將Umbrella配置為阻止Tor

目錄

簡介

本文描述如何使用Umbrella阻止Tor。

概觀

Tor網路使用志願者操作的中繼來託管一個分散的匿名網路。它確保沒有單點可以將使用者連結到其目的地，目標是降低流量分析的風險。雖然Tor有許多合法用途，但網路管理員仍有理由阻止公司網路上所有基於Tor的流量。

簡而言之，無法使用Umbrella完全封鎖Tor。阻止代理/匿名程式類別時，會阻止torproject.org;但是，使用者擁有的裝置可能已經安裝了Tor瀏覽器並將其引入網路。

說明

Tor是代理。開啟TCP連線後，將編碼目的主機地址和埠的負載傳送到退出節點。收到此地址後，退出節點會根據需要解析該地址。

請閱讀本文，瞭解要牢記的其他資訊：

- Tor onion服務使用.onion TLD，根DNS伺服器無法識別它。訪問.onion域需要Tor。
- 攔截Tor通訊最常見的方法是找到Tor退出節點的更新清單，並配置防火牆以攔截這些節點。公司禁止Tor使用的政策也會大大減少它的使用。
- 遺憾的是，OpenDNS/Cisco Umbrella無法幫助支援單個配置，因為每個防火牆都有唯一的配置介面，而且這些介面差異很大。如果您不確定，可以檢查您的路由器或防火牆文檔或聯絡製造商以瞭解是否可能。

有關阻止Tor的更多資訊，請參閱Tor Project的濫用常見問題。連結的常見問題大多數針對想要阻止Tor使用者訪問其服務的服務提供商，但也包含對網路管理員有用的連結。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。