

Konfigurieren der Service-Verwaltung für Zugriffsregeln auf den Routern RV160X/RV260X

Ziel

In diesem Artikel erfahren Sie, wie Sie Zugriffsregeln für die Router RV160 und RV260 konfigurieren.

Einführung

Zugriffsregeln definieren die Regeln, die der Datenverkehr erfüllen muss, um eine Schnittstelle zu passieren. Eine Zugriffsregel erlaubt oder verweigert Datenverkehr basierend auf dem Protokoll, einer Quell- und Ziel-IP-Adresse oder dem Netzwerk und optional den Quell- und Zielports.

Wenn Sie Zugriffsregeln für Geräte bereitstellen, werden diese zu einem oder mehreren Zugriffskontrolleinträgen (ACEs) für Zugriffskontrolllisten (ACLs), die an Schnittstellen angeschlossen sind. In der Regel sind diese Regeln die erste Sicherheitsrichtlinie, die auf Pakete angewendet wird. Sie sind Ihre erste Verteidigungslinie. Jedes Paket, das an einer Schnittstelle ankommt, wird anhand der von Ihnen festgelegten Kriterien überprüft, ob das Paket weitergeleitet oder verworfen werden soll. Wenn Sie Zugriffsregeln in die ausgehende Richtung definieren, werden auch Pakete analysiert, bevor sie eine Schnittstelle verlassen dürfen.

Anwendbare Geräte

- RV160
- RV260

Softwareversion

- 1,0 00,15

Zugriffsregeln konfigurieren

Führen Sie die folgenden Schritte aus, um die Zugriffsregeln für den RV160/RV260 zu konfigurieren.

Schritt 1: Melden Sie sich auf der Webkonfigurationsseite Ihres Routers an.



Router

cisco **1**

..... **2**

English ▾

Login **3**

©2018 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Hinweis: In diesem Artikel wird die RV260W zum Konfigurieren von Zugriffsregeln verwendet. Die Konfiguration kann je nach verwendetem Modell variieren.

Schritt 2: Navigieren Sie zu **Firewall > Zugriffsregeln**.



Schritt 3: Klicken Sie in der *Tabelle mit IPv4- oder IPv6-Zugriffsregeln* auf **Hinzufügen**, oder wählen Sie die Zeile aus, und klicken Sie auf **Bearbeiten**.

Access Rules Apply Restore Defaults

IPv4 Access Rules Table

+ ✎ 🗑️

<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input type="checkbox"/>	201	Enabled	Allowed	All Traffic	VLAN	Any	WAN	Any	MARKETING	▲ ▼
<input type="checkbox"/>	202	Enabled	Denied	All Traffic	WAN	Any	VLAN	Any	MARKETING	▲ ▼

IPv6 Access Rules Table

+ ✎ 🗑️

Schritt 4: Geben Sie im Abschnitt *Zugriffsregeln hinzufügen/bearbeiten* die folgenden Felder ein.

<i>Regelstatus</i>	Aktivieren Sie <i>Aktivieren</i> , um die spezifische Zugriffsregel zu aktivieren. Deaktivieren Sie
--------------------	---

	diese Option.
<i>Aktion</i>	Wählen Sie <i>Zulassen</i> oder <i>Ablehnen</i> aus der Dropdown-Liste aus.
<i>Services</i>	<ul style="list-style-type: none"> · <i>IPv4</i>: Wählen Sie den Dienst aus, um die IPv4-Regel anzuwenden. · <i>IPv6</i>: Wählen Sie den Service aus, um die IPv6-Regel anzuwenden. · <i>Services</i> - Wählen Sie den Service aus der Dropdown-Liste aus.
<i>Protokoll</i>	<p>Wählen Sie eine Option aus der Dropdown-Liste aus.</p> <ul style="list-style-type: none"> · <i>Always</i>: Für Pakete, die den Regeln entsprechen, werden Protokolle angezeigt. · <i>Nie</i> - Kein Protokoll erforderlich.
<i>Quellschnittstelle</i>	Wählen Sie die Quellschnittstelle aus der Dropdown-Liste aus.
<i>Quelladresse</i>	<p>Wählen Sie die Quell-IP-Adresse aus, auf die die Regel angewendet wird, und geben Sie Folgendes ein:</p> <p><i>Any (Beliebig ·)</i>: Wählen Sie diese Option aus, um alle IP-Adressen abzugleichen.</p> <ul style="list-style-type: none"> · <i>Single</i> - Geben Sie eine IP-Adresse ein. · <i>Subnetz</i> - Geben Sie ein Subnetz eines Netzwerks ein. · <i>IP-Bereich</i>: Geben Sie den IP-Adressbereich ein.
<i>Zielschnittstelle</i>	Wählen Sie die Quellschnittstelle aus der Dropdown-Liste aus.
<i>Zieladresse</i>	<p>Wählen Sie die Quell-IP-Adresse aus, auf die die Regel angewendet wird, und geben Sie Folgendes ein:</p> <p><i>Any (Beliebig ·)</i>: Wählen Sie diese Option aus, um alle IP-Adressen abzugleichen.</p> <ul style="list-style-type: none"> · <i>Single</i> - Geben Sie eine IP-Adresse ein. · <i>Subnetz</i> - Geben Sie ein Subnetz eines Netzwerks ein. · <i>IP-Bereich</i>: Geben Sie den IP-Adressbereich ein.
<i>Name des Zeitplans</i>	Wählen Sie <i>aus</i> der Dropdown-Liste <i>Always, Business, Evening hours, Marketing oder Work Hours (Immer, Geschäftszeiten, Abendstunden, Marketing oder Arbeitszeiten)</i> aus, um die Firewall-Regel anzuwenden. Klicken Sie dann <i>hier</i> , um die Zeitpläne zu konfigurieren.

