Configuración de Umbrella con el Blade de Software Anti-Bot de Check Point

Contenido

Introducción

Este documento describe cómo integrar Cisco Umbrella con el blade de software Check Point Anti-Bot.

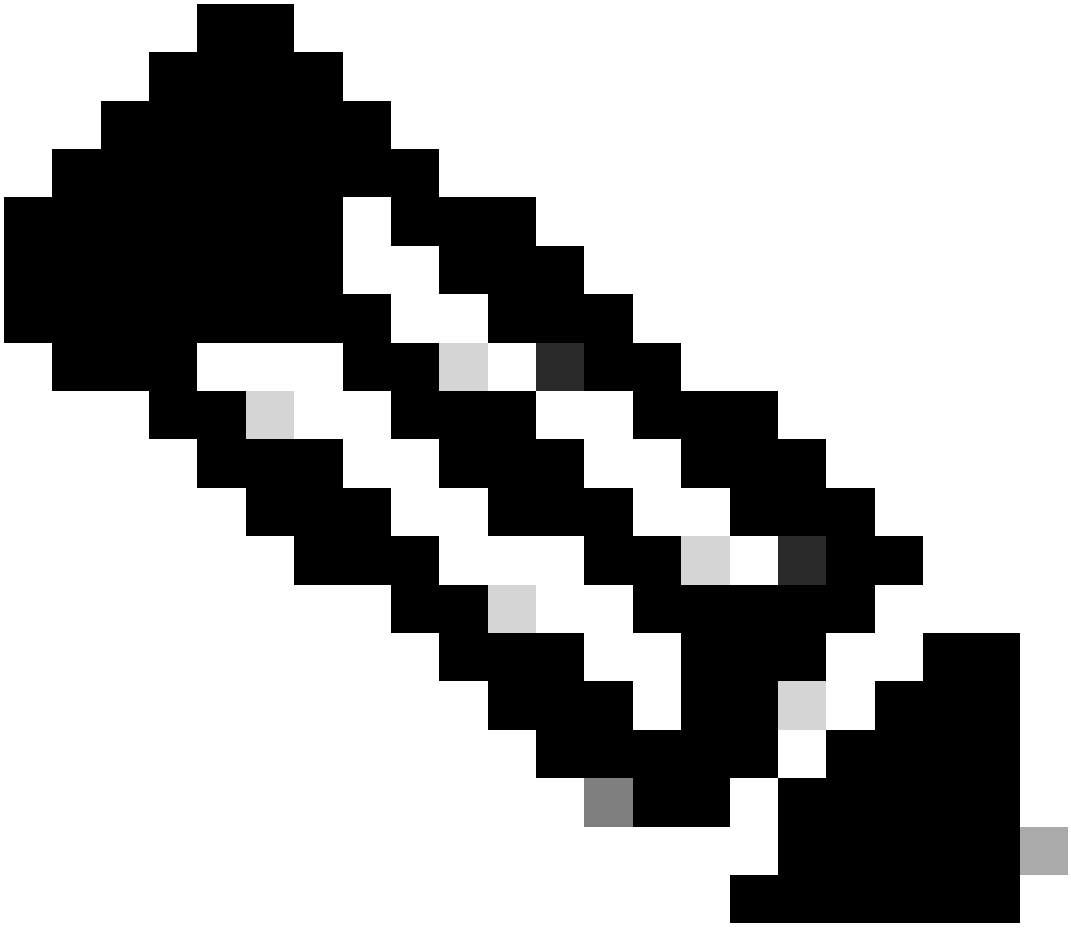
Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Un dispositivo Check Point con el blade de software antiarranque

- Software Check Point versión R80.40 o superior
- Asegúrese de que el dispositivo Check Point puede realizar solicitudes HTTP salientes a "https://s-platform.api.opendns.com".
- Un paquete de Cisco Umbrella como DNS Essentials, DNS Advantage, SIG Essentials o SIG Advantage
- Derechos administrativos de Cisco Umbrella Dashboard



Nota: La integración de Check Point solo se incluye en los paquetes de Cisco Umbrella como DNS Essentials, DNS Advantage, SIG Essentials o SIG Advantage. Si no dispone de uno de estos paquetes y desea disfrutar de la integración de Check Point, póngase en contacto con su Cisco Umbrella Account Manager. Si tiene el paquete Cisco Umbrella correcto pero no ve Check Point como una integración para su panel, póngase en contacto con el servicio de asistencia de Cisco Umbrella.

Componentes Utilizados

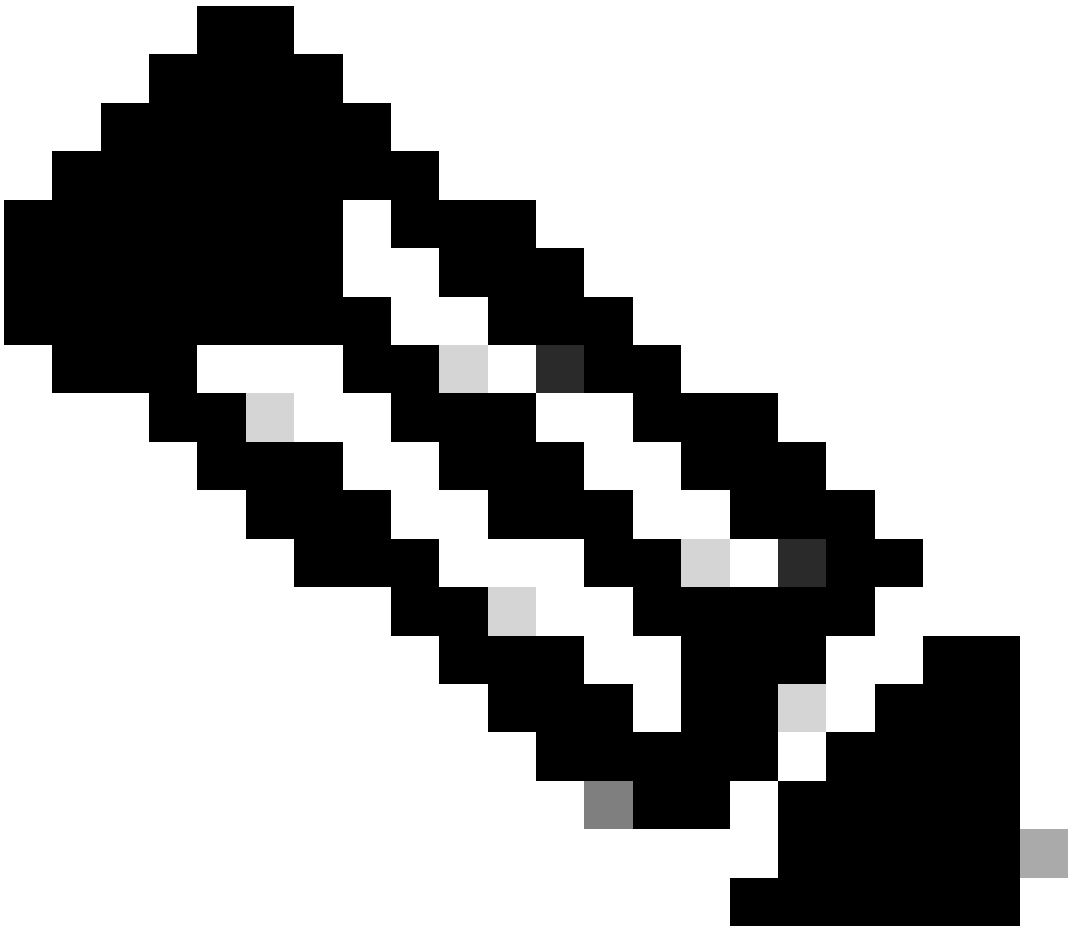
La información de este documento se basa en Cisco Umbrella.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

La integración de Cisco Umbrella con el blade de software antiarranque Check Point permite a un dispositivo Check Point enviar sus alertas del blade de software antiarranque a Cisco Umbrella cuando el blade detecta amenazas en el tráfico de red que inspecciona. Las alertas recibidas por Cisco Umbrella crean una lista de bloqueo que puede proteger los portátiles, tablets y teléfonos en itinerancia en redes no protegidas por el blade de software antiarranque de Check Point.

