Instalación de Sophos XG Firewall

.....

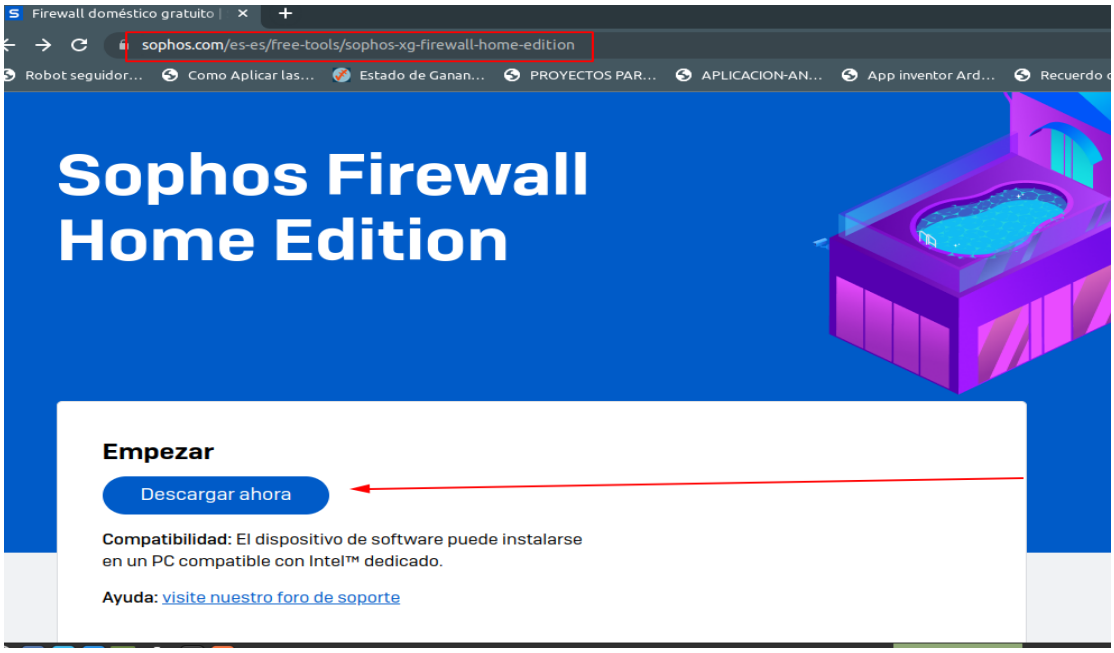
....

REDES II

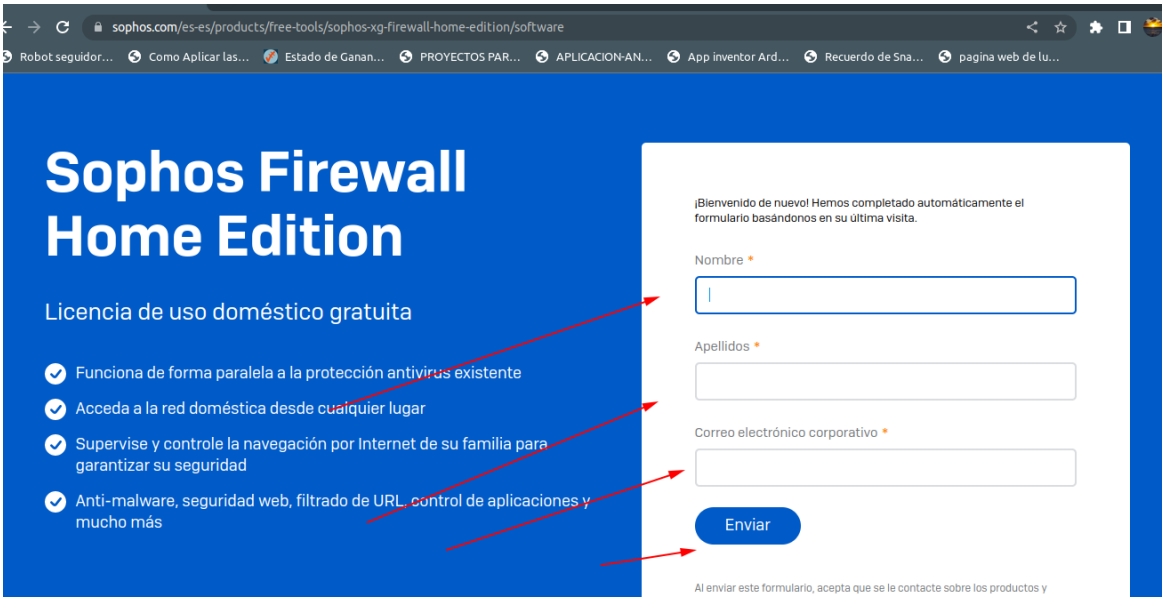
Universidad Luterana Salvadoreña

Instalación de Sophos XG Firewall Home Editión

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.

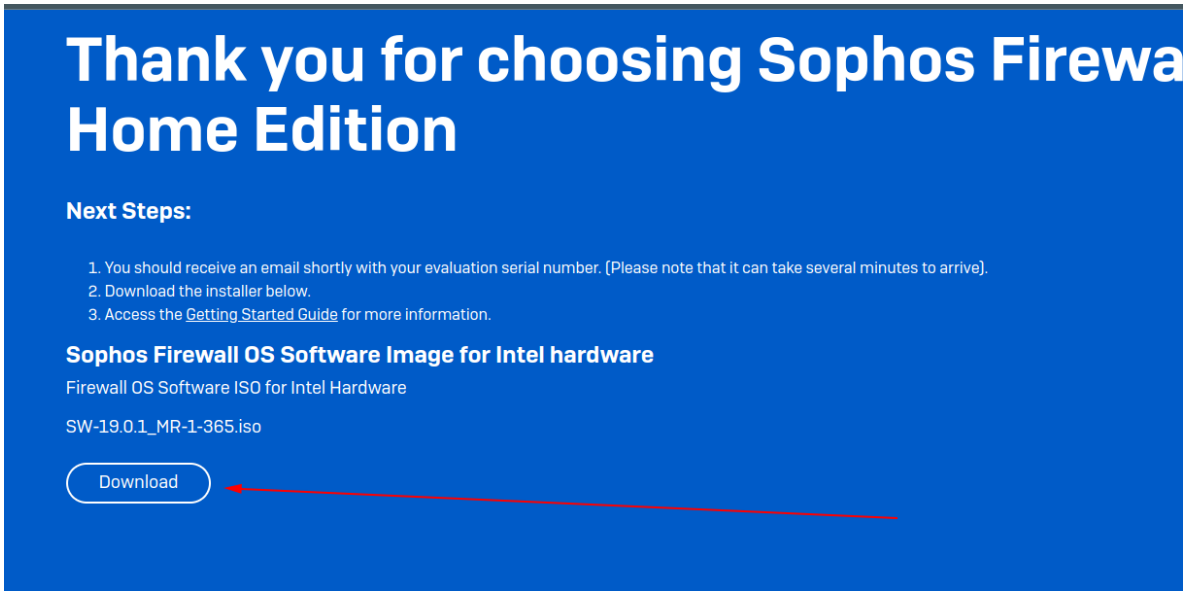


Luego pide que se registre para poder obtener la licencia de software para la implementación. Tenemos que registrarnos.



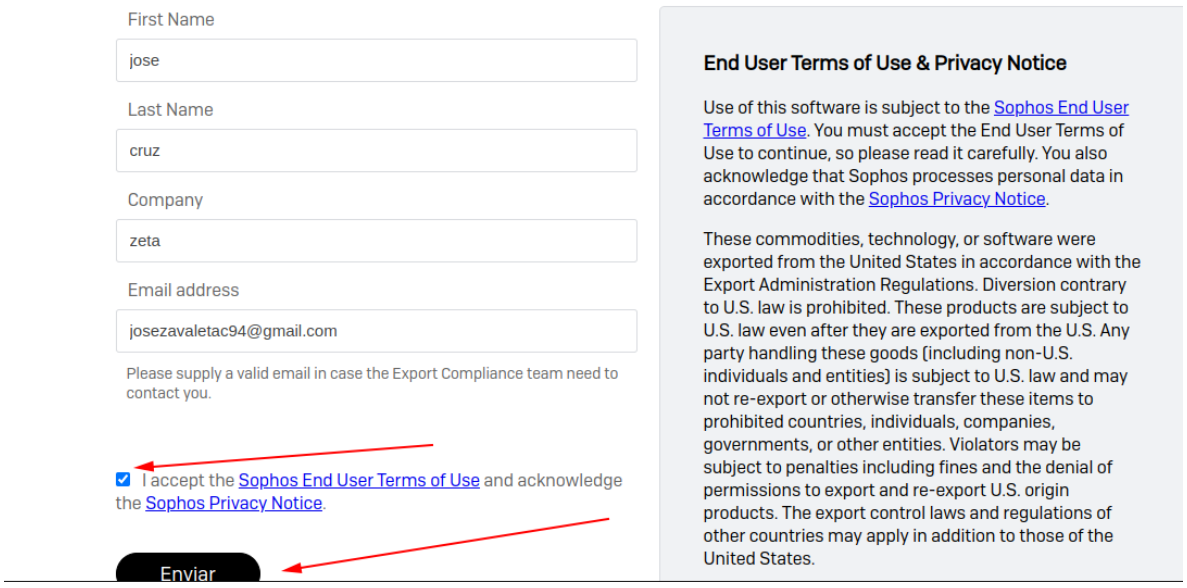
Después de registrarse se redirige a otra página donde si ya nos aparece el archivo a descargar, se procede a descargar la iso para la instalación, pesa 700mb.

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



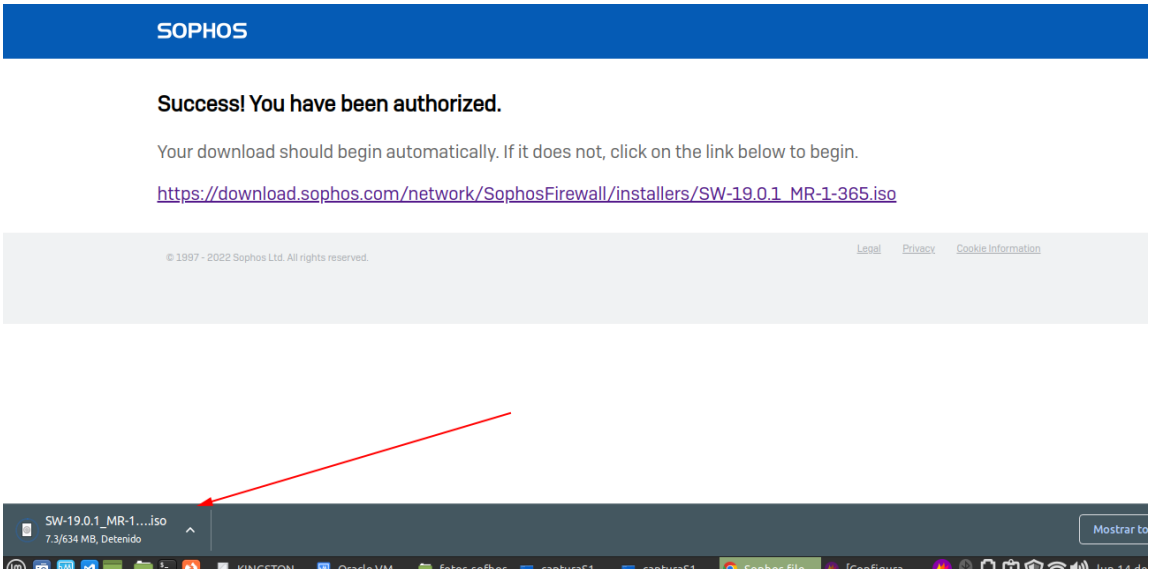
.

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.

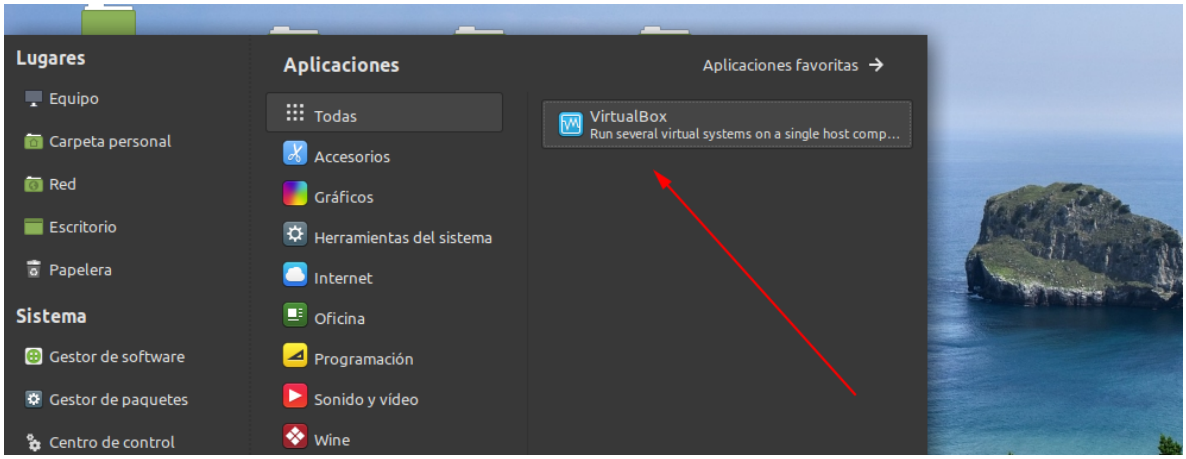


Revisar el correo para ver que ya nos han enviado el código de la licencia para activar el software Sophos XG.

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.

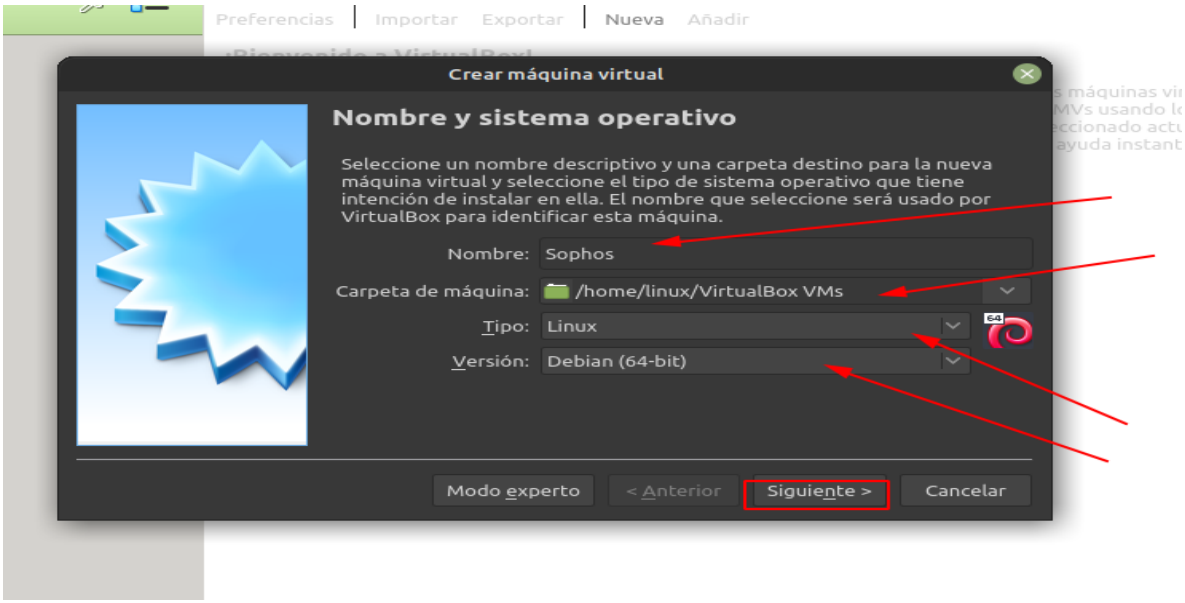


Mientras se descarga la iso de Software de Sophos se procede a utilizar un hipervisor para la instalación del software en este caso utilizaremos VirtualBox. Procedemos a crear una máquina virtual para la demostración.

