Lab 5 Outline

Background:

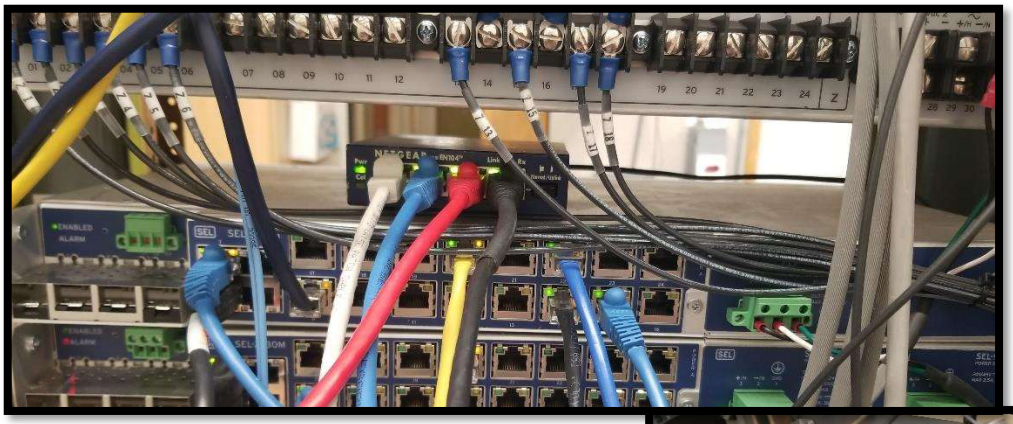
IEC 62433 series of standards and NIST 800-82 outline cybersecurity standards for securing industrial control systems(ICS) using modern IT cybersecurity practices. This lab outlines introductory practices to secure ICS networks. This is a secure network environment where IEDs do not have direct access to sensitive systems and lives are not in danger. Potential risk for implementing on a live system and recommend notifying IT/OT professionals before first proceeding. Use in real SCADA systems can cause adverse damage to equipment and bodily harm/injury.

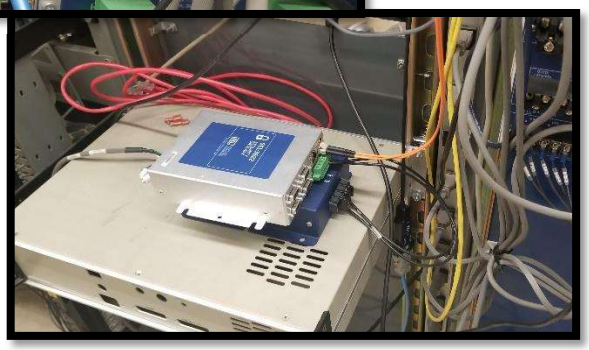
Introduction:

We will 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.