En este artículo se proporcionan instrucciones para configurar un dispositivo Check Point para enviar alertas de software antiarranque en formato blade a Cisco Umbrella.



Nota: Check Point dejó de utilizar esta integración en la versión R81.20 después de que se lanzara inicialmente en R80.40.

Funcionalidad

La integración de Cisco Umbrella con el dispositivo Check Point Anti-Bot Software Blade envía las amenazas que ha encontrado (por ejemplo, dominios que alojan malware, comandos y control de botnets o sitios de suplantación de identidad) a Cisco Umbrella para su aplicación global.

A continuación, Cisco Umbrella valida la amenaza para garantizar que se pueda agregar a una política. Si se confirma que la información del servidor blade de software antiarranque de Check Point es una amenaza, la dirección de dominio se agrega a la lista de destinos de Check Point como parte de una configuración de seguridad que se puede aplicar a cualquier política de Cisco Umbrella. Esa política se aplica inmediatamente a cualquier solicitud realizada desde dispositivos asignados a esa política.

De cara al futuro, Cisco Umbrella analiza automáticamente las alertas de Check Point y agrega sitios malintencionados a la lista de destinos de Check Point. Esto amplía la protección de Check Point a todos los usuarios y dispositivos remotos y proporciona otra capa de aplicación para la red corporativa.

Configuration Steps

La configuración de la integración implica estos pasos:

1. Habilite la integración en Cisco Umbrella para generar un token de API con un script personalizado.
2. Implemente el token API y el script personalizado en el dispositivo Check Point.
3. Crear o editar una alerta de Check Point para publicarla en este nuevo script.
4. Establezca que los eventos de Check Point se bloqueen en Cisco Umbrella.

Evitar interrupciones del servicio

Para evitar interrupciones del servicio no deseadas, Cisco Umbrella recomienda agregar nombres de dominio críticos que nunca se pueden bloquear (por ejemplo, google.com o salesforce.com) a la lista global de permitidos (u otras listas de destinos según su política) antes de configurar la integración.

Los dominios vitales pueden incluir:

- La página de inicio de su organización
- Dominios que representan los servicios proporcionados que pueden tener registros internos y externos. Por ejemplo, "mail.myservicedomain.com" y "portal.myotherservicedomain.com".
- Las aplicaciones basadas en la nube menos conocidas de las que depende Cisco Umbrella no pueden incluirse en la validación automática de dominios. Por ejemplo, "localcloudservice.com".

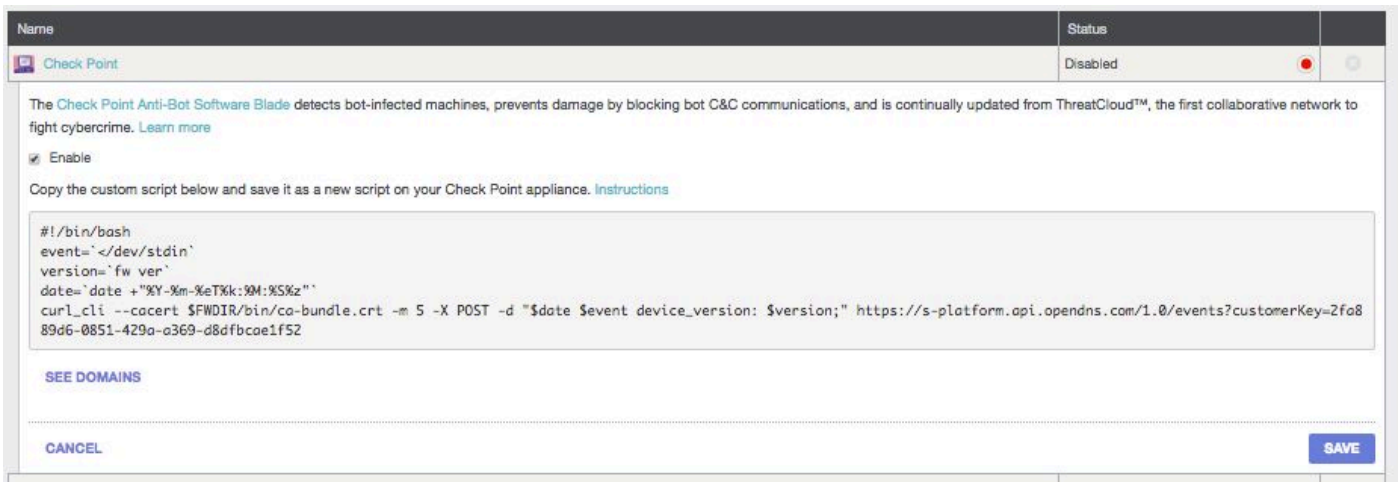
Estos dominios deben agregarse a la Lista global de permitidos, que se encuentra en Políticas > Listas de destino en Cisco Umbrella.

Paso 1: Generación de Umbrella Script y API Token

1. Inicie sesión en Cisco Umbrella Dashboard como administrador.

2. Navegue hasta Políticas > Componentes de Política > Integraciones y seleccione Check Point en la tabla para expandirla.

3. Seleccione la opción Activar.



4. Copie todo el guión, empezando por la línea con:

```
#!/bin/bash
```

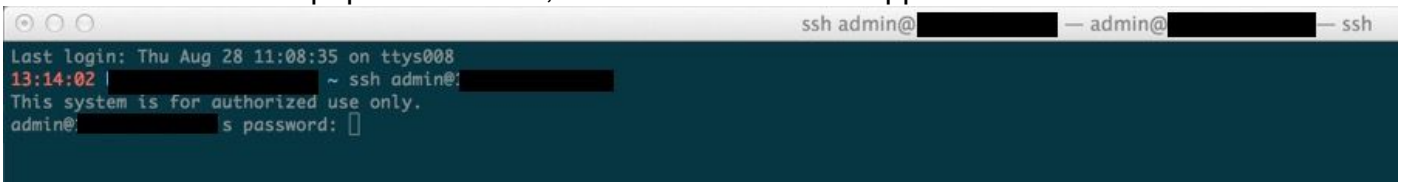
A continuación, puede utilizar la secuencia de comandos en pasos posteriores.

5. Seleccione Guardar para activar la integración.

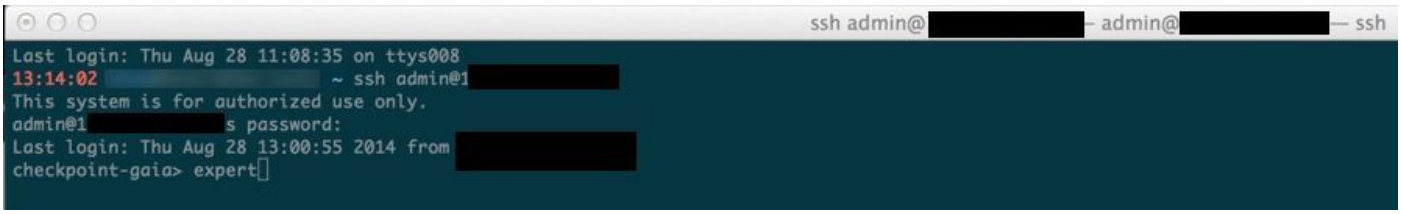
Paso 2: Implementación del script personalizado en el dispositivo Check Point

Los siguientes pasos son instalar la secuencia de comandos personalizada de Cisco Umbrella en su dispositivo Check Point y, a continuación, activarla en SmartDashboard.

