Integre Umbrella con FireEye

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Overview

Funcionalidad de integración

Configuración de Cisco Umbrella Dashboard para recibir información de FireEye

Configuración de FireEye para comunicarse con Cisco Umbrella

Garantizar la conectividad: "Prueba de fuego" entre FireEye y Cisco Umbrella

Observación de eventos agregados a la configuración de seguridad de FireEye en "modo auditoría"

- Revisar lista de destinos
- Revisar la configuración de seguridad de una directiva

Aplicación de la configuración de seguridad de FireEye en "modo de bloqueo" a una política para clientes gestionados

Informes en Cisco Umbrella para eventos de FireEye

- Informes sobre eventos de seguridad de FireEye
- Informes sobre cuándo se agregaron los dominios a la lista de destinos de FireEye

Gestión de detecciones no deseadas o falsos positivos

- Permitir listas
- Eliminación de dominios de la lista de destinos de FireEye

Introducción

Este documento describe cómo integrar Cisco Umbrella con FireEye.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Un appliance FireEye con acceso a Internet público.
- Derechos administrativos de Cisco Umbrella Dashboard.
- Cisco Umbrella Dashboard debe tener habilitada la integración de FireEye.

Componentes Utilizados

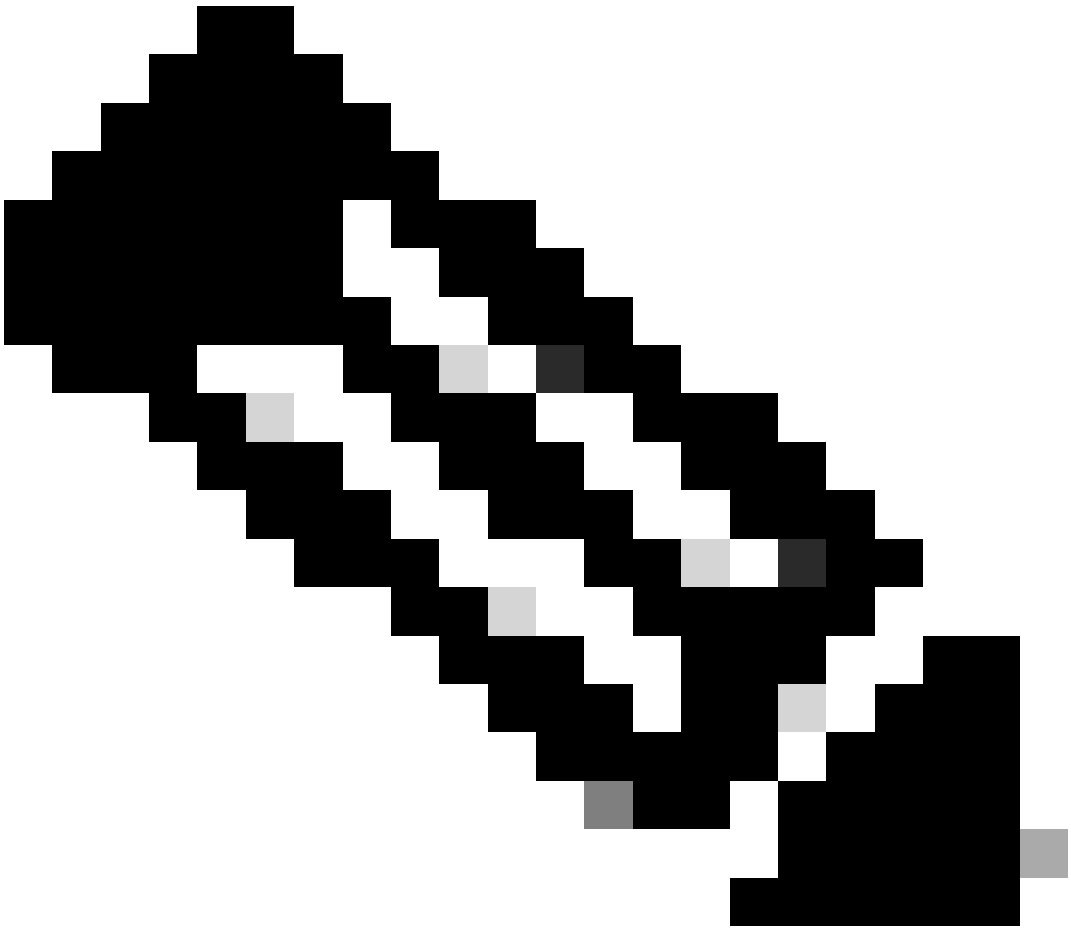
La información de este documento se basa en Cisco Umbrella.

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

Gracias a la integración entre el appliance de seguridad FireEye y Cisco Umbrella, los responsables de seguridad y los administradores pueden ahora ampliar la protección frente a amenazas avanzadas a los portátiles, tablets o teléfonos en roaming, a la vez que proporcionan otro nivel de aplicación a una red corporativa distribuida.

Esta guía describe cómo configurar FireEye para comunicarse con Cisco Umbrella de modo que los eventos de seguridad de FireEye se integren en las políticas que se pueden aplicar a los clientes protegidos por Cisco Umbrella.



Nota: La integración de FireEye solo se incluye en los paquetes de Cisco Umbrella como

---

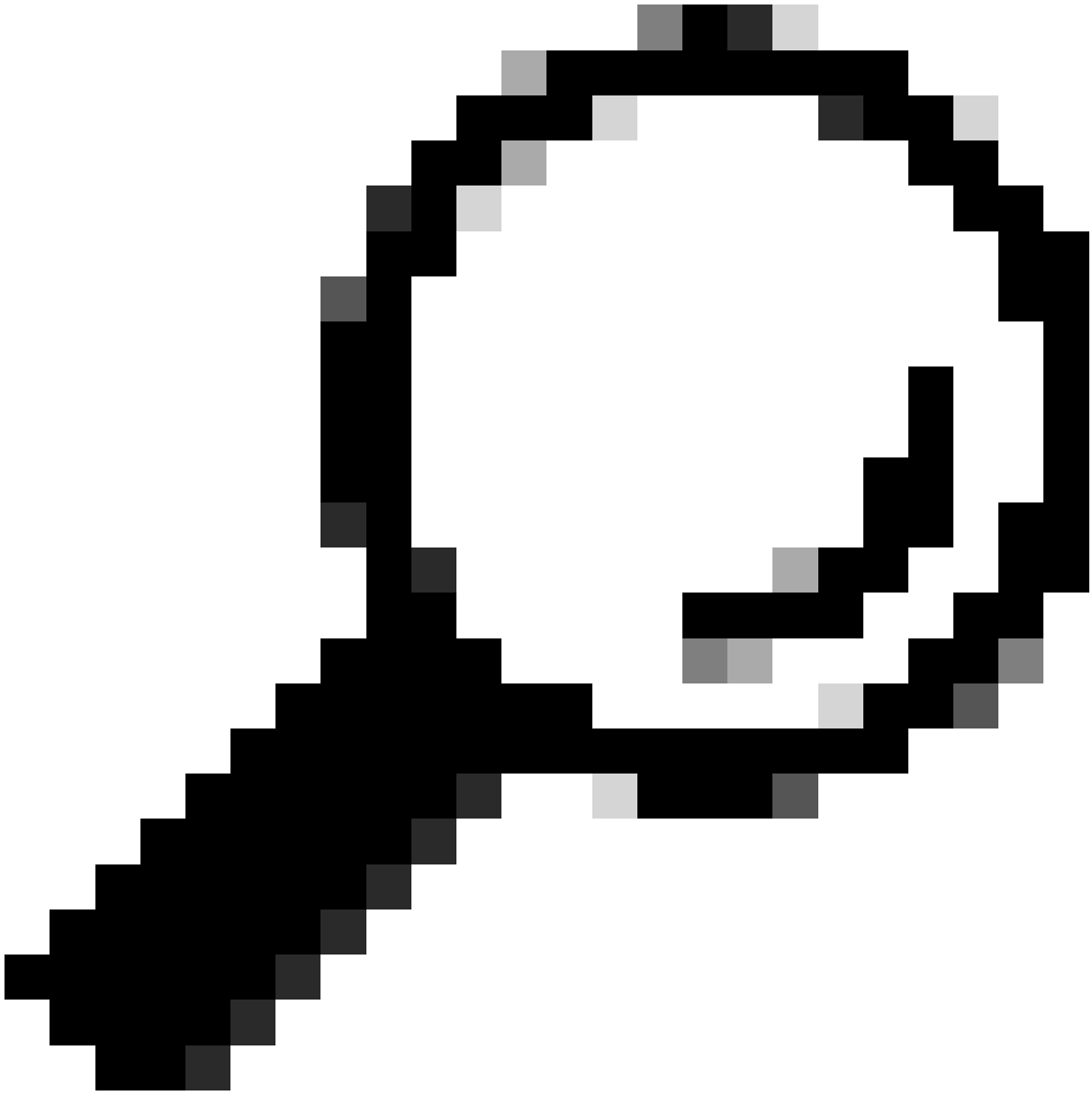
DNS Essentials, DNS Advantage, SIG Essentials o SIG Advantage. Si no dispone de ninguno de estos paquetes y desea disfrutar de la integración con FireEye, póngase en contacto con su Cisco Umbrella Account Manager. Si tiene el paquete Cisco Umbrella correcto pero no ve FireEye como una integración para su panel, póngase en contacto con el servicio de asistencia de Cisco Umbrella.

