

Jörg Fritsch, Steffen Gundel

Firewalls im Unternehmenseinsatz

Grundlagen, Betrieb und Produkte

2., überarbeitete und aktualisierte Auflage



dpunkt.verlag

Inhaltsverzeichnis

Vorwort	1
Was wir mit diesem Buch erreichen wollen	1
Zielgruppe	2
Der Aufbau dieses Buches	3
Teil I: Einführung	
1 Tatort: Das Testnetzwerk	9
1.1 Aufbau des Testnetzwerks	12
1.1.1 Server- und PC-Landschaft	13
1.1.2 Internetanbindung und Webplattform	16
1.1.3 Remote-Access-Zugänge	22
1.1.4 IP-Adresskonzept	24
1.2 Layer-2-Switche und VLANs im Umfeld von Firewalls	27
1.2.1 VLANs und Layer-2-Attacken	27
1.2.2 Topologische Aspekte von VLANs	29
2 Technologien in Umfeld von Firewalls	33
2.1 Was ist eine Firewall?	33
2.2 Einiges zu TCP/IP	34
2.2.1 Header und Kapselung	34
2.2.2 Fragmentierung	36
2.2.3 Ports und Netzwerkverbindungen	36

2.3	Paketfilter	38
2.3.1	Statische Paketfilter	38
2.3.2	Dynamische Paketfilter	42
2.4	Proxy-Firewalls	50
2.4.1	Vorteile von Proxy-Firewalls	52
2.4.2	Probleme von Proxy-Firewalls	52
2.5	Firewalls in der Praxis: Hybrid-Technologie	54
2.5.1	Hybrid-Firewalls auf Paketfilter-Basis	54
2.5.2	Hybrid-Firewalls auf Proxy-Basis	55
2.5.3	Die Begriffe »Firewall-Umgebung« und »DMZ«	55
2.6	Weitere Aufgaben von Firewalls	56
2.6.1	Logging, Alerting und Accounting	57
2.6.2	Authentifizierung	58
2.6.3	Adressübersetzung	59
2.6.4	Verschlüsselung	62
2.6.5	Content Security	63
2.6.6	Intrusion Prevention	66
3	IP-Forwarding	73
3.1	Verarbeitung von Netzwerkverkehr im PC-Router	75
3.2	Routing und Forwarding	77
3.3	Eine Appliance mit PC-Architektur: Cisco PIX Firewall	79
3.4	PC-Architekturen ausreizen: Check Point SecureXL API	79
3.5	Nutzung der SecureXL API Beispiel 1: Check Point FireWall-1 Performance Pack und Nokia IPSO ab rev. 3.8	80
3.6	Verarbeitung von Netzwerkverkehr in echten Routern	82
3.7	Nutzung der SecureXL API Beispiel 2: Nortel Networks Alteon Switched Firewall System (ASFS)	84

Teil 2: Implementierung und Betrieb von Firewalls

4	Integration von Firewalls in das Unternehmensnetzwerk	89
4.1	Absicherung des Internetzugangs mit einer Firewall	90
4.1.1	Ausgangssituation	90
4.1.2	Das Sicherheitsproblem	92
4.1.3	Netzwerkseitige Integration der Firewall	94
4.1.4	Bildung von DMZs	97
4.1.5	Das Produkt: Check Point FireWall-1	98
4.1.6	Sun als Plattform	98
4.1.7	Alternative Plattformen	104
4.1.8	Installation der Check Point FireWall-1	106
4.1.9	Konfiguration der Check Point FireWall-1	108
4.2	Aufbau einer Intranet-Firewall	124
4.2.1	Ausgangssituation	124
4.2.2	Sicherheitsprobleme und Lösungsansätze	129
4.2.3	Modifikation der Ausgangssituation	135
4.2.4	Netzwerkseitige Integration der Firewall	136
4.2.5	Das Produkt: Cisco PIX	139
4.2.6	Funktionsweise und Interna der Cisco PIX	140
4.2.7	Installation der Cisco PIX	142
4.2.8	Konfiguration der Cisco PIX	142
4.2.9	Ausblick	155
4.3	Grenzen von Firewalls	160
5	Virtual Private Networks und sichere Verbindungen	161
5.1	Überblick über VPN-Technologien	164
5.1.1	Layer-2-basierte VPNs: ATM	164
5.1.2	Layer-3-basierte VPNs: MPLS	165
5.1.3	IPSec-VPNs (Layer 3 und Layer 4)	167
5.1.4	Applikationstunnel auf Layer 4: SSL-VPNs	168
5.2	IPSec = AH + ESP + (IPcomp) + ISAKMP/IKE	168
5.2.1	IP Authentication Header (AH)	169
5.2.2	IP Encapsulation Security Payload (ESP; RFC 2604)	170
5.2.3	Internet Key Exchange (IKE)	177

