

SOPHOS NEXT-GEN FIREWALL

Installation, Setup & Security Policy Configuration

On VMware Workstation Pro 17.5 for Windows 10

With Kali OS & Parrot OS

Jeffrey Obi
November 2025

Contents

Introduction	2
Sophos Firewall	2
Step 1: Sophos Firewall Download & Pre-Installation	2
Step 2: VMware Network Configuration	5
Step 3: Firewall Machine Creation & Network Configuration	7
Step 4: Firewall Operating System Setup	11
Step 5: Firewall Web Admin Console Setup	16
Step 6: Firewall Console Access	26
Conclusion	27
Security Policy 1	29
Step 7: Confirm Network Settings	29
Step 8: Launch and Run the Firewall Virtual Machine	31
Step 9: Test LAN Virtual Machine Connection	31
Step 10: Configure the KaliOS Virtual Machine Network Settings	33
Step 11: Access the Firewall Using the Web Console	34
Step 12: Configure Firewall Rule	35
Step 13: Configure NAT Rule	37
Step 14: Confirm Firewall Internet Connectivity	38
Step 15: Confirm KaliOS VM Internet Connectivity	39
Conclusion	40
Security Policy 2	42
Step 16: Create Web Policy	42
Step 17: Add Policy to Firewall Rule	44
Step 18: Test News Blocking Rule from the Web Console	45
Step 19: Test News Blocking Rule from KaliOS VM Browser	47
Conclusion	47
Security Policy 3	48
Step 20: Launch and Set Up Virtual Machines	48
Step 21: Configure DoS & Spoof Protection	49
Step 22: Test DoS & Spoof Protection	51
Conclusion	52

Introduction

Background & Goals

Sophos Firewall is a network security software solution which provides services like firewall, VPN and ransomware protection services used to protect networks. The implementation of the firewall operating system (**SFOS**) helps defend against advanced threats.

In this guide, the firewall is implemented in the local lab environment inside the host machine (**Windows 10 x64**). The firewall operating system (**SFOS**) is added to the virtualizer (**VMware Workstation Pro 17.5**) as a virtual machine in order to provide protection services for the other virtual machines in the shared virtual network, as well as any machine which uses the firewall virtual machine as its gateway, routing its traffic through it.

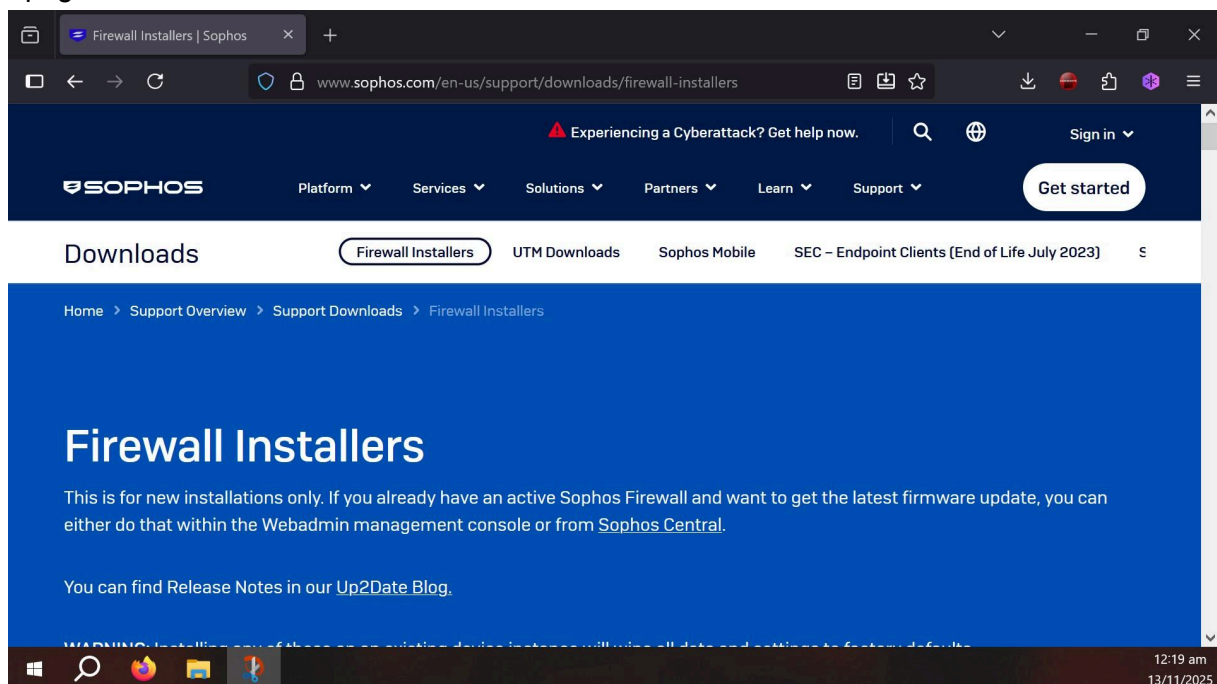
First, the firewall (Sophos) is downloaded, installed, configured and set up. Then, security rules and policies are configured on the firewall to enable it to apply its security services to all connected machines.

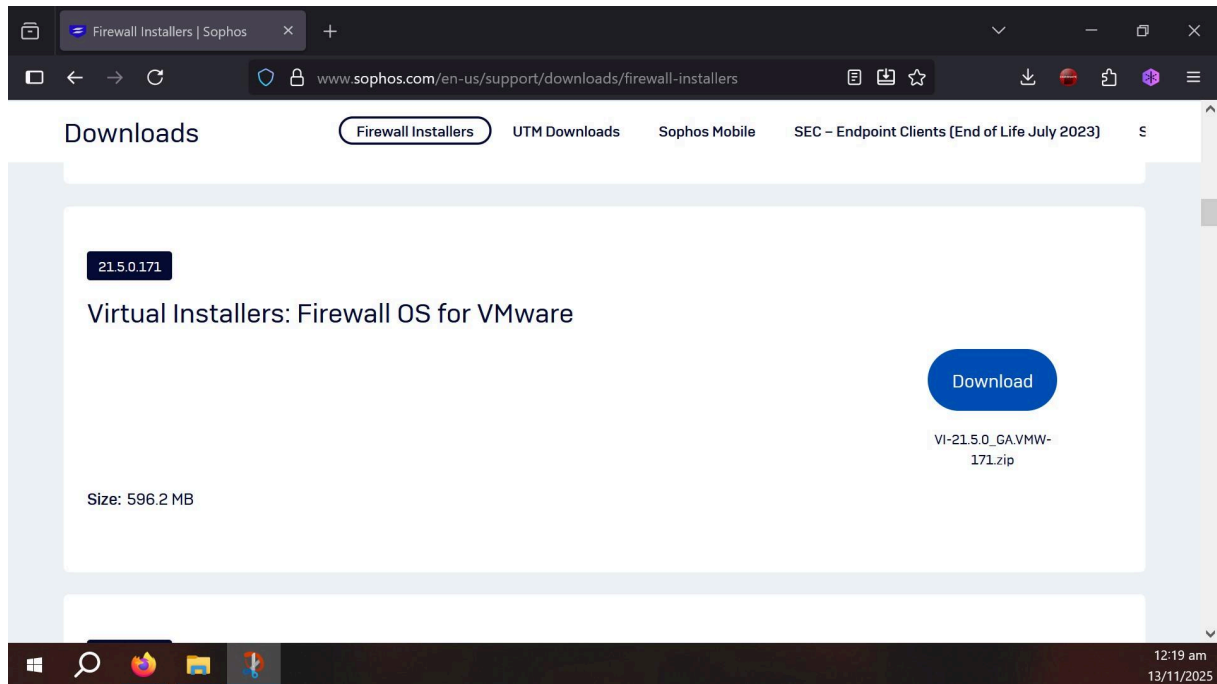
Sophos Firewall

Installation, Configuration & Setup

Step 1: Sophos Firewall Download & Pre-Installation

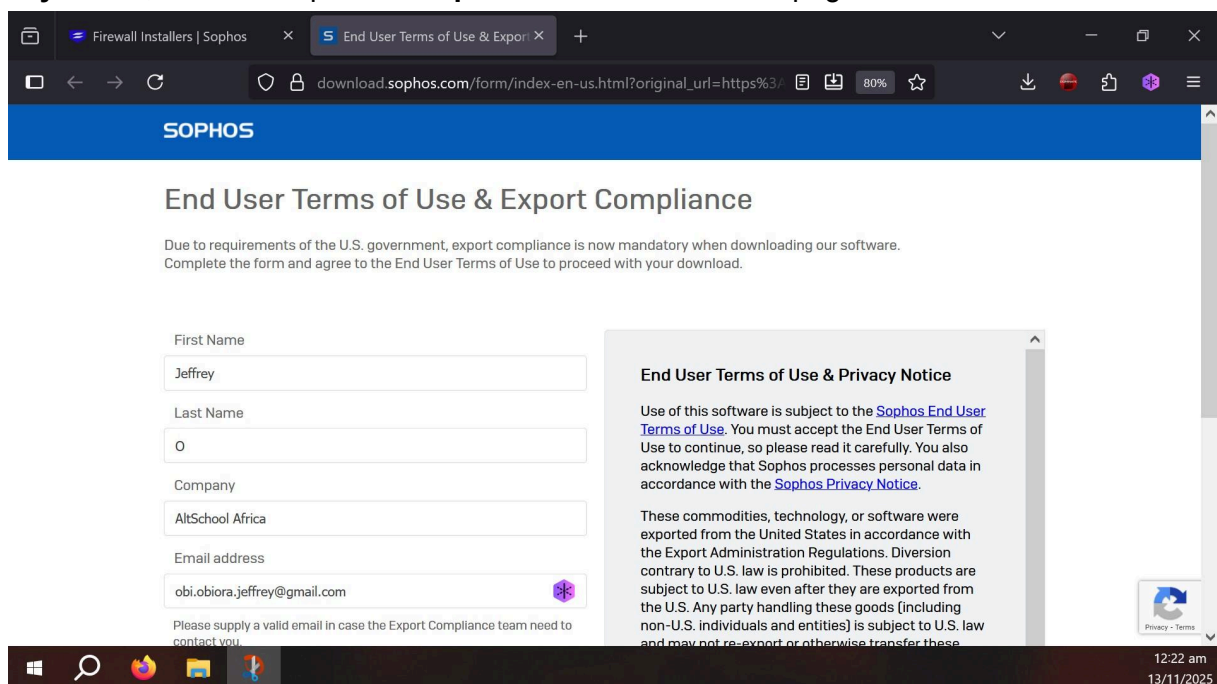
To begin, launch a browser (**Firefox**) and navigate to the Sophos **Firewall Installers** webpage at the link: <https://www.sophos.com/en-us/support/downloads/firewall-installers>. Scroll down on this page to find the card titled “**Virtual Installers: Firewall OS for VMware**” and click the associated **Download** button, which will open the *End User Terms of Use & Export Compliance* webpage in a new tab.





a. Agree to End User Terms of Use & Export Compliance

On the **End User Terms of Use & Export Compliance** webpage, fill out the form with your First Name, Last Name, Company, and Email address, then check the box to accept the **Sophos End User Terms of Use** and acknowledge the **Sophos Privacy Notice** before clicking the **Submit Query** button, which will open the **Sophos File Download** webpage.



Jeffrey

Last Name

O

Company

AltSchool Africa

Email address

obi.obiora.jeffrey@gmail.com

Please supply a valid email in case the Export Compliance team need to contact you.

☒ I accept the [Sophos End User Terms of Use](#) and acknowledge the [Sophos Privacy Notice](#).

Submit Query

End User Terms of Use & Privacy Notice

Use of this software is subject to the [Sophos End User Terms of Use](#). You must accept the End User Terms of Use to continue, so please read it carefully. You also acknowledge that Sophos processes personal data in accordance with the [Sophos Privacy Notice](#).

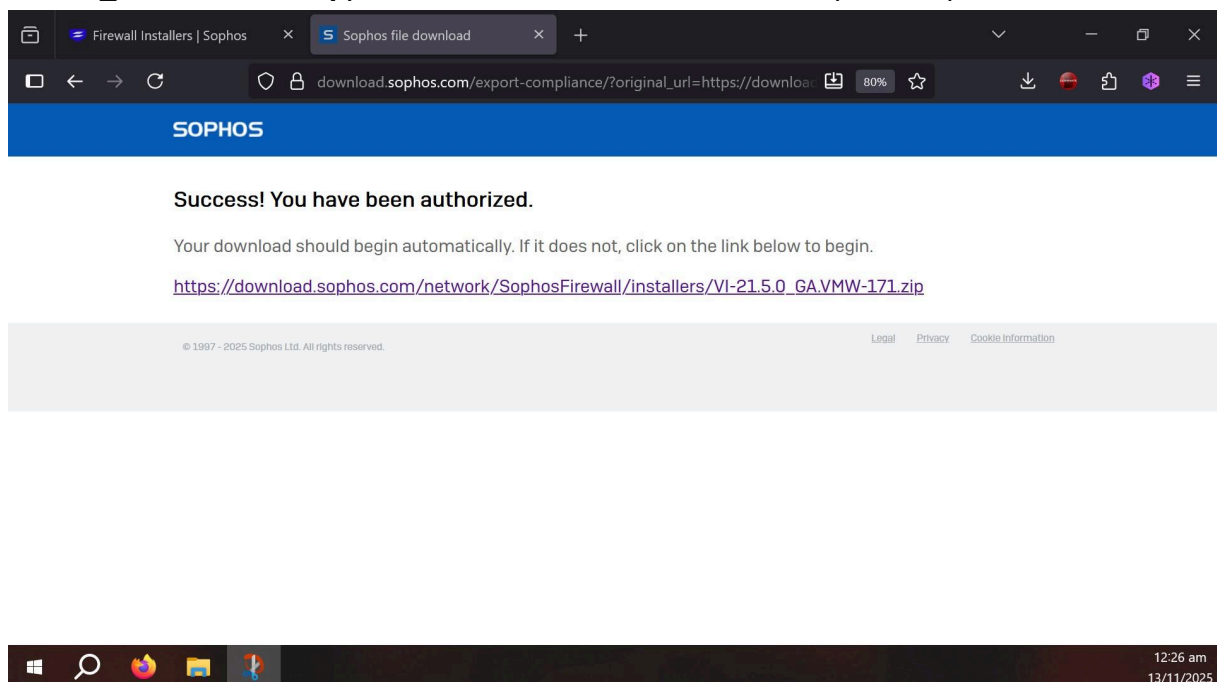
These commodities, technology, or software were exported from the United States in accordance with the Export Administration Regulations. Diversion contrary to U.S. law is prohibited. These products are subject to U.S. law even after they are exported from the U.S. Any party handling these goods (including non-U.S. individuals and entities) is subject to U.S. law and may not re-export or otherwise transfer these items to prohibited countries, individuals, companies, governments, or other entities. Violators may be subject to penalties including fines and the denial of permissions to export and re-export U.S. origin products. The export control laws and regulations of other countries may apply in addition to those of the United States.

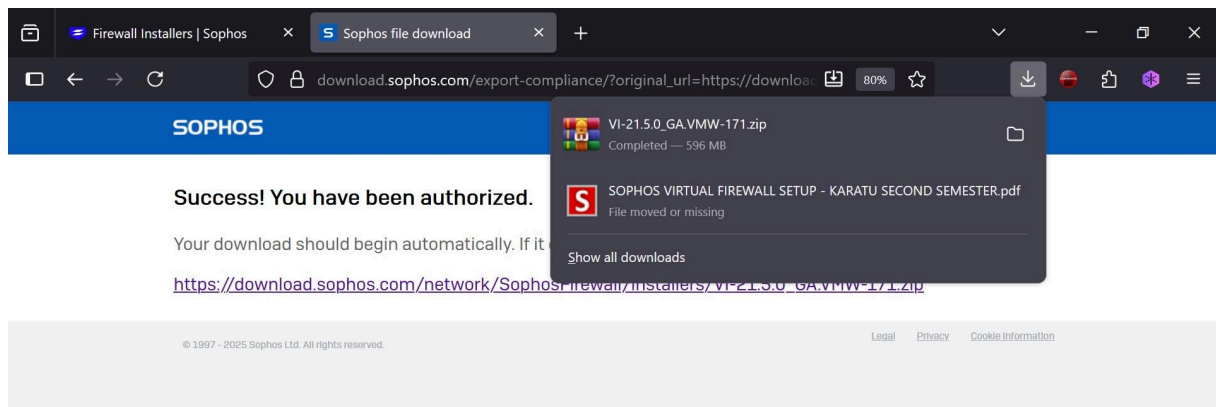
These goods may not be exported, in their entirety or in part, for use in connection with the development, production, handling, operation, maintenance, storage, detection, identification or dissemination of chemical, biological or nuclear weapons, or other nuclear

12:23 am
13/11/2025

b. Download the Sophos Installer

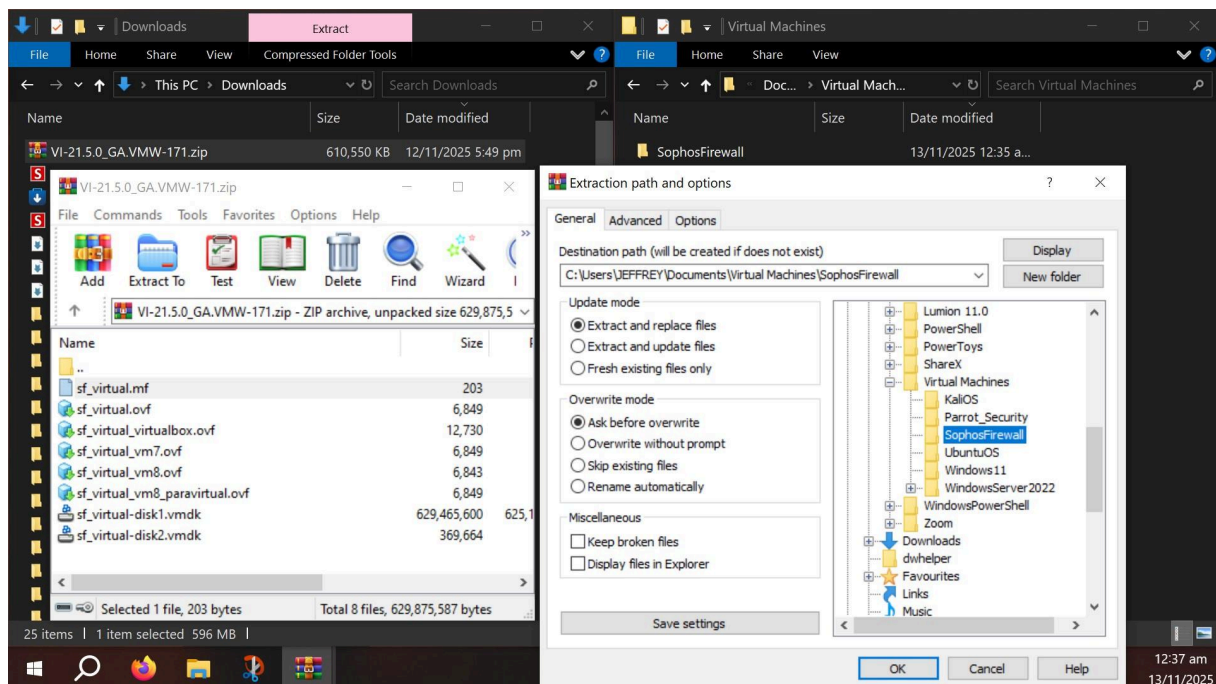
On the just opened **Sophos File Download** webpage, click the download link under “Success! You have been authorized” to download the **ZIP** file, which begins and progresses as **(VI-21.5.0_GA.VMW-171.zip)** and saves to the **Download** folder upon completion.





c. Arrange Pre-Installation Files

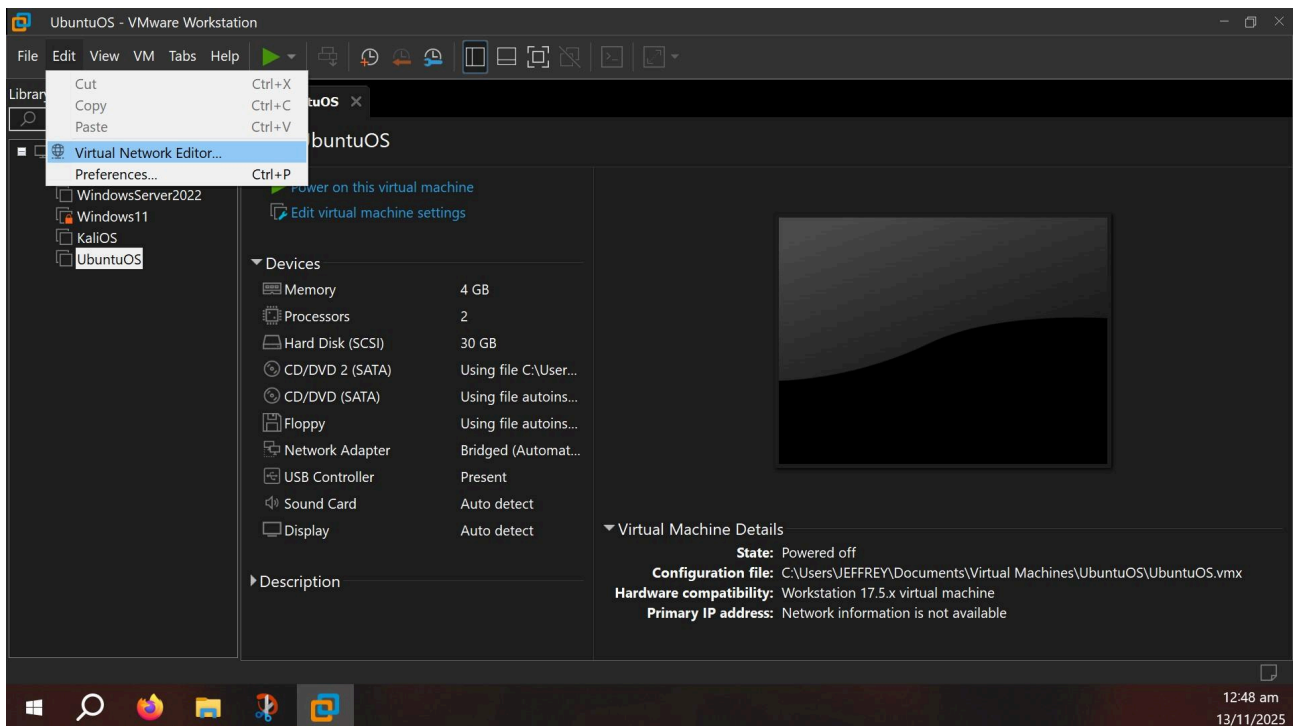
Launch the **ZIP** file, **VI-21.5.0_GA.VMW-171.zip**, using a file decompressor/extractor software (**WinRAR**), and extract its contents to a desired location, such as the **SophosFirewall** folder.



Step 2: VMware Network Configuration

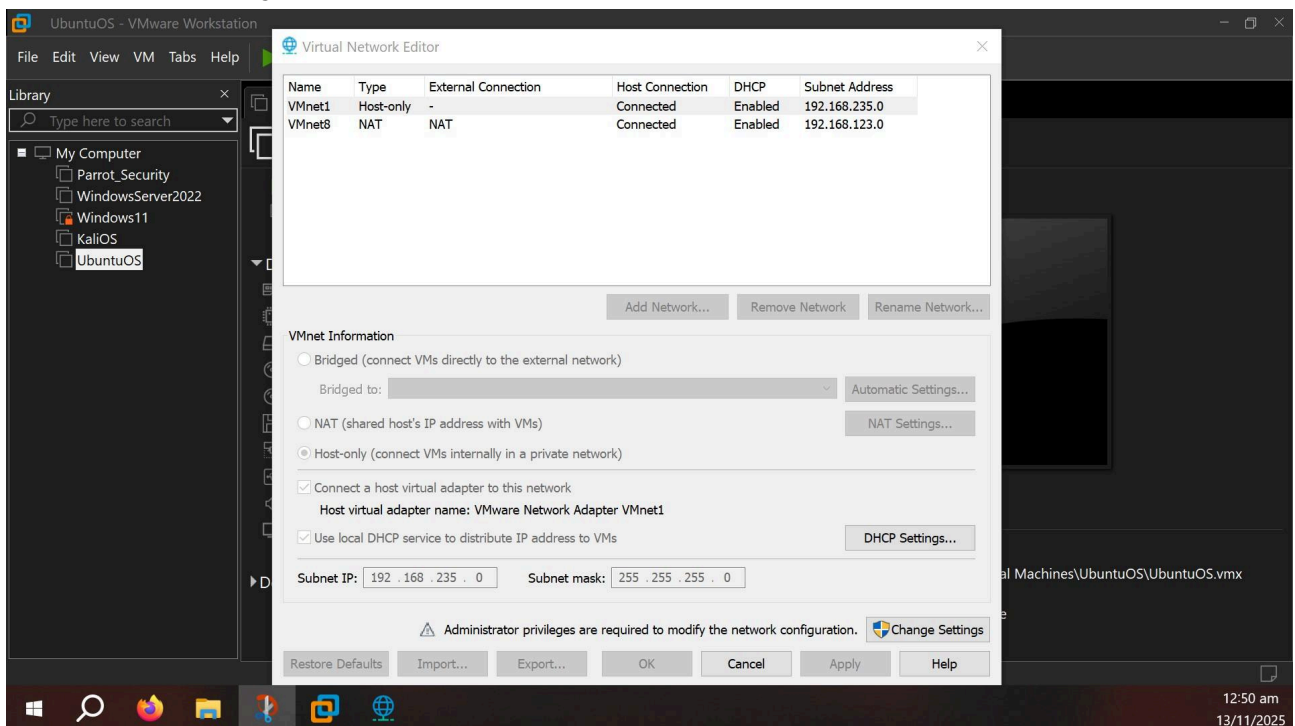
a. Launch Virtual Network Editor

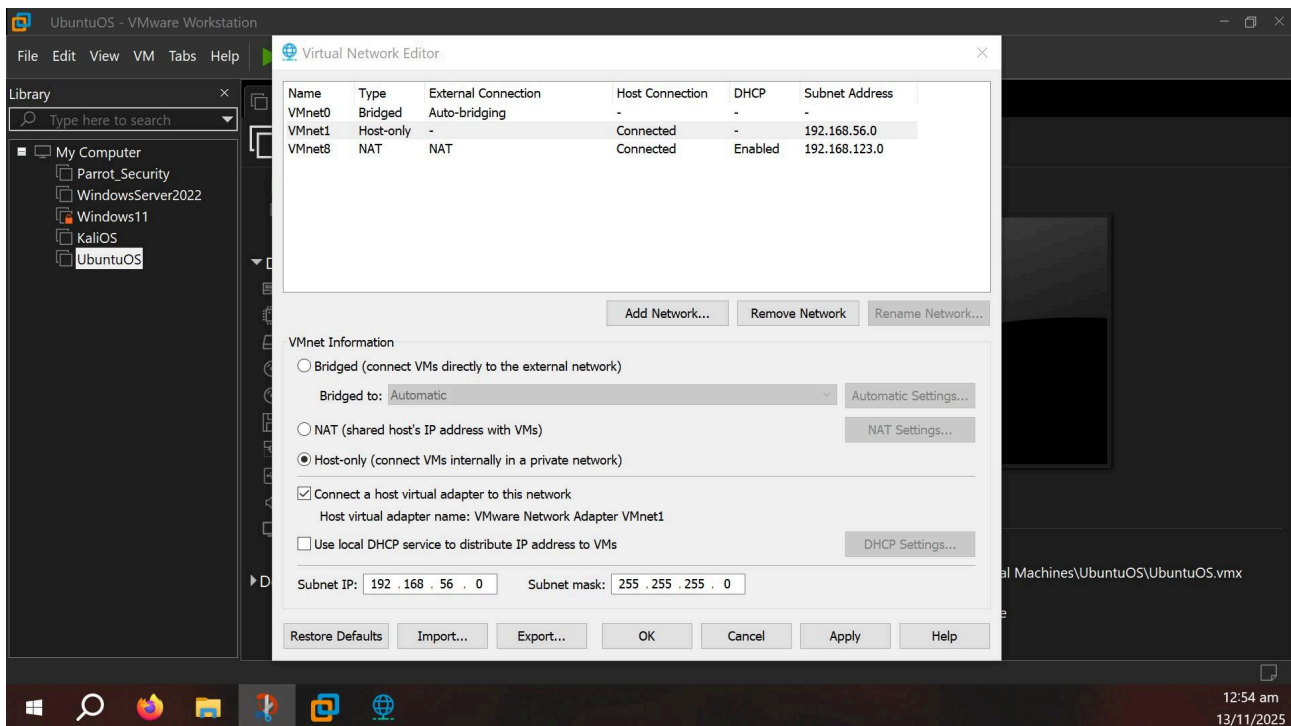
Launch **VMware Workstation Pro 17.5**. Click **Edit** and select **Virtual Network Editor**. *This opens the **Virtual Network Editor** window.*



b. Configure Virtual Network

To modify the network configuration, click **Change Settings** to secure Administrator permissions. In the network adapter list, select **VMnet1**, and under **VMnet Information**, select **Host-only (connect VMs internally in a private network)**, setting **Type** to **Host-only**. Ensure the **Use local DHCP service to distribute IP addresses to VMs** checkbox is unchecked. Finally, input **192.168.56.0** in the **Subnet IP** text box and **255.255.255.0** in the **Subnet mask** text box, then click **Apply** and **OK**.

