Enhance your Skype for Business user experience over VPN V1.1

INDEX

Author: Balu Ilag Microsoft MVP (Office Servers and Services)

Contact me at: balasaheb.ilag@hotmail.com

Blog: http://communicationsknowledge.blogspot.com/

. This document covers VPN Split Tunnel best practices. Target audience for this admin guide are Skype for Business / Lync Administrator, Skype for Business Online (Office365) Administrator and network Administrator who manages environment.

Introduction:

Virtual Private Network (VPN) are commonly used for securing network traffic. Organization using VPNs for securing their external connections when users are outside the corporate network and allowing them to access internal applications without the requirement of being in an internal physical office.

Basically, VPNs extend a corporate private network by transferring encrypted traffic over tunneling protocol. This encrypted traffic affects Skype for Business / Lync signaling and media traffic because Skype for Business traffic is already encrypted (TLS for SIP signaling and SRTP for media traffic), so there is no need to encrypt it again but VPN solution will encrypt already encrypted traffic.

This document walks you through how VPN affects Skype for Business signaling and media traffic and how to remediate this through different solutions.

How does VPN affect Skype for Business/ Lync traffic?

When user connect VPN that means all connection via local IP address will drop and all existing connection will reconnect via VPN encrypted tunnel. Before VPN connect, your Skype for Business client connected to Skype for Business external (access edge) server but as soon as you connect VPN your Skype for Business client will reconnect to internal server (FE / Director) using DNS query (DNS query move to internal DNS or corporate DNS depending on you VPN configuration).

Depending on the VPN solution configuration, Skype for Business may be tunneling media traffic through the VPN having a negative impact on users. Since Skype for Business traffic is already encrypted using TLS for SIP signaling and SRTP for media traffic), there is no need to encrypt it again but VPN solution will encrypt already encrypted traffic. This double encryption adds overhead to Skype / Lync media traffic.

If you initiate any call or join any conference, all the media traffic will have to go through the VPN encrypted tunnel. Even both users are on at home. Instead of having media going directly between the two-network gateway/router at home, the media will be running from UserA > UserA home router > VPN concentrator > Corporate network > VPN Concentrator> UserB home router <> UserB. Since users are going over more hops, and they have to do double encryption, as above explained. You can expect the call quality to drop, and the latency and jitter to increase. In fact, from the monitoring report you can see Peer-to-Peer and conference call quality show more poor call percentage.

Do we need double encryption for Skype for Business/ Lync traffic?

As far as the security concern, Skype for Business/Lync Client/Server traffic is encrypted by default. SIP signaling uses Transport Layer Security (TLS) for client-server connections and all media traffic is encrypted by using secure real-time transport protocol (SRTP), because of that Skype for Business/Lync traffic does not need an extra encryption layer through a VPN tunnel, unless there is a specific need for dual-layer security (I have not seen such request).

Think the scenario where both Skype for Business/ Lync users are located outside the corporate network. They each have their own individual VPN tunnels, and so Skype for Business/Lync Server media traffic is affected twice by the VPN overhead, latency, Jitter and users will have bad audio/video experience.

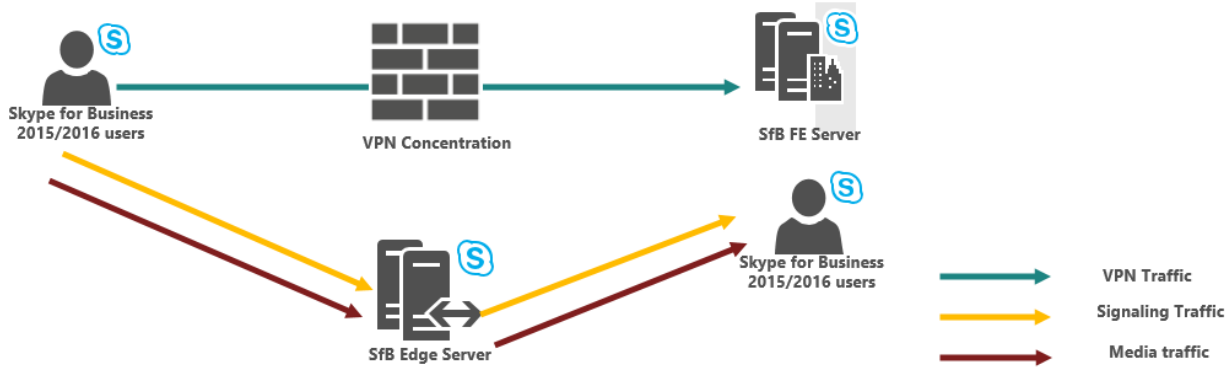
How to increase Quality of experience for VPN Users?

The solution is to use a split-tunnel VPN with Skype for Business/ Lync Server. In a split-tunnel VPN configuration, all IP addresses that are used by the Skype for Business/Lync Server environment are excluded, so that traffic to and from those addresses is not included in the VPN tunnel. Means the way VPN split tunnel must work exactly same as external Skype for Business client should.

Most VPN solution provider supports split tunnel, you must check the configuration for your VPN solution by checking seller documentation.

Below diagram shows, how Split tunnel works.

