

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	46
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	89

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	104
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	132
Technischer Hintergrund	134
Ausblick	135
Zusammenfassung	140
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	159
Grundlagen	159
Labor	160
Adressumsetzung	164
Best Practice	169
Schnelleres Failover	171
Lastverteilung	172
IP Version 6	174
Technischer Hintergrund	174
Zusammenfassung	175
13 NetFlow	177
Inhalt eines Flows	177
Labor	178
Kollektor	180
Troubleshooting	181
Einblick	181
Technischer Hintergrund	182
IPv6	183
Zusammenfassung	183
14 Web-Proxy	185
Laboraufbau	187
Expliziter Proxy	188
Proxy-Cluster	194
TLS Inspection	197
Transparenter Proxy	201
Technischer Hintergrund	204
Was geht nicht?	204
Ausblick	204

Zusammenfassung	205
15 Zentrale Authentifizierung	207
Protokolle	207
Laboraufbau	209
Microsoft Server	210
Directory-as-a-Service	217
Zwei-Faktor-Authentifizierung	226
Fehlersuche	226
Technischer Hintergrund	230
Zusammenfassung	231
 IV Für Praktiker	 233
16 Multi-WAN	235
Anforderung	236
Lastverteilung im WAN	237
Laborumgebung	237
Arbeitsweise	238
Einrichtung	239
Szenario	244
Monitoring	246
IPv6	246
Technischer Hintergrund	247
Zusammenfassung	248
 17 DSL-Router	 251
DSL-Anschlüsse	251
Laboraufbau	252
PPPoE-Einwahl	253
LAN-Ports	257
DNS und DHCP	257
IPv4 mit Adressumsetzung	259
IPv6 mit Präfix-Delegation	260
Firewall	262
Technischer Hintergrund	264

Zusammenfassung	265
18 Einbruchserkennung	267
IPS und IDS	267
Platzierung im Netz	268
Laboraufbau	269
Angriff	270
IDS einschalten	270
IPS einschalten	273
Transparentes IDS	274
Technischer Hintergrund	277
Zusammenfassung	279
19 Kommandozeile	281
configd	281
Konfigurationsänderungen	283
Rückgängig	288
Updates	288
Zusammenfassung	290
20 Performance Tuning	291
Laboraufbau	291
Auslastung	292
Virtueller Netzadapter	294
Routing-Durchsatz	296
IPsec-Durchsatz	298
Leistungssteigerung	301
Fazit	309
V Für Trickser	311
21 Best Practice	313
Factory-Default	313
Durchsatz messen	314
SSH-Login ohne Passworteingabe	316
Passwort zurücksetzen	319

22 Konfiguration	323
Dropbox	323
Google Drive	327
Zusammenfassung	330
23 Life Hacks	333
Zugriff von Windows	334
Mirror Port	334
Telegram	335
Firewallregeln mit Kategorien	338
Schnellsuche	339
24 Application Programming Interface	341
Wie funktioniert die API?	342
Lesender Zugriff	345
Schreibender Zugriff	347
Was kann die API leisten?	349
API-Browser	350
Sicherheit	351
Technischer Hintergrund	352
Ausblick	353
Zusammenfassung	353
Literaturverzeichnis	355
Index	359
A IP Version 6	367
B Editor unter FreeBSD	371
C Mustererkennung	375
D Zusatzmaterial	381