Configuración del registro del sistema en los routers RV320 y RV325 VPN

Objetivo

Los registros del sistema son registros de eventos de red. Los registros son una herramienta importante que se utiliza para entender cómo funciona una red. Son útiles para la gestión de redes y la resolución de problemas de red.

En este artículo se explica cómo configurar los tipos de registros que se van a grabar, cómo ver los registros en la Serie RV32x de Router VPN y cómo enviar los registros a un destinatario a través de SMS, a un servidor de registro del sistema o a un destinatario a través del correo electrónico.

Dispositivos aplicables

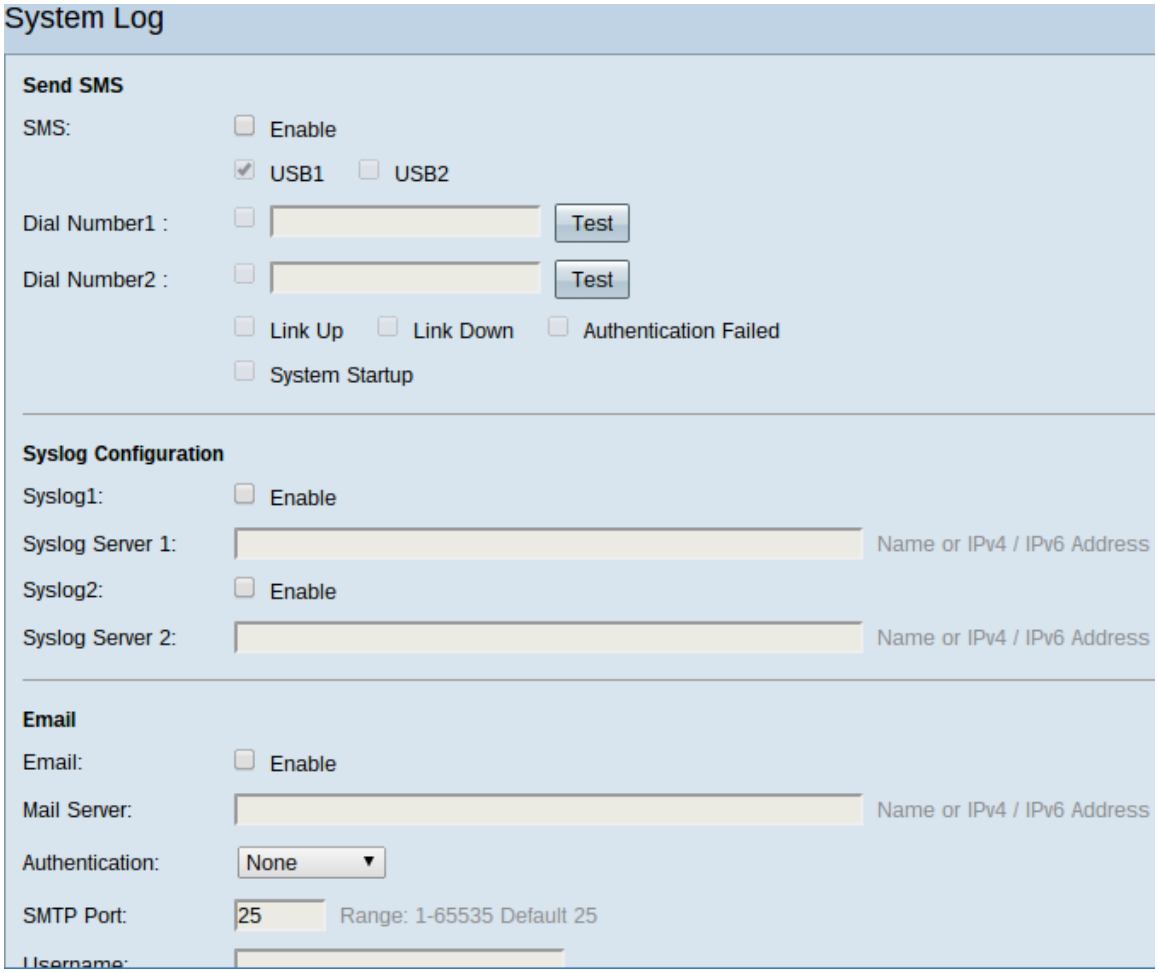
Router VPN Dual WAN · RV320
Router VPN Dual WAN · RV325 Gigabit

