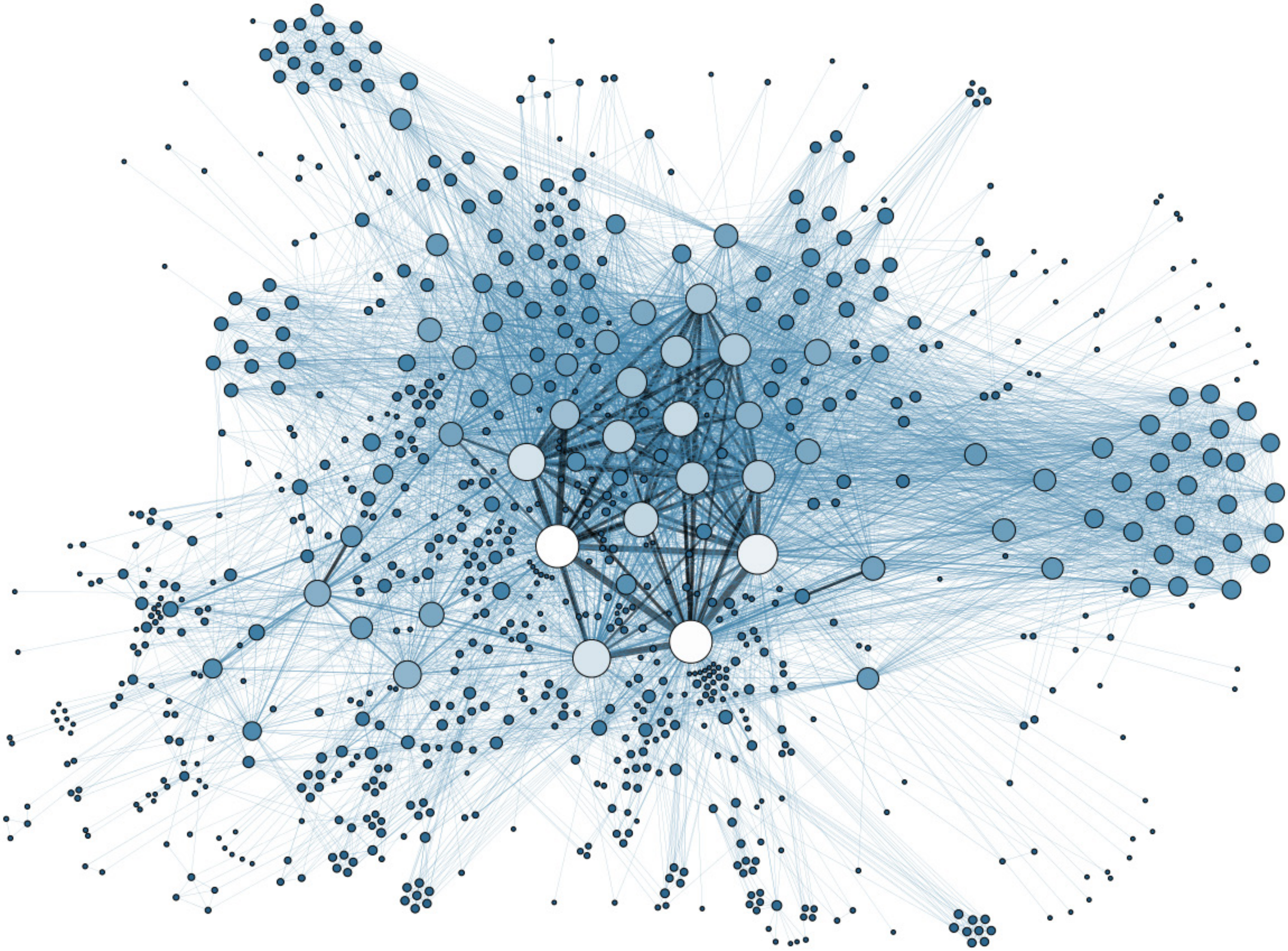
DisplayNote Technologies



Montage Security Whitepaper
DisplayNote Technologies

Introduction

Montage is a wireless presentation solution allowing connected devices to share their screen and video camera among those connected. The Montage is a tailored solution based on CentOS 7.1, an enterprise grade Linux distribution derived from the sources of Red Hat Enterprise Linux (RHEL). This provides the Montage platform a secure, stable and manageable system in which to execute. Security has been top priority in the design of the Montage platform where the operating system runs a minimal installation with a very limited set of services running.

