

# Inhaltsverzeichnis

<b>Vorwort</b>	<b>xii</b>
<b>I Für Einsteiger</b>	<b>21</b>
<b>1 Labornetzwerk</b>	<b>23</b>
Ressourcen . . . . .	23
Virtualisierung . . . . .	26
Hardware . . . . .	27
Netze . . . . .	27
Firewall . . . . .	28
Adressierung . . . . .	28
Labor-Server . . . . .	29
Verwendung . . . . .	29
<b>2 Plattform</b>	<b>31</b>
Vorbereitung . . . . .	32
VMware . . . . .	32
VirtualBox . . . . .	37
Hardware . . . . .	41
<b>3 Installation</b>	<b>45</b>
Betriebssystem . . . . .	45
Speichermedium . . . . .	47
Nacharbeiten . . . . .	48

---

<b>4</b>	<b>Ersteinrichtung</b>	<b>51</b>
	Ersteinrichtung . . . . .	52
	Zweiteinrichtung . . . . .	54
	Routing . . . . .	56
	Generalprobe . . . . .	58
	Zusammenfassung . . . . .	59
<b>5</b>	<b>IP Version 6</b>	<b>61</b>
	Grundlagen . . . . .	61
	Laboraufbau . . . . .	63
	Adressen und Routen . . . . .	63
	Clients . . . . .	64
	Verbindungen . . . . .	66
	Zusammenfassung . . . . .	67
<b>II</b>	<b>Für Fortgeschrittene</b>	<b>69</b>
<b>6</b>	<b>Firewall</b>	<b>71</b>
	OPNsense als Firewall . . . . .	72
	Laboraufbau . . . . .	73
	Filterregeln . . . . .	73
	Logging . . . . .	76
	Durchsatz . . . . .	77
	Best Practice . . . . .	77
	Zusätzliche Filter . . . . .	79
	Technischer Hintergrund . . . . .	83
	Reihenfolge der Abarbeitung . . . . .	84
	Fehlersuche . . . . .	85
	Zusammenfassung . . . . .	86
<b>7</b>	<b>Transparente Firewall</b>	<b>87</b>
	Vor- und Nachteile . . . . .	87
	Laboraufbau . . . . .	88
	Einrichtung . . . . .	89
	Filterlogik . . . . .	91
	Regelwerk . . . . .	92

---

Transparente Firewall aufdecken . . . . .	93
Technischer Hintergrund . . . . .	94
Zusammenfassung . . . . .	94
<b>8 Network Address Translation</b>	<b>95</b>
Laboraufbau . . . . .	96
Szenarios . . . . .	96
IPv6 . . . . .	104
NAT Reflection . . . . .	106
Technischer Hintergrund . . . . .	106
Zusammenfassung . . . . .	107
<b>9 Management Interface</b>	<b>109</b>
Zusammenfassung . . . . .	116
<b>III Für Experten</b>	<b>117</b>
<b>10 IPsec VPN</b>	<b>119</b>
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
<b>11 OpenVPN</b>	<b>141</b>
Arbeitsweise . . . . .	141
Authentifizierung . . . . .	142
Unterschiede zu IPsec . . . . .	143
Laboraufbau . . . . .	145
Site-to-Site-Tunnel . . . . .	146

