
                                   Maximize-Throughput 8 (0x08)
                                   Maximize-Reliability 4 (0x04)
```

```
Minimize-Cost 2 (0x02)
Normal-Service 0 (0x00)
```

21.2.10 TTL

Dieses Target ermöglicht es Ihnen, den TTL-Wert eines IP-Pakets zu modifizieren. Das Netfilter-Team rät stark von der Verwendung dieses Targets ab. Bei falscher Anwendung erzeugen Sie hiermit Endlosschleifen!

Mit diesem Target können Sie auf Ihrer Firewall den TTL-Wert jedes Pakets, das die Firewall passiert, um eins erhöhen. Wenn Ihre Firewall selbst nicht auf den `traceroute`-Befehl reagiert, aber die Time-Exceeded-Mitteilungen durchlässt, ist die Firewall scheinbar für Traceroute unsichtbar, da für jeden TTL-Wert eine Antwort zurückkommt. Die Reduktion des TTL-Wertes durch die Firewall, die zum Ausfall dieser Antwort führen würde, wird von Iptables durch die Erhöhung wieder rückgängig gemacht.

Das Target hat drei Optionen:

- `--ttl-set <wert>`. Hiermit setzen Sie fest einen neuen Wert fest.
- `--ttl-dec <wert>`. Hiermit ziehen Sie den Wert von dem aktuellen TTL-Wert ab.
- `--ttl-inc <wert>`. Hiermit addieren Sie die angegebene Zahl zum aktuellen TTL-Wert hinzu.

21.2.11 XOR

Dieses Target aus dem Patch-O-Matic kann eine »Verschlüsselung« des Pakets mittels einer XOR-Verknüpfung durchführen. Da dieses Target bereits in Abschnitt 18.4.6 beschrieben wurde, gehe ich hier nicht näher darauf ein.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

22 Die Raw-Tabelle

Die Raw-Tabelle wurde eingeführt, um Pakete, bevor sie vom Connection Tracking erfasst werden, bereits behandeln zu können. Die wichtigste Idee ist hierbei die Umgehung des Connection Tracking für bestimmte Pakete. Dies ist erstmalig mit der Raw-Tabelle möglich.

22.1 Die Raw-Tabelle

Die Raw-Tabelle besitzt zwei Ketten: `PREROUTING` und `OUTPUT`. Außerdem existieren zwei Targets, die nur in der Raw-Tabelle verwendet werden dürfen: `NOTRACK` und `TRACE`.

Mit dem Erscheinen der Raw-Tabelle existiert nun auch ein neuer Zustand, der mit dem `state`-Test geprüft werden kann: `UNTRACKED`.

Die Raw-Tabelle bietet Ihnen den ersten Zugriff auf die ankommenden (PREROUTING) und die lokal erzeugten (OUTPUT) Pakete. Neben den beiden Spezial-Targets `NOTRACK` und `TRACE` können Sie natürlich auch die eingebauten Targets `DROP` und `ACCEPT` verwenden. Außerdem verfügen die Ketten natürlich auch über Default-Policies, die Sie mit dem Befehl `iptables -t raw -P PREROUTING DROP` setzen können.

Jedoch ist die Tabelle in erster Linie dazu gedacht, dass Sie Ausnahmen von der Verbindungsüberwachung definieren können. Damit können Sie bestimmte Pakete, bei denen eine Verbindungsüberwachung sinnlos oder überflüssig ist, von dieser ausnehmen. Diese Funktion wird zum Beispiel von dem ct_sync-Cluster-Modul (siehe Abschnitt 26.6) genutzt, damit die Synchronisationsmeldungen des Firewall-Clusters nicht ebenfalls in der Zustandsüberwachung landen. Auch weitere Protokolle, die Sie unbedingt annehmen möchten und bei denen eine Zustandsüberwachung nicht sinnvoll ist (zum Beispiel IPsec-ESP), können Sie so ausklammern.

```
iptables -t raw -A PREROUTING -p 50 -j NOTRACK
iptables -A FORWARD -p 50 -j ACCEPT
```

Die Möglichkeit der Paketverfolgung ist mit dem `TRACE`-Target aus dem Patch-O-Matic gegeben. Damit können Sie zu Testzwecken genau den Weg eines Pakets durch Ihr Regelwerk und durch alle Tabellen und Ketten genau verfolgen. Dieses Target wurde aber bereits im Patch-O-Matic Kapitel besprochen (siehe Abschnitt 18.4.5).

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

23 Das /proc-Dateisystem

Linux besitzt einen sehr mächtigen TCP/IP-Stack und Paketfilter. Das Verhalten dieses Stacks und des Paketfilters ist sehr flexibel. Wenn Sie die Flexibilität kennen lernen möchten und den Stack oder den Paketfilter anpassen und modifizieren möchten, müssen Sie sich mit dem `/proc`-Dateisystem beschäftigen. Dieses virtuelle Dateisystem gibt Ihnen lesenden und schreibenden Zugriff auf wesentliche Variablen des Betriebssystems. Hierzu gehören auch der Netzwerkstapel und der Paketfilter.

23.1 Einführung in /proc

Das `/proc`-Dateisystem ist ein virtuelles Dateisystem, in dem der Kernel viele Variablen des Betriebssystems für den lesenden und häufig auch schreibenden Zugriff anbietet. Wesentliche Informationen des Betriebssystems können (nur) über diese Struktur ausgelesen werden.

Wenn Sie sich den Inhalt des `/proc`-Verzeichnisses ansehen, finden Sie sowohl Verzeichnisse als auch Dateien vor (Abbildung 23.1).

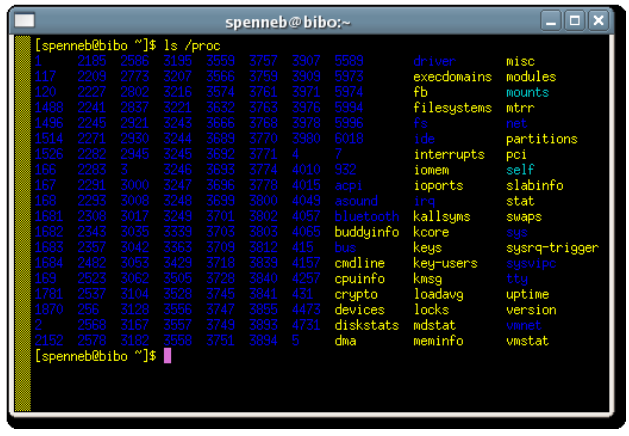


Abbildung 23.1: Das /proc-Dateisystem enthält sowohl Informationen über Prozesse als auch das laufende Betriebssystem.

Ein großer Teil der Verzeichnisse stellt Informationen über die laufenden Prozesse zur Verfügung. Jedes Verzeichnis mit einer Zahl als Verzeichnisnamen enthält Informationen über den Prozess mit der entsprechenden Prozess-ID. Die weiteren Einträge und Verzeichnisse enthalten Informationen über das laufende Betriebssystem und erlauben teilweise auch die Konfiguration dieser Parameter. So enthält zum Beispiel der Eintrag `/proc/cpuinfo` Informationen über den von dem Betriebssystem gefundenen Prozessor. In der Datei `/proc/partitions` finden Sie Informationen über die von dem Betriebssystem erkannten Partitionen:

```
$ cat /proc/partitions
major minor  #blocks  name

   3     0   78150744 hda
   3     1     104391 hda1
   3     2   78043770 hda2
  22     0   78150744 hdc
  22     1   78150712 hdc1
 253     0   75956224 dm-0
 253     1    2031616 dm-1
 253     2   20971520 dm-2
 253     3   20971520 dm-3
 253     4   20971520 dm-4
$ cat /proc/cmdline
ro root=/dev/VolGroup00/LogVol00
```

Die Datei `/proc/cmdline` enthält Informationen über die Kommandozeile, mit der der laufende Kernel aufgerufen wurde.

Teilweise können Sie die Werte in den (virtuellen) Dateien auch verändern. So definiert die Datei `/proc/sys/net/ipv4/icmp_echo_ignore_all`, ob der Kernel auf ICMP-Echo-Pakete reagiert oder diese ignoriert. Diese Datei kann den Wert 0 oder 1 enthalten. Ein Wert von 0 bedeutet, dass diese Funktion nicht aktiv ist. Ein Wert von 1 bedeutet in diesem Fall, dass der Kernel diese Pakete ignoriert.

Sie können das selbst sehr einfach prüfen und nachvollziehen. Zeigen Sie zunächst den Wert der Datei an:

```
$ cat /proc/sys/net/ipv4/icmp_echo_ignore_all
0
```

Starten Sie nun in einem eigenen Fenster den Ping-Befehl (`ping 127.0.0.1`). Sie sollten erfolgreich Ihren eigenen Rechner pingen können. Falls es nicht funktioniert, prüfen Sie bitte, ob eine Firewall aktiv ist und deaktivieren Sie diese im Zweifelsfall.

Während der Ping läuft, ändern Sie nun den Inhalt der Datei:

```
$ echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_all
```

Nun sollte der Ping sofort aufhören. Sobald Sie die 0 wieder in die Datei schreiben, läuft der Ping weiter. Anstelle des `echo`-Kommandos können Sie auch den Befehl `sysctl` verwenden. Dieser Befehl erwartet den Namen der Variablen etwas anders:

```
$ /sbin/sysctl net.ipv4.icmp_echo_ignore_all
net.ipv4.icmp_echo_ignore_all = 1
```

Entfernen Sie `/proc/sys/` von dem Pfad der Datei, und ersetzen Sie alle weiteren `/` (Schrägstrich) durch einen Punkt. Allerdings kann der Befehl auch die Schrägstriche statt Punkte verwenden:

```
$ /sbin/sysctl net/ipv4/icmp_echo_ignore_all
net.ipv4.icmp_echo_ignore_all = 0
```

Wenn Sie den Befehl nur mit dem Namen der Variablen verwenden, zeigt der Befehl nur den aktuellen Wert an. Wenn Sie den Wert ändern möchten, verwenden Sie zusätzlich die Option `-w` und geben den neuen Wert an:

```
$ /sbin/sysctl -w net/ipv4/icmp_echo_ignore_all=1
net.ipv4.icmp_echo_ignore_all = 1
```

Alle so durchgeführten Änderungen sind nach einem Neustart verloren und müssen neu gesetzt werden. Viele Distributionen verwenden hierzu inzwischen die Datei `/etc/sysctl.conf`. Sie können die Änderungen, die von der Distribution automatisch beim Systemstart durchgeführt werden sollen, in dieser Datei angeben:

```
# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8) and
# sysctl.conf(5) for more details.

# Controls IP packet forwarding
net.ipv4.ip_forward = 0

# Controls source route verification
net.ipv4.conf.default.rp_filter = 1

# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0
```

Im Folgenden werde ich die einzelnen Variablen vorstellen, die für die Konfiguration des Paketfilters und TCP/IP-Stacks interessant sind.

23.2 /proc/net/

Alle Einträge in diesem Verzeichnis sind lediglich lesbar. Ein Schreibzugriff ist nicht vorgesehen. Die Dateien dienen lediglich informativen Zwecken.

23.2.1 ip_conntrack

Dies ist die Connection Tracking-Tabelle. Alle bekannten Verbindungen werden in dieser Tabelle aufgenommen, sobald das `ip_conntrack`-Modul geladen wurde.

```
tcp      6 431842 ESTABLISHED src=192.168.0.108 dst=217.160.128.61 sport=56468 dport=993
  packets=79 bytes=5788 src=217.160.128.61 dst=192.168.0.108 sport=993 dport=56468
  packets=51 bytes=5864 [ASSURED] mark=0 use=1
```

Ab Kernelversion 2.6.10 und entsprechender Konfiguration (`CONFIG_IP_NF_CT_ACCT=y`) werden auch die Paket- und Byte-Zähler für die Verbindung angezeigt.

23.2.2 ip_conntrack_expect

Ab Kernel 2.6.9 werden die Expectations in dieser Datei angezeigt. Expectations sind Verbindungen, die von einem Conntrack-Helper-Modul erkannt werden und als `RELATED`-Verbindungen erlaubt werden.

23.2.3 ip_tables_*

Diese drei Dateien (`ip_tables_matches`, `ip_tables_targets` und `ip_tables_names`) enthalten die Namen der aktuell geladenen Matches (Tests), Targets (Ziele) und Tables (Tabellen). Sobald eine Regel einen neuen Match oder ein neues Target benötigt, das durch ein Modul zur Verfügung gestellt wird, wird das Modul geladen, und dessen Name taucht in diesen Dateien auf.

23.3 /proc/sys/net/ipv4

Dieses Verzeichnis enthält Variablen, auf die Sie sowohl lesend als auch schreibend zugreifen können. In vielen Fällen sollten Sie jedoch sich sehr genau überlegen, ob es sinnvoll ist, die entsprechenen Parameter zu verändern, da dies durchaus Auswirkungen (positive wie negative) auf die Leistungsfähigkeit des Systems haben kann.

23.3.1 icmp_*

Diese Variablen betreffen das ICMP-Protokoll. Falls Sie mehr oder weniger Optionen besitzen, so hängt dies von der verwendeten Kernelversion ab.

icmp_echo_ignore_all

Diese Variable entscheidet, ob der Kernel alle ICMP-Echo-Pakete (Ping) ignorieren soll. Schreiben Sie in diese Datei eine 1, und Ihr System wird auf ein Ping grundsätzlich nicht mehr reagieren.

icmp_echo_ignore_broadcasts

Wenn Sie diese Variable auf den Wert 1 setzen, ignoriert der Kernel alle Echo-Request-Pakete (Ping) an die Broadcast-Adresse. Üblicherweise beantworten alle Linux-/Unix-Betriebssysteme einen Echo-Request an ihre Broadcast-Adresse. So können Sie sehr leicht in einem Netzwerk alle verfügbaren Unix-Systeme ermitteln. Da aber viele Router in der Vergangenheit (und auch heute noch) derartige Broadcast-Ping-Anfragen nicht verworfen haben, konnte damit eine Verstärkung des Verkehrs erzeugt werden. Sie senden ein Ping an die Broadcast-Adresse eines Netzwerks mit 10 Unix-Rechnern und erhalten 10 Antworten zurück. Wenn Sie die Absenderadresse fälschen (IP-Spoofing), können Sie so einen anderen Rechner mit Ping-Antworten überschwemmen. Dieser Angriff trägt den Namen Smurf-Angriff. Die Netzwerke werden als Smurf Amplifier Networks bezeichnet. Auch heute gibt es noch derartige Netzwerke, deren Router die Broadcast-Pakete nicht verwerfen (*http://www.powertech.no/smurf/*). Um zu verhindern, dass Ihr System für diesen Angriff genutzt wird, sollten Sie die Beantwortung von Broadcast-Ping-Anfragen abschalten:

```
sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
```

icmp_errors_use_inbound_ifaddr

Normalerweise versendet ein Linux-System eine Fehlermeldung mit der Absenderadresse der Netzwerkkarte, über die die Fehlermeldung das System verlässt. Dies ist nicht zwingend die Netzwerkkarte, auf der die Fehlermeldung aufgetreten ist. Wird diese Option (ab 2.6.12) gesetzt, so wird die Fehlermeldung mit der Absenderadresse der Netzwerkkarte gesendet, auf der der Fehler auftrat. Da dies die Fehlersuche stark vereinfacht, sollte diese Variable aktiviert werden.

icmp_ignore_bogus_error_messages

Einige Router verletzen den RFC 1122 (Requirements for Internet Hosts – Communication Layers) und versenden Fehlermeldungen als Antwort auf Broadcast-Mitteilungen. Normalerweise protokolliert der Kernel diese Tatsache. Wenn Sie diese Variable aktivieren, protokolliert der Kernel dies nicht mehr und kann so Ihre Protokolldateien nicht mit unnötigen Meldungen füllen. Ich empfehle die Aktivierung dieser Option.

icmp_ratelimit

Um Denial-of-Service-Angriffe mit ICMP-Nachrichten zu verhindern und allgemein den Netzwerkverkehr zu reduzieren, bieten diese und die nächste Variable Ihnen die Möglichkeit, die Versendung von ICMP-Meldungen zu beschränken. In dieser Variable definieren Sie, wie viel Jiffies der Kernel zwischen zwei bestimmten ICMP-Meldungen an einen bestimmten Rechner warten soll. Ein Jiffie entspricht auf der i386-Plattform 1/100 Sekunde. Der Default-Wert dieser Variable ist 100. Das bedeutet, dass maximal einmal pro Sekunde eine bestimmte IMCP-Nachricht an denselben Rechner versendet wird. Ein Wert von 0 schaltet dieses Verhalten ab.

icmp_ratemask

Diese Variable definiert, welche ICMP-Nachrichten das Rate-Limiting betrifft. Hierzu bedient sich diese Variable einer Bitmaske:

```
Bits:    IHGFEDCBA9876543210
Default: 0000001100000011000 (6168)

0 Echo Reply
1 Nicht definiert
2 Nicht definiert
3 Destination Unreachable *
4 Source Quench *
5 Redirect
8 Echo Request
B Time Exceeded *
C Parameter Problem *
D Timestamp Request
E Timestamp Reply
F Info Request
G Info Reply
H Address Mask Request
I Address Mask Reply
```

23.3.2 igmp_*

Das Internet-Group-Management-Protokoll (IGMP) wird für die Verwaltung von Multicast-Gruppen verwendet. Der Kernel verfügt über zwei Variablen, die das Verhalten dieses Protokolls beeinflussen.

igmp_max_memberships

Diese Variable definiert die maximale Anzahl an Multicast-Gruppen, bei denen das Linux-System Mitglied werden kann. Üblicherweise müssen Sie diesen Wert nicht modifizieren.

igmp_max_msf

Diese Datei definiert die maximale Anzahl der Multicast-Source-Filter (MSF). Das IGMPv3-Protokoll erlaubt es einer Applikation, Filter auf Multicast-Gruppen zu definieren, mit denen die Absender der Multicast-Nachrichten eingeschränkt werden können. Dann akzeptiert der Linux-Kernel diese Nachrichten nur noch von wenigen Systemen. Diese Variable definiert, wie viele Multicast-Source-Filter gesetzt werden dürfen.

23.3.3 inet_peer_*

Ein Inet-Peer ist ein anderer Rechner im Internet, mit dem unser System im Moment kommuniziert. Für jeden derartigen Peer speichert unser System langlebige Informationen in einer eigenen Struktur. Aktuell handelt es sich hierbei nur um die IP-Identifikationsnummer (ID) des nächsten Pakets. Diese Nummer wird benötigt, um bei der Defragmentierung der Pakete die richtigen Fragmente eines Pakets zu erkennen. Diese weisen alle dieselbe IP-ID auf. Diese Variablen definieren, wie diese Strukturen verwaltet werden.

Achtung

Da ein Linux-System per Default Path-MTU-Discovery verwendet und so eine Fragmentierung des Pakets ausschließen kann, benötigen die versandten Pakete keine IP-ID. Daher werden in diesem Fall der entsprechende Code und diese Variablen nicht verwendet.

Da diese Variablen in den meisten Umgebungen nicht genutzt werden, werden sie hier nicht weiter erläutert. Sie finden eine aktuelle Dokumentation in dem Quellcode Ihres Kernels unter `Documentation/networking/ip-sysctl.txt`.

23.3.4 ip_*

Diese Variablen beeinflussen das IP-Protokoll.

ip_autoconfig

Der Kernel kann selbst die Protokolle DHCP oder BOOTP verwenden, um eine Autokonfiguration der Netzwerkkarten vorzunehmen. Dazu muss der Kernel entsprechend konfiguriert sein (`IP_PNP=y`).

ip_conntrack_max

Diese Variable definiert die maximal unterstützten Verbindungen in der Connection Tracking-Tabelle. Der Default-Wert hängt von dem zur Verfügung stehenden Arbeitsspeicher ab. Auf einer Firewall ist es sinnvoll, diesen Wert zu erhöhen. Dann sollten Sie aber auch die Hashsize erhöhen (siehe Abschnitt 19.2).

ip_default_ttl

Hiermit setzen Sie den Time-to-Live-Wert (TTL) der von dem Linux-System versandten Pakete. Alle normalen Pakete erhalten diesen TTL-Wert. Nach der entsprechenden Anzahl von Hops wird das Paket dann verworfen. Jeder Router, der von einem Paket auf dem Weg zum Ziel passiert wird, ist ein Hop. Hiermit wird verhindert, dass eine Routerfehlkonfiguration zu Paketen führt, die ewig transportiert

werden. ICMP-Fehlermeldungen werden von Linux unabhängig von diesem Wert immer mit einem TTL von 255 versendet.

ip_dynaddr

Wenn Sie in Ihrer Firewall dynamische IP-Adressen auf der externen Netzwerkkarte bei gleichzeitigem Masquerading verwenden, sollten Sie diese Variable aktivieren, um fehlerfreie Verbindungen zu ermöglichen. Ansonsten kann es zu Problemen bei der ersten Verbindung kommen, die die Einwahl in das Internet antriggert. Um dies zu verstehen, stellen Sie sich vor, Ihr Firewall-System sei im Moment nicht mit dem Internet verbunden. Ein Client hinter der Firewall möchte auf das Internet zugreifen. Er versendet sein erstes Paket, um die Verbindung aufzubauen. Die Firewall filtert das Paket, maskiert es mit der aktuellen IP-Adresse der externen Netzwerkkarte und übergibt das Paket an die Netzwerkkarte. Dies triggert die Einwahl, und das System baut die Internetverbindung auf. Dabei erhält das System eine neue IP-Adresse auf der externen Netzwerkkarte. Wenn nun das erste Paket unverändert versendet werden würde, hätte es die falsche Absender-IP-Adresse. Diese Variable erzwingt eine erneute Maskierung dieses ersten Pakets.

Wenn Sie eine 1 in die Variable schreiben, aktivieren Sie das Verhalten. Ein Wert größer 1 führt zusätzlich jedes Mal zur Protokollierung.

ip_forward

Diese Variable schaltet für sämtliche Netzwerkkarten des Linux-Systems die Weiterleitung (Forwarding) ein. Wenn diese Variable den Wert 0 enthält, leitet der Linux-Kernel keine Pakete zwischen zwei Netzwerkkarten weiter.

ip_local_port_range

Diese Datei enthält zwei Zahlen, die den Bereich der lokal erlaubten Client-Ports definieren. Wenn Sie diese Variable verändern möchten, müssen Sie auch gleichzeitig beide Zahlen in diese Variable schreiben:

```
echo "4096 7000" > ip_local_port_range
```

Die erste angegebene Nummer ist der kleinste Port, der verwendet werden kann, während die zweite Nummer der höchste Port ist. Wählen Sie hier keine Ports kleiner 1024, um Problemen vorzubeugen. Üblich sind hier 32768 und 61000.

ip_nonlocal_bind

Üblicherweise kann eine Applikation sich nur auf lokal definierte IP-Adressen binden. Wenn diese Variable gesetzt ist, kann eine Applikation auch IP-Adressen verwenden, die auf dem System nicht definiert sind, und mit dieser Adresse als Absenderadresse Pakete versenden und Pakete entgegennehmen. Diese Funktion wird für einen echten transparenten Proxy benötigt, der die Verbindung zum Server mit der IP-Adresse des echten Clients aufbaut.

ip_no_pmtu_disc

Der Linux-Kernel verwendet per Default die Path Maximum Transmission Unit Discovery (PMTU-Discovery). Damit verhindert der Linux-Kernel, dass eine Fragmentierung der Pakete unterwegs auftritt und bei gleichzeitigem Fragmentverlust unnötig viele Pakete wiederholt gesendet werden müssen. In einigen Umgebungen führt dieses Verhalten jedoch zu Problemen. Dann können Sie diese Funktion mit dieser Variablen abschalten (1).

23.3.5 ipfrag_*

Diese Parameter definieren, wie das Linux-System eine Defragmentierung durchführen soll.

ipfrag_*_thresh

Diese beiden Variablen definieren den Speicherbereich, der für die Speicherung der Fragmente bei der Defragmentierung genutzt wird. Der genutzte Speicher schwankt zwischen dem `ipfrag_low_thresh`- und `ipfrag_high_thresh`-Wert.

ipfrag_time

Dieser Wert definiert, wie lange Fragmente für eine Defragmentierung aufbewahrt werden. Ist innerhalb dieser Zeit keine Defragmentierung möglich, sendet der Rechner eine ICMP-Time-Exceeded-Fehlermeldung und verwirft das unvollständige Paket.

ipfrag_secret_interval

Ältere Kernel besitzen eine Sicherheitslücke in der Fragmentierung, die einen Denial-of-Service der Defragmentierung ermöglichen (CAN-2003-0364). Um dieses zu verhindern, wurde ein Secret eingeführt, so dass der Angreifer die benötigten Pakete nicht mehr vorhersagen kann. Dieses muss zur Sicherheit in regelmäßigen Abständen neu berechnet werden. Das Intervall in Sekunden wird in dieser Variable definiert.

ipfrag_max_dist

Diese neue Variable des Linux-Kernels 2.6.14 definiert die maximale Unordnung, mit der Fragmente den Kernel erreichen dürfen.

23.3.6 tcp_*

Hier sind sehr viele Variablen vorhanden, die das Verhalten des TCP-Protokolls beeinflussen.

tcp_abort_on_overflow

Diese Variable erzwingt einen Reset neuer Verbindungen, wenn der dazugehörige Dienst die neuen Verbindungen nicht schnell genug entgegennehmen kann. Bevor Sie diese Variable setzen, sollten Sie immer versuchen, den Dienst zu optimieren. Wenn es sich nicht um einen Dauerzustand handelt, sondern nur punktuell Probleme auftreten, kann diese Funktion hilfreich sein.

tcp_adv_win_scale

Die Variable `tcp_rmem` definiert den für den Empfang von Paketen reservierten Speicher eines Sockets. Dieser Speicher wird für das TCP-Window und den Applikationspuffer aufgeteilt. Diese Variable definiert dieses Verhältnis. Ist der Wert der Variable positiv, wird für das TCP-Window $1/(2^{\text{tcp\_adv\_win\_scale}})$ genutzt. Bei dem Default-Wert von 2 wird also ein Viertel des Speichers für das TCP-Window reserviert. Bei einem negativen Wert wird $1\text{-}1/(2^{-\text{tcp\_adv\_win\_scale}})$ verwendet – bei einem Wert von -2 also drei Viertel des Speichers.

tcp_app_win

Auch diese Variable definiert, wie viel Speicher für den Applikationspuffer eines Sockets maximal reserviert wird. Der Kernel nutzt folgende Formel: $\text{window}/(2^{\text{tcp\_app\_win}})$. Der Wert muss immer mindestens der Maximum Segment Size (MSS) entsprechen.

tcp_bic*

Die Binary Increase Congestion-(BIC-)Control versucht die Probleme des TCP-Protokolls bei der Übertragung großer Datenmengen über große Entfernungen zu beheben. TCP verschenkt bei großen Entfernungen einen Großteil der Bandbreite. BIC ist eine reine Modifikation des Absenders. Der Empfänger muss nicht ebenfalls das BIC-Protokoll beherrschen.

Das BIC-Protokoll ist noch sehr jung (2004) und stellt hier einige Variablen zur Verfügung, mit denen Sie sein Verhalten einstellen können. Die Erläuterung der Optionen benötigt aber recht viel Wissen über das Protokoll selbst. Sie finden Hintergrundinformationen unter *http://www.csc.ncsu.edu/faculty/rhee/export/bitcp/*.

tcp_congestion_control

Der Linux-Kernel 2.6.13 und neuer kann verschiedene Methoden verwenden, um Verstopfungen der Netzwerkverbindungen zu erkennen und zu vermeiden. Aktuell stehen die folgenden zur Verfügung:

- reno (klassisches TCP)
- bic
- highspeed (Sally Floyd)

- htcp (Hamilton TCP)
- hybla (Speziell für Satellitenverbindungen)
- scalable
- vegas
- westwood (speziell für verlustreiche Netzwerke)

Sie können ganz einfach die Methode wählen:

```
sysctl -w net.ipv4.tcp_congestion_control=htcp
```

Sie finden weitere Informationen über die Methoden auf *http://www-iepm.slac.stanford.edu/bw/tcp-eval/*.

tcp_dsack

Diese Variable bestimmt, ob doppelte selektive Acknowledgments (`sack`) versendet werden sollen. Damit kann einem Absender mitgeteilt werden, dass ein Paket doppelt empfangen worden ist. D-SACK ist eine Erweiterung des SACK-Standards und wird in dem RFC 2883 genauer beschrieben. SACK und D-SACK beschleunigt die Übertragung größerer Datenmengen enorm, da ein Empfänger genau die empfangenen Pakete bestätigen kann und nicht immer nur das Paket mit der kleinsten Sequenznummer (siehe auch `tcp_sack`).

tcp_ecn

Die Explicit Congestion Notification (ECN) ist eine neue Methode, bei der zwei Kommunikationspartner Informationen über Netzwerk-Verstopfungen austauschen. Beide Kommunikationspartner müssen ECN unterstützen. Leider verwerfen immer noch viele Firewalls Pakete mit ECN-Informationen als bösartige Pakete, da sie oder ihre Administratoren diesen neuen Standard noch nicht kennen. Dann können Sie mit dieser Variable ECN abschalten. Ansonsten können Sie für bestimmte IP-Adressen auch in der Mangle-Tabelle das ECN-Target verwenden (siehe Abschnitt 21.2.4).

ECN wird in den beiden RFCs *RFC 3168 – The Addition of Explicit Congestion Notification (ECN) to IP* und *RFC 2884 – Performance Evaluation of Explicit Congestion Notification (ECN) in IP Networks* besprochen.

tcp_fack

Forward Acknowledgment ist eine spezielle Methode, die bei selektiven Acknowledgments wesentlich radikaler nichtbestätigte Pakete zur Wiederversendung auswählt. Dabei geht diese Methode davon aus, dass, sobald ein selektives Acknowledgment empfangen wurde, alle Pakete mit kleineren Sequenznummern verloren gegangen sind und neu gesendet werden müssen. Da dies nur dann korrekt ist, wenn eine Umsortierung der Paketreihenfolge nicht erfolgt ist, wird für Verbindungen, bei denen eine Umsortierung erkannt wurde, das Verfahren abgeschaltet. Forward Acknowledgments sind nur aktiv, wenn auch selektive Acknowledgments

unterstützt werden. Da dies die Performance erhöht, sollte die Option eingeschaltet sein. Weitere Informationen finden Sie auf der Homepage des Entwicklers Matthew Mathis: *http://www.psc.edu/~mathis/*.

tcp_fin_timeout

Wenn das lokale System eine Verbindung mit einem FIN-Paket beendet, muss auch der Kommunikationspartner die Verbindung mit einem FIN-Paket beenden. Diese Variable definiert, wie lange Ihr System auf ein Antwort-FIN-Paket des Kommunikationspartners warten muss. Einige Systeme reagieren hier nicht entsprechend den TCP-Standards und beenden ihre Seite der Verbindung nicht korrekt.

Dies kann zu Speicherproblemen auf Webservern führen, wenn viele defekte Clients die Verbindungen aufbauen, da für jeden offenen Socket 1,5 kByte Speicher reserviert werden. Der Default-Wert von 60 Sekunden kann auf diesen Systemen auf 30 Sekunden reduziert werden.

tcp_frto

Plötzliche Timeouts bei der wiederholten Sendung von verlorenen TCP-Paketen (spurious retransmission timouts, RTO) können zu langsamen Übertragungsraten führen. Diese Timeouts treten vor allem bei unzuverlässigen Medien, zum Beispiel WLAN auf. Das RFC 4138 beschreibt die Forward RTO Recovery, die nur von dem Absender implementiert wird. Diese Option schaltet diese Methode im Kernel an.

tcp_keepalive_*

Eine Applikation kann einen Socket mit der Option SO_KEEPALIVE öffnen. Der Kernel sendet dann, selbst wenn der Socket nicht verwendet wird, in regelmäßigen Abständen TCP-Keepalive-Pakete, um die Verbindung geöffnet zu halten und um einen Verbindungsabbruch zu erkennen.

Diese Variablen definieren, wie diese Keepalive-Pakete versendet werden.

tcp_keepalive_time

Diese Variable definiert, in welchen Abständen der Linux-Kernel ein Paket für eine ungenutzte Verbindung aussendet. Der Default-Wert beträgt 7200 Sekunden oder 2 Stunden.

tcp_keepalive_probes

Diese Variable definiert, wie viele unbeantwortete Keepalive-Pakete ausgesendet werden, bevor der Kernel die Verbindung als unterbrochen ansieht (Default: 9).

tcp_keepalive_intv

Diese Variable definiert, in welchem Interval der Kernel ein weiteres Keepalive-Paket aussendet, wenn das letzte Paket nicht beantwortet wurde (Default: 75 Sekunden).

Der Kernel sendet also alle 2 Stunden ein Paket. Wird dieses nicht beantwortet, sendet er anschließend alle 75 Sekunden 9-mal ein weiteres Paket. Werden auch diese nicht beantwortet, ist die Verbindung tot.

tcp_low_latency

Diese Option definiert, welches Ziel der Kernel bei den TCP-Verbindungen verfolgen soll:

- Hoher Durchsatz (High Throughput, Default) oder
- Niedrige Verzögerung (Low Latency).

Ein High-Performance-Rechencluster hätte diese Variable typischerweise gesetzt.

tcp_max_orphans

Diese Variable definiert, wie viele verwaiste (orphan) TCP-Sockets der Kernel toleriert, die nicht mehr mit einem User-File-Handle verbunden sind. Sobald die Anzahl überschritten wird, setzt der Kernel alle (!) verwaisten Sockets zurück. Damit sollen einfache Denial-of-Service-Situationen behandelt werden, denn jeder verwaiste Socket benötigt 64 kByte Arbeitsspeicher, der nicht in den Swap ausgelagert werden kann.

Sobald diese Situation eintritt, protokolliert der Kernel Folgendes: `TCP: too many of orphaned sockets`. Dann sollten Sie die Variablen `tcp_fin_timeout` und `tcp_orphans_retries` modifizieren oder diesen Wert hochsetzen.

tcp_max_syn_backlog

Der Kernel hält alle halb offenen Verbindungen in einer Tabelle (SYN-Backlog) fest. Dies sind Verbindungen, bei denen der Client nach seinem `SYN` noch nicht das `ACK`-Paket gesendet hat, um die Verbindung zu bestätigen. Diese Tabelle (ist per Default 128 Einträge für Systeme mit weniger als 128 MByte und 1024 Einträge für alle anderen Systeme groß. Auf sehr beschäftigten Systemen (z.B. Webservern) sollten Sie diesen Wert erhöhen.

Siehe auch: `tcp_syncookies`

tcp_max_tw_buckets

Nachdem eine Applikation eine Verbindung beendet hat, wird der Socket in den Zustand Time-Wait versetzt. Diese Variable definiert, wie viele Time-Wait-Sockets insgesamt von dem Kernel unterstützt werden. Der Default-Wert von 180000 sollte nie reduziert, sondern im Fehlerfall nur erhöht werden.

tcp_mem

Diese Variable enthält drei Werte und definiert, wie der TCP-Stack seinen Speicher verwaltet. Die drei Werte sind:

- `low`: Unterer Schwellenwert.
- `pressure`: Bei Überschreiten dieses Wertes versucht TCP, Speicher zu sparen und Informationen im Speicher zu komprimieren. Das erfolgt so lange, bis der Speicherverbrauch wieder unter `low` sinkt.
- `high`: Mehr Speicher darf TCP nie verbrauchen.

Der Speicher wird nicht in Bytes, sondern in Speicherseiten gemessen. Leider ist die Größe der Speicherseite nicht ganz einheitlich bei den verschiedenen Linux-Plattformen. Die i386-Plattform verwendet meist eine 4 kByte große Speicherseite.

Modifikationen dieser Variable können große, auch positive Auswirkungen auf die Performance haben.

tcp_moderate_rcvbuf

Diese Option wurde im Kernel 2.6.7 eingeführt. Diese Funktion wird auch als Dynamic Right Sizing (DRS) bezeichnet. Sie passt die Größe des TCP-Windows automatisch an die Laufzeit (Round-Trip-Time, RTT) der Pakete an. Sie verursacht durch sehr große TCP-Windows mit einigen Routern und Firewalls Probleme. Falls es beim Zugriff auf einige Server zum scheinbaren Totalausfall von TCP kommt, können Sie versuchen, diese Variable auf 0 zu setzen. Der Fehler liegt nicht in den Servern selbst, sondern in den Firewalls und Routern.

Damit diese Funktion aktiv ist, müssen auch `tcp_adv_win_scal` und `tcp_window_scaling` aktiv sein.

tcp_no_metrics_save

Der Linux-Kernel 2.4 und 2.6 hat ein senderseitiges Autotuning. Dazu speichert er den TCP-Slow-Start-Threshold-(`ssthresh`-)Wert in dem Routing-Cache für einen bestimmten Host. Dieses Verhalten wird mit dieser Variable für den Kernel 2.6 abgeschaltet. Das ist für Hochgeschwindigkeitsnetze sinnvoll, da das Autotuning hier häufig nicht korrekt funktioniert.

tcp_orphan_retries

Diese Variable definiert, wie häufig das lokale System versucht, eine Verbindung beim Kommunikationspartner zu beenden, bevor die Verbindung lokal gelöscht wird. Diese Variable hat den Defaultwert 7, das entspricht bis zu 16 Minuten. Auf einem sehr beschäftigten Server (z.B. Webserver) ist es sinnvoll, diese Variable zu reduzieren. Die tatsächliche Zeitspanne hängt von dem Retransmission-Timeout (RTO) ab. Dieses Timeout wird dynamisch für die Verbindung bestimmt (RFC 793). Im Wesentlichen wird der Timeout von der beobachteten Laufzeit (Round Trip Time, RTT) abgeleitet.

tcp_reordering

Diese Variable definiert, wann ein Paket als verloren gilt. Der Default-Wert von 3 sollte nicht verkleinert werden. Siehe auch die RTO-Erklärung bei `tcp_orphan_retries`.

tcp_retrans_collapse

Einige Systeme, speziell Drucker, besitzen einen Fehler in ihrem TCP/IP-Stack, der eine Kommunikation unmöglich macht. Diese Variable schaltet einen Workaround ein, so dass ein Linux-System dennoch mit diesen Geräten sprechen kann.

Es sind keine negativen Nebenwirkungen bekannt.

tcp_retries1

Diese Variable definiert, wie häufig der TCP-Stack ein Paket erneut senden soll, bevor er einen Fehler melden soll (Default: 3). Siehe auch die RTO-Erklärung bei `tcp_orphan_retries`.

tcp_retries2

Diese Variable definiert, wie häufig der TCP-Stack ein Paket versenden soll, bevor die laufende Verbindung beendet wird (Default: 15). Siehe auch die RTO-Erklärung bei `tcp_orphan_retries`.

tcp_rfc1337

Das RFC 1337, *TIME-WAIT Assassination Hazards in TCP*, beschreibt Probleme, die auftreten, wenn alte duplizierte Pakete neue Verbindungen beeinflussen. Dies kann geschehen, da TIME_WAIT-Sockets für neue Verbindungen wiederverwendet werden können. Das RFC beschreibt drei verschiedene Lösungen zu diesem Problem. Der Kernel ignoriert alle RST-Pakete an Sockets im TIME_WAIT-Zustand, wenn diese Variable gesetzt ist.

tcp_rmem

Diese Variable bestimmt die Größe des TCP-Receive-Buffers. Die Variable enthält drei verschiedene Werte:

- `min`: Garantierte Mindestgröße des Receive-Buffers für jeden Socket (Default: 4 oder 8 kByte).
- `default`: Default-Größe des Receive-Buffers (Default: 87380). Dieser Wert überschreibt den Wert `/proc/sys/net/core/rmem_default` für das TCP-Protokoll.
- `max`: Dies ist die maximale Größe des Receive-Buffers für TCP. Dieser Wert wird von `/proc/sys/net/core/rmem_max` überschrieben, falls der IPv4-Wert größer ist.

Tipp

Wenn Sie diese Werte ändern möchten, sollten Sie sich den TCP-Tuning-Guide für Linux auf *http://www-didc.lbl.gov/TCP-tuning/linux.html* ansehen. Dort wird vorgeschlagen, die Maximalwerte zu vergrößern:

```
# increase TCP max buffer size
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
# increase Linux autotuning TCP buffer limits
# min, default, and max number of bytes to use
net.ipv4.tcp_rmem = 4096 87380 16777216
net.ipv4.tcp_wmem = 4096 65536 16777216
```

tcp_sack

Diese Variable aktiviert selektive Acknowledgments entsprechend dem RFC 2018, *TCP Selective Acknowledgement Options,* und dem RFC 2883, *An Extension to Selective Acknowledgement (SACK) Option for TCP*. Selektive Acknowledgments erhöhen insbesondere bei Netzwerkmedien mit Paketverlusten den Durchsatz. Da S-ACKs keine negativen Auswirkungen haben, sollte diese Option immer eingeschaltet werden.

tcp_stdurg

Es gibt zwei verschiedene Varianten, wie ein TCP/IP-Stack mit dem Urgent-Pointer und dem URG-TCP-Flag umgehen kann. RFC793 beschreibt das Verhalten, das auch von dem Betriebssystem BSD 4.2 verwendet wird. Dies ist das Standardverhalten des Linux-Kernels. Wenn Sie diese Variable aktivieren, verhält sich jedoch der Linux-Kernel wie in RFC 1122, *Requirements for Internet Hosts – Communication Layers,* beschrieben. Dieses Verhalten ist nicht kompatibel und kann zu Funktionsstörungen führen, daher ist die Funktion per Default nicht aktiv.

tcp_synack_retries

Diese Variable definiert, wie häufig ein Kernel versuchen soll, SYN/ACK-Pakete als Antwort auf einen Verbindungsaufbau zu senden. Der Default-Wert ist 5. Da ein Versuch etwa 30-40 Sekunden dauert, beträgt der gesamte Timeout 180 Sekunden.

tcp_syncookies

Hiermit aktivieren Sie SYN-Cookies im Linux-Kernel. Der Linux-Kernel wird anfangen, SYN-Cookies zu versenden, sobald der SYN-Backlog überläuft. Damit können Sie sich gegen einen SYN-Flood wehren.

Achtung

Diese Funktion ist lediglich ein Fallback für den Fall eines Angriffs. Sie kann zu großen Problemen führen. Achten Sie darauf, dass Ihr Linux-System die SYN-Cookies nicht im Normalbetrieb versendet! Wenn Ihr Server so beschäftigt ist, dass der SYN-Backlog im normalen Betrieb überläuft, sollten Sie den SYN-Backlog vergrößern (siehe `tcp_max_syn_backlog`).

Die TCP-SYN-Cookies ermöglichen es dem Linux-System, bei einem SYN-Flood ein späteres ACK-Paket eines echten Clients zu erkennen und trotzdem die Verbindung aufzubauen. Die SYN-Cookies wurden u.a. von DanBernstein entwickelt und hier beschrieben: *http://cr.yp.to/syncookies.html*.

tcp_syn_retries

Diese Variable definiert, wie häufig der Linux-Kernel versuchen soll, selbst eine Verbindung aufzubauen. Der Default-Wert beträgt 5. Da ein Versuch etwa 30-40 Sekunden dauert, beträgt der gesamte Timeout 180 Sekunden.

tcp_timestamps

RFC 1323, *TCP Extension for High Performance*, beschreibt die Verwendung von Timestamps, um die Round Trip Time (RTT) zu ermitteln. Grundsätzlich verbessert diese Option die Funktion des TCP-Protokolls.

Hinweis

Nmap verwendet die TCP-Timestamps, um die Uptime eines Systems zu ermitteln. Wenn Sie das verhindern möchten, müssen Sie diese Option abschalten.

tcp_tso_win_divisor

Die TCP-Segmentation-Offload-(TSO-)Funktion erlaubt es, die Aufteilung großer Pakete in kleine Pakete an die Netzwerkkarte abzugeben. Der `e1000`-Treiber unterstützt dies seit dem Kernel 2.5.33. Der TCP-Stack übergibt 64 kByte große Pakete an die Karte, die sie in 1500 Byte große Pakete entsprechend der MTU aufteilt. Dies reduziert die Prozessorlast enorm.

Achtung

Die Linux-Kernel 2.6.11 und älter haben einen Fehler in der Implementierung. Hier sollten Sie die TSO-Funktion für die Netzwerkkarte abschalten:

```
ethtool -K eth0 tso off
```

Diese Variable definiert, welchen Anteil (Prozent) des Netzwerkkartenpuffers ein TSO-Paket einnehmen darf.

tcp_tw_*

Diese Parameter beeinflussen die Behandlung der TIME_WAIT-Sockets. Die Variable `tcp_tw_reuse` bestimmt, ob eine Applikation einen TIME_WAIT-Socket wiederverwenden darf. Die Variable `tcp_tw_recycle` definiert, ob eine andere Applikation einen TIME_WAIT-Socket nutzen darf.

Achtung

Die Verwendung dieser Optionen kann zu großen Problemen führen. Stellen Sie auf jeden Fall sicher, dass gleichzeitig auch die Variable `tcp_rfc1337` aktiviert wurde.

Sie sollten diese Optionen nur nutzen, wenn Sie nicht über genug Sockets für Ihre Applikation verfügen.

tcp_vegas_*

TCP-Vegas ist eine senderseitige Veränderung des TCP-Protokolls, die versucht, Verstopfungen durch Schätzung der Bandbreite zu ermitteln. Hierzu ermittelt es die Verzögerungen der Pakete, anstatt den Paketverlust auszuwerten (TCP-Reno). TCP-Vegas modifiziert dann die Sendegeschwindigkeit durch Modifikationen des Congestion-Fensters. TCP-Vegas erzeugt damit einen geringeren Paketverlust als TCP-Reno (Default-TCP).

Sie finden weitere Informationen auf der Vegas-Homepage (*http://www.cs.arizona.edu/protocols/*).

Anstelle von TCP-Vegas verwenden moderne Linux-Kernel jedoch bereits TCP-BIC.

tcp_westwood

TCP-Westwood ist eine weitere Methode, mit der Verstopfungen der Netzwerkverbindung vorgebeugt werden kann. Auch hier handelt es sich um eine nur senderseitige Modifikation des Reno-TCP-Stacks. Auch diese Methode schätzt die Bandbreite der Verbindung, um das Congestion Window und die Slow Start Threshold (ssthresh) zu setzen.

Weitere Informationen über diese Methode finden Sie auf *http://193.204.59.123/c3lab/westwood.php* und *http://www.cs.ucla.edu/NRL/hpi/tcpw/*.

tcp_window_scaling

Diese Variable schaltet das TCP-Window-Scaling an. Damit können Absender und Empfänger größere TCP-Windows als 64 kByte verwenden. Dies verbessert die Performance bei Netzwerkmedien mit hoher Bandbreite und hoher Latenz und reduziert die Verluste durch nicht ausreichende Nutzung der Bandbreite.

tcp_wmem

Diese Variable verwaltet ähnlich `tcp_rmem` den Sende-Puffer des TCP-Stacks. Es handelt sich genauso um drei Werte: `min`, `default` und `max`. Sie finden bei `tcp_rmem` eine Beschreibung der Werte. Eine Anpassung des `max`-Wertes nach oben kann erstaunliche Leistungssteigerungen bringen.

23.4 /proc/sys/net/ipv4/conf

Dieses Verzeichnis enthält für jede verfügbare Netzwerkkarte ein Unterverzeichnis. Zusätzlich existieren die Verzeichnisse `all/` und `default/`. Änderungen der Variablen in dem Verzeichnis `all/` haben Auswirkungen auf alle Netzwerkkarten. Das Verzeichnis `default/` definiert, welche Werte den Variablen neuer Netzwerkkarten zugewiesen werden. Die Werte bereits aktivierter Netzwerkkarten werden nicht verändert.

```
$ ls -l /proc/sys/net/ipv4/conf
insgesamt 0
dr-xr-xr-x  2 root root 0  2. Nov 13:36 all
dr-xr-xr-x  2 root root 0  2. Nov 13:36 default
dr-xr-xr-x  2 root root 0  2. Nov 13:36 eth0
dr-xr-xr-x  2 root root 0  2. Nov 13:36 lo
dr-xr-xr-x  2 root root 0  2. Nov 13:36 vmnet1
dr-xr-xr-x  2 root root 0  2. Nov 13:36 vmnet2
dr-xr-xr-x  2 root root 0  2. Nov 13:36 vmnet3
dr-xr-xr-x  2 root root 0  2. Nov 13:36 vmnet8
```

23.4.1 accept_redirects

Diese Variable definiert, ob das System ICMP-Redirect-Nachrichten auswertet. Diese Nachrichten werden von Routern versendet, um andere Router und Rechner auf eine bessere Route hinzuweisen. Linux akzeptiert per Default ICMP-Redirects (1). Dies erlaubt aber auch ein Router-Spoofing, daher sollte es mindestens auf der Firewall ausgeschaltet werden.

Tipp

Wenn Sie gleichzeitig `secure_redirects` anschalten, ist die Gefahr des Router-Spoofings geringer.

23.4.2 accept_source_route

Dieser Parameter definiert, ob das System IP-Pakete mit der IP-Option Source-Routing akzeptiert. Da damit ein Angreifer Pakete über selbst gewählte Routen versenden kann, sollte diese Option abgeschaltet sein (0). Dies ist auch der Default.

23.4.3 arp_announce

Diese Variable definiert, welche Source-IP-Adresse in ARP-Requests verwendet wird.

- `0`: Verwendet eine beliebige IP-Adresse (Default).
- `1`: Vermeidet IP-Adressen, die sich nicht in demselben Subnetz wie das Ziel der ARP-Anfrage befinden.
- `2`: Verwendet die IP-Adresse, die auch für die Kommunikation mit dem Zielsystem verwendet werden würde.

23.4.4 arp_filter

Diese Variable definiert, wie der Kernel auf ARP-Anfragen antwortet. Wenn Sie mehrere Netzwerkkarten für das Load-Balancing in demselben Subnetz betreiben, sollten Sie diesen Parameter auf 1 setzen.

23.4.5 arp_ignore

Diese Variable definiert, wie das Linux-System auf ARP-Anfragen reagiert.

- `0`: Beantworte jede ARP-Anfrage für jede lokale IP-Adresse, selbst wenn diese nicht auf der betroffenen Netzwerkkarte definiert ist (Default).

- 1: Beantworte nur ARP-Anfragen für IP-Adressen, die auf der ankommenden Netzwerkkarte definiert sind.
- 2: Beantworte nur ARP-Anfragen für IP-Adressen, die auf der ankommenden Netzwerkkarte definiert sind und die sich im selben Subnetz mit der Source-Adresse der ARP-Anfrage befinden.
- 8: Beantworte keine ARP-Anfragen.

23.4.6 bootp_relay

Diese Option muss gesetzt werden, wenn Sie auf dem Linux-System einen Bootp-Relay-Daemon betreiben möchten. Die Netzwerkkarte akzeptiert dann auch Pakete mit der Source-Adresse 0.b.c.d.

23.4.7 disable_policy

Dies deaktiviert IPsec-Policies für diese Netzwerkkarte.

23.4.8 disable_xfrm

Dies deaktiviert IPsec-Verschlüsselung für diese Netzwerkkarte.

23.4.9 force_igmp_version

Hiermit können Sie die IGMP-Version für diese Netzwerkkarte erzwingen:

```
/sbin/sysctl -w net.ipv4.conf.eth0.force_igmp_version=3
```

23.4.10 forwarding

Hiermit aktivieren Sie das Forwarding nur für diese Netzwerkkarte. Wenn Sie diese Variable nutzen möchten, sollten Sie nicht die Variable ip_forward verwenden.

23.4.11 log_martians

Diese Variable protokolliert Pakete mit unmöglichen IP-Adressen. Dies sind Pakete, die von rp_filter erkannt wurden oder Source-Routing-IP-Optionen verwenden.

23.4.12 mc_forwarding

Wenn Sie einen Multicast-Routing-Daemon betreiben möchten, müssen Sie diese Variable einschalten.

23.4.13 medium_id

Diese Variable unterscheidet Geräte anhand des Netzwerkmediums, mit dem sie verbunden sind. Diese Variable wird für ProxyARP verwendet. ProxyARP wird

von dem Kernel nur für Pakete aktiviert, die zwischen zwei Geräten weitergeleitet werden, die nicht mit demselben Medium verbunden sind. Ein Wert von -1 bedeutet, dass das Medium unbekannt ist. Der Wert 0 bedeutet, dass dieses Gerät das einzige ist, das mit dem Medium verbunden ist.

23.4.14 promote_secondaries

Wenn Sie einen Alias auf einer Netzwerkkarte definieren und anschließend die primäre IP-Adresse löschen, wird automatisch auch der Alias gelöscht. Die Option `promote_secondaries` sorgt dafür, dass der Alias automatisch zur primären IP-Adresse wird.

23.4.15 proxy_arp

Diese Variable aktiviert ProxyARP für diese Netzwerkkarte.

23.4.16 rp_filter

Diese Variable schaltet einen Reverse-Path-Filter für diese Netzwerkkarte an. Dieser Filter prüft, ob eine Antwort an den Absender des Pakets auch über diese Netzwerkkarte versendet werden würde. Diese Variable bietet so einen gewissen Schutz vor IP-Spoofing-Angriffen. Jedoch verursacht diese Funktion auch häufig Probleme, wenn Sie Policy-Routing, Advanced-Routing oder IPsec einsetzen. Dann ist es sinnvoll, diese Funktion abzuschalten. Der Schutz, den diese Funktion bietet, kann auch leicht mit Firewall-Regeln erreicht werden.

23.4.17 secure_redirects

Normalerweise akzeptiert ein Linux-System sämtliche ICMP-Redirects. Wenn Sie diese Variable aktivieren, werden nur Redirects von bekannten Default-Gateways akzeptiert. Diese Funktion erfordert zusätzlich, dass die Variable `shared_media` gesetzt ist.

23.4.18 send_redirects

Diese Variable weist das Linux-System an, ICMP-Redirects auszusenden, falls das System ein Router ist und eine bessere Route kennt.

23.4.19 shared_media

Diese Variable definiert, ob das angeschlossene Netzwerkmedium von mehreren Netzen gleichzeitig genutzt wird. Nur dann versendet der Kernel ICMP-Redirect-Nachrichten als Router und akzeptiert sie als Host.

23.4.20 tag

Hier können Sie eine beliebige Nummer speichern. Diese Nummer wird nur von Ihnen verwendet. Der Kernel ignoriert diese Variable.

23.5 /proc/sys/net/ipv4/neigh

Diese Parameter betreffen das ARP-Protokoll. Jeden Parameter hier aufzuführen, würde das Format sprengen, daher möchte ich Sie auf die `arp(7)`-Manpage verweisen, in der die Parameter erläutert werden.

23.6 /proc/sys/net/ipv4/netfilter

Ab der Version 2.6.9 verfügt der Linux-Kernel über das Verzeichnis, in dem sich verschiedene Variablen befinden, die das Connection Tracking betreffen. Diese Variablen werden in dem entsprechenden Kapitel besprochen (siehe Kapitel 19).

Zusätzlich kann sich in diesem Verzeichnis auch ein weiteres Unterverzeichnis `ct_sync` befinden. Die Variablen in diesem Verzeichnis werden ebenfalls in dem Kapitel zu `ct_sync` besprochen (siehe Abschnitt 26.6).

23.7 /proc/sys/net/ipv4/route

Diese Variablen verwalten den Routing-Cache und die Versendung von Fehler-Nachrichten.

23.8 /proc/sys/net/ipv6

Dieses Verzeichnis enthält die Variablen für das IPv6-Protokoll. Da diese Variablen zum größten Teil identisch mit den IPv4-Variablen sind, sollen sie hier nicht erneut aufgeführt werden.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

24 Fortgeschrittene Protokollierung

Wenn Sie die Protokolle Ihrer Firewall anspruchsvoll weiterverarbeiten möchten, werden Sie möglicherweise schnell an die Grenzen des `LOG`-Targets stoßen. Dann sollten Sie sich das `ULOG`-Target ein wenig genauer ansehen. Es gibt mehrere Softwarepakete, die mit diesem Target zusammenarbeiten und die Protokolle schreiben können. Zwei davon möchte ich Ihnen vorstellen: `ulogd` und `specter`.

Die Auswertung kann mit einigen der im Kapitel 12, Protokollanalyse, vorgestellten Werkzeuge erfolgen.

24.1 Das ULOG-Target

Dieses Ziel erlaubt es Ihnen, Pakete zur Protokollierung an eine beliebige Userspace-Applikation weiterzuleiten. Diese Applikation muss den `netlink`-Socket betrachten. Am einfachsten verwenden Sie `ulogd` oder `specter` für die Protokollierung. Diese nehmen die Parameter und Pakete entgegen und können die Protokollierung in einer Datei oder einer Datenbank vornehmen (siehe Kapitel 24).

Damit der Protokolldienst zwischen den verschiedenen Protokolldateien oder Datenbanken unterscheiden kann, können Sie die Protokollierung mit den folgenden Optionen genauer bestimmen:

- `--ulog-nlgroup <nlgroup>`: `ULOG` unterstützt 32 verschiedene Netlink-Gruppen (1-32). Sie können in dem `ulogd` für jede Gruppe zum Beispiel eine andere Datenbank definieren.
- `--ulog-prefix »Zeichenkette«`: Ähnlich dem `LOG`-Target können Sie auch hier eine Zeichenkette (maximal 32 Zeichen) definieren, die jeder Meldung vorangestellt wird.
- `--ulog-cprange <paketgröße>`: Für die spätere Analyse ist es nützlich, das Paket oder zumindest Teile des Pakets untersuchen zu können. Hiermit können Sie angeben, wie viele Bytes des Pakets an das Userspace-Programm übergeben und damit möglicherweise protokolliert werden sollen. Der Default-Wert 0 kopiert das ganze Paket.
- `--ulog-qthreshold <queuegröße>`: Da die Übergabe des Pakets von dem Kernel in den Userspace mit aufwändigen Überprüfungen verbunden ist, können Sie hier de-

finieren, wie viele Pakete der Kernel vor der Übergabe sammeln (1-50) und gemeinsam übergeben soll. Der Default-Wert ist aus Gründen der Rückwärtskompatibilität 1. Diesen Wert können Sie für jede Regel einzeln definieren.

