Configuración de la inteligencia de seguridad basada en dominios (política DNS) en el módulo FirePOWER con ASDM (administración integrada)

Contenido

Introducción

Este documento describe cómo configurar la inteligencia de seguridad basada en dominio (SI) en el módulo ASA con FirePOWER con el uso de Adaptive Security Device Manager (ASDM).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento del firewall ASA (Adaptive Security Appliance)

- ASDM (administrador adaptable de dispositivos de seguridad)
- Conocimiento del módulo FirePOWER

Nota: El filtro de inteligencia de seguridad requiere una licencia de protección.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Módulos ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) con la versión de software 6.0.0 y posterior
- Módulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) con la versión de software 6.0.0 y posterior

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

Firepower system proporciona la capacidad de interceptar solicitudes de tráfico DNS y busca el nombre de dominio malintencionado. Si el módulo Firepower encuentra un dominio malintencionado, Firepower toma las medidas adecuadas para mitigar la solicitud según la configuración de la política DNS.

Nuevos métodos de ataque diseñados para infringir la inteligencia basada en IP, mal uso de las funciones de equilibrio de carga DNS para ocultar la dirección IP real de un servidor malintencionado. Mientras que las direcciones IP asociadas con el ataque se intercambian con frecuencia, el nombre de dominio rara vez se cambia.

Firepower ofrece la capacidad de redirigir la solicitud maliciosa a un servidor sinkhole, que puede ser un servidor honeypot para detectar, desviar o estudiar intentos de conocer más sobre el tráfico del ataque.

Descripción general de las listas de dominios y fuentes

Las Listas de dominios y fuentes contienen la lista del nombre de dominio malintencionado que se clasifica en las distintas categorías según el tipo de ataque. Normalmente, las fuentes se pueden clasificar en dos tipos.

Cisco TALOS proporcionó listas de dominios y fuentes

Atacantes DNS: Colección de nombres de dominio que buscan continuamente vulnerabilidades o intentan explotar otros sistemas.

DNS Bogon: Colección de nombres de dominio que no asignan sino que reenvían el tráfico, también conocido como IP falsas.

Bots DNS: Colección de nombres de dominio que participan activamente como parte de una botnet y que son controlados por un controlador botnet conocido.

DNS CnC: Colección de nombres de dominio identificados como servidores de control para una Botnet conocida.

Kit de aprovechamiento de vulnerabilidades DNS: Colección de nombres de dominio que intentan explotar otros sistemas.

Malware de DNS: colección de nombres de dominio que intentan propagar malware o atacan activamente a cualquiera que los visite.

DNS Open_proxy: colección de nombres de dominio que ejecutan Open Web Proxies y ofrecen servicios de exploración web anónimos.

DNS Open_relay: recopilación de nombres de dominio que ofrecen servicios de retransmisión de correo electrónico anónimos utilizados por atacantes de spam y phishing.

DNS Phish: Colección de nombres de dominio que intentan engañar activamente a los usuarios finales para que ingresen su información confidencial como nombres de usuario y contraseñas.

Respuesta DNS: recopilación de nombres de dominio que se observa repetidamente y que se dedican a comportamientos sospechosos o maliciosos.

DNS Spam: Colección de nombres de dominio identificados como el origen que envía mensajes de correo electrónico de spam.

DNS sospechoso: colección de nombres de dominio que muestran actividad sospechosa y están bajo investigación activa.

DNS Tor_exit_node: Colección de nombres de dominio que ofrecen servicios de nodo de salida para la red Tor Anonymizer.

Fuentes y listas de dominios personalizados

Lista negra global para DNS: Recopilación de la lista personalizada de nombres de dominio identificados como maliciosos por el administrador.

Lista blanca global para DNS: Recopilación de la lista personalizada de nombres de dominio identificados como auténticos por el administrador.

Configuración de la inteligencia de seguridad DNS

Hay varios pasos para configurar la inteligencia de seguridad basada en el nombre de dominio.

1. Configurar la fuente/lista DNS personalizada (opcional)

2. Configurar el objeto Sinkhole (opcional)
3. Configuración de la política DNS
4. Configuración de la política de control de acceso
5. Implementar la política de control de acceso

Paso 1. Configuración de la fuente/lista DNS personalizada (opcional).

Hay dos listas predefinidas que le permiten agregar los dominios. Cree sus propias Listas y fuentes para los dominios que desea bloquear.

