

Configuración de una regla de acceso IPv4 en routers VPN RV016, RV042, RV042G y RV082

Objetivo

Una regla de acceso ayuda al router a determinar, en función de los requisitos del usuario, el tráfico que puede pasar y el que se debe denegar a través del firewall. Esto ayuda a agregar seguridad al router.

Este documento explica el procedimiento para agregar o eliminar una regla de acceso en los routers VPN RV016, RV042, RV042G y RV082.

Dispositivos aplicables

•RV016

•RV042

•RV042G

•RV082

Versión del software

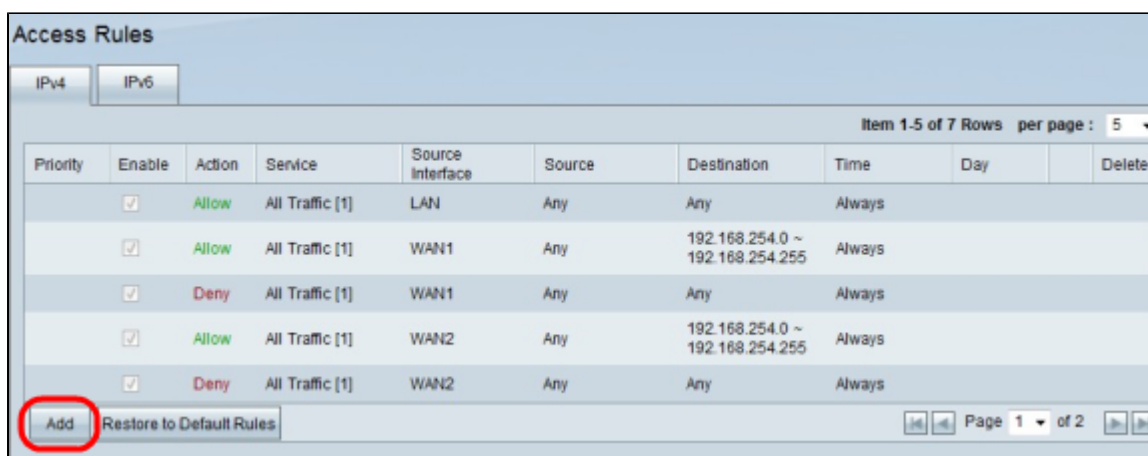
•4.2.1.02

Administrar reglas de acceso IPv4

La planificación de reglas de acceso IPv4 es una configuración opcional.

Agregar o eliminar reglas de acceso IPv4

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Firewall > Access Rules**. Se abre la página *Reglas de acceso IPv4*. Haga clic en Add (Agregar).



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. Se abre la página *Access Rules Service*. En la lista desplegable Acción, elija **Permitir** para permitir el tráfico. De lo contrario, elija **Denegar** para denegar el tráfico.

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. Seleccione el servicio adecuado en la lista desplegable Servicio. Si el servicio adecuado no está disponible, haga clic en **Administración de servicios**.

Nota: Si el servicio deseado está disponible, vaya directamente al paso 6.

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 4.

Aparecerá una nueva ventana. Introduzca un nombre de servicio en el campo Service Name (Nombre de servicio).

Service Name :

Protocol :

Port Range : to

All Traffic [TCP&UDP/1~65535]
 DNS [UDP/53~53]
 FTP [TCP/21~21]
 HTTP [TCP/80~80]
 HTTP Secondary [TCP/8080~8080]
 HTTPS [TCP/443~443]
 HTTPS Secondary [TCP/8443~8443]
 TFTP [UDP/69~69]
 IMAP [TCP/143~143]
 NNTP [TCP/119~119]
 POP3 [TCP/110~110]
 SNMP [UDP/161~161]

Paso 5. Elija el tipo de protocolo adecuado en la lista desplegable Protocolo.

- TCP (protocolo de control de transmisión): protocolo de capa de transporte utilizado por aplicaciones que requieren entrega garantizada.
- UDP (protocolo de datagrama de usuario): utiliza sockets de datagrama para establecer las comunicaciones entre hosts. Es más rápido que TCP, pero no es tan probable que se ejecute correctamente.
- IPv6 (protocolo de Internet versión 6): dirige el tráfico de Internet entre hosts en paquetes que se enrutan a través de redes especificadas por direcciones de enrutamiento.

Service Name :

Protocol : TCP ▼
TCP
UDP
IPv6

Port Range : to

All Traffic [TCP&UDP/1~65535]
DNS [UDP/53~53]
FTP [TCP/21~21]
HTTP [TCP/80~80]
HTTP Secondary [TCP/8080~8080]
HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]

Paso 6. Introduzca el intervalo de puertos en los campos Intervalo de puertos. Este intervalo depende del protocolo elegido.

Haga clic en **Agregar a la lista**. De este modo, se agrega el servicio a la lista desplegable Servicio.

Otras opciones incluyen **Delete**, **Update** o **Add New**.

