

Contents

Preface	xii
Introduction	17
I For Beginners	21
1 Lab Network	23
Resources	23
Virtualization	26
Hardware	27
Networks	27
Firewall	28
Addressing	28
Lab Server	29
Utilization	30
2 Platform	31
Preparation	32
VMware	32
VirtualBox	37
Hardware	41
3 Installation	45
Operating system	45
Storage	47
Post-installation tasks	48

4	Initial Setup	51
	Initial setup	52
	Secondary setup	54
	Routing	57
	Final testing	58
	Summary	59
5	IP Version 6	61
	Crash course	61
	Lab setup	63
	Addresses and routes	63
	Clients	65
	Connections	66
	Summary	66
II	For Intermediates	67
6	Firewall	69
	OPNsense as a firewall	70
	Lab setup	71
	Firewall rules	71
	Logging	73
	Throughput	74
	Best practice	75
	Additional filter	76
	Technical background	81
	Order of processing	82
	Troubleshooting	83
	Summary	84
7	Transparent Firewall	85
	Pros and cons	85
	Lab setup	86
	Configuration	87
	Filter operation	89
	Ruleset	89

Uncover transparent firewall	91
Technical background	91
Summary	92
8 Network Address Translation	93
Lab setup	94
Scenarios	95
IPv6	101
NAT Reflection	103
Technical background	104
Summary	104
9 Management Interface	105
Two-factor authentication	111
Summary	113
III For Experts	115
10 IPsec VPN	117
Security	118
Lab setup	119
Connection setup	120
Address translation	124
Dead Peer Detection	126
IPv6	127
VPN throughput	128
Troubleshooting	129
Technical background	131
Outlook	132
Summary	136
11 OpenVPN	137
Operation	137
Authentication	138
Differences to IPsec	139
Lab setup	141

Site-to-Site tunnel	141
Client-server tunnel	146
Troubleshooting	150
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	178
Summary	179
14 Web Proxy	181
Lab setup	183
Explicit proxy	184
Proxy cluster	189
TLS Inspection	192
Transparent proxy	197
Technical background	198
Limitations	198
Outlook	199

Summary	200
15 Central Authentication	201
Protocols	201
Lab setup	203
Microsoft Server	204
Directory-as-a-Service	211
Troubleshooting	219
Technical background	222
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	242
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	257
Attack	258
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	270
Updates	271
Summary	272
20 Performance Tuning	273
Lab setup	273
Baseline	274
Virtual network adapter	275
Routing throughput	278
IPsec throughput	280
Increasing performance	283
Summary	291
V For Admins	293
21 Best Practice	295
Factory reset	295
Benchmark throughput	296
SSH login without password	298
Password reset	301

22 Configuration	305
Dropbox	305
Google Drive	309
Summary	313
23 Life Hacks	315
Access from Windows	316
Span port	316
Telegram	317
Firewall rules with category	320
Quick search	321
24 Application Programming Interface	323
How does the API work?	323
Read Access	327
Write Access	329
What does the API cover?	330
API browser	331
Security	332
Technical background	333
Outlook	334
Summary	334
Bibliography	335
Index	339
A Editing Files in FreeBSD	347
B Pattern Matching	351
C Bonus Material	357