Unified Communications Private Cloud

By

Adam Colwell & Erich Botzki

Submitted to
the Faculty of the School of Information Technology
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

Adam Colwell — Date: 4/17/17

Erich Botzki — Date: 4/17/17

Brian Verkamp, Faculty Advisor — Date: 4/17/17

Bogdan Vykhovanyuk, Faculty Advisor — Date: 4/17/17

University of Cincinnati
College of
Education, Criminal Justice, and Human Services

April 2017

TABLE OF CONTENTS

FIGURES TABLE OF CONTENTS

TABLES TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS

ASA	Advanced Security Appliance
CUCM	Cisco Unified Communications Manager
DHCP	Dynamic Host Control Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
GUI	Graphical User Interface
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISDN	Intergraded Services Digital Network
IT	Information Technology
LAN	Local Area Network
MRA	Mobile Remote Access
MPLS	Multiprotocol Label Switching
OVA	Open Virtual Appliance
P2P	Peer to Peer
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SBC	Session Border Controller
SFTP	Secure File Transfer Protocol
SIP	Session Initialization Protocol
SME	Session Management
SRND	Solutions Reference Network Design
SSL	Secure Socket Layer
SSLVPN	Secure Socket Layer Virtual Private Network
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UC	Unified Communications
UCS	Unified Communications Server
VCS C	Video Communications Server Controller
VCS E	Video Communications Server Edge
VM	Virtual Machine
VoIP	Voice/Video over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

ABSTRACT

Organizations have deployed independent phone systems using traditional PSTN (Public Switched Telephone Network) trunks that are costly and often are negotiated into term-based contracts. Many companies have multiple office locations that have Internet, MPLS (Multiprotocol Label Switched) and/or VPN (Virtual Private Network) connections. The Unified Communications Private Cloud solution uses these existing connections to allow each user the ability contact one another regardless of geographic location. Unlike traditional cellular phones this solution offers G.722 codec calls (HD Voice) and H.264 codec connections (High Definition Video) while being secure. Some key benefits of this solution are that the user experience is synonymous across all locations, administrators centrally manage the solution for all locations, connectivity can be LAN (local area network) or via internet. Users can move devices without involving system administrators on their own. The UC (Unified Communications) Private Cloud is organic as it expands and contracts with business needs.

1.0 PROBLEM STATEMENT

1.1 Introduction

The UC Private Cloud solution is geared towards companies that would like to leverage their existing network infrastructure for voice and video communications. Companies typically use standalone communications systems that connect to legacy PSTN networks. For companies with multiple locations, these systems are managed individually and are often disparate systems.

1.2 Project Description

We designed and implemented a voice and video solution that allow users on and off the company's network to communicate via voice and video. This cloud voice and video solution is centrally located and managed. The on-network users utilize the company's existing network infrastructure to connect their Session Initialization Protocol (SIP) endpoint to the VoIP Cloud solution. Remote or off network users connect using their own broadband internet connection from their SIP endpoint. The VoIP cloud solution uses traditional Virtual Private Network (VPN) technologies for remote user's providing a secure tunneled connection over the internet.

1.3 Problem

Companies with multiple locations normally use traditional stand-alone voice and video Systems. These solutions are proprietary and costly to manage. Each location has its own PSTN access lines and the systems are administered individually. To connect each standalone system together a tie line is required between all the systems along with a complex dial plan that must be managed in each system. This creates exponential work for administrators, as they must access each system individually to make changes etc. The tie lines used for this effort are typically integrated in the PSTN lines connected from the local carrier to the site, which come at an added cost. Most if not all the office locations have, an existing MPLS or Peer-to-Peer (P2P) VPN connection for Internet Protocol (IP) connectivity and these standalone systems do not leverage that existing connectivity.

1.4 Solution

The solution to simplify a company's dial plan and connect locations together in an economical manner is the Private Cloud VoIP solution. The UC Private Cloud solution allows users the ability to call via voice or video across geographical locations using existing LAN and Wide Area Network (WAN) connections. This will significantly lower long-distance calling costs, as locations will not need PSTN circuits. The solution allows administrators to have a single system to perform profile administration for all users.

1.5 User Profile

There are two major user groups for this setup as well as the end users who will use the system. The first of the major user groups are service providers that provide VoIP services to companies that are not large enough to host their own VoIP/Unified Communications system but need the capabilities they provide. The second are large, geographically spread out company locations that need the ability to have a centrally managed VoIP/Unified Communications system for widely dispersed offices. Lastly, the end users of the system would be anyone who uses a voice or video endpoint as part of their daily routine at work, as you can see in *Table 1* on page 6.

1.5.1 Service Provider

Service providers that wish to provide off premises UC solutions to their customers currently provide insecure solutions. Given the use case, service providers will be able to provide secure, advanced UC solutions to customers who require only a small phone system that is both secure but has advanced features that are always up to date and always available.

1.5.2 Large Corporation

Large corporations that wish to provide a phone system to highly dispersed offices and location currently must have complex system that are connected by dedicated connections or many small individual systems that are not interconnected. Given the use case, large corporations will be able to configure one centrally managed UC system. They will also allow remote locations to use the same system securely.

1.5.3 End Users

End users are people, most likely working, who use a desk phone or soft phone as part of their daily routines. Given this use case, end users essentially see no difference in how they use their phones than they do any other phone or endpoint. *Figure 1* below on page 5 identifies the tasks that the two end users, the system administrators and UC endpoint users, would perform on a regular basis.

