

Project Title "Design and Implementation of a Network Security Monitoring System"

Project Description

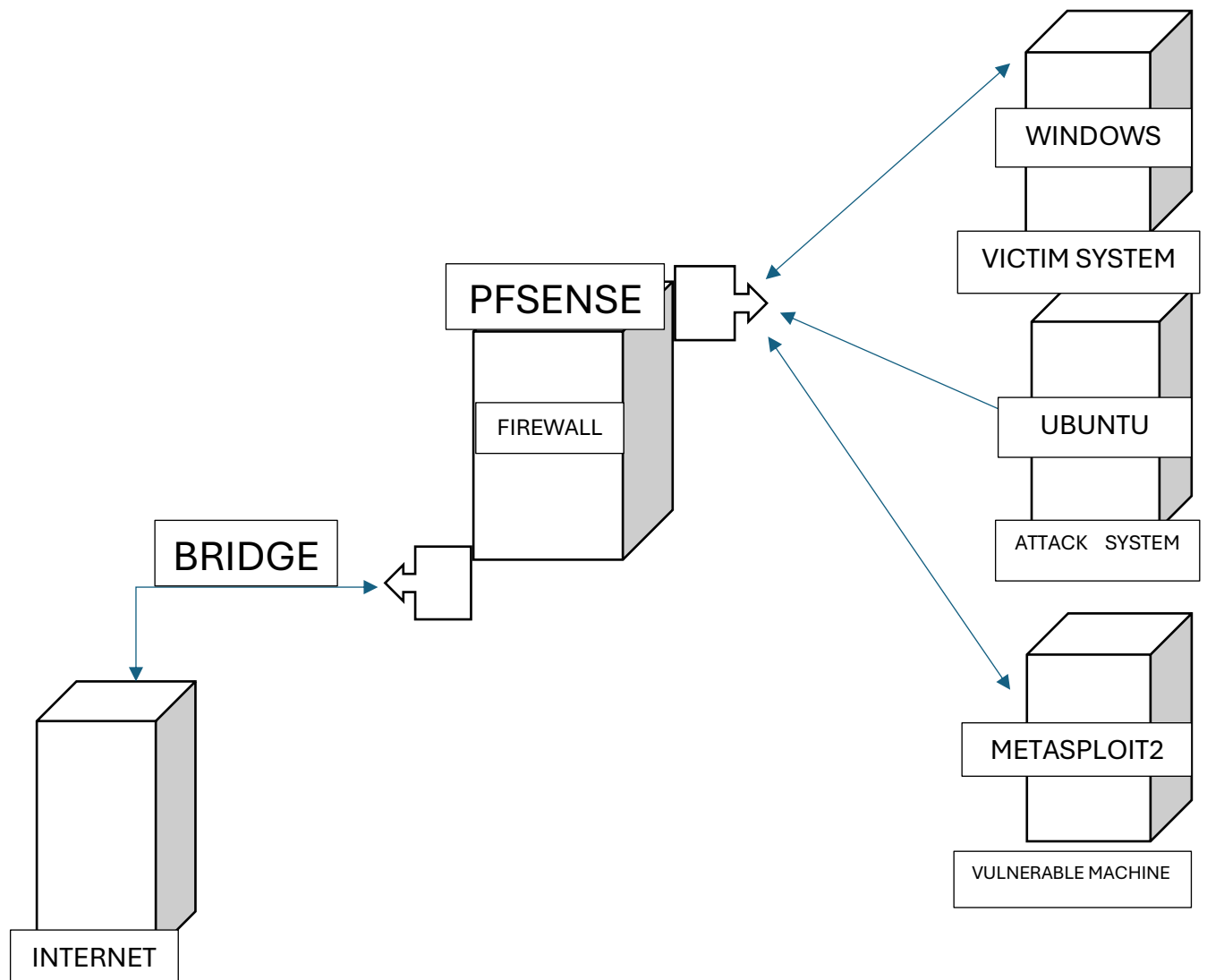
In this project, you will set up a virtual lab to simulate a secure network environment. You will use tools like pfSense, Snort, and Suricata for network monitoring and intrusion detection, and you will practice active and passive information gathering techniques. The goal is to learn how to monitor and secure a network by identifying threats and anomalies in network traffic.

Project Objectives

1. Understand and implement active and passive information-gathering techniques.
2. Set up and configure pfSense as a firewall and network gateway.
3. Install and configure Snort and Suricata for intrusion detection and prevention.
4. Analyze network traffic to identify malicious activities using IP addresses and protocols.
5. Document findings and propose security recommendations.

