Troubleshoot Connection to Hotspots via Captive Portal with AnyConnect SWG Module Enabled

Contents

Introduction

This document describes troubleshooting connections to hotspots via Captive Portal with AnyConnect SWG module enabled.

Problem

Users with the AnyConnect Secure Web Gateway (SWG) module might have trouble signing in at some public hotspot locations.

Fixes and Recommendations for Further Troubleshooting

Ensure that you are using AnyConnect version 4.10.05095(4.10MR5). Issues concerning captive portal are addressed in this version.

However, if the issue still persists even after upgrading to 4.10.05095 then please reach out to Umbrella Support.

In order to expedite the support process we ask customers to go through these steps and collect the requested logs before reaching out to Umbrella Support.

1. We request customers configure all security agents installed on their endpoints to exclude AnyConnect binaries and connections to avoid conflict of policies. Hence, TrendMicro and/or any other security agent needs to be configured accordingly.
   Plase refer to the relevant snippet from the AnyConnect release notes and make sure the exceptions for AnyConnect are made accordingly.
2. Visit both HTTP (for example, http://www.portquiz.net) and HTTPS (https://www.google.com) URLs in the browser and see if the redirection to the captive portal happens or not.
3. If the issue still persists, please collect a DART bundle (max debug enabled), PCAP file (including loopback), and a screen recording (optional) to investigate further.

Configuring Antivirus Applications for AnyConnect

Applications like antivirus, antimalware, and Intrusion Prevention System (IPS) can misinterpret the behavior of AnyConnect Secure Mobility Client applications as malicious. You can configure exceptions to

avoid such misinterpretation. After installing the AnyConnect modules or packages, configure your antivirus software to allow the AnyConnect Installation folder or make security exceptions for the AnyConnect applications. The common directories to exclude are listed, although the list might not be complete:

- C:\Users<user>\AppData\Local\Cisco
- C:\ProgramData\Cisco
- C:\Program Files x86)\Cisco

Details

Captive Portal issues can be caused by CSCwb39828 "Captive Portal page did not open when SWG is enabled for both fail open/fail close". After upgrading to AnyConnect 4.10.05095 later, no additional configuration or user interaction is necessary.

Some wireless hotspots and other guest networks interrupt Internet access and redirect web traffic to a captive portal (sometimes called a walled garden). AnyConnect SWG versions prior to 4.10.05095 might attempt to send this web traffic to the Umbrella cloud even if Internet access is unavailable, which prevents the system from locally interacting with the captive portal. This local interaction might be required to grant access through authentication, payment, or a click-through agreement page.

Versions Prior to 4.10.05095

Support is limited for captive portals with earlier versions of AnyConnect when using SWG. These actions of a captive portal likely make it unreachable to a SWG client:

- Redirecting to, or loading of assets from, a destination outside of the RFC-1918 private IP address space.
- Accepting a TCP handshake for Umbrella proxies on port 80 or 443 and then closing the connection or providing an unexpected response.

As a workaround, add exceptions in the Deployments --> Domain Management --> External Domains & IPs section of the Umbrella Dashboard, for any destination that fails to load. Captive portal behavior is implementation-specific, so the required redirect domain(s) or IP addresses varies with each hotspot.