

Configurar Umbrella para bloquear Tor

Contents

[Introdução](#)

[Overview](#)

[Explicação](#)

Introdução

Este documento descreve como bloquear o Tor com o Umbrella.

Overview

A rede Tor usa relés operados por voluntários para hospedar uma rede distribuída e anônima. Ele garante que nenhum ponto possa ligar um usuário ao seu destino, com o objetivo de reduzir os riscos da análise de tráfego. Embora o Tor tenha muitos usos legítimos, há razões para um administrador de rede querer bloquear todo o tráfego baseado em Tor em uma rede corporativa.

Em suma, não é possível bloquear completamente Tor com Umbrella. Ao bloquear a categoria Proxy/Anonymizer, torproject.org é bloqueado; no entanto, os dispositivos de usuários podem já ter o navegador Tor instalado e trazê-lo para a rede.

Explicação

Tor atua como um proxy. Depois de abrir uma conexão TCP, um payload codificando o endereço e a porta do host destino é enviado para o nó de saída. Ao receber isso, o nó de saída resolve o endereço conforme necessário.

Leia este texto para obter mais informações a serem lembradas:

- Os serviços Tor onion usam o TLD .onion, que não é reconhecido pelos servidores DNS raiz. Tor é necessário para acessar domínios .onion.
- A maneira mais comum de bloquear o tráfego Tor seria localizar uma lista de atualização de nós de saída Tor e configurar um firewall para bloquear esses nós. Uma política da empresa para evitar o uso de Tor também pode fazer um longo caminho para cessar seu uso.
- Infelizmente, as configurações individuais não são algo que o OpenDNS/Cisco Umbrella pode ajudar no suporte, pois cada firewall tem uma interface de configuração exclusiva e elas variam muito. Se não tiver certeza, verifique a documentação do roteador ou firewall ou entre em contato com o fabricante para ver se isso é possível.

Veja a [FAQ do Abuso do Projeto Tor](#) para mais informações sobre o bloqueio do Tor. A FAQ ligada é principalmente para provedores de serviços que querem bloquear o acesso dos usuários do Tor aos seus serviços, mas também contém links úteis para administradores de rede.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.