

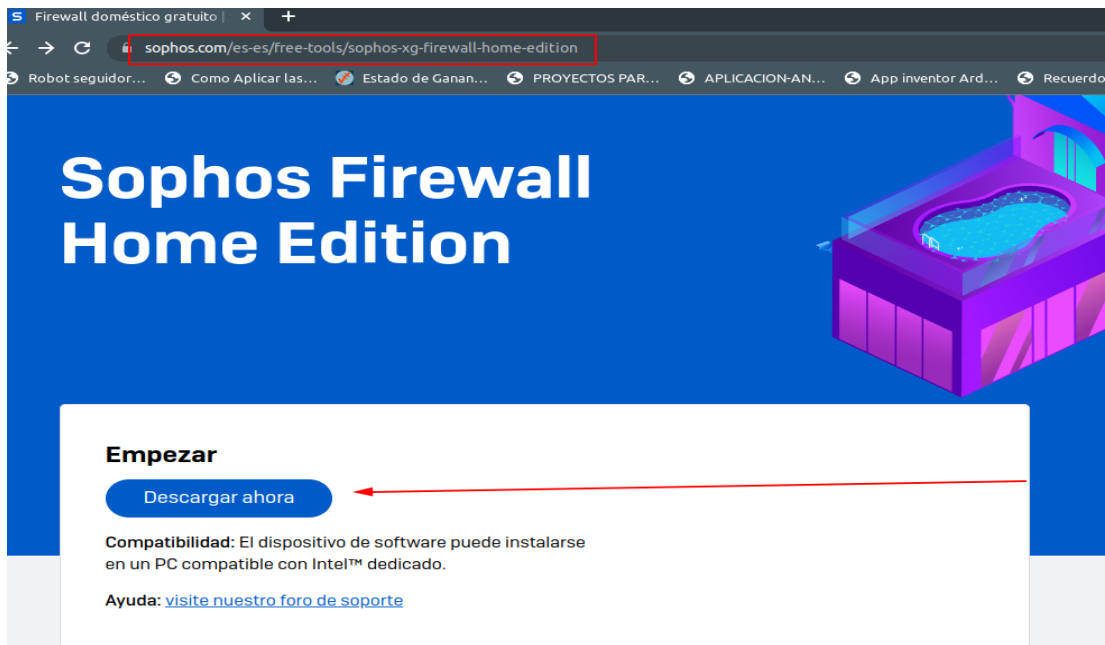
Instalación de Sophos XG Firewall



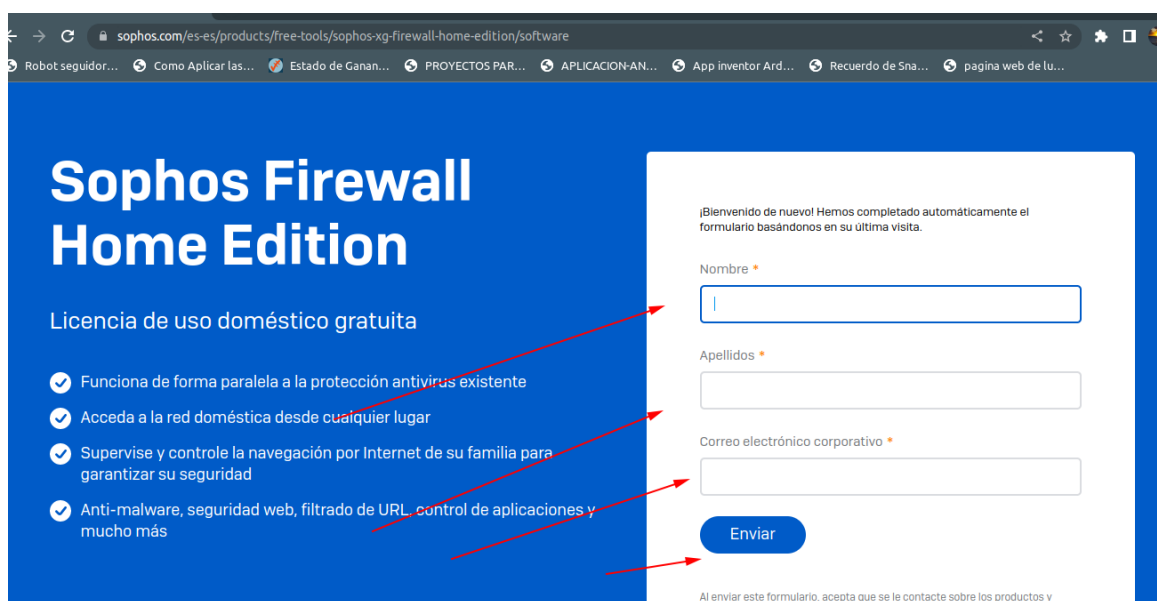
REDES II

Instalación de Sophos XG Firewall Home Edición

Primeramente, se ingresa a la página oficial de Sophos Firewall, en el siguiente link para poder descargar la y proceder a instalarla, presionamos el botón para descargar.

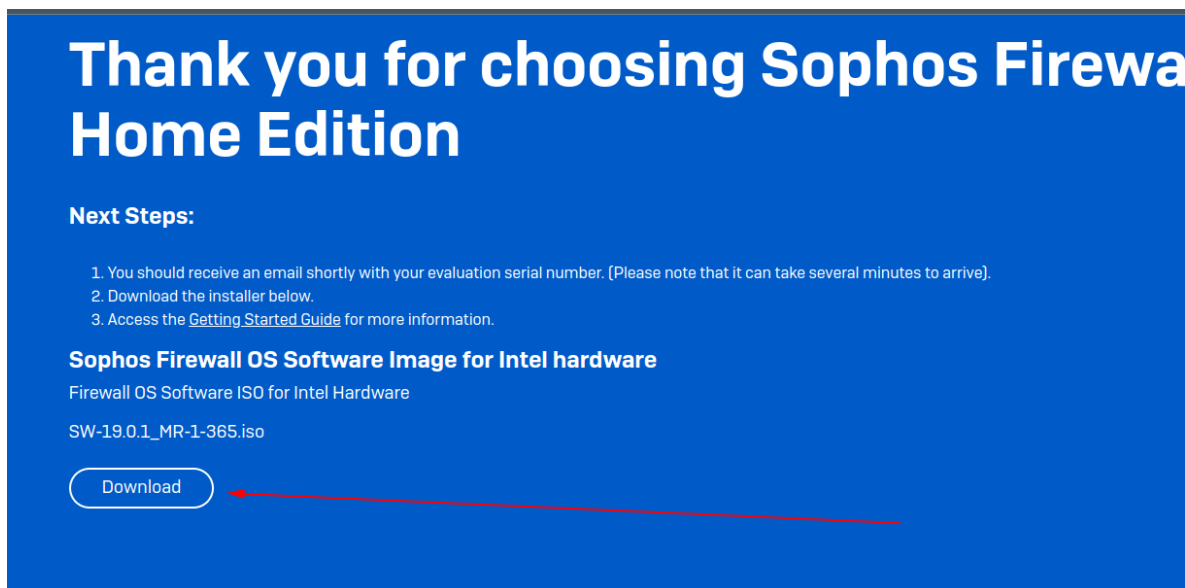


Luego pide que se registre para poder obtener la licencia de software para la implementación. Tenemos que registrarnos.



Después de registrarse se redirige a otra página donde si ya nos aparece el archivo a descargar, se procede a descargar la iso para la instalación, pesa 700mb.

Además, cae un correo en donde viene el código de la licencia a utilizar más adelante en la implementación del software.



Thank you for choosing Sophos Firewall Home Edition

Next Steps:

1. You should receive an email shortly with your evaluation serial number. (Please note that it can take several minutes to arrive).
2. Download the installer below.
3. Access the [Getting Started Guide](#) for more information.

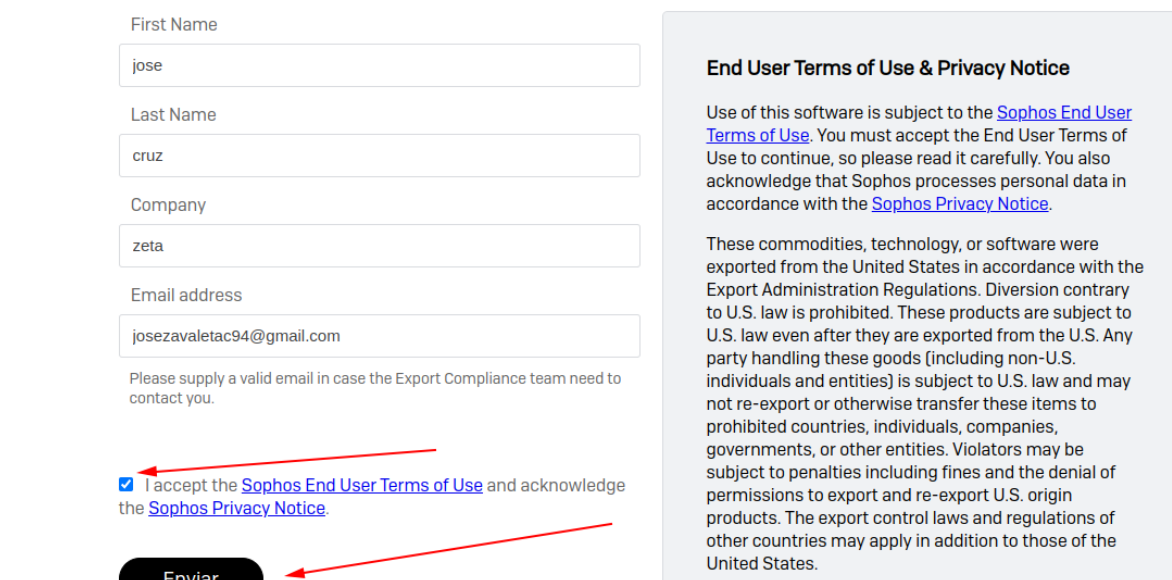
Sophos Firewall OS Software Image for Intel hardware

Firewall OS Software ISO for Intel Hardware

SW-19.0.1_MR-1-365.iso

[Download](#)

Por ser un software de los Estados Unidos se necesita un registro más, es que se tiene que llenar el siguiente formulario con la información requerida para descargar Sophos XG.



First Name

jose

Last Name

cruz

Company

zeta

Email address

josezavaletac94@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](#).

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](#).

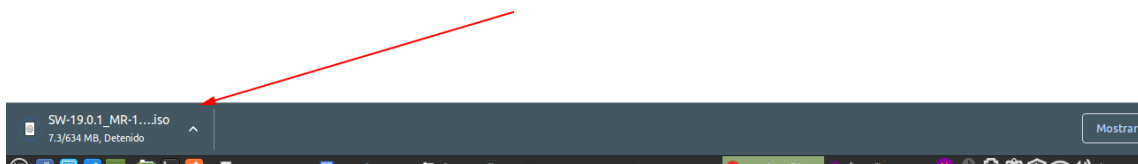
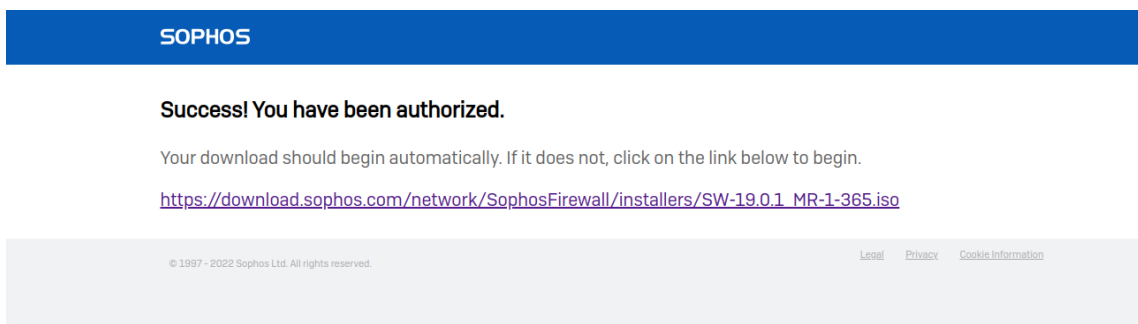
These commodities, technology, or software were exported from the United States in accordance with the Export Administration Regulations. Diversion contrary to U.S. law is prohibited. These products are subject to U.S. law even after they are exported from the U.S. Any party handling these goods (including 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.

