Lab 3 - Enterprise WLAN Management and Wireless Security

CNIT 346

Group 1

Ethan Hammond

Tommy Odle

Submitted To: Justin Anderson

Date Submitted: 11/17/2023

Date Due: 11/17/2023

Executive Summary

Wireless networking can be set up for a company using a variety of different equipment for layer 2 and layer 3 capabilities. For this lab environment, it was assigned to use a Cisco switch, Cisco Meraki AP, a Unifi security gateway, and Ubiquiti access points. The nature of this equipment requires specialized configurating of switching processes, VLAN configurations, and SSID manipulation and authentication. Appendix A shows problem solving that was necessary during the creation of this lab. An ESXi machine was used to manage VMs holding Unifi controllers and Windows Servers to house RADIUS authentication. The lab was configured with WDS for Ubiquiti AP Lites. For security, a RADIUS VM was used to authenticate users into the Active Directory to connect to the networks. The network was also split into 3 sections for guest, administrator, and engineering user access. The lab report includes procedures, recommendations, business cases, results, and references.

Business Case

In a medium sized enterprise environment, companies would not always use expensive Cisco products, and would venture into companies like Ubiquiti. Although these products do not follow cisco configuration guidelines, they have their own ways of being configured and is important to consider when choosing a product to purchase. Similarly, using a controller to manage multiple access points on separate VLANs including wireless distribution systems can be a viable option in a business environment. Separating local networks by public and private subnets is a way to separate private and public users of the network. This can further be broken down into security groups for users for specific networks. Furthermore, the Cisco Meraki was realistically used to block certain sites from being accessed through the network, which is commonly used in corporate networks to keep employees productive. All projects done in lab were applicable to an enterprise scenario.

Procedures:

3750 Switch Configuration

A 3750 switch was used to connect all devices to the network. The following steps show the port and VLAN configurations done on the switch.

1. Used `en|conf t` to enter configuration mode
2. Entered `vlan 2|vlan 3|vlan 3001` to create VLANs
3. Entered int `vlan2|int vlan3|int vlan3001` to create vlan interfaces
4. Entered `ip default-gateway 44.32.1.50 255.255.255.0` to set gateway
5. Entered `ip name-server 44.2.1.44` to set dns server
6. Typed `int g3/0/3`
7. Entered `switchport mode access|switchport access vlan 3001|desc “Meraki”`
8. Typed `int g3/0/5`
9. Entered `switchport trunk encapsulation dot1q|switchport mode trunk|switchport trunk allowed vlan 1-3,3001|desc “Link to USG; VLAN 3001”`
10. Typed `int g3/0/9`
11. Entered `switchport trunk encapsulation dot1q|switchport mode trunk|switchport trunk native vlan 3001|switchport trunk allowed vlan 1-3,3001|desc “ESXI”`
12. Typed `int g3/0/13`

13. Entered `switchport trunk encapsulation dot1q|switchport mode trunk|switchport trunk allowed vlan 1-3|desc “Link to USG; VLAN 1”`
14. Typed `int g3/0/15`
15. Entered `switchport trunk encapsulation dot1q|switchport mode trunk|switchport trunk vlan 1-3|desc “Link to UAP Pro”`

Meraki Registration and Network Configuration

These steps assume that you already have created a Meraki account before beginning and go through how the Meraki device was registered and configured on the Meraki dashboard. This is needed for the Meraki to function.

1. Plugged Meraki AP into port g3/0/3 on switch
2. Logged into Meraki Dashboard on web browser
3. Selected *Network Wide* | *Add Devices*
4. Clicked **Claim**
5. Entered `Q2CK-G56H-EZPX`
6. Clicked **Claim**
7. Selected *Wireless* | *Access Points*
8. Clicked **88:15:44:67:03:24**
9. Clicked **Edit** for LAN IP
10. Entered `44.32.1.30` for IP
11. Entered `255.255.255.0` for Subnet mask
12. Entered `44.32.1.1` for Gateway

13. Entered `3001` for VLAN
14. Entered `44.2.1.45` for primary DNS
15. Clicked **Save**

Meraki Policy Additions

These steps go through how basic policies like layer 7 firewall rules and access control by devices were configured. This prevents users performing unwanted tasks and prevents unwanted devices to join the network.