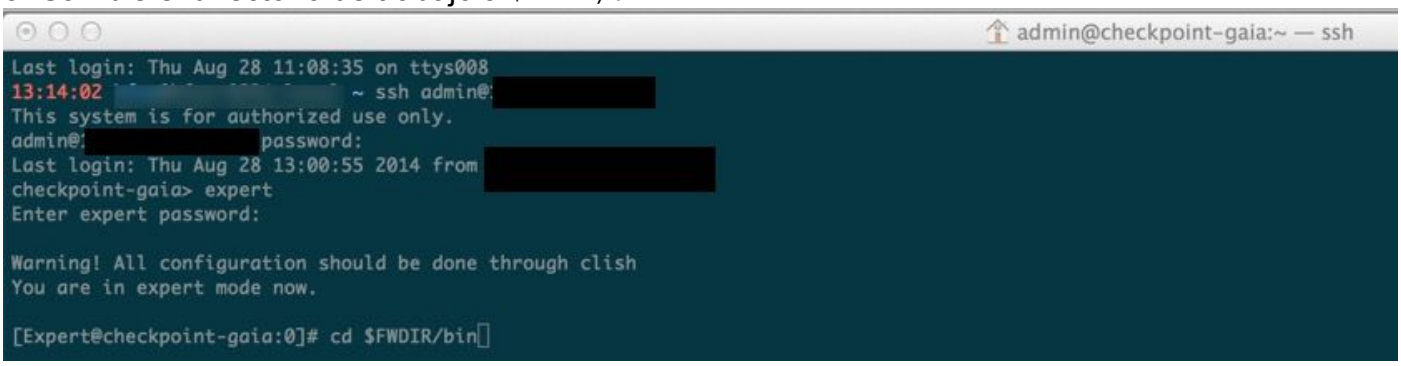
1. Para instalar el script personalizado, SSH en Check Point Appliance como administrador:



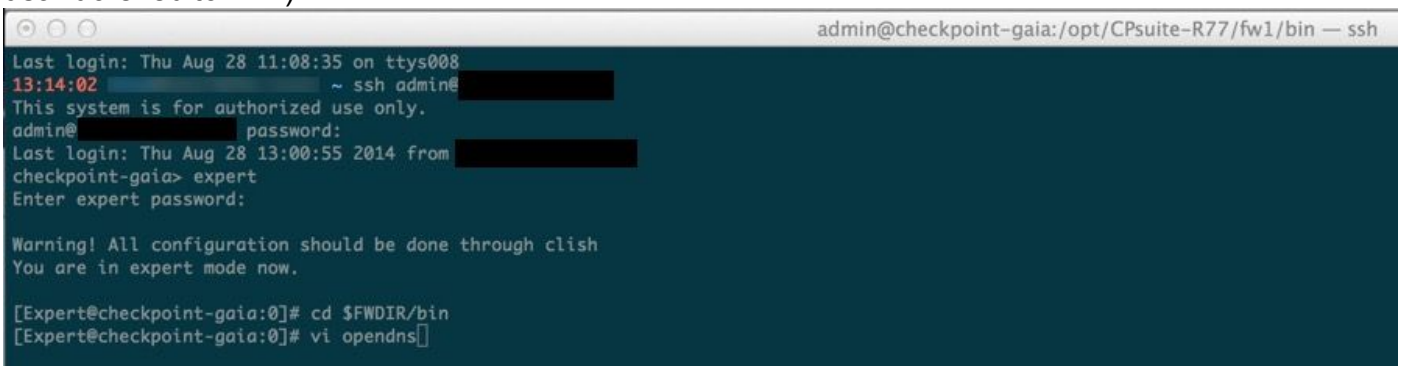
2. A continuación, inicie "Modo Experto" escribiendo "experto" en la línea de comandos:



3. Cambie el directorio de trabajo a `$FWDIR/bin`:

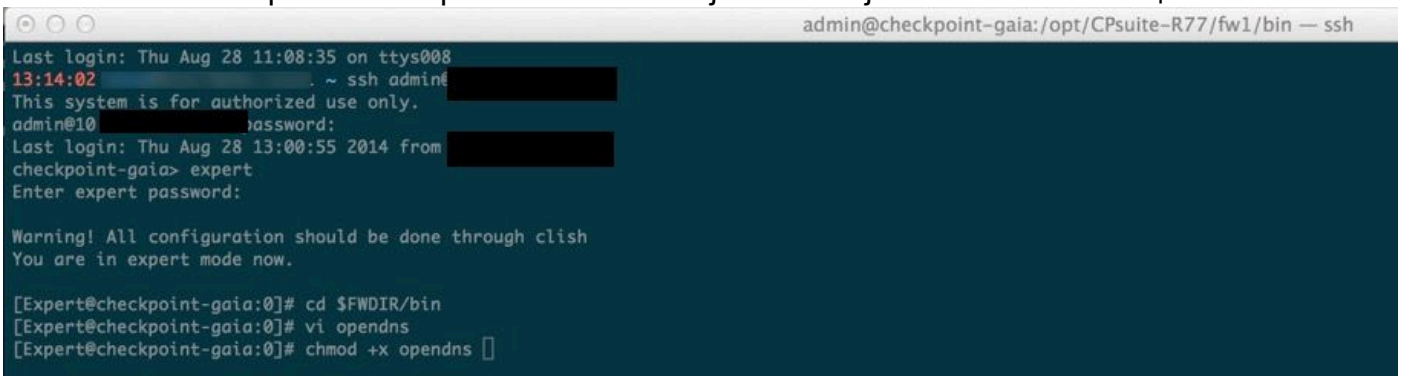


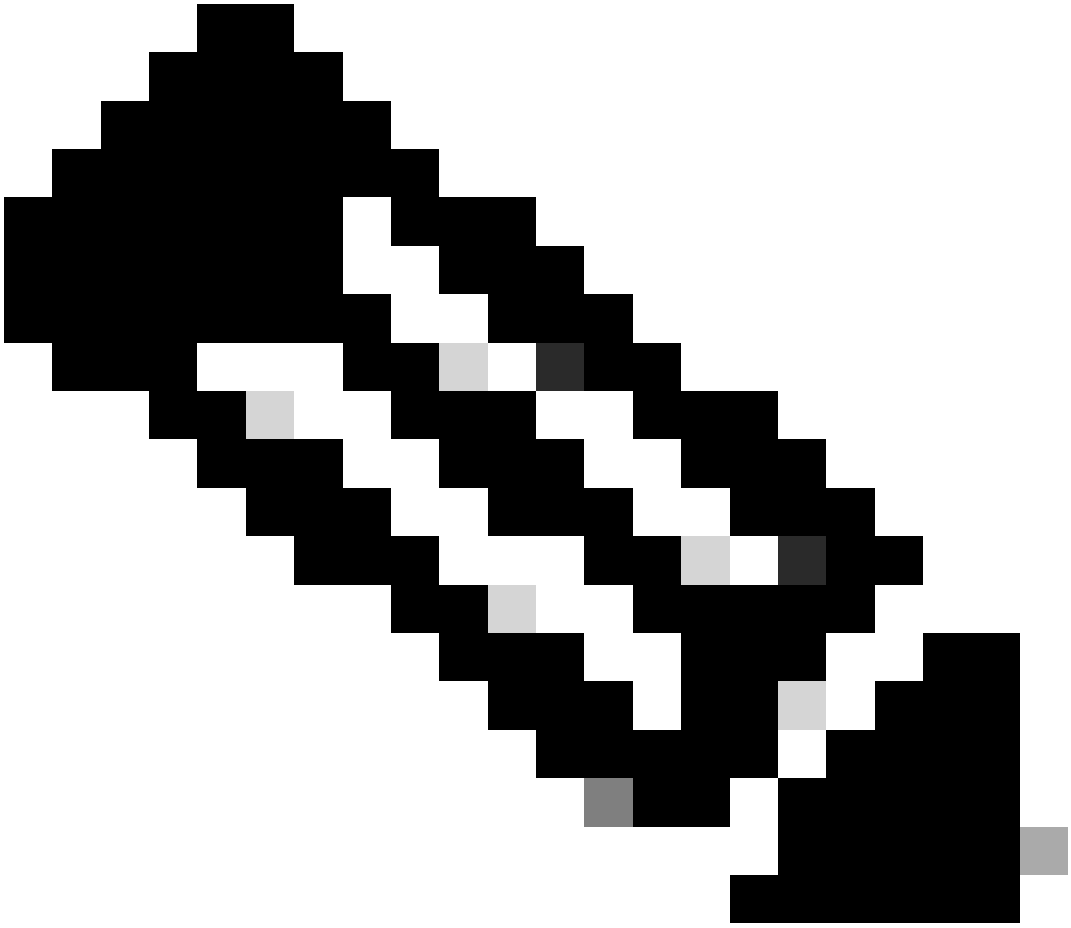
4. Abra un nuevo archivo llamado "opendns" usando un editor de texto (como en el ejemplo aquí usando el editor "vi"):



