Konfigurieren der grundlegenden Firewall-Einstellungen auf dem Router der Serie RV34x

Ziel

In diesem Artikel wird erläutert, wie Sie die grundlegenden Firewall-Einstellungen auf dem Router der Serie RV34x konfigurieren.

Einführung

Das Hauptziel einer Firewall ist die Kontrolle des ein- und ausgehenden Netzwerkverkehrs, indem die Datenpakete analysiert und anhand eines vordefinierten Regelsatzes ermittelt wird, ob sie durchgelassen werden sollen oder nicht. Ein Router gilt aufgrund von Funktionen, die das Filtern eingehender Daten ermöglichen, als starke Hardware-Firewall. Eine Netzwerk-Firewall baut eine Brücke zwischen einem internen Netzwerk, das als sicher und vertrauenswürdig gilt, und einem anderen Netzwerk, in der Regel einem externen Internetwork wie dem Internet, das als nicht sicher und nicht vertrauenswürdig angesehen wird.

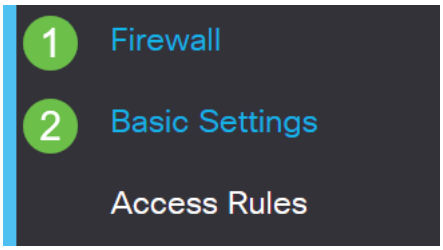
Unterstützte Geräte | Firmware-Version

- Serie RV34x | 1.0.03.21 (aktuelle Version herunterladen)

Konfigurieren der grundlegenden Firewall-Einstellungen

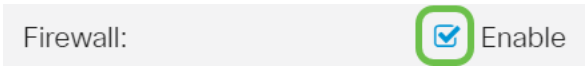
Schritt 1

Melden Sie sich bei der Webbenutzeroberfläche an, und wählen Sie **Firewall >Grundeinstellungen aus**.



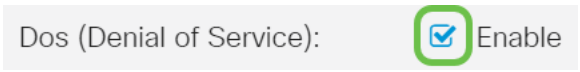
Schritt 2

Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Firewall-Funktion zu aktivieren. Dies ist standardmäßig aktiviert.



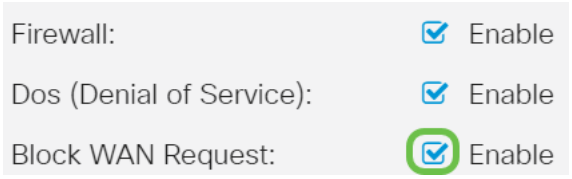
Schritt 3

Aktivieren Sie das Kontrollkästchen **Enable** Dos (Denial of Service), um Ihr Netzwerk vor DoS-Angriffen zu schützen. Dies ist standardmäßig aktiviert.



Schritt 4

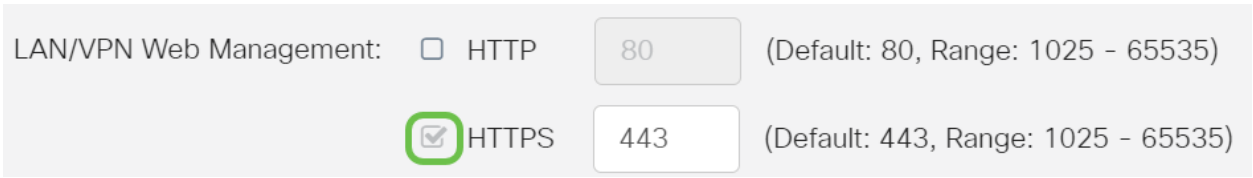
Aktivieren Sie das Kontrollkästchen **Enable** WAN Request, um Ping-Anfragen an den Router der Serie RV34x zu verweigern. Dies ist standardmäßig aktiviert.



Schritt 5

Aktivieren Sie im Bereich LAN/VPN-Webverwaltung das Kontrollkästchen **HTTP** und/oder **HTTPS**, um Datenverkehr aus diesen Protokollen zu aktivieren. In diesem Beispiel ist das Kontrollkästchen HTTPS aktiviert.

- HTTP - Hyper Text Transfer Protocol ist ein Datenübertragungsprotokoll, das im Internet verwendet wird.
- HTTPS - Hyper Text Transfer Protocol Secure ist eine sichere Version von HTTP, die Pakete zur Erhöhung der Sicherheit verschlüsselt.

