Enable Tunnel All DNS for Secure Client with Umbrella Module

Contents

Introduction

Background Information

Problem and Impact

Recommendation

Introduction

This document describes how to enable tunnel all DNS for Cisco Secure Client with Umbrella module.

Background Information

Cisco announced the End-of-Life of Cisco AnyConnect in 2023 and the Umbrella Roaming Client in 2024. Many Cisco Umbrella customers are already benefiting from migrating to Cisco Secure Client, and you are encouraged to begin migration as soon as possible to get a better roaming experience. Read more in this Knowledge Base article: How do I install Cisco Secure Client with the Umbrella Module?

The Cisco Secure Client (CSC) with Umbrella (formerly AnyConnect Roaming Security) module is designed to work with almost all CSC VPN modes with no extra configuration required.

However, additional consideration when these conditions are both true:

- **Split Tunnelling** is enabled
- The **"Tunnel All DNS"** feature is enabled

Problem and Impact

With "Tunnel All DNS" enabled, DNS traffic is intercepted at the kernel level and blocked if it is not going out of the correct VPN interface. This introduces a problem for the CSC module if Cisco Umbrella resolvers are not part of the Split Tunnel (Include) configuration.

The impact of this problem is minimal because by default, the CSC module uses encrypted DNS (UDP port 443) which is not blocked by "Tunnel All DNS". Therefore, the problem only occurs on networks where DNS encryption is not available.

The scenario is as follows:

- The Roaming Module attempts to route traffic to Cisco Umbrella via the normal LAN interface.
- The Local Network does not allow DNS encryption and therefore sends standard unencrypted DNS queries.
- This traffic is blocked by the "Tunnel All DNS" feature which requires DNS to go down the VPN.

In this scenario, DNS does not function as expected.

Recommendation

To ensure this condition is not possible, Cisco Umbrella recommends one of these actions.

- Disable "Tunnel All DNS" in the VPN group policy. The CSC module handles the routing of DNS.
  OR
- Add these Cisco Umbrella DNS resolvers to the Split Tunnel (Include) configuration:
  - 208.67.222.222
  - 208.67.220.220
  - 208.67.222.220
  - 208.67.220.222