

Agregar y configurar reglas de acceso en RV130 y RV130W

Objetivo

Los dispositivos de red ofrecen funciones básicas de filtrado del tráfico con reglas de acceso. Una regla de acceso es una entrada única de una lista de control de acceso (ACL) que especifica una regla de permiso o denegación (para reenviar o descartar un paquete) basada en el protocolo, una dirección IP de origen y destino o la configuración de red.

El objetivo de este documento es mostrarle cómo agregar y configurar una regla de acceso en el RV130 y el RV130W.

Dispositivos aplicables

- RV130
- RV130W

‘Versiones de software’

- Versión 1.0.1.3

Agregar y configurar una regla de acceso

Configuración de la política de salida predeterminada

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

Access Rules

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

Filter: Action matches All

Action	Service	Status	Connection Type	Source IP	Destination IP	Log
<input type="checkbox"/> No data to display						

Paso 2. En el área Política de salida predeterminada, haga clic en el botón de opción que desee para elegir una política para el tráfico saliente. La directiva se aplica siempre que no haya reglas de acceso o directivas de acceso a Internet configuradas. La configuración predeterminada es Allow, que permite el paso de todo el tráfico a Internet.

Access Rules

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

Las opciones disponibles se definen de la siguiente manera:

- Permitir: permite todos los tipos de tráfico que salen de la LAN a Internet.
- Denegar: Bloquea todos los tipos de tráfico que salen de la LAN a Internet.

Paso 3. Haga clic en Guardar para guardar la configuración.

Access Rules

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

Filter: Action matches All

Action	Service	Status	Connection Type	Source IP	Destination IP	Log
<input type="checkbox"/> No data to display						

Adición de una regla de acceso

Paso 1. Inicie sesión en la utilidad de configuración web y elija Firewall > Access Rules. Se abre la ventana Access Rules:

Access Rules

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

Filter: Action matches All

Action	Service	Status	Connection Type	Source IP	Destination IP	Log
No data to display						

No data to display

Paso 2. Haga clic en Agregar fila en la Tabla de reglas de acceso para agregar una nueva regla de acceso.

Access Rules

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

Filter: Action matches All

Action	Service	Status	Connection Type	Source IP	Destination IP	Log
No data to display						

No data to display

Se abre la página Agregar regla de acceso:

Add Access Rule

Connection Type: Outbound (LAN > WAN) ▾

Action: Always block ▾

Schedule: ▾

Services: All Traffic ▾

Source IP: Any ▾

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

Paso 3. En la lista desplegable Tipo de conexión, elija el tipo de tráfico al que se aplica la regla.

Connection Type: Outbound (LAN > WAN) ▾
Outbound (LAN > WAN)
Inbound (WAN > LAN)
Inbound (WAN > DMZ)

Action:

Schedule: ▾

Services: All Traffic ▾

Source IP: Any ▾

Start:

Finish:

Las opciones disponibles se definen de la siguiente manera:

- Saliente (LAN > WAN): la regla afecta a los paquetes que provienen de la red local (LAN) y salen a Internet (WAN).
- Entrantes (WAN > LAN): la regla afecta a los paquetes que provienen de Internet (WAN) y entran en la red local (LAN).
- Entrantes (WAN > DMZ): la regla afecta a los paquetes que provienen de Internet (WAN) y entran en la subred de la zona desmilitarizada (DMZ).

Paso 4. En la lista desplegable Acción, elija la acción que se llevará a cabo cuando se haga coincidir una regla.

