Understand Known Limitations with CDFW/SL VPN Tunnel

Contents

Introduction

This document describes known limitations with Cisco Umbrella cloud-delivered firewall (CDFW)/SL VPN tunnel.

Overview

Umbrella's cloud-delivered firewall (CDFW) provides firewall services without the need to deploy, maintain and upgrade physical or virtual appliances at each site. Umbrella’s CDFW also provides visibility and control for internet traffic across all branch offices. However, there are a few known limitations with CDFW.

Explanation

- IPSEC traffic over CDFW tunnel is not supported, but does support SSL/TLS tunnels over CDFW. SSL over IPSec is supported in CDFW, however, Umbrella forwards that to SWG and it drops that. Umbrella is planning to build a feature that allows admins to bypass SWG by Destination IP address.
- Each tunnel is limited to approximately 250 Mbps throughput per tunnel.
- IP Fragmentation is not supported with CDFW.
- Using SWG PAC File with CDFW is not supported.
- Only TCP, UDP and ICMP are supported. Others are dropped.*
  *traceroute in ICMP is not fully visible though the Umbrella infrastructure.
- NAT does not support pin-holing or inbound (towards branch) ports. So Active FTP is not supported, only Passive FTP. There is no capability to statically open inbound ports either.
- Only 1 child SA is supported today.
- Path MTU Discovery (PMTUD) is not supported in the CDFW Tunnel.
- Pings can be dropped if multiple devices are sending to the same destination.