Manage a Firewall Using your Plesk Control Panel

Contents

Goals

This guide will help you to be able to use a Plesk firewall to protect your Plesk-enabled server from unauthorized access. Your Plesk panel comes with a firewall, which you can configure. You will be able to create a set of firewall rules and manage them using Plesk.

The method for setting up a firewall is based on whether you have Plesk installed on a Linux-based or Windows-based platform. Both methods are described below.

Linux-Based Plesk Firewall

On our Linux-based Plesk server, the firewall module is already installed and configured. However, you can do the following:

- View and change predefined rules that control connections to the following system services:

Administrative Control panel

Webserver, FTP Server, SSH Server, MySQL Server, PostgreSQL server

Mail password change services

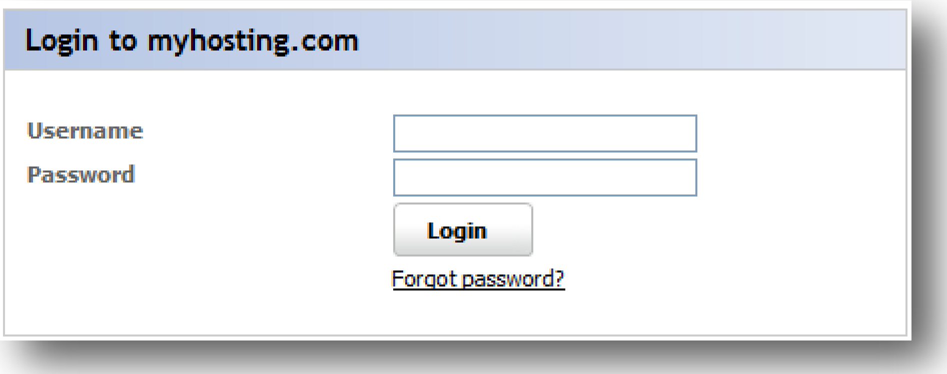
VPN, DNS

By default, these rules allow all incoming connections to these services. You have the following options to:

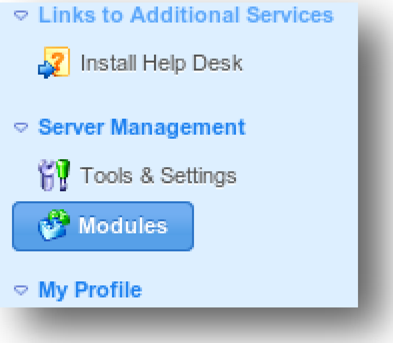
- View and change the predefined system policies
- Add, change, and remove custom rules

To locate the firewall module in Plesk, please follow the instructions below:

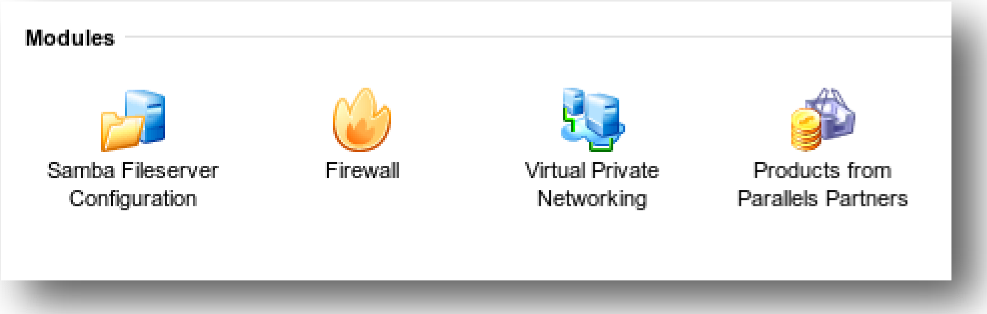
1. First log into your control panel at http://manage.myhosting.com.



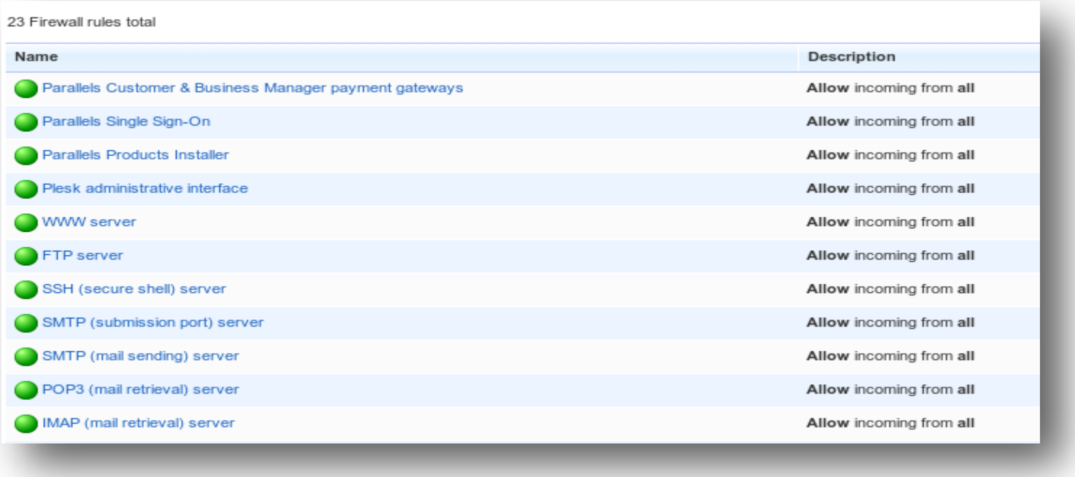
2. Once you have logged in, please click on the Modules option under the Server Management heading as show below. Modules are available only on Linux-based servers. You can use this section to install or manage additional modules that add useful functions to Plesk panel.



3. In the Modules section, you will find the Firewall icon.


Modules
Samba Fileserver Configuration
Firewall
Virtual Private Networking
Products from Parallels Partners

4. Click on the Firewall icon. You will then see a list of predefined firewall rules.



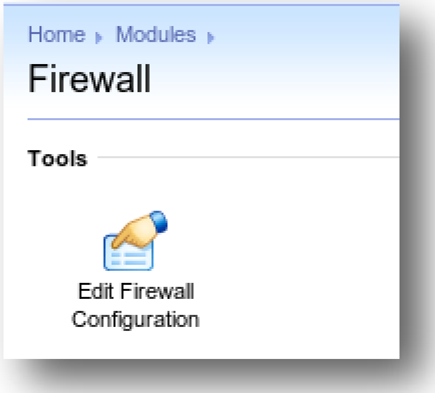
23 Firewall rules total

Name	Description
● Parallels Customer & Business Manager payment gateways	**Allow** incoming from **all**
● Parallels Single Sign-On	**Allow** incoming from **all**
● Parallels Products Installer	**Allow** incoming from **all**
● Plesk administrative interface	**Allow** incoming from **all**
● WWW server	**Allow** incoming from **all**
● FTP server	**Allow** incoming from **all**
● SSH (secure shell) server	**Allow** incoming from **all**
● SMTP (submission port) server	**Allow** incoming from **all**
● SMTP (mail sending) server	**Allow** incoming from **all**
● POP3 (mail retrieval) server	**Allow** incoming from **all**
● IMAP (mail retrieval) server	**Allow** incoming from **all**

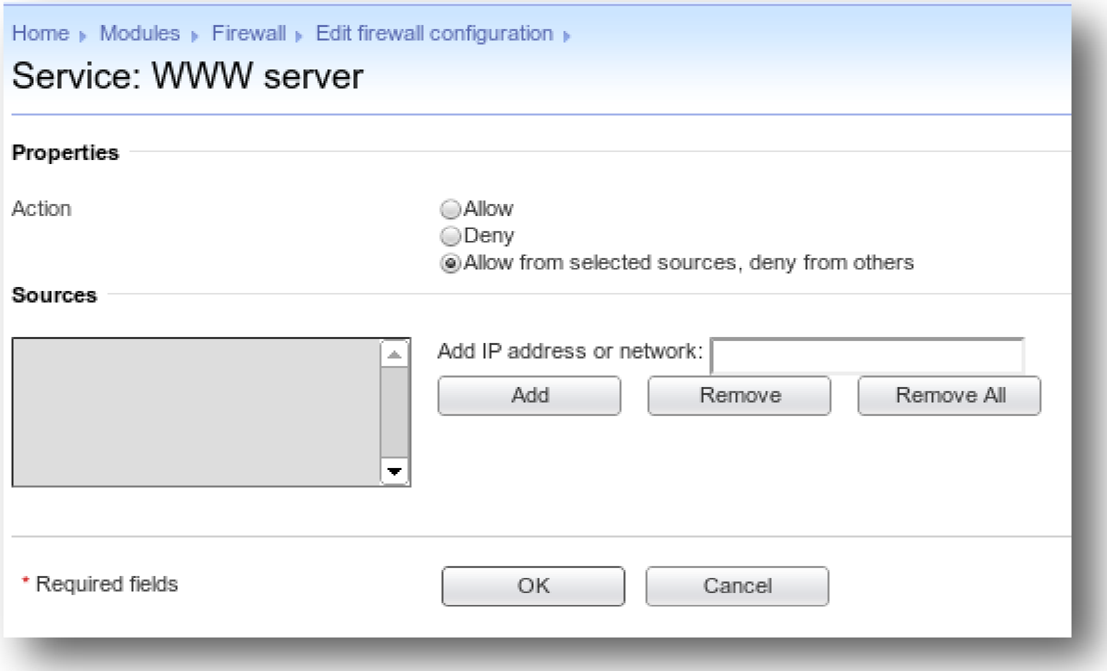
Allow or Restrict Access to a Service

For each system service, you can choose whether to allow or deny all incoming connections or allow only connections from a specific IP/network address.

1. Login to your Plesk panel. Go to the Modules section and click on the Firewall icon. Now click on the Edit Firewall Configuration icon.



2. To edit an existing system service rule, click on the service name you want to edit and you will find options to Allow, Deny, or Allow from selected sources, deny from others. You can make the necessary modification and click on OK to finish the process.



Service: WWW server

Properties

Action
○ Allow
○ Deny
● Allow from selected sources, deny from others

Sources

Add IP address or network:

* Required fields

Manage System Policies

System policies define what is done with all incoming, outgoing, and transit communications that do not match the rules defined. You can find these system policies displayed at the bottom of the list of rules.

1. To view these policies, go to Modules and click on the Firewall icon. Then click on the Edit Firewall Configuration icon. Scroll to the bottom of the page and you will see the system policies.

2. Click on the icon to the left of the policy name you want to change. If the policy is set to Allow all connections, clicking on this icon will deny all connections and vice versa.

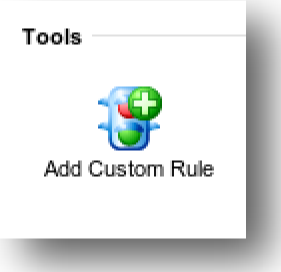
3. To apply the changes, click Activate, and then click Activate again.

Adding Custom Rules

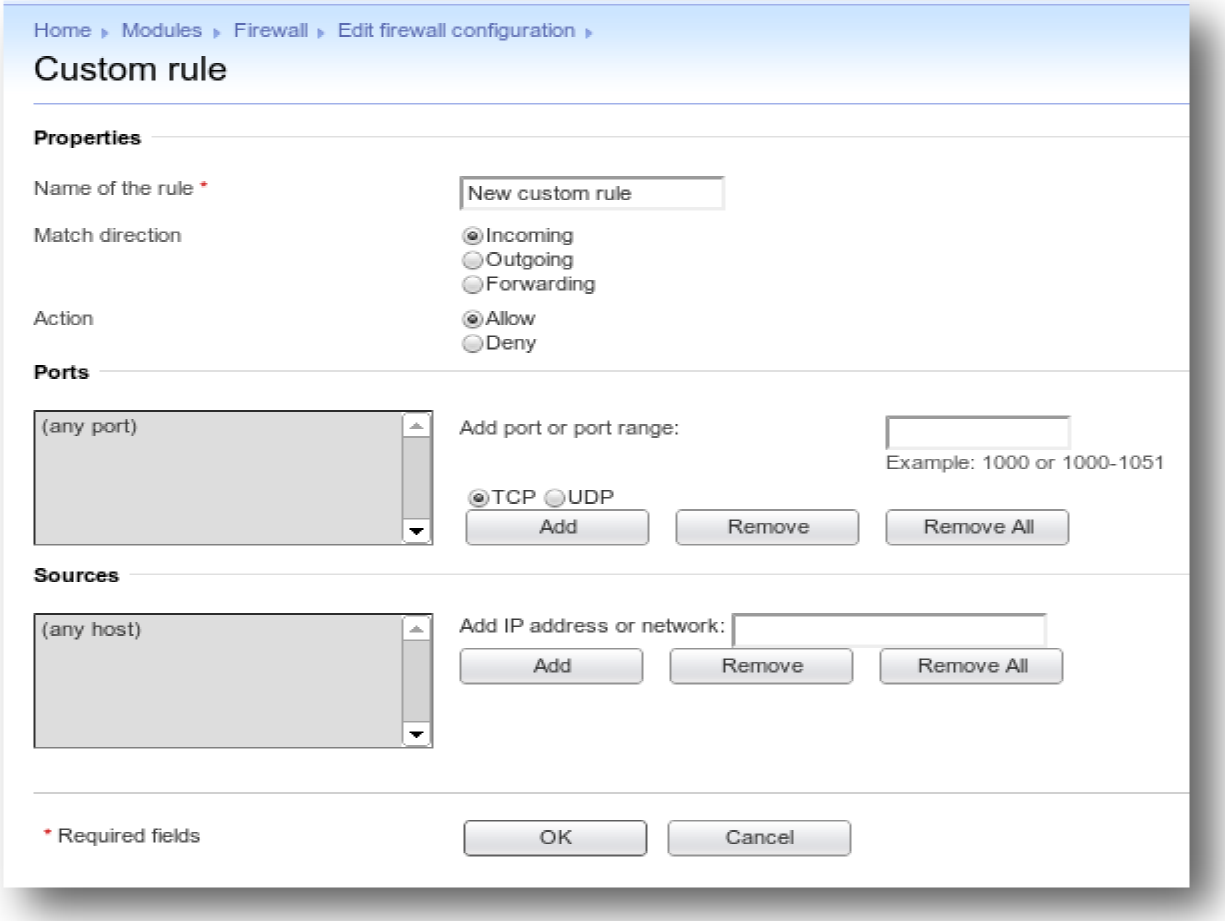
This section describes how you can create a custom rule for your firewall.

1. Once inside the Plesk control panel, click on Modules and then click on the Firewall icon.

2. Now click on the Edit Firewall Configuration icon. You will find another icon called Add Custom Rule; please click on this icon.



3. Specify the rule name, direction, action, and port. Then click on OK.


Home ▸ Modules ▸ Firewall ▸ Edit firewall configuration ▸

Custom rule

Properties

Name of the rule *: New custom rule

Match direction: ● Incoming ○ Outgoing ○ Forwarding

Action: ● Allow ○ Deny

Ports

(any port)

Add port or port range:

Example: 1000 or 1000-1051

● TCP ○ UDP

Sources

(any host)

Add IP address or network:

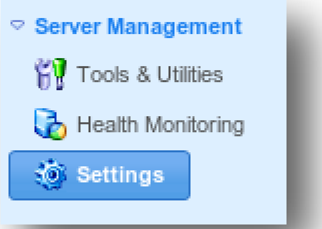
* Required fields

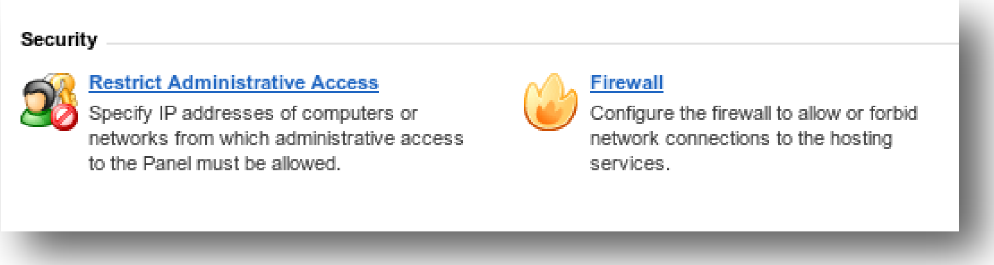
4. Click on Activate, and then click on Activate again.

Windows-based Plesk Firewall

Other than using Windows Firewall with Advanced Security to manage your server firewall inside your Window 2008 server, you can also use your Plesk control panel to configure your firewall rules. Configuring a firewall for a specific network interface is only available on a Windows 2003 server. For a Windows 2008 server, you will have to use the Firewall Rules tab to create or manage firewall rules.

1. Log into your Plesk control panel with your Plesk login link. It will usually follow this format: https://youriphere:8443. This will bring up the Plesk login page.
2. Once logged in, you will then need to click on the Settings option under the Server Management heading. Next, in the Security section, you will find a Firewall option.




Security

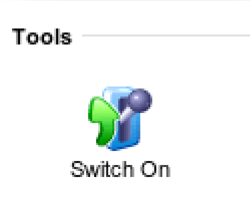
Restrict Administrative Access

Specify IP addresses of computers or networks from which administrative access to the Panel must be allowed.

Firewall

Configure the firewall to allow or forbid network connections to the hosting services.

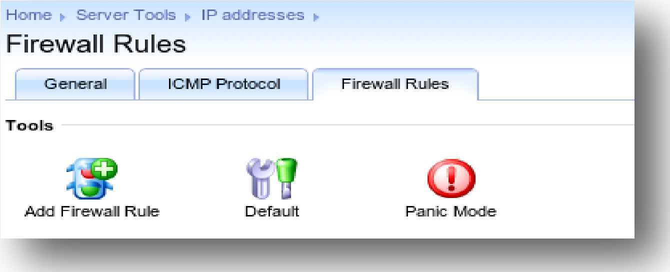
3. In the Tools section, click on the Switch On icon.



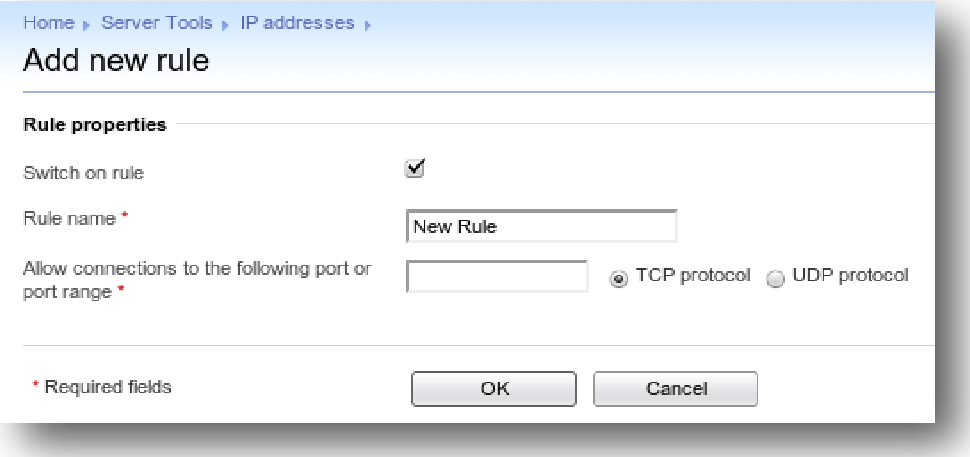
Create New Firewall Rule

Now that you have turned on the firewall, you can create additional firewall rules.

1. Click on the Firewall Rules tab and then click on the Add Firewall Rule icon.



2. Specify the rule name, the port number, and the protocol for which the incoming connection must be allowed.



Add new rule

Rule properties

Switch on rule ☑

Rule name * New Rule

Allow connections to the following port or port range * ● TCP protocol ○ UDP protocol

* Required fields

Note that the tab next to the Firewall Rule tab, ICMP Protocol, is used for network troubleshooting purposes. The predefined rules created for ICMP communications are listed there. You can create rules to block or allow the packets that match the rule.

Conclusion

Now that you know how to manage your firewall using your Plesk panel, you can create custom firewall rules. Apart from using Plesk to manage your firewall, you can use in-built server tools to manage your firewall. For example, on a Windows 2008 server you can use the Windows Firewall with Advanced Security tool. In case of Linux, you can create firewall rules using iptables. If you encountered any issues with this guide, please also note that there is additional information available in our Wiki database at http://tobeannounced.com. Finally, we encourage you to contact our technical support team by using our ticket submission engine, or calling us at 1-866-289-5091 with any questions or concerns.