IM and Presence

Legend

- 🟥 SIP traffic: signaling and IM
- 🟪 XMPP traffic
- 🟩 HTTPS traffic
- 🟦 MSMQ traffic
- 🟨 CLS traffic
- ← Arrow direction indicates which server initiates the connection. Actual traffic is bi-directional.

Services and Processes

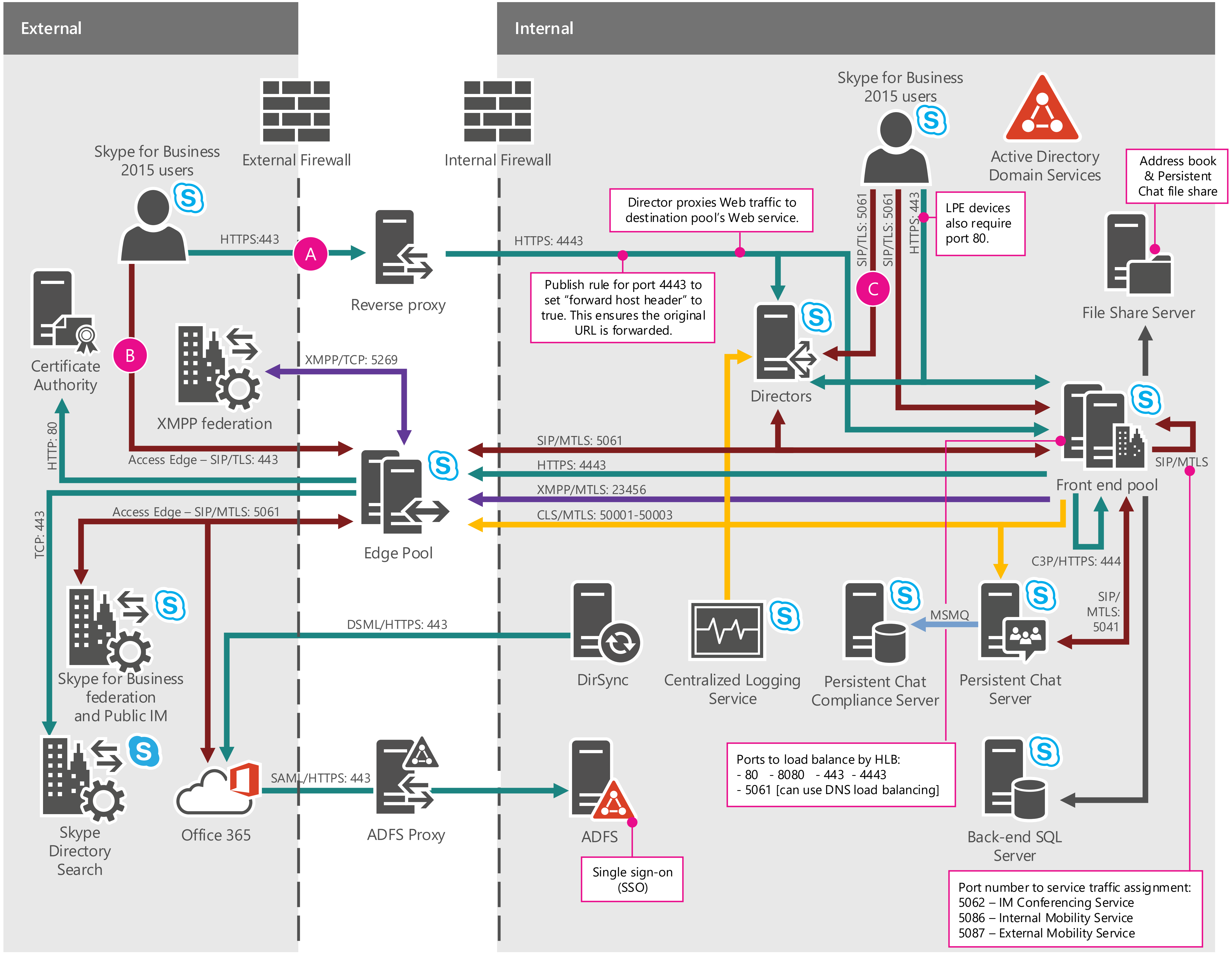
A This port is used to connect to Web Services:
- download the Address Book
- connect to Address Book Web query URL
- provide distribution list expansion
- download meeting content
- connect to the Mobility Service
- connect to the AutoDiscover Service
- connect to Dial-in URL
- connect to Lync Web App
- connect to CertProvisioningService

B External user sign-in process:

1. Client discovers Edge Server:
   a. lyncdiscoverinternal.<sip-domain>
   b. lyncdiscover.<sip-domain>
   c. _sipinternaltls._tcp.<sip-domain>
   d. _sipinternal._tcp.<sip-domain>
   e. _sip._tls.<sip-domain>
   f. sipinternal.<sip-domain>
   g. sip.<sip-domain>
   h. sipexternal.<sip-domain>
2. Client connects to Edge Server.
3. Edge Server proxies connection to Director.
4. Director authenticates user and proxy connection to user’s home pool.

