Grundlegende Firewall-Konfiguration auf Routern der Serien RV320 und RV325

Ziel

In diesem Artikel wird erläutert, wie Sie die grundlegenden Firewall-Einstellungen für die RV32x VPN Router-Serie konfigurieren.

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. Netzwerk-Firewalls schützen ein internes Computernetzwerk (zu Hause, in der Schule oder im Intranet) vor schädlichem Zugriff von außen. Netzwerk-Firewalls können auch so konfiguriert werden, dass der Zugriff von internen Benutzern auf die Außenwelt eingeschränkt wird.

Anwendbare Geräte

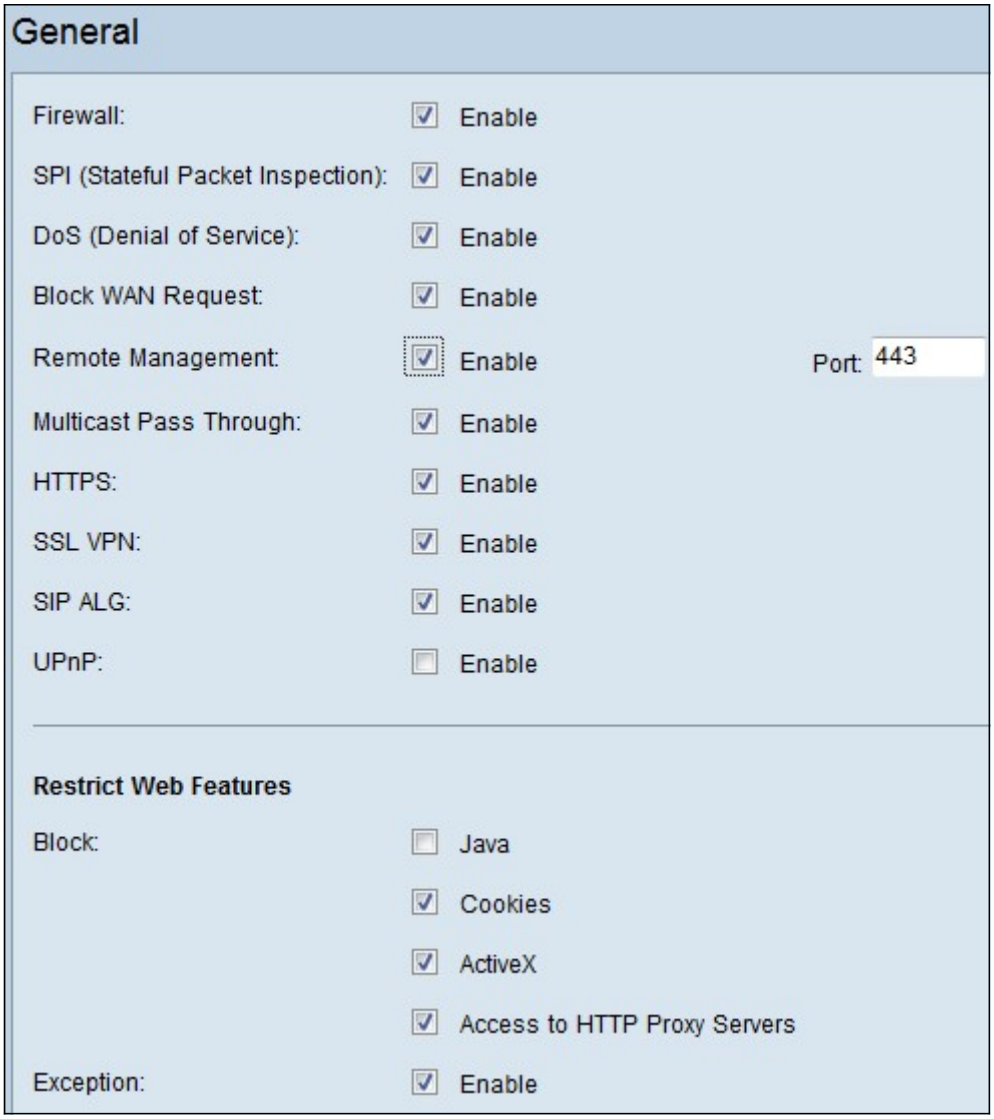
- RV320 Dual-WAN VPN-Router
- RV325 Dual-WAN-VPN-Router mit Gigabit

Softwareversion

- V1.1.0.09

Grundlegende Einstellungen

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



Schritt 2: Aktivieren Sie je nach Ihren Anforderungen das Kontrollkästchen **Aktivieren**, das den zu aktivierenden Funktionen entspricht.

