

Inhaltsverzeichnis

Vorwort	xii
I Für Einsteiger	21
1 Labornetzwerk	23
Ressourcen	23
Virtualisierung	26
Hardware	27
Netze	27
Firewall	28
Adressierung	28
Labor-Server	29
Verwendung	29
2 Plattform	31
Vorbereitung	32
VMware	32
VirtualBox	37
Hardware	42
3 Installation	45
Betriebssystem	45
Speichermedium	47
Nacharbeiten	48

4	Ersteinrichtung	51
	Ersteinrichtung	52
	Zweiteinrichtung	54
	Routing	57
	Generalprobe	58
	Zusammenfassung	59
5	IP Version 6	61
	Grundlagen	61
	Laboraufbau	63
	Adressen und Routen	63
	Clients	64
	Verbindungen	66
	Zusammenfassung	66
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	82
	Reihenfolge der Abarbeitung	83
	Fehlersuche	83
	Zusammenfassung	85
7	Transparente Firewall	87
	Vor- und Nachteile	87
	Laboraufbau	88
	Einrichtung	89
	Filterlogik	91
	Regelwerk	91

Transparente Firewall aufdecken	93
Technischer Hintergrund	93
Zusammenfassung	94
8 Network Address Translation	95
Laboraufbau	96
Szenarios	97
IPv6	104
NAT Reflection	105
Technischer Hintergrund	106
Zusammenfassung	106
9 Management Interface	109
Zwei-Faktor-Authentifizierung	116
Zusammenfassung	118
III Für Experten	119
10 IPsec VPN	121
Sicherheit	122
Laboraufbau	123
Verbindungsaufbau	124
Address Translation	129
Dead Peer Detection	131
IPv6	132
VPN-Durchsatz	133
Fehlersuche	134
Technischer Hintergrund	136
Ausblick	137
Zusammenfassung	142
11 OpenVPN	143
Arbeitsweise	143
Authentifizierung	144
Unterschiede zu IPsec	145
Laboraufbau	147

Site-to-Site-Tunnel	148
Client-Server-Tunnel	152
Fehlersuche	157
Zertifikate	158
Technischer Hintergrund	160
Zusammenfassung	160
12 Hochverfügbarkeit	163
Grundlagen	163
Labor	164
Adressumsetzung	169
Best Practice	173
Schnelleres Failover	175
Lastverteilung	175
IP Version 6	178
Technischer Hintergrund	178
Zusammenfassung	179
13 NetFlow	181
Inhalt eines Flows	181
Labor	182
Kollektor	184
Troubleshooting	185
Einblick	185
Technischer Hintergrund	186
IPv6	187
Zusammenfassung	187
14 Web-Proxy	189
Laboraufbau	191
Expliziter Proxy	192
Proxy-Cluster	198
TLS Inspection	200
Transparenter Proxy	205
Technischer Hintergrund	207
Was geht nicht?	207
Ausblick	207

Zusammenfassung	208
15 Zentrale Authentifizierung	211
Protokolle	211
Laboraufbau	213
Microsoft Server	214
Directory-as-a-Service	221
Fehlersuche	230
Technischer Hintergrund	233
Zusammenfassung	234
 IV Für Praktiker	 235
16 Multi-WAN	237
Anforderung	238
Lastverteilung im WAN	239
Laborumgebung	239
Arbeitsweise	240
Einrichtung	241
Szenario	246
Monitoring	248
IPv6	248
Technischer Hintergrund	249
Zusammenfassung	250
 17 DSL-Router	 253
DSL-Anschlüsse	253
Laboraufbau	254
PPPoE-Einwahl	255
LAN-Ports	258
DNS und DHCP	259
IPv4 mit Adressumsetzung	261
IPv6 mit Präfix-Delegation	261
Firewall	264
Technischer Hintergrund	265
Zusammenfassung	266

18 Einbruchserkennung	269
IPS und IDS	269
Platzierung im Netz	270
Laboraufbau	271
Angriff	272
IDS einschalten	272
IPS einschalten	275
Transparentes IDS	276
Technischer Hintergrund	279
Zusammenfassung	281
 19 Kommandozeile	 283
configd	283
Konfigurationsänderungen	285
Rückgängig	286
Updates	287
Zusammenfassung	289
 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	338
24 Application Programming Interface	341
Wie funktioniert die API?	341
Lesender Zugriff	345
Schreibender Zugriff	347
Was kann die API leisten?	349
API-Browser	350
Sicherheit	350
Technischer Hintergrund	352
Ausblick	353
Zusammenfassung	353
Literaturverzeichnis	355
Index	359
A Editor unter FreeBSD	367
B Mustererkennung	371
C Zusatzmaterial	377