
Linux VPS

Firewall Supplement

First Edition
April 2007

Table of Contents

Introduction	1
Two Options for Building a Firewall	2
Overview of the iptables Command-Line Utility	2
Overview of the set_fwlevel Command.....	2
File Locations	3
Services Affected By Your Firewall Security Settings.....	3
Protocols Affected by Your Firewall Security Settings.....	4
Specifying a Preset Firewall Security Level	5
Turning Off All Rules.....	5
Specifying Low Firewall Security	5
Block Port-Scans.....	5
Limit the effects of Denial of Service Attacks.....	5
Process Only Certain ICMP Packet Types.....	5
Specifying Medium Firewall Security	6
Specifying High Firewall Security.....	6
Modifying Your Firewall Security Settings.....	7
Specifying a Preset Server Type.....	8
How Web Server Settings Affect Firewall Security Settings	8
How Mail Server Settings Affect Firewall Security Settings	9
Modifying Your Server Type Settings.....	10

Introduction

A firewall monitors and controls the traffic coming into and out of your 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`).

Important: Although this document provides an overview of the `iptables` command line utility, it does not provide the details of how to build a firewall with the utility.

Knowledgeable administrators who wish to utilize the utility should refer to other resources and documentation. All who use the `iptables` command-line utility should carefully consider all of the tasks they perform with that utility. Always make back up files, stored remotely, for `iptables` configurations and settings you have previously tested and used.

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

- *Linux VPS Getting Started Guide*
- *Linux VPS Release Notes*
- *Linux VPS Technical Overview* (available only through the Backroom)
- *Linux VPS User's Guide*

There are also Web site resources such as Linux VPS Documentation Library and Frequently-Asked Questions (FAQ).

This document includes the following sections:

- “Two Options for Building a Firewall” on page 2.
- “Specifying a Preset Firewall Security Level” on page 5.
- “Specifying a Preset Server Type” on page 8.

Two Options for Building a Firewall

You have two options for building a firewall:

- Use a utility (`iptables`) based on the packet filtering rule language. The utility 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.

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

Overview of the `iptables` Command-Line Utility

The `iptables` command line utility (and generic table structure) enables knowledgeable administrators to configure your account to utilize the packet filtering rule set. The utility is developed, distributed, and maintained by the Netfilter Core Team (<http://www.netfilter.org>). The utility is distributed under the terms of GNU is not UNIX General Public License (GNU GPL).

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 `iptables` command-line utility. 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 Linux VPS.

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]
```

File Locations

The following table describes the rules files and provides the locations of the rules files.

Description	Location
You can issue the <code>set_fwlevel</code> command and utilize preset security level.	<code>usr/local/sbin/set_fwlevel</code>
When you issue the <code>set_fwlevel</code> command, the rules which are currently loaded are backed up.	<code>/root/.iptables/iptablesBK.<num></code>
When you issue the <code>set_fwlevel</code> command, rules information is moved from the location where it was previously stored.	<code>/etc/sysconfig/iptables</code>
When you issue the <code>set_fwlevel</code> command, rules information is moved to a new location.	<code>etc/sysconfig/iptables.bk.<num></code>

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:

- Domain name server (DNS) client
- Hypertext Transfer Protocol (HTTP)
- 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

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

Turning Off All Rules

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 and limits the effects of denial of service attacks. In addition, the setting specifies that only certain Internet Control Message Protocol (ICMP) packet types are processed. The ICMP protocol enables routers and hosts to exchange control messages. For example, a host might send an ICMP packet when a router is experiencing congestion. Or a router might send one when a destination host is unavailable. A firewall can prevent these ICMP packet exchanges from resulting in a compromise to your account.

Block Port-Scans

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.

Limit the effects of Denial of Service Attacks

When a malicious Internet user attempts a denial of service attack, your account limits the effects of that attempt if you have specified low security. The attacks are typically aimed at Web servers and usually involve an attempt to make hosted Web pages unavailable. Some of the following are means by which malicious Internet users may initiate the attacks:

- Flooding network traffic
- Disrupting server performance by sending many requests
- Preventing access to a particular Web service
- Preventing a particular individual from accessing a service

Process Only Certain ICMP Packet Types

When you specify low security, only the following ICMP packet types are processed:

- **0 (outgoing ping)** – You can use the ping computer network tool to verify whether a particular host is reachable. The tool sends an ICMP Echo Request and listens for a reply. When you specify a low security setting for your account, it may send outgoing ping packets only. Your account will not reply to another host's ping.
- **3 (destination unreachable)** – Your account will process ICMP packets which are generated by another host. These packets are received when a designated transport

protocol is unable to process data in the transport layer and the remote system or host has no means of replying with that information.

- **4 (source quench)** -- A remote host may discard data if it does not have the buffer space needed to queue the data for output to the next network on the route to the destination host. When you specify low security, your account will process ICMP packets which indicate this has occurred.
- **11(timeout)** – A remote host may not reply or acknowledge your account’s sent data in sufficient time. When you specify low security, your account will process ICMP packets which indicate this has occurred.
- **12 (parameter problems)** -- A remote host cannot process a packet due to a problem in the packet header (or, possibly, an incorrect argument in an option). The remote host has discarded the packet and has sent this ICMP packet to your account. When you specify low security, your account processed this type of ICMP packet.

For more information about ICMP, refer to the *Internet Control Message Protocol DARPA Internet Program Protocol Specification* available at the Internet Engineering Task Force (IETF) Web site (<http://www.ietf.org/rfc/rfc792.txt>).

Specifying Medium Firewall Security

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

Services	Ports	Protocols
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.

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

Services	Ports	Protocols
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, 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
```

When you specify that medium (2) firewall security settings apply to the Web server only (w), your account is open only to the following services, ports, and protocols:

Services	Ports	Protocols
FTP-S	989, 990	TCP
SSH	22	TCP
Telnet-S	992	TCP
Outbound SMTP	25	TCP
HTTP	80	TCP
HTTP-S	443	TCP
Web cache	8080	TCP
DNS client	53	UDP, TCP
NTP	123	UDP
Outbound Auth (or <i>identd</i>)	113	TCP

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
```

When you specify that high (3) firewall security settings apply to the Web server only (w), your account is open only to the following services, ports, and protocols:

Services	Ports	Protocols
SSH	22	TCP
Outbound SMTP	25	TCP
HTTP	80	TCP
HTTP-S	443	TCP
Web cache	8080	TCP
DNS client	53	UDP, TCP
NTP client	123	UDP
Outbound Auth (or <i>identd</i>)	113	TCP

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
```

When you specify that medium (2) firewall security settings apply to the Mail server only (m), your account is open only to the following services, ports, and protocols:

Services	Ports	Protocols
FTP-S	989, 990	TCP
SSH	22	TCP
Telnet-S	992	TCP
SMTP-S	465	TCP
POP3	110	TCP
POP3-S	995	TCP
IMAP	993	TCP
IMAP-S	143	TCP
DNS client	53	UDP, TCP
NTP client	123	UDP
Outbound Auth (or <i>identd</i>)	113	UDP

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
```

When you specify that high (3) firewall security settings apply to the Mail server only (m), your account is open only to the following services, ports, and protocols:

Services	Ports	Protocols
SSH	22	TCP
SMTP	25	TCP
SMTP-S	465	TCP
POP3-S	995	TCP
IMAP-S	993	TCP
DNS client	123	UDP, TCP
NTP client	123	UDP
Outbound Auth (or <i>identd</i>)	113	TCP

Modifying Your Server 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
```