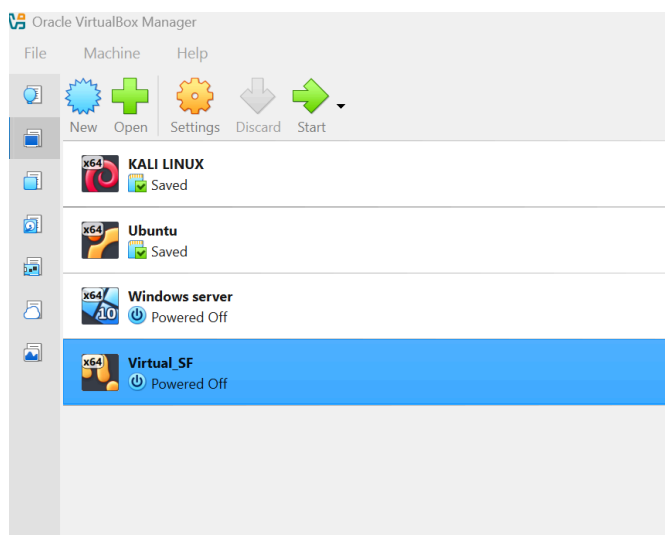
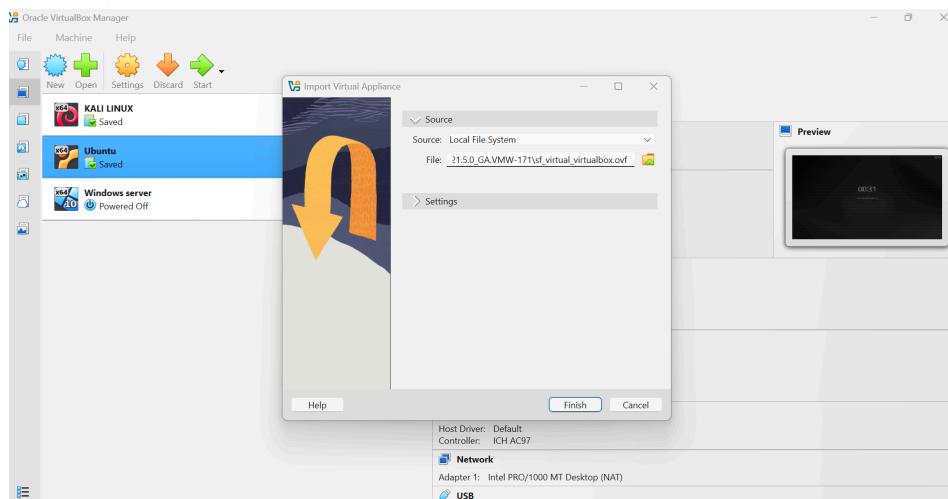
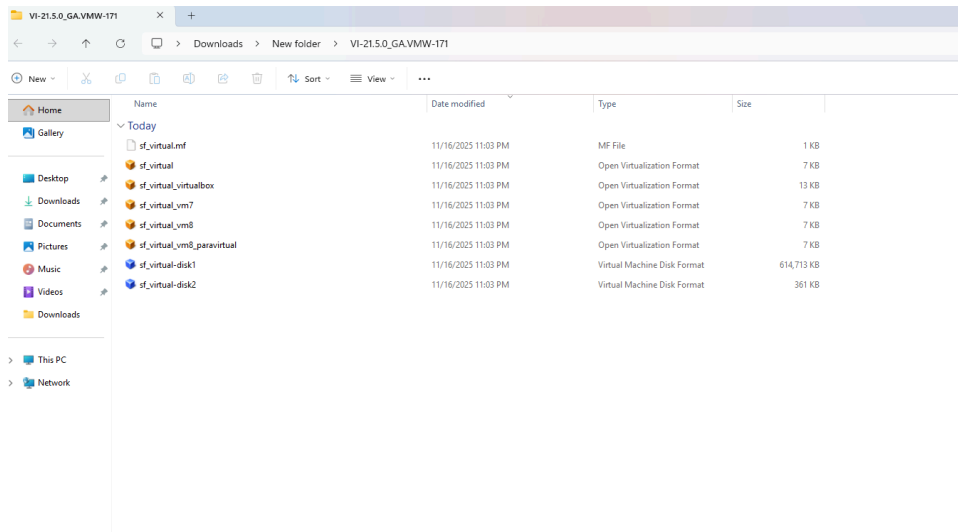
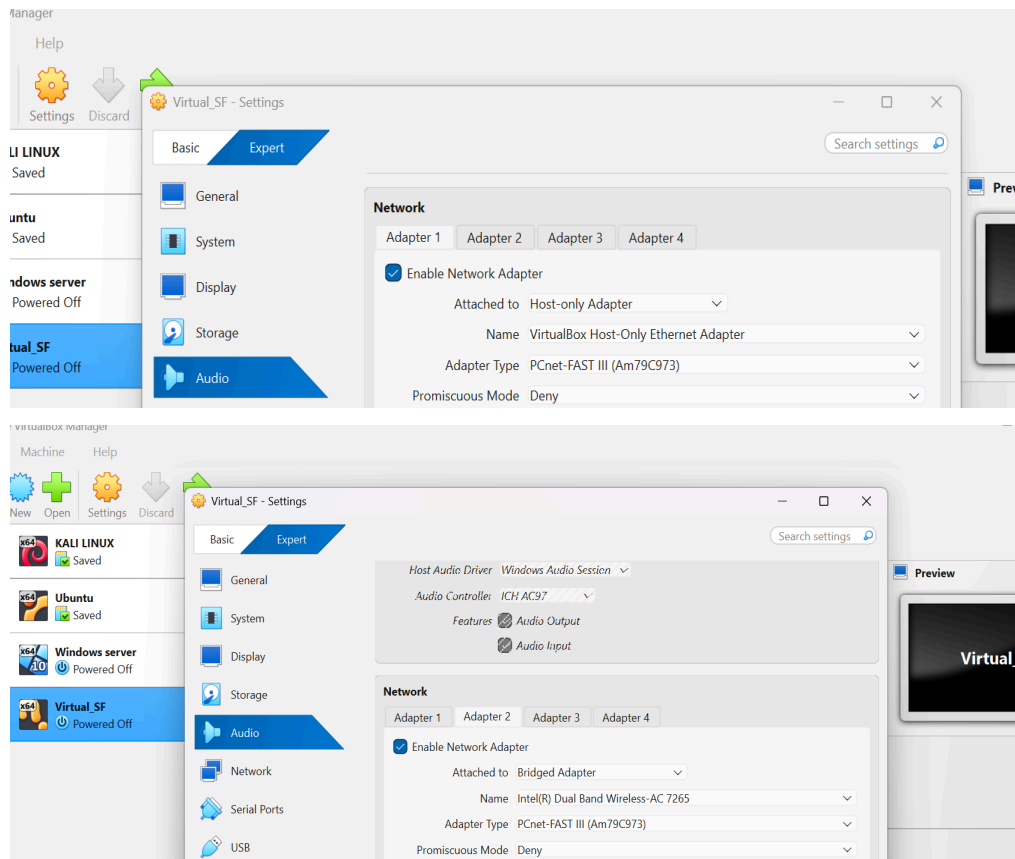


SOPHOS FIREWALL CONFIGURATION LAB REPORT

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”.

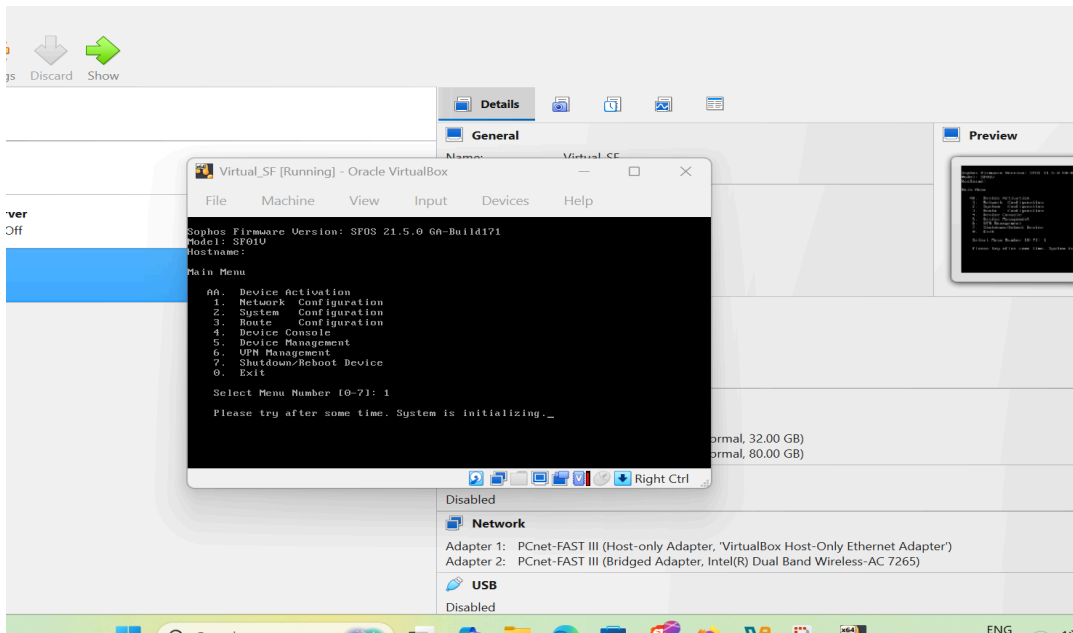


2. **Virtual Machine Network Adapter Configuration:** I configured the network adapters for the firewall VM.
- Adapter 1: Host-Only Adapter.
 - Adapter 2: Bridged Adapter

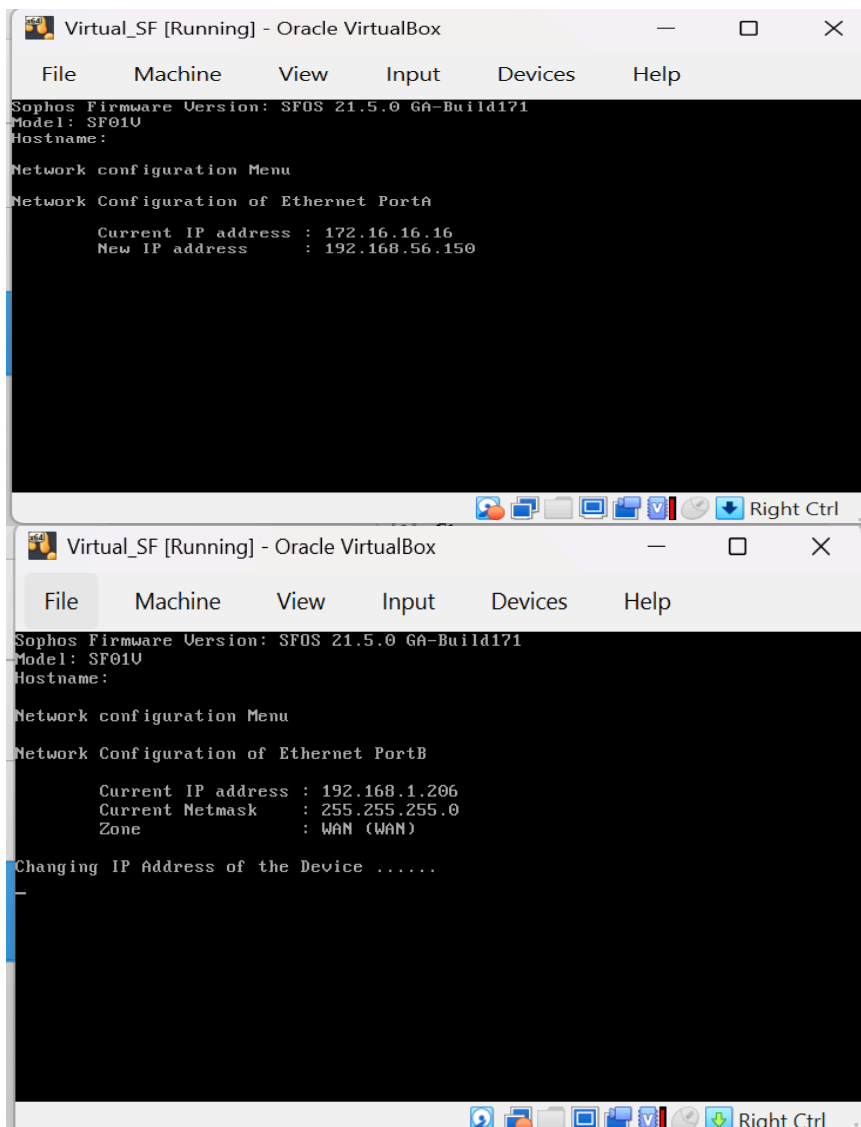


While Adapter 1(Host-Only) allows the SOPHOS Firewall to be configured securely from the host machine. Adapter 2(Bridged) connects the SOPHOS firewall to the network, enabling it to handle network traffic and protect devices.

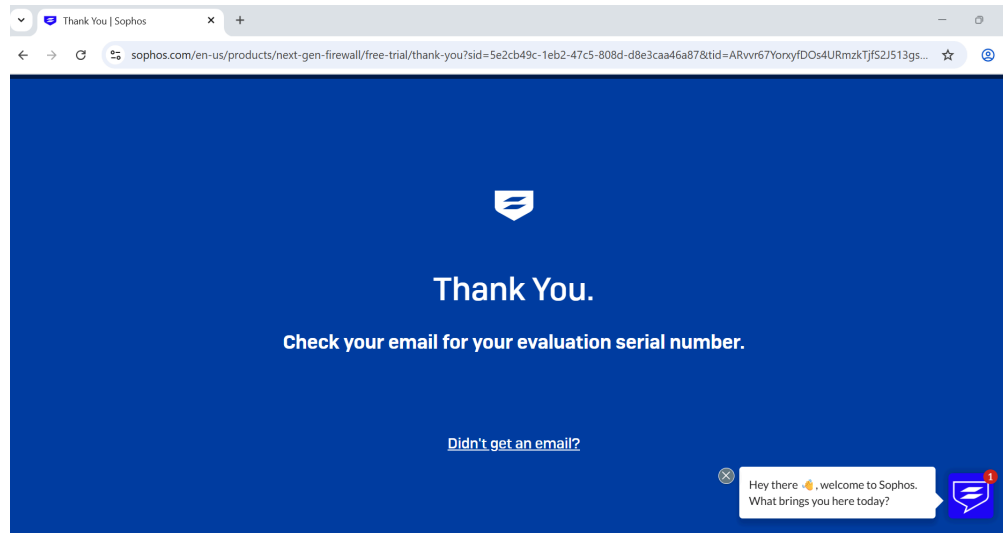
3. Initial firewall launch and configuration: I powered on the SOPHOS virtual firewall on my virtual machine. I was prompted to put in a password which was 'admin' by default. Accepted their licensing agreement by pressing "a". Activated device on Port A by selecting (1) for network configuration. I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



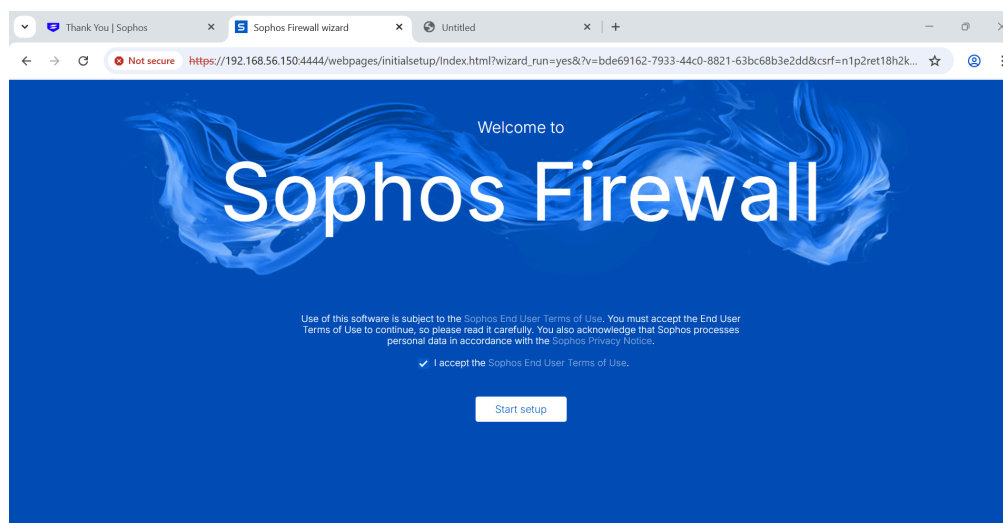
I set the IP address to 192.168.56.160, left the subnet mask as default and disabled IPV6. This activated the firewall on the vm.



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>.

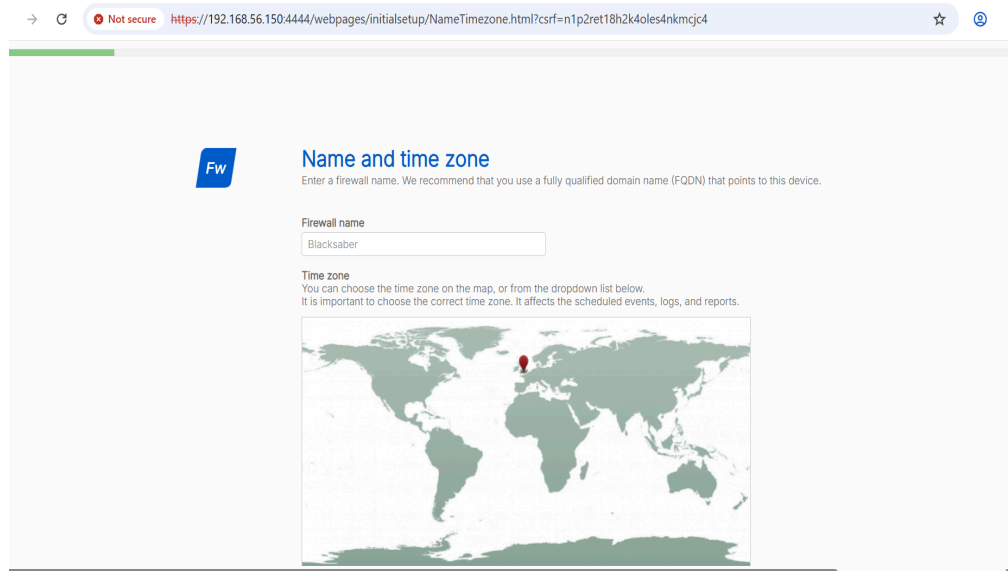


After accessing the Sophos Firewall web interface through <https://192.168.56.160:4444>, I was prompted to start the setup. Once I clicked the prompt, the setup wizard launched.



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.

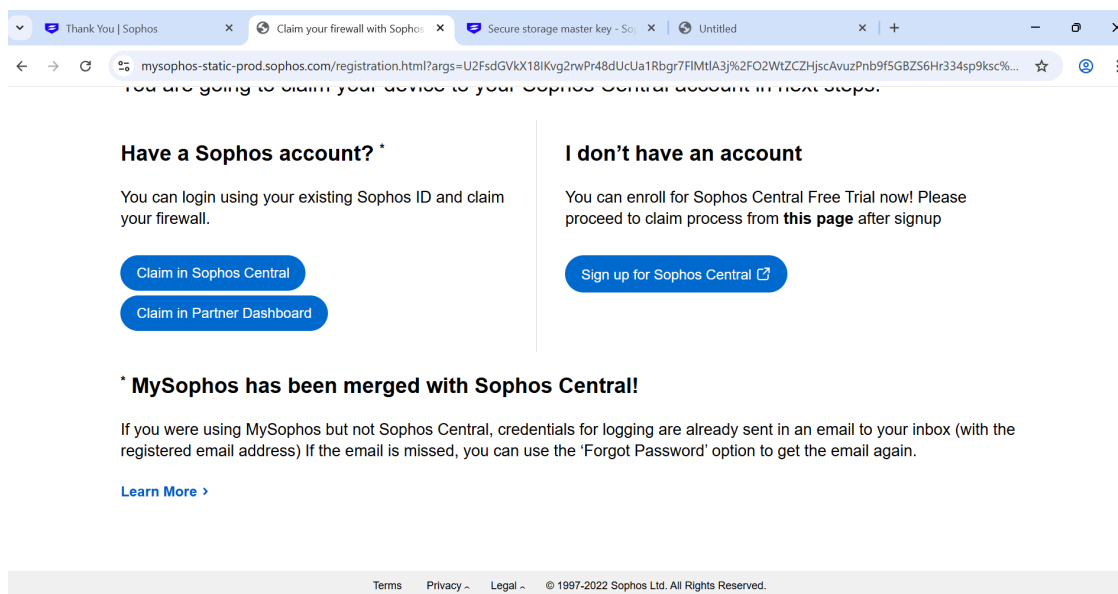
I proceeded to name the firewall "**BlackSaber**" and selected (Africa/Lagos) as the timezone. The system then requested the one-time serial number that had been sent to my email during registration, which I entered to continue.



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.

← → ↻ Not secure https://192.168.56.160:4444/webpages/initialsetup/NetworkConfig.html?csrf=epg9p8kti2vc4irtivacpamss ☆ ⓘ



Network configuration (LAN)

Select the ports, the deployment mode, and how to assign IP addresses.
Currently, you're connected to "PortA".

Port

PortA ▾ You can change the selected port.

Choose gateway

This firewall (route mode) ▾

Gateway mode: The firewall acts as a router.
Bridge mode: The firewall acts as a bridge between your network and your internet gateway.
The firewall secures your network in both modes.

LAN IP address **Subnet mask**

192.168.56.160 /24 (up to 254 client devices) ▾

[Edit internet connection](#)


☐ **Enable DHCP**
Let the firewall assign IP addresses to your internal devices.

[Enable TAP/discover mode](#) [Previous](#) [Continue](#)

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

← → ↻ Not secure https://192.168.56.160:4444/webpages/initialsetup/NetworkProtection.html?csrf=epg9p8kti2vc4irtivacpamss ☆ ⓘ

Connected to internet



Network protection

You can configure permissions for users on wired and wireless networks to protect them when they access the internet.

- ☒ **Protect users from network threats**
Protects users from network intrusion attempts. IPS protection is turned off by default. To turn it on, go to Intrusion prevention > IPS policies after you finish the setup.
- ☒ **Protect users from the suspicious and malicious websites**
Protects users from clicking malicious links, and from visiting harmful sites. It does not scan the SSL traffic.
[Click here to learn how to scan HTTPS traffic.](#)
- ☒ **Scan files that were downloaded from the web for malware**
Even reputed sites may contain malicious files. Scan files with Sophos malware detection engine to catch known malware and their variants.
- ☒ **Send suspicious files to zero-day protection**
Protects users from undiscovered malware through advanced detection techniques that involve running applications, and viewing documents in a safe sandbox in the cloud, before letting users download files to their computers.

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.

← → ↻ Not secure https://192.168.56.160:4444/webpages/initialsetup/NotificationBackup.html?csrf=epg9p8kti2vc4irtivacpamss ☆ ⓘ

Connected to internet

Notifications and backups

It is important to have quick access to backups. Enter the details to receive the latest backups and notifications by email.

Recipient's email address
jamesmeron44@gmail.com

Sender's email address
freshfrank40@gmail.com

☒ Send configuration backup every week

Encryption password

Confirm encryption password

☐ Use external mail server

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.

← → ↻ Not secure https://192.168.56.160:4444/webpages/initialsetup/AdvSummary.html?csrf=epg9p8kti2vc4irtivacpamss ☆ ⓘ

Configuration summary

Please review your choices in the window. Click Finish. This will apply the settings that you have specified, install the latest firmware, and reboot the firewall. It will take approximately five minutes to complete.

Basic settings
Hostname: Blacksaber
Time zone: Africa/Lagos

Network settings
Internet connection: DHCP on PortB
Local network: PortA
IP: 192.168.56.160/255.255.255.0
DHCP disabled

#Default_Network_Policy has been created with:
Scan HTTP: Enable
Use zero-day protection: Enable
Web policy: Default Policy
Intrusion prevention: Iantowan_general

Created linked NAT rule *#NAT_Default_Network_Policy* with source translated to MASQ.

Notifications and backups:
Send configuration backup every week: Enable
Built-in email server
Recipient's email address: jamesmeron44@gmail.com
Sender's email address: freshfrank40@gmail.com

← → ↻ Not secure https://192.168.56.160:4444/webconsole/webpages/login.jsp ☆ ⓘ

English

SOPHOS

Username
admin

Password

Login

© 2025 Sophos Ltd.

Welcome to
Sophos Firewall

Fw

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

The screenshot displays the 'Edit firewall rule' interface in the Sophos Firewall management console. The left sidebar shows the navigation menu with 'Rules and policies' selected. The main configuration area is divided into several sections:

- Rule status:** A toggle switch is turned on.
- Rule name:** 'Block-HTTP' is entered in the text field.
- Description:** 'Block all unencrypted HTTP traffic (port 80) from users on the network to enhance security and enforce HTTPS-only browsing' is shown in a dropdown menu.
- Action:** 'Drop' is selected in the dropdown menu.
- Log firewall traffic:** A checkbox is checked, with a note: 'Log traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.'
- Rule group:** 'None' is selected in the dropdown menu.
- Source:** A section titled 'Select the source zones, networks, and devices. The rule applies to traffic from these sources during the scheduled time period.' containing:
 - Source zones:** 'LAN' is selected.
 - Source networks and devices:** 'Any' is selected.
- During scheduled time:** 'All the time' is selected, with a note: 'Select to apply the rule to a specific time period and day of the week.'
- Destination and services:** A section titled 'Select the destination zones, networks, devices, and services. The rule applies to traffic to these destinations.' containing:
 - Destination zones:** 'WAN' is selected.
 - Destination networks:** 'Any' is selected.
 - Services:** 'HTTP' is selected.

At the bottom, there are 'Save' and 'Cancel' buttons.

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.

Not secure

https://192.168.56.160:4444/webconsole/webpages/logging/eventViewer.jsp?selectedTab=log_viewer&csrf=6qcg122dr7Ho7hghq1j1Ztk#93806

Log viewer

Policy test

Firewall

Search...

Filter: No filter active

Add filter

Timer filter

Reset

	Time	Log comp	Log subtype	Username	Firewall rule	Firewall rule name	NAT rule	NAT rule name	In interface	Out interface	Src IP	Dst IP	Src port	Dst port	Protocol	Rule type	Live PCAP	Message	Log occurrence
<div><div></div><div>Firewall</div></div>	2025-11-18 21:59:57	Invalid Traffic	Denied	N/A		0					34.253.174.54	192.168.1.206	443	40592	TCP	0	Open PCAP	Could not associate packet to any connection.	1
<div><div></div><div>Firewall</div></div>	2025-11-18 21:58:41	Invalid Traffic	Denied	N/A		0					34.253.174.54	192.168.1.206	443	40592	TCP	0	Open PCAP	Could not associate packet to any connection.	1
<div><div></div><div>Firewall</div></div>	2025-11-18 21:57:25	Invalid Traffic	Denied	N/A		0					34.253.174.54	192.168.1.206	443	40592	TCP	0	Open PCAP	Could not associate packet to any connection.	1
<div><div></div><div>Firewall</div></div>	2025-11-18 12:12:50	Invalid Traffic	Denied	N/A		0					34.253.174.54	192.168.1.206	443	36618	TCP	0	Open PCAP	Could not associate packet to any connection.	1
<div><div></div><div>Firewall</div></div>	2025-11-18 12:11:59	Invalid Traffic	Denied	N/A		0					34.253.174.54	192.168.1.206	443	36618	TCP	0	Open PCAP	Could not associate packet to any connection.	1
<div><div></div><div>Firewall</div></div>	2025-11-18 09:27:35	Invalid Traffic	Denied	N/A		0					34.253.174.54	192.168.1.206	443	34286	TCP	0	Open PCAP	Could not associate packet to any connection.	1
<div><div></div><div>Firewall</div></div>	2025-11-18 09:26:19	Invalid Traffic	Denied	N/A		0					34.253.174.54	192.168.1.206	443	34286	TCP	0	Open PCAP	Could not associate packet to any connection.	1
<div><div></div><div>Firewall</div></div>	2025-11-18 09:25:03	Invalid Traffic	Denied	N/A		0					34.253.174.54	192.168.1.206	443	34286	TCP	0	Open PCAP	Could not associate packet to any connection.	1
<div><div></div><div>Firewall</div></div>	2025-11-18 08:36:47	Invalid Traffic	Denied	N/A		0					52.214.45.136	192.168.1.206	443	46942	TCP	0	Open PCAP	Could not associate packet to any connection.	1
<div><div></div><div>Firewall</div></div>	2025-11-18 08:36:20	Invalid Traffic	Denied	N/A		0					52.214.45.136	192.168.1.206	443	46942	TCP	0	Open PCAP	Could not associate packet to any connection.	1
<div><div></div><div>Firewall</div></div>	2025-11-18 01:05:08	Invalid Traffic	Denied	N/A		0					52.213.151.96	192.168.1.206	443	50460	TCP	0	Open PCAP	Could not associate packet to any connection.	1
<div><div></div><div>Firewall</div></div>	2025-11-18 01:03:52	Invalid Traffic	Denied	N/A		0					52.213.151.96	192.168.1.206	443	50460	TCP	0	Open PCAP	Could not associate packet to any connection.	1
<div><div></div><div>Firewall</div></div>	2025-11-18 01:02:37	Invalid Traffic	Denied	N/A		0					52.213.151.96	192.168.1.206	443	50460	TCP	0	Open PCAP	Could not associate packet to any connection.	1

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.

The screenshot shows the 'Event Viewer' page in the Sophos Firewall web console. The 'Connection details' section on the left contains the following configuration:

- URL:**
- User:** ☐ Authenticated user
- Time and day:** 09 : 43 Tuesday
- Test method:** Firewall, SSL/TLS, and web
- Source IP:**
- Source zone:**

Buttons for 'Clear' and 'Test' are at the bottom of the configuration section.

The 'Connection' details on the right show the test results:

Connection	
Test time	09:43:13 Tuesday
Destination	http://streamhd4k.com/
Destination IP	199.59.243.228, port 80, TCP
Source IP	192.168.56.160
Source zone	LAN
User	User unauthenticated
Firewall rule	No matched rule (ID: 0)
Result	Blocked

The screenshot shows the 'Event Viewer' page in the Sophos Firewall web console. The 'Connection details' section on the left contains the following configuration:

- URL:**
- User:** ☐ Authenticated user
- Time and day:** 04 : 02 Wednesday
- Test method:** Firewall, SSL/TLS, and web
- Source IP:**
- Source zone:**

Buttons for 'Clear' and 'Test' are at the bottom of the configuration section.

The 'Connection' details on the right show the test results:

Connection	
Test time	04:02:20 Wednesday
Destination	https://www.google.com/
Destination IP	216.58.223.196, port 443, TCP
Source IP	192.168.56.160
Source zone	LAN
User	User unauthenticated
Firewall rule	#Default_Network_Policy (ID: 2) Accept
Web proxy	Proxy not used
Result	Allowed (Not decrypted)

Below the connection details, the 'Web protection' section shows:

- Category:** Search Engines
- Web policy:** Default Policy

The 'Matched web rule' table shows the following entry:

Users	Activities	Action	Constraints
	Default action	✓	

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

The screenshot displays the 'Add firewall rule' interface in the Sophos Firewall web console. The browser address bar shows a URL starting with 'https://192.168.56.160:4444/webconsole/webpages/index.jsp#73103'. The page title is 'Add firewall rule'. The configuration is as follows:

- Rule status:** Enabled (toggle switch).
- Rule name:** Allow FTP over TLS.
- Description:** Allow only FTPS traffic; block all other FTP traffic.
- Action:** Accept.
- Log firewall traffic:** Checked (checkbox). Subtext: Logs traffic matching this firewall rule, on the appliance (by default) or on the configured syslog server.
- Rule position:** Top (dropdown menu).
- Rule group:** None (dropdown menu).
- Source:**
 - Source zones:** WAN (dropdown menu).
 - Source networks and devices:** Any (dropdown menu).
- Destination and services:**
 - Destination zones:** LAN (dropdown menu).
 - Destination networks:** Any (dropdown menu).
 - Services:** FTPS (dropdown menu).
- During scheduled time:** All the time (dropdown menu).

At the bottom, there are 'Save' and 'Cancel' buttons.

Add firewall rule

Feedback [How-to guides](#) [Log viewer](#) [Help](#) [admin@Blacksaber](#) [altafica](#)

[Add exclusion](#)

[Create linked NAT rule](#)

Security features

Web filtering
Web policy
None
☐ Apply web category-based traffic shaping
☐ Block QUIC protocol

Malware and content scanning
☐ Scan HTTP and decrypted HTTPS
☐ Use zero-day protection
☒ Scan FTP for malware

Filtering common web ports
☐ Use web proxy instead of DPI engine
[DPI engine or web proxy?](#)
Web proxy options
☐ Decrypt HTTPS during web proxy filtering

[Configure Synchronized Security Heartbeat](#)

Other security features

Identify and control applications (App control)
☐ Block high risk (Risk Level 4 and 5) apps
☐ Apply application-based traffic shaping policy

Shape traffic
None

DSCP marking
Select DSCP marking

Detect and prevent exploits (IPS)
None

[Scan email content](#)

Save

Cancel

IV. Policy Behavior:

192.168.56.160/webconsole/webpages/logging/EventViewer.jsp?selectedTab=policy_test&csrf=kgfoctn606eibu00ddhj69c9b9 - Google Chrome

Not secure https://192.168.56.160/webconsole/webpages/logging/EventViewer.jsp?selectedTab=policy_test&csrf=kgfoctn606eibu00ddhj69c9b9#87453

Log viewer

Policy test

Connection details

URL
ftp://192.168.56.160

User
☐ Authenticated user

Time and day
20 : 46 Wednesday

Test method
Firewall, SSL/TLS, and web

Source IP
192.168.1.206

Source zone
WAN

Clear

Test

Connection
Test time
Destination
Destination IP
Source IP
Source zone
User
Firewall rule

20:46:37 Wednesday
ftp://192.168.56.160
192.168.56.160, port 21, TCP
192.168.1.206
WAN
User unauthenticated
No matched rule (ID: 0)

Result
Blocked

ult.
es it
his
al

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.