La inteligencia de seguridad de un sistema Cisco FireSIGHT bloquea o lista negra la dirección IP

Contenido

Introducción

La función Security Intelligence permite especificar el tráfico que puede atravesar la red en función de la dirección IP de origen o de destino. Esto es especialmente útil si desea incluir en la lista negra - denegar el tráfico hacia y desde - direcciones IP específicas, antes de que el tráfico sea sometido a análisis por reglas de control de acceso. En este documento se describe cómo controlar situaciones en las que un sistema Cisco FireSIGHT bloquea o pone en la lista negra una dirección IP.

Prerequisites

Requirements

Cisco recomienda que conozca Cisco FireSIGHT Management Center.

Componentes Utilizados

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

- Cisco FireSIGHT Management Center
- Dispositivo Cisco Firepower
- Módulo Cisco ASA con Firepower (SFR)
- Software versión 5.2 o 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.

Diferencia entre la fuente de inteligencia y la lista de inteligencia

Existen dos formas de utilizar la función de inteligencia de seguridad en un sistema FireSIGHT:

Fuente de inteligencia de seguridad

Una fuente Security Intelligence es una colección dinámica de direcciones IP que el Centro de defensa descarga desde un servidor HTTP o HTTPS. Para ayudarle a crear listas negras, Cisco proporciona la *fuente Security Intelligence*, que representa las direcciones IP determinadas por el Equipo de investigación de vulnerabilidades (VRT) para tener una reputación deficiente.

Lista de inteligencia de seguridad

Una lista de Security Intelligence, en contraste con una fuente, es una simple lista estática de direcciones IP que se cargan manualmente en FireSIGHT Management Center.

La dirección IP legítima está bloqueada o en la lista negra

Verifique si una dirección IP está en la fuente Security Intelligence

Si una dirección IP está siendo bloqueada por la lista negra de fuentes de inteligencia de seguridad, puede seguir los pasos que se indican a continuación para verificar esto:

Paso 1: Acceda a la CLI del dispositivo Firepower o del módulo de servicio.

Paso 2: Ejecute el siguiente comando. Reemplace <IP_Address> por la dirección IP que desea buscar:

```
admin@Firepower:~$ grep
```

Por ejemplo, si desea buscar la dirección IP 198.51.100.1, ejecute el siguiente comando:

```
admin@Firepower:~$ grep 198.51.100.1 /var/sf/iprep_download/*.blf
```

Si este comando devuelve cualquier coincidencia para la dirección IP proporcionada, indica que la dirección IP está presente en la lista negra de la fuente de inteligencia de seguridad.

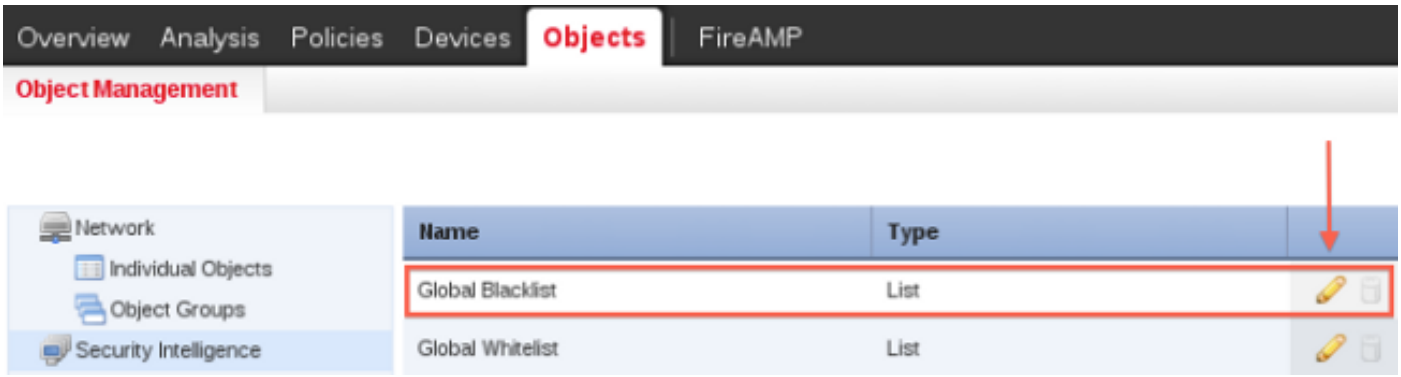
Comprobar la lista negra

Para encontrar una lista de las direcciones IP que se pueden incluir en la lista negra, siga estos pasos:

Paso 1: Acceso a la interfaz web del FireSIGHT Management Center.