1. PfSense: as a firewall has two interfaces, one for the internal network and the other for external network and each interface with its own IP address. The internal network IP is used as a default gateway for OS in the internal network. The bridge interface IP is used by the pfSense to browse with the help of the Network provider.
2. Metasploit 2: Has only one interface so we connect its adapter to the internal network.
3. The other OS (Windows 10, Ubuntu): Can power two adapters at once, so they are connected to the bridge and internal network interfaces.
 - a. Bridge network: Enables the OS to go to the network provider independently outside the internal network connection.
 - b. Internal network: Binds the OS together under an internal LAN and it doesn't browse, that is why the bridge network is included in the network design.
2. The other OS (Windows server, Windows 10 & 11, Ubuntu): Can power two
3. adapters at once, so they are connected to the bridge and internal network
4. interfaces.
 5. a. Bridge network: Enables the OS to go to the network provider independently
 6. outside the internal network connection.
 7. b. Internal network: Binds the OS together under an internal LAN and it doesn't
 8. browse, that is why the bridge network is included in the network design.

NETWORK DIAGRAM



- 1.Ubuntu (attack system)
- 2.Windows 10 (victim system)
- 3.Metasploit 2 (down vulnerable machine)
- 4.pfsense (firewall)

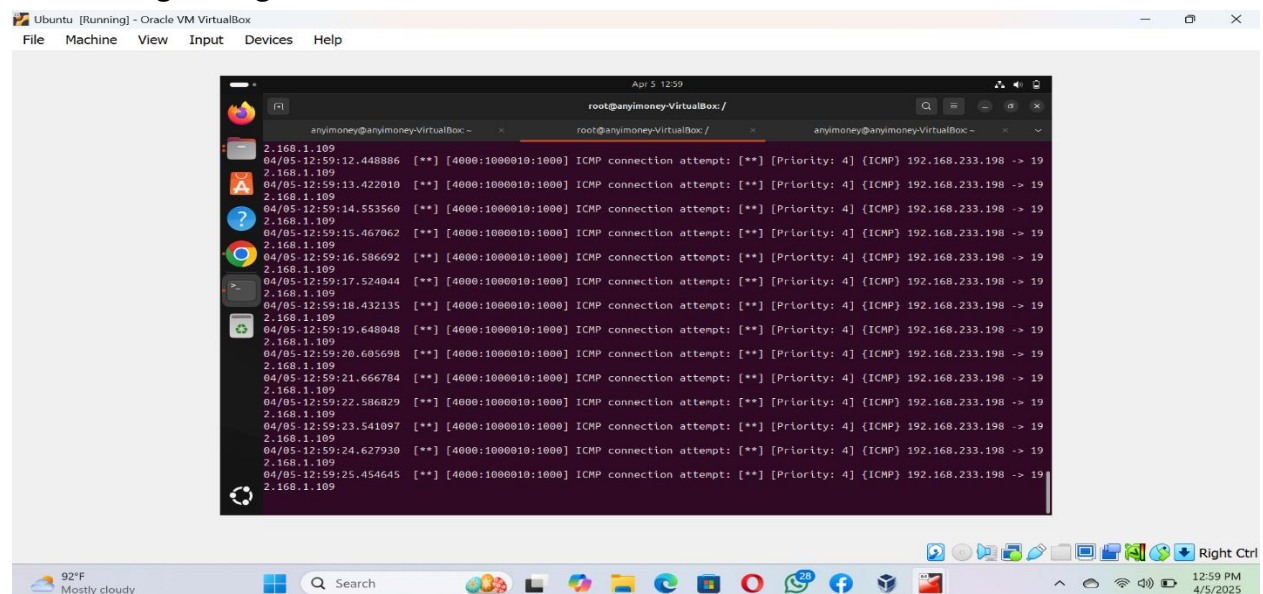
Note: I used a network configuration of bridge and internal network for a good result

Then you confirm the connection by pinging each machine to one another.

Step 1. {Using Snort as intrusion detection services.}

Then once the ping is successful, you enter your ubuntu machine update and upgrade your ubuntu and install snort via the curl process (Sudo apt install snort-y) while install you will be asked for the network you wants to monitor, if you are going with internal network then you will have to go with an Ip like this 192.168.1.0/24 then click okay and wait for it to fully load.

Then once it has fully downloaded, locate your part of the newly downloaded snort via your terminal configure your HOME_NET and set up the rest configuration then set up your local rules correctly with the message you wants it to drop once a traffic is detected, after that you update your snort if it went successful then restart the snort, then go and ping your ubuntu with kali after you might have turn on the console mode command at your ubuntu terminal then you should able to see the rules you wrote displaying at your dashboard with the message along with it



Step 2. {Using Suricata as Ips, Intrusion prevention services}.

