Basic Firewall Configuration on the CVR100W VPN Router

Objective

A firewall is a set of features designed to keep a network secure. A router is considered a strong hardware firewall. This is due to the fact that routers are able to inspect all inbound traffic and drop any unwanted packets. This article explains how to configure basic firewall settings on the CVR100W VPN Router.

Applicable Device

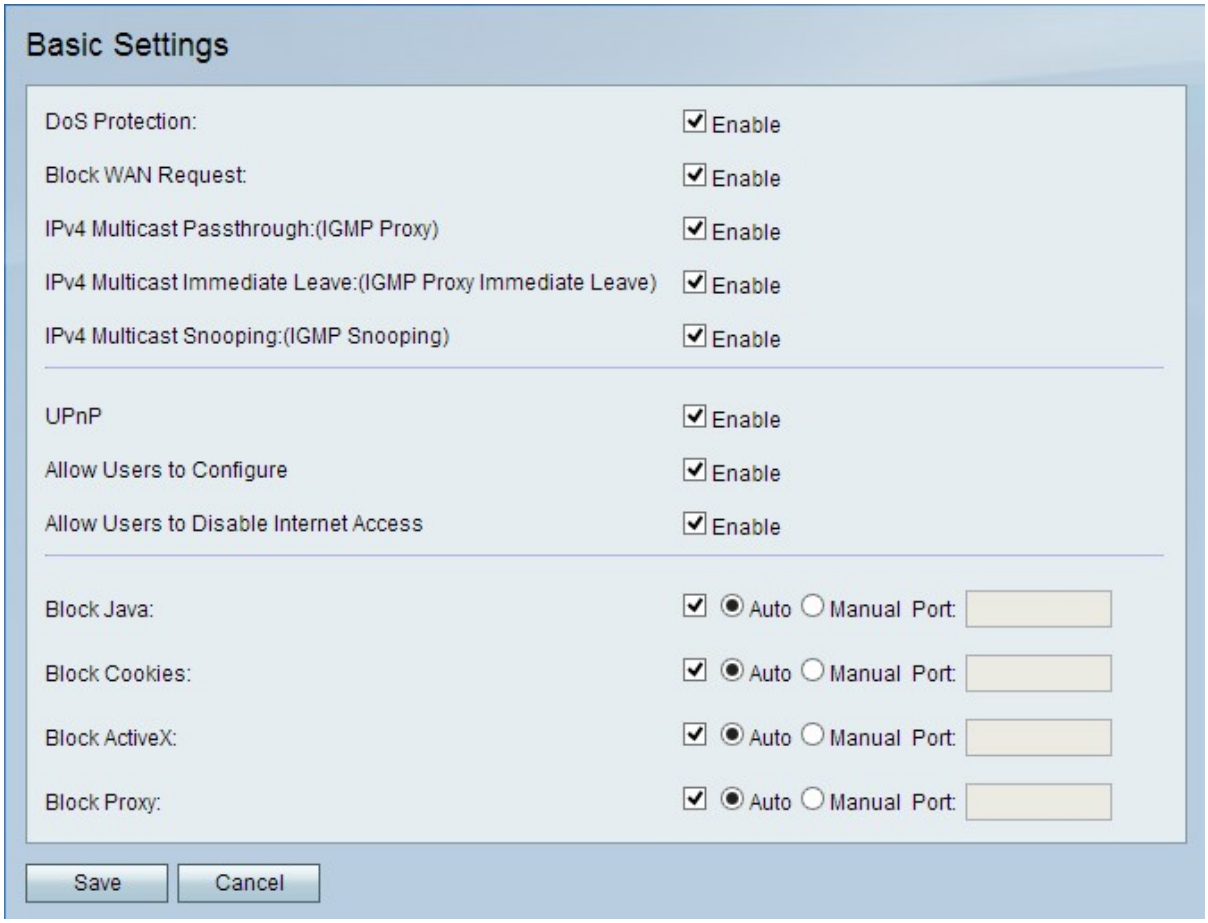
- CVR100W

Software Version

- 1.0.1.19

Basic Firewall Configuration

Step 1. Log in to the web configuration utility and choose **Firewall > Basic Settings**. The *Basic Settings* page opens:



Note: Steps 2 to 13 are optional. You can configure these options based on your needs.

Step 2. In order to enable Denial of Service (DoS) protection on the CVR100W, check **Enable** in the DoS Protection field. DoS protection is used to prevent a network from a Distributed Denial of Service (DDoS) attack. DDoS attacks are meant to flood a network to the point where the resources of the network become unavailable. The CVR100W uses DoS protection to protect the network through the restriction and removal of unwanted packets.

Step 3. In order to block all ping requests to the CVR100W from the WAN, check **Enable** in the Block WAN Request field.

Step 4. In order to allow IPv4 multicast traffic to come through the CVR100W from the Internet, check **Enable** in the IPv4 Multicast Passthrough field. IP multicast is a method that is used to send IP datagrams to a designated group of receivers in a single transmission.

Step 5. IGMP proxy is a way for the router to interact with other devices using IGMP messaging. Immediate Leave enables the CVR100W to leave the multicast group at optimal speed. To enable IGMP Proxy Immediate Leave, check **Enable** in the IPv4 Multicast Immediate Leave field.

Step 6. In order to enable IGMP Snooping which allows other switches on the network to listen into the messages going back and forth between the computer and the CVR100W, check **Enable** in the IPv4 Multicast Snooping field.

Step 7. In order to enable Universal Plug and Play (UPnP), check **Enable** in the UPnP field. UPnP allows for automatic discovery of devices that can communicate with the CVR100W.

Step 8. In order to allow users with UPnP capable devices to configure UPnP port-mapping rules, check **Enable** in the Allow Users to Configure field. Port-mapping or port forwarding is used to permit communications between external hosts and services provided within a private LAN.

Step 9. In order to allow users to disable Internet access to the device, check **Enable** in the Allow Users to Disable Internet Access field.

Step 10. In order to block java applets from being downloaded, check **Block Java** in the Block Java field. Java applets that are made for malicious intent can pose a security threat to a network. Once downloaded, a hostile java applet can exploit network resources. Click the radio button that corresponds to the desired block method.

- Auto — Automatically blocks java.
- Manual Port — Enter a specific port on which to block java.

Step 11. If you do not want a website to create cookies, check **Block Cookies** in the Block Cookies field. Cookies are created by websites to store information of these users. Cookies can track the web history of the user which may lead to an invasion of privacy. Click the radio button that corresponds to the desired block method.

- Auto — Automatically block cookies.
- Manual Port — Enter a specific port on which to block cookies.

Step 12. In order to block ActiveX applets from being downloaded, check **Block ActiveX** in the Block ActiveX field. ActiveX is a type of applet that lacks security. Once an ActiveX applet is installed on a computer, it can do anything a user can do. It may insert harmful code into the operating system, surf a secure intranet, change a password, or retrieve and

send documents. Click the radio button that corresponds to the desired block method.

- Auto — Automatically block ActiveX.
- Manual Port — Enter a specific port on which to block ActiveX.

Step 13. In order to block proxy servers, check **Block Proxy** in the Block Proxy field. Proxy servers are servers that provide a link between two separate networks. Malicious proxy servers can record any unencrypted data that is sent to them such as logins or passwords. Click the radio button that corresponds to the desired block method.

- Auto — Automatically block proxy servers.
- Manual Port — Enter a specific port on which to block proxy servers.

Step 14. Click **Save** to save any changes you made.