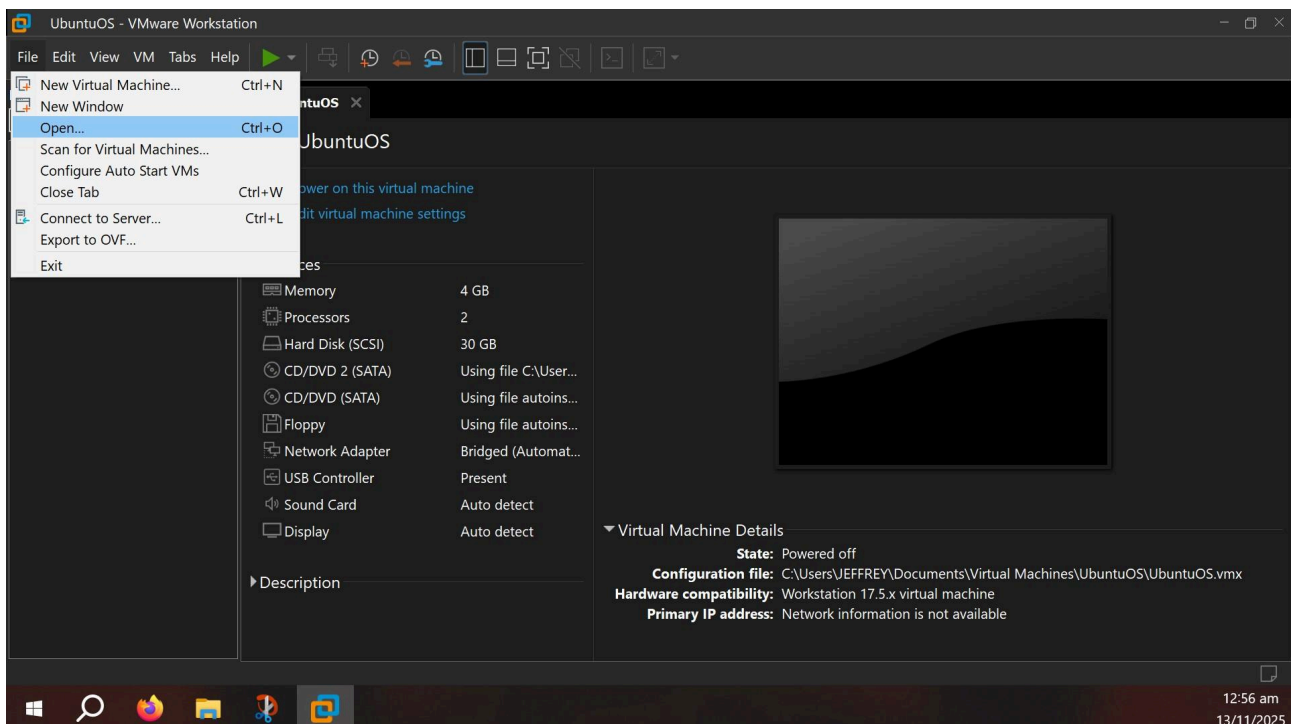




Step 3: Firewall Machine Creation & Network Configuration

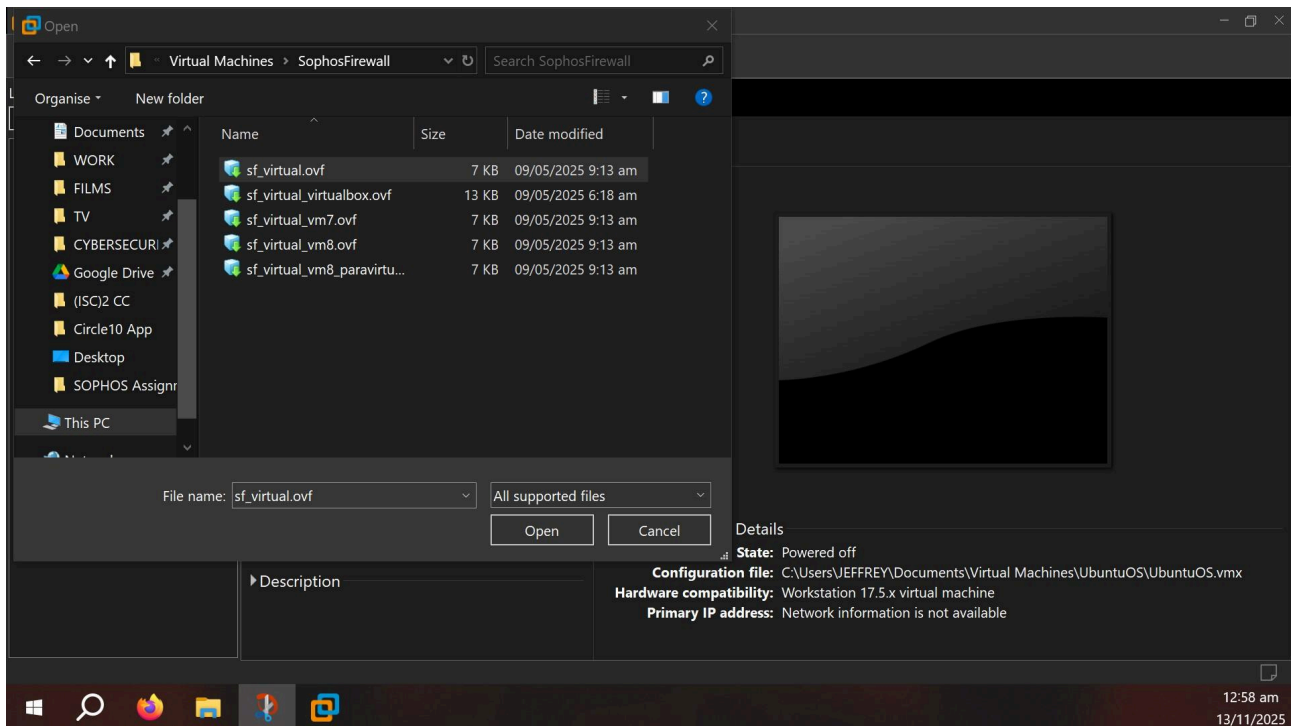
a. Import Firewall Virtual Machine.

i. Click **File** then click **Open**.

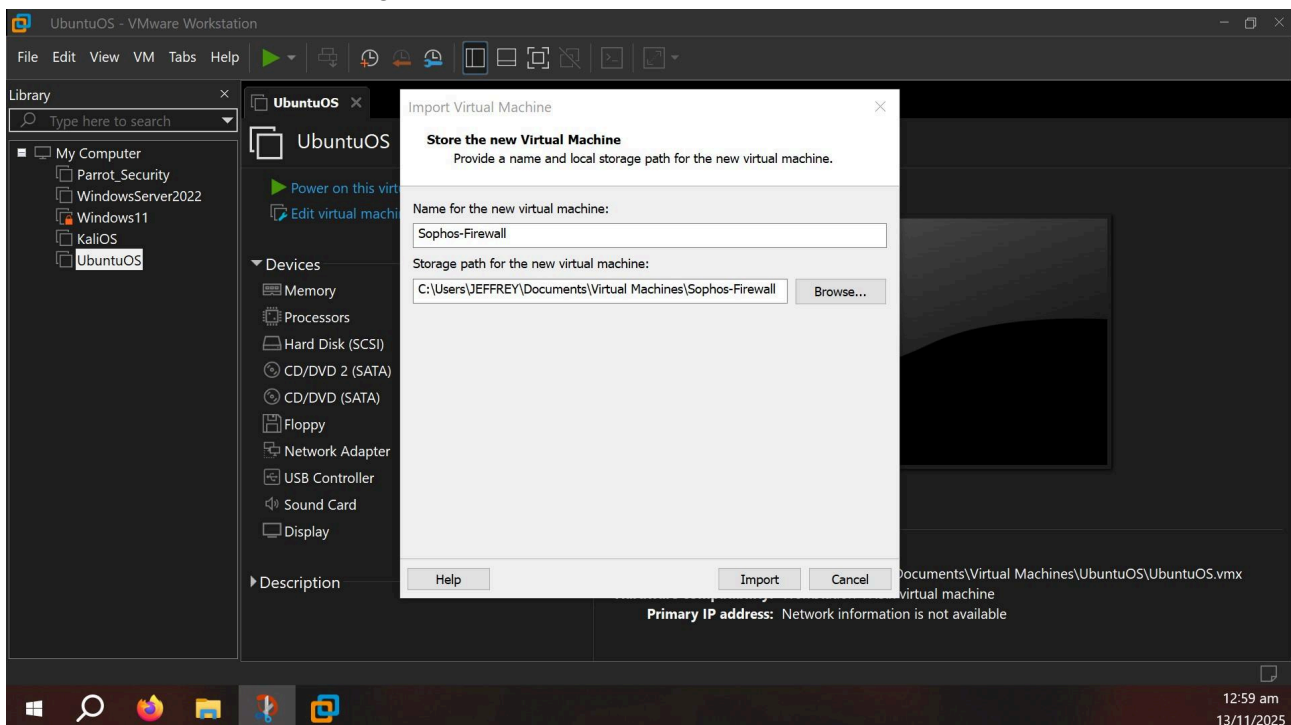


ii. Locate extracted contents of download Sophos Firewall **ZIP** file (inside the **SophosFirewall** folder).

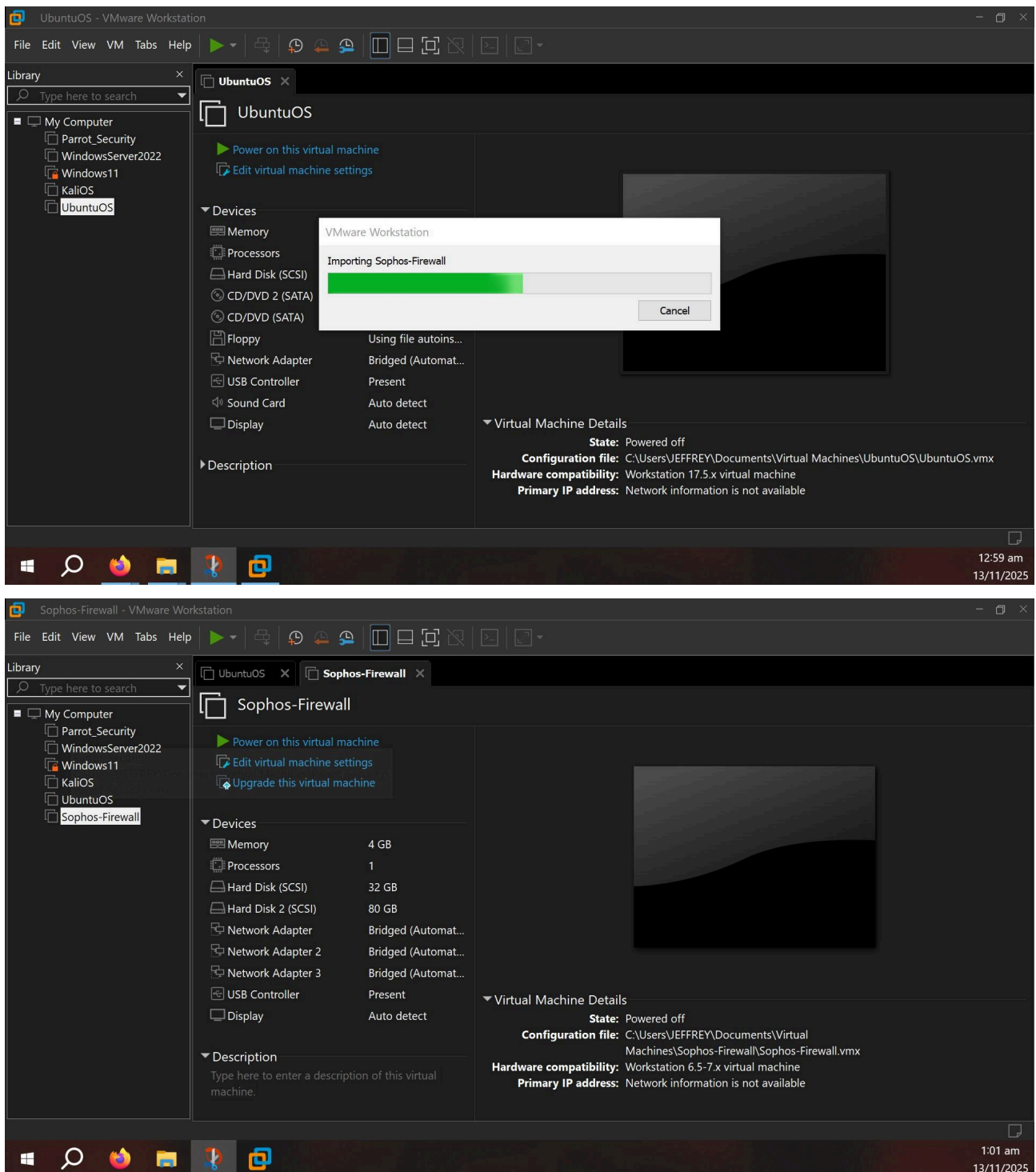
- iii. Select the **sf_virtual.ovf** file and click **Open**. This opens the **Import Virtual Machine** window.



- iv. In the **Import Virtual Machine** window, fill the **Name** text box with the virtual machine name: **Sophos-Firewall**, and fill the **Storage path** text box with the intended storage address of the virtual machine, then click **Import**.

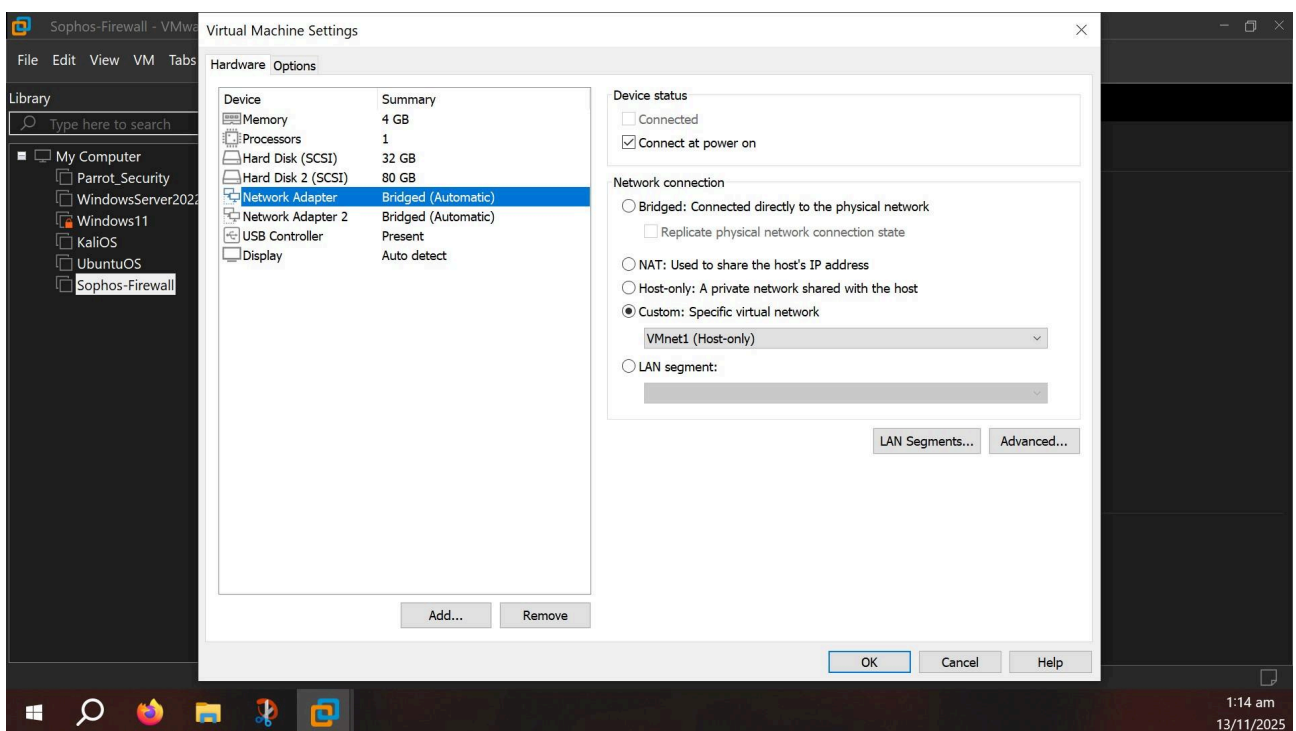
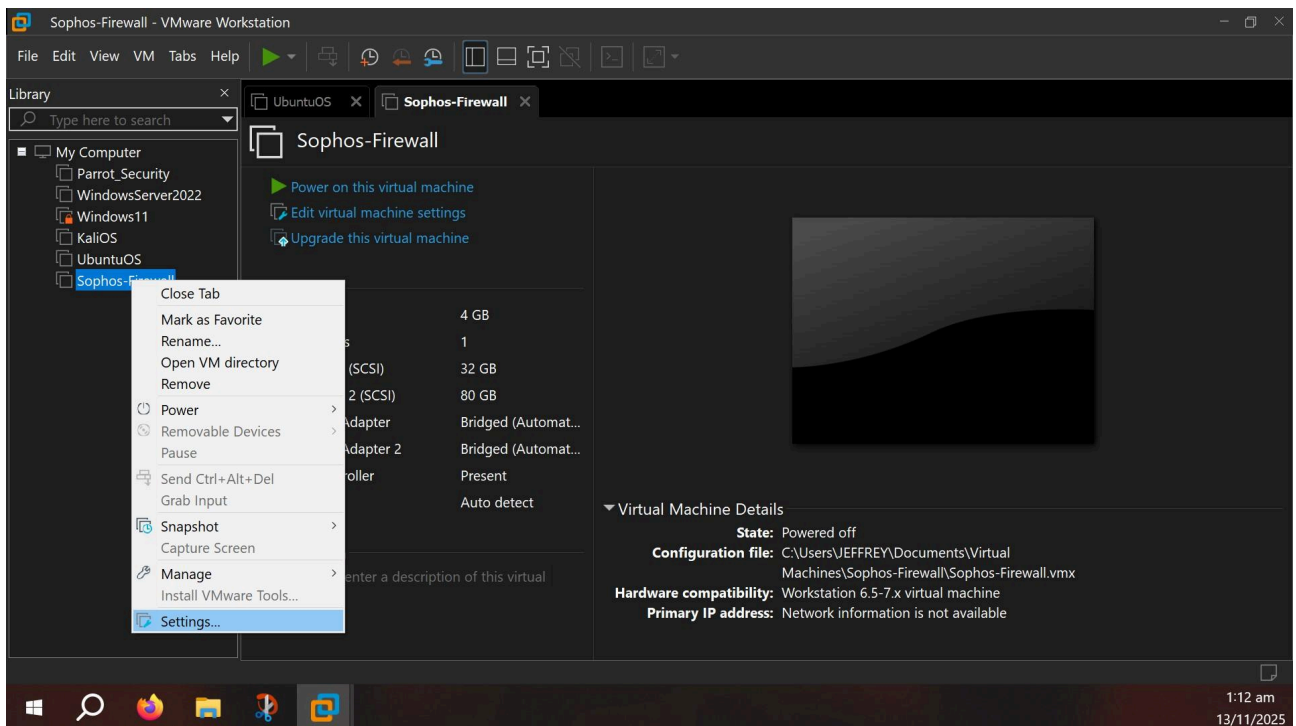


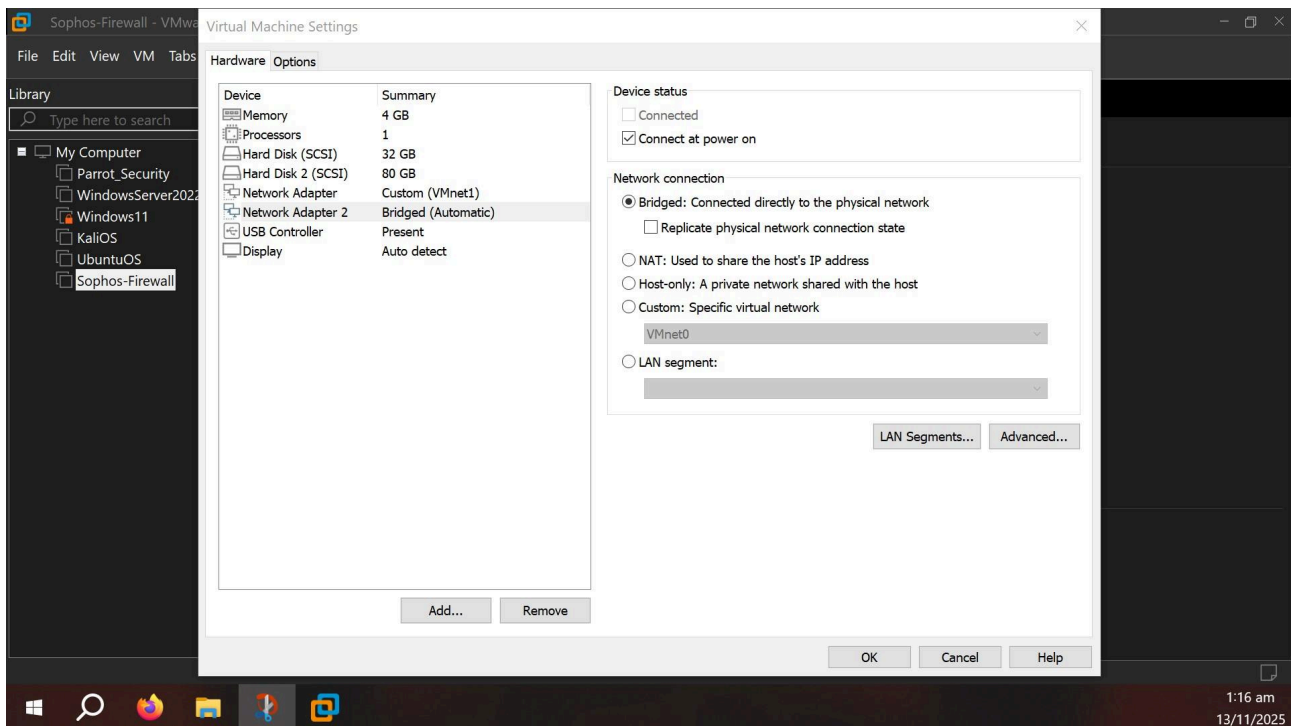
- v. After the **Importing Sophos-Firewall** progress bar completes, a new virtual machine called **Sophos-Firewall** is added to the Library panel on the **VMware Workstation Pro 17.5** main interface.



b. Configure Firewall Virtual Machine Network Adapters

To configure the **Sophos-Firewall** virtual machine in **VMware Workstation Pro 17.5**, right-click the VM in the Library panel and select **Settings...** to open the **Virtual Machine Settings** window. In the **Hardware** tab, select **Network Adapter** in the navigation pane and choose the **Host-only** option in the **Network Connection** section. Finally, ensure that **Network Adapter 2** in the navigation pane has the default summary, **Bridged (Automatic)**, before clicking the **OK** button.

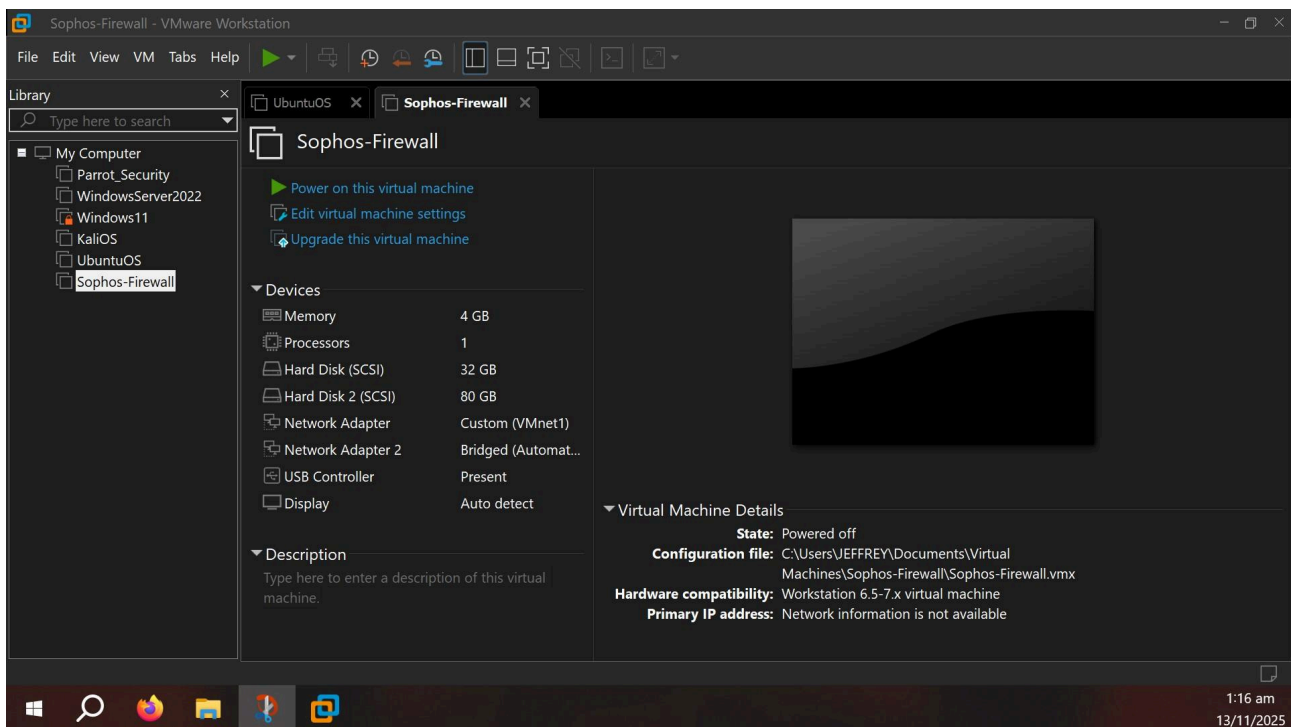




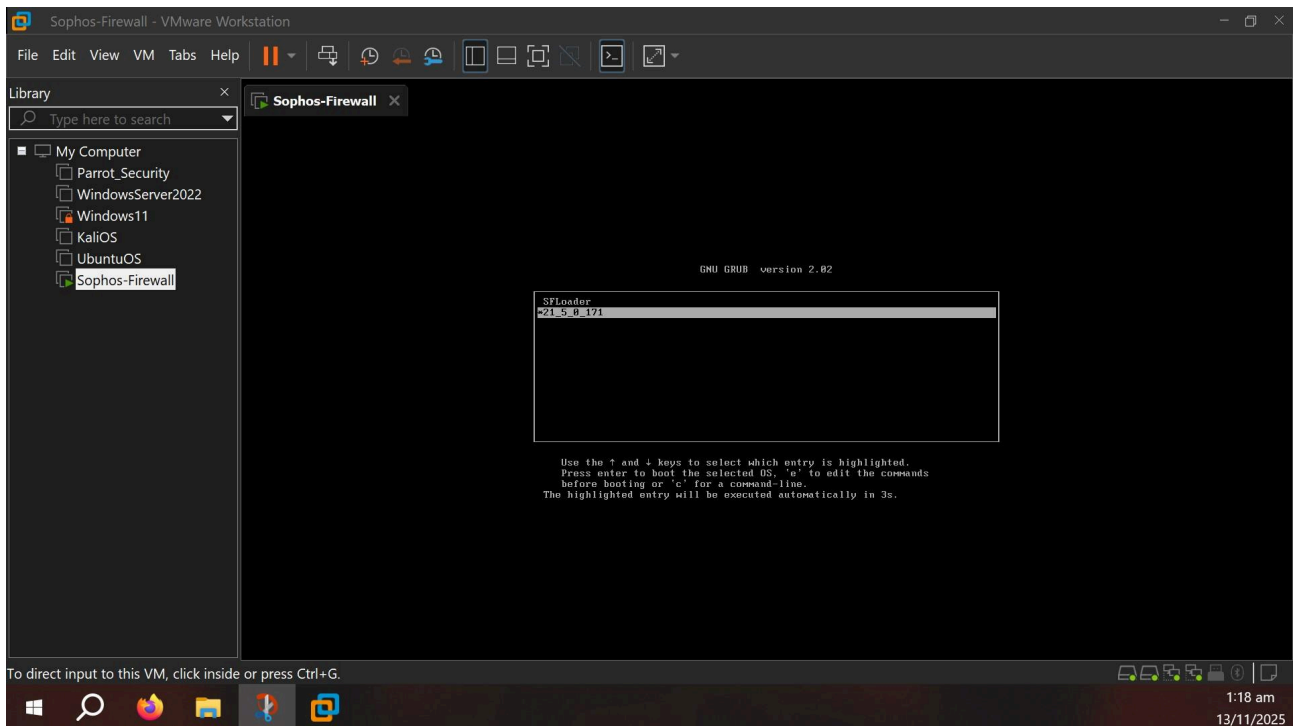
Step 4: Firewall Operating System Setup

a. Launch and Install the Firewall Operating System

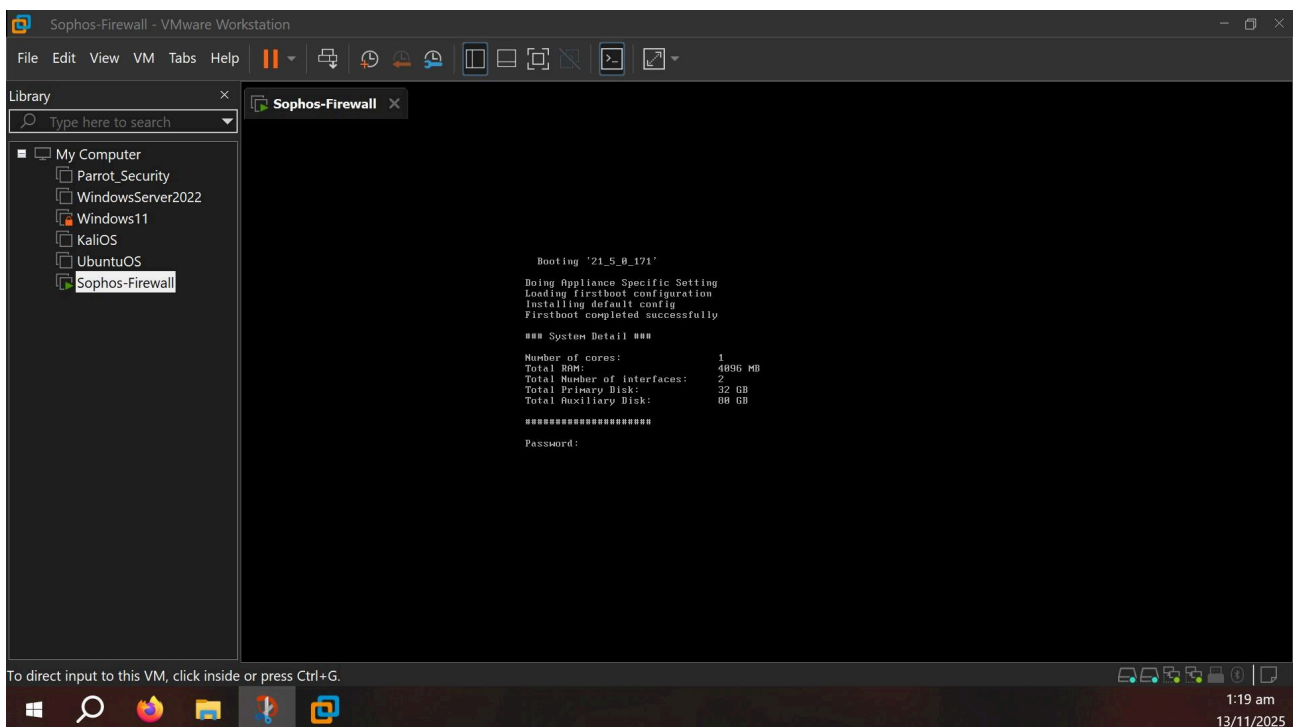
- i. In the Library panel, located on the left side of the **VMware Workstation Pro** main interface, select **Sophos-Firewall**. In the **Sophos-Firewall** tab, select **Power on this virtual machine**.



