pfSense: The Definitive Guide

The Definitive Guide to the pfSense Open Source Firewall and Router Distribution

Contents

1 Introduction **1**
1.1 What does pfSense stand for/mean? . . . 1
1.2 Why FreeBSD? . . . 1
1.3 Common Deployments . . . 2
1.4 Versions . . . 5
1.5 Platforms . . . 6
1.6 Networking Concepts . . . 7
1.7 Interface Naming Terminology . . . 13
1.8 Finding Information and Getting Help . . . 14

2 Hardware **15**
2.1 Hardware Compatibility . . . 15
2.2 Minimum Hardware Requirements . . . 16
2.3 Hardware Selection . . . 17
2.4 Hardware Sizing Guidance . . . 18

3 Installation Guide **23**
3.1 Downloading pfSense . . . 23
3.2 Full Installation . . . 24
3.3 Embedded Installation . . . 28
3.4 Alternate Installation Techniques . . . 33
3.5 Installation Troubleshooting . . . 35
3.6 Recovery Installation . . . 38
3.7 Upgrading an Existing Installation . . . 39

4 Configuration **43**
4.1 Connecting to the WebGUI . . . 43
4.2 Setup Wizard . . . 44
4.3 Interface Configuration . . . 52
4.4 General Configuration Options . . . 53
4.5 Advanced Configuration Options . . . 54
4.6 Console Menu Basics . . . 59
4.7 Time Synchronization . . . 62
4.8 Troubleshooting . . . 65
4.9 pfSense's XML Configuration File . . . 68
4.10 What to do if you get locked out of the WebGUI . . . 68
4.11 Final Configuration Thoughts . . . 72

5 Backup and Recovery 73
5.1 Backup Strategies . . . 73
5.2 Making Backups in the WebGUI . . . 74
5.3 Using the AutoConfigBackup Package . . . 74
5.4 Alternate Remote Backup Techniques . . . 77
5.5 Restoring from Backups . . . 78
5.6 Backup Files and Directories with the Backup Package . . . 80
5.7 Caveats and Gotchas . . . 81

6 Firewall 83
6.1 Firewalling Fundamentals . . . 83
6.2 Introduction to the Firewall Rules screen . . . 87
6.3 Aliases . . . 90
6.4 Firewall Rule Best Practices . . . 95
6.5 Rule Methodology . . . 98
6.6 Configuring firewall rules . . . 104
6.7 Methods of Using Additional Public IPs . . . 107
6.8 Virtual IPs . . . 108
6.9 Time Based Rules . . . 109
6.10 Viewing the Firewall Logs . . . 110
6.11 Troubleshooting Firewall Rules . . . 113

7 Network Address Translation 115
7.1 Default NAT Configuration . . . 115
7.2 Port Forwards . . . 116
7.3 1:1 NAT . . . 119
7.4 Ordering of NAT and Firewall Processing . . . 123
7.5 NAT Reflection . . . 127
7.6 Outbound NAT . . . 130
7.7 Choosing a NAT Configuration . . . 131
7.8 NAT and Protocol Compatibility . . . 132
7.9 Troubleshooting . . . 136

8 Routing 139
8.1 Static Routes . . . 139
8.2 Routing Public IPs . . . 141
8.3 Routing Protocols . . . 144
8.4 Route Troubleshooting . . . 145

9 Bridging 151
9.1 Bridging and firewalling . . . 151
9.2 Bridging two internal networks . . . 152
9.3 Bridging OPT to WAN . . . 153
9.4 Bridging interoperability . . . 153

10 Virtual LANs (VLANs) 159
10.1 Requirements . . . 159
10.2 Terminology . . . 160

10.3 VLANs and Security . . . 161
10.4 pfSense Configuration . . . 162
10.5 Switch Configuration . . . 167

11 Multiple WAN Connections 179
11.1 Choosing your Internet Connectivity . . . 179
11.2 Multi-WAN Terminology and Concepts . . . 180
11.3 Multi-WAN Caveats and Considerations . . . 182
11.4 Interface and DNS Configuration . . . 184
11.5 Multi-WAN Special Cases . . . 186
11.6 Multi-WAN and NAT . . . 186
11.7 Load Balancing . . . 187
11.8 Failover . . . 189
11.9 Verifying Functionality . . . 190
11.10 Policy Routing, Load Balancing and Failover Strategies . . . 192
11.11 Multi-WAN on a Stick . . . 194
11.12 Troubleshooting . . . 195

