

Configurar reglas de acceso en un router serie RV34x

Objetivo

El ruteador VPN Dual-WAN RV340 es un dispositivo de alto rendimiento, flexible y fácil de usar que se adapta a las pequeñas empresas. Con funciones de seguridad añadidas, como filtrado web, control de aplicaciones y protección de código fuente IP. El nuevo RV340 ofrece conectividad por cable, de banda ancha y muy segura a oficinas pequeñas y empleados remotos. Estas nuevas funciones de seguridad también facilitan el ajuste de la actividad permitida en la red.

Las reglas de acceso o las políticas del router serie RV34x permiten configurar reglas para aumentar la seguridad en la red. Una combinación de reglas y una lista de control de acceso (ACL). Las ACL son listas que bloquean o permiten el envío del tráfico hacia y desde determinados usuarios. Las reglas de acceso se pueden configurar para que estén en vigor todo el tiempo o en función de las programaciones definidas.

Las ACL tienen una negación implícita al final de la lista, por lo que a menos que lo permita explícitamente, el tráfico no puede pasar. Por ejemplo, si desea permitir que todos los usuarios accedan a una red a través del router excepto para direcciones específicas, debe denegar las direcciones particulares y luego permitir todas las demás.

El objetivo de este artículo es mostrarle cómo configurar las reglas de acceso en un router serie RV34x.

Dispositivos aplicables

- Serie RV34x

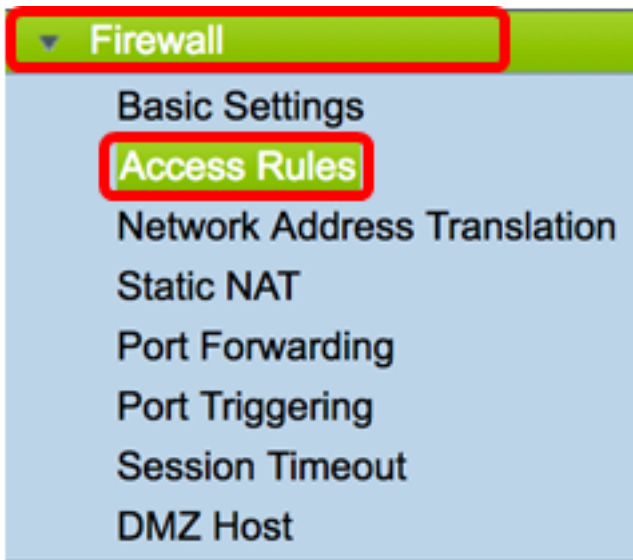
Versión del software

- 1.0.1.16
 - [Desde la publicación de este artículo, se encuentra disponible un firmware para actualizar la interfaz de usuario. Haga clic aquí para ir a la página de descargas y localizar allí su producto específico.](#)

Configuración de una regla de acceso en un router serie RV34x

Crear una regla de acceso

Paso 1. Inicie sesión en la utilidad basada en web del router y elija **Firewall > Access Rules**.

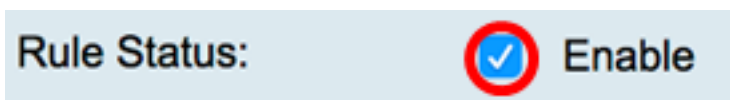


Paso 2. En la tabla Reglas de acceso IPv4 o IPv6, haga clic en **Agregar** para crear una nueva regla.

Nota: En el router serie RV34x, es posible configurar hasta 202 reglas. En este ejemplo, se utiliza IPv4.

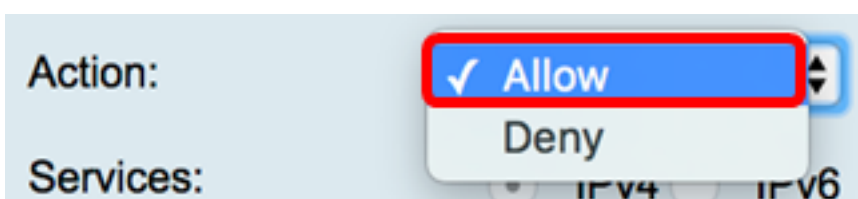


Paso 3. Marque la casilla de verificación **Enable Rule Status** para habilitar la regla.



Paso 4. En el menú desplegable Acción, elija si la directiva permitirá o denegará datos.