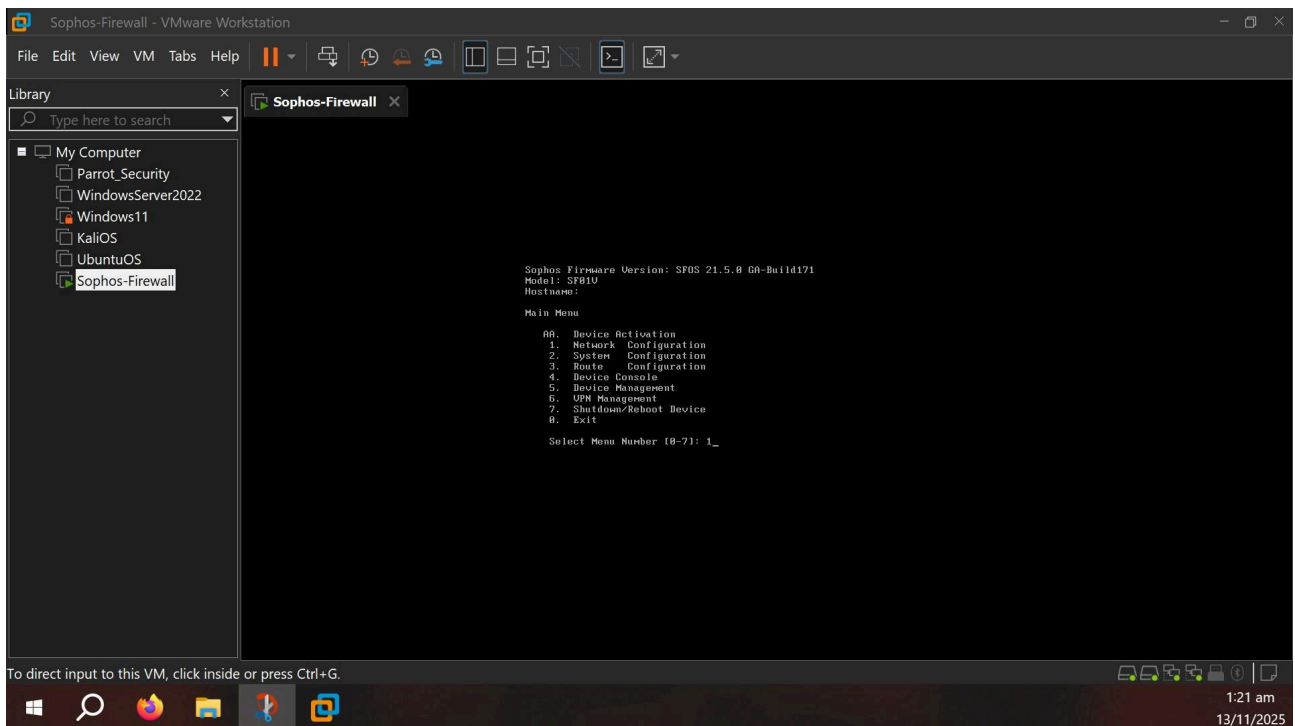
- ii. On the opening bootloader screen, titled **GNU GRUB version 2.02**, select ***21_5_0_171** and press **Enter**.



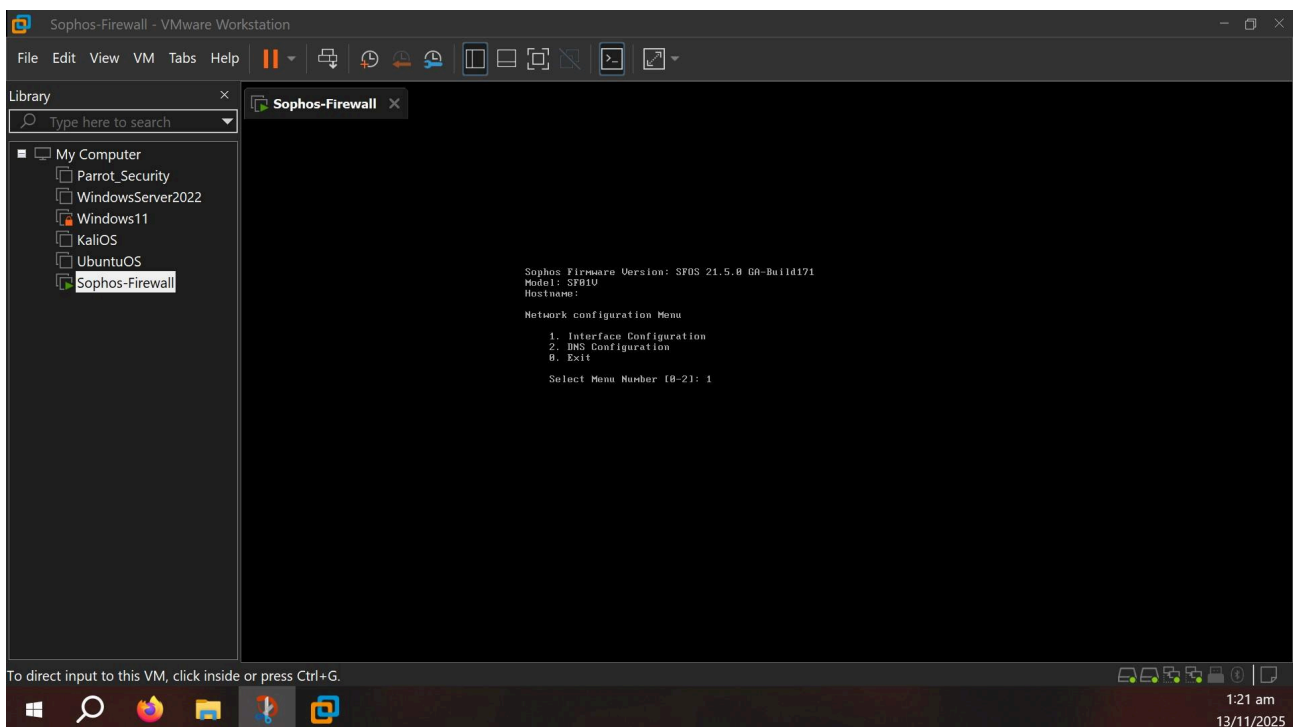
- iii. On the next screen titled **Booting '21_5_0_171'** type the password **admin** and press **Enter**.



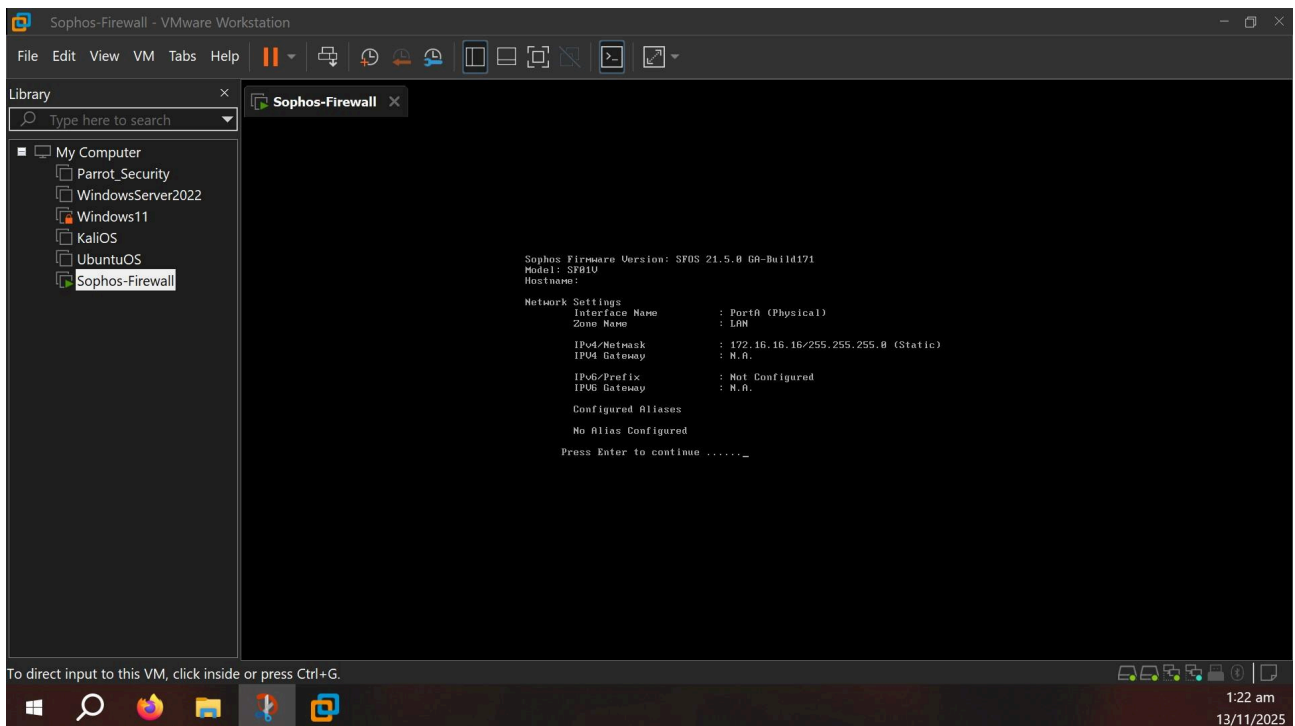
- iv. The next screen is the **Main Menu** screen. Press **1** to select **Network Configuration**. Press **Enter**.



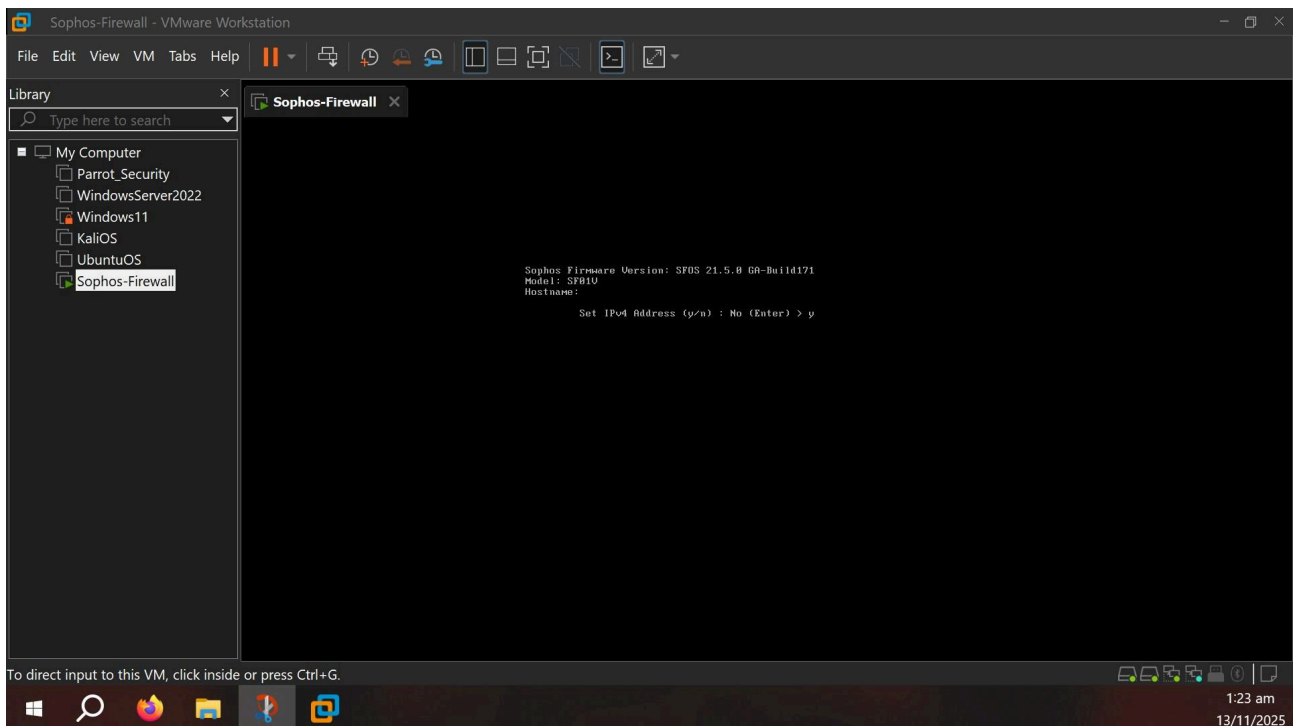
- v. The next screen is the **Network Configuration Menu** screen. Press **1** to select **Interface Configuration**. Press **Enter**.



- vi. The next screen is the **Network Settings** screen. Press **Enter** to continue.

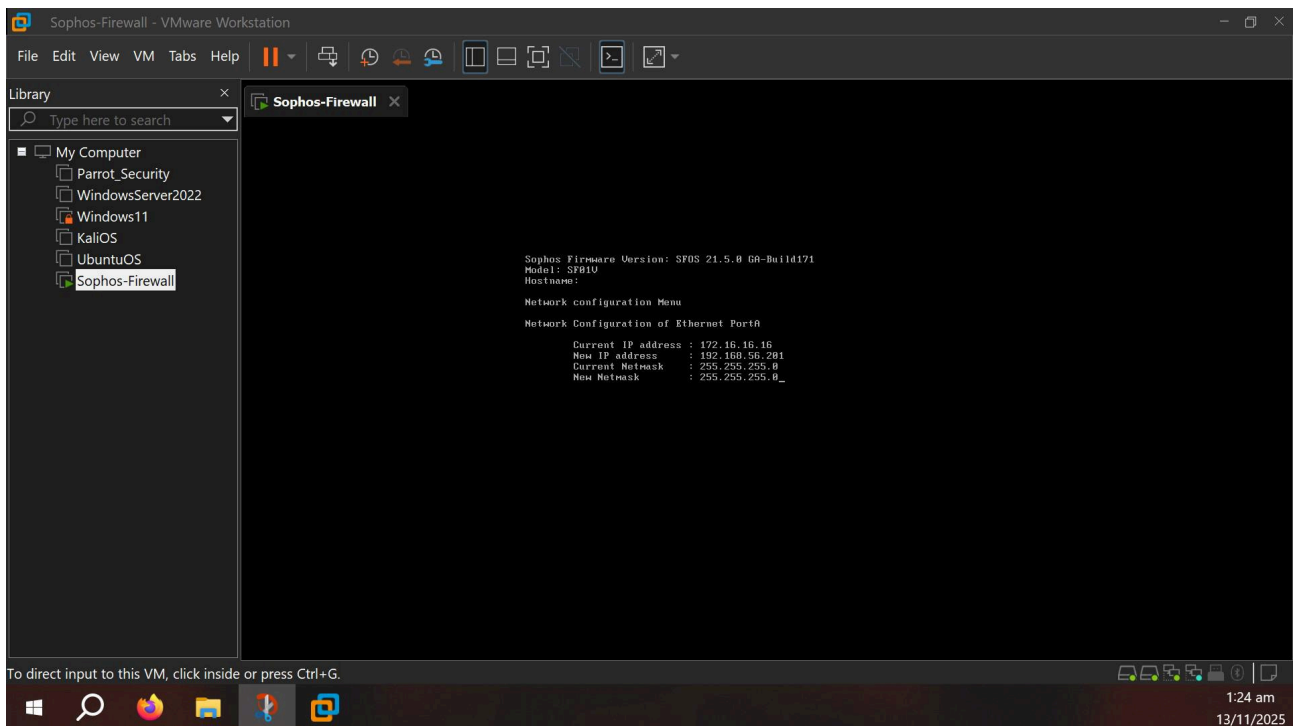


vii. On the next screen with the dialog **Set IPv4 Address (y/n) : No (Enter) >** type **Y**.

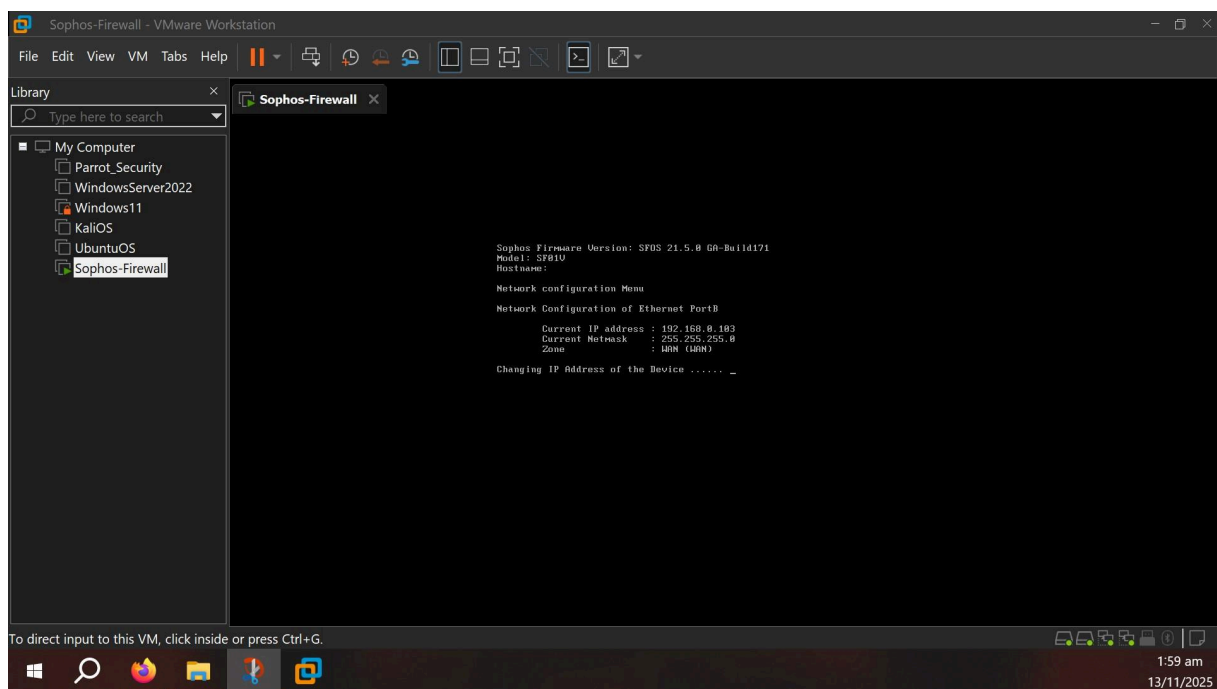


viii. The next screen is the **Network Configuration of Ethernet PortA**.

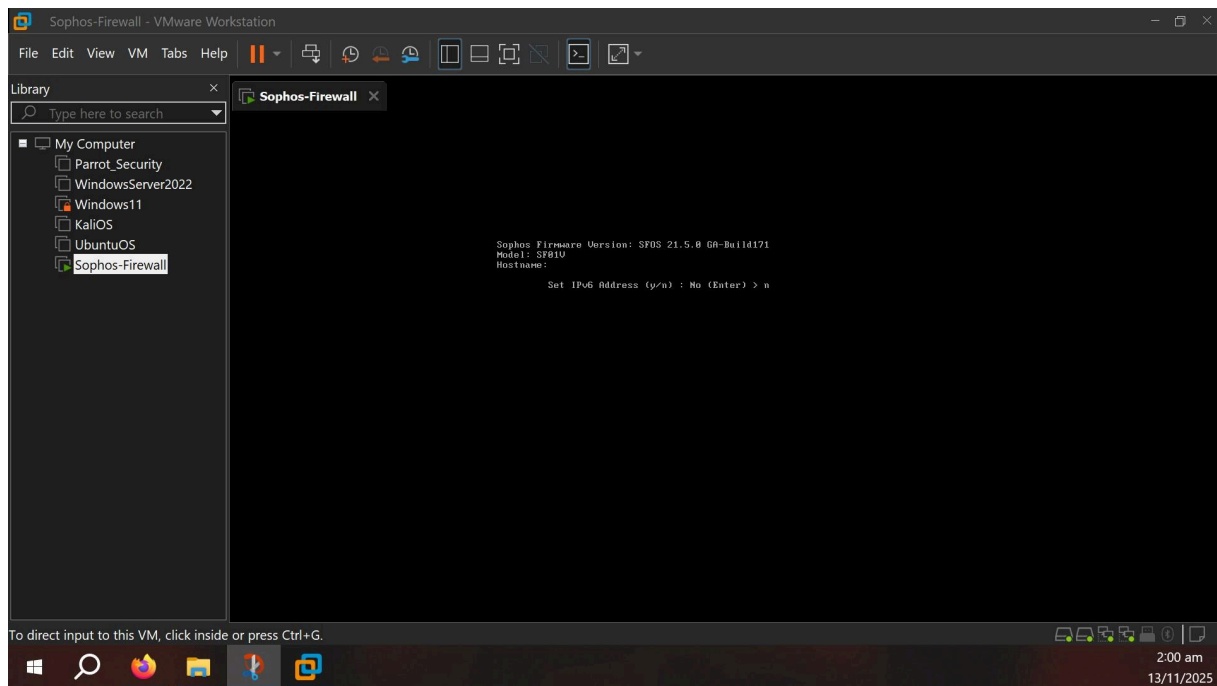
- For **New IP Address** type **192.168.56.201**. Press **Enter**.
- For **New Netmask** type **255.255.255.0**. Press **Enter**.



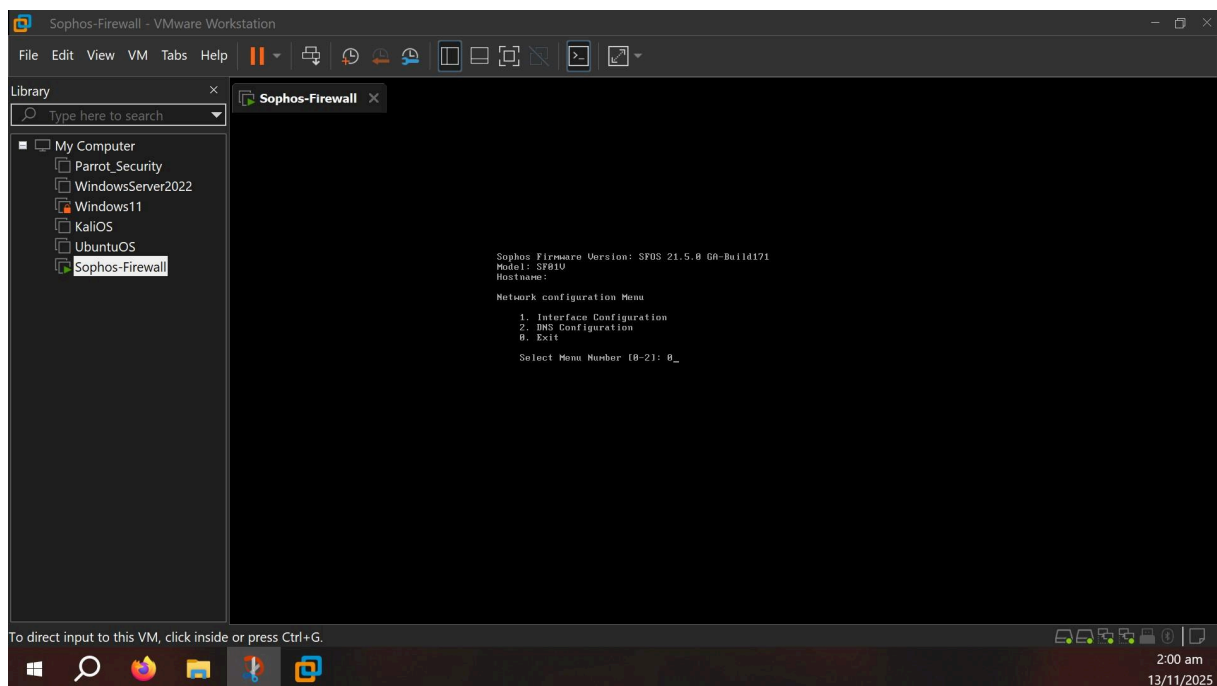
ix. The next screen is the **Network Configuration of Ethernet PortB**. Press **Enter**.



x. On the next screen with the dialog **Set IPv6 Address (y/n) : No (Enter)** > type **N**.



- xi. The next screen is the **Network configuration Menu** screen. Press **0** to select **Exit**. Press **Enter**.

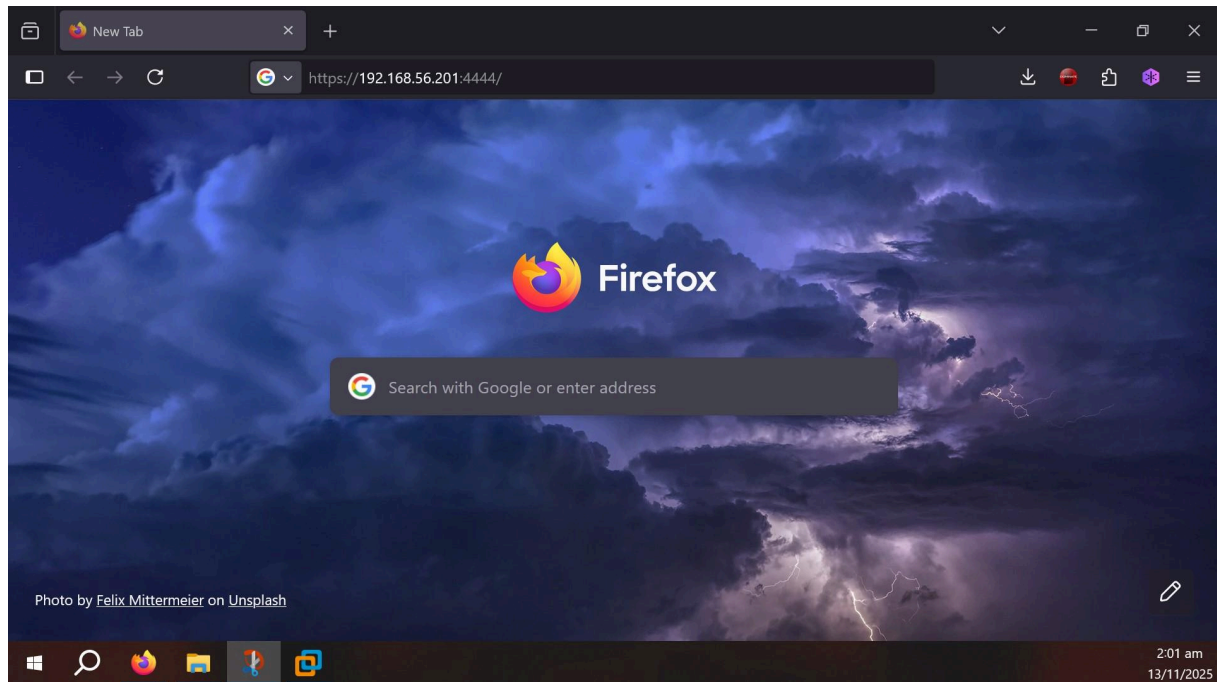


- xii. The next screen is the **Main Menu** screen.

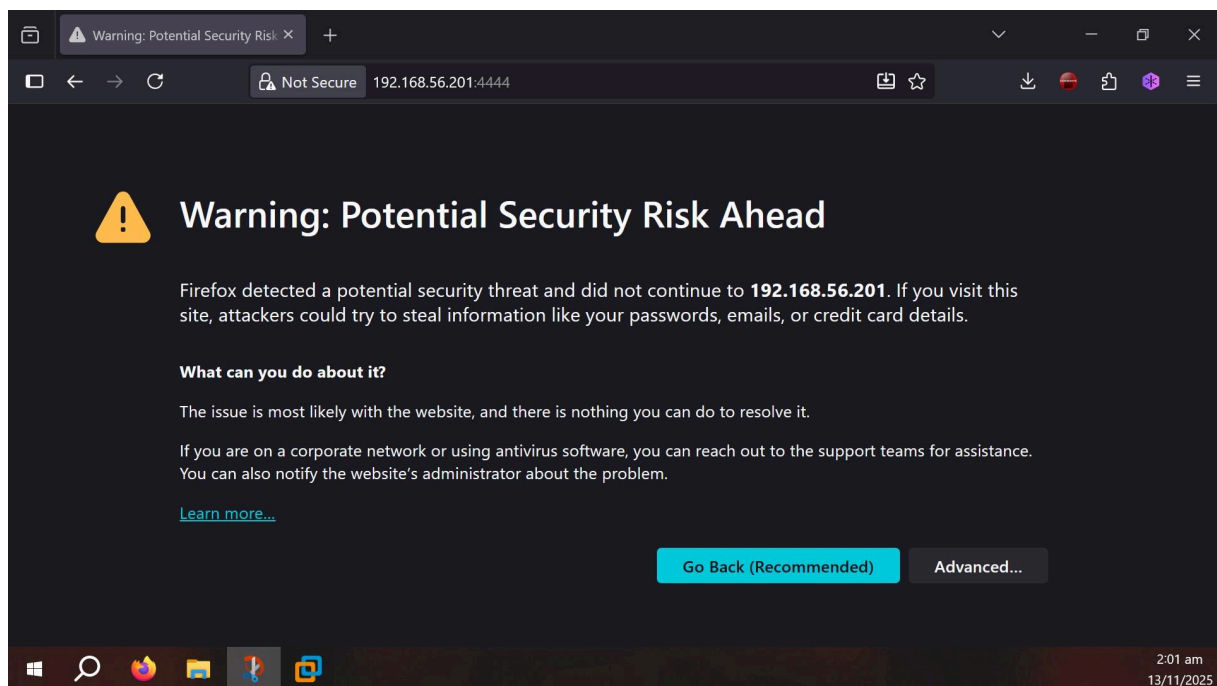
Step 5: Firewall Web Admin Console Setup

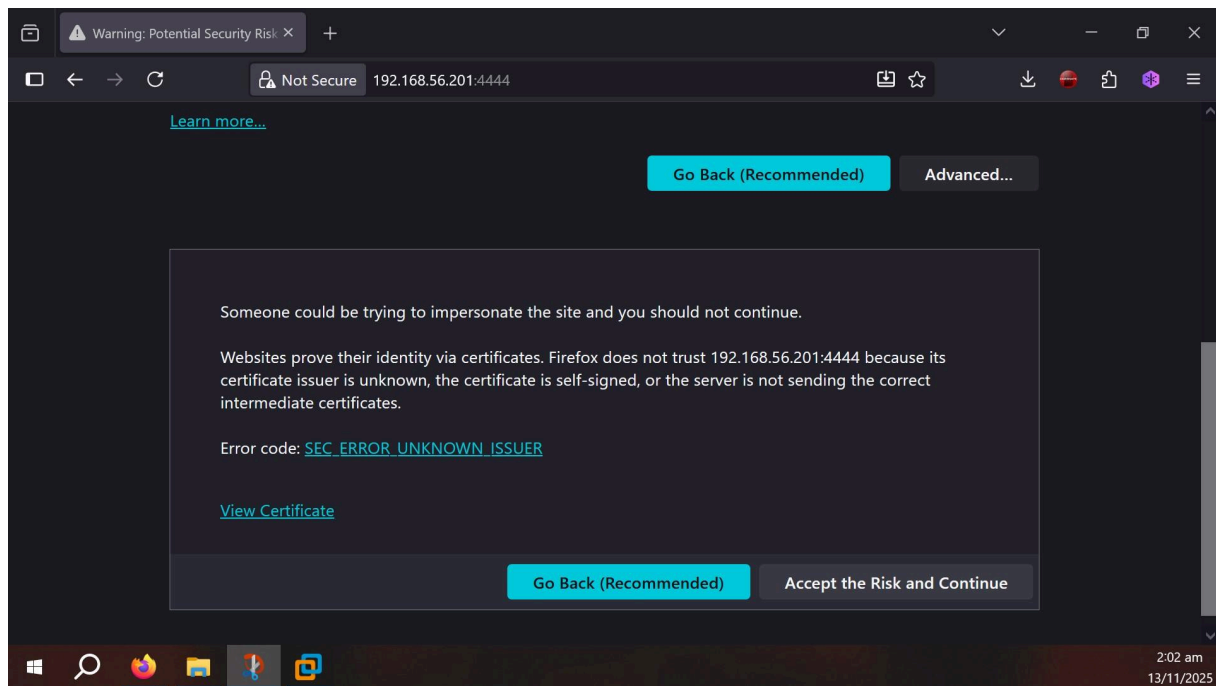
a. Setup the Firewall in the Web Admin Console

- i. Keep VMware running but minimized, then launch a browser (**Firefox**) and navigate to the Sophos Firewall setup interface by typing <https://192.168.56.201:4444> into the address bar and pressing **Enter**.

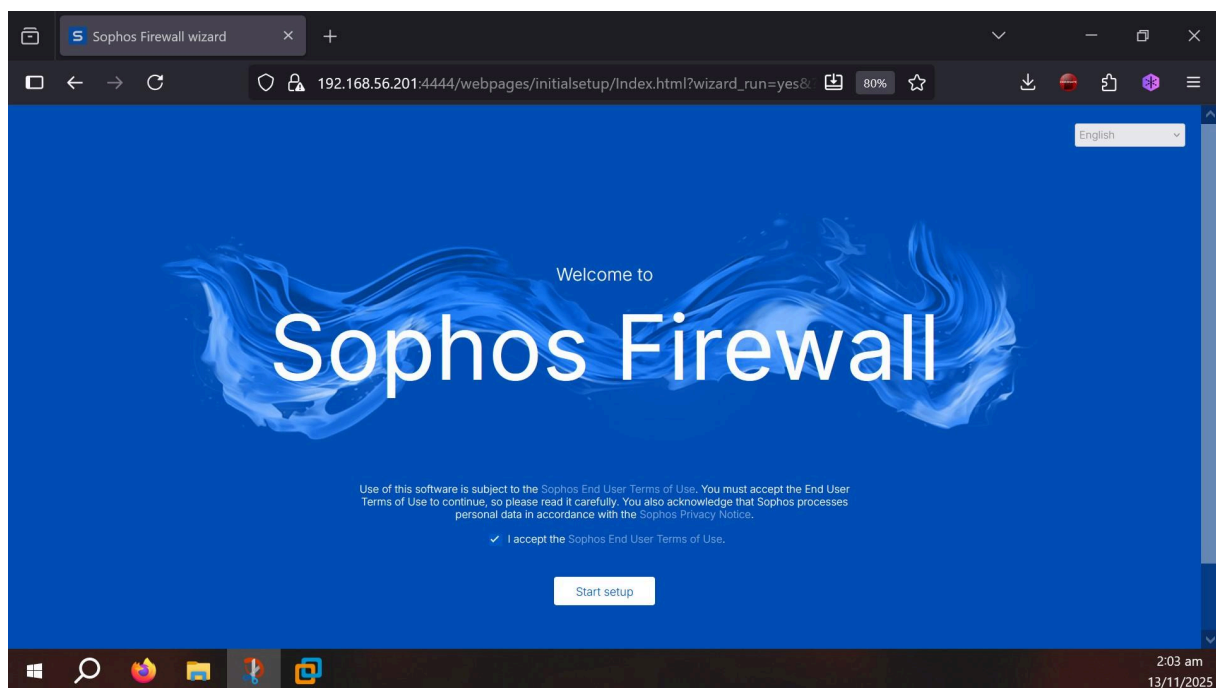


- ii. A notice page with the text **“Warning: Potential Security Risk Ahead”** appears because the port is not recognized by the browser as secure.
- Click the **Advanced...** button.
 - Click the **Accept the Risk and Continue** button.



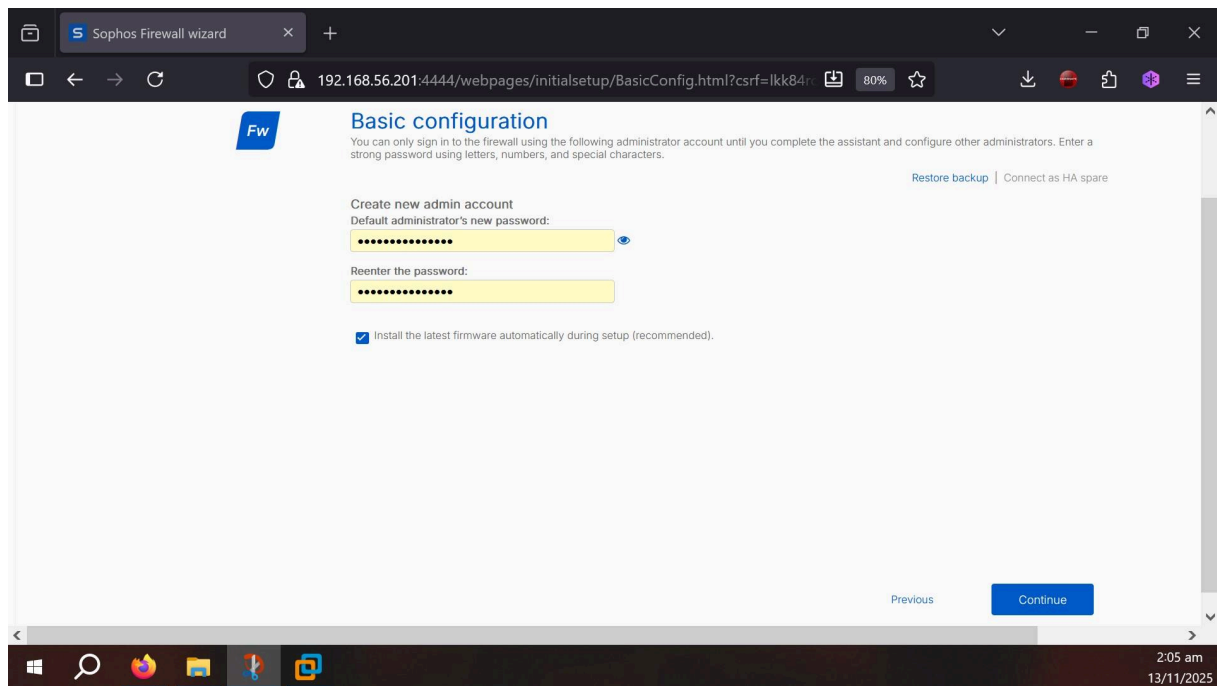


iii. The **Sophos Firewall** initial setup frontpage appears. Click **Start Setup**.



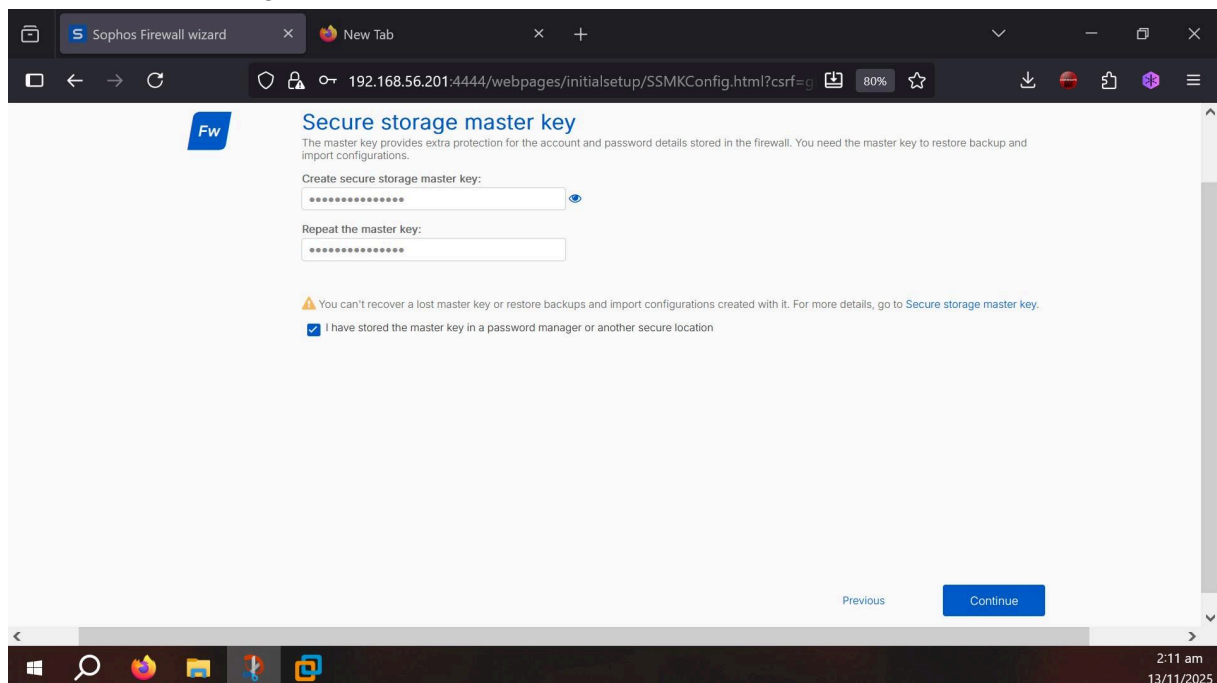
iv. On the **Basic configuration** webpage:

- Create a new administrator account password by typing it and re-typing it in the **Default administrator's new password** text box and the **Reenter the password** text box, respectively.
- Click the **Continue** button. *This opens the **Secure storage master key** webpage.*



v. On the **Secure storage master key** webpage:

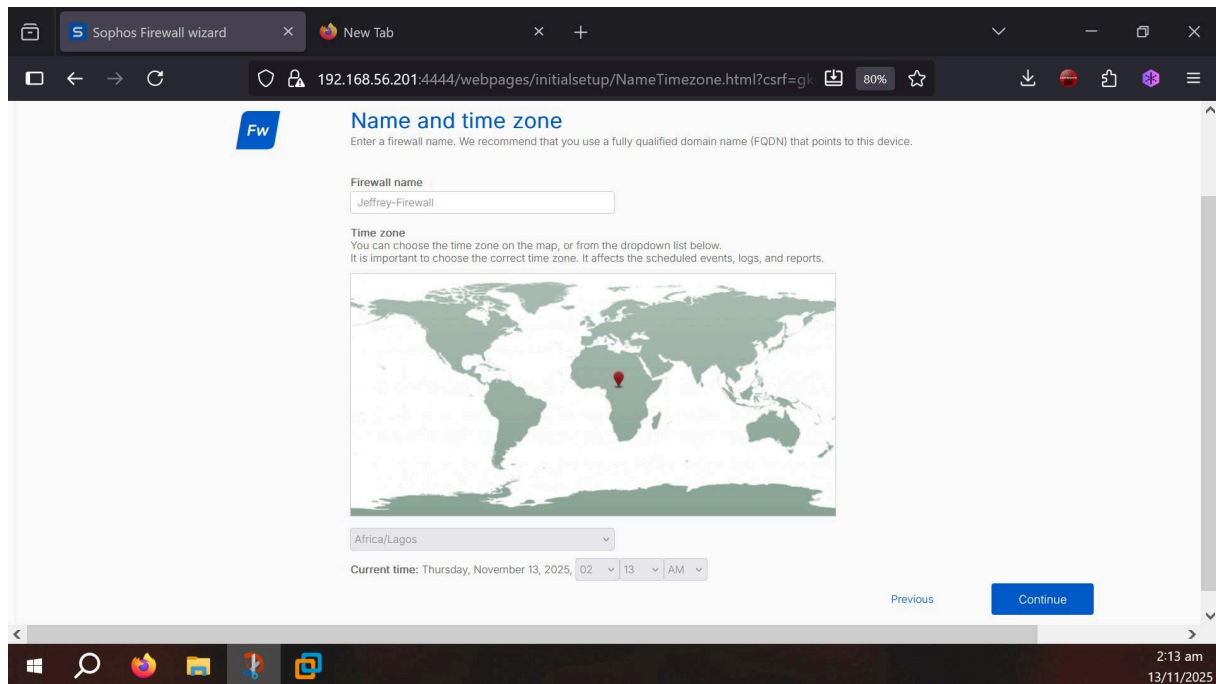
To proceed, you must create a new administrator account password by typing it and re-typing it in the **Create secure storage master key** text box and the **Repeat the master key** text box, respectively, and then check the **I have stored the master key in a password manager or another secure location** checkbox before clicking the **Continue** button, which will open the **Name and time zone** webpage.



vi. On the **Name and time zone** webpage:

In the Sophos Firewall setup, you must first type a name for the firewall in the **Firewall name** text box. Next, select the appropriate time zone from the dropdown menu and confirm that the time and date displayed in the **Current time** section on the web interface matches the current time on

the operating system. Finally, click the **Continue** button, which will open the **Register your firewall** webpage.



vii. On the **Register your firewall** webpage:

- Click the **I have an existing serial number** button.
- Since there is no serial number, it is time to register for one.

b. **Acquire serial number for free trial access.**

- While keeping the current browser tab open, open a new tab and visit the **Sophos Firewall free trial** webpage at [\[https://www.sophos.com/en-us/products/next-gen-firewall/free-trial\]](https://www.sophos.com/en-us/products/next-gen-firewall/free-trial). On this page, you must fill out and submit the registration form by entering the required details (First Name, Last Name, Email, Company, Number of Employees, Job role, Phone number, Country, and State), clearing the CAPTCHA, and clicking the **Submit** button.

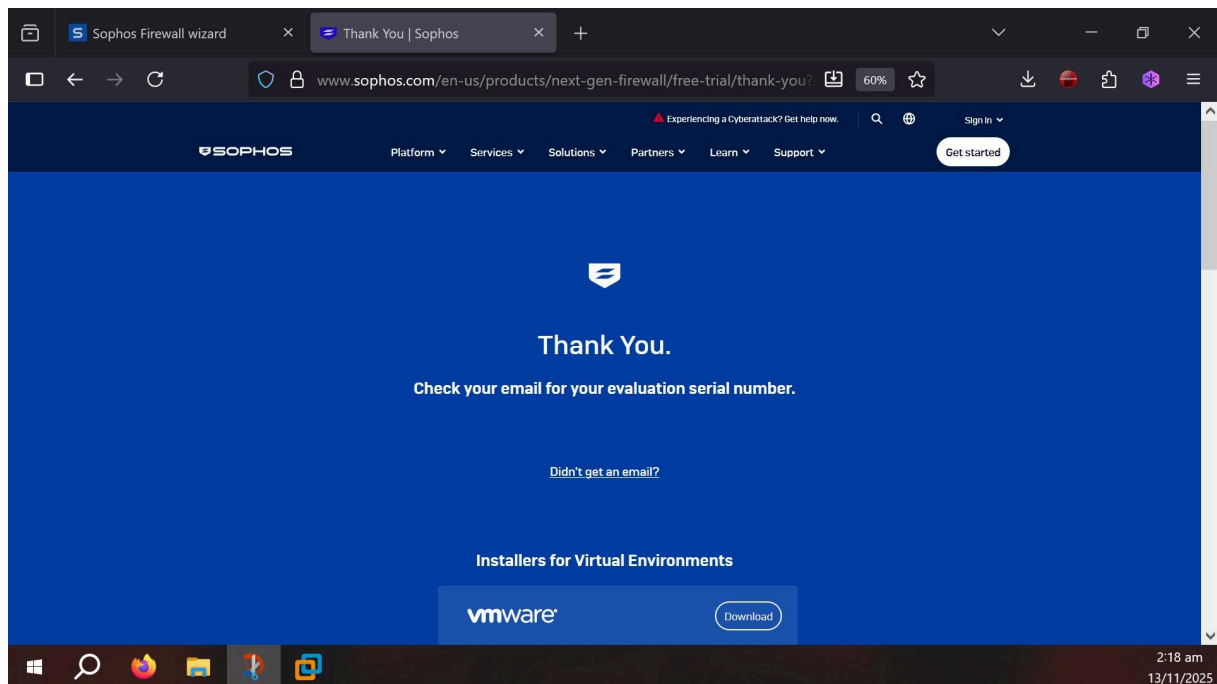
The screenshot shows the Sophos Firewall free trial registration page. The page has a blue header with the Sophos logo and navigation links: Overview, Features, Compare Models, Ecosystem, Central, Free Trial (selected), and How to Buy. The main content area is titled "Sophos Firewall free trial" and includes a sub-header "Sophos Firewall spots hidden risks other firewalls miss and automatically isolates active threats". Below this, there are three bullet points describing the features: "Blocks unknown threats with a comprehensive suite of advanced protection that includes intrusion prevention system (IPS), active threat prevention (ATP), sandboxing, dual antivirus (AV), web and app control, anti-phishing, a full-featured web application firewall, and more.", "Automatically responds to incidents by instantly identifying infected systems and isolating them until they can be cleaned up", and "Exposes hidden risks on your network, including unknown apps, top-risk users, advanced threats, suspicious payloads, and more".

Below the bullet points, there are "TWO EASY OPTIONS" listed: "1) Request a free trial with Sophos by submitting the form." and "2) Start your free trial through AWS Marketplace - for a streamlined procurement via your AWS account (link below)". A "Try free with AWS" button is present.

The registration form on the right includes the following fields: First Name (Jeffrey), Last Name (O), Business Email (redacted), Company (AltSchool Africa), Number of Employees (0-50), Job role (Home User/Student/Fa...), Phone number (redacted), Country (Nigeria), and State (Laos). There is a checkbox for "I agree to all the terms and conditions in the Sophos End User Terms of Use" and a CAPTCHA "I'm not a robot". A "Submit" button is at the bottom right of the form.

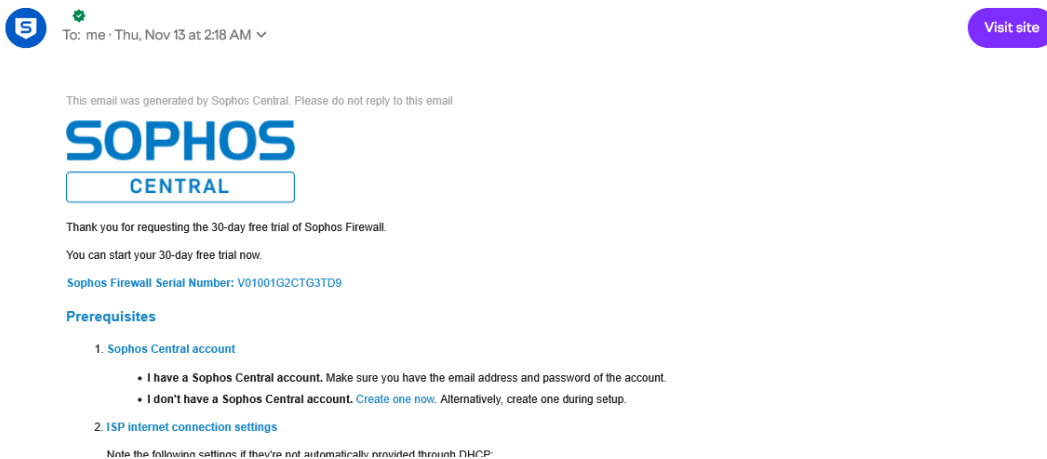
The Windows taskbar at the bottom shows the time as 2:18 am on 13/11/2025.

- ii. A **Thank You** confirmation page opens, instructing you to check your email inbox for the **evaluation serial number**.



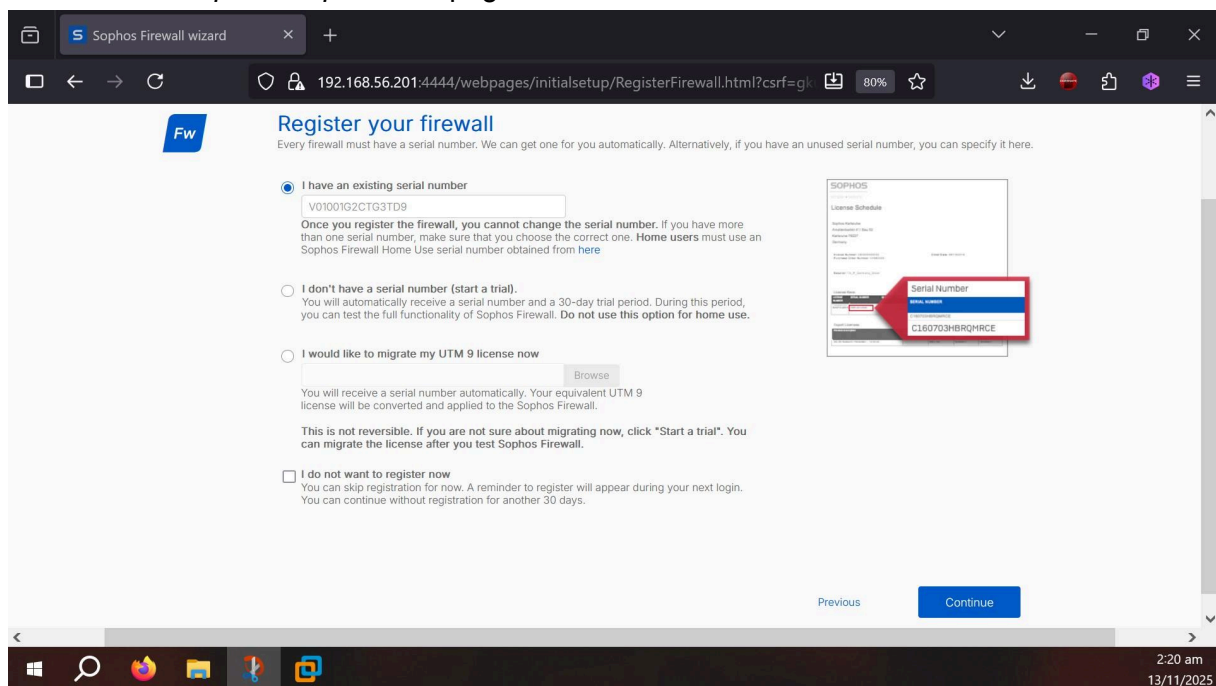
- iii. Locate the serial number in your email inbox and copy it.

Sophos Firewall 30-day free trial - Serial number V01001G2CTG3TD9

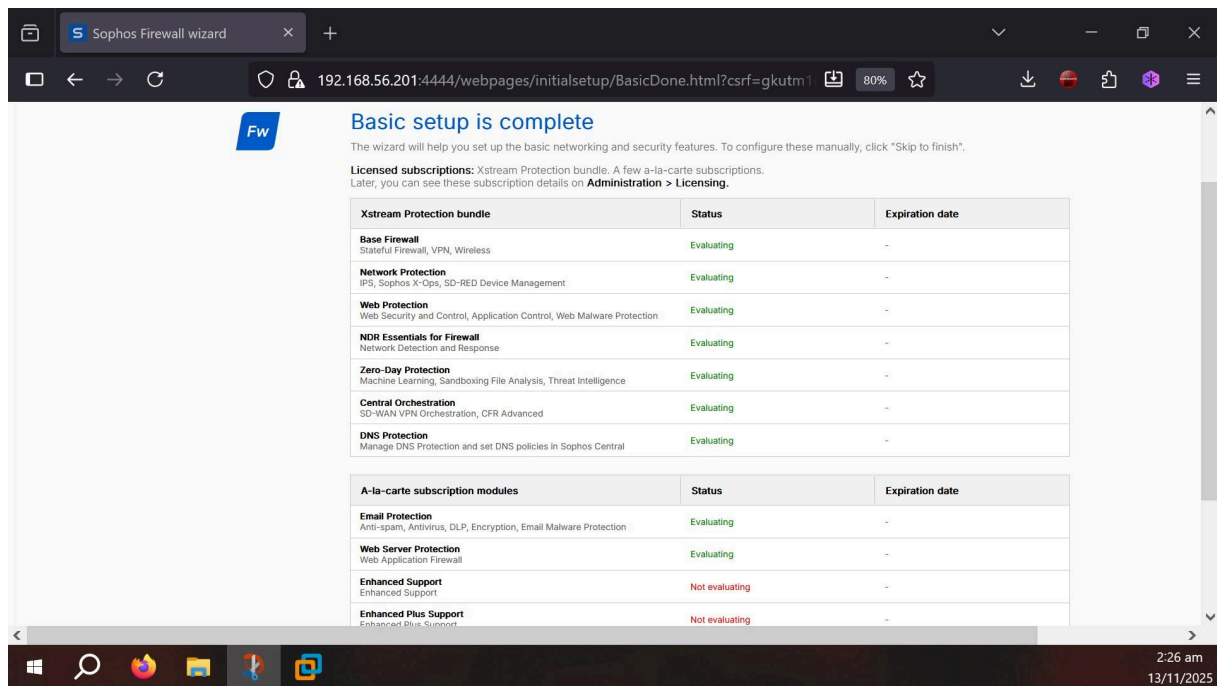


c. Resume Web Admin Console Setup

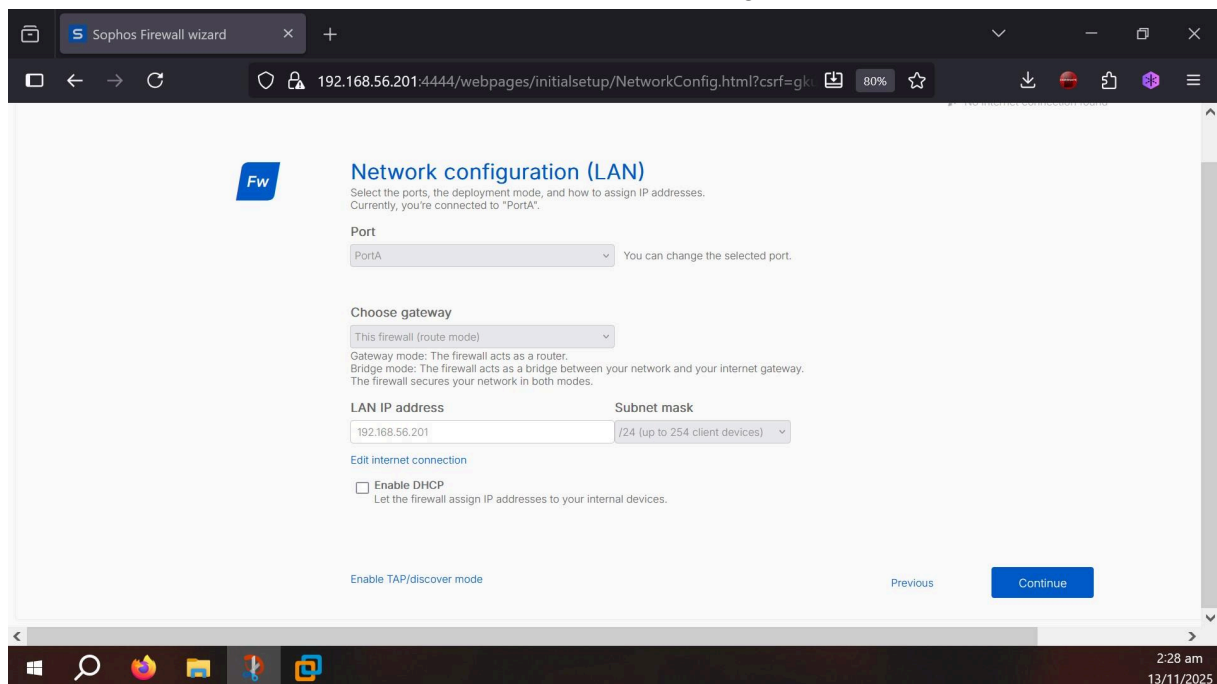
- i. Close the **Thank You** browser tab and return to the **Register your firewall** webpage. On this page, paste the copied serial number into the **I have an existing serial number** text box, and then click the **Continue** button. This opens the *Basic setup is complete* webpage.



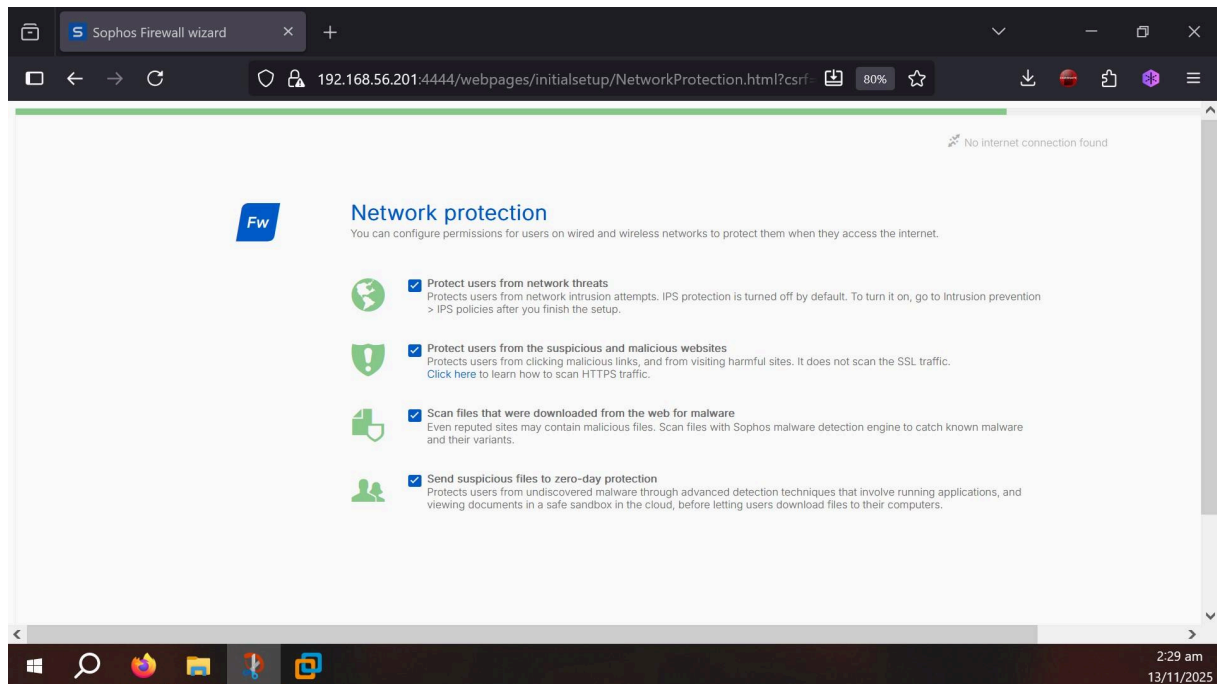
- ii. On the **Basic setup is complete** webpage: review the contents to see the details of the Sophos Firewall subscriptions, and then click the **Continue** button. *This opens the **Network configuration (LAN)** webpage.*



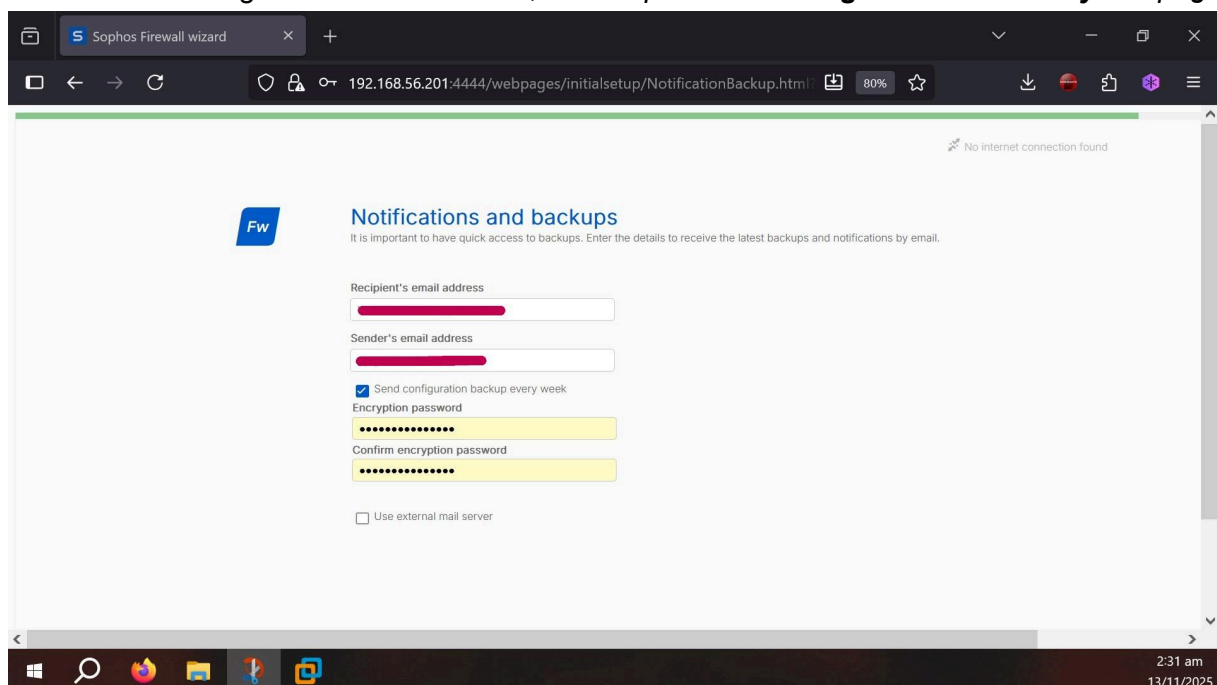
- iii. On the **Network configuration (LAN)** webpage: Confirm the IP address in the **LAN IP address** text box is the same as the previously configured PortA IP address, then uncheck the **Enable DHCP** checkbox before clicking the **Continue** button, which opens the **Network protection** webpage.



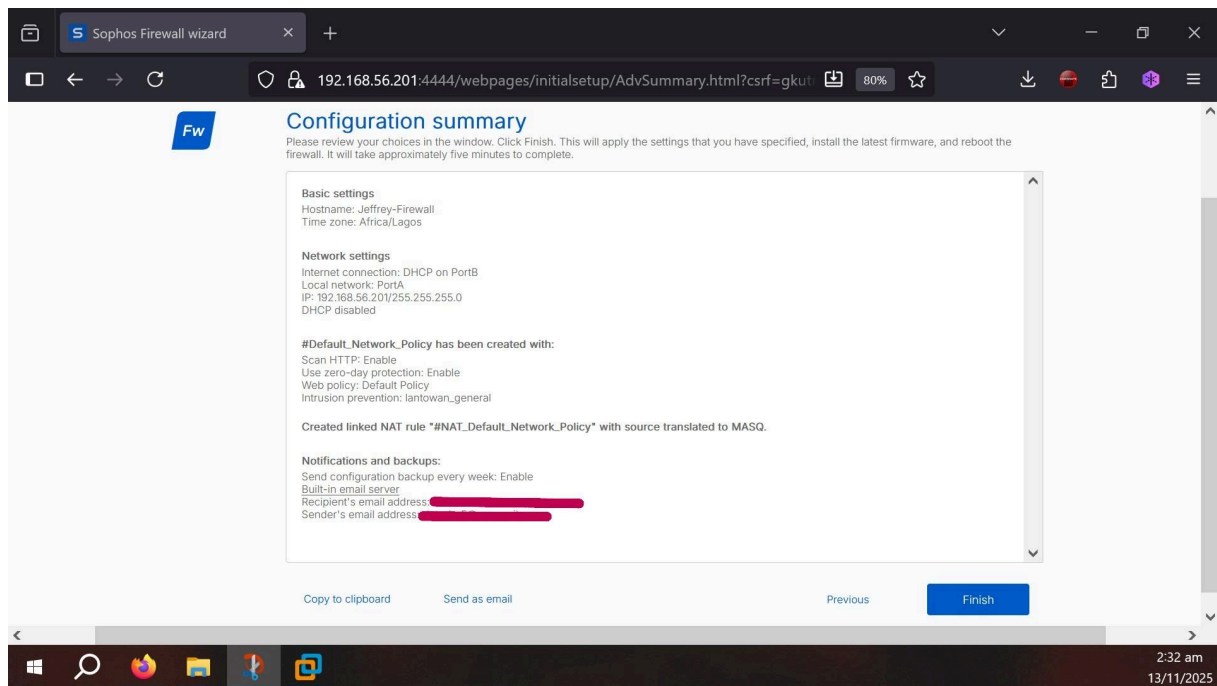
- iv. On the **Network protection** webpage: Ensure the following four checkboxes are selected: **Protect users from network threats**; **Protect users from the suspicious and malicious websites**; **Scan files that were downloaded from the web for malware**; and **Send suspicious files to zero-day protection**. After selecting all four, click the **Continue** button, which will open the **Notifications and backups** webpage.



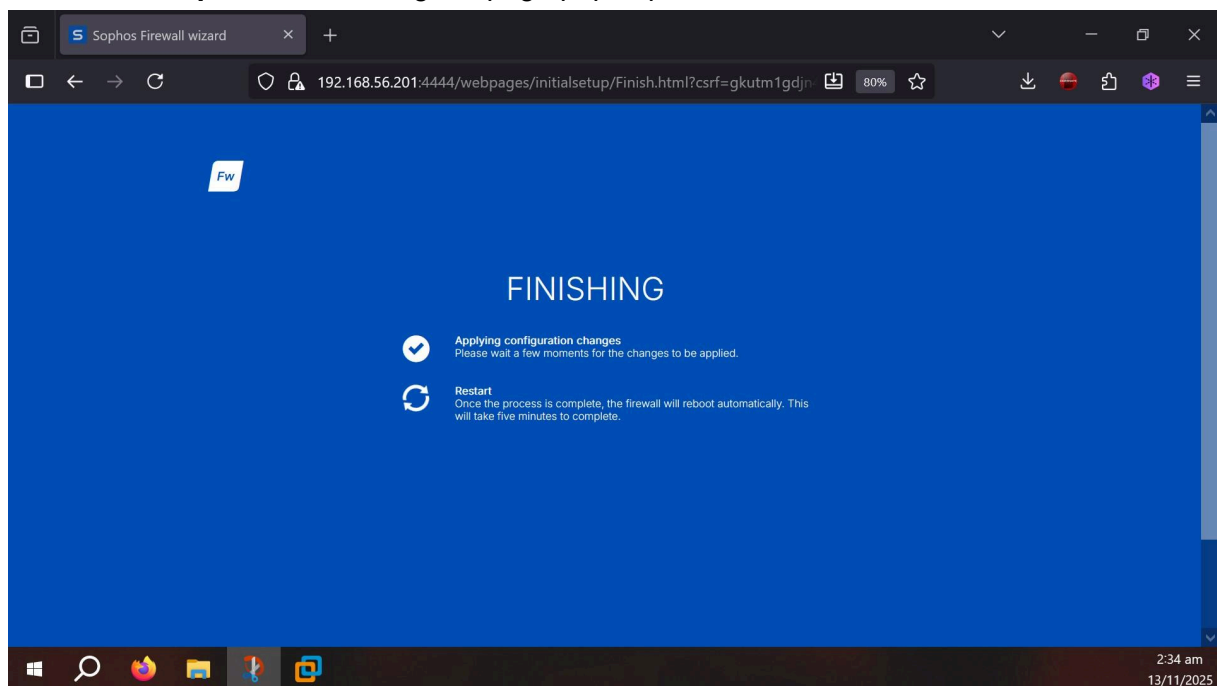
- v. On the **Notifications and backups** webpage: Input the two email addresses for notifications in the **Recipient's email address** and **Sender's email address** text boxes, and then input your encryption password for files and network resources in both the **Encryption password** and **Confirm encryption password** text boxes. Ensure that you leave the **Use external mail server** checkbox unchecked before clicking the **Continue** button, which opens the **Configuration summary** webpage.



- vi. On the **Configuration summary** webpage, you must first review all configuration details in the text area for a final approval before clicking the **Finish** button, which opens the **Finishing** webpage..



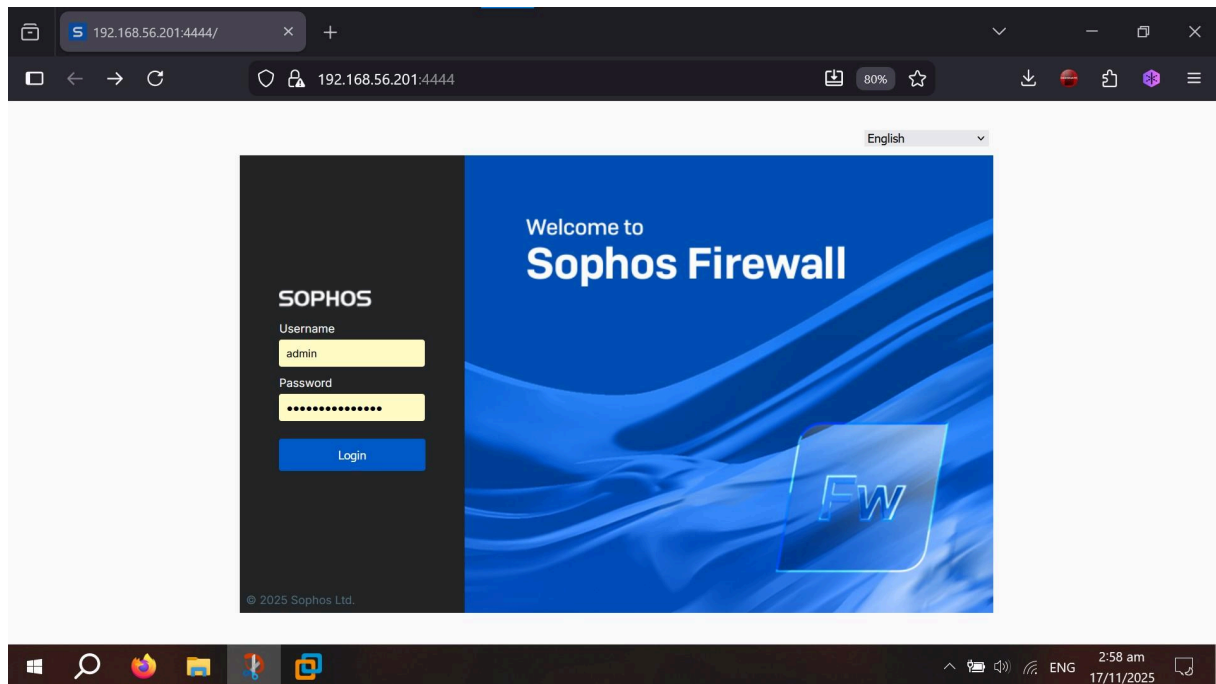
- vii. On the **Finishing** webpage: The loading spinner next to **Applying configuration changes** spins until the action is complete, at which point it changes to a checked circle. Similarly, the loading spinner next to **Restart** spins until the Sophos Firewall VM finishes restarting, after which it also changes to a checked circle, and then a **Sophos Firewall** sign-in page pops up.



Step 6: Firewall Console Access

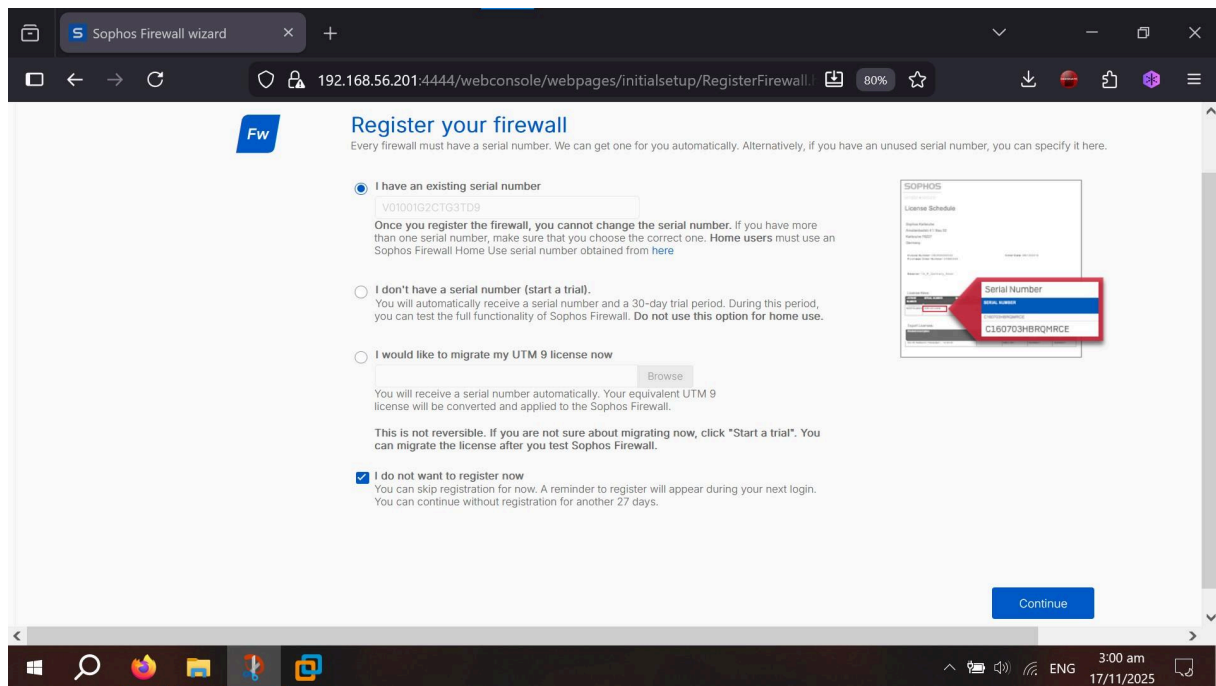
a. Login to the Firewall Console

To sign in to the **Sophos Firewall**, on the sign-in page, enter the username “**admin**” in the **Username** text box and the previously setup password in the **Password** text box, then click the **Login** button, which opens the *Register your firewall* webpage.



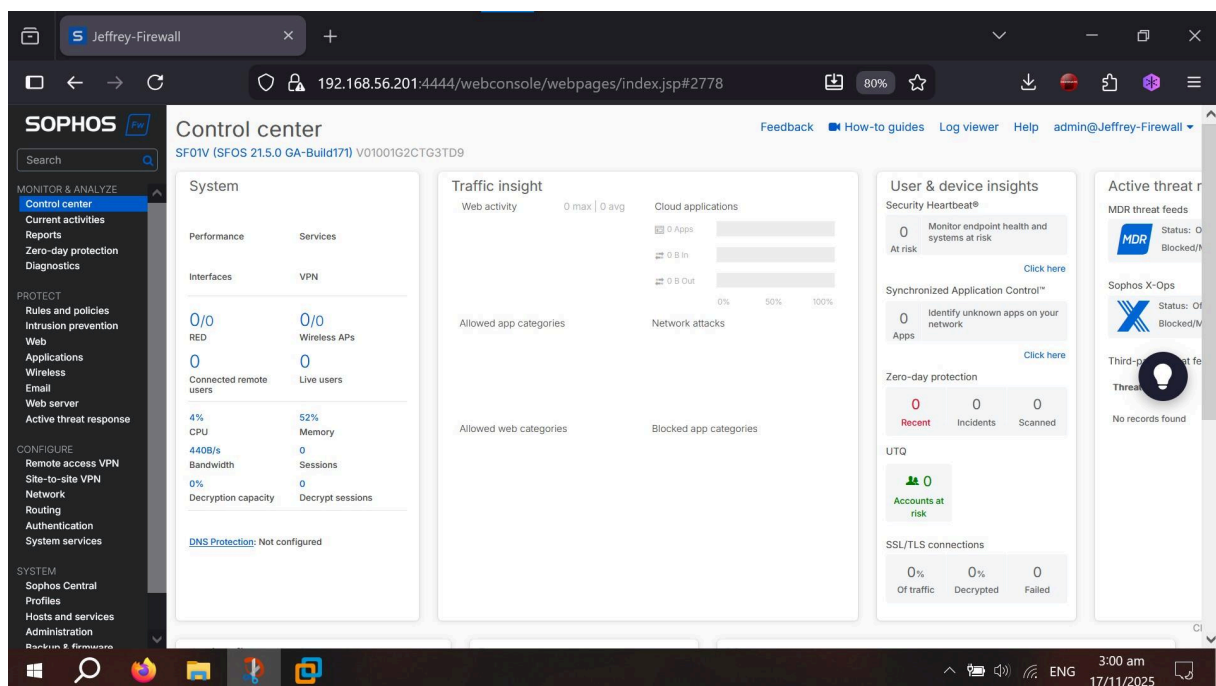
i. On the **Register your firewall** webpage:

The serial number is shown pasted in the **I have an existing serial number** text box, and clicking the **Continue** button leads to an error as the serial number registration and Sophos account authentication process fails; therefore, you must return to the page, check the **I do not want to register now** checkbox, and click the **Continue** button again, which opens the *Control center* interface.



b. Access the Control Center

- The main Firewall interface launches, giving access to the Firewall web console.
- The interface provides access to firewall analytics, controls and configurations.



- Note that despite clicking the **I do not want to register now** checkbox on the **Register your firewall** webpage, the serial number appears on the interface.

Conclusion

The Sophos Firewall virtual machine has been added and configured, and is ready for implementation in the lab environment. It is configured with two interfaces: one **Host-only**

port (**Port A**) which is confined to the LAN and another **Bridged** interface (**Port B**) which bridges the firewall to the same physical network the host is connected to, enabling the firewall virtual machine to function as a separate, independent device.

The LAN subnet (**192.168.56.0/24**) has been configured on the virtualizer and this will be utilized by other virtual machines in the lab.

Security Policy 1

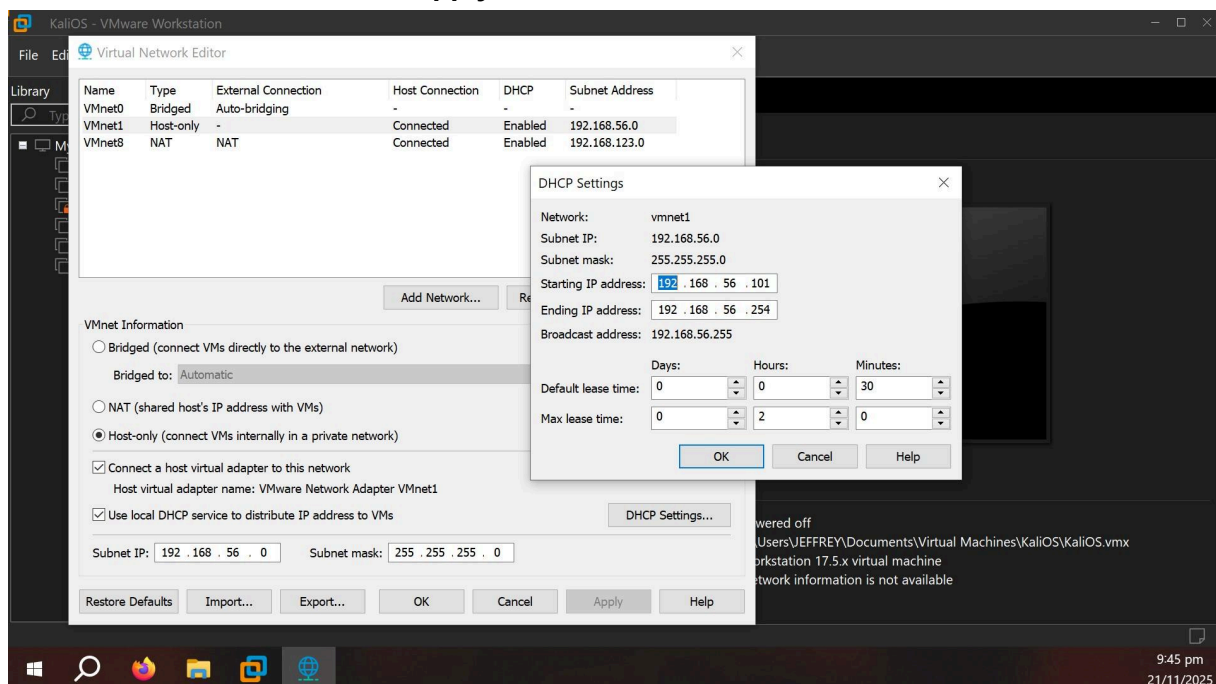
NAT Gateway

This configuration enables the firewall to serve as a gateway for the Host-only configured virtual machines in the LAN. The firewall provides Network Address Translation using its 2 interfaces with one in the LAN (Port A; Host-only; 192.168.56.201/24) and the other, facing the WAN (Port B; Bridged; 192.168.0.103/24). A Kali OS virtual machine (**KaliOS**) will be used to test this configuration.

Step 7: Confirm Network Settings

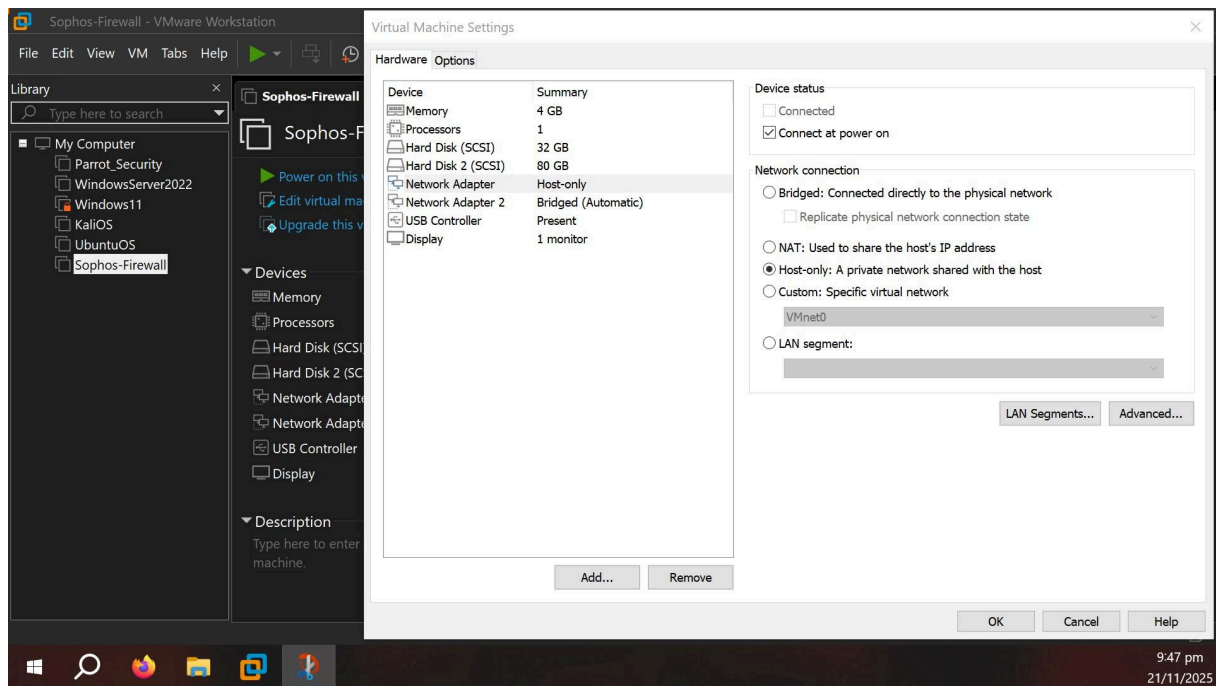
a. Confirm Network Adapter Settings for Virtualizer (VMware Workstation Pro 17.5).

Launch the **Virtual Network Editor** (As outlined in [Step 4a] above) and confirm the following settings: VMnet1 **Type** is set to **Host Only** with a **Subnet IP** of 192.168.56.0 and **Subnet mask** of 255.255.255.0, configured to **Use local DHCP** with limits 192.168.56.101—192.168.56.254 in the **DHCP Settings**; also, VMnet8 **Type** is set to **NAT** with a **Subnet IP** of 192.123.56.0 and **Subnet mask** of 255.255.255.0. Click the **Apply** button and then the **OK** button.



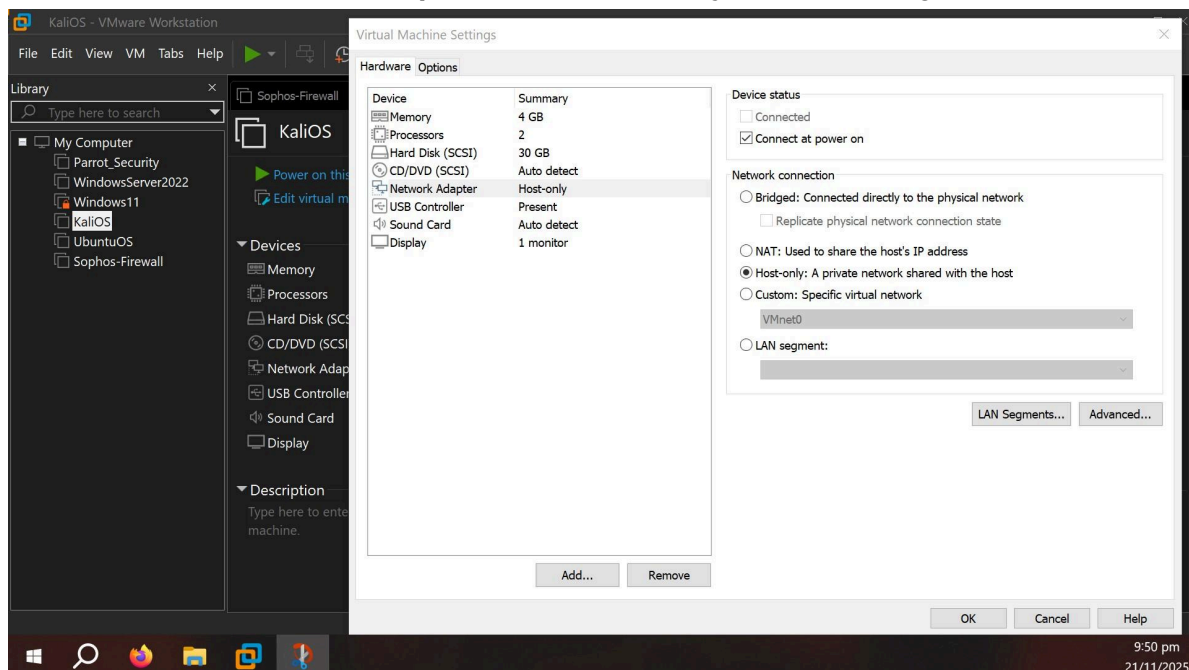
b. Confirm Network Adapter Settings for the Sophos Firewall (SFOS) virtual machine (Sophos-Firewall).

To begin, launch the **Sophos-Firewall** virtual machine **Settings**, then confirm that **Network Adapter** is set to **Host-only**; and **Network Adapter 2** is set to **Bridged**. before clicking **OK**.



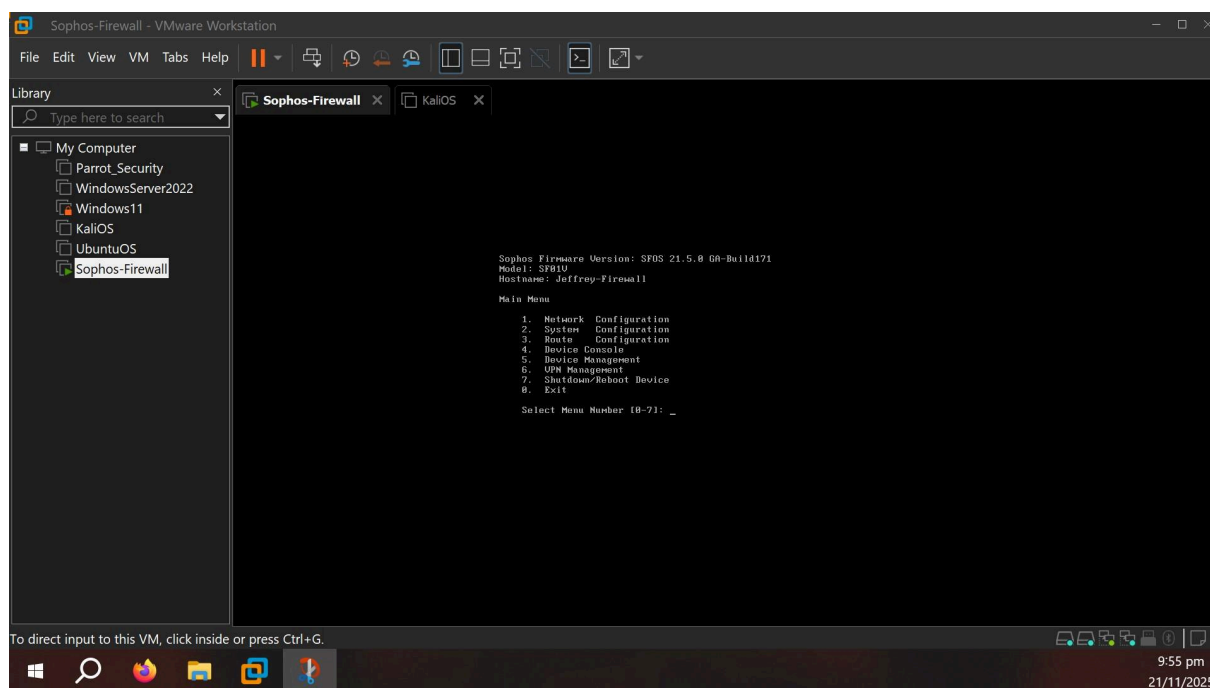
c. Confirm Network Adapter Settings for Kali operating system virtual machine (KaliOS).

To begin the Sophos Firewall setup, launch the **KaliOS** virtual machine **Settings** by right-clicking the **Sophos-Firewall** virtual machine in the Library panel of the **VMware Workstation Pro 17.5** main interface and selecting **Settings...** to open the **Virtual Machine Settings** window, where you must confirm that the **Network Adapter** is set to **Host-only**; before clicking the **OK** button.



Step 8: Launch and Run the Firewall Virtual Machine

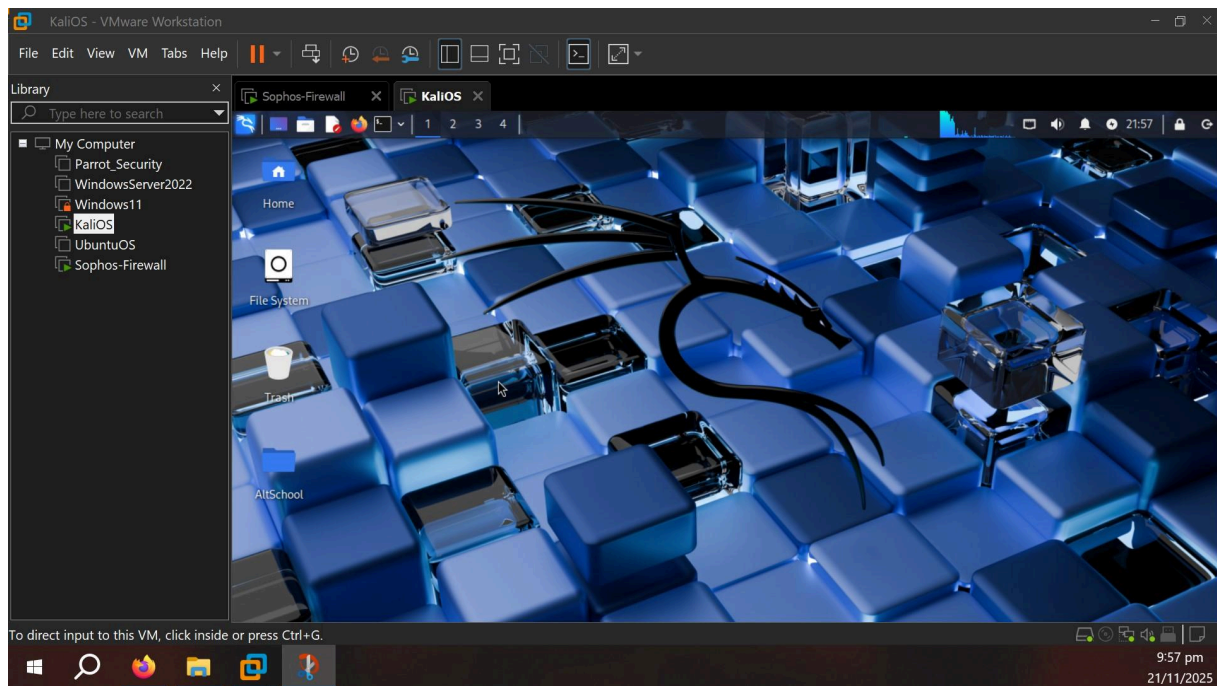
To begin the Sophos Firewall setup. Launch the **Sophos-Firewall Virtual Machine** by selecting **Sophos-Firewall** in the Library panel of **VMware Workstation Pro** and choosing **Power on this virtual machine**. Next, **Login** and run the firewall service by inputting the password at the **Booting** screen and pressing **Enter**, which leads to the **Main Menu** page, and keeping this page open confirms the Firewall is running.



Step 9: Test LAN Virtual Machine Connection

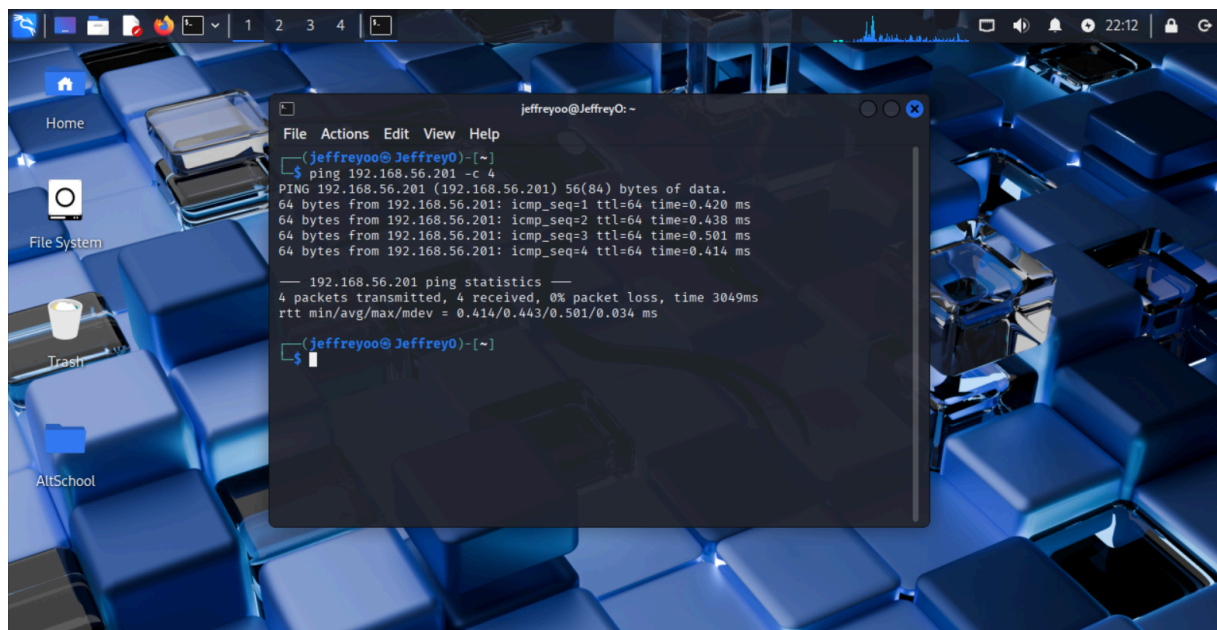
a. Launch the KaliOS Virtual Machine

To power on the **KaliOS** virtual machine, first navigate to the Library panel on the left side of the **VMware Workstation Pro** main interface, select **KaliOS**, and then choose **Power on this virtual machine** in the **KaliOS** tab before inputting the login credentials to access the Desktop.



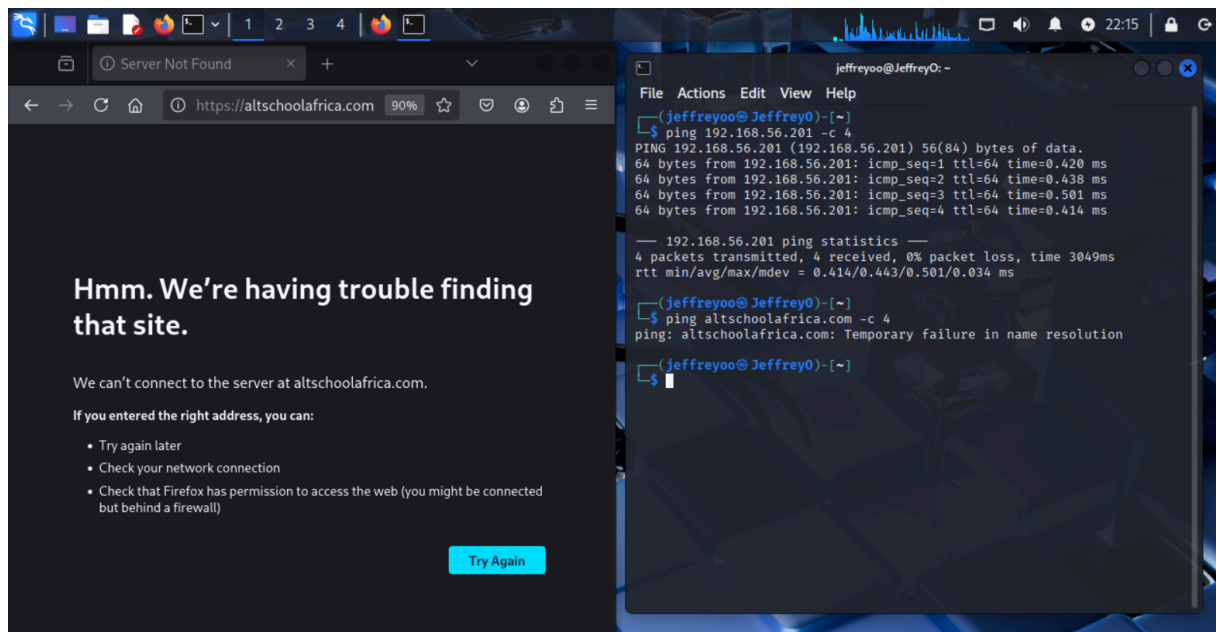
b. Test Firewall Connection

To confirm connectivity to the firewall, first open the **Terminal**. Then, type the command `ping 192.168.56.201 -c 4` to send **4 ICMP echo request packets** to the firewall; the connection is established if the packets return with 0% packet loss.



c. Test Internet Connection

After opening the **Terminal**, the command `ping altschoolafrica.com -c 4` was executed to confirm internet connectivity. The **4 ICMP echo request packets** did not return, resulting in 100% packet loss, which indicated the connection was **NOT** established. This was further confirmed by launching a browser (**Firefox**) and visiting <https://altschoolafrica.com/>, which returned a connection error message. This result establishes that both the KaliOS virtual machine and the Firewall require configuration to enable internet access.



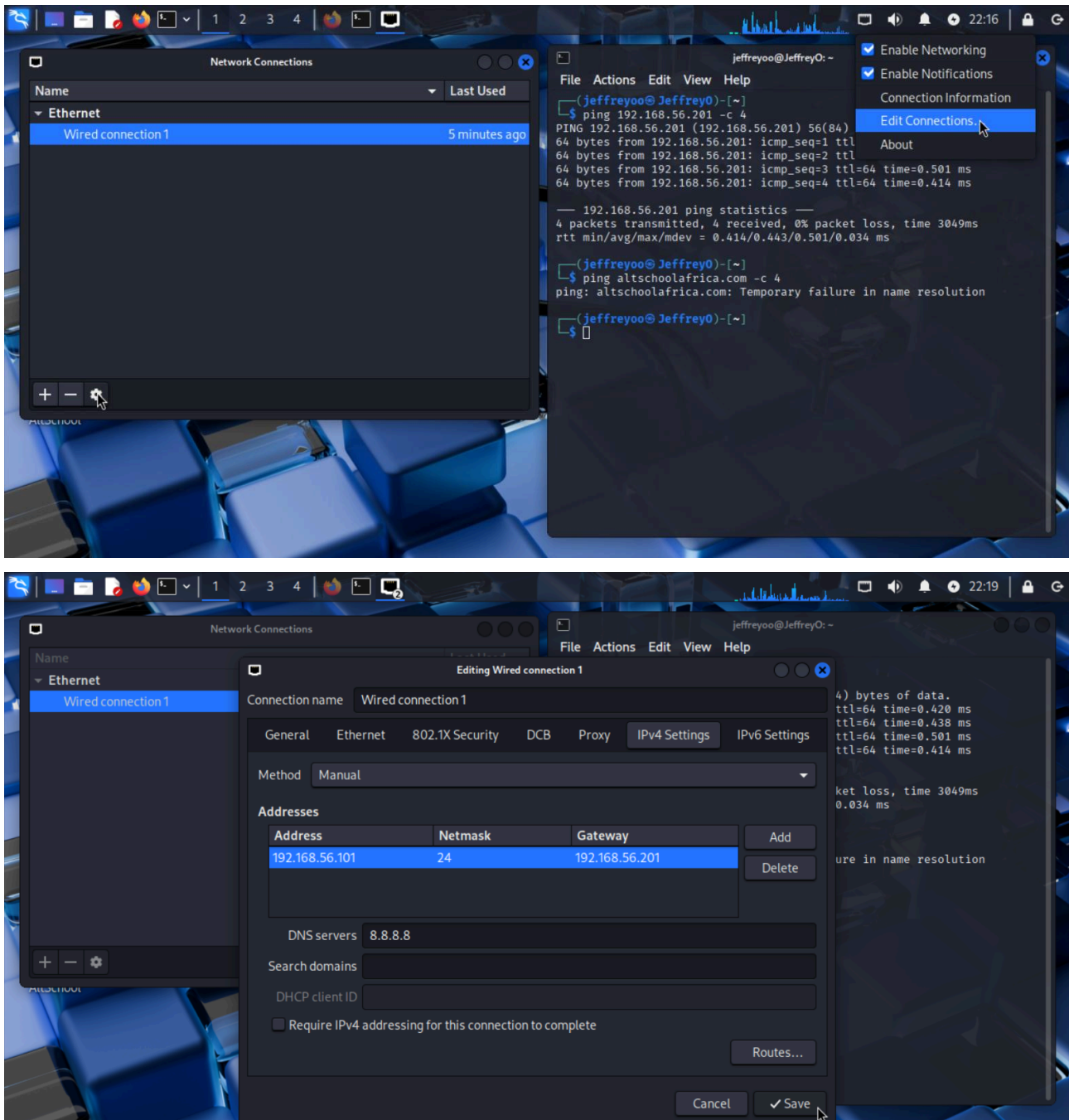
Step 10: Configure the KaliOS Virtual Machine Network Settings

a. Launch the KaliOS Network Settings Window

To access the network connection settings, locate the **Network Manager** icon on the Desktop taskbar, right-click it, and select **Edit Connections** to open the **Network Connections** window. Within this window, click the **Ethernet** drop-down menu, select **Wired connection 1**, and then click the gear icon to open the **Editing Wired connection 1** window.

b. Configure the KaliOS Network Settings

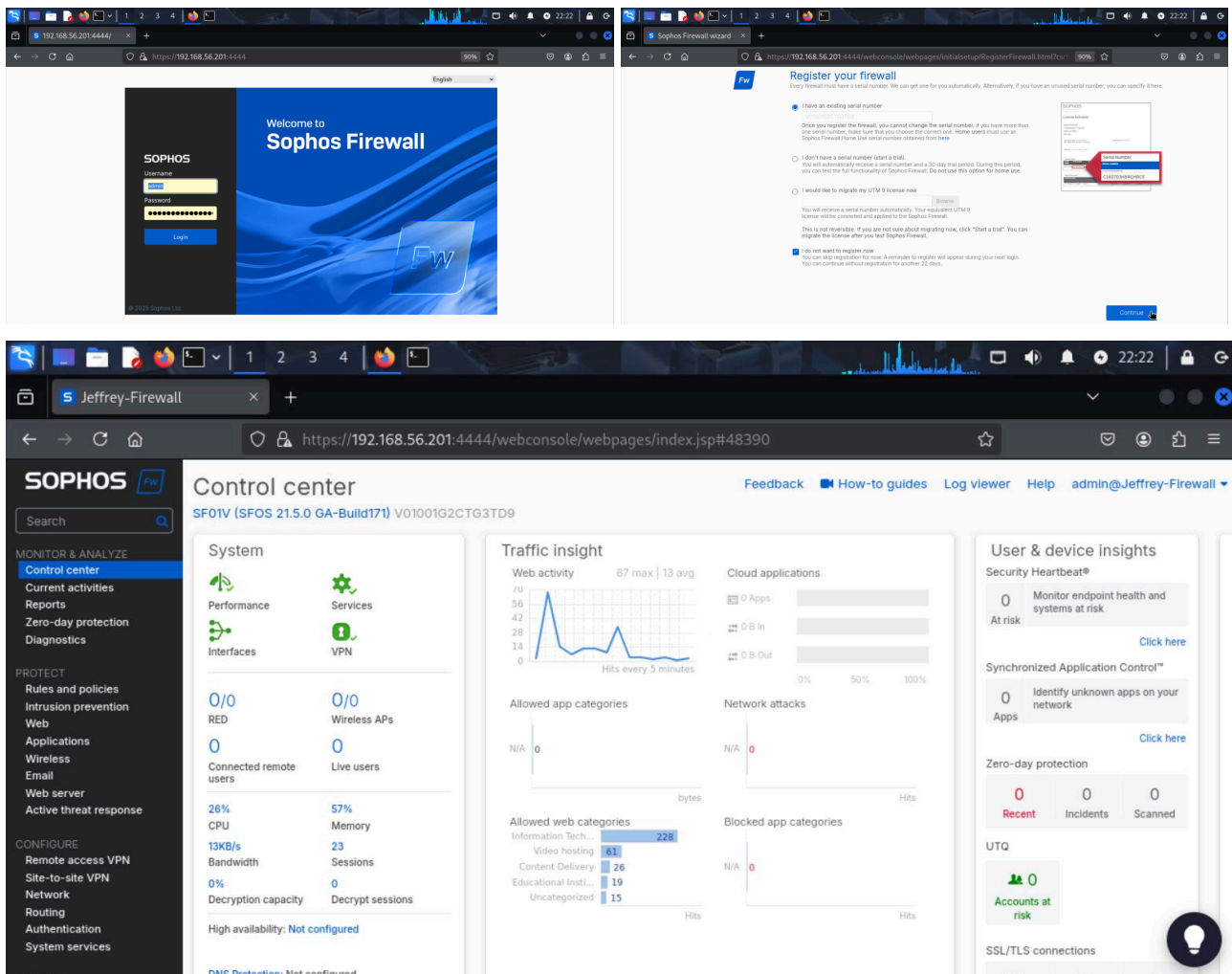
To configure the wired connection, go to the **IPv4 Settings** tab in the **Editing Wired connection 1** window and select **Manual** from the **Method** drop-down menu. Next, click **Add** in the **Addresses** section and configure the new entry with **Addresses** as **192.168.56.101**, **Netmask** as **24**, and **Gateway** as **192.168.56.201**. Finally, input **8.8.8.8** (Google DNS) in the **DNS servers** text box and click the **Save** button.



Step 11: Access the Firewall Using the Web Console

a. Launch the Sophos-Firewall Web Console

To begin, launch Firefox on the KaliOS VM Desktop and enter **192.168.56.201:4444** (the Firewall VM's LAN interface IP address) in the address bar to open the *Sophos Firewall Login* page. After inputting the credentials and clicking **Login**, which leads to the *Register your firewall* page, ensure the **I have an existing serial number** button is selected with the serial number pasted, then check the **I do not want to register now** box, and click **Continue** to access the web console titled **Control center**.



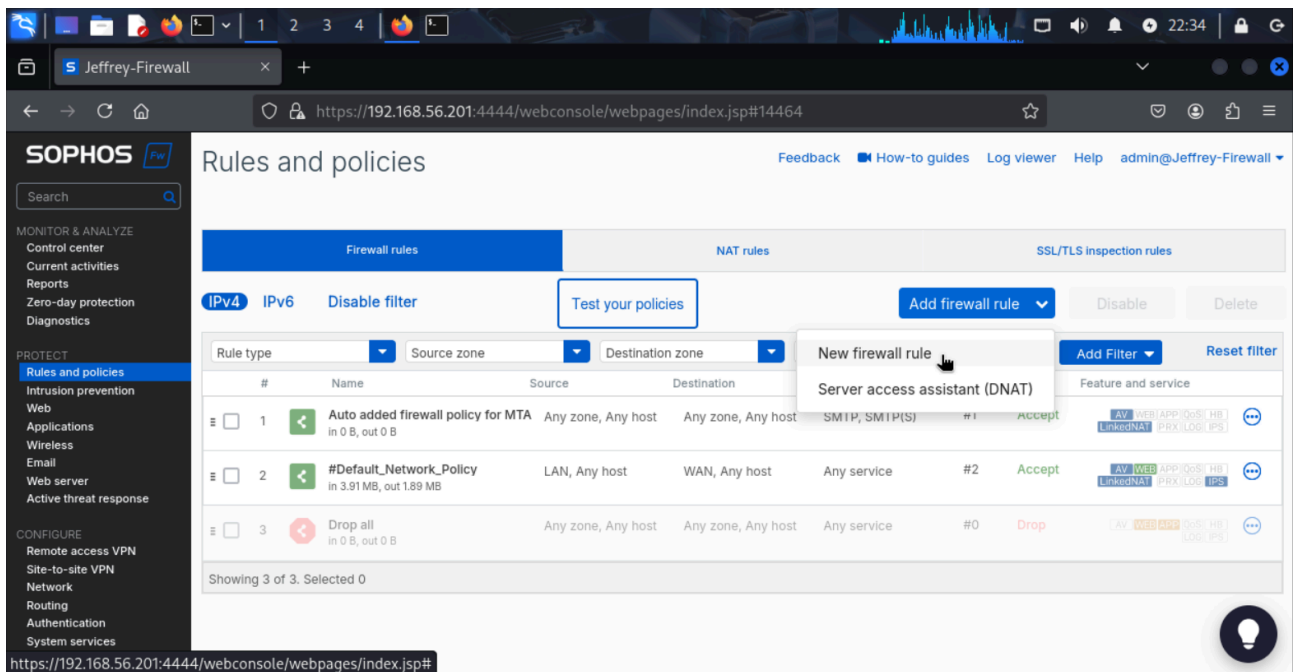
Step 12: Configure Firewall Rule

a. Access Rules and Policies Page

In the navigation pane (on the left), under **PROTECT**, select **Rules and policies**.

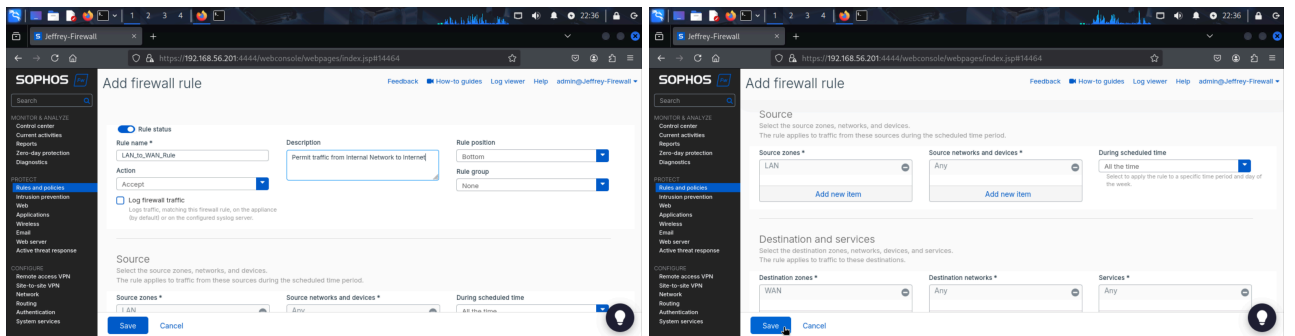
b. Add New Firewall Rule

To set up a new firewall rule, navigate to the **Rules and policies** page, select the **Firewall rules** tab and the **IPv4** button, then click the **Add firewall rule** drop-down and select **New firewall rule**, which opens an **Add firewall rule** page. On this page, configure the rule with the following details: Rule name: **LAN_to_WAN_Rule**, Action: **Accept**, Description: **Permit traffic from Internal Network to Internet**, Source zones: **LAN**, and Destination zones: **WAN**, leaving everything else on the default setting. Finally, click the **Save** button, which adds a new firewall rule called **LAN_to_WAN_Rule**.

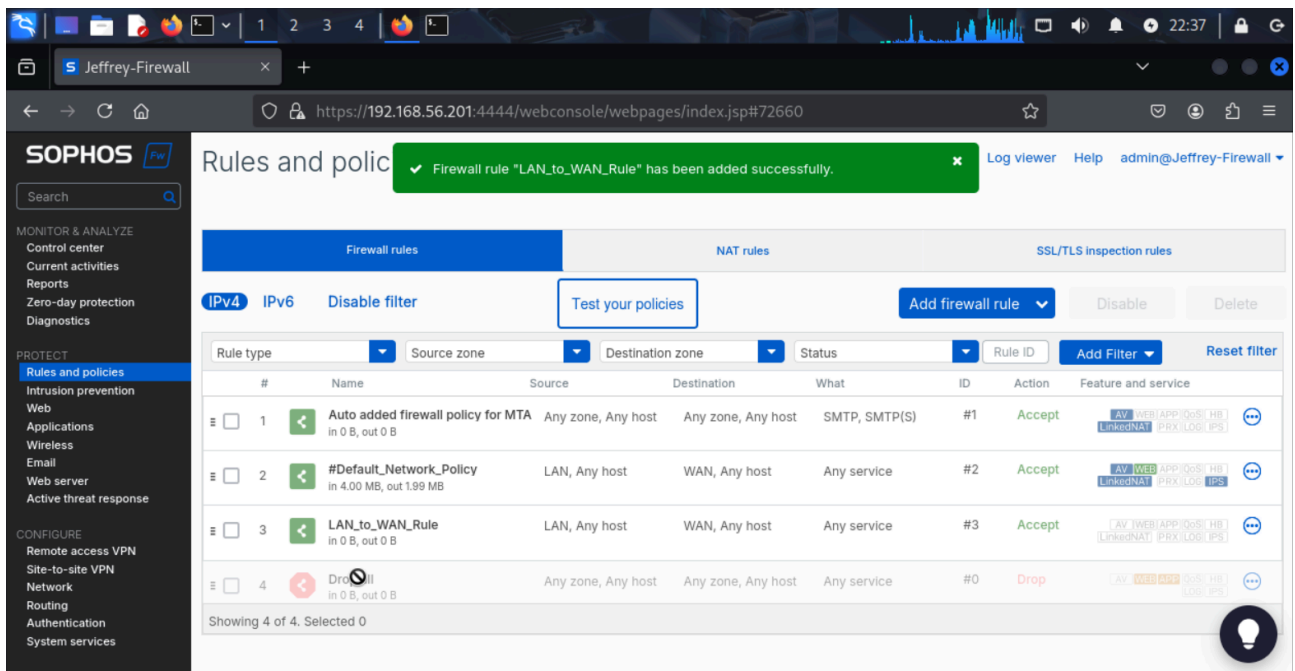


The screenshot shows the Sophos Firewall web console interface. The 'Rules and policies' section is active, displaying a list of firewall rules. A 'New firewall rule' dialog box is open, showing the 'Server access assistant (DNAT)' configuration. The dialog box includes fields for 'Source' (LAN), 'Destination' (WAN), and 'Services' (SMTP, SMTP(S)).

#	Name	Source	Destination	What	ID	Action	Feature and service
1	Auto added firewall policy for MTA	Any zone, Any host	Any zone, Any host	SMTP, SMTP(S)	#1	Accept	AV, WEB, APP, OS, HB, Linked NAT, PRX, LOG, IPS
2	#Default_Network_Policy	LAN, Any host	WAN, Any host	Any service	#2	Accept	AV, WEB, APP, OS, HB, Linked NAT, PRX, LOG, IPS
3	Drop all	Any zone, Any host	Any zone, Any host	Any service	#0	Drop	AV, OS, LOG, OS, HB, LOG, IPS



The left screenshot shows the 'Add firewall rule' dialog box with the 'Rule name' field set to 'LAN_to_WAN_Rule'. The right screenshot shows the 'Add firewall rule' dialog box with the 'Source' field set to 'LAN' and the 'Destination' field set to 'WAN'.



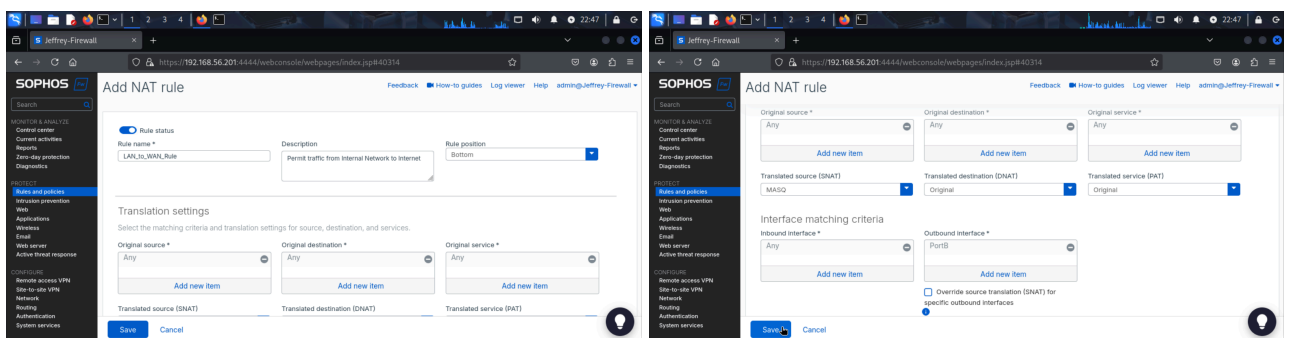
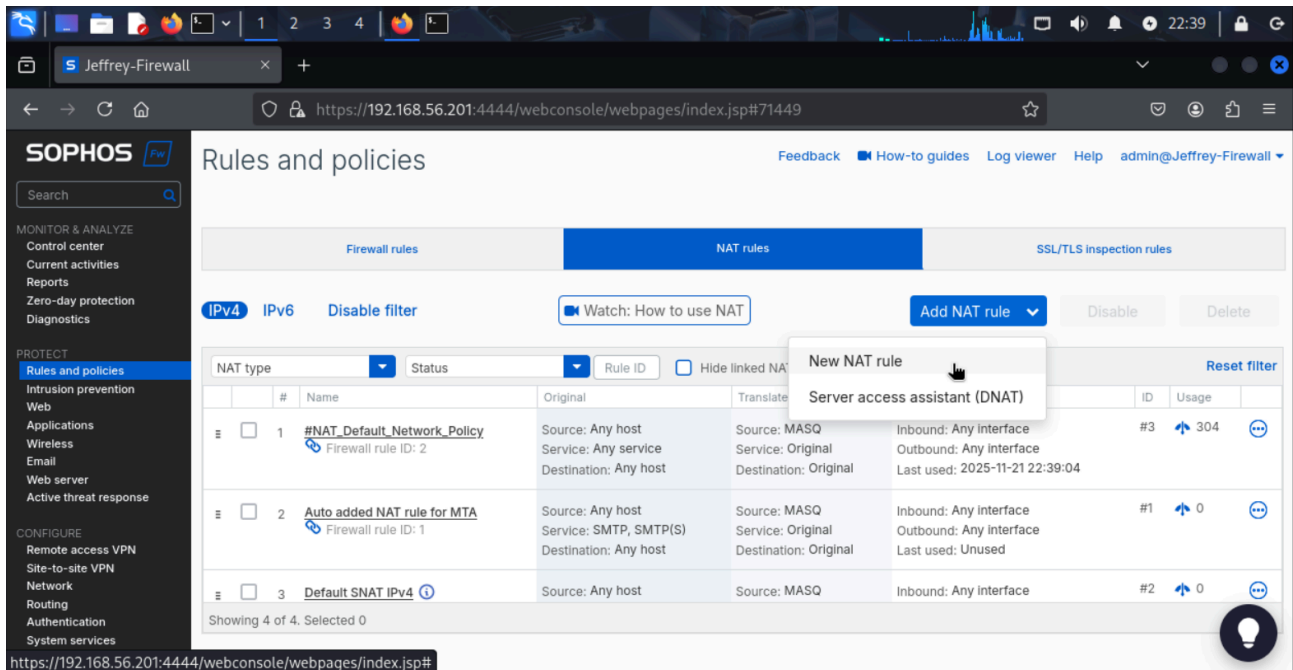
The screenshot shows the Sophos Firewall web console interface. A green notification banner at the top states 'Firewall rule "LAN_to_WAN_Rule" has been added successfully.' The 'Rules and policies' section is active, displaying a list of firewall rules, including the newly added 'LAN_to_WAN_Rule'.

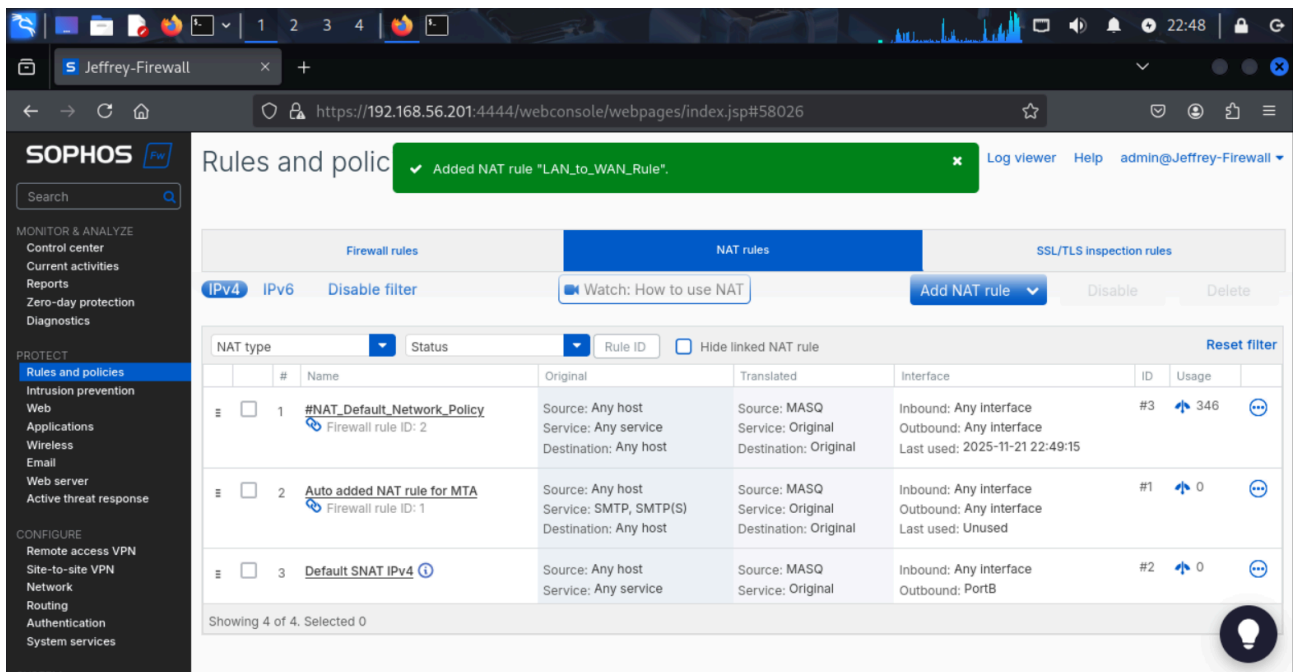
#	Name	Source	Destination	What	ID	Action	Feature and service
1	Auto added firewall policy for MTA	Any zone, Any host	Any zone, Any host	SMTP, SMTP(S)	#1	Accept	AV, WEB, APP, OS, HB, Linked NAT, PRX, LOG, IPS
2	#Default_Network_Policy	LAN, Any host	WAN, Any host	Any service	#2	Accept	AV, WEB, APP, OS, HB, Linked NAT, PRX, LOG, IPS
3	LAN_to_WAN_Rule	LAN, Any host	WAN, Any host	Any service	#3	Accept	AV, WEB, APP, OS, HB, Linked NAT, PRX, LOG, IPS
4	Drop all	Any zone, Any host	Any zone, Any host	Any service	#0	Drop	AV, OS, LOG, OS, HB, LOG, IPS

Step 13: Configure NAT Rule

a. Add New NAT Rule

To add a new NAT rule, first navigate to the Rules and policies page, select the NAT rules tab, and then select the IPv4 button. Next, click the **Add NAT rule** drop-down button and select **New NAT rule** (This opens an **Add NAT rule** page.). On the **Add NAT rule** page, configure the **Rule name** as **LAN_to_WAN_Rule**, the **Description** as **Permit traffic from Internal Network to Internet**, the **Translated source (SNAT)** as **MASQ**, and the **Outbound interface** as **PortB**, leaving everything else on the default setting. Finally, click the **Save** button (This adds a new NAT rule called **LAN_to_WAN_Rule**).

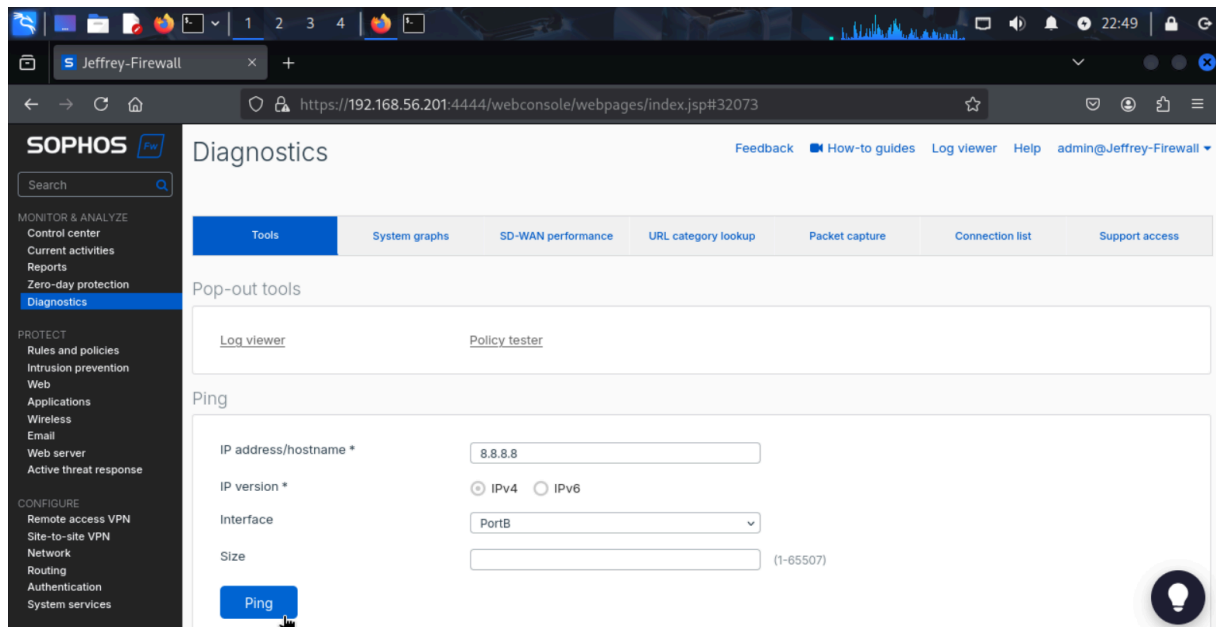


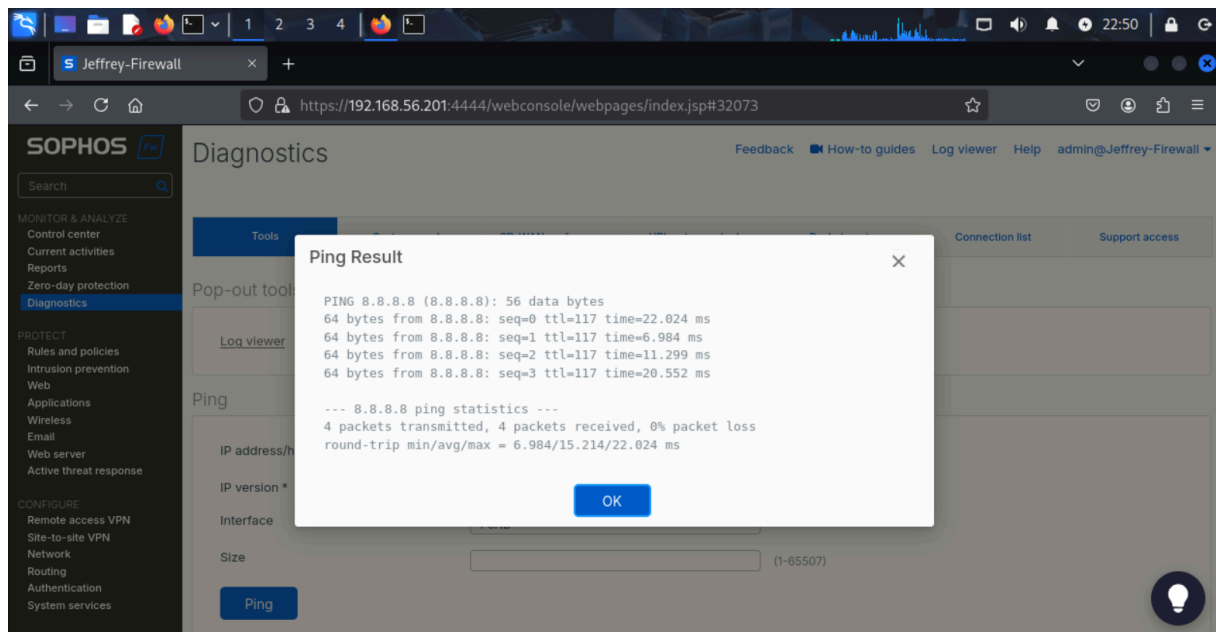


Step 14: Confirm Firewall Internet Connectivity

a. Ping external server

To diagnose connectivity on the Sophos Firewall, navigate to the **Diagnostics** page under **MONITOR & ANALYZE**, then select the **Tools** tab. In the **Ping** section, configure the IP address/hostname as **8.8.8.8** (Google DNS), set the IP version to **IPv4**, and the Interface to **PortB**. Upon clicking the **Ping** button, a **Ping Result** dialog box appears, which should display successful ping statistics with 0% packet loss.





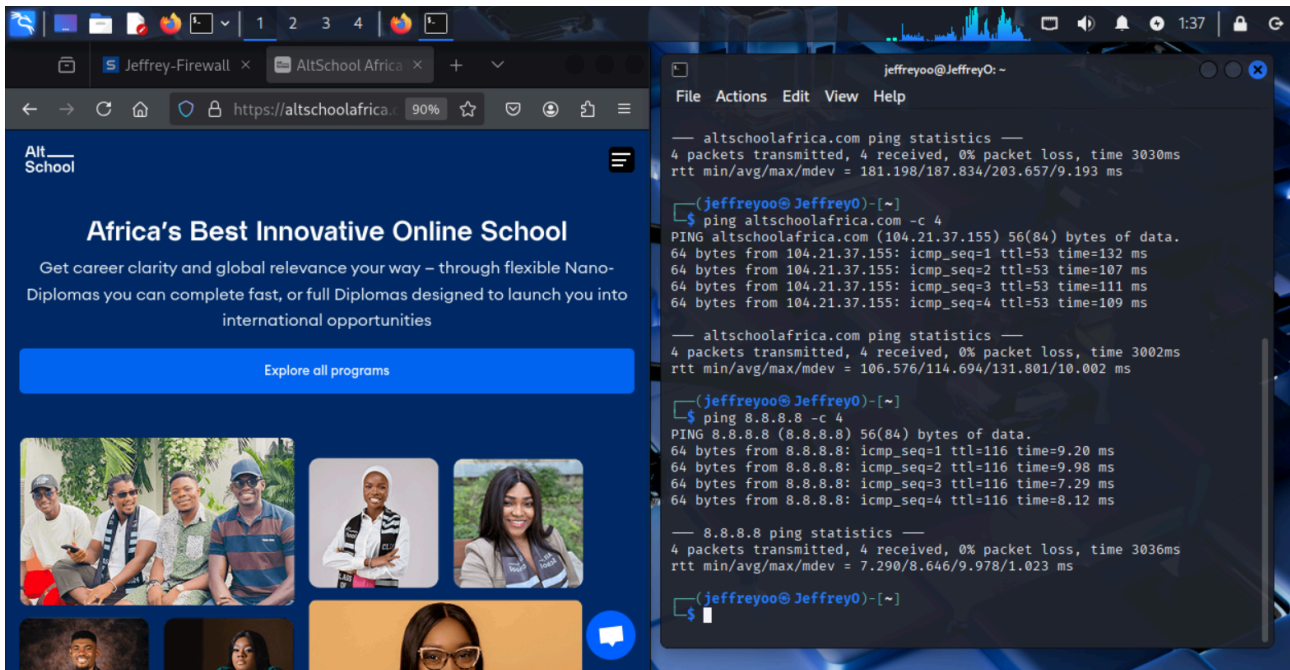
Step 15: Confirm KaliOS VM Internet Connectivity

a. Ping External Server

On the **KaliOS** VM Desktop, open the **Terminal** icon on the taskbar panel, and confirm connectivity to the internet by sending **4 ICMP echo request packets** to the Altschool Africa domain using the command `ping altschoolafrica.com -c 4`. The 0% packet loss indicates the connection **WAS** established. Similarly, confirm connectivity to the internet by sending **4 ICMP echo request packets** to the Google DNS using the command `ping 8.8.8.8 -c 4`, which also returns with 0% packet loss, confirming the connection **WAS** established.

b. Visit External Domain Webpage

On the **KaliOS** VM Desktop, click the **Firefox** icon on the taskbar panel to begin. Connectivity to the firewall was confirmed by successfully accessing the Altschool Africa domain at <https://altschoolafrica.com>, which resulted in the homepage opening on the browser.



c. Confirm Firewall Routing

To confirm internet connectivity **through the firewall**, open the **Terminal** on the **KaliOS VM Desktop** and use the **traceroute** command, which maps the path **ICMP packets** take to reach their destination, by executing `traceroute altschoolafrica.com`. The successful confirmation is indicated when the returned path shows the Firewall's PortB interface IP address as its first hop.



Conclusion

The above configurations on both the firewall (**Sophos-Firewall**) and the virtual machine (**KaliOS**) have enabled the firewall virtual machine to function as an NAT gateway for the VMs

hosted locally on the virtualizer. This ensures that the security services offered by the firewall benefit the VMs, essentially becoming a **Security NAT Gateway** which protects the local network.

Security Policy 2

Content Filtering

This configuration enables the firewall to function as a content screening intervention. Content filtering (or URL filtering) controls content access through firewalls by blocking access to undesired web-based content or web activity. The following configuration implements the firewall as a content filter which enforces acceptable use policies by preventing access to entire categories of URLs without listing individual sites. The content category to be screened out is **News and Media**.

Step 16: Create Web Policy

- a. Launch the Sophos-Firewall Web Console
- b. Add Web Policy

To configure a new web policy in **Sophos Firewall**, first navigate to **Web** under **PROTECT**, then go to the **Policies** tab. Click **Add Policy** and name it **Block_News_Sites** with the description **Block access to news sites**. Next, click **Add rule** and configure it to apply to **Anybody**, for **News** activities, with the **Block** action (indicated with a red shield icon with a white “x”), and the Status set to **On** (with the toggle button pushed to the right); *everything else is left on the default setting*. Finally, click **Save**, and when the *Add this policy to a firewall rule* dialog box appears, click **Go to firewall rules** to apply the new policy.

The screenshot shows the Sophos Firewall Web Console interface. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', and 'CONFIGURE'. The main area is titled 'Web' and shows the 'Policies' tab. A table lists the 'Default Policy' and its associated rules. The rules table has columns for Name, Description, In use, and Manage. The rules listed are:

Name	Description	In use	Manage
Default Policy	A typical starter policy with options suitable for many organizations	1	[+][⌂][✎][🗑]
Anybody	Blocked URLs for Default...	[+][⌂][✎][🗑]	[+][⌂][✎][🗑]
Anybody	Risky Downloads	[+][⌂][✎][🗑]	[+][⌂][✎][🗑]
Anybody	Suspicious	[+][⌂][✎][🗑]	[+][⌂][✎][🗑]
Anybody	Nudity and Adult Content	[+][⌂][✎][🗑]	[+][⌂][✎][🗑]
Anybody	Not Suitable for the Office	[+][⌂][✎][🗑]	[+][⌂][✎][🗑]

The first screenshot shows the 'Add web policy' dialog box in the Sophos web console. The 'Name' field is 'Block_News_Sites' and the 'Description' is 'Block access to news sites'. Below the form is a table with columns: Users, Activities, Action, Constraints, Manage, and Status.

Users	Activities	Action	Constraints	Manage	Status
Anybody	cat News	Red X icon		+ - trash	Toggle on
	Default action	Green check icon			

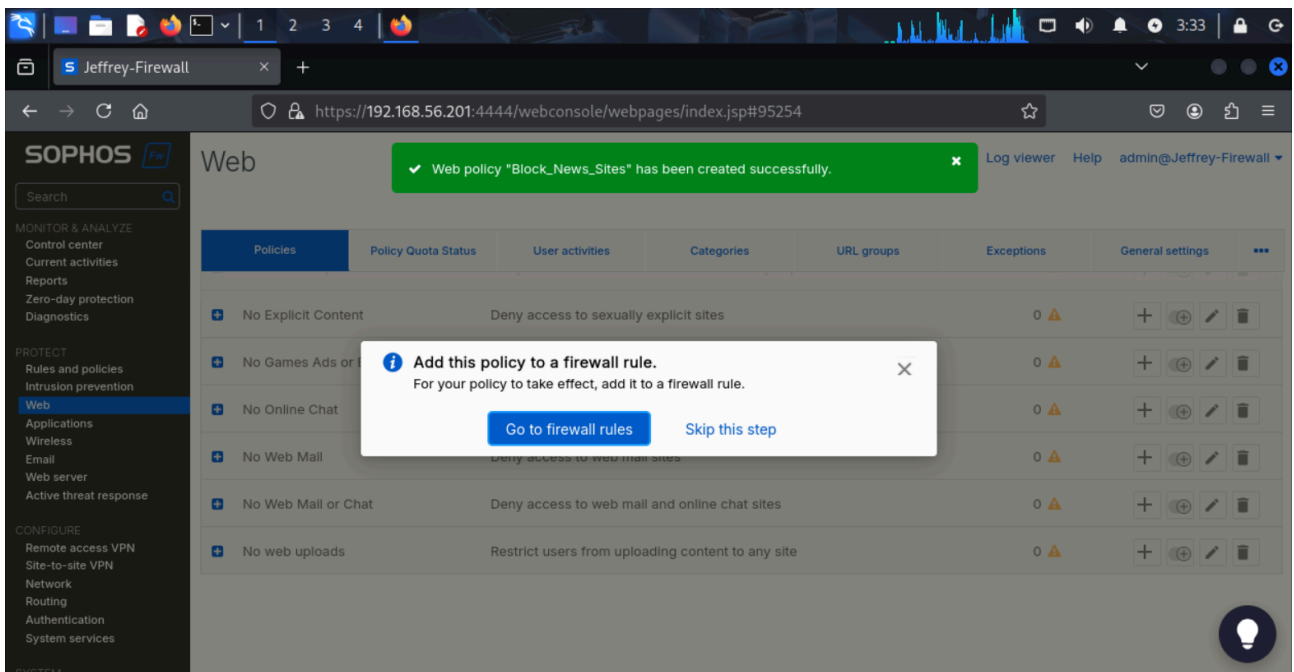
The second screenshot shows the 'Advanced settings' section of the web policy configuration. It includes checkboxes for 'Enable logging and reporting' (checked), 'Prevent download of files larger than' (with a field for MB), and 'Add X-Forwarded-For header to outgoing HTTP requests'. There are also sections for 'Restrict login domains for Google apps' and 'Apply Microsoft Azure AD tenant restrictions' with associated input fields and explanatory text.

Allowed time quota: 1 Hours 0 Minutes. Set the maximum allowed time for a single user to browse web content that falls into categories restricted by a quota policy action.

Advanced settings

- ☒ Enable logging and reporting
- ☐ Prevent download of files larger than MB. Values between 1 and 1536 MB are permitted.
- ☐ Add X-Forwarded-For header to outgoing HTTP requests. This can expose the user's internal IP address. Only use it with a properly configured upstream load balancer or proxy. ⚠ This option can be enforced by the web proxy only.
- ☐ Restrict login domains for Google apps. Allowed domain(s) . A comma-separated list of allowed domains for Google apps. ⚠ This option can be enforced by the web proxy only.
- ☐ Apply Microsoft Azure AD tenant restrictions. Restrict-Access-To-Tenants . Restrict-Access-Context . Comma-separated list of domain names and domain IDs in GUID format. Directory ID of the tenant setting the restrictions in GUID format. ⚠ This option can be enforced by the web proxy only.

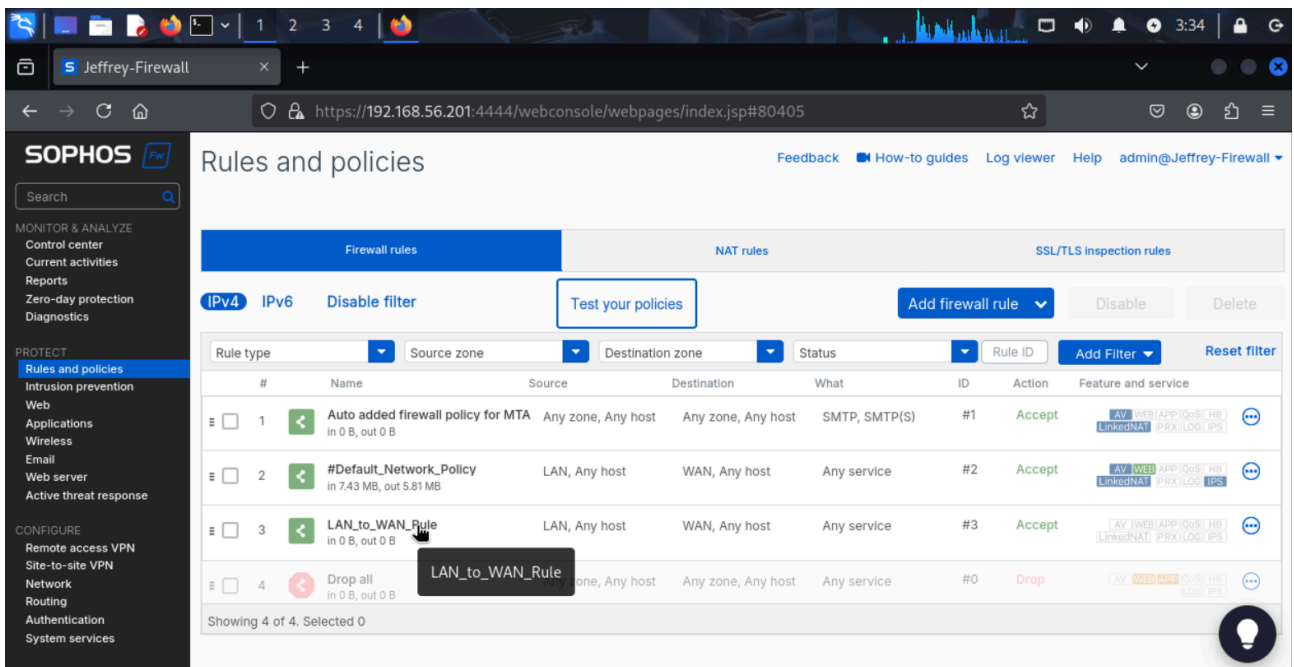
Buttons: Save, Cancel.



Step 17: Add Policy to Firewall Rule

a. Access the previously created LAN_to_WAN_Rule

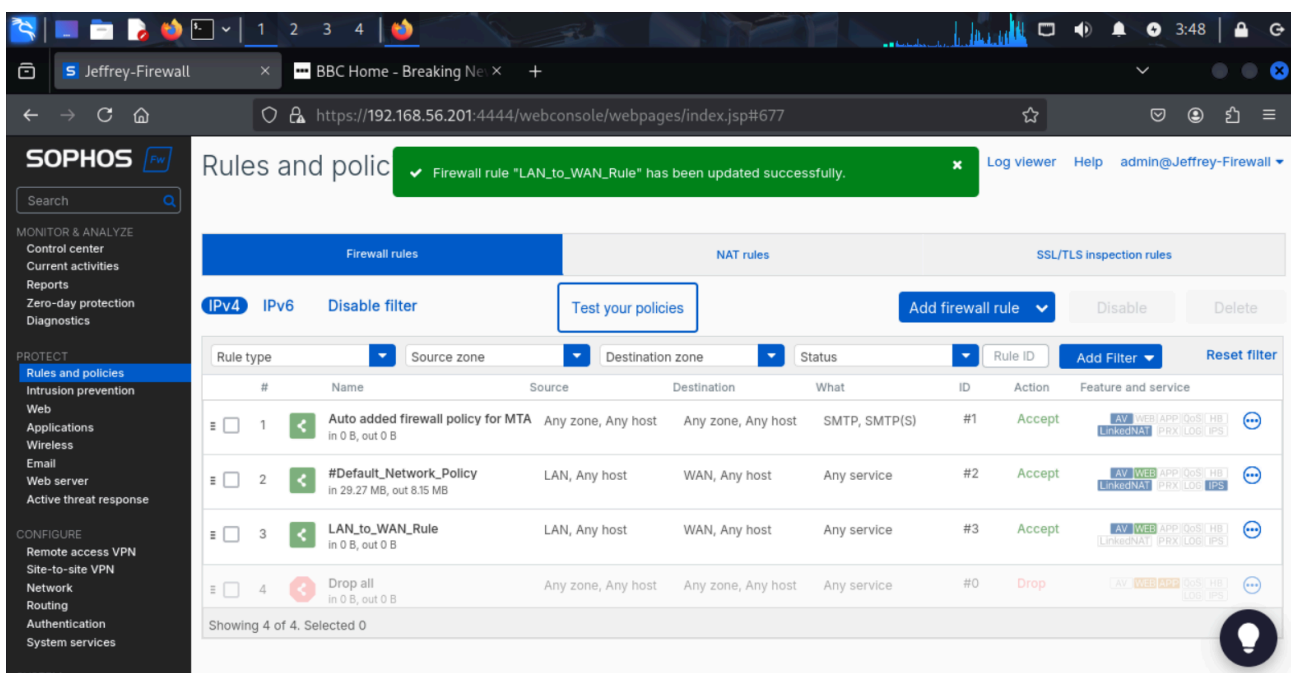
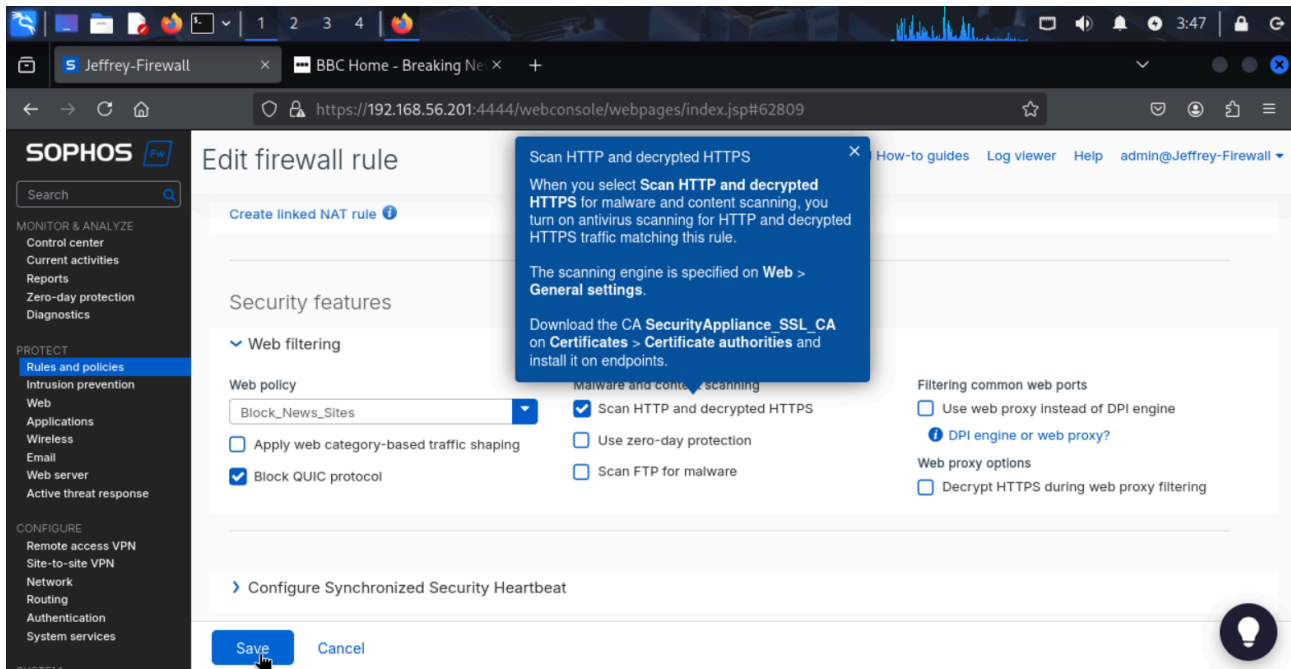
On the **Rules and policies** page, under the **Firewall rules** tab, locate and click the **LAN_to_WAN_Rule** firewall rule inside the data grid, which opens the **Edit firewall rule** page for editing the **LAN_to_WAN_Rule** firewall rule.



b. Edit the LAN_to_WAN_Rule

On the **Edit firewall rule** page, proceed to the **Security features** section and click the **Web filtering** drop-down menu, then apply the following configuration: set the Web policy to **Block_News_Sites**, Check the **Block QUIC protocol** box (because the QUIC protocol can bypass traditional deep packet inspection and security policies by using UDP), and Check the

Scan HTTP and decrypted HTTPS box (to apply antivirus scanning to traffic matching this rule), leaving everything else unchecked, before finally clicking the **Save** button at the bottom of the page, which successfully updates the **LAN_to_WAN_Rule** firewall rule.



Step 18: Test News Blocking Rule from the Web Console

a. Launch Firewall Policy Testing

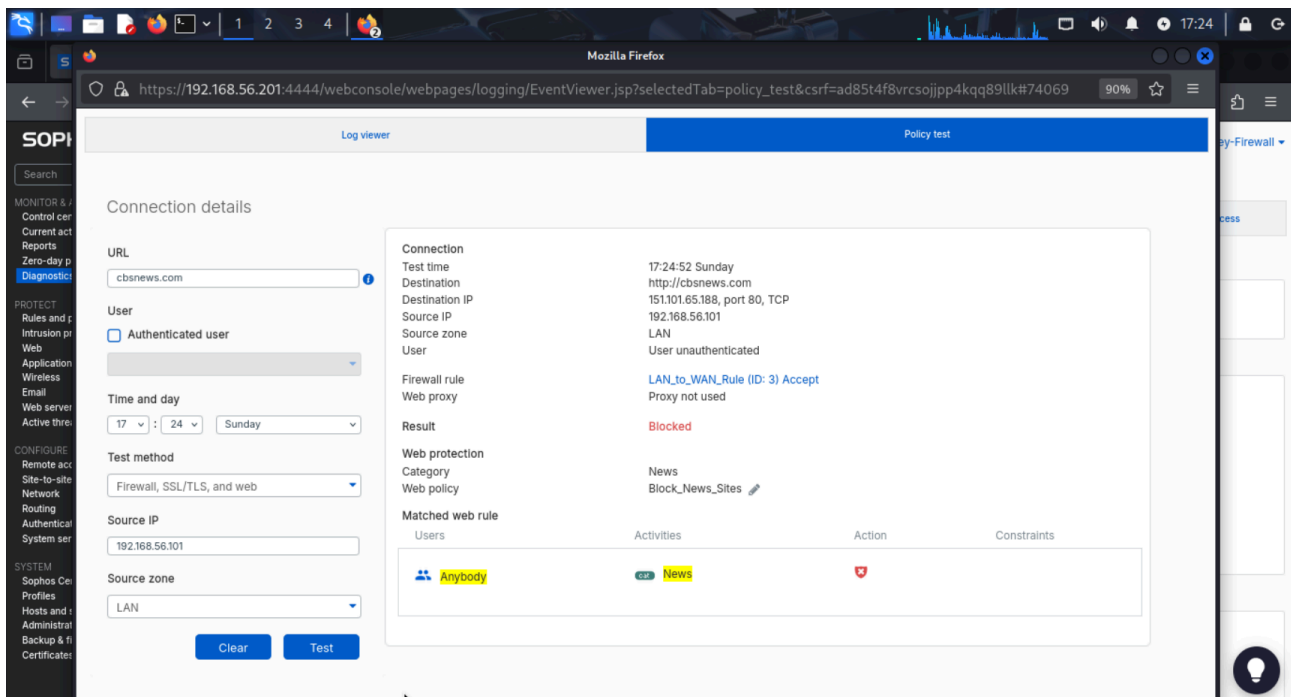
From the **Rules and policies** page, navigate to the **Firewall rules** tab and click **Test your policies**, which opens the **Diagnostics** page. On the **Diagnostics** page, under the **Tools** tab, locate the **Pop-out tools** section and click the **Policy tester** text located within the **Pop-out tools** section, which opens a pop-up **Policy test** window.

b. Set Up Firewall Policy Testing

In the **Policy test** window, after locating the **Connection details** section, input the query details: the URL as **cbsnews.com** (a web domain for **CBS News**), **Uncheck** the User checkbox (as the test isn't restricted to authenticated users), leave the Time and day as default, select **Firewall, SSL/TLS, and web** for the Test method, enter **192.168.56.101** as the Source IP (the IP address of the KaliOS VM), and select **LAN** for the Source zone (indicating the source of the packets). Finally, click the **Test** button, which will return the results of the policy test in the **Test result box**.

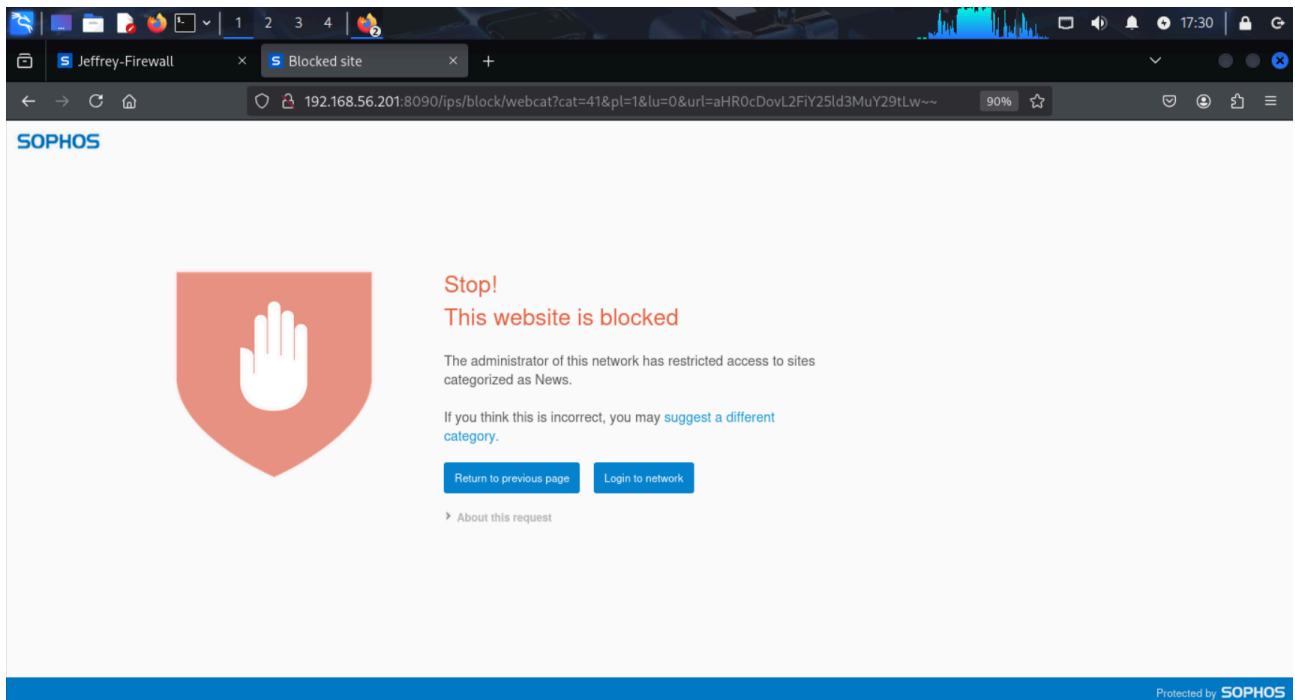
c. Confirm Firewall Policy

In the **Test result box**, the results indicate the connection was blocked, while indicating the rules and policies that were responsible.



Step 19: Test News Blocking Rule from KaliOS VM Browser

To begin, launch the **KaliOS Virtual Machine**, then launch the Browser (**Firefox**) by clicking its icon on the **KaliOS** VM Desktop taskbar, which opens to a new tab. **Test connectivity** by typing **abcnews.com** in the address bar and pressing **Enter**; the expected return is a Sophos page with the message “**Stop! This website is blocked,**” *This indicates the News filtering policy is active.*



Conclusion

This web policy and firewall rule configuration ensures the screening out/blocking of news sites. Restricting the internal network from access to online news journals can be implemented in organizations' networks to reduce distractions, minimize political engagement or enforce the compliance of acceptable use policies regarding company-owned devices.

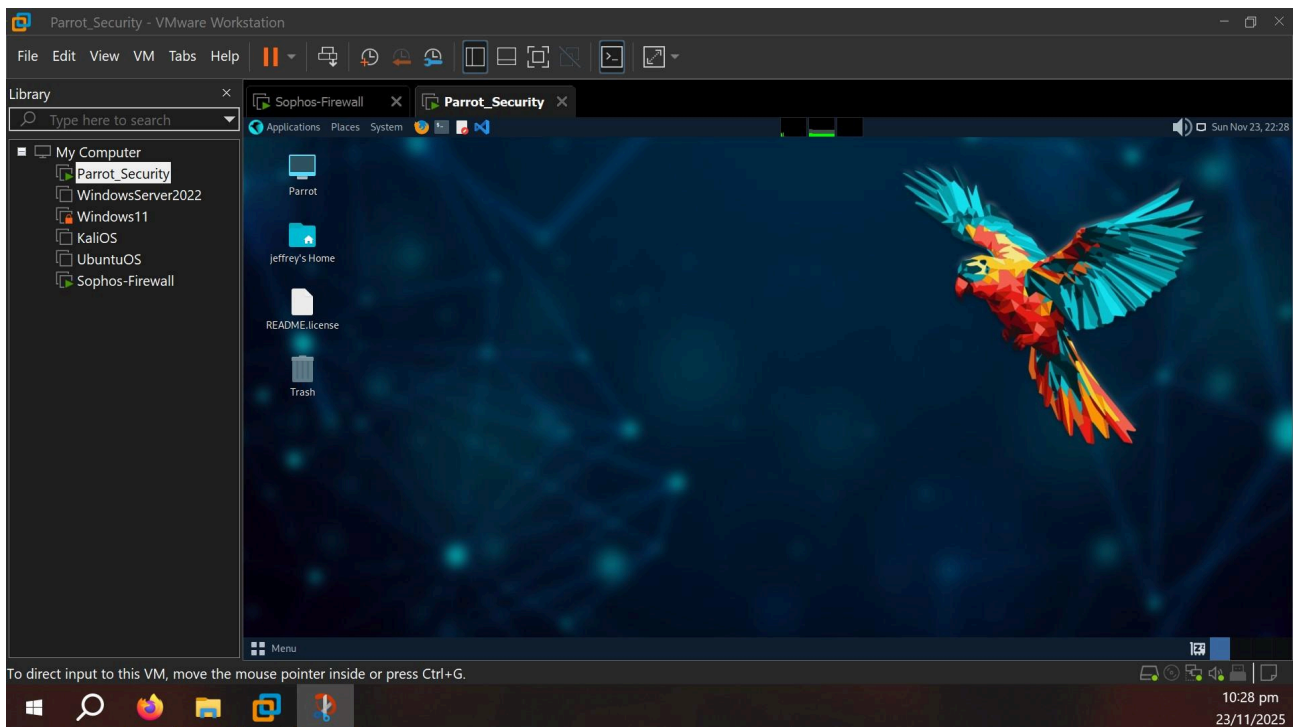
Security Policy 3

Denial of Service Protection

This configuration inhibits the efficacy of Denial-of-Service (DoS) attacks launched at the firewall. DoS attacks are often launched at organizations by malicious actors who seek to overwhelm private network infrastructure and weaken defenses often in order to gain unauthorized access. Configuring the firewall to drop high-volume high-burst packets keeps the network healthfully defended while ensuring availability for legitimate and authenticated users.

Step 20: Launch and Set Up Virtual Machines

- a. **First, launch the KaliOS Virtual Machine** (as demonstrated in [Step 11a]). Next, launch the **Parrot_Security Virtual Machine** by selecting it in the Library panel of **VMware Workstation Pro**, choosing **Power on this virtual machine** in its tab, and then entering the login credentials to access the Desktop.



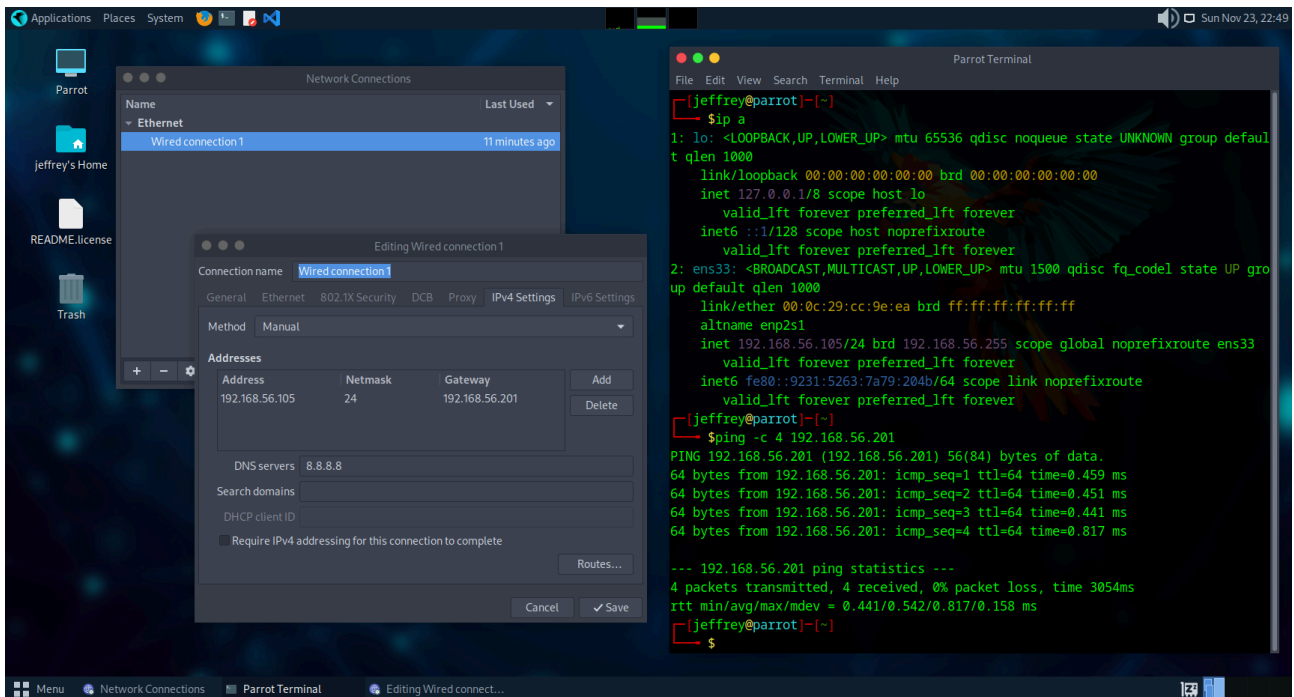
- b. Launch the **Parrot_Security Network Settings** Window
- c. **Configure the Parrot_Security Network Settings**

In the **Editing Wired connection 1** window, navigate to the **IPv4 Settings** tab and change the **Method** to **Manual**. In the **Addresses** section, click **Add** and configure the new entry with the **Addresses** as 192.168.56.105 (distinct from KaliOS), the **Netmask** as 24, and the **Gateway** as 192.168.56.201. Finally, set the **DNS servers** to 8.8.8.8 (Google DNS) and click the **Save** button.

- d. **Confirm Parrot_Security Network Settings and Connectivity**

Launch the **Terminal** and use the command `ip a` to display comprehensive network interface information, including IP addresses and subnets. Next, confirm connectivity to the firewall by typing

the command `ping 192.168.56.201 -c 4` to send four ICMP echo request packets. The connection is established if the packets return with 0% packet loss.



Step 21: Configure DoS & Spoof Protection

- a. Launch the Sophos-Firewall Web Console
- b. Configure DoS Settings

To configure DoS protection in Sophos Firewall, navigate to **Intrusion prevention** under **PROTECT** in the **Navigation** pane, then select the **Dos & spoof protection** tab and scroll to the **DoS settings** section. Apply the following configurations for **SYN flood**, **UDP flood**, **TCP flood**, and **ICMP/ICMPv6 flood**: set **Source (Packet rate per Source)** to 100, **Source (Burst rate per Source)** to 50, check the **Apply flag** box, set **Destination (Packet rate per Destination)** to 2000, and **Destination (Burst rate per Destination)** to 1000, leaving all other settings at default before clicking the **Apply** button.

Intrusion prevention

DoS settings has been applied successfully

DoS attacks | IPS policies | Custom IPS signatures | **DoS & spoof protection**

DoS settings

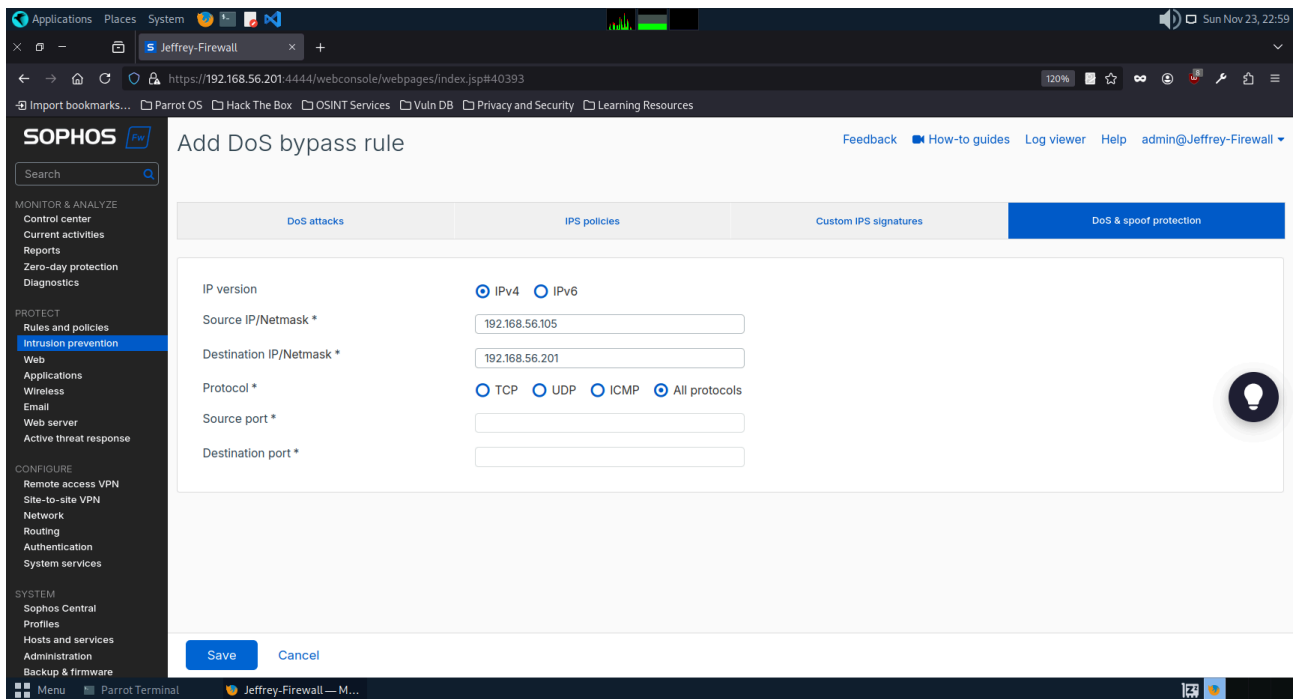
Attack type	Source		Apply Flag	Source Traffic Dropped	Destination		Apply Flag	Destination Traffic Dropped
	Packet rate per Source (Packet/min)	Burst rate per Source (Packet/sec)			Packet rate per Destination (Packet/min)	Burst rate per Destination (Packet/sec)		
SYN flood	100	50	☒	0	2000	1000	☐	0
UDP flood	100	50	☒	0	2000	1000	☐	0
TCP flood	100	50	☒	0	2000	1000	☐	0
ICMP/ICMPv6 flood	100	50	☒	0	2000	1000	☐	0
Dropped source routed packets	-	-	-	-	-	-	☒	-
Disable ICMP/ICMPv6 redirect packet	-	-	-	-	-	-	☒	-
ARP hardening	-	-	-	-	-	-	☐	-

Apply

Click here for DoS attacks status

c. Configure DoS Bypass Rule

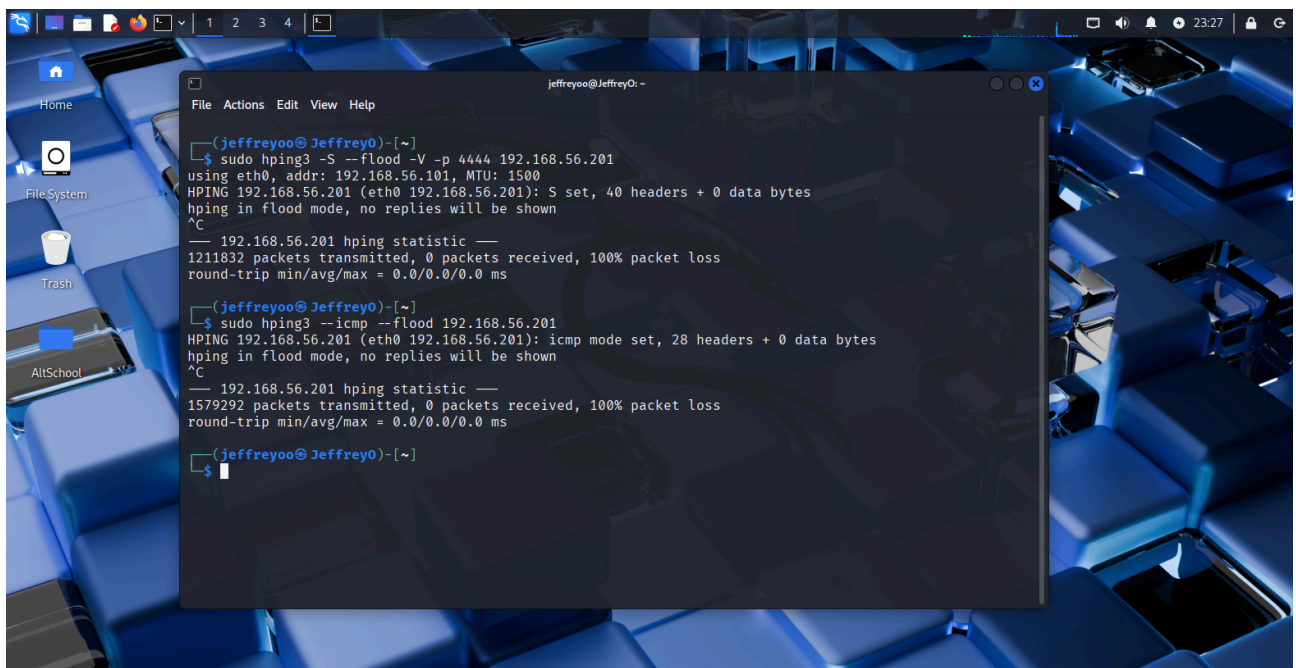
To add a DoS bypass rule, go to the **Intrusion prevention** page, select the **Dos & spoof protection** tab, and in the **DoS bypass rule** section, click **Add**. On the **Add DoS bypass rule** page, configure the rule with **IPv4** for the IP version, **192.168.56.105** for the Source IP/Netmask, **192.168.56.201** for the Destination IP/Netmask, and **All protocols** for the Protocol, then click **Save**.



Step 22: Test DoS & Spoof Protection

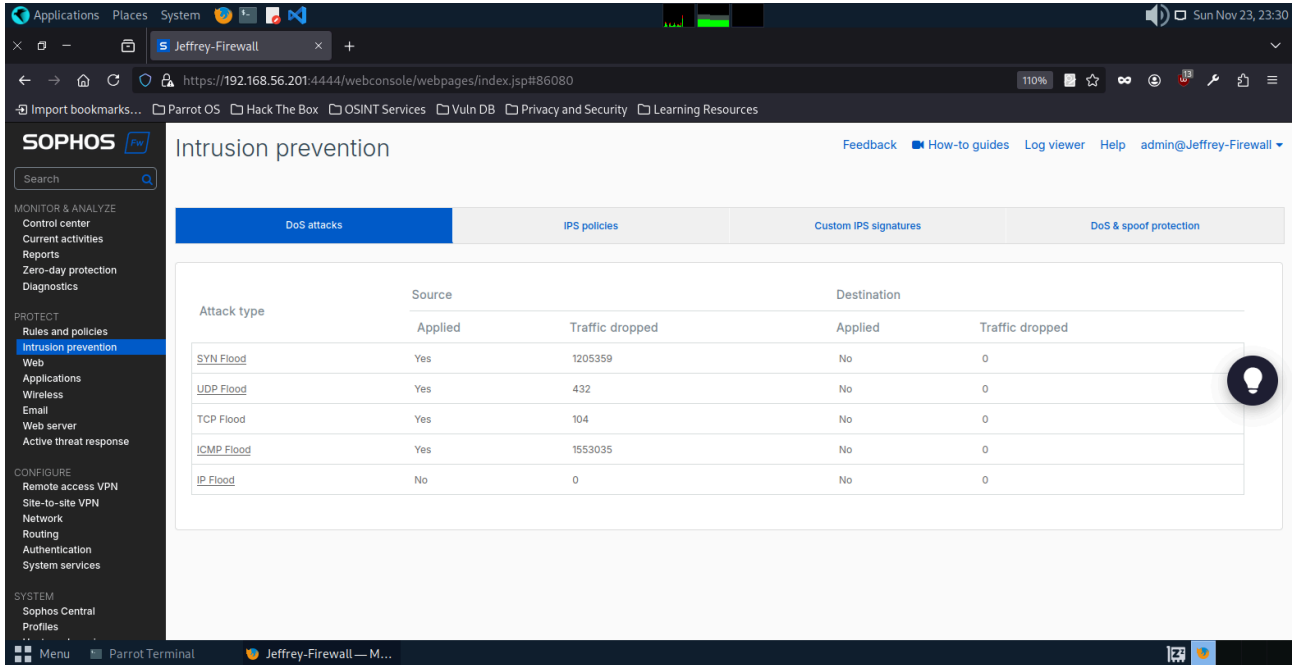
a. Launch a DoS Attack at the Firewall

To simulate network attacks for firewall testing, open the KaliOS machine and launch the **Terminal**. First, simulate a SYN flood attack by sending the command: `sudo hping3 -S --flood -V -p 4444 192.168.56.201`, which resulted in **1,211,832** packets sent. Next, simulate an ICMP flood attack using the command: `sudo hping3 --icmp --flood 192.168.56.201`, which resulted in **1,579,292** total packets sent, with the results of both simulations returned in the **Terminal**.



b. Confirm DoS Attack Protection

To view the dropped traffic from DoS attacks, open the **Parrot_Security** machine and access the web console via the **Firefox** browser; then, navigate to **Intrusion prevention** under **PROTECT** in the Navigation Pane. On the **Intrusion prevention** page, click the **Dos attacks** tab, where the table indicates traffic dropped, including **1,211,832** SYN flood attempts and **1,579,292** ICMP flood attempts.



The screenshot shows the Sophos Next-Gen Firewall web console interface. The left navigation pane is expanded to the **PROTECT** section, specifically **Intrusion prevention**. The main content area shows the **DoS attacks** tab selected. Below the tab, there is a table with columns for **Attack type**, **Source**, and **Destination**. The table lists several attack types and the corresponding traffic dropped.

Attack type	Source	Destination		
	Applied	Traffic dropped	Applied	Traffic dropped
SYN Flood	Yes	1205359	No	0
UDP Flood	Yes	432	No	0
TCP Flood	Yes	104	No	0
ICMP Flood	Yes	1553035	No	0
IP Flood	No	0	No	0

Conclusion

Configuring upper limits for packet rates and burst rates for sources and destinations can offer functional protections for the firewall, keeping the internal network secure. The configuration above