***CNIT 45600 Lab 2: Wireless Network Security & Management***

CNIT45600

Team Trash  
Ethan Hammond  
Tommy Odle  
Elliot Tuchscherer  
Submitted To: Justin Anderson  
Date Submitted: 05/03/24  
Date Due: 05/03/24

Table of Contents

[**EXECUTIVE SUMMARY 3**](#_4zpk7pvmqivq)

[**BUSINESS CASE 4**](#_7q2oziqj1n4a)

[**PROCEDURES 5**](#_51kz37jle3n5)

[Cable Hookups 5](#_tme9ij7ttnwt)

[3750 Switch Configuration 5](#_x5bl93if2ip9)

[ESXi Installation 6](#_wpyu43qy74a)

[ESXi Network Configuration 7](#_xru8ri5mp6e1)

[ESXi Port Group Creation 7](#_l9lh36vnh7ds)

[Cisco 9800 WLC VM Deployment and Network Configuration 8](#_px8bprb1zc00)

[Cisco 9800 WLC VLAN Creations 9](#_c1urzl42jxka)

[RADIUS Configuration 10](#_i98n0tfrhnfd)

[**RESULTS 12**](#_k5vyeyqflntm)

[**CONCLUSIONS AND RECOMMENDATIONS 15**](#_4tcqnhym0p02)

[**BIBLIOGRAPHY 16**](#_ckawy6md6ybt)

[**APPENDIX A: PROBLEM SOLVING 18**](#_94fsq7jqs45)

# EXECUTIVE SUMMARY

A secure wireless network environment can be constructed for the medical center Trash Hospital by using many different protocols, topologies, and equipment. For this scenario, two Cisco 3702 Access Points (APs), a Cisco Catalyst 3750 switch, and a VMware ESXi 8.0 server were used in conjunction with the 802.11 security protocols WPA PSK and WPA 2 Enterprise. The Cisco 3750 switch was configured to supply connectivity to the APs and ESXi server using L2 trunking protocols and did not serve any security or L3 functions. Each AP was configured with three different networks: Trash Hospital Network (WPA 2 Enterprise), Trash Hospital Legacy (WPA PSK), and Trash Hospital Guest (Open). A Windows Server 2019 VM, a Cisco 9800 WLC VM, and pfSense VM were deployed on the ESXi 8.0 server to virtualize many network operations. pfSense provided a gateway between the private and public networks via NAT and also enforced many firewall rules for each network. The Cisco 9800 WLC was used to create the WLANs for the Cisco APs to broadcast and for clients to connect to. Windows Server 2019 had Active Directory activated and RADIUS configured via 802.1X/EAP authentication for users on the Trash Hospital Network WLAN. The Trash Hospital Network WLAN pointed at the RADIUS server through a Cisco 9800 WLC security policy. A simple FTP server was also created on Windows Server 2019 to provide specific users access to specific resources.

# BUSINESS CASE

A mid-sized medical center called Trash Hospital requested a fast and secure wireless network for their growing enterprise environment. Six networks are needed for this topology: admin/staff/management, doctors, nurses, legacy devices, and visitors. There are also many departments needing access to different resources. These departments include: Accident & Emergencies, Admissions, Cardiology, Coronary Care Unit, Critical Care, Diagnostic Imaging, Finance, Information Technology, Pharmacy, Purchasing & Supplies, Radiology, Urology, All Nurses. Resources include: Patient Record, XRAY imaging, Financial, IT, Business Admin, Ordering System. They would also like this network with as little overhead as possible.