12 Virtual Private Networks 197
12.1 Common deployments . . . 197
12.2 Choosing a VPN solution for your environment . . . 199

13 IPsec 203
13.1 IPsec Terminology . . . 203
13.2 Choosing configuration options . . . 204
13.3 IPsec and firewall rules . . . 206
13.4 Site to Site . . . 206
13.5 Mobile IPsec . . . 214
13.6 IPsec Troubleshooting . . . 234
13.7 Configuring Third Party IPsec Devices . . . 242

14 PPTP VPN 247
14.1 PPTP Security Warning . . . 247
14.2 PPTP and Firewall Rules . . . 247
14.3 PPTP and Multi-WAN . . . 247
14.4 PPTP Limitations . . . 248
14.5 PPTP Server Configuration . . . 248
14.6 PPTP Client Configuration . . . 252
14.7 Increasing the Simultaneous User Limit . . . 271
14.8 PPTP Redirection . . . 272
14.9 PPTP Troubleshooting . . . 272
14.10 PPTP Routing Tricks . . . 273
14.11 PPTP Logs . . . 274

15 OpenVPN 275
15.1 Basic Introduction to X.509 Public Key Infrastructure . . . 275
15.2 Generating OpenVPN Keys and Certificates . . . 276
15.3 OpenVPN Configuration Options . . . 283

15.4 Remote Access Configuration 287
15.5 Site to Site Example Configuration 292
15.6 Filtering and NAT with OpenVPN Connections 294
15.7 OpenVPN and Multi-WAN 295
15.8 OpenVPN and CARP 297
15.9 Bridged OpenVPN Connections 297
15.10 Custom configuration options 297
15.11 Troubleshooting OpenVPN 299

16 Traffic Shaper **301**
16.1 Traffic Shaping Basics 301
16.2 What the Traffic Shaper can do for you 302
16.3 Hardware Limitations 303
16.4 Limitations of the Traffic Shaper implementation in 1.2.x 303
16.5 Configuring the Traffic Shaper With the Wizard 304
16.6 Monitoring the Queues 308
16.7 Advanced Customization 309
16.8 Troubleshooting Shaper Issues 314

17 Server Load Balancing **317**
17.1 Explanation of Configuration Options 317
17.2 Web Server Load Balancing Example Configuration 319
17.3 Troubleshooting Server Load Balancing 326

18 Wireless **329**
18.1 Recommended Wireless Hardware 329
18.2 Wireless WAN 330
18.3 Bridging and wireless 333
18.4 Using an External Access Point 334
18.5 pfSense as an Access Point 336
18.6 Additional protection for your wireless network 339
18.7 Configuring a Secure Wireless Hotspot 341
18.8 Troubleshooting Wireless Connections 343

19 Captive Portal **345**
19.1 Limitations 345
19.2 Portal Configuration Without Authentication 346
19.3 Portal Configuration Using Local Authentication 347
19.4 Portal Configuration Using RADIUS Authentication 347
19.5 Configuration Options 347
19.6 Troubleshooting Captive Portal 350

20 Firewall Redundancy / High Availability **351**
20.1 CARP Overview 351
20.2 pfsync Overview 352
20.3 pfSense XML-RPC Sync Overview 352
20.4 Example Redundant Configuration 352
20.5 Multi-WAN with CARP 362

20.6 Verifying Failover Functionality . . . 365
20.7 Providing Redundancy Without NAT . . . 366
20.8 Layer 2 Redundancy . . . 368
20.9 CARP with Bridging . . . 370
20.10 CARP Troubleshooting . . . 371

21 Virtualization 375
21.1 Security Risks with Virtualization . . . 375
21.2 Supported Hypervisors . . . 375
21.3 VMware and Networking . . . 376
21.4 Common Deployments . . . 376

22 Services 377
22.1 DHCP Server . . . 377
22.2 DHCP Relay . . . 382
22.3 DNS Forwarder . . . 382
22.4 Dynamic DNS . . . 384
22.5 SNMP . . . 386
22.6 UPnP . . . 388
22.7 OpenNTPD . . . 391
22.8 Wake on LAN . . . 391
22.9 PPPoE Server . . . 393

23 System Monitoring 395
23.1 System Logs . . . 395
23.2 System Status . . . 398
23.3 Interface Status . . . 398
23.4 Service Status . . . 400
23.5 RRD Graphs . . . 400
23.6 Firewall States . . . 403
23.7 Traffic Graphs . . . 403