Funcionalidad de integración

En primer lugar, el appliance FireEye envía a Cisco Umbrella amenazas basadas en Internet que ha detectado, como dominios que alojan malware, comandos y controles para botnet o sitios de suplantación de identidad.

A continuación, Cisco Umbrella valida la información que se pasa a Cisco Umbrella para garantizar que es válida y que se puede agregar a una política. Si se confirma que la información de FireEye tiene el formato correcto (por ejemplo, no es un archivo, una URL compleja o un dominio muy popular), la dirección del dominio se agrega a la lista de destinos de FireEye como parte de una configuración de seguridad que se puede aplicar a cualquier política de Cisco Umbrella. Esta política se aplica inmediatamente a cualquier solicitud que se realice desde dispositivos que utilicen políticas con la lista de destinos de FireEye.

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



Consejo: Aunque Cisco Umbrella hace todo lo posible por validar y permitir dominios que se sabe que son seguros en general (por ejemplo, Google y Salesforce), para evitar interrupciones no deseadas, le sugerimos que agregue dominios que nunca desee bloquear a la Lista global de permitidos u otras listas de destinos según su política. Entre los ejemplos, se encuentran los siguientes:

- 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".
- Aplicaciones basadas en la nube menos conocidas de las que depende que Cisco Umbrella no incluya en la validación automática de dominios. Por ejemplo, "localcloudservice.com".

Estos dominios se pueden agregar a la Lista global de permitidos, que se encuentra en

Políticas > Listas de destino en Cisco Umbrella.

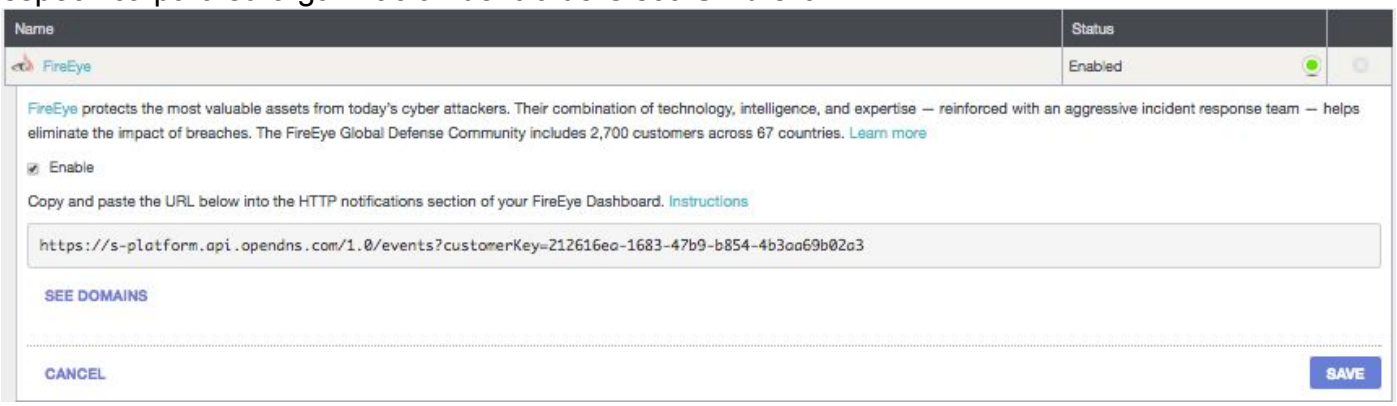
Configuración de Cisco Umbrella Dashboard para recibir información de FireEye

El primer paso consiste en encontrar la URL exclusiva en Cisco Umbrella para que el appliance FireEye se comunique con él.

1. Inicie sesión en Cisco Umbrella Dashboard como administrador.

2. Navegue hasta Políticas > Componentes de política > Integraciones y seleccione FireEye en la tabla para expandirla.

3. Active la casilla Activar y, a continuación, seleccione Guardar. Esto genera una URL única y específica para su organización dentro de Cisco Umbrella.

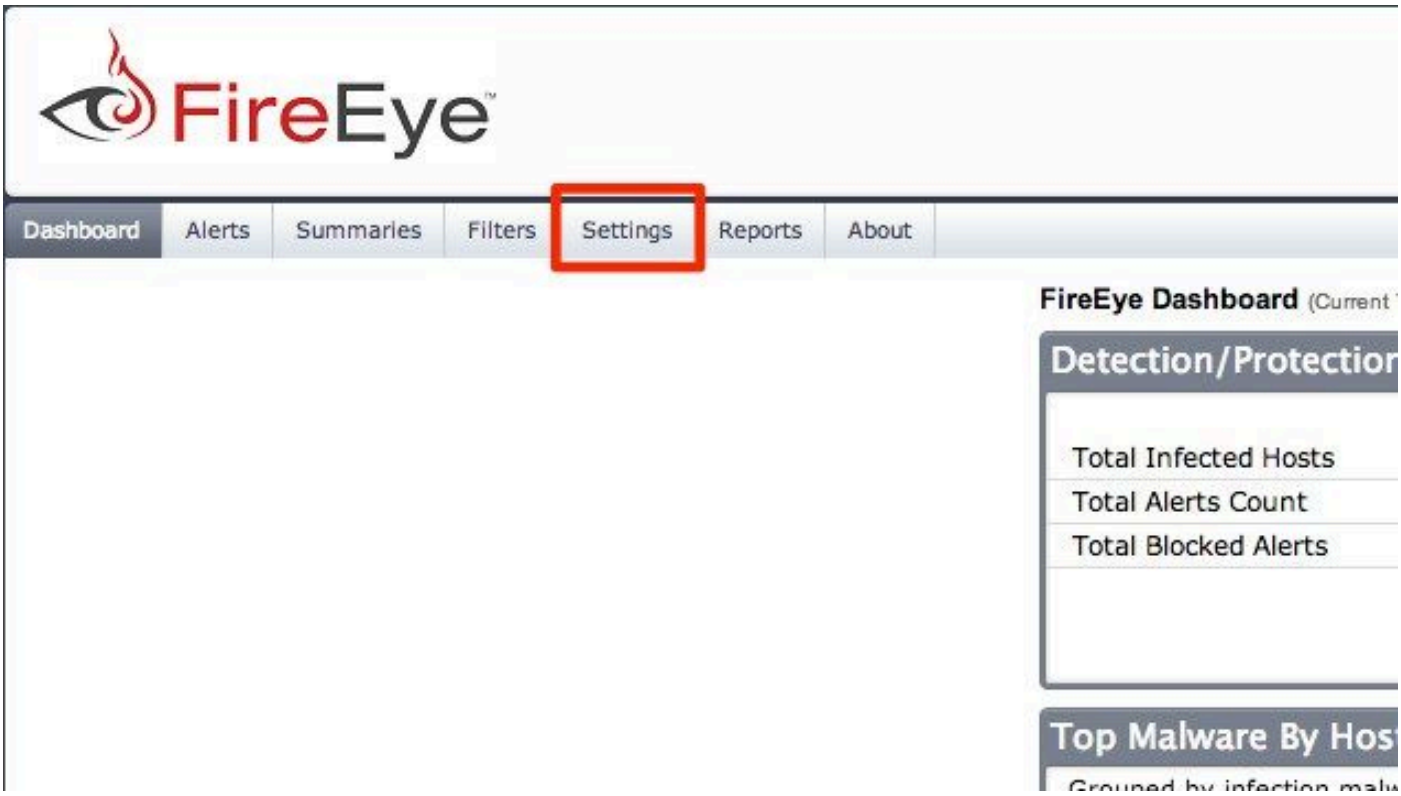


Puede utilizar esta URL más adelante para configurar el dispositivo FireEye para enviar datos a Cisco Umbrella, así que asegúrese de copiar la URL.

