Módulo de apertura de sesión de la potencia de fuego de la configuración para los eventos del tráfico del sistema usando el ASDM (Administración del En-cuadro)

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Antecedentes
Configurar
Configurar un destino de salida
Paso 1. Configuración de servidor de Syslog
Configuración del servidor del paso 2.SNMP
Configuración para enviar los eventos del tráfico
Registro externo del permiso para los eventos de conexión
Registro externo del permiso para los eventos de la intrusión
Habilite el registro externo para la inteligencia de Seguridad de la Seguridad Intelligence/URL de la seguridad IP Intelligence/DNS
Habilite el registro externo para los eventos SSL
Configuración para enviar los eventos del sistema
Registro externo del permiso para los eventos del sistema
Verificación
Troubleshooting
Información Relacionada
Discusiones relacionadas de la comunidad del soporte de Cisco

Introducción

Este documento describe los eventos del tráfico del sistema del módulo de la potencia de fuego y el diverso método de enviar estos eventos a un servidor de registro externo.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento del Firewall ASA (dispositivo de seguridad adaptante), ASDM (Administrador de dispositivos de seguridad adaptante).

- Conocimiento del dispositivo de la potencia de fuego.
- Syslog, conocimiento del protocolo SNMP.

Componentes Utilizados

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

- Versión de software corriente 5.4.1 de los módulos de la potencia de fuego ASA (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) y arriba.
- Versión de software corriente 6.0.0 del módulo de la potencia de fuego ASA (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) y arriba.
- ASDM 7.5(1) y arriba.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Tipo de eventos

Los eventos del módulo de la potencia de fuego se pueden categorizar en dos tipos: -

1. Eventos del tráfico (eventos de conexión/eventos de la intrusión/eventos/Malware de la inteligencia de Seguridad Events/SSL/eventos del archivo).
2. Eventos del sistema (eventos del operating system (OS) de la potencia de fuego).

Configurar

Configurar un destino de salida

Paso 1. Configuración de servidor de Syslog

Para configurar a un servidor de Syslog para los eventos del tráfico, navegar a la **configuración de la configuración > de la potencia de fuego ASA > a las directivas > a las alertas de las acciones** y hacer clic el menú desplegable de la **alerta del crear** y elegir la opción **crea la alerta del Syslog.** Ingrese los valores para el servidor de Syslog.

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

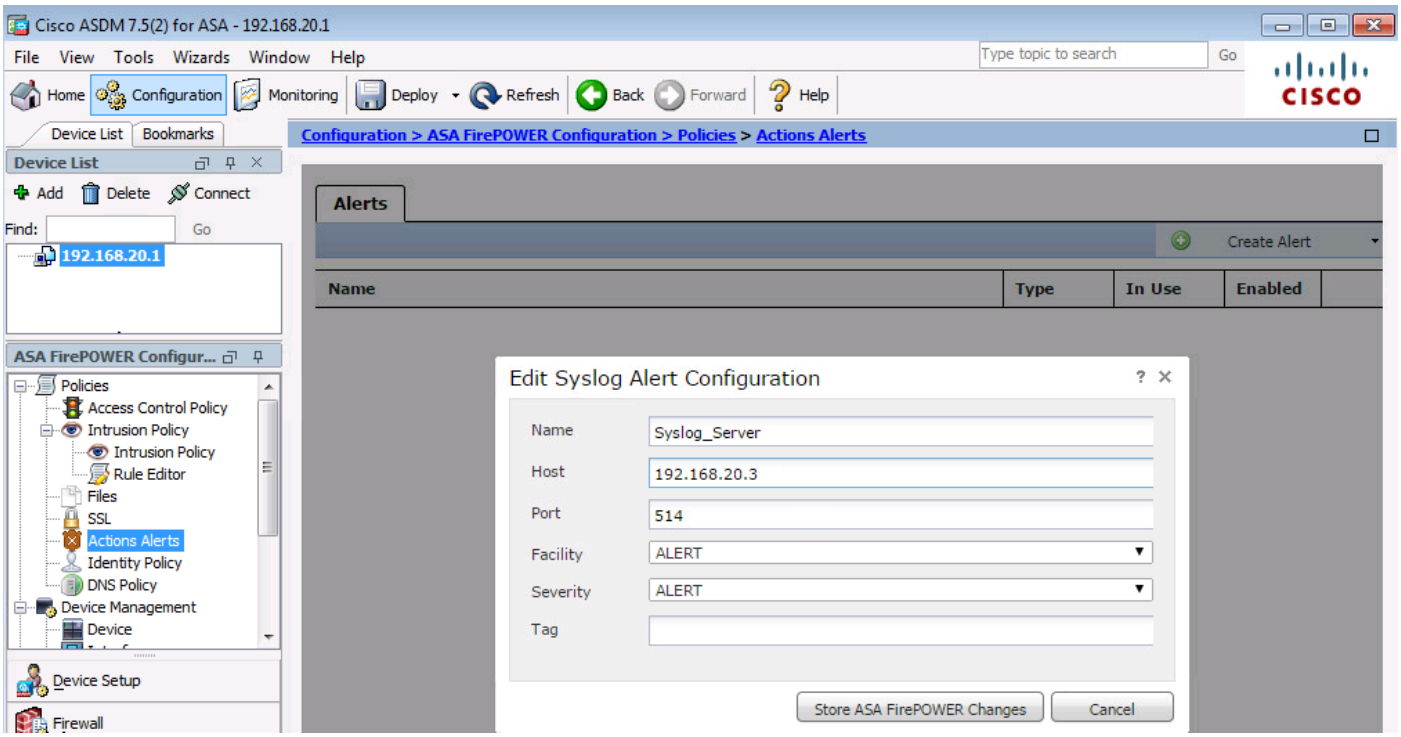
Host: Especifique la dirección IP/el nombre de host del servidor de Syslog.

