UNIVERSITAT POLITÈCNICA DE VALÈNCIA

_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería de Telecomunicación

Virtualización de redes con el emulador EVE-NG

Trabajo Fin de Grado

Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación

AUTOR/A: Climent Fornés, Jaime

Tutor/a: Romero Martínez, José Oscar

CURSO ACADÉMICO: 2022/2023

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN

Virtualización de redes con el emulador EVE-NG

Jaime Climent Fornés

Tutor: José Óscar Romero Martínez

Trabajo Fin de Grado presentado en la EscuelaTécnica Superior de Ingenieros de Telecomunicación de la Universitat Politècnica de València, para la obtención del Título de Graduado en Ingeniería de Tecnologías y Servicios deTelecomunicación.

Curso 2022-2023

Resumen

Hoy en día, vivimos en un mundo interconectado donde las redes juegan un papel fundamental en nuestra rutina diaria. La virtualización de redes es un concepto novedoso con grandes posibilidades en el campo de las comunicaciones y tecnologías de la información tanto en el ámbito laboral como en el educativo. En ambos ámbitos este tipo de herramienta se puede utilizar para simular distintos escenarios, evaluar diferentes soluciones y realizar cambios de configuración en un entorno experimental, aislado y seguro sin tener que correr el riesgo de afectar a la red física en producción.
En términos de eficiencia el hecho de tener la capacidad de poder prescindir de un laboratorio con hardware físico y simplemente tener servidores virtuales y dispositivos de red emulados, permite resolver problemas físicos de infraestructura y la reducción de costes sin tener que renunciar a las distintas funciones y aplicaciones que estos dispositivos ofrecen. Proporcionando accesibilidad, flexibilidad, eficiencia y optimización de recursos en la gestión de redes.
En este TFG se plasmará la gran cantidad de posibilidades que ofrece el entorno virtual de EVE-NG de forma gratuita, en el cual se diseñará una red empresarial funcional, se descargarán las imágenes de les dispositivos que nos interesen y se configurarán para cumplir las funciones necesarias.

Resum

Avui dia, vivim en un món interconnectat on les xarxes juguen un paper fonamental en la nostra rutina diària. La virtualització de xarxes és un concepte nou amb grans possibilitats en el camp de les comunicacions i tecnologies de la informació tant en l'àmbit laboral com en l'educatiu. En tots dos àmbits aquest tipus d'eina es pot utilitzar per a simular diferents escenaris, avaluar diferents solucions i fer canvis de configuració en un entorn experimental, aïllat i segur sense haver de córrer el risc d'afectar la xarxa física en producció.
En termes d'eficiència el fet de tenir la capacitat de poder prescindir d'un laboratori amb maquinari físic i simplement tenir servidors virtuals i dispositius de xarxa emulats, permet resoldre problemes físics d'infraestructura i la reducció de costos sense haver de renunciar a les diferents funcions i aplicacions que aquests dispositius ofereixen. Proporcionant accessibilitat, flexibilitat, eficiència i optimització de recursos en la gestió de xarxes.
En aquest TFG es plasmarà la gran quantitat de possibilitats que ofereix l'entorn virtual de EVE-NG de manera gratuïta, en el qual es dissenyarà una xarxa empresarial funcional, es descarregaran les imatges dels dispositius que ens interessin i es configuraran per a complir les funcions necessàries.

Abstract

Today, we live in an interconnected world where networks play a fundamental role in our daily routine. Network virtualisation is a new concept with great possibilities in the field of communications and information technology, both in the field of work and education. In both areas, this type of tool can be used to simulate different scenarios, evaluate different solutions and make configuration changes in an experimental, isolated and secure environment without having to run the risk of affecting the physical network in production.
In terms of efficiency, having the ability to dispense with a physical hardware lab and simply have virtual servers and network devices emulated allows for physical infrastructure problems to be solved and costs to be reduced without having to give up the various functions and applications that these devices offer. Providing accessibility, flexibility, efficiency and resource optimisation in network management.

This final degree project will show the great amount of possibilities offered by the virtual environment of EVE-NG for free, in which a functional enterprise network will be designed, the images of the devices we are interested in will be downloaded and configured to fulfil the necessary functions.

Índice

Índice de figuras

Capítulo 1. Introducción

La virtualización de redes es un tema clave en la industria de las telecomunicaciones y tecnologías de la información. Con la creciente demanda de redes más flexibles, escalables y eficientes, la virtualización de redes se ha convertido en una tecnología esencial para mejorar la eficiencia y el rendimiento de las redes de comunicación., convirtiéndose en una de las tendencias tecnológicas que está marcando el futuro empresarial.

La virtualización de redes hace referencia a la desvinculación de los recursos de red en forma de hardware como podría ser un firewall o un switch, es decir, virtualiza las funciones de red y elimina los dispositivos físicos, los operadores de red pueden mover, cambiar o agregar funciones de red en un proceso simplificado utilizando el software.

Para probar y validar soluciones de virtualización de redes, se requiere de herramientas que permitan simular y modelar la red. Los simuladores de redes son herramientas de software que permiten la simulación de diferentes topologías de red y escenarios de uso para poder probar nuevas soluciones de virtualización de redes.

Los simuladores de red tienen varias ventajas. En primer lugar, permiten la creación de una red virtual que se puede manipular y cambiar sin tener que realizar cambios en la infraestructura física. Esto significa que se pueden probar diferentes configuraciones de red y escenarios de uso sin tener que hacer cambios en la red física, lo que reduce el riesgo de interrupción de servicio.

Algunas de estas ventajas pueden ser:

Flexibilidad: Los simuladores de red permiten probar diferentes topologías de red y configuraciones de red. Esto significa que se pueden probar diferentes configuraciones y escenarios de uso sin tener que hacer cambios en la red física, lo que reduce el tiempo y el costo de implementación.

Reducción de costos: Los simuladores de red permiten probar diferentes escenarios de red sin tener que invertir en hardware y equipos físicos.

Reproducibilidad: Los simuladores de red permiten reproducir diferentes escenarios de red y resultados, lo que ayuda a las empresas a identificar y solucionar problemas de red de forma más eficiente. También ayuda a las empresas a documentar y compartir sus resultados de prueba con otros miembros del equipo o con terceros interesados como podrían ser clientes.

Análisis de rendimiento: Los simuladores de red permiten medir y analizar el rendimiento de la red en diferentes situaciones y escenarios de uso. Esto ayuda a las empresas a identificar posibles puntos débiles en la red, lo que puede ser especialmente útil para mejorar el rendimiento y la calidad de servicio de la red.

Además, los simuladores de red también son útiles para probar soluciones de red en diferentes entornos de red, lo que permite una mejor comprensión de las capacidades y limitaciones de la red. También permiten la identificación de posibles problemas de configuración y diseño antes

de que se implementen en la red real, lo que reduce el tiempo y el costo de resolución de problemas.

De acuerdo con resultados de una investigación de SpiceWorks, presentada en 2020, la adopción de la virtualización se ve principalmente en los servidores, pero su uso va más allá y se espera que en este 2022 haya un aumento de dos dígitos en la implementación de escritorio, aplicaciones, almacenamiento, datos y redes.

- Más flexibilidad con la configuración de la red **(51%)**.
- Capacidades de gestión mejoradas **(48%)**.
- Capacidad para reconfigurar redes sin cambios físicos **(46%)**.
- Capacidades de seguridad mejoradas **(45%)**.
- Más control sobre la segmentación de la red **(39%)**.
- Ahorro de costes **(33%)**, al reducir la infraestructura física y los gastos asociados al consumo energético de varios servidores, mantenimiento y actualización.
- Beneficios de la automatización (33%), que indirectamente impulsan la productividad y brindan al equipo TI más tiempo para la realización de otras tareas de alto impacto para el desarrollo tecnológico de la empresa.

En conclusión, la virtualización de redes se ha convertido en una tecnología fundamental para mejorar la eficiencia y el rendimiento de las redes de comunicación. Además, la adopción de la virtualización se espera que siga aumentando debido a sus ventajas que ofrece, como la flexibilidad, las capacidades de gestión mejoradas, el ahorro de costos y los beneficios de la automatización.

Capítulo 2. EVE-NG

EVE-NG es una herramienta de simulación de redes que permite la creación de entornos virtuales de red de manera rápida y sencilla. Es una solución de virtualización de red de muy completa que permite crear, configurar y gestionar topologías de red complejas en un entorno virtualizado.

EVE-NG es una plataforma abierta y gratuita, que brinda herramientas para usar en dispositivos virtuales e interconectarlos con otros dispositivos virtuales o físicos y se ejecuta en cualquier plataforma de virtualización. Proporciona una solución de virtualización de red completa que combina tecnologías como VirtualBox, VMware, Docker y KVM para permitir a los usuarios crear y gestionar entornos de red virtuales.

Se puede usar para recrear redes corporativas y probar cambios antes de ponerlos en producción, se puede recrear escenarios y mapas conceptuales para los clientes, hasta el punto el punto de recrear escenarios de redes empresariales y realizar pruebas sin riesgo para encontrar y solucionar los problemas de dicha red.

Además, EVE-NG ofrece una gran cantidad de características y funcionalidades que hacen que sea fácil de usar y personalizar para cualquier necesidad determinada. Algunas de estas características son:

- Múltiples protocolos y tecnologías de red como IPv4, IPv6, OSPF, MPLS, VXLAN, etc.
- Integración con proveedores de servicios de nube pública como AWS, Google Cloud y Azure.
- Interfaz de usuario HTML5 completa.
- Interfaz web intuitiva que facilita la configuración y administración de los entornos de red virtuales para los usuarios.
- Es una aplicación multiplataforma.

El emulador EVE-NG es una herramienta muy interesante para la virtualización de redes. Ofrece una solución de virtualización de red completa con muchas posibilidades que permite a los usuarios crear, configurar y gestionar topologías de red complejas en un entorno virtualizado de manera rápida y sencilla.

A todo esto, se le añade la gran accesibilidad que tiene que pese a ser nativo de Linux, mediante una máquina virtual como VMware es accesible para cualquier sistema operativo, que con muy pocos recursos ofrece una gran cantidad de posibilidades que estudiaremos y veremos más adelante.

Capítulo 3. Objetivos

En este trabajo de fin de grado, se estudiará las posibilidades y la implementación del emulador EVE-NG, una herramienta de simulación de redes que permite la creación y la ejecución de topologías de red complejas en un entorno virtualizado.
La máquina virtual que voy a utilizar durante todo el proyecto será VMware, que es una de las plataformas más populares ya que permite la creación y ejecución en una gran variedad de sistemas operativos y aplicaciones en un entorno seguro y aislado.

El objetivo principal de este proyecto es poder mostrar la gran cantidad de posibilidades que ofrece EVE-NG con el cual podré diseñar, configurar y probar soluciones de redes en un ambiente seguro y controlado.
De esta forma, mediante el uso de estas tecnologías voy a diseñar, configurar y poner en funcionamiento una red empresarial virtualizada. Con el objetivo principal de demostrar la capacidad de virtualización de redes para crear una solución de red empresarial funcional a coste 0. Lo que puede ser interesante tanto para empresas pequeñas con un presupuesto bajo, como para docencia y también incluso para empleados que se dediquen al departamento de redes y necesiten replicar configuraciones de clientes para encontrar y resolver problemas en las redes de los clientes sin generar ningún tipo de corte con pruebas para solucionar el problema.

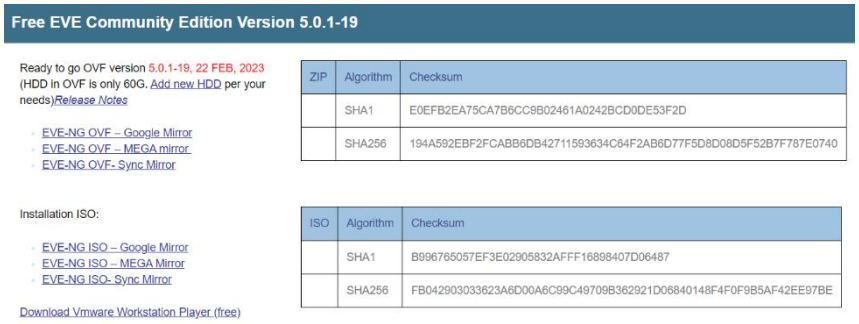
Durante la realización de este proyecto voy a mostrar cómo sin ningún coste, es decir, sin tener que invertir nada ni en licencias, ni en servidores para tener más capacidad, ni tampoco en hardware físico para montar un laboratorio de pruebas. Podemos tener una red empresarial en la cual tendremos distintos dispositivos virtuales como firewalls, switches, PCs, etc.

Para montar la red, se utilizarán diferentes dispositivos como los que he mencionado anteriormente, que se configurarán y se conectarán entre sí para conseguir que la red sea funcional. También mostraré de forma esquematizada la red completa para una mejor comprensión y detallaré la selección, la configuración y el uso de cada dispositivo teniendo en cuenta el rendimiento de cada uno con su consumo de recursos, de forma que obtendremos dispositivos balanceados en cuanto a consumo y rendimiento y más recursos disponibles para poder realizar el máximo de pruebas posibles, teniendo en cuenta el objetivo principal que es mostrar la gran cantidad de opciones que ofrece EVE-NG.

Capítulo 4. Desarrollo

4.1 Instalación EVE-NG y máquina virtual VMware

En este apartado únicamente dejaré constancia de los enlaces de descarga y algunas capturas orientativas de cómo realizar la instalación.
En cuanto a la instalación de la máquina virtual elegiremos la opción para Windows, en mi caso tengo la versión 16, *VMware Workstation 16 Player*. La descarga se realizará directamente desde la página principal en el apartado de descargas.



Free EVE Community Edition Version 5.0.1-19

Ready to go OVF version 5.0.1-19, 22 FEB, 2023 (HDD in OVF is only 60G. Add new HDD per your needs)*Release Notes*

- EVE-NG OVF – Google Mirror
- EVE-NG OVF – MEGA mirror
- EVE-NG OVF- Sync Mirror

ZIP	Algorithm	Checksum
	SHA1	E0EFB2EA75CA7B6CC9B02461A0242BCD0DE53F2D
	SHA256	194A592EBF2FCABB6DB42711593634C64F2AB6D77F5D8D08D5F52B7F787E0740

Installation ISO:

- EVE-NG ISO – Google Mirror
- EVE-NG ISO – MEGA Mirror
- EVE-NG ISO- Sync Mirror

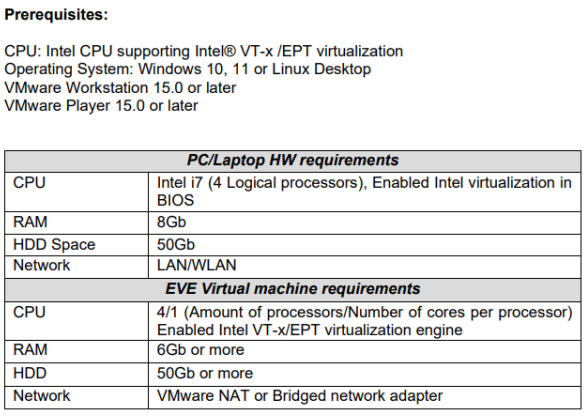
Download Vmware Workstation Player (free)

ISO	Algorithm	Checksum
	SHA1	B996765057EF3E02905832AFFF16898407D06487
	SHA256	FB042903033623A6D00A6C99C49709B362921D06840148F4F0F9B5AF42EE97BE

Figura 1: Versión EVE-NG

Una vez dentro del enlace escogeremos la versión para la comunidad que es la gratuita y tenemos dos opciones la ISO y la OVF. Escogeremos la opción OVF utilizando los servidores de Google que es la que está lista para ser implementada.

Dentro de la propia página de EVE-NG, tenemos un *Cookbook* en el cual aparece toda la información sobre el uso y requisitos del propio entorno de EVE-NG. En la primera parte podremos ver los requisitos mínimos que necesitamos para poder ejecutar el emulador, son los siguientes:



Prerequisites:

CPU: Intel CPU supporting Intel® VT-x /EPT virtualization
Operating System: Windows 10, 11 or Linux Desktop
VMware Workstation 15.0 or later
VMware Player 15.0 or later

PC/Laptop HW requirements	
CPU	Intel i7 (4 Logical processors), Enabled Intel virtualization in BIOS
RAM	8Gb
HDD Space	50Gb
Network	LAN/WLAN
EVE Virtual machine requirements	
CPU	4/1 (Amount of processors/Number of cores per processor) Enabled Intel VT-x/EPT virtualization engine
RAM	6Gb or more
HDD	50Gb or more
Network	VMware NAT or Bridged network adapter

Figura 2: Requisitos básicos

Por otra parte, en el mismo documento nos especifica cuales son las características recomendadas que son las siguientes:

Prerequisites:

CPU: Intel CPU supporting Intel® VT-x /EPT virtualization
Operation System: Windows 10, 11 or Linux Desktop
VMware Workstation 15.0 or later
VW Ware Player 15.0 or later

PC/Laptop HW requirements	
CPU	Intel i7 (16 Logical processors), Enabled Intel virtualization in BIOS
RAM	32Gb
HDD Space	200Gb
Network	LAN/WLAN
EVE Virtual machine requirements	
CPU	16/1 (Amount of processors/Number of cores per processor) Enabled Intel VT-x/EPT virtualization engine
RAM	24Gb or more
HDD	200Gb or more
Network	VMware NAT or Bridged network adapter

Figura 3: Requisitos recomendados

En este caso el trabajo se realiza con un portátil con 16 Gb de RAM. La diferencia más notable en cuanto a capacidad de hardware viene dada en función de la cantidad de funciones y dispositivos se vayan a implementar. Todo esto es necesario tenerlo en cuenta porque durante la instalación se tiene que definir la cantidad de CPU y RAM se va a asignar.

En primer lugar, una vez instalada la máquina virtual hay que importar el EVE-NG que hemos descargado.

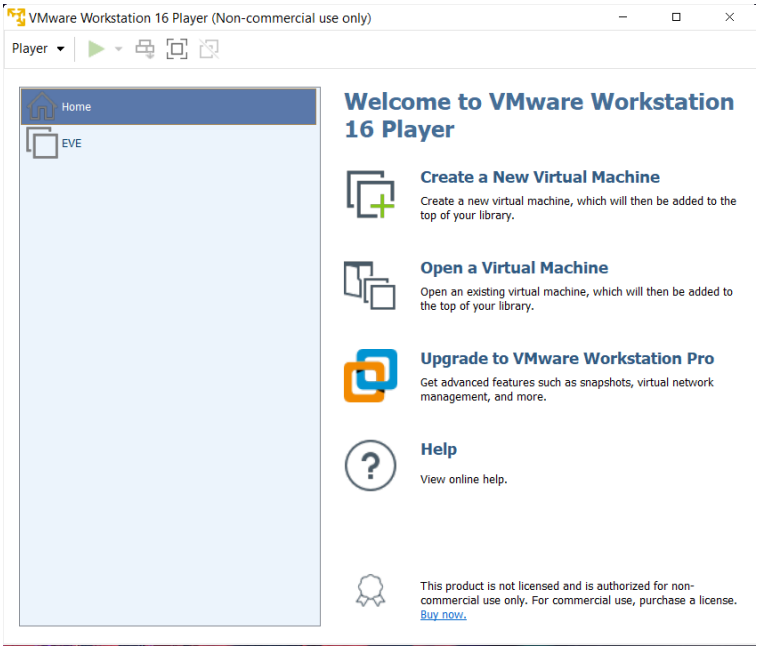


Figura 4: Interfaz de inicio VMware

A continuación, podremos personalizar en el apartado de configuración la configuración que más nos convenga, en mi caso he destinado 10 Gb de RAM y 4 procesadores.

También habrá que hacer una configuración de la red haciendo que la máquina virtual se conecte al segmento de red real en el cual estoy trabajando, por eso en el apartado del adaptador de red seleccionaré la opción *bridged.* Además también tengo que especificar dentro la configuración de adaptadores si estoy conectado a la red por cable o de forma inalámbrica.