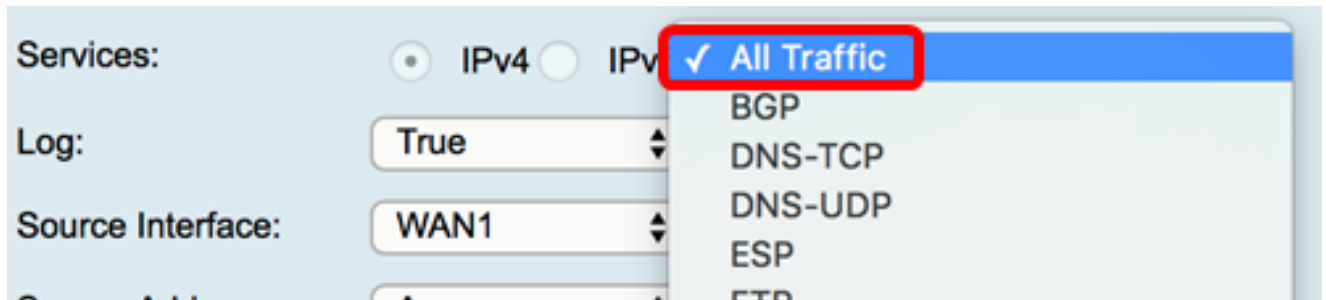
Nota: En este ejemplo, se elige Permitir.



Paso 5. En el menú desplegable Servicios, elija el tipo de tráfico que el router permitirá o

denegará.

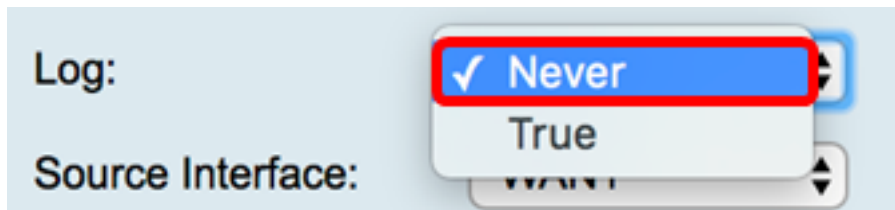
Nota: Para este ejemplo, se elige Todo el tráfico. Se permitirá todo el tráfico.



Paso 6. En el menú desplegable Registro, elija una opción para determinar si el router registrará el tráfico permitido o denegado. Las opciones son:

- Nunca: el router nunca registrará ningún tráfico permitido y denegado.
- True: el router registrará el tráfico que coincida con la política.

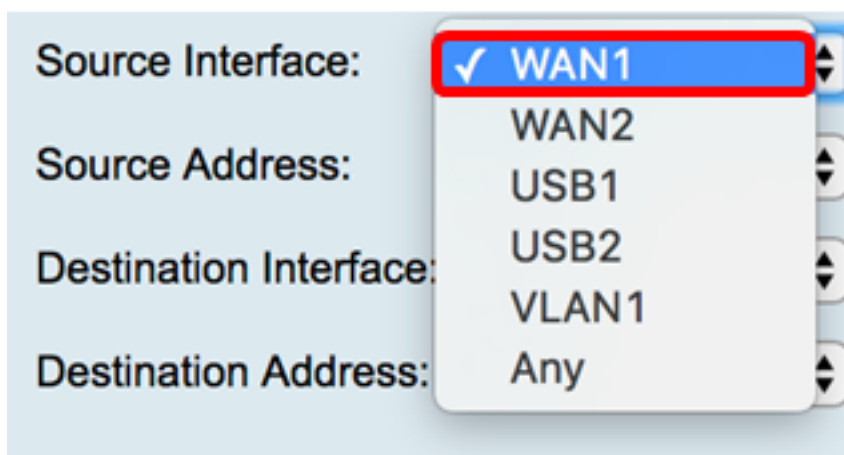
Nota: En este ejemplo, Nunca se elige.



Paso 7. En el menú desplegable Interfaz de origen, elija una interfaz para el tráfico entrante o entrante donde se debe aplicar la política de acceso. Las opciones son

- WAN1: la política se aplica solamente al tráfico de WAN1.
- WAN2: la política se aplica solamente al tráfico de WAN2.
- USB1: la política se aplica solamente al tráfico de USB1.
- USB2: la política se aplica solamente al tráfico de USB2.
- VLAN1: la política se aplica solamente a la VLAN1 de tráfico.
- Any: la política se aplica a cualquier interfaz.

Nota: Si se ha configurado una red de área local virtual (VLAN) adicional, aparecerá la opción VLAN en la lista. En este ejemplo, se elige WAN1.

