

Configure Basic Firewall Settings on the RV34x Series Router

Objective

The objective of this article is to explain how to configure the Basic Firewall Settings on the RV34x Series Router.

Introduction

The primary objective of a firewall is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A router is considered to be a strong hardware firewall due to functions that allow filtering of inbound data. A network firewall builds a bridge between an internal network that is assumed to be secure and trusted and another network, usually an external internetwork such as the Internet that is assumed not to be secure and untrusted.

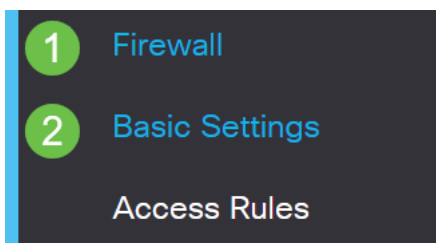
Applicable Devices | Firmware Version

- RV34x Series | 1.0.03.21 ([Download Latest Version](#))

Configure Basic Firewall Settings

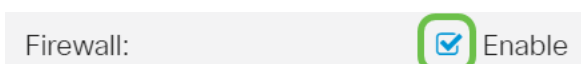
Step 1

Log in to the Web User Interface (UI) and choose **Firewall >Basic Settings**.



Step 2

Check the **Enable** Firewall check box to activate the Firewall feature. This is enabled by default.



Step 3

Check the **Enable** Dos (Denial of Service) check box to secure your network against DoS attacks. This is enabled by default.

Dos (Denial of Service): Enable

Step 4

Check the **Enable** Block WAN Request check box to deny ping requests to the RV34x Series Router. This is enabled by default.

Firewall: Enable

Dos (Denial of Service): Enable

Block WAN Request: Enable

Step 5

In the LAN/VPN Web Management area, check the **HTTP** and/or the **HTTPS** check box to enable traffic from these protocols. For this example, the HTTPS check box is checked.

- HTTP — Hyper Text Transfer Protocol is a data transfer protocol used on the Internet.
- HTTPS — Hyper Text Transfer Protocol Secure is a secure version of HTTP which encrypts packets for increased security.

LAN/VPN Web Management: HTTP 80 (Default: 80, Range: 1025 - 65535)
 HTTPS 443 (Default: 443, Range: 1025 - 65535)

Step 6 (Optional)

Check the **Enable** Remote Web Management check box to enable remote management. Otherwise, skip to Step 8.

Choose the type of protocol used to connect to the firewall by choosing a radio button. The options are **HTTP** and **HTTPS**.

Enter a port number ranging between 1025 to 65535, which remote management is allowed. The default is 443. In this example, 1666 is used.

Remote Web Management: Enable **1**
 HTTP HTTPS **2**
3 Port 1666 (Default: 443, Range: 1025 - 65535)

Step 7

In the Allowed Remote IP Addresses area, choose a radio button to either allow any IP address to access the network remotely or to specify a range of either IPv4 or IPv6 addresses. For this example, an IP Range was chosen. In this example, the starting IP

address is 128.112.59.21 and the ending IP address is 128.112.59.34.

Allowed Remote IP Addresses: Any IP Address

128.112.59.21 to 128.112.59.34 (IPv4 or IPv6 address range)

Step 8 (Optional)

Check the **Enable** SIP ALG check box to enable Session Initiation Protocol (SIP) Application Layer Gateway (ALG) to pass through the Firewall. This feature can be enabled to help SIP packets pass through the firewall. A SIP packet is used to initiate connections of voice traffic. If your VoIP provider uses a different Network Address Translation (NAT) traversal protocol, this feature can be disabled which is the default setting.

Specify the File Transfer Protocol (FTP) port of SIP ALG in the *FTP ALG Port* field. The default is 21.

Check the **Enable** UPnP check box to enable Universal Plug and Play (UPnP). This feature is disabled by default.

For this example, these options are kept disabled.

SIP ALG: 1 Enable

FTP ALG Port: 2

UPnP: 3 Enable

Step 9 (Optional)

Under the Restrict Web Feature area, check the checkboxes of the types of web features to block in the Block area. These checkboxes are disabled by default. The options are:

Java — All web elements containing this type of web element will be blocked. This setting can help prevent Java-based web attacks.

Cookies — Cookies are data that is stored in the computer to help websites understand who is accessing them. Blocking them can prevent malicious cookies from accessing data.

ActiveX — It is a plugin developed by Microsoft to improve a browsing experience. Blocking it can prevent malicious ActiveX plug-ins from harming network devices.

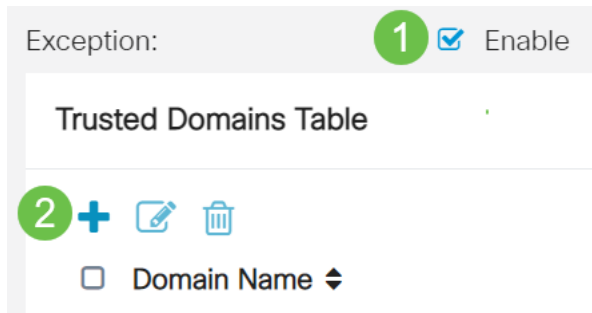
Access to Proxy HTTP Server — HTTP Proxy Servers hide details of end-users from hackers. They work as middlemen so a client does not access the Internet directly. However, if local users have access to WAN proxy servers, they may be able to find a way around the content filters on the router to access Internet sites blocked by the router.

For this example, the checkboxes are left disabled.

Step 11 (Optional)



Check the **Enable** Exception check box to allow only selected web features such as Java, Cookies, ActiveX, or Access to HTTP Proxy Servers and restrict all others. This is disabled by default. For this example, it is left disabled.

In the Trusted Domains Table, click the **add icon** to add domains that are trusted or permitted to access on the network.



Exception: 1 Enable

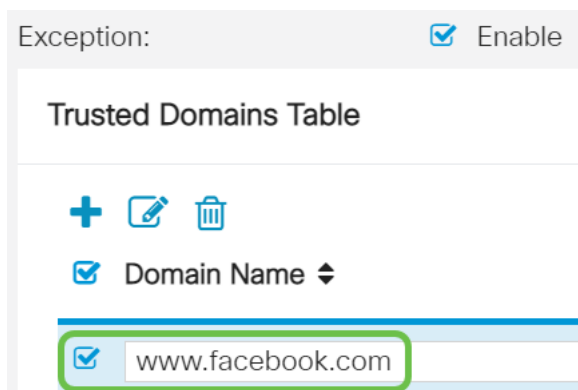
Trusted Domains Table

2 +  

Domain Name ⇅



Step 12

In the *Domain Name* field, enter a domain name to be granted access to the network. For this example, www.facebook.com is used.



Exception: Enable

Trusted Domains Table

+  

Domain Name ⇅

www.facebook.com

Step 13

Click **Apply**.



Apply Cancel

Step 14 (Optional)

To save the configuration permanently, go to the Copy/Save Configuration page or click the **save icon** at the upper portion of the page.



Conclusion

You should now have successfully configured the Basic Firewall Settings on your

RV34x Series Router.