So konfigurieren Sie grundlegende Firewall-Einstellungen für den RV130 und den RV130W

Ziel

Die grundlegenden Firewall-Einstellungen schützen Ihr Netzwerk, indem Regeln erstellt und angewendet werden, die vom Gerät verwendet werden, um eingehenden und ausgehenden Internetdatenverkehr selektiv zu blockieren und zuzulassen.
Funktionen wie Universal Plug and Play erleichtern die Verbindung von Geräten untereinander im Netzwerk, ohne dass zusätzliche Konfigurationen erforderlich sind.

UPnP (Universal Plug and Play) ermöglicht die automatische Erkennung von Geräten, die mit dem Gerät kommunizieren können. Das Blockieren von Inhalten kann zum Schutz Ihres Computers beitragen, da bestimmte Inhalte an Ihr Gerät gesendet werden können, die die Sicherheit gefährden oder Ihren Computer mit bösartiger Software infizieren können. Die Möglichkeit, bestimmte Inhalte an den Ports Ihrer Wahl zu blockieren, ist für eine höhere Firewall-Sicherheit von Vorteil.

In diesem Dokument wird erläutert, wie Sie die grundlegenden Firewall-Einstellungen für den RV130 und den RV130W konfigurieren.

Unterstützte Geräte

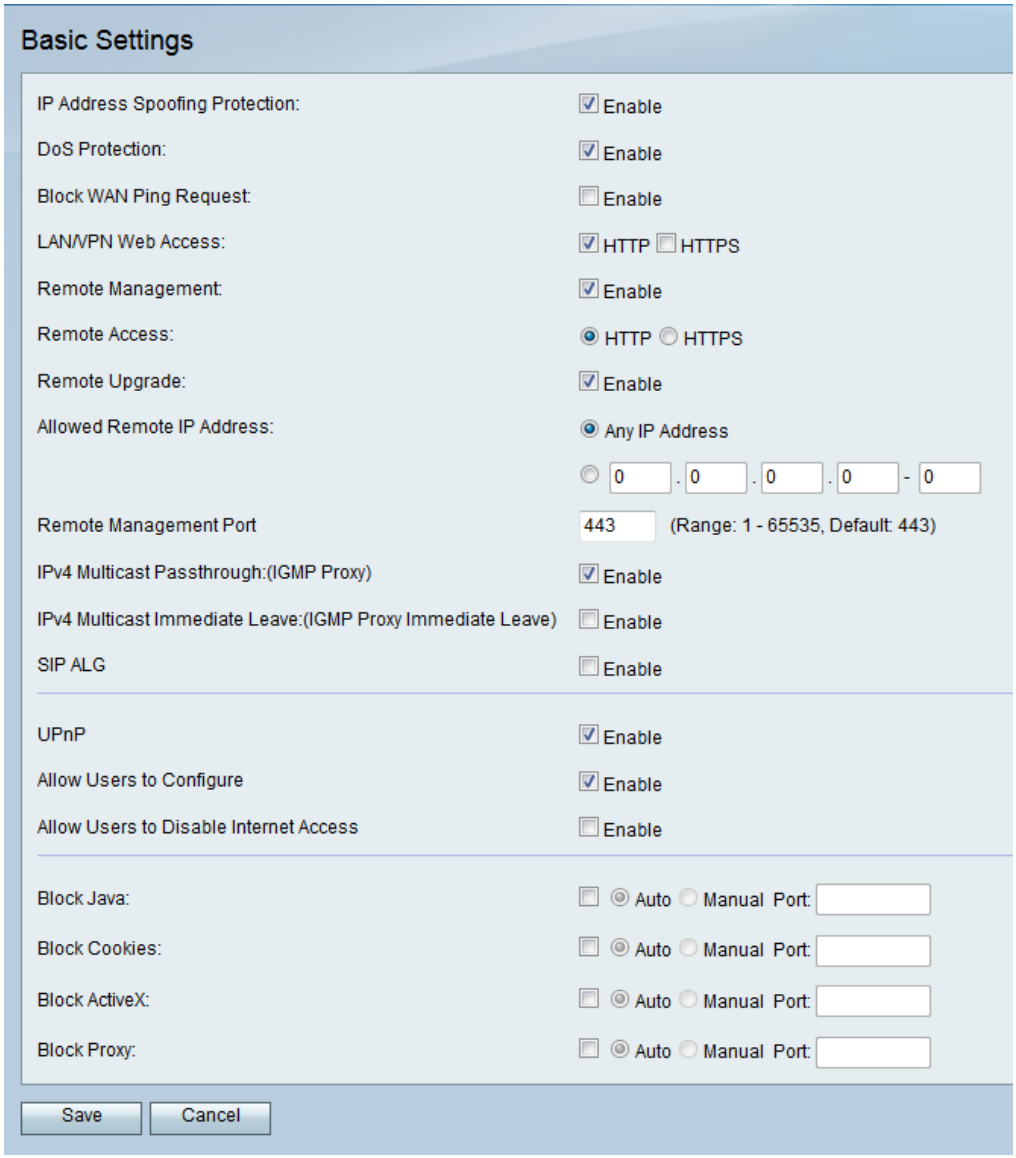
- RV130
- RV130W

Software-Version

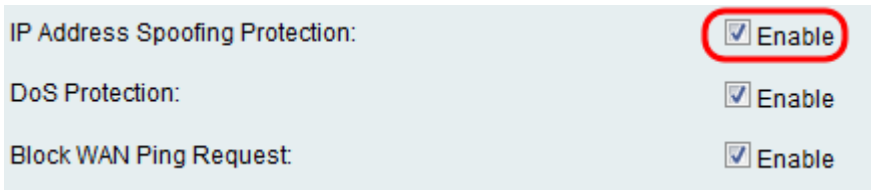
- v1.0.1.3

Konfigurieren der grundlegenden Firewall-Einstellungen

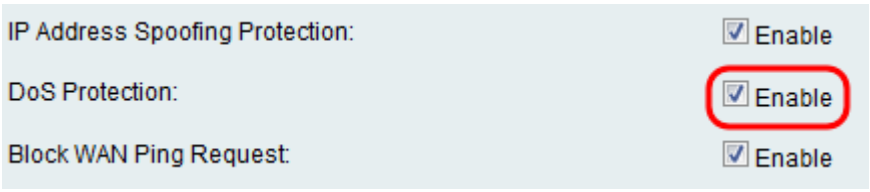
Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Firewall > Basic Settings**. Die Seite Grundeinstellungen wird geöffnet:



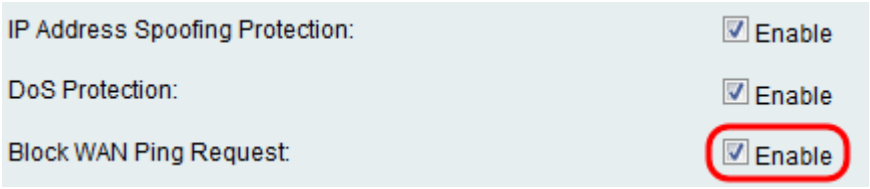
Schritt 2: Aktivieren Sie im Feld *IP Address Spoofing Protection* das Kontrollkästchen **Enable (Aktivieren)**, um Ihr Netzwerk vor IP Address Spoofing zu schützen. IP-Adressen-Spoofing ist der Fall, wenn ein nicht autorisierter Benutzer versucht, Zugriff auf ein Netzwerk zu erhalten, indem er die Identität eines anderen vertrauenswürdigen Geräts annimmt, das seine eigene IP-Adresse verwendet. Es wird empfohlen, *Schutz vor Spoofing von IP-Adressen.*



