# Configuración de reglas de acceso en RV215W

## Objetivo

El RV215W permite configurar reglas de acceso para aumentar la seguridad. Estas listas de control de acceso (ACL) son listas que bloquean o permiten el envío del tráfico a determinados usuarios y desde ellos. Se pueden configurar para que estén en vigor todo el tiempo o en función de las programaciones definidas.

En este artículo se explica cómo configurar las reglas de acceso en el RV215W.

### **Dispositivos aplicables**

·RV215W

### Versión del software

•1.1.0.5

### Reglas de acceso

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

ciudit U	utbound Policy							
olicy:	Allow O Deny							
Access	Rule Table							
Filter: Ar	ction matches All	•						
	1	Service	Status	Connection Type	Source IP	Destination IP	Log	Priorit
	Action	Service						
	Action No data to display	Service				L		
Add R	Action No data to display Row Edit	Enable	Disable Dele	ete Reorder				

Paso 2. Haga clic en el botón de opción correspondiente a la política saliente predeterminada deseada en el campo Política. La política de salida predeterminada determina si el tráfico saliente está permitido o denegado. Se utiliza cuando no hay reglas de acceso ni políticas de acceso a Internet configuradas para una dirección IP de un usuario.

Paso 3. Click Save.

#### Agregar regla de acceso

Paso 1. Haga clic en **Agregar fila** para agregar una nueva regla de acceso. Se abre la página Agregar regla de acceso:

Add Access R	ule	
Connection Type:	Outbound (LAN > WAN) -	
Action:	Always block -	
Schedule:	Schedule1 - Configure Schedules	
Services:	All Traffic   Configure Services	
Source IP:	Single Address 👻	
Start:	192.168.1.100	(Hint: 192.168.1.100 or fec0::64)
Finish:		(Hint: 192.168.1.200 or fec0::c8)
Destination IP	Address Range 👻	
Start:	192.168.15.1	
Finish:	192.168.15.254	
Log:	Never -	
QoS Priority:	1 (lowest) 👻	
Rule Status:	Enable	
Save	ancel Back	

Paso 2. En la lista desplegable Tipo de conexión, elija el tipo de regla que desea crear.

·saliente (LAN > WAN): la regla afecta a los paquetes que vienen de la LAN segura y van a la WAN no segura.

·entrante (WAN > LAN): la regla afecta a los paquetes que provienen de la WAN no segura y van a la LAN segura.

·entrante (WAN > DMZ): la regla afecta a los paquetes que proceden de la WAN no segura y van a la DMZ. Una DMZ es un segmento de red que separa la LAN de la WAN para proporcionar una capa adicional de seguridad.

Paso 3. En la lista desplegable Acción, elija la acción que se aplicará a la regla.

·Bloqueo siempre: bloquea siempre los paquetes.

·Permitir siempre: permite siempre los paquetes.

·Bloquear por programación: bloquea los paquetes según una programación especificada.

·Permitir por programación: permite paquetes según una programación especificada.

Paso 4. En la lista desplegable Programación, elija una programación para aplicarla a la regla.

Paso 5. En la lista desplegable Servicios, elija un servicio para permitir o bloquear.

**Nota:** Haga clic en **Configurar servicios** para configurar programaciones en la *página Administración de servicios*.

Paso 6. En la lista desplegable IP de origen, elija las direcciones IP de origen a las que la regla bloquea o permite el ingreso de paquetes.

Any: la regla se aplica a todas las direcciones IP de origen.

·dirección única: introduzca una única dirección IP a la que se aplica la regla en el campo Inicio.

Intervalo de direcciones : introduzca un intervalo de direcciones IP al que se aplica la regla en los campos Inicio y Finalizar.

Paso 7. En la lista desplegable IP de destino, elija las direcciones IP de destino a las que la regla bloquea o permite que los paquetes accedan.

Any: la regla se aplica a todas las direcciones IP de destino.

·dirección única: introduzca una única dirección IP a la que se aplica la regla en el campo Inicio.

Intervalo de direcciones : introduzca un intervalo de direcciones IP al que se aplica la regla en los campos Inicio y Finalizar.

