

CURSO ONLINE DE CIBERSEGURIDAD

Especialidad Administración de
Sistemas de Ciberseguridad

Taller 1

Unidad 4. Administración de
sistemas de ciberseguridad



GOBIERNO
DE ESPAÑA
VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD



Contenidos

- | | | |
|---|---------------------------------------|----|
| 1 | SEGREGACIÓN DE REDES CON GNS3 | 4 |
| 2 | INSTALACIÓN Y CONFIGURACIÓN DE VMWARE | 6 |
| 3 | INSTALACIÓN Y CONFIGURACIÓN DE GNS3 | 15 |
| 4 | PRÁCTICA: HOST CON ACCESO A INTERNET | 77 |

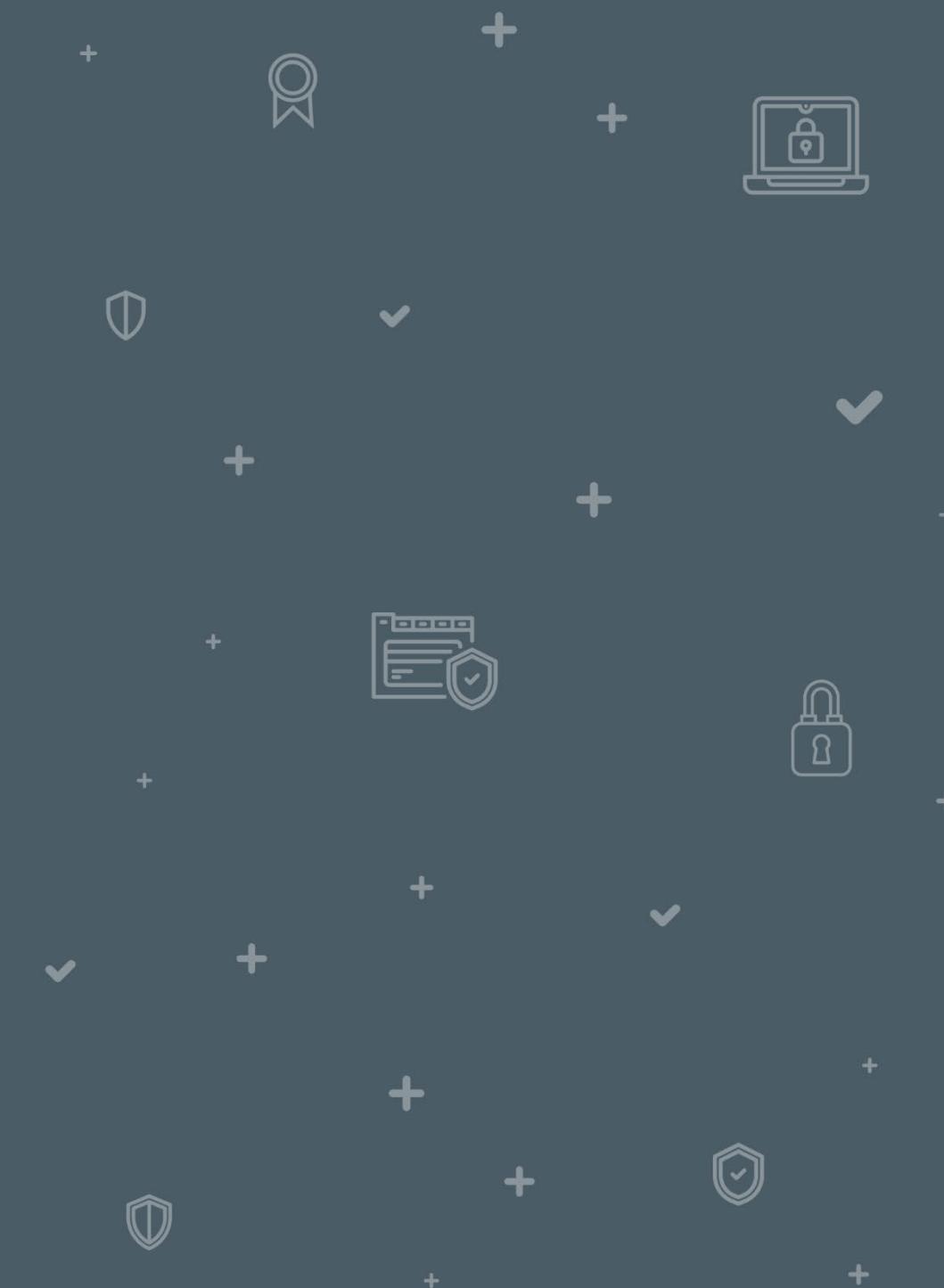
Contenidos

- 5 PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCS (ELEMENTO VPCs)** 122
- 6 PRÁCTICA: SEGMENTACIÓN EN VLANs** 151
- 7 PRÁCTICA: TOPOLOGÍA DE RED CON FW** 199

Duración total del taller: 6 horas.

SEGREGACIÓN DE REDES CON GNS3

1

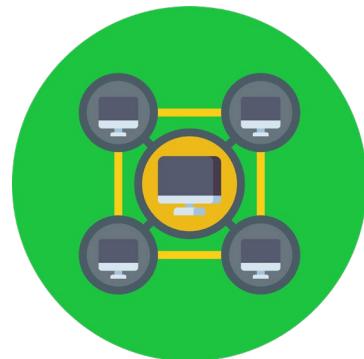


1

SEGREGACIÓN DE REDES CON GNS3

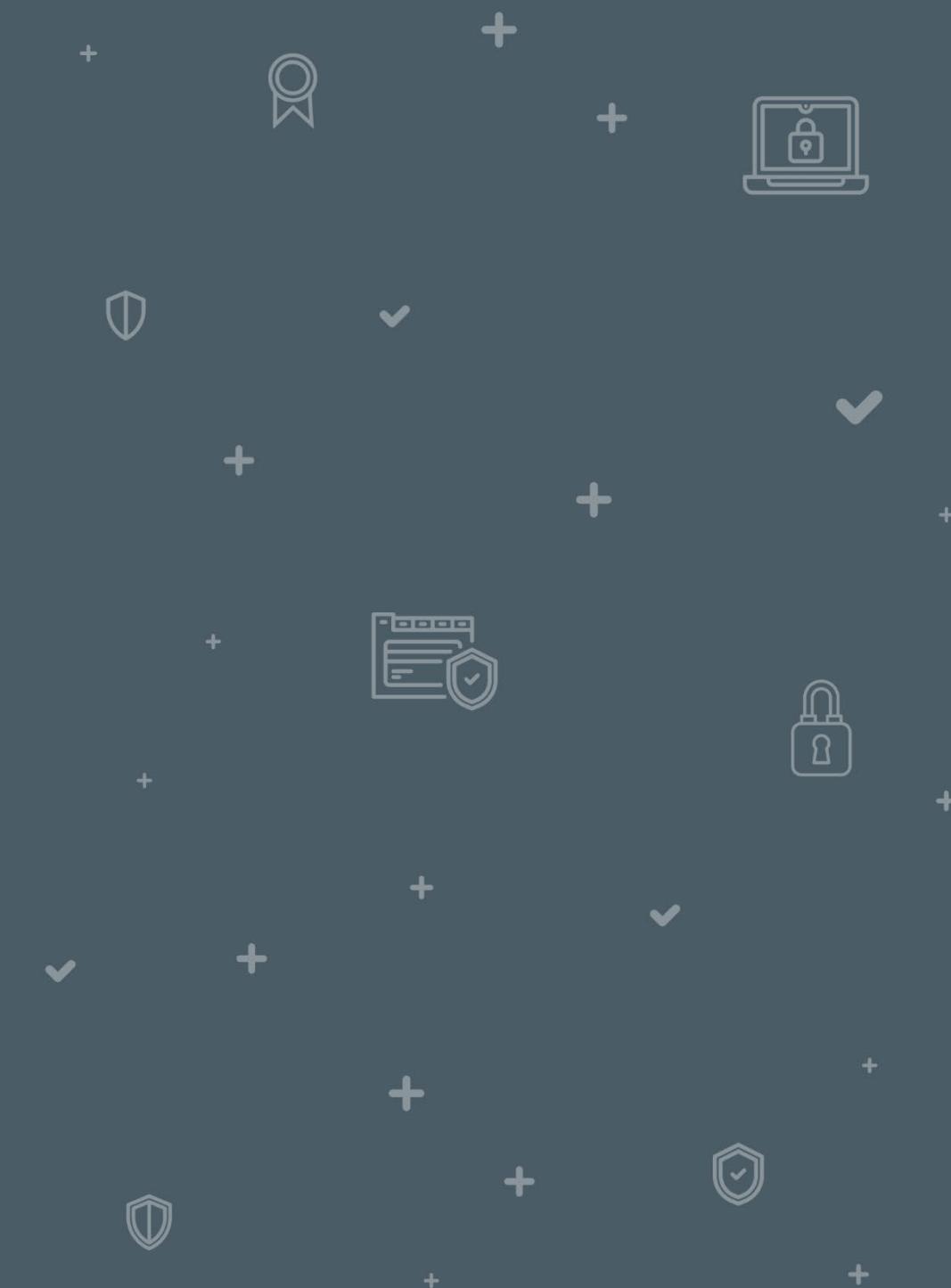
En esta práctica, aprenderás a realizar una segregación de red adecuada a través del uso de GNS3, un simulador gráfico de red que permite diseñar diferentes topologías de red complejas y poner en marcha simulaciones sobre ellas.

Esta herramienta se compone de dos entornos, primero la máquina virtual que será el servidor al que nos conectemos después desde el entorno gráfico de la propia herramienta.



INSTALACIÓN Y CONFIGURACIÓN DE VMWARE

2





2 INSTALACIÓN Y CONFIGURACIÓN DE VMWARE

Para esta práctica vamos a emplear VMWare. VMWare es similar a VirtualBox, con el que ya has trabajado. Estos programas se llaman **hipervisores o monitores de máquinas virtuales** y sirven para simular de forma virtual ser un ordenador, es decir, simular el *hardware*. También tienen, como ventaja, que se pueden ejecutar varios sistemas operativos en él.

El primer paso será instalar VMWare, por lo que, descárgalo desde este [enlace](#).

2

INSTALACIÓN Y CONFIGURACIÓN DE VMWARE

- Lo primero que debes hacer es elegir el sistema operativo de tu equipo. En nuestro caso Windows.

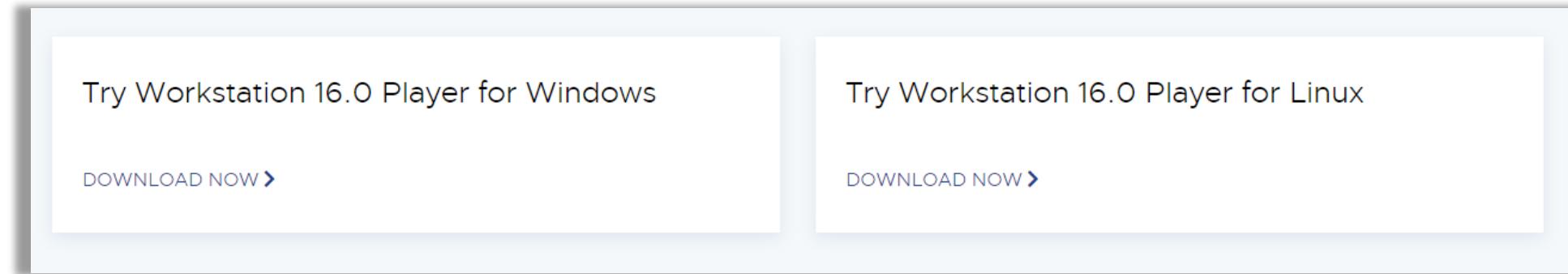


Ilustración 1: Elige el sistema operativo a utilizar.

2

INSTALACIÓN Y CONFIGURACIÓN DE VMWARE

- Una vez completada la descarga haz doble clic en el archivo .exe descargado. Aparecerá una ventana emergente en la que deberás hacer clic en «Next».

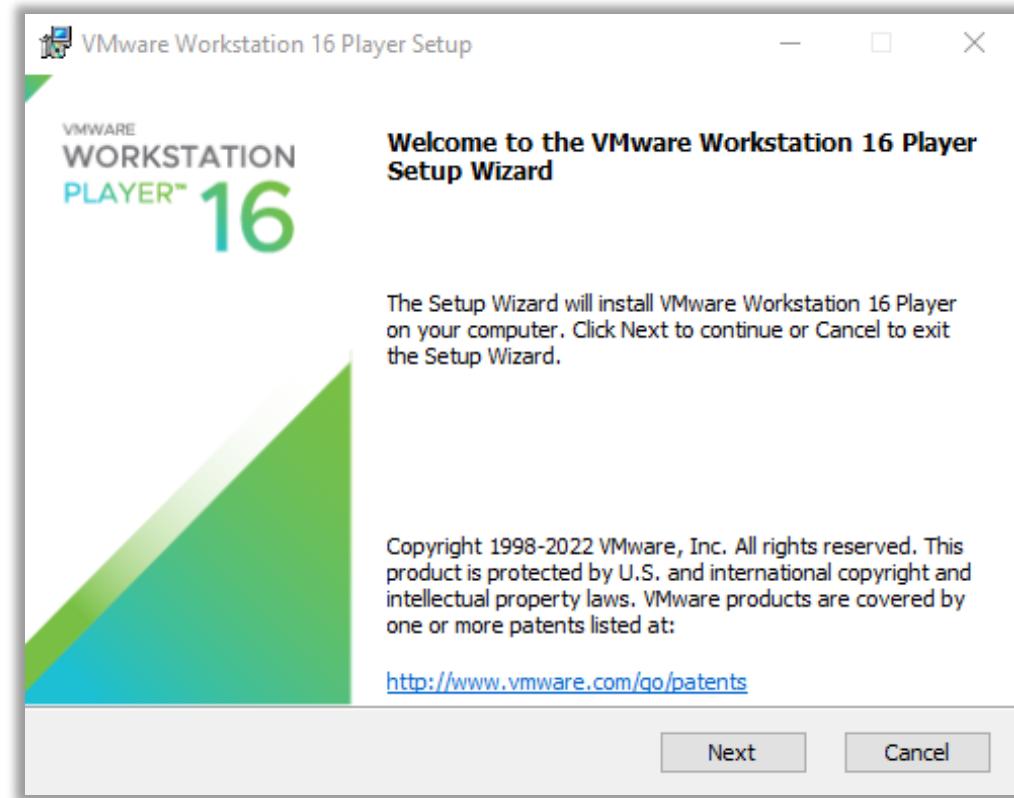


Ilustración 2: Ventana emergente de bienvenida a VMware Workstation 16 Player.

2

INSTALACIÓN Y CONFIGURACIÓN DE VMWARE

- El siguiente paso es aceptar los términos y condiciones y volver a hacer clic en «Next».

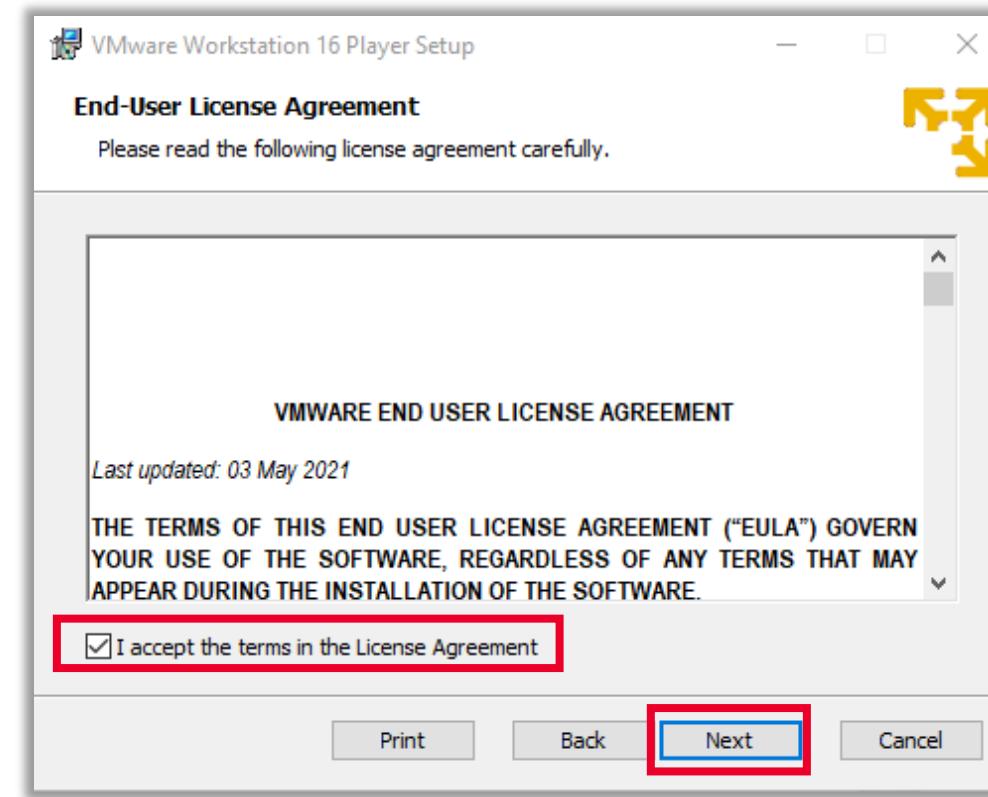


Ilustración 3: Acepta los términos y condiciones.

2

INSTALACIÓN Y CONFIGURACIÓN DE VMWARE

- Una vez aceptados los términos y condiciones nos dará a elegir la ubicación para guardar el programa. Como por defecto se almacenará en la ruta de «Archivos de programa», donde se suelen almacenar los programas, puedes, perfectamente, dar por válida esa ruta de almacenamiento, por lo que pulsa «Next».

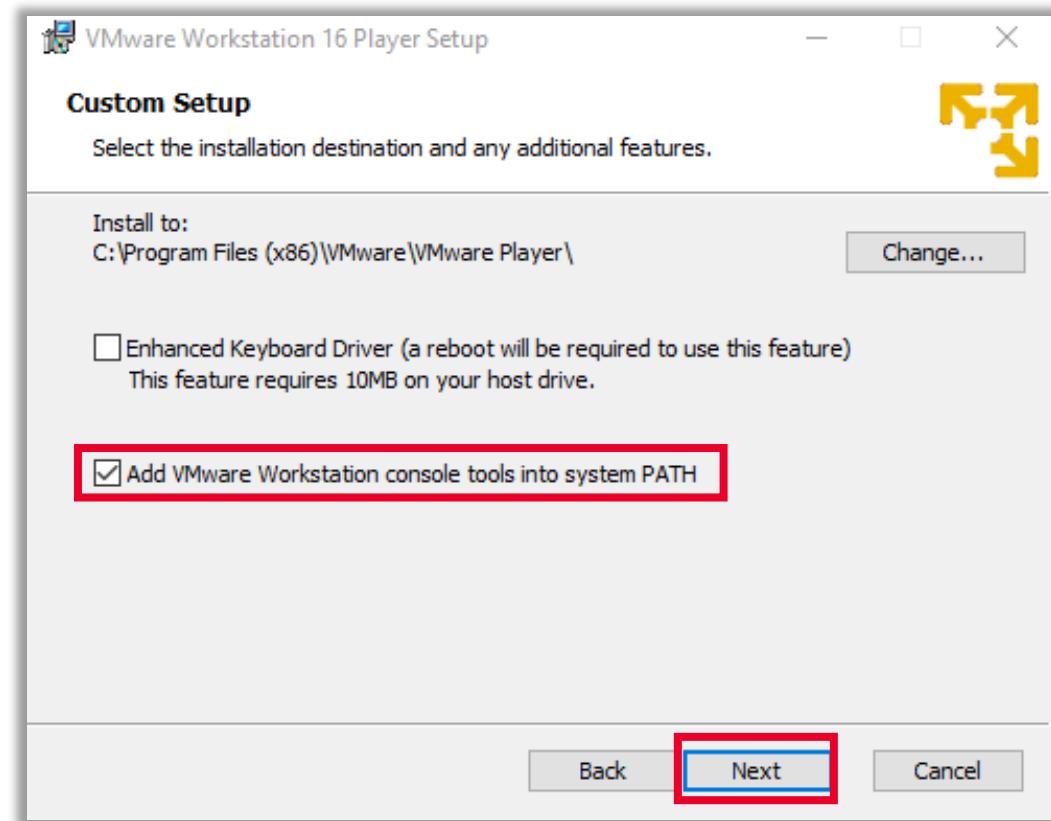


Ilustración 4: Selecciona la ubicación de instalación.

2

INSTALACIÓN Y CONFIGURACIÓN DE VMWARE

- Ahora, aparecerá una serie de opciones marcadas por defecto que mantendremos de esa forma y pulsa «Next».

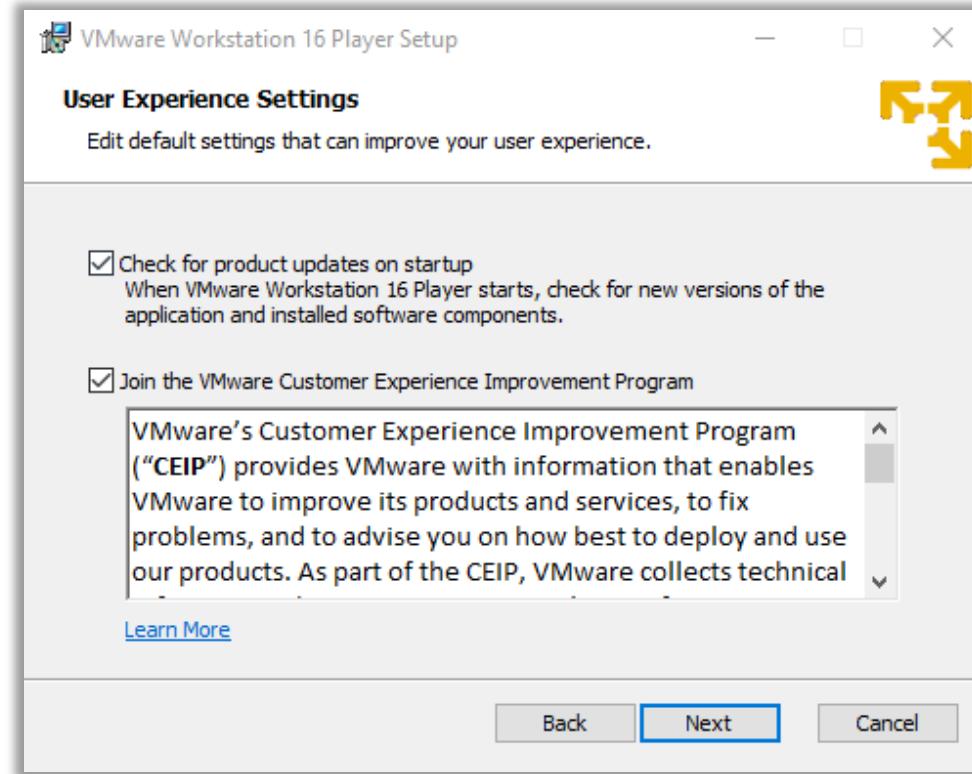


Ilustración 5: Edita la configuración predeterminada que pueda mejorar su experiencia.

2

INSTALACIÓN Y CONFIGURACIÓN DE VMWARE

- A continuación, da la opción de crear unos atajos de programa, es decir, la creación de unos iconos en la carpeta de programas de menú de inicio y en el escritorio para que resulte más cómodo encontrar este programa y pulsar para ejecutarlo. Puedes marcar las que prefieras, o ninguna. Nosotros vamos a mantener ambas opciones marcadas.

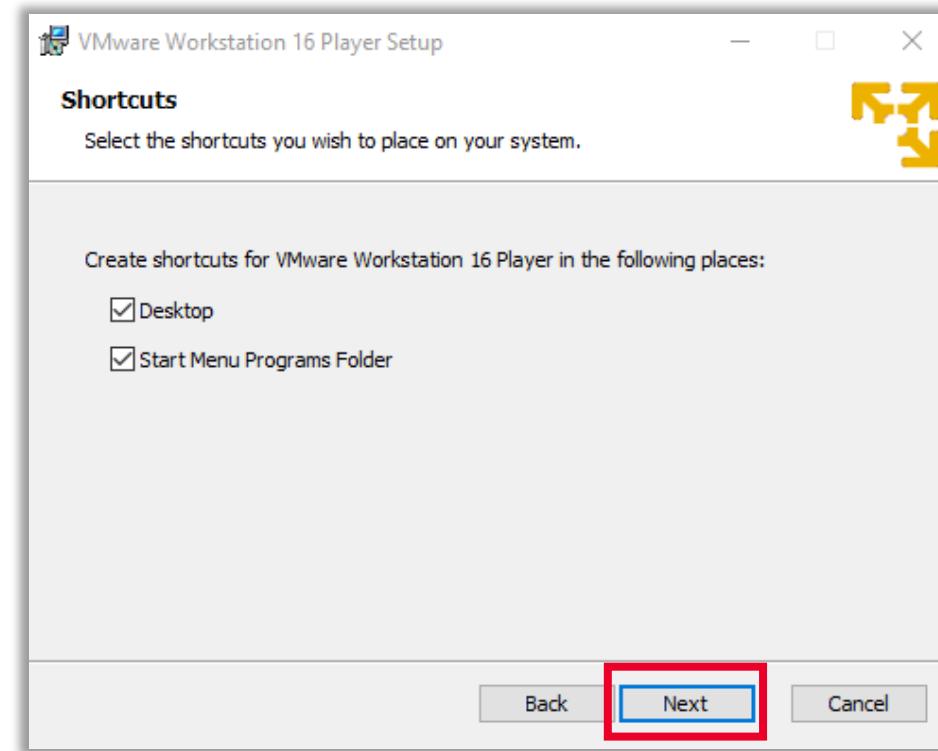


Ilustración 6: Selecciona los accesos directos que desea colocar en su sistema.

2

INSTALACIÓN Y CONFIGURACIÓN DE VMWARE

- Haz clic en «*Install*» y comenzará el proceso de instalación. Una vez completado ya tendrás disponible el programa VMWare.

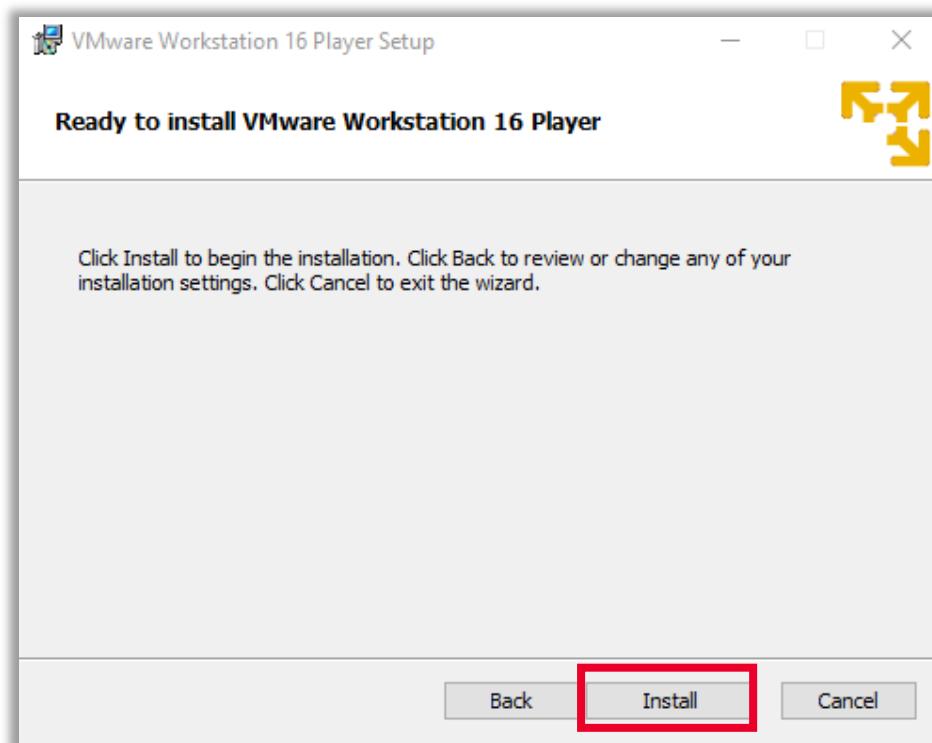


Ilustración 7: Clic en «*Install*» para comenzar la instalación.

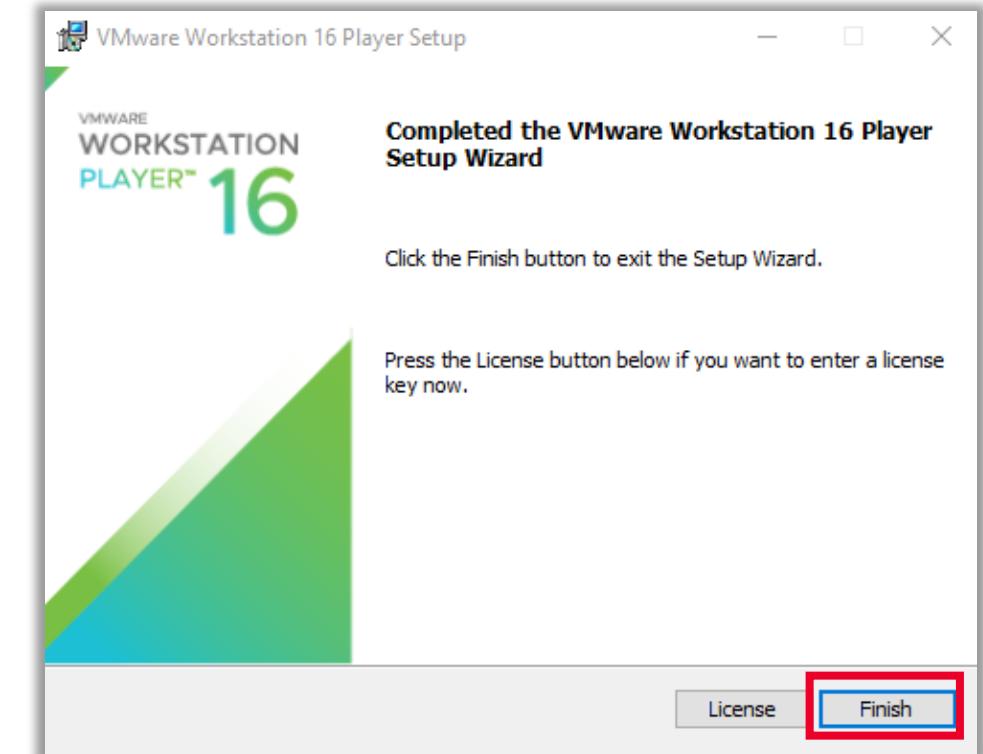


Ilustración 8: Instalación completada.

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

- 3.1 Instalación y configuración de la máquina virtual
- 3.2 Instalación del entorno gráfico de GNS3
- 3.3 Configuración de redes
- 3.4 Comprobación de actualizaciones
- 3.5 Configuración del entorno gráfico de GNS3
 - 3.5.1 Instalación y configuración de aplicaciones virtuales

3



3 INSTALACIÓN Y CONFIGURACIÓN DE GNS3

Una vez que has descargado e instalado VMWare, necesitarás la herramienta GNS3, para realizar estas prácticas.

Esta herramienta se compone de dos partes: una la máquina virtual y otra el entorno gráfico que se debe instalar en el ordenador, fuera de la máquina virtual. Como vamos a utilizar ambas durante la práctica y para que no haya confusión lo mencionaremos cada vez que cambiemos entre ellas.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.1 Instalación y configuración de la máquina virtual

- La primera que vas a instalar es la máquina virtual.
Se trata de un servidor en el que se alojan los dispositivos virtuales que vayamos creando durante la práctica.

Para ello, accede a este [enlace](#) y selecciona la opción «*VMware Workstation and Fusion*».

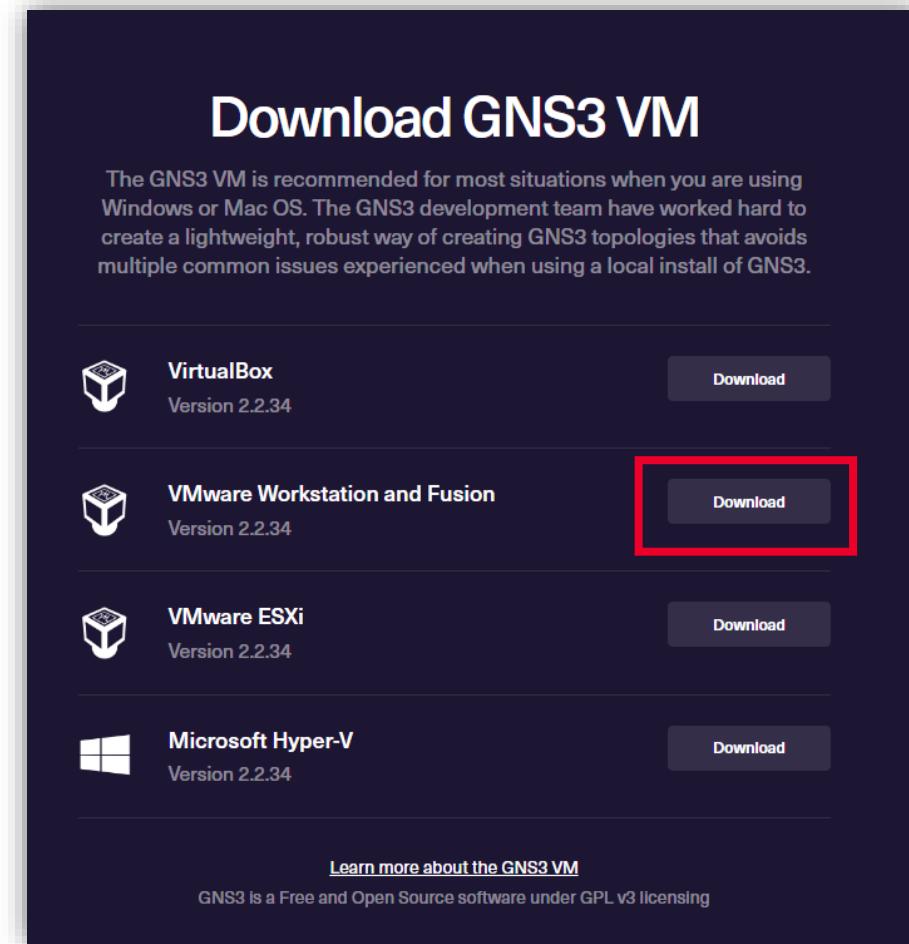


Ilustración 9: Selecciona la opción «*VMware Workstation and Fusion*».



3 INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.1 Instalación y configuración de la máquina virtual

- Se iniciará la descarga de un archivo .zip.
- Dentro de la carpeta donde estás almacenando la información y prácticas de este curso, crea una carpeta llamada GNS3, donde guardarás todo lo relacionado con esta herramienta.
- Mueve el archivo .zip descargado a esta carpeta GNS3.
- Descomprime el archivo .zip en esta carpeta.
- Una vez haya finalizado este proceso, haz doble clic directamente en la máquina «GNS3 VM». Se abrirá directamente una ventana de VMWare para importar la .ova.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.1 Instalación y configuración de la máquina virtual

- Pon el nombre que deseas a la máquina virtual y pulsa «*Import*». Espera a que se cargue la máquina virtual.

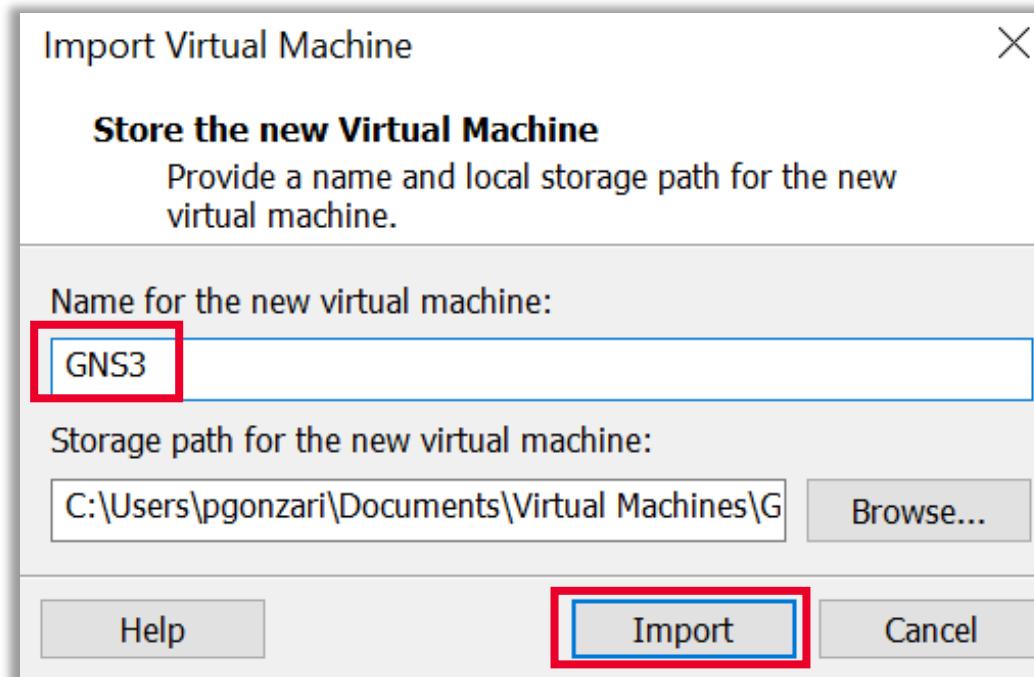


Ilustración 10: Nombra tu máquina virtual y pulsa «*Import*».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.1 Instalación y configuración de la máquina virtual

- Mantente a la espera hasta que termine el proceso de instalación, en ese momento se abrirá directamente la máquina virtual. Antes de nada, debemos cambiar a modo «bridge» la máquina virtual. Para eso ve al menú «Player > Manage > Virtual Machine Settings».
- Selecciona en esta ventana «Network Adapter» y luego la opción «Bridged».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.1 Instalación y configuración de la máquina virtual

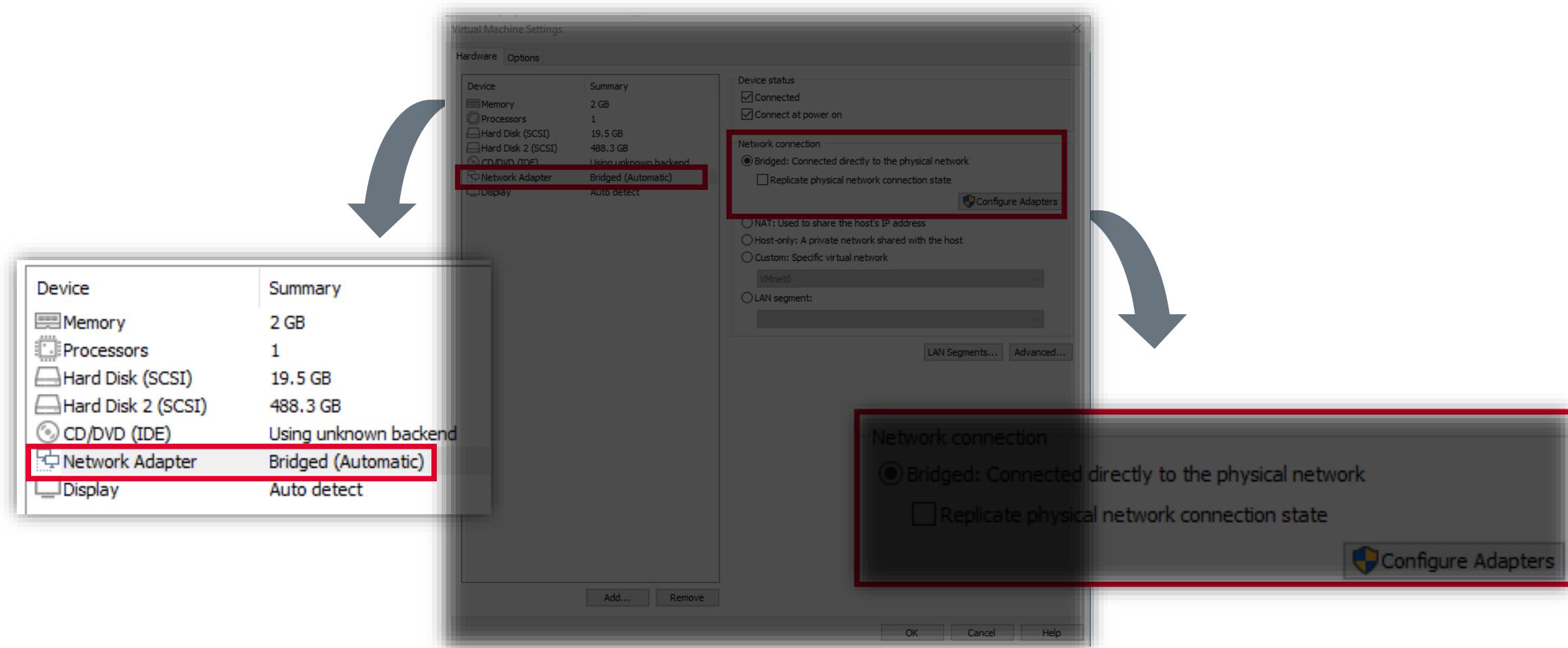


Ilustración 11: Ajustes de la máquina virtual.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

Después, en tu ordenador, es decir, sin ser en el hipervisor de VMWare, sino directamente en tu equipo, instalarás el entorno gráfico de GNS3 con el que trabajaremos. Para ello, descarga el entorno gráfico de GNS3 desde este [enlace](#).

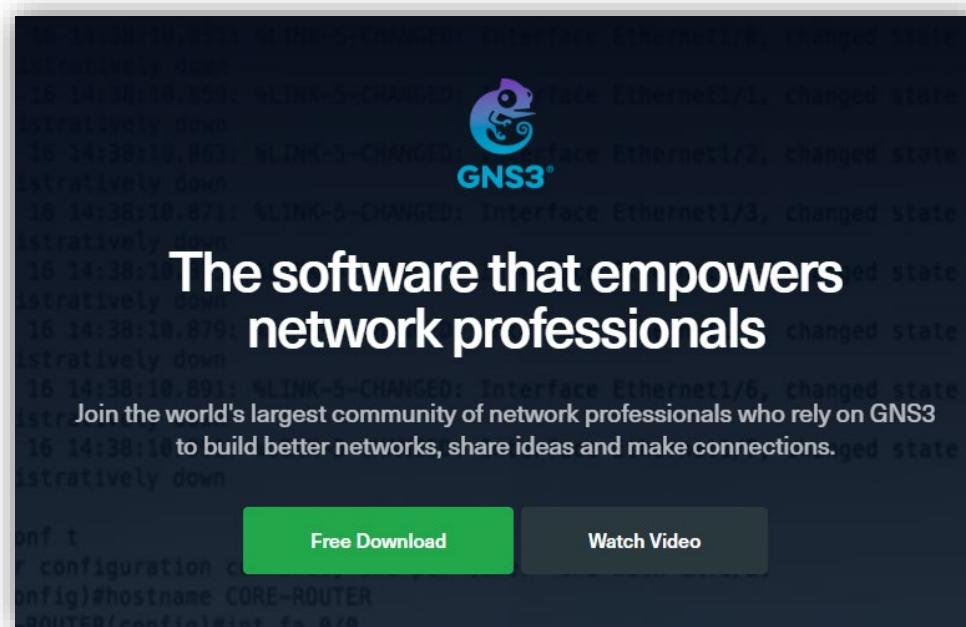


Ilustración 12: Instalación de la herramienta GNS3.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- A continuación, aparecerán dos opciones:

a) «*Sign up*»: para crear un nuevo usuario después de llenar un formulario.

b) «*Login*»: que redireccionará a la pantalla de acceso de usuarios registrados previamente mediante correo y contraseña.

En tu caso, si no estás registrado, deberás crear una cuenta nueva mediante la opción de «*Sign up*».

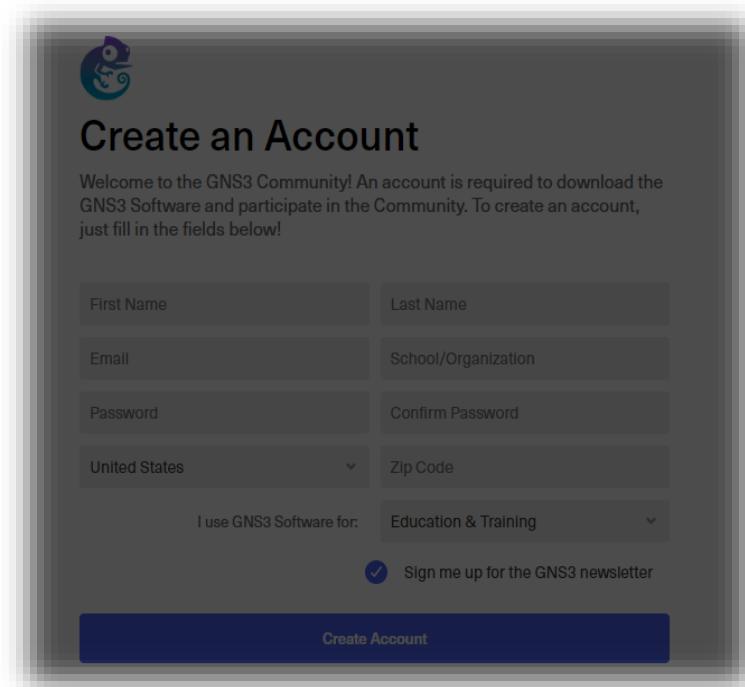


Ilustración 13: Opción «*Sign up*».

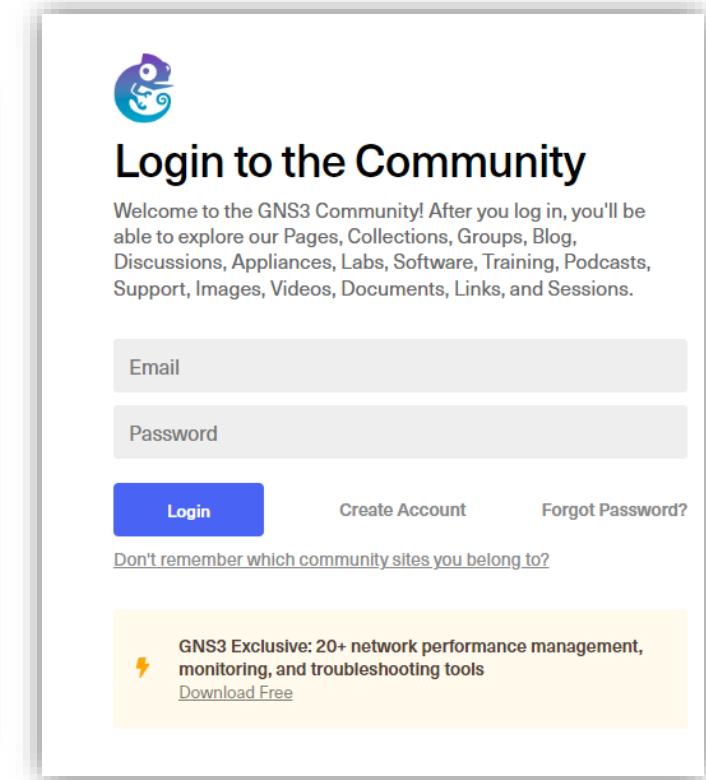


Ilustración 14: Opción «*Login*».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- Selecciona el sistema operativo de tu equipo para descargar GNS3 (Windows, Mac o Linux), en nuestro caso lo haremos en un ordenador Windows por lo que seleccionaremos esa opción y automáticamente comenzará la descarga.

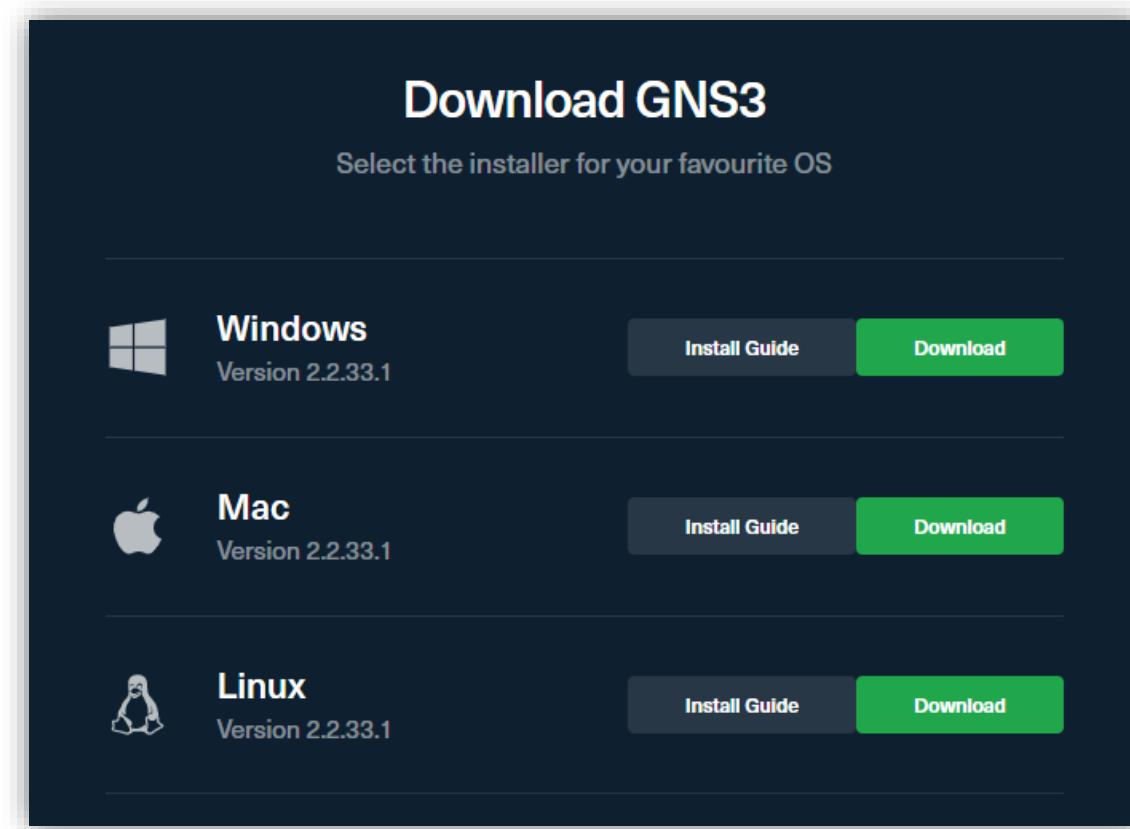


Ilustración 15: Opciones de sistema operativo.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- Una vez descargado, haz doble clic sobre el archivo para ejecutarlo y proceder a la instalación. Selecciona «Next».



Ilustración 16: Instalación de GNS3.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- Ahora, acepta los términos de la licencia.

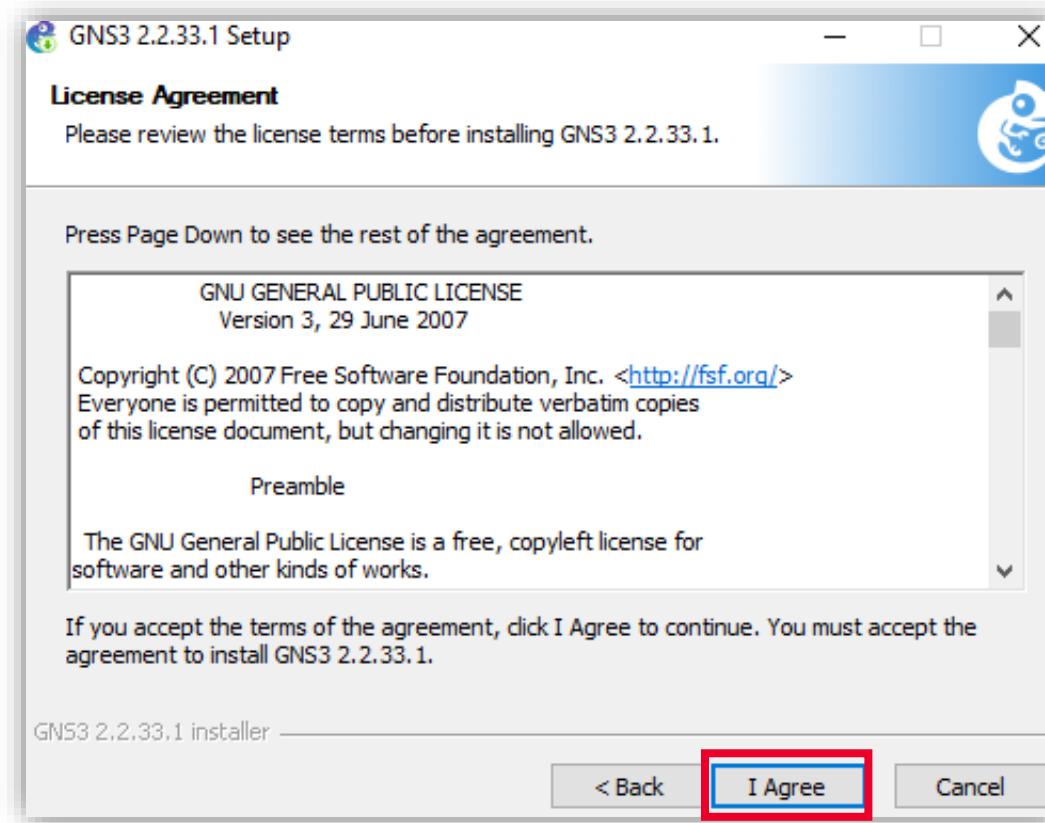


Ilustración 17: Términos y condiciones de la máquina virtual GNS3.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- Selecciona la carpeta del menú de Inicio en la que prefieras crear los accesos directos del programa. También podrás introducir un nombre para crear una nueva carpeta.

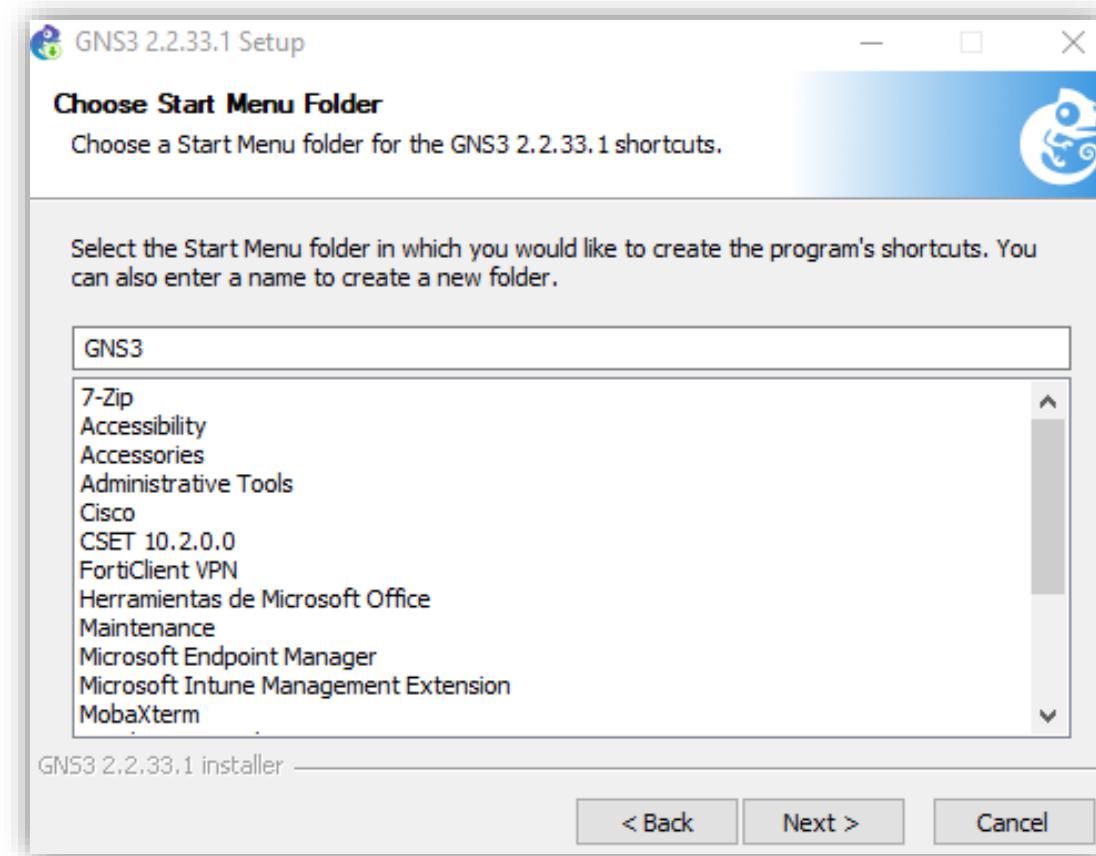


Ilustración 18: Elección de la ubicación y nombre de la carpeta.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- Mantén seleccionada la opción por defecto de «GNS3 Desktop».

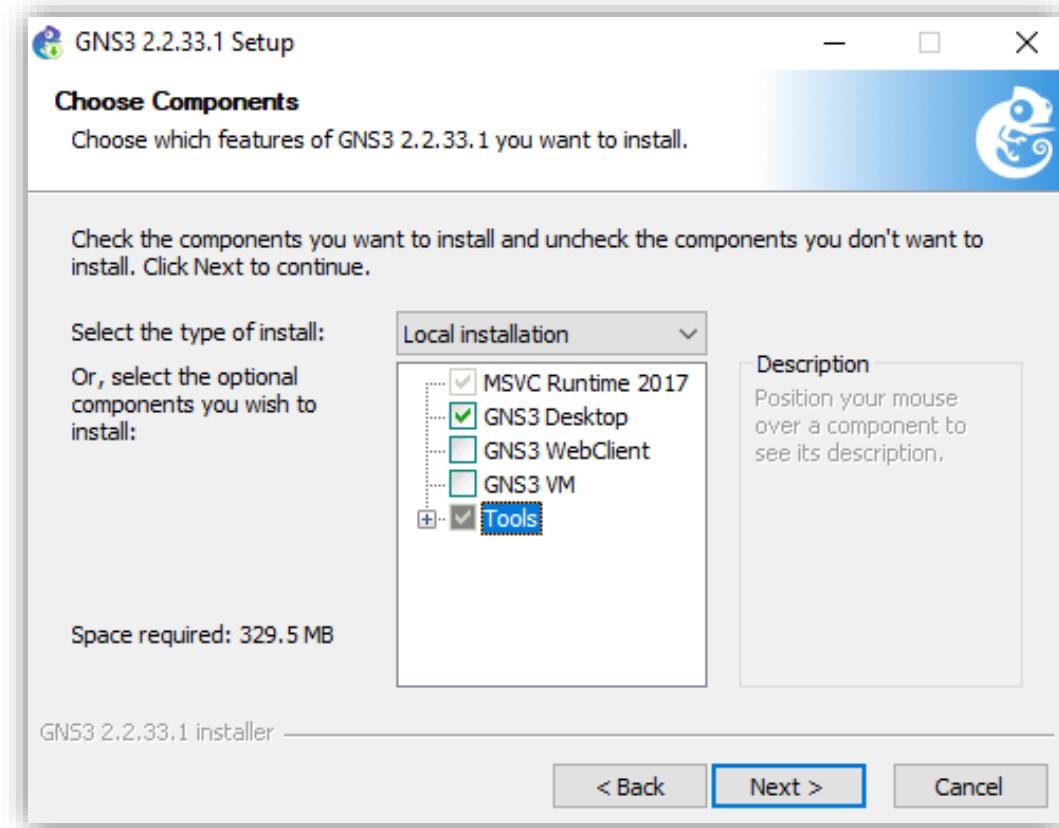


Ilustración 19: Elección de componentes de la máquina virtual.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- Pulsa en «Next».

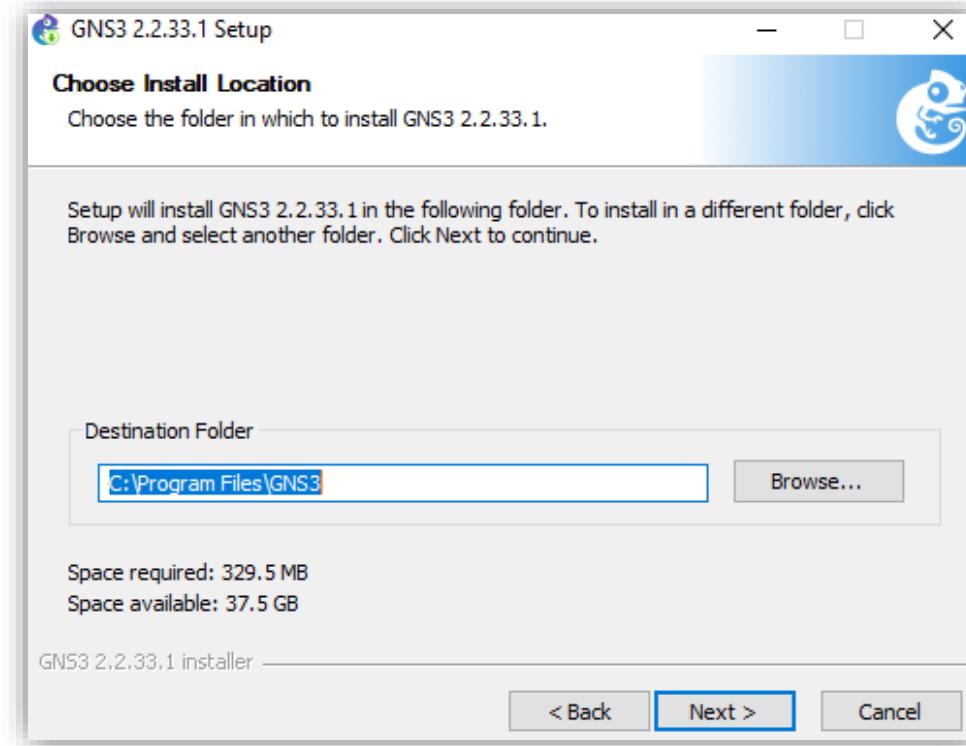


Ilustración 20: Localización de la instalación.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- A continuación, aparecerá una nueva ventana de la extensión WinPcap que necesita GNS3 para funcionar ya que esta extensión permite acceder a conexiones entre las capas de una red.
- Haz clic en «Next».

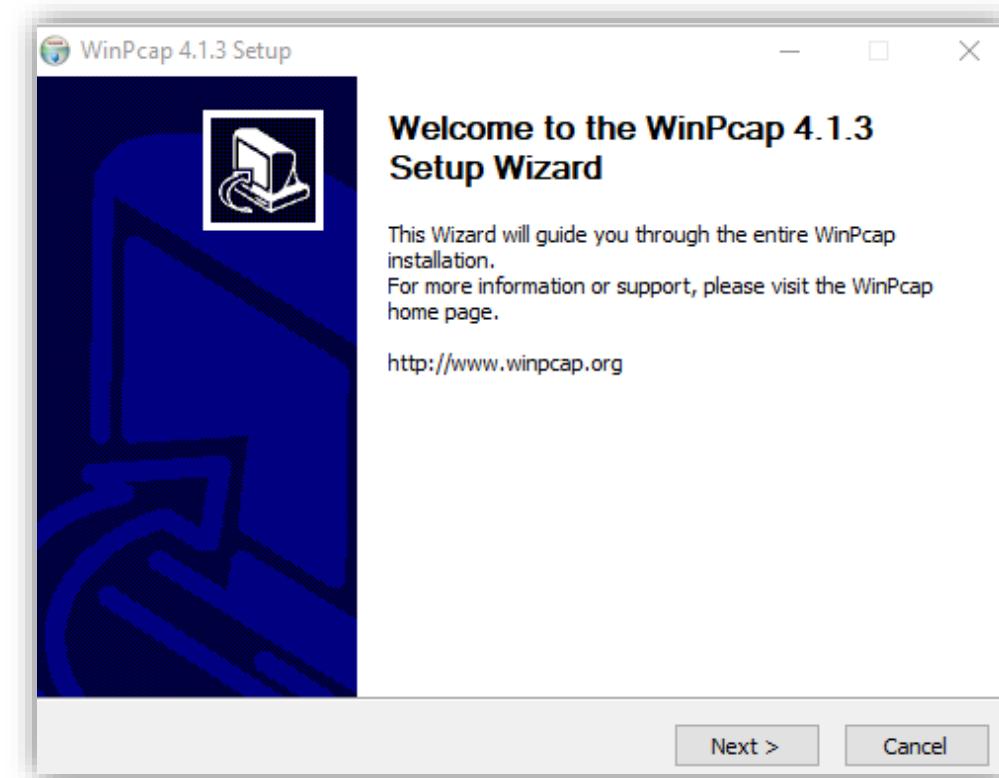


Ilustración 21: Guía de instalación.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- Acepta los términos y condiciones.

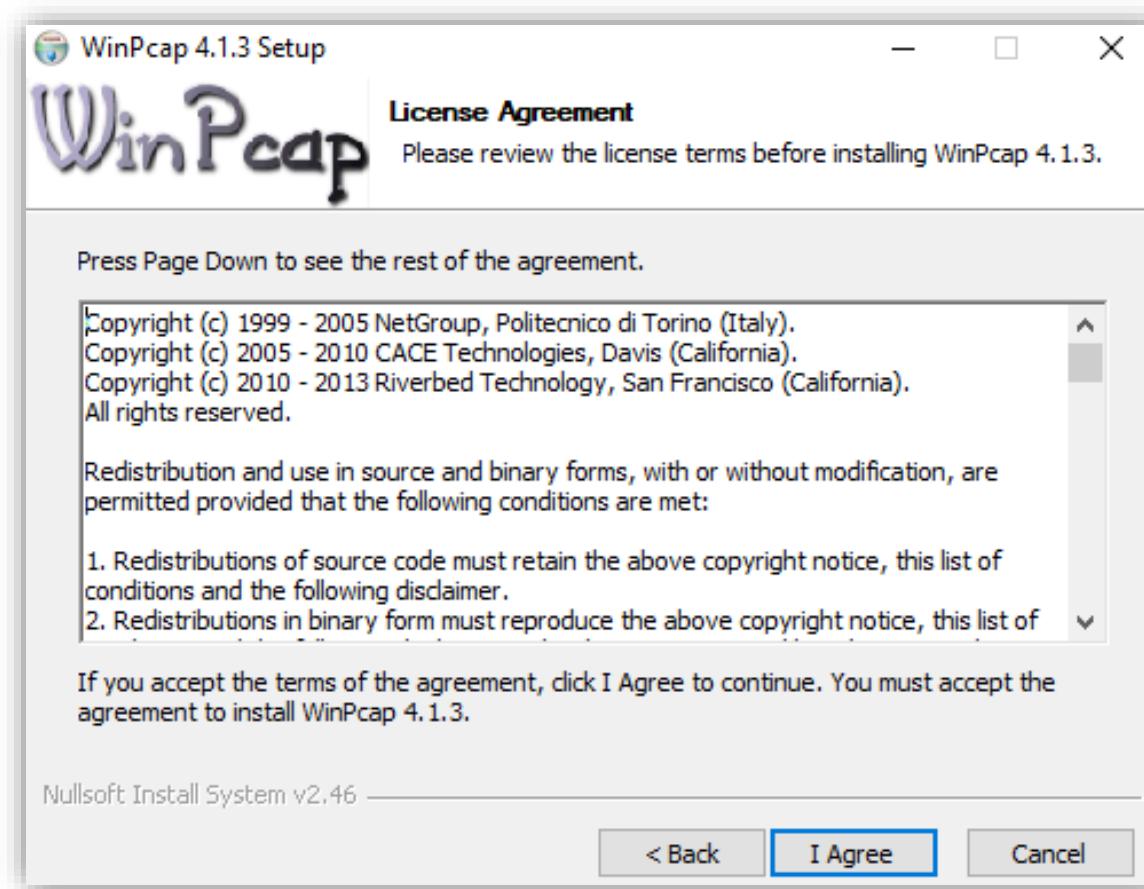


Ilustración 22: Términos y condiciones de la licencia.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- Pulsa en «Install».

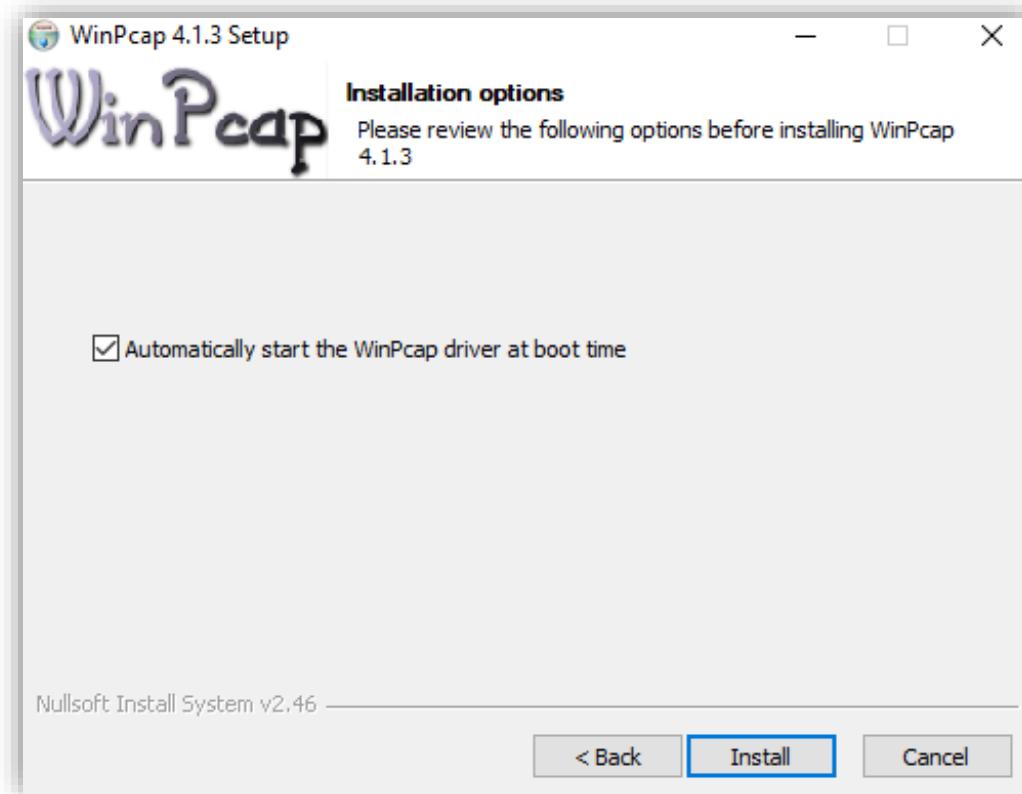


Ilustración 23: Opciones de instalación.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- Haz clic en «Finish».

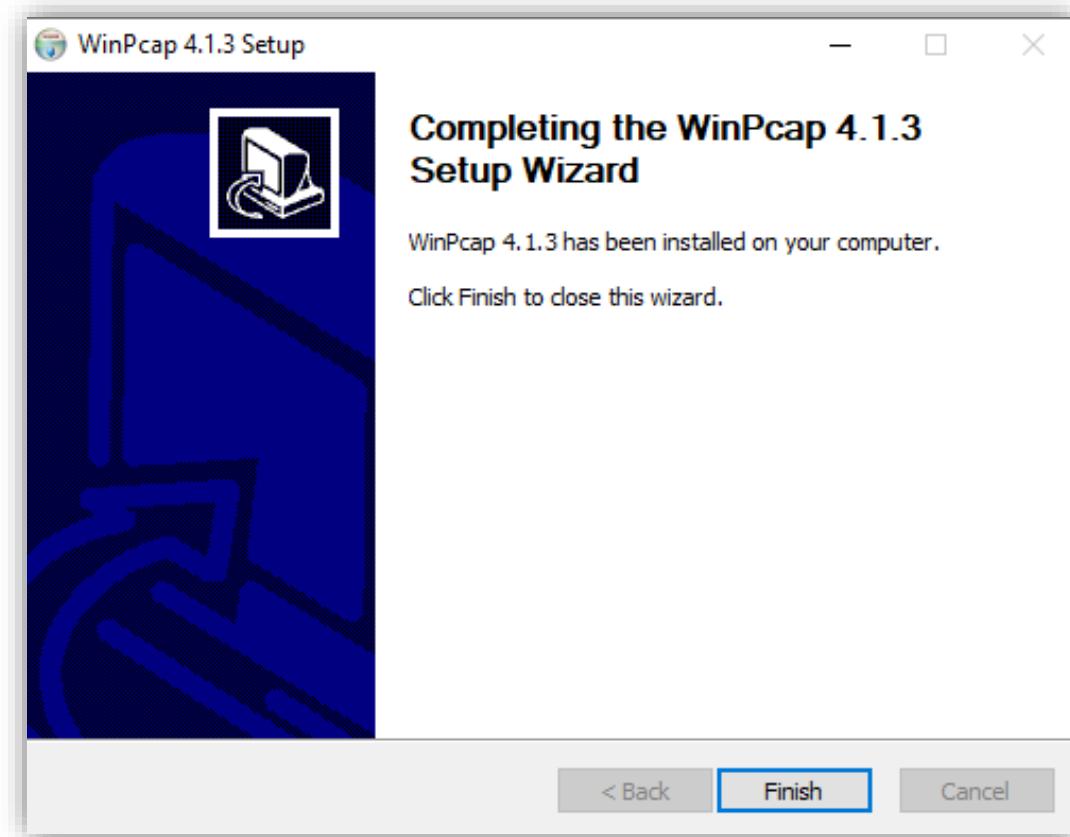


Ilustración 24: Finalizar la instalación.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- A continuación, aparecerá otra ventana emergente, sobre los términos y condiciones de la instalación, en este caso de «Npcap» (otra extensión necesaria para trabajar con GNS3). Esta se trata de una librería necesaria para el *sniffing* de paquetes.
- Acepta los términos pulsando en «I Agree».

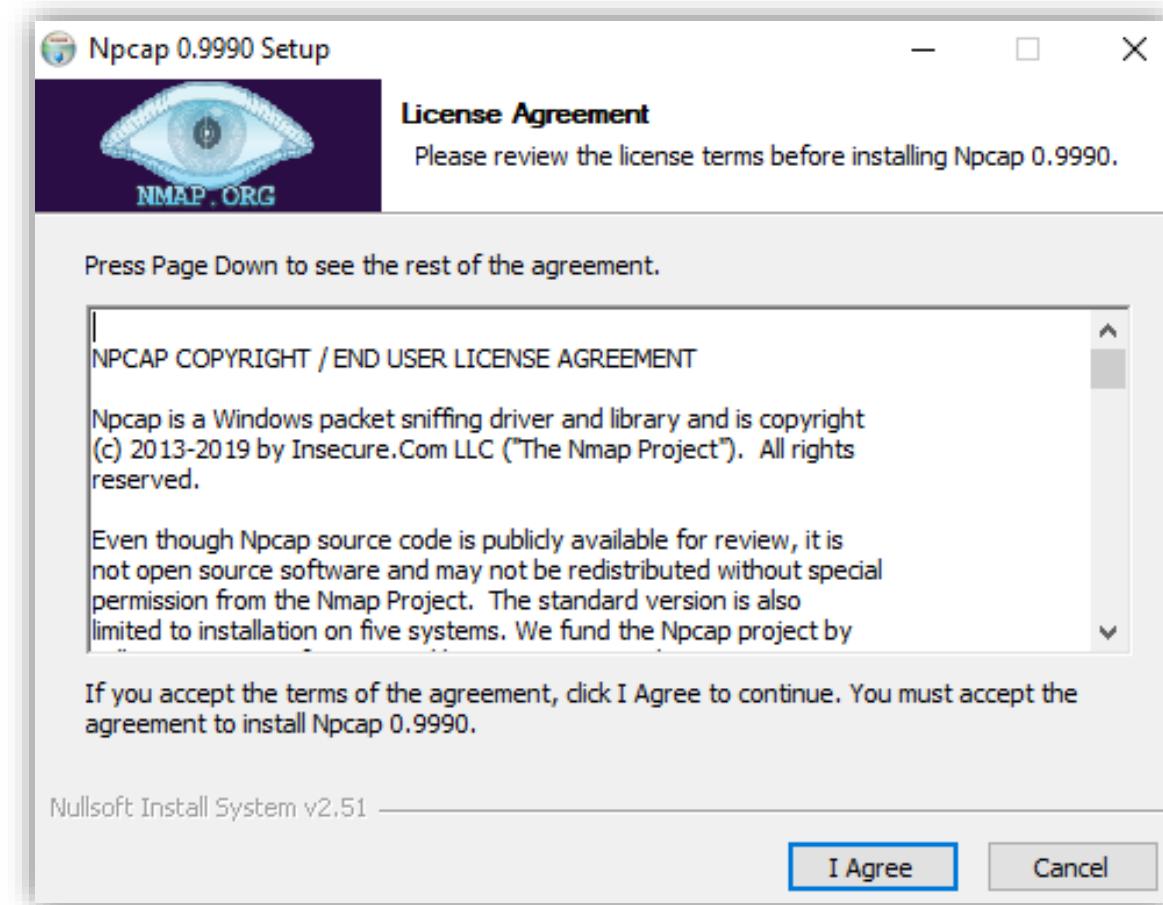


Ilustración 25: Términos y condiciones de Npcap.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- Deja la opción por defecto y pulsa en «*Install*».

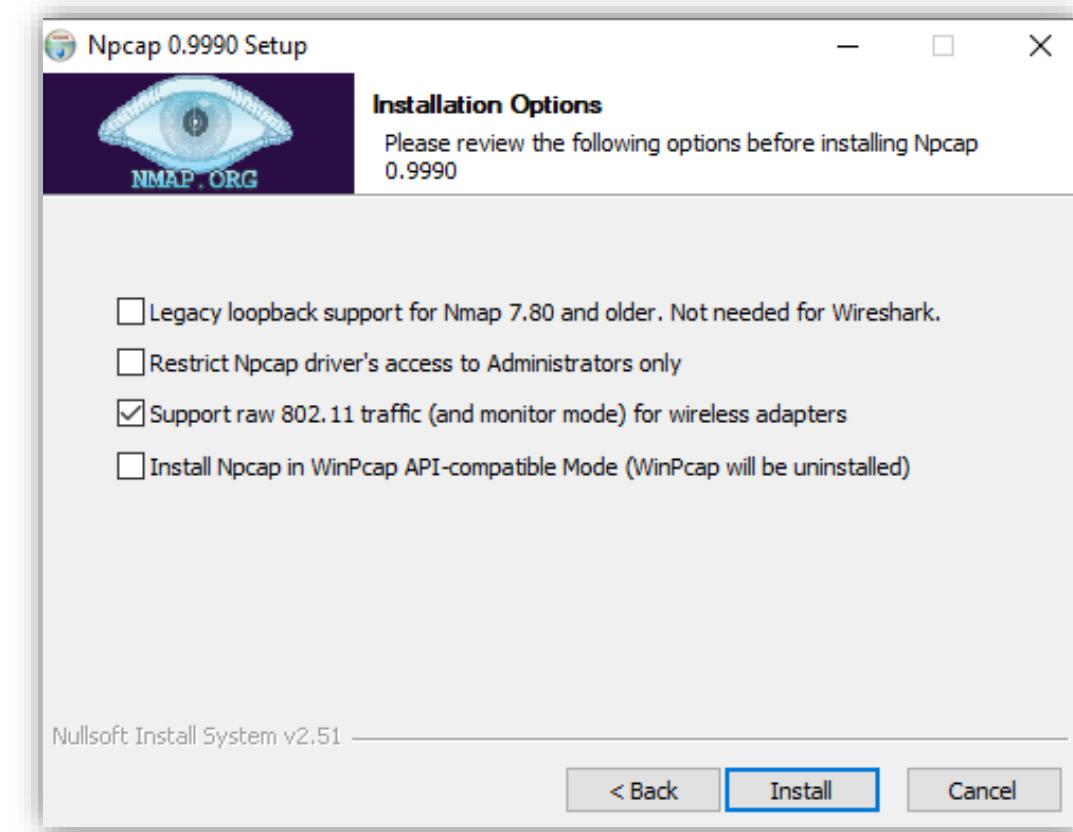


Ilustración 26: Opciones de instalación.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- Una vez completada la instalación de Npcap, haz clic en «Next».

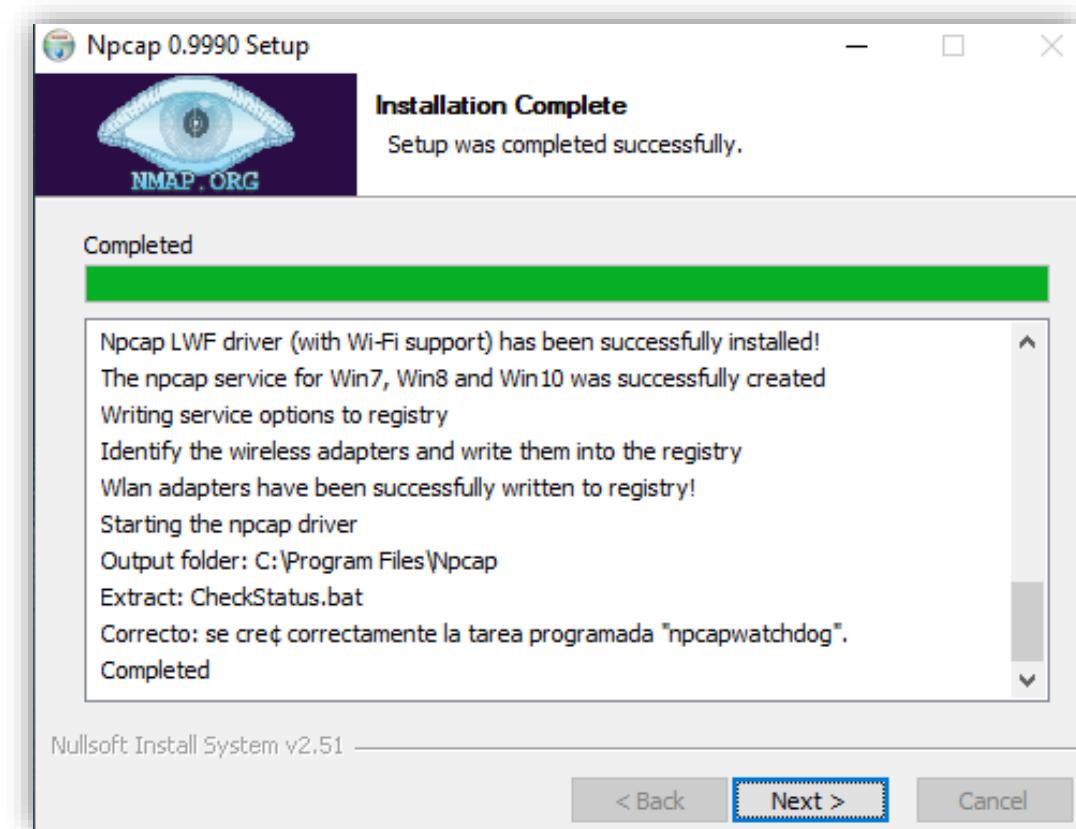


Ilustración 27: Instalación de Npcap completada.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- Pulsa en «Finish».

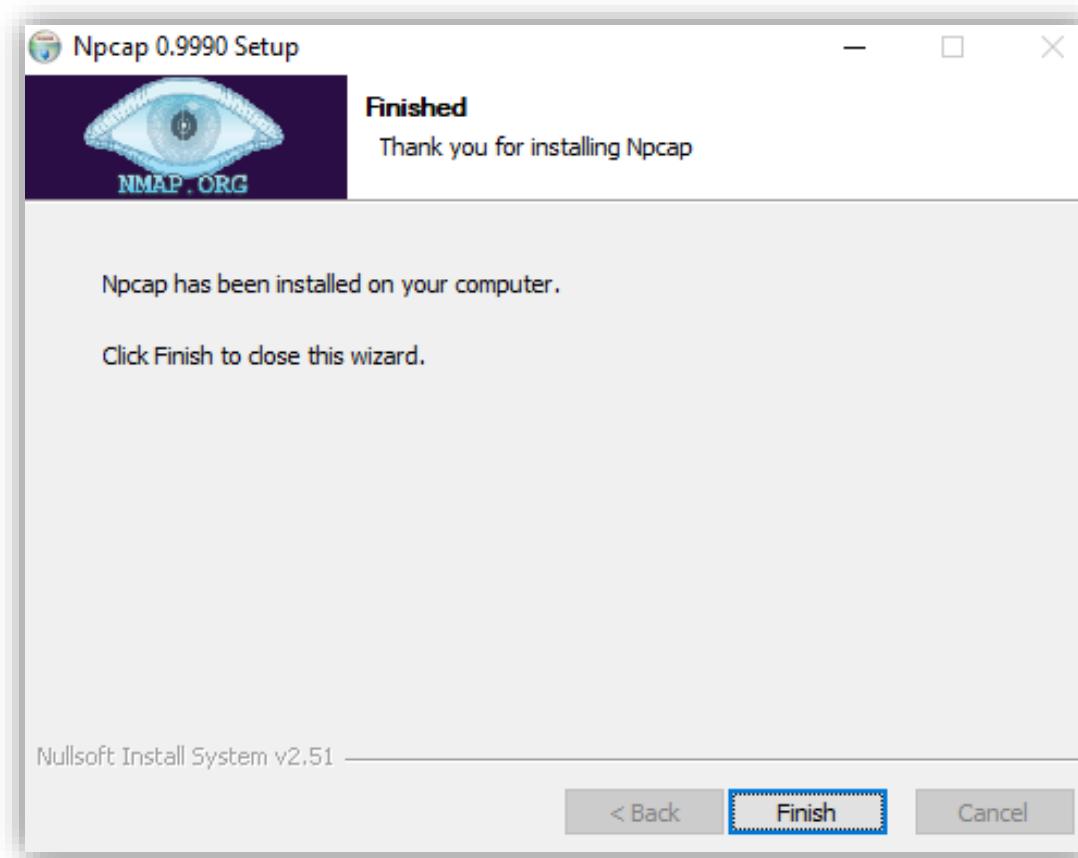


Ilustración 28: Finalización de la instalación de Npcap.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- Ahora, GNS3 continuará con su instalación hasta que termine.

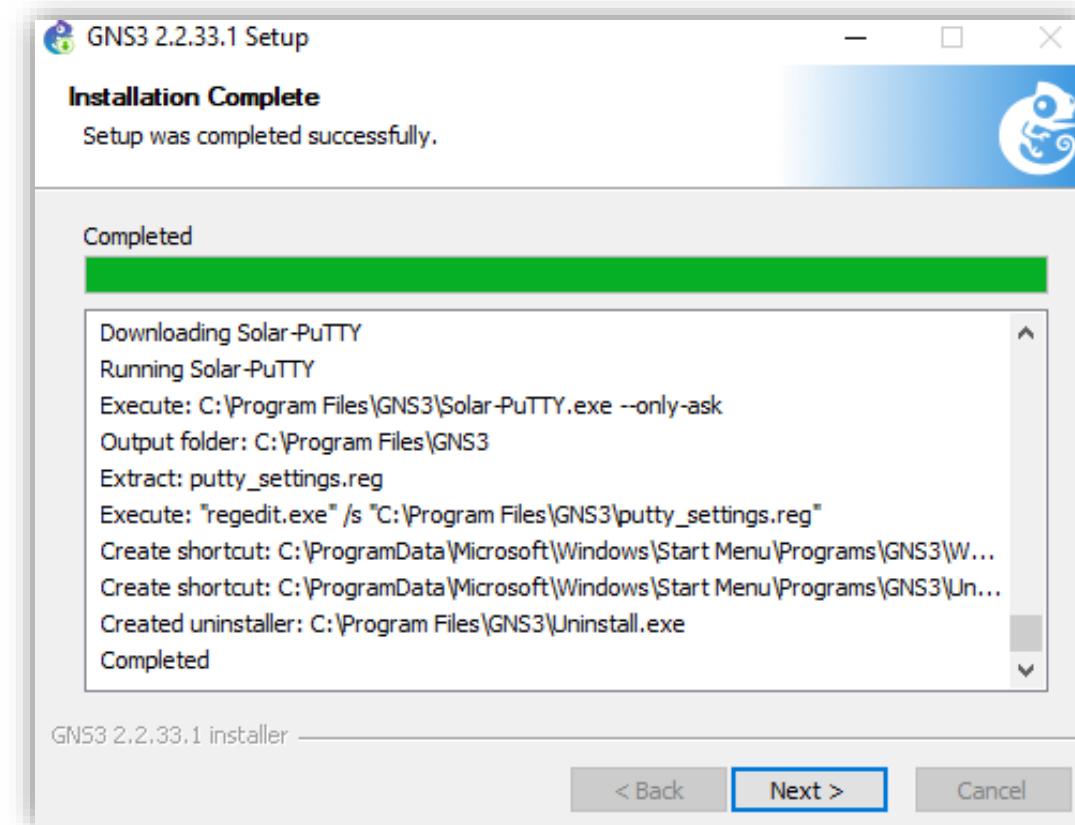


Ilustración 29: Instalación de GNS3 completada.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- Aparecerá la siguiente ventana emergente donde se te pregunta por tu interés en adquirir el programa Solarwinds, como no es necesario para la realización de esta práctica, selecciona la opción «No» y pulsa en el botón «Next».

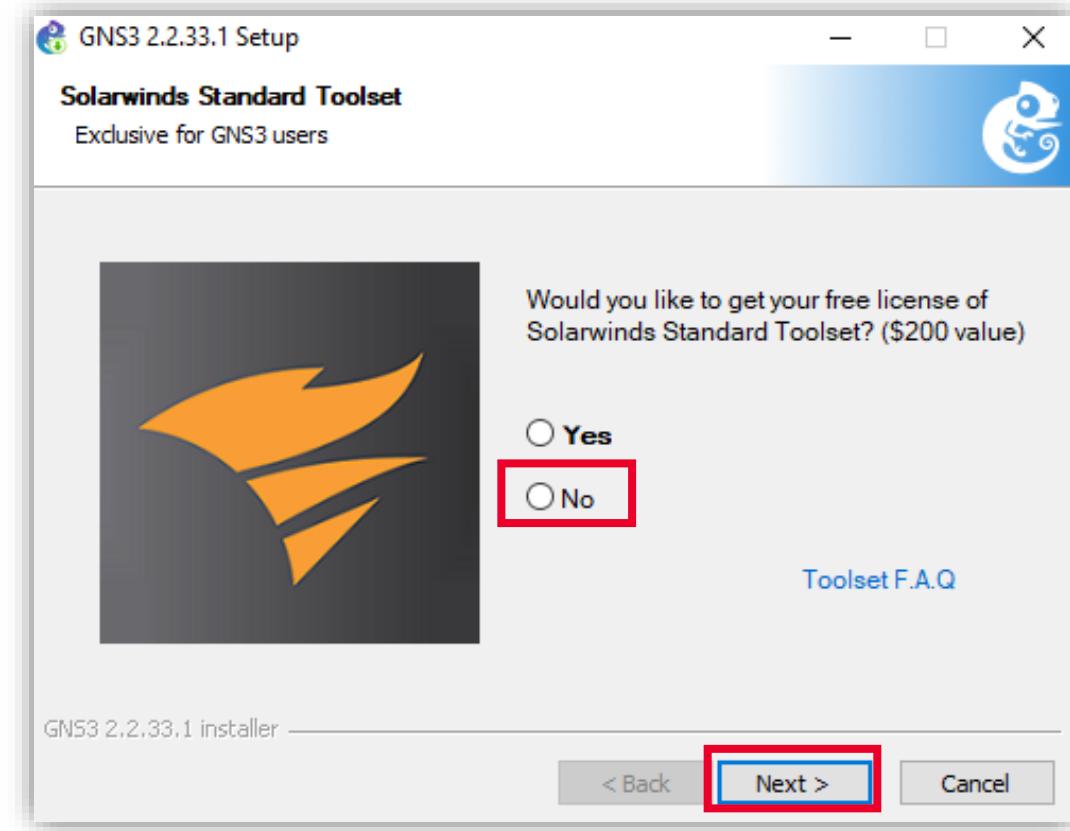


Ilustración 30: Instalación adicional de otra licencia de pago.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.2 Instalación del entorno gráfico de GNS3

- Cuando termine la instalación de GNS3, haz clic en «*Finish*».



Ilustración 31: Finalización de la instalación de GNS3.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.3 Configuración de redes

- Una vez descargado el entorno, deberás iniciar la máquina virtual desde VMware.
- Una vez iniciada, aparecerá una información que deberás guardar, ya que indicará la IP desde la cual deberás acceder desde el entorno gráfico de GNS3 (el que está instalado directamente en el ordenador) y la forma para conectarte a ella por medio de SSH en caso de ser necesario. De momento, utilizarás el entorno gráfico.

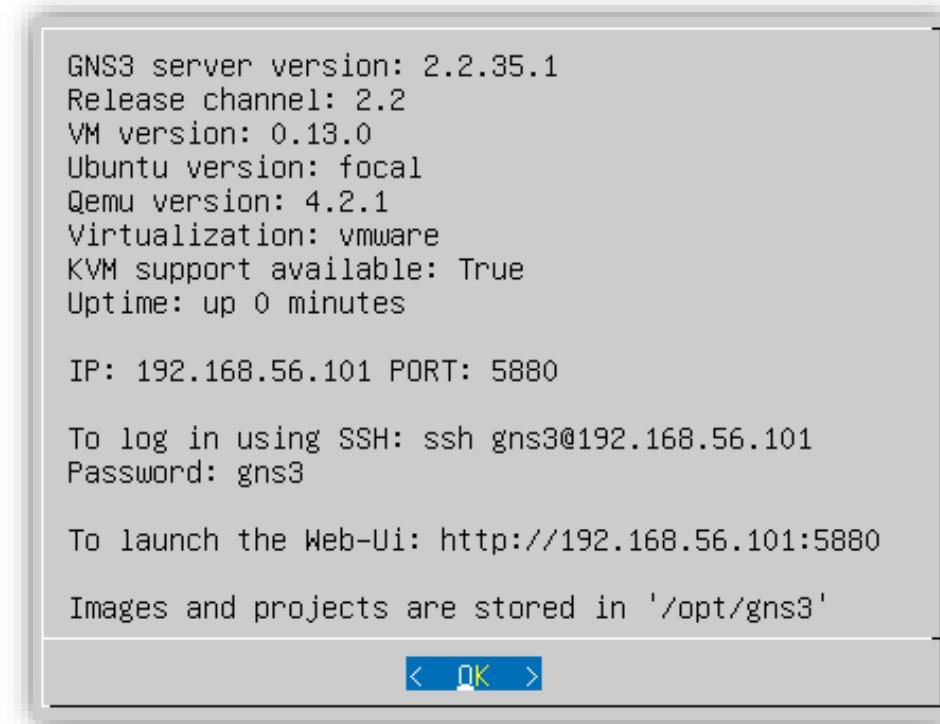


Ilustración 32: IP de acceso al entorno gráfico de la máquina.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.3 Configuración de redes

- Puede suceder que en este momento no te aparezca IP: esto sucedería en el caso que no se disponga de DHCP (*Dynamic Host Configuration Protocol*).
- Para solucionarlo debemos saber que la máquina virtual permite configurar IPs estáticas, puertas de enlace, etc., manualmente.
- Para ello, en el menú «*Network*» de la máquina virtual se ubica un archivo de texto, el cual, deberás configurar manualmente.
- Para realizar esta configuración desplázate con las flechas hasta «*Network*» y haz clic en «*enter*».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.3 Configuración de redes

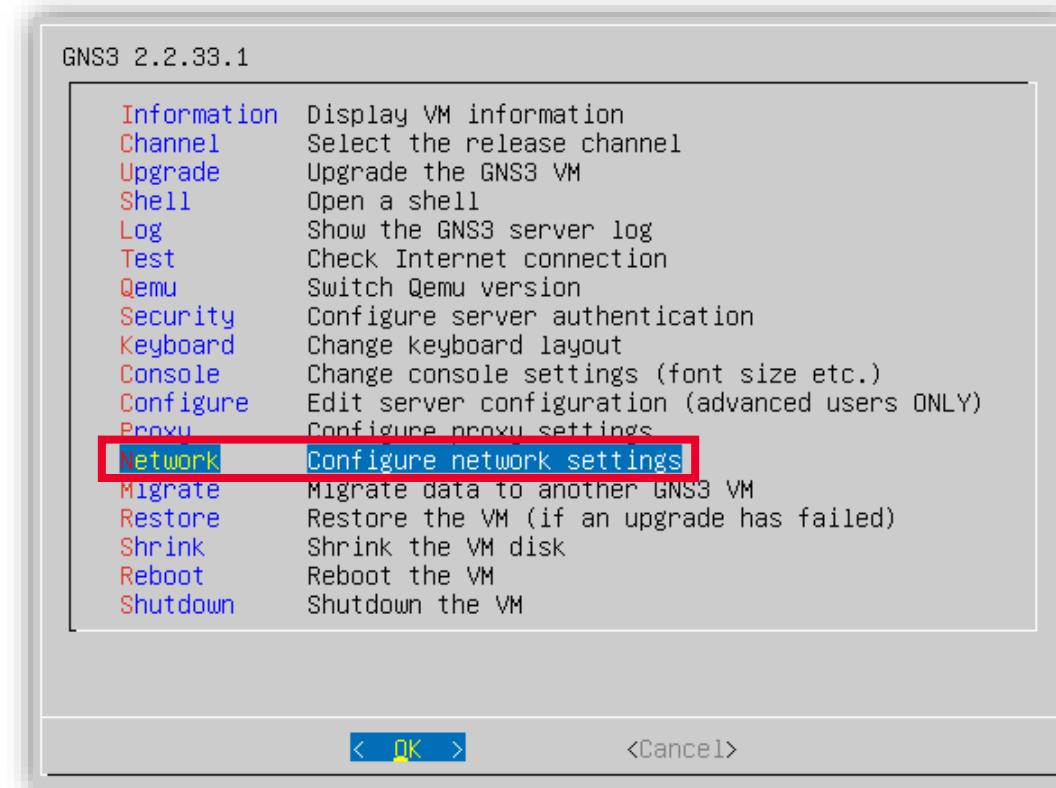


Ilustración 33: Opción de configuración «Network».



3 INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.3 Configuración de redes

- Una vez dentro de este archivo para configurarlo deberás «descomentar» (quitar las almohadillas al texto) desde la palabra «*network*» incluida y cambiar solamente los datos de los campos de IP y *Gateway* con los que correspondan según el caso.
- Antes de hacer este cambio tienes que saber qué IP corresponde en tu caso. Para saber cuál es, ejecuta el comando **ipconfig** en tu ordenador. Según la red a la que estés conectado deberás seleccionar una IP libre dentro del rango de esta red.
- Por ejemplo, en ese caso podrías utilizar como IP desde la 192.168.1.2 a la 192.168.1.254, exceptuando la 192.168.1.60. Si tienes más dispositivos conectados a la red comprueba que usas una IP que no se esté utilizando ya.



INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.3 Configuración de redes

```
Adaptador de LAN inalámbrica Wi-Fi:
```

```
Sufijo DNS específico para la conexión. . . :  
Dirección IPv4. . . . . : 192.168.1.60  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . . : 192.168.1.1
```

Ilustración 34: Rango de IPs disponibles y no disponibles.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.3 Configuración de redes

- Con respecto al *Gateway* deberás poner el dato que aparece en la imagen como «Puerta de enlace predeterminada».

```
# This file describes the network interfaces available on your system
# For more information, see netplan (5).

# Uncomment the following lines if you want to manually configure your network

network:
# version: 2
# renderer: networkd
# ethernets:
#   eth0:
#     dhcp4: no
#     addresses:
#       - 10.10.10.2/24
#     gateway4: 10.10.10.1
#     nameservers:
#       addresses: [8.8.8.8, 8.8.4.4]
```

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.3 Configuración de redes

```
GNU nano 4.8                               /etc/netplan/90_gns3vm_static_netcfg.yaml
# This file describes the network interfaces available on your system
# For more information, see netplan(5).

# Uncomment the following lines if you want to manually configure your network

network:
#  version: 2
#  renderer: networkd
#  ethernets:
#    eth0:
#      dhcp4: no
#      addresses:
#        - 10.10.10.2/24
#      gateway4: 10.10.10.1
#      nameservers:
#        addresses: [8.8.8.8, 8.8.4.4]
```

Ilustración 35: Contenido del fichero *Network* por defecto.



3 INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.3 Configuración de redes

- En caso de tener que modificarlo, este sería un ejemplo:

```
# This file describes the network interfaces available on your system
# For more information, see netplan (5).

# Uncomment the following lines if you want to manually configure your network

network:
# version: 2
# renderer: networkd
# ethernets:
#   eth0:
#     dhcp4: no
#     addresses:
#       - 192.168.1.56.101/24
#     gateway4: 192.168.1.1
#     nameservers:
#       addresses: [8.8.8.8, 8.8.4.4]
```



3 INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.3 Configuración de redes

```
GNU nano 4.8                               /etc/netplan/90_gns3vm_static_netcfg.yaml      Modified
# This file describes the network interfaces available on your system
# For more information, see netplan(5).

# Uncomment the following lines if you want to manually configure your network

network:
  version: 2
  renderer: networkd
  ethernets:
    eth0:
      dhcp4: no
      addresses:
        - 192.168.1.56.101/24
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

Ilustración 36: Ejemplo del fichero *Network* modificado, sin las # al principio de cada línea.



3 INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.3 Configuración de redes

- Para guardar el archivo deberás pulsar «**Ctrl + O**» y para salir de la configuración del archivo «**Ctrl + X**».
- Haz clic en «OK». A continuación, aparecerá un menú. Selecciona con las flechas del teclado la línea «*Network*» y pulsa «OK».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.4 Comprobación de actualizaciones

- Después vuelve al entorno gráfico de GNS3 instalado anteriormente. Es importante que tanto la máquina virtual como el entorno gráfico estén en la misma versión. Por lo que deberemos comprobar en ambos si hay actualizaciones disponibles. En las siguientes capturas se muestra dónde se actualizan tanto el entorno gráfico como la máquina virtual.

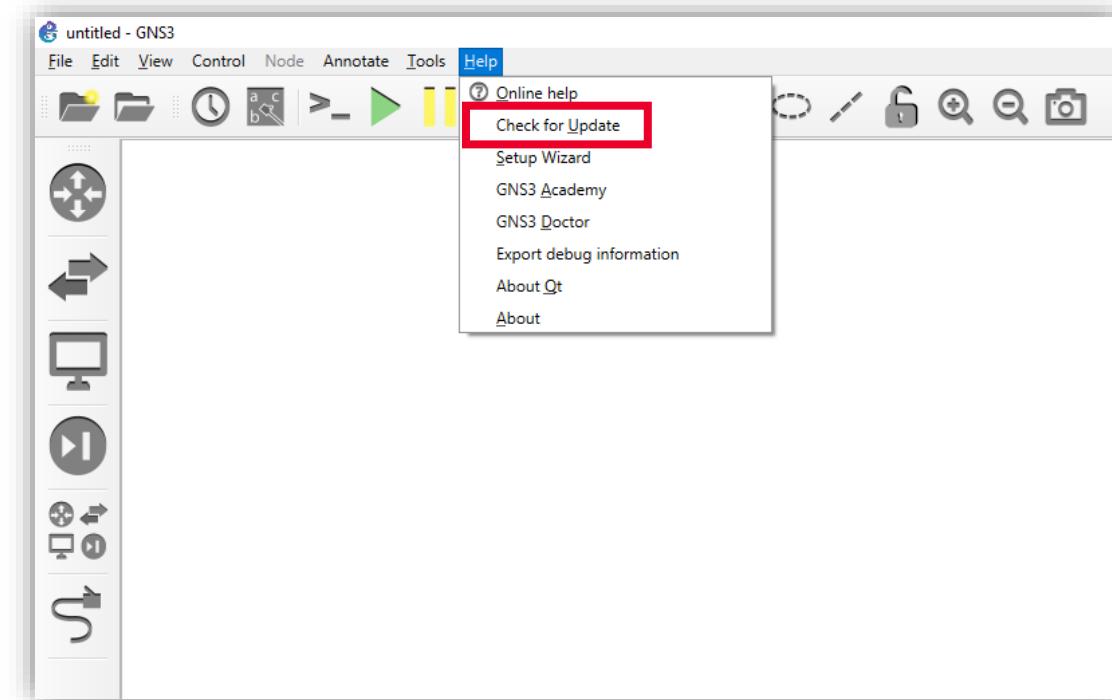


Ilustración 37: Comprobar actualizaciones en el entorno gráfico.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.4 Comprobación de actualizaciones

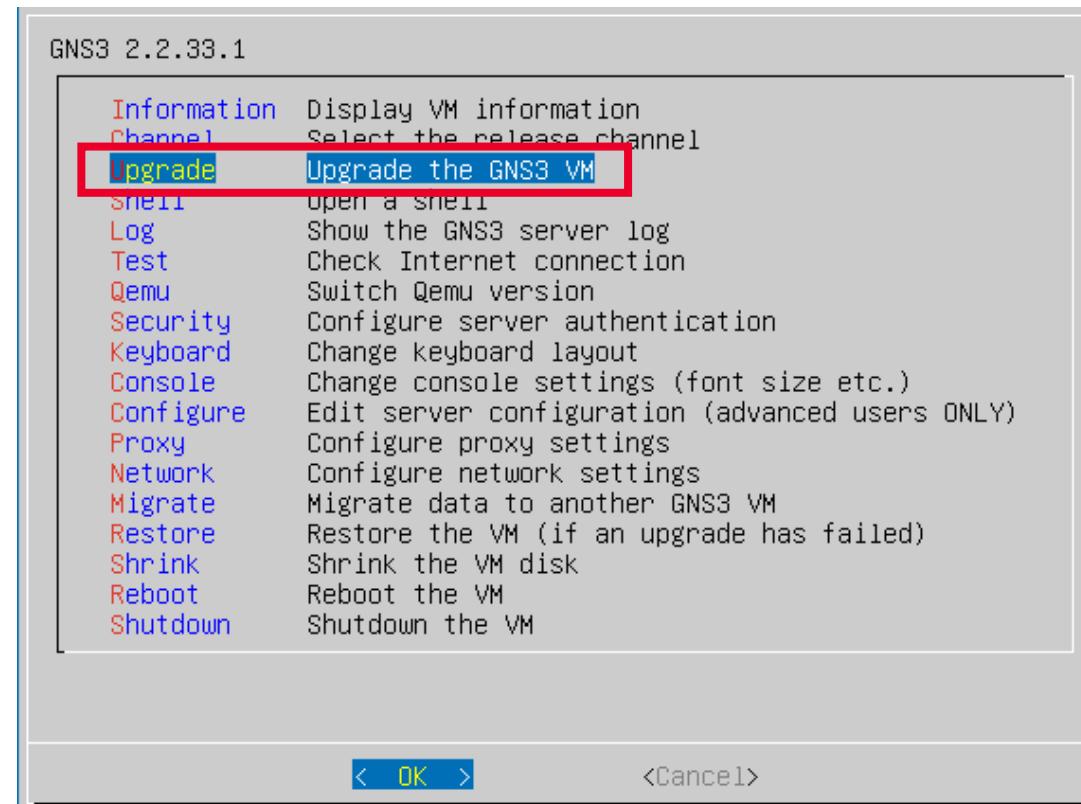


Ilustración 38: Comprobar actualizaciones en la máquina virtual.



3 INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5 Configuración del entorno gráfico de GNS3

- Una vez configurada la máquina virtual de GNS3, dirígete al entorno gráfico de esta herramienta.
- Para comenzar la configuración en el entorno gráfico selecciona el menú «Edit» y después «Preferences» y comprueba si la máquina virtual es detectada automáticamente en el menú «GNS3 VM».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5 Configuración del entorno gráfico de GNS3

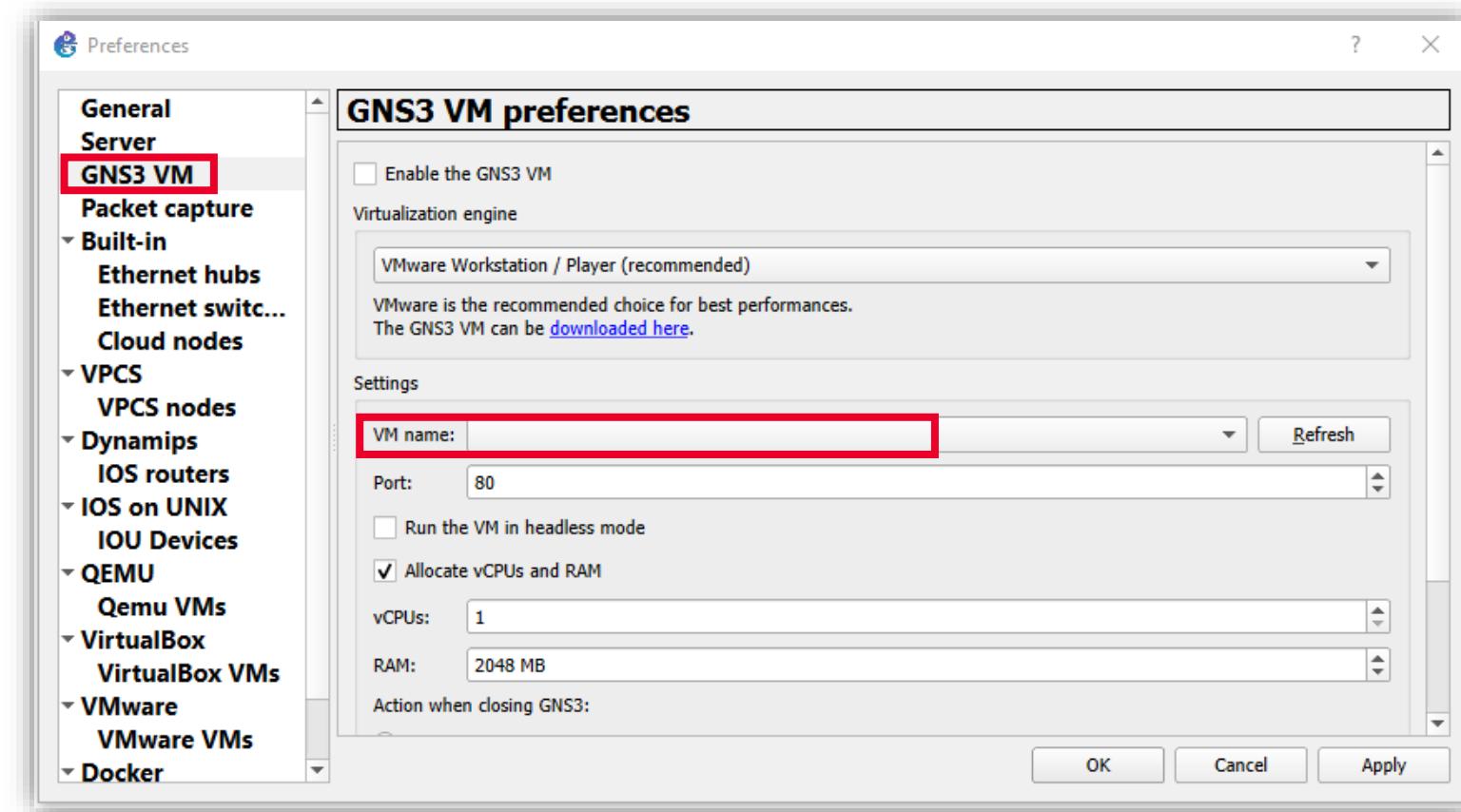


Ilustración 39: Selecciona el menú «Preferences».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5 Configuración del entorno gráfico de GNS3

- En nuestro caso, al no detectarse automáticamente la máquina virtual seleccionaremos el menú «Server», en él debes introducir los datos manualmente con la IP que aparecía al iniciar la máquina virtual.

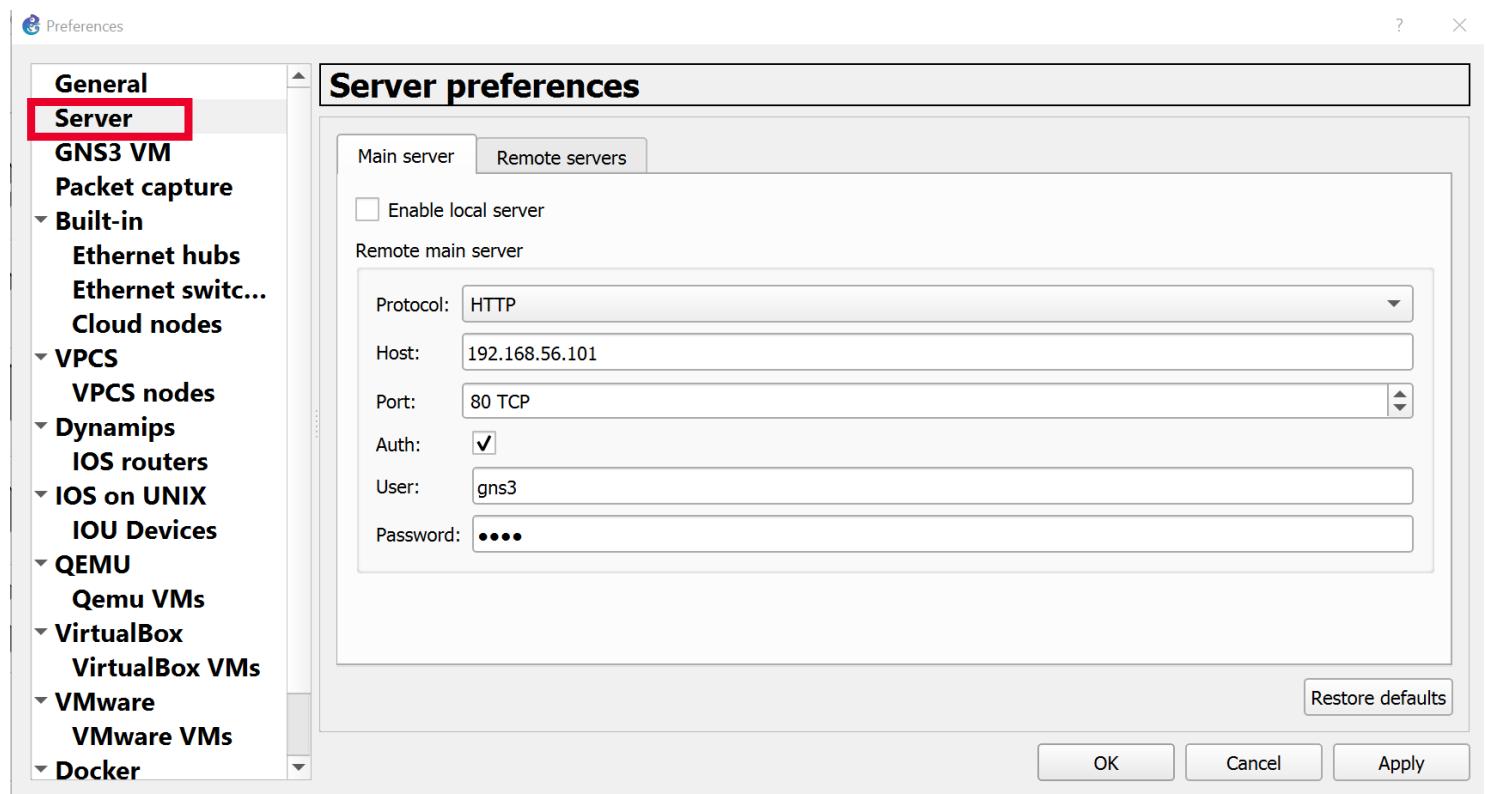


Ilustración 40: Selecciona el menú «Server».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5 Configuración del entorno gráfico de GNS3

- Si está bien configurado aparecerá un ícono verde para confirmar que la conexión se está realizando correctamente.

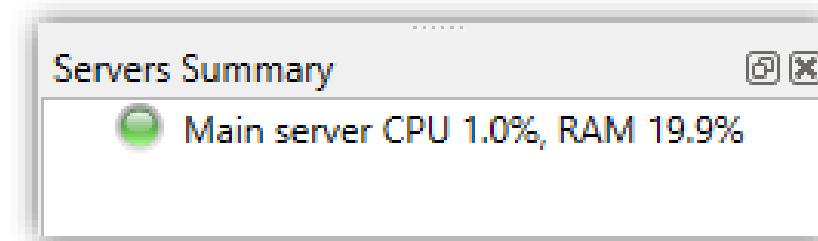


Ilustración 41: Comprobador de que la conexión es exitosa.

3

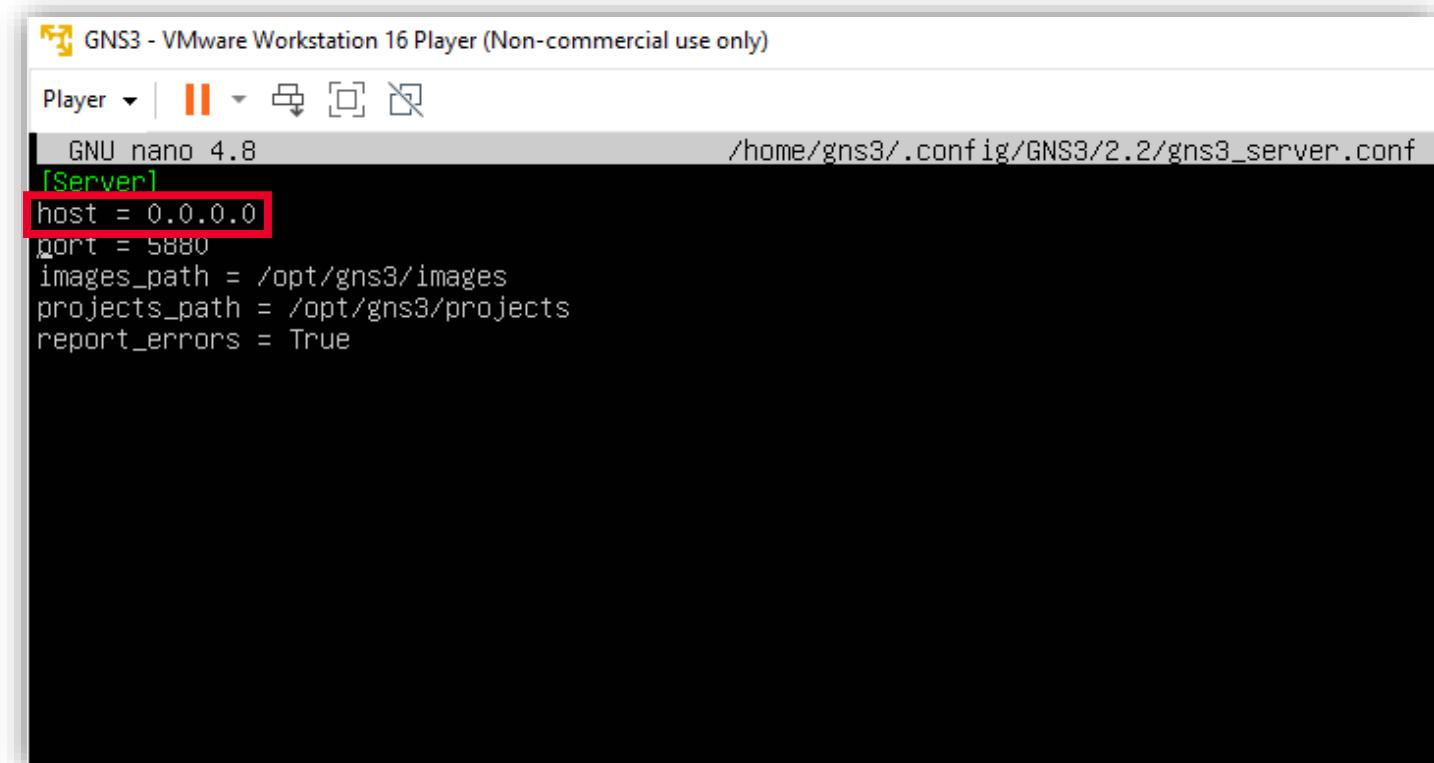
INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5 Configuración del entorno gráfico de GNS3

- Si no es así y no se realiza correctamente la conexión puede ser porque el puerto por defecto se esté utilizando para otra cosa y habría que cambiar este puerto por otro que no esté siendo utilizado.

Para ello, debes ir a la máquina virtual de GNS3 y seleccionar el menú «Configure».

Se abrirá un archivo de texto dónde simplemente habrá que cambiar el puerto 80 por otro que queramos, nosotros hemos indicado el 5880.



```
GNU nano 4.8
[Server]
host = 0.0.0.0
port = 5880
images_path = /opt/gns3/images
projects_path = /opt/gns3/projects
report_errors = True
```

Ilustración 42: Archivo de texto para cambiar el puerto 80.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5 Configuración del entorno gráfico de GNS3

- Para guardar los cambios hay que pulsar «**Ctrl + O**» y para salir «**Ctrl + X**». Para comprobar que el puerto se ha cambiado correctamente vamos al menú «*Information*».

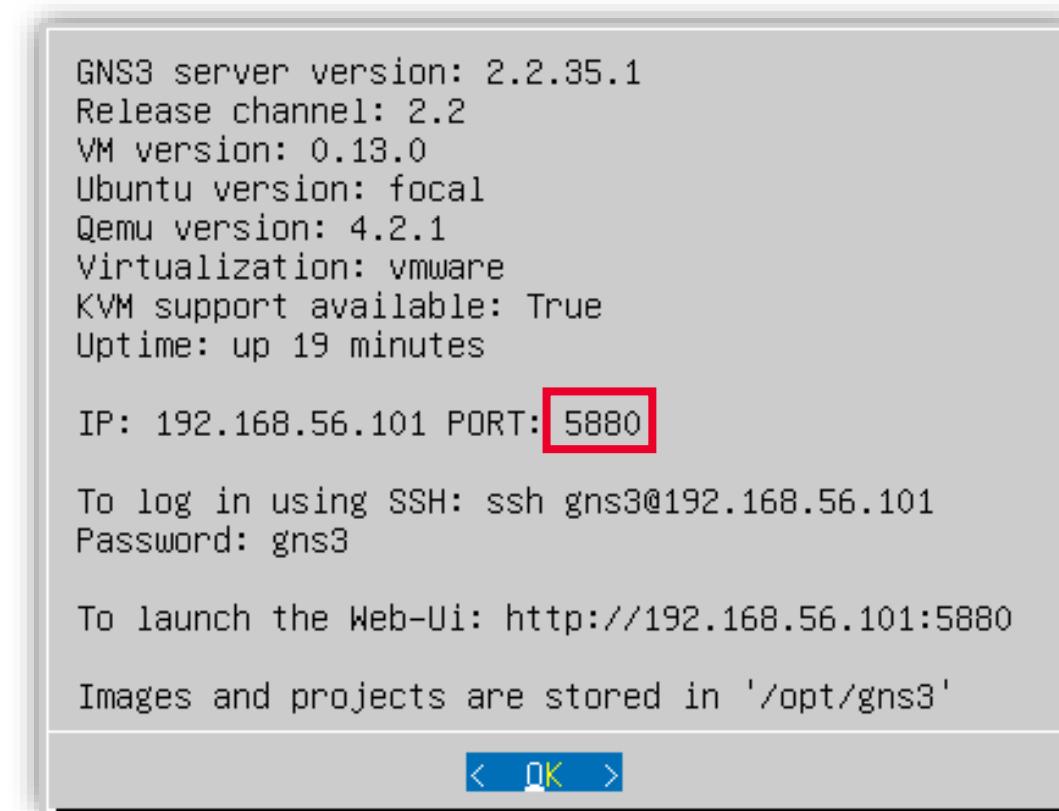


Ilustración 43: En el menú «*Information*» comprobamos que el puerto se ha cambiado correctamente.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

- Una vez configurado todo esto vamos a ver cómo se instalan aplicaciones virtuales, «appliances», de otros programas y herramientas. En este primer caso lo haremos con Ubuntu, para ello vuelve al entorno gráfico de GNS3, y abre un nuevo proyecto en el menú «**File > New Blank Project**».

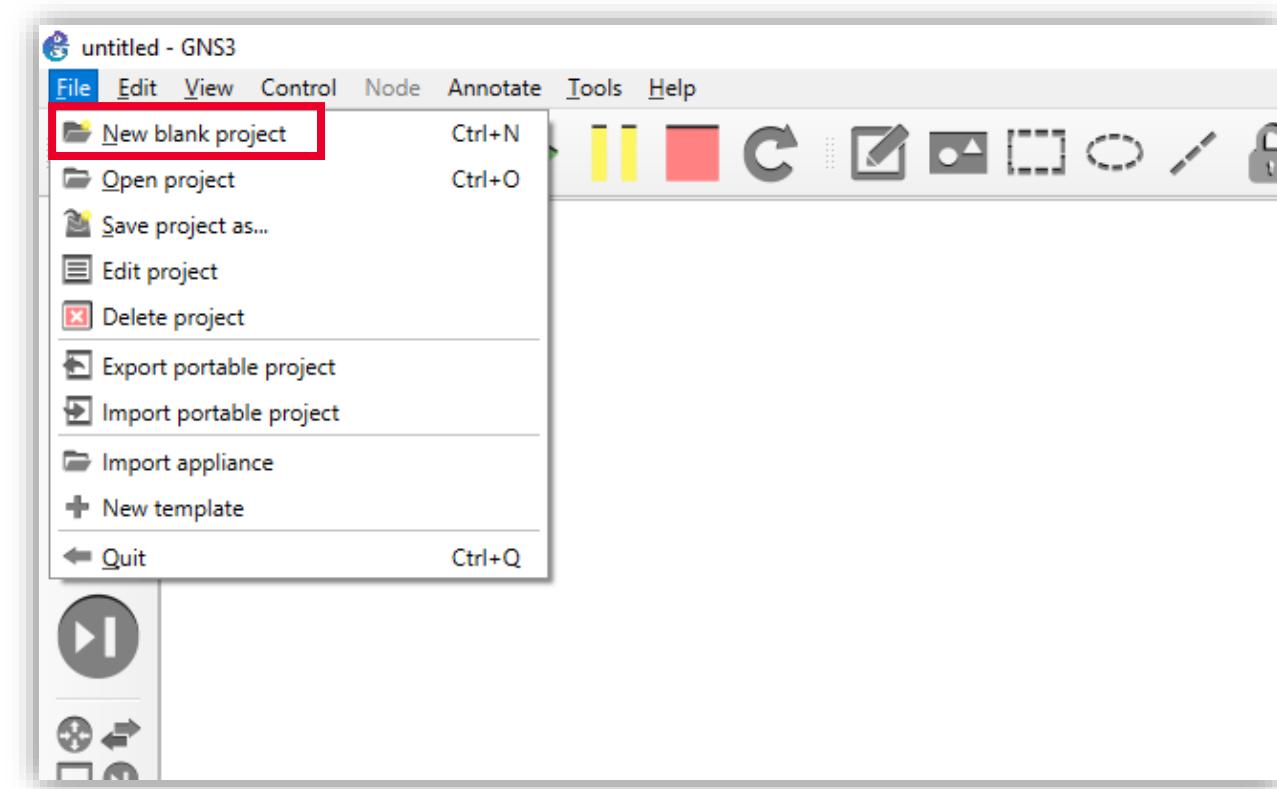


Ilustración 44: Abrimos nuevo proyecto.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

- Cambia el nombre al proyecto, pon el que tú quieras.

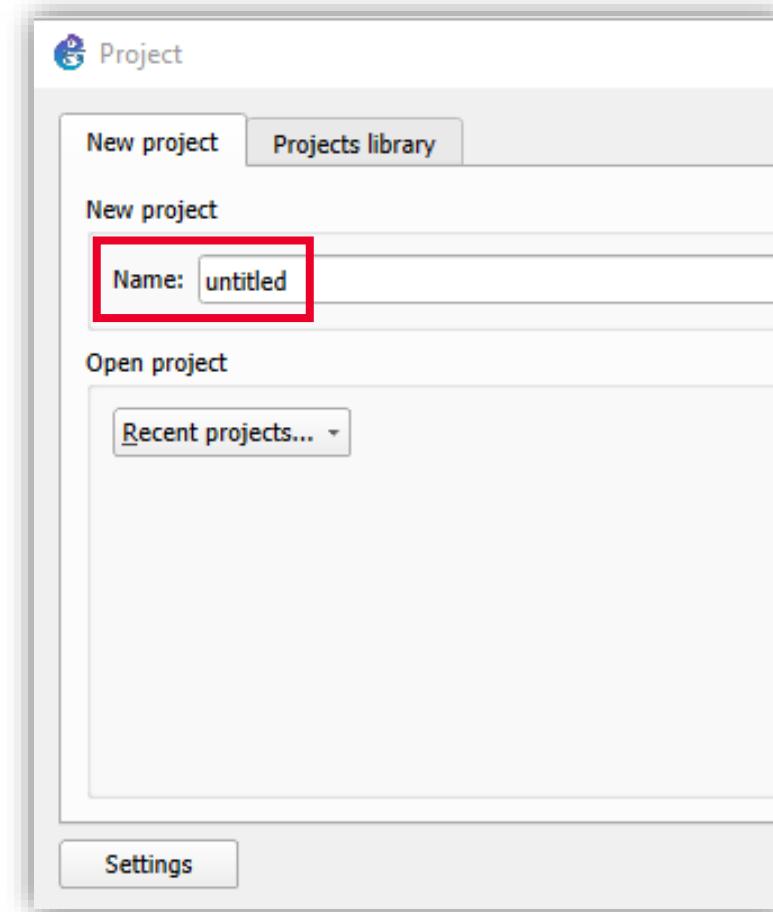


Ilustración 45: Cambiamos el nombre del proyecto.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

- Este es el menú inicial. Previo a la instalación de ninguna aplicación virtual que te vamos a explicar a continuación.

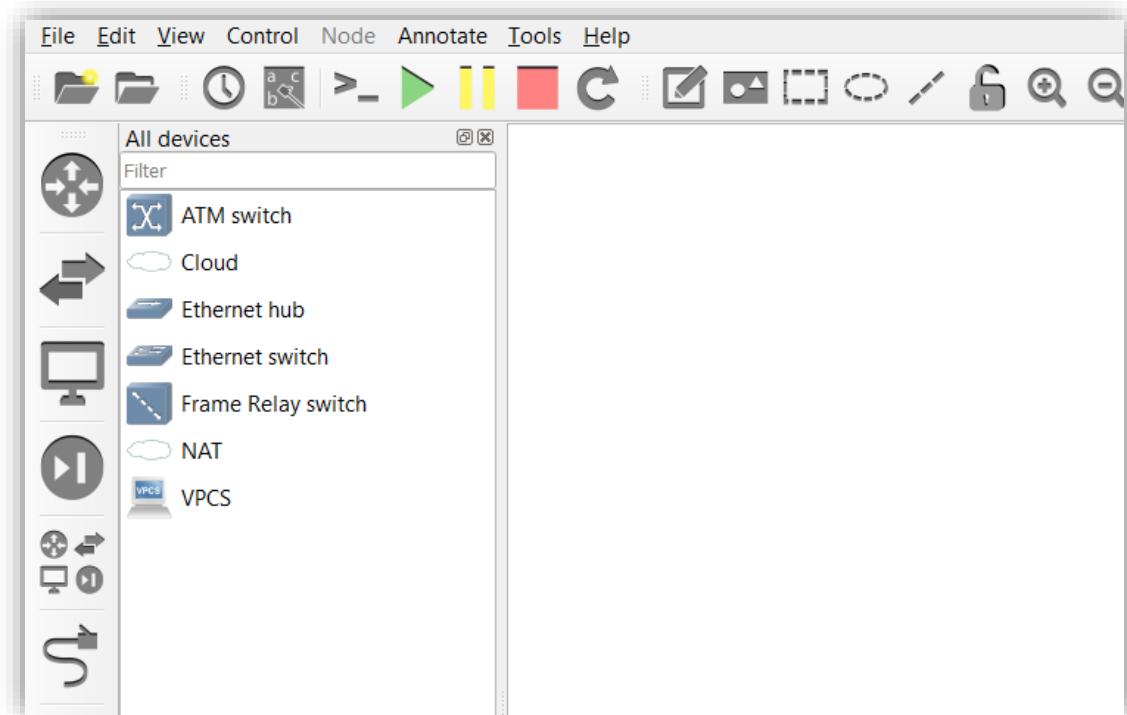


Ilustración 46: Menú previo a la instalación.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

- Una vez creado el nuevo proyecto, vamos a importar todos los «appliances» Ubuntu -aplicaciones virtuales de Ubuntu-.
- Para ello, dirígete a la página web de GNS3.

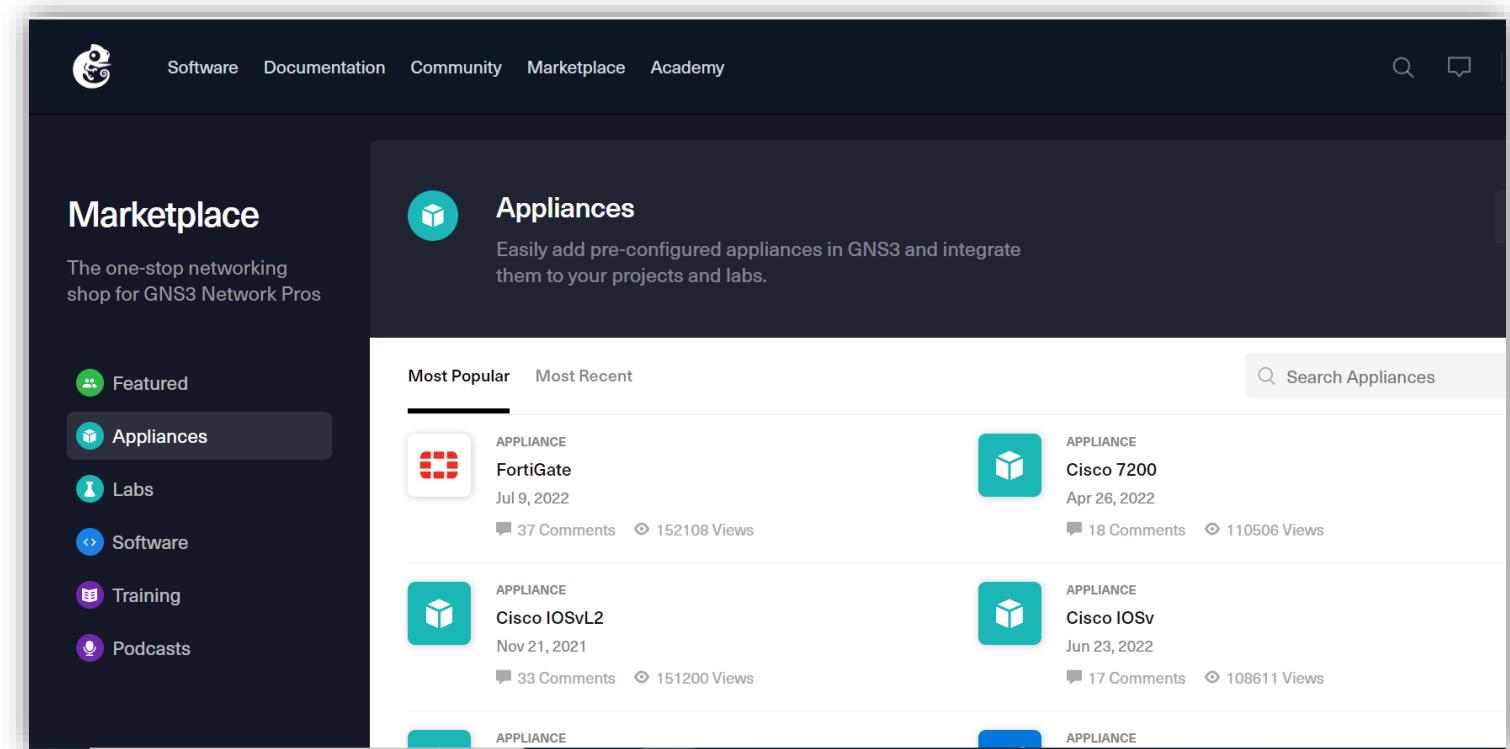


Ilustración 47: Importar todos los «appliances» Ubuntu.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

- En esta página busca «Ubuntu Desktop Guest» y descarga el archivo «.gns3a».

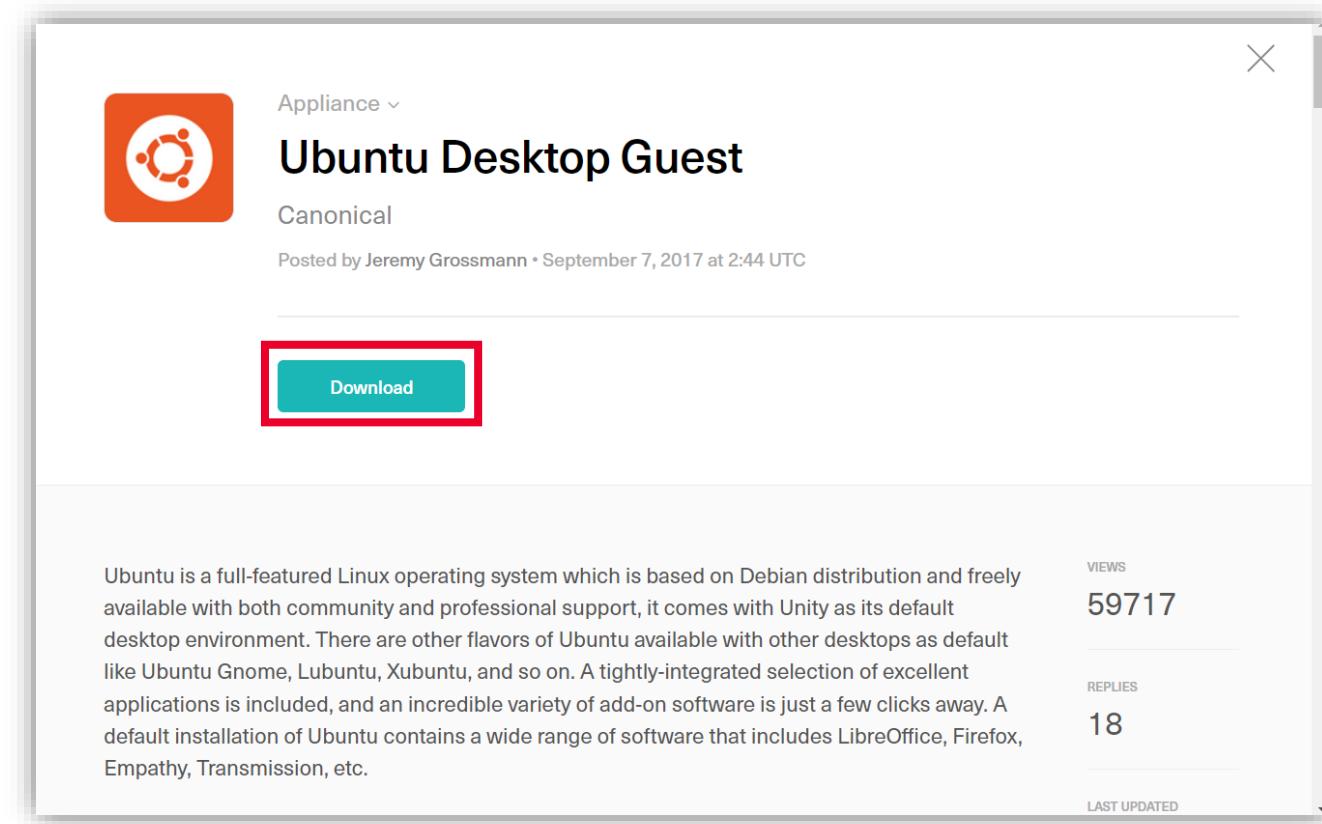


Ilustración 48: Descargar el archivo «gns3a».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

- Guarda el archivo descargado en la carpeta donde estés almacenando todo lo relacionado con esta práctica.
- Cuando se haya descargado el archivo vuelve al entorno gráfico de GNS3 y desde ahí accede al menú «File» y ahí dentro a «Import Appliance».

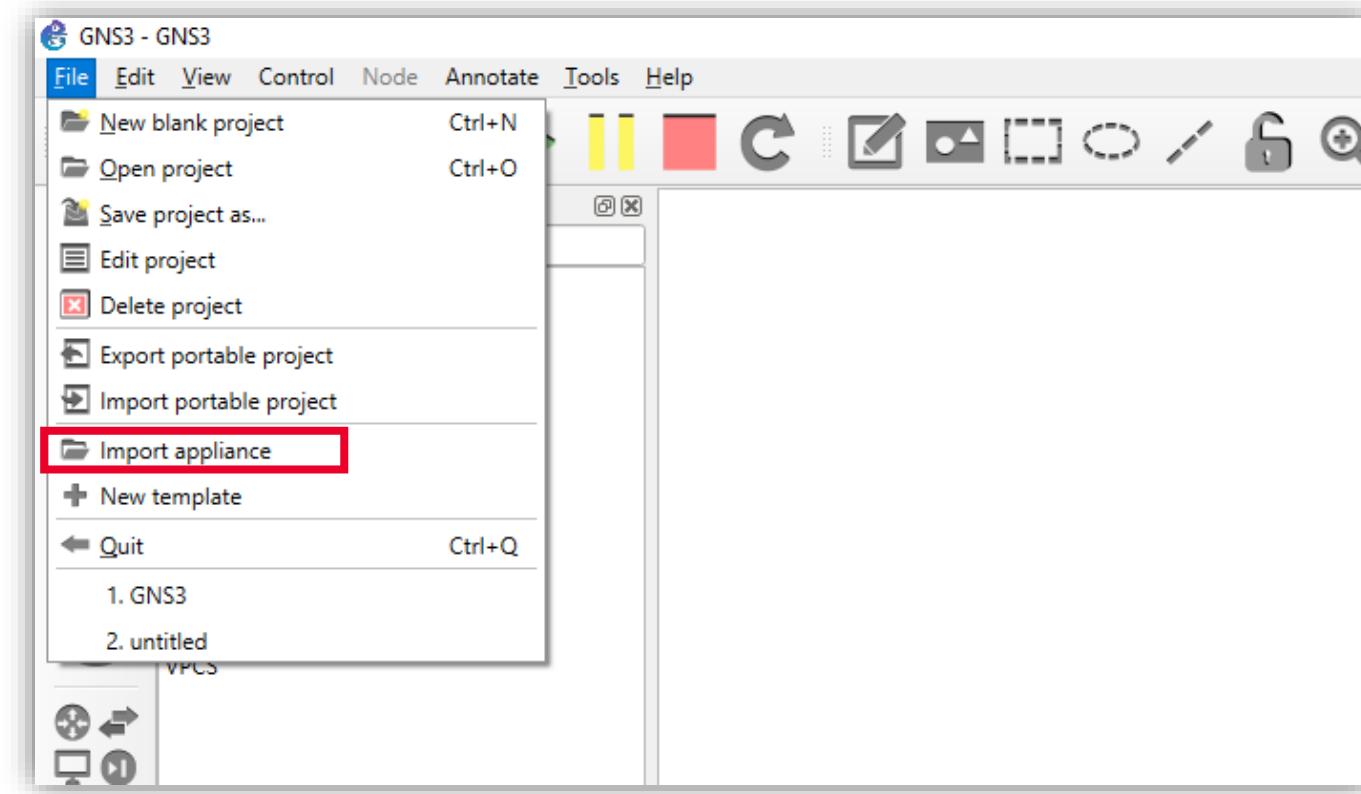


Ilustración 49: Menú «Import Appliance».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

- Se abrirá una ventana emergente en la que debes buscar y seleccionar el archivo descargado anteriormente.
- Selecciona «*Install the appliance on the main server*» y clic en «*Next*».

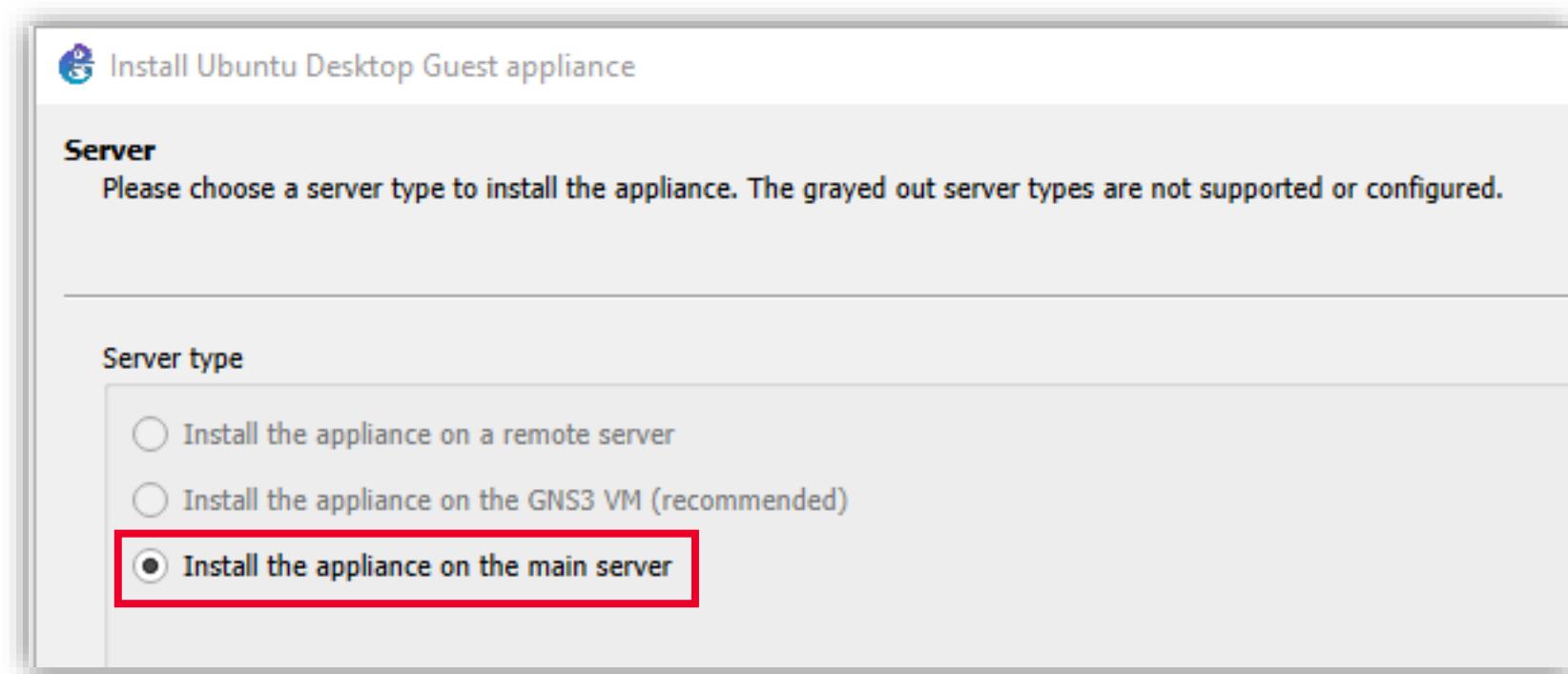


Ilustración 50: «Instalar el dispositivo en el servidor principal».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

- En la siguiente ventana, haz clic en «Next».

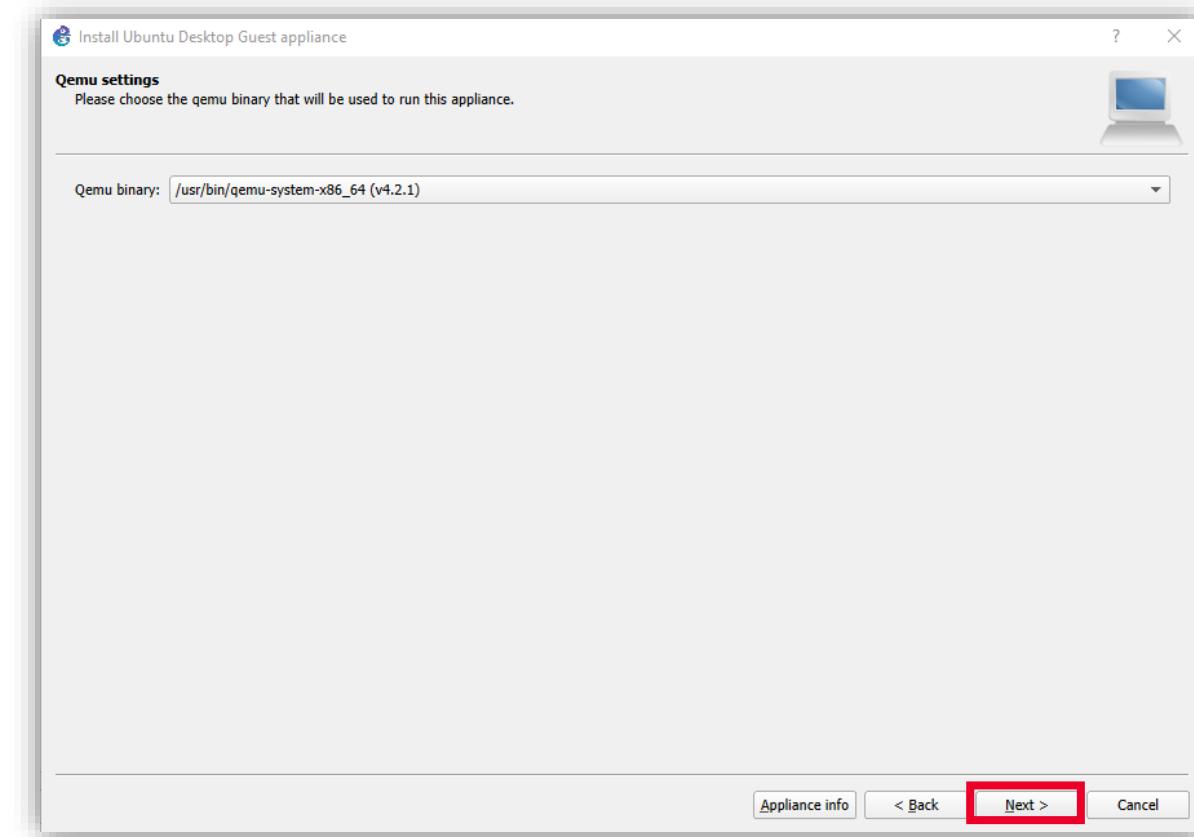


Ilustración 51: Clic en «next».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

- La siguiente ventana muestra que para este *appliance* faltan algunos archivos adicionales, en este caso, la imagen de la máquina virtual para cada uno.
- Selecciona la última versión y haz clic en «*Download*», te redirigirá directamente a la página de Ubuntu.

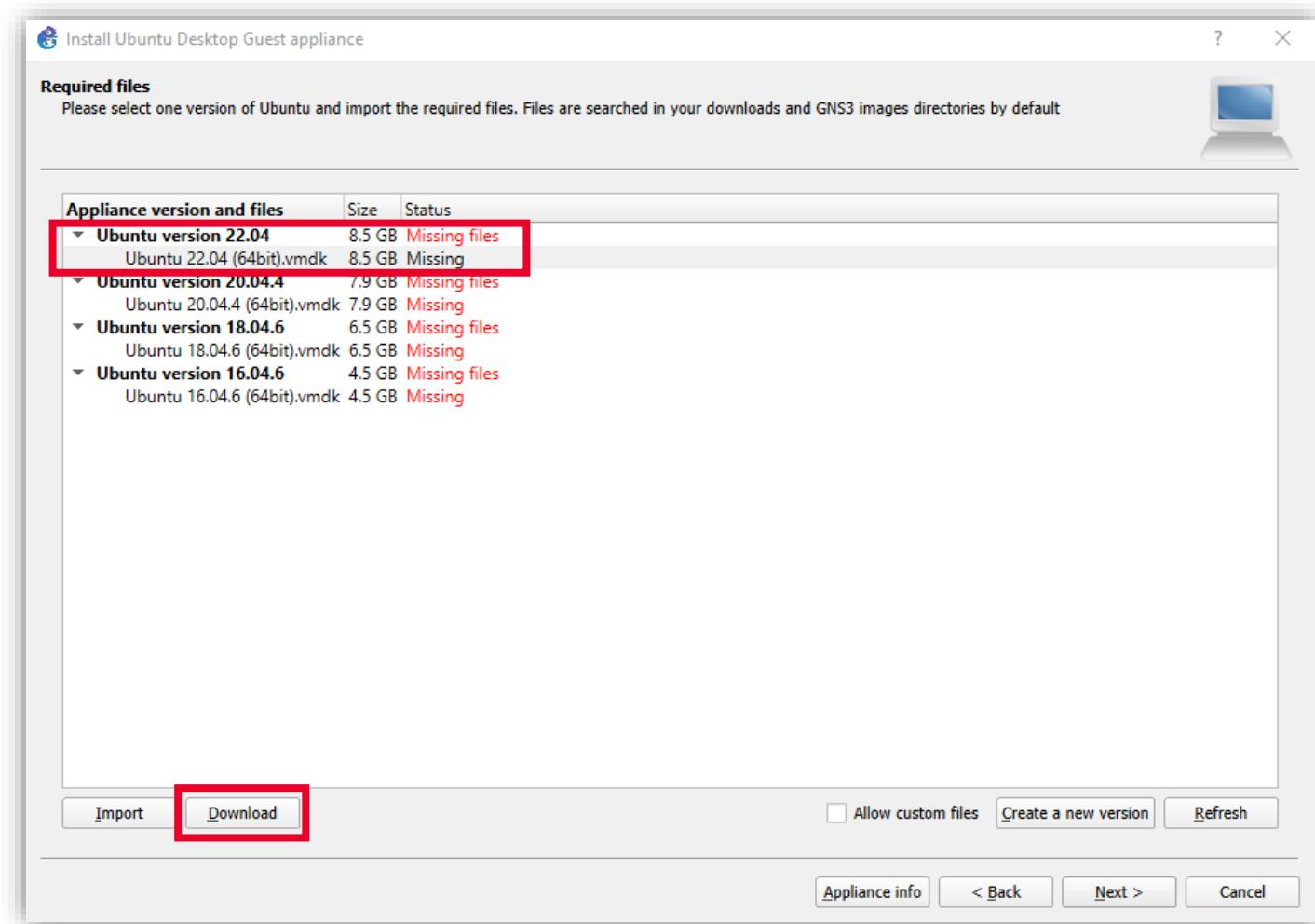


Ilustración 52: Pulsa en la última versión y clic en «*Download*».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

- En esta página descarga la última versión para VMWare.

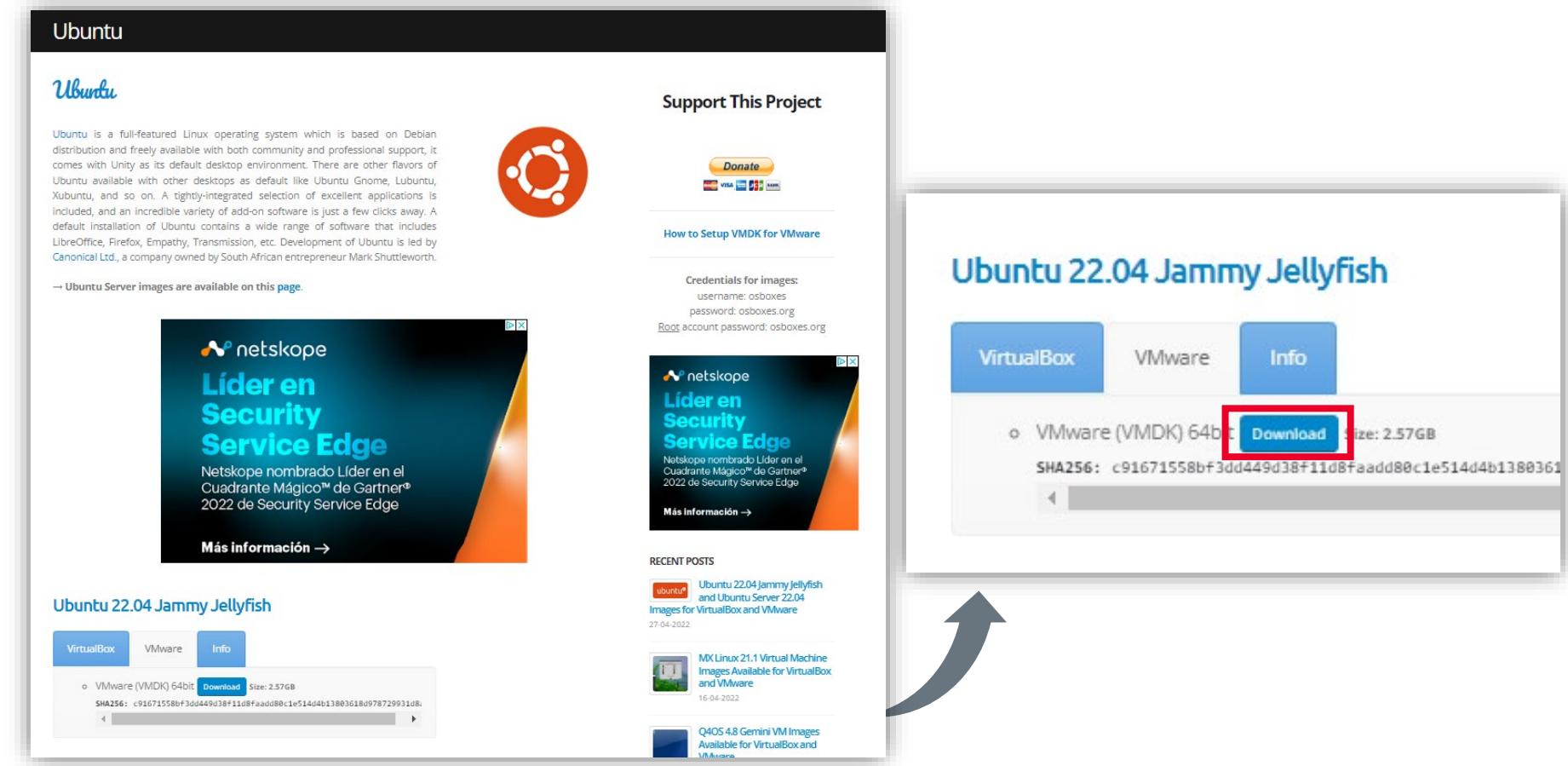


Ilustración 53: Descarga la última versión para VMWare.



3 INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

- Se descargará un archivo «.zip» el cual deberás descomprimir en la carpeta deseada que recomendamos que sea en la que estás almacenando toda la información de estas prácticas. Cuando esté listo, vuelve al entorno gráfico de GNS3 para importarlo.
- Haz clic en «*Import*» para seleccionar el archivo (Ubuntu 22.04 (64 bit) antes descargado.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

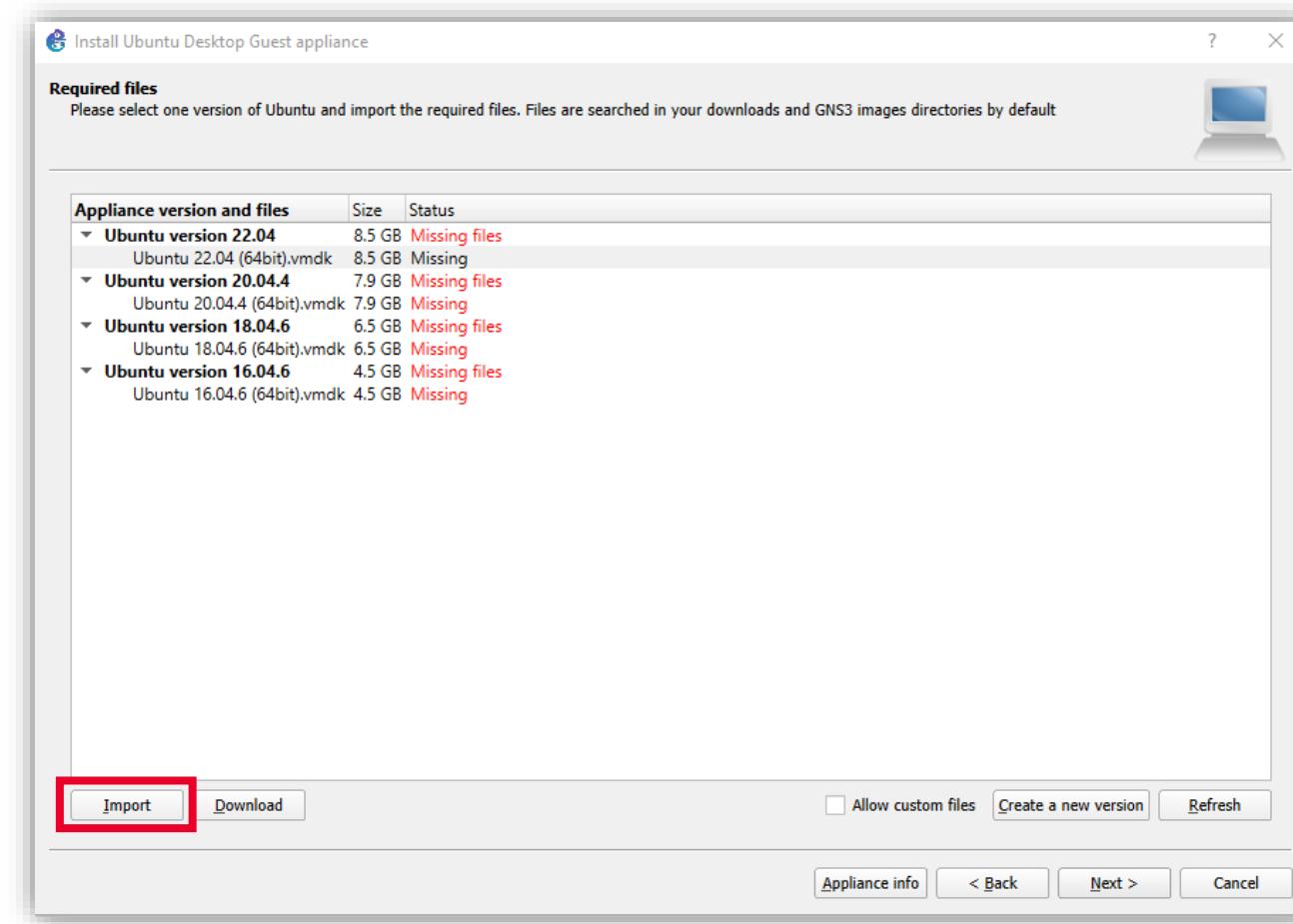


Ilustración 54: Clic en «Import».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

- Una vez seleccionado este archivo se abrirá directamente una ventana con el proceso de importación.

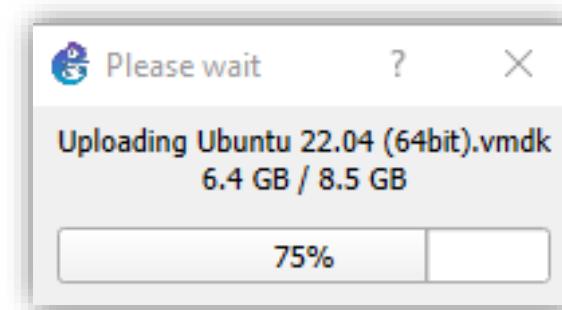


Ilustración 55: Ventana emergente con el proceso de importación.

- Espera mientras se realiza este proceso.
- Una vez terminado, aparecerá que «*Missing files*» ha cambiado a «*Ready to install*».
- Haz clic en «*Next*».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

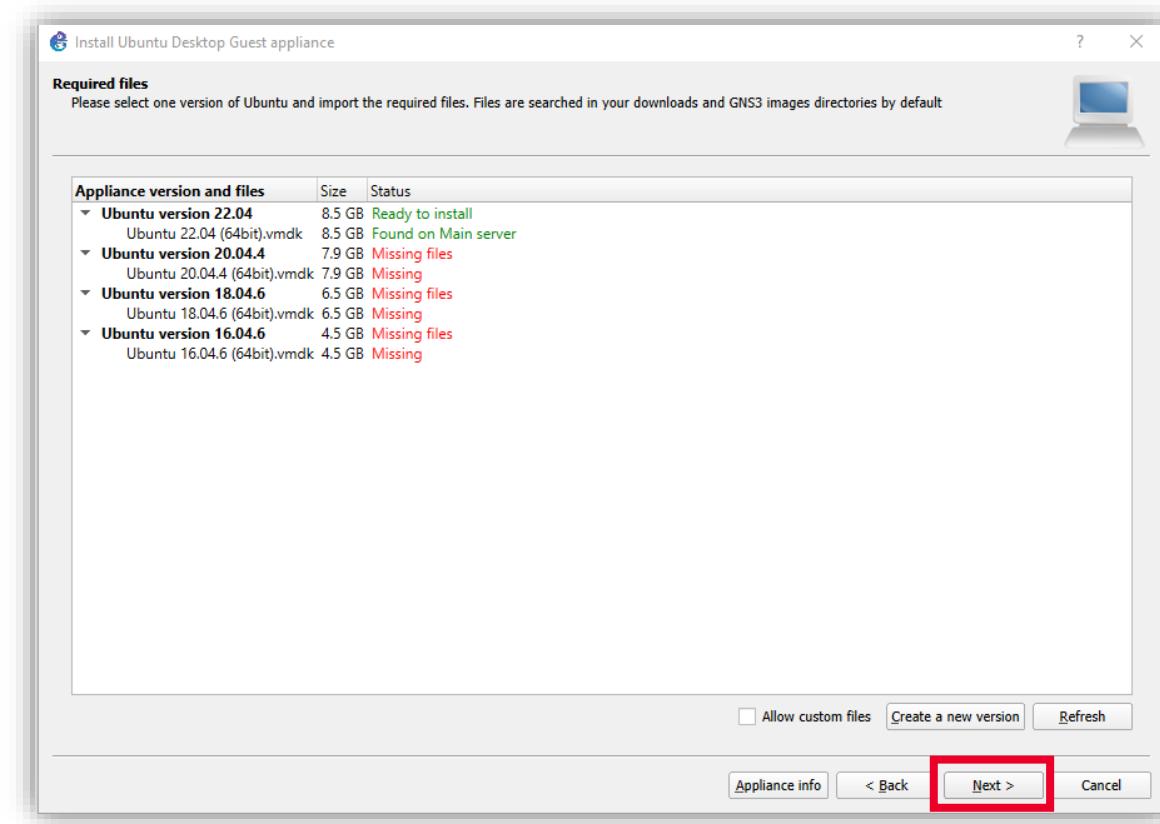


Ilustración 56: «Ubuntu 22.04 (64bit).vmdk» ha cambiado a «ready to install».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

- Acepta el aviso de confirmación.

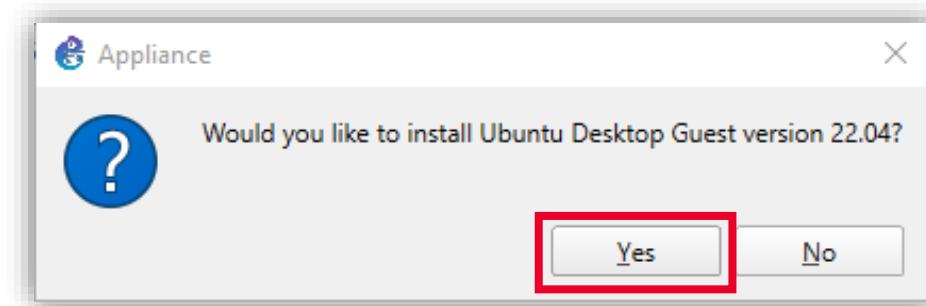


Ilustración 57: Aviso de confirmación.

- Aparecerá «usuario» y «contraseña» de la máquina virtual. Almacena bien estos valores porque los utilizarás más adelante.
- Haz clic en «Finish» y tendrás instalado el nuevo «appliance».

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

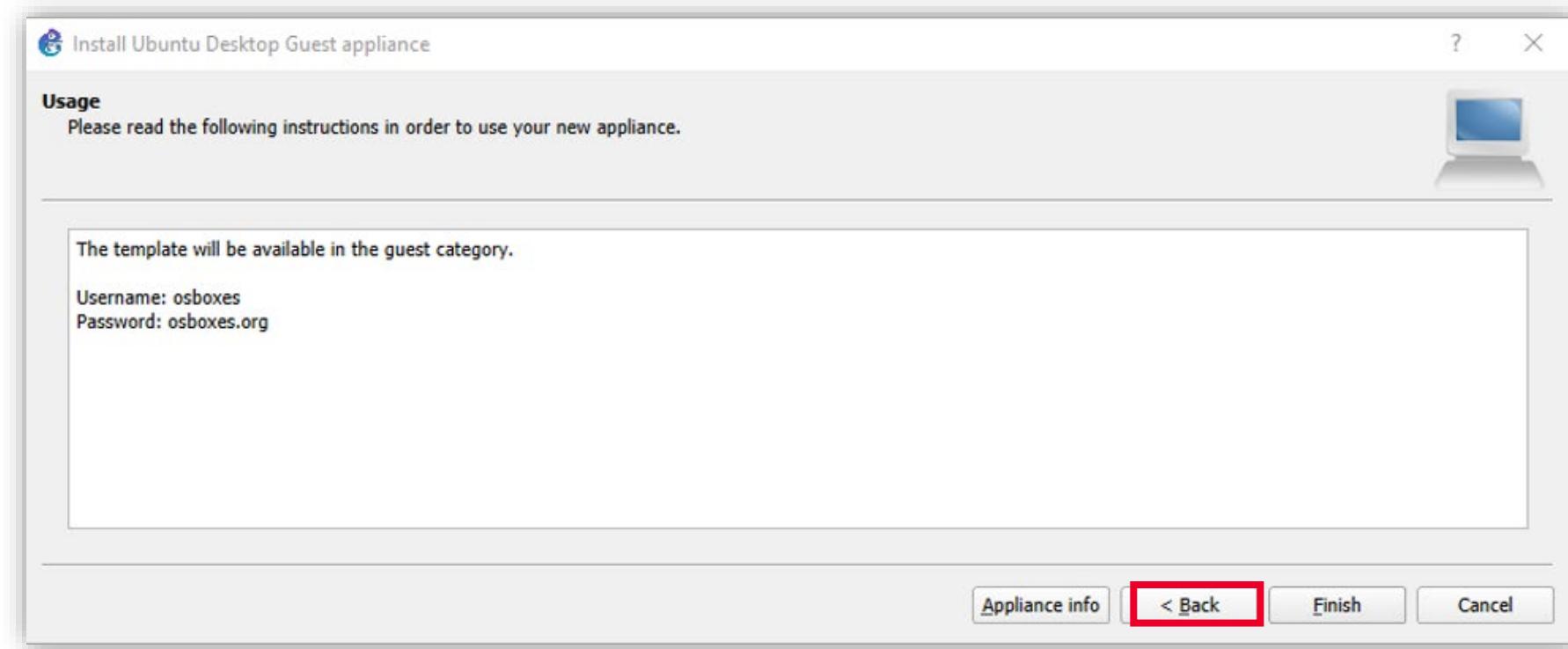


Ilustración 58: Usuario y contraseña de la máquina virtual.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

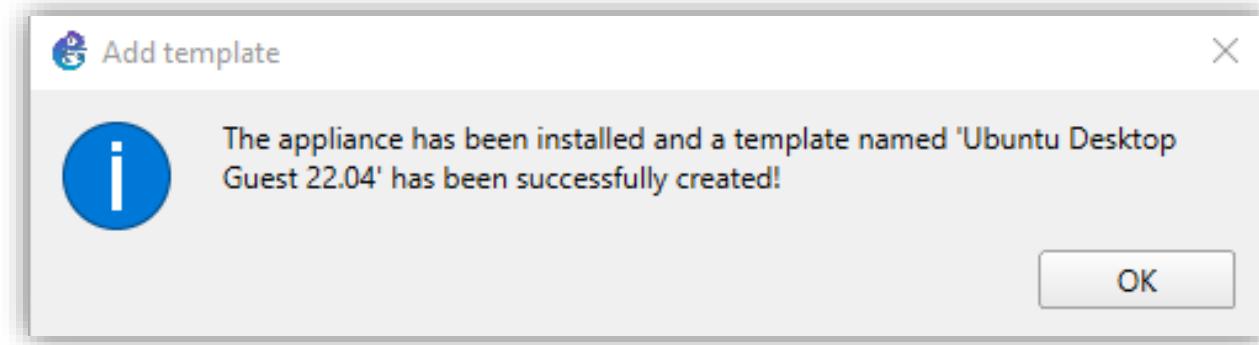


Ilustración 59: Confirmación de que la aplicación se instaló correctamente.

3

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

3.5.1 Instalación y configuración de aplicaciones virtuales

- En el menú de «All devices» de la izquierda, deberá aparecer una máquina, *host*, con Ubuntu.

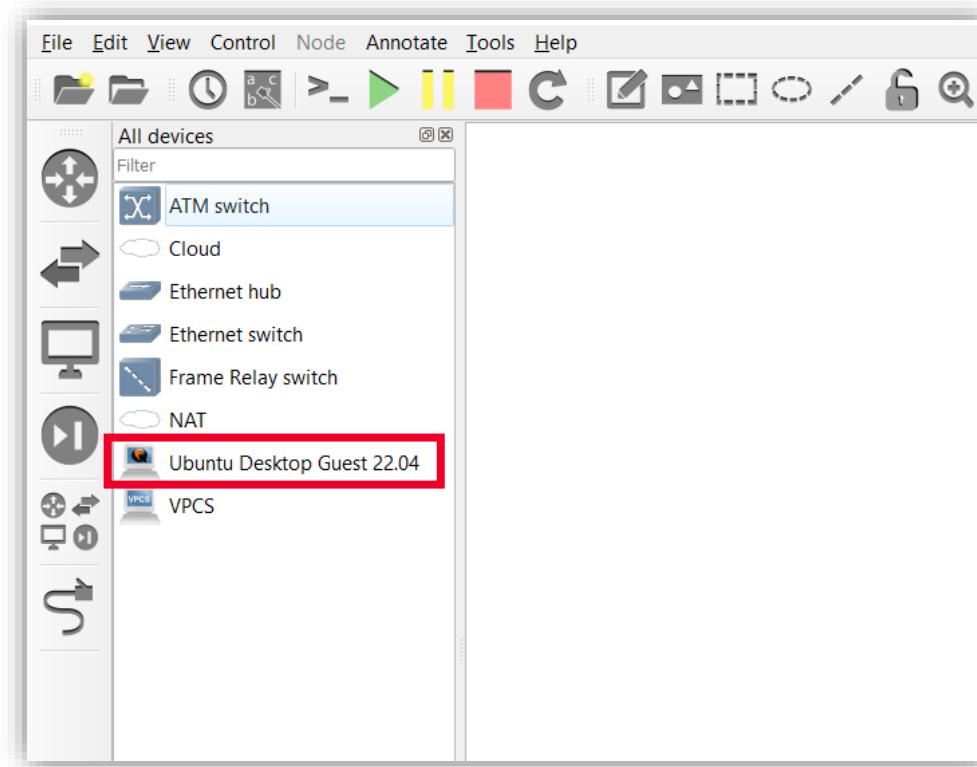


Ilustración 60: «Ubuntu Desktop Guest 22.04»
aparece en el menú.

PRÁCTICA: HOST CON ACCESO A INTERNET

4



4

PRÁCTICA: HOST CON ACCESO A INTERNET

En esta primera parte de la práctica crearás un proyecto el cual contenga un *host* (Ubuntu) con acceso a Internet.

- Dentro del servidor GNS3,
arrastra la máquina Ubuntu hacia
la pantalla en blanco y haz lo
mismo con el elemento «*Cloud*».

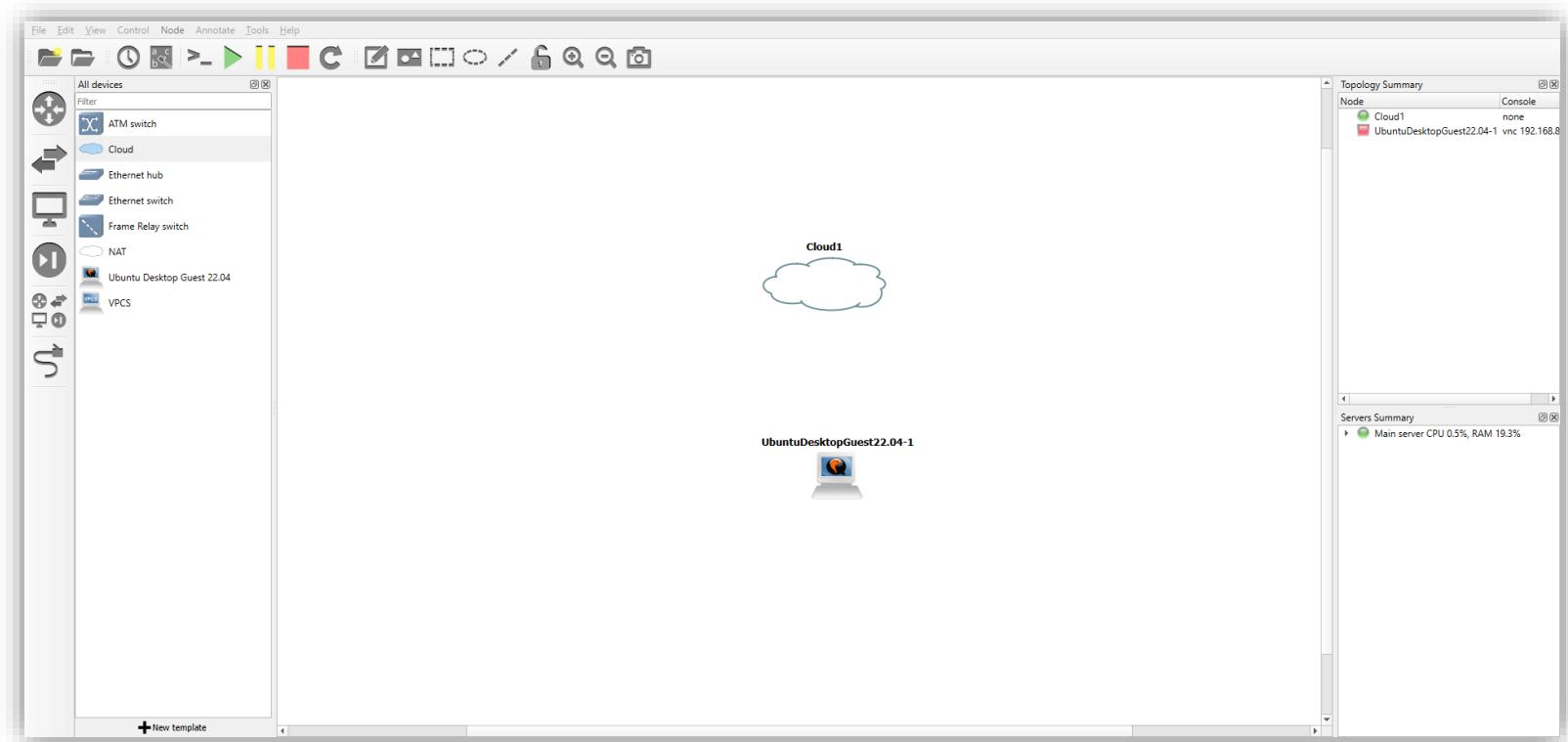


Ilustración 61: Arrastra la máquina Ubuntu y el elemento «*Cloud*».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Cuando ya tengas esto en la pantalla haz clic sobre el icono del cable «*Add link*» para conectarlos entre sí.

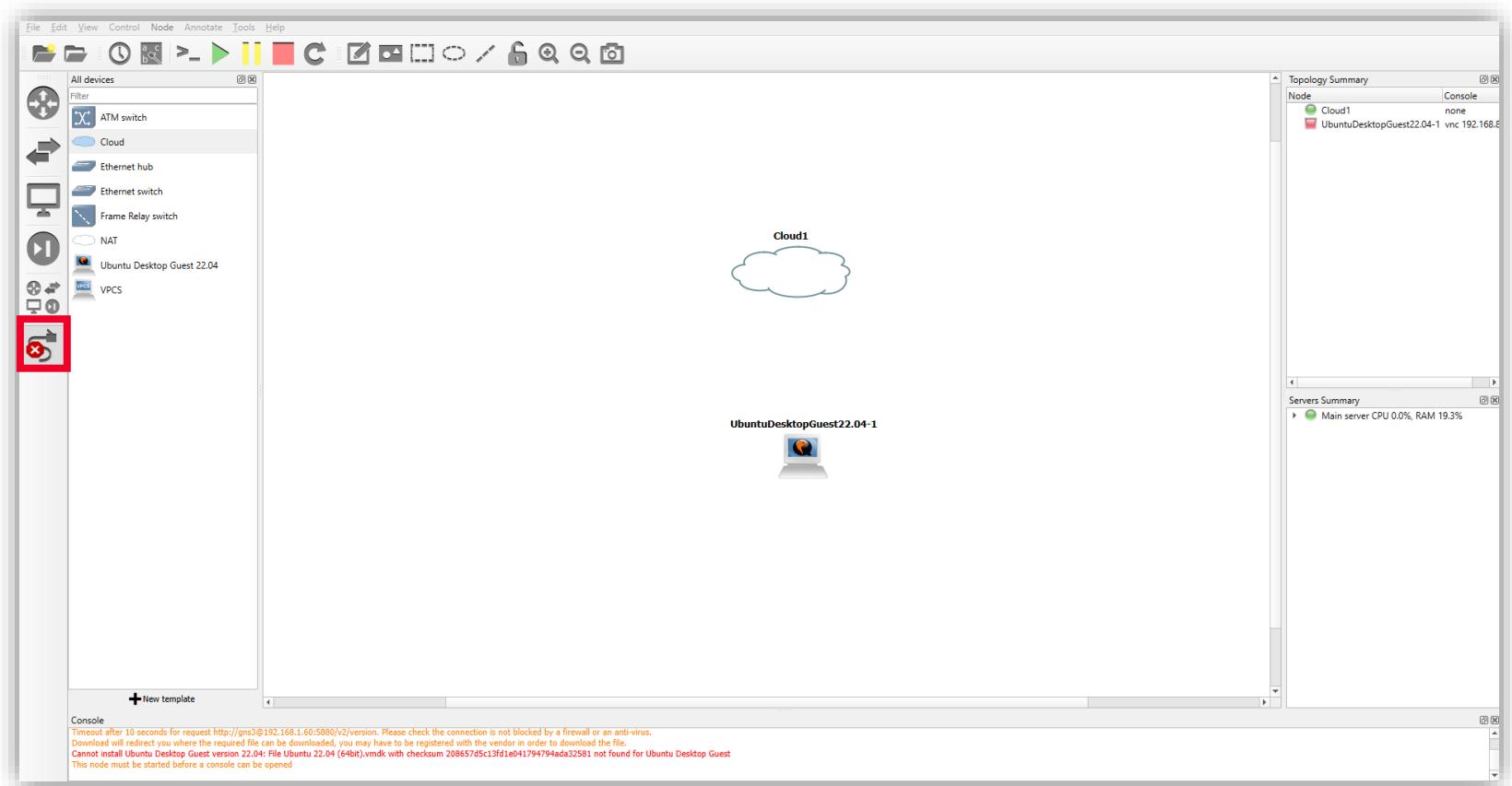


Ilustración 62: Clic sobre el ícono del cable «*Add link*».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Al hacer clic sobre el *host*. Saldrán las interfaces (puertos ethernet) disponibles para conectar. En este caso, «*eth0*». Haz clic en él.

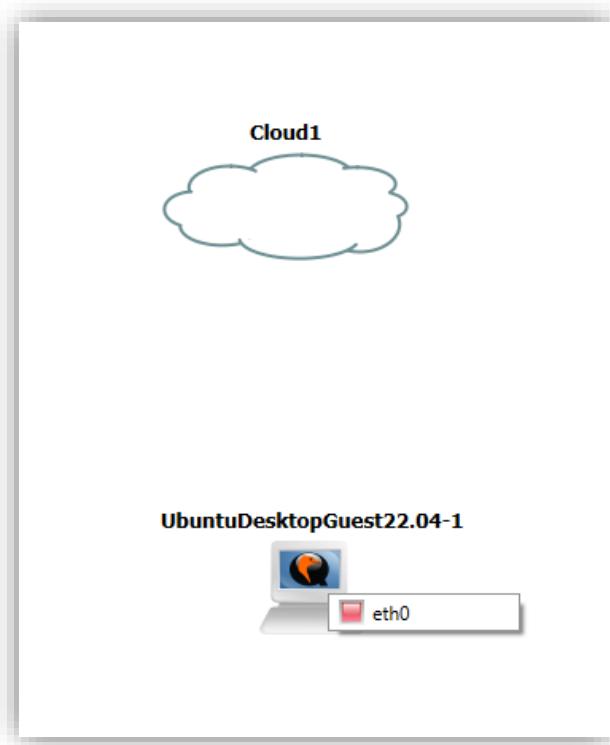


Ilustración 63: Clic sobre «*eth0*».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Cuando hayas pulsado «eth0» aparecerá una línea, llévala hasta la «Cloud» y vuelve a seleccionar «eth0».
- Mediante una serie de puntos de colores, GNS3 nos indica el estado de la conexión en tiempo real. En este caso, como aún no has encendido el ordenador, hay acceso a Internet, pero la máquina Ubuntu aparece en rojo.

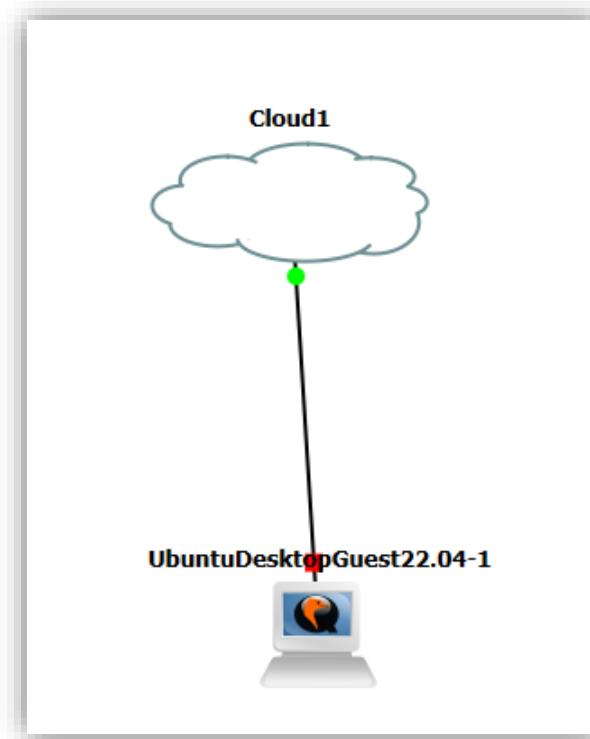


Ilustración 64: Con conexión a Internet, pero la máquina está apagada.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Haz clic con el botón derecho sobre la máquina Ubuntu y pulsa «Start».

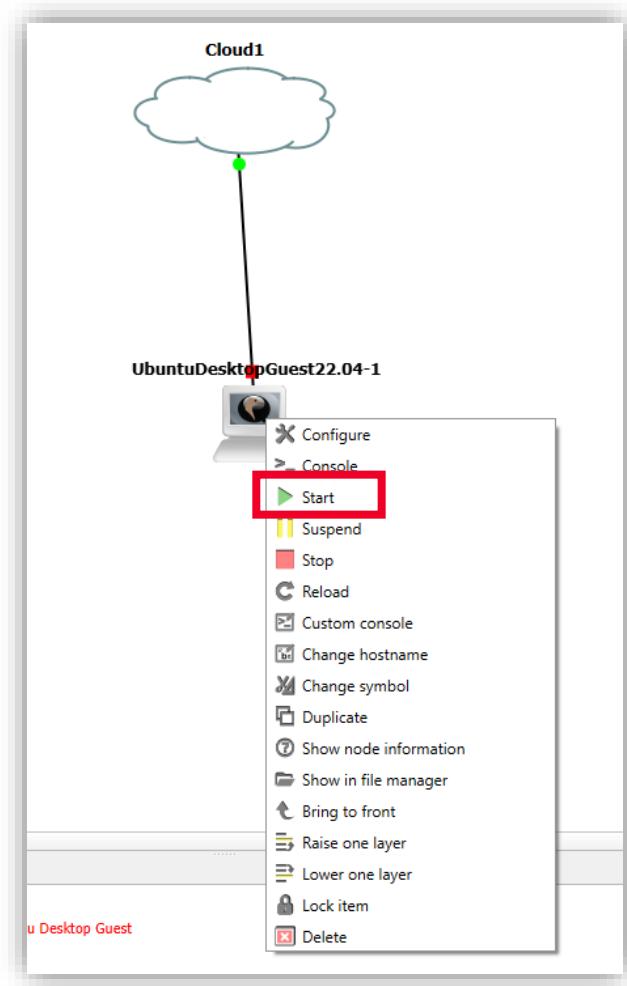


Ilustración 65: Pulsa «Start».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Vuelve a hacer clic derecho sobre la máquina y pulsa «Console».

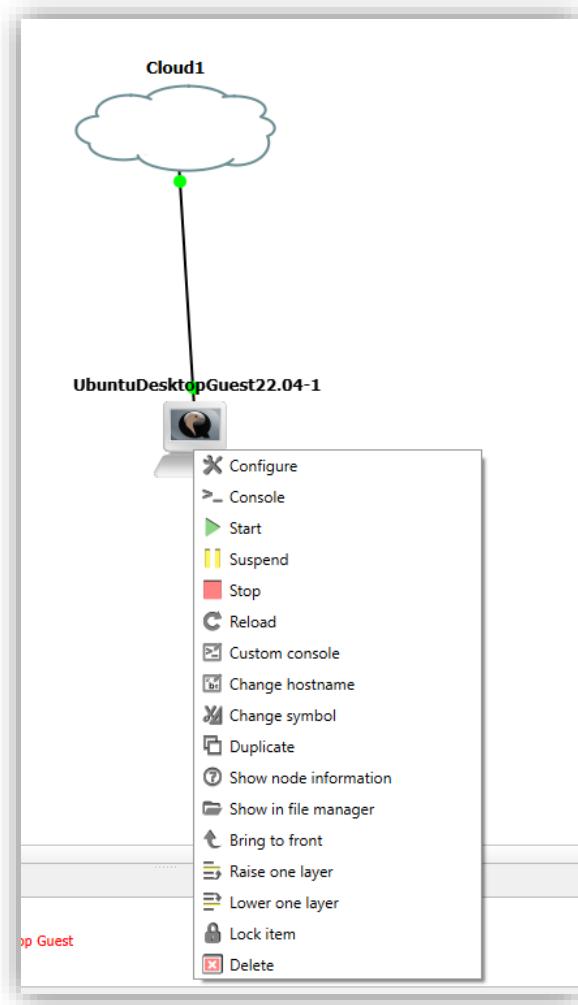


Ilustración 66: Abre la máquina y pulsa «Console».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Se abrirá directamente la interfaz gráfica de la máquina Ubuntu, en la cual deberás hacer *log in* con el usuario y la contraseña que antes nos proporcionó (osboxes/osboxes.org).

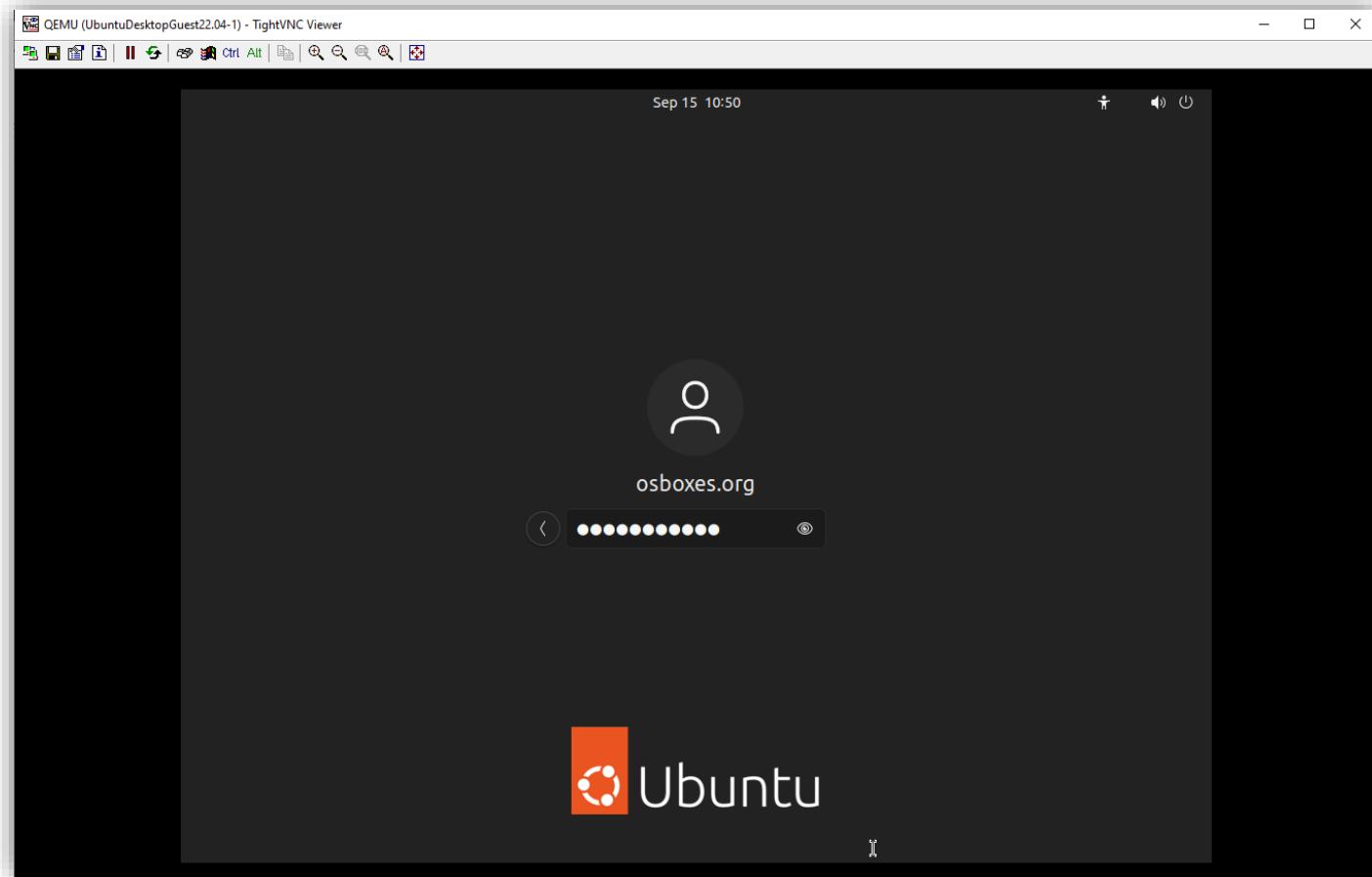


Ilustración 67: Accedemos a «osboxes.org» con usuario y contraseña.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Abre una terminal. Para ello, pulsa sobre el icono situado en la esquina inferior izquierda «Show Applications» y aparecerá entre ellas «Terminal». Si no aparece en la pantalla principal puedes utilizar el buscador y aparecerá directamente.

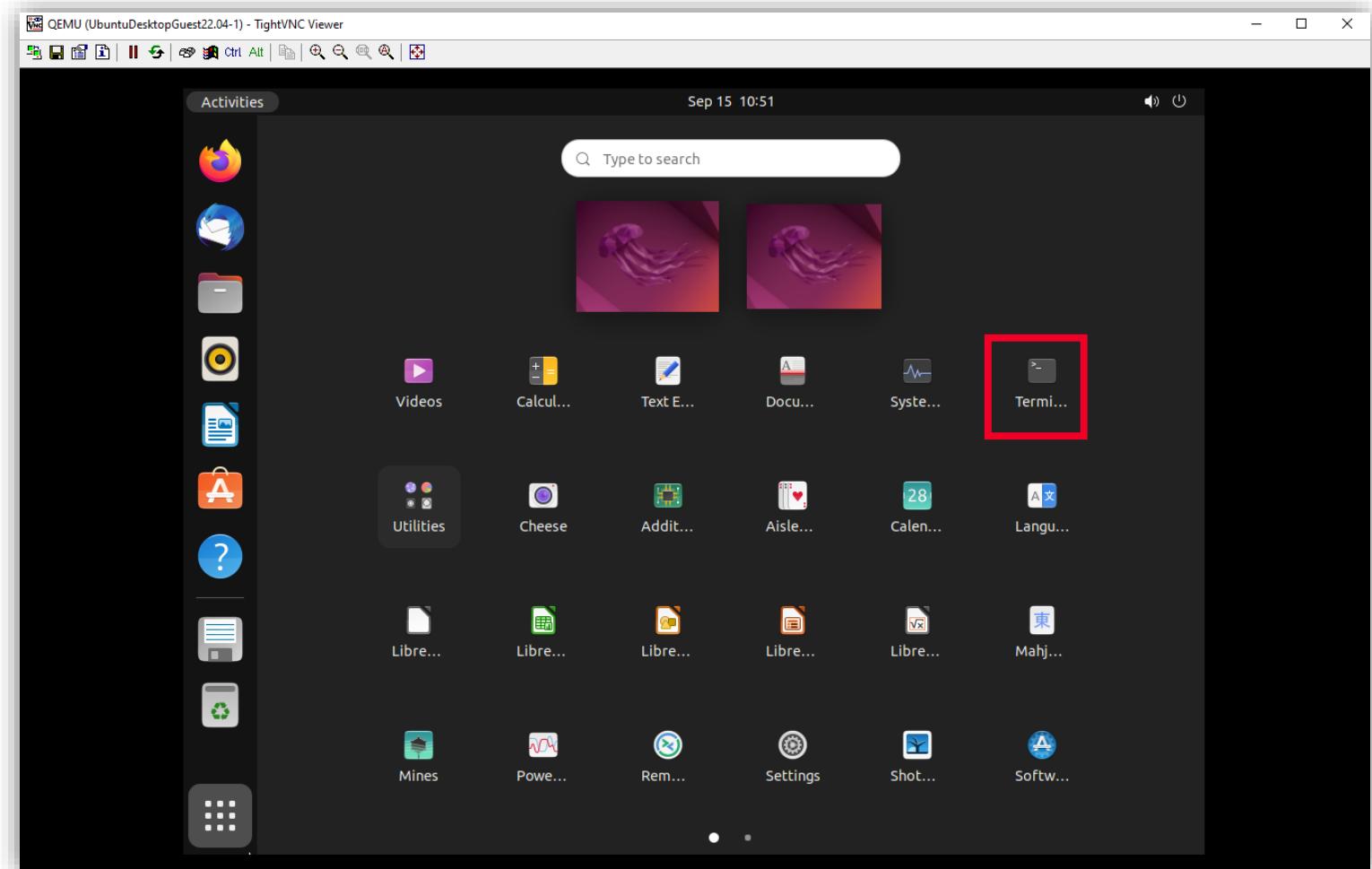


Ilustración 68: Abrimos una «Terminal».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Verás que, si introducimos el comando «**ping 8.8.8.8**» o «**ping www.google.es**» no tendremos respuesta, es decir, todavía no tenemos acceso a Internet.

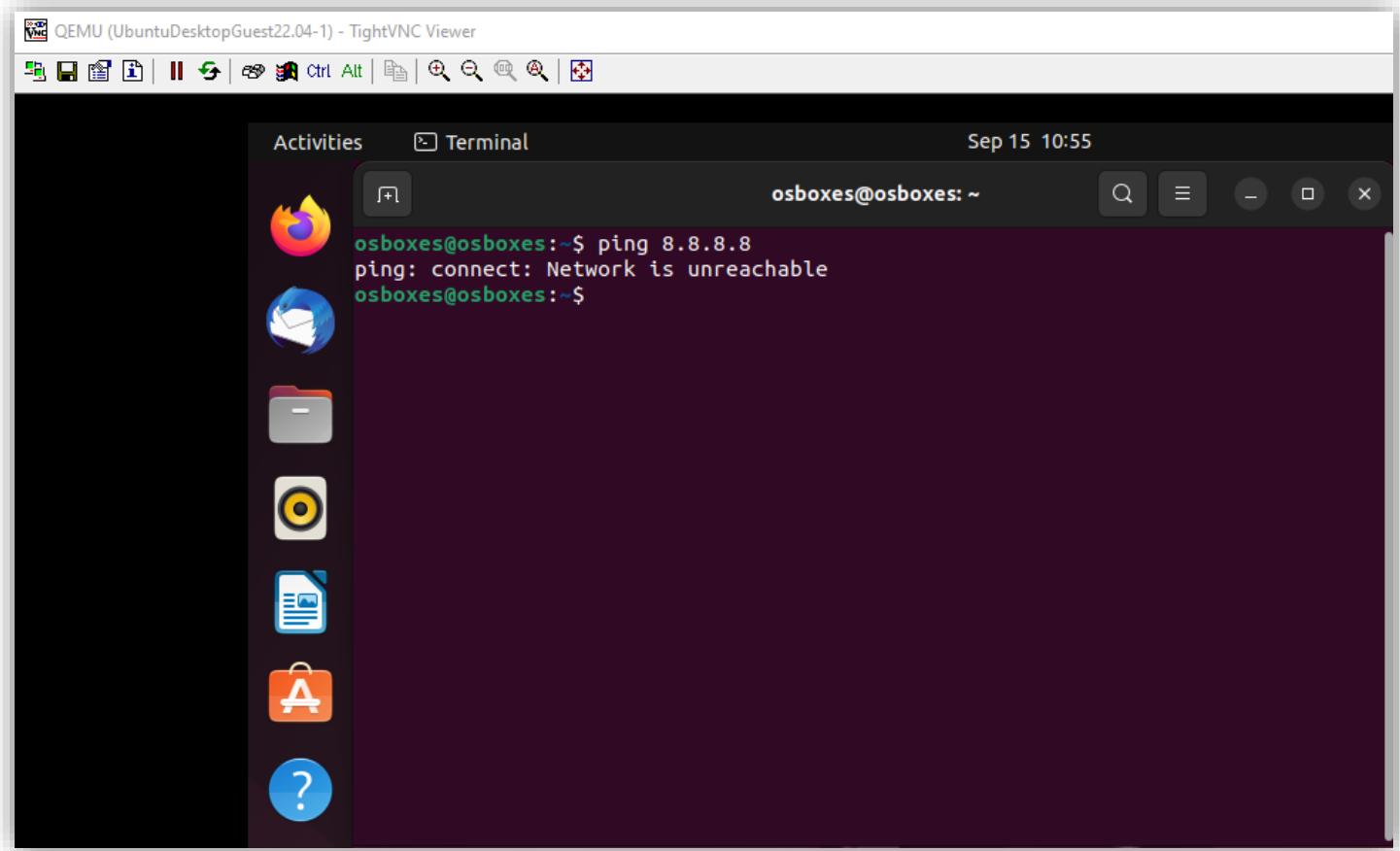


Ilustración 69: Comprobamos que no tenemos acceso a Internet.



PRÁCTICA: HOST CON ACCESO A INTERNET

- Como no tienes en tu arquitectura ningún *router* de por medio que ofrezca DHCP no tienes acceso a Internet, por lo que, el siguiente paso será descargar y añadir uno.
- Para ello, tendrás que volver a la página de «*Appliances*» de GNS3.
- Deberás descargar el *router* OpenWRT. Para encontrarlo utiliza el buscador.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

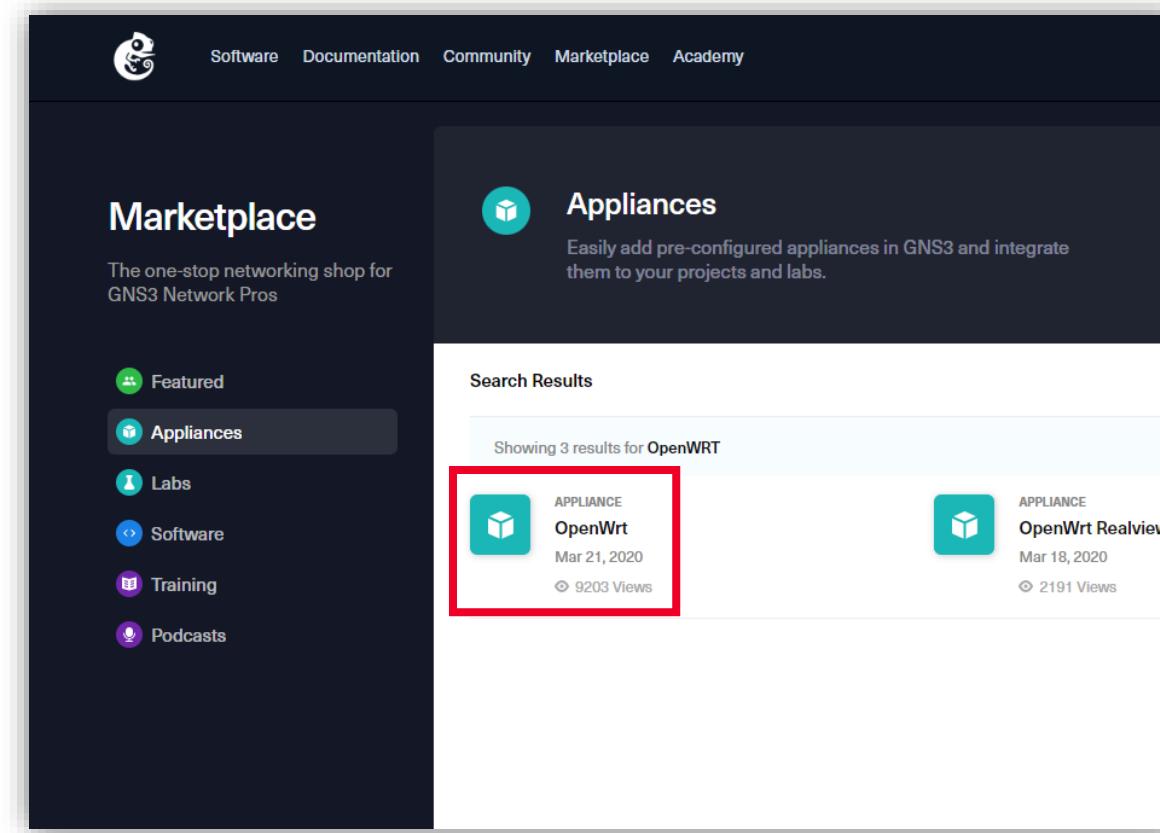


Ilustración 70: Buscamos OpenWrt.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Selecciona «OpenWrt» y pulsa «Download». Con esto te descargarás «.gns3a» del *router* de OpenWrt.

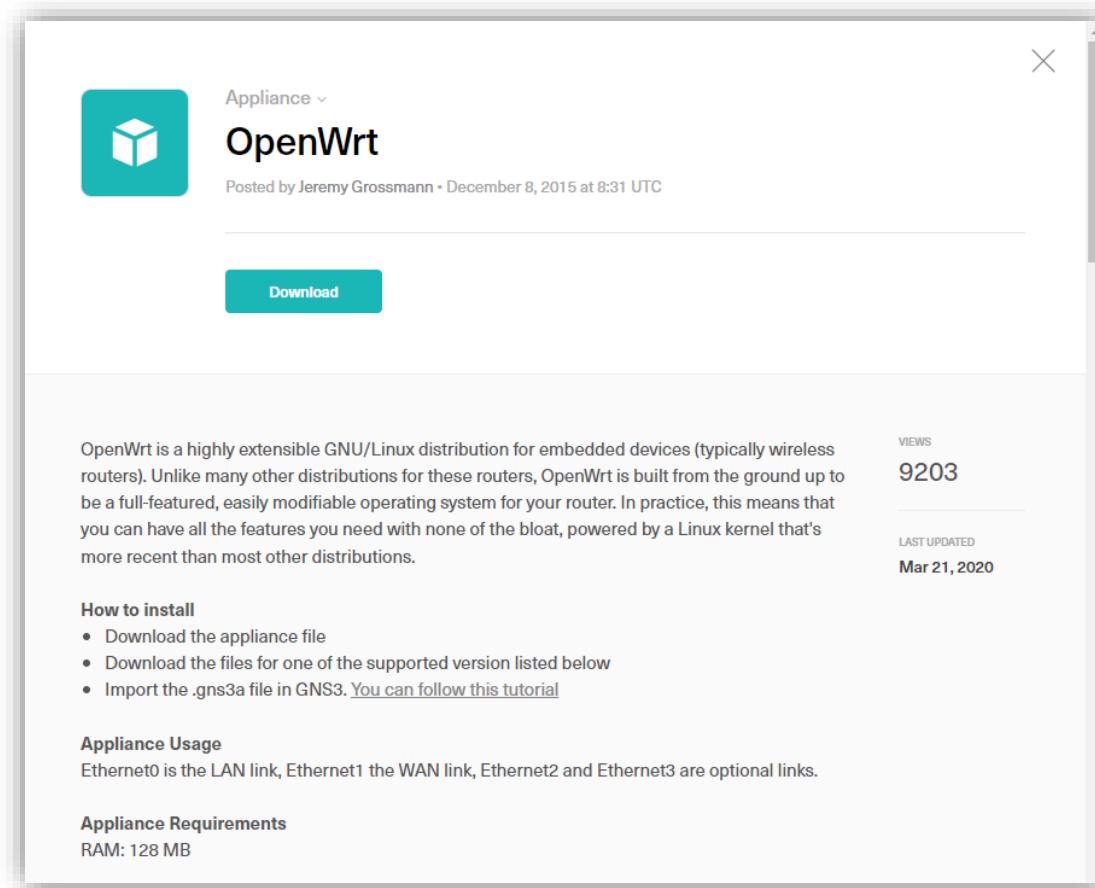


Ilustración 71: Descarga OpenWrt.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- También necesitarás la imagen de este *router*, por lo que un poco más abajo en la misma página, encontrarás todas las versiones disponibles.
- Descarga la última versión.

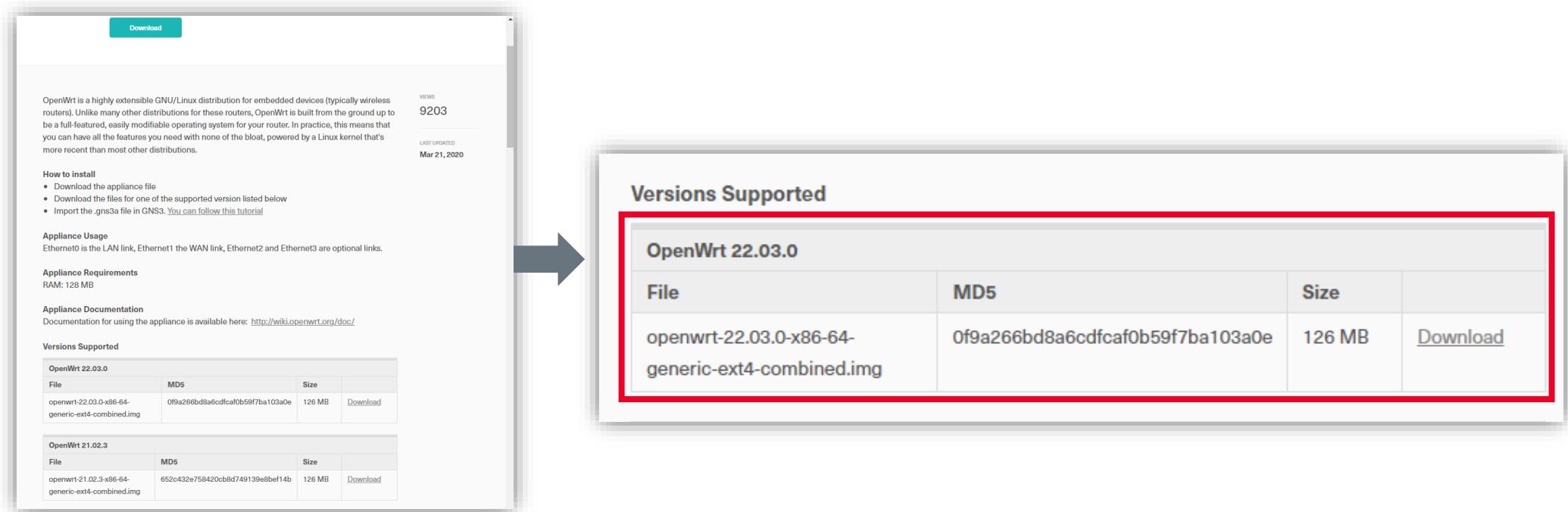


Ilustración 72: Descarga la última versión disponible de OpenWrt.



PRÁCTICA: HOST CON ACCESO A INTERNET

- Como buena práctica, te recomendamos que el archivo descargado lo almacenes en la carpeta de GNS3 donde estás almacenando todos los ficheros de esta práctica.
- Una vez descargado, ya puedes añadirlo al proyecto de GNS3, para ello, haz clic en «*File > Import Appliance*». Se abrirá un desplegable donde tendrás que localizar el archivo descargado anteriormente, selecciónalo y haz clic en abrir.
- Se volverá a abrir un desplegable en el cual deberás hacer clic en «*Next*».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

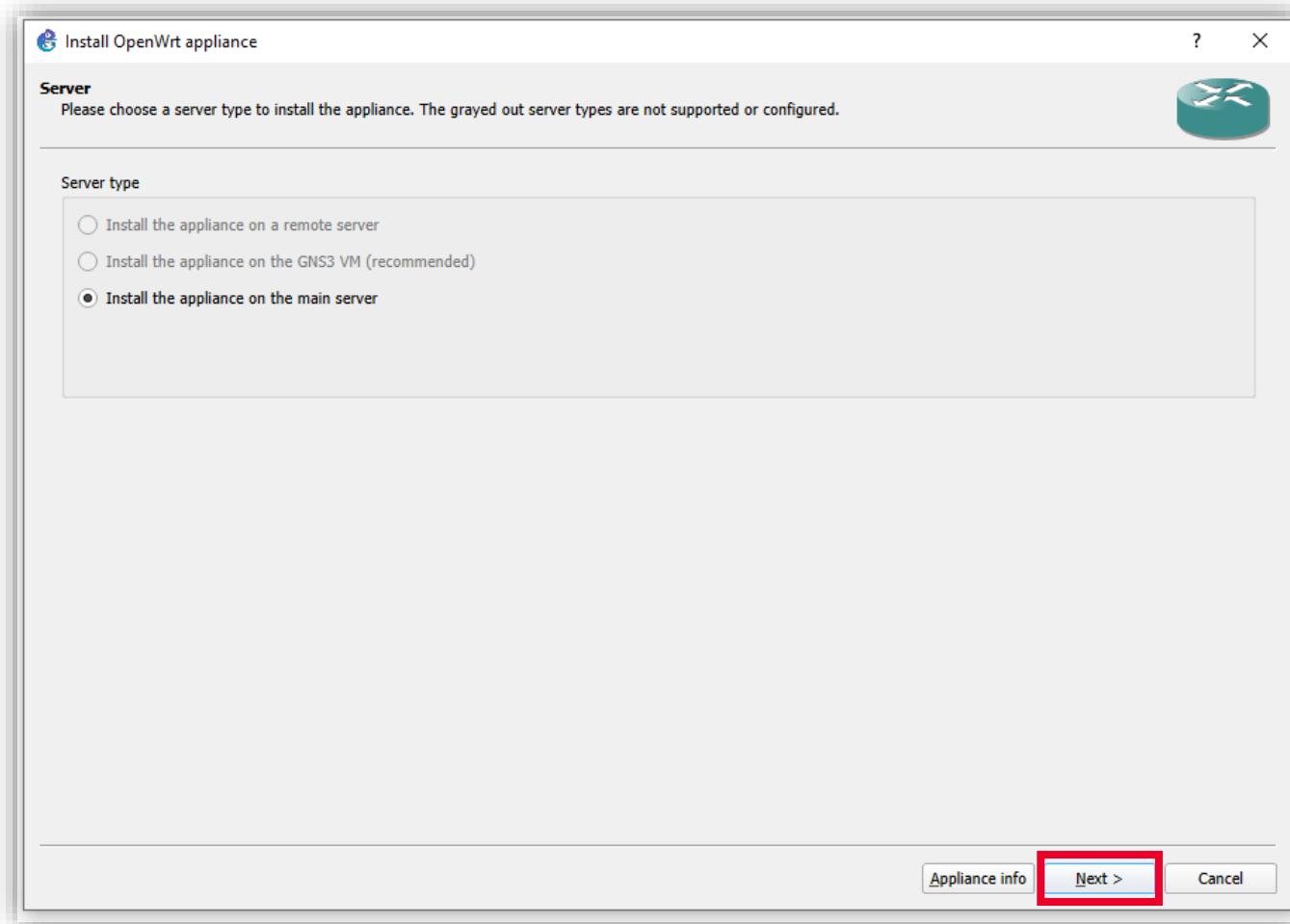


Ilustración 73: «Instala la aplicación en el servidor principal» y clic en «next».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Aparecerá otro menú en el que no debes hacer nada, ya que detectará la versión automáticamente. Simplemente haz clic en «Next».

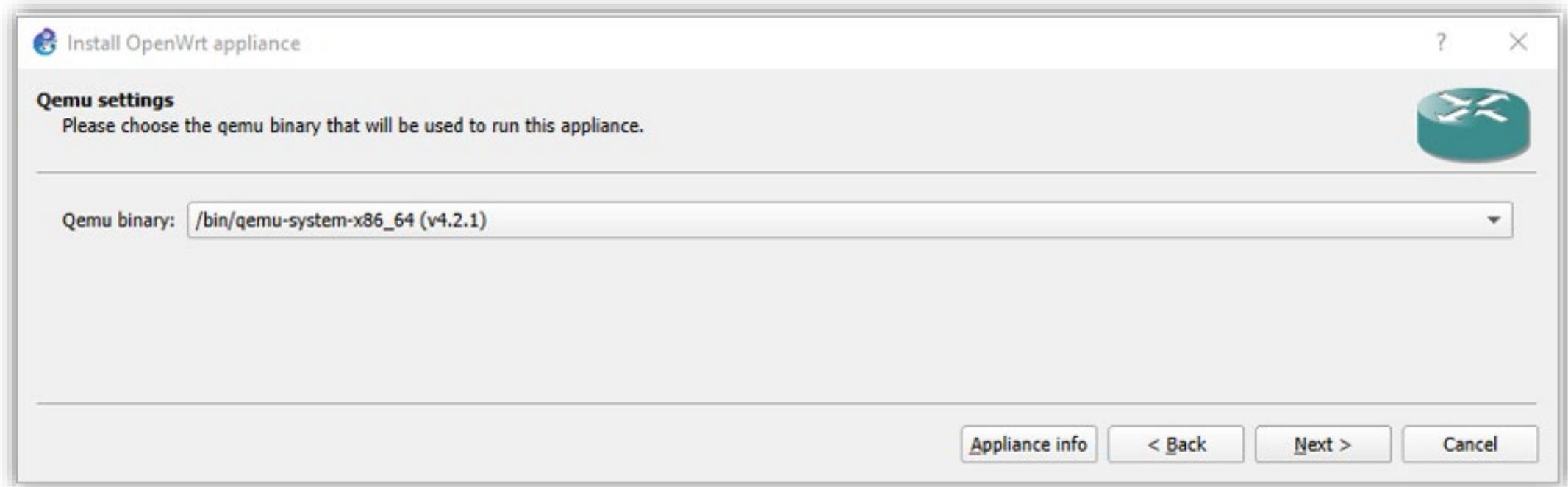


Ilustración 74: Detección automática de la versión.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Una vez aquí, aparecerán todas las versiones disponibles de OpenWrt para instalar. Debes seleccionar la versión del archivo que has descargado anteriormente. En nuestro caso es la 22.03.0.

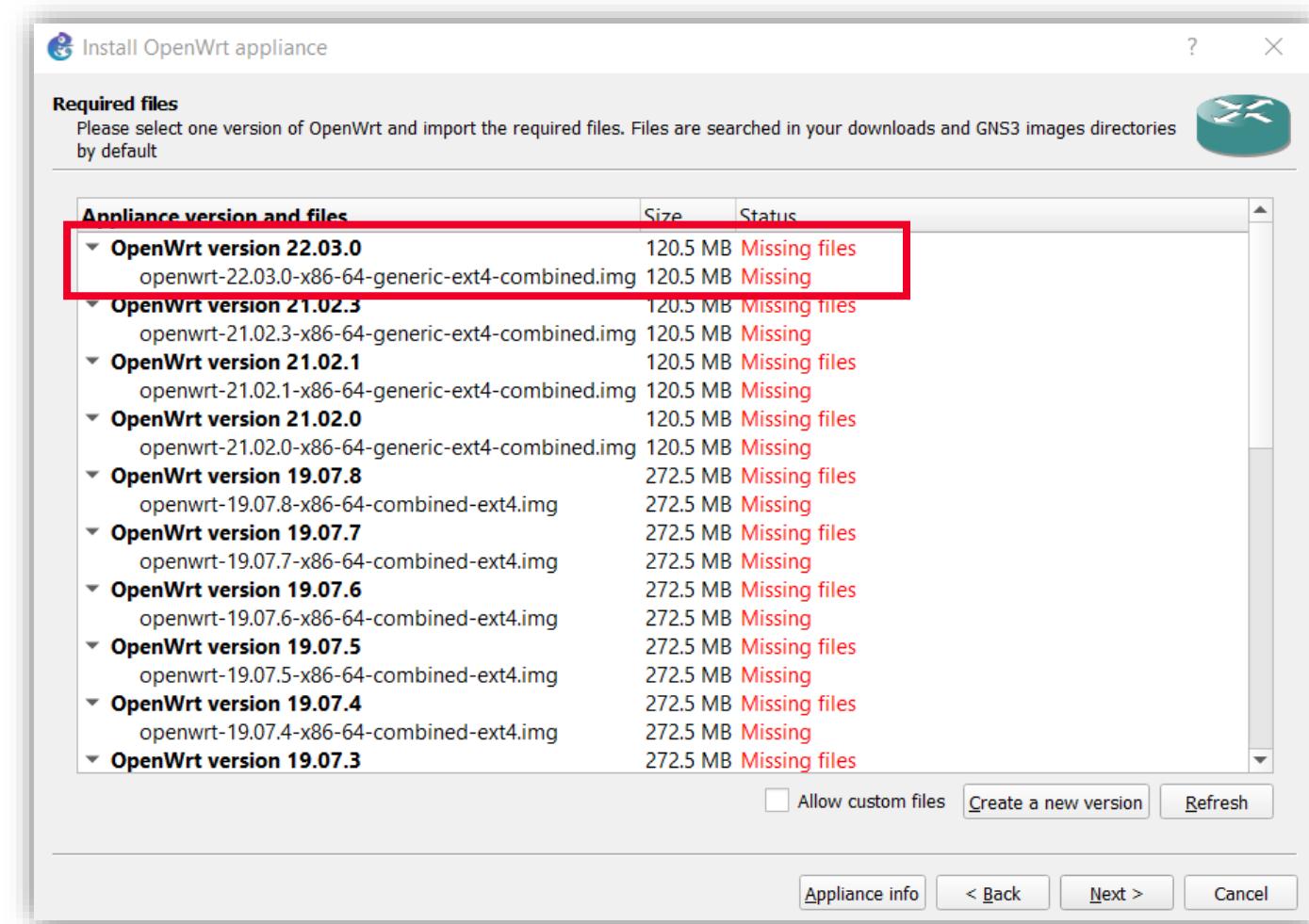


Ilustración 75: Selecciona la versión del archivo que has descargado anteriormente.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Como puedes observar indica que no encuentra los archivos para instalarla.

Para subir el archivo haz clic en la versión indicada y en el desplegable que aparece vuelve a hacer clic en él.

- Cuando lo hagas aparecerá un botón de «Import» donde debes clicar y seleccionar el archivo previamente descomprimido que descargaste antes.

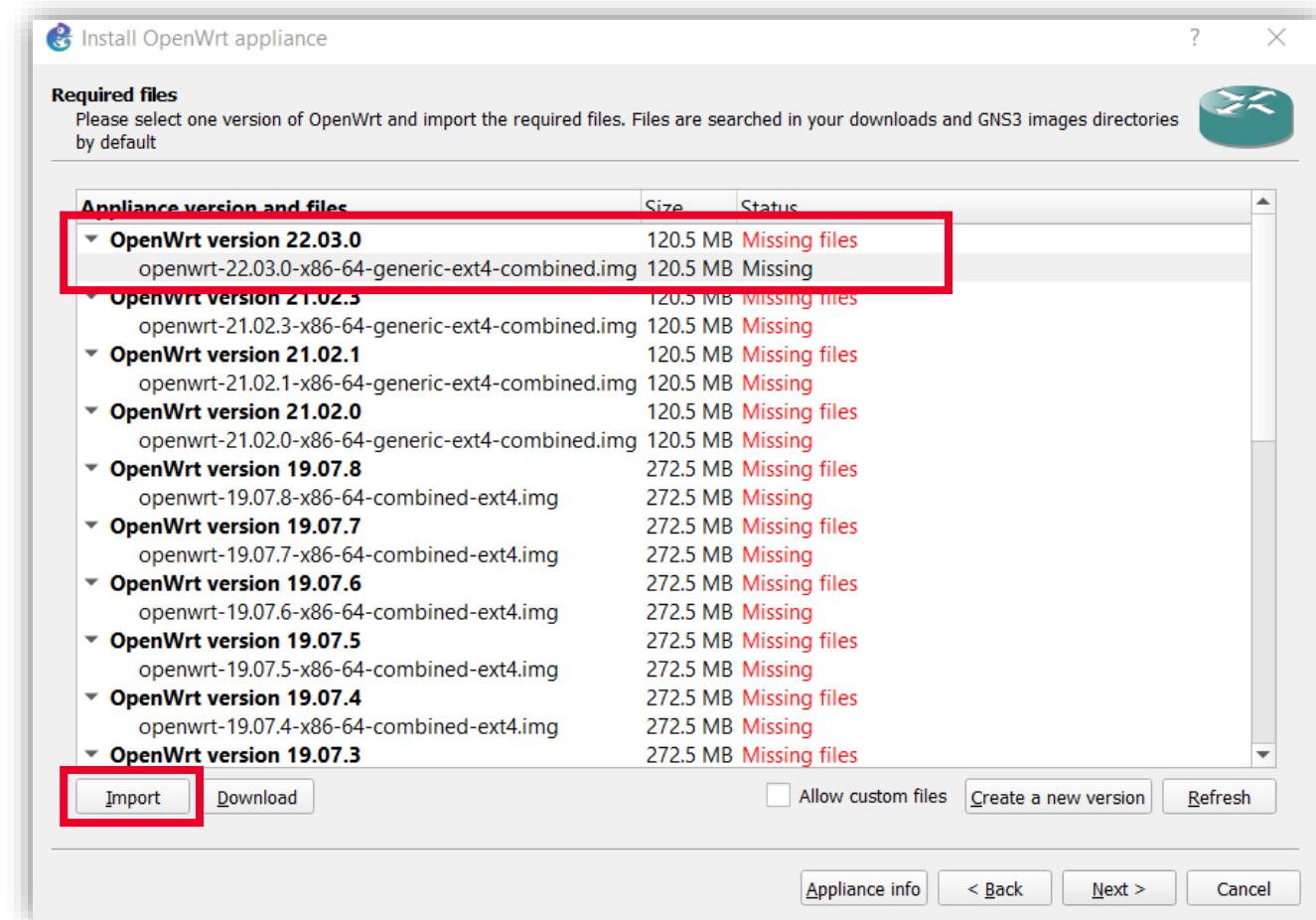


Ilustración 76: Clic en «Import» y selecciona el archivo antes descargado.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Espera mientras se carga el archivo.

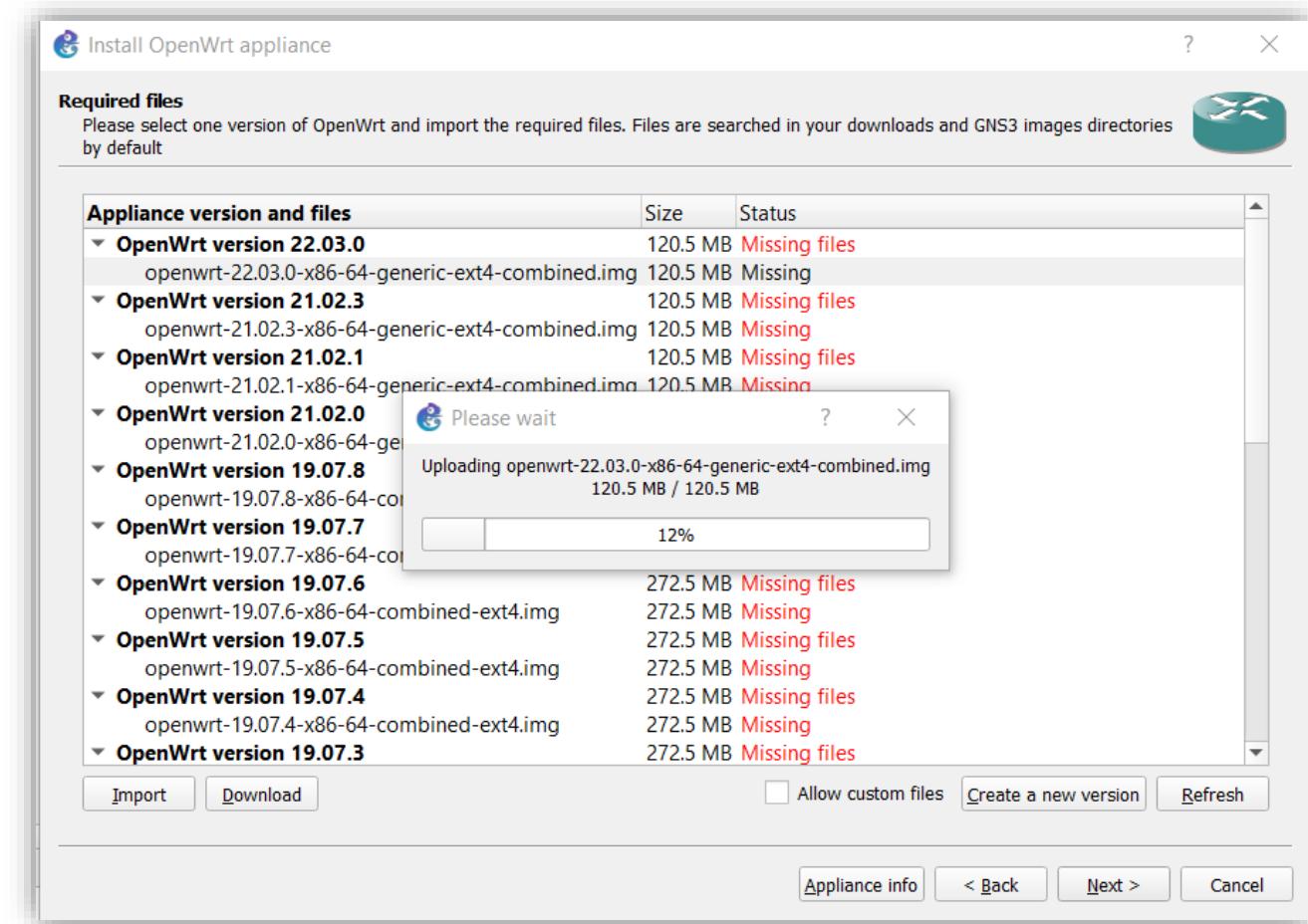


Ilustración 77: Ventana emergente con el proceso de importación.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Una vez completada la carga te deberá aparecer en verde «Ready to install». Si es así, haz clic en «Next».

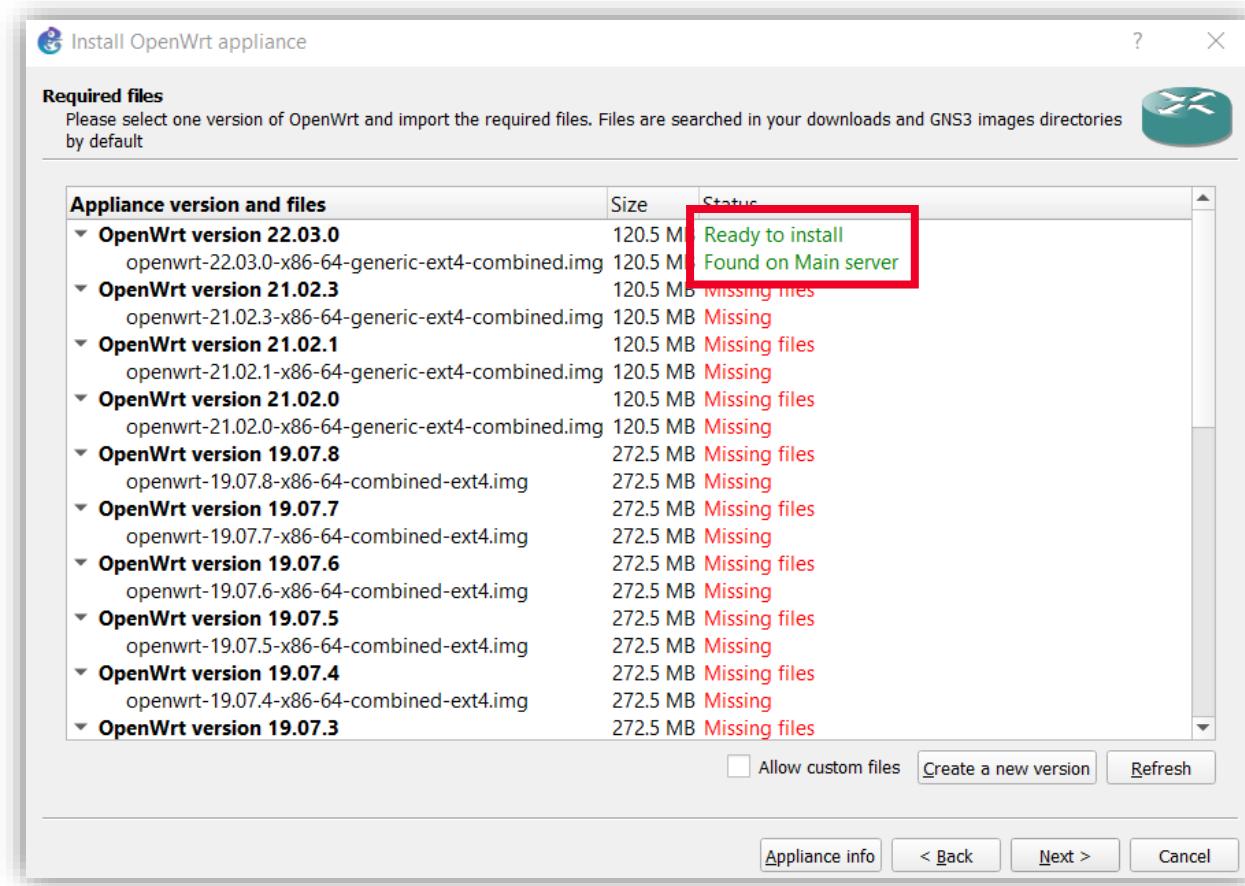


Ilustración 78: Instalación lista.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- En la siguiente ventana que aparece indica el tipo de configuración para próximos pasos que debes tener en cuenta. Lo que indica es qué interfaz debe ir conectada a la LAN y cuál a la WAN.

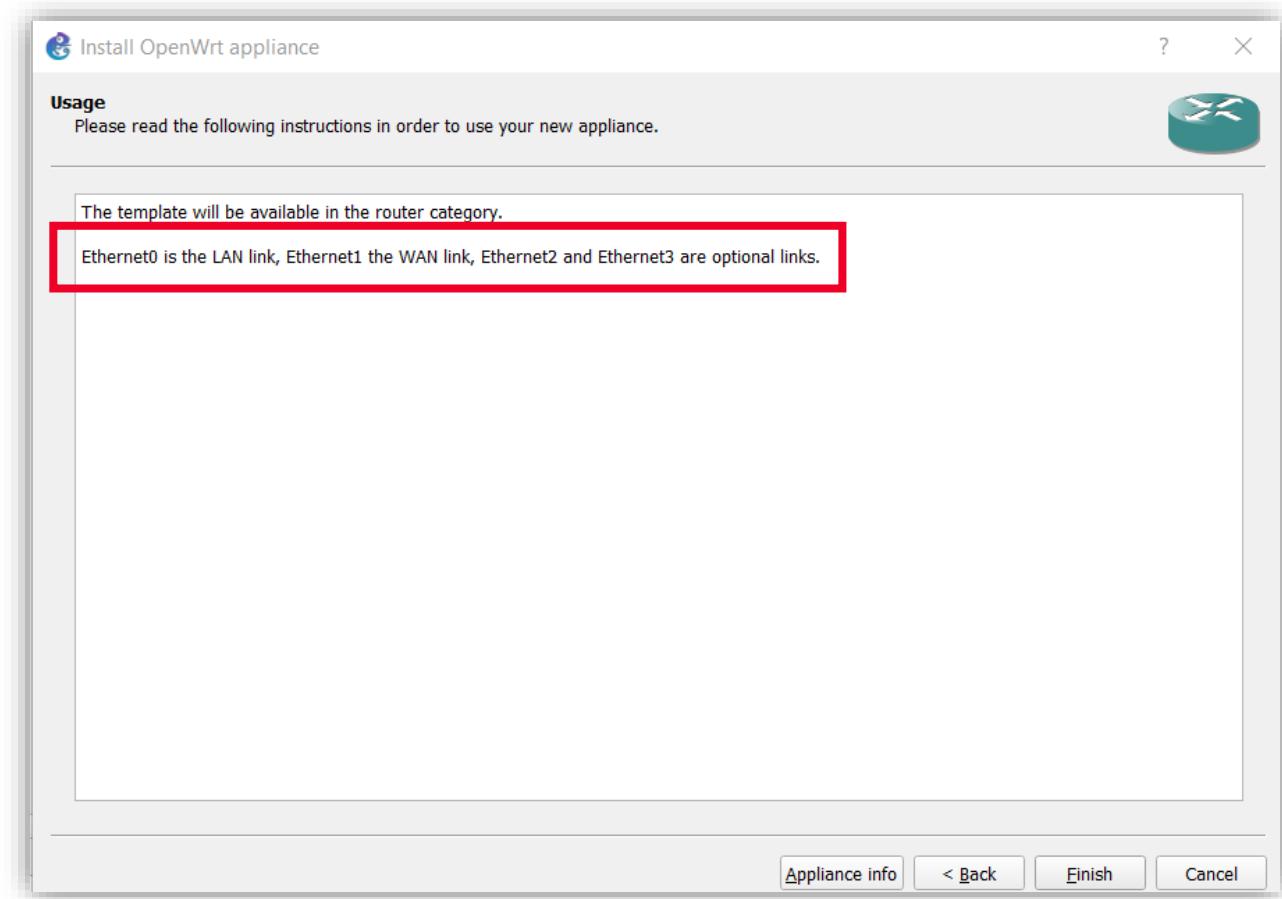


Ilustración 79: Indicación de que la interfaz debe ir a la LAN o la WAN.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Una vez terminado el proceso, el dispositivo aparecerá haciendo clic en el icono señalado, como podemos ver en la siguiente imagen.
- Ahora habrá que configurar la «Cloud», para ello ponte encima de ella, haz clic derecho y pulsa en «Configure».

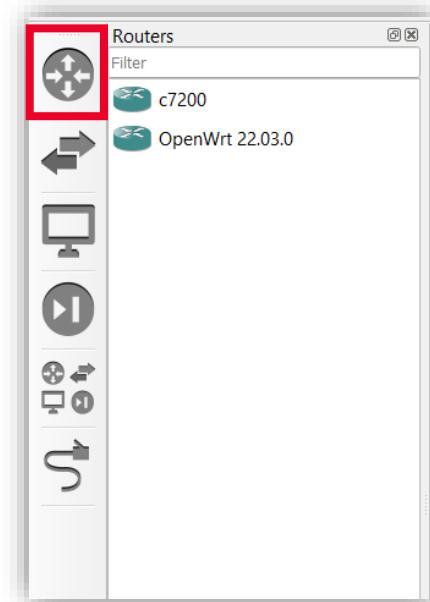


Ilustración 80: Visualización del dispositivo tras finalizar el proceso.

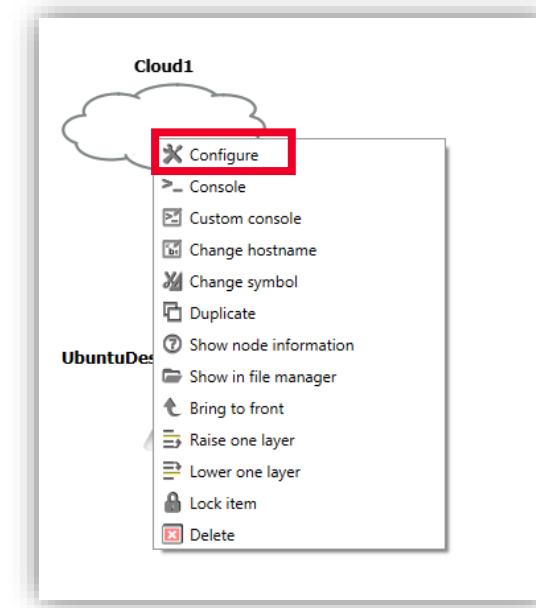


Ilustración 81: Pulsa «Configure» para configurar la «cloud».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Aparecerá una ventana en la que deberás marcar «*Show special Ethernet interfaces*» para que aparezcan todas las interfaces de red disponibles. Y, después, haz clic en «*Add all*».

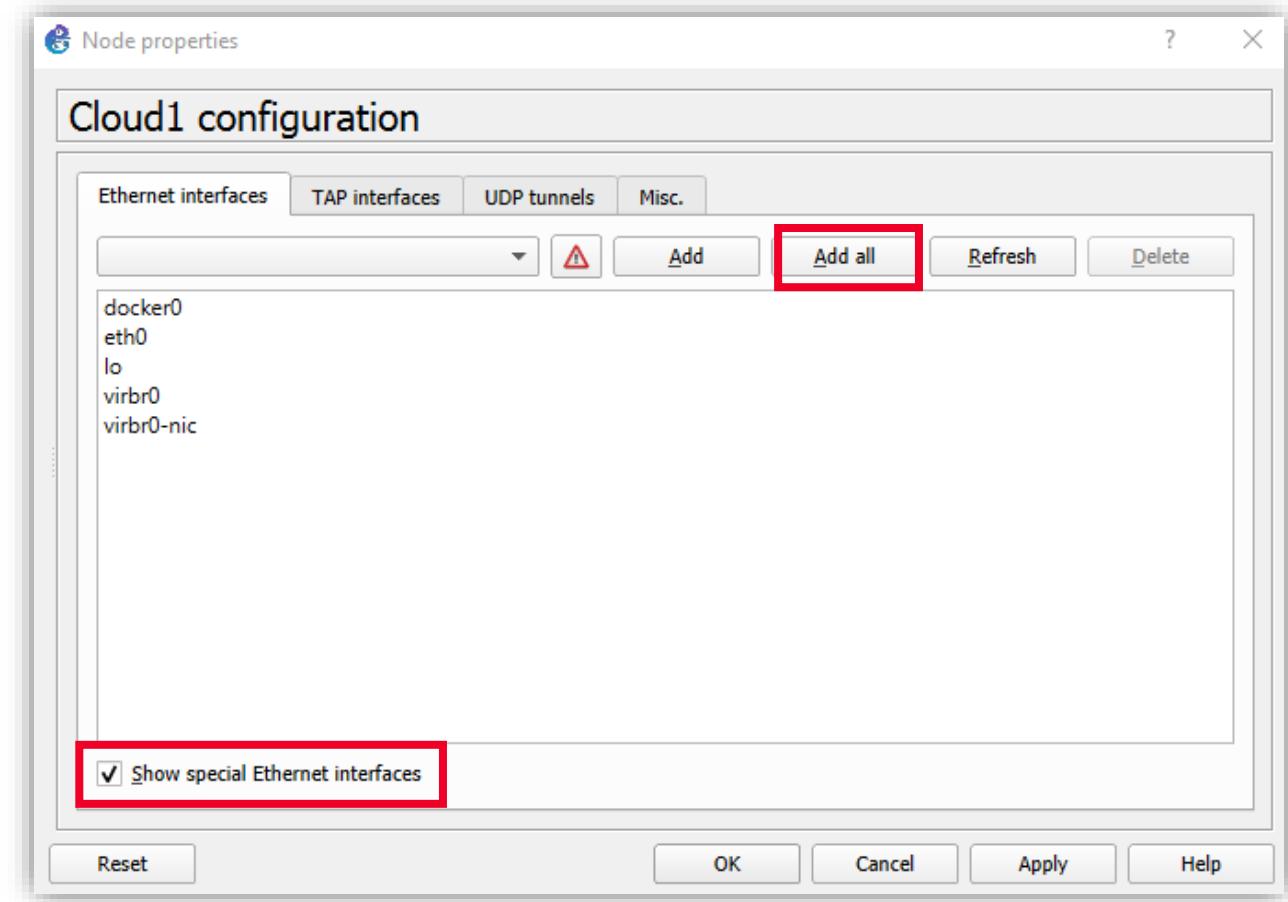


Ilustración 82: Añadimos todas las interfaces de red disponibles.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- El próximo paso será configurar los dispositivos para poder tener acceso a Internet.
- Lo primero que debes hacer es conectar los tres dispositivos como hiciste anteriormente.
- Selecciona el icono del cable y arrastra desde el pc hasta el *router*.

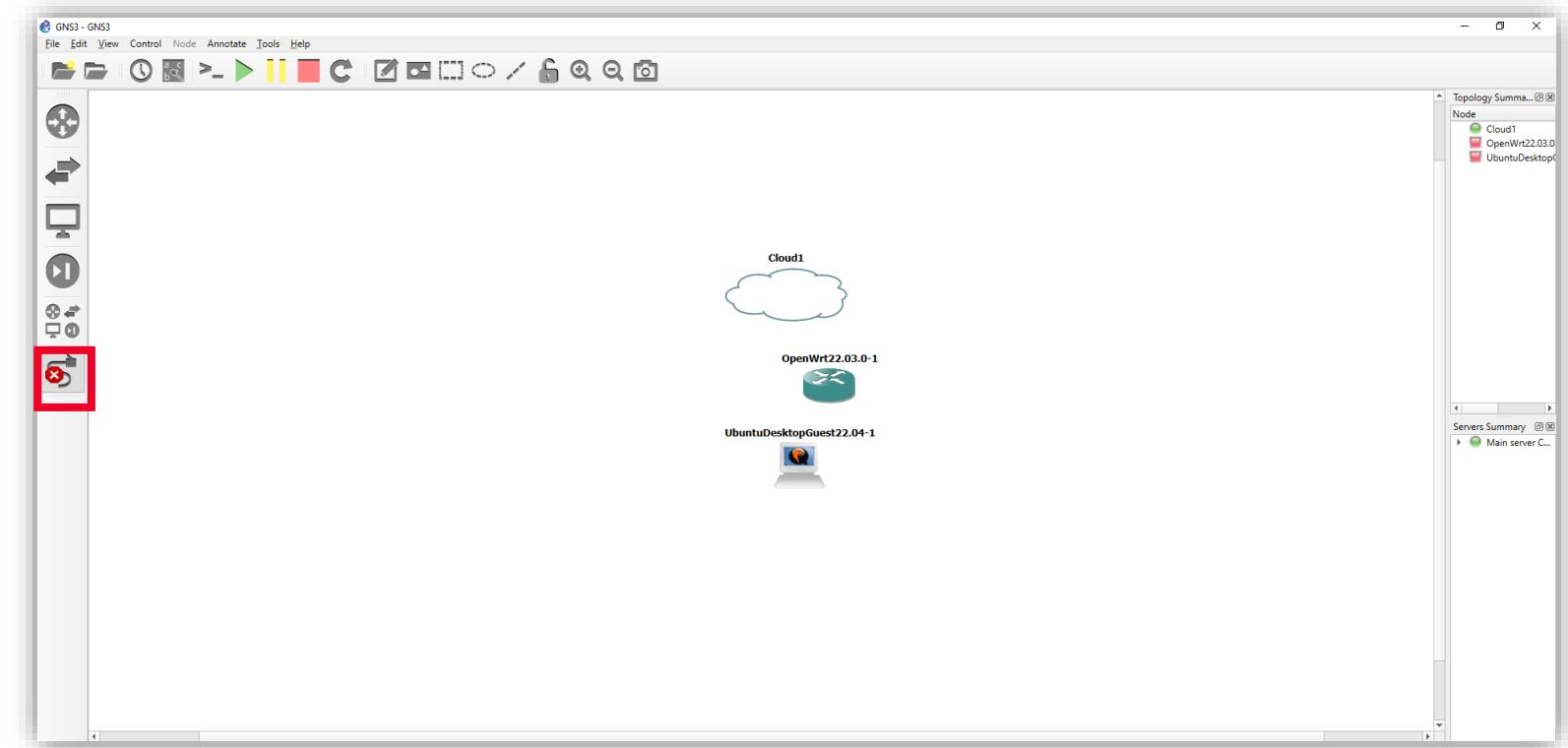


Ilustración 83: Selecciona el icono del cable y arrastra desde el pc hasta el *router*.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- En este caso, como vimos anteriormente, la interfaz «*eth0*» del *router* debe ser utilizada para la LAN, por lo que deberás seleccionar esta cuando arrastres el cable desde el ordenador al *router*.

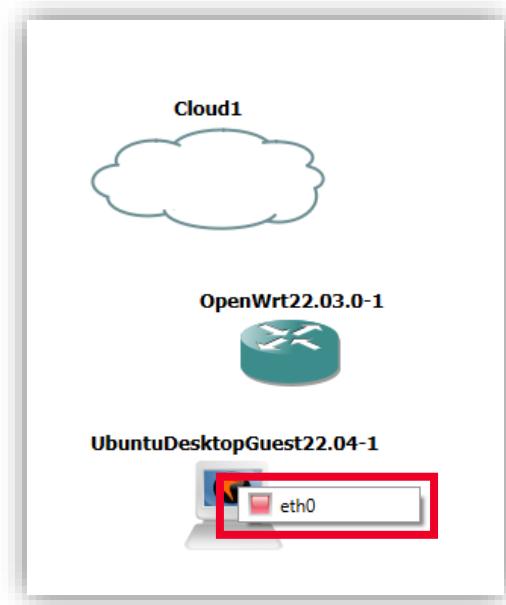


Ilustración 84: Utiliza la interfaz «*eth0*».

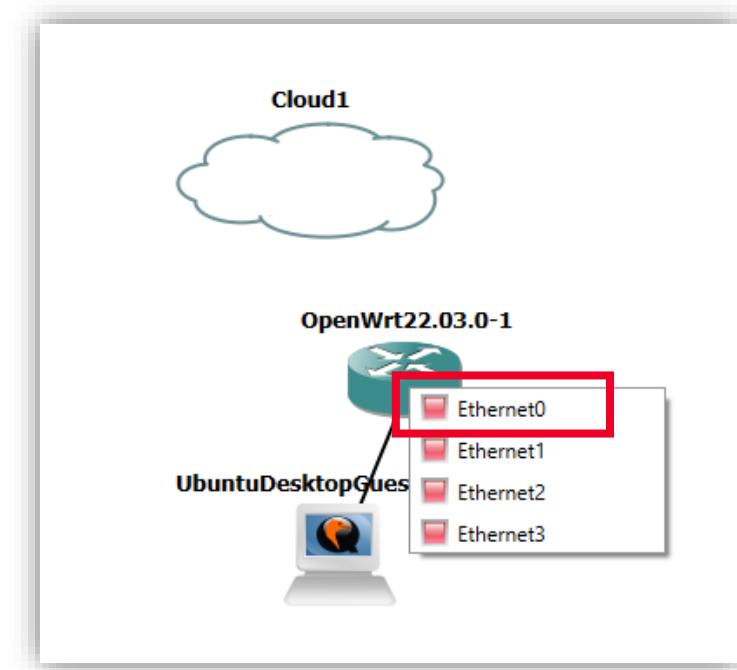


Ilustración 84: Selecciona «*ethernet0*».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- El siguiente paso será conectar el *router* con la «Cloud». Selecciona la interfaz «Ethernet 1» del *router* y arrastra hacia la «Cloud».

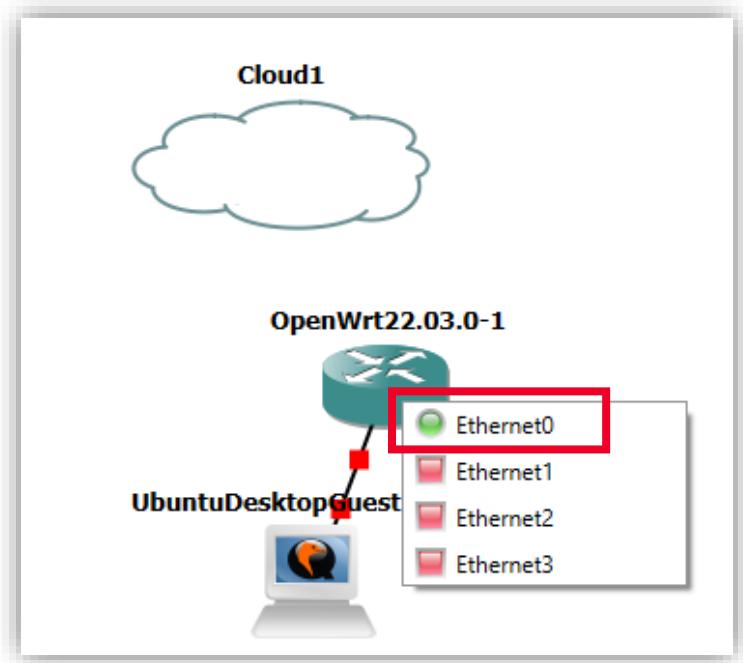


Ilustración 85: Selecciona la interfaz «Ethernet 1» para la conexión con la nube.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- En este caso, en la «Cloud», como hemos visto anteriormente, aparecen diferentes interfaces. Selecciona la denominada «virbr0».

Nota: En nuestro caso es esta, pero puede cambiar dependiendo de cada ordenador. En próximos pasos veremos cómo comprobarlo.

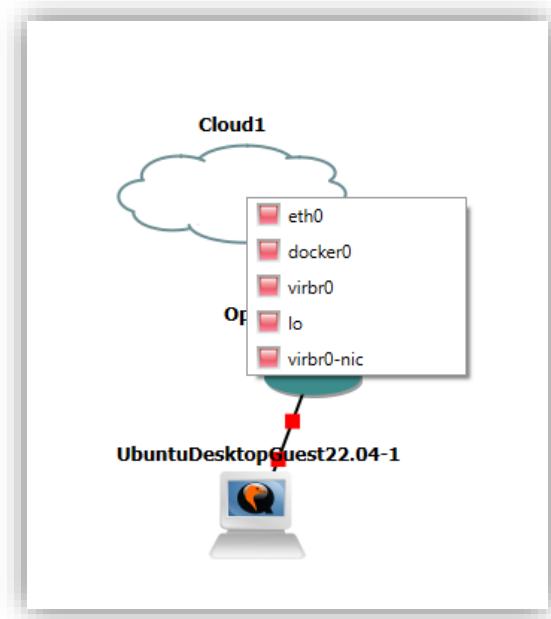


Ilustración 86: Selecciona la interfaz «virbr0».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Primero debes encender tanto el *router* como la máquina Ubuntu. Haz clic en el ícono de «play» de la parte de arriba de la pantalla.

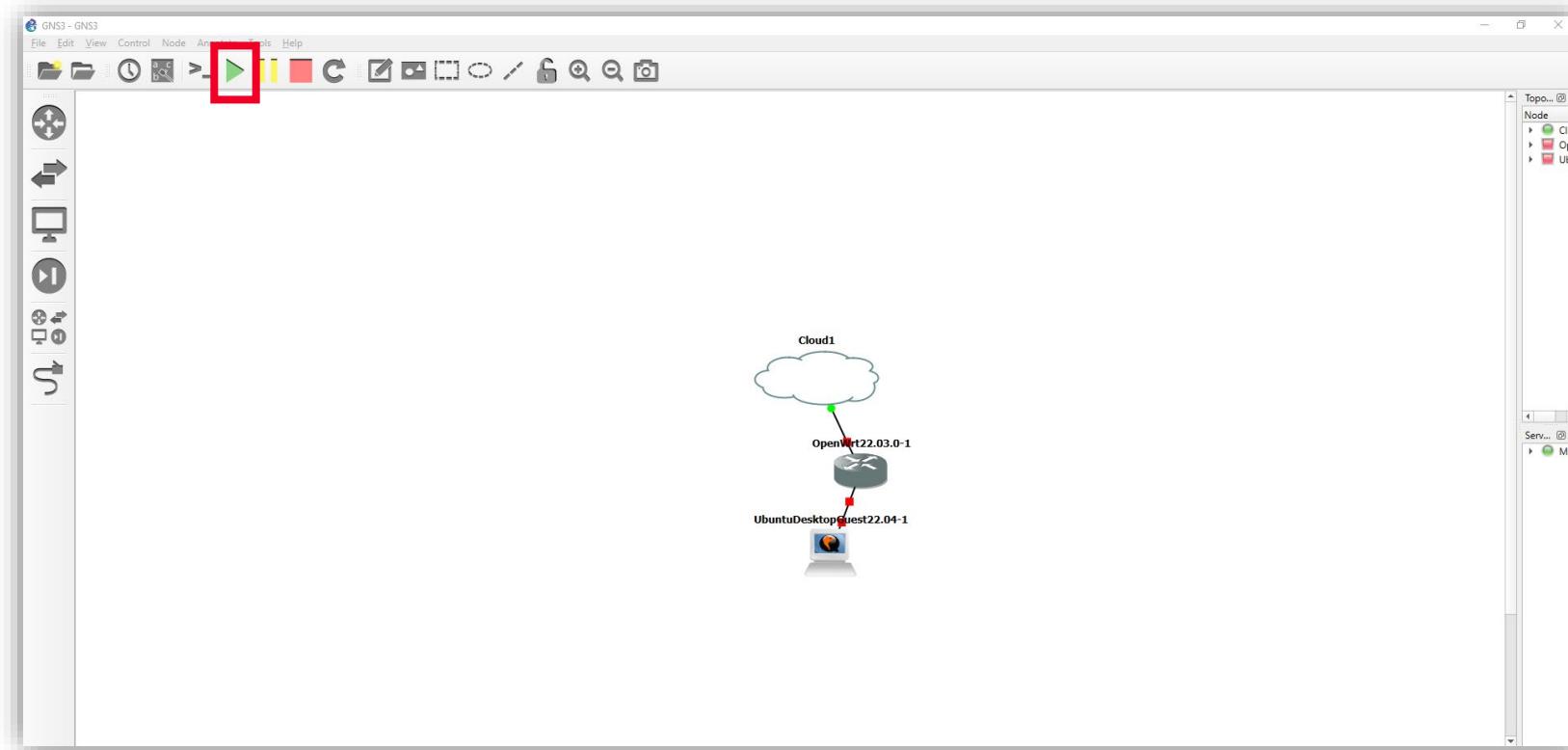


Ilustración 87: Clic en «play» para encender el *router* y la máquina virtual.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Una vez encendido, debes comprobar qué interfaz proporciona Internet ya que puede cambiar dependiendo de cada ordenador como mencionamos anteriormente.
- Para comprobarlo desde el *router* entra en «Console».

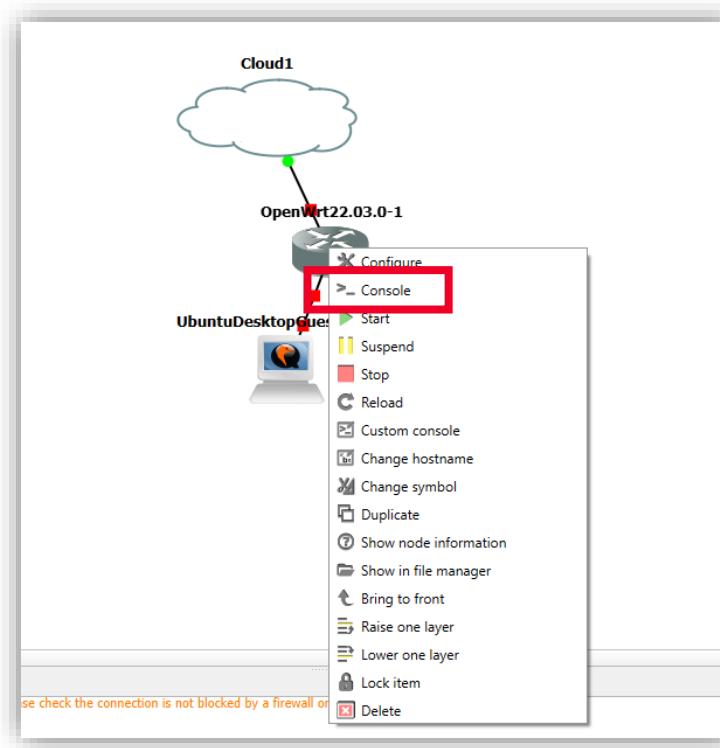


Ilustración 88: Accede a «Console».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Se abrirá la consola del *router*. El primer paso es comprobar con el comando **ifconfig** si la interfaz «*eth1*» (correspondiente a la WAN) nos proporciona IP.

```
root@OpenWrt:/# ifconfig
br-lan    Link encap:Ethernet HWaddr 0C:04:49:7F:00:00
          inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fd59:2b14:4992::1/60 Scope:Global
          inet6 addr: fe80::e04:49ff:fe7f:0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:215 errors:0 dropped:0 overruns:0 frame:0
          TX packets:99 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:23475 (22.9 KiB) TX bytes:11012 (10.7 KiB)

eth0      Link encap:Ethernet HWaddr 0C:04:49:7F:00:00
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:215 errors:0 dropped:0 overruns:0 frame:0
          TX packets:107 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:26485 (25.8 KiB) TX bytes:13614 (13.2 KiB)

eth1      Link encap:Ethernet HWaddr 0C:04:49:7F:00:01
          inet addr:192.168.122.188 Bcast:192.168.122.255 Mask:255.255.255.0
          inet6 addr: fe80::e04:49ff:fe7f:1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:153 errors:0 dropped:0 overruns:0 frame:0
          TX packets:243 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16053 (15.6 KiB) TX bytes:21794 (21.2 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:397 errors:0 dropped:0 overruns:0 frame:0
          TX packets:397 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:41376 (40.4 KiB) TX bytes:41376 (40.4 KiB)

root@OpenWrt:/#
```

Ilustración 89: Comprobar si la interfaz «*eth1*» proporciona IP.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- En el caso que no fuese la interfaz correcta y no asignase IP (como en la siguiente captura), es cuando debes probar con otra de las interfaces que aparece en la «Cloud» hasta que encuentres la que proporciona IP.

```
root@OpenWrt:/# ifconfig
br-lan    Link encap:Ethernet HWaddr 0C:04:49:7F:00:00
          inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::e04:49ff:fe7f:0/64 Scope:Link
          inet6 addr: fd59:2b14:4992::1/60 Scope:Global
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:804 errors:0 dropped:0 overruns:0 frame:0
          TX packets:594 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:63830 (62.3 KiB) TX bytes:56353 (55.0 KiB)

eth0      Link encap:Ethernet HWaddr 0C:04:49:7F:00:00
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:804 errors:0 dropped:0 overruns:0 frame:0
          TX packets:602 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:75086 (73.3 KiB) TX bytes:58955 (57.5 KiB)

eth1      Link encap:Ethernet HWaddr 0C:04:49:7F:00:01
          inet6 addr: fe80::e04:49ff:fe7f:1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:111 errors:0 dropped:1 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:34186 (33.3 KiB) TX bytes:29528 (28.8 KiB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:320 errors:0 dropped:0 overruns:0 frame:0
          TX packets:320 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:24960 (24.3 KiB) TX bytes:24960 (24.3 KiB)

root@OpenWrt:/#
```

Ilustración 90: Probamos con otras interfaces hasta encontrar la que proporciona IP.



PRÁCTICA: HOST CON ACCESO A INTERNET

- Una vez comprobado esto, pasaremos a configurar la interfaz «*eth0*» que es la correspondiente a la máquina Ubuntu.
- Para esto, dentro de la consola del *router*, introduce el comando **ifconfig eth0 10.0.0.1 netmask 255.255.255.0**. Con este comando configuras un rango de red específico para la interfaz LAN (pudiendo elegir la IP que tú quieras).

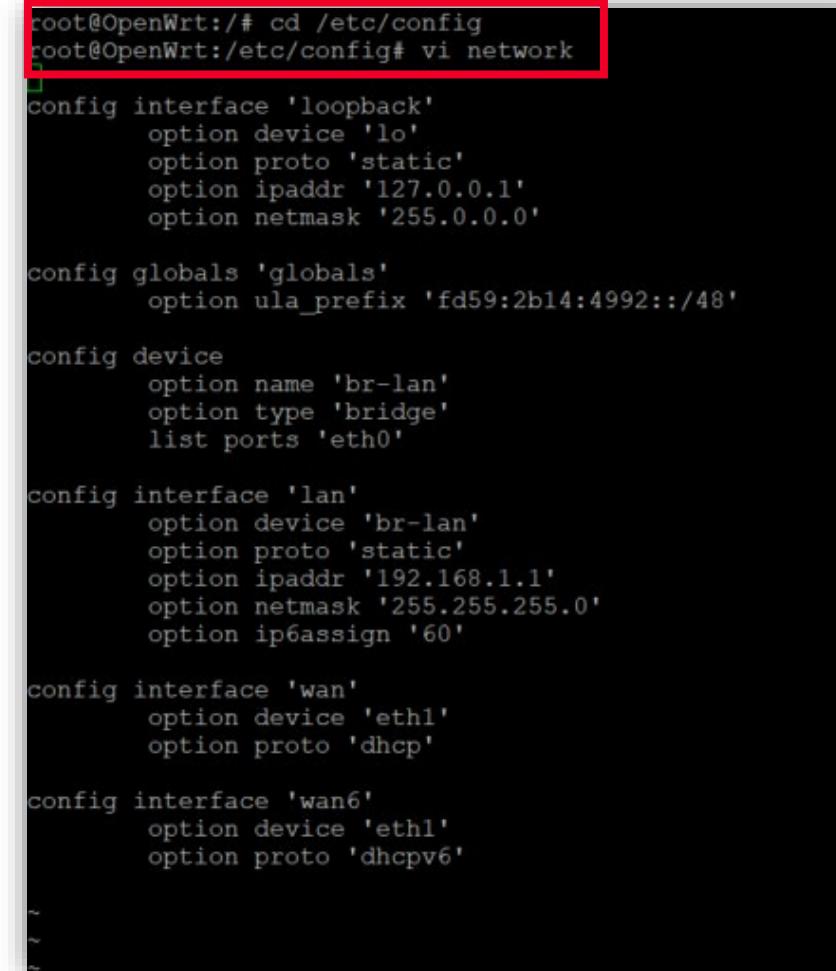
```
root@OpenWrt:/# ifconfig eth0 10.0.0.1 netmask 255.255.255.0
root@OpenWrt:/#
```

Ilustración 91: Introduce el comando **ifconfig eth0 10.0.0.1 netmask 255.255.255.0**.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Después de esto debes hacer la misma modificación en el archivo «*Network*» del *router*.
- Por consiguiente, debes situarte en el directorio **/etc/config/**. Utiliza el comando **cd /etc/config/** para desplazarte al directorio. Una vez ahí para modificar el archivo «*Network*» introduce el comando **vi network**.



```
root@OpenWrt:/# cd /etc/config
root@OpenWrt:/etc/config# vi network

config interface 'loopback'
    option device 'lo'
    option proto 'static'
    option ipaddr '127.0.0.1'
    option netmask '255.0.0.0'

config globals 'globals'
    option ula_prefix 'fd59:2b14:4992::/48'

config device
    option name 'br-lan'
    option type 'bridge'
    list ports 'eth0'

config interface 'lan'
    option device 'br-lan'
    option proto 'static'
    option ipaddr '192.168.1.1'
    option netmask '255.255.255.0'
    option ip6assign '60'

config interface 'wan'
    option device 'eth1'
    option proto 'dhcp'

config interface 'wan6'
    option device 'eth1'
    option proto 'dhcpv6'

~
~
~
```

Ilustración 92: Utiliza el comando **cd /etc/config/** para desplazarte al directorio.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Para editar el texto pon «:i» y modifica el archivo como se muestra en la captura, añadiendo la IP que elegiste anteriormente.

```
root@OpenWrt:/etc/config# vi network

config interface 'loopback'
    option device 'lo'
    option proto 'static'
    option ipaddr '127.0.0.1'
    option netmask '255.0.0.0'

config globals 'globals'
    option ula_prefix 'fd59:2b14:4992::/48'

config device
    option name 'br-lan'
    option type 'bridge'
    list ports 'eth0'

config interface 'lan'
    option device 'eth0'
    option proto 'static'
    option ipaddr '10.0.0.1'
    option netmask '255.255.255.0'
    option ip6assign '60'

config interface 'wan'
    option device 'eth1'
    option proto 'dhcp'

config interface 'wan6'
    option device 'eth1'
    option proto 'dhcpv6'
```

Ilustración 93: Modifica el archivo poniendo «:i».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Para salir y guardar pulsa primero «*Esc*» y después utiliza «*:wq!*». Comprueba que el archivo se ha modificado correctamente, para ello lee su contenido escribiendo en la terminal «*cat network*».
- Para asegurar que la configuración se aplica correctamente haremos un reinicio de la red. Para ello introduce el comando **cd /etc/init.d/** para ubicarte en el directorio correspondiente y después introduce el comando **./network restart**.

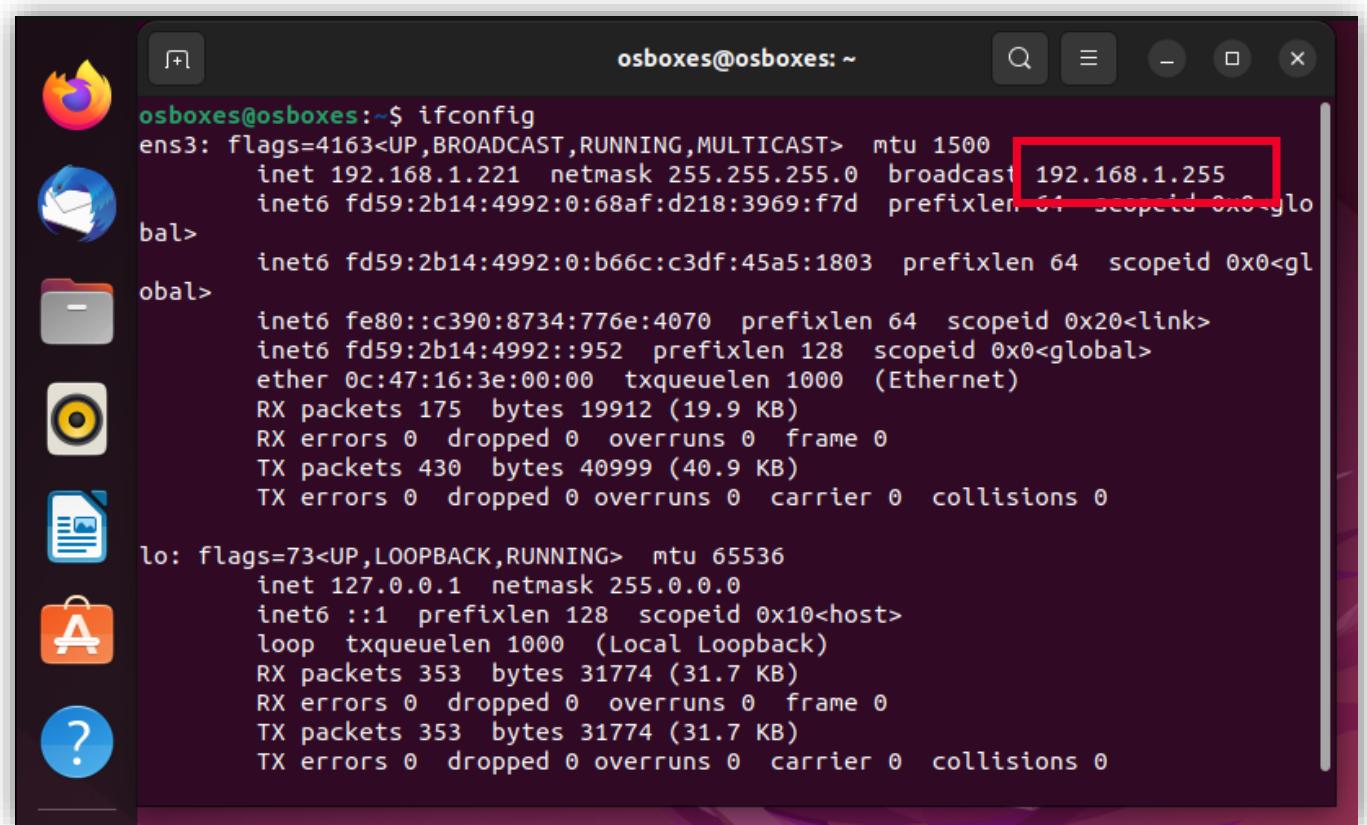
```
root@OpenWrt:/etc/config# cd /etc/init.d/
root@OpenWrt:/etc/init.d# ./network restart
[ 2145.608097] br-lan: port 1(eth0) entered disabled state
[ 2145.640845] device eth0 left promiscuous mode
[ 2145.645690] br-lan: port 1(eth0) entered disabled state
root@OpenWrt:/etc/init.d# [ 2146.751361] 8021q: adding VLAN 0 to HW filter on device eth0
[ 2146.758362] 8021q: adding VLAN 0 to HW filter on device eth1
```

Ilustración 94: Reinicia la red con «*./network restart*».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Una vez configurado el *router*, vamos a pasar a configurar la máquina Ubuntu. Abre la consola de la máquina, haz *log-in* y abre una terminal.
- El primer paso será comprobar qué IP tiene asignada automáticamente con *ifconfig*.
- Probablemente te indique que debes instalar la herramienta «*net-tools*», para ello introduce el comando ***sudo apt install net-tools***.



```
osboxes@osboxes:~$ ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.1.221 netmask 255.255.255.0 broadcast 192.168.1.255
      inet6 fd59:2b14:4992:0:68af:d218:3969:f7d prefixlen 64 scopeid 0x0<global>
      inet6 fd59:2b14:4992:0:b66c:c3df:45a5:1803 prefixlen 64 scopeid 0x0<global>
      inet6 fe80::c390:8734:776e:4070 prefixlen 64 scopeid 0x20<link>
      inet6 fd59:2b14:4992::952 prefixlen 128 scopeid 0x0<global>
ether 0c:47:16:3e:00:00 txqueuelen 1000 (Ethernet)
RX packets 175 bytes 19912 (19.9 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 430 bytes 40999 (40.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 353 bytes 31774 (31.7 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 353 bytes 31774 (31.7 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ilustración 95: Comprueba qué IP asigna automáticamente con «*ifconfig*».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- En nuestro caso, la IP que asigna automáticamente no corresponde con el segmento de red que configuramos anteriormente en el *router* (10.0.0.1/24) por lo que probablemente esta IP nos la está asignando el *router* del lugar donde nos encontramos. Para que sea el *router* de nuestro proyecto el que nos proporcione IP debemos modificarlo manualmente.
- Para este fin, pulsa en el menú superior derecho y aparecerá el menú «*Wired Off*», pulsa sobre él y se desplegará una serie de ajustes donde debes seleccionar «*Wired Settings*».

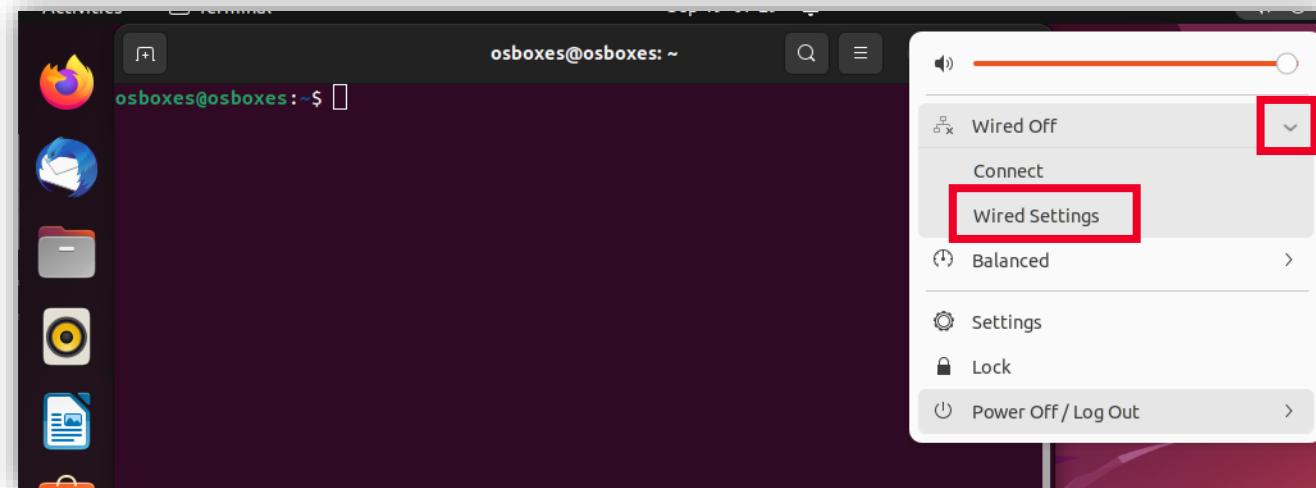


Ilustración 96: Seleccionar «*Wired Settings*» para modificar manualmente la IP.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- En esta ventana debes seleccionar «IPv4» y después «Manual». Una vez seleccionado esto podrás introducir la IP manualmente y, una vez hecho esto, pulsar el botón «Apply».

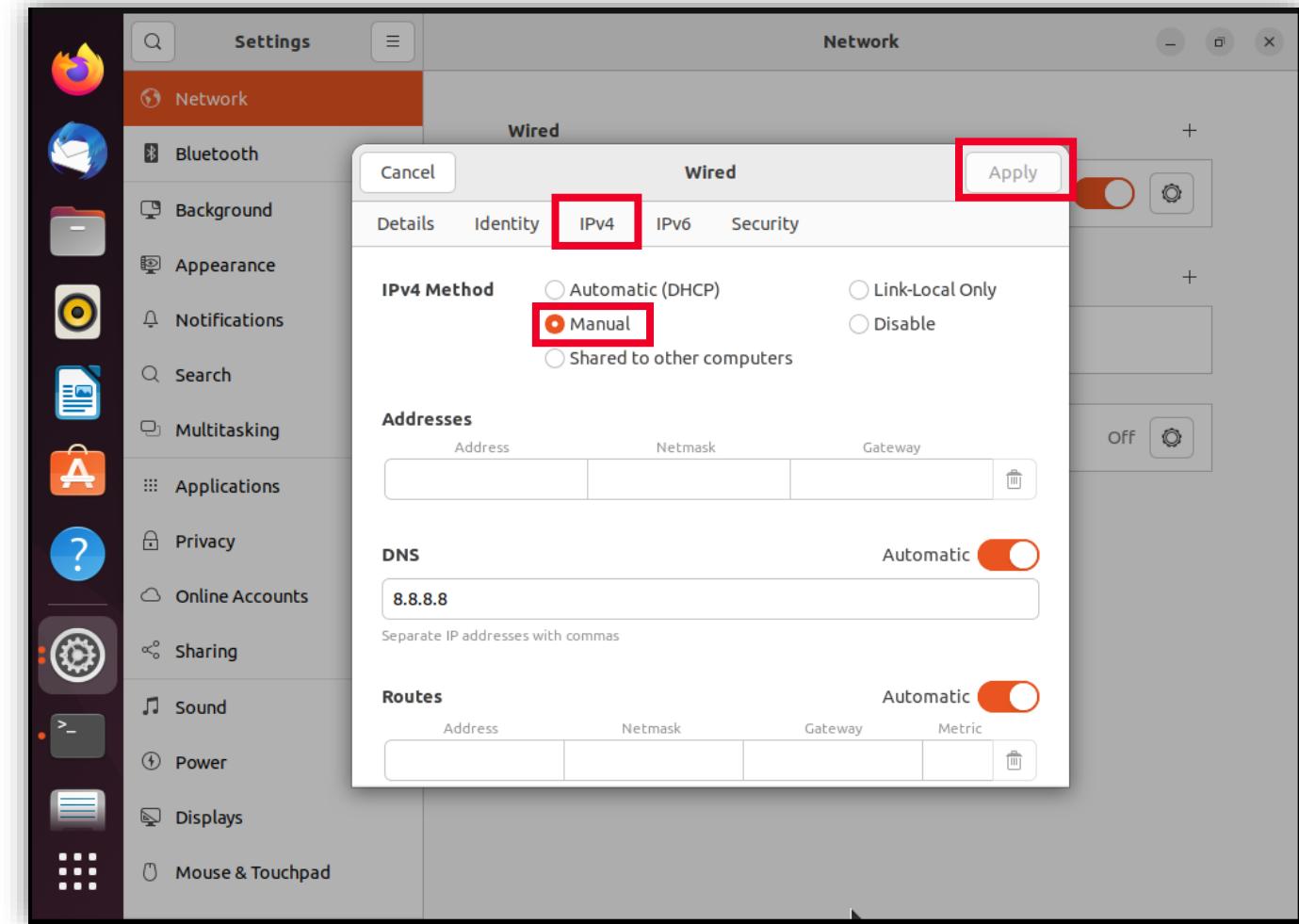


Ilustración 97: Seleccionar «IPv4» y después «Manual».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- En nuestro caso la configuración quedaría así. Recuerda configurarlo dentro del segmento de red que hayas elegido anteriormente.

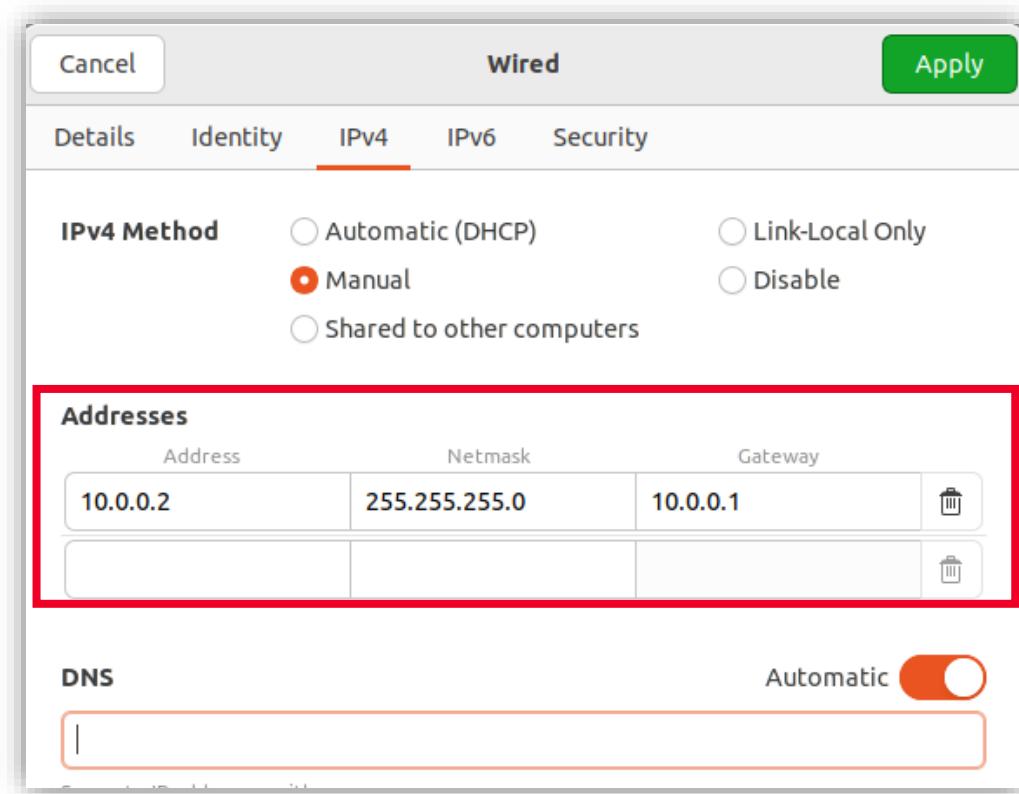


Ilustración 98: Configuración para este ejemplo.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Apaga y enciende el botón que aparece en «Wired» para que se reinicie y se actualice la configuración.

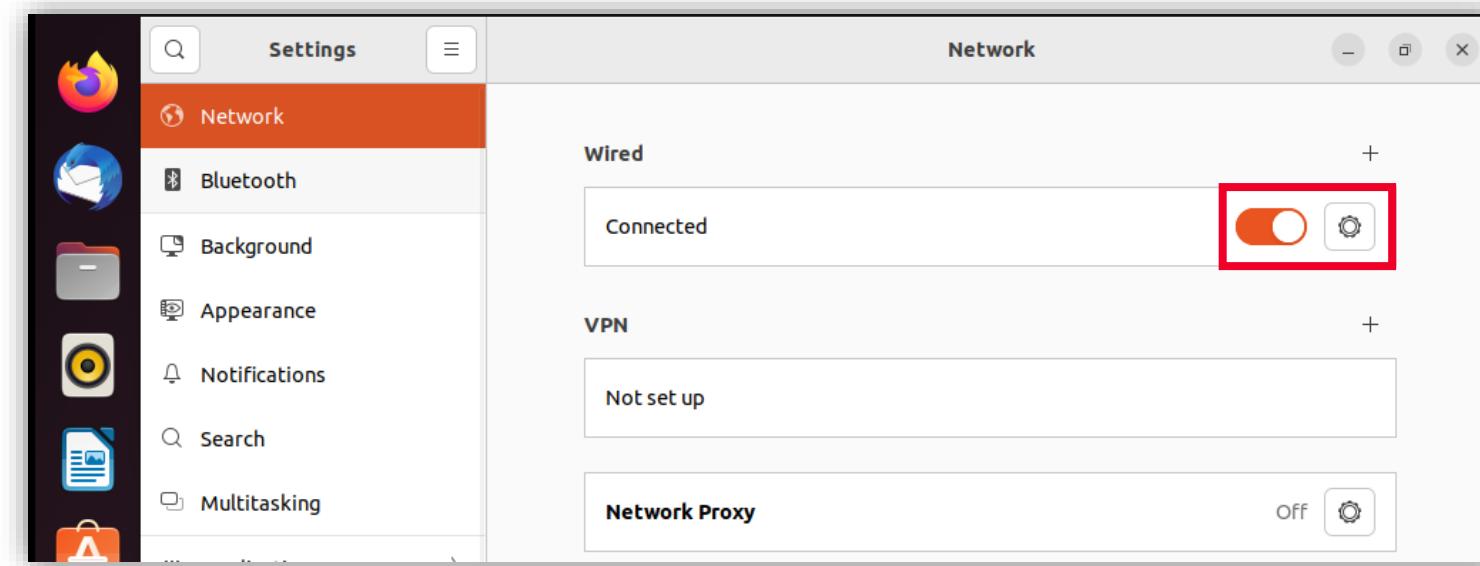


Ilustración 99: Apaga y enciende el botón en «Wired».

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Y comprueba que la configuración modificada es la correcta.

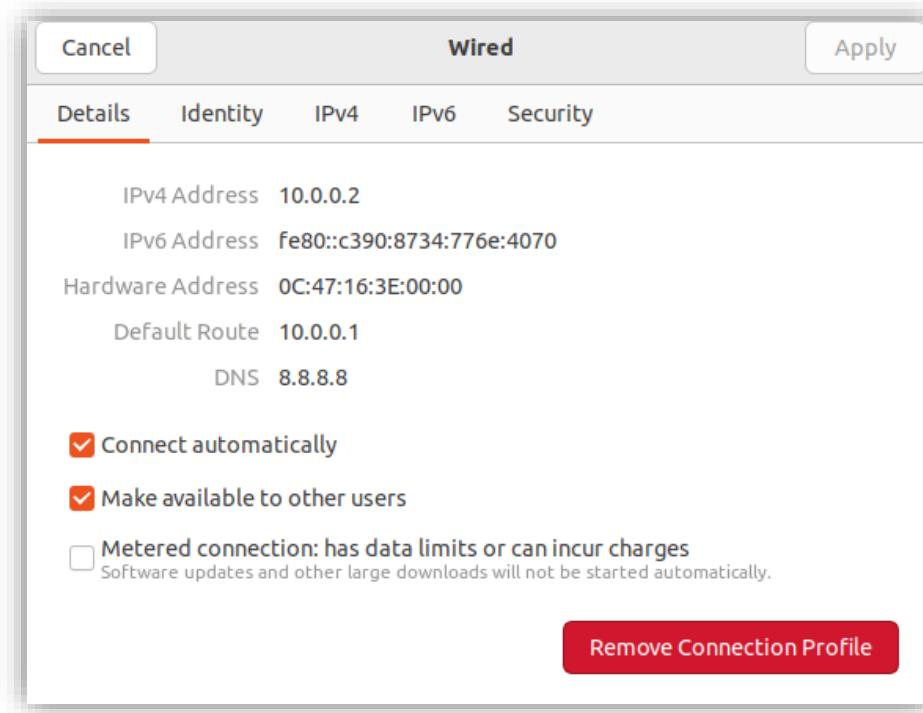


Ilustración 100: Comprueba que la configuración modificada es correcta.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

- Finalmente, y para comprobar que todo funciona correctamente vamos a utilizar el comando «**ping**». Primero, contra nuestro *router* (10.0.0.1), después contra la IP de Google (8.8.8.8) y, por último, contra la página web «Google.com» para comprobar que el DNS está correctamente configurado.

```
osboxes@osboxes:~$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=19.0 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.399 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.405 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.398 ms
^C
--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3054ms
rtt min/avg/max/mdev = 0.398/5.053/19.013/8.059 ms
osboxes@osboxes:~$
```

Ilustración 101: Usamos «**ping**» contra nuestro *router*.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

```
osboxes@osboxes:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=3.33 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=2.91 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=2.85 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=2.80 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=114 time=2.87 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 2.804/2.954/3.334/0.192 ms
```

Ilustración 102: Usamos «ping» contra la IP de Google.

4

PRÁCTICA: HOST CON ACCESO A INTERNET

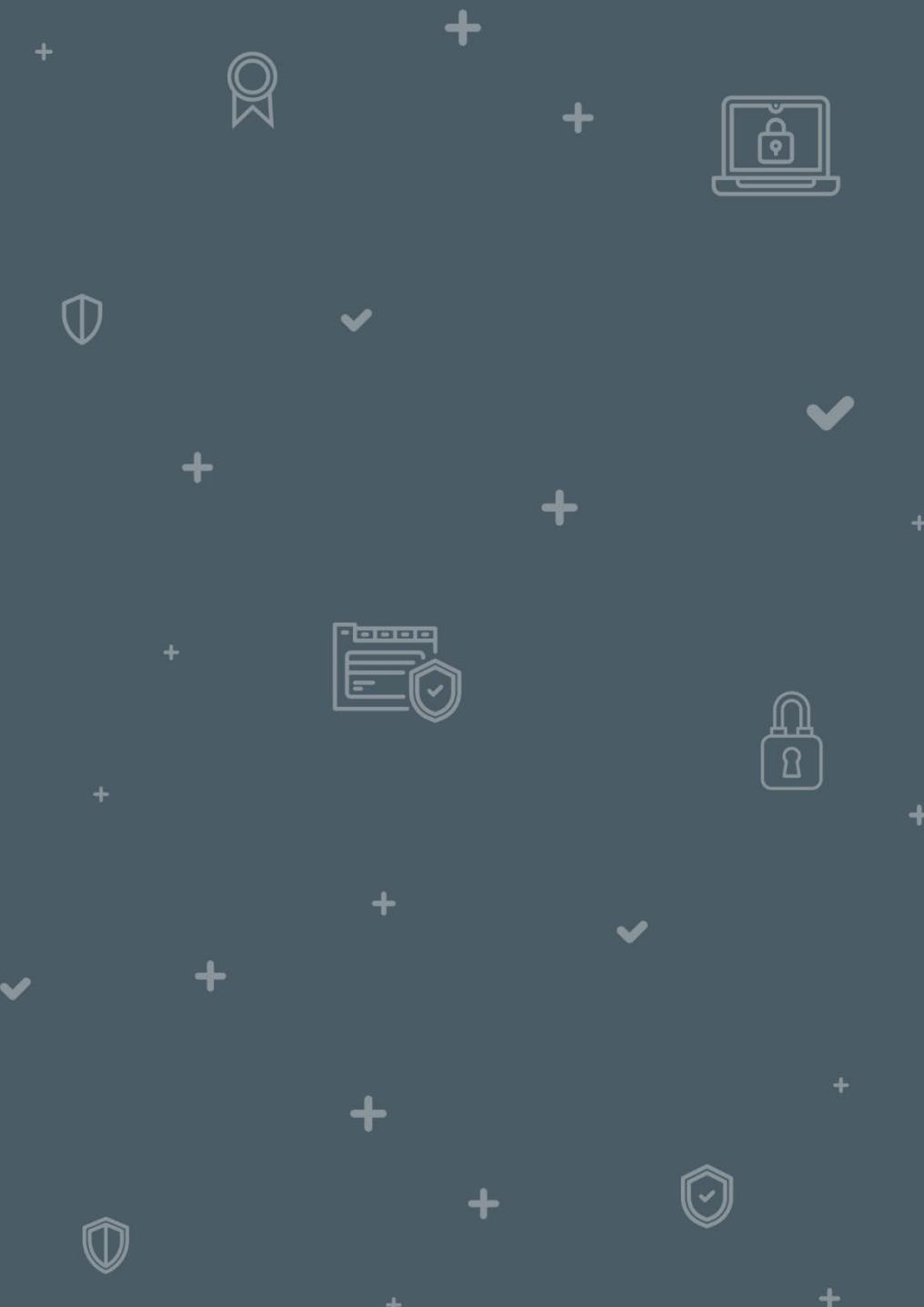
```
osboxes@osboxes:~$ ping google.es
PING google.es (142.250.200.131) 56(84) bytes of data.
64 bytes from mad41s14-in-f3.1e100.net (142.250.200.131): icmp_seq=1 ttl=113 time=9.76 ms
64 bytes from mad41s14-in-f3.1e100.net (142.250.200.131): icmp_seq=2 ttl=113 time=2.96 ms
64 bytes from mad41s14-in-f3.1e100.net (142.250.200.131): icmp_seq=3 ttl=113 time=2.66 ms
64 bytes from mad41s14-in-f3.1e100.net (142.250.200.131): icmp_seq=4 ttl=113 time=2.81 ms
^C
--- google.es ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 2.660/4.545/9.758/3.011 ms
```

Ilustración 103: Usamos «ping» contra la página de Google.

- Y de esta forma ya tienes configurado el *host* con salida a Internet.

PRÁCTICA: HOST CON ACCESO A INTERNET *(ROUTER CISCO)* Y VIRTUAL PCs *(ELEMENTO VPCs)*

5





PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

En esta parte de la práctica sustituirás tanto la máquina Ubuntu por un PC virtual, como el *router* OpenWrt por un *router* Cisco.

Para la realización de este taller, tendrás que descargarte el archivo «**c7200-adventerprisek9-mz.152-4.M7**» que encontrarás en los recursos descargables de la unidad.

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- El primer paso es eliminar la máquina Ubuntu y añadir el VPCS, que viene por defecto instalado en GNS3. Lo encontrarás en el lateral izquierdo de la pantalla, en el ícono de ordenador con título «End devices».

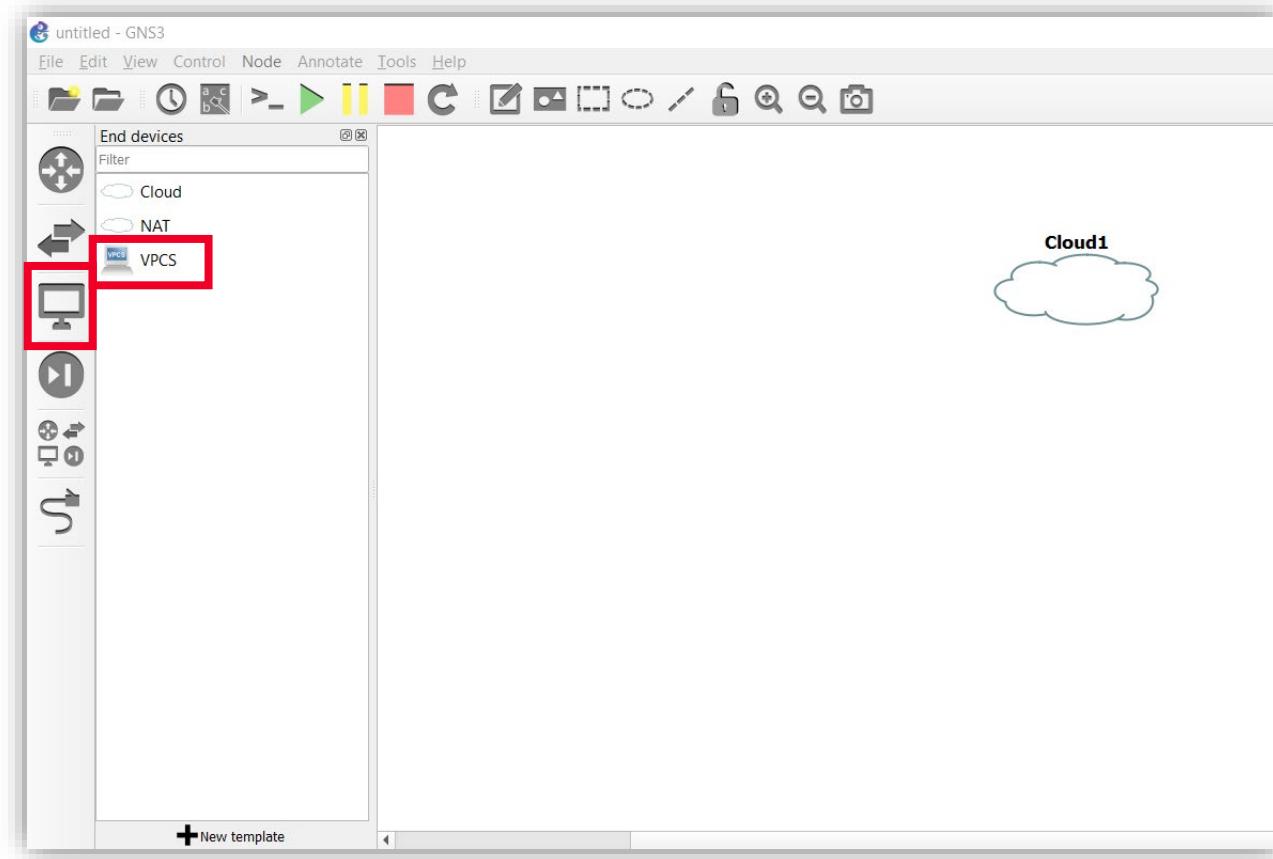


Ilustración 104: Añadir el VPCS.

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- Para añadir el router Cisco: selecciona «Edit > Preferences». Luego selecciona la pestaña «IOS routers» y haz clic en «New».

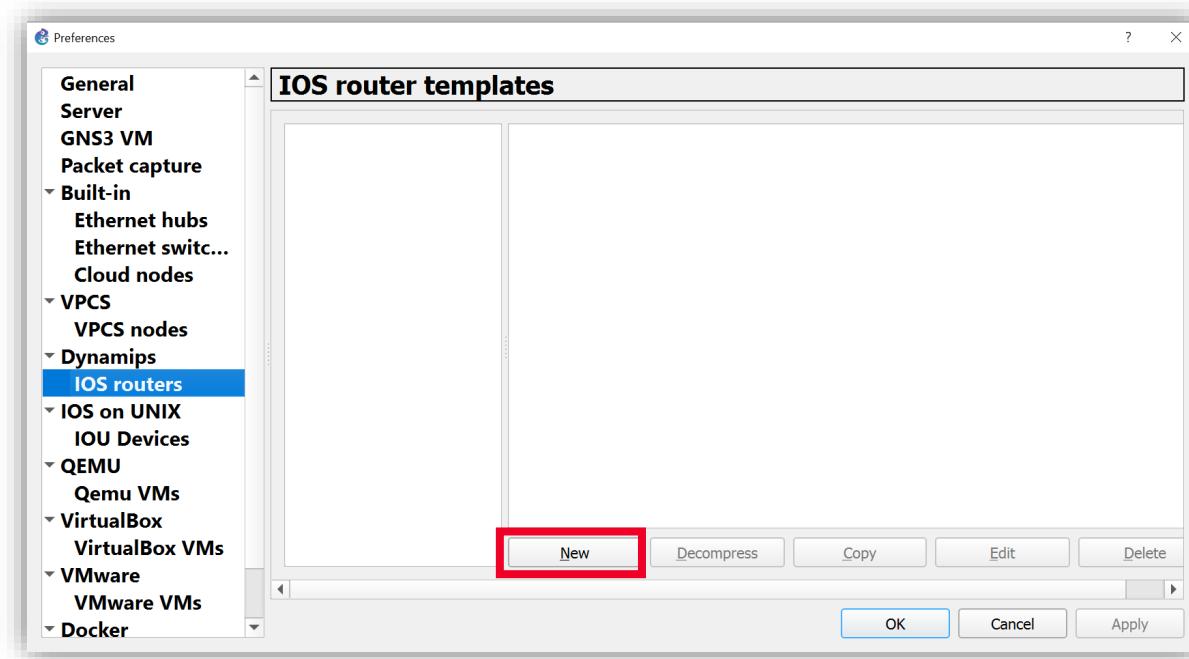


Ilustración 105: Selecciona la pestaña «IOS routers» y haz clic en «New».

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- Haz clic en «Browse» y selecciona el archivo que te hemos proporcionado e indicado anteriormente «c7200-adventureisek9-mz.152-4.M7».

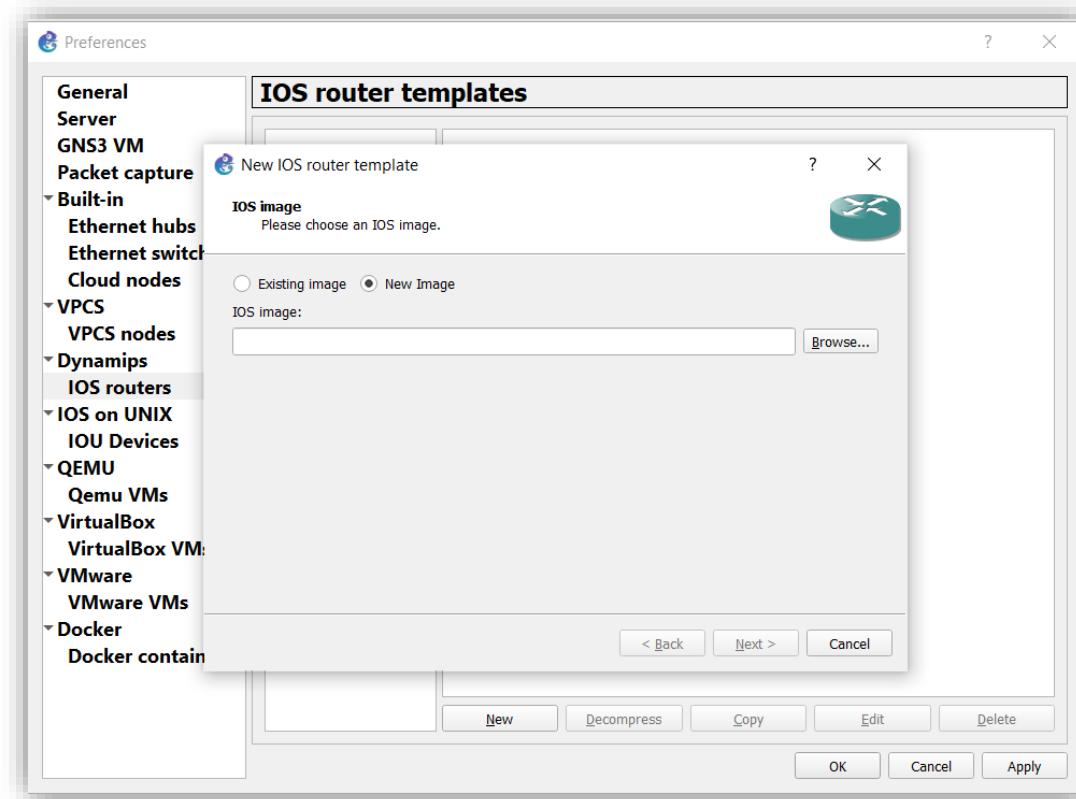


Ilustración 106: Selecciona el archivo proporcionado.

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- Selecciona el archivo previamente descargado y haz clic en «Next».

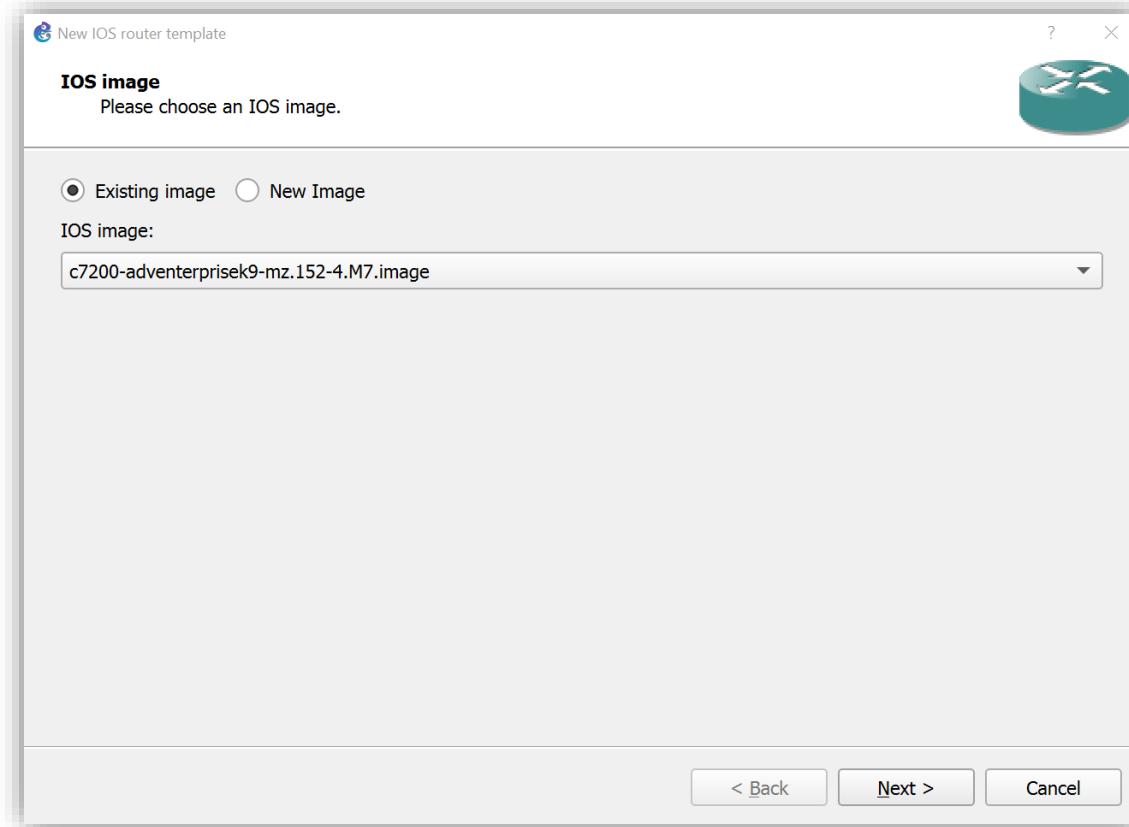


Ilustración 107: Selecciona el archivo previamente descargado y haz clic en «Next».

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- Haz clic en «Yes».

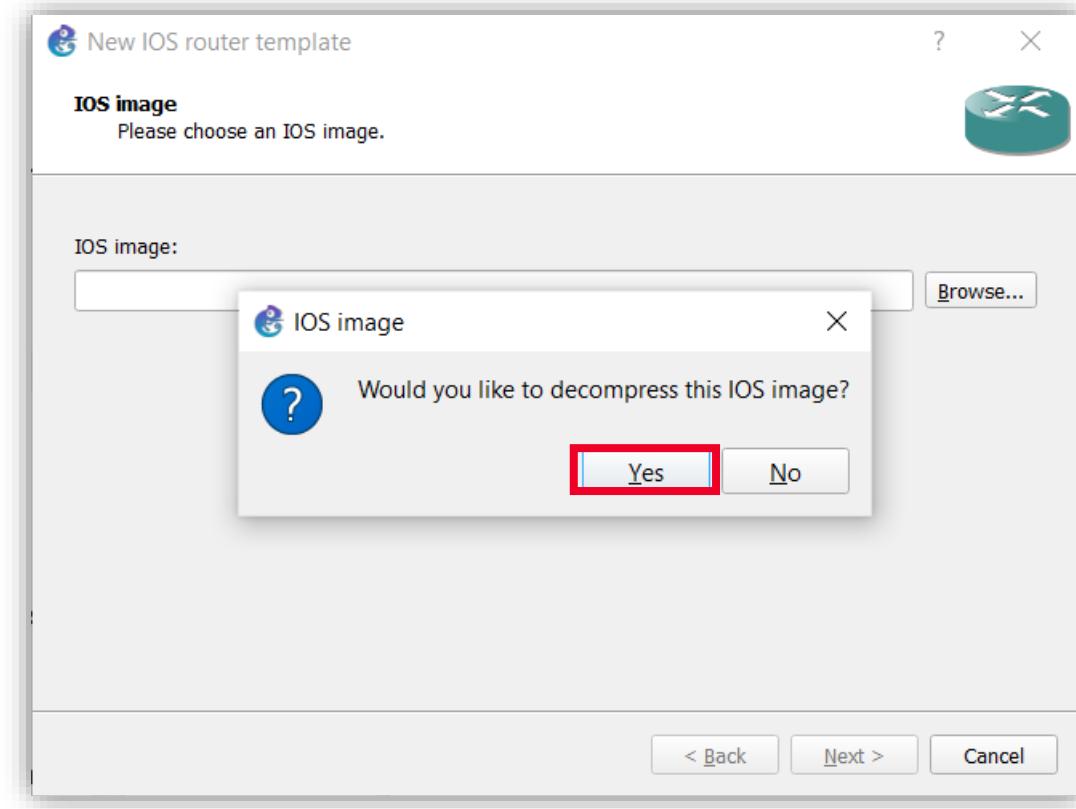


Ilustración 108: Selecciona «Yes» para descomprimir el «*IOS image*».

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- En el siguiente menú, sin cambiar nada, haz clic en «Next».

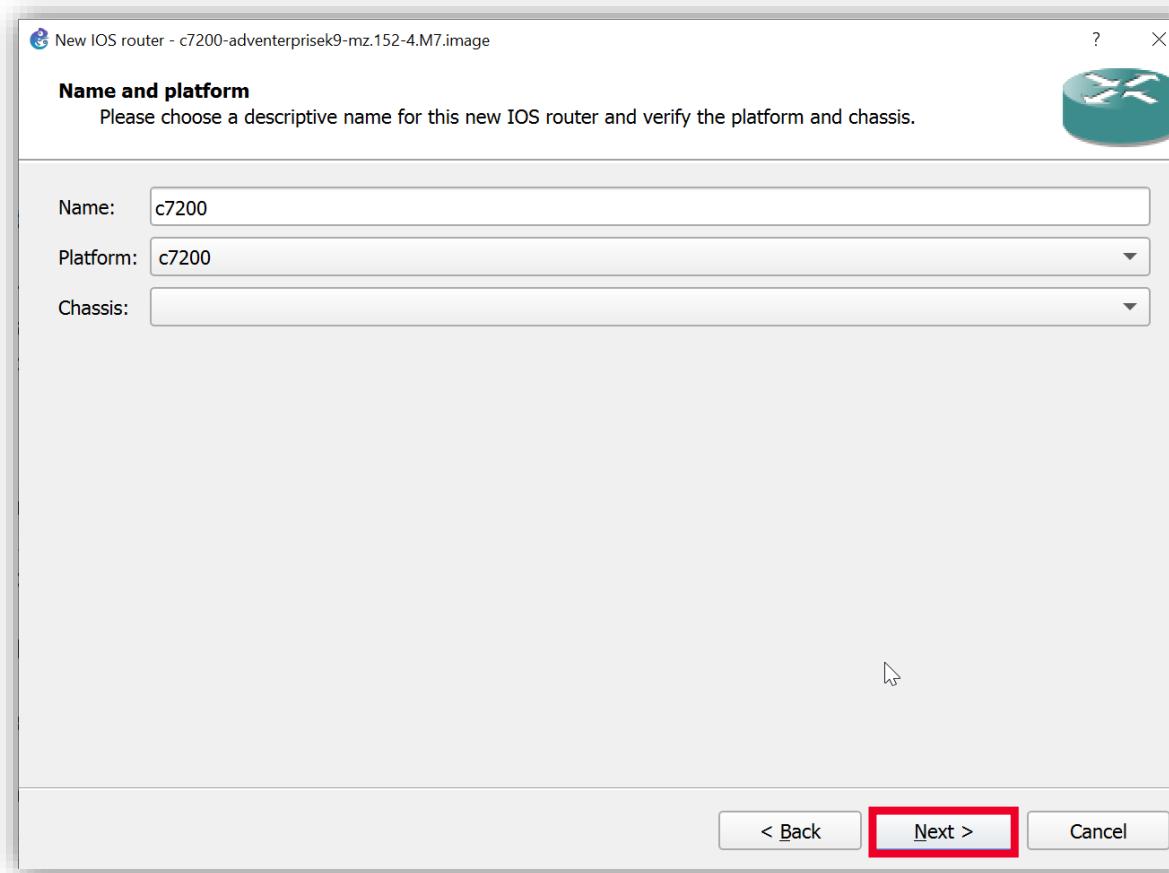


Ilustración 109: Haz clic en «next» en «name and platform».

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- Deja la RAM por defecto que nos indica y haz clic en «Next».

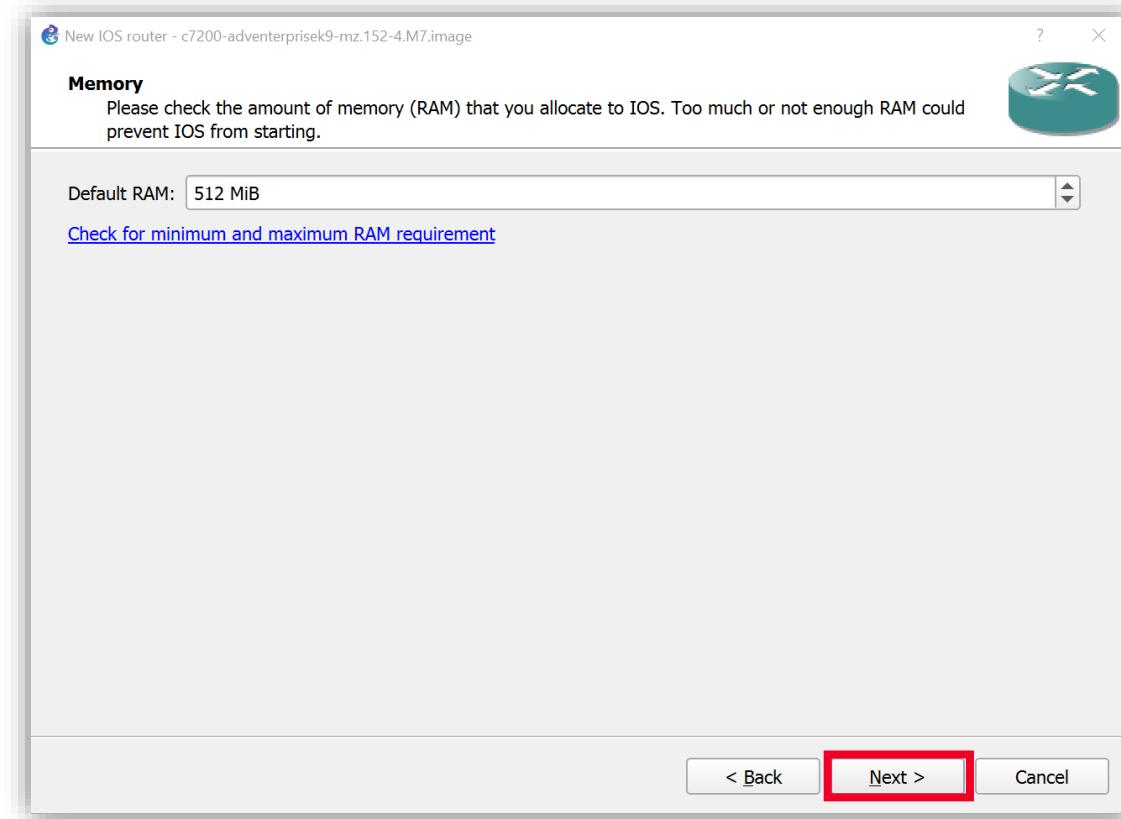


Ilustración 110: Deja la RAM por defecto y clic en «next».

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- En esta ventana debes seleccionar los adaptadores de red del *router*. Haz clic en el desplegable y configúralo como aparece en la imagen. Ahora mismo no necesitaremos las dos interfaces ya que sólo se va a conectar un dispositivo, pero lo dejaremos configurado para más adelante.

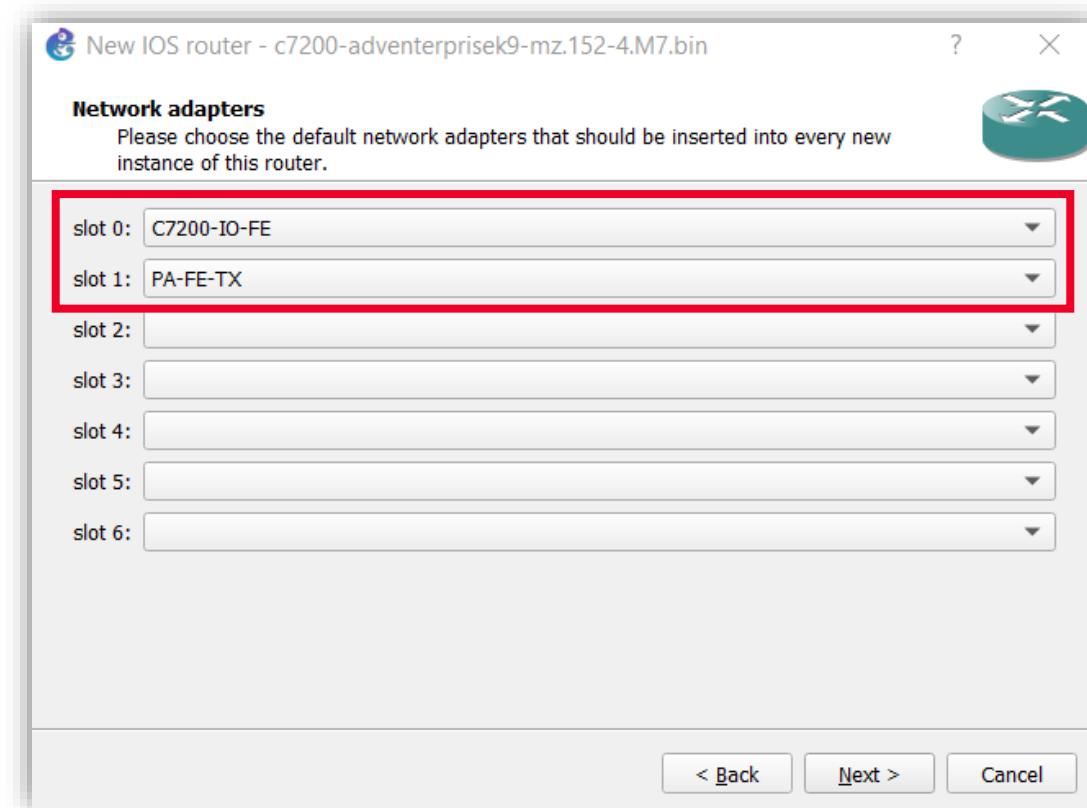


Ilustración 111: Configura los adaptadores de red del *router*.

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- En la siguiente ventana haz clic en «*Idle-PC Finder*» esto permitirá que nuestra CPU y memoria funcionen adecuadamente durante la simulación.

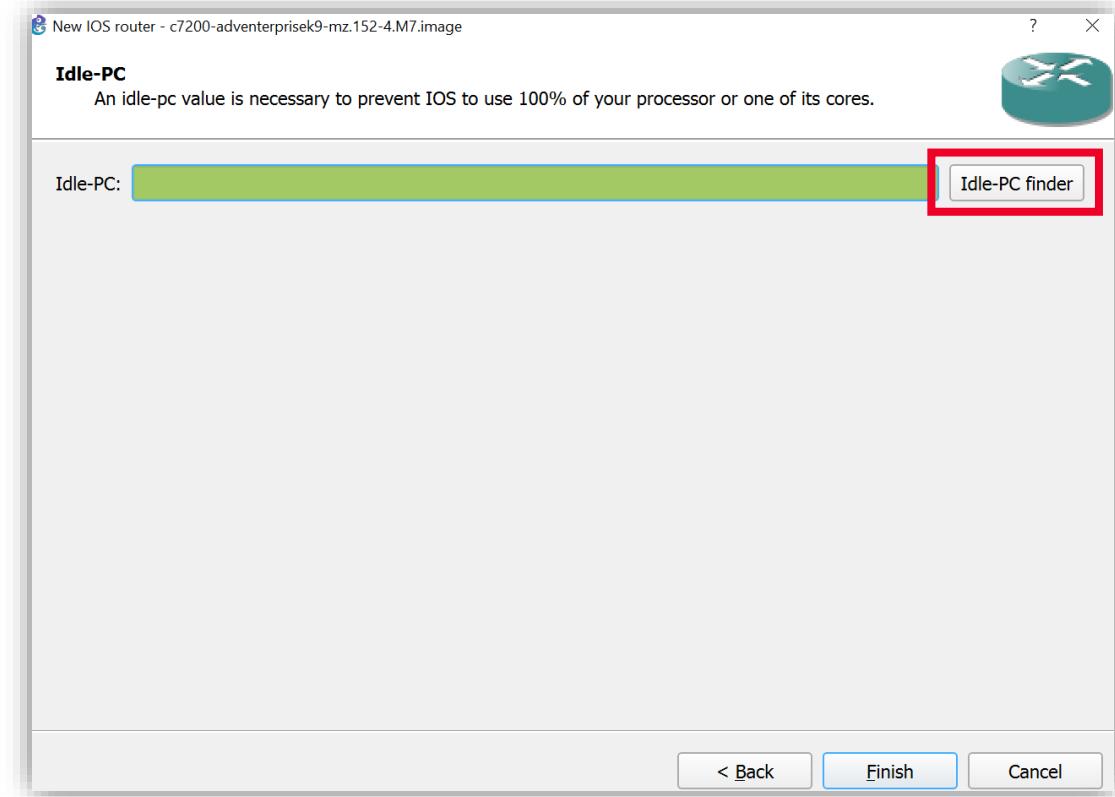


Ilustración 112: Clic en «*Idle-PC Finder*» para que nuestra CPU y memoria funcionen adecuadamente.

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- Espera hasta que termine el proceso.

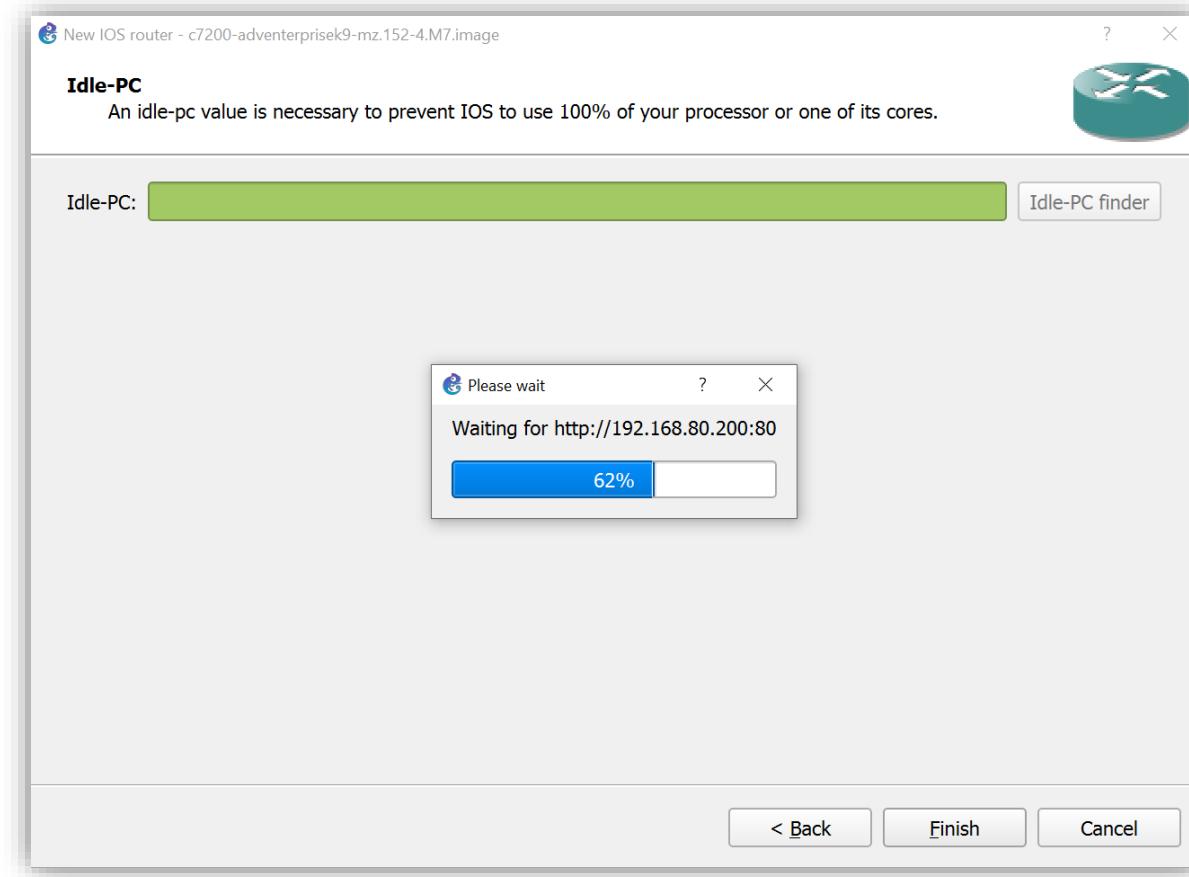


Ilustración 113: Ventana emergente en la que visualizamos cómo va el proceso.

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

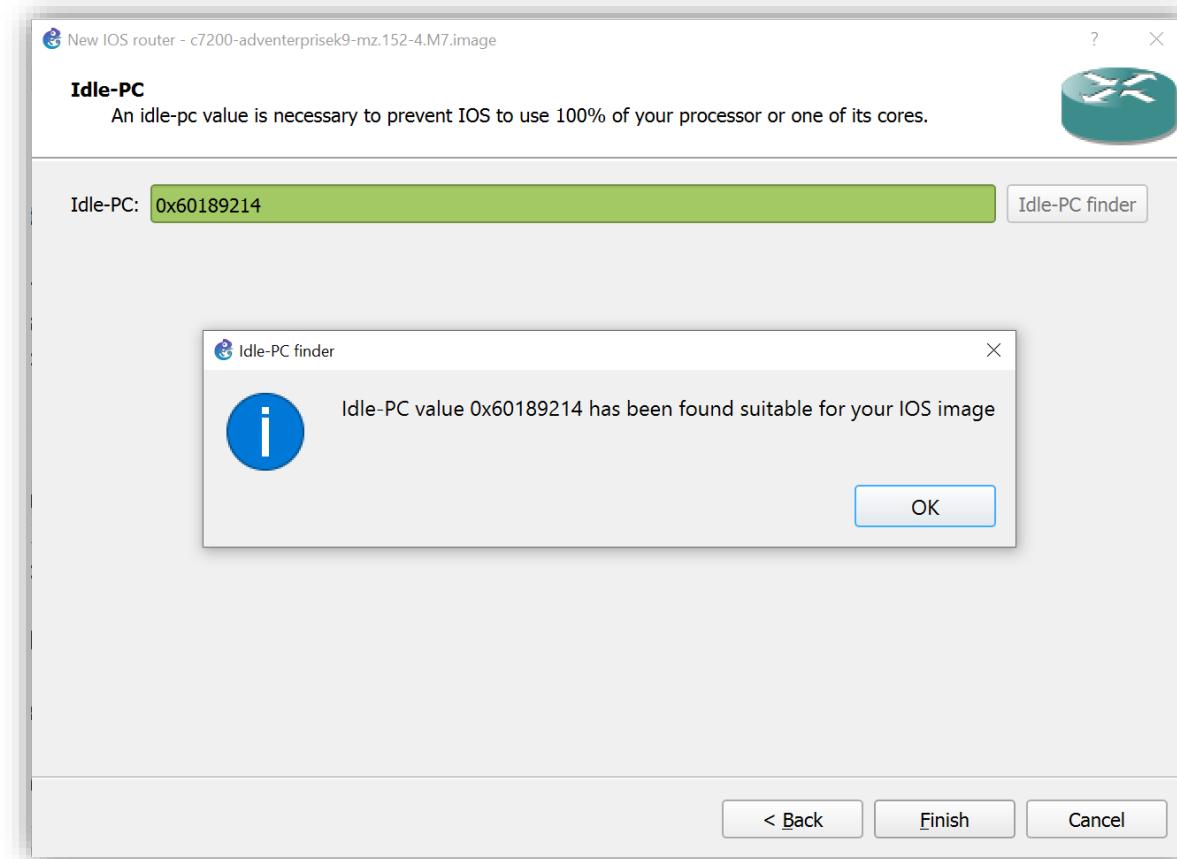


Ilustración 114: Venta emergente donde nos muestra que el proceso se ha completado.

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- Pulsa «*Finish*» para terminar este proceso.

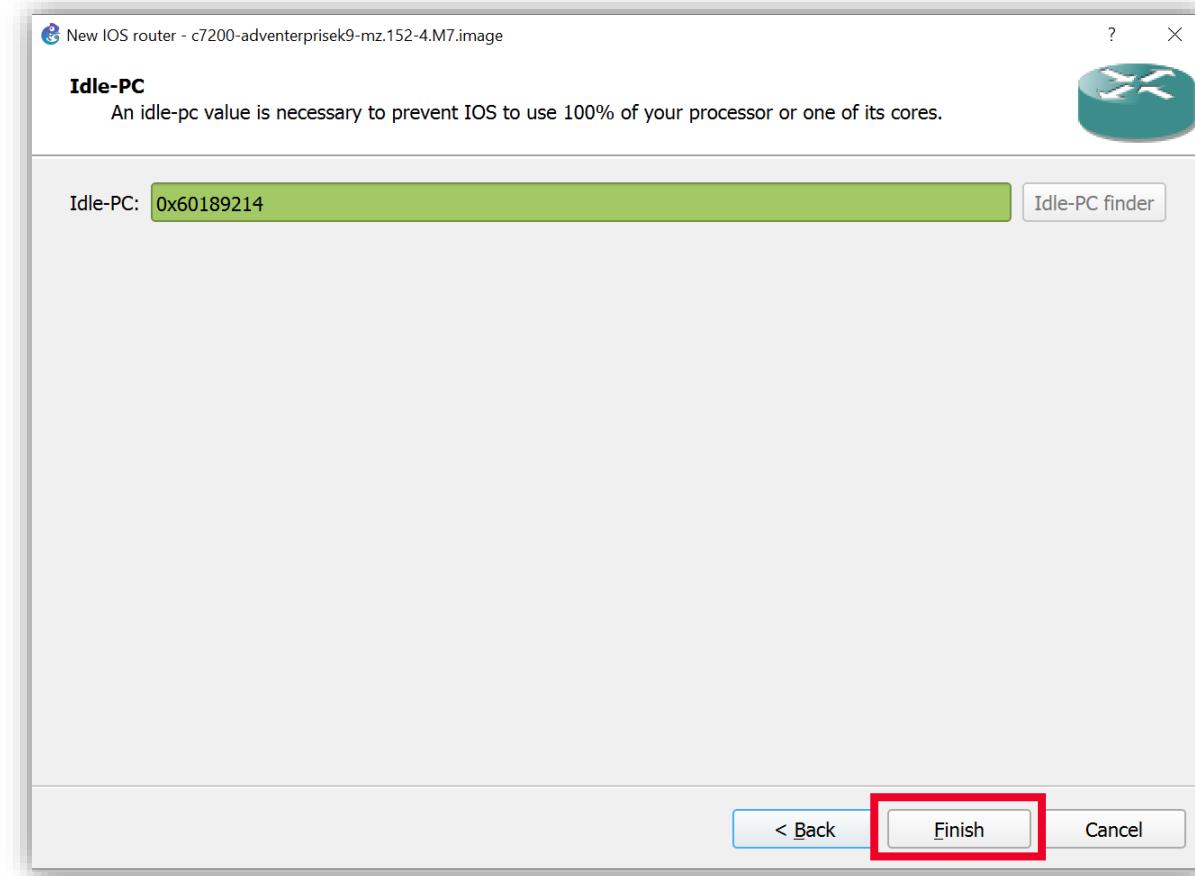


Ilustración 115: Pulsamos «*Finish*».

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- El siguiente paso será conectar entre sí los dispositivos, para ello sigue el proceso que realizaste anteriormente.
- Selecciona el icono «Add Link» y conecta el «PC1» a través de la interfaz «Ethernet0» hacia el router.

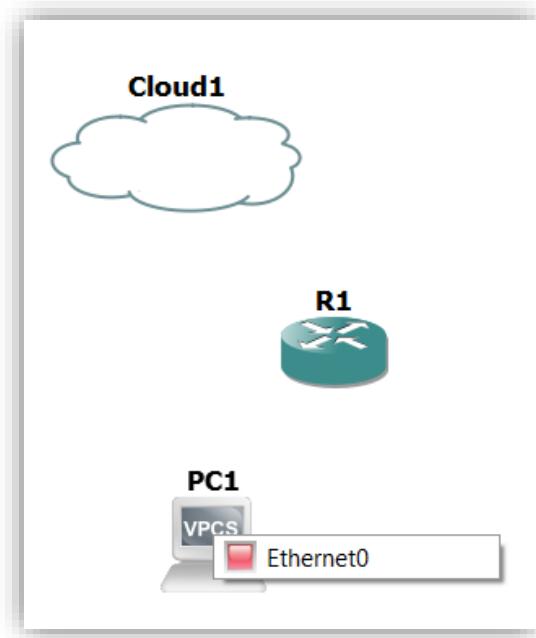


Ilustración 116: Conecta el «PC1» a través de la interfaz «Ethernet0» hacia el router.

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- Ahora selecciona la interfaz del router «FasEthernet1/0».

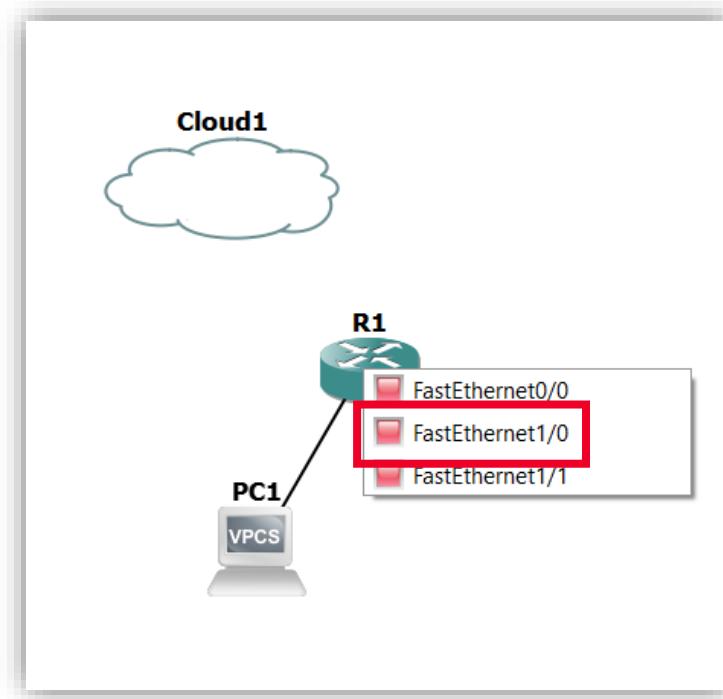


Ilustración 117: Selecciona la interfaz del router «FasEthernet1/0».

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- Para conectar el *router* a la «Cloud1» selecciona la interfaz «FastEthernet0/0» del *router* y llévalo hacia la «Cloud1».

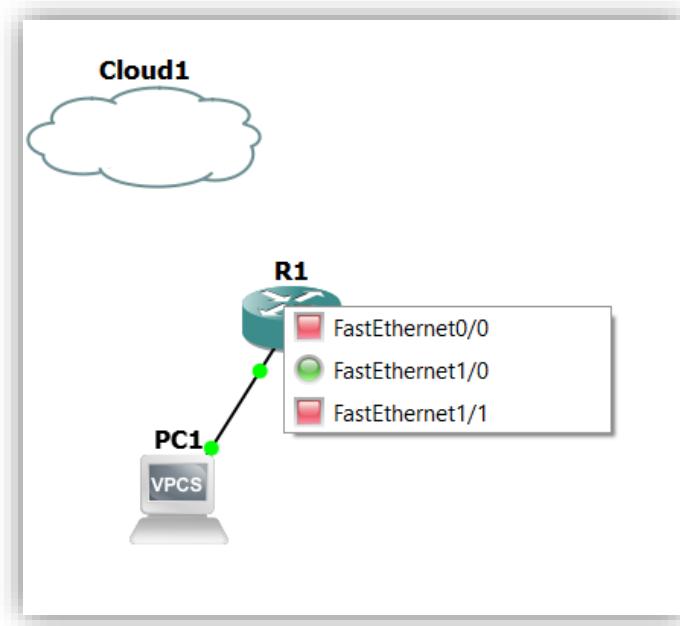


Ilustración 118: Seleccionamos
«FastEthernet0/0».

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- En el caso de la interfaz de «Cloud1» selecciona la interfaz que después se deberá comprobar si es la que asigna IP y da salida a Internet ya que, como en el ejercicio anterior, para cada equipo puede ser diferente. Recuerda añadir todas las interfaces especiales como vimos en el ejercicio anterior.

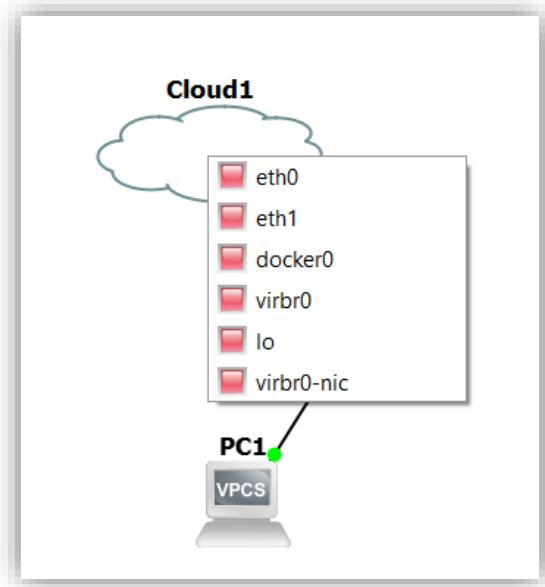


Ilustración 119: Añade todas las interfaces especiales.

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- Una vez esté todo conectado, pulsa el icono de «play» para encender todos los dispositivos.

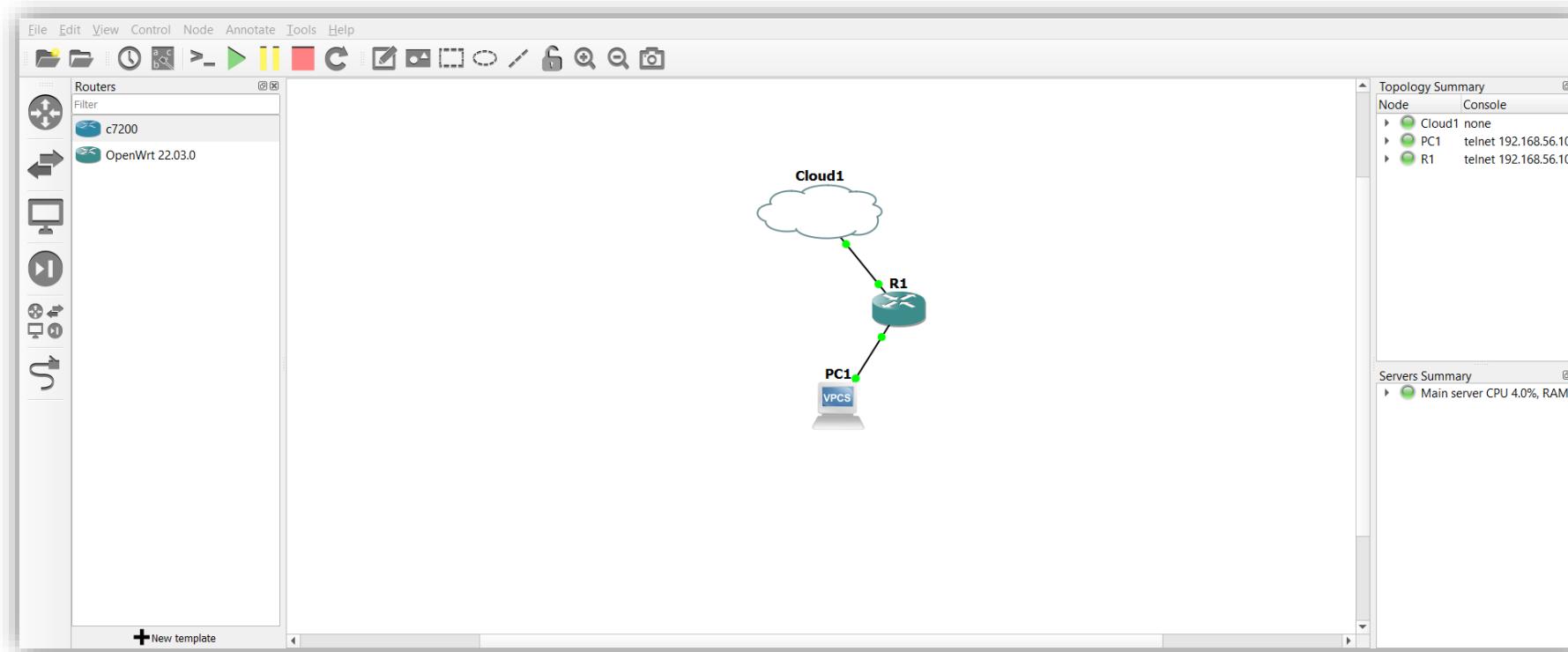


Ilustración 120: Pulsa «play» para encender todos los dispositivos.

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- Cuando esté todo conectado debes configurar tanto el VPC como el *router*.
- Lo primero que deberás hacer es configurar el VPC.
- Haz clic derecho sobre el «PC1» y selecciona «Console».
- Introduce el comando **dhcp** para que autoasigne una IP.

```
PC1> dhcp  
DDD  
Can't find dhcp server
```

Ilustración 121: Pon el comando «*dhcp*».



PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- En el caso de no hacerlo automáticamente, establecéla manualmente con el comando **<IP><Mascara><Gateway>**.
En nuestro caso el comando será **IP 10.0.0.1/24 10.0.0.2**

```
PC1> ip 10.0.0.1/24 10.0.0.2
Checking for duplicate address...
PC1 : 10.0.0.1 255.255.255.0 gateway 10.0.0.2
```

Ilustración 122: Establece manualmente la IP con el comando
«<IP><Mascara><Gateway>».

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- Ahora habrá que configurar el *router* para poder dar salida a Internet al PC.
- Primero configuraremos la interfaz «*FastEthernet0/0*», que es la interfaz que conectamos a la «*Cloud*», es decir, la red WAN.
- Para ello vuelve al servidor GNS3, haz clic derecho encima del *router* y pulsa «*Console*».



5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- Introduce los siguientes comandos:
 - «**configure terminal**»: para entrar en el modo configuración.
 - «**interface FastEthernet0/0**»: selecciona la interfaz que quieras configurar que es FastEthernet0/0.
 - «**no shut**»: para no perder la configuración en caso de que se cerrase la consola.
 - «**ip address dhcp**»: para asignar «**dhcp**» a la interfaz seleccionada. Con este protocolo DHCP lo que conseguimos es que asigne IP de forma dinámica cogiéndola de nuestro *router* de casa/empresa.
 - «**exit**»: para salir de la configuración de la interfaz seleccionada.

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface FastEthernet0/0
R1(config-if)#no shut
R1(config-if)#ip add
*Oct  4 23:27:04.341: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
R1(config-if)#ip add
*Oct  4 23:27:05.341: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#ip address dhcp
R1(config-if)#exit
R1(config)#[
```

Ilustración 123: Configuración del *router* con los comandos vistos.

5

PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- El siguiente paso será configurar la red LAN, es decir, la red que conecta el *router* con el PC.
- Para ello, pon los mismos comandos que en la interfaz anterior, pero en este caso asignaremos una IP manualmente más la máscara de subred.

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface FastEthernet1/0
R1(config-if)#no shut
R1(config-if)#ip
*Sep 29 08:02:22.047: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Sep 29 08:02:23.047: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R1(config-if)#ip address 10.0.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#exit
R1#
```

Ilustración 124: Asignaremos una IP manualmente más la máscara de subred.



PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- Ahora vamos a configurar la IP que has asignado anteriormente como un «pool» de DHCP. Es decir, se configuran el rango de IPs que esta interfaz (LAN) va a asignar automáticamente a cualquier dispositivo que se conecte.
 - «**configure terminal**».
 - «**ip dhcp pool PoolDHCP**»: para entrar en la configuración del DHCP.
 - «**network 10.0.1.0 255.255.255.0**»: asignamos el rango de IPs para el *pool* de DHCP.
 - «**default-router 10.0.1.1**»: ponemos una IP por defecto.
 - «**dns-server 10.0.1.1**»: asignamos la misma IP para el servidor de DNS.
 - «**exit**»: salimos de la configuración de DHCP.
 - «**service dhcp**»: configuramos el *router* para que funcione como servidor de DHCP.
 - «**exit**».



PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp pool PoolDHCP
R1(dhcp-config)#network 10.0.1.0 255.255.255.0
R1(dhcp-config)#default-router 10.0.1.1
R1(dhcp-config)#dns-server 10.0.1.1
R1(dhcp-config)#exit
R1(config)#service dhcp
R1(config)#exit
R1#
```

Ilustración 125: Configuramos la IP que has asignado anteriormente como un «pool» de DHCP.



PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- Desde el VPC utilizamos el comando «**dhcp**» para ver si la configuración es correcta y asigna IP automáticamente. Esto debería ser así ya que, como configuramos anteriormente, la IP de la interfaz LAN es un «*Pool de DHCP*» por lo que asignará a cada equipo que se conecte a esta una IP dentro del rango configurado.

```
PC1> dhcp  
DDORA IP 10.0.1.2/24 GW 10.0.1.1
```

Ilustración 126: utilizamos el comando «**dhcp**» para ver si la configuración es correcta.



PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

- Una vez realizada toda la configuración, vamos a ver si funciona correctamente. Comprueba la salida a Internet desde el VPC utilizando el comando «**ping**» hacia la IP de Google 8.8.8.8.

```
PC1> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=127 time=31.712 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=127 time=35.035 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=127 time=21.380 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=127 time=35.898 ms
^C
PC1>
```

Ilustración 127: Utilizamos el comando «**ping 8.8.8.8**».



PRÁCTICA: HOST CON ACCESO A INTERNET (ROUTER CISCO) Y VIRTUAL PCs (ELEMENTO VPCs)

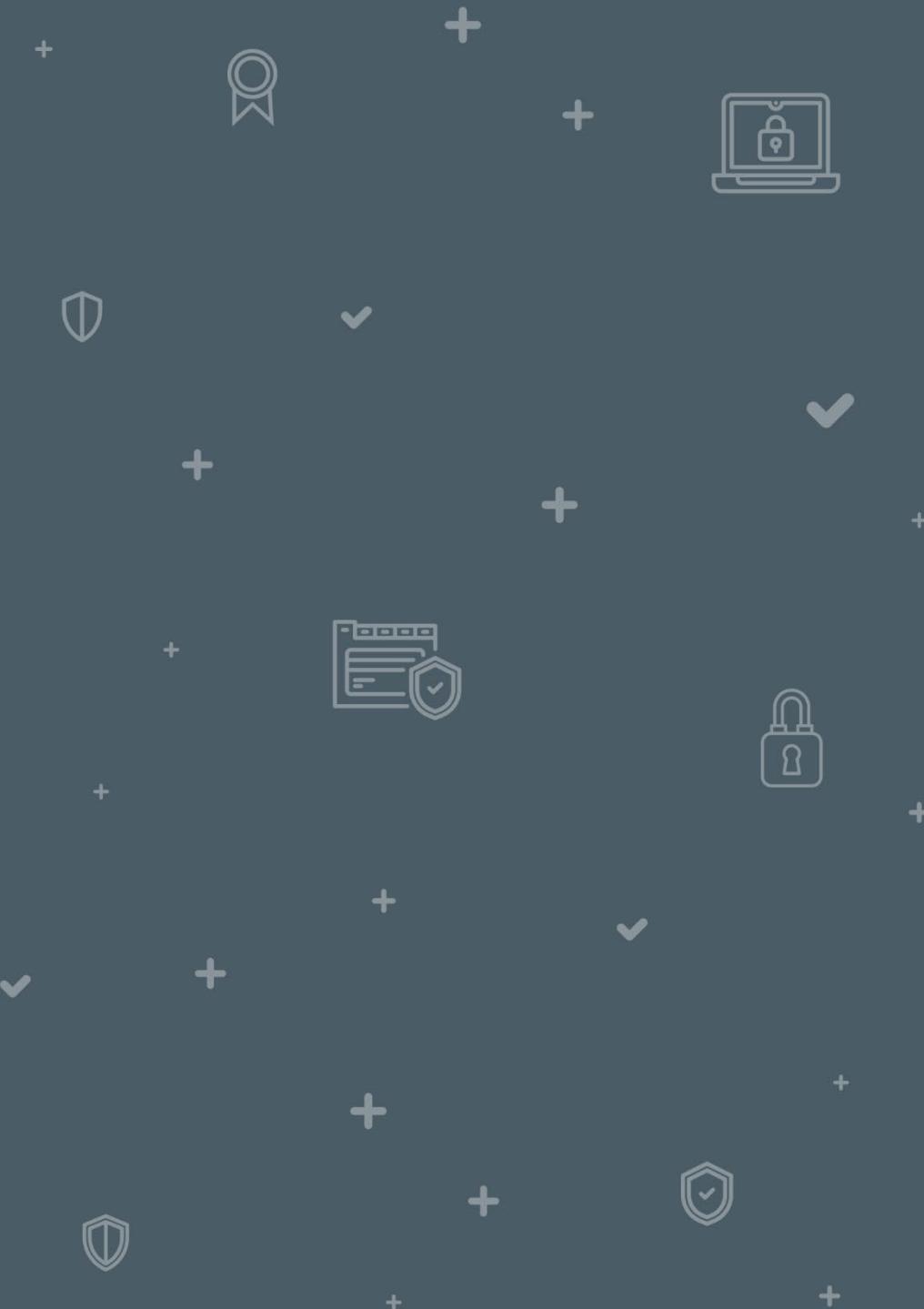
- Para comprobar la configuración y la asignación de IPs a cada interfaz utiliza el comando «**show ip interface brief**».

```
R1#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    192.168.122.230 YES  DHCP   up           up
FastEthernet1/0    10.0.1.1       YES  manual  up           up
FastEthernet1/1    unassigned     YES  unset   administratively down down
R1#
```

Ilustración 128: Utiliza el comando «**show ip interface brief**».

PRÁCTICA: SEGMENTACIÓN EN VLANs

6



6

PRÁCTICA: SEGMENTACIÓN EN VLANs

En esta parte de la práctica crearemos un ejemplo de empresa con una segmentación entre dos áreas diferentes. Una será RRHH y la otra finanzas, simulando así dos pequeña subredes. Para poner los nombres e identificar estas subredes haz clic en el menú «Annotate» y selecciona «Add note». Aparecerá un cursor en el que podrás añadir el texto deseado.

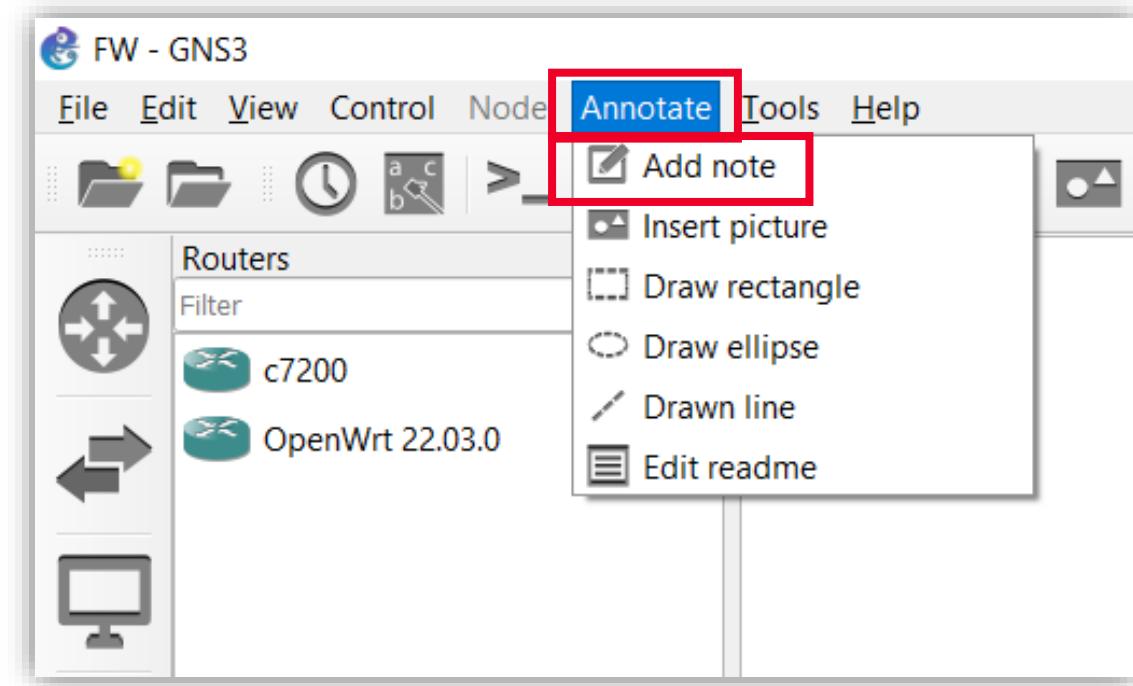


Ilustración 129: Añade los nombres e identifica las subredes.

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

Para ello, empezamos poniendo los componentes que tendrá la red que serán *switches* y ordenadores, de la forma indicada a continuación. Añadimos dos *switches* y 4 virtual PCs arrastrando los elementos como hemos ido viendo durante la práctica.

Pondremos un equipo de cada área en cada *switch* para simular dos plantas diferentes, es decir que, a pesar de pertenecer a diferentes *switches*, llegan entre sí por medio de la configuración que realizaremos a continuación.

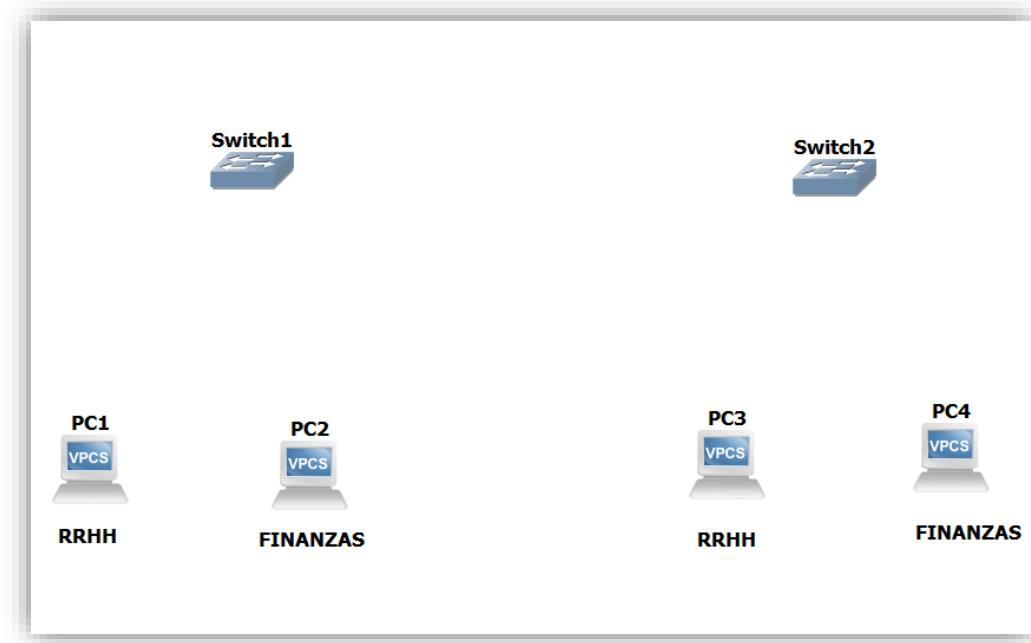


Ilustración 130: Añadimos dos *switches* y 4 virtual PCs.

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Lo primero que haremos será conectar entre sí los dispositivos. Conecta entre sí los dos *switches* a través de la interfaz «*Ethernet0*» en ambos.

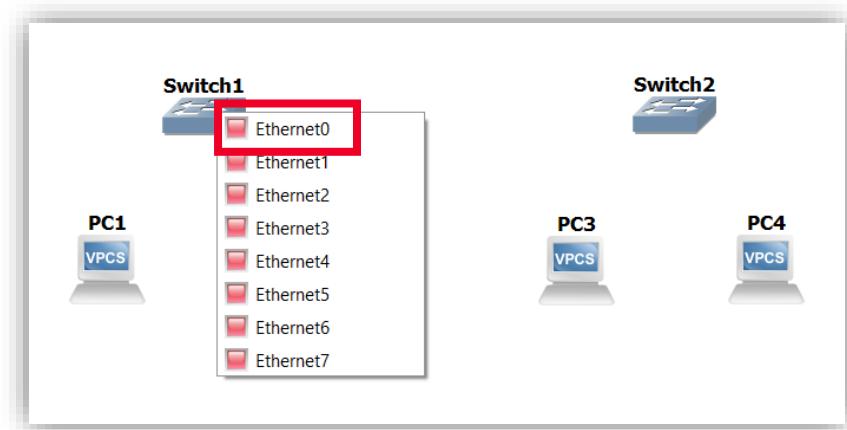


Ilustración 131: Conecta entre sí los dos *switches* a través de la interfaz «*Ethernet0*» (I).

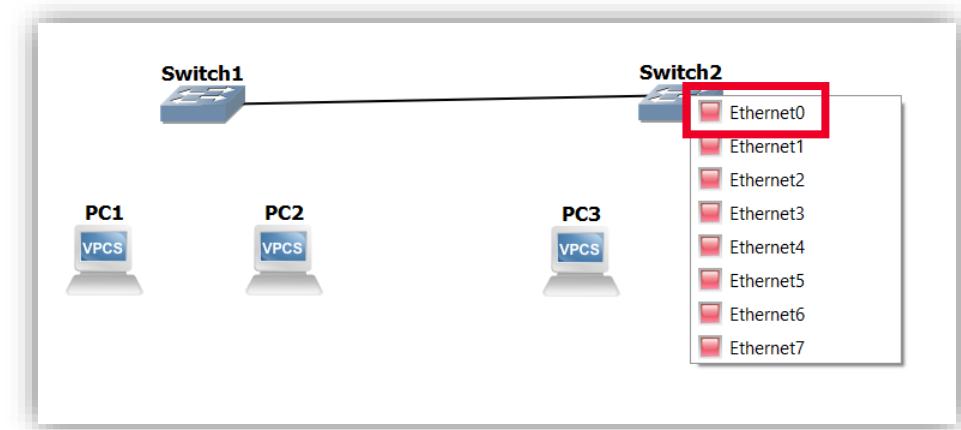


Ilustración 132: Conecta entre sí los dos *switches* a través de la interfaz «*Ethernet0*» (II).

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Después conecta los dos primeros PCs al «Switch1». Los PC a través de la interfaz «Ethernet0» y conectándolos a la interfaz «Ethernet1» del switch.

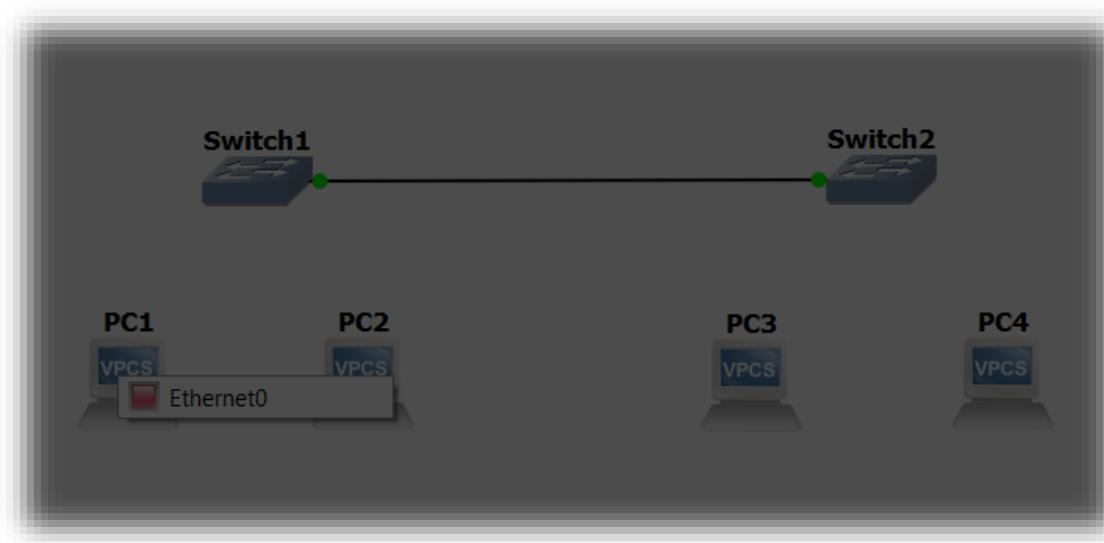


Ilustración 133: Conecta el primer PC a la interfaz «Ethernet0».

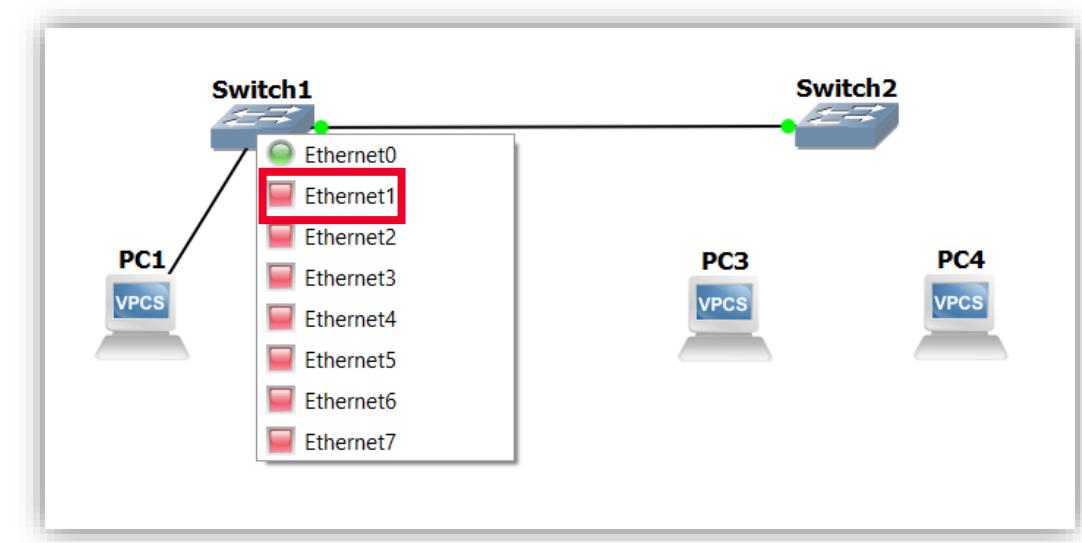


Ilustración 134: Conecta el «PC1» a la interfaz de la «Switch1».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

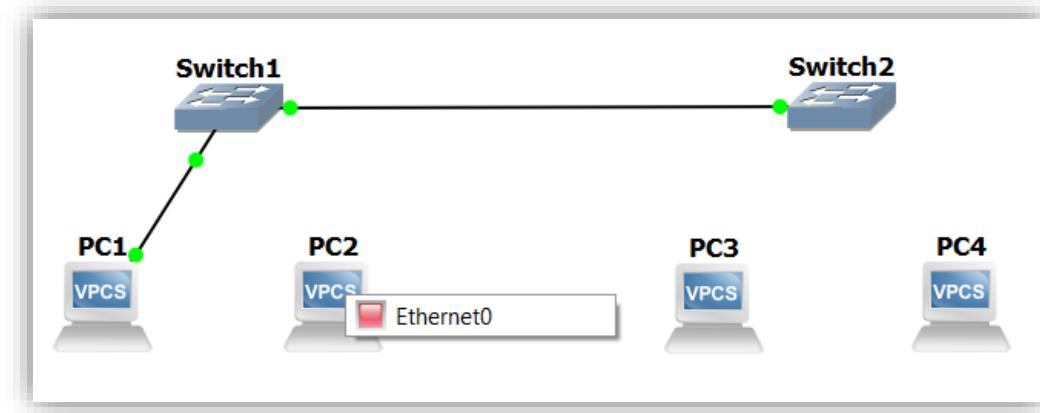


Ilustración 135: Conecta el segundo PC a la interfaz «Ethernet0».

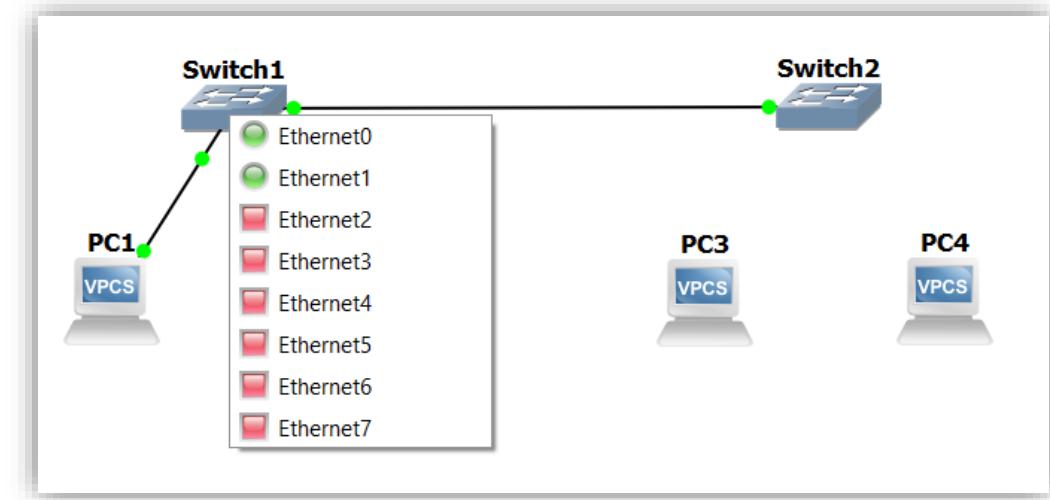


Ilustración 136: Conecta el «PC2» a la interfaz de la «Switch1».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Realiza el mismo proceso conectando el «PC3» y «PC4» al «Switch2», con los mismos valores indicados anteriormente.
- Una vez esté todo conectado, haz clic en el ícono de «Play» para encender todos los dispositivos.

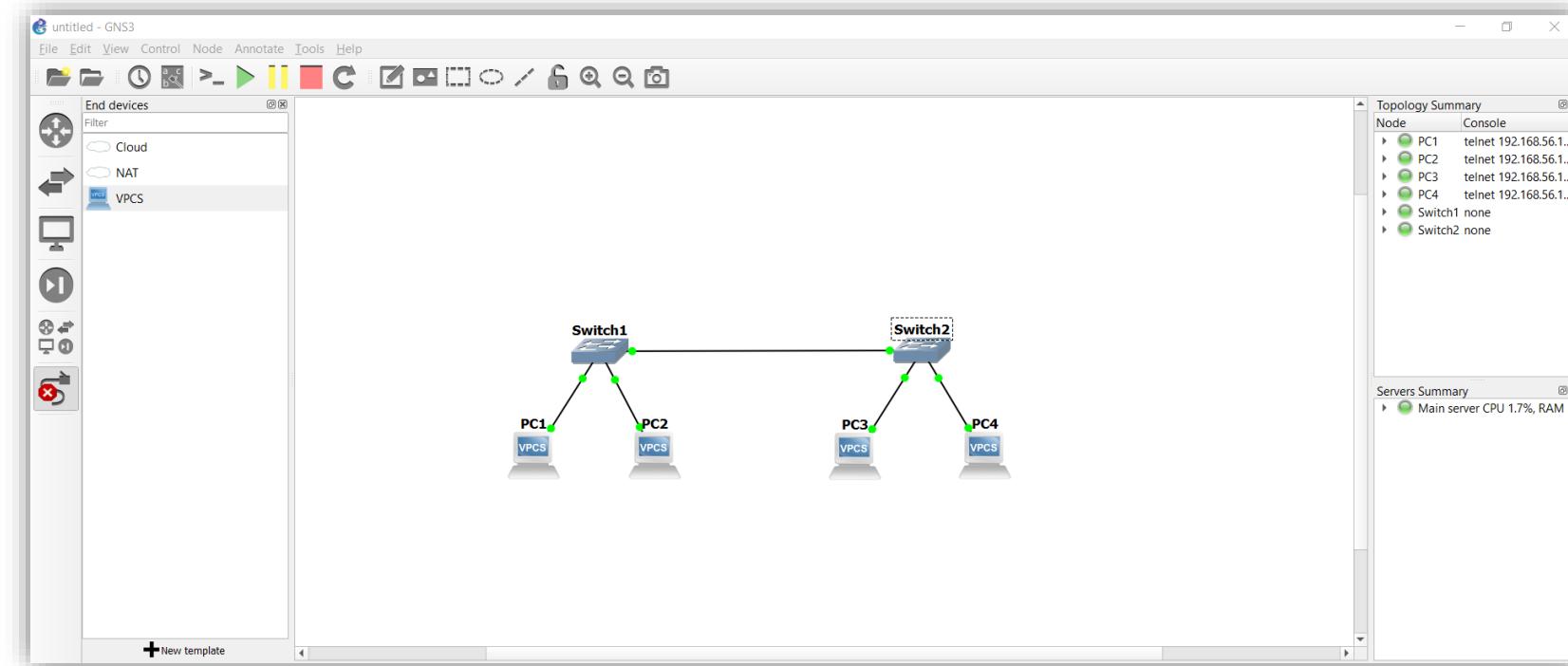


Ilustración 137: Conecta «PC3» y «PC4» al «Switch2» y pulsa «play».



PRÁCTICA: SEGMENTACIÓN EN VLANs

- Con todo conectado y encendido pasaremos a la configuración de los *switches*. Estos *Ethernet Switch*, por defecto, vienen configurados como *switches* de capa 2 que sólo trabajan con MACs y suelen estar presentes en las redes más sencillas, en este caso estos *switches* vienen con alguna función adicional para configurar VLANs, *Trunk*, *Spantree*, etc., integrado en GNS3.
- Para la configuración de los *switches* debes configurar primero los puertos que vamos a conectar.
- En el puerto 0 debes configurar un puerto con encapsulamiento «*dot1q*», estos son los llamados puertos *trunk* y sirven para mover el tráfico de varias VLANs diferentes correctamente etiquetadas.

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Empezaremos configurando el «Switch1». Para ello sitúate encima del «switch1», haz clic con el botón derecho y pulsa «Configure».

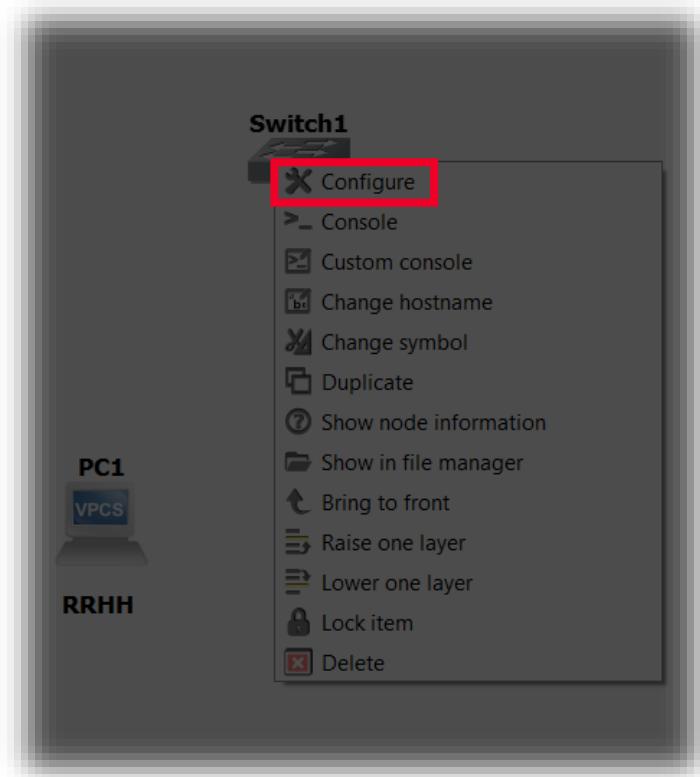


Ilustración 138: Pulsa «configure» para configurar el «switch1».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- En él selecciona el puerto 0 y en el menú de «Type» selecciona «dot1q». Para guardarlo haz clic en «Add».

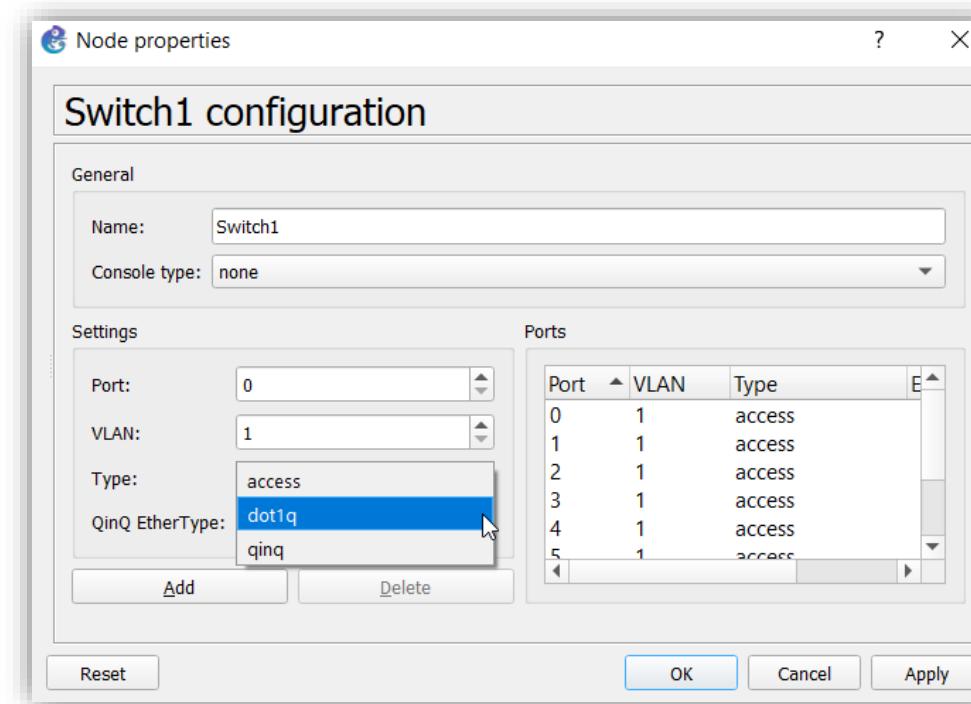


Ilustración 139: Selecciona el puerto 0 y en el menú de «Type» selecciona «dot1q».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Haz lo mismo con el puerto 3.

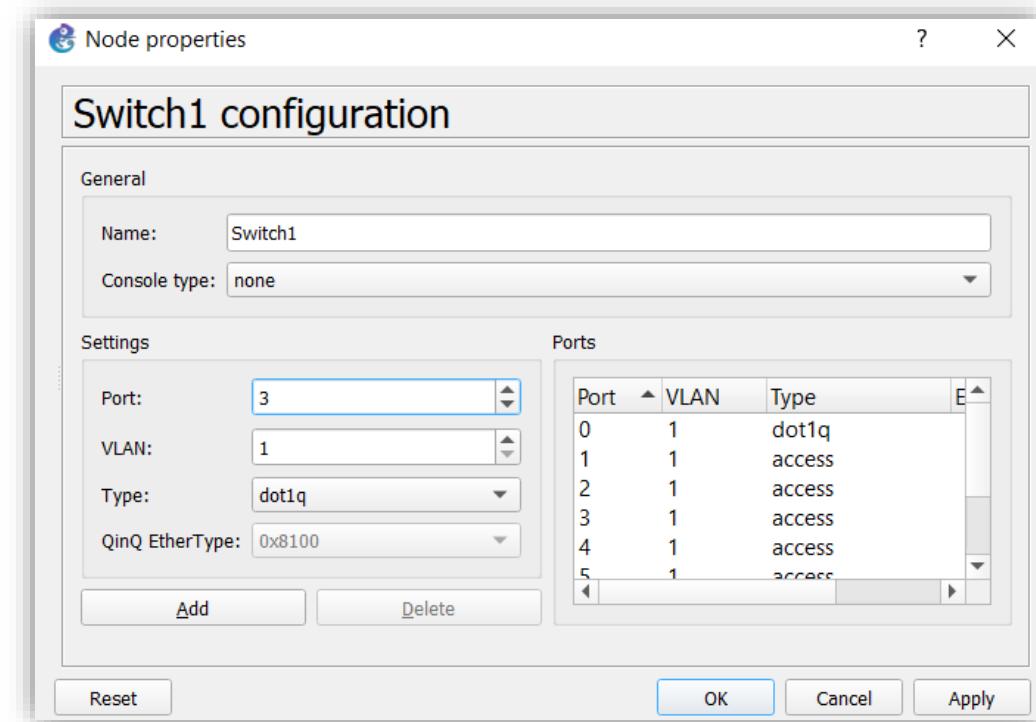


Ilustración 140: Selecciona el puerto 3 y en el menú de «Type» selecciona «dot1q».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Ahora configuraremos las diferentes VLANs: asigna la VLAN 10 al puerto 1. Como aparece en la siguiente imagen.

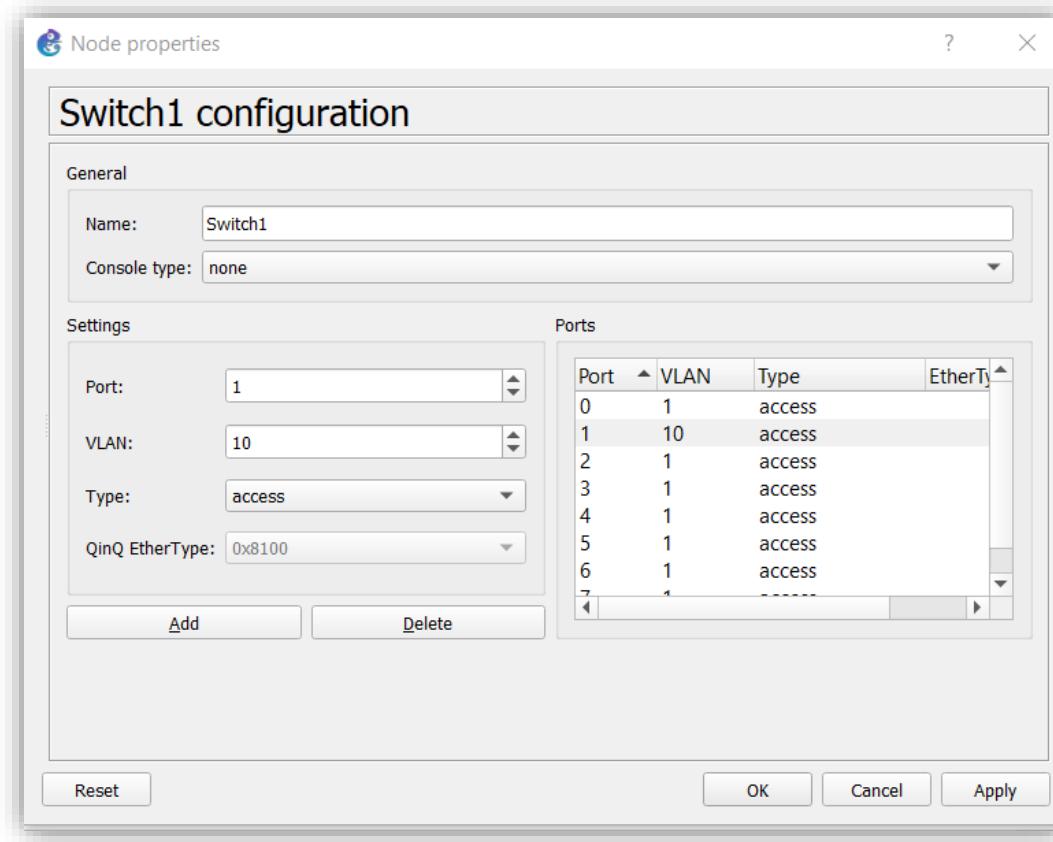


Ilustración 141: Asigna la VLAN 10 al puerto 1.

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Asigna la VLAN 20 al puerto 2 como aparece en la siguiente imagen y haz clic en «Add».

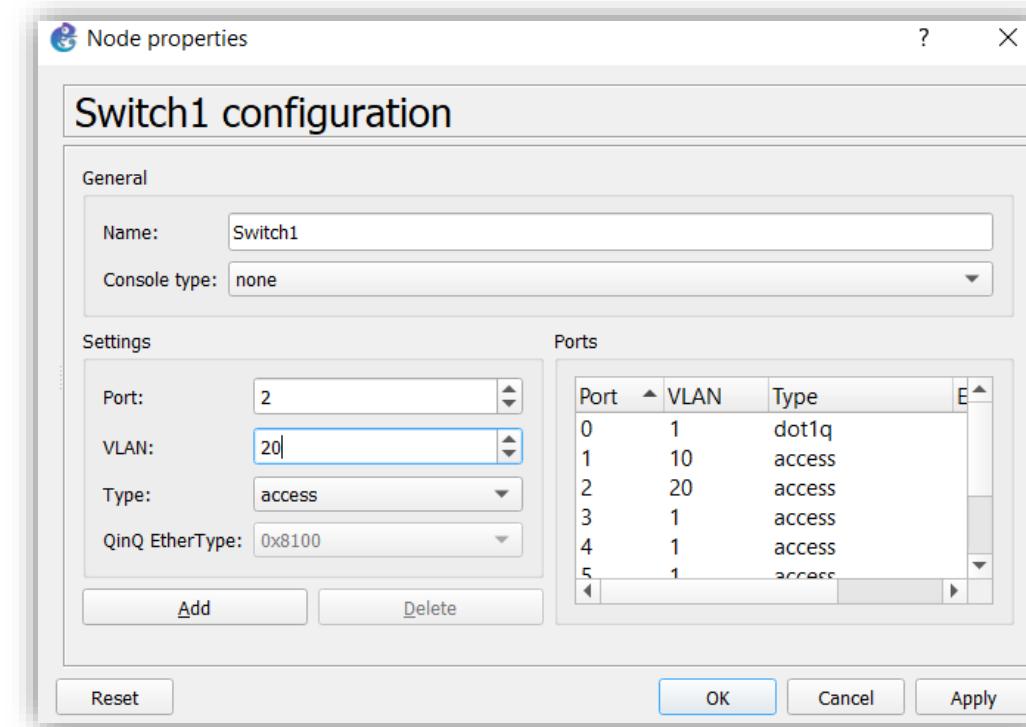


Ilustración 142: Asigna la VLAN 20 al puerto 2.

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Así debería quedar la configuración final del «switch1»:

Port	VLAN	Type	EtherTy
0	1	dot1q	
1	10	access	
2	20	access	
3	1	dot1q	
4	1	access	
5	1	access	
6	1	access	
7	1	-----	

Ilustración 143: Configuración de la «switch1».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- En el «switch2» la configuración será la misma, exceptuando el puerto 3 que en este caso no necesitamos que sea un puerto *trunk*, por lo que la configuración te deberá quedar de la siguiente forma.

Port	VLAN	Type
0	1	dot1q
1	10	access
2	20	access
3	1	access
4	1	access
5	1	access

Ilustración 144: Configuración de la «switch2».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- A continuación, pasaremos a configurar los VPC. En este caso debemos asignar manualmente la IP a cada uno de ellos a través del comando «**ip <IP/Mask> <Gateway>**». Optaremos en nuestro caso por unas IP genéricas, pero se podrá utilizar las que cada uno quiera.

Ten en cuenta que los VPC pierden la configuración cuando se apagan.

- Pulsa clic derecho sobre el VPC y haz clic en «Console». Después introduce los siguientes comandos en cada uno de ellos.
 - «PC1»:

```
PC1> ip 10.0.10.1/24 10.0.10.254
Checking for duplicate address...
PC1 : 10.0.10.1 255.255.255.0 gateway 10.0.10.254
```

Ilustración 145: Asignar IP para el «PC1».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- «PC2»:

```
PC2> ip 10.0.20.1/24 10.0.20.254
Checking for duplicate address...
PC2 : 10.0.20.1 255.255.255.0 gateway 10.0.20.254
```

Ilustración 146: Asignar IP para el «PC2».

- «PC3»:

```
PC3> ip 10.0.10.2/24 10.0.10.254
Checking for duplicate address...
PC3 : 10.0.10.2 255.255.255.0 gateway 10.0.10.254
```

Ilustración 147: Asignar IP para el «PC3».

- «PC4»:

```
PC4> ip 10.0.20.2/24 10.0.20.245
Checking for duplicate address...
PC4 : 10.0.20.2 255.255.255.0 gateway 10.0.20.245
```

Ilustración 148: Asignar IP para el «PC4».



PRÁCTICA: SEGMENTACIÓN EN VLANs

- Con el comando «**show ip**» podrás comprobar si se ha configurado de manera correcta.

```
PC1> show ip

NAME          : PC1[1]
IP/MASK       : 10.0.10.1/24
GATEWAY       : 10.0.10.254
DNS           :
MAC           : 00:50:79:66:68:00
LPORT          : 20010
RHOST:PORT    : 127.0.0.1:20011
MTU           : 1500
```

Ilustración 149: Comprobar que se ha configurado correctamente.

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Una vez finalizada la configuración, la red quedaría conectada de la siguiente manera:

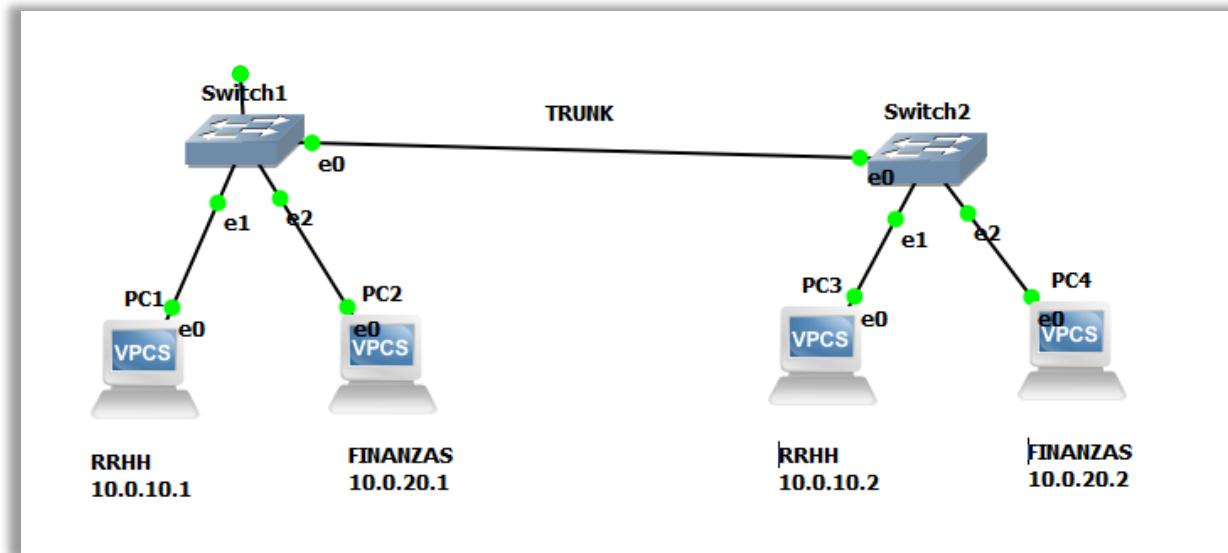


Ilustración 150: Distintos switches y PCs conectados.

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Cuando todo esté configurado y conectado, comprueba que funciona. Para ello, ejecuta el comando «**ping**» desde el «PC1» hacia la IP del «PC3» que pertenecen a la misma VLAN de RRHH y, por lo tanto, debería responder.

```
PC1> ping 10.0.10.2

84 bytes from 10.0.10.2 icmp_seq=1 ttl=64 time=0.532 ms
84 bytes from 10.0.10.2 icmp_seq=2 ttl=64 time=0.744 ms
84 bytes from 10.0.10.2 icmp_seq=3 ttl=64 time=0.736 ms
84 bytes from 10.0.10.2 icmp_seq=4 ttl=64 time=0.796 ms
84 bytes from 10.0.10.2 icmp_seq=5 ttl=64 time=1.051 ms
```

Ilustración 151: Ejecuta el comando «**ping**» desde el «PC1» hacia la IP del «PC3».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Prueba a hacer «ping» a otra IP de la VLAN de Finanzas, en este caso no debería haber respuesta.

```
PC1> ping 10.0.20.2  
host (10.0.10.254) not reachable  
  
PC1> ping 10.0.20.1  
host (10.0.10.254) not reachable
```

Ilustración 152: Haz «ping» a otra IP de la VLAN de Finanzas.

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Ahora añade un *router* Cisco y una «Cloud» para poder tener salida a Internet desde los PCs.

Recuerda añadir las interfaces de la «Cloud» como hiciste en ejercicios anteriores.

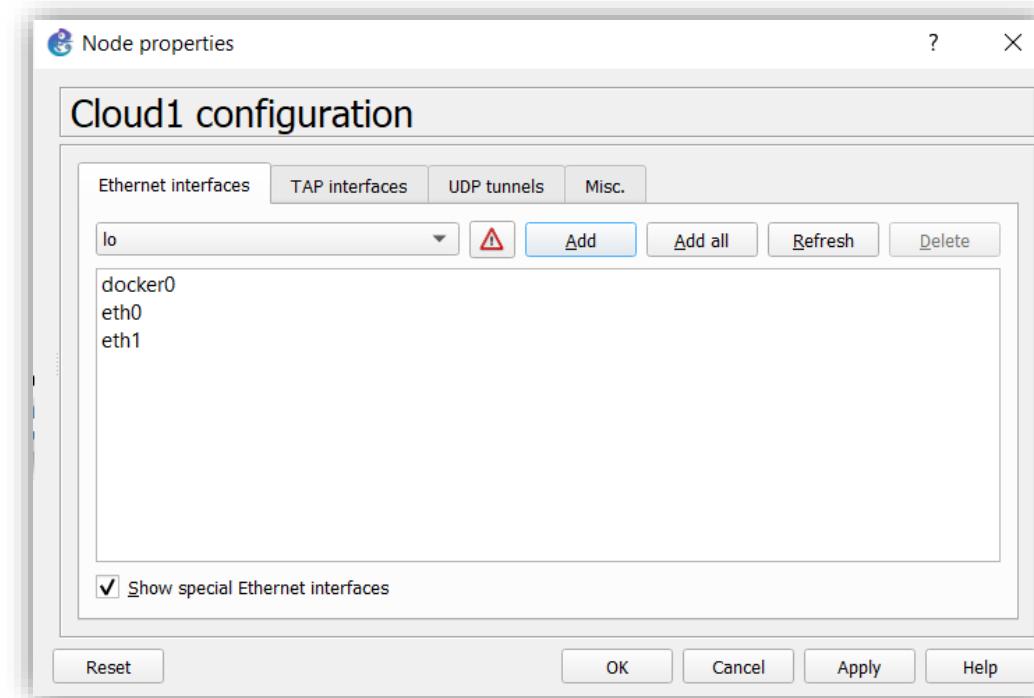


Ilustración 153: Añade un *router* cisco a una «Cloud».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Como comentamos anteriormente, y si no ejecutaste este paso, recuerda que debemos configurar el *router* Cisco con dos interfaces, ya que por defecto viene configurado sólo con una y en esta práctica necesitaremos conectar dos dispositivos.

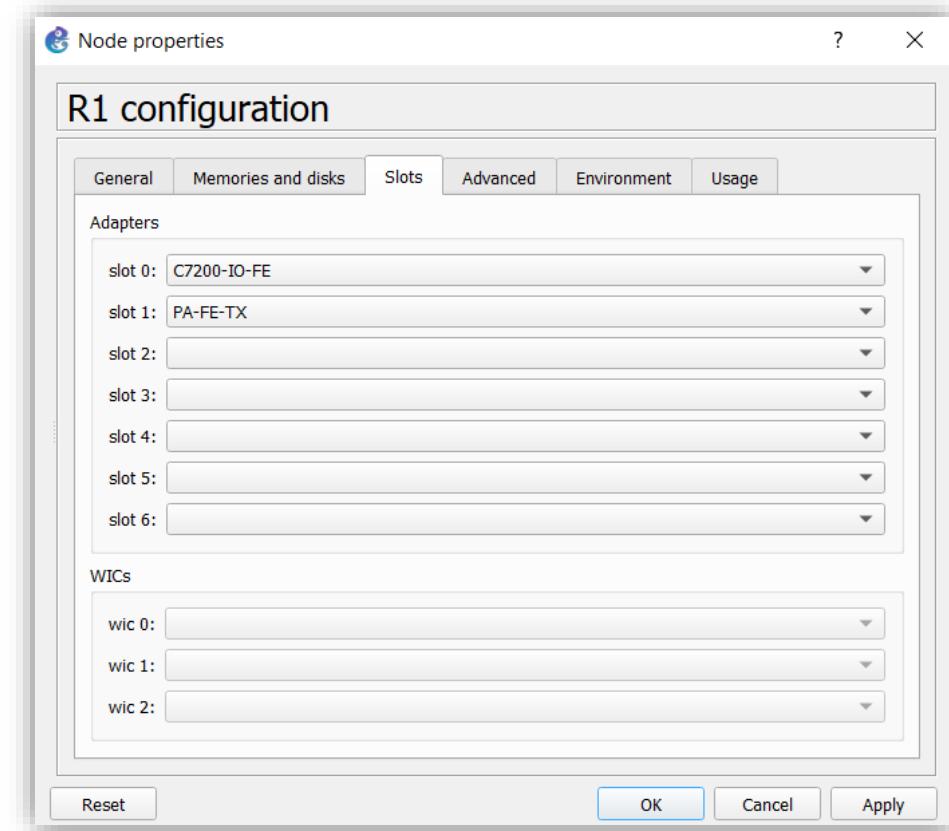


Ilustración 154: Configuración del *router* Cisco con dos interfaces.

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Ahora conecta la interfaz «FastEthernet0/0» al switch y la «FastEthernet1/0» a la «Cloud1».

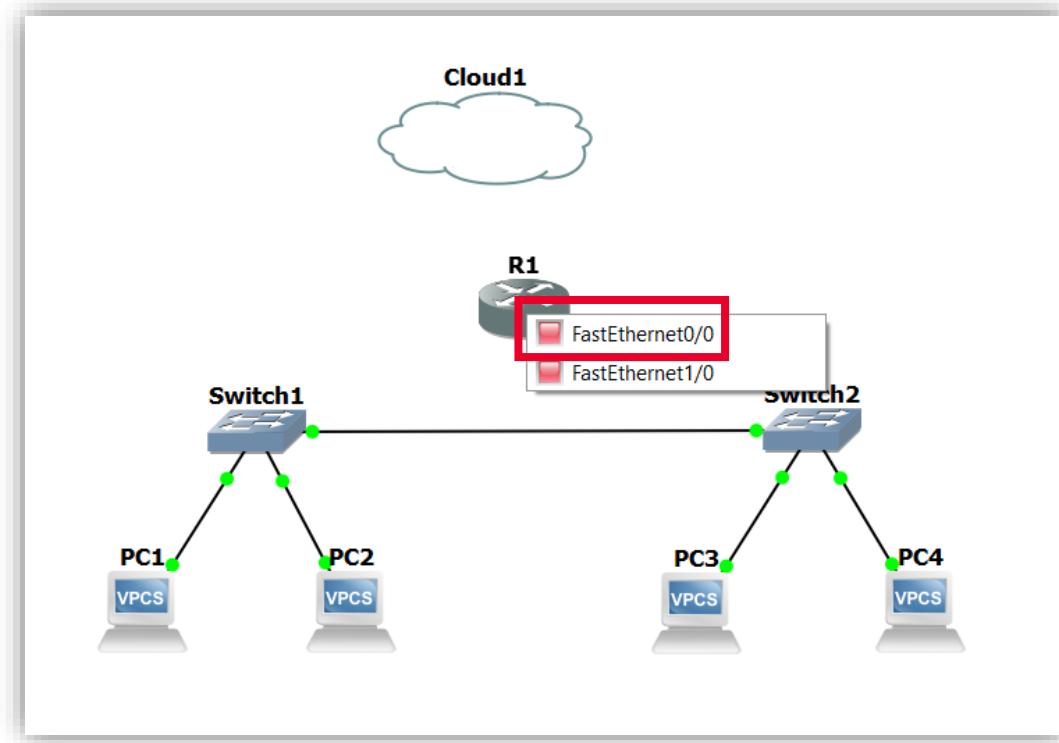


Ilustración 155: Conecta la interfaz «FastEthernet0/0» al switch.

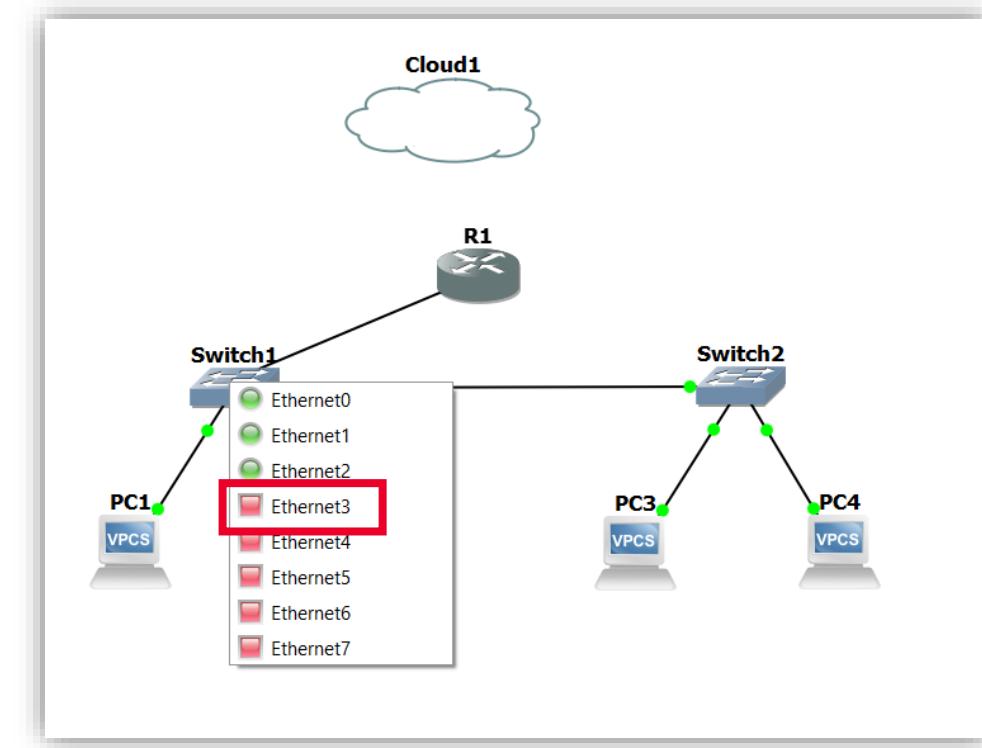


Ilustración 156: Conecta la «Ethernet3».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

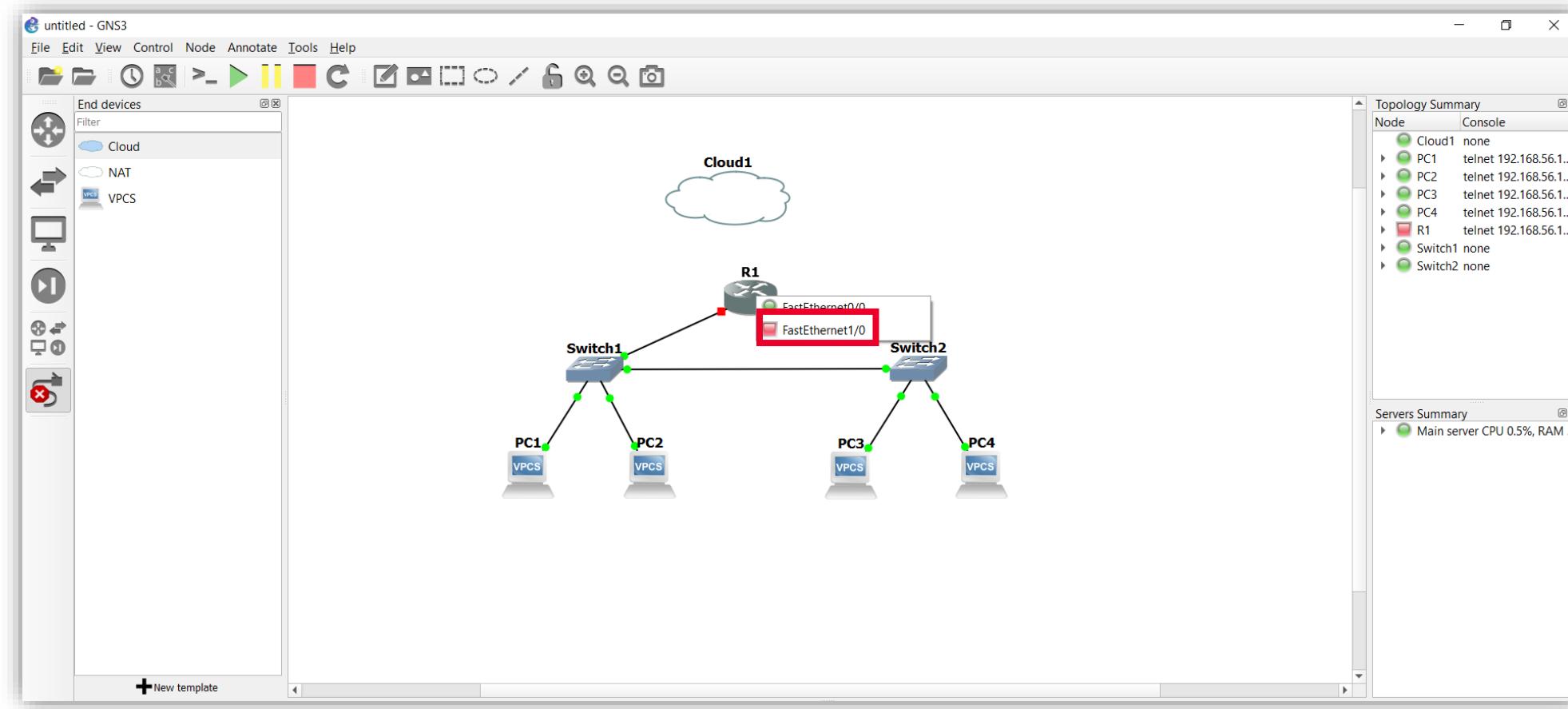


Ilustración 157: Conecta la interfaz «FastEthernet1/0» a la «Cloud1».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- En este caso elige la interfaz que te funcionó en el ejercicio anterior, aunque podrías tener que cambiarla si no asignase IP o esta no tuviese salida a Internet como vimos anteriormente.

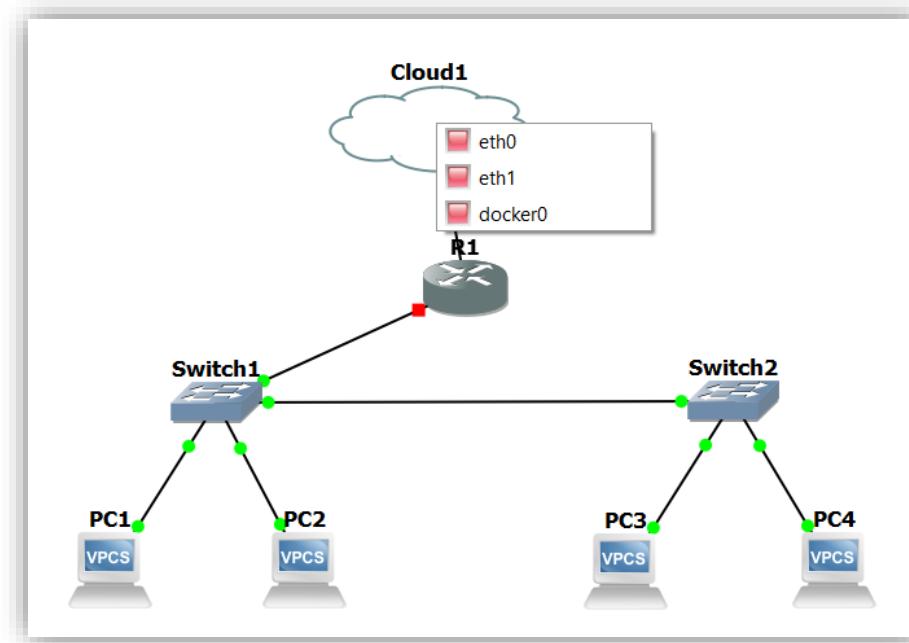


Ilustración 158: Elige la interfaz.

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Ahora, enciende el *router* que has añadido. ¡Comenzamos con la configuración!
- Haz clic derecho del ratón sobre el *router* y pulsa en «Console».
- Para la configuración del *router* ejecutaremos los siguientes comandos. Configura primero la interfaz que va al «switch1» (LAN):
 - «**configure terminal**»: entrar en modo configuración.
 - «**interface FastEthernet0/0**»: entra en la configuración de la interfaz seleccionada.
 - «**no shut**»: para no perder la configuración al apagar el *router*.
 - «**interface FastEthernet0/0.10**»: con esto creamos dos subinterfaces de la misma interfaz para poder asignar dos IPs a una interfaz para las dos VLANs que hemos creado.
 - «**encapsulation dot1Q 10**»: con esto configuramos el modo «trunk» para la VLAN 10 y permitir el tráfico entre las dos VLANs.

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- «**ip address 10.0.10.254 255.255.255.0**»: asignamos manualmente la IP que debe ser la misma que la del *Gateway* del «PC1» y «PC3» correspondientes a la VLAN de RRHH.
- «**Ctrl+Z**»: para salir.

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface FastEthernet0/0
R1(config-if)#no shut
R1(config-if)#interface FastEthernet0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 10.0.10.254 255.255.255.0
% 10.0.10.0 overlaps with FastEthernet0/0
R1(config-subif)#^Z
R1#
```

Ilustración 159: Configuración del *router* para la primera interfaz.



6 PRÁCTICA: SEGMENTACIÓN EN VLANs

- Sigue con la configuración del *router* ahora crearemos la otra subinterfaz para la VLAN de finanzas con los siguientes comandos:
 - «**configure terminal**»: entrar en modo configuración.
 - «**interface FastEthernet0/0**»: entra en la configuración de la interfaz seleccionada.
 - «**no shut**»: para no perder la configuración al apagar el *router*.
 - «**interface FastEthernet0/0.20**»: con esto crearemos la otra subinterfaz que necesitamos para la VLAN de finanzas y asignarle la otra IP.
 - «**encapsulation dot1Q 20**»: configurar el modo «*trunk*» para la VLAN 20 y permitir el tráfico entre las dos VLANs.

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- «**ip address 10.0.20.254 255.255.255.0**»: asignamos manualmente la IP que debe ser la misma que la del *Gateway* del «PC2» y «PC4» correspondientes a la VLAN de finanzas.
- «**Ctrl+Z**»: para salir.

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface FastEthernet0/0
R1(config-if)#no shut
R1(config-if)#interface FastEthernet0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 10.0.20.254 255.255.255.0
R1(config-subif)#^Z
R1#
```

Ilustración 160: Configuración de *router* para la segunda interfaz.

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Configura ahora la interfaz que va a la «Cloud» (WAN) para obtener salida a internet con los siguientes comandos:
 - «**configure terminal**»: entrar en modo configuración.
 - «**interface FastEthernet1/0**»: entra en la configuración de la interfaz seleccionada.
 - «**no shut**»: para no perder la configuración al apagar el *router*.
 - «**ip address dhcp**»: configura esta interfaz con DHCP para que asigne IP automáticamente.
 - «**Ctrl+Z**»: para salir.

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface FastEthernet1/0
R1(config-if)#no shut
R1(config-if)#ip add
*Oct  3 10:39:50.143: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Oct  3 10:39:51.143: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R1(config-if)#ip address dhcp
R1(config-if)#^Z
R1#
```

Ilustración 161: Configuración de la «Cloud» (WAN).

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Así debería quedar la configuración final de la arquitectura:

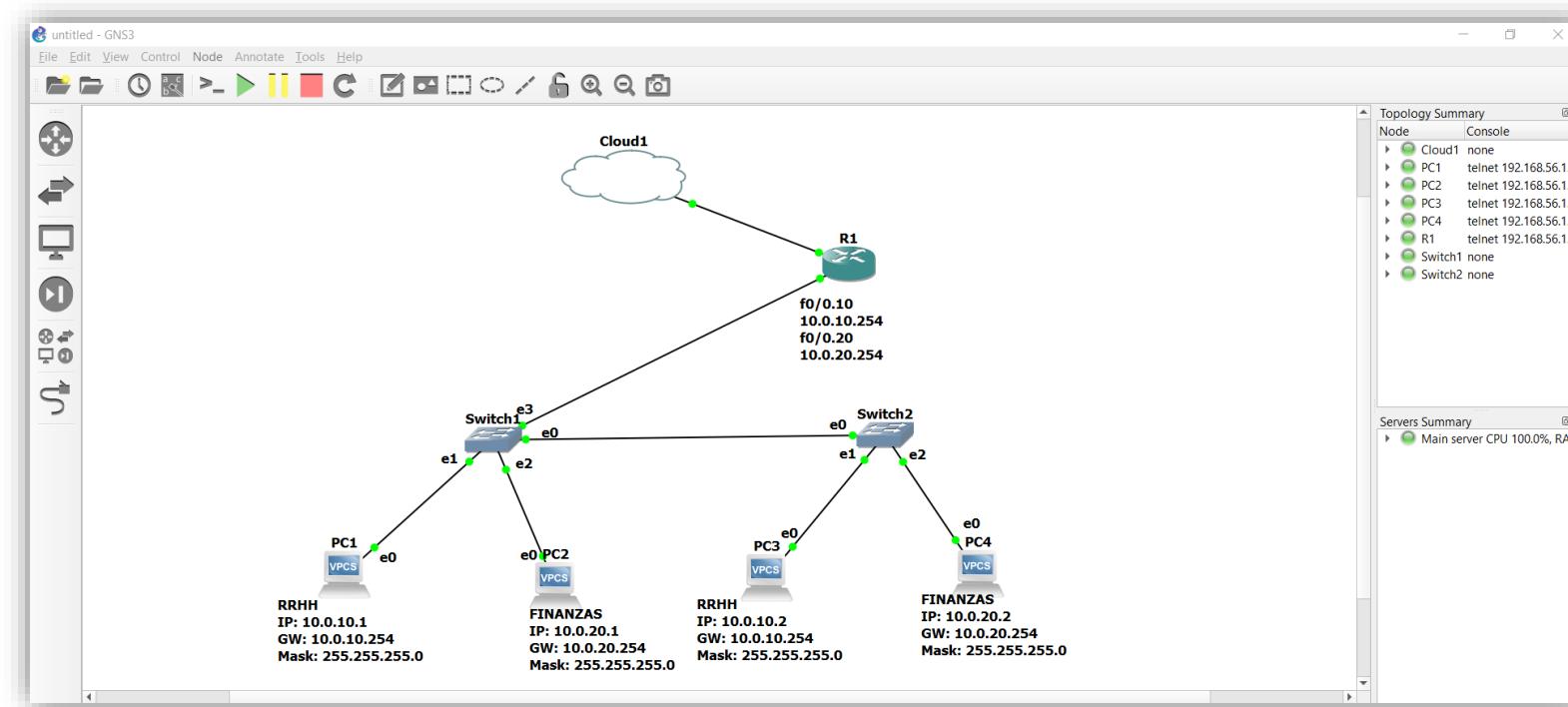


Ilustración 162: Configuración final de la arquitectura.

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Para comprobar que funciona y que has configurado todo de manera correcta ejecuta el comando «**ping**» desde el *router* a la IP de Google. Si responde es que se ha configurado de manera correcta.

```
R1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/31/52 ms
```

Ilustración 163: Comprueba con el comando «**ping**» que funciona correctamente.

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Al ejecutar el comando «**ping**» hacia la web de Google observamos que no da respuesta, ya que no hemos configurado el servidor de DNS, por lo procederemos a configurarlo.

```
R1#ping google.com
Translating "google.com"
% Unrecognized host or address, or protocol not running.
```

Ilustración 164: No hay respuesta si ejecutamos el comando «**ping**» hacia la web de Google.

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Configuración del *router* para que use el servidor de DNS correcto:
 - «**configure terminal**»: entra en el modo configuración.
 - «**ip domain-lookup**»: habilita la traducción de nombre a dirección basado en DNS del *host*.
 - «**ip name-server 8.8.8.8**»: este comando establece el servidor de nombres del *router* para las consultas de DNS, en este caso utilizaremos la IP de Google.
 - «**end**»: para terminar la configuración.

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip domain-lookup
R1(config)#ip name-server 8.8.8.8
R1(config)#end
R1#
```

Ilustración 165: Configuración del *router* para que use el servidor DNS correcto.



PRÁCTICA: SEGMENTACIÓN EN VLANs

- Comprueba que puedes hacer «ping» a Google.com

```
R1#ping google.com
Translating "google.com"...domain server (192.168.72.2) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 142.250.184.174, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/72/128 ms
o...■
```

Ilustración 166: Comprueba que puedes hacer «ping» a Google.com.



PRÁCTICA: SEGMENTACIÓN EN VLANs

- Ahora comprueba que los PC pueden hacer «ping» a su puerta de enlace predeterminada o *Gateway* que es el nodo que sirve como enlace entre dos redes y conecta y dirige el tráfico.

```
PC1> ping 10.0.10.254

10.0.10.254 icmp_seq=1 timeout
84 bytes from 10.0.10.254 icmp_seq=2 ttl=255 time=12.720 ms
84 bytes from 10.0.10.254 icmp_seq=3 ttl=255 time=8.210 ms
84 bytes from 10.0.10.254 icmp_seq=4 ttl=255 time=8.582 ms
```

Ilustración 167: Comprueba que puedes hacer «ping» a la puerta de enlace predeterminada para «PC1».



PRÁCTICA: SEGMENTACIÓN EN VLANs

```
PC2> ping 10.0.20.254

84 bytes from 10.0.20.254 icmp_seq=1 ttl=255 time=10.009 ms
84 bytes from 10.0.20.254 icmp_seq=2 ttl=255 time=8.169 ms
84 bytes from 10.0.20.254 icmp_seq=3 ttl=255 time=11.270 ms
84 bytes from 10.0.20.254 icmp_seq=4 ttl=255 time=11.442 ms
84 bytes from 10.0.20.254 icmp_seq=5 ttl=255 time=16.602 ms
```

Ilustración 168: Comprueba que puedes hacer «ping» a la puerta de enlace predeterminada para «PC2».

```
PC3> ping 10.0.10.254

84 bytes from 10.0.10.254 icmp_seq=1 ttl=255 time=14.018 ms
84 bytes from 10.0.10.254 icmp_seq=2 ttl=255 time=7.690 ms
84 bytes from 10.0.10.254 icmp_seq=3 ttl=255 time=15.793 ms
^C
```

Ilustración 169: Comprueba que puedes hacer «ping» a la puerta de enlace predeterminada para «PC3».



PRÁCTICA: SEGMENTACIÓN EN VLANs

```
PC4> ping 10.0.20.254  
84 bytes from 10.0.20.254 icmp_seq=1 ttl=255 time=149.115 ms  
84 bytes from 10.0.20.254 icmp_seq=2 ttl=255 time=14.506 ms  
84 bytes from 10.0.20.254 icmp_seq=3 ttl=255 time=4.784 ms  
^C
```

Ilustración 170: Comprueba que puedes hacer «ping» a la puerta de enlace predeterminada para «PC4».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- También comprobaremos que entre todos los PC se hacen «*ping*». Ya que al incluir el *router* con puerto *trunk* permite el paso de las dos VLAN.

```
PC1> ping 10.0.20.1

84 bytes from 10.0.20.1 icmp_seq=1 ttl=63 time=27.222 ms
84 bytes from 10.0.20.1 icmp_seq=2 ttl=63 time=13.592 ms
^C
PC1> ping 10.0.20.2

84 bytes from 10.0.20.2 icmp_seq=1 ttl=63 time=25.512 ms
84 bytes from 10.0.20.2 icmp_seq=2 ttl=63 time=11.703 ms
84 bytes from 10.0.20.2 icmp_seq=3 ttl=63 time=18.809 ms
^C
PC1> ping 10.0.10.2

84 bytes from 10.0.10.2 icmp_seq=1 ttl=64 time=0.486 ms
84 bytes from 10.0.10.2 icmp_seq=2 ttl=64 time=0.271 ms
84 bytes from 10.0.10.2 icmp_seq=3 ttl=64 time=0.320 ms
^C
```

Ilustración 171: Comprueba que todos los PC se hacen «*ping*».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Para que los VPC puedan hacer «ping» al «8.8.8.8» tenemos que configurar la NAT (*Network Address Translation*) en nuestro *router* en todas las interfaces.
- Para ello haz clic derecho en el *router* y pulsa «console». Después utiliza los siguientes comandos:
 - «**configure terminal**»: entrar en modo configuración.
 - «**interface FastEthernet1/0**»: entra en la configuración de la interfaz seleccionada.
 - «**no shut**»: para no perder la configuración al apagar el *router*.
 - «**ip nat outside**»: indica que va a inspeccionar los paquetes originados desde una interfaz interna hacia una externa.
 - «**Ctrl+Z**»: para salir.

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface FastEthernet1/0
R1(config-if)#no shut
R1(config-if)#ip nat outside
R1(config-if)#^Z
R1#
*21:56:28:22.575%NOVIC-CONNET-5-Serial-1
```

Ilustración 172: Configuración para hacer «ping» al «8.8.8.8» en la interfaz «FastEthernet1/0».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- «**configure terminal**»: entrar en modo configuración.
- «**interface FastEthernet0/0.10**»: entra en la configuración de la interfaz seleccionada.
- «**no shut**»: para no perder la configuración al apagar el *router*.
- «**ip nat inside**»: indica que va a inspeccionar los paquetes originados desde una interfaz externa hacia una interna.
- «**Ctrl+Z**»: para salir.

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface FastEthernet0/0.10
R1(config-subif)#no shut
R1(config-subif)#ip nat inside
R1(config-subif)#exit
R1(config)#[
```

Ilustración 173: Configuración para hacer «*ping*» al «8.8.8.8» en la interfaz «*FastEthernet0/0.10*».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- «**interface FastEthernet0/0.20**»: entra en la configuración de la interfaz seleccionada.
- «**no shut**»: para no perder la configuración al apagar el *router*.
- «**ip nat inside**»: indica que va a inspeccionar los paquetes originados desde una interfaz externa hacia una interna.
- «**exit**»: para salir de la configuración de la interfaz.

```
R1(config)#interface FastEthernet0/0.20
R1(config-subif)#no shut
R1(config-subif)#ip nat inside
R1(config-subif)#exit
R1(config)#[
```

Ilustración 174: Configuración para hacer «ping» al «8.8.8.8» en la interfaz «FastEthernet0/0.20».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Ahora, configura la lista de control de acceso en el *router*. Esto lo que hace es permitir todo lo que esté dentro del rango que le estas indicando, es decir, todo lo que está dentro del segmento de red de la 10.0.X.X.
 - «**ip nat inside source list 10 interface FastEthernet1/0 overload**»
 - «**ip nat inside**»: hace la traducción de direcciones IP que entran a pedir o llevar información a través del *router* y traduce las diferentes IPs privadas en una IP pública.
 - «**source list 10**»: lista que hemos creado con las IPs de origen que tendrán permitido hacer consultas o usar el *router*.
 - «**interface FastEthernet1/0**»: interfaz de red que usarán.
 - «**overload**»: se usará NAT con sobrecarga.

```
R1(config)#access-list 10 permit 10.0.0.0 0.0.255.255
R1(config)#ip nat inside source list 10 interface FastEthernet1/0 overload
R1(config)#end
R1#
```

Ilustración 175: Configura la lista de control de acceso.

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Para guardar la configuración ejecuta el comando «**write memory**».

```
R1#write memory
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]Y
Building configuration...
[OK]
```

Ilustración 176: Ejecuta el comando «*write memory*».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Además, y aunque en este caso no sea necesario, en algunas redes puede que necesites configurar una ruta por defecto en el *router*. Esto es por dónde irán todos los paquetes de red que no tengan un destino reconocido.
- El comando se compone de:
 - **ip route 0.0.0.0 0.0.0.0 FastEthernet1/0 <la IP de nuestra máquina GNS3 / máquina a la que deberá saltar el paquete>**
- Para eliminar las rutas estáticas (si la llamamos) podemos usar el comando:
 - **No ip route <ip> <mascara> <interfaz>**
 - O en el caso de querer borrarlas todas: **no ip route ***

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Comprueba que los VPC puedan hacer «ping» al «8.8.8.8», luego intenta comprobar si pueden hacer «ping» al dominio google.es, verás que no pueden.

```
PC4> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=127 time=130.579 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=127 time=82.173 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=127 time=11.513 ms
^C

PC4> ping google.es
Cannot resolve google.es
```

Ilustración 177: Comprobar que los VPCs pueden hacer «ping» al «8.8.8.8».

6

PRÁCTICA: SEGMENTACIÓN EN VLANs

- Esto se debe a que debemos configurar el servidor de DNS en los VPC. Para ello, introduce el comando «**ip dns 8.8.8.8**» y luego vuelve a hacer «**ping**» al dominio google.com, verás que ahora sí se obtiene respuesta.

```
PC4> ip dns 8.8.8.8

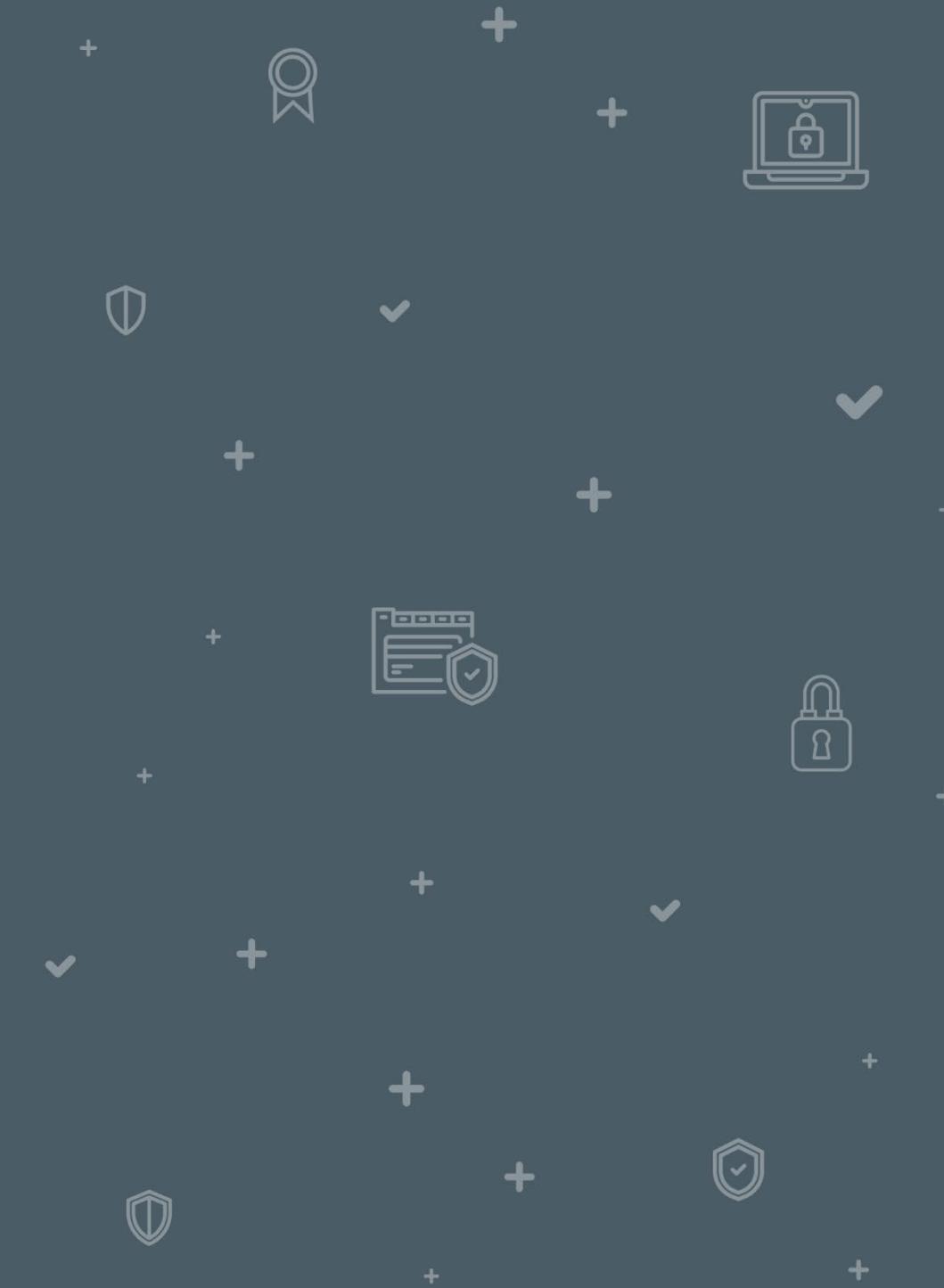
PC4> ping google.com
google.com resolved to 142.250.200.110

84 bytes from 142.250.200.110 icmp_seq=1 ttl=127 time=19.885 ms
84 bytes from 142.250.200.110 icmp_seq=2 ttl=127 time=20.466 ms
84 bytes from 142.250.200.110 icmp_seq=3 ttl=127 time=20.374 ms
^C
PC4>
```

Ilustración 178: Utiliza el comando «**ip dns 8.8.8.8**» y vuelve a comprobar que obtiene respuesta con el dominio de Google.com.

PRÁCTICA: TOPOLOGÍA DE RED CON FW

7



7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

Para la realización de esta práctica, tendrás que descargar los archivos «**FGT_VM64_KVM-v6-build1579-FORTINET.out.kvm**» y «**empty30G.qcow2**» que encontrarás entre los recursos descargables de la unidad.

- Entra en la página de «*Appliances*» de GNS3.

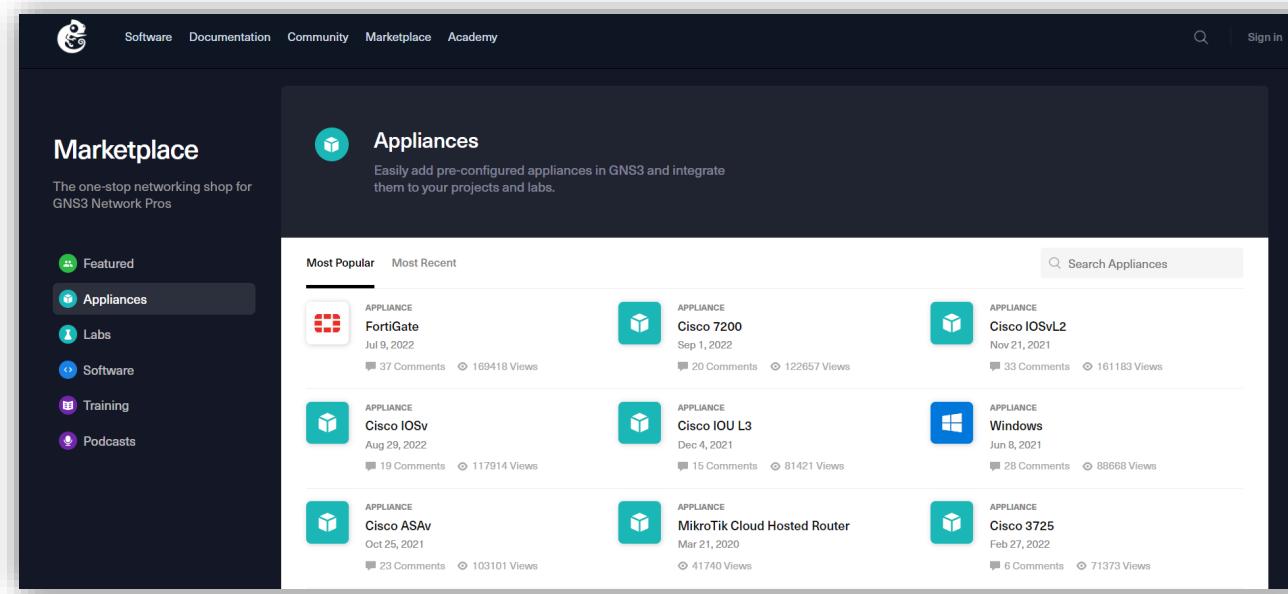


Ilustración 179: Accede a «*Appliances*».

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Selecciona «FortiGate» y pulsa «Download».

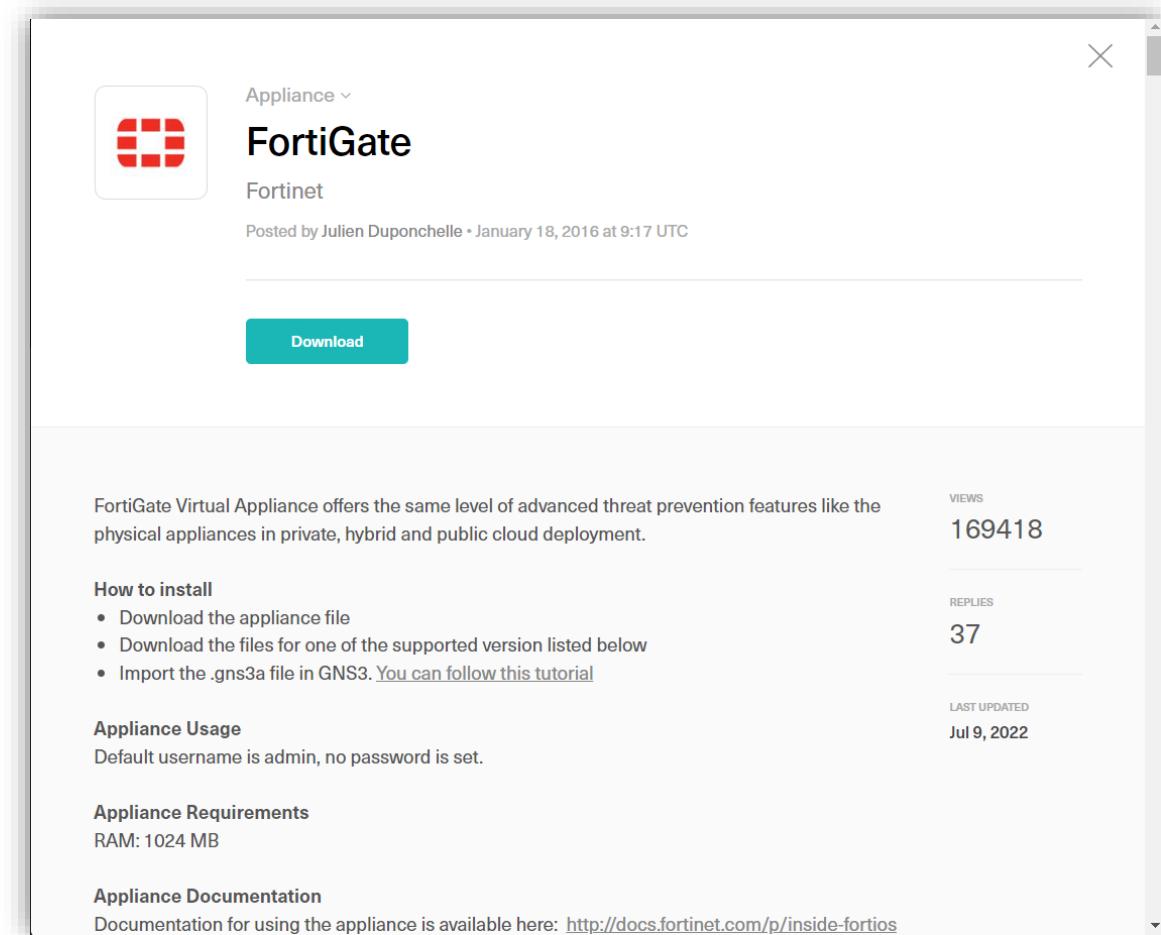


Ilustración 180: Descarga FortiGate.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Como buena práctica, te recomendamos que almacenes el archivo descargado en la carpeta de las prácticas de esta unidad.
- Para instalar selecciona «*File > Import new appliance*»

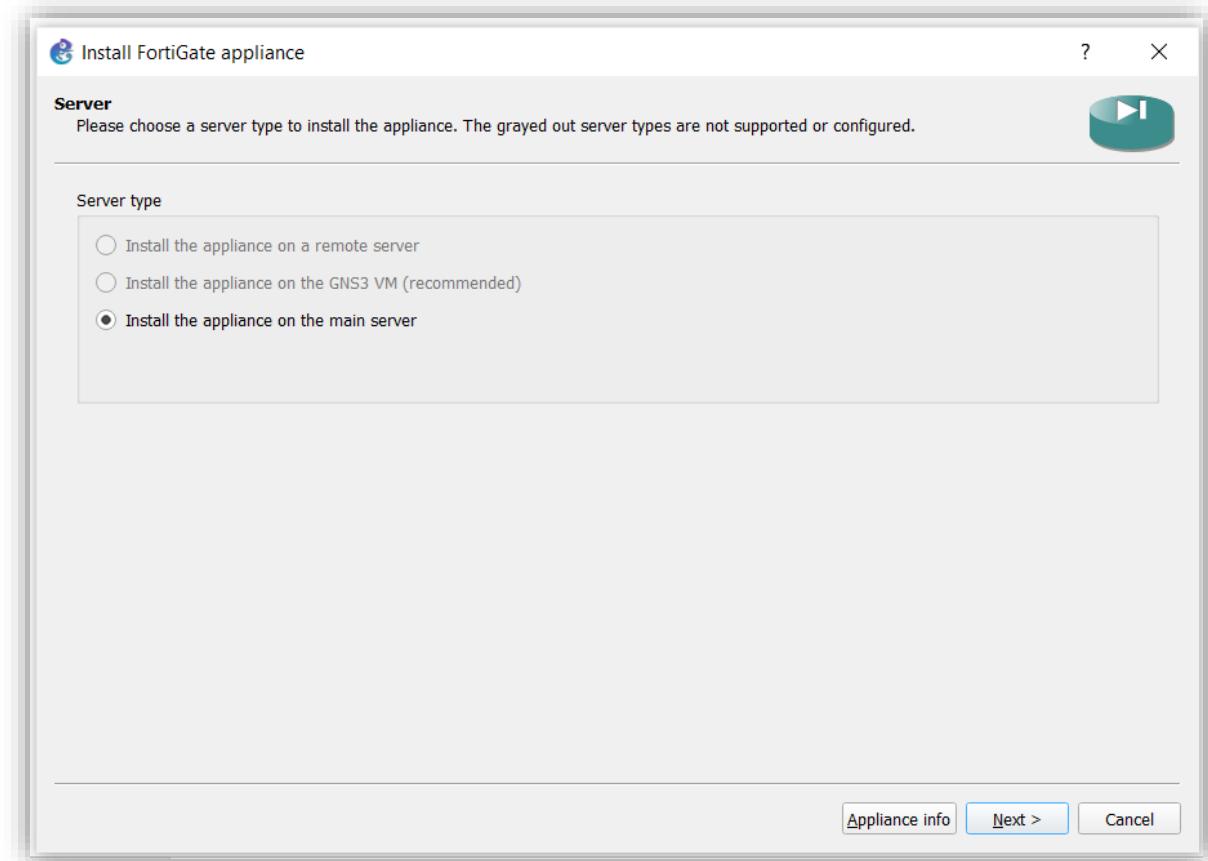


Ilustración 181: «Instalar el dispositivo en el servidor principal».

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

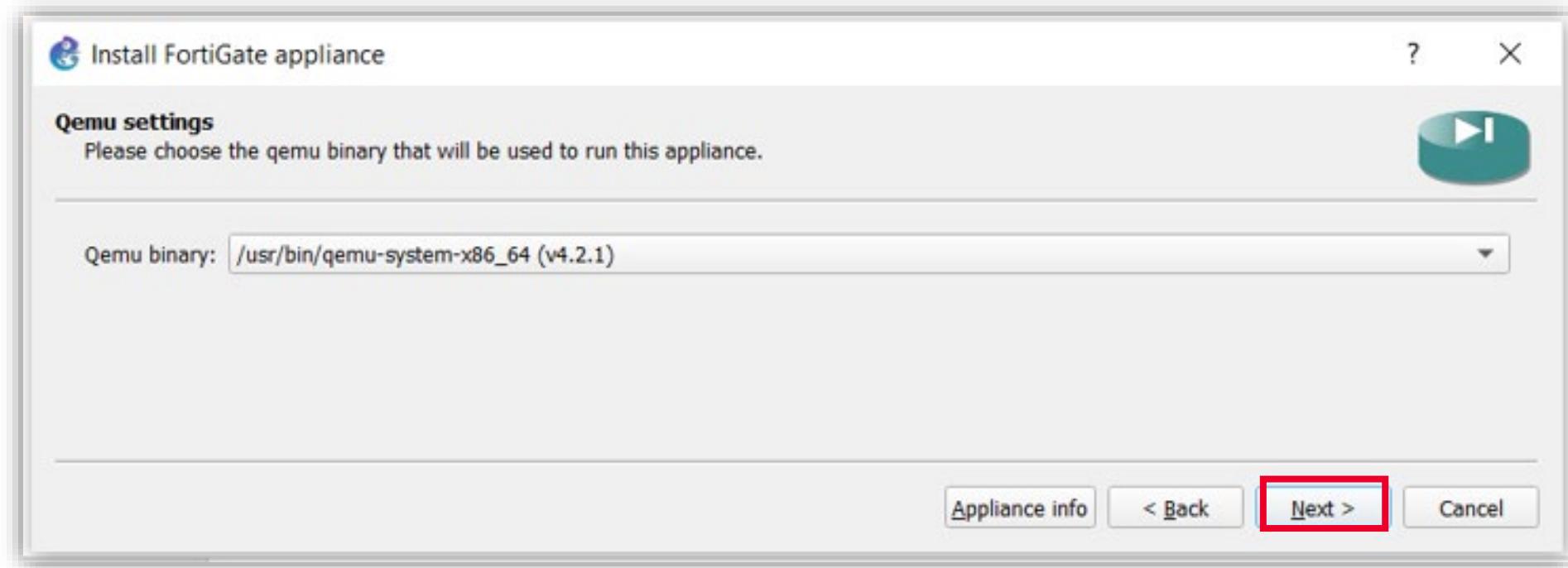


Ilustración 182: Clic en «next».

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Vamos a instalar una versión de «FortiGate» que no se encuentra dentro de las opciones por defecto, por lo que crearemos una nueva versión.
- Para ello, selecciona la versión 6.4.5 y haz clic en «*Create a new versión*».

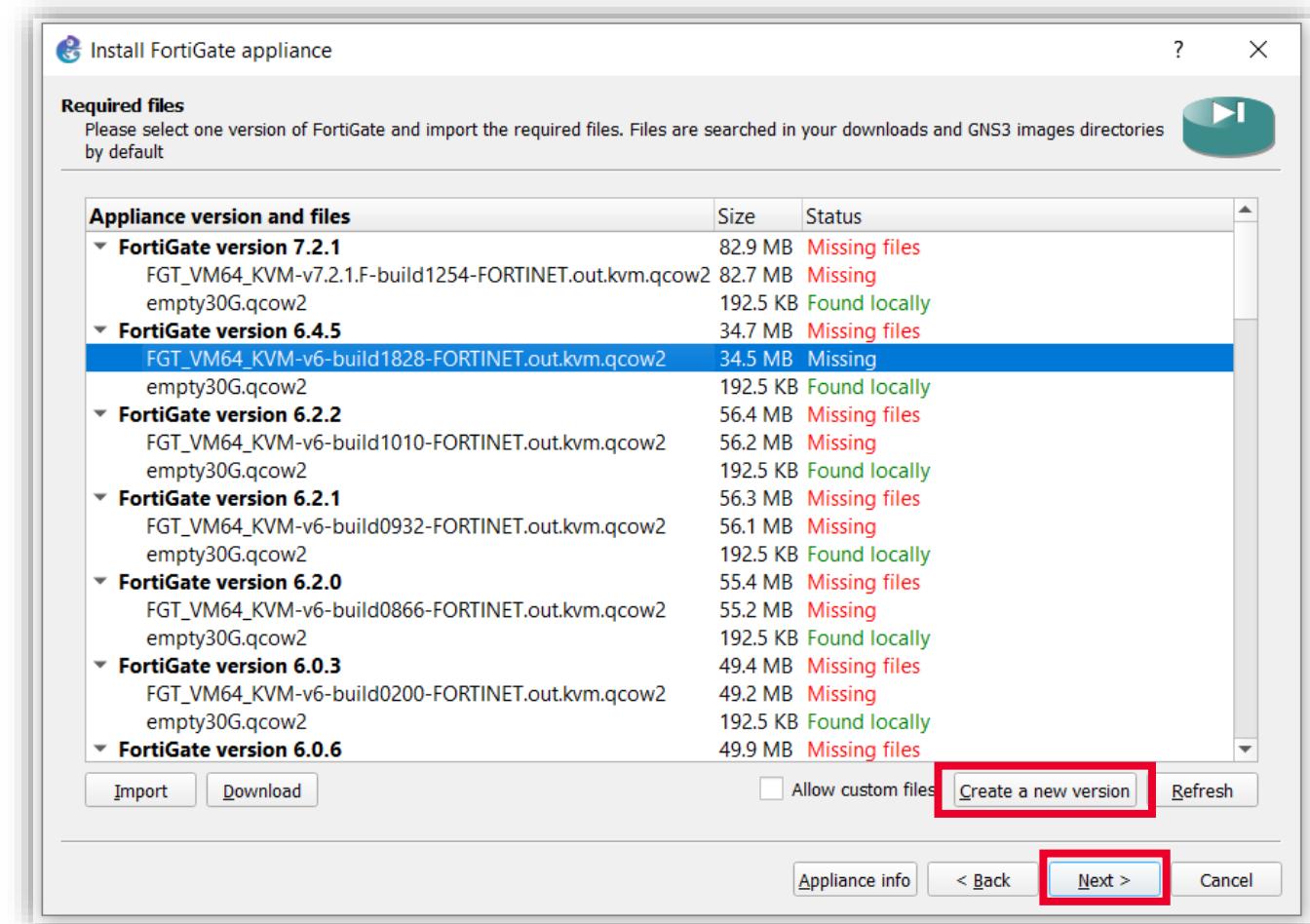


Ilustración 183: Selecciona la versión 6.4.5 y haz clic en «*Create a new versión*».

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Aparecerá un menú, en el cual debes cambiar el nombre del archivo que ya existe por el mismo nombre del archivo que nosotros te proporcionamos: «FGT_VM64_KVM-v6-build1579-FORTINET.out.kvm».

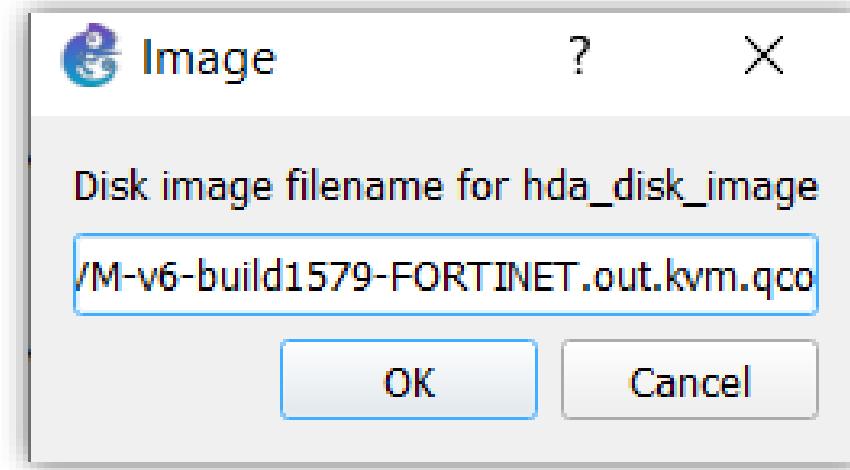


Ilustración 184: Añade «FGT_VM64_KVM-v6-build1579-FORTINET.out.kvm» en la ventana emergente.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Una vez realizados los pasos aparecerá la nueva versión disponible para importar los archivos necesarios.

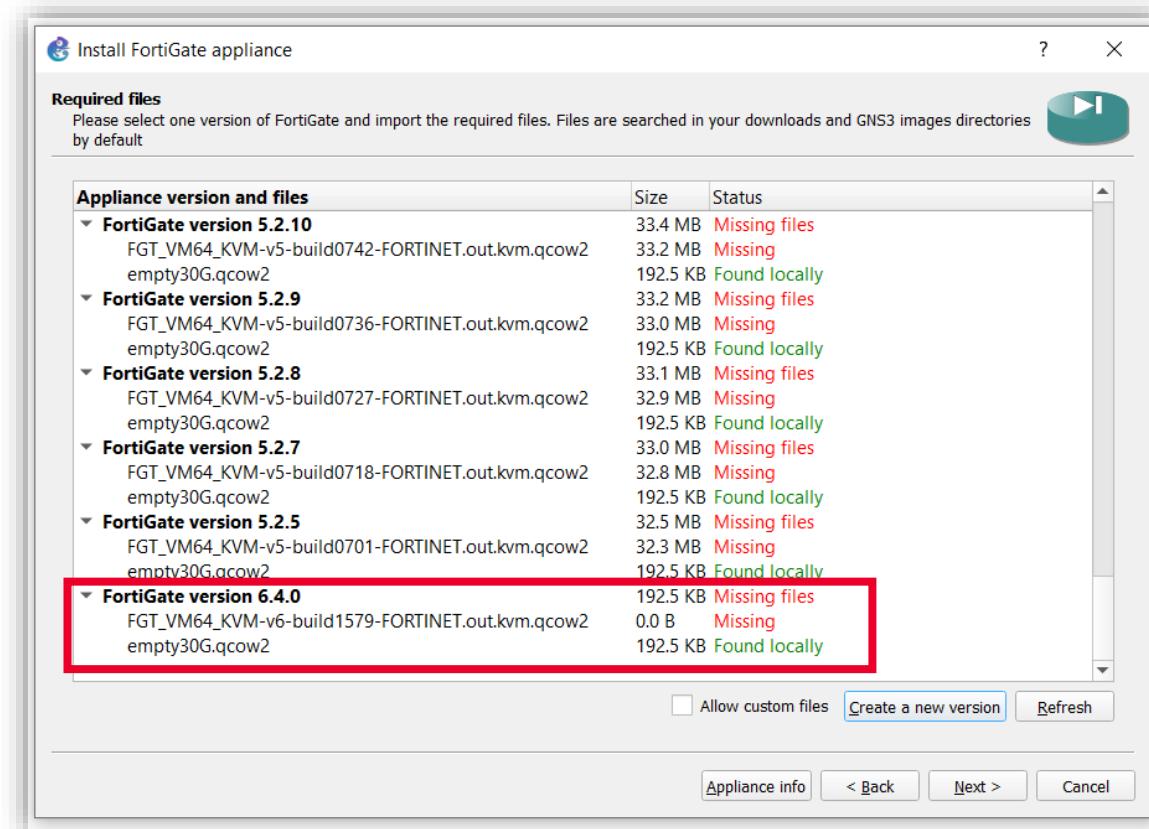


Ilustración 185: Nueva versión disponible para importar los archivos necesarios.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Selecciona el «FGT_VM64_KVM-v6-build1579-FORTINET.out.kvm» y haz clic en importar para seleccionar el archivo con el mismo nombre.
Haz lo mismo con el archivo «empty30G.qcow2».

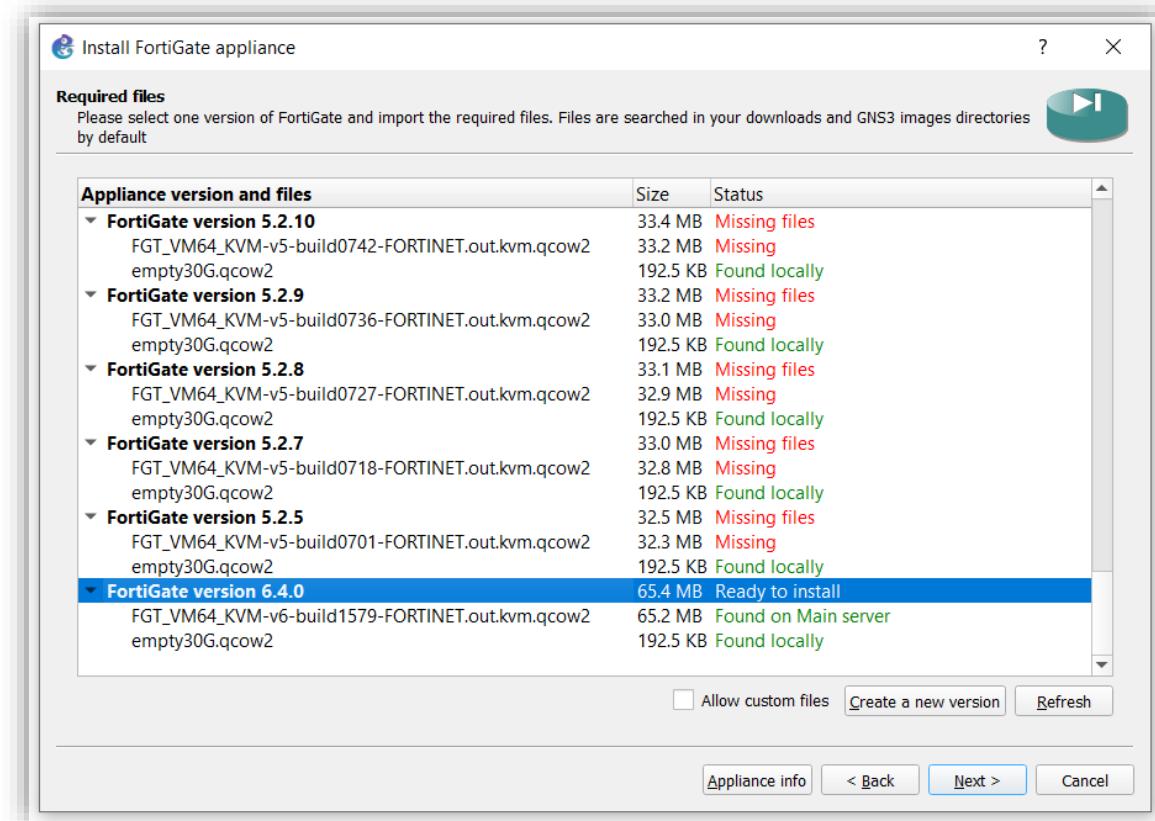


Ilustración 186: Importa el archivo «FGT_VM64_KVM-v6-build1579-FORTINET.out.kvm».

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Una vez estén importados te aparecerá el mensaje «*Ready to install*», pulsa «*Next*» y continúa con el proceso de instalación.

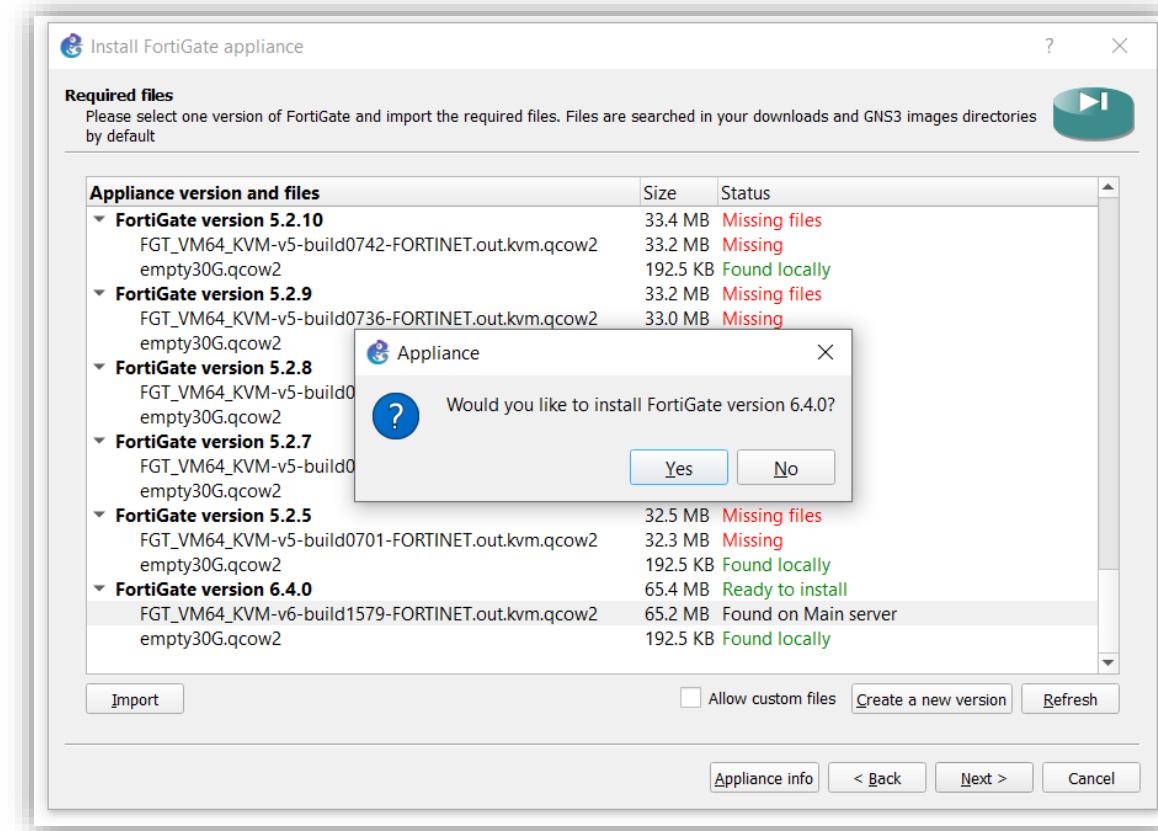


Ilustración 187: Aviso de confirmación para instalar FortiGate.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Como puedes observar nos indica el *username* para entrar en la gestión del *Firewall*.

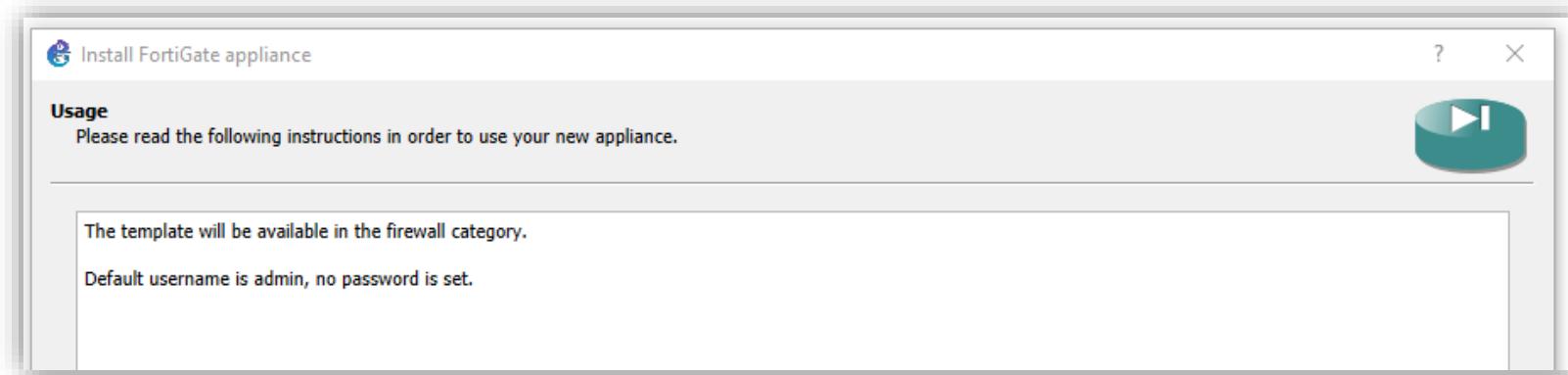


Ilustración 188: *Username* para entrar en la gestión del *Firewall*.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Para poder configurar, utilizar y gestionar el *Firewall* de Fortinet necesitarás una terminal Web. Por esta razón vamos a utilizar la máquina Ubuntu que instalaste al principio de estas prácticas.
- Como hemos visto anteriormente, arrastra los dispositivos a la pantalla y procede a la conexión entre ellos, como has visto en ejercicios anteriores. Para este ejercicio vamos a emplear la siguiente configuración, diseñada de esta forma únicamente para mostrar distintos elementos de la red.

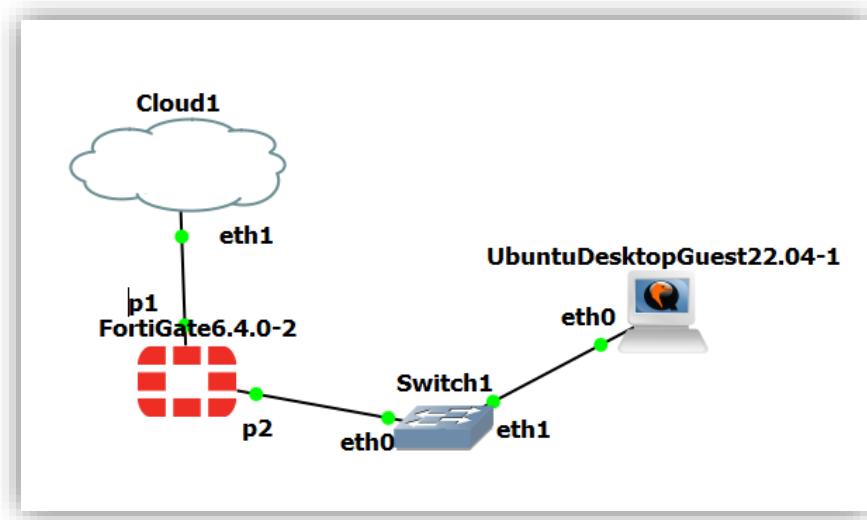
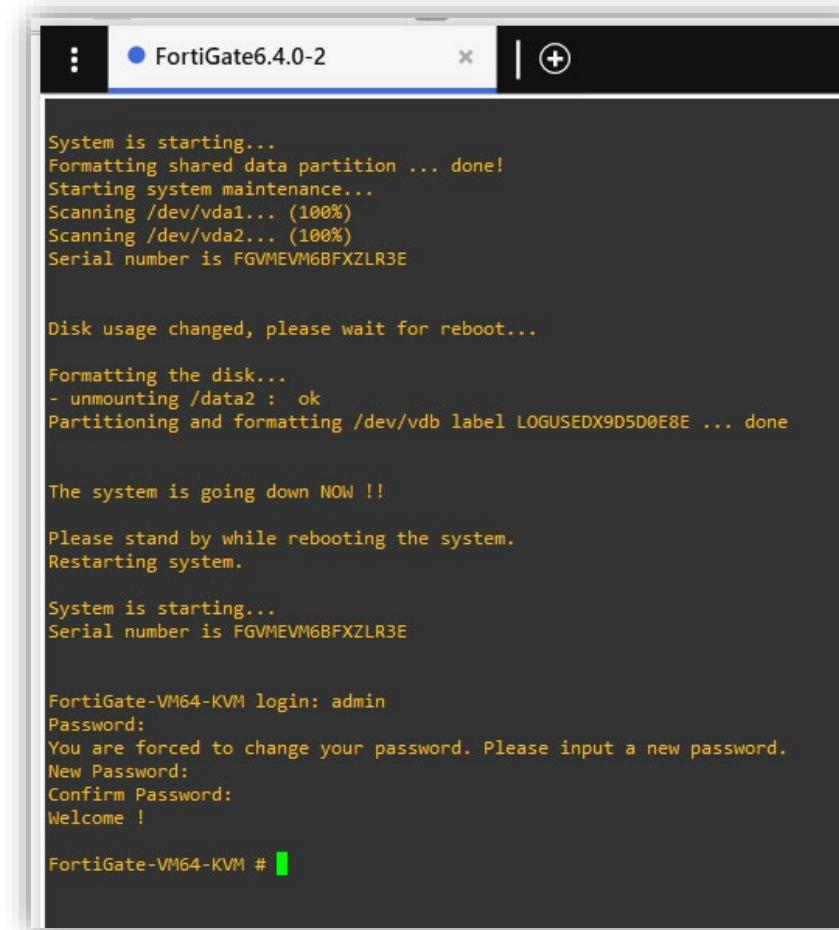


Ilustración 189: Conexiones realizadas para este ejemplo.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Cuando todo esté conectado, enciende todos los dispositivos.
- El primer paso será configurar el *Firewall* desde su consola para poder acceder a su entorno gráfico (GUI). Haz clic derecho sobre el cortafuegos FortiGate y pulsa «*console*».
- Primero te pedirá el *log-in*: como has visto antes, este será «*admin*» y sin contraseña.
- Te pedirá que cambies la contraseña, introduce una nueva que tú deseas y pulsa «*enter*».



The screenshot shows a terminal window with the title bar 'FortiGate6.4.0-2'. The window displays the following text:

```
System is starting...
Formatting shared data partition ... done!
Starting system maintenance...
Scanning /dev/vda1... (100%)
Scanning /dev/vda2... (100%)
Serial number is FGVMEVM6BFXZLR3E

Disk usage changed, please wait for reboot...

Formatting the disk...
- unmounting /data2 : ok
Partitioning and formatting /dev/vdb label LOGUSEDX9D5D0E8E ... done

The system is going down NOW !!

Please stand by while rebooting the system.
Restarting system.

System is starting...
Serial number is FGVMEVM6BFXZLR3E

FortiGate-VM64-KVM login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome !

FortiGate-VM64-KVM #
```

Ilustración 190: Configurar el *Firewall*: meter el *log in*.



PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Ejecuta los siguientes comandos:
 - «**config system interface**»: entra en el modo de configuración de interfaces.
 - «**edit port2**»: elige la interfaz a modificar.
 - «**set mode static**»: se configuran las IPs en modo estático.
 - «**set ip 10.0.0.1 255.255.255.0**»: configura la IP que quieras manualmente.
 - «**set role lan**»: pone nombre al rol de este puerto.
 - «**set allowaccess ping http https ssh telnet**»: configura los servicios que vamos a permitir en este puerto.
 - «**end**»: para salir del modo configuración.



PRÁCTICA: TOPOLOGÍA DE RED CON FW

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port2
FortiGate-VM64-KVM (port2) # set mode static
FortiGate-VM64-KVM (port2) # set ip 10.0.0.1 255.255.255.0
FortiGate-VM64-KVM (port2) # set role lan
FortiGate-VM64-KVM (port2) # set allowaccess ping http https ssh telnet fgfm
FortiGate-VM64-KVM (port2) # end
FortiGate-VM64-KVM #
```

Ilustración 191: Configurar el *Firewall*: ejecutar los comandos vistos.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Si quieres comprobar que la configuración ha sido correctamente modificada puedes utilizar el comando «**show system interface**» o «**show sys int port2**» para ver solo la configuración de este puerto concreto.

```
FortiGate-VM64-KVM # show sys int port2
config system interface
    edit "port2"
        set vdom "root"
        set ip 10.0.0.1 255.255.255.0
        set allowaccess ping https ssh http telnet fgfm
        set type physical
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 2
    next
end

FortiGate-VM64-KVM #
```

Ilustración 192: Configurar el *Firewall*: usa el comando «**show system interface**» para comprobar que la configuración ha sido correctamente modificada.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Ahora tendrás que configurar el «puerto1» el cual está conectado a la «Cloud», por lo tanto, será la red WAN.
- Ejecuta los siguientes comandos:
 - «**config system interface**»: entra en el modo de configuración de interfaces.
 - «**edit port1**»: elige la interfaz a modificar.
 - «**set mode dhcp**»: se asignará el servicio «*dhcp*» para este puerto.
 - «**set role wan**»: pone nombre al rol de este puerto.
 - «**end**»: para salir del modo configuración.

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port1
FortiGate-VM64-KVM (port1) # set mode dhcp
FortiGate-VM64-KVM (port1) # set role wan
FortiGate-VM64-KVM (port1) # end
```

Ilustración 193: Ejecuta los comandos vistos para configurar el «puerto1».

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Ahora tendrás que asignarle a la máquina Ubuntu una IP dentro del mismo rango que asignaste al *Firewall* para poder acceder a la GUI de FortiGate.
 - Como viste en ejercicios anteriores, entra en el menú «*Wired Connected > Wired Settings*».
 - Dentro de este menú configura de manera manual la IP y añade una que esté dentro del rango que asignaste antes en la configuración del «puerto2».

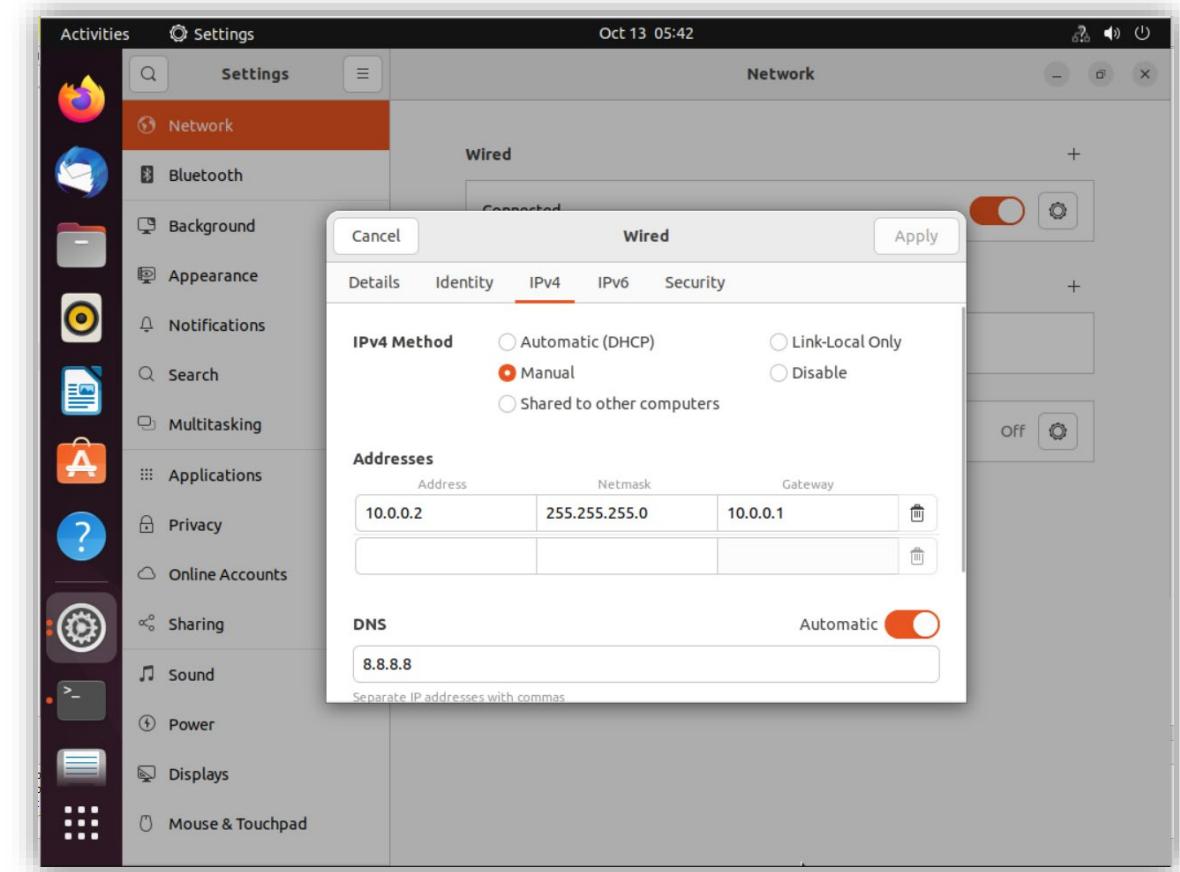


Ilustración 194: Configura la IP manualmente y añade una.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Cuando hayas terminado ya podrás abrir el navegador y escribir la IP que configuraste en el «puerto2», de esta forma abrirá el entorno gráfico de FortiGate donde podrás logarte.

IMPORTANTE: No intentes acceder a la GUI mediante HTTPS, ya que como es un producto sin licencia no se puede acceder a través de este protocolo.

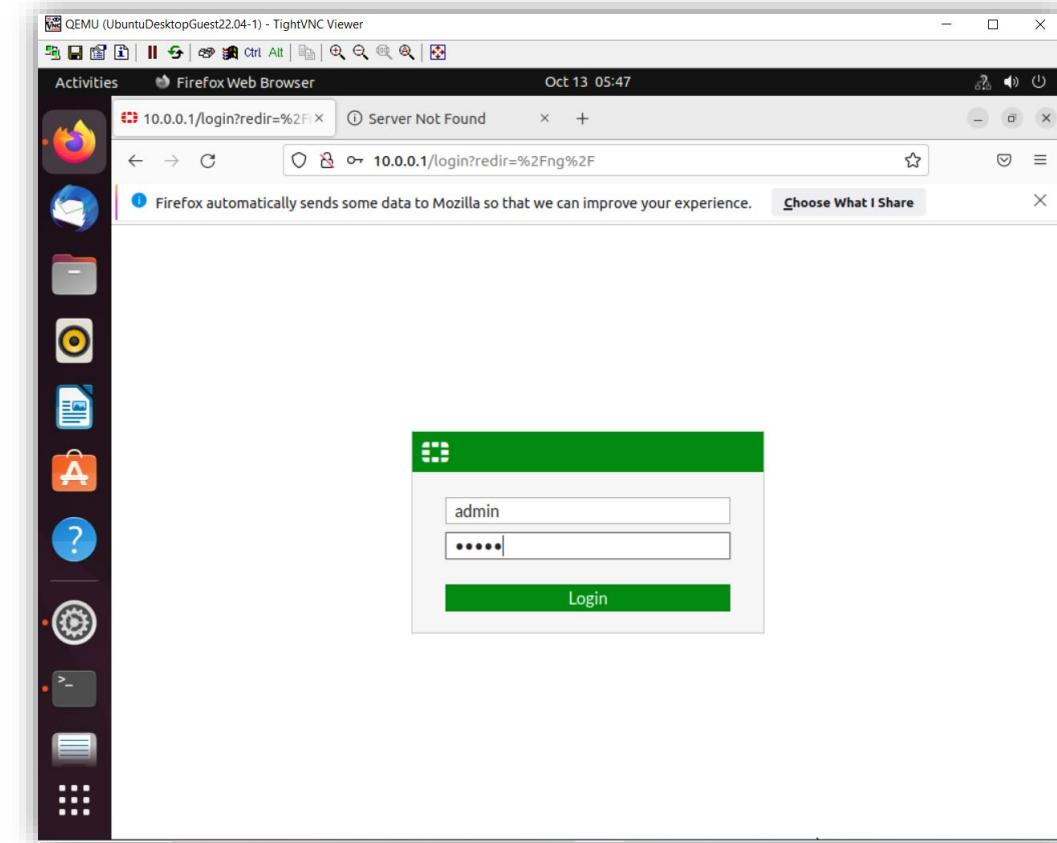


Ilustración 195: Accede al entorno gráfico de FortiGate.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Para acceder a la GUI hemos configurado la dirección IP de la máquina Ubuntu de manera estática, pero esta no es la forma correcta de administrar la dirección IP en el lado de la LAN. La configuración correcta sería usar un servidor DHCP o habilitar el servicio DHCP en el puerto LAN que es lo que faremos.
- Para ello, selecciona el menú «Network > Interfaces» y selecciona «port2» que es el que asignamos a la LAN.

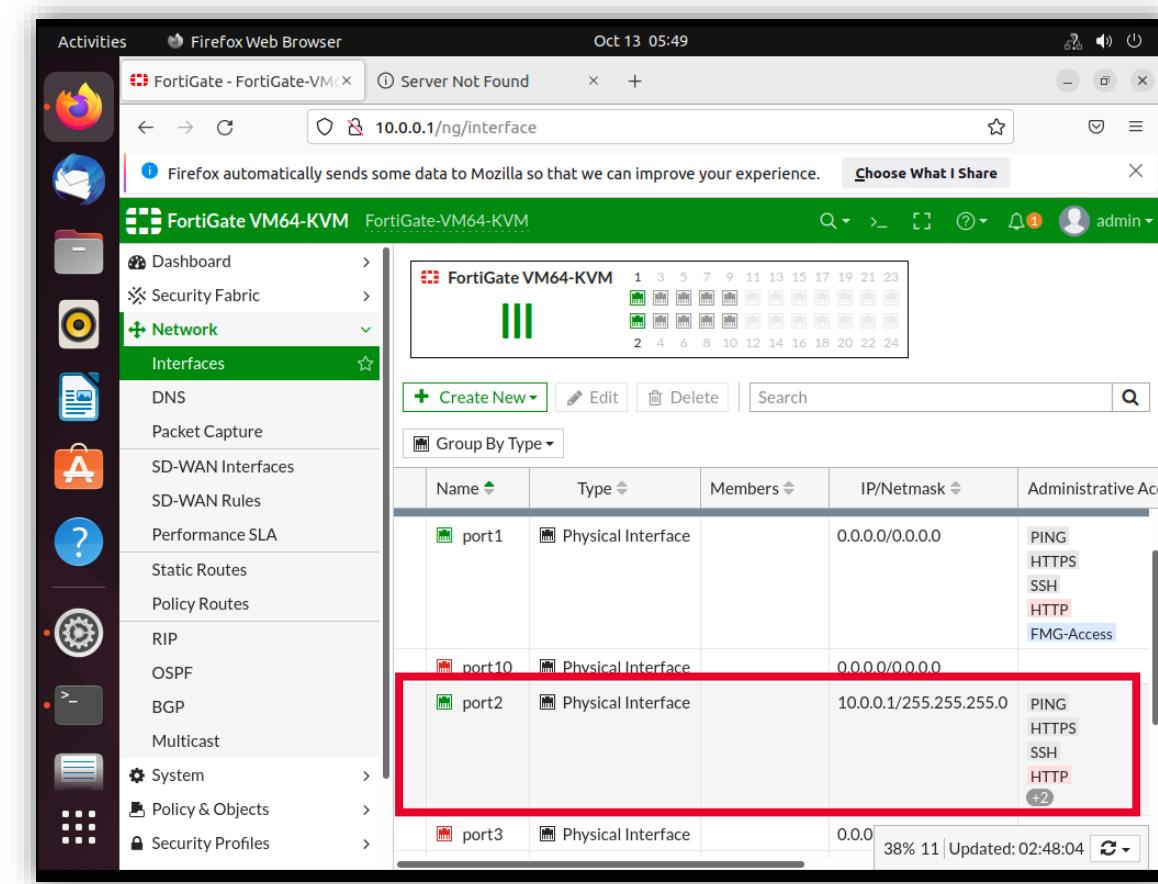


Ilustración 196: Habilitar el servicio DHCP en el puerto LAN.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Cambia el «Alias» para identificar el puerto (LAN) que utilizaremos.

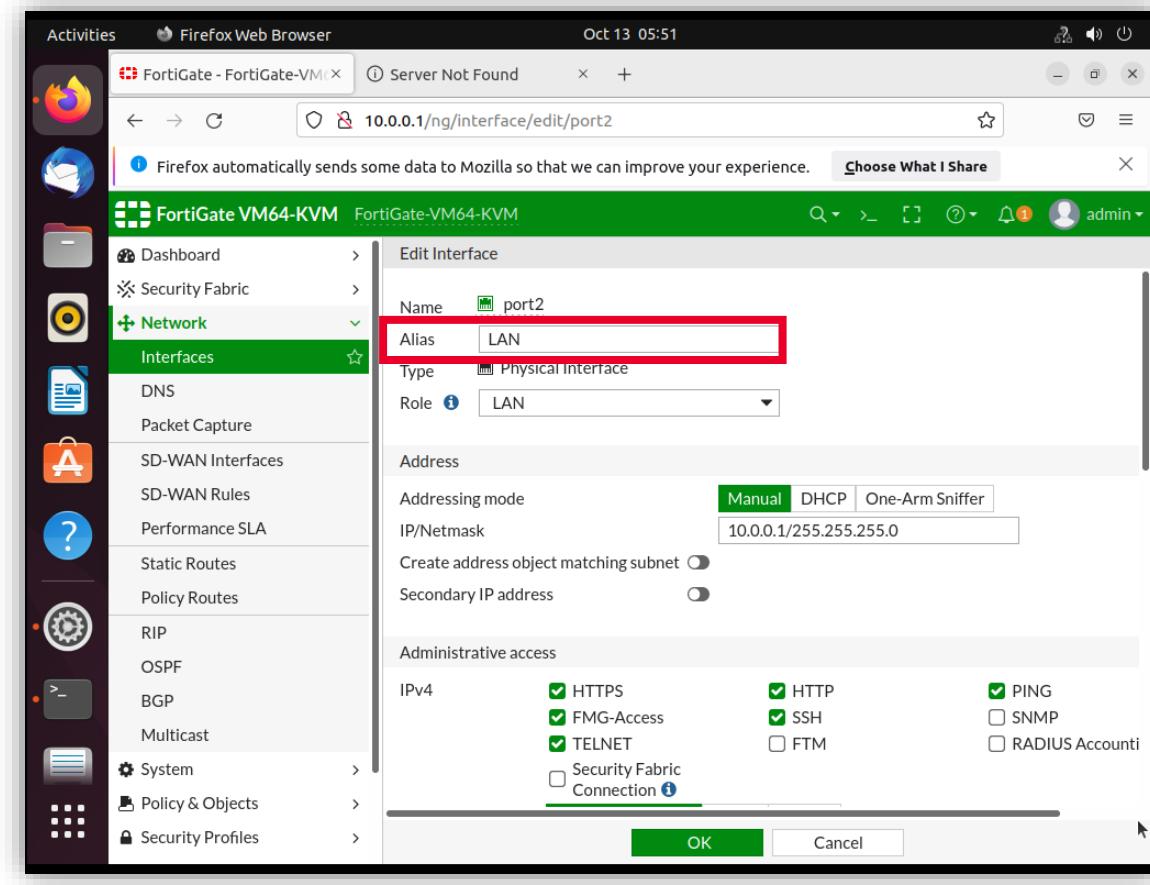


Ilustración 197: Cambiar el «Alias» del puerto LAN a utilizar.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Marca la casilla «DHCP» y aparecerá automáticamente un rango de IPs que utilizará para asignarlas automáticamente a los equipos que se conecten.

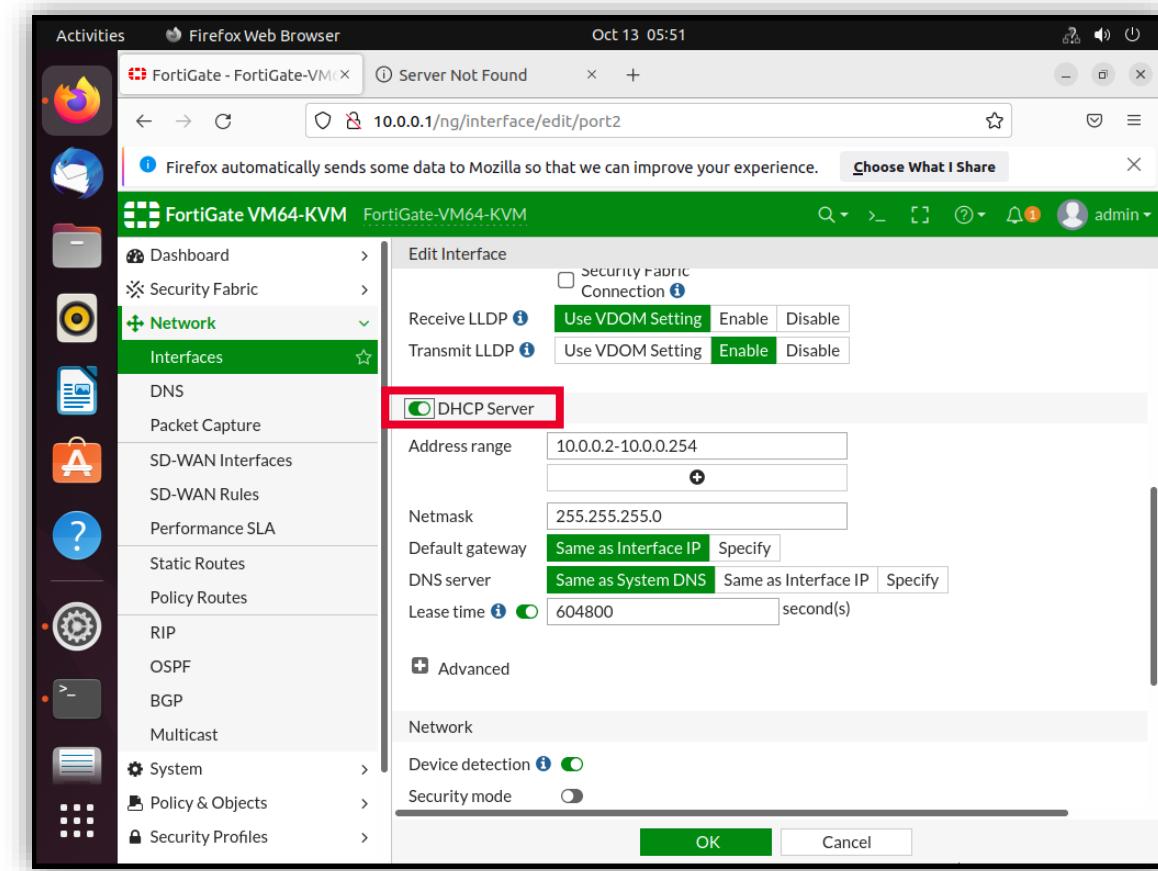


Ilustración 198: Marca la casilla «DHCP».

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Una vez esté configurado haz clic en «OK» y guarda la configuración. Deberá quedar así:

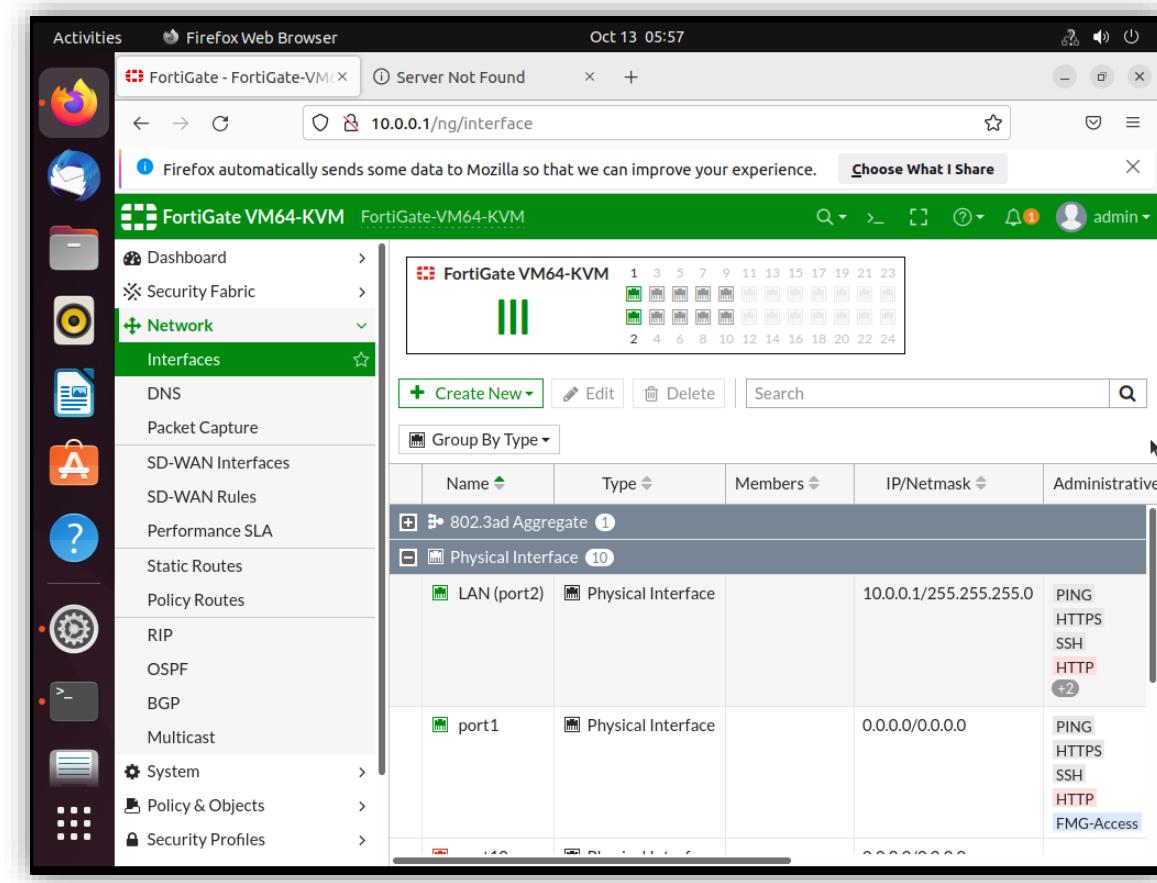


Ilustración 199: Habilitación del servicio DHCP en el puerto LAN finalizado.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Verificamos la configuración DHCP. Para esto cambia la configuración a automático para que sea el servidor de DHCP que hemos configurado en FortiGate el que asigne la IP.

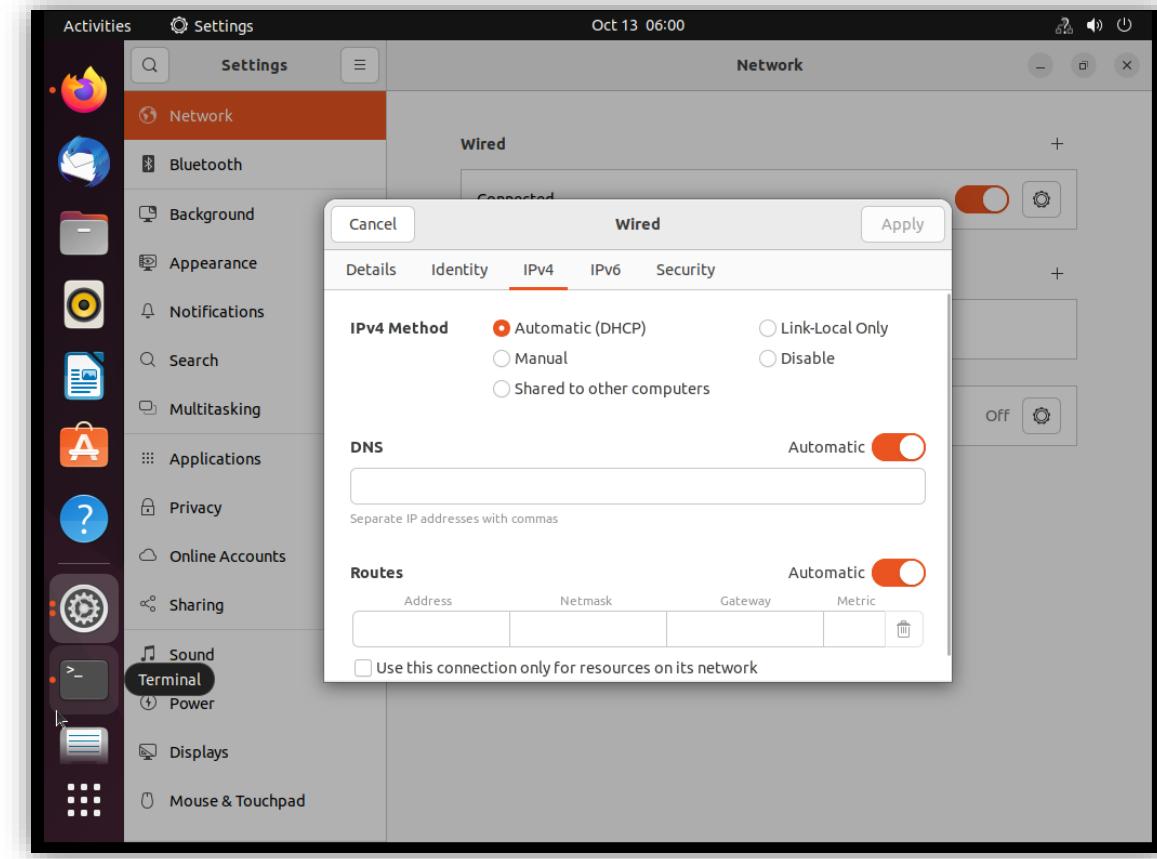


Ilustración 200: Cambia la configuración a automático.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Observa que automáticamente el servicio de DHCP de FortiGate asigna la IP 10.0.0.2.

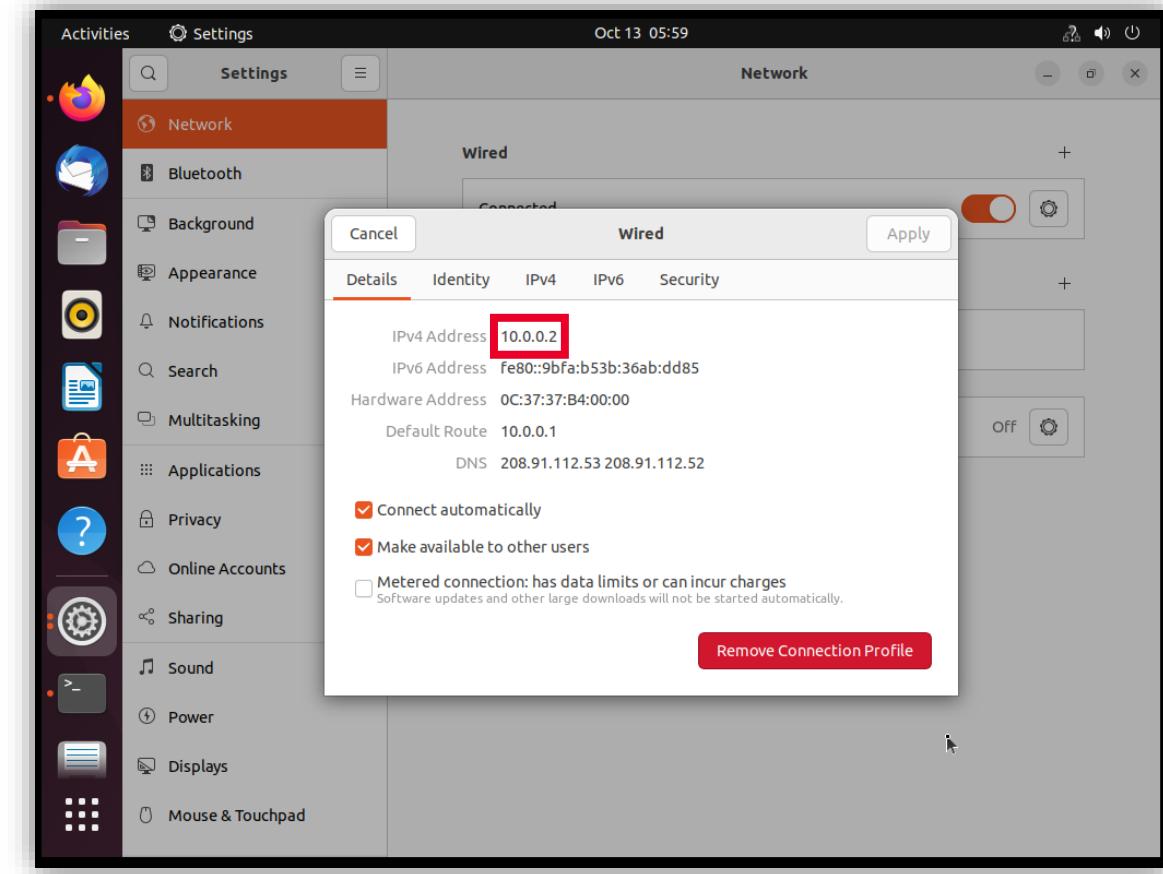


Ilustración 201: Asignación automática de la ip 10.0.0.2.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Ahora vamos a conectar FortiGate a Internet.

Hemos configurado el lado LAN del *firewall* de forma que cuando agreguemos más equipos FortiGate actuará como servidor DHCP y será el encargado de entregar direcciones IP. Pero, estos equipos no tienen salida a Internet porque el *firewall* todavía no está conectado a Internet.
- Para ello, debes comprobar primero qué interfaz de la *Cloud* es la correcta ya que como vimos en ejercicios anteriores cambiará dependiendo del PC. Añade las interfaces especiales como vimos en ejercicios anteriores.

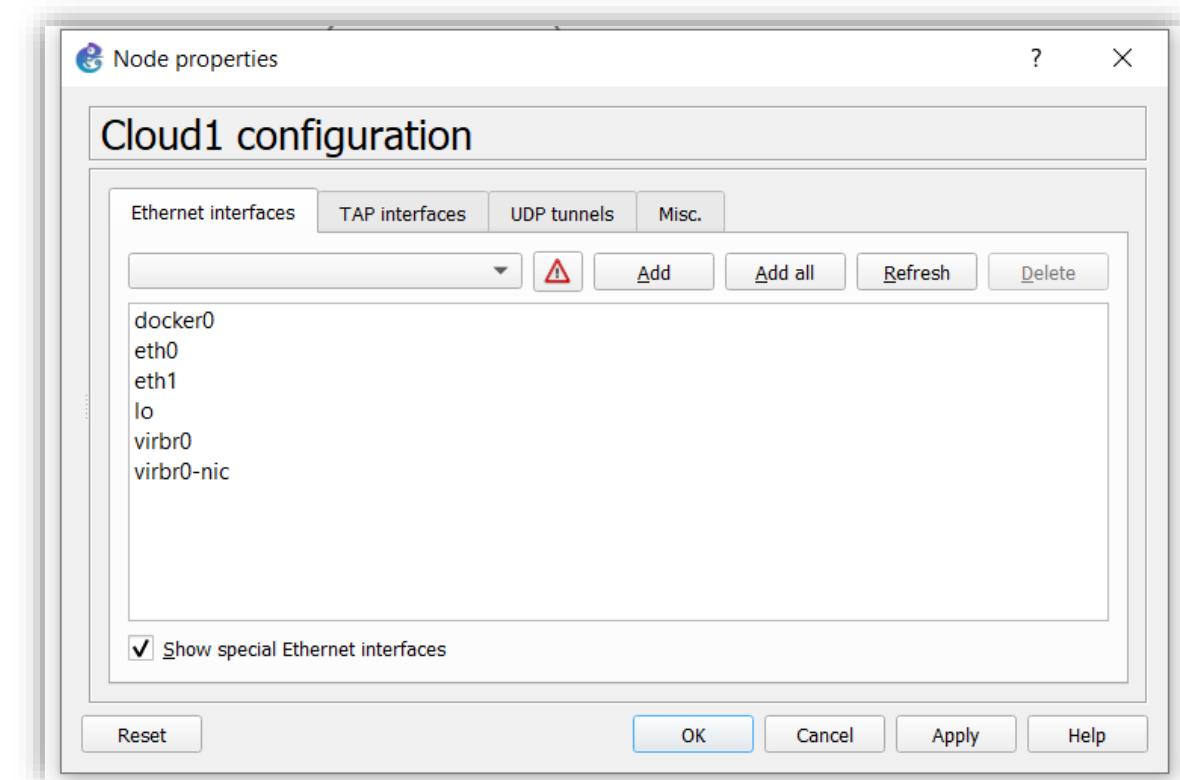


Ilustración 202: Añade las interfaces especiales.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- En nuestro caso la interfaz que nos proporciona IP es la «*eth1*».
- Para comprobarlo ejecuta el comando «**diagnose ip address list**» en FortiGate. Si es la interfaz correcta aparecerá una IP para el puerto 1 o el puerto seleccionado para la red WAN.

```
FortiGate-VM64-KVM # diagnose ip address list
IP=192.168.122.11->192.168.122.11/255.255.255.0 index=3 devname=port1
IP=10.0.0.1->10.0.0.1/255.255.255.0 index=4 devname=port2
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=13 devname=root
IP=169.254.1.1->169.254.1.1/255.255.255.0 index=15 devname=fortilink
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=16 devname=vsys_ha
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=18 devname=vsys_fgfm
```

Ilustración 203: IP para el puerto 1.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Dado que adquirimos la dirección IP a través de DHCP, también estará configurada la puerta de enlace predeterminada que actuará como ruta predeterminada para el FW, por lo que, cuando hagamos «ping» a Internet (8.8.8.8) deberías obtener respuesta.

```
FortiGate-VM64-KVM # execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=128 time=29.6 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=9.7 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 9.7/19.6/29.6 ms
```

Ilustración 204: Obtención de respuesta cuando hacemos «ping» a Internet.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Ahora que ya tenemos acceso a Internet desde FortiGate, debes configurar la política de seguridad en el FW y la configuración de la NAT para que el dispositivo salga a Internet utilizando el enlace del FW.
- Antes de crear la política deberás crear el «objeto» de la interfaz LAN. Para esto ve al menú «*Policy & Objects* > *Addresses* > *Create New*» y en el desplegable que aparecerá haz clic en «Address».

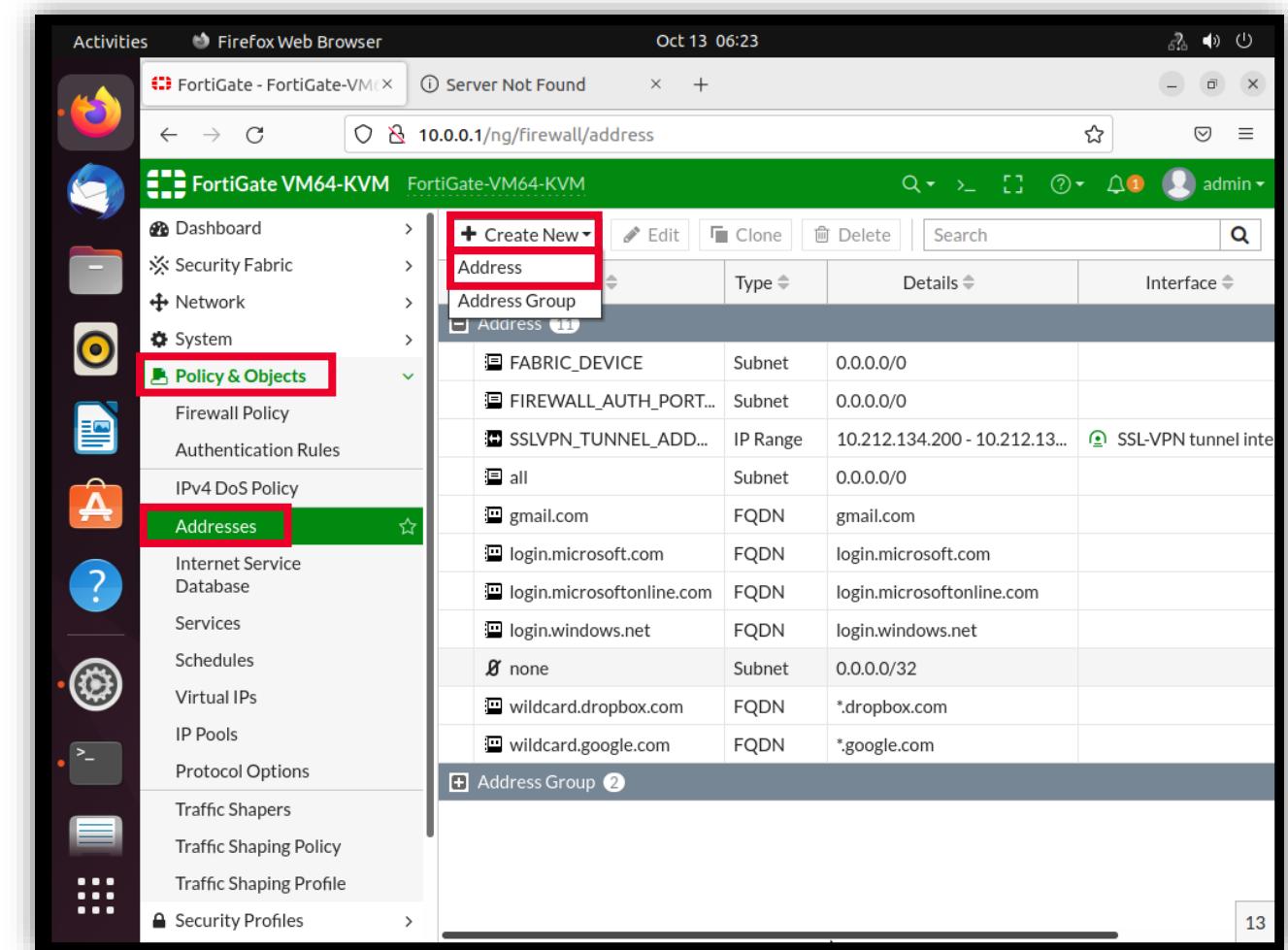


Ilustración 205: Menú «*Policy & Objects* > *Addresses* > *Create New*».



PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Cambia los siguientes campos:
 - **Name:** pon el nombre de la interfaz que estamos configurando en este caso «red LAN».
 - **IP/Netmask:** deberás poner la IP del mismo rango que configuramos anteriormente.
 - **Interface:** selecciona el puerto al que está conectado la red LAN. En nuestro caso el puerto dos que ya identificamos anteriormente.
 - **Comments:** para especificar lo que estamos configurando; en este caso es la subred de la LAN.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

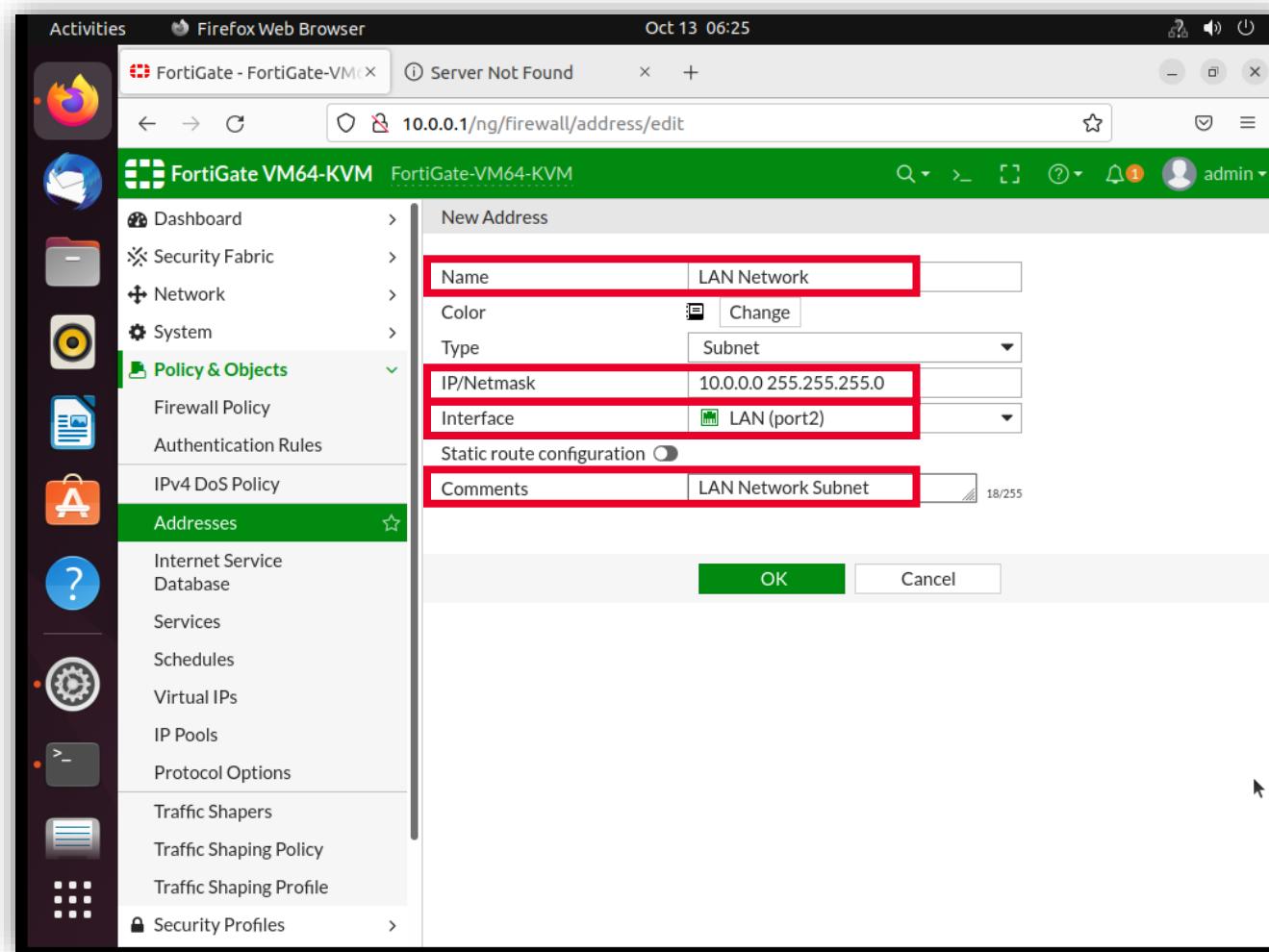


Ilustración 206: Modificación de los campos vistos.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Pulsa «OK» y deberá aparecer en el menú.

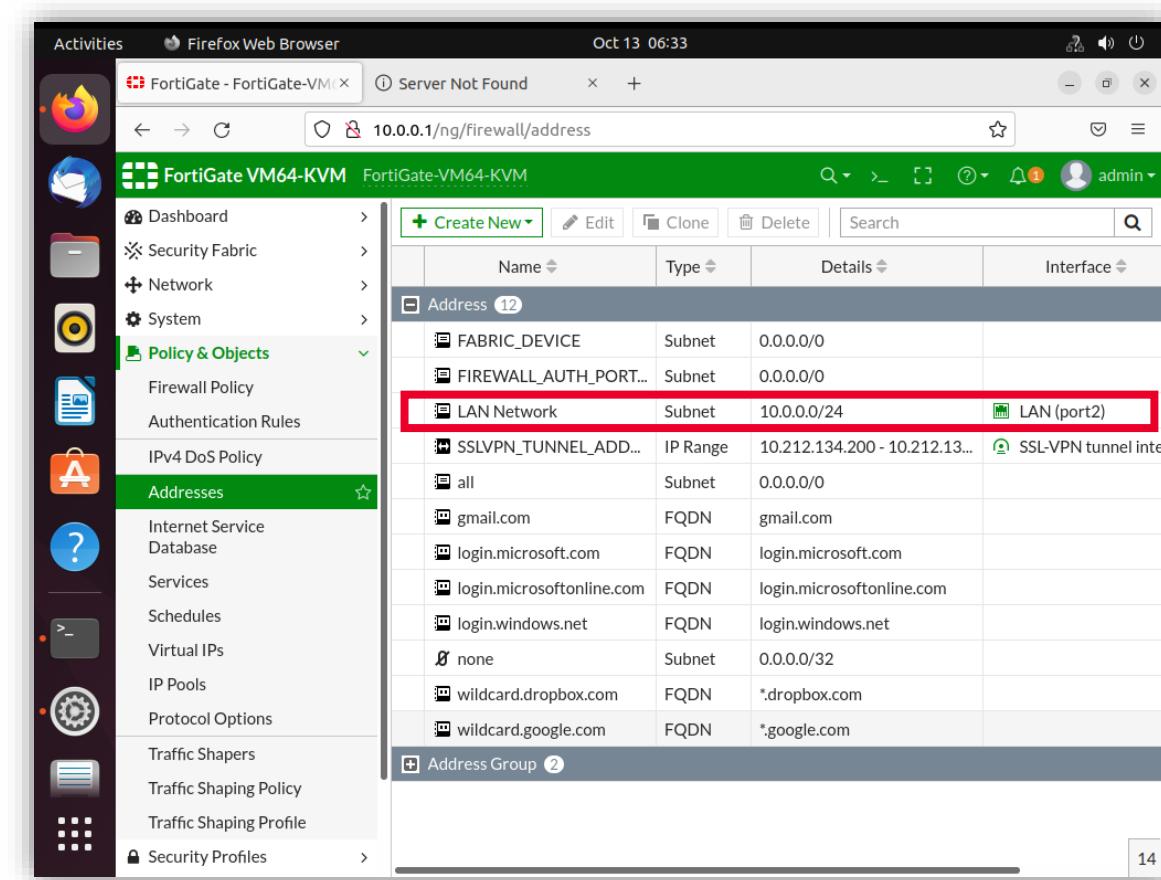


Ilustración 207: Menú para crear el «objeto» de la interfaz LAN.



PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Para identificar las interfaces antes de crear la política ve a «*Network > Interfaces*», selecciona el puerto 1 y denomínalo «WAN» para identificarlo rápidamente después.
- Una vez creado, podemos pasar a crear las políticas de seguridad para el acceso a Internet. Esta política de seguridad permitirá el tráfico de dentro hacia afuera, pero cuando el tráfico sale de la LAN sería una dirección IP privada y cuando sale la dirección IP debe traducirse a una dirección IP pública. Por eso es por lo que debemos configurar la NAT en la misma política de seguridad.
- Para ello vamos al menú de «*Policy & Objects > Firewall Policy > Create New*».

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

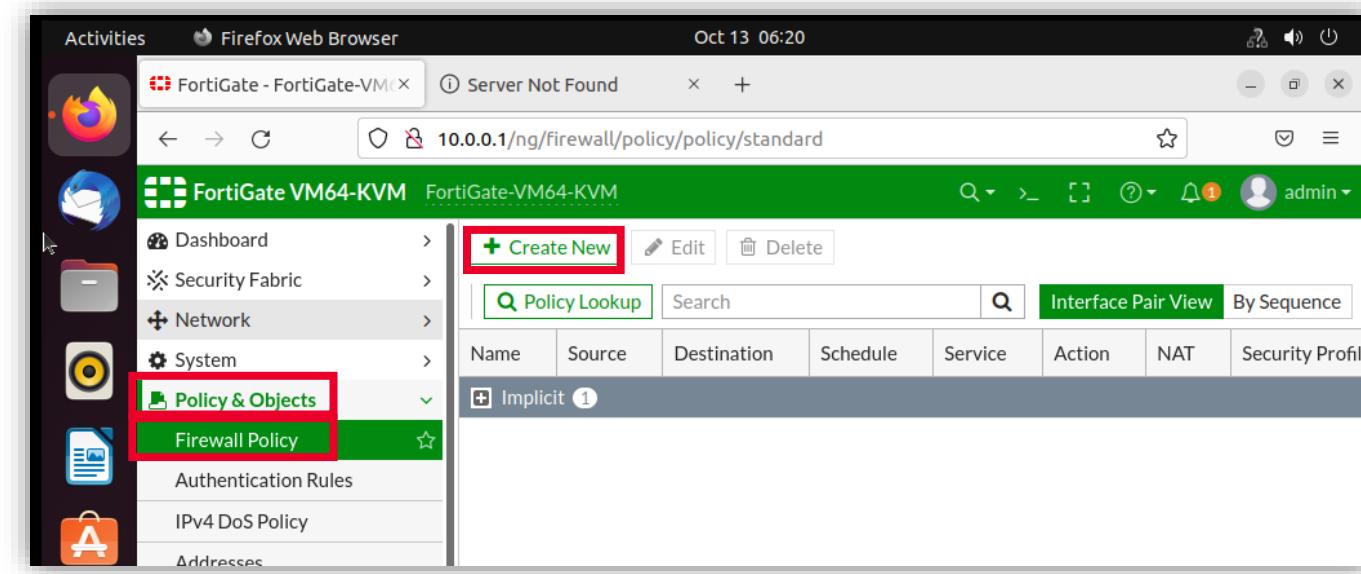


Ilustración 208: Abrimos nuevo proyecto.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Deberás llenar los siguientes campos
 - **Name:** nombre que denomine la política.
 - **Incoming interface:** desde dónde viene el tráfico.
 - **Outgoing interface:** hacia dónde va el tráfico.
 - **Source:** equipo desde el que viene el tráfico. En este caso pondremos todos para la simulación, pero una buena configuración debería tener sólo los dispositivos necesarios.
 - **Destination:** equipo hacia el que va el tráfico. En este caso pondremos todos para la simulación, pero una buena configuración debería tener sólo los dispositivos necesarios.
 - **Service:** elige y busca los servicios que permitiremos y que sean necesarios.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

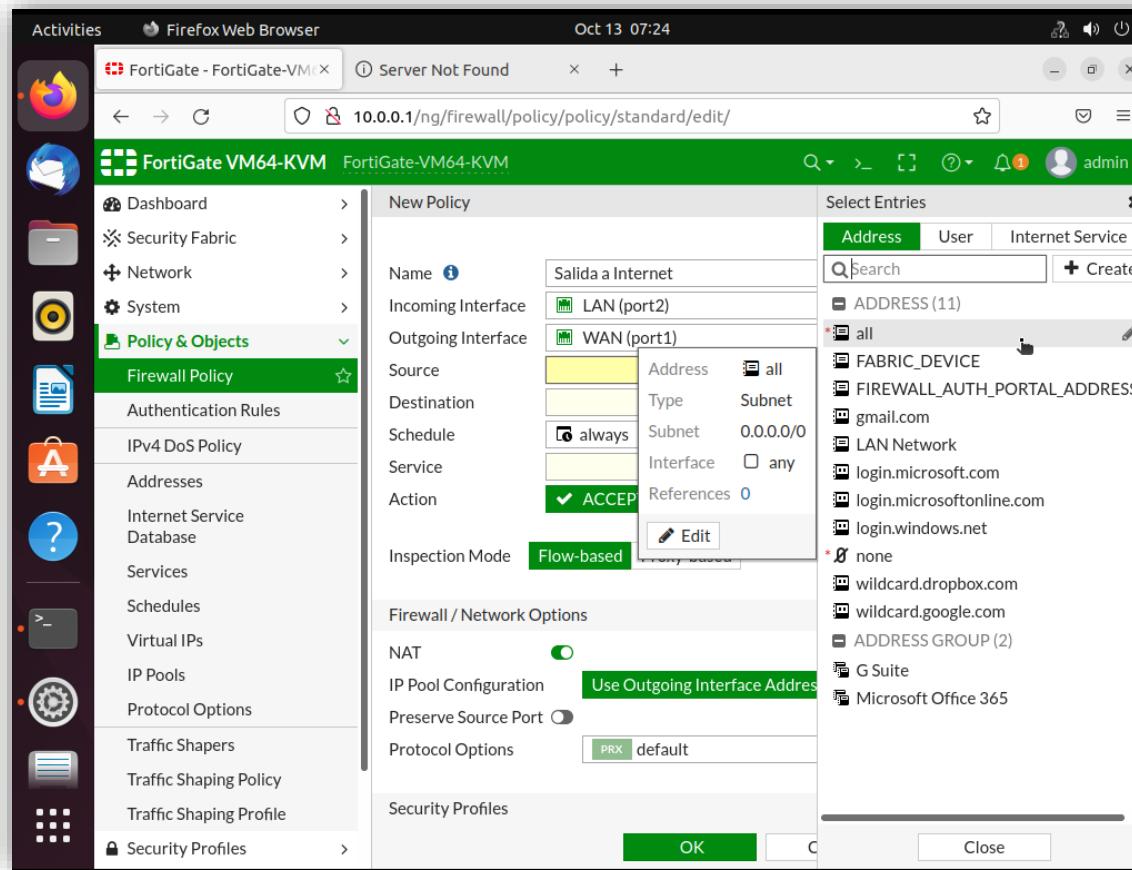


Ilustración 209: Configura los distintos campos (I).

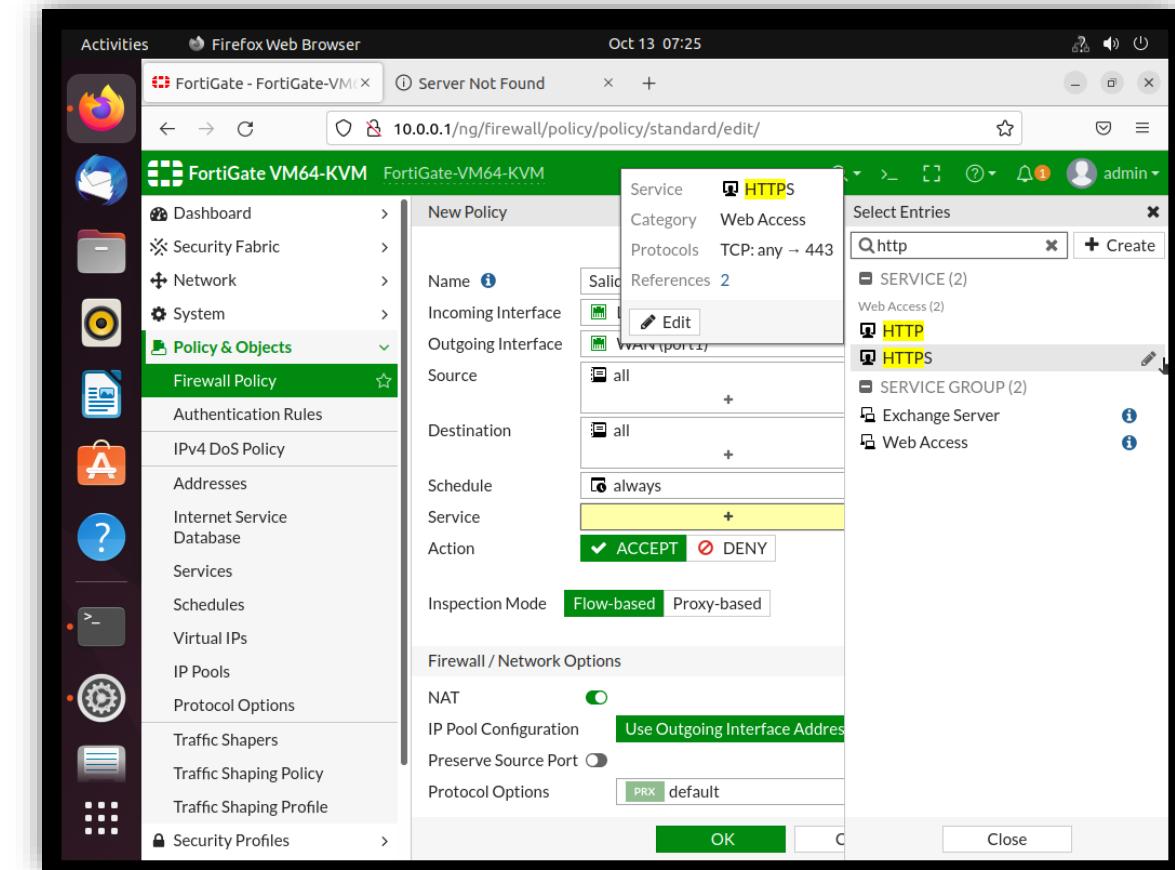


Ilustración 210: Configura los distintos campos (II).

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Así debería quedar la configuración final de la política.

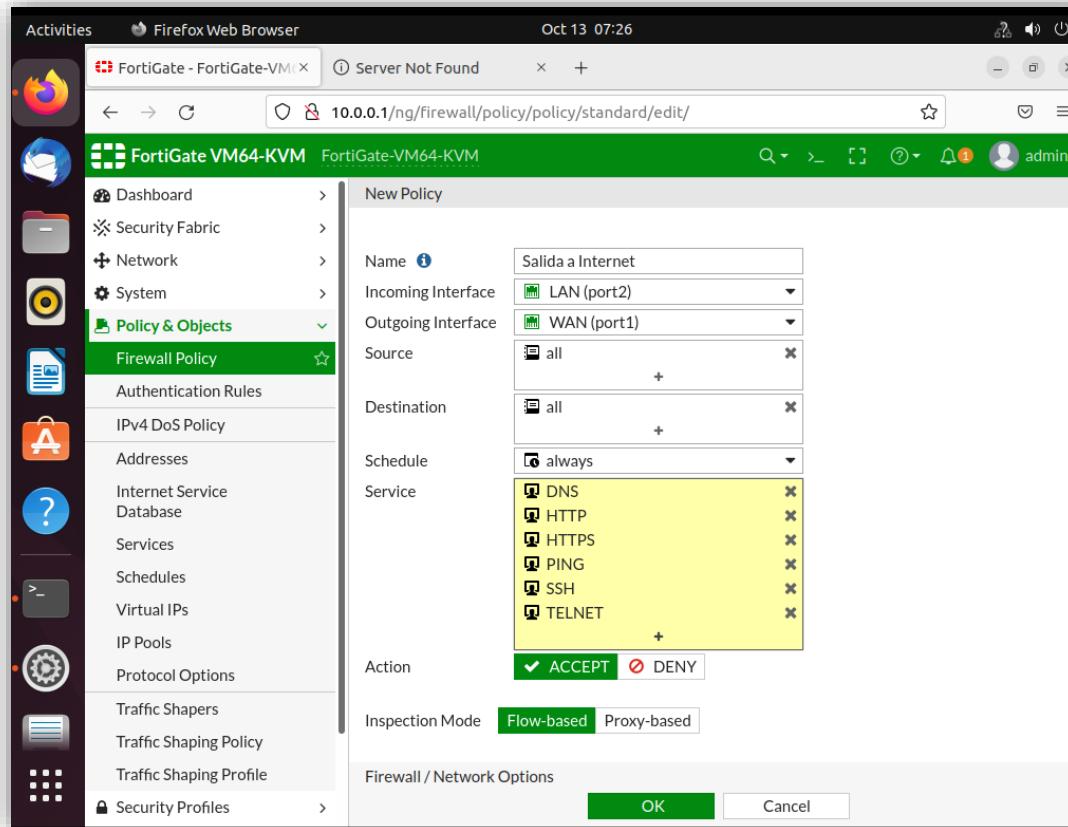


Ilustración 211: Configuración final de la política (I).

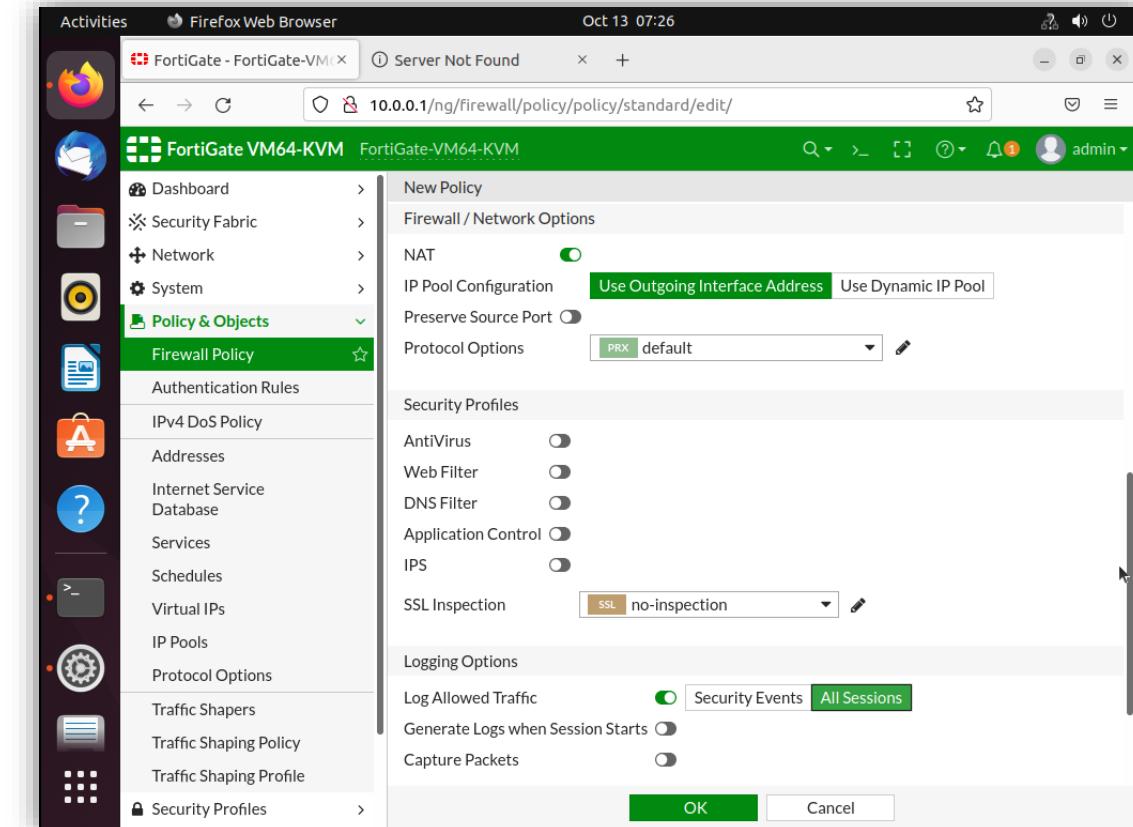


Ilustración 212: Configuración final de la política (II).

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Antes de aceptar y guardar la configuración comprueba que el «*ping*» al «8.8.8.8» no responde y después acepta la política y comprueba que obtienes respuesta.

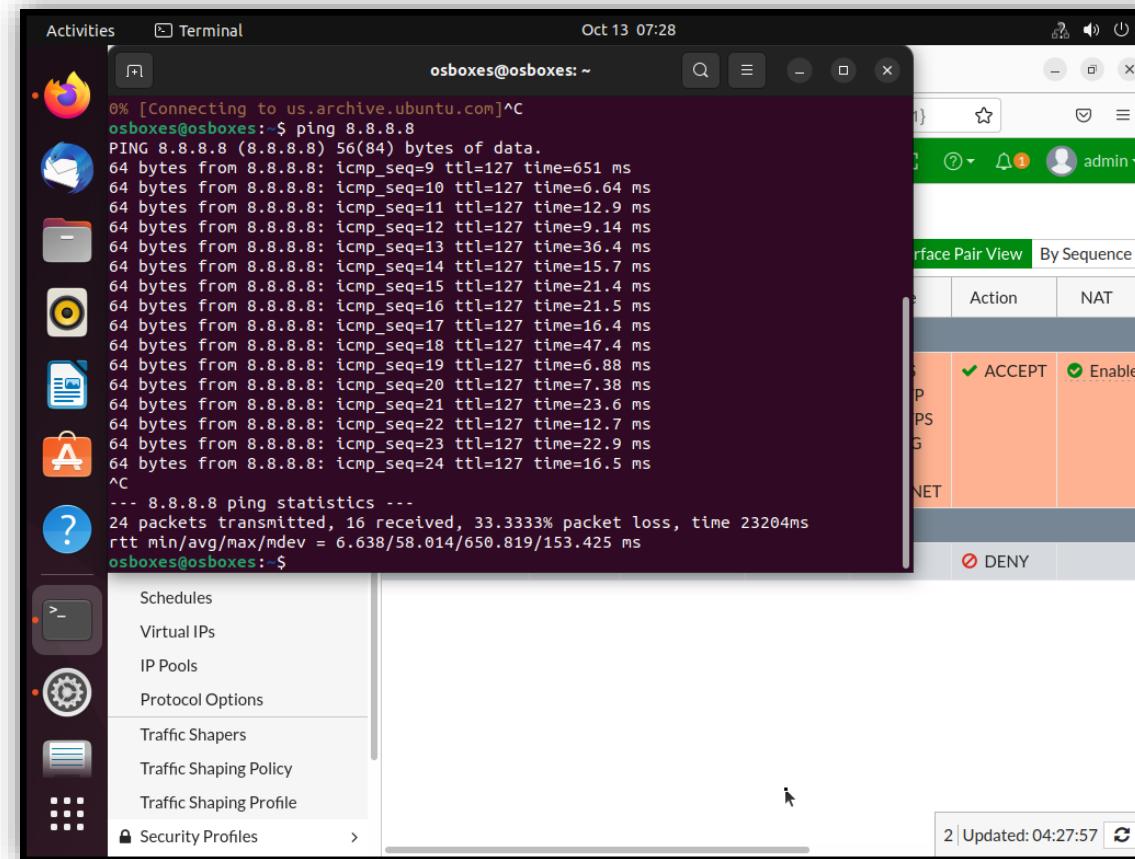
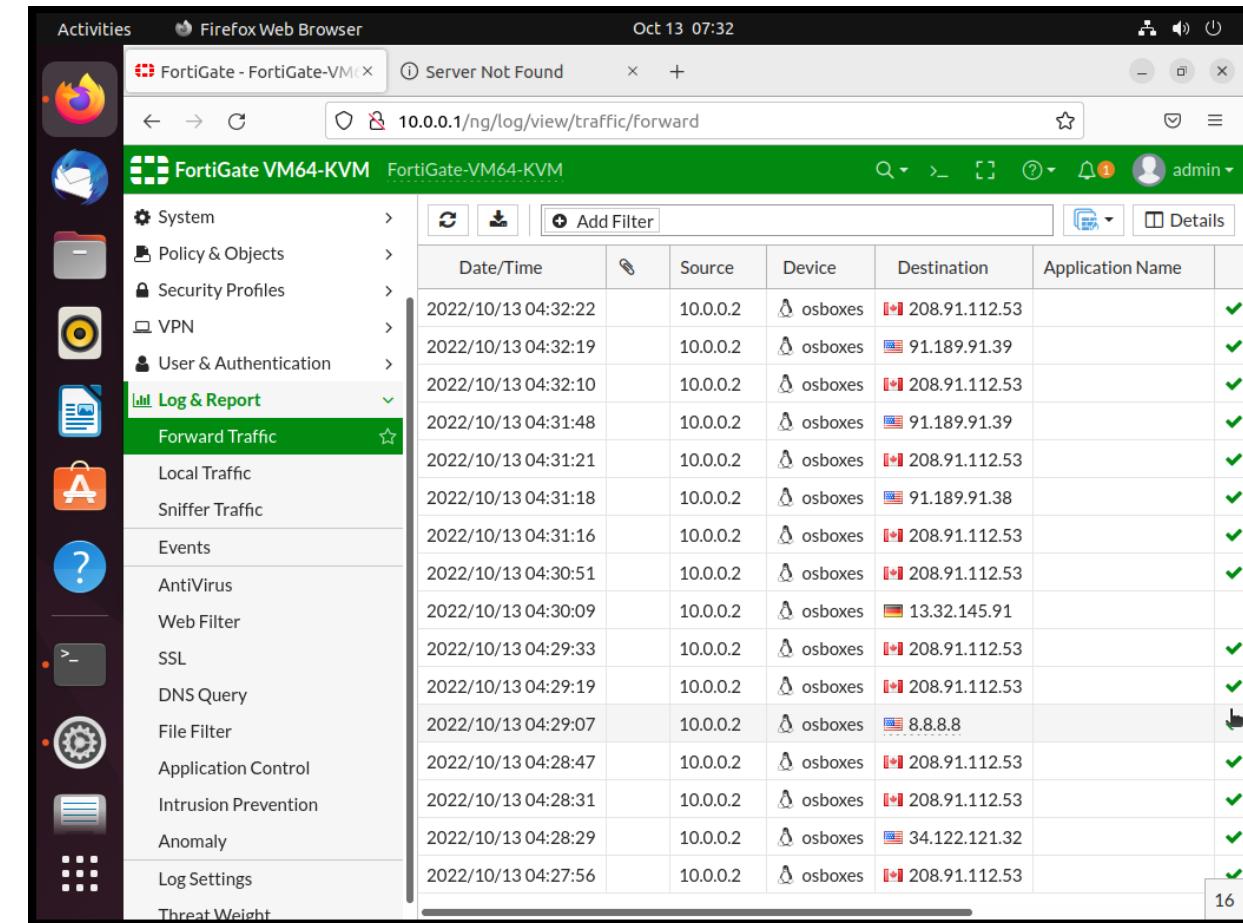


Ilustración 213: Comprueba que el «*ping*» al «8.8.8.8» no responde y después acepta la política.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Para comprobar que tienes salida a Internet también puedes ir al menú «*Log & Report > Forward Traffic*» donde podrás ver los logs que ha dejado nuestra máquina Ubuntu.



The screenshot shows a Firefox browser window titled "FortiGate - FortiGate-VM" with the URL "10.0.0.1/ng/log/view/traffic/forward". The page displays a table of forward traffic logs. The columns are Date/Time, Source, Device, Destination, and Application Name. The logs show traffic from source IP 10.0.0.2 to various destinations, including 208.91.112.53, 91.189.91.39, and 8.8.8.8. Most entries have a green checkmark icon to the right. The left sidebar of the interface includes options like Activities, System, Policy & Objects, Security Profiles, VPN, User & Authentication, Log & Report (which is selected), Forward Traffic, Local Traffic, Sniffer Traffic, Events, AntiVirus, Web Filter, SSL, DNS Query, File Filter, Application Control, Intrusion Prevention, Anomaly, Log Settings, and Threat Weight.

Date/Time	Source	Device	Destination	Application Name	
2022/10/13 04:32:22	10.0.0.2	osboxes	208.91.112.53		✓
2022/10/13 04:32:19	10.0.0.2	osboxes	91.189.91.39		✓
2022/10/13 04:32:10	10.0.0.2	osboxes	208.91.112.53		✓
2022/10/13 04:31:48	10.0.0.2	osboxes	91.189.91.39		✓
2022/10/13 04:31:21	10.0.0.2	osboxes	208.91.112.53		✓
2022/10/13 04:31:18	10.0.0.2	osboxes	91.189.91.38		✓
2022/10/13 04:31:16	10.0.0.2	osboxes	208.91.112.53		✓
2022/10/13 04:30:51	10.0.0.2	osboxes	208.91.112.53		✓
2022/10/13 04:30:09	10.0.0.2	osboxes	13.32.145.91		
2022/10/13 04:29:33	10.0.0.2	osboxes	208.91.112.53		✓
2022/10/13 04:29:19	10.0.0.2	osboxes	208.91.112.53		✓
2022/10/13 04:29:07	10.0.0.2	osboxes	8.8.8.8		
2022/10/13 04:28:47	10.0.0.2	osboxes	208.91.112.53		✓
2022/10/13 04:28:31	10.0.0.2	osboxes	208.91.112.53		✓
2022/10/13 04:28:29	10.0.0.2	osboxes	34.122.121.32		✓
2022/10/13 04:27:56	10.0.0.2	osboxes	208.91.112.53		✓

Ilustración 214: Visita la pestaña «Forward Traffic» para comprobar que tienes salida a Internet.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Crearemos una ruta estática apuntando al *router*. Estas rutas definen una ruta explícita entre dos dispositivos de red. Las rutas estáticas no se actualizan automáticamente y se deben reconfigurar de forma manual si se modifica la topología de la red.
- Para ello, ve a «*Network > Static Routes > Create New*».

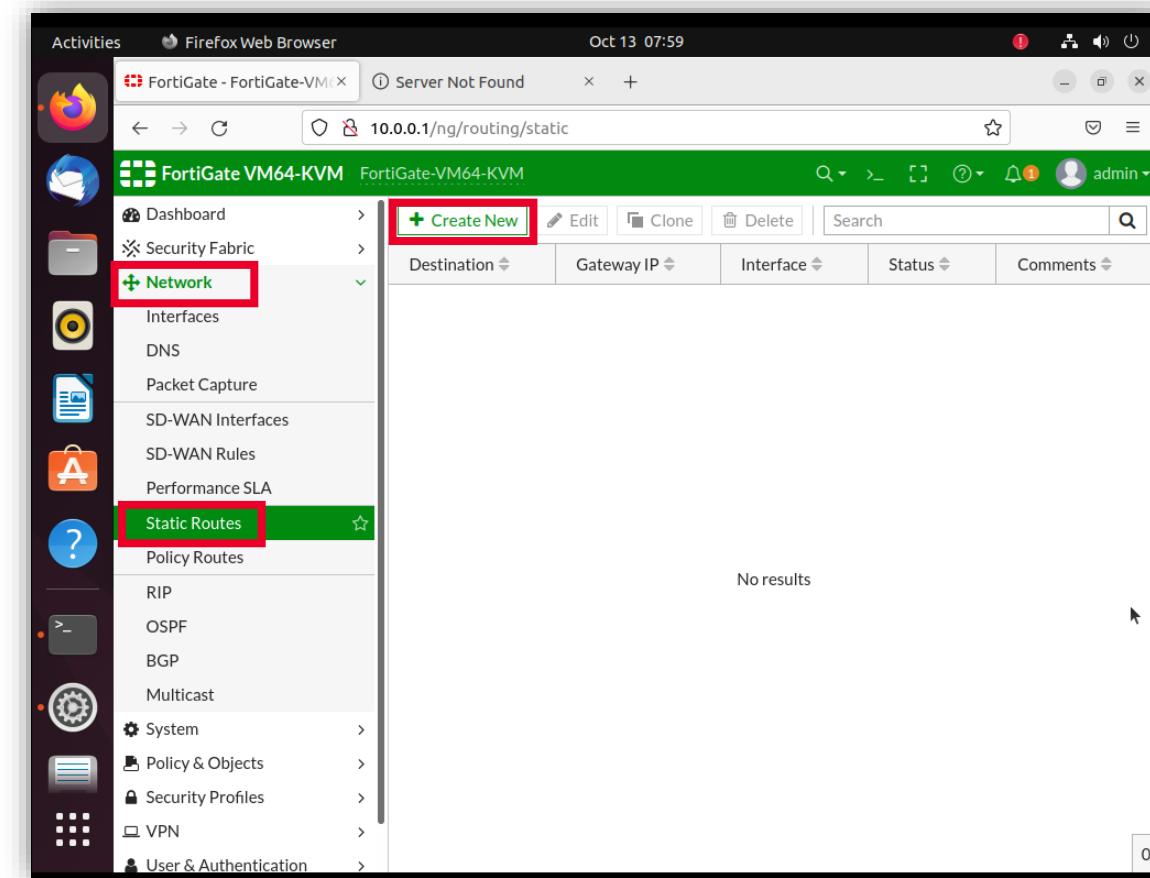


Ilustración 215: Creación de una ruta estática apuntando al *router*.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- En el *Gateway* añade una IP del mismo rango que la que nos asigna la WAN, en nuestro caso 192.168.72.X

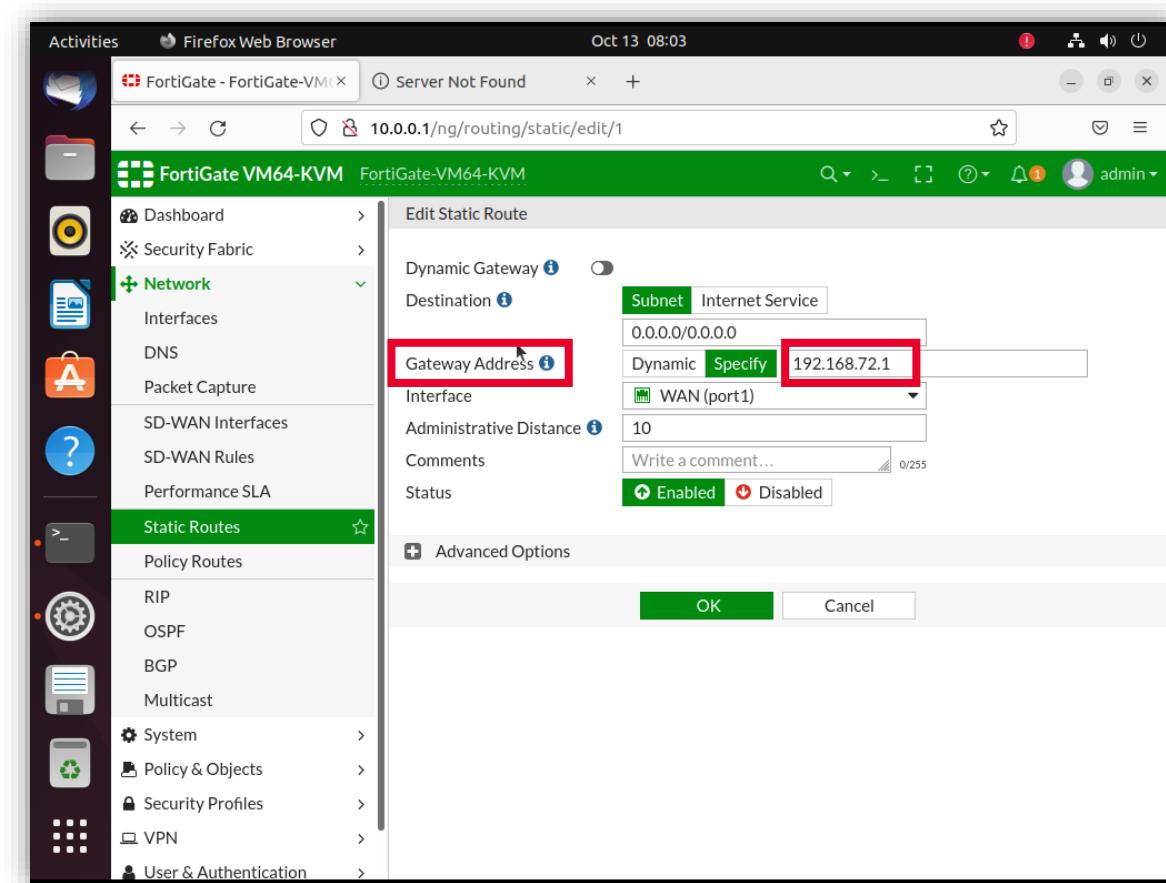


Ilustración 216: IP añadida por el *Gateway*.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Una vez tengamos todo esto configurado vamos a crear una topología configurando VLAN.
- Vamos a añadir 3 equipos y un *switch* y cada uno de los PC tendrá una VLAN diferente: 100, 200 y 300.

Así debería quedar la conexión entre dispositivos:

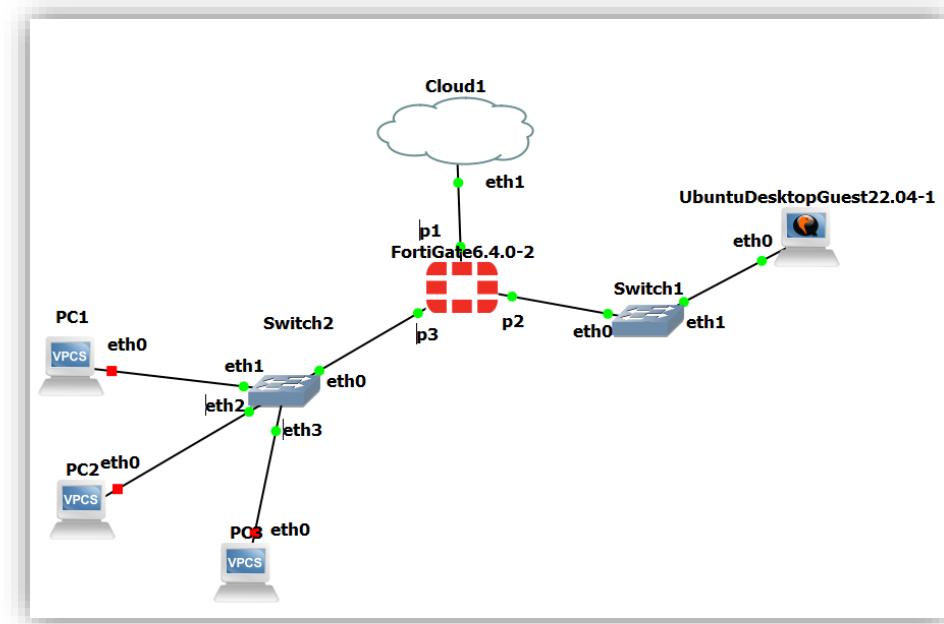


Ilustración 217: Conexión entre dispositivos.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Configura el *switch* para que las VLANs puedan comunicarse y permita pasar las conexiones entre ellas.

Así debe quedar la configuración del *switch*:

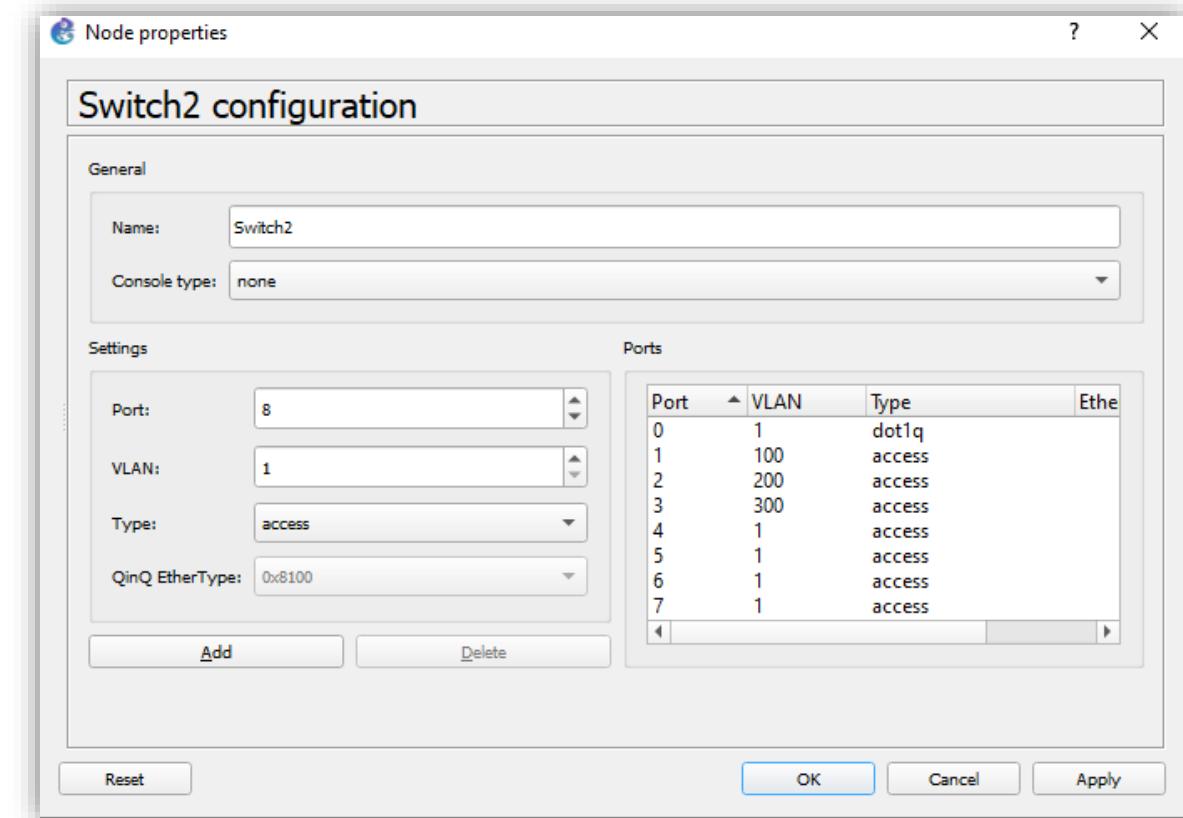


Ilustración 218: Configuración del *switch*.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Ahora vamos a crear las VLANs en FortiGate. Ve al menú «*Network > Interfaces*».
- Seleccionando el puerto 3 haz clic en «*Create New*».
- Rellena los siguientes campos:
 - **Name**.
 - **Alias**.
 - **Interface**: elige el puerto al que están conectados los nuevos equipos.
 - **VLAN ID**: en nuestro caso 100. Tendrás que poner la misma configuración que utilizaste al configurar el *switch*.
 - **Address**: selecciona el modo manual y asigna una IP.
 - **Administrative Access**: selecciona los servicios necesarios.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

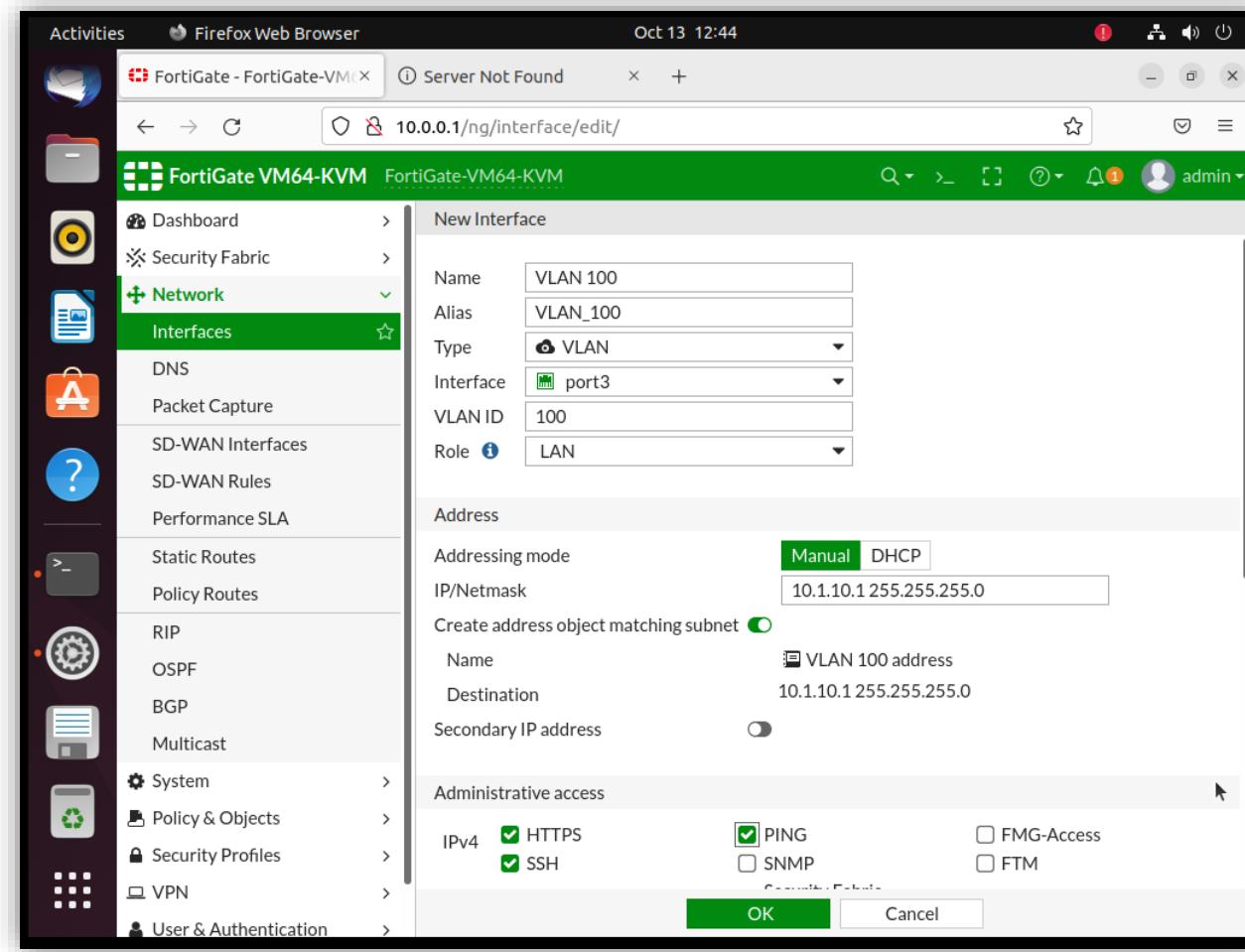


Ilustración 219: Completa los campos vistos.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- **DHCP Server:** activa esta pestaña y aparecerá un rango de IPs automáticamente.

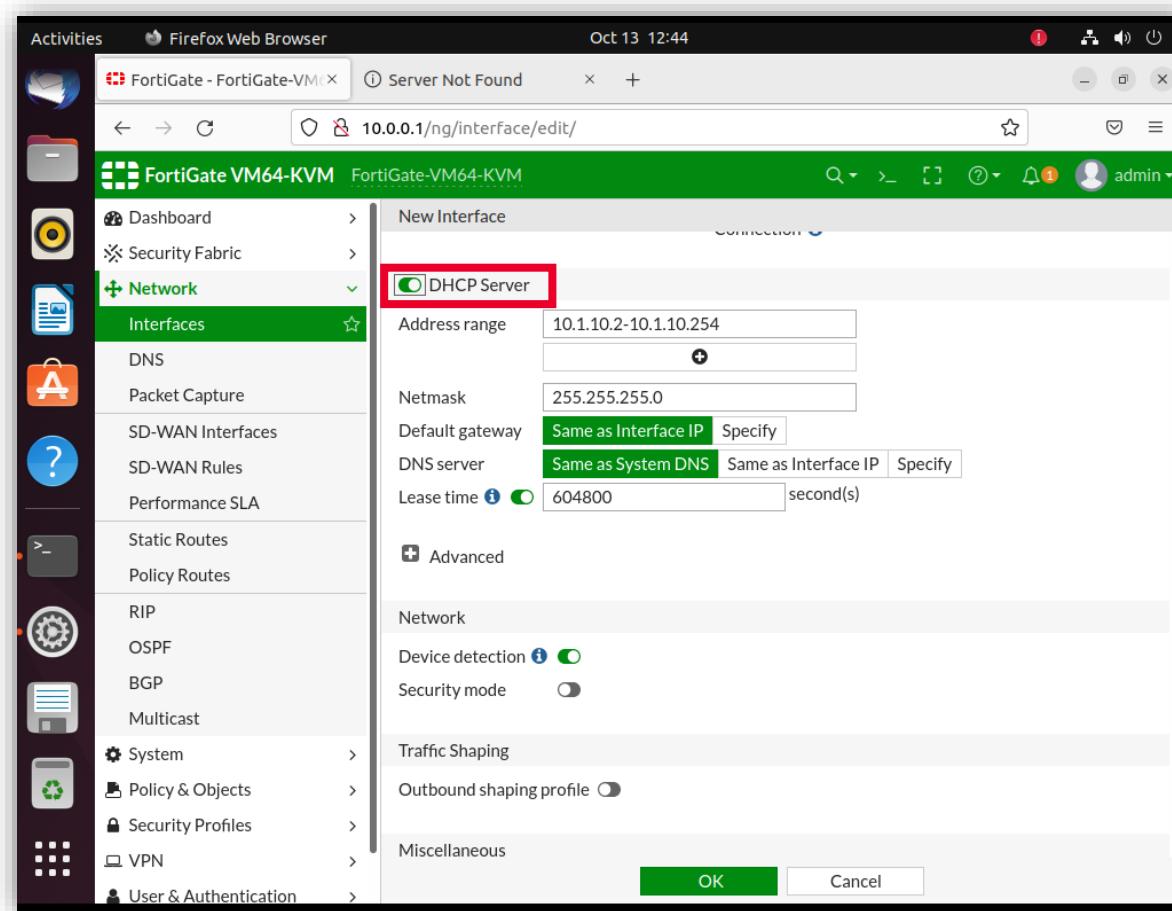


Ilustración 220: Activa DHCP server.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Configura el resto de VLANs como la anterior.

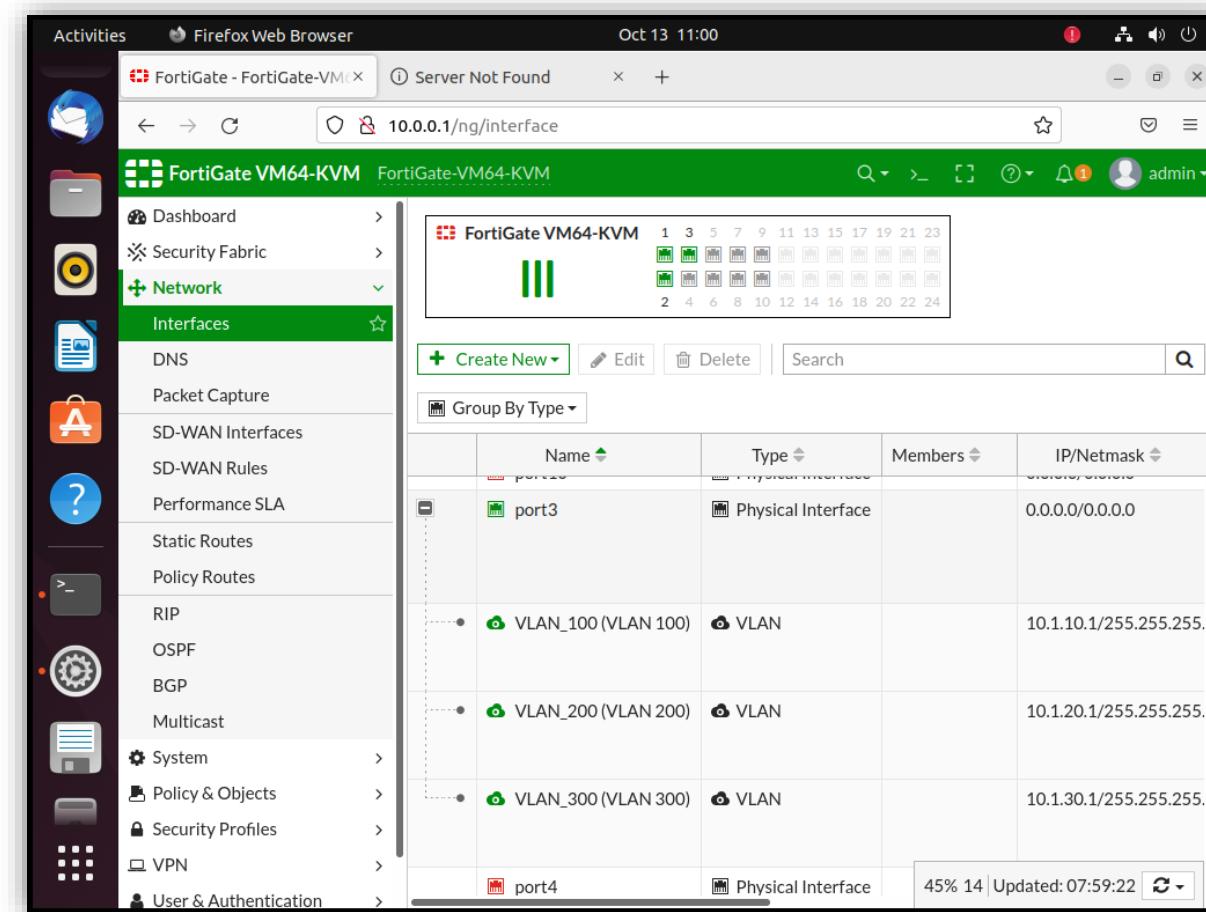


Ilustración 221: Configuración del resto de VLANs.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Para comprobar que la configuración está bien ejecuta el comando «**dhcp**» en cada uno de los PC para ver si se asigna una IP automáticamente dentro del rango asignado.

```
PC1> dhcp  
DDORA IP 10.1.10.2/24 GW 10.1.10.1
```

Ilustración 222: Comprueba que la configuración está bien ejecuta con el comando «**dhcp**» para el «PC1».

```
PC2> ip dhcp  
DDORA IP 10.1.20.2/24 GW 10.1.20.1
```

Ilustración 223: Comprueba que la configuración está bien ejecuta con el comando «**dhcp**» para el «PC2».

```
PC3> dhcp  
DDORA IP 10.1.30.2/24 GW 10.1.30.1
```

Ilustración 224: Comprueba que la configuración está bien ejecuta con el comando «**dhcp**» para el «PC3».



PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Ahora crearemos una política para que, por ejemplo, la VLAN100 tenga conexión con la VLAN200, pero que a su vez la VLAN200 no tenga conexión con la VLAN100. Para ello, ve al menú «*Policy&Objects > Firewall Policy > Create New*».
- Rellena los siguientes campos:
 - **Name:** nombre que denomine la política.
 - **Incoming interface:** desde dónde viene el tráfico.
 - **Outgoing interface:** hacia dónde va el tráfico.
 - **Source:** equipo desde el que viene el tráfico. En este caso seleccionaremos solo el equipo desde el que sale el tráfico.
 - **Destination:** equipo hacia el que va el tráfico. Ahora seleccionaremos los equipos a los cuales queremos llegar, podría ser sólo la VLAN200 o añadir también la VLAN300. En nuestro caso añadiremos sólo la VLAN200.
 - **Service:** elige y busca los servicios que permitiremos y que sean necesarios.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

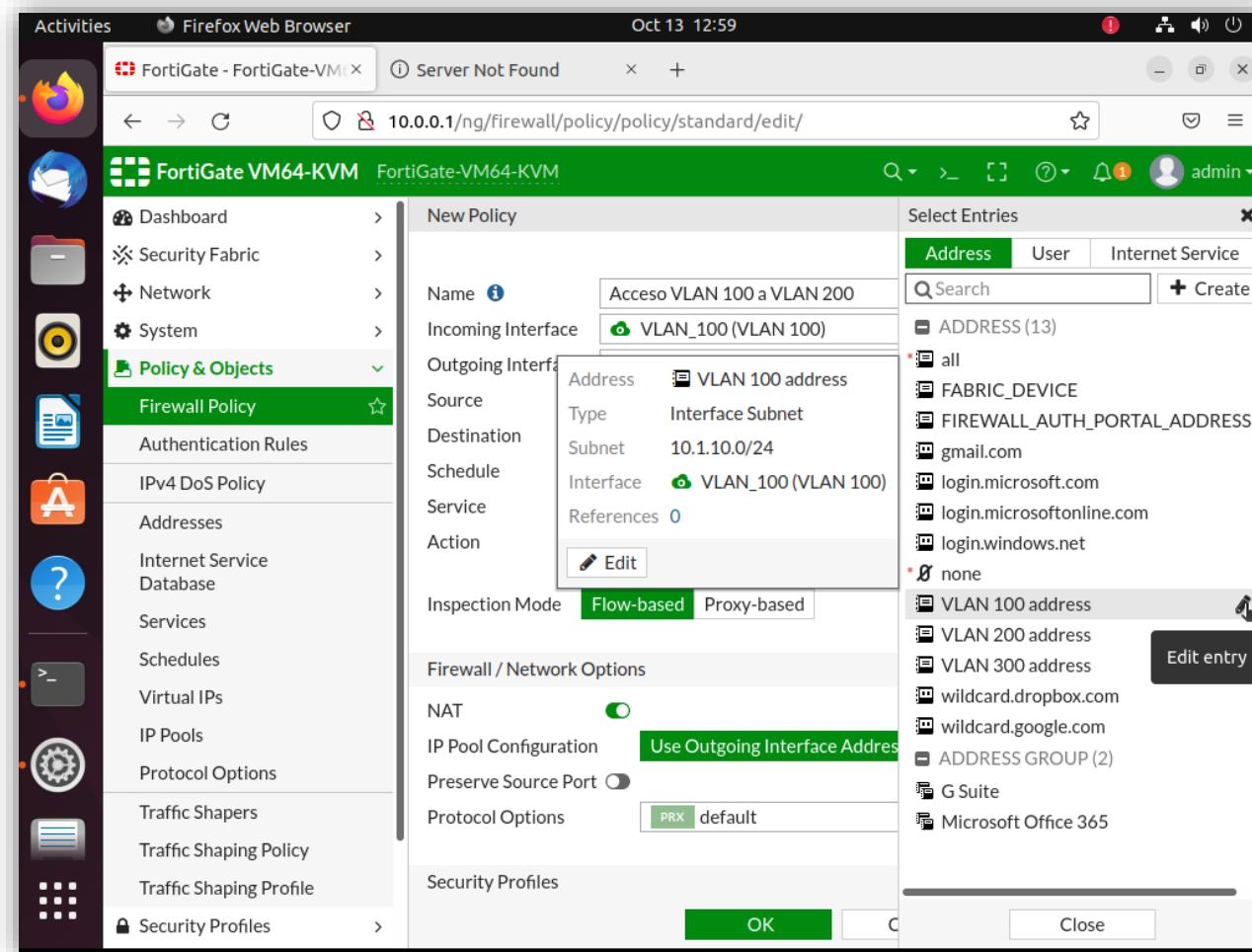


Ilustración 225: Completa los campos para crear una política para la conexión entre la VLAN100 y la VLAN200.

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Haz clic en «OK» para guardar la política.

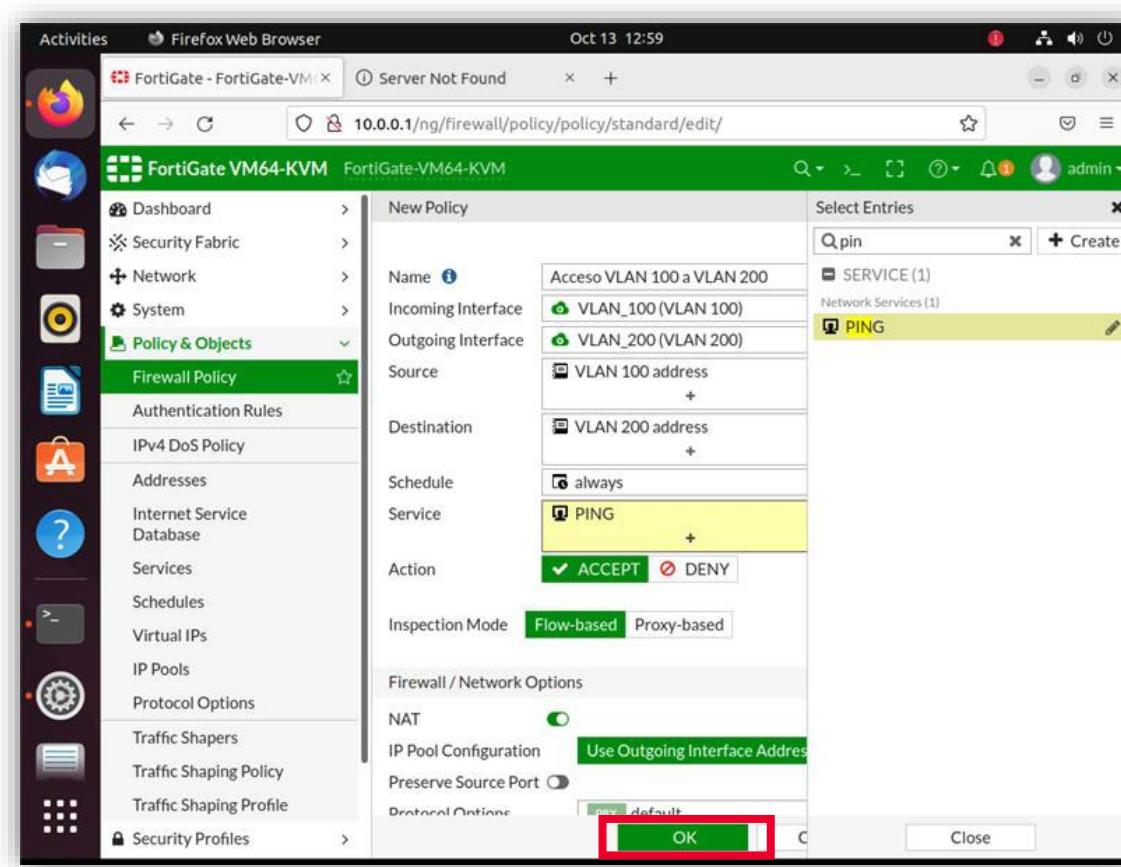


Ilustración 226: Guarda la política pulsando «ok».

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Para comprobar que esta política funciona haremos «ping» a la IP de la VLAN200 de la cual obtendremos respuesta.

```
PC1> ping 10.1.20.2

84 bytes from 10.1.20.2 icmp_seq=1 ttl=63 time=8.778 ms
84 bytes from 10.1.20.2 icmp_seq=2 ttl=63 time=5.489 ms
84 bytes from 10.1.20.2 icmp_seq=3 ttl=63 time=5.260 ms
84 bytes from 10.1.20.2 icmp_seq=4 ttl=63 time=2.685 ms
^C
```

Ilustración 227: Comprobación del funcionamiento de la política para la VLAN200 desde el «PC1».

- Pero al realizar «ping» a la IP de la VLAN300 podemos observar que no hay respuesta.

```
PC1> ping 10.1.30.2

10.1.30.2 icmp_seq=1 timeout
10.1.30.2 icmp_seq=2 timeout
^C
PC1>
```

Ilustración 228: Comprobación del funcionamiento de la política para la VLAN300 desde el «PC1».

7

PRÁCTICA: TOPOLOGÍA DE RED CON FW

- Y lo mismo si hacemos «ping» desde el «PC2» perteneciente a la VLAN200 hacia el «PC1» perteneciente a la VLAN100.

```
PC2> ping 10.1.10.2  
  
10.1.10.2 icmp_seq=1 timeout  
10.1.10.2 icmp_seq=2 timeout  
^C  
PC2>
```

Ilustración 229: Comprobación del funcionamiento de la política para la VLAN100 desde el «PC2».

- Mediante estas políticas podremos configurar el acceso y los permisos de cada una de las VLAN como consideremos.

¡GRACIAS!



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL

 incibe

INSTITUTO NACIONAL DE CIBERSEGURIDAD