24 Packages 405
24.1 Introduction to Packages . . . 405
24.2 Installing Packages . . . 406
24.3 Reinstalling and Updating Packages . . . 407
24.4 Uninstalling Packages . . . 407
24.5 Developing Packages . . . 408

25 Third Party Software and pfSense 409
25.1 RADIUS Authentication with Windows Server . . . 409
25.2 Free Content Filtering with OpenDNS . . . 414
25.3 Syslog Server on Windows with Kiwi Syslog . . . 423
25.4 Using Software from FreeBSD's Ports System (Packages) . . . 423

26 Packet Capturing and Sniffing 427
26.1 Selecting the Proper Interface . . . 427
26.2 Packet Captures from the WebGUI . . . 428

26.3 Using tcpdump from the command line 429
26.4 Using Wireshark with pfSense 438
26.5 Plain Text Protocol Debugging with tcpflow 441
26.6 Additional References 441

A Menu Guide 443

List of Figures

1.1 Subnet Mask Converter . . . 11
1.2 Network/Node Calculator . . . 11
1.3 Network/Node Calculator . . . 12

4.1 Setup Wizard Starting Screen . . . 44
4.2 General Information Screen . . . 45
4.3 NTP and Time Zone Setup Screen . . . 45
4.4 WAN Configuration . . . 46
4.5 General WAN Configuration . . . 47
4.6 Static IP Settings . . . 47
4.7 DHCP Hostname Setting . . . 47
4.8 PPPoE Configuration . . . 48
4.9 PPTP WAN Configuration . . . 49
4.10 Built-in Ingress Filtering Options . . . 49
4.11 LAN Configuration . . . 50
4.12 Change Administrative Password . . . 51
4.13 Reload pfSense WebGUI . . . 51
4.14 Setting up a port 80 SSH Tunnel in PuTTY . . . 71

5.1 WebGUI Backup . . . 74
5.2 WebGUI Restore . . . 78
5.3 Configuration History . . . 79

6.1 Increased state table size to 50,000 . . . 84
6.2 Default WAN rules . . . 88
6.3 Default LAN rules . . . 88
6.4 Add LAN rule options . . . 89
6.5 Example hosts alias . . . 91
6.6 Example network alias . . . 92
6.7 Example ports alias . . . 93
6.8 Autocompletion of hosts alias . . . 94
6.9 Autocompletion of ports alias . . . 94
6.10 Example Rule Using Aliases . . . 94
6.11 Hovering shows contents . . . 95
6.12 Hovering shows contents . . . 95
6.13 Firewall Rule to Prevent Logging Broadcasts . . . 97
6.14 Alias for management ports . . . 99
6.15 Alias for management hosts . . . 100

6.16 Alias list 100
6.17 Example restricted management LAN rules 101
6.18 Restricted management LAN rules — alternate example 101
6.19 Anti-lockout rule disabled 102
6.20 Testing name resolution for bogon updates 103
6.21 Example Log Entries viewed from the WebGUI 110

7.1 Add Port Forward 117
7.2 Port Forward Example 118
7.3 Port Forward List 119
7.4 Port Forward Firewall Rule 119
7.5 1:1 NAT Edit screen 120
7.6 1:1 NAT Example - Single inside and outside IP 121
7.7 1:1 NAT Entry 122
7.8 1:1 NAT entry for /30 CIDR range 123
7.9 Ordering of NAT and Firewall Processing 124
7.10 LAN to WAN Processing 125
7.11 WAN to LAN Processing 126
7.12 Firewall Rule for Port Forward to LAN Host 127
7.13 Enable NAT Reflection 128
7.14 Add DNS Forwarder Override 128
7.15 Add DNS Forwarder Override for example.com 129
7.16 DNS Forwarder Override for www.example.com 129

8.1 Static Route 139
8.2 Static route configuration 140
8.3 Asymmetric routing 140
8.4 WAN IP and gateway configuration 142
8.5 Routing OPT1 configuration 143
8.6 Outbound NAT configuration 143
8.7 OPT1 firewall rules 144
8.8 WAN firewall rules 144
8.9 Route Display 145

9.1 Firewall Rule to Allow DHCP 152

10.1 Interfaces: Assign 165
10.2 VLAN List 165
10.3 Edit VLAN 166
10.4 VLAN List 166
10.5 Interface list with VLANs 167
10.6 VLAN Group Setting 171
10.7 Enable 802.1Q VLANs 171
10.8 Confirm change to 802.1Q VLAN 171
10.9 Default 802.1Q configuration 172
10.10 Add new VLAN 172
10.11 Add VLAN 10 173
10.12 Add VLAN 20 173

