Configuración del registro del sistema en los routers VPN RV016, RV042, RV042G y RV082

Objetivo

Se utiliza un registro del sistema (Syslog) para registrar los datos del equipo. Puede definir las instancias que generarán un registro. Siempre que se produce una instancia, la hora y el evento se registran y se envían a un servidor syslog o se envían en un correo electrónico. Syslog se puede utilizar para analizar y solucionar problemas de una red junto con aumentar la seguridad de la red.

Este documento explica el procedimiento para configurar un servidor Syslog en los routers VPN RV016, RV042, RV042G y RV082.

Dispositivos aplicables

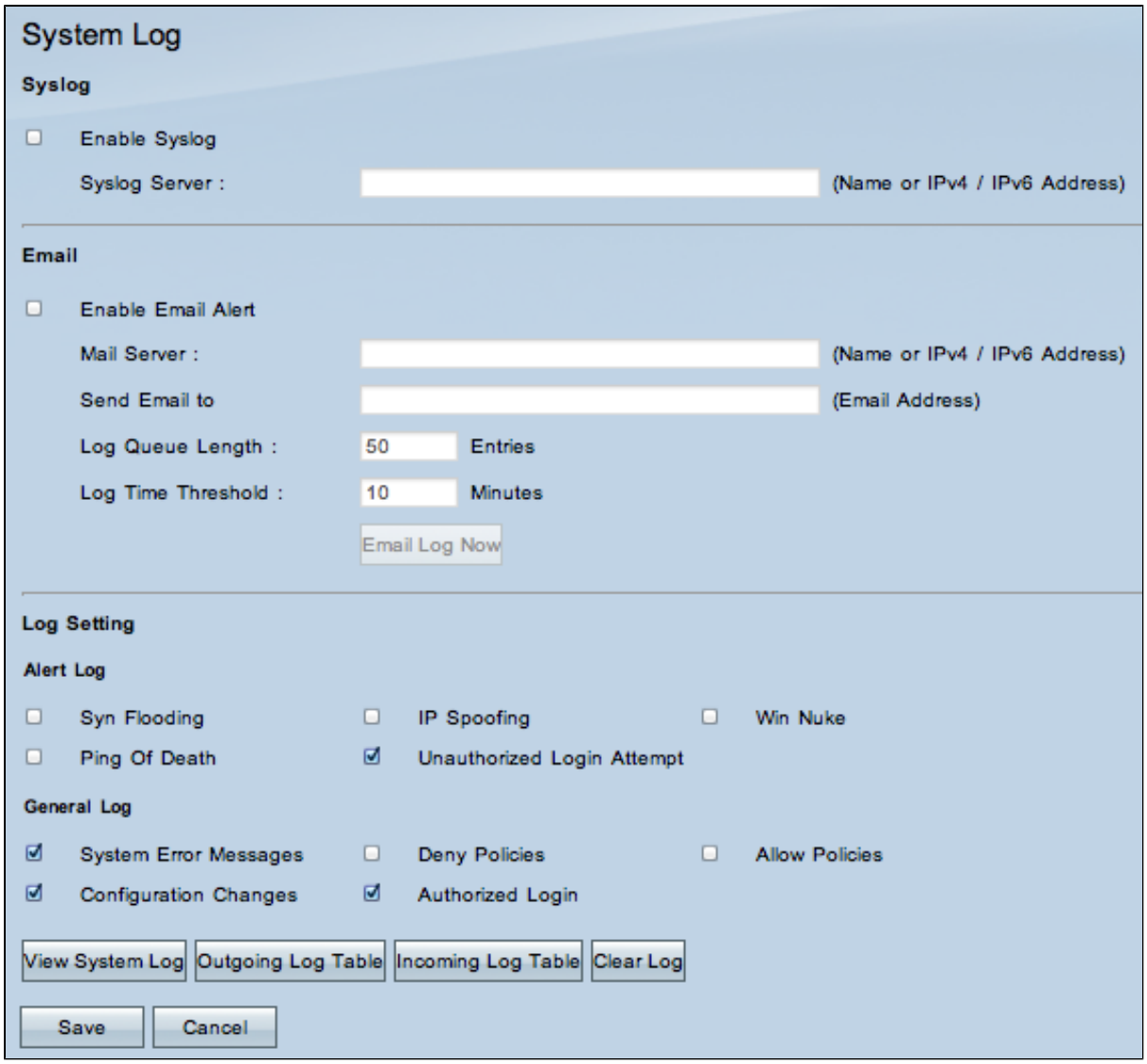
â€¢RV016
â€¢RV042
â€¢RV042G
â€¢RV082

Versión del software

â€¢v4.2.1.02

Configuración de Syslog y Alertas

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



Syslog

Esta sección explica cómo habilitar el router para enviar archivos de registro detallados a su servidor syslog cuando se registran eventos.

