

## 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:

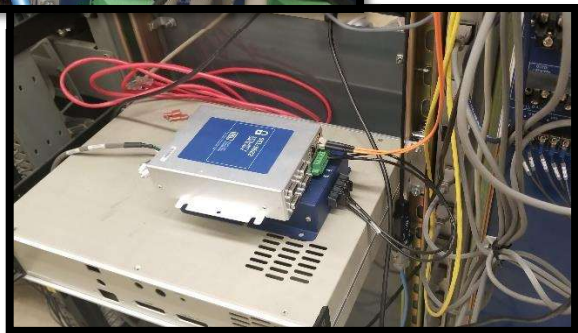
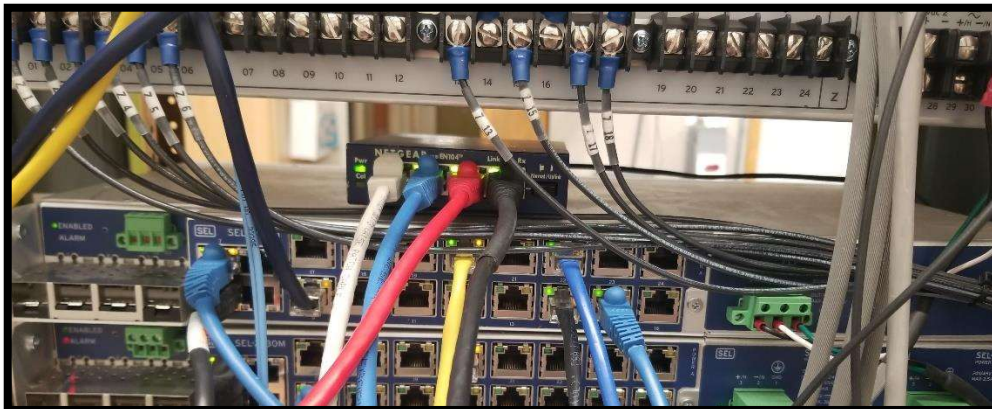
We will configure common devices to provide a secure connection between different subnetworks and gateways to places of concern. In order to so we will be using these devices to configure network switch security and implement a security gateway before entering the next subnetwork within our environment. We do this to restrict unauthorized entry and movement throughout the network.