Enviar

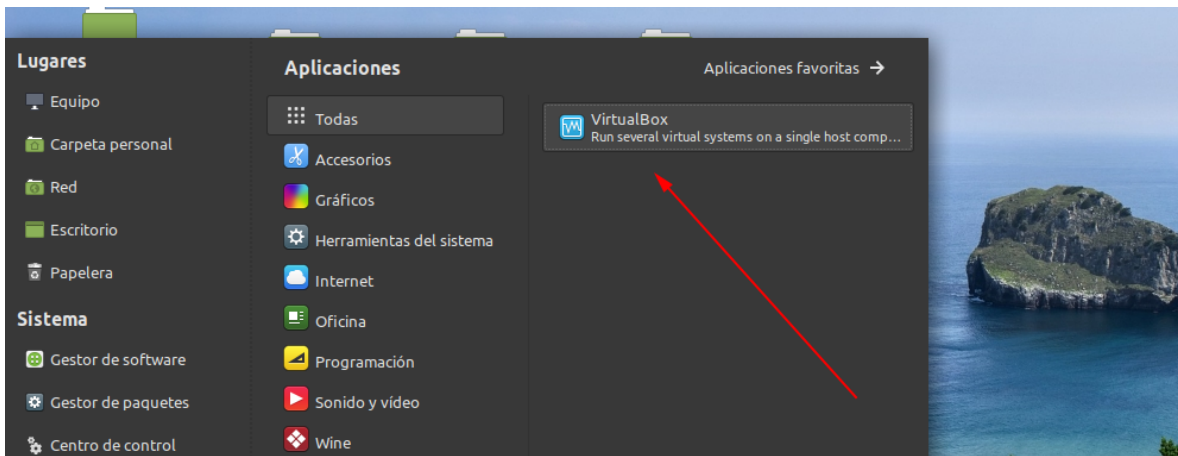
Revisar el correo para ver que ya nos han enviado el código de la licencia para activar el software Sophos XG.



Después de registrarnos del formulario nos redirige a la siguiente página donde automáticamente se descarga la iso del software. Observamos que ya se está descargando.



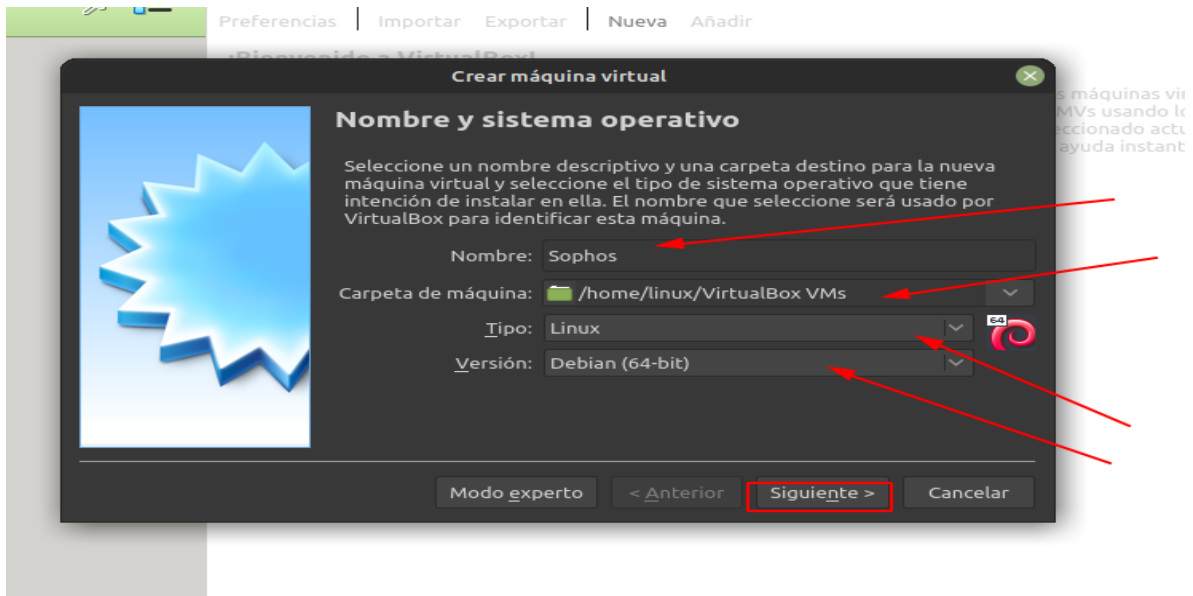
Mientras se descarga la iso de Software de Sophos se procede a utilizar un hipervisor para la instalación del software en este caso utilizaremos VirtualBox. Procedemos a crear una máquina virtual para la demostración.



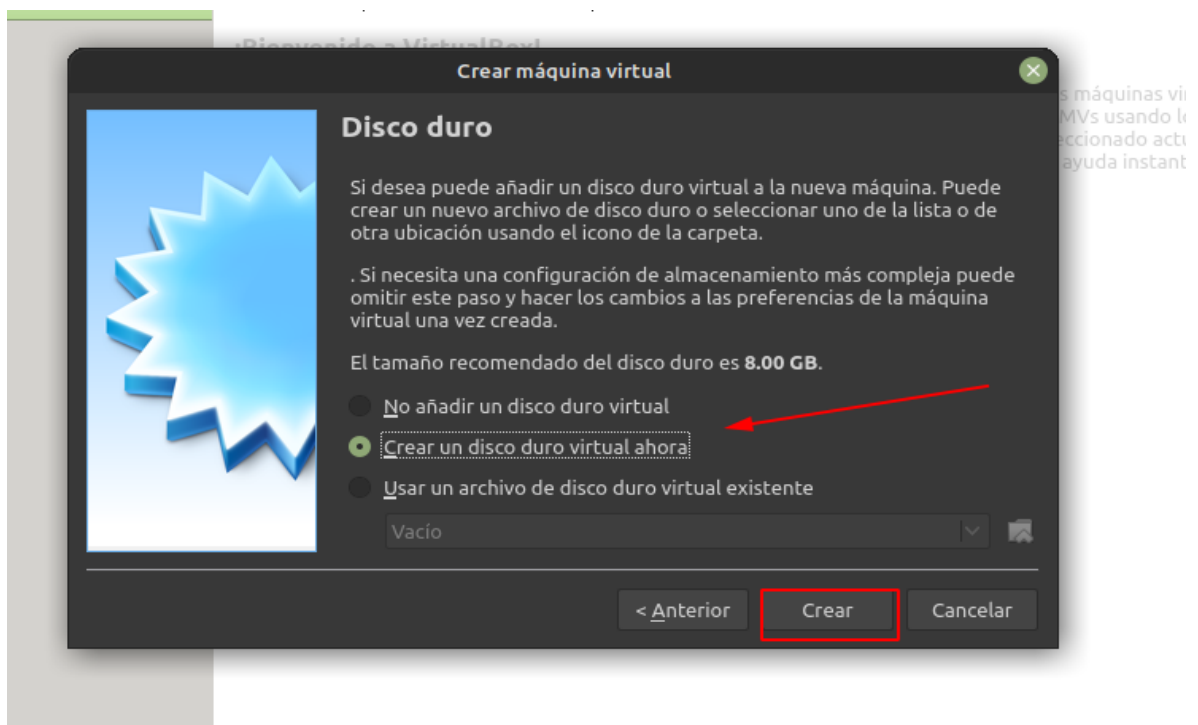
Se procede a crear una máquina virtual en la opción nuevo.



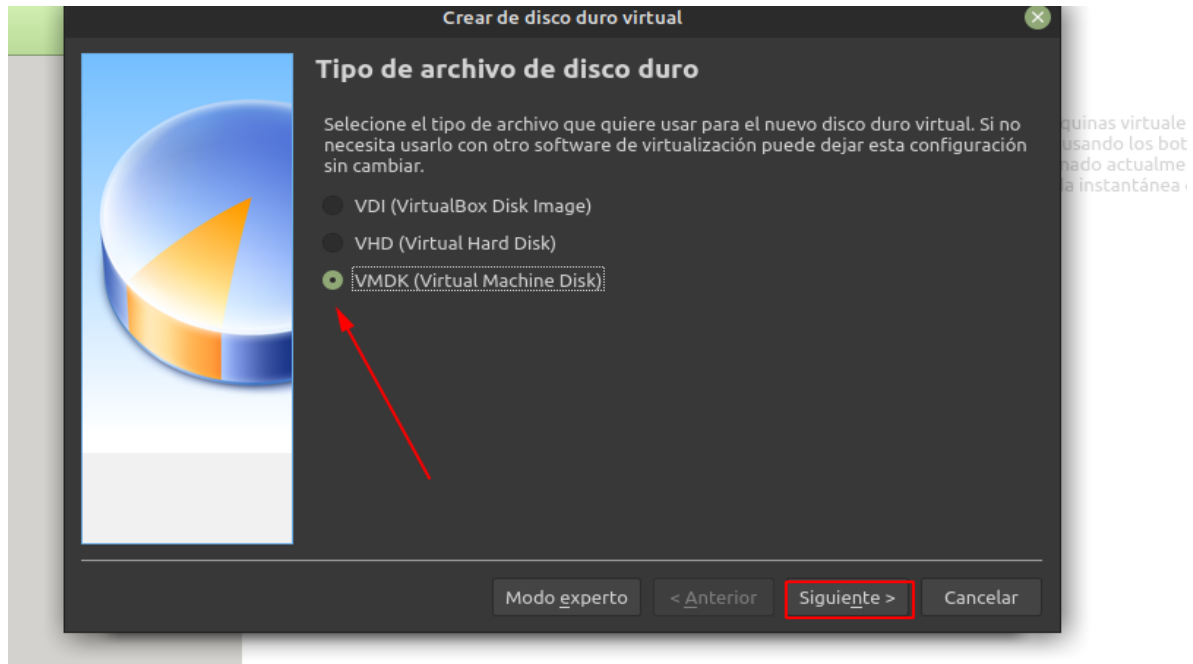
Realizar las configuraciones para la instalación colocamos el nombre, seleccionamos el sistema operativo y seleccionamos debían de 64bit o según tu sistema operativo. Dar clic en siguiente.



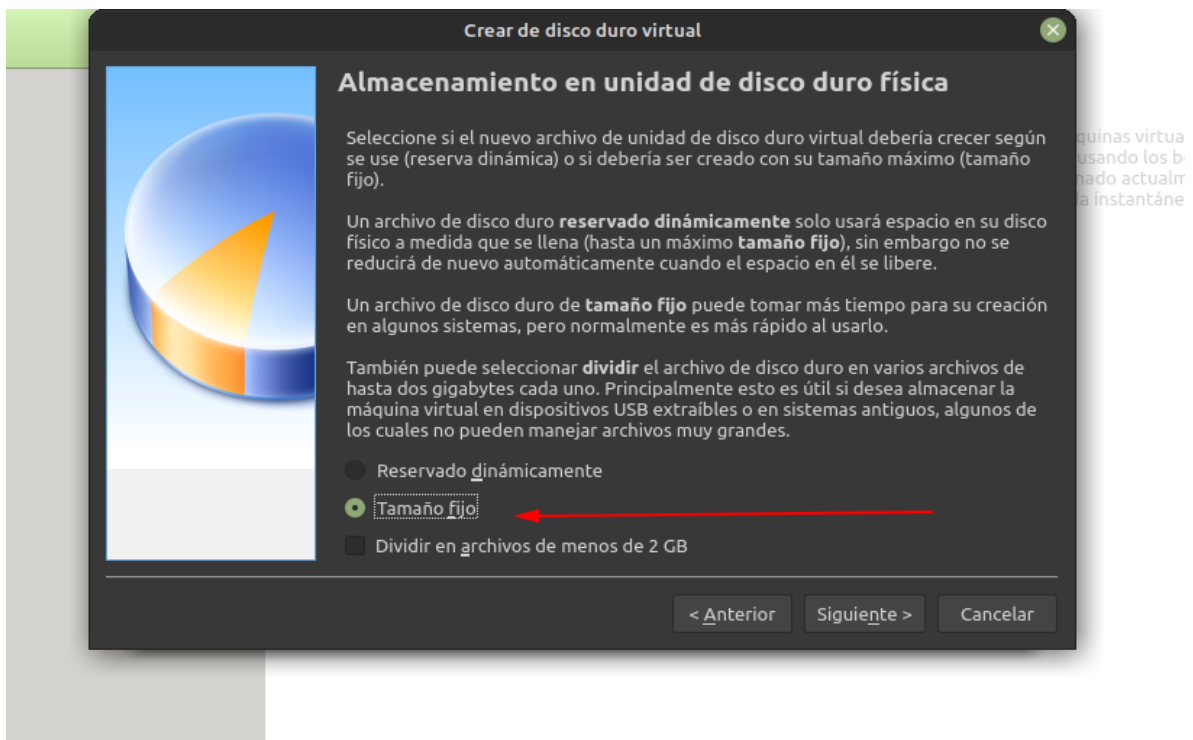
Seleccionar en crear un disco virtual duro ahora, y dar clic en crear.



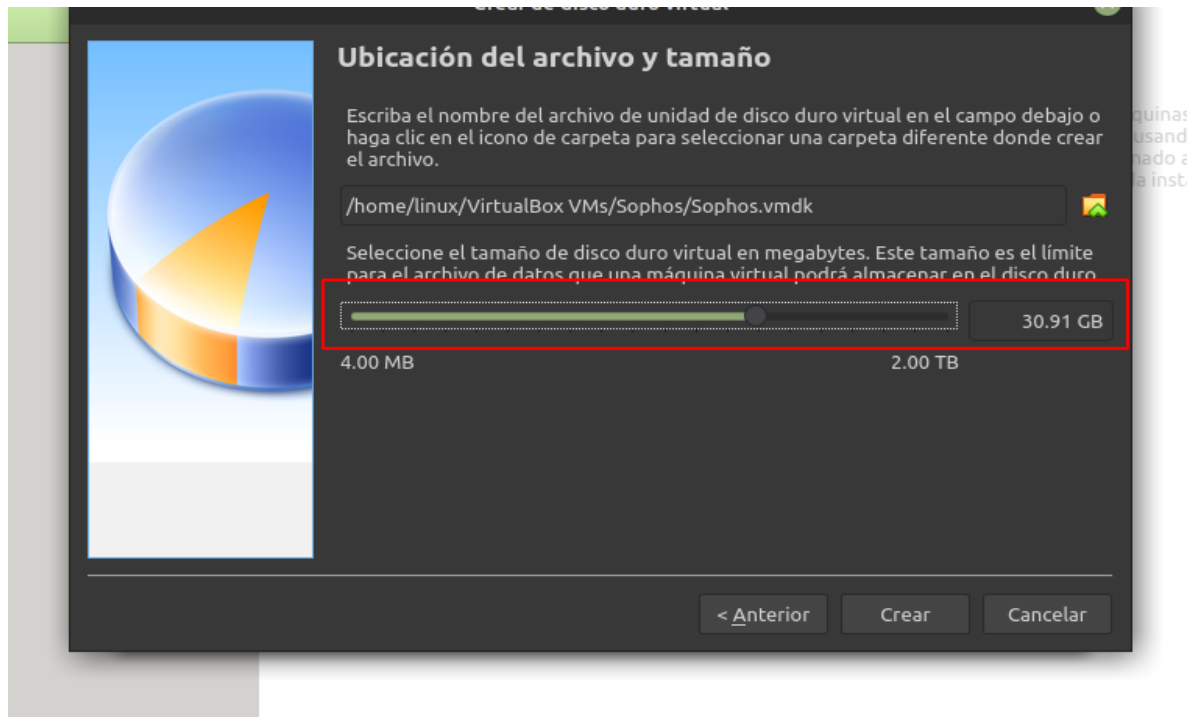
Elegir la opción de VMDK y dar clic en siguiente.



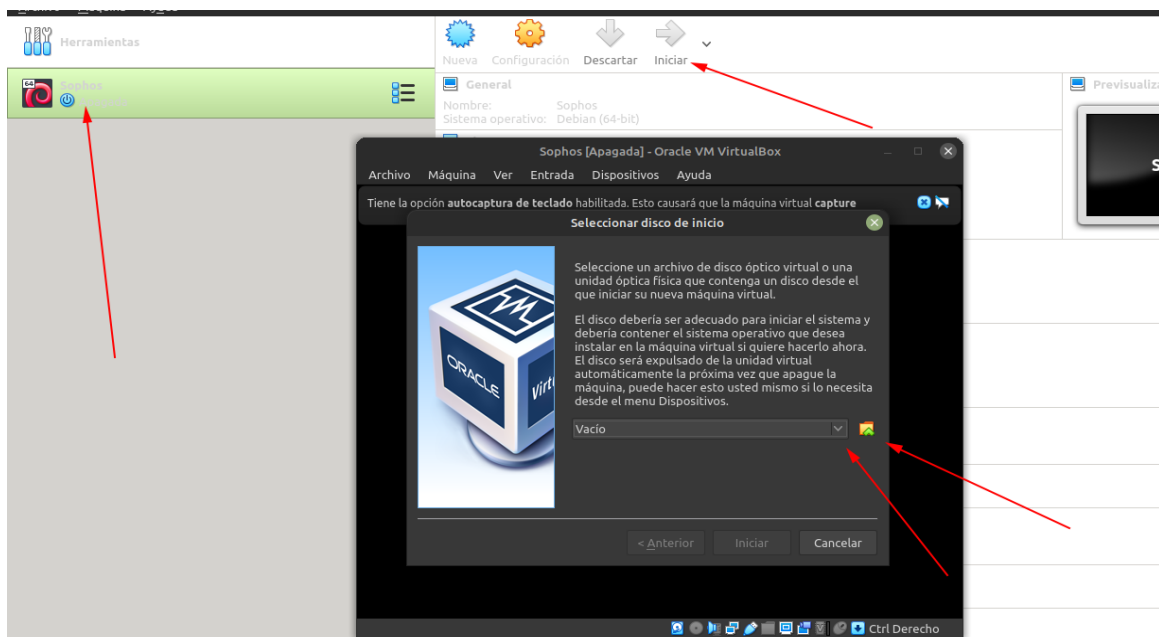
Elegimos la opción de tamaño fijo, damos clic en siguiente.



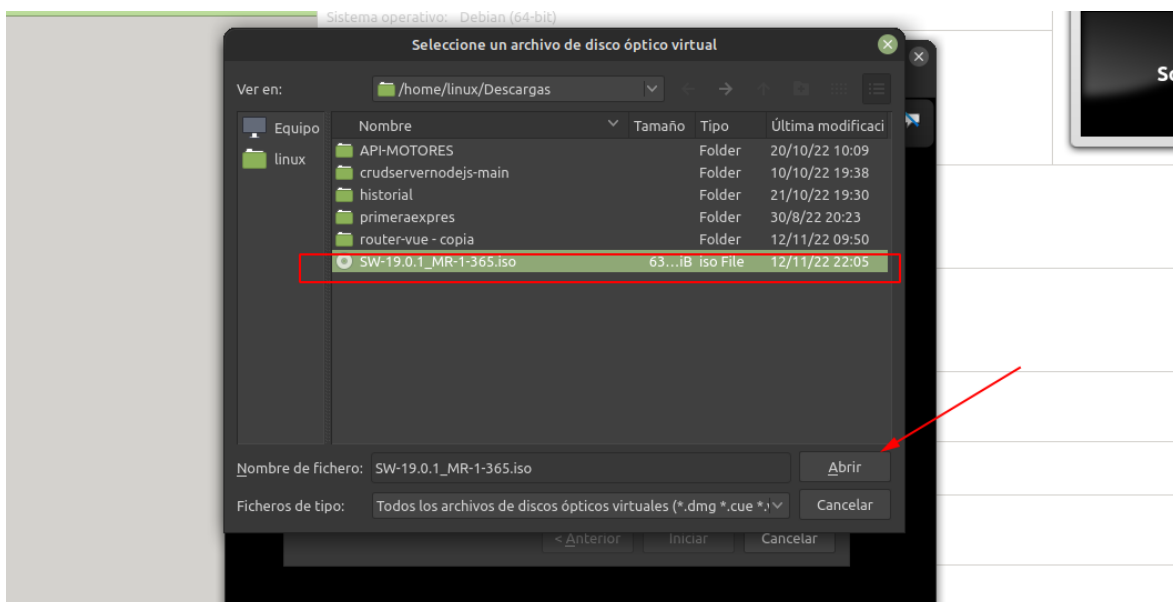
Elegir el tamaño del Disco virtual a crear, en este caso será de 30gb, dar clic en crear.



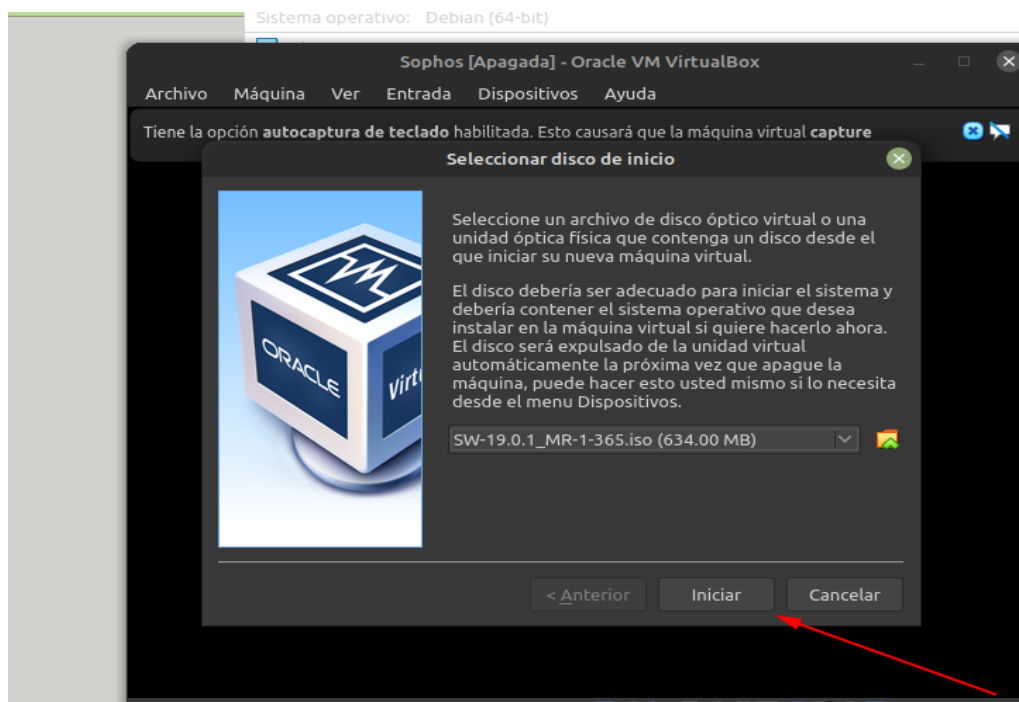
Se crea la máquina virtual esto puede demorar de acuerdo a tu procesador, una vez creada dar en iniciar la máquina virtual, aparece que no hay iso para la instalación dar clic en el folder para ir a buscarla.



Navegamos a donde esta la iso y le damos en abrir.



Ya seleccionada se procede a dar clic en iniciar para la instalación del software Sophos XG.



Aparece el siguiente mensaje en la cli escribir la letra “y” para proceder.

```
Sophos FIRMWARE INSTALLER

Created on: #Fri Aug  5 06:48:26 CEST 2022
Firmware version: #19.0.1.365
Contains Firmware for: SF01V_S001
Detected Platform: Oracle(VirtualBox) Virtual Platform

=====

=====
Using Disk /dev/sda : 30GB as Primary Disk
=====
Detected Appliance Model: SF01V_S001
This program will erase all data from the appliance
Do you want to continue (y/n)
```

Se observa que se está instalando el software Sophos XG.

```
=====
Completed: [ =====
===== 80%]
=====
Formatting Configuration Partition [OK]
Formatting Signature Partition [OK]
Creating Swap Space [OK]
Formatting Report Partition [OK]
Installing Loader for appliance SF01V_S001 [OK]
Installing firmware for appliance SF01V_S001 ...
```

La Instalación se ha completado y nos dice que iniciemos el equipo en esta ocasión en la máquina virtual. Escribir la letra “y” para reiniciar.

```
#####
#####
Completed: [ =====
===== 100%]
#####
#####
Formatting Configuration Partition [OK]
Formatting Signature Partition [OK]
Creating Swap Space [OK]
Formatting Report Partition [OK]
Installing Loader for appliance SF01V_S001 [OK]
Installing firmware for appliance SF01V_S001 [OK]
Firmware Installed
Remove Installer disk
press y to reboot
_
```

Al iniciar la máquina nos aparece el GRUB y se inicia automáticamente.

```
GNU GRUB version 2.02

SFLoader
*19_0_1_365

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the commands
before booting or 'c' for a command-line.
The highlighted entry will be executed automatically in 1s.
```

Nos pide la contraseña en este caso es admin. Se procede a colocarla
Recordar activar dos interfaces en la configuración de la máquina virtual.

```
Booting '19_0_1_365'

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 Disk Size:          30 GB

#####

Password: _
```

Después de loguearse nos aparece un menú de opciones. Escribir 1 para ver las configuraciones de red.

```
Sophos Firmware Version SFOS 19.0.1 MR-1-Build365

Main Menu

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

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

Aparece otro submenú también escribir 1

```
Sophos Firmware Version SFOS 19.0.1 MR-1-Build365
```

```
Network configuration Menu
```

- 1. Interface Configuration
- 2. DNS Configuration
- 0. Exit

```
Select Menu Number [0-2]: 1
```

Se puede ver la configuración de las redes por defecto Sophos configura en la red 0 la ip 172.16.16.16/255.255.255.0. presionar enter para continuar.

```
Sophos Firmware Version SFOS 19.0.1 MR-1-Build365
```

```
Network Settings
```

```
Interface Name      : Port1 (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 .....
```

y nos pregunta si queremos cambiar la ip configurada por Sophos. En esta ocasión escribimos la letra “y” para cambiar puesto que el hipervisor maneja otra ip la que toma de la máquina principal.

```
Sophos Firmware Version SFOS 19.0.1 MR-1-Build365
```

```
Set IPv4 Address (y/n) : No (Enter) > _
```

Procedemos a cambiar la ip que nos está proporcionando el proveedor de internet y agregamos la máscara de red también.

```
Sophos Firmware Version SFOS 19.0.1 MR-1-Build365

Network configuration Menu

Network Configuration of Ethernet Port1

Current IP address : 192.168.56.100
New IP address     : 192.168.56.200
Current Netmask    : 255.255.255.0
New Netmask        : 255.255.255.0_
```

Dar enter los cambios se están realizando.

```
Changing IP Address of the Device ..... Done.
_
```

Verificamos si los cambios se han realizado, efectivamente la ip se ha cambiado.

```
Sophos Firmware Version SFOS 19.0.1 MR-1-Build365

Network Settings
Interface Name      : Port1 (Physical)
Zone Name           : LAN

IPv4/Netmask        : 192.168.56.200/255.255.255.0 (Static)
IPv4 Gateway        : N.A.

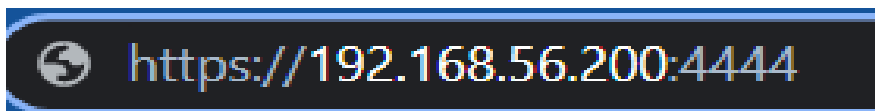
IPv6/Prefix         : Not Configured
IPv6 Gateway        : N.A.

Configured Aliases

No Alias Configured

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

Abrir un navegador escribir <https://192.168.56.200:4444>

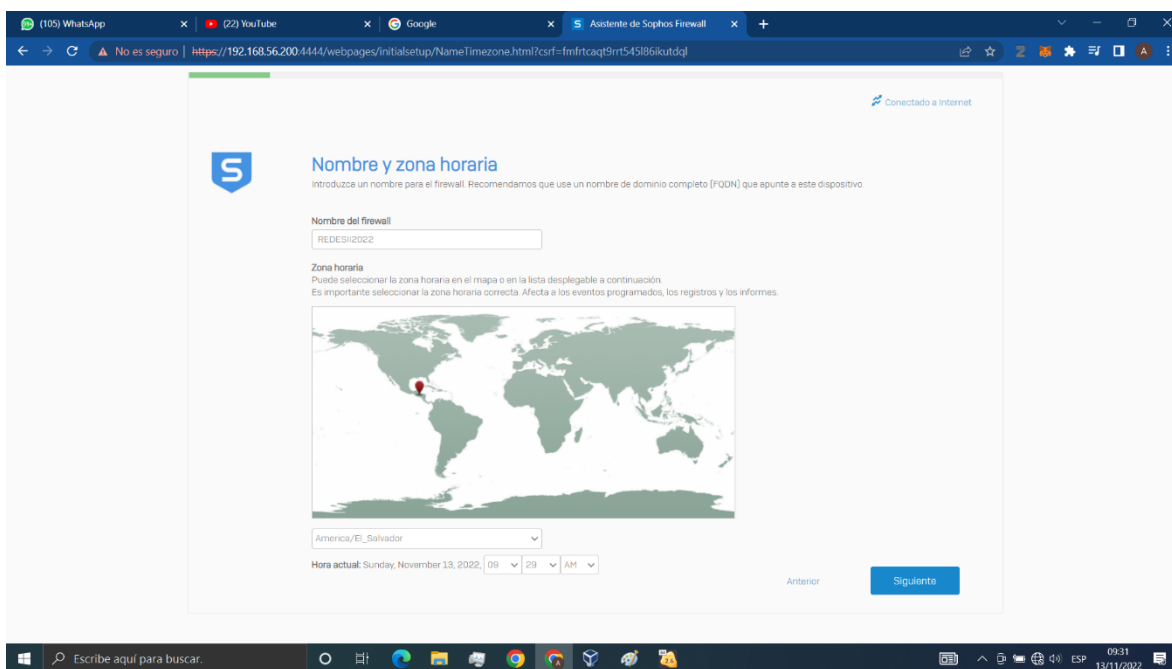


Aparecerá la interfaz gráfica del Sophos y aceptamos los términos y condiciones. Presionar en star setup

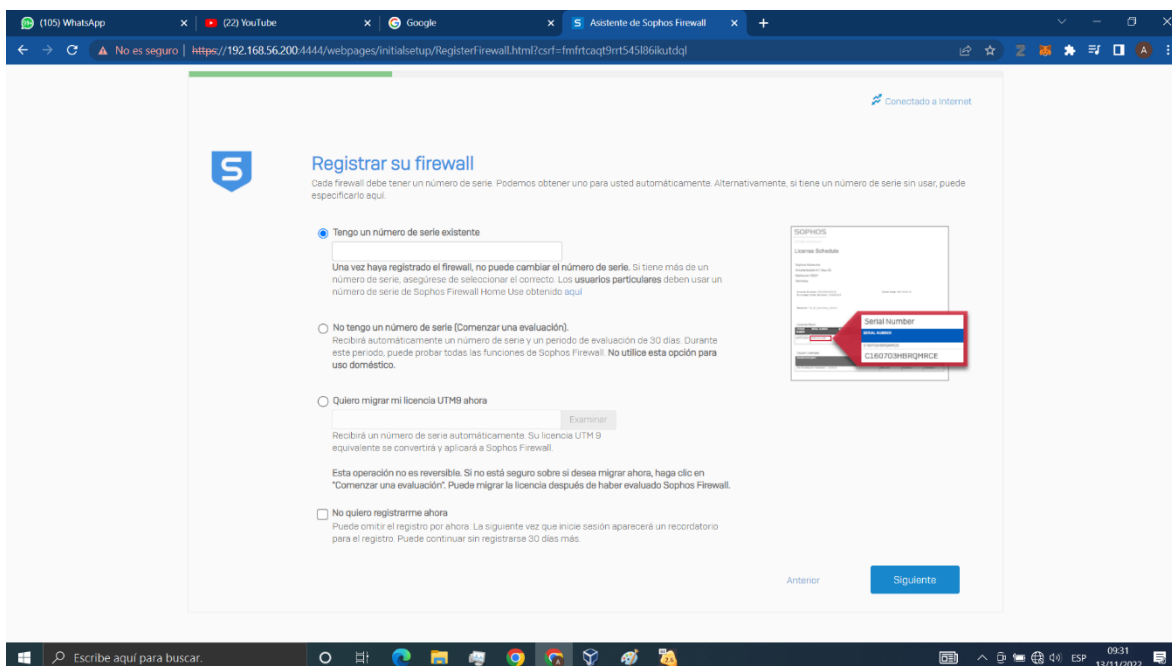
A screenshot of a web browser displaying the Sophos firewall configuration interface. The browser's address bar shows a long URL starting with 'https://192.168.56.200:4444/webpages/initialsetup/index.html'. The page has a dark blue header with the Sophos 'S' logo. The main content area is white and titled 'Configuración básica'. It contains instructions in Spanish about creating an administrator account. There are two input fields for a password, one labeled 'Nueva contraseña del administrador predeterminado:' and another labeled 'Repetir la contraseña:'. Below these is a checkbox labeled 'Instalar el firmware más reciente automáticamente durante la configuración (recomendado)'. At the bottom right, there are two buttons: 'Anterior' and 'Siguiente'.

Pide crear contraseña y usuario para ingresar al dashboard. Y proceder a la instalación de paquetes adicionales, dar clic en siguiente.

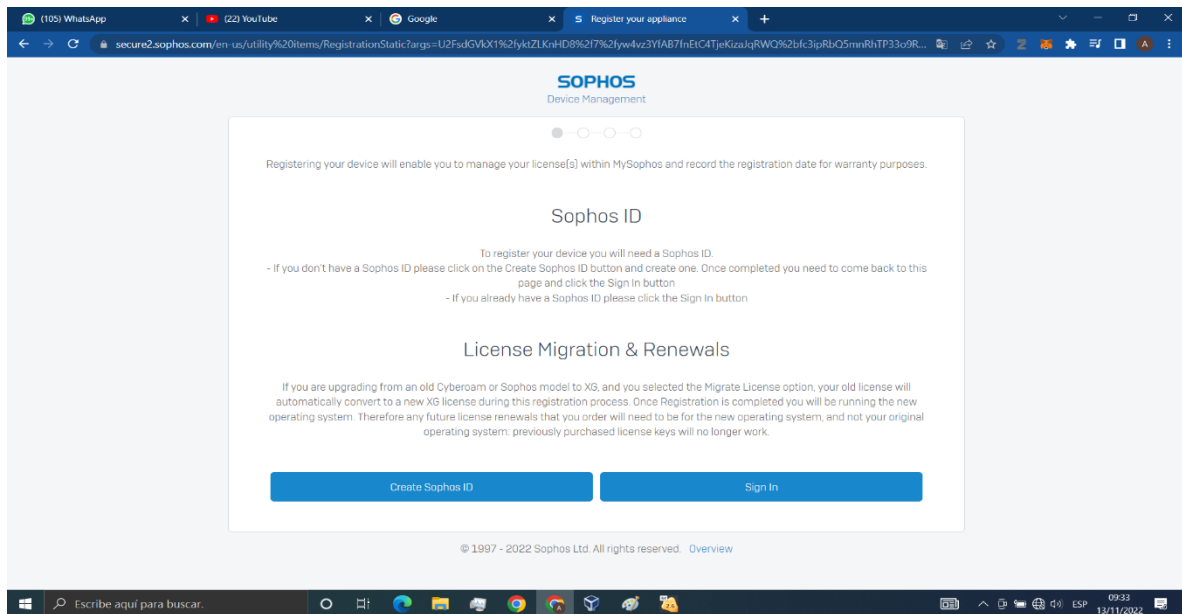
En esta ventana nos pide que se configure la información del nombre, firewall zona horaria, ubicación y fecha.



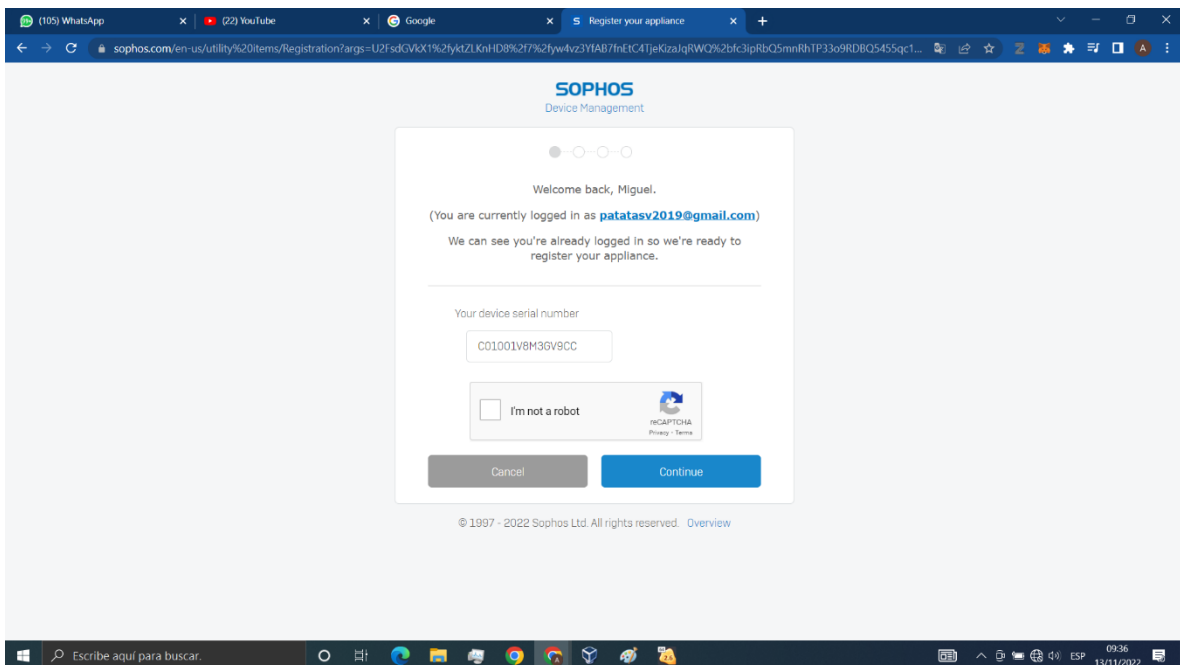
En esta ventana pide que introducimos el código de la licencia, este se manda cuando se registra por primera vez al descargar el software al correo que se introdujo en el formulario. Al colocar el código dar clic en siguiente.



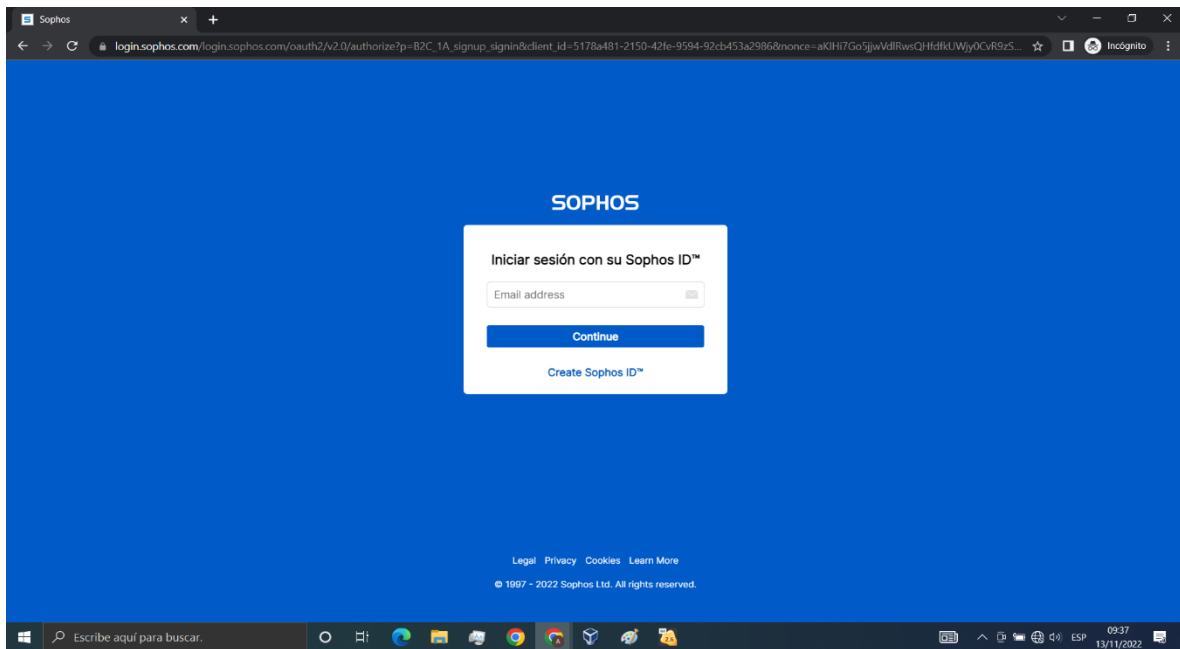
Nos pide un id tenemos que crear uno le damos en crear id dar clic en el botón crear id.



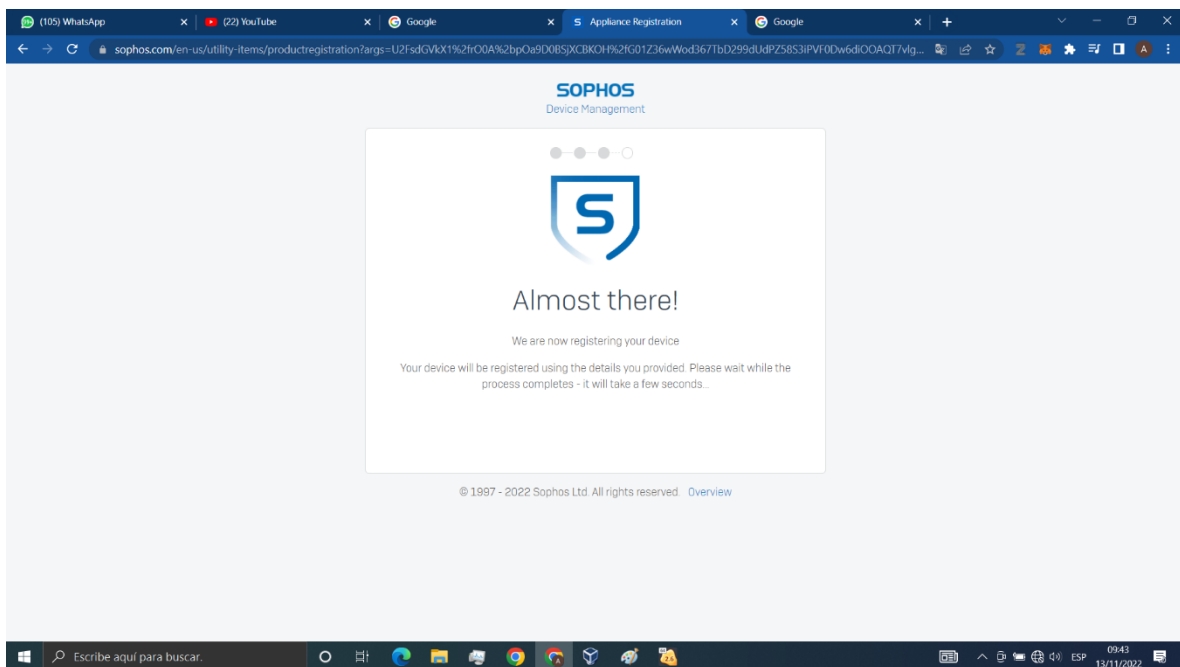
Nos aparece la siguiente ventana en donde nos pide que resolvamos el captcha y dar clic en el botón continuar.



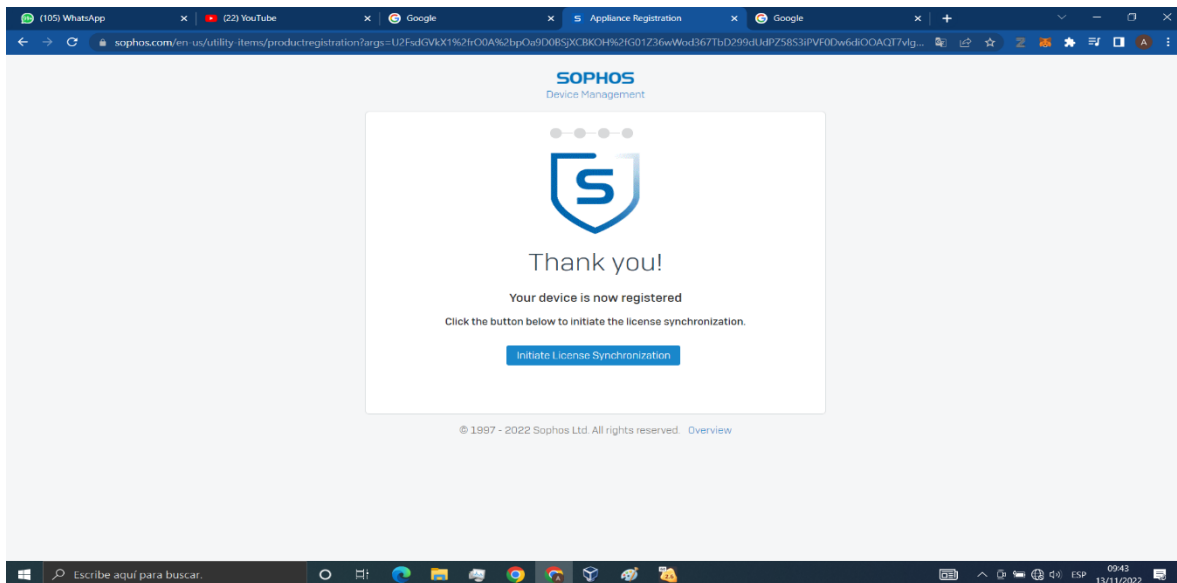
Aparece la siguiente ventana, dar clic en continuar.



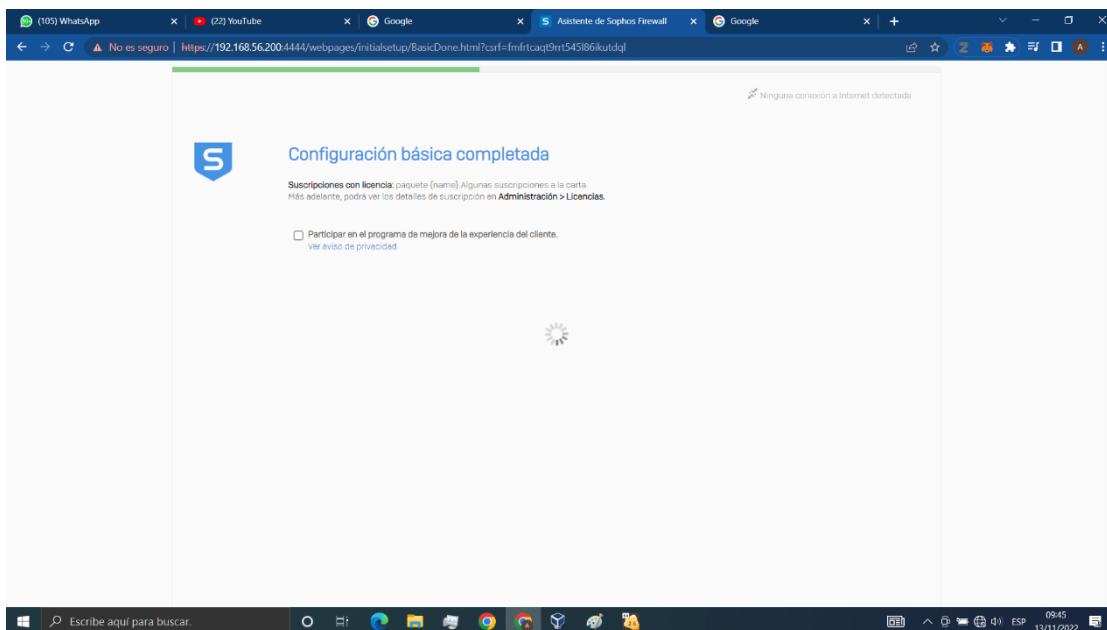
Aparecen ventanas de información del Sophos.



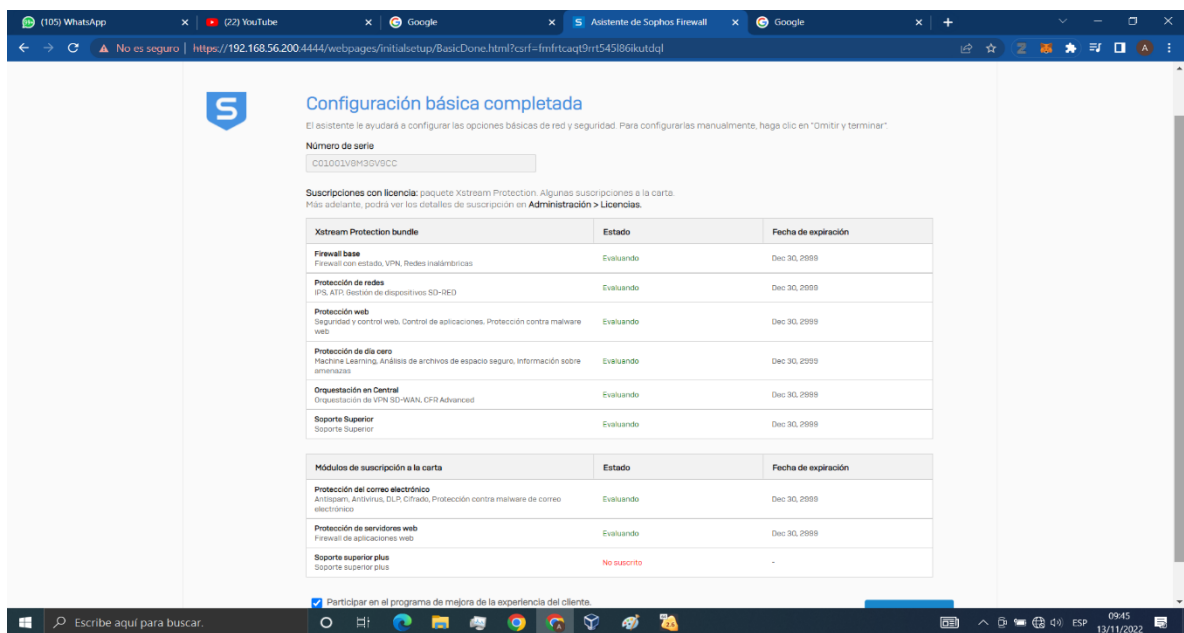
Le damos clic en iniciar sincronización de licencia.



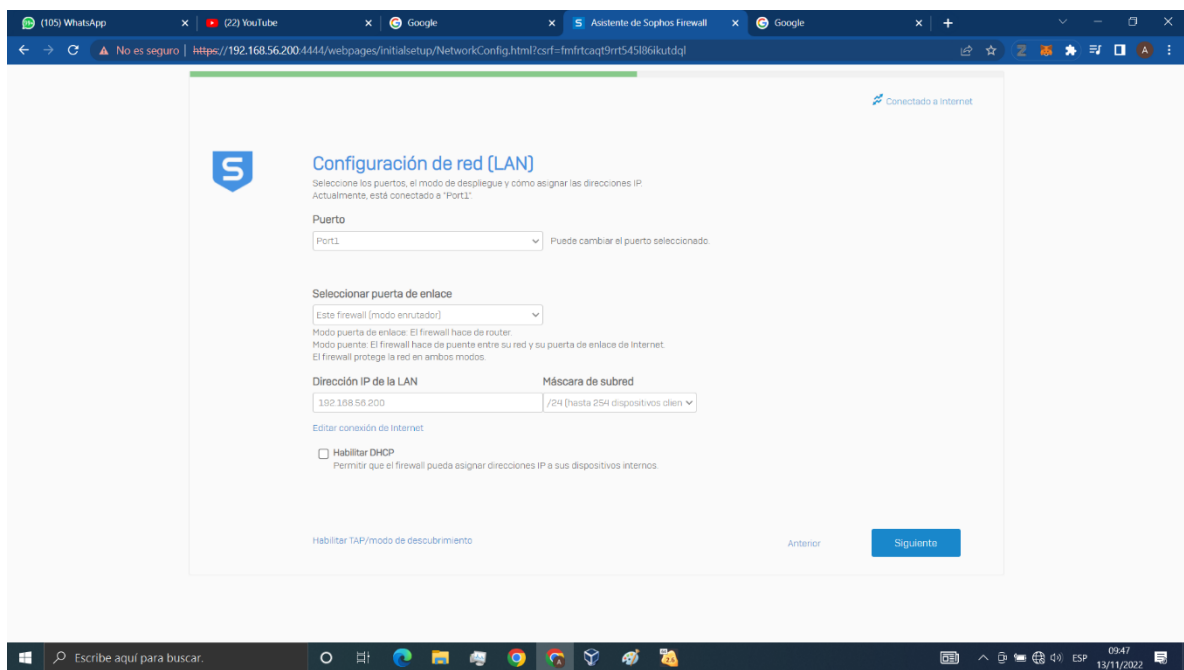
Aparece la siguiente información la configuración básica completada.



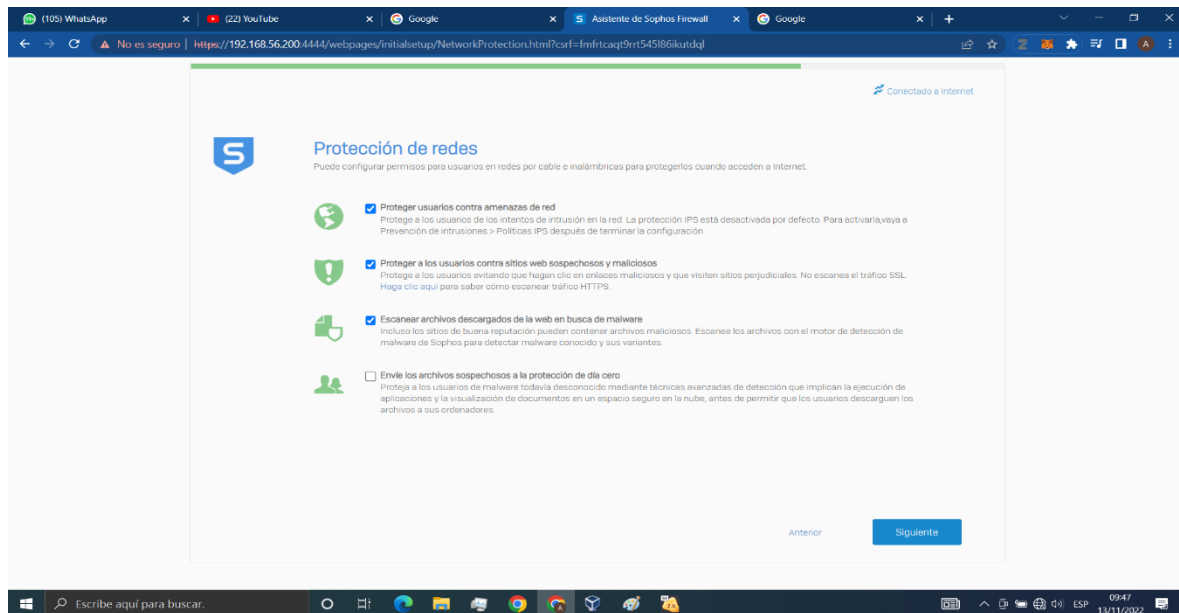
Siguiente imagen de configuraciones básicas, dar clic en siguiente.



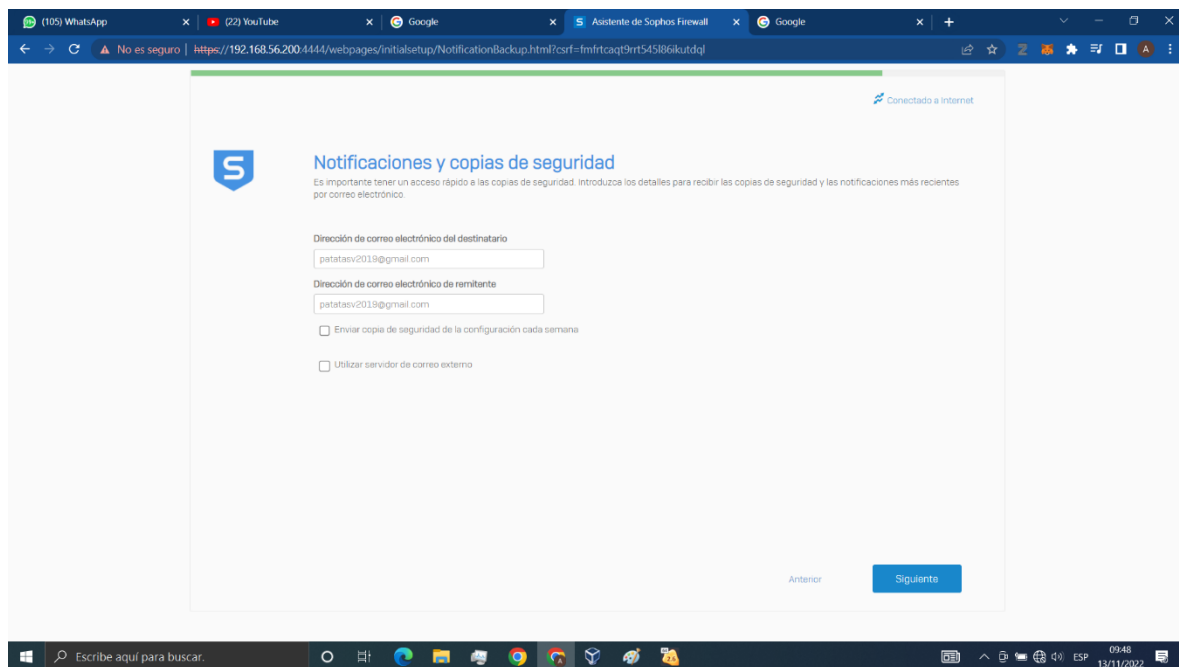
Configuraciones de la red realizadas, dar clic en siguiente.



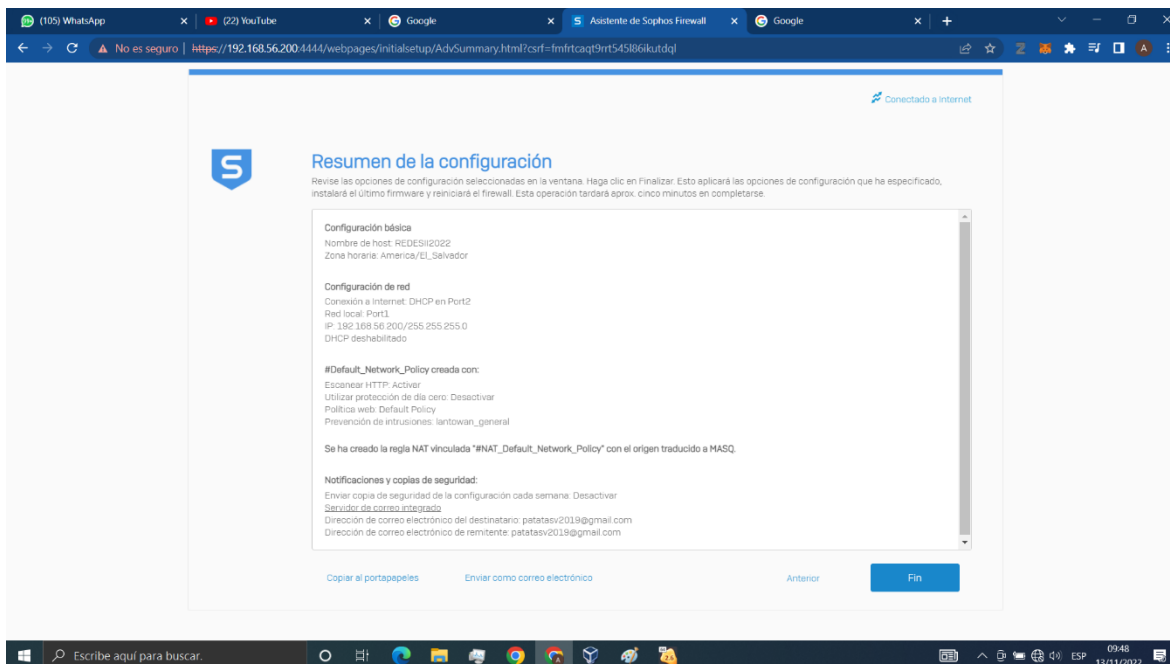
Siguiente imagen seleccionar las primeras tres opciones, dar clic en siguiente.



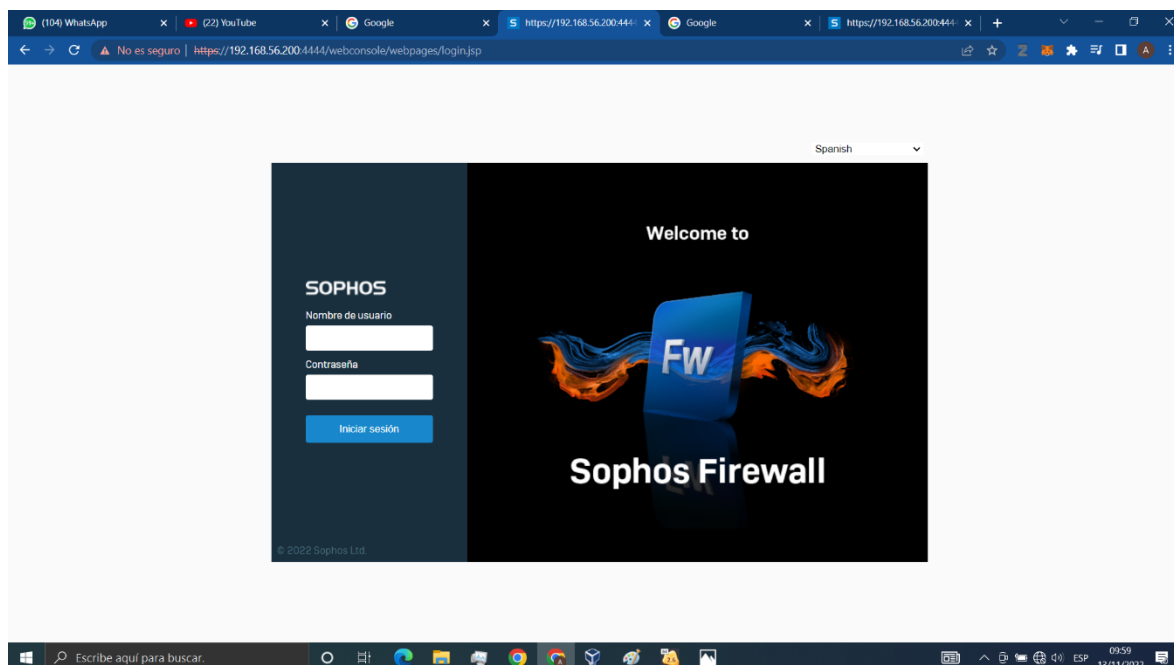
Siguiente ventana de configuraciones para recibir notificaciones del software, dar clic en siguiente.



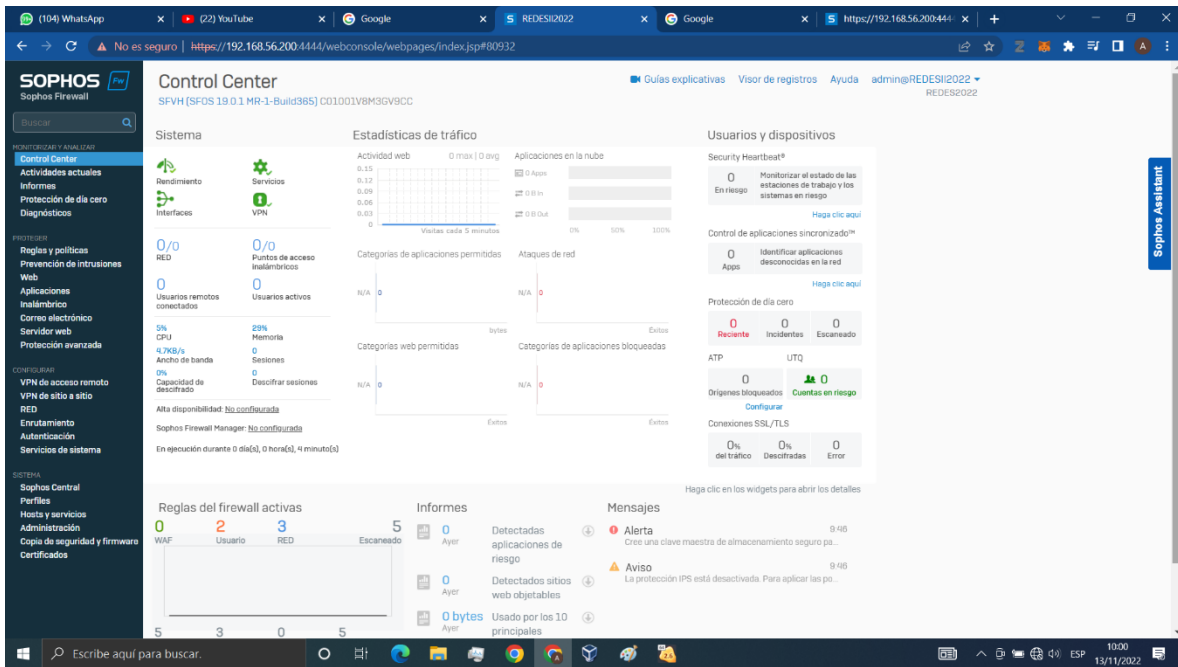
Resumen de las configuraciones, dar clic en botón de fin.



A continuación, los pide que iniciemos sección, poner usuario y contraseña.



Este es el panel de o dashboard de sophos XG



Configuración de red IPV4 e IPV6 y políticas con reglas.

En este apartado de RED se deberán asignar las redes que tendrán los puertos, en este caso se debe configurar los puertos 1 y 3 como LAN. Con respecto al puerto 2 por medio del DHCP obtendrá su IP para salida del internet y esta será WAN.

The screenshot shows the 'RED' configuration page in the Sophos Firewall interface. The left sidebar contains navigation options under 'MONITOREAR Y ANALIZAR', 'PROTEGER', 'CONFIGURAR', and 'SISTEMA'. The main content area displays a table of network interfaces:

| Interfaz | Estado/Velocidad de interfaz | Dirección IP | Misceláneo |
|--|--|--|-------------------|
| GuestAP WiFi Protección de redes inalámbricas | Desconectado Autonegociado | 10.255.0.1/255.255.255.0 Estática | Hardware: GuestAP |
| Port1 LAN Físico | Conectados 1000 Mbps - Full Duplex Autonegociado | 192.168.56.200/255.255.255.0 Estática 2800.94.232-1/64 Estática | Hardware: Port1 |
| Port2 WAN Físico | Conectados 1000 Mbps - Full Duplex Autonegociado | 192.168.1.205/255.255.255.0 DHCP | Hardware: Port2 |
| Port3 LAN Físico | Conectados 1000 Mbps - Full Duplex Autonegociado | 192.168.2.200/255.255.255.0 Estática 2800.94.222-1/64 Estática | Hardware: Port3 |

En los puertos se deben asignar sus redes correspondientes para que se reconozcan como gateways para el modo DHCP de las IPV4.

Puerto 1

The screenshot shows the configuration details for 'Port1' in the 'RED' section. The 'Zona de red' is set to 'LAN'. The 'Configuración IPv4' section is checked, and the 'Asignación IP' is set to 'Estática'. The 'IPv4/máscara de red' is set to '192.168.56.200 /24 (255.255.255.0)'. The 'Configuración IPv6' section is also checked, and the 'Asignación IP' is set to 'Estática'. The 'IPv6/prefijo' is set to '2800.94.232-1 /64'.

Puerto 3

SOPHOS FW
Sophos Firewall

Buscar

MONITORIZAR Y ANALIZAR

Control Center

Actividades actuales

Informes

Protección de día cero

Diagnósticos

PROTEGER

Reglas y políticas

Prevención de intrusiones

Web

Aplicaciones

Inalámbrico

Correo electrónico

Servidor web

Protección avanzada

CONFIGURAR

VPN de acceso remoto

VPN de sitio a sitio

RED

Enrutamiento

Autenticación

Servicios de sistema

SISTEMA

Sophos Central

Perfiles

Hosts y servicios

Administración

Copia de seguridad y firmware

Certificados

RED

Guías explicativas Visor de registros Ayuda admin REDES2022

Interfaces Zonas Administrador de vínculo WAN DNS DHCP Anuncio de enrutador IPv6 WAN móvil Túneles IP Vecinos (ARP-NDP) DNS dinámico

Nombre *

Port3

Hardware

Port3

Zona de red

LAN

☒ Configuración IPv4

Asignación IP

☒ Estática ☐ PPPoE (DSL) ☐ DHCP

IPv4/máscara de red *

192.168.2.200 /24 (255.255.255.0)

Detalle puerta de enlace

Nombre de puerta de enlace

IP de puerta de enlace

☒ Configuración IPv6

Asignación IP

☒ Estática ☐ DHCP

IPv6/prefijo *

2800:94:222::1 / 64

Detalle puerta de enlace

En la misma sección de RED ahora se configura el modo DHCP para los puertos 1 y 3, en lo cuales serán para las IPV4.

SOPHOS FW
Sophos Firewall

Buscar

MONITORIZAR Y ANALIZAR

Control Center

Actividades actuales

Informes

Protección de día cero

Diagnósticos

PROTEGER

Reglas y políticas

Prevención de intrusiones

Web

Aplicaciones

Inalámbrico

Correo electrónico

Servidor web

Protección avanzada

CONFIGURAR

VPN de acceso remoto

VPN de sitio a sitio

RED

Enrutamiento

Autenticación

Servicios de sistema

SISTEMA

Sophos Central

Perfiles

Hosts y servicios

RED

Guías explicativas Visor de registros Ayuda admin REDES2022

Interfaces Zonas Administrador de vínculo WAN DNS DHCP Anuncio de enrutador IPv6 WAN móvil Túneles IP Vecinos (ARP-NDP) DNS dinámico

Servidor

Nombre

Interfaz

Detalle de concesión

Dinámica

Estática

Versión IP

Estado

Gestionar

Default_DHCP_Server

Port1 - 192.168.56.200

192.168.56.2 - 192.168.56.199

-

IPv4

☒

GuestAccess_DHCP

GuestAP - 10.255.0.1

10.255.0.2 - 10.255.0.254

-

IPv4

☒

DHCP_TEST

Port3 - 192.168.2.200

192.168.2.2 - 192.168.2.199

-

IPv4

☒

DHCP_IPV6

Port3 - 2800:94:222::1

2800:94:222::2 - 2800:94:222::ffff

-

IPv6

☐

DHCP2_IPV6

Port1 - 2800:94:232::1

2800:94:232::2 - 2800:94:232::ffff

-

IPv6

☐

Añadir

Eliminar

Retransmisión

Puerto 1

InterfacesZonasAdministrador de vínculo WANDNSDHCPAnuncio de enrutador IPv6WAN móvilTúneles IPVecinos (ARP-NDP)DNS dinámico

Configuración general

Nombre *

Default_DHCP_Server

Interfaz

Port1 - 192.168.56.200

☐ Aceptar solicitud de cliente por retransmisión

Concesión IP dinámica

IP inicial

192.168.56.2

IP final

192.168.56.199

+ -

* Presione Tab para añadir un fila nueva

Asignación IP estática MAC

Nombre de host

Dirección MAC

Dirección IP

+ -

* Presione Tab para añadir un fila nueva

Máscara de subred *

/24 (255.255.255.0)

Nombre dominio

Puerta de enlace *

☒ Usar IP de interfaz como puerta de enlace

192.168.56.200

Tiempo de concesión predeterminado *

1440

1-43200 minutos (30 dias)

Tiempo de concesión máx. *

2880

1-43200 minutos (30 dias)

Servidor DNS

☐ Usar configuración DNS de dispositivo

DNS primario

192.168.56.200

DNS secundario

Puerto 3

InterfacesZonasAdministrador de vínculo WANDNSDHCPAnuncio de enrutador IPv6WAN móvilTúneles IPVecinos (ARP-NDP)DNS dinámico

Configuración general

Nombre *

DHCP_TEST

Interfaz

Port3 - 192.168.2.200

☐ Aceptar solicitud de cliente por retransmisión

Concesión IP dinámica

IP inicial

192.168.2.2

IP final

192.168.2.199

+ -

* Presione Tab para añadir un fila nueva

Asignación IP estática MAC

Nombre de host

Dirección MAC

Dirección IP

+ -

* Presione Tab para añadir un fila nueva

Máscara de subred *

/24 (255.255.255.0)

Nombre dominio

Puerta de enlace *

☒ Usar IP de interfaz como puerta de enlace

192.168.2.200

Tiempo de concesión predeterminado *

1440

1-43200 minutos (30 dias)

Servidor DNS

☐ Usar configuración DNS de dispositivo

DNS primario

192.168.2.200

DNS secundario

Servidor WAN1

En la sección de WEB se pueden configurar las políticas del Firewall, en la cuales se pueden crear y usar algunos que trae por defecto en firewall. Para uso de ejemplo se usará la política para un área de trabajo.

Web

[Guías explicativas](#) |
 [Visor de registros](#) |
 [Ayuda](#) |
 admin |
 REDES2022

MONITORIZAR Y ANALIZAR

Control Center

Actividades actuales

Informes

Protección de día cero

Diagnósticos

PROTEGER

Reglas y políticas

Prevención de intrusiones

Web

Aplicaciones

Inalámbrico

Correo electrónico

Servidor web

Protección avanzada

CONFIGURAR

VPN de acceso remoto

VPN de sitio a sitio

RED

Enrutamiento

Autenticación

Servicios de sistema

SISTEMA

Sophos Central

Perfiles




































































Hosts y servicios

Administración

Copia de seguridad y firmware

Certificados

| Políticas | Estado de la cuota de políticas | Actividades de usuario | Categorías | Grupos de URL | Excepciones | Configuración general | Tipos de archivo | Cuotas de navegación | *** |
|--|---------------------------------|---|------------|---------------|-------------|--|------------------|----------------------|-----|
| Prueba de política | | | | | | | | | |
| Añadir política | | | | | | | | | |
| Nombre | | Descripción | | En uso | | Gestionar | | | |
| + Default Policy | | A typical starter policy with options suitable for many organizations | | 1 | | + ⦿ ✎ 🗑️ | | | |
| + Ninguna carga web | | Restringir que los usuarios carguen contenido a cualquier sitio | | 0 ⚠️ | | + ⦿ ✎ 🗑️ | | | |
| + Ningún anuncio de juegos o contenido explícito | | Denegar el acceso a juegos, anuncios y sitios sexualmente explícitos | | 0 ⚠️ | | + ⦿ ✎ 🗑️ | | | |
| + Ningún chat o correo web | | Denegar el acceso a los sitios de chat online y correo web | | 0 ⚠️ | | + ⦿ ✎ 🗑️ | | | |
| + Ningún chat online | | Deny access to online chat sites | | 0 ⚠️ | | + ⦿ ✎ 🗑️ | | | |
| + Ningún contenido explícito | | Denegar el acceso a sitios sexualmente explícitos | | 0 ⚠️ | | + ⦿ ✎ 🗑️ | | | |
| + Ningún correo web | | Denegar el acceso a sitios de correo web | | 0 ⚠️ | | + ⦿ ✎ 🗑️ | | | |
| + No Ads or Explicit Content | | Deny access to advertisements and sexually explicit sites | | 0 ⚠️ | | + ⦿ ✎ 🗑️ | | | |
| + Política predeterminada en el lugar de trabajo | | Denegar el acceso a las categorías no deseadas con más frecuencia en entornos profesionales | | 1 | | + ⦿ ✎ 🗑️ | | | |

| Política predefinida en el lugar de trabajo | | Denegar el acceso a las categorías no deseadas con más frecuencia en entornos profesionales | | | 1 |     | | |
|--|---|---|--|---------------|--|---|--|--|
| Usuarios | Actividades | Acción | | Restricciones | Gestionar | Estado | | |
|  Cualquiera |  Social Networking |  | | |    |  | | |
|  Cualquiera |  Weapons |  | | |    |  | | |
|  Cualquiera |  Extreme |  | | |    |  | | |
|  Cualquiera |  Phishing & Fraud |  | | |    |  | | |
|  Cualquiera |  Militancy & Extremist |  | | |    |  | | |
|  Cualquiera |  Gambling |  | | |    |  | | |
|  Cualquiera |  Criminal Activity |  | | |    |  | | |
|  Cualquiera |  Pro-Suicide & Self-Harm |  | | |    |  | | |
|  Cualquiera |  Intellectual Piracy |  | | |    |  | | |

Estas son las actividades bloqueadas para un área de trabajo.

En la parte de Reglas y Políticas se van a crear las reglas que usarán las políticas creadas anteriormente, así como sus métodos de conexión de origen y destino.

Regla para IPV4

ON Estado de la regla

Nombre de regla *

PUERTO 3

Acción

Aceptar

☐ Registrar tráfico de firewall

Registra el tráfico que coincide con esta regla de firewall en el dispositivo (por defecto) o en el servidor syslog configurado.

Descripción

Introducir Descripción

Grupo de reglas

Ninguna

Origen

Seleccione las zonas, redes y dispositivos de origen.
La regla se aplica al tráfico de estos orígenes durante el periodo de tiempo programado.

Zonas de origen *

LAN

Añadir nuevo elemento

Dispositivos y redes de origen *

CUALQUIERA

Añadir nuevo elemento

Durante la hora programada

Siempre

Seleccione para aplicar la regla a un periodo de tiempo y día de la semana específicos.

Origen

Seleccione las zonas, redes y dispositivos de origen.
La regla se aplica al tráfico de estos orígenes durante el periodo de tiempo programado.

Zonas de origen *

LAN

Añadir nuevo elemento

Dispositivos y redes de origen *

CUALQUIERA

Añadir nuevo elemento

Durante la hora programada

Siempre

Seleccione para aplicar la regla a un periodo de tiempo y día de la semana específicos.

Destino y servicios

Seleccione las zonas, redes, dispositivos y servicios de destino.
La regla se aplica al tráfico hacia estos destinos.

Zonas de destino *

WAN

Añadir nuevo elemento

Redes de destino *

CUALQUIERA

Añadir nuevo elemento

Servicios *

CUALQUIERA

Añadir nuevo elemento

Los servicios son tipos de tráfico basados en una combinación de protocolos y puertos.

Uso de la política

Funciones de seguridad

✓ Filtrado web

Política web

Política predeterminada en el lugar de trab...

☐ Aplicar conformado de tráfico basado en categoría web

☒ Bloquear el protocolo QUIC

Escaneado de malware y contenido

☐ Escanear HTTP y descifrar HTTPS

☐ Utilizar protección de día cero

☐ Escanear FTP en busca de malware

Filtrando puertos web comunes

☐ Usar proxy web en lugar de motor DPI

[¿Motor DPI o proxy web?](#)

Opciones de proxy web

☐ Descifrar HTTPS durante filtrado de proxy web

Regla IPV6

Para el caso de las reglas IPV6 como es ruteo estático se deben asignar dos políticas para que puedan acceder de una red a otra.

ON Estado de la regla

Nombre de regla *

ipv62.0

Descripción

Introducir Descripción

Grupo de reglas

Ninguna

Acción

Aceptar

☒ Registrar tráfico de firewall

Registra el tráfico que coincide con esta regla de firewall en el dispositivo (por defecto) o en el servidor syslog configurado.

RED IPV6 del puerto 1

Editar RED

Nombre *

PORT1_IPV6

Versión IP *

IPv6

Tipo *

RED

Dirección IP *

2800:94:232::

Prefijo

64

Grupo de hosts IP

Añadir nuevo elemento

Guardar

Cancelar

RED IPV6 puerto 3

Editar RED

Nombre *

PORT3

Versión IP *

IPv6

Tipo *

RED

Dirección IP *

2800:94:222::

Prefijo

64

Grupo de hosts IP

Añadir nuevo elemento

Guardar

Cancelar

De la siguiente manera se pueden comunicar las redes, en este caso es para que el puerto 1 pueda acceder la red del puerto 3 y lo mismo se debe hacer para que el puerto 3 conozca como llegar a la red del puerto 1.

Origen

Seleccione las zonas, redes y dispositivos de origen.
La regla se aplica al tráfico de estos orígenes durante el periodo de tiempo programado.

Zonas de origen *

LAN

Añadir nuevo elemento

Dispositivos y redes de origen *

PORT1_IPV6

Añadir nuevo elemento

Durante la hora programada

Siempre

Selecione para aplicar la regla a un periodo de tiempo y día de la semana específicos.

Destino y servicios

Seleccione las zonas, redes, dispositivos y servicios de destino.
La regla se aplica al tráfico hacia estos destinos.

Zonas de destino *

LAN

Añadir nuevo elemento

Redes de destino *

PORT3

Añadir nuevo elemento

Servicios *

CUALQUIERA

Añadir nuevo elemento

Los servicios son tipos de tráfico basados en una combinación de protocolos y puertos.

Pruebas de testeo del firewall.

En este caso se usarán dos máquinas para verificar si se les asignó de forma automática las red IPV4 y asignarles las red IPV6 que corresponden al puerto conectado.

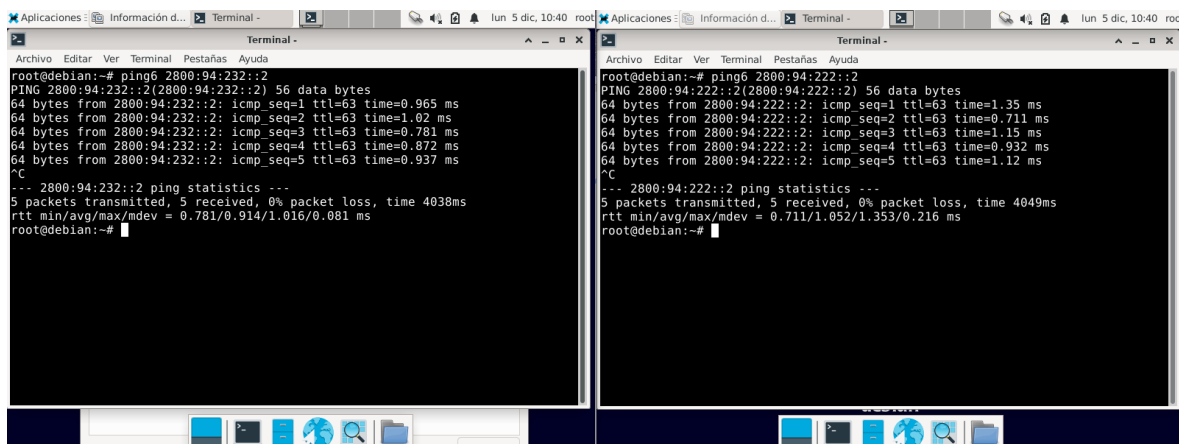
PC1

PC2

The image displays two side-by-side screenshots of a network configuration window titled 'Información de la conexión' (Connection Information) for 'Wired connection 1'. The left window is for PC1 and the right window is for PC2. Both windows show the following configuration details:

- General:**
 - Interfaz: Cableada (enp0s3)
 - Dirección hardware: 08:00:27:53:CD:40
 - Controlador: e1000
 - Velocidad: 1000 Mb/s
 - Seguridad: Ninguna
- IPv4:**
 - Dirección IP: 192.168.2.2 (PC1) / 192.168.56.3 (PC2)
 - Dirección de difusión: 192.168.2.255 (PC1) / 192.168.56.255 (PC2)
 - Máscara de subred: 255.255.255.0
 - Ruta predeterminada: 192.168.2.200 (PC1) / 192.168.56.200 (PC2)
 - DNS primario: 192.168.2.200 (PC1) / 192.168.56.200 (PC2)
 - DNS secundario: 192.168.2.1 (PC1) / 192.168.56.1 (PC2)
- IPv6:**
 - Dirección IP: 2800:94:222::2/64 (PC1) / 2800:94:232::2/64 (PC2)
 - Más direcciones: (Expandable section)
 - Ruta predeterminada: 2800:94:222::1 (PC1) / 2800:94:232::1 (PC2)
 - DNS primario: 2800:94:222::1 (PC1) / 2800:94:232::1 (PC2)

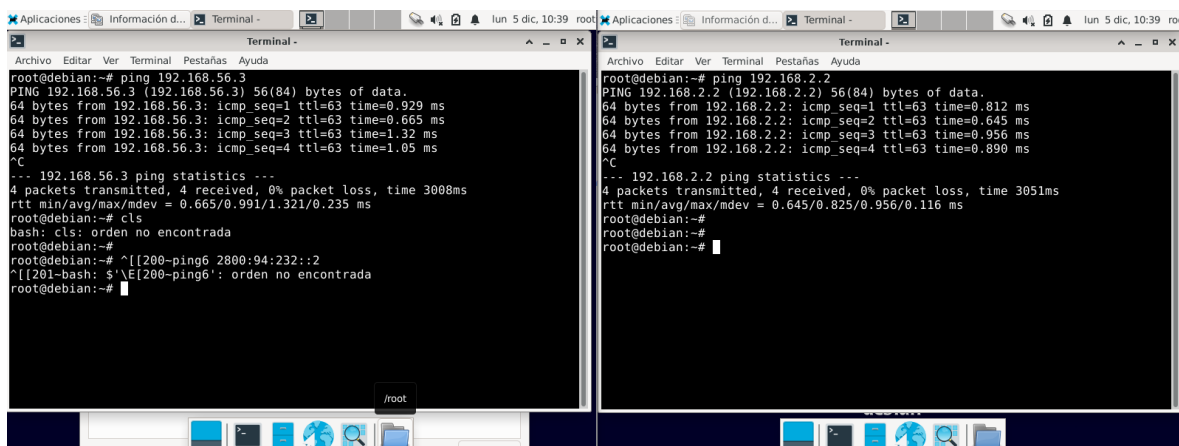
Pruebas de ping IPV4 en ambos equipos.



```
root@debian:~# ping6 2800:94:232::2
PING 2800:94:232::2(2800:94:232::2) 56 data bytes
64 bytes from 2800:94:232::2: icmp_seq=1 ttl=63 time=0.965 ms
64 bytes from 2800:94:232::2: icmp_seq=2 ttl=63 time=1.02 ms
64 bytes from 2800:94:232::2: icmp_seq=3 ttl=63 time=0.781 ms
64 bytes from 2800:94:232::2: icmp_seq=4 ttl=63 time=0.872 ms
64 bytes from 2800:94:232::2: icmp_seq=5 ttl=63 time=0.937 ms
^C
--- 2800:94:232::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4038ms
rtt min/avg/max/mdev = 0.781/0.914/1.016/0.081 ms
root@debian:~#
```

```
root@debian:~# ping6 2800:94:222::2
PING 2800:94:222::2(2800:94:222::2) 56 data bytes
64 bytes from 2800:94:222::2: icmp_seq=1 ttl=63 time=1.35 ms
64 bytes from 2800:94:222::2: icmp_seq=2 ttl=63 time=0.711 ms
64 bytes from 2800:94:222::2: icmp_seq=3 ttl=63 time=1.15 ms
64 bytes from 2800:94:222::2: icmp_seq=4 ttl=63 time=0.932 ms
64 bytes from 2800:94:222::2: icmp_seq=5 ttl=63 time=1.12 ms
^C
--- 2800:94:222::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4049ms
rtt min/avg/max/mdev = 0.711/1.052/1.353/0.216 ms
root@debian:~#
```

Pruebas de ping IPV6 en ambos equipos.



```
root@debian:~# ping 192.168.56.3
PING 192.168.56.3 (192.168.56.3) 56(84) bytes of data.
64 bytes from 192.168.56.3: icmp_seq=1 ttl=63 time=0.929 ms
64 bytes from 192.168.56.3: icmp_seq=2 ttl=63 time=0.665 ms
64 bytes from 192.168.56.3: icmp_seq=3 ttl=63 time=1.32 ms
64 bytes from 192.168.56.3: icmp_seq=4 ttl=63 time=1.05 ms
^C
--- 192.168.56.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 0.665/0.991/1.321/0.235 ms
root@debian:~# cls
bash: cls: orden no encontrada
root@debian:~#
root@debian:~# ^[[200-ping6 2800:94:232::2
^[[201-bash: '$\E[200-ping6': orden no encontrada
root@debian:~#
```

```
root@debian:~# ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=63 time=0.812 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=63 time=0.645 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=63 time=0.956 ms
64 bytes from 192.168.2.2: icmp_seq=4 ttl=63 time=0.890 ms
^C
--- 192.168.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3051ms
rtt min/avg/max/mdev = 0.645/0.825/0.956/0.116 ms
root@debian:~#
root@debian:~#
```

Verificación del uso de la política de trabajo.