10.13 Toggle VLAN membership . . . 174
10.14 Configure VLAN 10 membership . . . 174
10.15 Configure VLAN 20 membership . . . 175
10.16 PVID Setting . . . 175
10.17 Default PVID Configuration . . . 176
10.18 VLAN 10 and 20 PVID Configuration . . . 176
10.19 Remove VLAN 1 membership . . . 176
10.20 Management VLAN . . . 177

11.1 Example static route configuration for Multi-WAN DNS services . . . 185
11.2 Unequal cost load balancing configuration . . . 194
11.3 Multi-WAN on a stick . . . 195

13.1 Enable IPsec . . . 207
13.2 Site A VPN Tunnel Settings . . . 208
13.3 Site A Phase 1 Settings . . . 209
13.4 Site A Phase 2 Settings . . . 210
13.5 Site A Keep Alive . . . 210
13.6 Apply IPsec Settings . . . 210
13.7 Site B VPN Tunnel Settings . . . 211
13.8 Site B Keep Alive . . . 212
13.9 Site to Site IPsec . . . 213
13.10 Site A - Static route to remote subnet . . . 214
13.11 Site B - Static route to remote subnet . . . 214
13.12 Enable Mobile IPsec Clients . . . 215
13.13 Mobile Clients Phase 1 . . . 216
13.14 Mobile Clients Phase 2 . . . 217
13.15 Apply Mobile Tunnel Settings . . . 217
13.16 IPsec Pre-shared Key "User" List . . . 218
13.17 Adding an Identifier/Pre-Shared Key Pair . . . 218
13.18 Applying Changes; PSK List . . . 218
13.19 Shrew Soft VPN Access Manager - No Connections Yet . . . 220
13.20 Client Setup: General Tab . . . 221
13.21 Client Setup: Client Tab . . . 222
13.22 Client Setup: Name Resolution Tab . . . 223
13.23 Client Setup: Authentication, Local Identity . . . 224
13.24 Client Setup: Authentication, Remote Identity . . . 225
13.25 Client Setup: Authentication, Credentials . . . 226
13.26 Client Setup: Phase 1 . . . 227
13.27 Client Setup: Phase 2 . . . 228
13.28 Client Setup: Policy . . . 229
13.29 Client Setup: Policy, Add Topology . . . 230
13.30 Client Setup: New Connection Name . . . 231
13.31 Ready To Use Connection . . . 232
13.32 Connected Tunnel . . . 233

14.1 PPTP IP Addressing . . . 248
14.2 PPTP VPN Firewall Rule . . . 249

14.3 PPTP WAN2 Firewall Rule 250
14.4 PPTP Users Tab 250
14.5 Adding a PPTP User 251
14.6 Applying PPTP Changes 251
14.7 List of PPTP Users 252
14.8 Network Connections 252
14.9 Network Tasks 253
14.10 Workplace Connection 253
14.11 Connect to VPN 254
14.12 Connection Name 255
14.13 Connection Host 256
14.14 Finishing the Connection 257
14.15 Connect Dialog 258
14.16 Connection Properties 259
14.17 Security Tab 260
14.18 Networking Tab 261
14.19 Remote Gateway Setting 262
14.20 Vista Network Connections 263
14.21 Setup A Connection 263
14.22 Connect to a Workplace 263
14.23 Connect using VPN 263
14.24 Connection Setup 264
14.25 Authentication Settings 264
14.26 Connection is Ready 265
14.27 Get Connection Properties 265
14.28 VPN Security Settings 266
14.29 VPN Networking Settings 267
14.30 VPN Gateway 268
14.31 Add network connection 269
14.32 Add PPTP VPN connection 269
14.33 Configure PPTP VPN connection 270
14.34 Advanced options 271
14.35 Connect to PPTP VPN 271
14.36 PPTP Logs 274

15.1 easy-rsa Backup 279
15.2 OpenVPN example remote access network 288
15.3 OpenVPN server WAN rule 289
15.4 OpenVPN example site to site network 292
15.5 OpenVPN example site to site WAN firewall rule 293
15.6 Assign tun0 interface 294
15.7 Example static route for OpenVPN Client on OPT WAN 297

16.1 Starting the Shaper Wizard 304
16.2 Shaper Configuration 305
16.3 Voice over IP 305
16.4 Penalty Box 306
16.5 Peer-to-Peer Networking 307

16.6 Network Games . . . 307
16.7 Raise or Lower Other Applications . . . 308
16.8 Basic WAN Queues . . . 309
16.9 Traffic Shaper Queues List . . . 310
16.10 Traffic Shaper Rules List . . . 313

