

Configuración de reglas de acceso en routers VPN RV320 y RV325

Objetivo

Las listas de control de acceso (ACL) son listas que bloquean o permiten el envío del tráfico a determinados usuarios y desde ellos. Las reglas de acceso se pueden configurar para que estén en vigor todo el tiempo o en función de una programación definida. Una regla de acceso se configura en función de varios criterios para permitir o denegar el acceso a la red. La regla de acceso se programa en función del momento en que se deben aplicar las reglas de acceso al router. En este artículo se describe y describe el Asistente de configuración de reglas de acceso utilizado para determinar si el tráfico puede entrar en la red a través del firewall del router o no para garantizar la seguridad en la red.

Dispositivos aplicables | Versión del firmware

- Router VPN Dual WAN RV320 | V 1.1.0.09 ([Descarga más reciente](#))
- Router VPN Dual WAN RV325 Gigabit | V 1.1.0.09 ([Descarga más reciente](#))

Configuración de regla de acceso

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



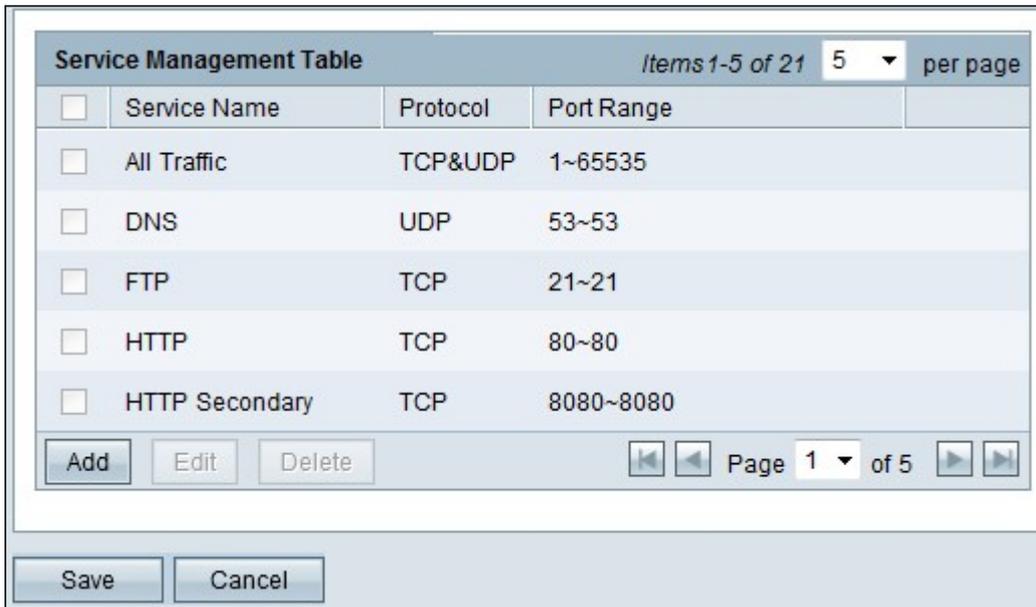
Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	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	

La Tabla de Reglas de Acceso contiene la siguiente información:

- Prioridad: muestra la prioridad de la regla de acceso
- Enable (Activar): muestra si la regla de acceso está activada o desactivada
- Acción: muestra que la regla de acceso está permitida o denegada.
- Servicio: muestra el tipo de servicio.
- SourceInterface: muestra a qué interfaz se aplica la regla de acceso.
- Origen: muestra la dirección IP del dispositivo de origen
- Destino: muestra la dirección IP del dispositivo de destino
- Hora: muestra la hora a la que se aplicará la regla de acceso
- Día: muestra durante una semana cuando se aplica la regla de acceso

