MANUAL PARA SIMULAR LA TOPOLOGIA DE RED Y SEGURIDADES DEL SERVIDOR WEB EN LA COOPERATIVA DE AHORRO Y CRÉDITO “RIOBAMBA” LTDA.

Universidad Nacional de Chimborazo
Realizado por: Francisco Pérez Rosero
Riobamba - Ecuador
2020

CONTENIDO

INTRODUCCIÓN

Debido a la globalización y el avance de la tecnología, la información ha tomado un papel muy importante en cualquier organización. Además, debido al avance tecnológico, todas las organizaciones se han visto en la necesidad de adaptarse y sistematizar su información. Es por esto que en todo el mundo ocurren diferentes tipos de ataques informáticos a diario, lo que puede llevar a daños y alteraciones en la información. Esto conlleva a un gran problema ya que actualmente la información se ha convertido en uno de los activos más importantes de las organizaciones y al verse afectada puede causar daños económicos irreparables.

Por otra parte, el impacto y costo del cibercrimen sigue en aumento. Un informe realizado por Cybersecurity señala que en 2021 habrá 3.5 millones de nuevos puestos de trabajo en ciberseguridad. Sin embargo, las previsiones de empleos en seguridad cibernética no han podido seguir el ritmo del espectacular aumento del cibercrimen, ya que se provee que este le costará al mundo 6 mil millones de dólares (mdd) anuales.

El presente trabajo de investigación presentará una técnica para la detección de vulnerabilidades en la web, como lo es Banner Grabbing de uso intuitivo y soportado integralmente en herramientas de software. Dicha técnica presenta un enfoque práctico y conceptual para la detección y evaluación de vulnerabilidades en la web. Adicionalmente, se detallará un caso de estudio práctico dentro de la Cooperativa de ahorro y crédito “Riobamba Ltda. Mediante el cual se logra establecer la utilidad y funcionalidad de esta.

1. Requisitos para instalación de la herramienta de simulación GNS3

GNS3 es una plataforma que permite simular topologías de red con imagenes de marcas como Cisco, Juniper y Fortigate entre otros. A continuación, se muestran los requerimientos para la instalación del software GNS3.

1.2 Compatibilidad con Windows

GNS3 es compatible con los siguientes sistemas operativos de Windows:

• Windows 7 SP1 (64 bit).

• Windows 8 (64 bit).

• Windows 10 (64 bit).

• Windows Server 2012 (64 bit).

• Windows Server 2016 (64 bit).

1.3 Requerimientos mínimos

Los siguientes son los requisitos mínimos para un entorno Windows en GNS3:

Ítem	Requerimientos mínimos
Sistema Operativo	Windows 7 (64 bit) o superior
Procesador	2 o más núcleos lógicos
Virtualización	Se requieren extensiones de virtualización. Es posible que deba habilitar esto a través del BIOS de su computadora.
Memoria	4 GB RAM
Espacio en disco	1GB de espacio disponible

Tabla 1: Requerimientos mínimos para GNS 3

2.4 Requerimientos recomendados

Ítem	Requerimientos mínimos
Sistema Operativo	Windows 7 (64 bit) o superior
Procesador	4 o más núcleos lógicos – AMD-V / RVI Series o Intel VT-X / EPT
Virtualización	Se requieren extensiones de virtualización. Es posible que deba habilitar esto a través del BIOS de su computadora.
Memoria	16 GB RAM
Espacio en disco	Disco de Estado Sólido (SDD) 35 GB de espacio disponible

Tabla 2: Requerimientos recomendados para GNS3

2. Descarga de GNS3

Para descargar GNS3 lo puede hacer desde la página oficial https://www.gns3.com/ donde encontrará el boto “Free Download” al dar click se mostrará aparece una pantalla como se muestra en la Fig.

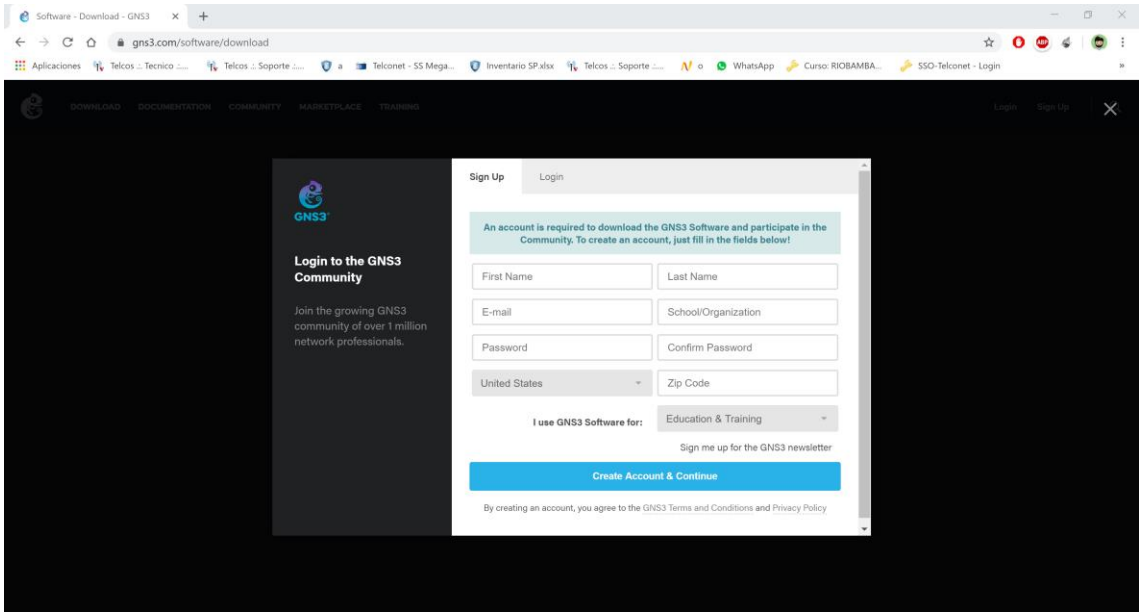


Figura 1: Pantalla de descarga GNS3.

Después es necesario registrarse para poder descargar el simulador una vez que se llene los datos podrá descargar y saldrá la siguiente pantalla que se muestra en la Fig. 2

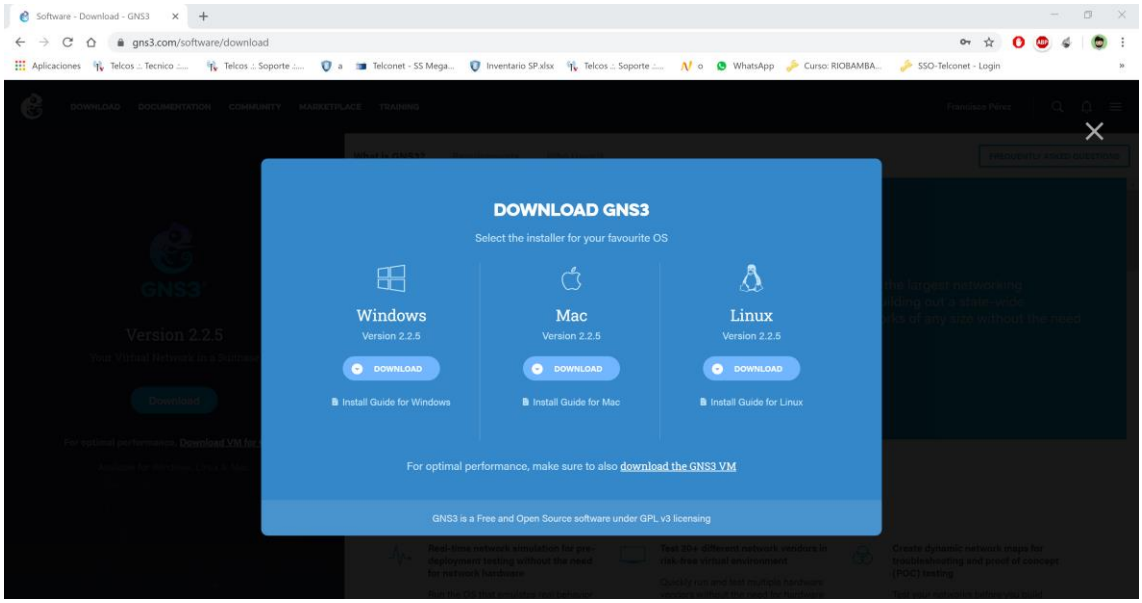


Figura 2: Imagen para descargar GNS3

Como se observa en la Fig. 2 se puede descargar para varias plataformas como son Windows, Linux o IOS. Una vez que de click en "Download" la descarga iniciará automáticamente.