### Hardware

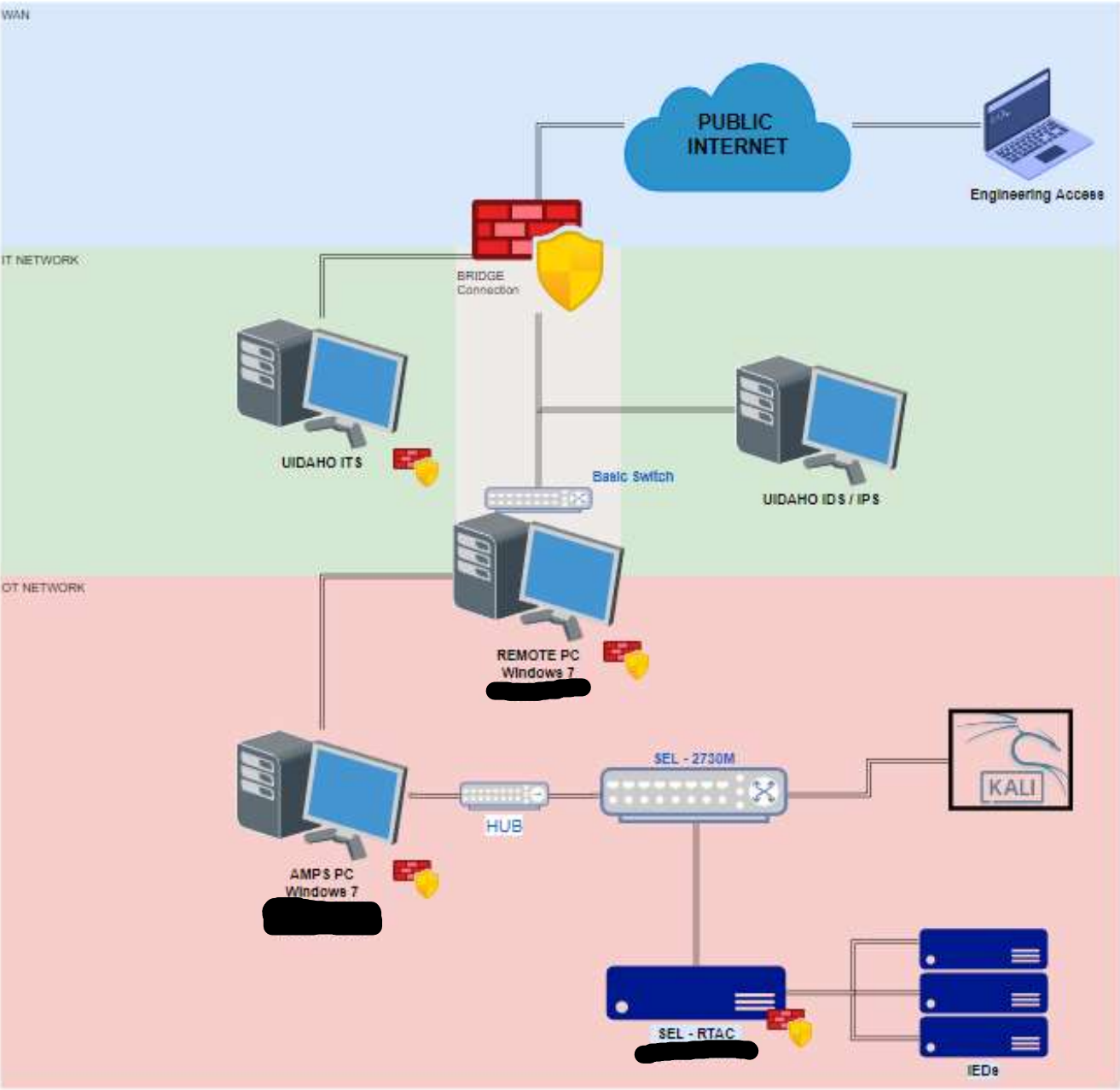
SEL-3622(NSG)  
SEL-2730M x2 (x1 Fiber  
Optic Switch)

SEL-3530(RTAC)  
Multiple SEL IEDs

AMPS PC  
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.

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.

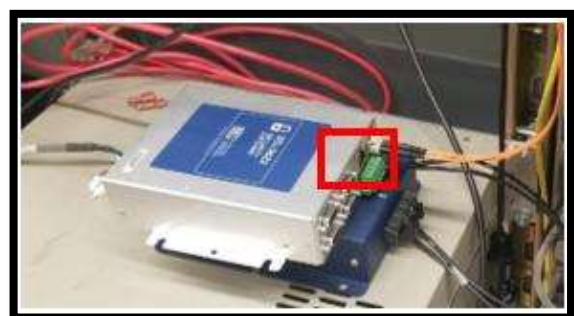
Following the [Defense-in-Depth](#) strategy of ICS, there are ample security on individual devices using software to create secure and encrypted connections to devices and closing all other communication ports. The devices we will be using have built systems as well, so let's focus on network architecture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

Defense in Depth Strategy Elements	
Risk Management Program	<ul style="list-style-type: none"> <li>Identify Threats</li> <li>Characterize Risk</li> <li>Maintain Asset Inventory</li> </ul>
Cybersecurity Architecture	<ul style="list-style-type: none"> <li>Standards/ Recommendations</li> <li>Policy</li> <li>Procedures</li> </ul>
Physical Security	<ul style="list-style-type: none"> <li>Field Electronics Locked Down</li> <li>Control Center Access Controls</li> <li>Remote Site Video, Access Controls, Barriers</li> </ul>
ICS Network Architecture	<ul style="list-style-type: none"> <li>Common Architectural Zones</li> <li>Demilitarized Zones (DMZ)</li> <li>Virtual LANs</li> </ul>
ICS Network Perimeter Security	<ul style="list-style-type: none"> <li>Firewalls/ One-Way Diodes</li> <li>Remote Access &amp; Authentication</li> <li>Jump Servers/ Hosts</li> </ul>
Host Security	<ul style="list-style-type: none"> <li>Patch and Vulnerability Management</li> <li>Field Devices</li> <li>Virtual Machines</li> </ul>
Security Monitoring	<ul style="list-style-type: none"> <li>Intrusion Detection Systems</li> <li>Security Audit Logging</li> <li>Security Incident and Event Monitoring</li> </ul>
Vendor Management	<ul style="list-style-type: none"> <li>Supply Chain Management</li> <li>Managed Services/ Outsourcing</li> <li>Leveraging Cloud Services</li> </ul>
The Human Element	<ul style="list-style-type: none"> <li>Policies</li> <li>Procedures</li> <li>Training and Awareness</li> </ul>

