
FreeBSD MPS v3

Firewall Supplement

First Edition
July 2007

Table of Contents

Introduction	1
Overview of the Documentation Library	1
Overview of this Document	1
Two Options for Building a Firewall	2
Overview of the IPFilter Software Package	2
Overview of the set_fwlevel Command	2
Services Affected By Your Firewall Security Settings	3
Protocols Affected by Your Firewall Security Settings	3
Specifying a Preset Firewall Security Level	4
Turning off Firewall Security	4
Specifying Low Firewall Security	4
Specifying Medium Firewall Security	4
Specifying High Firewall Security	5
Modifying Your Firewall Security Settings	6
Specifying a Preset Server Type	7
How Web Server Settings Affect Firewall Security Settings	7
How Mail Server Settings Affect Firewall Security Settings	7
Modifying Your account Type Settings	8
IPFilter Package Commands and Files	9

Introduction

Important: Although this document provides an overview of the IPFilter (also referred to as *ipf*) software package, it does not provide the details of how to build a firewall with that package. Knowledgeable administrators who wish to utilize the software package should refer to other resources and documentation, such as the *FreeBSD General Commands Manual* (or *Man Pages*). All who use the IPFilter software package should carefully consider all of the tasks they perform with that utility. Always make back up files, stored remotely, for IPFilter configurations and settings you have previously tested and used.

A firewall monitors and controls the traffic coming into and out of your FreeBSD Managed Private Server, version three (*FreeBSD MPS v3*) account. The traffic of the Internet consists of information which takes the form of data packets. A firewall evaluates each data packet and determines whether or not to pass the packet to your account. A firewall prevents your account from receiving an overwhelming quantity of unwanted traffic. Some of the unwanted traffic may be simply bothersome. Other traffic may actually be sent from malicious Internet users who intend to make your account inoperable. Either way, building a firewall is an important configuration task for you to consider.

This document provides you with the information you need to understand, get started, and utilize preset firewall security settings using a custom, simplified command (`set_fwlevel`).

Overview of the Documentation Library

This document provides an update to the following print-ready customer documentation which is included, at no cost, as a feature of your account:

- *FreeBSD MPS v3 Getting Started Guide*
- *FreeBSD MPS v3 Release Notes*
- *FreeBSD MPS v3 User's Guide*

There are also Web site resources such as FreeBSD MPS v3 Documentation Library and Frequently-Asked Questions (FAQ).

Overview of this Document

This document includes the following sections:

- “Two Options for Building a Firewall” on page 2.
- “Specifying a Preset Firewall Security Level” on page 4.
- “Specifying a Preset Server Type” on page 7.
- “IPFilter Package Commands and Files” on page 9.

Two Options for Building a Firewall

Important: If you utilize the IPFilter software package, do not also use the `set_fwlevel` command. The command may override the configuration you have set with the software package.

You have two options for building a FreeBSD MPS v3 firewall:

- Use an open-source software package (IPFilter). The software package is for administrators who are confident regarding the packet filtering rules set. This document provides an overview (and does not provide step-by-step instructions) regarding usage of the utility.
- Use a custom, simplified command (`set_fwlevel`). The command includes preset firewall settings. This document does provide an overview (as well as step-by-step instructions) regarding usage of the command. The command requires less detailed administrative knowledge on your part.

Overview of the IPFilter Software Package

Note: IPFilter, as it is implemented for your account, does not support Network Address Translation (NAT). Although NAT can potentially provide a second line of defense behind a server's firewall and the FreeBSD operating system supports NAT as well as firewall services, your account does not include support for both of them. Since NAT is similar in function to a firewall and is also based on IPFilter, this should not negatively impact the security of your account.

Included with the distribution of the FreeBSD operating system, the IPFilter open-source software package (and generic table structure) enables knowledgeable administrators to configure your account to utilize the packet filtering rule set. The software package is developed, distributed, and maintained by an open-source software community, headed by Darren Redd (<http://coombs.anu.edu.au/ipfilter/>). IPFilter is not distributed under the terms of a GPL or similar license.

Overview of the `set_fwlevel` Command

Your account provides a set of preset firewall security settings to establish an appropriate level of firewall security as well as to specify the services, ports, and protocols you wish those settings to apply to. The `set_fwlevel` command and supported arguments enable you to perform these tasks without extensive knowledge of the IPFilter software package. The command includes preset security settings which enable you to build a Red Hat Enterprise Linux (RHEL)-compatible firewall without knowing the packet filtering rule language. The command is a customized one which is unique to your account.