C Internal user sign-in process:

1. Client discovers Enterprise Pool:
   a. lyncdiscoverinternal.<sip-domain>
   b. lyncdiscover.<sip-domain>
   c. _sipinternaltls._tcp.<sip-domain>
   d. _sipinternal._tcp.<sip-domain>
   e. sipinternal.<sip-domain>
   f. sip.<sip-domain>
2. Client connects to Enterprise Pool server.
3. Enterprise pool server authenticates user and redirects connection to user’s home server.



Director proxies Web traffic to destination pool’s Web service.

Publish rule for port 4443 to set “forward host header” to true. This ensures the original URL is forwarded.

LPE devices also require port 80.

Address book & Persistent Chat file share

Ports to load balance by HLB:
- 80 - 8080 - 443 - 4443
- 5061 [can use DNS load balancing]

Single sign-on (SSO)

Port number to service traffic assignment:
5062 – IM Conferencing Service
5086 – Internal Mobility Service
5087 – External Mobility Service

Skype for Business

Version date 10/12/2016

Microsoft

A/V and Web Conferencing

Legend

🟥	SIP traffic: signaling
🟪	HTTP(S) traffic
🟩	RTP/SRTP traffic: A/V Conferencing
🟦	PSOM traffic: Web Conferencing
🟨	ICE traffic
←	Arrow direction indicates which server initiates the connection. Actual traffic is bi-directional.

A

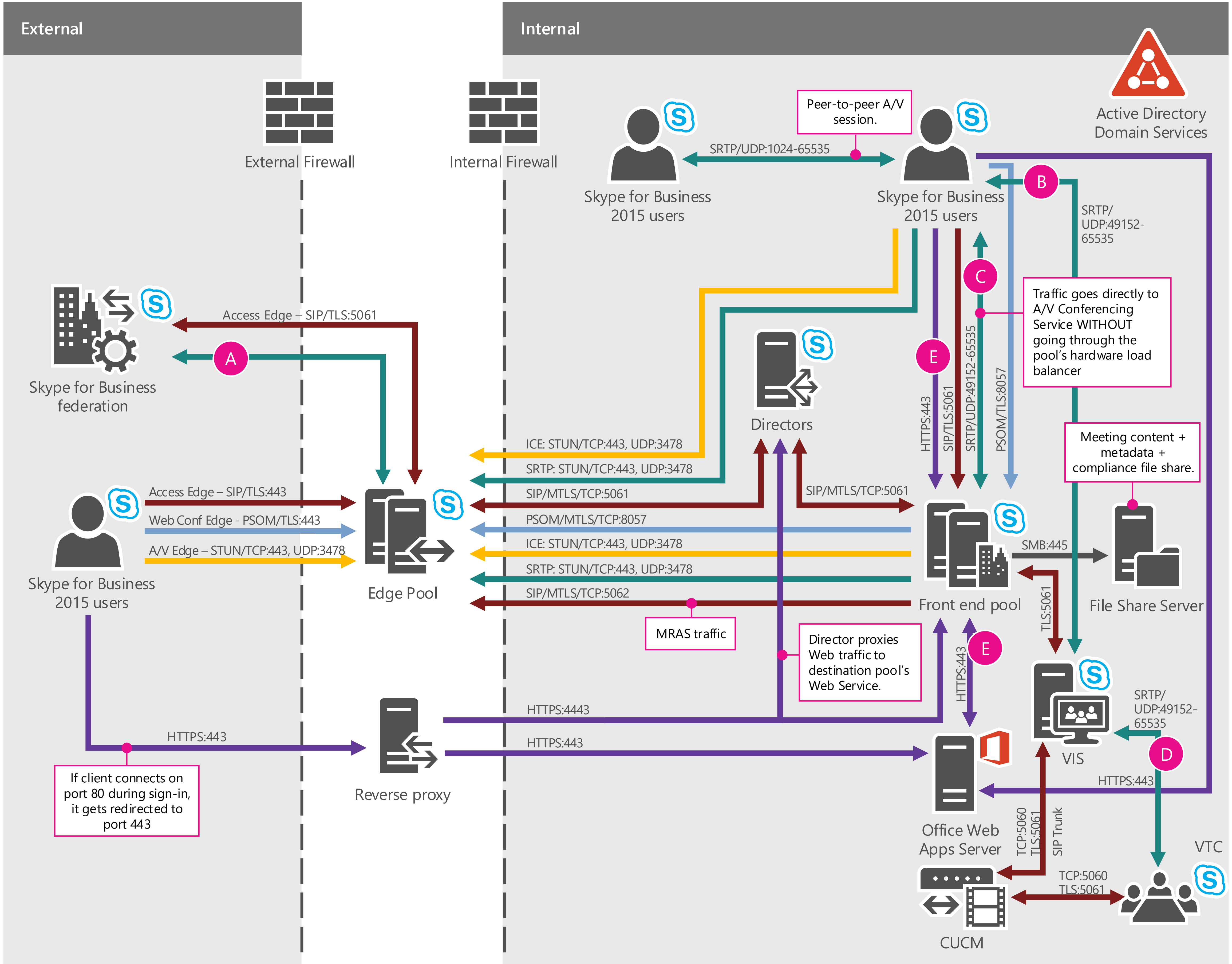
Source IP	Destination IP	Source Port	Destination Port
A/V Edge	Any	TCP 50,000-59,999	TCP 443
A/V Edge	Any	UDP 3478	UDP 3478
Any	A/V Edge	Any	TCP 443
Any	A/V Edge	Any	UDP 3478

