IPv6-only Remote Access VPN "A road less travelled"

Zsolt Horvath, Senior Service Engineer

Remote Access Engineering, CCE

Microsoft CSEO

April 2019

Disambiguation page

- Zsolt Horvath (zshorvat@microsoft.com)
  - Network Security Engineer, 2x CCIE
  - Supporting and managing remote access VPN solutions for 10+ years
  - Cloud and Connectivity Engineering (CCE) is not Azure ☺
- IPv6-only Remote Access VPN
  - Through the tunnel traffic is purely IPv6
  - Tunnel termination must remain dual stack
- The presentation is not endorsed by Palo Alto Networks
  - It is simply about our own experience using their product

The v6 route looks straightforward on the map

- IPv4 address space to be depleted in the foreseeable future on the internal network
- Most of the network has been dual-stack for quite some time
- Project for deploying NAT64 & DNS64 across the globe is underway
- Easy to find pockets in the network that could be turned into IPv6-only:
  - Corporate Wi-Fi
  - *Remote Access VPN*

The new motor seems perfect for the drive

- Brand new next-gen SSL VPN appliances supporting up to 30K/60K(!) users each, depending on the model
- Redundant 10G/40G design in 15 locations around the world
- Both *outside* and *inside* are dual-stack already from drawing board
- PAN-OS 8.0 promised supporting IPv6 for VPN clients

The first stop: garage

- In PAN-OS 8.0 and 8.1 the VPN gateway didn't allow removing the IPv4 pool!
  - There were IPv4-based dependencies under the hood in both the client and the server software
  - Temporary workaround: use 169.254.0.0/16 as your IPv4 VPN pool ☺
- Additional complication:
  - The Linux workaround with OpenConnect (allowing SAML authentication) uses only the v4 address even when dual stacked

Full servicing under warranty

- Early vendor engagement brought a good result
  - Palo Alto Networks took our request seriously and brought out the missing features super fast, so we started beta-testing end of 2018 (original ETA was summer 2019!)
- Latest production code (9.0/5.0) includes IPv6-only VPN, tested in our lab on:
  - Server side
  - Windows/MacOS/native Linux client (SAML support is being worked on)
- Something is still missing:
  - *Windows 10 VPN Platform* doesn't support IPv6-only VPN for UWP clients aka VPN provider plugins from Windows Store – we are expecting that this fix will get released shortly

On the road again

- After the successful lab testing, soon we can start a *User Acceptance Test (UAT)* with swapping out the original DNS servers with DNS64 (in locations where NAT64 & DNS64 is deployed)
  - This should reduce IPv4 traffic close to zero,
  - Catch flows that are using hardcoded IPv4 addresses,
  - Catch applications that are not IPv6 compatible.
- After the UAT, we can remove the IPv4 pool from non-Windows clients first
- Once Windows 10 VPN Platform is ready, we can pull the IPv4 addresses from all remaining clients
- Repeat the same change in all new sites where NAT64 & DNS64 gets deployed

Avoiding potholes

- Let's look at VPN, DNS and DNS64 a little closer:
  - By default DNS64 will respond all AAAA queries, essentially turning on full tunneling while we must do split-tunneling
- Must enforce split-DNS, i.e. resolve only *interesting (i.e. internal) suffixes* with DNS64
  - PAN-OS has a feature called DNS proxy that can be used for desktop clients
  - In case of UWP the client is using NRPT policies, so it was never affected

Driving into the sunset