University College Cork

Bachelor of Arts - Digital Humanities and Information Technology

Module 2025-DH4003 Research Project

Final Year Project

Supervisor : Mr Gavin Russell

Student name: William Power

Student ID: 121410376

Table of Contents

Introduction

This project was completed in conjunction with the supervision of the Pfizer Automation Infrastructure Team. The purpose of the project was to identify a secure Firewall and to configure it to segregate the site Building Management Systems from the rest of the Pfizer network infrastructure.

The project ran from October 2024 to April 2025. I would like to thank my college supervisor, Mr. Gavin Russell for his continuous support and insightful guidance throughout the year. I would also like to thank my work supervisor, Mr Paul O'Sullivan who is responsible for the management of the Pfizer Ringaskiddy API Automation Infrastructure Team.

1. Abstract

This project focuses on improving the security of the Pfizer Ringaskiddy Building Management System (BMS) and production network. This is done by deploying a layer 2 firewall manufactured by Cisco between the two networks which share the same subnet. The BMS, which shares the same IP range as the manufacturing 4TH LAN (Local Area Network), posed a significant risk due to unrestricted access from third-party contractors and a lack of segmentation from the broader production network. The objective was to isolate the BMS network without disrupting its existing IP addressing or communication data flows.

I first begin with analyzing and understanding the Pfizer Network, the potential security risks and identifying the right firewall. This was completed under the oversight of the Automation and Manufacturing systems infrastructure team. I then move onto researching and applying the right hardware configurations, using both

Cisco's Graphical user interface and Command Line Interface (CLI) tool to build the configurations. This was followed by a testing and simulation of the live environment using real Cisco switches, firewalls, and real Cisco simulators in a controlled test environment.

After incurring some issues with multiple VLAN's (Virtual LAN) and observing how the proposed firewall configuration responded with the installed VLAN's and network segmentation, the final deployment was enforced with strict rules, and easy access for maintainability and management by the infrastructure team. This solution provides a scalable security enhancement to Pfizer's industrial network, reducing the risk of internal threats and unauthorized access, and maintaining regulatory compliance without interrupting production operations.

2. Network Overview

2.1 Pfizer Network

Pfizer Ringaskiddy has a **multi-layered data network architecture**, with different segments serving specific purposes. This infrastructure is strategically important to the company. At the top of the hierarchy, the network **connects directly to the internal Pfizer internet which is also known as the 'Pfizer Intranet'**—this layer is called Entreprise LAN or **'ELAN'**.

- The **ELAN network** is where **Pfizer employee laptops** and **guest devices** (such as personal mobile phones) connect.
- This is the network used for **Microsoft Teams, email, internal website browsing, and other corporate applications**. The external public internet is also accessed via this network layer.

2.2 Middle LAN or MLAN – The Middle Layer

Underneath the ELAN network is the MLAN, known as the ‘middle-man’. What sits on this network is infrastructure such as the Symantec Antivirus Server: Downloads updates from the internet for plant operating systems. Scans updates for malware before distributing them across secure networks.

2.3 Control LAN (layer 2.5) or CLAN 2.5 - Secure Monitoring Layer.

On this network sits a system application called ‘Claroty’. This is a secure monitoring system application where:

1. Most master switches are either directly connected to ‘Claroty’ or linked through intermediary devices.
2. This network application monitors for suspicious activity and prevents malware from spreading.

2.4 CLAN - Manufacturing Network

The Clan network hosts all manufacturing-related systems:

- **DeltaV control systems**
- **4TH LAN**
- **PLANT LAN**
- **Backup systems**
- **BMS (Building Management System), which sits below the 4TH LAN**

2.5 4TH LAN/BMS Network

As the BMS sits below the 4th LAN, it communicates on the same IP range which the 4th LAN uses. The 4th LAN is the manufacturing network where:

Delta V (the distributed control system/application used for the control of production processes in equipment such as reactors, filters and other process

equipment for manufacturing products). Each process production plant at the site (there are six major plants in the Ringasiddy location) has an instance of Delta V installed. Each instance of Delta V hosts several servers linked with local networks for linking process controllers with the Delta V control systems.

PAT (Process Analytical Technology) **LAN** is a framework introduced by the U.S. Food and Drug Administration (FDA) to enhance pharmaceutical manufacturing by designing, analyzing, and controlling processes through real-time monitoring of critical parameters. This approach ensures consistent product quality and aligns with the principles of Quality by Design. The PAT network hosts process analytical instrumentations as well as applications for managing data and access control.

The 4th LAN network is also the home of the **BMS network** on the Pfizer network. Similar to the DeltaV system, the BMS network hosts servers for applications as well as:

HVAC Controllers – Regulate temperature, humidity, and airflow in clean rooms and production areas. The controllers are interfaced to a range of environmental sensors including:

Pressure Sensors – Ensure correct air pressure differentials to maintain contamination control.

Temperature & Humidity Sensors – Monitor conditions in controlled environments, storage rooms, and labs.

Air Quality Sensors – Detect airborne contaminants to maintain compliance with **GMP (Good Manufacturing Practices)**.

3. Previous work experience

In the summer of 2023, I was able to gain hands-on Cisco hardware experience. The project I worked on was the RCMF plant build. The job role title was 'Industrial Infrastructure and Automation Student Engineer'.

3.1 My day to day tasks included:

1. Interconnecting multiple switches to build networks across rooms using patch panels (including BMS)
3. Managing operator interface terminals (shop floor PCs), ensuring that they are working as networks often start up and shutdown.
4. Commissioning manufacturing equipment like valves, pumps and reactors with use of Delta V
5. DCS (application software which controls manufacturing equipment).
6. Shadowed Cisco expert in installation of Clan 2.5 to MLAN firewall.
7. Infrastructure maintenance when networks came down (rebooting switches/ reconnecting switches)

During my free time and lunch breaks, I also was able to complete the **Cisco Networking Basics** online course. This gave me the necessary foundational understanding to learn about the network topology and how it is organised and configured.

4. The BMS network security issue

The bms network is set up by the site infrastructure team, but the environmental monitoring and control work, and as well as the systems configuration is carried out by a subcontractor called Sygma automation. They have full access to the BMS

network, and could also knowingly/unknowingly carry malware into the BMS network, which could potentially impact the full site network, via the 4th LAN. Also an untrained engineer could interfere with network configurations exposing 4th LAN to more threats.

4.1 The Proposed Solution:

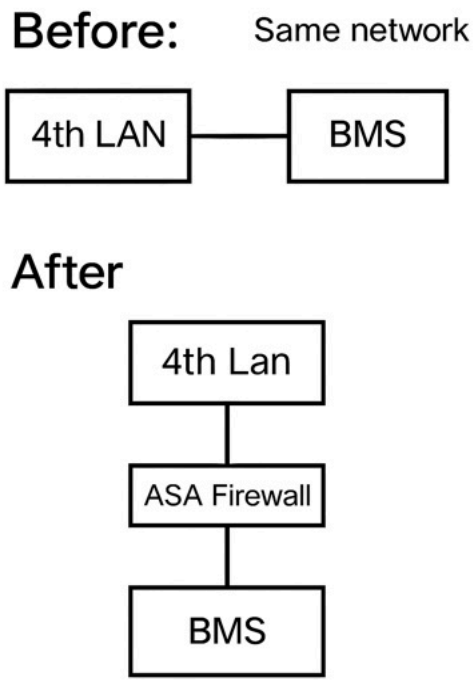


Figure 1 - The Proposed Solution

4.2 What does this firewall do?

(Cisco Systems. (n.d.). General ASA Configuration Guide (v9.12))

- Filters all traffic and allows only BMS traffic talk to the 4TH LAN (Manufacturing LAN)

- Limits allowed traffic to only communicate on allowed ports, which keeps network secure

- Allows both VLANS (Pfizer use one for management and another for BMS activity)

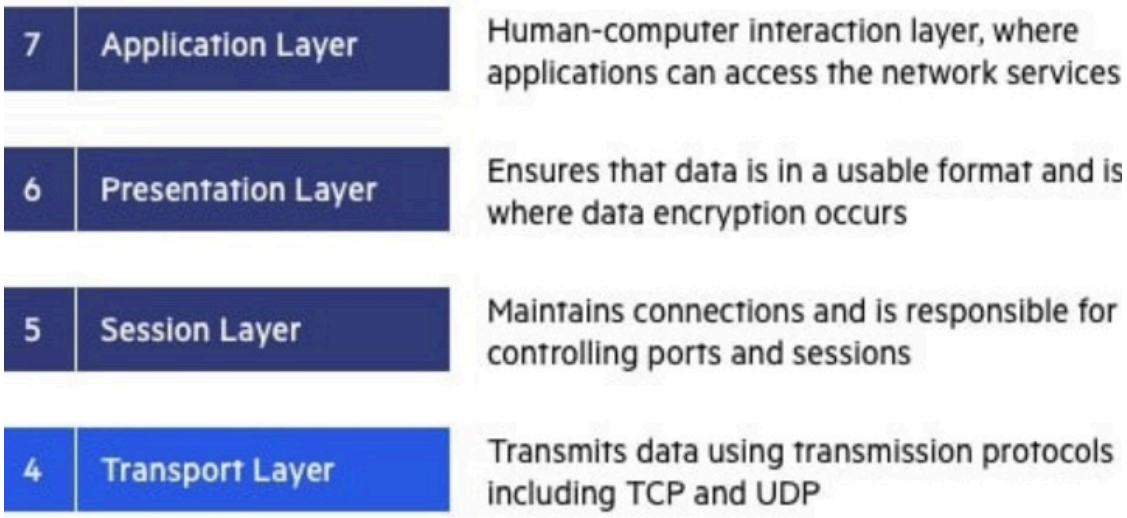
- Logs all network traffic and events

- Most importantly: Segments the 4Th LAN and the BMS from the rest of the site and company network.

4.3 Why Firewall Security? - What Is a Firewall? - Cisco

Firewall security offers protection against common network threats and attacks. The Cisco network Firewalls regulate incoming and outgoing network traffic based on preset security rules. Firewalls are paramount in shielding networks from unauthorized or harmful activities.

Firewalls can be set up in both transparent configuration (network data format layer 2) and routed configuration (physical path defined traffic layer 3), which depending on network design and configuration is an essential step. The differences are based upon the OSI (Open Systems Interconnection) industrial standards layer model - see diagram below (Figure 2).(**Cisco Systems.** (n.d.) *OSI Model Reference Chart*.)



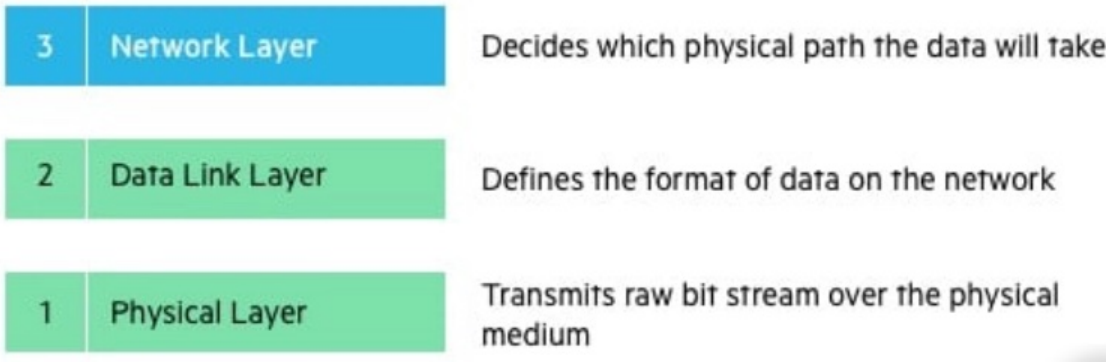


Figure 2 - Layer Diagram

The layer 2 switch, set in firewall transparent mode, works off the data link layer. The goal is to filter and monitor traffic without routing. It forwards ethernet frames between its interfaces.

According to the official Cisco website (2021), in layer 2, firewalls act as an 'invisible' device that works within the same IP subnet. It doesn't rely on IPS on each interface, but uses a bridge virtual interface (bridge group) for management purposes.

Cisco recommends this set up for environments (similar to the 4th LAN – BMS) where infrastructure engineers don't want to disrupt the current IP scheme.

Cisco Systems, Inc. (2021). Cisco ASA Series Firewall CLI Configuration Guide, 9.16: Transparent or Routed Firewall Mode. Cisco Systems.

4.4 What is an IP Address?

Every device has its own IP address. It is similar to a home address, you can trace where it originates from using an IP address.

Example:

1. The Area could be 192.168.230.0 is the network IP Address similar to ‘Firgrove Lawn, Bishopstown, Cork - i.e. the Area
2. The Specific house address could be 192.168.230.**17** = device IP address similar to ‘**17** Firgrove Lawn, Bishopstown, Cork’.

For a specific house in the area, the last number is individual (17) and the second last number is unique for a network. A network can have multiple devices in it. Every network has an IP address. A single network can have many devices, each with a different IP.

4.5 What is a VLAN?

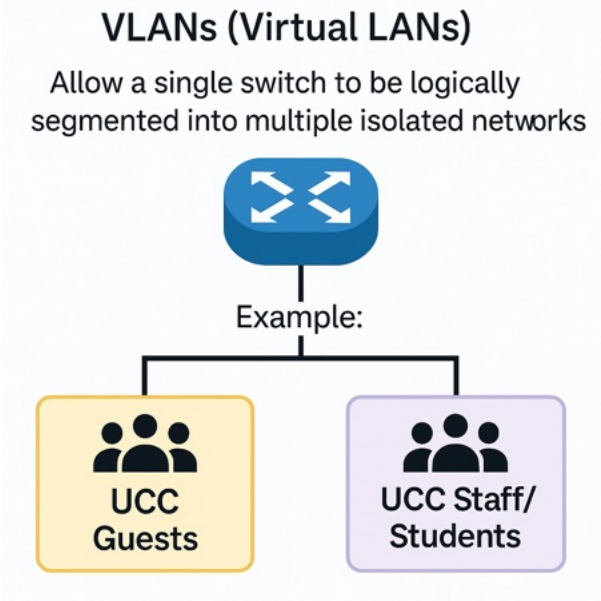


Figure 3 - Virtual LANS

A physical switch on campus (UCC) is hosting **two separate networks**:

- **UCC Guests**
- **UCC Staff/Students**

Even though they're both connected to the **same switch**, they are **logically separated** using **VLANs**, which prevent the networks from seeing each other.

In Pfizer, VLAN's are used for traffic management. In this document, I will only be referring to VLAN 800 and VLAN 500. VLAN 800 is the production LAN and VLAN 500 is used for infrastructure management.

(Cisco Systems. (n.d.). Understanding and Configuring VLANs on Catalyst 4500 Series Switches)

(Cisco Systems. (n.d.). IP Addressing and Subnetting Overview)

4.6 Layer 3 Firewall (routed)

A layer 3 firewall / 'Routed' firewall operates at the network layer. This type of firewall must have routes set. Layer 3 firewalls read incoming and set destination IP s and dictate where the packets are sent, also monitoring if they are malware or not.

Cisco explains that layer 3(routed) firewalls are implemented when multiple networks or when inter-subnet communication requires security.

While a layer 3 model can be favoured for futureproofing of network security, they can be quite complex and require high maintenance when changing the network.

Once done analysing your network requirements, then you should decide what type of firewall is needed.

Basically:

Layer 2 is when only 2 networks are connected to each other and the firewall passes devices through. Example:

Flying from Cork to Dublin

- **Cork and Dublin both have different IP addresses (can be in the same or different IP range).**
- The firewall acts like **border control**, deciding **who can pass, who gets checked, and who is blocked**.
- When a packet wants to travel from **Network A (Cork) to Network B (Dublin)**, the firewall **just passes it through.**

Layer 3 is when 3 or more networks are connected the firewall needs to create routes for the devices to travel through,example

Think of it like a **security checkpoint between two different countries**:

- **Each country (network) has its own address system (IP range/subnet).**
- The firewall acts like **border control**, deciding **who can pass, who gets checked, and who is blocked**.
- When a packet wants to travel from **Network A (Country A) to Network B (Country B)**, the firewall **doesn't just pass it through like in Layer 2**—it **looks at the destination, changes addresses if needed, and decides the best route**.

(Cisco Systems. (n.d.). General ASA Configuration Guide (v9.12))

(Cisco Systems. (n.d.). ASA Command Modes and CLI Guide)

5. Why is network security important for a company like Pfizer?

The strategic significance of network security for a business such as Pfizer is critical. Organizations throughout the world see an average of 1168 cyber attacks every week, a 38% rise from the year before, according to a 2023 analysis by Check Point.

Because of their position in the pharmaceutical industry, companies like Pfizer and Eli Lilly likely experience greater attacks, including sophisticated attempts to obtain vital data or obstruct corporate operations.

For example, Pfizer was the subject of a cyberattack during the COVID-19 pandemic in which hackers obtained papers pertaining to the company's vaccine development.

This explains why the security at the top end of the network is very secure. With the BMS network having a direct open connection into the 4th LAN creates a security breach.

5.1 Which Type of firewall suits the network Best:

A Layer 2 Firewall which only passes data from the allowed devices through the network. By using IP filtering - (limiting traffic to known IP addresses) and MAC - Media Access Control address locking (locking to a specific network switch to a port on a switch, so that the device can only access the network from that specific switch, or switch port) to identify these devices.

Setting up a layer 2 will also be a **non-disruptive deployment**.

This minimal-disruption strategy is beneficial in a complicated network like Pfizer's, where there are several fixed-IP devices and established communication flows (like controllers in an industrial network). It enables the addition of security without changing the network design. While allowing for new controllers to be added to the network without having to create routing in the firewall.

(Check Point. (2023). Check Point Research Security Report 2023)

(Cisco Systems. (n.d.). General ASA Configuration Guide (v9.12))

(Elsevier. (2014). Industrial Network Security (2nd ed.))

5.2 Ideal for segmenting and isolating the network segments

Industrial networks with fixed or older equipment benefit greatly from the ability to split and isolate sensitive network segments using a Layer 2 firewall without the need for IP-based intervention. Network attack surfaces are decreased and internal security is improved by segmenting sensitive regions, such a Building Management System (BMS) network. Network isolation and segmentation are essential tactics for industrial control systems to minimize lateral movement and restrict access to only authorized devices, claim Stouffer et al. (2015).

Also because **Layer 2 firewalls** don't require complicated routing setups, they provide easier management for networks with fixed assets. Because administrators can utilize simple MAC-based policies instead of intricate IP-based Routing configurations, this system is especially advantageous for controlling static devices in industrial settings. (Elsevier. (2014). Industrial Network Security (2nd ed.))

5.3 Which firewall to be used and why?

Using the company's suppliers, the infrastructure team identified the firewalls most suitable for this application as Cisco Model ASA 5516-X firewalls.

My role here was to research and preview how this firewall could and would be implemented. Also, I had to find out how this firewall could work under the circumstances prevailing in the current Pfizer network topology. Every device on the network could all be communicating simultaneously. For example, while the networks are operational, an engineer could be downloading updates from the Cisco system administration server ‘Cisco Aspect’.

Tasks for my role included researching the configuration guide for the Cisco Model ASA 5516-X, I had to ensure that the firewall was capable of:

- Filtering traffic using Access Control Lists (ACLs) - understanding how to configure modular firewall rules as well as understanding the implications of the rules in terms of network traffic controls - so you can design the firewall configuration for our needs.
- Supports transparent mode (Layer 2) - Layer 3 can be difficult to maintain and that level of complexity was not required for this application.
- Stateful packet inspection - Ensures that only the allowed traffic is allowed - even access for the allowed PCs' or allowed network devices is restricted to the data communication routes they need to function. This is achieved by opening and closing communication ports as required.

This was all deemed possible from the Cisco configuration guides and the firewalls were delivered by the vendor on the 14th of November, 2024.

5.4 What is a bridge group and why is it best suited for this network?

A bridge-group acts as a ‘gatekeeper’ on the connection of a network. It can be used to segment the network, such as the following:

The bridge-group on the CISCO ASA firewall will:

- Have the same subnet on each side of the firewall, a bridge group allows traffic to flow between **without changing IP addressing and routing.**
- Allows the firewall to control traffic without acting as a router, this will ensure no change to the network can be performed - as in layer two the firewall sits transparently.

The bridge group eliminates the need for routing (allowing for reduced maintenance) while creating the segmentation needed between the 4TH LAN and the BMS network. Due to the minimal requirements for alterations to the network design, the bridge group is the most optimal path to choose when configuring the firewall. Cisco Systems. (n.d.). General ASA Configuration Guide (v9.12)

6. What is Cisco ASDM and why is it important?

Cisco ASDM is a Graphical User Interface. As explained by Cisco, ‘Cisco Adaptive Security Device Manager (ASDM) lets you manage Cisco Secure Firewall ASA and the Cisco AnyConnect Secure Mobility Client through a local, web-based interface.’

This can support you in configuring the firewall using a user-friendly interface which can be used alongside the CLI (Command Line Interface) - the Cisco syntax used to code the firewall.

The benefits of the Cisco Adaptive Security Device Manager include:

- Setup wizards that help you configure and manage Cisco firewall devices. These prompt some of the more complex configurations.
- Real-time log viewer and monitoring dashboards that provide an at-a-glance view of firewall appliance status and health. I found this feature quite powerful.
- Troubleshooting features and powerful debugging tools such as packet trace and packet capture. This feature also helped in the testing and commissioning of the firewall.

(Cisco Systems. (n.d.). ASDM Product Page)

6.1 Accessing the GUI (Graphical User Interface)

All firewall configurations came from Cisco configurations guides like:

Cisco Systems. (n.d.). General ASA Configuration Guide (v9.12),

Cisco Systems. (n.d.). ASA CLI Configuration Guide – Logging. Available at: CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.16.

Cisco Systems. (n.d.). *ASA Access Rules and Service Object Definitions*

This guide was put into ‘Chat GPT’ and I requested what exactly was the command needed.

