

UNIVERSIDAD LUTERANA SALVADOREÑA

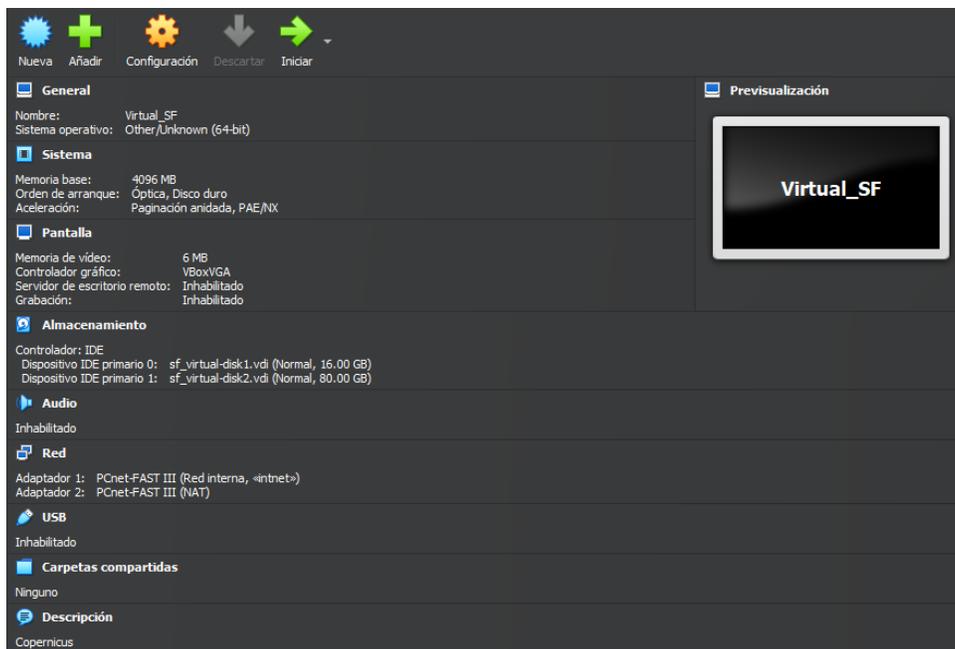
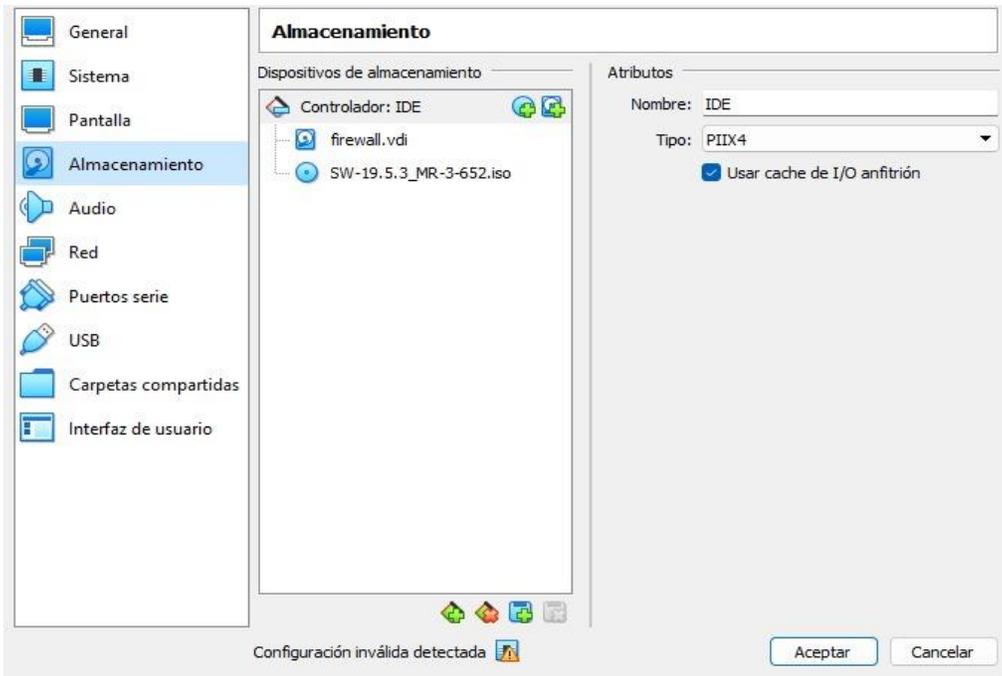
Facultad	Ciencias del hombre y la naturaleza			
Asignatura	REDES II			
Profesor	Eduardo Chachagua			
Año	2023	Ciclo	2	
Fecha de entrega			Actividad	
05/12/2023			PARCIAL 4	
Tema	PARCIAL 4			

Estudiante

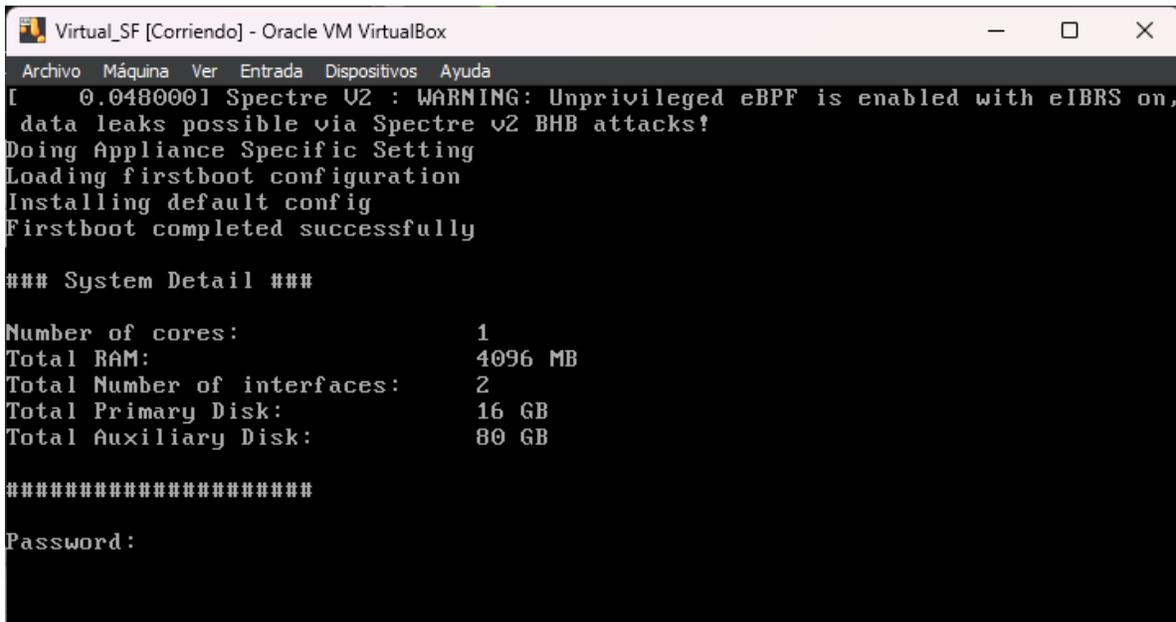
No	Apellidos	Nombres	Carnet
1	Cisneros Hernández	Salvador Josué	CH01137269
2	Vásquez Mejía	Sebastián Emilio	VM01137362
3	Henríquez Segovia	Diego Alejandro	HS01137376
4	Quinteros Valles	David Eugenio	QV01137367

Descargamos una ISO del firewall Sophos XG.





Ejecutamos la máquina virtual e Ingresamos la contraseña admin.



```
Virtual_SF [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[ 0.048000] Spectre v2 : WARNING: Unprivileged eBPF is enabled with eIBRS on,
data leaks possible via Spectre v2 BHB attacks!
Doing Appliance Specific Setting
Loading firstboot configuration
Installing default config
Firstboot completed successfully

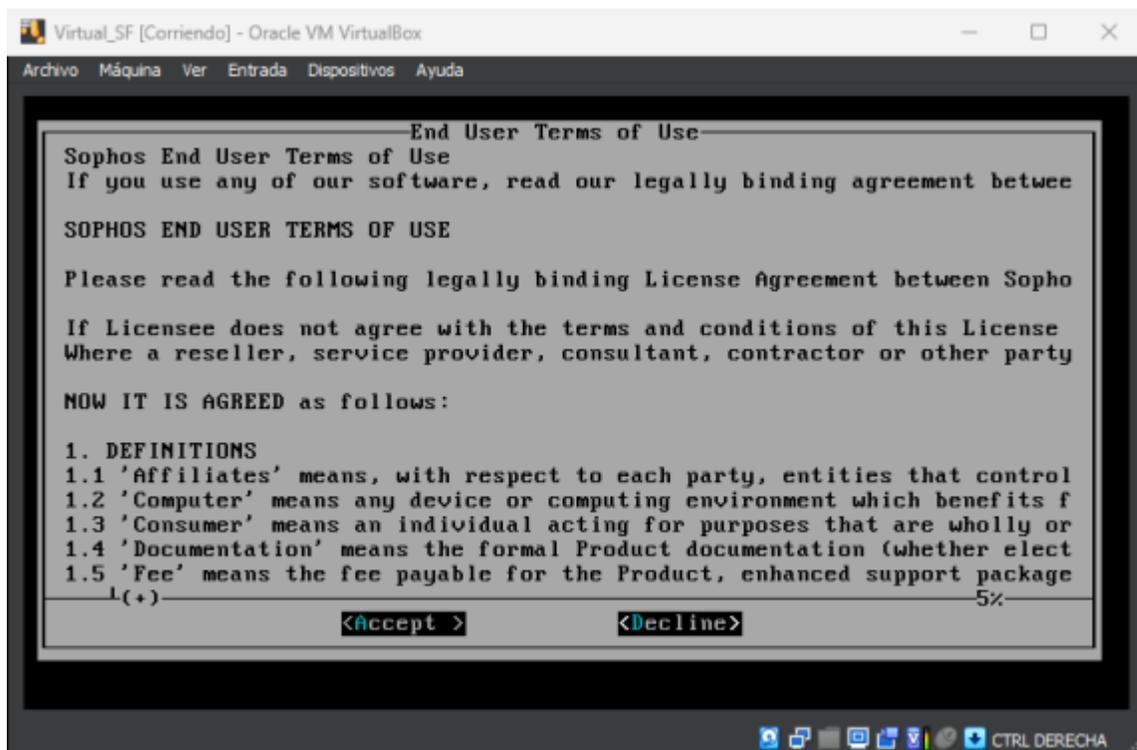
### System Detail ###

Number of cores:          1
Total RAM:                4096 MB
Total Number of interfaces: 2
Total Primary Disk:      16 GB
Total Auxiliary Disk:    80 GB

#####

Password:
```

Aceptamos los términos.



```
Virtual_SF [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

-----End User Terms of Use-----
Sophos End User Terms of Use
If you use any of our software, read our legally binding agreement between
SOPHOS END USER TERMS OF USE

Please read the following legally binding License Agreement between Sopho
If Licensee does not agree with the terms and conditions of this License
Where a reseller, service provider, consultant, contractor or other party
NOW IT IS AGREED as follows:

1. DEFINITIONS
1.1 'Affiliates' means, with respect to each party, entities that control
1.2 'Computer' means any device or computing environment which benefits f
1.3 'Consumer' means an individual acting for purposes that are wholly or
1.4 'Documentation' means the formal Product documentation (whether elect
1.5 'Fee' means the fee payable for the Product, enhanced support package
1(+)- 5%

<Accept >  <Decline>
```

Nos muestra un menú de opciones para configurar.

```
Sophos Firmware Version: SFOS 19.5.3 MR-3-Build652
Model: SF01U
Hostname:

Main Menu

AA. Device Activation
  1. Network Configuration
  2. System Configuration
  3. Route Configuration
  4. Device Console
  5. Device Management
  6. UPN Management
  7. Shutdown/Reboot Device
  0. Exit

Select Menu Number [0-7]: 1
```

Seleccionamos la primera opción para ver las conexiones de red y Presionamos Enter hasta regresar al menú principal ya que usaremos la configuración que tiene por defecto.

```
Sophos Firmware Version: SFOS 19.5.3 MR-3-Build652
Model: SF01U
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 .....
```

```
Sophos Firmware Version: SFOS 19.5.3 MR-3-Build652
Model: SF01U
Hostname:

Network Settings
Interface Name      : PortB (Physical)
Zone Name          : WAN

IPv4/Netmask       : 10.0.3.15/255.255.255.0 (DHCP)
IPv4 Gateway       : 10.0.3.2 (DHCP_PortB_GW)

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

Configured Aliases

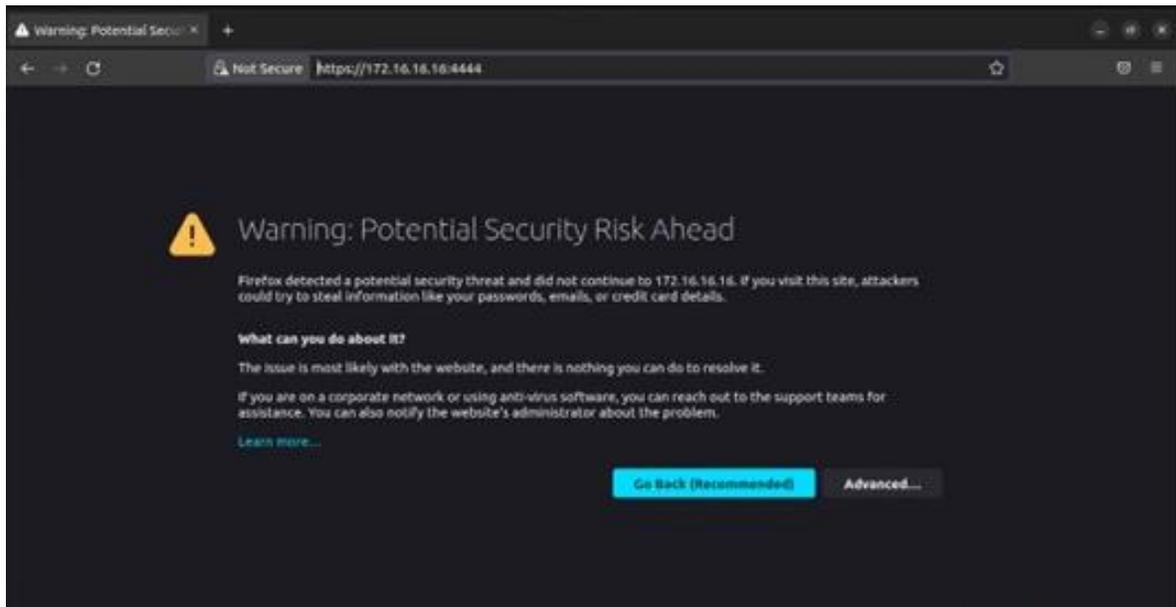
No Alias Configured

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

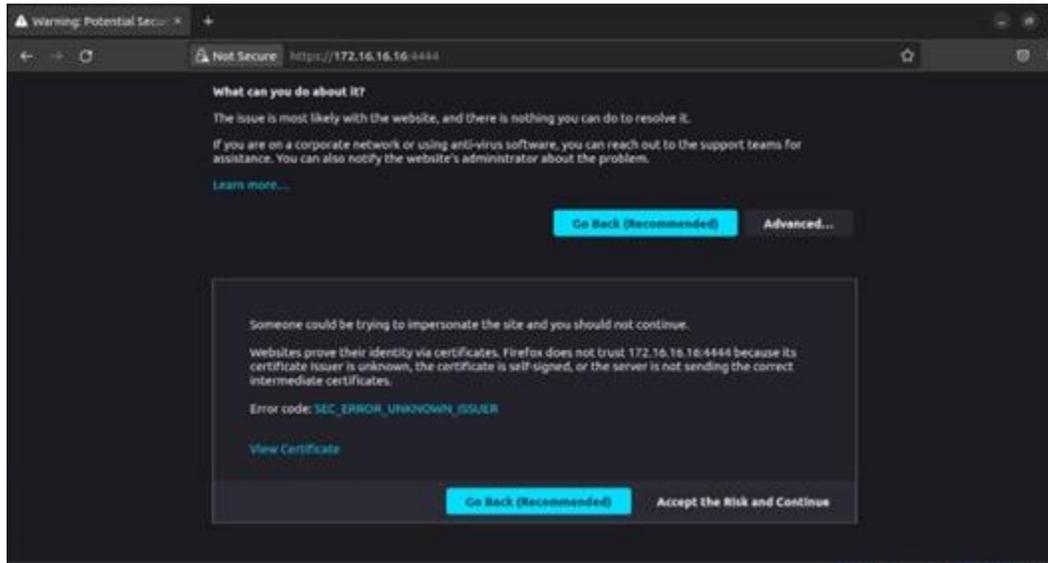
Para la ejecución del Firewall utilizaremos otra máquina virtual.



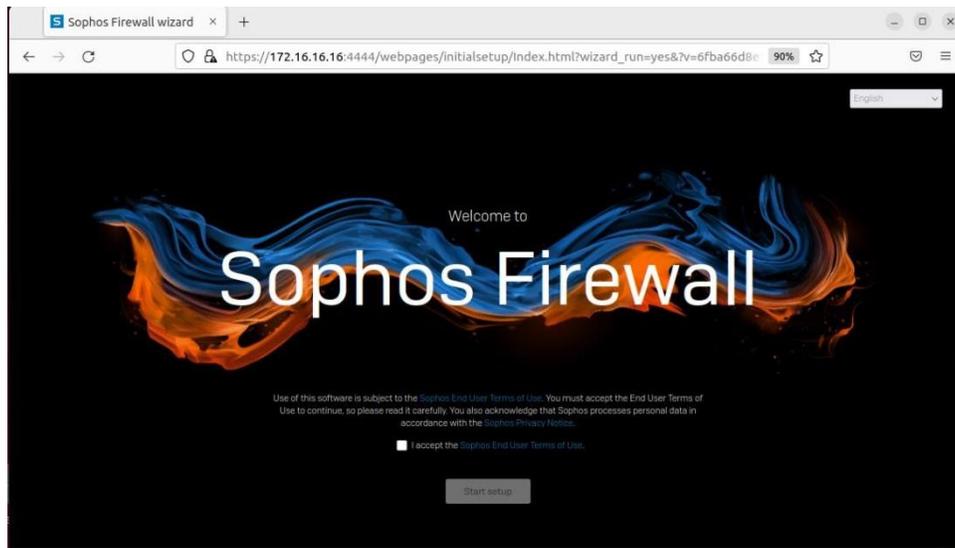
Abrimos el navegador en la maquina virtual e ingresamos la dirección <https://172.16.16.16:4444/>, aparecerá un mensaje de advertencia en el que seleccionaremos opciones avanzadas.



Aceptar el riesgo y continuar.



Podremos ver el entorno gráfico del firewall.

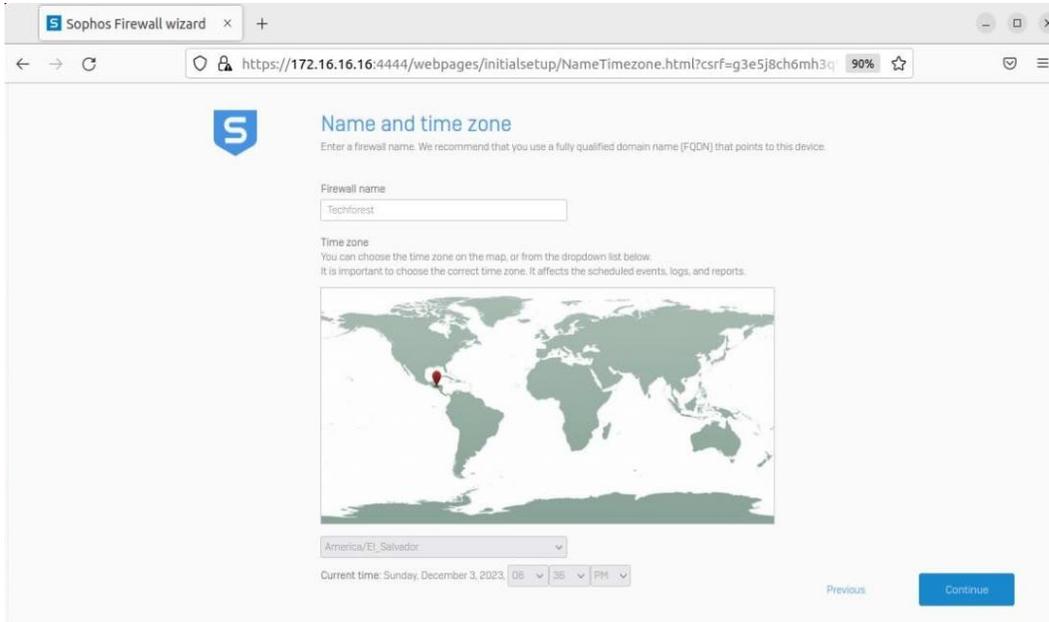


Aceptamos los términos de uso y presionamos Start Setup.

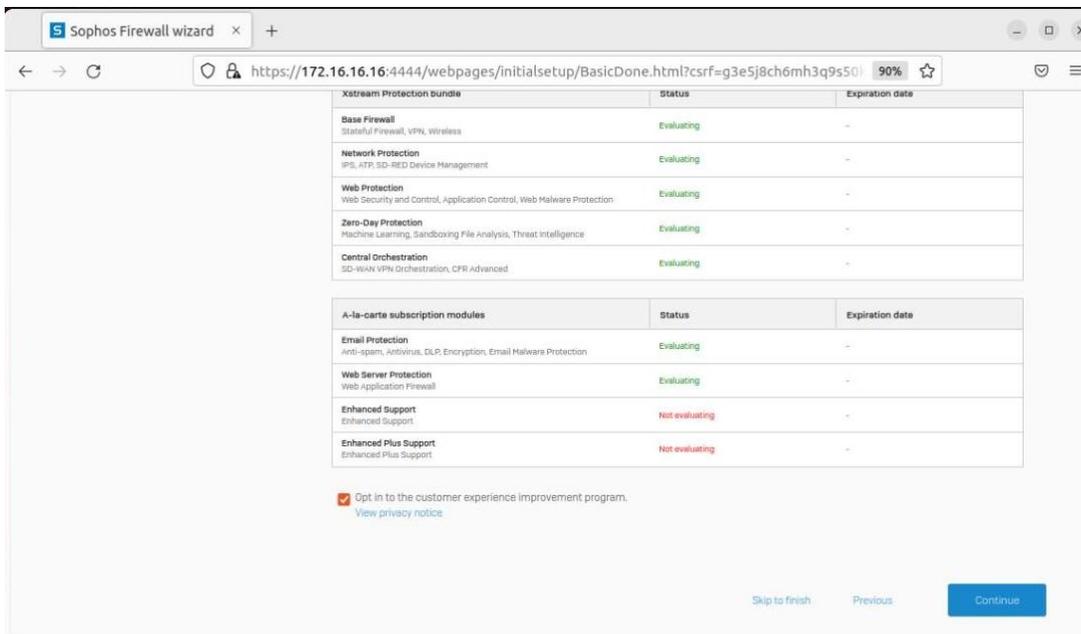
The screenshot shows the 'Basic configuration' page of the Sophos Firewall wizard. The browser address bar shows the URL: `https://172.16.16.16:4444/webpages/initialsetup/BasicConfig.html?csrf=g3e5j8ch6mh3q`. The page features the Sophos logo and a heading 'Basic configuration'. Below the heading, there is a paragraph of instructions: 'You can log in to the firewall only through the administrator account currently. You must create a password before you continue. We recommend that you use a long password, with a mix of letters, numbers and special characters to make it strong. If you have an existing configuration that you wish to use, or an existing firewall that you wish to connect to in HA, choose the relevant options below.' To the right of this text are links for 'Restore backup' and 'Connect as HA spare'. The main section is titled 'Create new admin account' and contains two input fields: 'Default administrator's new password:' and 'Reenter the password:'. Below these fields is a checked checkbox with the text 'Install the latest firmware automatically during setup (recommended)'. At the bottom right, there are 'Previous' and 'Continue' buttons.

Completamos los campos que pide.

The screenshot shows the 'Name and time zone' page of the Sophos Firewall wizard. The browser address bar shows the URL: `https://172.16.16.16:4444/webpages/initialsetup/NameTimezone.html?csrf=g3e5j8ch6mh3q`. The page features the Sophos logo and a heading 'Name and time zone'. Below the heading, there is a paragraph of instructions: 'Enter a firewall name. We recommend that you use a fully qualified domain name (FQDN) that points to this device.' Below this text is an input field for 'Firewall name'. The next section is titled 'Time zone' and contains a paragraph of instructions: '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.' Below this text is a world map with a red pin in Europe. At the bottom, there is a dropdown menu showing 'Europe/London'.



Podremos ver que la instalación básica está completa, continuamos.



Nos muestra la red LAN con los datos que configuramos y le damos continuar.

The screenshot shows the 'Network configuration [LAN]' step of the Sophos Firewall wizard. The page title is 'Network configuration [LAN]' and it includes a sub-header: 'Select the ports, the deployment mode, and how to assign IP addresses. Currently, you're connected to "PortA".' The configuration options are as follows:

- Port:** A dropdown menu set to 'PortA' with the note 'You can change the selected port.'
- Choose gateway:** A dropdown menu set to 'This firewall (route mode)'. Below it, there are three modes: 'Gateway mode: The firewall acts as a router.', 'Bridge mode: The firewall acts as a bridge between your network and your internet gateway.', and 'The firewall secures your network in both modes.'
- LAN IP address:** A text input field containing '172.16.16.16'.
- Subnet mask:** A dropdown menu set to '/24 (up to 254 client devices)'.
- Enable DHCP:** A checked checkbox with the text 'Let the firewall assign IP addresses to your internal devices.'
- DHCP lease range:** Two text input fields containing '172.16.16.17' and '172.16.16.254'.

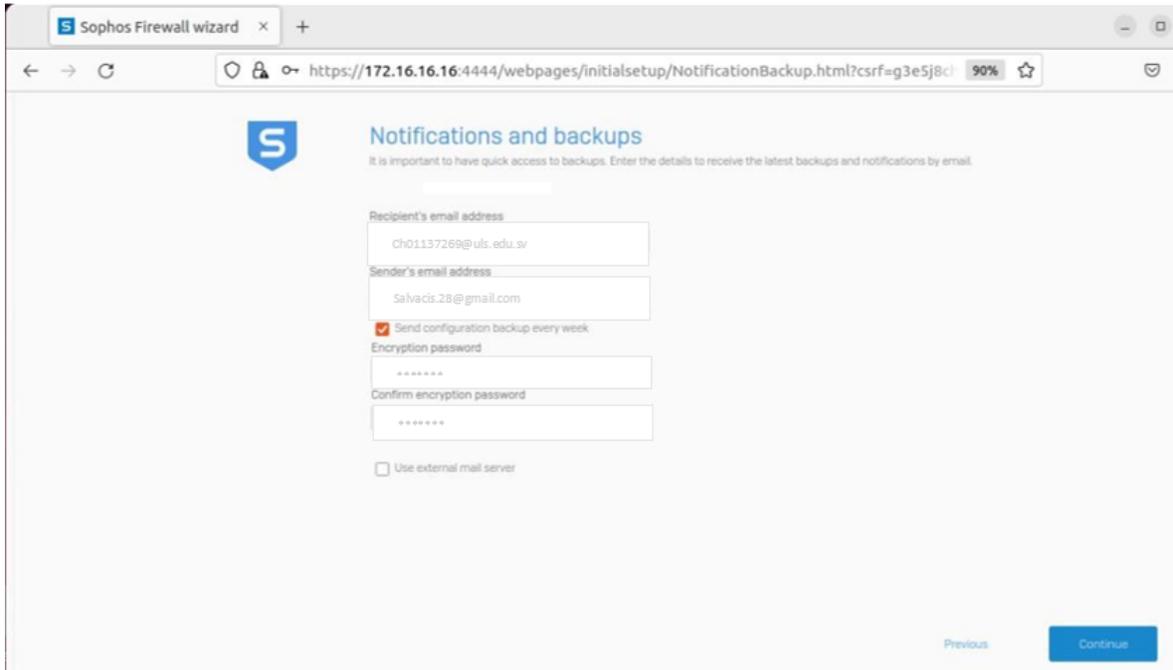
At the bottom, there is a link 'Enable TAP/discover mode', a 'Previous' button, and a 'Continue' button.

The screenshot shows the 'Network protection' step of the Sophos Firewall wizard. The page title is 'Network protection' and it includes a sub-header: 'You can configure permissions for users on wired and wireless networks to protect them when they access the internet.' The configuration options are as follows:

- Protect users from network threats:** An unchecked checkbox. Description: '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:** An unchecked checkbox. Description: '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:** An unchecked checkbox. Description: '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:** An unchecked checkbox. Description: '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 bottom, there is a 'Previous' button and a 'Continue' button.

Ingresamos los datos que solicita y continuar.

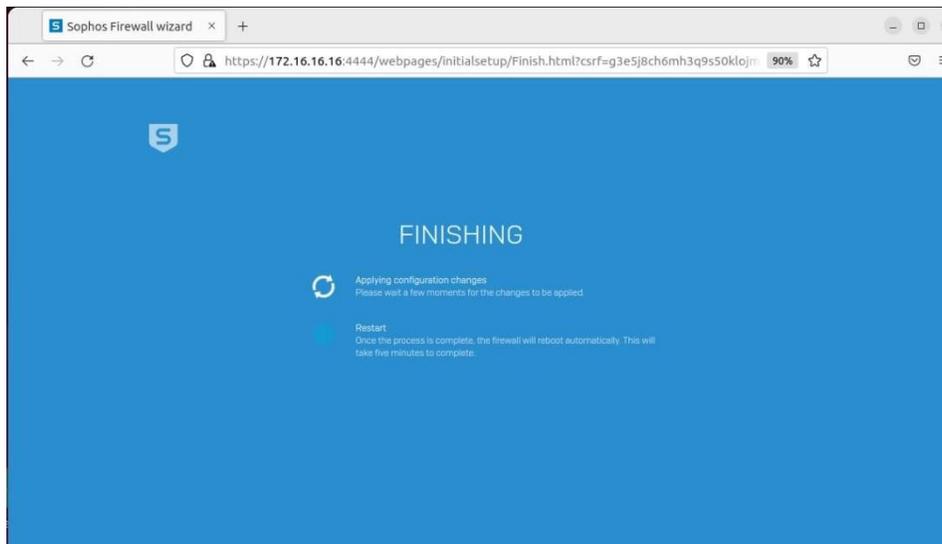


The screenshot shows a web browser window titled "Sophos Firewall wizard". The address bar displays the URL: `https://172.16.16.16:4444/webpages/initialsetup/NotificationBackup.html?csrf=g3e5j8c...`. The page content includes the Sophos logo and the heading "Notifications and backups". Below the heading, there is a form with the following fields and options:

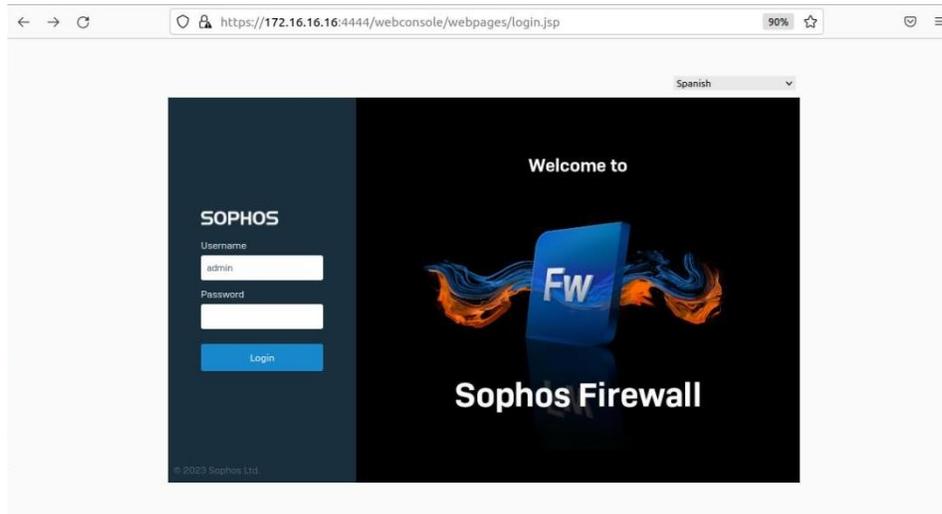
- Recipient's email address: `Ch01137269@uls.edu.sv`
- Sender's email address: `Salvacis.28@gmail.com`
- Send configuration backup every week
- Encryption password: `*****`
- Confirm encryption password: `*****`
- Use external mail server

At the bottom right of the form, there are two buttons: "Previous" and "Continue".

Tendremos nuestro firewall finalizado.



Ingresamos los datos que registramos.



Podremos hacer uso de nuestro firewall, con esto habremos concluido con la instalación y configuración de SOPHOS XG.