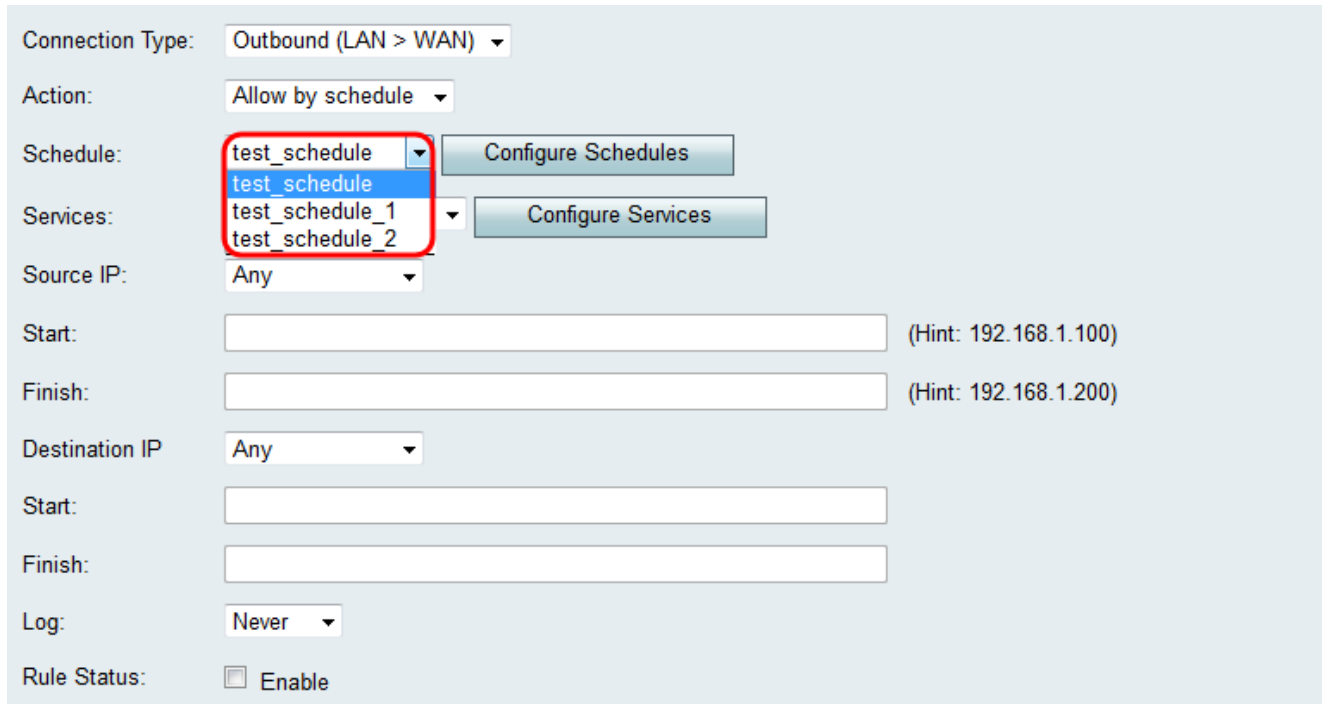
The screenshot shows a configuration window for a firewall rule. The 'Action' dropdown menu is open, with 'Always block' selected. The 'Connection Type' is set to 'Outbound (LAN > WAN)'. The 'Source IP' is set to 'Any'. The 'Destination IP' is also set to 'Any'. The 'Log' option is set to 'Never'. There are buttons for 'Schedules' and 'Configure Services'.

Las opciones disponibles se definen de la siguiente manera:

- Bloquear siempre: deniegue siempre el acceso si se cumplen las condiciones. Vaya al paso 6.
- Permitir siempre: permitir siempre el acceso si se cumplen las condiciones. Vaya al paso 6.
- Bloquear por programación: deniegue el acceso si se cumplen las condiciones durante una programación preconfigurada.

- Permitir por programación: permite el acceso si se cumplen las condiciones durante una programación preconfigurada.

Paso 5. Si ha seleccionado Bloquear por programación o Permitir por programación en el paso 4, elija la programación adecuada en la lista desplegable Programación.



Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: test_schedule_1 ▾

test_schedule_2

Source IP: Any ▾

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

Nota: Para crear o editar una planificación, haga clic en Configurar planificaciones. Refiérase a [Configuración de Programaciones en el RV130 y el RV130W](#) para obtener más información y pautas.

Paso 6. Elija el tipo de servicio al que se aplica la regla de acceso en la lista desplegable Servicios.