6.2 Configure the management pc for the Firewall

What do you need for this step?

- ➔ A Windows 10 pc
- ➔ Your asa 5516-x firewall
- ➔ Kettle lead power cable for firewall(comes in box)
- ➔ A usb type A to usb type B serial cable.(comes in box)
- ➔ Internet access

Setting up the configuration system

Plug in and power up the firewall. Also power up your pc. Get an ethernet cable and plug this into your computer's ethernet port. Put the other end into the ‘MGMT’ (Management) Port on the firewall to establish an interface.

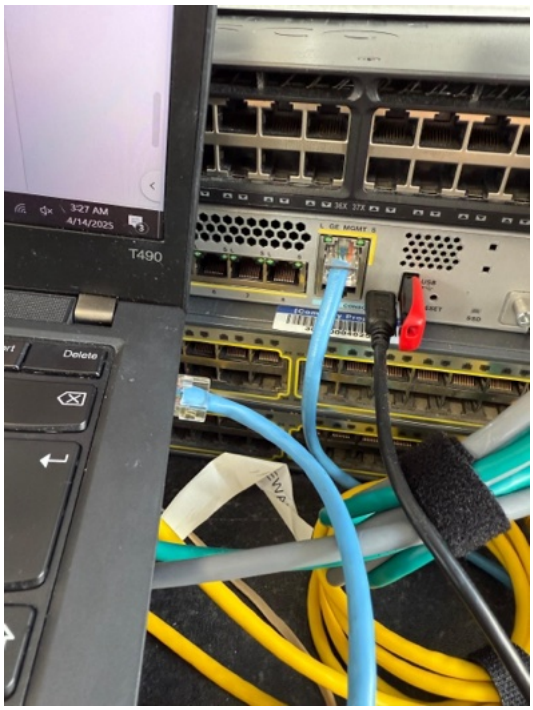


Figure 4 - Configuration System

6.3 PC Configuration

Go to your network settings and select ‘Ethernet’, then select change adapter options. A new tab will appear and you will see ethernet. Right click and select ‘properties’

It should look like this:

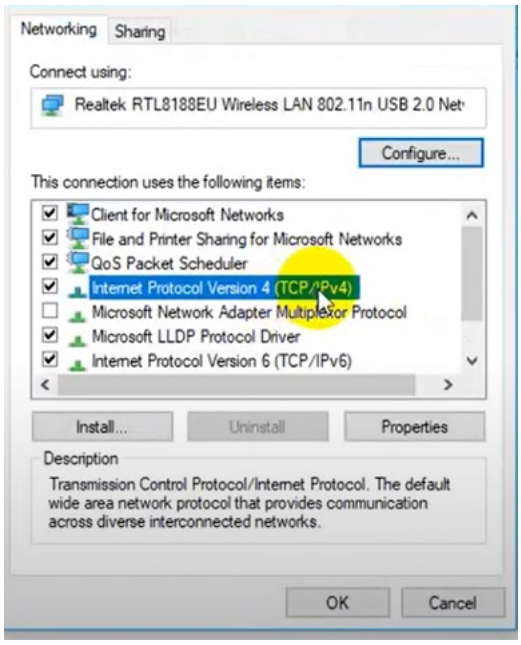


Figure 5 - PC Configuration

Head down to ‘internet protocol version IPv4’. Select ‘use the following IP address’ 192.168.10.10’ - ***we will configure the firewall to allow this pc on the network so it will be able to access the GUI.*** -save your IPv4 settings and close.

You will now have to connect your pc to your firewall. This is a management pc and will need a ‘serial cable’ (which comes with the firewall) to be able to code your firewall.

6.4 What is a serial cable?

This is a data transfer cable which will allow you to send configurations to your firewall to PC. As per Figure 6 below, plug the small end (USB type B) into the firewall-the console port and the USB (type A) into a USB port on your computer.

Figure 6 - USB Ports

You will have to download ‘putty’ from the putty.org website. Ensure you select the correct download for your PC.

Once ‘putty’ is downloaded and set up, you can use the search bar on your pc and open ‘**Device Manager**’. Here you will select ports and see what comm port you are using.

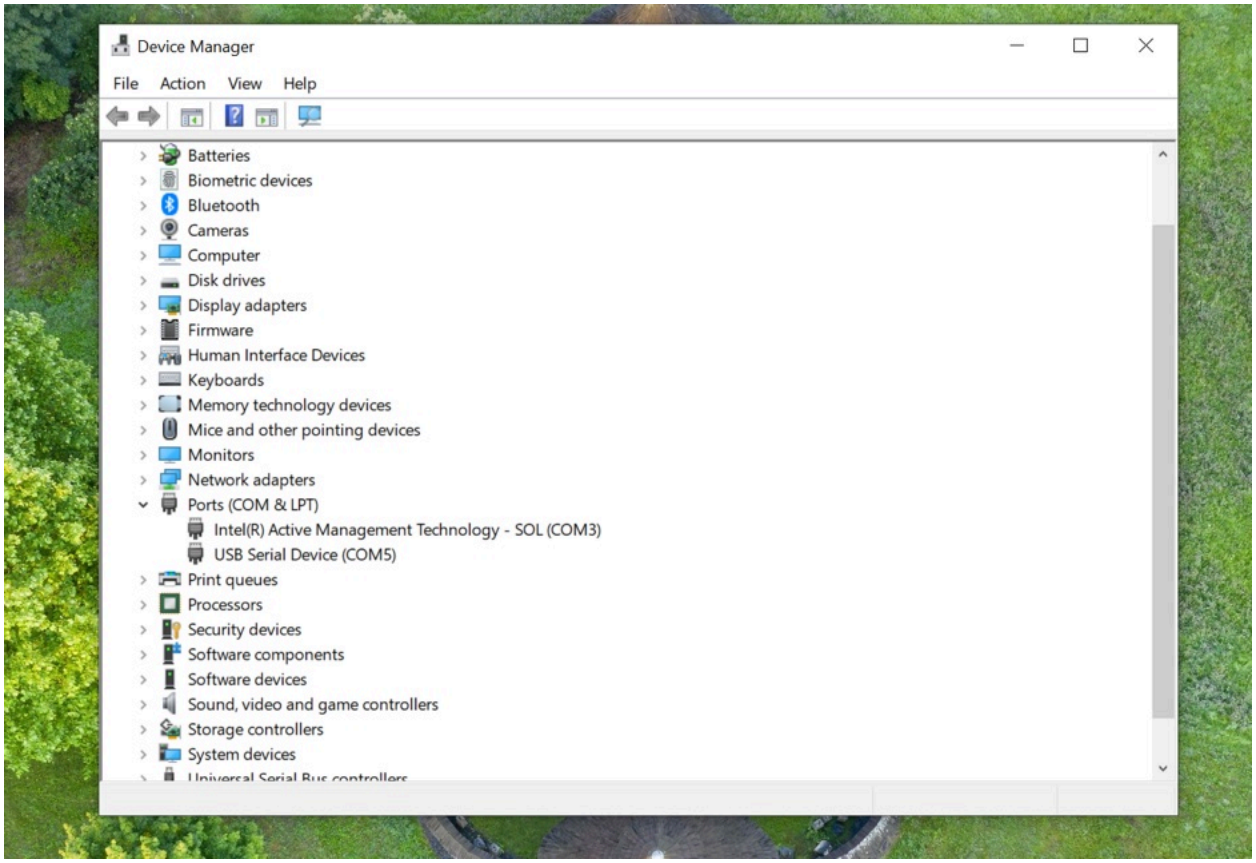


Figure 7 - Device manager

Now open ‘putty’. It should look like this:

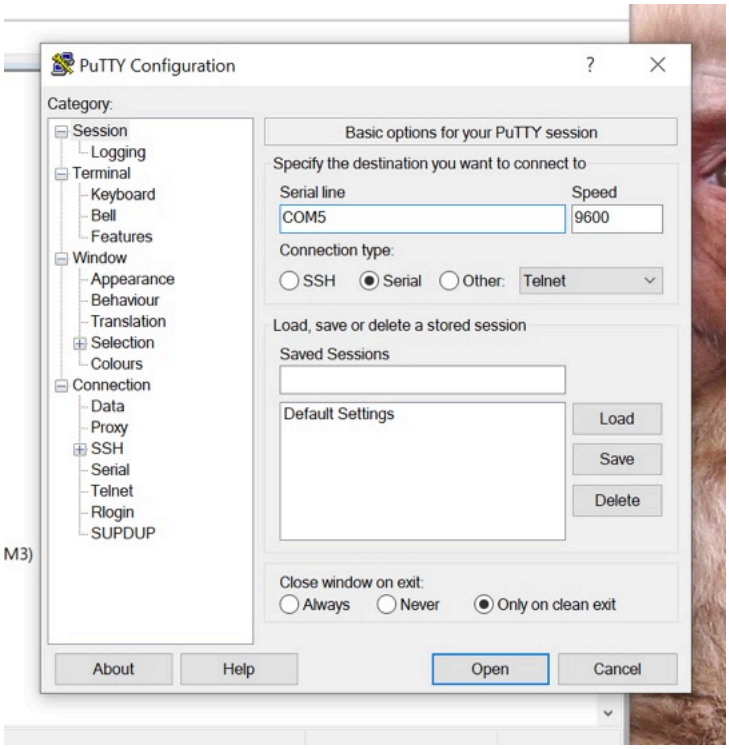


Figure 8 - PuTTY Configuration

Select '**Serial**'.

Now use the remember the comm number so 'putty' knows what USB port to talk to on your PC. This will open the CLI which you can control the firewall.

6.5 First power-up

This will be the firewalls first run, you will need to select the first basic settings:

- Date and time
- Firewall name
- Firewall password
- Enable password (to be able to make configuration changes)

The firewall will walk you through this set up and it will be straightforward.

6.5 Firewall configuration

After the initial set up is completed above, your cisco asa should look like

ciscoasa>

In which when you type commands in it will appear like:

ciscoasa>Enable

'Enable' puts the firewall in the USER EXEC mode. This will give you basic access to commands, to be able to see your network, and your current configurations but you won't be able to make any change.

Should now look like:

ciscoasa#

Everytime you want to enter configuration into the firewall you must be enter;

'*configuration terminal*'

('*conf t*' for short)

This will enter you into global configuration.

'Global configuration mode' **lets you change the ASA configuration**. All user EXEC, privileged EXEC, and global configuration commands are available in this mode. Enter the configure terminal command in privileged EXEC mode to start global configuration mode. The prompt enters you into the configurations mode- explanation from Cisco.

To identify you are in global configuration mode, it should look this: *ciscoasa(config)#*

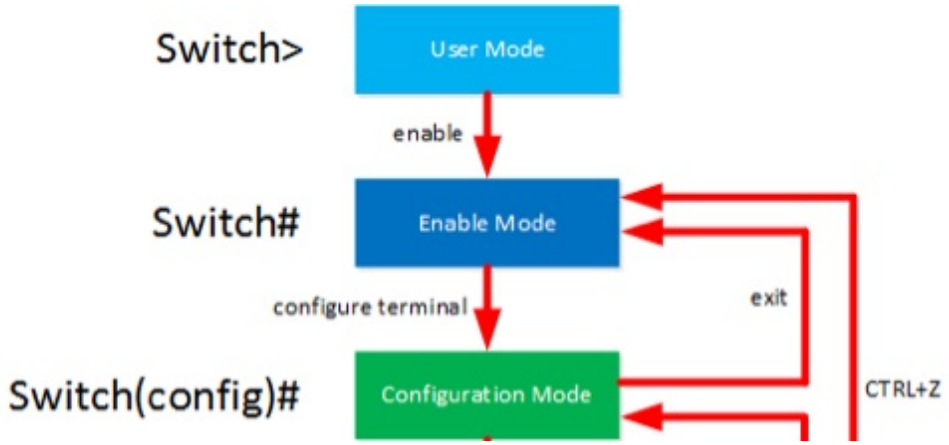


Figure 9 - Firewall Configuration

You can press CTRL Z to exit each one but as you enter layer by layer(enable mode to configuration mode) you'll exit layer by layer (by exiting configuration mode you'll be back to enable mode).

You must now check the status of the firewall to see if it is in 'routed' or 'transparent mode'. For this configuration we want it in transparent mode as there are no routes needed. To see if you're in routed (comes stock routed) or in transparent mode, you'll need to be in enable mode(USER EXEC).

ciscoasa#Show firewall

The firewall will spit back:

Firewall routed

Or

Firewall transparent

If it says **routed** we will need to change it to **transparent**.

You can do this by typing:

ciscoasa#conf t
ciscoasa(config)#firewall transparent

As you can see here we entered the firewall into global configurations mode (config t) to make a change to the config. Then we entered the firewall into transparent mode (firewall transparent).

```
EIRRCMFBMSFIREWALL01# conf t
EIRRCMFBMSFIREWALL01(config)# firewall transparent
```

We had to make this change as if you swap from transparent mode to routed it wipes any configurations made by the user.

6.6 We can now start to access the ASDM

The following steps are required to access the ASDM

Step 1: Connect to the ASA and configure the management interface
Step 2: Enable the HTTP server
Step 3: Allow HTTP access from your PC's network
Step 4: Create a username and password for ASDM access

Step 1: Connect to the ASA and configure the management interface

We need to turn on the http service on the firewall, but you will need to assign an interface to access the http service from, usually this is the management port as this is designed for management of the firewall - not for passing/routing traffic.

The management port, on the front of the firewall sits here:

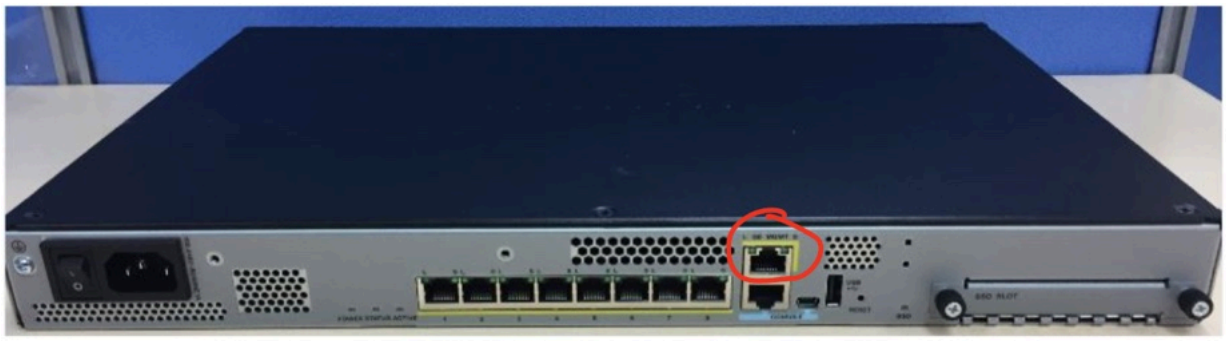


Figure 10 - Management Port

You can connect that to your PC using an ethernet cable. We will then need to know the IP addresses signed to your ethernet port on the PC's ethernet port we completed earlier.

We must now assign an IP address to access the http server. You can assign multiple IP's here, but we will only need one for now.

You will need to turn on and configure the management port and assign an IP address, on the same IP range as the management laptop.We can also give the port a name for ease of access. We will do this by:

```
ciscoasa>en
ciscoasa#conf
ciscoasa(config)#interface management0/0
ciscoasa(conif-if)#name if man
```

ciscoasa(conif-if)#no shutdown
ciscoasa(conif-if)#ip address 192.168.10.1 255.255.255.0

To make configurations as we just did, we entered sub-configurations mode, which essentially means we made configurations to the port. 'Interface' is what the firewalls call its ethernet port.

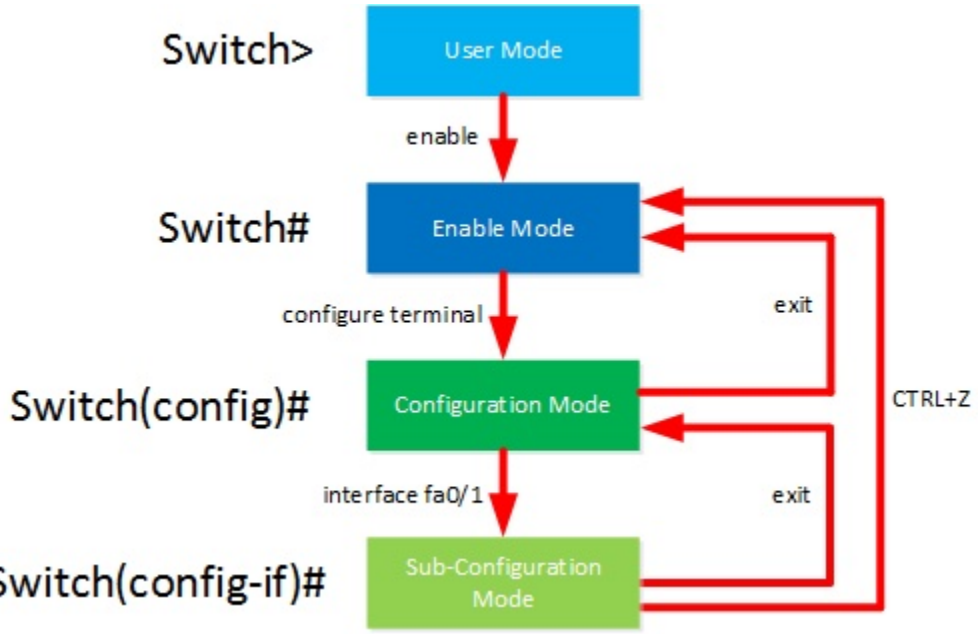


Figure 11 - Configuration

The configurations we just made were:

interface management0/0 - puts us into sub configuration mode for the management port

nameif man - we can now just type 'int man' if we want to enter sub config mode for the management port. I.e. 'int man' means **interface management0/0**

no shutdown- ports are down when out of the box, we must turn them like we did here.

IP address 192.168.10.1 255.255.255.0- we gave the interface(port) an IP address (192.168.10.0 and a subnet mask.(255.255.255.0)

What is a subnet mask? Simply, it defines how big the network is.

It also tells the firewall how to read the IP address-

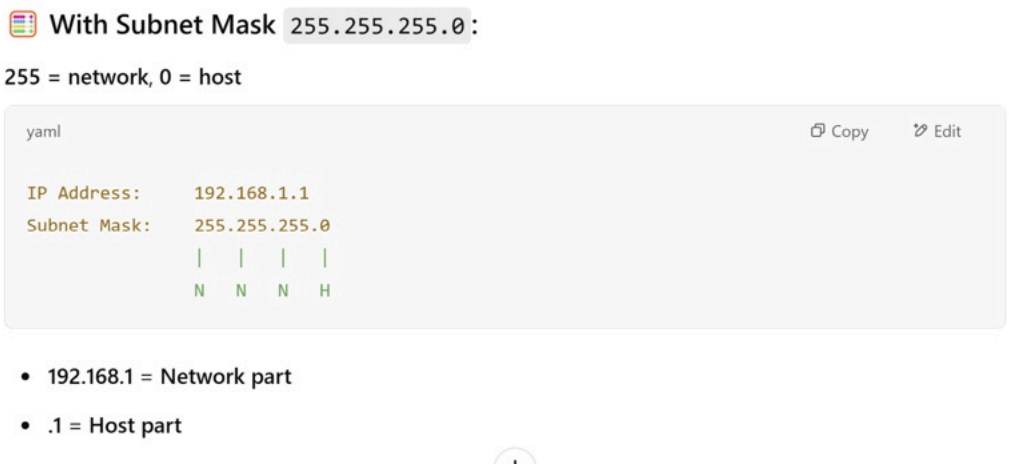


Figure 12 - Subnet Mask

Step 2: Turn on http server:

Now with the management port configured, the ASDM is a built-in http service which is accessed through the web browser. We will first have to turn on the http server. We can do this by doing the following:

ciscoasa>en
ciscoasa#conf t
ciscoasa(config)#http server enable

Step 3: Allow HTTP access from your PC's network:

We must now allow devices of a certain IP to access the http server, as this is blocked off. We do that by identifying the IP of the management pc given. They need to tie up on the same network.- management pc IP 192.168.10.10:

ciscoasa(config)#http 192.168.1.0 255.255.255.0 man

This code will allow PC's in the 192.168.230.1.`0` network, which are plugged into the management interface, only to connect to the ASDM.

Step 4: Create a username and password for ASDM access

To access the ASDM you will need to set up username and password:

ciscoasa>en
ciscoasa#conf t
ciscoasa(config)#username admin password admin123 privilege 15

What this means is:

The username is admin password is admin123 and you have maximum privileges
You can now access the ASDM by going to your browser and typing:
https://192.168.10.1

We have now successfully accessed the ASDM web GUI. This will allow us to download the ASDM app - no wifi needed, all off the firewall. The following page should load.