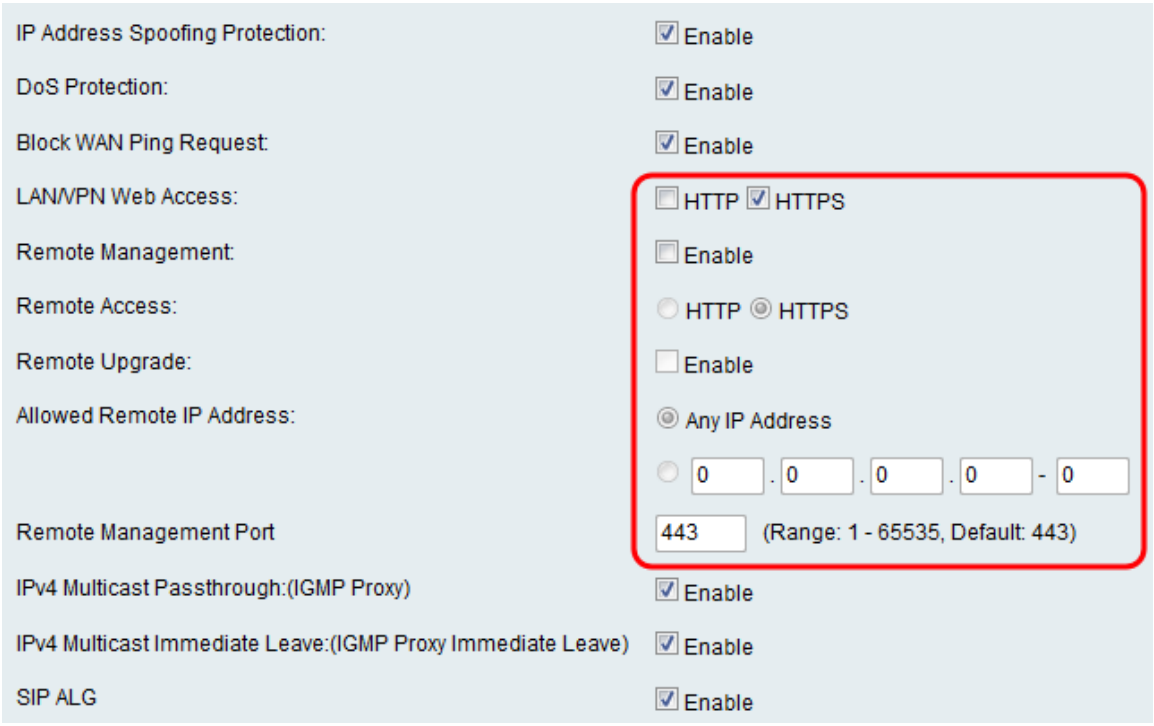
Schritt 3: Aktivieren Sie im Feld *DoS-Schutz* das Kontrollkästchen **Aktivieren**, um Ihr Netzwerk vor Denial-of-Service-Angriffen zu schützen. Der Denial of Service-Schutz wird verwendet, um ein Netzwerk vor einem Distributed Denial of Service (DDoS)-Angriff zu schützen. DDoS-Angriffe sollen ein Netzwerk so weit fluten, dass die Ressourcen des Netzwerks nicht mehr verfügbar sind.



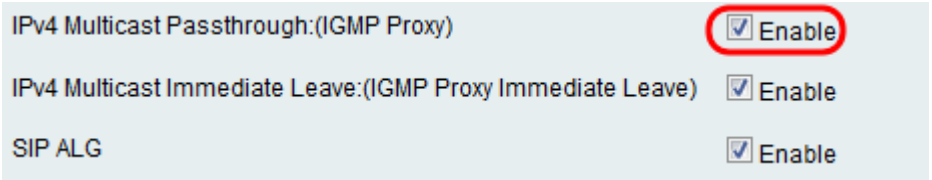
Schritt 4: Aktivieren Sie im Feld *Block WAN Ping Request* (*WAN-Ping-Anforderung blockieren)* das Kontrollkästchen **Enable (Aktivieren)**, um das Ping von Anforderungen an Ihr Gerät vom externen WAN-Netzwerk zu stoppen.



Schritt 5: Die aufgeführten Felder von *LAN/VPN-Webzugriff bis Remote-Management-Port* werden zum Konfigurieren von LAN und Remote-Management-Webzugriff verwendet. Weitere Informationen zu diesen Konfigurationen finden Sie unter Configuration of LAN and Remote Management Web Access on the RV130 and RV130W.

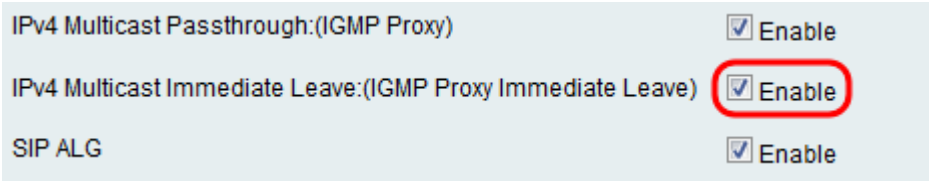


Schritt 6. Aktivieren Sie im Feld *IPv4 Multicast Passthrough:(IGMP Proxy)* das Kontrollkästchen **Enable (Aktivieren)**, um das Multicast Passthrough für IPv4 zu aktivieren. Dadurch werden IGMP-Pakete aus dem externen WAN-Netzwerk an Ihr internes LAN weitergeleitet.