B Codec varies per workload:
- G.722 for audio
- H264SVC for video

C Codec varies per workload:
- G.722, Siren or SILK for audio
- H264SVC for video [RTVideo for downlevel clients]

D Codec varies per workload:
- G.722 for audio
- H264AVC for video

E HTTPS: 443 is used to download conferencing content, including Powerpoint files and sharing.



Peer-to-peer A/V session.

Traffic goes directly to A/V Conferencing Service WITHOUT going through the pool's hardware load balancer

Meeting content + metadata + compliance file share.

MRAS traffic

Director proxies Web traffic to destination pool's Web Service.

If client connects on port 80 during sign-in, it gets redirected to port 443

Skype for Business

Version date 10/12/2016

Microsoft

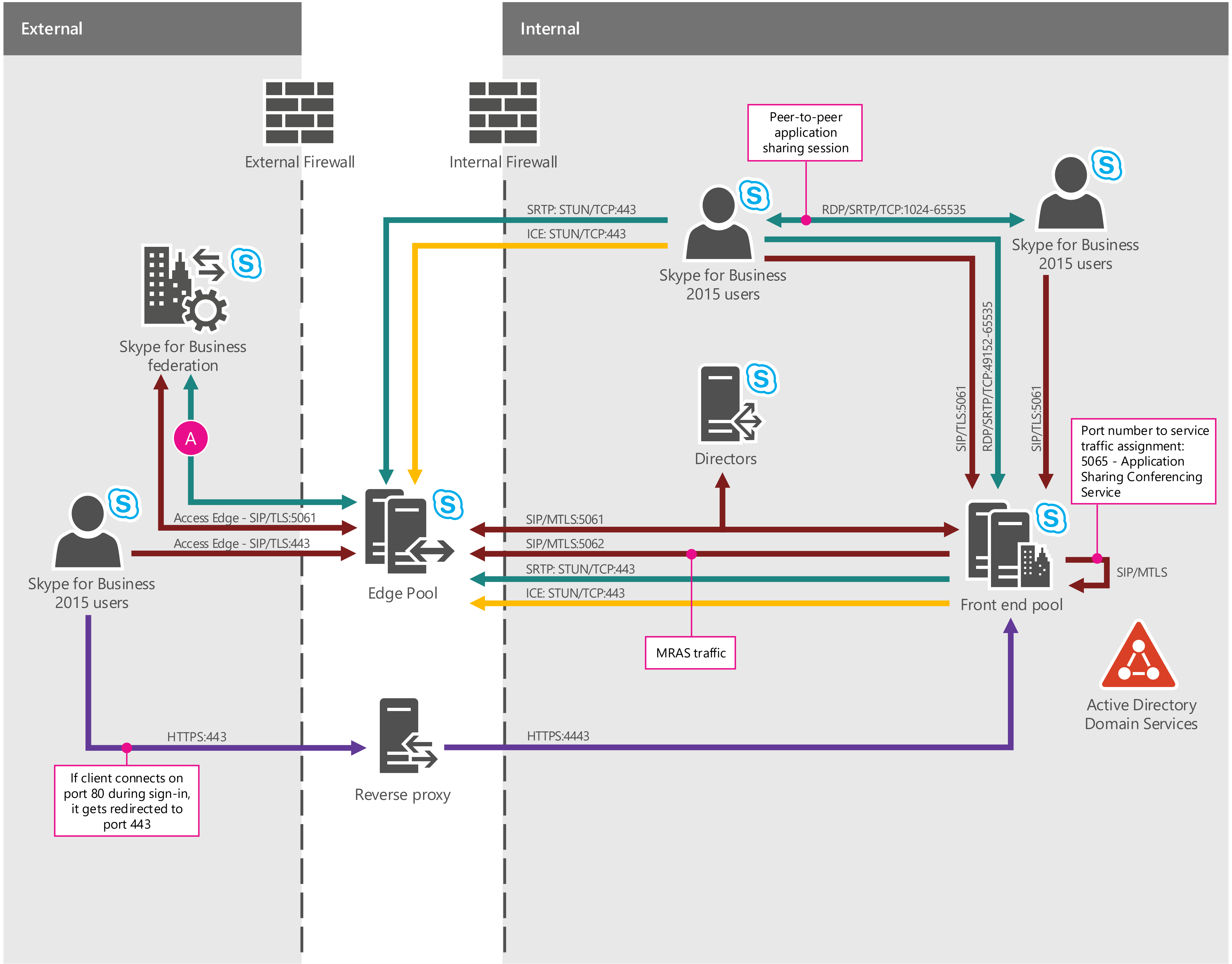
Application Sharing

Legend

- 🟥 SIP traffic: signaling
- 🟪 HTTP(S) traffic
- 🟩 RTP/SRTP traffic: A/V Conferencing
- 🟨 ICE traffic
- ← Arrow direction indicates which server initiates the connection. Actual traffic is bi-directional.

A

Source IP	Destination IP	Source Port	Destination Port
A/V Edge	Any	TCP 50,000-59,999	TCP 443
Any	A/V Edge	Any	TCP 443



Peer-to-peer application sharing session

Port number to service traffic assignment:
5065 - Application Sharing Conferencing Service

MRAS traffic

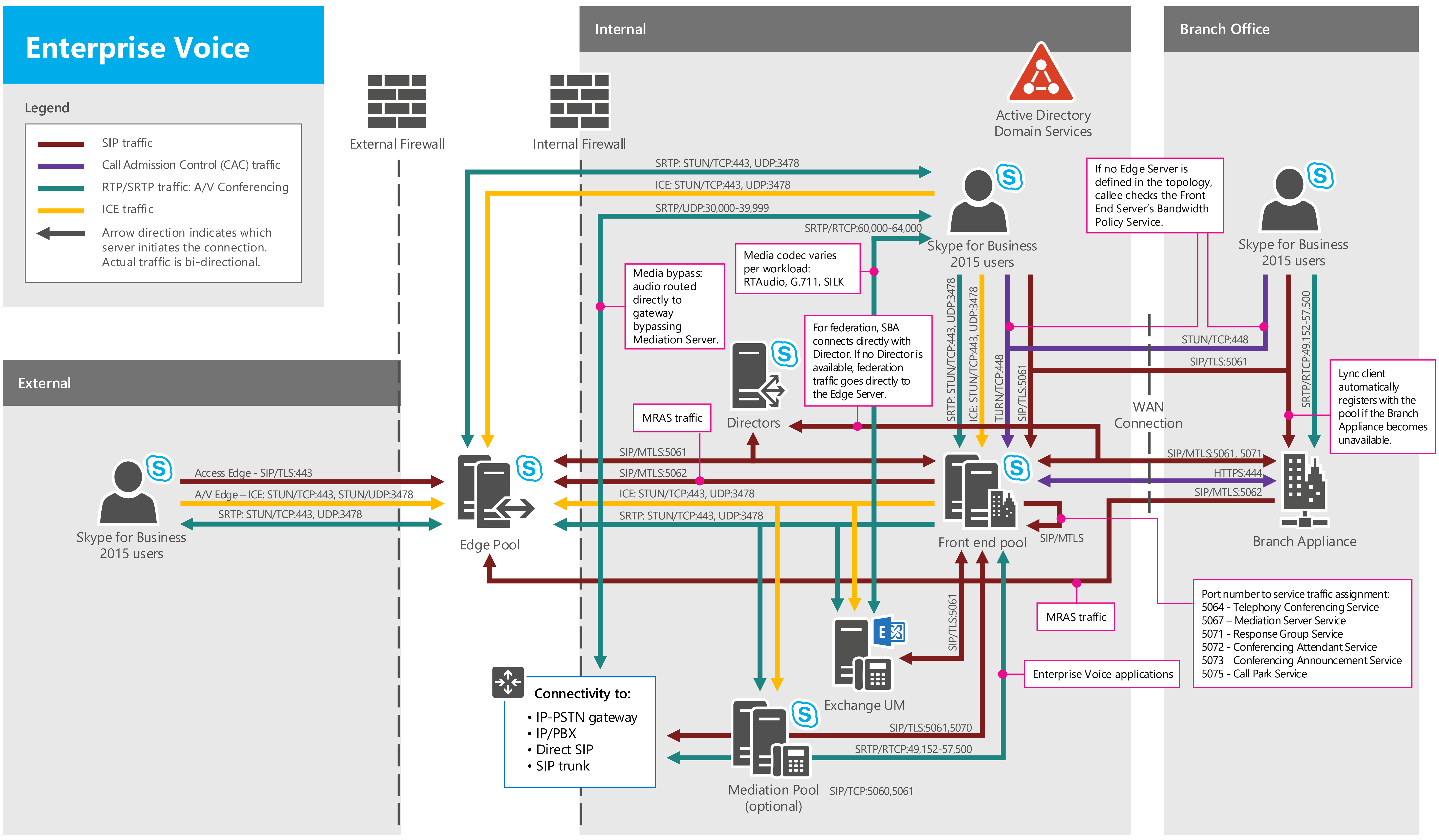
If client connects on port 80 during sign-in, it gets redirected to port 443

