Contenido

Introducción

Este documento describe la reputación de la inteligencia/de la dirección IP del Cisco Security y la configuración del IP que ponen (bloqueo) mientras que alimentación de encargo/auto el usar de la dirección IP baja de la reputación.

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

Nota: La filtración de la inteligencia de Seguridad requiere una licencia de la protección.

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

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

La inteligencia del Cisco Security comprende de varias colecciones regularmente actualizadas de IP Addresses que sean determinadas para tener una reputación pobre por el equipo de Cisco TALOS. El equipo de Cisco TALOS determina la reputación baja si alguna actividad maliciosa se origina de esos IP Addresses tales como Spam, malware, phishing los ataques etc.

La alimentación de la inteligencia de seguridad IP de Cisco sigue la base de datos de los atacantes, Bogon, los Bots, CNC, Dga, ExploitKit, Malware, Open_proxy, Open_relay, phishing, respuesta, Spam, sospechoso. El módulo de la potencia de fuego proporciona la opción para crear la alimentación de encargo de la dirección IP baja de la reputación.

Descripción de la alimentación de la inteligencia de Seguridad

Aquí está más información sobre el tipo de colecciones de la dirección IP que se puedan clasificar como diversas categorías en la inteligencia de Seguridad.

Atacantes: Colección de IP Addresses que está analizando para las vulnerabilidades o está intentando continuamente explotar otros sistemas.

Malware: Colección de IP Addresses que está intentando propagar el malware o está atacando activamente a cualquier persona que los visite.

Phishing: Colección de host que están intentando activamente engañar a los usuarios finales en ingresar la información confidencial como los nombres de usuario y contraseña.

Spam: Colección de host se han identificado que como la fuente de enviar los correos electrónicos del Spam.

Bots: La colección de host que estén participando activamente como parte de un botnet, y está siendo controlada por un regulador sabido de la red del bot.

CNC: Colección de host que se han identificado como los servidores que controlaban para un Botnet conocido.

OpenProxy: Colección de host que se saben para ejecutar los proxys abiertos de la red y para ofrecer exploración de la Web los servicios anónimos.

OpenRelay: La colección de host que se saben para ofrecer el correo electrónico anónimo que retransmite los servicios utilizó por los atacantes del Spam y del phishing.

TorExitNode: Colección de host que se saben para ofrecer los servicios de nodo de la salida para la red de Anonymizer del Tor.

Bogon: La colección de IP Addresses que no se afecta un aparato sino está enviando el tráfico.

Sospechoso: Colección de IP Addresses que está visualizando la actividad sospechosa y está bajo investigación activa.