Configuración de FireEye para comunicarse con Cisco Umbrella

Para comenzar a enviar tráfico desde su appliance FireEye a Cisco Umbrella, debe configurar FireEye con la información de URL generada en la sección anterior.

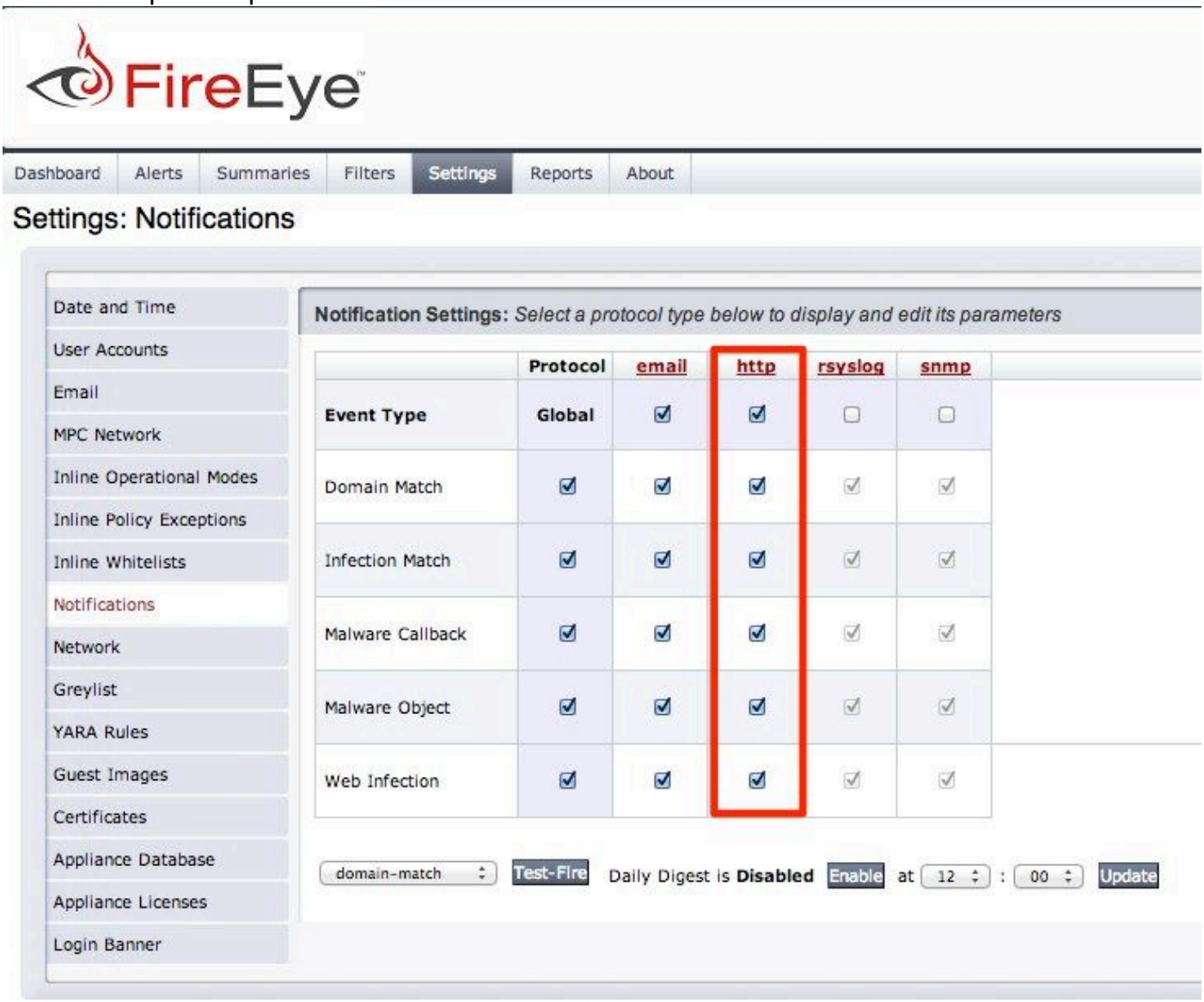
1. Inicie sesión en FireEye y seleccione Configuración.



2. Seleccione Notificaciones en la lista de configuraciones:

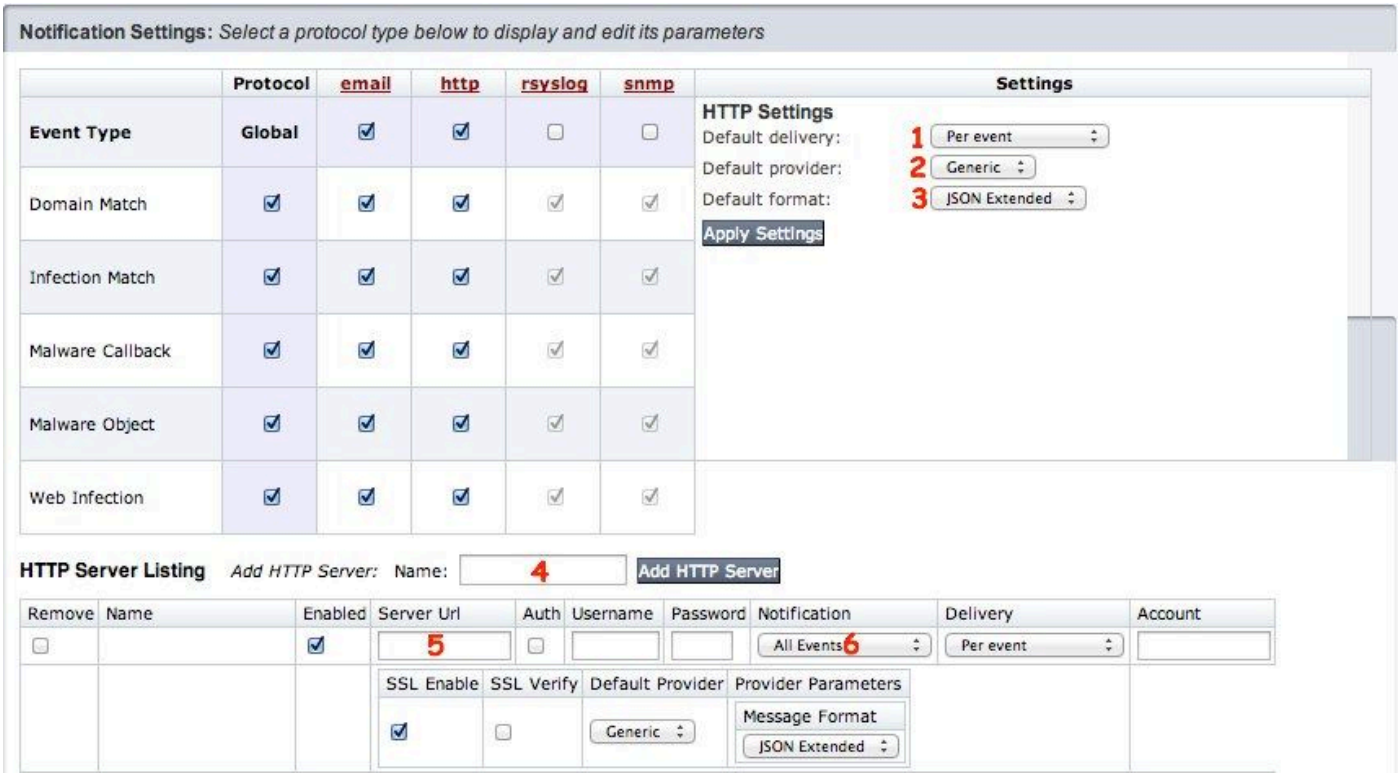
FireEye
Dashboard
Alerts
Summaries
Filters
Settings
Reports
About
Settings: Date and Time
Date and Time
User Accounts
Email
MPC Network
Inline Operational Modes
Inline Policy Exceptions
Inline Whitelists
Notifications
Network
Greylist
YARA Rules
Guest Images
Certificates
Appliance Database
Appliance Licenses
Login Banner
Date and Time Settings
Manually set the date, time, and time zone. Or, op
synchronization.
(Current Time: 11/11/13 17:29:24 UTC)
Set Manually:
November
11
2013
17
Enable NTP:
Add NTP Server:
NTP Server
Delete
Update T
pool.ntp.org
Update T
time.nist.gov
Update T
Remove Selected NTP Servers
Set Time Zone:
UTC
Set Time Zone

3. Asegúrese de que todos los tipos de eventos que se van a enviar a Cisco Umbrella estén seleccionados (Umbrella recomienda empezar por todos) y, a continuación, seleccione el enlace HTTP en la parte superior de la columna.