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: All Traffic ▾

Source IP:

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status:

All Traffic

All Traffic

DNS

FTP

HTTP

HTTP Secondary

HTTPS

HTTPS Secondary

TFTP

IMAP

NNTP

POP3

SNMP

SMTP

TELNET

TELNET Secondary

TELNET SSL

Voice(SIP)

Nota: Si desea agregar o editar un servicio, haga clic en Configurar servicios. Consulte [Configuración de la gestión de servicios en el RV130 y el RV130W](#) para obtener más información y directrices.

Configuración de IP de origen y destino para tráfico saliente

Siga los pasos de esta sección si se ha seleccionado Outbound (LAN > WAN) como el tipo de conexión en el paso 3 de [Agregar una regla de acceso](#).

Nota: Si se ha seleccionado un tipo de conexión entrante en el paso 3 de Agregar una regla de acceso, pase a la siguiente sección: [Configuración de IP de origen y destino para el tráfico entrante](#).

Paso 1. Elija cómo desea definir la IP de origen en la lista desplegable IP de origen. Para el tráfico saliente, la IP de origen se refiere a la dirección o direcciones (en la LAN) a las que se aplicaría la regla del firewall.

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status: Enable

Las opciones disponibles se definen de la siguiente manera:

- Cualquiera: se aplica al tráfico que se origina en cualquier dirección IP de la red local. Por lo tanto, deje en blanco los campos Start y Finish. Vaya al paso 4 si selecciona esta opción.
- Single Address (Dirección única): se aplica al tráfico que se origina en una única dirección IP de la red local. Introduzca la dirección IP en el campo Start.
- Intervalo de direcciones: se aplica al tráfico que se origina en un intervalo de direcciones IP de la red local. Ingrese la dirección IP inicial del rango en el campo Start y la dirección IP final en el campo Finish para establecer el rango.

Paso 2. Si selecciona Single Address en el paso 1, introduzca la dirección IP que se aplicará a la regla de acceso en el campo Start y, a continuación, vaya al paso 4. Si selecciona Intervalo de direcciones en el paso 1, introduzca una dirección IP inicial que se aplicará a la regla de acceso en el campo Inicio.

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Single Address ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

Paso 3. Si selecciona Intervalo de direcciones en el paso 1, introduzca la dirección IP final que encapsulará el intervalo de direcciones IP para la regla de acceso en el campo Finalizar.

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

Paso 4. Elija cómo desea definir la IP de destino en la lista desplegable IP de destino. Para el tráfico saliente, la IP de destino se refiere a la dirección o direcciones (en la WAN) a las que se permite o deniega el tráfico de la red local.

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status: Enable

Las opciones disponibles se definen de la siguiente manera:

- Cualquiera: se aplica al tráfico dirigido hacia cualquier dirección IP en la Internet pública. Por lo tanto, deje en blanco los campos Start y Finish.
- Single Address (Dirección única): se aplica al tráfico que se dirige a una única dirección IP en la Internet pública. Introduzca la dirección IP en el campo Start.
- Intervalo de direcciones: se aplica al tráfico dirigido hacia un intervalo de direcciones IP en la Internet pública. Ingrese la dirección IP inicial del rango en el campo Start y la dirección IP final en el campo Finish para establecer el rango.

Paso 5. Si selecciona Single Address en el paso 4, introduzca la dirección IP que se aplicará a la regla de acceso en el campo Start. Si selecciona Intervalo de direcciones en el paso 4, introduzca una dirección IP inicial que se aplicará a la regla de acceso en el campo Inicio.

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Single Address ▾

Start: 192.168.1.100

Finish:

Log: Never ▾

Rule Status: Enable

Paso 6. Si selecciona Intervalo de direcciones en el paso 4, introduzca la dirección IP final que encapsulará el intervalo de direcciones IP para la regla de acceso en el campo Finalizar.

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Address Range ▾

Start: 192.168.1.100

Finish: 192.168.1.170

Log: Never ▾

Rule Status: Enable

Configuración de IP de origen y destino para tráfico entrante

Siga los pasos de esta sección si se ha seleccionado Entrante (WAN > LAN) o Entrante (WAN > DMZ) como Tipo de conexión en el paso 3 de [Adición de una](#) regla de acceso.