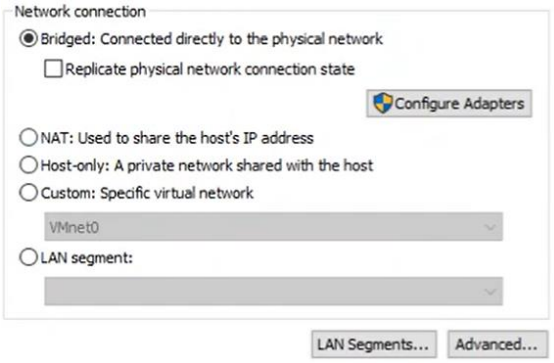


Figura 5: Configuración de red VMware

Una vez terminada esa parte de configuración inicial de la máquina virtual, ya podemos acceder a EVE-NG mediante las credenciales root y eve. Estas son las que aparecen por defecto, una vez introducidas las credenciales por defecto nos dará la opción de cambiar algunos parámetros como la contraseña, el hostname y la dirección IP.

En cuanto a la dirección IP es importante cambiar la selección a estática para que cada vez que queramos acceder no se renueve la dirección IP y cada vez que encendamos la máquina virtual aparezca con una dirección IP distinta.

Por último, configuraremos el direccionamiento IP de nuestra red, indicando dirección IP, máscara y puerta de enlace. También habrá que especificar los DNS primarios y secundarios.

Finalmente nos aparecerá de la siguiente forma y ya estará listo para usarse.

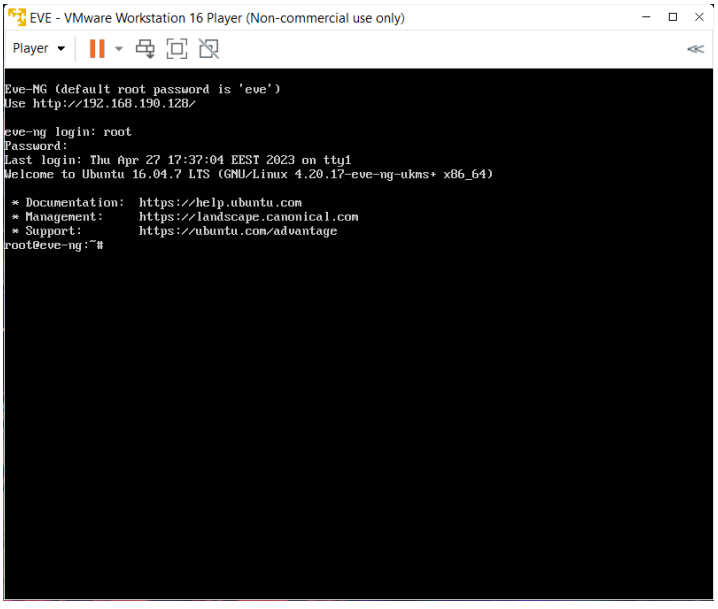


Figura 6: Inicio de sesión en VMware

Por otra parte, también es necesaria la descarga de un paquete de cliente para Windows que instalará todo lo necesario para ejecutar la gran mayoría de aplicaciones.

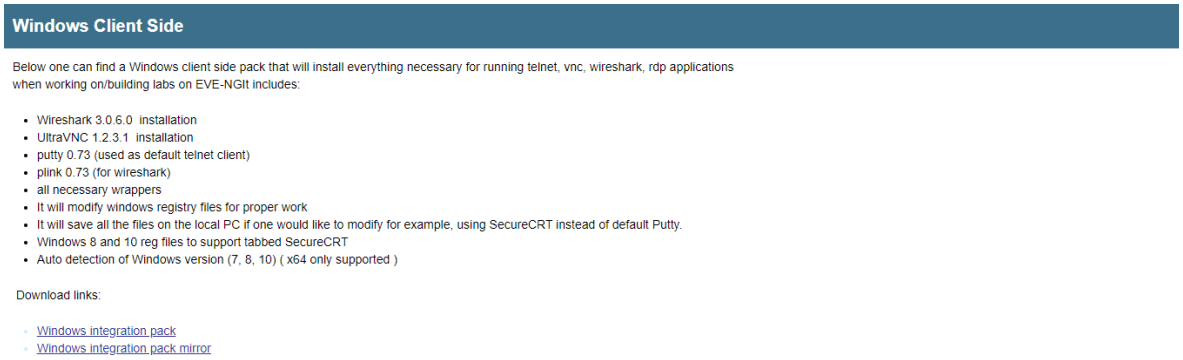


Figura 7: Paquete de cliente para Windows

De los dos enlaces de descarga elegiremos el enlace de la versión normal del paquete de cliente.

4.2 Putty

Putty es una herramienta que actúa como cliente de conexiones seguras a través de varios protocolos de red, pero principalmente utiliza el protocolo Telnet. Este software se utiliza principalmente como cliente para establecer conexiones seguras de acceso remoto a través del protocolo de administración remota SSH.

En cuanto al proceso de instalación es bastante sencillo. Desde la propia página web de Putty entramos al apartado de descargas y descargamos el paquete que nos convenga, en mi caso una máquina windows de 64 bits.

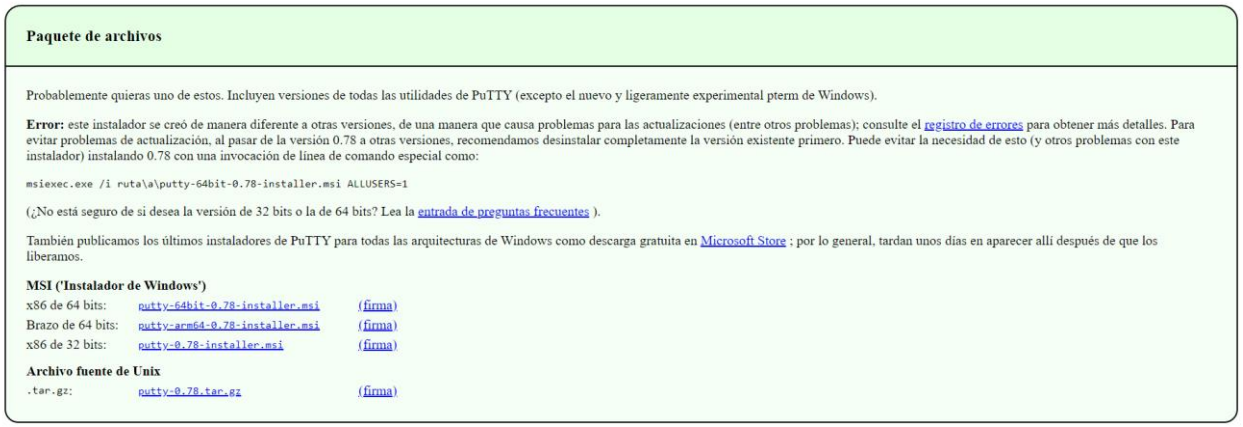


Figura 8: Instalación Putty

Una vez descargado el paquete pasaremos al proceso de instalación en el cual aceptaremos todos los valores por defecto que vayan apareciendo durante la instalación.

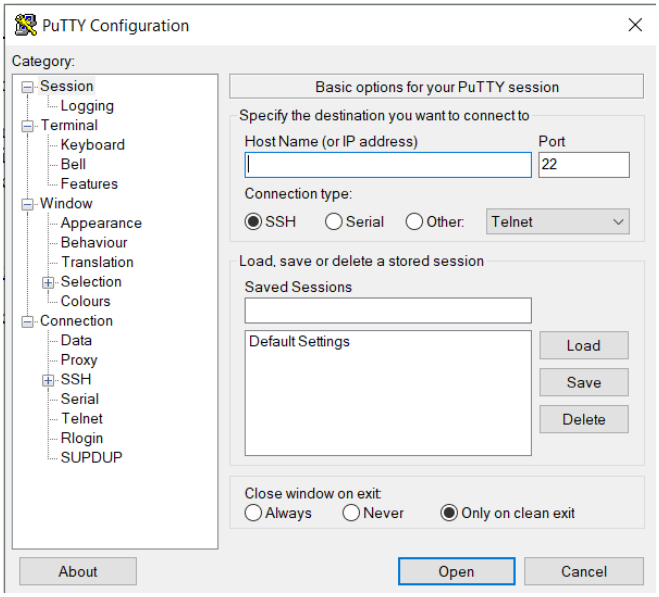


Figura 9: Interfaz de inicio Putty

Una vez realizada la instalación finalmente nos debería aparecer de esta forma si todo ha ido correctamente.

En cuanto a la configuración no será necesario hacer nada más. La conexión SSH con las distintas máquinas se realizará directamente gracias al paquete de cliente para Windows que hemos descargado anteriormente.

Putty es una herramienta de software que se utiliza para acceder a dispositivos de red a través de SSH y telnet. Dentro del entorno virtual de EVE-NG, la herramienta Putty nos sirve para poder acceder a los dispositivos virtuales que se ejecutan en EVE-NG y establecer una sesión SSH con la dirección IP asignada al dispositivo.

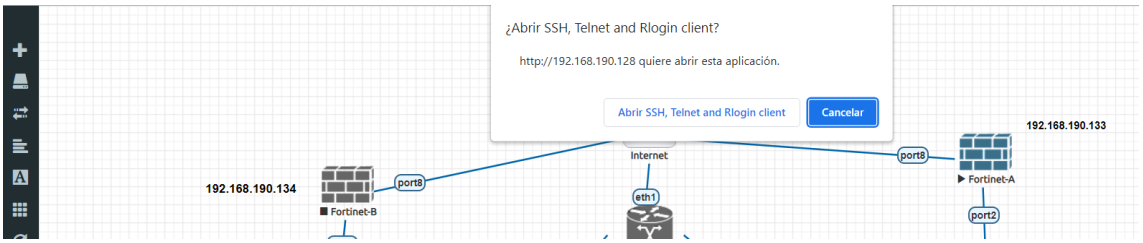


Figura 10: Ejecución dispositivo de red virtual

En esta imagen muestro cómo se accede al firewall sin tener aún IP para acceder a la interfaz mediante una sesión SSH usando la herramienta Putty.

4.3 Imágenes en EVE-NG

En este punto voy a mostrar cómo añadir imágenes al entorno virtual de EVE-NG. Para realizar este proceso será necesario descargar la aplicación *WinSCP*, esta aplicación nos sirve para transferir archivos de forma segura entre un cliente y un servidor remoto, en mi caso desde la máquina Windows a la máquina virtual de VMware donde tenemos el EVE-NG, utilizando los protocolos SFTP, FTP y la versión segura de FTP que es sobre SSL/TLS.

Dentro de la propia web de EVE-NG, en la parte de *documentation* hay una parte de *supported images* podemos ver una gran lista de imágenes que soporta. Además, la web también incluye dentro de la parte de *documentation*, *how to create images* cómo agregar las imágenes virtuales al emulador.

A continuación, voy a mostrar el proceso de agregación de una imagen hasta el punto de poder utilizarla dentro del entorno del EVE-NG.

Siguiendo los pasos que nos proporciona la propia web en la parte de *how to create images* buscamos la imagen que nos interese agregar en este caso será la de una Mikrotik. En primer lugar, vamos a la web de Mikrotik accedemos a la parte de *software* y en la parte de *download* buscamos algún apartado relacionado con imágenes virtuales en el caso de Mikrotik estas imágenes aparecen en la parte de *cloud hosted router*.

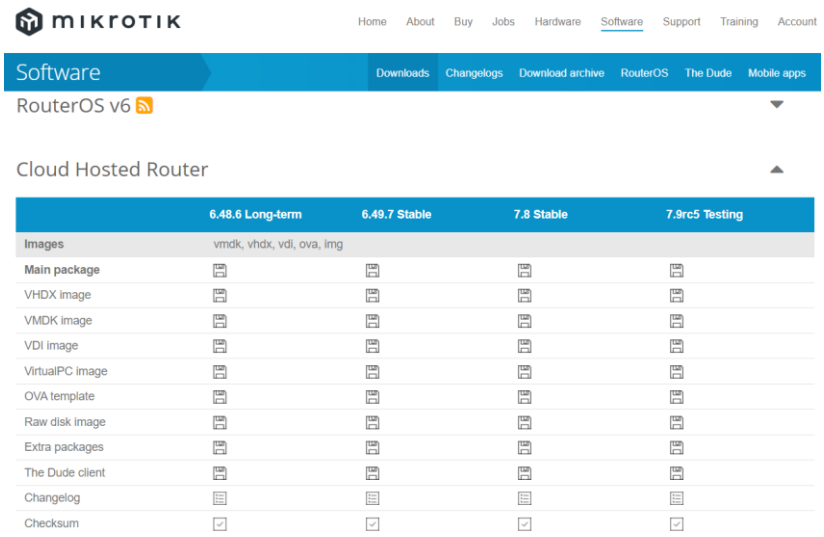


Figura 11: Descarga imagen virtual

En esta imagen podemos observar que existen varias versiones, nosotros descargaremos cualquiera de las que vengan especificadas en la página de EVE-NG. Observando la imagen anterior vemos que hay múltiples opciones de descarga. Elegiremos la opción *Raw disk image*, esta opción es una descarga de la imagen de disco exacta creada a partir de una copia bit a bit de un disco físico completo. El motivo por el cual descargamos la imagen con este formato es que el formato raw es el formato en el que trabaja EVE-NG, es decir, este formato es un requisito del software.

Una vez descargado el archivo comprimido habrá que extraer el archivo y abrir el EVE-NG desde la máquina virtual VMware y abrir también el WinSCP. Una vez abiertas las dos aplicaciones iniciaremos sesión en la máquina virtual para poder utilizar el EVE-NG y por otro lado iniciaremos sesión en WinSCP mediante la dirección IP del EVE-NG, el protocolo SFTP, el puerto 22 y las credenciales.

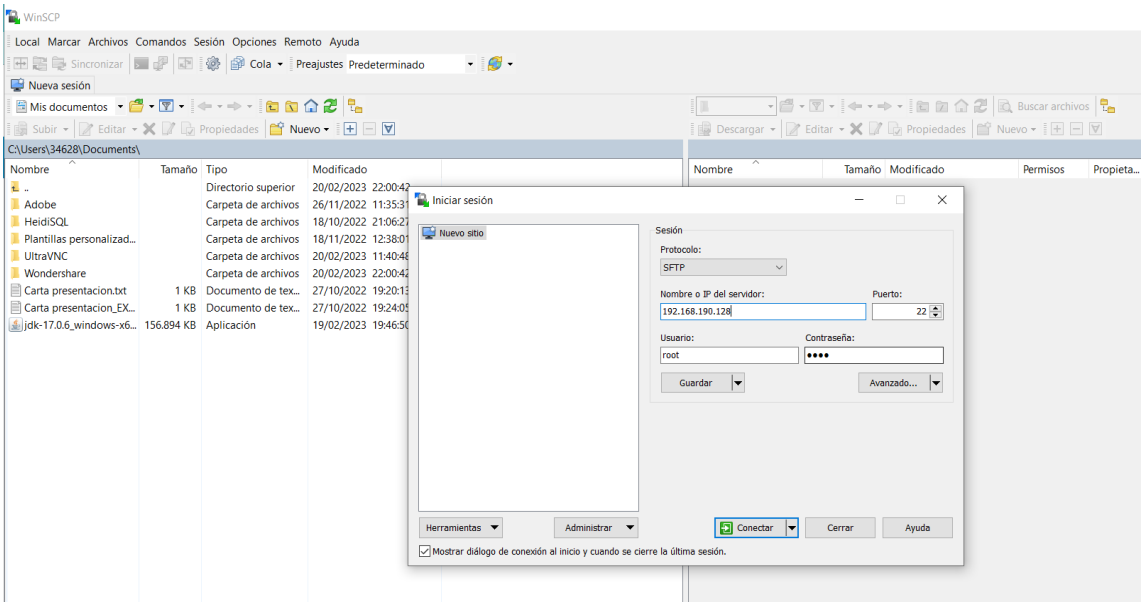


Figura 12: Interfaz de inicio WinSCP

Una vez iniciada la sesión tendremos una interfaz que está distribuida con el usuario local en la izquierda y el remoto en la derecha. En este momento habrá que dirigirse a la página web del EVE-NG en el apartado de *how to create images*, buscamos Mikrotik y seguimos los pasos.

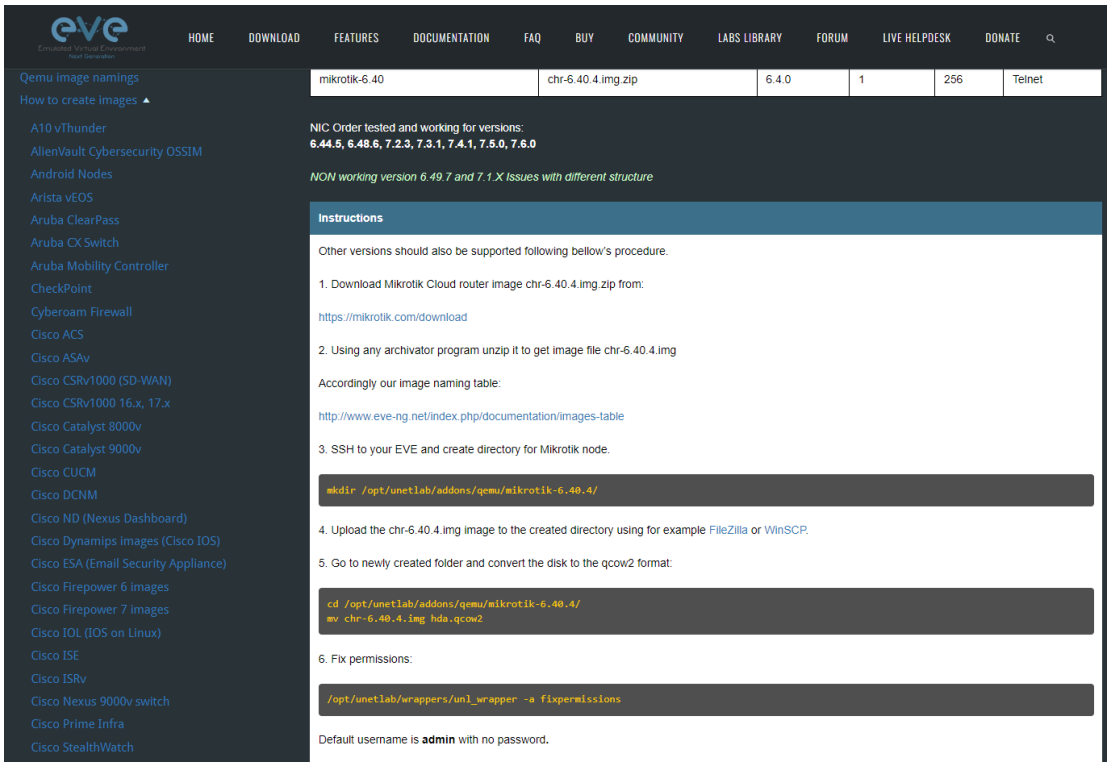


Figura 13: Añadir imágenes en EVE-NG

En este momento con el WinSCP abierto, el EVE-NG abierto y la imagen descargada, estaríamos en el paso 5 de la imagen anterior, entonces dentro del WinSCP en la parte del usuario remoto simplemente accedemos a la carpeta indicada, creamos una carpeta tal y como nos indica la guía de EVE-NG, de no hacerlo de esa forma no aparecerá luego en el emulador y por último copiamos la imagen descargada y extraída desde la parte local de la izquierda a la parte del usuario remoto en la parte derecha.