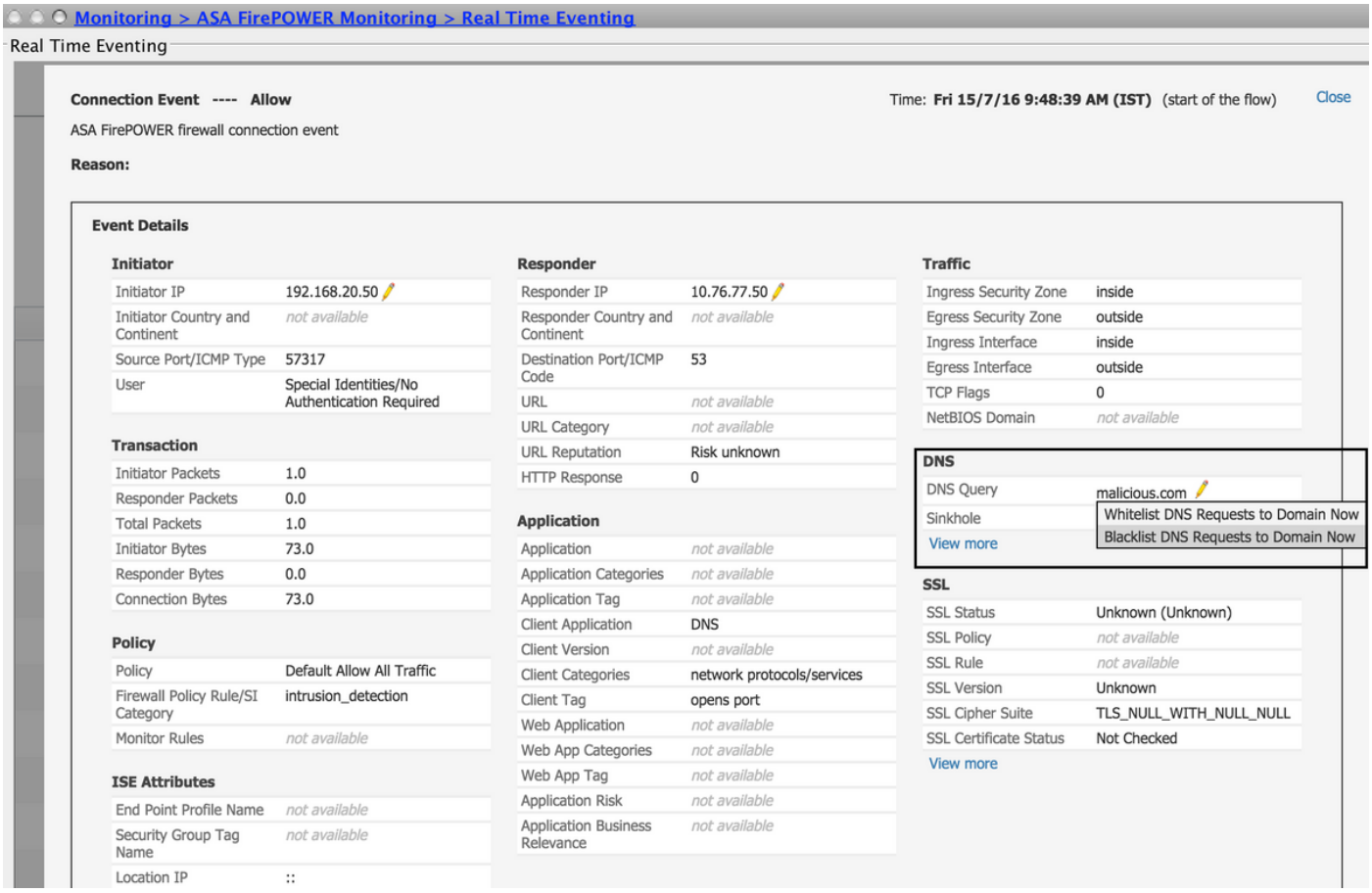
- Lista negra global para DNS
- Lista blanca global para DNS

Agregar manualmente direcciones IP a la lista negra global y a la lista blanca global

El módulo Firepower permite agregar ciertos dominios a la lista global negra cuando se sabe que forman parte de alguna actividad maliciosa. Los dominios también se pueden agregar a la lista blanca global si desea permitir el tráfico a ciertos dominios bloqueados por dominios de lista negra. Si agrega algún dominio a la lista negra global/lista blanca global, se aplicará inmediatamente sin necesidad de aplicar la política.