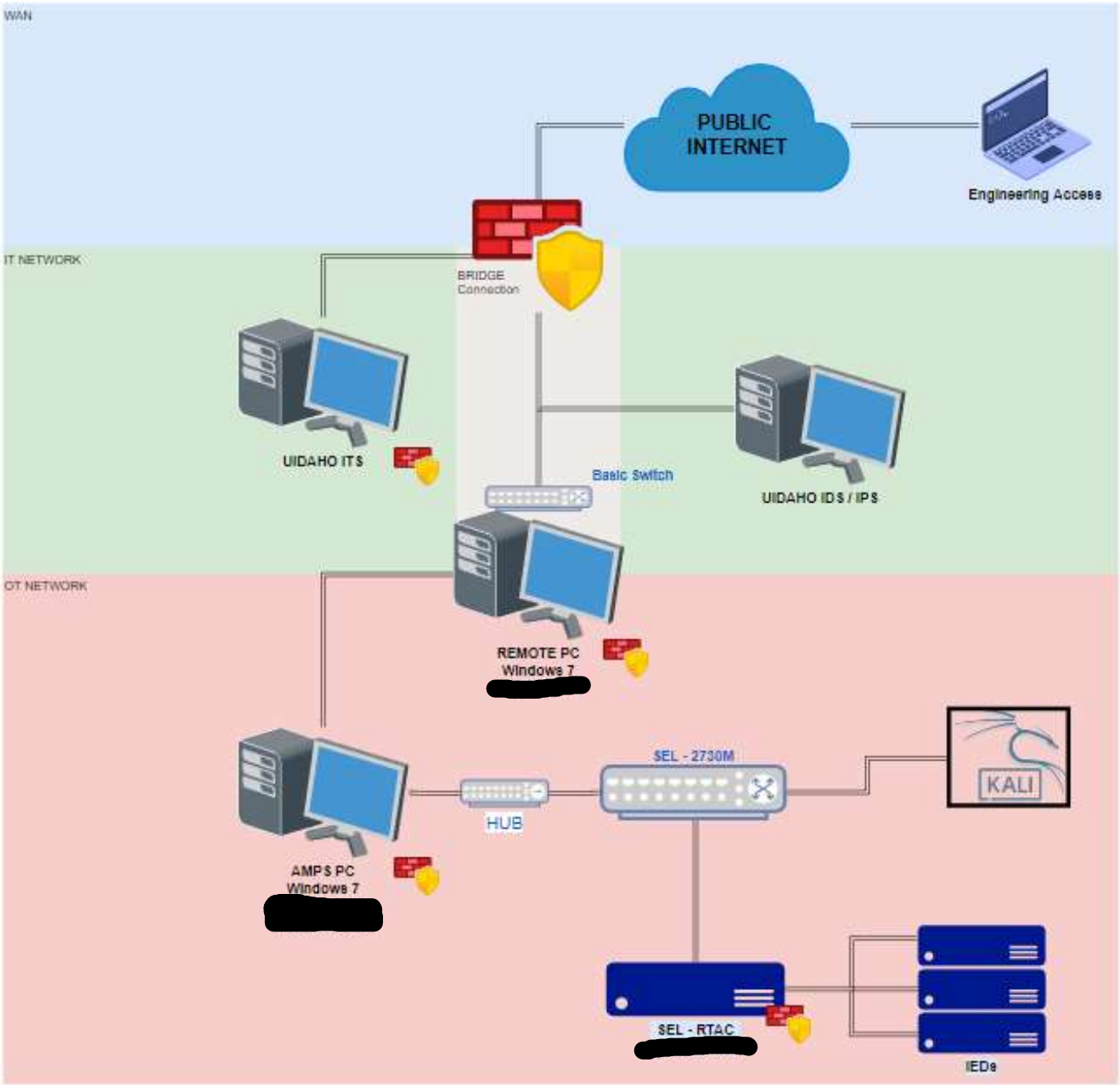
<u>Hardware</u>

SEL-3622(NSG)	SEL-3530(RTAC)	AMPS PC
SEL-2730M x2 (x1 Fiber Optic Switch)	Multiple SEL IEDs	Remote PC





Initial Network Diagram



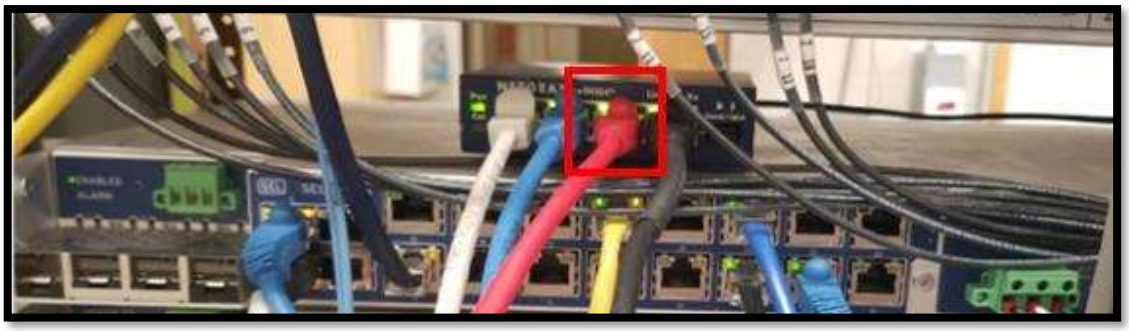
SEL provides hardened IEDs that by factory default offer high security standards. The SEL-3530(RTAC) offers many built in cybersecurity benefits to meet NERC CIP guidelines. One of which is a Stateful Firewall which is a layer 3 and 4 firewall that identifies, and blocks based on protocol and destination 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

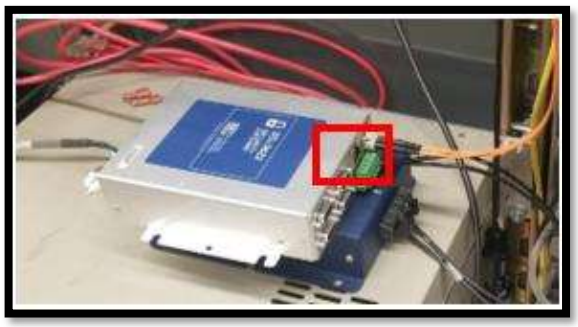
An Intrusion Prevention/Detection system(IDS/IPS) is a system that targets traffic after it has passed through the firewall and is responsible for targeting and preventing threats within the network. Configuration of network switches can also let us control and restrict traffic inside our network.

