Troubleshoot Compatibility Between Netskope and Umbrella Roaming Client

Contents

Introduction

Overview

Impact

Resolution: Bypass Roaming Client from Proxy

Introduction

This document describes how to troubleshoot compatibility issues between Netskope and the Umbrella roaming client.

Overview

This KBA is targeted at users of the Netskope proxy who are experiencing an issue where the roaming client fails to sync with the Umbrella Dashboard. This results in the roaming client failing to correctly activate on network. This article discusses excluding our syncs from Netskope proxying.

This information applies to roaming clients on both Windows and MacOS.

Impact

When SSL is tunneled through the Netskope proxy, directing SSL traffic to Netskope servers, the roaming client is not able to sync successfully with Umbrella. This causes it to remain in an unprotected unencrypted state. In some cases, the client can go encrypted prior to the first sync which results in a known issue resulting in a failure to resolve internal domains (that are not on the local DNS search suffix list).

Several native apps behave with Netskope as if they are certificate pinned, resulting in 3rd party certificates not being accepted. This pinning occurs as a result of the .NET crypto framework utilized by the roaming client.

Resolution: Bypass Roaming Client from Proxy

The solution is to exclude the roaming client's service process from being directed through Netskope's proxy via its "Certificate Pinned Applications" feature.

Applications, if defined, allows blocking or bypassing an app. **If you select Bypass (required for roaming client sync), the Netskope client does not steer traffic from the end point to the Netskope proxy in the cloud and apps continue to work.** If you select Block, traffic is blocked by the Netskope client. By default all apps are bypassed, but the required setting is to bypass the roaming client's service.

To edit Certificate Pinned Applications and add the Umbrella roaming client service, use these steps:

1. Navigate to **Settings > Manage > Certificate Pinned Applications > Advanced Settings**. The Advanced Settings window is displayed.

2. In the Advanced Settings window, select Custom Settings for Each Application. Use these sub-steps to add a custom service/application
    - Under the Application list select Microsoft Office 365 Outlook.com (there is no Umbrella option, this allows us to move forward) and for Action, select Bypass.
    - For Mode, select Direct.
    - In the Plugin Process field, enter “ercservice.exe” for the standalone roaming client. For the AnyConnect roaming module, enter "acumbrellaplugin.exe".
3. Click **Submit**. The Advanced Settings closes.
4. On the client machine, restart the Netskope agent to pull these new settings right away. (Normally the client updates within an hour as the clients contact Netskope for updates.)

Advanced Settings do exist. Either scenario is believed to work; however, Bypass + direct is recommended.

1. Bypass + Direct: Selecting this means, bypass the configured apps/domains from the client. It does not travel to Netskope.
2. Bypass + Tunnel: Selecting this means, the client tunnels the traffic from apps/domains but Netskope proxy bypasses it. This option is useful for domains associated with an SSO authentication service because these services use the source IP of the Netskope cloud to determine if access to the cloud app is protected by Netskope.