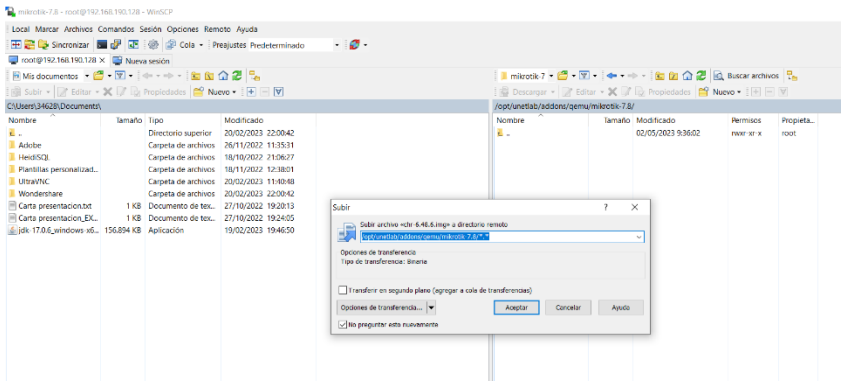


Figura 14: Conexión WinSCP

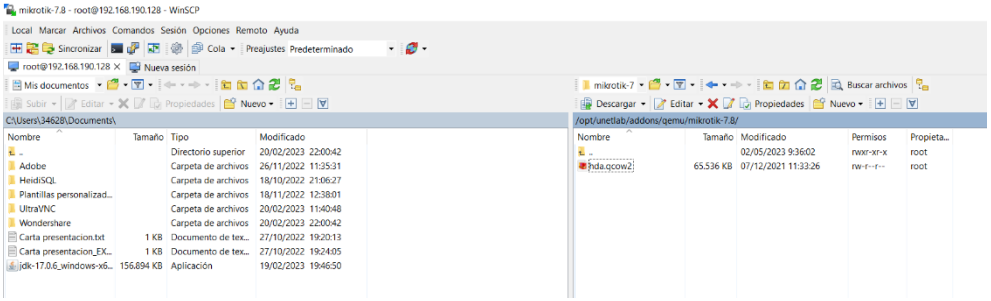


Figura 15: Añadir imagen al entorno virtual

Una vez hayamos pasado la imagen del local al remoto a la nueva carpeta creada, nombrada y situada correctamente, lo último que habría que hacer sería poner el nombre que nos indica que es el de *hda.qcow2.*

Finalmente habría que realizar el paso 6 de corregir permisos, este paso es simplemente ejecutar el comando tal y como aparece en la máquina virtual y ya podríamos ver la imagen en nuestro entorno virtual con el nombre que le hemos dado a nuestra carpeta.

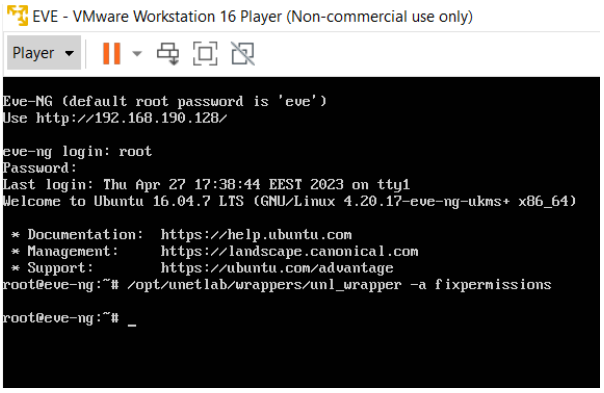


Figura 16: Corrección de permisos

4.4 Dispositivos

A continuación, comentaré todos los dispositivos de los cuales se compone la red virtual que voy a implementar, pero únicamente plasmaré qué dispositivos voy a utilizar especificando la versión y la cantidad de recursos que deberá consumir cada uno de forma optimizada para consumir los recursos mínimos sin que afecte al rendimiento.

4.4.0 Proveedor

El objeto que muestro a la derecha es el objeto que vemos en el escritorio dentro del entrono virtualizado de EVE-NG y se crea de la siguiente manera.

Seleccionamos la opción de elegir un objeto, en este momento nos saldrán distintas opciones de las cuales elegiremos el objeto de tipo Network y nos aparecerá la imagen que aparece en la derecha en la cual hay que especificar el tipo de Network. Tal y como vemos en la imagen elegimos la opción de Management(Cloud0), finalmente guardamos la configuración y ya nos aparecería el objeto como lo he presentado al principio.

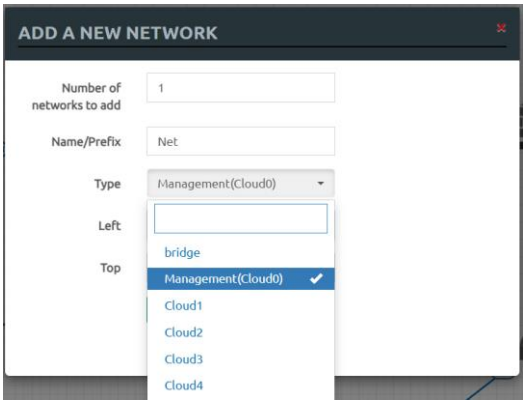


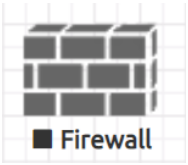
Figura 17: Añadir proveedor

Cuando creamos un objeto y seleccionamos la configuración Management(Cloud0) estamos creando una instancia virtual de la herramienta de administración y monitorización de red que se ejecutará dentro del entorno de EVE-NG. Cuando se crea dicha instancia, por defecto Management(Cloud0) asignará dos direcciones IP: una dirección IP privada para la comunicación con los distintos dispositivos de la red virtual dentro del entorno de EVE-NG y otra dirección IP pública para el acceso desde fuera del entorno de EVE-NG como podría ser mi red local.

El objeto que vemos con forma de nube dentro de nuestro entorno virtualizado tiene varias funciones importantes, pero la principal a destacar es la función de servidor DHCP para asignar direcciones IP automáticamente a otros dispositivos virtuales dentro de mi topología de red. Motivo por el cual lo he presentado como proveedor.

Por otro lado, también es importante entender como con este objeto proporcionamos salida a internet. La instancia Management(Cloud0) accede a internet a través de la red física a la que está conectada la interfaz de red de EVE-NG, accede a la red física porque durante la instalación de la máquina virtual tal y como aparece en el apartado “4.1 Instalación EVE-NG y máquina virtual VMware” configuramos la opción de adaptador de red en modo “bridge”.
Con esta configuración conseguimos que, si nuestra máquina está conectado a internet con una conexión WIFI o Ethernet, desde EVE-NG se puede conectar directamente a la red física del host y acceder a internet a través de la misma conexión.

4.4.1 Firewall



Para este dispositivo la imagen que vamos a cargar es la imagen de un firewall Fortinet FortiGate v6.4.7. Las imágenes se cargan todas de la misma forma siguiendo los pasos que se indican en la propia web de EVE-NG, de la misma forma que he mostrado antes con la Mikrotik.

Una vez tenemos la imagen cargada y lista para usar, hay que seleccionar algunos parámetros básicos de la configuración tal y como vemos en la siguiente imagen.

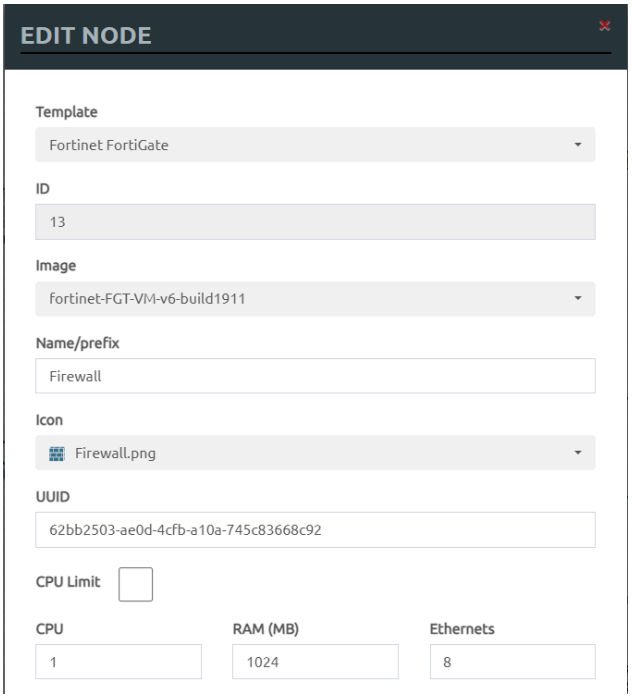


Figura 18: Configuración básica Firewall

Estos parámetros que vemos en esta imagen son los que he usado en ambos firewalls, me gustaría destacar los parámetros que he cambiado con respecto a los que se mantienen por defecto.
En primer lugar, habrá que seleccionar la versión de la imagen que hayamos bajado. A continuación, seleccionamos el nombre, en mi caso he puesto *Fortinet-A*, porque es la configuración del firewall que va a representar a una de las dos sedes, concretamente a la sede A situada a la derecha. Por último, hay que delimitar la cantidad de recursos (RAM) que va a consumir el firewall, en este caso será un consumo de 1024 MB de RAM, de haberle proporcionado 512 MB de RAM sí que notaríamos un funcionamiento muy lento de la máquina. En cambio, la diferencia de rendimiento de la máquina entre haber proporcionado 2048 MB y 1024 MB es prácticamente inapreciable.

Una vez vista la configuración ya podremos encender el firewall, al que por el momento únicamente podremos acceder por SSH, mediante la herramienta Putty tal y como hemos visto en el punto 4.2 donde hablo de la instalación y el uso de dicha herramienta.

Llegados a este punto aún no recibimos IP de nuestro proveedor. A continuación, veremos el proceso que hay que seguir para obtener una IP de nuestro proveedor.
En primer lugar, enlazamos el proveedor con nuestro firewall tal y como vemos en la imagen seleccionando el puerto al que queremos que se conecte, en este caso el puerto 8. A continuación una vez encendamos la máquina nos conectaremos por SSH al firewall e iniciamos sesión. La primera vez que accedemos a la máquina, nos pedirá que accedamos con unas credenciales por defecto, en este caso el nombre de usuario predeterminado es "admin" y la contraseña está en blanco.

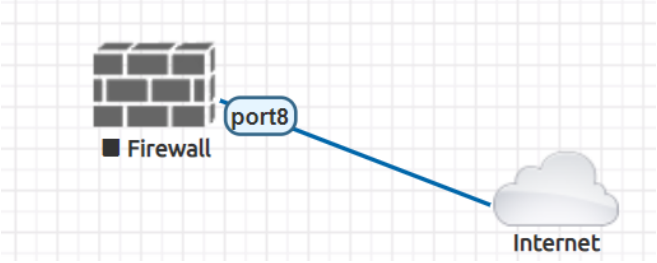


Figura 19: Conexión de puertos

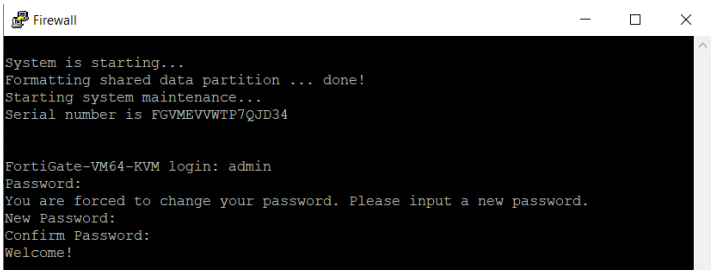


Figura 21: Inicio de sesión

Una vez hemos configurado nuestras propias credenciales de acceso, habrá que editar mediante líneas de comando el puerto que hemos seleccionado para poder recibir una IP por parte de nuestro proveedor.

 # Config system interface

Para poder configurar y administrar las interfaces de red del dispositivo.

 # show

Después de introducir el comando anterior, este comando nos muestra la configuración actual de las interfaces de red en el sistema.

En este momento aparecerá información sobre la configuración de cada interfaz de forma detallada, fijándonos en el puerto 8 que es el que tenemos conectado a nuestro proveedor vemos que no tiene activo el modo DHCP ni tampoco el HTTP. El modo DHCP es necesario para poder recibir una IP. Por otra parte, necesitamos permitir las conexiones y el tráfico por HTTP para poder acceder al firewall por internet mediante la IP que nos asigne nuestro proveedor.

```
    edit "port8"
        set vdom "root"
        set type physical
        set snmp-index 8
    next
```

Figura 22: Configuración por defecto del puerto 8

Una vez comprobada la configuración del puerto que nos interesa lo editaremos con los siguientes comandos.

 # edit port8

Con este comando accedemos a la configuración del puerto 8 y podremos cambiar los parámetros que sean necesarios.

 # set mode dhcp

Aquí estamos indicando que el dispositivo configure automáticamente la dirección IP en el puerto 8 mediante el protocolo DHCP.

 # set allowaccess ping ssh fgfm https http

Con este comando estamos configurando las políticas de acceso para permitir conexiones y tráfico de los protocolos que sean necesarios. Hay que destacar el protocolo HTTP para poder acceder al dispositivo por web mediante la IP que se asigne.

```
    edit "port8"
        set vdom "root"
        set mode dhcp
        set allowaccess ping https ssh http fgfm
        set type physical
        set snmp-index 8
    next
```

Figura 23: Configuración del puerto 8

Finalmente, a modo de comprobación utilizaremos el comando **# get.** Para que nos proporciona información detallada sobre el puerto que nos interesa.

```
FortiGate-VM64-KVM (interface) # edit port8

FortiGate-VM64-KVM (port8) # get
name                : port8
vdom                : root
vrf                 : 0
cli-conn-status     : 2
fortilink           : disable
mode                : dhcp
client-options:
distance            : 5
priority            : 0
dhcp-relay-interface-select-method: auto
dhcp-relay-service  : disable
ip                  : 192.168.190.147 255.255.255.0
allowaccess         : ping https ssh http fgfm
fail-detect         : disable
arpforward          : enable
broadcast-forward   : disable
bfd                 : global
l2forward           : disable
icmp-send-redirect  : enable
icmp-accept-redirect: enable
vlanforward         : disable
stpforward          : disable
ips-sniffer-mode    : disable
ident-accept        : disable
--More--
```

Figura 24: Tabla comando #get

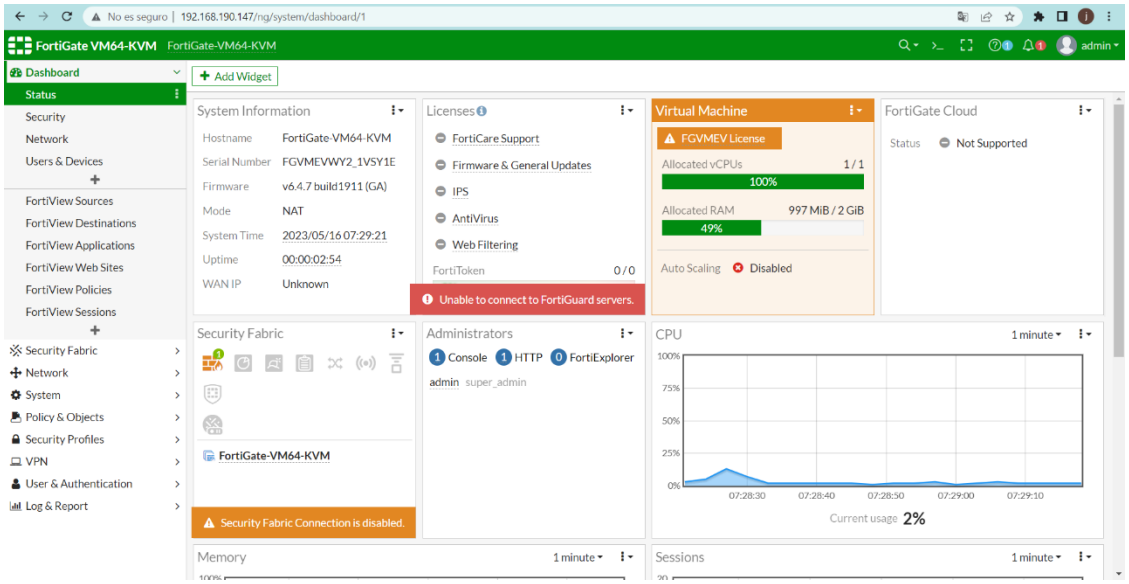
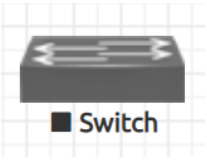


Figura 25: Interfaz web Fortinet

Finalmente, una vez hemos tenemos nuestras credenciales y hemos completado los cambios en la configuración del dispositivo que aparecía por defecto. Ya podemos acceder por web al dispositivo mediante la IP que nos proporciona el proveedor tal y como vemos en la captura anterior.

4.4.2 Switch



En el caso del Switch, se trata de un dispositivo de red que trabaja en la capa 2 del modelo OSI, que a diferencia de un enrutador de capa 3 que transmite las tramas ethernet a través de rutas basadas en direcciones IP. Un enrutador de capa 2 envía las tramas ethernet mediante las direcciones MAC. Cada dispositivo en una red local (LAN) tiene una dirección MAC única que identifica su tarjeta de interfaz de red (NIC).
Accediendo a la página web de EVE-NG observamos las imágenes que son compatibles con el software y de la misma forma que añadimos anteriormente la imagen del firewall y la de Mikrotik. Añadimos la imagen del enrutador de capa 2 que nos interesa.

Una vez añadida la imagen, hay que configurar los parámetros básicos de forma que podamos optimizar al máximo el uso de la memoria RAM de la cual disponemos. La configuración es la siguiente.

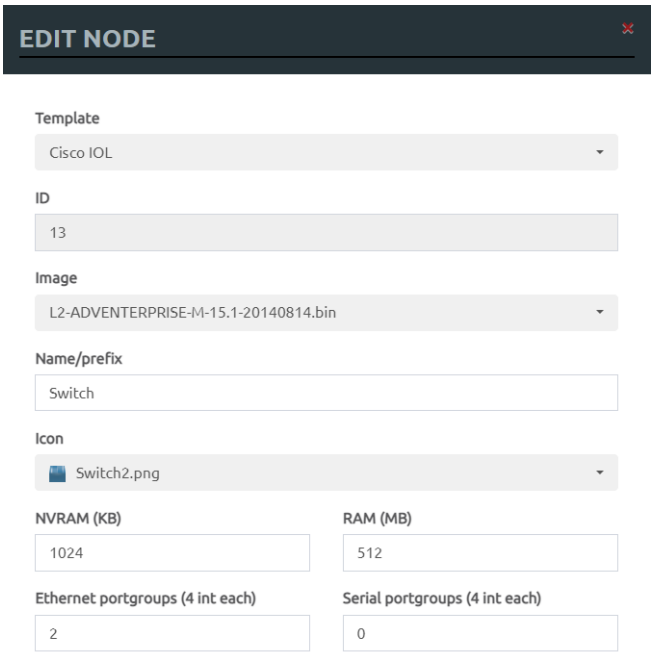


Figura 26: Configuración básica Switch

Tal y como podemos ver en la tabla, tenemos la imagen cargada de un enrutador de capa 2 de cisco, concretamente la versión experimental 15.1. En cuanto al uso de recursos y consumo de RAM, por defecto en la configuración inicial aparece un uso de 1024 MB de RAM. Sin embargo, se puede disminuir a 512 MB tal y como vemos en la imagen sin que afecte al funcionamiento del dispositivo de red.

Una vez configurados los parámetros, el switch estaría listo para usarse, de la misma forma que el firewall introduciremos los comandos por consola mediante la herramienta Putty.

4.4.3 MikroTik

En cuanto al dispositivo de red MikroTik se trata de un dispositivo que ejecuta el sistema operativo RouterOS, diseñado para proporcionar funciones de enrutamiento, conmutación y seguridad en entornos de red, es un dispositivo que ofrece una gran variedad de posibilidades con un coste muy asequible.

En el entorno virtual de EVE-NG, descargaremos la imagen del dispositivo tal y como hemos visto con el ejemplo en el punto 4.3. Sin embargo, en este caso, para acceder al MikroTik no accedemos a la interfaz del dispositivo mediante el Putty como lo hemos con los dispositivos anteriores. En este caso es necesario descargar la aplicación Winbox64, esta aplicación de software desarrollada por MikroTik, es una herramienta gráfica que se utiliza para administrar y configurar dispositivos MikroTik que ejecutan el sistema operativo RouterOS mediante una interfaz intuitiva para el usuario.

Previamente a ver la configuración básica del dispositivo dentro de nuestro entorno virtual veremos como descargar la aplicación Winbox64. La descarga se realizará directamente desde la página de MikroTik. Una vez realizada la descarga la interfaz que debería aparecer es la siguiente.

