Paraplu configureren om Tor te blokkeren

Inhoud

Inleiding

In dit document wordt beschreven hoe u Tor kunt blokkeren met Umbrella.

Overzicht

Het Tor-netwerk maakt gebruik van door vrijwilligers bediende relais om een gedistribueerd, anoniem netwerk te hosten. Het zorgt ervoor dat geen enkel punt een gebruiker kan koppelen aan zijn bestemming, met als doel de risico's van verkeersanalyse te verminderen. Hoewel Tor veel legitieme toepassingen heeft, zijn er redenen voor een netwerkbeheerder om al het op Tor gebaseerde verkeer op een bedrijfsnetwerk te willen blokkeren.

Kortom, het is niet mogelijk om Tor volledig te blokkeren met Umbrella. Wanneer u de categorie Proxy/Anonymizer blokkeert, wordt torproject.org geblokkeerd. Mogelijk is de Tor-browser echter al geïnstalleerd op apparaten die eigendom zijn van de gebruiker en wordt deze naar het netwerk gebracht.

verklaring

Tor fungeert als een proxy. Na het openen van een TCP-verbinding wordt een payload die het adres en de poort van de bestemmingshost codeert, naar het afsluitknooppunt verzonden. Na ontvangst van deze, de exit node lost het adres als nodig.

Lees dit voor aanvullende informatie om in gedachten te houden:

- Tor onion-services gebruiken het .onion TLD, dat niet wordt herkend door de root-DNS-servers. Tor heeft toegang tot .onion domeinen.
- De meest gebruikelijke manier om Tor-verkeer te blokkeren, is door een updatelijst van Tor-afsluitknooppunten te zoeken en een firewall te configureren om deze knooppunten te blokkeren. Een bedrijfsbeleid om het gebruik van Tor te voorkomen, kan ook een lange weg afleggen om het gebruik ervan te staken.
- Helaas zijn individuele configuraties niet iets dat OpenDNS / Cisco Umbrella kan ondersteunen, omdat elke firewall een unieke configuratie-interface heeft en deze sterk variëren. Als u niet zeker bent, kunt u de documentatie van uw router of firewall controleren of contact opnemen met de fabrikant om te zien of dit mogelijk is.

Zie de veelgestelde vragen over misbruik van Tor Project voor meer informatie over het blokkeren van Tor. De gekoppelde FAQ is vooral bedoeld voor serviceproviders die Tor-gebruikers willen blokkeren om toegang te krijgen tot hun service, maar bevat ook nuttige links voor netwerkbeheerders.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.