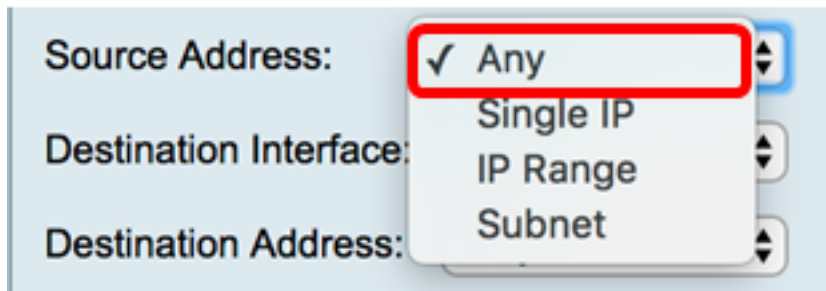


Paso 8. En el menú desplegable Dirección de origen, elija un origen para aplicar la política.

Las opciones son:

- Any: la política se aplicará a cualquier dirección IP de la red. Si selecciona esta opción, vaya directamente al [Paso 12](#).
- IP única: la política se aplica a un solo host o dirección IP. Si selecciona esta opción, vaya directamente al [paso 9](#).
- Intervalo IP: la política se aplica a un conjunto o rango de direcciones IP. Si selecciona esta opción, vaya directamente al [Paso 10](#).
- Subred: la política se aplica a toda una subred. Si selecciona esta opción, vaya directamente al [Paso 11](#).

Nota: En este ejemplo, se elige Any (Cualquiera).



The screenshot shows a configuration window with three fields: 'Source Address:', 'Destination Interface:', and 'Destination Address:'. A dropdown menu is open for 'Source Address:', showing four options: 'Any' (selected with a checkmark), 'Single IP', 'IP Range', and 'Subnet'. The 'Any' option is highlighted with a red box.

[Paso 9](#). (Opcional) En el Paso 8 se eligió una única IP, introduzca una única dirección IP para la política que se aplicará y, a continuación, vaya directamente al [Paso 12](#).

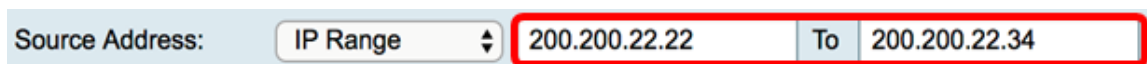
Nota: Para este ejemplo, se utiliza 200.200.22.52.



The screenshot shows a configuration window with a 'Source Address:' field. The dropdown menu is set to 'Single IP'. The input field contains the IP address '200.200.22.52', which is highlighted with a red box.

[Paso 10](#). (Opcional) Si se eligió el rango de IP en el paso 8, introduzca las direcciones IP inicial y final en los campos de dirección IP correspondientes.

Nota: En este ejemplo, 200.200.22.22 se utiliza como dirección IP inicial y 200.200.22.34 como dirección IP final.



The screenshot shows a configuration window with a 'Source Address:' field. The dropdown menu is set to 'IP Range'. The input fields contain the IP range '200.200.22.22 To 200.200.22.34', which is highlighted with a red box.

[Paso 11](#). (Opcional) Si se eligió Subred en el Paso 8, introduzca el ID de red y su máscara de subred respectiva para aplicar la política.

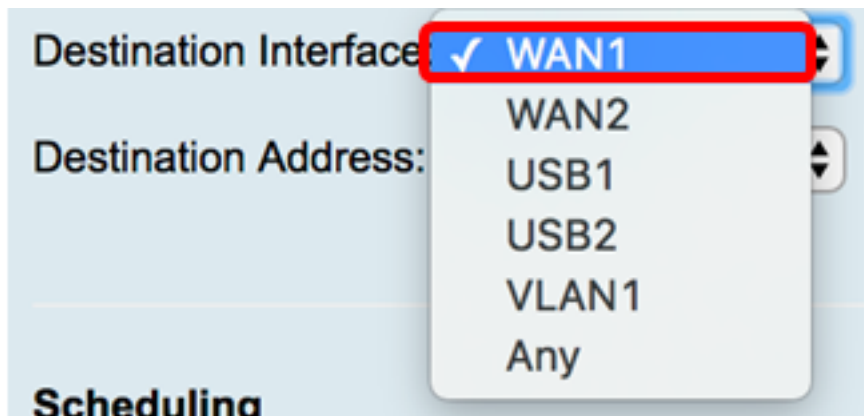
Nota: En este ejemplo, 200.200.22.1 se utiliza como ID de subred y 24 como máscara de subred.



