Descripción de las nuevas funciones de Umbrella Dashboard

Contenido

Introducción

Este documento describe la inspección de archivos y el bloqueo de URL personalizado a través de listas de destino en el Panel de Umbrella.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en el panel de Umbrella.

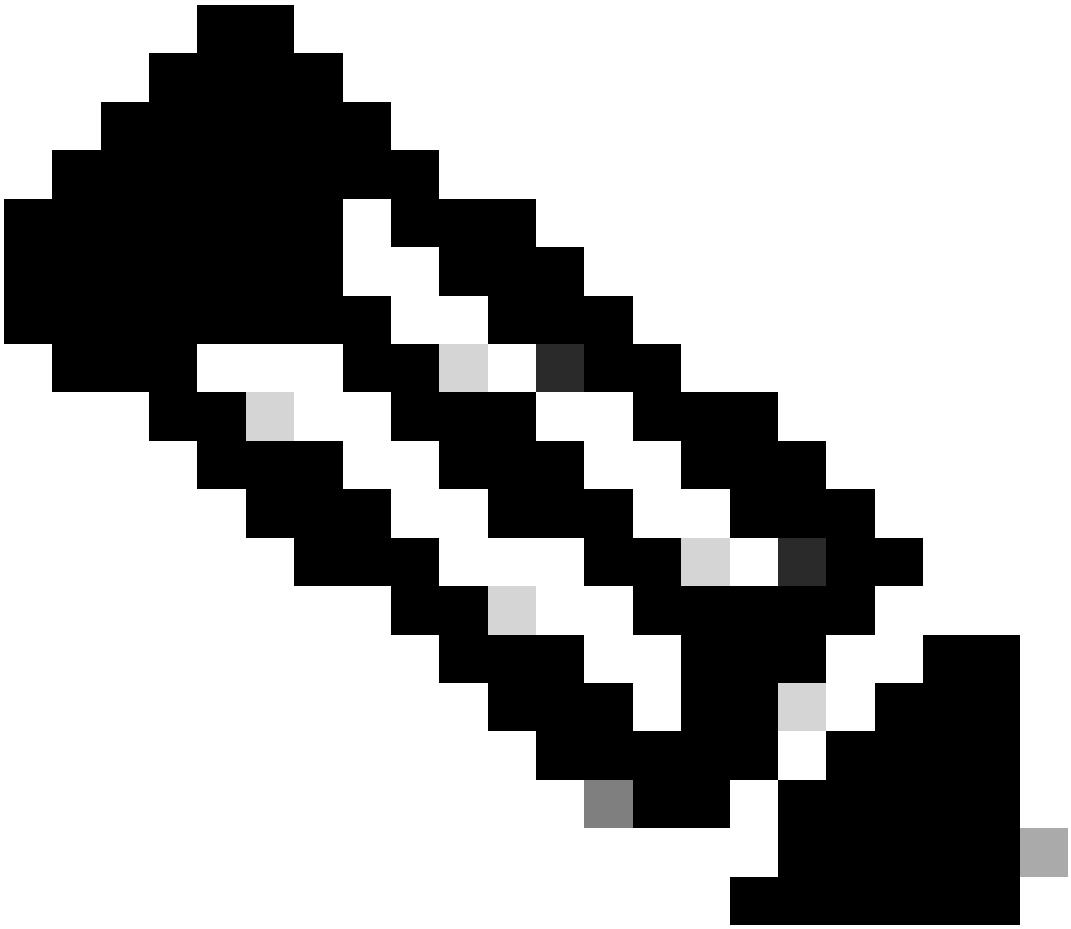
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Características nuevas

Umbrella presenta un nuevo conjunto de funciones que mejora su funcionalidad. Con este cambio, puedes ver dos nuevas funciones en tu panel ahora mismo:

- La inspección de archivos analiza los archivos que descargan sus identidades para ver si contienen código malintencionado y bloquearlos si lo tienen.
- Las URL bloqueadas personalizadas le permiten bloquear su propio conjunto de URL en una lista de destinos. Esto ahora le da la flexibilidad de bloquear páginas específicas sin bloquear dominios completos.