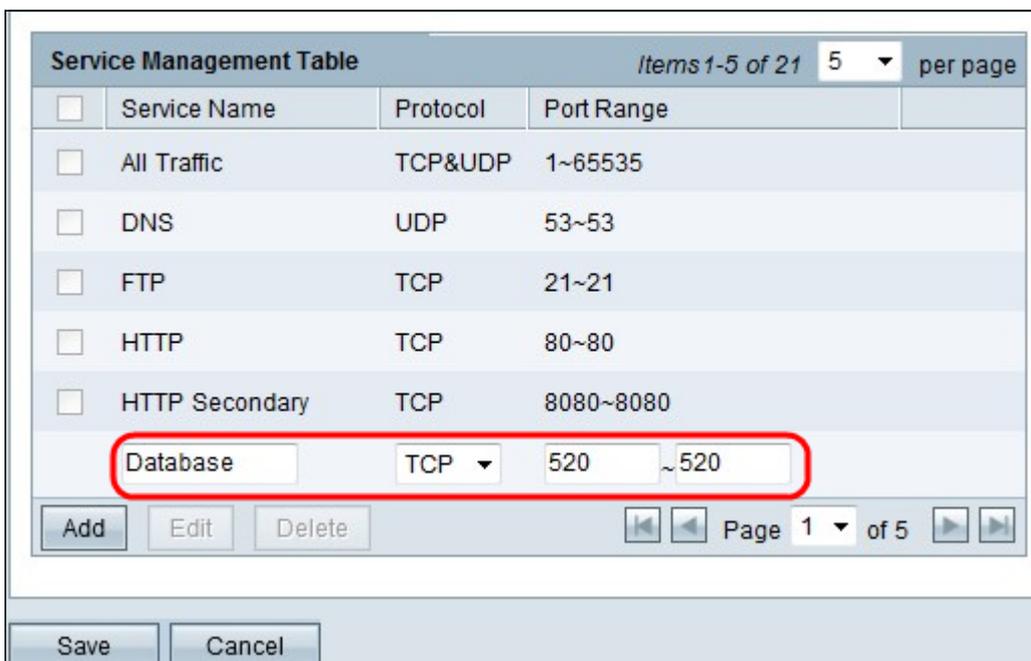
Administración de servicio

Paso 1. Haga clic en **Administración de servicios** para agregar un nuevo servicio. Se abre la página de la tabla *Administración de servicios*:



The screenshot shows a web interface titled "Service Management Table". At the top right, it says "Items 1-5 of 21" and "5 per page". Below this is a table with the following columns: "Service Name", "Protocol", and "Port Range". The table contains five rows of existing services: "All Traffic" (TCP&UDP, 1~65535), "DNS" (UDP, 53~53), "FTP" (TCP, 21~21), "HTTP" (TCP, 80~80), and "HTTP Secondary" (TCP, 8080~8080). Each row has a checkbox to its left. Below the table are three buttons: "Add", "Edit", and "Delete". At the bottom of the interface are "Save" and "Cancel" buttons.

Paso 2. Haga clic en **Agregar** para agregar un nuevo servicio.



This screenshot is similar to the previous one, but a new service entry is being added. The entry is highlighted with a red rectangle and contains the following information: "Database" in the Service Name field, "TCP" in the Protocol dropdown, and "520 ~ 520" in the Port Range field. The "Add" button is visible below the table.

Paso 3. Configure los siguientes campos.

- Nombre del servicio: en función de sus requisitos, indique un nombre para el servicio
- Protocolo: elija un protocolo TCP o UDP para su servicio
- Port Range (Intervalo de puertos): introduzca el intervalo de números de puertos según sus requisitos y el número de puerto debe estar en el intervalo (1-65536).

Paso 4. Haga clic en **Guardar** para guardar los cambios

Configuración de regla de acceso en IPv4

Access Rules

IPv4 IPv6

Access Rules Table Items 1-5 of 5 5 per page

	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
<input type="radio"/>		<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always	

Page 1 of 1

Paso 1. Haga clic en **Agregar** para configurar una nueva regla de acceso. Aparecerá la ventana *Editar reglas de acceso*.

Edit 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. Elija la opción adecuada en la lista desplegable Acción para permitir o restringir el tráfico para la regla que está a punto de configurar. Las reglas de acceso limitan el acceso a la red en función de diversos valores.

- Permitir: permite todo el tráfico.
- Denegar: restringe todo el tráfico.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP:

Destination IP:

Scheduling

Time:

From:

To:

Effective on:

Mon Tue Wed Thu Fri Sat

Paso 3. Elija el servicio adecuado que debe filtrar en la lista desplegable Servicio.

Edit 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. Elija la opción Registro adecuada en la lista desplegable Registro. La opción de registro determina si el dispositivo mantiene un registro del tráfico que corresponde al conjunto de reglas de acceso.

- Paquetes de registro que coinciden con esta regla de acceso: el router mantiene un registro que realiza un seguimiento del servicio seleccionado.
- Not Log: el router no guarda registros para la regla de acceso.

Edit 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. En la lista desplegable Interfaz, elija la interfaz de origen adecuada. En esta interfaz se aplica la regla de acceso.

- LAN: la regla de acceso afecta sólo al tráfico LAN.
- WAN 1: la regla de acceso afecta sólo al tráfico WAN 1.
- WAN 2: la regla de acceso sólo afecta al tráfico WAN 2.
- Any: la regla de acceso afecta a todo el tráfico en cualquiera de las interfaces del dispositivo.

Edit 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 el tipo de IP de origen adecuado al que se aplica la regla de acceso en la lista desplegable IP de origen.

