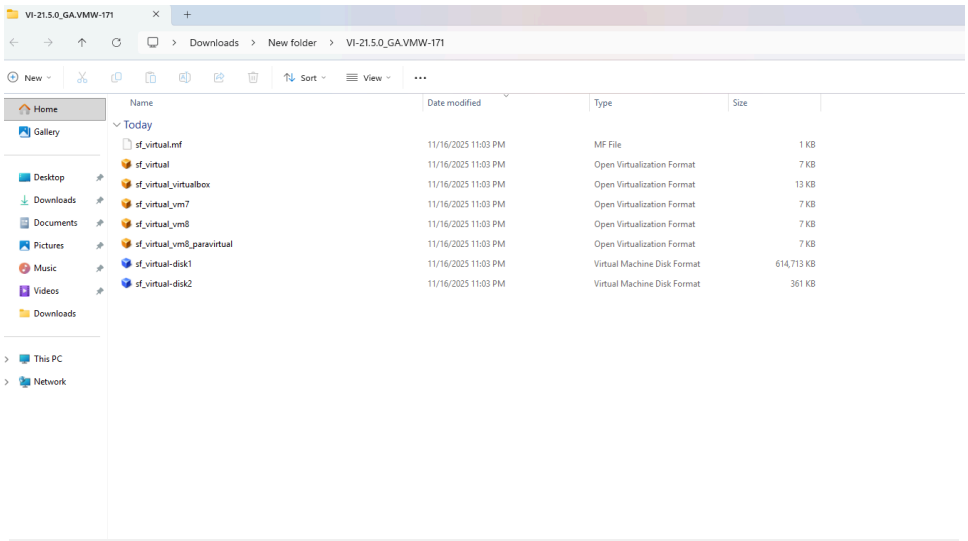
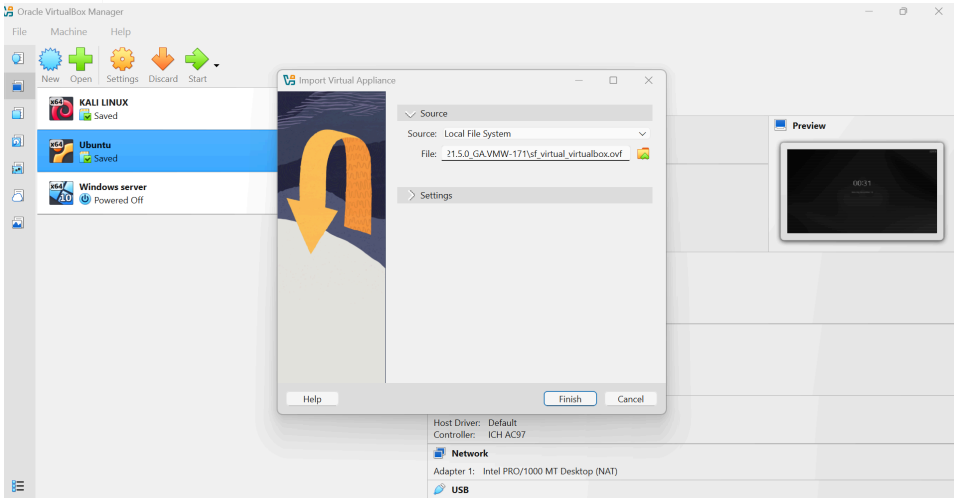
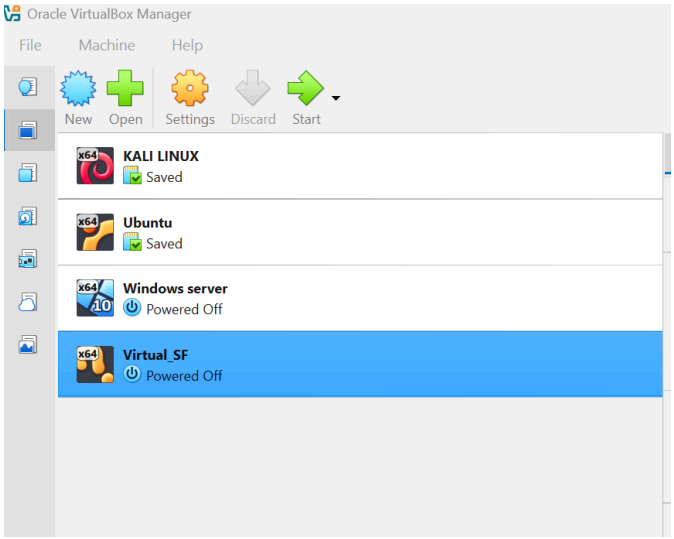
SOPHOS FIREWALL CONFIGURATION LAB REPORT

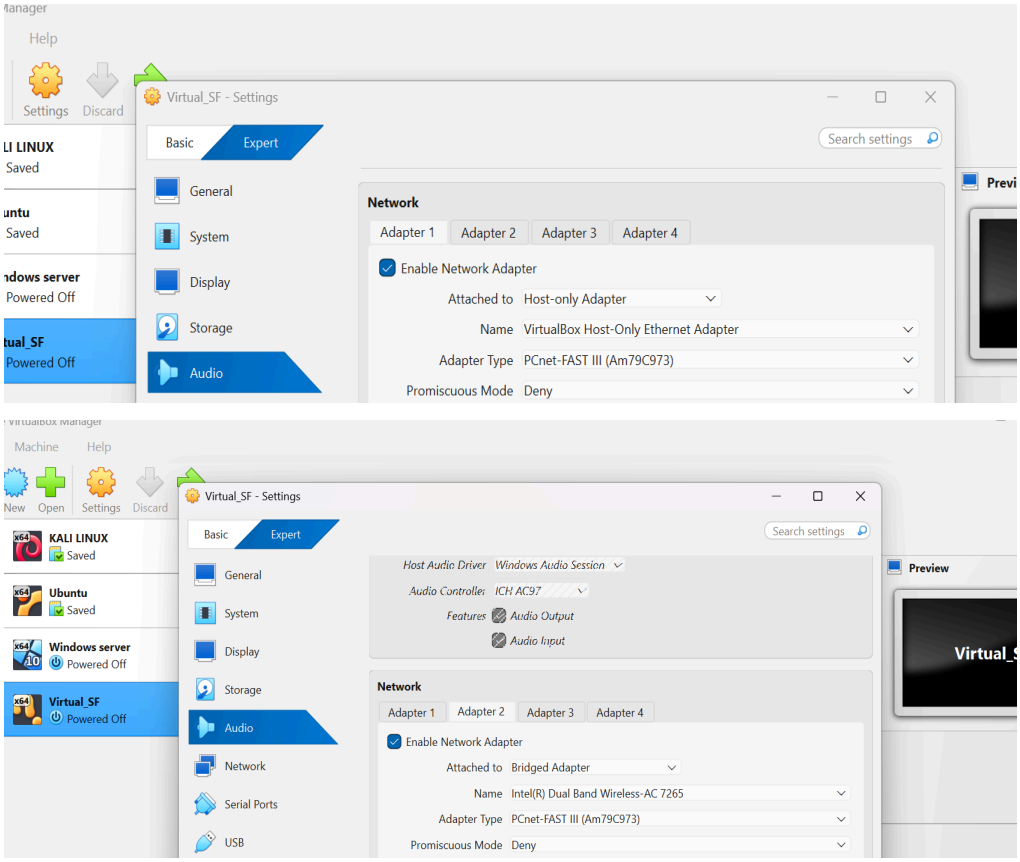
1. **Initial Download and Installation:** I downloaded the sophos firewall virtual installer and installed it on Virtual box. The file downloaded was tagged “Virtual Installers : Firewall OS for VMware”.