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).

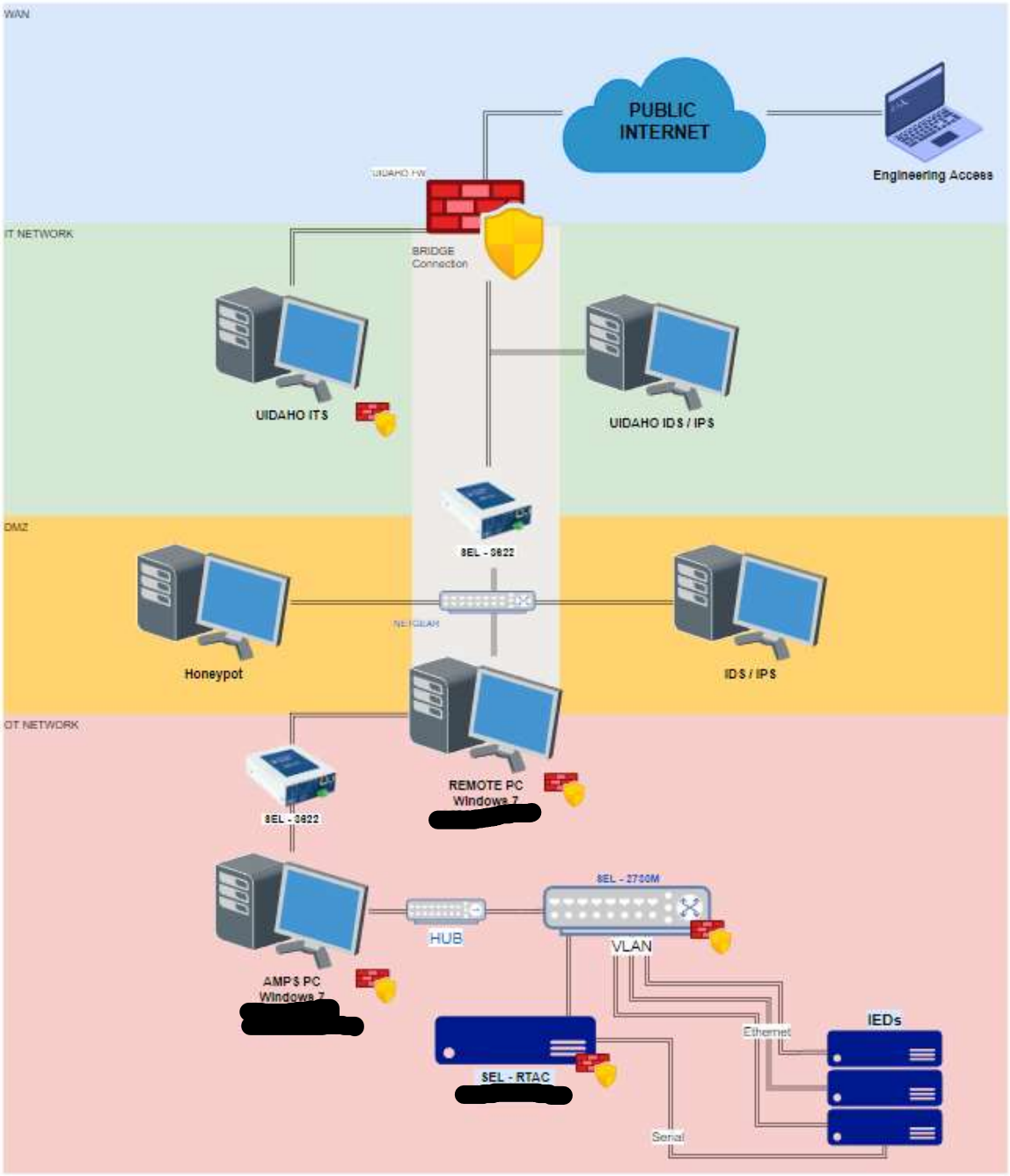
Configure to represent the following:



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



Suggested Network Diagram



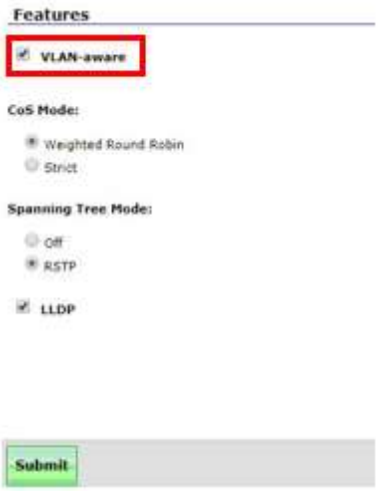
I Commissioning the SEL-2730M:

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	
Default Ethernet Port	

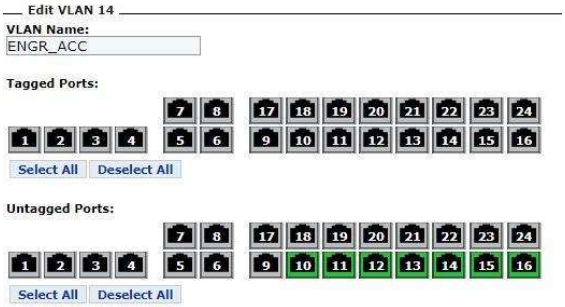
*Choose Complex Passwords and Rotate every 12 months/Change all passwords

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

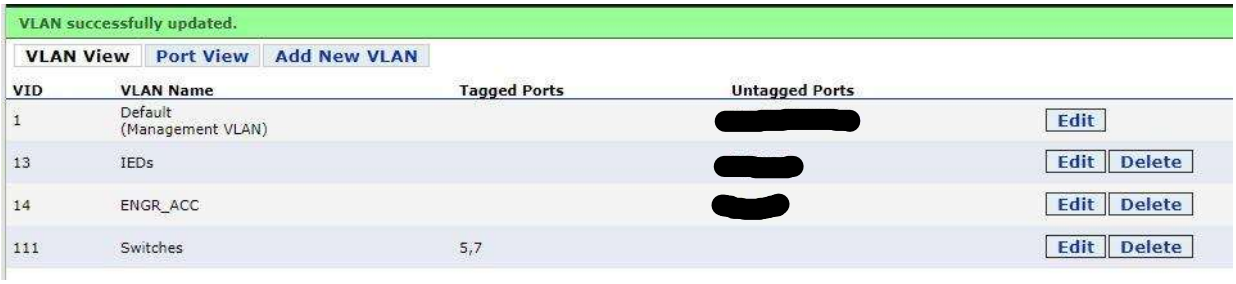
6. On another VLAN select ports 9 and 17-22

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
    - 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)

MAC-Based Port Security

List MAC Security | MAC Security Report

Ports	Enable MAC Security	Status	
1	Disabled		View Edit
2	Disabled		View Edit
3	Disabled		View Edit
4	Disabled		View Edit
5	Disabled		View Edit
6	Disabled		View Edit
7	Disabled		View Edit
8	Disabled		View Edit
9	Enabled : Learning	Total MACs : 1 Remaining Time : 4	View Stop
10	Disabled		View Edit
11	Disabled		View Edit
12	Disabled		View Edit
13	Disabled		View Edit
14	Enabled : Locked	Total MACs : 2	View Edit
15	Enabled : Learning	Total MACs : 1 Remaining Time : 4	View Stop
16	Disabled		View Edit
17	Disabled		View Edit
18	Disabled		View Edit
19	Disabled		View Edit
20	Enabled : Learning	Total MACs : 1 Remaining Time : 5	View Stop
21	Disabled		View Edit

