MOSAIC

SECURITY & NETWORK WHITEPAPER

DisplayNote Technologies

Introduction

With Mosaic Hub, teams in different locations can work together in real-time in a collaborative workspace like as if they're all in the same room.

Mosaic brings together video, voice, collaborative white-boarding, wireless presentation and document editing into one expansive workspace.

Infrastructure

All inbound and outbound data from 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 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 Backend tier provides four public services; REST API, Displaynote Realtime Collaboration Protocol (DRCP), XMPP and STUN / TURN.

We're using two different data centers for these purposes, to have replication around the world, improving latencies and having redundant solution for failure tolerance.

These are:

We use Azure to host and support the services we offer to our clients. Azure's Datacentres are geographically dispersed and comply to ISO/IEC 27001:2005, SOC 1 and SOC 2 and has CSA STAR certification.

These Datacentres 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 our 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.

We use also Amazon AWS to host and support the services we offer to our clients. Amazon AWS are geographically dispersed and has an huge amount of certifications, reports and third parties assessment , including ISO/IEC 27001:2005, SOC 1 and SOC 2 and CSA STAR certification. And in general their security mechanism are covered by their security whitepaper .

Amazon AWS is a well known and probed set of cloud services managed by Amazon twenty years ago. It’s a global reference on cloud services and geographical dispersion, allowing us to have a server more near to the final user reducing the latency needed.

All our cloud services running on Amazon AWS are running under a Virtual Private Cloud (VPC) and all of these environments has their own virtual network under Amazon availability zone; over all of that, the network is also restricted by Amazon Firewall.

Mosaic Hub Application

The Mosaic Hub software consumes a REST API provided by our Backend layer which is credential secured. All communication with the REST API, our XMPP services and DisplayNote Realtime Collaboration Protocol (DRCP), 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.

IIn 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.

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 Mosaic Hub user interface to indicate of an update from which the user can install.

For each Mosaic Hub ID is generated mediated from our SaaS layer which is used as a means for the clients to connect to that specific Hub. The The clients and boxes are authenticated on our servers using a 4 step authentication process with SASL .

All data transferred between Mosaic Hub instances 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 box, then the software will relay the data via our TURN server over TLS TCP port 443.

Firewall Considerations

Mosaic Hub needs to be able to access the Internet through these ports:

- TCP 80
- TCP 443
- UDP 53

If you're doing Layer 7 filtering or using proxy with protocol filtering on these ports then the following protocols will need to be allowed:

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

Our SaaS provides services at the following FQDNs:

- hub.displaynote.com
- netcheck.joinmontage.com
- swoodle.displaynote.com
- xmpp.displaynote.com
- stunturn-prod-ireland.displaynote.com
- stunturn-prod-mumbai.displaynote.com
- stunturn-prod-singapore.displaynote.com
- stunturn-prod-virginia.displaynote.com
- stunturn-prod-california.displaynote.com

Proxy Support

Montage software supports working on networks that needs proxy configuration, this is the list of proxy types we support:

- HTTP Proxy (with and without authentication).
- SOCKS 5 (with and without authentication).
- Proxy with Auto-Configuration File (PAC) (with and without authentication).
- System proxy, just for Windows version to infer system wide configured proxy

Links

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

https://downloads.cloudsecurityalliance.org/star/certification/STAR-658377-Microsoft-Azure.pdf

https://d0.awsstatic.com/whitepapers/compliance/AWS_Certifications_Programs_Reports_Third-Party_Attestations.pdf

https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

https://en.wikipedia.org/wiki/Simple_Authentication_and_Security_Layer