5. Pegue la secuencia de comandos de Cisco Umbrella en el archivo, guarde el archivo y salga del editor:

6. Convierta el script Umbrella personalizado en ejecutable ejecutando `chmod +x openns` :



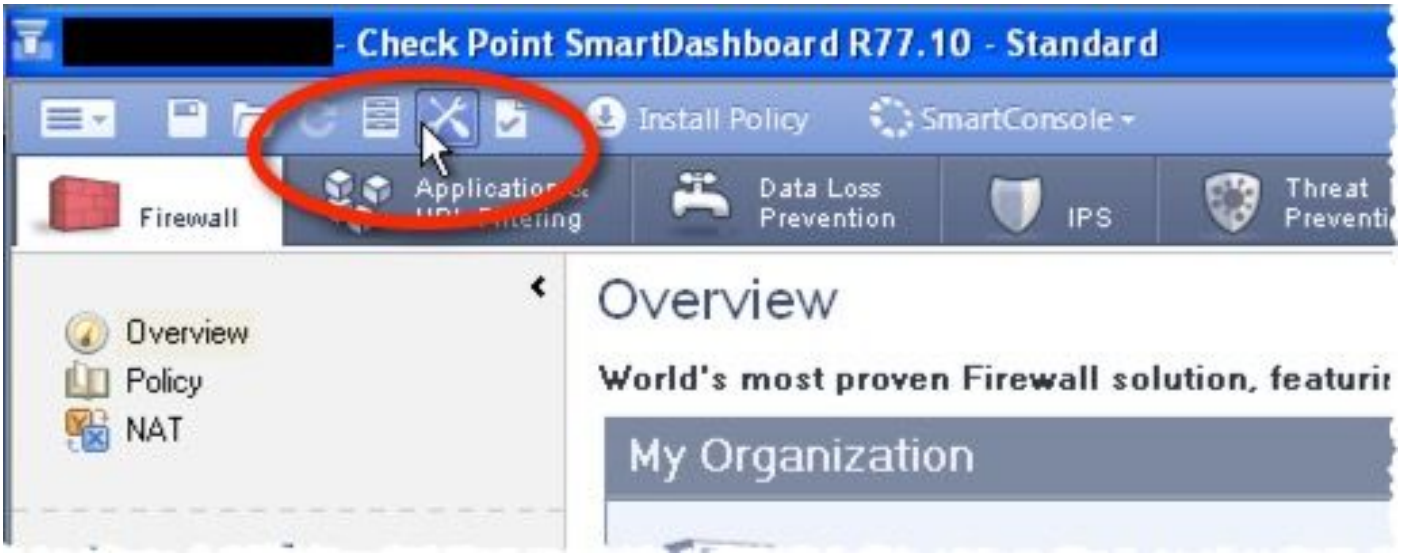


Nota: Si actualiza o cambia las versiones de blade, debe repetir estos pasos en la nueva versión.

Paso 3. Crear o editar una alerta de Check Point para publicarla en el nuevo script

1. Habilite SmartDashboard para publicar el nuevo script iniciando sesión e iniciando SmartDashboard:

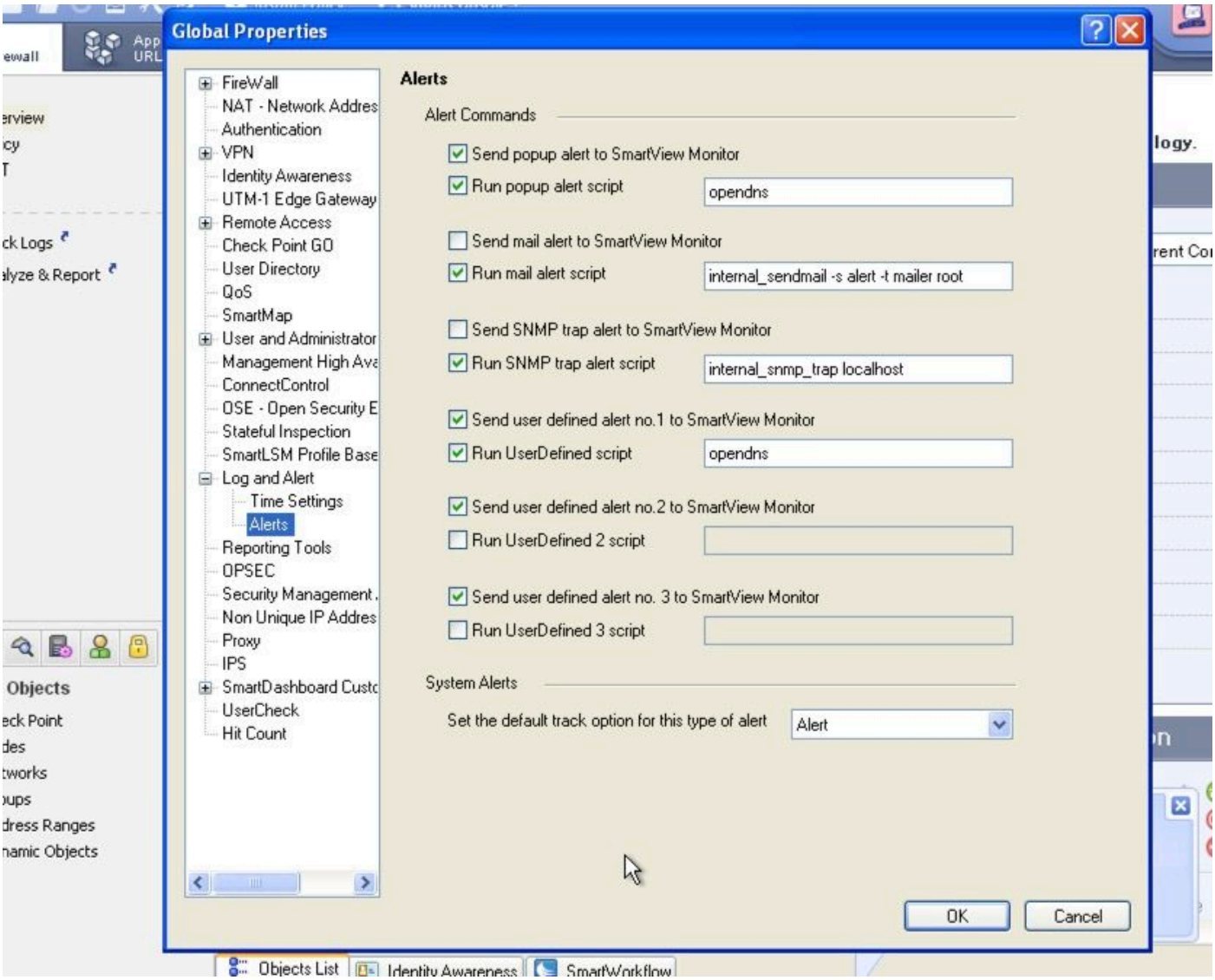
2. Abrir propiedades globales:



3. En Global Properties, abra Log and Alert > Alerts y complete estos pasos:

   - Seleccione Send popup alertscript y Run UserDefined script.
   - Defina "aperturas" en los campos de script para ambos.

4. Seleccione Aceptar. En SmartDashboard, guarde e instale la política actualizada.



Paso 4: Probar la integración y establecer los eventos de Check Point que se bloquearán

En primer lugar, genere un evento de prueba de servidor blade anti-bot para que aparezca en el panel de Cisco Umbrella:

1. Desde cualquier dispositivo de la red protegido por su dispositivo Check Point, cargue esta URL en su navegador:

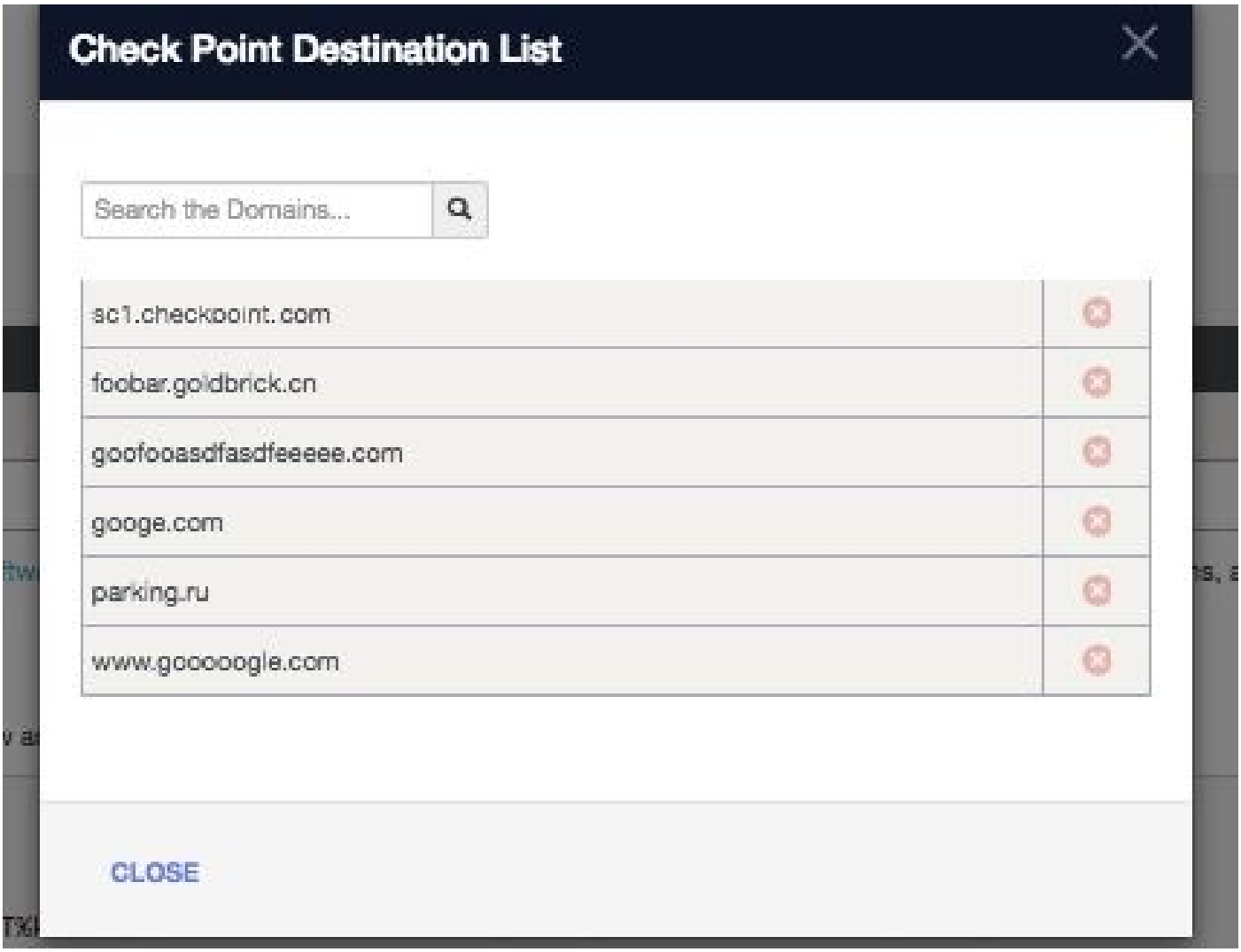
```
"http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html"
```

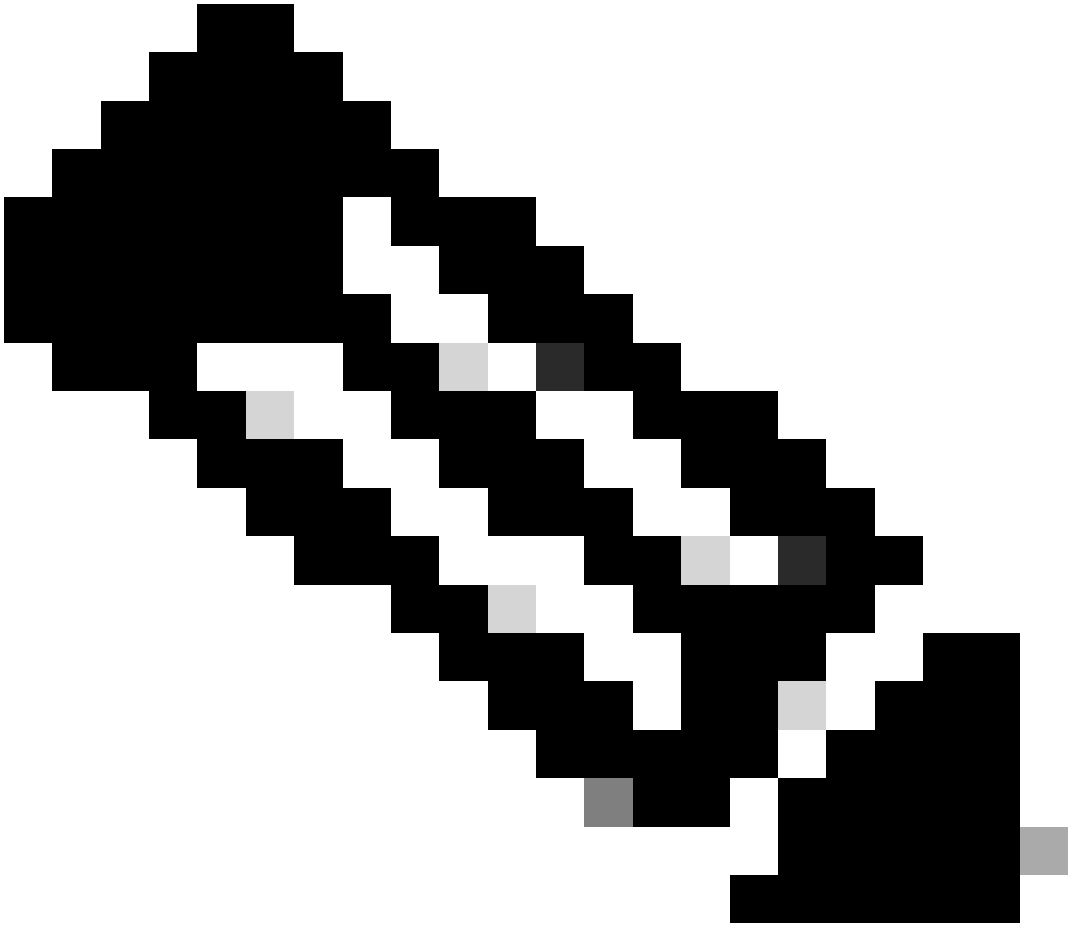
2. Inicie sesión en el panel de Cisco Umbrella como administrador.

3. Navegue hasta Políticas > Componentes de Política > Integraciones y seleccione Check Point en la tabla para expandirla.

4. Seleccione Consulte Dominios. Se abre una ventana en la que se muestra la lista de destinos

de Check Point que puede incluir "sc1.checkpoint.com". A partir de ese momento, una lista en la que se pueden realizar búsquedas comienza a rellenarse y a crecer.



