

Configuración de listas negras de IP mientras se utiliza Cisco Security Intelligence a través de ASDM (administración integrada)

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Descripción general de la fuente Security Intelligence](#)

[Agregar manualmente direcciones IP a la lista negra global y a la lista blanca global](#)

[Crear la lista personalizada de direcciones IP de lista negra](#)

[Configuración de la inteligencia de seguridad](#)

[Implementación de la política de control de acceso](#)

[Supervisión de eventos de la inteligencia de seguridad](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe la reputación de la dirección IP/de Cisco Security Intelligence y la configuración de la lista negra de IP (bloqueo) mientras se utiliza una fuente personalizada/automática de direcciones IP de baja reputación.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento del firewall ASA (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager)
- Conocimiento del dispositivo FirePOWER

Nota: El filtrado de Security Intelligence requiere una licencia de protección.

Componentes Utilizados

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

- Módulos ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) que ejecutan la versión de software 5.4.1 y superiores
- Módulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) que ejecuta 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

La inteligencia de seguridad de Cisco consta de varias colecciones de direcciones IP que se actualizan periódicamente y que el equipo de Cisco TALOS ha determinado que tienen una reputación deficiente. El equipo de Cisco TALOS determina la baja reputación si cualquier actividad maliciosa se origina a partir de esas direcciones IP como spam, malware, ataques de phishing, etc.

La fuente Cisco IP Security Intelligence realiza un seguimiento de la base de datos de atacantes, Bogon, bots, CnC, Dga, ExploitKit, malware, Open_proxy, Open_relay, phishing, Response, Spam, sospechoso. El módulo Firepower proporciona la opción de crear la fuente personalizada de una dirección IP de baja reputación.

Descripción general de la fuente Security Intelligence

A continuación se proporciona más información sobre el tipo de colecciones de direcciones IP que se pueden clasificar como categorías diferentes en la inteligencia de seguridad.

Atacantes: Recopilación de direcciones IP que buscan constantemente vulnerabilidades o intentan explotar otros sistemas.

Malware: Recopilación de direcciones IP que intentan propagar malware o atacan activamente a cualquier persona que las visite.

Suplantación de identidad: Recopilación de hosts que intentan engañar activamente a los usuarios finales para que introduzcan información confidencial, como nombres de usuario y contraseñas.

Spam: Colección de hosts que se han identificado como el origen del envío de mensajes de correo electrónico de spam.

Bots: Colección de hosts que participan activamente como parte de un botnet y que están siendo controlados por un controlador de red bot conocido.

CnC: Colección de hosts que se han identificado como los servidores de control de una Botnet conocida.

OpenProxy: Colección de hosts conocidos por ejecutar Open Web Proxies y ofrecer servicios de exploración web anónimos.

OpenRelay: Colección de hosts que ofrecen servicios de retransmisión de correo electrónico

anónimos utilizados por atacantes de spam y phishing.

TorExitNode: Colección de hosts que se sabe que ofrecen servicios de nodo de salida para la red Tor Anonymizer.

Bogon: Colección de direcciones IP que no están asignadas pero que están enviando tráfico.

Sospechoso: Recopilación de direcciones IP que muestran actividad sospechosa y están bajo investigación activa.

Respuesta: Colección de direcciones IP que se han observado repetidamente implicadas en comportamientos sospechosos o maliciosos.

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

El módulo Firepower permite agregar ciertas direcciones IP a la lista global negra cuando se sabe que forman parte de alguna actividad maliciosa. Las direcciones IP también se pueden agregar a la lista blanca global, si desea permitir el tráfico a ciertas direcciones IP que están bloqueadas por direcciones IP de lista negra. Si agrega alguna dirección IP a Global-Blacklist/Global-Whitelist, 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 la dirección IP de origen o de destino a la lista global negra/ lista blanca global. Haga clic en el botón **Edit** y seleccione **Lista blanca ahora/lista negra ahora** para agregar la dirección IP a la lista correspondiente, como se muestra en la imagen.

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

+ All ASA FirePOWER Events Connection Intrusion File Malware File Security Intelligence

Filter
Rule Action=Allow *

Pause Refresh Rate 5 seconds 1/25/16 9:11:25 AM (IST)

Receive Times	Action	First Packet	Last Packet	Reason
1/25/16 9:09:50 AM	Allow	1/25/16 9:09:48 AM	1/25/16 9:09:49 AM	
1/25/16 9:07:36 AM	Allow	1/25/16 9:07:03 AM	1/25/16 9:07:03 AM	
1/25/16 9:07:07 AM	Allow	1/25/16 9:07:06 AM	1/25/16 9:07:06 AM	

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

Initiator	Responder	Edit
Initiator IP 192.168.20.3	Responder IP 10.106.44.55	
Initiator Country and Continent not available	Responder Country and Continent not available	
Source Port/ICMP Type 60297	Destination Port/ICMP 49153	

Para verificar que la dirección IP de origen o destino se agrega a la lista Global-Blacklist/ Global-Whitelist, navegue hasta **Configuración > Configuración de ASA Firepower > Administración de objetos > Inteligencia de seguridad > Listas y fuentes de red** y edite **Lista Global-Blacklist/ Lista blanca global**. También puede utilizar el botón **Eliminar** para quitar cualquier dirección IP de la lista.

Crear la lista personalizada de direcciones IP de lista negra

Firepower permite crear una lista de direcciones IP/de red personalizada que se puede utilizar en la lista negra (bloqueo). Hay tres opciones para hacerlo:

1. Puede escribir las direcciones IP en un archivo de texto (una dirección IP por línea) y cargar el archivo en Firepower Module. Para cargar el archivo, navegue hasta **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds** y luego haga clic en **Add Network 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 la opción **Cargar** para cargar el archivo.
2. Puede utilizar cualquier base de datos IP de terceros para la lista personalizada para la que el módulo Firepower se pone en contacto con el servidor de terceros para obtener la lista de direcciones IP. Para configurar esto, navegue hasta **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds** y

luego haga clic en **Add Network Lists and Feeds**

Nombre: Especifique el nombre de la fuente personalizada.

Tipo: Seleccione la opción **Fuente** de la lista desplegable.

URL de la fuente: Especifique la dirección URL del servidor al que debe conectarse el módulo Firepower 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 sistema se conecta al servidor de fuentes URL.

The image displays two screenshots of the ASA FirePOWER configuration interface, specifically the 'Security Intelligence for Network List / Feed' dialog box. The breadcrumb navigation at the top of both screenshots is: Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > Network Lists and Feeds.

Top Screenshot: Shows the 'Add Network Lists and Feeds' dialog box with the following configuration:

- Name: Custom_Feed
- Type: List
- Upload List: C:\fakepath\Custom_IP_Feed. (with a 'Browse...' button)
- Buttons: Upload, Store ASA FirePOWER Changes, Cancel

Bottom Screenshot: Shows the 'Add Network Lists and Feeds' dialog box with the following configuration:

- Name: Custom_Network_Feed
- Type: Feed
- Feed URL: http://192.168.30.1/blacklist-IP.txt
- MD5 URL: (optional)
- Update Frequency: 30 minutes
- Buttons: Store ASA FirePOWER Changes, Cancel

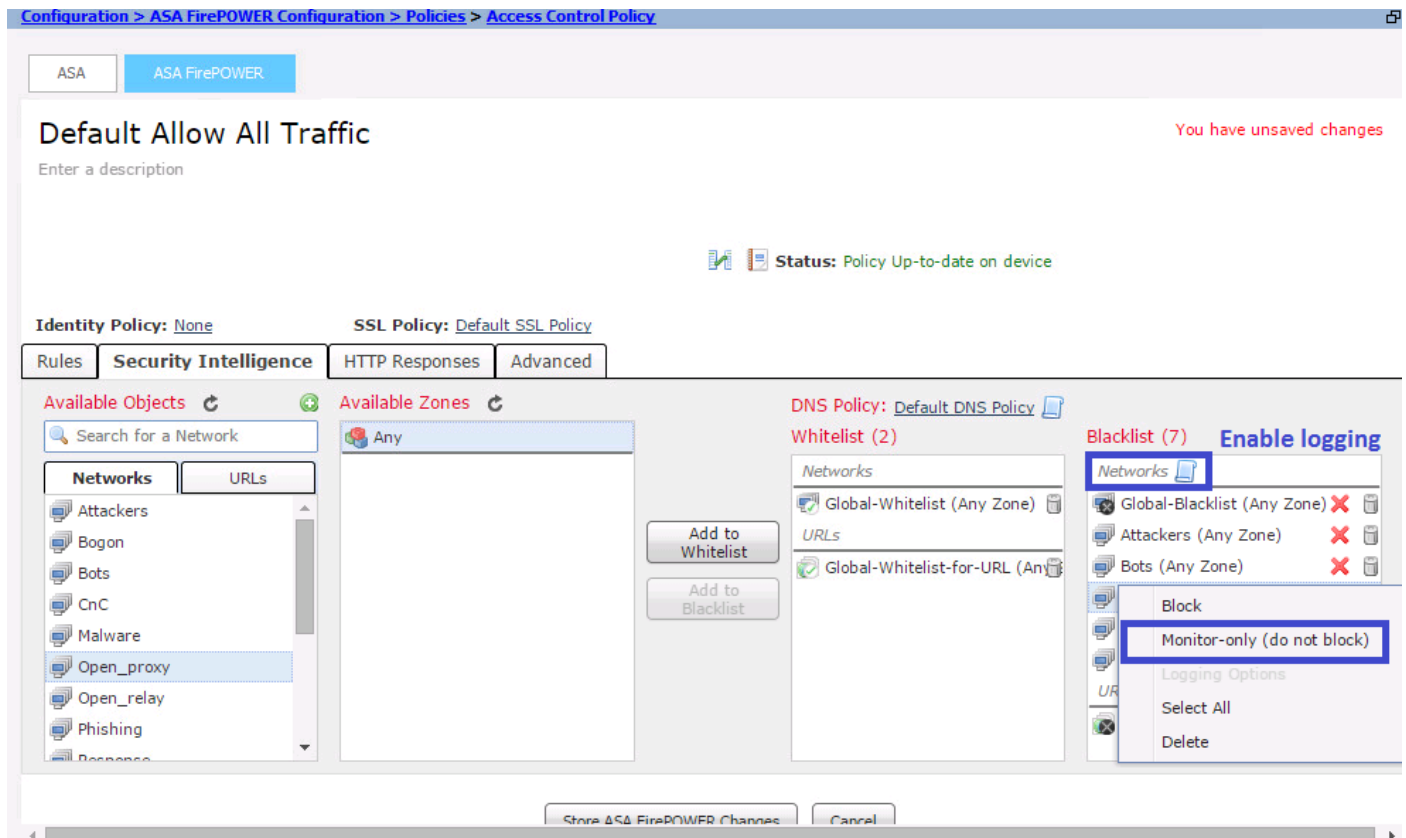
Configuración de la inteligencia de seguridad

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

Elija la fuente del objeto de red disponible, pase a la columna **Lista blanca/ Lista negra** para permitir/bloquear la conexión a la dirección IP malintencionada.

Puede hacer clic en el icono y activar el registro como se especifica en la imagen.

Si sólo desea generar el evento para conexiones IP malintencionadas en lugar de bloquear la conexión, haga clic con el botón derecho en la fuente, elija **Sólo monitor (no bloquear)**, como se muestra en la imagen:

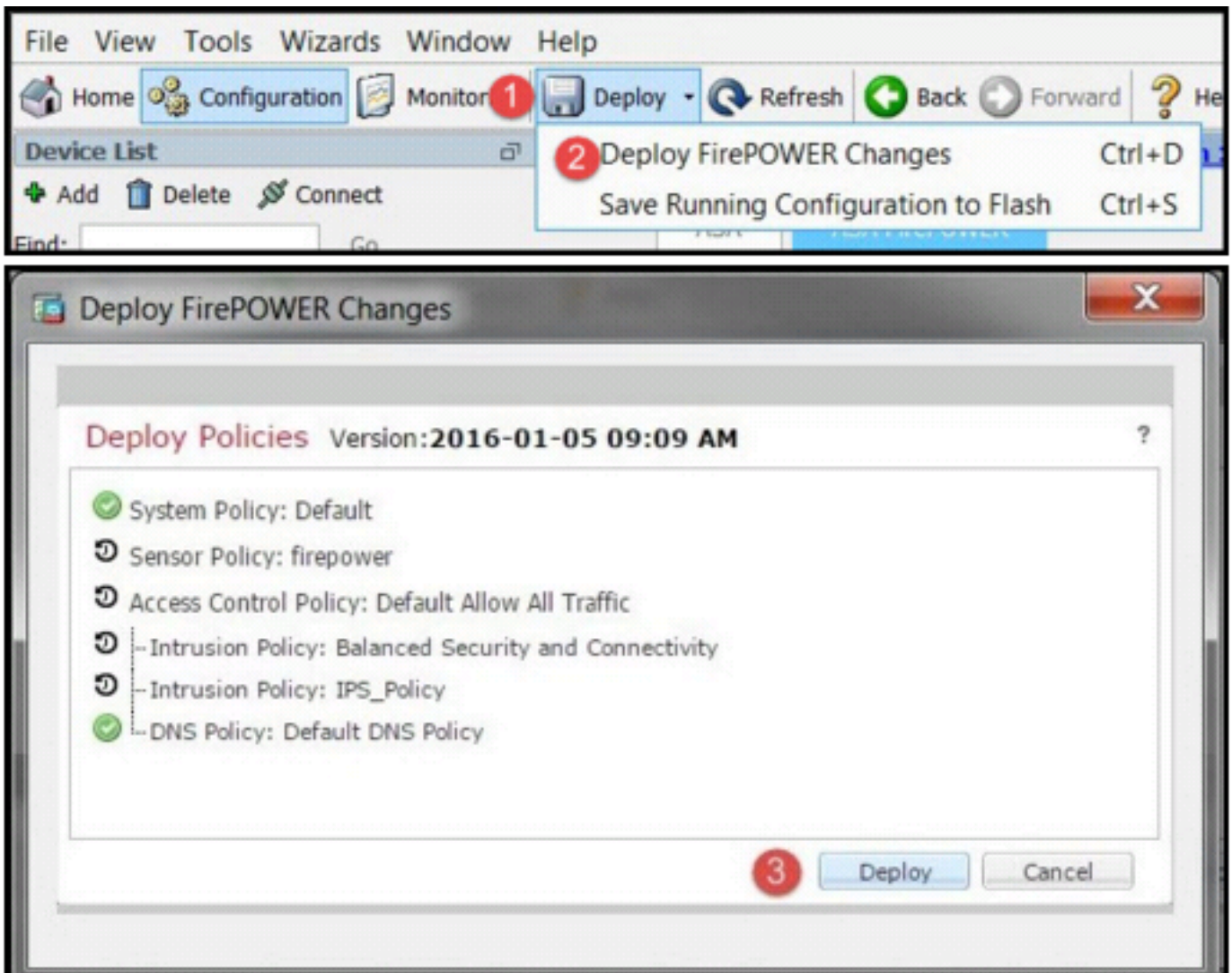


Elija la opción Store ASA Firepower Changes para guardar los cambios de la política de CA.

Implementación de 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 debe completarse para aplicar los cambios de configuración.

Supervisión de eventos de la inteligencia de seguridad

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 mostrará los eventos como se muestra en la imagen:

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

All ASA FirePOWER Events Connection Intrusion File Malware File Security Intelligence

Filter

Enter filter criteria

Pause Refresh Rate 5 seconds 2/9/16 1:03:31 PM (IST)

Receive Times	Action	First Packet	Last Packet	Reason	Initiator IP	Responder IP
2/9/16 1:01:48 PM	Block	2/9/16 1:01:47 PM		IP Block	192.168.20.3	184.26.162.43

Verificación









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

Troubleshoot

Para asegurarse de que las fuentes de Security Intelligence estén actualizadas, navegue hasta **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds** y verifique la hora en que se actualizó la fuente por última vez. Puede elegir el botón Editar para establecer la frecuencia de actualización de la fuente.

Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > Network Lists and Feeds

Update Feeds Add Network Lists and Feeds Filter

Name	Type	
Cisco-Intelligence-Feed Last Updated: 2016-02-08 10:03:14	Feed	 
Custom_Feed	Feed	 
Global-Blacklist	List	 
Global-Whitelist	List	 

Asegúrese de que la implementación de la política de control de acceso se ha completado correctamente.

Supervise la inteligencia de seguridad para ver si el tráfico está bloqueando o no.

Información Relacionada

- [Guía de inicio rápido del módulo Cisco ASA FirePOWER](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)