4. Cuando se expanda el menú, seleccione estas opciones para activar la notificación de eventos. Los pasos numerados se describen en la captura de pantalla:

1. Entrega predeterminada: Por evento
2. Proveedor predeterminado: GENÉRICO
3. Formato predeterminado: JSON extendido
4. Asigne al servidor HTTP el nombre "OpenDNS".
5. URL del servidor: Pegue la URL de Cisco Umbrella que generó desde su panel de Cisco Umbrella anteriormente aquí.
6. Lista desplegable de notificación: Seleccione Todos los eventos para garantizar la máxima cobertura.



5. Asegúrese de que las listas desplegables Entrega, Proveedor por Defecto y Parámetros del Proveedor coincidan con los valores por defecto, o si se están utilizando varios servidores de notificación:

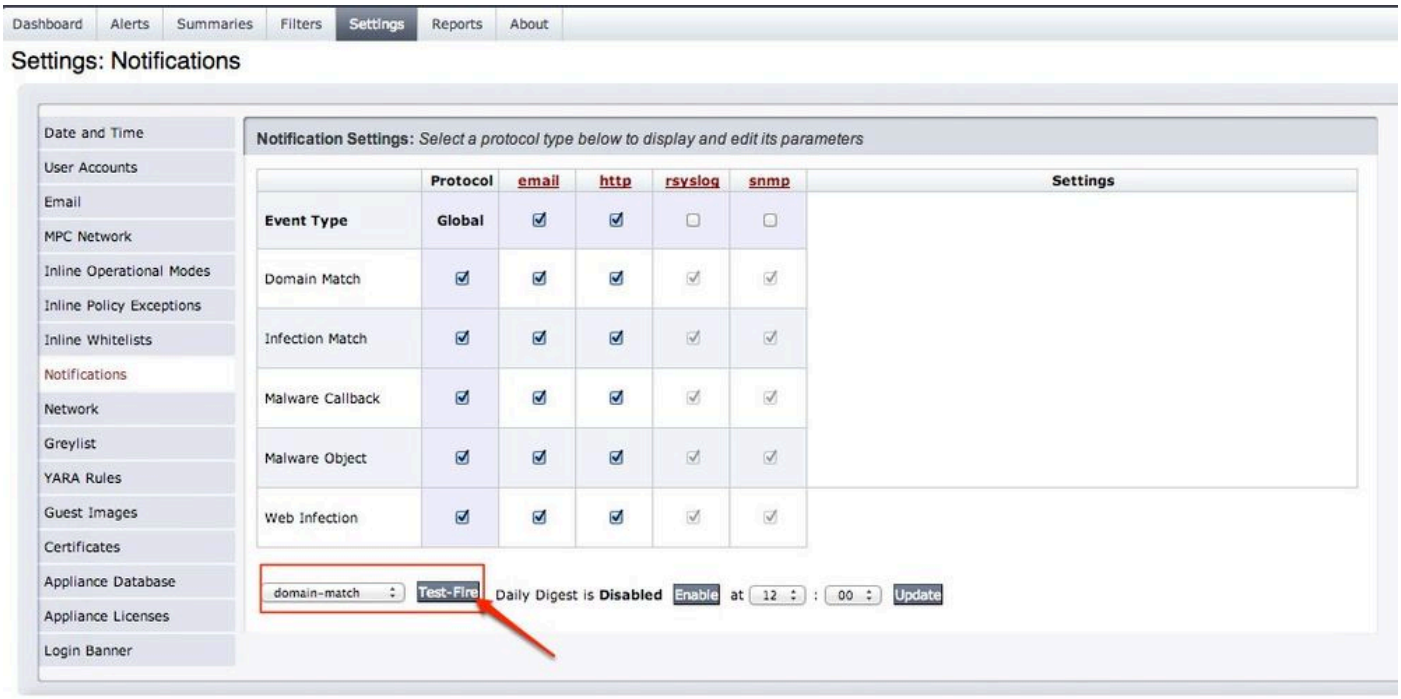
- Entrega: Por evento
- Proveedor predeterminado: GENÉRICO
- Parámetros del proveedor: Formato de mensaje JSON extendido
- (Opcional) Si prefiere enviar tráfico a través de SSL, seleccione SSL Enable.

En este momento, el dispositivo FireEye está configurado para enviar los tipos de eventos seleccionados a Cisco Umbrella. A continuación, aprenda a ver esta información en su Cisco Umbrella Dashboard y establezca una política para bloquear este tráfico.

Garantizar la conectividad: "Prueba de fuego" entre FireEye y Cisco Umbrella

En este momento, es recomendable probar la conectividad y asegurarse de que todo está configurado correctamente:

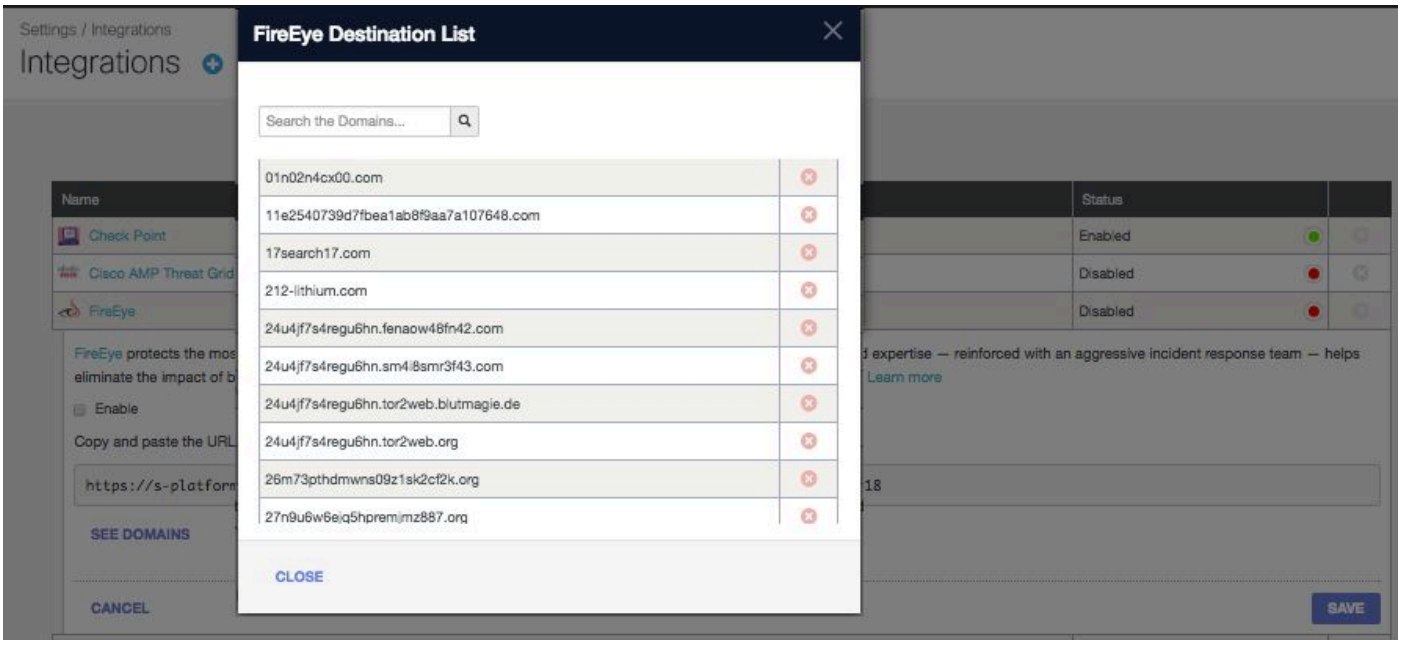
1. En FireEye, seleccione domain-match en el menú desplegable Test Fire y seleccione Test Fire:



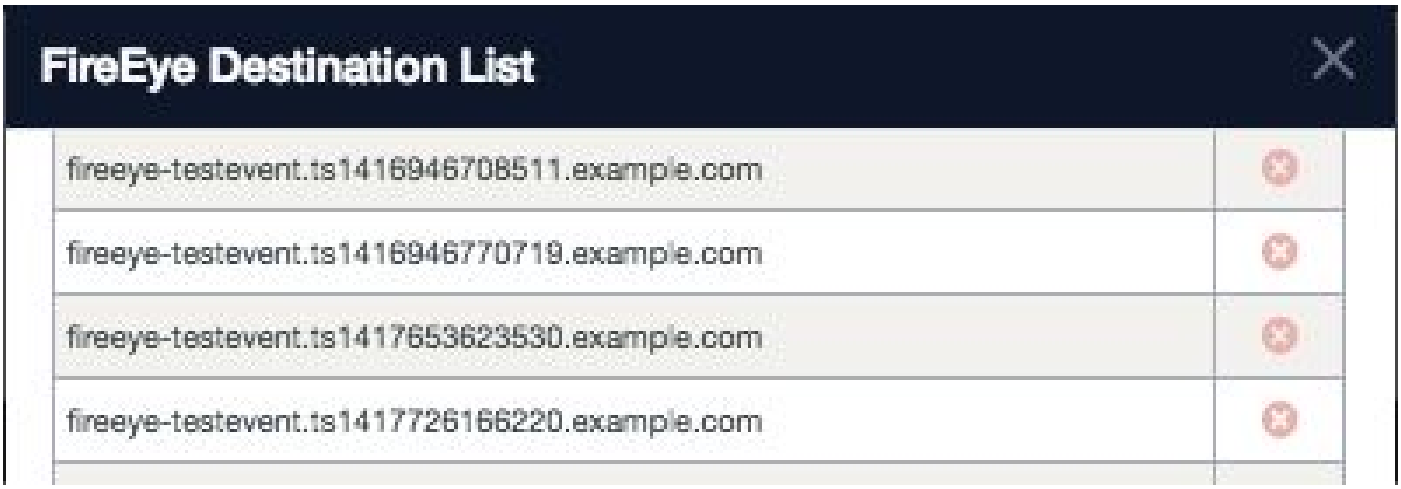
En Cisco Umbrella, la integración de FireEye incluye una lista de dominios proporcionada por el appliance FireEye para ver qué dominios se están agregando de forma activa.

2. Después de seleccionar Test Fire, en Cisco Umbrella, navegue hasta Settings > Integrations y seleccione FireEye en la tabla para expandirlo.

3. Seleccione Consulte Dominios.



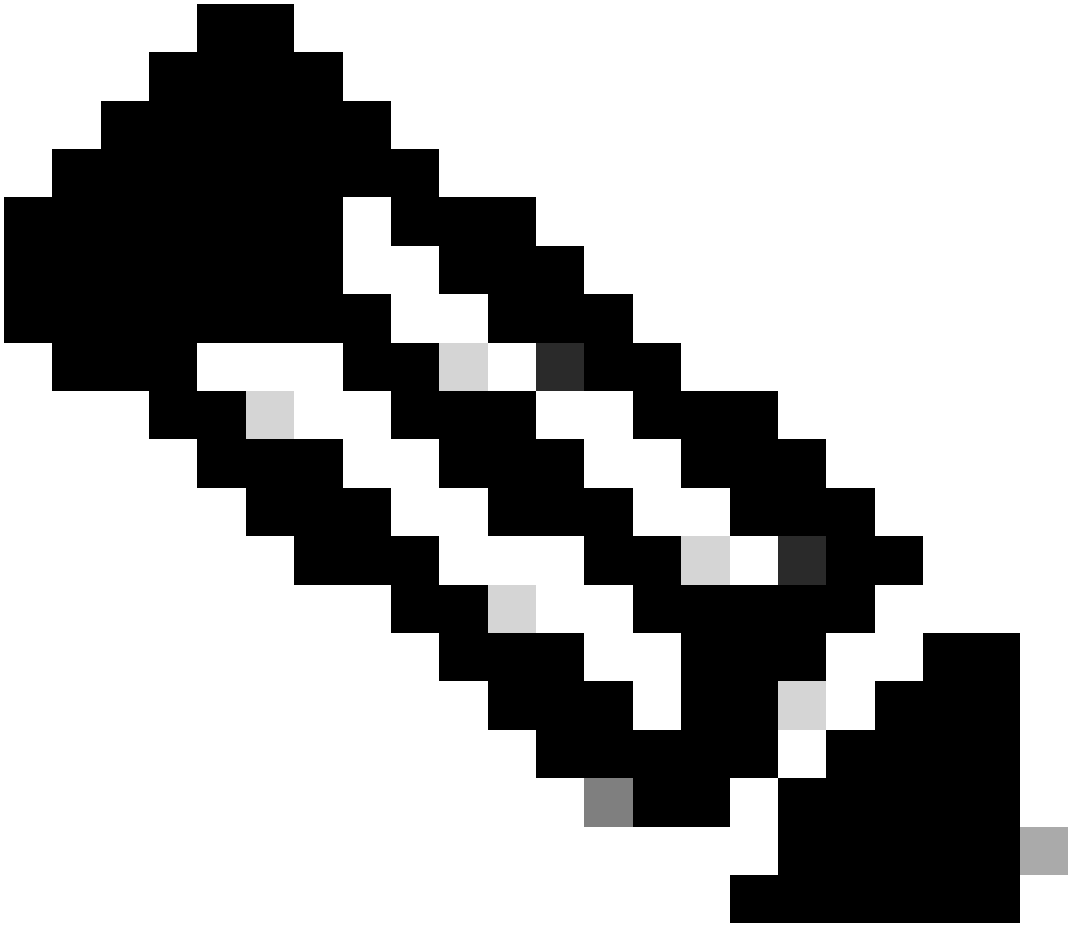
Al seleccionar Test Fire, se genera un dominio en la lista de destinos de FireEye denominado "fireeye-testevent.example.com-[date]". Cada vez que selecciona Test Fire en FireEye, se crea un dominio único con la fecha en UNIX Epoch time asociada a la prueba, de modo que las pruebas futuras puedan tener un nombre de dominio de prueba único.



Si la prueba de fuego tiene éxito, se envían más eventos de FireEye a Cisco Umbrella y comienza a cumplimentarse y a aumentar una lista de búsqueda.

Observación de eventos agregados a la configuración de seguridad de FireEye en "modo auditoría"

Los eventos del appliance FireEye comienzan a cumplimentar una lista de destinos específica que se puede aplicar a las políticas como categoría de seguridad de FireEye. 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.



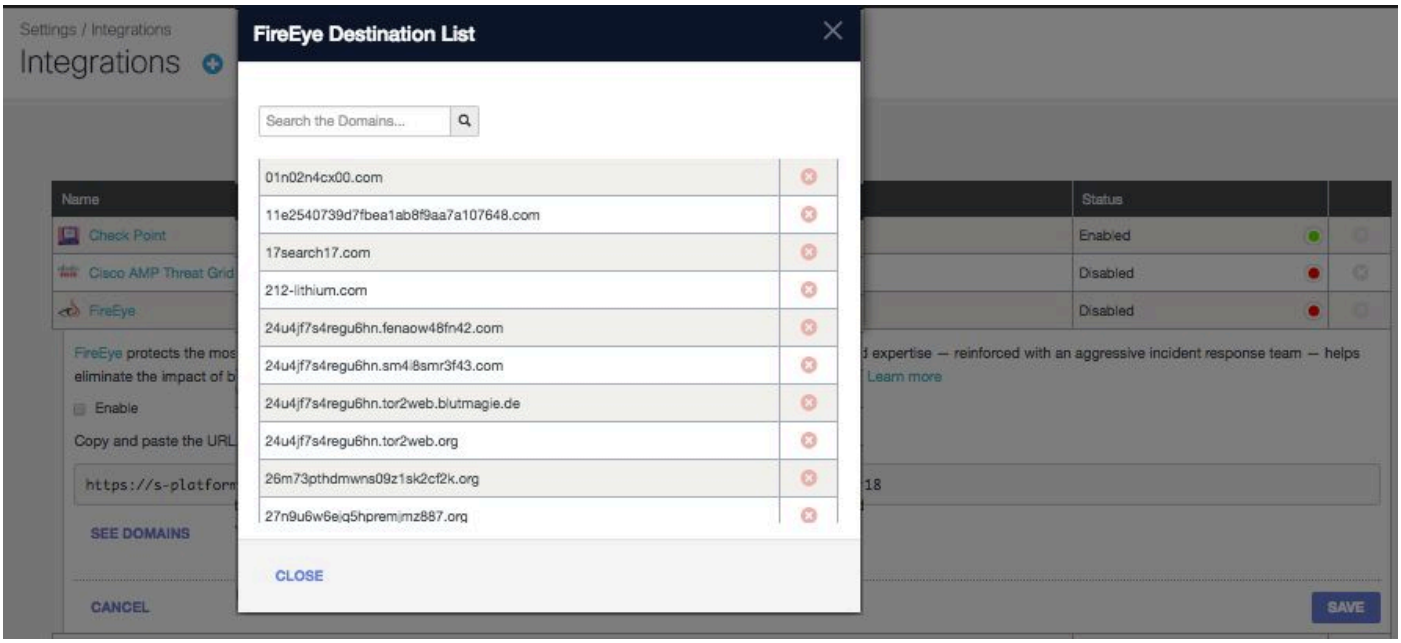
Nota: El "modo auditoría" puede activarse durante el tiempo que sea necesario en función del perfil de implementación y la configuración de red.