The Montage solution has two tiers; the Software as a Service (SaaS) and the Montage appliance software with its clients.

Content

Software as a Service (SaaS)

This encompasses our application services which support authentication, REST APIs, group messaging and video collaboration services. This layer can be hosted within our cloud or hosted by the Enterprise.

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*.

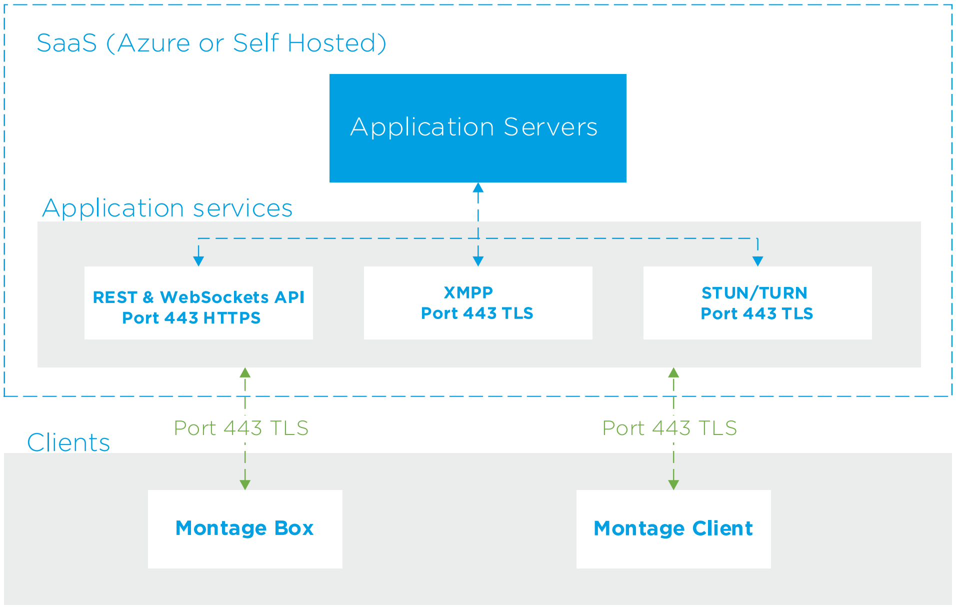


Figure 1. Montage Architecture

Azure

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.** 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.

Montage

The Montage 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 (ports: 3478, 3479) 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 (ports: 5349, 5350).

If a gateway is made available, then Montage can be configured to share the connection to devices connecting via the access point. If Montage has access to the Montage Cloud, then it will be able to allow devices connecting to it from outside of its local network - 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 settings on the Montage Box. The Montage Box can also function solely using its access point with which connecting devices will be assigned an IP address via DHCP.

In order to receive updates to the box 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 Montage user interface to indicate of an update from which the user can install. Updates can also be installed via USB disk connected to Montage if Internet cannot be made available.

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, and on each client connecting would request confirmation of the PIN.
On connecting the screen of the connected device is shared and the user can decide to continue sharing their screen and adding web camera video and audio.
The clients and boxes are authenticated on our servers using a 4 step authentication process with **SASL**.
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 Montage box 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.

The Montage box offers an internal access point, secured with WPA2 with TKIP encryption, allowing 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. *See Figure 2*.

