Configuración del Registro en Firepower Module para Eventos de Sistema/Tráfico Usando ASDM (Administración integrada)

Contenido

Introducción

Este documento describe los eventos de tráfico/ sistema del módulo Firepower y varios métodos para enviar estos eventos a un servidor de registro externo.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento del firewall ASA (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager).
- Conocimiento del dispositivo Firepower.

- Syslog, conocimiento del protocolo SNMP.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Módulos ASA Firepower (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) que ejecutan la versión de software 5.4.1 y superiores.
- Módulo ASA Firepower (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) que ejecuta la versión de software 6.0.0 y posterior.
- ASDM 7.5(1) y superiores.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Tipo de eventos

Los eventos del Módulo Firepower se pueden clasificar en dos tipos:-

1. Eventos de tráfico (eventos de conexión/eventos de intrusión/eventos de inteligencia de seguridad/eventos SSL/eventos de malware/archivos).
2. Eventos del sistema (eventos del sistema operativo Firepower (OS)).

Configurar

Configuración de un Destino de Salida

Paso 1. Configuración del servidor Syslog

Para configurar un servidor Syslog para eventos de tráfico, navegue hasta **Configuración > ASA Firepower Configuration > Políticas > Acciones Alertas** y haga clic en el menú desplegable **Crear alerta** y elija la opción **Crear alerta Syslog.** Introduzca los valores para el servidor Syslog.

Nombre: Especifique el nombre que identifica de forma única al servidor Syslog.

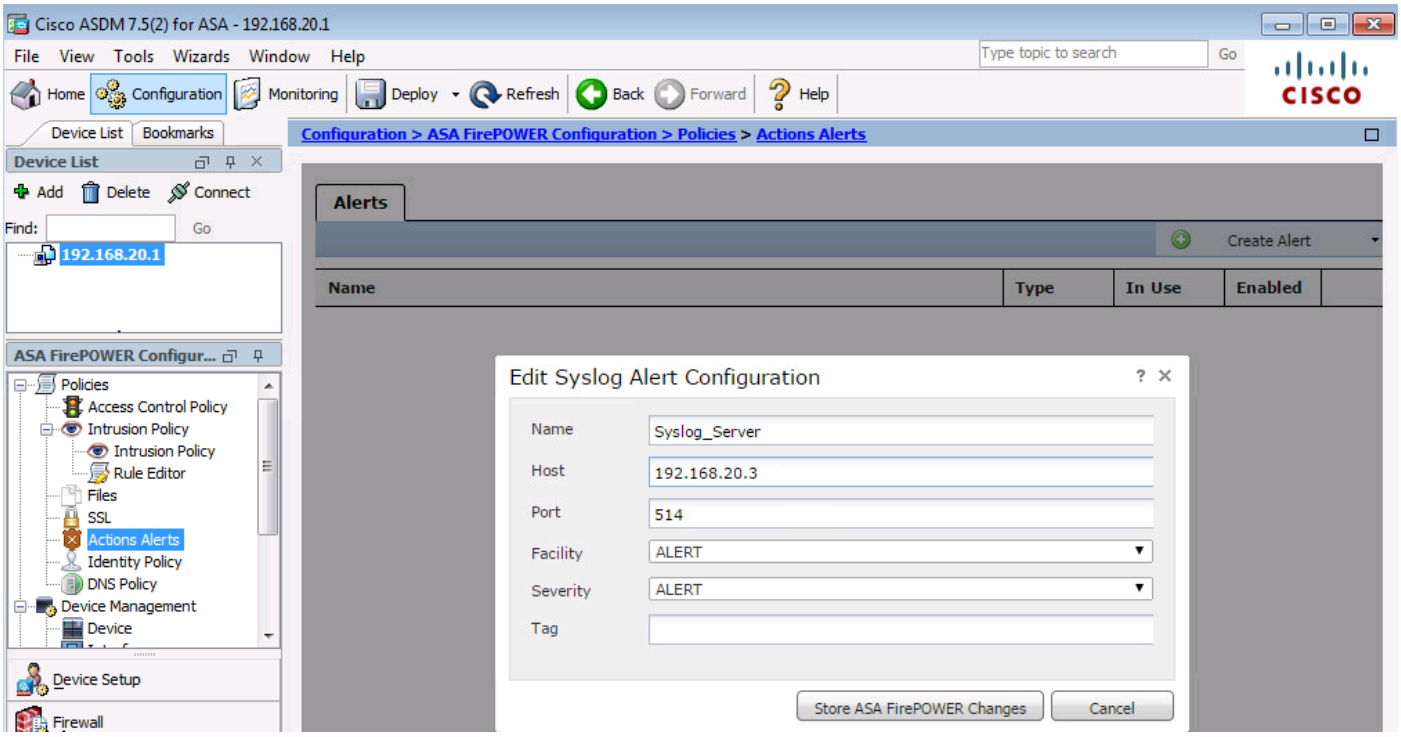
Host: Especifique la dirección IP/nombre de host del servidor Syslog.

