

Configurazione di Service Management per le regole di accesso sui router RV160X/RV260X

Obiettivo

In questo articolo viene spiegato come configurare le regole di accesso sui router RV160 e RV260.

Introduzione

Le regole di accesso definiscono le regole che il traffico deve rispettare per passare attraverso un'interfaccia. Una regola di accesso consente o nega il traffico in base al protocollo, a un indirizzo IP di origine e di destinazione o alla rete e, facoltativamente, alle porte di origine e di destinazione.

Quando si distribuiscono regole di accesso ai dispositivi, queste diventano una o più voci di controllo di accesso (ACE, Access Control Entries) negli elenchi di controllo di accesso (ACL, Access Control Lists) collegati alle interfacce. In genere, queste regole sono il primo criterio di sicurezza applicato ai pacchetti; sono la tua prima linea di difesa. Ogni pacchetto che arriva a un'interfaccia viene esaminato per determinare se inoltrarlo o eliminarlo in base ai criteri specificati. Se si definiscono le regole di accesso nella direzione di uscita, i pacchetti vengono analizzati anche prima di poter uscire da un'interfaccia.

Dispositivi interessati

- RV160
- RV260

Versione del software

- 1.0.00.15

Configura regole di accesso

Per configurare le regole di accesso per RV160/RV260, eseguire la procedura seguente.

Passaggio 1. Accedere alla pagina di configurazione Web del router.



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.

Nota: In questo articolo verrà utilizzato l'RV260W per configurare le regole di accesso. La configurazione può variare a seconda del modello in uso.

Passaggio 2. Passare a **Firewall > Regole di accesso**.



Passaggio 3. Nella *tabella Regole di accesso IPv4 o IPv6*, fare clic su **Aggiungi** o selezionare la riga e fare clic su **Modifica**.

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 ^

+ ✎ 🗑️

Passaggio 4. Nella sezione *Aggiungi/Modifica regole di accesso* immettere i campi riportati di seguito.

<i>Stato regola</i>	Selezionare <i>Abilita</i> per abilitare la regola di accesso specifica. Deselezionare per disabilitare.
---------------------	--

<i>Azione</i>	Selezionare <i>Consenti</i> o <i>Nega</i> dall'elenco a discesa.
<i>Servizi</i>	<ul style="list-style-type: none"> · <i>IPv4</i>: selezionare il servizio a cui applicare la regola IPv4. · <i>IPv6</i> - Selezionare il servizio a cui applicare la regola IPv6. · <i>Servizi</i> - Selezionare il servizio dall'elenco a discesa.
<i>Log</i>	<p>Selezionare un'opzione dall'elenco a discesa.</p> <ul style="list-style-type: none"> · <i>Always</i> (Sempre) - Vengono visualizzati i log per i pacchetti che soddisfano le regole. · <i>Mai</i> - Nessun registro richiesto.
<i>Interfaccia di origine</i>	Selezionare l'interfaccia di origine dall'elenco a discesa.
<i>Source address</i>	<p>Selezionare l'indirizzo IP di origine a cui applicare la regola e immettere quanto segue:</p> <ul style="list-style-type: none"> · <i>Any</i> (Qualsiasi) - Selezionare questa opzione per far corrispondere tutti gli indirizzi IP. · <i>Single (Singolo)</i> - Consente di immettere un indirizzo IP. · <i>Subnet</i>: consente di immettere una subnet di una rete. · <i>IP Range</i> (Intervallo IP) - Consente di immettere l'intervallo di indirizzi IP.
<i>Interfaccia di destinazione</i>	Selezionare l'interfaccia di origine dall'elenco a discesa.
<i>Indirizzo di destinazione</i>	<p>Selezionare l'indirizzo IP di origine a cui applicare la regola e immettere quanto segue:</p> <ul style="list-style-type: none"> · <i>Any</i> (Qualsiasi) - Selezionare questa opzione per far corrispondere tutti gli indirizzi IP. · <i>Single (Singolo)</i> - Consente di immettere un indirizzo IP. · <i>Subnet</i>: consente di immettere una subnet di una rete. · <i>IP Range</i> (Intervallo IP) - Consente di immettere l'intervallo di indirizzi IP.
<i>Nome pianificazione</i>	Selezionare <i>Sempre</i> , <i>Ufficio</i> , <i>Ore serali</i> , <i>Marketing</i> o <i>Ore lavorative</i> dall'elenco a discesa per applicare la regola firewall. Quindi, fare clic <i>qui</i> per configurare le pianificazioni.

Add/Edit Access Rules

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6

Log: Always Never

Source Interface:

Passaggio 5. (Facoltativo) Per configurare le pianificazioni, fare clic **qui** accanto a *Nome pianificazione*.

Schedule

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

Passaggio 6. (Facoltativo) Fare clic su **Aggiungi** per aggiungere una pianificazione o selezionare la riga e fare clic su **Modifica**.

Schedules Apply Cancel Back

[+](#) [✎](#) [🗑️](#)

<input type="checkbox"/>	Name	Start (24hh:mm:ss)	End (24hh: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

Nota: Per ulteriori informazioni sulla configurazione della pianificazione, fare clic [qui](#).

Passaggio 7. (Facoltativo) Fare clic su **Applica**.

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.

Passaggio 8. (Facoltativo) Fare clic su **Ripristina valori predefiniti** per ripristinare le impostazioni predefinite.

Access Rules Apply Restore Defaults

IPv4 Access Rules Table [^](#)

[+](#) [✎](#) [🗑️](#)

Gestione dei servizi

Passaggio 1. Per aggiungere o modificare una voce nell'elenco dei servizi, fare clic su **Gestione servizi**.

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...

Passaggio 2. Per aggiungere un servizio, fare clic su **Add** (Aggiungi) nella tabella Service (Servizio). Per modificare un servizio, selezionare la riga e fare clic su **Modifica**. I campi vengono aperti per la modifica.

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

Passaggio 3. Nell'elenco sono disponibili molti servizi:

- **Name:** nome del servizio o dell'applicazione.
- **Protocollo:** selezionare un protocollo dall'elenco a discesa.
- **Port Start/ICMP Type/IP Protocol:** intervallo di numeri di porta riservati per questo servizio.
- **Codice fine porta/ICMP:** ultimo numero della porta, riservato per questo servizio.

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

Passaggio 4. Se sono state aggiunte o modificate impostazioni, fare clic su **Applica**.

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

A questo punto, è necessario configurare correttamente le regole di accesso sul router RV160/ RV260.