1. Selected *Wireless* | *Access Control*
2. Selected *MAC OS X* in Device type dropdown
3. Selected *Blocked* in Group policy
4. Selected *Wireless* | *Firewall and Traffic Shaping*
5. Selected *Gaming* in application dropdown under Layer 7 firewall rules
6. Selected *Steam* in dropdown next to Application under Layer 7 firewall rules
7. Clicked **Save**

ESXI Deployment

The VM server OS used to host the UNIFI and RADIUS servers was ESXI 7.0. This was the easiest and cheapest option and does everything needed for this infrastructure.

1. Connected CAT6 cable from 3750 port g3/0/5 to PC
2. Plugged USB Stick with ESXI 7.0 ISO
3. Turned on PC

4. Repeatedly pressed F12 to boot into BIOS
5. Selected *SANDISK*
6. Pressed **Enter** | **F11** | **Enter** | **Enter**
7. Entered <password> for root password
8. Entered <password> for confirm password
9. Pressed **F11**
10. Removed USB stick when prompted
11. Pressed **Enter**

ESXI Network Configuration

The ESXI server was configured on the public side of the network, meaning it needed to be configured with public network configuration. The following steps show how this was done.

1. Pressed **F2**
2. Entered root credentials
3. Selected *Configure Management Network* | *IPv4 Configuration*
4. Entered `44.32.1.13` for IPv4 Address
5. Entered `255.255.255.0` for Subnet Mask
6. Entered `44.32.1.1` for Default Gateway
7. Pressed **Enter**
8. Selected *DNS Configuration*
9. Entered `44.2.1.44` for Primary DNS Server
10. Entered `44.2.1.45` for Alternate DNS Server
11. Pressed **Enter** | **Esc** | **y**

ESXI VLAN 1 Configuration

Since 2 VLANs need to be on the ESXI server, an additional VLAN (VLAN 1) was also connected un-natively to it. The following steps show how VLAN 1 was added as another network on the ESXI server.

1. Entered `44.32.1.13` into web browser on laptop
2. Typed root credentials
3. Pressed **Log In**
4. Selected *Networking*
5. Clicked **Add port group**
6. Entered VLAN 1 for port name
7. Entered `1` for VLAN ID
8. Clicked **Add**

Ubuntu Server VM Deployment

A VM needed to be created to host the UNIFI controller, and Ubuntu server was chosen for it's ease of installation and versatility. The steps below illustrate how this Ubuntu VM was deployed.

1. Right-clicked *Virtual Machines*
2. Selected *Create/Register VM*
3. Clicked **Next**
4. Entered `Ubuntu` for VM Name
5. Selected *Linux* for Guest OS Family

6. Selected *Ubuntu (64-bit)* for Guest OS Version
7. Clicked **Next** | **Next**
8. Entered `8` for for Memory
9. Selected *Datastore ISO file*
10. Clicked **Upload**
11. Selected Ubuntu Server ISO file from laptop
12. Clicked **OK** | **Next** | **Next** | **Finish**

Ubuntu Server Installation

This procedure shows how Ubuntu was installed on the Ubuntu VM. After doing this, the Ubuntu VM could be used to run the UNIFI controller.

1. Selected *Ubuntu*
2. Clicked play button to open VM
3. Selected *Try or Install Ubuntu Server*
4. Pressed **Enter** | **Enter**
5. Selected *Done* | *Done* | *Done* | *Done* | *Done* | *Done* | *Done* | *Done* | *Continue*
6. Entered `user` for name
7. Entered `CNIT346Group1` for server name
8. Entered `user` for username
9. Entered <password> for password
10. Entered <password> for confirm password
11. Selected *Done* | *Continue* | *Done* | *Done*

12. Entered
    ```
    sudo apt update|sudo apt upgrade|sudo apt install ubuntu-desktop
    ```

Unifi Controller Installation on Ubuntu

The following steps illustrate how UNIFI controller was installed on the Ubuntu VM. This gave a central interface where all Ubiquiti devices on the network could be managed.