Para ayudarle a aprovechar esta nueva función, puede utilizar los informes nuevos y actualizados, así como una nueva experiencia de creación de políticas. La función de inspección de archivos es una de las varias funciones planificadas para futuras versiones que se han creado para hacer avanzar la infraestructura de proxy inteligente con el fin de ofrecerle aún más seguridad basada en la nube.



Nota: Estas funciones se están implementando en pequeños incrementos para nuestros clientes y estas actualizaciones tienen una disponibilidad limitada a medida que Umbrella avanza con esta versión. Si ha recibido una alerta en su panel sobre estas funciones, ya las tiene. Si desea obtener más información sobre estas funciones, póngase en contacto con umbrella-support@cisco.com.

La función de inspección de archivos solo está disponible para los clientes que dispongan de los paquetes Umbrella Insights o Umbrella Platform. Obtenga más información sobre los paquetes y póngase en contacto con su representante de cuentas de Cisco si tiene alguna pregunta.

Cómo aprovechar estas funciones

El acceso a estas nuevas funciones está disponible en un par de ubicaciones: el asistente de directivas le permite activar la inspección de archivos desde la página de resumen y, mediante las listas de destinos, puede agregar direcciones URL personalizadas a las listas de destinos bloqueados. Además, el bloqueo de URL personalizado también se puede administrar específicamente desde la página de administración Listas de destino.

En el lado de los informes, la sección de navegación de informes del panel de Umbrella se ha actualizado para que pueda encontrar fácilmente los informes nuevos y actualizados. Puede obtener más información en este artículo sobre cómo habilitar estas funciones y consultar algunos informes.

Inspección de archivos

La inspección de archivos es una función del proxy inteligente que amplía su alcance y funcionalidad al añadir la capacidad de analizar archivos en busca de contenido malintencionado alojado en dominios sospechosos. Un dominio sospechoso no es de confianza ni se sabe que es malicioso.

Con el asistente de políticas de Umbrella, la inspección de archivos es fácil de implementar. Navegue hasta Políticas > Lista de políticas y expanda una política o seleccione el icono + (Agregar) para crear una nueva política. En el asistente de directivas, asegúrese de que la opción Inspección de archivos esté habilitada en la página de resumen o, desde una nueva directiva, seleccione Inspeccionar archivos después de habilitar el Proxy inteligente (en Configuración avanzada). Puede obtener más información en la documentación completa de esta función.

Prueba de inspección de archivos

Desde un dispositivo inscrito en una política con la inspección de archivos habilitada:

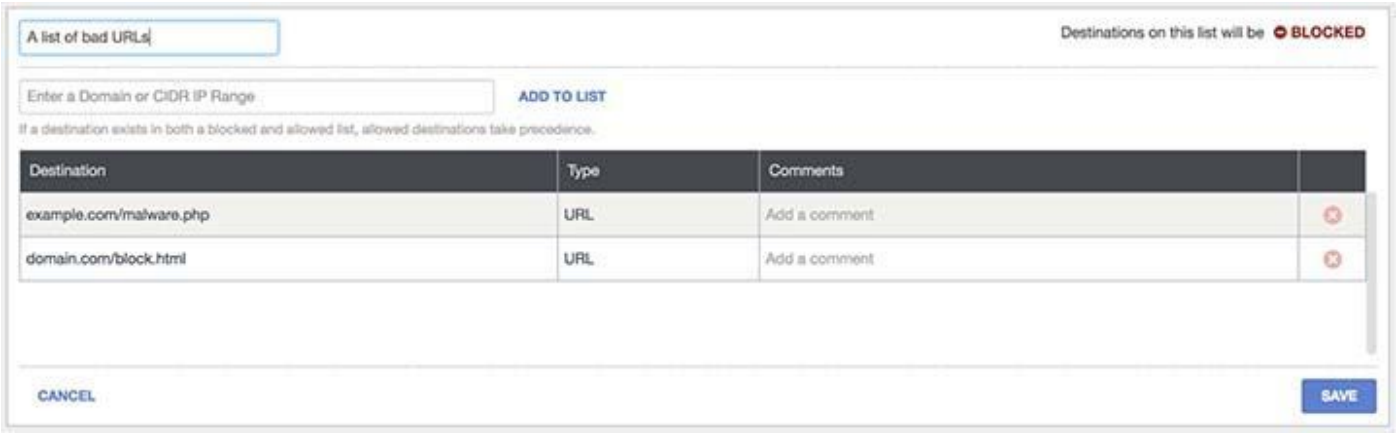
1. Vaya a http://proxy.opendnstest.com/download/eicar.com.