Puerto: Especifique al número del puerto de servidor de Syslog.

Recurso: Seleccione cualquier recurso que se configure en su servidor de Syslog.

Gravedad: Seleccione cualquier gravedad que se configure en su servidor de Syslog.

Etiqueta: Especifique el nombre de la etiqueta que usted quiere aparecer con el mensaje de Syslog.



Configuración del servidor del paso 2.SNMP

Para configurar un servidor del SNMP trap para los eventos del tráfico, navegar a la **configuración de la Configuración de ASDM > de la potencia de fuego ASA > a las directivas > a las alertas de las acciones** y hacer clic el menú desplegable de la **alerta del crear** y elegir la opción **crea la alerta SNMP.**

Nombre: Especifique el nombre que identifica únicamente el servidor del SNMP trap.

Servidor del desvío: Especifique la dirección IP/el nombre de host del servidor del SNMP trap.

Versión: Soportes del módulo SNMP v1/v2/v3 de la potencia de fuego. Seleccione la versión de SNMP del menú desplegable.

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

Nombre de usuario: Si usted selecciona el v3 en la opción de la **versión**, el sistema indica el campo de **Nombre de usuario**. Especifique el nombre de usuario.

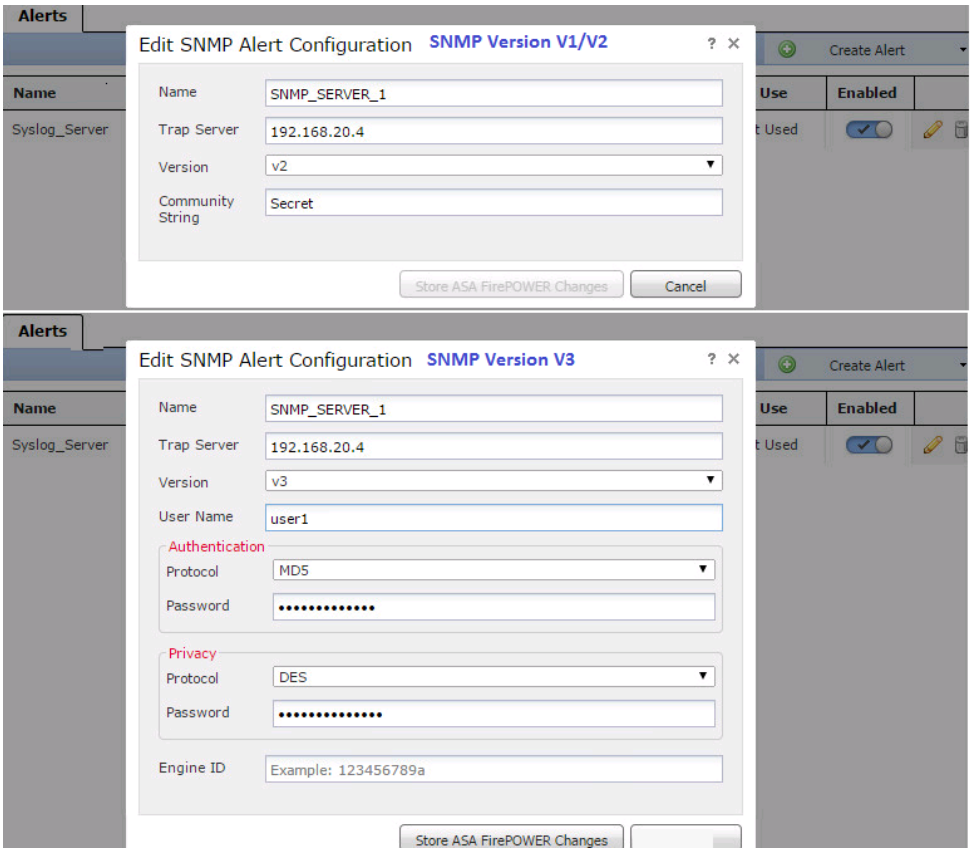
Autenticación: Esta opción es una configuración del v3 de la parte de SNMP. Proporciona la autenticación basada en el hash