3. Instalación de GNS3

A continuación, se describe el procedimiento de instalación de GNS3 en Windows 10, la ejecución es similar para otras versiones de Windows.

3.1 Inicio de instalación

Una vez finalizada la descarga se debe ejecutar el archivo, luego les pedirá permisos de administrador, le dan Ok y aparecerá la siguiente pantalla según la Figura 3.1, esta hace referencia al acuerdo de licencia para poder ejecutar la instalación GNS3. Dar Click en "Agree".

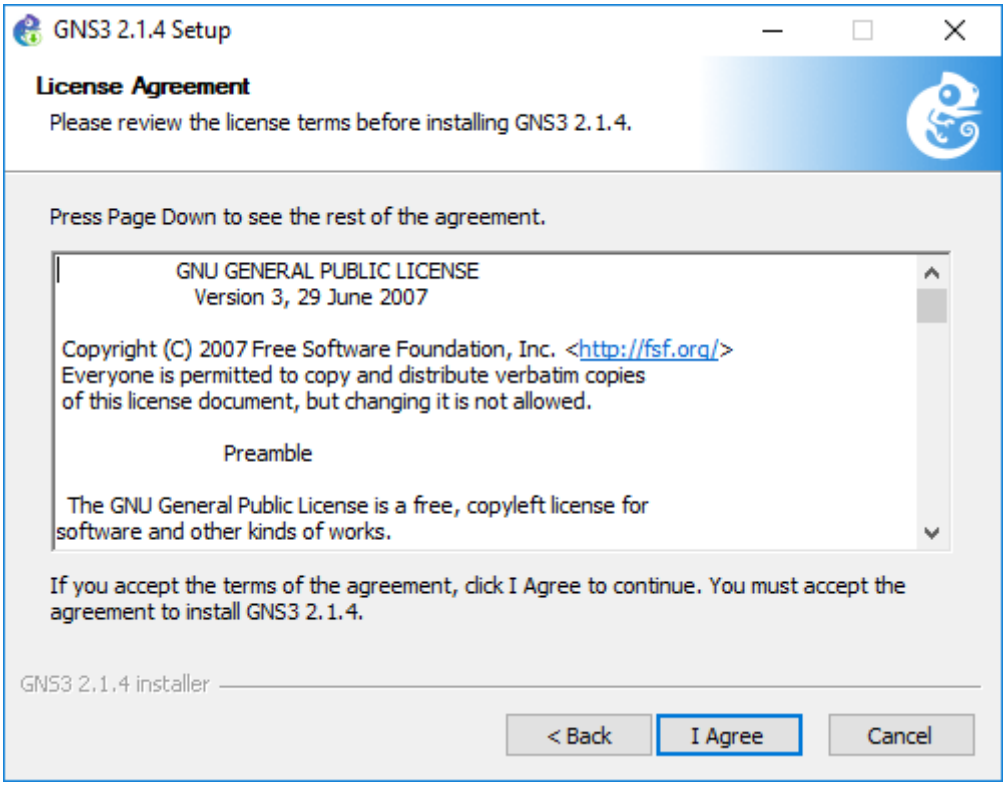


Figura 3: Acuerdos de Licencia para instalar el simulador GNS3

3.2 Selección de componentes para la instalación

A continuación, se solicitará seleccionar los componentes que se instalarán junto con el simulador tal como se muestra en la Figura 4. Considerar la Tabla 3. con relación a los componentes que están incluidos durante la instalación del GNS3, además de la función de cada uno de ellos y la web de sus desarrolladores. Se recomienda seleccionar e instalar los componentes que están en negrita.

Aplicación	Función	Web del Desarrollador
GNS3	Simulador gráfico de red	https://www.gns3.com/
WinPCAP	Permite enviar y capturar paquetes	https://www.winpcap.org/

WireShark	Analizador de paquetes	https://www.wireshark.org/
Dynamips	Emulador de router Cisco	https://rednectar.net/tag/dynamips/
QEMU	Ejecuta máquinas virtuales	https://www.qemu.org/
Cpulimit	Limita el uso que hace la CPU en un proceso	https://sourceforge.net/projects/vpcs/
TightVNC Viewer	Control remoto de máquinas virtuales	https://www.tightvnc.com
Solar Winds Response	Analizador de paquetes trabaja con WireShark	https://www.solarwinds.com
Npcap	Sniffer de puertos	https://nmap.org/npcap/
VPCS	Simulador de Terminales (PC)	https://sourceforge.net/projects/vpcs/

Tabla 3: Lista de componentes incluidos en la instalación del GNS3

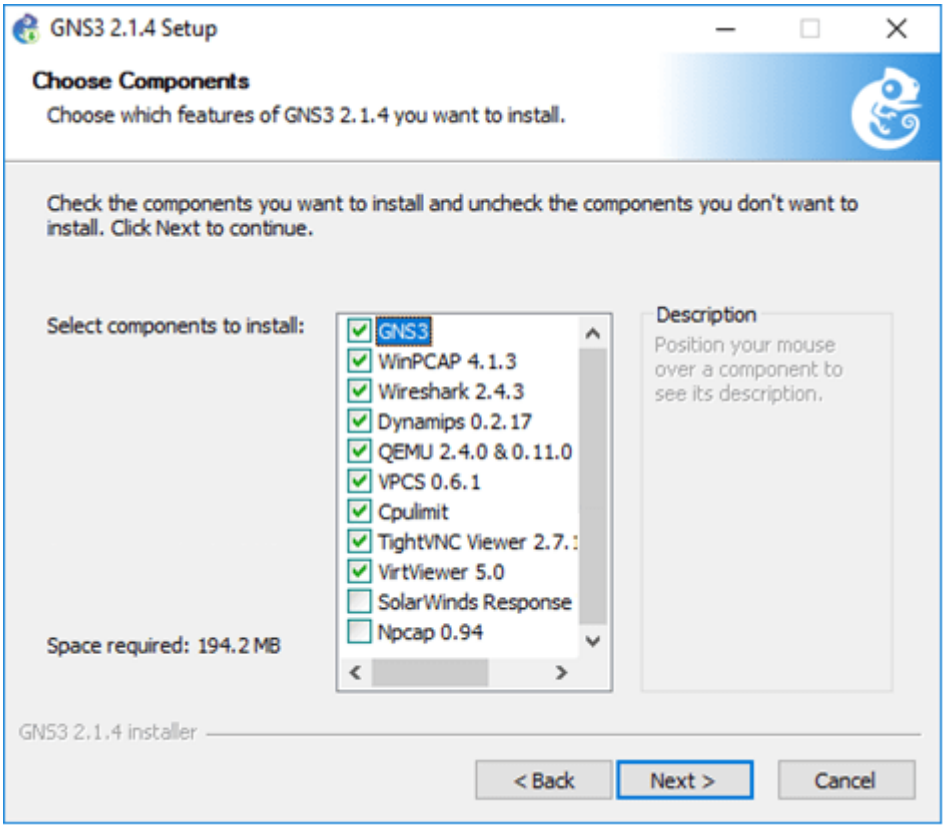


Figura 4: Selección de componentes para la instalación de GNS3

Posteriormente, seleccionar la carpeta donde se instalará la aplicación, en este caso se ha dejado la carpeta por defecto tal como se muestra en la Figura 5.

