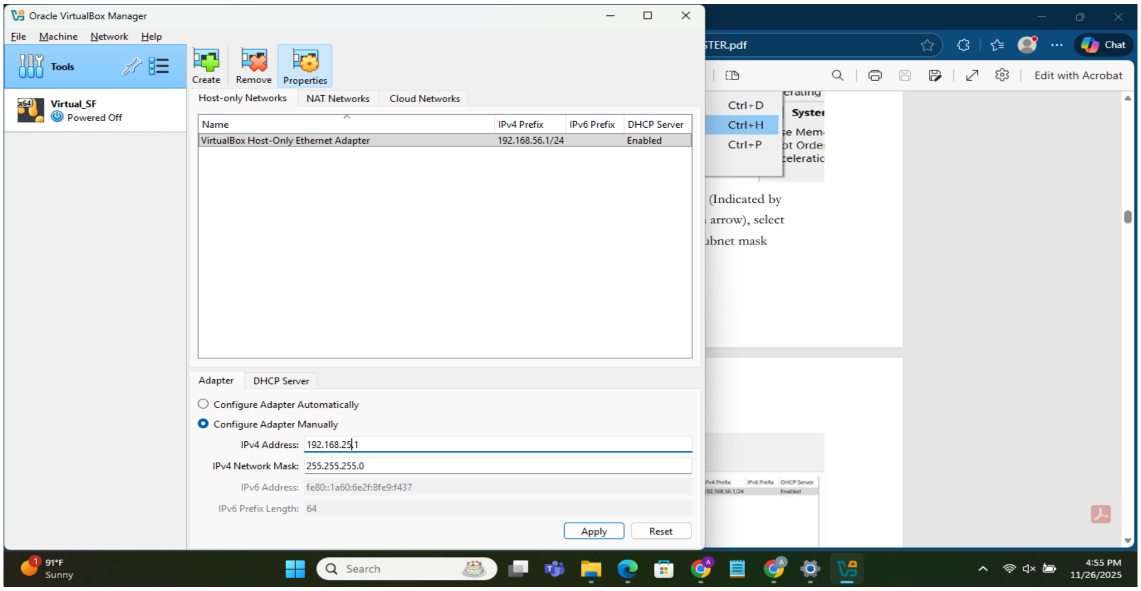
SOPHOS FIREWALL INTALLATION AND CONFIGURATION USING VIRTUALBOX.

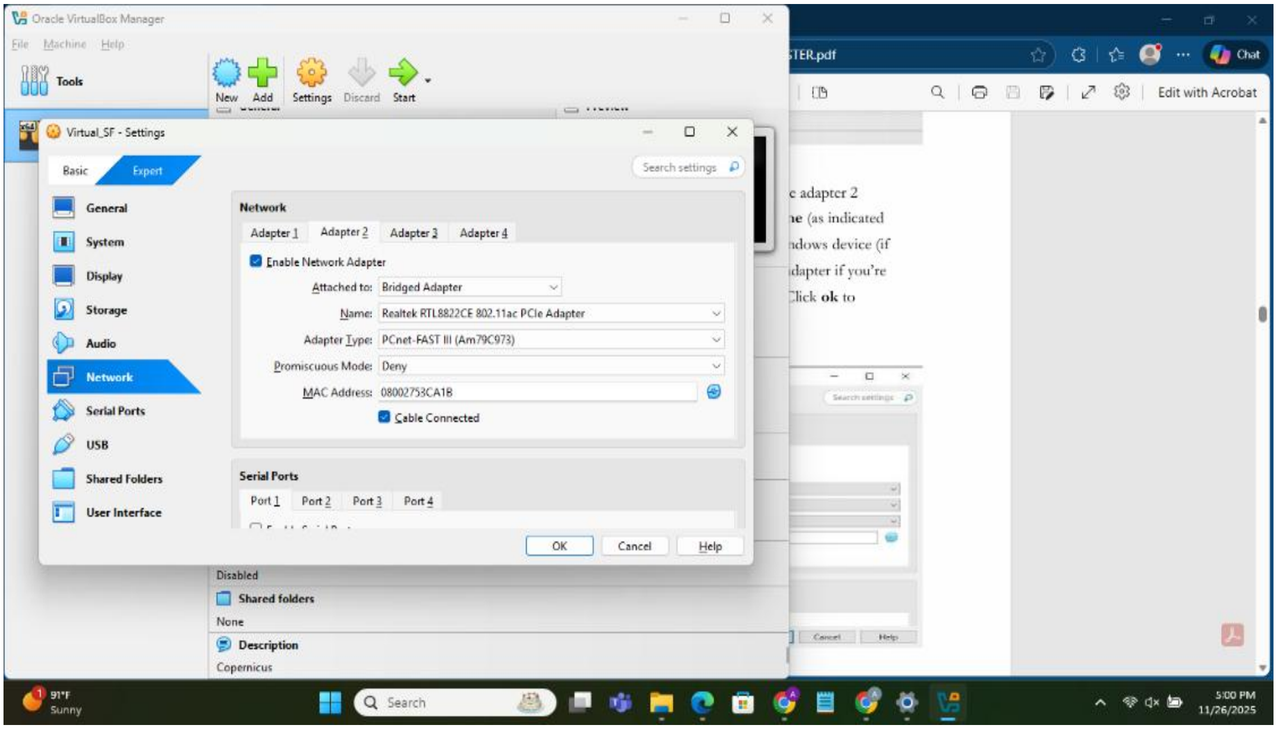
1. VirtualBox and Sophos VM were downloaded.
   Then the installation and import the Sophos file.



Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
VirtualBox Host-Only Ethernet Adapter	192.168.56.1/24		Enabled

○ Configure Adapter Automatically
● Configure Adapter Manually
IPv4 Address: 192.168.25.1
IPv4 Network Mask: 255.255.255.0
IPv6 Address: fe80::1a60:6e2f:8fe9:f437
IPv6 Prefix Length: 64

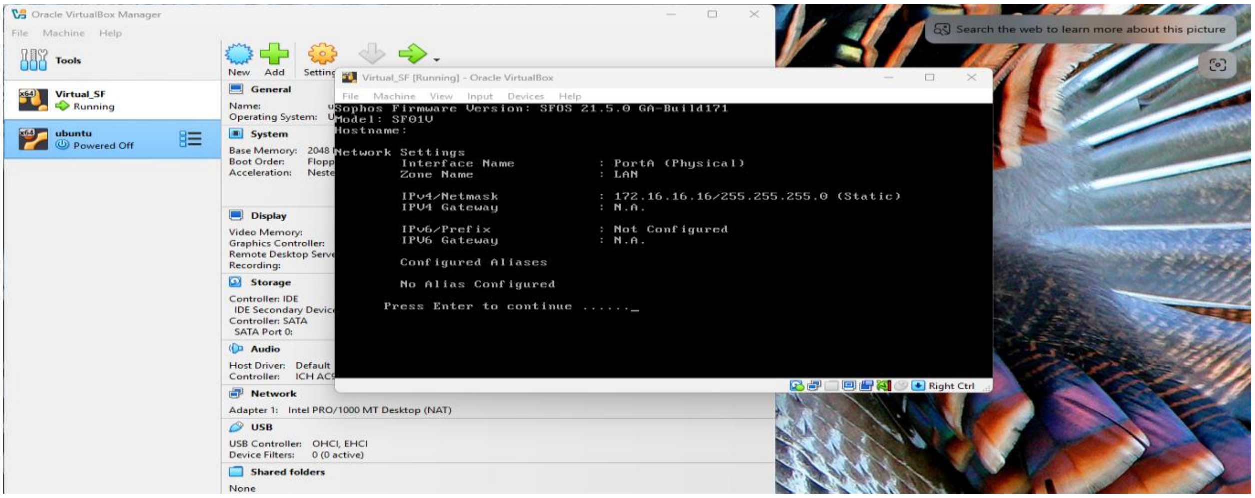
2. Setting up network adapter and Ip address assigned.



Network
Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4
☑ Enable Network Adapter
Attached to: Bridged Adapter
Name: Realtek RTL8822CE 802.11ac PCIe Adapter
Adapter Type: PCnet-FAST III (Am79C973)
Promiscuous Mode: Deny
MAC Address: 08002753CA1B
☑ Cable Connected

Serial Ports
Port 1 | Port 2 | Port 3 | Port 4

3. Accessing the Sophos console interface and setting up of determine the ip address.


Oracle VirtualBox Manager
File Machine Help
Tools
New Add Settings
Virtual_SF Running
ubuntu Powered Off
Virtual_SF [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Right Ctrl
Search the web to learn more about this picture

General
Name:
Operating System:

System
Base Memory: 2048
Boot Order: Flopp
Acceleration: Neste

Display
Video Memory:
Graphics Controller:
Remote Desktop Serve
Recording:

Storage
Controller: IDE
IDE Secondary Devic
Controller: SATA
SATA Port 0:

Audio
Host Driver: Default
Controller: ICH AC

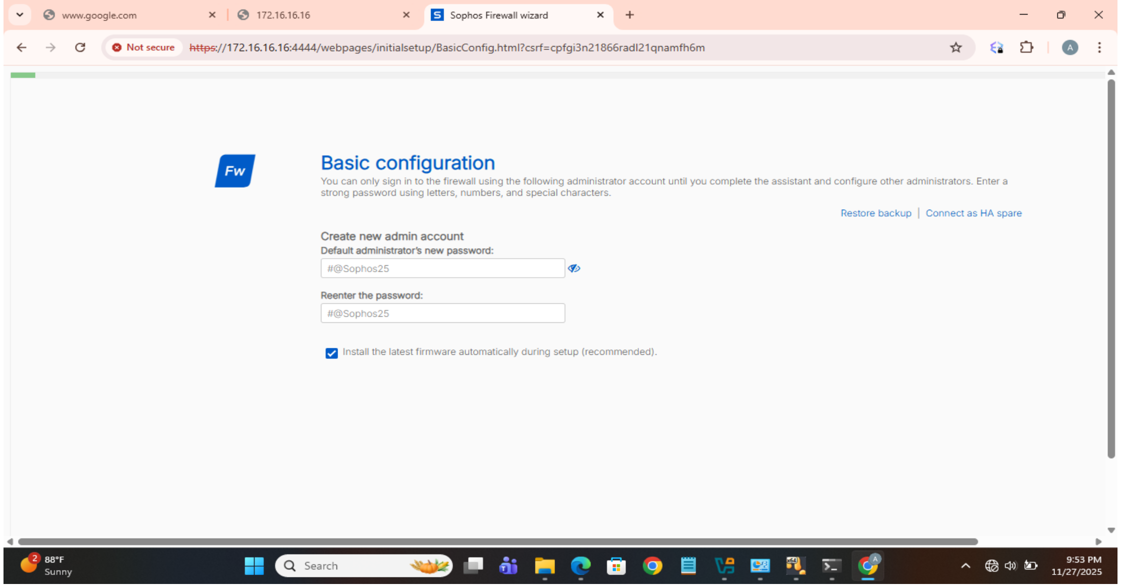
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders
None

```
Sophos Firmware Version: SFOS 21.5.0 GA-Build171
Model: SF01V
Hostname:

Network Settings
        Interface Name              : PortA (Physical)
        Zone Name                   : LAN

        IPv4/Netmask                : 172.16.16.16/255.255.255.0 (Static)
        IPV4 Gateway                : N.A.

        IPv6/Prefix                 : Not Configured
        IPV6 Gateway                : N.A.

        Configured Aliases

        No Alias Configured

      Press Enter to continue ......_
```

4. Accessing the Sophos GUI via a web address (using the assigned Ip address and port 444)



~~https~~://172.16.16.16:4444/webpages/initialsetup/BasicConfig.html?csrf=cpfgi3n21866radl21qnamfh6m

Basic configuration

You can only sign in to the firewall using the following administrator account until you complete the assistant and configure other administrators. Enter a strong password using letters, numbers, and special characters.

Restore backup | Connect as HA spare

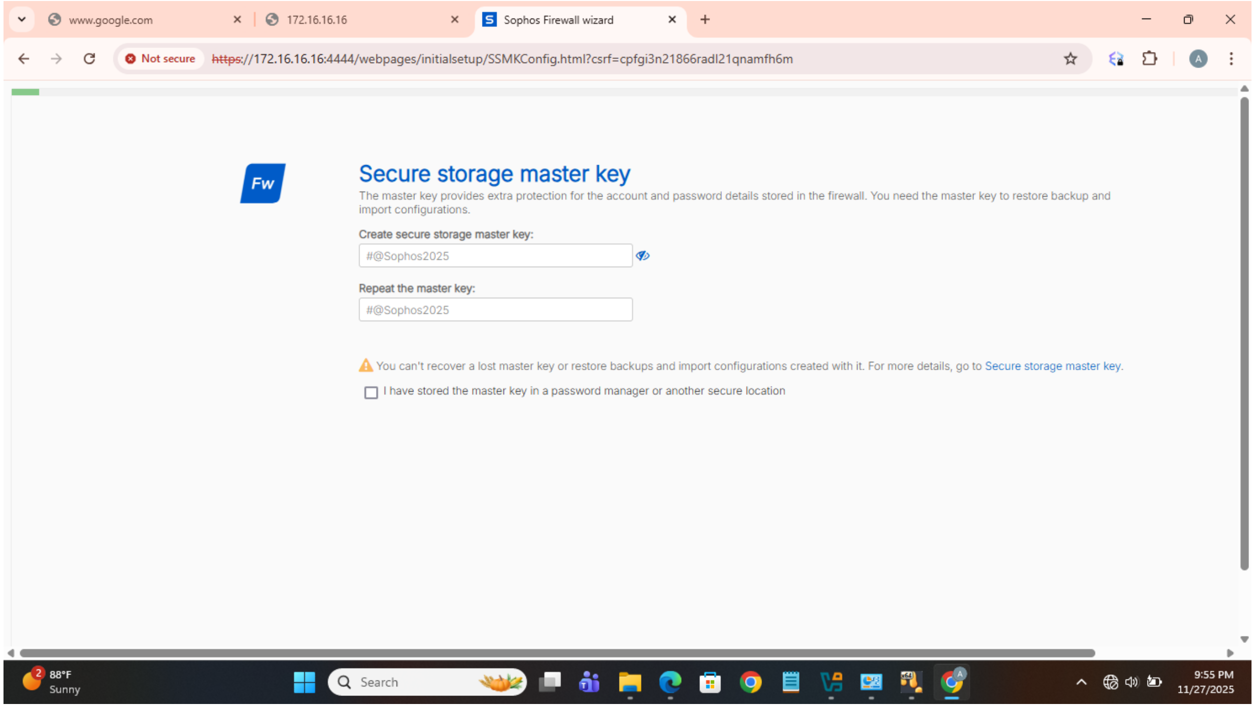
Create new admin account

Default administrator's new password: #@Sophos25

Reenter the password: #@Sophos25

☑ Install the latest firmware automatically during setup (recommended).

5. Setting up admin password Username, secure storage key encryption key and region.



www.google.com
172.16.16.16
Sophos Firewall wizard
Not secure
https://172.16.16.16:4444/webpages/initialsetup/SSMKConfig.html?csrf=cpfgi3n21866radl21qnamfh6m
Fw
88°F
Sunny
Search
9:55 PM
11/27/2025

Secure storage master key

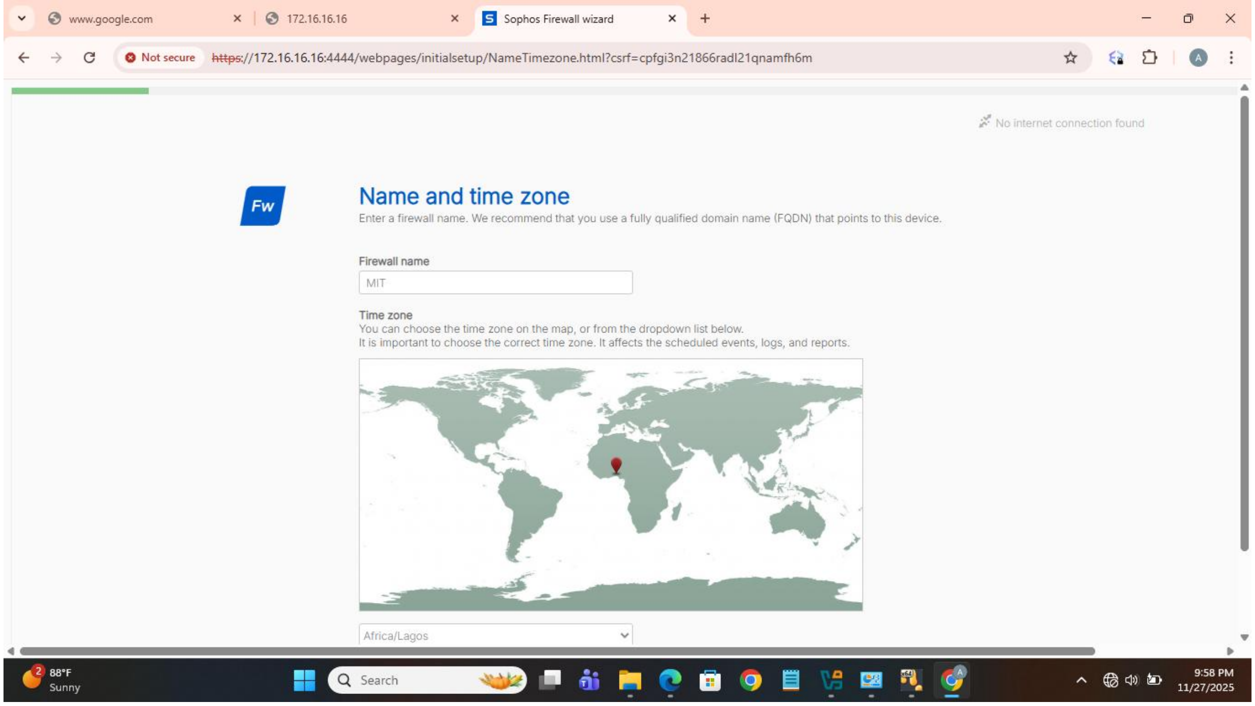
The master key provides extra protection for the account and password details stored in the firewall. You need the master key to restore backup and import configurations.

Create secure storage master key: #@Sophos2025

Repeat the master key: #@Sophos2025

⚠ You can't recover a lost master key or restore backups and import configurations created with it. For more details, go to Secure storage master key.

□ I have stored the master key in a password manager or another secure location



www.google.com
172.16.16.16
Sophos Firewall wizard
Not secure
https://172.16.16.16:4444/webpages/initialsetup/NameTimezone.html?csrf=cpfgi3n21866radl21qnamfh6m
No internet connection found
Fw
88°F
Sunny
Search
9:58 PM
11/27/2025

Name and time zone

Enter a firewall name. We recommend that you use a fully qualified domain name (FQDN) that points to this device.

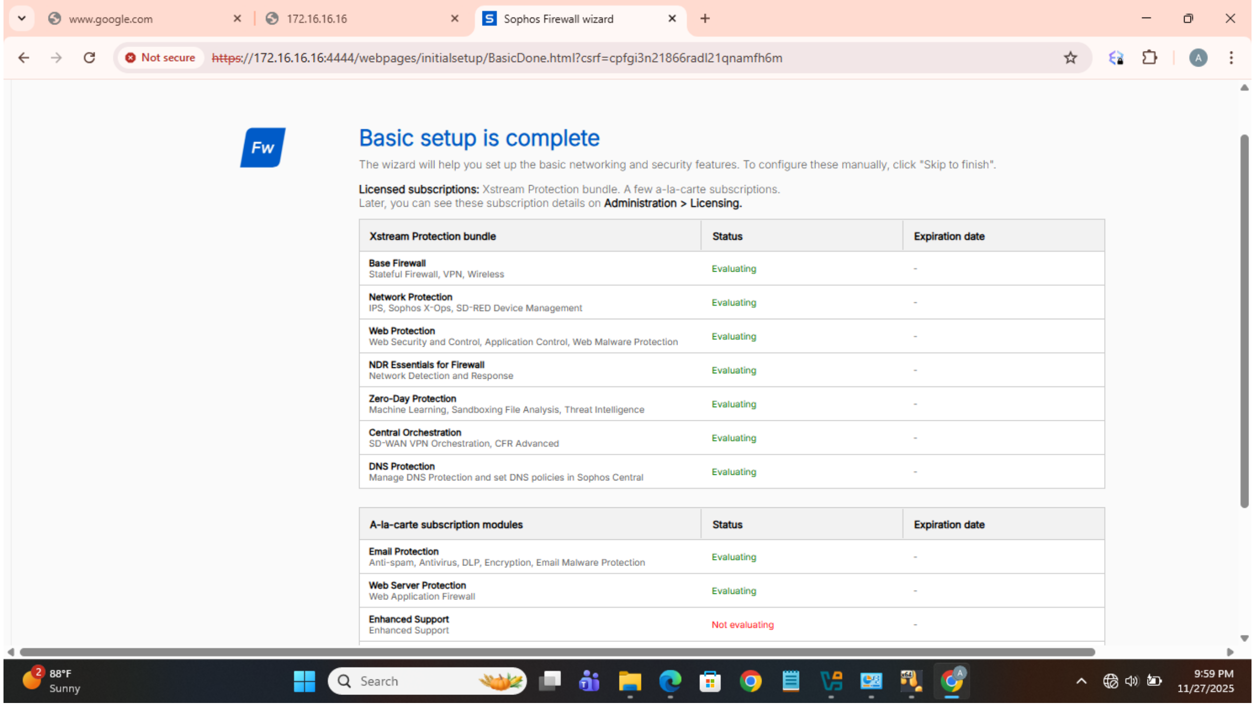
Firewall name: MIT

Time zone

You can choose the time zone on the map, or from the dropdown list below.

It is important to choose the correct time zone. It affects the scheduled events, logs, and reports.

Africa/Lagos


www.google.com
172.16.16.16
Sophos Firewall wizard
Not secure
https://172.16.16.16:4444/webpages/initialsetup/BasicDone.html?csrf=cpfgi3n21866radl21qnamfh6m
Fw
88°F
Sunny
Search
9:59 PM
11/27/2025

Basic setup is complete

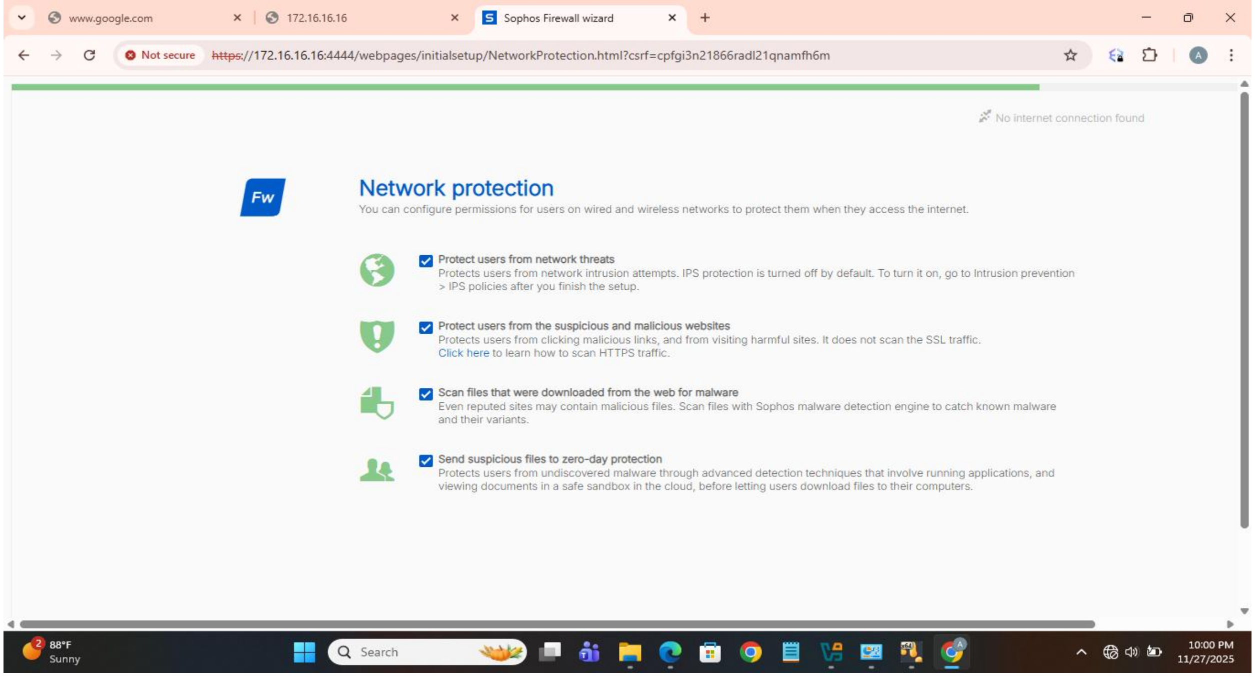
The wizard will help you set up the basic networking and security features. To configure these manually, click "Skip to finish".

Licensed subscriptions: Xstream Protection bundle. A few a-la-carte subscriptions.
Later, you can see these subscription details on **Administration > Licensing.**

Xstream Protection bundle	Status	Expiration date
Base Firewall Stateful Firewall, VPN, Wireless	Evaluating	-
Network Protection IPS, Sophos X-Ops, SD-RED Device Management	Evaluating	-
Web Protection Web Security and Control, Application Control, Web Malware Protection	Evaluating	-
NDR Essentials for Firewall Network Detection and Response	Evaluating	-
Zero-Day Protection Machine Learning, Sandboxing File Analysis, Threat Intelligence	Evaluating	-
Central Orchestration SD-WAN VPN Orchestration, CFR Advanced	Evaluating	-
DNS Protection Manage DNS Protection and set DNS policies in Sophos Central	Evaluating	-

A-la-carte subscription modules	Status	Expiration date
Email Protection Anti-spam, Antivirus, DLP, Encryption, Email Malware Protection	Evaluating	-
Web Server Protection Web Application Firewall	Evaluating	-
Enhanced Support Enhanced Support	Not evaluating	-

6. Selection of best network protection options.


www.google.com
172.16.16.16
Sophos Firewall wizard
Not secure
https://172.16.16.16:4444/webpages/initialsetup/NetworkProtection.html?csrf=cpfgi3n21866radl21qnamfh6m
No internet connection found
Fw
88°F
Sunny
Search
10:00 PM
11/27/2025

Network protection

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

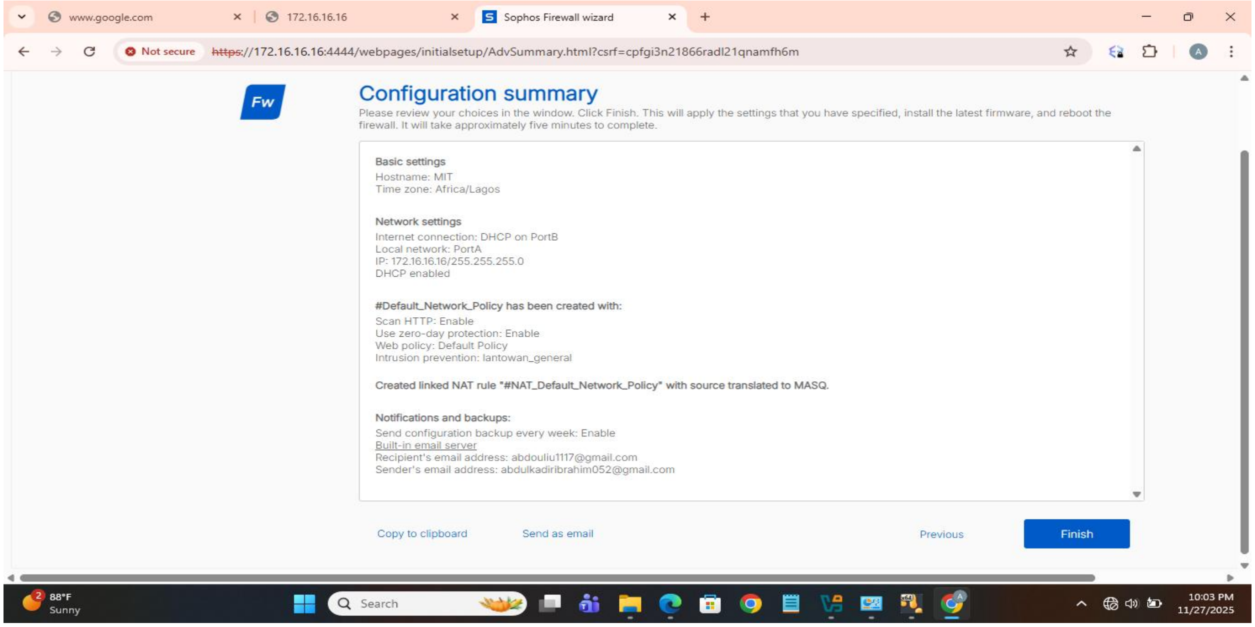
☑ Protect users from network threats
Protects users from network intrusion attempts. IPS protection is turned off by default. To turn it on, go to Intrusion prevention > IPS policies after you finish the setup.

☑ 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.

7. The configuration summary, which give the highlight of all you initial set up.


www.google.com
172.16.16.16
Sophos Firewall wizard
Not secure
https://172.16.16.16:4444/webpages/initialsetup/AdvSummary.html?csrf=cpfgi3n21866radl21qnamfh6m
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: MIT
Time zone: Africa/Lagos

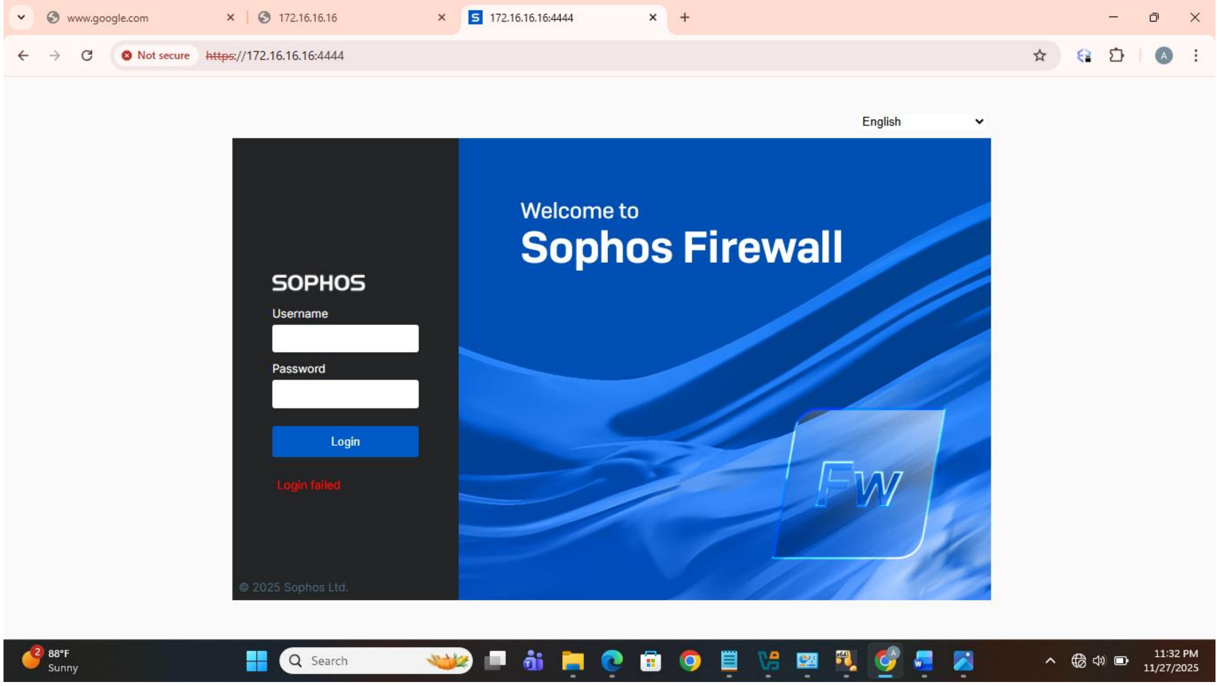
Network settings
Internet connection: DHCP on PortB
Local network: PortA
IP: 172.16.16.16/255.255.255.0
DHCP enabled

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

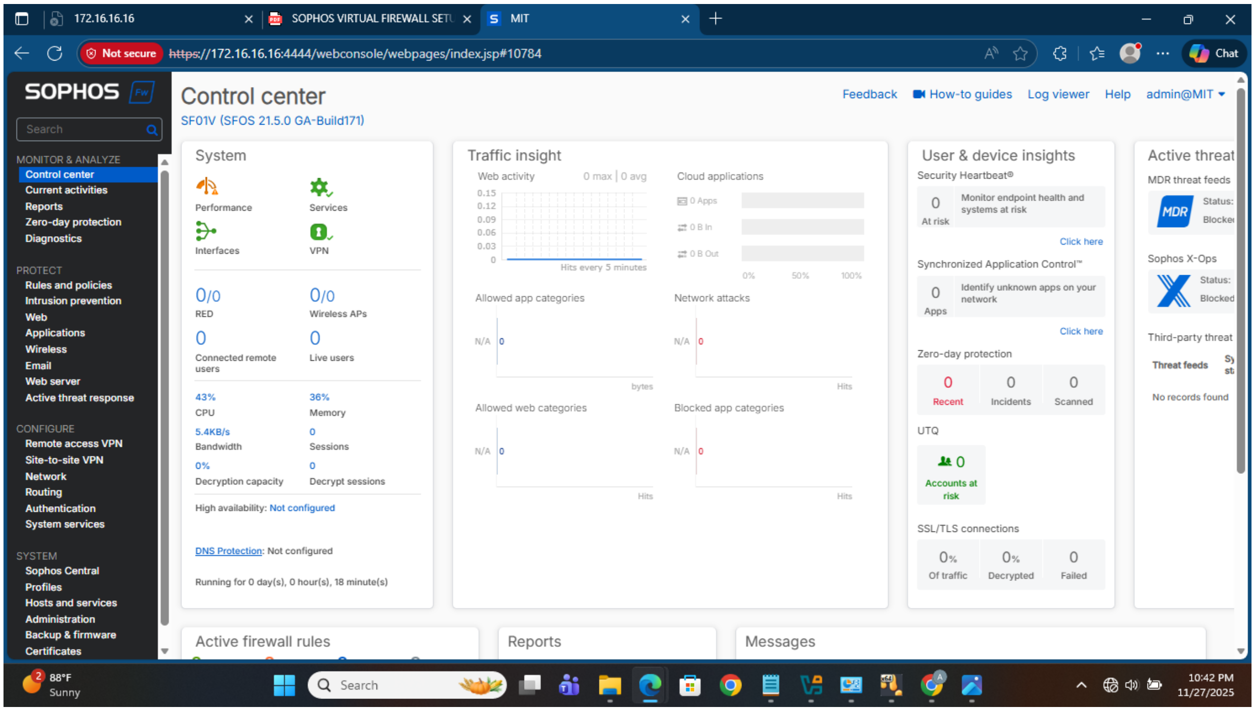
Created linked NAT rule "#NAT_Default_Network_Policy" with source translated to MASQ.

Notifications and backups:
Send configuration backup every week: Enable
Built-in email server
Recipient's email address: abdouliu1117@gmail.com
Sender's email address: abdulkadiribrahim052@gmail.com

8. After successful setting up configuration, the firewall will reboot so as the setups take effect.
9. After reloading it will show the interface as to input username and admin password to access the main firewall dashboard.



10. If the credentials are correct, then it will give access to the GUI main dashboard of the firewall where all the magic is happening.



Control center

SF01V (SFOS 21.5.0 GA-Build171)

System

Performance
Services
Interfaces
VPN

0/0 RED
0/0 Wireless APs
0 Connected remote users
0 Live users

43% CPU
36% Memory
5.4KB/s Bandwidth
0 Sessions
0% Decryption capacity
0 Decrypt sessions

High availability: Not configured

DNS Protection: Not configured

Running for 0 day(s), 0 hour(s), 18 minute(s)

Traffic insight

Web activity 0 max | 0 avg

Cloud applications
0 Apps
0 B In
0 B Out

Allowed app categories
N/A 0

Network attacks
N/A 0

Allowed web categories
N/A 0

Blocked app categories
N/A 0

User & device insights

Security Heartbeat®
0 At risk — Monitor endpoint health and systems at risk
Click here

Synchronized Application Control™
0 Apps — Identify unknown apps on your network
Click here

Zero-day protection
0 Recent
0 Incidents
0 Scanned

UTQ
0 Accounts at risk

SSL/TLS connections
0% Of traffic
0% Decrypted
0 Failed

Active threat

MDR threat feeds
Status: Blocke

Sophos X-Ops
Status: Blocked

Third-party threat
Threat feeds Sy st
No records found

Active firewall rules

Reports

Messages