algoritmo usando los algoritmos MD5 o SHA. En el **protocolo el** menú de persiana seleccionan el algoritmo de troceo y ingresan

contraseña en la **opción de contraseña**. Si usted no quiere utilizar esta característica, después no seleccione **ninguno** opción.

Aislamiento: Esta opción es una configuración del v3 de la parte de SNMP. Proporciona el cifrado

usando el algoritmo DES. En el menú del descenso del **protocolo** seleccione la opción como **DES&** ingresan la contraseña en el campo de **contraseña**. Si usted no quiere utilizar la función de encripción de datos, después no elija **ninguno** opción.



Configuración para enviar los eventos del tráfico

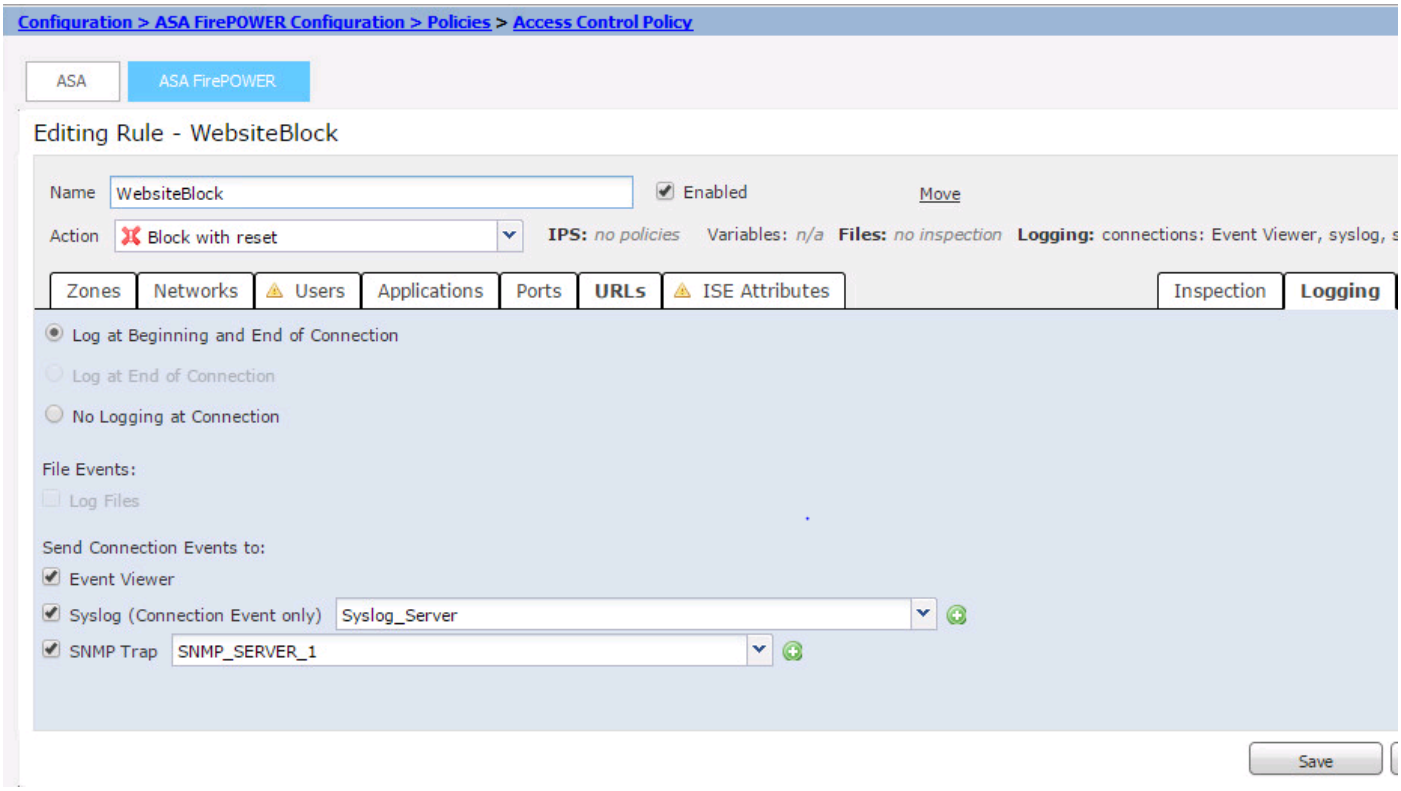
Registro externo del permiso para los eventos de conexión

