

Configure la expedición/el puerto Triggering/NAT del puerto en el Routers de las RV34x Series

Objetivo

Explique el propósito de la expedición del puerto y del puerto que accionan y proporcione a las instrucciones de poner estas características en su router de las RV34x Series.

- Comparar la expedición del puerto y accionar del puerto
- Determinación de la expedición del puerto y de accionar del puerto
- Determinación del Network Address Translation (NAT)

Dispositivos aplicables

- Serie del router RV34x

Versión de software

- 1.0.01.17

Comparar la expedición del puerto y accionar del puerto

Estas características permiten que algunos usuarios de Internet tengan acceso a los recursos específicos en su red, mientras que protegen los recursos que usted quiere guardar el soldado. Algunos ejemplos de cuando se utiliza esto: recibiendo la red/envíe por correo electrónico los servidores, el sistema de alarma y las cámaras de seguridad (enviar el vídeo de nuevo a un ordenador exterior). La expedición del puerto abre los puertos en respuesta al tráfico entrante para un servicio especificado.

Una lista de estos puertos y su descripción se ponen cuando usted ingresa la información en la sección de administración del servicio del asistente para la configuración. Cuando usted configura éstos, usted no puede utilizar el número del mismo puerto para la expedición del puerto y virar accionar hacia el lado de babor.

Expedición del puerto

La expedición del puerto es una tecnología que permite el acceso público a los servicios en los dispositivos de red en el red de área local (LAN) abriendo un puerto específico para un servicio en respuesta al tráfico entrante. Esto se asegura de que los paquetes tengan una trayectoria clara al destino deseado, que permite velocidades más rápidas de la transferencia directa y un tiempo de espera más bajo. Esto se fija para un solo ordenador en su red. Usted necesita agregar la dirección IP del ordenador específico y no puede cambiar.

Ésta es una operación estática que abre un rango de puertos específico que usted seleccione y no cambia. Esto puede aumentar el riesgo de seguridad pues los puertos configurados están siempre abiertos.

Imagínese que una puerta está siempre abierta en ese puerto a ese dispositivo que fue asignada.

Vire accionar hacia el lado de babor

El accionar del puerto es similar virar la expedición hacia el lado de babor pero un poco más seguro. La diferencia es que el puerto del activador no está siempre abierto para ese tráfico específico. Después de que un recurso en su LAN envíe el tráfico saliente a través de un puerto del activador, el router está atento el tráfico entrante a través de un rango del puerto especificado o del puerto. Los puertos accionados son cerrados cuando no hay actividad, que agrega a la Seguridad. Otra ventaja es que más de un ordenador en su red puede tener acceso a este puerto en los momentos diferentes. Por lo tanto, usted no necesita conocer la dirección IP del ordenador que la accionará por adelantado, él hace esto automáticamente.

Piense en usted que da a alguien un paso pero allí es un doorman allí que controla su paso que usted ingresa cada vez y después que cierra la puerta hasta que llegue la persona siguiente con un paso.

Determinación de la expedición del puerto y de accionar del puerto

Expedición del puerto

Para configurar la expedición del puerto, siga los siguientes pasos:

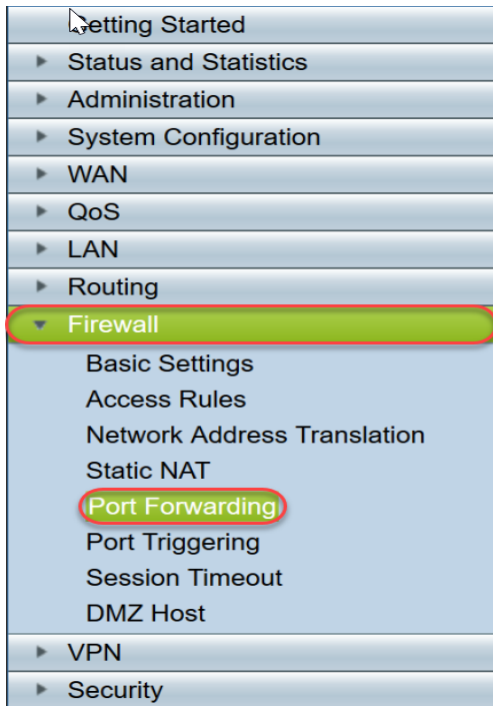
Paso 1. Clave a la utilidad de configuración de la red. Ingrese el IP address para el ranurador en la búsqueda/la barra de dirección. El navegador pudo publicar una advertencia que el sitio web es untrusted. Continúe al sitio web. Para más dirección con este paso, haga clic [aquí](#).

Ingrese el nombre de usuario y contraseña para el ranurador y haga clic la **clave**. El nombre de usuario y contraseña del valor por defecto es Cisco.