All Skype for Business signaling and media traffic split from VPN secure tunnel and going though Skype for Business edge (external) server.



Solution / Approach:

There are different ways to achieve split tunnel:

1. Use Windows Firewall- All Skype for Business executable path (32 and 64 bit), all traffic both in-bound and out-bound for TCP and UDP will be blocked. Allow Skype for Business client to resolve DNS request using local Adaptor instead of VPN (virtual) Adaptor, that way client resolve external DNS records and connect. Also make sure all traffic going via local adaptor should be preferred verses VPN adaptor. This works great for windows client but not for non-windows machine, like Mac client.
2. **Using 3rd party VPN solution:**
   This document covering VPN split tunnel configuration based on Pulse secure VPN solution**:**

   There are different approach and solution to implement VPN Spilt tunnel, I am showing here combined solution to using VPN Concentrator and firewall.

   What we are doing is, creating policy on VPN concentrator to exclude Skype for Business/Lync external server IP addresses traffic from VPN tunnel, mean deny signaling and media traffic via VPN tunnel for Skype for Business / Lync External IP address. Then using your corporate Firewall create deny rule to deny traffic source from VPN user subnet to Skype for Business/Lync internal server IP address and from Skype for Business / Lync internal IP addresses to VPN User subnets both ways.

   Note: You may use dedicated DNS server for VPN client however make sure your Skype for Business internal Server SRV and A record must not resolve by this DNS server.

Split Tunnel solution is combine solution using VPN concentrator and your firewall.

a. First get all external IP address of your Skype for Business access edge, AV edge, Web conference, Reverse proxy (external Web Service), Meet and dial-in VIPs and OWA public IP addresses.
b. Create policy on VPN concentrator which will '**Exclude**' traffic via VPN tunnel for all external Server Public IP addresses. In otherward deny traffic or split tunnel to this IP addresses from your VPN Tunnel and assign this policy to all other policy/users.
c. Now work with your network Firewall team and do below:

Split conferencing (media) traffic to external Server (not via VPN Tunnel),

Remember all conference modality traffic involved through MCU (Multi Control Unit) running on Skype for Business/ Lync Server. First do below firewall rules:

a. Create firewall rule which will block traffic going from VPN User subnets to Skype for Business/ Lync Server (only internal IP address of FE, Mediation, Edge internal interface).
b. Create another Firewall rule which will says, block traffic going from Skype for Business/ Lync Server (only internal IP address of FE, Mediation, Edge internal interface) to VPN User Subnet.

To split Peer-to-peer traffic, you must create below rule on your firewall.

Second thing is to enable the blockage the UPD/TCP source port for Audio Video, File share and application sharing. Basically, Skype for Business/Lync by default has a limited scope of UDP/TCP port it will be using as source port for communication. If you block these source port from coming in the VPN tunnel, then the media should go via the external (Edge) Server. That will ensure that even two users both connected via VPN, their AV media will not hair pin via their VPN connection, but do directly goes from their internet connection to each other.

These rules look like,

a. Create firewall rule Source address from "VPN_Users" Subnet to destination as "Any" with application "Stun" and Service port (UDP/TCP port ranges of AV, App Share, file transfer etc.)
b. Create another firewall rule Source from "any" address to destination "VPN_Users" Subnet with application "Stun" and Service port (UDP/TCP port ranges of AV, App Share, file transfer etc.)

*You can get Audio/Video, AppShare, and file transfer client port ranges from Skype for Business / Lync Server using below PowerShell command. *Get-CsConferencingConfiguration*.

Does this document apply to Skype for Business Online?

Yes, this document is applicable to Skype for Business Online as well. Just consider Office 365 URLs and IP Address Ranges as Skype for Business Server IP addresses.

How to verify VPN Split Tunneling?

From External network connect VPN which has Split Tunnel implemented.

- Then make Peer to peer call and capture UCCAPILOG and network traces using Wireshark or Network monitor and verify final candidate pair in SDP it should be STUN or TURN candidate not host candidate.
- Join meeting and capture UCCAPILOG and network traces using Wireshark or Network monitor and verify final candidate pair in SDP it should be STUN or TURN candidate not host candidate.
- Attempt a Telnet to internal Skype pools server should not work.
- Attempt a traceroute to the internal Skype pools server should not work.

Lesson learned:

1. For internal Skype server block rule on firewall, action set as RESET instead of denying making Skype client sign-in process faster.

Acronyms:

- TLS: Transport Layer Security
- SIP: Session Initiation Protocol
- SDP: Session Description Protocol
- TCP: Transmission Control Protocol
- UDP: User Datagram Protocol
- RTP: Real-time Transport Protocol
- SRTP: Secure Real-time Transport Protocol
- Candidate: Possible combination of IP address and port for media channel
- ICE: Interactive Connectivity Establishment
- STUN: Session Traversal Utilities for NAT
- TURN: Traversal Using Relay NAT

Conclusion:

Providing optimal experience to the end-user community is our main goal, and using VPN split tunneling is helps to achieving this through blocking the client from connecting to the internal (FE) server directly, and the media will always go through the external sever (Edge). Which will eliminate extra hop, double encryption etc.

Thank you.