Revisar lista de destinos

Puede consultar la lista de destinos de FireEye en cualquier momento:

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

2. Expanda FireEye en la tabla y seleccione Ver dominios.

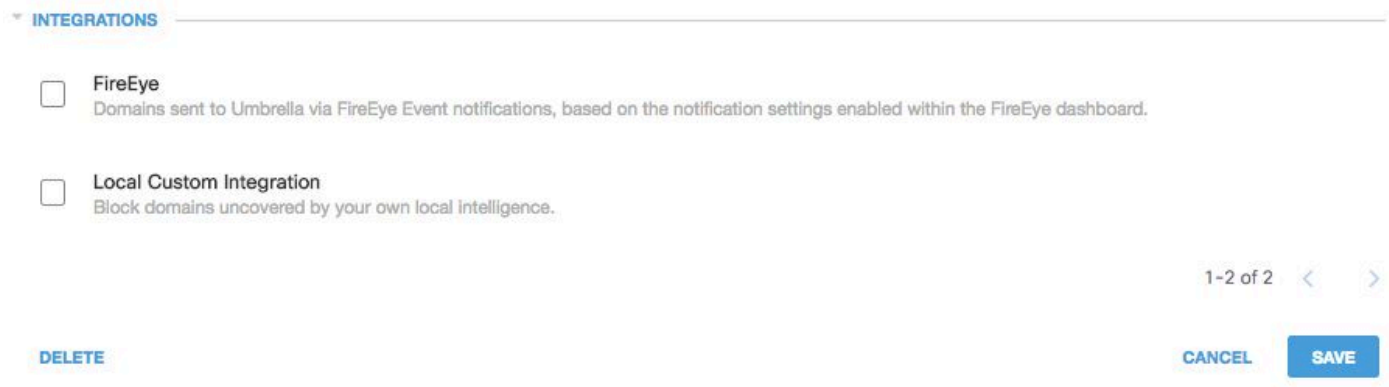


Revisar la configuración de seguridad de una directiva

Puede revisar la configuración de seguridad que se puede agregar a una directiva en cualquier momento:

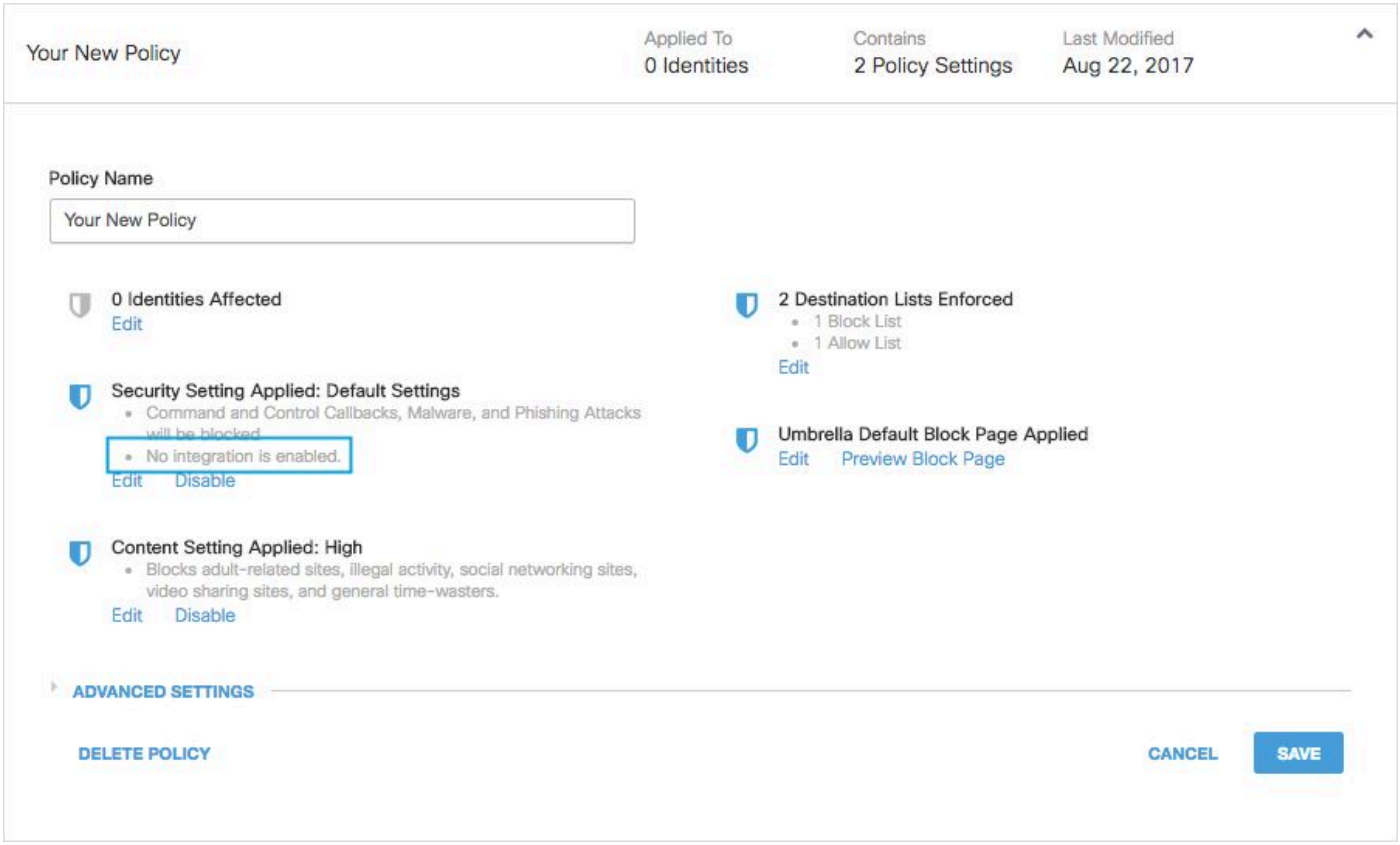
1. Vaya a Políticas > Componentes de Política > Configuración de Seguridad.

2. Seleccione una configuración de seguridad en la tabla para expandirla y desplácese hasta Integraciones para localizar la configuración de FireEye.



115014080803

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



115013920526

Al empezar, es mejor dejar esta configuración de seguridad desactivada para asegurarse de que los dominios se estén rellenando correctamente en un "modo auditoría".

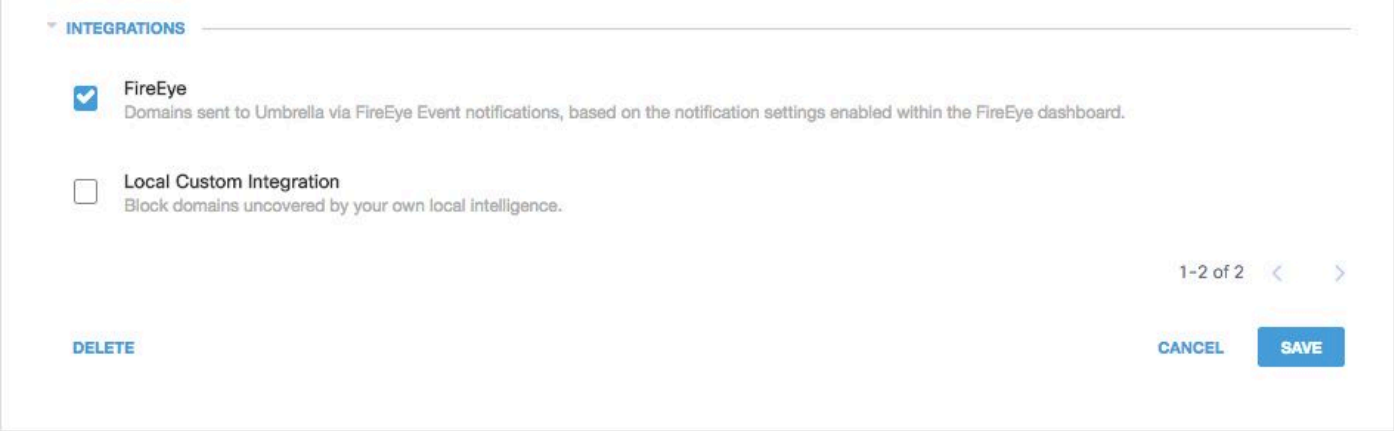
Aplicación de la configuración de seguridad de FireEye en "modo de bloqueo" a una política para clientes gestionados

Una vez que esté preparado para que los clientes que gestiona 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.

