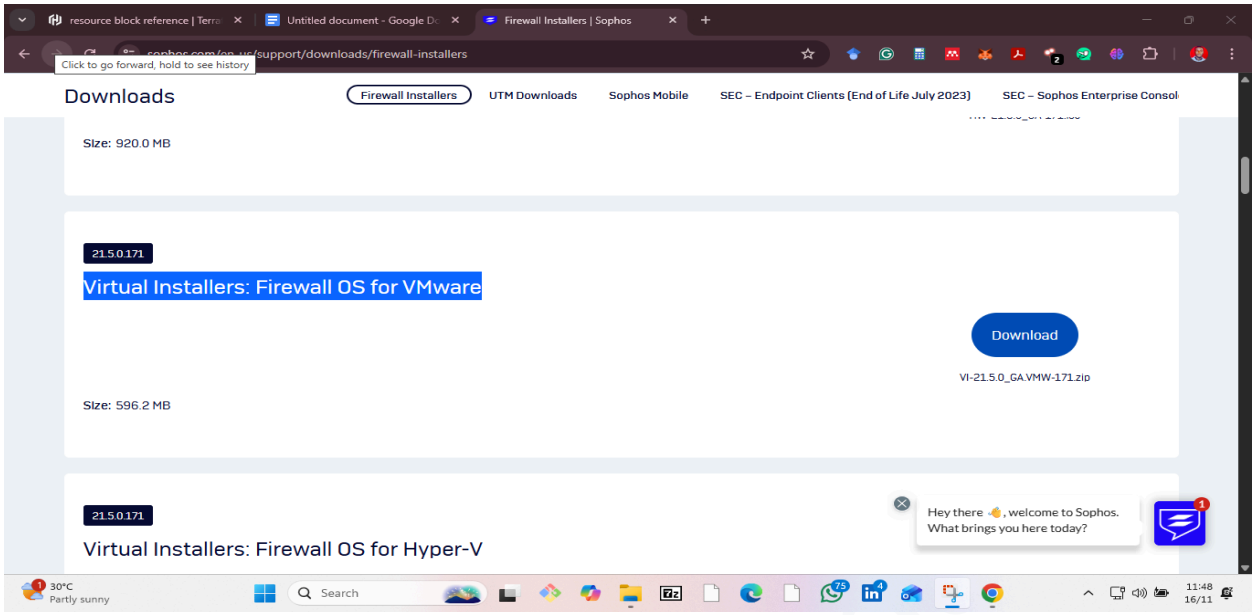
Set-up, Installation, and Configuration of the Sophos Firewall in VirtualBox

Description: The Sophos Firewall is a next-generation firewall (NGFW) designed to provide comprehensive network security, including intrusion prevention, deep packet inspection, web application firewall, and advanced threat protection. It unifies security management and uses a synchronized security approach to share threat intelligence and health status between the firewall and other Sophos security products, offering a coordinated defense against cyber threats.

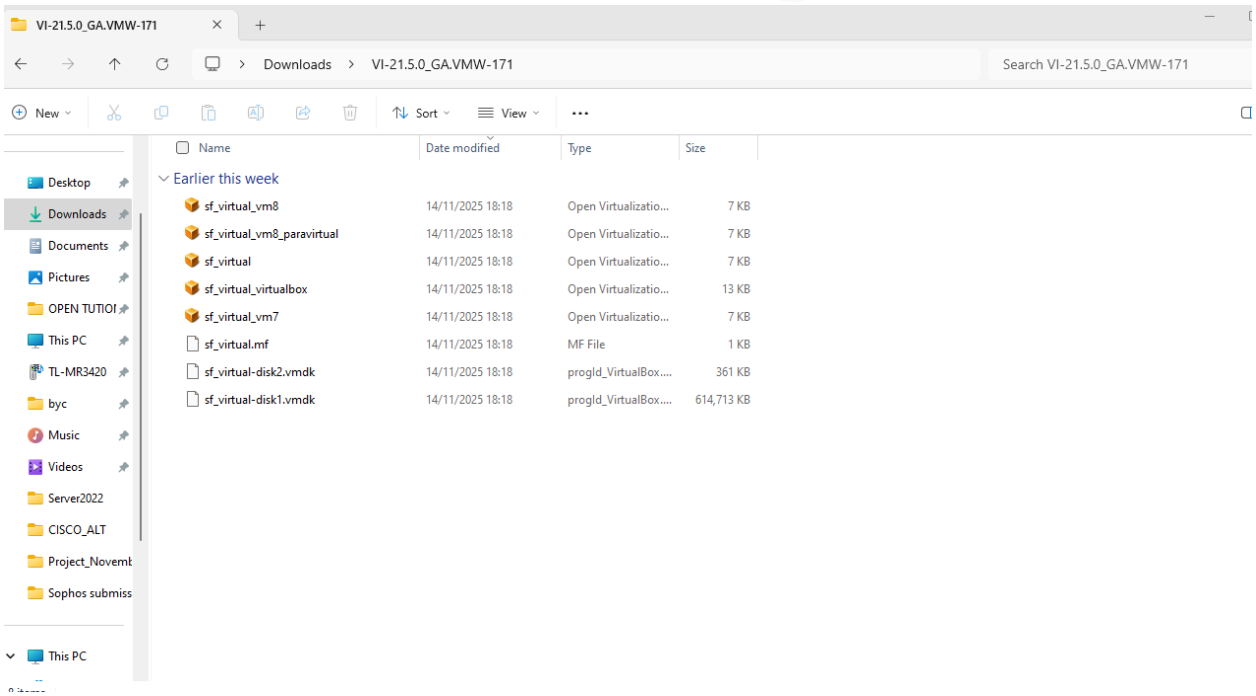
This documentation would detail its setup, installation, and Configurations.

Download of the Sophos Virtual Firewall Machine

To download the Sophos virtual Firewall, you should head over to their website: https://www.sophos.com/en-us/support/downloads/firewall-installers and scroll down to the section titled: **Virtual Installers: Firewall OS for VMware**, and then click download. This will download a Zip file, which is about **592MB** in size, and you will be required to input certain details, such as your email and the organization you are working for, to check if you can download. You will also receive an email that contains your firewall serial number, which will be vital as you proceed further in this installation process.



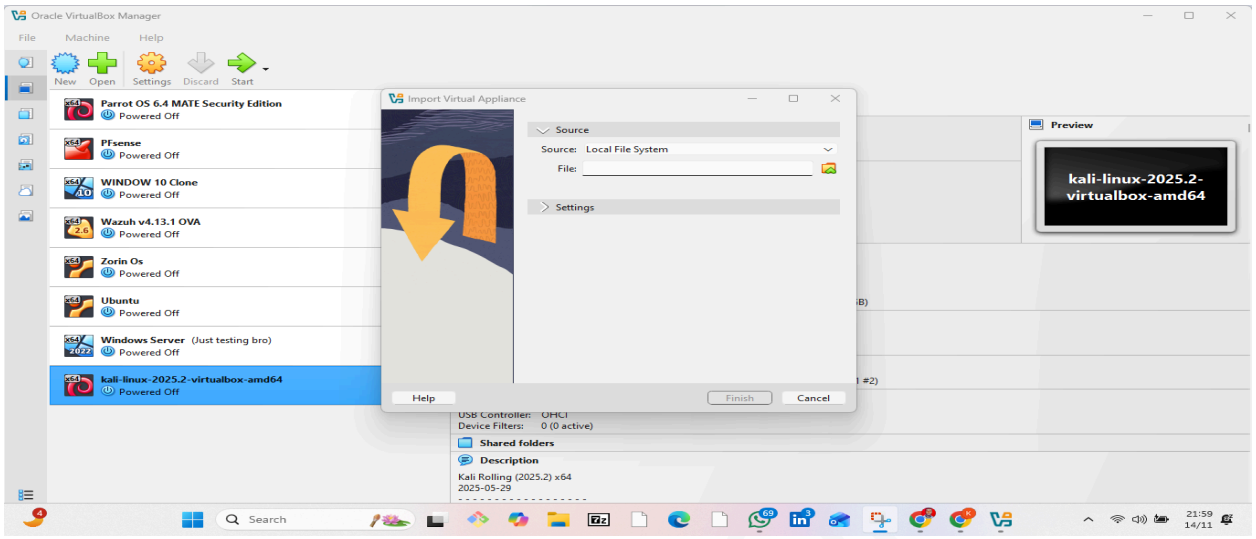
You can then extract the contents of the zip file with your preferred compression software. You will find the folder containing various OVF files for installation.



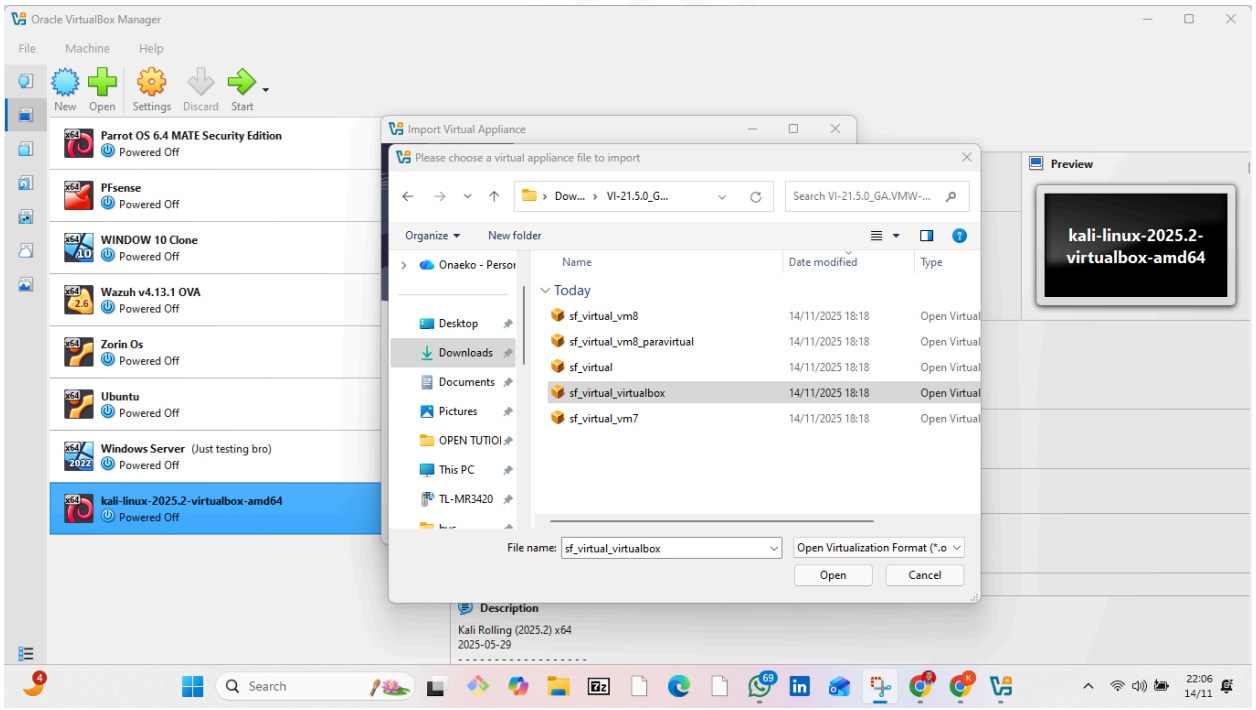
Installation and Configuration of the Sophos Virtual Firewall On VirtualBox

Step 1: Access VirtualBox to start installation

Open VirtualBox and click on **“File”** and then click on **“Import Appliances”**, and you should see this.



Then browse to the folder where you have the OVF files and select the one with the suffix of **“virtualbox”**, as our installation is being carried out on VirtualBox. After clicking on **“open”**, and then finish the importation of the virtual appliances.



Step 2: Select the right adapters needed for installation

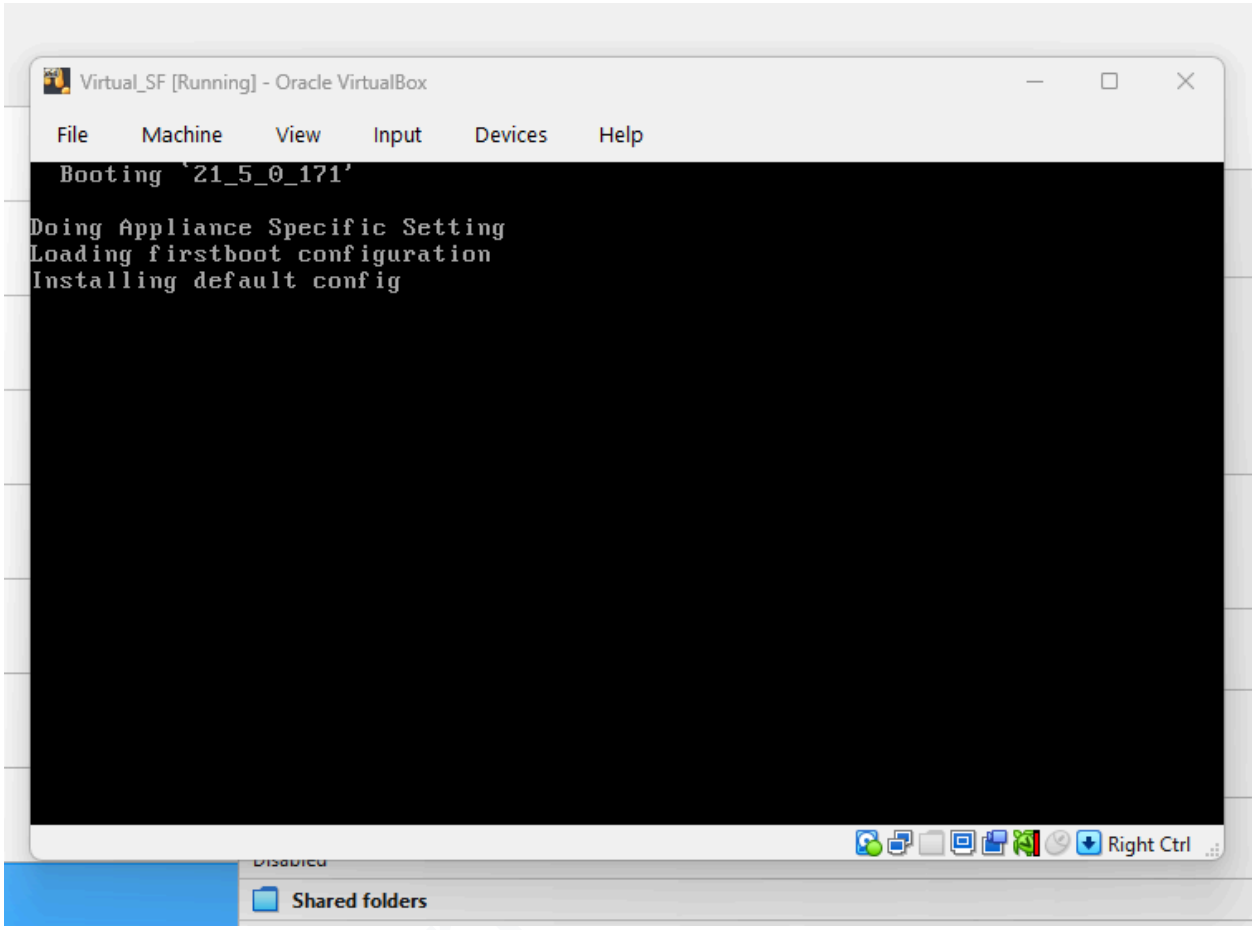
Before continuing with this installation by powering on the virtual machine, click on **“File”** and navigate to the **“Tools”** and then to the **“Network”** section, and then configure the adapter manually with the following address **“192.168.56.1”** and Network mask of **“255.255.255.0”**, and then click on the DHCP server to enable it as part of the Host-Only Network interface configurations

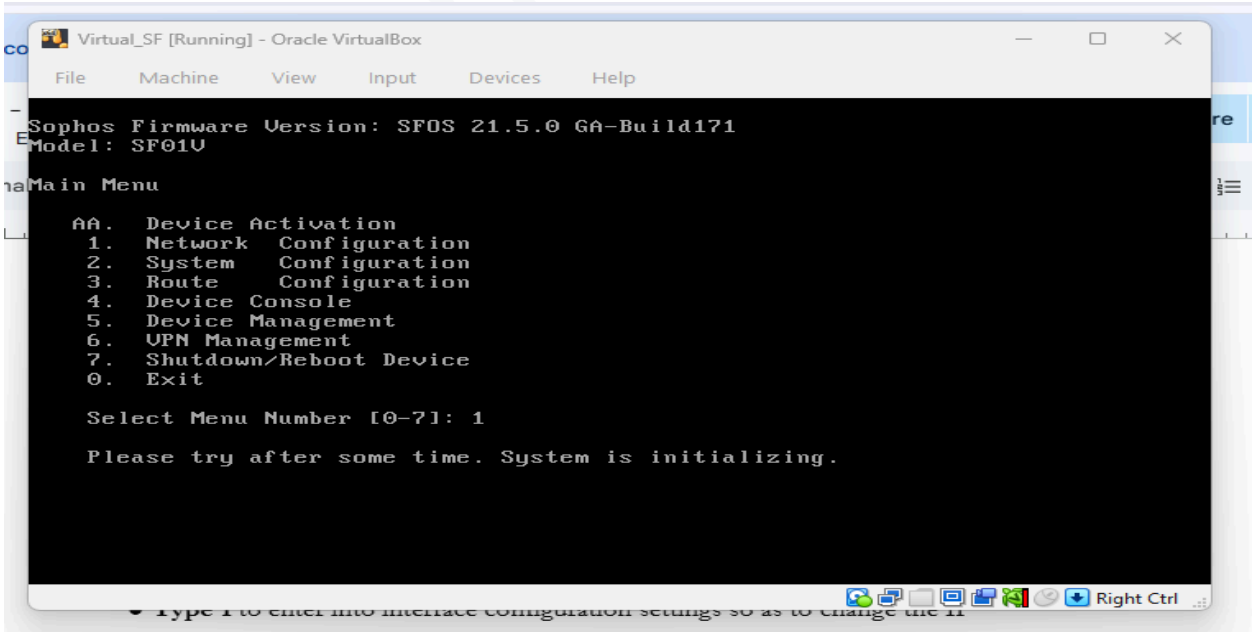
And then navigate to the settings section in VirtualBox dashboard then select Adapter 1 and configure it as a **“host-only network”** (configuring Adapter 1 as host-only would create a scenario where the host and VM can communicate together, with the isolation of not accessing the internet), also we would add another adapter by selecting Adapter 2 and configure it as a **“bridged adapter”** and configure the **“name”** to reflect the interface that would give internet to your computer which could wireless be or Ethernet (configuring Adapter 2 as bridged adapter creates the environment where both the hosts and VMs can communicate and also still have internet, which would be vital for further updates in our Sophos Installation)

Step 3: Start up the Sophos installation

After configuring the previous step, ensure that to start the Sophos Virtual Firewall and follow up on the installation wizard process as seen in the snippet below, and allow it to initialize

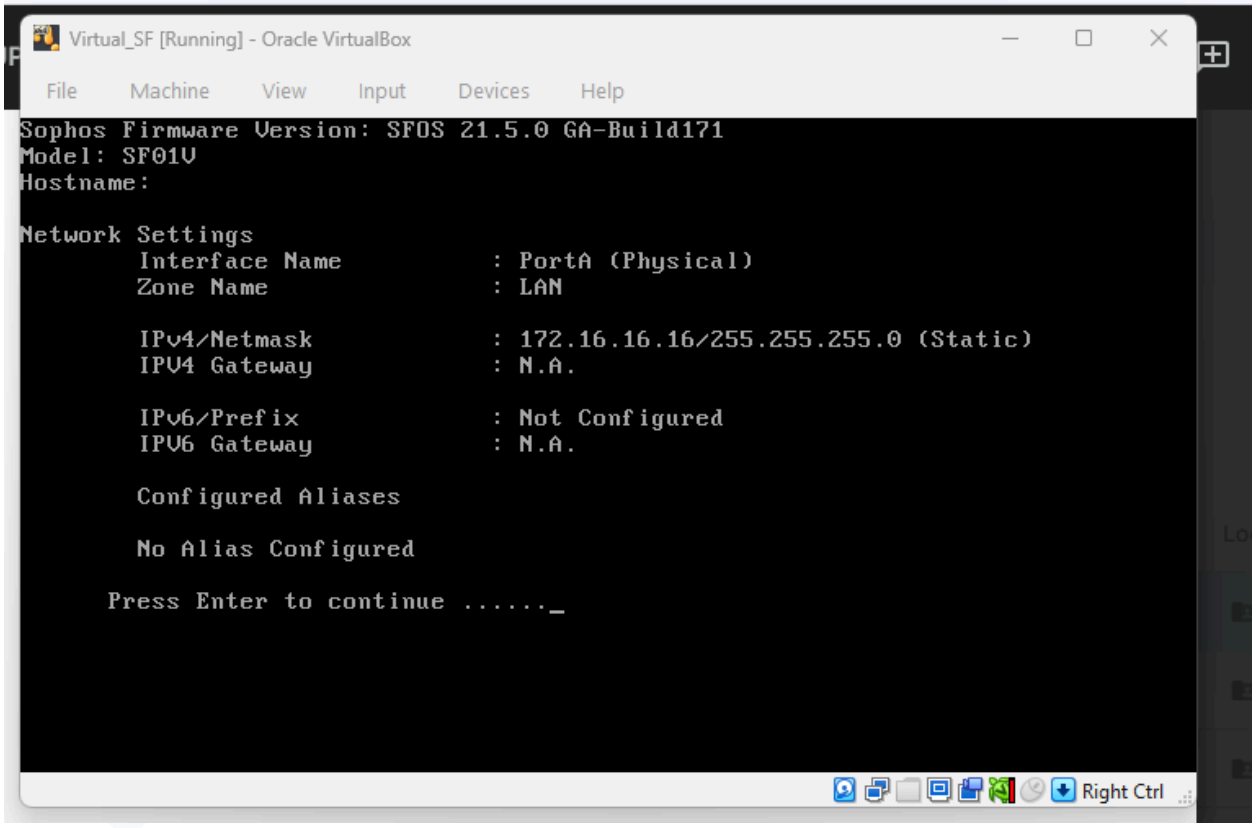
after some minutes. And to log in to the CLI would require an admin password, which by default is **“admin.”**

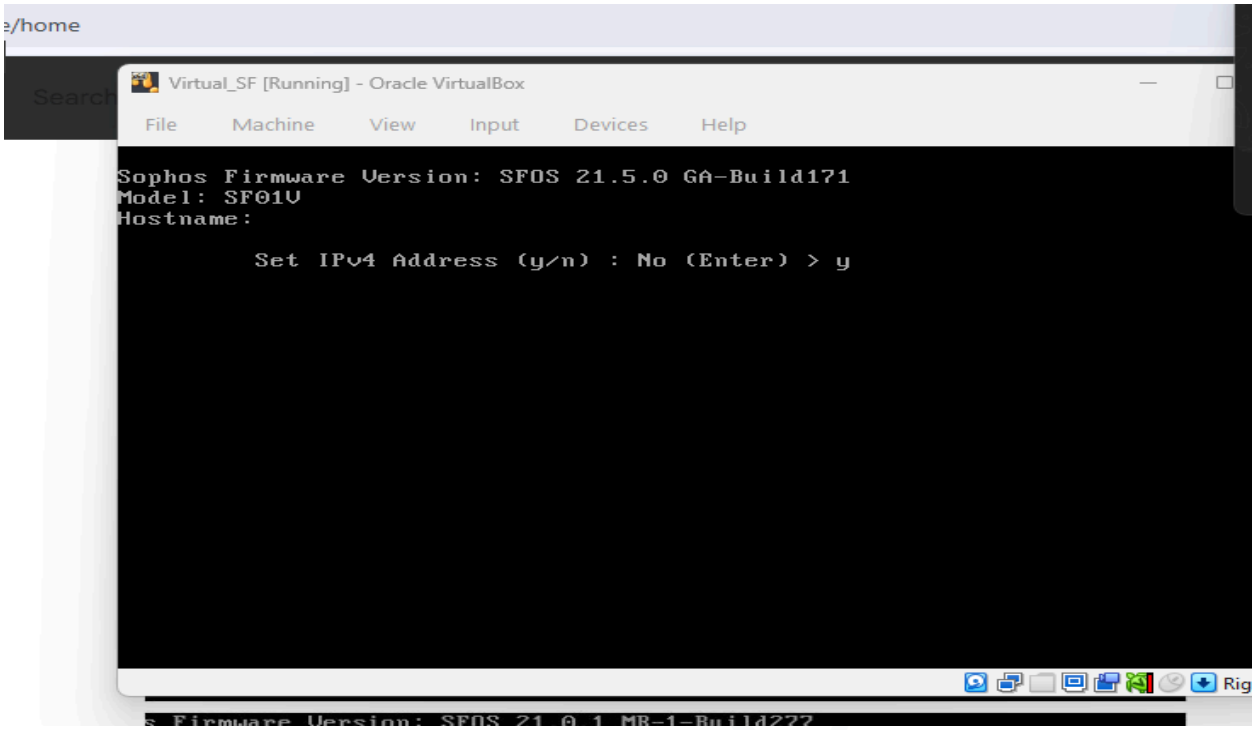


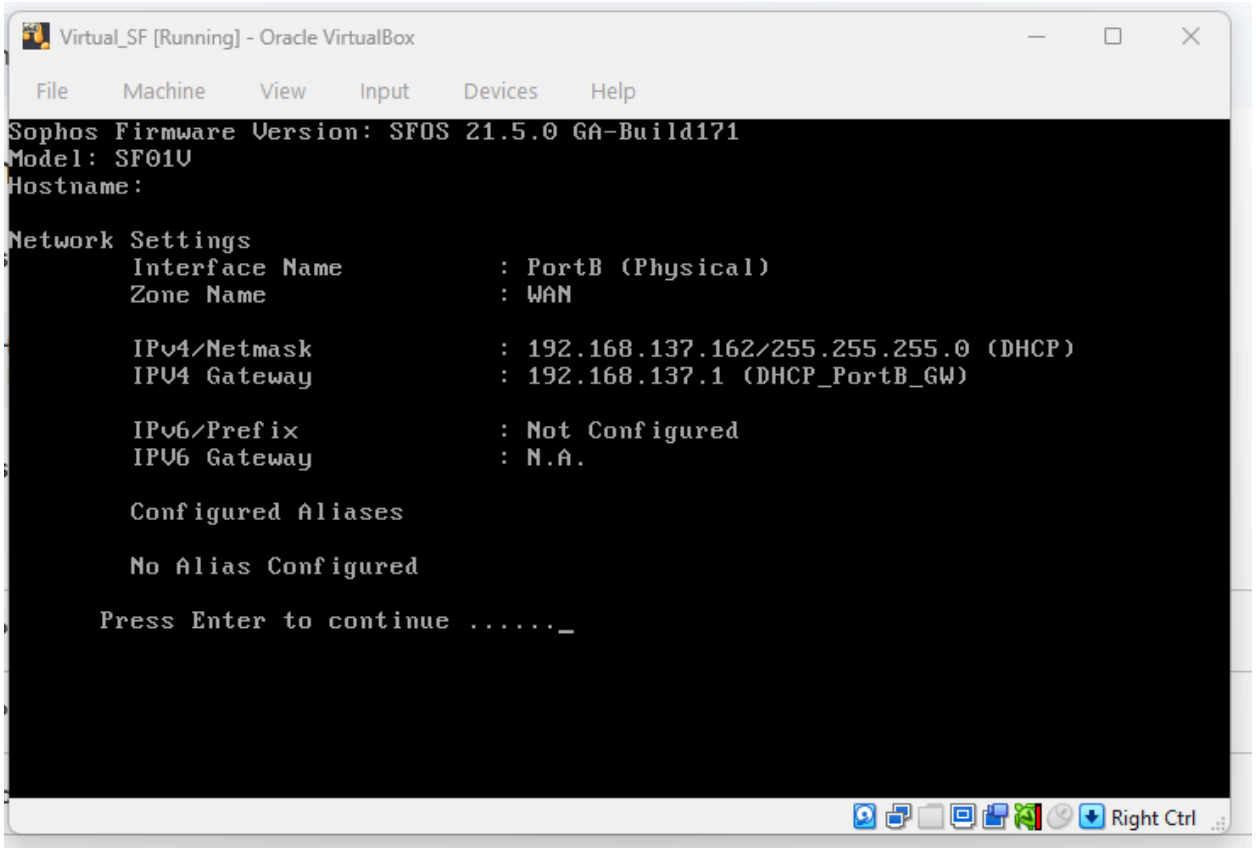


Step 4: Interface Configuration

After initialization, we have a CLI where we can begin to configure certain settings on Sophos. To change the interface configuration, we press **“1”** and continue to the interface settings overview and press Enter until we are taken to the section to change our settings then we press **“y”** symboling **“Yes”** which means that we are ready to change our setting, we are to change the IPv4 address to be in the range for the Port A, which we configure it earlier which in my case is **“192.168.56.101/24”** and your computer would give ip address to Port B as this is your bridged adapter to access the internet. Snippet below shows the configuration, and we are not to configure the IPv6 address as we will not be requiring it in this lab.

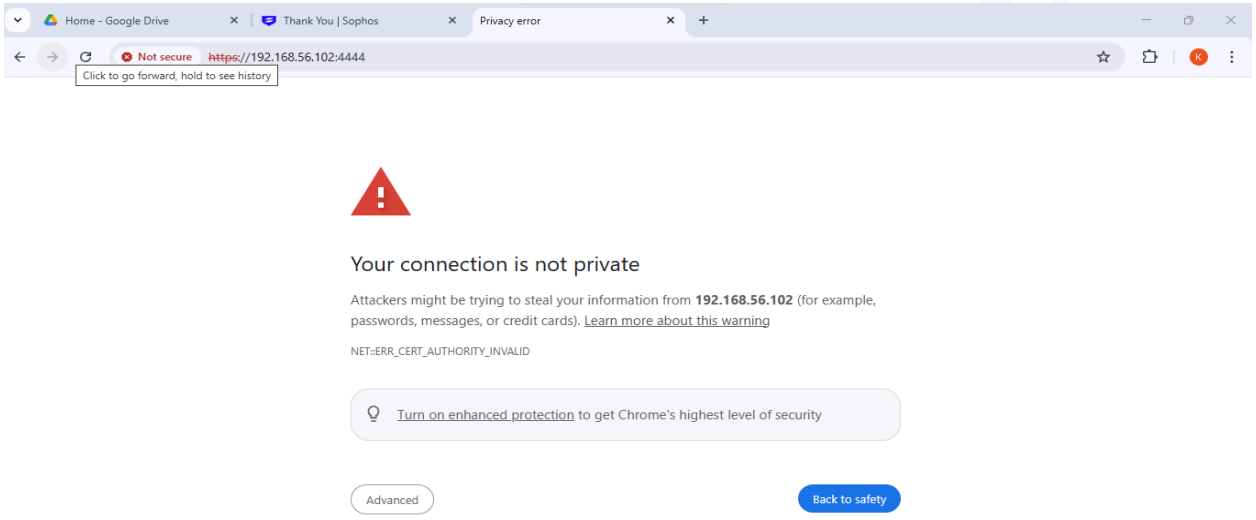


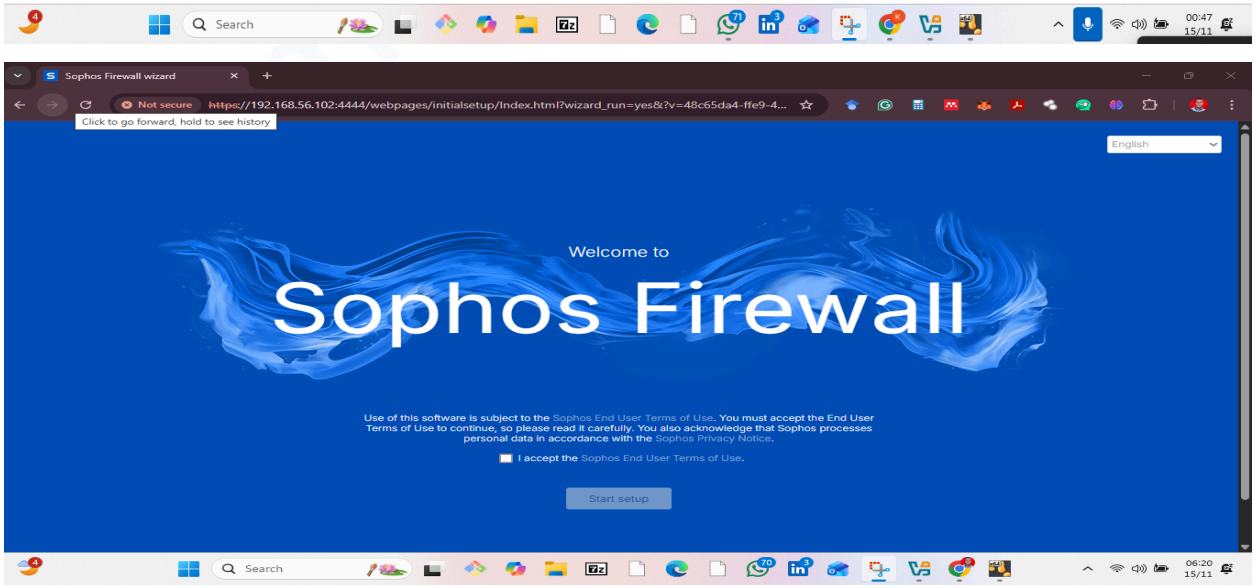




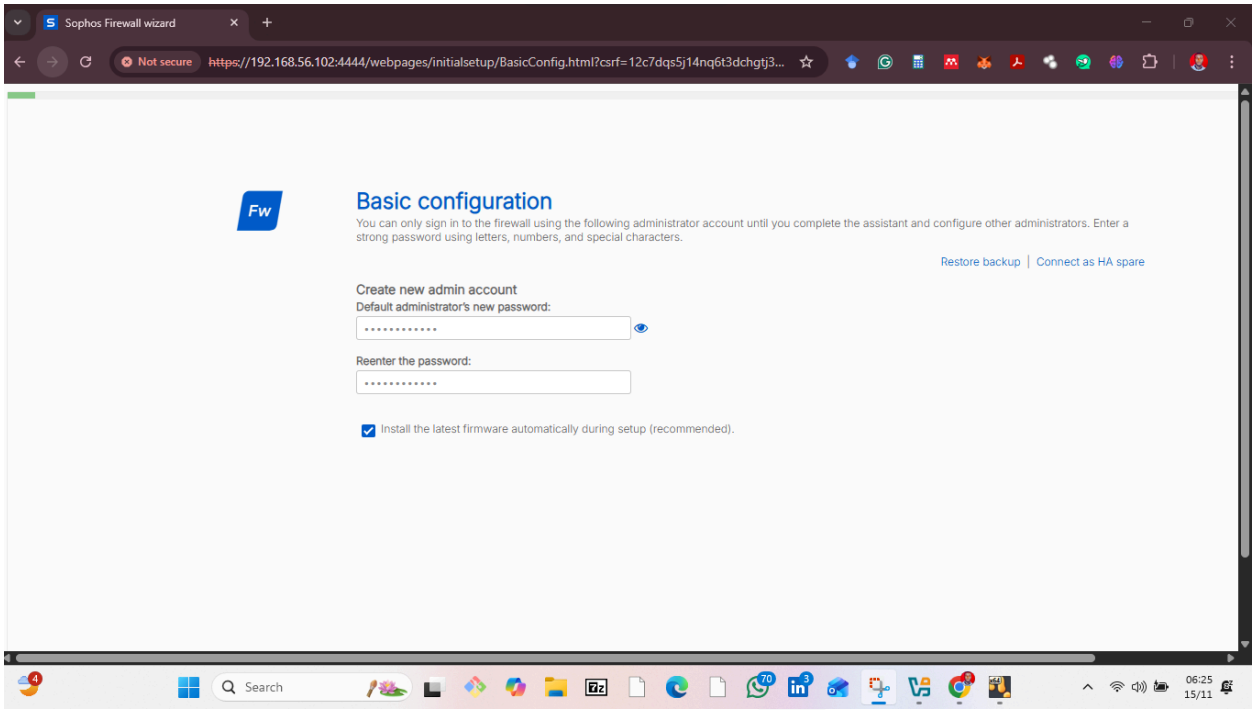
Step 5: Browser Access to further configure the Sophos Firewall

To further configure the Sophos Firewall through the browser, we would require the IP address that we configured to the interface in the previous step, which in my case is **“192.168.56.101”**, and through the port **“4444”** and using the **“HTTPS”** protocol, so the URL to access the Sophos firewall in my case is https://192.168.56.101:4444 (yours would be different)
The snippet below shows the process of accessing my Sophos firewall dashboard through my browser (It might take a while before the dashboard is ready)

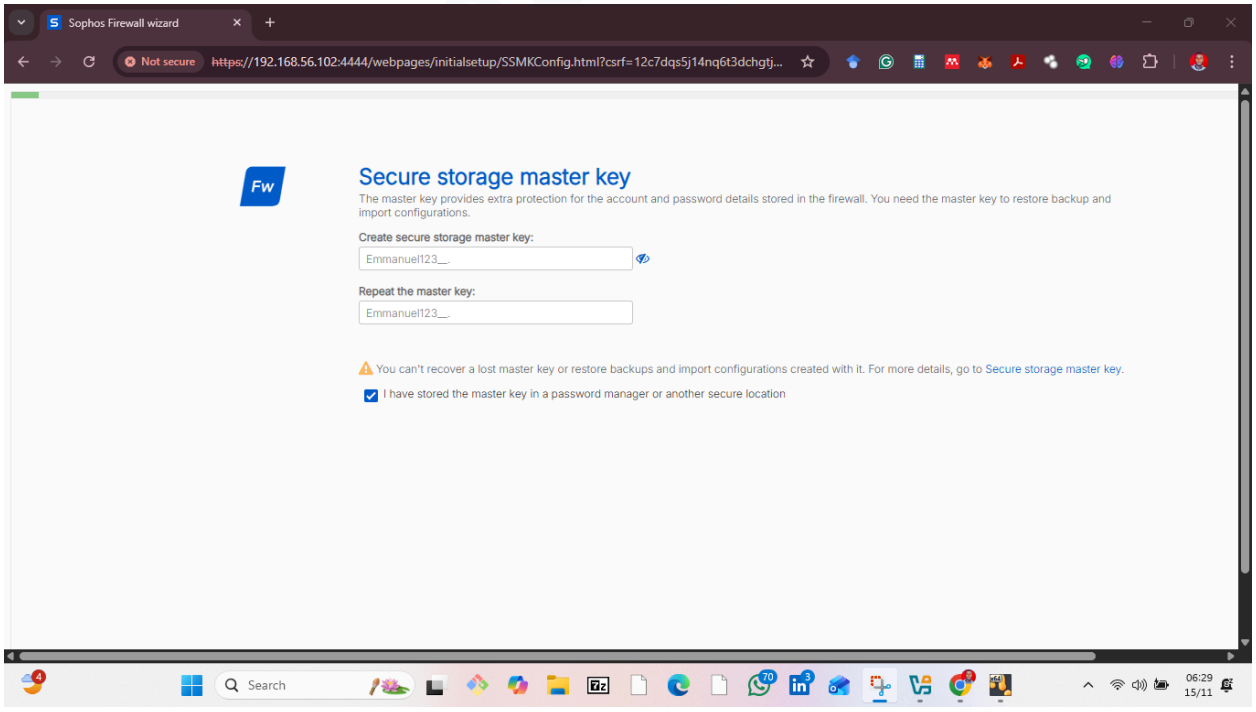




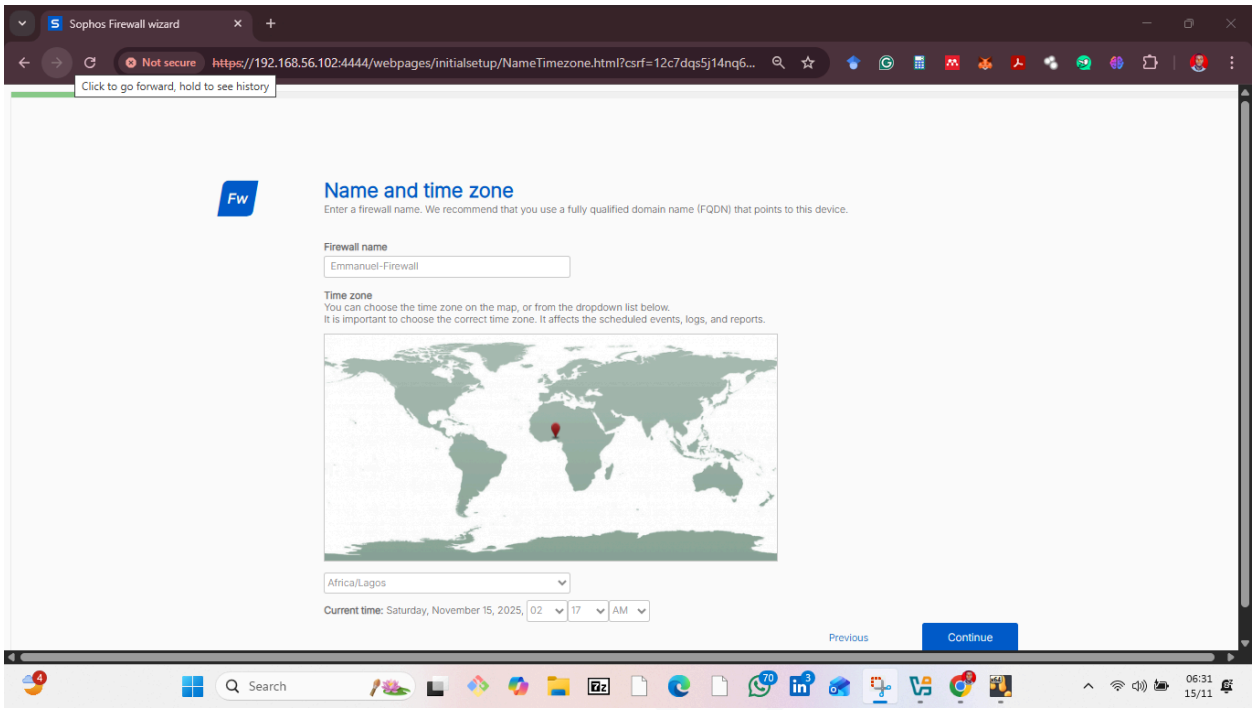
Step 6: Further Configuration on Browser's Dashboard



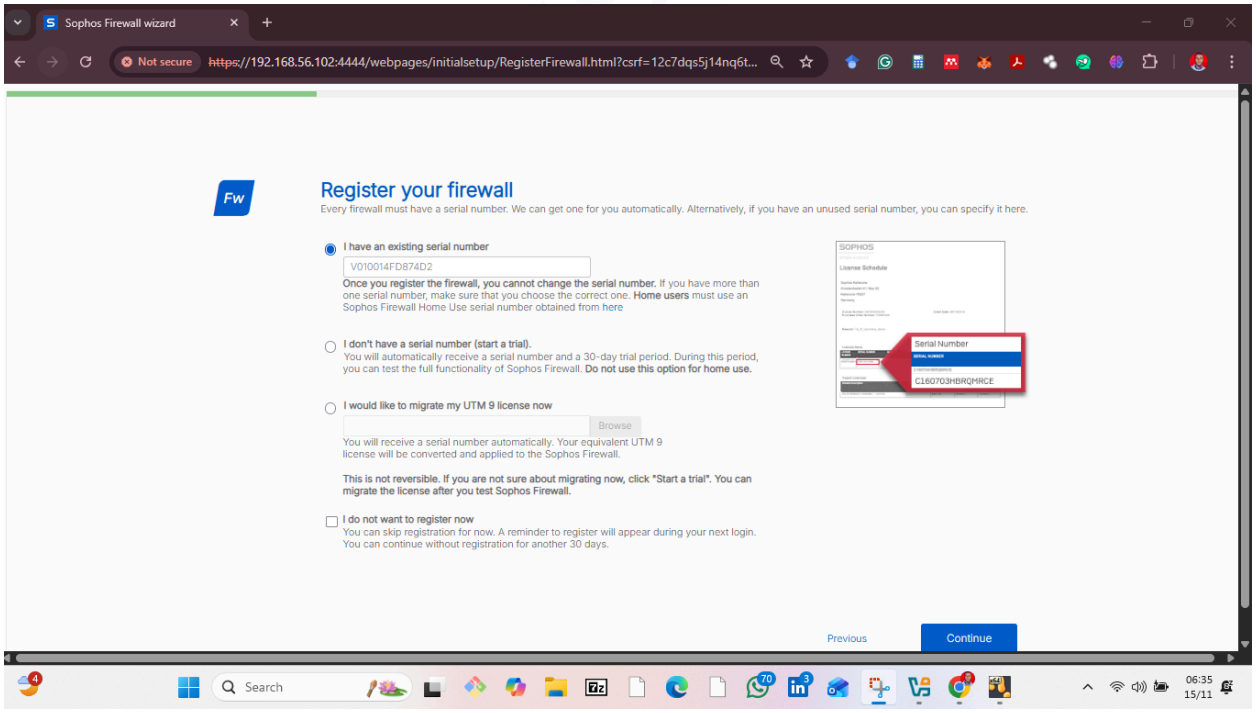
As seen above, after accessing the Sophos dashboard on the browser, we would perform certain basic configurations, which include setting a new admin account password (this is the password to access your browser's dashboard and Sophos CLI going further)



The snippet shows the setting of a secure storage Key. This would be helpful if you ever need to restore a backup or import configurations.

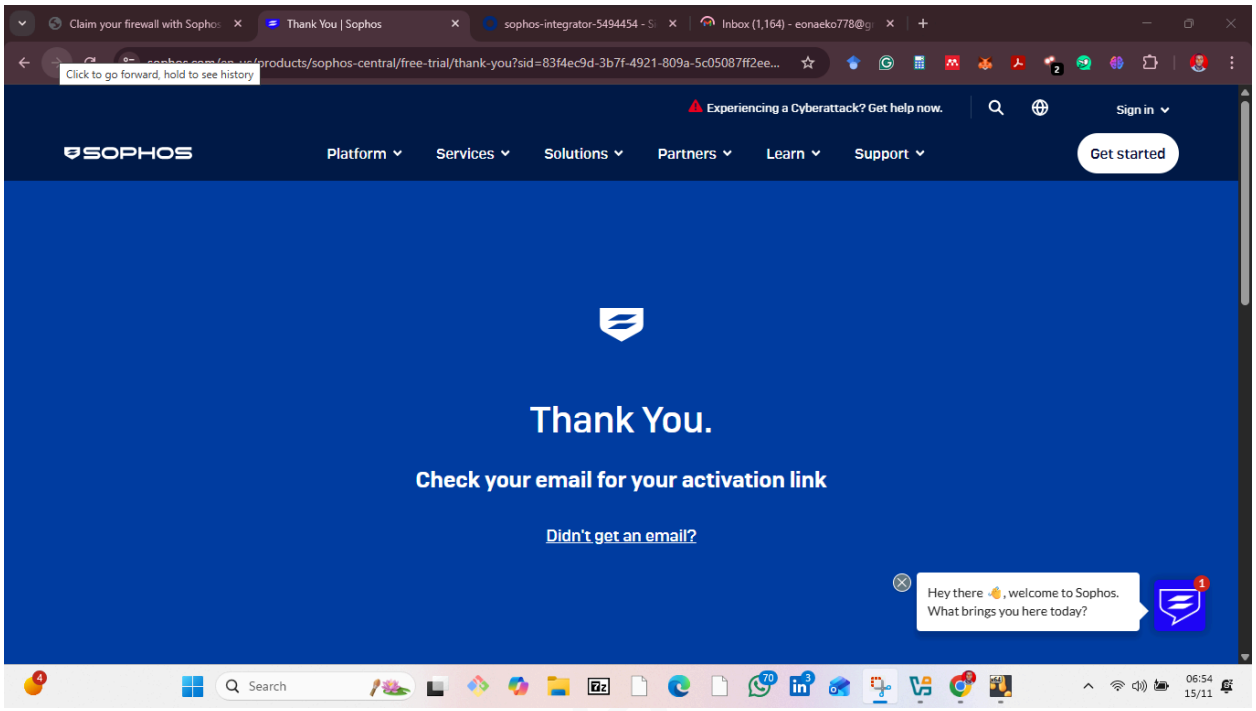


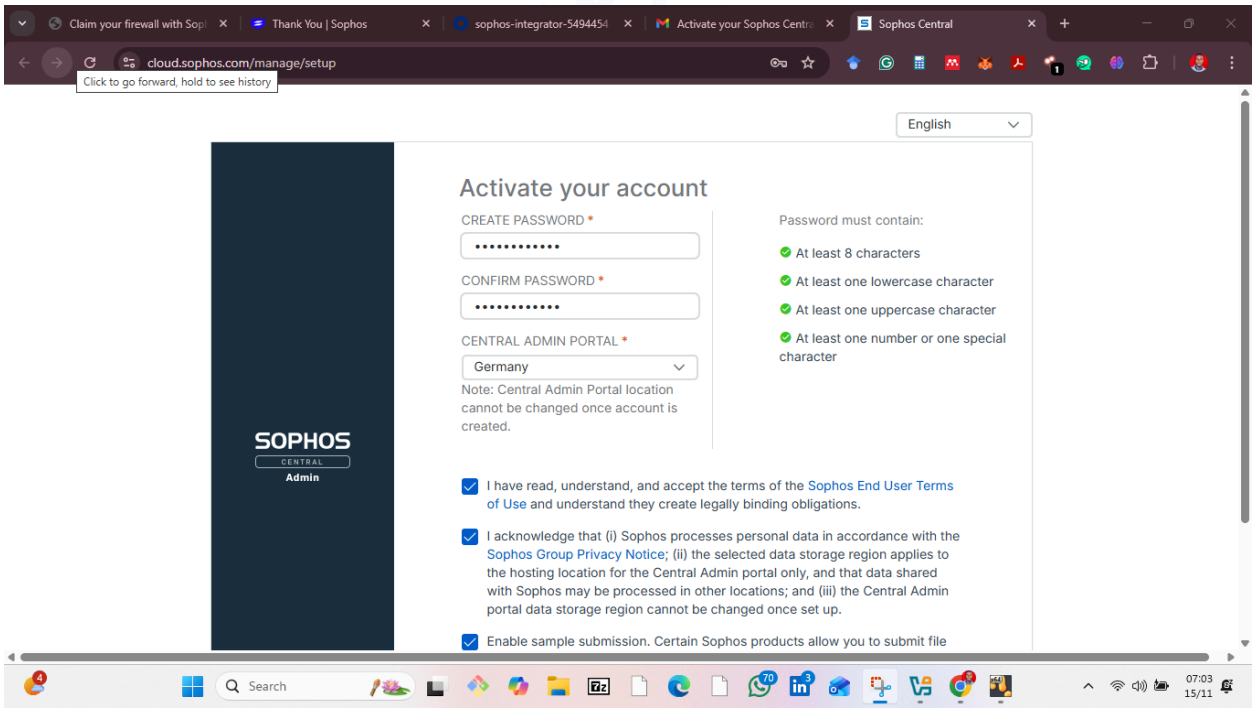
This snippet above sets the Name and time zones of the firewall

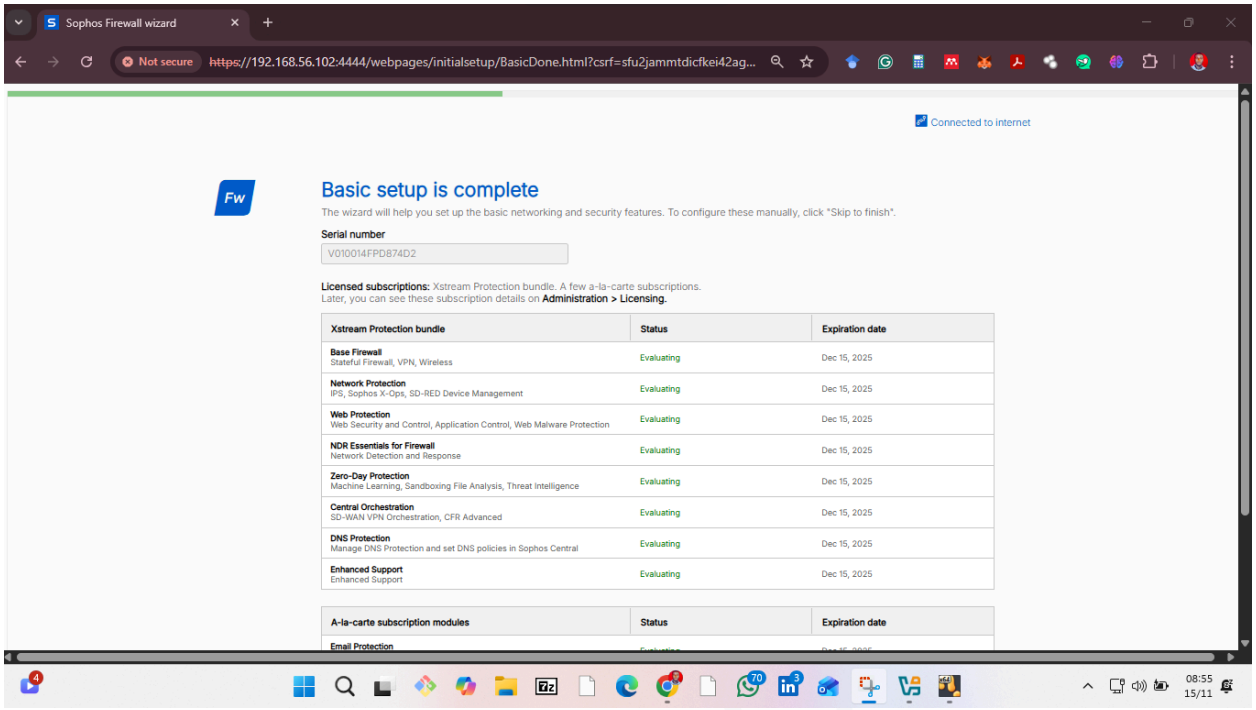


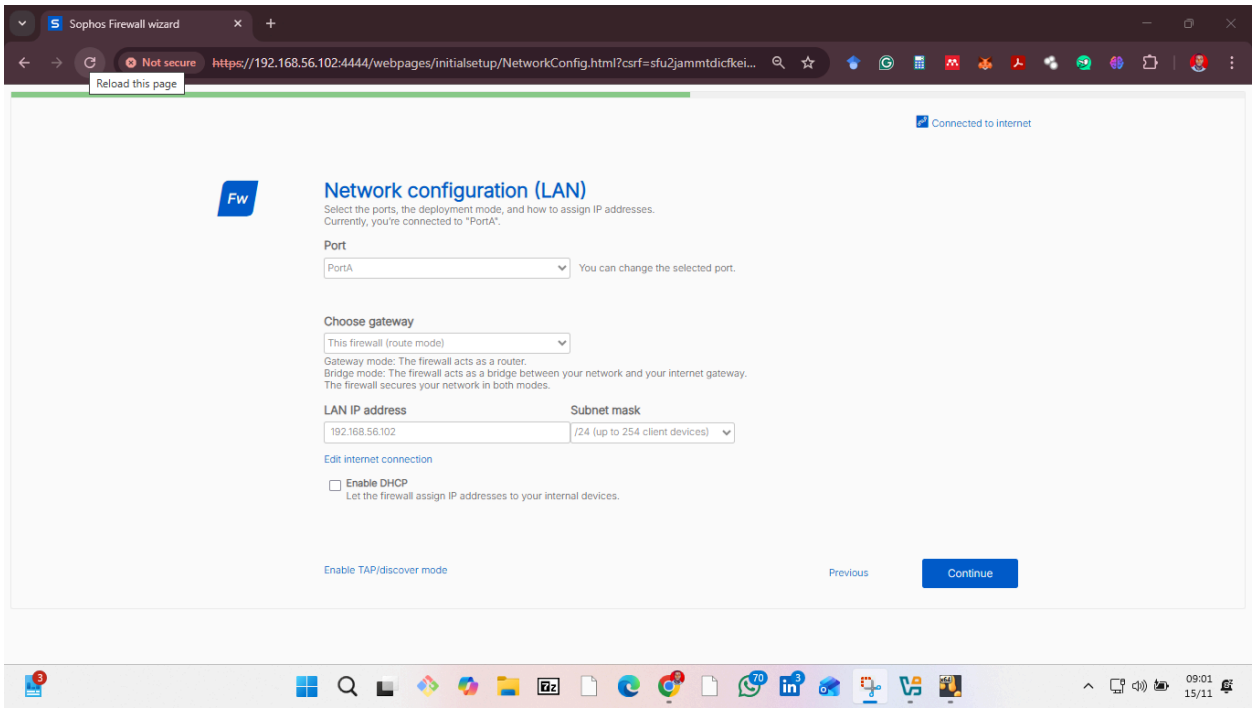
Afterwards, we need to register our firewall with our serial number, which was sent to us in our email when registering to

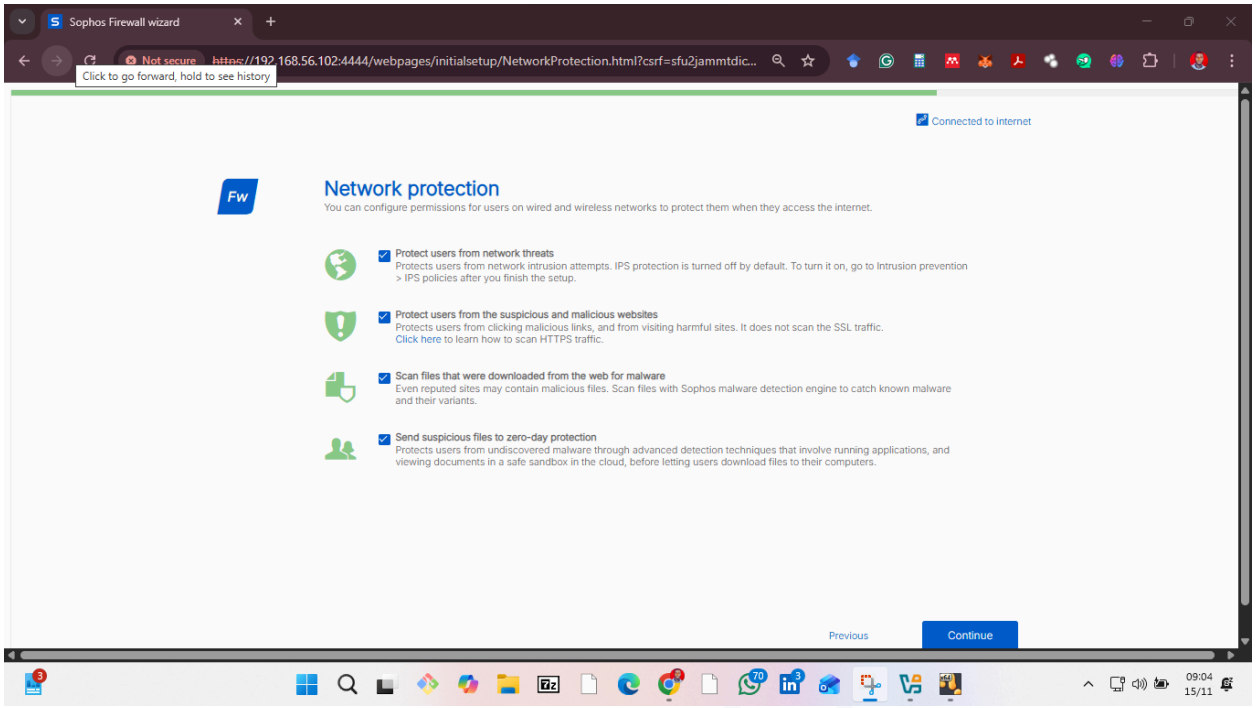
download our firewall, and then we create an account with Sophos Central, creating our password and activating the firewall, and finish up by setting up the network configuration and setting up network protection.



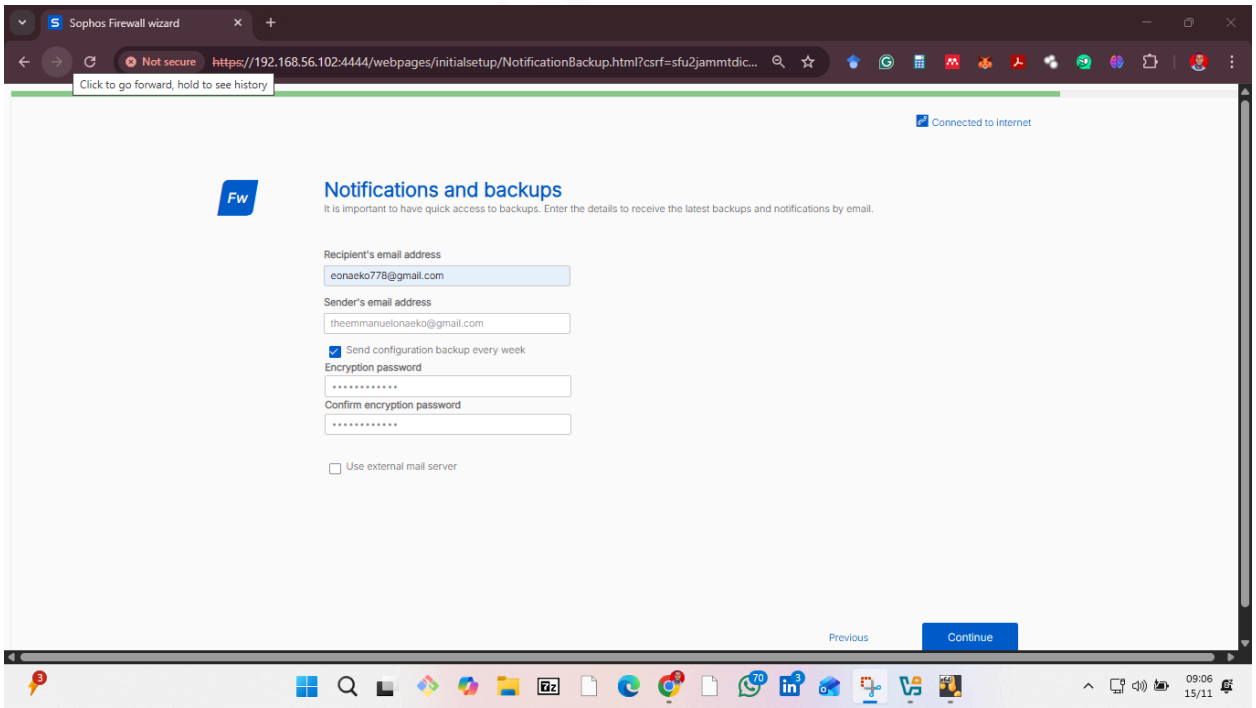


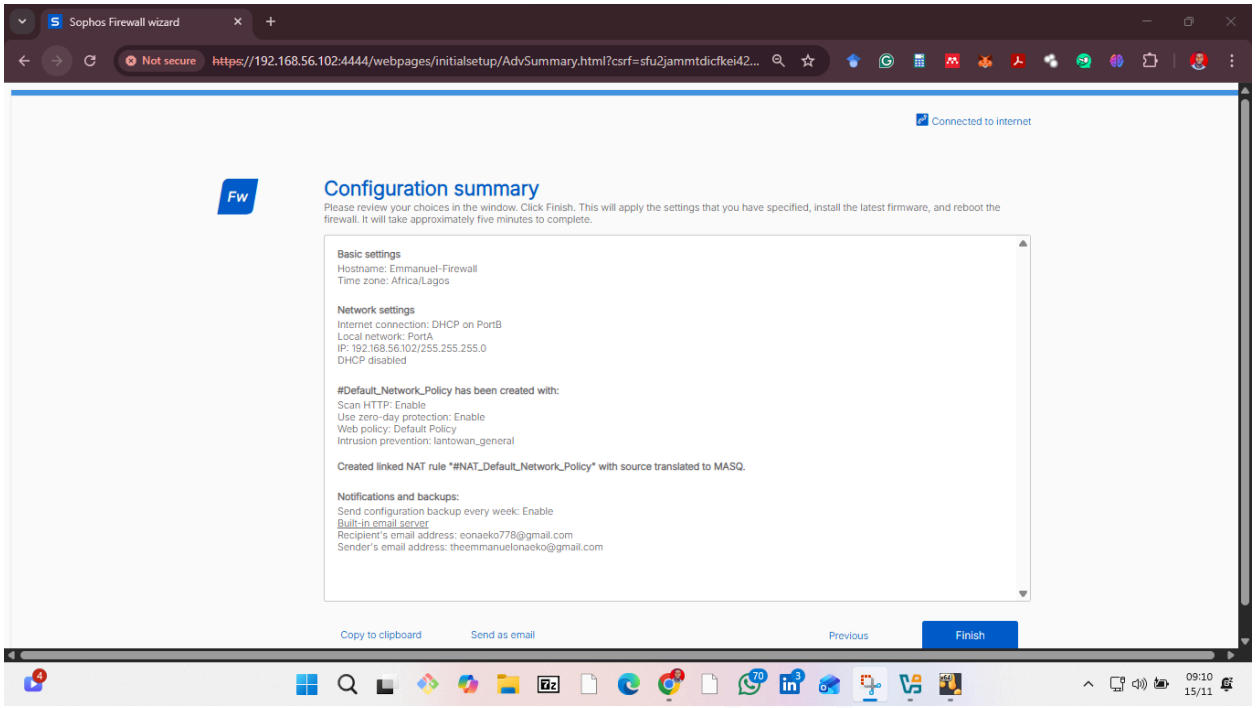

Sophos Firewall wizard
Not secure
https://192.168.56.102:4444/webpages/initialsetup/BasicDone.html?csrf=sfu2jammtdicfkei42ag...
Connected to internet
Basic setup is complete
The wizard will help you set up the basic networking and security features. To configure these manually, click "Skip to finish".
Serial number
V010014FPD874D2
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
Dec 15, 2025
Network Protection
IPS, Sophos X-Ops, SD-RED Device Management
Evaluating
Dec 15, 2025
Web Protection
Web Security and Control, Application Control, Web Malware Protection
Evaluating
Dec 15, 2025
NDR Essentials for Firewall
Network Detection and Response
Evaluating
Dec 15, 2025
Zero-Day Protection
Machine Learning, Sandboxing File Analysis, Threat Intelligence
Evaluating
Dec 15, 2025
Central Orchestration
SD-WAN VPN Orchestration, CFR Advanced
Evaluating
Dec 15, 2025
DNS Protection
Manage DNS Protection and set DNS policies in Sophos Central
Evaluating
Dec 15, 2025
Enhanced Support
Enhanced Support
Evaluating
Dec 15, 2025
A-la-carte subscription modules
Status
Expiration date
Email Protection
08:55
15/11

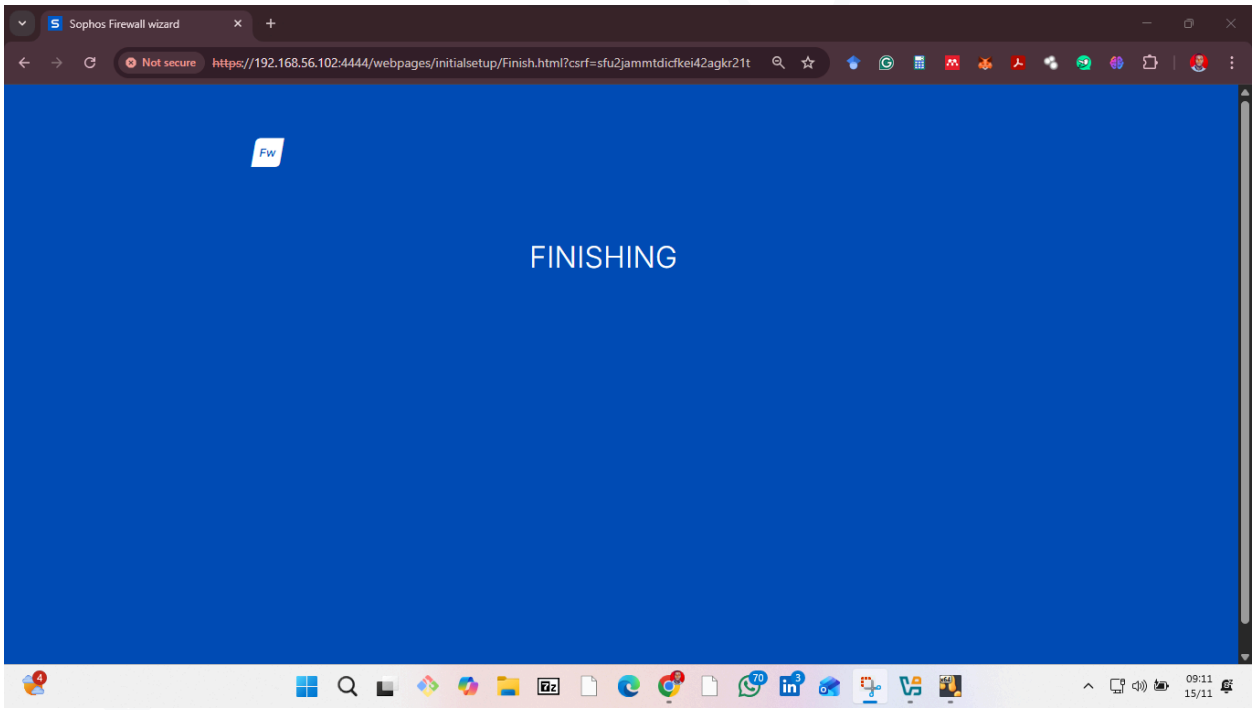

Sophos Firewall wizard
Not secure
Reload this page
https://192.168.56.102:4444/webpages/initialsetup/NetworkConfig.html?csrf=sfu2jammtdicfkei...
Connected to internet
Network configuration (LAN)
Select the ports, the deployment mode, and how to assign IP addresses.
Currently, you're connected to "PortA".
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
192.168.56.102
Subnet mask
/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
09:01
15/11



Also, set up the notification and backup account with your e-mail, set your encryption password and review the configuration summary, and click Finish. This would cause the firewall to implement the configuration and restart to finish the basic setup.



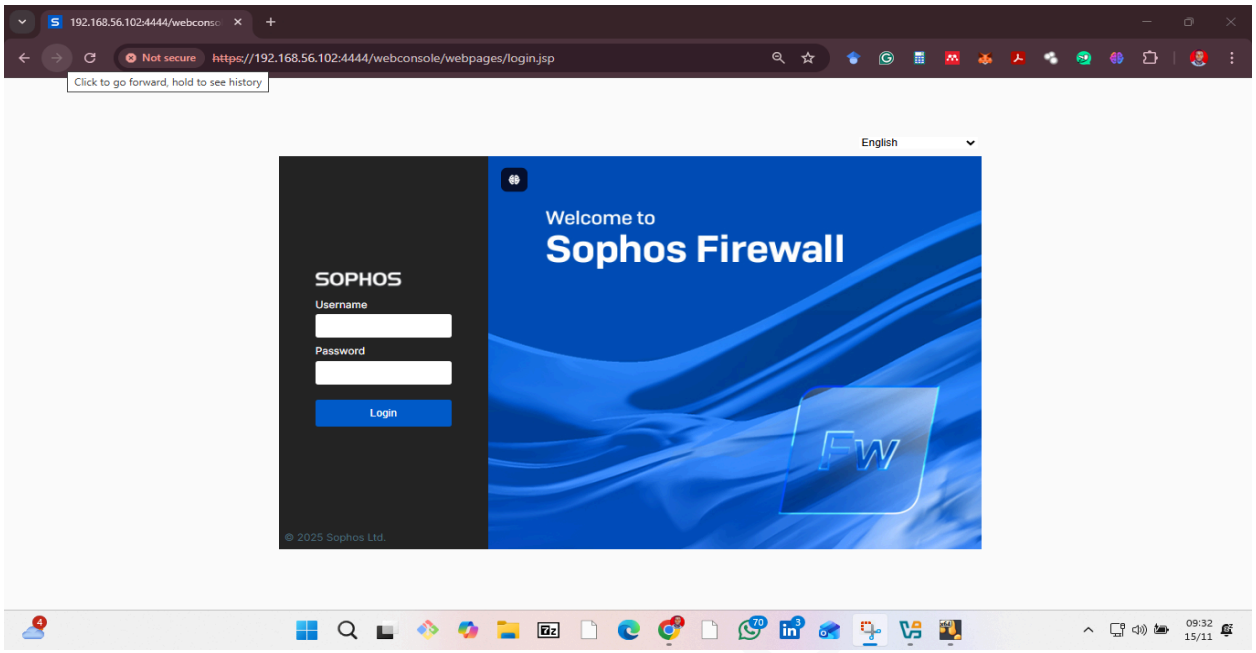


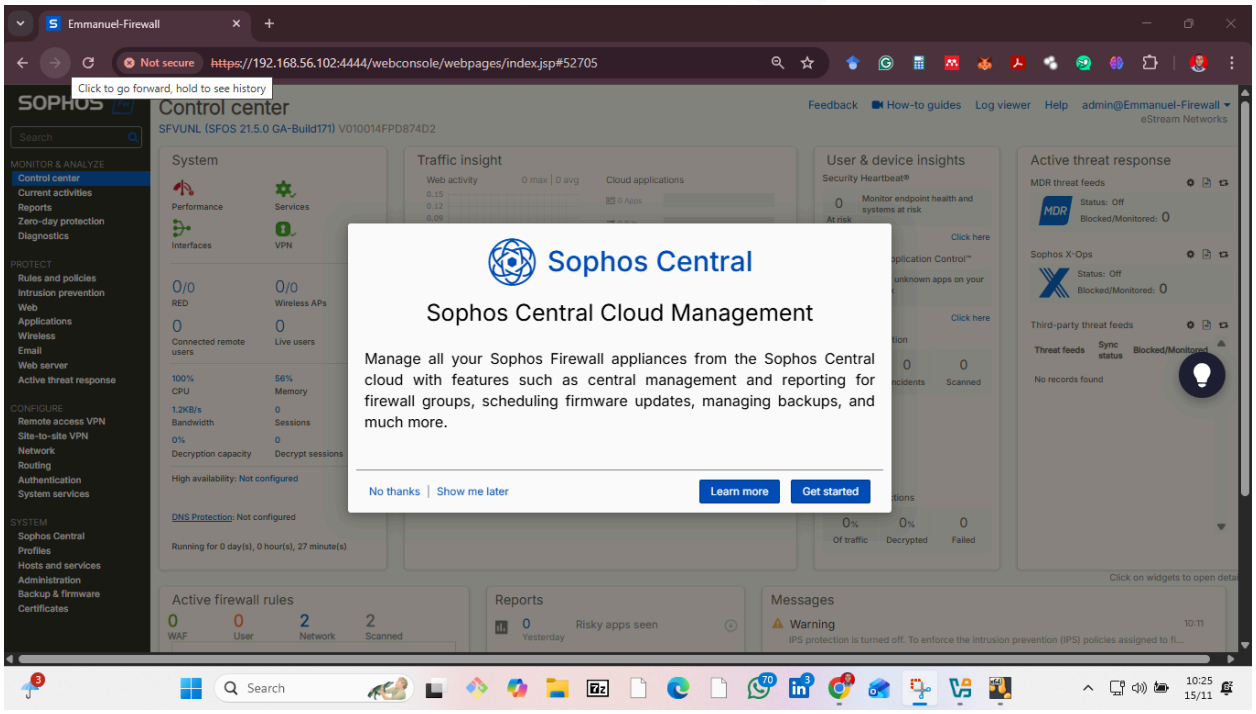


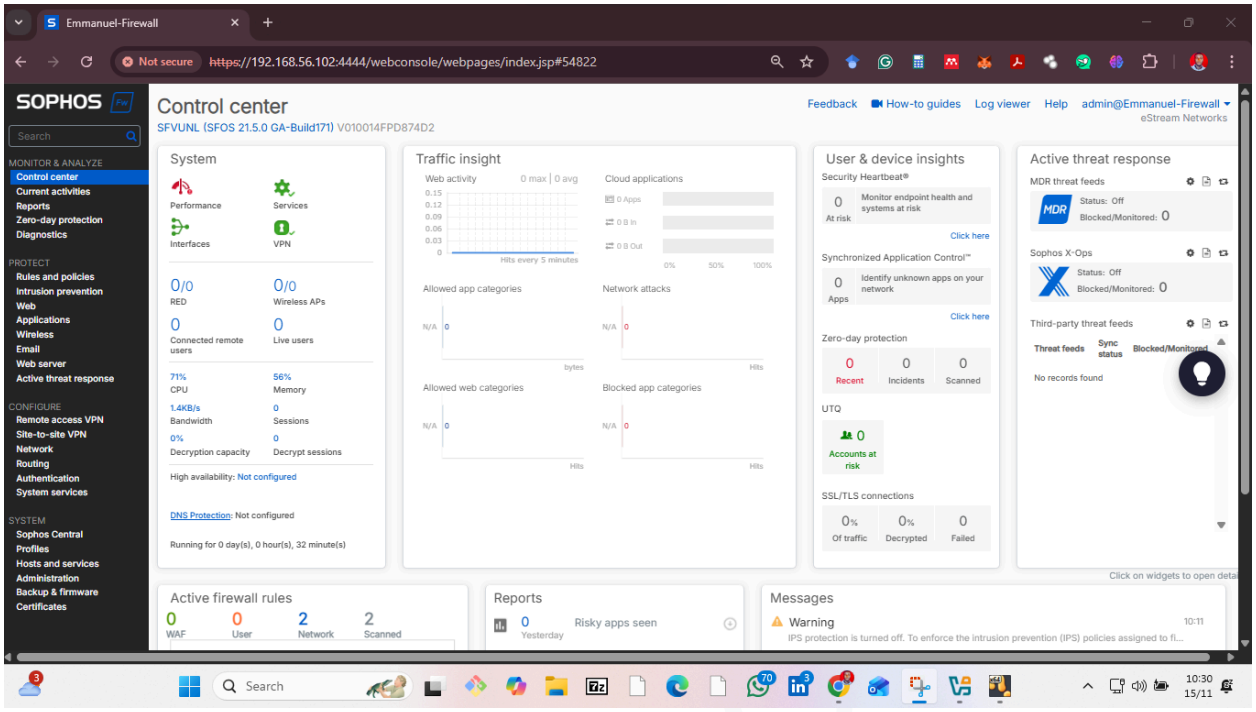
Step 7: Entering into the Sophos Web Console

After a complete restart of the Sophos Firewall, it takes you to the Web console for you to log in with credentials, where the username is **“admin,”** and the password is the **“password set up**

earlier” in the basic setup to log on to the web console of Sophos Central Cloud Management.

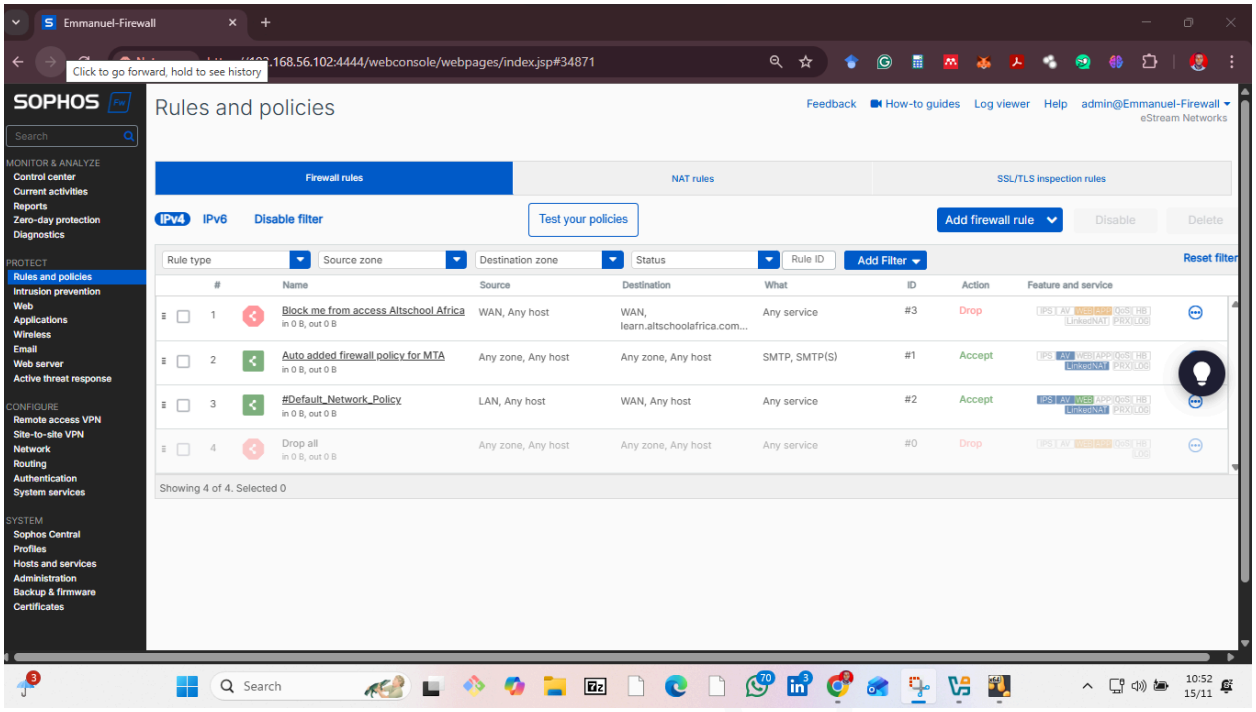




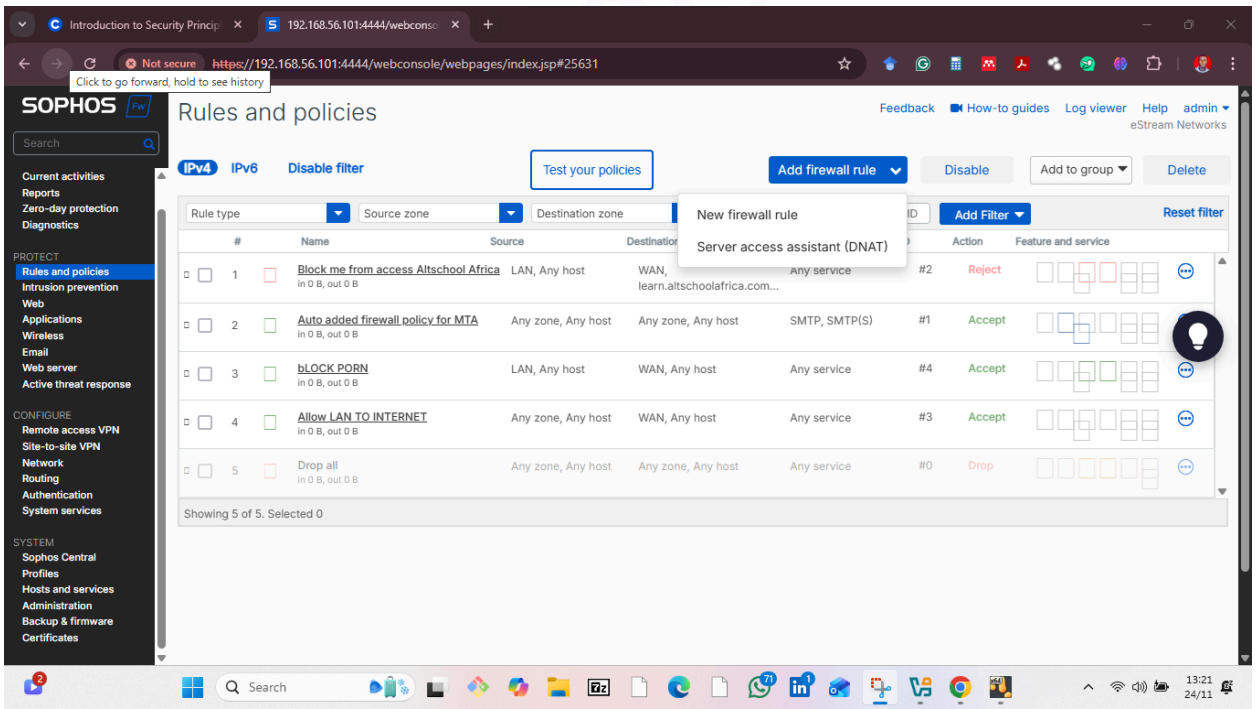


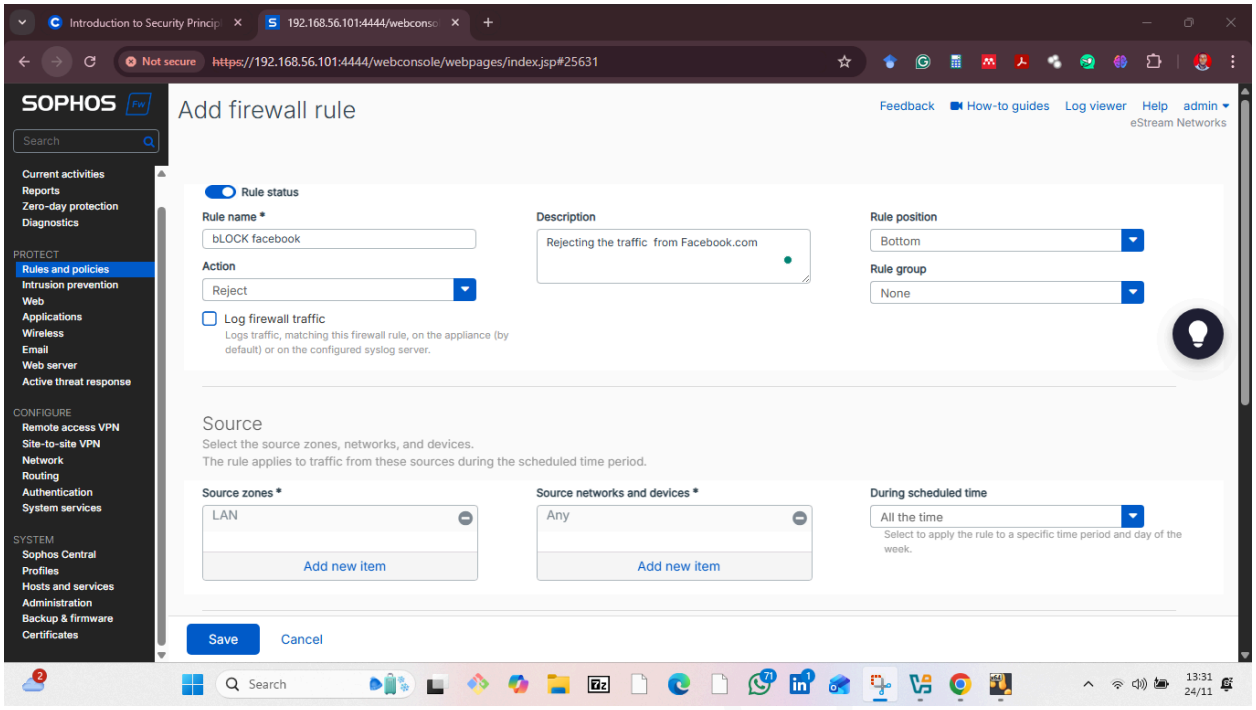
Firewall Rules, Configuration, and Testing

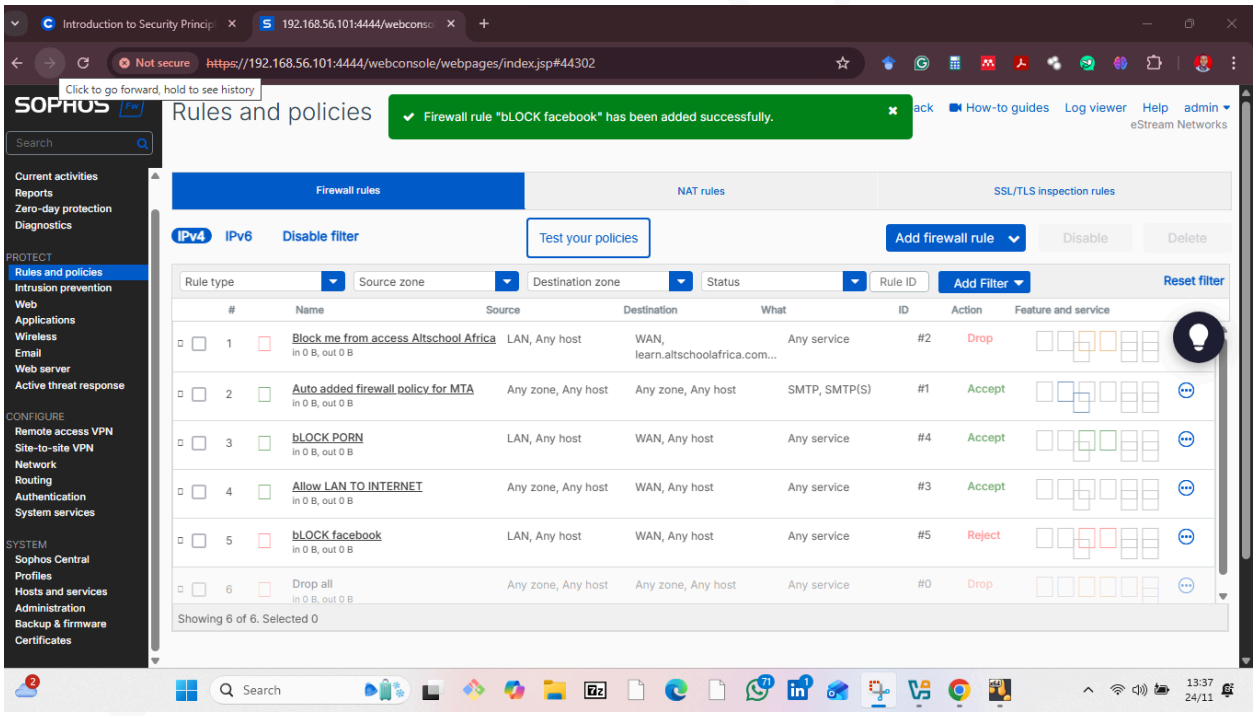
The Sophos Firewall is a next-generation firewall capable of a lot of various functions, such as web filtering, setting up VPNs, Intrusion detection, and prevention. After being able to access the **"Control Center"** on the web console dashboard, navigate to the "**Rules and Policies"** section to begin configuration of rules and policies. By default, you would meet three default configurations, which include **"Default_Network_policy"** *responsible for allowing necessary network traffic for essential system functions and default configurations to operate correctly without requiring users to manually create them*, **"Auto added_firewall_policy_for_MTA"** *responsible for enabling the Mail Transfer Agent (MTA) mode for the Email Protection Feature*, and **"Drop all"** *which acts as the final and most secure gatekeeper that ensure that any network traffic that does not explicitly match and is not allowed by a preceding firewall rule is blocked and discarded*, and those rules are all responsible for the essential setup and smooth running of the firewall, so they should not be tampered with in any way.



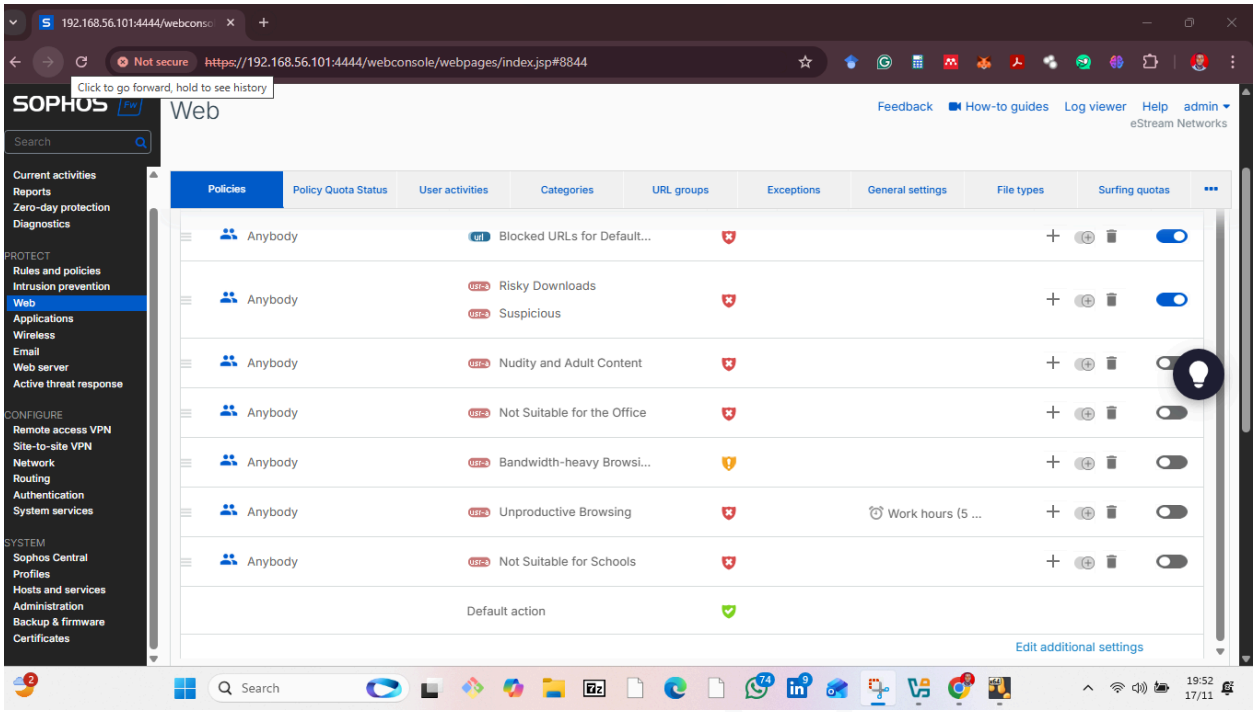
Clicking on the **"Add Firewall rule"** initiates a process to set up firewall rules to block or permit traffic as specified. The snippets below show the setup of a new firewall rule.

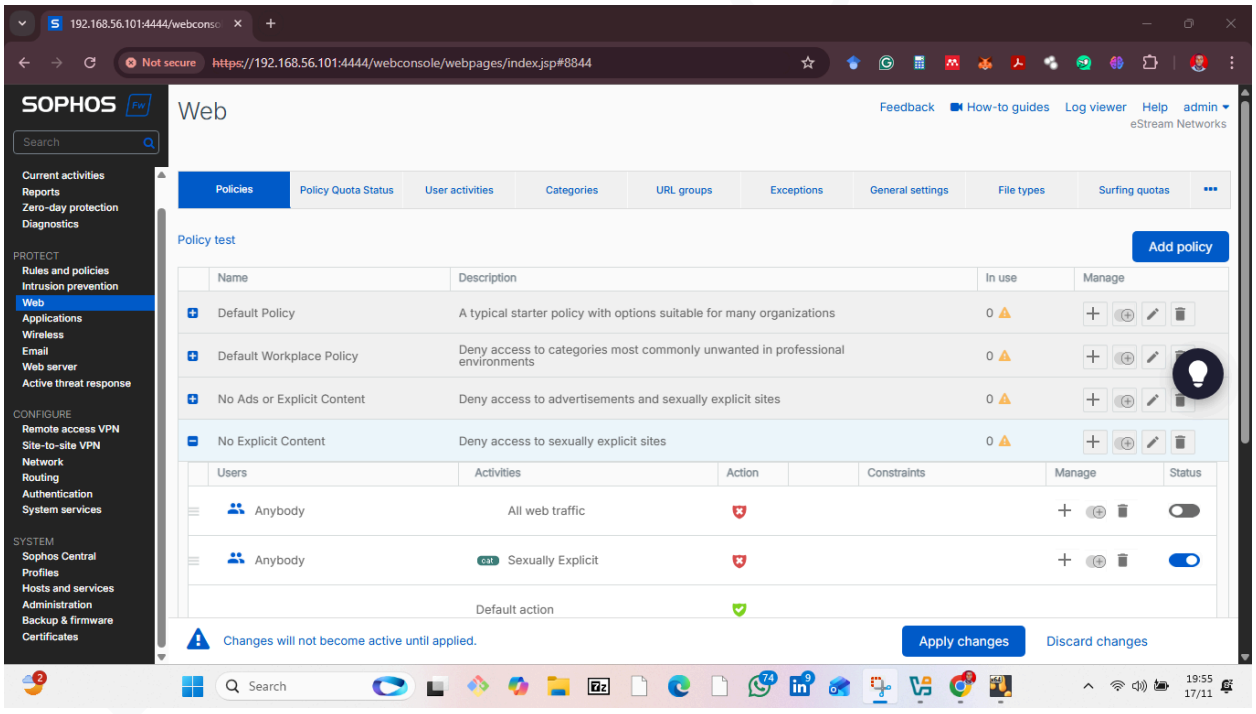






We can also set up web filtering policies to block specific types of traffic. To do this, we navigate to the **“web section”** and then explore different web polices that can be set up and then used during the creation of rules as web filters.
Snippets below show the exploration of web policies.

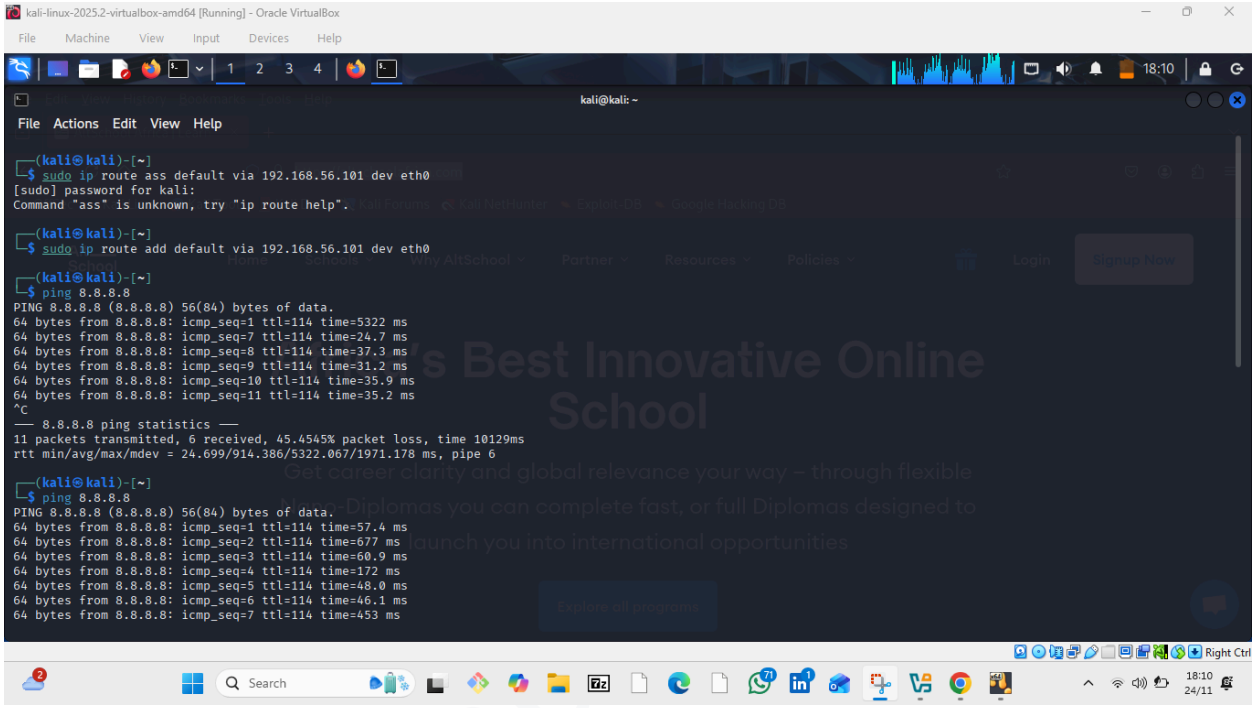


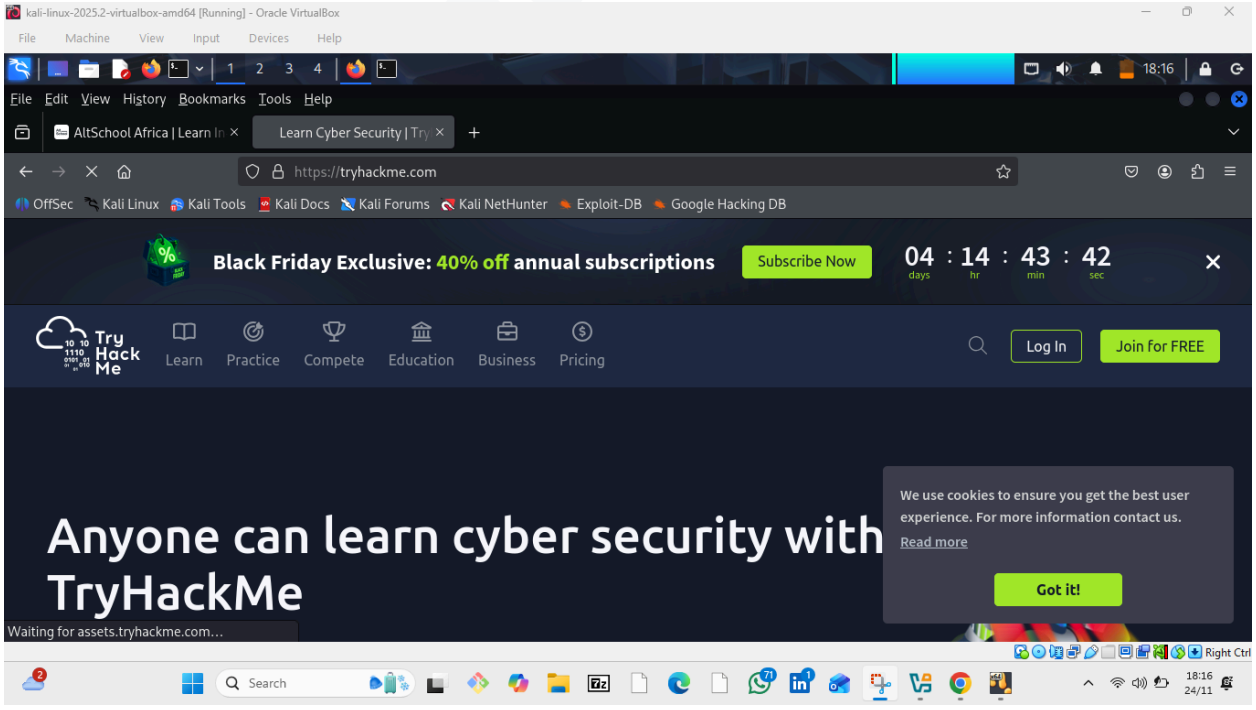


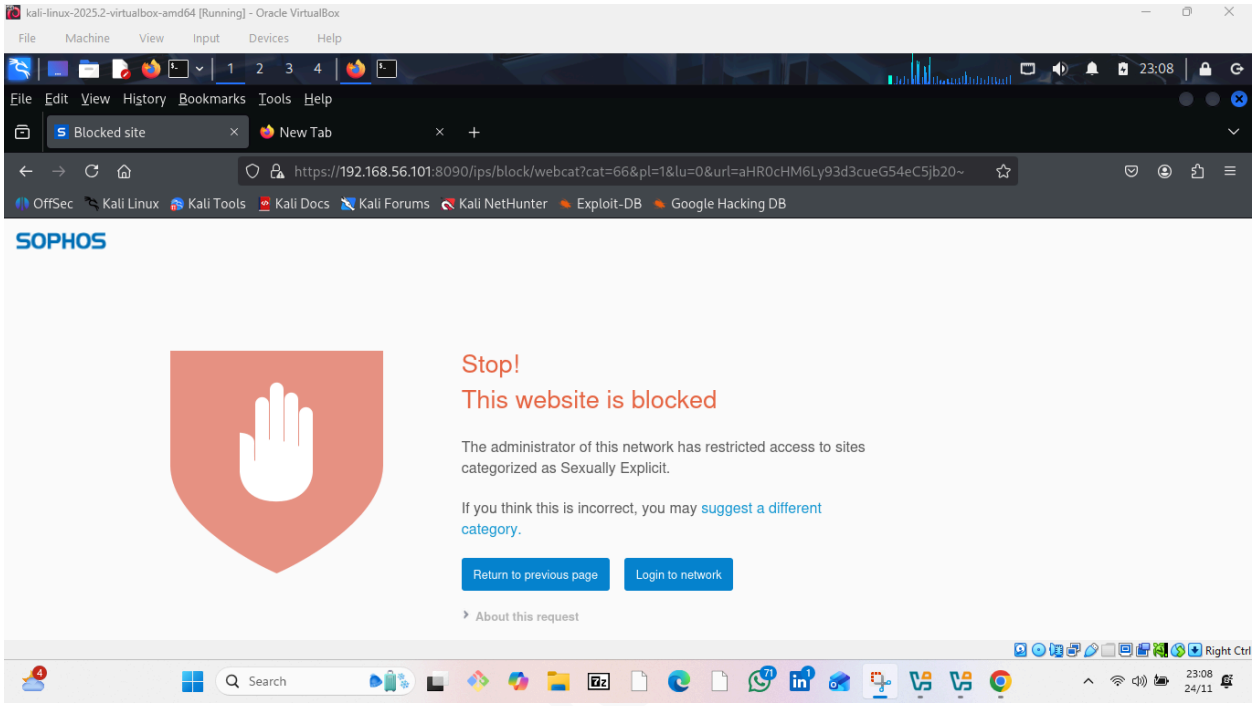
Testing of Firewall Rules

To test the firewall rules that were set up and configured, I set up a virtual machine with host only adapter, meaning that the adapter would belong to the LAN zone of the firewall, and then I routed traffic through the firewall so that it acted as the

gateway of the LAN zone using the command **“sudo ip route add default via 192.168.56.101 dev eth 0”**, and verified internet connectivity through ping tests to 8.8.8.8 and access a website page on the Kali VM after I visited a prohibited site to see how Sophos responds by blocking the traffic as seen in the snippets below.







Summary: This serves as a step-by-step guide for deploying the Sophos next-generation firewall (NGFW) in a virtual environment.

The process begins with downloading the virtual installer from the Sophos website and importing the corresponding OVF file into VirtualBox. Critical to the installation is the network setup, which involves configuring two virtual adapters: Adapter 1 is set up as a host-only network to facilitate communication between the host machine and the VM, while Adapter 2 is configured as a bridged adapter to provide the VM with internet access for updates. The initial installation wizard requires an admin password, which by default is "admin".

Following the initial startup, the user moves to the Command Line Interface (CLI) to configure the network interfaces. This includes assigning a static IPv4 address within the host-only

range (e.g., 192.168.56.101/24) to Port A, while allowing Port B (the bridged adapter) to obtain its address automatically.

Finally, the remaining configuration is performed via the web-based dashboard, which is accessed using the static IP and port 4444 (e.g., https://192.168.56.101:4444). This phase covers essential security steps such as setting a new admin password, creating a secure storage key for backups, setting the firewall's name and time zone, registering the firewall with a serial number to Sophos Central, setting up the notification and backup account, and completing network protection before the firewall implements the changes and restarts. The user can then log into the Sophos Web Console with the username "admin" and the newly established password.

The documentation concludes with the section on Firewall Rules, Configuration, and Testing. The system loads with three essential default rules: **"Default_Network_policy"** (allows necessary network traffic), **"Auto added_firewall_policy_for_MTA"** (enables the Mail Transfer Agent mode for Email Protection), and **"Drop all"** (blocks all non-matching traffic). The documentation guides the user on how to Add Firewall rules and set up web filtering policies. Rules are tested by setting up a virtual machine in the LAN zone and verifying internet access and the firewall's blocking response to prohibited sites.