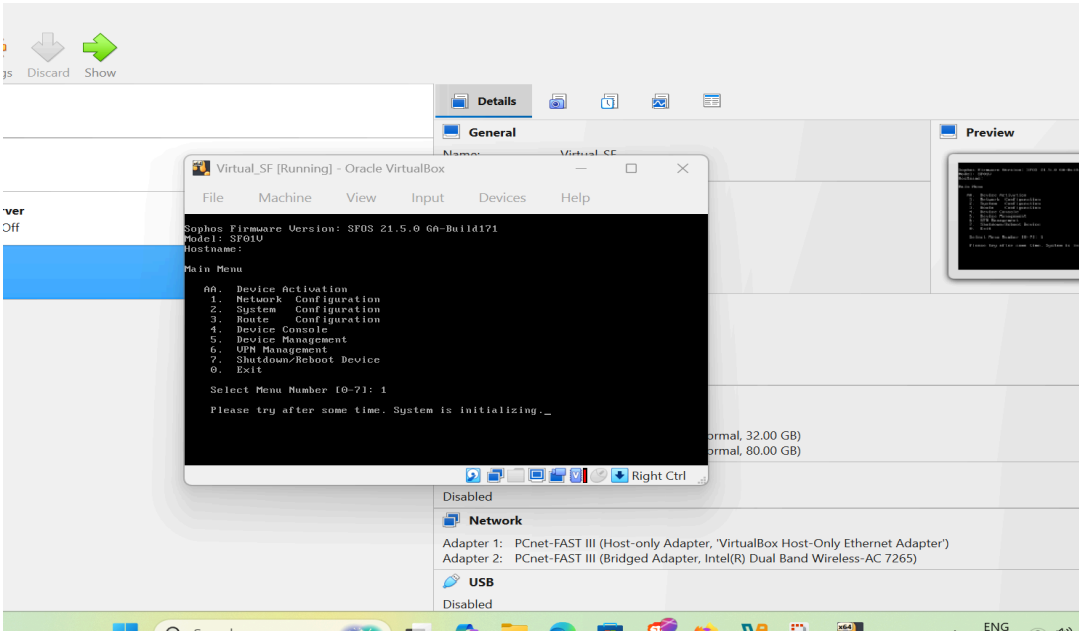


2. **Virtual Machine Network Adapter Configuration**: I configured the network adapters for the firewall VM.
    a. Adapter 1: Host-Only Adapter.
    b. Adapter 2: Bridged Adapter

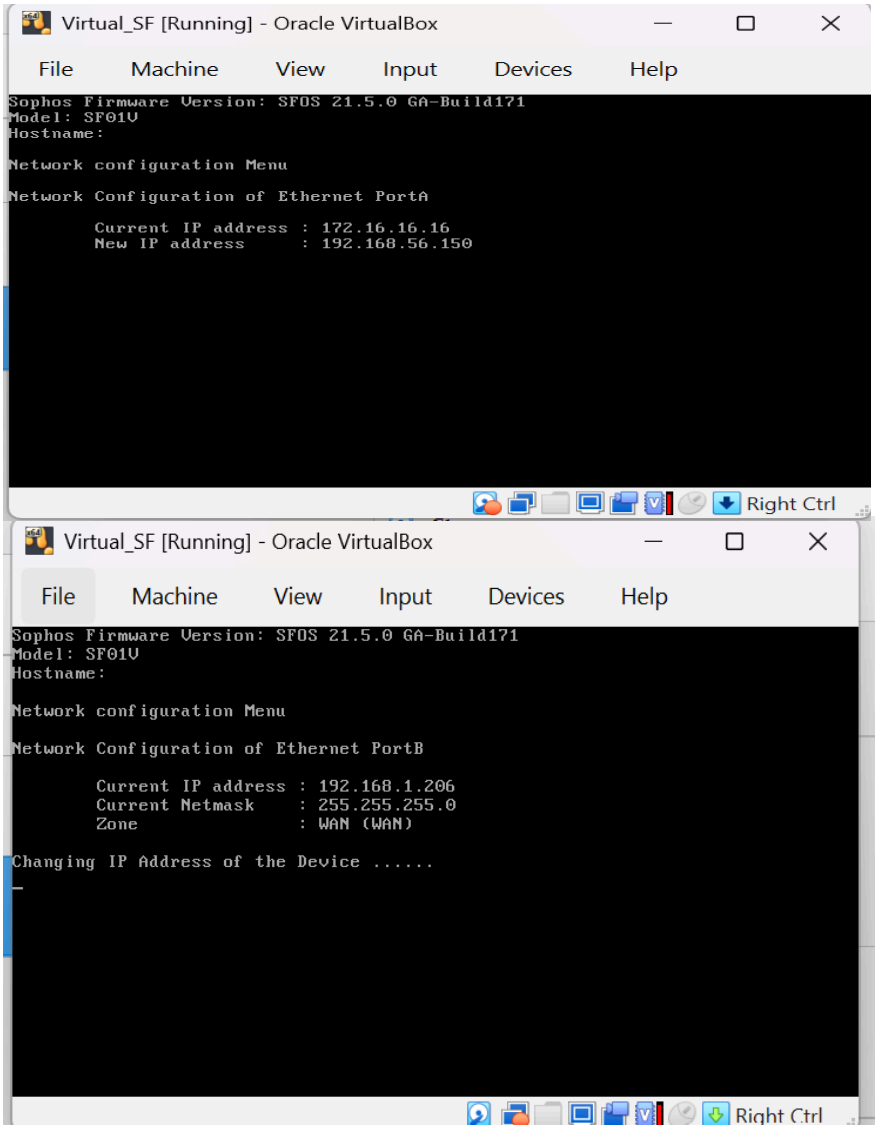


While Adapter 1(Host-Only) allows the SOPHOS Firewall to be configured securely from the host machine. Adapter 2(Bridged) connects the SOPHOS firewall to the network, enabling it to handle network traffic and protect devices.