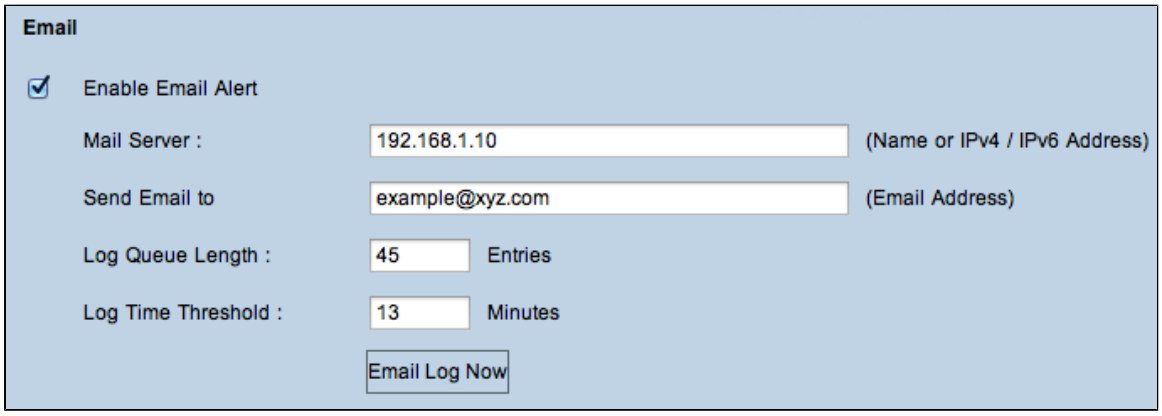
Paso 2. Marque la casilla de verificación **Enable Syslog** para habilitar el servicio syslog en el dispositivo.

Ahorro de tiempo: vaya al paso 4 si es necesario deshabilitar Syslog.

Paso 3. Introduzca el nombre de dominio o la dirección IP del servidor syslog en el campo Servidor Syslog.

Correo electrónico

Esta sección explica cómo habilitar el router para enviar alertas de correo electrónico cuando se registran eventos.



Paso 4. Marque **Activar alerta de correo electrónico** para activar la función. Esto permite que el router envíe alertas de correo electrónico a la dirección de correo especificada por el usuario.

Ahorro de tiempo: vaya al paso 10 si es necesario desactivar la alerta de correo electrónico.

Paso 5. Introduzca la dirección IPv4 o IPv6 del servidor SMTP del ISP en el campo Servidor de correo.

Nota: Es posible que el ISP requiera que identifique el router con un nombre de host. Elija **Setup > Network** para definir el nombre de host del router.

Paso 6. Introduzca la dirección de correo electrónico a la que desea enviar las alertas en el campo Enviar correo electrónico a.

