Configuración de Umbrella para bloquear Tor

Contenido

Introducción

Este documento describe cómo bloquear Tor con Umbrella.

Overview

La red Tor utiliza relés operados por voluntarios para alojar una red distribuida y anónima. Garantiza que ningún punto único pueda vincular a un usuario con su destino, con el objetivo de reducir los riesgos del análisis del tráfico. Aunque Tor tiene muchos usos legítimos, hay razones para que un administrador de red quiera bloquear todo el tráfico basado en Tor en una red corporativa.

En resumen, no es posible bloquear completamente Tor con Umbrella. Al bloquear la categoría Proxy/Anonymizer, torproject.org se bloquea; sin embargo, es posible que los dispositivos propiedad de los usuarios ya tengan instalado el navegador Tor y lo traigan a la red.

Explicación

Tor actúa como un proxy. Después de abrir una conexión TCP, se envía una carga útil que codifica la dirección y el puerto del host de destino al nodo de salida. Al recibir esto, el nodo de salida resuelve la dirección según sea necesario.

Lea esto para obtener información adicional que debe tener en cuenta:

- Los servicios Tor onion utilizan el TLD .onion, que no es reconocido por los servidores DNS raíz. Se requiere Tor para acceder a los dominios .onion.
- La manera más común de bloquear el tráfico Tor sería localizar una lista actualizada de nodos de salida Tor y configurar un firewall para bloquear estos nodos. Una política de la compañía para evitar el uso de Tor también puede ayudar mucho a dejar de usarlo.
- Desafortunadamente, las configuraciones individuales no son algo que OpenDNS/Cisco Umbrella pueda ayudar a soportar, ya que cada firewall tiene una interfaz de configuración única y estas varían enormemente. Si no está seguro, consulte la documentación del router o del firewall o póngase en contacto con el fabricante para ver si es posible.

Vea las Preguntas Frecuentes sobre Abuso del Proyecto Tor para obtener más información sobre el bloqueo de Tor. Las Preguntas Frecuentes vinculadas son principalmente para proveedores de

servicios que desean bloquear el acceso de los usuarios de Tor a su servicio, pero también contienen enlaces útiles para administradores de red.

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).