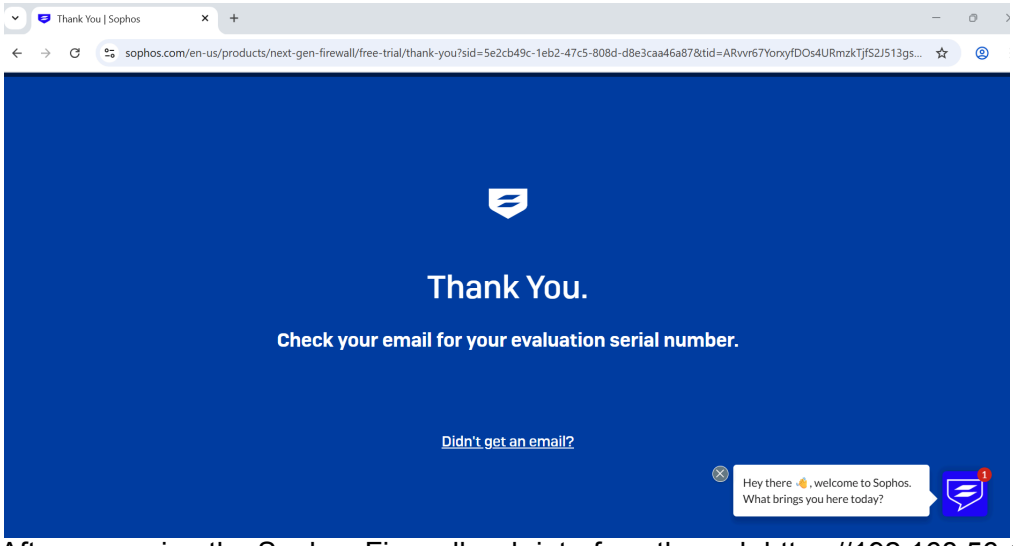
3. Initial firewall launch and configuration: I powered on the SOPHOS virtual firewall on my virtual machine. I was prompted to put in a password which was ‘admin’ by default. Accepted their licensing agreement by pressing “a”.
Activated device on Port A by selecting (1) for network configuration. I then chose interface Configuration by clicking (1) on the network configuration menu.



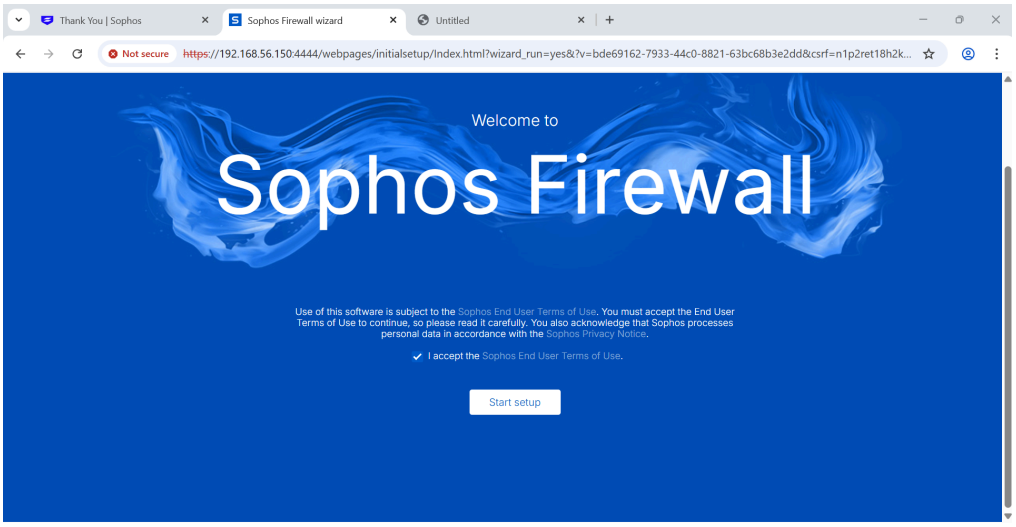
I set the IP address to 192.168.56.160, left the subnet mask as default and disabled IPV6. This activated the firewall on the vm.



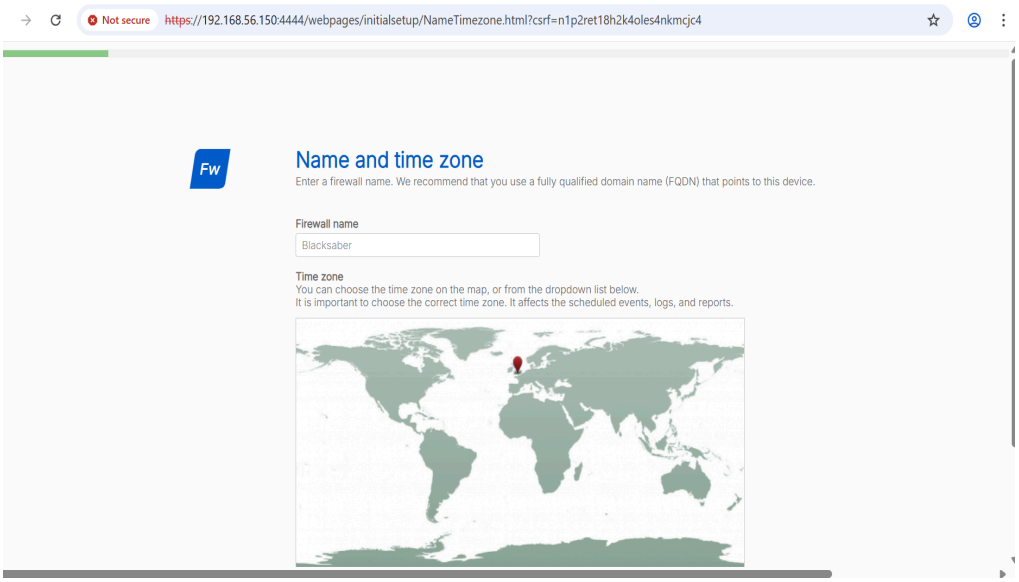
4. Sophos Environment Setup: Minimized the VM and opened Chrome to register for the 30-day free trial of Sophos Firewall. Received a one-time serial number for the VM environment to my email. Accessed the Sophos web interface using the configured IP address: https://192.168.56.160:4444.



After accessing the Sophos Firewall web interface through https://192.168.56.160:4444, I was prompted to start the setup. Once I clicked the prompt, the setup wizard launched.