- Any — Cualquier dirección IP de la red del dispositivo tiene la regla aplicada a ellos.
- Single: sólo una única dirección IP especificada en la red del dispositivo tiene la regla aplicada. Introduzca la dirección IP deseada en el campo adyacente.
- Rango: sólo un rango especificado de direcciones IP en la red del dispositivo tienen la regla aplicada a ellas. Si selecciona Range (Intervalo), debe introducir las direcciones IP primera y última del intervalo en los campos adyacentes.

Edit Access Rules

Services

Action:

Service:

Log:

Source Interface:

Source IP: To

Destination IP:

- ANY
- Single
- Range

Scheduling

Time:

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu

Paso 7. Elija el tipo de IP de destino adecuado al que se aplica la regla de acceso en la lista desplegable disponible.

- Any — Cualquier dirección IP de destino tiene la regla aplicada a ellos.
- Single: sólo una única dirección IP especificada tiene la regla aplicada. Introduzca la dirección IP deseada en el campo adyacente.
- Rango: sólo un rango especificado de dirección IP fuera del alcance de la red del dispositivo tiene la regla aplicada a ellos. Si selecciona Range (Intervalo), debe introducir las direcciones IP primera y última del intervalo en los campos adyacentes.

Scheduling

Time:

- Always
- Interval

From: (hh:mm)

To: (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Timesaver: De forma predeterminada, la hora se establece en Always (Siempre). Si desea aplicar la regla de acceso a una hora o un día específicos, siga el paso 8 al paso 11. Si no es así, vaya

directamente al paso 12.

Paso 8. Elija **Interval** en la lista desplegable, las reglas de acceso están activas durante algunas horas específicas. debe introducir el intervalo de tiempo para que se aplique la regla de acceso.

Scheduling

Time: Interval ▾

From: 3:00 (hh:mm)

To: 7:00 (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel Back

Paso 9. Introduzca la hora a la que desea empezar a aplicar la lista de acceso en el campo Desde. El formato de la hora es hh:mm.

Paso 10. Introduzca la hora a la que no desea aplicar la lista de acceso en el campo Para. El formato de la hora es hh:mm.

Scheduling

Time: Interval ▾

From: 3:00 (hh:mm)

To: 7:00 (hh:mm)

Effective on: Everyday Sun Mon Tue Wed Thu Fri Sat

Save Cancel Back

Paso 11. Active la casilla de verificación de los días específicos en los que desea aplicar la lista de acceso.

Paso 12. Haga clic en **Guardar** para guardar los cambios.

Access Rules

IPv4 IPv6

Access Rules Table Items 1-5 of 6 5 ▾

Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
1 ▾	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	192.168.1.10 ~ 192.168.1.100	Any	03:00 ~ 07:00	All week
<input type="radio"/>	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always	
<input type="radio"/>	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always	
<input type="radio"/>	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always	
<input type="radio"/>	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always	

Add Edit Delete Restore to Default Rules Service Management... Page 1 of 2

Paso 13. (Opcional) Si desea restaurar las reglas predeterminadas, haga clic en **Restaurar a las reglas predeterminadas**. Se perderán todas las reglas de acceso configuradas por usted.

Configuración de regla de acceso en IPv6

The screenshot shows the 'Access Rules' configuration page. At the top, there are two tabs: 'IPv4' and 'IPv6'. The 'IPv6' tab is selected and highlighted with a red circle. Below the tabs is a table titled 'Access Rules Table' with columns: Priority, Enable, Action, Service, SourceInterface, Source, Destination, Time, and Day. The table contains five rows of rules. At the bottom, there are buttons for 'Add', 'Edit', 'Delete', 'Restore to Default Rules', and 'Service Management...'. The 'Add' button is highlighted with a red circle.

Paso 1. Haga clic en la ficha IPv6 para configurar las reglas de acceso IPv6.

The screenshot shows the 'Access Rules' configuration page with the 'IPv6' tab selected. The 'Access Rules Table' is visible with the same five rows of rules. At the bottom, the 'Add' button is highlighted with a red circle.

Paso 2. Haga clic en Agregar para agregar una nueva regla de acceso IPv6. Aparecerá la ventana *Editar reglas de acceso*.

The screenshot shows the 'Edit Access Rules' dialog box. It has several fields: 'Action' (set to 'Allow'), 'Service' (set to '[TCP&UDP/1~65535]'), 'Log' (set to 'No Log'), 'Source Interface' (set to 'LAN'), 'Source IP / Prefix Length' (set to 'ANY'), and 'Destination IP / Prefix Length' (set to 'ANY'). The 'Action' dropdown menu is open, and the 'Allow' option is highlighted with a red circle. At the bottom, there are buttons for 'Save', 'Cancel', and 'Back'.

