Comprender las limitaciones de Umbrella DNS Policy Tester

Contenido

Introducción

Este documento describe las restricciones y limitaciones de Umbrella DNS Policy Tester.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Gateway web seguro
- Gateway de Internet seguro
- Paraguas (capa DNS añadida)

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

El Umbrella Policy Tester se puede utilizar para determinar si un destino determinado puede ser

bloqueado o permitido por Cisco cuando es visitado por una identidad determinada. Sin embargo, hay algunas circunstancias en las que el Policy Tester actualmente no puede devolver información precisa (o alguna) para un destino determinado. En este artículo se describen estas restricciones.

Detalles técnicos

La descripción general de Policy Tester se puede encontrar en la documentación de Umbrella para Umbrella Policy Tester.

Estos resultados de Policy Tester pueden ser incorrectos:

Gateway web seguro

- No admitido

Gateway de Internet seguro

- No admitido

Paraguas (capa DNS añadida)

- El Policy Tester puede informar incorrectamente de los destinos bloqueados por el proxy inteligente como "permitidos". Esto también incluye:
  - Listas de bloqueo de URL personalizadas
  - Dominios de lista de bloqueo de proxy o de lista gris
  - Bloques de inspección de archivos
- El Policy Tester puede informar incorrectamente de que el tipo de destino "Aplicación" (como Dropbox, Box, Facebook, etc. por nombre) bloqueada es "Permitida".
- Cuando una red también se aplica a una política web, la política web puede mostrarse incorrectamente. En este momento, el polítómetro no es compatible con las redes que también forman parte de las políticas web.
- Las pruebas que no proporcionan toda la información de identidad relevante pueden mostrar resultados incorrectos. Por ejemplo, un equipo móvil con la integración de Active Directory (AD) activada mientras se encuentra en una red protegida: la prueba puede fallar si sólo se proporciona el usuario de AD pero el equipo móvil gana las decisiones de directiva.
- Los destinos bloqueados debido a categorías de contenido pueden mostrarse como permitidos si se introducen con letras mayúsculas y minúsculas o se escriben en mayúsculas. Por ejemplo, si está bloqueando la categoría "desnudez", el dominio playboy.com puede mostrarse como bloqueado mientras que Playboy.com aparece como permitido.
- Los destinos de "DNS dinámico" se pueden bloquear si se selecciona la categoría de seguridad, pero el Policy Tester puede informar incorrectamente de que la categoría de "permitidos".
- Los destinos permitidos por el control de aplicaciones pueden mostrarse incorrectamente como bloqueados en el Policy Tester.
- El Policy Tester puede informar incorrectamente de los destinos bloqueados por la API de

Umbrella Enforcement para integraciones personalizadas como "permitidos".

- Los destinos bloqueados por la integración de Umbrella AMP Threat Grid se pueden notificar de forma incorrecta como "permitidos" por el Policy Tester.
- El Policy Tester puede informar incorrectamente de los destinos bloqueados debido a un CNAME como "permitidos".
- Los destinos que son direcciones IP no se soportan en el Policy Tester en este momento.
- Los destinos que son URLs no son compatibles conPolicy Tester en este momento.
- El Policy Tester puede informar incorrectamente de que los destinos bloqueados para la resolución a una IP malintencionada están "permitidos".
- Los destinos "potencialmente dañinos" se pueden bloquear si se selecciona la categoría de seguridad, pero el Policy Tester puede informar incorrectamente de que la categoría de seguridad está "permitida".
- Los destinos en los que las protecciones DDOS automatizadas impiden temporalmente que DNS responda al dominio afectado no son visibles para Policy Tester.
- Los destinos bloqueados en la categoría de contenido "Protección juvenil alemana" pueden ser informados incorrectamente como "Permitidos" por el Policy Tester. Esta categoría no se puede mencionar en los resultados de Policy Tester.
- Los destinos bloqueados debido a la clasificación de seguridad "Criptomoneda" pueden aparecer incorrectamente como "Permitidos" incluso cuando los bloquean las opciones de seguridad.
- Los bloqueos debidos a categorías VPN de tunelización DNS no pueden mostrar correctamente los resultados en el Policy Tester. Aparecen incorrectamente como permitidos.
- Los dispositivos Chromebook detrás de un dispositivo virtual pueden mostrar una política incorrecta. Los bloques de identidad de Chromebook (UCC) pueden anular las políticas aplicadas de Virtual Appliance, pero los bloques de Virtual Appliance pueden anular las políticas de UCC.
- Los miembros de los grupos AD en los que el grupo no se sincroniza con Umbrella (incluidos los grupos que forman parte de un dominio principal o secundario y los grupos que son miembros de grupos que no se sincronizan selectivamente con Umbrella) pueden mostrarse como coincidentes con la política mostrada en el Policy Tester. La política de usuario no se puede aplicar en la nube. Confirme agregando el usuario único a su política y confirme que se aplica correctamente en 5 minutos.
- Destinos que se encuentran en la lista Dominios internos. El Policy Tester no toma la lista de Dominios Internos cuando informa un resultado de prueba.
- No se garantiza que las categorías que no aparecen en el sitio de etiquetado de dominios de la comunidad OpenDNS muestren la categoría correcta en el Policy Tester. Sólo se representa una fuente de categorías.
- Policy Tester se limita a mostrar 20 resultados al buscar una identidad.
- Un usuario de AD es miembro de un grupo de AD anidado, pero solo se selecciona el grupo de AD principal en las identidades al crear la política DNS. La búsqueda de Policy Tester puede no coincidir con la política correcta.
- El Policy Tester puede informar incorrectamente de los destinos de la lista de permitidos protegidos como "bloqueados".

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).