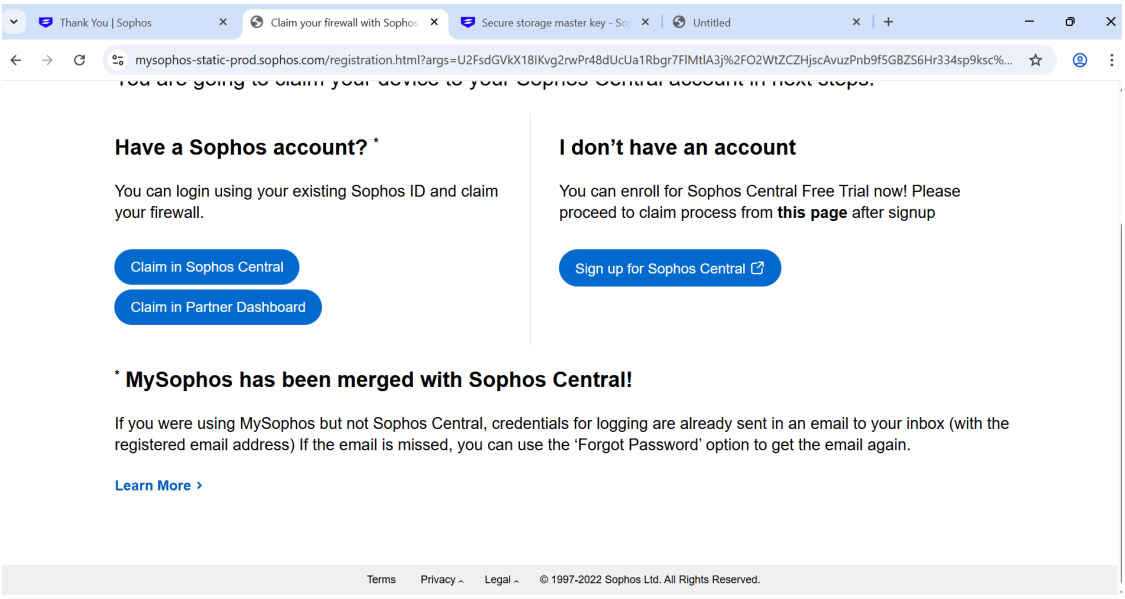
The wizard first required me to create a new administrator password. After that, I was prompted to set a Storage Master Key, which is used for restoring important backup configurations and securing recovery operations.
I proceeded to name the firewall "**BlackSaber**" and selected (Africa/Lagos) as the timezone. The system then requested the one-time serial number that had been sent to my email during registration, which I entered to continue.



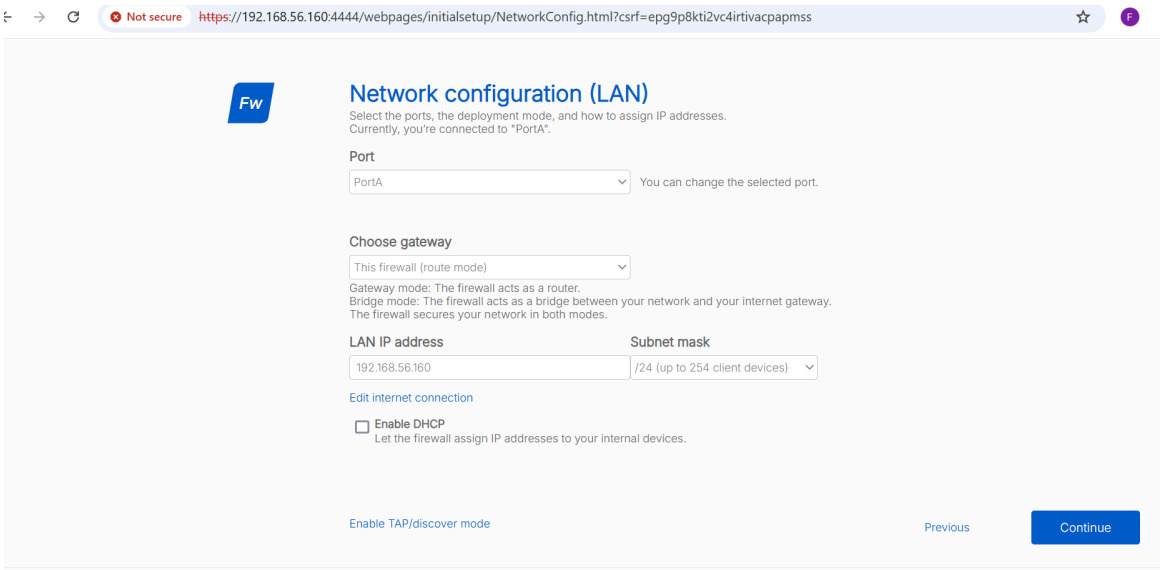
After clicking on continue, I was taken to a page that did not match the steps in the provided PDF guide.

At this stage, I was presented with three options:

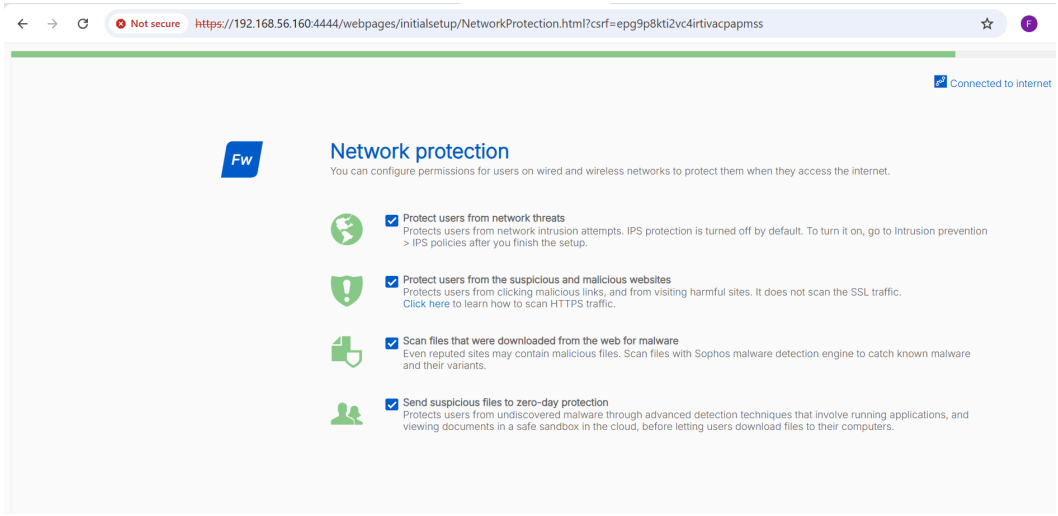
- Claim in Sophos Central
- Claim in Partner Dashboard
- Sign up for Sophos Central (if I did not already have an account)