```
iptables -A FORWARD -p icmp -m length --length 200: -j ULOG \
  --ulog-nlgroup 2 --ulog-prefix "Großes ICMP: " \
  --ulog-qthreshold 10
```

24.2 Das ipt_ULOG-Kernelmodul

Beim Laden des `ipt_ULOG`-Kernelmoduls können Sie einige zusätzliche Parameter definieren, die das Verhalten und die Geschwindigkeit beeinflussen können. Diese Optionen möchte ich Ihnen hier vorstellen. Wenn nicht alle hier aufgeführten Optionen von Ihrem Modul unterstützt werden, setzen Sie wahrscheinlich eine ältere Kernel-Version ein. Um diese Optionen zu nutzen, müssen Sie vor der ersten Regel, die das `ULOG`-Target verwendet, das Modul manuell mit `modprobe` laden.

- `nlbufsiz=<zahl>`: Hiermit geben Sie die Größe des Netlink-Puffers an. Der Puffer darf maximal eine Größe von 128 KByte haben. Größere Puffer erhöhen die Geschwindigkeit, verzögern aber möglicherweise die Protokollierung leicht. Default: 4096.
- `flushtimeout:int`: Dieser Wert definiert, in welchen Intervallen spätestens der Puffer geleert werden muss, auch wenn der Puffer nicht voll ist. Damit kann die mögliche Verzögerung durch einen großen Puffer beschränkt werden. Die Zeiteinheit ist 10 ms auf x86-Systemen. Der Default ist 10 (100 ms).
- `nflog:int`: Diese Option definiert, ob dieses Modul auch für die Filterung von internen Netfilter-Meldungen verwendet werden soll. Dies sind zum Beispiel Meldungen über ungültige Pakete. Der Default ist 1 (Ja).

24.3 Der Ulogd-Daemon

Der Ulogd-Daemon wurde von Harald Welte geschrieben und existiert im Moment in zwei Versionen. Auf *http://gnumonks.org/projects* finden Sie den Ulogd-Daemon in der Version 1 für die Verwendung mit dem `ULOG`-Target. Wenn Sie bereits den Kernel 2.6.14 mit dem `NFLOG`-Target einsetzen, können Sie den Ulogd-Daemon in der Version 2 verwenden, der im Moment (Okt. 2005) nur auf dem Subversion-Server verfügbar ist *http://svn.gnumonks.org/branches/ulog/ulogd2/*. Um den Ulogd-2-Daemon auszuchecken und zu übersetzen, verwenden Sie:

```
$ svn co http://svn.gnumonks.org/branches/ulog/ulogd2
$ cd ulogd2/
$ aclocal
$ automake
$ autoconf
$ ./configure
$ make
```

Der Ulogd verwendet Plugins, um die verschiedenen Funktionen zur Verfügung zu stellen. Diese Plugins werden in einer Konfigurationsdatei beschrieben, in der Sie festlegen, welche Meldungen wie protokolliert werden sollen. Eine Beispieldatei ist im Folgenden abgedruckt:

```
# Example configuration for ulogd
# $Id: ulogd.conf.in 714 2005-02-19 21:33:43Z laforge $
#

[global]
########################################################################
# GLOBAL OPTIONS
########################################################################

# netlink multicast group (the same as the iptables --ulog-nlgroup param)
nlgroup=1

# logfile for status messages
logfile="/var/log/ulogd/ulogd.log"

# loglevel: debug(1), info(3), notice(5), error(7) or fatal(8)
loglevel=5

# socket receive buffer size (should be at least the size of the
# in-kernel buffer (ipt_ULOG.o 'nlbufsiz' parameter)
rmem=131071

# libipulog/ulogd receive buffer size, should be > rmem
bufsize=150000

########################################################################
# PLUGIN OPTIONS
########################################################################

# We have to configure and load all the plugins we want to use
# general rules:
# 1. load the plugins _first_ from the global section
# 2. options for each plugin in seperate section below


#
# ulogd_BASE.so - interpreter plugin for basic IPv4 header fields
#                 you will always need this
plugin="/usr/lib/ulogd/ulogd_BASE.so"
```

```
# output plugins.
plugin="/usr/lib/ulogd/ulogd_LOGEMU.so"
#plugin="/usr/lib/ulogd/ulogd_OPRINT.so"
#plugin="/usr/lib/ulogd/ulogd_MYSQL.so"
#plugin="/usr/lib/ulogd/ulogd_PGSQL.so"
#plugin="/usr/lib/ulogd/ulogd_SQLITE3.so"
#plugin="/usr/lib/ulogd/ulogd_PCAP.so"


[LOGEMU]
file="/var/log/ulogd/ulogd.syslogemu"
sync=1

[OPRINT]
file="/var/log/ulogd/ulogd.pktlog"

[MYSQL]
table="ulog"
pass="g3h31m"
user="ulog"
db="ulogd"
host="localhost"

[PGSQL]
table="ulog"
schema="public"
pass="g3h31m"
user="ulog"
db="ulogd"
host="localhost"

[SQLITE3]
table="ulog"
db="/path/to/sqlite/db"
buffer=200

[PCAP]
file="/var/log/ulogd/ulogd.pcap"
sync=1
```

Der Ulogd-Daemon unterstützt aktuell ein Input-Plugin, das IPv4-Pakete lesen und analysieren kann, und mehrere verschiedene Output-Plugins, mit denen Sie die Pakete in verschiedenen Formaten protokollieren können. Sie können zwischen den folgenden Output-Plugins wählen:

- MySQL
- PostgreSQL
- SQLite3
- Pcap-Datei
- LOGEMU (ähnlich Syslog-Protokollierung)
- OPRINT (einfache Protokollierung in einer Datei für Debugging)
- SYSLOG (protokolliert via Syslogd)

Die folgenden Input-Plugins können Sie nutzen:

- BASE (Grundfunktion, sollten Sie immer laden)
- LOCAL (protokolliert nur den Rechnernamen und den Zeitpunkt der Protokollierung)
- PWSNIFF (experimentelles Plugin für die Protokollierung der POP-3- und FTP-Kennwörter)

Sie müssen mindestens ein Input- und ein Output-Plugin wählen. Außerdem müssen Sie in der Konfigurationsdatei die folgenden Parameter setzen:

- `nlgroup=<gruppe>`: Hiermit wählen Sie die Gruppe, an die sich dieser Ulogd-Prozess binden soll. Jeder Ulogd-Prozess kann sich nur an eine Gruppe binden. Diese Zahl muss mit der Angabe in der Option `--ulog-nlgroup` des `ULOG`-Targets übereinstimmen. Wenn Sie verschiedene Gruppen in Ihren Regeln verwenden, benötigen Sie für jede Gruppe einen eigenen Ulogd-Prozess.
- `logfile=<datei>`: Dies ist die Protokolldatei des Ulogd-Daemons. Hier protokolliert der Daemon Fehler und Warnungen. Durch Angabe von `syslog` oder `stdout` protokolliert der Ulogd diese Informationen über den Syslogd oder auf der Standardausgabe.
- `loglevel=<level>`: Hiermit stellen Sie den Detailgrad der Ulogd-eigenen Protokollierung in dem `logfile` ein. Die Level sind in der Beispielkonfigurationsdatei angegeben.
- `plugin=<pfad/plugin>`: Mit diesem Parameter laden Sie die Plugins, die Sie verwenden möchten. Sie können diesen Parameter mehrfach verwenden. Die einzelnen Plugins benötigen teilweise zusätzliche Konfigurationsparameter (z.B. MySQL).
- `rmem=<größe>`: Mit diesem Parameter stellen Sie die Größe des Ulogd-Netlink-Socket-Empfangspuffers ein. Dieser muss mindestens der Größe des Netlink-Puffers des `ipt_ULOG`-Moduls entsprechen. Wenn Sie mit der Option `nlbufsiz=<größe>` diesen gesetzt haben, müssen Sie auch diesen Wert anpassen.
- `bufsize=<größe>`: Dies ist der eigentliche Ulogd-Empfangspuffer. Dieser muss mindestens die Größe des `rmmem`-Puffers haben.

Einzelne Plugins verfügen über zusätzliche Konfigurationsparameter. Bevor diese in eigenen Abschnitten besprochen werden, möchte ich kurz die Optionen erläutern, die Sie beim Start des Ulogd verwenden können:

- `-d, --daemon`: Daemon-Modus. Hiermit wechselt der Prozess in den Hintergrund.
- `-V, --version`: Anzeige der Version.
- `-h, --help`: Anzeige der Hilfe.
- `-c, --config <datei>`: Hiermit wählen Sie eine alternative Konfigurationsdatei aus. Die Default-Datei ist `/etc/ulog.conf`. Diese Option ist wichtig, wenn Sie mehrere Instanzen des Ulogd auf Ihrem System betreiben möchten. Das ist immer dann der Fall, wenn Sie in Ihren Regeln das `ULOG`-Target mit verschiedenen Netlink-Gruppen verwenden, um die Ausgabe in unterschiedliche Protokolle zu schreiben.

24.3.1 [OPRINT]

Dies ist ein sehr einfaches Ausgabemodul, das nur für Debugzwecke eingesetzt werden kann. Das Modul benötigt als einzigen Parameter den Dateinamen für die Ausgabe:

```
[OPRINT]
dumpfile=<datei>
```

24.3.2 [LOGEMU]

Dieses Modul protokolliert in eine Datei und emuliert dabei das Format der Syslog-Protokollierung ähnlich dem `LOG`-Target. Die Protokollierung erfolgt aber ohne Umweg über den Syslog direkt in die Datei. Sie müssen den Dateinamen angeben und können mit dem Parameter `sync` definieren, ob das Protokoll synchron (1) geschrieben werden soll (Default 0, asynchron). Dann tauchen neue Meldungen in dem Protokoll zu Lasten der Geschwindigkeit sofort auf.

```
[LOGEMU]
file=<datei>
sync=0|1
```

24.3.3 [MYSQL]

Hiermit protokollieren Sie in eine MySQL-Datenbank. Damit Sie dieses Plugin nutzen können, muss der Ulogd mit MySQL-Unterstützung übersetzt werden (`./configure --with-mysql`). Welche Informationen von diesem Plugin protokolliert werden, hängt von Ihrer MySQL-Tabelle ab. Dieses Plugin liest die verfügbaren Spalten der MySQL-Tabelle und vergleicht deren Namen mit den zur Verfügung stehenden Informationen. Als Beispiel für eine derartige Tabelle und die zu verwendenden Spalten-Typen können Sie auf die Datei `doc/mysql.table` zurückgreifen.

Wenn Sie an bestimmten Informationen nicht interessiert sind, können Sie durch Entfernen der Spalte dafür sorgen, dass dieses Plugin die Daten auch nicht protokolliert. Dadurch wird Ihre Datenbank schlanker. Wenn Sie die IP-Adresse als Zeichenkette in der Datenbank ablegen möchten, können Sie auch die Tabelle aus der

Datei `doc/mysql.table.ipaddr-as-string` verwenden. Dann müssen Sie aber auch Ulogd mit der Option `--with-mysql-log-ip-as-string` beim `./configure`-Aufruf übersetzen.

Das Modul benötigt die folgenden zusätzlichen Angaben:

- `table=<tabelle>`: Der Name der SQL-Tabelle.
- `ldb=<datenbank>`: Der Name der SQL-Datenbank.
- `host=<mysql_rechner>`: Der Rechner, auf dem der MySQL-Server läuft. Damit können Sie die Datenbank auf einem anderen Rechner unterbringen. Denken Sie nur daran, dass Ihre Firewall den Zugriff auf diesen Rechner erlauben muss.
- `port=<mysql_port>`: Der Port der MySQL-Datenbank.
- `user=<mysql_user>`: Der Benutzer, der für die Anmeldung an der Datenbank verwendet wird. Verwenden Sie aus Sicherheitsgründen bitte nicht das root-Konto.
- `pass=<mysql_password>`: Das Kennwort für die Anmeldung an der Datenbank.

24.3.4 [PGSQL]

Dieses Output-Plugin arbeitet ähnlich wie das MySQL-Plugin. Damit das Plugin zur Verfügung steht, müssen Sie Ulogd mit der Option `--with-pgsql` bei der Übersetzung konfiguriert haben. Es verfügt über die gleichen Parameter, und Sie finden in der Ulogd-Distribution auch eine Beispiel-Tabelle `doc/pgsql.table`. Je nach PostgreSQL-Version müssen Sie jedoch einen zusätzlichen Parameter angeben: `schema=<schema>`. PostgreSQL ab Version 7.3 unterstützt diese Schemas. Damit können Sie datenbankübergreifende Views erzeugen. (Für Hintergrundinformationen über Schemas lesen Sie bitte auf *http://sql-info.de/postgresql/schemas.html* nach.) Wenn Sie PostgreSQL 7.3 oder eine neuere Version einsetzen, müssen Sie zusätzlich ein Schema angeben. PostgreSQL stellt für diese Zwecke das Default-Schema `public` zur Verfügung.

```
[PGSQL]
table="ulog"
schema="public"
pass="g3h31m"
user="ulog"
db="ulogd"
host="localhost"
```

24.3.5 [PCAP]

Dieses Output-Plugin protokolliert das Paket im Libpcap-Format. Damit können Sie später die Protokolldatei in Ethereal oder Tcpdump öffnen und analysieren. Dies kann eine spätere forensische Analyse des Angriffs stark erleichtern. Dazu sollte dann aber von dem ULOG-Target auch das gesamte Paket protokolliert werden.

Das Plugin benötigt mindestens die Angabe der Pcap-Datei. Zusätzlich können Sie mit dem Parameter `sync` angeben, ob die Datei synchron (1) oder asynchron (0, Default) geschrieben werden soll.

```
[PCAP]
file="/var/log/ulogd/ulogd.pcap"
sync=1
```

24.3.6 [SQLITE3]

SQLite (*http://www.sqlite.org/*) ist eine kleine C-Bibliothek, die eine komplette, in andere Programme einbettbare SQL-Datenbank ohne zusätzliche Konfiguration darstellt. Sie benötigen keinen Dienst und müssen keinen Client oder Server konfigurieren. In vielen Umgebungen ist SQLite schneller als ein komplettes Datenbank-Managementsystem (DBMS). Um SQLite zu verwenden, müssen Sie Ulogd mit der Option `--with-sqlite` bei der Übersetzung konfiguriert haben.

Für die Erzeugung der Datenbank finden Sie in dem `doc/`-Verzeichnis der Distribution auch eine Datei `sqlite3.table`. Die einzigen Parameter, die Sie angeben müssen, sind der Pfad der Datenbank, der Name der Tabelle und die Größe des SQLite Puffers.

```
[SQLITE3]
table="ulog"
db="/path/to/sqlite/db"
buffer=200
```

24.3.7 [SYSLOG]

Das Syslog-Plugin protokolliert über den Syslog-Dienst. Damit sind die Protokollmeldungen identisch zu den Meldungen, die normalerweise das `LOG`-Target erzeugt. Sie müssen hier lediglich die Priorität der Meldung (Level, Priority) und die protokollierende Quelle (Facility) angeben.

```
[SYSLOG]
facility=LOG_KERN
level=LOG_INFO
```

24.4 Der Specter-Daemon

Der Specter-Daemon (*http://joker.linuxstuff.pl/specter/*) von Michal Kwiatkowski basiert auf dem Ulogd, wurde aber um einige Funktionen erweitert. Er wird genauso wie Ulogd unter der GPL-Lizenz vertrieben.

Zu den wesentlichen Unterschieden zum Ulogd zählen:

- Anderes Format der Konfigurationsdatei. Das Skript `ulogd2specter.pl` wandelt die Konfigurationsdatei `ulog.conf` in die Datei `specter.conf` um.
- Die Gruppierung mehrerer Netlink-Gruppen ist möglich. Sie müssen nicht für jede Netlink-Gruppe einen eigenen Prozess starten.
- Eine Gruppierung der Meldungen ist auch in Abhängigkeit von der Netfilter-Markierung möglich.

- Ein weiteres Output-Plugin `EXEC` kann externe Befehle aufrufen.
- Die Output-Plugins `MYSQL` und `PGSQL` unterstützen SSL für die Datenbankverbindung.
- Die Output-Plugins `SYSLOG` und `LOGEMU` unterstützen die Protokollierung der IP- und TCP-Optionen, der TCP-Sequenznummern und des MAC-Headers.

Specter befindet sich wie Ulogd in aktiver Entwicklung. Die aktuelle Version 1.4 wurde Juli 2005 veröffentlicht. Da es ansonsten in der Anwendung dem Ulogd gleicht und die Dokumentation sehr ausführlich ist, zeige ich hier nur eine Beispielkonfiguration mit einer kurzen Beschreibung:

```
plugins {
          BASE    /lib/specter/specter_BASE.so
          MYSQL   /lib/specter/specter_MYSQL.so
   }

   13 {
          :BASE
          :MYSQL
          db mydb
          host localhost
          user username
          pass password
          table ext_attacks
   }

   15 {
          :BASE
          :MYSQL
          db mydb
          host localhost
          user username
          pass password
          table int_attacks
   }
```

In dem Block `plugins` definieren Sie die zu ladenden Plugins. Diese werden dann weiter unten konfiguriert. Die weiteren Blöcke beginnen mit der Netlink-Gruppe. Anschließend definieren Sie die zu verwendenden Plugins und geben zusätzliche Parameter an.

Wenn Sie nicht die Netlink-Gruppe, sondern die Firewall-Markierung für die Aufteilung der Meldungen verwenden möchten, müssen Sie zuvor noch einen Block `global` definieren:

```
global {
          grouping nfmark
```

```
        nlgroup 1
    }
```

Nun nimmt Specter die Meldungen der Netlink-Gruppe 1 an und kann diese entsprechend der Firewall-Markierung aufteilen. Die Nummern vor jedem Block entsprechen nun nicht mehr der Netlink-Gruppe, sondern dieser Firewall-Markierung.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

25 Ipset

Das Kommando `ipset` und die dazugehörigen Patches aus dem Patch-O-Matic lösen den alten Befehl `ippool` und den entsprechenden obsoleten Patch aus Patch-O-Matic ab. Ipset erlaubt es Ihnen, Gruppen von IP-Adressen, Port-Nummern oder anderen Informationen anzulegen, mit Werten zu füllen und in Ihren Regeln für einen Test zu nutzen. Dabei ist besonders interessant, dass Sie diese Gruppen dynamisch in Ihren Regeln verändern können. Die Gruppen können auch untereinander verknüpft werden.

Da diese Funktion mächtige Möglichkeiten bietet und in einem eigenen Befehl implementiert wurde, widme ich ihr ein eigenes Kapitel.

25.1 ipset und iptables

Wenn Sie Ihren Kernel und den Iptables-Befehl mit dem `set`-Patch aus dem Base-Repository des Patch-O-Matic gepatcht haben, stehen Ihnen für die Verwendung des `iptables`-Befehls ein neues Target `-j SET --add-set|--del-set` und ein neuer Match (Test) `-m set --set <set> src|dest` zur Verfügung. Der Test erlaubt es Ihnen, die Mitgliedschaft des Absenders oder des Ziels des Pakets in einer Gruppe zu testen. Mit dem Target können Sie einen Absender oder ein Ziel zu einer Gruppe hinzufügen. Welche Informationen des Absenders oder des Ziels zu einer Gruppe hinzugefügt werden, hängt von der Gruppenart ab. Die verschiedenen Gruppen werden im nächsten Abschnitt genauer besprochen.

Der Befehl `ipset` gibt Ihnen die Möglichkeit, diese Gruppen unabhängig von dem Iptables-Kommando zu definieren und Mitglieder hinzuzufügen oder zu entfernen.

Die Verwendung wird am einfachsten anhand eines Beispiels deutlich. Stellen Sie sich vor, dass Sie in Ihrem Netzwerk fünf Systeme besitzen, die als Administrationsrechner per Secure-Shell auf die Firewall zugreifen können sollen. Anstatt für jeden dieser Rechner eine eigene Regeln zu definieren, können Sie folgendes Konstrukt verwenden:

```
ipset -N admin ipmap --network 192.168.0.0/24
ipset -A admin 192.168.0.5
ipset -A admin 192.168.0.31
ipset -A admin 192.168.0.57
ipset -A admin 192.168.0.91
ipset -A admin 192.168.0.211
```

```
iptables -A INPUT -p tcp --dport 22 -m set --set admin src ↵
  -m state --state NEW -j ACCEPT
```

In der ersten Zeile wird zunächst eine neue Gruppe vom Typ `ipmap` erzeugt. Dies ist die einfachste Gruppe, die von dem Befehl Ipset zur Verfügung gestellt wird. Hier wird eine Gruppe erzeugt, in der anschließend die IP-Adressen für das Netzwerk 192.168.0.0/24 verwaltet werden können. Anschließend fügen die nächsten fünf Zeilen fünf verschiedene IP-Adressen der Gruppe hinzu. Die `iptables`-Zeile prüft schließlich, ob der Zugriff erlaubt ist. Hierzu überprüft diese Zeile, ob der Absender des Pakets (`src`) in der Gruppe `admin` ist.

Eine besondere, sehr interessante zusätzliche Funktion erlaubt auch die Verknüpfung einzelner Gruppen untereinander. Vielleicht möchten Sie auch, dass die Admin-Rechner auf alle Ports der Firewall zugreifen dürfen. Lediglich ein bestimmter Rechner (192.168.0.211) darf nur auf die beiden Ports 22 und 443 zugreifen. Auch diese Aufgabe können Sie mit Hilfe von Sets lösen. Hierzu erzeugen Sie zunächst eine zweite Gruppe:

```
ipset -N adminports portmap --from 1 --to 1023
ipset -A adminports 22
ipset -A adminports 443
```

Nun binden Sie diese Gruppe an den Eintrag für die IP-Adresse 192.168.0.211:

```
ipset -B admin 192.168.0.211 -b adminports
```

Jetzt müssen Sie nur noch die Iptables-Regel ändern:

```
iptables -A INPUT -p tcp -m set --set admin src,dst
  -m state --state NEW -j ACCEPT
```

Diese Regel prüft nun, ob der Absender des Pakets in der Gruppe `admin` vorhanden ist. Falls eine Bindung an die IP-Adresse erfolgt ist, prüft die Regel zusätzlich, ob die gebundenen Informationen mit dem Ziel (`dst`) übereinstimmen. Ist keine Bindung vorhanden, wird keine zusätzliche Prüfung durchgeführt.

Diese Informationen sollen zunächst als Einführung genügen. Die nächsten Abschnitte stellen die Gruppen und die genaue Syntax der Befehle vor.

25.2 Die Ipset-Typen

Mit dem Ipset-Befehl können Sie viele verschiedene Arten von Gruppen verwalten. Die Art der Gruppe bestimmt die in der Gruppe gespeicherten Informationen.

Ipset unterstützt die folgenden Gruppen:

- `ipmap`: Speichert IP-Adressen oder Netzwerke identischer Größe.
- `portmap`: Speichert Portnummern.

- `macipmap`: Speichert MAC/IP-Adresspaare.
- `iphash`: Speichert IP-Adressen oder Netzwerke identischer Größe.
- `nethash`: Speichert Netzwerke unterschiedlicher Größe.
- `ipporthash`: Speichert IP/Port-Paare.
- `iptree`: Speichert IP-Adressen mit einer begrenzten Lebensdauer.

Diese verschiedenen Gruppen werden im Folgenden genauer besprochen und mit Beispielen vorgestellt.

25.2.1 ipmap

Die `ipmap`-Gruppe ist eine Bitmap, bei der jede IP-Adresse durch ein einzelnes Bit repräsentiert wird. Sie eignet sich daher sehr gut zur Speicherung nahe beieinander liegender IP-Adressen. Die maximale Größe der Bitmap beträgt 65.536 Adressen und entspricht damit einem Klasse-B-Netzwerk. Eine Bitmap dieser Größe belegt nur 8 kByte Arbeitsspeicher, da pro Adresse ein Bit benötigt wird. Die `ipmap`-Gruppe ist daher sehr speicherschonend und gleichzeitig sehr schnell, da direkt auf die Information, ob eine Adresse in der Gruppe vorhanden ist, zugegriffen werden kann.

Bei der Erzeugung einer neuen `ipmap`-Gruppe müssen Sie entweder das zu verwaltendene Netzwerk angeben (`--network <net/mask>`) oder die Start- und die Ziel-IP-Adresse definieren (`--from <ip> --to <ip>`).

Wenn Sie nicht IP-Adressen, sondern Netzwerke testen möchten, können Sie das auch mit dieser Gruppe bewerkstelligen. Dafür müssen die Netzwerke lediglich eine identische Größe aufweisen. Diese Größe geben Sie gleichzeitig mit der Option `--netmask <CIDR>` an. Um zum Beispiel eine Gruppe zu erzeugen, in der Sie alle IP-Adressen als Klasse-A-Netzwerke verwalten können, können Sie die folgende Zeile verwenden:

```
ipset -N badnetworks ipmap --network 0/0 --netmask 8
```

Die entstehende Bitmap ist 256 Netze groß. Sie können nun einzelne Netze hinzufügen oder entfernen. Dies erleichtert zum Beispiel eine Prüfung auf die noch nicht zugewiesenen und damit nicht erlaubten Netze sehr. Die IANAAssigned Number Authority pflegt eine Liste sämtlicher IP-Adressen (*http://www.iana.org/assignments/ipv4-address-space*). Sie könnten alle hier als *Reserved* aufgeführten Netze dieser Liste hinzufügen und in der `raw`-Table bereits alle diese Pakete verwerfen. Hiermit schützen Sie sich vor Spoofing-Angriffen, bei denen der Angreifer diese IP-Adressen nutzt.

25.2.2 portmap

Diese Gruppe ist in ihrem internen Aufbau mit der `ipmap` identisch. Es handelt sich ebenfalls um eine Bitmap mit einer maximalen Größe von 65.536 Ports. Daher können Sie sämtliche möglichen Ports in einer Bitmap speichern. Genau wie die `ipmap`-Gruppe ist auch diese Gruppe sehr schnell und benötigt nur wenig Speicherplatz.

Für die tatsächliche Anwendung können Sie auch den Speicherverbrauch durch die Angabe der Größe weiter einschränken. Sie können den ersten und den letzten in der Gruppe zu verwaltenden Port mit `--from <port>` und `--to <port>` angeben.

Diese Gruppe ist besonders interessant, da Sie diese Gruppe wie alle anderen für Verknüpfungen der Gruppen untereinander nutzen können und so einzelne IP-Adressen aus der `ipmap`-Gruppe auf bestimmte Ports beschränken können.

25.2.3 macipmap

Diese Gruppe speichert nicht nur wie die Gruppe `ipmap` IP-Adressen, sondern die Kombination aus einer IP-Adresse und der MAC-Adresse. Die maximale Größe dieser Gruppe beträgt wie bei der `ipmap`-Gruppe 65.536 Adressen. Da jedoch zusätzlich die MAC-Adresse gespeichert werden muss, erhöht sich der Speicheraufwand pro IP-Adresse von 1 Bit auf 8 Byte. Bei 65.536 Adressen benötigen Sie also 512 kByte Arbeitsspeicher. Daher ist es sinnvoll, die Größe der Gruppe sinnvoll zu beschränken. Hierfür geben Sie entweder die Start- und End-IP-Adresse mit `--from <ip>` und `--to <ip>` an, oder Sie definieren das Netzwerk mit `--network <net/mask>`.

Tipp

Sie können hiermit eine Datenbank mit allen IP-Adressen und den dazugehörigen MAC-Adressen in Ihrem Netzwerk aufbauen. Anschließend verwerfen Sie in der `raw`-Tabelle alle Pakete, deren Absender nicht in der Tabelle aufgeführt wird. So unterdrücken Sie wirkungsvoll jedes IP- und ARP-Spoofing in Ihrem Netzwerk. Speziell für diesen Zweck besitzt diese Gruppe auch noch die Option `--matchunset`, die Sie bei der Erzeugung der Gruppe angeben können. Damit wird jede IP-Adresse, die nicht in der Gruppe gespeichert wurde, aber aufgrund des Bereichs in der Gruppe gespeichert werden könnte, als Treffer bewertet. Wenn Sie diese Pakete verwerfen, kommen nur noch Pakete durch Ihre Firewall, deren IP/MAC-Adresskombinationen Sie zuvor in der Gruppe definiert haben. Dies ist in großen Netzen oder in mit DHCP verwalteten Netzen jedoch leider nur schlecht umsetzbar.

Achtung

Die MAC-Adresse ist nur sinnvoll als Absenderadresse auswertbar. Daher wird die MAC-Adresse auch immer als Source-Adresse von dem `set`-Match und dem `SET`-Target genutzt. Die Verwendung als Ziel-MAC-Adresse ist nicht möglich.

Um nun eine IP-Adresse der Gruppe hinzuzufügen, verwenden Sie die folgende Syntax:

```
ipset -N valid_ip_macs macipmap --network 192.168.0.0/24 --matchunset
ipset -A valid_ip_macs 192.168.0.100%00:50:56:C0:00:03
```

25.2.4 iphash

Es gibt insgesamt drei verschiedene Möglichkeiten, IP-Adressen in einer Gruppe zu speichern: `ipmap`, `iphash` und `iptree`. Während `ipmap` nahe beieinander liegende IP-Adressen speicherschonend und schnell verwalten kann, ist `iphash` optimiert, um beliebige, zufällige IP-Adressen aus dem gesamten Adressraum in einer Gruppe zusammenzufassen. Das ist mit der `ipmap`-Gruppe nicht möglich. Die `ipmap`-Gruppe kann maximal einen Bereich von 65.536 benachbarten IP-Adressen verwalten.

Die `iphash`-Gruppe besitzt einige Optionen, mit denen Sie bei der Erzeugung der Gruppe ihr Verhalten beeinflussen können. Mit der Option `--hashsize <größe>` setzen Sie die initiale Größe des Hashs (1024). Wenn Sie einen neuen Eintrag hinzufügen, definieren Sie mit `--probes <versuche>`, wie viele Versuche für die Einfügung der neuen IP-Adresse durchgeführt werden sollen, bevor der Hash vergrößert wird (8). Mit `--resize <prozent>` geben Sie an, wie der Hash vergrößert werden soll (50%). Wenn Sie keine Vergrößerung wünschen, definieren Sie hier 0.

Die Anzahl der Versuche (`--probes`) hat direkte Auswirkungen auf die Geschwindigkeit und die Größe des Hashs. Während kleine Werte (1-3) einen schnellen, aber großen Hash erzeugen, optimieren große Werte (6-10) die Größe des Hashs, erzeugen dabei aber einen langsameren Hash. Die Geschwindigkeit hängt linear von der Versuchsanzahl ab.

Ähnlich wie bei der `ipmap`-Gruppe können Sie in dem `iphash` auch Netzwerke identischer Größe speichern. Dazu definieren Sie bei der Erzeugung des Hashs deren Größe mit `--netmask <CIDR>`.

25.2.5 nethash

Sie können Netzwerke in mehreren Gruppen verwalten. Sowohl die Gruppen `ipmap` als auch `iphash` bieten Ihnen die Möglichkeit, auch Netzwerke identischer Größe zu verwalten. Wenn Sie aber Netze unterschiedlicher Größe in einer gemeinsamen Gruppe verwalten möchten, müssen Sie den Typ `nethash` verwenden.

Dieser Typ verfügt über die identischen Optionen wie der `iphash`: `--hashsize <größe>`, `--probes <versuche>` und `--resize <prozent>`. Diese Optionen haben auch die gleiche Bedeutung wie beim `iphash`. Wenn Sie Netze der Gruppe hinzufügen, müssen Sie diese als `IP/CIDR-Mask` angeben.

Die Geschwindigkeit des Hashs ist linear abhängig von der Anzahl der Versuche und der Anzahl der verschiedenen Netzwerkmasken, die von den gespeicherten Netzen genutzt werden.

25.2.6 ipporthash

Der `ipporthash` ist eine besondere Variante des `ipmap`-Typs. Diese Gruppe speichert zusätzlich zu der IP-Adresse auch einen Port in der Syntax `IP%Port` ab. Insgesamt können Sie für 65.536 IP-Adressen beliebige Portnummern in dieser Gruppe speichern. Den IP-Adressbereich müssen Sie bei der Erzeugung der Gruppe angeben. Hierfür verwenden Sie wieder `--from <ip>` und `--to <ip>` oder `--network <ip/mask>`. Die anderen Parameter sind in ihrer Verwendung und Funktion mit den Parametern des `iphash` identisch.

25.2.7 iptree

Dieser Typ erlaubt die Generierung einer weiteren dritten Gruppe, in der Sie IP-Adressen speichern können. Im Gegensatz zu `ipmap` und `iphash` können Sie aber für die IP-Adressen eine Lebensdauer angeben (`--timeout <sekunden>`). Jede neu hinzugefügte IP-Adresse wird nur für diese Zeit in der Gruppe gespeichert. Entweder geben Sie die Lebensdauer mit der genannten Option bei der Erzeugung der Gruppe an, oder Sie geben für jede IP-Adresse beim Hinzufügen eine spezifische Lebensdauer an (`IP%<Lebensdauer>`).

Tipp

Diese Funktion können Sie hervorragend nutzen, um Clients für eine bestimmte Zeit, zum Beispiel nach Bezahlung eines bestimmten Betrags, Zugriff auf ein Netz zu geben. Programmieren Sie nur ein Web-Interface, das die Bezahlung entgegennimmt und die IP-Adresse des Clients für die bezahlte Zeit der Gruppe hinzufügt.

Auch wenn Sie bestimmte Zugänge erst durch ein Web-Interface für eine bestimmte Zeit freischalten möchten, können Sie das hiermit erreichen. Das Web-Interface fügt einfach die entsprechende IP-Adresse zur Gruppe hinzu. Die Gruppe entfernt nach Ablauf der Lebensdauer die IP-Adresse selbstständig.

25.3 Das Kommando ipset

Mit dem Kommando `ipset` können Sie die Gruppen erzeugen, Einträge hinzufügen, entfernen und die Gruppen auch zerstören. Hierfür verwendet der `ipset`-Befehl ähnliche Optionen wie `iptables`:

- `-N <set> <type>`: Hiermit erzeugen Sie eine neue Gruppe. Sie müssen dabei mindestens den Namen und den Typ der Gruppe angeben. Bei einigen Typen müssen Sie zusätzlich weitere Optionen definieren.

  ```
  ipset -N badnetworks ipmap --network 0/0 --netmask 8
  ```

- `-X [<set>]`: Hiermit löschen Sie eine oder alle Gruppen. Bevor die Gruppe jedoch gelöscht wird, werden alle Referenzen (Bindungen) von dieser Gruppe auf an-

dere Gruppen gelöscht. Falls diese Gruppe selbst von einer anderen Gruppe referenziert wird, kann der Löschvorgang nicht durchgeführt werden.

- `-F [<set>]`: Hiermit löschen Sie alle Einträge in einer oder allen Gruppen.
- `-E <oldname> <newname>`: Hiermit benennen Sie eine Gruppe um.
- `-W <set> <set>`: Dies tauscht zwei Gruppen im Kernel aus. Damit können Sie sehr einfach eine Gruppe offline vorbereiten und für die Verwendung atomar austauschen. Es entsteht kein Zeitfenster, in dem während des Aufbaus der Gruppe diese nicht vollständig definiert ist.
- `-L [<set>]`: Diese Option zeigt den Inhalt einer oder aller Gruppen an. Mit der Option `-n` erzeugen Sie eine numerische Ausgabe. Die Option `-s` sortiert die Einträge.
- `-S`: Diese Option sichert die Einträge einer oder aller Gruppen auf der Standardausgabe. Zum Speichern können Sie die Ausgabe in eine Datei umleiten und später mit der Option `-R` wieder einlesen.
- `-R`: Hiermit stellen Sie die gespeicherten Informationen wieder her. Diese Option liest Ihre Befehle über die Standardeingabe.

  Wenn Sie die Datei nicht mit der Option `-S` erzeugen möchten, sondern dies manuell oder über ein anderes Skript erreichen, achten Sie bitte darauf, dass die Reihenfolge der Befehle wichtig ist. Als letzter Befehl ist auch jedes Mal der `COMMIT` anzugeben! Dieser Befehl beendet die Liste der Einträge. Zur Verdeutlichung speichern Sie einfach mit der Option `-S` die Einträge in einer Datei und nehmen diese als Beispiel.
- `-A <set> <IP>`: Diese Option fügt einen Eintrag einer Gruppe hinzu.
- `-D <set> <IP>`: Diese Option löscht einen Eintrag von einer Gruppe.
- `-T <set> <IP>`: Hiermit können Sie testen, ob ein Eintrag in einer Gruppe enthalten ist.
- `-B <set> <IP> --binding <set>`: Hiermit können Sie einen Eintrag in einer Gruppe zusätzlich an eine andere Gruppe binden. Damit dieser Eintrag später zutrifft, muss auch die gebundene Gruppe zutreffen.
- `-U <set> <IP>`: Hiermit lösen Sie die Bindung eines Eintrags.
- `-H`: Dies zeigt Ihnen die Hilfe an.

Tipp

Immer wenn Sie eine administrative Änderung der Gruppen durchführen müssen, die eine Erzeugung einer neuen leeren Gruppe verlangt, die anschließend aufgefüllt wird, bietet es sich an, die Gruppe zu erzeugen und anschließend auszutauschen.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

26 Hochverfügbare Firewalls

Wenn Sie verschiedene Firewalls geplant und implementiert haben, werden Sie irgendwann an den Punkt geraten, wo Ihre erste Firewall hochverfügbar sein soll. Das bedeutet, dass die Internetverbindung trotz eines Ausfalls des Firewall-Systems weiter gewährleistet sein muss. Dieses Kapitel zeigt Ihnen verschiedene Wege, das Ziel zu erreichen. Dabei betrachte ich auch die ganz neue und noch nicht ganz fertige Zustandssynchronisation über `ct_sync`.

26.1 Was ist Hochverfügbarkeit, und wo ist das Problem?

Hochverfügbarkeit ist eine heute übliche Anforderung an geschäftskritische Systeme. In vielen Unternehmen zählt auch die Firewall hierzu. Ein Ausfall der Firewall oder der Internetverbindung verursacht hohe Kosten. Potenzielle Kunden können nicht auf die Website gelangen, und wichtige E-Mails erreichen nicht ihren Empfänger. Wenn eine Firewall hochverfügbar ist, bedeutet das, dass ein Ausfall der Funktion sehr selten ist.

Die Verfügbarkeit wird in Prozent gemessen. Wenn Ihre Firewall eine 99%ige Verfügbarkeit aufweisen soll, bedeutet das, dass sie nur 1% im Jahr ausfallen darf. Bei 365 Tagen sind das 3 Tage, 15 Stunden und 36 Minuten. Dies können Sie vielleicht noch mit einem einfachen System gewährleisten. Bei einem Ausfall pro Jahr haben Sie sicherlich innerhalb von 1 bis 2 Tagen Ersatz geschaffen. Meist wird aber eine Verfügbarkeit von 99,9% oder sogar 99,99% gefordert. Das bedeutet, dass das System nur 0,1% (8 Stunden, 46 Minuten) oder gar 0,01% (52 Minuten) im Jahr ausfallen darf. Ein einfacher Stromausfall, Upgrade des Betriebssystems oder Reboot bereitet da unter Umständen schon Kopfschmerzen.

Falls Sie eine derartige Verfügbarkeit garantieren müssen, können Sie das nur leisten, wenn im Falle des Ausfalls des primären Systems die Funktion durch ein zweites Backup-System aufrechterhalten wird. Daher werden derartige Lösungen meist als Cluster aus zwei Knoten implementiert, die sich gegenseitig ersetzen können.

Bei einem einfachen Hochverfügbarkeits-Cluster ist einer der beiden Knoten aktiv (Master) und stellt die Funktion zur Verfügung, während der zweite Knoten passiv als Hot-Standby nur im Fehlerfall die Funktion des Masters übernimmt (Slave, Hot-Standby). Dies nennt man auch einen Hot-Standby-Cluster. Fortgeschrittene Cluster können die Hochverfügbarkeit auch mit zwei aktiven Knoten realisieren. Solange beide Knoten zur Verfügung stehen, wird die Funktion über beide Knoten realisiert.

Sobald ein Knoten ausfällt, übernimmt der zweite Knoten die komplette Funktion. In dieser Konstellation ist die Backup-Hardware nicht die meiste Zeit ungenutzt, sondern wird sinnvoll eingesetzt. Diese Cluster werden als Active-Active-Cluster bezeichnet.

Das wesentliche Problem bei einem Cluster ist die gemeinsame Nutzung der identischen Daten für die Bereitstellung der Funktion. Ein Datenbank- oder Webserver-Cluster muss sowohl auf dem Master als auch auf dem Hot-Standby-Knoten über identische Webseiten oder Datenbanken verfügen. Handelt es sich um statische Daten, so können diese einfach einmalig synchronisiert werden. Werden diese Daten jedoch bei der Verwendung des Systems dynamisch modifiziert, weil zum Beispiel neue Einträge in der Datenbank vorgenommen werden oder vorhandene Einträge geändert werden, so müssen diese Änderungen auch sofort auf den Hot-Standby übertragen (synchronisiert) werden. Ansonsten sind die Informationen bei einem anschließenden Ausfall des Masters verloren. Bei Datenbanken und Webservern wird dies häufig durch ein gemeinsam genutztes Dateisystem (Shared Storage) zum Beispiel in einem Storage-Area-Network (SAN) realisiert.

Noch komplizierter wird die Realisierung eines Active-Active-Clusters, beim theoretisch auf beiden Knoten gleichzeitig ein Schreibzugriff auf das identische Feld in einer Datenbank erfolgen kann. Hier sind sehr intelligente Mechanismen erforderlich, um die Datenkonsistenz zu gewährleisten.

Wo ist nun das Problem bei Firewalls? Eine Firewall verfügt doch über einen statischen Regelsatz, der sehr einfach über alle Knoten in einem Cluster synchronisiert werden kann und nur selten verändert wird. Da die Modifikationen des Regelwerks durch einen geschulten Administrator vorgenommen werden, ist es sehr unwahrscheinlich, dass dieser die Regeln gleichzeitig auf zwei Systemen verändern wird. Ein Konflikt kann daher nicht entstehen. Dennoch tauchen Probleme auf, denn moderne Firewalls wie Iptables/Netfilter sind zustandsorientierte Firewalls. Diese Firewalls werten nicht nur ihre statischen Regeln aus, sondern auch eine Zustandstabelle, die sich in Abhängigkeit von den bereits betrachteten Paketen ändert. Die statischen Firewall-Regeln entscheiden nicht allein, ob ein Paket die Firewall passieren darf oder verworfen wird. Damit beim Ausfall des Masters der Hot-Standby die Funktion komplett übernehmen kann, müssten auch die Zustandsinformationen zwischen den Knoten synchronisiert werden.

26.2 Einfache Hochverfügbarkeit

Eine einfache Hochverfügbarkeit kann gewährleistet werden, wenn die Firewall die Zustände der Verbindungen nicht überwacht. Das bedeutet, dass Sie sowohl Regeln für eingehende Pakete als auch für ausgehende Pakete definieren müssen und kein NAT oder Masquerading verwenden dürfen. Sobald Sie diese Voraussetzungen gewährleisten können, ist es recht einfach, eine hochverfügbare Firewall aufzubauen. Sie müssen dann nur mit einer der verfügbaren Clusterlösungen die Ausfallsicherheit der Systeme herstellen und bei einem Ausfall die Übernahme der IP-Adressen von dem ausgefallenen System auf das Ersatzsystem veranlassen. Wenn auf bei-

den Systemen identische Regelsätze zum Einsatz kommen, ist die Funktionalität sofort wiederhergestellt. Da keine Zustandsinformationen gespeichert werden, müssen diese auch nicht zwischen den Firewalls synchronisiert werden. Sämtliche Verbindungen laufen ohne Unterbrechung weiter.

Nun ist dieses Buch aber kein Buch über `ipchains` (eine zustandslose Firewall), sondern betrachtet mit Netfilter/Iptables eine zustandsorientierte Firewall. Sicherlich kann man auch mit Iptables zustandslose Firewalls konfigurieren, allerdings ist das unter sicherheitstechnischen Gesichtspunkten nicht sinnvoll. Daher werde ich diesen Punkt hier nicht weiter ausführen und direkt zur Hochverfügbarkeit bei einer zustandsorientierten Firewall übergehen.

26.3 Hochverfügbarkeit bei zustandsorientierten Firewalls

Natürlich können Sie auch bei einer zustandsorientierten Firewall denselben Ansatz wählen, wie ich ihn gerade bei der zustandslosen Firewall beschrieben habe. Sie wählen eine Cluster-Software Ihrer Wahl (zum Beispiel Heartbeat oder KeepAlived) und konfigurieren diese so, dass sie bei Ausfall des Master-Nodes automatisch ein Fail-Over zum Hot-Standby durchführt. Bei diesem Fail-Over werden automatisch von der Cluster-Software auch die IP-Adressen übertragen. Verfügt nun der Hot-Standby-Node über ein identisches Regelwerk, ist eine gewisse Funktionalität sofort wiederhergestellt. Sie können sofort wieder neue Verbindungen über die Firewall aufbauen. Leider sind alle zum Zeitpunkt des Fail-Overs aufgebauten Verbindungen nun tot. Die Information, welche Verbindungen von der ausgefallenen Firewall zugelassen wurden, befand sich in deren Zustandstabelle. Deren Inhalt ist verloren und steht der neuen Firewall nicht zur Verfügung. Daher kennt diese nicht die vor dem Fail-Over existenten Verbindungen und wird diese nicht erlauben.

Wenn Sie den Verlust der aufgebauten Verbindungen beim Fail-Over akzeptieren können, ist die Realisierung dieser Hochverfügbarkeitslösung die einfachste und eine sehr unproblematische Variante.

Tipp: Automatische Erkennung aufgebauter Verbindungen nach dem Fail-Over

Sie können mit dieser Lösung, wenn Sie kein NAT einsetzen, sogar in vielen Fällen echte Hochverfügbarkeit garantieren. Dafür müssen Sie jedoch Ihre Regeln unter Umständen anpassen.

Die Wiedererkennung aufgebauter Verbindungen nach einem Fail-Over ist insbesondere für Langzeit-TCP-Verbindungen wichtig. Das bedeutet, dass der Hot-Standby nach einem Fail-Over besonders diese Verbindungen erkennen und wieder in seine Zustandstabelle aufnehmen muss. Der Connection-Tracking-Code von Netfilter ist hierzu in der Lage. Bei dem Protokoll TCP werden die folgenden zwei Pakete als neue Pakete (State: `NEW`) akzeptiert:

- TCP-SYN-Pakete. Diese Pakete bauen normalerweise eine Verbindung auf.
- TCP-ACK-Pakete. Diese Pakete werden nach dem Aufbau einer Verbindung ausgetauscht. Dieses Paket überführt eine unbekannte Verbindung sofort in den Zustand `ESTABLISHED`.

Wenn Sie folgende Regeln verwenden, kann Ihre Firewall nach einem Fail-Over vorher vorhandene Verbindungen erkennen und automatisch wieder erlauben:

```
$INTDEV=eth0
$EXTDEV=eth1
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p tcp --dport 22 -m state ↵
  --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state ESTABLISHED,RELATED -j ACCEPT
```

Wenn vor dem Fail-Over nun ein interner Client eine SSH-Verbindung zu einem Server in dem Internet aufbaut, wird er den kompletten TCP-Handshake durchlaufen, und die Firewall wird die Verbindung in Ihrer Zustandstabelle eintragen. Alle weiteren Pakete, die der Client nun mit dem Server austauscht, tragen bis zur Beendigung der Verbindung lediglich das TCP-ACK-Bit. Kommt es nun zum Fail-Over, so verfügt der Hot-Standby über den identischen Regelsatz, aber nicht über die Zustandstabelle. Die Verbindung ist daher unbekannt. Wenn nun der Server ein weiteres TCP-ACK-Paket an den Client sendet, wird die Firewall dieses Paket nicht zulassen, da sie die Verbindung nicht kennt. Sendet der Client jedoch ein TCP-ACK-Paket an den Server, so akzeptiert die Firewall auch dieses Paket als Verbindungsaufbau und trägt die Verbindung sofort wieder in der Zustandstabelle mit dem Zustand `Established` ein. Alle weiteren Pakete dieser Verbindung, des Clients und des Servers, dürfen dann auch den Hot-Standby passieren.

Diese Funktionalität ist nicht gegeben, wenn Sie in den Regeln zusätzlich die Option `--syn` angeben:

```
$INTDEV=eth0
$EXTDEV=eth1
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p tcp --dport 22 ↵
  --syn -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state ESTABLISHED,RELATED -j ACCEPT
```

Nun wird nur dann ein Paket als Verbindungsaufbau akzeptiert, wenn es sich tatsächlich um ein TCP-SYN-Paket handelt. Eine Wiederaufnahme einer alten Verbindung nach einem Fail-Over oder

auch einem Neustart der Firewall ist nicht mehr möglich. Die Verbindungen »hängen« und müssen komplett neu aufgebaut werden.

Auch wenn Sie den Parameter `/proc/sys/net/ipv4/netfilter/ip_conntrack_tcp_loose=0` setzen, funktioniert dies nicht mehr (siehe Abschnitt 19.4.8).

Außerdem funktioniert die Wiederaufnahme von alten Verbindungen nicht richtig, wenn die Firewall zusätzlich noch ein Masquerading oder ein N:1-NAT durchführt.

26.4 Praktische Implementierung mit KeepAlived

Um nun eine derartige hochverfügbare Firewall aus zwei Knoten zu implementieren, benötigen Sie eine Software, mit der Sie die Verfügbarkeit prüfen und einen Fail-Over durchführen können. Ein Kandidat für diese Aufgabe ist KeepAlived. Diese Software von dem Linux-Virtual-Server-Projekt (LVS) ist ein Userspace-Daemon, der die Gesundheit der Cluster-Knoten überwacht und einen Fail-Over durchführen kann. Sie können die KeepAlived-Software von der Homepage *http://www.keepalived.org* herunterladen. Die KeepAlived-Software ist aber auch Bestandteil von vielen Distributionen. Prüfen Sie zunächst, ob Ihre Distribution ein Paket zur Verfügung stellt.

Nach der Installation müssen Sie KeepAlived konfigurieren. KeepAlived soll eine hochverfügbare Firewall realisieren. Wenn wir für einen Moment die Firewall-Regeln vernachlässigen, handelt es sich bei der Funktion, die wir hochverfügbar anbieten möchten, um die Routing-Funktionalität der Firewall. Dass die Firewall nebenbei auch noch filtert, ist ja nur ein zusätzliches Bonbon. Speziell für diesen Zweck implementiert KeepAlived das Virtual Router Redundancy Protocol (VRRP, RFC2338).

Tipp

Das VRRP-Protokoll ist möglicherweise durch Patente geschützt. Sowohl Cisco (*http://www.ietf.org/ietf/IPR//VRRP-CISCO*) als auch IBM (*http://www.ietf.org/ietf/IPR/NAT-VRRP-IBM*) behaupten, dass das VRRP-Protokoll ihre Patente verletzen würde. Deshalb hat das OpenBSD-Projekt mit dem Common Address Redundant Protocol (CARP) ein patentfreies und sicheres Protokoll geschaffen. Mit UCARP, einem Userspace-Daemon (*http://www.ucarp.org*), kann dieses Protokoll auf Linux und BSD benutzt werden. Ich verwende hier den KeepAlived mit VRRP, da dies auch die bevorzugte Variante des Netfilter-Teams ist.

So können Sie zwei oder mehr redundante Router zusammenfassen, so dass sie sich als ein virtueller Router dem lokalen Netz präsentieren. Hierzu beobachtet KeepAlived mit dem VRRP-Protokoll die redundanten Router und deren Gesundheit und wählt einen Master-Router, der zusätzlich zu seiner realen IP-Adresse die

virtuelle Adresse des virtuellen Routers erhält. Alle weiteren Router werden als Slave bezeichnet. Diese kontrollieren die Gesundheit des Masters und übernehmen bei dessen Ausfall die virtuelle Router-IP-Adresse. Ist der Master später wieder verfügbar, so übergibt der Slave die virtuelle Router-IP-Adresse wieder an den Master.

Tipp

Das VRRP-Protokoll ist von der Internet Engineering Task Force (IETF) spezifiziert worden und wird von vielen kommerziellen Routern ebenfalls unterstützt.

Die Konfiguration des KeepAlived-Daemons erfolgt in der Datei `/etc/keepalived/keepalived.conf`. Eine Beispieldatei für einen Master könnte folgendermaßen aussehen:

```
vrrp_sync_group VG1 {
  group {
    eth0
    eth1
  }
}
! Interne virtuelle IP-Adresse
vrrp_instance VI_1 {
 state MASTER
 interface eth0
 virtual_router_id 1
 priority 100
 authentication {
  auth_type AH
  auth_pass password
 }
 virtual_ipaddress {
  192.168.1.1/24 brd 192.168.1.255 dev eth0
 }
}
! Externe virtuelle IP-Adresse
vrrp_instance VE_1 {
 state MASTER
 interface eth1
 lvs_sync_daemon_interface eth0
 virtual_router_id 2
 priority 100
 authentication {
  auth_type AH
```

```
  auth_pass password
 }
 virtual_ipaddress {
  192.168.2.1/24 brd 192.168.1.255 dev eth1
 }
}
```

Die entsprechende Datei für den Slave hat folgenden Inhalt:

```
vrrp_sync_group VG1 {
  group {
    eth0
    eth1
  }
}
vrrp_instance VI_1 {
 state BACKUP
 interface eth0
 virtual_router_id 1
 priority 50
 authentication {
  auth_type AH
  auth_pass password
 }
 virtual_ipaddress {
  192.168.1.1/24 brd 192.168.1.255 dev eth0
 }
}
vrrp_instance VE_1 {
 state BACKUP
 interface eth1
 lvs_sync_daemon_interface eth0
 virtual_router_id 2
 priority 50
 authentication {
  auth_type AH
  auth_pass password
 }
 virtual_ipaddress {
  192.168.2.1/24 brd 192.168.1.255 dev eth1
 }
}
```

Wichtig ist, dass sowohl der Slave als auch der Master die identische `virtual_router_id` für die jeweilige Instanz besitzen. Jede Instanz ist für eine virtuelle IP-Adresse des Routers verantwortlich. Damit diese IP-Adressen beim Ausfall

einer IP-Adresse auch beide gemeinsam übertragen werden, werden sie in einer `vrrp_sync_group` zusammengefasst. Die vergebene Priorität entscheidet, welches der beiden Systeme der Master ist. Bei mehreren Slaves variieren Sie die Priorität leicht zwischen den verschiedenen Slaves (50, 49, 48 etc.). Mit dem Parameter `state` können Sie entscheiden, in welchem Zustand der KeepAlived-Daemon auf diesem System starten soll: `MASTER` oder `BACKUP`. Die `virtual_ipaddress` ist einmal die interne und einmal die externe IP-Adresse des virtuellen Routers. Bei der Authentifizierung sollten Sie darauf achten, dass Sie AH wählen, da die PASS-Authentifizierung das Kennwort im Klartext austauscht. Der Parameter `lvs_sync_daemon_interface` definiert die Netzwerkkarte, über die die Kommunikation zwischen den KeepAlived-Daemons für diese Instanz erfolgen soll. Auf einer Firewall ist es sinnvoll, diese Informationen in dem internen Netz zu halten oder sogar auf ein eigenes getrenntes Netz auszuweichen.

Wenn Sie nun den KeepAlived-Daemon starten, wird das erste System sich als Master konfigurieren und die virtuelle IP-Adresse übernehmen. Sobald der Master ausfällt, wird der Slave die Funktion übernehmen. Sie müssen nun nur allen internen Clients als Standard-Gateway die virtuelle IP-Adresse des Routers zuweisen: 192.168.1.1/24. Dann können Sie Ihre neue hochverfügbare Firewall nutzen!

26.5 Hochverfügbarkeit und Masquerading/NAT

Sobald Sie SNAT oder Masquerading nutzen, wird Ihr hochverfügbarer Firewall-Cluster nicht mehr richtig funktionieren. Um das zu verstehen, müssen Sie sich vor Augen führen, dass eine Firewall bei einem Masquerading oder N:1-SNAT[1] die Firewall häufig nicht nur die IP-Adresse, sondern auch den TCP- oder UDP-Port austauscht. Stellen Sie sich vor, ein Client1 baut durch Ihre Firewall eine Verbindung zu einem Webserver in dem Internet auf. Der Client1 verwendet den Quellport 1027. Dieser Port ist jedoch auf der Firewall bereits durch eine andere genattete Verbindung belegt. Dann wird die Firewall beim NAT nicht nur die IP-Adresse, sondern auch den Quellport modifizieren. Hierfür wählt sie den nächsten geeigneten freien Port aus. Dieser ist natürlich stark abhängig von den anderen gerade aktiven und in der Vergangenheit aktiven Verbindungen. In unserem Beispiel (Abbildung 26.1) ist es der Port 1275. Für den Webserver wird die Verbindung nun von 3.0.0.1:1275 aufgebaut.

Nach dem Fail-Over wird der zweite Knoten des Firewall-Clusters die Verbindung wieder aufnehmen. Da sich dieser aber nicht in demselben Zustand befindet wie der alte Master vor dem Fail-Over, wird er bei der Wahl des NAT-Ports entweder den Port gar nicht verändern, da dieser Port 1027 noch frei ist, oder sicherlich einen anderen wählen. Der Webserver wird die Pakete aber nicht zu der Verbindung zählen, da sie über einen falschen Quellport verfügen und die Pakete verwerfen. Die Verbindung hängt bis zum Timeout.

[1] Ein N:1-SNAT ist ein Source-NAT, bei dem viele verschiedene Absender-IP-Adressen gegen eine IP-Adresse ausgetauscht werden. Dies ist der häufigste Fall des SNAT. Masquerading bezeichnet unter Linux dann den Umstand, dass diese IP-Adresse dynamisch zugewiesen wird.

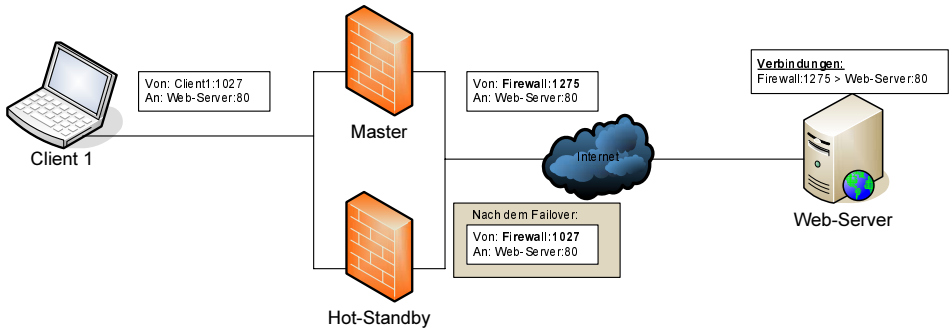


Abbildung 26.1: NAPT (Network Address and Port Translation) macht bei einem einfachen Firewall-Cluster einen Strich durch die Rechnung.

Sobald Sie NAT einsetzen, ist es daher zwingend erforderlich, dass die Zustandstabelle von dem Master auf alle Slaves in dem Cluster synchronisiert wird, da die hier gespeicherten Informationen (NAT) für die Modifikation der Pakete beim NAT der Verbindung zwingend erforderlich sind. Diese Zustandssynchronisation kann mit `ct_sync` durchgeführt werden.

26.6 Zustandssynchronisation mit ct_sync

Viele kommerzielle Firewalls verfügen seit einigen Jahren über eine Synchronisation der Zustandstabelle in einem Firewall-Cluster. Selbst OpenBSD hat mit `pfsync` eine seit Jahren stabile Implementierung dieser Funktion. In dem Linux-Kernel ist bis heute keine derartige Lösung integriert. Bisher existiert nur Beta-Code, der sich jedoch mit einigen wenigen Einschränkungen bereits sehr gut einsetzen lässt. Dieser Code ist für den Linux-Kernel 2.4.26 und den Linux-Kernel 2.6.10 verfügbar. Er implementiert mit `ct_sync` ein Connection Tracking-Synchronisationsframework, das den Aufbau eines Hot-Standby-Clusters ermöglicht. Da die Entwicklung hier noch stark im Fluss ist, empfehle ich Ihnen bei Interesse die Netfilter-Failover-Mailingliste zu abonnieren. Das Volumen dieser Mailingliste ist aktuell sehr gering und stellt daher keine Belastung dar. Sie finden die Mailingliste auf *http://lists.netfilter.org/mailman/listinfo/netfilter-failover*.

Achtung

Der aktuelle Entwicklungsstand (Oktober 2005) erlaubt noch nicht die Verwendung von Conntrack- oder NAT-Helfermodulen. So können FTP-Datenverbindungen, die von dem `ip_conntrack_ftp`-Helfermodul erkannt und zugelassen werden, noch nicht synchronisiert werden. Im Gegenteil, die Anwendung einiger Module hat auch schon in Kombination mit `ct_sync` zur Kernel-Panic geführt.

Wenn Sie auf diese Helfermodule für die Funktionalität Ihrer Firewall angewiesen sind, ist `ct_sync` aktuell für Sie nicht einsetzbar. Sie sollten die Netfilter-Failover-Mailingliste beobachten, um diesbezügliche Änderungen zu erfahren.

Tipp

Neueste Entwicklungen ermöglichen auch schon den Aufbau eines Active-Active-Clusters. Dieser Code ist zum aktuellen Zeitpunkt (Oktober 2005) aber noch sehr fehlerbehaftet und kann lediglich unter Verzicht auf NAT eingesetzt werden.

Wenn Sie mit dem Code experimentieren möchten, können Sie ihn mit folgendem Befehl aus dem Netfilter-Subversion-Server auschecken:

```
$ svn co http://svn.netfilter.org/netfilter/branches/netfilter-ha/linux-↵
  2.6-actact
```

26.6.1 Installation

Der Code ist in zwei verschiedenen Versionen für den Linux-Kernel 2.6.10 und den Linux-Kernel 2.4.26 verfügbar. Die aktuelle Entwicklung findet im Moment in dem Linux-Kernel 2.6.10 statt. Sie können den Code mit den folgenden Befehlen aus dem Netfilter-Subversion-Server auschecken:

```
$ svn co http://svn.netfilter.org/netfilter/branches/netfilter-ha/linux-2.6
$ svn co http://svn.netfilter.org/netfilter/trunk/netfilter-ha
```

Um über Updates auf dem Laufenden zu bleiben, sollten Sie in regelmäßigen Abständen in die angelegten Verzeichnisse wechseln und dort den Befehl `svn update` aufrufen:

```
$ cd linux-2.6
$ svn update
Revision 4351.
```

Sollte ein Update des Codes erfolgt sein, werden Ihnen die betroffenen Dateien beim Update angezeigt.

Nun müssen Sie Hand an Ihren Kernel legen, um `ct_sync` zu übersetzen. Zunächst benötigen Sie einen Vanilla-Kernel von *http://www.kernel.org*. Entweder wählen Sie die Version 2.4.26 oder 2.6.10. Wenn Sie dieses Buch lesen, werden möglicherweise auch schon weitere Kernel unterstützt. Entpacken Sie den Kernel, und wechseln Sie in das entstandene Verzeichnis. Dann kopieren Sie aus dem `ct_sync`-Quelltext das Verzeichnis `./patches` in den Kernel-Quelltextbaum. Außerdem kopieren Sie einige Dateien aus dem Verzeichnis `./ct_sync` in den Kernel-Quelltextbaum:

```
$ tar xjf linux-2.6.10.tar.bz2
$ cd linux-2.6.10
$ cp -r ../svn/linux-2.6/patches .
$ cp ../svn/linux-2.6/ct_sync/*.h include/linux/netfilter_ipv4/
$ cp ../svn/linux-2.6/ct_sync/*.c net/ipv4/netfilter/
```

Nun müssen Sie die kopierten Patches anwenden. Hierfür benötigen Sie den Befehl `quilt`. Falls dieser Befehl nicht Bestandteil Ihrer Linux-Distribution ist, können Sie ihn von *http://savannah.nongnu.org/projects/quilt* herunterladen und installieren. Um die Patches anzuzeigen und anschließend anzuwenden, verwenden Sie die folgenden Befehle:

```
$ quilt unapplied
$ quilt push -a
```

Nun können Sie den Kernel wie gewohnt konfigurieren und übersetzen. Wenn Sie bereits einen Kernel mit derselben Version verwenden, editieren Sie bitte die Datei `Makefile` im Wurzelverzeichnis des Kernel-Quelltextbaums und tragen dort eine EXTRAVERSION ein, um spätere Konflikte der Kernel untereinander zu vermeiden:

```
EXTRAVERSION = -ha
```

Für die Konfiguration und Übersetzung verwenden Sie die folgenden Befehle:

```
$ make xconfig
$ make dep
$ make bzImage
$ make modules
$ make modules_install
$ make install
```

Bei der Konfiguration sollten Sie dann die Synchronisation der Zustandstabelle auswählen (Abbildung 26.3). Wenn Sie den Active-Active-Cluster konfigurieren, achten Sie bitte auf Abbildung 26.2. Diese Einstellungen finden Sie am Ende unter *Device Drivers/Networking Support/Networking Options/Network Paket Filtering (replaces ipchains)/Netfilter Configuration*. Damit Sie die Optionen für den Active-Active-Cluster angezeigt bekommen, müssen Sie NAT deaktivieren!

Nach dem Reboot des neuen Kernels steht Ihnen die Zustandssynchronisation zur Verfügung.

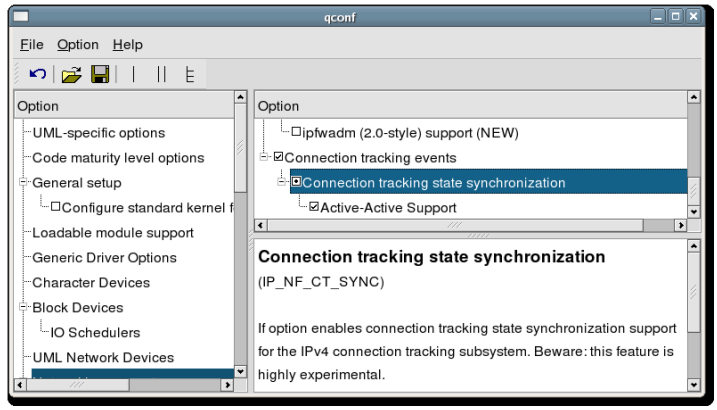


Abbildung 26.2: Für den Active-Active-Cluster muss NAT deaktiviert sein.

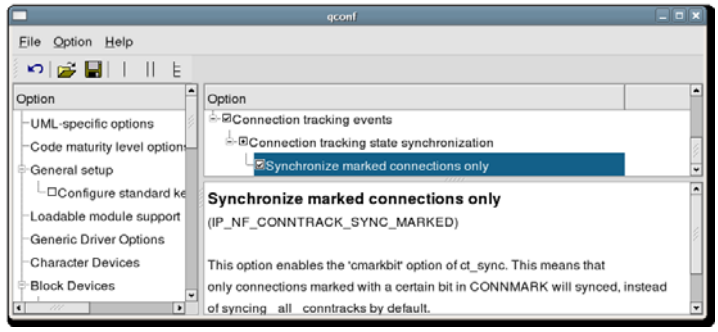


Abbildung 26.3: Bei dem Hot-Standby-Cluster können Sie die zu synchronisierenden Verbindungen durch Markierungen auswählen.

26.6.2 Funktion von ct_sync

Die Synchronisation der Zustandstabelle läuft in mehreren Schritten ab. Der aktive Master analysiert jedes Paket, ermittelt die Zustandsinformationen des Pakets und aktualisiert die Zustandstabelle. Diese Aktualisierung löst einen Connection Tracking-Event aus, der in einer Event-Queue gespeichert wird. Diese Queue wird von dem `ct_sync`-Sender-Thread abgearbeitet. Das maximale Alter der Events in dieser Queue und die maximale Größe der Queue, bevor sie abgearbeitet werden muss, kann konfiguriert werden. Der `ct_sync`-Sender-Thread verpackt bis zu 4 Nachrichten in einem Paket und überträgt dieses Paket mit einem Multicast-Protokoll an alle Slaves. Auf dem Slave werden die Pakete entgegengenommen, von der Zustandsüberwachung ignoriert (Option `notrack=1`) und an den `ct_sync`-Receive-Thread übergeben. Der extrahiert die Meldungen und aktualisiert die Zustandstabelle. Auch im `ct_sync`-Receive-Thread exisitiert eine Queue, deren maximale Größe eingestellt werden kann.

Für die Übertragung der Pakete wird ein UDP-basiertes Multicast-Protokoll verwendet, das das Netfilter-Team speziell für diesen Zweck entwickelt hat. Dieses Protokoll bietet keinerlei Authentifizierung oder Verschlüsselung und ist auf ein sicheres Medium, zum Beispiel ein dediziertes Netzwerk (Cross-Over Kabel), angewiesen. Als Schutz vor Paketverlust versieht der Master jedes Paket mit einer Sequenznummer, so dass der Slave die Vollständigkeit kontrollieren und ein verlorenes Paket neu anfordern kann.

Das Protokoll unterstützt außerdem die initiale Synchronisation eines Slaves mit einem Master. Dies ist erforderlich, da nach einem Neustart eines Slaves, zum Beispiel aus Wartungsgründen, der Slave zwar Synchronisationsmeldungen erhält, es sich dabei aber nur um Änderungen der Zustandstabelle handelt. Der Slave besitzt aber nach dem Neustart eine leere Zustandstabelle. Um diese zu füllen, müssen sämtliche Informationen des Masters übertragen werden. Diese Komplettsynchronisation wird auch durchgeführt, wenn zu viele Pakete zwischen dem Master und dem Slave verloren gegangen sind oder der Master ein verlorenes Paket nicht mehr in seinem Backlog findet. Die Anzahl der verlorenen Pakete, ab der eine Neusynchronisation auftritt, ist ebenfalls konfigurierbar.

Bei dem Laden des `ct_sync`-Kernel-Moduls können Sie vier Parameter angeben:

- `syncdev=ethX`: Die Angabe der Netzwerkkarte für die Synchronisation ist erforderlich. Es sollte sich dabei um eine Netzwerkkarte handeln, die über ein dediziertes Netzwerk mit den anderen Knoten in dem Cluster verbunden ist, denn das Protokoll bietet keinen Schutz vor Angriffen. Ein serielles Kabel genügt nicht. Eine Resynchronisation erfordert hohe Bandbreiten von mindestens 1,5 MBit/s. In vielen Fällen genügt hier ein Cross-Over-Kabel. Es kann keine zweite Netzwerkkarte genutzt werden, um für Ausfallsicherheit zu sorgen.
- `l2drop=0|1`: Hiermit geben Sie an, ob der Slave einen Layer-2-Drop durchführen soll. Damit ist es möglich, sämtliche Knoten bereits mit identischer IP-Adresskonfiguration auszustatten. In einem normalen Setup führt dies zu Adresskonflikten. Der Layer-2-Drop verwirft jedoch bereits auf der Schicht 2 sämtliche Pakete auf allen Netzwerkkarten außer dem `syncdev`. So können Sie schon die IP-Adressen aktivieren, Dienste starten und alle Knoten identisch konfigurieren. Der jeweilige Master deaktiviert den Layer-2-Drop und bietet seine Dienste an.
- `notrack=0|1`: Mit dieser Option ignoriert der lokale Connection-Tracking-Code sämtliche Pakete, die über die `syncdev`-Schnittstelle transportiert werden. Die Synchronisationspakete lösen dadurch nicht selbst auch noch Änderungen der Zustandstabelle aus.
- `cmarkbit=0-31`: Diese Option steht zur Verfügung, wenn Sie bei der Übersetzung des Kernel die Unterstützung für das `CONNMARK`-Target in Kombination mit der Synchronisation aktiviert haben. Dann können Sie durch Markierung der Verbindungen die Verbindungen auswählen, die synchronisiert werden sollen. Das ist nützlich, da häufig die Synchronisation von zum Beispiel DNS-Verkehr und ICMP-PING-Verkehr unsinnig ist. Diese »Verbindungen« bestehen nur aus ei-

nem Request- und einem Response-Paket. Bei einem Fail-Over kann der Client das Request-Paket auch erneut senden. Häufig tritt durch den Fail-Over sowieso eine Verzögerung auf, die bei diesen Verbindungen zu einem Timeout führen kann.

Achtung

Ich beschreibe hier die Funktionen des 2.6.10-Kernel-Patches. Der 2.4.26-Kernel-Patch verwendet teilweise andere Optionen und verfügt noch nicht über das mächtige `/proc`-Interface, das im Weiteren beschrieben wird. Möglicherweise ist der 2.4.26-Code, wenn Sie dieses Buch lesen, bereits aktualisiert worden. Ansonsten möchte ich Sie auf die dem Code beiliegende README-Datei verweisen.

Sobald Sie das Modul mit den geeigneten Optionen geladen haben, müssen Sie dem Modul mitteilen, in welchem Zustand sich das System befindet. Hierfür können Sie in dem `/proc`-Verzeichnis die Datei `/proc/sys/net/ipv4/netfilter/ct_sync/state` verwenden. Nach dem Laden des Moduls befindet sich in dieser Datei eine `0`. Dadurch wird effektiv das Modul deaktiviert. Durch das Schreiben von `1` wird der Knoten zum Slave. Eine `2` macht den Knoten zum Master[2]. Zusätzlich befinden sich in dem Verzeichnis `/proc/sys/net/ipv4/netfilter/ct_sync` noch weitere Dateien, deren Inhalt Sie modifizieren und so das Verhalten von `ct_sync` anpassen können:

- `maxage`: Sobald ein Event in der Sender-Event-Queue dieses Alter erreicht, muss er übertragen werden.
- `send_burst`: Sobald die Sender-Event-Queue diese Anzahl an Meldungen enthält, muss sie verarbeitet werden.
- `recv_burst`: Sobald der Slave diese Anzahl an Paketen erhalten hat, muss er die Meldungen extrahieren und die Zustandstabelle aktualisieren.
- `recovery_threshold`: Beim Verlust von Paketen wird ab diesem Schwellenwert eine komplette Neusynchronisation durchgeführt.

Tipp

Laut Aussagen des Netfilter-Teams von Sommer 2005 wird diese `/proc`-Schnittstelle in der nächsten Zeit unverändert bleiben.

[2] Achtung, auch dies hat sich gegenüber dem 2.4.26-Kernel-Patch geändert. Dort bedeutete eine `0` Slave und eine `1` Master!

Achtung

Wenn Sie das `ct_sync`-Modul auf dem Linux-Kernel 2.6.10 oder neuer verwenden, müssen Sie das seit 2.6.9 in dem Kernel befindliche TCP-Window-Tracking durch Netfilter auf dem Slave abschalten. Dies kollidiert aktuell mit der Synchronisation. Das können Sie sehr einfach erreichen, indem Sie im `/proc`-Verzeichnis die folgende Datei schreiben:

```
echo 1 > /proc/sys/net/ipv4/netfilter/ip_conntrack_tcp_be_liberal
```

26.6.3 Aufbau des ct_sync-Clusters

Um nun einen `ct_sync`-Cluster aufzubauen, können Sie zwei unterschiedliche Wege einschlagen. Entweder Sie beginnen mit dem im Abschnitt 26.4 beschriebenen Cluster und erweitern diesen um die `ct_sync`-Funktionalität, oder Sie beginnen mit zwei identisch konfigurierten Maschinen, bei denen Sie zum Test zunächst manuell `ct_sync` bedienen, und erweitern diese anschließend um eine Heartbeat-Software wie KeepAlived oder Linux-HA-Heartbeat (*http://www.linux-ha.org*). Ich werde hier den zweiten Weg einschlagen.

Beim Einsatz des Layer-2-Drops ist bei einem Fail-Over der Take-Over der IP-Adresse nicht mehr zwingend erforderlich. Daher können Sie auch andere Lösungen als KeepAlived einsetzen! Die eingesetzte Software muss lediglich in der Lage sein, die Gesundheit des Masters zu überwachen und bei einem Ausfall auf dem Slave ein Skript aufzurufen. Dieses Skript aktiviert den Slave zum Master. Dabei versendet der neue Master über das Synchronisationsprotokoll Nachrichten, die den alten Master automatisch zum Slave degradieren. Dieses Skript darf sehr einfach sein:

Listing 26.1: Das Skript script_master.sh befördert einen Slave.

```
#!/bin/sh
/usr/bin/logger -p kernel.crit "Slave zum Master aktiviert."
/bin/echo 2 > /proc/sys/net/ipv4/netfilter/ct_sync/state
```

Bauen Sie zunächst Ihren Firewall-Cluster wie in Abbildung 26.4 auf. Achten Sie darauf, dass Ihre Cluster-Knoten über eine dedizierte Netzwerkkarte miteinander verbunden sind. Aktivieren Sie nun die Netzwerkkarte zur Synchronisation und weisen Sie ihr eindeutige Adressen zum Beispiel in dem Netzwerk 10.0.0.0/24 zu. Sie sollten nun die anderen Knoten in dem Synchronisationsnetzwerk pingen können. Laden Sie nun auf allen Knoten das `ct_sync`-Modul, bevor Sie die weiteren Netzwerkkarten aktivieren:

```
# modprobe ct_sync syncdev=eth2 l2drop=1 notrack=1 cmarkbit=30
```

Nun deklarieren Sie einen Knoten zum Master und die restlichen Knoten jeweils zum Slave. Geben Sie auf dem Master hierzu folgenden Befehl ein:

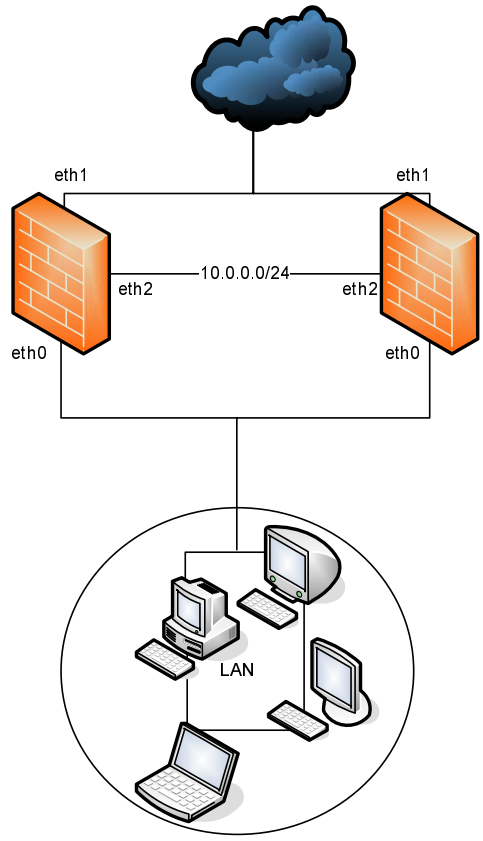


Abbildung 26.4: Der Firewall-Cluster besteht aus zwei Knoten, die sich gegenseitig ersetzen.

```
# echo 2 > /proc/sys/net/ipv4/netfilter/ct_sync/state
```

Auf dem Slave geben Sie den folgenden Befehl ein:

```
# echo 1 > /proc/sys/net/ipv4/netfilter/ct_sync/state
```

Konfigurieren Sie nun die IP-Adressen auf den internen und externen Netzwerkkarten auf allen Knoten identisch. Nun müssen Sie die Firewall-Regeln erzeugen und auf allen Knoten verteilen. Für einen ersten Test mögen die folgenden Regeln genügen:

```
INTDEV=eth0
EXTDEV=eth1
SYNCDEV=eth2

IPTABLES=/usr/sbin/iptables
```

```
SYSCTL=/usr/sbin/sysctl

$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP

$IPTABLES -F
$IPTABLES -F -t nat
$IPTABLES -F -t mangle

$IPTABLES -A INPUT -i $SYNCDEV -j ACCEPT
$IPTABLES -A OUTPUT -o $SYNCDEV -j ACCEPT
$IPTABLES -A INPUT -i lo -j ACCEPT
$IPTABLES -A OUTPUT -o lo -j ACCEPT

$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A FORWARD -i $INTDEV -m state --state NEW -j ACCEPT

$IPTABLES -t mangle -A PREROUTING -p udp --dport 53 -j ACCEPT
$IPTABLES -t mangle -A PREROUTING -p icmp -j ACCEPT

$IPTABLES -t mangle -A PREROUTING -m state --state NEW -j CONNMARK --mark
    0x40000000

$IPTABLES -t nat -A POSTROUTING -o $EXTDEV -j MASQUERADE
```

Die letzte Regel markiert sämtliche Verbindungen mit der Zahl 0x4000000. Bei dieser Zahl ist als Connmark-Bit das Bit 30 gesetzt.

Wenn Sie nun Verbindungen über den Master aufbauen, sollten Sie die Verbindungen auf dem Master in der Verbindungstabelle beobachten können. Diese Verbindungen sollten auch auf dem Slave in der Verbindungstabelle auftauchen. Für Troubleshooting-Zwecke können Sie den Netzwerkverkehr zwischen den Knoten mit Ethereal überwachen. Hierfür ist in dem `ct_sync`-Quelltext auch ein Ethereal-Plugin vorhanden, das Sie in den Ethereal-Quelltext patchen können. Dieses Plugin kann das Protokoll analysieren und verständlich anzeigen (Abbildung 26.5).

Tipp

Benutzen Sie Verbindungen, die über eine lange Zeit offen bleiben. Telnet- und SSH-Verbindungen haben sich hier für den Test bewährt. Eine HTTP-Verbindung wird nach dem Datentransport meist direkt wieder von dem Server geschlossen.

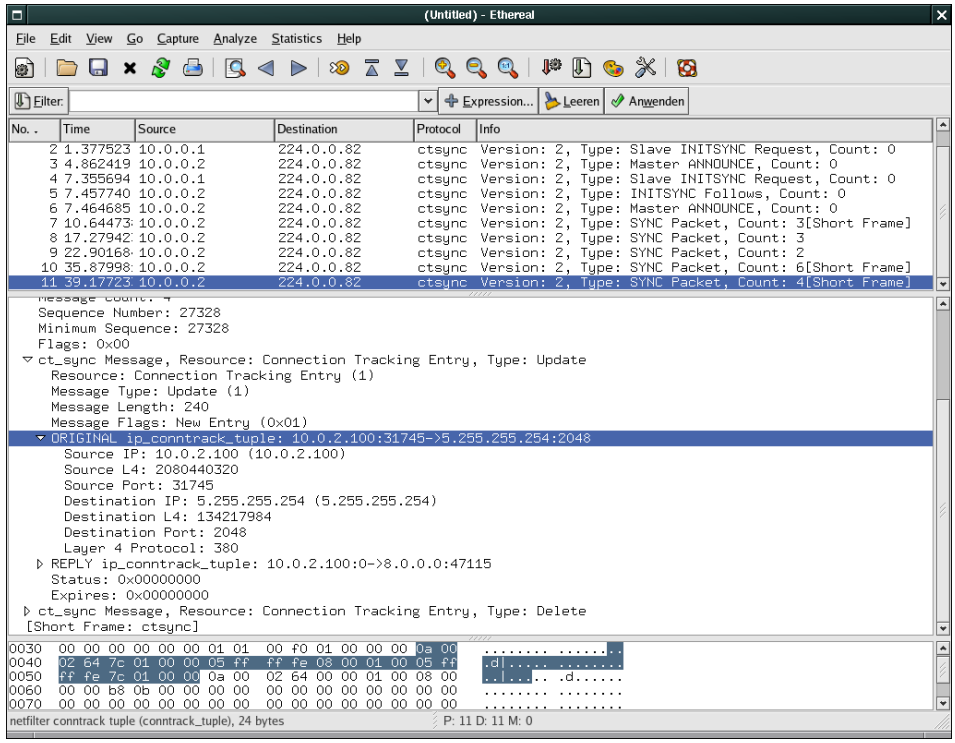


Abbildung 26.5: Ethereal kann mit einem Patch das ct_sync-Multisync-Protokoll parsen.

Zur weiteren Fehleranalyse befindet sich in dem `ct_sync`-Quelltext auch ein Werkzeug `cts_dump`, mit dem Sie ebenfalls die Nachrichten des Synchronisationsprotokolls anzeigen können.

Wenn Sie die Synchronisation einige Zeit betrachtet haben und sich von der Funktion überzeugt haben, können Sie manuell auf dem Slave das Skript aufrufen, das den Slave zum Master befördert. Der alte Master sollte den Layer2Drop aktivieren, und der Slave sollte sichtbar werden.

Wahrscheinlich werden die vorher von Ihnen aufgebauten Netzwerkverbindungen für eine gewisse Zeit »hängen«. Dies hängt mit der MAC-Adresse des neuen Masters zusammen. Der neue Master besitzt zwar die richtige IP-Adresse, aber die »falsche« MAC-Adresse. Erst nach Ablauf des ARP-Caches der Clients werden diese einen neuen ARP-Request aussenden, der von dem neuen Master beantwortet werden wird. Sie können das beschleunigen, indem Sie auf dem neuen Master den Befehl `arping -A <eigene IP-Adresse>` aufrufen. Dies ist ein *gratious ARP*, der die ARP-Caches der benachbarten Rechner aktualisiert.

Tipp

Wenn Sie den KeepAlived-Daemon einsetzen, versendet er selbstständig den gratious ARP.

Wenn der Fail-Over zu Ihrer Zufriedenheit manuell funktioniert, können Sie eine Software installieren, mit der Sie die Gesundheit des Firewall-Clusters überwachen und bei einem erforderlichen Fail-Over das Skript für die Beförderung des Slaves zum Master aufrufen. Wenn Sie das mit KeepAlived erledigen möchten, achten Sie darauf, dass beim Einsatz des Layer-2-Drops der KeepAlived seine Nachrichten über das Synchronisationsnetzwerk versenden muss. In dem oben gewählten Szenario ist dies die Netzwerkkarte `eth2`. Um dies zu erreichen, müssen Sie in beiden Instanzen die folgende Zeile einfügen:

```
lvs_sync_daemon_interface eth2
```

Damit der KeepAlived-Daemon auch den Slave zum Master befördert, tragen Sie das Skript ebenfalls in der Konfiguration ein. Die komplette Konfiguration sieht dann für den initialen Master so aus:

```
vrrp_sync_group VG1 {
  group {
    eth0
    eth1
  }
  notify_master /etc/keepalived/script_master.sh
  notify_backup /etc/keepalived/script_slave.sh
}
! Interne virtuelle IP-Adresse
vrrp_instance VI_1 {
 state MASTER
 interface eth0
 lvs_sync_daemon_interface eth2
 virtual_router_id 1
 priority 100
 authentication {
  auth_type AH
  auth_pass password
 }
 virtual_ipaddress {
  192.168.1.1/24 brd 192.168.1.255 dev eth0
 }
```

```
}
! Externe virtuelle IP-Adresse
vrrp_instance VE_1 {
 state MASTER
 interface eth1
 lvs_sync_daemon_interface eth2
 virtual_router_id 2
 priority 100
 authentication {
  auth_type AH
  auth_pass password
 }
 virtual_ipaddress {
  192.168.2.1/24 brd 192.168.1.255 dev eth1
 }
}
```

Das Skript `script_slave.sh` ist für die Funktion nicht zwingend erforderlich, da `ct_sync` es nicht erlaubt, einen aktiven Master über die `/proc`-Schnittstelle zu degradieren. Hier wird es eingesetzt, um eine Protokollierung des Vorgangs durchzuführen:

Listing 26.2: Das Skript script_slave.sh protokolliert die Degradierung.

```
#!/bin/sh
/usr/bin/logger -p kernel.crit "Master zum Slave degradiert."
```

Achten Sie darauf, dass beim Einsatz von KeepAlived nun wieder eine virtuelle IP-Adresse für die Firewall verwendet wird. Die Netzwerkkarten müssen nun mit anderen IP-Adressen oder ohne IP-Adresse konfiguriert und aktiviert werden! Die Netzwerkkarte für das Synchronisationsnetzwerk benötigt natürlich eine IP-Adresse und muss auch die anderen Knoten erreichen können.

Hinweis

Ich habe bereits einige dieser Firewall-Cluster implementiert, die sich auch jetzt noch im täglichen Einsatz befinden. Außerdem kenne ich Firewall-Cluster, die mehrere 100 Mbit/s Verkehr abwickeln. Wenn Sie auf die Conntrack- und NAT-Helfermodule, die von der Synchronisation noch nicht unterstützt werden, verzichten können, steht Ihnen mit `ct_sync` ein mächtiger Firewall-Cluster zur Verfügung.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

27 Nfnetlink und Kernel 2.6.14

Mit dem Kernel 2.6.14 wurde eine neue Architektur in dem Kernel eingeführt: `nfnetlink`. Obwohl der Anwender davon zunächst nicht viel mitbekommen wird, hat sich unter der Haube damit sehr viel getan. Die gesamte Kommunikation zwischen dem Userspace und dem Kernelspace wurde standardisiert und wird von der `nfnetlink`-Schicht übernommen. Dies wurde nötig, da die aktuellen Lösungen drei Probleme aufwiesen:

1. Code-Replikation: `iptables`, `ip6tables`, `arptables` und `ebtables` enthalten große Teile identischen Codes, der so nur schwer wartbar ist. Einzelne Code-Teile sind sehr eng mit dem IPv4-Protokoll verkuppelt, wie zum Beispiel das Connection Tracking.

2. Dynamische Regeln: Die aktuelle Struktur unterstützt nur umständlich dynamische Regelsätze, wie sie von einem Intrusion-Prevention-System benötigt werden würden.

3. API für eine GUI: Es existiert keine einheitliche Schnittstelle, über die eine grafische Oberfläche die Funktionen auslesen und Regeln setzen kann.

Um diese Probleme zu lösen, wurde die `nfnetlink`-Struktur geschaffen, und mit `nfnetlink_log`, `nfnetlink_conntrack` und `nfnetlink_queue` wurden IPv4-unabhängige Strukturen geschaffen, die nun auch von anderen Protokollen wie IPv6 genutzt werden können. Dies ist der erste Schritt auf dem Weg zu `pkttables`. Pkttables ist ein Langzeitziel des Netfilter-Teams. Mit Pkttables soll eine einheitlicher Oberfläche für alle Firewall-Regeln unabhängig vom Layer-3-Protokoll geschaffen werden.

27.1 Der conntrack-Befehl

Die wesentliche Neuerung für den Endanwender beim Einsatz der `nfnetlink`-Architektur ist der Befehl `conntrack`, der nun zur Verfügung steht. Mit diesem Befehl können Sie den Inhalt der Verbindungstabelle anzeigen, nach einzelnen Einträgen suchen, neue Einträge hinzufügen und Einträge löschen. Genauso können Sie auch die Tabelle der erwarteten Verbindungen (Expectations) anzeigen und auch hier neue Verbindungen hinzufügen oder löschen.

Achtung

Der Befehl `conntrack` ist noch sehr jung und im Moment (Oktober 2005) noch stark in der Entwicklung. Verwenden Sie immer die neuesten Versionen der Bibliotheken und des Befehls von dem Subversion-Server, wenn Sie diesen Befehl testen möchten. Aktuell ist zum Beispiel das Löschen von Einträgen nicht möglich.

Der Befehl `conntrack` kann von der Iptables-Homepage heruntergeladen werden (*http://www.Iptables.org/projects/conntrack/downloads.html*). Anschließend müssen Sie das Paket nur auspacken und übersetzen. Achten Sie darauf, dass Sie mindestens einen Linux-Kernel 2.6.14 verwenden und vorher die `libnfnetlink`-Bibliotheken installieren.

Der Befehl kann dann sowohl die normale Verbindungstabelle als auch die Expectations-Tabelle betrachten. Sie können die folgenden Befehle ausführen:

- `-L, --dump`: Anzeige der Tabelle.
- `-G, --get`: Sucht nach einem Eintrag in der Tabelle.
- `-D, --delete`: Löscht einen Eintrag aus der Tabelle.
- `-I, --insert`: Fügt einen Eintrag in die Tabelle ein.
- `-E, --event`: Zeigt ein Echtzeit-Protokoll an.
- `-F, --flush`: Löscht die gesamte Tabelle.

Viele der Befehle benötigen zusätzliche Optionen, um die Verbindung zu spezifizieren. Hierfür haben Sie die folgenden Möglichkeiten:

- `-z, --zero`: In Kombination mit dem Kommando `-L` löscht diese Option die Zähler nach der Anzeige.
- `-e, --event-mask <mask>`. Diese Option ist nur gültig in Kombination mit dem Kommando `-E`. Hiermit können Sie die Ereignisse einstellen, die in dem Echtzeitprotokoll angezeigt werden sollen. Die folgenden Events können Sie verwenden: `ALL|NEW|RELATED|DESTROY|REFRESH|STATUS|PROTOINFO|HELPER|HELPINFO|NATINFO`.
- `-g, --group-mask <mask>`. Auch diese Option ist nur gültig mit dem Kommando `-E`. Sie erlaubt Ihnen die Auswahl des Protokolls (`ALL|TCP|UDP|ICMP`).
- `-s, --orig-src <ip>`: Mit dieser Option geben Sie Quell-IP-Adresse der Verbindung an.
- `-d, --orig-dst <ip>`: Mit dieser Option geben Sie die Ziel-IP-Adresse der Verbindung an.
- `-r, --reply-src <ip>`: Mit dieser Option geben Sie bei einer genatteten Verbindung die DNAT-IP-Adresse an. Ist die Verbindung nicht genattet, ist sie identisch mit der `orig-dst`-Adresse.

- `-q, --reply-dst <ip>`: Mit dieser Option geben Sie bei einer genatteten Verbindung die SNAT-IP-Adresse an. Ist die Verbindung nicht genattet, ist sie mit der `orig-src` Adresse identisch.
- `-p, --proto <protokoll>`: Hiermit wählen Sie das Protokoll (TCP, UDP ...).
- `-t, --timeout <sekunden>`: Hiermit geben Sie den Timeout der Verbindung an.
- `-u, --status <status>`: Hiermit wählen Sie den Status der Verbindung (`[EXPECTED|ASSURED|SEEN_REPLY|CONFIRMED|SNAT|DNAT|SEQ_ADJUST|UNSET]`).
- `-i, --id <id>`: Jede Verbindung hat eine Conntrack-ID, über die Sie auf die Verbindung zugreifen können. Die aktuelle Version zeigt jedoch die ID leider nicht an.
- `--tuple-src <ip>`: Hiermit geben Sie bei einer Expectation das Quell-Tuple an.
- `--tuple-dst <ip>`: Hiermit geben Sie bei einer Expectation das Ziel-Tuple an.
- `--mask-src <ip>`: Hiermit können Sie bei einer Expectation die Quell-Maske angeben.
- `--mask-dst <ip>`: Hiermit können Sie bei einer Expectation die Ziel-Maske angeben.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

28 nf-HiPAC

Sobald Sie mehrere tausend Regeln in einer Kette in Ihrer Firewall verwenden müssen, werden Sie feststellen, dass die Geschwindigkeit der Paketverarbeitung stark sinkt. Dann sollten Sie sich nf-HiPAC (*http://www.hipac.org*) genauer ansehen. Dabei handelt es sich um einen Patch, der mit dem HiPAC-Paketklassifizierungsalgorithmus bei mehr als 1000 Regeln immer noch schneller arbeitet als Iptables mit 100 Regeln. nf-HiPAC unterstützt aktuell fast alle Iptables-Funktionen. Nur NAT wird (noch) nicht unterstützt.

28.1 Was ist nf-HiPAC?

nf-HiPAC ist ein kompletter Paketfilter für Linux, der mit HiPAC einen neuen Algorithmus für die Klassifizierung von Paketen verwendet. Dieser Algorithmus reduziert die Speicherzugriffe je Paket enorm und erreicht so hohe Verarbeitungsgeschwindigkeiten auch bei großen Regelsätzen und Netzen mit großer Auslastung.

nf-HiPAC stellt die gleichen Funktionen wie Iptables zur Verfügung. Die Konfiguration des Paketfilters erfolgt mit dem Werkzeug `nf-hipac`, das in weiten Teilen kompatibel zum Iptables-Befehl ist. Dadurch können viele Skripten durch einen einfachen Austausch des Befehls auf nf-HiPAC umgestellt werden.

Achtung

nf-HiPAC ist ein reiner Paketfilter. NAT oder Mangling werden nicht unterstützt.

Im Gegensatz zu Iptables ist die Geschwindigkeit von nf-HiPAC in fast allen Umgebungen unabhängig von der Größe des Regelsatzes besser. Dieser Unterschied fällt besonders bei großen Regelsätzen auf. Während die Geschwindigkeit von Iptables linear mit der Zahl der Regeln abnimmt, bleibt die von nf-HiPAC nahezu konstant.

Ein Regel-Update führt bei nf-HiPAC nicht zu Verzögerungen in der Bearbeitung. Dynamische Regelsätze können sehr schnell umgesetzt werden. Einzelne Regeln

können entfernt oder ausgetauscht werden, ohne dass es wie bei Iptables zu Verzögerungen kommt.

Da es sich bei nf-HiPAC noch um ein Werkzeug handelt, das sich im Moment in starker Weiterentwickung befindet und sicherlich nur für einen ganz kleinen Bereich der Leser interessant ist, verweise ich für weitere Informationen auf die Homepage *http://www.hipac.org*.

Hinweis

Eine letzte Bemerkung noch zu nf-HiPAC: Es gibt im Netfilter-Team Überlegungen, nf-HiPAC in das Iptables-Projekt aufzunehmen. Dann ist ein Patchen überflüssig.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

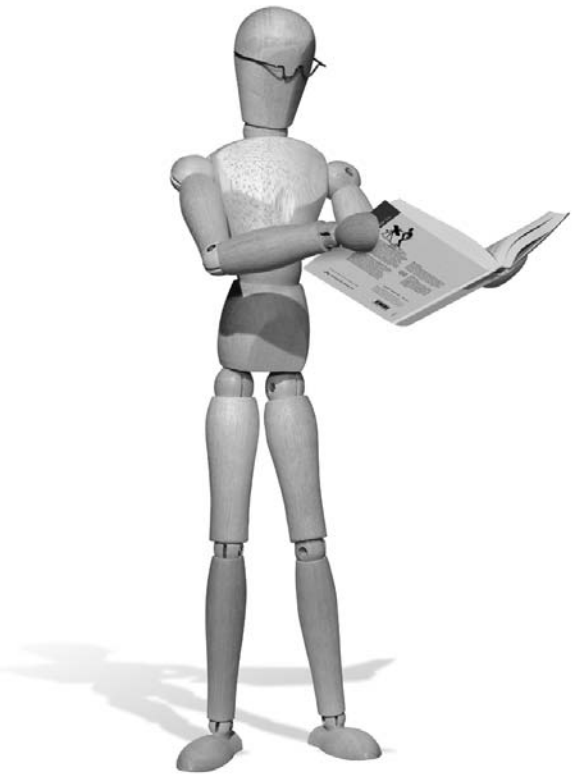
ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Teil VI

Transparente Firewalls



29 ProxyARP

Die Verwendung von ProxyARP ist eine der einfachsten Varianten für die transparente Filterung von Paketen in einem Netzwerk. Hierbei wird ein Router in ein vorhandenes Netzwerk eingebracht, ohne dass das Netzwerk neu konfiguriert wird. Auf beiden Seiten des Routers befinden sich Systeme aus demselben Netzwerk. Um dennoch eine Kommunikation zwischen den Systemen zu ermöglichen und ARP-Auflösungen durchzuführen, unterstützt der Router ProxyARP. Eine Filterung ist dann ganz normal mit Iptables möglich.

29.1 Wie funktioniert ProxyARP?

Bei dem ProxyARP antwortet ein Rechner auf eine ARP-Anfrage an Stelle (als Proxy) eines anderen Rechners. Eigentlich sehr einfach, aber wann braucht man das und wofür?

Eine häufige Anwendung ist die Einwahl eines Rechners in ein Netzwerk. In der Abbildung 29.1 sehen Sie ein typisches Beispiel.

Der Client wählt sich per Modem in ein Netzwerk ein und verwendet das PPP-Protokoll für die Anmeldung. Über das PPP-Protokoll erhält er eine IP-Adresse, ein Default-Gateway, einen DNS-Server und einen WINS-Server mitgeteilt. In vielen Fällen handelt es sich wie hier bei der IP-Adresse um eine IP-Adresse aus dem

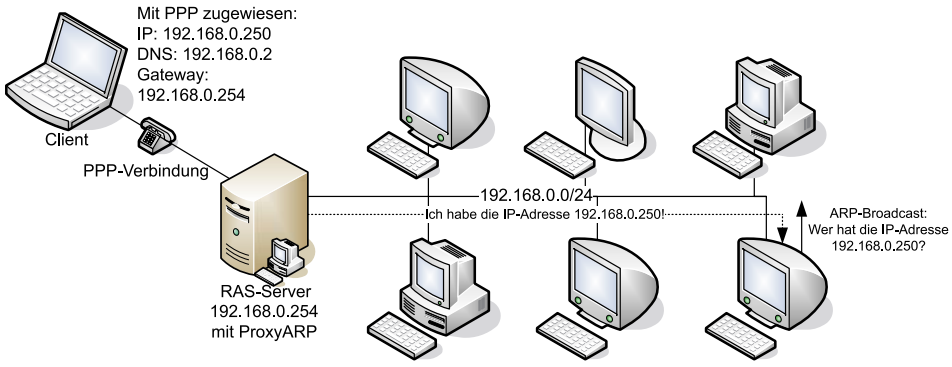


Abbildung 29.1: Bei der Einwahl erhält der Client eine IP-Adresse aus dem internen Netzwerk.

internen Netzwerk. Wenn nun der Client ein Paket an einen Rechner in dem internen Netz schicken möchte, ist dies zunächst kein Problem, da er das Paket nur an den Remote-Access-Service-(RAS-)Server schicken kann. Wenn jedoch der Rechner A aus dem internen Netz ein Paket an den Client schicken möchte, entsteht ein Problem. Der Rechner A in dem internen Netz prüft über seine Netzmaske und die IP-Adresse des Clients, ob sich der Client in seinem eigenen Netz befindet. Da beide Rechner sich in dem Netzwerk 192.168.0.0/24 befinden, sendet er eine ARP-Anfrage für die IP-Adresse 192.168.0.250 aus. ARP-Anfragen werden nur in dem lokalen Netz weitergeleitet. Router wie der RAS-Server arbeiten auf der Schicht (Layer) 3 und leiten diese Pakete der Schicht 2 nicht weiter! Die ARP-Anfrage kann nie den Client erreichen, und der Client kann diese ARP-Anfrage nie beantworten. Der Rechner A erhält keine Antwort auf seine ARP-Anfrage und gibt eine Fehlermeldung aus.

ProxyARP behebt dieses Problem. Hierbei wird auf dem RAS-Server ProxyARP angeschaltet. Dann beantwortet der RAS-Server die ARP-Anfrage für den Client. Der Rechner A sendet das Paket an den RAS-Server, der nach Betrachtung der Ziel-IP-Adresse das Paket weiter an den Client sendet. Die Verbindung kommt zustande.

Mit dieser Methode können Sie an beliebigen Stellen in einem Netzwerk ohne eine Änderung der Konfiguration (IP-Adressen, Netzmaske und Gateway) Router einfügen. Diese Router können anschließend auch die gerouteten Pakete mit Iptables filtern. Im Folgenden erkläre ich zunächst die Konfiguration des ProxyARP und anschließend die Filterung der Pakete.

29.2 ProxyARP-Konfiguration

Die Konfiguration des ProxyARP beschränkt sich auf die aktuellen Kernel 2.4 und 2.6. In den älteren Kerneln wurde die ProxyARP-Funktionalität unterschiedlich gehandhabt (*http://www.tldp.org/HOWTO/Proxy-ARP-Subnet/*). Teilweise wird die ProxyARP-Funktionalität auch je nach Hardware unterschiedlich gehandhabt. So verwendet Linux auf der Z-Series von IBM ganz andere Dateien zur Steuerung der ProxyARP-Funktion (*http://www-1.ibm.com/servers/eserver/zseries/library/techpapers/pdf/lnux-14mg.pdf*).

Die Konfiguration des ProxyARP unter Linux ist sehr einfach. Beginnen Sie damit, die Netzwerkkarten in Ihrem Router zu konfigurieren. Hierbei ist es durchaus möglich, dass beide Netzwerkkarten identische IP-Adressen erhalten. Sie können aber auch die Netzwerkkarten mit unterschiedlichen IP-Adressen ausstatten:

```
# ip addr ip add 192.168.0.2 dev eth0
# ip addr ip add 192.168.0.2 dev eth1
# ip link set eth0 up
# ip link set eth1 up
```

Nun müssen Sie in der Routing-Tabelle die entsprechenden Routen eintragen. Wenn sich auf der einen Seite des ProxyARP-Routers nur ein Rechner befindet und auf der

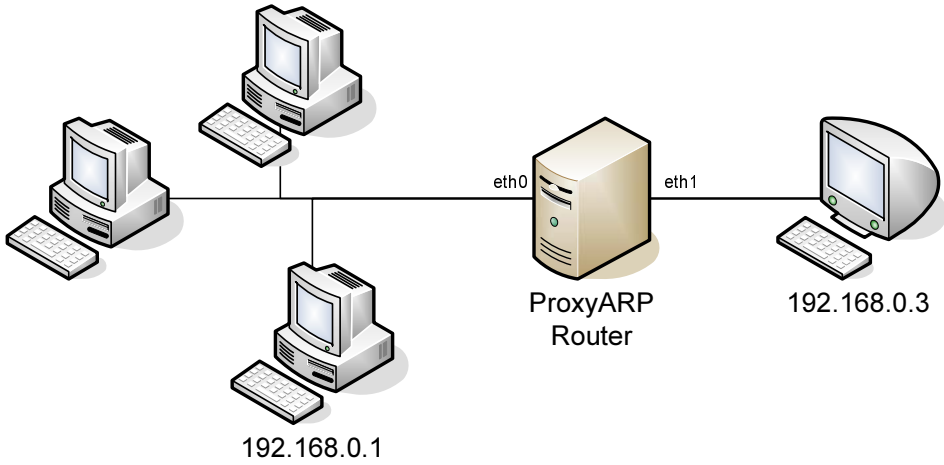


Abbildung 29.2: Ein einfaches Beispiel, in dem sich links und rechts von einem ProxyARP-Router zwei Rechner 192.168.0.1 und 192.168.0.3 befinden.

anderen Seite der Rest des Netzwerks (siehe Abbildung 29.2), dann können Sie die Routen folgendermaßen setzen:

```
# ip route add 192.168.0.3/32 dev eth1
# ip route add 192.168.0.0/24 dev eth0
```

Nun müssen Sie lediglich für jede Netzwerkkarte, die ProxyARP unterstützen soll, dies zunächst anschalten. Dies erfolgt in dem `/proc`-Verzeichnis. Dort existiert für jede Netzwerkkarte ein Eintrag `/proc/sys/net/ipv4/conf/ethX/proxy_arp`. Tragen Sie hier eine Eins ein, um die Funktion anzuschalten:

```
# echo "1" > /proc/sys/net/ipv4/conf/eth0/proxy_arp
# echo "1" > /proc/sys/net/ipv4/conf/eth1/proxy_arp
```

Tipp

Wenn Sie eine Option für alle Netzwerkkarten aktivieren möchten, genügt es auch, die Option in `/proc/sys/net/ipv4/conf/all` anzuschalten.

Anschließend müssen Sie noch die IP-Weiterleitung aktivieren und eine Kommunikation sollte nun zwischen 192.168.0.1 und 192.168.0.3 möglich sein.

```
# echo "1" > /proc/sys/net/ipv4/ip_forward
```

ProxyARP ist eine sehr einfache Möglichkeit, um in einem Netzwerk nachträglich ohne Änderung der Konfiguration einen Router einzuführen. Ganz transparent ist jedoch dieser Router nicht. Er wird, wie jeder andere Router, den TTL-Wert der weitergeleiteten Pakete um eins heruntersetzen. Ansonsten ist aber auf der Schicht 3 (IP) keine weitere Modifikation der Pakete erkennbar.

29.3 Filterung mit Iptables

Die Filterung mit Iptables ist beim Einsatz von ProxyARP sehr einfach. Da es sich beim ProxyARP-System um einen Router handelt, können Sie ganz normal die Pakete filtern. Die Pakete durchlaufen, wie auf einem normalen Router, die Ketten PREROUTING (Tabellen Mangle und NAT), FORWARD (Tabellen Mangle und Filter) und POSTROUTING (Tabellen Mangle und NAT). Sie müssen nur aufpassen, wenn Sie in Ihren Regeln IP-Adressen angeben, dass Sie darauf achten, dass auf beiden Seiten der Firewall IP-Adressen aus demselben Netzwerk vorhanden sind.

Handelt es sich beim Rechner 192.168.0.3 aus Abbildung 29.2 um einen MySQL-Datenbankserver, den Sie zusätzlich mit einer Firewall vor dem lokalen Netz 192.168.0.0/24 schützen möchten, dann könnten Sie die folgenden Regeln verwenden:

```
MYSQL_SRV=192.168.0.3
DIENSTE="mysql,ssh"
LANDEV=eth0 # An dieser Schnittstelle ist das restliche LAN angeschlossen
MYSQLDEV=eth1 # Hier ist der MySQL-Server angeschlossen

$IPTABLES -P FORWARD DROP

$IPTABLES -A FORWARD -i $LANDEV -o $MYSQLDEV -d $MYSQL_SRV
   -p tcp -m multiport --dport $DIENSTE -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

29.4 Fazit

So können Sie mit einfachen Mitteln auch den Verkehr in einem Netz ohne Änderungen der Adressen, Netzmasken und Default-Gateways filtern.

Um jedoch tatsächlich die Firewall ohne IP-Adressen zu betreiben, benötigen Sie den Bridge-Modus. Der nächste Abschnitt erläutert diesen und die Anwendung von Iptables.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

30 Iptables auf einer Bridge

Eine Bridge ist eine Software, die ähnliche Funktionen übernimmt wie ein Switch, der in Hardware implementiert wurde. Die Bridge verfügt häufig über zusätzliche Möglichkeiten, wie zum Beispiel die Änderung des Mediums. So gibt es Bridges, die Token-Ring- und Ethernet-Netze miteinander verbinden können. Linux kann derartige Bridges betreiben und auch mit Iptables die von der Bridge weitergeleiteten Pakete filtern.

30.1 Wie funktioniert die Bridge?

Wie funktioniert nun eine Bridge? Zunächst definieren Sie die Netzwerkkarten, die Teil der Bridge werden sollen. Nach Aktivierung der Bridge lernt die Bridge ähnlich wie ein Switch die MAC-Adressen der Rechner, die an der Bridge angeschlossen sind. Dazu betrachtet die Bridge bei jedem Paket die Absender-MAC-Adresse und speichert diese in einer Tabelle ab (siehe Abbildung 30.1).

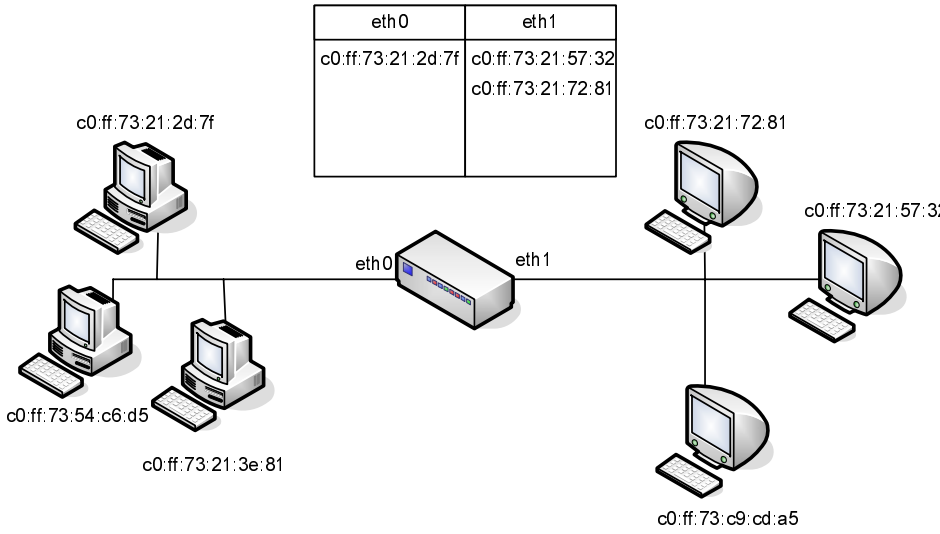


Abbildung 30.1: Eine Bridge lernt selbstständig die MAC-Adressen der angeschlossenen Geräte.

Solange die Bridge die Ziel-MAC-Adresse eines Pakets noch nicht kennt, kopiert die Bridge dieses Paket in alle angeschlossenen Netze, so dass auf jeden Fall eine Kommunikation möglich ist. Sobald aber die Bridge die Ziel-MAC-Adresse bereits kennt, ermittelt sie mit ihrer Tabelle die Netzwerkkarte, an der der entsprechende Rechner angeschlossen ist, und leitet das Paket auf dieser Netzwerkkarte weiter. So unterdrückt die Bridge Broadcasts und vermeidet Kollisionen in dem Netzwerk durch gleichzeitig gesendete Pakete. Damit erhöht die Bridge die Leistung des Ethernet-Netzwerks, das bei einer Kollision die Pakete erneut senden muss.

30.2 Bau einer Bridge mit Linux

Um mit einem Linux-System eine Bridge zu bauen, benötigen Sie lediglich einen Kernel 2.4 oder 2.6. Für die älteren Kernel benötigen Sie zusätzlich den Bridge-Patch von *http://bridge.sourceforge.net*. Für die Konfiguration der Bridge müssen Sie die Bridge-Utilities installieren. Diese sind in den meisten Distributionen enthalten. Das Paket heißt üblicherweise `bridge-utils`. Die aktuelle Version ist die Version 1.0.6 und kann ebenfalls von der oben angegebenen URL heruntergeladen werden. Sie benötigen die aktuellen Versionen nur für die neuesten Kernel. Meist genügen auch die älteren Versionen der Distributionen.

Der wesentliche Befehl der Bridge-Utilities ist `brctl`. Hiermit steuern Sie die gesamte Bridge:

```
[root@bibo ~]# brctl
commands:
        addbr           <bridge>                add bridge
        delbr           <bridge>                delete bridge
        addif           <bridge> <device>       add interface to bridge
        delif           <bridge> <device>       delete interface from bridge
        setageing       <bridge> <time>         set ageing time
        setbridgeprio   <bridge> <prio>         set bridge priority
        setfd           <bridge> <time>         set bridge forward delay
        sethello        <bridge> <time>         set hello time
        setmaxage       <bridge> <time>         set max message age
        setpathcost     <bridge> <port> <cost>  set path cost
        setportprio     <bridge> <port> <prio>  set port priority
        show                                    show a list of bridges
        showmacs        <bridge>                show a list of mac addrs
        showstp         <bridge>                show bridge stp info
        stp             <bridge> <state>        turn stp on/off
```

Um nun eine Bridge zu erzeugen, verwenden Sie den Befehl `brctl addbr br0`. Das Gerät `br0` ist anschließend sofort verfügbar:

```
[root@bibo ~]# ip link show br0
4: br0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
```

Nun können Sie der Bridge Netzwerkkarten hinzufügen. Hierzu verwenden Sie den Befehl `brctl addif`. Dabei ist es wichtig, dass diese Netzwerkkarten keine IP-Adressen tragen. Dann können Sie mit dem `ip`-Befehl die Netzwerkkarten aktivieren.

```
[root@bibo ~]# brctl addif br0 eth0
[root@bibo ~]# brctl addif br0 eth1
[root@bibo ~]# ip link set eth0 up
[root@bibo ~]# ip link set eth1 up
[root@bibo ~]# ip link set br0 up
[root@bibo ~]# ip link show
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,PROMISC,UP> mtu 1500 qdisc pfifo_fast
qlen 100
    link/ether 00:20:e0:6c:72:1e brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,PROMISC,UP> mtu 1500 qdisc pfifo_fast
qlen 100
    link/ether 00:10:a4:c3:26:cb brd ff:ff:ff:ff:ff:ff
4: br0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue
    link/ether 00:10:a4:c3:26:cb brd ff:ff:ff:ff:ff:ff
```

Wenn bei Ihnen der `ip link show`-Befehl nicht das `PROMISC`-Flag bei den Netzwerkkarten anzeigt, arbeiten Sie wahrscheinlich auf einem Linux-Kernel 2.6. Hier wird dieses Flag nicht mehr angezeigt.

Mit dem Befehl `brctl` können Sie sich die Einzelheiten der Bridge anzeigen lassen:

```
[root@bibo ~]# brctl show
bridge name     bridge id               STP enabled     interfaces
br0             8000.0010a4c326cb       yes             eth0
                                                        eth1
```

Wenn Sie die Bridge für Firewall-Zwecke einsetzen möchten, sollten Sie das Spanning-Tree-Protokoll (STP) abschalten. Dies ermöglicht den Aufbau von redundanten Bridges. Da das Protokoll aber keine Sicherheit bietet, sollte es im Zusammenhang mit Firewalls nicht genutzt werden: `brctl stp br0 off`. Dann können Sie auch die Forward-Delay Zeit auf null setzen. Bei dem Einsatz des Spanning-Tree-Protokolls werden hiermit Schleifen zum Startzeitpunkt der Bridge ausgeschlossen:

`brctl fd br0 0`.

Nun sollte bereits eine Kommunikation über die Bridge möglich sein. Dazu können Sie bereits durch die Bridge pingen. Anschließend können Sie sich die MAC-Adressen, die von der Bridge bereits gelernt wurden, anzeigen lassen:

```
[root@bibo ~# brctl showmacs br0
port no mac addr                is local?       ageing timer
  1     00:20:e0:6c:72:1e       yes                0.00
  2     00:20:e0:6c:72:10       yes                0.00
```

```
1     00:20:e0:73:71:20       yes             0.00
2     00:20:e0:73:71:21       yes             0.00
```

30.3 Filtern auf der Bridge mit iptables

Nun können Sie wie üblich auf der Bridge filtern. Die Pakete durchlaufen nacheinander die Mangle-PREROUTING-, die NAT-PREROUTING-, die Mangle-FORWARD-, die Filter-FORWARD-, die Mangle-POSTROUTING- und die NAT-POSTROUTING-Kette.

Achtung

Ich habe bei mir auf einigen Kerneln feststellen müssen, dass die Pakete die Mangle-PREROUTING-Kette teilweise dreimal durchlaufen. Dies scheint ein Artefakt zu sein.

Wenn Sie nun die Pakete filtern möchten, können Sie das ganz normal in der FORWARD-Kette tun. Allerdings sollten Sie darauf achten, dass die Bridge, während sie die MAC-Adressen lernt, auch noch Pakete weiterleitet, die nicht weitergeleitet werden müssen. Das bedeutet, dass Sie mit REJECT-Regeln sehr vorsichtig sein sollten. In der Abbildung 30.2 ist ein Szenario gezeigt, in dem eine REJECT-Regel zum Abbruch gültiger Verbindungen führt. Hier baut der Rechner A zum Rechner B in demselben Netzwerk eine Verbindung auf. Die Bridge sieht ebenfalls das Paket und muss es weiterleiten, da sie die Ziel-MAC-Adresse noch nicht kennt. Es durchläuft die FORWARD-Kette und wird abgelehnt. Da die Ablehnung durch eine REJECT-Regel erfolgt, sendet die Bridge einen Fehler an Rechner A, obwohl die Verbindung sehr wohl aufgebaut werden darf.

Bei der Definition der Regeln ist es häufig sinnvoll zu prüfen, über welche Netzwerkkarte der Bridge das Paket die Bridge erreicht. Hierfür verwenden Sie beim Linux-Kernel 2.4 wie gewohnt die Optionen `-i` bzw. `--in-interface` und `-o` bzw. `--out-interface`. Bei dem Linux-Kernel 2.6 wurden hierfür neue Optionen geschaffen, da insgesamt die Firewall-Möglichkeiten auf der Bridge erweitert wurden (siehe das nächste Kapitel 31). Diese Optionen heißen `--physdev-in` und `--physdev-out`. Um diese Optionen zu nutzen, müssen Sie die Erweiterung `physdev` in Ihren Regeln laden. Ein Beispiel zeigt die Anwendung:

```
$IPTABLES -A FORWARD -m physdev --physdev-in eth0 --physdev-out eth1 -d ↵
192.168.0.1 -j ACCEPT
```

Die weiteren Optionen (`--physdev-is-in`, `--physdev-is-out` und `--physdev-is-bridged`) der `physdev`-Erweiterung werden nur selten benötigt und erklären sich von selbst.

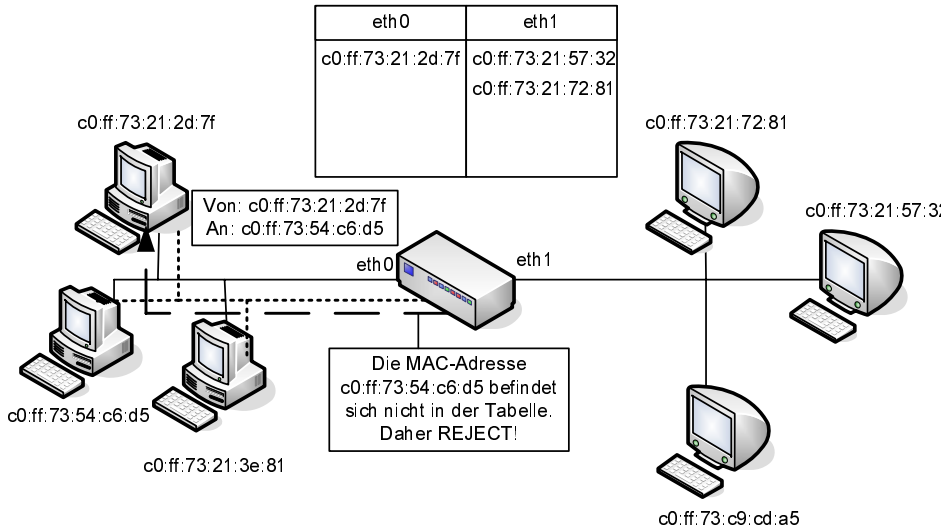


Abbildung 30.2: Ein REJECT kann auf einer Bridge Probleme erzeugen.

Wenn Sie mit einer Bridge ein Netzwerk in zwei Kollisionsdomänen aufgeteilt haben und nun auf der Bridge filtern möchten, ist häufig die `ipset`-Erweiterung des Linux-Kernels hilfreich. Dies ist eine Weiterentwicklung des Befehls `ippool`. Damit ist es sehr leicht möglich, mehrere nicht zusammenhängende IP-Adressen in einer Regel zusammenzufassen. Dies reduziert den Regelaufwand und erlaubt das Erzeugen übersichtlicher Regelwerke. Sie finden die Informationen über diese Erweiterungen in Kapitel 25.

30.4 Filtern auf der Bridge mit arptables

Der Befehl `arptables` ist in den meisten modernen Distributionen enthalten. Er erlaubt die Filterung der Address-Resolution-Protocol-Pakete (ARP), die das IPv4-Protokoll benötigt, um ausgehend von einer IP-Adresse die MAC-Adresse eines Rechners zu ermitteln.

Eine Filterung der ARP-Pakete auf einem Router oder einem einzelnen Rechner ist ungewöhnlich, da dies nur dazu führt, dass ein Rechner scheinbar unsichtbar in dem IPv4-Netzwerk wird.

Wesentlich interessanter ist die Anwendung auf einer Bridge, die im Gegensatz zu einem Router ARP-Pakete weiterleitet. Hier kann durch eine sinnvolle Filterung der ARP-Pakete erreicht werden, dass die von der Firewall-Bridge geschützten Systeme auch auf der Ebene des ARP-Protokolls nur für bestimmte Clients erreichbar sind.

Der `arptables`-Befehl kann auf einem Linux-Kernel 2.4 zwei Ketten (`INPUT` und `OUTPUT`) und auf einem Linux-Kernel 2.6 drei Ketten (zusätzlich `FORWARD`) in der Filter-Tabelle verwalten. Die `FORWARD`-Kette ist auf einem Linux-Kernel 2.4 nur nach Anwendung

des Bridge-nf-Patches verfügbar. Diese Ketten verwalten lediglich die ARP-Pakete. Die INPUT-Filter-Kette betrachtet alle ARP-Pakete, die an den Rechner gerichtet sind. Die OUTPUT-Filter-Kette betrachtet alle lokal erzeugten ARP-Pakete, während die FORWARD-Filter-Kette auf einer Bridge alle von der Bridge durchgeleiteten ARP-Pakete betrachtet.

So ist es möglich, dass nur bestimmte Clients eine ARP-Anfrage für eine bestimmte IP-Adresse senden dürfen. Mit arptables können Sie das mit dem folgenden Befehl erreichen:

```
ARPTABLES=/usr/sbin/arptables
$ARPTABLES -A FORWARD -s 192.168.0.7 -d 192.168.0.25 -j ACCEPT
$ARPTABLES -A FORWARD -d 192.168.0.25 -j DROP
```

30.5 Fazit

Dieser Abschnitt hat Ihnen gezeigt, wie Sie sehr einfach mit iptables auf einer Bridge die Pakete filtern können. So können Sie sehr einfach auf der IP-Ebene transparente Paketfilter aufbauen. Jedoch möchten Sie vielleicht eine noch speziellere Funktion implementieren. Es besteht die Möglichkeit, einige Pakete (zum Beispiel alle IP-Pakete) zu routen und andere Pakete (zum Beispiel NETBEUI-Pakete) über die Bridge zu senden und dort zu filtern. Hierzu benötigen Sie den Befehl ebtables, und die entsprechenden Funktionen müssen in Ihrem Kernel aktiviert worden sein. Das nächste Kapitel erklärt die Funktion.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

31 Ebtables

Der `ebtables`-Befehl ist ein zusätzlicher Befehl zur Filterung von Netzwerkpaketen auf einer Linux-Bridge. Mit diesem Befehl können Sie auch Nicht-IP-Pakete eingeschränkt filtern. Außerdem können Sie entscheiden, ob ein Paket geroutet oder gebridget werden soll. Der Aufbau eines kombinierten Routers mit Bridge-Funktionalität ist für Nicht-IP-Pakete möglich. Derartige Systeme werden als Brouter bezeichnet.

Die Anwendung des Befehls erfordert zusätzliche Patches für die 2.4er Linux-Kernel. Diese Patches sind in den 2.6er Kerneln bereits enthalten und bei den meisten Distributionen auch aktiviert. Viele Distributionen liefern jedoch den Befehl selbst nicht mit. Daher wird zunächst die Installation des Befehls beschrieben.

