Configurer le parapluie pour bloquer Tor

Table des matières

Introduction

Ce document décrit comment bloquer Tor avec Umbrella.

Aperçu

Le réseau Tor utilise des relais gérés par des volontaires pour héberger un réseau distribué et anonyme. Elle garantit qu'aucun point unique ne peut relier un utilisateur à sa destination, dans le but de réduire les risques liés à l'analyse du trafic. Bien que Tor ait de nombreuses utilisations légitimes, il y a des raisons pour qu'un administrateur réseau veuille bloquer tout le trafic basé sur Tor sur un réseau d'entreprise.

En bref, il n'est pas possible de bloquer complètement Tor avec Umbrella. Lorsque vous bloquez la catégorie Proxy/Anonymizer, torproject.org est bloqué ; cependant, les appareils appartenant à l'utilisateur peuvent déjà avoir le navigateur Tor installé et l'amener sur le réseau.

Explication

Tor agit comme un proxy. Après l’ouverture d’une connexion TCP, une charge utile codant l’adresse et le port de l’hôte de destination est envoyée au noeud de sortie. À la réception de ce message, le noeud de sortie résout l’adresse si nécessaire.

Lisez ceci pour plus d'informations à garder à l'esprit :

- Les services Tor onion utilisent le TLD .onion, qui n'est pas reconnu par les serveurs DNS racine. Tor est nécessaire pour accéder aux domaines .onion.
- La façon la plus courante de bloquer le trafic Tor serait de localiser une liste de mise à jour des noeuds de sortie Tor et de configurer un pare-feu pour bloquer ces noeuds. Une politique de l'entreprise pour empêcher l'utilisation de Tor peut également faire beaucoup pour cesser son utilisation.
- Malheureusement, les configurations individuelles ne sont pas prises en charge par OpenDNS/Cisco Umbrella, car chaque pare-feu dispose d'une interface de configuration unique, qui varie considérablement. Si vous avez des doutes, vous pouvez consulter la documentation de votre routeur ou de votre pare-feu ou contacter le fabricant pour savoir si cela est possible.

Voir la FAQ sur les abus du projet Tor pour plus d'informations sur le blocage de Tor. La FAQ liée est principalement destinée aux fournisseurs de services qui veulent bloquer l'accès des utilisateurs de Tor à leur service, mais contient aussi des liens utiles pour les administrateurs réseau.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.