- Firewall - Router-Firewalls können deaktiviert oder aktiviert werden, um bestimmte Arten von Netzwerkverkehr durch so genannte Firewall-Regeln zu filtern. Mithilfe einer Firewall können der gesamte ein- und ausgehende Datenverkehr gefiltert und auf Basis von Firewall-Regeln.
- SPI (Stateful Packet Inspection) - Überwacht den Zustand von Netzwerkverbindungen wie TCP-Streams und UDP-Kommunikation. Die Firewall unterscheidet legitime Pakete für verschiedene Verbindungsarten. Nur Pakete, die mit einer bekannten aktiven Verbindung übereinstimmen, werden von der Firewall zugelassen, alle anderen werden abgelehnt.
- DoS (Denial of Service) - Dient zum Schutz eines Netzwerks vor DDoS-Angriffen (Distributed Denial of Service). DDoS-Angriffe sollen ein Netzwerk so weit überfluten, dass die Ressourcen des Netzwerks nicht mehr verfügbar sind. Der RV320 nutzt den DoS-Schutz, um das Netzwerk durch die Beschränkung und Entfernung unerwünschter Pakete zu schützen.
- WAN-Anfrage blockieren - Blockiert alle Ping-Anfragen an den Router vom WAN-Port.
- Remote Management - Ermöglicht den Zugriff auf den Router über ein Remote-WAN-Netzwerk.
  - Port - Geben Sie eine Portnummer ein, die remote verwaltet werden soll.
- Multicast Pass Through (Multicast-Durchleitung): Ermöglicht die Weiterleitung von IP-Multicast-Nachrichten durch das Gerät.
- HTTPS (Hypertext Transfer Protocol Secure) ist ein Kommunikationsprotokoll für die sichere

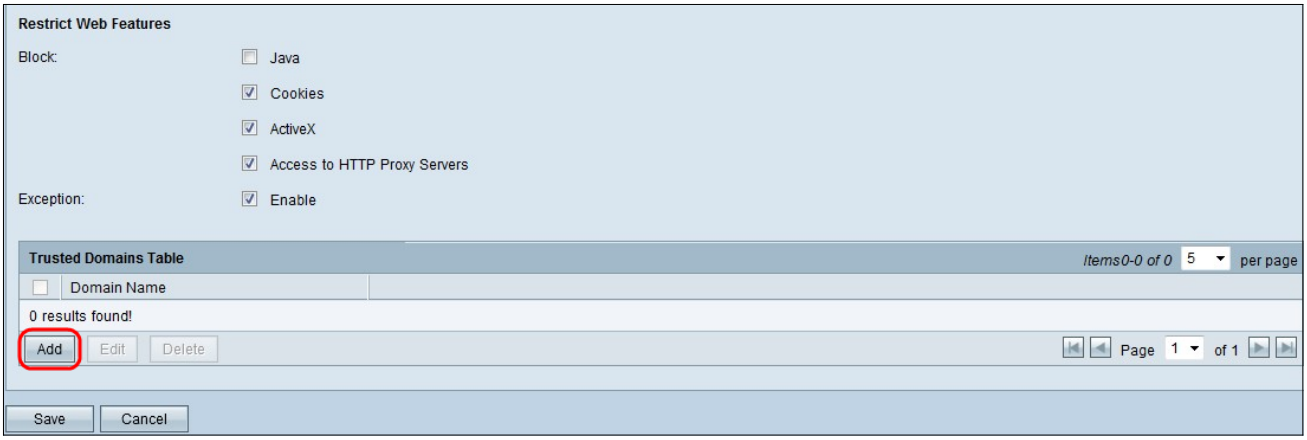
Kommunikation über ein Computernetzwerk. Es bietet bidirektionale Verschlüsselung von Client und Server.
- SSL VPN - Ermöglicht eine SSL VPN-Verbindung, die über den Router hergestellt wird.
- SIP ALG - SIP ALG bietet Funktionen, die Voice-over-IP-Datenverkehr sowohl von der privaten als auch von der öffentlichen und zur privaten Seite der Firewall zulassen, wenn Netzwerkadresse und Port Translation (NAPT) verwendet werden. NAPT ist die häufigste Netzwerkadressenübersetzung.
- UPnP (Universal Plug and Play) - Ermöglicht die automatische Erkennung von Geräten, die mit dem Router kommunizieren können.

Schritt 3: Aktivieren Sie je nach Ihren Anforderungen das Kontrollkästchen **Aktivieren**, das den Funktionen entspricht, die Sie blockieren möchten.

