pfSense: The Definitive Guide

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

Christopher M. Buechler and Jim Pingle

Contents

Foreword **xix**

Preface **xxi**

1 Introduction **1**
1.1 Project Inception . . . 1
1.2 What does pfSense stand for/mean? . . . 1
1.3 Why FreeBSD? . . . 2
1.4 Common Deployments . . . 3
1.5 Versions . . . 5
1.6 Platforms . . . 6
1.7 Networking Concepts . . . 7
1.8 Interface Naming Terminology . . . 13
1.9 Finding Information and Getting Help . . . 15

2 Hardware **17**
2.1 Hardware Compatibility . . . 17
2.2 Minimum Hardware Requirements . . . 18
2.3 Hardware Selection . . . 19
2.4 Hardware Sizing Guidance . . . 20

3 Installing and Upgrading **25**
3.1 Downloading pfSense . . . 25
3.2 Full Installation . . . 26
3.3 Embedded Installation . . . 31
3.4 Alternate Installation Techniques . . . 37
3.5 Installation Troubleshooting . . . 39
3.6 Recovery Installation . . . 44
3.7 Upgrading an Existing Installation . . . 45

4 Configuration **49**
4.1 Connecting to the WebGUI . . . 49
4.2 Setup Wizard . . . 50
4.3 Interface Configuration . . . 58
4.4 General Configuration Options . . . 59
4.5 Advanced Configuration Options . . . 60
4.6 Console Menu Basics . . . 65

4.7 Time Synchronization . . . 69
4.8 Troubleshooting . . . 72
4.9 pfSense's XML Configuration File . . . 75
4.10 What to do if you get locked out of the WebGUI . . . 75
4.11 Final Configuration Thoughts . . . 79

5 Backup and Recovery **81**
5.1 Backup Strategies . . . 81
5.2 Making Backups in the WebGUI . . . 82
5.3 Using the AutoConfigBackup Package . . . 82
5.4 Alternate Remote Backup Techniques . . . 85
5.5 Restoring from Backups . . . 86
5.6 Backup Files and Directories with the Backup Package . . . 89
5.7 Caveats and Gotchas . . . 90

6 Firewall **91**
6.1 Firewalling Fundamentals . . . 91
6.2 Introduction to the Firewall Rules screen . . . 96
6.3 Aliases . . . 98
6.4 Firewall Rule Best Practices . . . 102
6.5 Rule Methodology . . . 105
6.6 Configuring firewall rules . . . 111
6.7 Methods of Using Additional Public IPs . . . 115
6.8 Virtual IPs . . . 119
6.9 Time Based Rules . . . 120
6.10 Viewing the Firewall Logs . . . 123
6.11 Troubleshooting Firewall Rules . . . 126

7 Network Address Translation **129**
7.1 Default NAT Configuration . . . 129
7.2 Port Forwards . . . 130
7.3 1:1 NAT . . . 135
7.4 Ordering of NAT and Firewall Processing . . . 139
7.5 NAT Reflection . . . 143
7.6 Outbound NAT . . . 146
7.7 Choosing a NAT Configuration . . . 147
7.8 NAT and Protocol Compatibility . . . 147
7.9 Troubleshooting . . . 151

8 Routing **155**
8.1 Static Routes . . . 155
8.2 Routing Public IPs . . . 157
8.3 Routing Protocols . . . 160
8.4 Route Troubleshooting . . . 161

9 Bridging **167**
9.1 Bridging and Layer 2 Loops . . . 167
9.2 Bridging and firewalling . . . 167

9.3 Bridging two internal networks . . . 168
9.4 Bridging OPT to WAN . . . 169
9.5 Bridging interoperability . . . 169

10 Virtual LANs (VLANs) 175
10.1 Requirements . . . 175
10.2 Terminology . . . 176
10.3 VLANs and Security . . . 177
10.4 pfSense Configuration . . . 179
10.5 Switch Configuration . . . 183