Click OK. De esta forma, se cierra la ventana y el usuario vuelve a la página *Access Rule Service*.

Service Name :

Protocol :

Port Range : to

All Traffic [TCP&UDP/1~65535]

DNS [UDP/53~53]

FTP [TCP/21~21]

HTTP [TCP/80~80]

HTTP Secondary [TCP/8080~8080]

HTTPS [TCP/443~443]

HTTPS Secondary [TCP/8443~8443]

TFTP [UDP/69~69]

IMAP [TCP/143~143]

NNTP [TCP/119~119]

POP3 [TCP/110~110]

SNMP [UDP/161~161]

Paso 7. En la lista desplegable Registro, elija **Registrar paquetes que coincidan con esta regla** para registrar los paquetes entrantes que coincidan con la regla de acceso. De lo contrario, elija **No registrar**.

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 la interfaz a la que afecta esta regla en la lista desplegable Interfaz de origen. La interfaz de origen es la interfaz desde la que se inicia el tráfico.

- LAN: la red de área local del router.
- WAN1: red de área extensa o red desde la cual el router obtiene acceso a Internet del ISP o del router de salto siguiente.
- WAN2: igual que WAN1, excepto en que es una red secundaria.
- 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 9. En la lista desplegable Source IP (IP de origen), elija una opción para especificar el intervalo de direcciones IP de origen que debe permitir o denegar la interfaz. La IP de origen y la IP de destino verifican los paquetes que llegan a la interfaz.

- Cualquiera: la regla de acceso se aplicará a todo el tráfico de la interfaz de origen. No habrá ningún campo a la derecha de la lista desplegable disponible.
- Único: la regla de acceso se aplicará a una única dirección IP desde la interfaz de origen. Introduzca la dirección IP que desee en el campo de dirección.
- Rango: la regla de acceso se aplicará en una red de subred desde la interfaz de origen. Introduzca la dirección IP y la longitud del prefijo.

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 9. En la lista desplegable Destination (Destino), elija una opción para especificar el intervalo de direcciones de destino que debe permitir o denegar la interfaz. La IP de origen y la IP de destino verifican los paquetes que llegan a la interfaz.

- Cualquiera: la regla de acceso se aplicará a todo el tráfico a la interfaz de destino. No habrá ningún campo a la derecha de la lista desplegable disponible.
- Único: la regla de acceso se aplicará en una única dirección IP a la interfaz de destino. Introduzca la dirección IP que desee en el campo de dirección.
- Rango: la regla de acceso se aplicará en una red de subred a la interfaz de destino. Introduzca la dirección IP y la longitud del prefijo.

Haga clic en **Guardar** para guardar todos los cambios realizados en la regla de acceso. Aparecerá una ventana de confirmación que indica el estado de los cambios realizados en el dispositivo.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP : to

Scheduling

Time :

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

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Paso 10. Haga clic en **Aceptar** para agregar otra regla de acceso. Haga clic en **Cancelar** para volver a la página *Reglas de acceso*.

Settings are successful. Press 'OK' to add another access rule, or press 'Cancel' to return to the page of Access Rules.

Paso 11 (opcional). Elija la regla de acceso que desee de la lista y, a continuación, haga clic en el **botón Editar** para editar la configuración de la regla de acceso.

Access Rules

IPv4


Item 1-5 of 5 Rows per page : 5



Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
1	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	192.0.2.1 ~ 192.0.2.254	Always		<input checked="" type="button" value="Edit"/> <input type="button" value="Delete"/>
2	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		<input type="button" value="Edit"/> <input type="button" value="Delete"/>
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		<input type="button" value="Edit"/> <input type="button" value="Delete"/>
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always		<input type="button" value="Edit"/> <input type="button" value="Delete"/>
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always		<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Page 1 of 1

Paso 12 (opcional). Elija las reglas de acceso que desee de la lista y, a continuación, haga clic en el **botón**

Eliminar para eliminar la regla de acceso de la lista de reglas de acceso.