31.1 Ebtables-Installation

Die letzte Ebtables-Version ist vom 1. November 2003. Falls Ihre Distribution (zum Beispiel Fedora Core 4) bereits Ebtables enthält, handelt es sich wahrscheinlich um diese Version, und ein Update ist nicht erforderlich. Für den Fall, dass Ihre Distribution nicht das Paket enthält und Sie möglicherweise auch noch den Kernel 2.4 einsetzen, schildere ich im Weiteren kurz die Installation des Pakets.

31.1.1 Konfiguration des Linux-Kernels

Während der Linux-Kernel 2.6 bereits den notwendigen Code enthält, müssen Sie den Linux-Kernel 2.4 noch patchen. Unter *http://ebtables.sf.net* finden Sie für den Linux-Kernel 2.4 die notwendigen Patches. Um den Patch anzuwenden, wechseln Sie in das Quelltextverzeichnis Ihres Kernels und rufen den Befehl `zcat patch.gz | patch -p1` auf. Anschließend müssen Sie Ihren Kernel noch konfigurieren. Zusätzlich zu den üblichen Iptables-Optionen wählen Sie die Option *802.1d Ethernet Bridging* an. Dann erscheint unter dieser Option die Option *Bridge: ebtables*. Wählen Sie diese und die anschließend erscheinenden Optionen ebenfalls aus.

Den Linux-Kernel 2.6 müssen Sie nicht mit einem Patch vorbereiten. Hier müssen Sie nur darauf achten, dass die entsprechenden Optionen ausgewählt wurden. Auch hier benötigen Sie die Option *802.1d Ethernet Bridging*, und unter *Bridge: Netfilter configuration* wählen Sie die gewünschten Ebtables-Funktionalitäten.

31.1.2 Installation des Userspace-Werkzeugs

Um den Befehl `ebtables` zu installieren, laden Sie zunächst das Paket `ebtables-2.0.6.tar.gz` von der Homepage und packen es aus. Anschließend übersetzen Sie das Paket mit dem Befehl `make`. Bei dem anschließenden `make install` können Sie mit den Variablen `KERNEL_INCLUDES`, `LIBDIR`, `MANDIR`, `BINDIR`, `ETCDIR`, `ETHERTYPEPATH` und `DESTDIR` die Zielverzeichnisse angeben.

Die Nutzung des CVS-Verzeichnisses, um den aktuellsten Code einzusetzen, ist nicht empfehlenswert, da sich hier seit November 2003 kaum Änderungen ergeben haben.

31.2 Die Ebtables-Tabellen

Ebtables verfügt über insgesamt 3 Tabellen. Die `broute`-Tabelle enthält die `BROUTING`-Kette. Die `filter`-Tabelle enthält die Ketten `FORWARD`, `INPUT` und `OUTPUT`. Die `nat`-Tabelle schließlich enthält die `PREROUTING`-, `OUTPUT`- und `POSTROUTING`-Ketten. Abbildung 31.1 zeigt die Ketten.

Achtung

Die Ebtables-Tabellen haben keinerlei Bezug zu den Iptables-Tabellen und Ketten. Es handelt sich um vollkommen eigenständige Tabellen und Ketten. Die `filter` und die `nat`-`OUTPUT`-Ketten sind ebenfalls eigenständig und werden nacheinander (zuerst `nat`, dann `filter`) durchlaufen.

Mit der `BROUTING`-Kette der `broute`-Tabelle können Sie einen Brouter aufbauen. Ein Brouter nach Definition des Maintainers des Ebtables-Codes ist ein System, das zwei Netze verbindet und einige Pakete routet (zum Beispiel IP-Pakete), während es andere Frames (zum Beispiel NETBEUI-Frames) über die Bridge weiterleitet. Dabei können Sie in der `BROUTING`-Kette entscheiden, ob Sie die Frames/Pakete routen oder bridgen möchten.

Wie bereits weiter oben ausgeführt wurde, erfolgt das Bridging auf der Schicht 2 (Data-Link) des OSI-Modells. Dies ist die Schicht 1 des TCP-Modells. Das Routing erfolgt auf der Schicht 3 des OSI-Modells beziehungsweise auf der Schicht 2 des TCP-Modells. Pakete auf der Data-Link-Schicht des OSI-Modells werden üblicherweise als Rahmen (Frame) bezeichnet, während der Begriff »Paket« für die Netzwerkschicht (Schicht 3) reserviert ist. Ich werde im Folgenden versuchen, diese beiden Begriffe korrekt zu verwenden.

Wie durchlaufen nun die Frames/Pakete die einzelnen Ketten? Um dies nachzuvollziehen, ist es sinnvoll, einige Szenarien durchzuspielen.

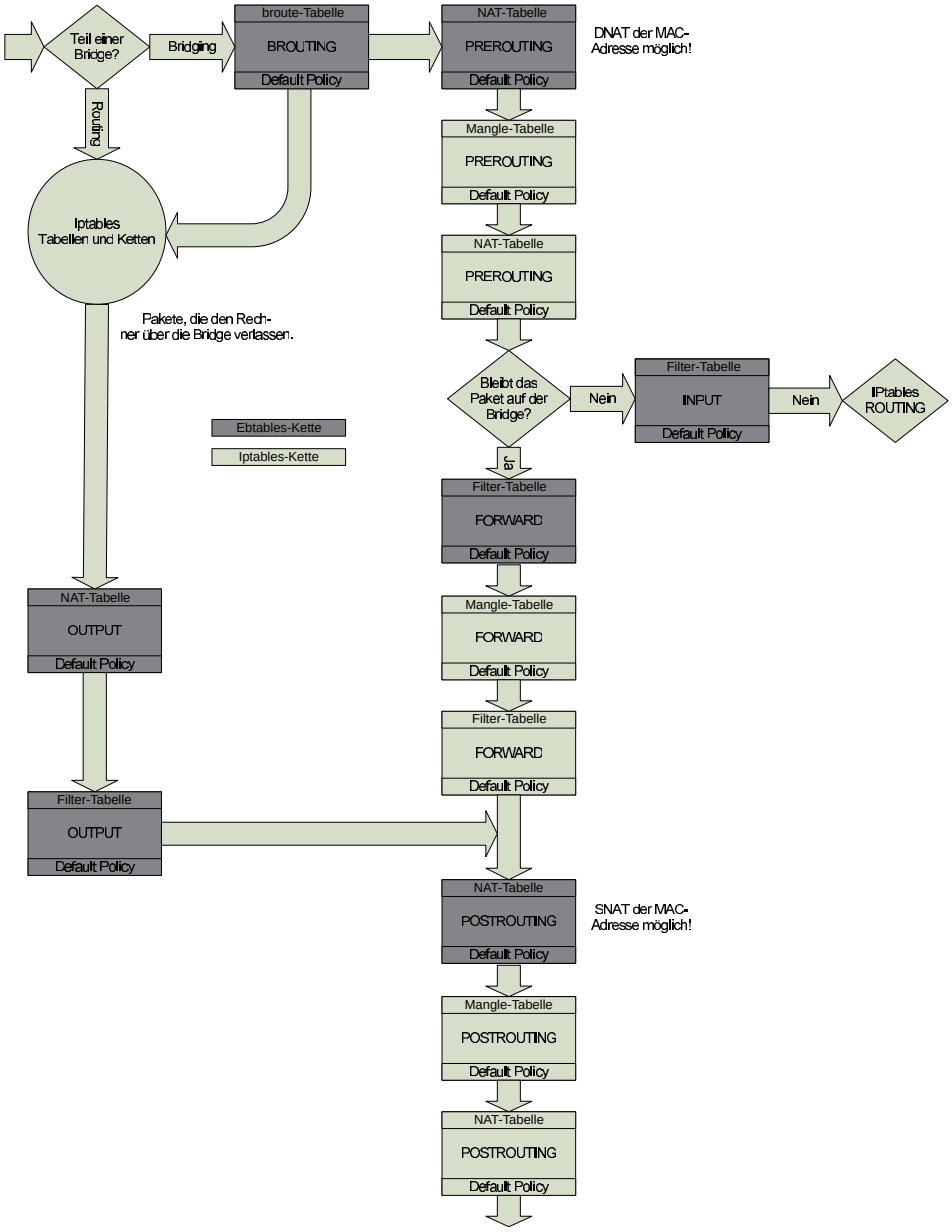


Abbildung 31.1: Ebtables verfügt über drei eigene Tabellen.

31.2.1 Der Rahmen erreicht über ein Bridge-Interface das System

Wenn das Paket über ein Bridge-Interface das System erreicht, wird in der Abbildung 31.2 das Paket an die BROUTING-Kette weitergegeben.

Hier können Sie mit einer Regel entscheiden, ob das Paket geroutet oder der Rahmen gebridgt werden soll. Default ist das Bridging. Bleibt der Rahmen in dem Bridging-Code, so wird er an die PREROUTING-Ketten weitergegeben. Hier werden nacheinander die Ebtables- und die Iptables-PREROUTING-Ketten durchlaufen. Anschließend erfolgt die Prüfung, ob das Paket gebridgt werden muss oder ob sein Ziel das lokale System ist. Ist Letzteres der Fall, so wird der Rahmen an die Ebtables-INPUT-Kette weitergereicht und anschließend weiter an die Netzwerkschicht geschickt. Dort wird dann die Routen-Entscheidung getroffen.

Muss der Rahmen gebridgt werden, so wird er durch die Ebtables- und Iptables-FORWARD-Ketten und die entsprechenden POSTROUTING-Ketten an das entsprechende Interface gesendet.

31.2.2 Der Rahmen erreicht über ein Nicht-Bridge-Interface das System

Falls das Paket über ein Bridge-Interface das System verlassen soll, durchläuft das Paket ganz normal die mangle- und nat-PREROUTING-Ketten. Wird das Paket geroutet, merkt der Kernel, dass das Paket über ein gebridgtes Interface den Rechner verlässt. Das Paket durchläuft die mangle- und filter-FORWARD-Ketten von Iptables und wird dann nach der Bridging-Entscheidung über die Ebtables-nat- und -filter-OUTPUT-Ketten an die Ebtables-POSTROUTING- und die Iptables-POSTROUTING-Ketten gesendet.

31.2.3 Ein lokal erzeugtes Paket verlässt das System über die Bridge

Dies ist der dritte mögliche Fall. Hierbei erzeugt ein lokaler Prozess ein Paket. Dies wird zunächst von den Iptables-OUTPUT-Ketten der mangle-, nat- und filter-Tabellen geprüft. Anschließend wird es über die Ebtables-OUTPUT-Ketten wie im letzten Fall transportiert.

31.3 Die broute-Tabelle

In manchen Umgebungen kann es sinnvoll sein, eine Bridge mit einem Router auf denselben Netzwerkkarten zu kombinieren (siehe Abbildung 31.3).

Dies kann zum Beispiel dann interessant sein, wenn Sie noch einige nicht routingfähige Protokolle in Ihrem Netzwerk einsetzen. Dies können zum Beispiel NETBEUI, Appletalk oder DEC-LAT sein. Während ein normaler IP-Router diese Protokolle nicht weiterleiten würde, kann dies eine Bridge für diese Rahmen.

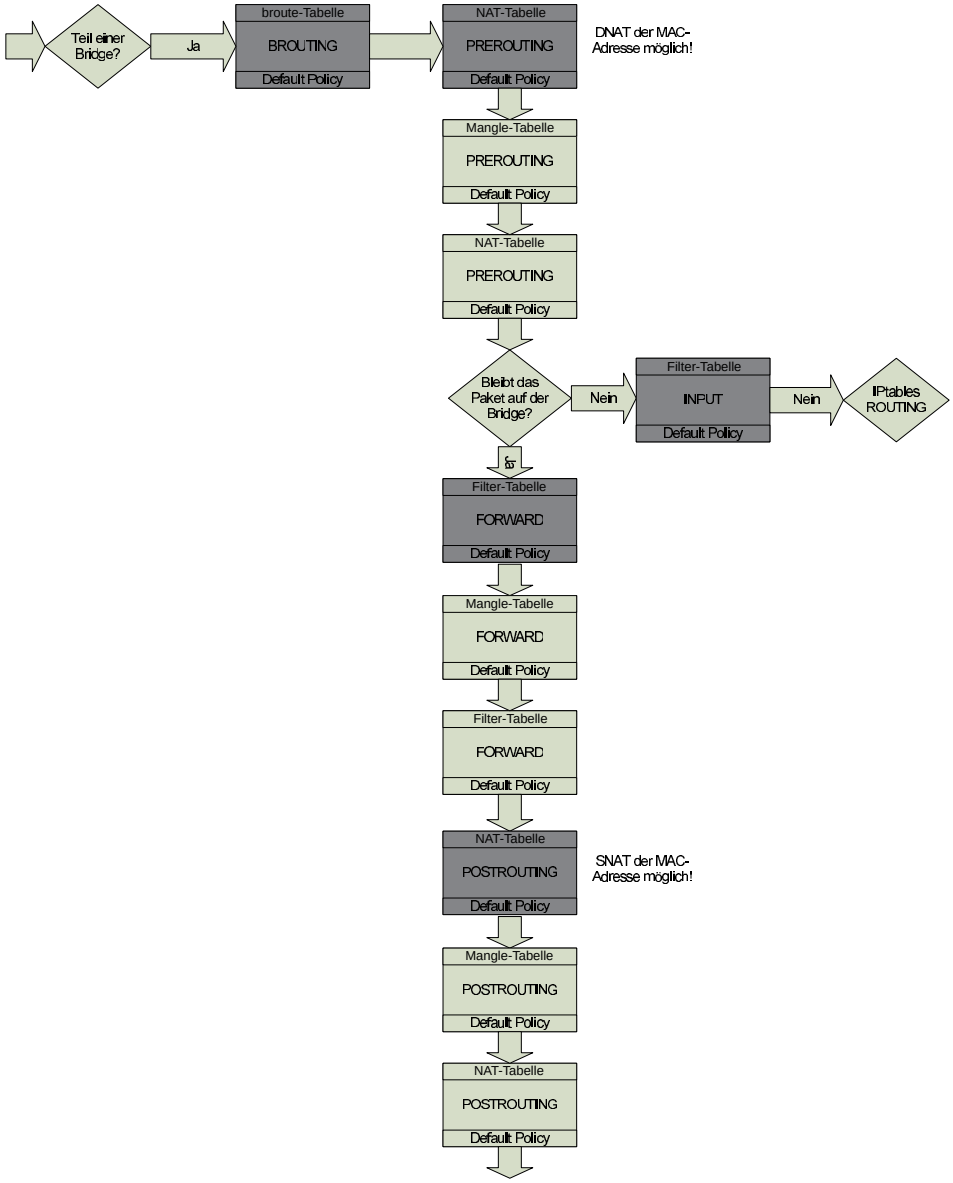


Abbildung 31.2: Die Ebtables- und Iptables-Ketten werden nacheinander durchlaufen.

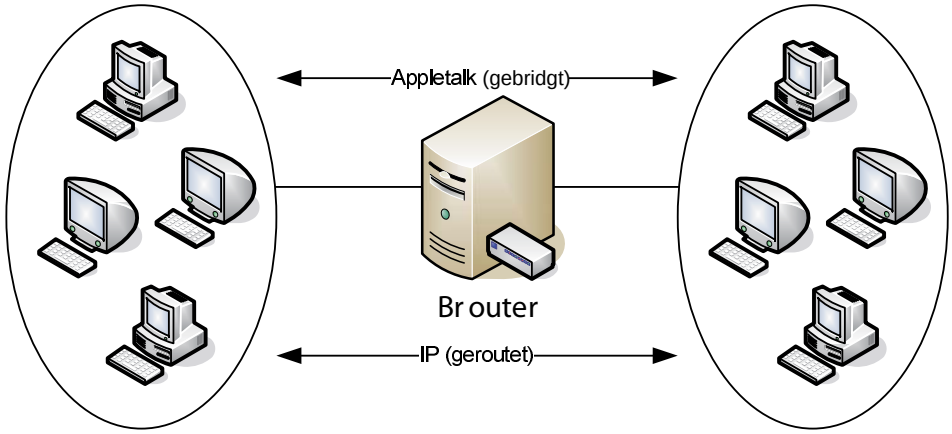


Abbildung 31.3: Ein Brouter routet einige Pakete, während er andere Rahmen bridgt.

In der `BROUTING`-Kette der `broute`-Tabelle können Sie entscheiden, ob ein Rahmen, der normalerweise gebridgt werden würde, doch geroutet werden soll. Hierfür müssen Sie hier eine Regel hinzufügen, die das entsprechende Paket verwirft (`DROP`). Alle Pakete, die in der `BROUTING`-Kette verworfen werden, verlassen die Data-Link-Schicht und werden an den Routing-Prozess und die Netzwerk-Schicht weitergegeben. Um zum Beispiel IP-Pakete zu routen, ARP-Anfragen zu verwerfen und alle weiteren Rahmen über die Bridge weiterzuleiten, können Sie folgendes Skript verwenden:

```
EBTABLES=/sbin/ebtables
BRCTL=/usr/sbin/brctl
IP=/sbin/ip

$EBTABLES -t filter -F
$EBTABLES -t nat -F
$EBTABLES -t broute -F

$BRCTL addbr br0
$BRCTL addif br0 eth0
$BRCTL addif br0 eth1

$IP addr add 172.16.1.1/24 dev eth0
$IP addr add 172.16.2.1/24 dev eth1
$IP link set eth0 up
$IP link set eth1 up
$IP link set br0 up

$EBTABLES -t broute -A BROUTING -p IPv4 -j DROP
$EBTABLES -t broute -A BROUTING -p ARP -j DROP
```

31.4 Die ebtables-Syntax

Der `ebtables`-Befehl verhält sich sehr ähnlich dem `iptables`-Befehl. Jedoch gibt es einige wesentliche Unterschiede, die hier kurz zusammengefasst werden sollen. Außerdem gibt es beim `ebtables`-Befehl einige zusätzliche Matches und Targets, die ich im Weiteren erläutern werde.

Zunächst weist der Befehl `ebtables` die identischen Kommandos wie der Befehl `Iptables` auf. Es gibt im Einzelnen:

- `-A, --append`. Anhängen einer Regel.
- `-D, --delete`. Löschen einer Regel.
- `-P, --policy`. Ändern der Kettenrichtlinie.
- `-F, --flush`. Löschen einer Tabelle oder Kette.
- `-Z, --zero`. Löschen der Zähler einer Tabelle oder Kette.
- `-L, --list`. Anzeige der Regeln. Hier gibt es einen Unterschied. Zunächst zeigt dieser Befehl die Regeln in einem anderen Format an:

  ```
  # ebtables -t broute -L
  Bridge table: broute

  Bridge chain: BROUTING, entries: 2, policy: ACCEPT
  -p IPv4 -j DROP
  -p ARP -j DROP
  ```

  Um zusätzlich auch Zeilennummern angezeigt zu bekommen, müssen Sie auch die Option `--Ln` angeben. Die Rahmen- und Byte-Zähler erhalten Sie mit `--Lc`:

  ```
  # ebtables -t broute -L --Ln --Lc
  Bridge table: broute

  Bridge chain: BROUTING, entries: 2, policy: ACCEPT
  1. -p IPv4 -j DROP , pcnt = 1016 -- bcnt = 320521
  2. -p ARP -j DROP , pcnt = 3 -- bcnt = 138
  ```

  Wenn Sie die Regeln so anzeigen möchten, dass Sie diese direkt in ein Skript übernehmen können, müssen Sie die Option `--Lx` beim Befehl spezifizieren:

  ```
  # ebtables -t broute -L --Lx
  ebtables -t broute -A BROUTING -p IPv4 -j DROP
  ebtables -t broute -A BROUTING -p ARP -j DROP
  ```

  Schließlich zeigt die Option `-Lmac2` die MAC-Adressen an.

- `-N, --new-chain`. Erzeugt eine benutzerdefinierte Kette.
- `-X, --delete-chain`. Löscht eine benutzerdefinierte Kette.
- `-E, --rename-chain`. Benennt eine benutzerdefinierte Kette um.

- `--init-table`. Initialisiert die Tabelle. Dies löscht alle Regeln und setzt die Richtlinie (Policy) auf den Default zurück.
- `--atomic-init`. Das Kommando `ebtables` kann die Regeln einer Tabelle aus einer Datei lesen. Außerdem kann jeder Befehl auch auf eine Datei angewendet werden (siehe `--atomic-file`). Mit diesem Befehl initialisieren Sie die Datei.
- `--atomic-save`. Dieses Kommando speichert den aktuellen Zustand einer Ebtables-Tabelle in der angegebenen Datei.
- `--atomic-commit` Dieses Kommando lädt die Regeln aus der angegebenen Datei. Dies ist ein atomarer Vorgang. Die Regeln werden alle gleichzeitig geladen! Die Datei kann mit dem Kommando `--atomic-save` oder `--atomic-init` erzeugt werden.

Sie können für die Verwendung mit dem Ebtables-Befehl zunächst alle Regeln in einer Datei aufbauen und dann atomar in einem einzigen Schritt aktivieren. So stellen Sie sicher, dass kein Paket ungefiltert Ihre Bridge passiert. Diese Gefahr besteht, wenn Sie zunächst die Tabelle löschen und dann inkrementell die Regeln aufbauen. Das folgende Listing zeigt beispielhaft, wie Sie die Regeln aufbauen können:

```
$EBTABLES --atomic-file filter_table -t filter --atomic-init
$EBTABLES --atomic-file filter_table -A FORWARD -s 00:11:22:33:44:55 -p IPV4 -j ↵
  ACCEPT
# ... weitere Befehle

# Lade die Tabelle
$EBTABLES --atomic-file filter_table -t filter --atomic-commit
```

Wenn Sie nicht in jeder Zeile die Datei angeben möchten, können Sie auch die Umgebungsvariable `EBTABLES_ATOMIC_FILE` verwenden.

Um die Rahmen in den Regeln zu prüfen, verfügt Ebtables über eingebaute Tests (Matches) und über Erweiterungen (Match-Extensions und Watcher-Extensions). Diese werden im Folgenden kurz erläutert.

Zunächst können Sie das Protokoll des Rahmens mit der Option `-p, --protocol` prüfen. Hierbei handelt es sich nicht um ein Protokoll wie TCP oder UDP. Denken Sie daran, dass Sie hier einen Ethernet-Frame betrachten. Mögliche Protokolle sind IPv4, ARP und NetBEUI. Eine Liste aller möglichen Protokolle finden Sie in der Datei `/etc/ethertypes`. Das Protokoll kann sowohl mit seinem Namen als auch hexadezimal (IPv4 = 0x0800) angegeben werden. Einige Protokolle (802.2) verwenden dieses Feld als Längenangabe. Sobald der Wert in diesem Feld kleiner als 0x600 ist, handelt es sich um eine Länge. Dann verwenden Sie hier bitte `LENGTH`.

Natürlich kann Ebtables auch die Netzwerkkarten prüfen, über die das Paket die Bridge erreicht hat. Hier wird jedoch zwischen dem physikalischen Interface (z.B. eth0) und dem logischen Interface (z.B. br0) unterschieden. Die eingehenden Interfaces können Sie in den Ketten `INPUT`, `FORWARD`, `PREROUTING` und `BROUTING` testen, während Sie die ausgehenden Interfaces in den Ketten `OUTPUT`, `FORWARD` und `POSTROUTING` testen können. Die Optionen heißen:

- `-i, --in-if, --in-interface`
- `--logical-in`
- `-o, --out-if, --out-interface`
- `--logical-out`

Um die MAC-Adressen des Rahmens zu prüfen, gibt es die Optionen `-s, --src, --source` beziehungsweise `-d, --dst, --destination`. Die Adresse wird als hexadezimale Adresse mit Doppelpunkten geschrieben: `00:50:56:C0:00:03`. Beide Optionen erlauben auch die Angabe einer Netzmaske. Alternativ können Sie als Absenderadresse auch `Unicast`, `Broadcast`, `Multicast` oder `BGA` (Bridge Group Address) angeben. Um diese Typen als Zieladresse zu prüfen, existiert die Option `--pkt-type` (siehe unten).

Der Ebtables-Befehl verfügt über eine Reihe von Erweiterungen, die für die Prüfung von Rahmen genutzt werden können. Diese Erweiterungen müssen nicht wie bei `iptables` mit der Option `-m` geladen werden. Sie werden jedoch in eigenen Kernel-Modulen implementiert.

Für die Prüfung von 802.2- oder 802.3-Rahmen stehen die Optionen `--802_3-sap` und `--802_3-type` zur Verfügung.

Für das ARP- und das RARP-Protokoll können Sie die folgenden Optionen verwenden. Diese Optionen sind nur gültig, wenn Sie auch als Protokoll (`-p`) ARP oder RARP spezifiziert haben.

- `--arp-opcode`. Diese Option gibt den ARP-Operation-Code an. Insgesamt existieren neun verschiedene Opcodes:
  - Request (1)
  - Reply (2)
  - Request_Reverse (3)
  - Reply_Reverse (4)
  - DRARP_Request (5)
  - DRARP_Reply (6)
  - DRARP_Error (7)
  - InARP_Request (8)
  - ARP_NAK (9)

  Diese Opcodes können als Zeichenkette oder numerisch angegeben werden.
- `--arp-htype`. Der Hardware-Typ. Eigentlich immer Ethernet (1).
- `--arp-ptype`. Der Protokoll-Typ. Eigentlich immer IPv4 (0x0800).
- `--arp-ip-src, --arp-ip-dst`. Die IP-Absender- beziehungsweise IP-Zieladresse des ARP-Pakets.
- `--arp-mac-src, --arp-mac-dst`. Die MAC-Absender- beziehungsweise MAC-Zieladresse des ARP-Pakets.

Wenn Sie als Protokoll (`-p`) IPv4 in der Regel spezifizieren, dürfen Sie die folgenden Optionen nutzen, um rudimentär das IP-Paket zu prüfen. Diese Optionen erreichen bei weitem nicht die Mächtigkeit des `iptables`-Kommandos.

So können Sie mit den Optionen `--ip-source`, `--ip-src` und `--ip-destination`, `--ip-dst` die Absender- und Ziel-IP-Adresse prüfen. Mit `--ip-tos` kann durch Angabe der hexadezimalen Nummer der Type-of-Service geprüft werden. Die Option `--ip-protocol`, `--ip-proto` erlaubt die Prüfung des IP-Protokolls (z.B. TCP oder UDP). Handelt es sich um ein TCP- oder UDP-Paket, können Sie mit `--ip-source-port`, `--ip-sport` und `--ip-destination-port`, `--ip-dport` die Ports testen.

Ebtables unterstützt genauso wie Iptables die Markierung von Paketen. Mit der Option `--mark` können Sie diese Markierung testen.

Die Option `--pkt-type` gibt Ihnen die Möglichkeit, den Pakettyp zu testen. Mögliche Typen sind `broadcast`, `multicast`, `host` und `otherhost`. Ist das Paket an den lokalen Rechner gerichtet, so ist der Typ `host`. Alle anderen Unicast-Pakete sind `otherhost`.

Für die Prüfung von Spanning-Tree-Protokoll-Rahmen (STP) gibt es eine Vielzahl von Optionen, die hier nur verwirren würden. Auf der Manpage finden Sie weitere Informationen. Auch die VLAN-Testoptionen sollen hier nicht besprochen werden.

Um Pakete zu protokollieren, existiert die Option `--log`. Die Protokollierung ist bei Ebtables im Gegensatz zu Iptables eine Option und kein Ziel (Target). Die Option `--log` protokolliert das Paket mit den Defaultwerten für den Level, das Präfix und ohne IP- und ARP-Informationen. Wenn Sie diese Defaultwerte ändern möchten, nutzen Sie anstelle der Option `--log` die Optionen `--log-prefix`, `--log-level`, `--log-ip` und `--log-arp`.

Sobald eine Regel auf einen Rahmen zutrifft, kann Ebtables verschiedene Aktionen ausführen. Zusätzlich zu den von Iptables bekannten Aktionen `ACCEPT`, `DROP` und `RETURN` besitzt Ebtables auch noch `CONTINUE` und Erweiterungen (Target Extensions). Wurde `CONTINUE` als Ziel (Target) einer Regel angegeben, so wird bei Zutreffen dieser Regel die Kette nicht verlassen, sondern die weiteren Regeln der Kette werden abgearbeitet.

Als Erweiterungen stehen `arpreply`, `dnat`, `mark`, `redirect` und `snat` zur Verfügung. Achtung, diese Ziele werden entgegen der Konvention kleingeschrieben! Bei allen diesen Zielen müssen Sie zusätzlich noch angeben, was anschließend mit dem Paket passieren soll. Hierfür gibt es bei jedem Ziel noch eine zusätzliche Option, die weiter unten erläutert wird.

- `-j arpreply`. Das `arpreply`-Ziel erlaubt es, ARP-Anfragen zu beantworten. Dieses Ziel dürfen Sie nur in der `PREROUTING`-Kette der `nat`-Tabelle verwenden. Die Regel erkennt selbstständig, ob es sich um ARP-Anfragen handelt. Mit der Option `--arpreply-mac` können Sie die MAC-Adresse angeben, die in der Antwort verwendet werden soll. Mit der Option `--arpreply-target` geben Sie an, wie Ebtables anschließend den originalen Rahmen behandeln soll. Die Default-Einstellung ist DROP. Dies hat den Nachteil, dass der lokale ARP-Cache nicht mit den Absenderinformationen aktualisiert wird. Wenn Sie das Target auf `ACCEPT` oder `CONTINUE` setzen, ist dies dennoch der Fall. Sie müssen dann nur aufpassen, dass nicht ein weiterer ARP-Reply ausgesendet wird!

- `-j dnat`. Dieses Ziel darf in der `BROUTING`-Kette und in den `PREROUTING`- und `OUTPUT`-Ketten der `nat`-Tabelle genutzt werden. Die Ziel-MAC-Adresse geben Sie mit `--to-destination`, `--to-dst` an. Anschließend wird das Paket akzeptiert. Wenn Sie dies ändern möchten, können Sie mit `--dnat-target` ein anderes Ziel angeben.
- `-j mark`. Ebtables unterstützt wie Iptables eine Markierung der Rahmen/Pakete. Die Markierung geben Sie mit `--set-mark` als hexadezimale unsignierte Zahl an. Anschließend wird das Paket akzeptiert. Wenn Sie weitere Modifikationen des Pakets in der gleichen Kette vornehmen wollen, können Sie das mit `--mark-target CONTINUE` erreichen.
- `-j redirect`. Dieses Ziel ist analog dem `REDIRECT`-Ziel von Iptables und erlaubt es, Pakete in der `BROUTING`- und `PREROUTING`-Kette, die eigentlich an eine andere MAC-Adresse gerichtet sind und gebridgt werden müssten, auf die lokale MAC-Adresse umzuleiten. Dabei wird als neue Ziel-MAC-Adresse die Adresse der Netzwerkkarte genutzt, über die der Rahmen das System erreicht hat. Anschließend wird das Paket akzeptiert. Das Verhalten können Sie mit `--redirect-target` ändern.

  Mit dieser Option können Sie auf einer Bridge Verbindungen über einen transparenten Proxy lenken!
- `-j snat`. Hiermit können Sie in der `POSTROUTING`-Kette die Absender-MAC-Adresse ändern. Die neue MAC-Adresse geben Sie mit `--to-source`, `--to-src` an. Mit `--snat-target` können Sie ein anderes Ziel als `ACCEPT` (Default) angeben.

31.5 Start einer Bridge auf Fedora Core

Die Linux-Distribution Fedora Core enthält bereits in ihren Startskripten die Möglichkeit, eine Bridge zu initialisieren. Hierzu erzeugen Sie die folgenden Dateien in dem Verzeichnis `/etc/sysconfig/network-scripts`:

- `ifcfg-br0`

```
DEVICE=br0
ONBOOT=yes
BOOTPROTO=static
IPADDR=10.1.2.3
NETMASK=255.255.255.0
TYPE=Bridge
STP=off
DELAY=0
GCINT=30
```

- `ifcfg-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
BRIDGE=br0
```

- ifcfg-eth1
  ```
  DEVICE=eth1
  ONBOOT=yes
  BOOTPROTO=static
  BRIDGE=br0
  ```
- Für jede weitere Netzwerkkarte der Bridge gibt es eine entsprechende Datei.

Fedora Core wird nun beim Booten die entsprechende Bridge initialisieren und die physikalischen Netzwerkkarten hinzufügen. Mit dem Parameter `STP` können Sie das STP-Protokoll an- beziehungsweise abschalten.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

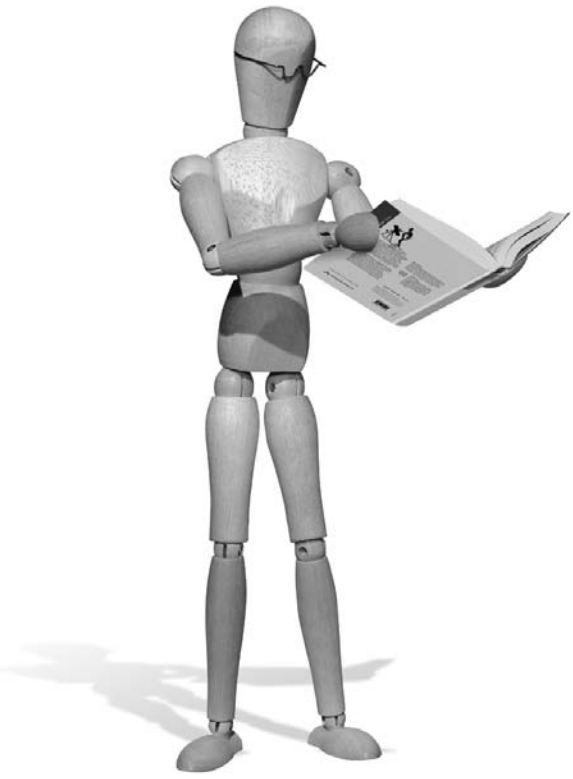
ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Teil VII

Protokolle und Applikationen



32 Behandlung einzelner Protokolle

Dieses Kapitel bespricht einzelne IP-Protokolle bei ihrer Filterung durch Iptables und gibt Ihnen wertvolle Tipps für die sichere Konfiguration Ihrer Firewall. Dabei werden zunächst immer die Möglichkeiten aufgezeigt, die Sie in einer Standard-Linux-Distribution vorfinden. Wenn es darüber hinaus besondere Patches oder Erweiterungen gibt, werden diese extra behandelt und ihre Vorteile erläutert, so dass Sie selbst entscheiden können, ob Sie diese nutzen möchten.

32.1 DHCP

Das Dynamic Host Configuration Protocol erlaubt die automatische IP-Konfiguration der Komponenten in einem Netzwerk. Es benötigt hierzu einen Server, der diese Konfigurationsparameter verwaltet und verteilt. Dabei löst der DHCP-Server das Problem der Zurordnung eindeutiger IP-Adressen, da er eine IP-Adresse nicht gleichzeitig an zwei Netzwerkkomponenten verteilt.

Grundsätzlich gibt es zwei verschiedene Möglichkeiten der Verteilung der IP-Adressen, die aber auch kombiniert eingesetzt werden können:

- Manuelle Zuordnung: Sie ordnen in der Konfiguration des DHCP-Servers jeder MAC-Adresse eine feste IP-Adresse zu. Sobald ein Client mit der MAC-Adresse sich beim DHCP-Server meldet, erhält er die entsprechende IP-Adresse.
- Dynamische Zuordnung: Sie weisen dem Server einen bestimmten Bereich von IP-Adressen zu, die er dynamisch verteilen darf. Sobald sich ein Client bei ihm meldet, weist er diesem Client für eine bestimmte Zeit eine IP-Adresse zu. Der Client darf diese Adresse für den genannten Zeitraum (Lease) nutzen. Anschließend kann der Server die Adresse an einen weiteren Client vergeben. Um die Adresse länger benutzen zu dürfen, muss der Client sich um eine Verlängerung bemühen.

Obwohl es zwei verschiedene Varianten der Zuordnung gibt, ist das Protokoll bei beiden Varianten identisch.

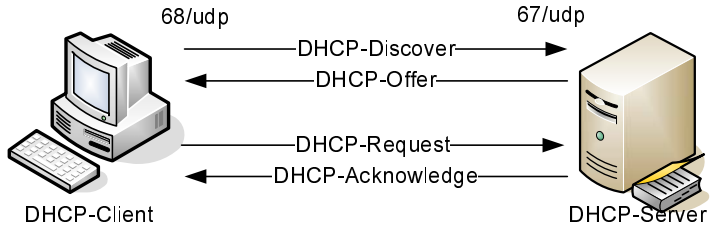


Abbildung 32.1: Das DHCP-Protokoll

32.1.1 Das DHCP-Protokoll

Das DHCP-Protokoll basiert auf dem UDP-Protokoll. Der Server bindet sich auf den Port 67 (bootps), während der Client den Port 68 (bootpc) verwendet. Die gewählten IP-Adressen hängen stark von dem Zustand des Clients ab (siehe Abbildung 32.1).

Eine DHCP-Verbindung besteht aus folgenden Paketen:

1. Der Client sendet eine DHCP-Discover-Nachricht an sämtliche DHCP-Server in dem lokalen Netzwerk. Dieses UDP-Paket hat die IP-Absenderadresse 0.0.0.0:68 und die Zieladresse 255.255.255.255:67.
2. Alle verfügbaren DHCP-Server antworten mit einer DHCP-Offer-Nachricht, in der sie eine IP-Adresse anbieten.
3. Der Client wählt eines der Angebote aus und sendet einen DHCP-Request.
4. Dieser DHCP-Request wird von dem Server mit einem DHCP-Acknowledge bestätigt.
5. Jetzt darf der Client die IP-Adresse verwenden.
6. Bei einer Verlängerung (Renewal) der Nutzungsdauer (Lease) sendet der Client einen DHCP-Request als Unicast-Paket direkt an die Adresse des DHCP-Servers und trägt seine noch gültige IP-Adresse auch als Quell-IP-Adresse ein.

32.1.2 Iptables-Regeln

Es ist eher unwahrscheinlich, dass Sie das DHCP-Protokoll auf einer normalen Firewall filtern möchten, da das Protokoll auf einer Broadcast-Kommunikation basiert und daher nicht über Router und damit auch nicht über Paketfilter arbeiten kann. Jedoch kann es sein, dass Sie für die Kommunikation über den Paketfilter ein DHCP-Relay einsetzen, das genau diese Aufgabe übernimmt. Es nimmt die Broadcast-Anfrage entgegen und leitet sie per Unicast-Paket an den DHCP-Server in einem anderen Netz weiter. Dann benötigen Sie folgende Regeln:

Listing 32.1: Regeln für die Kommunikation eines DHCP-Relays mit einem DHCP-Server

```
DHCP_SERVER=192.168.0.2
DHCP_RELAY=192.168.1.2

$IPTABLES -A FORWARD -s $DHCP_RELAY -d $DHCP_SERVER -p udp --sport bootpc --dport bootps ↵
  -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Wenn Sie einen DHCP-Server mit einer lokalen Firewall schützen möchten, benötigen Sie die folgenden Regeln:

```
$IPTABLES -A INPUT -p udp --sport bootpc --dport bootps -m state --state NEW -j ACCEPT
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Es gibt jedoch auch einen Fall, bei dem es Sinn machen kann, das DHCP-Protokoll tatsächlich über eine Firewall zu erlauben. Dies ist der Fall, wenn Sie eine transparente Firewall im Bridge-Mode aufbauen. Dann arbeitet die Firewall nicht als Router, sondern wie eine Bridge und sollte DHCP-Pakete erlauben.

```
DHCP_SERVER=192.168.0.2
CLIENTS=192.168.0.0/24

$IPTABLES -A FORWARD -s $CLIENTS -d $DHCP_SERVER -p udp --sport bootpc --dport bootps ↵
  -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -s 0.0.0.0 -d 255.255.255.255 -p udp --sport bootpc --dport bootps ↵
  -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

32.2 DNS

Das Domain Name System (DNS) ist einer der wichtigsten Dienste im Internet. Es handelt sich dabei um eine große hochverfügbare und verteilte Datenbank, die den Namensraum im Internet verwaltet. Seine wesentliche Aufgabe ist die Auflösung von Namen in IP-Adressen und umgekehrt. Zusätzlich ist es aber auch für das Mail-Routing verantwortlich und wird immer mehr für den Schlüsselaustausch von PKI-Systemen genutzt.

32.2.1 Das DNS-Protokoll

Das DNS-Protokoll unterscheidet sich von den meisten anderen Protokollen dadurch, dass es sowohl UDP als auch TCP als Transportprotokoll nutzen kann. Die Auswahl des Transportprotokolls erfolgt dabei jedoch nicht beliebig. Der Client stellt zunächst die Anfrage mit dem UDP-Protokoll. Dabei verwendet der Server

den Port 53/udp und der Client einen beliebigen UDP-Port > 1023. Der Server beantwortet die Anfrage. Wenn jedoch die Antwort ein Paket > 512 Bytes benötigt, dann wird das Paket bei 512 Bytes abgeschnitten und das TC-Flag im DNS-Header gesetzt. Dieses Flag bedeutet *truncated* (abgeschnitten). Der Client muss dann erneut die Anfrage stellen. Diese neue Anfrage wird mit dem TCP-Protokoll gestellt.

Achtung

Das RFC 2671 hat zumindest die Voraussetzungen geschaffen, dass diese letzte Einschränkung fällt. Mit dem RFC *Extension Mechanisms for DNS (EDNS0)* ist es möglich, dass der Client die Größe seines Empfangspuffers angibt und so auch größere Pakete als 512 Bytes gesendet werden dürfen.

Ein Betriebssystem, das jetzt bereits diese Funktion nutzt, ist Microsoft Windows 2003 Server. Dies kann zu Problemen führen, wenn Firewalls DNS-UDP-Pakete > 512 Bytes verwerfen (z.B. Cisco PIX < 6.3). Diese Funktionalität kann bei Win2k3 mit dem Kommando `dnscmd` abgeschaltet werden:

```
dnscmd /config /enableednsprobes 0
```

Zur Synchronisation der sekundären Nameserver mit den primären Nameservern werden Zonentransfers durchgeführt. Diese Zonentransfers werden grundsätzlich mit dem TCP-Protokoll durchgeführt.

Das DNS-Protokoll ist ein Klartextprotokoll. Eine Authentifizierung und Signatur ist bei Bedarf möglich (TSIG, DNSSEC), wird aber im täglichen Einsatz meistens nicht verwendet.

32.2.2 Iptables-Regeln

Da häufig nur bestimmte DNS-Server für die Namensauflösung eingesetzt werden, kann es sinnvoll sein, die erlaubten DNS-Anfragen speziell auf diese Nameserver zu begrenzen.

Achtung

Selbst wenn Sie die Nutzung auf spezielle Nameserver beschränken, besteht die Gefahr, dass das DNS-Protokoll zur Übertragung anderer Informationen genutzt wird.

Seit einigen Jahren existieren Anwendungen, die beliebige Protokolle über DNS tunneln können. Das bekannteste Programm für einen DNS-Tunnel ist sicher nstx (*http://nstx.dereference.de/nstx/*). Eine Beschreibung dieses Programmes finden Sie hier: *http://www.heise.de/security/artikel/print/43716/*.

Ein weiteres mächtigeres Programm wurde von Dan Kaminsky auf der Blackhat 2005 in Amsterdam vorgestellt. Sein Fragile-Router-Protocol ist in der Lage, 65 Kbit/s Daten über das DNS-Protokoll zu streamen.

Da DNS-Server Anfragen, die sie nicht beantworten können, weiterleiten, ist die Einschränkung der Nutzung auf bestimmte Nameserver nicht ausreichend.

Im Folgenden stelle ich die Regeln für drei Szenarien vor.

1. Ein LAN greift auf einen DNS-Server zu. Dann benötigen Sie die folgenden Regeln:

```
LANDEV=eth0
EXTDEV=eth1
DNSSERVER="3.0.0.1 5.0.0.1"
for DNSSRV in $DNSSERVER
do
  $IPTABLES -A FORWARD -i $LANDEV -o $EXTDEV -p udp --dport 53 -d $DNSSRV -m state↵
  --state NEW -j ACCEPT
  $IPTABLES -A FORWARD -i $LANDEV -o $EXTDEV -p tcp --dport 53 -d $DNSSRV -m state↵
  --state NEW -j ACCEPT
done
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

2. Ein DNS-Server greift auf weitere DNS-Server zu. Hier können Sie den Client der DNS-Verbindung zusätzlich einschränken. Dies erhöht die Sicherheit vor einem eventuellen DNS-Tunnel.

```
LANDEV=eth0
EXTDEV=eth1
MYDNS=192.168.255.2
DNSSERVER="3.0.0.1 5.0.0.1"
for DNSSRV in $DNSSERVER
do
  $IPTABLES -A FORWARD -i $LANDEV -o $EXTDEV -p udp --dport 53 -s $MYDNS -d $DNSSRV↵
  -m state --state NEW -j ACCEPT
  $IPTABLES -A FORWARD -i $LANDEV -o $EXTDEV -p tcp --dport 53 -s $MYDNS -d $DNSSRV↵
  -m state --state NEW -j ACCEPT
done
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

3. Sie möchten einen DNS-Server mit einer lokalen Firewall schützen. Dieser muss sowohl auf weitere DNS-Server für die rekursive Auflösung zugreifen als auch den Zugriff der lokalen Clients erlauben.

```
# Der DNS-Server muss auf andere DNS-Server zugreifen
```

```
DNSSERVER="3.0.0.1 5.0.0.1"
CLIENTS=192.168.0.0/24

for DNSSRV in $DNSSERVER
do
  $IPTABLES -A OUTPUT -p udp --dport 53 -d $DNSSRV -m state --state NEW -m owner ↲
  --uid-owner named --cmd-owner named -j ACCEPT
  $IPTABLES -A OUTPUT -p tcp --dport 53 -d $DNSSRV -m state --state NEW -m owner ↲
  --uid-owner named --cmd-owner named -j ACCEPT
done

# Die Clients müssen auf ihn zugreifen
$IPTABLES -A INPUT -s $CLIENTS -p udp --dport 53 -m state --state NEW -j ACCEPT
$IPTABLES -A OUTPUT -s $CLIENTS -p tcp --dport 53 -m state --state NEW -j ACCEPT

$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

32.3 HTTP/HTTPS/Proxy

Das HTTP-Protokoll ist mit Abstand das am häufigsten verwendete Protokoll im Internet. Etwa 70-80% des gesamten Internetverkehrs wird von diesem Protokoll transportiert. Es dient dem Zugriff auf Webserver und verwendet üblicherweise auf der Seite des Servers den TCP-Port 80. Clientseitig wird ein beliebiger TCP-Port > 1024 verwendet.

Das HTTPS-Protokoll ist mit dem HTTP-Protokoll identisch. Es verwendet nur zusätzlich die Secure Socket Layer (SSL). Dies erlaubt eine Authentifizierung des Servers und des Clients mit einer anschließenden Verschlüsselung der gesamten Verbindung. Für die Authentifizierung benötigt das SSL-Protokoll öffentliche Schlüssel in Form von X.509-Zertifikaten. Der zu authentifizierende Rechner muss zusätzlich über den passenden privaten Schlüssel verfügen. Das HTTPS-Protokoll verwendet einen eigenen Port (443/tcp) und verlangt auf diesem Port den Einsatz von SSL.

Bei dem Zugriff auf einen Proxy wird ebenfalls das HTTP-Protokoll verwendet. Auch hier nutzt der Client nur einen einzigen Port für die Kommunikation mit dem Server. Dieser TCP-Port ist häufig frei wählbar. Jedoch hat auch jeder Proxy einen typischen Standardport (Squid: 3128/tcp). Wenn der Proxy mehrere Protokolle (z.B. HTTP, HTTPS und FTP) erlaubt, erfolgt der Zugriff des Clients immer mit HTTP.

Das HTTP-Protokoll ist ein zustandsloses Protokoll. Normalerweise baut der Client für jede Information, die er wünscht, eine eigene Verbindung auf und fordert die Daten an. Der Server überträgt die Daten und baut die Verbindung ab. Für den Server handelt es sich bei jeder Verbindung um einen neuen Client. Damit eine Webapplikation auf dem Server erkennen kann, dass es sich bei allen Aufrufen um denselben Benutzer handelt, wurden Cookies erfunden. Es gibt clientseitige

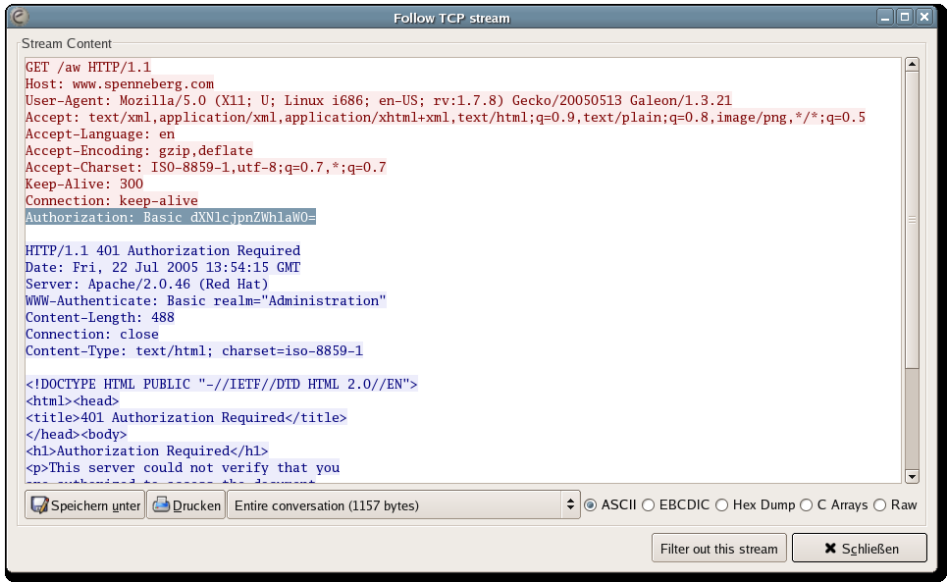


Abbildung 32.2: Ethereal kann die BASIC-HTTP-Authentifizierung anzeigen.

Cookies, die von dem Server an den Browser übertragen werden und beim nächsten Besuch von dem Browser wieder an den Server geschickt werden. Im Gegensatz dazu werden serverseitige Cookies meist in der URL als Zeichenkette kodiert. Der Server stattet alle Verknüpfungen auf der Webseite mit derselben Zeichenkette aus und kann so den Weg des Benutzers durch die Seiten verfolgen.

Das HTTP-Protokoll erlaubt auch eine Authentifizierung des Benutzers mit Benutzernamen und Kennwort. Dabei existieren insgesamt drei Möglichkeiten der Übertragung dieser Informationen:

- BASIC: Hier werden der Benutzername und das Kennwort, durch einen Doppelpunkt getrennt, in Base64-Kodierung übertragen. Es handelt sich also um eine Übertragung in Klartext. Mit der Anwendung Ethereal können Sie sich diese Zeichenkette ansehen (Abbildung 32.2)

  Die Zeichenkette lässt sich dann auf jedem Linux-System leicht dekodieren:

  ```
  [spenneb@bibo screenshots]$ echo "dXNlcjpnZWhlaW0=" | openssl base64 -d
  user:geheim
  ```

- DIGEST: Hier wird lediglich der Benutzername übertragen. Anstelle des Kennworts wird das Ergebnis einer mathematischen Berechnung übertragen. Dazu übermittelt der Server eine Zufallszahl an den Client, der aus dieser Zahl und dem Kennwort eine Antwort errechnet und diese zurückschickt. Der Server führt dieselbe Berechnung durch und vergleicht das Ergebnis.

- NTLM: Hier erfolgt die Anmeldung analog einer Anmeldung an einem Microsoft Windows-Server. Die Anmeldeinformationen werden hier verschlüsselt übertragen.

Bei der Verwendung der Authentifizierung direkt durch das HTTP-Protokoll ist zu beachten, dass diese Informationen bei jedem Verbindungsaufbau erneut übertragen werden, da der Server nicht in der Lage ist zu erkennen, dass die Verbindungen immer von demselben Benutzer aufgebaut werden! Daher ist es sinnvoll, entweder die gesamten Verbindungen mit Secure Socket Layer (SSL) zu schützen oder auf alternative Authentifizierungsverfahren umzustellen. Hierzu werden häufig Webapplikationen genutzt, die eine Authentifizierung verlangen. Diese Phase wird mit SSL geschützt. Anschließend erzeugt die Webapplikation eine Zufallszahl, die in einem Cookie gespeichert wird, der anschließend für die Authentifizierung genutzt wird. Die weiteren Verbindungen können dann wieder in Klartext übertragen werden, da kein Kennwort mehr übertragen wird. Es besteht nur die Gefahr, dass der Cookie geklaut wird. Daher wird häufig dieser Cookie mit einer maximalen Lebensdauer von wenigen Minuten versehen.

32.3.1 Iptables-Regeln

Die Iptables-Regeln für dieses Protokoll sind sehr einfach, da es lediglich zwei Ports (HTTP: 80/tcp und HTTPS: 443/tcp) verwendet. Wenn Sie keine HTTPS-Verbindungen erlauben wollen, entfernen Sie den Port 443 zu den Regeln.

Zunächst werden Beispielregeln demonstriert, so dass ein LAN auf beliebige Webserver im Internet zugreifen darf.

Listing 32.2: Zugriff auf Webserver im Internet

```
LANDEV=eth0
EXTDEV=eth1

$IPTABLES -A FORWARD -i LANDEV -o EXTDEV -p tcp -m multiport --dport 80,443 -m state ↵
  --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Natürlich können Sie auch einen Webserver mit einer lokalen Firewall sichern. Dann können Sie folgende Regeln verwenden:

Listing 32.3: Eine lokale Firewall schützt den Webserver.

```
$IPTABLES -A INPUT -p tcp -m multiport --dport 80,443 -m state --state NEW -j ACCEPT
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

32.4 ELSTER

Die elektronische Steuererklärung (ELSTER) überträgt die Steuerdaten über das Internet an die Finanzämter in Deutschland. Hierbei werden die Daten verschlüsselt übertragen. Über ELSTER können die folgenden Informationen übermittelt werden:

- Einkommensteuererklärung
- Umsatzsteuer-Voranmeldung
- Antrag auf Dauerfristverlängerung
- Antrag auf Sondervorzahlung
- Umsatzsteuererklärung
- Gewerbesteuererklärung
- Lohnsteuererklärung
- und Lohnsteuerbescheinigungen

Leider gibt es inzwischen verschiedene Möglichkeiten der Übertragung, die von unterschiedlichen Systemen unterschiedlich genutzt werden. Elster selbst ist eine Software, die nicht einzeln erhältlich ist, sondern in andere Programme, zum Beispiel Buchhaltungs- oder Lohn- und Gehaltssoftware eingebaut wird. Des Weiteren gibt es mit der Software ElsterFormular eine kostenlose Software, die zum Ausfüllen der Formulare und deren Übertragung genutzt werden kann. Ab Mitte September 2005 wird mit ElsterOnline ein zusätzlicher Weg eröffnet, der nur noch einen Browser benötigt. Die Übertragung erfolgt dann über HTTPS. Ab 2006 wird dies wahrscheinlich das ElsterFormular ablösen. ElsterFT ist schließlich eine Software für Behörden, um verfahrensabhängige Formulare herunterzuladen, Sende- und Abholaufträge zu erstellen und Monitor- und Protokollfunktionen zu übernehmen. Eine Übertragung von Steuererklärungen oder deren Daten ist nicht möglich.

Das ElsterFormular benötigt für die Übertragung der Daten Zugriff auf den TCP-Port 8000. Alternativ ist auch die Übertragung über einen HTTP-Proxy möglich. Dann muss dieser aber den Zugriff auf den TCP-Port 8000 ermöglichen.

ElsterFT benötigt Zugriff auf den TCP-Port 80. Ein Zugriff über einen Proxy ist möglich. Elster selbst benötigt je nach Version Zugriff auf den TCP-Port 8000 oder 80.

32.4.1 Iptables-Regeln

Im Wesentlichen benötigt Elster Zugriff auf die Server der Finanzverwaltung. Hier muss der Zugriff auf den TCP-Port 80 und 8000 möglich sein. Die aktuelle Liste der Elster-Server (Stand Oktober 2005): 62.157.211.58, 62.157.211.59, 62.157.211.60, 193.109.238.26, 193.109.238.27 und 213.182.157.55. Folgende Regeln erlauben den Zugriff:

```
ELSTER_SERVER="62.157.211.58 62.157.211.59 62.157.211.60 193.109.238.26 193.109.238.27 ↵
  213.182.157.55"
```

```
for SRV in $ELSTER_SERVER
do
  $IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -d $SRV -p tcp -m multiport --dport 80,8000 ↵
    -m state --state NEW -j ACCEPT
done
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Wenn Ihr Kernel und Ihr Iptables-Befehl den Befehl `ipset` unterstützen, können Sie das auch einfacher konfigurieren:

```
IPSET=/sbin/ipset
$IPSET -N elster iphash
$IPSET -A elster 62.157.211.58
$IPSET -A elster 62.157.211.59
$IPSET -A elster 62.157.211.60
$IPSET -A elster 193.109.238.26
$IPSET -A elster 193.109.238.27
$IPSET -A elster 213.182.157.55
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -m set --set elster dst -p tcp -m multiport ↵
  --dport 80,8000 -m state --state NEW -j ACCEPT
```

Diese Regeln benutzen nur eine einzige Iptables-Regel. Damit ist das Regelwerk wesentlich übersichtlicher als mit sechs Regeln.

32.5 Telnet

Das Telnet-Protokoll simuliert eine Terminal-Umgebung über ein Netzwerk (**T**erminal **E**mu**L**ation over **NET**work). Es überträgt sämtliche Daten in Klartext. Dies trifft auch auf den Benutzernamen und das Kennwort zu. Daher wird eine Anmeldung als *root* üblicherweise auch abgelehnt. Achtung, das Kennwort wird trotzdem übertragen. Es gibt moderne sichere Alternativen, wie Telnet über SSL, kerberosiertes Telnet und die Secure Shell (SSH). Der Telnet-Server nimmt auf dem TCP-Port 23 Verbindungen entgegen. Der Client wählt einen beliebigen Port > 1023.

32.5.1 Iptables-Regeln

Obwohl ich grundsätzlich gegen den Einsatz von Telnet in modernen Netzwerken plädiere, da es wesentliche Sicherheitslücken aufweist, wird der Einsatz dennoch häufig gefordert. Häufig werden noch Netzwerkkomponenten wie Router, Switches oder Drucker per `telnet` konfiguriert. Eine Aufrüstung auf SSH ist teilweise zwar möglich, kostet aber zusätzliche Lizenzgebühren.

```
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p tcp --dport 23 -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Wenn Sie einen Telnet-Server mit einer lokalen Firewall schützen möchten, verwenden Sie die folgenden Regeln:

```
$IPTABLES -A INPUT -p tcp --dport 23 -m state --state NEW -j ACCEPT
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

32.6 SSH

Die Secure Shell (SSH) stellt eine sichere Alternative zu den folgenden Portokollen und Anwendungen dar: `telnet`, `rlogin`, `rcp`, `ftp` etc. Dabei überprüft die Secure Shell im ersten Schritt die Identität des Servers, zu dem die Verbindung aufgebaut wird, bevor das Kennwort über einen verschlüsselten Tunnel übertragen wird. Achtung: Das Kennwort erreicht den Serverprozess in Klartext. Lediglich die Übertragung ist verschlüsselt. Ein bösartiger Server könnte das Kennwort in Klartext abspeichern. Um auch hiervor Schutz zu bieten, bietet die SSH auch die Authentifizierung des Clients mit öffentlichen Schlüsseln an. Sämtliche anschließend übertragenen Daten werden dann von der SSH verschlüsselt, und jedes einzelne Paket wird auf seine Integrität und Authentizität geprüft.

Die meisten Implementierungen der Secure Shell bieten inzwischen nicht nur den `ssh`-Befehl, sondern auch die Befehle `scp` und `sftp`. Mit diesen Befehlen können Dateien kopiert oder ftp-ähnlich transportiert werden. Unabhängig von dem gewählten Namen werden die Daten rein über die SSH-Verbindung transportiert. Ein zusätzlicher FTP-Server ist nicht erforderlich.

Der SSH-Server bindet sich auf den TCP-Port 22 und nimmt dort Verbindungen entgegen.

32.6.1 Iptables-Regeln

Die Regeln für die Filterung von SSH sind sehr einfach und mit den Regeln für einen HTTP-Server vergleichbar.

Listing 32.4: Zugriff auf SSH-Server im Internet

```
LANDEV=eth0
EXTDEV=eth1

$IPTABLES -A FORWARD -i LANDEV -o EXTDEV -p tcp --dport 22 -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Natürlich können Sie auch einen SSH-Server mit einer lokalen Firewall sichern. Dann können Sie folgende Regeln verwenden:

Listing 32.5: Eine lokale Firewall schützt den SSH-Server.

```
$IPTABLES -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

32.7 P2P: Edonkey

Bei den Peer2Peer-Netzwerken gibt es grundsätzlich zwei Ansätze eines Firewall-Administrators. Der Heimanwender möchte diese Dienste häufig nutzen, um einfach auf bestimmte Dateien zugreifen zu können. Der Administrator in einer Firma möchte möglichst jede Anwendung verhindern, da die Gefahr besteht, dass mit diesen Protokollen Copyright-Verletzungen erfolgen, die negative Folgen für die Firma haben können. Wir werden daher beide Varianten darstellen. Wie können Sie möglichst einfach P2P-Verkehr erkennen und verhindern, und wie ermöglichen Sie diesen Verkehr?