The `set_fwlevel` command enables you to specify which of the preset security settings you wish to apply to your account. The following provides an example of the command as it is enabled for your account:

```
set_fwlevel level [serverType]
set_fwlevel 0|1|2|3 [m|w]
```

Services Affected By Your Firewall Security Settings

The preset firewall security settings enable you to specify that there are no firewall rules regarding the services processed by your account. There are also several settings which enable you to specify that firewall rules do apply. In those cases, the setting you specify indicates that certain services in the following list are allowed or disallowed:

- America Online Instant Messaging (AIM)
- Domain name server (DNS) client
- Hypertext Transfer Protocol (HTTP)
- ICQ
- Internet Message Access Protocol (IMAP)
- Network Time Protocol (NTP) client
- Outbound Auth (or *identd*)
- Post Office Protocol, version three (POP3)
- Secure Shell (SSH)
- Secure Socket Layer (SSL)-enabled File Transfer Protocol (FTP-S)
- Simple Mail Transfer Protocol (SMTP)
- SSL-enabled HTTP (HTTP-S)
- SSL-enabled IMAP (IMAP-S)
- SSL-enabled POP3 (POP3-S)
- SSL-enabled SMTP (SMTP-S)
- SSL-enabled Telnet (Telnet-S)
- Web cache

Protocols Affected by Your Firewall Security Settings

The following protocols are the ones which your firewall security settings affect:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

Specifying a Preset Firewall Security Level

Note: To ensure that custom settings are not destroyed, `set_fwlevel` creates a backup file of `/etc/sysconfig/iptables` in the `/etc/sysconfig` directory with a number appended to the file name.

You can use the `set_fwlevel` command to turn off all rules (0) on your FreeBSD MPS v3 account. You can also use the command to specify low, medium, or high security.

Turning off Firewall Security

Following is an example where the command specifies no firewall security:

```
#set_fwlevel 0
```

When you specify no firewall security settings (0), all firewall rules are turned off. This means that no firewall rules apply to any of the ports and services your account processes.

Specifying Low Firewall Security

Following is an example where the command specifies a low (1) level of firewall security:

```
#set_fwlevel 1
```

When you specify low firewall security, your account blocks port-scan attempts, spoofing attempts, and remote loopback attacks.

Port-scans are series of messages from a malicious sender. The messages are used to determine which ports are being used by your account configuration. Once the malicious sender determines which of the ports are being utilized by your account, they attempt to use those ports to usurp control of communications, processes, and services on your account. Spoofing attacks are conducted by malicious Internet users who use TCP Flooding, DNS Server spoofing attempts, misleading Web site names, misleading email identifications, and Web link redirection to give the impression that your customers and Web site visitors have reached the correct Web content when, in fact, they have not.

Specifying Medium Firewall Security

We are requesting that the Urchin port (9878) be left open on the medium setting in addition to port 5190. However, on the highest level of firewall protection, all these ports should be closed.

Following is an example where the command specifies a medium (2) level of firewall security:

```
#set_fwlevel 2
```

When you specify medium firewall security, all of the low security firewall settings apply. In addition, specific security criteria are added to your account's firewall so that only essential and convenient ports and protocols are allowed.

When you specify medium firewall security, all of the low security firewall settings apply. In addition, specific security criteria are added to your account's firewall. With this setting, your account allows only the following services, ports, and protocols:

Services	Ports	Protocols
Google Analytics (formerly Urchin)	9878	UDP, TCP
ICQ and/or AIM	5190	TCP
FTP-S	989,990	TCP
SSH	22	TCP
Telnet-S	992	TCP
SMTP	25	TCP
SMTP-S	465	TCP
HTTP	80	TCP
HTTP-S	443	TCP
Web cache	8080	TCP
POP3	110	TCP
POP3-S	995	TCP
IMAP	143	TCP
IMAP-S	993	TCP
DNS client	53	UDP, TCP
NTP client	123	UDP
Outbound Auth (or <i>identd</i>)	113	TCP

Specifying High Firewall Security

Following is an example where the command specifies a high (3) level of firewall security:

```
#set_fwlevel 3
```

When you specify high firewall security, all of the low security firewall settings apply. In addition, specific security criteria are added to your account's firewall so that only essential secure ports and protocols are allowed.

When you specify high firewall security, all of the low security firewall settings apply. In addition, specific security criteria are added to your account's firewall.

With this setting, your account allows only the following services, ports, and protocols:

Services	Ports	Protocols
Google Analytics (formerly Urchin)	9878	UDP, TCP
ICQ and/or AIM	5190	TCP
SSH	22	TCP
SMTP	25	TCP
SMTP-S	465	TCP
HTTP	80	TCP
HTTP-S	443	TCP
Web cache	8080	TCP
POP3-S	995	TCP
IMAP-S	993	TCP
DNS	53	UDP, TCP
NTP	123	UDP
Outbound Auth (or <i>identd</i>)	113	TCP

Modifying Your Firewall Security Settings

In order to modify the firewall security settings on your account, run the `set_fwlevel` command again with the setting you would like to establish. For example, if you had previously specified a high (3) level of firewall security and you wish to modify that level to medium (2), you must issue the following command:

```
#set_fwlevel 2
```

If, after you have specified a medium (2) level of firewall security, you wish to return to a high (3) level of firewall security, you must issue the following command:

```
#set_fwlevel 3
```

Specifying a Preset Server Type

As well as specifying a firewall security level for your FreeBSD MPS v3 account, you can specify the server types for which the firewall security settings apply. You can specify that all server types apply the firewall security settings. When you do not specify a server type, in effect, you are actually applying the firewall security settings to all server types. Otherwise, you can specify that the firewall security settings apply only to Web servers or Mail services.