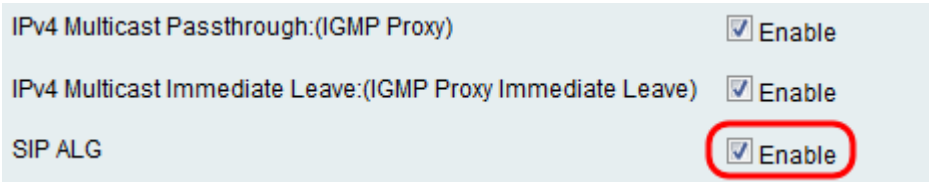


Schritt 7: Aktivieren Sie im Feld *IPv4 Multicast Immediate Leave: (IGMP Proxy Immediate Leave)* das Kontrollkästchen **Enable (Aktivieren)**, um Multicast Immediate Leave zu aktivieren. Durch die Aktivierung der sofortigen Freigabe wird sichergestellt, dass die

optimale Bandbreitenverwaltung für Hosts in Ihrem Netzwerk selbst in Zeiten gleichzeitiger Multicast-Gruppennutzung gewährleistet ist.



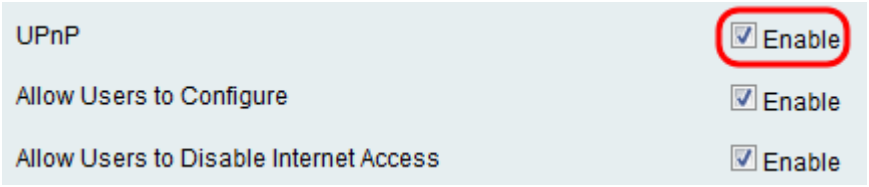
Schritt 8: Aktivieren Sie im Feld *Session Initiation Protocol (SIP) Application Layer Gateway (ALG)* das Kontrollkästchen **Enable (Aktivieren)**, damit der Session Initiation Protocol (SIP)-Datenverkehr die Firewall passieren kann. Session Initiation Protocol (SIP) stattet Plattformen aus, um die Einrichtung von Sprach- und Multimedia-Anrufen über IP-Netzwerke zu signalisieren. Application Layer Gateway (ALG) oder auch als Application Level Gateway bezeichnet, ist eine Anwendung, die IP-Adressinformationen innerhalb der Nutzlast eines Anwendungspakets übersetzt.



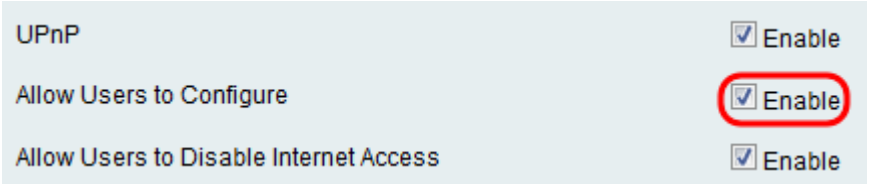
Anmerkung: Das Gerät unterstützt maximal 256 SIP-ALG-Sitzungen.

Konfigurieren von Universal Plug and Play

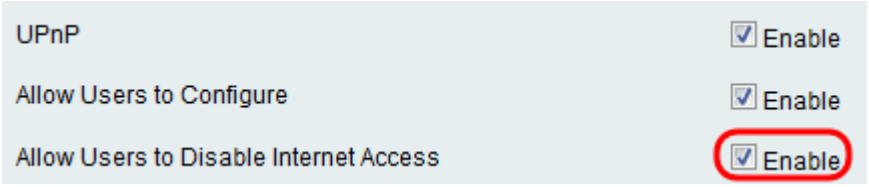
Schritt 1: Aktivieren Sie im Feld *UPnP* das Kontrollkästchen **Enable** to enable the Universal Plug and Play (UPnP).



