Lab 5 Procedure

Background:

IEC 62433 series of standards and NIST 800-82 outline cybersecurity standards for securing industrial control systems(ICS) using modern IT cybersecurity practices. This lab outlines introductory practices to secure ICS networks, or operational technology(OT), by pentesting via network reconnaissance tools and common IT/OT implementations. Use of these tools on networks without permission is advised against before notifying IT/OT professionals and internet service providers(ISP). This is a secure network environment where IEDs do not have direct access to sensitive systems and lives are not in danger. Use in real SCADA systems can cause adverse damage to equipment and bodily harm/injury.

Introduction:

In most cases, when penetration testing a network, we want to avoid damages to devices on the network and possible down time that can result from our tests. In order to do so, this lab will be broken up into two sections. The first of which is doing reconnaissance in the form of network mapping/routing and port/packet sniffing to see what is available and secure from different points in our OT network. We will then configure common devices to provide a secure connection between different subnetworks and gateways to places of concern. In order to so we will be using these devices to configure network switch security and implement a security gateway before entering the next subnetwork within our environment. We do this to restrict unauthorized entry and movement throughout the network.

There is also a third lab, link provided, that takes an in-depth view of virtual networking and modeling. These resources use VMware Workstation with a simulated view of our lab setup to test and implement open-source security options. Taking a virtual configuration lets us safely test and develop cybersecurity options that can later be used to increase the security of our current network without disrupting ICS/SCADA routines.

Configuration:

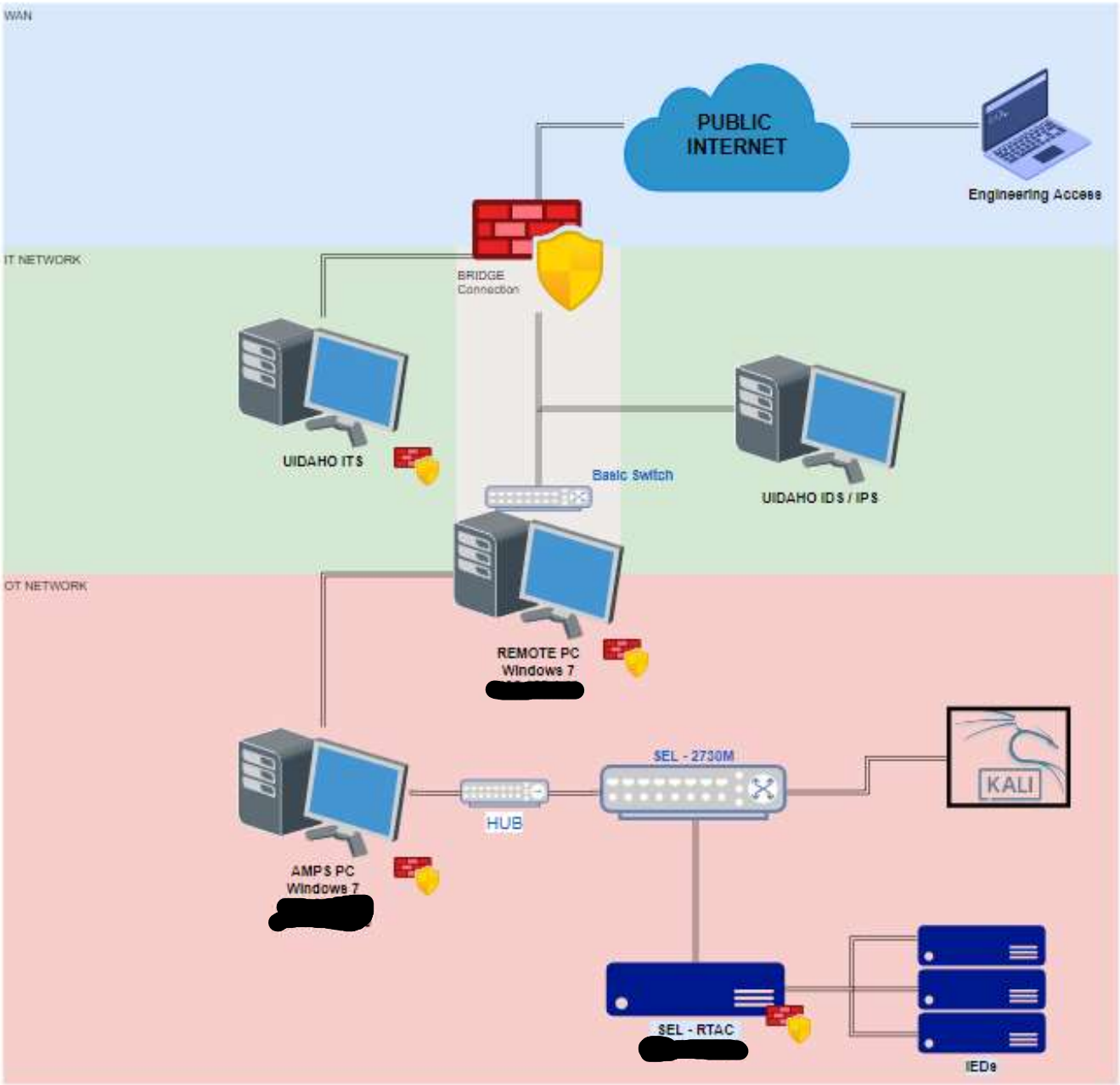
<u>Hardware</u>

SEL-3622(NSG)
SEL-2730M
SEL-3530(RTAC)
Multiple SEL IEDs
AMPS PC
Raspberry Pi(RPi)
    Insert Kali SD card into RPi C from previous labs and use same setup.

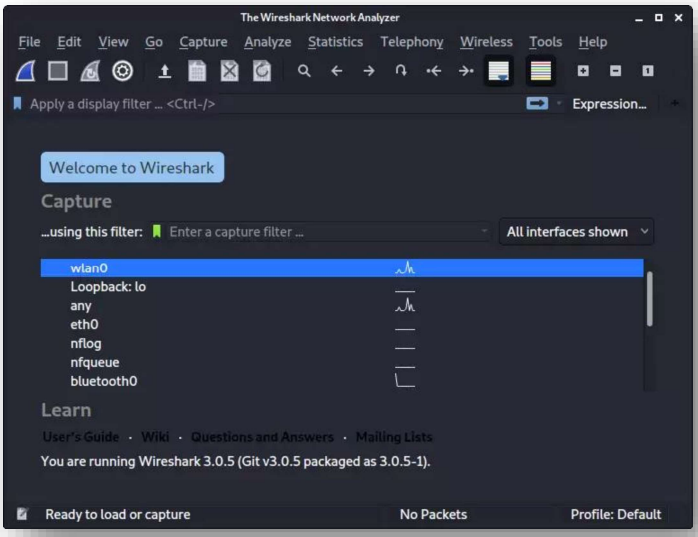
<u>Software</u>

Kali Linux
    Install:
    Netdiscover
    Nmap
    Wireshark

Initial Network Diagram



OT Network:



I Network Scanning:

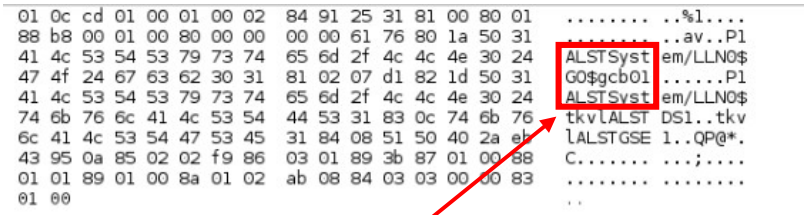
1. Log onto the Kali Linux RPi
   a. Username/Password -[redacted]
2. Make sure that the RPi is connected to a port on the Hub
3. Open terminal windows
4. Use *ifconfig*
   a. Locate your IP Details
      - IPv4, Subnetmask, and Default Gateway
      - Subnetting Videos

