InterWorx Firewall Guide

by InterWorx LLC

Contents

Chapter 1

Firewall

1.1 Introduction:

1.1.1 What is a firewall?

A firewall is a device that analyzes incoming and outgoing network traffic and decides whether it should be allowed through or not based on a set of rules as determined by the user.

1.1.2 APF

InterWorx uses APF, which is an acronym for Advanced Policy Firewall. APF is a policy based iptables-based firewall. APF provides an easy to use front end for iptables.

1.2 Use

1.2.1 Firewall Control

Figure 1.1: Service Control for FireWall

In figure 1.1 you can see the box allows the user to start, restart, and stop APF via gui. [1]

1.2.1.1 Start on boot-up

Toggles whether or not you wish that InterWorx starts APF when the system reboots.

[1] **The panel will automatically indicate whether or not APF is running.**

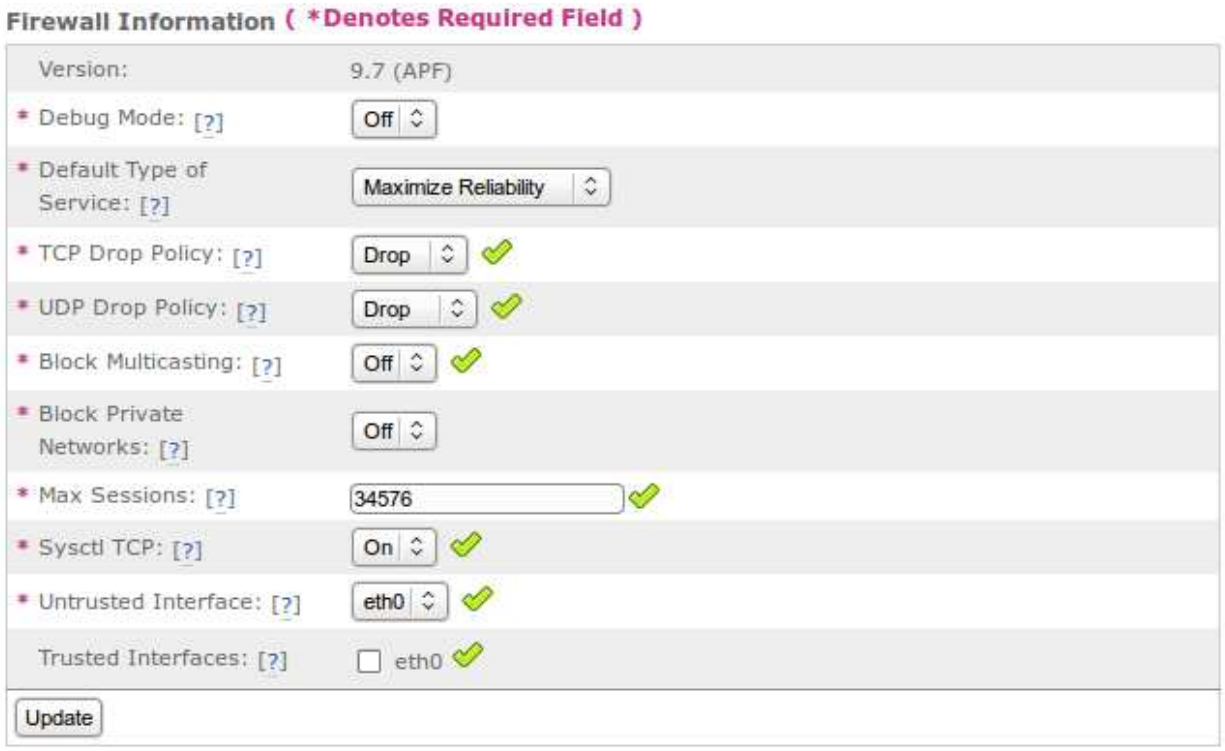

Figure 1.2: This section displays and edits configuration information for APF (note: the default configuration is best for most users)

1.3 Firewall Information

1.3.0.2 Debug mode

When debug mode is enabled, all firewall rules are flushed every 5 minutes to prevent being locked out of the server due to a firewall misconfiguration.

1.3.0.3 Default Type of Service

Defines the default type of service (Maximize Reliaibility, Maximize Throughput, Minimize Delay).

1.3.0.4 TCP Drop Policy

Defines how to handle TCP packet filtering. “Reset” sends a tcp-reset message, “Drop” silently drops the packet, “Reject” rejects the packet.

1.3.0.5 UDP Drop Policy

Defines how to handle UDP packet filtering. “Reset” sends an icmp-port-unreachable message, “Drop” will silently drop the packet, “Reject” will reject the packet, and “Prohibit” will send an icmp-host-prohibited message.

1.3.0.6 Block Multicasting

Defines if the firewall should block multicast traffic.

Figure 1.3: Gloal IP Access Control

1.3.0.7 Block Private Networks

Defines if the firewall should block all private ipv4 addresses (reserved address space, generally unroutable on the internet). If the server sites behind a NAT or other routing setup that would make use of private addressing, leave this option “Off”.

1.3.0.8 Max Sessions

Defines the maximum number of connection tracking entries that can be handled by the firewall simultaneously.

1.3.0.9 Sysctl TCP

Enables or Disables sysctl hook changes to harden the kernel from certain network-based attacks.

1.3.0.10 Untrusted Interface

All traffic on defined interface will be subject to all firewall rules. This should be your internet exposed interface.

1.3.0.11 Trusted Interfaces

All traffic on defined interface(s) will bypass all firewall rules.
Click ’Update’ to commit changes.

1.4 Global IP Access Control

1.4.0.12 Trusted IPs

Add one trusted IP per line to allow all traffic to and from that address.

1.4.0.13 Blocked IPs

Add one blocked IP to prevent all traffic to and from that address.

1.5 Port Access

This table is used to open and close specific ports on your firewall. The port rules defined here will apply to all incoming IPs that are not defined in either the Trusted or Blocked IP lists. (Note: The default configuration is best for most users.)

Note: Port 2443 must be open for the control panel to function correctly.

Port Access [?]

	Service	Port(s) [?]	TCP In	TCP Out	UDP In	UDP Out
Add			Open	Open	Open	Open
☐	ftp-data	20	Closed	Closed	Open	Open
☐	ftp	21	Open	Closed	Open	Open
☐	ssh	22	Open	Open	Closed	Closed
☐	lmtp	24	Open	Closed	Closed	Closed
☐	smtp	25	Open	Open	Closed	Closed
☐	domain	53	Closed	Closed	Open	Open
☐	http	80	Open	Open	Closed	Closed
☐	pop3	110	Open	Closed	Closed	Closed
☐	ntp	123	Closed	Closed	Open	Open
☐	imap	143	Open	Closed	Closed	Closed
☐	https	443	Open	Open	Closed	Closed
☐	imaps	993	Open	Closed	Closed	Closed
☐	pop3s	995	Open	Closed	Closed	Closed
☐	autodesk-nlm	2080	Open	Open	Closed	Closed
☐	powerclientcsf	2443	Open	Open	Closed	Closed
☐	mysql	3306	Open	Open	Closed	Closed
☐	N/A	50000-51000	Open	Open	Closed	Closed

[check all] [check none] [?] with selected:

Figure 1.4: Port Access Table