Puerto: Especifique el número de puerto del servidor Syslog.

Instalación: Seleccione cualquier recurso que esté configurado en su servidor Syslog.

Gravedad: Seleccione cualquier Gravedad configurada en su servidor Syslog.

Etiqueta: Especifique el nombre de la etiqueta que desea que aparezca con el mensaje Syslog.



Paso 2.configuración del servidor SNMP

Para configurar un servidor de trampa SNMP para eventos de tráfico, Navegue hasta **Configuración de ASDM > Configuración de ASA Firepower > Políticas > Alertas de acciones** y haga clic en el menú desplegable **Crear alerta** y elija la opción Crear alerta SNMP.

Nombre: Especifique el nombre que identifica de forma única al servidor de trampa SNMP.

Servidor de trampa: Especifique la dirección IP/nombre de host del servidor de trampa SNMP.

Versión: Firepower Module soporta SNMP v1/v2/v3. Seleccione la versión SNMP en el menú desplegable.

Cadena de comunidad: Si selecciona v1 o v2 en la opción **Version**, especifique el nombre de comunidad SNMP.

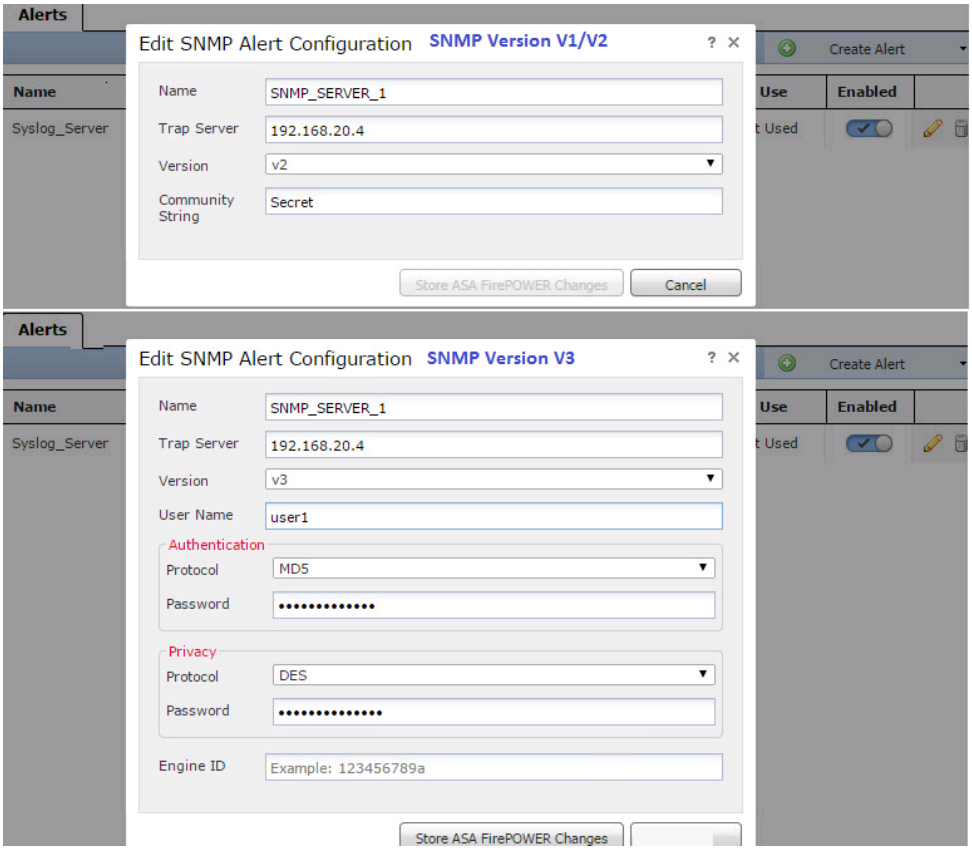
Nombre de usuario: Si selecciona v3 en la opción **Version**, el sistema solicita el **campo User Name**. Especifique el nombre de usuario.