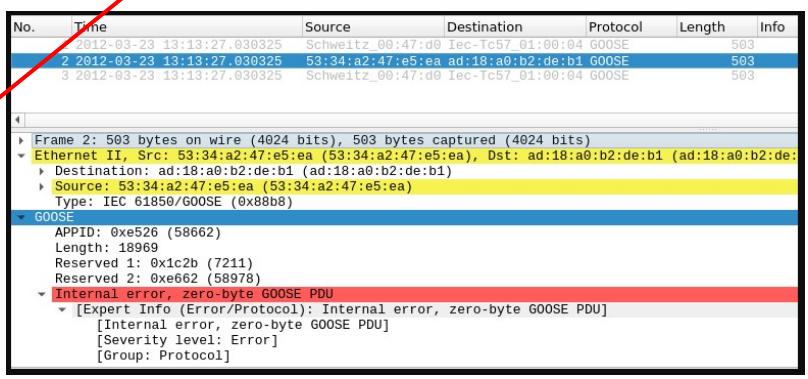
Online Devices

1. Use command netdiscover -h
2. Use command *sudo netdiscover*
   a. Let cycle through till[redacted] (All IP addresses under subnet[redacted])
      - Netdiscover actively sends ARP requests as-well-as passively monitors these packets
   b. Press Q to stop search
      - Set list aside for reference
        - Take note of different devices on network
3. Open another terminal window
   a. Use command *sudo wireshark*
   b. Select eth0
   c. Select File > Start Capture
      - Stop after 15 seconds
   d. Type in filter bar
      - GOOSE
        - Try other protocols TCP, UDP, ARP
        - You can also combine filters w/ 'and'
      - ip.addr == xxx.xxx.xxx.xxx
        - View traffic filtered using some IPs from netdiscover list
   e. Search GOOSE in filter
   f. Select GOOSE packet > Ethernet II dropdown
      - View Destination MAC Address
      - View Source Address

      If unencrypted, we can view the manufacturer, destination, and source addresses, and sometimes the specific model of device

      What are some devices you?





Nmap on ICS devices

4. Open a third terminal window
   a. Use command *sudo su*
      - *Password -* [redacted]
   b. Use command *nmap -h*
      - Look through list of possible commands
      - Nmap cheat sheet
   c. Use command *nmap -Pn -sT -p502 --script modbus-discover <target>*
      - Try on [redacted]
        - SEL - RTAC
      - From wireshark traffic
        - Known devices trying to communicate
        - Filter wireshark using ip.addr == [redacted]
   d. Use command *nmap -Pn -sT -p502 --script modbus-discover* [redacted]
      - The asterisk is a wildcard and will search throughout all 256 ports.
        - May take a while.
        - Press enter to check progress.
   e. Use command *nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p *
   *80,102,443,502,530,593,789,1089-1091,1911,1962,2222,2404, *
   *4000,4840,4843,4911,9600,19999,20000,20547, *
   *34962-34964,34980,44818,46823,46824,55000-55003 *
   <target>
        - Will take significantly more time

Common scan types

- *-sS(Stealth scan)*
  - In the three-way TCP/IP handshake, this will not complete the handshake.
- *-Pn(Disable Ping Return)*
- *-sT(TCP Scan)*
- *-sV(Version of service on device)*
- *-O(OS Detection)*
- *-T#(Timing and Performance)*
  - *# = 0-5*
    (i) *T0/1 IDS Evasion*
    (ii) *T2-3 Light Network Speeds*
    (iii) *T4-5 Fast Network Speeds*

Perform vulnerability scan of network

f. Use Command *nmap -sV --script nmap-vulners/ <target>*
- List vulnerabilities
  - Vulnerable to ____ DDoS, ____ MiTM, etc.
  - List open ports(Holes in the network)