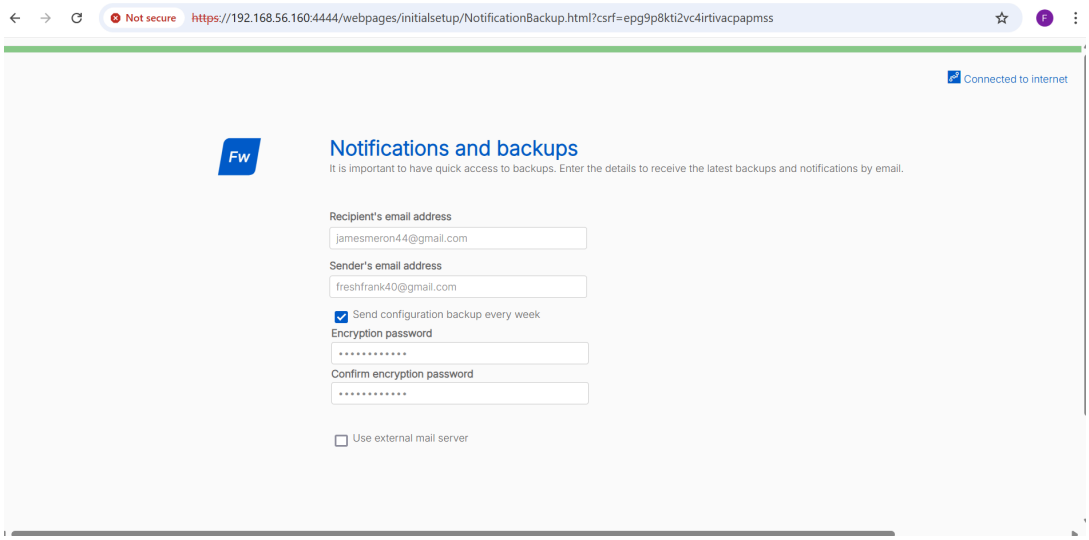
From there, I proceeded to the network configuration section,where I was instructed to disable DHCP before proceeding.



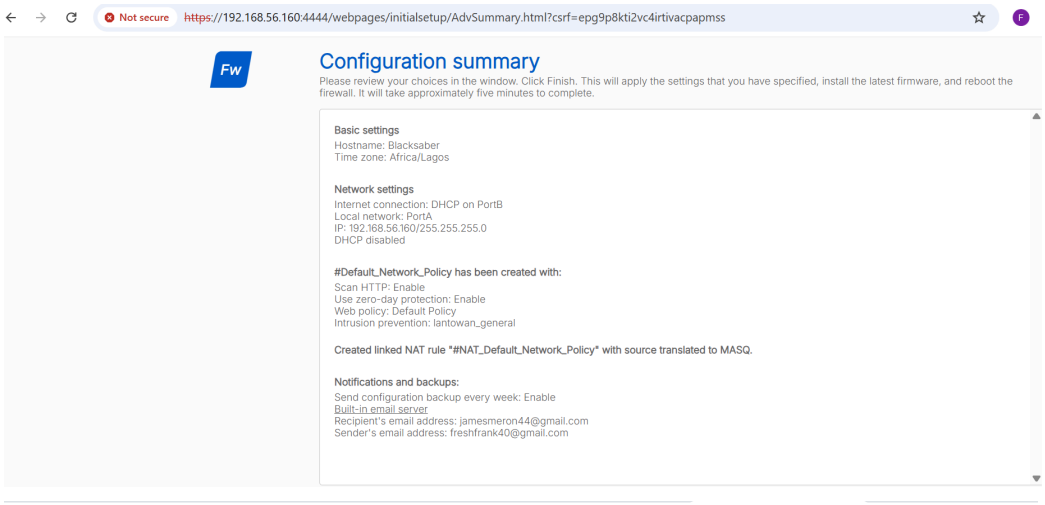
Under the network protection settings, I enabled all available security features to ensure maximum protection.

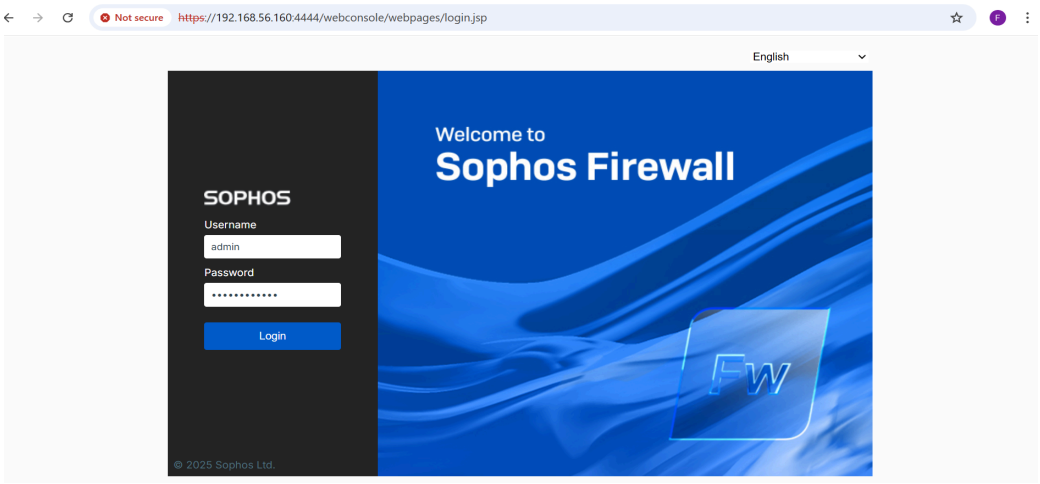


I also configured two email addresses, one as the sender and one as the recipient, for system alerts and notifications. After confirming the settings and entering my password again, I continued.



Once all configurations were completed, the setup wizard finalized the process. When the system finished applying the settings, I successfully logged in using the username admin and the password I created earlier.





POLICY REPORT

1. **Block-HTTP Firewall Rule Implementation on Sophos Firewall:** This report documents the implementation of a security rule on a Sophos Firewall to strengthen web security within the network by blocking all unencrypted HTTP traffic. The goal of the configuration was to enforce secure browsing practices by ensuring that users access only encrypted HTTPS websites.