11 Multiple WAN Connections 197
11.1 Choosing your Internet Connectivity . . . 197
11.2 Multi-WAN Terminology and Concepts . . . 198
11.3 Multi-WAN Caveats and Considerations . . . 200
11.4 Interface and DNS Configuration . . . 201
11.5 Multi-WAN Special Cases . . . 203
11.6 Multi-WAN and NAT . . . 204
11.7 Load Balancing . . . 205
11.8 Failover . . . 206
11.9 Verifying Functionality . . . 208
11.10 Policy Routing, Load Balancing and Failover Strategies . . . 210
11.11 Multi-WAN on a Stick . . . 212
11.12 Troubleshooting . . . 213

12 Virtual Private Networks 215
12.1 Common deployments . . . 215
12.2 Choosing a VPN solution for your environment . . . 217
12.3 VPNs and Firewall Rules . . . 220

13 IPsec 221
13.1 IPsec Terminology . . . 221
13.2 Choosing configuration options . . . 222
13.3 IPsec and firewall rules . . . 224
13.4 Site to Site . . . 224
13.5 Mobile IPsec . . . 232
13.6 Testing IPsec Connectivity . . . 251
13.7 IPsec and NAT-T . . . 251
13.8 IPsec Troubleshooting . . . 252
13.9 Configuring Third Party IPsec Devices . . . 260

14 PPTP VPN 265
14.1 PPTP Security Warning . . . 265
14.2 PPTP and Firewall Rules . . . 265
14.3 PPTP and Multi-WAN . . . 265
14.4 PPTP Limitations . . . 266
14.5 PPTP Server Configuration . . . 266
14.6 PPTP Client Configuration . . . 269

14.7 Increasing the Simultaneous User Limit . . . 289
14.8 PPTP Redirection . . . 290
14.9 PPTP Troubleshooting . . . 290
14.10 PPTP Routing Tricks . . . 291
14.11 PPTP Logs . . . 292

15 OpenVPN 293
15.1 Basic Introduction to X.509 Public Key Infrastructure . . . 293
15.2 Generating OpenVPN Keys and Certificates . . . 294
15.3 OpenVPN Configuration Options . . . 301
15.4 Remote Access Configuration . . . 305
15.5 Site to Site Example Configuration . . . 321
15.6 Filtering and NAT with OpenVPN Connections . . . 322
15.7 OpenVPN and Multi-WAN . . . 326
15.8 OpenVPN and CARP . . . 327
15.9 Bridged OpenVPN Connections . . . 328
15.10 Custom configuration options . . . 328
15.11 Troubleshooting OpenVPN . . . 329

16 Traffic Shaper 333
16.1 Traffic Shaping Basics . . . 333
16.2 What the Traffic Shaper can do for you . . . 334
16.3 Hardware Limitations . . . 335
16.4 Limitations of the Traffic Shaper implementation in 1.2.x . . . 335
16.5 Configuring the Traffic Shaper With the Wizard . . . 336
16.6 Monitoring the Queues . . . 340
16.7 Advanced Customization . . . 341
16.8 Troubleshooting Shaper Issues . . . 346

17 Server Load Balancing 349
17.1 Explanation of Configuration Options . . . 349
17.2 Web Server Load Balancing Example Configuration . . . 351
17.3 Troubleshooting Server Load Balancing . . . 357

18 Wireless 361
18.1 Recommended Wireless Hardware . . . 361
18.2 Wireless WAN . . . 362
18.3 Bridging and wireless . . . 365
18.4 Using an External Access Point . . . 366
18.5 pfSense as an Access Point . . . 368
18.6 Additional protection for your wireless network . . . 372
18.7 Configuring a Secure Wireless Hotspot . . . 374
18.8 Troubleshooting Wireless Connections . . . 375

19 Captive Portal 377
19.1 Limitations . . . 377
19.2 Portal Configuration Without Authentication . . . 377
19.3 Portal Configuration Using Local Authentication . . . 379

19.4 Portal Configuration Using RADIUS Authentication . . . 379
19.5 Configuration Options . . . 379
19.6 Troubleshooting Captive Portal . . . 382

20 Firewall Redundancy / High Availability 383
20.1 CARP Overview . . . 383
20.2 pfsync Overview . . . 384
20.3 pfSense XML-RPC Sync Overview . . . 384
20.4 Example Redundant Configuration . . . 384
20.5 Multi-WAN with CARP . . . 393
20.6 Verifying Failover Functionality . . . 397
20.7 Providing Redundancy Without NAT . . . 398
20.8 Layer 2 Redundancy . . . 401
20.9 CARP with Bridging . . . 403
20.10 CARP Troubleshooting . . . 403