Paso 2: Vaya a **Objetos > Administración de objetos > Inteligencia de seguridad**.

Paso 3: Haga clic en el icono *del lápiz* para abrir o editar la **lista negra global**. Aparece una ventana emergente con una lista de direcciones IP.



Trabajar con una dirección IP bloqueada o en lista negra

Si la fuente de inteligencia de seguridad bloquea o lista negra una dirección IP determinada, puede considerar cualquiera de las siguientes opciones para permitirla.

Opción 1: Lista blanca de inteligencia de seguridad

La inteligencia de seguridad puede incluir una dirección IP en la lista negra. Una lista blanca anula su lista negra. El sistema FireSIGHT evalúa el tráfico con una dirección IP de origen o de destino con lista blanca utilizando reglas de control de acceso, incluso si una dirección IP también se encuentra en la lista negra. Por lo tanto, puede utilizar una lista blanca cuando una lista negra sigue siendo útil, pero tiene un alcance demasiado amplio y bloquea incorrectamente el tráfico que desea inspeccionar.

Por ejemplo, si una fuente de confianza bloquea incorrectamente el acceso a un recurso vital pero, en general, es útil para su organización, puede enumerar las direcciones IP clasificadas incorrectamente únicamente, en lugar de eliminar toda la fuente de la lista negra.

> **Precaución:** Después de realizar cualquier cambio en una política de control de acceso, debe volver a aplicar la política a los dispositivos administrados.

Opción 2: Aplicar el filtro de inteligencia de seguridad por zona de seguridad

Para obtener mayor granularidad, puede aplicar el filtrado de la inteligencia de seguridad en función de si la dirección IP de origen o de destino de una conexión reside en una zona de seguridad determinada.

Para extender el ejemplo de la lista blanca anterior, puede enumerar las direcciones IP clasificadas incorrectamente, pero después restringir el objeto de la lista blanca utilizando una

zona de seguridad utilizada por aquellos de su organización que necesitan acceder a esas direcciones IP. De esta manera, solo aquellos que necesiten una empresa pueden acceder a las direcciones IP de la lista blanca. Como otro ejemplo, es posible que desee utilizar una fuente de spam de terceros para incluir en la lista negra el tráfico en una zona de seguridad de servidor de correo electrónico.

Opción 3: Supervisar, en lugar de lista negra

Si no está seguro de si desea incluir en la lista negra una dirección IP determinada o un conjunto de direcciones, puede utilizar una configuración de "solo monitor", que permite al sistema pasar la conexión coincidente a las reglas de control de acceso, pero también registra la coincidencia en la lista negra. Tenga en cuenta que no se puede establecer la lista negra global en solo supervisión

Considere un escenario en el que desee probar una fuente de terceros antes de implementar el bloqueo mediante dicha fuente. Cuando se configura la fuente para que sólo la supervise, el sistema permite que el sistema analice las conexiones que se habrían bloqueado en mayor medida, pero también registra un registro de cada una de esas conexiones para su evaluación.

Pasos para configurar la inteligencia de seguridad con el parámetro "solo monitor":

1. En la ficha **Security Intelligence** de una política de control de acceso, haga clic en el icono de registro. Aparecerá el cuadro de diálogo Opciones de lista negra.
2. Active la casilla de verificación **Conexiones de registro** para registrar los eventos de inicio de conexión cuando el tráfico cumple las condiciones de Seguridad Inteligente.
3. Especifique dónde enviar los eventos de conexión.
4. Haga clic en **Aceptar** para establecer las opciones de registro. La ficha Security Intelligence aparece de nuevo.
5. Click **Save**. Debe aplicar la política de control de acceso para que los cambios surtan efecto.

Opción 4: Póngase en contacto con el centro de asistencia técnica de Cisco

Siempre puede ponerse en contacto con el Centro de asistencia técnica de Cisco si:

- Tiene preguntas con las opciones 1, 2 o 3 anteriores.
- Desea realizar más investigaciones y análisis sobre una dirección IP que aparece en la lista negra de la inteligencia de seguridad.
- La inteligencia de seguridad desea obtener una explicación de por qué la dirección IP está en la lista negra.