Understand Umbrella Roaming Client and F5 VPN Compatibility

Contents

Introduction

This document describes compatibility between the Cisco Umbrella Roaming Client and F5 VPN.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella Roaming Client.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Introduction

The Umbrella roaming client can be used in a wide variety of network and software configurations. This article documents all known compatibility topics with the F5 VPN client. This article begins with the current expected detection behaviors and then discusses F5 VPN specific compatibility notes.

The Umbrella client has implemented automated detection mechanisms to react to VPN changes to ensure that DNS functionality is maintained. This can cause the client to temporarily remain unprotected while the VPN is connected. Please refer to the article Third-Party VPN Detection Heuristics with the Umbrella Roaming Client for more details.

F5 VPN Compatibility

In many configurations, F5 VPN functions by inserting the VPN DNS addresses to non-VPN NICs by pre-pending the VPN servers to the NIC's DNS. So, for a local DNS configuration of x.x.x.x and a VPN configuration of y.y.y.y, the result is y.y.y.y, x.x.x.x.

With the Umbrella roaming client, this overrides the 127.0.0.1 placed. To ensure that F5 VPN is not impaired with an endless change loop, Umbrella stops redirecting if 127.0.0.1 is placed at the end of the DNS list or is rapidly changed back away from 127.0.0.1.

In most cases, Umbrella recommends the use of the Umbrella roaming security module that is part of the AnyConnect roaming security client. VPN is not required to be deployed (it can be removed from display to the user at the time of install).

F5 compatibility at this time is defined as a successful F5 VPN connection with fully functional local and public DNS. This can be as a result of a graceful backoff by the roaming client into an unprotected state. Please ensure that your on-network coverage is in place while using F5 by configuring your network for Cisco Umbrella.

BigIP F5 VPN Client

The BigIP F5 edge client is the most common F5 VPN client at this time. However, it is being replaced with the new F5 client in many deployments. This article discusses all known interoperability concerns with the F5 BigIP client.

F5 DNS Relay Proxy

The roaming client is not compatible with VPN client 2.2+ in configurations that activate the F5 DNS Relay Proxy service. This relay proxy is known to activate in split-dns mode and DNS-based split tunneling modes. F5 cannot be used with DNS names defined with the roaming client To use split tunneling with F5 and the roaming client at this time, use IP-based split tunneling rather than DNS based split tunneling. Additionally, some configurations and versions can result in Umbrella being overridden despite showing green when the DNS Relay Proxy is activated.

Find the split-dns or DNS-Based Split Tunneling Setting

F5 VPN Split Tunneling with split-dns appears in the form of the "DNS Address Space" setting. When active, this spins up F5's own DNS proxy which conflicts with the roaming client. The symptom is a failure to resolve A-records while both the roaming client and the VPN is active. See this screenshot for a working configuration:

Client Settings: Advanced ▼

Traffic Options	○ Force all traffic through tunnel ◉ Use split tunneling for traffic
IPV4 LAN Address Space	IP Address Mask Add 0.0.0.0/0.0.0.0 Edit Delete
DNS Address Space	DNS Add Edit Delete
IPV4 Exclude Address Space	IP Address Mask Add Edit Delete
DNS Exclude Address Space	DNS Add

Ensure this is empty!