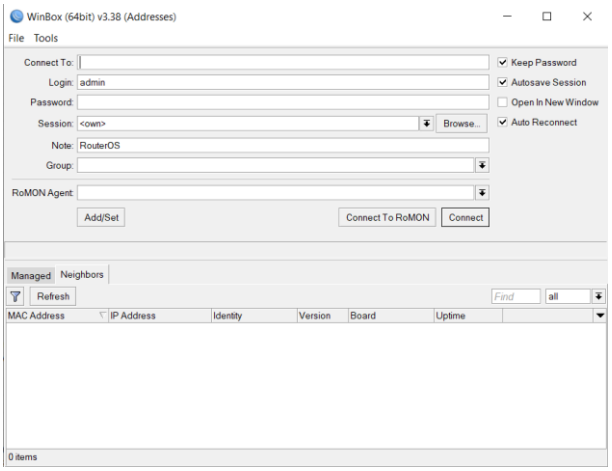


Figura 27: Interfaz de inicio Winbox64

A continuación, veremos cual es la configuración básica de este dispositivo de red dentro de nuestro entorno virtual.

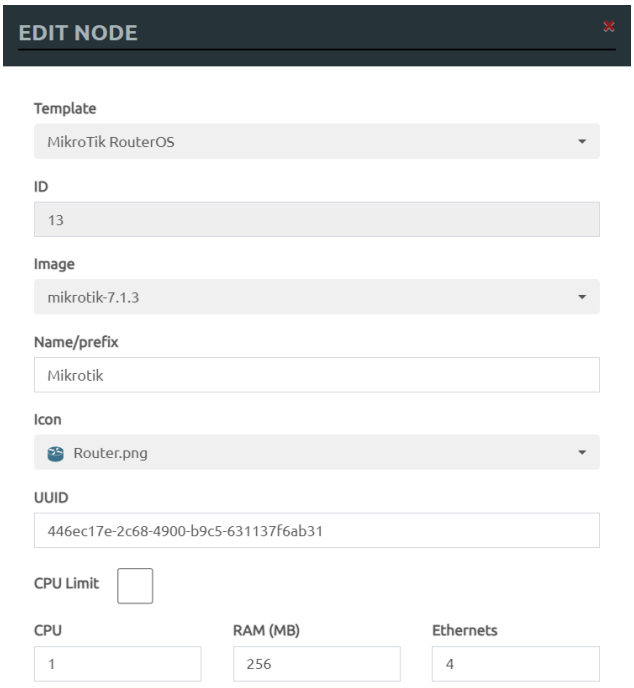
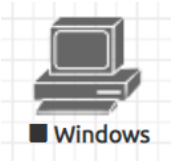


Figura 28: Configuración básica MikroTik

Como podemos observar en la imagen anterior vemos que la versión de MikroTik que vamos a trabajar es la versión emulada 7.1.3. Un aspecto notable de MikroTik, tanto en el mundo real como en el virtual, es su capacidad para funcionar eficientemente con una cantidad relativamente en cuanto a recursos se refiere, una demostración de ello es la imagen anterior, en la que podemos observar que el consumo de memoria RAM es mucho menor que el del resto de dispositivos de red.

4.4.4 Máquina Windows



Las máquinas virtuales de Windows son sistemas operativos completos que se ejecutan en entornos virtualizados, permitiendo crear entornos de prueba y desarrollo para probar configuraciones, aplicaciones y escenarios específicos sin afectar el entorno de producción.
En nuestro caso al tener una cantidad de memoria RAM limitada optaremos por la versión de Windows 7 que requiere menos recursos que una versión de Windows más actual.

De la misma forma que hemos hecho con los dispositivos anteriores, basándonos en las imágenes compatibles que nos ofrece la web de EVE-NG en la sección de documentación, escogemos la que mas nos interese, en este caso buscamos la imagen de Windows 7.
Una vez introducida la imagen en nuestro entorno virtual es momento de ver la configuración básica que requiere la máquina para un correcto funcionamiento.

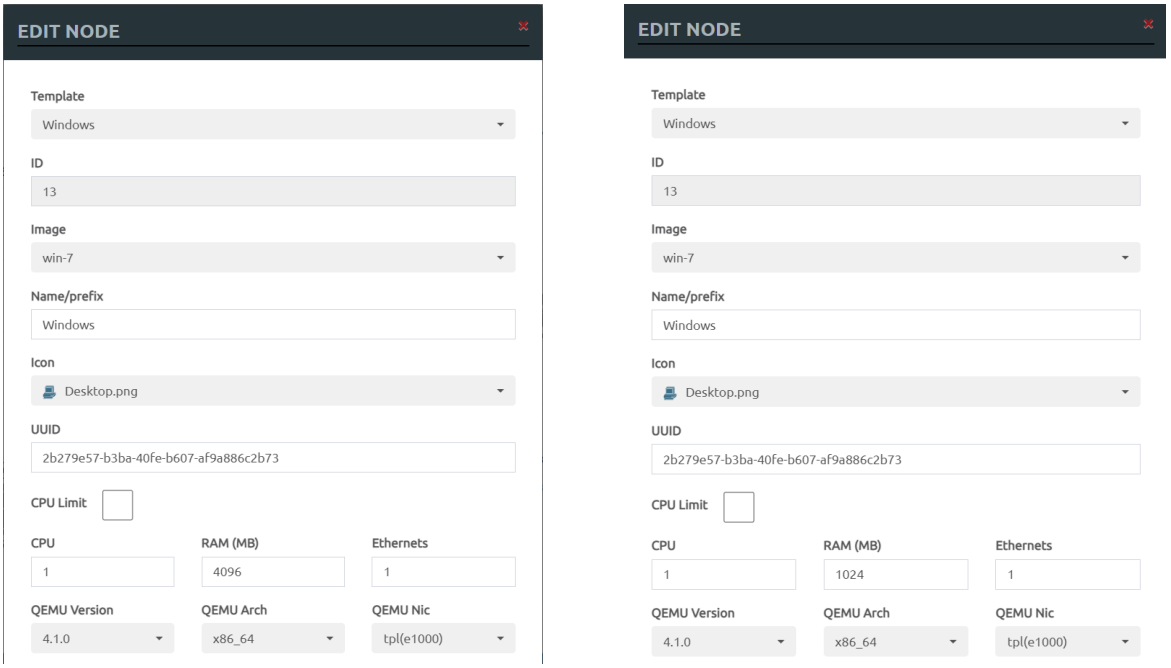


Figura 29: Configuración básica Windows

La imagen de la izquierda muestra la configuración por defecto cuando añadimos el dispositivo virtual, en esta podemos ver un valor de consumo de memoria RAM de 4096 MB, que es un valor considerablemente alto. Por otro lado, la imagen de la derecha a modo de comparativa podemos ver como este consumo de memoria se puede reducir a 1024 MB sin afectar a su correcto funcionamiento, un gasto asumible teniendo en cuenta que partimos de una cantidad de memoria RAM bastante limitada.

En caso de haber escogido una imagen de Windows 10, el consumo de memoria como mínimo ascendería a 2048 MB de RAM para que el dispositivo de red funcionase correctamente, es por eso que teniendo en cuenta en los escenarios que se va a trabajar durante este proyecto y las configuraciones que se van a realizar, valorar el uso de una versión de Windows más primitiva pero que suponga un menor gasto de memoria RAM.

4.4.5 Máquina Linux

Las máquinas virtuales de Linux dentro del entorno virtual de EVE-NG son herramientas versátiles que permiten emular sistemas operativos basados en Linux en un entorno virtualizado. Una de las ventajas de utilizar máquinas Linux en EVE-NG es la capacidad de probar y experimentar con diferentes configuraciones y aplicaciones.
Por otra parte, también es interesante que dentro del mismo entorno de EVE-NG se puedan realizar pruebas de interoperabilidad y configuraciones de red con distintos sistemas operativos en un entorno controlado.

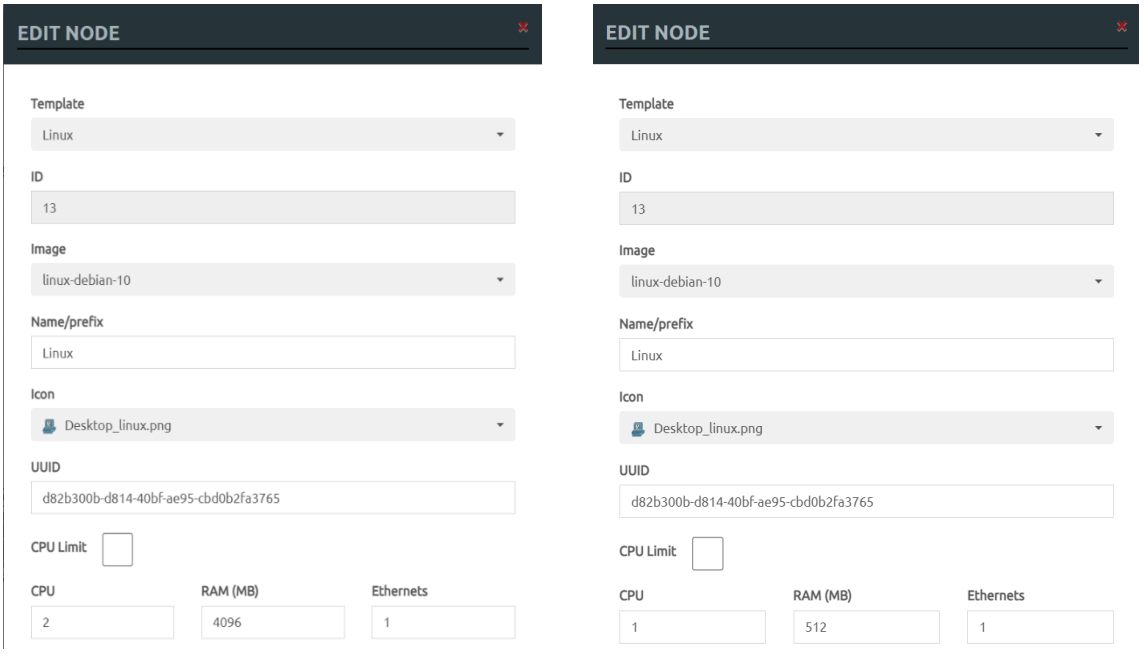


Figura 30: Configuración básica Linux

Tal y como vemos en las imágenes anteriores, el sistema operativo que utilizaremos durante este proyecto es el Debian 10 de Linux. Debian 10 es una opción popular dentro de las distribuciones de Linux con una gran cantidad de usuarios.

En cuanto a los recursos requeridos para que el dispositivo funcione correctamente, podemos ver comparando las dos imágenes que los requisitos de consumo que aparecen por defecto son demasiado altos en comparación con lo que realmente se necesita para que funcione correctamente el Debian 10, lo que supone una gran ventaja para realizar más pruebas y crear diferentes escenarios.

4.5 Esquema de red

A continuación, mostraré una imagen en la cual podremos ver de forma esquemática la distribución de la red empresarial que he implementado dentro del entorno virtual de EVE-NG. Esta red ha sido distribuida de manera que simula dos sedes empresariales ubicadas en diferentes sitios geográficos, la sede A representada a la derecha del esquema y la sede B representada a la izquierda.

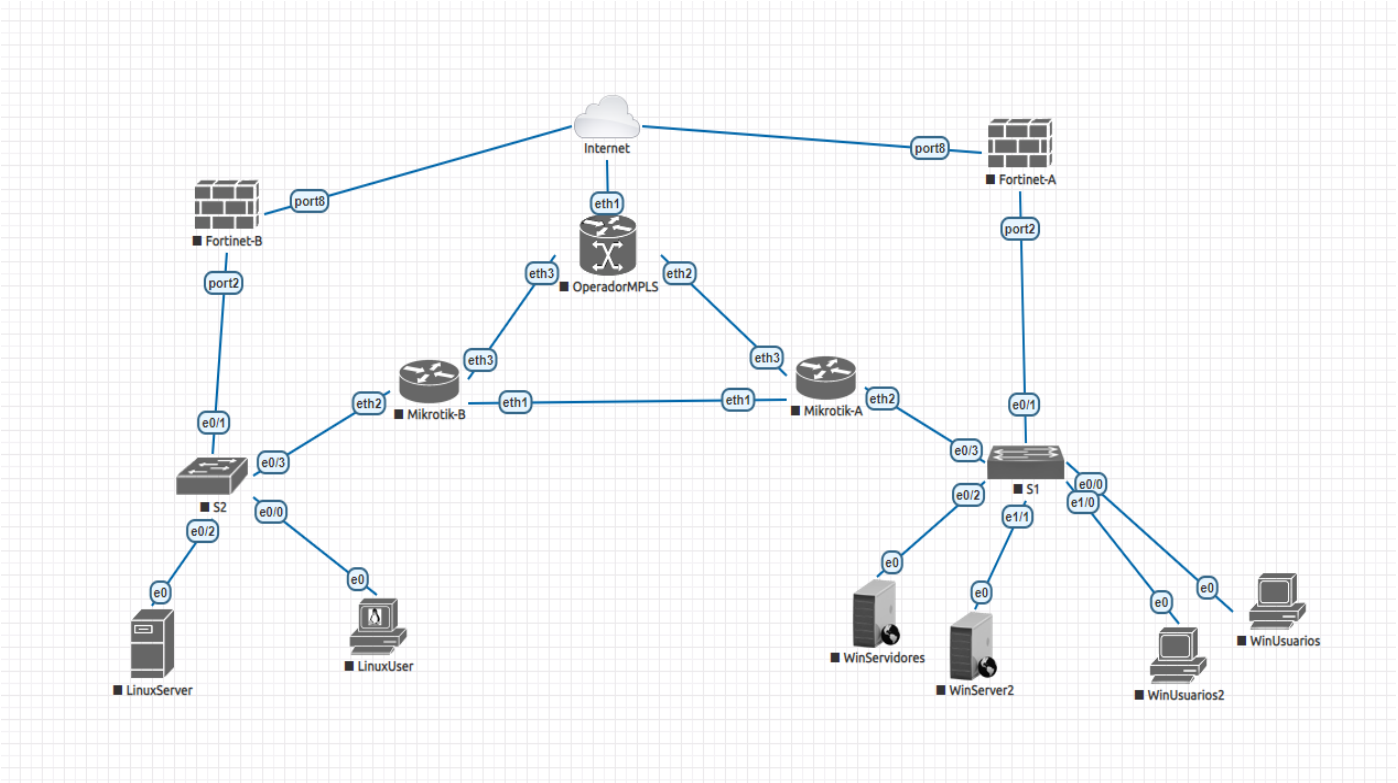


Figura 31: Esquema de red virtual

La *sede A* situada a la derecha la cual actuará como red principal de nuestra simulación de red empresarial, ha sido diseñada para simular una infraestructura más amplia en la cual tenemos la gran mayoría de dispositivos tanto usuarios como servidores.

Por otro lado, en la parte de la izquierda de la imagen tendremos la *sede B*, que siendo de menor tamaño presenta una infraestructura de red más reducida que actuará como una sede secundaria en la cual tenemos un menor número de servidores y usuarios.

4.6 Implementaciones

4.6.1 Distribución de VLAN

En un entorno de red empresarial, la distribución de los diferentes dispositivos y servicios en VLANs ofrece numerosas ventajas a la infraestructura de la red. Al distribuir en VLANs, se obtiene una mayor seguridad al restringir el acceso a recursos y evitar la propagación de amenazas.
El tener una red distribuida en VLANs por dispositivos y servicios permite que la gestión de la red sea mucho más simple a la hora de poder aplicar políticas específicas para cada una de las VLAN y que en caso de fallo en la red también simplifica mucho más la resolución del problema.
Los dispositivos de red que permiten la conexión a los dispositivos locales por capa 2 son los switches. Mientras que los dispositivos de capa 3 como puede ser el firewall son los que enrutan el tráfico entre VLANs.
A continuación, veremos la configuración de los dispositivos y la distribución de la diferentes VLAN de la red.

4.6.1.1 Switch

Un Switch es un dispositivo de red que se utiliza para conectar diferentes dispositivos dentro de una red local (**LAN**). Este dispositivo recibe, procesa y transmite los datos entre los dispositivos conectados. Cunado un dispositivo conectado a un switch envía una trama de red, el switch analiza la dirección MAC de origen y determina la **VLAN** a la que pertenece. Luego el switch etiqueta la trama con un identificador de VLAN antes de transmitirla. De esta manera, asegura que el tráfico de una VLAN específica se mantenga aislado de otras VLAN en la red.

A continuación, veremos la distribución de nuestra LAN y que comandos hemos utilizado para la configuración de los distintos dispositivos de red.

En cuanto a la distribución de las VLANs de la red local, se distribuyen de la siguiente manera:

En la sede B, ubicada la izquierda del esquema tenemos únicamente dos dispositivos, ambos con un sistema operativo Linux, de los cuales uno actuara como usuario y el otro dispositivo actuara como servidor.
La primera VLAN con ID 11, está destinada a los usuarios. En esta VLAN podría haber varios dispositivos conectados, pero en este caso utilizaremos solamente 1 para poder realizar las pruebas necesarias y recrear escenarios básicos. Esta es una forma de poder segmentar el tráfico y aplicar políticas de seguridad a para este grupo de usuarios.

La segunda VlAN con ID 20, esta reservada para servidores. Aquí se encuentran ubicados los servidores Linux que ofrecen diversos servicios a esta supuesta red empresarial.

Por otro lado, tenemos la sede A, situada a la derecha del esquema, en la cual se han establecido las siguientes VLANs para satisfacer las necesidades de la red:

La VLAN de usuarios, con ID 10, se destina a los dispositivos de sistema operativo Windows utilizados por los usuarios en la sede A, obteniendo una organización y estructuración de la red.

Por último, tenemos la VLAN de servidores, con un ID 20, que se utiliza para alojar los servidores Windows de la sede A. De forma que conseguimos segmentar el tráfico de los servidores.

Una vez planteada la estructura que tendrá la red local de nuestra red empresarial, veremos los distintos comandos que se deben saber para llevar a cabo la configuración de la LAN con las distintas VLANs en un switch.

#enable
Cuando se inicia una sesión de configuración en un switch, se ingresa en modo usuario. Este comando nos sirve para acceder al modo privilegiado, que proporciona un nivel más alto de acceso y control sobre la configuración del switch.

#configure terminal
Se utiliza para acceder al modo de configuración global. Este modo permite realizar cambios en la configuración a nivel global como configuración de interfaces o VLANs.

#vlan 10
Sirve para poder crear una VLAN en este caso a modo de ejemplo se crea una VLAN con identificador (ID) 10. Una vez creada, se pueden realizar otras configuraciones relacionadas con dicha VLAN.

#name usuarios
Dentro de la configuración de la VLAN, este comando nos permite asignarle un nombre, en este caso “usuarios” a modo de etiqueta descriptiva para facilitar la administración y la comprensión.

#write
Se utiliza en la configuración de un switch para guardar los cambios realizados en la configuración en la memoria del dispositivo.

#interface ethernet 0/1
Se utiliza en la configuración global del switch para poder acceder a la interfaz ethernet especifica, en este caso la 0/1, permitiendo la configuración y ajustes específicos en esa interfaz.

#switchport trunk encapsulation dot1q
Una vez dentro de la configuración de la interfaz específica, este comando se utiliza para especificar el protocolo de encapsulación que se utilizara en el enlace trunk, que en este caso el protocolo de encapsulación es dot1q.

#switchport mode trunk
Se utiliza para especificar el modo de funcionamiento de un puerto como enlace trunk.

#switchport trunk allowed vlan all
Configura el enlace trunk para que transporte y permita el tráfico de todas las VLANs configuradas en el switch.

#switchport mode access
Partiendo desde la configuración de una interfaz específica, este comando se utiliza para que un puerto se configure en modo acceso.

