

# InterWorx Firewall Guide

by InterWorx LLC

# Contents

- 1 Firewall** **2**
- 1.1 Introduction: . . . . . 2
- 1.2 Use . . . . . 2
- 1.3 Firewall Information . . . . . 3
- 1.4 Global IP Access Control . . . . . 4
- 1.5 Port Access . . . . . 4

# 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. <sup>1</sup>

##### 1.2.1.1 Start on boot-up

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

---

<sup>1</sup>

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

**Firewall Information ( \*Denotes Required Field )**

Version:	9.7 (APF)
* Debug Mode: [?]	Off <input type="button" value="v"/>
* Default Type of Service: [?]	Maximize Reliability <input type="button" value="v"/>
* TCP Drop Policy: [?]	Drop <input type="button" value="v"/> <input checked="" type="checkbox"/>
* UDP Drop Policy: [?]	Drop <input type="button" value="v"/> <input checked="" type="checkbox"/>
* Block Multicasting: [?]	Off <input type="button" value="v"/> <input checked="" type="checkbox"/>
* Block Private Networks: [?]	Off <input type="button" value="v"/>
* Max Sessions: [?]	34576 <input checked="" type="checkbox"/>
* Sysctl TCP: [?]	On <input type="button" value="v"/> <input checked="" type="checkbox"/>
* Untrusted Interface: [?]	eth0 <input type="button" value="v"/> <input checked="" type="checkbox"/>
Trusted Interfaces: [?]	<input type="checkbox"/> eth0 <input checked="" type="checkbox"/>
<input type="button" value="Update"/>	

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 Reliability, 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.

**Global IP Access Control ( \*Denotes Required Field )**

Trusted IPs: (One per Line)	<input type="text"/>
Blocked IPs: (One per Line)	<input type="text"/>
<input type="button" value="Update"/>	

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
<input type="button" value="Add"/>		<input type="text"/>	Open ▾	Open ▾	Open ▾	Open ▾
<input type="checkbox"/>	ftp-data	20	Closed ▾	Closed ▾	Open ▾	Open ▾
<input type="checkbox"/>	ftp	21	Open ▾	Closed ▾	Open ▾	Open ▾
<input type="checkbox"/>	ssh	22	Open ▾	Open ▾	Closed ▾	Closed ▾
<input type="checkbox"/>	lmtpt	24	Open ▾	Closed ▾	Closed ▾	Closed ▾
<input type="checkbox"/>	smtp	25	Open ▾	Open ▾	Closed ▾	Closed ▾
<input type="checkbox"/>	domain	53	Closed ▾	Closed ▾	Open ▾	Open ▾
<input type="checkbox"/>	http	80	Open ▾	Open ▾	Closed ▾	Closed ▾
<input type="checkbox"/>	pop3	110	Open ▾	Closed ▾	Closed ▾	Closed ▾
<input type="checkbox"/>	ntp	123	Closed ▾	Closed ▾	Open ▾	Open ▾
<input type="checkbox"/>	imap	143	Open ▾	Closed ▾	Closed ▾	Closed ▾
<input type="checkbox"/>	https	443	Open ▾	Open ▾	Closed ▾	Closed ▾
<input type="checkbox"/>	imaps	993	Open ▾	Closed ▾	Closed ▾	Closed ▾
<input type="checkbox"/>	pop3s	995	Open ▾	Closed ▾	Closed ▾	Closed ▾
<input type="checkbox"/>	autodesk-nlm	2080	Open ▾	Open ▾	Closed ▾	Closed ▾
<input type="checkbox"/>	powerclientcsf	2443	Open ▾	Open ▾	Closed ▾	Closed ▾
<input type="checkbox"/>	mysql	3306	Open ▾	Open ▾	Closed ▾	Closed ▾
<input type="checkbox"/>	N/A	50000-51000	Open ▾	Open ▾	Closed ▾	Closed ▾

Figure 1.4: Port Access Table