CONNECT

Network and Security Whitepaper

October 2018

Mosaic Connect Network and Security Guide.
Published October 2018.

Introduction

Mosaic Connect is a wireless presentation solution allowing individual connected devices to share their screen to a large format display. Mosaic Connect is available on multiple platforms:

- Windows software, available for Windows 10. This allows the Mosaic Connect software to be deployed securely across existing hardware.
- Android
    - Box based on Android 6.0.
    - Software for CVTE screens.

Note: features vary per platform

Infrastructure

All inbound and outbound data from our backend 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 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 network ports used can be found further within this document.

The backend tier provides four public services; REST API, XMPP and STUN / TURN. We use a combination of both Azure and Amazon services to provide a resilient and redundant backend whilst providing the lowest latency possible.

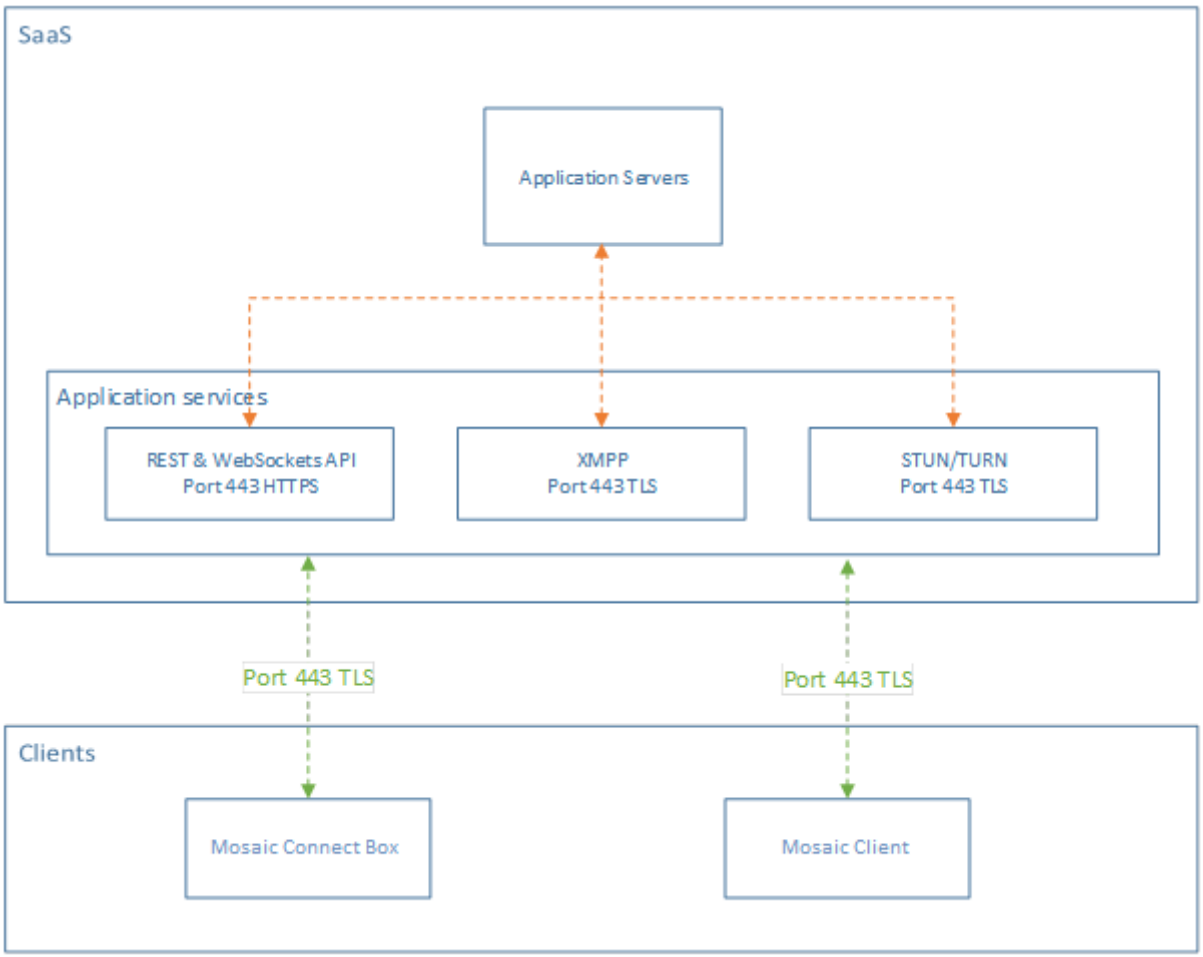

Figure 1. Mosaic Connect Architecture

Amazon AWS

Amazon AWS is a market leading cloud service managed by Amazon, a trusted provider of cloud services that offers geographical dispersion - allowing us to have a server closer to the end user, which reduces latency in cloud connectivity.
All our cloud services running on Amazon AWS are running under a Virtual Private Cloud (VPC) and each environment has its own virtual network protected by Amazon's availability zone and firewall.

