Disable Protected Networks for Umbrella Roaming Clients on Enterprise Networks

Contents

Introduction

This document describes how to disable the Umbrella roaming clients (standalone and AnyConnect) on a corporate networks and enable it off the corporate network.

Background Information

This article is targeted at administrators. If you do not desire to back off the roaming client on network, stop here.

The Umbrella protected networks feature is intended for a single egress network. For any networks with more than one egress, an alternate feature is required.

Today, this feature exists in production as the trusted network domain feature. Read on to learn how to request the feature and what is required on your network.

What Is The Trusted Network Domain Feature?

The trusted network by domain feature is a way to disable the roaming client on your corporate network, but keep it enabled off network. When activated, the feature:

- Disables DNS protection provided by the roaming client
  - Defers policy to the network policy
- Stops all network probes except the trusted network domain check
  - Great for busy networks!
  - Great alternative to the VA backoff
    - Use in conjunction with VAs for less network talk

IPv6 Behavior, Windows Versus MacOS

- On Windows, the domain is queried on IPv4 and IPv6. The shut-down behavior is handled separately on each network stack. For example, if the domain resolves on IPv4 but not IPv6, then the roaming client shuts down on IPv4 **only**, and stay operation on IPv6. If you wish to have the client shut down completely, then IPv4 **and** IPv6 queries must resolve.
- On MacOS, the domain is queried on IPv4 and IPv6. Unlike Windows, if the domain resolves on

either network stack, then the roaming client shuts down for both IPv4 and IPv6.

How Do I Enable The Feature?

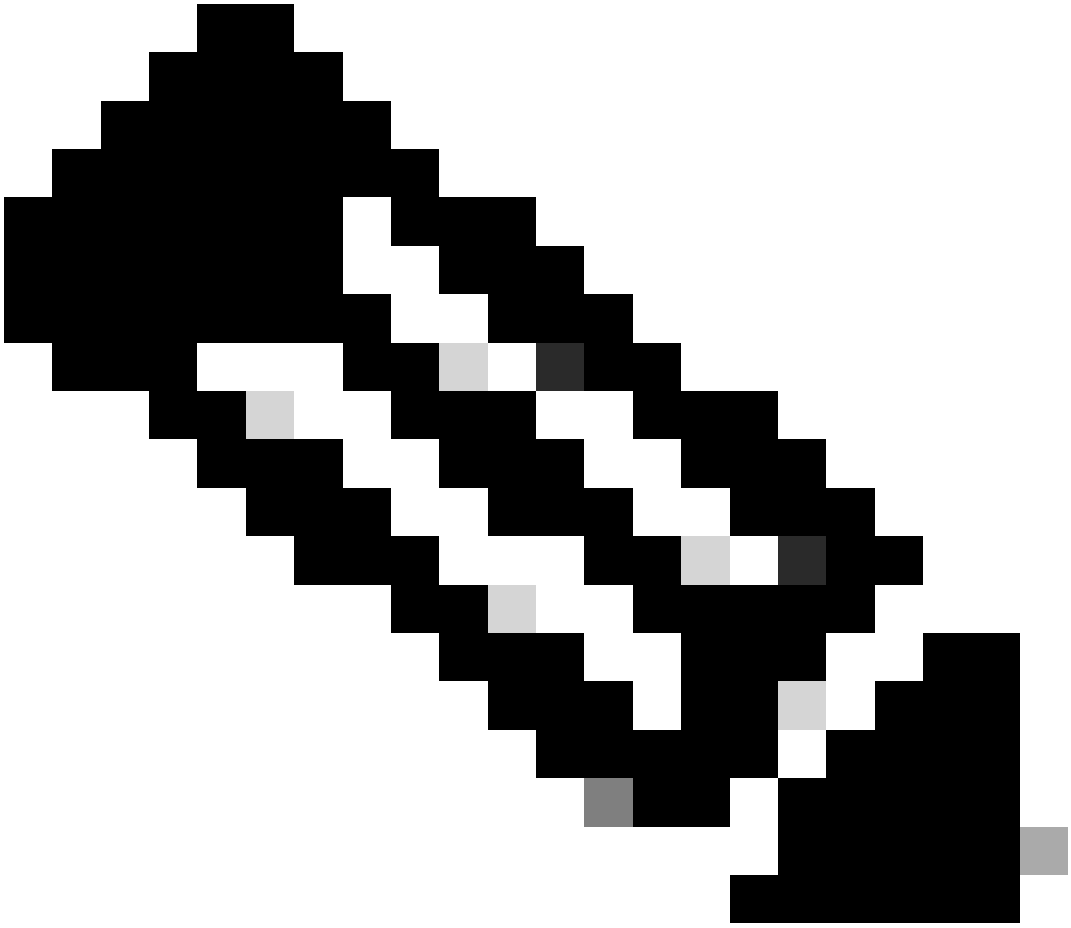
This feature is now controlled in the dashboard. Please see Roaming Computers Settings.

- The desired Umbrella disable subdomain. This domain must:
  - Have an A record that resolves to a RFC-1918 internal IP address (for IPv4)
  - Have an AAAA record that resolve to an RFC-4193 IP on IPv6 (if IPv6 is used)
    - RFC-1918 IPs typically look like 10.x.x.x, 172.x.x.x, or 192.168.x.x
    - RFC-4193 IPv6 addresses start with 'FD'
    - The IP addresses do not have to be reachable
    - Must be a subdomain
      - sub.domain.com - good!
      - subdomain.com - no good.
  - Resolve off network to NXDOMAIN, NODATA, or public IP address (so the client remains enabled in this scenarios)
    - No SERVFAIL please
  - Be a domain in a zone you control to ensure you control the public and local space
- Supports:
  - Umbrella Roaming Client
  - AnyConnect Umbrella Roaming Security Module 4.5 MR4+ only

How Do I Test the Feature For One Machine?

To test locally before having the Umbrella team apply the setting globally, apply this override.

1. Create a file "customer_network_probe.flag"
    1. Ensure the file is not .flag.txt
2. Put the desired domain into the contents of the file
3. Place the file into:
    1. Roaming client
        1. Windows: %ProgramData\OpenDNS\ERC\
    2. AnyConnect
        1. Windows: %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\data\
    3. Cisco Secure Client
        1. Windows: C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\data\
        2. macOS: /opt/cisco/secureclient/umbrella/data/
4. Restart the roaming client
    1. Roaming client: Umbrella Roaming Client: Manually Disabling or Restarting.
    2. AnyConnect: Restart the parent vpnagent AnyConnect service



Note: MacOS Roaming client, AnyConnect versions do not support this flag.