1. Opened Terminal
2. Entered
   ```
   sudo apt install curl haveged gpg openjdk-8-jre-headless
   ```
3. Entered
   ```
   curl https://dl.ui.com/unifi/unifi-repo.gpg | sudo tee /usr/share/keyrings/ubiquiti-archive-keyring.gpg >/dev/null
   ```
4. Entered
   ```
   echo 'deb [signed-by=/usr/share/keyrings/ubiquiti-archive-keyring.gpg] https://www.ui.com/downloads/unifi/debian stable ubiquiti' | sudo tee /etc/apt/sources.list.d/100-ubnt-unifi.list > /dev/null
   ```
5. Entered
   ```
   wget http://archive.ubuntu.com/ubuntu/pool/main/o/openssl/libssl1.1_1.1.1f-1ubuntu2_amd64.deb -O libssl1.1.deb
   ```
6. Entered
   ```
   sudo dpkg -i libssl1.1.deb
   ```
7. Entered
   ```
   curl https://pgp.mongodb.com/server-3.6.asc | sudo gpg --dearmor | sudo tee
   ```

`/usr/share/keyrings/mongodb-org-server-3.6-archive-keyring.gpg >/dev/null`

8. Entered `echo 'deb [signed-by=/usr/share/keyrings/mongodb-org-server-3.6-archive-keyring.gpg] https://repo.mongodb.org/apt/ubuntu bionic/mongodb-org/3.6 multiverse' | sudo tee /etc/apt/sources.list.d/mongodb-org-3.6.list > /dev/null`
9. Entered `sudo apt update`
10. Entered `sudo apt install -y mongodb-org-server`
11. Entered `sudo systemctl enable mongod`
12. Entered `sudo systemctl start mongod`
13. Entered `sudo apt install unifi`

USG Configuration

The procedure below shows how the UniFi Security Gateway (USG) was initially configured and connected to the network. This provided a way for VLANs 1,2, and 3 to reach the public side of the network.

1. Plugged USG LAN port to g3/0/13 on switch
2. Plugged USG WAN port to g3/0/5 on switch
3. Opened Ubuntu Server VM in ESXI
4. Opened Firefox browser
5. Entered `192.168.1.1` in address bar
6. Entered `ubnt` for username and password

7. Selected *Configuration | Static IP*
8. Entered `44.32.1.95` for IP address
9. Entered `255.255.255.0` for Subnet mask
10. Entered `44.32.1.1` for Router
11. Entered `44.2.1.44` for Preferred DNS
12. Entered `3001` for VLAN ID
13. Turned on DHCP Server
14. Set range from 192.168.1.100 - 192.168.1.200
15. Clicked **APPLY CHANGES**

Adopting Devices into Unifi Controller

The Ubiquiti devices were added to the network by adopting them on the UNIFI controller. These steps show how this was done.

1. Switched Ubuntu VM to VLAN 1 on ESXI server
2. Opened Firefox browser
3. Entered `192.168.1.101:8443` into address bar
4. Selected *Devices*
5. Clicked **Adopt** on USG-3P
6. Plugged UAP Pro into port g3/0/15 on switch
7. Held reset button on bottom of UAP Pro for 10 seconds
8. Clicked **Adopt** on Unifi Controller
9. Plugged UAP Lite into PoE injector
10. Held reset button on bottom of UAP Lite for 10 seconds

11. Clicked **Adopt** on Unifi Controller
12. Repeated steps 8-10 for other UAP Lite

Networks Creation on Unifi Controller

These steps show how the three networks were created on the UNIFI controller. These networks allow the engineering, administration, and guest users to reach the network.

