VMR Firewall Port Requirements

General Requirements

To access AVI-SPL's Virtual Meeting Room (VMR) service platform, security considerations must be accounted for successful user access to use VMR for audio/video/content collaboration.

As most organizations have strict perimeter firewall security rules, users may not be able access the public Internet on the required TCP/IP ports typically used for AVI-SPL's VMR service that requires audio, video and content streams. If an organization does not have a Session Boarder Controller (SBC), such as a Cisco VCS-Expressway or Polycom RPAD device, or intends to use WebRTC or Skype for Business to collaborate, traffic to and from the VMR media ports must be open in path firewall(s).

The following information is provided for the specific enablement to limit exposure to organization security policies when open ports to AVI-SPL's VMR service.

The following Internet IP Range, DNS and TCP/IP port list and diagram must be accommodated for service availability:

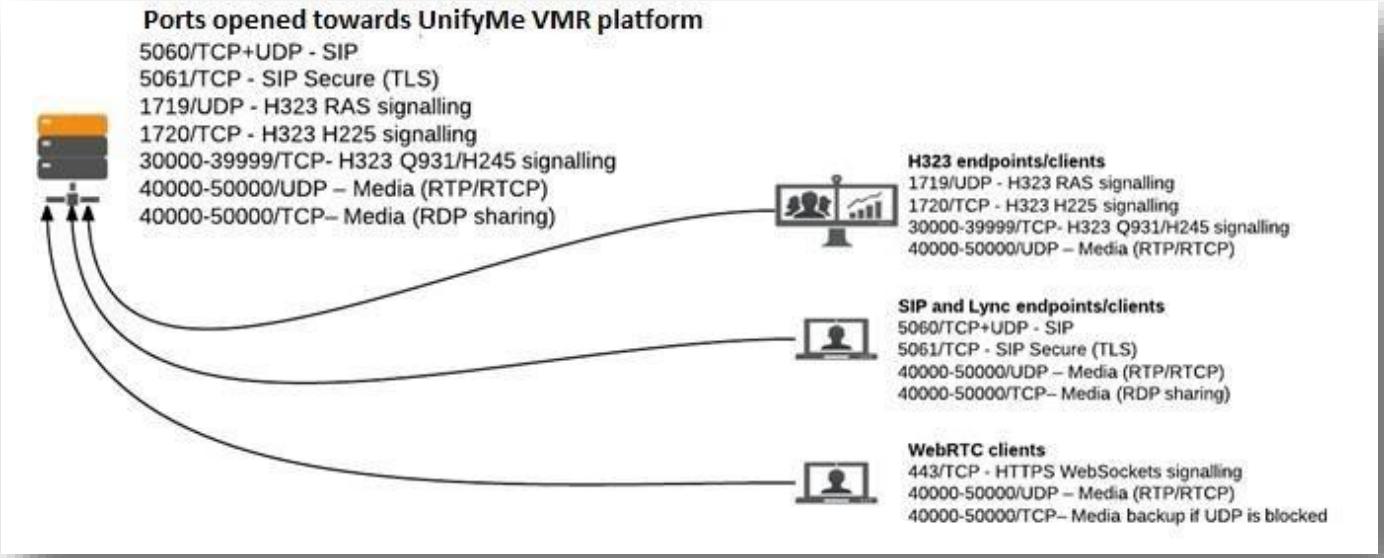
- Unify ME™ Exchange Internet IP space - 209.251.0.0/20
  - 209.251.7.30-37 UVMR-USA
  - 37.252.213.244-246 UVMR-AUS
  - 37.252.210.244-246 UVMR-UK
  - 209.251.7.61-65 vmrdemo.me (Demo environment)

- DNS lookup for A and SRV records to **uvmr.me** , **vmrdemo.me**, **vmr.avispl.com** or **mycospace.com**

- Microsoft Lync/Skype for Business: For direct federation, please use the following address: **_sipfederationtls._tcp.uvmr.me** which resolves to **sip.uvmr.me 209.251.7.31** in the Americas **37.252.210.245** in Europe and **37.252.213.245** in APAC.

VMR Firewall Port Requirements

- Audio, Video and Content Ports – The following accommodates SIP, H323, Lync or WebRTC traffic flows. Source ports are defined by the calling client, which may require local owner manual review. The following are destination ports:



Additional Considerations

Protocol fixups and inspection are generally used to enable audio calls across a firewall in some circumstances and is known to cause unpredictably with video calls across a firewall. **Inspection and fixup of H.323 and SIP should be disabled per the firewall manufacturer's guidance.**

Firewall traversal without a corporate infrastructure can require configuration of the codec. Improper NAT configurations can cause various connectivity issues with the Unify ME VMR service and other external calling. **Please ensure that all codecs are properly configured** for use with the Unify ME VMR service.