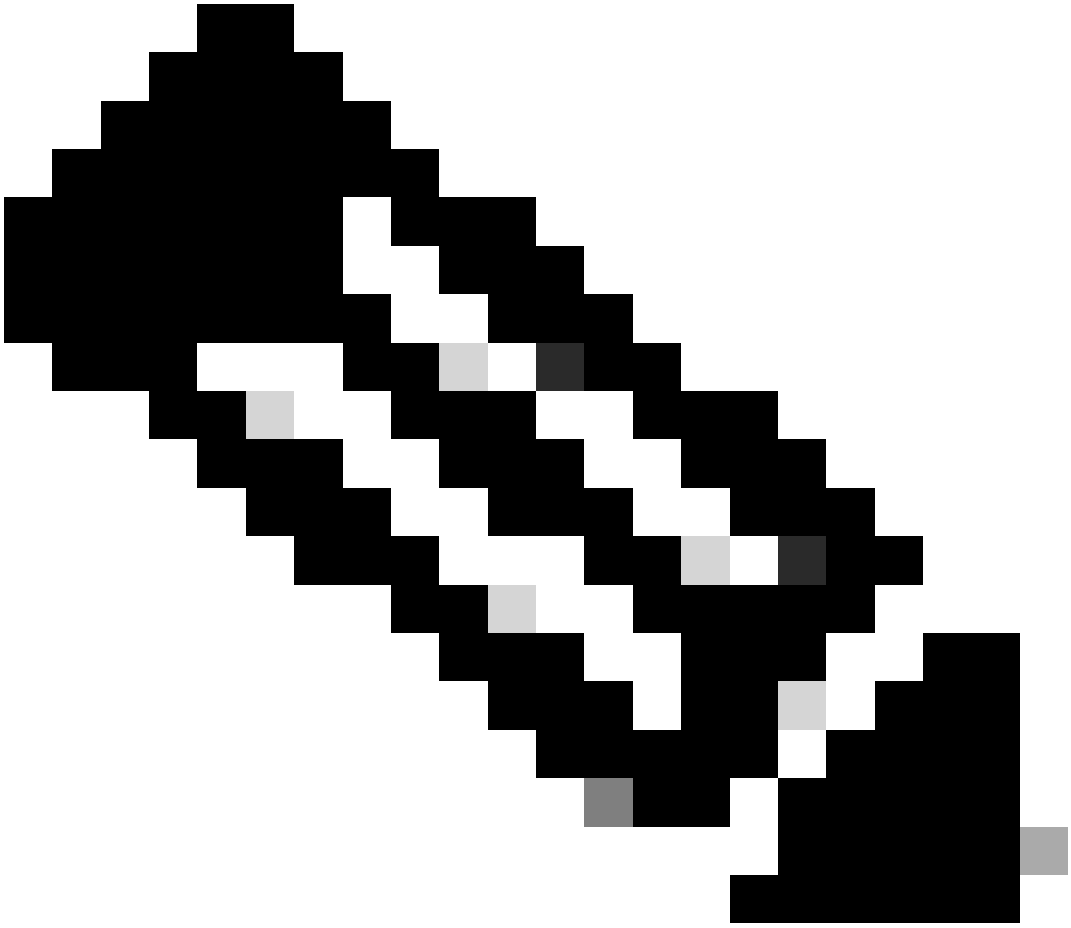


Nota: También puede modificar esta lista de destinos si aparece un dominio en el que no desea aplicar la política. Seleccione el icono Eliminar para eliminar el dominio.

Observación de eventos agregados a la categoría de seguridad de Check Point en "Modo auditoría"

El siguiente paso consiste en observar y auditar los eventos agregados a la nueva categoría de seguridad de Check Point.

Los eventos del dispositivo Check Point comienzan a rellenar una lista de destinos específica que se puede aplicar a las directivas como categoría de seguridad de Check Point. De forma predeterminada, la lista de destino y la categoría de seguridad se encuentran en "modo auditoría" y no se aplican a ninguna política y no pueden dar lugar a ningún cambio en las políticas de Cisco Umbrella existentes.



Nota: El "modo auditoría" puede activarse durante el tiempo que sea necesario en función del perfil de implementación y la configuración de red.

Revisar lista de destinos

Puede revisar la lista de destinos de Check Point en cualquier momento en Cisco Umbrella:

1. Acceda a Políticas > Componentes de Política > Integraciones.

2. Expanda Check Point en la tabla y seleccione Consulte Dominios.

Revisar la configuración de seguridad de una directiva

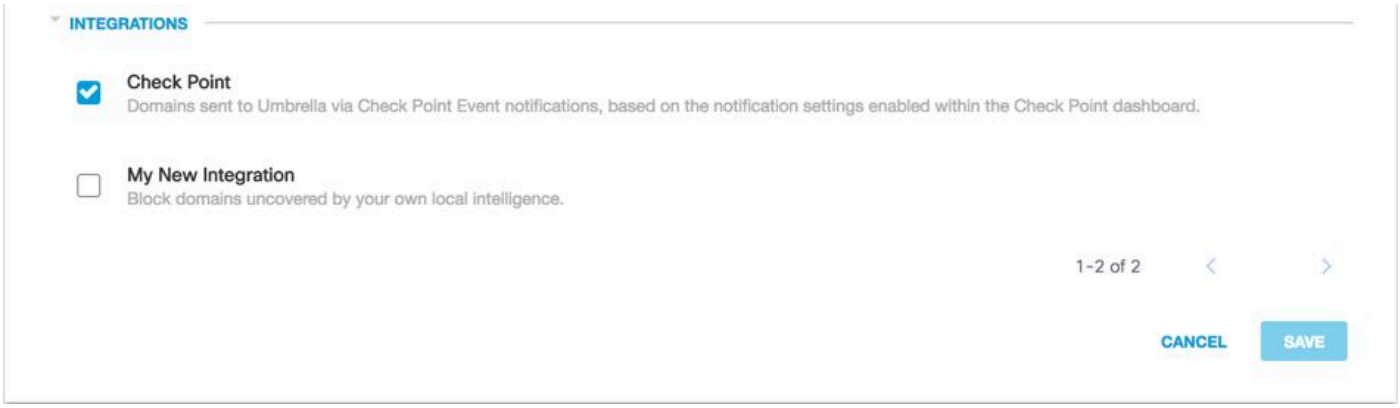
Puede revisar la configuración de seguridad que se puede habilitar para una política en cualquier momento en Cisco Umbrella:

1. Vaya a Políticas > Componentes de Política > Configuración de Seguridad.

2. Seleccione una configuración de seguridad en la tabla para expandirla.

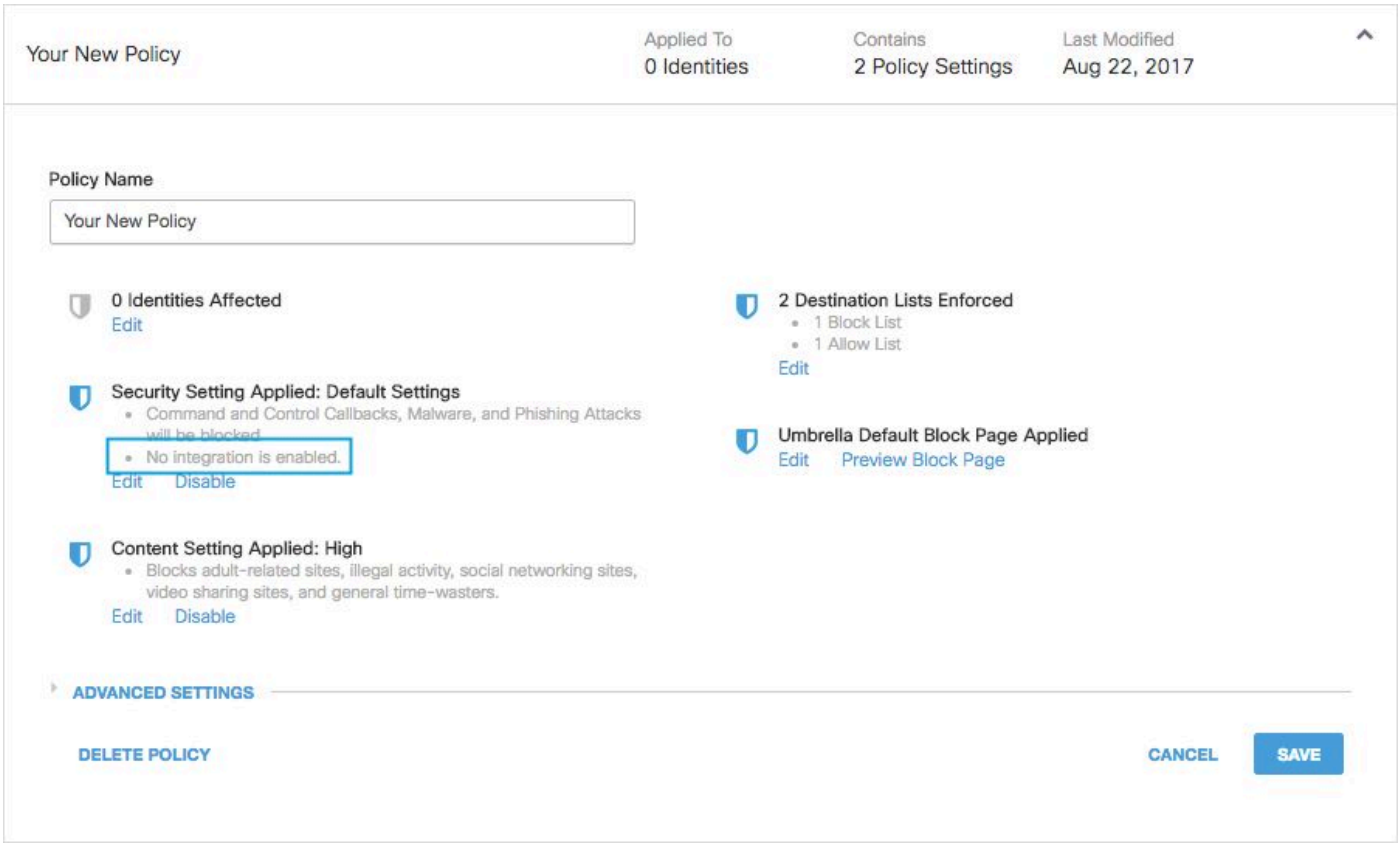
3. Desplácese hasta la sección Integraciones y amplíe la sección para mostrar la integración de Check Point.