1. Selected *Settings* | *Networks*
2. Clicked **EDIT** for default
3. Entered `CNIT346Group1 - Engineer` for Name
4. Clicked **CREATE A NEW NETWORK**
5. Entered `CNIT346Group1 - Guest` for Name
6. Selected *Guest* for Purpose
7. Entered `2` for VLAN
8. Clicked **Save**
9. Entered Clicked **CREATE A NEW NETWORK**
10. Entered `CNIT346Group1 - Admin` for Name
11. Entered `3` for VLAN
12. Clicked **Save**

SSIDs Creation on Unifi Controller

Once the networks were created, the wireless networks needed to be created by specifying an SSID and which network the SSID should broadcast. This lets the three networks be visible to all users.

1. Selected *Settings | Wireless Networks*
2. Clicked **CREATE NEW WIRELESS NETWORK**
3. Entered `CNIT346Group1 - Engineer` for Name/SSID
4. Selected *CNIT 346Group1 - Engineer* for Network
5. Clicked **Save**
6. Entered `CNIT346Group1 - Guest` for Name/SSID
7. Selected *CNIT 346Group1 - Guest* for Network
8. Selected *Apply guest policies*
9. Clicked **Save**
10. Entered `CNIT346Group1 - Admin` for Name/SSID
11. Selected *CNIT 346Group1 - Admin* for Network
12. Clicked **Save**

RADIUS Box / AD Creation

For authentication and security purposes, a RADIUS server was configured on a Windows Server 2022 VM created on the ESXI server. This is important because it allows for authentication through Active Directory (AD).

1. Logged into the ESXi VmWare and created a Windows Server 2022 VM.
2. Added the following IP addresses to the machine:
    a. IP: 192.168.1.110/24
    b. Gateway: 192.168.1.1
    c. Port group: VLAN 1 Port group.

3. Opened Server Manager and clicked *Manage* | *Add Roles and Features* | *Active Directory Domain Services*.
4. Promoted the server to domain controller with a new forest.
5. Restarted the machine.
6. Opened Server Manager and clicked *Manage* | *Add Roles and Features* | *ADCS*.
7. Opened Server Manager and clicked *Manage* | *Add roles and Features* | *Network Policy and Access Services*.
8. Restarted the machine and reopened Server Manager.
9. Clicked *Tools* | *Active Directory Users and Computers* and right-clicked *Users* | *New…*.
10. Created three security groups (engineerUsers, adminUsers, and guestUsers).
11. Created three users (engineerUser, adminUser, guestUser) with passwords.
12. Added the users to their respective security group.

Radius Configuration

The specific security needed for the RADIUS server was configured in the steps below. This gave each of the three different networks their own group and users who can log into the network.

1. Opened Server Manager and clicked *Tools* | *Network Policy Server* and right-clicked NPS (Local) and clicked Register server in Active Directory.
2. Right-Clicked *RADIUS Clients* and entered the names and IP addresses of the access points and VLANs for the security groups.
3. Created a new Connection Request Policy for the admin security group.
4. Added a condition of Called Station ID of value ‘*.CNIT346Group1 - Admin’

5. Repeated steps 3-4 for the guest and engineer user SSIDs.
6. Created a Network Policy for the admin security group.
7. Added a condition of ‘CNIT346G1\adminUsers’.
8. Added a constrained authentication method of PEAP and EAP-MSCHAP v2 and unchecked all less secure encryption methods.
9. Added a setting for standard attribute of:
    a. Framed-Protocol: PPP.
    b. Service-Type: Framed.
    c. Tunnel-Medium-Type: 802
    d. Tunnel-Pvt-Group-ID: 3 (VLAN ID).
    e. Tunnel-Type: VLAN.
10. Edited the Network Policy and right clicked “PEAP” and added a created certificate from ADCS.
11. Repeated Steps 6-10 for the engineer and guest user groups.

Results

The results of the lab included correct configuration of a Cisco switch with 2 VLANs, housing public and private networks for users to connect to. The public network housed a Cisco Meraki AP, and an ESXi server accessible from the public network. A Ubiquiti Security Gateway was used to route the public traffic into private network segments on an RFC 1918 address pool. This public address space housed separate private networks for access points to connect users to. These Ubiquiti access points were managed by a Unifi Controller VM housed on the ESXi machine on the private network. Also housed on the ESXi box was a RADIUS server used for authentication of users onto their respective network segments and access points. The logical diagram containing IP addresses can be seen below in Figure 1, and a physical diagram with physical equipment can be seen below in Figure 2.