2. Aparecerá una página de bloqueo como esta captura de pantalla.

Página bloqueada de Umbrella

Activar el bloqueo de URL en las listas de destino

Para bloquear una URL, simplemente introdúzcala en una lista de destinos bloqueados o cree una nueva lista de destinos bloqueados solo para URL. Para ello, navegue hasta Políticas > Listas de destino, expanda una lista de Destino, agregue una URL y, a continuación, seleccione Guardar.



Lista de destinos bloqueados de paraguas

Puede obtener más información en la documentación completa de esta función.

Para que la infraestructura de Umbrella inspeccione una URL para determinar si coincide con las definidas en su lista de destinos bloqueados, debe tener lo siguiente:

- El proxy inteligente y el descifrado SSL deben estar habilitados como parte de la política.

Para obtener más información, lea los documentos de Umbrella.
- La CA raíz de Cisco Umbrella debe estar instalada en los equipos que utilicen esta directiva; además, garantiza que las conexiones https también se filtren. Para obtener más información, lea los documentos de Umbrella.

Es importante especificar una dirección URL correctamente para que la información de la política coincida con la que el usuario intenta acceder (y, por tanto, se bloquea). Para obtener más información sobre qué URL puede o no puede utilizar, lea Cómo usar la lista de destinos de URL personalizados.

Informes

Umbrella ahora tiene informes nuevos y mejorados:

- El informe de descripción general de la seguridad: ofrece una instantánea fácil de leer de la actividad de la red a través de gráficos. Puede ver rápidamente la actividad de sus identidades y su tráfico, lo que ilustra dónde pueden estar ocurriendo los problemas. Obtenga más información al respecto en los documentos de Umbrella.
- El informe de actividad de seguridad: resalta los eventos de seguridad marcados, pero no bloqueados necesariamente, por la inteligencia de amenazas de Umbrella. Esto incluye los eventos de seguridad filtrados a través del proxy inteligente y la inspección de archivos. Obtenga más información al respecto en los documentos de Umbrella.

- Informe de búsqueda de actividad: le ayuda a encontrar el resultado de cada solicitud de DNS, URL e IP de sus diversas identidades, ordenadas por fecha y hora descendentes. Este informe puede enumerar toda la actividad relacionada con la seguridad dentro de Umbrella durante el período de tiempo seleccionado y le permite refinar su búsqueda usando filtros para ver sólo lo que desea ver. Obtenga más información al respecto en los documentos de Umbrella.

Estos informes también son fáciles de obtener.

Enviando comentarios de paraguas

A Umbrella le encantaría escuchar lo que piensas sobre estas nuevas características. Cualquier pregunta o comentario que tenga, Umbrella quiere saber de usted! Envíe sus comentarios a umbrella-support@cisco.com e incluya tantos detalles como sea posible. Por ejemplo, capturas de pantalla, el navegador que está utilizando, su sistema operativo y el escenario en el que está utilizando estas funciones.

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).