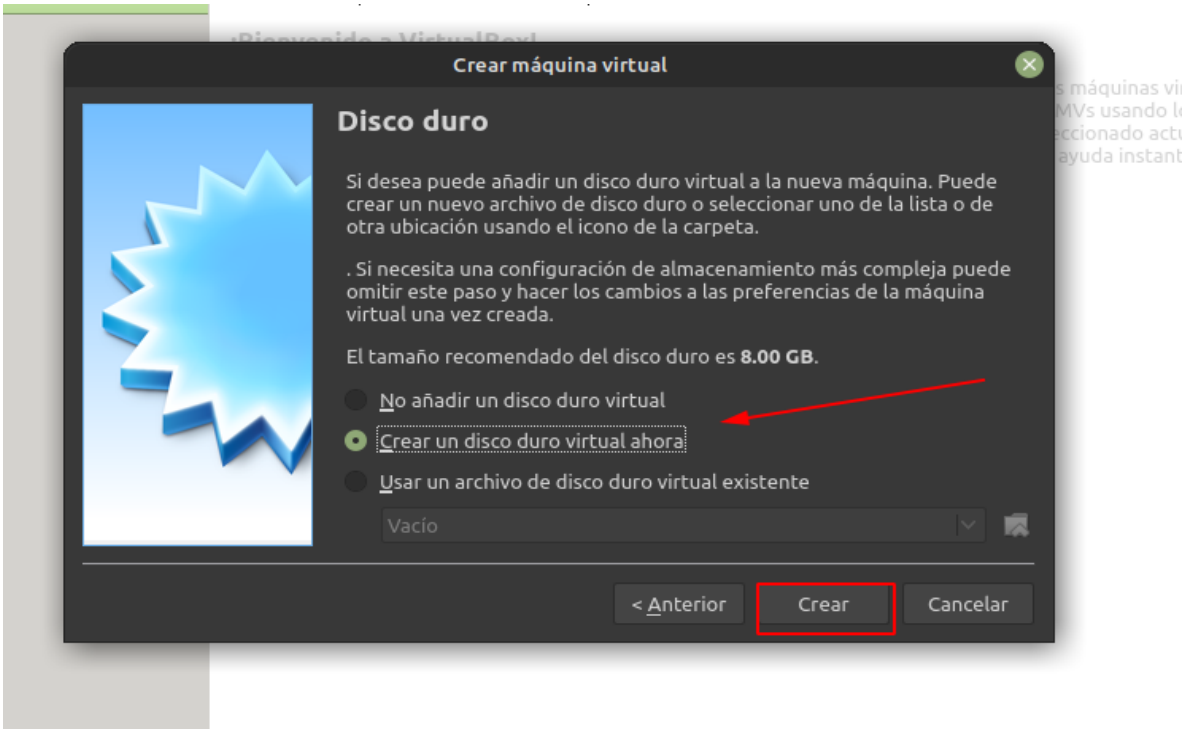


Se procedes a crear una máquina virtual en la opción nuevo.

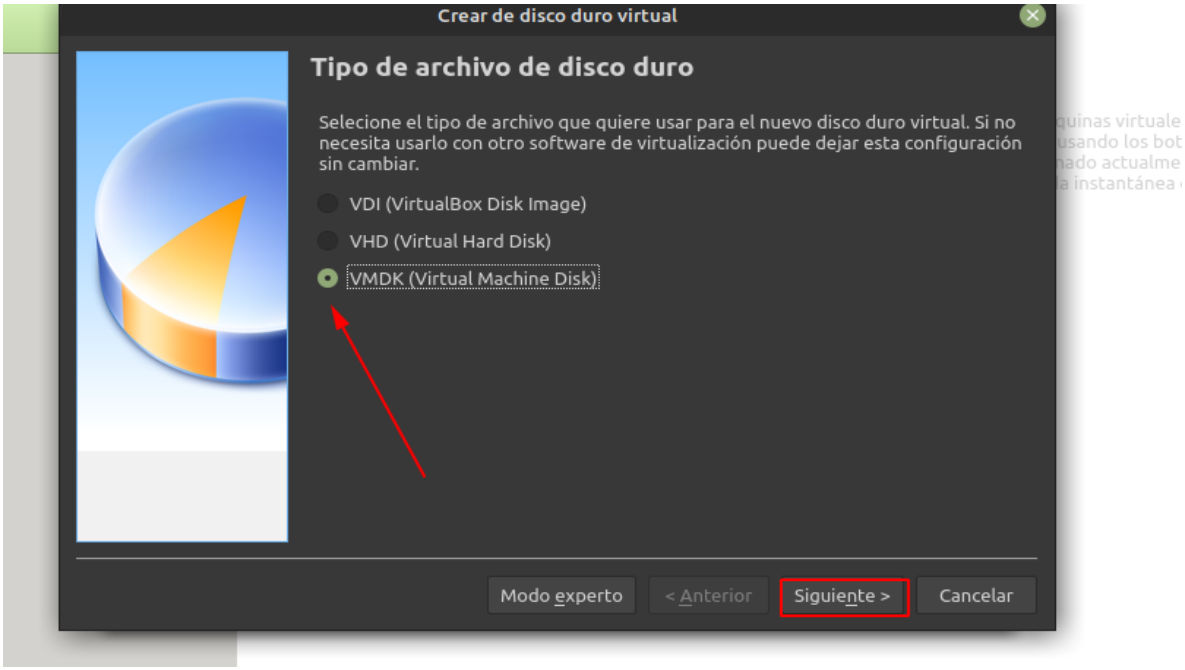
Realizar las configuraciones para la instalación colocamos el nombre, seleccionamos el sistema operativo y seleccionamos debían de 64bit o según tu sistema operativo. Dar clic en siguiente.



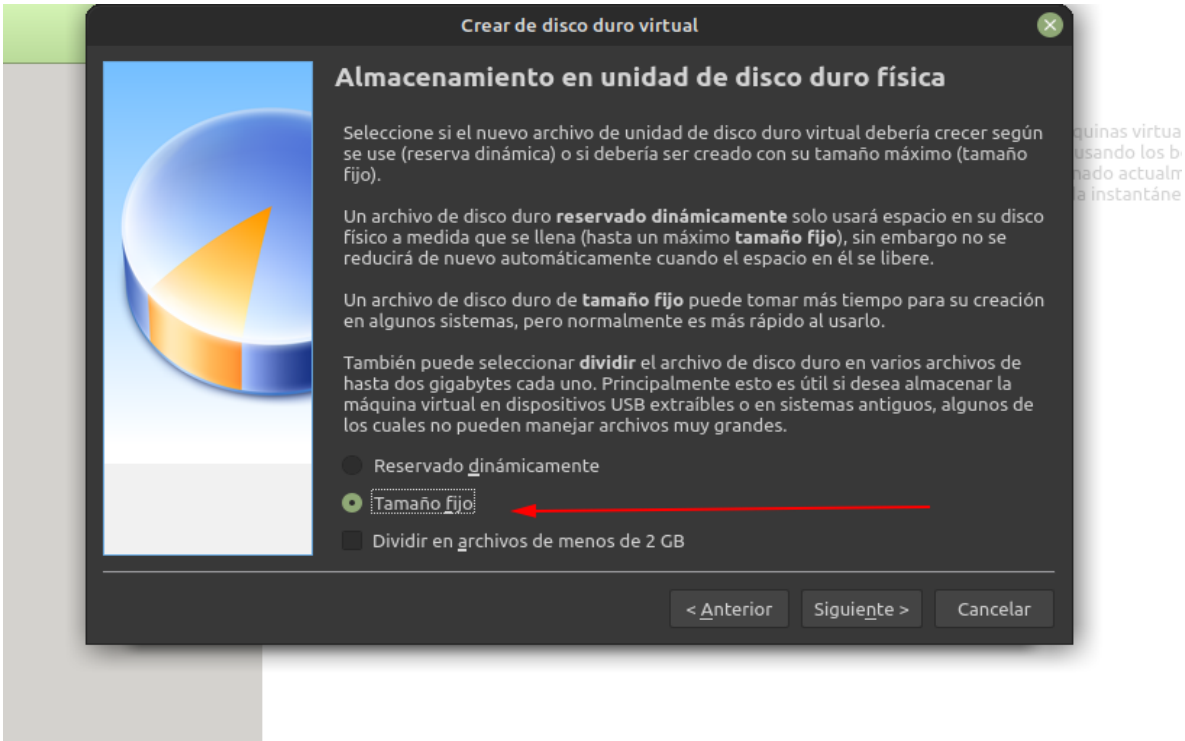
Seleccionar en crear un disco virtual duro ahora, y dar clic en crear.



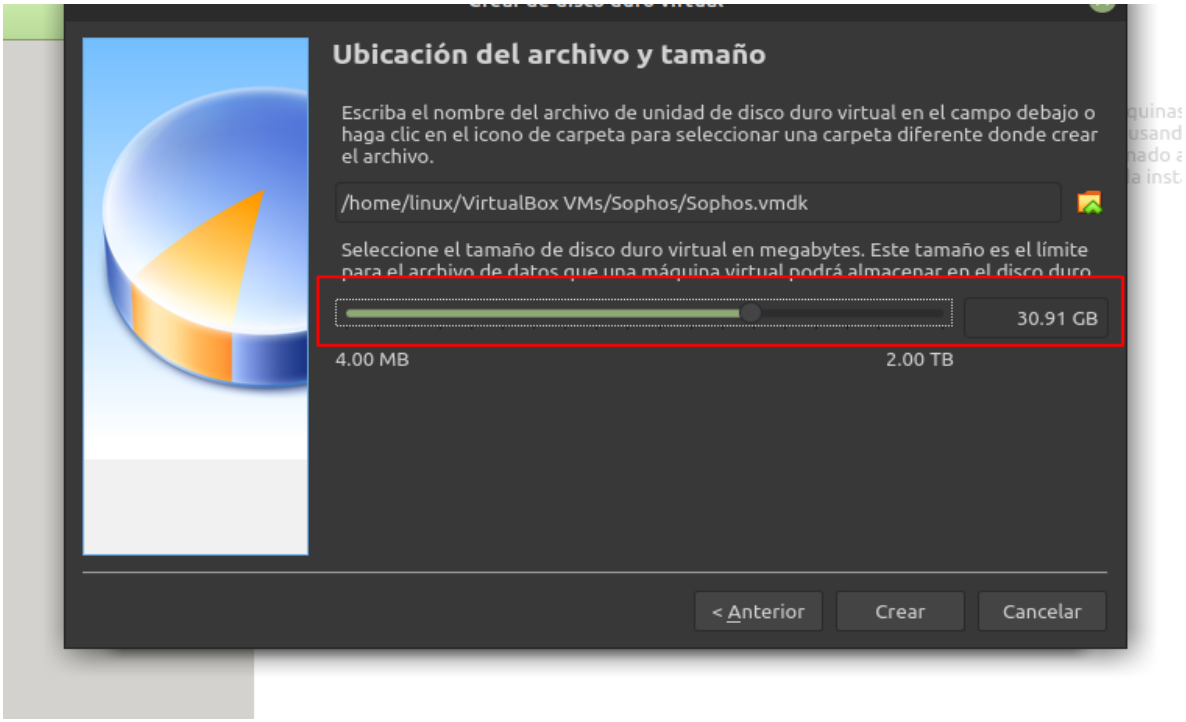
Elegir la opción de VMDK y dar clic en siguiente.



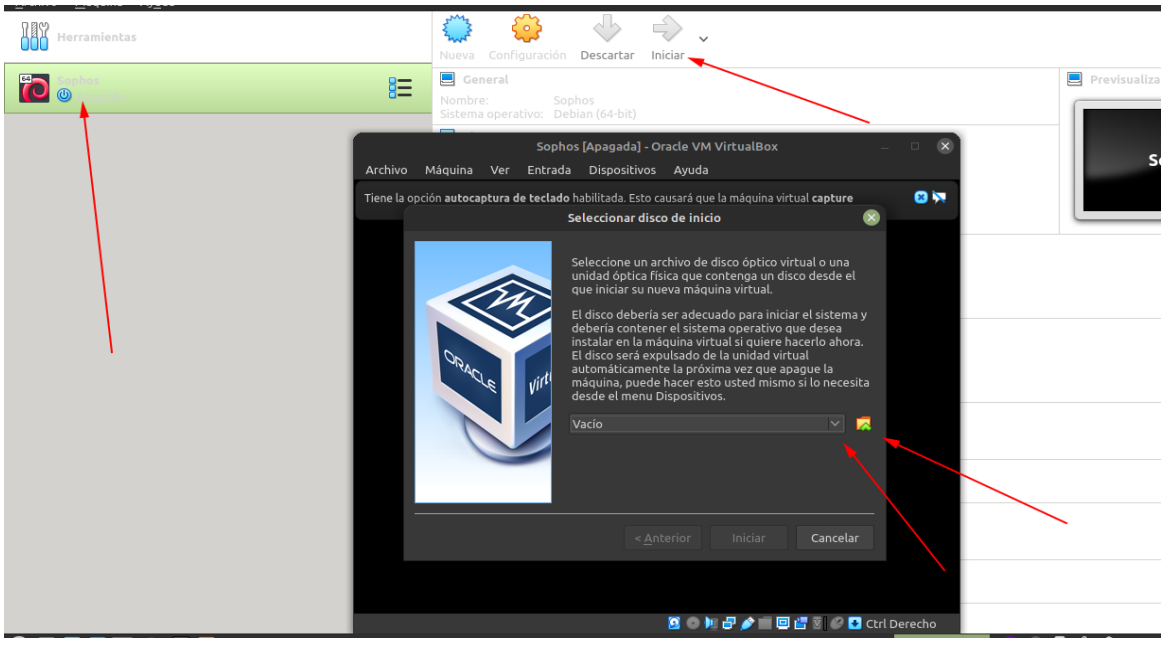
Elegimos la opción de tamaño fijo, damos clic en siguiente.



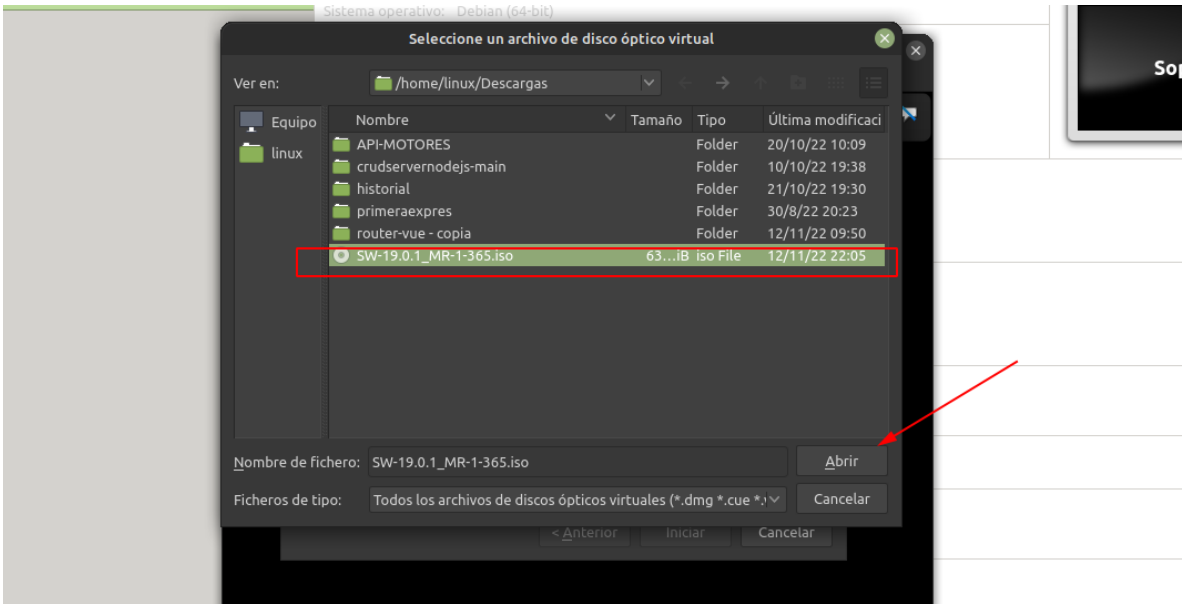
Elegir el tamaño del Disco virtual a crear, en este caso será de 30gb, dar clic en crear.