---

Client-Server-Tunnel . . . . .	150
Fehlersuche . . . . .	154
Zertifikate . . . . .	157
Technischer Hintergrund . . . . .	158
Zusammenfassung . . . . .	159
<b>12 Hochverfügbarkeit</b>	<b>161</b>
Grundlagen . . . . .	161
Labor . . . . .	162
Adressumsetzung . . . . .	167
Best Practice . . . . .	171
Schnelleres Failover . . . . .	173
Lastverteilung . . . . .	174
IP Version 6 . . . . .	175
Technischer Hintergrund . . . . .	176
Zusammenfassung . . . . .	177
<b>13 NetFlow</b>	<b>179</b>
Inhalt eines Flows . . . . .	179
Labor . . . . .	180
Kollektor . . . . .	182
Troubleshooting . . . . .	183
Einblick . . . . .	184
Technischer Hintergrund . . . . .	185
IPv6 . . . . .	185
Zusammenfassung . . . . .	186
<b>14 Web-Proxy</b>	<b>187</b>
Labora Aufbau . . . . .	189
Expliziter Proxy . . . . .	190
Proxy-Cluster . . . . .	196
SSL Inspection . . . . .	198
Transparenter Proxy . . . . .	203
Technischer Hintergrund . . . . .	205
Was geht nicht? . . . . .	205
Ausblick . . . . .	206
Zusammenfassung . . . . .	207

---

<b>15 Zentrale Authentifizierung</b>	<b>209</b>
Protokolle . . . . .	209
Laboraufbau . . . . .	211
Microsoft Server . . . . .	212
Directory-as-a-Service . . . . .	219
Fehlersuche . . . . .	228
Technischer Hintergrund . . . . .	232
Zusammenfassung . . . . .	233
<b>IV Für Praktiker</b>	<b>235</b>
<b>16 Multi WAN</b>	<b>237</b>
Anforderung . . . . .	238
Lastverteilung im WAN . . . . .	239
Laborumgebung . . . . .	239
Arbeitsweise . . . . .	241
Einrichtung . . . . .	241
Szenario . . . . .	246
Monitoring . . . . .	248
IPv6 . . . . .	249
Technischer Hintergrund . . . . .	250
Zusammenfassung . . . . .	251
<b>17 DSL-Router</b>	<b>253</b>
DSL-Anschlüsse . . . . .	253
Laboraufbau . . . . .	254
PPPoE-Einwahl . . . . .	255
LAN-Ports . . . . .	259
DNS und DHCP . . . . .	259
IPv4 mit Adressumsetzung . . . . .	261
IPv6 mit Präfix-Delegation . . . . .	262
Firewall . . . . .	264
Technischer Hintergrund . . . . .	266
Zusammenfassung . . . . .	267

---

<b>18 Einbruchserkennung</b>	<b>269</b>
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
 <b>19 Kommandozeile</b>	 <b>283</b>
configd . . . . .	283
Konfigurationsänderungen . . . . .	285
Rückgängig . . . . .	287
Updates . . . . .	287
Zusammenfassung . . . . .	289
 <b>20 Performance Tuning</b>	 <b>291</b>
Laboraufbau . . . . .	291
Auslastung . . . . .	292
Virtueller Netzadapter . . . . .	294
Routing-Durchsatz . . . . .	297
IPsec-Durchsatz . . . . .	298
Leistungssteigerung . . . . .	301
Fazit . . . . .	310
 <b>V Für Trickser</b>	 <b>311</b>
 <b>21 Best Practice</b>	 <b>313</b>
Factory-Default . . . . .	313
Durchsatz messen . . . . .	314
SSH-Login ohne Passworteingabe . . . . .	316
Passwort zurücksetzen . . . . .	319

<b>22 Konfiguration</b>	<b>323</b>
Dropbox . . . . .	324
Google Drive . . . . .	327
Zusammenfassung . . . . .	331
<b>23 Life Hacks</b>	<b>333</b>
Zugriff von Windows . . . . .	334
Mirror Port . . . . .	334
Telegram . . . . .	335
Firewallregeln mit Kategorien . . . . .	338
Schnellsuche . . . . .	340
<b>24 Application Programming Interface</b>	<b>341</b>
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
<b>Literaturverzeichnis</b>	<b>355</b>
<b>Index</b>	<b>359</b>
<b>A Editor unter FreeBSD</b>	<b>367</b>
<b>B Mustererkennung</b>	<b>371</b>
<b>C Zusatzmaterial</b>	<b>377</b>