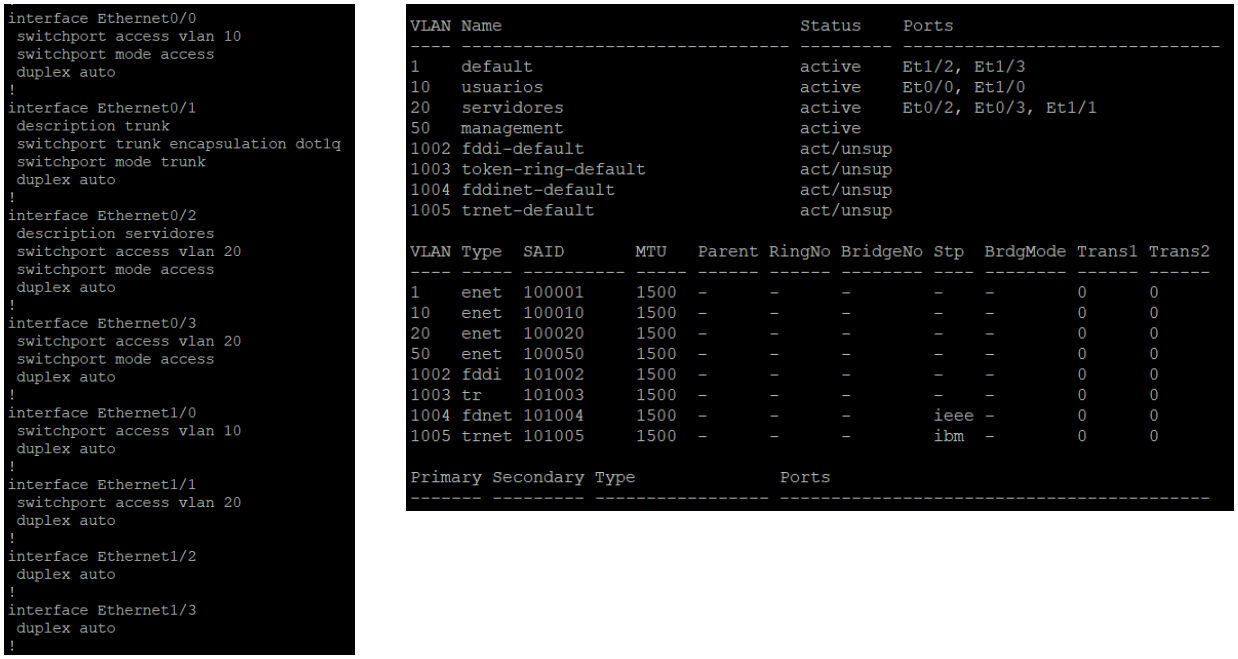
#switchport Access vlan 10
En la propia configuración de una interfaz en concreto, este comando especifica que el tráfico que ingresa o sale estará asociado a la VLAN con el ID que necesitemos y se transmitirá únicamente dentro de esa VLAN.

#show run
Se utiliza en la configuración del switch para mostrar una representación completa de la configuración actual del dispositivo

#show vlan
Este comando sirve para mostrar información detallada sobre las VLANs configuradas en el dispositivo.

A continuación, se mostrarán dos imágenes en las cuales se podrá ver la configuración de ambos switches, tanto el de la sede A como el de la sede B.

Sede A



```
interface Ethernet0/0
 switchport access vlan 10
 switchport mode access
 duplex auto
!
interface Ethernet0/1
 description trunk
 switchport trunk encapsulation dot1q
 switchport mode trunk
 duplex auto
!
interface Ethernet0/2
 description servidores
 switchport access vlan 20
 switchport mode access
 duplex auto
!
interface Ethernet0/3
 switchport access vlan 20
 switchport mode access
 duplex auto
!
interface Ethernet1/0
 switchport access vlan 10
 duplex auto
!
interface Ethernet1/1
 switchport access vlan 20
 duplex auto
!
interface Ethernet1/2
 duplex auto
!
interface Ethernet1/3
 duplex auto
!
```

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et1/2, Et1/3
10   usuarios                          active    Et0/0, Et1/0
20   servidores                        active    Et0/2, Et0/3, Et1/1
50   management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
50   enet  100050     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Primary Secondary Type              Ports
------- --------- ----------------- ----------------------------------------
```

Figura 32: Configuración Switch A

En estas dos imágenes podemos ver, por un lado, la imagen de la izquierda con la configuración de cada interfaz de forma detallada y por otro lado podemos ver la imagen de la derecha en la que podemos ver información detallada de las VLANs.

Sede B