The image shows a screenshot of the Cisco Router configuration page. On the left, there is the Cisco logo and the word "Router". On the right, there is a login form with the following fields: "Username:" with a text input field, "Password:" with a text input field, and "Language:" with a dropdown menu set to "English". Below these fields is a "Log In" button.

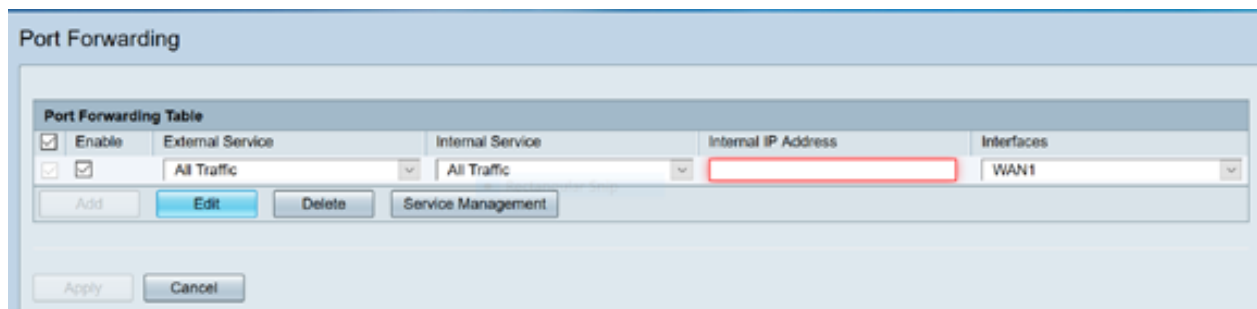
Paso 2. From el menú principal en el lado izquierdo, **Firewall del teclado > expedición del puerto**



En la tabla de reenvío del puerto, el tecleo **agrega** o selecciona la fila y el tecleo **corrige** para configurar el siguiente:

Servicio externo	Seleccione un servicio externo de la lista desplegable. (Si un servicio no es mencionado, usted puede agregar o modificar la lista siguiendo las instrucciones en la sección de administración del servicio.)
Servicio interno	Seleccione un servicio interno de la lista desplegable. (Si un servicio no es mencionado, usted puede agregar o modificar la

	lista siguiendo las instrucciones en la sección de administración del servicio.)
Dirección IP interna	Ingrese los IP Addresses internos del servidor.
Interfaces	Seleccione el interfaz de la lista desplegable, para aplicar la expedición del puerto encendido.
Estatus	Active o inhabilite la regla de la expedición del puerto.



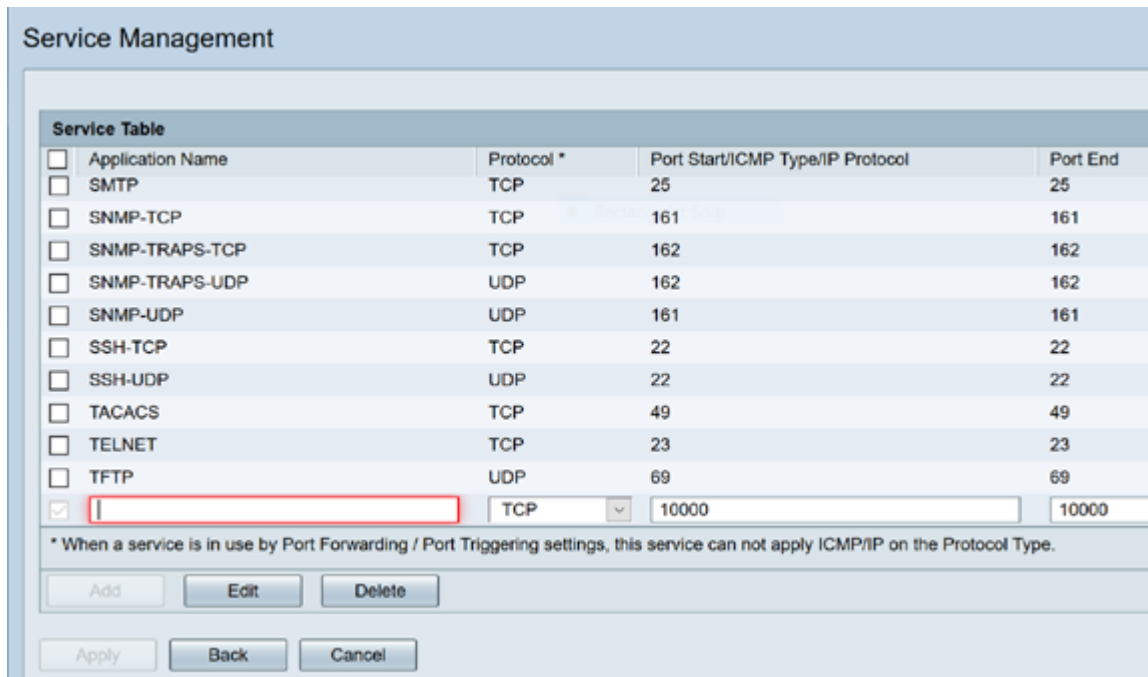
Por ejemplo, un servidor Web de los host A de la compañía (con una dirección IP interna de 192.0.2.1) en su LAN. Una regla de la expedición del puerto para el tráfico HTTP podía ser activada. Esto permitiría las peticiones de Internet en esa red. La compañía fija el número del puerto 80 (HTTP) que se remitirá a la dirección IP 192.0.2.1, después todas las solicitudes HTTP de los usuarios externos serán remitidas a 192.0.2.1. Se pone para ese dispositivo específico en la red.