Para agregar la dirección IP a Global-Blacklist/ Global-Whitelist, navegue hasta **Monitoring > ASA FirePOWER Monitoring > Real Time Eventing**, pase el ratón sobre los eventos de conexión y seleccione **View Details**.

Puede agregar dominios a la lista global-negra/lista blanca global. Haga clic en **Editar** en la sección DNS y seleccione **Solicitudes DNS de lista blanca al dominio ahora/lista negra Solicitudes DNS al dominio ahora** para agregar el dominio a la lista respectiva, como se muestra en la imagen.



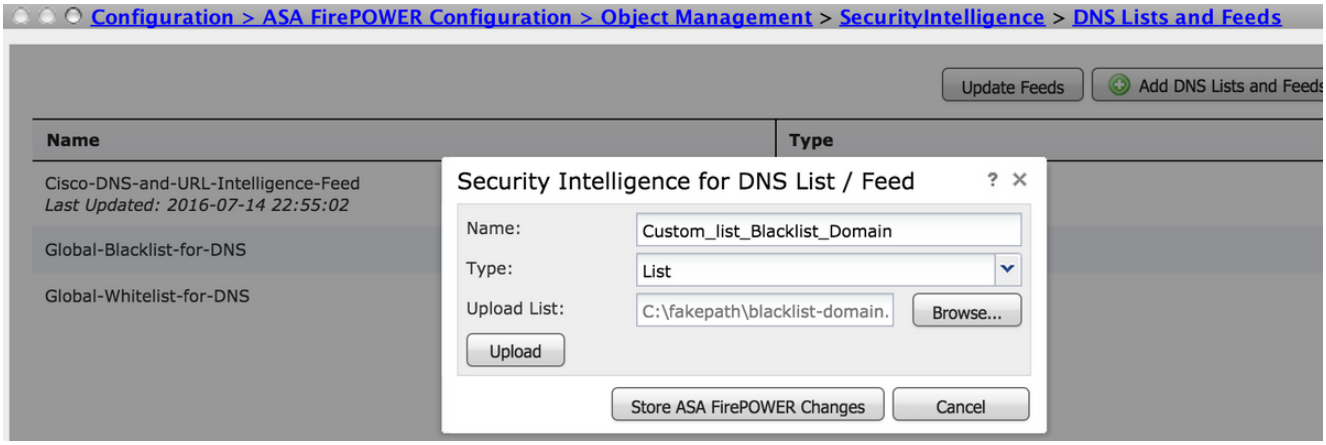
Para verificar que los dominios se agregan a la lista global negra/ lista blanca global, navegue hasta **Configuración > Configuración de ASA FirePOWER > Administración de objetos > Inteligencia de seguridad > Listas y fuentes DNS** y edite **Lista global negra para DNS / Lista blanca global para DNS**. También puede utilizar el botón Eliminar para quitar cualquier dominio de la lista.

Crear la lista personalizada de dominios de lista negra

Firepower permite crear una lista de dominios personalizada que se puede utilizar para incluir en la lista negra (bloquear) mediante dos métodos diferentes.

1. Puede escribir nombres de dominio en un archivo de texto (un dominio por línea) y cargar el archivo en el módulo FirePOWER.

   Para cargar el archivo, navegue hasta **Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > DNS Lists and Feeds** y luego seleccione **Add DNS Lists and Feeds** **Nombre:** Especifique el nombre de la lista Personalizada. **Tipo:** Seleccione **List** en la lista desplegable. **Cargar lista:** Elija **Browse** para localizar el archivo de texto en su sistema. Seleccione **Cargar** para cargar el archivo.



Haga clic en **Store ASA FirePOWER Changes** para guardar los cambios.

2. Puede utilizar cualquier dominio de terceros para la lista personalizada para la que el módulo Firepower pueda conectar el servidor de terceros para obtener la lista de dominios.