21 Services 407
21.1 DHCP Server . . . 407
21.2 DHCP Relay . . . 412
21.3 DNS Forwarder . . . 412
21.4 Dynamic DNS . . . 414
21.5 SNMP . . . 416
21.6 UPnP . . . 418
21.7 OpenNTPD . . . 422
21.8 Wake on LAN . . . 422
21.9 PPPoE Server . . . 424

22 System Monitoring 425
22.1 System Logs . . . 425
22.2 System Status . . . 428
22.3 Interface Status . . . 430
22.4 Service Status . . . 430
22.5 RRD Graphs . . . 430
22.6 Firewall States . . . 433
22.7 Traffic Graphs . . . 434

23 Packages 435
23.1 Introduction to Packages . . . 435
23.2 Installing Packages . . . 436
23.3 Reinstalling and Updating Packages . . . 437
23.4 Uninstalling Packages . . . 438
23.5 Developing Packages . . . 438

24 Third Party Software and pfSense 439
24.1 RADIUS Authentication with Windows Server . . . 439
24.2 Free Content Filtering with OpenDNS . . . 444
24.3 Syslog Server on Windows with Kiwi Syslog . . . 453
24.4 Using Software from FreeBSD's Ports System (Packages) . . . 453

25 Packet Capturing **457**
25.1 Capture frame of reference 457
25.2 Selecting the Proper Interface 457
25.3 Limiting capture volume 459
25.4 Packet Captures from the WebGUI 459
25.5 Using tcpdump from the command line 460
25.6 Using Wireshark with pfSense 470
25.7 Plain Text Protocol Debugging with tcpflow 473
25.8 Additional References 474

A Menu Guide **475**

List of Figures

1.1 Subnet Mask Converter . . . 11
1.2 Network/Node Calculator . . . 12
1.3 Network/Node Calculator Example . . . 13

3.1 Interface Assignment Screen . . . 29

4.1 Setup Wizard Starting Screen . . . 50
4.2 General Information Screen . . . 51
4.3 NTP and Time Zone Setup Screen . . . 51
4.4 WAN Configuration . . . 52
4.5 General WAN Configuration . . . 53
4.6 Static IP Settings . . . 53
4.7 DHCP Hostname Setting . . . 53
4.8 PPPoE Configuration . . . 54
4.9 PPTP WAN Configuration . . . 55
4.10 Built-in Ingress Filtering Options . . . 55
4.11 LAN Configuration . . . 56
4.12 Change Administrative Password . . . 57
4.13 Reload pfSense WebGUI . . . 57
4.14 Setting up a port 80 SSH Tunnel in PuTTY . . . 78

5.1 WebGUI Backup . . . 82
5.2 WebGUI Restore . . . 87
5.3 Configuration History . . . 87

6.1 Increased state table size to 50,000 . . . 92
6.2 Default WAN rules . . . 96
6.3 Default LAN rules . . . 96
6.4 Add LAN rule options . . . 97
6.5 Example hosts alias . . . 99
6.6 Example network alias . . . 100
6.7 Example ports alias . . . 100
6.8 Autocompletion of hosts alias . . . 101
6.9 Autocompletion of ports alias . . . 101
6.10 Example Rule Using Aliases . . . 101
6.11 Hovering shows Hosts contents . . . 102
6.12 Hovering shows Ports contents . . . 102
6.13 Firewall Rule to Prevent Logging Broadcasts . . . 104

6.14 Alias for management ports . . . 106
6.15 Alias for management hosts . . . 107
6.16 Alias list . . . 108
6.17 Example restricted management LAN rules . . . 108
6.18 Restricted management LAN rules — alternate example . . . 109
6.19 Anti-lockout rule disabled . . . 109
6.20 Testing name resolution for bogon updates . . . 110
6.21 Multiple public IPs in use — single IP block . . . 117
6.22 Multiple public IPs in use — two IP blocks . . . 118
6.25 Schedule List after Adding . . . 121
6.23 Adding a Time Range . . . 122
6.24 Added Time Range . . . 122
6.26 Choosing a Schedule for a Firewall Rule . . . 123
6.27 Firewall Rule List with Schedule . . . 123
6.28 Example Log Entries viewed from the WebGUI . . . 124