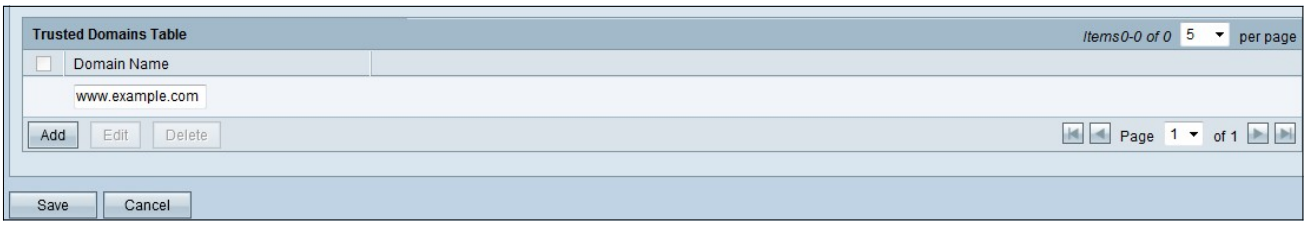
- Java - Wenn Sie dieses Kontrollkästchen aktivieren, werden Java-Applets nicht heruntergeladen und ausgeführt. Java ist eine gängige Programmiersprache, die von vielen Websites verwendet wird. Java-Applets, die aus böswilligen Gründen erstellt wurden, können jedoch eine Sicherheitsbedrohung für ein Netzwerk darstellen. Nach dem Herunterladen kann ein feindseliges Java-Applet Netzwerkressourcen ausnutzen.
- Cookies - 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.
- ActiveX - ActiveX ist eine Art von Applet, das von vielen Websites verwendet wird. Obwohl im Allgemeinen sicher, kann ein bösartiges 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.
- Zugriff auf HTTP-Proxy-Server - Proxy-Server sind Server, die eine Verbindung zwischen zwei separaten Netzwerken bereitstellen. Bösartige Proxy-Server können alle unverschlüsselten Daten aufzeichnen, die an sie gesendet werden, z. B. Anmeldungen oder Kennwörter.
- Ausnahme - Ermöglicht die ausgewählten Funktionen (Java, Cookies, ActiveX oder Zugriff auf HTTP-Proxy-Server), schränkt jedoch alle nicht ausgewählten Funktionen auf konfigurierten vertrauenswürdigen Domänen ein. Eine vertrauenswürdige Domäne, die Zugriff auf das vertrauenswürdige Netzwerk hat. Sie können eine vertrauenswürdige Domäne einrichten, die Benutzern einer externen Domäne den Zugriff auf Ihre Netzwerkressourcen ermöglicht. Wenn diese Option deaktiviert ist, ermöglicht eine vertrauenswürdige Domäne alle Funktionen.

Hinweis: Zeitersparnis: Wenn Sie das Kontrollkästchen Ausnahme nicht aktiviert haben, überspringen Sie Schritt 4.

Schritt 4: Klicken Sie auf Hinzufügen, geben Sie eine neue vertrauenswürdige Domäne ein, und klicken Sie auf Speichern, um eine vertrauenswürdige Domäne zu erstellen.

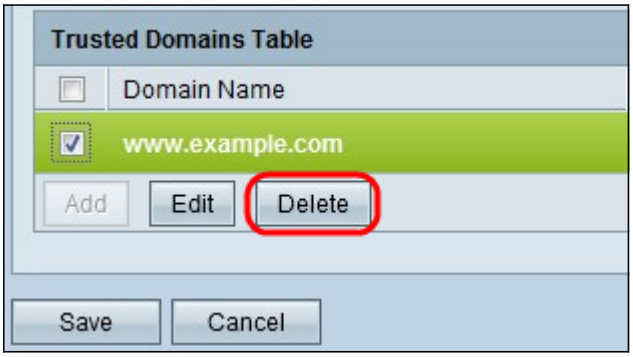


Schritt 5: Klicken Sie auf Speichern, um die Änderungen zu aktualisieren.



Schritt 6: (Optional) Um den Namen der vertrauenswürdigen Domäne zu bearbeiten, aktivieren Sie das Kontrollkästchen der vertrauenswürdigen Domäne, die Sie bearbeiten möchten, und klicken Sie auf Bearbeiten, bearbeiten Sie den Domänennamen, und klicken Sie dann auf Speichern.

Schritt 7: (Optional) Um eine Domäne in der Liste der vertrauenswürdigen Domäne zu löschen, aktivieren Sie das Kontrollkästchen der vertrauenswürdigen Domäne, die Sie löschen möchten, und klicken Sie auf Löschen.



Sehen Sie sich ein Video zu diesem Artikel an..

Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.