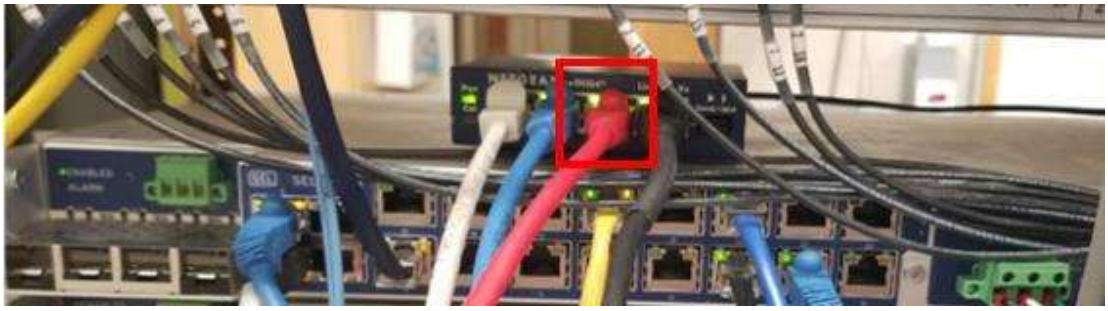
SEL provides hardened IEDs that by factory default offer high security standards. The SEL-3530(RTAC) offers many built in cybersecurity benefits to meet NERC CIP guidelines. One of which is a Stateful Firewall which is a layer 3 and 4 firewall that identifies, and blocks based on protocol and destination of traffic. Depending on how the firewalls are configured, the system will either allow, reject, or drop the packets sent to it.

Defense in Depth Strategy Elements	
Risk Management Program	· Identify Threats · Characterize Risk · Maintain Asset Inventory
Cybersecurity Architecture	· Standards/ Recommendations · Policy · Procedures
Physical Security	· Field Electronics Locked Down · Control Center Access Controls · Remote Site Video, Access Controls, Barriers
ICS Network Architecture	· Common Architectural Zones · Demilitarized Zones (DMZ) · Virtual LANs
ICS Network Perimeter Security	· Firewalls/ One-Way Diodes · Remote Access & Authentication · Jump Servers/ Hosts
Host Security	· Patch and Vulnerability Management · Field Devices · Virtual Machines
Security Monitoring	· Intrusion Detection Systems · Security Audit Logging · Security Incident and Event Monitoring
Vendor Management	· Supply Chain Management · Managed Services/ Outsourcing · Leveraging Cloud Services
The Human Element	· Policies · Procedures · Training and Awareness

An Intrusion Prevention/Detection system(IDS/IPS) is a system that targets traffic after it has passed through the firewall and is responsible for targeting and preventing threats within the network. Configuration of network switches can also let us control and restrict traffic inside our network.