Se generan los eventos de conexión cuando el tráfico golpea una regla de acceso con el registro habilitado. Para habilitar el registro externo para los eventos de conexión, navegue a **(Configuración de ASDM > configuración de la potencia de fuego ASA > las directivas > directiva del control de acceso)** editan la **regla de acceso** y navegan a la **opción de registro**.

Seleccione el **registro de la** opción de registro al **principio y al extremo de la conexión** o el **registro en el extremo de la conexión**. Navegue **para enviar los eventos de conexión a la** opción y para especificar donde enviar los eventos.

Para enviar los eventos a un servidor Syslog externo, a un **Syslog** selecto, y después seleccionar una respuesta de la alerta del Syslog de la lista desplegable. Opcionalmente, usted puede agregar una respuesta de la alerta del Syslog haciendo clic el **icono del** agregar.

Para enviar los eventos de conexión a un servidor del SNMP trap, a un **SNMP trap** selecto, y después seleccionar una respuesta de la alerta SNMP de la lista desplegable. Opcionalmente, usted puede agregar una respuesta de la alerta SNMP haciendo clic el **icono del** agregar.



Registro externo del permiso para los eventos de la intrusión

Se generan los eventos de la intrusión cuando una firma (reglas del snort) hace juego un cierto tráfico malévolo. Para habilitar el registro externo para los eventos de la intrusión, navegue a la **configuración de la Configuración de ASDM > de la potencia de fuego ASA > a la directiva de la intrusión de Policies> > a la directiva de la intrusión.** Cree una nueva directiva de la intrusión o edite la intrusión existente Policy.Navigate a la **configuración avanzada** > las **respuestas externas.**

Para enviar los eventos de la intrusión a un servidor SNMP externo, seleccione la opción **habilitada** en el **SNMP alertando** y después haga clic la opción del **editar**.

Tipo de trampa: Utilizan al tipo de trampa para los IP Addresses que aparece en las alertas. Si su sistema de administración de red rinde correctamente el tipo de dirección INET_IPV4, después usted puede seleccionar como binario. Si no, seleccione como cadena.

Versión de SNMP: Seleccione el botón de radio de la **versión 2** o de la **versión 3**.

Opción del v2 SNMP

Servidor del desvío: Especifique la dirección IP/el nombre de host del servidor del SNMP trap, tal y como se muestra en de esta imagen.

Cadena de comunidad: Especifique el nombre de la comunidad.

