Configure Umbrella to Block Tor

Contents

Introduction

This document describes how to block Tor with Umbrella.

Overview

The Tor network uses volunteer-operated relays to host a distributed, anonymous network. It ensures that no single point can link a user to their destination, with the goal of reducing the risks of traffic analysis. Although Tor has many legitimate uses, there are reasons for a network administrator to want to block all Tor-based traffic on a corporate network.

In short, it is not possible to completely block Tor with Umbrella. When blocking the Proxy/Anonymizer category, torproject.org is blocked; however, user-owned devices might already have the Tor browser installed and bring it onto the network.

Explanation

Tor acts as a proxy. After opening a TCP connection, a payload encoding the address and port of the destination host is sent to the exit node. Upon receiving this, the exit node resolves the address as necessary.

Read this for additional information to keep in mind:

- Tor onion services use the .onion TLD, which is not recognized by the root DNS servers. Tor is required to access .onion domains.
- The most common way to block Tor traffic would be to locate an updating list of Tor exit nodes and configure a firewall to block these nodes. A company policy to prevent Tor use can also go a long way to cease its use.
- Unfortunately, individual configurations are not something OpenDNS/Cisco Umbrella is able to assist in supporting, as each firewall has a unique configuration interface and these vary greatly. If you are uncertain, you can check your router or firewall documentation or contact the manufacturer to see if this is possible.

See the Tor Project's Abuse FAQ for more information on blocking Tor. The FAQ linked is mostly for service providers wanting to block Tor users from accessing their service, but also contains useful links for network administrators.