Paso 8. En la lista desplegable Registro, elija una opción de registro. Los registros se generan en registros del sistema que se utilizan para la administración de la seguridad.

·Nunca: Inhabilita Los Registros.

·Siempre: el RV215W crea un registro cada vez que un paquete coincide con la regla.

Paso 9. En la lista desplegable Prioridad de QoS, elija una prioridad para los paquetes IP salientes de la regla. La prioridad uno es la más baja, mientras que la prioridad cuatro es la más alta. Los paquetes en colas de mayor prioridad se enviarán antes que los que se encuentren en colas de menor prioridad.

Paso 10. Marque **Enable** en el campo Rule Status para habilitar la regla.

Paso 11. Click Save.

#### Reordenar reglas de acceso

La función de reordenamiento es una opción importante en el RV215W. El orden en el que se muestran las reglas de acceso en la tabla de reglas de acceso indica el orden en el que se aplican las reglas. La primera regla de la tabla es la primera que se aplica.

efault Ou	utbound Policy							
olicy:	C Allow 🖲 Deny							
Access	Rule Table							
Filter: Ac	ction matches All	-						
	Action	Service	Status	Connection Type	Source IP	Destination IP	Log	Priorit
	Always block	All Traffic	Enabled	Outbound (LAN > WAN)	192.168.1.100	192.168.15.1 ~ 192.168.15.254	Never	Low
<b></b>	Always allow	FTP	Enabled	Inbound (WAN > LAN)	Any	192.168.1.50	Never	
			1					

Paso 1. Haga clic en **Reordenar** para reordenar las reglas de acceso.

Paso 2. Active la casilla de la regla de acceso que desea reordenar.

Access	Rule Table							
	Priority	Action	Service	Status	Connection Type	Source IP	Destination IP	Log
	Low	Always block	All Traffic	Enabled	Outbound (LAN > WAN)	192.168.1.100	192.168.15.1 - 192.168.15.254	Never
1		Always allow	FTP	Enabled	Inbound (WAN > LAN)	Any	192.168.1.50	Never
▲ 💌 Save	Move to	Back						

Paso 3. En la lista desplegable, elija la posición a la que desea mover la regla especificada.

Paso 4. Haga clic en **Mover a** para reordenar la regla. La regla se mueve a la posición especificada en la tabla.

**Nota:** Los botones de flecha hacia arriba y hacia abajo también se pueden utilizar para reordenar las reglas de acceso.

Paso 5. Click Save.

#### Configuración de administración de programación

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

Schedule Tal	ble		
Name	Days	Start Time	End Time
No data t	o <mark>displa</mark> y		
Add Row	Edit	Delete	

Paso 2. Haga clic en **Agregar fila** para agregar una nueva programación. Se abre la página *Agregar/Editar programaciones*:

Add/Edit Schedules						
Add/Edit Sche	Add/Edit Schedules Configuration					
Name:	Schedule1					
Scheduled Da	iys					
Do you want th	his schedule to be active on all days or specific days?					
	Specific Days 👻					
Monday:						
Tuesday:						
Wednesday:						
Thursday:						
Friday:						
Saturday:						
Sunday:						
Scheduled Time of Day						
Do you want this schedule to be active on all days or at specific times during the day?						
	Specific Times 👻					
Start time:	08 - Hours 00 - Minutes AM -					
End time:	10 - Hours 30 - Minutes PM -					
Save	Cancel Back					

Paso 3. Introduzca un nombre para la programación en el campo Nombre.

Paso 4. En la lista desplegable Días programados, elija los días en los que la programación está activa.

·Todos los días: la programación está activa para todos los días de la semana.

·días específicos: active las casillas de verificación de los días para que la programación esté activa.

Paso 5. En la lista desplegable Hora del día programada, seleccione la hora a la que está activa la programación.

·Todas las horas: la programación está activa en todo momento del día.

·horas específicas: en la lista desplegable Hora de inicio y Hora de finalización, elija la hora a la que se inicia la programación y la hora a la que finaliza.

Paso 6. Click Save.