La dirección IP es bloqueada o puesta por la inteligencia de Seguridad de un sistema de Cisco FireSIGHT

ID del Documento: 117993

Actualizado: De oct el 21 de 2015

Contribuido por Nazmul Rajib, ingeniero de Cisco TAC.

Descarga PDF
Imprimir
Feedback

Productos Relacionados

- Centro de administración 750 de Cisco FireSIGHT
- Centro de administración 3500 de Cisco FireSIGHT
- Centro de administración 1500 de Cisco FireSIGHT
- Centro de administración de Cisco FireSIGHT

Contenido

Introducción

La característica de la inteligencia de Seguridad permite que usted especifique el tráfico que puede atravesar su red basada en la fuente o el IP Address de destino. Esto es especialmente útil si usted quiere poner - niegue el tráfico a y desde - los IP Addresses específicos, antes de que el tráfico sea sujetado al análisis por las reglas del control de acceso. Esto documenta describe cómo manejar los escenarios cuando una dirección IP está siendo bloqueada o puesta por un sistema de Cisco FireSIGHT.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento en el centro de administración de Cisco FireSIGHT.

Componentes Utilizados

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

- Centro de administración de Cisco FireSIGHT
- Dispositivo de Cisco FirePOWER
- Cisco ASA con el módulo de FirePOWER (SFR)
- Versión de software 5.2 o más adelante

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.

Diferencia entre la alimentación de la inteligencia y la lista de la inteligencia

Hay dos maneras de utilizar la característica de la inteligencia de Seguridad en un sistema de FireSIGHT:

Alimentación de la inteligencia de Seguridad

Una alimentación de la inteligencia de Seguridad es una colección dinámica de IP Addresses que el centro de la defensa descarga de un HTTP o de un servidor HTTPS. Para ayudarle a construir las listas negras, Cisco proporciona la *alimentación de la inteligencia de Seguridad*, que representa los IP Addresses determinados por el equipo de investigación de la vulnerabilidad (VRT) para tener una reputación pobre.

Lista de la inteligencia de Seguridad

Una lista de la inteligencia de Seguridad, puesta en contraste con una alimentación, es una lista estática simple de IP Addresses que usted manualmente carga a FireSIGHT el centro de administración.

Se bloquea o se pone el IP Address legítimo

Verifique si una dirección IP está en la alimentación de la inteligencia de Seguridad

Si una dirección IP está siendo bloqueada por la lista negra de la alimentación de la inteligencia de Seguridad, usted puede seguir los pasos abajo para verificar esto:

Paso 1: Acceda el CLI del dispositivo o del módulo de servicio de FirePOWER.

Paso 2: Funcione con el siguiente comando. Substituya `<ip_address>` por la dirección IP para la cual usted quiere buscar:

```
admin@Firepower:~$ grep <IP_Address> /var/sf/iprep_download/*.blf
```

Por ejemplo, si usted quiere buscar para la dirección IP 198.51.100.1, funcione con el siguiente comando:

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

Si este comando vuelve cualquier coincidencia para la dirección IP que usted proporcionó, indica que la dirección IP está presente en la lista negra de la alimentación de la inteligencia de Seguridad.

Marque la lista negra

Para encontrar una lista de los IP Addresses que pudieron ser puestos, siga los pasos abajo:

Paso 1: Acceso a la interfaz Web del centro de administración de FireSIGHT.

Paso 2: Navegue a los **objetos > a la inteligencia del > Security (Seguridad) de la Administración del objeto**.

Paso 3: Haga clic en el icono del *lápiz* para abrir o para editar la **lista negra global**. Un hacer estallar encima de la ventana con una lista de IP Addresses aparece.

Trabajo con una dirección IP bloqueada o puesta

Si la alimentación de la inteligencia de Seguridad bloquea o es puesto a un IP Address particular, usted puede considerar las opciones de siguiente unas de los para permitirla.