Skype for Business

Version date 10/12/2016

Microsoft

Enterprise Voice



Legend

- 🟥 SIP traffic
- 🟪 Call Admission Control (CAC) traffic
- 🟩 RTP/SRTP traffic: A/V Conferencing
- 🟨 ICE traffic
- ← Arrow direction indicates which server initiates the connection. Actual traffic is bi-directional.

External
Internal
Branch Office
External Firewall
Internal Firewall
Active Directory Domain Services
Skype for Business 2015 users
Access Edge - SIP/TLS:443
A/V Edge – ICE: STUN/TCP:443, STUN/UDP:3478
SRTP: STUN/TCP:443, UDP:3478
Skype for Business 2015 users
Edge Pool
SRTP: STUN/TCP:443, UDP:3478
ICE: STUN/TCP:443, UDP:3478
SRTP/UDP:30,000-39,999
SRTP/RTCP:60,000-64,000
Skype for Business 2015 users
Directors
MRAS traffic
SIP/MTLS:5061
SIP/MTLS:5062
ICE: STUN/TCP:443, UDP:3478
SRTP: STUN/TCP:443, UDP:3478
SRTP: STUN/TCP:443, UDP:3478
ICE: STUN/TCP:443, UDP:3478
TURN/TCP:448
SIP/TLS:5061
Front end pool
SIP/MTLS
STUN/TCP:448
SIP/TLS:5061
WAN Connection
SIP/MTLS:5061, 5071
HTTPS:444
SIP/MTLS:5062
SRTP/RTCP:49,152-57,500
Skype for Business 2015 users
Branch Appliance
MRAS traffic
SIP/TLS:5061
Exchange UM
Enterprise Voice applications
SIP/TLS:5061,5070
SRTP/RTCP:49,152-57,500
SIP/TCP:5060,5061
Mediation Pool (optional)

Media bypass: audio routed directly to gateway bypassing Mediation Server.

Media codec varies per workload: RTAudio, G.711, SILK

For federation, SBA connects directly with Director. If no Director is available, federation traffic goes directly to the Edge Server.

If no Edge Server is defined in the topology, callee checks the Front End Server's Bandwidth Policy Service.

Lync client automatically registers with the pool if the Branch Appliance becomes unavailable.

Connectivity to:

- IP-PSTN gateway
- IP/PBX
- Direct SIP
- SIP trunk

Port number to service traffic assignment:
5064 - Telephony Conferencing Service
5067 – Mediation Server Service
5071 - Response Group Service
5072 - Conferencing Attendant Service
5073 - Conferencing Announcement Service
5075 - Call Park Service

Skype for Business

Version date 10/12/2016

Microsoft

Certificate Requirements

Core elements

Front End Pool

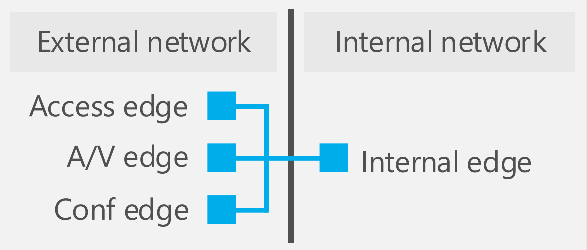
Front End Server 1, Front End Server 2

FQDN:	pool.<ad-domain>
Certificate SN:	pool.<ad-domain>
Certificate SAN:	pool.<ad-domain>, fe.<ad-domain>, sip.<sip-domain>, lyncdiscoverinternal.<sip-domain>, lyncdiscover.<sip-domain>, admin URL, meet URL, dial-in URL,
EKU:	server
Root certificate:	private CA

Edge Servers

Edge Server 1, Edge Server 2

Internal FQDN:	internal.<ad-domain>
Certificate SN:	internal.<ad-domain>
Certificate SAN:	
EKU:	server
Root certificate:	private CA



External FQDN:	access.<sip-domain>
Certificate SN:	access.<sip-domain>
Certificate SAN:	access.<sip-domain>, sip.<sip-domain>, conf.<sip-domain>
EKU:	server
Root certificate:	public CA

Persistent Chat Server

FQDN:	chatsrv.<ad-domain>
Certificate SN:	chatsrv.<ad-domain>
Certificate SAN:	N/A
EKU:	server, client
Root certificate:	private CA