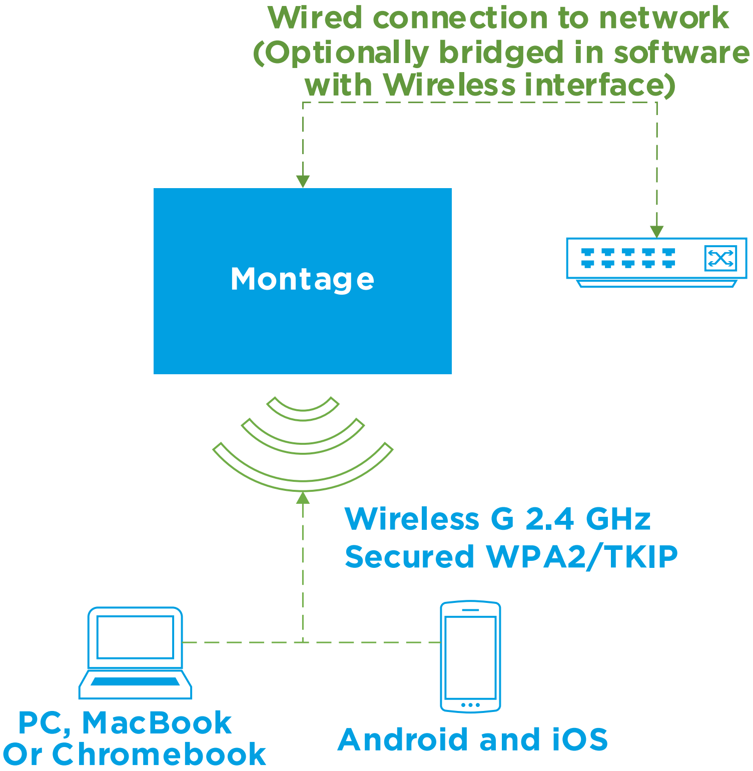


Figure 2. Montage Box running in Access Point mode.

The Montage box can also connect as a Wi-Fi client to an external Access Point and network. *See Figure 3*. If the box is also cabled to a network, then the two interfaces can also be optionally bridged if access between the two networks is needed.

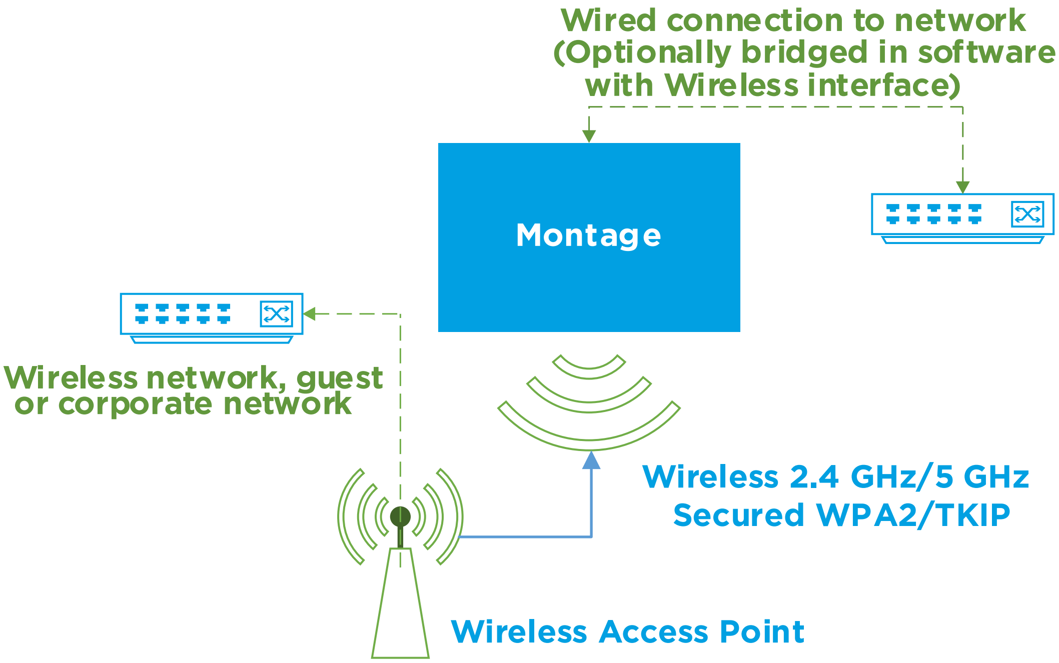


Figure 3. Montage Box connected-as WiFi client

The box also allows clients to connect via **Miracast** which is encrypted with WPA2 and Airplay which is encrypted using AES CRT128. *See Figure 4*. For Airplay Mirroring and Airplay Video the box publishes services on the connected networks using **Zero-configuration networking**.