Edonkey nutzt wie fast alle anderen P2P-Netze hohe Ports (> 1023) für die Kommunikation des Clients mit dem Server. Bei Edonkey handelt es sich um die folgenden Ports:

- 4661/tcp: Der Client verbindet sich mit diesem Port auf dem Server und meldet sich dort an.
- 4662/tcp: Der Server verbindet sich mit diesem Port auf dem Client. Die Erreichbarkeit dieses Ports durch den Server auf dem Client entscheidet auch darüber, ob der Client eine hohe ($\geq$ 16777217) oder eine niedrige ID ($\leq$ 16777216) erhält. Dieser Port kann auf dem Client geändert werden. Die ID ist ausschlaggebend für die eigene Download-Rate auf fremden Servern.
- 4665/udp: Dieser Port wird benötigt, um Quellen auf Servern zu finden, auf denen man nicht angemeldet ist.
- 4672/udp: Dieser Port wird für direkte Client-Client-Verbindungen genutzt. Auch dieser Port ist einstellbar.

32.7.1 Iptables-Regeln

Um nun mit einem Client eine Verbindung zum Edonkey-Netzwerk aufzubauen, sollte eine Verbindung zu den entsprechenden Ports erlaubt werden:

```
# Client-Zugriff auf den Server
EDONKEY_CLIENT=192.168.0.5
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -s $EDONKEY_CLIENT -p tcp -m multiport ↵
  --dport 4661,4662 -m state --state -NEW -j ACCEPT
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -s $EDONKEY_CLIENT -p udp -m multiport ↵
  --dport 4665,4672 -m state --state -NEW -j ACCEPT

# Zugriff auf den Client
```

```
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tcp --dport 4662 -j DNAT ↲
  --to-destination $EDONKEY_CLIENT
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p udp --dport 4672 -j DNAT ↲
  --to-destination $EDONKEY_CLIENT
$IPTABLES -A FORWARD -i $EXTDEV -o $INTDEV -d $EDONKEY_CLIENT -p tcp --dport 4662 ↲
  -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -i $EXTDEV -o $INTDEV -d $EDONKEY_CLIENT -p udp --dport 4672 ↲
  -m state --state NEW -j ACCEPT

$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Falls Sie den Edonkey-Client mit einer lokalen Firewall direkt schützen möchten, benötigen Sie folgende Regeln:

```
$IPTABLES -A OUTPUT -p tcp -m multiport --dport 4661,4662 -m state --state -NEW -j ACCEPT
$IPTABLES -A OUTPUT -p udp -m multiport --dport 4665,4672 -m state --state -NEW -j ACCEPT
$IPTABLES -A INPUT -p tcp --dport 4662 -m state --state NEW -j ACCEPT
$IPTABLES -A INPUT -p udp --dport 4672 -m state --state NEW -j ACCEPT

$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Häufiger jedoch möchten Sie den Edonkey-Verkehr unterbinden. Am einfachsten ist das, wenn Ihre Firewall grundsätzlich alles verbietet und nur bestimmte Protokolle erlaubt. Edonkey ist dann einfach nicht dabei.

Vielleicht müssen Sie aber die Firewall für eine Universität implementieren. Hier wird häufig bewusst ein anderer Ansatz gewählt. Um die freie Forschung nicht zu behindern, wird alles erlaubt und werden nur bestimmte Protokolle unterbunden.

Um Edonkey zu verhindern, können Sie den Zugriff auf die Ports unterbinden:

```
$IPTABLES -A FORWARD  -p tcp -m multiport --dport 4661,4662 -j REJECT
$IPTABLES -A FORWARD  -p udp -m multiport --dport 4665,4672 -j REJECT
```

Es gibt jedoch auch noch zwei weitere mögliche Lösungen: L7-Filter (*http://l7-filter.sourceforge.net/*) und das Iptables-Modul *Iptables-p2p* (*http://community.sidestep.pt/~filipe/Iptables-p2p/*). Leider wird das Letztere seit September 2004 nicht mehr aktiv weiterentwickelt. Die aktuellste Version befindet sich im CVS. Diese Module versuchen, den Netzwerkverkehr durch eine Inhaltsanalyse zu erkennen. Während das Iptables-p2p-Modul nur Peer2Peer-Verkehr erkennen kann (FastTrack, eDonkey, Gnutella, BitTorrent und OpenFT), erkennt L7-Filter bereits eine Vielzahl von Protokollen und wird aktiv weitergepflegt.

Der Vorteil dieser Module ist, dass sie das P2P-Protokoll unabhängig von dem verwendeten Port erkennen. So kann der P2P-Verkehr auch bei Modifikation der

Ports noch sicher erkannt werden. Um Edonkey-Verbindungen mit dem Iptables-p2p-Modul zu verhindern, müssen Sie Ihren Kernel entsprechend patchen und die folgenden Befehle in Ihrem Skript eintragen:

```
$IPTABLES -A FORWARD -m p2p --p2p-protocol edonkey -j REJECT
```

Tipp

Dieses Modul kann auch sehr gut genutzt werden, um den Verkehr zu erkennen, zu markieren und anschließend zu priorisieren. So kann die Bandbreite, die der P2P-Verkehr einnimmt, beschränkt werden.

Hinweis

Der Versuch, das Modul auf einer Fedora Core-4-Distribution zu übersetzen, schlug fehl. Dieses Modul kann wahrscheinlich nur auf älteren Distributionen, die die Iptables-Version 1.2.9 verwenden, eingesetzt werden.

32.8 P2P: KaZaA

Kazaa ist ebenfalls wie Edonkey ein P2P-Filesharing-Protokoll. Auch hier gibt es grundsätzlich zwei Zielsetzungen: erlauben oder verbieten. Während es bei Edonkey relativ leicht war, den Verkehr zu verbieten, ist dies bei KaZaA wesentlich schwieriger. KaZaA benutzt den Standardport 1214/tcp. Dieser Port kann jedoch auch frei gewählt werden. Für eine volle Funktionalität muss dieser Port auf dem Client auch von außen erreichbar sein. Verhindert die Firewall den Zugriff auf diesen Port, kann KaZaA auch den Port 80 verwenden. Dies ist sogar bei den aktuellen KaZaA-Clients die Default-Einstellung. Eine Unterdrückung dieses Ports wird jedoch in den meisten Netzwerken nicht möglich sein. KaZaA kann sogar über einen Proxy arbeiten!

32.8.1 Iptables-Regeln

Um die volle KaZaA-Funktionalität mit dem Standardport zu erhalten, können Sie die folgenden Regeln verwenden:

```
KAZAA_PORT=1214
KAZAA_CLIENT=192.168.0.5
```

```
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -s $KAZAA_CLIENT -p tcp --dport $KAZAA_PORT ↵
   -m state --state NEW -j ACCEPT
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tcp --dport $KAZAA_PORT -j DNAT ↵
  --to-destination $KAZAA_CLIENT
$IPTABLES -A FORWARD -i $EXTDEV -o $INTDEV -d $KAZAA_CLIENT -p tcp --dport $KAZAA_PORT ↵
  -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Wenn Sie den KaZaA-Verkehr unterbinden möchten, benötigen Sie eine intelligente Protokollerkennung. Hier können Sie dieselben Systeme einsetzen wie bei Edonkey. Zusätzlich gibt es für KaZaA, das das Fasttrack-Protokoll verwendet, noch die FT-wall von Chris Lowth (*http://www.lowth.com/p2pwall/ftwall/*). Außerdem können Sie versuchen, mit dem Iptables-`string`-Modul spezielle KaZaA-Pakete zu erkennen und die Verbindungen abzubrechen:

```
$IPTABLES -A FORWARD -p tcp -m string --string "X-Kazaa-Username:" -j REJECT
$IPTABLES -A FORWARD -p tcp -m string --string "X-Kazaa-Network:" -j REJECT
$IPTABLES -A FORWARD -p tcp -m string --string "X-Kazaa-IP:" -j REJECT
$IPTABLES -A FORWARD -p tcp -m string --string "X-Kazaa-SupernodeIP:" -j REJECT
```

Mit dem `iptables-p2p`-Modul könnten Sie die folgende Regel verwenden:

```
$IPTABLES -A FORWARD -m p2p --p2p-protocol fasttrack -j REJECT
```

Außerdem gibt es noch das `ipp2p`-Modul aus Patch-O-Matic. Dieses Modul erlaubt ebenfalls den Test des Verkehrs:

```
iptables -A FORWARD -m ipp2p --edk --kazaa --bit -j DROP
iptables -A FORWARD -p tcp -m ipp2p --ares -j DROP
iptables -A FORWARD -p udp -m ipp2p --kazaa -j DROP
```

Dieses Modul aus Patch-O-Matic ist in der Lage die folgenden Protokolle (teilweise) zu erkennen: eDonkey/eMule, KaZaA, Gnutella, Direct Connect, BitTorrent, AppleJuice, SoulSeek, WinMX und Ares/AresLite.

32.9 P2P: BitTorrent

BitTorrent beschreibt sich selbst als ein Werkzeug zur freien Meinungsäußerung. Es handelt sich auch um ein Filesharing-System, das aber nicht mit dem Ziel geschaffen wurde, urheberrechtlich geschützte Dateien zu tauschen. BitTorrent wurde geschaffen, um Firmen und Personen, die interessante Dateien anzubieten haben, eine optimale Download-Plattform zu bieten. Wenn eine Firma eine neue Demodatei eines Spiels anbieten möchte, wird die Download-Rate rapide in die Höhe schnellen. Die Anwender müssen sich mit langsameren Downloads zufrieden geben, und die Firma muss die hohen Kosten für die Übertragung tragen. BitTorrent löst das Problem, indem die Anwender, die die Datei gerade herunterladen, wieder

anderen Anwendern als Download-Plattform zur Verfügung stehen. Dadurch wird die maximale Download-Geschwindigkeit vervielfacht. Dieser verteilte gemeinsame Download ist das Geheimnis des Erfolges von BitTorrent. Diese Plattform wird von immer mehr Firmen (zum Beispiel auch Red Hat) genutzt, um große Datenmengen (zum Beispiel CD-ISO-Abbilder) schnell und preiswert zur Verfügung zu stellen.

Das BitTorrent-Protokoll verwendet die TCP-Ports 6969 und 6881-6889. Um die volle Funktionalität und hohe Download-Geschwindigkeiten zu erreichen, muss der Client auf diesen Ports auch von außen erreichbar sein. Dieses Modell kennen Sie schon von anderen P2P-Protokollen.

32.9.1 Iptables-Regeln

Wenn Sie den BitTorrent-Verkehr durch Ihre Firewall für einen Client erlauben möchten, können Sie die folgenden Regeln verwenden:

```
# Client-Zugriff auf den Server
BITT_CLIENT=192.168.0.5
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -s $BITT_CLIENT -p tcp --dport 6969 ↵
  -m state --state -NEW -j ACCEPT
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -s $EDONKEY_CLIENT -p tcp --dport 6881:6889 ↵
  -m state --state -NEW -j ACCEPT

# Zugriff auf den Client
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tcp --dport 6881:6889 -j DNAT ↵
  --to-destination $BITT_CLIENT
$IPTABLES -t nat -A PREROUTING -i $EXTDEV -p tdp --dport 6969 -j DNAT ↵
  --to-destination $BITT_CLIENT
$IPTABLES -A FORWARD -i $EXTDEV -o $INTDEV -d $BITT_CLIENT -p tcp --dport 6881:6889 ↵
  -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -i $EXTDEV -o $INTDEV -d $BITT_CLIENT -p tcp --dport 6969 ↵
  -m state --state NEW -j ACCEPT

$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Wenn Sie den Zugriff verhindern möchten, ist es am sinnvollsten, grundsätzlich nur bestimmte Protokolle zu erlauben und BitTorrent nicht mit aufzunehmen. Sollten Sie sich in der Lage befinden, dass Sie grundsätzlich alles erlauben, aber nur BitTorrent unterbinden möchten, so können Sie die Ports 6881-6889 in Ihrer Firewall schließen. Jedoch kann dieser Portbereich beliebig eingestellt werden. Sinnvoller ist auch hier der Einsatz eines intelligenten Protokollerkennungswerkzeugs. Dies kann `iptables-p2p` (siehe Abschnitt 32.7) sein oder das L7-Filter-Modul. Das Letztere wird in einem eigenen Kapitel besprochen. Das Erstere kann sehr einfach eingesetzt werden:

```
$IPTABLES -A FORWARD -m p2p --p2p-protocol bittorrent -j REJECT
```

32.10 FTP

Das File Transfer Protocol ist eines der ältesten Applikationsprotokolle, die heute noch im Einsatz sind. Es wurde 1973 entwickelt und als RFC veröffentlicht. Nur zum Vergleich: Ethernet wurde 1974 und UUCP 1978 entwickelt. Das Internetprotokoll IP hat erst 1980 das Network Control Protocol (NCP) abgelöst.

Dennoch ist FTP eines der kompliziertesten Protokolle. Es verlangt zu Beginn eine Authentifizierung und überträgt sämtliche Informationen im Klartext. Auch der Benutzername und das Kennwort werden ungeschützt übertragen.

Achtung

Es existieren kerberosierte Versionen, die einen Single-Sign-On ermöglichen und auch anschließend sämtliche Daten bei der Übertragung schützen. Außerdem bietet die SSH häufig einen SFTP-Zugang an. Dies ist ein geschützter FTP-ähnlicher Zugang zum Dateitransfer.

32.10.1 Das FTP-Protokoll

Das FTP-Protokoll ist deswegen so kompliziert, weil die Anmeldeinformationen und die Befehle von dem FTP-Client zum Server über die Steuerungsverbindung übertragen werden, während alle Daten, die der Server an den Client übermittelt, über eigene separate Datenverbindungen transportiert werden.

Die Steuerungsverbindung (Control Connection) wird von dem Client zum Server auf dem Port 21/tcp aufgebaut. Der Client verwendet für den Aufbau einen beliebigen Port > 1023. Diese Verbindungen werden genutzt, um alle Anmeldeinformationen zu übertragen und die Befehle des Clients an den Server zu übertragen. Dateien werden über eigene Datenverbindungen übertragen. Dies trifft auch schon auf die Inhaltsangabe eines Verzeichnisses beim Befehl `ls` bzw. `dir` zu. Ebenso ist dies unabhängig von der Richtung des Transfers. Sowohl der `PUT`- als auch der `GET`-Befehl triggert eine Datenverbindung.

Für den Aufbau dieser Datenverbindungen gibt es grundsätzlich zwei Möglichkeiten. Bei dem aktiven FTP baut der Server diese Datenverbindungen auf. Dazu übermittelt der Client dem Server in einem `PORT`-Kommando die IP-Adresse und den Port, auf dem er die Verbindung des Servers entgegennimmt. Der Server baut dann von dem Port 20/tcp (ftp-data) die Verbindung zu dem Port auf, den er von dem Client erhalten hat (Abbildung 32.3). Für jede zu transportierende Datei wird eine neue Datenverbindung geöffnet. Die Verbindung wird nach dem Transport nicht für zukünftige Dateien offen gehalten.

Bei dem passiven FTP sendet der Client ein `PASV`-Kommando über die Steuerungsverbindung an den Server. Der Server antwortet mit einer IP-Adresse und einer

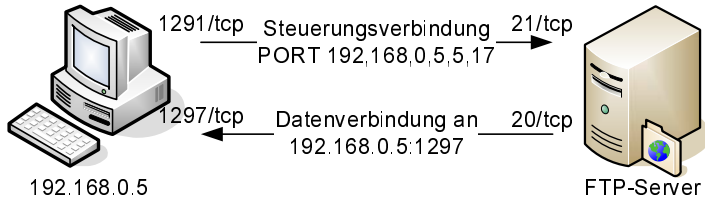


Abbildung 32.3: Der Server baut bei aktivem FTP die Datenverbindung auf.

Portnummer, auf der er den Aufbau der Datenverbindung erwartet. Hier verwendet der Server einen TCP-Port > 1023!

Achtung

Der FTP-Server kann als Antwort auf ein `PASV`-Kommando eine andere IP-Adresse zurückliefern, als er für die Steuerungsverbindung verwendet!

Der Client baut nun die Verbindung von einem beliebigen TCP-Port > 1023 zum angegebenen Port des FTP-Servers auf (Abbildung 32.4).

Für den Administrator einer Firewall stellen sich nun mehrere Probleme. Stellen wir uns vor, Sie möchten den FTP-Client mit Ihrer Firewall schützen. Dies ist sicherlich der Standardfall.

Sie werden mit folgenden Problemen konfrontiert:

- Das FTP-Protokoll baut eine Vielzahl von Verbindungen auf.
- Einige der verwendeten Zielports und -adressen werden dynamisch während der Verbindung ausgehandelt und stehen nicht zu Beginn bereits fest! Eine Berücksichtigung in statischen Regeln ist nicht möglich.

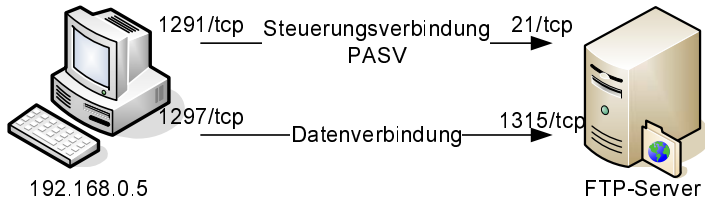


Abbildung 32.4: Der Server baut bei aktivem FTP die Datenverbindung auf.

- Bei dem aktiven FTP müssen Sie Verbindungen von dem Server zu Ihrem geschützten FTP-Client durch die Firewall erlauben. Dabei kennen Sie den Zielport der Verbindung nicht. Es handelt sich um einen beliebigen Port > 1023.
- Bei dem passiven FTP ist es nicht ganz so schlimm. Dennoch müssen Sie beliebige Verbindungen von Ihrem Client zum Server unter Verwendung beliebiger Ports > 1023 erlauben. Achtung, auch KaZaA, eDonkey etc. verwenden diese Ports.
- Da Ihr Firewall-Skript nicht in der Lage ist, einen Zusammenhang zwischen den Steuerungsverbindungen und den Datenverbindungen zu erstellen, müssen Sie in Ihrem Skript sogar die Datenverbindungen erlauben, wenn gar keine Steuerungsverbindung existiert. Schlimmer noch, Sie müssen die Datenverbindungen von und zu beliebigen Servern und Clients erlauben!

Um diese Probleme zu beseitigen, wurde die Stateful Inspection entwickelt.

32.10.2 Die Stateful Inspection des FTP-Protokolls

Die Stateful Inspection des FTP-Protokolls wurde ursprünglich in kommerziellen Firewalls entwickelt. Sie wird inzwischen auch von Linux unterstützt. Hierbei passiert nun Folgendes: Sobald der Linux-Kernel erkennt, dass eine FTP-Steuerungsverbindung durch die Firewall erlaubt wurde, betrachtet er jedes Paket dieser Verbindung. Dabei achtet er speziell auf das `PORT`- und das `PASV`-Kommando. Sobald der Kernel eines dieser Kommandos erkennt, trägt er die resultierende Verbindung selbstständig und automatisch in der Zustandstabelle (Connection Tracking Table) ein. Die Stateful Inspection erfordert auch den Einsatz des Connnection Tracking. Diese Verbindung und alle zu ihr gehörenden Pakete erhalten nun den Zustand `RELATED`, da sie mit einer anderen Verbindung (der Steuerungsverbindung) verwandt sind[1]. Um nun die Stateful Inspection für das FTP-Protokoll in Ihrer Linux-Firewall anzuschalten, genügt es, das entsprechende Kernelmodul `ip_conntrack_ftp` zu laden. Dieses Modul erkennt automatisch die FTP-Steuerungsverbindung und beobachtet die transportierten FTP-Befehle. Es unterstützt sowohl aktives als auch passives FTP. Die Erkennung erfolgt über den TCP-Zielport 21. Wenn Sie auf FTP-Server zugreifen wollen, die einen anderen Port für die Steuerungsverbindung verwenden beziehungsweise die aktive Datenverbindung von einer anderen IP-Adresse aufbauen, müssen Sie dieses Modul beim Laden mit dem Befehl `modprobe` auch noch konfigurieren.

Der Befehl `modinfo` zeigt Ihnen die Möglichkeiten des Moduls `ip_conntrack_ftp`:

```
    [root@bibo ~]# modinfo ip_conntrack_ftp
filename:       /lib/modules/2.6.12-1.1390_FC4/kernel/net/ipv4/netfilter/ip_conntrack_ftp.ko
license:        GPL
author:         Rusty Russell <rusty@rustcorp.com.au>
description:    ftp connection tracking helper
```

[1] Diese verwandten Verbindungen werden auch Expectation genannt, da es sich um erwartete Verbindungen handelt.

```
parmtype:       ports:array of int
parmtype:       loose:int
vermagic:       2.6.12-1.1390_FC4 686 REGPARM 4KSTACKS gcc-4.0
depends:        ip_conntrack
srcversion:     7A102256C83E32975182EEF
```

Fett hervorgehoben sind die Parameter, die beim Laden des Moduls mit angegeben werden können. Wenn Sie zum Beispiel auf einen FTP-Server zugreifen möchten, der auf dem Port 2121 seine Dienste anbietet, so sollten Sie das Modul mit folgendem Befehl in Ihrem Skript laden:

```
MODPROBE=/sbin/modprobe
$MODPROBE ip_conntrack_ftp ports=21,2121
```

Vergessen Sie bitte nicht, auch den Port 21 anzugeben. Ansonsten können Sie nicht mehr mit regulären FTP-Servern kommunizieren. Sie können maximal 8 Ports angeben.

Die Option `loose=1` erlaubt es, mit FTP-Servern zu kommunzieren oder FTP-Server zu betreiben, die für die Datenverbindung eine andere IP-Adresse verwenden als für die Steuerungsverbindung. Normalerweise ist dieser Parameter jedoch nicht erforderlich. Wenn Sie aber zu einem bestimmten FTP-Server absolut keine Verbindung aufbauen können, lohnt es sich, den Parameter auszuprobieren. Leider ist es nicht möglich, diesen Parameter nur für eine bestimmte IP-Adresse anzuschalten.

Befindet sich der Client oder der FTP-Server hinter einer Firewall, die gleichzeitig auch noch eine Network Address Translation (NAT) durchführt, dann müssen die Datenverbindungen auch noch korrekt genattet werden. Hierzu gibt es ein weiteres Kernelmodul, das die korrekte Adressumsetzung garantiert. Auch dieses Modul, `ip_nat_ftp`, müssen Sie selbst laden, wenn Sie die Funktionalität wünschen. Es wird nicht automatisch von dem Kernel geladen.

```
$MODPROBE ip_nat_ftp ports=21,2121
```

Sie müssen bei diesem Modul genauso wie beim `ip_conntrack_ftp`-Modul die zu überwachenden Ports angegeben. Erst ab Kernel 2.6.11 fällt diese Anforderung weg und das Modul liest die Ports aus dem `ip_conntrack_ftp`-Modul aus.

32.10.3 Iptables-Regeln

Bei Anwendung der Stateful Inspection sind die Regeln nun sehr einfach. Zunächst betrachten wir die Regeln für eine Firewall, die Clients den Aufbau einer FTP-Verbindung erlaubt.

```
$MODPROBE ip_conntrack_ftp   # Aktiviert die Stateful Inspection
$MODPROBE ip_nat_ftp         # Nur bei NAT
```

```
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p tcp --dport 21 -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Einige Leser werden sich wahrscheinlich verwundert die Augen reiben. Nach den komplizierten Ausführungen über das FTP-Protokoll, sollen die Regeln nun so einfach sein? Nun, das ganze Geheimnis liegt in dem Modul `ip_conntrack_ftp`. Durch das Laden des Moduls aktivieren Sie die Stateful Inspection für das FTP-Protokoll. Alle Datenverbindungen werden erkannt und mit dem Zustand `RELATED` in der Verbindungstabelle eingetragen. Die zweite Regel akzeptiert alle Verbindungen mit diesem Zustand. Sie müssen sich als Firewall-Administrator nicht mehr mit aktivem oder passivem FTP herumschlagen. Darum kümmert sich nun Ihre Firewall. Dabei ist diese Behandlung auch besonders sicher, da nun nur dann eine Datenverbindung erlaubt wird, wenn diese zuvor durch eine Steuerungsverbindung angefordert wurde. Obwohl für FTP-Datenverbindungen nun die Ports > 1023 geöffnet sind, können Anwendungen wie KaZaA oder eDonkey diese nicht nutzen. Sie müssten zunächst eine FTP-Steuerungsverbindung etablieren.

Achtung

Sie sollten zusätzlich auch folgende Regel auf Ihrer Firewall eintragen:

```
$IPTABLES -A INPUT -p tcp --dport 113 -j REJECT
```

Viele FTP-Server (besonders auf dem Betriebssystem Unix) bauen bei einer FTP-Verbindung eine identd-Verbindung zum Client auf. Wenn Sie diese Verbindung auf Ihrer Firewall nur verwerfen (DROP), kommt es zu einer Verzögerung bei Ihrem Verbindungsaufbau. Lehnen Sie die Verbindung hingegen ab, erkennt der Server, dass kein Aufbau möglich ist, und fährt mit Ihrer Anmeldung fort.

Weitere Dienste, die dieses Verhalten zeigen, sind SMTP-Server und IRC-Server.

Das Laden des `ip_nat_ftp`-Moduls ist nur erforderlich, wenn Sie auf Ihrer Firewall auch gleichzeitig ein NAT durchführen.

Wenn Sie einen FTP-Server mit einer lokalen Firewall schützen möchten, können Sie auch das recht einfach mit der Stateful Inspection erreichen. Hierzu verwenden Sie folgende Regeln:

```
$MODPROBE ip_conntrack_ftp   # Aktiviert die Stateful Inspection

$IPTABLES -A INPUT -p tcp --dport 21 -m state --state NEW -j ACCEPT
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

32.11 SNMP

Das Simple Network Management Protocol (SNMP) ist ein sehr einfaches Protokoll für die Überwachung und Verwaltung von Netzwerkkomponenten wie zum Beispiel Routern. Dieses Protokoll erlaubt das Auslesen von Leistungsdaten und die Konfiguration des Geräts. Da sensible Daten im Klartext übertragen werden, sollte das Protokoll nicht in ungeschützten Netzwerken eingesetzt werden. Meistens baut der Client (Manager) die Verbindung zum Server (Agent) auf. Jedoch kann auch der Agent sich in wichtigen Fällen beim Manager melden. Dies bezeichnet man als SNMP-Trap. Als Transportprotokoll verwendet SNMP das UDP-Protokoll. Während die normalen Abfragen an den UDP-Port 161 gesendet werden, werden SNMP-Traps an den UDP-Port 162 gesendet.

Bei gleichzeitiger Verwendung der Network Address Translation auf der Firewall gibt es jedoch Probleme, da die IP-Adresse des SNMP-Systems auch in dem Paket transportiert wird. NAT tauscht jedoch nur die Adresse in dem IP-Header aus. Wenn Sie auch einen Austausch der IP-Adresse in der SNMP-Payload des Pakets wünschen, müssen Sie ein NAT-Helfermodul laden:

```
$MODPROBE ip_nat_snmp_basic
```

Mit der Option `debug=1` können Sie zusätzliche Protokolleinträge bei der Arbeit des Moduls erhalten.

32.11.1 Iptables-Regeln

Die Regeln für SNMP sind sehr einfach. Wenn Ihr Network-Management-System durch eine Firewall geschützt ist, genügen die folgenden Regeln:

```
MANAGER=192.168.0.5
AGENT=192.168.0.6

# Erlaube SNMP-Zugriff
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -s $MANAGER -d $AGENT -p udp --dport 161 ↵
  -m state --state NEW -j ACCEPT

# Erlaube SNMP-Traps
$IPTABLES -A FORWARD -i $EXTDEV -o $INTDEV -s $AGENT -d $MANAGER -p udp --dport 162 ↵
  -j ACCEPT

$IPTABLES -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Wenn Sie auf Ihrer Firewall gleichzeitig Source-NAT verwenden, denken Sie daran, dass Sie für die SNMP-Traps ein Destination-NAT zu Ihrer Management-Station einrichten müssen. Sobald Sie SNAT oder DNAT einsetzen, sollten Sie zusätzlich das Modul `ip_nat_snmp_basic` laden. Dieses Modul ist bei allen aktuellen Linux-Distributionen enthalten.

32.12 Amanda

Der Advanced Maryland Automatic Network Disc Archiver (Amanda) ist ein Backup-System, mit dem automatisch verteilte Unix-Clients über ein Netzwerk auf einem zentralen Backup-Server gesichert werden können (*http://www.amanda.org*). Dieses System wird in vielen Umgebungen eingesetzt, da es unter der GPL veröffentlicht worden ist.

Amanda zeichnet sich dadurch aus, dass der Server sich bei Bedarf mit dem Client verbindet und ihn auffordert, jetzt seine Daten für die Sicherung bereitzustellen. So kommt es auf dem Server nicht zur Überlastung, und der Server kann auch die genutzte Netzwerkbandbreite regulieren.

32.12.1 Das Amanda-Protokoll

Amanda verwendet ein recht kompliziertes Protokoll für das Backup. Der Server verbindet sich über das UDP-Protokoll auf Port 10080 auf dem Client mit dem Amandad. Der Client forkt einen Amandad-Prozess, der sich anschließend mit einem vom Server bestimmten UDP-Port auf dem Server verbindet. Anschließend verbindet sich der Server wieder mit zwei oder drei TCP-Ports auf dem Client. Auch diese Ports werden zwischen dem Amanda-Client und dem Backup-Server ausgehandelt.

Die Dynamik der Ports ist für jeden Firewall-Administrator ein Gräuel. Sie können nicht in Ihrer Firewall feste Regeln für die Verbindung definieren. Das Amanda-Handbuch beschreibt in Kapitel 21, wie Sie die Ports auf einen bestimmten Bereich einschränken können (*http://www.amanda.org/docs/portusage.html*). Dies ist aber auch keine richtige Lösung.

32.12.2 Iptables-Regeln

Eine richtige Filterung des Amanda-Netzwerkverkehrs ist nur unter Anwendung der Stateful Inspection möglich. Diese wurde bereits im Kapitel zu FTP (siehe Abschnitt 32.10) als auch in Kapitel 19 besprochen. Auch für Amanda gibt es zwei Kernel-Module, die die einfache Filterung des Protokolls erlauben:

```
$MODPROBE ip_conntrack_amanda
$MODPROBE ip_nat_amanda
```

Das Modul `ip_conntrack_amanda` verfügt über die Option `master_timeout`. Hiermit können Sie den Timeout für die Zustandsüberwachung der Master-Verbindung auf Port 10080 einstellen. Der übliche Timeout für die Master-Verbindungen beträgt 300 Sekunden und ist häufig zu kurz. Dies ist aber bereits mehr, als üblicherweise von Iptables für UDP-Verbindungen genutzt wird (180 Sekunden). Sie können hier aber auch eine Stunde angeben:

```
$MODPROBE ip_conntrack_amanda master_timeout=3600
```

Die weiteren Regeln gestalten sich dann sehr einfach:

```
AM_SERVER=192.168.0.5
AM_CLIENTS=192.168.1.0/24

$IPTABLES -A FORWARD -s $AM_SERVER -d $AM_CLIENTS -p udp --dport 10080 -m state ↵
  --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Wenn Sie eine lokale Firewall auf dem Amanda-Server betreiben möchten, können Sie folgenden Regelsatz verwenden:

```
$MODPROBE ip_conntrack_amanda master_timeout=3600
$MODPROBE ip_nat_amanda

AM_CLIENTS=192.168.1.0/24

$IPTABLES -A OUTPUT -d $AM_CLIENTS -p udp --dport 10080 -m state --state NEW -j ACCEPT
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

32.13 PPTP

Das PPTP-Protokoll wird häufig für den Aufbau von Einwahl- und VPN-Verbindungen genutzt. Es verwendet einen Steuerungskanal auf dem TCP-Port 1723 und einen Datenkanal, der das GRE-Protokoll (IP-Protokoll 47) nutzt. Dabei erlaubt das PPTP-Protokoll die Zuweisung von IP-Adresse, Netzmaske, Route, DNS- und WINS-Servern.

Grundsätzlich ist die Konfiguration einer Firewall für die Anwendung des PPTP-Protokolls sehr einfach. Schwierig wird die gesamte Konstruktion nur bei gleichzeitiger Anwendung der Network Address Translation (NAT). Sobald Sie eine Firewall einsetzen, die ein Source-NAT für die dahinter befindlichen Clients durchführt, und gleichzeitig zwei oder mehr Clients mit dem PPTP-Protokoll auf einen Server zugreifen möchten, werden beide Verbindungen nicht mehr richtig funktionieren. Dieser Fall ist, nebenbei bemerkt, sehr häufig. In jedem WLAN-Hotspot im Hotel und Flughafen kommt es regelmäßig zu diesem Szenario.

Warum ist Source-NAT kritisch? Die Firewall muss sich bei einem Source-NAT merken, welcher Client die Verbindung aufgebaut hat, um anschließend die Antwort-Pakete der Verbindung auch an den richtigen Client zurückzusenden. Hierzu pflegt die Firewall eine Tabelle, in der alle genatteten Verbindungen eingetragen werden[2]. Sobald ein Paket zurückkommt, schaut die Firewall in die Tabelle, um nachzusehen, an welchen Client das Paket intern weiterzusenden ist. Hierbei verwendet die Firewall als Kriterium das IP-Protokoll, die Zieladresse und den Zielport des Pakets.

[2] Bei Linux ist dies auch die Connection-Tracking-Tabelle.

Leider besitzt das GRE-Protokoll keine Ports. Daher bleiben als Unterscheidungsmerkmale nur das IP-Protokoll (immer GRE) und die Zieladresse (immer die der Firewall). Sobald also zwei GRE-Verbindungen gleichzeitig genattet werden müssen, kann die Firewall die Pakete nicht mehr auseinander halten und weist sie immer der zuletzt aktiven Verbindung zu.

Dieses Problem lässt sich mit der Stateful Inspection lösen.

32.13.1 Iptables-Regeln

Die Iptables-Regeln sind recht einfach. Möchten Sie mit Ihrer Firewall einen Client beim Zugriff auf einen PPTP-Server im Internet schützen, so können Sie folgende Regeln verwenden:

```
PPTP_SRV=5.0.0.1
GRE=47

$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p tcp --dport 1723 -d $PPTP_SRV -m state ↵
  --state NEW -j ACCEPT
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p $GRE -m state -d $PPTP_SRV --state NEW ↵
  -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Falls Sie nur die zweite GRE-Verbindung erlauben wollen, wenn diese durch die erste Verbindung angefordert wurde, können Sie die Stateful Inspection nutzen. Leider sind die erforderlichen Kernelmodule nicht bei allen Distributionen enthalten. Dann müssen Sie Ihren Kernel bis einschließlich 2.6.13 selbst patchen und übersetzen (siehe Kapitel 18).

Achtung

Dieses Modul hat momentan noch einige Einschränkungen: Es funktioniert nicht mit den Linux-Kerneln zwischen 2.6.10 und 2.6.13. Ab 2.6.14 ist es im Kernel enthalten! Außerdem ist auch eine Neukompilierung des Kommandos `iptables` erforderlich.

Sie benötigen die folgenden Module:

```
$MODPROBE ip_conntrack_proto_gre
$MODPROBE ip_conntrack_pptp
```

Dann genügen die folgende Firewall-Regeln:

```
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p tcp --dport 1723 -d $PPTP_SRV -m state ↵
  --state NEW -j ACCEPT
```

```
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Sobald die PPTP-Steuerungsverbindung erkannt wurde, wird die entsprechende GRE-Verbindung im Zustand `RELATED` erlaubt.

Sobald nun aber mehrere Clients mit dem PPTP-Protokoll gleichzeitig zugreifen möchten, wird die Verbindung wieder fehlschlagen. Hier hilft ein NAT-Helper-Modul, das ebenfalls nicht in allen Distributionen enthalten ist. Mit dem obigen Patch stehen diese Module aber zur Verfügung.

```
$MODPROBE ip_nat_proto_gre
$MODPROBE ip_nat_pptp
```

Natürlich kann es auch sein, dass Sie einen PPTP-Server in Ihrer DMZ betreiben möchten. Dann benötigen Sie die folgenden Regeln:

```
PPTP_SRV=192.168.0.5
GRE=47

$IPTABLES -t nat -A PREROUTING -p tcp --dport 1723 -j DNAT --to-destination $PPTP_SRV
$IPTABLES -t nat -A PREROUTING -p $GRE -j DNAT --to-destination $PPTP_SRV

$IPTABLES -A FORWARD -d $PPTP_SRV -p tcp --dport 1723 -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -d $PPTP_SRV -p $GRE -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Die ersten beiden DNAT-Regeln sorgen dafür, dass der PPTP-Verkehr, der von außen die Firewall erreicht, an den PPTP-Server weitergereicht wird.

32.14 SMTP

Das Simple Mail Transport Protocol wird für den Transport von E-Mail zwischen den E-Mail-Servern im Internet genutzt. Auch E-Mail-Clients wie Evolution, Kontact und Outlook nutzen dieses Protokoll für den Versand von E-Mail.

32.14.1 Das SMTP-Protokoll

Das SMTP-Protokoll ist ein Klartextprotokoll und verwendet Befehle, die vier Buchstaben lang sind. Im Folgenden ist eine Beispielsitzung abgedruckt. Sie können das SMTP-Protokoll mit einem Telnet-Client und ein wenig Wissen um die Befehle leicht selbst testen.

```
[root@bibo ~]# telnet mail.spenneberg.net 25
Trying 217.160.128.61...
Connected to mail.spenneberg.net (217.160.128.61).
Escape character is '^]'.
220 mail.spenneberg.net ESMTP Postfix
```

```
helo linuxclient.spenneberg.net  (1)
250 mail.spenneberg.net
mail from: ralf@gmx.de   (2)
250 Ok
rcpt to:ralf@spenneberg.net   (3)
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: SMTP-Test  (4)
From: Ich bins <ralf@gmx.de>
To: Ralf

Test   (5)
.    (6)
250 Ok: queued as 556B857AAA
quit
221 Bye
Connection closed by foreign host.
```

Zunächst begrüßt der Client den Server und stellt sich selbst vor (1). Anschließend nennt der Client die Envelope-Absenderadresse (2). Dies ist vergleichbar mit der Adresse außen auf einem Briefumschlag. Dann gibt er den Envelope-Empfänger an (3). Es folgt der Inhalt der E-Mail (Inhalt des Briefumschlages). Dort gibt der Client im Header einen Betreff, den Absender und den Empfänger an. Diese Angaben sind optional und können auch weggelassen werden. Das Verhalten des Mailservers bei fehlenden Angaben ist von dem Produkt abhängig und kann nicht allgemein gültig angegeben werden. Abgetrennt durch eine Leerzeile folgt dann der tatsächliche Inhalt der E-Mail (5). Die Eingabe wird durch einen Punkt auf einer ansonsten leeren Zeile beendet (6). Der Client beendet die Verbindung mit `quit`.

Das SMTP-Protokoll überträgt normalerweise sämtliche Informationen im Klartext. Jedoch gibt es mit SMTP über SSL (smtps, Port 465) auch die Möglichkeit, SMTP über die Secure Socket Layer zu verwenden. Dies hat sich jedoch nicht durchgesetzt. Heute beherrschen fast alle Mailserver als Alternative die Transport Layer Security (TLS). Nachdem das Kommando `STARTTLS` auf dem unverschlüsselten Wege übertragen wurde, handeln der Client und der Server innerhalb der bestehenden Verbindung eine TLS-Verbindung aus. Die Verbindung wird nicht unterbrochen oder auf einem anderen Port geöffnet. Es genügt der Standardport 25/tcp hierfür.

32.14.2 Iptables-Regeln

Die Behandlung des SMTP-Protokolls in einer Firewall ist sehr einfach. Da das Protokoll wie Telnet, HTTP und SSH nur einen einzigen Port verwendet, genügt eine Zeile, um das Protokoll über eine Firewall zu erlauben.

```
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p tcp --dport 25 -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Achtung

Sie sollten zusätzlich auf Ihrer Firewall Identd-Anfragen ablehnen. Ansonsten kann es beim Aufbau einer SMTP-Verbindung zu Verzögerungen kommen, da einige SMTP-Server bei einer Verbindungsanfrage zunächst eine Identd-Verbindung zum Client aufbauen und erst anschließend fortfahren. Erhalten sie eine Fehlermeldung, fahren sie ebenfalls sofort fort.

```
$IPTABLES -A INPUT -i $EXTDEV -p tcp --dport 113 -j REJECT
```

Wenn Sie einen Mailserver direkt mit einer lokalen Firewall schützen möchten, können Sie die folgenden Regeln einsetzen:

```
$IPTABLES -A INPUT -p tcp --dport 25 -m state --state NEW -j ACCEPT
$IPTABLES -A OUTPUT -p tcp --dport 25 -m state --state NEW -j ACCEPT
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Achtung

Ein E-Mail-Server benötigt zusätzlich auch noch Zugang zu DNS-Diensten. Denken Sie daran, ihm auch diesen Zugriff zu gestatten!

```
$IPTABLES -A OUTPUT -p tcp --dport 53 -m state --state NEW -j ACCEPT
$IPTABLES -A OUTPUT -p udp --dport 53 -m state --state NEW -j ACCEPT
```

Weitere Beispiele für die Konfiguration einer Firewall bei Einsatz eines E-Mail-Servers in einer DMZ finden Sie im Kapitel 9.

32.15 IRC

Das Protokoll Internet Relay Chat ist ein Kommunikationsmedium, das es ermöglicht, weltweit mit anderen Benutzern textgestützt in Echtzeit zu kommunizieren. Realisiert wird es von einem verteilten Netzwerk aus miteinander vernetzten Servern. Dabei erfolgt die Kommunikation in thematisch organisierten Chaträumen, so genannten Channels. Die Channels tragen Namen wie #Linux oder #VPn. Bei den größeren Channels sind mehrere tausend Benutzer gleichzeitig angemeldet. Die Anfänge gehen auf das BITNET zurück, für das das Relay-Chat-Protokoll entwickelt wurde. Dieses wurde 1988 auf das Internet übertragen. Auf Grund von organisatorischen Problemen entstanden ab 1993 mehrere unabhängige Netzwerke. 1996 erfolgte die Aufspaltung in zwei große Netze, die heute unter den Namen IRCNet und EFnet wiederzufinden sind. Auf Grund der besonderen Struktur genügt es,

wenn der Client Zugang zu einem Server dieser Netzwerke hat, um an sämtlichen Chaträumen teilzunehmen. Weitere heute übliche Netze sind QuakeNet, Undernet, DALnet, Freenode etc.

Das IRC-Protokoll erlaubt neben dem reinen Chat auch den Austausch von Dateien über eigene dedizierte Verbindungen (ähnlich den Datenverbindungen bei FTP). Diese Verbindungen werden Direct-Client-to-Client-Verbindung (DCC) genannt. Die für diese Verbindungen verwendeten Ports werden von dem Client und Server dynamisch ausgehandelt. Um diese Verbindungen sicher zuzulassen, bietet der Linux-Kernel ein Stateful-Inspection-Modul `ip_conntrack_irc` (siehe auch Abschnitt 32.10).

32.15.1 Iptables-Regeln

Die Iptables-Regeln für den IRC-Verkehr sind bei Anwendung der Stateful Inspection sehr einfach. Es genügt, das Modul zu laden und anschließend die Verbindung zum IRC-Server zuzulassen.

```
$MODPROBE ip_conntrack_irc ports=6667
$MODPROBE ip_nat_irc    # bei gleichzeitiger Anwendung von NAT

$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p tcp --dport 6667 -m state --state NEW ↵
  -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Das `ip_conntrack_irc`-Modul erkennt automatisch angekündigte DCC-Verbindungen und trägt diese mit dem Zustand `RELATED` in der Verbindungstabelle als Expectation ein. Diese Verbindung wird dann von der zweiten Regel auch erlaubt. Bei dem Laden des Moduls können Sie einige Werte als Parameter angeben. Zunächst ist dies der Port, auf dem der IRC-Server angesprochen wird: `ports=6667,6668`. Der Parameter `max_dcc_channels` gibt die maximale Anzahl gleichzeitiger DCC-Verbindungen an (Default 8). Der Parameter `dcc_timeout` definiert schließlich den Timeout für nicht beantwortete DCC-Verbindungen (Default 300 Sekunden).

32.16 TFTP

Das Trivial File Transfer Protocol hat mit dem FTP-Protokoll nur den Namen gemeinsam. Es verwendet das UDP-Protokoll und den Port 69. Außerdem kennt es keine Anmeldung. Es wird häufig eingesetzt, um auf Netzwerkkomponenten eine neue Firmware einzuspielen oder um Konfigurationseinstellungen zu laden. Auch das Preboot Execution Environment (PXE) verwendet TFTP.

Eine Implementierung des Protokolls in einer Firewall ist daher selten, aber soll trotzdem hier kurz vorgestellt werden, da es ebenfalls dynamisch zugewiesene Ports verwendet.

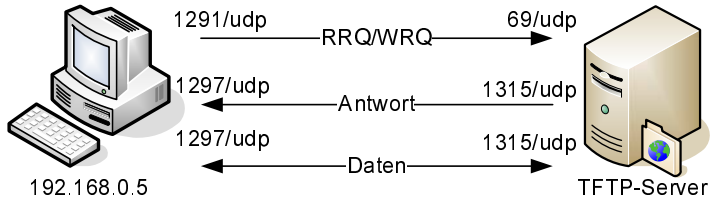


Abbildung 32.5: Das TFTP-Protokoll verwendet beliebige Ports.

Der Client sendet eine Anfrage (Request: RRQ/WRQ) an den Server auf Port 69. Der Client verwendet in seiner Anfrage einen beliebigen Port > 1023. Der Server antwortet und verwendet in seiner Antwort als Sourceport nicht 69, sondern ebenfalls einen Port > 1023. Die erste Antwort wird also bereits mit einem neuen Port gesendet. Der Client erkennt die Antwort lediglich an dem gleich gebliebenen Zielport. Die nun gewählten Ports bleiben für die gesamte Übertragung der Datei identisch (siehe Abbildung 32.5).

Eine Implementierung dieses Protokolls in einer Firewall ist nur möglich, wenn die Stateful Inspection dieses Protokoll unterstützt. Ansonsten müssen ernorme Löcher in der Firewall geöffnet werden, damit von einem beliebigen UDP-Port eine Verbindung zu einem beliebigen UDP-Port aufgebaut werden kann.

32.16.1 Iptables-Regeln

Erfreulicherweise unterstützen die meisten Distributionen in Ihrem Kernel bereits das `ip_conntrack_tftp`-Modul. Wenn dies bei Ihrer Distribution nicht der Fall ist, müssen Sie Ihren Kernel neu übersetzen.

Wenn Sie dieses Modul laden, können Sie analog dem FTP-Stateful-Inspection-Modul maximal acht Ports angeben, auf denen Sie eine Verbindung zu einem TFTP-Server aufbauen.

Wenn die Verbindung gleichzeitig genattet wird, müssen Sie auch das Modul `ip_nat_tftp` laden. Dieses Modul benötigt in einer älteren Ausgabe auch die Angabe der Ports. Das können Sie aber selbst prüfen:

```
[root@bibo ~]# modinfo ip_nat_tftp
filename:       /lib/modules/2.6.12-1.1390_FC4/kernel/net/ipv4/netfilter/ip_nat_tftp.ko
author:         Magnus Boden <mb@ozaba.mine.nu>
description:    tftp NAT helper
license:        GPL
vermagic:       2.6.12-1.1390_FC4 686 REGPARM 4KSTACKS gcc-4.0
depends:        ip_conntrack_tftp,ip_conntrack,iptable_nat
srcversion:     F97654AA2851F38C31D9F7B
```

Dieses Modul benötigt die Angabe nicht mehr. Nun können Sie mit der folgenden Regel TFTP-Verbindungen erlauben:

```
$MODPROBE ip_conntrack_tftp
```

```
$MODPROBE ip_nat_tftp   # bei SNAT oder DNAT

$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p udp --dport 69 -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

32.17 IMAP

Das Internet Message Access Protocol (IMAP, RFC 3501) erlaubt den Zugriff auf und die Verwaltung von E-Mails und Dateien auf dem Server. Im Gegensatz zum POP3-Protokoll verbleiben die E-Mails beim IMAP-Protokoll auf dem Server und werden nicht nach einem Download gelöscht. Dadurch können Sie mit mehreren Clients von unterschiedlichen Orten die E-Mails lesen und bearbeiten.

Der IMAP-Server verwendet zum Anbieten seines Dienstes den TCP-Port 143. Verbindungen auf diesem Port übertragen die Daten normalerweise unverschlüsselt. Lediglich die Authentifizierung kann verschlüsselt erfolgen. Allerdings kann auch das IMAP-Protokoll auf die Dienste des SSL-Protokolls zurückgreifen. Der IMAP-Server bietet dann IMAP-über-SSL-Verbindungen auf dem TCP-Port 993 an. Zusätzlich unterstützen moderne IMAP-Server die Transport Layer Security. Hier wird nach einem `STARTTLS`-Kommando die Verbindung auf dem Port 143/tcp verschlüsselt.

Achtung

Die Verwendung des `STARTTLS`-Kommandos und der TLS ist optional. Wenn Sie eine verschlüsselte Verbindung erzwingen möchten, müssen Sie auf SSL (Port 993/tcp) ausweichen.

Sie können das IMAP-Protokoll selbst mit einem Telnet-Client nachstellen:

```
[root@bibo ~]# telnet mail.spenneberg.net 143
Trying 217.160.128.61...
Connected to mail.spenneberg.net (217.160.128.61).
Escape character is '^]'.
* OK dovecot ready.
a001 LOGIN test test
a001 OK Logged in.
a142 SELECT INBOX
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags permitted.
* 0 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1122315709] UIDs valid
* OK [UIDNEXT 1] Predicted next UID
```

```
a142 OK [READ-WRITE] Select completed.
a752 close
a752 OK Close completed.
```

32.17.1 Iptables-Regeln

Die Iptables-Regeln sind angesichts des einfachen Protokolls sehr einfach. Zunächst die Regeln für ein Gateway:

```
IMAP_PORTS="143,993"

$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p tcp -m multiport --dport $IMAP_PORTS ↵
  -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Wenn Sie einen IMAP-Server mit einer lokalen Firewall schützen möchten, sehen die Regeln analog wie folgt aus:

```
IMAP_PORTS="143,993"

$IPTABLES -A INPUT -p tcp -m multiport --dport $IMAP_PORTS -m state --state NEW -j ACCEPT
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

32.18 POP3

Das Post Office Protocol 3 (RFC 1939) wird von einem E-Mail-Client verwendet, um E-Mails von einem Server abzuholen. Dazu werden die E-Mails anschließend üblicherweise auf dem Server gelöscht. Das ASCII-Protokoll verwendet zur Steuerung vier Buchstaben lange Befehle, die an den Server auf dem Port 110/tcp gesendet werden. Auch POP3 kann wie IMAP über eine SSL-gesicherte Verbindung genutzt werden. Dann verwendet der Server den TCP-Port 995.

Achtung

Das POP3-Protokoll überträgt sämtliche Daten unverschlüsselt. Lediglich die Anmeldung kann bei Unterstützung des `APOP`-Befehls verschlüsselt erfolgen. Leider unterstützen nur sehr wenige Anbieter den `APOP`-Befehl.

Sie können das POP3-Protokoll ganz einfach mit einem Telnet-Client testen:

```
[root@bibo ~]# telnet mail.spenneberg.net 110
Trying 217.160.128.61...
```

```
Connected to mail.spenneberg.net (217.160.128.61).
Escape character is '^]'.
+OK dovecot ready.
user test
+OK
pass test
+OK Logged in.
list
+OK 1 messages:
1 754
.
retr 1
+OK 754 octets
Return-Path: <root@bibo.spenneberg.de>
Received: from bibo.spenneberg.de (bibo.spenneberg.de [127.0.0.1])
        by bibo.spenneberg.de (8.13.4/8.13.4) with ESMTP id j6PIRfDM018622
        for <test@bibo.spenneberg.de>; Mon, 25 Jul 2005 20:27:41 +0200
... gelöscht ...

.
dele 1
+OK Marked to be deleted.
quit
+OK Logging out, messages deleted.
Connection closed by foreign host.
```

32.18.1 Iptables-Regeln

Die Iptables-Regeln für das POP3-Protokoll sind sehr einfach und entsprechen denen für das IMAP-Protokoll. Zunächst die Regeln für ein Gateway:

```
POP3_PORTS="110,995"

$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p tcp -m multiport --dport $POP3_PORTS ↵
  -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Wenn Sie einen POP3-Server mit einer lokalen Firewall schützen möchten, sehen die Regeln analog wie folgt aus:

```
POP3_PORTS="110,995"

$IPTABLES -A INPUT -p tcp -m multiport --dport $POP3_PORTS -m state --state NEW -j ACCEPT
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

32.19 NTP

Das Network Time Protocol (NTP) dient zur Synchronisation der Systemzeit mit einer oder mehreren zentralen Zeitquellen (RFC 2030). Das NTP-Protokoll unterstützt eine Authentifizierung des Servers, um Spoofing-Angriffen vorzubeugen. Leider bieten viele öffentliche NTP-Server diese Authentifizierung nicht an.

Das NTP-Protokoll verwendet den UDP-Port 123 für den Austausch der Informationen. Wenn NTP-Server untereinander miteinander kommunizieren, verwenden sie auch als Client den Port 123. Alle anderen Clients, die zur Synchronisation eingesetzt werden, verwenden einen UDP-Port > 1023.

32.19.1 Iptables-Regeln

Die Regeln für die Unterstützung des NTP-Protokolls sind recht einfach. Die folgenden Regeln erlauben das NTP-Protokoll durch ein Gateway:

```
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p udp --dport 123 -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

32.20 NNTP

Das Network News Transfer Protocol (NNTP, RFC 997) dient zum Transport von Nachrichten zu und von einem Newsserver. Das textbasierte Protokoll erlaubt das Auflisten der Newsgruppen, das Abfordern der vorhandenen Artikel und das Posten weiterer Artikel.

Das NNTP-Protokoll verwendet den TCP-Port 119. Um eine sichere und verschlüsselte Übertragung der Daten zu ermöglichen, bietet das NNTP-Protokoll eine Sicherung mit Secure Socket Layer (SSL). Hierzu wird der Port 563/tcp verwendet.

32.20.1 Iptables-Regeln

Die Iptables-Regeln für das NNTP-Protokoll sind sehr einfach und entsprechen denen für das IMAP-Protokoll. Zunächst die Regeln für ein Gateway:

```
NNTP_PORTS="119,563"

$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p tcp -m multiport --dport $NNTP_PORTS ↵
   -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Wenn Sie einen NNTP-Server mit einer lokalen Firewall schützen möchten, sehen die Regeln analog wie folgt aus:

```
NNTP_PORTS="119,563"
```

```
$IPTABLES -A INPUT -p tcp -m multiport --dport $NNTP_PORTS -m state --state NEW -j ACCEPT
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

32.21 H.323

Das H.323-Protokoll ist in Wirklichkeit ein ganzer Satz von Protokollen, die von Programmen wie Microsoft Netmeeting oder Gnomemeeting verwendet werden, um Audio- und Video-Informationen über das Internet zu transportieren. Einen Überblick über die beteiligten Protokolle und Standards erhält man auf *http://www.packetizer.com/voip/h323/standards.html*.

H.323 verwendet die folgenden Ports für seine unterschiedlichen Dienste:

Port	Beschreibung
389/tcp	Internet Locator Server
522/tcp	User Location Server
1503/tcp	T.120 Protocol
1720/tcp	H.323 (H.225 call setup)
1731/tcp	Audio Call Control
> 1023/tcp	H.245 Call Control
> 1023/udp	RTCP/RTP Streamin

Die Vielzahl der beteiligten Protokolle und die Verwendung von dynamischen Ports zeigt die Komplexität des Protokolls. Daher soll hier auf eine Beschreibung des Protokolls verzichtet werden. Interessierte Leser finden auf *http://www.packetizer.com/voip/h323/* ausführliche Informationen über das Protokoll.

32.21.1 Iptables-Regeln

Die Komplexität des Protokolls ist auf einer Firewall durch Einsatz der Stateful Inspection handhabbar. Erfreulicherweise gibt es sowohl für den Linux-Kernel 2.4 als auch den Linux-Kernel 2.6 im Iptables-Patch-O-Matic Kernel-Module, die dies unterstützen. Ob Ihre Distribution diese Module enthält, können Sie sehr leicht mit dem folgenden Befehl prüfen:

```
[root@bibo ~]# modinfo ip_conntrack_h323
modinfo: could not find module ip_conntrack_h323
```

In diesem Fall müssen Sie das Modul mit Patch-O-Matic in Ihrem Kernel einführen, aktivieren und übersetzen.

Achtung

Ab Version 2.6.11 wird ein neuer Patch benötigt.

Anschließend müssen Sie die Module laden und mindestens die Verbindung zum TCP-Port 1720 öffnen, um internen Clients die Verbindung mit Gegenstellen im Internet zu erlauben.

```
$MODPROBE ip_conntrack_h323
$MODPROBE ip_nat_h323

$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p tcp --dport 1720 -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Die Connection Tracking-Helper-Module erkennen dann die Verbindungen auf den dynamischen Ports und tragen diese im Zustand `RELATED` in der Zustandstabelle ein.

Tipp

Wenn Sie auch Verbindungen von außen entgegennehmen möchten, so ist ein DNAT des TCP-Ports 1720 nach innen erforderlich.

32.22 SIP

Das Session Initiation Protocol (SIP) wurde entwickelt, um allgemeine Sitzungen zwischen mehreren Clients auszuhandeln. Es wird im Moment in erster Linie für die Sprachübertragung über das Internet (VoIP, Voice over IP) verwendet. Für die Sprachübertragung verwendet das SIP-Protokoll zusätzlich das Real Time Transport Protocol (RTP). SIP handelt die Verbindung aus, und RTP überträgt tatsächlich die Sprachdaten.

Auf Grund der dynamischen Aushandlung der UDP-Ports für das RTP-Protokoll stellt SIP hohe Anforderungen an eine Firewall. Dies ist insbesondere der Fall, wenn auch NAT zum Zuge kommt, da auch in den Paketen die IP-Adressen der Clients transportiert werden. In der Vergangenheit wurden daher häufig für diesen Zweck SIP-Proxys eingesetzt.

32.22.1 Iptables-Regeln

Die Komplexität des Protokolls mit dynamisch ausgehandelten UDP-Ports verlangt für eine sichere Firewall-Implementierung die Unterstützung von Stateful Inspection. Da diese für den Linux-Kernel aber erst ab der Version 2.6.11 zur Verfügung steht, sollen hier zunächst die Regeln ohne Stateful Inspection für eine Firewall als Gateway vorgestellt werden.

```
# SIP verwendet den UDP-Port 5060
$IPTABLES  -A FORWARD -i $INTDEV -o $EXTDEV -p udp -m udp --dport 5060 -m state↵
  --state NEW -j ACCEPT

# RTP - the media stream
iptables -A FORWARD -i $INTDEV -o $EXTDEV -p udp -m udp --dport 10000:20000 -m state↵
  --state NEW -j ACCEPT -j ACCEPT

$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Falls Sie gleichzeitig auch NAT einsetzen, kann es in Abhängigkeit von dem Client aber wieder zu Problemen kommen.

Als Lösung können Sie den Kernel > 2.6.11 einsetzen. Dann gibt es im Patch-O-Matic Stateful-Inspection-Module für SIP, die Sie in Ihren Kernel patchen, aktivieren (`CONFIG_IP_NF_SIP`, `CONFIG_IP_NF_NAT_SIP`) und kompilieren können. Diese erkennen die dynamischen RTP-Verbindungen und führen ein korrektes NAT durch.

```
$MODPROBE ip_conntrack_sip
$MODPROBE ip_nat_sip

# SIP verwendet den UDP-Port 5060
$IPTABLES  -A FORWARD -i $INTDEV -o $EXTDEV -p udp -m udp --dport 5060 -m state↵
  --state NEW -j ACCEPT

$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

33 IPsec

Die Filterung von IPsec-Verbindungen ist bei jeder Firewall eine besondere Aufgabe. Unter Linux wird dies zusätzlich durch die unterschiedlichen Implementierungen und die vielen unterschiedlichen Patches kompliziert.

33.1 IPsec

Die IPsec-Protokolle werden verwendet, um Informationen über das Internet in geschützter Form zu transportieren. Sie schützen die Authentizität, Integrität und Vertraulichkeit der Pakete.

Dies wird mit drei verschiedenen Protokollen realisiert:

- **Authentication Header** (AH, IP-Protokoll 51). Dieses Protokoll kann die Authentizität und Integrität von Paketen garantieren. Dabei schließt die Garantie auch die unveränderlichen Bestandteile des äußeren IP-Headers mit ein. Eine nachträgliche Änderung dieser Bestandteile (z.B. NAT) wird von dem AH-Protokoll als Fehler erkannt, und das Paket wird verworfen.
- **Encapsulated Security Payload** (ESP, IP-Protokoll 50). Dieses Protokoll kann die Authentizität, Integrität und Vertraulichkeit von Paketen garantieren. Es schließt nicht den äußeren IP-Header in seine Überprüfung mit ein. Ein NAT erzeugt also kein ungültiges Paket. Daher wird heute häufig nur noch dieses Protokoll eingesetzt.
- **Internet Key Exchange** (IKE, 500/udp). Sowohl AH als auch ESP benötigen Schlüsselmaterial für die Realisierung ihrer Aufgaben. Das IKE-Protokoll authentifiziert die Kommunikationspartner und erzeugt dieses Schlüsselmaterial.