Versión del software

•v1.1.0.09

Configuración del registro del sistema

Paso 1. Inicie sesión en la utilidad de configuración Web y elija **Log > System Log**. Se abre la página *Registro del sistema*:



Consulte las secciones siguientes para obtener información sobre la página *Registro del sistema*.

·Registros del sistema por SMS: cómo enviar los registros del sistema a un teléfono a través de SMS.

·Registros del sistema en los Servidores de registro del sistema: cómo enviar los registros del sistema a un servidor de registro del sistema.

·Registros del sistema de correo electrónico: cómo enviar los registros del sistema a una dirección de correo electrónico.

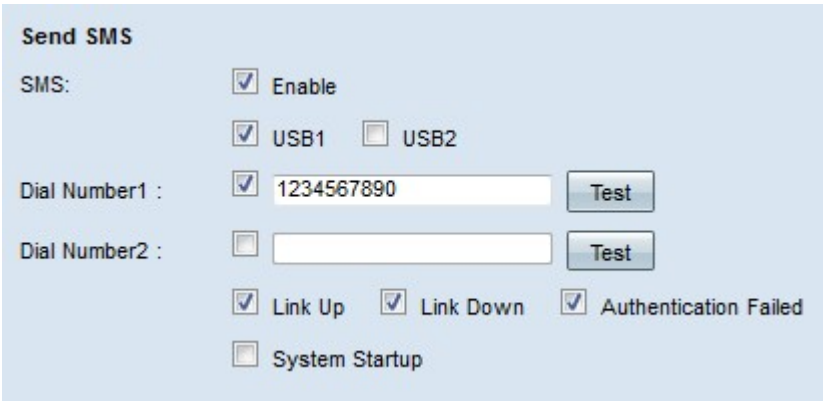
Configuración de registro: cómo configurar el tipo de mensajes guardados en el registro.

Ver registro del sistema: cómo ver los registros del sistema en el dispositivo.

·Ver Tabla de Registro de Salida: Cómo ver los registros del sistema que sólo se relacionan con los paquetes salientes.

·Ver Tabla de Registro Entrante: Cómo ver los registros del sistema que sólo se relacionan con los paquetes entrantes.

Registros del sistema por SMS



Paso 1. Marque **Enable** en el campo SMS para enviar registros del sistema a un cliente a través de mensajes SMS (Servicio de mensajes cortos).

Paso 2. Active las casillas de verificación de los puertos USB a los que está conectado el módem USB 3G.

Paso 3. Marque la casilla de verificación en el campo Número de marcación 1 e introduzca el número de teléfono al que se envían los mensajes.

Nota: Haga clic en **Prueba** para probar la conexión al número de marcación 1. Si el número configurado no recibe el mensaje de prueba, asegúrese de que el número de teléfono se ha introducido correctamente en el campo Número de marcación 1.

Paso 4. (Opcional) Marque la casilla de verificación en el campo Número de marcación 2 e introduzca el número de teléfono al que se envían los mensajes.

Nota: Haga clic en **Prueba** para probar la conexión al número de marcación 2. Si el número configurado no recibe el mensaje de prueba, asegúrese de que el número de teléfono se ha introducido correctamente en el campo Número de marcación 2.

Paso 5. Active las casillas de verificación de los eventos que activarán el envío de un registro.

·Link Up: se ha activado una conexión al RV320.

·Link Down: se ha caído una conexión al RV320.

Error de autenticación ·: error de autenticación.

Inicio · sistema: el router se ha iniciado.

