

Configurer la gestion des services pour les règles d'accès sur les routeurs RV160X/RV260X

Objectif

L'objectif de cet article est de vous montrer comment configurer les règles d'accès sur les routeurs RV160 et RV260.

Introduction

Les règles d'accès définissent les règles que le trafic doit respecter pour passer par une interface. Une règle d'accès autorise ou refuse le trafic en fonction du protocole, d'une adresse IP source et de destination ou du réseau, et éventuellement des ports source et de destination.

Lorsque vous déployez des règles d'accès aux périphériques, ils deviennent une ou plusieurs entrées de contrôle d'accès (ACE) aux listes de contrôle d'accès (ACL) qui sont connectées aux interfaces. En règle générale, ces règles sont la première stratégie de sécurité appliquée aux paquets ; ce sont vos premières lignes de défense. Chaque paquet qui arrive sur une interface est examiné pour déterminer s'il doit transférer ou abandonner le paquet en fonction des critères que vous spécifiez. Si vous définissez des règles d'accès dans la direction de sortie, les paquets sont également analysés avant d'être autorisés à quitter une interface.

Périphériques pertinents

- RV160
- RV260

Version du logiciel

- 1.0.00.15

Configurer les règles d'accès

Pour configurer les règles d'accès sur le routeur RV160/RV260, procédez comme suit.

Étape 1. Connectez-vous à la page de configuration Web de votre routeur.



Router

cisco **1**

•••••••• **2**

English ▾

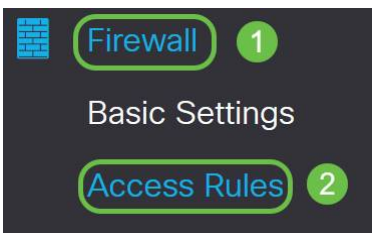
Login **3**

©2018 Cisco Systems, Inc. All Rights Reserved.

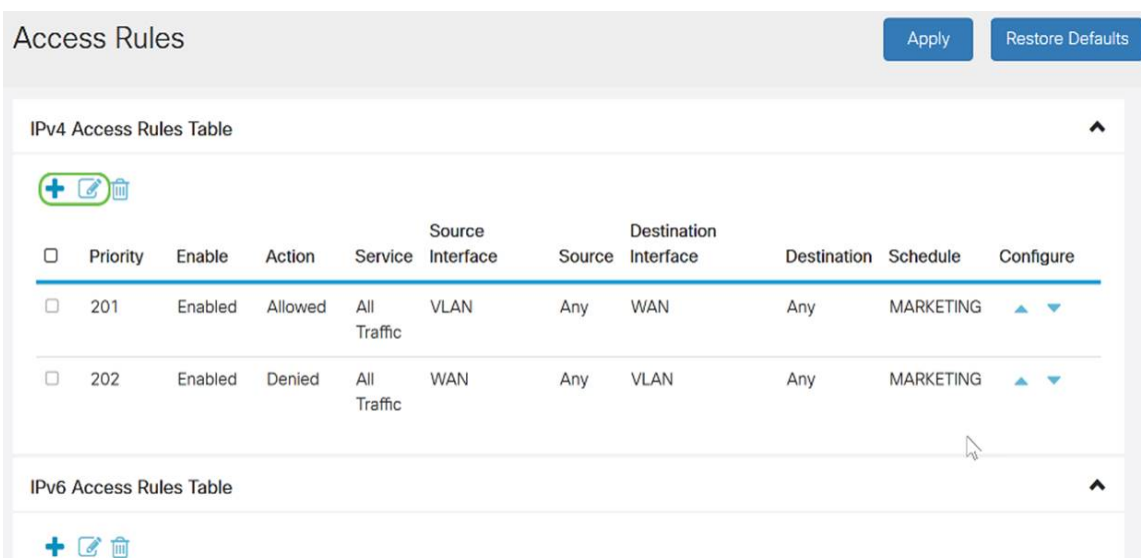
Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Remarque: Dans cet article, nous allons utiliser le RV260W pour configurer les règles d'accès. La configuration peut varier en fonction du modèle que vous utilisez.

Étape 2. Accédez à **Firewall > Access Rules**.



Étape 3. Dans le *tableau Règles d'accès IPv4 ou IPv6*, cliquez sur **Ajouter** ou sélectionnez la ligne et cliquez sur **Modifier**.



