



Plesk 8.3 for Linux/Unix Firewall Module Administrator's Guide

Copyright Notice

ISBN: N/A

SWsoft.

13755 Sunrise Valley Drive

Suite 600

Herndon

VA 20171 USA

Phone: +1 (703) 815 5670

Fax: +1 (703) 815 5675

© Copyright 1999-2007,

SWsoft Holdings, Ltd.

All rights reserved

Distribution of this work or derivative of this work in any form is prohibited unless prior written permission is obtained from the copyright holder.

Patented hosting technology protected by U.S. Patents 7,099,948; 7,076,633.

Patents pending in the U.S.

Linux is a registered trademark of Linus Torvalds.

ASPLinux and the ASPLinux logo are registered trademarks of SWsoft.

RedHat is a registered trademark of Red Hat Software, Inc.

Solaris is a registered trademark of Sun Microsystems, Inc.

X Window System is a registered trademark of X Consortium, Inc.

UNIX is a registered trademark of The Open Group.

Intel, Pentium, and Celeron are registered trademarks of Intel Corporation.

MS Windows, Windows 2003 Server, Windows XP, Windows 2000, Windows NT, Windows 98, and Windows 95 are registered trademarks of Microsoft Corporation.

IBM DB2 is a registered trademark of International Business Machines Corp.

SSH and Secure Shell are trademarks of SSH Communications Security, Inc.

MegaRAID is a registered trademark of American Megatrends, Inc.

PowerEdge is a trademark of Dell Computer Corporation.

Request Tracker is a trademark of Best Practical Solutions, LLC

All other trademarks and copyrights referred to are the property of their respective owners.

Contents

Preface	4
<hr/>	
Typographical Conventions	4
Feedback	5
About Plesk Firewall Module	6
<hr/>	
Installing Plesk Firewall Module	7
<hr/>	
Setting Up Firewall	8
<hr/>	
Managing Access to System Services	8
Managing System Policies	9
Managing Custom Rules	10
Appendix A. Predefined Firewall Rules Specifications	13
<hr/>	

Preface

In this section:

Typographical Conventions	4
Feedback	5

Typographical Conventions

Before you start using this guide, it is important to understand the documentation conventions used in it.

The following kinds of formatting in the text identify special information.

Formatting convention	Type of Information	Example
Special Bold	Items you must select, such as menu options, command buttons, or items in a list.	Go to the System tab.
	Titles of chapters, sections, and subsections.	Read the Basic Administration chapter.
<i>Italics</i>	Used to emphasize the importance of a point, to introduce a term or to designate a command line placeholder, which is to be replaced with a real name or value.	The system supports the so called <i>wildcard character</i> search.
Monospace	The names of commands, files, and directories.	The license file is located in the http://docs/common/licenses directory.
Preformatted	On-screen computer output in your command-line sessions; source code in XML, C++, or other programming languages.	<pre># ls -al /files total 14470</pre>
Preformatted Bold	What you type, contrasted with on-screen computer output.	<pre># cd /root/rpms/php</pre>
CAPITALS	Names of keys on the keyboard.	SHIFT, CTRL, ALT

KEY+KEY	Key combinations for which the user must press and hold down one key and then press another.	CTRL+P, ALT+F4
---------	--	----------------

Feedback

If you have found a mistake in this guide, or if you have suggestions or ideas on how to improve this guide, please send your feedback to userdocs@swsoft.com. Please include in your report the guide's title, chapter and section titles, and the fragment of text in which you have found an error.

CHAPTER 1

About Plesk Firewall Module

Plesk™ Firewall is a module that protects your Plesk-enabled server and private network from unauthorized access. With this module, you can easily set firewall rules and fine tune them through a user-friendly interface.

Installing Plesk Firewall Module

You can install the Plesk Firewall module to the Plesk server in two ways: from the control panel (recommended), and from the command line.

➤ *To install the Plesk Firewall module through the control panel:*

- 1 Login as administrator to the control panel.
- 2 Select the **Modules** shortcut in the navigation pane
- 3 Click **Manage Modules**.
- 4 Click **Add New Module**.
- 5 Select a module package file, and click **OK**.

➤ *To install the Plesk Firewall module through the command line:*

- 1 Login as root to the server, where Plesk is installed.
- 2 Run the command

```
/plesk_installation_directory/admin/bin/modulemng --install --file=<plesk_firewall_module_filename>, where 'plesk_installation_directory' is the directory you installed Plesk to.
```

Example:

```
/usr/local/psa/admin/bin/modulemng --install --file=/opt/modules/firewall.rpm
```

Note: Plesk Firewall module and other modules that come with Plesk are located in the directory `/opt/modules` of Plesk distribution.

Setting Up Firewall

After you installed the module, you can do the following:

- View and change the predefined rules that control connections to the following system services: Administrative Plesk control panel; Web server; FTP server; SSH server; SMTP server; POP3 server; IMAP server; mail password change service; MySQL server; PostgreSQL server; Samba file sharing server for Windows clients; VPN; domain name server; ICMP echo requests. By default, these rules allow all incoming connections to these services.
- View and change the predefined system policies that define what to do with all incoming, outgoing and transit communications that do not match the explicitly defined rules.
- Add, change, and remove custom rules. For example, you may want to add a rule that will allow access to FTP accounts on the server in passive mode.

In this chapter:

Managing Access to System Services	8
Managing System Policies	9
Managing Custom Rules.....	10

Managing Access to System Services

For each system service, you can choose whether to allow or deny all incoming communications, or allow only communications coming from specific IP/network addresses.