Paso 6. Click **Save**. Se configuran los registros del sistema a través de SMS.

Registros del sistema en servidores de registro del sistema

Paso 1. Marque **Enable** en el campo Syslog1 para enviar registros del sistema a un servidor de registro del sistema.

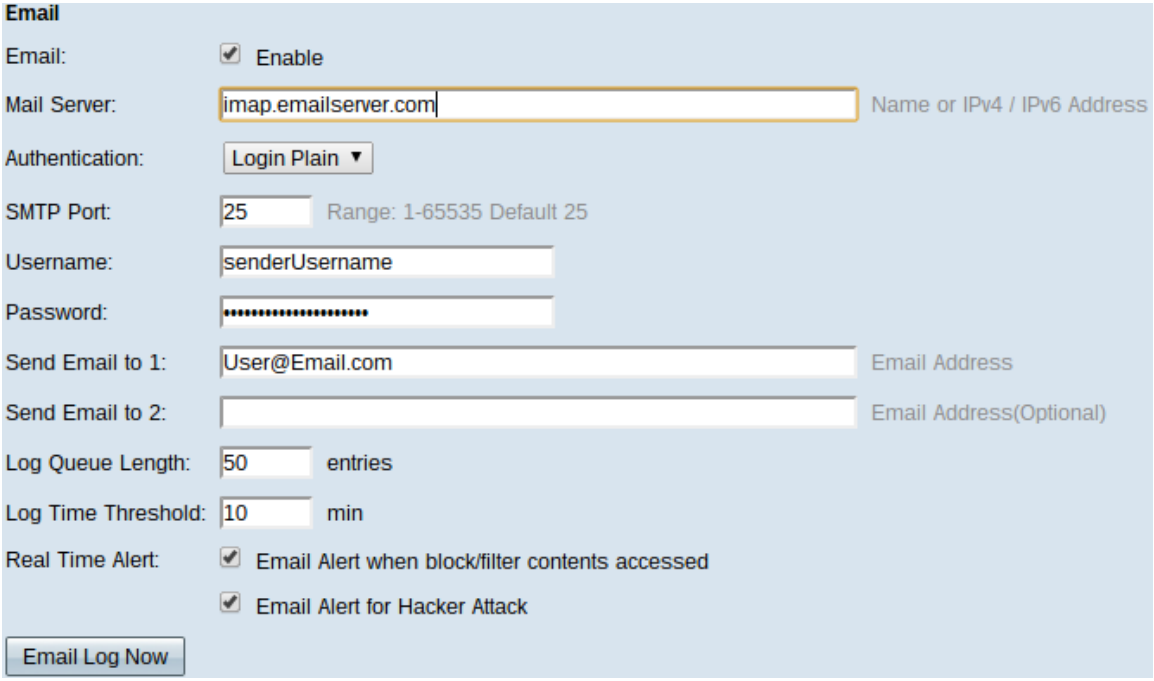
Paso 2. Introduzca el nombre de host o la dirección IP del servidor de registro del sistema en el campo Servidor de registro del sistema 1.

Paso 3. (Opcional) Para enviar registros a otro servidor de registro del sistema, marque **Enable** en el campo Syslog2.

Paso 4. Si la casilla de verificación está activada en el campo Syslog2, introduzca el nombre de host o la dirección IP del servidor de registro del sistema en el campo Servidor de registro del sistema 2.

Paso 5. Click **Save**. Se configuran los registros del sistema a través de los servidores de registro del sistema.

Registros del sistema de correo electrónico



Paso 1. Marque **Enable** en el campo Email para enviar registros del sistema a un destinatario a través del correo electrónico.

Paso 2. Introduzca el nombre de dominio o la dirección IP del servidor de correo en el campo Servidor de correo.

Paso 3. Elija el tipo de autenticación que utiliza el servidor de correo en el campo Authentication (Autenticación).