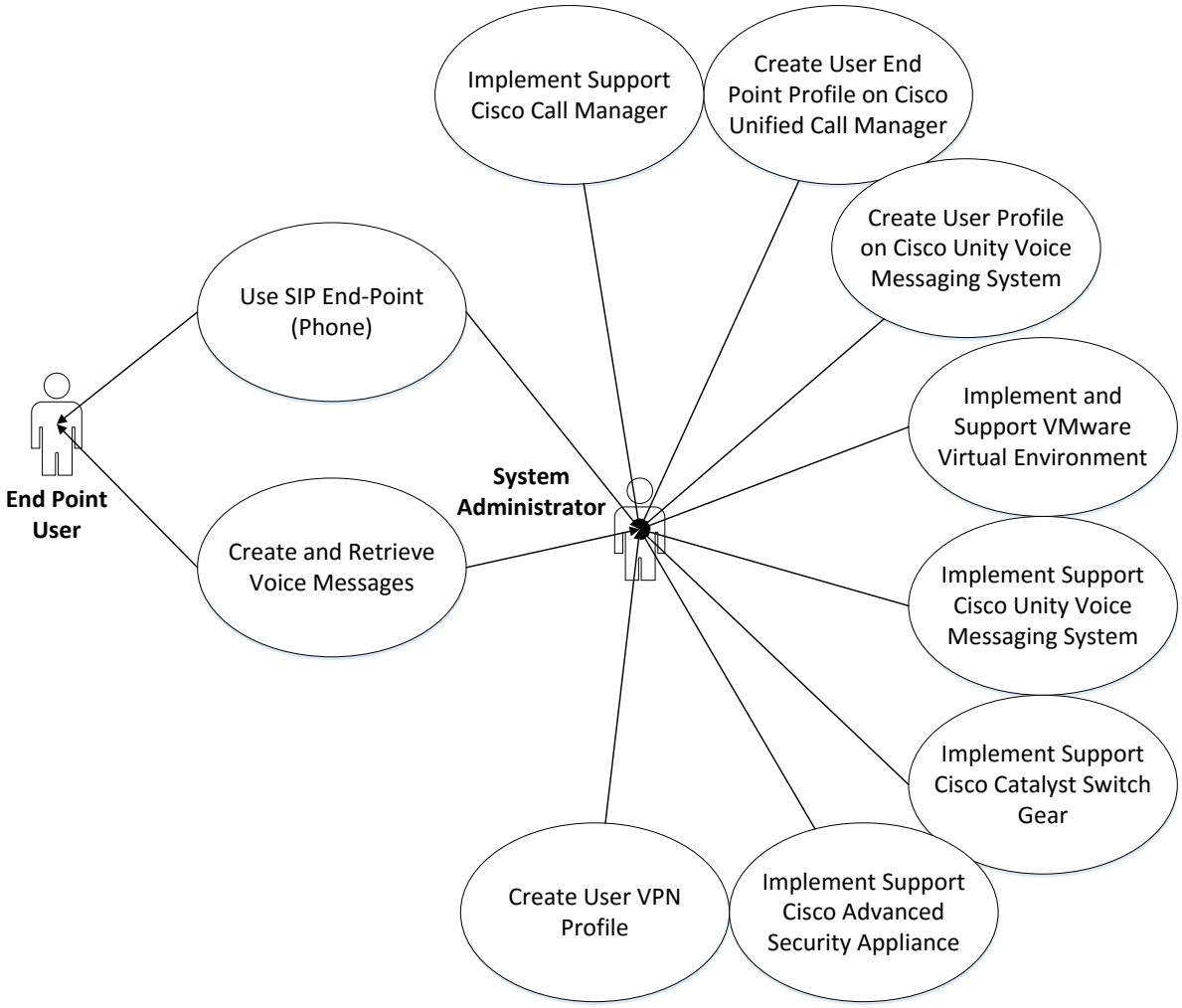


Figure 1: User Profile Diagram

User Profile Form
Application: UC Private Cloud Solution
Potential Users UC System Administrators UC Endpoint Users
Software and Interface Experience: Cisco Unified Call Manager & Cisco Unity VMware – Virtualization environment Cisco Advanced Security Appliance Cisco Catalyst Switch Gear Traditional Phone and Cell Phone
Experience with Similar Applications: Voice & Video over IP Phone Systems VMware Environments IP Network Infrastructure Traditional Telephone & Communications Endpoints
Task Experience: Deploy VMs Interaction between multiple virtual machines Setting up a Unified Communications system Set up Cisco Security Appliances Using a phone
Frequency of Use: Initial Setup of the UC Cloud Solution Operation Support of UC Cloud Solution Daily use of Cloud VoIP System
Key Interface Design Requirements that the Profile Suggests: N/A – The systems interfaces are pre-built GUI systems of the used products the challenge is configuring them to do what we require of them.