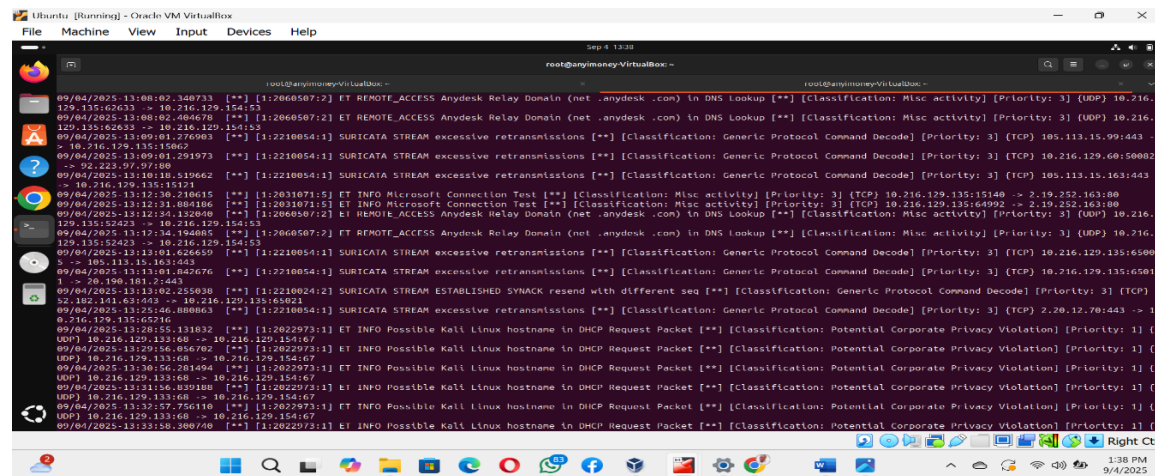
Still making use of your Ubuntu machine install suricata via curl:{sudo apt install suricata – y, then once it has successfully download} locate the part of the downloaded suricata via your ubuntu terminal then locate the HOME_NET and input your network IP and also set the network interface you want to monitor Enp0s8 or Ether, make the community id true and make sure you set the right interface you wants to monitor after that you locate your default rule then test it with your console mode if it went well you are going to receive a successful message, then after that you locate your suricata.conf look for the costume

roles then create your own role folder and file inside then nano it and add your costume role inside you can make use of snorpy to write a blocking role copy and paste it there save and exit then update your suricata once it's done successful then you should go to kali browser and search for suricata documentation then locate the suricata rules copy the curl command and paste on the kali terminal then you should restart your suricata and activate the console mode which should stop your kali from pinging your ubuntu then you should check your log file for the message concerning the rule you have written.

Step 3. Active and passive information gathering via Nmap {Nmap -T4 -A -v -Pn {internal network}}

Report = total host [255] , Total host up [3] = 255 - 3 = 252, Total host down [252]