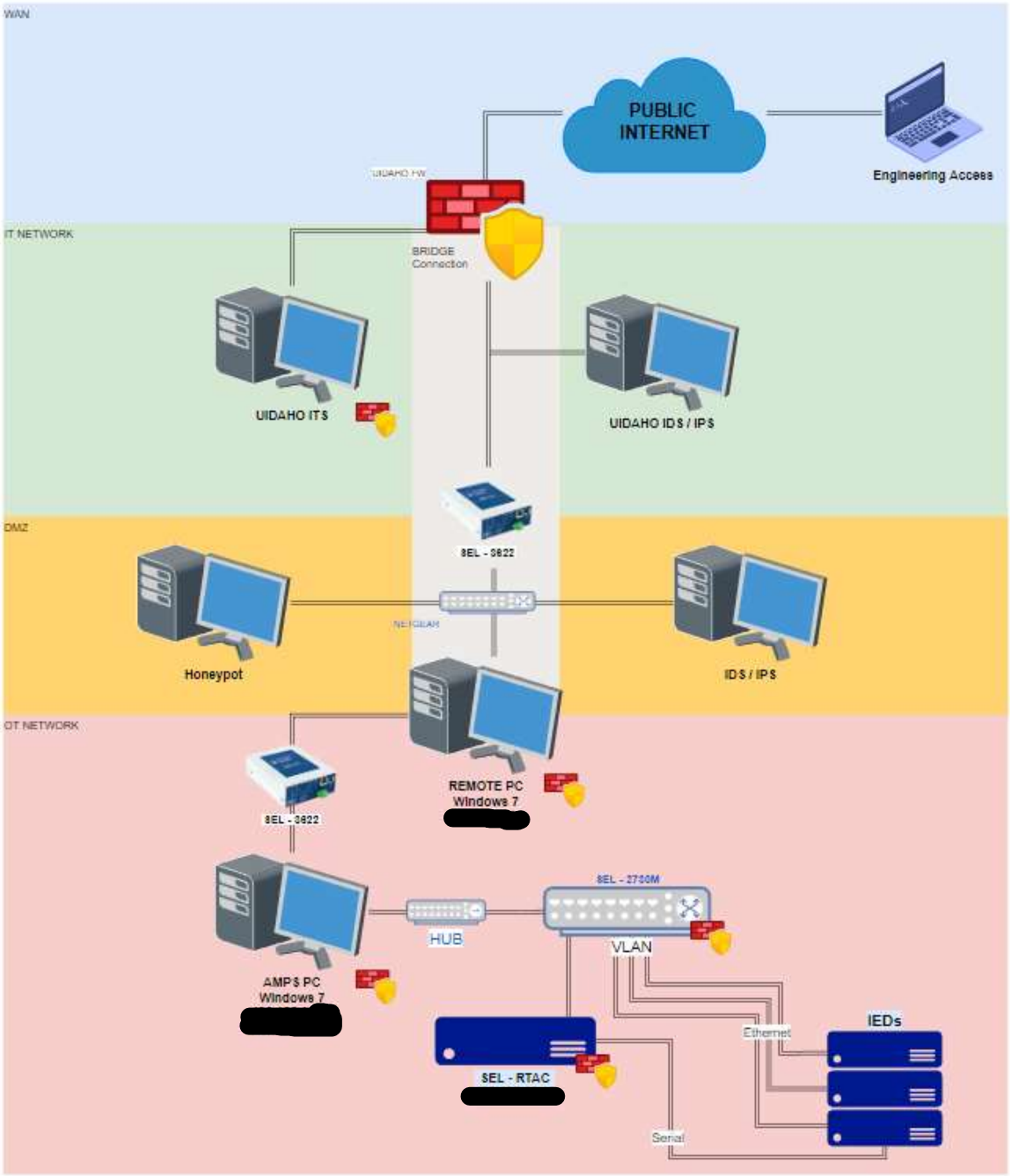
Following the Defense-in-Depth strategy of ICS, there are ample security on individual devices using software to create secure and encrypted connections to devices and closing all other communication ports. The devices we will be using have built systems as well, so let's focus on network architecture and segmenting our network to further regulate and restrict unauthorized communications(Assuming this is an already established ICS).

Configure to represent the following:



1. Take out Selected Ethernet cable and place into NSG
2. Take another cable from 2730M #3 and connect port 12
    - Port 12 is mirroring traffic from Fiber optic cable
3. Connect Eth cable to Port 13 on 2730M #4

Suggested Network Diagram



II Commissioning the SEL-2730M:

1. Connect an RJ45 cable to Port F(on front) of the 2730M(4)
2. Using a web browser enter https://[redacted] into the address bar
   Set IPv4 address on device to[redacted], and the subnet mask to[redacted]
3. Login to the SEL2730M

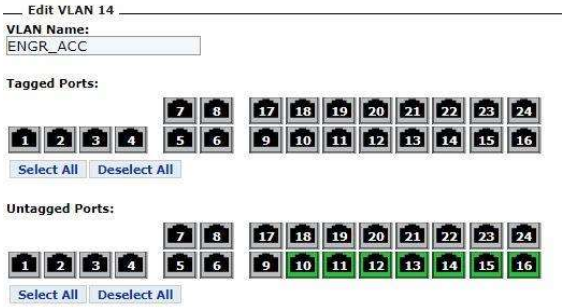
Username	[redacted]
Password	[redacted]
Default Ethernet Port	[redacted]