En primer lugar, cree o actualice una configuración de seguridad:

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

2. En Integraciones, seleccione FireEye y seleccione Guardar.



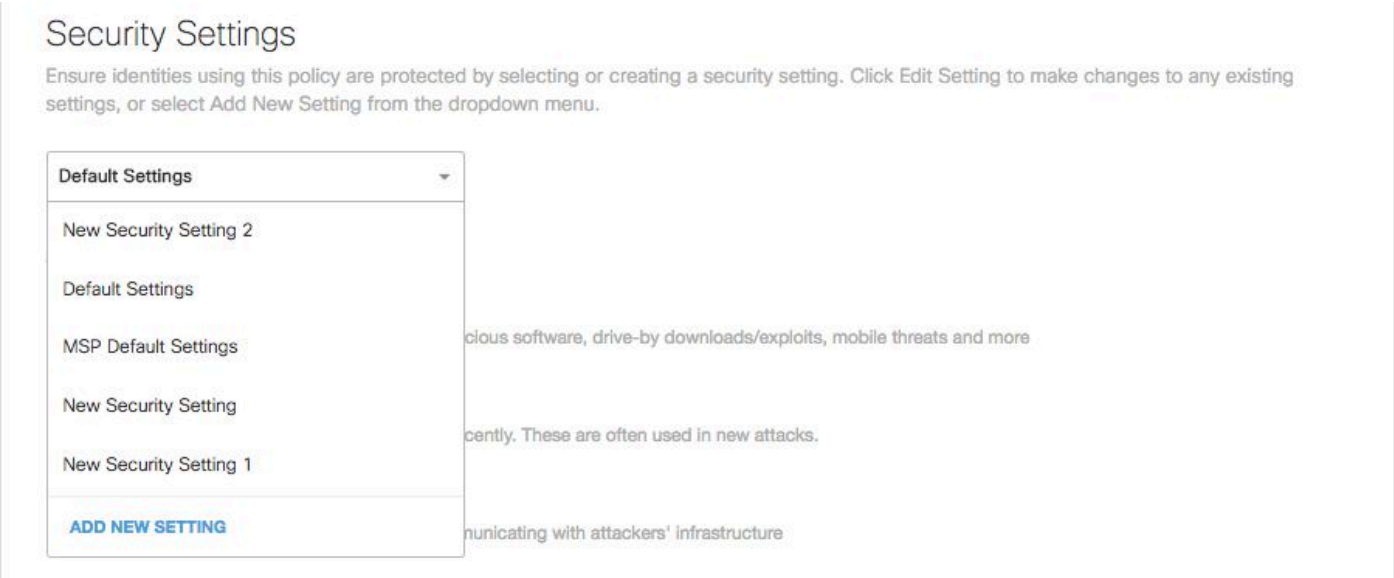
115013921406

A continuación, en el Asistente para directivas, agregue esta configuración de seguridad a la directiva que está editando:

1. Acceda a Políticas > Lista de Políticas.

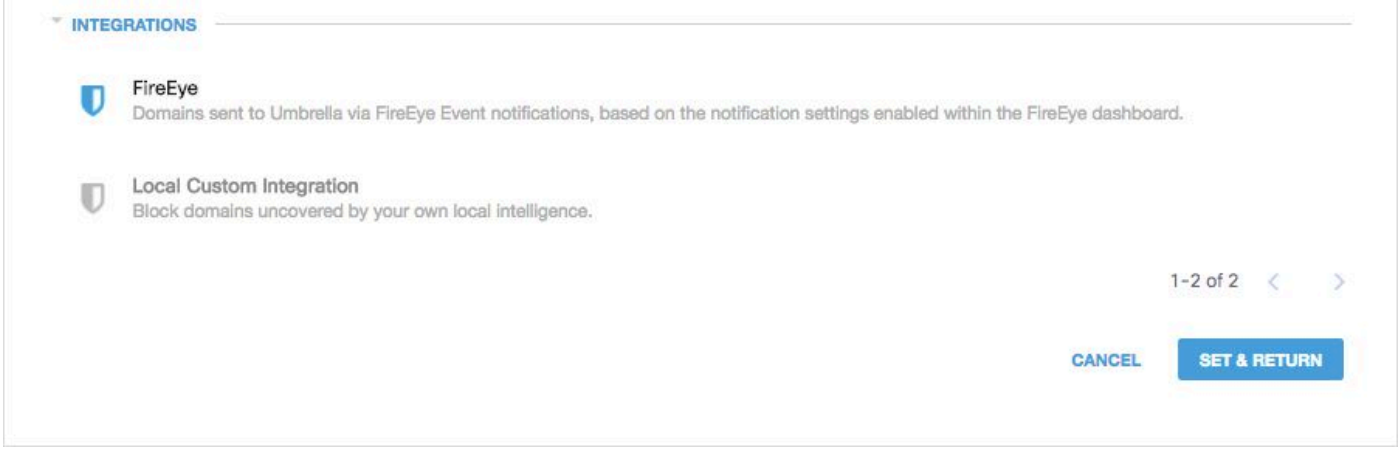
2. Expanda una política y en Configuración de seguridad aplicada y seleccione Editar.

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



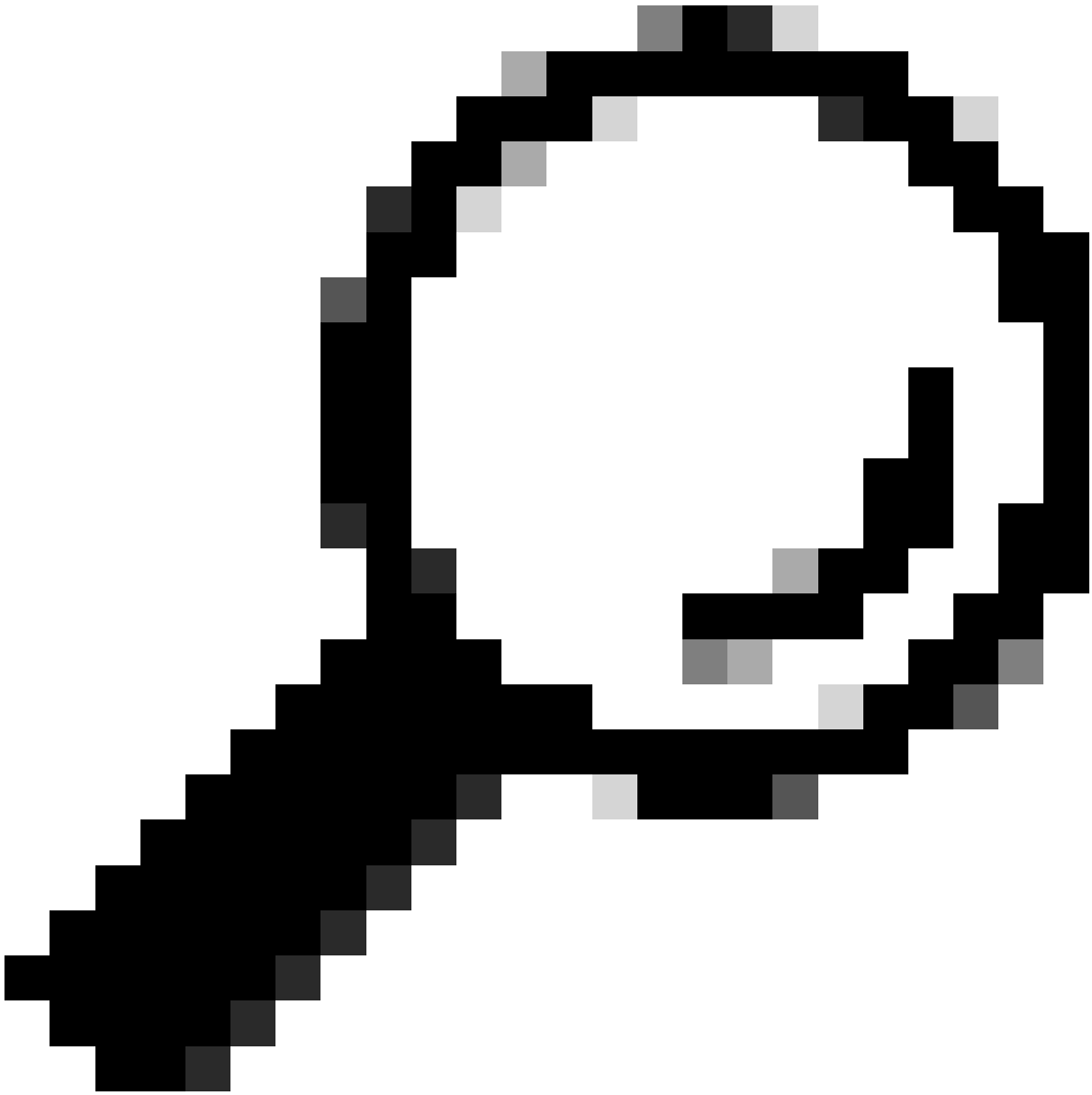
115014083083

El icono de escudo de Integraciones se actualiza a azul.



