

Inhaltsverzeichnis

Vorwort	xii
Einleitung	17
I Für Einsteiger	21
1 Quickstart	23
Was ist OPNsense?	23
IP-Adresse	23
Einrichtung	24
Übersicht	25
Zusammenfassung	26
2 Labornetzwerk	27
Ressourcen	27
Virtualisierung	30
Hardware	31
Netze	31
Firewall	32
Adressierung	32
Labor-Server	33
Verwendung	34
3 Plattform	35
Vorbereitung	36
VMware	36

VirtualBox	41
Hardware	45
4 Installation	49
Betriebssystem	49
Speichermedium	51
Nacharbeiten	52
5 Ersteinrichtung	55
Ersteinrichtung	56
Zweiteinrichtung	59
Routing	62
Generalprobe	64
Zusammenfassung	65
II Für Fortgeschrittene	67
6 Firewall	69
OPNsense als Firewall	70
Laboraufbau	71
Filterregeln	71
Logging	74
Durchsatz	75
Best Practice	75
Zusätzliche Filter	77
Technischer Hintergrund	81
Reihenfolge der Abarbeitung	82
Fehlersuche	83
Zusammenfassung	84
7 Transparente Firewall	85
Vor- und Nachteile	85
Laboraufbau	86
Einrichtung	87
Filterlogik	89
Regelwerk	90

Transparente Firewall aufdecken	91
Technischer Hintergrund	91
Zusammenfassung	92
8 Network Address Translation	93
Laboraufbau	94
Szenarios	95
IPv6	102
NAT Reflection	103
Technischer Hintergrund	104
Zusammenfassung	105
9 Management-Interface	107
Zwei-Faktor-Authentifizierung	113
Zusammenfassung	116
III Für Experten	117
10 IPsec VPN	119
Sicherheit	120
Laboraufbau	121
Verbindungsaufbau	122
Address Translation	127
Dead Peer Detection	129
IPv6	130
VPN-Durchsatz	131
Fehlersuche	131
Technischer Hintergrund	134
Ausblick	135
Zusammenfassung	139
11 OpenVPN	141
Arbeitsweise	141
Authentifizierung	142
Unterschiede zu IPsec	143
Laboraufbau	145

Site-to-Site-Tunnel	146
Client-Server-Tunnel	150
Fehlersuche	155
Zertifikate	157
Technischer Hintergrund	158
Zusammenfassung	158
12 Hochverfügbarkeit	161
Grundlagen	161
Labor	162
Adressumsetzung	166
Best Practice	171
Schnelleres Failover	173
Lastverteilung	174
IP Version 6	176
Technischer Hintergrund	176
Zusammenfassung	177
13 NetFlow	179
Inhalt eines Flows	179
Labor	180
Kollektor	182
Troubleshooting	183
Einblick	183
Technischer Hintergrund	184
IPv6	185
Zusammenfassung	185
14 Web-Proxy	187
Laboraufbau	189
Expliziter Proxy	190
Proxy-Cluster	198
TLS Inspection	201
Transparenter Proxy	205
Technischer Hintergrund	207
Ausblick	208
Zusammenfassung	209

15	Zentrale Authentifizierung	211
	Protokolle	211
	Laboraufbau	213
	Microsoft Server	214
	Directory-as-a-Service	221
	Zwei-Faktor-Authentifizierung	229
	Fehlersuche	230
	Technischer Hintergrund	234
	Zusammenfassung	234
IV	Für Praktiker	237
16	Multi-WAN	239
	Anforderung	240
	Lastverteilung im WAN	241
	Laborumgebung	241
	Arbeitsweise	242
	Einrichtung	243
	Szenario	248
	Monitoring	250
	IPv6	250
	Technischer Hintergrund	252
	Zusammenfassung	253
17	DSL-Router	255
	DSL-Anschlüsse	255
	Laboraufbau	256
	PPPoE-Einwahl	257
	LAN-Ports	260
	DNS und DHCP	262
	IPv4 mit Adressumsetzung	264
	IPv6 mit Präfix-Delegation	264
	Firewall	267
	Technischer Hintergrund	268
	Zusammenfassung	269

18 Einbruchserkennung	271
IPS und IDS	271
Platzierung im Netz	272
Laboraufbau	273
Angriff	274
IDS einschalten	274
IPS einschalten	277
Transparentes IDS	278
Technischer Hintergrund	281
Zusammenfassung	283
19 Kommandozeile	285
configd	285
Konfigurationsänderungen	287
Rückgängig	292
Updates	293
Zusammenfassung	294
20 Performance Tuning	295
Laboraufbau	295
Auslastung	296
Virtueller Netzadapter	298
Routing-Durchsatz	300
IPsec-Durchsatz	302
Leistungssteigerung	305
Fazit	313
V Für Trickser	315
21 Best Practice	317
Factory-Default	317
Durchsatz messen	318
SSH-Login ohne Passworteingabe	320
Passwort zurücksetzen	323

22 Konfiguration	327
Dropbox	328
Google Drive	331
Zusammenfassung	335
23 Life Hacks	337
Zugriff von Windows	338
Mirror Port	338
Telegram	339
Firewallregeln mit Kategorien	342
Schnellsuche	343
Snapshots	344
24 Application Programming Interface	347
Wie funktioniert die API?	348
Lesender Zugriff	351
Schreibender Zugriff	353
Was kann die API leisten?	355
API-Browser	356
Sicherheit	357
Technischer Hintergrund	359
Ausblick	359
Zusammenfassung	359
Literaturverzeichnis	361
Index	365
A IP Version 6	373
B Editor unter FreeBSD	377
C Mustererkennung	381
D Zusatzmaterial	387