

# Contents

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

---

<b>4</b>	<b>Initial Setup</b>	<b>51</b>
	Initial setup . . . . .	52
	Secondary setup . . . . .	54
	Routing . . . . .	57
	Final testing . . . . .	58
	Summary . . . . .	59
<b>5</b>	<b>IP Version 6</b>	<b>61</b>
	Crash course . . . . .	61
	Lab setup . . . . .	63
	Addresses and routes . . . . .	63
	Clients . . . . .	65
	Connections . . . . .	66
	Summary . . . . .	66
<b>II</b>	<b>For Intermediates</b>	<b>67</b>
<b>6</b>	<b>Firewall</b>	<b>69</b>
	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
<b>7</b>	<b>Transparent Firewall</b>	<b>85</b>
	Pros and cons . . . . .	85
	Lab setup . . . . .	86
	Configuration . . . . .	87
	Filter operation . . . . .	89
	Ruleset . . . . .	89

---

Uncover transparent firewall . . . . .	91
Technical background . . . . .	91
Summary . . . . .	92
<b>8 Network Address Translation</b>	<b>93</b>
Lab setup . . . . .	94
Scenarios . . . . .	95
IPv6 . . . . .	101
NAT Reflection . . . . .	103
Technical background . . . . .	104
Summary . . . . .	104
<b>9 Management Interface</b>	<b>105</b>
Two-factor authentication . . . . .	111
Summary . . . . .	113
<b>III For Experts</b>	<b>115</b>
<b>10 IPsec VPN</b>	<b>117</b>
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
<b>11 OpenVPN</b>	<b>137</b>
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
<b>12 High Availability</b>	<b>155</b>
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
<b>13 NetFlow</b>	<b>173</b>
The content of a flow . . . . .	173
Lab setup . . . . .	174
Collector . . . . .	176
Troubleshooting . . . . .	177
Insight . . . . .	177
Technical background . . . . .	178
IPv6 . . . . .	178
Summary . . . . .	179
<b>14 Web Proxy</b>	<b>181</b>
Lab setup . . . . .	183
Explicit proxy . . . . .	184
Proxy cluster . . . . .	189
TLS Inspection . . . . .	192
Transparent proxy . . . . .	197
Technical background . . . . .	198
Limitations . . . . .	198
Outlook . . . . .	199

---

Summary . . . . .	200
<b>15 Central Authentication</b>	<b>201</b>
Protocols . . . . .	201
Lab setup . . . . .	203
Microsoft Server . . . . .	204
Directory-as-a-Service . . . . .	211
Troubleshooting . . . . .	219
Technical background . . . . .	222
Summary . . . . .	223
 <b>IV For Hackers</b>	 <b>225</b>
<b>16 Multi-WAN</b>	<b>227</b>
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
 <b>17 DSL router</b>	 <b>241</b>
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

---

<b>18 Intrusion Detection</b>	<b>255</b>
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
<b>19 Command Line</b>	<b>267</b>
configd . . . . .	267
Configuration changes . . . . .	269
Undo changes . . . . .	270
Updates . . . . .	271
Summary . . . . .	272
<b>20 Performance Tuning</b>	<b>273</b>
Lab setup . . . . .	273
Baseline . . . . .	274
Virtual network adapter . . . . .	275
Routing throughput . . . . .	278
IPsec throughput . . . . .	280
Increasing performance . . . . .	283
Summary . . . . .	291
<b>V For Admins</b>	<b>293</b>
<b>21 Best Practice</b>	<b>295</b>
Factory reset . . . . .	295
Benchmark throughput . . . . .	296
SSH login without password . . . . .	298
Password reset . . . . .	301

<b>22 Configuration</b>	<b>305</b>
Dropbox . . . . .	305
Google Drive . . . . .	309
Summary . . . . .	313
<b>23 Life Hacks</b>	<b>315</b>
Access from Windows . . . . .	316
Span port . . . . .	316
Telegram . . . . .	317
Firewall rules with category . . . . .	320
Quick search . . . . .	321
<b>24 Application Programming Interface</b>	<b>323</b>
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
<b>Bibliography</b>	<b>335</b>
<b>Index</b>	<b>339</b>
<b>A Editing Files in FreeBSD</b>	<b>347</b>
<b>B Pattern Matching</b>	<b>351</b>
<b>C Bonus Material</b>	<b>357</b>