Table 1: User Profile Form

2.0 PROJECT MANAGEMENT

2.1 Objectives/Deliverables

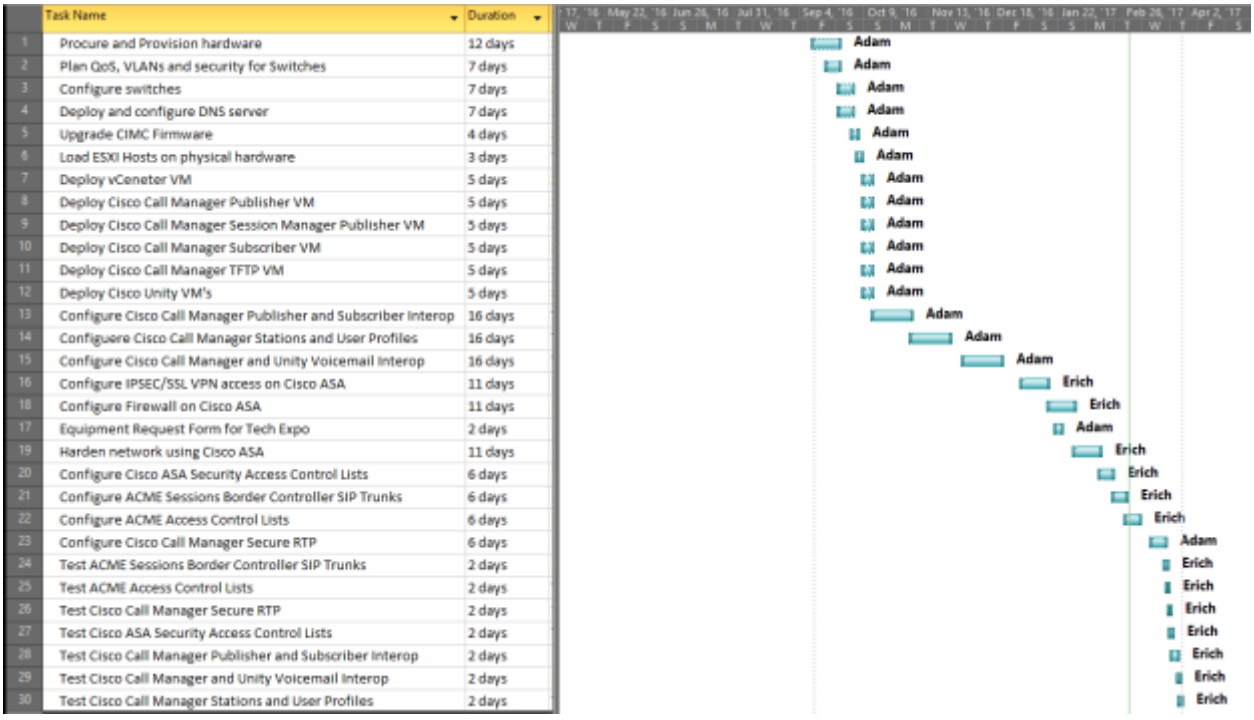
Table 2 below shows the project deliverables with associated delivery dates.

Table 1. Major Project Milestones (Deliverables)			
Planning Milestone	9-19-2016	SIP Endpoint Deployment	11-24-2016
Network Deployment	10-2-2016	VoIP Cloud Presentation S-1	11-30-2016
UCS Server Deployment	10-7-2016	Harden System Security	3-24-2017
VMWare Deployment	10-13-2016	Local VoIP User Testing	3-29-2017
CUCM Deployment	11-3-2016	Remote VoIP User Testing	3-29-2017

Table 2: Objectives/Deliverables

2.2 Project Schedule

Figure 2 below shows the project tasks with associated duration and dates.



	Task Name	Duration
1	Procure and Provision hardware	12 days
2	Plan QoS, VLANs and security for Switches	7 days
3	Configure switches	7 days
4	Deploy and configure DNS server	7 days
5	Upgrade CIMC Firmware	4 days
6	Load ESXI Hosts on physical hardware	3 days
7	Deploy vCeneter VM	5 days
8	Deploy Cisco Call Manager Publisher VM	5 days
9	Deploy Cisco Call Manager Session Manager Publisher VM	5 days
10	Deploy Cisco Call Manager Subscriber VM	5 days
11	Deploy Cisco Call Manager TFTP VM	5 days
12	Deploy Cisco Unity VM's	5 days
13	Configure Cisco Call Manager Publisher and Subscriber Interop	16 days
14	Configuere Cisco Call Manager Stations and User Profiles	16 days
15	Configure Cisco Call Manager and Unity Voicemail Interop	16 days
16	Configure IPSEC/SSL VPN access on Cisco ASA	11 days
18	Configure Firewall on Cisco ASA	11 days
17	Equipment Request Form for Tech Expo	2 days
19	Harden network using Cisco ASA	11 days
20	Configure Cisco ASA Security Access Control Lists	6 days
21	Configure ACME Sessions Border Controller SIP Trunks	6 days
22	Configure ACME Access Control Lists	6 days
23	Configure Cisco Call Manager Secure RTP	6 days
24	Test ACME Sessions Border Controller SIP Trunks	2 days
25	Test ACME Access Control Lists	2 days
26	Test Cisco Call Manager Secure RTP	2 days
27	Test Cisco ASA Security Access Control Lists	2 days
28	Test Cisco Call Manager Publisher and Subscriber Interop	2 days
29	Test Cisco Call Manager and Unity Voicemail Interop	2 days
30	Test Cisco Call Manager Stations and User Profiles	2 days

Figure 2: Project Schedule and Gantt Chart

2.3 Budget

Table 3 below shows the VoIP Cloud project budget from the perspective of real world costs. The total cost of this project would be $23,360 (WestCon Comstor Group 2016) however, because this was a Senior Design project and Cincinnati Bell Technologies donated the equipment for this effort our costs are $0.00.