7.1 Add Port Forward . . . 131
7.2 Port Forward Example . . . 132
7.3 Port Forward List . . . 132
7.4 Port Forward Firewall Rule . . . 133
7.5 Example redirect port forward . . . 134
7.6 1:1 NAT Edit screen . . . 135
7.7 1:1 NAT Entry . . . 136
7.8 1:1 NAT Example — Single inside and outside IP . . . 137
7.9 1:1 NAT entry for /30 CIDR range . . . 138
7.10 Ordering of NAT and Firewall Processing . . . 140
7.11 LAN to WAN Processing . . . 141
7.12 WAN to LAN Processing . . . 142
7.13 Firewall Rule for Port Forward to LAN Host . . . 143
7.14 Enable NAT Reflection . . . 144
7.15 Add DNS Forwarder Override . . . 144
7.16 Add DNS Forwarder Override for example.com . . . 145
7.17 DNS Forwarder Override for www.example.com . . . 145

8.1 Static Route . . . 155
8.2 Static route configuration . . . 156
8.3 Asymmetric routing . . . 156
8.4 WAN IP and gateway configuration . . . 158
8.5 Routing OPT1 configuration . . . 159
8.6 Outbound NAT configuration . . . 159
8.7 OPT1 firewall rules . . . 160
8.8 WAN firewall rules . . . 160
8.9 Route Display . . . 161

9.1 Firewall Rule to Allow DHCP . . . 168

10.1 Interfaces: Assign . . . 181
10.2 VLAN List . . . 182

10.3 Edit VLAN . . . 182
10.4 VLAN List . . . 182
10.5 Interface list with VLANs . . . 183
10.6 VLAN Group Setting . . . 188
10.7 Enable 802.1Q VLANs . . . 188
10.8 Confirm change to 802.1Q VLAN . . . 189
10.9 Default 802.1Q configuration . . . 189
10.10 Add new VLAN . . . 190
10.11 Add VLAN 10 . . . 190
10.12 Add VLAN 20 . . . 191
10.13 Toggle VLAN membership . . . 192
10.14 Configure VLAN 10 membership . . . 192
10.15 Configure VLAN 20 membership . . . 193
10.16 PVID Setting . . . 193
10.17 Default PVID Configuration . . . 193
10.18 VLAN 10 and 20 PVID Configuration . . . 194
10.19 Remove VLAN 1 membership . . . 194

11.1 Example static route configuration for Multi-WAN DNS services . . . 203
11.2 Unequal cost load balancing configuration . . . 212
11.3 Multi-WAN on a stick . . . 213

13.1 Enable IPsec . . . 225
13.2 Site A VPN Tunnel Settings . . . 226
13.3 Site A Phase 1 Settings . . . 227
13.4 Site A Phase 2 Settings . . . 227
13.5 Site A Keep Alive . . . 228
13.6 Apply IPsec Settings . . . 228
13.7 Site B VPN Tunnel Settings . . . 229
13.8 Site B Keep Alive . . . 229
13.9 Site to Site IPsec Where pfSense is not the Gateway . . . 230
13.10 Site to Site IPsec . . . 231
13.11 Site A — Static route to remote subnet . . . 232
13.12 Site B — Static route to remote subnet . . . 232
13.13 Enable Mobile IPsec Clients . . . 233
13.14 Mobile Clients Phase 1 . . . 234
13.15 Mobile Clients Phase 2 . . . 235
13.16 Apply Mobile Tunnel Settings . . . 235
13.17 IPsec Pre-shared Key "User" List . . . 236
13.18 Adding an Identifier/Pre-Shared Key Pair . . . 236
13.19 Applying Changes; PSK List . . . 236
13.20 Shrew Soft VPN Access Manager — No Connections Yet . . . 238
13.21 Client Setup: General Tab . . . 239
13.22 Client Setup: Client Tab . . . 240
13.23 Client Setup: Name Resolution Tab . . . 241
13.24 Client Setup: Authentication, Local Identity . . . 242
13.25 Client Setup: Authentication, Remote Identity . . . 243
13.26 Client Setup: Authentication, Credentials . . . 244

