Application Note – AN17061

MT- AppNote 17061
November, 2019

MiCloud Connect Security

Security of Cloud Unified Communications Suite
Mitel Technical Content Delivery

Description: This Application Note describes the security features designed into the MiCloud Connect Unified Communications System.

Environment: MiCloud Connect System

Contents

Introduction

Security is often top-of-mind for many organizations considering moving their applications and sensitive data to the cloud, and the same goes for their consideration and usage of cloud-based unified communications as a service (UCaaS) systems. Security, for the purpose of this discussion is the resistance to, or protection from, harm. It applies to any vulnerable and/or valuable asset, such as an organization, or the organization's data.

Mitel Connect CLOUD is one of the most secure cloud communication solutions available in the market today. When we started designing Mitel Connect CLOUD, security was paramount on our mind for every part of the system that we developed.

Mitel designed the Connect CLOUD system to natively, and by default, use the most secure, industry standard protocols and systems. Protocols like HTTPS and WebRTC ride on top of TLS and include both encryption of their payload and authentication, to decrypt and allow access to the data payload. SRTP is another industry standard protocol for the transport of secure real-time data, like VoIP traffic.

There are always threats when using a publicly accessible system such as the public internet. With a cloud Connected UCaaS system however, there's more to secure than just the data travelling from the endpoint/client to the cloud system at the data center. This brief note focuses on 3 segments where security is key: Real-time data in transport to and from the data center, as mentioned, intra-system communications at the data center, and the physical security of the data centers themselves.

Additionally, monitoring of these systems for attacks and breaches is critical to maintain defense and act quickly, if needed.

Real-Time Transported Data

Endpoints to a UCaaS system include desk phones, softphones, and smartphones. These "clients" are the interface to the system and to ensure integrity, employ several layers of security.

Mitel's desk phones (all current 400 series) use industry standard HTTPS, SIP/SIPS (TLS) and SRTP (DTLS) Connections for data, signaling and real-time media respectively to secure the transport of VoIP traffic. Of note is that Mitel Connect CLOUD uses SRTP to secure real-time VoIP traffic by default, so ALL VoIP media Connections are secure. Unfortunately, some UC vendors do not support it or charge an additional fee for using SRTP.

In addition to providing for secure transport, Mitel employs Signed Firmware on these phones. Signed Firmware is a unique cryptographic signature/fingerprint, called a hash that's calculated for the firmware. Mitel secures the firmware on the phones by implementing strong cryptographic hashing and signing. The phones will only allow loading a signed image of the software which ensures the phones are operating and Connecting securely.

Further, the Connect CLOUD system is designed to ensure unauthorized IP end points cannot access system resources, while still providing plug- and-play deployment. When an IP telephone is plugged into the network, it is automatically discovered by the system and granted minimal privileges. The telephone has no feature privileges, is not able to make outbound calls, and cannot receive inbound calls. To become active with features, a user must login to the telephone with credentials that are configured by the administrator.

The Mitel Connect Desktop client and Teamwork for Web use HTTPS for all data transfers to the Connect CLOUD data center servers. Mitel Connect Teamwork and Mitel Connect Mobility softphone apps use WebRTC (HTTPS, DTLS) for both signaling and media.

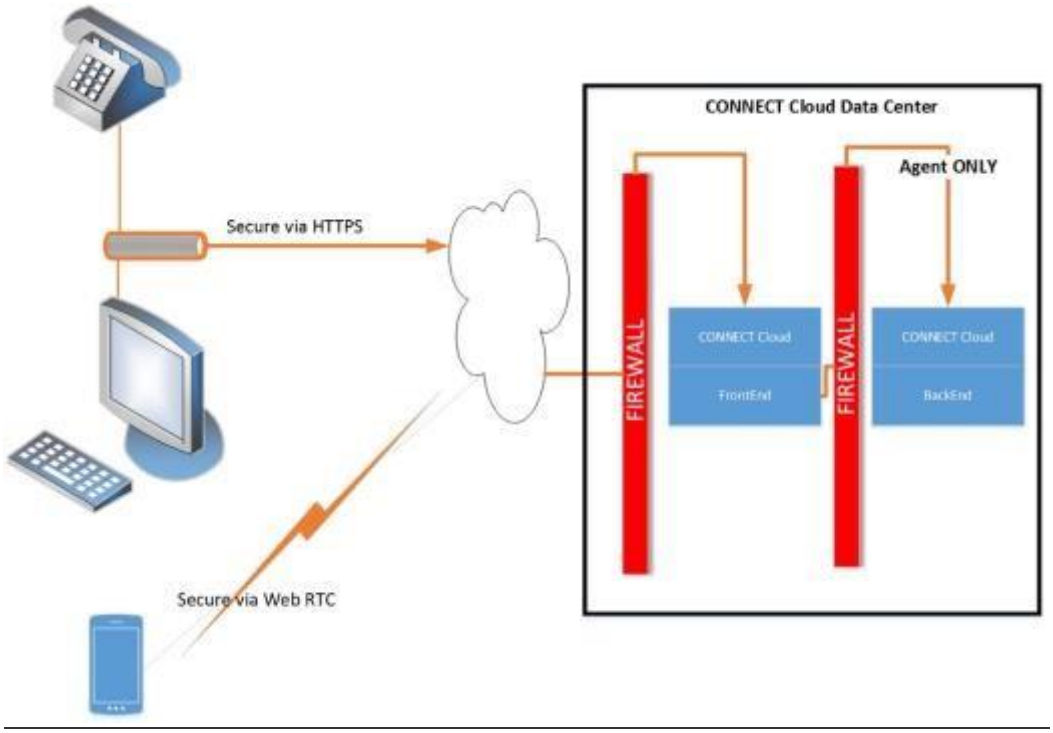

Figure 1 - Secure Communication from Endpoints

Intra Data Center Communications

Upon arriving at the data center, traffic must traverse several layers of outer shells in the form of firewalls. In the case of normal operations, traffic traverses the first layer of firewall security and then must traverse a second layer before arriving at the core of the UC system. In fact, users can not traverse this second layer so a user's or endpoint's agent takes over the responsibility of moving the traffic thru the second firewall. To be clear, no user traffic can reach the beyond the inner firewall to the backend system layer. It must be controlled by a system agent. Where possible, the internal protocols for intra data center communication are also secure, so there is a high level of defense in the cloud.