➤ *To allow or restrict access to a service on your Plesk server:*

- 1 Go to **Modules > Firewall**, and click **Edit Firewall Configuration**.
- 2 Click the service name.
- 3 Do any of the following:
 - To allow all incoming connections, select the **Allow** option and click **OK**.
 - To deny all incoming connections, select the **Deny** option and click **OK**.
 - To deny access to a service from specific IP/network addresses, select the **Allow from selected sources, deny from others** option, specify the IP address or network address from which access to the selected service is allowed, and click **Add**. After you specify the required addresses, click **OK**.
- 4 To apply all changes to the firewall configuration, click **Activate**, and then click **Activate** again.

Managing System Policies

System policies define what to do with all incoming, outgoing and transit communications that do not match the explicitly defined rules. The system policies are usually displayed at the bottom of the list of rules.

- *To allow or deny communications of specific type:*
 - 1 Go to **Modules > Firewall**, and click **Edit Firewall Configuration**.
 - 2 Click the icon to the left of the policy name you want to change. If the policy currently allows all connections, clicking this icon will prohibit all connections and vice versa.
 - 3 To apply the changes, click **Activate**, and then click **Activate** again.

Managing Custom Rules

This section describes how to add, modify, remove custom rules, and change the order in which the rules are applied. This section also covers the steps required for enabling passive mode for FTP connections.

➤ **To add a custom rule:**

- 1 Go to **Modules > Firewall**, and click **Edit Firewall Configuration**.
- 2 Click **Add Custom Rule**.
- 3 Enter the name of the new rule in the **Name of the rule** field.
- 4 Select one of the following communication directions: **Incoming** for the communications inbound to the server, **Outgoing** for communications outbound from this server, or **Forwarding** for communications transiting through your server in any direction.

For incoming communications you can specify the destination ports on your server, the protocol used for this communication, and the IP address the communications come from.

For outgoing communications you can specify the destination ports, destination IP address, and the protocol used for the communication.

For transit communications going through the server, you can specify the destination ports and source / destination IP addresses.

- 5 To specify the port number, type it into the **Add port** input box, and click **Add**. To remove a port number from an existing rule, select it from the list and click **Remove**. If the list of ports is empty, this rule will be applied to all TCP and UDP ports.
- 6 To specify the IP address or network address, type it into the **Add IP address or network** input box, and click **Add**. To remove an IP address or network from the list, select it in the list and click **Remove**. If the list of IP addresses is empty, this rule will be valid for all IP addresses.
- 7 Specify the action that will be applied to the communications that match the defined criteria: **allow** or **deny**.
- 8 Click **OK** to submit the rule.
- 9 After you have defined the required rules, click **Activate** to apply them to your system. A confirmation screen will open, in which you can preview the shell script generated to apply your rules (this might be of interest only to advanced users). Click **Activate** to apply the new configuration.

When the new configuration is being applied, the module will check for connection with the control panel. If there are some connection problems, the Firewall module will automatically revert to the previous active configuration in 60 seconds. Thus, if you misconfigure your firewall in such a way that access to your control panel is prohibited even for you, this wrong configuration will be automatically discarded and you will be able to access your server in any case.

Note: Unless your configuration is activated, you have a chance to discard all the rules you configured. To do this, click the **Revert to Active Configuration** button.

Under FreeBSD, all currently established TCP connections will drop when the new configuration is activated!



➤ **To edit a custom rule:**

- 1 Go to **Modules > Firewall**, and click **Edit Firewall Configuration**.
- 2 Click the rule name in the list of existing rules. Make necessary changes (the options are the same as when creating a new rule).

➤ **To remove a custom rule:**

- 1 Go to **Modules > Firewall**, and click **Edit Firewall Configuration**.
- 2 Select the check box corresponding to the rule you want to remove and click **Remove Selected**.

➤ **To change the order in which your custom rules are applied:**

- 1 Go to **Modules > Firewall**, and click **Edit Firewall Configuration**.
- 2 Click the icons  **Up** or  **Down** in the **Order** column. This will move the rule relatively to other rules covering the same direction (incoming communications, outgoing communications, or data forwarding).

➤ **To enable passive mode for FTP connections on your server:**

- 1 Log in as "root" to the server shell over SSH.
- 2 Edit your ProFTPD configuration file.
 - a Issue the command `vi /etc/proftpd.conf`
 - b Add the following lines anywhere within the <Global> section:

```
PassivePorts 49152 65534
```
 - c Save the file
- 3 Log in to Plesk as "admin", go to **Modules > Firewall**, and click **Edit Firewall Configuration**.
- 4 Click **Add Custom Rule**.
- 5 Specify the following:
 - a Rule name
 - b Direction: select Incoming.
 - c Action: select Allow.
 - d Ports: in the Add port input box, enter the value 49152-65534. Leave the TCP option selected, and click **Add**.

- 6 Click **OK**.
- 7 Click **Activate**, and then click **Activate** again.

Appendix A. Predefined Firewall Rules Specifications

The following table lists the system services to which you can restrict access using the Firewall's predefined rules.

Service name	Ports used by service
Plesk administrative interface	TCP 8443
Samba (file sharing on Windows networks)	UDP 137, UDP 138, TCP 139, TCP 445
Plesk VPN	UDP 1194
WWW server	TCP 80, TCP 443
FTP server	TCP 21
SSH (secure shell) server	TCP 22
SMTP (mail sending) server	TCP 25, TCP 465
POP3 (mail retrieval) server	TCP 110, TCP 995
IMAP (mail retrieval) server	TCP 143, TCP 993
Mail password change service	TCP 106
MySQL server	TCP 3306
PostgreSQL server	TCP 5432
Tomcat administrative interface	TCP 9008, TCP 9080
Domain name server	UDP 53, TCP 53
Ping service	<ICMP echo request>