VoIP Cloud Project Budget			
Item	Unit Each	Qty	Line Item Total
Cisco 5510 ASA	$150.00	1	$150.00
Cisco ASA Platform Licensing	$110.00	1	$110.00
Cisco 3750 Catalyst Switch	$400.00	2	$800.00
Cisco C210 UCS Server	$500.00	2	$1000.00
Cisco CUWL User Licensing	$580.00	10	$5,800.00
ACME 3800 SBC	$2000.00	1	$2000.00
ACME Session 250 Session Licensing	$1000.00	1	$1000.00
Implementation Labor	$100.00	125	$12,500.00
			Total $23,360.00

Table 3: VoIP Cloud Project Budget

3.0 TECHNICAL ELEMENTS

3.1 Network

The UC Private Cloud solution is deployed on a company's existing LAN and WAN infrastructure. Users that are in a company office use the company's existing LAN connections to connect their SIP endpoints to the VoIP Cloud. Company LAN/WAN network infrastructure will have 802.1 p/q implemented for Quality of Service (QoS). Remote office workers without a company LAN/WAN connection use a broadband internet connection to create a VPN tunnel from the SIP

endpoint to the UC Private Cloud solution. All SIP endpoints that connect via a VPN tunnel over internet connections do not have QoS and are best effort.

3.2 Virtual Environment

The UC Private Cloud solution is deployed as Open Virtual Appliance (OVA) templates onto VMware ESXI hosts. These hosts are running on Cisco Unified Communications Servers (UCS) meeting the Solutions Reference Network Design (SRND) guide requirements for Cisco Call Manager and Cisco Unity Messaging. The Virtual Machines (VM) are managed by either VMware vSphere or VMware vCenter.

3.3 VPN/Security

Security is a major concern with this solution, since the main goal of this solution is for voice traffic to travel over the public internet the data must be secured. This implementation uses Secure Socket Layer Virtual Private Network (SSLVPN) tunnels from SIP endpoints, over the internet, to the VoIP cloud. This solution fully encrypts the data to make it near impervious to any form of snooping attack that may be encountered. The implementation utilizes Cisco Advanced Security Appliance (ASA) set up as a; firewall, antivirus system, and as an Intrusion Detection System/ Intrusion Prevention System (IDS/IPS), to protect all the VoIP equipment from many if not most hostile attacks that would compromise the system. A detailed vulnerability test is performed to verify that known vulnerabilities are patched or workarounds found to ensure the security of the UC Private Cloud Solution.

3.4 Backup/Disaster Recovery

The Cisco Call Manager and Unity Voice Messaging servers are backed up via Secure File Transfer Protocol (SFTP) to a centralized server. This server can be located offsite for disaster recovery purposes. In this instance for our Senior Design project, it is in the same location as the Cisco Voice Application Servers.

4.0 VOIP PRIVATE CLOUD ARCHITECTURE

4.1 VoIP Private Cloud High-level Diagram

Figure 3 on page 11 shows a high-level view of the VoIP Private Cloud architecture and network diagram. This includes the location of the SIP endpoints, ASA, Video Communications Server Edge (VCS E) and the ACME Session Boarder Controller(SBC), Cisco Catalyst 3750 layer 3 switch, Cisco C210 virtual environment, which houses the Windows Domain Name System(DNS) server, Cisco Call Manager server, Cisco Unity Messaging server and Cisco Video Communications Server Control (VCS C). These devices are interconnected with the proper telecommunication cables.