*Choose Complex Passwords and Rotate every 12 months/Change all passwords

VLAN Connections

1. First enable VLAN by going to System > Global Settings
2. Select VLAN-aware
3. Submit

1. Navigate to Switch Management > VLAN Settings
2. Select Add New VLAN
3. Create three VLANs for Engineering Access, Devices, and GOOSE Protocols(For future development)



4. Set VID any value
   - This is the VLANs unique identifier
   - Remember each one for later steps
5. Select ports 11 – 16 as untagged

a. Name it VLAN Eng_Acc

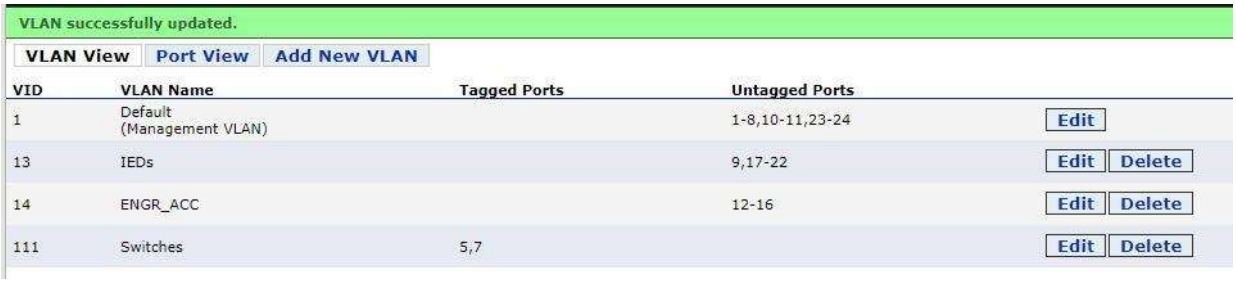
6. On another VLAN select ports 9 and 17-22

a. Name it VLAN IEDs or Devices

7. Create another VLAN for GOOSE protocols to travel between switches.
8. Place the unused ports in separate VLANs to avoid attacks/communication risks across other VLANs.
   - VLAN Attacks

But the better option is to Disable All Unused Ports

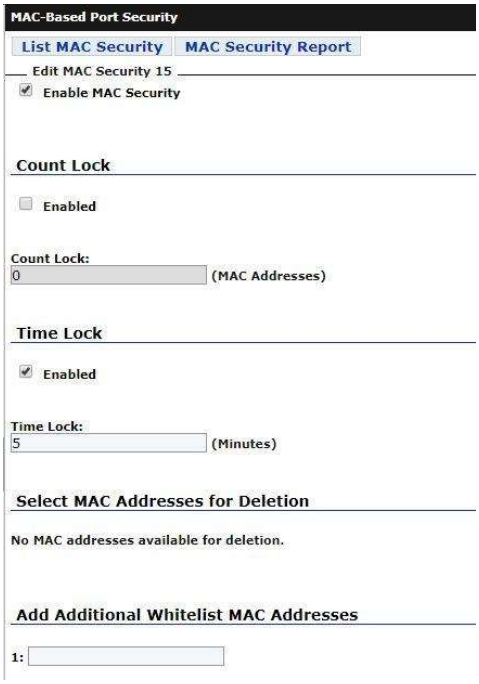
1. Navigate to Network > Port Settings
2. Disable all unused ports
   - There are also flow restriction options



Network Segmentation

MAC Filtering

1. Navigate to Security > MAC-Based Port Security
2. Select Edit on connections that are being used
3. Enable MAC Security
4. Hover over the ‘Enabled’ radical of each option to see description of Count Lock and Time Lock
    a. Whitelisting is allowed list of programs/connections and Blacklisting is the denied.
5. Enable Time Lock
6. Set time to 5-15 minutes
7. Submit
8. Go through and secure all known ports
    - Just do ports 9, 20, 22, and 13 – 15(Just the ones being used)



II Commission the SEL-3622.