Da fast alle Router mit dem NAT von port-losen Protokollen Schwierigkeiten bekommen (siehe Abschnitt 32.13), wurden noch Erweiterungen für diese Protokolle vorgesehen, die heute von fast allen Implementierungen unterstützt werden. Sobald das IKE-Protokoll während der Verhandlung der Verbindung ein NAT erkennt, wechselt es den Port auf den UDP-Port 4500. Sobald die ESP-Verbindung ausgehandelt wurde, werden auch die ESP-Pakete erneut in UDP-Pakete mit dem Port 4500 gekapselt. Damit weisen die Pakete für einen NAT-Router unterwegs wieder einen Port auf, der als Erkennungsmerkmal genutzt werden kann.

Es gibt mindestens zwei IPsec-Implementierungen für den Linux-Kernel:

1. KLIPS. KLIPS ist als Patch für den Kernel 2.4 in FreeSwan, Openswan und strongSwan enthalten. Für den Kernel 2.6 gibt es im Moment nur einen Patch in der Openswan-Distribution. Diese Implementierung stellt virtuelle Netzwerkkarten mit dem Namen `ipsecX` zur Verfügung. Der Verkehr auf diesen Netzwerkkarten findet im Klartext statt. Alle über diese Netzwerkkarten transportierten Pakete werden im Weiteren verschlüsselt über die physikalischen Netzwerkkarten gesendet oder empfangen.
2. 26sec. Dieser Name hat sich für den neuen IPsec-Stack des Linux-Kernels 2.6 eingebürgert. Dieser Stack ist ohne Patch verfügbar. Er besitzt keine virtuellen Netzwerkkarten.

33.2 Iptables-Regeln zum Durchleiten von IPsec

Wenn Sie einem Client die Möglichkeit geben möchten, durch eine Firewall auf ein VPN-Gateway zuzugreifen, können Sie die folgenden Regeln verwenden:

```
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p udp -m multiport --dport 500,4500 -m state ↵
   --state NEW -j ACCEPT
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p 50 -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p 51 -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Achtung

Die Connection Tracking-Timeout-Werte sind möglicherweise zu klein für das VPN. Daher sollten Sie diese anpassen und für UDP und generische Protokolle erhöhen (siehe Kapitel 19).

Wenn Sie ein VPN-Gateway hinter einer Firewall in einer DMZ betreiben möchten, müssen Sie die Protokolle von der Firewall an das Gateway weiterleiten. Dies können Sie mit den folgenden Befehlen erreichen:

```
VPN_GW=192.168.0.5

$IPTABLES -t nat -A PREROUTING -p udp -m multiport --dport 500,4500 -j DNAT ↵
   --to-destination $VPN_GW
$IPTABLES -t nat -A PREROUTING -p 50 -j DNAT --to-destination $VPN_GW

$IPTABLES -A FORWARD -i $EXTDEV -o $INTDEV -d $VPN_GW -p udp -m multiport --dport 500,4500 ↵
  -m state --state NEW -j ACCEPT
```

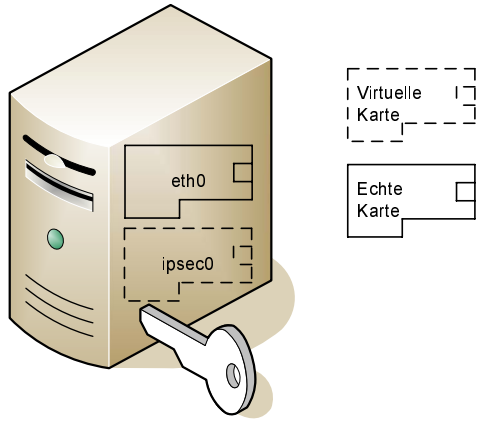


Abbildung 33.1: KLIPS stellt eine virtuelle Netzwerkkarte zur Verfügung.

```
$IPTABLES -A FORWARD -i $EXTDEV -o $INTDEV -d $VPN_GW -p 50 -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Das Protokoll AH (51) kommt in den Regeln nicht vor, da es kein NAT erlaubt.

33.3 KLIPS

Wenn Sie das VPN-Gateway direkt auf der Firewall betreiben möchten, hängen die Regeln und die Möglichkeiten stark von dem verwendeten IPsec-Stack ab. Zunächst betrachten wir KLIPS, dann das aktuelle 26sec.

KLIPS ist der Kernel-Patch des FreeS/Wan-Projekts. Er kommt bei allen Linux-Kerneln 2.4 zum Einsatz, die FreeS/Wan verwenden. Die Weiterentwicklung des FreeS/WAN-Projekts Openswan (*http://www.openswan.org*) unterstützt ab der Version 2.3 auch KLIPS auf dem Kernel 2.6. Bei dem Einsatz von KLIPS werden virtuelle Netzwerkkarten `ipsecX` für das Routing der zu verschlüsselnden und entschlüsselten Pakete verwendet. Auf der physikalischen Netzwerkkarte (`ethX`) tauchen die Klartextpakete nicht auf. Dies erlaubt es, sehr einfach und sauber die Regeln zu definieren und zu entscheiden, welches Paket durch den VPN-Tunnel darf und welches im Klartext versandt werden darf (siehe Abbildung 33.1).

Um den Zugriff auf das VPN-Gateway auf der Firewall zu erlauben, müssen Sie sicherstellen, dass Sie die folgenden Regeln verwenden:

```
EXTDEV=eth0
$IPTABLES -A INPUT -i $EXTDEV -p udp -m multiport --dport 500,4500 -j ACCEPT
$IPTABLES -A OUTPUT -o $EXTDEV -p udp -m multiport --dport 500,4500 -j ACCEPT
$IPTABLES -A INPUT -i $EXTDEV -p 50 -j ACCEPT
$IPTABLES -A OUTPUT -o $EXTDEV -p 50 -j ACCEPT
$IPTABLES -A INPUT -i $EXTDEV -p 51 -j ACCEPT
$IPTABLES -A OUTPUT -o $EXTDEV -p 51 -j ACCEPT
```

Diese Regeln akzeptieren grundsätzlich jeglichen verschlüsselten IPsec-Verkehr und sämtliche IKE-Verbindungen zur Aushandlung der Tunnel. Ich habe hier auf den Einsatz des Connection Tracking verzichtet, da zum einen die Tunnel in beiden Richtungen häufig aufgebaut werden und zum anderen die kurzen Timeouts des Connection Tracking für UDP und die generischen Protokolle ESP und AH zu Problemen führen können.

Nun müssen Sie noch entscheiden, welche Pakete Sie durch den Tunnel durchlassen möchten. Hierfür können Sie das Interface `ipsecX` nutzen, das verwendet wird, um die Klartext-Pakete zu transportieren.

Möchten Sie grundsätzlich alle Verbindungen aus dem internen Netz über den Tunnel zulassen, so können Sie folgende Regeln nutzen:

```
VPNDEV=ipsec0
$IPTABLES -A FORWARD -i $VPNDEV -o $INTDEV -j ACCEPT
$IPTABLES -A FORWARD -i $INTDEV -o $VPNDEV -j ACCEPT
```

Soll es nur möglich sein, HTTP-Verbindungen von außen aufzubauen, können Sie die Regeln einschränken:

```
VPNDEV=ipsec0
$IPTABLES -A FORWARD -i $VPNDEV -o $INTDEV -p tcp --dport 80 -m state --state NEW -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Ihnen stehen sämtliche Freiheiten des `iptables`-Befehls offen, um den Verkehr zu filtern.

33.4 26sec

Bei der Verwendung des IPsec-Stacks, der im Linux-Kernel 2.6 enthalten ist, ist die Filterung der relevanten Pakete weitaus schwieriger. Zunächst sollten Sie sich selbst Klarheit darüber verschaffen, wie Ihr Kernel die Pakete in die verschiedenen Ketten einsortiert. Dies ist nämlich abhängig von den Patches, die Ihre Distribution bereits in den Kernel eingearbeitet hat. Leider ist es nicht möglich, dies allgemein gültig für alle Distributionen und alle Kernel anzugeben. Auch kann ich nicht garantieren, dass Sie die Informationen, die Sie zum Beispiel für einen SUSE-Professional-9.2-Kernel ermitteln, unverändert auf einen SUSE-Professional-9.3-Kernel übertragen können. Wahrscheinlich existieren sogar Unterschiede für die verschiedenen Kernel innerhalb einer Distributionsversion. Mit viel Glück wurden diese Modifikationen aber in dem Changelog des RPM- oder Debian-Pakets hinterlegt. Sie können das Changelog eines RPM-Pakets mit dem folgenden Befehl auslesen:

```
rpm -q --changelog kernel-<version>.<arch>.rpm
```

Um sich einen Überblick über die Einsortierung der Pakete in den Ketten zu verschaffen, sollten Sie sich eine Testumgebung wie in Abbildung 33.2 aufbauen. Dann

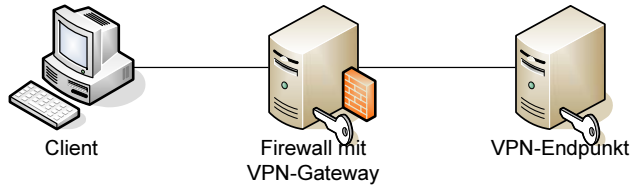


Abbildung 33.2: Bauen Sie sich eine Testumgebung, in der Sie Ihren Kernel testen können.

fügen Sie zu allen Ketten in allen Tabellen LOG-Regeln hinzu und erzeugen IPsec-Verkehr. Achten Sie darauf, dass es ein Unterschied ist, ob Sie die Pakete auf dem VPN-Gateway selbst oder von einem Client hinter dem Gateway erzeugen lassen. Außerdem ist es ein Unterschied, ob eine IPsec-Tunnel-Security-Association oder eine IPsec-Transport-Security-Association genutzt wird. Versuchen Sie möglichst Ihre Konstellation nachzubilden.

Im Folgenden wird das Verhalten der Standard-Kernel bis einschließlich 2.6.14 beschrieben.

33.4.1 Transport-Modus

Im Transport-Modus ist die Betrachtung besonders einfach. Da die Pakete direkt als IPsec-Pakete erzeugt werden, kann Iptables nur die verschlüsselten Pakete filtern. Diese treten ganz normal in der INPUT- und in der OUTPUT-Kette auf. Der Inhalt dieser Pakete kann vor ihrer Verschlüsselung nicht gefiltert werden.

33.4.2 Tunnel-Modus

Anders ist das bei Paketen, die in dem Tunnel-Modus übertragen werden. Hier müssen Sie zwischen Paketen unterscheiden, die von dem Tunnel-Gateway selbst erzeugt werden, und Paketen, die von anderen Systemen erzeugt werden, die den Tunnel nutzen.

In der Abbildung 33.3 sehen Sie den Paketverlauf durch die Ketten, wenn ein anderer Rechner durch das Tunnel-Gateway auf den IPsec-Tunnel zugreift. Oben ist der Paketverlauf des ausgehenden Pakets und unten der Paketverlauf des eingehenden Pakets gezeichnet. Der Stern zeigt den Ort der Verschlüsselung/Entschlüsselung an.

In der Abbildung 33.4 sehen Sie den Verlauf, wenn das Gateway selbst durch den Tunnel kommuniziert.

Sie sollten erkennen, dass die Filter-Ketten das ausgehende Paket im Klartext analysieren. Das ausgehende verschlüsselte Paket durchläuft die Filter-Ketten nicht mehr. Das eingehende IPsec-Paket wird zunächst im verschlüsselten Zustand in der Filter-INPUT-Kette gefiltert, dann entschlüsselt und durchläuft dann erneut sämtliche Ketten, als ob das Paket gerade erst angekommen sei.

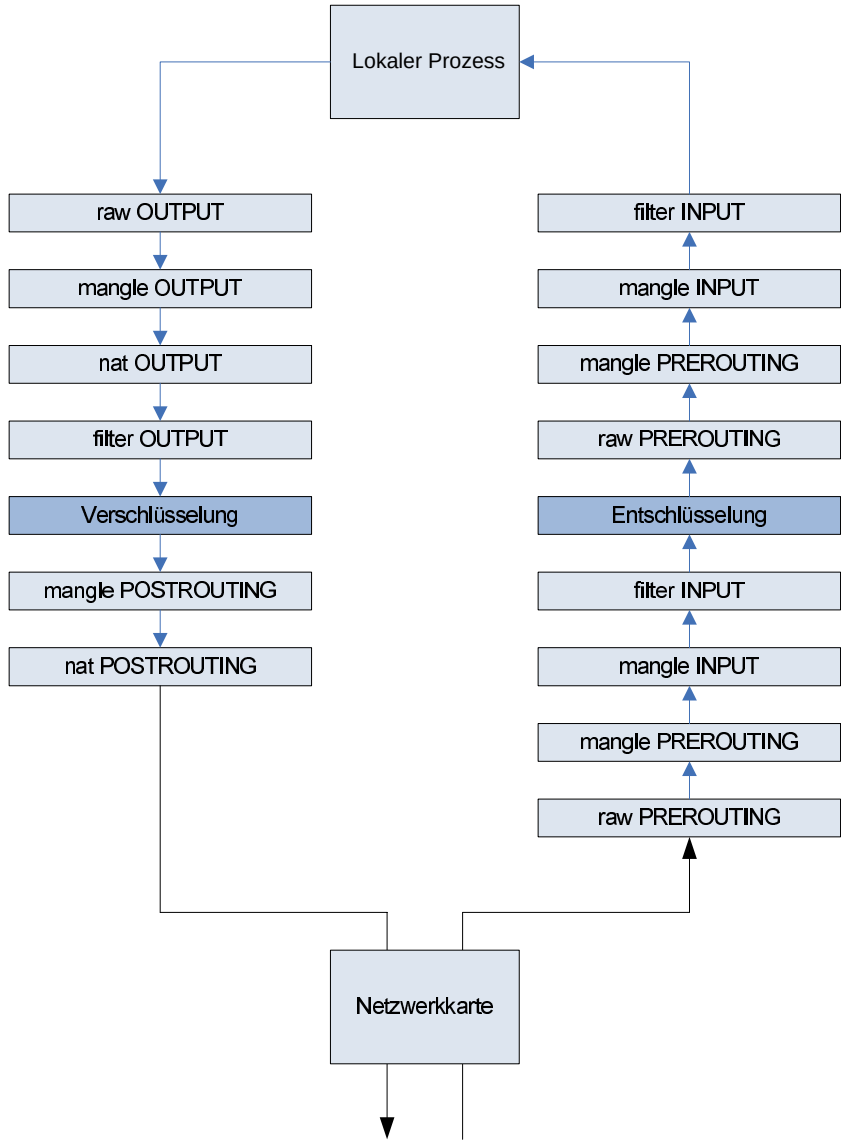


Abbildung 33.3: Paketverlauf durch die Ketten auf einem Host

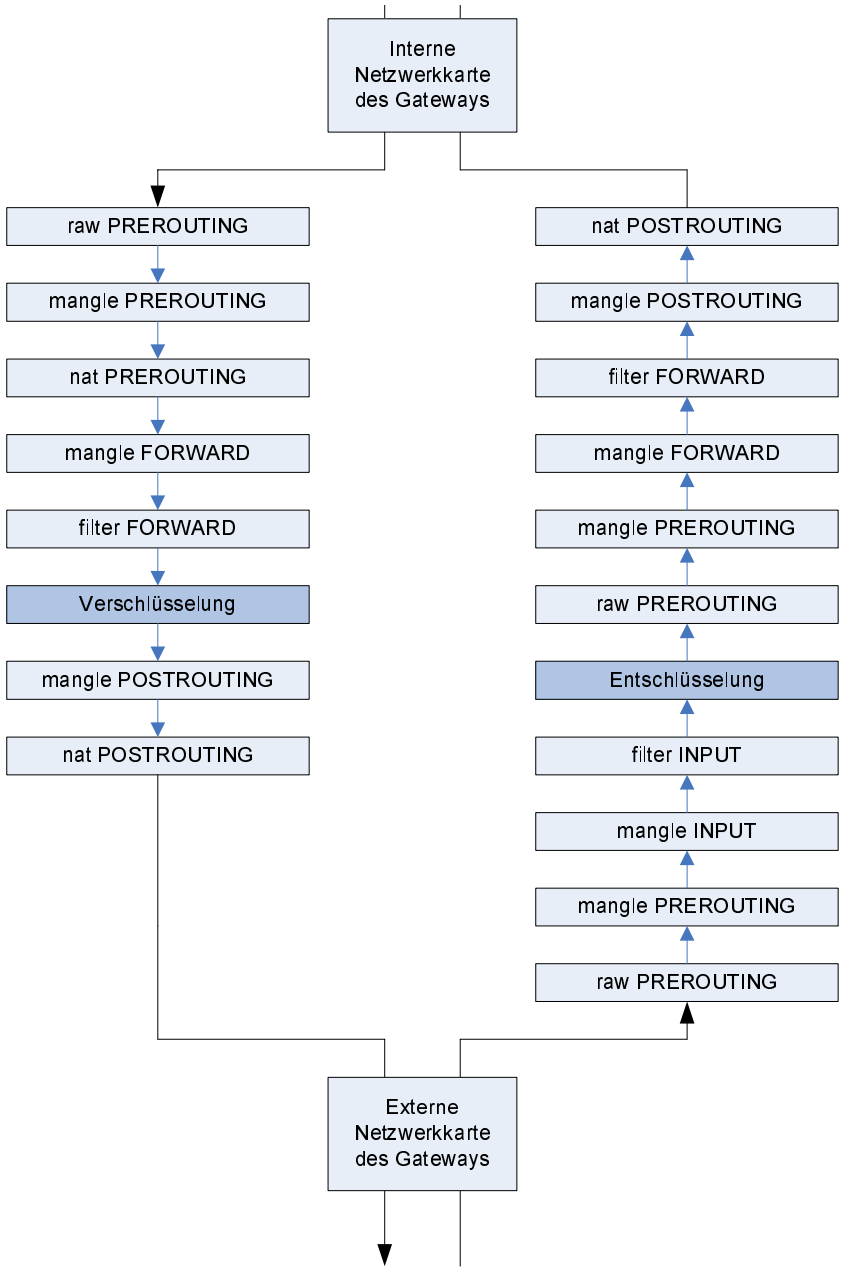


Abbildung 33.4: Paketverlauf durch die Ketten auf einem Gateway

Tipp

Dieses Verhalten können Sie auch mit `tcpdump` verfolgen. Der Befehl `tcpdump` zeigt Ihnen das ausgehende Paket lediglich verschlüsselt an. Das eingehende Paket wird verschlüsselt und dann ein weiteres Mal entschlüsselt dargestellt.

Die NAT-POSTROUTING-Kette wird von dem ausgehenden Paket in jedem Fall immer in verschlüsselter Form durchlaufen. Dadurch ist ein Source-NAT des Pakets vor der Verschlüsselung nicht möglich.

Achtung

Um ein Source-NAT der Pakete vor der Verschlüsselung zu ermöglichen, hat Patrick McHardy einige Patches im Patch-O-Matic (`ipsec-01-output-hooks`, `ipsec-02-input-hooks`, `ipsec-03-policy-lookup` und `ipsec-04-policy-checks`) zur Verfügung gestellt, die jedoch im Moment nicht funktionieren, da sie alle auf dem `nf_reset`-Patch aufbauen, der zurückgezogen wurde. Diese Patches sorgen dafür, dass die NAT-POSTROUTING-Kette zweimal, unverschlüsselt und verschlüsselt, durchlaufen wird. Außerdem führten diese Patches dazu, dass die Filter-OUTPUT-Kette auch von dem verschlüsselten Paket durchlaufen wird.

Solange diese Patches nicht wieder einsatzfähig sind, stehen diese Funktionen nicht zur Verfügung.

33.4.3 Filterung mit Firewall-Markierung

Es gibt zwei Möglichkeiten, den Verkehr, der durch das 26sec-VPN gesendet wird, zu filtern. Die einfache, alte Variante ist die Firewall-Markierung. Die moderne, bessere und sichere Variante ist der `policy`-Match, der in dem nächsten Abschnitt besprochen wird.

Das Problem bei der Filterung des VPN-Verkehrs ist, dass Sie in der FORWARD-Kette entscheiden müssen, ob Sie den Verkehr zulassen möchten. Sie können dort aber nicht direkt prüfen, ob das Paket später durch das VPN geschickt wird oder ob das Paket aus dem IPsec-Tunnel kommt. Diese Information können Sie aber in einer Firewall-Markierung verstecken.

Die Firewall-Markierung kann für ESP-Pakete in der PREROUTING-Mangle-Kette an einem ESP-Paket angebracht werden. Diese Markierung mit MARK überlebt die Entschlüsselung des Pakets. Anschließend können Sie in der Filter-FORWARD- oder Filter-INPUT-Kette nur die Klartext-Pakete akzeptieren, die diese Markierung

aufweisen. Dann war das Paket bei seinem Transport über das Internet durch das VPN geschützt.

```
$IPTABLES -t mangle -A PREROUTING -i $EXTDEV -p 50 \
  -j MARK --set-mark 0x01
$IPTABLES -A FORWARD -m mark  --mark 0x01 -j ACCEPT
```

Wenn Sie sicherstellen möchten, dass bestimmte Pakete auch immer durch das VPN versendet werden, können Sie diese Pakete in der Mangle-FORWARD-Kette markieren und in der Mangle-POSTROUTING-Kette alle Pakete verwerfen, die nicht verschlüsselt, aber markiert sind.

```
$IPTABLES -t mangle -A FORWARD -i $INTDEV -j MARK --set-mark 0x02
$IPTABLES -t mangle -A POSTROUTING -m mark --mark 0x02 -p ! 50 -j DROP
```

So stellen Sie sicher, dass jedes Paket, das Sie in der FORWARD-Kette erlaubt haben, auch tatsächlich verschlüsselt wird.

33.4.4 Filterung mit dem policy-Match

Besser ist es jedoch, mit dem `policy`-Match zu arbeiten. Dieser Match ist in dem Patch-O-Matic enthalten. Hiermit können Sie ohne umständliche Markierung die Pakete erkennen, die von einer IPsec-Policy geschützt werden. Zusätzlich können Sie sogar den Tunnel prüfen, der von dem Paket genutzt wird. Der Test hat die folgenden Optionen, um auf das Vorhandensein einer Policy zu testen:

- `--dir in|out`: Hiermit definieren Sie, ob Sie eine `in`- oder `out`-Policy testen möchten. Diese Option müssen Sie angeben.
- `--pol none|ipsec`: Hiermit wählen Sie aus, ob die Policy einen Schutz mit IPsec verlangen soll oder nicht.
- `--strict`: Wenn Sie diese Option angeben, müssen Sie die Policy genau beschreiben.
- `--reqid <id>`: Hiermit können Sie die genaue ID der Policy angeben. Diese ID kann mit dem `setkey`-Kommando mit der Angabe `unique:id` bei der Definition der Policy gesetzt werden.
- `--spi`: Hiermit können Sie die genaue SPI der Security Association auswählen, die genutzt werden muss.
- `--proto ah|esp|ipcomp`: Hiermit fragen Sie das Protokoll der Policy ab.
- `--mode tunnel|transport`: Dies wählt zwischen den IPsec-Modi Tunnel und Transport.
- `--tunnel-src <ip>[/<maske>]`: Bei einem Tunnel können Sie die spezifischen Tunnelendpunkte angeben. Dies definiert die Quelladresse.
- `--tunnel-dst <ip>[/<maske>]`: Dies definiert die Zieladresse.

- `--next`: Bei der Verwendung von `--strict` können Sie hiermit das nächste Element definieren.

Um nun in der FORWARD-Kette nur den Verkehr zuzulassen, der später von dem VPN geschützt wird oder über das VPN den Rechner erreicht hat, können Sie folgende Regeln verwenden:

```
$IPTABLES -P FORWARD DROP
$IPTABLES -A FORWARD -m policy --dir in --mode tunnel \
  --pol ipsec --proto esp -j ACCEPT
$IPTABLES -A FORWARD -m policy --dir out --mode tunnel \
  --pol ipsec --proto esp -j ACCEPT
```

Die erste Zeile setzt die Default-Policy der FORWARD-Kette auf DROP. Alle Pakete, die nicht explizit akzeptiert werden, werden verworfen. Die zweite Zeile prüft, ob das Paket von einer IPsec-Policy in der Richtung `in` im Tunnel-Modus mit dem Protokoll ESP geschützt wird, und akzeptiert diese Pakete. Die letzte Zeile prüft, ob das Paket von einer entsprechenden Policy in der Richtung `out` geschützt wird. Damit haben Sie beide Richtungen abgedeckt und stellen sicher, dass die in der FORWARD-Kette akzeptierten Pakete im Internet immer von einer IPsec-Policy geschützt sind.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

34 ICMP

Ohne ICMP würde das Internet nicht funktionieren. Häufig ist dieses Protokoll auch für Funktionsstörungen verantwortlich. Teilweise hängt dies mit falsch konfigurierten Firewalls zusammen. Dieses Kapitel zeigt Ihnen, wie Sie das Protokoll richtig filtern.

34.1 ICMP

Die Filterung des ICMP-Protokolls (RFC 792) ist ein recht kompliziertes und umfangreiches Thema, da es recht viele wichtige ICMP-Nachrichten gibt. Das Internet Control and Message Protocol ist in erster Linie für die Übertragung von Fehlermeldungen verantwortlich. Außerdem wird dieses Protokoll von dem `ping`-Befehl und dem `traceroute`-Befehl eingesetzt.

Erfreulicherweise unterstützt die Stateful-Inspection des Linux-Kernels auch das ICMP-Protokoll. Das bedeutet, dass der Kernel erkennen kann, ob eine ICMP-Fehlermeldung sich auf eine existente Verbindung bezieht oder nicht. So ist es möglich, ICMP-Fehlermeldungen nur zuzulassen, wenn sie sich tatsächlich auf eine aufgebaute Verbindung beziehen, und jede andere Form direkt zu verwerfen. Die Fehlermeldungen, die sich auf existente Verbindungen beziehen, werden von dem Linux-Kernel als `RELATED` eingeordnet. Wenn Sie `RELATED`-Pakete zulassen, dann werden auch diese Pakete akzeptiert. Dabei löscht dann der Linux-Kernel auch die Verbindung, auf die sich die Fehlermeldung bezog, aus der Verbindungsliste, denn es trat ja ein Fehler auf.

Eine derart allgemeine Betrachtung ist jedoch in einigen Fällen nicht ausreichend. In Abhängigkeit der Firewall-Richtlinien müssen die ICMP-Nachrichten einzeln betrachtet werden. Das wird im Folgenden gezeigt. Dazu betrachten wir zunächst die einzelnen Fehlernachrichten, um uns dann anschließend einzelne Befehle näher anzusehen, die diese Funktionen nutzen (`ping` und `traceroute`).

Im Einzelnen betrachten wir die folgenden ICMP-Nachrichten:

- destination-unreachable
- destination-unreachable: fragmentation-needed
- source-quench
- redirect
- router-advertisment

- router-solicitation
- time-exceeded
- parameter-problem
- timestamp-request/timestamp-reply
- address-mask-request/address-mask-reply
- echo-request/echo-reply

Ein grundsätzliches Filtern der Meldungen ist sehr einfach. Wenn Sie einfach alle gültigen ICMP-Meldungen akzeptieren möchten, nutzen Sie einfach folgende Regel:

```
$IPTABLES -A FORWARD -p icmp -m state --state RELATED -j ACCEPT
```

Achtung

Denken Sie daran, dass Sie vielleicht sowieso schon eine Regel in Ihrem Skript haben, die alle `RELATED`-Pakete erlaubt!

Wenn Sie nur bestimmte Meldungen akzeptieren möchten, können Sie folgende Regel verwenden:

```
$IPTABLES -A FORWARD -p icmp --icmp-type destination-unreachable -m state --state RELATED
-j ACCEPT
```

Was nun wo und in welcher Richtung Sinn macht, erläutern die nächsten Abschnitte.

34.2 ICMP destination-unreachable

Die ICMP-Fehlermeldung `destination-unreachable` wird immer dann gesendet, wenn ein Ziel nicht erreichbar ist. Dabei kann es mehrere Gründe für diese Meldung geben. Im Folgenden sehen Sie eine Auswahl der häufigsten Gründe:

- Der angesprochene UDP-Port wird von keiner Applikation bedient.
- Der angesprochene Rechner kennt das IP-Protokoll nicht.
- Der angesprochene Rechner reagiert nicht auf eine ARP-Anfrage. Er ist wahrscheinlich ausgeschaltet.
- Das Netzwerk, in dem sich der Zielrechner befindet, ist nicht erreichbar.
- Der Rechner oder das Netzwerk werden durch eine Firewall geschützt. Einige Firewalls senden dann ein `destination-unreachable: network-prohibited`.

- Das Paket ist zu groß, um in das nächste Netzwerk geroutet zu werden. Eine Fragmentierung ist erforderlich, aber nicht erlaubt. Nähere Informationen über diese Meldung finden Sie im nächsten Abschnitt.

Die meisten dieser Fehlermeldungen weisen auf fatale Fehler bei der Verbindung hin. Ein Client, der diese Meldungen erhält, erkennt den Fehler und bricht die Verbindungsversuche ab. Lediglich bei der Meldung `fragmentation-needed` wird ein erneuter Versuch mit einem kleineren Paket unternommen. Für eine Firewall bedeuten alle diese Fehlermeldungen mit Ausnahme der `fragmentation-needed`-Meldung, dass die Verbindung nicht aufrechterhalten werden kann. Die Firewall kann daher die Verbindung aus ihrer Zustandstabelle löschen.

Ein Filtern der ICMP-Meldungen ist sehr einfach möglich. Bereits im letzten Abschnitt habe ich die folgende Regel vorgestellt:

```
$IPTABLES -A FORWARD -p icmp --icmp-type destination-unreachable -m state --state RELATED
-j ACCEPT
```

Diese Regel akzeptiert alle ICMP-Fehlermeldungen vom Typ `destination-unreachable` unabhängig von ihrer Richtung und den IP-Adressen. Es ist lediglich erforderlich, dass die Firewall die Fehlermeldung einer Verbindung zuordnen kann.

Jedoch können diese Pakete auch Informationen über interne Systeme preisgeben. Zum einen kann ein Angreifer erkennen, ob ein System exisitiert, Protokolle erkannt werden und die entsprechenden Ports offen sind.

Hinweis

So kann ein Angreifer zum Beispiel durch Senden eines ESP- oder AH-Pakets herausfinden, ob das System ein VPN-Gateway ist oder nicht. Normale Systeme antworten mit einer `protocol-unreachable`-Meldung. Ein VPN-Gateway versucht das Paket zu analysieren und zu verarbeiten.

Teilweise geben die Systeme in den Fehlermeldungen mehr Informationen preis, als dem Administrator lieb ist. So schickten Linux-Kernel der Version 2.0 beliebige Speicherinhalte in den Fehlermeldungen: *http://www.cartel-securite.fr/pbiondi/adv/CARTSA-20030314-icmpleak.txt*. Diese Lücke ist behoben. Jedoch sind mindestens einige Windows-Systeme von ähnlichen Problemen betroffen.

Daher ist es sinnvoll, die Anzahl der Meldungen zu begrenzen. Wenn Sie eine Firewall implementieren, um ein internes Netz beim Zugriff auf das Internet zu schützen, so sollten Sie ICMP-`destination-unreachable`-Meldungen aus dem Internet in Ihr geschütztes Netz erlauben. Tun Sie dies nicht, werden Ihre Clients beim Zugriff auf das Internet nicht über Fehler beim Verbindungsaufbau informiert und werden es mehrfach erneut versuchen, bis ein client-interner Timeout auftritt. Ihre Benutzer werden über diese Verzögerung nicht begeistert sein. Wenn Sie die Fehlermeldun-

gen zulassen, erhält der Client sofort eine entsprechende Nachricht und kann die Information sofort an den Benutzer oder die Applikation weitergeben.

Den Transport von ICMP-`destination-unreachable`-Meldungen aus Ihrem internen Netz in das Internet ist mit einer Ausnahme (siehe den nächsten Abschnitt 34.3) nicht erforderlich.

Sie können also folgende Regel verwenden:

```
$IPTABLES -A FORWARD -i $EXTDEV -o $INTDEV -p icmp --icmp-type destination-unreachable
-m state --state RELATED -j ACCEPT
```

Natürlich ist der Transport von ICMP-`destination-unreachable`-Nachrichten aus der DMZ unter Umständen sinnvoll. Das hängt davon ab, ob Sie den Clients, die auf Ihre Dienste zugreifen, Fehlermeldungen senden möchten oder nicht. Sie können mit der folgenden Regel die `destination-unreachable`-Meldungen zulassen:

```
$IPTABLES -A FORWARD -i $DMZDEV -o $EXTDEV -p icmp --icmp-type destination-unreachable
-m state --state RELATED -j ACCEPT
```

34.3 ICMP fragmentation-needed

Diese ICMP-Meldung (beziehungsweise ihre falsche Filterung) ist für eine Vielzahl von Problemen im Internet verantwortlich. Schuld ist die Tatsache, dass unterschiedliche Netzwerkmedien unterschiedliche Paketgrößen transportieren können. Die maximale Größe ist die Maximum Transmission Unit (MTU). Befindet sich nun ein Client in einem Netz A mit einer besonders großen MTU und versendet ein Paket an einen Empfänger in einem Netz B mit einer kleineren MTU, so besteht die Gefahr, dass das Paket zu groß für das Netz B ist. Entweder wird das Paket fragmentiert oder es wird verworfen und diese Fehlermeldung erzeugt. Da eine Fragmentierung bei einem Paketverlust mit einem Overhead verbunden ist, führen fast alle modernen Betriebssysteme eine Path Maximum Transmission Unit Discovery (RFC 1191) durch. Sie ermitteln die MTU für den kompletten Pfad und bauen ihre Pakete dann in passender Größe. Die PMTUD ist aber auf diese Fehlermeldung angewiesen. Erreicht die Fehlermeldung nicht ihr Ziel, kann die Verbindung nicht aufgebaut werden. Dummerweise kann der betroffene Client kaum etwas an dieser Tatsache ändern (siehe auch Abschnitt 16.31). Eine genauere technische Betrachtung finden Sie in dem Exkurs MTU und PMTUD (siehe folgenden Exkurs).

Exkurs: MTU und die Path-MTU-Discovery

Da die MTU für unterschiedliche Netzwerkmedien unterschiedliche Werte haben kann, kann es vorkommen, dass ein Rechner so große Pakete erzeugt, dass ein Router auf dem Weg zum Ziel diese Pakete nicht weiterleiten kann. In der Abbildung 34.1 ist ein Token-Ring-Netz und ein Ethernet dargestellt. Die MTU des Token-Ring (16 MBit/s) beträgt 17914 Bytes. Die MTU des Ethernet beträgt

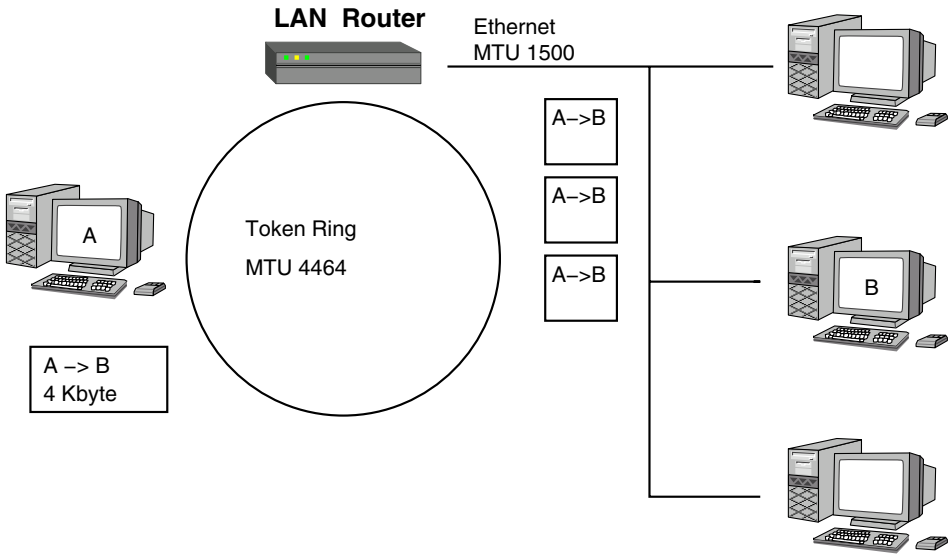


Abbildung 34.1: Im Paket-Switched Network können die Pakete über unterschiedliche Wege das Ziel finden.

1500 Bytes. Sendet nun der Rechner Eins an den Rechner Zwei 20 Kbyte Daten, so erzeugt er zwei Pakete. Das erste Paket ist etwa 17 Kbyte groß und das zweite etwa 3 Kbyte. Der Router kann diese Pakete jedoch nicht unverändert weitersenden, da die MTU des Ethernet nur 1500 Bytes beträgt. Er fragmentiert die Pakete. Dazu schneidet er zunächst das Paket in kleinere Bestandteile und kopiert jeweils den original IP-Header des Pakets davor. Die Länge dieser Bestandteile muss ein Vielfaches von acht aufweisen. Zusätzlich setzt der Router in allen Fragmenten außer dem letzten das More-Fragments-Bit (MF). Dieses zeigt dem Empfänger an, dass weitere Fragmente folgen. Damit der Empfänger die Fragmente richtig zusammensetzen kann, gibt er noch den Offset des Fragments im Gesamtpaket als Vielfaches von acht an. Die Fragmente werden nun weiter zum Empfänger gesendet, der die Fragmente zusammenbaut und das IP-Paket prozessiert.

Wenn nun aber eines dieser Fragmente verloren geht, wartet der Empfänger vergebens auf dieses Fragment. Nach einem Timeout sendet er eine ICMP-time-exceeded-Fehlermeldung (siehe Abschnitt 34.6). Der Absender sendet das Paket erneut, es wird erneut fragmentiert, und es besteht wieder die Gefahr, dass ein Fragment verloren geht. Das einzelne Fragment kann nicht neu angefordert werden. Der Router hat das Fragment nicht gespeichert, und der Absender weiß nichts von einer Fragmentierung. Bei einem Verlust von 1500 Bytes werden ca. 17.000 Bytes neu übertragen!

Die Path-MTU-Discovery versucht, dieses Problem intelligent zu lösen. Hierzu sendet ein Client, bei dem PMTUD aktiviert ist, alle Pakete mit einem gesetzten Don't-Fragment-Bit (DF). Dieses Bit weist alle Router an, das Paket nicht zu fragmentieren. In unserem Fall kann das Paket jedoch nicht weiter gesendet werden. Der Router verwirft das Paket und sendet eine Fehlermeldung an den Absender. In dieser Fehlermeldung informiert der Router den Absender auch über die MTU des nächsten Hops. Der Absender kann das Paket neu mit einer passenderen Größe bauen. Dieses Paket kann dann weitertransportiert werden. Befindet sich anschließend ein weiteres Netz mit einer noch kleineren MTU auf dem Weg zum Ziel, erfolgt dieser Vorgang erneut.

Sicherlich setzt kaum noch jemand heutzutage Token-Ring-Netze ein. Da fast alle Netze auf Ethernet basieren, könnte man annehmen, dass sich dieses Problem überlebt hat. Jedoch taucht es verstärkt seit der Einführung von DSL-Internetzugängen wieder auf. Die DSL-Anbindung des Rechners an das Modem erfolgt über eine Ethernet-Leitung. Dennoch beträgt die MTU für das IP-Protokoll nicht 1500 Bytes, da das IP-Protokoll noch in ein weiteres Protokoll eingepackt wird. In Deutschland handelt es sich meist um PPPOE. In anderen Ländern wird auch PPTP eingesetzt. Dadurch verringert sich die MTU für das IP-Protokoll um mindestens acht Bytes (PPPOE) auf 1492 Bytes.

In Kombination mit einer Firewall können nun zwei Probleme auftreten:

1. Die Firewall kann fragmentierte Pakete nicht richtig filtern.
2. Die Firewall erlaubt nicht die `fragmentation-needed`-Nachricht.

1. Wenn ein Paketfilter fragmentierte Pakete filtern soll, taucht ein besonderes Problem auf. Die Filterung des ersten Fragments eines HTTP-Pakets ist kein Problem, denn dieses Fragment weist sowohl einen IP- als auch einen TCP-Header auf. Ab dem zweiten Fragment enthält das Fragment aber nur noch einen IP-Header, da der Router lediglich den IP-Header kopiert. Schließlich arbeitet ein Router auch auf der Schicht Drei und nicht auf der Schicht Vier. Ein klassischer Router kann mit einem TCP-Header gar nichts anfangen. Der Paketfilter kann nun ab dem zweiten Fragment nicht mehr entscheiden, ob es sich um ein HTTP- oder ein Telnet-Paket handelt. Soll er das Paket akzeptieren oder verwerfen?

Die ersten Paketfilter hatten eine einfache Lösung parat: Sie filterten das erste Fragment und ließen automatisch alle Fragmente außer dem ersten durch! Erhielt der Empfänger auch das erste

Fragment, so konnte er das Paket defragmentieren und auswerten. Wurde das erste Fragment durch eine Firewall verworfen, konnte der Empfänger das Paket nicht defragmentieren und musste auch alle weiteren Fragmente verwerfen. Leider gab es in der Vergangenheit mehrfach Angriffe (z.B. *http://cert.uni-stuttgart.de/archive/bugtraq/1999/07/msg00232.html*), die diese einfache Lösung umgingen. Daher sammeln heute alle Paketfilter bereits die Fragmente, defragmentieren sie und analysieren erst anschließend das Paket mit ihren Regeln. Wird das Paket akzeptiert, so wird es weitertransportiert und möglicherweise hierzu erneut fragmentiert. Wird das Paket verworfen, so werden auch alle Fragmente verworfen.

2. Bei dem zweiten Problem handelt es sich nicht um ein Sicherheitsproblem, sondern vielmehr um eine Art von Denial-of-Service. In Abbildung 34.2 sehen Sie eine typische Konstellation, wie sie heute im Internet anzutreffen ist.

Der DSL-Anwender greift auf einen Webserver im Internet zu. Dieser Webserver wird durch eine Firewall geschützt, die grundsätzlich keine ICMP-Meldungen von außen erlaubt. Dies ist nicht ungewöhnlich, da bis vor einigen Jahren die Paketfilter kaum in der Lage waren, ICMP-Meldungen sicher zu filtern. Die Firewall-1 des Marktführers CheckPoint konnte in der Version 4 dies von Haus aus nicht.

Solange der Webserver nur kleine Datenmengen versendet, tritt kein Problem auf. Sobald der Webserver aber mehr als 1492 Byte große Pakete erzeugt, werden diese von dem DSL-Router auf der Seite des Internet-Service-Providers als zu groß abgelehnt. Dieser Router erzeugt eine ICMP-`fragmentation-needed`-Nachricht und sendet sie an den Webserver. Die Firewall verhindert, dass diese Nachricht den Webserver erreicht. Der Webserver erhält keine Empfangsbestätigung und sendet das Paket nach einiger Zeit erneut. Da er den Grund für den Paketverlust nicht kennt, sendet er das Paket unverändert neu. Dieses neue Paket wird erneut verworfen, und eine Fehlermeldung wird generiert. Nach einiger Zeit wird der Webserver aufgeben und die Verbindung abbrechen. Die Daten werden den Client nicht erreichen.

Dummerweise ist der Client davon betroffen und kann kaum etwas zur Behebung des Problems tun. Als einzige Lösung im Fall des TCP-Protokolls kann er die Maximum Segment Size (MSS) setzen (siehe Abschnitt 16.31).

Die Fehlermeldung `fragmentation-needed` sollten Sie grundsätzlich in allen Richtungen durch Ihre Firewall erlauben. Ansonsten kann es bei der heutigen IT-Infrastruktur

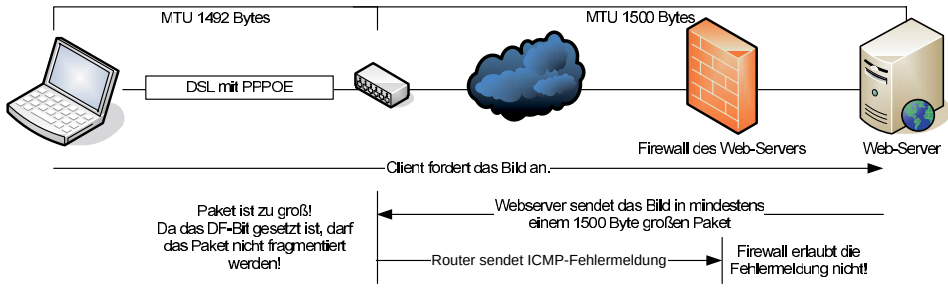


Abbildung 34.2: Ein DSL-Anwender greift auf einen Webserver zu. Der Webserver wird durch eine Firewall geschützt. Die PMTUD funktioniert auf Grund der Firewall-Konfiguration nicht.

mit DSL und VPNs zu Verbindungsproblemen kommen, die Sie und Ihre Kunden betreffen. Am einfachsten erfolgt das mit der folgenden Zeile:

```
$IPTABLES -A FORWARD  -p icmp --icmp-type fragmentation-needed -m state --state RELATED↵
  -j ACCEPT
```

34.4 ICMP source-quench

Diese Meldung kann ein Router oder ein Rechner versenden, wenn er die empfangenen Pakete nicht schnell genug verarbeiten kann und daher einzelne Pakete aus seiner Empfangswarteschlange unverarbeitet verwerfen muss. Da diese Pakete später erneut gesendet werden müssen und dadurch Verzögerungen auftreten, ist es sinnvoller, den Absender zu informieren, so dass die Pakete dann langsamer gesendet werden.

Heutzutage verwendet kaum noch ein Router diese Meldungen. Source-Quench ist durch moderne Algorithmen abgelöst worden. Auch die meisten TCP-Stacks verfügen über mächtigere Methoden der Flusskontrolle. Jedoch reagieren alle mir bekannten Betriebssysteme noch auf `source-quench`-Nachrichten. So ist es möglich, mit gefälschten `source-quench`-Nachrichten existierende Verbindungen zu verlangsamen. Dies kann bis zum Denial-of-Service führen (siehe *http://xforce.iss.net/xforce/xfdb/17429*).

Ein einfaches Werkzeug für die Erzeugung dieser Meldungen ist `tcpnice` von Dug Song. Es ist Teil des `dsniff`-Pakets: *http://www.monkey.org/~dugsong/dsniff*.

Sie sollten diese `source-quench`-Nachrichten nicht durch Ihre Firewall erlauben. Es könnte sinnvoll sein, diese Nachrichten zu protokollieren, so dass Sie erkennen können, ob diese Nachrichten vielleicht doch gültig sind.

```
$IPTABLES -A FORWARD -p icmp --icmp-type source-quench -j LOG --log-prefix "Source-Quench: "
```

34.5 ICMP redirect

Die ICMP-`redirect`-Nachricht erlaubt es einem Router, einen Rechner auf einen besseren Router hinzuweisen. Wann wird eine ICMP-Redirect-Nachricht versandt (Abbildung 5.17 auf Seite 127)?

1. Rechner A sendet ein Paket an Rechner B. Da Rechner B sich in einem anderen Netz befindet, sendet Rechner A das Paket an sein Default-Gateway G1.
2. Das Gateway G1 prüft seine Routing-Tabelle und stellt fest, dass der nächste Hop für das Paket das Gateway G2 ist.
3. Wenn sich der Rechner A, das Gateway G2 und das Gateway G1 in demselben Netz befinden, sendet das Gateway G1 eine Redirect-Nachricht an den Rechner A und teilt ihm mit, dass das Gateway G2 ein besserer Router auf dem Weg zum Ziel Rechner B sei.
4. Außerdem leitet das Gateway G1 das Paket an das Gateway G2 weiter.
5. Der Rechner A trägt das neue Gateway G2 in seiner Routing-Tabelle oder seinem Routing-Cache ein und verwendet nun dieses Gateway, um den Rechner B zu erreichen.

Sicherlich möchten Sie nicht, dass irgendjemand Ihrer Firewall oder einem Rechner in Ihrer DMZ oder Ihrem internen Netzwerk von außen einen besseren Router mitteilen kann. Diese ICMP-Nachricht kann natürlich für Angriffe in Form von Router-Spoofing verwendet werden. Sie sollten diese Nachricht nicht über Ihre Firewall zulassen. Vielleicht ist es sinnvoll, diese Nachrichten zu protokollieren (wenn Sie die Protokolle auch lesen).

```
$IPTABLES -A FORWARD  -p icmp --icmp-type redirect -j LOG --log-prefix "Source-Quench: "
```

34.6 ICMP time-exceeded

Diese ICMP-Nachricht zeigt eine Zeitüberschreitung beim Pakettransport an. Bei dem Transport eines Pakets kann es zu zwei Arten der Zeitüberschreitung kommen:

- Bei der Defragmentierung eines Pakets hat der Empfänger nicht alle Fragmente innerhalb seiner vorgeschriebenen Zeit erhalten. Er verwirft das Paket und schickt eine `time-exceeded: ttl-zero-during-reassembly`-Nachricht zurück.
- Bei dem Transport eines Pakets hat das Paket seine Lebensdauer überschritten. Jedes Paket trägt im IP-Header einen Time-to-Live-Wert (TTL). Jeder Router, der das Paket weiterleitet, reduziert diesen Wert um eins. Zusätzlich wird dieser Wert jede Sekunde, die das Paket auf einem Router in der Warteschlange verweilt, um eins reduziert. Dies tritt heute jedoch kaum noch auf. Erreicht der Wert 0, so verwirft der Router das Paket und sendet eine `time-exceeded: ttl-zero-during-transit`-Meldung an den Absender. Hiermit sollen Paket-Irrläufer durch fehlerhafte Routerkonfiguration vermieden werden.

Wenn Sie eine Firewall zum Schutz eines internen Netzes beim Zugriff auf das Internet einsetzen, möchten Sie wahrscheinlich diese Fehlermeldungen in Richtung Ihrer Clients zulassen, damit diese bei Fehlern in der Konfiguration eines Routers von Paketen informiert werden. Fehler bei der Defragmentierung treten heute so gut wie gar nicht mehr auf, da die meisten Betriebssysteme die Path-MTU-Discovery (siehe den Exkurs auf Seite 572) unterstützen.

```
$IPTABLES -A FORWARD -i $EXTDEV -o $INTDEV -p icmp --icmp-type time-exceeded -m state ↵
  --state RELATED -j ACCEPT
```

34.7 ICMP parameter-problem

Diese Fehlermeldung wird von einem System gesendet, wenn es auf Grund eines Fehlers in dem IP-Header ein Paket nicht verarbeiten konnte. Hierfür gibt es viele verschiedene Gründe. Die Fehlermeldung weist den Absender mit einem Zeiger auf den Grund hin. Es kann jedoch auch sein, dass eine IP-Option im Header für die Zustellung fehlte. Da die Option fehlt, kann nicht auf sie verwiesen werden. Hierfür gibt es dann die besondere Meldung `parameter-problem: required-option-missing`.

Diese Fehlermeldungen treten in modernen Netzen mit den ausgereiften IP-Stacks nur sehr selten auf, so dass ich üblicherweise empfehle, die Meldungen zu protokollieren und zu verwerfen.

```
$IPTABLES -A FORWARD  -p icmp --icmp-type parameter-problem -j LOG ↵
  --log-prefix "Parameter-Problem: "
```

34.8 ICMP router-advertisment/router-solicitation

Für das Funktionieren des IP-Protokolls ist es erforderlich, dass jeder Rechner die für ihn zuständigen Router kennt. Üblicherweise werden die Router eines Systems in Konfigurationsdateien festgelegt. Da dies aber einen gewissen manuellen Administrationsaufwand erzeugt, wurde die automatische Routererkennung entwickelt. Diese Routererkennung (Router Discovery, RFC 1256) basiert auf den Router-Advertisment- und Router-Solicitation-Nachrichten. Jeder Router sendet in regelmäßigen Abständen (üblicherweise alle 10 Minuten) ICMP-`router-advertisment`-Nachrichten aus. Diese Nachrichten enthalten wichtige Informationen über den Router, wie zum Beispiel seine IP-Adresse. So kann der Rechner die Informationen in seiner Routingtabelle eintragen.

Wenn nun ein Rechner neu gestartet wird, erhält er spätestens nach 10 Minuten die notwendigen Routerinformationen. Da dies häufig nicht akzeptabel ist, kann der Rechner auch eine `router-solicitation`-Nachricht senden. Diese weist alle Router in dem lokalen Netzwerk an, jetzt ihre Router-Advertisment-Nachricht zu senden.

Die `router-advertisment`-Nachricht wird an die *All-Devices*-Multicast-Adresse (224.0.0.1) und die `router-solictation`-Nachricht wird an die *All-Routers*-Multicast-Adresse (224.0.0.2) gesendet.

Sicherlich wollen Sie derartige Nachrichten nicht durch Ihre Firewall erlauben.

34.9 ICMP timestamp-request/timestamp-reply

Mit den ICMP-`timestamp-request`- und `timestamp-reply`-Nachrichten (RFC 792) kann ein Rechner sowohl die Uhrzeit eines anderen Rechners ermitteln als auch die Wegezeit berechnen. Der Absender der `timestamp-request`-Nachricht trägt seine Uhrzeit in Millisekunden seit Mitternacht (UTC) ein (Originator's Timestamp). Der Empfänger trägt bei Erhalt der Nachricht seine eigene Uhrzeit in dem *Receive Timestamp*-Feld ein. Die *Transmit Timestamp* trägt er kurz vor dem Versand der `timestamp-reply`-Nachricht ein (Abbildung 34.3).

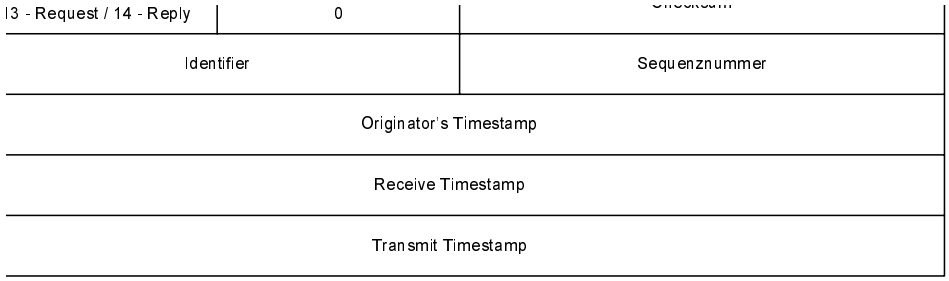


Abbildung 34.3: Die Timestamp-Nachrichten

In einer gewissen Weise ähnelt dieser Mechanismus dem Ping (siehe unten), bietet aber mit der absoluten Uhrzeit noch zusätzliche Informationen. Die meisten modernen Betriebssysteme reagieren auf diese Nachrichten, obwohl nur sehr wenige Werkzeuge existieren, die diese Nachrichten erzeugen und auswerten können. Ein allgemein verfügbares Werkzeug ist Nmap. Weitere Werkzeuge sind `icmppush` und `sing` (*http://sourceforge.net/projects/sing/*). Nmap kann mit der Option `-PP` den Ping nach anderen Systemen im lokalen Netz durchführen.

```
[root@bibo ~]# nmap -PP -sP 192.168.255.0/24

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-07-29 13:23 CEST
Host 192.168.255.1 appears to be up.
MAC Address: 00:13:10:1F:B7:D1 (Unknown)
Host 192.168.255.100 appears to be up.
Host inspiron-8100.opensource-training.de (192.168.255.125) appears to be up.
MAC Address: 00:20:E0:6C:72:1E (Actiontec Electronics)
Nmap finished: 256 IP addresses (3 hosts up) scanned in 2.295 seconds
```

Das Werkzeug `sing` ist noch mächtiger und erlaubt es, jede Art von ICMP-Nachricht zu erzeugen.

Sicherlich wollen Sie diese Nachrichten nicht von außen durch Ihre Firewall erlauben. Die Filterung dieser Nachrichten unterscheidet sich von den anderen ICMP-Nachrichten, da es sich hier nicht um eine Fehlermeldung handelt. Man kann fast

von einem Client und einem Server, die miteinander kommunizieren, sprechen. Daher filtert auch Iptables diese Nachrichten anders! Jeder Timestamp-Request wird als neuer Verbindungsaufbau (State: NEW) gewertet. Jeder Timestamp-Reply wird als Teil einer aufgebauten Verbindung gewertet (State: ESTABLISHED). Zusätzlich beendet jeder Timestamp-Reply auch die Verbindung und entfernt sie aus der Tabelle. Die Zuordnung der Reply-Nachrichten zu den entsprechenden Request-Nachrichten erfolgt neben der IP-Adresse über den Identifier und die Sequenznummer der Nachricht.

Möchten Sie die Verwendung dieser Nachrichten für Testzwecke oder für Nmap von innen durch Ihre Firewall nach außen zulassen, können Sie folgende Regel nutzen:

```
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p icmp --icmp-type timestamp-request -m state ↵
  --state NEW -j ACCEPT
```

Die Funktion dieser Regel setzt natürlich voraus, dass Sie eine allgemeine Regel für die Akzeptanz aller `ESTABLISHED`-Pakete verwenden.

34.10 ICMP address-mask-request/address-mask-reply

Diese Nachrichten (RFC 950) erlauben es einem Rechner, einen anderen Rechner nach seiner Netzmaske zu fragen. Ursprünglich wurde diese Funktion implementiert, um einem Rechner, der keine Informationen über sein lokales Netz besitzt, die Möglichkeit zu geben, andere Rechner in demselben Netz nach der gültigen Netzmaske zu fragen. Dazu sendet der Rechner eine Address-Mask-Request-Nachricht entweder an die Broadcast-Adresse (255.255.255.255) oder, falls er den lokalen Router kennt, an den Router. Dies ähnelt der Möglichkeit, mit Hilfe der Router-Solicitation-Nachricht den lokalen Router zu ermitteln. Normalerweise werden Address-Mask-Reply-Nachrichten nur von Routern versandt.

Auch diese Nachrichten möchten Sie normalerweise nicht durch eine Firewall in Ihr geschütztes Netz lassen. Vielleicht möchten Sie Werkzeuge wie `sing -mask <ziel>` nutzen. Dann benötigen Sie die folgende Regel:

```
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p icmp --icmp-type address-mask-request ↵
  -m state --state NEW -j ACCEPT
```

34.11 ICMP echo-request/echo-reply (Ping)

Diese Nachrichten werden Sie sicherlich kennen. Wenn Sie auch nicht die Nachrichten kennen, so kennen Sie zumindest den Befehl, der diese Nachrichten erzeugt: `ping`. Der Ping-Befehl erzeugt eine `echo-request`-Nachricht und sendet diese an den Zielrechner. Dieser beantwortet sie mit einer `echo-reply`-Nachricht. Da hier die Nachrichten wieder in einem scheinbaren Client-Server-Verhältnis stehen, kann Iptables die Nachrichten auch so filtern. Jedes Echo-Request-Paket wird als neue Verbindung erkannt (State: NEW) und eingetragen. Jedes Echo-Reply-Paket wird

der entsprechenden Verbindung zugeordnet (State: ESTABLISHED) und beendet die Verbindung. So können die Echo-Nachrichten sicher von einer Iptables-Firewall gefiltert werden.

Hinweis

Der `ping`-Befehl auf einem Linux-System kann auch einen Broadcast-Ping durchführen. Manche Implementierungen erlauben auch einen Multicast-Ping. Hierbei wird der Echo-Request an die Broadcast- oder Multicast-Adresse geschickt. Sämtliche Rechner, die auf diese Anfrage reagieren (Unix, Router, kein MS Windows), antworten. Da nun aber nur eine Echo-Reply-Antwort von Iptables zugelassen wird und anschließend die Verbindung aus der Zustandstabelle gelöscht wird, ist ein Broadcast-Ping nicht möglich, wenn die Echo-Request- und Echo-Reply-Pakete zustandsorientiert gefiltert werden.

Mit der folgenden Regel erlauben Sie Ihren Benutzern, die Erreichbarkeit von Rechnern im Internet mit dem `ping`-Befehl zu testen:

```
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p icmp --icmp-type echo-request -m state ↵
  --state NEW -j ACCEPT
```

Häufig wird zusätzlich auch die Ping-Funktionalität beim Zugriff auf die DMZ gewünscht. Sie möchten aus Ihrem internen Netz und aus dem Internet prüfen, ob Ihr Webserver noch läuft.