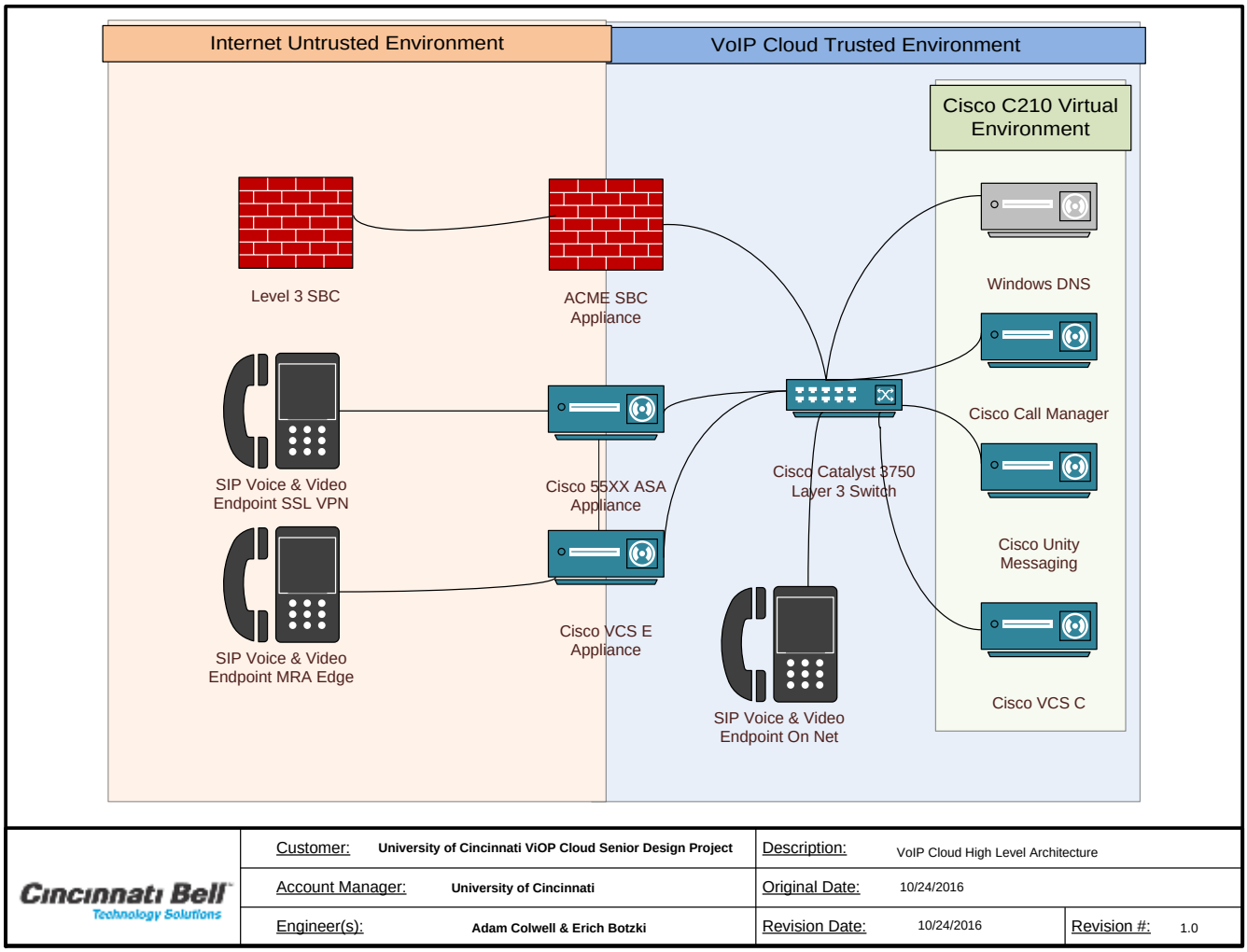


Figure 3: High-level Diagram

4.2 VoIP Private Cloud VMware Server Environments

Figure 4 and *Figure 5* below show the Cisco UCS C210 VM layouts and how the virtual servers are deployed on the 2 physical UCS C210s. Specifically how UCS C210-1 contains the Cisco Unified Communications Manager (CUCM) publisher, and CUCM subscriber 1 as well as the Session Management Edition (SME) Subscriber 0. UCS C210-2 will contain CUCM Subscriber 0, SME publisher 0, Video Communications Server Control (VCS-C) and the Windows DNS server.

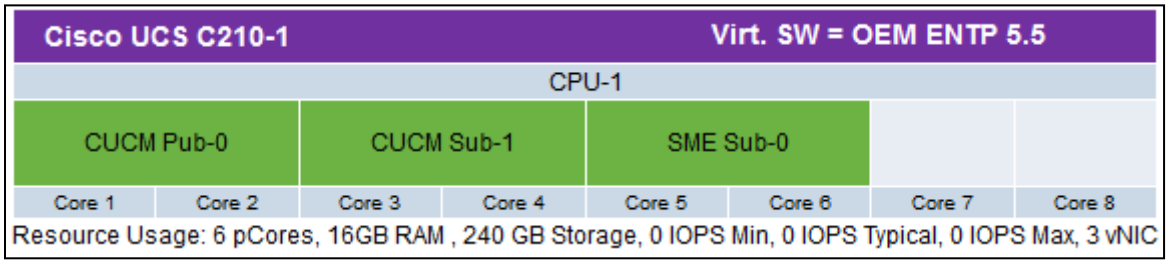


Figure 4: C210-1 Layout

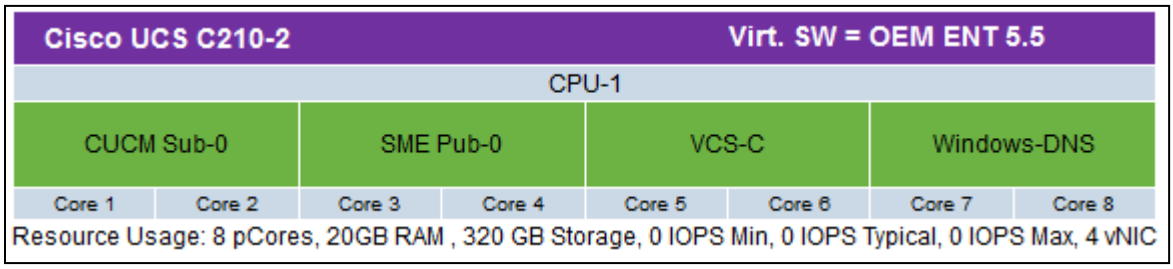


Figure 5: C210-2 Layout

5.0 TESTING

5.1 Overview

The testing section of this document will explain the testing methodology for the UC Private Cloud system and should be used as a guide. The following individuals should use this section:

- Managers
- Team Members

5.2 Scope

The scope of testing is to test the operation and functionality of the UC Private Cloud and its devices, as they would be used in a production environment.

5.3 Objective

The objective of testing is to verify and ensure that the endpoints are all able to connect to the Unified Communications Private cloud system and then contact other endpoints. These tests are to test the endpoints in all predicted scenarios and situations. Managers or team members will run the tests for the situations that are to be expected to be encountered using the Unified Communications Private Cloud.