   Para configurar esto, navegue hasta **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > DNS Lists and Feeds** y luego seleccione **Add DNS Lists and Feeds**

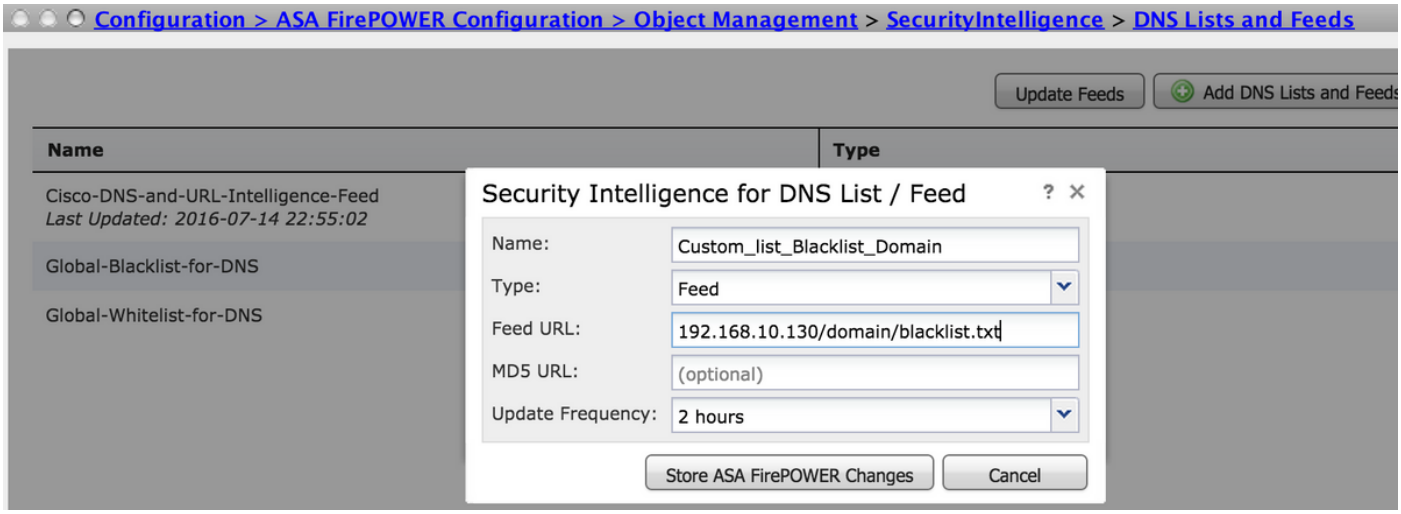
   Nombre: Especifique el nombre de la fuente personalizada.

   Tipo: Seleccione **Fuente** en la lista desplegable.

   URL de la fuente: Especifique la dirección URL del servidor a la que el módulo FirePOWER puede conectarse y descargar la fuente.

   URL MD5: Especifique el valor hash para validar la ruta de la URL de la fuente.

   Actualizar frecuencia: Especifique el intervalo de tiempo en el que el módulo se conecta al servidor de fuente de URL.



Seleccione **Store ASA FirePOWER Changes** para guardar los cambios.

Paso 2. Configurar un objeto Sinkhole (opcional).

La dirección IP de sinkhole se puede utilizar como respuesta a una solicitud DNS maliciosa. El

equipo cliente obtiene la dirección IP del servidor sinkhole para la búsqueda de dominio malintencionado y el equipo final intenta conectarse al servidor sinkhole. Por lo tanto, el sinkhole puede actuar como Honeypot para investigar el tráfico del ataque. El orificio de conexión se puede configurar para activar un indicador de compromiso (IOC).

Para agregar el servidor sinkhole, **Configuration > ASA FirePOWER Configuration > Object Management > Sinkhole** y haga clic en la opción **Add Sinkhole**.

Nombre: Especifique el nombre del servidor sinkhole.