6	VPNs im Umfeld von Firewalls	181
6.1	Remote-Access-VPNs	183
6.1.1	IPSec-basierte Remote-Access-VPNs	184
6.1.2	Anforderungen an IPSec-basierte Remote-Access-VPNs	186
6.1.3	SSL-basierte Remote-Access-VPNs	188
6.1.4	Vergleich von SSL- und IPSec-VPNs	192
6.2	Check Point VPN-1 und SecuRemote/SecureClient	193
6.3	Konfiguration eines Remote-Access-VPNs für das Firmennetzwerk .	196
6.3.1	Ausgangssituation	196
6.3.2	Konfiguration der Check Point FireWall-1/VPN-1	197
6.3.3	Clientseitige Konfiguration	209
6.3.4	Aufbau eines Tunnels zum Firmennetzwerk	210
6.4	Konfiguration eines Site-to-Site-VPNs für das Firmennetzwerk	211
6.4.1	Ausgangssituation	211
6.4.2	Vorbereitungen zum Aufbau eines Site-to-Site-VPNs	212
6.4.3	Konfiguration der Check Point FireWall-1/VPN-1 (Unternehmensseite)	214
6.4.4	Konfiguration der Cisco-PIX-Firewall (Partnerfirma)	218
7	Management von Firewalls	221
7.1	Management-Architekturen	222
7.1.1	2-Tier- und 3-Tier-Architekturen	222
7.1.2	Metamanagement	226
7.1.3	Virtuelle Interfaces und virtuelle Firewalls	234
7.2	Betrieb von Firewalls	237
7.2.1	Analyse der Logdatei der Firewall	237
7.2.2	Troubleshooting von Kommunikationsproblemen	245
7.2.3	Pflege der Regelbasis	248

Teil 3: Hochverfügbarkeit

8	Redundanz und Loadbalancing	255
8.1	Statussynchronisation bei Firewalls	255
8.1.1	Firewallsynchronisation bei der Cisco PIX	257
8.1.2	Firewallsynchronisation bei der Check Point FireWall-1	258
8.2	Hot-Standby-Lösungen	259
8.2.1	Cisco-PIX-HA-Cluster	260
8.2.2	Stonebeat HA	264
8.2.3	Nokia HA: VRRP	269
8.2.4	Check Point Cluster XL	278
8.3	Lastverteilte Systeme	281
8.3.1	Stonebeat FullCluster: Multicast-MAC-Adressen	283
8.3.2	Rainfinity RainWall: gratuitous ARP (gARP)	294
8.3.3	Check Point Cluster XL	305
8.4	Hardware-Loadbalancing	306
8.4.1	Nortel Networks Alteon Webswitch	307
8.4.2	Radware FireProof	316
9	Multilink-Anbindungen und Multihoming	323
9.1	Nutzen von Multilink-Anbindungen	324
9.2	Multilink-Anbindungen mit Routing-Protokollen: BGP	328
9.3	Multilink-Anbindungen mittels DNS und NAT	329
9.3.1	Rainfinity RainConnect	332
9.3.2	Radware LinkProof	342