

Configuración de las reglas de acceso en los routers de las series RV160 y RV260

Objetivo

El router es responsable de recibir datos de la red externa y es la primera línea de defensa en lo que respecta a la seguridad de la red local. Al habilitar las reglas de acceso en el router, puede filtrar los paquetes según parámetros específicos como la dirección IP o el número de puerto. Con los pasos proporcionados a continuación, este documento tiene como objetivo guiarle en la configuración de las reglas de acceso para controlar mejor los paquetes que ingresan a su red. Este documento también resaltaré algunas prácticas recomendadas para utilizar las reglas de acceso a todo su potencial para lograr la mejor seguridad.

Dispositivos aplicables

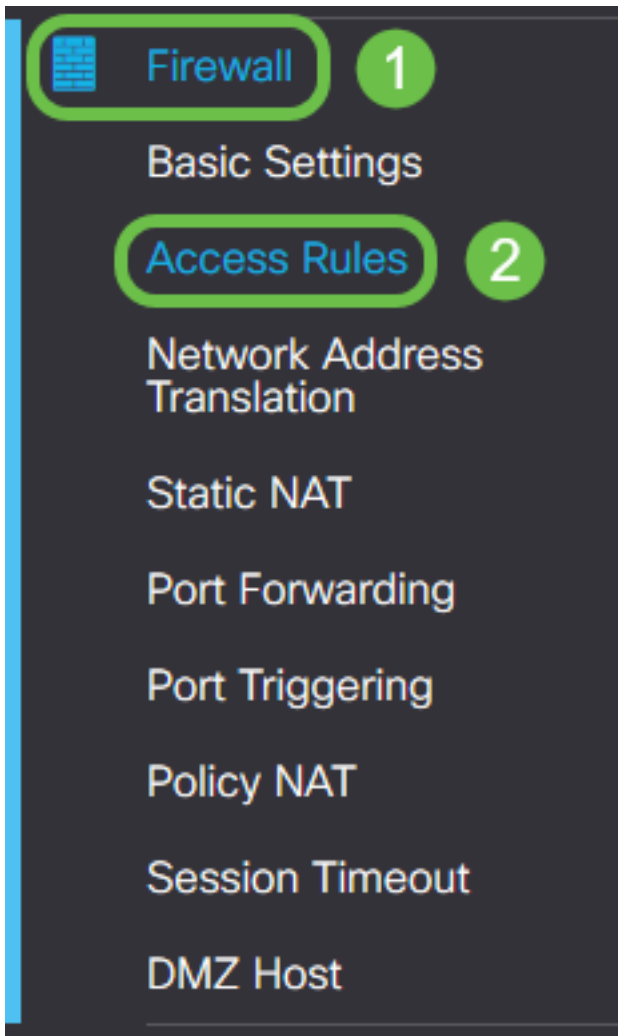
- RV160x
- RV260x

Versión del software

- 1.0.00.13

Configurar reglas de acceso

Paso 1. En el panel de navegación del lado izquierdo de la utilidad de configuración, seleccione **Firewall > Reglas de acceso**.



Aparecerá la página Access Rules (Normas de acceso). En esta página hay tablas que contienen listas de reglas de acceso y sus atributos para IPv4 e IPv6 respectivamente. Desde aquí puede agregar una nueva regla de acceso, editar una existente o quitar una existente.

Agregar/editar una regla de acceso

Paso 2. Para agregar una nueva regla de acceso, haga clic en el icono azul para agregar en la tabla Reglas de acceso IPv4 o Reglas de acceso IPv6, según el protocolo al que desee aplicar la regla. En este caso, se utiliza IPv4.

IPv4 Access Rules Table



Para editar una entrada existente, active la casilla de verificación situada junto a la regla de acceso que desea modificar. A continuación, seleccione el icono de edición azul en la parte superior de la tabla correspondiente. Sólo se puede seleccionar una regla a la vez para editarla.

IPv4 Access Rules Table

<input checked="" type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	Any	Any	Any
<input type="checkbox"/>	201	Enabled	Allowed	All Traffic	VLAN	Any	WAN
<input type="checkbox"/>	202	Enabled	Denied	All Traffic	WAN	Any	VLAN

Aparece la página *Agregar/Editar reglas de acceso*.

Paso 3. Marque o desmarque la casilla de verificación Estado de regla para activar o desactivar la regla de acceso durante la operación. Esto es útil cuando tiene una regla de acceso que desea guardar para aplicar en una fecha posterior.

Add/Edit Access Rules

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6

Paso 4. En el campo *Acción*, seleccione si la regla debe permitir o denegar el acceso al tráfico de red entrante para que se especifique.

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

Log: Always Never

Source Interface: Any

Nota: Se recomienda que la mejor seguridad establezca reglas de acceso que permitan solamente el tráfico que espera recibir, en lugar de intentar sólo denegar el tráfico no deseado. Esto protegerá mejor su red frente a amenazas desconocidas.

Paso 5. En el campo *Services*, seleccione en el menú desplegable el tipo de servicio de red al que desea aplicar la regla de acceso.