How Web Server Settings Affect Firewall Security Settings

Following is an example where the command specifies no firewall security with an additional argument to specify that that the firewall settings apply only to the Web server:

```
#set_fwlevel 0 w
```

Following is an example where the command specifies a low level of firewall security with an additional argument to specify that that the firewall settings apply only to the Web server:

```
#set_fwlevel 1 w
```

When you specify that firewall security settings apply to Web server (*w*) process and services, the setting does not change the firewall if you have also specified no (0) or low (1) security applies. However, when you have specified medium (2) or high (3), changes do apply.

Following is an example where the command specifies a medium firewall level of security with an additional argument to specify that that the firewall settings apply only to the Web server:

```
#set_fwlevel 2 w
```

Following is an example where the command specifies a high level of firewall security with the additional argument to specify that that the firewall settings apply only to the Web server:

```
#set_fwlevel 3 w
```

How Mail Server Settings Affect Firewall Security Settings

Following is an example where the command specifies no firewall security with an additional argument to specify that that the firewall settings apply only to the Mail server:

```
#set_fwlevel 0 m
```

Following is an example where the command specifies a low level of firewall security with an additional argument to specify that that the firewall settings apply only to the Mail server:

```
#set_fwlevel 1 m
```

When you specify that firewall security settings apply to Mail server (*m*) processes and services, the setting does not change the firewall if you have also specified no (0) or low (1) security applies. However, when you have specified medium (2) or high (3), changes do apply.

Following is an example where the command specifies a medium level of firewall security with an additional argument to specify that that the firewall settings apply only to the Mail server:

```
#set_fwlevel 2 m
```

Following is an example where the command specifies a high level of firewall security with an additional argument to specify that that the firewall settings apply only to the Web server:

```
#set_fwlevel 3 w
```

Modifying Your account Type Settings

Important: If you issue the `set_fwlevel` command after you have specified a setting for the server type and you do so without including an argument to specify a server type, then the firewall will apply to all processes on the mail server (`m`) and Web server (`w`).

In order to modify the server type settings on your account, run the `set_fwlevel` command again with the setting you would like to establish. For example, if you had previously specified a high (3) level of firewall security with the additional argument that the firewall applies only to the mail server (`m`) and you wish to switch that argument so that the firewall applies only to the Web server (`w`), you must issue the following command:

```
#set_fwlevel 3 w
```

If, after you have specified that the firewall applies only to the Web server, you wish to switch the firewall security settings to the mail server, you must issue the following command:

```
#set_fwlevel 3 m
```

IPFilter Package Commands and Files

Important: If you are a knowledgeable administrator, you can utilize the IPFilter software package to configure a custom firewall. If you accidentally lock yourself out of your server (or otherwise block the SSH port), the package provides a reset function. Also, keep in mind that your server stores a back up of your most recent `/root/.ipfilter`.

An IPFilter firewall denies or permits packets in an explicit manner and maintains the ability to distinguish between the interfaces your FreeBSD MPS v3 account utilizes. Not all of the commands and functions provided by the IPFilter software package are supported by your account. At the time of this release, your account supports the `ipf` and `ipftest` commands which provide support for the following tasks:

- Read a firewall rule set into your account.
- Remove (or *flush*) a firewall rule set.
- Deleting an individual firewall rule.
- Test a firewall rule set prior to implementing it on your account.

The `ipf` command is in the following location on your account:

```
/sbin/ipf
```

As a root user, you can issue the command to read in a set of rules, from either a standard input (`stdin`) or a file you specify, and adds them to your account's current firewall list. In general, it does this by appending the rules you previously composed and applied. You can also use the command to remove the current firewall rule set or to delete an individual firewall rule.

The `ipftest` command is in the following location on your account:

```
/sbin/ipftest
```

As a root user, you can issue the command to run a set of test programs. The command enables you to test a set of filter rules without having to put them in place, in operation and proceed to test their effectiveness. This can minimize disruptions in providing a secure IP environment. The command will parse any standard rule set for use with the command and apply input, returning output as to the result. However, the command returns one of three values for packets passed through the filter:

- Pass
- Block
- No match

The syntax of the command follows:

```
ipftest <options><filename>
```

If you install a rule set that unintentionally blocks a port, you can change the offending rule in the rules file and then reload the file. You can also run `reset_firewall` which clears all rules you have previously established. A backup of their rules will be saved in the following location:

```
/root/.ipfilter
```

For more about the usage of the `ipf` and `ipftest` commands, refer to the Man Pages provided as part of the FreeBSD Operating System as well as on the FreeBSD Project Web site at the following location:

<http://www.freebsd.org/cgi/man.cgi>