4. Seleccione la opción para la integración de Check Point y, a continuación, seleccione Guardar.



115013984226

También puede revisar la información de integración a través de la página Resumen de parámetros de seguridad:



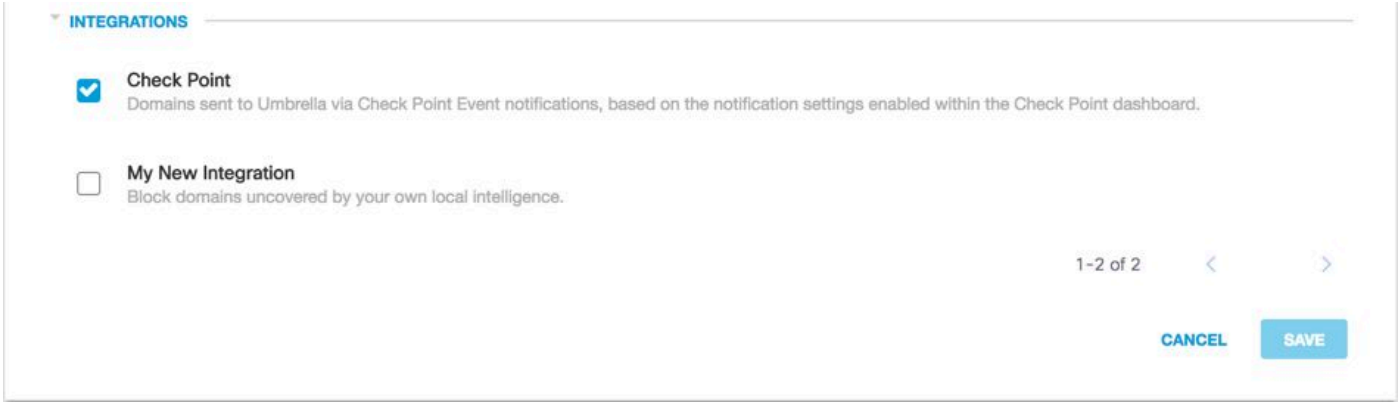
19916943300244

Aplicación de la configuración de seguridad de Check Point en "Modo de bloqueo" a una directiva para clientes gestionados

Una vez que esté preparado para que los clientes que administra Cisco Umbrella apliquen estas amenazas de seguridad adicionales, cambie la configuración de seguridad de una política existente o cree una nueva política que se sitúe por encima de la política predeterminada para asegurarse de que se aplica en primer lugar:

1. Asegúrese de que la integración de Check Point sigue activada, como se hizo en la sección anterior. Navegue hasta Políticas > Componentes de política > Configuración de seguridad y abra la configuración pertinente.

2. En Integraciones, verifique que la opción Check Point esté seleccionada. Si no es así, seleccione la opción y seleccione Guardar.



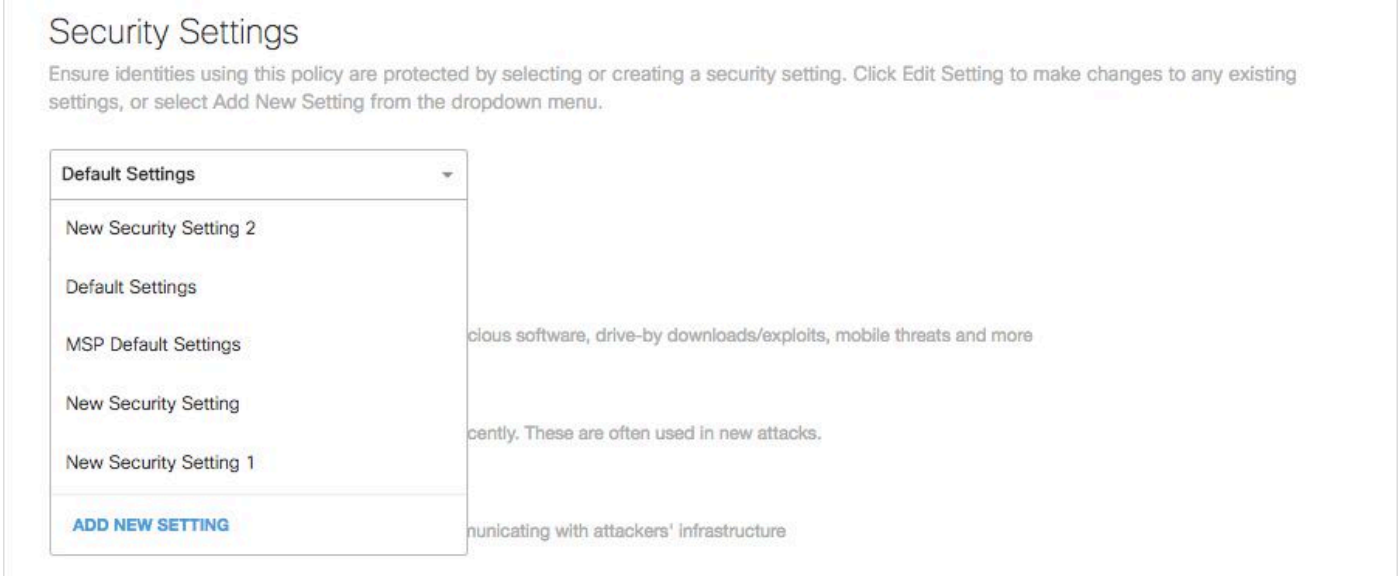
115013984226

A continuación, en el Asistente para directivas de Cisco Umbrella, agregue esta configuración de seguridad a una directiva que esté editando:

1. Acceda a una política: Policies > DNS Policies o Policies > Web Policy.

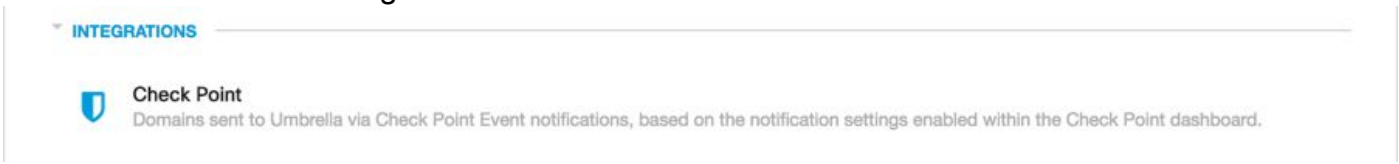
2. Expanda una directiva y, en Configuración de seguridad aplicada (Directivas DNS) o Configuración de seguridad (Directiva web), seleccione Editar.

3. En el menú desplegable Security Settings, seleccione una configuración de seguridad que incluya Check Point.



19916943316884

El icono de escudo de Integraciones se actualiza a azul.



115014149783

4. Seleccione Set & Return (DNS Policies) o Save (Web Policy).

Los dominios de Check Point incluidos en la configuración de seguridad de Check Point se pueden bloquear para esas identidades mediante la directiva.

