TorをブロックするためのUmbrellaの設定

内容

はじめに

このドキュメントでは、UmbrellaでTorをブロックする方法について説明します。

概要

Torネットワークは、ボランティアで動作するリレーを使用して、分散された匿名ネットワークをホストします。トラフィック分析のリスクを軽減することを目的として、シングルポイントでユーザを宛先にリンクできないようにします。Torには多くの用途がありますが、ネットワーク管理者が企業ネットワーク上のすべてのTorベースのトラフィックをブロックする必要がある理由があります。

要するに、傘でTorを完全にブロックすることは不可能です。Proxy/Anonymizerカテゴリをブロックすると、torproject.orgはブロックされますが、ユーザ所有のデバイスにはTorブラウザがすでにインストールされている場合があり、それをネットワークに持ち込む可能性があります。

説明

Torはプロキシとして機能します。TCP接続をオープンした後、宛先ホストのアドレスとポートをエンコードするペイロードが出口ノードに送信されます。これを受信すると、出口ノードは必要に応じてアドレスを解決します。

次の追加情報をお読みください。

- Tor onionサービスは.onion TLDを使用しますが、これはルートDNSサーバでは認識されません。.onionドメインにアクセスするにはTorが必要です。
- Torトラフィックをブロックする最も一般的な方法は、Tor出口ノードの更新リストを検索し、これらのノードをブロックするようにファイアウォールを設定することです。Torの使用を防止するための会社のポリシーも、使用を停止するのに長い道のりを行くことができます。
- 残念ながら、個々の設定はOpenDNS/Cisco Umbrellaがサポートできる機能ではありません。各ファイアウォールには固有の設定インターフェイスがあり、これらは大きく異なるためです。確信が持てない場合は、ルータまたはファイアウォールのマニュアルを確認するか、製造元に問い合わせて確認してください。

Torをブロックする方法の詳細については、『Tor Project's Abuse FAQ』を参照してください。

リンクされているFAQは、主にTorユーザのサービスへのアクセスをブロックするサービスプロバイダー向けですが、ネットワーク管理者向けの便利なリンクも含まれています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。