```
$IPTABLES -A FORWARD -o $DMZDEV -p icmp --icmp-type echo-request -m state ↵
  --state NEW -j ACCEPT
```

Hier habe ich auf die Angabe der eingehenden Schnittstelle verzichtet. So wird nun jedes Echo-Request-Paket, das in die DMZ geroutet werden soll, akzeptiert. Dies erfolgt unabhängig davon, ob das Paket von innen oder von außen die Firewall erreicht hat.

Achtung

Gerade bei Ping ist die zustandsorientierte Filterung wichtig. Sie könnten auf die Idee kommen, grundsätzlich jedes Echo-Reply-Paket zu akzeptieren, um so auch Broadcast-Pings zu ermöglichen. Dann öffnen Sie aber möglichen Tunnel-Werkzeugen Tür und Tor. Es existieren eine Reihe von Werkzeugen, die auf der Basis von Echo-Paketen jedes beliebige Protokoll tunneln können. Eines der ersten Werkzeuge war `itunnel` von dem Hacker-Team Teso. Die zustandsorientierte Filterung würde diesen Tunnel nicht erlauben. Der Ping Tunnel (`ptunnel`, *http://www.cs.uit.no/~daniels/PingTunnel/*)

ist sicherlich das mächtigste aktuell verfügbare Werkzeug. Es kann sogar einen Tunnel trotz Anwendung der Zustandsüberwachung aufbauen und betreiben!

34.12 Traceroute

Traceroute ist keine ICMP-Nachricht. Dennoch habe ich den Befehl hier aufgenommen, da die Antworten der Traceroute-Funktion komplett auf ICMP-Nachrichten basieren. Vielleicht haben Sie sich schon immer gefragt, wie der Traceroute-Befehl funktioniert. Die folgende Ausgabe kennen Sie sicherlich:

```
[spenneb@bibo ~]$ traceroute www.bsd-training.de
traceroute to www.bsd-training.de (81.169.129.12), 30 hops max, 38 byte packets
 1  192.168.255.1 (192.168.255.1)  0.846 ms  0.764 ms  0.711 ms
 2  217.0.116.135 (217.0.116.135)  77.835 ms  46.357 ms  47.983 ms
 3  217.0.73.82 (217.0.73.82)  47.190 ms  46.582 ms  48.130 ms
 4  l-ea1.L.DE.net.DTAG.DE (62.154.89.122)  57.817 ms  57.110 ms  57.894 ms
 5  so-1-1-1-0.lpz2-j2.mcbone.net (62.104.199.89)  59.129 ms  58.560 ms  171.903 ms
 6  LO.bln2-g.mcbone.net (62.104.191.139)  61.900 ms  62.711 ms  60.838 ms
 7  strato-bln1.fdknet.de (194.97.172.146)  60.145 ms  59.459 ms  65.330 ms
 8  81.169.160.38 (81.169.160.38)  57.699 ms  58.237 ms  58.084 ms
 9  81.169.160.158 (81.169.160.158)  57.951 ms  57.246 ms  58.089 ms
10  bsd-training.de (81.169.129.12)  59.158 ms  59.379 ms  58.027 ms
```

Der Traceroute-Befehl ermittelt die Router, über die ein Paket sein Ziel erreicht. Dabei geht das nicht immer so gut wie in diesem Fall. Häufig werden ab einem bestimmten Zeitpunkt Sternchen (* * *) angezeigt. Dann filtert eine Firewall den Verkehr:

```
[spenneb@bibo ~]$ traceroute www.redhat.de
traceroute to www.redhat.de (66.187.229.16), 30 hops max, 38 byte packets
 1  192.168.255.1 (192.168.255.1)  0.871 ms  4.139 ms  0.940 ms
 2  217.0.116.135 (217.0.116.135)  49.293 ms  79.062 ms  47.944 ms
 3  217.0.73.82 (217.0.73.82)  46.832 ms  46.187 ms  48.056 ms
 4  f-ea2.F.DE.net.DTAG.DE (62.154.18.18)  53.053 ms  51.602 ms  52.912 ms
 5  62.156.139.146 (62.156.139.146)  55.010 ms  53.860 ms  55.884 ms
 6  ar1.str.de.colt.net (212.121.151.242)  63.789 ms  70.990 ms  57.906 ms
 7  * * *
 8  * * <Strg-C>
```

Was versendet der Traceroute-Befehl, und warum erhält er eine Antwort von den Routern auf dem Weg zum Ziel? Häufig hört man auch von langjährigen Administratoren Erklärungen, dass das Paket die Router unterwegs aufzeichne oder ähnlichen Unsinn. Im Grunde ist es ganz einfach. Der Befehl versendet ein IP-Paket mit der Zieladresse, die beim Aufruf angegeben wird. Um eine Antwort von den Routern und nicht vom Ziel zu erhalten, modifiziert der Befehl den TTL-Wert im

IP-Header des Pakets. Zunächst sendet der Befehl drei Pakete mit einem TTL-Wert von eins. Der erste Router reduziert den TTL-Wert um eins und muss das Paket verwerfen, da der TTL-Wert null erreicht hat. Zusätzlich sendet er eine ICMP-Time-Exceeded-Fehlermeldung an den Absender. Der Absender erhält also drei Fehlermeldungen von dem Router mit dessen IP-Adresse. Für die IP-Adresse führt der Befehl nun noch eine Rückwärts-Namensauflösung durch (außer Sie geben beim Aufruf des Befehls die Option `-n` an). Der Befehl gibt nun diese Informationen aus:

```
1  192.168.255.1 (192.168.255.1)  0.871 ms  4.139 ms  0.940 ms
```

Nun erzeugt der Befehl drei weitere Pakete, die sich nur in dem TTL-Wert unterscheiden. Dieser ist nun zwei. Der erste Router reduziert den TTL-Wert und routet das Paket weiter an den zweiten Router, der dann das Paket verwirft und nun die Time-Exceeded-Mitteilung mit seiner Absenderadresse verschickt. So erhält der Client die IP-Adresse des zweiten Routers.

Nun stellt sich die Frage, was für ein Paket der Traceroute-Befehl versendet? Ein IP-Paket mit wachsendem TTL-Wert, aber was für ein IP-Paket? Wenn Sie den Windows-`tracert.exe`-Befehl verwenden, handelt es sich um ein ICMP-Echo-Request-Paket. So kann der `tracert.exe`-Befehl leicht ermitteln, wann er das tatsächliche Ziel erreicht hat. Solange der TTL-Wert zu klein ist, um das Ziel zu erreichen, erhält er Time-Exceeded-Meldungen. Sobald das Ziel erreicht wurde, erhält der Befehl eine Echo-Reply-Nachricht.

Der Unix-`traceroute`-Befehl arbeitet anders, auch wenn einige Varianten (z.B. RedHat/Fedora) auch mit der Option `-I` ICMP-Echo-Request-Nachrichten verwenden können. Dieser Befehl versendet UDP-Pakete. UDP-Pakete benötigen einen Quell- und einen Zielport. Der Quellport wird zufällig gewählt (> 1023). Der Zielport wird nach einer einfachen Formel gewählt: BASE + TTL - 1. Der BASE-Wert kann beim Befehl mit der Option `-p` frei gewählt werden. Der Defaultwert ist 33434. Die Zielports liegen also im Bereich 33434-33689. Solange der TTL-Wert zu klein ist, um den Zielrechner zu erhalten, erhält der `traceroute`-Befehl eine Time-Exceeded-Nachricht. Sobald der Zielrechner erreicht wird, basiert die Portwahl auf der Hoffnung, dass auf diesen Ports kein Dienst horcht. Üblicherweise sendet dann ein Betriebssystem eine ICMP-Port-Unreachable-Nachricht zurück. So kann der `traceroute`-Befehl erkennen, dass er sein Ziel erreicht hat.

Wenn Sie nun die Traceroute-Funktionalität von innen über Ihre Firewall erlauben möchten, müssen Sie folgende Regeln verwenden:

```
# Akzeptiere Time-Exceeded-Nachrichten von außen. Für Windows und Unix
# erforderlich
$IPTABLES -A FORWARD -i $EXTDEV -o $INTDEV -p icmp --icmp-type time-exceeded -m state ↵
  --state RELATED -j ACCEPT

# Für Windows-tracert.exe erlaube echo-request-Pakete
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p icmp --icmp-type echo-request -m state ↵
  --state NEW -j ACCEPT
```

```
# Die folgende Regel akzeptiert die Antworten. Diese Regel ist in den meisten
# Skripten bereits vorhanden
$IPTABLES -A FORWARD -m state --state ESTABLISHED -j ACCEPT


# Für Unix-traceroute erlaube UDP-Pakete
$IPTABLES -A FORWARD -i $INTDEV -o $EXTDEV -p udp --dport 33434:33689 -m state↵
  --state NEW -j ACCEPT

# Erlaube Port-Unreachable-Nachrichten
# Dies ist meistens bereits der Fall, da von außen meistens alle Dest-Unreach
# Nachrichten akzeptiert werden
$IPTABLES -A FORWARD -i $EXTDEV -o $INTDEV -p icmp --icmp-type port-unreachable -m state↵
  --state RELATED -j ACCEPT
```

Die Firewall selbst wird nun in den Ausgaben der Traceroute-Befehle nicht auftauchen, da sie selbst nicht das Recht hat, Time-Exceeded-Nachrichten zu versenden. Statt der Firewall werden drei Sterne in der Ausgabe erscheinen. Wenn Sie möchten, dass auch die Firewall angezeigt wird, können Sie die folgende Regel hinzufügen:

```
$IPTABLES -A OUTPUT -o $INTDEV -p icmp --icmp-type time-exceeded -m state↵
  --state RELATED -j ACCEPT
```

Diese Regel erlaubt es der Firewall, das lokal erzeugte Time-Exceeded-Paket nach innen zu versenden.

34.13 Optimierung der ICMP-Regeln

Wenn Sie das ICMP-Protokoll so detailliert filtern möchten, wie ich es in diesem Kapitel beschrieben habe, ist es sinnvoll, die Regeln irgendwie ein wenig zu optimieren. Hierfür bieten sich die benutzerdefinierten Ketten an (siehe Abschnitt 9.3). Im Folgenden demonstriere ich das am Beispiel der ICMP-Pakete der FORWARD-Kette. Zunächst müssen Sie sicherstellen, dass auch Ihre ICMP-Regeln die Pakete tatsächlich betrachten können. Hierfür ist es wichtig, dass diese Regeln früh genug in der FORWARD-Kette betrachtet werden. Am einfachsten erstellen Sie zu Beginn Ihrer FORWARD-Kette die folgenden beiden Regeln:

```
$IPTABLES -A FORWARD -m state --state ESTABLISHED -j ACCEPT
$IPTABLES -A FORWARD -p icmp -j MY_ICMP
```

Die erste Regel akzeptiert sämtliche Pakete, die zu aufgebauten Verbindungen gehören. Dies sollte immer in jeder Kette die erste Regel sein, da die meisten Pakete in diese Kategorie gehören. Bei einer einfachen DNS-Anfrage ist es jedes zweite Paket, bei einer TCP-Verbindung sind es alle ab dem zweiten Paket. Das können schnell

auch mal mehrere hundert Pakete sein. Da Sie entscheiden, welche Verbindung aufgebaut werden darf (State: NEW), ist dies auch sicher.

Anschließend prüfen Sie in der zweiten Regel, ob es sich um ein ICMP-Paket handelt, und springen dann in die benutzerdefinierte Kette `MY_ICMP`. Diese müssen Sie nun anlegen und mit Regeln füllen. Wenn Sie meinem Rat folgen, werden Sie alle Destination-Unreachable-Meldungen von außen, alle Fragmentation-Needed-Meldungen, Time-Exceeded-Meldungen von außen (für Traceroute) und Echo-Request-Pakete von innen (für den Ping) zulassen. Ihre Regeln könnten dann folgendermaßen aussehen:

```
$IPTABLES -N MY_ICMP

# Destination-Unreachable von außen
$IPTABLES -A MY_ICMP -i $EXTDEV -p icmp --icmp-type destination-unreachable -m state ↵
  --state RELATED -j ACCEPT

# Fragmentation-Needed
$IPTABLES -A MY_ICMP -p icmp --icmp-type fragmentation-needed -m state --state RELATED ↵
  -j ACCEPT

# Time-Exceeded von außen für traceroute
$IPTABLES -A MY_ICMP -i $EXTDEV -o $INTDEV -p icmp --icmp-type time-exceeded -m state ↵
  --state RELATED -j ACCEPT

# Echo-Request von innen für ping
$IPTABLES -A MY_ICMP -i $INTDEV -o $EXTDEV -p icmp --icmp-type echo-request -m state ↵
  --state NEW -j ACCEPT

# Protokolliere Parameter-Problem und Source-Quench
$IPTABLES -A MY_ICMP -p icmp --icmp-type source-quench -j LOG --log-prefix "Source-Quench: "
$IPTABLES -A MY_ICMP -p icmp --icmp-type parameter-problem -j LOG ↵
  --log-prefix "Parameter-Problem: "

# Alle weiteren ICMP-Nachrichten werden unterdrückt
$IPTABLES -A MY_ICMP -j DROP
```

Die letzte Regel verwirft alle ICMP-Pakete, die im Vorfeld nicht akzeptiert wurden. Damit ist sichergestellt, dass am Ende dieser benutzerdefinierten Kette auch kein Rücksprung in die FORWARD-Kette erfolgt und dort möglicherweise noch Pakete akzeptiert werden oder einfach nur Prozessorleistung für unnötige Tests vergeudet wird.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

35 IPv6

Das IPv6-Protokoll wird bisher kaum eingesetzt. Dennoch unterstützt Iptables bereits das IPv6-Protokoll. Während die Linux-Kernel bis einschließlich 2.6.13 das IPv6-Protokoll nur wenig unterstützen, wird ab dem Kernel 2.6.14 eine wesentliche Änderung eintreten. Bei den älteren Kerneln unterstützt das Connection Tracking noch nicht das IPv6-Protokoll. Hierfür ist immer ein Patch des USAGI-Projekts erforderlich gewesen, da das Connection Tracking nur das IPv4-Protokoll unterstützt. Um nicht das ganze Connection Tracking für das IPv6-Protokoll erneut schreiben zu müssen, hat das Netfilter-Team diese Funktionalität komplett überarbeitet und neu geschrieben (siehe Kapitel 27), so dass nun auch bald das IPv6-Protokoll komplett unterstützt wird.

Aktuell ist dies aber leider noch nicht der Fall.

35.1 Filterung mit ip6tables

Der Befehl `ip6tables` funktioniert identisch zum Befehl `iptables`. Ihnen stehen leicht andere Tests und Ziele zur Verfügung. Eine große Anzahl der in Patch-O-Matic verfügbaren Patches sind auch für IPv6 verfügbar. Lediglich alle Funktionen, die auf dem Connection Tracking aufbauen, stehen nicht für IPv6 zur Verfügung. Dies wird sich aber in nächster Zukunft ändern. Dann können Sie auch diese Funktionen nutzen.

Im Moment haben Sie die folgenden Ziele im Kernel 2.6.14 zur Verfügung:

- `ACCEPT`, `DROP`, `RETURN` und `QUEUE`, da es sich hier um fest eingebaute Ziele handelt. Alle weiteren Ziele werden über ladbare Kernelmodule realisiert.
- `LOG`, `MARK`, `NFQUEUE`, `REJECT`, `ROUTE` und `TRACE` stehen, wie für das IPv4-Protokoll, zur Verfügung.
- `HL`: Dies ist ein Ziel, das nur für das IPv6-Protokoll zur Verfügung steht. Es wird weiter unten erläutert.

Diese Ziele können Sie in den drei Tabellen `raw`, `filter` und `mangle` einsetzen. Die Tabelle `nat` steht nicht zur Verfügung, da es (noch) keine Unterstützung für Connection Tracking und Network Address Translation gibt.

Um die Pakete zu prüfen, können Sie auf die folgenden Tests zurückgreifen:

- `-p`, `--protocol`, `-s`, `--source`, `-d`, `--destination`, `-i`, `--in-interface`, `-o`, `--out-interface` haben dieselbe Funktion wie bei IPv4.
- `-p icmpv6 --icmpv6-type`: Um das spezielle ICMPv6-Protokoll zu unterstützen, haben Sie hier einen eigenen Test.
- Erweiterungen, die identisch den Iptables-Erweiterungen funktionieren, sind:
  - `-m ah`
  - `-m esp`
  - `-m length`
  - `-m limit`
  - `-m mac`
  - `-m mark`
  - `-m multiport`
  - `-m owner`
  - `-m physdev`
- Neu hinzugekommen für das Protokoll IPv6 sind:
  - `-m dst`: Hiermit können Sie Optionen im IPv6-Destination-Header prüfen.
  - `-m eui64`: Dies prüft, ob der EUI64-Teil einer autokonfigurierten IPv6-Adresse stimmt.
  - `-m hbh`: Dies prüft den IPv6-Hop-by-Hop-Header.
  - `-m hl`: Dieser Test prüft das Hop-Limit-Feld im IPv6-Header.
  - `-m ipv6header`: Hiermit können Sie Optionen im IPv6-Header prüfen.
  - `-m rt`: Hiermit prüfen Sie den IPv6-Routing-Header.

35.2 Neue IPv6-Targets

35.2.1 HL

Mit diesem Ziel können Sie das IPv6-Hoplimit-Feld modifizieren. Der Hoplimit ist mit dem TTL-Feld des IPv4-Protokolls vergleichbar. Dieses Target darf nur in der Mangle-Tabelle eingesetzt werden. Die Verwendung des Targets ist gefährlich, da eine Erhöhung des Hoplimits Routing-Loops erzeugen kann.

Das Target hat die folgenden Optionen:

- `--hl-set <hops>`: Hiermit setzen Sie den Wert absolut.
- `--hl-dec <wert>`: Hiermit reduzieren Sie das Hoplimit um den angegebenen Wert.
- `--hl-inc <wert>`: Hiermit erhöhen Sie das Hoplimit um den angegebenen Wert.

35.3 Neue IPv6-Matches

35.3.1 dst

Mit diesem Test können Sie den IPv6-Destination-Header prüfen. Der Test hat zwei zusätzliche Optionen:

- `--dst-len <länge>`: Dies prüft die totale Länge des Headers.
- `--dst-opts <TYPE>[:<LEN>],[]`: Hiermit prüfen Sie einzelne Optionen und ihre Länge.

35.3.2 eui64

Wenn die IPv6-Adresse per Autokonfiguration zugewiesen wurde, enthalten die niedrigen 64 Bit der IP-Adresse die MAC-Adresse der Netzwerkkarte. Dieser Test prüft, ob das tatsächlich der Fall ist.

35.3.3 hbh

Hiermit können Sie die IPv6-Hop-by-Hop-Optionen testen. Die Option `--hbh-len <länge>` prüft die totale Länge, während Sie mit `--hbh-opts <Type>[:<länge>]` die einzelnen Optionen und ihre Länge prüfen können.

35.3.4 hl

Dieses Modul prüft das Hoplimit-Feld. Sie können prüfen, ob der Wert mit einem bestimmten Wert übereinstimmt, kleiner oder größer ist. Dieser Test ist mit dem `ttl`-Test vergleichbar.

- `--hl-eq <hops>`: Gleich.
- `--hl-lt <hops>`: Kleiner.
- `--hl-gt <hops>`: Größer.

35.3.5 ipv6header

Mit diesem Test können Sie die Optionen im IPv6-Header testen. Mit der Option `--header <headers>` können Sie die Header angeben, die in dem Paket enthalten oder nicht (`!`) enthalten sein müssen. Dabei müssen Sie alle Header angeben, damit der Test zutrifft. Wenn Sie nur einen Teil angeben möchten, müssen Sie zusätzlich die Option `--soft` definieren.

Sie können die folgenden Header testen: `hop`, `dst`, `route`, `frag`, `auth`, `esp`, `none`, `proto`.

35.4 rt

Dieser Test prüft den Routing-Header. Hierfür haben Sie die folgenden Optionen:

- `--rt-type <typ>`: Hiermit prüfen Sie den numerischen Typ des Routing-Headers.
- `--rt-segsleft <num>[<num>]`: Dies prüft das Segments-Left-Feld.
- `--rt-len <länge>`: Hiermit prüfen Sie die Länge des Headers.
- `--rt-0-res`: Dies prüft, ob das reservierte Feld gesetzt ist.
- `--rt-0-addrs <ip>[,<ip>]`: Dies prüft, ob im reservierten Feld (Typ 0) eine Adresse vorhanden ist.
- `--rt-0-not-strict`: Die letzte Option muss alle IP-Adressen im Routing-Header definieren. Wenn Sie lediglich eine prüfen möchten, müssen Sie zusätzlich diese Option angeben.

PEARSON Education

ADDISON-WESLEY

open source library

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und -Netzwerke

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

A Postfix-E-Mail-Relay

Eine komplette Beschreibung des Postfix-Mail-Transport-Agenten (MTA) würde den Rahmen dieses Buches sprengen und soll hier auch nicht durchgeführt werden. Alternative Literatur, auch in deutscher Sprache, existiert inzwischen reichlich im Internet und auch in Buchform. Hier möchte ich Ihnen nur kurz die Installation und Konfiguration eines einfachen E-Mail-Relays vorstellen, das Sie für den Austausch der E-Mails in der DMZ nutzen können.

A.1 Postfix als E-Mail-Relay

Der Postfix-MTA besitzt zwei wesentliche Konfigurationsdateien: `/etc/postfix/master.cf` und `/etc/postfix/main.cf`. Die Konfiguration des Postfix als Relay kann damit sehr einfach durchgeführt werden. Sie müssen lediglich in der Datei `/etc/postfix/main.cf` einige Parameter anpassen.

Zunächst sollten Sie dafür sorgen, dass die Parameter `myhostname` und `mydomain` für Ihren Mailserver passen. Tragen Sie hier den Namen Ihres Postfix-Servers und der Domäne ein, für die der Postfix als Relay arbeiten soll. Der Zugriff auf den Postfix-Mailserver in der DMZ soll nicht direkt durch die Clients erfolgen, sondern Sie verwenden intern in Ihrem Netzwerk einen eigenen Mailserver. Dies kann ein beliebiges Produkt (auch ein Microsoft Exchange Server) sein. Erzeugen Sie in der Datei eine eigene Variable, `internal_mail`, und weisen Sie dieser die IP-Adresse Ihres internen Mailservers zu. Die Variable `inet_interfaces` setzen Sie entweder auf `all` oder `$myhostname`, damit Postfix auch tatsächlich über das Netzwerk E-Mails entgegennimmt. Häufig ist dieser Parameter auf Localhost beschränkt!

Damit Postfix nun E-Mails aus dem Internet für Ihre Domäne annimmt, setzen Sie den Parameter `mydestination=$mydomain`. Damit Postfix E-Mails von Ihrem internen Mailserver zur Weiterleitung in das Internet annimmt, tragen Sie Ihren internen Mailserver in der Variable `mynetworks` ein: `mynetworks = $internal_mail, 127.0.0.0/8`. Prüfen Sie, ob die Variable `smtpd_recipient_restrictions = permit_mynetworks, reject_unauth_destination` gesetzt ist. Das bedeutet, dass Clients in der Gruppe `mynetworks` jeden beliebigen Empfänger in der E-Mail verwenden dürfen. Alle anderen Clients dürfen nur an die Domänen senden, für die Postfix zuständig ist (`mydestination`).

Nun müssen Sie Postfix noch sagen, wie er die E-Mails für Ihre Domäne zustellen soll. Hierzu setzen Sie den Parameter `transport_maps = hash:/etc/postfix/transport`. In

dieser Datei müssen Sie nun alle Domänen eintragen, die Postfix zum internen Mailserver weiterleiten soll. Legen Sie also die Datei mit folgendem Inhalt an:

```
example.com    smtp:[ip_internal_mail]
```

Ersetzen Sie dabei `example.com` durch Ihre Domäne und `ip_internal_mail` durch die IP-Adresse Ihres internen E-Mail-Servers. Achten Sie darauf, dass die eckigen Klammern gesetzt sind! Haben Sie die Datei erzeugt, erzeugen Sie die Hash-Datenbank mit `postmap /etc/postfix/transport`.

Das wars. Herzlichen Glückwunsch. Jetzt müssen Sie nur noch Ihren internen Mailserver so konfigurieren, dass er die E-Mails nicht direkt in das Internet zustellt, sondern an dieses Postfix-E-Mail-Relay. Ist der interne E-Mail-Server ein Sendmail-Server, so müssen Sie den Smart-Host setzen. Ist er ein Postfix-Server, heißt der Parameter `relayhost`.

A.2 Adressverifizierung

Wenn Sie das Relay so betreiben, werden Sie schnell den Spaß verlieren, da das Postfix-Relay zunächst jede E-Mail annimmt und zum internen System zustellt. Das Postfix-Relay führt keine Verifizierung der E-Mail-Adresse durch. Dadurch werden auch E-Mails an nicht existente Benutzer angenommen und nach innen weitergeleitet. Dies führt zu Fehlermeldungen auf dem internen System und einer Bounce-E-Mail. Diese Bounces werden auch als Spam angesehen, und Sie landen mit Ihrem Relay recht schnell auf der einen oder anderen Spam-Block-Liste (häufig auch Blacklist genannt).

Damit das nicht passiert, müssen Sie die Empfänger überprüfen. Postfix bietet hier zwei Möglichkeiten. Entweder stellen Sie die Empfängerliste direkt Postfix zur Verfügung, oder Sie verwenden den Verify-Server.

Um Postfix die Liste der gültigen Empfänger zur Verfügung zu stellen, benutzen Sie den Parameter `local_recipient_maps` und übergeben diesem eine Datei. Sie können auch LDAP oder SQL-Datenbanken hier einbinden. Sie finden weitere Informationen unter *http://www.postfix.org/LOCAL_RECIPIENT_README.html*.

Angenehmer ist die Verwendung des Verify-Servers. Diese Funktion in Postfix verzögert zunächst jede E-Mail an einen unbekannten lokalen Empfänger. Gleichzeitig versucht Postfix eine scheinbare Zustellung an den internen Mailserver. Lässt dieser eine Zustellung an den Benutzer zu, merkt sich Postfix diesen Benutzer und nimmt auch für diesen Benutzer E-Mails an. Lässt der interne Mailserver die Zustellung für diesen Benutzer nicht zu, lehnt auch Postfix die E-Mail ab. Das Ergebnis speichert Postfix in der Address Verification Database.

Um diese Funktion zu aktivieren, müssen Sie lediglich den Parameter `smtpd_recipient_restrictions` in der Datei `/etc/postfix/main.cf` modifizieren:

```
smtpd_recipient_restrictions =
        permit_mynetworks
```

```
        reject_unauth_destination
        reject_unknown_recipient_domain
        reject_unverified_recipient
```

Postfix wird zunächst jeden Benutzer, der von dem internen Mailserver abgelehnt wird, nur temporär mit dem Fehler 450 ablehnen. Das bedeutet, dass die Clients später erneut eine Zustellung versuchen sollen. Wenn Sie die Protokolle eine Weile beobachtet haben und sicher sind, dass Postfix alles richtig macht, können Sie den Fehlercode ändern:

```
unverified_recipient_reject_code = 550
```

A.3 Amavisd-New

Für eine zusätzliche Filterung auf einem Postfix-Mail-Relay bietet sich Amavisd-New (*http://www.ijs.si/software/amavisd/*) an. Viele Distributionen enthalten bereits ein Amavisd-New-Paket. Für alle anderen können Sie von der Homepage ein Paket herunterladen. Installieren Sie das Paket nach der Anleitung. Je nach Ihrer Distribution müssen Sie einige Pakete der Distribution oder aus dem Internet nachinstallieren, die Amavisd-New vorraussetzt. Amavisd-New kann einen Virenscan und auch eine Spam-Analyse über SpamAssassin durchführen und benötigt dafür auch die entsprechenden Pakete.

Die Filterung mit Amavisd-New erfolgt als externes Mail-Relay (Abbildung A.1). Postfix nimmt die E-Mail zunächst entgegen und prüft die DNS-Namen und Adressen. Dann übergibt Postfix per SMTP die E-Mail an Amavisd-New, das als lokaler Dienst auf dem Port 10024 läuft. Dieses zerlegt die E-Mail und scannt die E-Mail mit einem Virenscanner und SpamAssassin. Wird ein Virus gefunden, nimmt Amavisd-New die E-Mail in Quarantäne. Ist das nicht der Fall, so übergibt Amavisd-New die E-Mail wieder per SMTP an eine zweite Postfix-Instanz auf Port 10025. Diese wird so konfiguriert, dass keine erneuten Prüfungen der E-Mail durchgeführt werden und die E-Mail direkt weitergeleitet wird.

Für die Konfiguration müssen Sie zwei Einträge in der Postfix-Konfigurationsdatei `/etc/postfix/master.cf` hinzufügen:

```
127.0.0.1:10025 inet n - y - - smtpd
    -o content_filter=
    -o local_recipient_maps=
    -o smtpd_helo_restrictions=
    -o smtpd_client_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks, \
reject_unauth_destination
    -o mynetworks=127.0.0.0/8

smtp-amavis unix - - y - 2 smtp
```

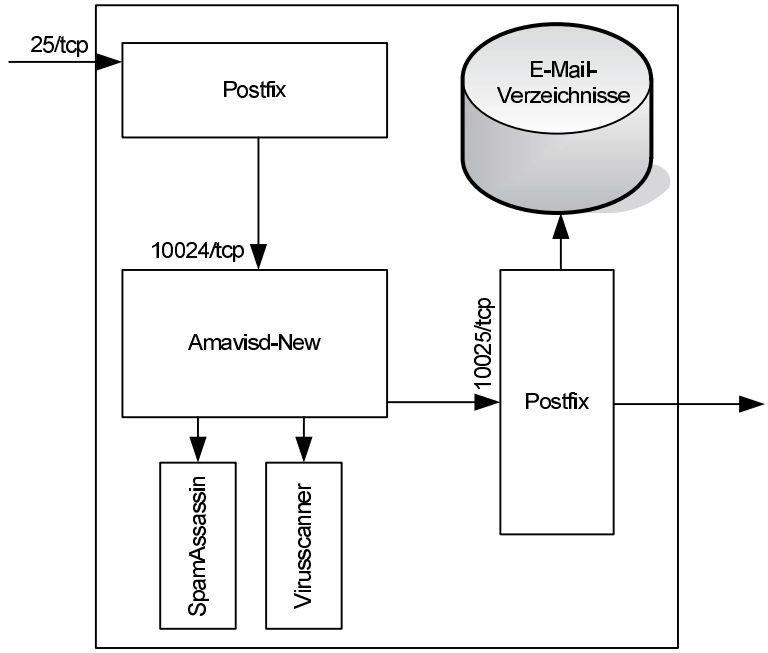


Abbildung A.1: Amavisd wird als Content-Filter über SMTP eingebunden.

```
-o smtp_data_done_timeout=1200
-o disable_dns_lookups=yes
```

Zusätzlich müssen Sie einen Eintrag in der Datei `/etc/postfix/main.cf` hinzufügen:

```
content_filter = smtp-amavis:[127.0.0.1]:10024
```

Damit weisen Sie Postfix an, als Content-Filter Amavisd-New zu verwenden.

Nun können Sie Amavisd-New in der Konfigurationsdatei `/etc/amavisd.conf` konfigurieren und anpassen. Diese Datei ist sehr gut kommentiert. In den meisten Fällen entspricht die Default-Konfiguration bereits den meisten Ansprüchen.

B Firewall-Skript

In diesem Kapitel finden Sie ein Skript zum Stoppen der Firewall.

B.1 Stopp der Firewall

Dieses Skript stoppt die Firewall. Es nimmt ein Argument entgegen. Dieses Argument kann entweder `stop` oder `panic` sein. Mit `stop` setzt das Skript den Rechner in den Ausgangszustand zurück. Alle Ketten werden geleert, alle benutzerdefinierten Ketten gelöscht, alle Policies auf `ACCEPT` gesetzt und das Routing deaktiviert. Bei dem Argument `panic` handelt es sich um die gleichen Schritte mit dem Unterschied, dass anschließend alle Policies der Ketten auf `DROP` gestellt werden.

Hinweis

Dieses Skript ist auch auf der CD im Verzeichnis »Beispielskripte« vorhanden.

```
#!/bin/sh
# Dieses Skript stoppt die Firewall
#
# (c) 2005 Ralf Spenneberg
# OpenSource Training
# http://www.opensource-training.de
#
#
IPTABLES=/sbin/iptables
SYSCTL=/sbin/sysctl


flush_und_loeschen() {
    # Flush
    # Check if firewall is configured (has TABLES)
    TABLES=$(cat /proc/net/ip_tables_names 2>/dev/null)
```

```
    [ -z "$TABLES" ] && return 1

    echo -n $"Lösche Firewall-Regeln und benutzerdefinierte Ketten: "
    ret=0
    # Für alle Tabellen
    for i in $TABLES; do
        # Flush
        $IPTABLES -t $i -F;
        let ret+=$?;

        # Loesche Ketten
        $IPTABLES -t $i -X;
        let ret+=$?;

        # Reset Zaehler
        $IPTABLES -t $i -Z;
        let ret+=$?;
    done

    [ $ret -eq 0 ] && echo "OK" || echo "Fehler"
    echo
    return $ret
}

setze_policy() {
    # Setze die Policy auf den Übergabeparameter
    policy=$1

    TABLES=$(cat /proc/net/ip_tables_names 2>/dev/null)
    [ -z "$TABLES" ] && return 1
    echo -n $"Setze die Policy der Ketten auf $policy: "
    ret=0
    for i in $TABLES; do
        echo -n "$i "
        case "$i" in
            filter)
                $IPTABLES -t filter -P INPUT $policy \
                    && $IPTABLES -t filter -P OUTPUT $policy \
                    && $IPTABLES -t filter -P FORWARD $policy \
                    || let ret+=1
                ;;
            nat)
                $IPTABLES -t nat -P PREROUTING $policy \
                    && $IPTABLES -t nat -P POSTROUTING $policy \
                    && $IPTABLES -t nat -P OUTPUT $policy \
```

```
                    || let ret+=1
                ;;
            mangle)
                $IPTABLES -t mangle -P PREROUTING $policy \
                    && $IPTABLES -t mangle -P POSTROUTING $policy \
                    && $IPTABLES -t mangle -P INPUT $policy \
                    && $IPTABLES -t mangle -P OUTPUT $policy \
                    && $IPTABLES -t mangle -P FORWARD $policy \
                    || let ret+=1
                ;;
            *)
                let ret+=1
                ;;
        esac
    done

    [ $ret -eq 0 ] && echo " OK" || echo " Fehler"
    echo
    return $ret
}

case "$1" in
    stop)
        flush_und_loeschen
        setze_policy ACCEPT
        RETVAL=$?
        ;;
    panic)
        flush_und_loeschen
        setze_policy DROP
        RETVAL=$?
        ;;
    *)
        echo $"Usage: $0 {stop|panic}"
        exit 1
        ;;
esac