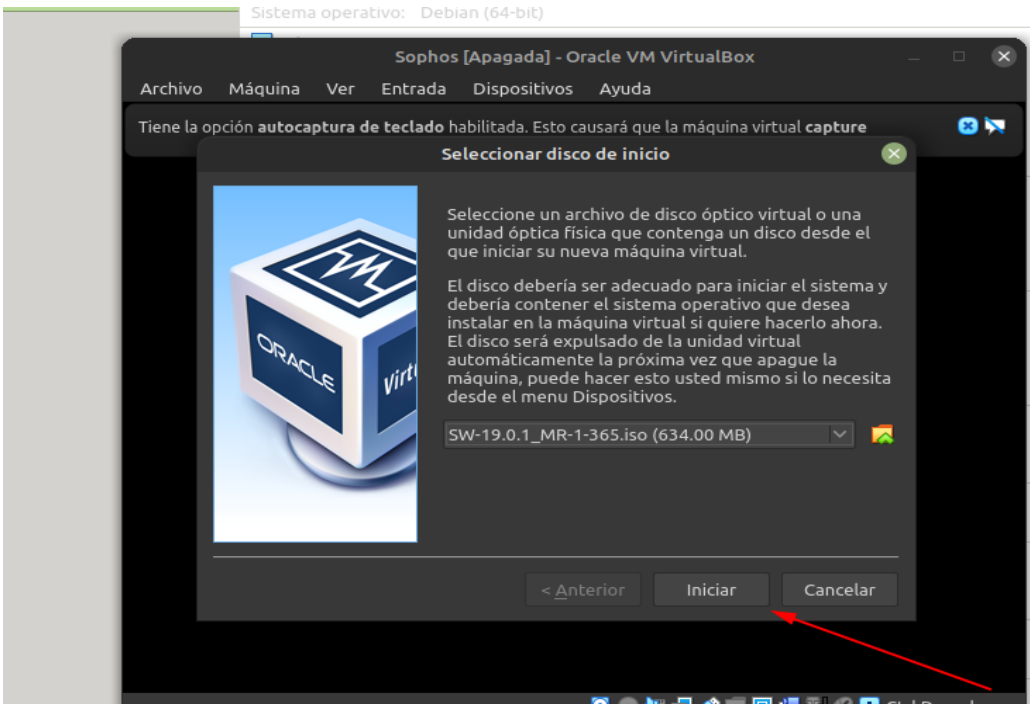
Se crea la máquina virtual esto puede demorar de acuerdo a tu procesador, una vez creada dar en iniciar la máquina virtual, aparece que no hay iso para la instalación dar clic en el folder para ir a buscarla.



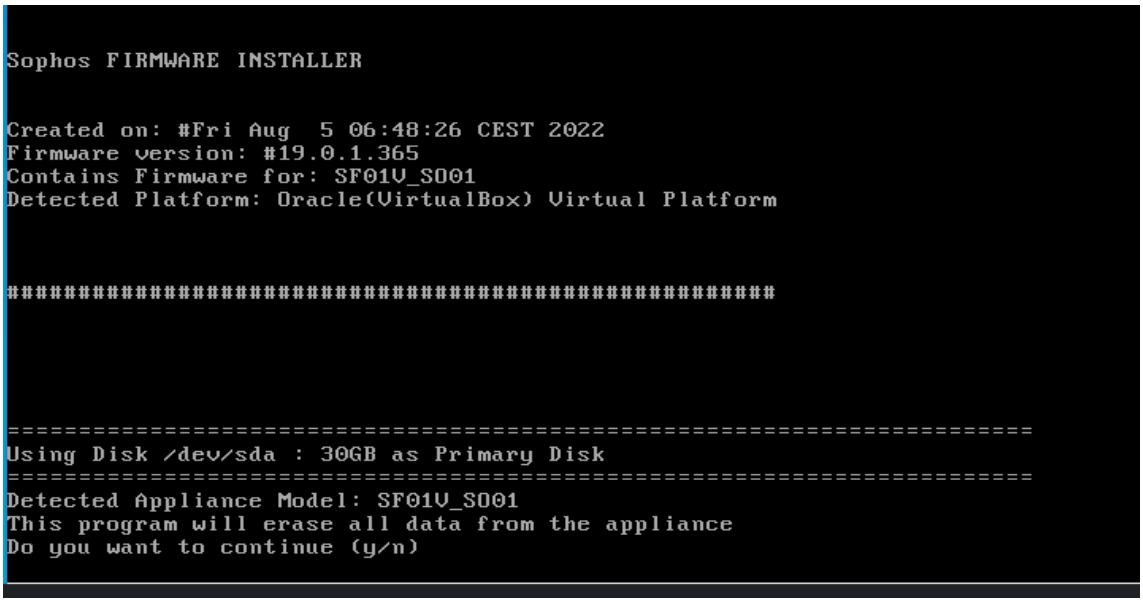
Navegamos a donde esta la iso y le damos en abrir.



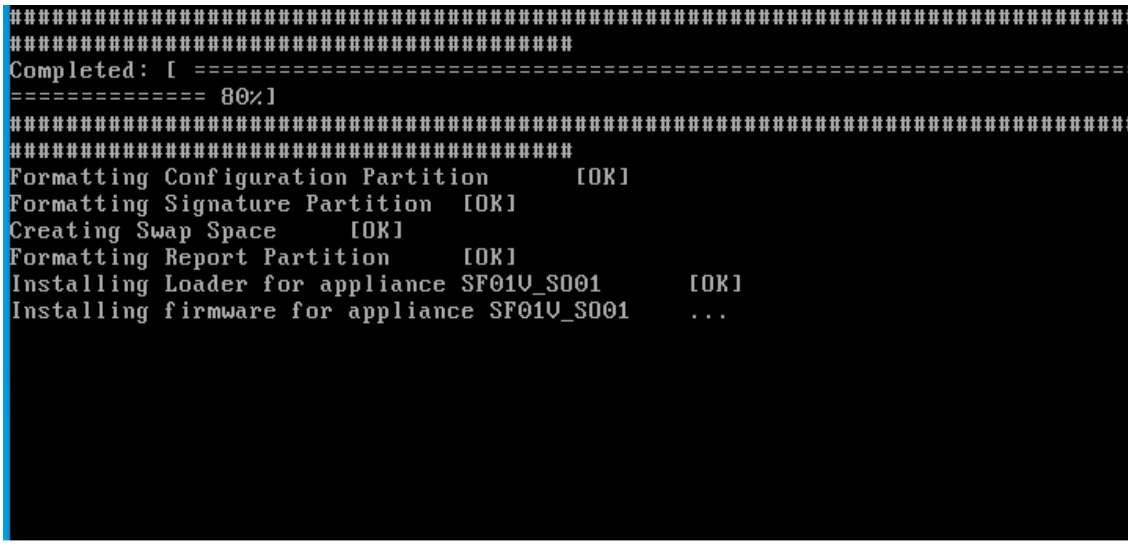
Ya seleccionada se procede a dar clic en iniciar para la instalación del software Sophos XG.



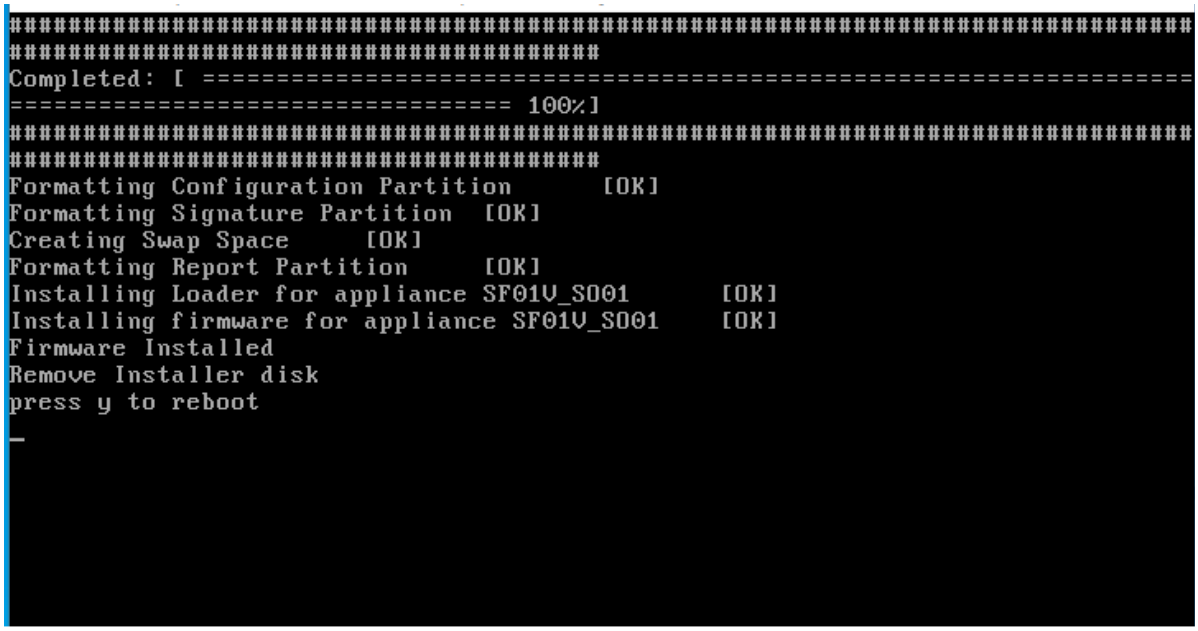
Aparece el siguiente mensaje en la cli escribir la letra “y” para proceder.



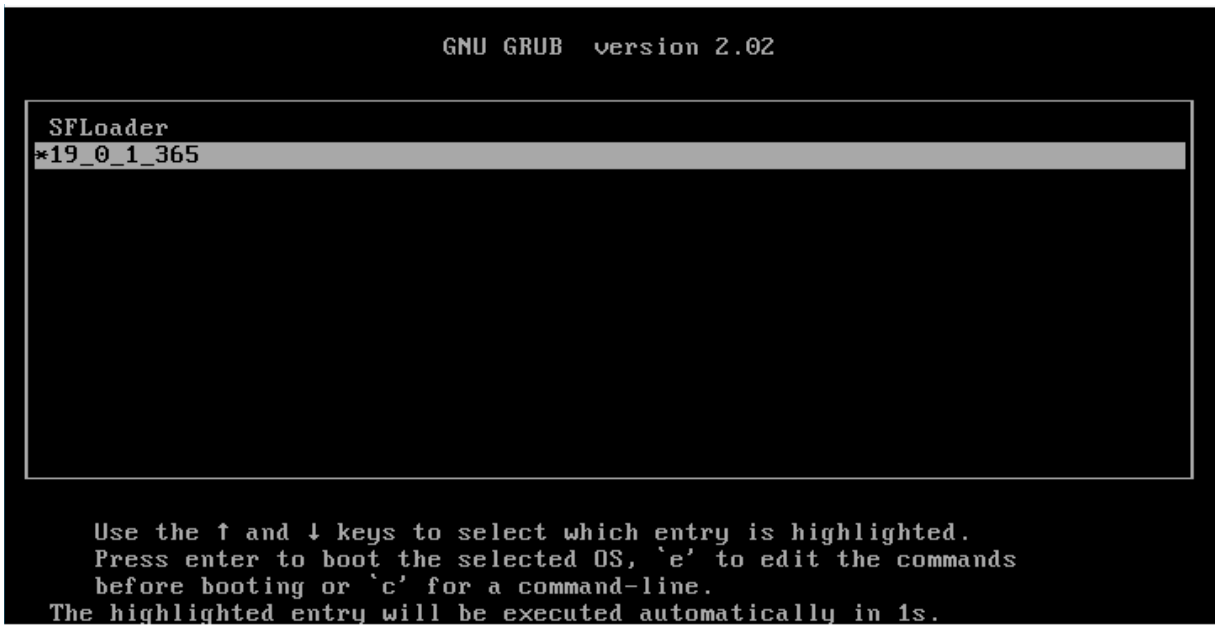
Se observa que se está instalando el software Sophos XG.



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.

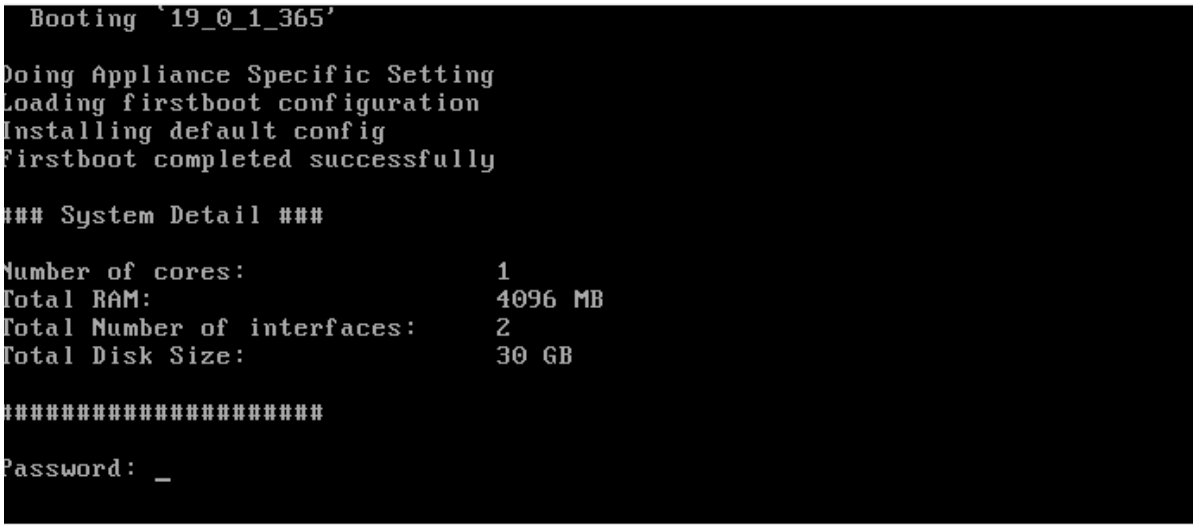


Al iniciar la máquina nos aparece el GRUB y se inicia automáticamente.



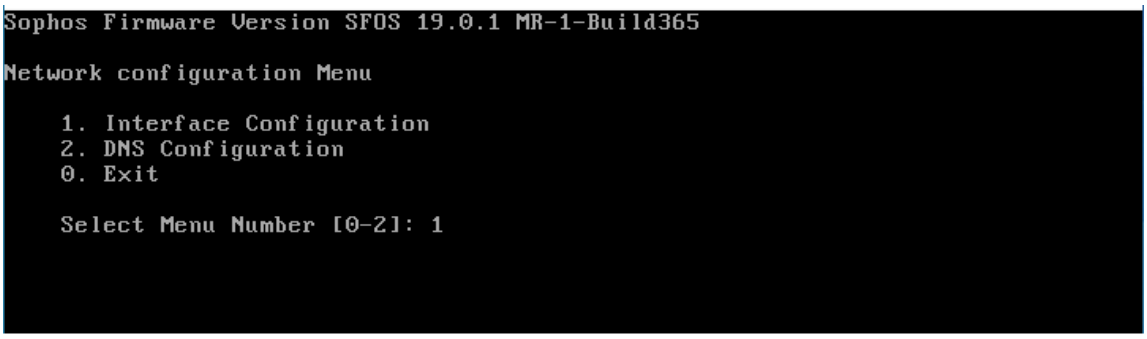
Nos pide la contraseña en este caso es admin. Se procede a colocarla

Recordar activar dos interfaces en la configuración de la máquina virtual.

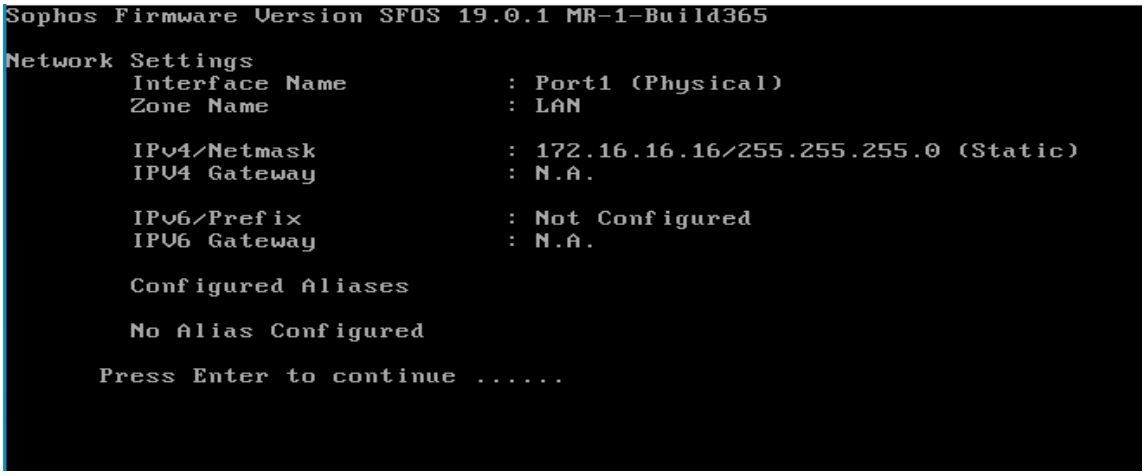


Después de loguearse nos aparece un menú de opciones. Escribir 1 para ver las configuraciones de red.

