Contents

Preface **xii**

Introduction **17**

I For Beginners **21**

1 Quickstart **23**
What is OPNsense? 23
IP address 23
Setup 24
Overview 25
Summary 26

2 Lab Network **27**
Resources 27
Virtualization 30
Hardware 31
Networks 31
Firewall 32
Addressing 32
Lab Server 33
Utilization 34

3 Platform **35**
Preparation 36
VMware 36

VirtualBox . . . 41
Hardware . . . 45

4 Installation 49
Operating system . . . 49
Storage . . . 51
Post-installation tasks . . . 52

5 Initial Setup 55
Initial setup . . . 56
Secondary setup . . . 58
Routing . . . 61
Final testing . . . 63
Summary . . . 64

II For Intermediates 65

6 Firewall 67
OPNsense as a firewall . . . 68
Lab setup . . . 69
Firewall rules . . . 70
Logging . . . 71
Throughput . . . 72
Best practice . . . 73
Additional filter . . . 74
Technical background . . . 79
Order of processing . . . 80
Troubleshooting . . . 81
Summary . . . 82

7 Transparent Firewall 83
Pros and cons . . . 83
Lab setup . . . 84
Configuration . . . 85
Filter operation . . . 87
Ruleset . . . 87

Uncover transparent firewall 89
Technical background 89
Summary 90

8 Network Address Translation 91
Lab setup 92
Scenarios 93
IPv6 99
NAT Reflection 101
Technical background 102
Summary 102

9 Management Interface 103
Two-factor authentication 109
Summary 111

III For Experts 113

10 IPsec VPN 115
Security 116
Lab setup 117
Connection setup 118
Address translation 122
Dead Peer Detection 124
IPv6 125
VPN throughput 126
Troubleshooting 127
Technical background 129
Outlook 130
Summary 134

11 OpenVPN 135
Operation 135
Authentication 136
Differences to IPsec 137
Lab setup 139

Site-to-Site tunnel 140
Client-server tunnel 144
Troubleshooting 149
Certificates 150
Technical background 151
Summary 152

12 High Availability 153
Basics 153
Lab network 154
Address translation 158
Best practice 162
Quicker failover 165
Load balancing 165
IP version 6 167
Technical background 168
Summary 169

13 NetFlow 171
The content of a flow 171
Lab setup 172
Collector 174
Troubleshooting 175
Insight 175
Technical background 176
IPv6 177
Summary 177

14 Web Proxy 179
Lab setup 181
Explicit proxy 182
Proxy cluster 190
TLS Inspection 193
Transparent proxy 197
Technical background 199
Outlook 200
Summary 201

15 Central Authentication 203
Protocols 203
Lab setup 205
Microsoft Server 206
Directory-as-a-Service 213
Two-factor authentication 221
Troubleshooting 221
Technical background 225
Summary 225

IV For Hackers 227

16 Multi-WAN 229
Requirements 230
Load distribution in the WAN 231
Lab environment 231
Operation 232
Configuration 233
Scenario 238
Monitoring 239
IPv6 240
Technical background 241
Summary 242

17 DSL router 243
DSL types 243
Lab setup 244
PPPoE Dial-in 245
LAN adapters 249
DNS and DHCP 249
IPv4 with Address Translation 251
IPv6 with prefix delegation 252
Firewall 254
Technical background 256
Summary 257

18 Intrusion Detection **259**
IPS and IDS . . . 259
Network integration . . . 260
Lab setup . . . 260
Attack . . . 261
Activate IDS . . . 262
Activate IPS . . . 264
Transparent IDS . . . 265
Technical background . . . 268
Summary . . . 270

19 Command Line **271**
configd . . . 271
Configuration changes . . . 273
Undo changes . . . 277
Updates . . . 278
Summary . . . 279

20 Performance Tuning **281**
Lab setup . . . 281
Baseline . . . 282
Virtual network adapter . . . 283
Routing throughput . . . 286
IPsec throughput . . . 288
Increasing performance . . . 291
Summary . . . 298

V For Admins **299**

21 Best Practice **301**
Factory reset . . . 301
Benchmark throughput . . . 302
SSH login without password . . . 304
Password reset . . . 307

22 Configuration **311**
Dropbox 312
Google Drive 315
Summary 319

23 Life Hacks **321**
Access from Windows 322
Span port 322
Telegram 323
Firewall rules with category 326
Quick search 327
Snapshots 327

24 Application Programming Interface **329**
How does the API work? 329
Read Access 333
Write Access 335
What does the API cover? 336
API browser 338
Security 339
Technical background 340
Outlook 340
Summary 341

Bibliography **343**

Index **347**

A IP Version 6 **355**

B Editing Files in FreeBSD **359**

C Pattern Matching **363**

D Bonus Material **369**