Opción 1: Listas blancas de la inteligencia de Seguridad

Usted puede lista blanca una dirección IP que sea puesta por la inteligencia de Seguridad. Una lista blanca reemplaza su lista negra. El sistema de FireSIGHT evalúa el tráfico con una fuente o un IP Address de destino whitelisted usando las reglas del control de acceso, incluso si una dirección IP también se pone. Por lo tanto, usted puede utilizar una lista blanca cuando una lista negra es todavía útil, pero es demasiado amplio en el alcance y bloquea incorrectamente el tráfico que usted quiere examinar.

Por ejemplo, si una alimentación reputable bloquea incorrectamente su acceso a un recurso vital pero es en conjunto útil a su organización, usted puede lista blanca los IP Addresses incorrectamente clasificados solamente, bastante que quitando la alimentación del conjunto de la lista negra.

> **Caution**: Después de que usted realice cualquier cambio en una directiva del control de acceso, usted debe reaplicar la directiva a los dispositivos administrados.

Opción 2: Aplique el filtro de la inteligencia de Seguridad por la zona de Seguridad

Para el granularity agregado, usted puede aplicar la filtración de la inteligencia de Seguridad basada encendido si la fuente o el IP Address de destino en una conexión reside en una zona de Seguridad determinada.

Para ampliar el ejemplo anterior de la lista blanca, usted podría lista blanca los IP Addresses incorrectamente clasificados, pero por otra parte restringir el objeto de la lista blanca usando una zona de Seguridad usada por las en su organización que necesitan acceder esos IP Addresses. Esa manera, solamente ésos con una necesidad comercial puede acceder los IP Addresses whitelisted. Como otro ejemplo, usted puede ser que quiera utilizar una alimentación de tercera persona del Spam para poner el tráfico en una zona de Seguridad del servidor de correo electrónico.

Opción 3: Monitor, bastante que la lista negra

Si usted no está seguro si usted quiere poner un IP Address particular o un conjunto de los direccionamientos, usted puede utilizar una configuración del “monitor-solamente”, que permite que el sistema pase la conexión que corresponde con a las reglas del control de acceso, pero también registra la coincidencia a la lista negra. Observe que usted no puede fijar el monitor-solamente de la lista negra global

Considere un escenario donde usted quiere probar una alimentación de tercera persona antes de que usted implemente el bloqueo usando esa alimentación. Cuando usted fija el monitor-solamente de la alimentación, el sistema permite las conexiones que habrían sido bloqueadas para ser analizadas más a fondo por el sistema, pero también registra un expediente de cada uno de esas conexiones para su evaluación.

Pasos para configurar la inteligencia de Seguridad con la configuración del “monitor-solamente”:

1. En la lengueta de la **inteligencia de Seguridad** en una directiva del control de acceso, haga

clic el icono del registro. El cuadro del diálogo de opciones de la lista negra aparece.
2. Seleccione la casilla de verificación de las **conexiones del registro** para registrar los eventos de la principio-de-conexión cuando el tráfico cumple las condiciones de la inteligencia de Seguridad.
3. Especifique donde enviar los eventos de conexión.
4. Haga Click en OK para fijar sus opciones de registro. La lengueta de la inteligencia de Seguridad aparece otra vez.
5. Click **Save**. Usted debe aplicar la directiva del control de acceso para que sus cambios tomen el efecto.

Opción 4: Centro de Asistencia Técnica de Cisco del contacto

Usted puede entrar en contacto siempre el Centro de Asistencia Técnica de Cisco, si:

- Usted tiene preguntas con las opciones antedichas 1, 2 o 3.
- Usted quiere la investigación y el análisis adicionales en una dirección IP que sea puesta por la inteligencia de Seguridad.
- Usted quiere una explicación porqué la dirección IP es puesta por la inteligencia de Seguridad.

Discusiones relacionadas de la comunidad del soporte de Cisco

La comunidad del soporte de Cisco es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Refiera a los convenios de los consejos técnicos de Cisco para la información sobre los convenios usados en este documento.

Actualizado: De oct el 21 de 2015
ID del Documento: 117993