

Firewall Lösungen mit Linux

Kurs 1004

© 2005-2012 OpenSource Training Ralf Spenneberg

Am Bahnhof 3-5

48565 Steinfurt

<http://www.opensource-training.de>

<http://www.os-t.de>

Copyright

Die in diesem Kurs zur Verfügung gestellten Folien, Unterlagen und Übungen sind urheberrechtlich geschützt. Wir behalten uns alle Rechte vor, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Die gewerbliche Nutzung ist nicht erlaubt.

Die Informationen in diesem Produkt werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit genutzt. Fast alle Hardware- und Softwarebezeichnungen, die in dieser Unterlage erwähnt werden, sind gleichzeitig auch eingetragene Warenzeichen.

Bei der Zusammenstellung der Texte und Abbildungen wurde mit größter Sorgfalt vorgegangen. Jedoch können Fehler nicht vollständig ausgeschlossen werden. Die Firma OpenSource Training Ralf Spenneberg kann für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Für Verbesserungsvorschläge und Hinweise auf Fehler sind wir dankbar.

Inhaltsverzeichnis

1	Firewall Einführung	5
1.1	Einführung	5
1.2	Firewall-Technologien	9
1.2.1	Paketfilter	11
1.2.2	Application-Level-Gateway	13
1.3	Architekturen	15
1.3.1	Screening Router	15
1.3.2	Dreibeinige Firewall	17
1.3.3	Multiple DMZ	19
2	Iptables I	21
2.1	Einführung	21
2.2	Übersicht Firewall-Tabellen	23
2.3	Filtertabelle	25
2.3.1	Filterregeln in Ketten organisieren	27
2.4	Syntax	31
2.4.1	Der iptables-Befehl	31
2.4.2	Filteraktionen	35
2.4.3	Protokoll-spezifische Regeln	39
2.4.4	Zustandsbasierte Filterung (Stateful Firewall)	43
2.5	Lokale Firewall	47
2.5.1	Loopback-Device	49
2.6	Typische Protokolle	51
3	Iptables II	53
3.1	Network Address Translation	53
3.2	Funktionsweise von NAT	55
3.3	NAT-Tabelle und Ketten	57
3.4	Typische Network Address Translation Regeln	59
3.5	Hilfsmittel	61
3.5.1	Mehrere Ports mittels multiport filtern	61
3.5.2	Verbindungen zählen	63
3.6	Connection Tracking Helpers (Stateful Inspection)	65
3.7	Mangle-Tabelle	67
3.7.1	Filteraktionen	69
3.7.2	Explicit-Congestion-Notification	71
3.7.3	TCP MSS	73
3.7.4	Markieren von Paketen	75
3.8	Benutzerdefinierte Ketten	81
3.8.1	Verwaltung benutzerdefinierter Ketten	83
3.9	Accounting Regeln	87

3.10	Administrationsoberflächen	89
4	Application Layer Gateways	91
4.1	Überblick	91
4.2	HTTP/FTP - Apache/Squid	93
4.2.1	HAVP	93
4.2.2	Squid	99
4.3	SMTP - Postfix	107
4.3.1	Standalone Postfix	109
4.3.2	Relay Postfix	111
4.3.3	Amavisd-New	113
4.3.4	Virens Scanner einbinden	117
5	Firewall Test	123
5.1	Testwerkzeuge	123
5.1.1	Nmap	125
5.1.2	Nessus	127
5.1.3	BOSS	129
6	Protokolle und Zeitsynchronisation	131
6.1	Zentrale Protokollierung	131
6.2	Syslog-ng	133
6.2.1	Konfiguration	135
6.3	Protokolle auswerten	139
6.4	Zeitsynchronisation	141
6.4.1	Clientseitiger NTP-Daemon	143
6.4.2	NTP-Server	145
6.4.3	NTP Überwachung	147
7	Härtung	151
7.1	Gefahren für IT-Systeme	151
7.2	Systemhärtung	153
7.3	Angriffsverläufe	155
7.4	Rootkits	157
7.5	Systemsicherheit erhöhen	159
7.6	SELinux	163