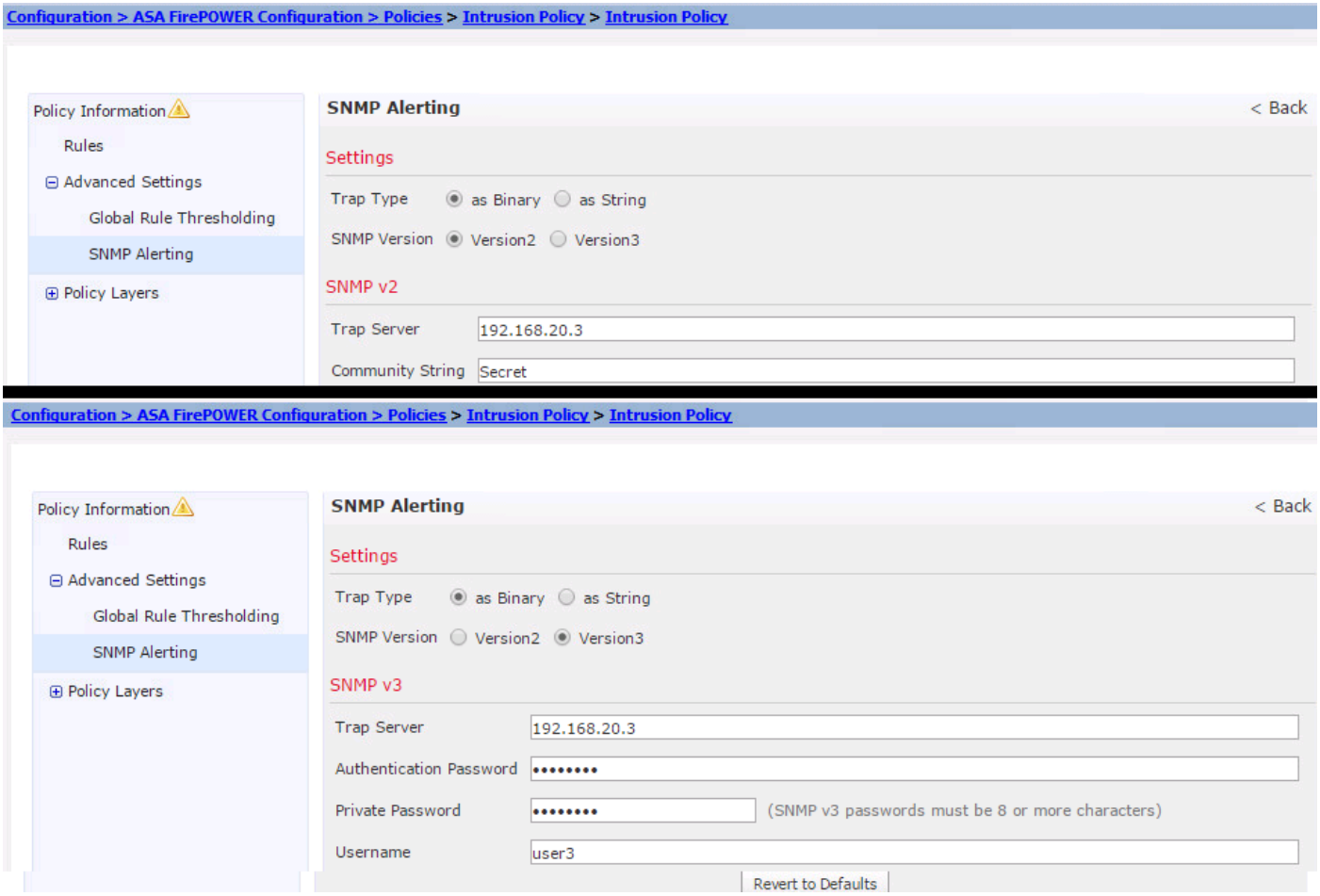
Opción del v3 SNMP

Servidor del desvío: Especifique la dirección IP/el nombre de host del servidor del SNMP trap, tal y como se muestra en de esta imagen.

Contraseña de autenticación: Specifypassword requirió para la autenticación. El v3 SNMP utiliza la función de troceo para autenticar la contraseña.

Contraseña privada: Especifique la contraseña para el cifrado. El v3 SNMP utiliza el cifrado en bloque del Data Encryption Standard (DES) para cifrar esta contraseña.

Nombre de usuario: Especifique el nombre de usuario.



Para enviar los eventos de la intrusión a un servidor Syslog externo, la opción selecta **habilitada** en el **Syslog** entonces **alertando** hace clic la opción del **editar**, tal y como se muestra en de esta imagen.

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

Recurso: Seleccione cualquier recurso que se configure en su servidor de Syslog.

Gravedad: Seleccione cualquier gravedad que se configure en su servidor de Syslog.