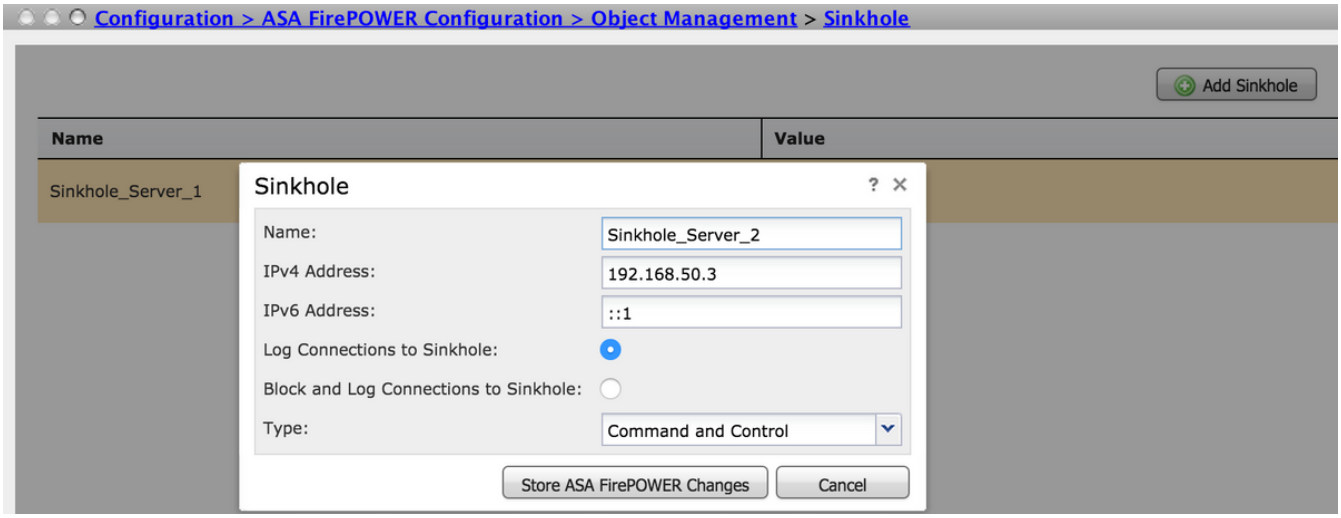
Dirección IP: Especifique la dirección IP del servidor sinkhole.

Conexiones de registro a Sinkhole: Active esta opción para registrar todas las conexiones entre el terminal y el servidor sinkhole.

Bloquear y registrar conexiones a sinkhole: Active esta opción para bloquear la conexión y sólo iniciar sesión al inicio de la conexión de flujo. Si no hay ningún servidor sinkhole físico, puede especificar cualquier dirección IP y ver los eventos de conexión y el disparador IOC.

Tipo: Especifique la fuente de la lista desplegable para la que desea seleccionar el tipo de IOC (Indicación de compromiso) asociado a eventos sinkhole. Hay tres tipos de IOC de agujero único que se pueden etiquetar.

- Malware
- Comando y control
- Phish



Paso 3. Configuración de la política DNS.

La política DNS debe configurarse para decidir la acción de la fuente/lista DNS. Vaya a **Configuration > ASA FirePOWER Configuration > Policies > DNS Policy .**

La política de DNS predeterminada contiene dos reglas predeterminadas. La primera regla, **Lista blanca global para DNS**, contiene la lista personalizada del dominio permitido (**Lista blanca global para DNS**). Esta regla se encuentra en la parte superior para coincidir primero antes de que el

sistema intente coincidir con cualquier dominio de lista negra. La segunda regla, **Lista negra global para DNS**, contiene la lista personalizada del dominio bloqueado (**Lista negra global para DNS**).

Puede agregar más reglas para definir las diversas acciones para las **Listas de Dominios y Fuentes proporcionadas por Cisco TALOS**. Para agregar una nueva regla, seleccione **Agregar regla DNS.**