The screenshot shows a configuration window with a 'Source Address:' field. The dropdown menu is set to 'Subnet'. The input field contains the subnet '200.200.22.1 / 24', which is highlighted with a red box.

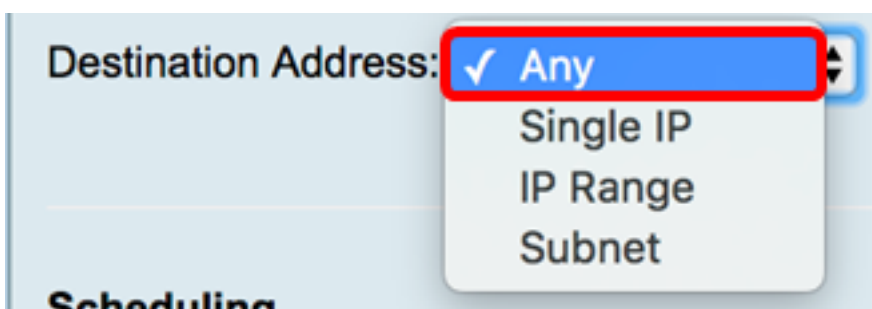
[Paso 12](#). En el menú desplegable Destination Interface, elija una interfaz para el tráfico saliente o saliente donde se debe aplicar la política de acceso. Las opciones son WAN1, WAN2, USB1, USB2, VLAN1 y Any.

Nota: Para este ejemplo, se elige WAN1.



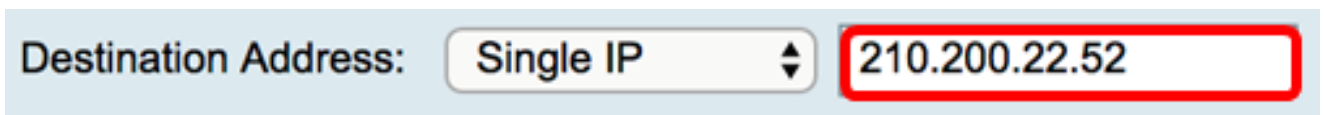
Paso 13. En el menú desplegable Destination Address (Dirección de destino), elija un destino para aplicar la política. Las opciones son Any (Cualquiera), Single IP (IP única), IP Range (Intervalo IP), Subnet (Subred).

Nota: En este ejemplo, se elige Any (Cualquiera). Saltar al [Paso 17](#).



Paso 14. (Opcional) Si se eligió una sola IP en el Paso 13, introduzca una sola dirección IP para la política que se aplicará.

Nota: Para este ejemplo, se utiliza 210.200.22.52.



Paso 15. (Opcional) Si se eligió IP Range en el Paso 13, introduzca las direcciones IP inicial y final en los campos de dirección IP correspondientes.

Nota: En este ejemplo, 210.200.27.22 se utiliza como dirección IP inicial y 210.200.27.34 como dirección IP final. Saltar al [Paso 17](#).

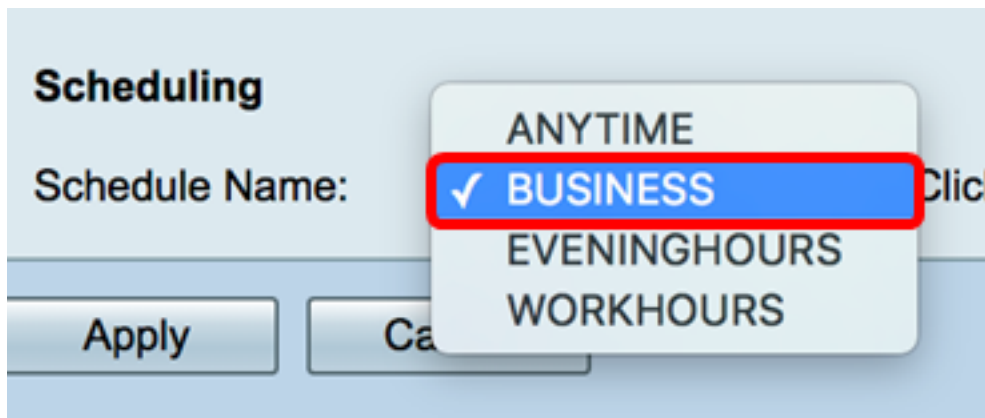


Paso 16. (Opcional) Si se eligió Subnet en el Paso 13, introduzca la dirección de red y su máscara de subred respectiva para aplicar la política.

