Configurar el Inspector de archivos para permitir archivos protegidos por contraseña y otros archivos no malintencionados

Contenido

Introducción

Este documento describe cómo evitar que un archivo no malintencionado sea bloqueado por la inspección de archivos.

Problema

Si se activa la "inspección de archivos", en algunos casos se bloquearán los archivos no malintencionados. Estos tipos de archivos incluyen:

- Archivos protegidos por contraseña
- Archivos de aplicaciones potencialmente no deseadas (dañados)

Umbrella bloquea estos archivos porque no pueden ser descomprimidos y analizados por nuestra herramienta antivirus. Los archivos protegidos por contraseña pueden aparecer bloqueados en la categoría "Archivo protegido". Los archivos dañados podrían incluir archivos con contenido cifrado, con contenido archivado que no se puede extraer, con datos comprimidos no válidos o un encabezado de archivo no válido, o simplemente comprimidos o archivados en un formato no compatible. Aunque estos archivos pueden no ser maliciosos, Umbrella los bloquea de forma predeterminada como medida de precaución, ya que los archivos no se pueden analizar.

Solución

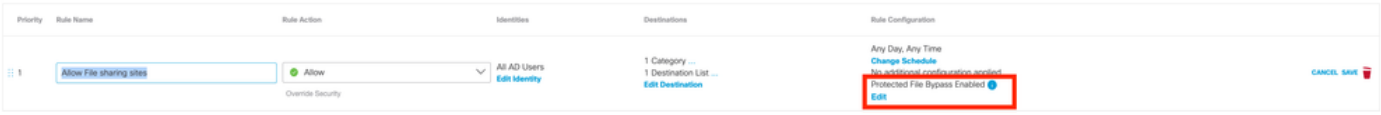
Si sabe de un archivo no malintencionado que se ha bloqueado por uno de los motivos anteriores, puede evitar esto permitiendo Archivos protegidos. El comportamiento de bloqueo de archivos protegidos ahora se puede cambiar a nivel global o en una regla web individual.

- Regla (recomendada): permite archivos protegidos para una identidad o un destino. Haga esto si desea confiar en archivos protegidos de un destino determinado o si desea anular el comportamiento de un usuario o grupo individual.
- Global: permite archivos protegidos para todos los usuarios de todas las reglas/conjuntos de

reglas. Haga esto si acepta el riesgo de descargas de archivos protegidos y prefiere esta opción sobre la carga administrativa de hacer excepciones más granulares.

Regla

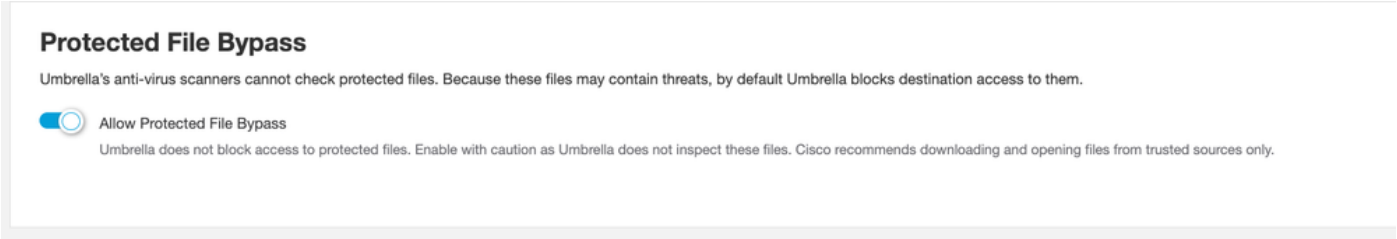
La funcionalidad se puede cambiar editando una regla web en la página Políticas > Políticas web.



10588971481748

Global

La funcionalidad se puede cambiar en Políticas > Políticas web > Configuración global.

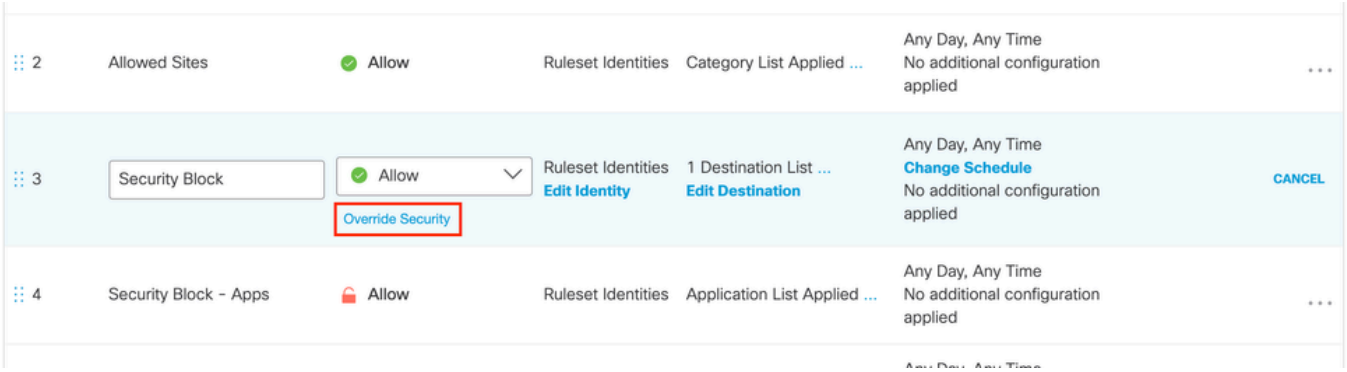


10589018672020

Solución alternativa

También es posible evitar problemas con la inspección de archivos mediante la opción Override Security en cualquier política web. Esta opción se debe utilizar con precaución, ya que deshabilita todas las demás configuraciones de seguridad, incluido el bloqueo de archivos maliciosos.

- Para archivos protegidos, utilice en su lugar una de las soluciones descritas en este documento.
- Utilice esto solo en circunstancias en las que confíe en el destino con absoluta certeza y no tenga otra opción para solucionar el problema.
- En el caso de falsos positivos de antivirus, obtenga confirmación de que el archivo está limpio de Cisco Talos antes de implementar soluciones alternativas.



Screen_Shot_2021-10-07_at_2.59.04_PM.png

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).