Resolve DNS Penalization in MacOS and Access Issue with Internal Domains

Contents

Introduction

This document describes how to solve a problem with newer versions of MacOS Big Sur that impacts DNS resolution.

Background Information

Scope

- AnyConnect Roaming Security Module or Umbrella on network (such as VA or forwarding)
  - Umbrella standalone roaming client not affected. Single-DNS environment is present where all DNS is overwritten with 127.0.0.1).
- Occurs in environments with multiple network interfaces, but only one can resolve internal addresses. For example:
  - VPN and off-VPN
  - Multiple NIC - one corporate and one non-corporate

Symptoms

- Inability (or intermittent ability) to access local domains while retaining ability to access public domains
  - nslookup is not specifically not affected and continues to function
    - ping, traceroute, etc resolves incorrectly or not find the internal domain

Problem

This issue is caused by code in MacOS that handles the way DNS resolutions are managed in the presence of multiple DNS servers. These can be multiple resolvers on a single network adaptor or multiple resolvers across different network adaptors. A DNS server that responds with REFUSED is "penalized" for 60 seconds. When this happens, any further DNS queries that occur during this time period is tried on alternate DNS servers that are not penalized.

For example, if DHCP advertises two DNS servers for a network, A and B, and A responds with REFUSED, then B is favored over A for 60 seconds so long as B is not penalized.

If all DNS servers are penalized, then MacOS favors the least recently penalized server. For example, if B becomes penalized while A was already penalized, then MacOS favors A over B.

This is compounded by the way MacOS 11 and higher try to assert DoH (DNS over HTTPS). MacOS is programmed to prefer a user set DoH provider when possible. This would circumvent Umbrella DNS security, which means we return a REFUSED response (as per RFC) when MacOS initiates a DoH request. Because of DNS Penalization, this can result in internal domains not being resolved correctly. For more information on this issue, see this article: DNS Resolver Selection in iOS 14 and macOS 11.

Solution

We are not yet aware if Apple plans to change this behavior or if Umbrella is able to change their behavior to work around this issue. For the time being, there are two options that serves as work arounds:

Option 1

Enable split-DNS in the group policy and specifically add the internal domains to the split-DNS configuration so that they are only resolvable over tunnel. This ensures that those domains are only resolvable over tunnel by the native OS resolver, whereas any other domains are only resolvable outside tunnel.

Option 2

Enable tunnel-all-DNS in the group policy to prevent any DNS traffic from going outside the tunnel.