Autenticación: Esta opción forma parte de la configuración SNMP v3. Proporciona autenticación basada en Hash

mediante algoritmos MD5 o SHA. En el menú desplegable **Protocol** seleccione el algoritmo hash & enter

contraseña en la opción **Password**. Si no desea utilizar esta función, seleccione la opción **Ninguno**.

Privacidad: Esta opción forma parte de la configuración SNMP v3. Proporciona cifrado mediante el algoritmo DES. En el menú desplegable **Protocol**, seleccione la opción **DES** e introduzca la contraseña en el campo **Password**. Si no desea utilizar la función de cifrado de datos, elija la opción **Ninguno**.



Configuración para enviar los eventos de tráfico

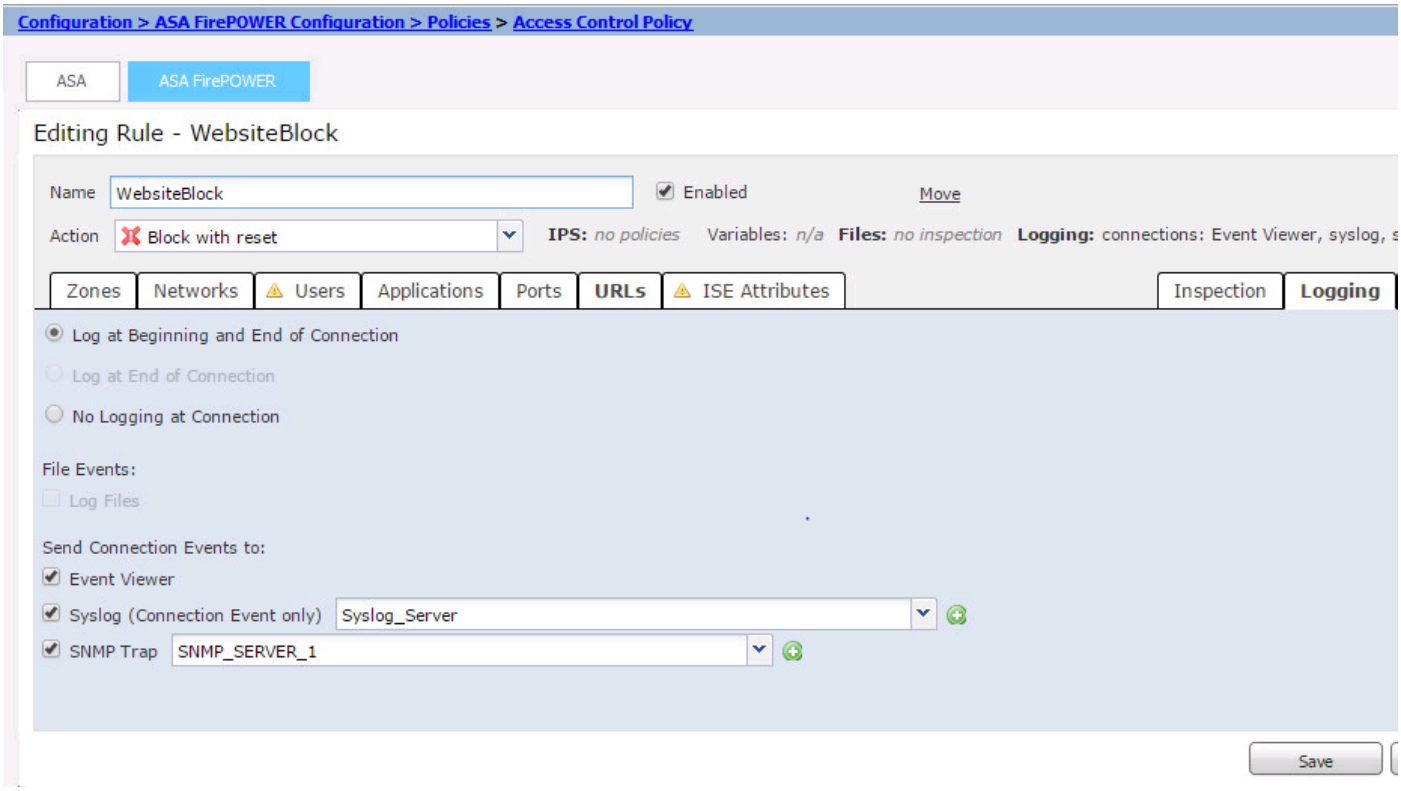
Habilitar registro externo para eventos de conexión

Los eventos de conexión se generan cuando el tráfico llega a una regla de acceso con el registro habilitado. Para habilitar el registro externo para los eventos de conexión, navegue hasta **(Configuración de ASDM > Configuración de ASA Firepower > Políticas > Política de control de acceso)** editar la **regla de acceso** y navegue hasta la opción registro.

Seleccione la opción de registro o bien **iniciar sesión al principio y al final de la conexión** o **iniciar sesión al final de la conexión**. Navegue hasta la opción **Enviar eventos de conexión a** y especifique dónde enviar eventos.

Para enviar eventos a un servidor Syslog externo, seleccione **Syslog** y luego seleccione una respuesta de alerta Syslog en la lista desplegable. Opcionalmente, puede agregar una respuesta de alerta de Syslog haciendo clic en el **icono** agregar.

Para enviar eventos de conexión a un servidor de trampa SNMP, seleccione **SNMP Trap** y, a continuación, seleccione una respuesta de alerta SNMP en la lista desplegable. Opcionalmente, puede agregar una respuesta de alerta SNMP haciendo clic en el **icono** agregar.



Habilitar registro externo para eventos de intrusión

Los eventos de intrusión se generan cuando una firma (reglas de sondeo) coincide con algún tráfico malintencionado. Para habilitar el registro externo para los eventos de intrusión, navegue hasta **Configuración de ASDM > Configuración de ASA Firepower > Políticas> Política de intrusión > Política de intrusión.** Cree una nueva directiva de intrusiones o edite la existente.Vaya a **Configuración avanzada > Respuestas externas.**

Para enviar eventos de intrusión a un servidor SNMP externo, seleccione la opción **Enabled** en **SNMP Alerting** y luego haga clic en la opción **Edit**.

Tipo de trampa: El tipo de trampa se utiliza para las direcciones IP que aparecen en las alertas. Si el sistema de administración de red representa correctamente el tipo de dirección INET_IPV4, puede seleccionarlo como binario. De lo contrario, selecciónelo como String.

Versión SNMP: Seleccione una de las opciones **Versión 2** or **Versión 3** botón de opción.

opción SNMP v2

Servidor de trampa: Especifique la dirección IP/nombre de host del servidor de trampa SNMP, como se muestra en esta imagen.

Cadena de comunidad: Especifique el nombre de la comunidad.