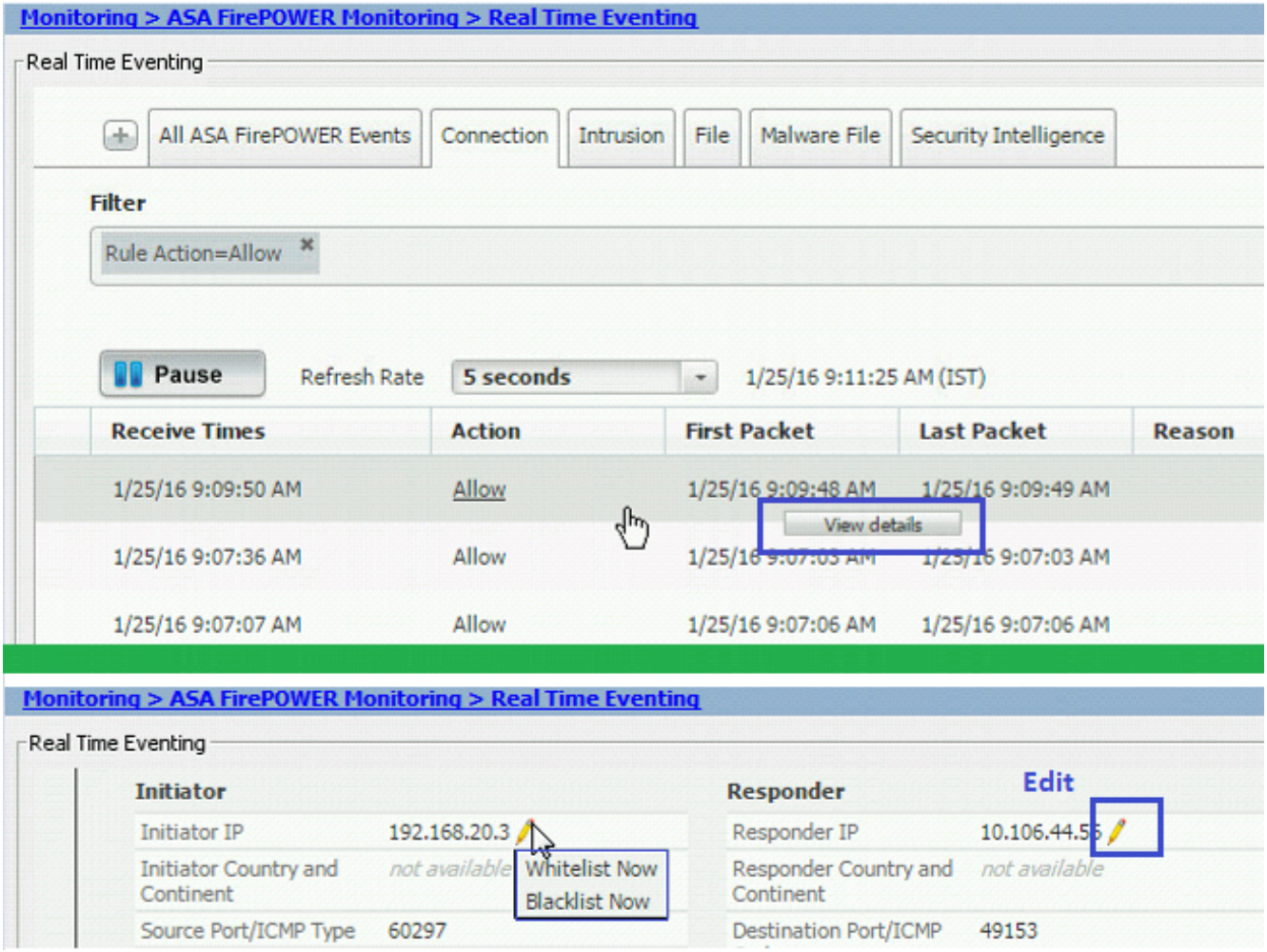
Respuesta: Colección de IP Addresses que en varias ocasiones se ha observado dedicado al comportamiento sospechoso o malévolo.

Agregue manualmente los IP Addresses a la lista negra global y a la lista blanca global

El módulo de la potencia de fuego permite que usted agregue ciertos IP Addresses a la lista negra global cuando usted sabe que son parte de una cierta actividad maliciosa. Los IP Addresses se pueden también agregar a la lista blanca global, si usted quiere permitir el tráfico a ciertos IP Addresses que son bloqueadas por los IP Addresses de la lista negra. Si usted agrega cualquier dirección IP a la lista negra global/a la lista blanca global, toma el efecto inmediatamente sin la necesidad de aplicar la directiva.

Para agregar la dirección IP a la lista blanca global Global-Blacklist/, navegar a **monitorear > supervisión de la potencia de fuego ASA > Eventing en tiempo real**, asomar el ratón en los eventos de conexión y seleccionar los **detalles de la visión**.

Usted puede agregar la fuente o el IP Address de destino a la lista blanca global Global-Blacklist/. **Ahora** haga clic en el **botón Edit** y **ahora** selecto**/lista negra de Whitelist** para agregar el IP Address a la lista respectiva, tal y como se muestra en de la imagen.



Para verificar que la fuente o el IP Address de destino esté agregada a la lista blanca global Global-Blacklist/, navegue a la **inteligencia del > Security (Seguridad) de la configuración de la configuración > de la potencia de fuego ASA > de la Administración del objeto > Network Lists y alimenta** y edita la **lista blanca global Global-Blacklist/**. Usted puede también utilizar el botón Delete Button para quitar cualquier dirección IP de la lista.

Cree la lista de encargo de dirección IP de la lista negra

La potencia de fuego permite que usted cree la lista de encargo de la red/de los IP Addresses que puede ser utilizada en poner (bloqueo). Hay la opción tres para hacer esto:

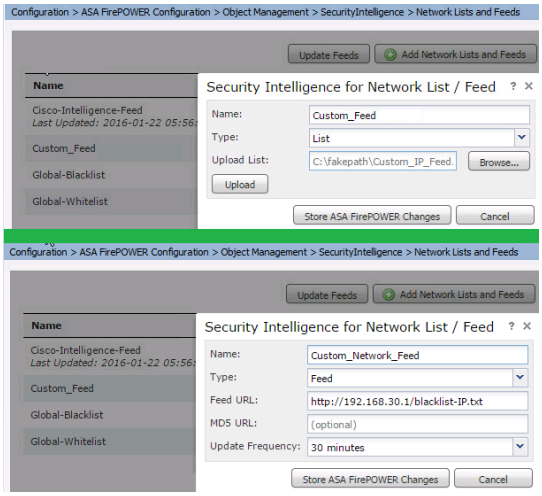
1. Usted puede escribir los IP Addresses a un archivo de texto (una dirección IP por la línea) y puede cargar el archivo al módulo de la potencia de fuego. Para cargar el archivo, navegue a la **inteligencia del > Security (Seguridad) de la configuración de la configuración > de la potencia de fuego ASA > de la Administración del objeto > Network Lists y a las alimentaciones** y después haga clic **agregan las listas de red y las alimentaciones**
   Nombre: Especifique el nombre de la lista de encargo. **Tipo:** Seleccione la **lista de la** lista desplegable. **Lista de la carga:** Elija **hojean** para localizar el archivo de texto en su sistema. Seleccione la **carga de la** opción para cargar el archivo.
2. Usted puede utilizar cualquier base de datos de tercera persona IP para la lista de encargo para la cual el módulo de la potencia de fuego entra en contacto el servidor del otro vendedor para traer la lista de IP Address. Para configurar esto, navegue a la **inteligencia del > Security (Seguridad) de la configuración de la configuración > de la potencia de fuego ASA > de la Administración del objeto > Network Lists y a las alimentaciones** y después haga clic **agregan las listas de red y las alimentaciones**
   Nombre: Especifique el nombre de la alimentación de encargo.

   Tipo: Alimentación selecta de la opción de la lista desplegable.

   Alimentación URL: Especifique el URL del servidor con el cual el módulo de la potencia de fuego debe conectar y descargue la alimentación.

   MD5 URL: Especifique el valor de troceo para validar el trayecto del URL de la alimentación.

   Frecuencia de la actualización: Especifique el intervalo de tiempo en el cual el sistema conecta con el servidor de la alimentación URL.