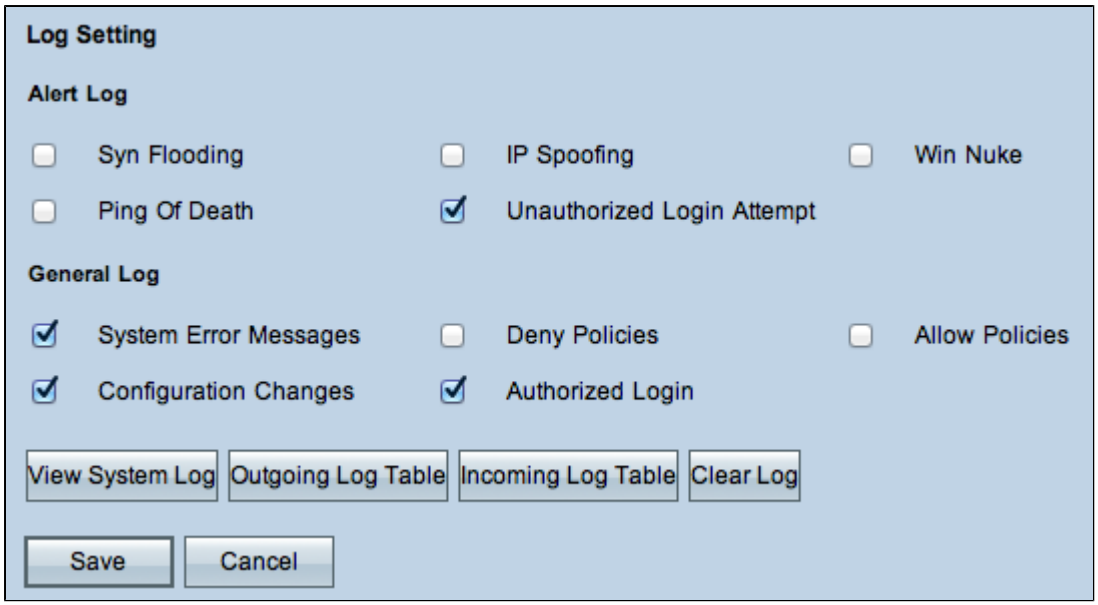
Paso 7. Introduzca el número de entradas de registro que se incluirán en el correo electrónico en el campo Longitud de la cola de registro. El valor predeterminado es 50.

Paso 8. Introduzca el número de minutos para recopilar datos antes de enviar el registro en el campo Log Time Threshold (Umbral de tiempo de registro). El umbral de tiempo de registro es el tiempo de espera máximo antes de enviar un mensaje de registro de correo electrónico. Cuando vence el umbral de tiempo del registro, se envía un correo electrónico independientemente de si el búfer del registro de correo electrónico está lleno o no. El valor predeterminado es 10 minutos

Paso 9. (Opcional) Haga clic en **Email Log Now** para enviar instantáneamente un mensaje a la dirección de correo electrónico especificada para probar la configuración.

Configuración de registro

Esta sección explica la variedad de eventos de los que se puede informar en los registros:



Paso 10. El área Registro de alertas contiene tipos comunes de ataques e intentos de inicio de sesión no autenticados. Marque las casillas de verificación de cualquier tipo de ataques deseados para incluirlos en el registro de eventos, o desmárquelos para omitirlos del registro de eventos.

· Inundación SYN: el atacante envía muchos paquetes SYNC de forma continua, lo que hace que el router abra varias sesiones para que el tráfico se llene de gente y el router rechace el tráfico legítimo.

· Suplantación de IP: el atacante envía paquetes desde una dirección IP de origen falsa para que el ataque parezca tráfico legítimo.

· Win Nuke: el atacante envía un mensaje fuera de banda a una máquina con Windows para hacer que el equipo de destino se bloquee.

· Ping de la muerte: el atacante envía un paquete IP grande para hacer que el equipo objetivo se bloquee.

· Intento de inicio de sesión no autorizado: alguien intentó iniciar sesión en la utilidad de configuración del router sin la autenticación adecuada.

Paso 11. El área Registro general incluye las acciones que se realizan para aplicar las políticas configuradas, así como los eventos rutinarios como los inicios de sesión autorizados y los cambios de configuración. Marque la casilla de verificación de cualquier evento que desee para incluirlo en el registro general. Desmarque la casilla de verificación para omitirla del registro general.

· Mensajes de error del sistema: todos los mensajes de error del sistema.

· Políticas de denegación: instancias en las que el router denegó el acceso según sus reglas de acceso.