An ESXI server could be deployed on a physical machine to act as a hypervisor, enabling VM creation and network virtualization. A Cisco 9800 WLC could provide central management and configuration of this wireless network. This Cisco 9800 WLC could create the six networks needed and all of their needed configurations and assets. Older Cisco 3702 APs and a 3750 switch can offer 802.11ac speeds (up to 13400Mbps) on 5Ghz along with WPA2 802.1X/EAP authentication. A Windows server could run AD and RADIUS to provide enterprise-level security for clients. RADIUS could also be used to consolidate the three RADIUS networks into one SSID via VLAN tunneling in the RADIUS policies. The legacy network could use WPA PSK and the visitors network could be open with a web portal login. A pfSense box could be set up to provide a gateway between the private and public sides of the network and act as a secure and robust firewall for each network. A group for each department could also be made on a Windows server, and an FTP server could be activated and configured to provide resources to users depending on their group membership.

# PROCEDURES

The following procedures outline the steps taken to complete this project. For reference,

*Italicized* words represent options, **bold** words represent buttons, and words in Courier New represent inputs that are typed. Pipes | are used to represent chained selections, clicks or commands.

## Cable Hookups

To ensure everything could communicate properly, a switch was used to interconnect all of the devices and provide an uplink in the network via CAT5e/6 cables. Below are the procedures for doing this.

1. Plugged CAT5e/6 cable from port 13 on switch to Cisco 3702 AP
2. Plugged CAT5e/6 cable from port 15 on switch to Cisco 3702 AP
3. Plugged CAT5e/6 cable from port 48 on switch to Precision 3620
4. Plugged uplink cable into port 1 on switch

## 3750 Switch Configuration

Below are the steps for configuring the Cisco Catalyst 3750 Switch. This was needed to ensure VLANs were accessible from all devices and that the network had a working uplink.

1. Plugged power cable into switch
2. Plugged serial cable from serial port on switch to laptop
3. Opened COM1 terminal in PuTTy on laptop
4. Entered enable | conf t | hostname CNIT456TeamTrash SW
5. Entered vlan 1010 | vlan 1030 | vlan 1040 | vlan 1050 | vlan 1060 | vlan 1070
6. Entered int g1/0/13 to enter configuration mode for port 13
7. Entered switchport trunk encapsulation dot1q | switchport mode trunk | switchport trunk allowed vlan 1010 1030 1040 1050 1060 1070 | switchport trunk native vlan 1070
8. Entered int g1/0/15 to enter configuration mode for port 15
9. Entered switchport trunk encapsulation dot1q | switchport mode trunk | switchport trunk allowed vlan 1010 1030 1040 1050 1060 1070 | switchport trunk native vlan 1070
10. Entered int g1/0/1 to enter configuration mode for port 1
11. Entered switchport trunk encapsulation dot1q | switchport mode trunk | switchport trunk allowed vlan 1010 1030 1040 1050 1060 1070
12. Entered end | wr to save configuration

## ESXi Installation

Since most of the network needs to be virtualized, VMware’s ESXi was chosen as the hypervisor for the Precision 3620 to host all of the VMs. Below are the steps for how it was installed.

1. Plugged USB drive into Precision 3620
2. Plugged Precision 3620 into power
3. Hit F12 on keyboard repeatedly until one-time boot screen came up
4. Selected *SANDISK* | *ESXI-8.0-installer*
5. Pressed **Enter** | **F11** | **Enter** | **Enter**
6. Entered <password> for Root password and Confirm password
7. Pressed **F11** | **Enter**

## ESXi Network Configuration

For ESXi to be accessible via web GUI, the management network must be configured properly. Below shows how this was done.

1. Pressed **F2** after installation
2. Entered root credentials
3. Selected *Configure Management Network* | *IPv4 Configuration*
4. Typed 44.102.122.10 for IPv4 Address
5. Typed 255.255.255.0 for Subnet Mask
6. Typed 44.102.122.1 for Default Gateway
7. Pressed **Enter**
8. Selected *DNS Configuration*
9. Typed 44.2.1.44 for Primary DNS Server
10. Typed 44.2.1.45 for Alternate DNS Server
11. Pressed **Enter** | **Esc** | **Y**

## ESXi Port Group Creation

Now that ESXi was accessible via web browser, a port group needed to be created that allowed all VLANs to communicate with any future VMs. The steps below show how this was done.