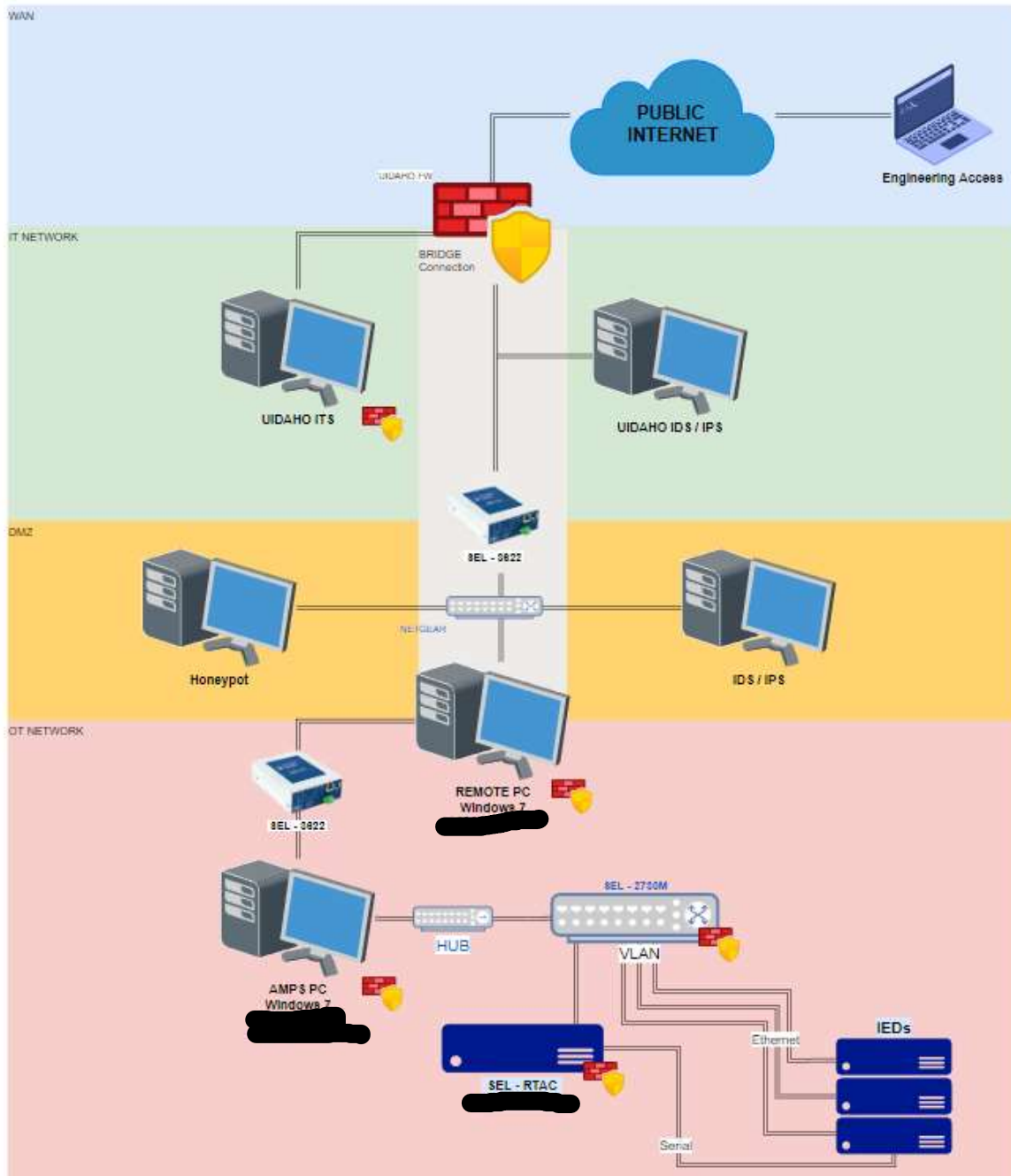
Configure to represent the following:



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

Features

☒ VLAN-aware

CoS Mode:

☐ Weighted Round Robin

☐ Strict

Spanning Tree Mode:

☐ Off

☒ RSTP

☒ LLDP

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)

Edit VLAN 14

VLAN Name:  
ENGR\_ACC

Tagged Ports:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Select All Deselect All

Untagged Ports:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Select All Deselect All

## 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

VLAN successfully updated.

VLAN View Port View Add New VLAN

VID	VLAN Name	Tagged Ports	Untagged Ports	
1	Default (Management VLAN)		[REDACTED]	Edit
13	IEDs		[REDACTED]	Edit Delete
14	ENGR_ACC		[REDACTED]	Edit Delete
111	Switches	5,7		Edit Delete

## 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 SecurityMAC Security Report

Edit MAC Security 15

☒ Enable MAC Security

Count Lock

☐ Enabled

Count Lock: 0 (MAC Addresses)

Time Lock

☒ Enabled

Time Lock: 5 (Minutes)

Select MAC Addresses for Deletion

No MAC addresses available for deletion.

Add Additional Whitelist MAC Addresses

1:

MAC-Based Port Security			
List MAC Security		MAC Security Report	
Ports	Enable MAC Security	Status	
1	Disabled		<a href="#">View</a> <a href="#">Edit</a>
2	Disabled		<a href="#">View</a> <a href="#">Edit</a>
3	Disabled		<a href="#">View</a> <a href="#">Edit</a>
4	Disabled		<a href="#">View</a> <a href="#">Edit</a>
5	Disabled		<a href="#">View</a> <a href="#">Edit</a>
6	Disabled		<a href="#">View</a> <a href="#">Edit</a>
7	Disabled		<a href="#">View</a> <a href="#">Edit</a>
8	Disabled		<a href="#">View</a> <a href="#">Edit</a>
9	Enabled : Learning	Total MACs : 1 Remaining Time : 4	<a href="#">View</a> <a href="#">Stop</a>
10	Disabled		<a href="#">View</a> <a href="#">Edit</a>
11	Disabled		<a href="#">View</a> <a href="#">Edit</a>
12	Disabled		<a href="#">View</a> <a href="#">Edit</a>
13	Disabled		<a href="#">View</a> <a href="#">Edit</a>
14	Enabled : Locked	Total MACs : 2	<a href="#">View</a> <a href="#">Edit</a>
15	Enabled : Learning	Total MACs : 1 Remaining Time : 4	<a href="#">View</a> <a href="#">Stop</a>
16	Disabled		<a href="#">View</a> <a href="#">Edit</a>
17	Disabled		<a href="#">View</a> <a href="#">Edit</a>
18	Disabled		<a href="#">View</a> <a href="#">Edit</a>
19	Disabled		<a href="#">View</a> <a href="#">Edit</a>
20	Enabled : Learning	Total MACs : 1 Remaining Time : 5	<a href="#">View</a> <a href="#">Stop</a>
21	Disabled		<a href="#">View</a> <a href="#">Edit</a>

## 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]

**Add Network Address**

Interface\*: Eth F ▼

☐ Enable DHCP Client

Manual IP Address\*: [ ] [ ] [ ] [ ] / 24 ▼

☐ VLAN: [ ]

☒ Native

Alias\*: [ ]

\*required

Submit

**NETWORK SETTINGS**

Add Ethernet Address Add Bridge Edit Global Settings

Ethernet address added.