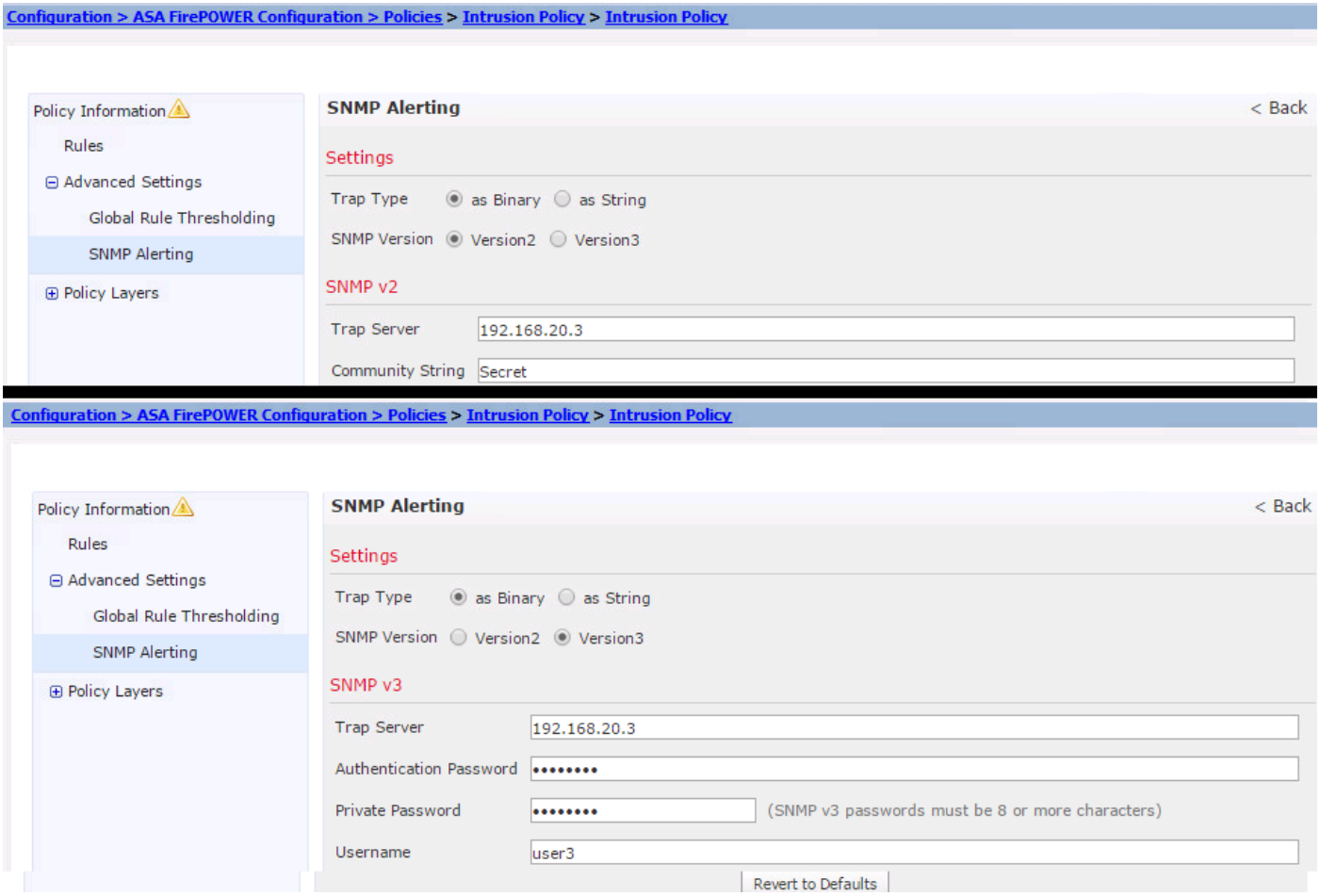
Opción SNMP v3

Servidor de trampa: Especifique la dirección IP/nombre de host del servidor de trampa SNMP, como se muestra en esta imagen.

Contraseña de autenticación: Especificarcontraseña requerida para la autenticación. SNMP v3 utiliza la función hash para autenticar la contraseña.

Contraseña privada: especifique la contraseña para el cifrado. SNMP v3 utiliza el cifrado de bloques Data Encryption Standard (DES) para cifrar esta contraseña.

User Name: Especifique el nombre de usuario.



Para enviar eventos de intrusión a un servidor Syslog externo, seleccione la opción **Habilitado** en **Syslog Alertas** a continuación, haga clic en el **Editar** como se muestra en esta imagen.

logging host: Especifique la dirección IP/nombre de host del servidor Syslog.

RECURSO: Seleccionar cualquier recurso que está configurado en el servidor Syslog.

Gravedad: Seleccione cualquier Gravedad configurada en su servidor Syslog.