1. Logged into ESXi using web browser
2. Selected *Networking* | *Port Groups*
3. Clicked **Add port group**
4. Entered Hospital Network for Name
5. Entered 4095 for VLAN ID
6. Clicked **Add**

## Cisco 9800 WLC VM Deployment and Network Configuration

Below are the steps for deploying a Cisco Catalyst 9800-CL WLC controller on ESXi as an OVF template. This is important because this WLC controller will be doing most of the network operations.

1. Logged into ESXi using web browser
2. Selected *Virtual Machines*
3. Clicked **Create / Register VM**
4. Selected *Deploy a virtual machine from an OVF or OVA file*
5. Entered CiscoWLC for VM name
6. Dragged Cisco 9800 WLC ova file from file explorer to drag-and-drop box on ESXi
7. Clicked **Next** | **Next**
8. Selected *Hospital Network* for GigabitEthernet 1, 2, and 3
9. Clicked **Next** | **Finish**
10. Powered on VM
11. Opened VM through web browser
12. Entered no | en | int gig 1 | ip address 192.168.7.30 255.255.255.0 | no shut | ip route 192.168.7.0 255.255.255.0 192.168.7.99 | exit
13. Entered int gig 2 | sw mo tr | sw tr all vlan 1010,1030,1040,1050,1060,1070 | no shut | exit
14. Entered hostname C9800-WLC
15. Entered end | wr to save configuration

## Cisco 9800 WLC VLAN Creations

To separate the network into different segments, six VLANs per the business case were created. Below is the procedure for how they were created.

1. Logged into Cisco 9800 Controller over web browser
2. Selected *Configuration* | *VLAN* | *VLAN*
3. Clicked **Add**
4. Entered 1010 for VLAN ID
5. Entered Admin for Name
6. Clicked **Apply to Device**
7. Repeated steps 3-6 for the following VLANs:

* VLAN 1030 - Doctors
* VLAN 1040 - Visitors
* VLAN 1050 - Nurses
* VLAN 1060 - Legacy
* VLAN 1070 - Internal Management

1. Selected *SVI*
2. Clicked **Add**
3. Selected *VLAN 1010*
4. Entered 192.168.1.1 for IPv4 address
5. Clicked **Apply to Device**
6. Repeated steps 9-12 for the following SVIs:

* VLAN 1030 - 192.168.3.1
* VLAN 1040 - 192.168.10.1
* VLAN 1050 - 192.168.5.1
* VLAN 1060 - 192.168.6.1

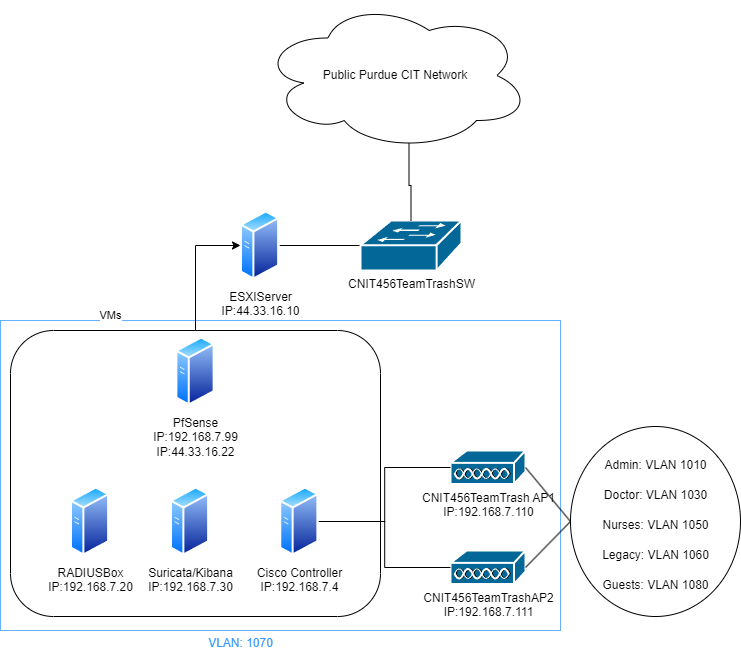
## RADIUS Configuration

1. Logged into the Windows Server and opened Server Manager | Add roles and features | Network Policy Server
2. Opened Tools | Network Policy Server and created a new server group with the DC in it.
3. Created a new client group with all APs and the WLC IP addresses.
4. Set a connection request policy with the Doctor AD group.
5. Created a network policy with the Called Station ID of \*.Team Trash Hospital.
6. Set the VLAN to the Doctors VLAN.
7. Recreate steps 5-6 for each AD group to their respective VLAN.
8. Set the Framed-Protocol to EAP.
9. Set the tunnel-type to VLAN and set for each AD group.
10. Set the Authentication method to EAP-MSCHAPv2.
11. Set the WLC authentication method to EAP-MSCHAPv2.
12. Set the RADIUS Server IP address to the IP of the Windows Server.

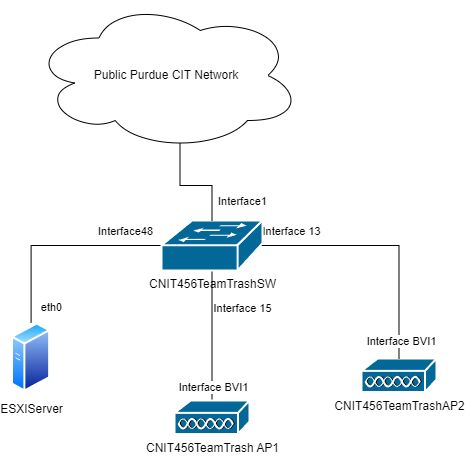
## 

# RESULTS

In total an entire new network was set up from scratch. This network made use of four physical machines being the two Access Points, the one switch, and the one Dell that was converted to an ESXi Hypervisor which can be seen in the physical diagram of the network included in the Figure below. From that ESXi, four Virtual Machines were created to meet certain requirements of the network. A Cisco 9800 WLC was deployed in order to manage and configure the access points. An Active Directory/RADIUS server was set up which when combined with the WLC allowed the creation of WPA2-Enterprise connection. It was also used as an FTP server to provide access to certain files. Additionally, it was configured so that based on the login credentials entered, the user would be placed in a specific VLAN with defined access rights. There were also two other SSIDs created and deployed, one being an open network to provide complimentary internet access to guests and a legacy WPA-PSK network for legacy devices. The final VM created was a PfSense firewall that would help segment the private from the public network through NAT, while also creating rules to prevent certain traffic between private VLANs. The VLANs, VMs, and IP addresses used can be seen in the logical diagram included below.



*Figure 1: Logical Diagram of the Network*

**

*Figure 2: Physical Diagram of the Network*

# 

# CONCLUSIONS AND RECOMMENDATIONS

All goals that were set out in the Business Scenario have been accomplished, except for setting up a captive portal on the open network. In a medium-sized hospital environment, wireless security is absolutely critical. To test security protocols and practices, it can be effective to create a network environment and either pentest the network yourself, or hire external parties to pentest it for you. The network is finalized with RADIUS authentication on the main SSID that identifies VLAN per AD user, an open SSID for guest networks, and an SSID with WPA-PSK for legacy devices in the hospital. Security devices include a Cisco WLC, a pfSense machine, and a Linux server running Suricata with an ELK stack. The WPA-PSK network is inevitably vulnerable with older encryption mechanisms with the WPA2 Enterprise network being very secure.

Recommendation 1: An interface should be created on pfSense per VLAN being used, or at least more than just the 2 interfaces in its current configuration. This would allow firewall rules to be more efficient and makes it easier to troubleshoot and access specific firewall rules for groups.