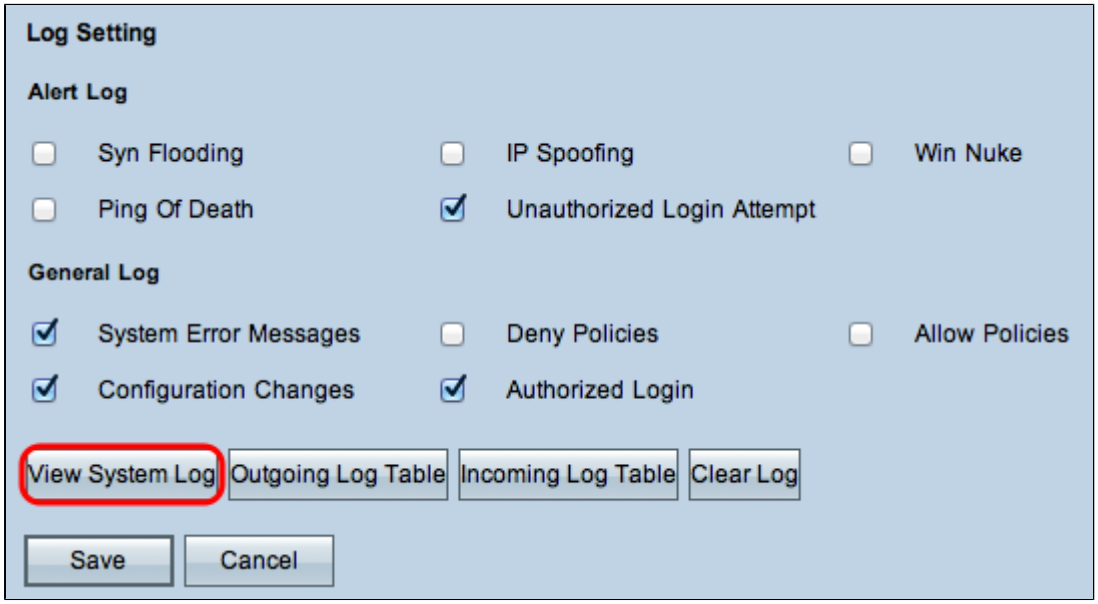
· Permitir Políticas: Instancias en las que el router permitió el acceso según sus Reglas de Acceso.

· Cambios de configuración: casos en los que alguien ha guardado cambios en la configuración.

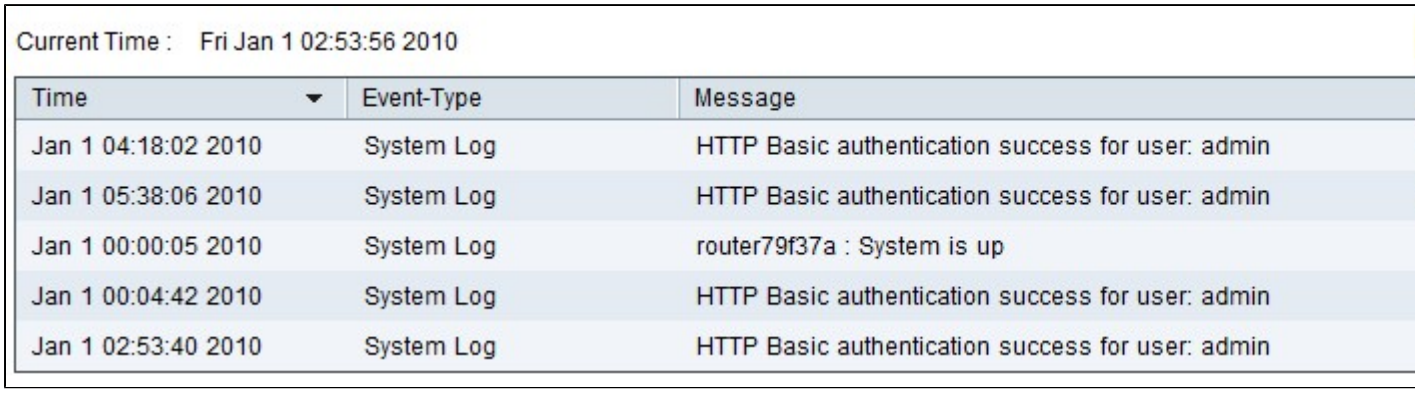
· Inicio de sesión autorizado: casos en los que alguien ha iniciado sesión correctamente en la utilidad de configuración del router después de introducir el nombre de usuario y la contraseña correctos.

· Evento de bloqueo de salida: instancias en las que hay un evento en la reputación web de ProtectLink o filtrado de URL.

Nota: El evento de bloqueo de salida solo está disponible en los routers VPN RV082.



Paso 12. (Opcional) Para ver el registro del sistema, haga clic en **Ver registro del sistema**. Aparece la ventana *Registro del sistema*:



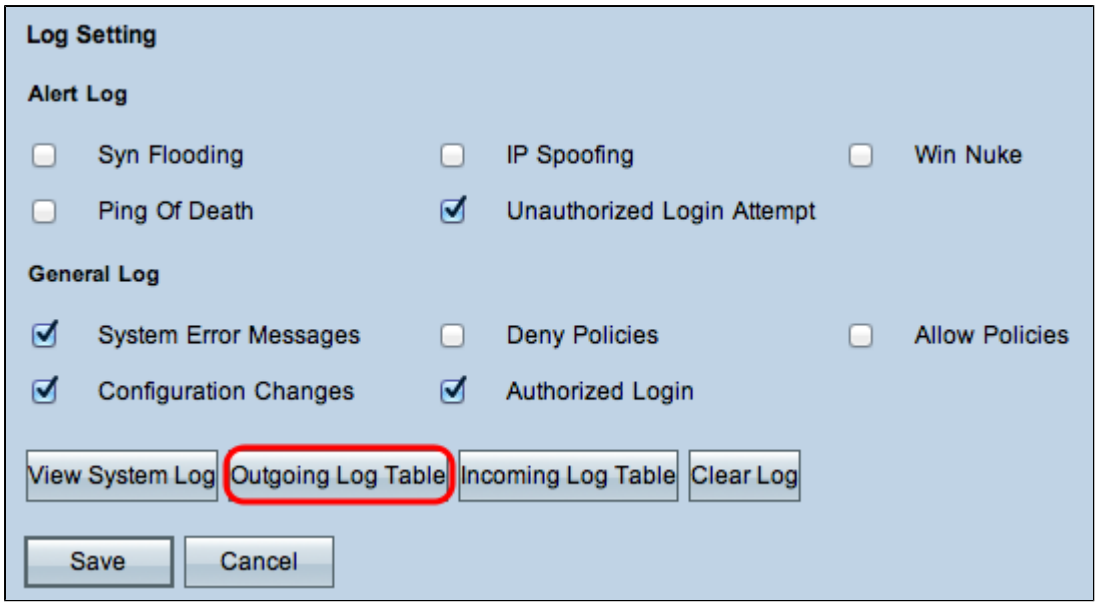
Nota: Las entradas del registro indican la fecha y la hora del tipo de evento y un mensaje. Este mensaje indica el tipo de política, como la regla de acceso, la dirección IP LAN del origen y la dirección MAC.

Paso 13. Elija un registro concreto de la lista desplegable.

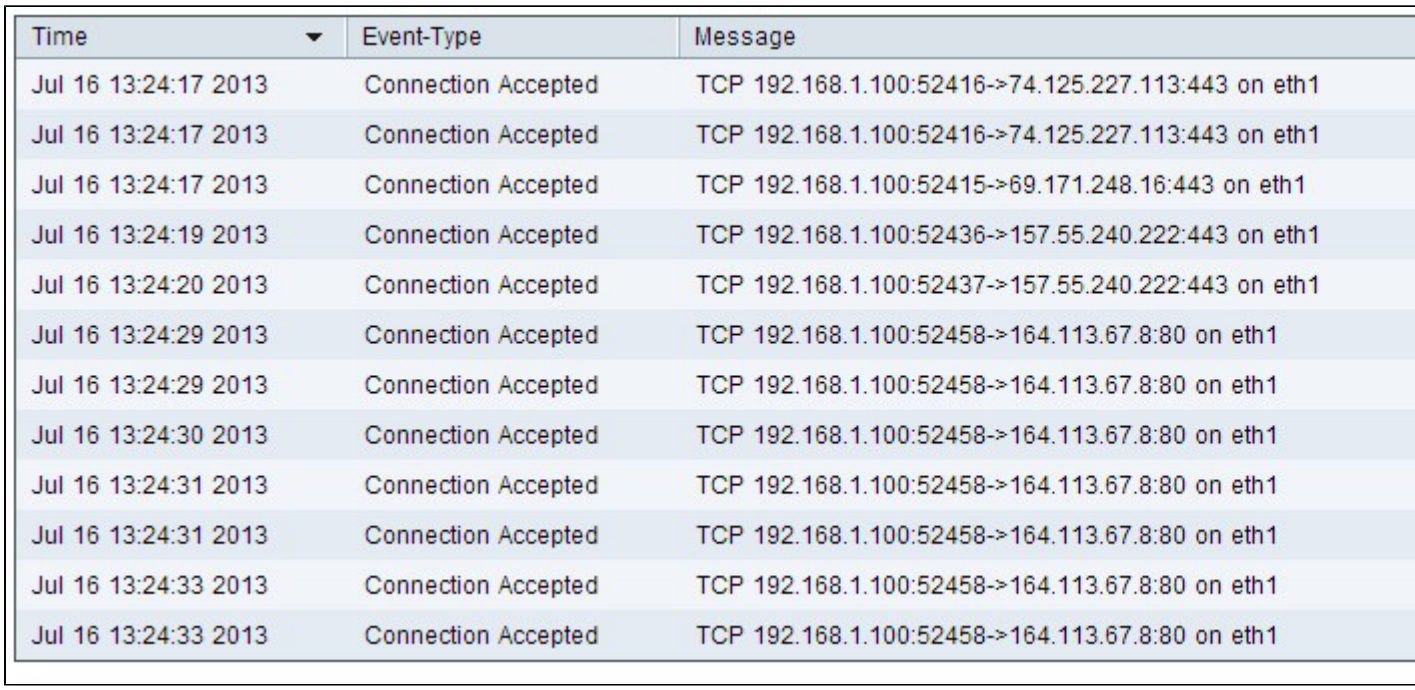
Paso 14. (Opcional) Para actualizar los datos, haga clic en **Actualizar**.