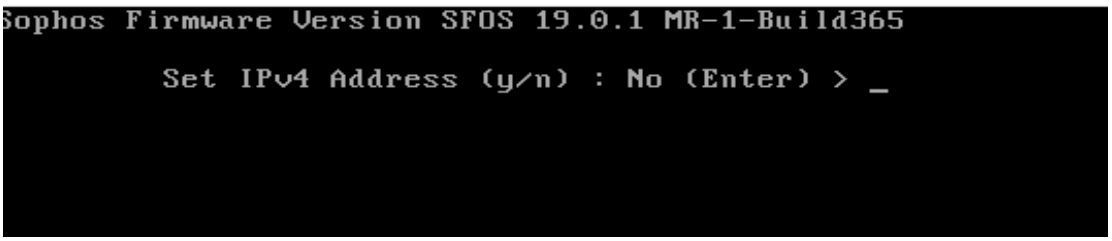
Aparece otro submenú también escribir 1



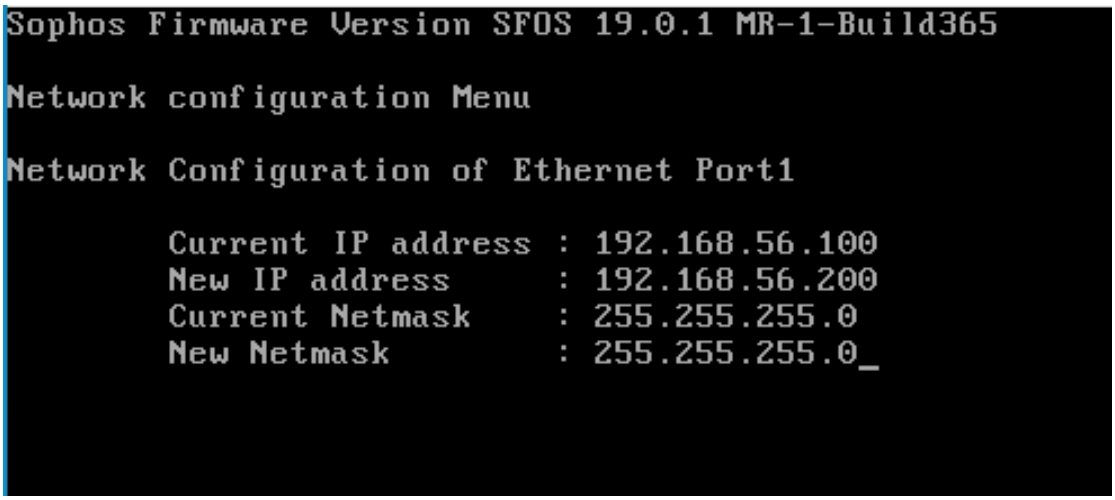
Se puede ver la configuración de las redes por defecto Sophos configura en la red 0 la ip 172.16.16.16/255.255.255.0. presionar enter para continuar.



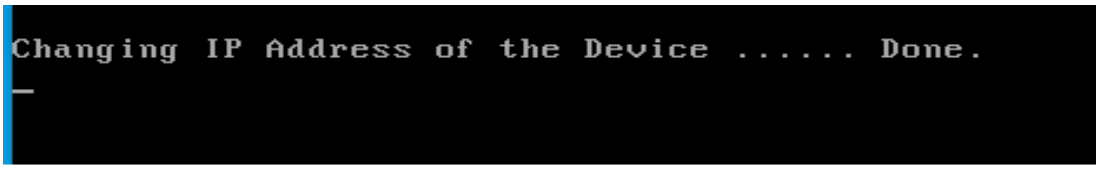
y nos pregunta si queremos cambiar la ip configurada por Sophos. En esta ocasión escribimos la letra “y” para cambiar puesto que el hipervisor maneja otra ip la que toma de la máquina principal.



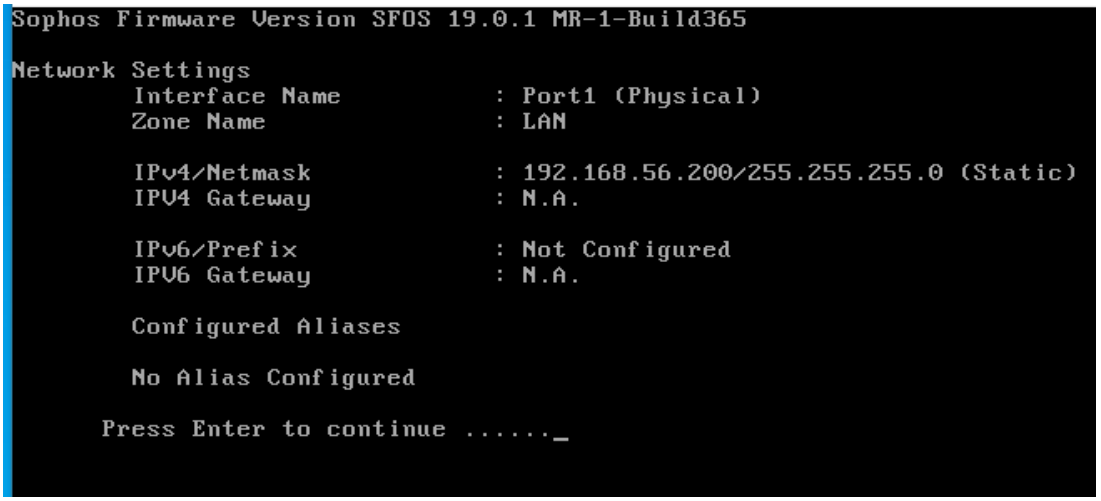
Procedemos a cambiar la ip que nos está proporcionando el proveedor de internet y agregamos la máscara de red también.



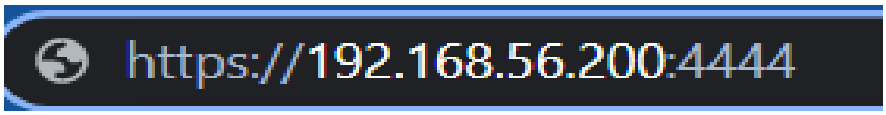
Dar enter los cambios se están realizando.



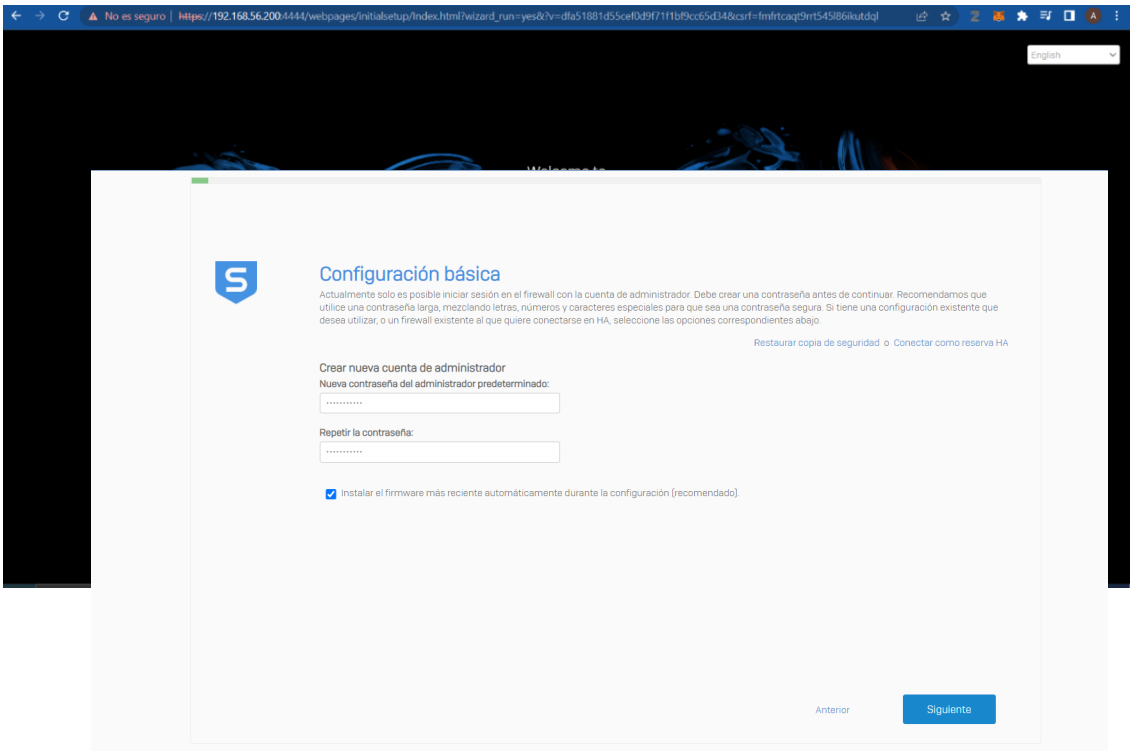
Verificamos si los cambios se han realizado, efectivamente la ip se ha cambiado.



Abrir un navegador escribir https://192.168.56.200:4444

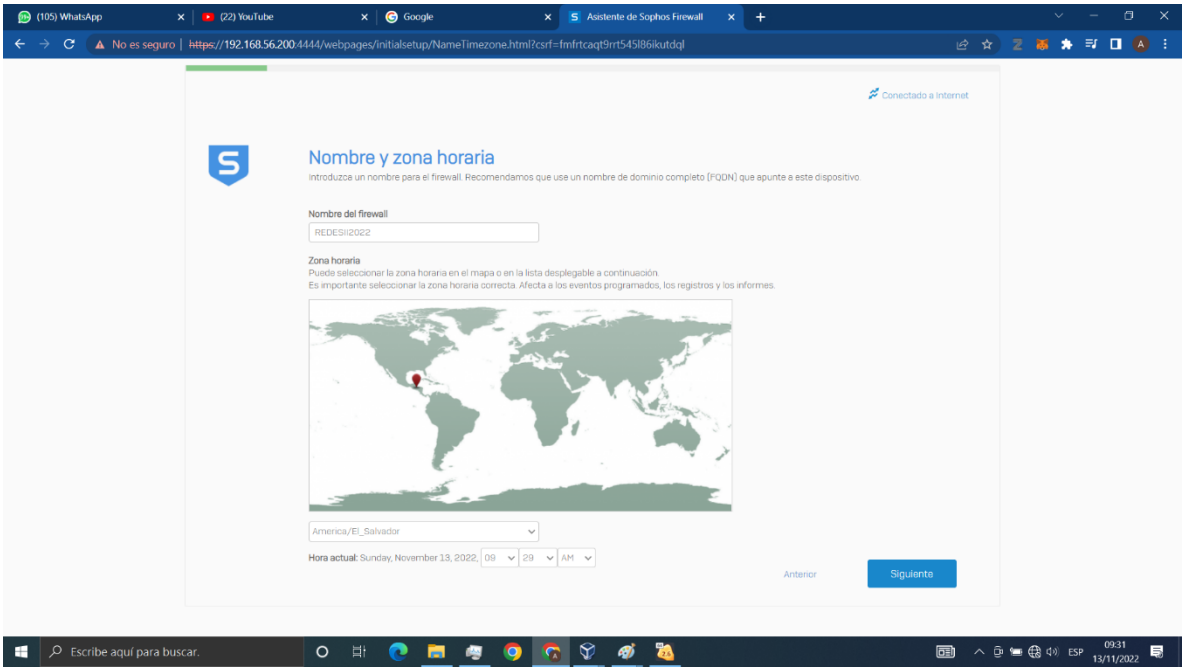


Aparecerá la interfaz gráfica del Sophos y aceptamos los términos y condiciones. Presionar en star setup

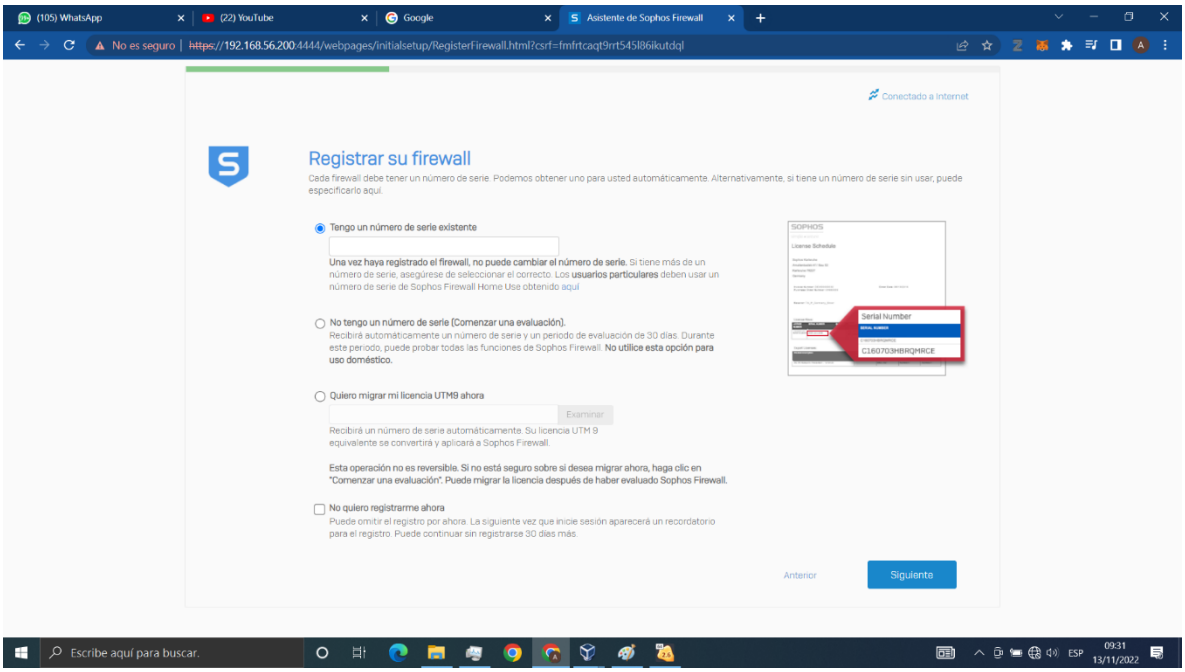


Pide crear contraseña y usuario para ingresar al dashboard. Y proceder a la instalación de paquetes adicionales, dar clic en siguiente.

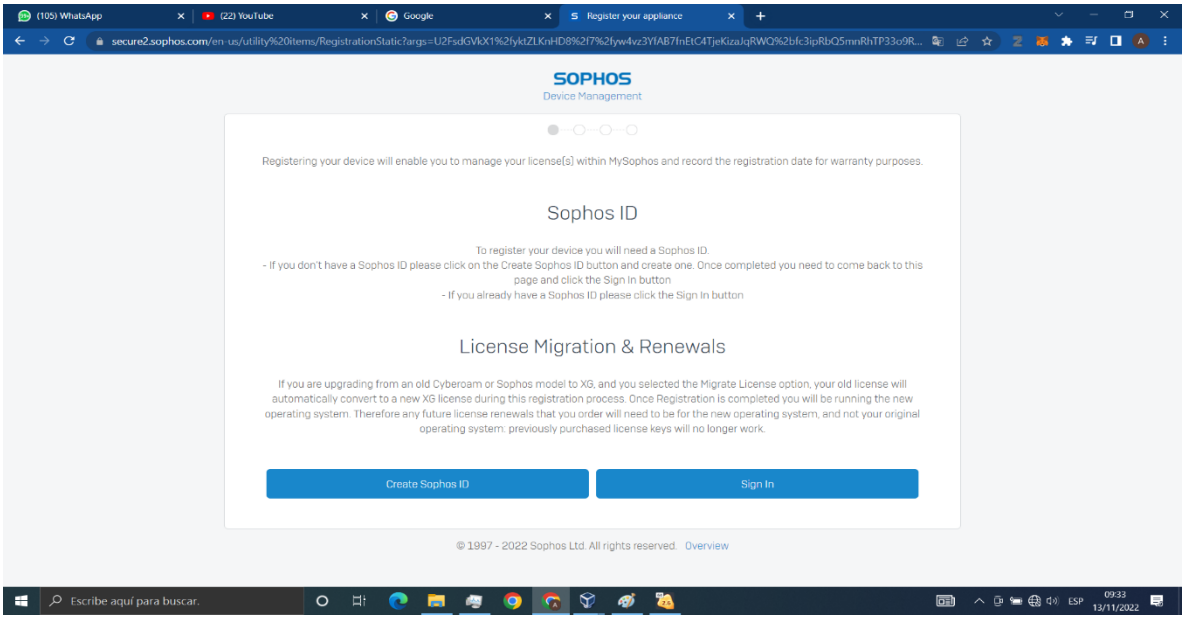
En esta ventana nos pide que se configure la información del nombre, firewall zona horaria, ubicación y fecha.