   I. **Rule Identification**
   - Rule Name: Block-HTTP
   - Rule Type: Firewall Rule
   - Action: Drop
   - Rule Group: None

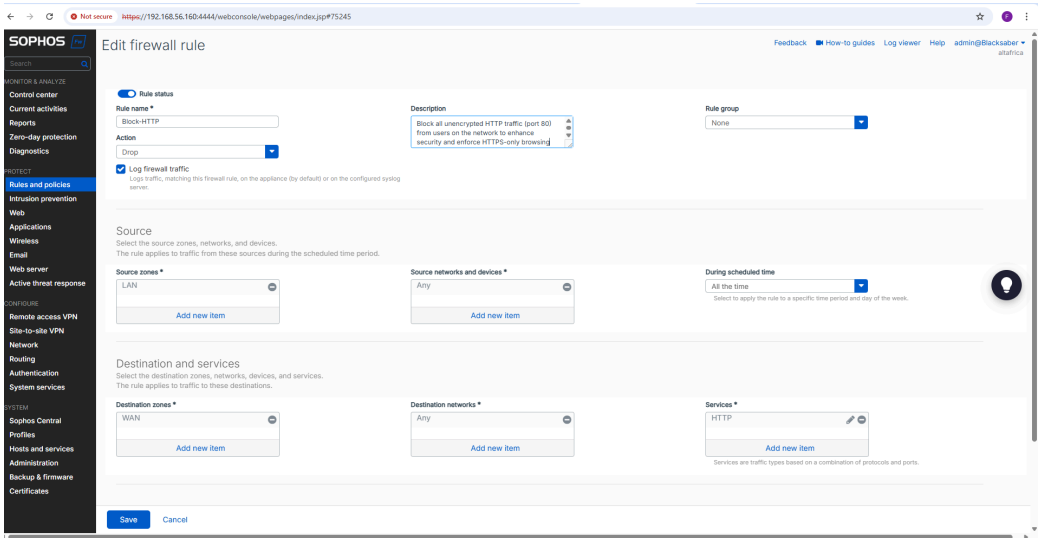
   II. **Objective of the Rule:** The Block-HTTP rule was created to prevent users on the internal network from accessing websites that rely on unsecured HTTP connections. Since HTTP traffic is transmitted in clear text and is vulnerable to interception, blocking it ensures that all outbound web communications occur over encrypted HTTPS channels.

   III. **Configuration Summary**

      I. **Traffic Direction and Zones:**
      - Source Zone: LAN (internal users)
      - Destination Zone: WAN (internet)

      II. **Source and Destination Networks:**
      - Source Network: Any
      - Destination Network: Any

      III. **Service Specification And Scheduled Time:**
      - Service Controlled: HTTP (port 80**)**
      - During Scheduled Time**:** All the time



IV. Security Action

The rule was configured with the following action:

Action: Drop

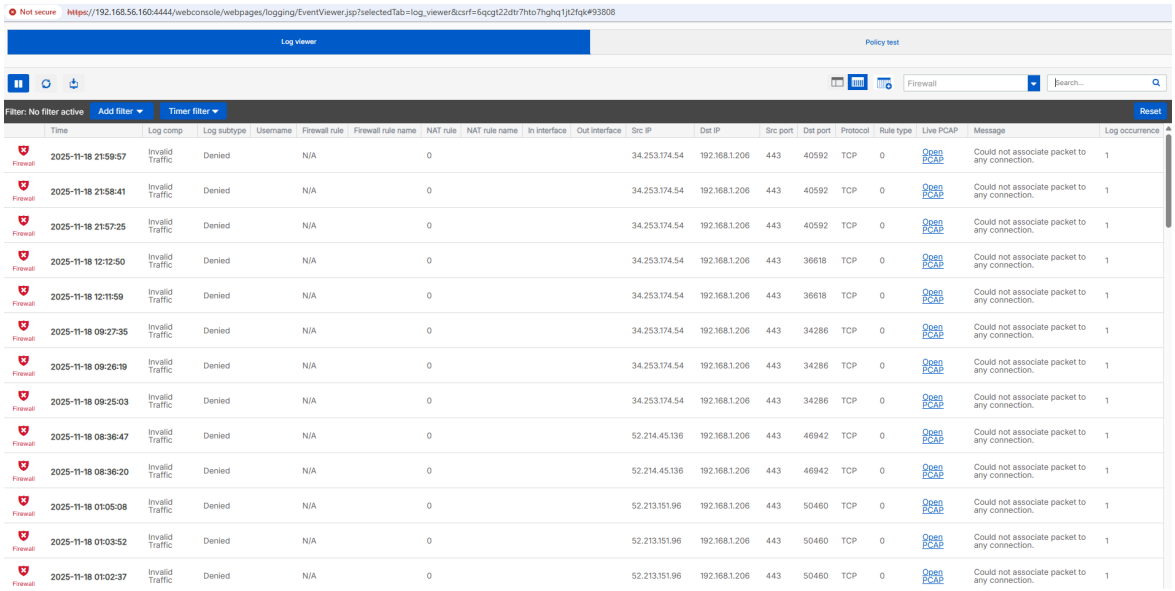
The drop action silently blocks the traffic without sending a rejection response.This choice minimizes unnecessary network noise and is standard for blocking policies.

V. Policy Behavior

Once activated, the Block-HTTP rule successfully prevents all outbound HTTP connections from the internal network. Attempts to access unencrypted websites (HTTP) are denied, while HTTPS websites remain accessible. This ensures that internal network users cannot unknowingly access insecure web pages, thereby reducing exposure to risks such as credential theft, eavesdropping, and man-in-the-middle attacks.

VI. Log and Monitoring Outcome

Firewall logs confirmed that the HTTP connection attempts are dropped by the BlockHTTP rule. The logs show entries indicating denied connections matching the HTTP service on port 80, confirming that the policy is functioning as intended.



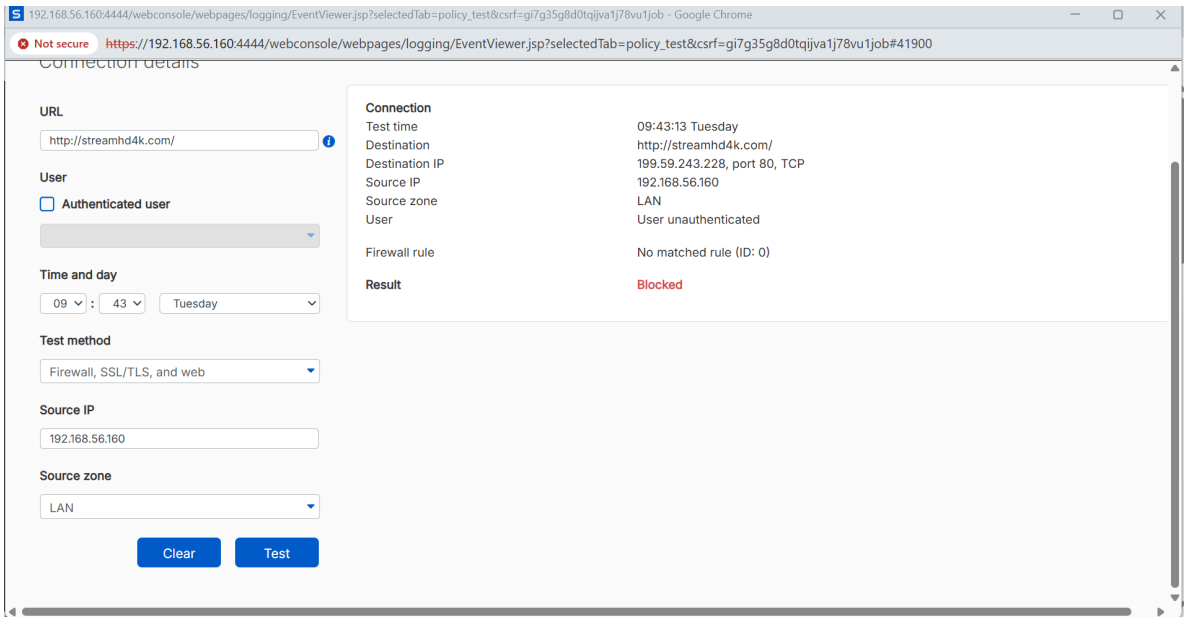
VII. Conclusion

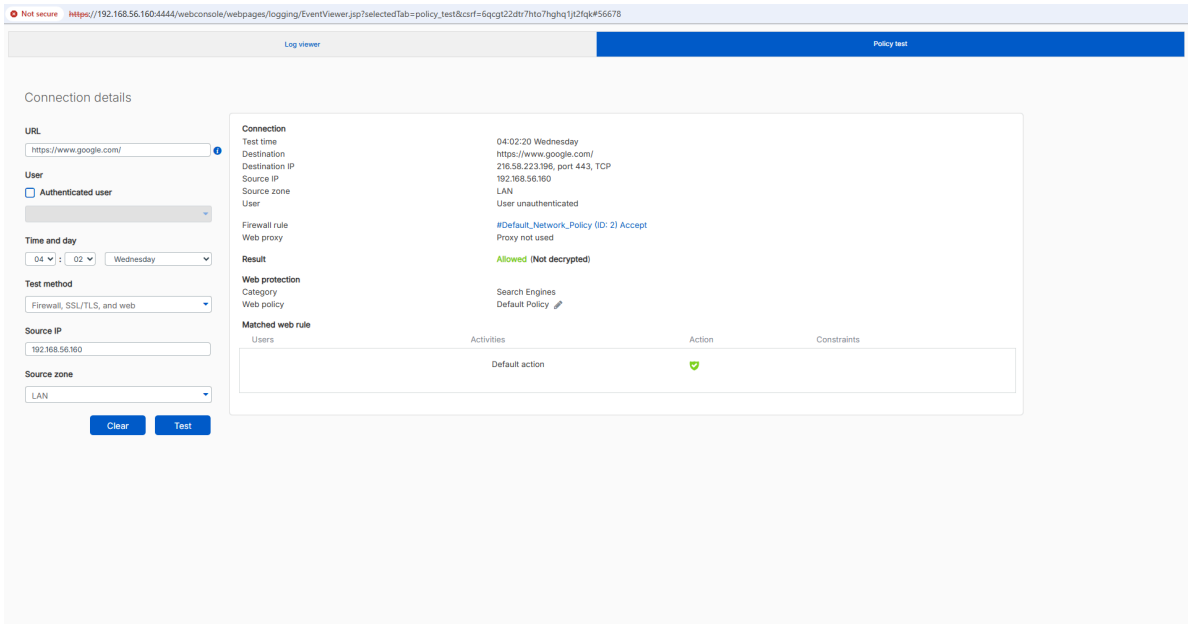
In conclusion, the Sophos Firewall configuration and policy implementation was successful. The custom firewall rule created to block HTTP traffic performed exactly as intended. When I attempted to access an unsecured HTTP website, www.streamhd4k.com, the connection was successfully blocked, demonstrating that the rule was properly enforced.

To further validate the policy behavior, I tested the same rule on a secure HTTPS website, www.google.com. As shown in the results, the connection was allowed, which is expected because HTTPS traffic is encrypted and not subject to the same blocking conditions unless SSL/TLS inspection is enabled. This confirms that the firewall correctly

distinguishes between HTTP and HTTPS traffic and applies the configured rule accurately.

Overall, the test results show that the security policy worked effectively and the Sophos Firewall was able to enforce the desired network control based on the defined rule.





VIII. Side Note / Limitation Observe

During the practical session, I observed that my instance of the Sophos Firewall did not contain all the features demonstrated by the lecturer. Several advanced options and modules available on the lecturer's system were missing on mine. This limitation prevented me from exploring some of the additional functionalities that were showcased during the class demonstration. The difference in available features may be due to variations in licensing or some kind of restrictions.

2. Allow FTP over TLS: This rule was created with the purpose of accepting FTPS traffic (port 990) from the WAN to the LAN, ensuring that only encrypted file-transfer sessions are permitted while all non-secure FTP attempts are denied by default.

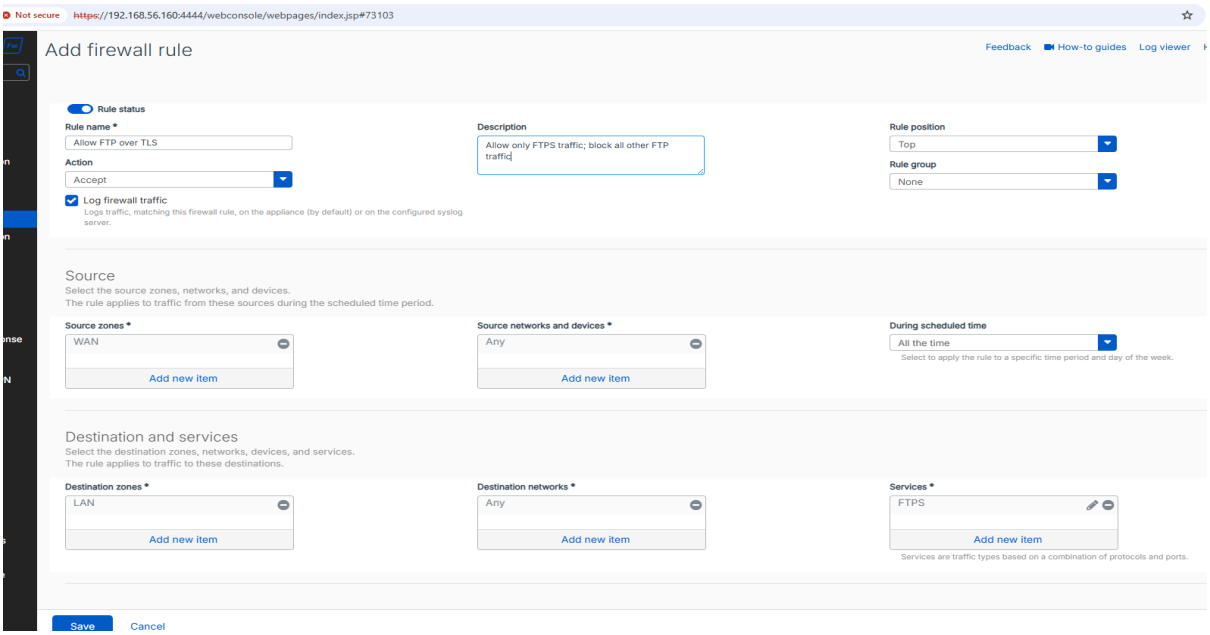
I. Network Setup:

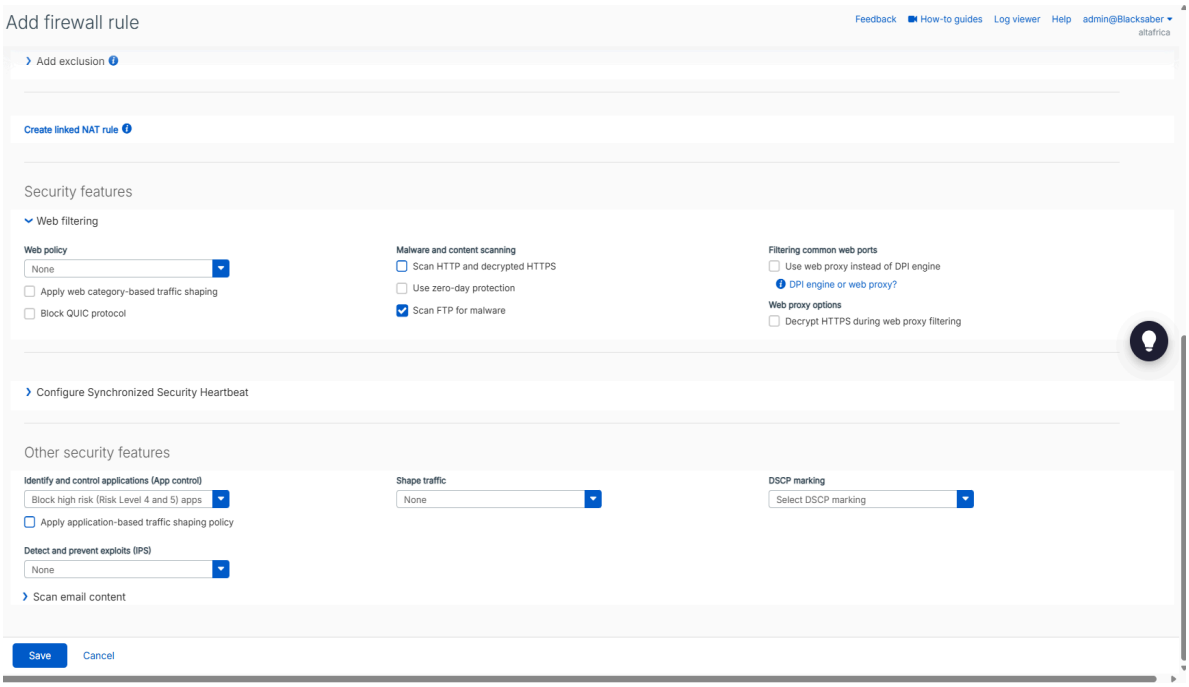
- WAN: Port B / Public IP.
- LAN: Port A / Internal network IP.
- Devices: Firewall, LAN devices, WAN interface.

II. Objective of the rule: To configure firewall rules to allow specific secure traffic (FTPS) while blocking unwanted traffic. And also to test firewall functionality between WAN and LAN interfaces.

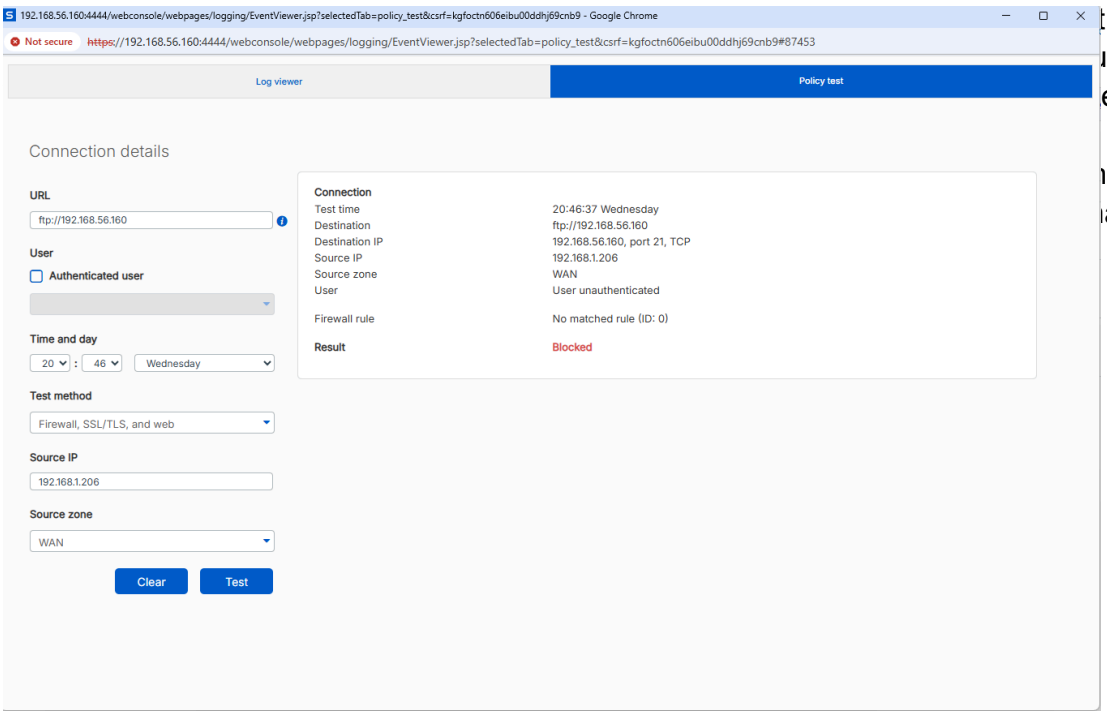
III. Firewall Configuration:

- Rule Name: Allow FTP over TLS
- Rule Implemented: Allow FTPS traffic (TCP port 990) from WAN to LAN.
- Rule Group: None
- Action: Accept.
- Source Zones: WAN
- Source Network and Devices: Any





IV. Policy Behavior:



V. Conclusion:

The FTPS policy was implemented to permit TCP/990 from WAN to LAN. During testing using ftps://<LAN IP>, the firewall test reported the connection as blocked. I learnt this outcome was consistent with the lab limitations (no running FTPS service or active FTPS handshake on the target host), so the blocked result did not necessarily indicate a misconfiguration. To fully validate the rule, I would have to run it in a real environment, deploy a working FTPS server on the LAN host (or simulate a TCP/990 session) and re-run the test; additionally I checked the firewall logs to confirm whether the rule matched or whether packets were dropped for another reason.