Schritt 2. Aktivieren Sie im Feld *Allow Users to Configure (Benutzer zur Konfiguration zulassen)* das Kontrollkästchen **Enable (Aktivieren),** um die Festlegung der UPnP-Portzuordnungsregeln durch Benutzer zu ermöglichen, deren UPnP-Unterstützung auf ihren Computern oder anderen UPnP-fähigen Geräten aktiviert ist. Wenn das Gerät deaktiviert ist, kann die Anwendung die Weiterleitungsregel nicht hinzufügen.



Schritt 3. Aktivieren Sie im Feld *Allow Users to Disable Internet Access* (*Benutzer* den Internetzugriff *deaktivieren*) das Kontrollkästchen **Enable (Aktivieren**), damit Benutzer den Internetzugriff deaktivieren können.



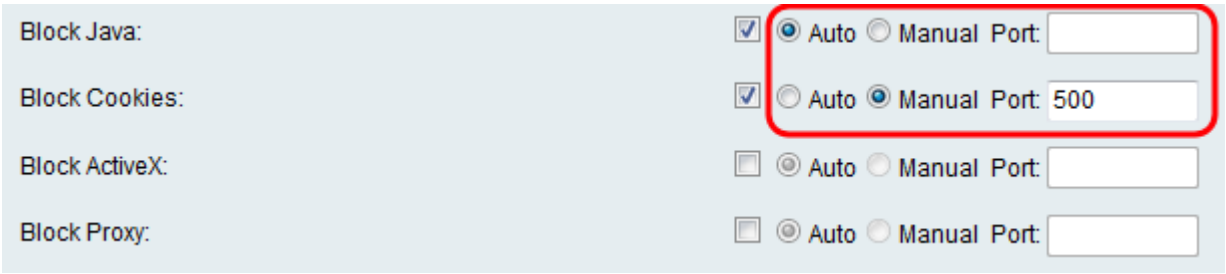
Blockieren von Inhalten

Schritt 1: Aktivieren Sie das Kontrollkästchen in dem Feld, das dem Inhalt entspricht, den Sie vom Gerät blockieren möchten.

Die verfügbaren Optionen sind wie folgt definiert:

- Java blockieren — Blockiert das Herunterladen von Java-Applets.
- Blockieren von Cookies — Blockiert den Empfang von Cookie-Informationen von Webseiten durch das Gerät.
- ActiveX blockieren — Blockiert ActiveX-Applets, die bei Verwendung von Internet Explorer unter dem Windows-Betriebssystem vorhanden sein können.
- Proxy blockieren — Das Gerät wird daran gehindert, über einen Proxyserver mit externen Geräten zu kommunizieren. Dadurch wird verhindert, dass das Gerät Firewall-Regeln umgeht.

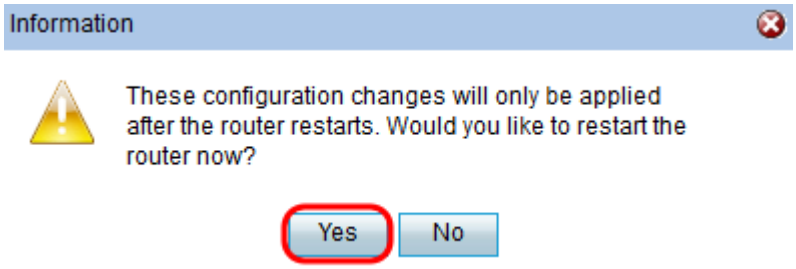
Schritt 2: Wählen Sie entweder das Optionsfeld **Auto (Automatisch)**, um automatisch alle Instanzen dieses bestimmten Inhalts zu blockieren, oder klicken Sie auf das Optionsfeld **Manual (Manuell)** und geben Sie einen bestimmten Port in das entsprechende Feld ein, an dem der Inhalt blockiert wird.



Anmerkung: Sie können eine beliebige Zahl im Bereich (1-65535) für Ihren Port-Wert eingeben.

Schritt 3: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Schritt 4: Ein Fenster wird angezeigt, in dem Sie aufgefordert werden, den Router neu zu starten. Klicken Sie auf **Ja**, um den Router neu zu starten und die Änderungen zu übernehmen.


Information
These configuration changes will only be applied after the router restarts. Would you like to restart the router now?
Yes
No

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.