Dns resolution = 0 Syn Scan = 10.216.129.198

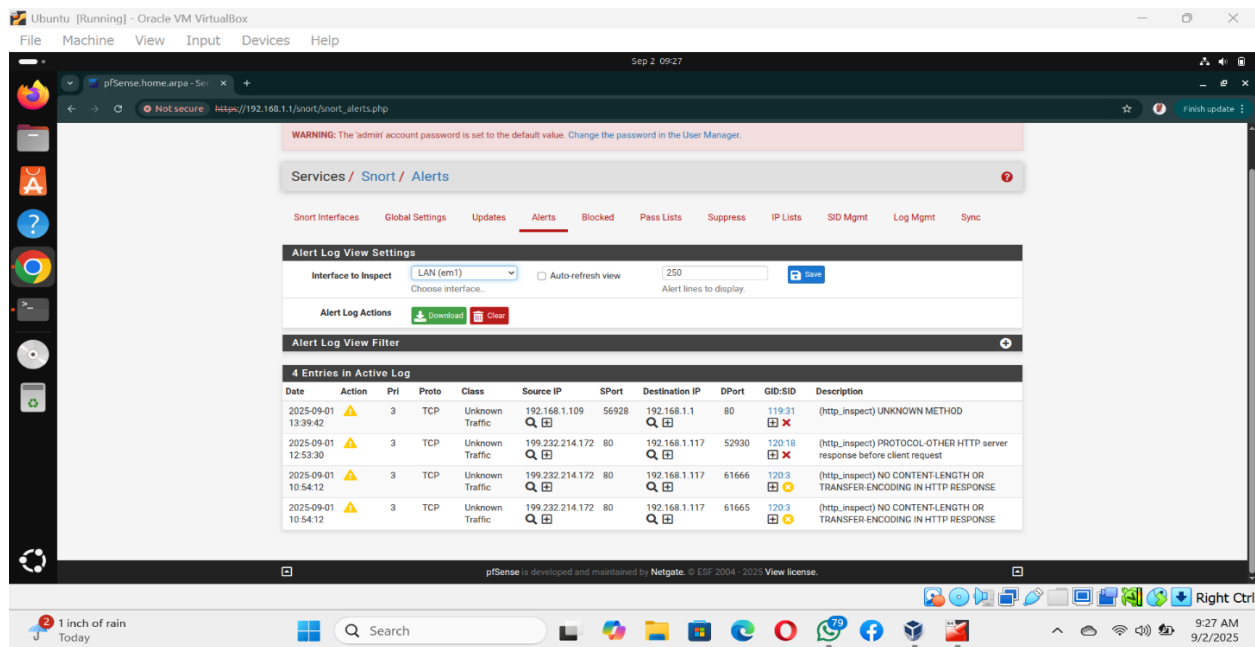


```
root@anyimoney-VirtualBox: ~
09/04/2025:13:08:02.368733 [**] [1:2060507:2] ET REMOTE_ACCESS Anydesk Relay Domain (net.anydesk.com) in DNS Lookup [**] [Classification: Misc activity] [Priority: 3] (UDP) 10.216.129.135:62633 -> 10.216.129.154:53
09/04/2025:13:08:02.404678 [**] [1:2060507:2] ET REMOTE_ACCESS Anydesk Relay Domain (net.anydesk.com) in DNS Lookup [**] [Classification: Misc activity] [Priority: 3] (UDP) 10.216.129.135:62633 -> 10.216.129.154:53
09/04/2025:13:09:01.276903 [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] (TCP) 105.113.15.99:443 -> 10.216.129.135:15062
09/04/2025:13:09:01.291973 [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] (TCP) 10.216.129.60:50082 -> 92.223.97.97:80
09/04/2025:13:10:10.519662 [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] (TCP) 105.113.15.163:443 -> 10.216.129.135:15121
09/04/2025:13:12:30.210615 [**] [1:2031071:5] ET INFO Microsoft Connection Test [**] [Classification: Misc activity] [Priority: 3] (TCP) 10.216.129.135:15148 -> 2.15.252.163:80
09/04/2025:13:12:31.080106 [**] [1:2031071:5] ET INFO Microsoft Connection Test [**] [Classification: Misc activity] [Priority: 3] (TCP) 10.216.129.135:64992 -> 2.15.252.163:80
09/04/2025:13:12:34.132040 [**] [1:2060507:2] ET REMOTE_ACCESS Anydesk Relay Domain (net.anydesk.com) in DNS Lookup [**] [Classification: Misc activity] [Priority: 3] (UDP) 10.216.129.135:62633 -> 10.216.129.154:53
09/04/2025:13:12:34.194085 [**] [1:2060507:2] ET REMOTE_ACCESS Anydesk Relay Domain (net.anydesk.com) in DNS Lookup [**] [Classification: Misc activity] [Priority: 3] (UDP) 10.216.129.135:62633 -> 10.216.129.154:53
09/04/2025:13:13:01.626619 [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] (TCP) 10.216.129.135:6500 -> 105.113.15.163:443
09/04/2025:13:13:01.642676 [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] (TCP) 10.216.129.135:6501 -> 105.113.15.163:443
09/04/2025:13:13:02.255030 [**] [1:2210054:1] SURICATA STREAM ESTABLISHED SYNACK resend with different seq [**] [Classification: Generic Protocol Command Decode] [Priority: 3] (TCP) 10.216.129.135:6501 -> 10.216.129.135:6501
09/04/2025:13:25:46.888063 [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] (TCP) 2.20.12.78:443 -> 10.216.129.135:6501
09/04/2025:13:28:55.131832 [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] (UDP) 10.216.129.133:68 -> 10.216.129.154:67
09/04/2025:13:29:56.056702 [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] (UDP) 10.216.129.133:68 -> 10.216.129.154:67
09/04/2025:13:30:56.281494 [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] (UDP) 10.216.129.133:68 -> 10.216.129.154:67
09/04/2025:13:31:56.039188 [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] (UDP) 10.216.129.133:68 -> 10.216.129.154:67
09/04/2025:13:32:57.756110 [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] (UDP) 10.216.129.133:68 -> 10.216.129.154:67
09/04/2025:13:33:58.300740 [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] (UDP) 10.216.129.133:68 -> 10.216.129.154:67
```

