BLACK BOX WHITE PAPER: COALESCE SECURITY FEATURES

LEAVE THE TECH TO US

INTRODUCTION:

Coalesce™ MPE (Meeting Place Edition) is a wireless presentation solution enabling meeting attendees to share the screens of their connected devices and video cameras. Coalesce™ MPE is a tailored solution on Android 6.0 hardware.

Software as a Service (SaaS)

This encompasses our application services which support authentication, REST APIs, group messaging and video collaboration services. This layer is hosted within our cloud.

SaaS

All inbound and outbound data from SaaS layer is encrypted and transmitted over TLS or DTLS with 2048-bit asymmetric encryption and 256-bit symmetric encryption using certificates from third party credited authorities. Network communication is protected using the latest in technology to secure all your video, audio and data. Using the TLS and DTLS cryptography protocols, previously referred to as SSL, we provide protection using a 2048-bit asymmetric key in conjunction with a 256-bit symmetric session key. More information on ports used can be seen in Firewall Considerations.

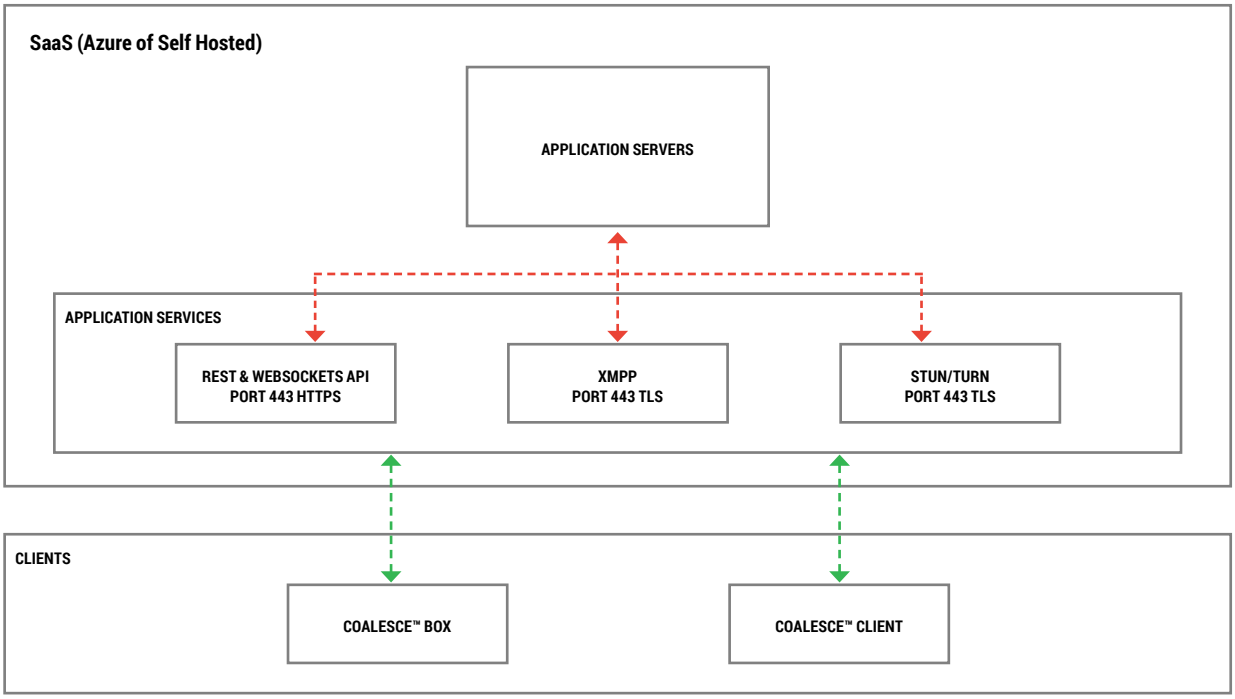
The SaaS tier provides three public services; REST API, XMPP and STUN and TURN. See Figure 1 on the next page.