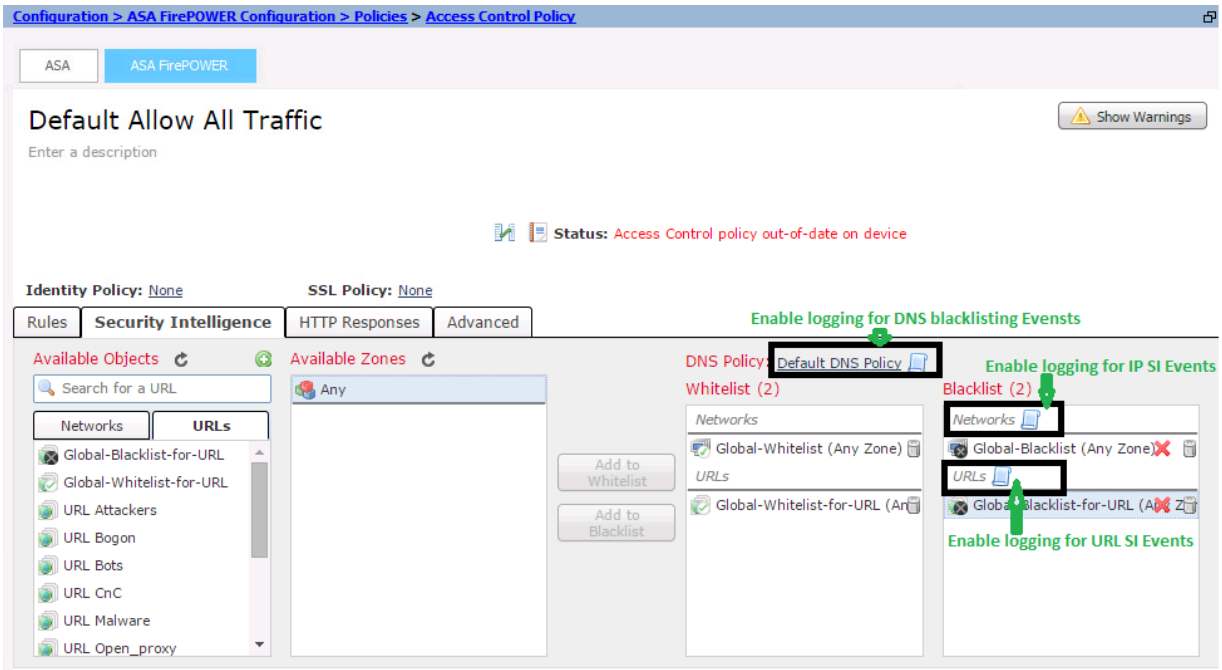
Habilitar registro externo para inteligencia de seguridad IP/inteligencia de seguridad DNS/inteligencia de seguridad URL

Inteligencia de seguridad IP/Inteligencia de seguridad DNS/Inteligencia de seguridad de URL se generan eventos cuando el tráfico coincide con cualquier dirección IP/nombre de dominio/base de datos de Inteligencia de seguridad de URL. Para habilitar el registro externo para los Eventos de Inteligencia de Seguridad IP/ URL/DNS, navegue hasta **(Configuración de ASDM > Configuración de ASA Firepower > Políticas > Política de Control de Acceso > Inteligencia de Seguridad)**,

Haga clic en el **icono** como se muestra en la imagen para habilitar el registro de IP/DNS/URL Security Intelligence. Al hacer clic en el icono, aparecerá un cuadro de diálogo para activar el registro y la opción para enviar los eventos al servidor externo.

Para enviar eventos a un servidor Syslog externo, seleccione **Syslog** y luego seleccione una respuesta de alerta Syslog en la lista desplegable. Opcionalmente, puede agregar una respuesta de alerta de Syslog haciendo clic en el icono de agregar.

Para enviar eventos de conexión a un servidor de trampa SNMP, seleccione **SNMP Trap** y luego seleccione una respuesta de alerta SNMP de la lista desplegable. Opcionalmente, puede agregar una respuesta de alerta SNMP haciendo clic en el icono agregar.



