Umbrella so konfigurieren, dass Tor blockiert wird

Inhalt

Einleitung

Dieses Dokument beschreibt, wie man Tor mit Umbrella blockiert.

Überblick

Das Tor-Netzwerk nutzt von Freiwilligen betriebene Relais, um ein verteiltes, anonymes Netzwerk zu hosten. Es stellt sicher, dass ein Benutzer nicht über einen einzelnen Punkt mit seinem Ziel verbunden werden kann, um die Risiken der Datenverkehrsanalyse zu reduzieren. Obwohl Tor viele legitime Nutzungen hat, gibt es Gründe für einen Netzwerkadministrator, den gesamten Tor-basierten Datenverkehr in einem Unternehmensnetzwerk blockieren zu wollen.

Kurz gesagt, es ist nicht möglich, Tor mit Umbrella komplett zu blockieren. Wenn die Kategorie Proxy/Anonymizer blockiert wird, wird torproject.org blockiert. Auf eigenen Geräten ist der Tor-Browser jedoch bereits installiert und kann in das Netzwerk integriert werden.

Erläuterung

Tor fungiert als Stellvertreter. Nach dem Öffnen einer TCP-Verbindung wird eine Nutzlast, die die Adresse und den Port des Ziel-Hosts codiert, an den Exit-Knoten gesendet. Beim Empfang löst der Exit-Knoten die Adresse nach Bedarf auf.

Hier finden Sie weitere Informationen, die Sie beachten sollten:

- Tor-Zwiebeldienste verwenden die TLD .onion, die von den Root-DNS-Servern nicht erkannt wird. Tor ist für den Zugriff auf .onion Domains erforderlich.
- Die gängigste Methode, Tor-Traffic zu blockieren, wäre eine aktualisierende Liste von Tor-Exit-Knoten zu finden und eine Firewall zu konfigurieren, um diese Knoten zu blockieren. Eine Unternehmenspolitik, die die Nutzung von Tor verhindern soll, kann ebenfalls einen großen Beitrag dazu leisten, die Nutzung von Tor einzustellen.
- Unglücklicherweise können einzelne Konfigurationen nicht von OpenDNS/Cisco Umbrella unterstützt werden, da jede Firewall über eine eigene Konfigurationsschnittstelle verfügt, die sehr unterschiedlich ist. Wenn Sie sich nicht sicher sind, können Sie die Dokumentation zu Ihrem Router oder Ihrer Firewall einsehen oder sich an den Hersteller wenden, um dies zu

überprüfen.

Weitere Informationen zum Blockieren von Tor finden Sie in der Tor Project Missuse FAQ. Der FAQ-Link ist hauptsächlich für Service Provider gedacht, die Tor-Nutzern den Zugriff auf ihren Service verweigern wollen, enthält aber auch nützliche Links für Netzwerkadministratoren.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.