5.4 Entry and Exit Criteria

5.4.1 Entry Criteria

- Completion of setting up new configuration settings, users, and endpoints
- Access to new location where endpoints could be used.
- Final setup is complete

5.4.2 Exit Criteria

- All tests are run
- All issues and errors are documented and rectified
- All Vulnerabilities are documented and rectified if practical and feasible

5.5 Logging and Test Reporting

If an issue or error is discovered while testing then, the tester will document the error/issue. The managers will then consider what configuration or setting error could cause the error/issue or if it is a system problem. Once issues/errors are decided on, the managers will fix any configuration or settings issues or escalate the errors/issues to outside help if it is a system problem. The order or the fixes implemented will be determined by the severity of the error/issue.

5.6 Testing Procedures

- The following are steps that are needed for testing consisting of:

- Create all the test scenarios and test cases

- Create a document of all the steps to use to conduct the test and there expected results

- Report on issues/errors/vulnerabilities and any system problems in the correct report

- Below are the tests that will be performed:

- General Back End Configuration tests – These tests will focus on back end configuration settings to ensure that back end communication settings are correct

- Call Usability Testing – this test will focus on if calls coming from different configurations and locals can be connected to each other.

- Vulnerability Analysis – This test will focus on searching the Unified Communications Private Cloud and its endpoints for vulnerabilities that can be exploited.

5.7 Pass/Fail Conditions

General Back End Configuration tests must all pass before other tests can be completed. If any part fails, the issue will be documented and rectified. It will be expected that an endpoint must all pass the Call Usability Test in its expected situation. If it does not pass, the tester will document the issue. All devices will also pass a vulnerability analysis with any found vulnerabilities being documented.

5.8 Test Plan Documentation

5.8.1 General Back End Configuration Test Plan

Table 4 shows the general back end configuration test plan and what is expected of the system to work as designed after some configuration.

General Back End Configuration Test Plan						
Participant(s)	**Date**	**Test No.**	**Test Name**	**Counts**	**Expected Results**	**Results**
Adam / Erich	**1/29/17**	**1.01**	**CUCM Registrations**	**N/A**	6 Registered Devices	Pass
Adam / Erich	**1/29/17**	**1.03**	**On Net Web GUI Access to CUCM**	**N/A**	Accessible Web GUI	Pass
Adam / Erich	**1/29/17**	**1.04**	**On Net Web GUI Access to Unity**	**N/A**	Accessible Web GUI	Pass
Adam / Erich	**1/29/17**	**1.05**	**CUCM Phone Reboot/Registration**	**N/A**	Device Re-registers	Pass
Adam / Erich	**1/29/17**	**1.06**	**On Net Vsphere to vCenter**	**N/A**	Accessible vCenter	Pass
Adam / Erich	**1/29/17**	**1.07**	**CUCM Database Replication**	**N/A**	Database Summary equal to 10	Pass
Adam / Erich	**1/29/17**	**1.08**	**On Net Web GUI Access to CIMC**	**N/A**	Accessible Web GUI	Pass
Adam / Erich	**1/29/17**	**1.09**	**On Net RTMT Access**	**N/A**	Accessible RTMT Client	Pass
Adam / Erich	**1/29/17**	**1.10**	**ACME SBC Session Agents**	**N/A**	Agents show I for in-service	Pass

Table 4: General Back End Configuration Test Plan

5.8.2 Call Usability Test Plan

Table 5 presents the plan of what endpoints will be tested in what situation and what the end call destination will be and its expected results.

Call Usability Test Plan

Participant(s)	Date	Test No.	Test Call	Call From Number	Call To Number	Expected Results	Test Results
Adam / Erich	1/29/17	2.01	On Net Cisco to Local Level 3	12133944710	15132411010 / 15135659890	Call Successful	Pass
Adam / Erich	1/29/17	2.02	Local Level 3 DID to On Net Cisco	12165383677	12133944710	Call Successful	Pass
Adam / Erich	1/29/17	2.03	Local Level 3 DID to VPN Cisco	12165383677	12133944710	Call Successful	Pass
Adam / Erich	1/29/17	2.04	Local Level 3 DID to MRA Cisco	12165383677	12133944710	Call Successful	Pass
Adam / Erich	1/29/17	2.05	On Net Cisco to LD Level 3	12133944710	13122222222	Call Successful	Pass
Adam / Erich	1/29/17	2.06	On Net Cisco to Int. Level 3	12133944710	1161396694916	Call Successful	Pass
Adam / Erich	1/29/17	2.07	On Net Cisco to On Net Cisco	12133944710	12133944711	Call Successful	Pass
Adam / Erich	1/29/17	2.08	VPN Cisco to On Net Cisco	12133944710	12133944711	Call Successful	Pass
Adam / Erich	1/29/17	2.09	MRA Cisco to On Net Cisco	12133944710	12133944711	Call Successful	Pass
Adam / Erich	1/29/17	2.10	On Net Cisco to On Net Cisco	12133944710	12133944711	Call Successful	Pass
Adam / Erich	1/29/17	2.11	MRA Cisco to MRA Cisco	12133944710	12133944711	Call Successful	Pass
Adam / Erich	1/29/17	2.12	VPN Cisco to VPN Cisco	12133944710	12133944711	Call Successful	Pass
Adam / Erich	1/29/17	2.13	On Net to VM MWI On/Off Cisco Unity	12133944710	15132143272	Call Successful	Pass

Table 5: Call Usability Test Plan

5.9 Vulnerability Testing

The Unified Communications Private Cloud system will also undergo vulnerability analysis on all severs and several endpoints to test for vulnerabilities. A full report will be completed with any recommendations implemented if the ability exists. There are three areas of concern for the vulnerability analysis as shown below.