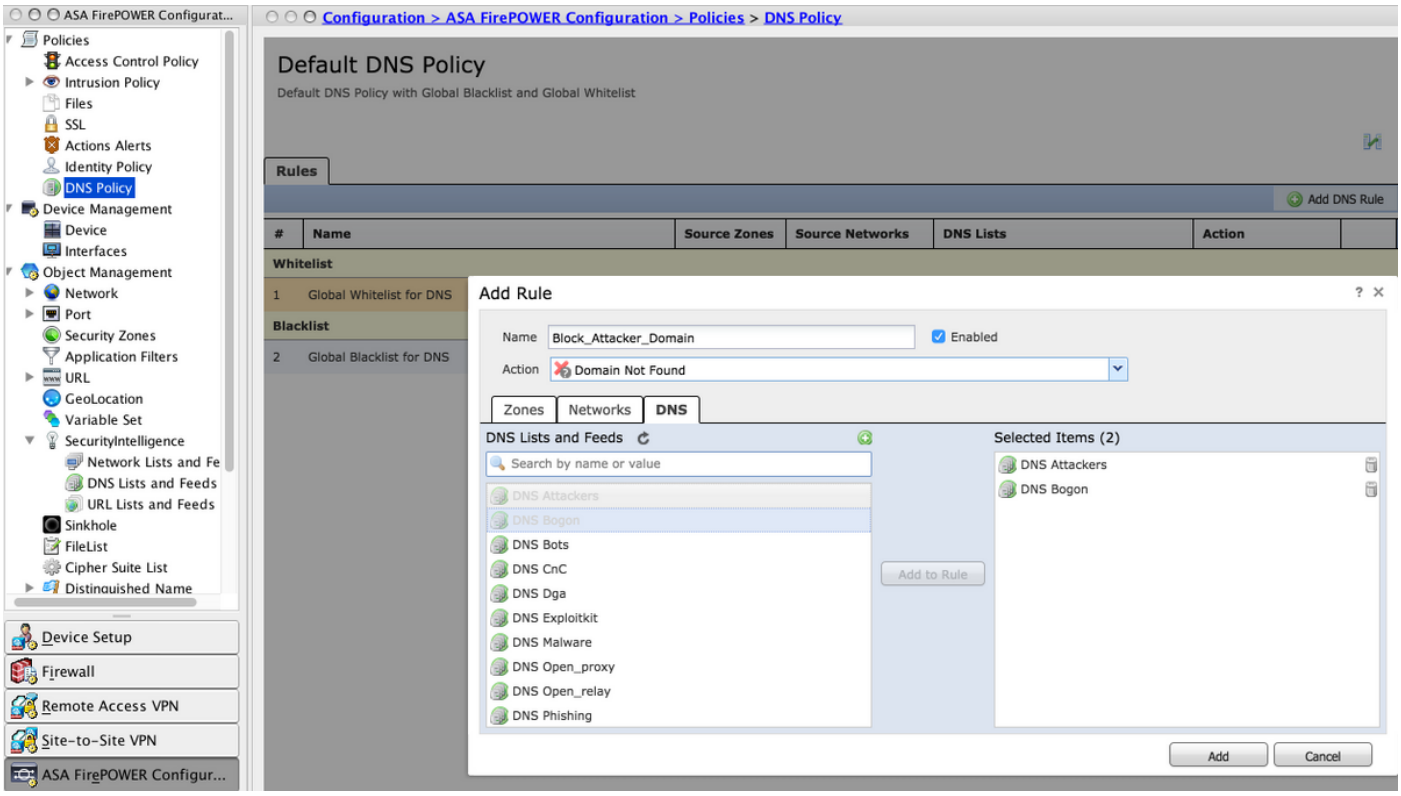
Nombre: Especifique el nombre de la regla.

Acción: Especifique la acción que se activará cuando esta regla coincida.

- **Lista blanca:** Esto permite la consulta DNS.
- **Monitor:** Esta acción genera el evento para la consulta DNS y el tráfico sigue coincidiendo con las reglas subsiguientes.
- **Dominio no encontrado:** Esta acción envía una respuesta DNS como Dominio no encontrado (Dominio inexistente).
- **Abandonar:** Esta acción bloquea y descarta la consulta DNS silenciosamente.
- **Sinkhole:** Esta acción envía la dirección IP del servidor Sinkhole como respuesta a la solicitud DNS.

Especifique las **Zonas/ Red** para definir las condiciones de regla. En la ficha DNS, elija las **listas y fuentes DNS** y vaya a la opción **Elementos seleccionados**, donde puede aplicar la acción configurada.

Puede configurar varias reglas DNS para diferentes listas y fuentes DNS con una acción diferente según las necesidades de su organización.

