TODO: NEED TITLE
TODO: need a subtitle
By Jeremy C. Reed
April 2016

ISBN: 978-1-937516-04-8

Publisher: Reed Media Services

Contents

1 Introduction **3**

2 Installation **5**

2.1 Installation Prerequisites 5

2.2 Recovery Mode 8

Setup GEOM Mirror 8

2.3 Quick/Easy Install 9

2.4 Custom Install 10

2.5 Network Interface Assignments (Console) 11

2.6 First Boot After Installation 13

3 The Text Console **15**

3.1 0) Logout (SSH only) 16

3.2 1) Assign Interfaces 16

3.3 2) Set interface(s) IP address 16

3.4 3) Reset webConfigurator password 16

3.5 4) Reset to factory defaults 17

3.6 5) Reboot system 17

3.7 6) Halt system 17

3.8 7) Ping host . . . 18
3.9 8) Shell . . . 18
3.10 9) pfTop . . . 19
3.11 10) Filter Logs . . . 20
3.12 11) Restart webConfigurator . . . 20
3.13 12) pfSense Developer Shell . . . 20
3.14 13) Update from console . . . 23
3.15 14) Enable or Disable Secure Shell (sshd) . . . 23
3.16 15) Restore recent configuration . . . 24
3.17 16) Restart PHP-FPM . . . 25
3.18 98) Move configuration file to removable device . . . 25
3.19 99) Install pfSense to a hard drive, etc. . . . 25
3.20 100) Verify webConfigurator is running . . . 25
3.21 Adding network interfaces . . . 26

4 The pfSense webConfigurator 27

4.1 First Web Login . . . 28
4.2 System menu . . . 29
4.3 Interfaces menu . . . 30
4.4 Firewall menu . . . 30
4.5 Services menu . . . 31
4.6 VPN menu . . . 32
4.7 Status menu . . . 32
4.8 Diagnostics menu . . . 34
4.9 Dashboard . . . 35
4.10 General Setup . . . 37
System . . . 38

DNS Server Settings . . . 38
Localization . . . 38
webConfigurator (General Setup) . . . 39
4.11 Admin Access Options . . . 39
webConfigurator . . . 39
Secure Shell . . . 40
Serial Communications . . . 41
Console Options . . . 41
4.12 Crash Reporter . . . 41

5 TODO 43

5.1 User Manager . . . 43
5.2 Backup and restore of configurations . . . 43
Restore configuration . . . 44
Configuration history . . . 45
5.3 Upgrading pfSense . . . 45
5.4 Hardware suggestions (like wifi or network cards for high loads) for using pfSense and maybe special installation instructions for specific types of hardware. System planning. . . . 47

6 Networking 49

6.1 Network Interfaces ??? TODO . . . 49
6.2 IPv6 Basics . . . 51
6.3 Disable an interface . . . 51
6.4 TODO: General networking and routing configuration if not covered yet. . . . 51
6.5 Bridging . . . 51
6.6 Virtual LANs (VLANs) . . . 51

6.7 Multi-WAN 51

7 Firewall **53**

7.1 Firewall Rules 53

Creating firewall rules in pfSense. Overview default PF rules. Firewalling fundamentals. 53

Firewall Aliases 54

Configuring a two zone gateway firewall (LAN and the internet) using pfSense (with examples of blocking traffic, all traffic, and allowing some). Stateful firewalling. 54