Étape 4. Dans la section *Ajouter/modifier des règles d'accès*, saisissez les champs suivants.

<i>État de la règle</i>	Cochez <i>Enable</i> pour activer la règle d'accès spécifique. Décochez cette case pour désactiver.
<i>Action</i>	Choisissez <i>Allow</i> ou <i>Deny</i> dans la liste déroulante.

<i>Services</i>	<ul style="list-style-type: none"> · <i>IPv4</i> - Sélectionnez le service à appliquer à la règle IPv4. · <i>IPv6</i> - Sélectionnez le service à appliquer à la règle IPv6. · <i>Services</i> - Sélectionnez le service dans la liste déroulante.
<i>Journal</i>	<p>Sélectionnez une option dans la liste déroulante.</p> <ul style="list-style-type: none"> · <i>Always</i> - Les journaux s'affichent pour le paquet qui correspond aux règles. · <i>Jamais</i> - Aucun journal requis.
<i>Interface source</i>	Sélectionnez l'interface source dans la liste déroulante.
<i>Adresse source</i>	<p>Sélectionnez l'adresse IP source à laquelle la règle est appliquée et saisissez les informations suivantes :</p> <ul style="list-style-type: none"> · <i>Any</i> - Sélectionnez cette option pour faire correspondre toutes les adresses IP. · <i>Single</i> - Entrez une adresse IP. · <i>Subnet</i> - Entrez un sous-réseau d'un réseau. · <i>IP Range</i> : saisissez la plage d'adresses IP.
<i>Interface de destination</i>	Sélectionnez l'interface source dans la liste déroulante.
<i>Adresse de destination</i>	<p>Sélectionnez l'adresse IP source à laquelle la règle est appliquée et saisissez les informations suivantes :</p> <ul style="list-style-type: none"> · <i>Any</i> - Sélectionnez cette option pour faire correspondre toutes les adresses IP. · <i>Single</i> - Entrez une adresse IP. · <i>Subnet</i> - Entrez un sous-réseau d'un réseau. · <i>IP Range</i> : saisissez la plage d'adresses IP.
<i>Nom de la planification</i>	<p>Sélectionnez <i>Toujours, Heures de bureau, de soirée, Marketing ou Heures de travail</i> dans la liste déroulante pour appliquer la règle de pare-feu. Ensuite, cliquez <i>ici</i> pour configurer les plannings.</p>

Add/Edit Access Rules

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 ▾

Log: Always Never

Source Interface: ▾

Source Address: ▾

Destination Interface: ▾

Destination Address: ▾

Étape 5. (Facultatif) Pour configurer les planifications, cliquez [ici](#) en regard de *Nom de la planification*.

Schedule

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

Étape 6. (Facultatif) Cliquez sur **Ajouter** pour ajouter un planning ou sélectionnez la ligne et cliquez sur **Modifier**.

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

Note: Pour plus d'informations sur la configuration du planning, cliquez [ici](#).

Étape 7. (Facultatif) Cliquez sur **Apply**.

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.

Étape 8. (Facultatif) Cliquez sur **Restaurer les paramètres par défaut**, pour restaurer les paramètres par défaut.

Access Rules Apply Restore Defaults

IPv4 Access Rules Table [^](#)

[+](#) [✎](#) [🗑️](#)

Gestion des services

Étape 1. Pour ajouter ou modifier une entrée dans la liste Service, cliquez sur **Gestion des services**.

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...

Étape 2. Pour ajouter un service, cliquez sur **Ajouter** sous la table Service. Pour modifier un service, sélectionnez la ligne et cliquez sur **Modifier**. Les champs sont ouverts pour modification.

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

Étape 3. Vous pouvez avoir de nombreux services dans la liste :

- *Nom* - Nom du service ou de l'application.
- *Protocol* - Sélectionnez un protocole dans la liste déroulante.
- *Port Start/ICMP Type/IP Protocol* - Plage de numéros de port réservés à ce service.
- *Port End/ICMP Code* - Dernier numéro du port, réservé à ce service.

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

Étape 4. Si vous avez ajouté ou modifié des paramètres, cliquez sur **Appliquer**.

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

Vous devez maintenant avoir correctement configuré les règles d'accès sur votre routeur RV160/RV260.