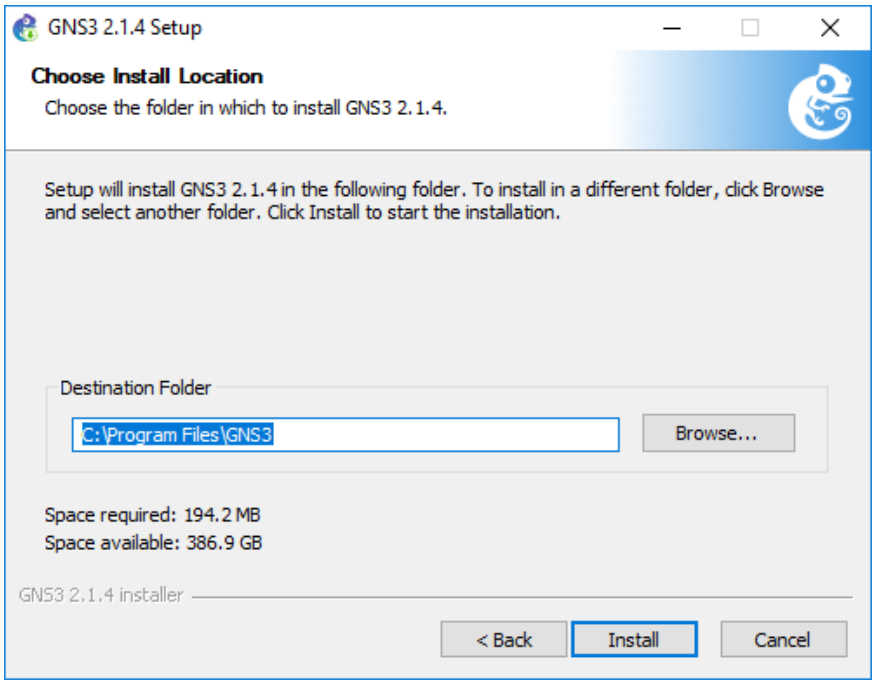


Figura 5: Selección de la carpeta para la instalación

Después se realiza el inicio de la copia de archivos tal como se muestra en la Figura 6. Se instalarán aplicaciones adicionales como el Visual C++, darle los accesos para que pueda ejecutarse la aplicación sin problemas.

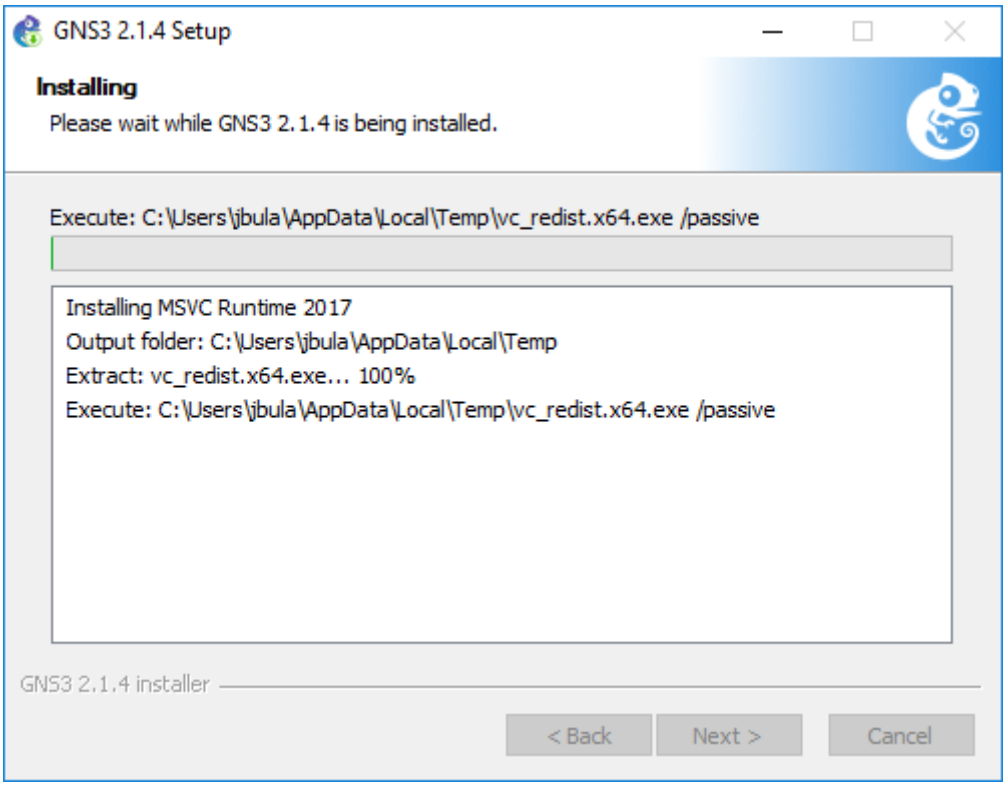


Figura 6: Inicio de instalación en el disco local

En algunos casos se requerirá la conexión a internet para poder descargar aplicaciones como WireShark. (Ver Figura 7).

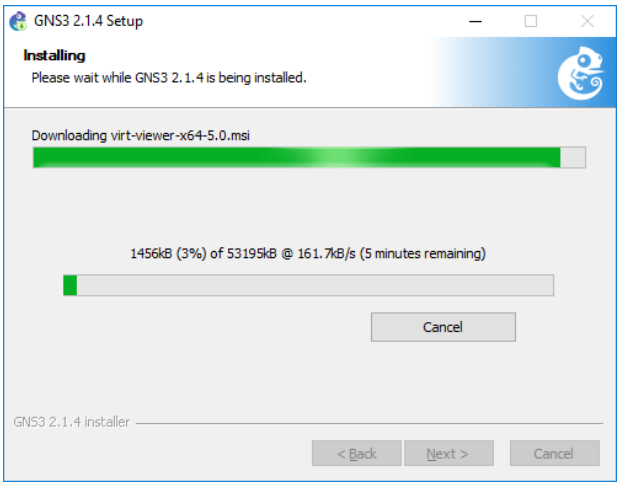


Figura 7: Descarga de aplicaciones de internet

Luego se completa la copia de los archivos como se muestra en la Figura 8. click en Next para continuar