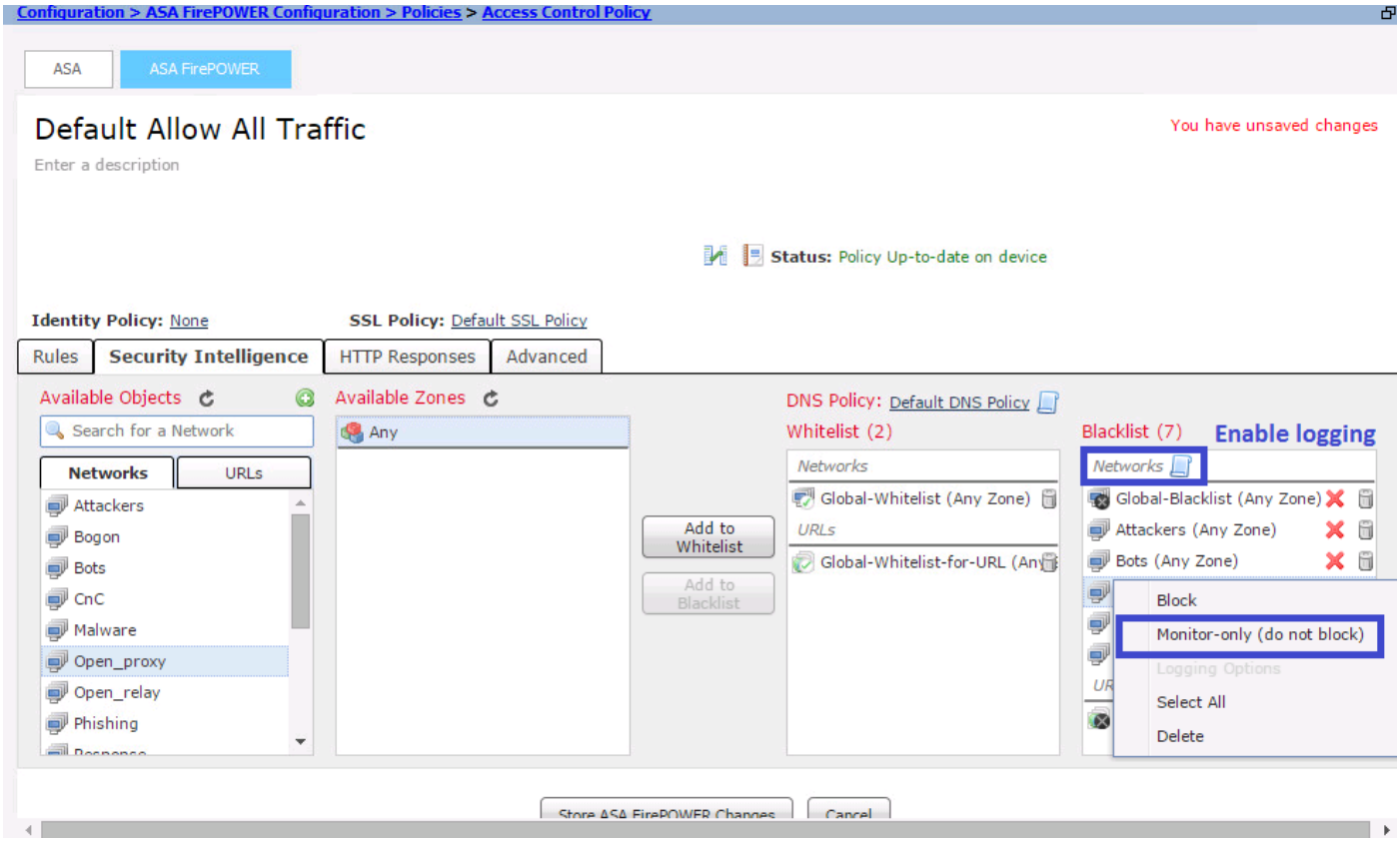
Configure la inteligencia de Seguridad

Para configurar la inteligencia de Seguridad, navegue a la **configuración de la configuración > de la potencia de fuego ASA > a las directivas > a la directiva del control de acceso,** lengueta selecta de la **inteligencia de Seguridad**.

Elija la alimentación del objeto disponible de la red, movimiento a la permitir/bloque de la columna de la **lista negra Whitelist/la** conexión a la dirección IP malévola.

Usted puede hacer clic el icono y habilitar el registro como se especifica en la imagen.

Si usted apenas quiere generar el evento para las conexiones IP malévolas en vez de bloquear la conexión, después haga clic con el botón derecho del ratón en la alimentación, eligen el **monitor-solamente (no hace el bloque)**, tal y como se muestra en de la imagen:



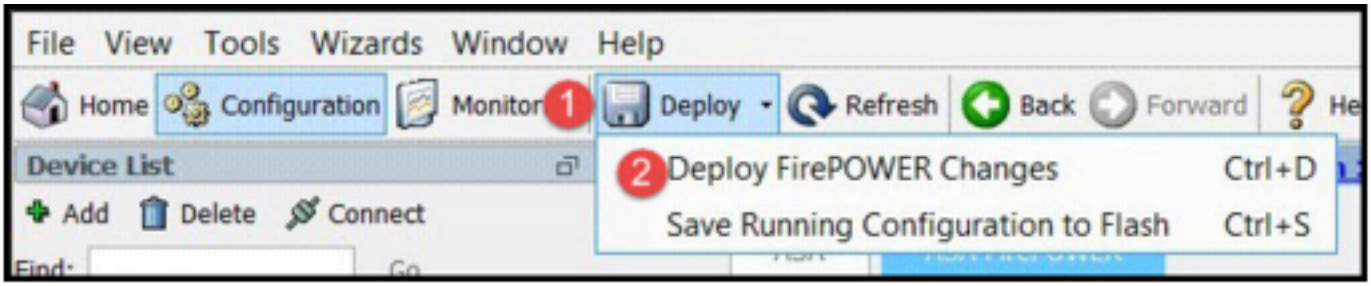
Elija los cambios de la potencia de fuego del almacén ASA de la opción para salvar los cambios