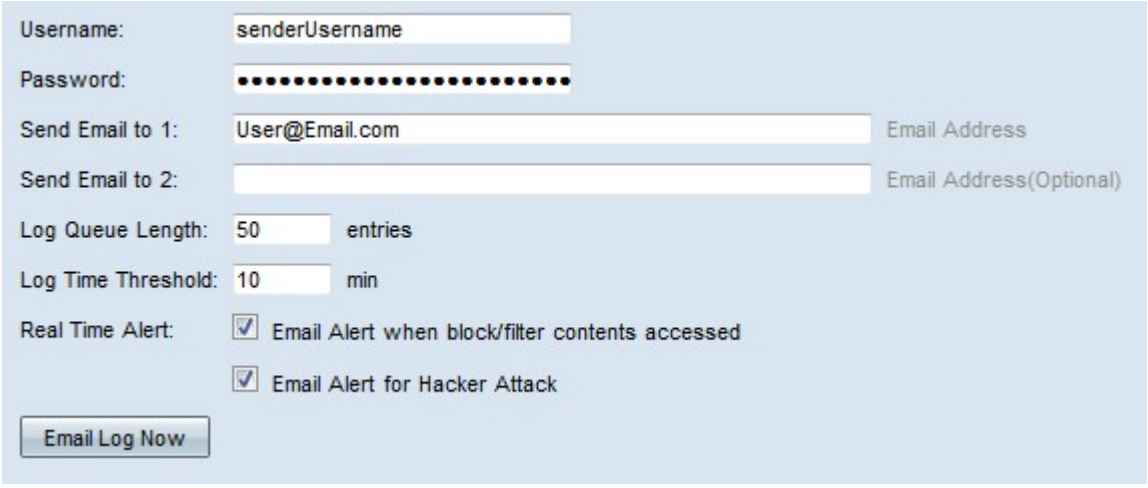
·Ninguno: el servidor de correo no utiliza autenticación.

·de inicio de sesión: el servidor de correo utiliza una autenticación que está en un formato de texto sin formato.

·TLS: el servidor de correo utiliza la seguridad de la capa de transporte (TLS) para permitir que el cliente y el servidor intercambien información de autenticación de forma segura.

·SSL: el servidor de correo utiliza Secure Sockets Layer (SSL) para permitir que el cliente y el servidor intercambien información de autenticación de forma segura.

Paso 4. Introduzca el puerto SMTP (protocolo simple de transferencia de correo) que utiliza el servidor de correo en el campo Puerto SMTP. SMTP es un protocolo que permite que los correos electrónicos se transmitan a través de redes IP.



Paso 5. Introduzca el nombre de usuario del remitente del correo electrónico en el campo Nombre de usuario.

Paso 6. Introduzca la contraseña del remitente del correo electrónico en el campo Password (Contraseña).

Paso 7. Introduzca la dirección de correo electrónico del destinatario en el campo Enviar correo electrónico a 1.

Paso 8. (Opcional) Introduzca una dirección de correo electrónico adicional a la que enviar correos electrónicos de registro en el campo Enviar correo electrónico a 2.

Paso 9. Introduzca el número de entradas de registro que se deben realizar antes de enviar el registro al destinatario del correo electrónico en el campo Longitud de cola de registro.

Paso 10. Introduzca el intervalo en el que el dispositivo envía el registro al correo electrónico en el campo Umbral de tiempo de registro.

Paso 11. Marque la primera casilla de verificación del campo Alerta en tiempo real para enviar inmediatamente un correo electrónico cuando alguien, que ha sido bloqueado o filtrado, intenta acceder al router.

Paso 12. Marque la segunda casilla del campo Alerta en tiempo real para enviar un correo electrónico inmediatamente cuando un hacker intente acceder al router mediante un ataque de denegación de servicio (DOS).

Nota: Haga clic en **Email Log Now** para enviar inmediatamente el registro.

Paso 13. Click **Save**. Se configuran los registros del sistema a través del correo electrónico.

Configuración de registro

Paso 1. Active las casillas de verificación de los eventos que activarán una entrada de registro.