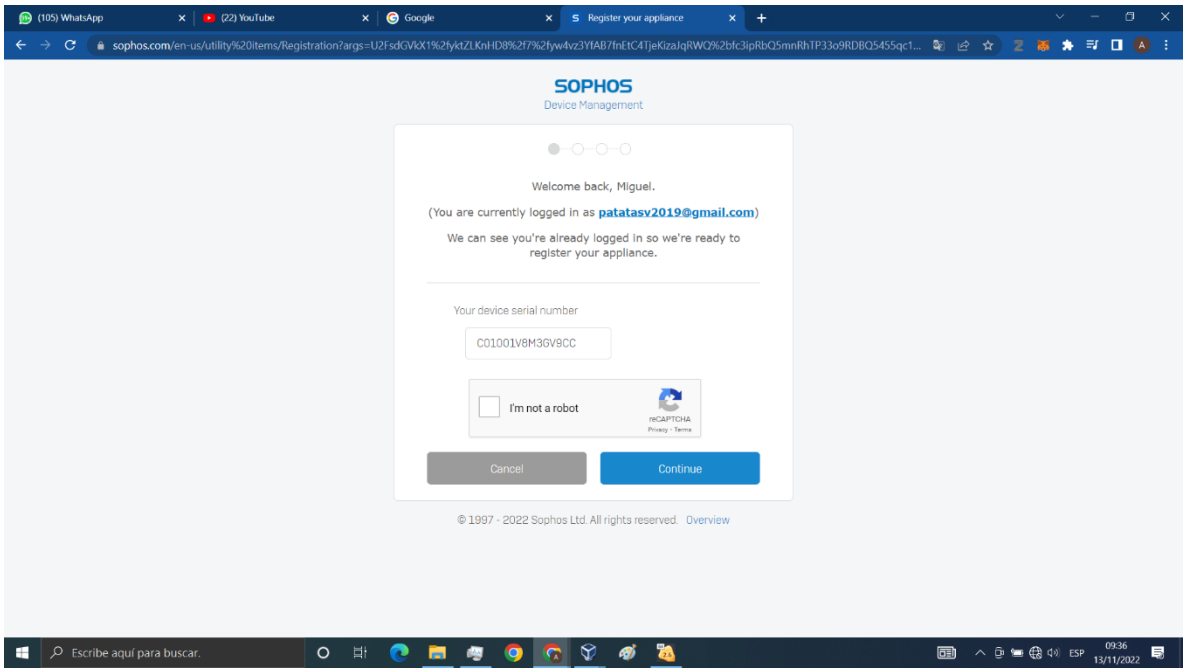
En esta ventana pide que introducimos el código de la licencia, este se manda cuando se registra por primera vez al descargar el software al correo que se introdujo en el formulario. Al colocar el código dar clic en siguiente.



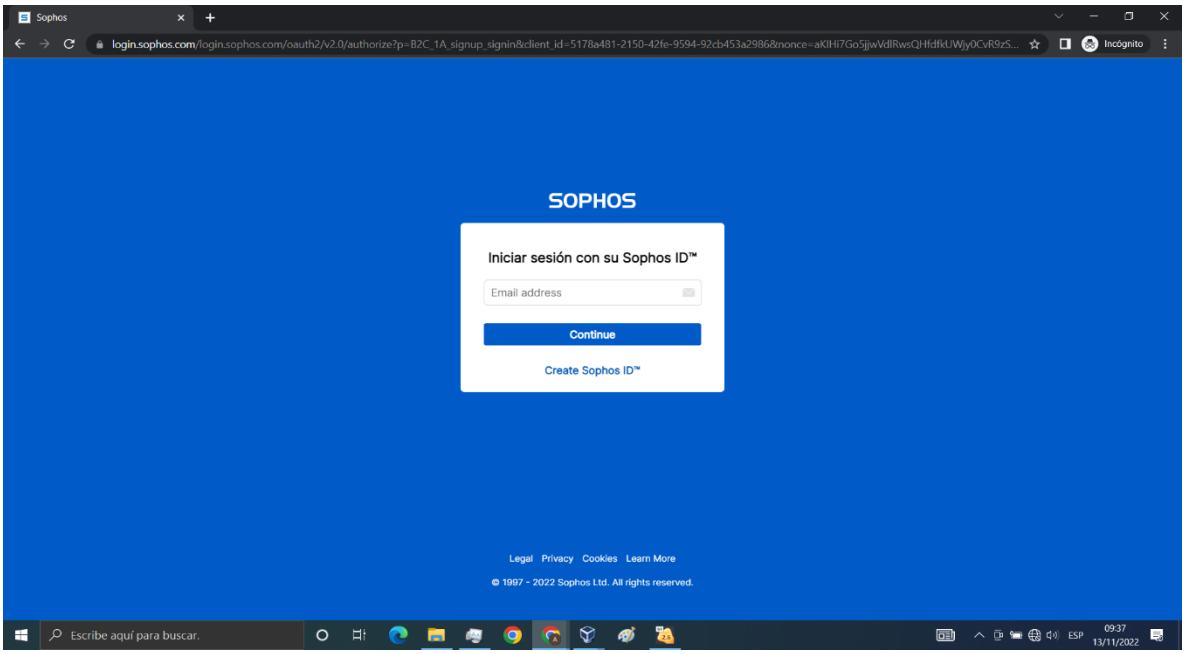
Nos pide un id tenemos que crear uno le damos en crear id dar clic en el botón crear id.



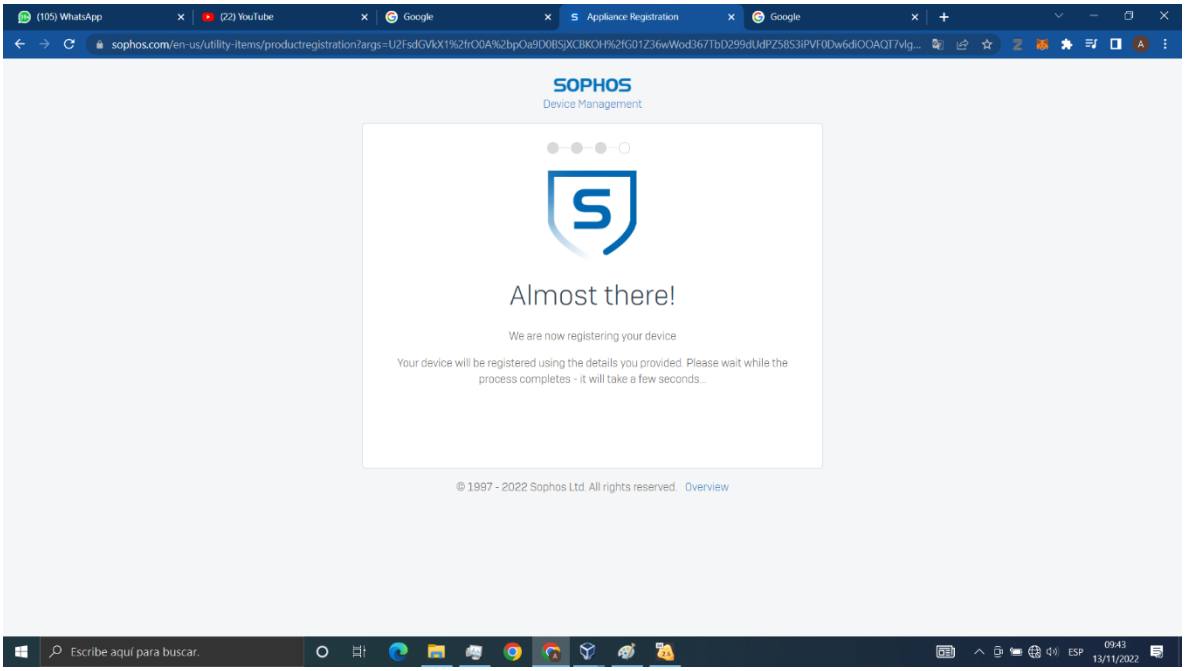
Nos aparece la siguiente ventana en donde nos pide que resolvamos el captcha y dar clic en el botón continuar.



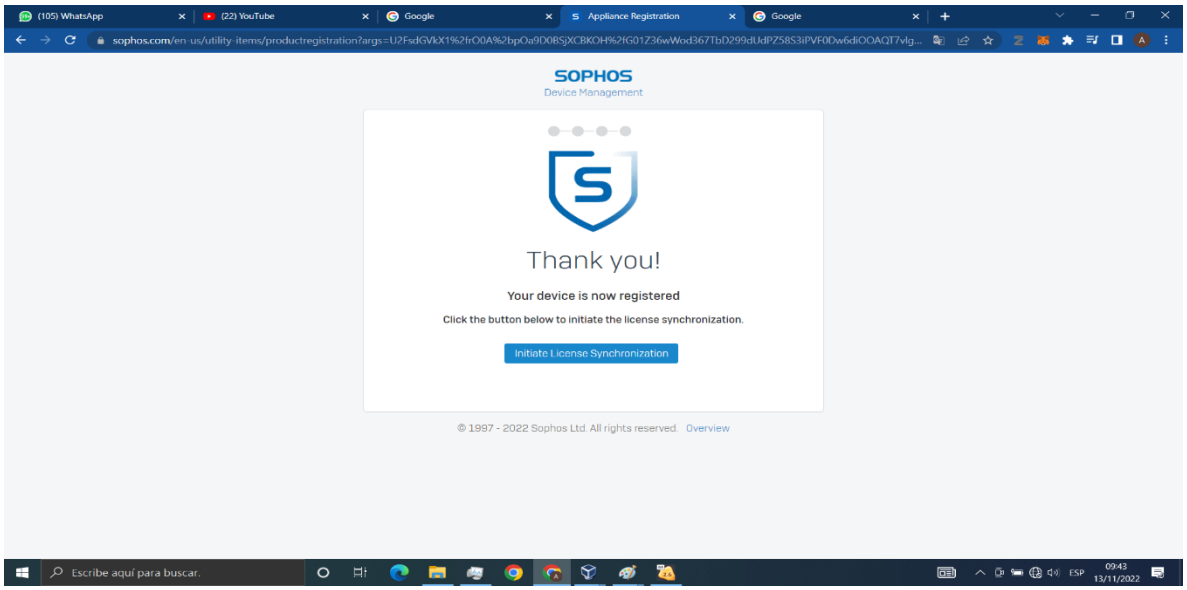
Aparece la siguiente ventana, dar clic en continuar.



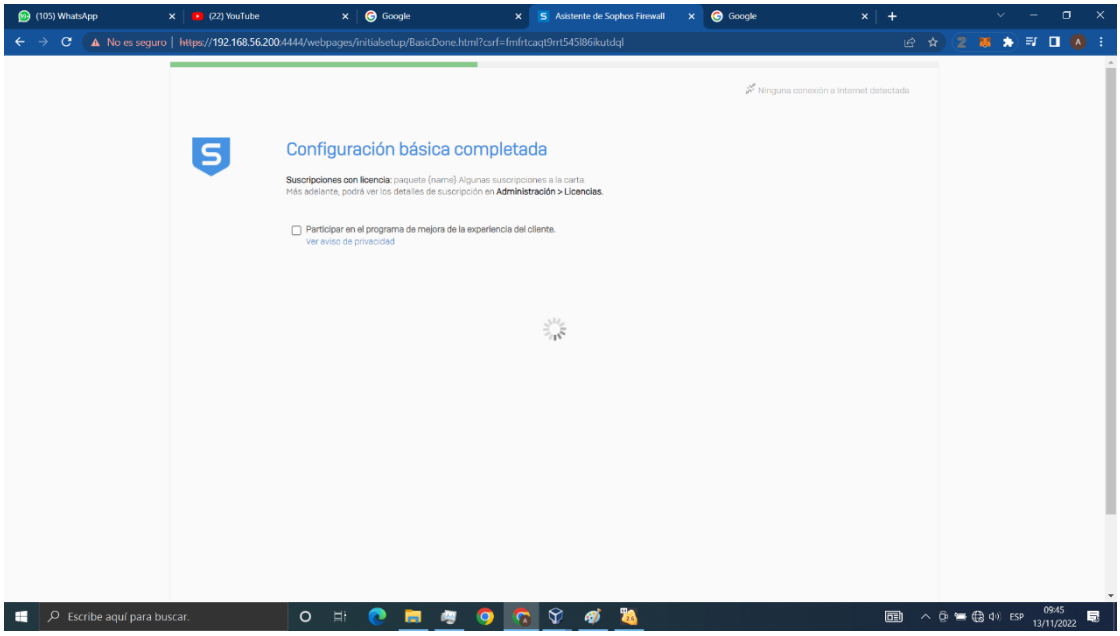
Aparecen ventanas de información del Sophos.



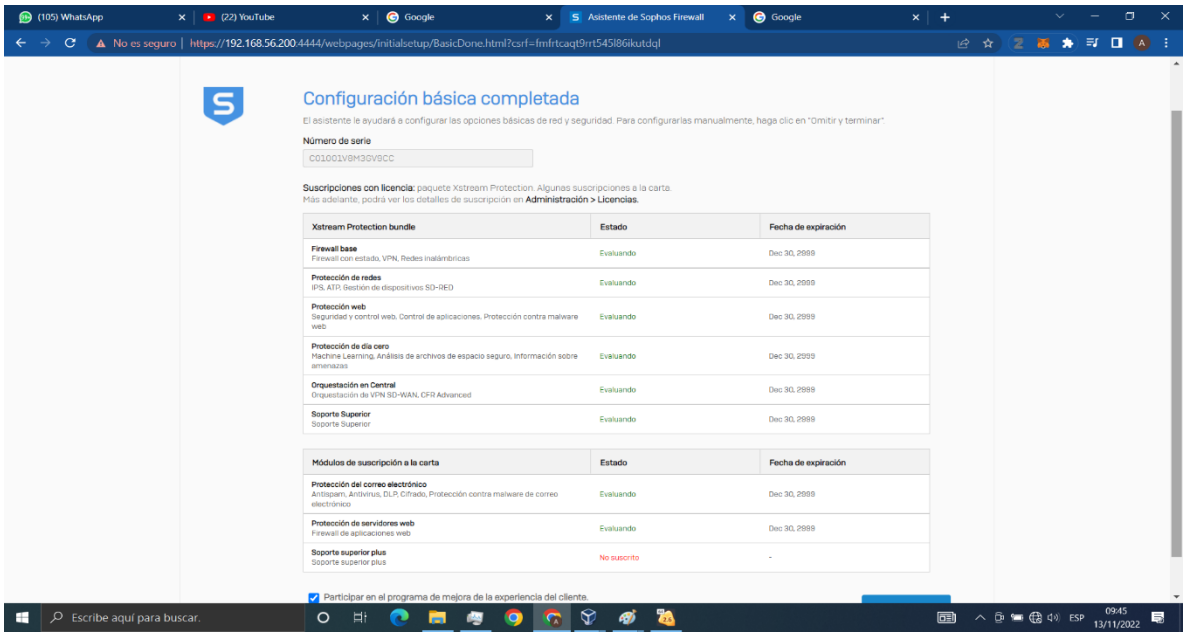
Le damos clic en iniciar sincronización de licencia.