```
interface Ethernet0/0
 switchport access vlan 11
 switchport mode access
 duplex auto
!
interface Ethernet0/1
 description trunk
 switchport trunk encapsulation dot1q
 switchport mode trunk
 duplex auto
!
interface Ethernet0/2
 switchport access vlan 20
 switchport mode access
 duplex auto
!
interface Ethernet0/3
 switchport access vlan 20
 switchport mode access
 duplex auto
!
interface Ethernet1/0
 duplex auto
!
interface Ethernet1/1
 duplex auto
!
interface Ethernet1/2
 duplex auto
!
interface Ethernet1/3
 duplex auto
!
```

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et1/0, Et1/1, Et1/2, Et1/3
11   LinuxUser                         active    Et0/0
20   LinuxServer                       active    Et0/2, Et0/3
50   management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
11   enet  100011     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
50   enet  100050     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Figura 33: Configuración Switch B

En este caso tenemos 2 imágenes que representan lo mismo que las dos anteriores pero esta vez proporcionan información detallada sobre la configuración del switch de la sede B.

Tal y como podemos observar, ambas sedes siguen la misma distribución en cuanto a los modos de los distintos enlaces.
En ambos casos vemos que la interfaz ethernet 0/1 está configurada en modo trunk, que es la interfaz que conecta el switch con el firewall tal y como podemos ver en la figura 31 del esquema de red y que permite el tráfico de múltiples VLAN a través de un solo cable, facilitando la segmentación y la gestión del tráfico de la red. De esta manera, los switches y los firewalls pueden distinguir y enviar los datos a la VLAN correspondiente.

En cuanto al resto de interfaces que están configuradas como enlaces en modo acceso, son las que conectan los switches con los distintos PCs. Los enlaces en modo acceso son útiles para conectar los dispositivos finales de la red. Estos enlaces permiten que los dispositivos accedan a los recursos de red y se comuniquen dentro de la misma VLAN.

4.6.1.2 Firewall

En el proceso de configuración de los firewalls de la red, mediante el protocolo dhcp se asignan las siguientes IPs a los firewalls de nuestra red.
Por un lado, tenemos el firewall de la sede A al cual el proveedor le ha asignado la dirección IP **192.168.190.133** y en el otro lado tenemos el firewall de la sede B al cual se le ha asignado la IP **192.168.190.134.** Mediante dichas IP seremos capaces de acceder a la interfaz web para la configuración de los firewalls.

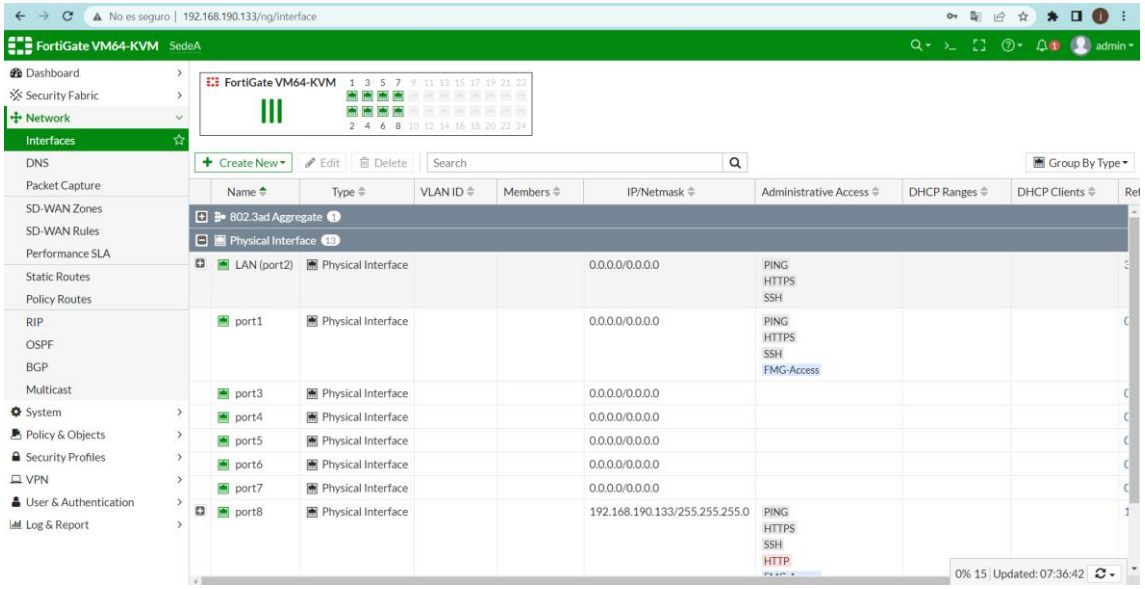


Figura 34: Sección de interfaces fortigate sede A

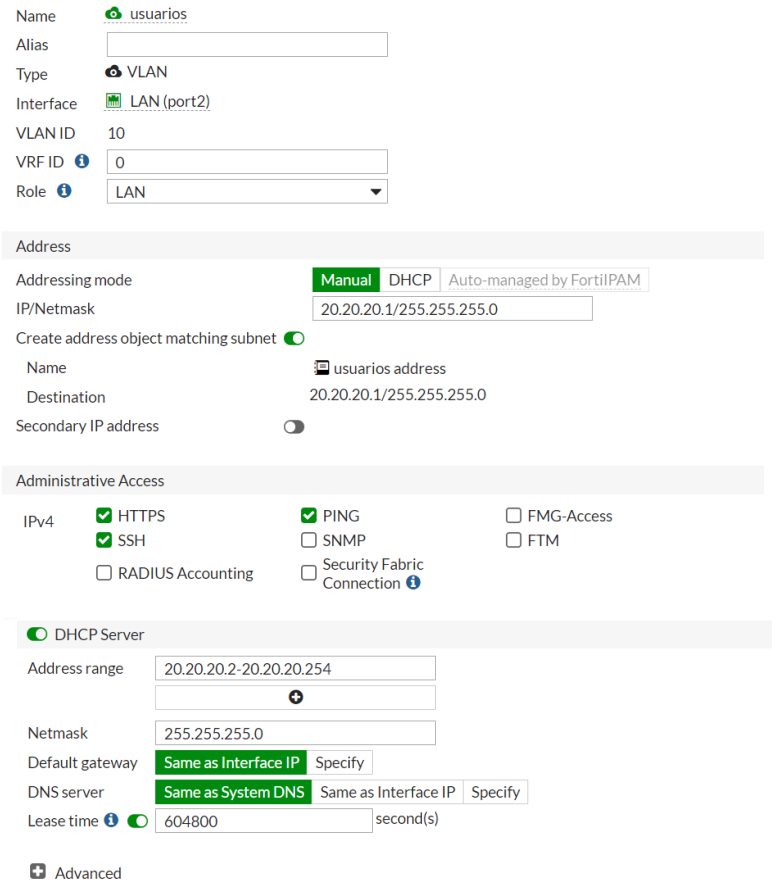


Figura 35: Configuración fortigate VLAN usuarios sede A

Las imágenes anteriores representan una captura de la sección de interfaces en la que podemos encontrar información y podemos configurar las interfaces del firewall. También aparece la configuración para crear una VLAN en el entorno web de fortigate.

En la sede A, se ha creado una VLAN con el ID 10, denominada "Usuarios", la cual esta destinada a los PCs con sistemas operativos Windows. A los dispositivos dentro de esta VLAN se les ha asignado un rango de direcciones IP que va desde **20.20.20.2** hasta **20.20.20.254**. Además, se ha implementado un servidor DHCP para asignar de forma automática las direcciones IP a los dispositivos en esta VLAN.

Por otro lado, en la sede B, se ha establecido una VLAN con el ID 11, conocida como "UsuariosLinux", para satisfacer las necesidades de los PCs con sistemas operativos Linux. En esta VLAN, los dispositivos reciben las direcciones IP a través del servidor DHCP, con un rango que abarca desde **21.21.21.2** hasta **21.21.21.254.**

4.6.1.3 PC Windows

En cuanto a los PCs con sistema operativo Windows situado en la sede A, al encenderse y conectarse a la red, el servidor DHCP asignará una dirección IP disponible dentro de ese rango a cada PC (20.20.20.2 – 20.20.20.254).
Para realizar la conexión a la red es necesario asignar la opción de recibir la IP mediante DHCP y no la asignación de IP de forma manual.

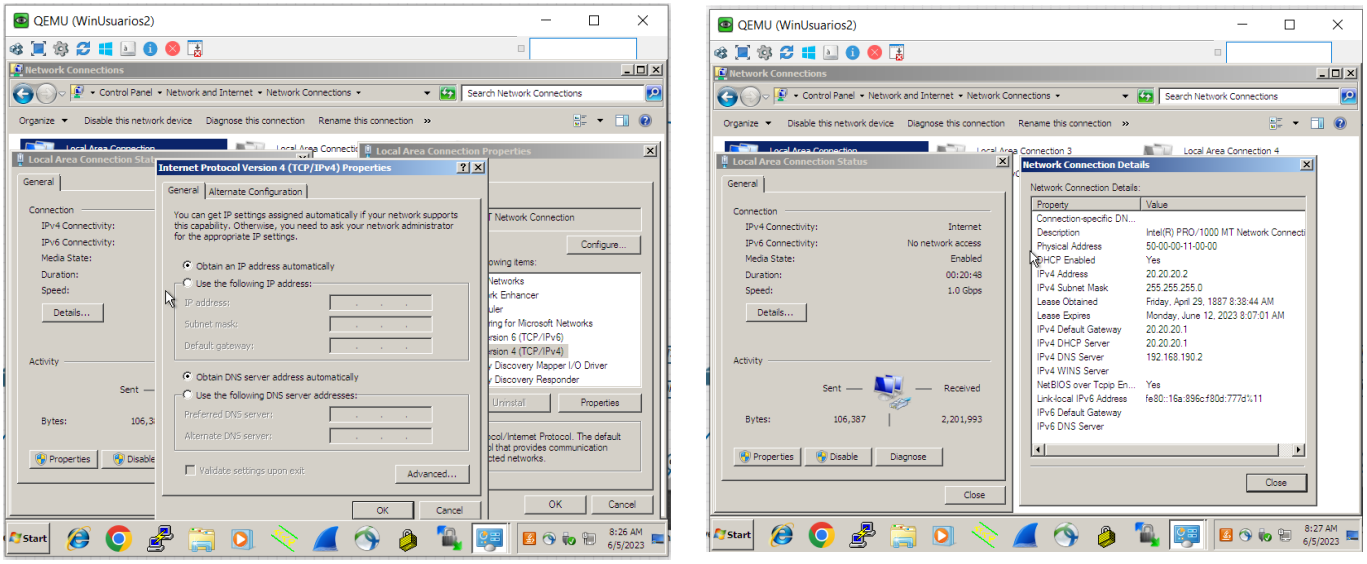


Figura 36: Configuración IP máquina Windows (Usuarios)

En las imágenes anteriores podemos ver como conectar a la red el PC, cambiando la configuración de conexión de red desde el panel de control para que la asignación de IP la reciba de forma automática. Además, en la imagen de la derecha podemos ver los detalles de la conexión de red después de activar la asignación automática como recibimos una de las IPs del rango de la VLAN que habíamos configurado anteriormente en el fortigate.

4.6.1.4 PC Linux

Por otro lado, en la sede B, tenemos los usuarios que utilizan el sistema operativo Debian 10, a los cuales se le asigna un IP de la VLAN 11 dentro del rango (21.21.21.2 – 21.21.21.254). Al igual que con los dispositivos Windows hay que configurar la conexión a la red para recibir una IP de forma automática.

#sudo apt-get update
Cuando se ejecuta este comando, el sistema operativo se conecta a los servidores de los repositorios configurados en el sistema y descarga las últimas versiones de los paquetes instalados.

#sudo apt-get install isc-dhcp-client
Este comando se utiliza para instalar el cliente de DHCP proporcionado por el paquete "isc-dhcp-client". El cliente DHCP es un software que permite que un dispositivo en una red obtenga automáticamente una configuración de red IP, incluyendo dirección IP, máscara de red, puerta de enlace predeterminada (Gateway) y servidores DNS.

#sudo dhclient -v
Este comando sirve para ejecutar manualmente el cliente de DHCP. Donde el cliente de DHCP envía una solicitud de DHCP broadcast a la red, solicitando una dirección IP y otra información sobre la configuración de red al servidor DHCP disponible en la red.

#sudo apt install net-tools
Se utiliza para instalar el paquete "net-tools", este paquete proporciona un conjunto de herramientas de red útiles para la administración y el diagnóstico de redes.

#ifconfig
Una de las herramientas que ofrece el paquete "net-tools" es "ifconfig". Permite configurar y mostrar información de las interfaces de red.

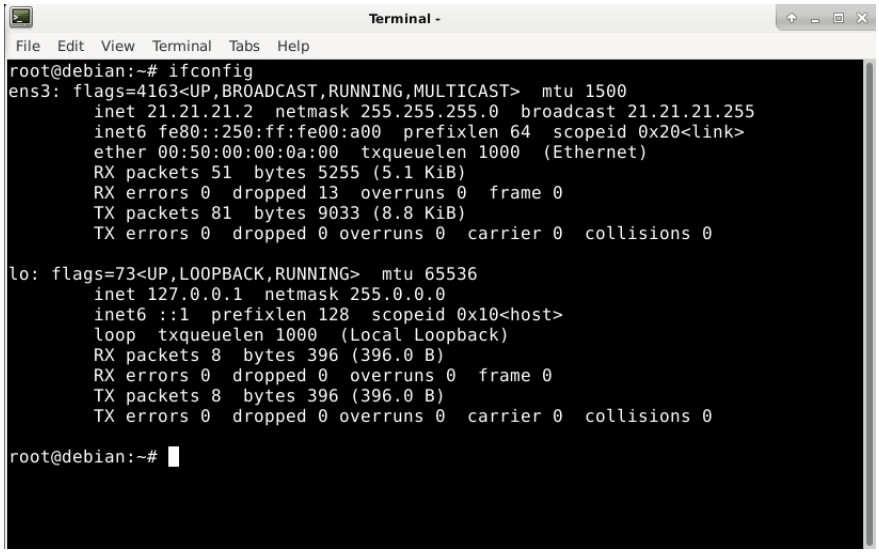


Figura 37: Interfaz de red Debian 10

En la figura anterior podemos comprobar como se le ha asignado una IP del rango que habíamos seleccionado para la VLAN 11 en el fortigate.

4.6.2 Túnel EoIP

Un túnel EOIP (Ethernet over IP) es una tecnología que permite la transmisión de tramas Ethernet a través de una red IP. Aunque opera en capa 2, su conexión y gestión se realizan mediante capa 3. Al establecer un túnel EOIP, se crea una conexión virtual entre dos puntos finales, utilizando direcciones MAC en el encapsulamiento de tramas Ethernet en paquetes IP.
El túnel EOIP ofrece la capacidad de extender una red al agregarlo a un bridge, lo que permite la integración de redes locales y remotas a través de una infraestructura IP existente. Al agregar el túnel EOIP a un bridge, las tramas Ethernet se envían a través del túnel y se entregan a la red remota, manteniendo las características de una red local.
Esta capacidad de extensión de red a través del túnel EOIP y su integración con un bridge proporcionan flexibilidad y escalabilidad en la gestión de redes extendidas. Además, se pueden implementar políticas de calidad de servicio (QoS) para priorizar ciertos tipos de tráfico, lo que garantiza un rendimiento óptimo y una transmisión de voz y video de calidad en la red extendida.

A continuación, veremos el uso de esta tecnología para poder conectar de forma segura los servidores de ambas redes.

4.6.2.1 MikroTik

En primer lugar, veremos la configuración de los dispositivos de red MikroTik para realizar la simulación de red MPLS.
Observando el esquema de red (Figura 31), podemos observar 3 routers: OperadorMPLS, Mikrotik-A y Mikrotik-B.

Por un lado, tenemos conectado directamente a nuestro proveedor nuestro rouoter con nombre OperadorMPLS, el cual simplemente une mediante un bridge las dos MikroTik a internet para que el servidor DHCP les asigne una IP, con la intención de representar un proveedor de servicios.

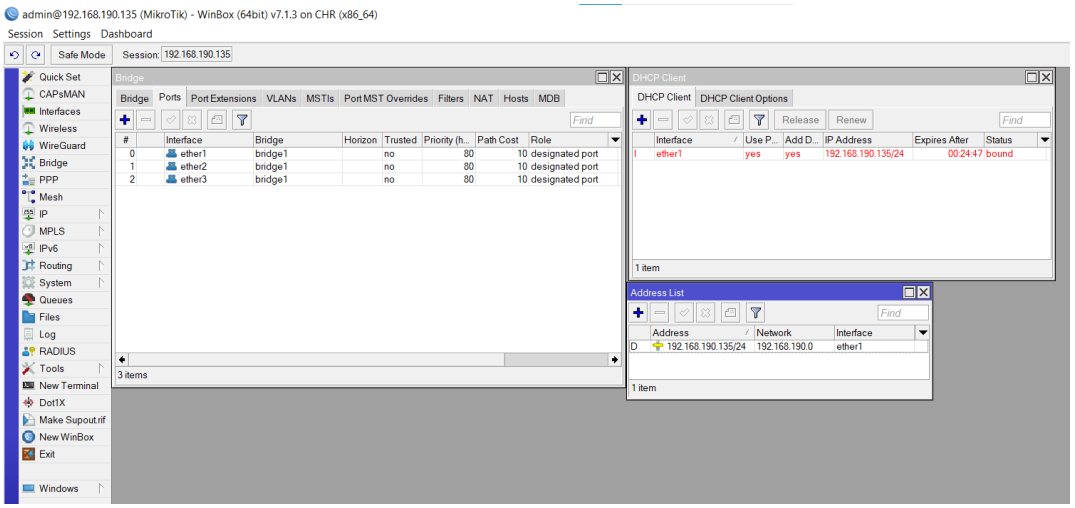


Figura 38: Interfaz Winbox64 OperadorMPLS

En la imagen anterior podemos observar la configuración del supuesto proveedor de servicios el cual únicamente se encarga de conectar mediante un bridge las distintas interfaces de forma que reciban una IP por parte del proveedor de servicios.

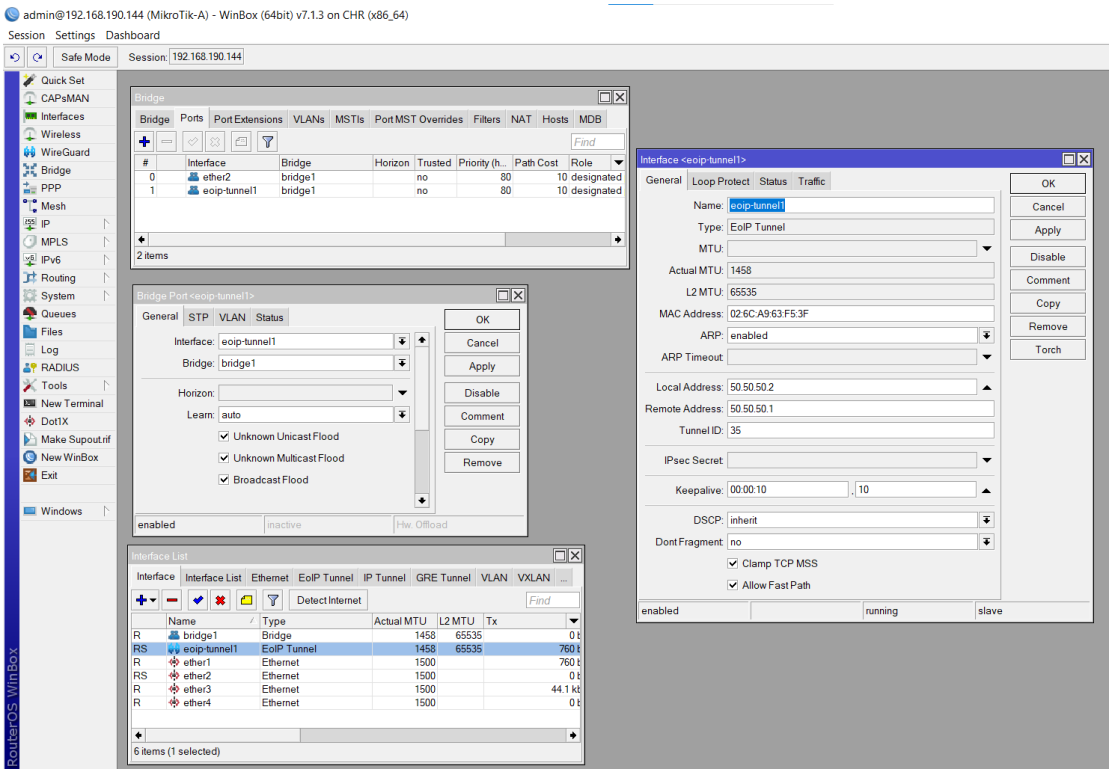


Figura 39: Configuración Mikrotik-A

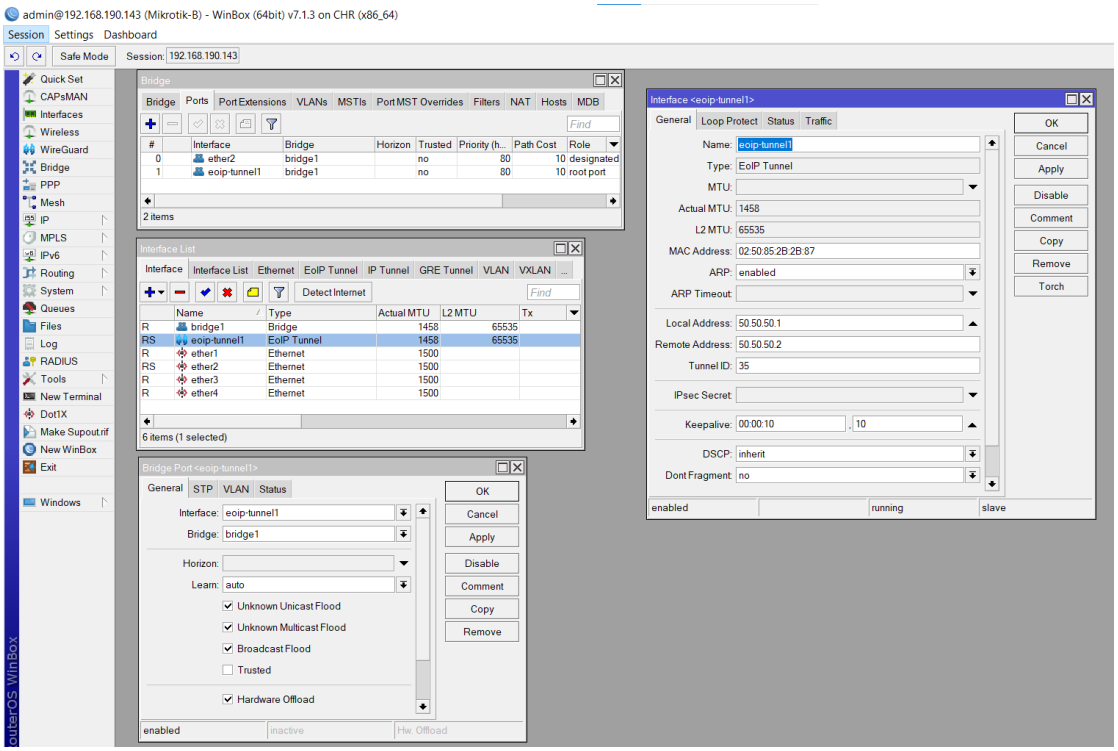


Figura 40: Configuración Mikrotik-B

Con el objetivo de simular el funcionamiento de una red MPLS, se ha utilizado dos dispositivos, Mikrotik-A y Mikrotik-B, los cuales están conectados entre sí mediante un túnel EoIP. Este túnel establece una conexión virtual punto a punto entre los dos dispositivos MikroTik, permitiéndoles comunicarse entre sí a través de una red IP existente. Cada MikroTik tiene asignada una dirección IP de origen y destino para el túnel EoIP.
El túnel EoIP crea un enlace virtual a nivel de capa 3, esto permite a los dispositivos de ambos extremos del túnel comunicarse entre sí como si estuvieran conectados directamente en la misma red local.

También es necesario crear un bridge en cada MikroTik. El bridge combina las interfaces de red conectadas a los dispositivos MikroTik en una única interfaz lógica. Esto permite a los dispositivos conectados a las interfaces del bridge se comuniquen entre sí como si estuvieran en la misma red local. En este caso, las interfaces del túnel EoIP y las interfaces conectadas a los switches.

En cuanto al funcionamiento de esta configuración, cuando los servidores de una sede envíen tráfico a través de las interfaces conectadas a los switches, este tráfico se dirige al bridge correspondiente en el MikroTik de esa sede. El bridge, reenvía el tráfico a través del túnel EoIP hacia el otro MikroTik. El túnel EoIP encapsula el tráfico ethernet y lo envía a través de la red IP existente entre los MikroTik. Finalmente, el bridge del MikroTik del otro extremo reenvía el tráfico a las interfaces conectadas al switch de esa sede. De esta manera, los servidores de ambas sedes pueden comunicarse entre sí de forma segura como si estuvieran en la misma LAN.

4.6.2.2 Switch

En relación con las figuras 32 y 33, se puede observar la configuración completa de ambos switches. En el caso de la sede B, se ha asignado la interfaz Ethernet 0/2 para el servidor con sistema operativo Linux y la interfaz Ethernet 0/3 para la conexión del switch con el MikroTik.

En cuanto a la sede A, se han asignado las interfaces Ethernet 0/2 y 1/1 para las conexiones de los dos servidores con sistema operativo Windows con el switch, mientras que la interfaz Ethernet 0/3 se utiliza para la conexión del switch con el MikroTik.

Para lograr esta conexión, se ha configurado una VLAN específica, la VLAN 20, para los servidores de la red. Cuando los servidores envían datos, los paquetes se etiquetan con la VLAN 20 y se transmiten a través de los switches hacia el MikroTik correspondiente.

Se ha creado la VLAN 20 para todas las interfaces de ambos switches, lo cual permite agrupar los datos de cada sede. Al transmitir los datos a través del túnel EoIP a nivel de enlace de datos, los servidores de ambas sedes pueden comunicarse de forma segura, como si estuvieran en la misma red local, utilizando una única VLAN para los servidores.
Mediante la configuración de una VLAN específica y la asignación de las interfaces de los servidores y los switches, se establece una conexión segura entre las sedes A y B. Los datos de los servidores se transmiten a través de los switches y se etiquetan con la VLAN 20, permitiendo la comunicación eficiente entre los servidores a través del túnel EoIP.

4.6.2.3 Firewall

Name	Type	VLAN ID	Members	IP/Netmask	Administrative Access	DHCP Ranges
802.3ad Aggregate 1						
Physical Interface 13						
LAN (port2)	Physical Interface			0.0.0.0/0.0.0.0	PING HTTPS SSH	
Management	VLAN	50		172.16.10.1/255.255.255.0	PING HTTPS SSH	
servidores	VLAN	20		0.0.0.0/0.0.0.0		
usuarios	VLAN	10		20.20.20.1/255.255.255.0	PING HTTPS SSH	20.20.20.2-20.20.20.254

Figura 41: LAN Fortigate A

Name	Type	VLAN ID	IP/Netmask	Administrative Access
802.3ad Aggregate 1				
Physical Interface 12				
LAN (port2)	Physical Interface		0.0.0.0/0.0.0.0	PING HTTPS SSH
management	VLAN	50	172.16.0.1/255.255.255.0	PING HTTPS SSH
VlanLinuxServer	VLAN	20	0.0.0.0/0.0.0.0	
VlanLinuxUser (VlanUser)	VLAN	11	21.21.21.1/255.255.255.0	PING HTTPS SSH

Figura 42: LAN Fortigate B

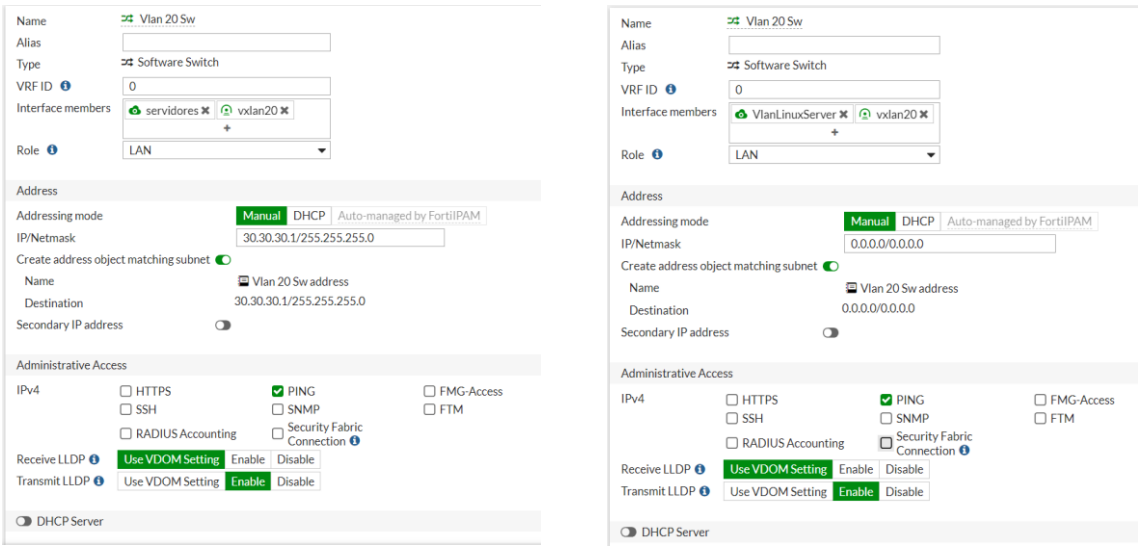


Figura 43: Software switch Fortigate A y B

En las figuras 41 y 42 podemos ver las configuraciones de las LAN de ambos firewalls, en este caso para la implementación del túnel EoIP, al trabajar en la capa de enlace de datos no necesitan que la VLAN 20 tenga una dirección IP. Es por eso que en ambos dispositivos la dirección IP de la VLAN 20 es 0.0.0.0.

Por otro lado, en la figura 43 podemos ver la configuración del software switch de cada firewall. Un software switch permite consolidar múltiples interfaces físicas en un solo switch virtual, lo que simplifica la administración y configuración de la red.

En este caso, el uso del software switch permite establecer una conexión entre una red VXLAN y VLAN para permitir la comunicación y la interconexión entre los dos dominios de red. Al implementar un software switch somos capaces de segmentar y aislar el tráfico de la VXLAN y la VLAN de forma que nos permite una segmentación del tráfico y una simplificación de la configuración y administración de la red.

Dentro de la configuración del software switch del firewall de la sede A, vemos que hay una dirección IP de destino. Esta dirección IP especifica la dirección a la que se enviará el tráfico que ingresa al switch y no tiene una ruta específica definida.