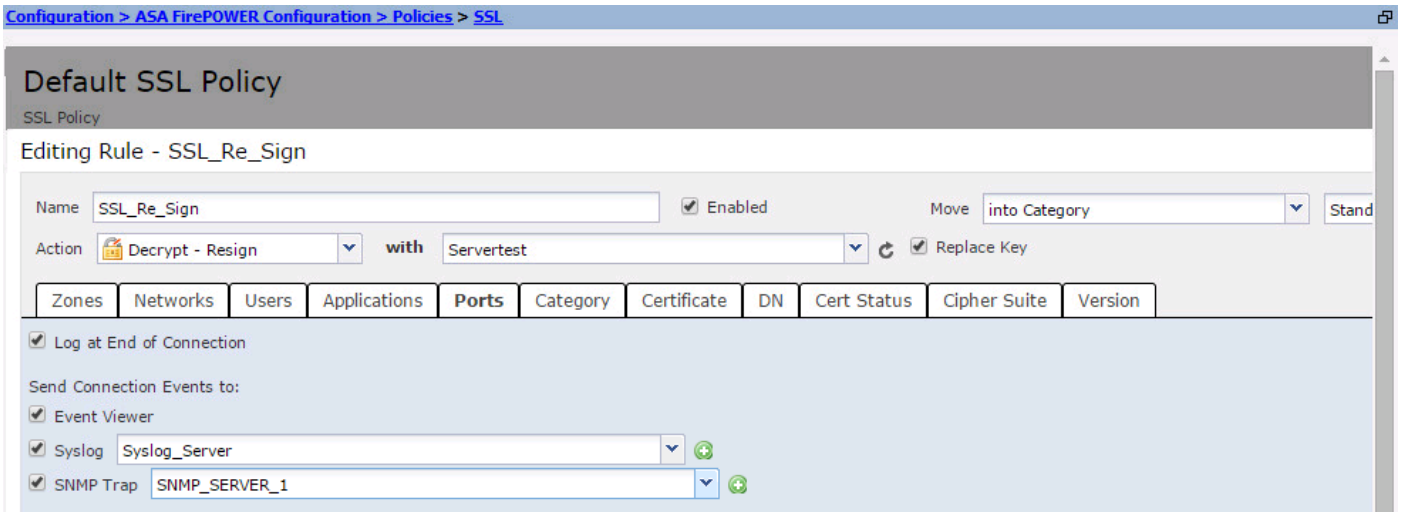
Habilitar registro externo para eventos SSL

Los eventos SSL se generan cuando el tráfico coincide con cualquier regla de la política SSL, en la que el registro está habilitado. Para habilitar el registro externo para el tráfico SSL, navegue hasta **Configuración ASDM > Configuración de ASA Firepower > Políticas > SSL.** Edite la regla existente o cree una nueva y navegue hasta la opción **logging**.Seleccione **log at End of Connection** option.

A continuación, navegue hasta **Enviar eventos de conexión** y especifique dónde enviar los eventos.

Para enviar eventos a un servidor Syslog externo, seleccione **Syslog** y, a continuación, seleccione una respuesta de alerta de Syslog en la lista desplegable. Opcionalmente, puede agregar una respuesta de alerta de Syslog haciendo clic en el icono de agregar.

Para enviar eventos de conexión a un servidor de trampa SNMP, seleccione **SNMP Trap** y, a continuación, seleccione una respuesta de alerta SNMP en la lista desplegable. Opcionalmente, puede agregar una respuesta de alerta SNMP haciendo clic en el icono agregar.



Configuración para enviar los eventos del sistema

Habilitar registro externo para eventos del sistema

Los eventos del sistema muestran el estado del sistema operativo Firepower. El administrador SNMP se puede utilizar para sondear estos eventos del sistema.

Para configurar el servidor SNMP para sondear los eventos del sistema desde el Módulo Firepower, necesita configurar una política del sistema que haga que la información esté disponible en la MIB de firepower (Base de información de administración) que puede ser consultada por el servidor SNMP.

Navegue hasta **Configuración de ASDM > Configuración de ASA Firepower > Local > Política del sistema** y haga clic en el **SNMP**.

Versión SNMP: Firepower Module admite SNMP v1/v2/v3. Especifique la versión SNMP.