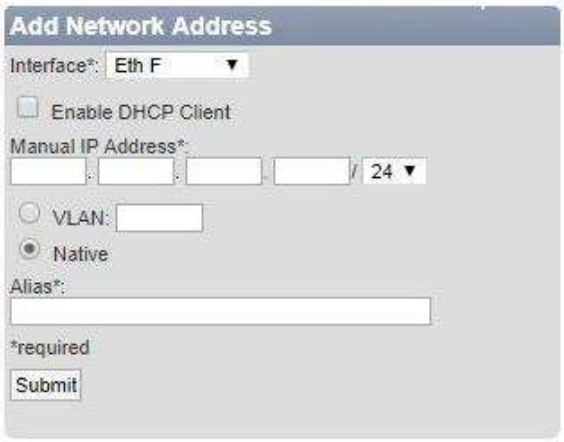
1. Set the IPv4 address on the laptop/PC to [redacted] and the subnet mask to [redacted]
2. Go to https://[redacted] using a web browser of any kind.
3. Username provided by TA (Check important notes of Setup Doc)

**Refer to Lab Setup document if web browser doesn't reload

Configure the NSG

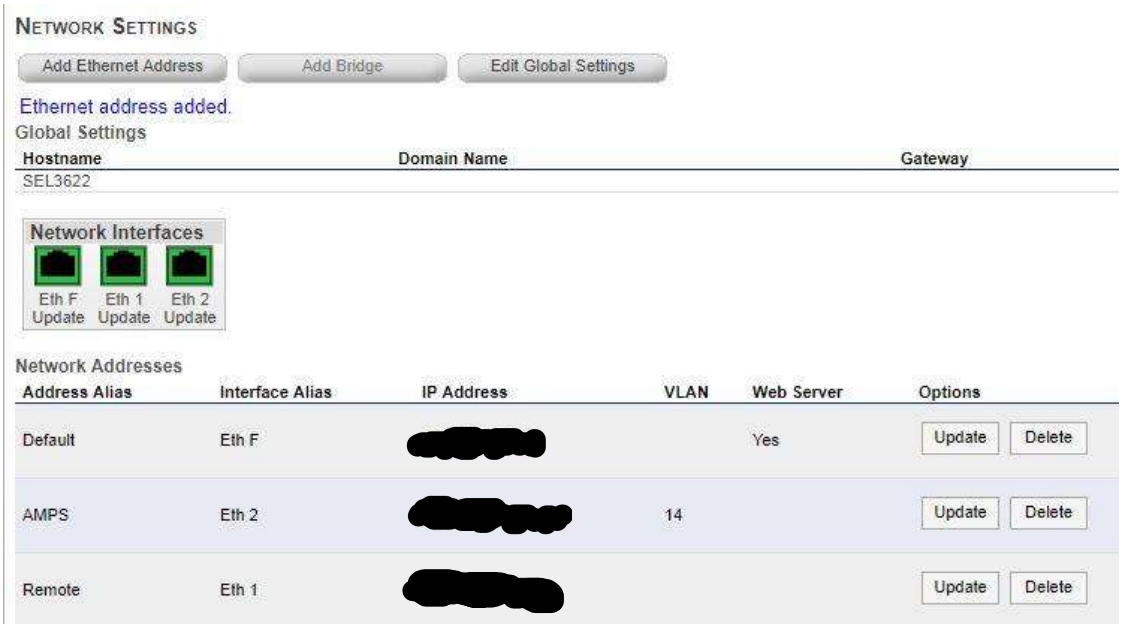
Enabling Ports

1. Go to Network > Network Settings
2. Select "Update" under Eth 1
3. Select "Enabled"
4. Enter Alias "AMPS PC"
5. Submit
6. Repeat with Eth 2 with Alias "Remote PC"