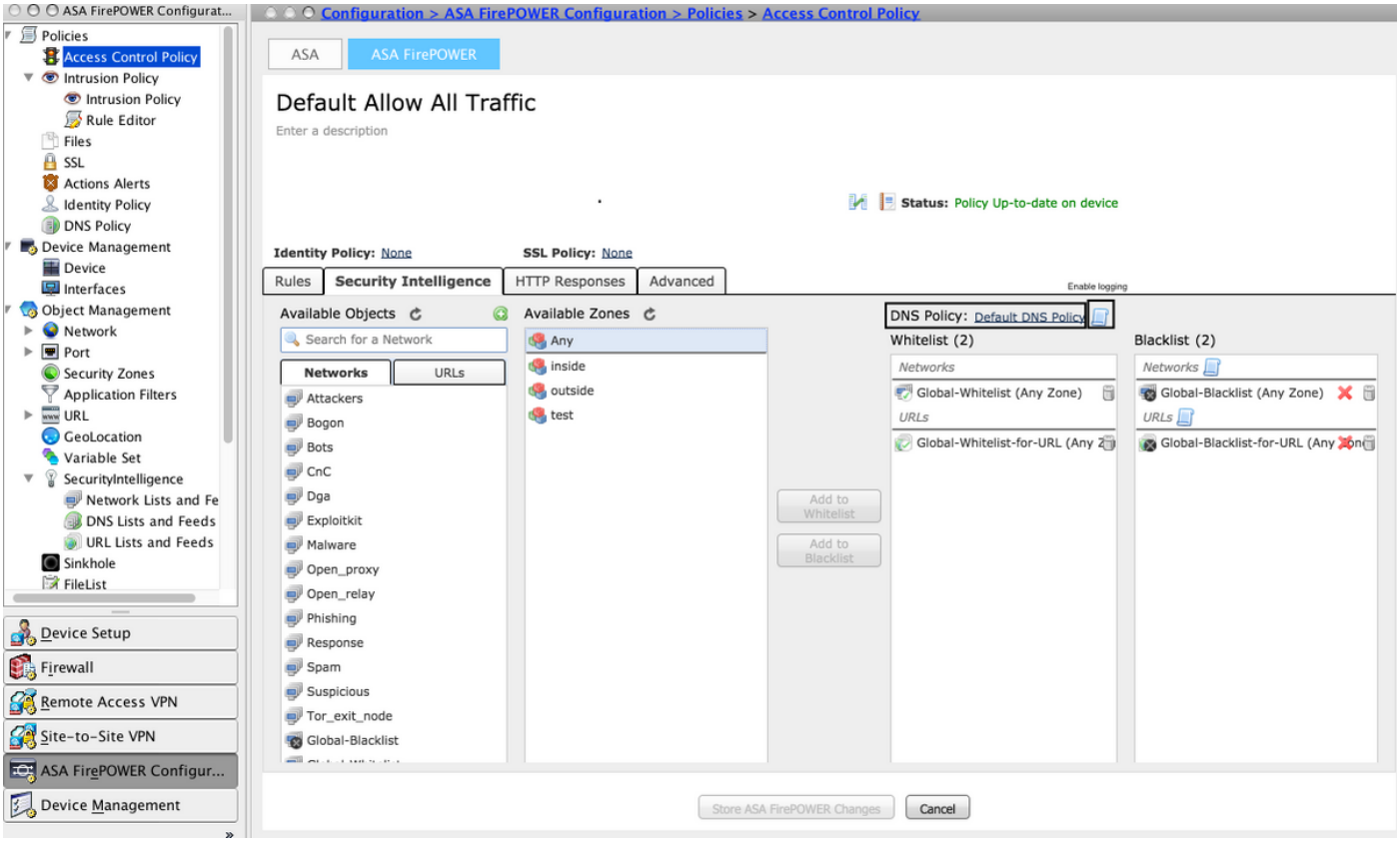


Haga clic en la opción **Add** para agregar la regla.

Paso 4. Configure la política de control de acceso.

Para configurar la inteligencia de seguridad basada en DNS, navegue hasta **Configuration > ASA Firepower Configuration > Policies > Access Control Policy,** seleccione la pestaña **Security Intelligence**.

Asegúrese de que la política DNS esté configurada y opcionalmente, puede habilitar los registros al hacer clic en el icono de registros como se muestra en la imagen.



Elija la opción **Store ASA Firepower Changes** para guardar los cambios de política de CA.

Paso 5. Implemente la política de control de acceso.

Para que los cambios surtan efecto, debe implementar la política de control de acceso. Antes de aplicar la política, vea una indicación de si la política de control de acceso está desactualizada en el dispositivo o no.

Para implementar los cambios en el sensor, haga clic en **Implementar** y elija **Implementar cambios de FirePOWER** luego seleccione **Implementar** en la ventana emergente para implementar los cambios.