Registro de alertas ·: estos registros se crean cuando se ha producido un ataque o un intento de ataque.

- Inundación Syn: la solicitud SYN se recibe más rápido de lo que el router puede procesarlos.

- Suplantación de IP: el RV320 ha recibido paquetes IP con direcciones IP de origen falsificadas.

- Intento de inicio de sesión no autorizado: Ha fallado un intento rechazado para iniciar sesión en la red.

- Ping of Death (Ping de la muerte): se ha enviado un ping de un tamaño anormal a una interfaz en un intento de bloquear el dispositivo de destino.

- Win Nuke: el ataque remoto de denegación de servicio distribuido (DDOS) conocido como WinNuke, se ha enviado a una interfaz en un intento de bloquear el dispositivo de destino.

Registro general ·: estos registros se crean cuando se producen acciones de red generales.

- Denegar políticas: se ha denegado el acceso a un usuario según las políticas configuradas del router.

- Inicio de sesión autorizado: un usuario ha sido autorizado para acceder a la red.

- Mensajes de error del sistema: se ha producido un error del sistema.

- Permitir políticas: se ha concedido acceso a un usuario en función de las políticas configuradas del router.

- Kernel — Incluya todos los mensajes del núcleo en el registro. El núcleo es la primera parte del sistema operativo que se carga en la memoria al arrancar. Los mensajes del núcleo son registros que están asociados con el núcleo.

- Cambios de configuración: se ha modificado la configuración del router.

- VPN IPSEC y PPTP: se ha producido una negociación, conexión o desconexión IPSEC y PPTP VPN.

- SSL VPN: se ha producido una negociación, conexión o desconexión SSL VPN.

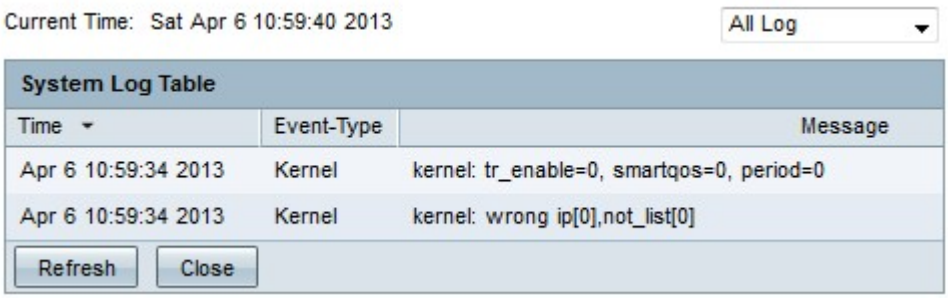
- Red: se ha realizado o perdido una conexión física en las interfaces WAN o DMZ.

Paso 2. Click **Save**. Se configuran los parámetros de registro.

Nota: Haga clic en **Borrar registro** para borrar el registro actual.

Ver registro del sistema

Paso 1. Haga clic en **Ver registro del sistema** para ver la tabla de registro del sistema. Aparece la ventana *Tabla de registro del sistema*.



Paso 2. (Opcional) En la lista desplegable, elija el tipo de registros que desea ver.

·Todos los registros: incluye todos los mensajes de registro.

·Registro del sistema: sólo incluye los mensajes de error del sistema.

·Firewall/DoS Log: sólo incluye los registros de alertas.

Registro de VPN ·: solo incluye los registros VPN IPSec y PPTP y SSL.

Registro de red ·: sólo incluye los registros de red.

Registro · Kernel — Sólo incluye mensajes del kernel.

Registro de usuario ·: solo incluye políticas de denegación, políticas permitidas, registros de cambios de configuración e inicio de sesión autorizados

Registro · SSL: sólo incluye registros SSL VPN.

La Tabla de registro del sistema muestra la siguiente información.

Hora ·: la hora en la que se creó el registro.