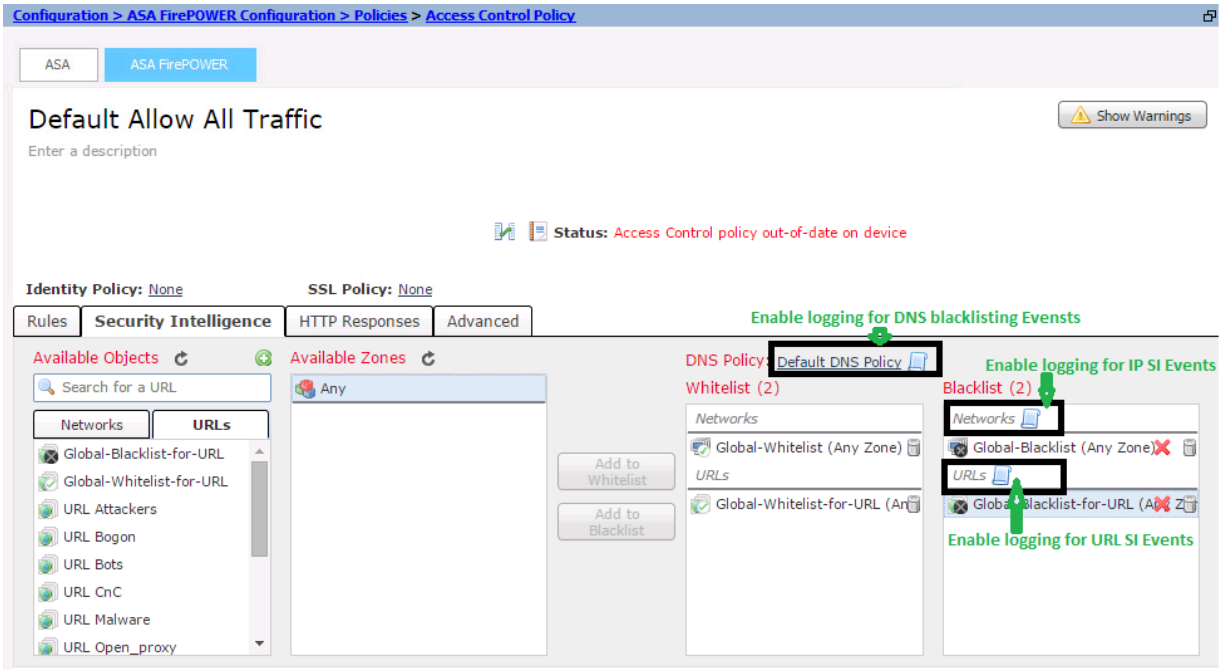
Habilite el registro externo para la inteligencia de Seguridad de la Seguridad Intelligence/URL de la seguridad IP Intelligence/DNS

Se generan los eventos de la **inteligencia de Seguridad de la Seguridad Intelligence/URL de la seguridad IP Intelligence/DNS** cuando el tráfico hace juego cualquier base de datos de la dirección IP/de la inteligencia de Seguridad del Domain Name /URL. Para habilitar el registro externo para los eventos de la inteligencia de Seguridad IP URL/DNS, navegue a **(Configuración de ASDM > configuración de la potencia de fuego ASA > las directivas > la inteligencia del > Security (Seguridad) de la directiva del control de acceso)**,

Haga clic el **icono** tal y como se muestra en de la imagen para habilitar el registro para la inteligencia de Seguridad IP/DNS/URL. Hacer clic el icono indica a un cuadro de diálogo que permita al registro y a la opción para enviar los eventos al servidor externo.

Para enviar los eventos a un servidor Syslog externo, a un **Syslog** selecto, y después seleccionar una respuesta de la alerta del Syslog de la lista desplegable. Opcionalmente, usted puede agregar una respuesta de la alerta del Syslog haciendo clic el icono del agregar.

Para enviar los eventos de conexión a un servidor del SNMP trap, a un **SNMP trap** selecto, y después seleccionar una respuesta de la alerta SNMP de la lista desplegable. Opcionalmente, usted puede agregar una respuesta de la alerta SNMP haciendo clic el icono del agregar.



