Configure Umbrella and BlueCoat Webfilter/K9

Contents

Introduction

This document describes how to configure compatibility between the Umbrella roaming client and BlueCoat Webfilter/K9.

Overview

This article refers to computers where the Umbrella roaming Client and BlueCoat are installed. This article refers to the use of a BlueCoat filtering agent installed on a the machine. This might coincide with a PAC or proxy configuration.

The Umbrella roaming client and Umbrella Roaming Security Module in AnyConnect are currently not compatible with BlueCoat software-based filtering which attempts to control DNS.

Impacted software:

- Cisco AnyConnect Umbrella Roaming Security Module
- Umbrella Roaming Client

Symptoms

AnyConnect Roaming Module and roaming client older than 2.2.150

When the roaming client or roaming module is active, all DNS appear to fail. This causes an apparent loss of usability on the machine and a loss of the ability to access web resources. More specifically, any DNS requests to an A record fails; however, other record types such as AAAA or TXT succeeds.

When the roaming client is uninstalled or temporarily stopped, normal network behavior returns.

The roaming client does not recognize DNS is failing since only A records fail, and therefore the client remains active and encrypted.

Roaming client 2.2.150 and newer

When the roaming client is active, the client fails over into an open state with the message

"we have detected potential interference with A and/or AAAA DNS queries; there may be some software on the system that is causing problems"

This is a new detection method for software that overrides A-Records but does not modify TXT records. We flag this behavior and disable to prevent loss of DNS.

Troubleshooting

To validate if you are currently observing this issue, confirm these are true:

- These scenarios result in failing DNS (or A-record mode disable)
  - BlueCoat active and:
    - Roaming client or module protected and encrypted
    - Roaming client or module protected and unencrypted
  - BlueCoat process manually killed (not uninstalled). Redirection is active, but the underlying proxy is offline.
    - Roaming client or module protected
    - Roaming client uninstalled or stopped
- These result in no issue
  - The roaming client or module active with BlueCoat uninstalled (after a reboot)
  - The BlueCoat web filter installed and no roaming client running

When DNS is failing, all A records fail, but TXT records continue to not be redirected by BlueCoat and function.

Root Cause and Solution

The root cause of this compatibility issue is twofold.

1. The BlueCoat software redirects A record queries (the most common DNS records for viewing web pages) so that only it can answer these queries. This DNS can leave the network, but it is prevented from responding to the system. The roaming client has no way to override this.
2. The roaming client determines DNS availability by checking TXT record responses which are unique to the Umbrella resolvers. Since BlueCoat is not enforcing TXT records, the roaming client's tests continue to succeed even after all A records begin to fail. This A record failure and TXT record success causes the roaming client to stay encrypted, effectively perpetuating a broken state with the BlueCoat software.

The BlueCoat's selective DNS proxy enforcement at a low level in the system causes a direct compatibility issue with the roaming client. The user impact is a loss of DNS and web browsing ability based on DNS.

The only solution at this time is to cease the use of the BlueCoat workstation software that redirects DNS and instead utilize Umbrella-based content restrictions. BlueCoat can add an ability to disable DNS enforcement at a future time.