Azure

We use Azure to host and support the services we offer to our clients. Azure's Datacenters are geographically dispersed and comply to ISO/IEC 27001:2005, SOC 1 and SOC 2[1]. These Datacenters are managed and operated by Microsoft who have decades-long experience building enterprise software and running some of the largest online services in the world. Using Azure's Network Security Groups (NSG), access to the virtual machines hosting our services is limited to those ports configured within the NSG only. All our virtual machines are located within the same virtual LAN and communication between virtual machines is via private network interfaces behind the Azure firewall.

1 http://www.iso.org/iso/catalogue_detail?csnumber=42103

FIGURE 1 | COALESCE™ MPE ARCHITECTURE



COALESCE™

The Coalesce™ MPE software consumes a REST API provided by our SaaS layer which is credential secured. All communication with the REST API and our XMPP services are over TLS (port 443) with 2048-bit asymmetric encryption and 256-bit symmetric encryption. For video calls, STUN is used to establish a peer to peer connection. If this fails, then the client will attempt to use our relay service using the TURN protocol.

In addition to DTLS encryption, we also encrypt data through Secure Real-Time Protocol, which safeguards IP communications from hackers, so that your video and audio data is kept private point to point.

Cloud

If Coalesce™ MPE has access to the Coalesce™ Cloud, then it will be able to enable devices connecting to it from outside of its local network – e.g. A Chromebook™ client on a remote network and a Windows® client connected on another network within your organization. The Coalesce™ MPE hardware unit can also function solely using its access point with which connecting devices will be assigned IP address.

Updates

In order to receive updates, an internet connection will be needed. The updates are downloaded over a secure connection, port 443, and are installed on demand. A notification will appear in the Coalesce™ MPE user interface to indicate an update which the user can install.

Meeting ID

For each meeting, a unique meeting ID is generated mediated from our SaaS layer, which is used as a means for the clients to connect to that specific meeting. The host can also specify a PIN, which is configured at the box directly. Each client connecting requests confirmation of the PIN. On connection, the screen of the connected device is shared and the user can decide to continue sharing their screen and adding web camera.

Security

The clients and boxes are authenticated on our servers using a four-step authentication process with SASL[2]. At any time, administrators can remove a client or box from the authorized zone temporarily and permanently.

All data transferred between the user's device and Coalesce™ MPE is peer to peer (P2P) and is over TLS or DTLS with 2048-bit asymmetric encryption and 256-bit symmetric encryption. If a P2P connection fails to connect between the client and Coalesce™ MPE, then the software will relay the data via our TURN server over TLS TCP port 443.

Access Point

The Coalesce™ MPE hardware units offer an internal access point, secured with WPA2 with TKIP encryption, enabling clients to connect directly to the box and in so creating a local network. The box can be configured to allow these locally connected devices to have access to an external network which would be cabled to the box.

The Coalesce™ MPE hardware units can also connect as a Wi-Fi client to an external access point and network. See Figure 2. If the unit is also cabled to a network, then the two interfaces can also be optionally bridged if access between the two networks is needed.

For Airplay Mirroring and Airplay Video, the box publishes services on the connected networks using Zero-configuration networking[3].