1. An internal analysis on the phones external to the security appliances

2. An internal analysis on all the equipment behind the firewalls and security appliances

3. An external analysis on the security appliances themselves trying to find exploitable vulnerabilities

Figure 6 illustrates a high-level overview of the vulnerability analysis as well as from where each analysis was administered. The vulnerability scan was completed while connected to the same LAN or from an external network such as the internet.

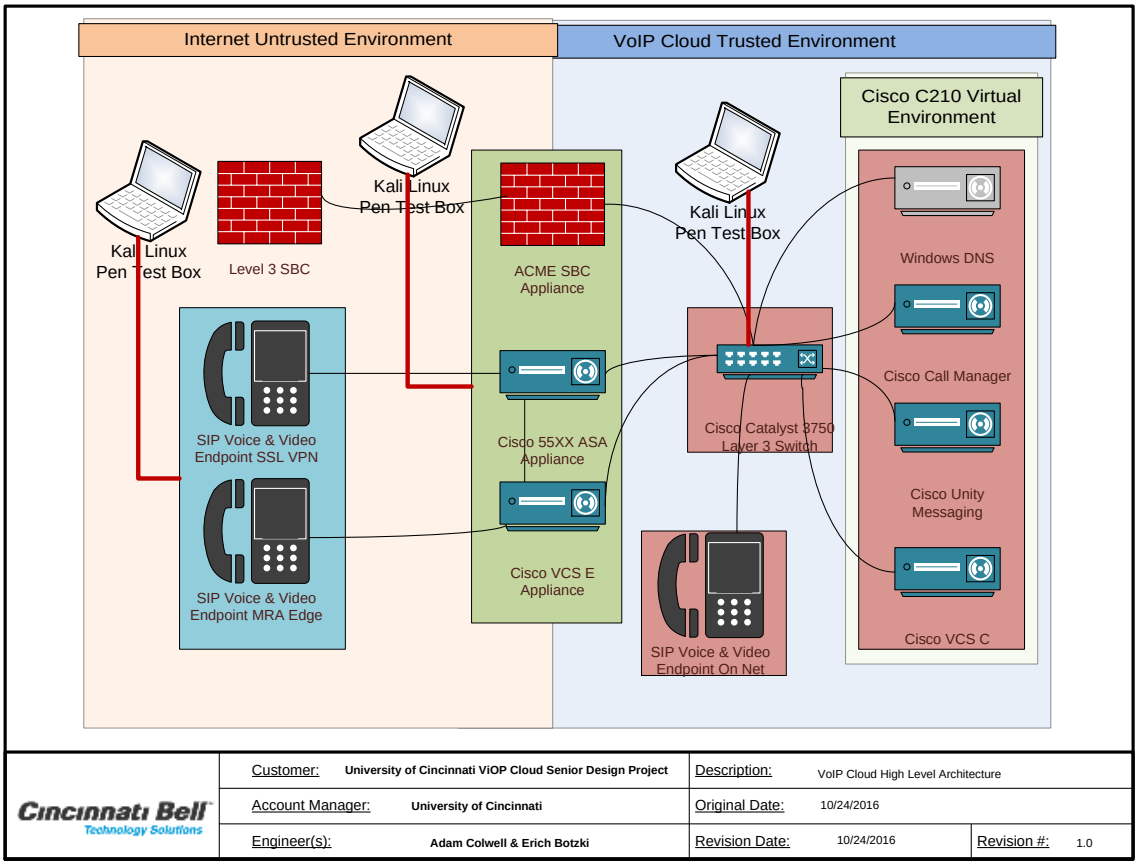


Figure 6: Vulnerability Analysis

6.0 CONCLUSION

6.1 Fall Semester 2016

During the Fall Semester of 2016, the group implemented the basic design and standing up of the VoIP Cloud infrastructure. This was set up in a lab-testing environment with outside internet access. The setup had basic functionality with some basic configurations already loaded for administrative use.

6.2 Spring Semester 17

The Unified Communications Private Cloud Solution was completed and fully functional in the 17 Spring Semester. The remaining tasks that have been completed were:

1. Deployment and configuration of Cisco Call Manger
2. Deployment and configuration of Cisco Unity Voice Messaging
3. Deployment and configuration of security appliances
4. Penetration testing of system to ensure it is secure
5. End user testing for both internal and external connections

After these tasks, were completed, the Unified Communications Private Cloud solution shows a test case that the plan is viable and able to be shown off to CBTS customers as alternatives to current communication solutions.

7.0 WORKS CITED

WestCon Comstor Group. *WestCon Comstor Group Pricing Portal.* 2016. https://www.westconcomstor.com/global/en.html#home (accessed October 19, 2016).

AI APENDIX I

VULNERABILTIY ANAYLSIS

This section goes over the vulnerability analysis and what the planned solutions are for all medium or higher potential problems.

AI.I Unity Voice Messaging

Medium (CVSS: 4.0)

NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate chain that has been signed using a crypto-graphically weak hashing algorithm.

What we would do to rectify this.
In a real implementation, we would use certificates from the companies CA using the most secure certificate signing available thereby eliminating this problem

Medium (CVSS: 4.3)

NVT: SSH Weak Encryption Algorithms Supported

Summary
The remote SSH server is configured to allow weak encryption algorithms.