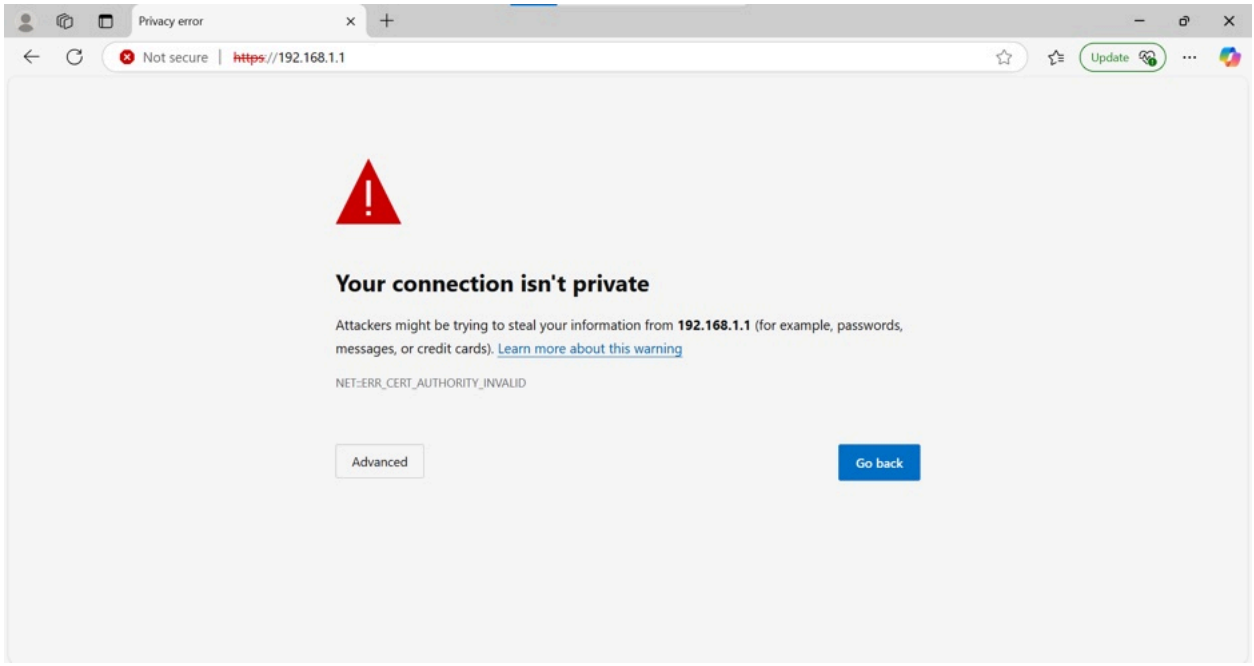


Figure 13 - Connection Privacy Warning Page

Select advanced. You will be asked to download. Once downloaded you can then run the application.

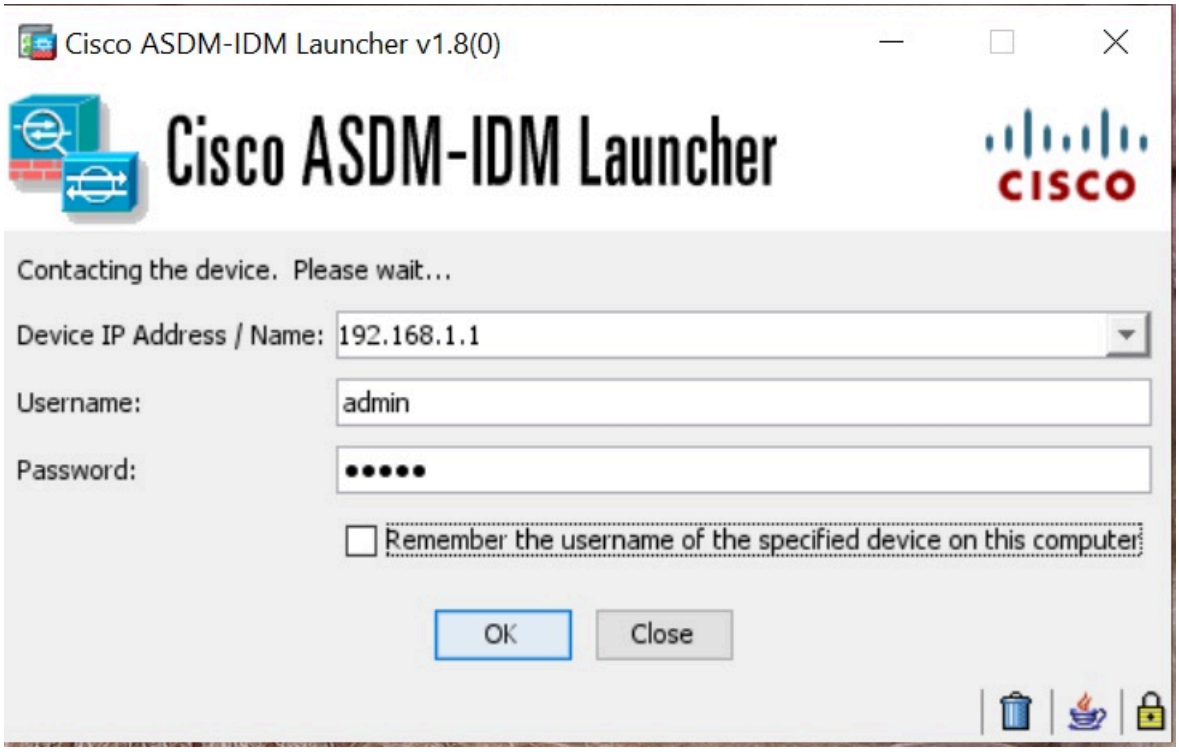


Figure 14 - Cisco ASDM - IDM Launcher

7. We will now set up the basic configuration which will allow activity ping through the firewall.

7.1 What is Ping?

Ping *is a basic* ***network test tool*** *that checks if another device is* ***reachable*** *on a network.*

We will do this by:

Step 1: Creating a bridge group

Step 2: Assigning interfaces to that bridge group

Step 3:Create rules to allow access through

7.2 What is a bridge group and how does it work?

The bridge group acts as a filter, inspecting data which flows through the firewall. Firewalls block all data first, you must configure the firewall first to pass data. Bridge-groups inspect and transfer data between two or more nodes on the same IP subnet. You can define rules which will then allow or deny data through the bridge-group.

Step 1: Creating a bridge group

ciscoasa>en
ciscoasa#config t
ciscoasa(config)#interface BVI1

You have created the interface for the bridge-group. Now you must assign an IP address to it.

ciscoasa(cofig-if)#ip address 192.168.230.111 255.255.255.0

We have now created a bridge-group.

Step 2: Assigning interfaces to that bridge group

We will now attach two ports to the bridge group. We will configure the two interfaces and turn them on. We will not need to give them IP's as they will use the IP of the bridge group.

The configurations will be:

ciscoasa(config)#interface GigabitEthernet1/1
ciscoasa(config-if)#nameif 4TH
ciscoasa(config-if)#bridge-group 1
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#noshutdown

Here we entered the sub configuration mode for the first interface. We then gave it a name as according to the 'Cisco configuration guide', interfaces will not activate without a name. We then attached it to the BVI1 and made sure the port is not in shutdown mode. We must do this to the second interface:

ciscoasa(config)#interface GigabitEthernet1/2
ciscoasa(config-if)#nameif BMS
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#bridge-group 1
ciscoasa(config-if)#no shutdown

Step 3:**Create rules to allow access through**

Since the firewall is set to deny all data to flow. We can use the ASDM to permit all data. This will allow us to test the bridge group, we will redesign the rules later but for testing purposes we will keep it open.

Let's use the ASDM for simplicity reasons. Let's first go to the homepage.

Click the Configuration tab', as shown in Figure 15 below. Towards the bottom of the screen, the 'Firewall tab' (seen in Figure 15), we will then click 'Access Rules'.

We want to add a 'global' (meaning across all interfaces) rule to permit any data using service 'IP' which means 'all ports'. This means that all ports on any IP can be accessed through the firewall.

See ‘add; rule in the top left corner of Figure 15. Click into this and fill out the pop up tab as the following:

Action: Permit
Source: Any
Destination: Any
Service: IP (ip)
Description (optional): Allow all IP traffic

Now click **apply.**

It should now look like the following:

any any destination service : **ip**

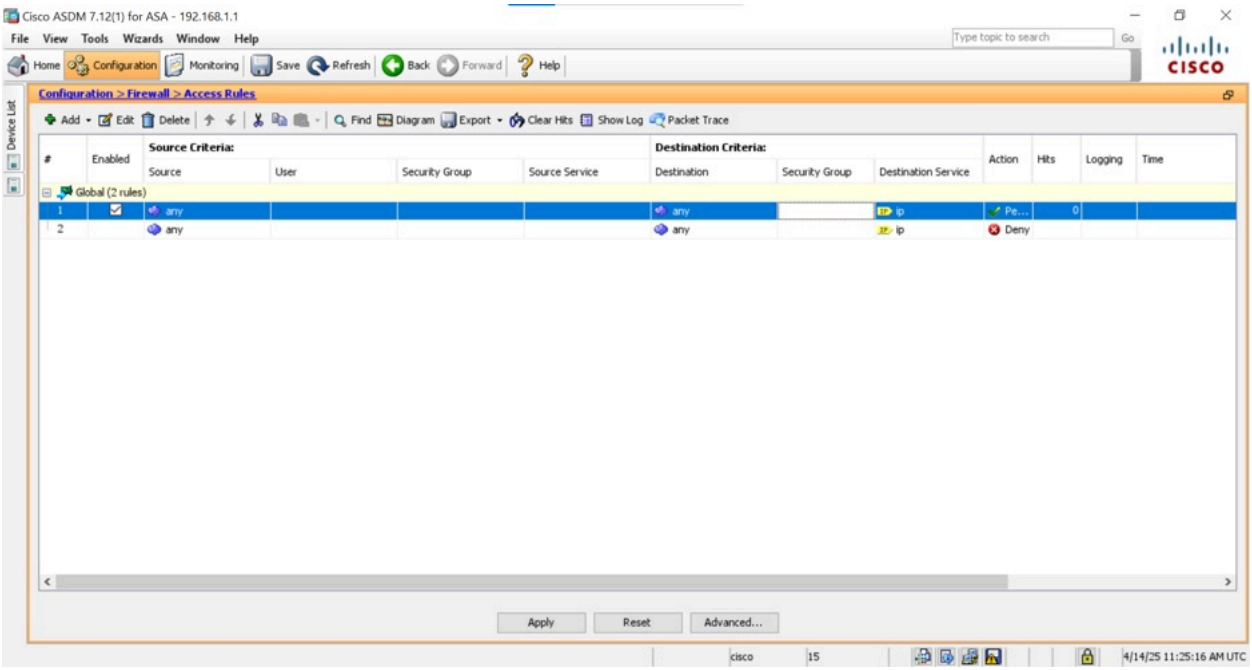


Figure 15 - Configuration tab

7.3 Ping through firewall

Testing the communications by ‘pinging’ through the firewall.

Step 1: Set up two Cisco switches on VLAN 800 and test ping between the switches.
Step2: Connect them to the bridge group interfaces on the firewall.
Step3: Test ping from switch to switch through firewall.

Step 1: Set up two Cisco switches on VLAN 800 and test ping between the switches.

Lets power on the two switches and connect our serial adapter (USB to USB mini cable) from the firewall to the first switch. We must connect and use ‘putty’ for this. This needs the same setup as before with the firewall.

First we will wipe the switch.

Enable
write erase
reload

The switch will request to confirm reload and you'll say yes. Now with the switch wiped and no other configurations on it (I had to do this due to taking old reusable switches from our stores but it also wipes older configurations used in testing).

Now we will set up configure a VLAN 800 on the switch as this is what the BMS communicates on.

Enable
Conf t
VLAN 800

name VLAN800
exit

We will then assign an ip address to VLAN 800.

interface VLAN 800
ip address 192.168.230.254 255.255.255.0
no shutdown

exit

Now we must assign VLAN 800 to an interface/port.

interface fastethernet 0/1
switchport mode access
switchport access VLAN 800
exit

Step2: Connect them to the bridge group interfaces on the firewall

We should now test the switch. We can do this by connecting the firewall to the very first port on both switches - as those are the ones configured with an ethernet cable. We should see the green lights on the physical switches.

Now from the switch while we are plugged in, using cli (putty) we now can ping the bridge group-192.168.230.111

It should look like this:

```
EIRRCMF4THSW08#ping 192.168.230.111
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.230.111, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

We must now repeat **Step 1 and Step 2** again but on the second Cisco switch. Plug into the second port in the firewall and assign it a different IPs, as this could create an **IP clash.** (use 192.166.230.10)

Step 3: Test ping from switch to switch through firewall.

You should now be able to ping through from the first switch to the second switch.

If you can't ping the firewall, try unplugging both switches from the firewall and plugging into each switch directly. If you can't successfully ping each switch from the firewall then let's look at the configurations of both switches. Run this code to see the configurations.

Enable
conf t
show running-config

This will print the running config and you can check to see if your config looks like this below:

```
interface Vlan500
 ip address 192.168.50.242 255.255.255.0
!
interface Vlan800
 ip address 192.168.230.242 255.255.255.0
!
```

```
interface GigabitEthernet1/0/47
 switchport access vlan 500
 switchport mode access
!
interface GigabitEthernet1/0/48
 switchport access vlan 800
 switchport mode access
```

Now, you need to check if you can ping the firewall. If not, ensure your bridgegroup is set up correctly. You can use the same code to check the running config of the firewall, with interfaces one and two assigned to the bridge-group one. Also ensure the IP address of bridge-group one is correct. They should look like this:

```
EIRRCMFBMSFIREWALL01# show running-config
: Saved

:
: Serial Number: JAD25492HLA
: Hardware:   ASA5516, 8192 MB RAM, CPU Atom C2000 series 2
:
ASA Version 9.12(1)2
!
firewall transparent
hostname EIRRCMFBMSFIREWALL01
enable password ***** pbkdf2
names
no mac-address auto

!
interface GigabitEthernet1/1
 bridge-group 1
 nameif BMS
 security-level 0
!
interface GigabitEthernet1/2
 bridge-group 1
 nameif 4TH
 security-level 100
!
```