13.27 Client Setup: Phase 1 . . . 245
13.28 Client Setup: Phase 2 . . . 246
13.29 Client Setup: Policy . . . 247
13.30 Client Setup: Policy, Add Topology . . . 248
13.31 Client Setup: New Connection Name . . . 249
13.32 Ready To Use Connection . . . 249
13.33 Connected Tunnel . . . 250

14.1 PPTP IP Addressing . . . 266
14.2 PPTP VPN Firewall Rule . . . 267
14.3 PPTP Users Tab . . . 268
14.4 Adding a PPTP User . . . 268
14.5 Applying PPTP Changes . . . 269
14.6 List of PPTP Users . . . 269
14.7 Network Connections . . . 270
14.8 Network Tasks . . . 270
14.9 Workplace Connection . . . 271
14.10 Connect to VPN . . . 272
14.11 Connection Name . . . 273
14.12 Connection Host . . . 274
14.13 Finishing the Connection . . . 275
14.14 Connect Dialog . . . 276
14.15 Connection Properties . . . 277
14.16 Security Tab . . . 278
14.17 Networking Tab . . . 279
14.18 Remote Gateway Setting . . . 280
14.19 Vista Network Connections . . . 281
14.20 Setup A Connection . . . 281
14.21 Connect to a Workplace . . . 281
14.22 Connect using VPN . . . 282
14.23 Connection Setup . . . 282
14.24 Authentication Settings . . . 283
14.25 Connection is Ready . . . 283
14.26 Get Connection Properties . . . 284
14.27 VPN Security Settings . . . 284
14.28 VPN Networking Settings . . . 285
14.29 VPN Gateway . . . 286
14.30 Add network connection . . . 287
14.31 Add PPTP VPN connection . . . 287
14.32 Configure PPTP VPN connection . . . 288
14.33 Advanced options . . . 289
14.34 Connect to PPTP VPN . . . 289
14.35 PPTP Logs . . . 292

15.1 easy-rsa Backup . . . 297
15.2 OpenVPN example remote access network . . . 306
15.3 OpenVPN server WAN rule . . . 307
15.4 Viscosity Preferences . . . 310

15.5 Viscosity Add Connection . . . 311
15.6 Viscosity Configuration: General . . . 312
15.7 Viscosity Configuration: Certificates . . . 313
15.8 Viscosity Configuration: Options . . . 314
15.9 Viscosity Configuration: Networking . . . 315
15.10 Viscosity connect . . . 316
15.11 Viscosity menu . . . 317
15.12 Viscosity details . . . 318
15.13 Viscosity details: Traffic Statistics . . . 319
15.14 Viscosity details: Logs . . . 320
15.15 OpenVPN example site to site network . . . 321
15.16 OpenVPN example site to site WAN firewall rule . . . 322
15.17 Assign tun0 interface . . . 323
15.18 Site to site with conflicting subnets . . . 324
15.19 Site A 1:1 NAT configuration . . . 325
15.20 Site B 1:1 NAT configuration . . . 325
15.21 Example static route for OpenVPN Client on OPT WAN . . . 327

16.1 Starting the Shaper Wizard . . . 336
16.2 Shaper Configuration . . . 337
16.3 Voice over IP . . . 337
16.4 Penalty Box . . . 338
16.5 Peer-to-Peer Networking . . . 339
16.6 Network Games . . . 339
16.7 Raise or Lower Other Applications . . . 340
16.8 Basic WAN Queues . . . 341
16.9 Traffic Shaper Queues List . . . 342
16.10 Traffic Shaper Rules List . . . 345

17.1 Server load balancing example network . . . 352
17.2 Pool configuration . . . 353
17.3 Virtual Server configuration . . . 354
17.4 Alias for web servers . . . 355
17.5 Adding firewall rule for web servers . . . 356
17.6 Firewall rule for web servers . . . 356
17.7 Virtual Server status . . . 357

18.1 Interface assignment — wireless WAN . . . 363
18.2 Wireless WAN Associated . . . 364
18.3 No carrier on wireless WAN . . . 365
18.4 Wireless Status . . . 365
18.5 Rules to allow only IPsec from wireless . . . 373
18.6 Rules to allow only OpenVPN from wireless . . . 373
18.7 Rules to allow only PPTP from wireless . . . 374

