# 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 . . . . . 41

**3 Installation** **45**
Betriebssystem . . . . . 45
Speichermedium . . . . . 47
Nacharbeiten . . . . . 48

**4 Ersteinrichtung** **51**
Ersteinrichtung . . . . . 52
Zweiteinrichtung . . . . . 54
Routing . . . . . 56
Generalprobe . . . . . 58
Zusammenfassung . . . . . 59

**5 IP Version 6** **61**
Grundlagen . . . . . 61
Laboraufbau . . . . . 63
Adressen und Routen . . . . . 63
Clients . . . . . 64
Verbindungen . . . . . 65
Zusammenfassung . . . . . 67

**II Für Fortgeschrittene** **69**

**6 Firewall** **71**
OPNsense als Firewall . . . . . 72
Laboraufbau . . . . . 73
Filterregeln . . . . . 73
Logging . . . . . 76
Durchsatz . . . . . 77
Best Practice . . . . . 77
Zusätzliche Filter . . . . . 79
Technischer Hintergrund . . . . . 82
Reihenfolge der Abarbeitung . . . . . 83
Fehlersuche . . . . . 84
Zusammenfassung . . . . . 85

**7 Transparente Firewall** **87**
Vor- und Nachteile . . . . . 87
Laboraufbau . . . . . 88
Einrichtung . . . . . 89
Filterlogik . . . . . 91
Regelwerk . . . . . 92

Transparente Firewall aufdecken . . . . . 93
Technischer Hintergrund . . . . . 93
Zusammenfassung . . . . . 94

**8 Network Address Translation 95**
Laboraufbau . . . . . 96
Szenarios . . . . . 96
IPv6 . . . . . 104
NAT Reflection . . . . . 106
Technischer Hintergrund . . . . . 106
Zusammenfassung . . . . . 107

**9 Management Interface 109**
Zusammenfassung . . . . . 116

**III Für Experten 117**

**10 IPsec VPN 119**
Sicherheit . . . . . 120
Laboraufbau . . . . . 121
Verbindungsaufbau . . . . . 122
Address Translation . . . . . 126
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
Ausblick . . . . . 159

**12 Hochverfügbarkeit** **161**
Grundlagen . . . . . 161
Labor . . . . . 162
Adressumsetzung . . . . . 167
Best Practice . . . . . 171
Schnelleres Failover . . . . . 173
Lastverteilung . . . . . 174
IP Version 6 . . . . . 175
Technischer Hintergrund . . . . . 176
Zusammenfassung . . . . . 177

**13 NetFlow** **179**
Inhalt eines Flows . . . . . 179
Labor . . . . . 180
Kollektor . . . . . 182
Troubleshooting . . . . . 183
Einblick . . . . . 184
Technischer Hintergrund . . . . . 185
IPv6 . . . . . 185
Zusammenfassung . . . . . 186

**14 Web-Proxy** **187**
Laboraufbau . . . . . 189
Expliziter Proxy . . . . . 190
Proxy-Cluster . . . . . 196
SSL Inception . . . . . 198
Transparenter Proxy . . . . . 203
Technischer Hintergrund . . . . . 205
Was geht nicht? . . . . . 205
Ausblick . . . . . 206
Zusammenfassung . . . . . 207

**15 Zentrale Authentifizierung** **209**
Protokolle . . . . . 209
Laboraufbau . . . . . 211
Microsoft Server . . . . . 212
Directory-as-a-Service . . . . . 219
Fehlersuche . . . . . 228
Technischer Hintergrund . . . . . 231
Zusammenfassung . . . . . 232

**IV Für Praktiker** **233**

**16 Multi WAN** **235**
Anforderung . . . . . 236
Lastverteilung im WAN . . . . . 237
Laborumgebung . . . . . 237
Arbeitsweise . . . . . 239
Einrichtung . . . . . 239
Szenario . . . . . 244
Monitoring . . . . . 246
IPv6 . . . . . 247
Technischer Hintergrund . . . . . 247
Zusammenfassung . . . . . 248

**17 DSL-Router** **251**
DSL-Anschlüsse . . . . . 251
Laboraufbau . . . . . 252
PPPoE-Einwahl . . . . . 253
LAN-Ports . . . . . 256
DNS und DHCP . . . . . 257
IPv4 mit Adressumsetzung . . . . . 258
IPv6 mit Präfix-Delegation . . . . . 259
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 . . . . . 272
Transparentes IDS . . . . . 274
GeoIP . . . . . 278
Technischer Hintergrund . . . . . 279
Zusammenfassung . . . . . 280

**19 Kommandozeile** **283**
configd . . . . . 283
Konfigurationsänderungen . . . . . 285
Rückgängig . . . . . 287
Updates . . . . . 287
Zusammenfassung . . . . . 289

**20 Performance Tuning** **291**
Laboraufbau . . . . . 291
Auslastung . . . . . 292
Virtueller Netzadapter . . . . . 294
Routing-Durchsatz . . . . . 297
IPsec-Durchsatz . . . . . 298
Leistungssteigerung . . . . . 301
Fazit . . . . . 310

**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 . . . . . 324
Google Drive . . . . . 327
Zusammenfassung . . . . . 331

**23 Life Hacks** **333**
Zugriff von Windows . . . . . 334
Mirror Port . . . . . 334
Telegram . . . . . 335
Firewallregeln mit Kategorien . . . . . 338
Schnellsuche . . . . . 340

**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**