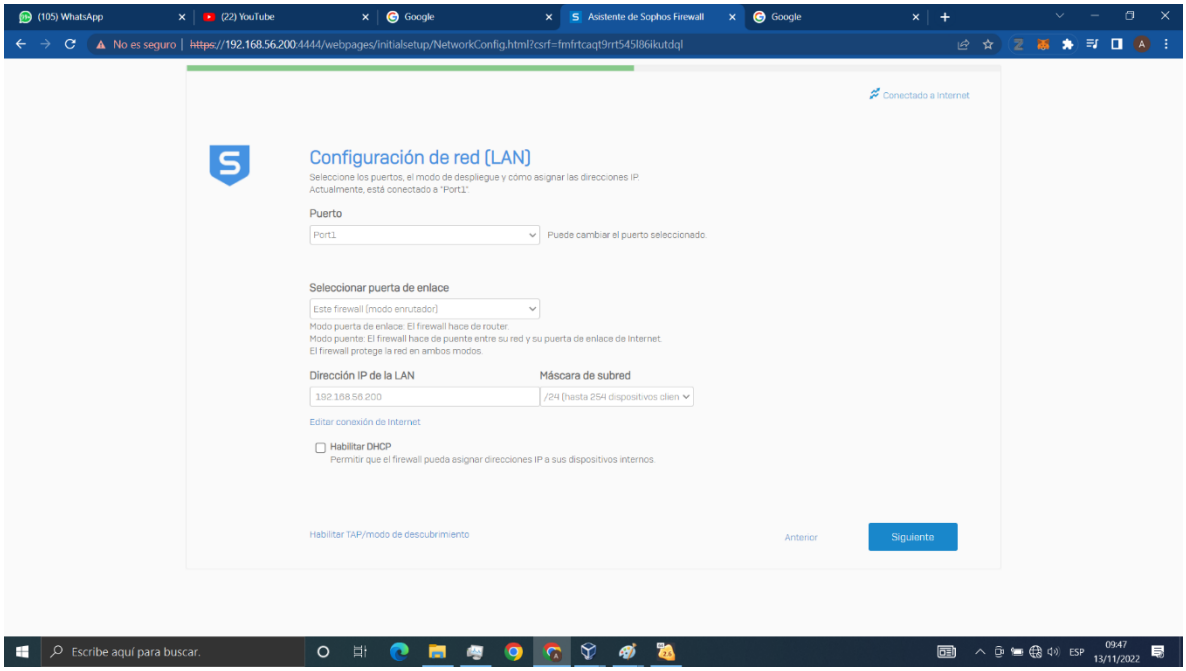
Aparece la siguiente información la configuración básica completada.



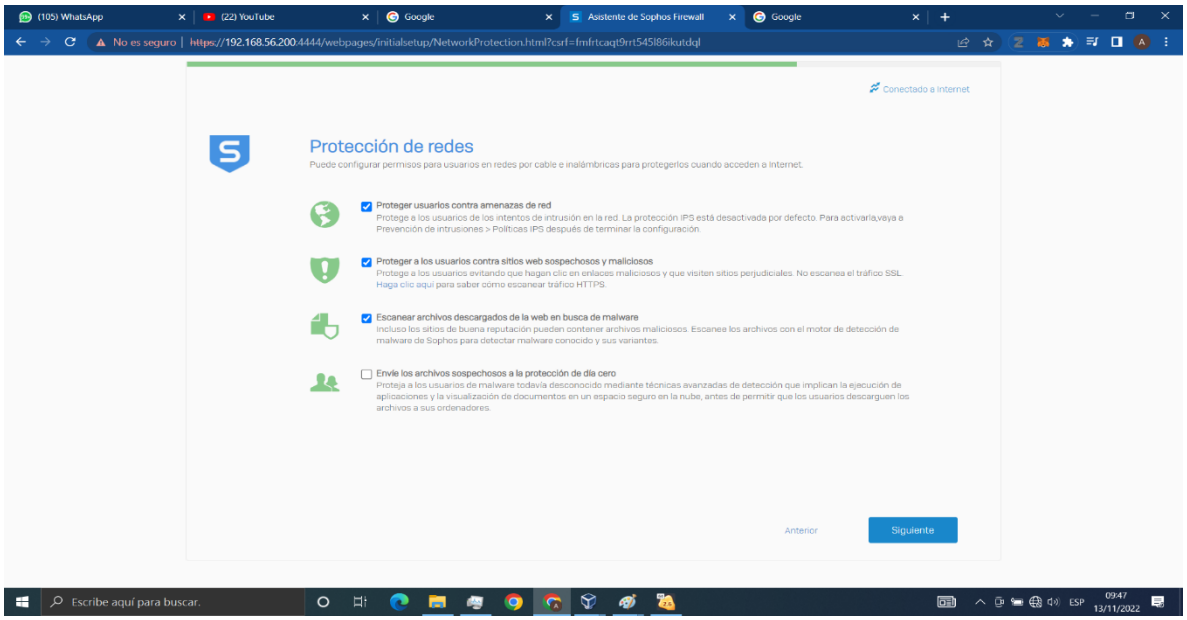
Siguiente imagen de configuraciones básicas, dar clic en siguiente.



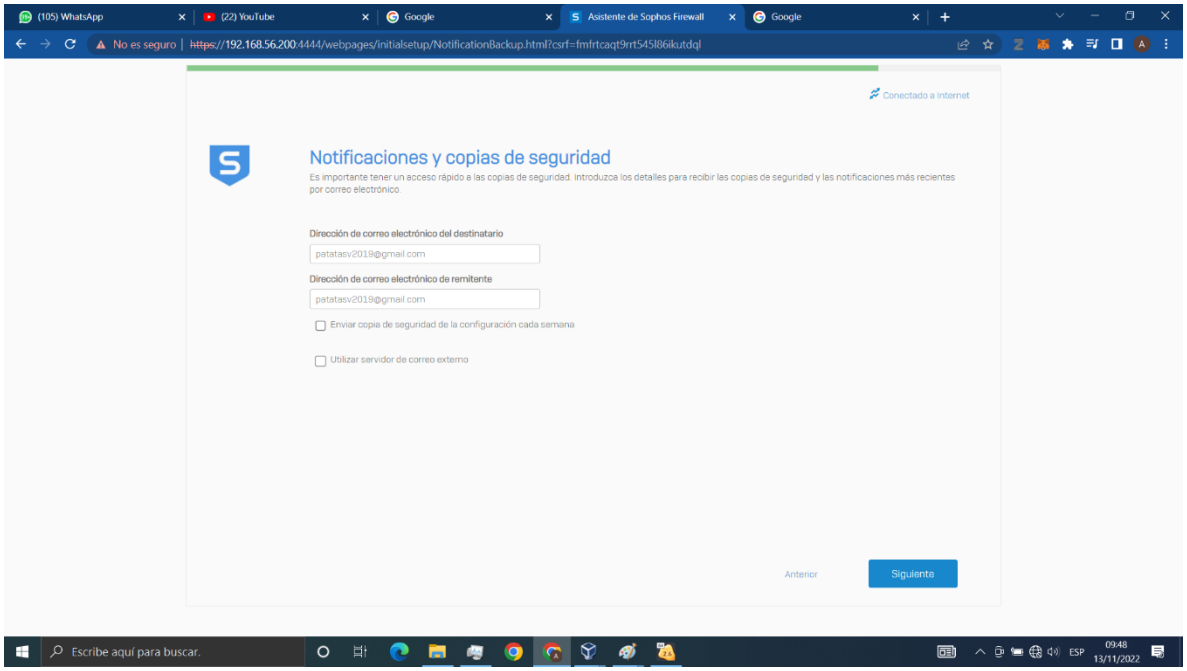
Configuraciones de la red realizadas, dar clic en siguiente.



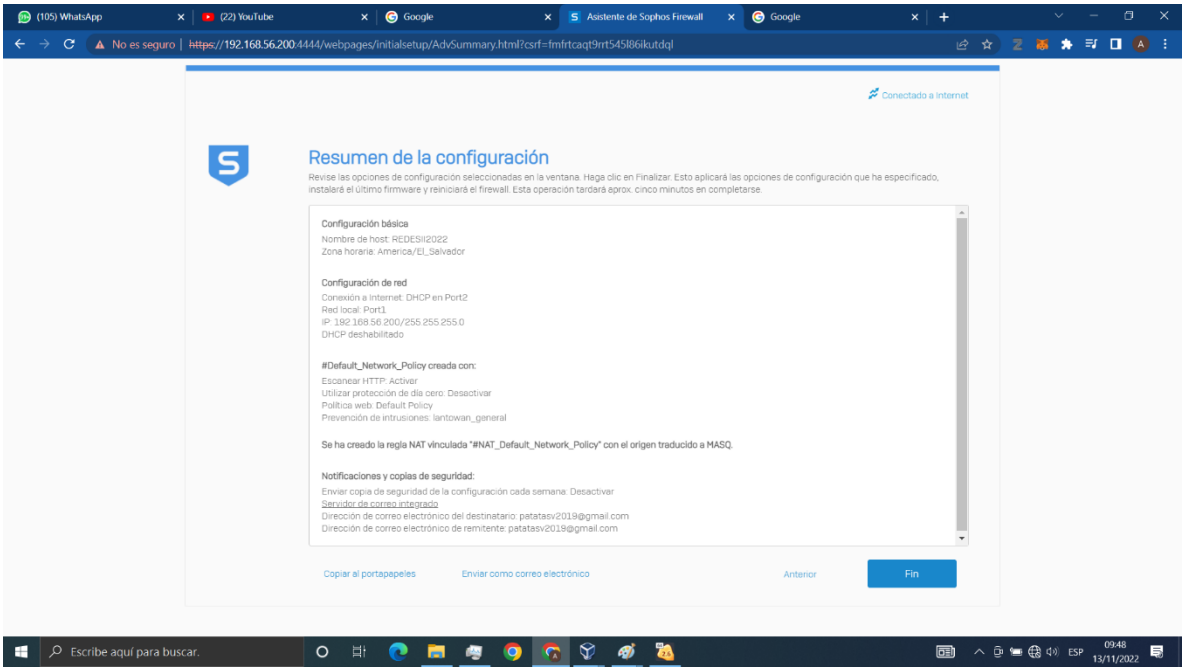
Siguiente imagen seleccionar las primeras tres opciones, dar clic en siguiente.



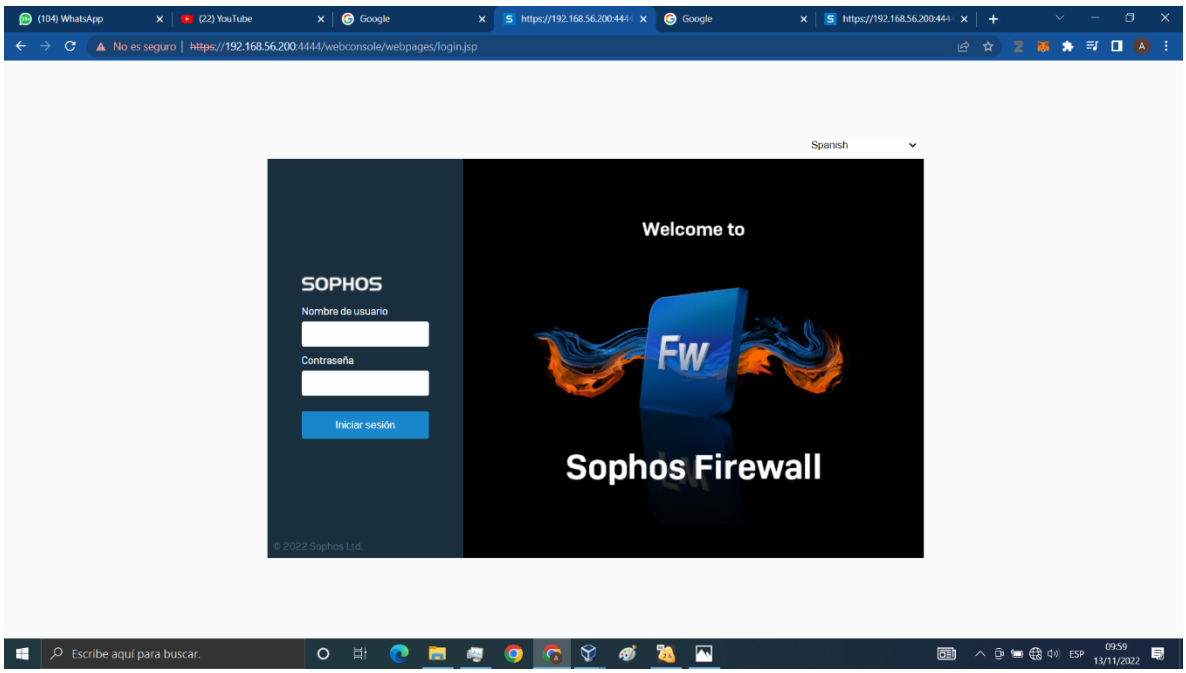
Siguiente ventana de configuraciones para recibir notificaciones del software, dar clic en siguiente.



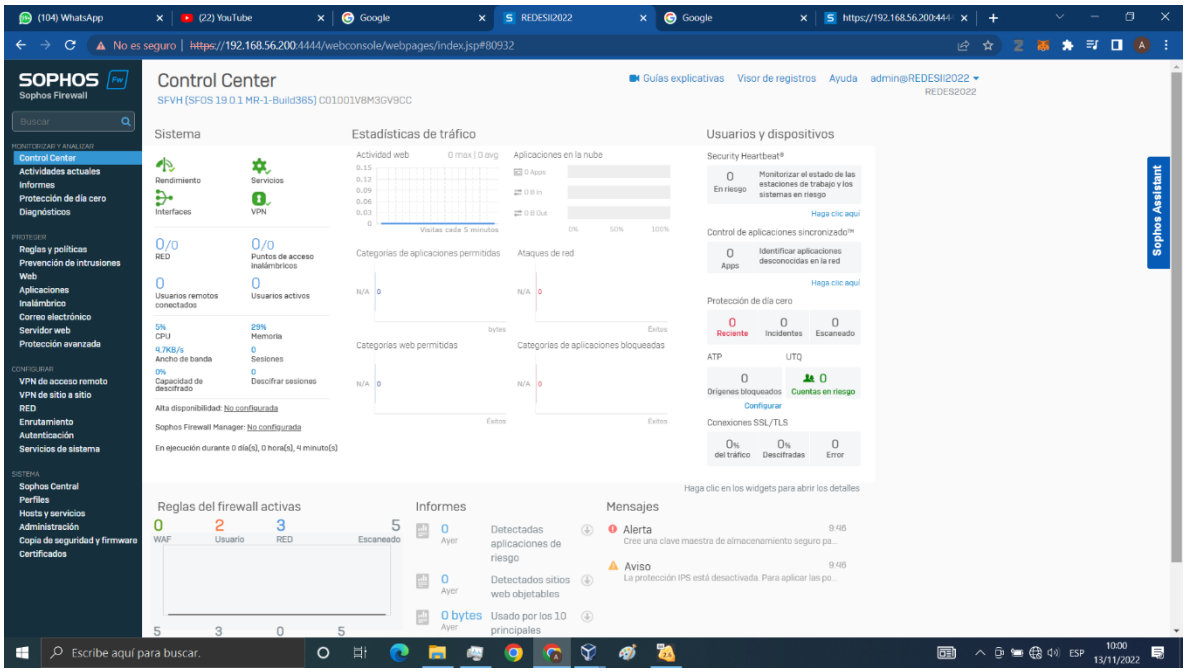
Resumen de las configuraciones, dar clic en botón de fin.



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

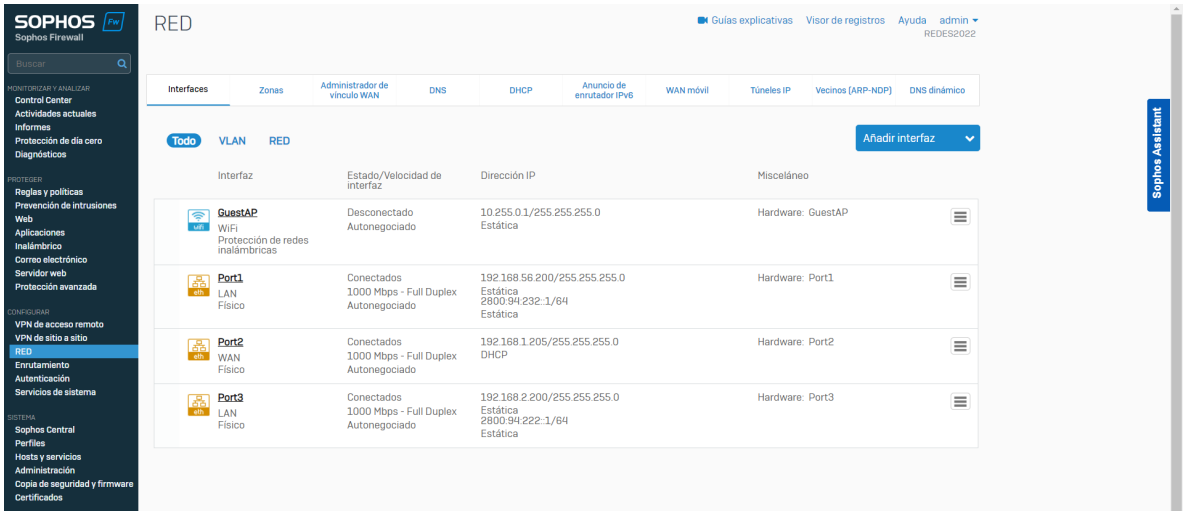


Este es el panel del o dashboard de sophos XG



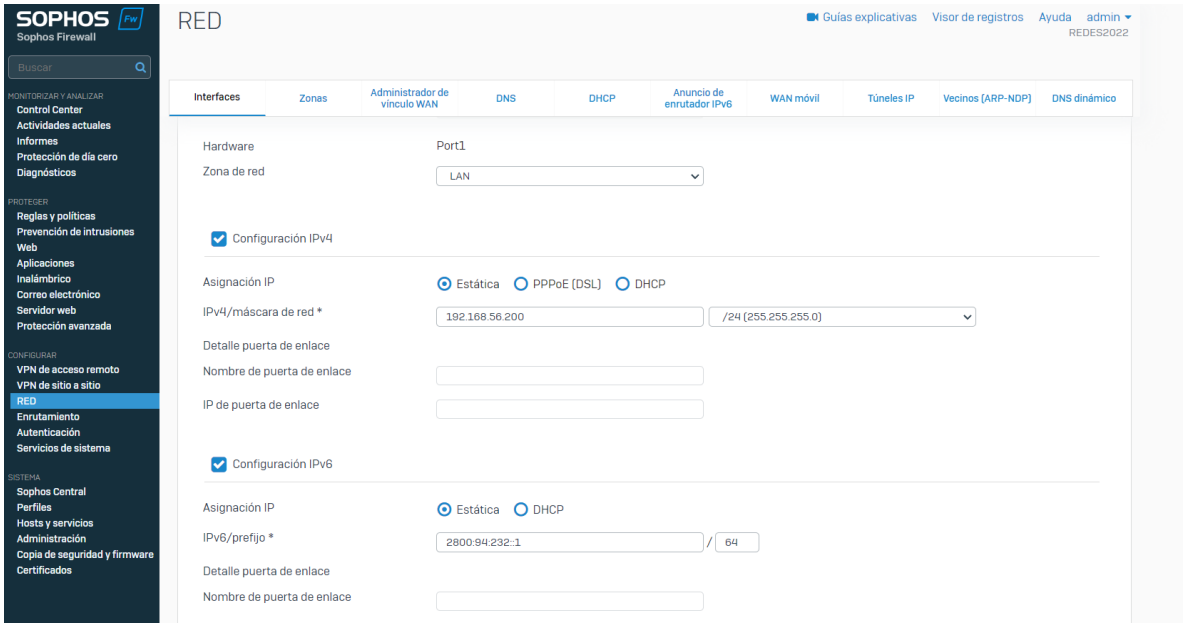
Configuración de red IPV4 e IPV6 y políticas con reglas.

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 obtendra su IP para salida del internet y esta sera WAN.

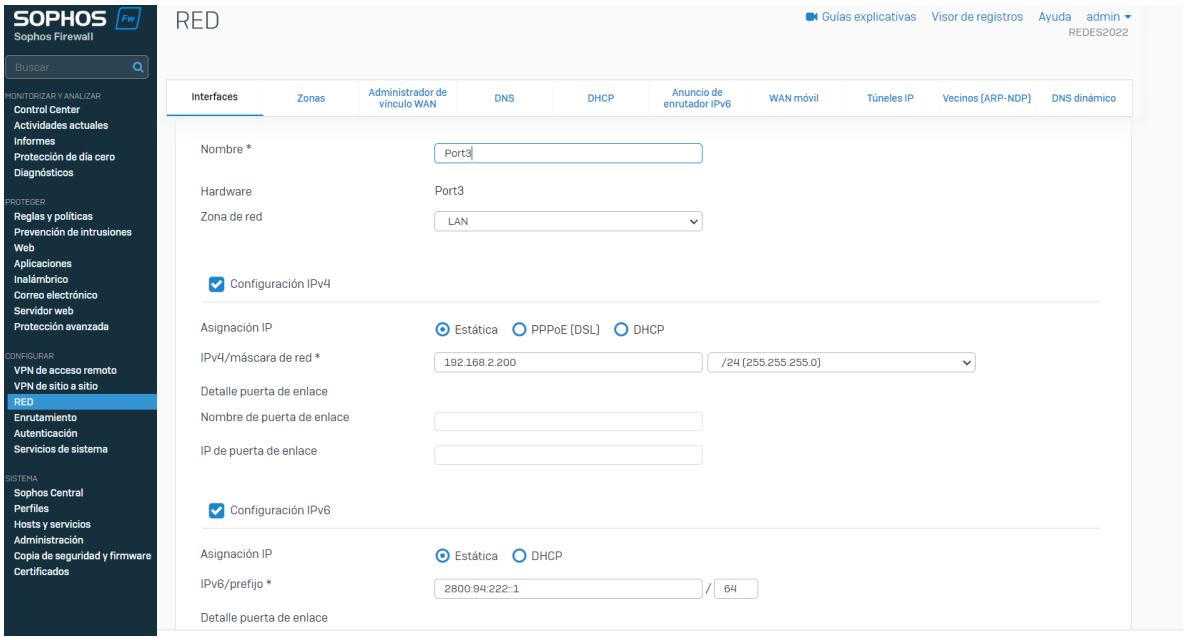


En los puertos se deben asignar sus redes correspondientes para que se reconozcan como gateways para el modo DHCP de las IPV4.

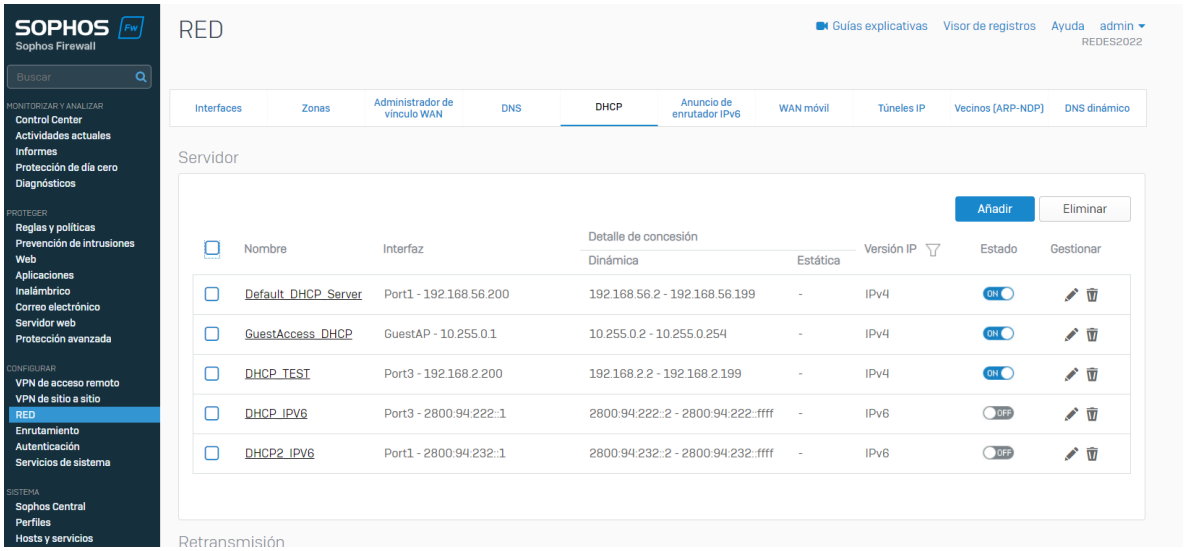
Puerto 1



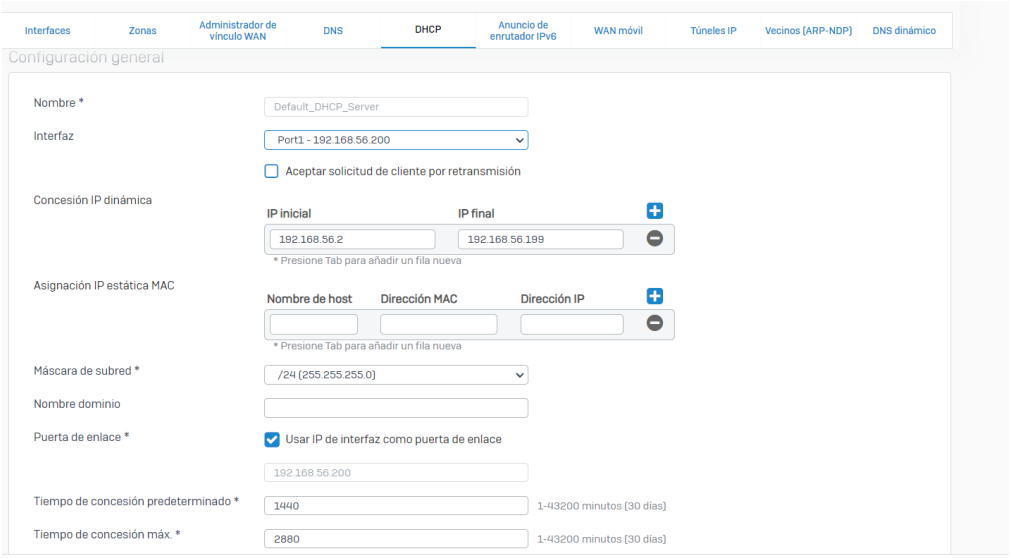
Puerto 3

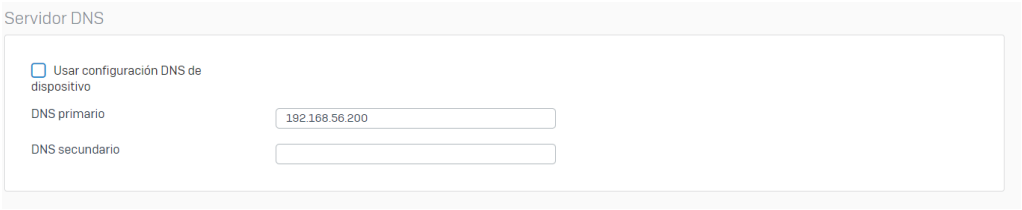


En la misma sección de RED ahora se configura el modo DHCP para los puertos 1 y 3, en lo cuales serán para las IPV4.

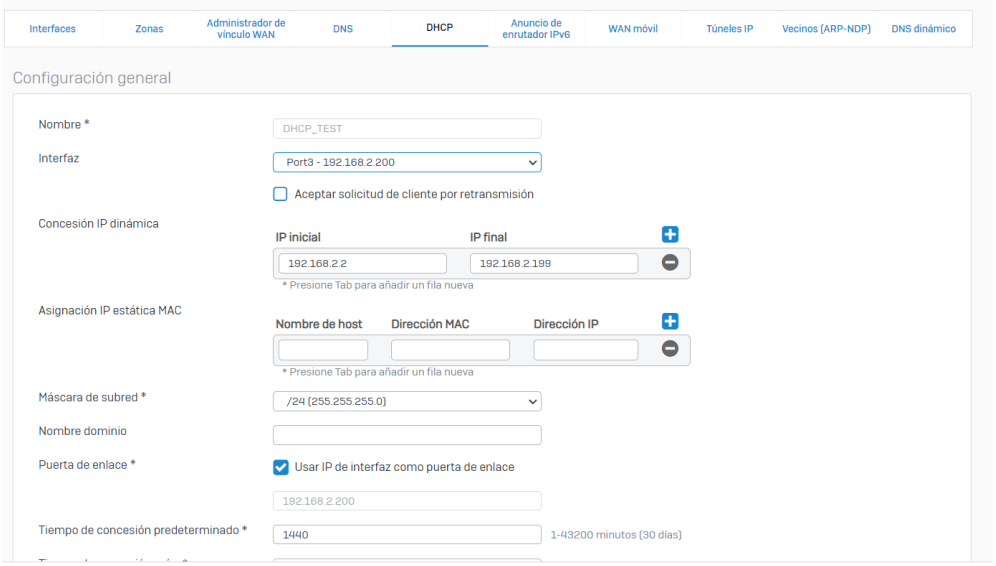


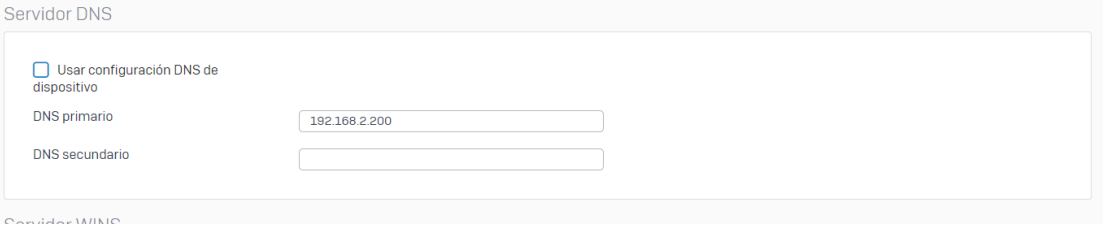
Puerto 1



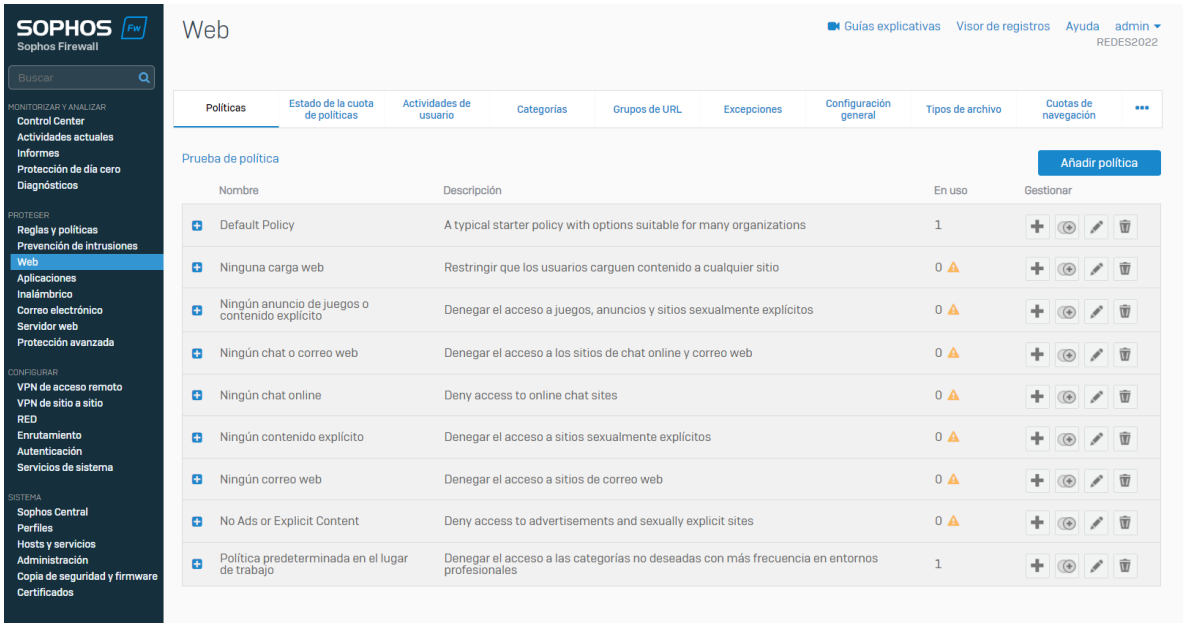


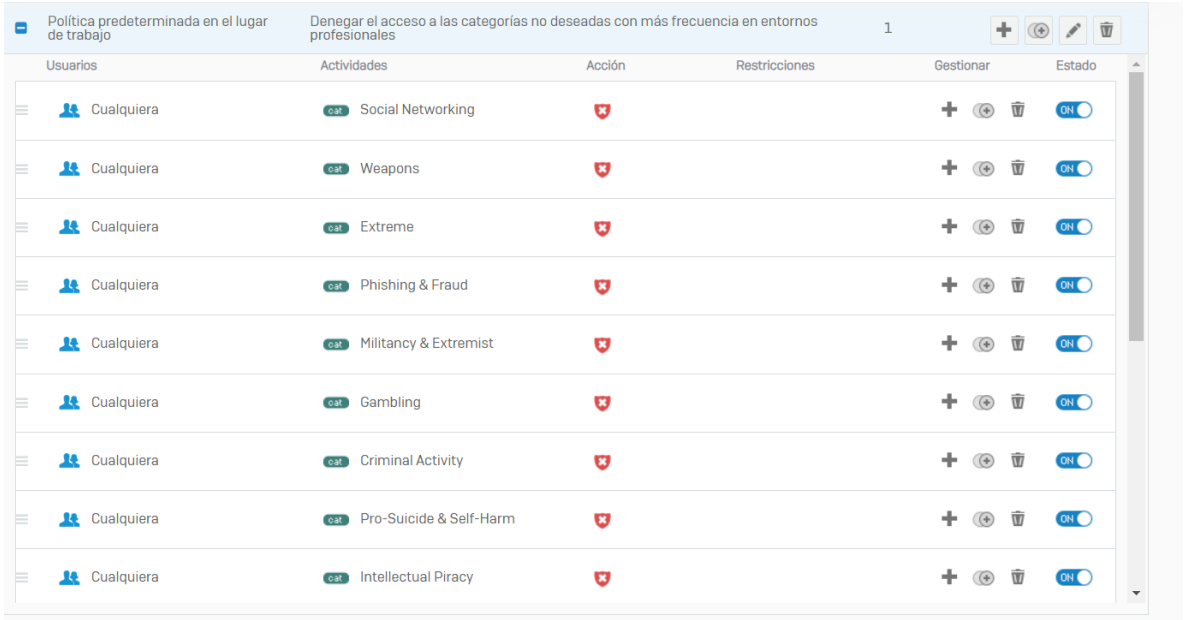
Puerto 3





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.

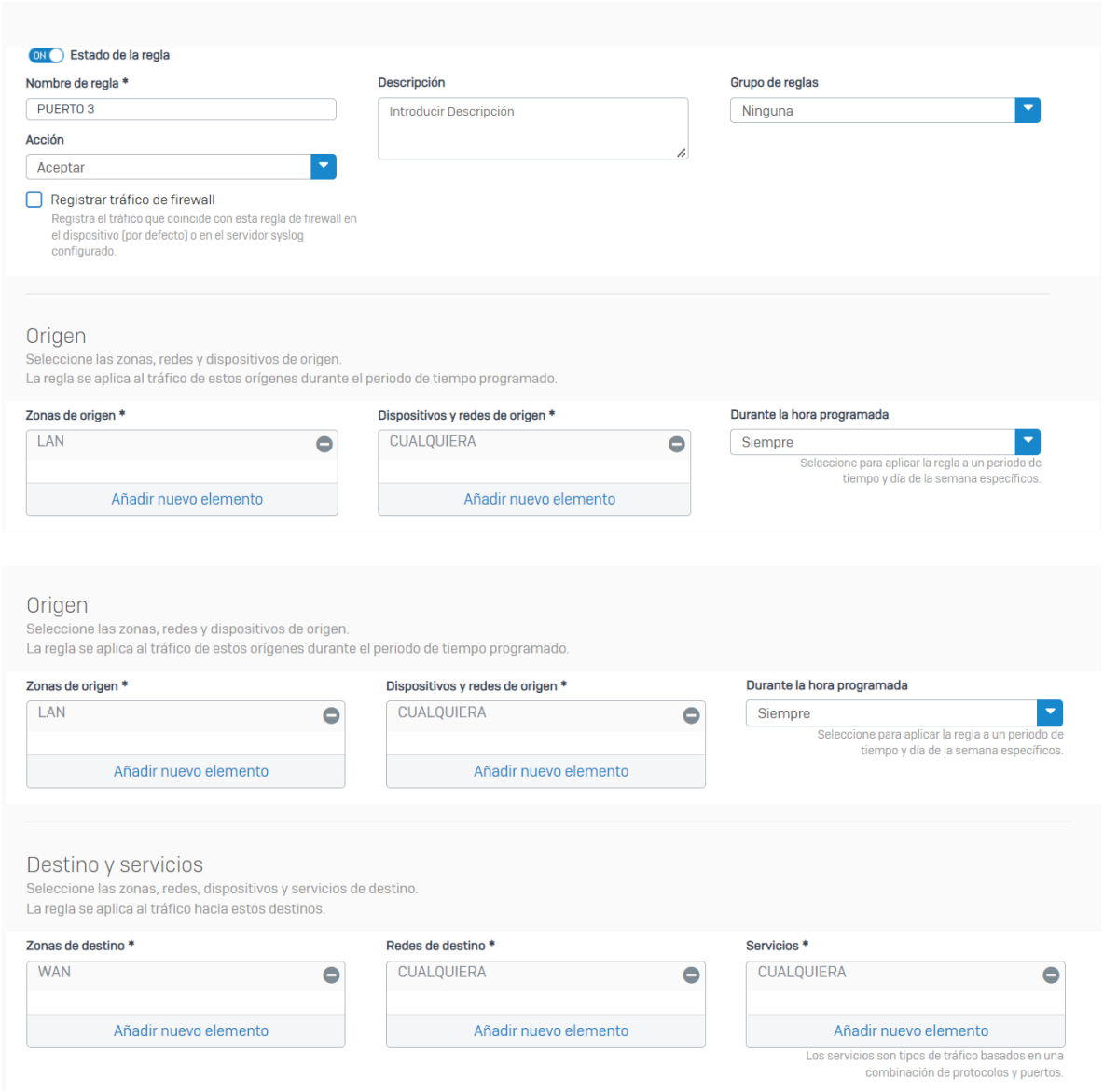




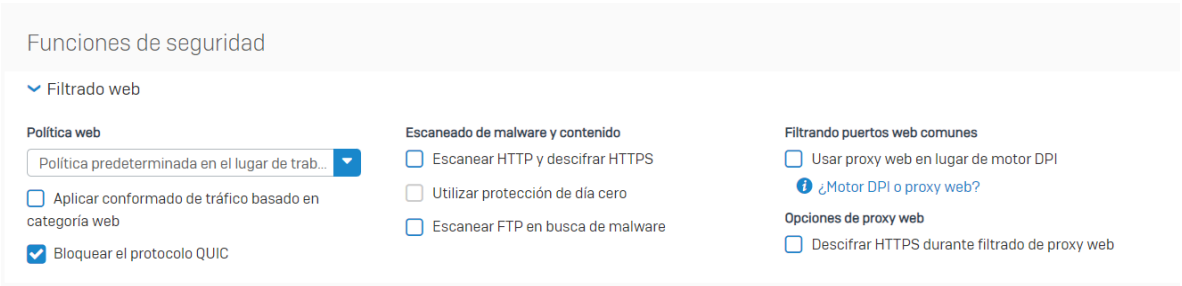
Estas son las actividades bloqueadas para un área de trabajo.

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



Uso de la política

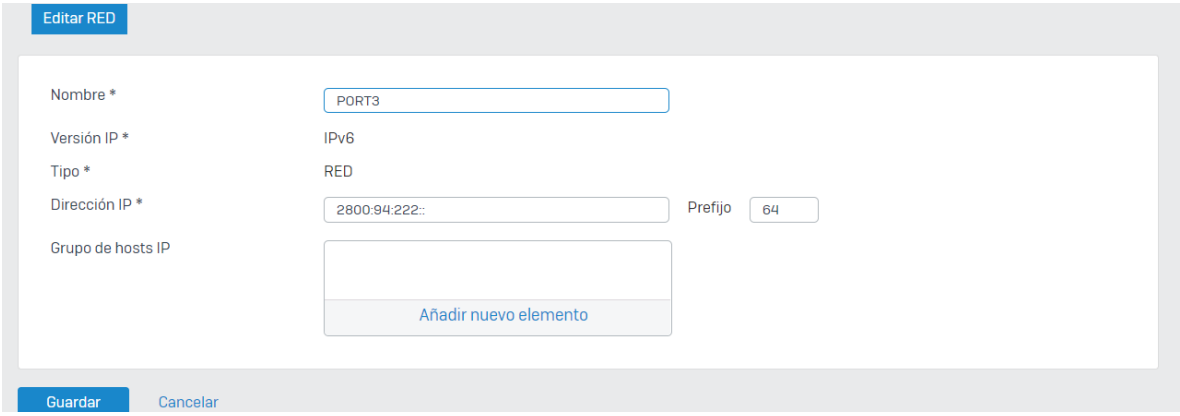


Regla IPV6

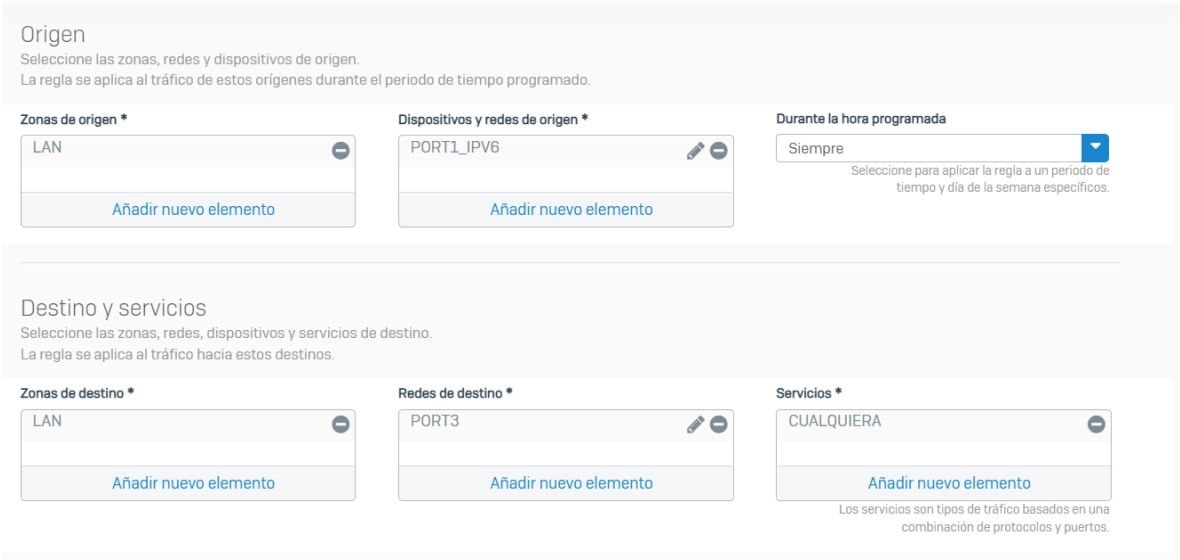
Para el caso de las reglas IPV6 como es ruteo estático se deben asignar dos políticas para que puedan acceder de una red a otra.

RED IPV6 del puerto 1

RED IPV6 puerto 3



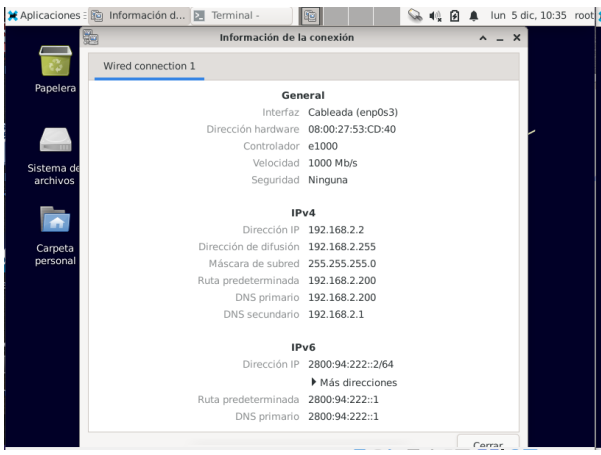
De la siguiente manera se pueden comunicar las redes, en este caso es para que el puerto 1 pueda acceder la red del puerto 3 y lo mismo se debe hacer para que el puerto 3 conozca como llegar a la red del puerto 1.



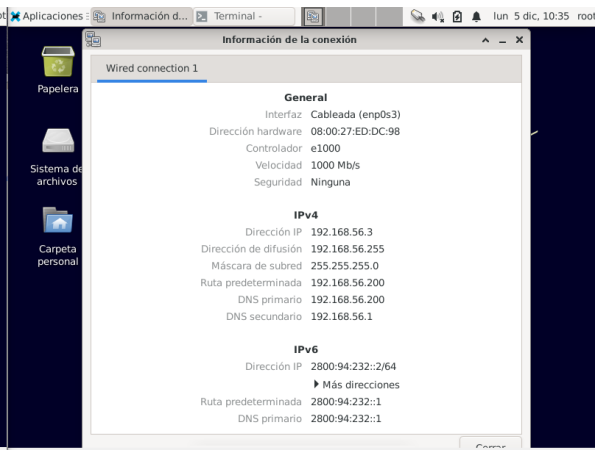
Pruebas de testeo del firewall.

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.

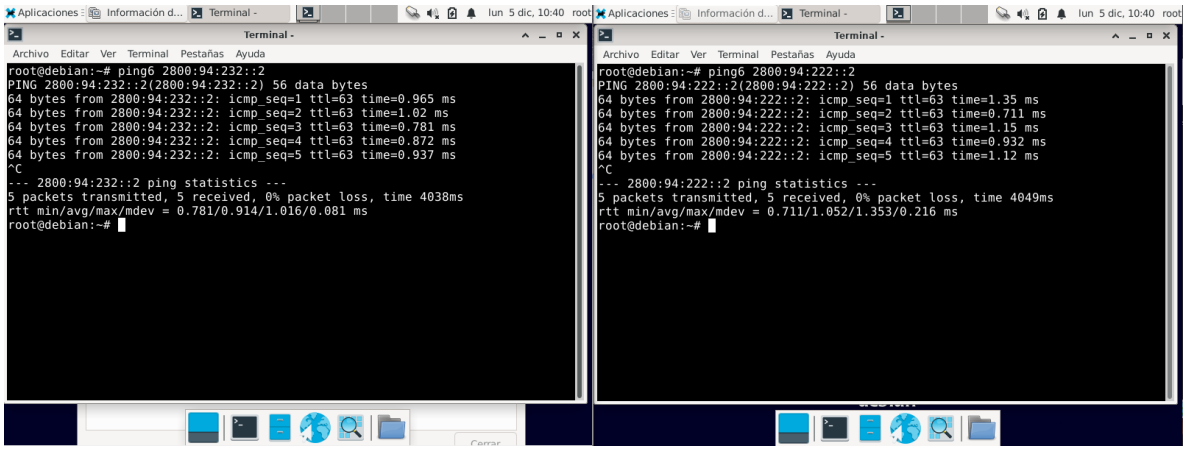
PC1



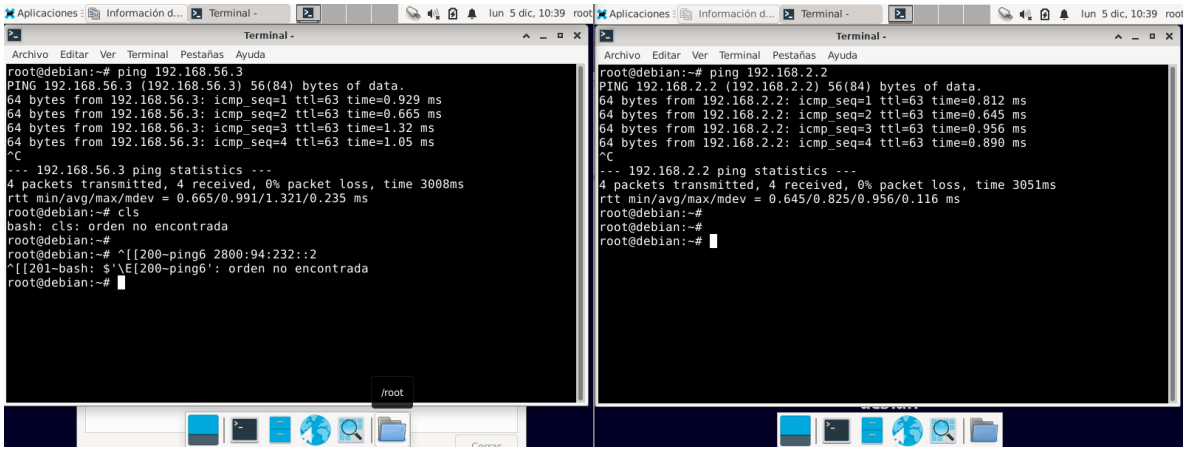
PC2



Pruebas de ping IPV4 en ambos equipos.



Pruebas de ping IPV6 en ambos equipos.



Verificación del uso de la política de trabajo.