Add/Edit Access Rules

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

Log: Always Never

Source Interface: Any

Nota: El botón de opción IPv4 o IPv6 se selecciona automáticamente en función de la tabla a la que se ha seleccionado aplicar la regla de acceso desde la página *Access Rules*.

Paso 6. Seleccione en el campo *Log* si desea que el router genere un mensaje de registro una vez que los paquetes que ingresan a su red coincidan con las reglas aplicadas.

Rule Status: Enable

Action: Allow Deny

Services: IPv4 IPv6 All Traffic

Log: Always Never

Source Interface: Any

Paso 7. En la lista desplegable *Interfaz de Origen*, seleccione la interfaz de red para los paquetes entrantes a los que se aplicará la regla de acceso.

Log: Always Never

Source Interface: Any

Source Address:

Destination Interface: Any

Destination Address: Any

Paso 8. Seleccione en la lista desplegable *Dirección de origen* el tipo de dirección entrante al que se aplicará la regla de acceso. Las opciones son las siguientes:

- Any - La regla se aplicará a cualquier dirección IP entrante
- Single - La regla se aplicará a una única dirección IP definida
- Subred: la regla se aplicará a una subred definida de una red
- Intervalo IP: la regla se aplicará a un intervalo definido de direcciones IP

Nota: Si selecciona Single (Single), Subnet (Subred) o IP Range (Intervalo IP), aparecerán los campos correspondientes a la derecha del menú desplegable, donde podrá introducir los detalles de la dirección. En este ejemplo, se ingresa un rango IP para demostrar.

Source Interface: Any

Source Address: IP Range 1.2.3.1 To 1.2.3.100 (1.2.3.1 To 1.2.3.4)

Destination Interface: Any

Destination Address: IP Range

Paso 9. En la lista desplegable *Interfaz de destino*, seleccione la interfaz de red para los paquetes

salientes a los que se aplicará la regla de acceso.

The screenshot shows a configuration form with the following fields:

- Log: Always Never
- Source Interface: Any
- Source Address: Any
- Destination Interface: Any (dropdown menu is open, showing options: WAN, USB, VLAN1, Any)
- Destination Address:

The 'Destination Interface' dropdown menu is highlighted with a green rounded rectangle. Below the form, the word 'Schedule' is visible.

Paso 10. Seleccione en la lista desplegable *Dirección de destino* el tipo de dirección saliente al que se aplicará la regla de acceso. Las opciones son las siguientes:

- Any - La regla se aplicará a cualquier dirección IP saliente
- Single - La regla se aplicará a una única dirección IP definida
- Subred: la regla se aplicará a una subred definida de una red
- Intervalo IP: la regla se aplicará a un intervalo definido de direcciones IP

Nota: Si selecciona Single (Single), Subnet (Subred) o IP Range (Intervalo IP), aparecerán los campos correspondientes a la derecha del menú desplegable, donde podrá introducir los detalles de la dirección. En este ejemplo, se ingresa una subred para demostrar.

The screenshot shows a configuration form with the following fields:

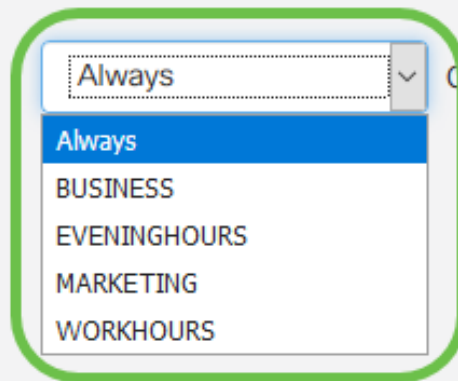
- Destination Interface: Any
- Destination Address: Subnet (dropdown menu is open, showing options: Any, Single, Subnet, IP Range)
- Schedule Name: Always

The 'Destination Address' dropdown menu and its associated input fields (1.2.3.4 / 16) are highlighted with a green rounded rectangle. Below the form, the text 'Click [here](#) to configure the schedules.' is visible.

Paso 11. En la lista desplegable *Nombre de programación*, seleccione la programación de tiempo a la que desea aplicar la regla de acceso.

Schedule

Schedule Name:

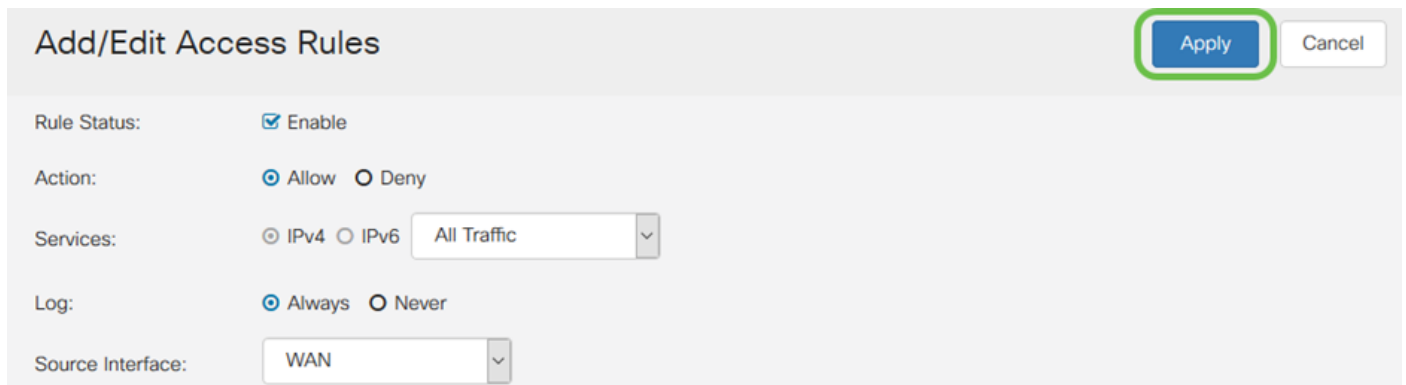
A dropdown menu with a green border. The selected option is 'Always'. Other options listed are BUSINESS, EVENINGHOURS, MARKETING, and WORKHOURS.

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

Nota: Para aumentar la seguridad, se recomienda restringir el acceso no crítico a la red durante el horario comercial para asegurarse de que se nieguen las conexiones no deseadas cuando su empresa no esté en funcionamiento.

Nota: Haga clic en el enlace situado a la derecha del menú desplegable *Nombre de programación* si desea configurar las horas de programación para las reglas de acceso. Puede encontrar más información sobre cómo configurar estas programaciones [aquí](#).

Paso 12. Cuando esté satisfecho con la configuración de la regla de acceso, haga clic en **Aplicar** para confirmar.

A form titled 'Add/Edit Access Rules' with an 'Apply' button highlighted in green. The form contains the following fields:


- Rule Status: Enable
- Action: Allow Deny
- Services: IPv4 IPv6 All Traffic
- Log: Always Never
- Source Interface: WAN

Ahora volverá a la página principal *Access Rules*.

Nota: Cuando se crea una nueva regla de acceso, su prioridad se coloca en la parte inferior de la lista. Esto significa que si una regla de acceso entra en conflicto con otra en un parámetro específico, las restricciones de la regla de prioridad más alta tendrán prioridad. Para mover una regla hacia arriba o hacia abajo en prioridad, puede utilizar las flechas azules situadas en la columna Configurar.

IPv4 Access Rules Table



<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	WAN	1.2.3.1-1.2.3.100	WAN	1.2.3.4/16	BUSINESS	

Paso 13 (opcional). Si desea devolver la lista de reglas de acceso a la predeterminada, haga clic en **Restaurar valores predeterminados** en la esquina superior derecha de la página.

Access Rules

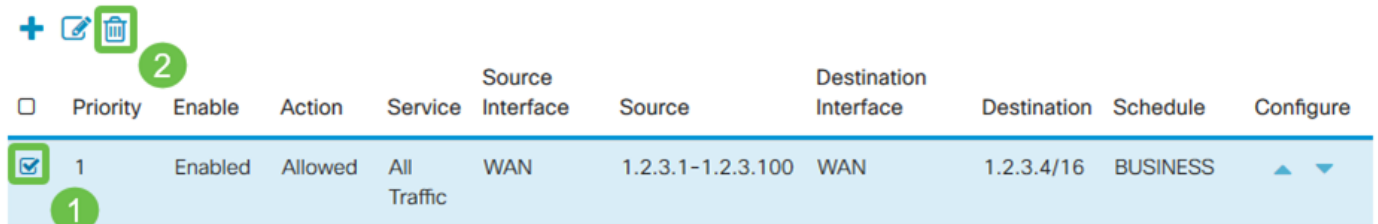
Apply

Restore Defaults

Eliminar una regla de acceso

Paso 14. Para quitar una regla de acceso de la lista, simplemente seleccione la casilla de verificación de la regla correspondiente que desea eliminar. A continuación, seleccione el icono de la papelera azul en la parte superior de la lista. Se pueden eliminar varias entradas de regla de acceso a la vez.

IPv4 Access Rules Table



<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	WAN	1.2.3.1-1.2.3.100	WAN	1.2.3.4/16	BUSINESS	▲ ▼

Administración de servicio

La administración de servicios permite agregar o editar servicios de red existentes por su número de puerto, protocolo y otros detalles. Estos servicios de red estarán disponibles en el menú desplegable Servicios al configurar las reglas de acceso. A través del menú de configuración de la lista de administración de servicios, puede crear servicios personalizados que luego se pueden aplicar a las reglas de acceso para un control más preciso del tráfico que entra en la red. Para obtener más información sobre cómo configurar Service Management, haga clic [aquí](#).

Conclusión

Las reglas de acceso cuando se aplican correctamente son una herramienta valiosa para proteger la conexión WAN. Con la guía anterior y las prácticas descritas anteriormente, debe disponer de todo lo necesario para configurar correctamente las reglas de acceso seguro para el router RV160x o RV260x.