Troubleshoot Captive Portal Interaction with Umbrella Roaming Client

Contents

Introduction

Overview

Expected Behaviors and Scenarios

- Cisco Security Connector (CSC)
- Third-party DNS Blocked
- Third-party DNS Redirected
  - Third-party DNS Allowed

Introduction

This document describes captive portal interations with the Umbrella roaming client.

Overview

Captive portals are the common name for public or "as-a-service" Internet Connections which require payment, authentication, or terms of service/acceptable use policy (TOS/AUP) acceptance before allowing connectivity to a device.

Captive portals are typically seen in airports, hotels, coffee shops or really anywhere which gratis or paid wifi is offered. You might also see them in guest wifi networks in corporate or school environments.

A captive portal usually presents itself as a "gate" or pop-up in the browser wherein action is required by the end-user to provide credentials, payment, or accept the terms of service in order to reach the internet. Until the captive portal is cleared, the user is unable to browse any resource besides those within the subnet that the portal exists in.

Expected Behaviors and Scenarios

Most captive portals redirect all browser requests (HTTP/HTTPS) to its local web portal. The local web portal is usually IP-based and not DNS-based. This means that there are no behavioral issues caused when using the Umbrella roaming client on a computer which is connecting to a captive portal.

In the rare case where a captive portal uses DNS in some way to facilitate its service, this behavior occurs before completing the requirements of the captive portal (payment, TOS/AUP acceptance, etc).]

DNS-based captive portals might only be able to redirect HTTP queries without failure. Modern browsers automatically handle known requests like google.com to be https://www.google.com/which might break some captive portals. Try using Apple's captive portal check site to access the captive portal login page which is http only. To do so, visit http://captive.apple.com.

Cisco Security Connector (CSC)

Just like the roaming client, the CSC remains protected and encrypted if UDP 443 is allowed behind a captive portal. This results in local DNS to the captive portal failing to resolve to the local result. **Therefore, to access the captive portal, a domain on the internal domains list must be visited for these semi-captive portals.**

To allow iOS automatic captive portal detection to function:

- Add these to the internal domains list
  - captive.apple.com
  - www.airport.us
  - www.thinkdifferent.us

Third-party DNS Blocked

If the captive portal is blocking DNS requests destined for Umbrella, DNS connectivity is blocked for approximately six seconds by the Umbrella roaming client. After six seconds, the Umbrella roaming client transitions to the Unprotected/Unencrypted state until it can again communicate with Umbrella.

Third-party DNS Redirected

If the captive portal is redirecting DNS requests destined for Umbrella, DNS connectivity is blocked for approximately two to six seconds by the Umbrella roaming client. After this time, the Umbrella roaming client transitions to the Unprotected/Unencrypted state until it can again communicate with Umbrella.

Third-party DNS Allowed

If the captive portal is not manipulating or blocking DNS requests destined for Umbrella, the Umbrella roaming client works as intended and might result in bypassing the login portion of the captive portal completely.

Solution: Visit a domain on your internal domains list. This allows for captive portal redirection even when third party DNS is allowed. **Do this when the roaming client remains in a protected state behind a captive portal.**