```
!
interface Management1/1
 management-only
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface BVI1
 ip address 192.168.230.111 255.255.255.0
!
boot system disk1:/asa9-12-1-2-lfbff-k8.SPA
```

If this is all correct, we now look at the rules. As you can ping the firewall, but not through it, this shows the rules aren't allowing data through the firewall.

Your rules should look like the below image, Figure 16, in the ASDM. If not, ensure you added the correct rule. The ‘any’ rule sits at the top of the rule sequence in the interface displayed below.

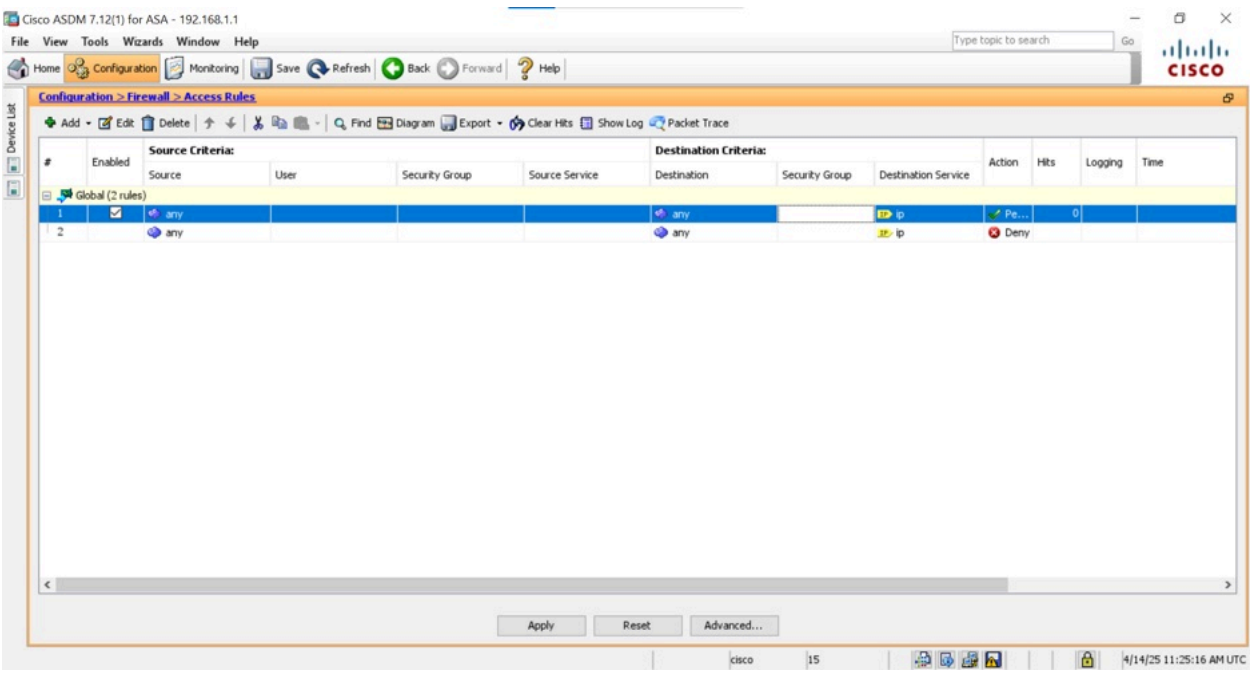


Figure 16 - Rules in ASDM

Next step:

Once I managed to get this working successfully and I was able to prove that this configuration was working as required, I then notified my project supervisor. While I was giving weekly updates to my supervisor, this was seen as a very successful milestone achievement in the whole project. My supervisor was delighted with this breakthrough and he responded to my notification to him with the following email:

"Fair play William….good progress.
Ok so, first anyway we need to be 100% sure that the IP list you have for BMS equipment on the plant is the full list – Do an IP scan on the live RCMF 4th LAN (using the "Advanced IP scanner" app – the OT lads in the OT porta have this on a secure OT laptop I should think, which you can use to connect to the 4th LAN – they can get you a free IP) and ensure from what the scan finds that all the BMS devices are captured in your list and BMS group (Check with Steve later to see if he can find out if all BMS equipment is active over there at this stage as there might be some turned off, not installed, or installed but not live/commissioned yet

Re "In the inside group(RCMF aspect server and 4thlan sw01 IPs have been added) And in the outside group I have added the list which Steve sent on a few weeks ago.."
The group viewed as the inside group would be the BMS devices on the BMS network. The outside group would be devices on the layers up from that then such as the DMZ C network devices where the Aspect server sits, so other way round perhaps.

***Re rules:** You will have a number of rules. Ok so you have the rule allowing all the required the BMS related group's traffic (src IPs group, dst IPs group) and ports (port groups) in/out through the firewall yes?*
And that (last rule) you have is a deny all rule to block everything else…. Possibly may need two of deny-denys for both directions depending on which side initiates comms? If you need that depends on the firewall model and capabilities (The firewall tech docs, YouTube or Google info for the model will tell you I should think, in the old days some firewalls needed two but I suspect modern ones like the one you have don't but need to be 100% sure

For the BMS switch mgmt from outside the BMS network (from 4th LAN tools server, usually IPMON01) you will need to leave SSH traffic through from the IPMON server IP to allow PUTTY SSH connections
For Cisco switch monitoring you will need to allow port(s) for Cisco Prime. Check with Andrew Leonard on that as he looks after Cisco Prime for us, he will have the 4th LAN Cisco prime VM IP of the Cisco Prime VM used to monitor 4th LAN switches (which will/should include the BMS switches)

For IP Mon BMS switches & devices up/down monitoring you will need to allow ping traffic from the RCMF IP mon server to all devices in the BMS devices group (Julie looks after IPMON if you have Qs on that)
When Stephen M is back from his sabbatical leave 😊 *he can check to see what other rules may be needed for monitoring, maintenance, access, other, etc….as I doubt I have captured everything (I am too far removed from the*

detail of a lot these systems these days due to old age & memory loss to know/remember such things :)

Re simulation and testing phases

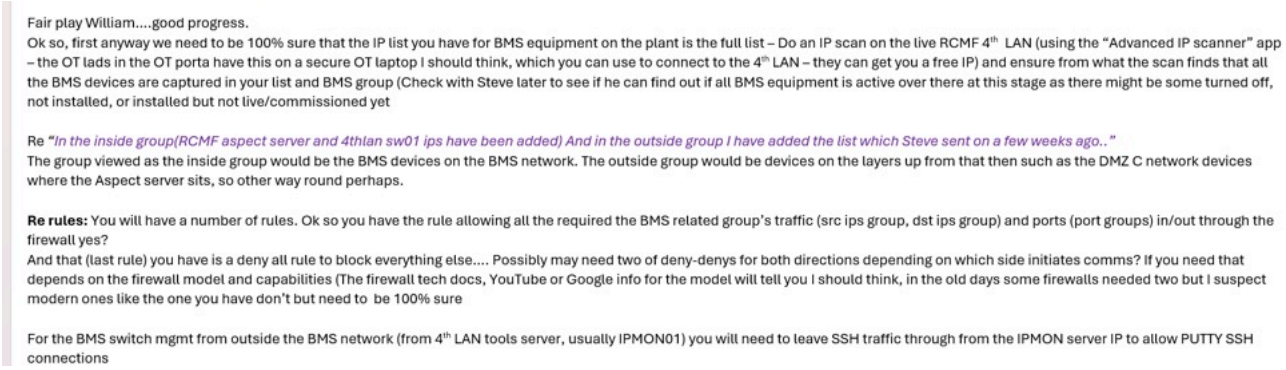
Apart from the software simulation of the system you were doing, ideally later you may be able to set up a cut down replica copy of RCMF 4th LAN (VLAN, subnets, etc…) above and below the firewall (with physical switches) and use laptops with IPs to act as devices on the various layers above and below your firewalls for testing (and documenting those tests for you project documentation) e.g. telnet to test the allowed ports from various layers from device to device, etc… . Maybe even use a second firewall with another physical switch attached (to act a DMZ C network) to simulate some of the functions our DMZ firewall does for BMS traffic and in that way bench test the comms all the way up and down from the DMZ C Aspect server to the BMS network controllers and devices behind your hosted system firewall.

When Stephen is back talk to him about this above to see if it (or parts of it) are doable without being over complex and/or taking too much time

Cheers

Paul"

Screenshots of the above correspondence are shown below, Figure 17 and Figure 18.



Fair play William....good progress.
Ok so, first anyway we need to be 100% sure that the IP list you have for BMS equipment on the plant is the full list – Do an IP scan on the live RCMF 4th LAN (using the "Advanced IP scanner" app – the OT lads in the OT porta have this on a secure OT laptop I should think, which you can use to connect to the 4th LAN – they can get you a free IP) and ensure from what the scan finds that all the BMS devices are captured in your list and BMS group (Check with Steve later to see if he can find out if all BMS equipment is active over there at this stage as there might be some turned off, not installed, or installed but not live/commissioned yet

Re *"In the inside group(RCMF aspect server and 4thlan sw01 ips have been added) And in the outside group I have added the list which Steve sent on a few weeks ago.."*
The group viewed as the inside group would be the BMS devices on the BMS network. The outside group would be devices on the layers up from that then such as the DMZ C network devices where the Aspect server sits, so other way round perhaps.

Re rules: You will have a number of rules. Ok so you have the rule allowing all the required the BMS related group's traffic (src ips group, dst ips group) and ports (port groups) in/out through the firewall yes?
And that (last rule) you have is a deny all rule to block everything else.... Possibly may need two of deny-denys for both directions depending on which side initiates comms? If you need that depends on the firewall model and capabilities (The firewall tech docs, YouTube or Google info for the model will tell you I should think, in the old days some firewalls needed two but I suspect modern ones like the one you have don't but need to be 100% sure

For the BMS switch mgmt from outside the BMS network (from 4th LAN tools server, usually IPMON01) you will need to leave SSH traffic through from the IPMON server IP to allow PUTTY SSH connections

Figure 17 - Email Correspondence Part 1

For Cisco switch monitoring you will need to allow port(s) for Cisco Prime. Check with Andrew Leonard on that as he looks after Cisco Prime for us, he will have the 4th LAN Cisco prime VM IP of the Cisco Prime VM used to monitor 4th LAN switches (which will/should include the BMS switches)

For IP Mon BMS switches & devices up/down monitoring you will need to allow ping traffic from the RCMF IP mon server to all devices in the BMS devices group (Julie looks after IPMON if you have Qs on that)
When Stephen M is back from his *sabbatical leave* 😊 he can check to see what other rules may be needed for monitoring, maintenance, access, other, etc....as I doubt I have captured everything (I am too far removed from the
detail of a lot these systems these days due to old age & memory loss to know/remember such things :)

Re simulation and testing phases
Apart from the software simulation of the system you were doing, ideally later you may be able to set up a cut down replica copy of RCMF 4th LAN (VLAN, subnets, etc...) above and below the firewall (with physical switches) and use laptops with IPs to act as devices on the various layers above and below your firewalls for testing (and documenting those tests for you project documentation) e.g. telnet to test the allowed ports from various layers from device to device, etc... . Maybe even use a second firewall with another physical switch attached (to act a DMZ C network) to simulate some of the functions our DMZ firewall does for BMS traffic and in that way bench test the comms all the way up and down from the DMZ C Aspect server to the BMS network controllers and devices behind your hosted system firewall.
When Stephen is back talk to him about this above to see if it (or parts of it) are doable without being over complex and/or taking too much time

Cheers
Paul

Figure 18 - Email Correspondence Part 2

Following receipt of the above email, I inserted the instructions into 'CoPilot', which is the AI tool provided in our work environment email application. I then asked for a plan to implement the proposal from my supervisor. CoPilot proposed a detailed task list.

8.To-Do List

From the email above, CoPilot proposed the following tasks which I have described more clearly below.

8.1 Verify IP List

- Perform an IP scan on the live RCMF 4th LAN using the 'Advanced IP Scanner' app.

- Coordinate with the OT team to access a secure OT laptop with the scanner tool.

- Compare the scanned results with the current BMS IP list to ensure all BMS devices are captured.

- Consult Steve (one of the more experienced infrastructure engineers) to verify if all BMS equipment is active, turned off, not installed, or not yet commissioned.

8.2 Update Inside and Outside Groups

- Ensure correct group assignments for Inside and Outside groups.
- Inside Group: Assign BMS devices on the BMS network.
- Outside Group: Assign DMZ C network devices (e.g., Aspect server).
- Reverse group assignments if current setup is incorrect.

8.3 Configure Firewall Rules

- Confirm existing rules for traffic allowance for BMS-related groups.
- Verify deny-all rule(s) to block everything else.
- Check firewall documentation or resources to confirm whether one deny-all rule or two are needed.

8.4 Enable Access for Management and Monitoring

- Allow SSH traffic from the IPMON server (4th LAN tools server, IPMON01) to BMS switches for PUTTY SSH connections.

- Allow necessary ports for Cisco Prime traffic.

- Consult Andrew Leonard (another experienced Infrastructure Engineer) for Cisco Prime VM IP and required ports.Enable IPMON monitoring: Allow ping traffic from the RCMF IPMON server to all devices in the BMS group.

- Coordinate with Julie for questions on IPMON monitoring.

8.5 Simulation and Testing