4.6.2.4 Máquina Windows

En cuanto a la configuración de los servidores con sistema operativo Windows es necesario asignarles unas IP fijas que entren dentro del rango de la dirección IP establecida en el software switch del firewall de la sede A de forma que pertenezcan también a la VLAN 20 asociada.

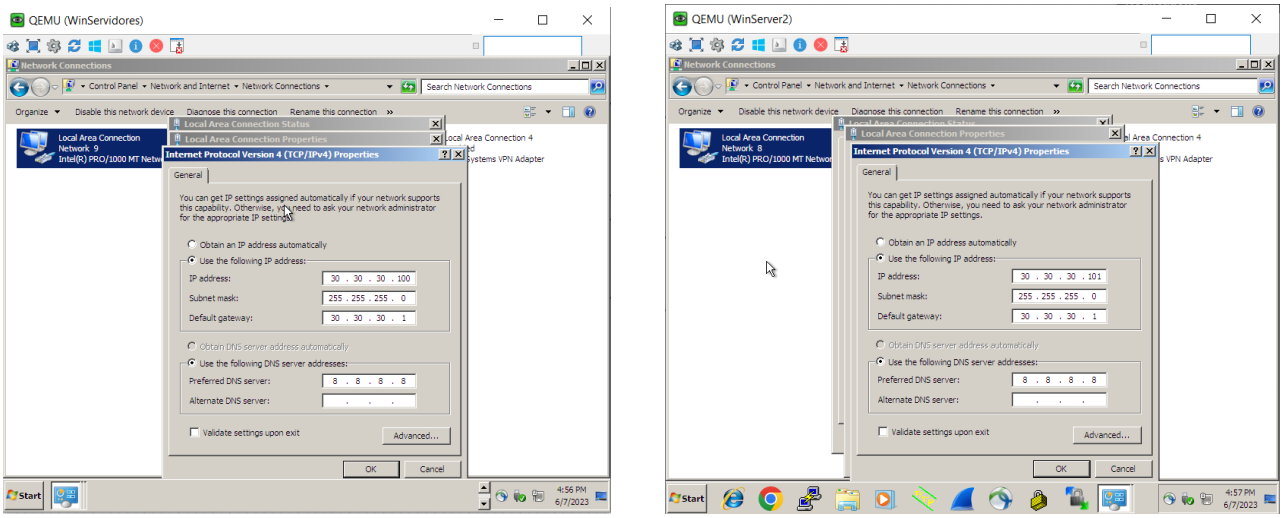


Figura 44: IP servidores Windows

4.6.2.5 Máquina Linux

En el caso del servidor con sistema operativo Linux sucederá lo mismo y habrá que asignarle una IP fija dentro del rango de la IP del software switch asociado a la VLAN 20.

#nano etc/network/interfaces

Este comando se utiliza para editar el archivo de configuración de red en sistemas basados en Debian. Este archivo, ubicado en la ruta "/etc/network/interfaces", contiene la configuración de las interfaces de red del sistema.

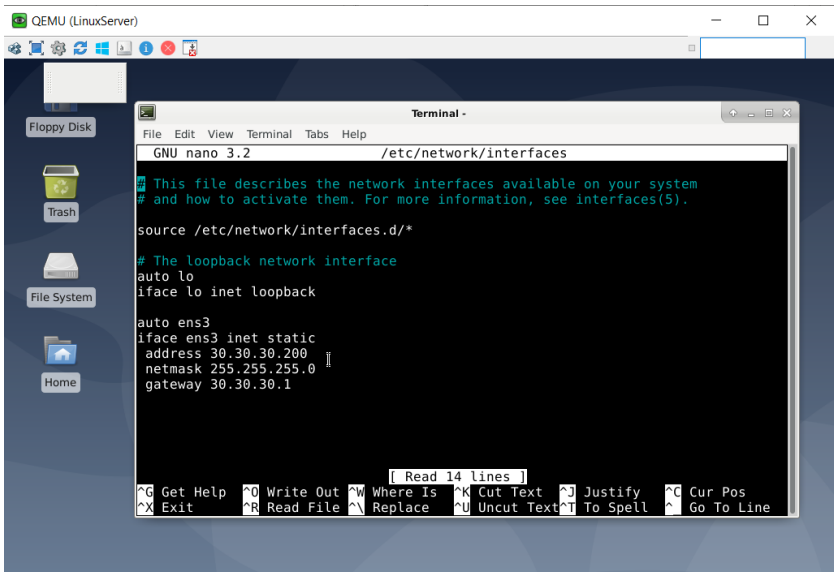


Figura 45: IP servidor Linux

Una vez dentro de la configuración de interfaces del sistema es necesario escribir de forma manual tanto la interfaz, la dirección IP, la máscara y la puerta de enlace (Gateway).

4.6.3 VXLAN

VXLAN (Virtual Extensible LAN), es un protocolo de encapsulación que proporciona conectividad del centro de datos mediante túneles para ampliar las conexiones de capa 2 a través de una red de capa 3. VXLAN utiliza la encapsulación para transportar paquetes de red existentes en una red virtual. Estos paquetes se envuelven en un encabezado VXLAN y se transmiten a través de una red IP existente.

El protocolo de tunelización VXLAN que encapsula tramas Ethernet de capa 2 en paquetes UDP de capa 3 le permite crear subredes o segmentos virtualizados de capa 2 que abarcan redes físicas de capa 3. Cada subred de capa 2 se identifica de forma única mediante un identificador de red VXLAN (VNI) que segmenta el tráfico.

Cuando un host en una red virtual desea comunicarse con otro host en la misma red virtual, los paquetes se encapsulan en paquetes VXLAN y se envían a través de la red física hasta llegar al host receptor. Una vez allí, se elimina el encabezado VXLAN y se entrega el paquete original al host receptor dentro de la red virtual.

En nuestra red usaremos el protocolo VXLAN para permitir la transmisión de datos entre servidores. La implementación del protocolo VXLAN nos permite extender la VLAN 20 desde la sede principal (sede A), hasta una sede remota (sede B). Esto permite que los servidores en ambas ubicaciones formen parte de la misma red virtual, como si estuvieran conectados directamente en una red local. De forma que con esta conexión somos capaces de mantener una conexión entre servidores en caso de algún tipo de fallo en el túnel EoIP implementado mediante las MikroTik.

4.6.3.1 Firewall

Para la realizar la configuración de la VXLAN utilizaremos los siguientes comandos.

#config system vxlan
se utiliza para configurar los parámetros relacionados con la implementación y el funcionamiento de VXLAN en el dispositivo FortiGate.

#edit vxlan20
se utiliza para acceder al modo de configuración específico de una instancia VXLAN con un identificador VXLAN (VXLAN ID) específico, en este caso, 20. Este comando también crea dicha VXLAN específica.

#set vni 20
Se utiliza dentro del modo de configuración de una instancia VXLAN para establecer el identificador de red virtual (VNI, Virtual Network Identifier) de la instancia VXLAN en 20.
El VNI es un número de identificación único asignado a cada instancia VXLAN y se utiliza para distinguir y enrutar los paquetes en la red virtual.

#set interface port8
se utiliza dentro del modo de configuración de una instancia VXLAN para asignar una interfaz específica, en este caso el puerto 8, a la instancia VXLAN.

#set remote-ip 192.168.190.133
se utiliza dentro del modo de configuración de una instancia VXLAN para establecer la dirección IP remota a la cual se conectarán los dispositivos que forman parte de la red virtual VXLAN.
Esto significa que los dispositivos dentro de la red virtual VXLAN utilizarán esta dirección IP para establecer conexiones y comunicarse con otros dispositivos que se encuentren en esa dirección IP remota.
La IP que vemos en el comando es la IP del firewall de la sede A, lo que implica que esta configuración es la configuración del firewall de la sede B.

Esta configuración se repite en ambos firewalls tanto en la sede A como en la sede B, con la diferencia de que la IP remota será contraria, es decir, la IP remota de la sede B será la que vemos en el ejemplo 192.168.190.133 y la IP que utilizaremos para el comando de la sede A será la del firewall de la sede B, es decir, 192.168.190.134.

Una vez tenemos la VXLAN creada con el identificativo VNI 20. Es necesario asociar dentro del software switch tal y como vemos en la figura 43, la VLXAN con la VLAN 20 en los firewalls de ambas sedes.

En el FortiGate de la sede principal (sede A), cuando creas un software switch para conectar la VXLAN con la VLAN 20, se configura la dirección IP del software switch en 30.30.30.1/24. Esta dirección IP se asigna como la puerta de enlace para los servidores de la VLAN 20 en la sede A. Al definir la dirección IP como 30.30.30.1, estás estableciendo una puerta de enlace dentro de la misma red (30.30.30.0/24) que los servidores de la VLAN 20 en la sede A. Esto permite que los servidores se comuniquen con el software switch a través de esta dirección IP.

Por otro lado, en el software switch del firewall de la sede B, se configura la dirección IP como 0.0.0.0. Esta configuración indica que el software switch del firewall de la sede B no necesita una dirección IP específica asignada. Esta configuración se utiliza cuando el software switch actúa como un puente o un enlace de red y no requiere una dirección IP asignada directamente a él.

La razón de esta configuración particular se basa en el hecho de que la VXLAN está siendo transportada a través de un túnel VPN. Al establecer el túnel VPN entre las sedes A y B, se crea una conexión segura a través de una red pública, como Internet. Dentro de este túnel VPN, puedes encapsular y transportar diferentes protocolos de red, como la VXLAN en este caso.

Dado que la VXLAN se transporta a través del túnel VPN, no es necesario tener múltiples gateways en ambas sedes. Todo el tráfico destinado a la VLAN 20 en la sede A se envía a través del túnel VPN hacia la sede B. En la sede B, el firewall recibe los paquetes y los enruta internamente a los servidores de la VLAN 20, sin necesidad de un gateway explícito en el software switch del firewall de la sede B. Por lo tanto, asignar la dirección IP 0.0.0.0 en ese software switch es apropiado, ya que no se requiere una dirección IP específica para su funcionamiento dentro de la sede B.

4.6.4 VPN

Un túnel VPN (Virtual Private Network) es una conexión segura y cifrada que se establece entre dos puntos de una red a través de una infraestructura de red pública, como Internet.

El túnel VPN actúa como un canal protegido que encapsula los datos en paquetes cifrados antes de enviarlos a través de la red pública. Esto proporciona un nivel adicional de seguridad, asegurando que los datos transmitidos estén protegidos contra accesos no autorizados y asegurando la confidencialidad de la información.

4.6.4.1 Firewall

La creación y configuración del túnel VPN se realiza desde la interfaz web de los Fortigate y se realizaría de la siguiente manera.

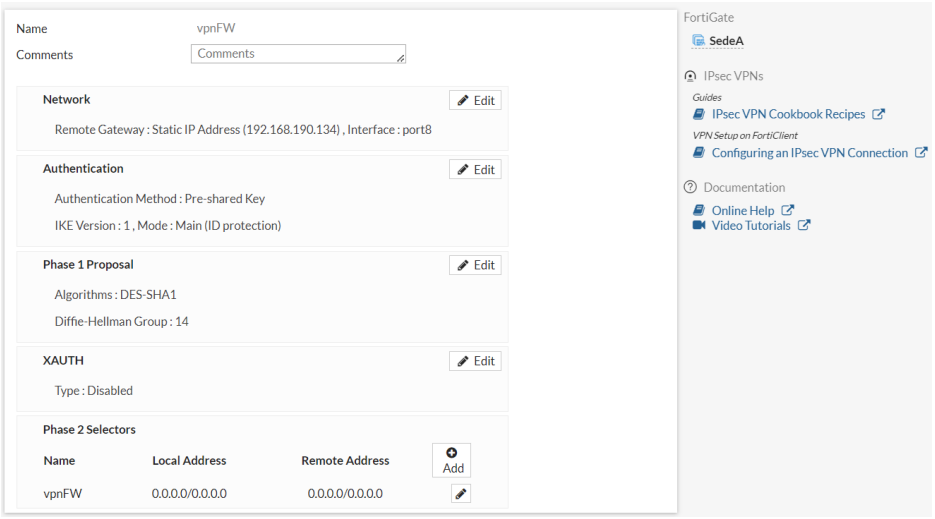


Figura 46: Configuración VPN sede A

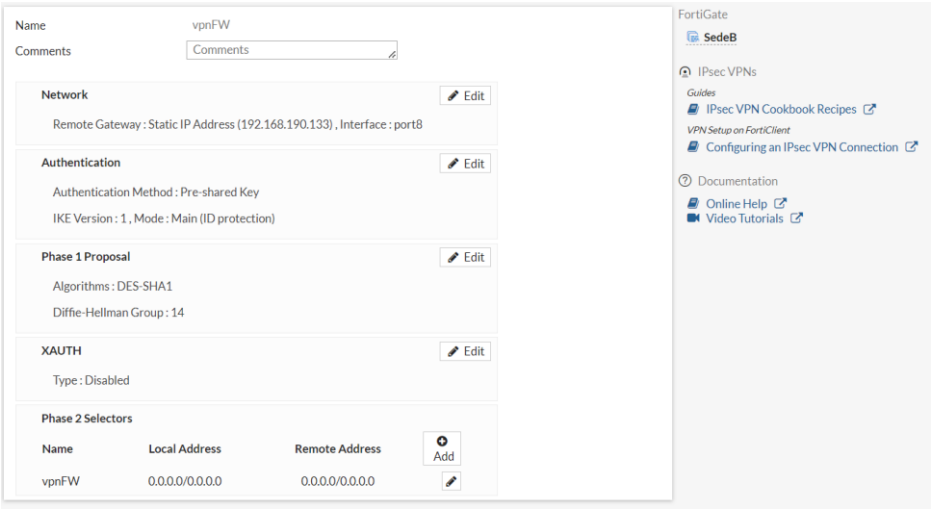


Figura 47: Configuración VPN sede B

En las figuras anteriores vemos la configuración del túnel VPN en ambos firewalls que actuarán como puntos finales del túnel IPsec VPN, este túnel utiliza el protocolo IPsec para garantizar la confidencialidad, integridad y autenticación de los datos transmitidos a través de redes no seguras, como Internet.

Para lograr esto, es necesario configurar los firewalls en ambas sedes. En el firewall de la sede A, se debe especificar la dirección IP remota del firewall de la sede B, que en este caso es 192.168.190.134. Además, se debe configurar la interfaz de salida del firewall de la sede A para que utilice el puerto 8, que es el puerto que tenemos conectado a internet.

Por otro lado, en el firewall de la sede B, se debe asignar la dirección IP remota del firewall de la sede A, que es 192.168.190.133. Al igual que en la sede A, se configura la interfaz de salida del firewall de la sede B para utilizar el puerto 8.

4.6.5 Políticas Firewall

Las políticas de un firewall son reglas configuradas para permitir o bloquear el tráfico de red con base en una serie de criterios predefinidos. Estas políticas determinan qué tipo de tráfico se permite o se niega en función de factores como la dirección IP de origen o destino, el puerto utilizado, el protocolo de comunicación y otras características relevantes.

La función principal de las políticas de un firewall es proteger la red y los sistemas que lo utilizan, controlando y filtrando el tráfico de red entrante y saliente. Estas políticas permiten establecer reglas personalizadas para gestionar el flujo de datos y asegurar que solo el tráfico autorizado y seguro se permita atravesar el firewall.

A continuación, veremos todas las políticas que hay que configurar en el firewall para hacer funcionar las implementaciones que se han visto hasta ahora.

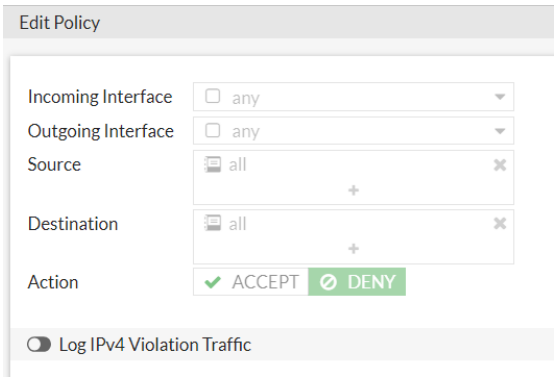


Figura 48: Política implicita

Todos los firewalls, como medida de protección, tienen una política implícita de denegar todo. Esta política establece que, a menos que se especifique lo contrario, todo el tráfico será bloqueado por defecto. Al implementar esta política, los administradores de red tienen un mayor control sobre el tráfico y pueden configurar reglas de firewall específicas según las necesidades de la organización. Esto ayuda a prevenir errores de configuración y asegura que solo el tráfico autorizado sea permitido.

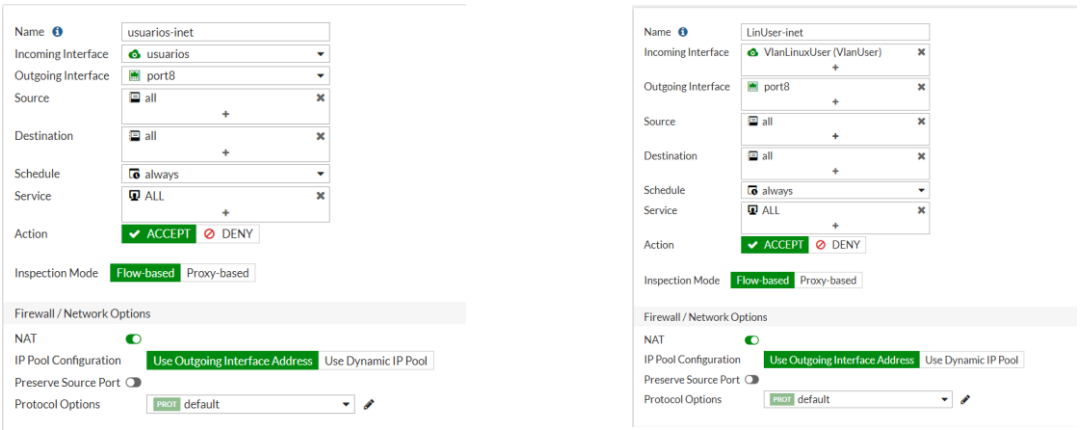


Figura 49: salida a internet usuarios

En las imágenes de la figura 49, podemos ver la configuración para que la VLAN de usuarios de ambas sedes, es decir, las VLAN 10 y 11. En esta configuración estamos permitiendo todo el tráfico que le llega al firewall desde ambas VLANs y sale por el puerto 8, que es el que sale a internet.
Al tratarse de una política con tráfico dirigido a internet es necesario tener activa la función NAT de enmascaramiento. Esta consiste en coger una dirección IP privada y traducirla a una dirección IP pública o viceversa, una función necesaria para que nuestros dispositivos en la red con IP privadas se comuniquen a través de internet.

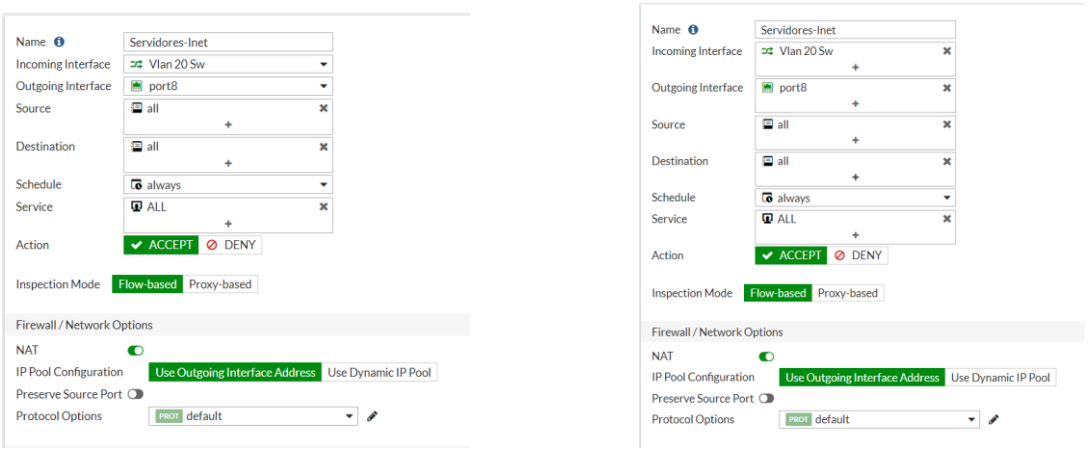


Figura 50: Salida a internet servidores

Del mismo modo habrá que crear una política en ambos firewalls para permitir la salida a internet de los servidores. La configuración es la misma para ambas sedes ya que tenemos una extensión de la VLAN 20 entre sedes. Además, también habrá que activar la función NAT para el tráfico enviado hacia internet.

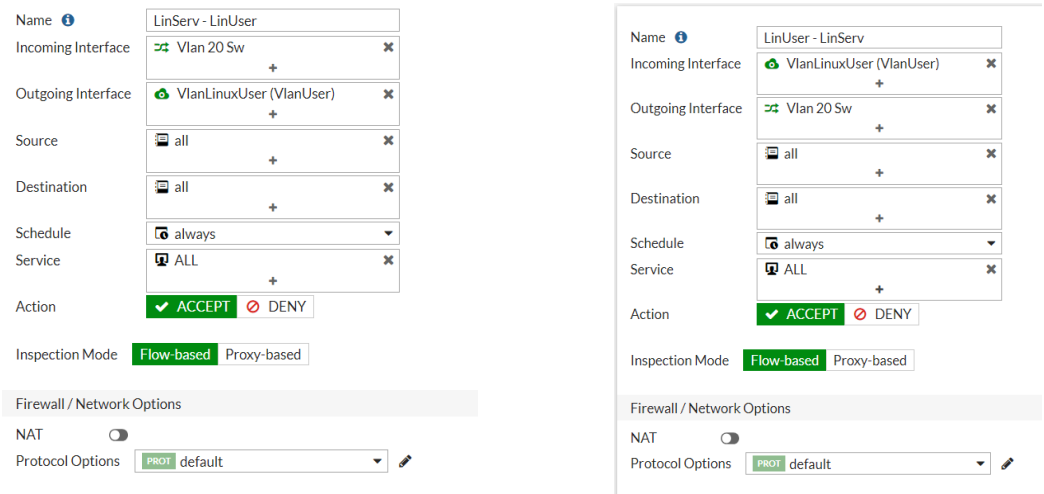


Figura 51: Conexión usuarios – servidores (Linux)

La figura anterior representa mediante dos capturas la política que permite el tráfico entre los usuarios y los servidores con sistema operativo Linux ubicados en la sede B. Es necesarios ser muy explícito en cuanto a la configuración de políticas de un firewall, esto se debe a que por defecto bloquea todo el tráfico. Por lo tanto, es necesario crear dos políticas diferentes que permitan tanto el tráfico de la VLAN de usuarios como el tráfico de la VLAN de servidores. Al ser una política que permite tráfico dentro de la LAN no es necesario activar la función NAT.

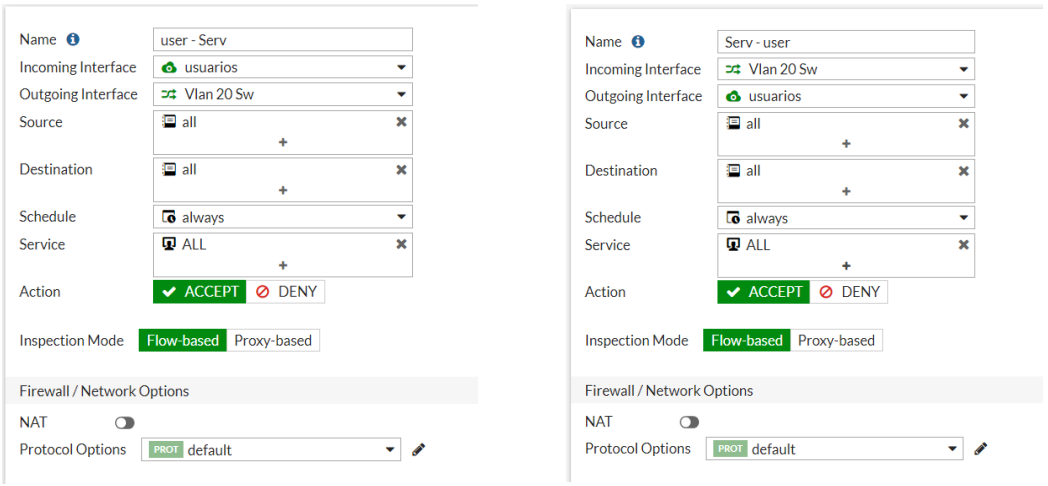


Figura 52: Conexión usuarios – servidores (Windows)

En este caso, la figura muestra la conexión entre usuarios y servidores, pero de la sede A, los cuales utilizan un sistema operativo Windows. Del mismo modo que en la otra sede es necesario crear dos políticas contrarias representando los dos sentidos del tráfico y sin la función NAT activa.

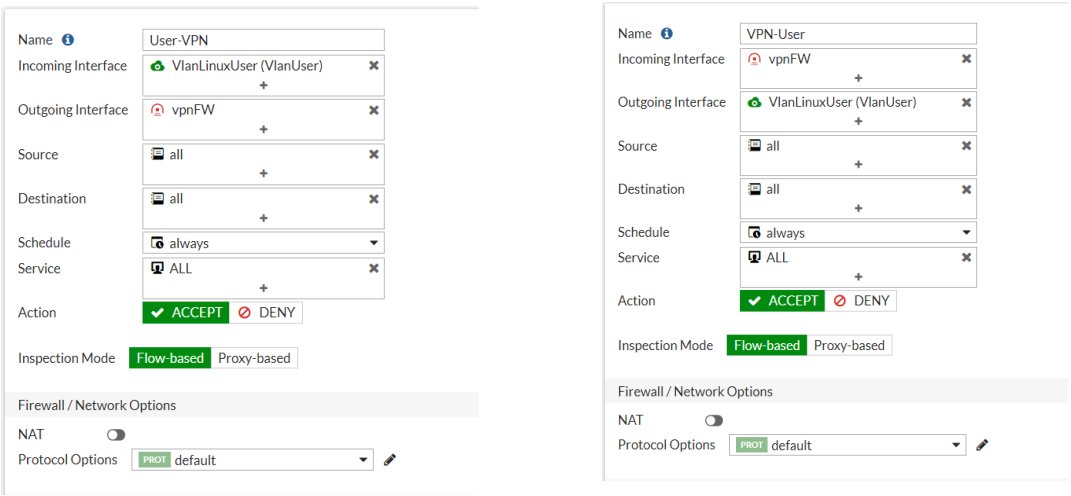


Figura 53: Conexión usuarios – túnel VPN (sede B)

En la figura anterior, la conexión para la transmisión de datos en ambos sentidos. En este caso no se aplica la función NAT debido a que modifica las direcciones IP de origen o destino de los paquetes de datos, lo cual puede causar problemas en la conexión VPN. Al aplicar NAT, se alteran los encabezados de los paquetes, lo que interfiere con el enrutamiento adecuado a través del túnel VPN y puede provocar fallas en la transmisión de datos.

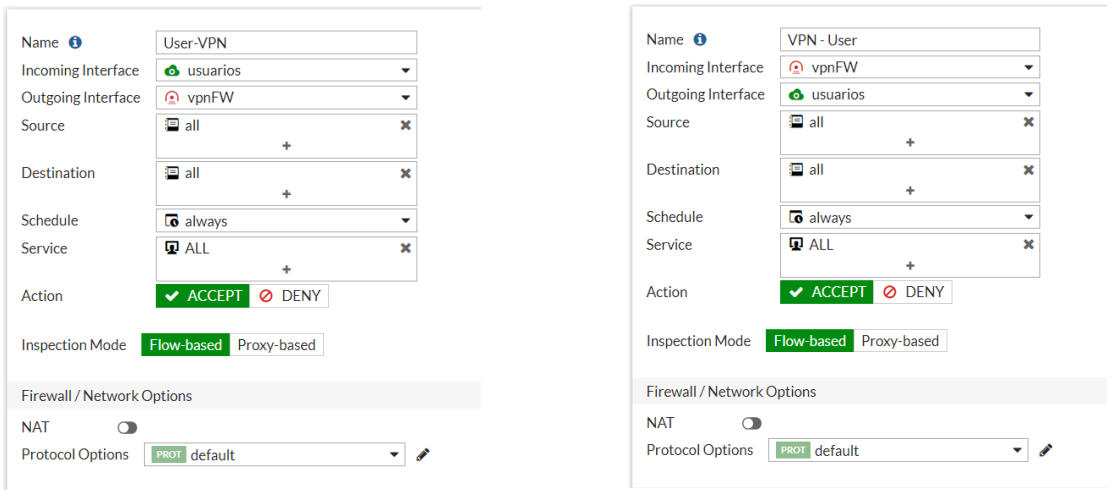


Figura 53: Conexión usuarios – túnel VPN (sede A)

Lo mismo sucede en la sede A, en este caso el único cambio con respecto a la figura 52, es que en la sede A realizaremos la conexión con la VLAN de usuarios que tienen sistema operativo Windows.

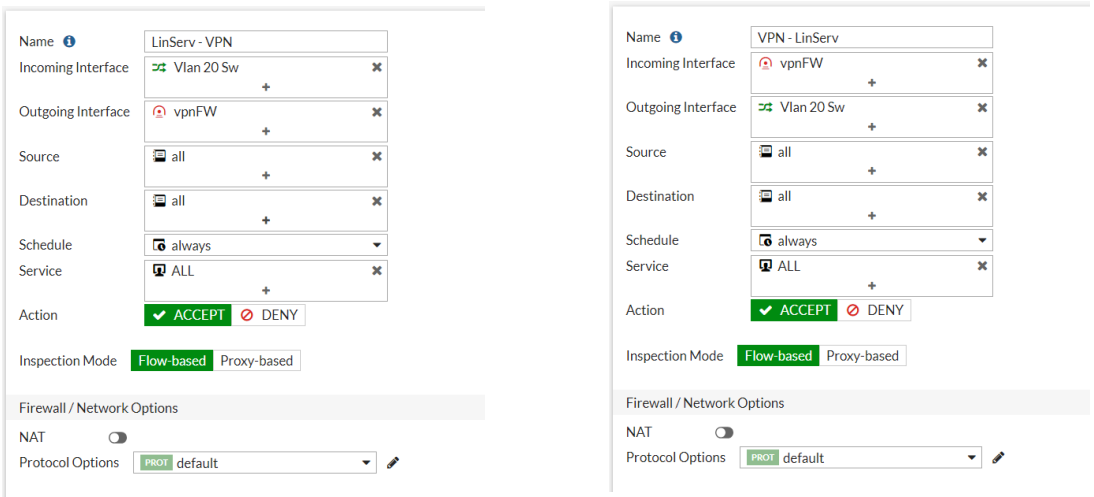


Figura 54: Conexión servidores – túnel VPN (sede B)

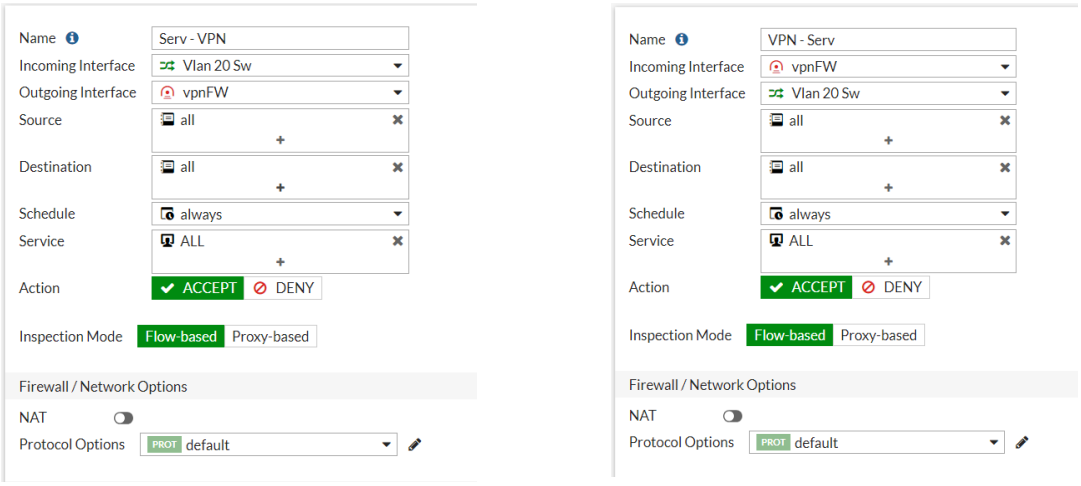


Figura 55: Conexión servidores – túnel VPN (sede A)

Finalmente habrá que crear una política que conecte los servidores de ambas sedes con el túnel VPN. En este caso al enviarse el tráfico a través del túnel es importante desactivar la función NAT del mismo modo que las políticas que conectan los usuarios con el túnel VPN.
De esta forma, se consigue tener todos los dispositivos conectados entre sí, y que todos tengan salida a internet, consiguiendo recrear una red empresarial funcional.

Teniendo en cuanta que el objetivo principal de este proyecto mostrar las posibilidades que tiene este entorno sin tener que invertir en licencias ni asumir ningún coste, hay que cuenta que la versión gratuita del servicio solo ofrece la posibilidad de crear un máximo de 10 políticas en el firewall. Esta limitación tiene implicaciones significativas en términos de administración y configuración de la seguridad de la red.