Global Settings

Hostname	Domain Name	Gateway
SEL3622		

Network Interfaces

Eth F	Eth 1	Eth 2
Update	Update	Update

Network Addresses

Address Alias	Interface Alias	IP Address	VLAN	Web Server	Options
Default	Eth F	[REDACTED]		Yes	Update Delete
AMPS	Eth 2	[REDACTED]	14		Update Delete
Remote	Eth 1	[REDACTED]			Update Delete

## 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

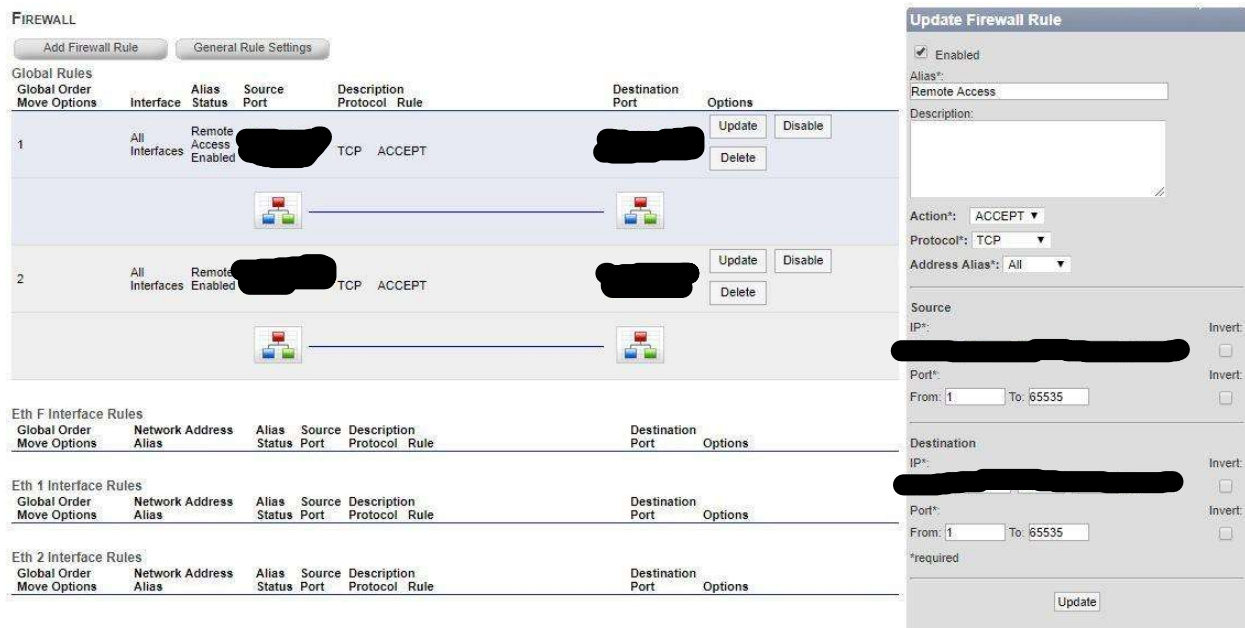


**General Rule Settings**

Move From Above To  
Move From to End

☒ Drop Ping  
☒ Drop Traceroute  
☒ Must Be Encrypted  
☒ Allow All Encrypted  
☐ Verbose Logging  
☐ Text-only View  
☐ Integrated View

Save



**FIREWALL**

Add Firewall Rule    General Rule Settings

**Global Rules**

Global Order	Interface	Alias	Status	Source	Description	Protocol	Rule	Destination	Port	Options
1	All Interfaces	Remote Access	Enabled	[REDACTED]	TCP	ACCEPT		[REDACTED]		Update Delete
2	All Interfaces	Remote Access	Enabled	[REDACTED]	TCP	ACCEPT		[REDACTED]		Update Delete

**Eth F Interface Rules**

Global Order	Network Address	Alias	Status	Source	Description	Protocol	Rule	Destination	Port	Options

**Eth 1 Interface Rules**

Global Order	Network Address	Alias	Status	Source	Description	Protocol	Rule	Destination	Port	Options

**Eth 2 Interface Rules**

Global Order	Network Address	Alias	Status	Source	Description	Protocol	Rule	Destination	Port	Options

**Update Firewall Rule**

☒ Enabled  
 Alias\*: Remote Access  
 Description:

Action\*: ACCEPT  
 Protocol\*: TCP  
 Address Alias\*: All

Source IP\*: [REDACTED] Invert: ☐  
 Port\*: [REDACTED] Invert: ☐  
 From: 1 To: 65535

Destination IP\*: [REDACTED] Invert: ☐  
 Port\*: [REDACTED] Invert: ☐  
 From: 1 To: 65535

\*required

Update

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 Uldaho 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.