Setting IP Addresses

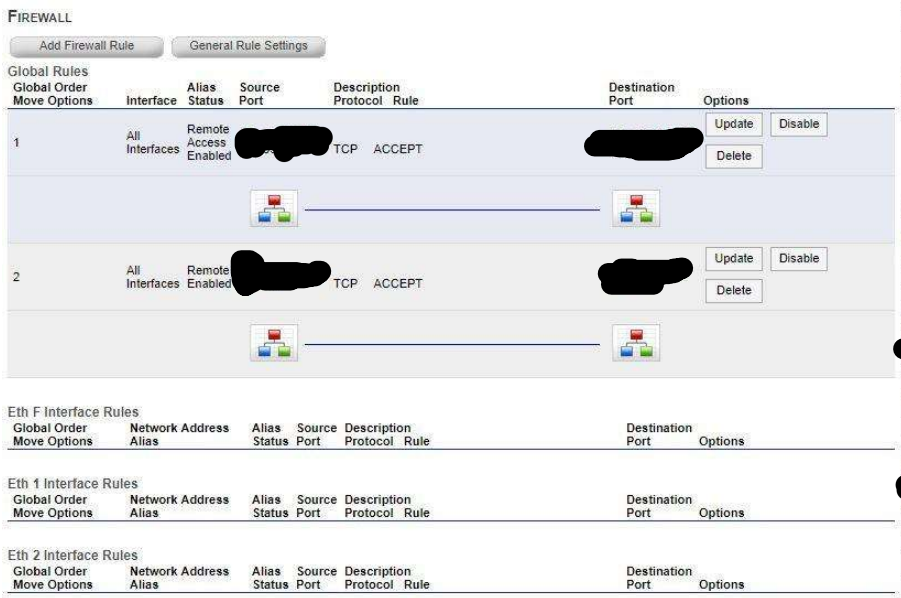
1. Select "Add Ethernet Address" at top of same page
2. Change AMPS PC
3. Enter IP [redacted]
   - Taken IP Addresses will automatically be flagged
4. Select VLAN __ that was set on 2730M for Eng_Acc
5. Submit
6. Select Update for Default
7. Change IP to [redacted]
   - If not on emergency connection, you will be disconnected
   - Change IP of PC to [redacted] and Connect to browser [redacted] or use emergency connection
8. Add connection for Remote PC
9. Enter IP [redacted]

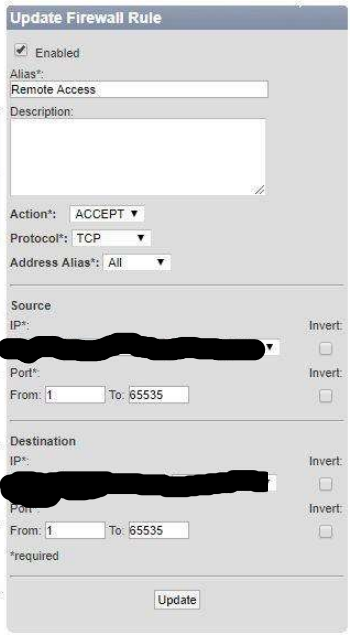


Adding Firewall Rules

1. Go to Security > Firewall
2. Select General Rule Settings
3. Enable Drop Ping, Traceroute and both encryption rules
4. Save

1. Select Add Firewall Rule
2. Enable Rule
3. Set Alias to Remote to AMPS
4. Source [redacted]
5. Destination [redacted]
6. Update
7. Repeat for AMPS to Remote
    - Take note of Source and Destination and configure





Check by trying to remote into the AMPS PC using Remote Desktop Connection and IP [redacted]. Make sure top port of AMPS PC is connected to VLAN of Eng_Acc which is going from NSG > 2730M #3 > Mirrored Port > 2730M #4. Use black F Port cable and connect to top port. Change back any IP altered during setup of 3622.

Setup can be repeated with NSG at UIdaho PC to Remote PC. Likewise, two NSG can be connected with servers or other devices connected between them to act as a DMZ. Most network routers have the ability to implement DMZ networks and can also be done virtually for cloud-based services.