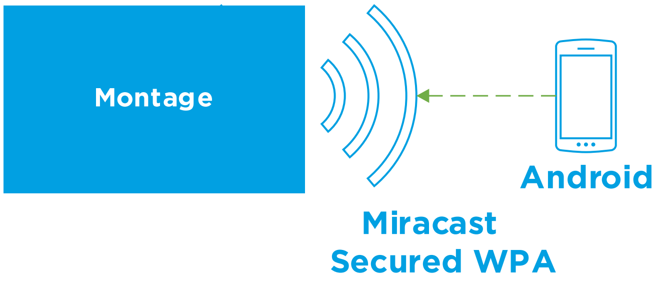


Figure 4. Montage Box running in Miracast mode

In a typical configuration the Montage Box is cabled to an existing network infrastructure, either using a static IP or DHCP. Clients can connect either via the access point on the Montage box 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 5.*

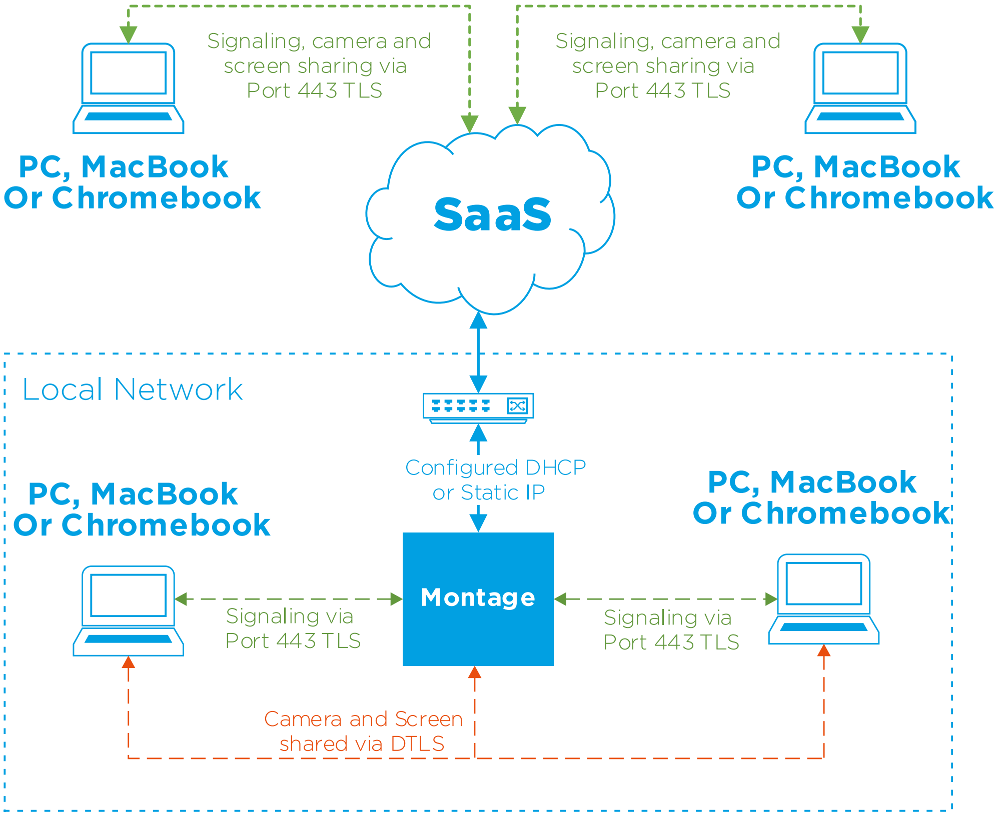

Signaling, camera and screen sharing via Port 443 TLS
Signaling, camera and screen sharing via Port 443 TLS
PC, MacBook Or Chromebook
SaaS
PC, MacBook Or Chromebook
Local Network
Configured DHCP or Static IP
PC, MacBook Or Chromebook
PC, MacBook Or Chromebook
Montage
Signaling via Port 443 TLS
Signaling via Port 443 TLS
Camera and Screen shared via DTLS

Figure 5. Network architecture of Montage, internal and external connections.

Firewall Considerations

Our client software uses ports inbound and outbound:

- TCP 443
- TCP 3478
- TCP 3479
- TCP 5349
- TCP 5350
- TCP 4700
- TCP 7000
- TCP 7100

Our SaaS provides services at the following FQDNs:

- netcheck.joinmontage.com
- montage.displaynote.com
- stunturn-mtg.displaynote.com
- google-analytics.com
- xmpp.displaynote.com