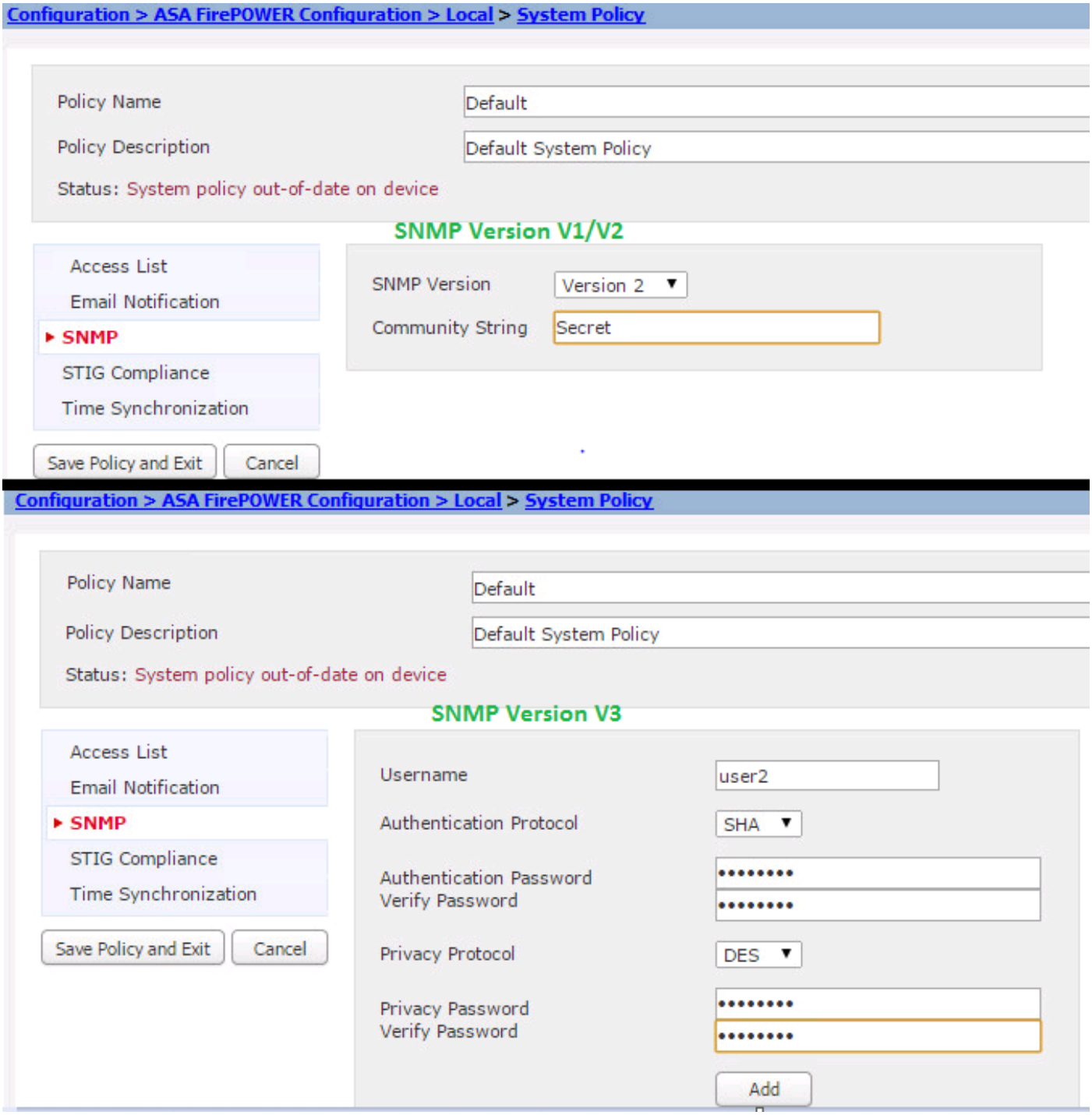
Cadena de comunidad: Si selecciona **v1/ v2** en la opción de versión SNMP, escriba el nombre de comunidad SNMP en el campo Cadena de comunidad.

Nombre de usuario: Si selecciona la opción **v3** en la versión. Haga clic en el botón **Add User** y especifique el **Username** en el campo username.

Autenticación: Esta opción forma parte de la configuración SNMP v3. Proporciona autenticación basada en el código de autenticación de mensajes hash usando algoritmos MD5 o SHA. Elija **Protocol** para el algoritmo hash e introduzca la contraseña

en el campo **Contraseña**. Si no desea utilizar la función de autenticación, seleccione la opción **Ninguno**.

Privacidad: Esta opción forma parte de la configuración SNMP v3. Proporciona cifrado mediante el algoritmo DES/AES. Seleccione el protocolo para el cifrado e introduzca la contraseña en el campo **Contraseña**. Si no desea la función de cifrado de datos, elija la opción **Ninguno**.



Nota: Una base de información de administración (MIB) es una colección de información organizada jerárquicamente. El archivo MIB (DCEALERT.MIB) para el Módulo Firepower está disponible en la ubicación del directorio (/etc/sf/DCEALERT.MIB) que se puede obtener desde esta ubicación de directorio.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems