将Umbrella配置为阻止Tor

目录

简介

本文档介绍如何使用Umbrella阻止Tor。

概述

Tor网络使用志愿者操作的中继来托管一个分布式匿名网络。它确保没有任何单点能够将用户链接到其目的地，目的是降低流量分析的风险。虽然Tor有许多合法用途，但网络管理员有理由希望阻止企业网络上所有基于Tor的流量。

简而言之，不可能使用Umbrella完全阻塞Tor。当阻止代理/匿名器类别时，会阻止torproject.org;但是，用户自有设备可能已经安装了Tor浏览器并将其引入网络。

说明

Tor充当代理。打开TCP连接后，会将编码目的主机地址和端口的负载发送到送出节点。收到此信息后，送出节点会根据需要解析地址。

请阅读本文，了解更多要牢记的信息：

- Tor onion服务使用.onion TLD，根DNS服务器无法识别该TLD。必须使用Tor来访问.onion域。
- 阻止Tor流量的最常见方法是查找Tor送出节点的更新列表并配置防火墙以阻止这些节点。公司禁止Tor使用的政策也可以大大减少其使用。
- 遗憾的是，OpenDNS/Cisco Umbrella无法帮助支持单个配置，因为每个防火墙都有唯一的配置接口，而且这些接口差异很大。如果您不确定，可以查阅路由器或防火墙文档或联系制造商以了解是否有可能做到这一点。

有关阻止Tor的更多信息，请参阅Tor项目的滥用常见问题。链接的常见问题大多数针对想要阻止Tor用户访问其服务的服务提供商，但也包含对网络管理员有用的链接。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。