Index

/usr/lib/squid/*, 104

ACCEPT, 14

Accounting, 87

Administrationsoberflächen, 89

Amavisd-New, 91, 115

Angriffe, 155

Angriffsverlauf, 155

Apache, 91

AppArmor, 159, 161

Application-Level-Gateway, 9, 13

arptables, 21

BOSS, 123, 129

BSI, 123

Circuit-Level Gateway, 9

CLASSIFY, 69

Connection Tracking, 44

Dienste

 anbieten, 17

 Ports, 51

 Protokolle, 51

DMZ, 17

 multiple, 19

DNAT, 53

DSCP, 69

eatables, 21

ECN, 69, 71

Filterregeln, *siehe* Regeln

Filtertabelle, *siehe* Tables, 25

 Gateway, 29

 Ketten, 25

 Server, 29

Firestarter, 89

Firewall

 Aufgaben, 7

 Definition, 5

 DMZ, 17

 Ketten, 23

 lokale, 47

 Technologien, 9

 testen, 123

Firewall Builder, 89

Frox, 91

Gefahren, 151

 Buffer-Overflows, 151

 Formatstring, 151

 Race Conditions, 151

grsecurity, 159

Härtung, 151

hashlimit, 63

HAVP, 91, 93

 Aufbau, 95

 Installation, 97

Hochverfügbarkeit, 7

htpasswd, 104

httpf, 91

ICMP, 12

Identd, 37

idfwadm, 21

Inhaltsanalyse, 14

 Modifikation, 14

IP, 12

 Header, 12

ip6tables, 21

ipchains, 21

iptables, 21, 31

 -A, 31

 -F, 31

 -I, 31

 -L, 31

 -N, 83

 -P, 31

 -X, 83

 -j, 83

 -m, 61

 -p icmp -h, 33

 -vL, 33

 -vnL, 33

 --set-mark, 75

- state, 45
- CLASSIFY, 79
- Filtertabelle, 25
 - Ketten, *siehe* Ketten
- hashlimit, 63
- limit, 63
- Matches, 39
- ROUTE, 77
- Tabellen, 23

- Ketten, 23, 25
 - Aufbau, 27
 - benutzerdefinierte, 81
 - Funktion, 27

- LIDS, 159
- loopback, 49

- MARK, 69
- MASQUERADE, 57
- Matches, 39
- Multiport, 61

- NAT, 23, 53
 - Funktionsweise, 55
- NAT-Tabelle, 57
- Nessus, 123, 127
- Network Address Translation, *siehe* NAT
- Network Time Protocol, 141
- Nmap, 123, 125
- ntp, 141
- ntpd, 143, 145

- OUTPUT, 57

- Pakete
 - markieren, 75
 - zählen, 87
- Paketfiler
 - stateful Inspection, 65
- Paketfilter, 9
 - Aufgaben, 11
 - Funktionen, 11
 - stateful, 43
- Path-MTU-Discovery, 73
- pktables, 21
- Postfix, 91, 107

- Relay, 111
 - Standalone Mailserver, 109
- POSTROUTING, 57
- PREROUTING, 57
- Privoxy, 91
- Protokoll, 39
- Proxy, *siehe* Application-Level-Gateway, 17
- Proxy-Kaskade, 105

- QoS, 7, 75
- Quality of Service, *siehe* QoS
- Quarantäne, 119

- Regeln
 - ACCEPT, 12, 35
 - DROP, 12, 35, 37
 - Interface, 39
 - loopback, 49
 - Matches, 39
 - NAT, 59
 - Ports, 41
 - Quelladresse, 39
 - REJECT, 12, 35, 37
 - TCP-Flags, 41
 - Verwaltung, 31
 - Zieladresse, 39
- REJECT, 14
- Rootkit, 157
 - dateibasierte, 157
 - kmem-Patching, 157
 - LKM, 157
 - Samhain, 157
- ROUTE, 69
- Routing, 77
- RSBAC, 159
- Rsyslog, 131

- SELinux, 159, 163
- Shorewall, 89
- SMTP, 91
- SNAT, 53
- SOCKS, 9
- Squid, 91, 99
 - ACL, 101
 - Benutzerauthentifizierung, 103
- stateful Inspection Paketfilter, 65

Stratum, 147
 Syslog-ng, 131, 133
 Konfiguration, 135

Tabelle
 Mangle, 67

Tables, 23
 Broute, 23
 Filter, 23, 25
 FORWARD, 25, 29
 INPUT, 25, 29, 47
 OUTPUT, 25, 29, 47
 Mangle, 23
 FORWARD, 67
 INPUT, 67
 OUTPUT, 67
 POSTROUTING, 67
 PREROUTING, 67
 Ziele, 69
 NAT, 23, 57
 MASQUERADE, 57
 OUTPUT, 57
 POSTROUTING, 57
 PREROUTING, 57
 Raw, 23

TCP, 12
 ACK-Scan, 125
 Fin-Scan, 125
 Maximum-Segment-Size, 23
 MSS, 23, 73
 Syn-Scan, 125
 Tests, 41

TCPMSS, 69

Testwerkzeuge, 123

TOS, 69

TTL, 69

UDP, 12
 Tests, 41

Virensscanner, 97, 117

Zentrale Protokollierung, 131

Zustandsüberwachung, 43
 ESTABLISHED, 43
 INVALID, 43
 NEW, 43

RELATED, 43
 UNTRACKED, 43