What we have done to rectify this.
We have since disabled the weak SSH encryption algorithms on the server thereby preventing them from being exploited.

Medium (CVSS: 5.0)

NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

What we have done to rectify this.
We have configured the HTTPS service to not accept any weak ciphers thereby eliminating the threat of there being used and exploited.

AI.II Windows 2012 R2 DNS

High (CVSS: 10.0)

NVT: SMBv1 Unspecified Remote Code Execution (Shadow Brokers)

Summary
The remote Windows host is prone to an unspecified remote code execution vulnerability in SMBv1 protocol.

What we have done to rectify this.
We have disabled the use of SMBv1 on the server thereby preventing its exploitation.

Medium (CVSS: 5.0)

NVT: DCE Services Enumeration Reporting

Summary
Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

What we have done to rectify this.
Since this only effects enumeration and finding out services to exploit we have chosen to ignore it in this instance. Also since this server is inside the firewall it is already protected by that keeping it from being exploited in the first place. If it were needed to be secured more we would filter all incoming traffic on this port to only hosts that need access to this data. Since this is a test environment though with constantly changing pieces we have decided to leave it as is to prevent future problems in this environment.

AI.III Cisco Call Manager Publisher

Medium (CVSS: 4.3)

NVT: SSH Weak Encryption Algorithms Supported

Summary
The remote SSH server is configured to allow weak encryption algorithms.

What we have done to rectify this.
We have since disabled the weak SSH encryption algorithms on the server thereby preventing them from being exploited.

Medium (CVSS: 4.0)

NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate chain that has been signed using a cryptographically weak hashing algorithm.

What we would do to rectify this.
In a real implementation, we would use certificates from the companies CA using the most secure certificate signing available thereby eliminating this problem

Medium (CVSS: 5.0)

NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

What we have done to rectify this.
We have configured the HTTPS service to not accept any weak ciphers thereby eliminating the threat of there being used and exploited.

Medium (CVSS: 5.0)

NVT: SSL/TLS: Report 'Null' Cipher Suites

Summary
This routine reports all 'Null' SSL/TLS cipher suites accepted by a service.

What we have done to rectify this.
We have configured the SSL/TLS service to not accept any Null ciphers thereby eliminating the threat of there being used and exploited.

AI.IV Cisco Catalyst PoE Switch

High (CVSS: 9.0)

NVT: HTTP Brute Force Logins With Default Credentials Reporting

Summary
It was possible to login into the remote Web Application using default credentials.
As the NVT 'HTTP Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108041) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

What we have done to rectify this.
We have since changed the passwords for all logins to meet standard security best practices.

High (CVSS: 9.0)

NVT: SSH Brute Force Logins With Default Credentials Reporting

Summary
It was possible to login into the remote SSH server using default credentials.
As the NVT 'SSH Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

What we have done to rectify this.
We have since changed the passwords for all logins to meet standard security best practices.

High (CVSS: 9.0)

NVT: Cisco Default Telnet Login

Summary
It was possible to login into the remote host using default credentials.

What we have done to rectify this.
We have since changed the passwords for all logins to meet standard security best practices.
Also, we have disabled telnet as an available remote administration function.

Medium (CVSS: 4.3)

NVT: SSL/TLS: Report Weak Cipher Suites

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp(Transimmision Control Protocol) is reported. If too strong cipher suites are configured for this service the alternative would
be to fall back to an even more insecure cleartext communication.

What we have done to rectify this.
We have configured the service to not use or accept any weak ciphers thereby eliminating the threat of there being used and exploited.

Medium (CVSS: 4.3)

NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

Summary
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

What we have done to rectify this.
We have configured the service to not use or accept any weak deprecated SSL protocols and it will now only use TLSv1+ protocols thereby eliminating the threat of old vulnerable protocols from being used.

Medium (CVSS: 4.3)

NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POO-DLE)

Summary
This host is prone to an information disclosure vulnerability.

What we have done to rectify this.
We have configured the service to not use or accept any weak deprecated SSL protocols and it will now only use TLSv1+ protocols thereby eliminating the threat of old vulnerable protocols from being used. This will prevent a man in the middle attack from being performed if SSLv3 is used

Medium (CVSS: 4.0)

NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate chain that has been signed using a crypto-graphically weak hashing algorithm.

What we would do to rectify this.
In a real implementation we would use certificates from the companies CA using the most secure certificate signing available thereby eliminating this problem

Medium (CVSS: 4.3)

NVT: SSH Weak Encryption Algorithms Supported

Summary
The remote SSH server is configured to allow weak encryption algorithms.

What we have done to rectify this.
We have since disabled the weak SSH encryption algorithms on the server thereby preventing them from being exploited.

AI.V Cisco MRA(Mobile Remote Access)/VCS

Medium (CVSS: 4.0)

NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

What we have done to rectify this.

In a full implementation of this solution we would use an either an Elliptic-Curve Diffie-Hellman or 2048 bit or stronger Diffie-Hellman group to ensure that the key can not be cracked

Medium (CVSS: 4.3)

NVT: SSH Weak Encryption Algorithms Supported

Summary
The remote SSH server is configured to allow weak encryption algorithms.

What we have done to rectify this.
We have since disabled the weak SSH encryption algorithms on the server thereby preventing them from being exploited.

AI.VI ACME Session Border Controller

There was nothing to report on this host so nothing needed done to harden it.