

Permitir o bloquear el tráfico de servicio en IPv6 en RV0xx

Objetivo

Este documento explica cómo permitir o bloquear cualquier tráfico de servicio basado en la programación específica si la solicitud se origina en una máquina específica. El artículo explica que se puede denegar a los usuarios en función de las direcciones IP. Las programaciones se pueden realizar en función de cualquier día u hora. Las direcciones IP permitidas o denegadas pueden ser un intervalo específico o cualquier dirección IP específica.

Dispositivos aplicables

• RV016

• RV082

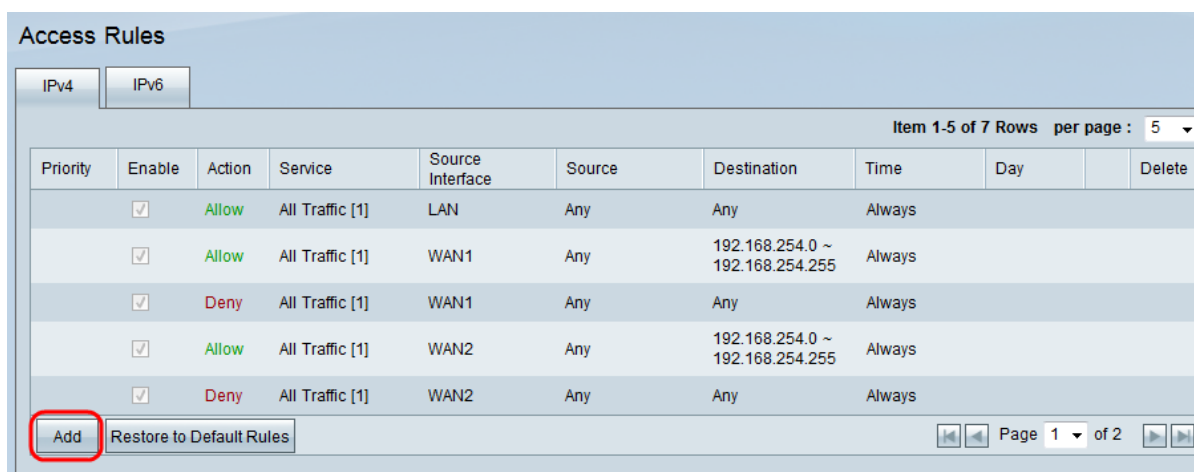
• RV042

• RV042G

Pasos para permitir o bloquear el tráfico del servicio

Pasos para configurar servicios

Paso 1. Inicie sesión en la utilidad de configuración del router y elija **Firewall > Access Rules**. Se abre la página *Access Rules*:



Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	WAN1	Any	192.168.254.0 ~ 192.168.254.255	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always		
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	WAN2	Any	192.168.254.0 ~ 192.168.254.255	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always		

Item 1-5 of 7 Rows per page : 5

Add Restore to Default Rules Page 1 of 2

Paso 2. Haga clic en **Agregar** para crear una programación de tráfico de servicio. Se abre la página *Access Rules*:

Access Rules

Services

Action : Allow ▼

Service : Allow
Deny [TCP&UDP/1~65535] ▼

Service Management

Log : Log packets match this rule ▼

Source Interface : LAN ▼

Source IP : Single ▼

Destination IP : Single ▼

Scheduling

Time : Always ▼

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel

Paso 3. En la lista desplegable Acción, elija **Permitir** para permitir que el tráfico siga o elija **Denegar** para bloquear el tráfico.

Access Rules

Services

Action : Allow ▼

Service : All Traffic [TCP&UDP/1~65535] ▼

Log : All Traffic [TCP&UDP/1~65535]

Source Interface : All Traffic [TCP&UDP/1~65535]

Source IP : All Traffic [TCP&UDP/1~65535]

Destination IP : All Traffic [TCP&UDP/1~65535]

Scheduling

Time : Always ▼

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel

Paso 4. Seleccione un servicio de la lista desplegable Servicio.

Nota: Haga clic en **Administración de servicios** si un servicio determinado no se menciona en la lista desplegable Servicio.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Paso 5. Seleccione una opción de la lista desplegable Registro.

- Los paquetes de registro coinciden con esta regla " para registrar los paquetes entrantes que coinciden con la regla de acceso.
- No registrar: no registrar paquetes entrantes que coincidan con la regla de acceso.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Paso 6. Elija una interfaz de la lista desplegable Interfaz de origen. La interfaz de origen es la interfaz desde la cual se inicia el tráfico.

- LAN: la red de área local. Conecta ordenadores en las proximidades de una red, como un edificio de oficinas o un colegio.
- WAN1: la red de área extensa. Esto conecta equipos en un área grande de una red. Podría tratarse de cualquier red que conecte una región o incluso un país. Las empresas y el gobierno lo utilizan para conectarse a otras ubicaciones.
- WAN2: igual que WAN1, excepto en que se trata de una segunda red.
- DMZ: permite que el tráfico exterior acceda a un ordenador de la red sin exponer la red LAN.
- ANY: permite utilizar cualquier interfaz.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Paso 7. Elija una opción para especificar la dirección IP de origen en la lista desplegable IP de origen.

- Cualquiera: se utilizará cualquier dirección IP para reenviar el tráfico. No habrá ningún campo a la derecha de la lista desplegable disponible.
- Única: se utilizará una única dirección IP para reenviar el tráfico. Introduzca la dirección IP que desee en el campo situado a la derecha de la lista desplegable.
- Rango: se utilizará una dirección IP de rango para reenviar el tráfico. Introduzca el intervalo de direcciones IP deseado en los campos situados a la derecha de la lista desplegable.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Paso 8. Elija una opción para especificar la dirección IP de destino en la lista desplegable IP de destino.

- Cualquiera: se utilizará cualquier dirección IP para reenviar el tráfico. No habrá ningún campo a la derecha de la lista desplegable disponible.
- Única: se utilizará una única dirección IP para reenviar el tráfico. Introduzca la dirección IP que desee en el campo situado a la derecha de la lista desplegable.
- Rango: se utilizará una dirección IP de rango para reenviar el tráfico. Introduzca el intervalo de direcciones IP deseado en los campos situados a la derecha de la lista desplegable.

Pasos para configurar la programación

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time : (dropdown menu with options: Always, Interval)

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Paso 1. Seleccione una opción de hora en la lista desplegable Hora.

- Siempre: esta opción permitirá o bloqueará el tráfico del servicio durante toda la semana.
- Intervalo: esta opción permitirá o bloqueará el tráfico de servicio en un día o días específicos en un momento específico.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Paso 2. Introduzca una hora específica en los campos De y A para especificar una hora que permita o bloquee el tráfico del servicio.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :

Scheduling

Time :

From : (hh:mm) To : (hh:mm)

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Paso 3. Deje activada la casilla de verificación Todos los días de forma predeterminada para permitir o bloquear el tráfico de servicio todos los días a una hora determinada, o bien desactive la casilla de verificación Todos los días para marcar los días que desea permitir o bloquear el tráfico de servicio.

Paso 4. Haga clic en **Guardar** para guardar la regla de acceso configurada.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).