Recommendation 2: When working with VMs, snapshots should be taken regularly and especially before major configuration changes to ensure there is always a working copy that can be reverted to. Additionally, it serves as a possible recovery system in case of a catastrophic attack.

Recommendation 3: Work in previous labs should be cleaned up so that the environment is pristine for the next task. Aspects such as test users, temporary rules, and/or servers made for troubleshooting should either be removed or properly documented.

# 

# BIBLIOGRAPHY

Cisco. (2021, August 13). *Reset a CBW AP back to factory default settings*. Cisco. https://www.cisco.com/c/en/us/support/docs/smb/wireless/CB-Wireless-Mesh/2120-reset-to-factory-default-cbw.html

Cisco. (2024a, March 5). *Configure vlans on Wireless Lan Controllers*. Cisco. https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-vlan/68100-wlan-controllers-vlans.html

Cisco. (2024b, March 25). *Cisco Catalyst 9800-CL Cloud Wireless Controller Installation Guide - Installing Controller in vmware environment [cisco catalyst 9800 series wireless controllers]*. Cisco. https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-cloud/installation/b-c9800-cl-install-guide/installing\_the\_controller.html

Horovits, D. (2024, February 12). *The Complete Guide to the elk stack*. Logz.io. https://logz.io/learn/complete-guide-elk-stack/

*How to update access point firmware using TFTP when it is not possible to perform update through the HTTP interface.* Cisco Community. (2020, November 18). <https://community.cisco.com/t5/wireless-mobility-knowledge-base/how-to-update-access-point-firmware-using-tftp-when-it-is-not/ta-p/3131109>

(n.d). *Lab report template*. Brightspace. Retrieved May 1st, 2024. From https://purdue.brightspace.com/d2l/le/content/171363/viewContent/3726799/View

LiquidWeb. (n.d.). *How to create an FTP server and account in AlmaLinux*. Liquid Web. https://www.liquidweb.com/kb/create-ftp-account-almalinux/

Nayarasi, & Nayarasi. (2013, July 22). *Called & calling station Id*. mrn. <https://mrncciew.com/2013/07/22/called-calling-station-id/>

Ping Labz. (2023). *Cisco Catalyst 9800 WLC WLAN Setup*. Youtube. https://www.youtube.com/watch?v=Sbz1G\_elNLE

r00t. (2022, October 31). *How to install suricata on almalinux 8*. idroot. https://idroot.us/install-suricata-almalinux-8/

VMware knowledge base. (n.d.). https://kb.vmware.com/s/article/1004074

Ruckus Networks Education. (2020) *Unleashed: Setting Up 802.1x EAP with Dynamic VLAN with Windows NPS Server.* Youtube. https://www.youtube.com/watch?v=KAGEA7OnPvY

# APPENDIX A: PROBLEM SOLVING

Found within this section are several issues experienced during the development of this project. Each problem below can be divided by a *Problem Description* detailing the issue, any *Solutions Attempted*, and finally a detailed description of the *Final Solution*.

**Problem 1:**

**Problem Description:** The access points ran out of licenses and had to be renewed.

**Solutions Attempted:** It was attempted to find a license online and thought of to reflash the APs, but would take a long time to complete.

**Final Solution:** We were able to find a license on the Purdue TFTP server and were able to apply it to the APs.

**Problem 2:**

**Problem Description:** Suricata was picking up logs in a tough-to-read way and we wanted a solution for efficient log aggregation.

**Solutions Attempted:** It was attempted to write a script to consolidate the information into another file. This would have taken too long and not as effective as possible.

**Final Solution:** An ELK stack was created for the Suricata machine to show the data in a visual format for easy readability.

**Problem 3:**

**Problem Description:** VLANs were not passing through to the APs to broadcast via SSID.

**Solutions Attempted:** It was attempted to add the VLANs on the switch. It was also attempted to change the NPS policies to let all VLANs through.

**Final Solution:** It was solved by adding the VLAN information into the pfSense VLAN tab which let all tags through.