Setting up port forwarding and network address translation (NAT) in pfSense. 54

7.2 Creating VLAN 55

7.3 Blocking Traffic 63

7.4 Advanced Firewall & NAT 69

Firewall Advanced 69

Bogon Networks 71

Network Address Translation 71

State Timeouts 72

7.5 Advanced firewall tuning 73

8 Network Services **75**

8.1 IGMP Proxy 75

8.2 NTP 75

8.3 PPPoE 75

8.4 SNMP 76

8.5 UPnP & NAT-PMP 76

8.6 Wake-on-LAN 76

8.7 BGP 76

9 DHCP Services 77

9.1 DHCP Relay 77

9.2 DHCP Server 77

General Options (DHCP Server) 77

Additional Pools (DHCP Server) 78

Servers (DHCP Options) 78

Other Options (DHCP Server) 78

Network Booting (DHCP Server) 78

DHCP Static Mappings for this Interface 79

TODO 79

9.3 DHCPv6 Relay 79

9.4 DHCPv6 Server & RA 79

10 DNS 81

10.1 DNS Lookup 81

10.2 Dynamic DNS 83

Add or edit a Dynamic DNS Client 83

RFC 2136 DNS Updates 86

10.3 DNS Resolver 86

DNS Resolver Advanced Settings 87

DNS Resolver Access Lists 89

Host Overrides (unbound) 90

Domain Overrides (unbound) 90

10.4 DNS Forwarder 90

10.5 Host Overrides (dnsmasq) 92

10.6 Domain Overrides (dnsmasq) 93

11 Wireless Access Point 95

11.1 Common Wireless Configuration 95

11.2 Regulatory Settings 95

11.3 Network-Specific Wireless Configuration 96

11.4 97

11.5 802.1x RADIUS Options 97

12 QoS with traffic shaping and bandwidth limiting 99

12.1 Traffic shaping 99

12.2 By Interface 99

12.3 By Queue 100

12.4 Traffic Shaper Wizards 100

Multiple Lan/Wan Traffic Shaper Wizard 100

Dedicated Links Traffic Shaper Wizard 100

12.5 Traffic Shaping 106

Now Creating Firewall Rule for the traffic shaping on Windows 7 . . . 112

12.6 Quality of Service (QOS) 115

12.7 Queues status 122

12.8 Limiters 122

13 Status 125

13.1 Traffic Graph 125

13.2 RRD graphics 127

14 Diagnostics 131

14.1 ARP Table . . . 131
14.2 Authentication . . . 131
14.3 Backup & Restore . . . 132
14.4 Command Prompt . . . 132
14.5 Edit File . . . 134
14.6 Factory Defaults . . . 135
14.7 GEOM Mirrors . . . 135
14.8 Halt System . . . 136
14.9 Limiter Info . . . 136
14.10 NanoBSD . . . 136
14.11 NDP Table . . . 137
14.12 Packet Capture . . . 137
14.13 pfInfo . . . 137
14.14 pfTop . . . 138
14.15 Ping . . . 139
14.16 Reboot . . . 140
14.17 Routes . . . 141
14.18 S.M.A.R.T. Status . . . 142
S.M.A.R.T. Information . . . 142
Perform self-tests . . . 143
View Logs (S.M.A.R.T.) . . . 144
Abort (S.M.A.R.T.) . . . 144
Config (S.M.A.R.T.) . . . 145
14.19 Sockets . . . 145
14.20 States . . . 147
Source Tracking . . . 149

Reset States 149
14.21 States Summary 149
14.22 System Activity 150
14.23 Tables 153
14.24 Test Port 154
14.25 Traceroute 155