Paso 15. (Opcional) Para borrar toda la información mostrada, haga clic en **Borrar**.

Paso 16. Haga clic en **Cerrar** para cerrar la ventana.



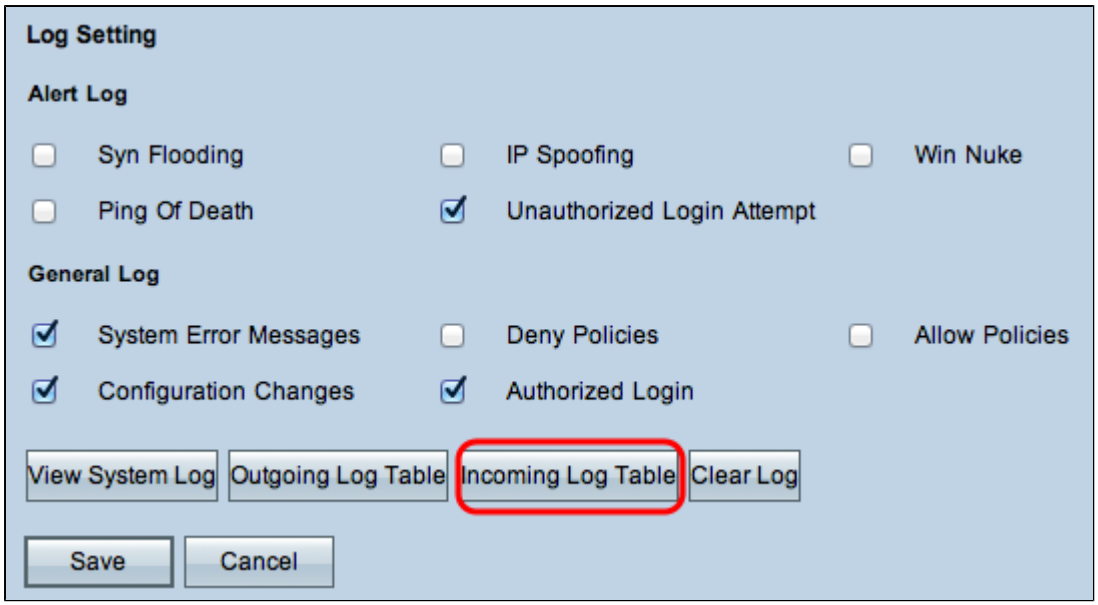
Paso 17. (Opcional) Para ver la información sobre los paquetes salientes, haga clic en **Tabla de registro de salida**. La información aparecerá en una ventana nueva.