exit $RETVAL
```

C Netzwerkgrundlagen

Dieses Kapitel soll eine kurze Einführung in die im Internet verwendeten Protokolle geben. Es soll sowohl als Einführung wie auch als Wiederauffrischung und als Nachschlagekapitel dienen. Die wesentlichen Punkte, um die Netzwerkprotokolle im Zusammenhang mit der Intrusion Detection zu verstehen, sollen erklärt werden. Ausführliche Darstellungen finden Sie in [29] und [11].

C.1 TCP/IP

Die TCP/IP-Protokollfamilie wird seit 1973 entwickelt. 1978 wurde die Version IPv4 fertig gestellt. Diese Version findet heute die meiste Verwendung. Ab 1982 wurde das damalige ARPANET auf das neue Protokoll IP umgestellt. Heutzutage ist TCP/IP das im Internet verwendete Protokoll. Viele Firmen haben in den vergangenen Jahren ihre Netze ebenfalls auf TCP/IP umgestellt, um so intern Internetähnliche Dienste anbieten zu können und eine einfache Kommunikation auch mit dem Internet zu ermöglichen.

Das OSI-Referenzmodell wird verwendet, um die Netzwerkprotokolle in sieben verschiedene Schichten aufzuteilen. Hierbei handelt es sich um die folgenden Schichten: Physical, Data-Link, Network, Transport, Session, Presentation und Application. Das TCP/IP-Protokoll wurde vor dem OSI-Modell entwickelt. Es besitzt daher nicht diese exakte Unterteilung in sieben Schichten, sondern verwendet nur vier Schichten:

1. Netzzugang: Diese Schicht entspricht im OSI-Modell der Schicht 1 und 2.
2. Internet: Diese zweite Schicht des TCP-Modells entspricht im OSI-Modell der Schicht 3. Hier arbeitet das IP-Protokoll. Daher wird häufig umgangsprachlich auch von der Schicht 3 gesprochen, wenn das IP-Protokoll gemeint ist.
3. Transport: Dies entspricht der Schicht 4 des OSI-Modells. Hier arbeiten die Protokolle TCP und UDP.
4. Anwendung: Diese Schicht bildet die Schichten 5-7 des OSI-Modells ab. Hier arbeiten die Applikationsprotokolle wie HTTP, Telnet, FTP etc.

C.2 IP

Das Internet Protocol (IP, RFC 791, STD 5) ist dafür verantwortlich, IP-Datagramme in Paketen von einer Quelle zu einem Zielrechner zu übertragen. Hierbei kümmert sich das IP-Protokoll um die Zustellung des Pakets zu diesem Zielrechner. Die revolutionäre Neuerung bei der Einführung des IP-Protokolls war die Tatsache, dass eine IP-Kommunikation keine dedizierte Verbindung (circuit switched network) mehr benötigte, sondern die Daten in einzelnen Paketen (packet switched network) unabhängig ihr Ziel erreichten (Abbildung C.1).

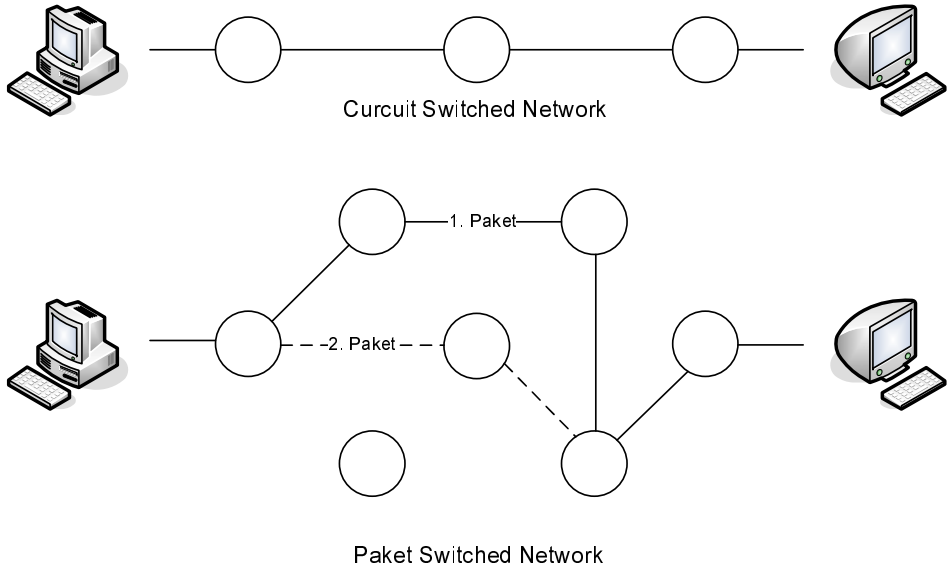


Abbildung C.1: Im Paket-Switched Network können die Pakete über unterschiedliche Wege das Ziel finden.

Dies ermöglicht es, die Kommunikation bei Ausfall redundanter Netzwerkkomponenten durch dynamische Routing-Protokolle aufrechtzuerhalten. Diese sind in der Lage, den Ausfall zu erkennen und die Daten über andere Knoten weiterhin zu übermitteln. Die hierzu benötigten Informationen werden im IP-Header des Pakets abgespeichert (Abbildung C.2). Dennoch ist IP ein Protokoll, das die Zustellung des Pakets nicht garantiert und überprüft. Es wird auch als Best-Effort-Protokoll bezeichnet. Die höheren Protokolle oder die Anwendungen müssen die erfolgreiche Übertragung prüfen, wenn dies erforderlich ist.

Die Felder und ihre Bedeutung sollen nun kurz vorgestellt werden.

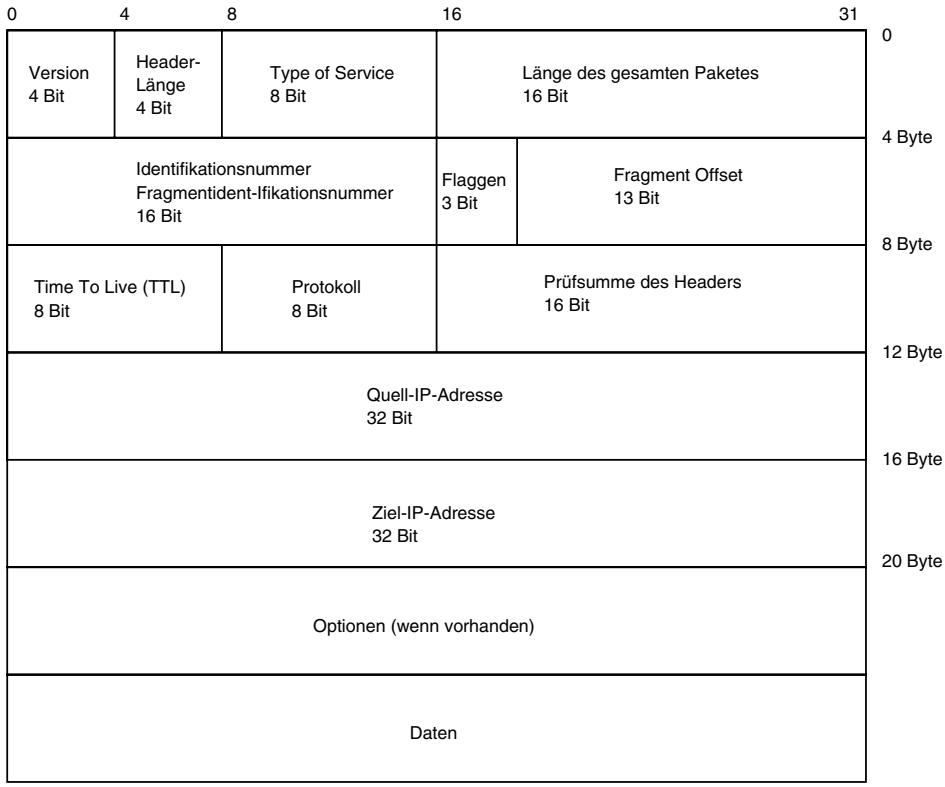


Abbildung C.2: IP-Header Version 4

C.2.1 Version

Dieses Feld ist vier Bits lang. Es enthält die IP-Version. Üblicherweise enthält dieses Feld im Moment die Zahl 4. Jedoch werden in der nahen Zukunft sicherlich vermehrt auch IPv6-Pakete auftreten. Diese enthalten dann hier die Zahl 6.

C.2.2 Header-Länge

Dieses Feld enthält die Länge des Headers. Es ist selbst 4 Bits lang. Jedoch wird die Länge nicht in Bits oder Bytes gemessen, sondern in Doppelworten. Ein Doppelwort entspricht 4 Bytes oder 32 Bits. Ein üblicher IP-Header ohne Optionen ist 20 Bytes lang. Daher befindet sich bei den meisten Paketen hier eine 5. Weist der Header weitere IP-Optionen auf (z.B. Source Routing, s.u.), so befindet sich hier entsprechend eine größere Zahl. Der Header kann maximal eine Länge von 15 (4 Bits) Doppelworten, also 60 Bytes einnehmen.

C.2.3 Type-of-Service

Das Type-of-Service-Feld ist 8 Bits lang. Es steht seit der Entwicklung des IPv4-Protokolls zur Verfügung. Es wurde ursprünglich implementiert, um eine Art Quality-of-Service zu bieten. Es wird heutzutage nur von wenigen Anwendungen gesetzt. Die Anwendungen unter Linux nutzen es jedoch recht häufig. Dennoch unterstützen nur wenige Router im Internet seine Auswertung. Eine Verwendung durch die Anwendungen hat daher nur wenig Auswirkung auf den tatsächlichen Transport des Pakets. Es existieren die folgenden Werte: Minimize-Delay 16 (0x10), Maximize-Throughput 8 (0x08), Maximize-Reliability 4 (0x04), Minimize-Cost 2 (0x02) und Normal-Service 0 (0x00). Sie werden heute abgelöst durch Diffserv und ECN (s.u.).

C.2.4 Gesamtpaketlänge

Dieses Feld definiert die Gesamtpaketlänge in Bytes. Das Feld ist 16 Bit lang, daher kann ein Paket maximal 65.535 Byte lang sein. Üblicherweise sind die übertragenen Pakete wesentlich kleiner, da die Übertragungsmedien nicht in der Lage sind, derartig große Pakete zu transportieren.

C.2.5 Identifikationsnummer

Jedes Paket wird üblicherweise mit einer eindeutigen 16 Bit langen Identifikationsnummer verschickt. Dies erfolgt, damit im Falle einer Fragmentierung der Empfänger die Fragmente eines Pakets zuordnen kann. Daher wird in der Literatur häufig bei einem nicht fragmentierten Paket von der IP-Identifikationsnummer und bei einem fragmentierten Paket von der Fragment-Identifikationsnummer gesprochen.

Der Absender inkrementiert diese Zahl üblicherweise immer um 1. Hiermit sind jedoch gespoofte Portscans möglich (siehe Abschnitt »Gespoofter Portscan« auf Seite 63). Daher existieren einige Betriebssysteme (z.B. OpenBSD), die diese Zahl zufällig vergeben. Der aktuelle Linux-Kernel 2.4 setzt diesen Wert auf null, wenn das Paket gleichzeitig das DF-Flag (s.u.) gesetzt hat. In diesem Fall darf das Paket nicht fragmentiert werden, daher hat diese Zahl auch keinen Sinn.

C.2.6 Flaggen

Der IP-Header enthält drei Bits, die Informationen über die Fragmentierung des Pakets enthalten.

Das erste dieser drei Bits wird momentan nicht verwendet und muss immer null sein.

Das folgende Bit ist das *Don't Fragment*-(DF-)Bit. Ist dieses Bit gesetzt (1), so darf das Paket nicht fragmentiert werden. Ein Router, der dieses Paket aufgrund seiner Größe nicht zustellen kann, muss das Paket verwerfen und eine ICMP-Fehlermeldung an den Absender schicken.

Das dritte und letzte Bit ist das *More Fragments follow*-(MF-)Bit. Dieses Bit zeigt an, dass weitere Fragmente folgen. Beim letzten Fragment und allen nicht fragmentierten Paketen ist dieses Bit gelöscht.

C.2.7 Fragment-Offset

Dieses Feld gibt bei einem Fragment dessen Beginn im Gesamtpaket an. Hierbei erfolgt die Angabe in Vielfachen von 8. Das bedeutet, dass ein Fragment (außer dem letzten) immer eine Länge aufweisen muss, die durch 8 ohne Rest teilbar ist. Das Feld ist 13 Bit lang und kann damit den ganzen Bereich von maximal 65.535 Bytes eines Pakets abdecken.

Der Empfänger verwendet diese Information, um das Paket in der richtigen Reihenfolge zusammenzusetzen.

Der Ping of Death nutzte Fragmente, um den TCP/IP-Stack einiger Betriebssysteme mit einem Bufferoverflow zum Absturz zu bringen. Es ist möglich, Fragmente so zu konstruieren, dass bei der Defragmentierung ein Paket größer 65.535 Bytes entsteht. Dies ist möglich, da das erste Fragment eine Größe von 1500 Bytes aufweist. Jedes weitere Fragment ist 1480 Byte lang. 1500 Bytes plus 43 mal 1480 Bytes ergeben 65.140 Bytes. Nun kann ein weiteres Fragment erzeugt werden, das erneut 1480 Byte lang ist. Erlaubt wären jedoch nur noch 395. Bei der Defragmentierung kommt es daher zum Bufferoverflow. Dieser Angriff erhielt den Namen Ping of Death, da es besonders einfach war, mit dem Kommando `ping` diese Pakete zu erzeugen.

C.2.8 Time To Live (TTL)

Bei dem Feld Time To Live handelt es sich um ein 8 Bit langes Feld. Es kann somit Werte von 0 bis 255 aufnehmen. Dieser Wert wird von jedem Router, der das Paket weiterleitet, gelesen und pro Hop um 1 dekrementiert. Erreicht hierbei das Feld den Wert null, so muss der Router das Paket verwerfen und eine Fehlermeldung an den Absender zurücksenden.

Diese Funktion erlaubt es, mit dem Werkzeug `traceroute` die Route eines Pakets zu ermitteln. Hierzu werden Pakete mit steigenden TTL-Werten an den Zielrechner gesendet. Jeder Router wird entsprechende Pakete verwerfen müssen und eine Fehlermeldung an den Absender schicken. So wird die IP-Adresse eines jeden Routers ermittelt.

Diese Funktion eignet sich jedoch auch zur Verwirrung von IDS-Systemen und zur Ermittlung von Firewall-Regeln. Hierzu werden spezielle Pakete erzeugt. Diese weisen eine TTL auf, so dass die Firewall beziehungsweise das IDS-System die Pakete sieht, sie aber nie den entsprechenden Empfänger erreichen. Bei dem *Firewalking* handelt es sich um eine ähnliche Technik.

Verschiedene Betriebssysteme verwenden üblicherweise unterschiedliche Standard-TTL-Werte. Linux verwendet 64.

C.2.9 Protokoll

IP ist in der Lage, eine große Anzahl von Protokollen zu übertragen. Dies sind zum Beispiel ICMP (1), TCP (6) und UDP (17). Dieses Feld gibt die Nummer des enthaltenen Protokolls an. Unter Linux werden alle Nummern in der Datei `/etc/protocols` aufgeführt.

Werden ungewöhnliche Protokolle im Netzwerk entdeckt, so kann es sich hierbei auch um einen Tunnel handeln. Das Honeynet Project hat ein Werkzeug entdeckt, das zum Beispiel einen NVP-(11-)Tunnel aufbaut.

C.2.10 Prüfsumme

Dies ist die Prüfsumme des IP-Headers des Pakets. Hiermit können Netzwerkgeräte und auch der Empfänger die Validität des Paket-Headers bestimmen. Die Prüfsumme enthält nicht den Datenanteil des Pakets. Da einige Werte des Headers sich während der Übertragung ändern (z.B. TTL), wird diese Prüfsumme von jedem Netzwerkgerät (z.B. Router), das Änderungen durchführt, neu berechnet. Pakete mit fehlerhaften Header-Prüfsummen können daher nur im lokalen Netzwerk erzeugt worden sein. Der Empfänger verwirft Pakete mit fehlerhaften Prüfsummen. Dies kann verwendet werden, um ein IDS-System zu verwirren, wenn dieses keine Prüfsummenermittlung durchführt.

C.2.11 Quell-IP-Adresse

Dieses Feld enthält die IP-Adresse des Absenders. Wenn beim Transport des Pakets ein Source-NAT (Network Address Translation) durchgeführt wurde, befindet sich hier die entsprechende Adresse. Ein Source-NAT ist im Header nicht erkennbar.

C.2.12 Ziel-IP-Adresse

Dieses Feld enthält die IP-Adresse des Empfängers. Wenn beim Transport des Pakets ein Destination-NAT (Network Address Translation) durchgeführt wurde, befindet sich hier die entsprechende Adresse. Ein Destination-NAT ist im Header nicht erkennbar.

C.2.13 IP-Optionen

Sämtliche für den Transport des IP-Pakets erforderlichen Informationen werden in den 20 Bytes des IP-Headers gespeichert. Jedoch besteht gelegentlich die Notwendigkeit, zusätzliche Informationen zu senden, die das Verhalten des IP-Protokolls modifizieren. Diese werden als Option übertragen. Insgesamt können 40 Bytes Optionen übertragen werden. Standardmäßig werden keine Optionen verwendet.

Die Optionen bestehen aus einem Byte, das den Typ definiert, einem Byte für die Länge und entsprechenden Bytes für die Daten. Abbildung C.3 veranschaulicht das.

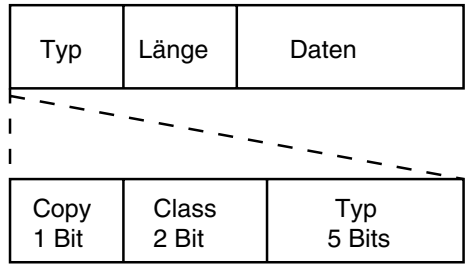


Abbildung C.3: IP-Optionen-Aufbau

End of Optionlist

Dies definiert das Ende der Optionenliste. Es ist eine Option der Klasse 0 und des Typs 0. Diese Option besitzt kein Längenfeld und kein Datenfeld.

No Operation

No Operation ist eine Option der Klasse 0 mit Typ 1. Sie wird verwendet, um die Optionenliste aufzufüllen. Die Länge des IP-Headers kann nur in Doppelworten angegeben werden. Wenn die Länge der Optionen nicht durch 4 teilbar ist, werden sie mit dieser Option aufgefüllt. Diese Option weist weder ein Längenfeld noch ein Datenfeld auf.

Security Options

Diese Option der Klasse 0 mit Typ 2 ist 88 Bits lang und wird für militärische Zwecke genutzt. Üblicherweise wird diese Option nicht im Internet beobachtet. Sie hat keine Verwandtschaft mit IPsec.

Record Route

Diese Option verwendet die Klasse 0 und den Typ 7. Router, die diese Option im Paket erkennen, sollen ihre IP-Adresse im IP-Header aufzeichnen. Da die Größe des IP-Headers beschränkt ist, können hier nur maximal acht Router ihre IP-Adressen eintragen. Daher wird diese Funktion nur selten im Internet genutzt und stattdessen auf `traceroute` zurückgegriffen. Während diese Funktion jedoch für jedes Paket tatsächlich die Route protokolliert, zeigt `traceroute` nur die wahrscheinliche Route an.

Loose Source Routing

Loose Source Routing ist eine Option der Klasse 0 und mit Typ 3. Die Größe dieser Option hängt von der Anzahl der angegebenen Router ab. Loose Source Routing erlaubt es dem Absender, eine Liste von Routern im IP-Header anzugeben, über die das Paket neben anderen transportiert wird. Es können aus Platzgründen maximal

acht Router angegeben werden. Verschiedene Befehle unterstützen diese Funktion: `traceroute`, `netcat` etc.

Loose Source Routing erlaubt es, Pakete zu routen, die ansonsten nicht geroutet werden würden. Es erlaubt zum Beispiel, auf den meisten Internet-Routern Pakete an RFC-1918-Netze (z.B. 192.168.0.0/24) zu routen. So kann ein Angreifer von außen ein Paket an diese Adresse senden und eine Loose Source Route angeben, damit die Internet-Router auch wissen, wohin das Paket gesendet werden soll.

Strict Source Routing

Strict Source Routing ist eine Option mit der Klasse 0 und mit Typ 9. Hier definiert die Liste die exakte Abfolge der zu verwendenden Router. Es dürfen keine weiteren Router verwendet werden.

Router Alert

Diese Option (Klasse 0, Typ 20) definiert, dass der Router das Paket modifizieren muss, bevor er es weiterroutet. Es wird für experimentelle Erweiterungen genutzt.

TimeStamp

Diese Option (Klasse 2, Typ 4) verlangt, dass der Router ähnlich der Record-Route-Option seine IP-Adresse im Header ablegt, aber zusätzlich noch die Zeit hinterlegt, zu der das Paket verarbeitet wurde.

Es besteht die Möglichkeit, nur die Timestamps oder Router-IP-Adressen und Timestamps anzufordern.

C.3 UDP

Das User Datagram Protocol (UDP, RFC 768, STD 6) stellt eines der beiden am häufigsten eingesetzten Protokolle auf Basis von IP dar. Die meisten Internetapplikationen verwenden TCP (s.u.). TCP garantiert die vollständige und korrekte Übertragung der Daten. Hierzu generiert es jedoch einen gewaltigen Overhead. Viele Anwendungen benötigen diese Garantie nicht oder können sie gar nicht nutzen, da es sich um Multicast- oder Broadcast-Anwendungen handelt, bei denen ein Paket gleichzeitig an mehrere Empfänger zugestellt wird. In diesen Fällen wird meist das UDP-Protokoll verwendet.

UDP ist ein unzuverlässiges und Datagramm-orientiertes Protokoll. Es garantiert weder die Ablieferung eines Datagramms noch bietet es Vorkehrungen gegen eine Duplizierung oder eine Vertauschung der Reihenfolge der Daten. Aufgrund seiner Unzuverlässigkeit bieten die höheren Protokolle meist eine gewisse Fehlerkontrolle. Dies äußert sich oft in einer gewissen Unempfindlichkeit gegenüber verlorenen Paketen. Wenn zum Beispiel ein Paket bei einer Videostreaming-Anwendung verloren geht, so macht sich das meistens nur durch ein leichtes Zittern der Darstellung be-

merkbar. Eine TCP-ähnliche Fehlerkontrolle mit einer erneuten Sendung des Pakets würde meist zu einem Stottern und Anhalten des Streams führen.

UDP ist nur in der Lage, ein Datagramm gleichzeitig zu verarbeiten. Wenn gewisse Informationen mit UDP versendet werden, so werden diese nicht bereits von UDP sinnvoll auf einzelne Pakete aufgeteilt (TCP teilt die Daten entsprechend der MSS-Maximum Segment Size auf, s.u.), sondern es werden unter Umständen sehr große UDP-Datagramme gebaut, die anschließend von der darunter liegenden IP-Schicht auf IP-Paketfragmente aufgeteilt werden müssen.

Um mehreren Anwendungen die Verwendung des UDP-Protokolls zu ermöglichen, verwendet UDP einen Multiplexer. Client- wie Server-Anwendungen müssen sich vor der Verwendung des UDP-Protokolls registrieren. Während dieser Registrierung weist die UDP-Schicht diesen Anwendungen einen Port zu. Die Verwendung der Ports durch die verschiedenen Dienste ist grundsätzlich willkürlich, jedoch haben sich im Laufe der Jahre bestimmte Ports für bestimmte Dienste etabliert. Die Zuweisung der Ports zu den einzelnen Diensten erfolgt durch die Internet Assigned Number Authority (IANA), die die Liste der *well-known ports* pflegt (*http://www.iana.org/assignments/port-numbers*).

Der UDP-Header (Abbildung C.4) ist acht Byte lang. Er enthält den Quell- und den Zielport, die Datagrammlänge und eine Prüfsumme.

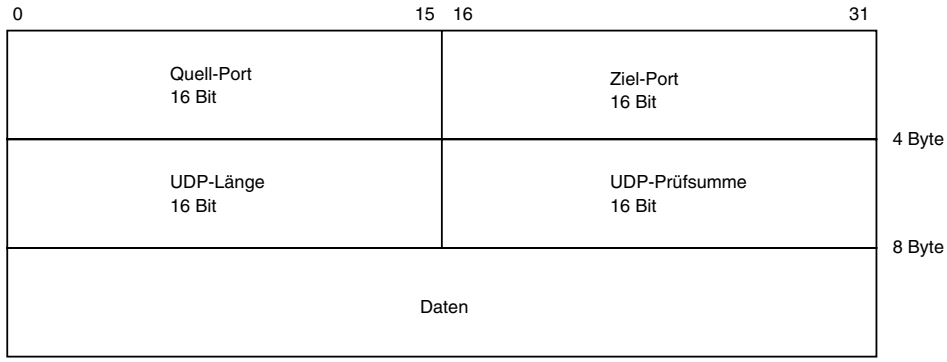


Abbildung C.4: UDP-Header

Der UDP-Header enthält keine IP-Adressen. Diese werden im IP-Header spezifiziert. Der UDP-Header stellt bei einem UDP-IP-Paket die ersten acht Bytes im Datenanteil des IP-Pakets dar.

Der UDP-Quellport (Source Port) ist wie der UDP-Zielport (Destination Port) 16 Bit oder 2 Byte lang. Die UDP-Protokollschicht verwendet diese Information, um die übertragenen Daten einzelnen Anwendungen zuzuordnen.

Die Länge des UDP-Datagramms wird ebenfalls im UDP-Header übertragen. Da ein UDP-Header mindestens acht Byte lang ist, ist die kleinste mögliche UDP-Nachricht acht Byte lang. Ein IP-Paket darf maximal 65.535 Byte lang sein. Abzüglich des IP-

Headers von mindestens 20 Bytes kann eine UDP-Nachricht maximal 65.515 Byte lang werden. Die Größe des UDP-Datagramms wird von der Anwendung bestimmt. Erzeugt diese Anwendung ein UDP-Datagramm, das größer ist als die MTUMaximum Transmission Unit (Maximum Transmission Unit), so wird das Paket auf IP-Ebene fragmentiert.

Die UDP-Prüfsumme im UDP-Header ist optional. Das bedeutet, dass die Anwendung entscheiden kann, ob diese Prüfsumme berechnet werden soll oder nicht. Viele Anwendungen verzichten auf die Erzeugung einer Prüfsumme zugunsten der Performance. Wenn jedoch eine Prüfsumme erzeugt wurde, ist der Empfänger des Pakets laut RFC 1122 verpflichtet, diese Prüfsumme zu überprüfen und im Zweifelsfall das Paket zu verwerfen. Bei der Berechnung der Prüfsumme wird der Inhalt des UDP-Datagramms zusammen mit einem Pseudo-Header aus Quell- und Zielport, der UDP-Protokollnummer 17 und der Größe als Eingabe verwendet.

Es existieren verschiedene Anwendungen, die das UDP-Protokoll nutzen. UDP wird zum Beispiel verwendet, um Namensauflösungen durchzuführen. Hier sendet der Client ein UDP-Paket an einen DNS-Server mit der Bitte, den enthaltenen Namen aufzulösen. Der DNS-Server sendet seine Antwort in einem UDP-Paket an den Client zurück. Da UDP kein verlässliches Protokoll darstellt, achtet der DNS-Server darauf, maximal 512 Bytes Daten in seinem UDP-Datagramm zurückzusenden. Dies garantiert, dass nicht durch eine mögliche Fragmentierung des Pakets Daten verloren gehen können. Ist die zu sendende Antwort jedoch größer, so sendet der DNS-Server eine trunkierte (truncated) Antwort. Der Client ist nun verpflichtet, den DNS-Server erneut zu kontaktieren und die Anfrage erneut mit dem TCP-Protokoll zu stellen. TCP ist in der Lage, die fehlerfreie und komplette Übertragung größerer Datenmengen zu garantieren.

C.4 TCP

Das Transmission Control Protocol (TCP, RFC 793, STD 7) ist das im Internet hauptsächlich eingesetzte Protokoll. TCP garantiert die korrekte und vollständige Übertragung der Informationen. Hierzu setzt TCP unter anderem eine sehr intelligente Flussüberwachung und -steuerung ein. TCP ist ein verbindungsorientiertes Transportprotokoll für den Einsatz in paketvermittelten Netzen. Der häufigste Einsatz baut auf dem Internet-Protokoll IP auf. Es konzentriert sich auf die Verbindung und ihre Integrität. Hierzu bietet es die folgenden Dienste:

- **Virtuelle Verbindung.** Die beiden TCP-Endpunkte kommunizieren über eine dedizierte virtuelle Verbindung. Diese ist für die Flusskontrolle, die garantierte Übertragung und das I/O-Management verantwortlich.
- **I/O-Management**
  - **für die Anwendung.** TCP bietet der Anwendung einen I/O-Puffer. Die Anwendung kann ihre Informationen als fortlaufende Daten in diesen Puffer schreiben, beziehungsweise aus ihm lesen. TCP wandelt diesen fortlaufenden Strom anschließend in Pakete um. Nicht die Anwendung definiert die Paketgröße (wie bei UDP), sondern das TCP-Protokoll erzeugt die Pakete.

  - **auf Netzwerkebene.** TCP wandelt den Datenstrom der Anwendung in Segmente um. Hierbei werden die Segmente so erzeugt, dass sie effizient über das Netzwerk transportiert werden.

- **Flusskontrolle.** TCP bietet eine fortgeschrittene Flusskontrolle, die die unterschiedlichen Sende- und Empfangsfähigkeiten der vielfältigen Geräte berücksichtigt. Es ist in der Lage, vollkommen transparent für die Anwendung die Geschwindigkeit der Verbindung optimal anzupassen.
- **Zuverlässigkeit.** Jedes übertragene Byte wird mit einer Sequenznummer versehen. Dies ermöglicht eine Einordnung der übertragenen Daten in der richtigen Reihenfolge. Zusätzlich bestätigt der Empfänger mit dieser Nummer den Empfang der Daten. Stellt TCP fest, dass bestimmte Informationen nicht übertragen wurden, so werden sie transparent für die Anwendung automatisch erneut gesendet.

Zusätzlich bietet TCP wie UDP einen Multiplexer, so dass mehrere Anwendungen auf einem Rechner gleichzeitig das TCP-Protokoll verwenden können. Hier werden ebenfalls Ports eingesetzt. Jede Anwendung muss vor der Verwendung des Protokolls einen derartigen Port reservieren.

C.4.1 Auf- und Abbau einer TCP-Verbindung

Damit TCP die oben erwähnten Funktionen wahrnehmen kann, ist einiger Verwaltungsaufwand erforderlich. TCP muss zunächst eine Verbindung öffnen. Hierbei führen die beiden TCP-Kommunikationspartner eine Synchronisation ihrer Sequenznummern durch. Anschließend können die Daten ausgetauscht werden. Nach der Verbindung sollte diese auch wieder korrekt abgebaut werden, so dass die beiden Kommunikationspartner die Verwaltungsstrukturen wieder freigeben können.

Die Abbildung C.5 zeigt schematisch den Auf- und Abbau einer TCP-Verbindung. Diese Abbildung führt bereits in einige Funktionen von TCP ein.

Der TCP-Handshake beginnt zunächst mit einem so genannten SYN-Paket. TCP besitzt sechs Bits im TCP-Header (s.u.), die die Funktion des TCP-Pakets bestimmen. Es handelt sich hierbei um die Bits SYN, FIN, ACK, RST, URG und PSH. Ein SYN-Paket ist ein Paket, bei dem die eigene Sequenznummer an den Kommunikationspartner übermittelt wird. Dies ist für die Synchronisation der Verbindung erforderlich. Der Kommunikationspartner erhält hiermit die Information, dass die Datenzählung mit dieser Sequenznummer beginnt. Jedes übertragene Byte besitzt eine eigene Sequenznummer. In diesem Beispiel überträgt der Client an den Server die Sequenznummer 1234. Diese initiale Sequenznummer wird für jede Verbindung neu bestimmt.

Der Server beantwortet dieses Paket mit einem eigenen SYN/ACK-Paket. Das ACK- oder Acknowledge-Bit zeigt an, dass dieses Paket den Empfang von Daten bestätigt. Um der Gegenseite mitzuteilen, welche Daten bestätigt werden, übermittelt der Server eine Acknowledgement-Nummer: 1235. Diese Zahl definiert das nächste erwartete Byte von der Gegenstelle. Es entspricht also der Sequenznummer des letz-

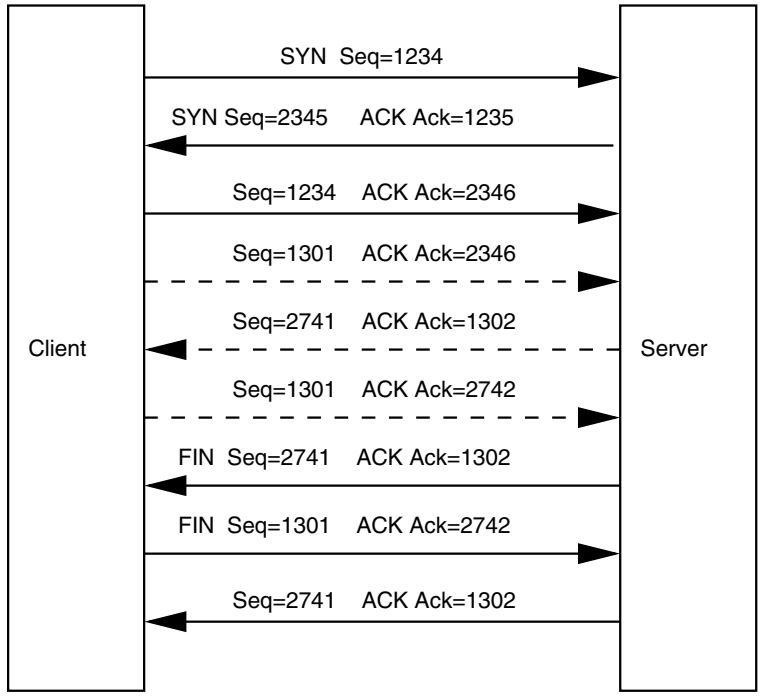


Abbildung C.5: Der TCP-Handshake

ten empfangenen Bytes plus 1. Mit dieser Bestätigung ist die Verbindung zwischen Client und Server in einer Richtung geöffnet worden. Man spricht von einer halb offenen Verbindung. In demselben Paket übermittelt jedoch der Server seinerseits seine Sequenznummer mit dem gesetzten SYN-Bit. Hiermit fordert er den Client auf, seine Seite mit dieser Nummer zu synchronisieren.

Eine Vollduplex-Verbindung, die in beide Richtungen Daten versenden kann, entsteht, wenn der Client diese Synchronisationsanfrage im dritten Paket bestätigt. Da der Client keine Daten übermittelt, erhöht er seine Sequenznummer nicht. Nun können Daten zwischen Client und Server ausgetauscht werden.

Der Client übermittelt nun zunächst 67 Bytes an den Server (4. Paket). Dies kann aus der Differenz der Sequenznummern des dritten und vierten Pakets errechnet werden. Anschließend bestätigt der Server den Empfang dieser Daten und sendet seinerseits 396 Bytes (5. Paket). Der Empfang wird erneut vom Client im 6. Paket bestätigt.

Nun beschließt der Server, dass die Verbindung beendet werden soll. Hierzu bestätigt er den letzten Empfang vom Client und setzt selbst das Bit FIN. Dieses Bit ist die Aufforderung, die Verbindung zu schließen. Hierbei werden keine Daten übermittelt. Daher wird die Sequenznummer nicht erhöht. Der Client bestätigt das FIN.

Hiermit ist die Verbindung halb geschlossen. Um nun seine Richtung zu schließen, sendet der Client in demselben oder einem zusätzlichen Paket ebenfalls ein FIN an den Server. Dieser bestätigt dieses FIN ebenfalls in einem letzten Paket, und die Verbindung ist in beiden Richtungen geschlossen.

C.4.2 TCP-Header

Das TCP-Segment besteht ähnlich wie ein UDP-Datagramm aus einem Header und den Daten. Bevor nun das weitere Verhalten von TCP bezüglich der Flusskontrolle und der Zuverlässigkeit besprochen wird, soll kurz der TCP-Header mit seinen Informationen vorgestellt werden.

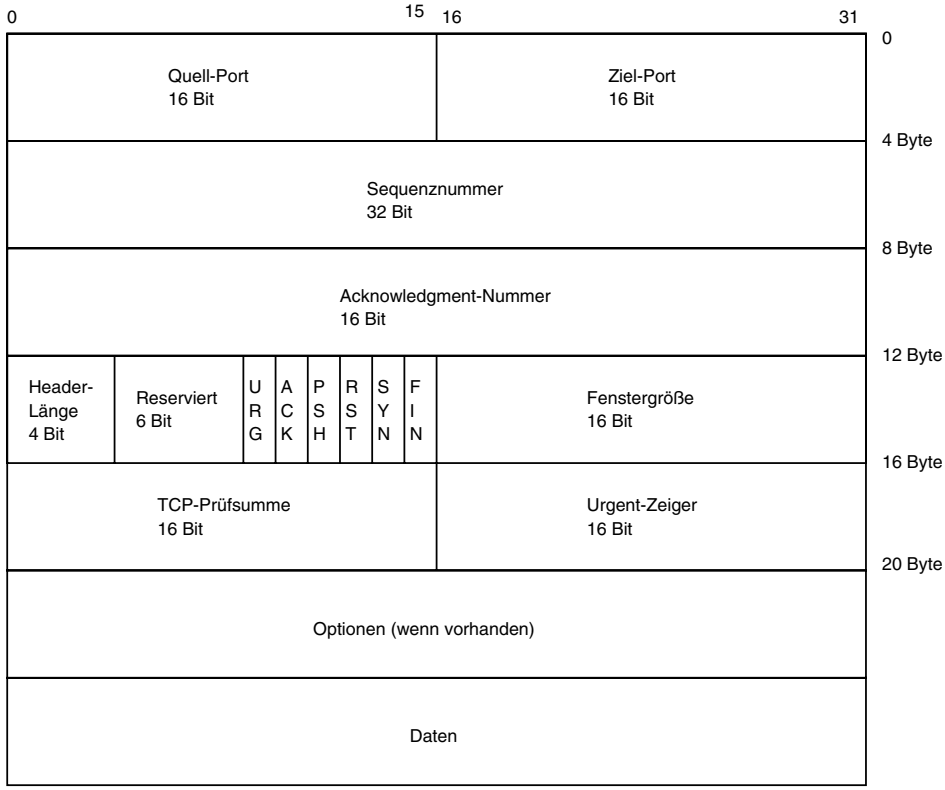


Abbildung C.6: TCP-Header

Quell- und Zielport

Die TCP-Ports werden vom TCP-Protokoll verwendet, um Multiplexer-Funktionalität zur Verfügung zu stellen. Das TCP-Protokoll ist hiermit in der Lage, mehrere Anwendungen gleichzeitig zu unterstützen. Hierzu bindet sich eine Anwendung

zunächst an einen Port. Anschließend kann das TCP-Protokoll dieser Anwendung spezifisch ihre Daten zukommen lassen.

Das TCP-Protokoll unterstützt 65.536 Ports von 0 bis 65.535. Die Zuordnung der Ports zu den Applikationen ist grundsätzlich willkürlich. Jedoch wurden von der IANA einige Ports gewissen Diensten fest zugewiesen (s. UDP).

Sequenznummer

TCP garantiert die Zustellung der zu übertragenden Daten. Damit die Kommunikationspartner diese Übertragung bestätigen und die Daten in der richtigen Reihenfolge zusammensetzen können, wird jedes übertragene Byte mit einer Sequenznummer versehen. Die Zuordnung der Daten und die Entscheidung über die Annahme der Daten erfolgt über diese Sequenznummer (s.u.). Die initiale Sequenznummer sollte für jede Verbindung zufällig ermittelt werden. Besteht die Möglichkeit, die Sequenznummer von einer Verbindung zur nächsten vorherzusehen, so kann dies für gespoofte Angriffe auf das TCP-Protokoll genutzt werden (siehe auch Mitnick-Angriff).

Die Sequenznummer ist eine 32-Bit-Zahl.

Acknowledgement-Nummer

Wie bereits bei der Sequenznummer angesprochen, erhält jedes übertragene Byte eine eindeutige Sequenznummer. In dem Maße, in dem die Daten empfangen werden, übermittelt der Empfänger die Information an den Absender, dass er in der Lage ist, weitere Daten zu empfangen. Die Acknowledgement-Nummer enthält die Information, welches Byte als nächstes erwartet wird. Alle Bytes mit einer kleineren Sequenznummer wurden bereits empfangen.

Sendet der Absender vier Pakete mit den Bytes 1-100, 101-200, 201-300 und 301-400, so antwortet der Empfänger entsprechend mit einer Acknowledgement-Nummer von 101, 201, 301 und 401. Geht das zweite Paket während der Übertragung verloren, so antwortet der Empfänger mit 101, 101, 101 und 101. Dies weist den Absender darauf hin, dass das zweite Paket erneut gesendet werden muss. Sendet der Absender anschließend das Paket 101-200 erneut, so bestätigt der Empfänger dies mit 401, da er die Daten 201-400 ebenfalls bereits erhalten hat.

Um dies noch zusätzlich zu optimieren, besteht die Möglichkeit, verzögerte oder selektive Bestätigungen des Empfangs zu versenden (s.u.).

Header-Länge

Dieses vier Bit lange Feld gibt die Länge des Headers in Doppelworten an. Die Länge in Bytes lässt sich aus dem Wert dieses Feld nach Multiplikation mit 4 ermitteln. Ein TCP-Header ist immer mindestens 20 Byte lang. Dieses Feld trägt also mindestens die Zahl 5. Maximal kann ein TCP-Header 60 Byte lang sein (15 mal 4). TCP definiert also nicht die Gesamtlänge des Pakets wie UDP, sondern nur die

Länge des Headers. Die Gesamtlänge des Pakets lässt sich jedoch aus der Gesamtlänge des IP-Pakets minus der Länge des TCP-Headers ermitteln.

Reservierte Bits

Hierbei handelt es sich um sechs Bits, die bis vor kurzem keine weitere Verwendung hatten. Diese Bits mussten daher bisher gelöscht sein. Viele Firewalls und Intrusion-Detection-Systeme lösen bei einer Verwendung dieser Bits einen Alarm aus. Viele Werkzeuge zur Erkennung von Betriebssystemen nutzen diese Bits, um entfernte Systeme zu untersuchen. Unterschiedliche Betriebssysteme reagieren meist unterschiedlich, wenn diese Bits gesetzt sind.

Seit einigen Jahren existieren jedoch Bemühungen, einige dieser Bits für die Explicit Congestion Notification (ECN) zu verwenden (RFC 3168). Hierbei handelt es sich um einen Mechanismus, bei dem die Kommunikationspartner eine Verstopfung des Internets im Vorfeld erkennen und die Übertragungsrate automatisch anpassen, um eine echte Verstopfung zu vermeiden.

Da ECN sowohl den IP- als auch den TCP-Header betrifft, wird es in einem eigenen Abschnitt behandelt (C.5).

TCP-Flags

Bei den TCP-Flags handelt es sich um sechs Bits. Diese Bits klassifizieren die übertragenen Daten. Es sind nur sehr wenige Kombinationen dieser Bits in einem gültigen Paket erlaubt. Sie haben die folgenden Funktionen:

- **URG.** Das URG-Bit (Urgent) wird verwendet, um der Gegenstelle mitzuteilen, dass das Paket wichtige Daten enthält, die sofort verarbeitet werden müssen. Um den Anteil der wichtigen Daten zu definieren, wird der Urgent-Zeiger verwendet (s.u.). Ist das URG-Bit nicht gesetzt, so ist der Wert des Zeigers zu ignorieren.
- **ACK.** Das ACK-Bit (Acknowledgement) wird verwendet, um den Empfang von Daten zu bestätigen. Jedes TCP-Segment einer Verbindung, außer dem ersten Segment und RST-Segmenten zum Abbruch einer Verbindung, muss dieses Bit gesetzt haben.
- **PSH.** Das PSH-Bit (Push) kennzeichnet Segmente, die von der sendenden Anwendung »gedrückt« werden. Häufig müssen Anwendungen (z.B. telnet) nur sehr wenige Daten versenden. TCP würde zur Optimierung die Daten aber erst versenden, wenn ein komplettes Segment gefüllt wäre. Das PSH-Bit weist das TCP-Protokoll an, die Daten sofort zu versenden, da keine weiteren Daten in diesem Moment folgen.
- **RST.** Das RST-Bit (Reset) wird nur verwendet, wenn ein Fehler in einer Verbindung aufgetreten ist oder wenn der Wunsch eines Verbindungsaufbaus abgelehnt wird.
- **SYN.** Das SYN-Bit (Synchronize) wird verwendet, um die eigene Sequenznummer zur Synchronisation an den Kommunikationspartner zu übermitteln. Dies

erfolgt während des TCP-Handshakes (s.o.). Das SYN-Bit darf nur in diesem Moment gesetzt werden.

- **FIN.** Das FIN-Bit (Finish) wird gesetzt, wenn eine Seite der Kommunikation diese beenden will. Wenn die Gegenseite ebenfalls in der Lage ist, die Verbindung zu beenden, so antwortet sie ebenfalls mit einem FIN-Paket. Ein Paket mit gesetztem FIN-Bit ist nur in einer zuvor aufgebauten Verbindung gültig.

Grundsätzlich müssen alle TCP-Pakete das ACK-Bit gesetzt haben. Lediglich zwei Ausnahmen sind erlaubt. Hierbei handelt es sich um das erste Paket einer TCP-Verbindung, in dem lediglich das SYN-Bit gesetzt ist, und ein RST-Paket, das einen Fehler in einer TCP-Verbindung anzeigt und diese abbricht. Die weiteren Bits können in Kombinationen mit dem ACK-Bit vorkommen.

Kombinationen von SYN/FIN, SYN/RST oder RST/FIN sind jedoch nicht erlaubt. Netzwerk-Intrusion-Detection-Systeme ermitteln üblicherweise sämtliche Pakete mit fehlerhaften TCP-Flag-Kombinationen. Der *Unclean*-Match des Linux-Paketfilters Netfilter ist ebenfalls in der Lage, diese Kombinationen zu erkennen und sogar zu verwerfen (Achtung: Ältere Implementierungen von *Unclean* wiesen hier Fehler auf).

Fenstergröße

Das TCP-Fenster (Receive Window) gibt die Größe des Empfangsspeichers des sendenden Systems an. Diese Angabe wird von der TCP-Flusskontrolle verwendet. Die Größe dieses Feldes ist 16 Bit. Damit kann das Fenster maximal 64 Kbit groß werden. Da dies für einige Netzwerke (z.B. Token Ring) nicht ausreicht, existiert zusätzlich die Möglichkeit, die Window Scale-Option zu verwenden. Hiermit können 30 Bits für die Angabe der Fenstergröße verwendet werden. Dies erlaubt Fenster bis zu 1 Gbyte Größe.

Wurden so viele Daten gesendet, dass dieses Empfangsfenster gefüllt ist, so muss der Sender zunächst auf eine Bestätigung dieser Daten warten, bevor weitere Daten gesendet werden dürfen.

TCP-Prüfsumme

Dieses Feld speichert die TCP-Prüfsumme. Diese Prüfsumme erstreckt sich sowohl auf den Header als auch auf die Daten des TCP-Segments. Zusätzlich wird ein Pseudo-Header mit aufgenommen, der die IP-Adressen und das Protokoll (TCP, 6) enthält.

Die TCP-Prüfsumme ist 16 Bit lang und nicht optional. Der Absender muss die TCP-Prüfsumme berechnen, und der Empfänger muss diese Prüfsumme kontrollieren. Wenn die Prüfsumme nicht gültig ist, wird das Paket verworfen. Der Absender erhält keinerlei Fehlermeldung.

Diese Eigenschaft wird sehr häufig verwendet, um Network-Intrusion-Detection-Systeme oder zustandsorientierte Paketfilter zu verwirren. Wenn diese Systeme ver-

suchen, den Zustand der Verbindung zu überwachen, aber nicht die Prüfsumme testen, so besteht die Möglichkeit, weitere Pakete (z.B. RST-Pakete) einzuschleusen, die vom NIDS oder vom Paketfilter als gültige Pakete akzeptiert werden (und scheinbar die Verbindung abbrechen), aber vom echten Empfänger verworfen werden.

Urgent-Zeiger

TCP ist in der Lage, bestimmte Teile der Nachricht als wichtig zu kennzeichnen. Hierzu wird das URG-Flag in den TCP-Flags gesetzt. Zusätzlich wird der Urgent-Zeiger gesetzt. Der Urgent-Zeiger (oder Pointer) zeigt auf das Ende der wichtigen Informationen im aktuellen Segment.

Pakete, die das URG-Bit gesetzt haben, müssen vom Empfänger sofort bearbeitet werden. Dieses Paket sollte Vorrang vor allen weiteren Paketen in der Empfangswarteschlange haben.

Wenn der Urgent-Zeiger gesetzt, das URG-Bit jedoch gelöscht ist, muss das Paket wie ein normales Paket behandelt werden.

Optionen

Die bisher im TCP-Header spezifizierten Angaben genügen für eine erfolgreiche TCP-Verbindung. Jedoch werden häufig zusätzliche Optionen genutzt, um eine Anpassung der Eigenschaften zu ermöglichen.

TCP unterstützt die folgenden neun Optionen:

- **End of Option List.** Diese Option markiert das Ende der Optionen im TCP-Header. Die Option ist acht Bit lang und hat den Typ 0.
- **No Operation.** Diese Option wird verwendet, um Bereiche zwischen den TCP-Optionen aufzufüllen. Es ist sinnvoll, dass einige Optionen auf einer 32-Bit-Grenze beginnen. Dann wird der Bereich zwischen diesen Optionen mit NOP aufgefüllt. NOP ist acht Bit lang und vom Typ 1.
- **Maximum Segment Size.** Die Maximum Segment Size (MSS) wird von den Endpunkten verwendet, um die Gegenseite über ihre MTUMaximum Transmission Unit (Maximum Transmission Unit) beziehungsweise MRU (Maximum Receive Unit) zu informieren. Diese Funktion kann auch von Routern gesetzt werden. Netfilter besitzt zum Beispiel eine TCPMSS-Funktion. Dieser Austausch erfolgt lediglich bei der Synchronisation der Verbindung. Die MSS ist üblicherweise gleich der MTU minus 40 Bytes.

  Es handelt sich um eine Option von 32 Bit Länge und Typ 2. Wird keine MSS angegeben, so verlangt RFC 1122, dass als MSS 536 (IP-Default-Größe 576 - Header 40) verwendet wird.
- **Window Scale.** Hiermit ist es möglich, größere Empfangsfenster anzugeben als die üblichen 64 Kbyte. Maximal sind Fenster in der Größenordnung von 1 Gbyte möglich. Diese Option von Typ 3 ist drei Byte lang. Das dritte Byte definiert

den Maßstab des im Header angegebenen Empfangsfensters. Die Window Scale-Option darf lediglich in den beiden ersten Paketen ausgetauscht werden. Ansonsten wird sie ignoriert.

- **Selective Acknowledgment Permitted.** Bevor selektive Bestätigungen erlaubt sind, müssen beide Endpunkte sich darauf einigen. Die Option *Selective Acknowledgment Permitted* vom Typ 4 ist 16 Bit lang. Sie muss ebenfalls in den ersten beiden TCP-Segmenten ausgetauscht werden. Später wird sie ignoriert.
- **Selective Acknowledgment Data.** Hiermit besteht für den Empfänger die Möglichkeit, einen unterbrochenen Strom von Daten zu bestätigen. Normalerweise kann der Empfänger nur das letzte Byte eines ununterbrochenen Datenstroms bestätigen. Dass der Empfänger bereits weitere Pakete erhalten hat, kann er dem Absender nicht mitteilen. Mit dieser Option *Selective Acknowledgment Data* vom Typ 5 und einer variablen Länge ist der Empfänger in der Lage, exakt ein fehlendes Segment nachzufordern und die bereits empfangenen diskontinuierlichen Segmente dem Absender mitzuteilen.

  Diese Option darf in jedem TCP-Segment verwendet werden.
- **Timestamp.** Die Option *Timestamp* vom Typ 8 erlaubt den beiden Endpunkten, die Latenzzeit kontinuierlich zu messen. Diese Option mit einer Länge von zehn Byte enthält die Zeitstempel beider Endpunkte in jedem Paket.

  Diese Option darf in jedem TCP-Segment verwendet werden.

C.4.3 Fortgeschrittene Eigenschaften von TCP

Flusskontrolle

Wenn eine Anwendung unter Verwendung des TCP-Protokolls Daten versendet, so schreibt sie die Daten in einen Sendepuffer. TCP wird in regelmäßigen Abständen die Daten dieses Sendepuffers in TCP-Segmenten versenden. Die Senderate wird hierbei ständig angepasst.

Ursprünglich wurde hierzu die Möglichkeit geschaffen, dass der Empfänger die Geschwindigkeit über sein Empfangsfenster (Receive Window Sizing) anpasst. Dazu übermittelt der Empfänger in jedem Paket die maximale Datenmenge, die er im Moment zu verarbeiten in der Lage ist. Der Sender darf nicht mehr Daten als die vorgeschriebene Menge übertragen. Anschließend muss der Sender zunächst auf eine Bestätigung des Empfangs und der Verarbeitung warten.

Das Empfangsschiebefenster (Sliding Receive Windows) erlaubt es dann dennoch dem Sender, einige weitere Pakete zu versenden, da er eine Bestätigung der bereits gesendeten Pakete in Kürze erwartet. Hierdurch ist ein wesentlich reibungsärmerer Austausch der Daten möglich.

Dies stellt jedoch eine rein vom Empfänger gesteuerte Flusskontrolle dar. Benötigt der Empfänger mehr Zeit zur Verarbeitung der Daten, so kann er sein Empfangsfenster verkleinern. Ist er in der Lage, die Daten schnell zu verarbeiten, so kann er es derart vergrößern, dass die Geschwindigkeit nur noch durch das Netzwerk selbst

gesteuert wird. Dies reicht jedoch nicht aus. Es ist auch eine durch den Sender gesteuerte Flusskontrolle sinnvoll.

Die vom Sender gesteuerte Flusskontrolle verwendet ein Congestion Window (Verstopfungsfenster), den langsamen Start (Slow Start) und die Verstopfungsvermeidung (Congestion Avoidance).

Lediglich der Sender ist in der Lage, Verstopfungen zu erkennen. Hierzu existieren drei Möglichkeiten:

1. Der Sender erhält eine ICMP-Source-Quench-Meldung eines Routers. Dies zeigt an, dass der Router nicht in der Lage ist, die Pakete schnell genug zu verarbeiten.
2. Der Sender erhält mehrfache Acknowledgements mit identischer Acknowledgment-Nummer. Man bezeichnet diese auch als doppelte Acknowledgements. Der Empfänger sendet ein Acknowledgement, wenn er ein weiteres Paket erhält. Wenn ihm jedoch ein Paket fehlt, so weisen alle diese Pakete dieselbe Acknowledgement-Nummer auf. Die Acknowledgement-Nummer zeigt das nächste vom Empfänger erwartete Datenbyte an! Daher sind für den Sender doppelte Acknowledgements ein Hinweis darauf, dass wahrscheinlich ein Paket zwischendurch verloren gegangen ist.
3. Der Sender erhält innerhalb einer bestimmten Zeit kein Acknowledgement (Acknowledgment Timer). Dies weist ebenfalls auf verloren gegangene Pakete hin.

Wenn nun der Sender weiterhin die Pakete mit gleicher Geschwindigkeit sendet, wird die Verstopfung bestehen bleiben und möglicherweise schlimmer werden. Es ist also erforderlich, dass der Sender reagiert und die Rate senkt, um die Verstopfung zu beheben und schließlich den alten Paketdurchsatz wieder zu erreichen.

Hierzu wird ein Congestion Window verwendet. Dieses definiert, wie viele Daten der Sender ohne eine Bestätigung der Gegenseite versenden darf. Zu Beginn weist dieses Fenster die gleiche Größe auf wie das Empfangsfenster (Receive Window). Dieses Fenster wird nun in Abhängigkeit von der Verstopfung reduziert.

- Wurden mehr als drei doppelte Acknowledgements erkannt, so wird das Congestion Window halbiert. Anschließend wird die Congestion Avoidance aktiviert. Diese vergrößert das Fenster wieder in sehr kleinen Schritten.
- Wurde eine Source-Quench-Meldung erhalten oder fehlen Acknowledgements, so wird das Fenster so stark reduziert, dass jeweils nur ein Segment gesendet werden kann. Anschließend wird der Slow Start aktiviert.

Der Slow Start vergrößert das Congestion Window exponentiell. Würde das Congestion Window sofort wieder auf den Ausgangswert reinitialisiert, so würde die Verstopfung sofort wieder auftreten. Beim Slow Start wird das Congestion Window **für jedes** bestätigte Segment um **ein** weiteres Segment vergrößert. Diese Technik wird verwendet, wenn eine neue Verbindung aufgebaut wird und eine Verstop-

fung aufgetreten ist. Im Falle einer Verstopfung wird jedoch beim Erreichen des halb maximalen Congestion Windows auf Congestion Avoidance umgeschaltet.

Congestion Avoidance stellt eine langsamere vorsichtigere Methode zur Vergrößerung des Congestion Windows dar. Wurden **alle** Pakete, die innerhalb eines Congestion Windows versandt wurden, bestätigt, so wird das Congestion Window um **ein** Segment vergrößert.

Zuverlässigkeit

Die Zuverlässigkeit ist eine der wichtigsten Eigenschaften des TCP-Protokolls. Daher soll hier kurz beschrieben werden, welche Mechanismen von TCP verwendet werden, um dies effizient garantieren zu können.

RFC 793 verlangt, dass TCP in der Lage ist, Daten, die beschädigt, verloren, dupliziert oder in falscher Reihenfolge übermittelt wurden, so zu handhaben, dass dies transparent für die Anwendung erfolgt. Um dieses Ziel zu erreichen, verwendet TCP Prüfsummen, Sequenznummern, Acknowledgement-Nummern und Zeitgeber.

Die TCP-Prüfsummen ähneln den UDP-Prüfsummen. Im Gegensatz zu UDP sind sie bei TCP jedoch obligatorisch. Hierbei werden zusätzlich zum TCP-Header und zu Daten die IP-Adressen und das IP-Protokoll zur Ermittlung der Prüfsumme verwendet. Diese Prüfsumme garantiert die fehlerfreie Übertragung der Daten.

Die Sequenznummern ermöglichen es dem Empfänger, die Daten in der richtigen Reihenfolge zu verarbeiten, auch wenn die Daten möglicherweise in einer anderen Reihenfolge erhalten wurden. Jedes übertragene Byte besitzt seine eigene eindeutige Sequenznummer. Diese Sequenznummern erlauben auch die Erkennung duplizierter Informationen, da diese identische Sequenznummern aufweisen. Um eine Störung durch veraltete Pakete beim Empfang zu vermeiden, sollte der Empfänger nur Pakete mit Sequenznummern verarbeiten, die seinem Empfangsfenster (Receive Window) entsprechen.

Die Acknowledgement-Nummern erlauben es dem Absender, den korrekten Empfang der gesendeten Daten zu prüfen. Der Empfänger bestätigt den Empfang der Daten und bestätigt, dass er in der Lage ist, weitere Daten zu verarbeiten. Wurden gesendete Daten nicht mit der entsprechenden Acknowledgement-Nummer bestätigt, so werden diese Daten nach Ablauf des entsprechenden Zeitgebers erneut versendet.

Da häufig nur wenige Pakete verloren gehen, wurde mit dem RFC 1072 die Möglichkeit geschaffen, selektive Bestätigungen (Selective Acknowledgements) zu versenden. Meist hat der Empfänger bereits zehn Segmente erhalten, jedoch fehlt das erste Segment. Ein klassisches Verhalten des Empfängers, bei dem dieser mehrfach nur dieselbe Acknowledgement-Nummer versendet, führt häufig dazu, dass sämtliche Pakete erneut versendet werden. Dies ist jedoch nicht erforderlich und beinträchtigt die Bandbreite. Die Selective Acknowledgements erlauben es mithilfe der TCP-Option *Selective Acknowledgement*, trotz doppelter Acknowledgement-Nummern weitere Segmente selektiv zu bestätigen.

Wenn der Datendurchsatz sehr hoch ist, ist es sinnvoller, nicht jedes Paket zu bestätigen, sondern die Bestätigung verzögert zu versenden (Delayed Acknowledgements). Hierbei wird nur der Empfang jedes zweiten oder dritten Pakets bestätigt. Dies stellt kein Problem dar, da ein Acknowledgement bedeutet, dass alle Daten bis zu dieser Acknowledgement-Nummer empfangen wurden.

C.5 Explicit Congestion Notification

TCP ist in der Lage, bereits sehr gut mit einer Netzwerkverstopfung umzugehen und trotz Verstopfung die Datenübertragung zuverlässig zu garantieren. Jedoch kann es weiterhin zu einer Verstopfung und damit auch zu einer Verzögerung der Übertragung kommen. Die Explicit Congestion Notification (ECN) versucht nun, dies zu verhindern, indem die Kommunikationspartner bereits vor dem Auftreten der Verstopfung gewarnt werden und dem Entstehen entgegenwirken können.

Die Erweiterung des IP-Protokolls um die Explicit Congestion Notification wird in RFC 3168 beschrieben. Linux ist eines der ersten Betriebssysteme, die dieses RFC umgesetzt haben. Es beschreibt die notwendigen Modifikationen des IP- und des TCP-Protokolls zur Umsetzung von ECN.

Die bisher besprochenen Verfahren des TCP-Protokolls zur Vermeidung einer Netzwerkverstopfung gehen davon aus, dass es sich beim Netzwerk um eine Black Box handelt. Das Netzwerk selbst ist nicht in der Lage, eine Verstopfung anzuzeigen. Die Verstopfung zeichnet sich dadurch aus, dass keine Pakete mehr transportiert werden.

Moderne Netzwerke und ihre Komponenten sind jedoch wesentlich intelligenter und sehr wohl in der Lage, eine Verstopfung bereits in ihrem Entstehen zu erkennen. Ein Router ist bei aktiver Verwaltung (Random Early Detection, RED) seiner Warteschlangen in der Lage, eine Verstopfung zu erkennen, bevor die Warteschlange überläuft und der Router die Pakete verwerfen muss. Er ist in der Lage, diese Informationen an die Endpunkte einer Kommunikation zu übermitteln, wenn die Protokolle dies vorsehen und verstehen. Dies erfolgt durch die Angabe *Congestion Experienced (CE)*.

Damit dies möglich ist, müssen das IP-Protokoll und das Transport-Protokoll (TCP) dies auch unterstützen. Hierzu werden im IP-Header ein ECN-Feld und in dem TCP-Header zwei neue ECN-Flags definiert. Diese Definition erlaubt eine fließende Migration, da diese Felder von Systemen, die nicht ECN-fähig sind, ignoriert werden. Leider werden Pakete, die diese Felder verwenden, von vielen Firewalls und Network-Intrusion-Detection-Systemen noch als gefährlich eingestuft.

Das ECN-Feld im IP-Header ist zwei Bits lang. Ist dieses Feld gelöscht, so ist der Absender des Pakets nicht ECN-fähig. Tragen die beiden Bits den Wert 01 oder 10, so ist der Absender des Pakets ECN-fähig. Trägt dieses Feld den Wert 11, so hat ein Router dies gesetzt, da er eine Congestion bemerkt hat: Congestion Experienced. Das ECN-Feld entspricht den bisher ungenutzten Bits 6 und 7 des Type-Of-Service-

Feldes. Die ehemalige Verwendung des Type-Of-Service-Feldes wird nun durch die Differentiated Services ersetzt. Diese nutzen die Bits 0 bis 5 dieses Feldes.

Erhält ein Endpunkt ein Paket, bei dem *Congestion Experienced (CE)* gesetzt ist, so muss dieser Endpunkt sich so verhalten, als ob das Paket verloren gegangen wäre. Im Falle von TCP muss das TCP-Protokoll das Congestion Window halbieren.

ECN benötigt eine Unterstützung durch das Transport-Protokoll. Dieses muss zunächst die ECN-Fähigkeit der Endpunkte aushandeln. Anschließend sollten die Endpunkte jeweils Informationen über CE-Pakete austauschen.

Insgesamt sind drei Funktionalitäten für ECN in TCP erforderlich. Hierbei handelt es sich um die Aushandlung der ECN-Fähigkeit zwischen den beiden Endpunkten. Zusätzlich ist ein ECN-Echo erforderlich, mit dem der Empfänger eines CE-Pakets dem Absender diese Tatsache mitteilt, und ein Congestion Window Reduced – (CWR-)Flag, mit dem der Absender dem Empfänger mitteilt, dass das Congestion Window reduziert wurde.

Diese Fähigkeiten werden in TCP mit zwei neuen Flags realisiert. Hierbei handelt es sich um zwei bisher reservierte Bits im TCP-Header. Das Bit 9 der Bytes 13 und 14 im TCP-Header ist das ECN-Echo-Bit (ECE). Das CWR-Bit ist das Bit 8 im TCP-Header. Abbildung C.7 zeigt den veränderten Header.

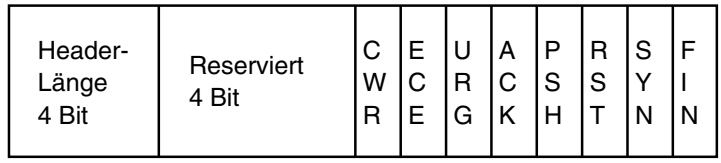


Abbildung C.7: ECN-Header

Während des Verbindungsaufbaus sendet ein ECN-fähiger Rechner nun ein TCP-SYN-Paket, bei dem das ECE- und das CWR-Bit gesetzt sind. Ein ECN-fähiger Rechner kann dies mit einem TCP-SYN/ACK-Paket beantworten, bei dem das ECE-Bit gesetzt und das CWR-Bit gelöscht ist. Anschließend kann ECN genutzt werden.

Weitere Informationen finden Sie im RFC 3168. Für die Intrusion Detection ist nun wichtig zu erkennen, dass derartige Pakete nicht grundsätzlich als fehlerhaft und gefährlich einzustufen sind. Wenn die gesamte TCP-Kommunikation überwacht wird, lässt sich während des Verbindungsaufbaus der Austausch der ECN-Informationen überwachen.

Der Linux-Kernel bietet die Möglichkeit, die ECN-Funktionalität ein- oder abzuschalten. Um die Funktionalität einzuschalten, genügt:

```
# sysctl -w net.ipv4.tcp_ecn=1
```

Das Abschalten erfolgt über die Zuweisung einer 0.

C.6 ICMP

IP ist ein Protokoll, das die Zustellung des Pakets nicht garantiert. Dies ist die Aufgabe der höheren Protokolle. Diese müssen bei Verlust eines Pakets diesen bemerken und das Paket erneut senden. Jedoch können Situationen auftreten, in denen kein Paket zum Ziel übertragen wird. In diesem Fall sollte der Absender informiert werden, um dauernde Neuübertragungen zu vermeiden oder um die Pakete modifiziert zu versenden. Es ist die Aufgabe des Internet Control Message Protocol (ICMP, RFC 792, STD 5), diese Informationen zu übertragen.

Hinweis

ICMP kann eingesetzt werden, um das Betriebssystem eines Rechners zu bestimmen. Ofir Arkin und Fyodor Yarochkin haben das Werkzeug X entwickelt, das mit einigen wenigen ICMP-Paketen und den Antworten ermitteln kann, mit welchem Betriebssystem es sich gerade unterhält. Das Werkzeug und Whitepapers sind verfügbar unter *http://www.sys-security.com/html/projects/X.html*.

ICMP ist das IP-Protokoll Nummer eins. Es wird in einem IP-Datagramm übertragen. Der ICMP-Header besteht aus dem acht Bit langen ICMP Type-Feld, dem acht Bit langen ICMP Code-Feld und einer 16 Bit langen Prüfsumme. Anschließend können Daten in Abhängigkeit vom Typ und Code angehängt werden.

Die folgenden ICMP-Typen und -Codes sind definiert:

Nachricht	Type	Code
Echo reply	0	0
Destination unrechable	3	
Network unreachable	3	0
Host unreachable	3	1
Protocol unreachable	3	2
Port unreachable	3	3
Fragmentation needed but DF set	3	4
Source route failed	3	5
Destination network unkown	3	6
Destination host unkown	3	7
Source host isolated (obsolete)	3	8
Destination network admin. prohibited	3	9
Destination host admin prohibited	3	10
Network unreachable for TOS	3	11
Host unreachable for TOS	3	12
Communication admin prohibited	3	13
Host precedence violation	3	14
Precedence cutoff in effect	3	15
Source quench	4	0

```
Redirect                              5
  Redirect for network                5      0
  Redirect for host                   5      1
  Redirect for TOS and network        5      2
  Redirect for TOS and host           5      3
Echo request                          8      0
Router advertisment                   9      0
Router solicitation                  10      0
Time exceeded                        11
  Time exceeded during transit       11      0
  Time exceeded during reassembly    11      1
Parameter problem                    12
  IP header bad                      12      0
  Required option missing            12      1
Timestamp request                    13      0
Timestamp reply                      14      0
Information request (obsolete)       15      0
Information reply   (obsolete)       16      0
Address mask request                 17      0
Address mask reply                   18      0
```

Die wichtigsten dieser Nachrichten sollen im Weiteren erläutert werden.

C.6.1 Destination Unreachable

Destination Unreachable ist eine der wichtigsten ICMP-Nachrichten. Sie wird verwendet, um dem Absender mitzuteilen, dass der Empfänger nicht erreichbar ist. Diese Nachricht verwendet verschiedene Subtypen, die über den ICMP-Code unterschieden werden.

Die häufigsten Subtypen sind: `Network Unreachable`, `Host Unreachable` und `Port Unreachable`. Die Nachricht `Network Unreachable` wird versendet, wenn ein Router keine Route für das Zielnetzwerk kennt. Die Nachricht `Host Unreachable` wird vom letzten Router versendet, wenn er den Zielrechner nicht erreichen kann (z.B. weil er ausgestellt ist). `Port Unreachable` wird vom Zielrechner verwendet, wenn das Paket versucht, einen nicht existenten UDP-Dienst auf dem Zielrechner anzusprechen. Handelt es sich um einen TCP-Dienst, so versendet der Zielrechner ein TCP Reset-Paket (siehe TCP).

Firewalls in Form eines Paketfilters verwenden ebenfalls häufig diese Meldungen, um einen Zugriff auf bestimmte Rechner und Dienste abzulehnen. Einfache Paketfilter können so auch erkannt werden, da sie häufig TCP-Anfragen mit einem ICMP-`Port Unreachable` beantworten. Das Zielsystem hätte ein TCP-Reset geschickt.

Die Meldung *Fragmentation Needed but DF-Bit set* wird verwendet, wenn ein Router das Paket nicht weiter senden kann, da es für das nächste Netzwerk zu groß ist. Zusätzlich wird dann die MTU des nächsten Netzwerks mit der Fehlermeldung übertragen. Diese Fehlermeldung wird von der Path Maximum Transmission Unit

Discovery (Path MTU Discovery) eingesetzt. Hierbei versucht das Betriebssystem, eine Fragmentierung der Pakete zu vermeiden, indem es zunächst die MTUMaximum Transmission Unit für den gesamten Pfad ermittelt. Anschließende Pakete werden dann mit dieser PMTU versandt.

Damit der Empfänger der Fehlermeldung `Destination Unreachable` erfährt, auf welches Paket sich die Fehlermeldung bezieht, enthält diese den IP-Header des originalen Pakets mit den ersten acht folgenden Bytes des Pakets. Dies erlaubt eine eindeutige Zuordnung des Pakets durch den Empfänger.

Achtung

Viele Paketfilter erlauben die Definition einer Network Address Translation. Das bedeutet, dass die Adressen der Pakete im IP-Header modifiziert werden. Einige Paketfilter kontrollieren jedoch nicht die IP-Adressen, die im IP-Header enthalten sind, der in der ICMP-Meldung eingebettet ist. So können private IP-Adressen nach außen gelangen!

C.6.2 Source Quench

Dies ist eine sehr einfache Fehlermeldung. Mit ihr teilt der Absender mit, dass er die Pakete nicht schnell genug verarbeiten kann und einige Pakete verwerfen muss. Diese Meldung wurde früher auch von Routern versendet. Diese verwenden jedoch heutzutage modernere Quality-of-Service-Funktionen. Source-Quench-Meldungen tauchen daher nur noch recht selten auf.

Achtung

Source-Quench-Meldungen können für einen Denial-of-Service-Angriff genutzt werden, wenn sie geeignet gespooft werden.

C.6.3 Time Exceeded

Die Time Exceeded-Meldungen werden in erster Linie heute vom Werkzeug `traceroute` verursacht. Dieses Werkzeug versendet Pakete mit steigendem Time To Live-(TTL-)Wert an den Empfänger. Die Router, über die die Pakete zum Ziel transportiert werden, werden die entsprechenden Pakete verwerfen und Fehlermeldungen mit ihrer Absender-IP-Adresse zurücksenden. So kann der Weg des Pakets rekonstruiert werden.

Es existieren zwei wesentliche Varianten des Programms Traceroute: `traceroute` (Unix) und `tracert.exe` (Microsoft Windows). Diese Programme versenden un-

terschiedliche Pakete. `tracert.exe` versendet an die Ziel-IP-Adresse jeweils drei Echo-Request-Pakete mit identischer TTL und inkrementiert dann den TTL-Wert. Die Rücklaufzeit der Pakete wird gemessen und angezeigt. Das Unix-Programm `traceroute` versendet UDP-Pakete an die Ports 33434 ff. Hierbei werden ebenfalls immer drei Pakete mit identischer TTL an einen Port gesendet. Jedes Mal, wenn das Programm die TTL inkrementiert, wird auch der Port inkrementiert.

C.6.4 Redirect

Die Redirect-Nachrichten werden von einem Router versendet, der den Absender eines Pakets über einen kürzeren Pfad informieren möchte. Router können ihre Routing-Tabellen dynamisch untereinander mit dem Routing Information Protocol (RIP) austauschen. Hierdurch kennt ein Router alle weiteren Router und sämtliche möglichen Routen. Erhält ein Router nun ein Paket und stellt fest, dass sich in demselben Netzwerk ein weiterer besser geeigneter Router befindet, so übermittelt er diese Information an den Client. Der speichert die Information in seinem Routing-Cache ab und wird das nächste Paket direkt an diesen geeigneteren Router versenden. Der Routing-Cache kann unter Linux mit dem Befehl `route -Cn` betrachtet werden.

Achtung

Redirect-Meldungen können verwendet werden, um Router zu spoofen. Wenn ein Netzwerk keine dynamischen Routing-Protokolle einsetzt, sollten derartige Meldungen starkes Misstrauen hervorrufen. Unter Linux kann die Annahme derartiger Meldungen mit der Kernel-Variablen `/proc/sys/net/ipv4/conf/*/accept_redirects` abgestellt werden.

C.6.5 Parameter Problem

Die Fehlermeldung `Parameter Problem ICMP` wird versendet, wenn das IP-Datagramm selbst Fehler aufweist. Meistens wurde eine IP-Option falsch verwendet. Da die meisten IP-Implementierungen inzwischen jedoch recht ausgereift sind, kommen diese Fehlermeldungen eigentlich nur noch gehäuft vor, wenn Pakete manuell fehlerhaft konstruiert werden.

C.6.6 Echo-Request und Reply

Echo-Request und -Reply sind die ICMP-Nachrichten, die vom Kommando `ping` verwendet werden. Hierbei sendet ein Rechner den ICMP-Echo-Request. Der Empfänger antwortet auf jedes Echo-Request-Paket mit einem Echo-Reply-Paket. Um die Pakete voneinander trennen zu können, enthalten sie eine eindeutige Identifikationsnummer und eine Sequenznummer. Die Identifikationsnummer wird verwendet, um die Pakete mehrerer gleichzeitiger `ping`-Aufrufe voneinander zu trennen. Die Sequenznummer wird für jedes versandte Paket inkrementiert und identifiziert

die einzelnen Pakete. Dies erlaubt die eindeutige Zuordnung eines Reply-Pakets zu dem Request-Paket und die Ermittlung der Übertragungszeit.

Die meisten Implementierungen des `ping`-Kommandos erlauben es, die Anzahl der zu übertragenden Bytes und den Inhalt zu definieren. So kann unter Linux mit der Option `-p` ein Muster (Pattern) definiert und mit der Option `-s` die Größe angegeben werden. Werden diese Informationen nicht modifiziert, so erlauben häufig die Größe und der Inhalt des Pakets einen Rückschluss auf das sendende Betriebssystem.

Eine weitere Option, die vor allem in Unix-Implementierungen des Befehls existiert, ist `-b`. Diese erlaubt ein Broadcast-Ping. Hierbei werden die Echo-Request-Pakete an eine Broadcast-Adresse gesendet. Üblicherweise antworten sämtliche Unix- und Linux-Rechner auf eine derartige Anfrage. In der Vergangenheit konnten hiermit Denial-of-Service-Angriffe erzeugt werden. Der Angreifer spoofte ein Echo-Request-Paket und sendete es an eine Broadcast-Adresse. Sämtliche Rechner antworteten und schickten ihre Antwort an den gespooften Rechner. Wurden hierzu Netzwerke mit mehreren hundert Rechnern verwendet, konnte der gespoofte Rechner häufig überflutet werden. Heute existieren kaum noch Netzwerke, die diese Pakete, die an die Broadcast-Adresse gerichtet sind, hineinlassen. Dieser Angriff ist unter dem Namen SMURF berühmt geworden. Die Netzwerke bezeichnet man als SMURF-Amplifier-Netzwerk (Verstärker). Informationen hierzu finden Sie zum Beispiel unter *http://www.powertech.no/smurf/*.

Ping-Pakete sind in modernen Netzwerken vollkommen normal. Das Vorkommen lediglich von Echo-Reply-Paketen sollte jedoch Ihre Aufmerksamkeit erregen. Hierbei könnte es sich um einen Tunnel handeln.

C.6.7 Address Mask Request und Reply

Diese beiden Nachrichten können verwendet werden, um die Subnetzmaske eines Rechners zu ermitteln. Diese Nachrichten verwenden ähnlich dem Echo eine Identifikationsnummer und eine Sequenznummer, um die Nachrichten zuordnen zu können.

Diese Anfragen werden häufig verwendet, um herauszufinden, ob ein bestimmter Rechner erreichbar ist und welche Adressmaske er verwendet. Leider existiert kein klassisches Kommandozeilenwerkzeug für die Erzeugung der Anfrage. Ein Werkzeug, das jedoch genutzt werden kann, ist `icmpquery`. Dieses Werkzeug ist unter *http://www.angio.net/security/* erhältlich. Hiermit können Rechner erreicht werden, bei denen ein Ping durch eine Firewall blockiert wird. Linux reagiert auf einen Address Mask Request nicht.

C.6.8 Timestamp Request und Reply

Diese Meldungen sind in der Lage, die Latenz des Netzwerks zu messen. Hierzu ist es jedoch erforderlich, dass sowohl der Absender als auch der Empfänger synchrone Uhrzeiten verwenden. Ähnlich den Echo-Meldungen und den Address-

Mask-Meldungen verwenden diese Meldungen auch eine Identifikationsnummer und eine Sequenznummer, um die Pakete zuordnen zu können. Ein Werkzeug, das in der Lage ist, diese Meldungen zu erzeugen, ist `icmpquery`. Es wurde bereits bei den Address-Mask-Meldungen erwähnt. Der Linux-Kernel 2.4 reagiert auf eine derartige Anfrage nicht mehr. Der Linux-Kernel 2.2 beantwortet diese Anfrage.

C.6.9 Router Solicitation und Advertisement

Wenn ein Netzwerkgerät, das das Router-Discovery-Protokoll unterstützt, eingeschaltet wird, sendet es eine Router-Solicitation-Meldung. Alle weiteren Router in demselben Netzwerk antworten mit einer Router-Advertisement-Nachricht. Damit alle Router die Solicitation-Nachricht erhalten, wird diese entweder an die Broadcast-Adresse 255.255.255.255 oder die *All-Routers*-Multicast-Adresse 224.0.0.2 gesendet. Alle Router antworten auf diese Anfragen mit einem Unicast-Paket. Zusätzlich versenden die Router regelmäßig ohne Aufforderung Router-Advertisement-Meldungen an die Adresse 224.0.0.1.

C.7 ARP

Wenn zwei IP-fähige Netzwerkgeräte sich in einem lokalen Netz unterhalten möchten, so müssen sie zunächst ihre Hardware-Adressen austauschen. Die tatsächliche Kommunikation erfolgt nicht auf Basis der IP-Adressen, sondern anhand dieser Hardware-Adressen. Für das Medium Ethernet wurde das Address Resolution Protocol (ARP) entwickelt. Dieses Protokoll wurde inzwischen auf die meisten anderen Netzwerkmedien portiert. Es erlaubt einem Netzwerkgerät, eine Anfrage (ARP Request) zu senden, die von der entsprechenden Gegenstelle mit einer Antwort (ARP Reply) beantwortet wird.

ARP-Pakete werden auf der Data-Link-Schicht versendet. Das ist dieselbe Schicht, die von IP-Paketen genutzt wird. ARP-Pakete sind also unabhängig von IP-Paketen.

ARP-Anfragen werden üblicherweise an alle Rechner eines Netzes versandt. Die Zieladresse des Pakets ist daher ff:ff:ff:ff:ff:ff. Dies ist die Ethernet-Broadcast-Adresse. Alle Rechner des Netzes verarbeiten das Paket. Es antwortet aber nur derjenige Rechner, der die richtige IP-Adresse besitzt.

Die Ergebnisse dieser Anfragen werden von den Rechnern in einem ARP-Cache zwischengespeichert. Das Verhalten des ARP-Caches wird unter Linux über das `sysctl`-Interface in `/proc/sys/net/ipv4/neigh/*/` gesteuert. Die Manpage des ARP-Kernel-Moduls `arp (7)` gibt nähere Auskunft über die Werte. Der Inhalt des ARP-Caches kann mit dem Befehl `arp` angezeigt werden:

```
# tcpdump -np arp
tcpdump: listening on eth1
15:22:23.374171 0:10:a4:c3:26:cb Broadcast arp 42: arp who-has 192.168.0.101
  tell 192.168.0.202 15:22:23.374625 0:e0:7d:7d:70:69 0:10:a4:c3:26: arp 60:cb
  arp reply 192.168.0.101 is-at 0:e0:7d:7d:70:69
```

```
Ctrl-C
# arp -an
? (192.168.0.1) auf 00:50:BF:11:23:DF [ether] auf eth1
? (192.168.0.101) auf 00:E0:7D:7D:70:69 [ether] auf eth1
```

Der Linux-Kernel kann maximal 1024 Einträge in seinem Cache verwalten.

Hinweis: ARP-Spoofing

ARP führt keine Authentifizierung durch. ARP-Antworten können daher gefälscht werden. Viele Betriebssysteme verarbeiten alle ARP-Antworten, die sie sehen, ohne dass sie jemals eine ARP-Anfrage gesendet hätten. Des Weiteren gibt es die Möglichkeit des so genannten Gratuitous ARP. Hierbei aktualisiert der Empfänger einen bereits vorhandenen Eintrag.

Literaturverzeichnis

[1]. Anonymous: *Der neue Hacker's Guide*. 2., überarbeitete Aufl. München: Markt+Technik 2001.

[2]. Anonymous: *Der neue Linux Hacker's Guide*. 1. Aufl. München: Markt+Technik 2001.

[3]. Bace, Rebecca Gurly: *Intrusion Detection*. 1. Aufl. Indianapolis: Newriders 2000.

[4]. Barman Scot: *Writing Information Security Policies*. 1. Aufl. Indianapolis: New Riders 2002.

[5]. Barrett, Daniel J., Richard E. Silverman: *SSH: Secure Shell – Ein umfassendes Handbuch*. 1. Aufl. Köln: O'Reilly 2001.

[6]. Bellovin, William, Steven Cheswick: *Firewalls und Sicherheit im Internet*. 2., überarbeitete Aufl. Bonn u.a.: Addison-Wesley 1995.

[7]. Blaze, Matt, Whitfield Diffie, Ronald I. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thomson, Michael Wiener: *Minimal Key Length of Symmetric Ciphers to Proved Adequate Commercial Security*. 1996. *http://www.counterpane.com/keylength.html*

[8]. Cavallar, Stefania, Bruce Dodson, Arjen K. Lenstra, Walter Lioen, Peter L. Montgomery, Brian Murphy, Herman te Riele, Karen Aardal, Jeff Gilchrist, Gérard Guillerm, Paul Leyland, et al.: *Factorisation of a 512-bit RSA modulus*. In: Theory and Application of Cryptographic Techniques, *ftp://ftp.gage.polytechnique.fr/pub/publications/jma/rsa-155.ps*.

[9]. Erickson, Jon: Hacking: *The Art of Exploitation*. San Francisco: No Starch Press 2003.

[10]. Friedl, Jeffrey E.F.: *Reguläre Ausdrücke*. 1. Aufl. Köln: O'Reilly 1997.

[11]. Hall, Eric A.: *Internet Core Protocols: The Definitive Guide*. 1. Aufl. Sebastopol u.a.: O'Reilly 2000.

[12]. Hildebrandt, Ralf, Patrick B. Koetter: *Postfix*. Heidelberg: Dpunkt Verlag 2005.

[13]. Kahn, David: *The Codebreakers*. 2., überarbeitete Aufl. New York: Simon & Schuster Inc. 1997.

[14]. Klein, Tobias: *Buffer Overflows und Format-String-Schwachstellen*. Heidelberg: Dpunkt Verlag 2003.

[15]. Kurtz, George, Stuart McClure, Joel Scambray: *Das Anti-Hacker Buch*. 3. Aufl. Bonn: MITP 2001.

[16]. Lenstra, Arjen K., Eric R. Verheul: *Selecting Cryptographic Key Sizes*. In: Journal of Cryptology. Bd. 14(4) 2001. S. 255-293.

[17]. MacDonald, Alistair: *SpamAssassin*. München u.a.: Addison-Wesley 2005.

[18]. Mandia, Kevin, Chris Prosise: *Incident Response: Investigating Computer Crime*. 1. Aufl. New York u.a.: Osborne/McGraw Hill 2001.

[19]. Mann, Scott, Ellen L. Mitchell: *Linux System Security*. 1. Aufl. Upper Saddle River: Prentice Hall 2002.

[20]. Northcutt, Stephen, Mark Cooper, Matt Fearnow, Karen Frederick: *Intrusion Signatures and Analysis.* 1. Aufl. Indianapolis: New Riders 2001.

[21]. Northcutt, Stephen, Judy Novak: *Network Intrusion Detection: An Analyst's Handbook*. 2. Aufl. Indianapolis: New Riders; 2001; ISBN 0-7357-1008-2

[22]. Proctor, Paul E.: *The Practical Intrusion Detection Handbook*. 1. Aufl. Upper Saddle River: Prentice Hall PTR 2001.

[23]. The Honeynet Project: *Know Your Enemy*. 1. Aufl. Reading u.a.: Addison Wesley 2002.

[24]. Toxen, Bob: *Real World Linux Security*. 1. Aufl. Upper Saddle River: Prentice Hall 2001.

[25]. Schneier, Bruce: *Applied Cryptography*. 2., überarbeitete Aufl. New York u.a.: John Wiley & Sons 1995.

[26]. Schultz, E. Eugene, Russell Shumway: *Incident Response.* 1. Aufl. Indianapolis: New Riders 2001.

[27]. Spenneberg, Ralf: *Intrusion Detection und Prevention mit Snort und Co*. Bonn u.a.: Addison-Wesley 2004.

[28]. Spenneberg, Ralf: *VPN mit Linux*. München u.a.: Addison-Wesley 2003.

[29]. Stevens, W. Richard: *TCP/IP Illustrated*. Bd. 1., 1. Aufl. Reading u.a.: Addison Wesley 1994.

[30]. Stoll, Clifford: *Kuckucksei*. 5. Aufl. Frankfurt am Main: Fischer Taschenbuchverlag 1998.

[31]. Wyk, Kenneth R. van, Richard Forno: *Incident Response*. 1. Aufl. Sebastopol u.a.: O'Reilly 2001.

[32]. Ziegler, Robert L.: *Linux Firewalls*. 2., überarbeitete Aufl. München: Markt+ Technik Verlag 2002.

Stichwortverzeichnis

S

U

Über den Autor

Ralf Spenneberg ist seit vielen Jahren als freier Trainer, Berater und Autor im Linux- und Unix-Umfeld tätig. Das vorliegende Buch ist aus verschiedenen Kursen und Workshops entstanden, die er im Laufe der Jahre gehalten hat. Nach dem Studium der Biochemie war er lange Zeit als Systemadministrator tätig. Anschließend begann er bereits 1998, Schulungen für Linux und Unix anzubieten. Seit Januar 2000 ist er zertifiziert als RHCE und RHCX und führt auch für Red Hat in Deutschland und England Schulungen durch. Im Rahmen dieser Zusammenarbeit hat er für Red Hat zwei Kurse zu den Themen Firewalling und VPN entwickelt. Weitere Informationen bietet er auf seiner Homepage *http://www.spenneberg.com* an. Wenn Sie eine Schulung bei ihm besuchen möchten, können Sie sich auf *http://www.opensource-training.de* informieren.