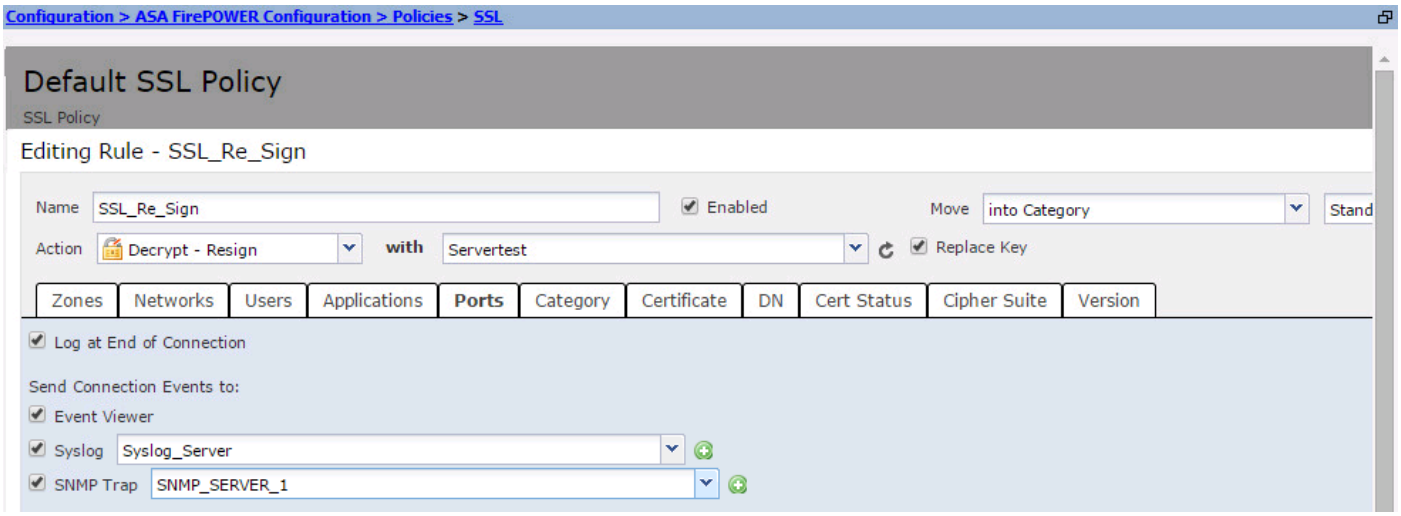
Registro externo del permiso para los eventos SSL

Se generan los **eventos SSL** cuando el tráfico hace juego cualquier regla en la directiva SSL, en la cual se habilita el registro. Para habilitar el registro externo para el tráfico SSL, navegue al **SSL de la Configuración de ASDM > de la potencia de fuego ASA a configuración > a las directivas >.** Edite la existencia o cree una nueva regla y navegue a la **opción de registro**. Seleccione el **registro en el final de la opción de conexión**.

Entonces navegue **para enviar los eventos de conexión a** y para especificar donde enviar los eventos.

Para enviar los eventos a un servidor Syslog externo, a un **Syslog** selecto, y después seleccionar una respuesta de la alerta del Syslog de la lista desplegable. Opcionalmente, usted puede agregar una respuesta de la alerta del Syslog haciendo clic el icono del agregar.

Para enviar los eventos de conexión a un servidor del SNMP trap, a un **SNMP trap** selecto, y después seleccionar una respuesta de la alerta SNMP de la lista desplegable. Opcionalmente, usted puede agregar una respuesta de la alerta SNMP haciendo clic el icono del agregar.



Configuración para enviar los eventos del sistema

Registro externo del permiso para los eventos del sistema

Los eventos del sistema muestran el estatus del sistema operativo de la potencia de fuego. El SNMP Manager puede ser utilizado para sondear estos eventos de sistemas.

Para configurar al servidor SNMP para sondear los eventos del sistema del módulo de la potencia de fuego, usted necesita configurar una política del sistema que haga la información disponible en la potencia de fuego MIB (Management Information Base) que se puede sondear por el servidor SNMP.

Navegue a la **política del sistema de la Configuración de ASDM > de la potencia de fuego ASA a configuración > a Local >** y haga clic el **SNMP**.

Versión de SNMP: Soportes del módulo SNMP v1/v2/v3 de la potencia de fuego. Especifique la versión de SNMP.