Generación de informes para eventos de Check Point

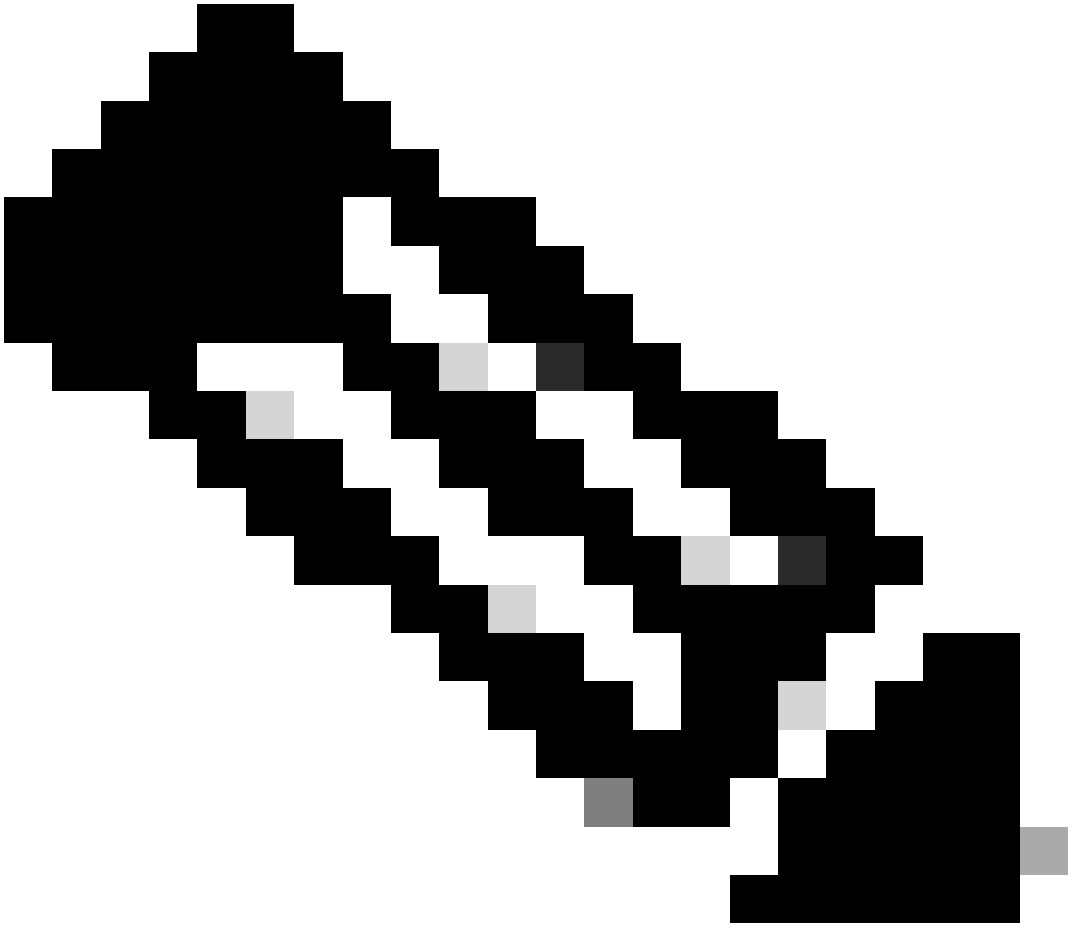
Informes sobre eventos de seguridad de Check Point

La lista de destinos de Check Point es una de las categorías de seguridad disponibles para los informes. La mayoría de los informes, o todos ellos, utilizan las categorías de seguridad como filtro. Por ejemplo, puede filtrar las categorías de seguridad para mostrar solamente la actividad relacionada con Check Point:

1. Vaya a Informes > Informes principales > Búsqueda de actividad.

2. En Categorías de seguridad, seleccione Check Point para filtrar el informe y mostrar sólo la categoría de seguridad de Check Point.

115014197623



Nota: Si la integración de Check Point está desactivada, no puede aparecer en el filtro Categorías de seguridad.

3. Seleccione Aplicar para consultar la actividad relacionada con Check Point del período seleccionado en el informe.

Notificación de adición de dominios a la lista de destinos de Check Point

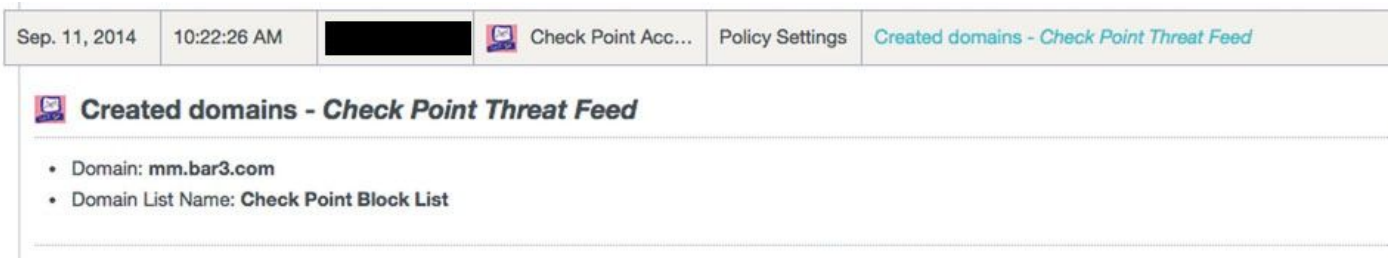
El registro de auditoría de administración de Cisco Umbrella incluye eventos del dispositivo Check Point a medida que agrega dominios a la lista de destinos. Estos dominios parecen agregarse mediante una etiqueta de "cuenta de Check Point", en la columna Usuario del registro de auditoría.

Para buscar el registro de auditoría de administración de Umbrella, vaya a Informes > Registro de auditoría de administración.

Para informar sobre cuándo se agregó un dominio, filtre para incluir sólo los cambios de Check

Point aplicando un filtro Filtrar por identidades y configuración para la lista de bloqueo de Check Point.

Una vez ejecutado el informe, puede ver una lista de dominios agregados a la lista de destinos de Check Point.



Gestión de detecciones no deseadas o falsos positivos

Administración de una lista de permitidos para la detección no deseada

Aunque es poco probable, es posible que los dominios agregados automáticamente por su dispositivo Check Point puedan desencadenar un bloqueo no deseado que pueda bloquear el acceso de los usuarios a sitios web concretos. En una situación como esta, Cisco Umbrella recomienda agregar los dominios a una lista de permitidos, que tiene prioridad sobre todos los demás tipos de listas de bloqueo, incluida la configuración de seguridad. Una lista de permitidos tiene prioridad sobre una lista de bloqueo cuando un dominio está presente en ambos.

Hay dos razones por las que se prefiere este enfoque:

- En primer lugar, en caso de que el dispositivo Check Point tuviera que volver a agregar el dominio después de que se haya eliminado, la lista de permitidos protege frente a este hecho y provoca más problemas.
- En segundo lugar, la lista de permitidos muestra un registro histórico de dominios problemáticos para informes de diagnóstico o auditoría posteriores.

De forma predeterminada, existe una lista global de permitidos que se aplica a todas las políticas. Al agregar un dominio a la lista global de permitidos, el dominio se permite en todas las directivas.

Si la configuración de seguridad de Check Point en modo de bloqueo sólo se aplica a un subconjunto de las identidades administradas de Cisco Umbrella (por ejemplo, sólo se aplica a equipos móviles y dispositivos móviles), puede crear una lista de permitidos específica para esas identidades o políticas.

Para crear una lista de permitidos:

1. Navegue hasta Políticas > Listas de Destino y seleccione el icono Agregar.

2. Seleccione Permitir y agregue su dominio a la lista.

3. Seleccione Guardar.

Una vez guardada la lista, puede agregarla a una directiva existente que cubra los clientes afectados por el bloqueo no deseado.

Eliminación de dominios de la lista de destinos de Check Point

Junto a cada nombre de dominio de la lista de destinos de Check Point se encuentra el icono Eliminar. La eliminación de dominios le permite limpiar la lista de destinos de Check Point en caso de detección no deseada.

Sin embargo, la eliminación no es permanente si el dispositivo Check Point vuelve a enviar el dominio a Cisco Umbrella.

Para eliminar un dominio:

1. Navegue hasta Configuraciones > Integraciones, luego seleccione Check Point para expandirlo.

2. Seleccione Consulte Dominios.

3. Busque el nombre de dominio que desea eliminar.

4. Seleccione el icono Suprimir.

5. Seleccione Cerrar.

6. Seleccione Guardar.

Si se produce una detección no deseada o un falso positivo, Cisco Umbrella recomienda crear una lista de permitidos en Cisco Umbrella inmediatamente y, a continuación, remediar el falso positivo en el dispositivo Check Point. Posteriormente, puede quitar el dominio de la lista de destinos de Check Point.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).