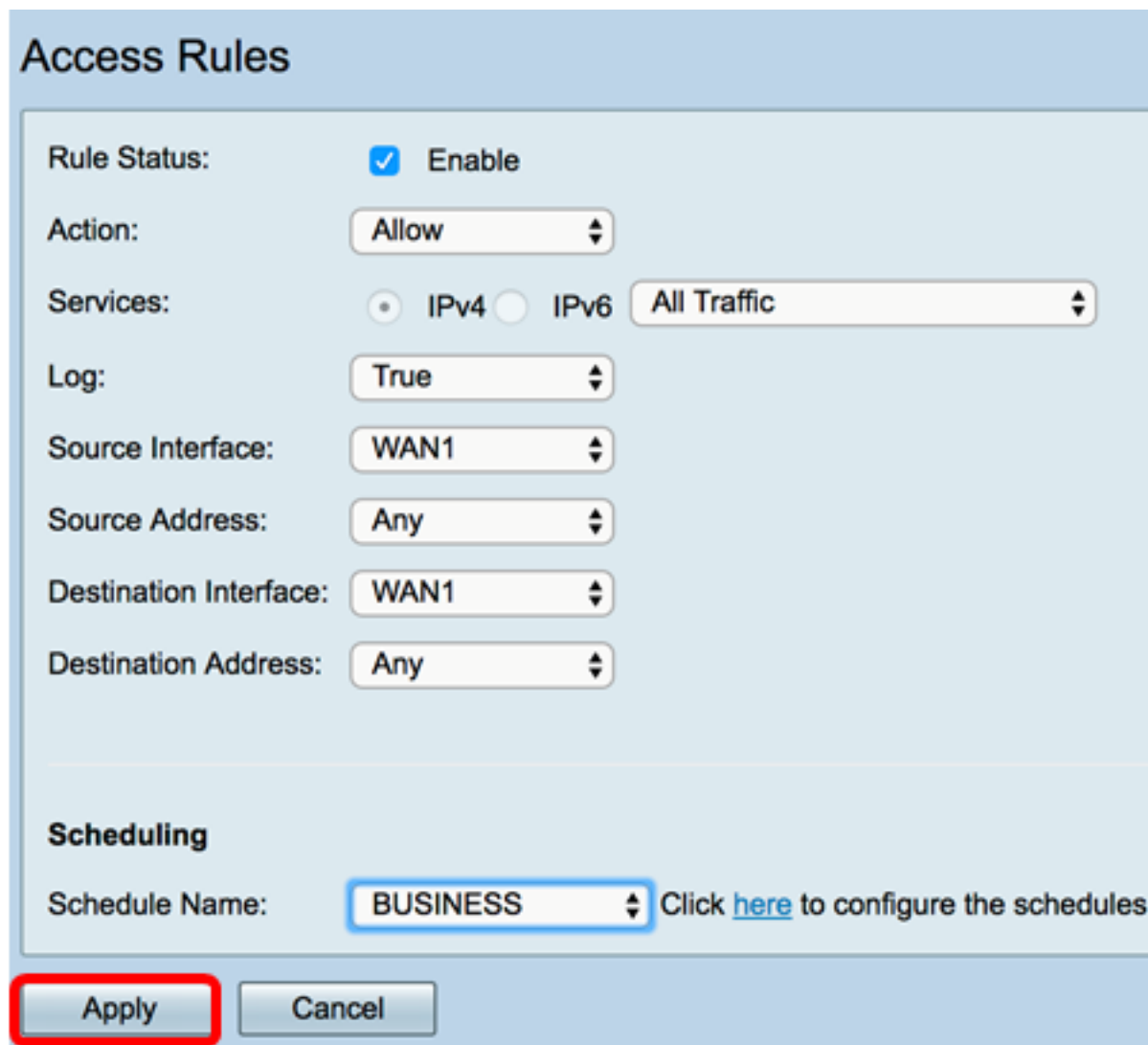
Nota: En este ejemplo, 210.200.27.1 se utiliza como dirección de subred y 24 como máscara de subred.



[Paso 17](#). En la lista desplegable Nombre de programación, elija una programación para aplicar esta política. Para aprender a configurar una programación, haga clic [aquí](#).



Paso 18. Haga clic en Apply (Aplicar).



Ahora debería haber creado correctamente una regla de acceso en un router de la serie RV.

Editar una regla de acceso

Paso 1. En la tabla de reglas de acceso IPv4 o IPv6, active la casilla de verificación junto a la regla de acceso que desea configurar.