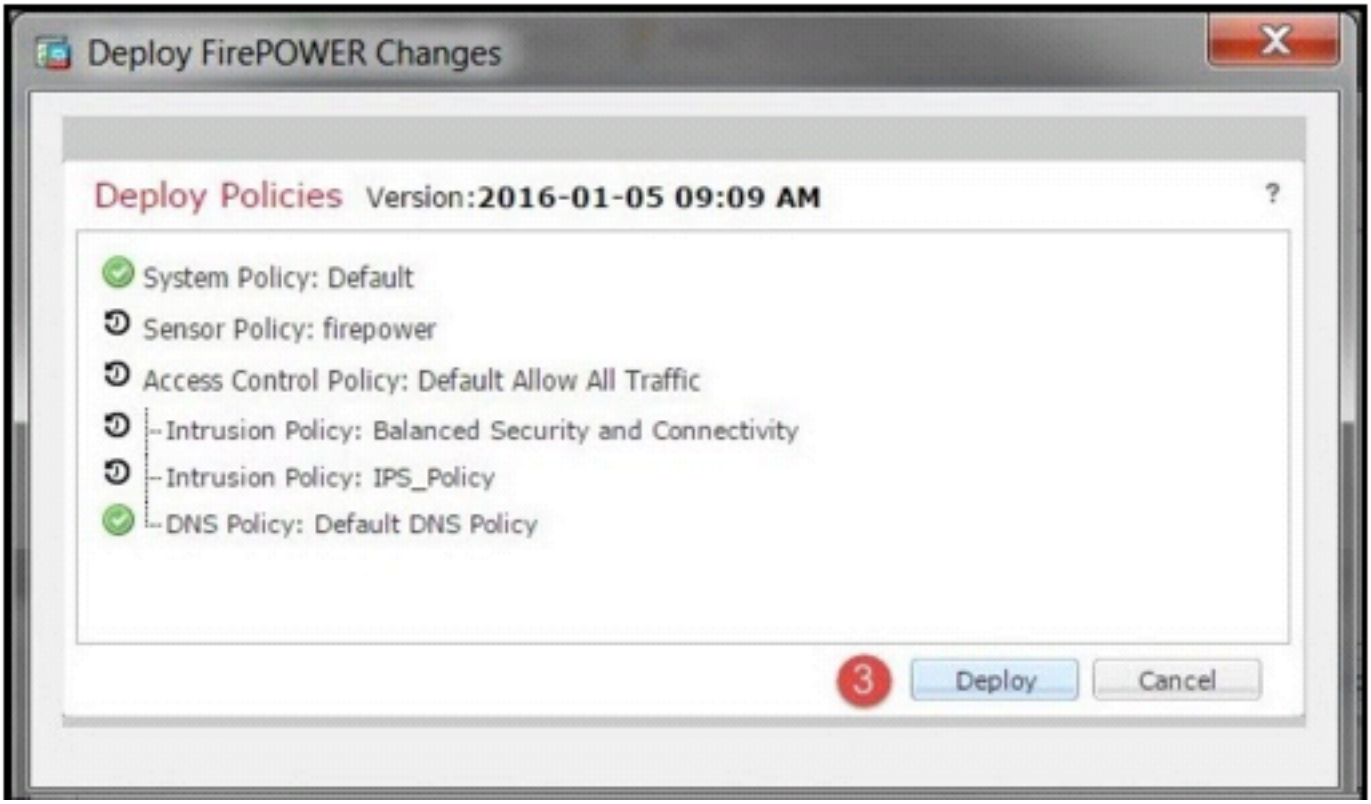
de política AC.

Despliegue la directiva del control de acceso

Para que los cambios tomen el efecto, usted debe desplegar la directiva del control de acceso. Antes de que usted aplique la directiva, vea una indicación que si la directiva del control de acceso es en el dispositivo o no anticuada.

Para desplegar los cambios al sensor, el tecleo **despliega** y elige **despliega los cambios de la potencia de fuego** después los selecciona **despliega** en la ventana emergente para desplegar los cambios.





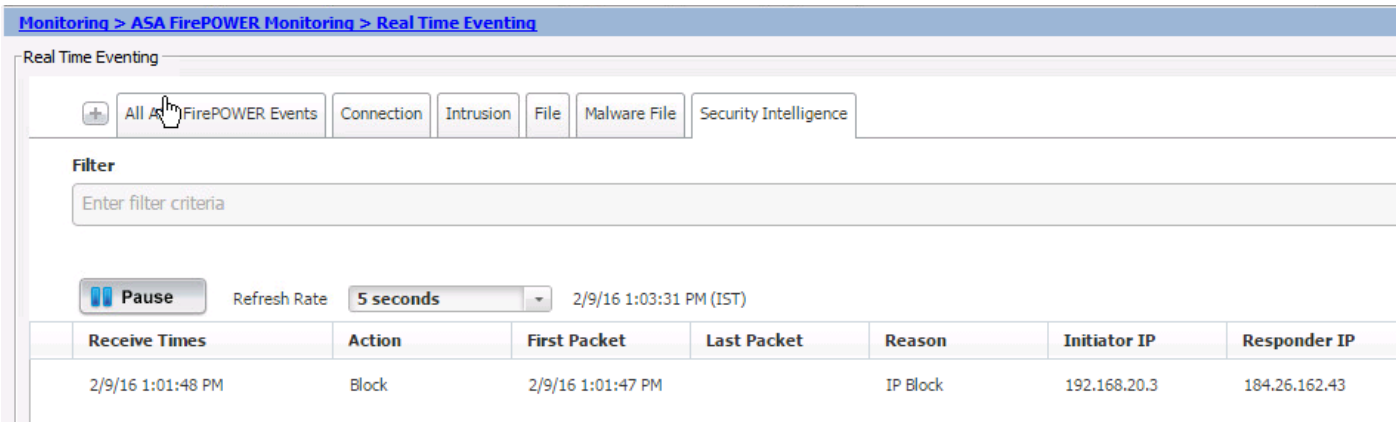
Nota: En la versión 5.4.x, aplicar la política de acceso al sensor, usted necesita hacer clic **aplica los cambios de la potencia de fuego ASA**