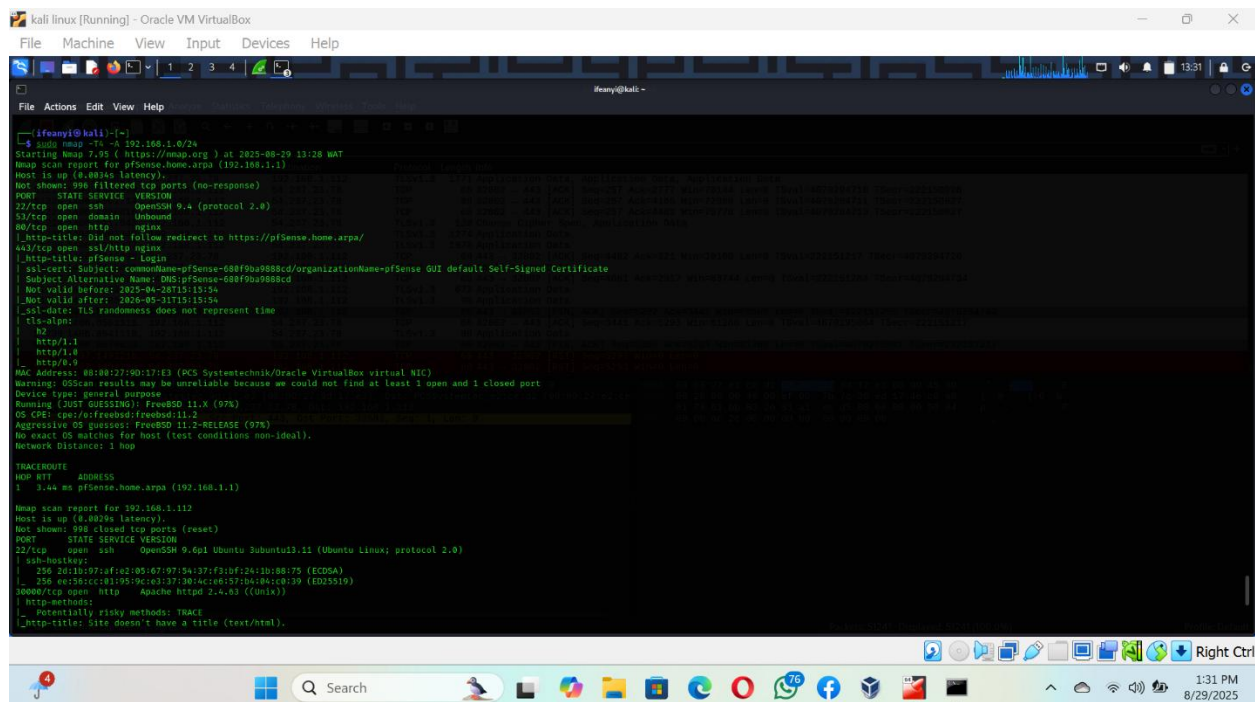
Pfsense firewall rule = pass. Any. Lan subnet. Any . this firewall . Any. Msg [passing role]

When you go into the pfsense dashboard you navigate to the package manager and download snort so you can push and analyze your snort logs over there.

Then check your snort alert on pfsense.



Then launch an active information gathering attack with your kali to see the os, ports, and services running in that entire network.



Then I discovered the ports running which are port: 22,53,80,443, which are majorly SSH & Tcp which is not secure.

Then I discovered the ip in the network through the help of Nmap which are:

Pfsense – 192.168.1.1

Windows-192.168.1.117

Ubuntu-192.168.1.112

SECURITY RECOMMENDATION

1. Keep the operating system and installed open-source software up to date by regularly applying security patches and updates. Open-source systems often release frequent security fixes for vulnerabilities.
 2. Disable unused ports and services that are not required, for example, disable the SSH service if not needed or restrict access using firewalls.
 3. Secure essential services like SSH by configuring SSH key-based authentication and disabling password-based authentication.
 4. Implement network segmentation to isolate sensitive systems or critical services from less secure parts of the network.
 5. Review configuration files regularly, especially for critical services (such as Apache, SSH), and ensure they follow secure configuration guidelines.
 6. Encrypt data in transit using protocols like TLS/SSL for web traffic (if hosting websites or services) and ensure SSH connections are secured using strong cryptographic algorithms.
 7. Encrypt sensitive data both at rest and in transit.
3. By following these recommendations, you can strengthen the security posture of the firewall at 192.168.1.1, helping to protect your network from a variety of cyber threats.

Following this recommendation above you will be able to have a better and more secure network...