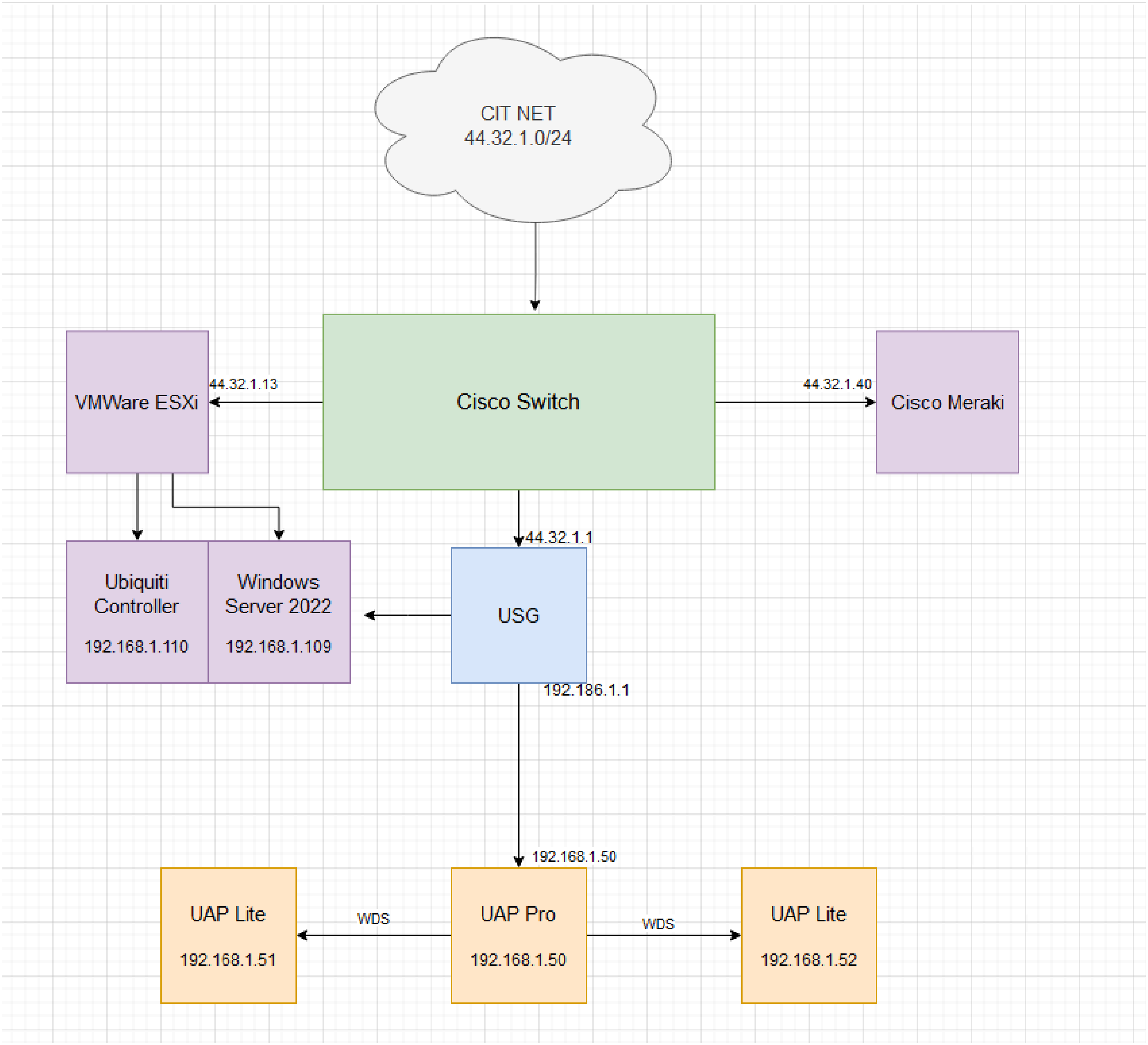

Figure 1: Logical Diagram

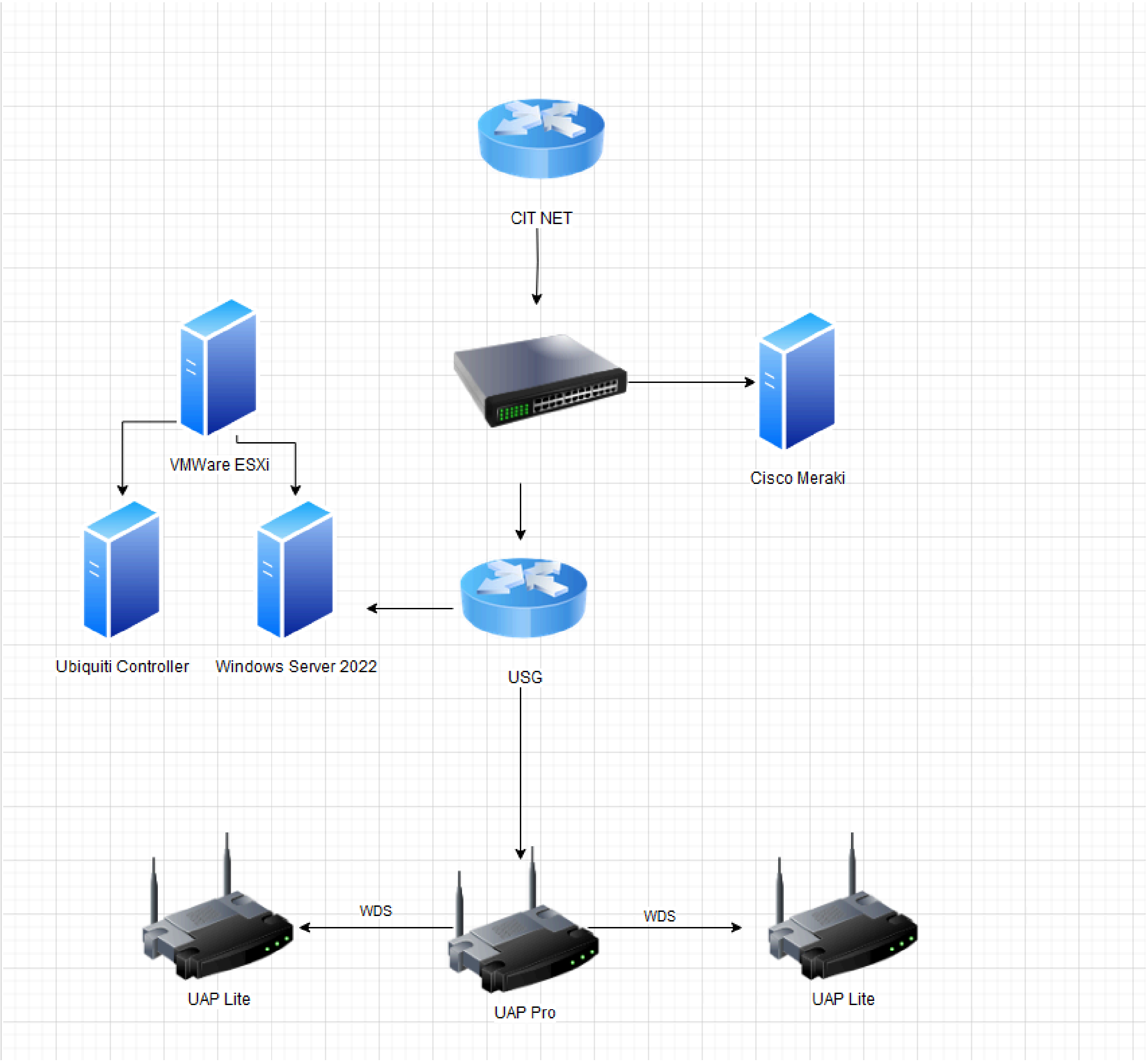

Figure 2: Physical Diagram

Conclusions and Recommendations

For a wireless networking enterprise environment, it was concluded that the network can work effectively given the current specifications. A switch can effectively be used to split up a network into public and private VLANs with access points broadcasting SSIDs for its respective network. Similarly, it can be very effective to utilize a security gateway/router to route traffic between public and private networks. Network controllers were used very effectively to create multiple SSIDs with specified authentication to each identifying network segment. Recommendations to strengthen the infrastructure of this environment for a company would be to utilize wired distribution systems with ethernet between the AP pro and AP lites for a stronger connection. Another recommendation would be to utilize the Cisco Meraki for more than a test SSID and further integrate it into the network. Lastly, it would be effective to require the optional tasks in the lab to add more networking capabilities to the core of the network including a Cisco 3502, 3702, and a separate switch.