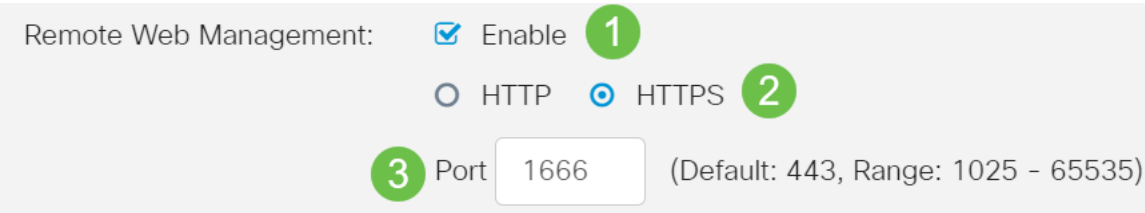


Schritt 6 (optional)

Aktivieren Sie das Kontrollkästchen **Enable Remote** Web Management (Remote-Webverwaltung aktivieren), um die Remoteverwaltung zu aktivieren. Fahren Sie andernfalls mit Schritt 8 fort.

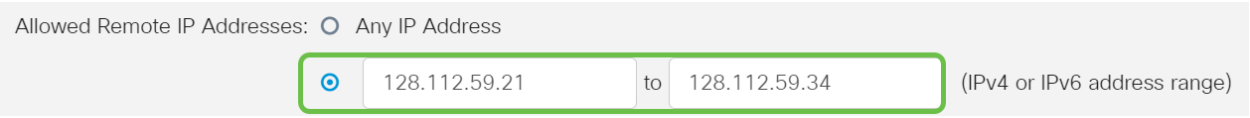
Wählen Sie den Protokolltyp aus, der für die Verbindung mit der Firewall verwendet wird, indem Sie ein Optionsfeld auswählen. Die Optionen sind **HTTP** und **HTTPS**.

Geben Sie eine Portnummer zwischen 1025 und 65535 ein, die für die Remote-Verwaltung zulässig ist. Der Standardwert ist 443. In diesem Beispiel wird 1666 verwendet.



Schritt 7

Wählen Sie im Bereich Zugelassene Remote-IP-Adressen ein Optionsfeld, um entweder eine beliebige IP-Adresse für den Remote-Zugriff auf das Netzwerk zuzulassen oder einen Bereich von IPv4- oder IPv6-Adressen anzugeben. Für dieses Beispiel wurde ein IP-Bereich ausgewählt. In diesem Beispiel ist die Start-IP-Adresse 128.112.59.21 und die End-IP-Adresse 128.112.59.34.



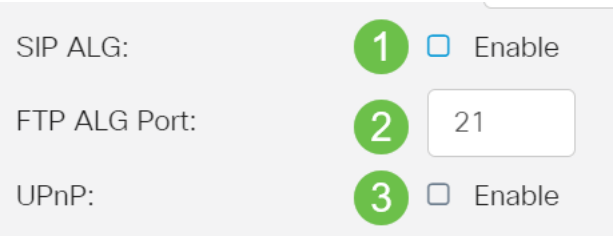
Schritt 8 (optional)

Aktivieren Sie das Kontrollkästchen **SIP-**ALG **aktivieren**, um das Durchlaufen des Session Initiation Protocol (SIP) Application Layer Gateway (ALG) durch die Firewall zu aktivieren. Diese Funktion kann aktiviert werden, damit SIP-Pakete die Firewall passieren können. Ein SIP-Paket wird verwendet, um Verbindungen des Sprachdatenverkehrs zu initiieren. Wenn Ihr VoIP-Anbieter ein anderes NAT-Traversal-Protokoll (Network Address Translation) verwendet, kann diese Funktion deaktiviert werden. Dies ist die Standardeinstellung.

Geben Sie den FTP-Port (File Transfer Protocol) von SIP ALG im Feld *FTP-ALG-Port an*. Der Standardwert ist 21.

Aktivieren Sie das Kontrollkästchen **Enable** UPnP (UPnP aktivieren), um Universal Plug and Play (UPnP) zu aktivieren. Diese Funktion ist standardmäßig deaktiviert.

In diesem Beispiel werden diese Optionen deaktiviert beibehalten.



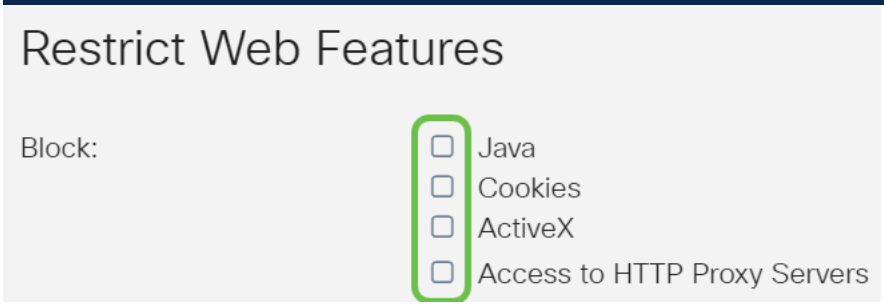
Schritt 9 (optional)

Aktivieren Sie im Bereich Web-Feature einschränken die Kontrollkästchen der Arten von Webfunktionen, die im Bereich Sperren blockiert werden sollen. Diese Kontrollkästchen sind standardmäßig deaktiviert. Folgende Optionen sind verfügbar:

Java - Alle Web-Elemente, die diesen Typ von Web-Element enthalten, werden blockiert. Diese Einstellung kann dazu beitragen, Java-basierte Webangriffe zu verhindern.