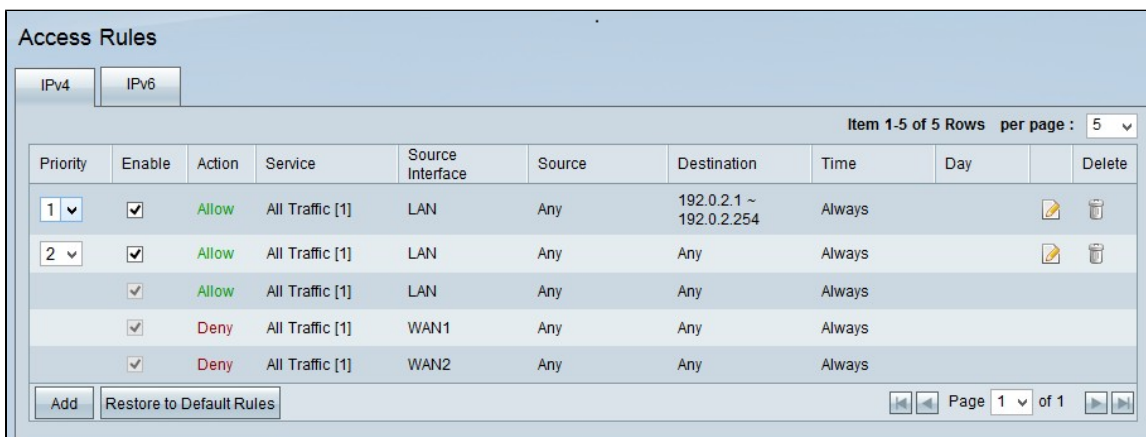




Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
1	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	192.0.2.1 ~ 192.0.2.254	Always		
2	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always		

Programar reglas de acceso IPv4

La programación de las reglas de acceso ayuda a especificar una programación cuando estas reglas de acceso están activas en términos de día y hora. Solo funciona con IPv4.

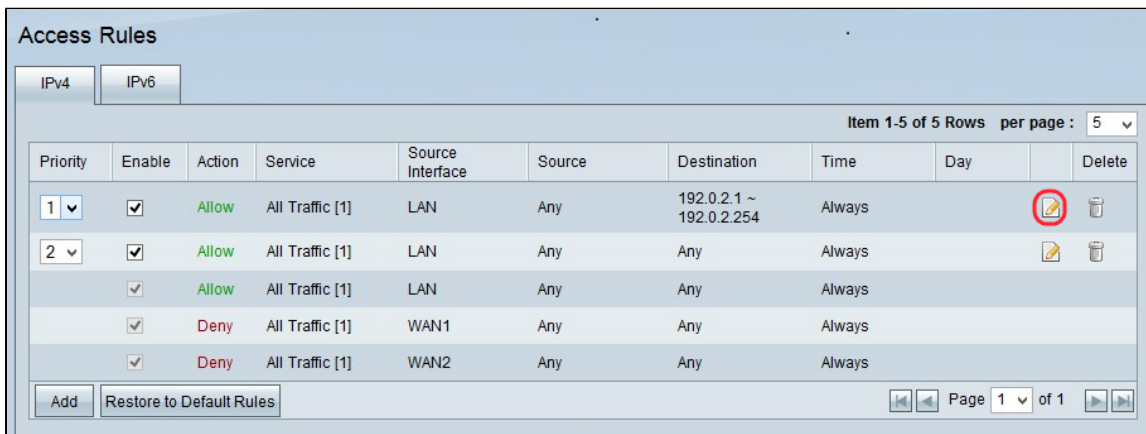
Paso 1. Utilice la utilidad de configuración web y elija **Firewall > Access Rules**. Se abre la página *Reglas de acceso IPv4*:





Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
1	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	192.0.2.1 ~ 192.0.2.254	Always		
2	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always		

Paso 2. Elija la regla de acceso de la tabla y pulse en el icono **Editar** para añadir la función de planificación a dicha regla de acceso.

Nota: También puede agregar la función de programación al agregar una nueva regla de acceso.



Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
1	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	192.0.2.1 ~ 192.0.2.254	Always		
2	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always		

Paso 3. Elija la hora en la lista desplegable Hora. Especifica cuándo se debe utilizar la programación.

- Siempre: la regla de acceso se aplica en todo momento y todos los días de la semana. Se elige de forma predeterminada. Si elige esta opción, haga clic en *Save* y vaya al paso 6.
- Intervalo: en función del intervalo de tiempo dado por el usuario, se aplica la regla de acceso.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP : to

Scheduling

Time :

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

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Paso 4. Introduzca el intervalo de tiempo en formato de 24 horas durante el cual se aplica la regla de acceso en los campos *De* y *A*.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP : to

Scheduling

Time :

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

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Paso 5. Active las casillas de verificación situadas junto a los días en los que desea aplicar la regla de acceso. La regla de acceso sólo entrará en vigor los días marcados. De forma predeterminada, se elige *Everyday*.

Haga clic en **Guardar** para guardar todos los cambios realizados en la regla de acceso. Aparecerá una ventana de confirmación que indica el estado de los cambios realizados en el dispositivo.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP : to

Scheduling

Time :

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

Effective on : Everyday Sun Mon Tue Wed Thu Fri Sat

Paso 6. Haga clic en **Aceptar** para agregar otra regla de acceso. Haga clic en **Cancelar** para volver a la página de reglas de acceso.

Settings are successful. Press 'OK' to add another access rule, or press 'Cancel' to return to the page of Access Rules.

Conclusión

Ya ha configurado las reglas de acceso IPv4 en el router VPN RV016, RV042, RV042G o RV082.

Si desea acceder a todos los servicios de soporte para estos routers, consulte la página del producto haciendo clic [aquí](#).

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).