Nota: Navegue a **monitorear > supervisión de la potencia de fuego ASA > estatus de la tarea.** Asegúrese de que la tarea deba completar para aplicar los cambios de configuración.

¿Inteligencia de Seguridad? el monitorear de los eventos s

Para ver la inteligencia de Seguridad por el módulo de la potencia de fuego, navegue a

monitorear > supervisión de la potencia de fuego ASA > Eventing en tiempo real. Seleccione la lengueta de la **inteligencia de Seguridad**. Esto aparecerá los eventos tal y como se muestra en de la imagen:

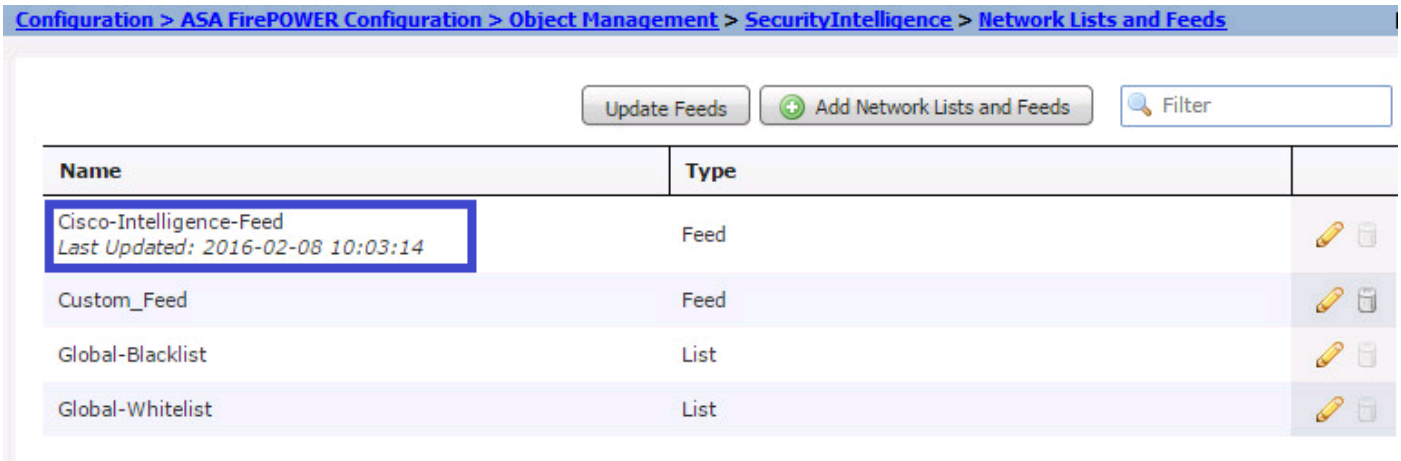


Verificación

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

Troubleshooting

Para asegurarse de que las alimentaciones de la inteligencia de Seguridad sean actualizadas, navegue a la **inteligencia del > Security (Seguridad) de la configuración de la configuración > de la potencia de fuego ASA > de la Administración del objeto > Network Lists y alimenta** y marca el tiempo en que la alimentación era la actualizada más reciente. Usted puede elegir el botón Edit para fijar la frecuencia de la actualización de la alimentación.



Asegúrese de que la implementación de política del control de acceso haya completado con éxito.

Monitoree la inteligencia de Seguridad de ver si el tráfico está bloqueando o no.

Información Relacionada

- **Guía de inicio rápido del módulo de la potencia de fuego de Cisco ASA**
- **Soporte Técnico y Documentación - Cisco Systems**