Al tener un límite de 10 políticas en el firewall, es crucial priorizar y planificar cuidadosamente la implementación de las reglas. Se deben considerar cuidadosamente los requisitos de seguridad y las necesidades de la red para garantizar que las políticas seleccionadas aborden los aspectos más críticos y fundamentales de la protección de la red.

4.6.6 Rutas estáticas

Una ruta estática es una entrada manual en la tabla de enrutamiento de un dispositivo de red, como un enrutador o un firewall. Se utiliza para especificar la dirección IP de un destino de red y la dirección IP del próximo salto o gateway necesario para alcanzar ese destino. A diferencia de las rutas aprendidas automáticamente a través de protocolos de enrutamiento dinámico, las rutas estáticas se configuran manualmente por un administrador de red.

Las rutas estáticas son comúnmente utilizadas cuando se necesita enrutar el tráfico desde una red hacia una red de conexión única, donde solo hay una ruta de entrada y salida. Esto evita la sobrecarga de tráfico generada por los protocolos de enrutamiento. Se configura una ruta estática para establecer conectividad con un enlace de datos que no está directamente conectado al enrutador.

En nuestra red son necesarias para lograr la comunicación entre las sedes, se deben configurar rutas estáticas en cada firewall para indicar la dirección IP de la sede remota y la interfaz o dirección IP del otro firewall como el próximo salto. Esto permite que los paquetes de datos se envíen al firewall remoto y se enruten hacia la red de la sede de destino.

Destination	Gateway IP	Interface	Status
IPv4 3			
0.0.0.0/0	Dynamic Gateway (192.168.190.2)	port8	Enabled
21.21.21.0/24	0.0.0.0	vpnFW	Enabled
30.30.30.0/24	0.0.0.0	vpnFW	Enabled

Figura 56: Configuración rutas estáticas sede A

Destination	Gateway IP	Interface	Status
IPv4 3			
20.20.20.0/24	0.0.0.0	vpnFW	Enabled
0.0.0.0/0	Dynamic Gateway (192.168.190.2)	port8	Enabled
30.30.30.0/24	0.0.0.0	vpnFW	Enabled

Figura 57: Configuración rutas estáticas sede B

La configuración de las rutas estáticas en las figuras 56 y 57, con destino a las VLANs y utilizando un gateway de 0.0.0.0 en una interfaz VPN, implica que el tráfico dirigido a direcciones IP dentro de las redes asociadas a las VLANs se enruta directamente a través de la interfaz VPN sin necesidad de un gateway adicional ya que interfaz VPN se encarga de enrutar todo el tráfico de manera segura hacia las direcciones IP de las VLANs, actuando como la puerta de enlace predeterminada para esas redes. Esta configuración se emplea para enrutar el tráfico de una red específica a través de una conexión VPN segura.

Por otro lado, para dar salida a Internet desde una red local, se configura una ruta estática con destino 0.0.0.0/0, lo cual significa que cualquier paquete que no coincida con una ruta específica utilizará esta ruta como la ruta de salida predeterminada. Se utiliza una dirección IP dinámica como gateway, que actúa como el punto de entrada/salida hacia Internet. Además, se configura el puerto 8 como interfaz, que es la conexión directa a Internet desde el enrutador o dispositivo de red. Esto permite que los paquetes de datos salgan de la red local a través del gateway y la interfaz designada hacia Internet.

Capítulo 5. Conclusión y futuros trabajos

En conclusión, este proyecto de fin de grado ha logrado cumplir satisfactoriamente los objetivos planteados inicialmente. Se ha estudiado y analizado en detalle el emulador EVE-NG como una herramienta de simulación de redes, capaz de crear y ejecutar topologías complejas en un entorno virtualizado. Además, se ha utilizado VMware como plataforma principal para la implementación de la máquina virtual y se ha demostrado su versatilidad y seguridad en la creación y ejecución de sistemas operativos y aplicaciones.

El objetivo principal de este proyecto consistía en mostrar las amplias posibilidades que ofrece EVE-NG para el diseño, configuración y prueba de soluciones de redes en un ambiente seguro y controlado. Esto se ha logrado al diseñar, configurar y poner en funcionamiento una red empresarial virtualizada, demostrando así la capacidad de virtualización de redes para crear una solución funcional a coste cero. Esta solución puede resultar de gran interés tanto para empresas pequeñas con presupuestos limitados, como para fines educativos y profesionales, como el departamento de redes. Con EVE-NG, es posible replicar configuraciones de clientes y resolver problemas en las redes sin interrumpir su funcionamiento, lo que representa una ventaja significativa.

Durante el desarrollo del proyecto, se ha demostrado que es posible construir una red empresarial virtualizada sin incurrir en costes adicionales, como licencias, servidores o hardware físico para montar un laboratorio de pruebas. La utilización de dispositivos virtuales como firewalls, switches y PCs ha permitido crear una red funcional, optimizando el rendimiento y el consumo de recursos. La presentación esquemática de la red ha facilitado su comprensión, y se han detallado tanto la selección como la configuración de cada dispositivo, teniendo en cuenta su rendimiento y consumo de recursos. EVE-NG ha demostrado ser un entorno virtual de gran potencial y versatilidad para la simulación de redes. Su capacidad para diseñar, configurar y probar soluciones de redes en un ambiente seguro y controlado, sin costes adicionales, lo convierte en una herramienta altamente valiosa. Con su amplia gama de posibilidades, EVE-NG se posiciona como una opción destacada para empresas, educadores y profesionales en la resolución de problemas y la optimización de redes. En resumen, EVE-NG ofrece un entorno virtual poderoso que abre las puertas a un mundo de oportunidades en la simulación y gestión de redes.

A pesar de haber alcanzado los objetivos planteados en este proyecto, existen varias líneas de trabajo futuro que podrían explorarse para mejorar y expandir el uso de EVE-NG y potenciar su aplicabilidad en diferentes contextos:

Ampliar la variedad de dispositivos y topologías: En este proyecto se han utilizado dispositivos virtuales básicos como firewalls, switches y PCs. Sería interesante investigar y agregar nuevos dispositivos virtuales, como routers avanzados, servidores de aplicaciones o sistemas de gestión de red, para crear topologías más complejas y realistas. Esto permitiría simular y probar escenarios más diversos y desafiantes.

Un área de investigación futura prometedora sería el desarrollo de trabajos que se enfoquen en utilizar dispositivos virtuales con licencias para crear escenarios de red más realistas en EVE-NG. Al simular entornos de red con licencias, se podría replicar de manera precisa el comportamiento y las restricciones de los dispositivos físicos utilizados en implementaciones reales. Esto permitiría a los profesionales de redes experimentar y probar configuraciones, implementaciones y soluciones en un entorno controlado pero auténtico, lo que a su vez ayudaría a mejorar su capacidad para resolver problemas y enfrentar desafíos en entornos de producción.

También sería interesante el estudio de casos de uso específicos: Se puede realizar un análisis más profundo de casos de uso específicos en diferentes ámbitos, como implementación de servicios en la nube y la implementación de herramientas de análisis de tráfico y monitoreo de red, entre otros. Al explorar estos casos de uso, se podrían identificar nuevos desafíos y requerimientos, lo que podría conducir a mejoras y adaptaciones en la funcionalidad de EVE-NG.

Actualmente, la computación en la nube desempeña un papel fundamental en el despliegue de infraestructuras de red y servicios. Por lo tanto, sería valioso desarrollar trabajos que permitan la simulación y emulación de entornos en la nube en EVE-NG. Esto podría implicar la creación de imágenes de dispositivos virtuales compatibles con proveedores de servicios en la nube. Al simular estas configuraciones en EVE-NG, los profesionales de redes podrían diseñar, implementar y probar soluciones en entornos en la nube de forma segura y controlada. La investigación también podría abordar aspectos como la gestión de recursos en la nube, la interconexión de redes virtuales y la integración de servicios adicionales ofrecidos por los proveedores en la nube.

Por otro lado, tendríamos el análisis de tráfico y monitoreo de red son actividades cruciales para garantizar el rendimiento, la seguridad y la resolución de problemas. Sería interesante desarrollar trabajos que permitan la captura, visualización y análisis de tráfico en EVE-NG, con el objetivo de proporcionar una experiencia más realista y detallada. Esto podría incluir la integración de herramientas de captura de paquetes, como Wireshark, directamente en los nodos virtuales de EVE-NG, lo que permitiría el análisis en tiempo real de los flujos de tráfico generados en los escenarios de red. Además, se podrían explorar técnicas de visualización avanzadas para representar gráficamente el tráfico de red y detectar patrones o anomalías de manera más efectiva.

Capítulo 6. Bibliografía

Capítulo 1. Introducción

https://www.vmware.com/es/topics/glossary/content/network-virtualization.html

https://docs.oracle.com/cd/E26921_01/html/E25833/gfkbw.html

https://www.telefonica.com/es/sala-comunicacion/blog/las-ventajas-de-la-virtualizacion-de-la-red/

Capítulo 2. EVE-NG

https://www.eve-ng.net/

Capítulo 4. Desarrollo

https://www.vmware.com/es/products/workstation-player/workstation-player-evaluation.html

https://winscp.net/eng/index.php

https://www.eve-ng.net/

https://www.putty.org/

https://mikrotik.com/

https://docs.fortinet.com/document/fortigate/6.4.7/fortios-release-notes/236526

https://www.fortinet.com/lat/products/next-generation-firewall

Anexo

Funciones de red. Las funciones de red son los distintos servicios y capacidades que se proporcionan en una red de telecomunicaciones como la conmutación de paquetes, el filtrado de paquetes, la autenticación de usuarios, la optimización del tráfico, entre otros.

LAN. Una LAN (Local Area Network) es una red de computadoras y dispositivos que permite la comunicación de dispositivos en un área geográfica limitada, permitiendo la comunicación y el intercambio de información entre ellos.

VLAN. Una VLAN (Virtual Local Area Network) es una tecnología de redes que permite segmentar una red física en múltiples redes virtuales, aislando grupos de dispositivos. Esto se logra mediante la configuración de switches de red para que los dispositivos asignados a una VLAN específica puedan comunicarse entre sí, independientemente de su ubicación física

Enlace modo trunk. Un enlace modo trunk es una configuración de red que permite transmitir múltiples VLAN a través de un solo enlace de red. El enlace modo trunk etiqueta los paquetes de datos con información adicional, como etiquetas de VLAN, para identificar y separar las diferentes VLAN durante la transmisión de datos. Esto permite el paso simultáneo de múltiples VLAN a través de un único enlace.

Dot1q. El protocolo Dot1q, es un estándar de etiquetado de VLAN utilizado en redes Ethernet. Permite la segmentación y el transporte de múltiples VLAN a través de una red troncal (trunk). El protocolo Dot1q agrega una etiqueta adicional de 4 bytes en el encabezado del marco Ethernet, llamada etiqueta de VLAN, que identifica la pertenencia de cada paquete a una VLAN específica.

Enlace modo acceso. Un enlace modo acceso es una configuración de puerto en un switch de red que se utiliza para conectar dispositivos finales individuales a la red. En este modo, el puerto del switch se configura para pertenecer a una única VLAN específica. Esto significa que el tráfico de red que llega a través de ese puerto se asigna a esa VLAN en particular y se limita a esa VLAN solamente.

Servidor DHCP. Un servidor DHCP (Dynamic Host Configuration Protocol) es un dispositivo o software que asigna de manera automática y dinámica las direcciones IP y otra información de configuración de red a los dispositivos que se conectan a una red, eliminando la necesidad de configurar manualmente cada dispositivo de manera individual.

Gateway. Cuando configuramos una IP, el gateway o puerta de enlace es la dirección IP del dispositivo que permite la comunicación entre nuestra red local y otras redes externas, como Internet. Actúa como el punto de salida para el tráfico de red hacia destinos fuera de nuestra red local. El gateway se encarga de enrutar los paquetes de datos correctamente, asegurando que lleguen a su destino en la red externa.

Servidor DNS. Un servidor DNS (Domain Name System) es un sistema que se encarga de traducir los nombres de dominio de Internet en direcciones IP. El servidor DNS ayuda a establecer conexiones entre dispositivos y facilita la navegación web al convertir los nombres de dominio en direcciones IP reconocibles por las máquinas.

Bridge. Un bridge, es una función de un router que permite combinar dos o más interfaces de red en un solo dominio de broadcast. Actúa como un puente virtual que conecta diferentes segmentos de red, lo que permite que los dispositivos conectados en diferentes interfaces se comuniquen entre sí como si estuvieran en la misma red local.

Protocolo IPSec. IPSec (Internet Protocol Security) es un protocolo de seguridad utilizado para establecer conexiones seguras en redes IP. IPSec opera a nivel de protocolo de red y se encarga de encapsular los paquetes IP dentro de túneles seguros. Utiliza diferentes componentes y protocolos, como Encapsulating Security Payload (ESP) y Authentication Header (AH), para garantizar la autenticación y confidencialidad de los datos transmitidos. Proporciona autenticación, confidencialidad e integridad de los datos transmitidos. IPSec se utiliza comúnmente en VPN (redes virtuales privadas) para proteger las comunicaciones en redes públicas como Internet.