Directors

Director 1, Director 2

FQDN:	dir.<ad-domain>
Certificate SN:	dir.<ad-domain>
Certificate SAN:	dir.<ad-domain>, sipinternal.<sip-domain>, sip.<sip-domain>, lyncdiscoverinternal.<sip-domain>, lyncdiscover.<sip-domain>, admin URL, meet URL, dial-in URL
EKU:	server
Root certificate:	private CA

Additional elements

Reverse proxy

FQDN:	external Web Service FQDN
Certificate SN:	external Web Service FQDN
Certificate SAN:	external Web Service FQDN, lyncdiscover.<sip-domain>, meet URL, dial-in URL, OwaExtWeb.<sip-domain>
EKU:	server
Root certificate:	public CA

Branch Appliance

FQDN:	sba.<ad-domain>
Certificate SN:	sba.<ad-domain>
Certificate SAN:	sba.<ad-domain>
EKU:	server
Root certificate:	private CA

Exchange UM Server

FQDN:	umsrv.<ad-domain>
Certificate SN:	umsrv.<ad-domain>
Certificate SAN:	N/A
EKU:	server
Root certificate:	private CA

Office Web Apps Server

FQDN:	OwaExtWeb.<sip-domain>
Certificate SN:	OwaExtWeb.<sip-domain>
Certificate SAN:	wacsrv1.<ad-domain>
Certificate SAN:	wacsrv2.<ad-domain>
EKU:	server
Root certificate:	private CA

Skype for Business

Version date 10/12/2016

Microsoft

CMS

Legend

▬ SMB traffic

▬ HTTPS traffic

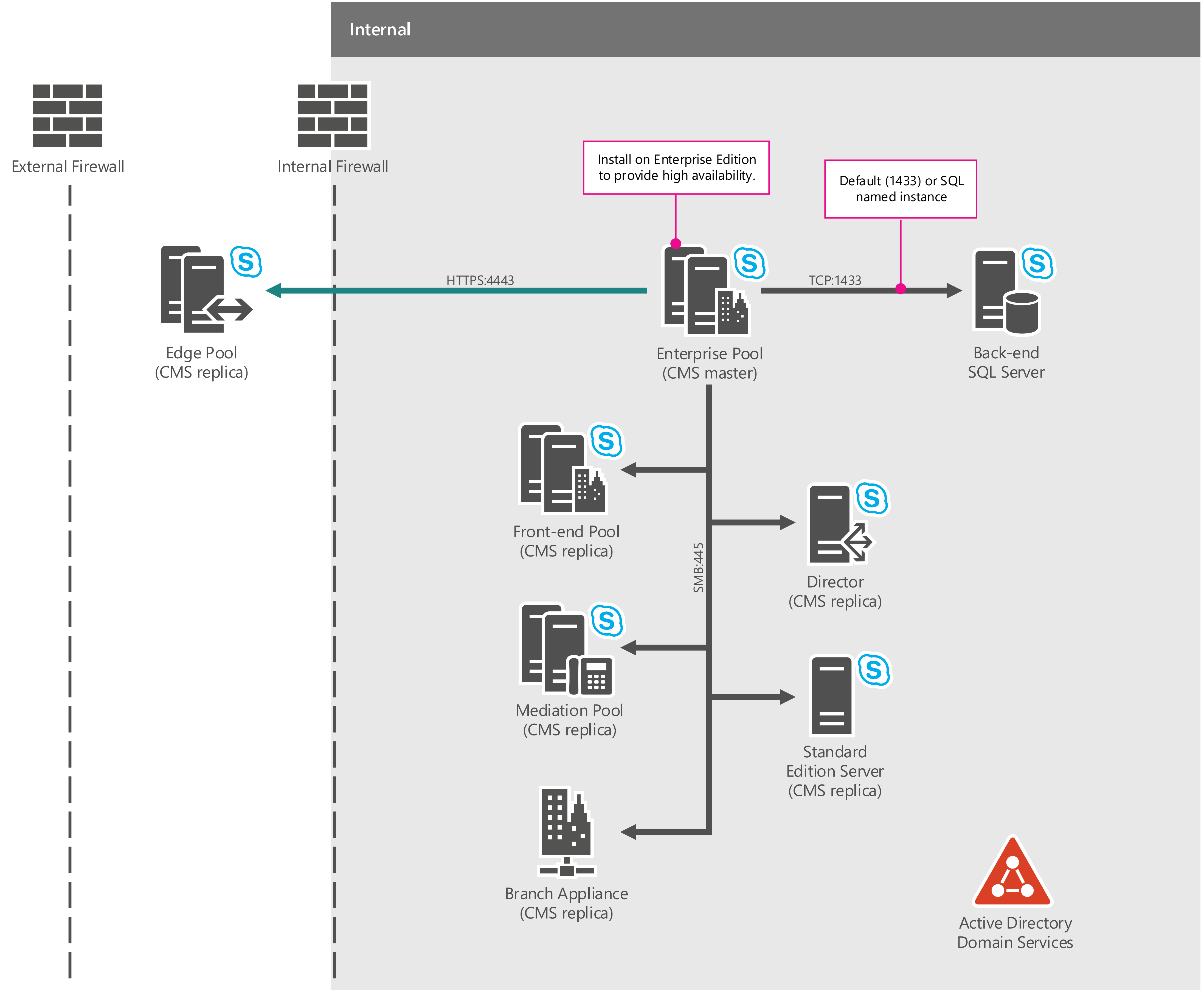
← Arrow direction indicates which server initiates the connection. Subsequent traffic is bi-directional.