115013922146

4. Seleccione Establecer &Devolver.



Consejo: También es posible editar la configuración de seguridad desde el asistente de directivas.

Los dominios FireEye incluidos en la configuración de seguridad de FireEye se bloquean para las identidades que utilizan la política.

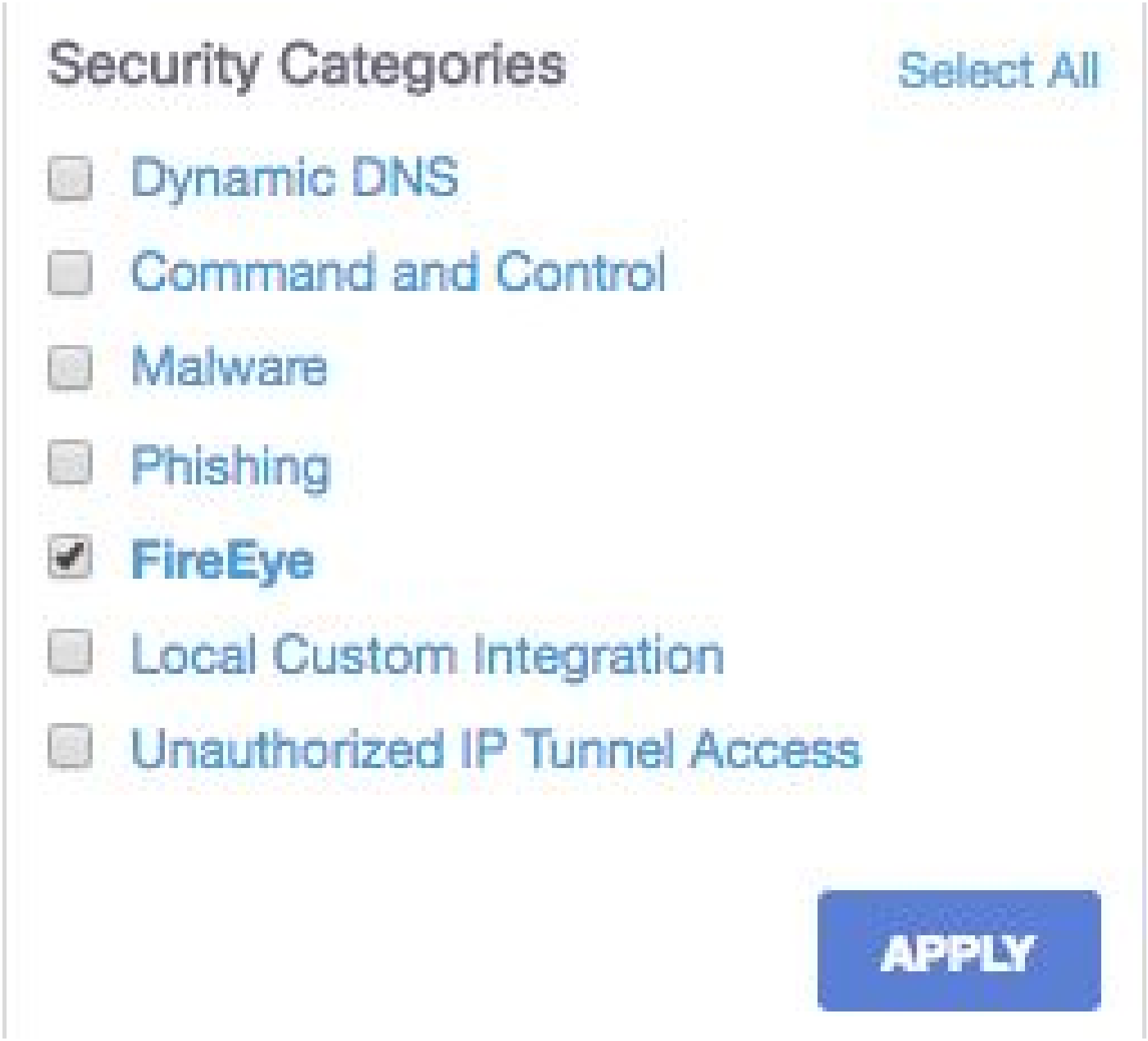
Informes en Cisco Umbrella para eventos de FireEye

Informes sobre eventos de seguridad de FireEye

La lista de destinos de FireEye 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 únicamente la actividad relacionada con FireEye:

1. Vaya a Informes > Búsqueda de actividad.

2. En Categorías de seguridad, seleccione FireEye para filtrar el informe y mostrar solo la categoría de seguridad de FireEye.



115013924986

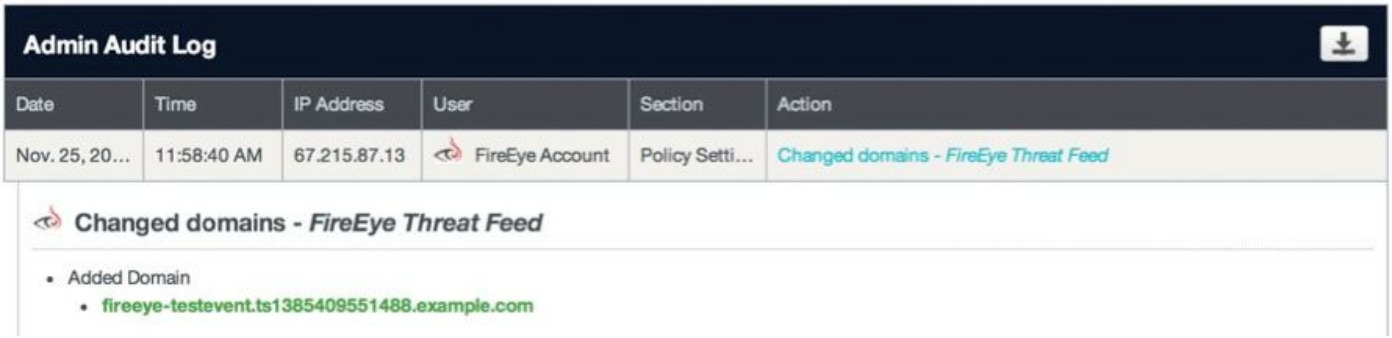
3. Seleccione Aplicar para ver la actividad relacionada con FireEye del período seleccionado en el informe.

Informes sobre cuándo se agregaron los dominios a la lista de destinos de FireEye

El registro de auditoría de administración incluye eventos del dispositivo FireEye a medida que agrega dominios a la lista de destinos. Un usuario llamado "Cuenta FireEye", que también lleva el logotipo de FireEye, genera los eventos. Estos eventos incluyen el dominio que se agregó y la hora a la que se agregó.

Puede filtrar para incluir solo los cambios de FireEye aplicando un filtro para el usuario de la cuenta de FireEye.

Si se realizó el paso anterior de "Prueba de fuego", la adición del dominio de prueba de FireEye puede aparecer en el registro de auditoría.



Gestión de detecciones no deseadas o falsos positivos

Permitir listas

Aunque es poco probable, es posible que los dominios agregados automáticamente por su dispositivo FireEye puedan activar potencialmente una detección no deseada que bloquee el acceso de los usuarios a sitios web concretos. En una situación como esta, Umbrella recomienda agregar el dominio o dominios a una lista de permitidos (Políticas > Listas de destino), que tiene prioridad sobre todos los demás tipos de listas de bloqueo, incluida la configuración de seguridad.

Hay dos razones por las que este enfoque es preferible.

- En primer lugar, en caso de que el appliance FireEye 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 que se pueden utilizar para informes de diagnóstico o auditoría.

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 FireEye en modo de bloqueo sólo se aplica a un subconjunto de las identidades administradas de Cisco Umbrella (por ejemplo, solo se aplica a equipos móviles y a dispositivos móviles), puede crear una lista de permitidos específica para dichas 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 de destinos, 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 FireEye

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

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

Para eliminar un dominio:

1. Navegue hasta Configuraciones > Integraciones, luego seleccione "FireEye" 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.

En el caso de una detección no deseada o un falso positivo, Umbrella recomienda crear una lista de permitidos en Cisco Umbrella inmediatamente y, a continuación, remediar el falso positivo dentro del appliance FireEye. Posteriormente, puede eliminar el dominio de la lista de destinos de FireEye.

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).