References

Anderson, Q. Justin, (Personal Communication, November 2023).

802.11ac dual-radio pro access point - ubiquiti. (n.d.-a). https://dl.ubnt.com/guides/UniFi/UniFi_AP-AC-Pro_QSG.pdf

802.11ac dual-radio pro access point - ubiquiti. (n.d.-b). https://dl.ubnt.com/guides/UniFi/UniFi_AP-AC-Pro_QSG.pdf

Emmet. (2023, March 1). *Installing the Unifi controller on ubuntu*. Pi My Life Up. https://pimylifeup.com/ubuntu-unifi-controller/

Enterprise gateway router with Gigabit Ethernet - Ubiquiti. (n.d.-c). https://dl.ubnt.com/guides/UniFi/USG_QSG.pdf

Google. (n.d.). Google search. https://www.google.com/search?client=firefox-b-1-d&q=how%2Bto%2Bconfigure%2Ba%2Bcisco%2Bmeraki

Meena, S. (2022, October 17). *How to set up a microsoft radius server*. SecureW2. https://www.securew2.com/blog/how-to-set-up-a-microsoft-radius-server

MohamedO. (2017, February 10). *Help with ESXI and Multi vlans*. The Spiceworks Community. https://community.spiceworks.com/topic/1964396-help-with-esxi-and-multi-vlans

YouTube. (2020, December 29). *Unifi Security Gateway - first time setup*. YouTube. https://www.youtube.com/watch?v=x2BjgWBcv7Q

Appendix A: Problem Solving

Problem 1: Ubiquiti USG was not showing up on the Unifi controller.

Attempted solutions: It was attempted to add a public IP address onto the public NIC of the USG. It was also attempted to console into the USG and add IP addresses and encryption methods manually.

Final Solution: It was solved by factory resetting the USG and reaching it locally on 192.168.1.1 and configuring it through its setup wizard on the GUI.

Problem 2: It was not identified how to bridge 2 VLANs through ESXi.

Attempted solutions: It was attempted to put the ESXi box on a private address. It was also attempted to bridge port groups on ESXi.

Final Solution: It was solved by putting the ESXi on a public address, and trunking all VLANs through the switch, putting the VMs on the private port group.

Problem 3: RADIUS was not allowing authentication into the networks.

Attempted Solutions: It was attempted to create profiles on the USG. It was also attempted to link profiles on the RADIUS box and the USG. It was attempted to add WPA3 Enterprise encryption on the SSIDs.

Final solution: The issue was solved by installing Active Directory Certificate Services on the RADIUS machine, creating a certificate, and adding it on PEAP within the settings in the Network Policy Server.