The Central Management Store provides a robust, schematized storage of the data needed to define, set up, maintain, administer, describe, and operate a Skype for Business Server deployment. It also validates the data to ensure configuration consistency.

All changes to this configuration data happen at the Central Management store, eliminating “out-of-sync” issues. Read-only copies of the data are replicated to all servers in the topology, including Edge Servers and Survivable Branch Appliances.

The Active Directory Domain Services (AD DS) are still used to store basic user information, such as the user’s SIP URI and phone number. User policy information is stored in the Central Management store. The use of Active Directory Domain Services (AD DS) also provides backward compatibility with earlier releases of Lync Server.

To administer servers and services, you use Skype for Business Server Management Shell or the Skype for Business Server Control Panel, which then configure the settings in the Central Management store. The Central Management Server, which runs on one Front End pool or one Standard Edition server in your deployment, replicates the configuration changes to all of the servers in your deployment.


Internal
External Firewall
Internal Firewall
Install on Enterprise Edition to provide high availability.
Default (1433) or SQL named instance
HTTPS:4443
TCP:1433
Edge Pool (CMS replica)
Enterprise Pool (CMS master)
Back-end SQL Server
SMB:445
Front-end Pool (CMS replica)
Director (CMS replica)
Mediation Pool (CMS replica)
Standard Edition Server (CMS replica)
Branch Appliance (CMS replica)
Active Directory Domain Services

Skype for Business

Version date 10/12/2016

Microsoft

DNS Configuration

Internal DNS Configuration

DNS Type	Value	Enterprise Edition Resolution	Standard Edition Resolution	Purpose
SRV	_sipinternaltls._tcp.<sip-domain>	pool FQDN	pool FQDN	internal user access
A/CNAME	lyncdiscoverinternal.<sip-domain>	HLB FE Pool VIP	pool IP address	internal AutoDiscover Service
A	Pool FQDN	individual FE IPs	pool IP address	Internal pool name
A	admin URL	HLB FE Pool VIP	pool IP address	Lync Server Control Panel (LSCP)
A	meet URL	HLB FE Pool VIP	pool IP address	Lync Server Web Service
A	dial-in URL	HLB FE Pool VIP	pool IP address	Lync Server Web Service
A	internal Web Services FQDN	HLB FE Pool VIP	pool IP address	Lync Server Web Service
A	external Web Services FQDN	Reverse proxy public IP address	Reverse proxy public IP address	Proxied to Lync Server Web Service

External DNS Configuration

DNS Type	Value	Resolution	Purpose
SRV	_sipfederationtls._tcp.<sip-domain>	Access Edge FQDN: access.<sip-domain>	Federation and public IM connectivity
SRV	_sip._tls.<sip-domain>	Access Edge FQDN: access.<sip-domain>	external user access
SRV	_xmpp-server._tcp.<sip-domain>	Access Edge FQDN: access.<sip-domain>	XMPP federation
A	sip.<sip-domain>	Access Edge FQDN: access.<sip-domain>	locate Edge Server
A	Access Edge FQDN: access.<sip-domain>	Access Edge IP address	Edge Server Access edge
A	A/V Edge FQDN: av.<sip-domain>	A/V Edge IP address	Edge Server A/V edge
A	Conf Edge FQDN: conf.<sip-domain>	Conf Edge IP address	Edge Server Conf edge
A/CNAME	lyncdiscover.<sip-domain>	reverse proxy public IP address	external AutoDiscover Service
A	meet URL	reverse proxy public IP address	proxied to Lync Server Web Service
A	dial-in URL	reverse proxy public IP address	proxied to Lync Server Web Service
A	external Web Services FQDN	reverse proxy public IP address	proxied to Lync Server Web Service