17.1 Server load balancing example network . . . 320
17.2 Pool configuration . . . 321
17.3 Virtual Server configuration . . . 322
17.4 Alias for web servers . . . 323
17.5 Firewall rule for web servers . . . 324
17.6 Firewall rule for web servers . . . 324
17.7 Virtual Server status . . . 325
17.8 Virtual Server status . . . 325

18.1 Interface assignment - wireless WAN . . . 331
18.2 Wireless WAN Associated . . . 332
18.3 No carrier on wireless WAN . . . 333
18.4 Wireless Status . . . 333
18.5 Rules to allow only IPsec from wireless . . . 340
18.6 Rules to allow only OpenVPN from wireless . . . 341
18.7 Rules to allow only PPTP from wireless . . . 341

19.1 Captive Portal on multiple subnets . . . 346

20.1 Diagram of this network . . . 355
20.2 WAN CARP IP . . . 356
20.3 LAN CARP IP . . . 357
20.4 Virtual IP list . . . 357
20.5 Outbound NAT Entry . . . 358
20.6 Advanced Outbound NAT Configuration . . . 359
20.7 pfsync Interface Configuration . . . 360
20.8 Firewall rule on pfsync interface . . . 361
20.9 Diagram of Multi-WAN CARP with DMZ . . . 364
20.10 DHCP Failover Pool Status . . . 365
20.11 Diagram of CARP with Routed IPs . . . 368
20.12 Diagram of CARP with Redundant Switches . . . 369

22.1 DHCP Daemon Service Status . . . 381
22.2 DNS Override Example . . . 383
22.3 UPnP status screen showing client PCs with forwarded ports . . . 390
22.4 pfSense system as seen by Windows 7 when browsing the Network . . . 391

23.1 Example System Log Entries . . . 396
23.2 System Status . . . 398
23.3 Interface Status . . . 399
23.4 Services Status . . . 400
23.5 WAN Traffic Graph . . . 401

23.6 Example States 403
23.7 Example WAN Graph 404

24.1 Package information retrieval failed 406
24.2 Package Listing 406
24.3 Post-Install Package Screen 407
24.4 Installed Package List 407

25.1 Add new RADIUS client 410
25.2 Add new RADIUS client - name and client address 411
25.3 Add new RADIUS client - Shared secret 412
25.4 Listing of the RADIUS Client 412
25.5 IAS Ports 413
25.6 Configuring OpenDNS on pfSense 414
25.7 Windows Server DNS Properties 415
25.8 Windows Server DNS Forwarders 416
25.9 Add a network 417
25.10 Adding a dynamic IP connection 418
25.11 Adding a static IP connection 419
25.12 Network successfully added 420
25.13 Content filtering level 421
25.14 Manage individual domains 421
25.15 DNS servers alias 422
25.16 LAN rules to restrict DNS 423

26.1 Wireshark Capture View 439

List of Tables

1.1 RFC 1918 Private IP Address Space 8
1.2 CIDR Subnet Table 10
1.3 CIDR Route Summarization 10

2.1 Maximum Throughput by CPU 18
2.2 1 Mpps throughput at various frame sizes 19
2.3 Large State Table RAM Consumption 20
2.4 IPsec Throughput by Encryption Protocol - ALIX 20
2.5 IPsec Throughput with Crypto Card - ALIX 20

3.1 Kernel Choices 28

6.1 Egress traffic required 86

7.1 /30 CIDR mapping - matching final octet 122
7.2 /30 CIDR mapping - non-matching final octet 122

8.1 WAN IP Block 142
8.2 Inside IP Block 142
8.3 Route Table Flags and Meanings 147

10.1 Netgear GS108T VLAN Configuration 170

11.1 Dissecting the ping monitoring 182
11.2 Unequal cost load balancing 193

12.1 Features and Characteristics by VPN Type 202

13.1 IPsec Endpoint Settings 207

20.1 WAN IP Address Assignments 353
20.2 LAN IP Address Assignments 353
20.3 pfsync IP Address Assignments 354
20.4 WAN IP Addressing 362
20.5 WAN2 IP Addressing 362
20.6 LAN IP Address Assignments 363
20.7 DMZ IP Address Assignments 363
20.8 pfsync IP Address Assignments 363

26.1 Real Interface vs. Friendly Names 428
26.2 tcpdump commonly used command line flags 429
26.3 Example uses of tcpdump -s 430