

# Contents

<b>Preface</b>	<b>xii</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 . . . . .	29
<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 . . . . .	56
	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 . . . . .	64
	Connections . . . . .	65
	Summary . . . . .	67
<b>II</b>	<b>For Intermediates</b>	<b>69</b>
<b>6</b>	<b>Firewall</b>	<b>71</b>
	OPNsense as a firewall . . . . .	72
	Lab setup . . . . .	73
	Firewall rules . . . . .	73
	Logging . . . . .	76
	Throughput . . . . .	76
	Best practice . . . . .	77
	GeoIP . . . . .	82
	Technical background . . . . .	82
	Order of processing . . . . .	84
	Troubleshooting . . . . .	84
	Summary . . . . .	85
<b>7</b>	<b>Transparent Firewall</b>	<b>87</b>
	Pros and cons . . . . .	87
	Lab setup . . . . .	88
	Configuration . . . . .	89
	Filter operation . . . . .	91
	Ruleset . . . . .	91

---

Uncover transparent firewall . . . . .	93
Technical background . . . . .	93
Summary . . . . .	94
<b>8 Network Address Translation</b>	<b>95</b>
Lab setup . . . . .	96
Scenarios . . . . .	97
IPv6 . . . . .	103
NAT Reflection . . . . .	105
Technical background . . . . .	106
Summary . . . . .	106
<b>9 Management Interface</b>	<b>107</b>
Summary . . . . .	112
<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 . . . . .	140
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 . . . . .	165
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 . . . . .	179
Summary . . . . .	179
<b>14 Web Proxy</b>	<b>181</b>
Lab setup . . . . .	183
Explicit proxy . . . . .	183
Proxy cluster . . . . .	189
SSL inspection . . . . .	192
Transparent proxy . . . . .	196
Technical background . . . . .	198
Limitations . . . . .	199
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 . . . . .	248
IPv6 with prefix delegation . . . . .	249
Firewall . . . . .	252
Technical background . . . . .	253
Summary . . . . .	254

---

<b>18 Intrusion Detection</b>	<b>257</b>
IPS and IDS . . . . .	257
Network integration . . . . .	258
Lab setup . . . . .	259
Attack . . . . .	260
Activate IDS . . . . .	260
Activate IPS . . . . .	262
Transparent IDS . . . . .	263
Technical background . . . . .	266
Summary . . . . .	268
<b>19 Command Line</b>	<b>269</b>
configd . . . . .	269
Configuration changes . . . . .	271
Undo changes . . . . .	272
Updates . . . . .	273
Summary . . . . .	274
<b>20 Performance Tuning</b>	<b>275</b>
Lab setup . . . . .	275
Baseline . . . . .	276
Virtual network adapter . . . . .	277
Routing throughput . . . . .	280
IPsec throughput . . . . .	282
Increasing performance . . . . .	285
Summary . . . . .	293
<b>V For Admins</b>	<b>295</b>
<b>21 Best Practice</b>	<b>297</b>
Factory reset . . . . .	297
Benchmark throughput . . . . .	298
SSH login without password . . . . .	300
Password reset . . . . .	303

<b>22 Configuration</b>	<b>307</b>
Dropbox . . . . .	307
Google Drive . . . . .	311
Summary . . . . .	315
<b>23 Life Hacks</b>	<b>317</b>
Access from Windows . . . . .	318
Span port . . . . .	318
Telegram . . . . .	319
Firewall rules with category . . . . .	322
Quick search . . . . .	322
<b>24 Application Programming Interface</b>	<b>325</b>
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
<b>Bibliography</b>	<b>337</b>
<b>Index</b>	<b>341</b>
<b>A Editing Files in FreeBSD</b>	<b>349</b>
<b>B Pattern Matching</b>	<b>353</b>
<b>C Bonus Material</b>	<b>359</b>