19.1 Captive Portal on multiple subnets . . . 378

20.1 Example CARP network diagram . . . 386

20.2 WAN CARP IP . . . 387
20.3 LAN CARP IP . . . 388
20.4 Virtual IP list . . . 389
20.5 Outbound NAT Entry . . . 390
20.6 Advanced Outbound NAT Configuration . . . 391
20.7 pfsync Interface Configuration . . . 391
20.8 Firewall rule on pfsync interface . . . 392
20.9 Diagram of Multi-WAN CARP with DMZ . . . 396
20.10 DHCP Failover Pool Status . . . 397
20.11 Diagram of CARP with Routed IPs . . . 400
20.12 Diagram of CARP with Redundant Switches . . . 402

21.1 DHCP Daemon Service Status . . . 411
21.2 DNS Override Example . . . 414
21.3 UPnP status screen showing client PCs with forwarded ports . . . 421
21.4 pfSense system as seen by Windows 7 when browsing the Network . . . 421

22.1 Example System Log Entries . . . 426
22.2 System Status . . . 428
22.3 Interface Status . . . 429
22.4 Services Status . . . 430
22.5 WAN Traffic Graph . . . 431
22.6 Example States . . . 433
22.7 Example WAN Graph . . . 434

23.1 Package information retrieval failed . . . 436
23.2 Package Listing . . . 437
23.3 Post-Install Package Screen . . . 437
23.4 Installed Package List . . . 438

24.1 Add new RADIUS client . . . 440
24.2 Add new RADIUS client — name and client address . . . 441
24.3 Add new RADIUS client — Shared secret . . . 442
24.4 Listing of the RADIUS Client . . . 443
24.5 IAS Ports . . . 444
24.6 Configuring OpenDNS on pfSense . . . 445
24.7 Windows Server DNS Properties . . . 445
24.8 Windows Server DNS Forwarders . . . 446
24.9 Add a network . . . 447
24.10 Adding a dynamic IP connection . . . 448
24.11 Adding a static IP connection . . . 449
24.12 Network successfully added . . . 450
24.13 Content filtering level . . . 451
24.14 Manage individual domains . . . 451
24.15 DNS servers alias . . . 452
24.16 LAN rules to restrict DNS . . . 453

25.1 Capture reference . . . 458

25.2 Wireshark Capture View 471
25.3 Wireshark RTP Analysis 472

List of Tables

1.1 RFC 1918 Private IP Address Space . . . 8
1.2 CIDR Subnet Table . . . 10
1.3 CIDR Route Summarization . . . 11

2.1 Maximum Throughput by CPU . . . 21
2.2 500,000 pps throughput at various frame sizes . . . 21
2.3 Large State Table RAM Consumption . . . 22
2.4 IPsec Throughput by Cipher — ALIX . . . 23
2.5 IPsec Throughput by CPU . . . 23

3.1 Kernel Choices . . . 31

6.1 Egress traffic required . . . 94

7.1 /30 CIDR mapping — matching final octet . . . 138
7.2 /30 CIDR mapping — non-matching final octet . . . 138

8.1 WAN IP Block . . . 158
8.2 Inside IP Block . . . 158
8.3 Route Table Flags and Meanings . . . 163

10.1 Netgear GS108T VLAN Configuration . . . 188

11.1 Dissecting the ping monitoring . . . 200
11.2 Unequal cost load balancing . . . 211

12.1 Features and Characteristics by VPN Type . . . 220

13.1 IPsec Endpoint Settings . . . 225

20.1 WAN IP Address Assignments . . . 385
20.2 LAN IP Address Assignments . . . 385
20.3 pfsync IP Address Assignments . . . 386
20.4 WAN IP Addressing . . . 394
20.5 WAN2 IP Addressing . . . 394
20.6 LAN IP Address Assignments . . . 394
20.7 DMZ IP Address Assignments . . . 395
20.8 pfsync IP Address Assignments . . . 395

25.1 Real Interface vs. Friendly Names 459
25.2 Commonly used tcpdump flags 461
25.3 Example uses of tcpdump -s 462