

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	78
Order of processing	79
Troubleshooting	80
Summary	81
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	89
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	137
Operation	137
Authentication	138
Differences to IPsec	139
Lab setup	141

Site-to-Site tunnel	142
Client-server tunnel	146
Troubleshooting	151
Certificates	152
Technical background	153
Summary	154
12 High Availability	155
Basics	155
Lab network	156
Address translation	160
Best practice	164
Quicker failover	167
Load balancing	167
IP version 6	169
Technical background	170
Summary	171
13 NetFlow	173
The content of a flow	173
Lab setup	174
Collector	176
Troubleshooting	177
Insight	177
Technical background	178
IPv6	179
Summary	179
14 Web Proxy	181
Lab setup	183
Explicit proxy	184
Proxy cluster	190
TLS Inspection	192
Transparent proxy	197
Technical background	199
Limitations	199
Outlook	199

Summary	200
15 Central Authentication	201
Protocols	201
Lab setup	203
Microsoft Server	204
Directory-as-a-Service	211
Two-factor authentication	219
Troubleshooting	219
Technical background	223
Summary	223
IV For Hackers	225
16 Multi-WAN	227
Requirements	228
Load distribution in the WAN	229
Lab environment	229
Operation	230
Configuration	231
Scenario	236
Monitoring	237
IPv6	238
Technical background	239
Summary	240
17 DSL router	241
DSL types	241
Lab setup	243
PPPoE Dial-in	243
LAN adapters	246
DNS and DHCP	247
IPv4 with Address Translation	249
IPv6 with prefix delegation	249
Firewall	252
Technical background	253

Summary	254
18 Intrusion Detection	255
IPS and IDS	255
Network integration	256
Lab setup	256
Attack	257
Activate IDS	258
Activate IPS	260
Transparent IDS	261
Technical background	264
Summary	266
19 Command Line	267
configd	267
Configuration changes	269
Undo changes	273
Updates	274
Summary	275
20 Performance Tuning	277
Lab setup	277
Baseline	278
Virtual network adapter	279
Routing throughput	282
IPsec throughput	284
Increasing performance	287
Summary	294
V For Admins	295
21 Best Practice	297
Factory reset	297
Benchmark throughput	298
SSH login without password	300
Password reset	303

22 Configuration	307
Dropbox	307
Google Drive	311
Summary	315
23 Life Hacks	317
Access from Windows	318
Span port	318
Telegram	319
Firewall rules with category	322
Quick search	323
24 Application Programming Interface	325
How does the API work?	325
Read Access	329
Write Access	331
What does the API cover?	332
API browser	333
Security	334
Technical background	335
Outlook	336
Summary	336
Bibliography	337
Index	341
A IP Version 6	349
B Editing Files in FreeBSD	353
C Pattern Matching	357
D Bonus Material	363