15 TODO: Captive Portal 157
15.1 TODO2 157
15.2 Captive Portal Status 157
15.3 Captive Portal Logs 157

16 VPN 159
16.1 IPsec 159
16.2 L2TP 159
16.3 OpenVPN 159

17 Load balancing 161
17.1 Advanced settings 161
17.2 Failover and Load balancing. 161

18 Custom packages and addons 163
18.1 TODO2 163

19 TODO: 165
19.1 Intrusion detection using pfSense. 165

19.2 High Availability and redundant firewalls. failover? maybe all in the load balacning chapter? 165

List of Figures

2.1 Boot Menu 6

2.2 Choose Installer Menu 7

2.3 Installer Menu 9

2.4 Interface assignment option 12

3.1 Menu at Text Console 16

4.1 Panel (with System → User Manager highlighted) 29

4.2 Dashboard 36

4.3 System → General Setup (in Turkish) 37

5.1 System Update - Confirm 47

7.1 56

7.2 57

7.3 58

7.4 59

7.5 60

7.6 61

7.7 62

7.8 63

7.9 64
7.10 65
7.11 66
7.12 67
7.13 68
7.14 68

10.1 Diagnostics → DNS Lookup 82

12.1 106
12.2 107
12.3 108
12.4 109
12.5 110
12.6 110
12.7 111
12.8 112
12.9 113
12.10 114
12.11 114
12.12 115
12.13 116
12.14 117
12.15 118
12.16 119
12.17 120
12.18 121
12.19 122

13.1 126
13.2 126
13.3 127
13.4 128
13.5 129
13.6 129
13.7 130

14.1 Diagnostics → Authentication failure 132
14.2 Diagnostics → Command Prompt shell example 133
14.3 Diagnostics → Edit File example 134
14.4 138
14.5 139
14.6 Diagnostics → Ping results 140
14.7 Diagnostics → S.M.A.R.T. Status Self-test logs 144
14.8 Diagnostics → Sockets → Show all socket connections 146
14.9 Diagnostics → States Summary By Destination IP 150
14.10 Diagnostics → System Activity 152

List of Tables

10.1 Dynamic DNS Providers 84

14.1 Route Flags 141
14.2 Common TCP States 148

TODO: need a subtitle

1 Introduction

pfSense is a free operating system used for deploying a firewall and router for a network on standard Intel or AMD based computers. It is a do-it-yourself network utility appliance commonly used in small offices and homes, but is also used in many large organizations and corporate environments. It is used by novice computer operators to experienced network engineers, especially because of its rapid deployment and proven history. It provides many features also available in commercial firewalls and is viewed as a unified threat management (UTM) solution. It may be used to establish a VPN to encrypt all traffic, a wireless access point, a perimeter firewall for a DMZ (demilitarized zone network), and as an intrusion detection and prevention system. It offers time-based packet filtering, network monitoring, network address translation, IPv6 networking, Dynamic DNS, traffic shaping, captive portal, firewall redundancy for high availability, system backups and updates, and many other features. It provides a wide-range of services like caching DNS, DHCP, web proxying, and many more. It provides many additional component packages for furthering its functionality. It also offers many diagnostic interfaces to troubleshoot or understand network and system behavior, including graphs, log monitoring, and network probes and traces.

pfSense is managed via an intuitive web interface. While pfSense is not as simple and easy to understand as some other free firewall distributions, it is also considered the most feature-rich. It is known for its stability and solid performance and fast startup and operations.

pfSense is based on free, open source software and includes over 900 individual tools and programs for troubleshooting, diagnostics, system management, scripting, and network and system services. Its core operating system is FreeBSD, a popular Unix-type system with proven experience dating back to the 1970's but continually improved and extended for modern hardware and technologies. pfSense includes OpenSSH for remote encrypted console access, the NGINX HTTP server and PHP for the web-based management interface, Unbound for recursive and caching DNS service, ISC DHCP for managing IP address leases, ntpd for synchronizing clocks using the Network Time Protocol, OpenBSD's relay daemon and PF packet filtering, and much more. Using the Unix shell and direct access to the tools and servers is not required as pfSense provides a user interface for configurations, control, and analysis.

This book covers many of the commonly-used features in pfSense. It corresponds to the latest supported pfSense release version at the time of this book's printing: version 2.3. It also covers some details related to the older 2.2 versions. This book is a completely new rewrite done by the same publisher of the Definitive Guide to pfSense. pfSense has changed a lot in the eight years since the long-out-of-date book was written. This book also covers installation and basic configuration through advanced networking and firewalling — using the new interface and, in many cases,

new configurations and different software. For details about this book, please see the website at http://www.reedmedia.net/books/pfsense/.