Paso 1. Elija cómo desea definir la IP de origen en la lista desplegable IP de origen. Para el tráfico entrante, la IP de origen hace referencia a la dirección o direcciones (en la WAN) a las que se aplicaría la regla del firewall.

Connection Type: Inbound (WAN > LAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: All Traffic ▾

Source IP: Any ▾
Any
Single Address
Address Range

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

Las opciones disponibles se definen de la siguiente manera:

- Cualquiera: se aplica al tráfico que se origina en cualquier dirección IP de la Internet pública. Por lo tanto, deje en blanco los campos Start y Finish. Vaya al paso 4 si selecciona esta opción.
- Single Address (Dirección única): se aplica al tráfico que se origina en una única dirección IP en la Internet pública. Introduzca la dirección IP en el campo Start.
- Intervalo de direcciones: se aplica al tráfico que se origina en un intervalo de direcciones IP en la Internet pública. Ingrese la dirección IP inicial del rango en el campo Start y la dirección IP final en el campo Finish para establecer el rango.

Paso 2. Si selecciona Single Address en el paso 1, introduzca la dirección IP que se aplicará a la regla de acceso en el campo Start y, a continuación, vaya al paso 4. Si selecciona Intervalo de direcciones en el paso 1, introduzca una dirección IP inicial que se aplicará a la regla de acceso en el campo Inicio.

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status: Enable

Paso 3. Si selecciona Intervalo de direcciones en el paso 1, introduzca la dirección IP final que encapsulará el intervalo de direcciones IP para la regla de acceso en el campo Finalizar.

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status: Enable

Paso 4. Ingrese una dirección única para la IP de destino en el campo Inicio debajo de la

lista desplegable IP de destino. Para el tráfico entrante, la IP de destino se refiere a la dirección (en la LAN) a la que se permite o deniega el tráfico desde la Internet pública.

Connection Type: Inbound (WAN > LAN) ▾
Action: Allow by schedule ▾
Schedule: test_schedule ▾ [Configure Schedules](#)
Services: All Traffic ▾ [Configure Services](#)
Source IP: Address Range ▾
Start: 192.168.1.100 (Hint: 192.168.1.100)
Finish: 192.168.1.200 (Hint: 192.168.1.200)
Destination IP: Single Address ▾
Start: 10.10.14.2
Finish:
Log: Never ▾
Rule Status: Enable

Nota: Si se ha seleccionado Inbound (WAN > DMZ) como el tipo de conexión en el paso 3 de Agregar una regla de acceso, la dirección única para la IP de destino se configura automáticamente con la dirección IP del host de DMZ habilitado.

Registro y activación de la regla de acceso

Paso 1. Seleccione Always en la lista desplegable Log si desea que el router cree registros cada vez que un paquete coincida con una regla. Seleccione Never si desea que el registro no se produzca nunca cuando se coincida una regla.

Start: 192.168.1.100
Finish: 192.168.1.170
Log:
Never ▾
Never
Always
Rule Status:

Paso 2. Marque la casilla de verificación Enable para activar la regla de acceso.

Add Access Rule

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Address Range ▾

Start: 192.168.1.100

Finish: 192.168.1.170

Log: Never ▾

Rule Status: Enable

Paso 3. Haga clic en Save para guardar la configuración.

Add Access Rule

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Address Range ▾

Start: 192.168.1.100

Finish: 192.168.1.170

Log: Never ▾

Rule Status: Enable

La Tabla de Reglas de Acceso se actualiza con la regla de acceso recién configurada.

Access Rules



Configuration settings have been saved successfully

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

Filter: Action matches All

	Action	Service	Status	Connection Type	Source IP	Destination IP	Log
<input type="checkbox"/>	Allow by schedule	VOIP	Enabled	Outbound (LAN > WAN)	10.10.14.100 ~ 10.10.14.175	192.168.1.100 ~ 192.168.1.170	Never

Add Row

Edit

Enable

Disable

Delete

Reorder

Save

Cancel

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).