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

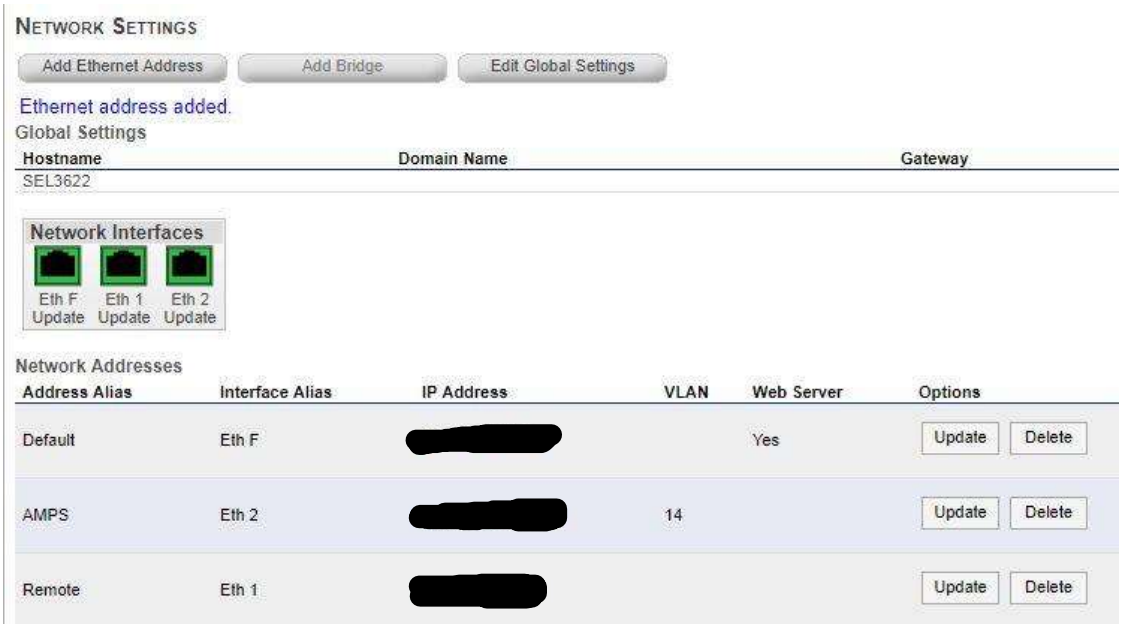
Configure the NSG

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

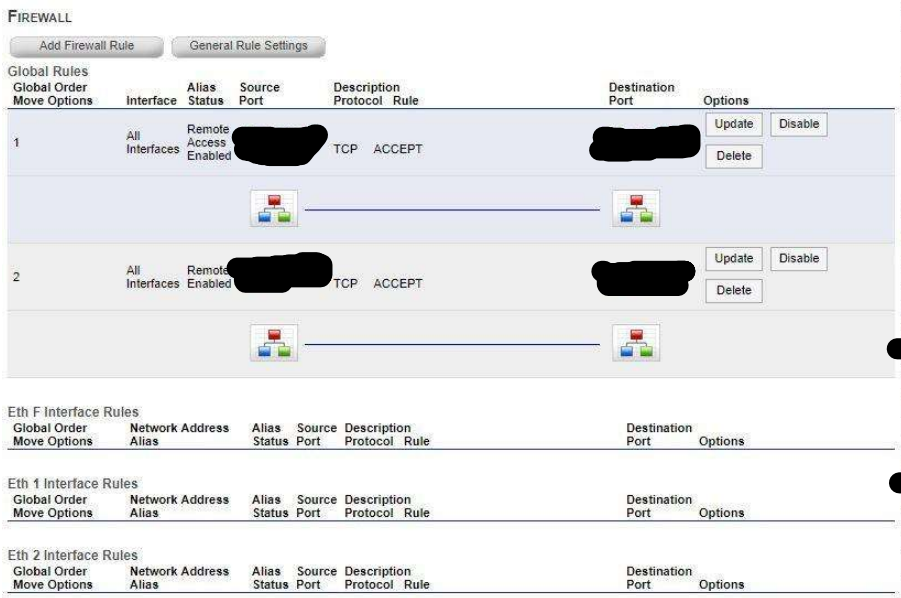
1. Select "Add Ethernet Address" at top of same page
2. Change AMPS PC
3. Enter IP [redacted]
   - Taken IP Addresses will automatically be flagged
4. Select VLAN __ that was set on 2730M for Eng_Acc
5. Submit
6. Select Update for Default
7. Change IP to [redacted]
   - If not on emergency connection,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

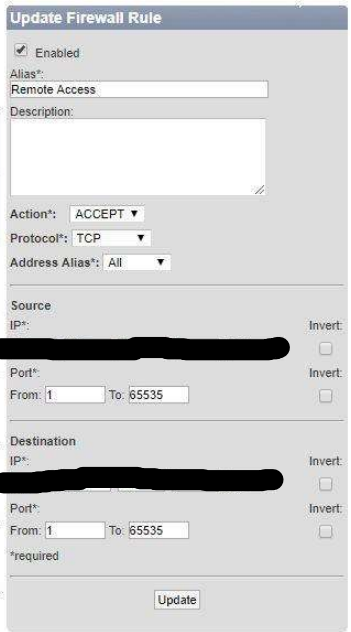


Adding Firewall Rules

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.