
SWsoft, Inc.

Plesk™ Firewall

Administrator's Guide



(c) 1999-2004

ISBN: N/A
SWsoft Inc
13800 Coppermine Drive
Suite 112
Herndon
VA 20171 USA
Tel: +1 (703) 815 5670
Fax: +1 (703) 815 5675

Copyright © 1999-2004 by SWsoft, Inc. 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.
Linux is a registered trademark of Linus Torvalds.
ASPLinux and the ASPLinux logo are registered trademarks of SWsoft, Inc.
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.

Contents

Preface	5
About This Guide	5
Documentation Conventions.....	5
Typographical Conventions.....	5
General Conventions	6
Feedback.....	6
Using Plesk™ Firewall	7
Terms and Definitions	8
How to Access Plesk Firewall	9
Adding a Custom Rule.....	10
Managing Custom Rules.....	13
Managing Access to System Services.....	13
Managing System Policies.....	14
Appendix	15
Index	16

Table of Figures

Figure 1: Firewall management page.....	9
Figure 2: Adding a new custom rule	12

CHAPTER 1

Preface

In This Chapter

About This Guide.....	5
Documentation Conventions.....	5
Feedback	6

About This Guide

This Guide provides detailed instructions on how to use the Plesk™ Firewall, 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.

Documentation Conventions

Before you start reading this guide, it is important to understand the documentation conventions used in it. For information on specialized terms used in the documentation, see the Terms and Definitions section at the beginning of this document.

Typographical Conventions

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 QoS 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.	These are the so-called <i>shared VPSs</i> . To destroy a VPS, type <code>vzctl destroy vpsid</code> .
Monospace	The names of commands, files, and directories.	Use <code>vzctl start</code> to start a VPS.

<code>Preformatted</code>	On-screen computer output in your command-line sessions; source code in XML, C++, or other programming languages.	<code>Saved parameters for VPS 101</code>
<code>Monospace Bold</code>	What you type, contrasted with on-screen computer output.	<code># rpm -V virtuo- release</code>
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

General Conventions

Be aware of the following conventions used in this book.

- Chapters in this guide are divided into sections, which, in turn, are subdivided into subsections. For example, **Documentation Conventions** is a section, and **General Conventions** is a subsection.
- When following steps or using examples, be sure to type double-quotes ("), left single-quotes ('), and right single-quotes (') exactly as shown.
- The key referred to as RETURN is labeled ENTER on some keyboards.

The root path usually includes the `/bin`, `/sbin`, `/usr/bin` and `/usr/sbin` directories, so the steps in this book show the commands in these directories without absolute path names. Steps that use commands in other, less common, directories show the absolute paths in the examples.

Feedback

If you spot a typo in this guide, or if you have thought of a way to make this guide better, we would love to hear from you!

If you have a suggestion for improving the documentation (or any other relevant comments), try to be as specific as possible when formulating it. If you have found an error, please include the chapter/section/subsection name and some of the surrounding text so we can find it easily.

Please submit a report by e-mail to userdocs@sw-soft.com.

CHAPTER 2

Using Plesk™ Firewall

A firewall is a system designed to prevent unauthorized access to or from a private network and restrict access to the services running on a firewall-enabled server. In other words, firewalls use policies or set of rules that govern the flow of data packets to and from the outside world. This helps you prevent unauthorized Internet users from accessing private networks connected to the Internet.

The Firewall module adds firewall functionality to your Plesk™ control panel. All data packets entering or leaving the local network shall pass through the firewall, which serves as a gate between your network and the Internet. The firewall shall examine each packet and handle it in accordance with specified filtering rules.

In This Chapter

Terms and Definitions.....	8
How to Access Plesk Firewall.....	9
Adding a Custom Rule	10
Managing Custom Rules	13
Managing Access to System Services.....	13
Managing System Policies	14

Terms and Definitions

Below are the most basic terms related to firewalling. You might be already familiar with them. If so, you can skip this section and start configuring your firewall.

Rules

The Plesk Firewall module enforces user-defined rules (or custom rules) to process data packets. Each packet is first assessed and then handled depending on how this packet matches the security criteria set in the rules. The Plesk Firewall will consequently apply the rules that go first in the list of rules.

Hosts

A host is any computer that is connected to (or a part of) a network. The Firewall can be configured to prohibit access by specific hosts.

Ports

Ports are virtual connection points used by networking services (do not confuse virtual ports with physical ports like USB ports). Each port has an identification number, and common services are associated with specific ports by convention. See Appendix (on page 15) for the list of services and associated ports.

Packets

Communication protocols, such as TCP, divide the data flowing between hosts into chunks that are called *packets*. Each packet includes the data being transmitted and bears information on the type of the packet, destination address and the packet source. Using this information, the Firewall analyzes an individual packet and accepts or rejects it based on comparison with the specified rules.

Services


In simple terms, services are based on protocols that let one computer access a type of data stored on another computer. Many host computers that are connected to the Internet offer services. For example, HTTP servers use the HyperText Transfer Protocol to provide World Wide Web service, FTP servers offer File Transfer Protocol services, SMTP servers use the Simple Mail Transport Protocol to exchange e-mail, and POP servers use the Post Office Protocol to exchange e-mail.

The Plesk Firewall offers you a predefined set of services that can be controlled using the firewall rules. For the list of services and ports commonly associated with them, see Appendix (on page 15).

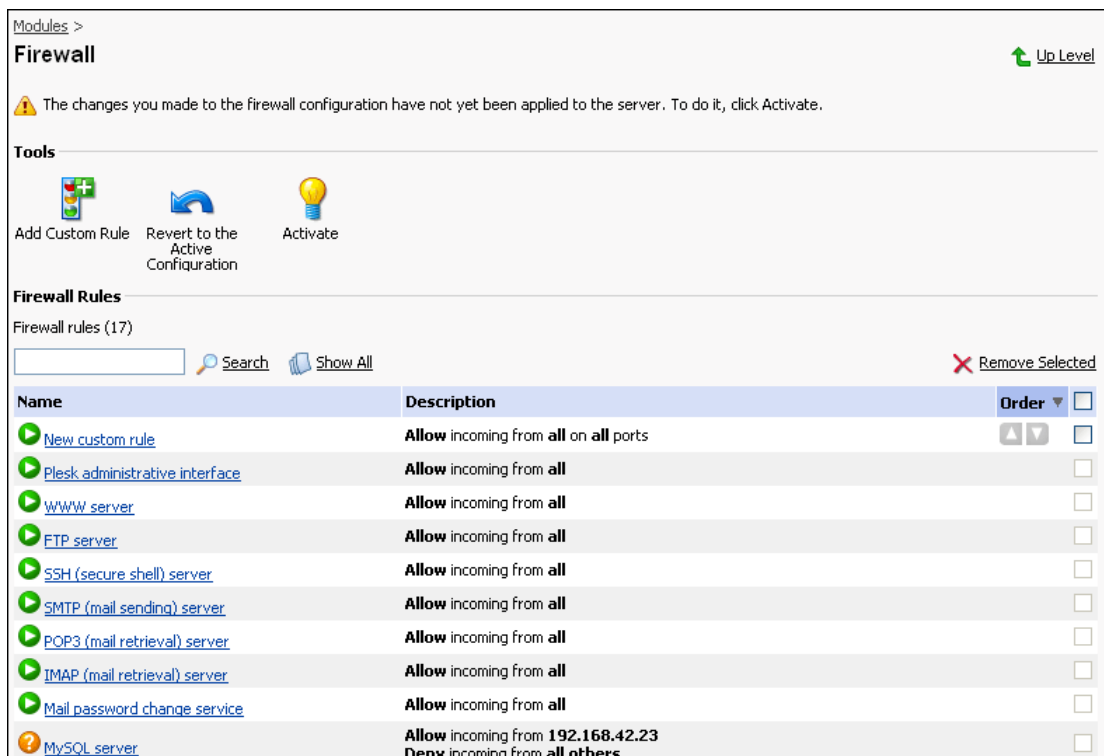
System Policies

System policies are rules defining how the firewall will handle all incoming, outgoing and forwarded communications that do not match the explicitly defined firewall rules. In the Plesk Firewall, the system policies are displayed at the bottom of the rules list.

How to Access Plesk Firewall

To access the Plesk Firewall, select the **Modules** shortcut in the navigation pane and click the  Firewall button.

The page that opens is called the Firewall management page displaying the list of active custom rules and system policies. Using the buttons located on this page, you can configure your firewall filtering rules.



Modules > **Firewall** [Up Level](#)

Tools

[Add Custom Rule](#) [Revert to the Active Configuration](#) [Activate](#)

Firewall Rules

Firewall rules (17) [Search](#) [Show All](#) [Remove Selected](#)

Name	Description	Order	
New custom rule	Allow incoming from all on all ports	1	<input type="checkbox"/>
Plesk administrative interface	Allow incoming from all		<input type="checkbox"/>
WWW server	Allow incoming from all		<input type="checkbox"/>
FTP server	Allow incoming from all		<input type="checkbox"/>
SSH (secure shell) server	Allow incoming from all		<input type="checkbox"/>
SMTP (mail sending) server	Allow incoming from all		<input type="checkbox"/>
POP3 (mail retrieval) server	Allow incoming from all		<input type="checkbox"/>
IMAP (mail retrieval) server	Allow incoming from all		<input type="checkbox"/>
Mail password change service	Allow incoming from all		<input type="checkbox"/>
MySQL server	Allow incoming from 192.168.42.23 Deny incoming from all others		<input type="checkbox"/>

Figure 1: Firewall management page

Adding a Custom Rule

On the Firewall management page you can perform the following operations:

- view a list of existing rules
- switch to the **Edit mode** and revert to the **Active mode**
- change the priority of a rule
- add new custom rules
- edit custom rules
- remove rules


This section describes how to choose a required mode and add new rules.