The physical data centers hosting the Mitel Connect CLOUD systems are very secure facilities. They are compliant with/to ISO/IEC 27001, ISO 9001 BSI, ISAE 3402 Type II. More information can be found at: https://community.rackspace.com/products/f/25/t/7777

Mitel NOC

Mitel operates two Network Operations Centers (NOCs) to monitor and control the daily operations of all Connect CLOUD systems. These NOCs are staffed 24 hours / 7 days a week by Mitel engineers who monitor normal daily operations or, in the case of an emergency, ensure that counter measures are taken to ensure access to the systems is not compromised. Should traffic appear to be intrusion, the Mitel Network Operations Center (NOC) alerts to the situation and addresses it, as needed.

Telephony Class of Service Protection

The IP telephony system itself should protect companies against service thefts such as toll fraud and feature abuse. That protection is built right into the Mitel Connect CLOUD System. With Mitel, anything that costs your organization money or can lead to feature abuse can be controlled through class of service. This includes the ability to restrict calling (i.e., long distance and international), overhead paging, trunk-to-trunk transfers, and transferring and forwarding to external numbers. Connect CLOUD gives administrators complete control over telephony, call and voice mail feature permissions.

Users are placed into user groups which in turn are assigned telephony, call, and voice mail permissions.

The following telephony permissions can be controlled:

- Maximum Number of Calls
- Maximum Buddies per User
- Maximum Parties in Make Me Conference
- Allow Inter-site Video Calls
- Allow Call Pickup
- Allow Trunk-to-Trunk Transfer
- Allow Overhead and Group Paging
- Allow Make Hunt Group Busy
- Allow Extension Reassignment
- Allow PSTN Failover
- Show Caller ID on Monitored Extensions
- Allow Customization of IP Phone Buttons
- Show Extensions with Different Prefixes
- Allow Collaboration Features
- Allow Recording of Own Calls
- Allow Directed Intercom / Paging
- Accept Director Intercom / Paging
- Allow Barge In
- Accept Barge In
- Allow Record Other's Calls
- Accept Record Other's Calls
- Allow Silent Monitor Other's Calls
- Accept Silent Monitor Other's Calls
- Allow Call Handling Changes
- Allow External Call Forwarding and Find Me Destinations

The following call permissions can be controlled:

- Internal Only
- Local Only
- National Long Distance
- National Mobile International Long Distance
  - Wildcards allow complete customization of outbound calling

The following voice mail permissions can be controlled:

- Maximum Incoming Messages
- Incoming Message Length
- Outgoing Message Length
- Saved / Unheard Message Retention Period
- Heard Message Retention Period
- Lifespan of Voice Mail Password
- Allow Access to Broadcast Distribution List
- Allow Access to System Distribution Lists
- Allow Message Notification
- Allow Message Notification to Ext. Number

The Connect CLOUD system also supports authorization codes and associated reporting. This allows users with the proper authorization to place outbound calls from restricted telephones.

The Connect CLOUD system has been purposely designed not to provide dial tone to any calling party from the voice mail user interface. This reduces the chance of someone hacking the credentials on a mailbox and having free calling anywhere in the world. Other UC systems that support “Direct Inward System Access (DISA)” can expose the customer to potential toll fraud.

Conclusion

Mitel understands the value of your data and designed the Connect CLOUD system with the highest level of security to provide for a world-class, secure, cloud-based unified communications suite that you can count on to provide a secure environment for your company’s critical operations and data.

Glossary

Data Center TIA942 https://en.wikipedia.org/wiki/TIA-942

DTLS is a communications protocol that provides security for datagram-based applications by allowing them to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
https://en.wikipedia.org/wiki/Datagram_Transport_Layer_Security

Firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules
https://en.wikipedia.org/wiki/Firewall_(computing)

HTTPS is a communications protocol for secure communication over a computer network which is widely used on the Internet
https://en.wikipedia.org/wiki/HTTPS

Network Operations Center (NOC) is a location from which network monitoring and control or management, is exercised over a computer or telecommunications network
https://en.wikipedia.org/wiki/Network_operations_center

Session Border Controller (SBC) is a device to control the signaling and media streams involved in telephone calls or other interactive media communications https://en.wikipedia.org/wiki/Session_border_controller

Single Sign-On (SSO) is a property of access control of multiple related, yet independent, software systems to gain access to a Connected system or systems without using different usernames or passwords
https://en.wikipedia.org/wiki/Single_sign-on

Session Initiation Protocol (SIP) is a communications protocol for signaling and controlling multimedia communication sessions in applications of Internet telephony for voice and video calls
https://en.wikipedia.org/wiki/Session_Initiation_Protocol

SRTP defines a secure profile of RTP (Real-time Transport Protocol), intended to provide encryption, message authentication and integrity, and replay protection to RTP data https://en.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol

TLS is a cryptographic protocol that provides communications security over a computer network
https://en.wikipedia.org/wiki/Transport_Layer_Security

WebRTC is a collection of communications protocols and application programming interfaces that enable real-time communication
https://en.wikipedia.org/wiki/WebRTC

Version	Date	Contributor	Content
1.0	November, 2017	J. Mancebo	Original App Note