Nota: En este ejemplo, en la Tabla de Reglas de Acceso IPv4, se elige Prioridad 1.

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

Paso 2. Haga clic en **Editar**.

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

Paso 3. (Opcional) En la columna Configurar, haga clic en el botón **Editar** en la fila de la regla de acceso deseada.

Schedule	Configure			
BUSINESS	<input checked="" type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
BUSINESS	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
ANYTIME	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
ANYTIME	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>
ANYTIME	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>

Paso 4. Actualice los parámetros necesarios.

Access Rules

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface:

Destination Address:

Scheduling

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

Apply

Cancel

Paso 5. Haga clic en Apply (Aplicar).

Access Rules

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface:

Destination Address:

Scheduling

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

Paso 6. (Opcional) Para cambiar la prioridad de una regla de acceso en la columna Configurar, haga clic en el botón **Arriba** o **Abajo** de la regla de acceso que desea mover.

Nota: Cuando una regla de acceso se mueve hacia arriba o hacia abajo, se mueve un paso por encima o por debajo de su posición original. En este ejemplo, la Prioridad 1 se desplazará hacia abajo.

Priority	Enable	Action	Service	Source Interf...	Source	Destinat...	Destination	Schedule	Configure
<input type="checkbox"/> 1	<input checked="" type="checkbox"/>	Allowed	IPv4: All T...	WAN1	Any	USB1	192.168.1.1	BUSINESS	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
<input type="checkbox"/> 2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1	Any	WAN1	Any	BUSINESS	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
<input type="checkbox"/> 3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1	Any	USB2	Any	ANYTIME	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
<input type="checkbox"/> 201	<input checked="" type="checkbox"/>	Allowed	IPv4: All T...	VLAN	Any	WAN	Any	ANYTIME	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
<input type="checkbox"/> 202	<input checked="" type="checkbox"/>	Denied	IPv4: All T...	WAN	Any	VLAN	Any	ANYTIME	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>

Nota: En este ejemplo, la Prioridad 1 es ahora Prioridad 2.

IPv4 Access Rules Table										
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Inter...	Source	Destina...	Destination	Schedule	Configure
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1	Any	WAN1	Any	BUSINESS	Edit Delete Up Down
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Allowed	IPv4: All Tr...	WAN1	Any	USB1	192.168.1.1	BUSINESS	Edit Delete Up Down
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1	Any	USB2	Any	ANYTIME	Edit Delete Up Down
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Tr...	VLAN	Any	WAN	Any	ANYTIME	Edit Delete Up Down
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Tr...	WAN	Any	VLAN	Any	ANYTIME	Edit Delete Up Down

Add Edit Delete

Paso 7. Haga clic en Apply (Aplicar).

Access Rules

IPv4 Access Rules Table

<input type="checkbox"/>	Priority	Enable	Action	Service	Source Inter
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

Add Edit Delete

IPv6 Access Rules Table

<input type="checkbox"/>	Priority	Enable	Action	Service	Source Inter
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv6: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv6: All Traffic	WAN

Add Edit Delete

Apply Restore to Default Rules Service Management

Ahora debería haber editado correctamente una regla de acceso en un router serie RV34x.

Eliminación de una regla de acceso

Paso 1. En la tabla de reglas de acceso IPv4 o IPv6, active la casilla de verificación junto a la regla de acceso que desea eliminar.

Nota: En este ejemplo, en la Tabla de Reglas de Acceso IPv4, se elige Prioridad 1.

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

Paso 2. Haga clic en **Eliminar** ubicado debajo de la tabla o haga clic en el botón Eliminar en la columna Configurar.

IPv4 Access Rules Table					
<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

Paso 3. Haga clic en Apply (Aplicar).

Access Rules

IPv4 Access Rules Table

<input type="checkbox"/>	Priority	Enable	Action	Service	Source
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Denied	IPv4: BGP	WAN1
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	Allowed	IPv4: FTP	WAN1
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN

IPv6 Access Rules Table

<input type="checkbox"/>	Priority	Enable	Action	Service	Source
<input type="checkbox"/>	201	<input checked="" type="checkbox"/>	Allowed	IPv6: All Traffic	VLAN
<input type="checkbox"/>	202	<input checked="" type="checkbox"/>	Denied	IPv6: All Traffic	WAN

Ahora debería haber eliminado correctamente una regla de acceso en el router serie RV34x.

[Ver un vídeo relacionado con este artículo...](#)

[Haga clic aquí para ver otras charlas técnicas de Cisco](#)