- Set up a replica of the RCMF 4th LAN (VLAN, subnets, etc.) for testing.

- Include physical switches and laptops with IPs to simulate devices on different layers.

- Use telnet to test allowed ports from various layers and document results.

- Explore feasibility of using a second firewall and physical switch for DMZ C network simulation.

- Test communications between DMZ C Aspect server and BMS devices behind the firewall.

- Discuss simulation and testing ideas with Stephen M upon his return.

8.6 Documentation

- Document all test setups and results for project documentation.
- Highlight dependencies on Stephen M's return to identify missing rules and configurations.

I completed the above tasks and they are now fully described below.

9. Scan network

Use 'Advanced IP Scanner' to scan the 4th LAN network and identify the BMS objects on the network.

Advanced IP Scanner is a tool which we use to scan the network. This can be used to see if any devices pop up or down onto the network. The process I follow to use this tool begins with me using my Pfizer automation account which has access to the Delta V Emerson 'Pro Plus Server' which sits on the 4th LAN. This is a server which is on the production system, used for maintenance, infrastructure management and more in which my team does not deal with.

Simply, I would remote from my Pfizer laptop onto this server, and start the Advanced IP scanner on it. This would look like the following (image taken from web).

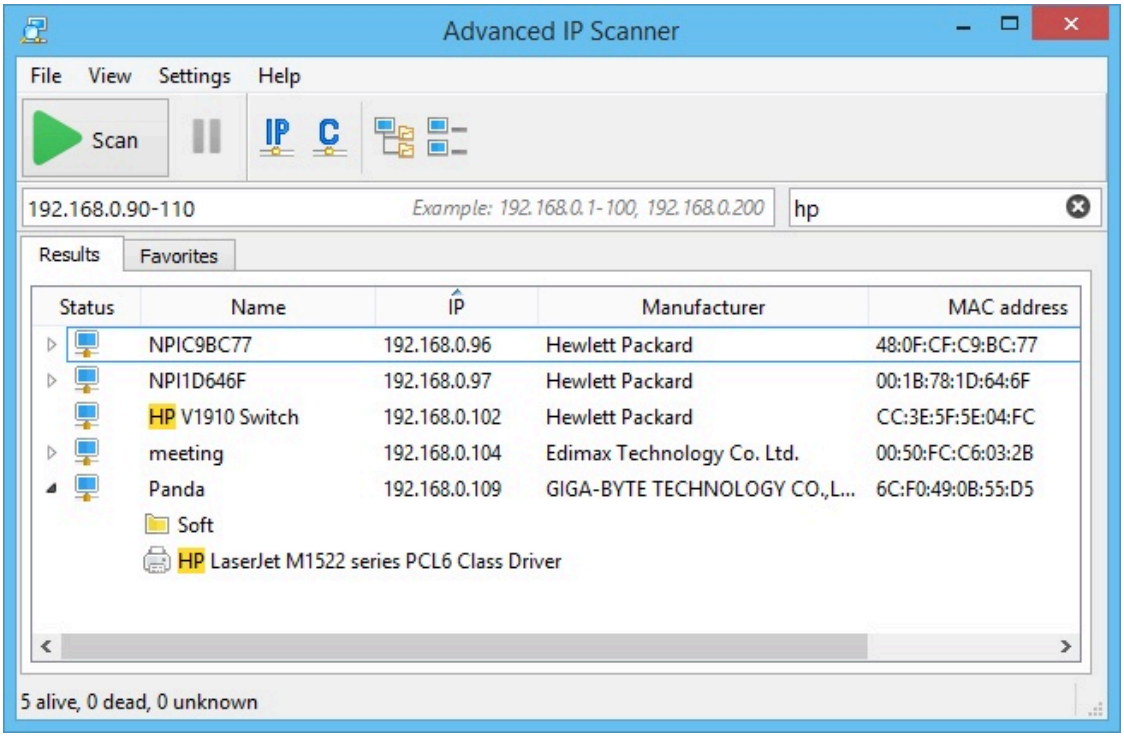


Figure 19 - Advanced IP Scanner (rbytes.net, 2025)

Once scanned, I would then see all the devices. I cannot display this as for security reasons, I cannot screenshot that server, but it would show the device name and the IP. The BMS shares the same IP subnet as the 4th LAN. So after creating a list of IP's, I contacted Sygma asking for their list of network objects and what ports are used. I then double checked my 'Live List', and compared it to Sygma's list to ensure no object was missing. The list I received from Sygma was the following:

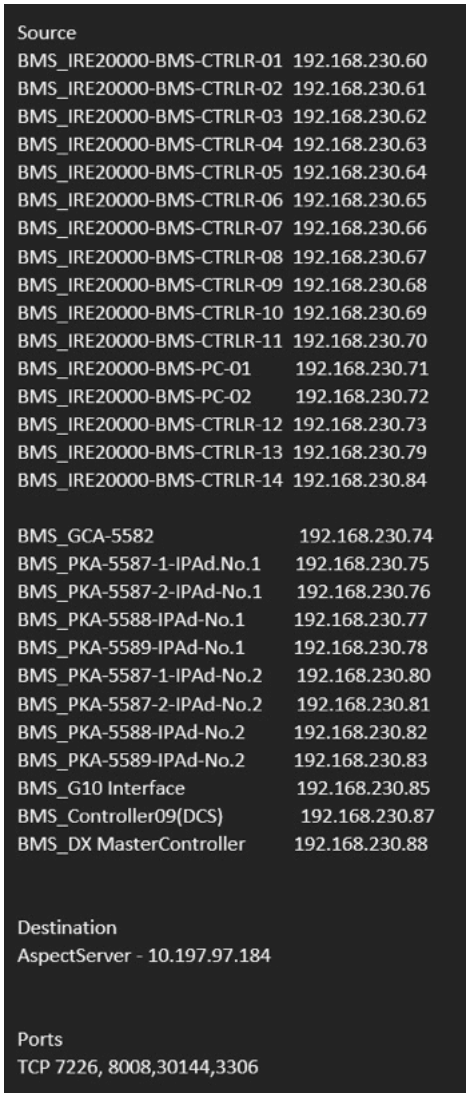


Figure 20 - Sygma Object List

In the next step, I then emailed both a colleague on the infrastructure team, and a colleague at the Sygma Automation company, to ensure across both teams that there were no upcoming future plans to add any more BMS objects. Both verified that there were no pending projects in the next year.

10. Create 2 network object groups one for BMS and another for 4th LAN and aspect server.

Network Object Group (Cisco ASA):

A network object group is a named collection of IP addresses, subnets, or host addresses that are grouped together to simplify and centralize firewall configurations. It allows administrators to reference multiple network objects with a single group name when creating access control lists (ACLs), NAT rules, or other security policies.

*(**Cisco Systems.** (n.d.) CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.6 – Access Objects.)*

The purpose of a Network Object group is to enable us to group the full list of IP's we want to refer to, by a single group name, when applying rules within the CISCO Firewall. This is much more efficient than having to directly address each object individually.

For our project, I created two groups:

One group:

INSIDE (later called BMS)

- The list of BMS objects (controllers, BMS PC's, HVAC device units including sensor interfaces)
- 8 BMS switches which were scattered around the plant.

OUTSIDE (later called 4TH LAN)

- This contained firstly one switch but soon changed to two 4th LAN switches.
- The aspect server - this is a server which is connected to the internet and releases security rule updates on an automated basis to the site's Cisco network equipment. One of the first tasks it completes is to scan the files currently installed and then it allows the network equipment devices to receive the update.
- DMZ firewall- This firewall will do the routing for all devices on 4th LAN or similar networks to the aspect server.

10.1 Creating the group on the ASDM

- **Select configurations- Firewall**
- **Than select Objects than selecting add network objects**
- **Create all your objects like so**
- **Select add a network object group**
- **Add your objects to the group**

- **Select configurations- Firewall**

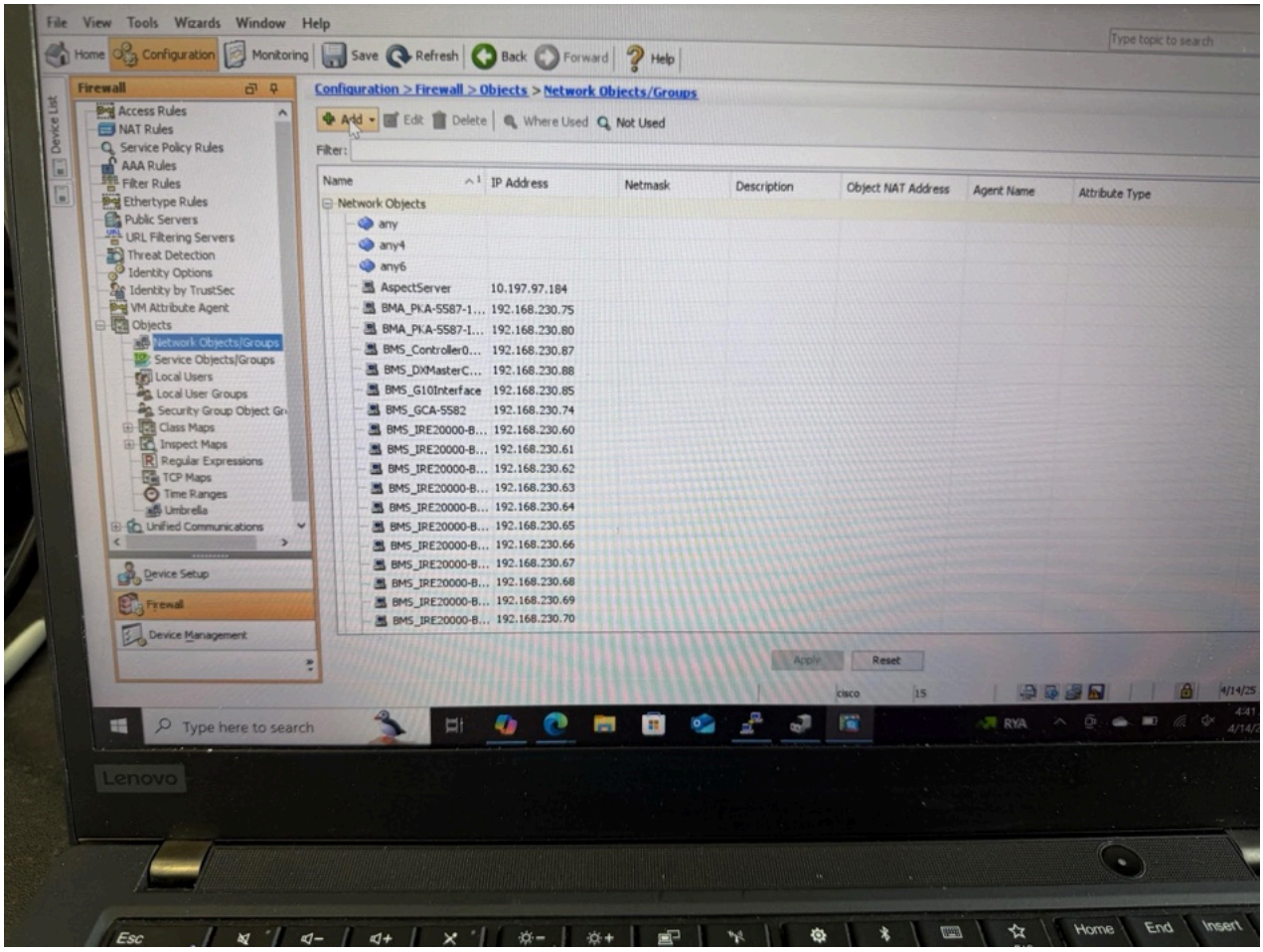


Figure 21

- **Than select Objects than selecting add network objects**
  Create all your objects like so:

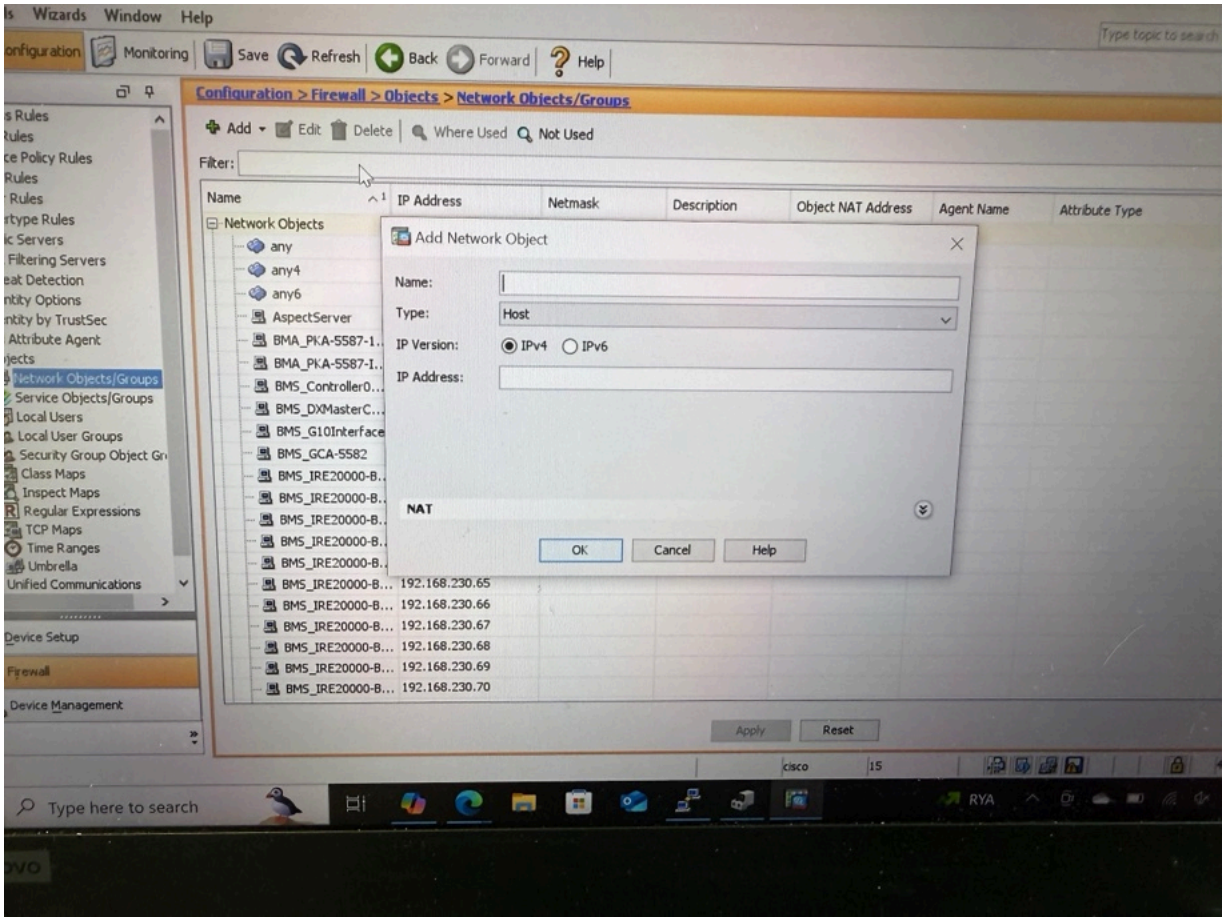


Figure 22

- **Add your objects to the group**

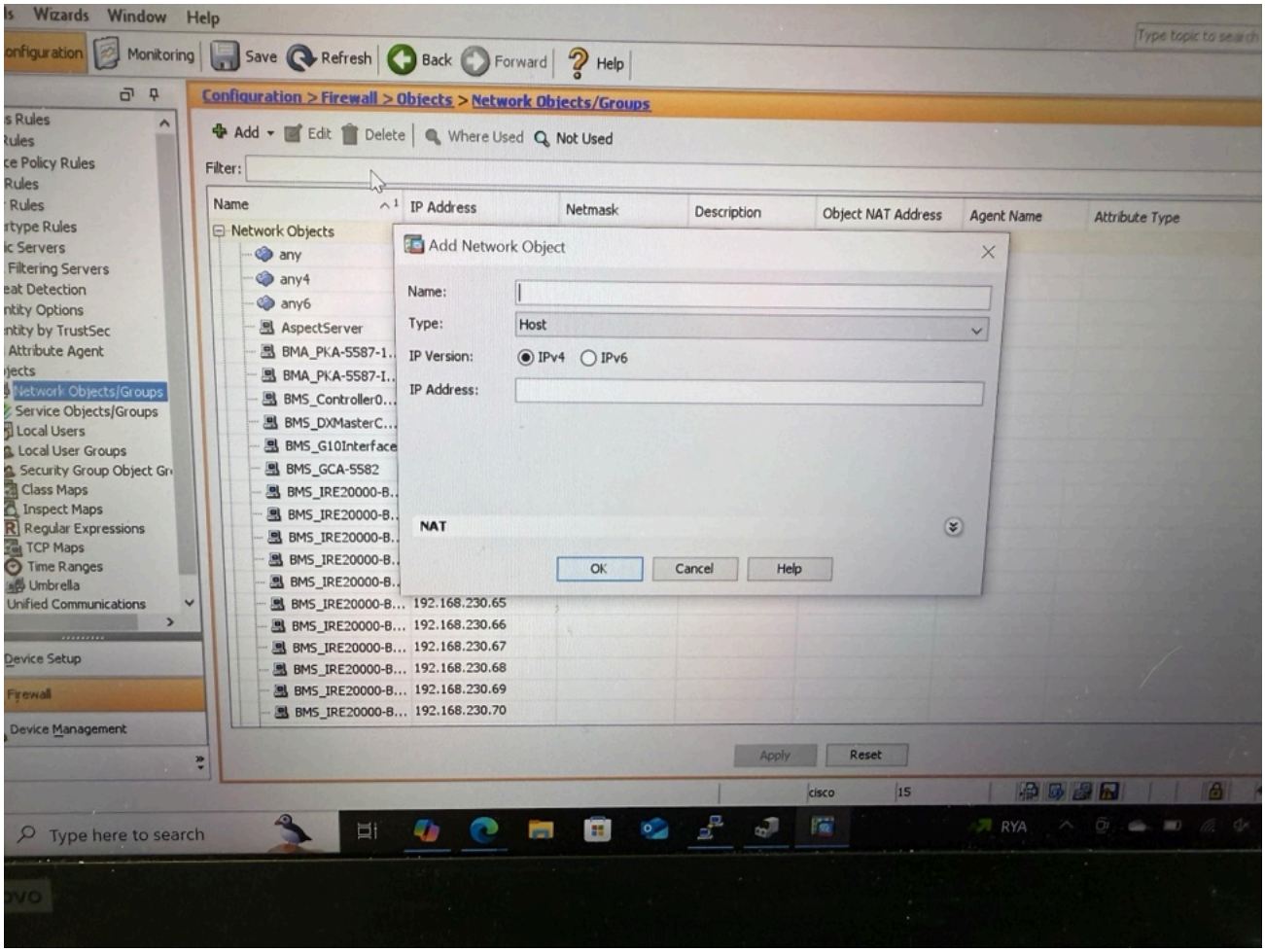


Figure 23

- **Select add a network object group**

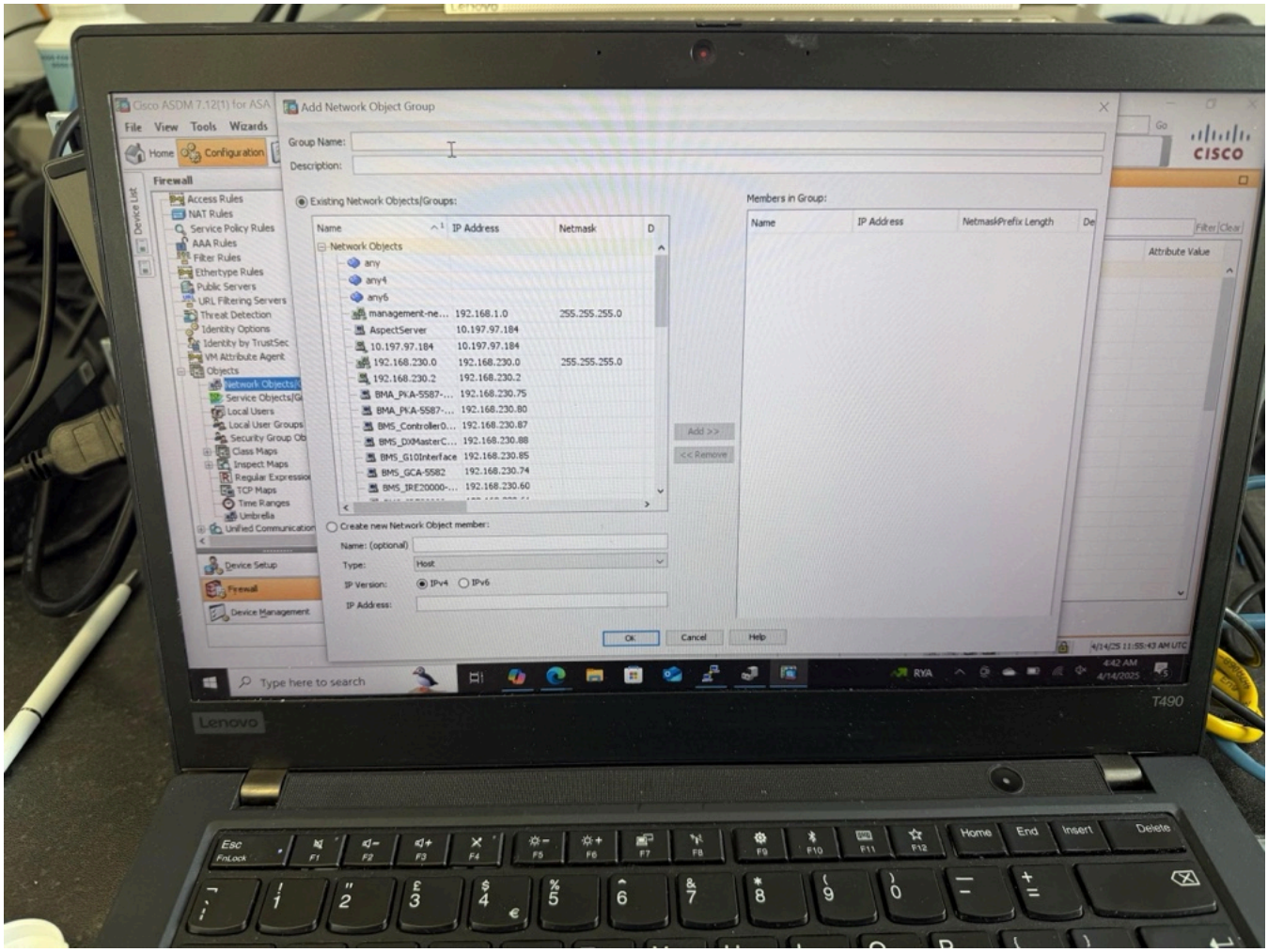


Figure 24

- **Add your objects to the group**

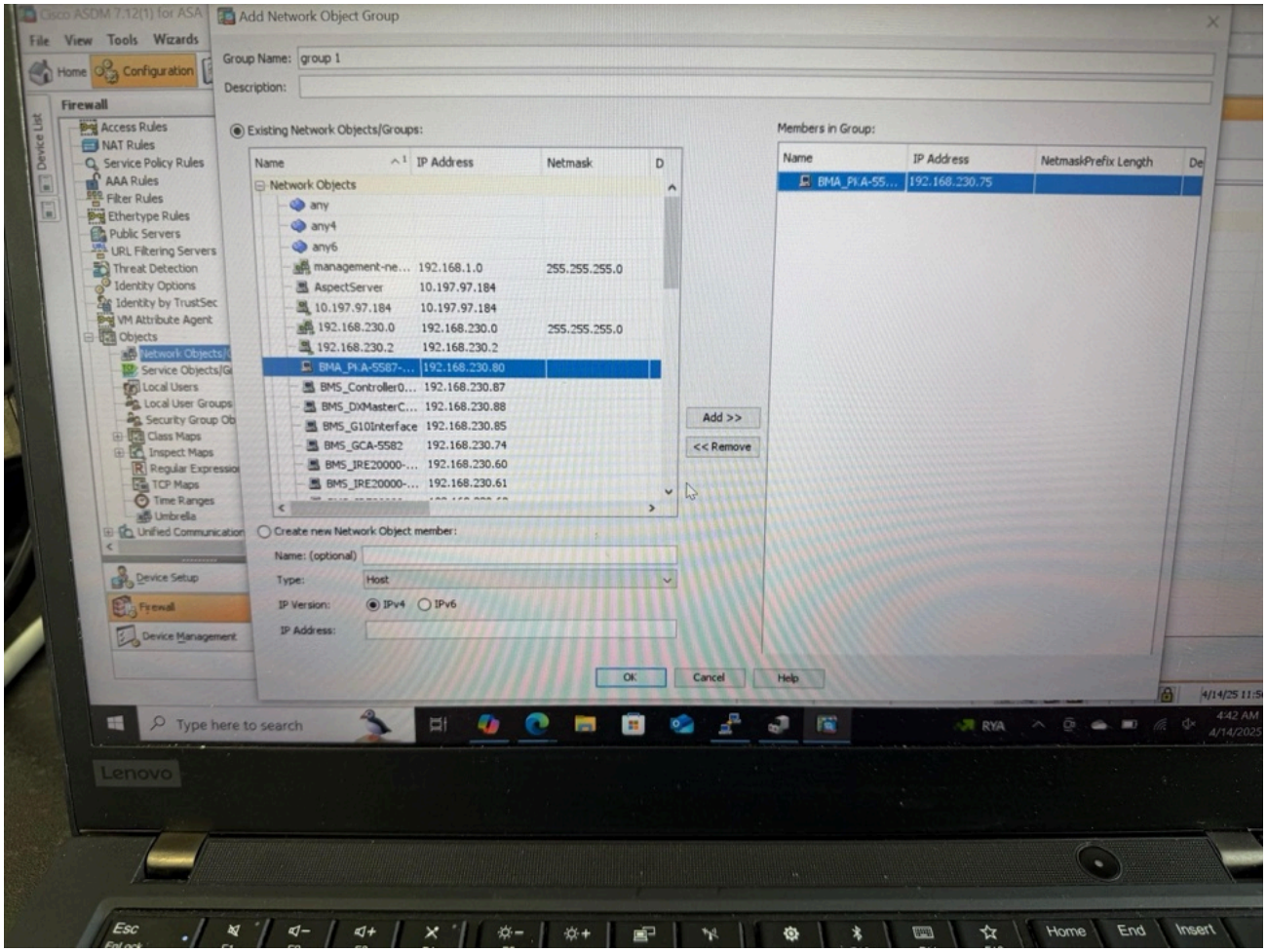


Figure 25

(Cisco Systems. (n.d.). General ASA Configuration Guide (v9.12))

11. Creating firewall rules

Before I could make any rules in the firewall, I first had to understand how the network communicates.

Basically, an IP address labels the device, but each time a device communicates, it uses a port - depending on what the device is trying to do. For example:

- Google uses port 443-secure browning pages use 443
- But when you send an email you login on to gmail using 443- then you send the email using 587 on modern systems.

Most common ports have tags (often multiple ports share the same tag):

587 has a tag called SMTP= simple mail Transfer Protocol
443 has a tag called HTTP= Hypertext Transfer Protocol

Not all ports have these tags.

So understanding that the BMS itself uses these 4 ports:

7226
8008
30144
2206

I can then create rules which allow my groups to communicate on these ports alone.

What does this mean?

Knowing the IP address of the allowed devices, we also know what communication paths they actually communicate on, we can now use the firewall

to block all other paths and IP addresses, meaning if an allowed IP address is breached and malware coming through, the port used would be blocked.

Also no outside IP address will be able to communicate with the 4TH LAN.

(Cisco Systems. (n.d.). General ASA Configuration Guide (v9.12))

11.1 Create rules for firewalls only allowing IP's using the correct ports.

Using ASDM we have created two groups, 4TH LAN and another group called BMS.

We open ASDM, where we left off at the rules.

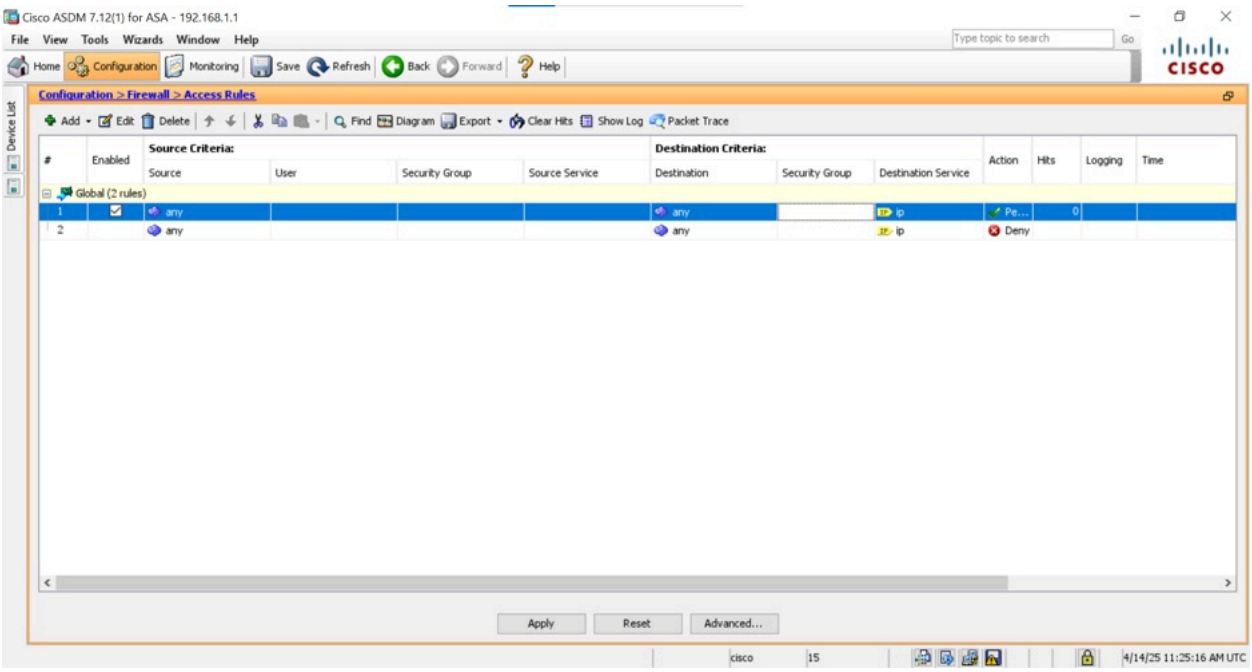


Figure 25 - ASDM

If we click on the rule we have set, and select ‘edit’ (this is a tab at the top left), we can edit the rule. Here we will select our groups we created from the ‘source’ and destination tabs (see Figure 26 below).

Now where service is (you can type in the first port: 7226). You will have to create a new rule for each port as during simulation. The ASA fails when multiple ports are opened in one rule.

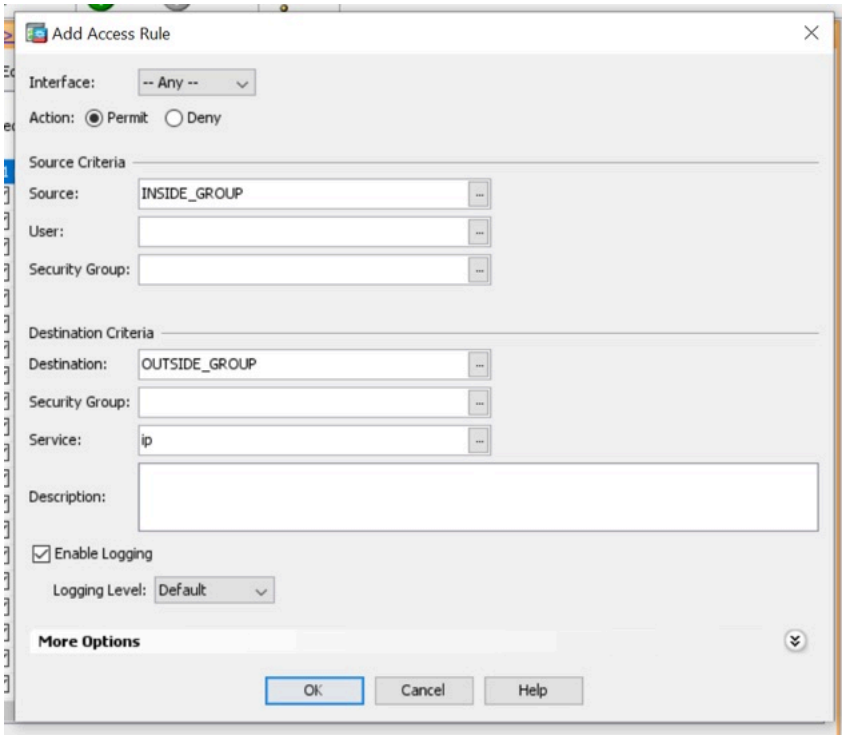


Figure 26 - Source and Destination Tabs

After, your rules should look like this:

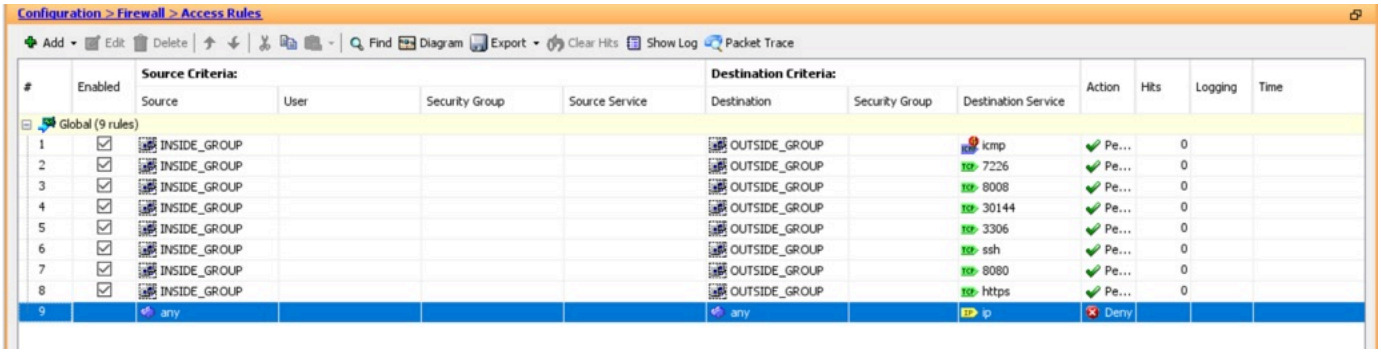


Figure 27 - Rules

The rules are not bidirectional by default, and there is no command which creates a bidirectional rule as this would be a security flaw, you must create the rules in the opposite direction. So instead of allowing 4th talk to BMS you now must allow BMS talk to 4th. Repeat for each port (swap around where source and destination were selected).

(Cisco Systems. (n.d.). General ASA Configuration Guide (v9.12))

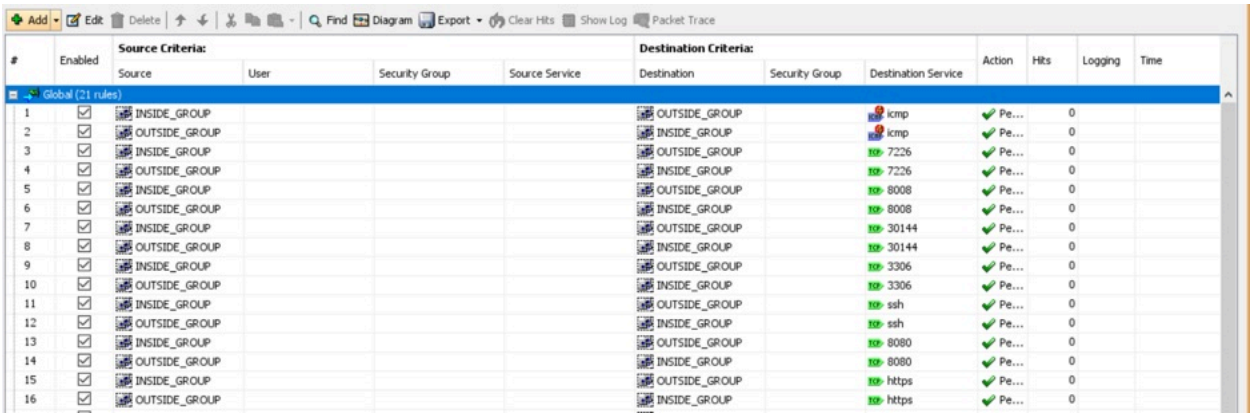


Figure 28 - Rules

11.2 Access Control Implicit Deny

All ACLs have an implicit deny statement at the end, so unless you explicitly permit traffic to pass, it will be denied. For example, if you want to allow all users to access a network through the ASA except for one or more particular addresses, then you need to deny those particular addresses and then permit all others.

Cisco Systems. (n.d.). ASA CLI Configuration Guide – Logging. Available at: CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.16

This means if a packet does not belong to a rule it is automatically blocked. My project supervisor found that on older firewalls, you needed to have 2 of these rules at the end - but that fault has since been corrected by Cisco. We will also allow the ICMP rule (ping).

What is done so far (briefly)?

- Bridge-group created and assigned an IP.
- Two interfaces on the firewall have been assigned to the Bridge-group.
- The IP's of the BMS has been gathered.
- The IP's of 4TH lan,DMZ Firewall and Aspect server have been gathered.
- The Ports used by bms network have been identified.
- Two groups have been created and IP's have been entered into them
- Rules were first created to allow the two groups to communicate
- Rules are then updated to allow the two groups to communicate on certain ports.

What is next?

- Allow IPMON server to communicate with BMS
- Allow Cisco Prime traffic
- Coordinate with andrew and julie for all IPMON questions

- Set up RCMFreplica and simulate traffic
- Simulate and Document test set ups
- Write test specifications and installation operation manual for Pfizer.
- Install firewall

12 What is IPMON and how is it used for BMS?

IPMON is a server in which it does regular sweeps of the network traffic and ensures that no device comes off the network. This could include switches which have multiple devices hanging off, or just a singular device.

The infrastructure team will then receive an email notification from the IPMON application of the exact device in which it has come offline. It uses the advanced IP scanner tool to sweep the network.

12.1 How to ensure the firewall will not block IPMON

Step 1: Discover correct IPs and ports used
Step 2: Add the IP addresses to the 4TH Lan group
Step 3: Open the ports used by IPMON

Step 1: Discover correct IPs and ports used:

Enquire the IPMON VLAN 800 IP address:

- Since there is IPMON primary and secondary there are **two IP addresses.**

192.168.230.54 -*IPMON01*
192.168.230.55 -IPMON02

Enquire what ports advanced IP scanner uses:

- I will also allow access through the firewall as for maintenance the Ipmon server is used to ssh through to the bms switches.

Allow http through the firewall:

Port 22 = port for 'ssh'.

Step 2:Add the IP addresses to the 4TH Lan group:

Create 2 new network objects using ASDM.

Edit the current network object groups and add the 2 new network objects to 4TH.

Step 3:Ensure the ports used by IPMON are open

Ipmon uses ports 22 and 8080, which are open.

13 Allow Cisco prime server to communicate through the firewall

I had to enquire from my infrastructure colleagues to identify the Cisco prime server IP address. My colleague had a map of all of the server IP addresses and he identified this for me as follows:

Cisco prime server IP:192.168.230.27

I needed to know what ports the Cisco prime will use and allow those ports open.

The 30 ports prime uses was:

13.1 Cisco Prime Infrastructure – Common Ports and Their Purpose:

1. **22 (SSH)** – Secure remote command-line access
2. **23 (Telnet)** – Unsecured remote access (legacy)
3. **25 (SMTP)** – Sends email alerts and notifications
4. **80 (HTTP)** – Basic web access (not secure)
5. **123 (NTP)** – Syncs time between devices
6. **161 (SNMP)** – Polling devices for status and data
7. **162 (SNMP Trap)** – Receives SNMP alerts from devices
8. **443 (HTTPS)** – Secure web access to the Prime GUI
9. **514 (Syslog)** – Receives log messages from network devices
10. **3306 (MySQL)** – Database communication
11. **8080 (HTTP Alternate)** – Web service communication between modules
12. **8443 (HTTPS Alternate)** – Secure internal web communication

13. **9002 (TCP)** – Service data exchange
14. **9009 (TCP)** – Job manager communication
15. **9101 (TCP)** – Indexing and search service
16. **9161 (TCP)** – Platform services
17. **9443 (TCP)** – Secure client-server communication
18. **9999 (TCP)** – Inventory manager service
19. **2195 (TCP)** – Apple Push Notification service
20. **27017 (MongoDB)** – Database service for certain modules
21. **50000+ (Dynamic Ports)** – Used for internal service communication
22. **69 (TFTP)** – Used to transfer configs/images to devices
23. **179 (BGP)** – Routing protocol (used with BGP-capable devices)
24. **44369 (TCP)** – Cisco secure service communication
25. **5246/5247 (CAPWAP)** – Wireless controller and access point communication
26. **8444 (HTTPS Alternate)** – Secure WLC access

27. **8005 (TCP)** – Tomcat server shutdown control

28. **8009 (TCP)** – Tomcat AJP connector

29. **16101 (TCP)** – Device polling and monitoring

30. **14150 (TCP)** – Data collection and analytics engine

13.2 Cisco prime RULE

I determined that based on the above, there are too many ports to handle in one rule. I opted to give Cisco prime a unique rule:

Cisco prime server can talk to the allowed IPs on the bms on any ports

Cisco Prime:

Figure 29 - Cisco Prime

This rule would be bidirectional. When the firewall is installed and in the real world environment I will then use the logs from the ASA firewall and see if it still uses all 30 of those ports or not. I will then update the rules depending on these results.

14 .Build replica simulation of RCMF

First plant of installation-Ringaskiddy Clinical Manufacturing Facility.

14 .1 Set Up the test environment for testing and simulation.

- **4Th LAN replica switch on top**

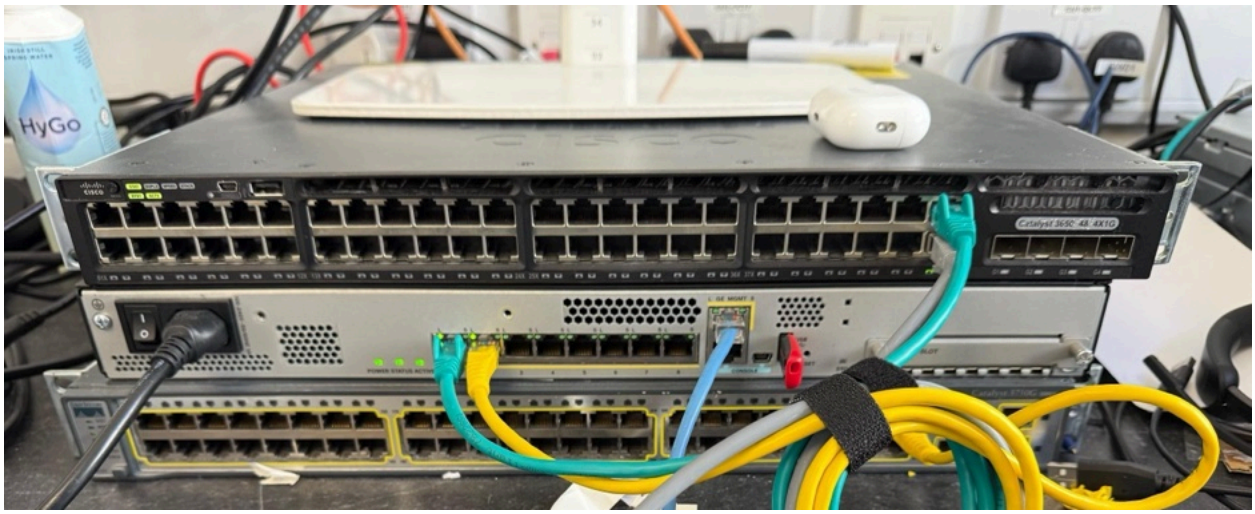


Figure 30 - Replica Simulation

- **Bms replica switch at bottom**
- **ASA firewall between**

These are the two real switches in the live production environment in which we will be using. I was fortunate enough to have access to a test environment where one exact same model and one similar model were installed. I was able to copy the running configuration from one switch to another to verify my configurations.

This provided me with a safe environment for testing. Without risking any real life systems, the test environment could be used to prove the configurations. This also helps identify any issues early on, and finally, it allows me to grow my knowledge on the BMS system network, as well as the individual switch configurations installed.

Step 1: Download configurations from live plant switches to usb

step 2: Get same/similar model switches

step 3: Upload the plant configurations to the old switches.

Step 4 :Set up VLAN 800 interfaces

Tools needed:

- Management laptop
- Serial cable needed
- Usb stick-empty as will possibly need to be formatted

Step 1: Download configurations from live plant switches to usb

- Format usb stick to FAT32

Open the file explorer and right click on the usb
click format and choose FAT32 and click quick format.

Eject safely

Plug USB stick into switch and serial cable into pc and cable.
Using device manager set up putty for the CLI onto 4TH LAN switch
ensure the switch can see the USB.

switch>show disk:1

The switch will spit out the following:
disk1: 524288000 bytes total (free space shown)

Now you will want to save the running config to the switch:

copy running-config disk1:/backup-config.txt

This code copies the running-config to disk 1(your usb) as a txt file called backup-config

Repeat this for the BMS Switch.

Step 2:Get same/similar model switches

Getting the same switches, this step was easy for me as Pfizer has a big stock of non used infrastructure gear.

Step 3: Upload the plant configurations to the old switches.

I was able to utilize a Spare CISCO 3650 4th LAN master switch, and a spare CISCO 3750 BMS master switch. In which I uploaded the configurations previously downloaded.

The code needed was:

Enable
conf t
wr erase
wr mem

This will have wiped any configurations, next we will upload our new configuration.

Enable
show disk 1:
copy usbflash0:backup-config.txt running-config

This will have copied the .txt file onto the running configuration.

Step 4: Set up VLAN 800 interfaces.

Using CLI we want to set up an interface on each switch using VLAN 800. The switches will already have VLAN 800 IP addresses so we will need to assign VLAN 800 to an interface.

interface fastethernet 0/1
switchport mode access
switchport access VLAN 800
exit

Repeat this on both switches.

The replica environment is now set up. Connect both switches to the firewalls bridge-group interfaces.

(Cisco Systems. (n.d.). ASA Command Modes and CLI Guide)

(Cisco Systems. (n.d.). Configure VLAN and Access Port Settings)

Next step:

15.Testing

15.1 Simulate and Document test set ups

The set up should now look like this:

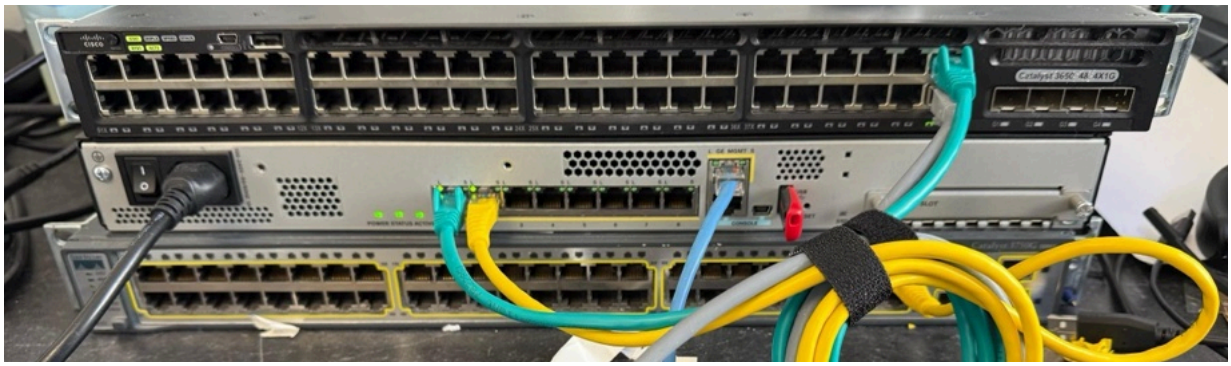


Figure 31 - Simulation Set Up

Equipment needed:

- 2 simulation pcs
- 2 Ethernet cables

Add the simulation IPs and set up a pc at each switch.

With the firewall segmenting the two networks, ensure we have one management pc still connected to the firewalls management port. Access the ASDM and edit the two network object groups. We want to add one simulation IP per group:

192.168.230.2-4th lan group
192.168.230.3-BMS Group.

On one pc give it the .2 IP and connect it to the 4th LAN switch. On the second simulator pc give it the .3 IP and connect it to the bms switch.

15.2 Successful ping

Open on both cmd and ping each other. It should look like the following:

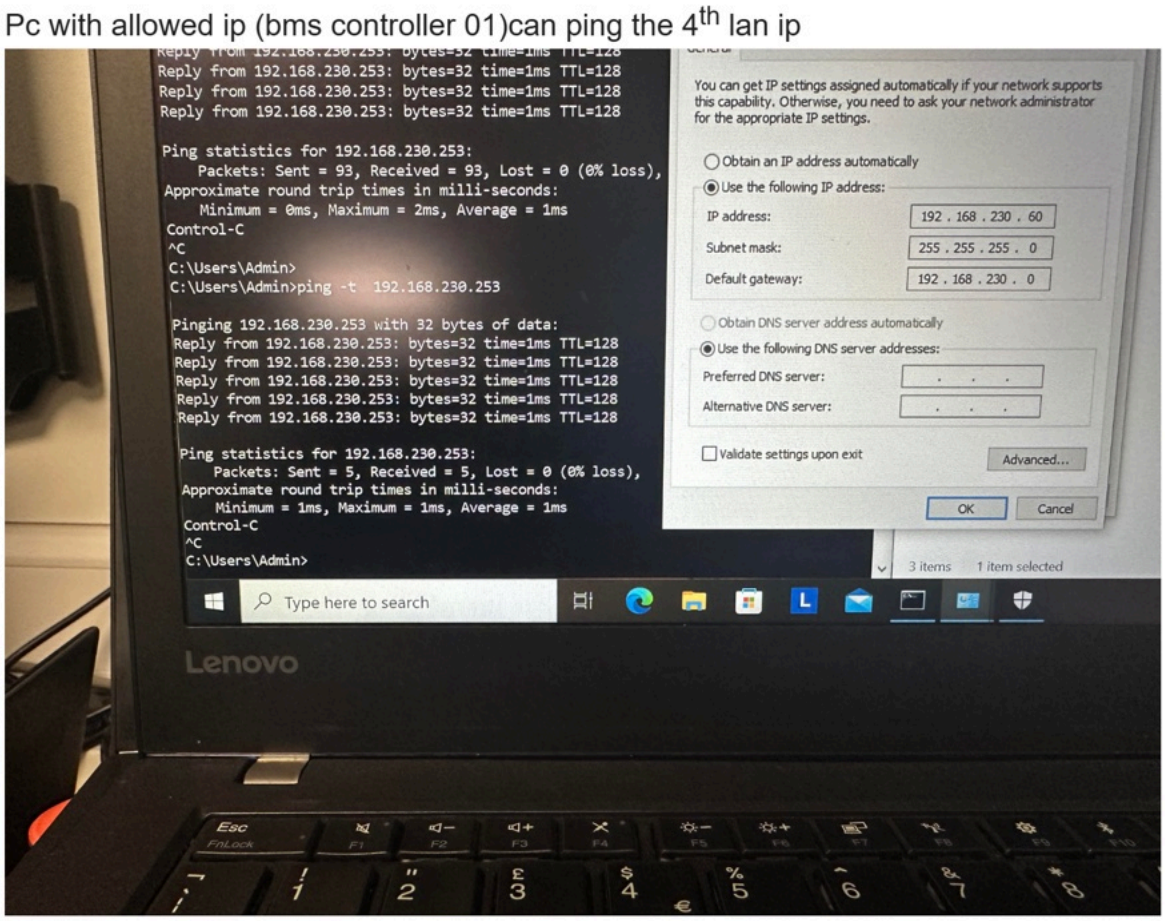


Figure 32 - Ping

4th Lan Ip can ping the bms controller ip

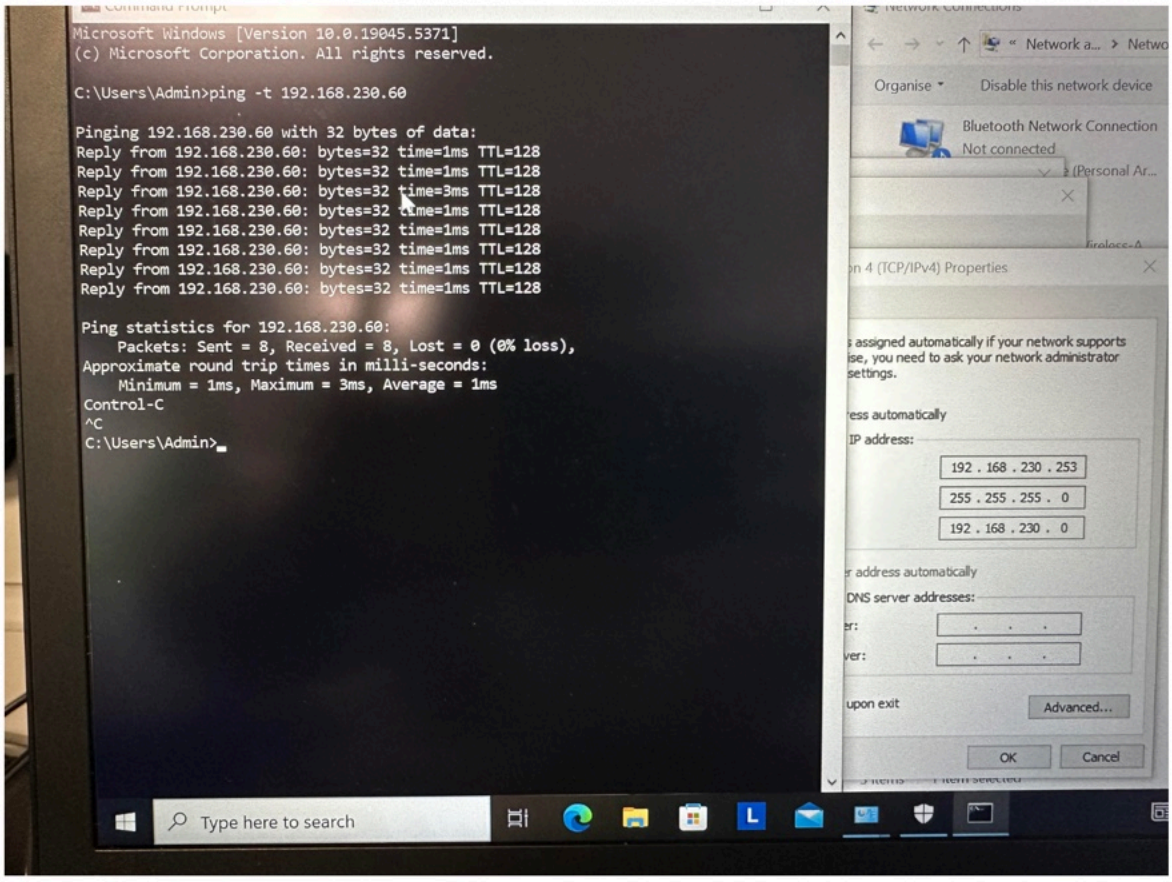


Figure 33 - Ping

Ping only uses ICMP, which is different to the ports we have opened. I had to prove that ports were open or closed, depending on the rules.

My project supervisor asked for me to use ‘Telnet’, but the firewall wouldn't allow it. See the correspondence below:

Figure 34 - Email Correspondance

Good stuff…. 👍
Other proofs/tests: You can also use telnet to check/test ports for open/blocked access (telnet used for troubleshooting port sometimes)
e.g. a test for an allowed src/dst IP but on a port that not explicitly listed in the rule/port-group as allowed – such a port should fail to connect on telnet to that IP

telnet <IP ADDRESS OF SERVER PC> <PORT>

(you may need to ensure telnet enabled on machine you are using to do such tests)

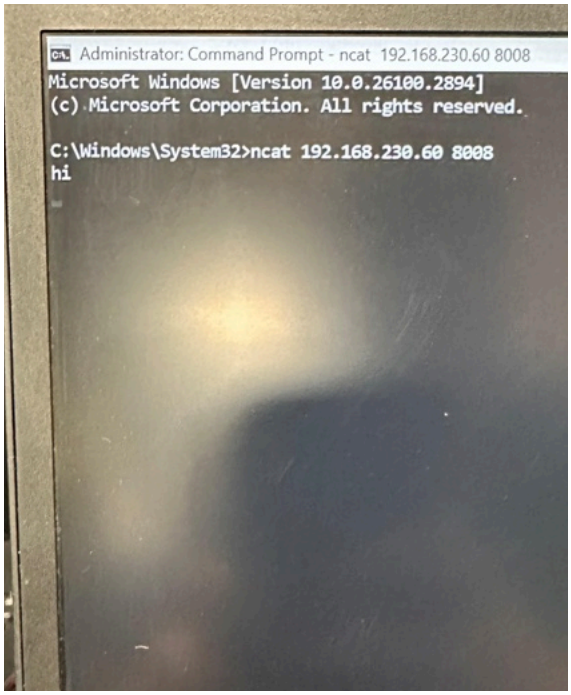
OR
from powershell with tnc command :

15.3 How I overcame this problem:

What is nmap and how did I use it?

Nmap-short for network mapper is a tool used to show the activity of a network, what ports are used and what devices are on. Due to the firewall, the scan nmap usually does is blocked due to it not being permitted.

We can test the firewalls ports individually using nmap and cmd together. By opening the port you create a communication channel in which you create a chat through, like the following:



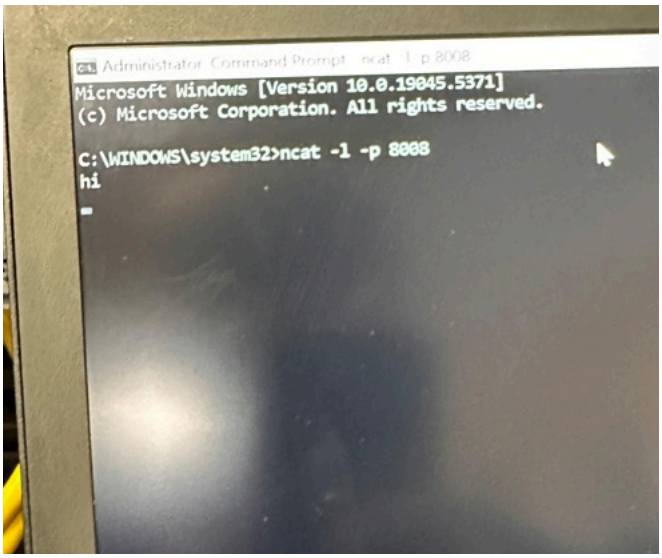


Figure 35 - NMap 'ncat' tool ***Figure 36 - NMap 'ncat' tool***

Above we can see the two different PCs on either side of the bridge group, communicating over Network mapper's tool, 'ncat', allowing you to open a communication port. This proves that port 8008 on the allowed IP address is open.

Test Scenario	Results
Check ICMP (Ping) For Allowed IP's Only	Success
Test Allowed Ports (TCP)	Success
Test Blocked Ports	Connection refused
Check ASA ACLs	Shows allowed rules
TCP Three Way Handshake	Success

Figure 37 - Test Results

(Nmap Project. (n.d.). Ncat Users' Guide)

(Nmap. (n.d.). Nmap Installation on Windows)

16. Loose ends tie up:

- Allow ASDM access from the 4TH LAN
- Create ASDM accounts for infrastructure team
- Enable logging

16.1 Allowing ASDM access from 4th LAN

By allowing devices on the 4th LAN- the firewall is manageable remotely. ASDM is secure, as username and password are needed to log in. Users will also be able to download logs to see if there's any traffic purposely being blocked, whether it should or shouldn't be.

How to allow ASDM access from the 4th LAN:

Step 1: Identify the correct interface

Step 2: Configure the interface to allow ASDM

Step 3: Test ASDM through 4th

Step 1:Identify the correct interface

Run command:Show running-config

Identify the 4TH interface by the name if. Should look like:

interface GigabitEthernet1/2

nameif 4T

security-level 100

bridge-group 1

no shutdown

Step 2:configure the interface to allow ASDM

http 192.168.1.0 255.255.255.0 4TH

This configuration allows the http server from the interface called 4TH.

Step 3:Test ASDM through 4th

To access the ASDM through the 4th LAN, we can use the simulator tool connected to the 4th LAN. We can now access the ASDM as usual:

Open web browser and enter the IP address below:

https://192.168.1.0

We can now access the ASDM through the 4TH LAN

16.2 Create logging accounts for ASDM

Everyone who makes configurations using the ASDM needs to have their own account. This keeps everyone accountable and if there is an issue there is traceability. Also, not every engineer needs access. This is done by:

configure terminal

username admin password admin123 privilege 15

admin= username given.

admin123= password

Privilege 15 = max admin rights.

16.3 Create logging

Using CLI enter the following code:

conf t

logging enable

logging monitor informational

- 'Logging enable' – generates logging information in the ASA firewall
- 'Logging monitor informational' - prints the logging information

17 Install firewall

Equipment needed:

- Firewall
- Management pc
- six ethernet cables
- Firewall power lead
- Label machine

4TH LAN - BMS hardware overview:

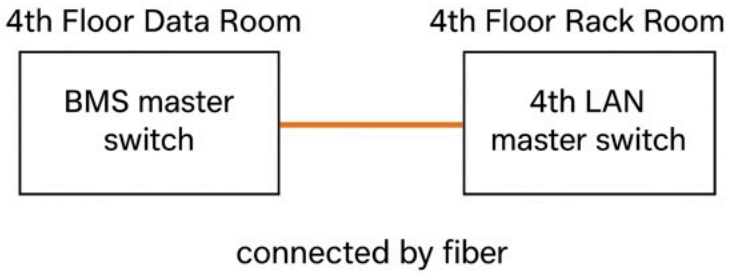


Figure 38 - BMS / 4th Lan Switch Diagram

As seen by the diagram above the two switches sit in different rooms in the plant. They are also connected through a fiber optic patch panel.

17.1 What is a patch panel?

Every data room + rack room (server rooms) are connected using patch panels, cables which in our case are usually both copper and ethernet cables. They are clearly labeled to show exactly where they are going.

In my case, the server rooms are only connected using fiber, but the firewall needs to sit in between the connection and does not have a fiber connection.

17.2 Two potential solutions:

- Use a fiber to ethernet converter (A box in which converts fiber to ethernet).
- Use another 4Th LAN switch in a different room with an ethernet connection available.

While **solution one** seems the easier route, with fiber cables you also need fiber SFP. A fibre SFP module is needed to plug into the network device and translate light to data for the switch/firewall. They are expensive and cause multiple points of failure when using media converters.

Due to my experience when working on the RCMF plant when it was being built, I have great knowledge of all network infrastructure devices and how they are interconnected. I proposed the second solution, which is inexpensive and more robust.

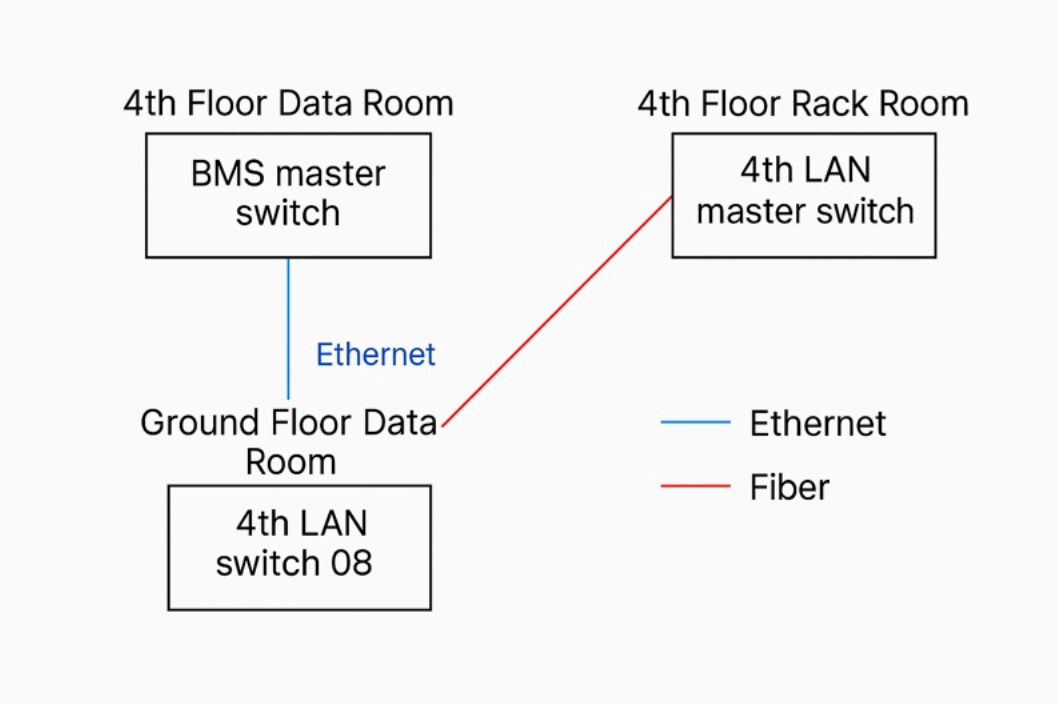


Figure 39 - BMS / 4th LAN Switch Room Diagram

Step 1: Run cables with patch panels and test:

By using patch panels I was able to change the connection and ensure the BMS is still connected to the 4th LAN (The 4Th LAN switch 8 was already connected). When doing this I ran the cables first. But, to ensure that the connection was correct, as this was a live production system I was working with, I plugged 2 PCs together using this connection, one on the ground floor and another on the 4th floor data room. I was able to ping both PCs. This guaranteed my connection was correct.

Step 2: Configure ethernet ports on both switches.

Free ports are disabled on switches in the plant. I had to ensure the ports were up and configured. When configuring I was requested by my colleague that I allow all VLAN's through from BMS to 4th LAN.

17.3 Next setback

While VLAN 800 is the network used by the BMS for operation, the infrastructure team wants to allow VLAN 500 for infrastructure management.

I was requested to reconfigure the firewall to allow multiple ports with multiple same VLAN's, i.e. (interface 1 and 2 accepting VLAN 500 and VLAN 800). After trial and error for a month, I used the deep research tool on ‘ChatGPT’ and asked if it has ever been done before. Other people had this issue, but no fix.

Chat gpt also specified that this was impossible and referenced the Cisco configurations guide book.

> You cannot assign the same VLAN to multiple subinterfaces. You cannot assign a VLAN to the physical interface. Each subinterface must have a VLAN ID before it can pass traffic. To change a VLAN ID, you do not need to remove the old VLAN ID with the **no** option; you can enter the **vlan** command with a different VLAN ID, and the ASA changes the old ID. To remove some secondary VLANs from the list, you can use the **no** command and only list the VLANs to remove. You can only selectively remove listed VLANs; you cannot remove a single VLAN in a range, for example.

Cisco Systems. (2018) *CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.6*.

My resolution:

Create another bridge-group for the firewall, as there are enough physical ports to support this. **How will this work?**

17.4. What This Means

In **transparent mode**, your ASA uses **bridge groups** to forward traffic between interfaces at Layer 2.

When trying to pass **multiple VLANs (e.g., VLAN 500 and VLAN 800)** through the ASA **using one bridge group**, you'd typically try to:

- Tag both VLANs on one trunk interface
- Pass them through a **single subinterface or bridge**

But this breaks the Cisco rule because:

- Each **VLAN must be associated with only one subinterface**.
- A single bridge group **cannot be tied to multiple VLANs via a single trunk** in this manner.

17.5 What I Tried (and Why It Fails):

- One bridge group
- Tagged VLAN 500 and 800 traffic coming in
- Wanted the firewall to bridge both

But ASA doesn't allow multiple VLANs to be handled that way on a single bridge group **because you can't assign the same VLAN ID to more than one interface/subinterface**.

17.6 What the fix is:

- **Two bridge groups**
- **Assign 1 bridge-group per VLAN**
- **Firewall will bridge both individually**
- **Using 4 physical ports on the firewall instead of 2**

So with the firewall having 6 ports on the firewall, we can use 4, creating 2 bridge groups. The bridge-groups will look like:

BVI1(VLAN800)-192.168.230.111
BVI2(VLAN500)-192.168.200.111

I then needed to update the network objects and add a VLAN 500 for the switches only. They are the only objects that use VLAN 500. All the IP's are similar, but instead of .230 they have .200.

17.7 Updated Network Overview

The network will now look like this:

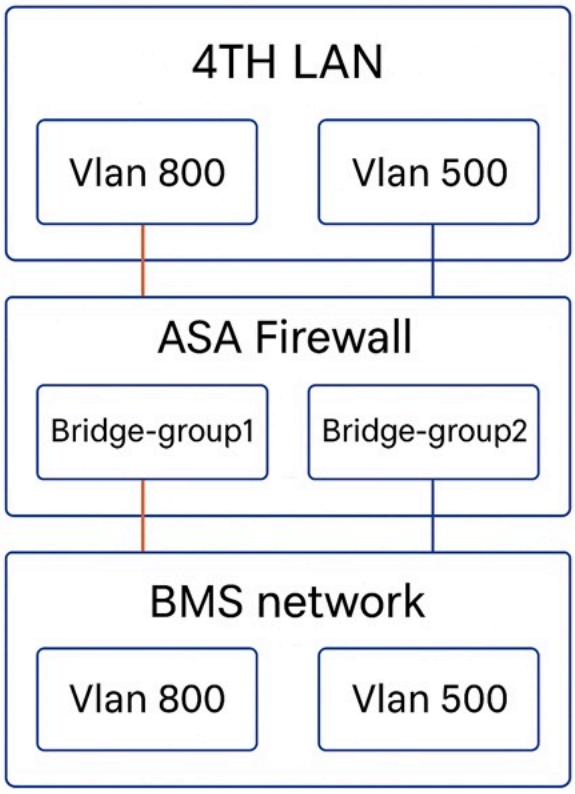


Figure 40 - Network Overview Diagram

Figure 41 - RCMF Firewall Racked

17.8 Implementation

Next step: Install all cables needed and configure switches

As I had one set of cables run for VLAN 800, I ran the same again for VLAN 500, as each used a separate connection to 4TH LAN switch 8. I also ensured they worked again with the ‘ping’ test.

I then configured two interfaces on the 4th LAN switch 08. One interface carried VLAN 800, and the other VLAN 500. This was repeated for the BMS. The ports were configured to switch port access, as this means they use one VLAN which needs to be assigned only. This will ensure the firewall will not drop any traffic, as if there was any mistake made by our configurations, the firewall would block all traffic. However, I first ensured that they worked without the firewall, from switch to switch, a connection for each VLAN.

Next step: Open firewall and close down

Using ASDM I can configure the firewall to allow all traffic first. This is common practise to ensure that the firewall won't block traffic in real world, and to see if there are any ports missing

With the firewall open, I finally plugged the firewall into the connection between the VLAN's.

The rules should look like:

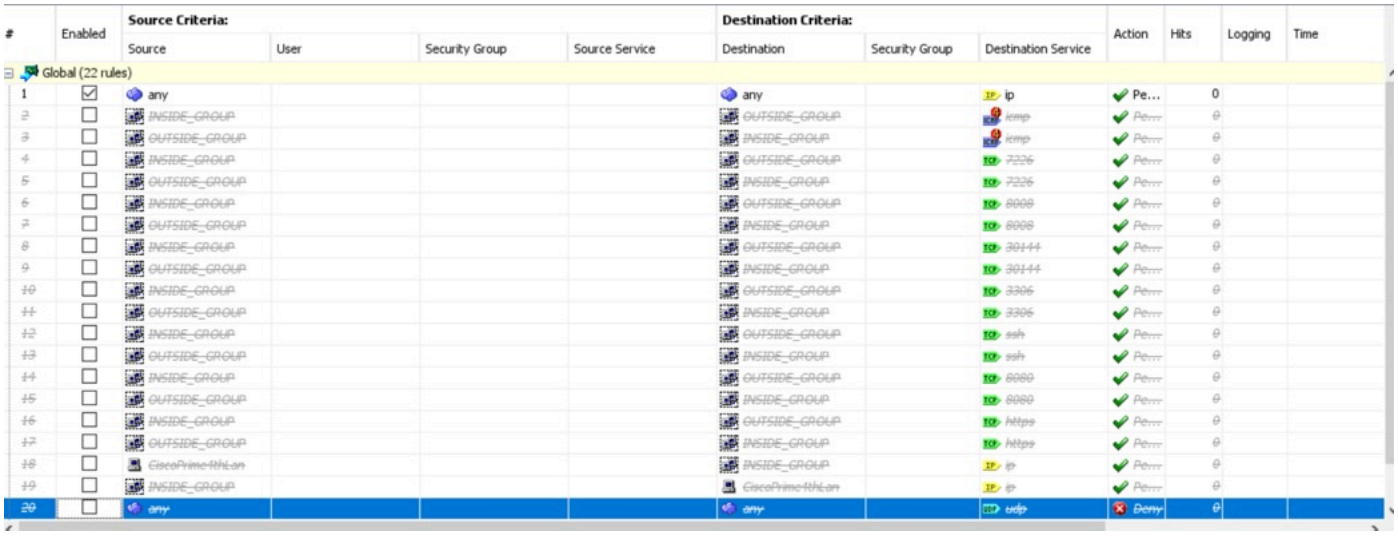


Figure 42 - Rules

I then added the rule ‘Service IP’ which will allow all ports open. Finally, I closed down the firewall using the rules I configured alone. The installation was a success.

18. Digital Artifact:

When I first created the digital artifact, I built the network on **Cisco packet tracer**, a network simulator app which can be downloaded onto your pc. I built the BMS

network without the firewall first, adding all devices and IP addresses. However, I ran into the issue that packet tracer does not support layer 2 configurations.

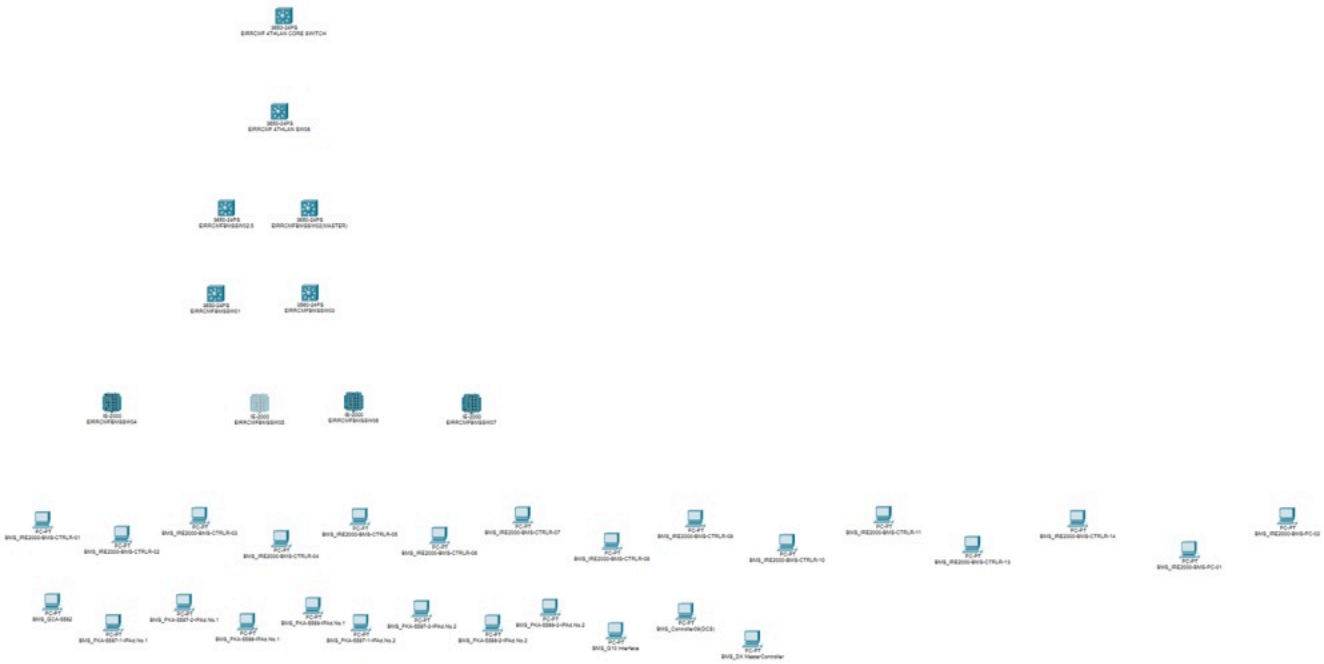


Figure 43 - Digital Artifact

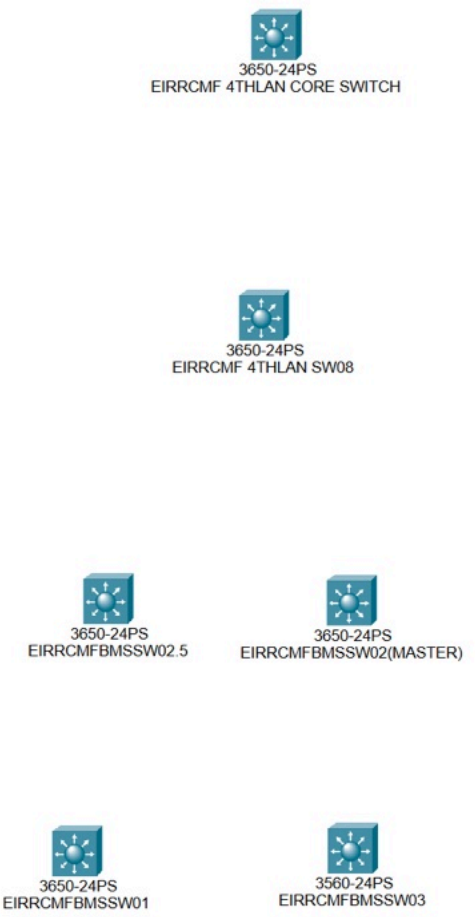


Figure 44 - Digital Artifact

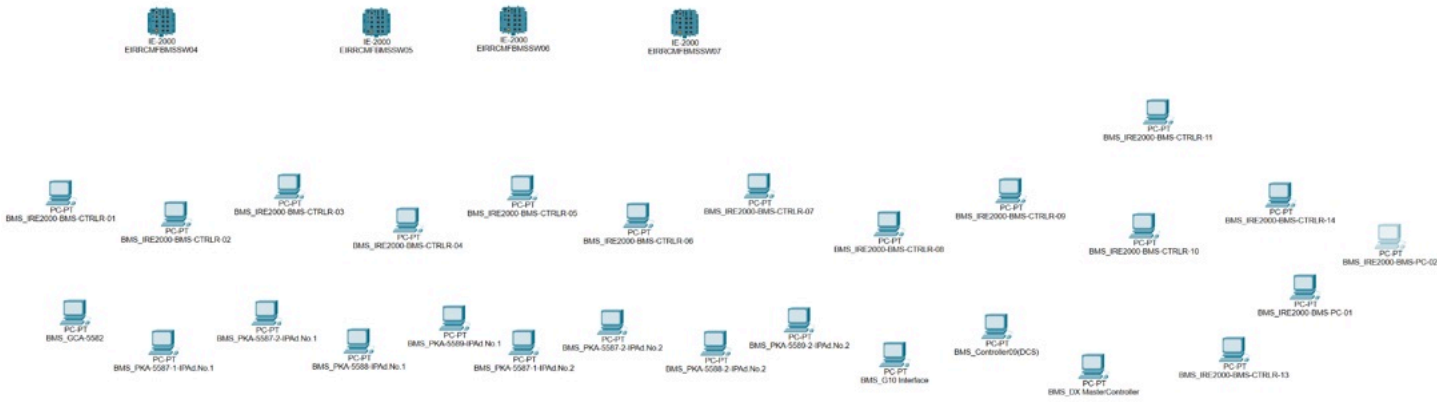


Figure 45 - Digital Artifact

I then attempted to use **GNS3,** which requires the 'Virtual Machine VM workstation' to run. Once I set up GNS3, I then found out that each node on the network needs a license. This created more issues, as I didn't have the finance to buy a license for each device I needed. I finally overcame this issue by using CISCO CML:

18.1 CISCO CML

A network simulator, which

- Supports layer 2 firewall configurations
- Allows up to 5 free network devices
- Needs to be ran off a vm workstation

18.2 How I set up CML

I first attempted to set it up using my personal laptop, but found that with only 8GB ram, I needed more. I then set it up using my Gaming PC, which I built at

home. This gaming PC has 16GB of ram and a power CPU. I was then able to run it. I followed along with '2DtechBG's' youtube guide (Cisco Modeling Labs Course - EP 1 Installation in VMWare Workstation) on how to set it up using VM workstation. This was to ensure I made no mistakes along the way.

Step one: **Download VM workstation and cml.iso download on Gaming PC:**

Go to the VM workstation website (link found in description of video). Create an account and follow the steps to download the free version. This will also have to be done for the Cisco cml. An account is required.

Step two: **Follow along the video.**

Start up a VM workstation and click '**open a virtual machine'.** It will open your files and in 'downloads', you should find the **cml.ovo** image, which you will open. It will ask you to name the VM. I named mine **CML**. Click '**import**'..

Step three: Configure the settings of CML VM.

- Select ram at 16GB
- Select 'network adapter;. It should be bridged.

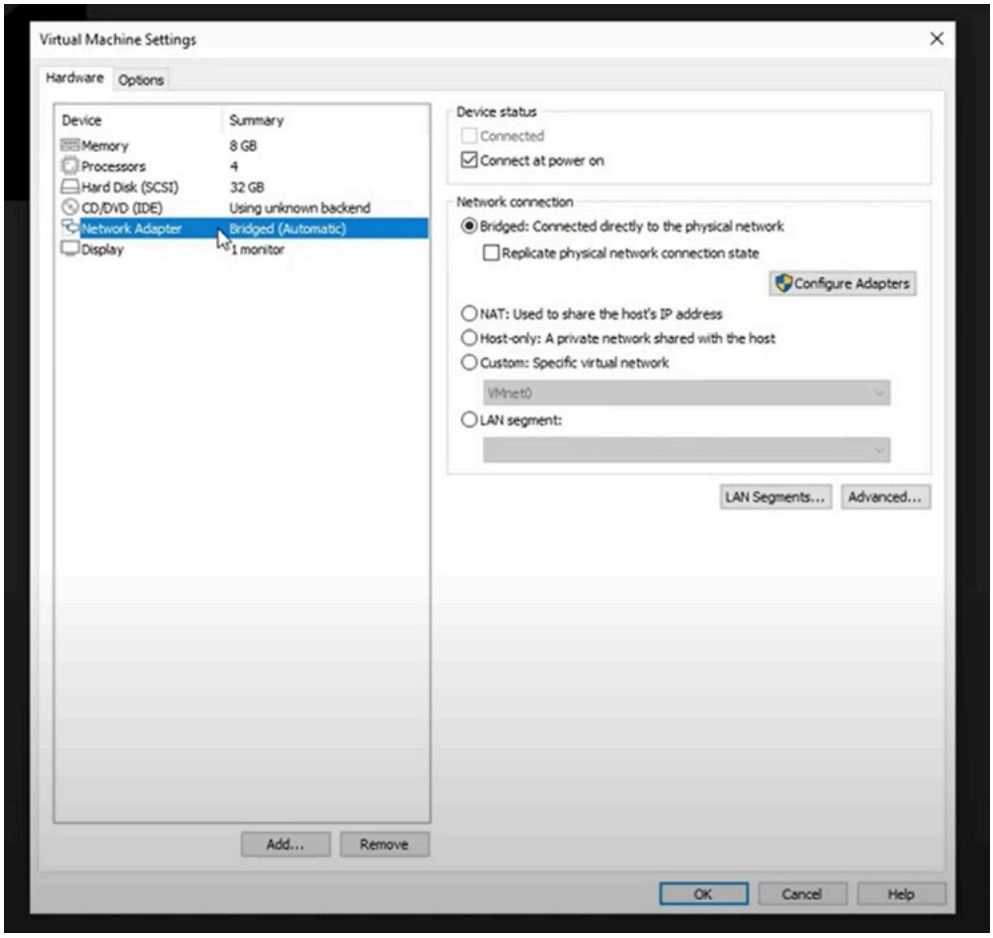


Figure 46 - Network Adapter

- Finally select **CD**. Select '**iso' 'refplat…'**

Step four: Logging.

Start the virtual machine. CML will ask you to input a username and password. Remember this, as you are required to log on every time.

Once CML is fully started, you must find the IP address of your cml server. This will be listed here:

Figure 47 - CML Server IP

You can then enter that into your browser and it will ask you to log in.

I then built the network using the same configurations as I did for the real build. This allowed me to simulate the network.

However, this was still very early on and took me a few weeks to build. To ensure I could reach this from anywhere, I ‘port forwarded’ my cml IP address from my router so that I could log on from any PC.

18.4 What is port forwarding?

Port forwarding is when a combination of a port and IP address from inside the network are available for an external network.

How is it done?

Step one: Find the port you are using and internal IP address.

Step two: Create the rule on the router to forward like so and save:

- Logging into the router GUI
- Accessing advanced settings
- Going into Port Forwarding
- Create and enable rule

Image of the routers rule can be seen in Figure 48 below:

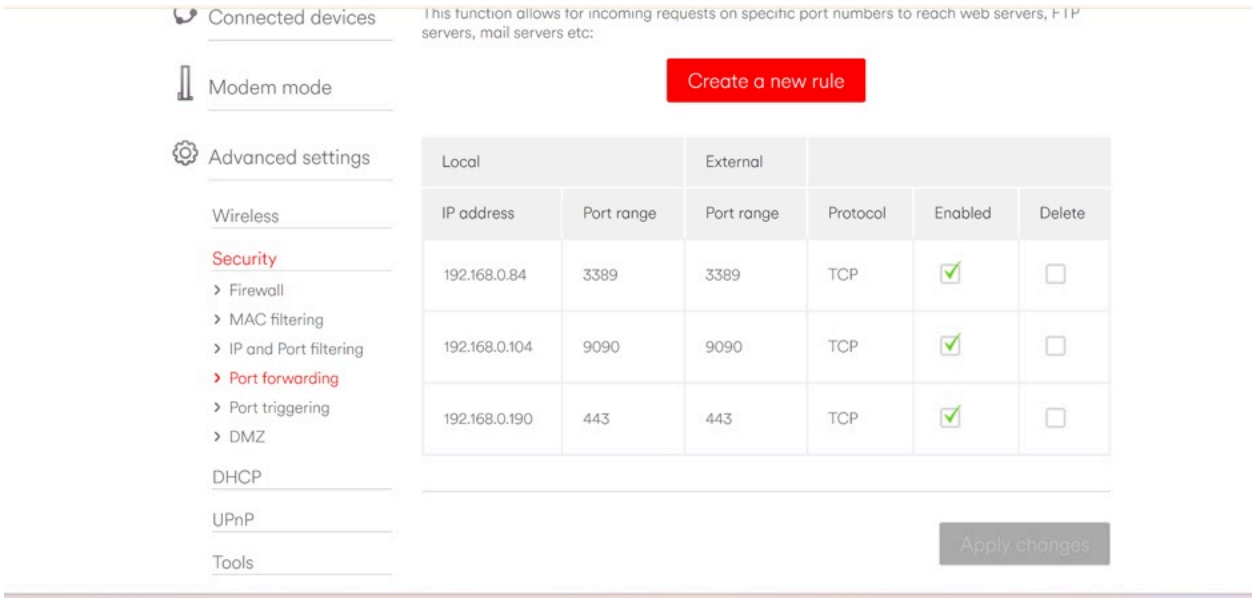


Figure 48 - Routers Rule (Virgin Media Community. (n.d.). How to set up Port Forwarding)

Step three: Find out your external IP address.

Use a website like ‘what is my IP address’ from the PC you are trying to port forward to ensure you're on the right network.

From outside the network, type in the public IP address and port being used like so:

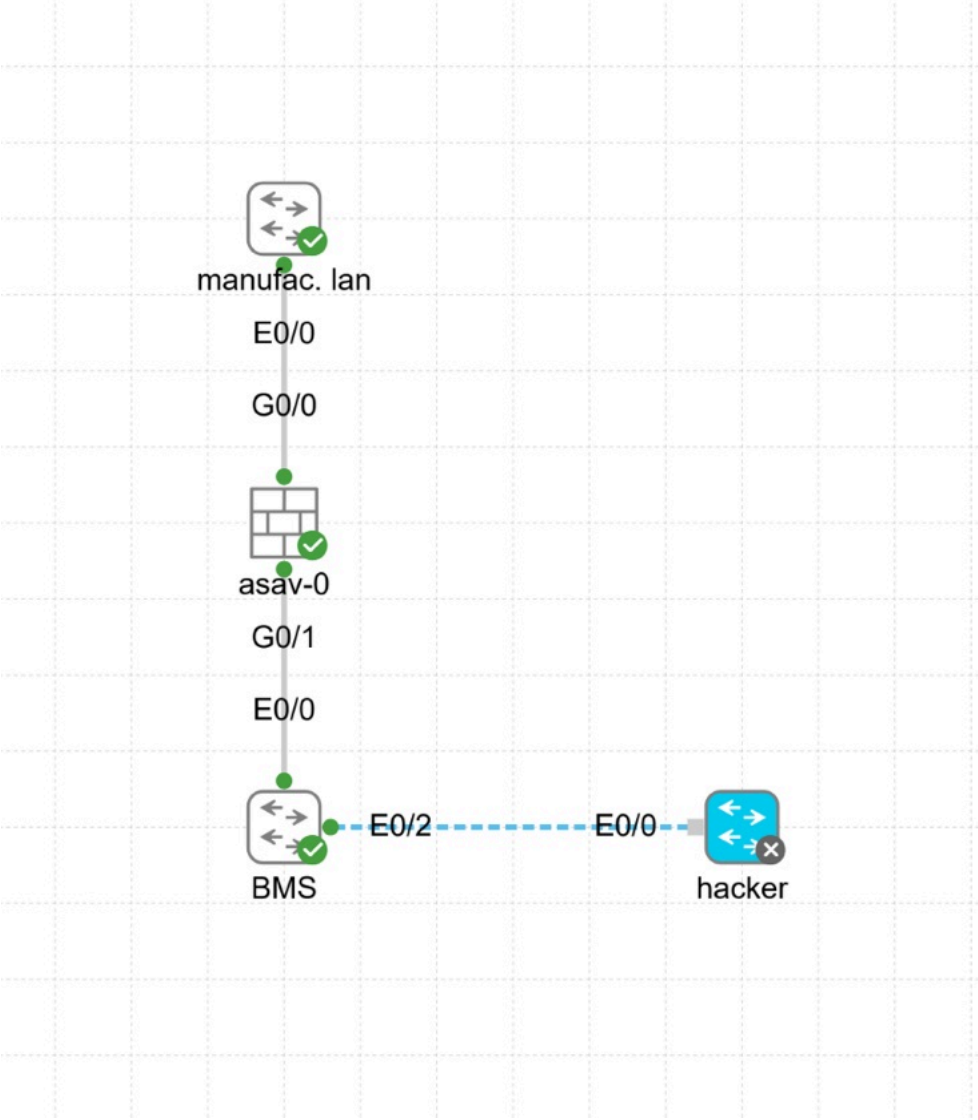


Figure 49 - Image simulation of a network hacker PC unable to pass firewall.