Paso 3. Elija la opción adecuada en la lista desplegable Acción para permitir o restringir la regla que necesita configurar. Las reglas de acceso limitan el acceso a la red al permitir o denegar el acceso al tráfico desde servicios o dispositivos específicos.

- Permitir: permite todo el tráfico.
- Denegar: restringe todo el tráfico.

Edit Access Rules

Services

Action: Allow

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

Log:

Source Interface:

Source IP / Prefix Length:

Destination IP / Prefix Length:

Save Cancel

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]
 SMTP [TCP/25~25]
 TELNET [TCP/23~23]
 TELNET Secondary [TCP/8023~8023]
 TELNET SSL [TCP/992~992]
 DHCP [UDP/67~67]
 L2TP [UDP/1701~1701]
 PPTP [TCP/1723~1723]
 IPSec [UDP/500~500]
 Ping [ICMP/255~255]
 data [TCP/520~521]

Paso 4. Elija el servicio adecuado que debe filtrar en la lista desplegable Servicio.

Nota: Para permitir todo el tráfico, elija **Todo el tráfico [TCP&UDP/1~65535]** en la lista desplegable de servicio si se ha establecido la acción para permitir. La lista contiene todos los tipos de servicios que puede querer filtrar.

Edit Access Rules

Services

Action: Allow

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

Log: Enabled

Source Interface: No Log

Source IP / Prefix Length: ANY

Destination IP / Prefix Length: ANY

Save Cancel Back

Paso 5. Elija la opción Registro adecuada en la lista desplegable Registro. La opción de registro determina si el dispositivo mantendrá un registro del tráfico que corresponde al conjunto de reglas de acceso.

- **Habilitado:** permite al router mantener el seguimiento de registro para el servicio que se ha

seleccionado.

- Not Log: Inhabilita el router para mantener el seguimiento del registro.

Edit Access Rules

Services

Action: Allow ▾

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

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: LAN

Destination IP / Prefix Length: ANY

Save Cancel Back

Paso 6. Haga clic en la lista desplegable Interfaz y elija la interfaz de origen adecuada. En esta interfaz se aplica la regla de acceso.

- LAN: la regla de acceso afecta sólo al tráfico LAN.
- WAN 1: la regla de acceso afecta sólo al tráfico WAN 1.
- WAN 2: la regla de acceso sólo afecta al tráfico WAN 2.
- Any: la regla de acceso afecta a todo el tráfico en cualquiera de las interfaces del dispositivo.

Edit Access Rules

Services

Action: Allow ▾

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

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: ANY ▾

Destination IP / Prefix Length: ANY

Save Cancel Back

Paso 7. Elija el tipo IP de origen adecuado al que se aplica la regla de acceso en la lista desplegable IP de origen/ Longitud de prefijo.

- ANY: cualquier paquete que se recibe de una red del dispositivo tiene la regla aplicada a ellos.

Edit Access Rules

Services

Action: Allow ▾

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

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Single ▾ 2607:f0d0:1002:51::4 / 128

Destination IP / Prefix Length: ANY ▾

Save Cancel Back

- Single: sólo una única dirección IP especificada en la red del dispositivo tiene la regla aplicada. Introduzca la dirección IPv6 deseada en el campo adyacente.

Edit Access Rules

Services

Action: Allow ▾

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

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Subnet ▾ 2607:f0d0:1002:51::4 / 45

Destination IP / Prefix Length: ANY ▾

Save Cancel Back

- Subred: sólo las direcciones IP de una subred tienen la regla aplicada. Introduzca la dirección de red IPv6 y la longitud del prefijo de la subred deseada en los campos adyacentes.

Edit Access Rules

Services

Action: Allow ▾

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

Log: Enabled ▾

Source Interface: LAN ▾

Source IP / Prefix Length: Subnet ▾ 2607:f0d0:1002:51::4 / 45

Destination IP / Prefix Length: ANY ▾

- ANY
- Single
- Subnet

Save Cancel Back

Paso 8. Elija el tipo de IP de destino adecuado al que se aplica la regla de acceso en la lista desplegable Destination IP / Prefix Length .

- Any — Cualquier dirección IP de destino tiene la regla aplicada a ellos.
- Single: sólo una única dirección IP especificada en la red del dispositivo tiene la regla aplicada. Introduzca la dirección IPv6 deseada.
- Subred: sólo las direcciones IP de una subred tienen la regla aplicada. Introduzca la dirección de red IPv6 y la longitud del prefijo de la subred deseada en los campos adyacentes.

Paso 9. Haga clic en **Guardar** para que los cambios sean efectivos.

Ver un vídeo relacionado con este artículo...

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