FIGURE 2 | COALESCE™ MPE BOX CONNECTED AS WI-FI CLIENT

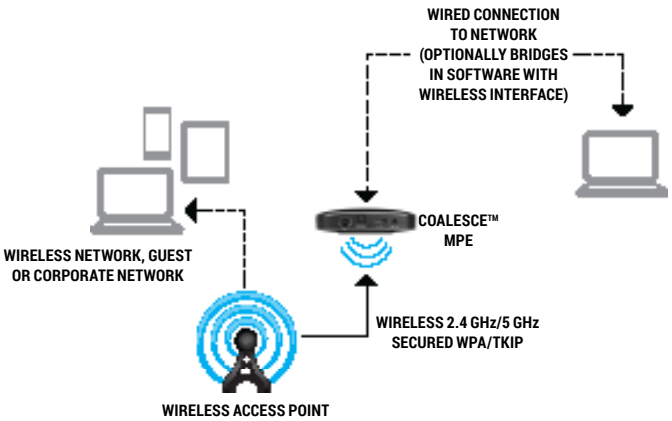
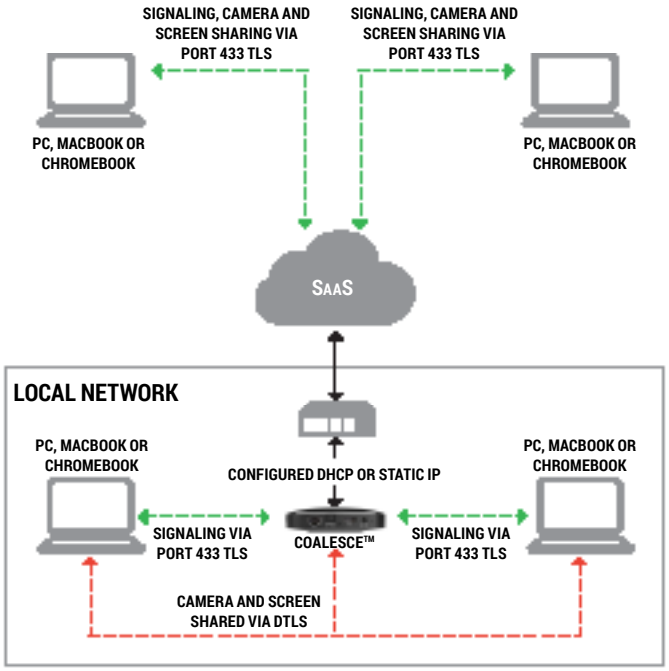


FIGURE 3 | NETWORK ARCHITECTURE OF COALESCE™ MPE, INTERNAL AND EXTERNAL CONNECTIONS.



In a typical configuration, Coalesce™ MPE is connected to an existing network infrastructure, either using a static IP or DHCP. Clients can connect via the access point on the Coalesce™ MPE unit or via the existing network infrastructure. When connected locally, then signaling data is communicated over port 443 TLS and video and audio over DTLS. When the client is connected from a remote network, then all signaling, video and audio data are relayed via our SaaS tier via port 443 TLS. See Figure 3.

2 https://en.wikipedia.org/wiki/Simple_Authentication_and_Security_Layer
3 https://en.wikipedia.org/wiki/Zero-configuration_networking

FIREWALL CONSIDERATIONS

For remote connections, receiver and clients need to be able to access the Internet through these ports:

- TCP 80
- TCP 443
- UDP 53

For local connections (i.e. clients on the same network or connecting through Coalesce™ Access Point) the following ports are used:

- UDP 1025 – 65535
- TCP 4700, 7000, 7100 (For Airplay connections)

If there is Layer 7 filtering or proxy with protocol filtering on these ports, then the following protocols will need to be allowed:

- HTTP
- HTTPS
- DTLS
- XMPP
- Bonjour protocols
- SRTP
- DNS
- STUN
- TURN
- ICE

Our SaaS provides services at the following FQDNs:

- www.joincoalesce.com
- api.joincoalesce.com
- services.joincoalesce.com
- xmpp.joincoalesce.com
- stunturn-virginia.joincoalesce.com
- stunturn-california.joincoalesce.com
- stunturn-ireland.joincoalesce.com
- stunturn-singapore.joincoalesce.com
- stunturn-mumbai.joincoalesce.com

PROXY SUPPORT

Coalesce™ MPE works on networks that require proxy configuration. The following proxy types are supported:

- HTTP Proxy (with or without authentication)
- SOCKS 5 (with or without authentication)
- Proxy with Auto-Configuration File (PAC) (with and without authentication)
- System proxy to inherit proxy settings from Windows