Amazon AWS servers are geographically dispersed and have many certifications and third-party assessments, including ISO/IEC 27001:2005, SOC 1 and SOC 2 and CSA STAR certification[1]. Further information can be found in their security whitepaper[2].

Mosaic Connect features

The Mosaic Connect 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.

Meeting ID and PIN

For each meeting a unique meeting ID is generated using our SaaS layer which is used as a means for the clients to connect to that specific meeting. If there is an Internet connection, this meeting ID will be 6 digits long.

If no Internet is available (or local connections only is enabled) the Meeting ID will be 10 digits long. This 10 digit meeting ID is generated using the device IP address, which enables connection from different subnets on the same network.

If devices connect using the 6 digit meeting ID, connection is attempted locally, however if this is not possible then the connection is made via XMPP. The host can also specify a PIN which is configured at the box directly, and on each client connecting would request confirmation of the PIN.

Cloud

If Mosaic Connect has access to the Mosaic Connect Cloud, then it will be able to allow 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 organisation,

This can be restricted by deactivating access to the cloud in Mosaic Connect settings. The Mosaic Connect hardware units can also function solely using their access point (Android only) with each connecting device ingbe assigned an IP address.

Updates

An Internet connection is required for updates. The updates are downloaded over a secure connection (using port 443) and are installed on demand. A notification will appear in the Mosaic Connect user interface to indicate an available update that the user can install.

Security
The clients and boxes are authenticated on our servers using a 4-step authentication process with SASL[3]. At any time, administrators can remove a client or box from the authorised zone temporarily and permanently.

All data transferred between the user's device and Mosaic Connect 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 Mosaic Connect, then the software will relay the data via our TURN server over TLS TCP port 443.

Access Point and Wi-Fi

The Mosaic Connect (Android) unit offers an internal access point, secured with WPA2 with PSK encryption, allowing clients to connect directly to the box and in so creating a local network.

The Mosaic Connect Android unit can also connect as a Wi-Fi client to an external Access Point and network.

For Airplay Mirroring and Airplay Video the box publishes services on the connected networks using Zero-configuration networking [4].

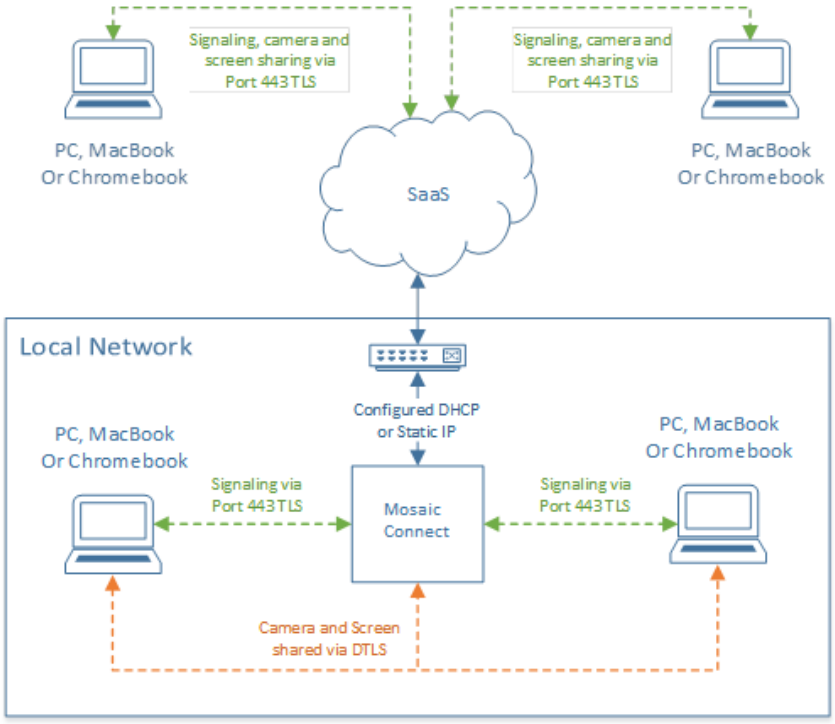

Figure 3. Network architecture of Mosaic Connect, internal and external connections.

In a typical configuration Mosaic Connect is connected to an existing network infrastructure, either using a static IP or DHCP. Clients can connect either via the access point on the Mosaic Connect (android hardware only) unit or via the existing network infrastructure.

When connected locally then signalling data is communicated over port 443 TLS and video and audio over DTLS. When the client is connected from a remote network then all signalling, video and audio data are relayed via our SaaS tier via port 443 TLS. See Figure 3.

Firewall and Proxy

Firewall

- 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 Mosaic Connect Access Point) the following ports are used;

    - TCP 1-65535 (It will be selected from available ones)
    - 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;

- netcheck.connectmosaic.com
- api.connectmosaic.com
- xmpp.connectmosaic.com
- stt01.connectmosaic.com
- stt02.connectmosaic.com
- stt03.connectmosaic.com
- stt04.connectmosaic.com
- stt05.connectmosaic.com

Proxy support

The Mosaic Connect Windows/OSX software support 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). Windows only.
- System proxy. Windows only.