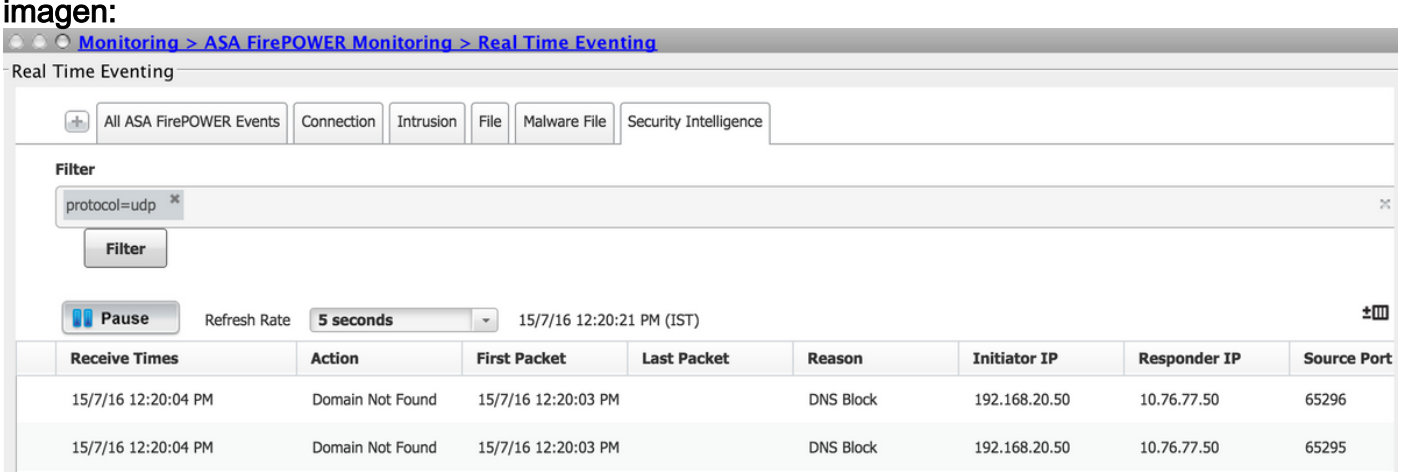
> **Nota:** En la versión 5.4.x, para aplicar la política de acceso al sensor, debe hacer clic en **Aplicar cambios de FirePOWER ASA.**

Nota: Vaya a Monitoring > ASA Firepower Monitoring > Task Status . Asegúrese de que la tarea está completa para confirmar los cambios de configuración. **Verificación** **La configuración sólo se puede verificar si se activa un evento. Para ello, puede forzar una consulta DNS en un equipo. Sin embargo, tenga cuidado con las repercusiones cuando se dirige a un servidor**

malintencionado conocido. Después de generar esta consulta, puede ver el evento en la sección Eventos en tiempo real.

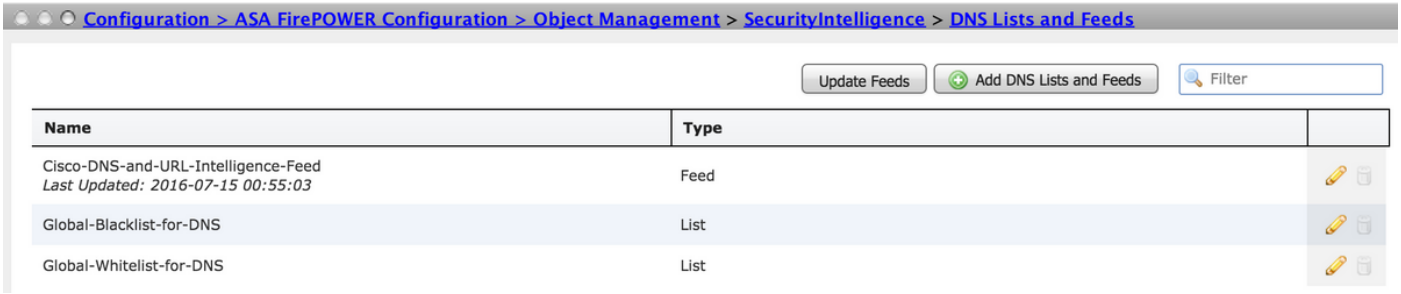
Supervisión de eventos de inteligencia de seguridad DNS

Para ver la Inteligencia de Seguridad por el Módulo Firepower, navegue hasta Monitoring > ASA Firepower Monitoring > Real Time Event. Seleccione la pestaña Security Intelligence. Esto muestra los eventos como se muestra en la imagen:



Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.Para asegurarse de que las fuentes de Security Intelligence estén actualizadas, navegue hasta Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > DNS Lists and Feeds y verifique la hora en que se actualizó la fuente por última vez. Puede elegir Editar para establecer la frecuencia de actualización de la fuente.



Asegúrese de que la implementación de la política de control de acceso se ha completado correctamente. Supervise la ficha Security Intelligence Real Time Eventing para ver si el tráfico está bloqueado o no.

Información Relacionada

- Guía de inicio rápido del módulo Cisco ASA FirePOWER
- Soporte Técnico y Documentación - Cisco Systems