Appendix B: Device Configurations

Switch Config:

```
Current configuration : 4122 bytes
!
! Last configuration change at 06:50:54 UTC Mon Feb 27 2006 by user
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 3750G1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$uxzb$9NdDBZ0C4hFOWbJv7F2IP/
!
username user password 0 CNIT346g1
no aaa new-model
switch 3 provision ws-c3750e-48pd
```

```
system mtu routing 1500
!
!
!
!
!
!
ip domain-name cnit346g1.lcl
ip name-server 44.2.1.44
vtp mode transparent
!
!
!
!
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
!
```

```
!
vlan internal allocation policy ascending
!
vlan 2-3
!
vlan 99
 name vlan-mgt
!
vlan 3001
 name vlan 3001
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0
```

```
 no ip address
!
interface GigabitEthernet3/0/1
 description "Access port to VLAN 3001"
 switchport access vlan 3001
 switchport mode access
!
interface GigabitEthernet3/0/2
!
interface GigabitEthernet3/0/3
 description "Meraki"
 switchport access vlan 3001
 switchport trunk native vlan 3001
 switchport mode access
!
interface GigabitEthernet3/0/4
 switchport access vlan 3001
 switchport mode access
!
interface GigabitEthernet3/0/5
 description "Link to USG; VLAN 3001"
 switchport trunk allowed vlan 1-3,3001
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet3/0/6
!
interface GigabitEthernet3/0/7
 switchport access vlan 3001
 switchport mode access
!
interface GigabitEthernet3/0/8
!
interface GigabitEthernet3/0/9
 description "Link to ESXI"
 switchport access vlan 3001
 switchport trunk allowed vlan 1-3,3001
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 3001
 switchport mode trunk
!
interface GigabitEthernet3/0/10
!
interface GigabitEthernet3/0/11
!
interface GigabitEthernet3/0/12
```

```
!
interface GigabitEthernet3/0/13
 description "Link to USG; VLAN 1"
 switchport trunk allowed vlan 1-3,3001
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet3/0/14
!
interface GigabitEthernet3/0/15
 description "Link to UAP Pro"
 switchport trunk allowed vlan 1-3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet3/0/16
!
interface GigabitEthernet3/0/17
 description "Access port to VLAN 1"
 switchport mode access
!
interface GigabitEthernet3/0/18
!
```

```
interface GigabitEthernet3/0/19
!
interface GigabitEthernet3/0/20
!
interface GigabitEthernet3/0/21
!
interface GigabitEthernet3/0/22
!
interface GigabitEthernet3/0/23
!
interface GigabitEthernet3/0/24
!
interface GigabitEthernet3/0/25
!
interface GigabitEthernet3/0/26
!
interface GigabitEthernet3/0/27
!
interface GigabitEthernet3/0/28
!
interface GigabitEthernet3/0/29
!
interface GigabitEthernet3/0/30
```

```
!
interface GigabitEthernet3/0/31
!
interface GigabitEthernet3/0/32
!
interface GigabitEthernet3/0/33
!
interface GigabitEthernet3/0/34
!
interface GigabitEthernet3/0/35
!
interface GigabitEthernet3/0/36
!
interface GigabitEthernet3/0/37
!
interface GigabitEthernet3/0/38
!
interface GigabitEthernet3/0/39
!
interface GigabitEthernet3/0/40
!
interface GigabitEthernet3/0/41
!
```

```
interface GigabitEthernet3/0/42
!
interface GigabitEthernet3/0/43
!
interface GigabitEthernet3/0/44
!
interface GigabitEthernet3/0/45
!
interface GigabitEthernet3/0/46
!
interface GigabitEthernet3/0/47
!
interface GigabitEthernet3/0/48
 switchport access vlan 3001
 switchport mode access
!
interface GigabitEthernet3/0/49
!
interface GigabitEthernet3/0/50
!
interface GigabitEthernet3/0/51
!
interface GigabitEthernet3/0/52
```

```
!
interface TenGigabitEthernet3/0/1
!
interface TenGigabitEthernet3/0/2
!
interface Vlan1
 no ip address
!
interface Vlan2
 no ip address
!
interface Vlan3
 no ip address
!
interface Vlan3001
 ip address 44.32.1.50 255.255.255.0
!
ip default-gateway 44.32.1.1
ip forward-protocol nd
!
ip http server
ip http secure-server
ip ssh version 2
```

```
!
!
!
!
line con 0
 logging synchronous
 login local
line vty 0 4
 privilege level 15
 login local
 transport input ssh
 transport output ssh
line vty 5 15
 privilege level 15
 login local
 transport input ssh
 transport output ssh
!
!
End
```