Cookies - Cookies sind Daten, die im Computer gespeichert werden, um Websites zu helfen, zu verstehen, wer auf sie zugreift. Blockieren von Cookies kann den Zugriff auf Daten durch schädliche Cookies verhindern.
ActiveX — Es ist ein Plugin, das von Microsoft entwickelt wurde, um das Surfen zu verbessern. Das Blockieren kann verhindern, dass Netzwerkgeräte durch schädliche ActiveX-Plug-Ins beschädigt werden.
Zugriff auf den Proxy-HTTP-Server - HTTP-Proxy-Server verbergen Details von Endbenutzern vor Hackern. Sie arbeiten als Mittelsmänner, sodass ein Kunde nicht direkt auf das Internet zugreift. Wenn lokale Benutzer jedoch Zugriff auf WAN-Proxy-Server haben, können sie möglicherweise einen Weg finden, um die Content-Filter auf dem Router zu umgehen, um auf vom Router blockierte Websites im Internet zuzugreifen.

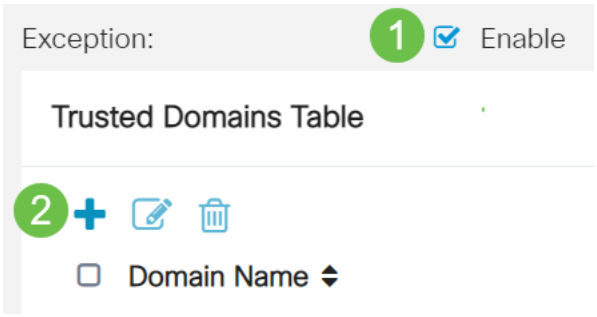
In diesem Beispiel sind die Kontrollkästchen deaktiviert.



Schritt 11 (optional)

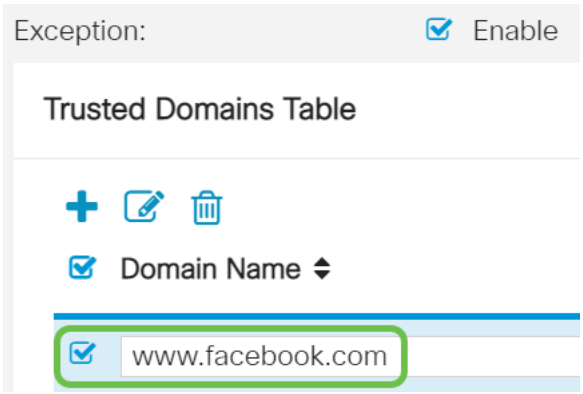
Aktivieren Sie das Kontrollkästchen **Enable** Exception (Ausnahme aktivieren), um nur bestimmte Webfunktionen wie Java, Cookies, ActiveX oder Zugriff auf HTTP-Proxy-Server zuzulassen und alle anderen einzuschränken. Dies ist standardmäßig deaktiviert. In diesem Beispiel ist es deaktiviert.

Klicken Sie in der Tabelle Trusted Domains (Vertrauenswürdige Domänen) auf das **Symbol Add (Hinzufügen)**, um Domänen hinzuzufügen, die vertrauenswürdig sind oder auf das Netzwerk zugreifen dürfen.



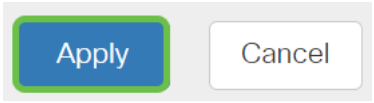
Schritt 12

Geben Sie im Feld *Domänenname* einen Domänennamen ein, dem der Zugriff auf das Netzwerk gewährt werden soll. In diesem Beispiel wird www.facebook.com verwendet.



Schritt 13

Klicken Sie auf Apply (Anwenden).



Schritt 14 (optional)

Um die Konfiguration dauerhaft zu speichern, rufen Sie die Seite "Copy/Save Configuration" (Konfiguration kopieren/speichern) auf, oder klicken Sie auf das **Speichersymbol** oben auf der Seite.

Fazit

Sie sollten jetzt die grundlegenden Firewall-Einstellungen auf Ihrem Router der Serie RV34x erfolgreich konfiguriert haben.