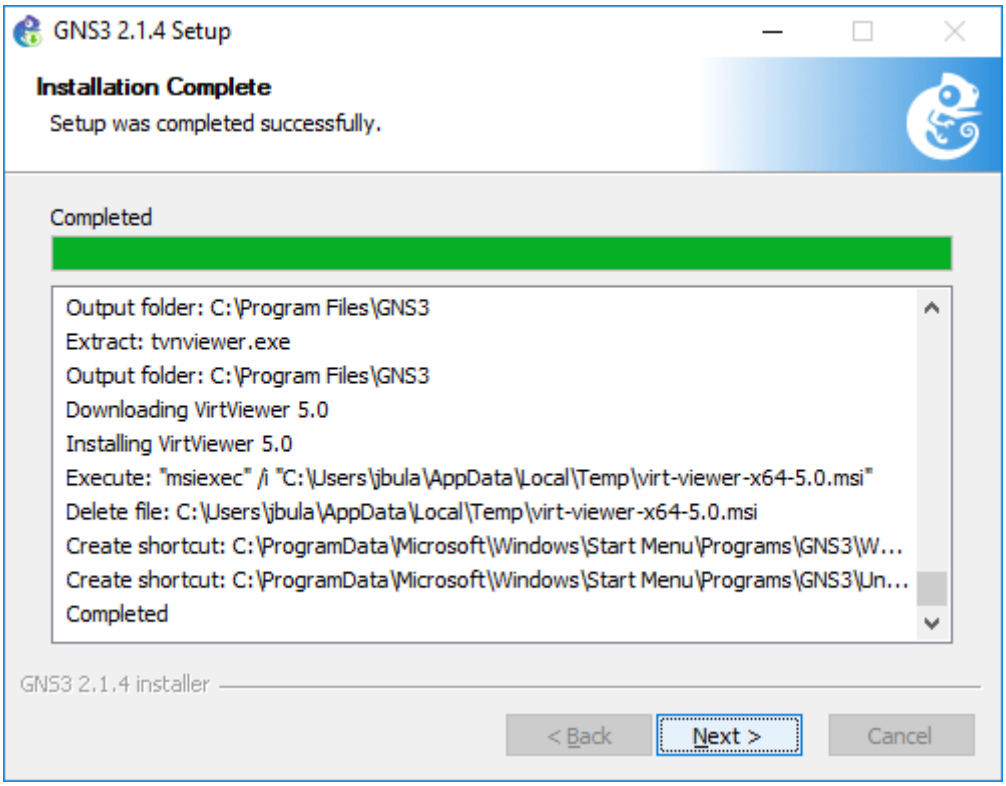


Figura 8: Finalización de copiados de archivos

3.3 Finalización de la instalación de GNS3

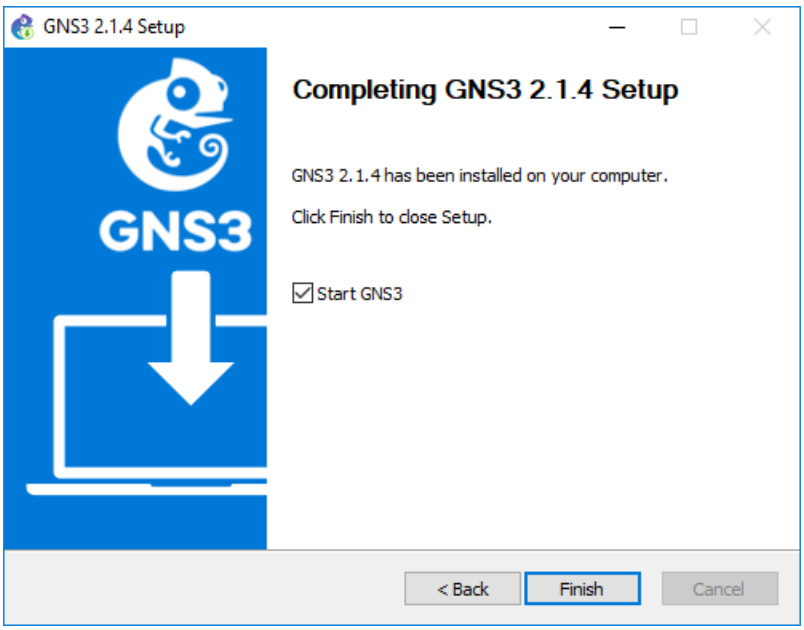


Figura 9: Finalización de la instalación de GNS3

4. Primer inicio de GNS3: Setup Wizard

Luego de la instalación el siguiente paso a seguir es la configuración de la interfaz gráfica de usuario mediante el Setup Wizard, para poder alojar las imagenes IOS, esto se puede realizar mediante una máquina virtual o servidor, la Figura 4.1. muestra la pantalla en el primer inicio de GNS3.

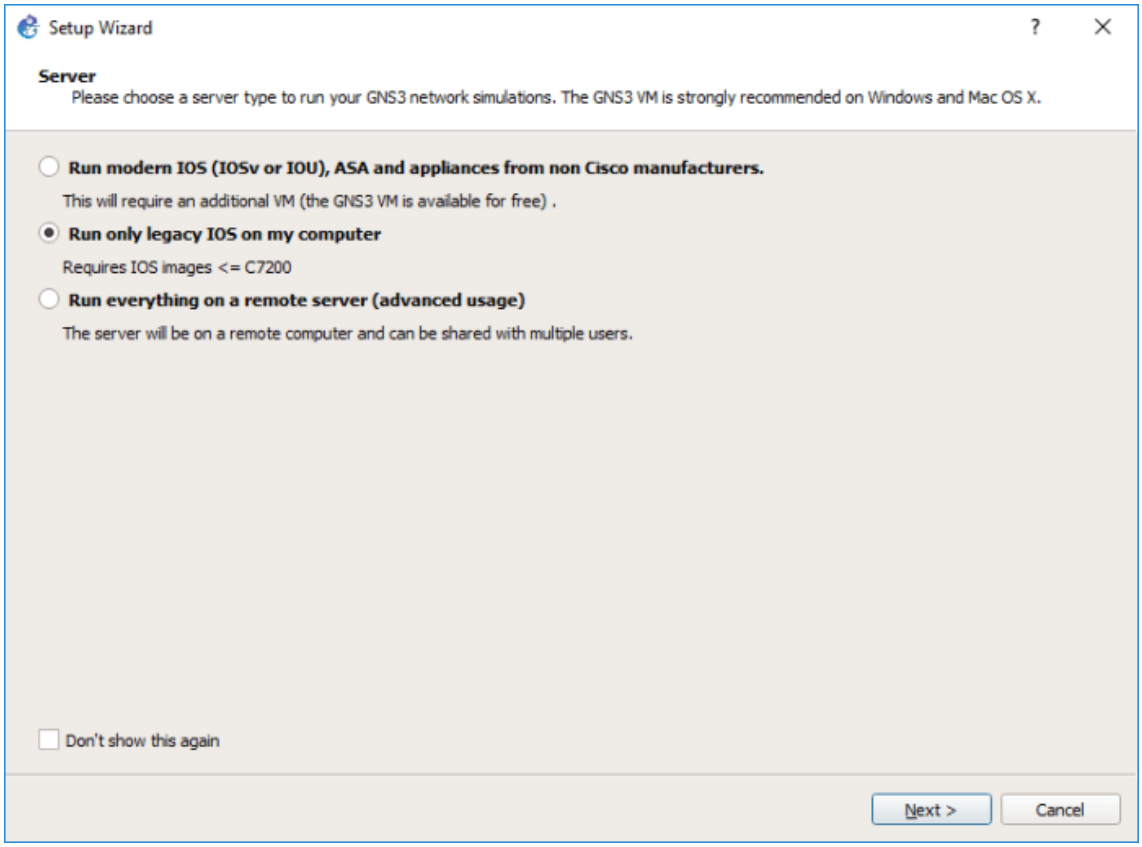


Figura 10: Selección del servidor para la simulación en GNS3.

De acuerdo al menú se tienen tres opciones:

- Run Modern IOS (IOSv or IOU), ASA and appliances from non Cisco manufacturers: Requiriere la configuración de una Máquina Virtual.
- Run only legacy IOS on my computer: La carga de IOS se puede realizar directamente en la plataforma GNS3 mediante servidor local.
- Run everything on a remote server (para usuarios avanzados): se realiza la carga de los dispositivos a través de Servidores remotos.

5. Configuración de Imagenes y Dispositivos

5.1 Iniciar dispositivos IOS modernos (IOSv or IOU) con GNS3 VM

Si se decide usar la máquina virtual GNS3 (recomendado), puede ejecutar la máquina virtual GNS3 localmente en su PC utilizando software de virtualización como VMware Workstation o Virtualbox; o puede ejecutar la máquina virtual GNS3 de forma remota en un servidor utilizando VMware ESXi o incluso en la nube.

Se puede usar GNS3 solo con el servidor local, sin usar la máquina virtual GNS3, esta es una buena manera de comenzar, sin embargo, esta configuración es limitada y no ofrece tantas opciones con respecto al tamaño de topología y los dispositivos admitidos. Si desea crear topologías GNS3 más avanzadas o desea incluir dispositivos como los dispositivos Cisco VIRL (IOSvL2, IOSvL3, ASAv) u otros dispositivos que requieran Qemu, se recomienda la máquina virtual GNS3 VM (y a menudo se requiere).

5.2 Iniciar imagenes IOS antiguas mediante el Servidor Local GNS3

Mediante esta opción se ejecuta las imagenes y dispositivos en la misma PC donde instaló el software todo en uno GNS3. Si, por ejemplo, está utilizando una PC con Windows, tanto la GUI GNS3 como el servidor local GNS3 se están ejecutando como procesos en Windows. Procesos adicionales como Dynamips también se ejecutarán en su PC, en la

siguiente sección se detalla la configuración del servidor local y la carga de imagenes IOS legacy.

6. Configuración del servidor Local GNS3

Mediante el Setup Wizard elegir «Run only legacy IOS on my computer» y dar Next, a continuación, se debe elegir la ubicación donde se encuentra la aplicación «gns3server.exe», además, la IP y el puerto. Se recomienda colocar los siguientes parámetros:

- Server path: Ubicación por defecto del ejecutable gns3server.EXE,
- Host Binding: Colocar IP 127.0.0.1 que es la dirección IP de loopback,
- Port: 3080 TCP

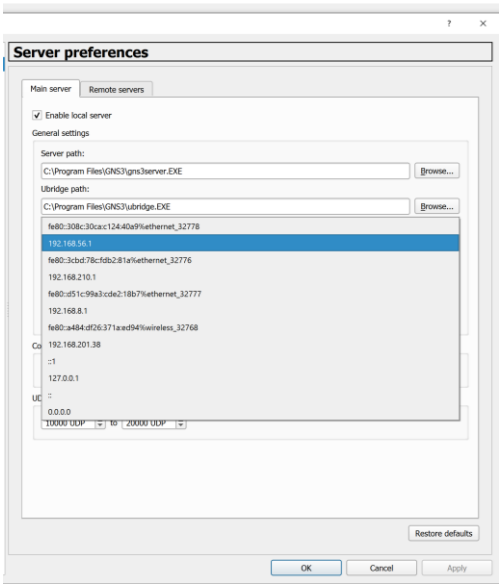


Figura 11: Setup Wizard local server.

En esta sección podemos elegir bajo que host se va ejecutar la VM de GNS3 es recomendable usar la que se muestra en la figura 11. Para que no existan errores en conexiones con dispositivos.

7. Configura una Imagen IOS al Servidor Local GNS3 (Dynamips)

En la pantalla «New appliance template», se podrá agregar una Imagen IOS para GNS3 mediante el servidor Local GNS3 previamente configurado, en este caso es se utilizará la Imagen de un Router Cisco 7200 el cual sirvió para simular el router que da salida a internet a la cooperativa.

Se debe seleccionar "Ad dan IOS router using a real IOS image (supported by Dynamips)", tal como se muestra en la Figura 12

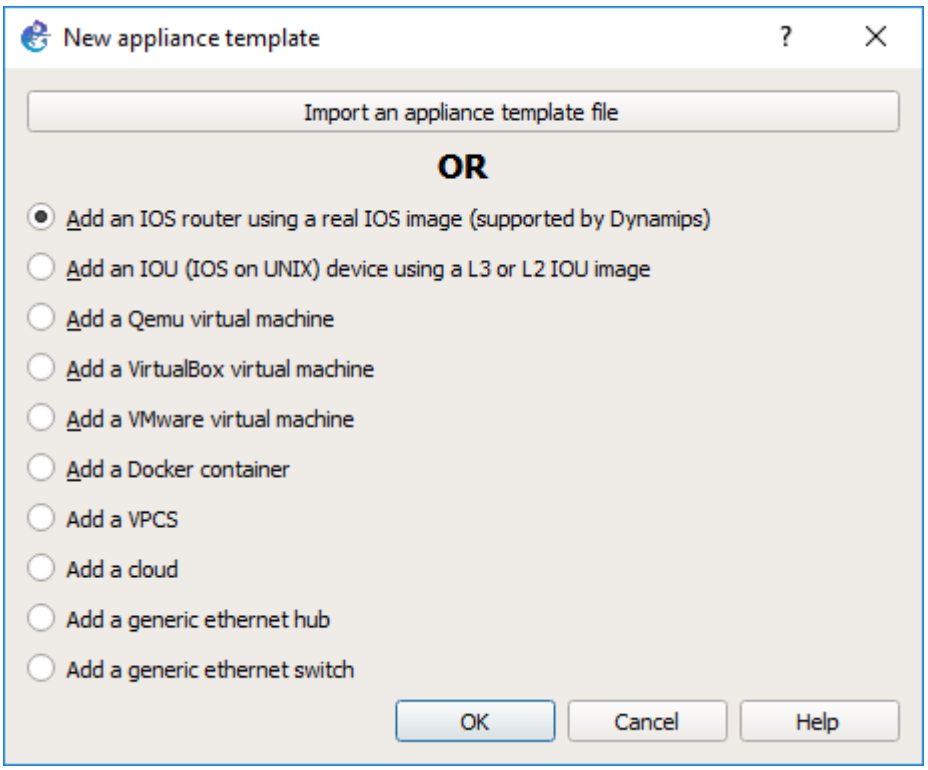


Figura 12: Pantalla que permite agregar un nuevo dispositivo

Luego se debe seleccionar la ubicación del IOS del router Cisco, damos click en "Browse". (Ver Figura 13)

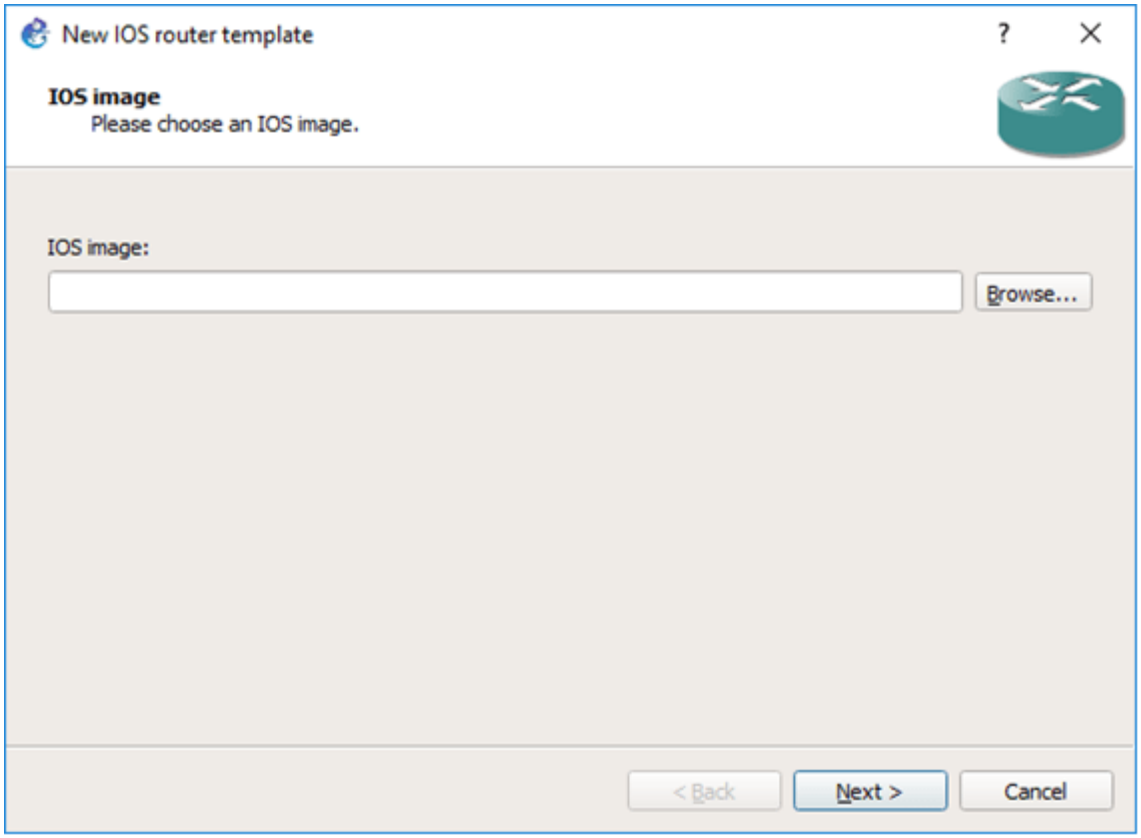


Figura 13: Pantalla para la carga del IOS

Seleccionaremos la ubicación del IOS. (Ver Figura 14)

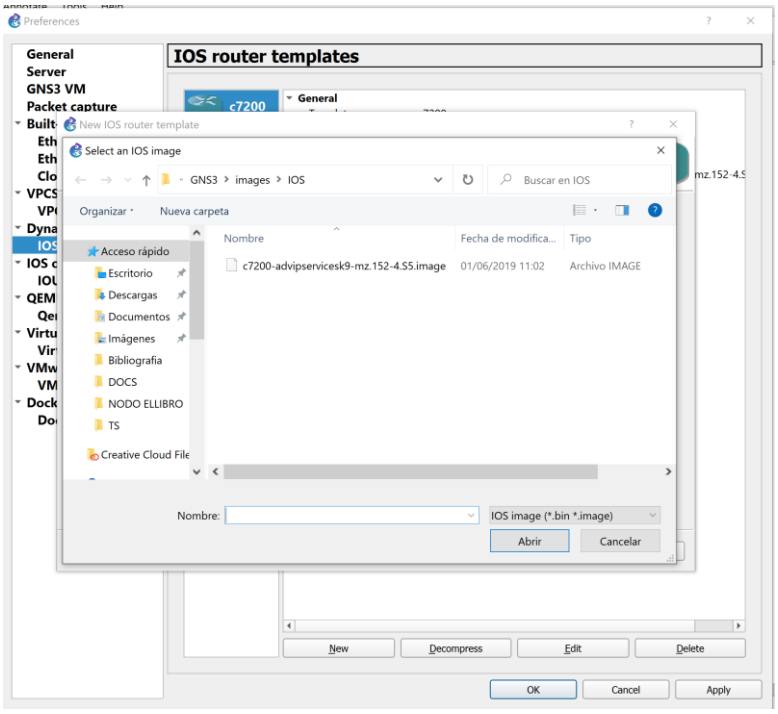


Figura 14: Selección del IOS del router Cisco.

Luego de realizar la selección de la imagen, aparecerá un mensaje que pide si se desea descomprimir la imagen IOS (Ver Figura 15).

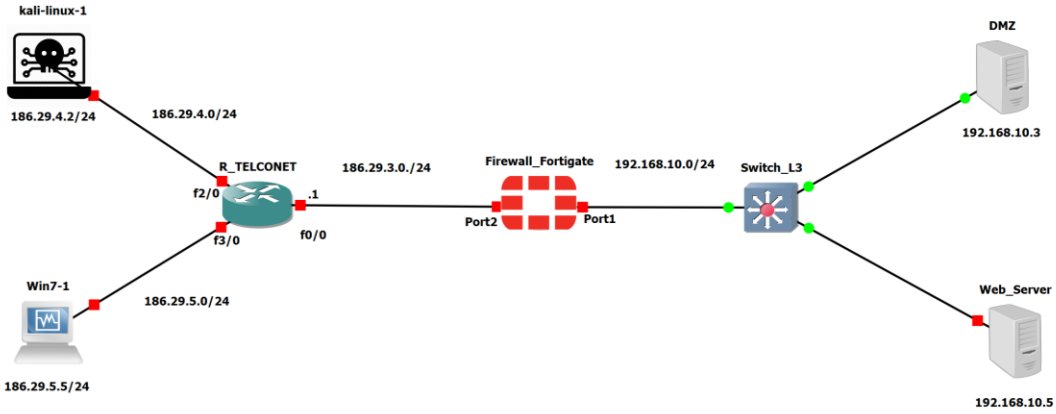
8. Tabla de IPs usadas en la simulación

Tabla 4: Hosts, Interfaces e Ips usadas en la simulación

IP	INTERFACE	HOST
186.29.3.1/24	F0/0	R_TELCONET
186.29.3.2/24	Port1	FortiGate_Firewall
186.29.4.1/24	F2/0	R_TELCONET
186.29.4.2/24	Eth0	Kali Linux
186.29.5.1/24	F3/0	R_TELCONET
186.29.5.2/24	Eth0	Usr_1
192.168.5.1/24	Port2	FortiGate_Firewall
192.168.5.2/24	Port1	FortiWeb_Firewall
192.168.10.1/24	Port2	FortiWeb_Firewall
192.168.10.3/24	Eth0	Servidor DMZ
192.168.10.5/24	Eth0	Servidor WEB

Para la simulación del escenario se usó las ips que se muestran en la tabla 4, se implantaron en base a la configuración mostrada en el esquema de la COAC “Riobamba” Ltda. Se modificaron y adaptaron para ejemplificar de la mejor manera posible en la simulación sin que haya alteraciones en la topología original.

9. Escenario de la COAC con su topología y un ataque externo



10. Configuración Firewall_Fortigate

En primer lugar, verificamos el estado de las interfaces del router Comando: su system interface ver figura 15.

```
FortiGate-VM64-KVM login: admin
Password:
Welcome !

FortiGate-VM64-KVM # sh system interface
config system interface
    edit "port1"
        set vdom "root"
        set mode dhcp
        set allowaccess ping https ssh http fgfm
        set type physical
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set type physical
        set snmp-index 2
    next
    edit "port3"
        set vdom "root"
        set type physical
        set snmp-index 3
    next
    edit "port4"
        set vdom "root"
        set type physical
        set snmp-index 4
    next
    edit "port5"
        set vdom "root"

FortiGate-VM64-KVM #
```

Figura 15: Estado de interfaces Fortigate al iniciar

Posteriormente configuramos las interfaces que van conectadas a la WAN y al switch de nuestro escenario, para el puerto1, ver figura 16.

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port1
FortiGate-VM64-KVM (port1) # set mode static
FortiGate-VM64-KVM (port1) # set ip 192.168.10.1/24
FortiGate-VM64-KVM (port1) # set allowaccess https http ping
FortiGate-VM64-KVM (port1) # end
FortiGate-VM64-KVM #
```

Figura 16: Comandos para configurar puerto 1

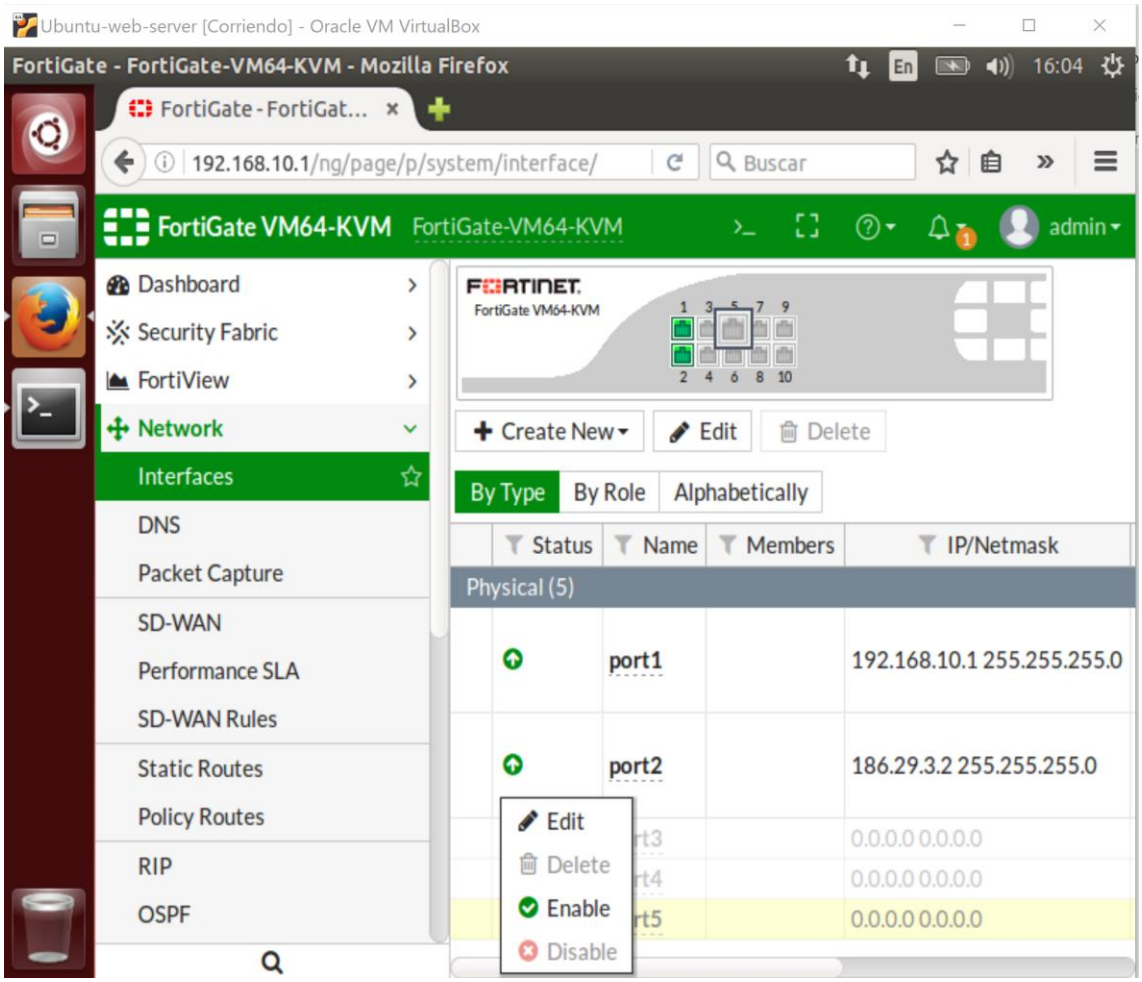
Para el puerto 2:

```
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 186.29.3.2/24
FortiGate-VM64-KVM (port2) # set allowaccess https http ping
FortiGate-VM64-KVM (port2) # end
FortiGate-VM64-KVM #
```

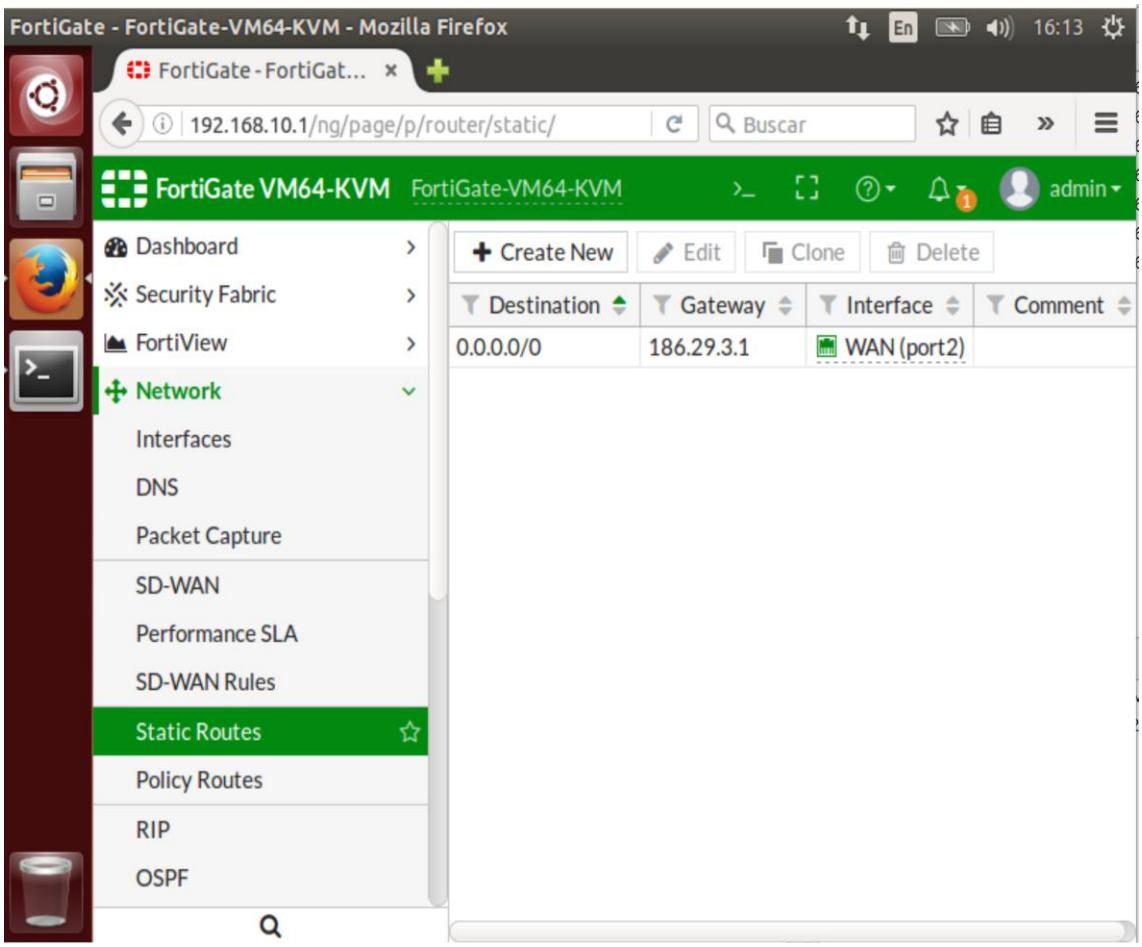
Figura 17: Comandos para configurar puerto 2

Se configuran los puertos con ip estáticas de acuerdo al escenario planteado una vez hecho esto tendremos acceso a configurar el router mediante la interfaz gráfica.

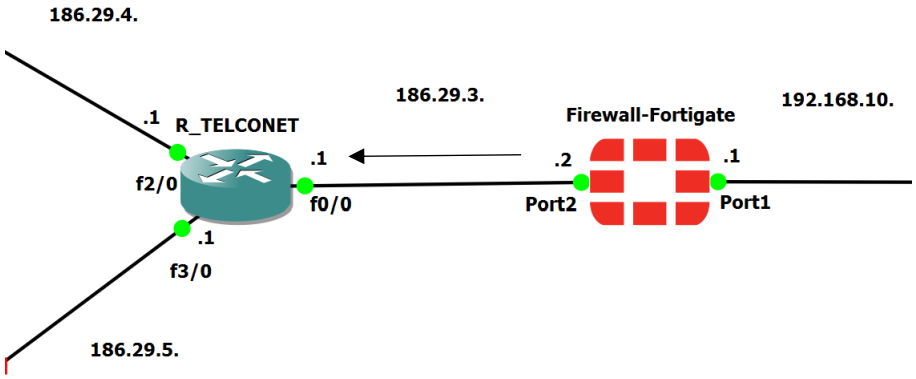
Dentro de la interfaz configuramos los puertos, debemos desactivar administrativamente los que no se usarán por seguridad:



Posteriormente configuramos una ruta estática para que reconozca la red que viene de la WAN en nuestro escenario:



Por cuestiones investigativas en la IP destino dejamos 0.0.0.0 para que puedan acceder todas las ips a nuestro servidor web en el Gateway configuramos el siguiente salto de red como se puede ver en el escenario planteado.



Como siguiente paso debemos configurar una política de IPv4 para que haya comunicación dentro del escenario planteado:

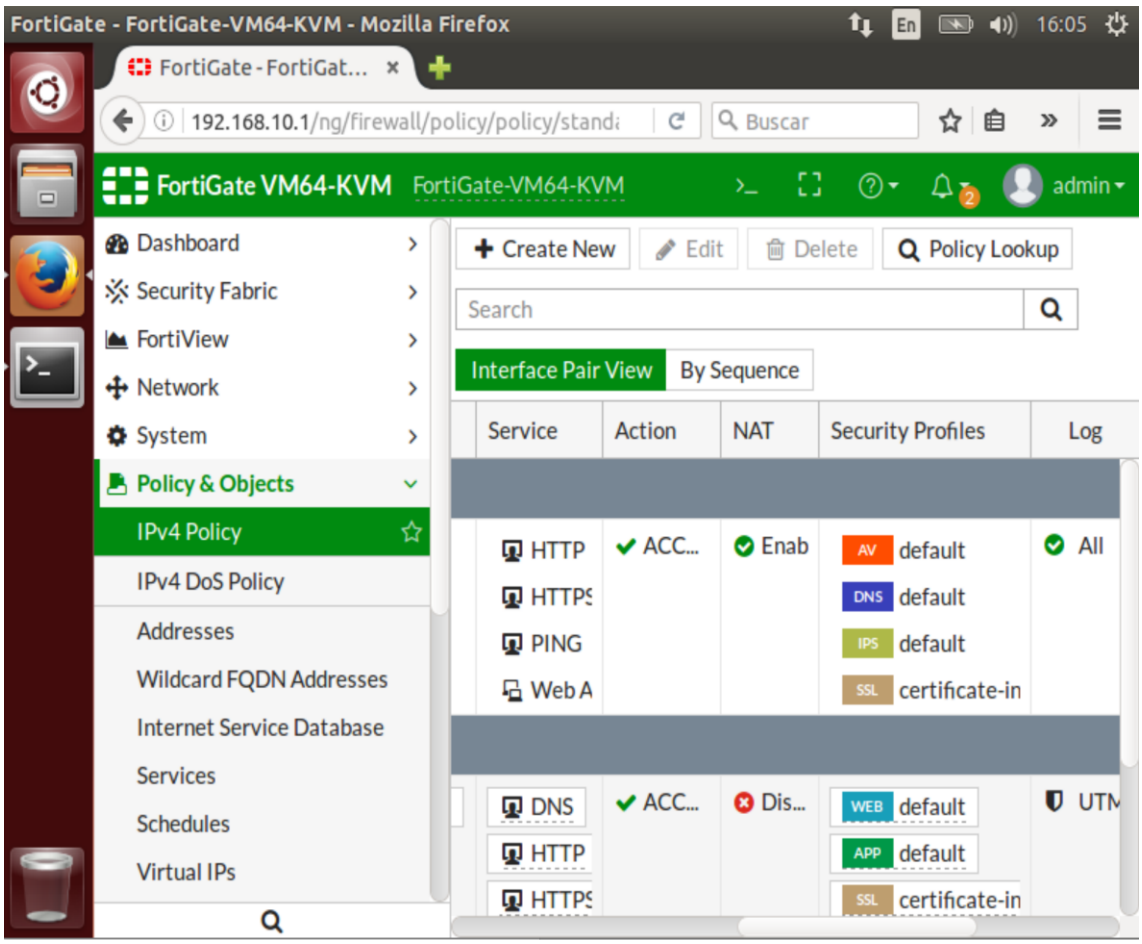


Figura 18: Políticas IPv4 para el Firewall Fortigate

Como se muestra en la figura 18, la configuración de las políticas para IPv4 es importante para que el router pueda comunicarse con las interfaces que entran a la LAN y sales a la WAN es decir a internet. Además, en este apartado aplicamos ciertos filtros para mayor seguridad en la red.

Una vez realizada esta configuración está listo el primer router del escenario virtual.

11. Configuración de Firewall_Fortiweb

En el siguiente paso se procede a configurar el router que funciona como firewall web

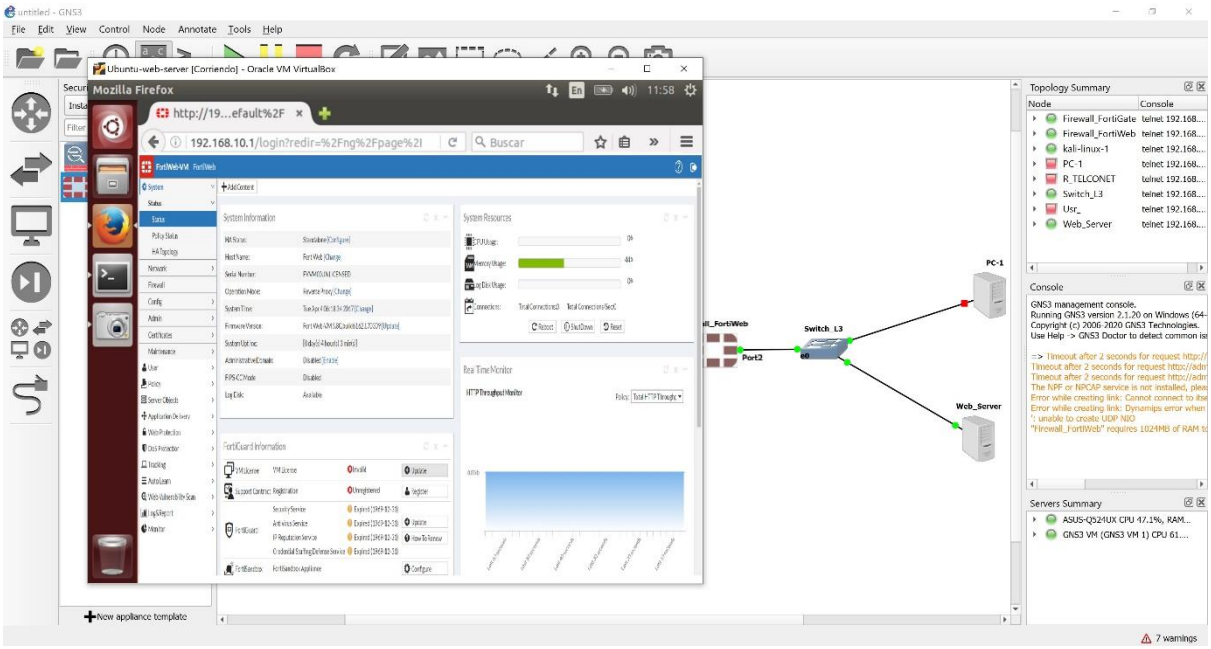


Figura 19: Pantalla de inicio firewall FortiWeb

La figura 19, muestra la pantalla principal del FortiWeb usado para la simulación este router tiene 5 interfaces Gigabit Ethernet, 1024 MB de RAM y 1 vCPU. Este firewall cuenta con herramientas de protección completa y especializada a todos los niveles para las aplicaciones y servicios Web. Algunas de las características de seguridad que ofrece son:

- Cross-Site Scripting (XSS).
- Cross-Site Request Forgery (CSRF).
- Insecure Cryptographic Storage.
- Failure to Restrict URL Access.

BUENAS PRACTICAS DE LOS USUARIOS