Microsoft Always-On VPN: A Seamless VPN Experience for Users?

John Perkins
Computer Systems Lab - Computer Sciences Department
IT Professionals Conference May 31, 2018
Goals

• Automatic VPN initiation/drop during undock/dock
• VPN connection live when booted remotely
• Allow current redirected desktop and other folders to function as users expect
Potential Solutions

• Campus Departmental VPN
• Microsoft Direct Access
• Microsoft Remote Access VPN
Campus Departmental VPN

• Advantage: already running

• Disadvantages:
  • Requires additional 3\textsuperscript{rd} party software component
  • Requires action from the user to initiate connection
  • Network connection not necessarily present when the user logs in
  • Desktop would hang when docked network connection was disconnected
Microsoft Direct Access

• Present since Windows 7
• Can be configured in “Always-On” state
  • Requires Enterprise SKU license on clients
• Originally designed to be a bridge work in conjunction with Microsoft user VPN
• In testing:
  • Could authenticate while connected via UWNet wireless
  • Home drive was mapped, but other SMB shares were not
  • Sometimes unreliable (would work for one attempt, hang at another)
• Microsoft has documentation to migrate from Direct Access to Always On VPN
Microsoft Always-On VPN

• Microsoft lists this as a “replacement solution” for Direct Access
• Always-On VPN present in Windows 10 1709 and later
• VPN instance runs as user “system”, can start once network connection is live
• Can be configured to run full or split tunnel
• Requires
  • Microsoft Remote Access Server
  • Microsoft Network Policy Server
  • PKI infrastructure (AD Certificate Services preferred)
Always-On VPN Setup

• Certificate Services
  • Enable auto-enrollment GPO settings on client computers (for host certs)
  • Create groups for NPS and VPN servers
  • Enable NPS and VPN certificate templates for servers, restrict access
  • Request NPS and VPN server certificates via ADCS
  • VPN user certificates are mentioned in documentation, but not necessary if using machine certificates
Always-On VPN Setup
Always-On VPN Setup

• Network Policy Server
  • Add VPN server to RADIUS client list
    • Can list multiple Remote Access servers
  • Add Connection Request Policy to allow VPN authentication
  • Add Network Policy to allow VPN connections
Always-On VPN Setup

• Configure Remote Access (VPN) Server
  • Enable VPN connections
    • Set to use certificate authentication
    • Determine the block of addresses to be used and how those are managed
      • Static address pool
      • DHCP server
    • Configure authentication and accounting providers
      • RADIUS
      • Windows
    • Disable unused protocols: PPTP, SSTP, L2TP, PPPOE
    • Adjust number of ports available based on client count and address pool size
Always-On VPN Setup

• Network configuration/security
  • VPN Server interface setup
    • Can run with single interface and external firewall rules
    • One internal and one external interface also possible
  • Adjust firewall rules appropriately to minimize exposure

• DNS
  • DNS name or IP address of external interface must be present in VPN server certificate
  • Can add both elements to certificate in certificate request
Always-On VPN Setup

• Create XML file
  • Use certificates, IKEv2 protocol
  • Add domain network information for detection of “home” network where VPN can drop
  • Restrict which IP address ranges can pass through the VPN tunnel
  • Can add additional triggers if desired
Always-On VPN: Testing

• Forcing the VPN to fall over to wireless worked well while user was logged in
• Login sessions were a different issue (dropped connection)
Always-On VPN Testing

- Multiple tweaks to VPN configuration file tested
- Narrowed down to “Preparing Windows” screen
- No mention of cause found—time for Microsoft support call
  - $500 up front
  - Case taken by Microsoft support engineer just before Easter
  - Called back 5 business days later
    - Known bug!
    - Would be fixed in 1803 release
    - Support fee would be refunded because it was a known bug
    - Release expected by the end of April
Microsoft explains why it delayed Windows 10 version 1803 release

by Martin Brinkmann on April 17, 2018 in Windows - 25 comments

Microsoft planned to release the Spring Creators Update for Windows 10, Windows 10 version 1803, last Tuesday on the April 2018 Patch Day.

The company decided against the rollout of the new version of Windows 10 in what seemed like a last minute attempt at preventing that a buggy release hit consumer systems worldwide.

Microsoft did not reveal back then why it decided to delay the release of the new version; in fact, the company never confirmed that April 10, 2018 was the day that it planned to release Windows 10 version 1803 to the public.
Another Windows 10 bug in build 17134 may again delay the April 2018 Update

By Steven Parker  ·  Apr 19, 2018 06:25 EDT  ·  HOT!

The Windows 10 spring update, or 'April 2018 Update' build 17133 was supposed to be the version that shipped to everyone starting nine days ago on April 10, but "reliability issues" blocked it from being the absolute RTM build, despite a cumulative update (17133.73) being released that could have fixed those issues. In an unprecedented move by Microsoft, a second RTM candidate (build 17134.1) was released a couple of days ago, but it seems this too has a bug that needs squashing.
Announcing Windows 10 Insider Preview Build 17133 for Fast

By Dona Sarkar and Brandon LeBlanc

UPDATE 4/10: We have released KB4100375 (OS Build 17133.73) to Windows Insiders running Build 17133 in the Fast, Slow, and Release Preview rings. This update includes the following quality improvements (no new OS features):

- Addresses a PDF security issue in Microsoft Edge.
- Addresses an issue that, in some instances, prevents Internet Explorer from identifying custom controls.
Always-On VPN Result

- Wired connection
Always-On VPN Result

Wireless
Always-On VPN Results

```
Always configuration Enabled . . . : Yes

C:\Users\john.AD.000> tracert 128.104.254.254

Tracing route to rdns1.doit.wisc.edu [128.104.254.254] over a maximum of 30 hops:
1  3 ms  3 ms  2 ms  10.140.0.2
2  4 ms  3 ms  4 ms  10.140.0.3
3  4 ms  2 ms  2 ms  10.151.128.141
4  3 ms  3 ms  2 ms  10.151.128.96
5  2 ms  1 ms  1 ms  r-cscc-b299c-9-core-vlan-1529.net.wisc.edu [146.151.166.113]
6  88 ms  2 ms  1 ms  r-432rm-b3a-1-core-vlan-2039.net.wisc.edu [146.151.167.29]
7  71 ms  2 ms  2 ms  rdns1.doit.wisc.edu [128.104.254.254]

Trace complete.

C:\Users\john.AD.000> tracert thugbert.cs.wisc.edu

Tracing route to thugbert.cs.wisc.edu [128.105.20.19] over a maximum of 30 hops:
1  4 ms  2 ms  2 ms  wisc-admin10-128-105-826-055.cs.wisc.edu [128.105.26.55]
2  4 ms  3 ms  3 ms  wisc-admin10-128-105-826-002.cs.wisc.edu [128.105.26.2]
3  3 ms  2 ms  3 ms  thugbert.cs.wisc.edu [128.105.20.19]

Trace complete.

C:\Users\john.AD.000>
```
Always-On VPN Future Work

• More complete network boundary definition
• New Remote Access server for other laptop pools
• Departmental VPN if new configuration can authenticate via machine certificates
• Similar service for Linux and/or Mac clients
Always-On VPN References

• Press releases:

• Microsoft docs (includes instructions and feature summary):
  • https://docs.microsoft.com/en-us/windows-server/remote/remote-access/remote-access

• Useful how-tos:
  • https://4sysops.com/archives/always-on-vpn-directaccess-for-windows-10/
Thank you!

Questions? Feel free to email or call

John Perkins
john@cs.wisc.edu
608-262-0438