

Firewall-Konfiguration auf dem RV315W VPN-Router

Ziel

Eine Firewall baut eine Brücke zwischen einem sicheren internen Netzwerk und einem unsicheren externen Netzwerk. Die Firewall steuert die eingehende und ausgehende Analyse des Netzwerkverkehrs von Datenpaketen. In diesem Artikel wird erläutert, wie verschiedene Funktionen wie Proxy, Cookies usw. auf dem RV315W VPN-Router blockiert werden.

Anwendbares Gerät

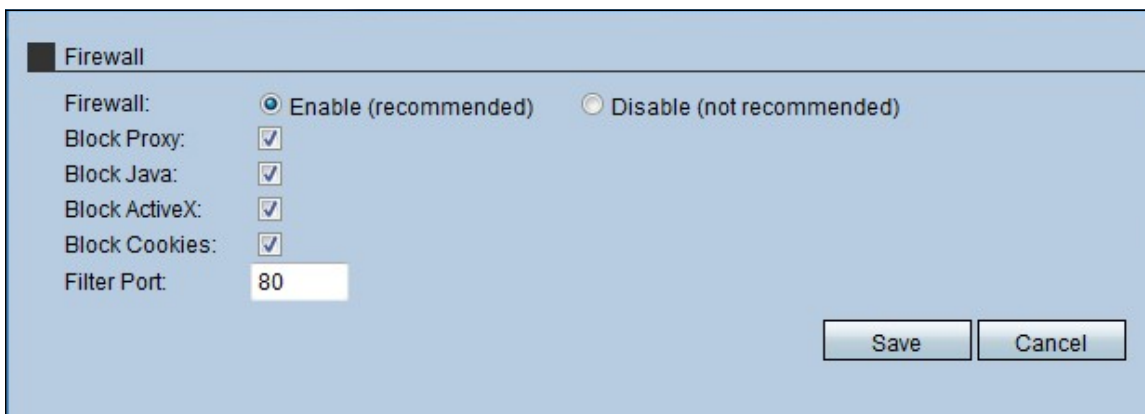
RV315W

Softwareversion

·1.01.03

Firewall-Konfiguration

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > Firewall aus**. Die Seite *Firewall* wird geöffnet:



Schritt 2: Klicken Sie auf das **Optionsfeld Aktivieren**, um die Firewall-Funktionen des RV315W zu aktivieren.

Hinweis: Die Schritte 3 bis 7 sind optionale Schritte.

Schritt 3: Aktivieren Sie das Kontrollkästchen **Proxy blockieren**, um den Proxy auf dem Gerät zu blockieren. Proxyserver sind Server, die eine Verbindung zwischen zwei separaten Netzwerken bereitstellen. Bösertige Proxy-Server können alle unverschlüsselten Daten aufzeichnen, die an sie gesendet werden, z. B. Anmeldungen oder Kennwörter.

Schritt 4: Aktivieren Sie das Kontrollkästchen **Java sperren**, um das Herunterladen der Java-Applets zu verhindern. Java ist eine gängige Programmiersprache, die von vielen Websites verwendet wird. Java-Applets, die aus böswilligen Gründen erstellt wurden, können jedoch eine Sicherheitsbedrohung für ein Netzwerk darstellen. Nach dem Herunterladen kann ein

feindseliges Java-Applet Netzwerkressourcen ausnutzen.

Schritt 5: Aktivieren Sie das Kontrollkästchen **ActiveX blockieren**, um das Herunterladen von ActiveX-Anwendungen zu blockieren. ActiveX ist ein Applet-Typ, der von vielen Websites verwendet wird. Obwohl im Allgemeinen sicher, kann ein böses ActiveX-Applet, sobald es auf einem Computer installiert ist, alle Aktionen ausführen, die ein Benutzer ausführen kann. Es kann schädlichen Code in das Betriebssystem einfügen, ein sicheres Intranet durchsuchen, ein Kennwort ändern oder Dokumente abrufen und senden.

Schritt 6: Aktivieren Sie das Kontrollkästchen **Blockcookies**, um das Herunterladen der Cookies-Anwendungen zu verhindern. Cookies werden von Websites erstellt, um Informationen über Benutzer zu speichern. Cookies können die Web-Geschichte des Benutzers verfolgen, was zu einer Verletzung der Privatsphäre führen kann.

Schritt 7: Geben Sie die Portnummer ein, die das Gerät verwendet, um den HTTP-Datenverkehr im Feld Filter Port (Filter-Port) zu filtern. Diese Datenverkehrssteuerung wird nur für den HTTP-Datenverkehr durchgeführt. HyperText Transfer Protocol (HTTP) wird verwendet, um mithilfe der Verbindung, die der Server und der Host herstellen, auf Informationen im Internet zuzugreifen und diese zu verteilen.

Schritt 8: Klicken Sie auf **Speichern**, um die Änderungen in der Firewall-Konfiguration zu speichern.