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

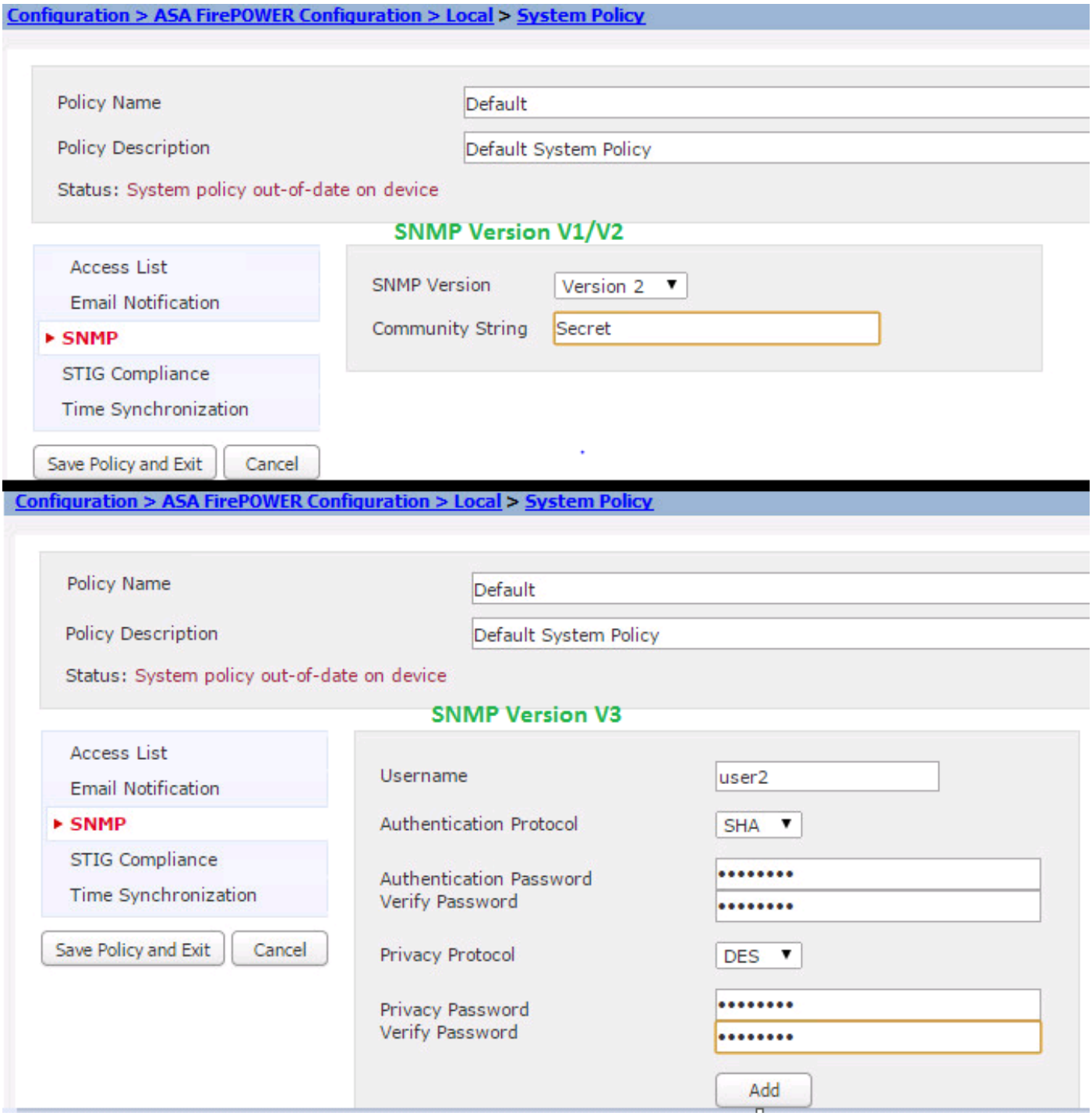
Nombre de usuario: Si usted selecciona la opción del **v3** en la opción de la versión. Haga clic el botón del **usuario del agregar** y especifique el **nombre de usuario** en el campo de nombre de usuario.

Autenticación: Esta opción es una configuración del v3 de la parte de SNMP. Proporciona la autenticación basada en el Message Authentication Code desmenuzado usando los algoritmos

MD5 o SHA. Elija el **protocolo** para el algoritmo de troceo y ingrese la contraseña

en el campo de **contraseña**. Si usted no quiere utilizar la característica de autenticación después no seleccione **ninguno** opción.

Aislamiento: Esta opción es una configuración del v3 de la parte de SNMP. Proporciona el cifrado usando el algoritmo DES/AES. Seleccione el protocolo para el cifrado y ingrese la contraseña en el campo de **contraseña**. Si usted no quiere la función de encripción de datos después no elija **ninguno** opción.



Nota: Una Base de información para administración (MIB) (MIB) es una Recolección de información que se ordena jerárquico. El archivo MIB (DCEALERT.MIB) para el módulo de la potencia de fuego está disponible en la ubicación del directorio (/etc/sf/DCEALERT.MIB) que se puede traer de esta ubicación del directorio.

Verificación

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

Troubleshooting

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

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems