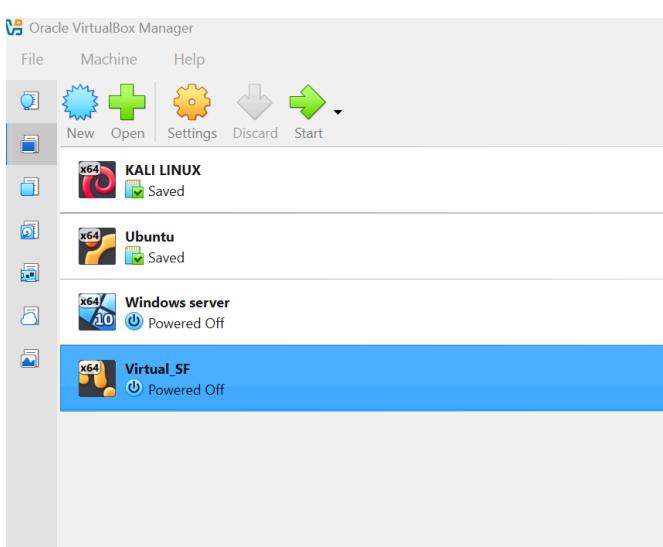
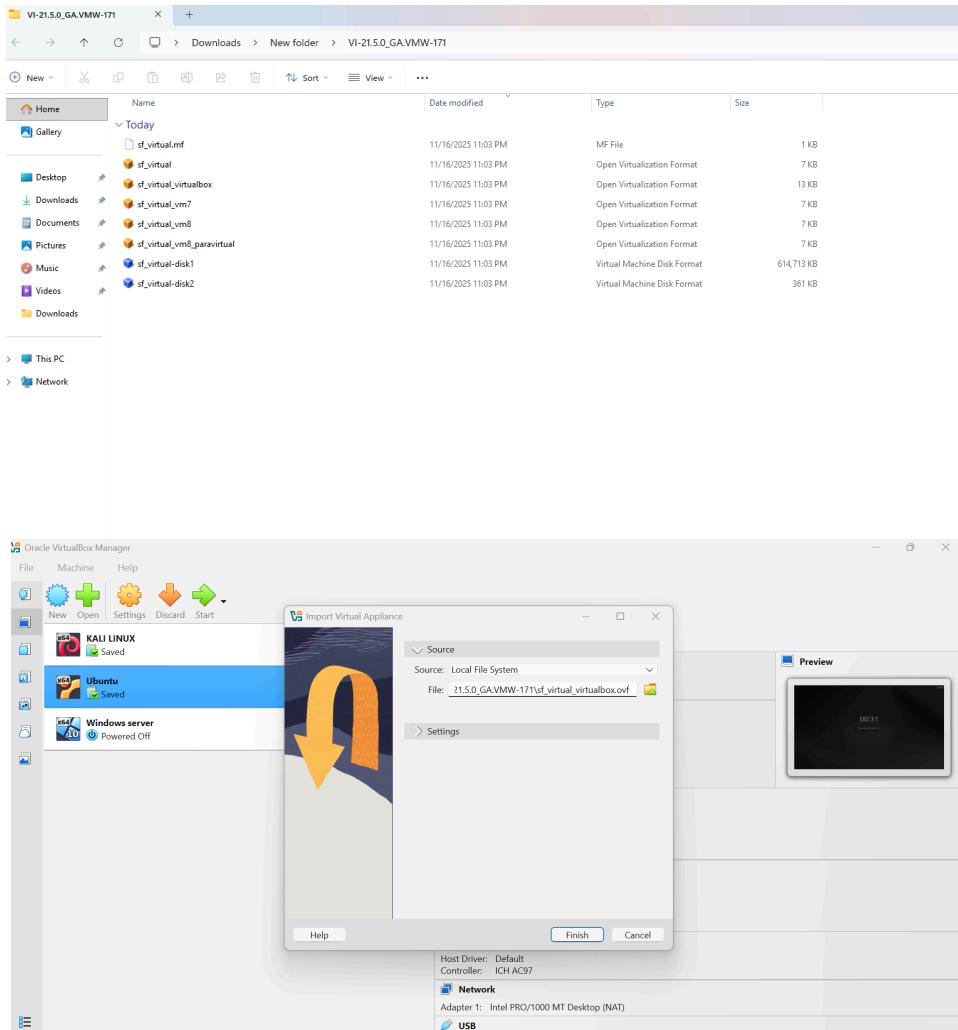


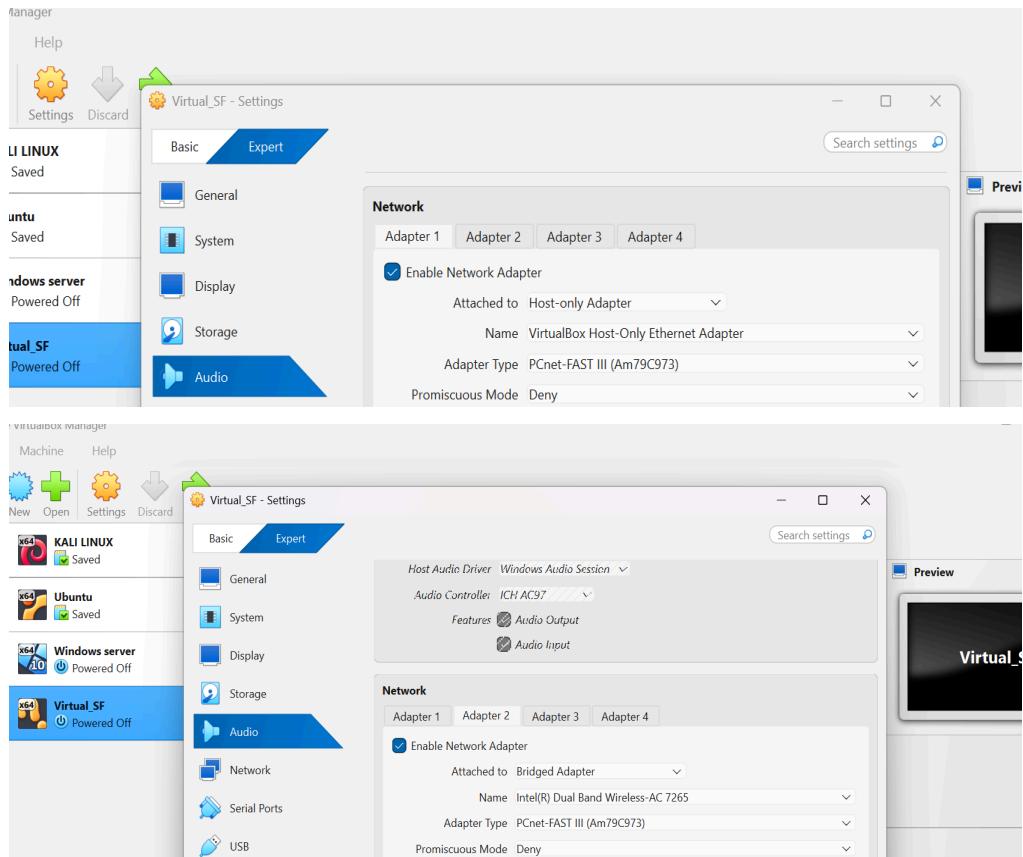
SOPHOS FIREWALL CONFIGURATION LAB REPORT

- 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.

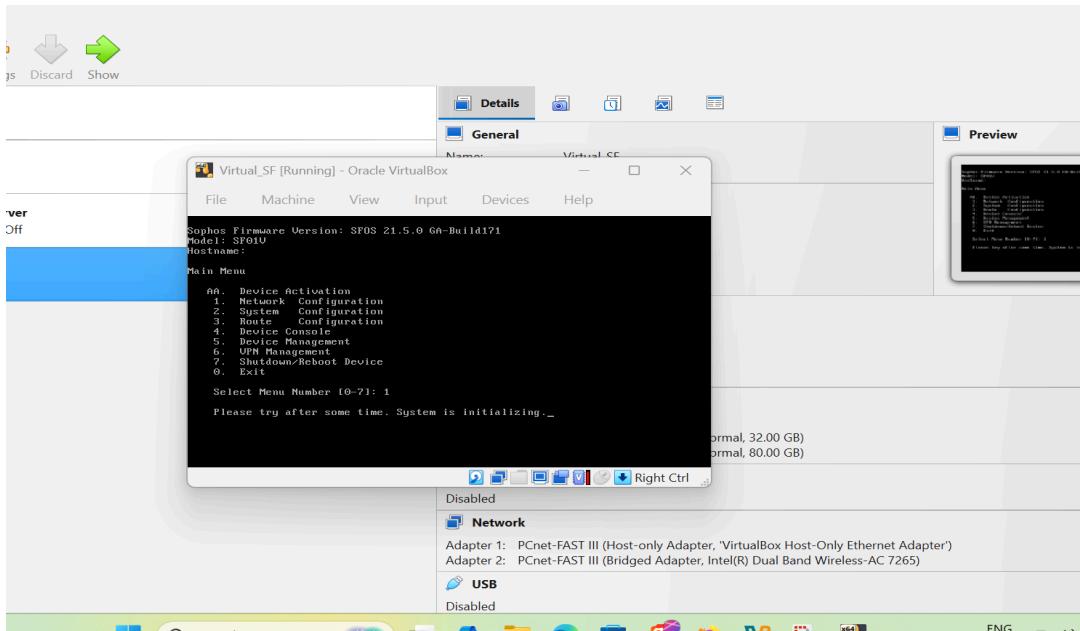
- a. Adapter 1: Host-Only Adapter.
- b. Adapter 2: Bridged Adapter



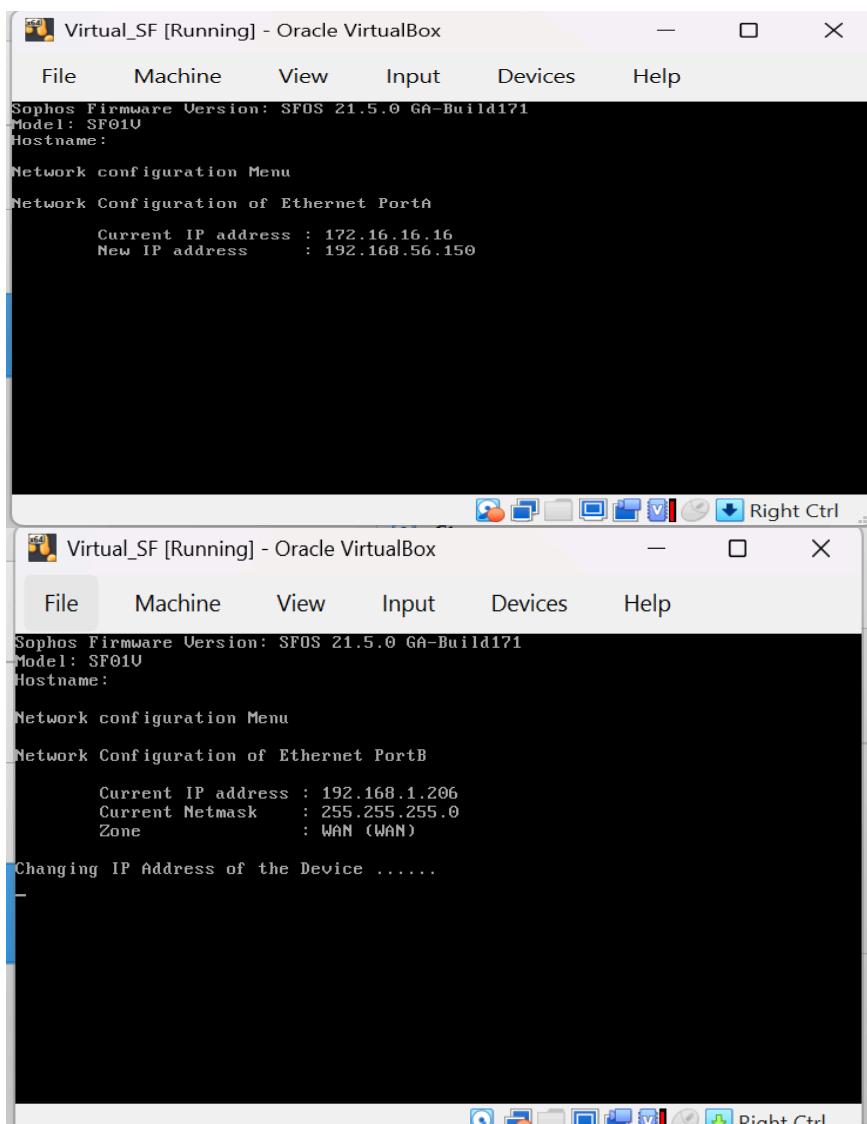
While Adapter 1(Host-Only) allows the SOPHOS Firewall to be configured securely from the host machine. Adapter 2(Bridged) connects the SOPHOS firewall to the network, enabling it to handle network traffic and protect devices.

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".

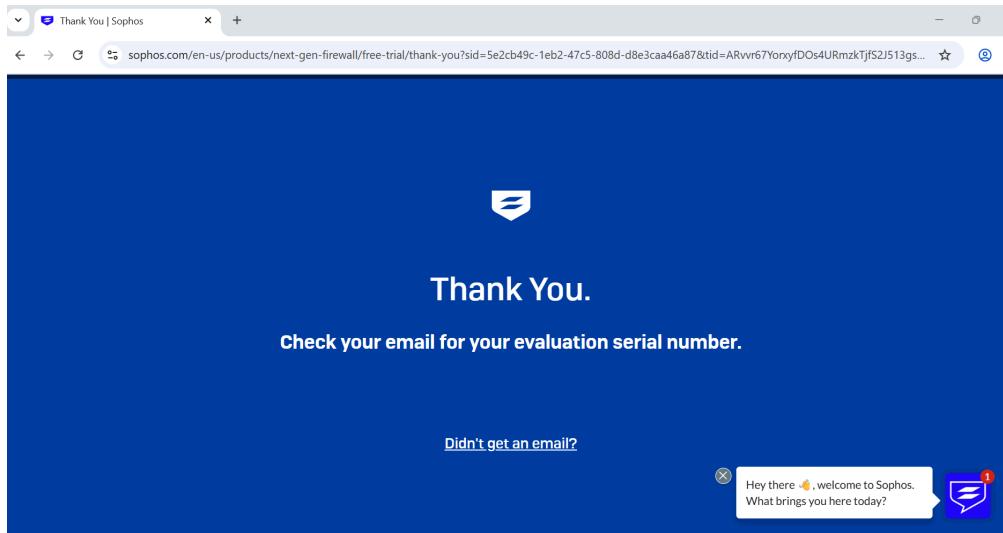
Activated device on Port A by selecting (1) for network configuration. I then chose interface Configuration by clicking (1) on the network configuration menu.



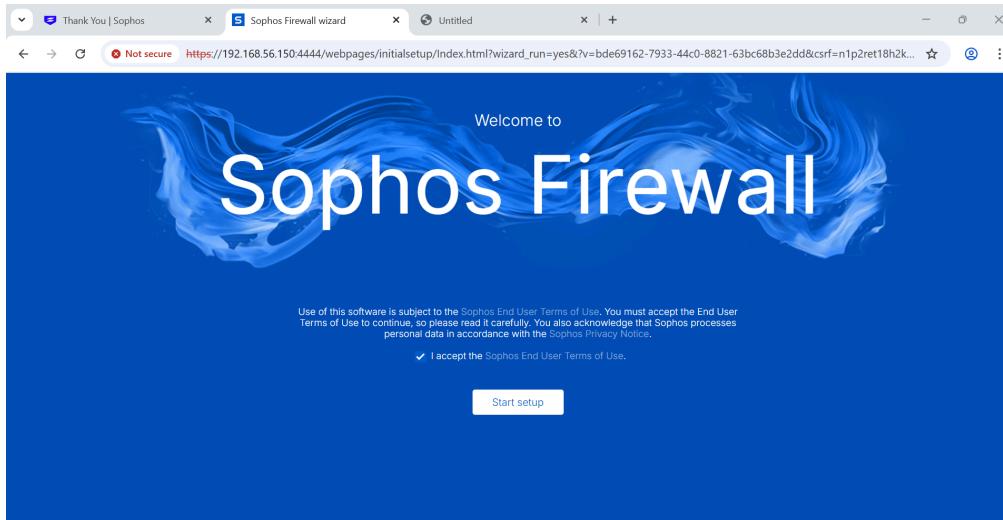
I set the IP address to 192.168.56.160, left the subnet mask as default and disabled IPV6. This activated the firewall on the vm.



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>.

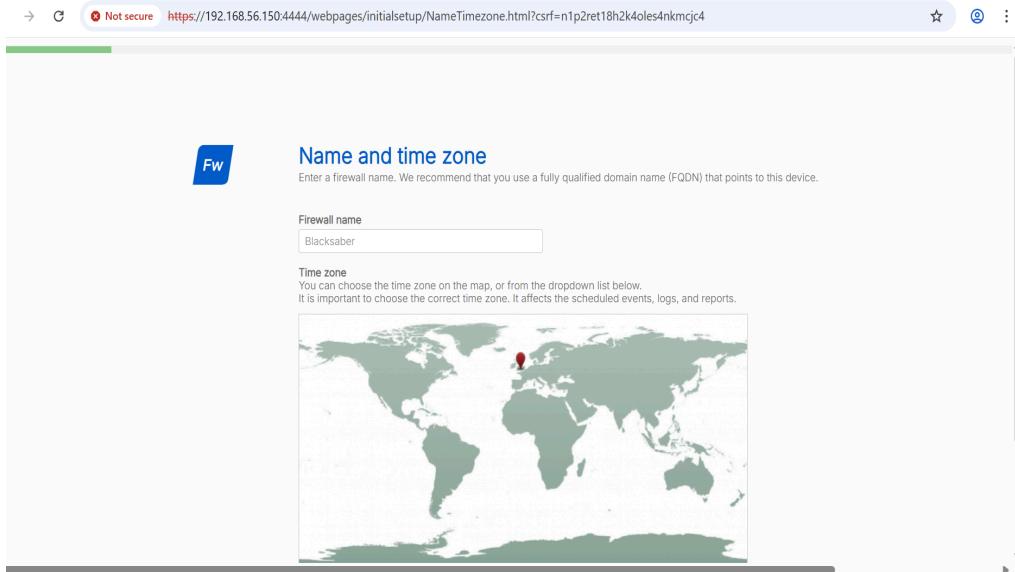


After accessing the Sophos Firewall web interface through <https://192.168.56.160:4444>, I was prompted to start the setup. Once I clicked the prompt, the setup wizard launched.



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)

A screenshot of a web browser showing the Sophos Central registration page at mysophos-static-prod.sophos.com/registration.html?args=U2FsdGVkX18IKvg2rwPr48dUcUa1Rbgr7FIMtlA3j%2FO2WtZCZHjscAvuzPnb9f5GBZS6Hr334sp9ksc%. The page has two main sections: 'Have a Sophos account?*' and 'I don't have an account'. The 'Have a Sophos account?' section contains the text 'You can login using your existing Sophos ID and claim your firewall.' and two buttons: 'Claim in Sophos Central' and 'Claim in Partner Dashboard'. The 'I don't have an account' section contains the text 'You can enroll for Sophos Central Free Trial now! Please proceed to claim process from [this page](#) after signup' and a button 'Sign up for Sophos Central'. At the bottom of the page, there is a note: '* MySophos has been merged with Sophos Central! If you were using MySophos but not Sophos Central, credentials for logging are already sent in an email to your inbox (with the registered email address). If the email is missed, you can use the 'Forgot Password' option to get the email again.' and a link 'Learn More >'. The footer of the page includes links to 'Terms', 'Privacy', 'Legal', and a copyright notice: '© 1997-2022 Sophos Ltd. All Rights Reserved.'

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

The screenshot shows the 'Network configuration (LAN)' page. At the top, it says 'Select the ports, the deployment mode, and how to assign IP addresses. Currently, you're connected to "PortA".' A dropdown menu for 'Port' shows 'PortA' is selected. Below this, there's a section titled 'Choose gateway' with a dropdown set to 'This firewall (route mode)'. A note explains: '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.' Under 'LAN IP address', the input field contains '192.168.56.160' and the subnet mask is set to '/24 (up to 254 client devices)'. There's also an 'Edit internet connection' link and a checkbox for 'Enable DHCP' which is unchecked. At the bottom, there are links for 'Enable TAP/discover mode', 'Previous', and a large blue 'Continue' button.

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

The screenshot shows the 'Network protection' page. It says 'You can configure permissions for users on wired and wireless networks to protect them when they access the internet.' There are four checked options: 1. 'Protect users from network threats' (protects from network intrusion attempts, IPS protection is turned off by default). 2. 'Protect users from the suspicious and malicious websites' (protects from clicking malicious links and visiting harmful sites, does not scan SSL traffic). 3. 'Scan files that were downloaded from the web for malware' (even reputed sites may contain malicious files, uses Sophos malware detection engine). 4. 'Send suspicious files to zero-day protection' (protects users from undiscovered malware through advanced detection techniques). A note says: '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.' At the top right, it says 'Connected to internet'.

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=epg9p8kti2vc4irtivacpapmss

Connected to internet

Fw 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=epg9p8kti2vc4irtivacpapmss

Fw 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: lanitowan_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

Welcome to
Sophos Firewall

English

SOPHOS

Username
admin

Password

Login

© 2025 Sophos Ltd.

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 shows the Sophos Firewall's 'Edit firewall rule' interface. The left sidebar navigation includes 'Control center', 'Reports', 'Diagnostics', 'PROTECT', 'Rules and policies' (which is selected), 'Intrusion prevention', 'Web', 'Applications', 'Email', 'Web server', 'Active threat response', 'CONFIDE', 'Remote access VPN', 'Site-to-site VPN', 'Network', 'Routing', 'Authentication', 'System services', 'SYSTEM', 'Sophos Central', 'Profiles', 'Hosts and services', 'Administration', 'Backup & Firmware', and 'Certificates'. The main content area has tabs for 'Rule status', 'Action', 'Description', 'Log firewall traffic', 'Source', 'Destination zones', and 'Services'. The 'Rule name' is 'Block-HTTP', 'Action' is 'Drop', and 'Description' is 'Block all unencrypted HTTP traffic (port 80) from users on the network, to enhance security and enforce HTTPS-only browsing'. Under 'Source', 'Source zones' is 'LAN' and 'Source networks and devices' is 'Any'. Under 'Destination zones', 'Destination networks' is 'Any' and 'Services' is 'HTTP'. A note at the bottom states 'Services are traffic types based on a combination of protocols and ports.' At the bottom left 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.

Log viewer														Policy test					
														Search...					
Filter: No filter active		Add filter ▾		Timer filter ▾		Firewall										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	
2025-11-18 21:59:57	Not secure	https://192.168.160.4444/webconsole/webpages/logging/EventViewer.jsp?selectedTab=log_viewer&ccsr=6qcg12dtr7hto7hgh1j12fqk#93808		Firewall		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
2025-11-18 21:58:41				Firewall		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
2025-11-18 21:57:25				Firewall		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
2025-11-18 21:12:50				Firewall		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
2025-11-18 12:11:58				Firewall		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
2025-11-18 09:27:35				Firewall		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
2025-11-18 09:26:19				Firewall		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
2025-11-18 09:25:03				Firewall		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
2025-11-18 08:36:47				Firewall		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
2025-11-18 08:36:20				Firewall		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
2025-11-18 01:05:08				Firewall		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
2025-11-18 01:03:52				Firewall		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
2025-11-18 01:02:37				Firewall		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 a connection test configuration in the Sophos Firewall's web console. The URL is set to <http://streamhd4k.com/>. The user is selected as "Authenticated user". The time and day are set to 09:43 on Tuesday. The test method is set to "Firewall, SSL/TLS, and web". The source IP is 192.168.56.160 and the source zone is LAN. The connection details on the right show the test time as 09:43:13 Tuesday, destination as <http://streamhd4k.com/>, destination IP as 199.59.243.228, port 80, TCP, source IP as 192.168.56.160, source zone as LAN, and user as User unauthenticated. The firewall rule is listed as "No matched rule (ID: 0)" and the result is "Blocked".

The screenshot shows a connection test configuration in the Sophos Firewall's web console. The URL is set to <https://www.google.com/>. The user is selected as "Authenticated user". The time and day are set to 04:02 on Wednesday. The test method is set to "Firewall, SSL/TLS, and web". The source IP is 192.168.56.160 and the source zone is LAN. The connection details on the right show the test time as 04:02:20 Wednesday, destination as <https://www.google.com/>, destination IP as 216.58.223.196, port 443, TCP, source IP as 192.168.56.160, source zone as LAN, and user as User unauthenticated. The firewall rule is listed as "[IDefault_Network_Policy](#) (ID: 2) Accept" and the proxy is noted as "Proxy not used". The result is "Allowed (Not decrypted)". The "Matched web rule" section shows a single row for "Default action" with an "Activities" column containing "Search Engines" and "Default Policy".

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 shows the 'Add firewall rule' configuration interface on a Sophos Firewall web console. The URL is https://192.168.56.160:4444/webconsole/webpages/index.jsp#73103. The page has a header with 'Not secure' and the URL. It includes links for 'Feedback', 'How-to guides', and 'Log viewer'. The main form fields are as follows:

- Rule status:** Enabled (radio button selected).
- Rule name ***: Allow FTP over TLS.
- Action**: Accept (selected from a dropdown).
- Description**: Allow only FTPS traffic; block all other FTP traffic.
- Rule position**: Top (selected from a dropdown).
- Rule group**: None (selected from a dropdown).
- Log firewall traffic**: Checked (checkbox selected). Description: Logs traffic matching this rule to the appliance or syslog server.
- Source**:
 - Source zones ***: WAN (selected from a dropdown).
 - Source networks and devices ***: Any (selected from a dropdown).
 - During scheduled time**: All the time (selected from a dropdown). Description: Select to apply the rule to a specific time period and day of the week.
- Destination and services**:
 - Destination zones ***: LAN (selected from a dropdown).
 - Destination networks ***: Any (selected from a dropdown).
 - Services ***: FTPS (selected from a dropdown). Description: Services are traffic types based on a combination of protocols and ports.
- Buttons**: Save (blue button), Cancel.

Add firewall rule

Feedback How-to guides Log viewer Help admin@Blacksaber alafrica

[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:

192.168.56.160:4444/webconsole/webpages/logging/EventViewer.jsp?selectedTab=pol... - Google Chrome

Not secure https://192.168.56.160:4444/webconsole/webpages/logging/EventViewer.jsp?selectedTab=pol...#87453

Log viewer Policy test

Connection details

URL	192.168.56.160	Connection	Test time: 20:46:37 Wednesday Destination: ftp://192.168.56.160 Destination IP: 192.168.56.160, port 21, TCP Source IP: 192.168.1.206 Source zone: WAN User: User unauthenticated
User	<input type="checkbox"/> Authenticated user	Firewall rule	No matched rule (ID: 0)
Time and day	20 : 46 : Wednesday	Result	Blocked
Test method	Firewall, SSL/TLS, and web		
Source IP	192.168.1.206		
Source zone	WAN		
	Clear	Test	

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.