Figure 49 above is an image simulation of a network hacker PC unable to get past the firewall, as shown as part of my presentation at the UCC open day.

19.Evaluation

19.1.Rule evaluation

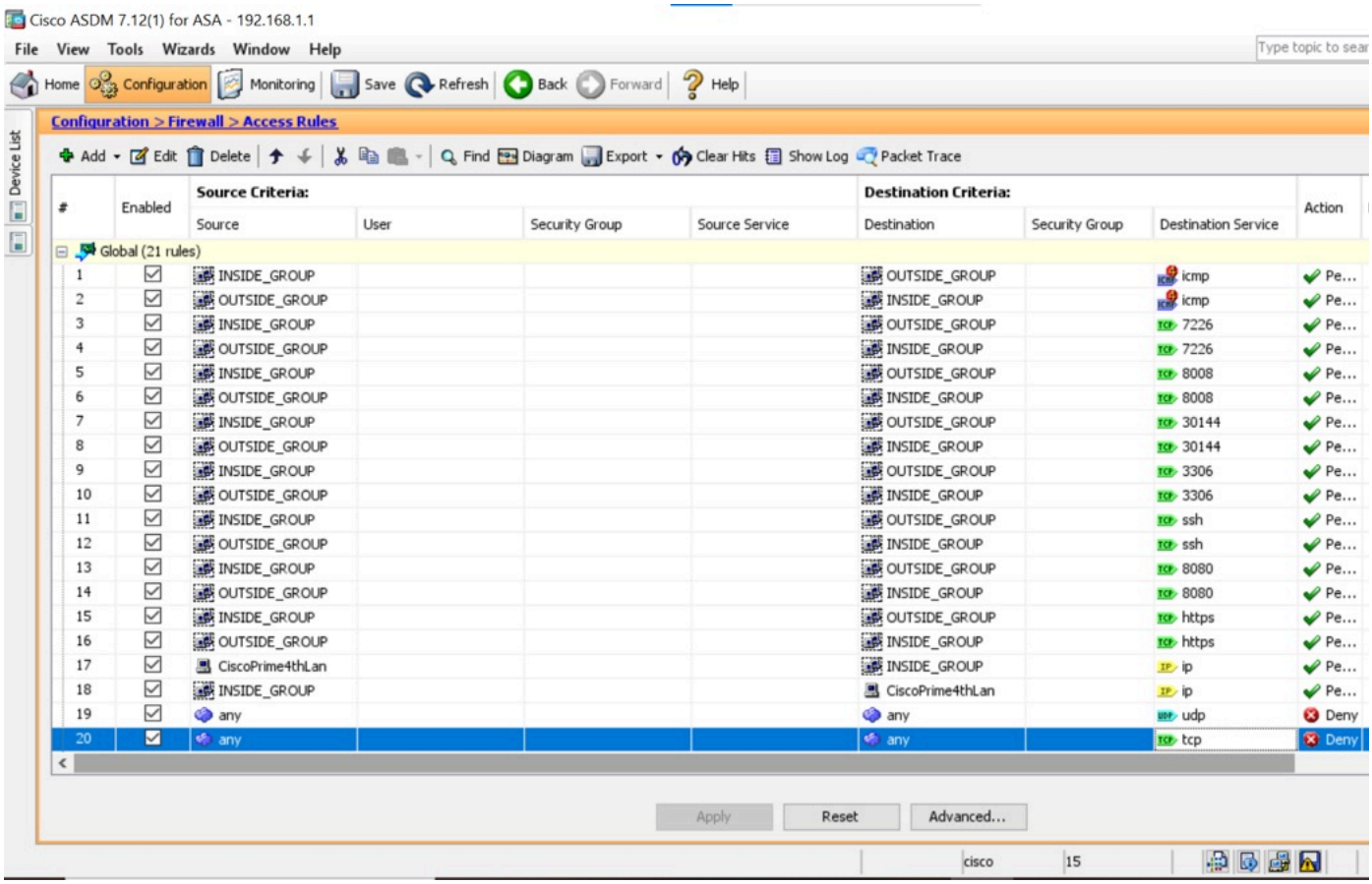


Figure 50 - Rule Evaluation

After building the final rules of the firewall, I hosted a team meeting where I included my boss, Paul (my project supervisor), and two of the senior infrastructure engineers, Cian Fieldenstein and Stephen Morley, to confirm rules and answer questions.

Rule order:

Rules 1 & 2: Both allow ping, this is used in IPmon tools, for our testing to ensure basic data connection is up.

Rules 3,4,5,6,7,8,9 & 10: All are BMS activity ports

Rules 11 & 12: Allow ssh- which is used to access the CLI from the IPMON server, and advanced IP scanner tools.

Rules 13 & 14: Allow port 8080 which allows http, ports which support web based applications like ASDM. needed for IPMON for the GUI of Cisco switches.

Rules 15 & 16: Allow port 443 which also allows http, ports which support web based applications. Again similar needs for IPMON.

Rules 17& 18: The Cisco prime specific rules, since Cisco prime uses too many ports, we have allowed all ports open for that IP only.

Rules 19 & 20: Ensures all traffic coming in under tcp and UDP is blocked, this is followed by the firewall explicitly blocking all traffic.

19.2 Test Evaluation:

Test Scenario	Results
Check ICMP (Ping) For Allowed IP's Only	Success
Test Allowed Ports (TCP)	Success
Test Blocked Ports	Connection refused
Check ASA ACLs	Shows allowed rules

Figure 51 - Test Evaluation

All tests have been documented and handed to the Pfizer Infrastructure Team, which have been overlooked and signed off. This was needed before the firewall was completed.

1.**ICMP:**Ping test was successful and proven by pinging through the firewall.

2.**Testing allowed ports:**using tools like nmap and Ncat specifically the rules are proven to work by allowing coms through the working ports.

3.**Testing blocked ports:**No coms through blocked ports using these tools.

4.**Confirm Rules:**meeting hosted to confirm firewall access control list(rules).

20. Conclusion

The result of this project, in which I deployed a CISCO model ASA 5516-x firewall on a manufacturing network, has written the blueprint for **four other BMS systems**, and networks alike across the site. From initial network mapping and stakeholder consultation, to the final implementation and simulation testing, each phase was approached with precision and a deep understanding of the site's operational constraints.

With being upheld to Pharmaceutical standards, strengthening a part of Pfizer Ringaskiddy's manufacturing network has given me an abundance of learnings.

My own knowledge of Information Technology Infrastructure has grown to a point where I can now usefully contribute to the designing, building and commissioning of data networks with specialist learnings in the area of network infrastructure security.

- My understanding of the Open Systems Interoperability OSI standards has enabled me to apply these standards conventions in the application of additional cybersecurity to an industrial network. Building a sophisticated firewall in transparent mode has enabled me to master layer 2 configurations, for not only firewalls but also switches.
- Network traffic management applies conventions in terms of data systems addressing via Internet Protocol. Consistent with this addressing, data applications and data groups associated with specific applications can be routed via data port conventions. Grasping knowledge about data ports, and how network communications work as a whole, using ports and IP Addresses can be the basis for a sophisticated Firewall security application.
- Networks can be both physical and virtual. The application of virtual networks is a powerful tool for compartmentalizing applications and data for both security and system application integrity. In the application I have developed, I have applied a physical Firewall that integrates Virtual LANS.

The integration of the VLANS in the physical Firewall proved to be limited due to the requirements to segregate traffic to different ports. This application demonstrates how they operate and issues which can arise when configuring them.

- The project demonstrated the requirement for the access to a development environment for secure testing, commissioning and verification of a modification to a complex network environment. In order to integrate the additional cybersecurity features, I had to design, document, test and verify the installation in the test and verification environment. The site Quality Assurance team oversaw the process to ensure I had fully verified the design intent. These steps are needed when deploying a firewall on the network, on a pharmaceutical network, and the risks that come with mismanaging and incorrect simulation became clear during the project lifecycle.
- While much of the infrastructure was proprietary Cisco equipment, the application of these proprietary tools such as CISCO CML, are critical to understanding the application of the industry interoperability standards and I now appreciate how that will help me when designing future networks.
- A key learning for me was to work as a team member of a group of Subject Matter Experts (SME's) in a controlled environment. Central to the success of this project is the interaction and collaboration with both Pfizer's Infrastructure team and the specialist HVAC BMS vendor Sygma Automation, while I was delivering my own individual project within set deadlines and functional requirements. Teamwork is critical to success.

- Finally, in an Open Systems environment, the application of cybersecurity extends beyond individual component security controls and requires an integrated design approach to the overall network topology. This design approach has to be carefully architected in an organizational enterprise environment such as Pfizer. The application of central policies and local rules (such as the firewall rules configured as shown above) are the basis of a holistic cyber security environment.

Ultimately this project segments the network successfully and efficiently, while also allowing for little network architecture change. This deployment has also increased the visibility and control for the infrastructure team. The next step is to deploy this system across the site, using the configuration developed in this project, to enable this additional layer of security to an already secure environment.

21. References:

Cisco Modeling Labs. (n.d.). *Cisco Modeling Labs – Official Product Page & Documentation*. Cisco Systems. Available at: https://www.cisco.com/c/en/us/products/cloud-systems-management/modeling-labs/index.html

check Point. (2023). *Check Point Research Security Report 2023*. Available at:https://research.checkpoint.com/2023/2023-security-report-cyberattacks-reach-an-all-time-high-in-response-to-geo-political-conflict-and-the-rise-of-disruption-and-destruction-malware/

Cisco Modeling Labs. (n.d.). *System Requirements*. Cisco Systems Learning Network. Available at: https://developer.cisco.com/docs/modeling-labs/system-requirements/

Cisco Systems. (n.d.). *Cisco IOS XE 17 – Installation and Configuration Guides*. Available at: https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/products-installation-and-configuration-guides-list.html

Cisco Systems. (n.d.). *ASA 5516-X Data Sheet*. Available at: https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733916.html

Cisco Systems. (n.d.). *ASA Access Rules and Service Object Definitions*. Available at: **CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.16**

Cisco Systems. (n.d.). *ASA CLI Configuration Guide – Logging*. Available at:**CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.16**

Cisco Systems. (n.d.). *ASA Command Modes and CLI Guide*. Available at: https://www.cisco.com/c/en/us/td/docs/security/asa/asa916/configuration/general/asa-916-general-config.pdf

Cisco Systems. (n.d.). *ASA Configuration: Access ASDM via Management Port*. Available at: https://community.cisco.com/t5/security-knowledge-base/how-to-access-the-cisco-asa-using-asdm/ta-p/3122862#toc-hId--1446998985

Cisco Systems. (n.d.). *ASDM Product Page*. Available at: https://www.cisco.com/c/en/us/products/security/adaptive-security-device-manager/index.html

Cisco Systems. (n.d.). *Configure VLAN and Access Port Settings*. Available at: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swint.html#wp1002391

Cisco Systems. (n.d.). *General ASA Configuration Guide (v9.12)*. Available at: https://www.cisco.com/c/en/us/td/docs/security/asa/asa912/configuration/general/asa-912-general-config.html

Cisco Systems. (n.d.). *Understanding and Configuring VLANs on Catalyst 4500 Series Switches*. Available at: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html

Cisco Systems. (n.d.). *IP Addressing and Subnetting Overview*. Available at: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/blogs/200404.html

Cisco Systems. (n.d.). *Port Number Usage Reference Guide*. Available at: https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/I-R/asa-command-ref-I-R/pr-pz-commands.html

Cisco Systems. (2021). *Cisco Prime Ports*. Available at: https://community.cisco.com/t5/wireless/cisco-prime-ports/td-p/4501110

Elsevier. (2014). *Industrial Network Security (2nd ed.)*. Available at: https://www.elsevier.com/books/industrial-network-security/knapp/978-0-12-420114-9

Virgin Media Community. (n.d.). *How to set up Port Forwarding*. Available at: https://community.virginmedia.com/blog/Digital-life/how-to-set-up-port-forwarding/3530654

NIST. (2015). *Guide to Industrial Control Systems (ICS) Security – SP 800-82 Rev. 2*. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Nmap. (n.d.). *Nmap Installation on Windows*. Available at: https://nmap.org/book/inst-windows.html

Nmap Project. (n.d.). *Ncat Users' Guide*. Available at: https://nmap.org/ncat/guide/

U.S. Food and Drug Administration. (2004). *PAT – A Framework for Innovative Pharmaceutical Development, Manufacturing, and Quality Assurance*. Available at: https://www.fda.gov/media/71012/download

Cisco Systems. (n.d.) *OSI Model Reference Chart*. Available at: **https://learningnetwork.cisco.com/s/article/osi-model-reference-chart**

Cisco Systems. (n.d.) *CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.6 – Access Objects*. **Available at: https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/firewall/asa-96-firewall-config/access-objects.html**

2DtechBG. (2022) *Cisco Modeling Labs Course - EP 1 Installation in VMWare Workstation*. YouTube video, 17 November. Available at: **https://www.youtube.com/watch?v=t2CZ_43yi4M**