Paso 3. Administración del servicio del teclado

En la tabla del servicio, el teclado **agrega** o selecciona una fila y el teclado **corrige** y configura el siguiente:

- Nombre de la aplicación – Nombre del servicio o de la aplicación
- Protocolo – Protocolo requerido. Refiera a la documentación para el servicio que usted está recibiendo

- Vire el protocolo Start/ICMP hacia el lado de babor Type/IP – Números de rango de puertos reservados para este servicio
- Extremo del puerto – Número pasado del puerto, reservado para este servicio

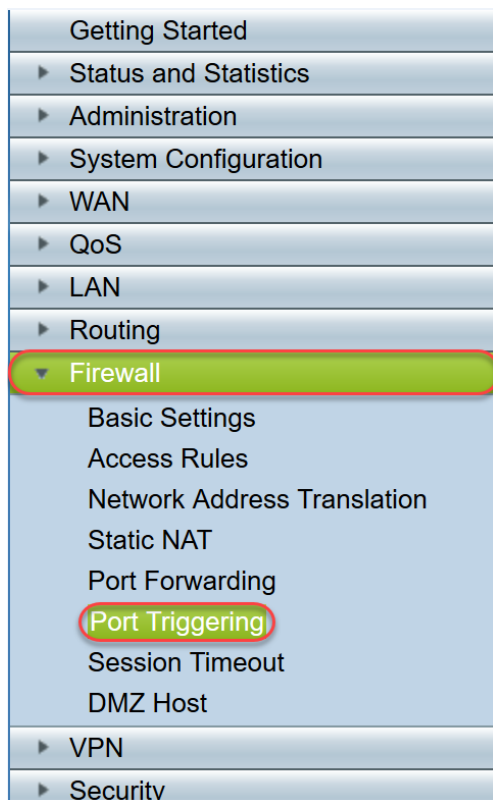


Paso 4. El tecleo **se aplica**

El accionar del puerto

Para configurar el puerto que acciona, siga los siguientes pasos:

Paso 1. Log adentro a la utilidad de configuración de la red. Del menú principal en el lado izquierdo, **Firewall del tecleo > el accionar del puerto**



El paso 2.To agrega o corrige un servicio al puerto que acciona la tabla, configura el siguiente:

Nombre de la aplicación	Ingrese el nombre de la aplicación.
Accione el servicio	Seleccione un servicio de la lista desplegable. (Si un servicio no es mencionado, usted puede agregar o modificar la lista siguiendo las instrucciones en la sección de administración del servicio.)
Servicio entrante	Seleccione un servicio de la lista desplegable. (Si un servicio no es mencionado, usted puede agregar o modificar la lista siguiendo las instrucciones en la sección de administración del servicio.)
Interfaces	Seleccione el interfaz de la lista desplegable.
Estatus	Active o inhabilite el puerto que acciona la

regla.

El tecleo **agrega** (o seleccione la fila y el tecleo **corrige**) y ingresa la información siguiente:

Enable	Application Name	Trigger Service	Incoming Service	Interfaces
<input type="checkbox"/>	c	All Traffic	FTP	WAN1
<input type="checkbox"/>	d	All Traffic	FTP	WAN1

Paso 3. Haga clic la **Administración del servicio**, para agregar o para corregir una entrada en la lista del servicio.