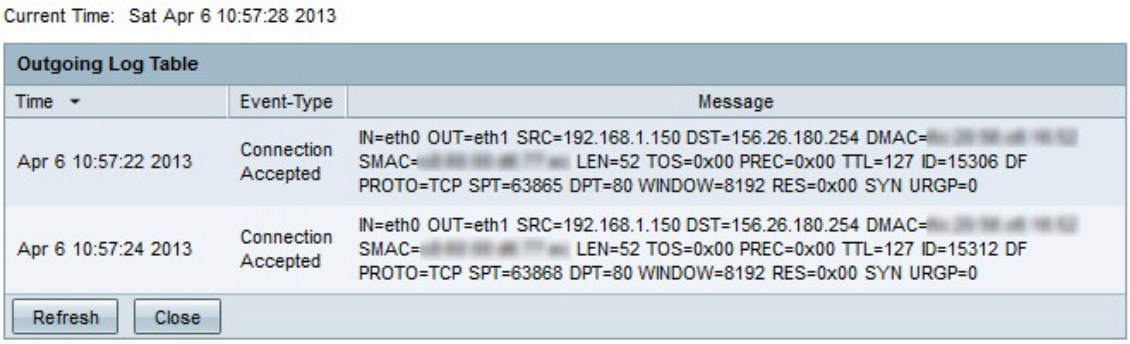
·Event-Type: el tipo de registro.

Mensaje ·: información que corresponde al registro. Esto incluye el tipo de política, la dirección IP de origen y la dirección MAC de origen.

Nota: Haga clic en **Actualizar** para actualizar la tabla de registro.

Ver tabla de registro saliente

Paso 1. Haga clic en **Tabla de registro saliente** para ver la tabla de registro que se relaciona solamente con los paquetes salientes. Aparece la ventana *Outgoing Log Table*.



La tabla de registro saliente muestra la siguiente información.

Hora ·: la hora en la que se creó el registro.

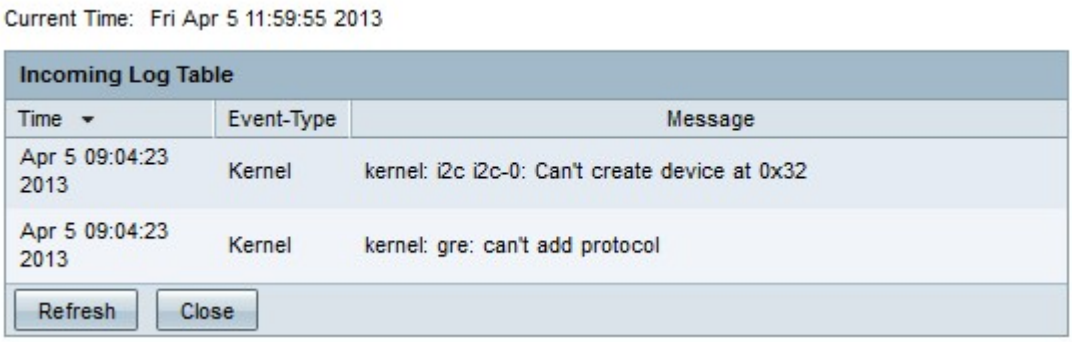
·Event-Type: el tipo de registro.

Mensaje ·: información que corresponde al registro. Esto incluye el tipo de política, la dirección IP de origen y la dirección MAC de origen.

Nota: Haga clic en **Actualizar** para actualizar la tabla de registro.

Ver tabla de registro entrante

Paso 1. Haga clic en **Incoming Log Table** para ver la tabla de registro que se relaciona solamente con los paquetes entrantes. Aparece la ventana *Incoming Log Table*.



La tabla de registro de entrada muestra la siguiente información.

Hora ·: la hora en la que se creó el registro.

·Event-Type: el tipo de registro.

Mensaje ·: información que corresponde al registro. Esto incluye el tipo de política, la dirección IP de origen y la dirección MAC de origen.

Nota: Haga clic en **Actualizar** para actualizar la tabla de registro.