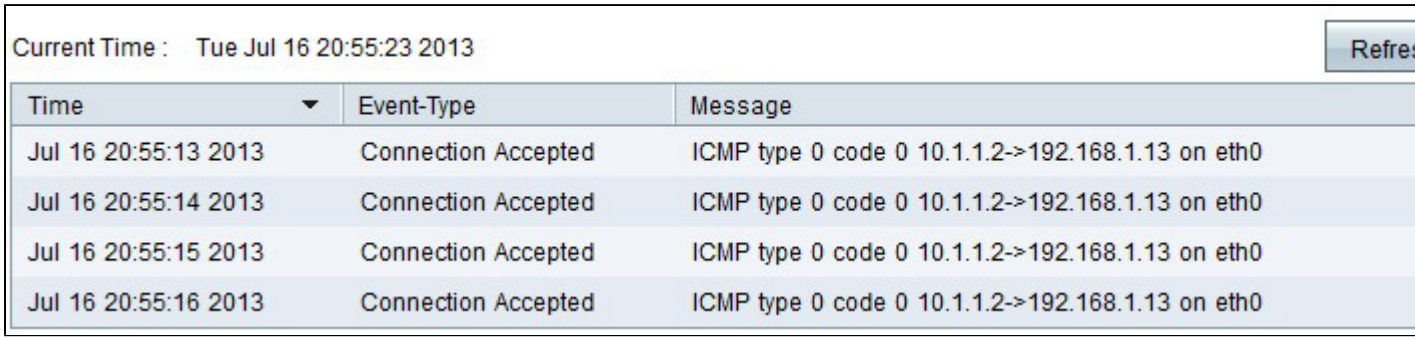
Time	Event-Type	Message
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52416->74.125.227.113:443 on eth1
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52416->74.125.227.113:443 on eth1
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52415->69.171.248.16:443 on eth1
Jul 16 13:24:19 2013	Connection Accepted	TCP 192.168.1.100:52436->157.55.240.222:443 on eth1
Jul 16 13:24:20 2013	Connection Accepted	TCP 192.168.1.100:52437->157.55.240.222:443 on eth1
Jul 16 13:24:29 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:29 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:30 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:31 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:31 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:33 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:33 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1

Paso 18. (Opcional) Para actualizar los datos, haga clic en **Actualizar**.

Paso 19. Haga clic en **Cerrar** para cerrar la ventana.

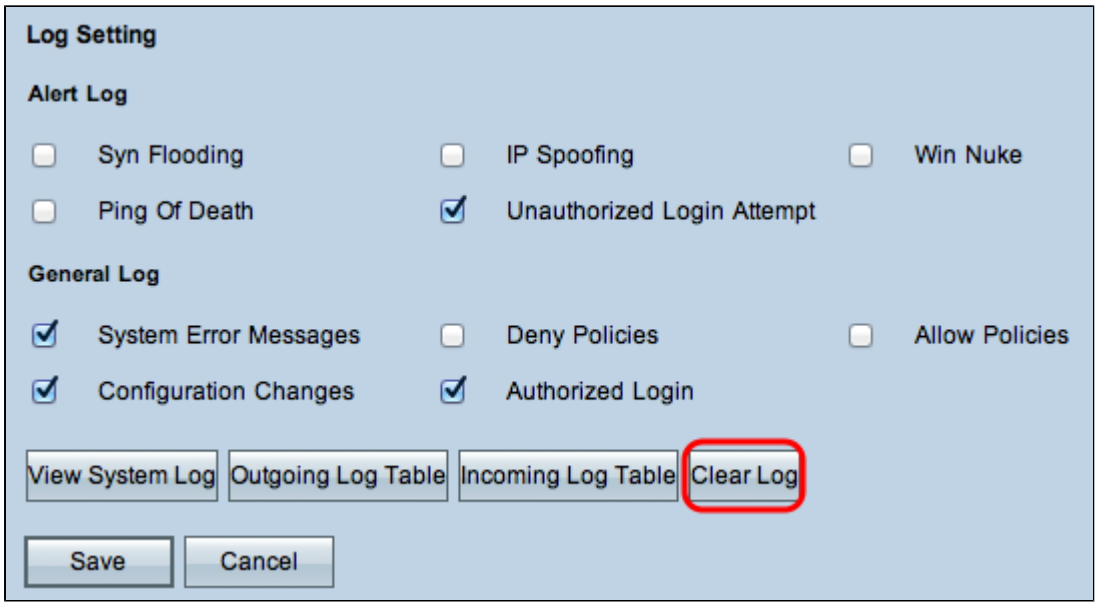


Paso 20. (Opcional) Haga clic en **Tabla de registro de entrada** para ver la información sobre los paquetes entrantes. La información se abre en una ventana nueva. Si aparece una advertencia sobre la ventana emergente, permita el contenido bloqueado.



Paso 21. (Opcional) Para actualizar los datos, haga clic en **Actualizar**.

Paso 22. Haga clic en **Cerrar** para cerrar la ventana.



Paso 23. (Opcional) Para borrar el registro, haga clic en **Borrar registro ahora**. Haga clic en este

botón sólo si no es necesario volver a ver la información en el futuro.

Paso 24. Haga clic en **Save** para guardar la configuración.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).