The Firewall module has two modes:

- Active mode
- Edit mode

In the **Active mode**, you cannot make changes to the active firewall configuration or apply individual rules on the fly as immediate application of a misconfigured rule could expose your server to a security threat or result in network disruption. In this mode, you can only view the existing firewall configuration. To configure firewall rules, you need to switch the firewall to the **Edit mode**.


To switch to the **Edit mode**:

Click the  **Edit Firewall Configuration** button on the Firewall management page.

To switch to the **Active mode**:

Click the  **Revert to the Active Configuration** button.

To add a custom rule:

- 1 Switch to the **Edit mode** and click  **Add Custom Rule** (in the **Active mode**, this button is not available).
- 2 On the **Custom Rule** page, enter the name of the new rule in the **Name of the rule** field.
- 3 Using the option buttons below, 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 the incoming communications you can also specify the destination ports on your server, the protocol used for this communication, and IP address the communications come from (see steps 4 and 5).

For the outgoing communication you can specify the destination ports, destination IP address, and the protocol used for the communication (see steps 4 and 5).

For the transit communications going through the server, you can specify the destination ports, source and destination IP addresses (see steps 4 and 5).

- 4** To specify a port number, type it into the **Add port** input box, and click **Add**. To remove a port number from the rule, select it from the list and click **Remove**. Leaving the list of ports empty designates that this rule should apply to all TCP and UDP ports.
- 5** To specify an IP address or network, type it into the **Add IP address or network** input box, and click **Add**. To remove an IP address or network, select it from the list and click **Remove**. Leaving the list of IP addresses empty designates that this rule should apply to all IP addresses.
- 6** Specify the action that will be applied to the communications that match the defined criteria: **allow** or **deny**.

7 Click OK to submit the rule.

Modules > Firewall >

Custom rule Up Level

Properties

Name of the rule *

Match direction

Incoming

Outgoing

Forwarding

Action

Allow

Deny

Ports

(any port)

Add port:

TCP UDP


Sources

(any host)

Add IP address or network: . . . /

* Required fields

Figure 2: Adding a new custom rule

After you have defined all required rules, click  **Activate** to apply them to your system. A confirmation screen will open, and you will be able to preview the shell script that will be used for applying your rules (this might be of interest only to advanced users). Click **Activate** to apply the new configuration.




When the module will be applying new configuration, it 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!

Managing Custom Rules

You can view existing firewall rules on the Firewall management page. All existing firewall rules are given in a list with the following columns:

Status icon defines the type of the rule:  means that the rule allows communications,  indicates that the rule denies communications, and  shows that the rule allows specific communications, and prohibits all others.



Name displays the name of the rule;

Description contains the description of the rule as specified during its creation

Order contains buttons used to change the order of rule application.

Note: You can change the order and remove only the custom rules that you created! The order of default rules cannot be changed.

To change the order in which the rules are applied:

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 remove a custom rule:

- 1 Switch to the **Edit mode**.
- 2 Select the checkboxes corresponding to the rules you want to remove and click **Remove Selected**.

To edit a custom rule:

- 1 Switch to the **Edit mode**.
- 2 Click the rule's name in the list of existing rules. Make necessary changes (the options are the same as when creating a new rule).

Managing Access to System Services

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

To enable/disable access to a service on your Plesk server:

Switch to the **Edit mode** and click on the icon that accompanies the service name

OR

Switch to the **Edit mode** and click on the service name. Then select the required option (**Allow** or **Deny**) and click **OK**.

To allow access to a service from specific IP/network addresses:

- 1 Switch to the **Edit mode** and click on the service name.
- 2 Select the **Allow from selected sources, deny from others** option to specify the IP or networks addresses from which you would allow access to a given service.
- 3 After you specify all required addresses, click **OK**.

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 entries corresponding to the system policies are usually located in the bottom of the rules list.

To allow/deny the communications of a specific type:

- 1 Switch to the **Edit mode**.
- 2 Click the icon to the left of the policy name you want to edit. If the policy currently allows all connections, clicking this icon will prohibit them and vice versa.

APPENDIX A

Appendix

System services to which you can restrict access using the Firewall module

<u>Service name</u>	<u>Ports used by service</u>
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>

Index

A

About This Guide • 5
Adding a Custom Rule • 10
Appendix • 15

D

Documentation Conventions • 5

F

Feedback • 6

G

General Conventions • 6

H

How to Access Plesk Firewall • 9

M

Managing Access to System Services • 13
Managing Custom Rules • 13
Managing System Policies • 14

P

Preface • 5

T

Terms and Definitions • 8
Typographical Conventions • 5

U

Using Plesk™ Firewall • 7