Add/Edit Access Rules

Apply

Cancel

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 v

Log: Always Never

Schritt 5: (Optional) Klicken Sie zum Konfigurieren von Zeitplänen neben *Name* des *Zeitplans* **hier**.

Schedule

Schedule Name: Click [here](#) to configure the schedules.

Schritt 6: (Optional) Klicken Sie auf **Hinzufügen**, um einen Zeitplan hinzuzufügen, oder wählen Sie die Zeile aus, und klicken Sie auf **Bearbeiten**.

Schedules Apply Cancel Back



<input type="checkbox"/>	Name	Start (24h:mm:ss)	End (24h:mm:ss)	Days
<input type="checkbox"/>	Always	00:00:00	23:59:59	Everyday
<input type="checkbox"/>	BUSINESS	09:00:00	17:30:00	Weekdays
<input type="checkbox"/>	EVENINGHOURS	18:01:00	23:59:59	Everyday
<input type="checkbox"/>	MARKETING	00:00:00	23:59:59	Everyday
<input type="checkbox"/>	WORKHOURS	08:00:00	18:00:00	Weekdays

Hinweis: Weitere Informationen zur Konfiguration des Zeitplans erhalten Sie [hier](#).

Schritt 7: (Optional) Klicken Sie auf **Übernehmen**.

Add/Edit Access Rules Apply Cancel

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6

Log: Always Never

Source Interface:

Source Address:

Destination Interface:

Destination Address:

Schedule

Schedule Name: Click [here](#) to configure the schedules.

Schritt 8: (Optional) Klicken Sie auf **Standardeinstellungen wiederherstellen**, um die Standardeinstellungen wiederherzustellen.

Access Rules Apply Restore Defaults

IPv4 Access Rules Table 



Service-Management

Schritt 1: Zum Hinzufügen oder Bearbeiten eines Eintrags in der Liste Dienste klicken Sie auf **Service Management**.

Access Rules

Apply Restore Defaults

Traffic

<input type="checkbox"/>	202	Enabled	Denied	All Traffic	WAN	Any	VLAN	Any	MARKETING	▲ ▼
--------------------------	-----	---------	--------	-------------	-----	-----	------	-----	-----------	-----

IPv6 Access Rules Table

+ ✎ 🗑

<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input type="checkbox"/>	201	Enabled	Allowed	All Traffic	VLAN	Any	WAN	Any	MARKETING	▲ ▼
<input type="checkbox"/>	202	Enabled	Denied	All Traffic	WAN	Any	VLAN	Any	MARKETING	▲ ▼

Service Management...

Schritt 2: Um einen Dienst hinzuzufügen, klicken Sie in der Diensttabelle auf **Hinzufügen**. Um einen Dienst zu bearbeiten, wählen Sie die Zeile aus, und klicken Sie auf **Bearbeiten**. Die Felder können geändert werden.

Service Management

Apply Cancel Back

+ ✎ 🗑 ⬇ ⬆

<input type="checkbox"/>	Name	Protocol	Port Start/ICMP Type/IP Protocol	Port End/ICMP Code
<input type="checkbox"/>	All Traffic	ALL	--	--
<input type="checkbox"/>	BGP	TCP	179	179
<input type="checkbox"/>	DNS-TCP	TCP	53	53
<input type="checkbox"/>	DNS-UDP	UDP	53	53
<input type="checkbox"/>	ESP	IP	50	--
<input type="checkbox"/>	FTP	TCP	21	21
<input type="checkbox"/>	HTTP	TCP	80	80

Schritt 3: Sie können viele Dienste in der Liste haben:

- *Name* - Name des Dienstes oder der Anwendung.
- *Protokoll* - Wählen Sie ein Protokoll aus der Dropdown-Liste aus.
- *Port Start/ICMP Type/IP Protocol* - Bereich der für diesen Service reservierten Portnummern.
- *Port-End/ICMP-Code* - Letzte Nummer des Ports, reserviert für diesen Service.



<input type="checkbox"/>	Name	Protocol	Port Start/ICMP Type/IP Protocol	Port End/ICMP Code
<input type="checkbox"/>	All Traffic	ALL	--	--
<input type="checkbox"/>	BGP	TCP	179	179
<input type="checkbox"/>	DNS-TCP	TCP	53	53
<input type="checkbox"/>	DNS-UDP	UDP	53	53
<input type="checkbox"/>	ESP	IP	50	--
<input type="checkbox"/>	FTP	TCP	21	21
<input type="checkbox"/>	HTTP	TCP	80	80

Schritt 4: Wenn Sie Einstellungen hinzugefügt oder bearbeitet haben, klicken Sie auf **Übernehmen**.



<input type="checkbox"/>	Name	Protocol	Port Start/ICMP Type/IP Protocol	Port End/ICMP Code
<input type="checkbox"/>	All Traffic	ALL	--	--
<input type="checkbox"/>	BGP	TCP	179	179
<input type="checkbox"/>	DNS-TCP	TCP	53	53
<input type="checkbox"/>	DNS-UDP	UDP	53	53
<input type="checkbox"/>	ESP	IP	50	--
<input type="checkbox"/>	FTP	TCP	21	21
<input type="checkbox"/>	HTTP	TCP	80	80

Sie sollten jetzt die Zugriffsregeln für Ihren RV160/RV260-Router erfolgreich konfiguriert haben.