

Grundlegende Firewall-Konfiguration des CVR100W VPN-Routers

Ziel

Eine Firewall ist ein Funktionssatz, der die Sicherheit des Netzwerks gewährleistet. Ein Router gilt als starke Hardware-Firewall. Dies liegt daran, dass Router den gesamten eingehenden Datenverkehr überprüfen und unerwünschte Pakete verwerfen können. In diesem Artikel wird erläutert, wie Sie grundlegende Firewall-Einstellungen auf dem CVR100W VPN-Router konfigurieren.

Anwendbares Gerät

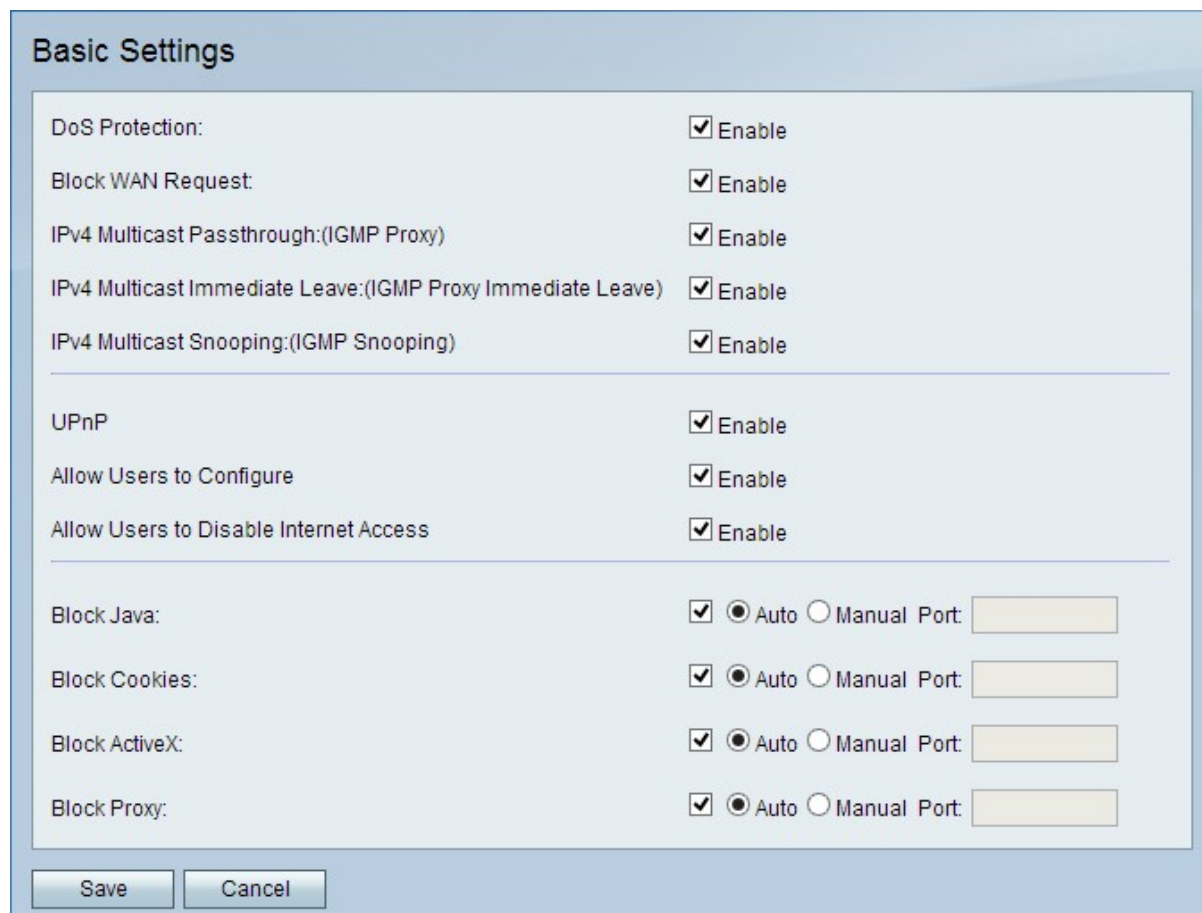
CVR100W

Softwareversion

·1.0.1.19

Grundlegende Firewall-Konfiguration

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Firewall > Basic Settings (Firewall > Grundeinstellungen)**. Die Seite *Grundeinstellungen* wird geöffnet:



The screenshot displays the 'Basic Settings' configuration page. It contains several sections of settings:

- DoS Protection:** Enable
- Block WAN Request:** Enable
- IPv4 Multicast Passthrough:(IGMP Proxy)** Enable
- IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)** Enable
- IPv4 Multicast Snooping:(IGMP Snooping)** Enable

- UPnP** Enable
- Allow Users to Configure** Enable
- Allow Users to Disable Internet Access** Enable

- Block Java:** Auto Manual Port:
- Block Cookies:** Auto Manual Port:
- Block ActiveX:** Auto Manual Port:
- Block Proxy:** Auto Manual Port:

At the bottom of the page, there are two buttons: 'Save' and 'Cancel'.

Hinweis: Die Schritte 2 bis 13 sind optional. Sie können diese Optionen auf Basis Ihrer Anforderungen konfigurieren.

Schritt 2: Um den Denial of Service (DoS)-Schutz auf dem CVR100W zu aktivieren, aktivieren Sie im Feld DoS Protection (DoS-Schutz) die Option **Enable (Aktivieren)**. Der DoS-Schutz dient dazu, ein Netzwerk vor DDoS-Angriffen (Distributed Denial of Service) zu schützen. DDoS-Angriffe sollen ein Netzwerk so weit überfluten, dass die Ressourcen des Netzwerks nicht mehr verfügbar sind. Der CVR100W nutzt den DoS-Schutz, um das Netzwerk durch die Beschränkung und Entfernung unerwünschter Pakete zu schützen.