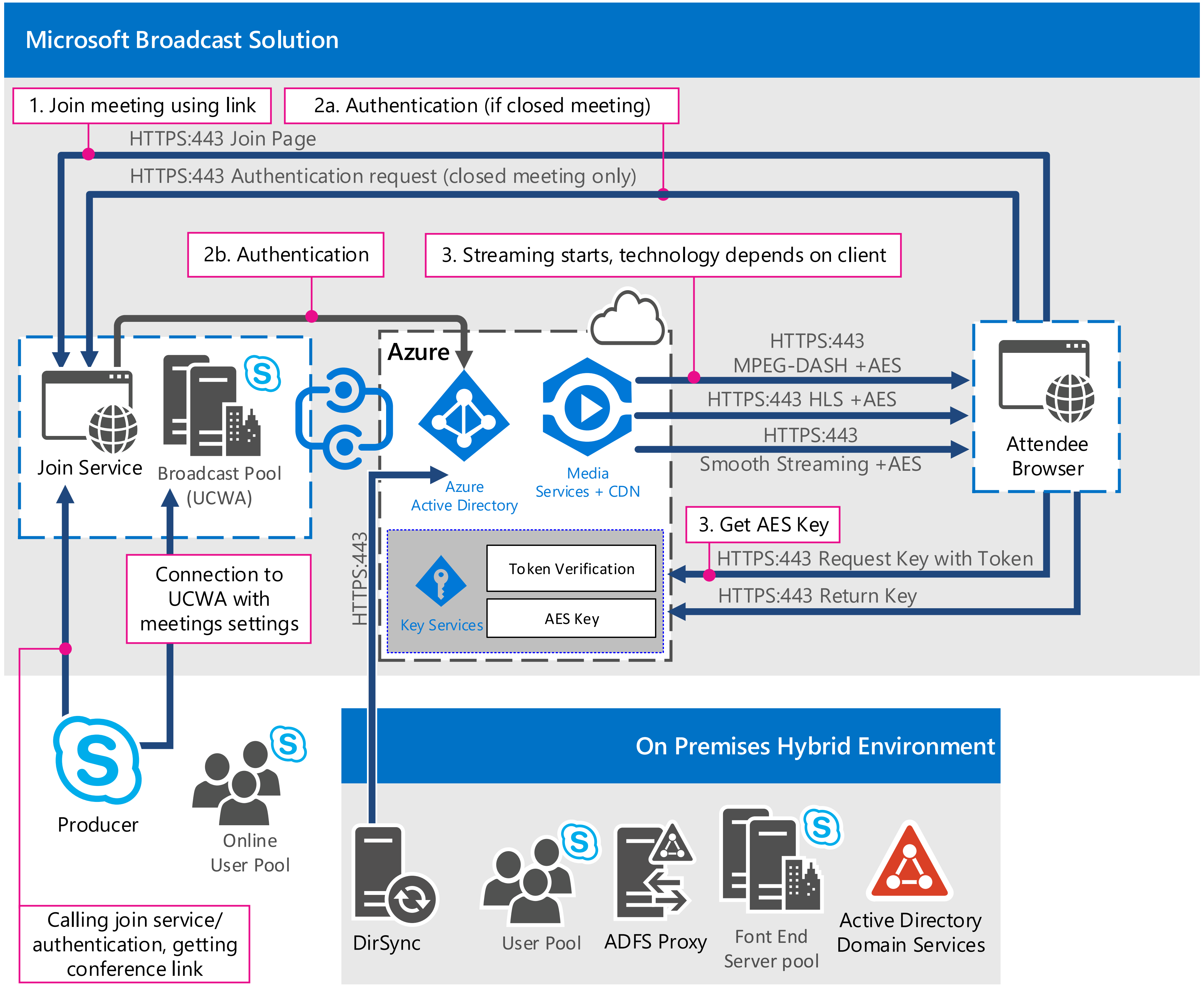
OWA

DNS Type	Value	Office Web Apps Farm Resolution	Office Web Apps Server Resolution	Purpose
A	OWA internal URL	HLB OWA VIP	OWA server IP	internal user access to PowerPoint Presentations
A	OWA external URL	Reverse proxy public IP address	Reverse proxy public IP address	external user access to PowerPoint Presentations

Broadcast Conferencing

Legend

▬	HTTPS traffic
←	Arrow direction indicates which server initiates the connection. Actual traffic is bi-directional.



Microsoft Broadcast Solution

1. Join meeting using link

2a. Authentication (if closed meeting)

HTTPS:443 Join Page

HTTPS:443 Authentication request (closed meeting only)

2b. Authentication

3. Streaming starts, technology depends on client

Join Service

Broadcast Pool (UCWA)

Azure

Azure Active Directory

Media Services + CDN

HTTPS:443 MPEG-DASH +AES

HTTPS:443 HLS +AES

HTTPS:443 Smooth Streaming +AES

Attendee Browser

3. Get AES Key

HTTPS:443 Request Key with Token

HTTPS:443 Return Key

Token Verification

AES Key

Key Services

HTTPS:443

Connection to UCWA with meetings settings

Producer

Online User Pool

Calling join service/ authentication, getting conference link

On Premises Hybrid Environment

DirSync

User Pool

ADFS Proxy

Font End Server pool

Active Directory Domain Services

Skype for Business

Version date 10/12/2016

Microsoft