En la tabla del servicio, el tecleo **agrega** o **corrige** y configura el siguiente:

- Nombre de la aplicación – Nombre del servicio o de la aplicación
- Protocolo – Protocolo requerido. Refiera a la documentación para el servicio que usted está recibiendo
- Vire el protocolo Start/ICMP hacia el lado de babor Type/IP – Números de rango de puertos reservados para este servicio
- Extremo del puerto – Número pasado del puerto, reservado para este servicio

Application Name	Protocol *	Port Start/ICMP Type/IP Protocol	Port End
SMTP	TCP	25	25
SNMP-TCP	TCP	161	161
SNMP-TRAPS-TCP	TCP	162	162
SNMP-TRAPS-UDP	UDP	162	162
SNMP-UDP	UDP	161	161
SSH-TCP	TCP	22	22
SSH-UDP	UDP	22	22
TACACS	TCP	49	49
TELNET	TCP	23	23
TFTP	UDP	69	69
<input type="checkbox"/>	TCP	10000	10000

Paso 4. El tecleo **se aplica**

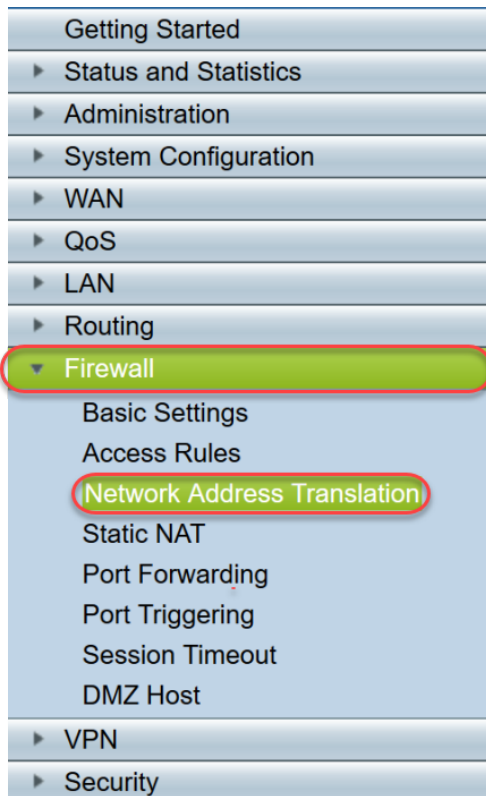
Traducción de la dirección de red

El Network Address Translation (NAT) permite a las redes de IP privado con los IP Addresses no registrados conectar con la red pública. Esto es un protocolo comúnmente configurado en la mayoría de las redes. El NAT traduce los IP Addresses privados de la red

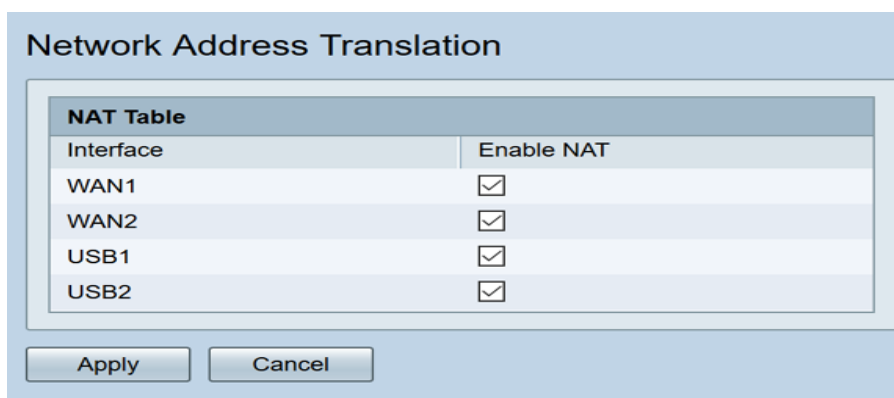
interna a los IP Addresses públicos antes de que los paquetes se remitan a la red pública. Esto permite que un gran número de host en una red interna tengan acceso a Internet a través de un número limitado de IP Addresses públicos. Esto también ayuda a proteger los IP Addresses privados contra cualquier ataque malicioso o descubrimiento mientras que los IP Addresses privados se mantienen ocultos.

Para configurar el NAT, siga los siguientes pasos

Firewall del paso 1. Click > traducción de la dirección de red



Paso 2. En la tabla NAT, controle el permiso NAT para saber si hay cada interfaz correspondiente en la lista para activar



Paso 3. El tecleo se aplica

Usted ahora ha configurado con éxito la expedición del puerto, el puerto que accionaba, y el NAT.

Otros recursos

- Para la configuración del NAT estático, haga clic [aquí](#)

- Para las respuestas a muchas preguntas sobre el Routers, incluyendo las RV3xx Series, haga clic [aquí](#)
- Para los FAQ en las RV34x Series, haga clic [aquí](#)
- Para más información sobre RV345 y RV345P, haga clic [aquí](#)
- Para más información sobre configurar la Administración del servicio en las RV34x Series, haga clic [aquí](#)

Vea un vídeo relacionado con este artículo...

[Haga clic aquí para ver otras conversaciones sobre aspectos teóricos de Cisco](#)