Schritt 3: Um alle Ping-Anfragen an den CVR100W aus dem WAN zu blockieren, aktivieren Sie im Feld "Block WAN Request" (WAN-Anfrage blockieren) die Option **Enable (Aktivieren)**.

Schritt 4: Damit IPv4-Multicast-Datenverkehr vom Internet über den CVR100W übertragen werden kann, aktivieren Sie im Feld IPv4 Multicast Passthrough (IPv4-Multicast-Passthrough) die Option **Aktivieren**. IP-Multicast ist eine Methode, mit der IP-Datagramme an eine bestimmte Gruppe von Empfängern in einer einzigen Übertragung gesendet werden.

Schritt 5: Der IGMP-Proxy bietet dem Router die Möglichkeit, mithilfe von IGMP-Messaging mit anderen Geräten zu interagieren. Beim sofortigen Austritt kann der CVR100W die Multicast-Gruppe mit optimaler Geschwindigkeit verlassen. Um IGMP Proxy Immediate Leave zu aktivieren, aktivieren Sie im Feld IPv4 Multicast Immediate Leave (Sofort verlassen) die **Option Enable (Aktivieren)**.

Schritt 6: Um IGMP-Snooping zu aktivieren, mit dem andere Switches im Netzwerk Nachrichten abhören können, die zwischen dem Computer und dem CVR100W hin und her gesendet werden, aktivieren Sie im Feld IPv4-Multicast-Snooping die Option **Aktivieren**.

Schritt 7: Um Universal Plug and Play (UPnP) zu aktivieren, aktivieren Sie im Feld UPnP die **Option Enable (Aktivieren)**. UPnP ermöglicht die automatische Erkennung von Geräten, die mit dem CVR100W kommunizieren können.

Schritt 8: Damit Benutzer mit UPnP-fähigen Geräten UPnP-Port-Zuordnungsregeln konfigurieren können, aktivieren Sie im Feld "Allow Users to Configure" (Benutzer zum Konfigurieren zulassen) die **Option Enable (Aktivieren)**. Port-Mapping oder Port-Forwarding wird verwendet, um die Kommunikation zwischen externen Hosts und Diensten in einem privaten LAN zu ermöglichen.

Schritt 9: Um Benutzern zu ermöglichen, den Internetzugriff auf dem Gerät zu deaktivieren, aktivieren Sie im Feld "Benutzer zum Deaktivieren des Internetzugangs zulassen" die **Option Aktivieren**.

Schritt 10: Um zu verhindern, dass Java-Applets heruntergeladen werden, aktivieren Sie im Feld Java sperren **das Kontrollkästchen Java** blockieren. Java-Applets, die für böswillige Absichten erstellt werden, können eine Sicherheitsbedrohung für ein Netzwerk darstellen. Nach dem Herunterladen kann ein feindseliges Java-Applet Netzwerkressourcen ausnutzen. Klicken Sie auf das Optionsfeld für die gewünschte Blockmethode.

- Auto (Automatisch): Blockiert automatisch Java.

- Manual Port (Manueller Port) - Geben Sie einen bestimmten Port ein, an dem Java blockiert werden soll.

Schritt 11: Wenn Sie nicht möchten, dass eine Website Cookies erstellt, aktivieren Sie im Feld "Cookies blockieren" die Option **Cookies blockieren**. Cookies werden von Websites

erstellt, um Informationen dieser Benutzer zu speichern. Cookies können die Web-Geschichte des Benutzers verfolgen, was zu einer Verletzung der Privatsphäre führen kann. Klicken Sie auf das Optionsfeld für die gewünschte Blockmethode.

·Auto (Automatisch): Cookies automatisch blockieren.

·Manual Port (Manueller Port) - Geben Sie einen bestimmten Port ein, an dem Cookies blockiert werden sollen.

Schritt 12: Um zu verhindern, dass ActiveX-Applets heruntergeladen werden, aktivieren Sie **ActiveX** im Feld ActiveX blockieren. ActiveX ist ein Applet-Typ, dem es an Sicherheit fehlt. Wenn ein ActiveX-Applet auf einem Computer installiert ist, kann es alles tun, was ein Benutzer kann. Es kann schädlichen Code in das Betriebssystem einfügen, ein sicheres Intranet durchsuchen, ein Kennwort ändern oder Dokumente abrufen und senden. Klicken Sie auf das Optionsfeld für die gewünschte Blockmethode.

·Auto (Automatisch): ActiveX wird automatisch blockiert.

·Manual Port (Manueller Port) - Geben Sie einen bestimmten Port ein, an dem ActiveX blockiert werden soll.

Schritt 13: Um Proxy-Server zu blockieren, aktivieren Sie im Feld **Proxy** sperren die Option **Proxy blockieren**. Proxyserver sind Server, die eine Verbindung zwischen zwei separaten Netzwerken bereitstellen. Böartige Proxy-Server können alle unverschlüsselten Daten aufzeichnen, die an sie gesendet werden, z. B. Anmeldungen oder Kennwörter. Klicken Sie auf das Optionsfeld für die gewünschte Blockmethode.

·Auto (Automatisch): Proxy-Server werden automatisch blockiert.

·Manual Port (Manueller Port) - Geben Sie einen bestimmten Port ein, an dem Proxy-Server blockiert werden sollen.

Schritt 14: Klicken Sie auf **Speichern**, um alle vorgenommenen Änderungen zu speichern.