NethSecurity como Plataforma de Seguridad Perimetral: Implementación de OpenVPN Road Warrior en Linux con QEMU/KVM

Wilfredo Torres Ariza
e-mail: wtorresar@unadvirtual.edu.co

RESUMEN: *Este artículo describe el diseño e implementación de los servicios de seguridad perimetral y administración de redes utilizando tecnologías de código abierto, NethSecurity como firewall principal sobre un laboratorio de red montado en un host Linux Ubuntu, utilizando la plataforma de virtualización QEMU/KVM.*
La instalación de la Máquina virtual de NethSecurity, la más reciente iteración de la plataforma de seguridad Nethserver, permite evaluar la instalación de utilidades de seguridad como OpenVPN Server, DHCP Server, DNS Server y Controladores de Dominio, en este artículo nos centraremos en la implementación del servidor VPN OpenVPN Road Warrior, integrado en la plataforma NethSecurity y su utilización para conectarse de forma remota a una red local.
.

PALABRAS CLAVE: Firewall, Linux, NethSecurity, OpenVPN.

1 INTRODUCCIÓN

La seguridad perimetral es un aspecto importante al realizar la planeación de la infraestructura digital de cualquier empresa, al implementar infraestructuras seguras, flexibles y escalables es necesario tener en cuenta los riesgos inherentes al trabajo distribuido, los accesos remotos y la información contenida en los servidores o equipos dentro de las instalaciones, para de esta manera manejarlos de forma que se reduzca la probabilidad de un evento inseguro que afecte el funcionamiento normal de los equipos.

Las soluciones de software libre se han venido estableciendo como alternativas confiables, para la implementación de este tipo de herramientas tenemos a disponible un sin número de opciones, dentro de ellas Nethserver ha venido desarrollándose como una plataforma de seguridad con soporte de la comunidad, manuales en línea y amplia documentación publicada tanto en español como en inglés.

NethServer se estableció como una opción de seguridad desde 2013, el proyecto llegó a la versión 7.9 siendo parte del sistema operativo para lo cual era necesario instalarlo sobre la distribución CentOS minimal o directamente desde una ISO precompilada que se puede descargar aun de la página web del proyecto nethserver.org.

Sin embargo, CentOS 7 llegó al final de su vida util (EOL) el 30 de junio de 2024 por esto el equipo de desarrollo decidió separar la plataforma de seguridad a un producto independiente denominado NethSecurity que surge como una distribución dedicada exclusivamente a seguridad de red basada en OpenWrt, destinada a remplazar soluciones comerciales como pfSense, OPNsense, Fortinet Fortigate, Sophos Firewall.

Nethsecurity incorpora Firewall Avanzado, Multi.WAN, VPN WireGuard e IPsec, IDS/IPS con Suricata, Filtrado DNS, QoS, VLANs, Portal Cautivo, integración cloud y alta disponibilidad.

.

2 INSTALACIÓN DE NETHSECURITY

2.1 REQUISITOS DEL SISTEMA

Ref. [1] Actualmente NethSecurity está disponible únicamente para arquitectura x86-64 con los siguientes requerimientos mínimos de hardware:

- 1 vCPU/Cores
- 1 GB de memoria RAM
- 1 GB de espacio en disco
- 2 tarjetas de red Ethernet

Los requerimientos recomendados son:

- 2 vCPU/Cores
- 2 GB de memoria RAM
- 1 GB de espacio en disco y una USB adicional para datos persistentes como logs.

2.2 DESCARGA DE LA IMAGEN DE INSTALACIÓN

La descarga se hace directamente de la página del proyecto en https://nethsecurity.org/download donde encontraremos además el enlace a la documentación del proyecto que contiene el manual de instalación y configuración de las herramientas de seguridad.

El archivo descargado se llama **nethsecurity-8.7.2-x86-64-generic-squashfs-combined-efi.img.gz** es una imagen de disco comprimida a la cual se le puede realizar el chequeo de integridad con el hashfile que se puede descargar del enlace https://updates.nethsecurity.nethserver.org/stable/8.7.2/targets/x86/64/sha256sums, el comando utilizado para la verificación es:

~$ **grep** nethsecurity-8.7.2-x86-64-generic-squashfs-combined-efi.img.gz sha256sums | sha256sum -c

[2]

2.3 ENTORNO VIRTUAL PARA LA INSTALACIÓN

Para realizar la instalación del sistema NethSecurity en un entorno virtual que nos permita realizar las pruebas con las herramientas de seguridad a considerar utilizamos la plataforma de virtualización incluida en Ubuntu Linux, QEMU/KVM, para realizar la instalación del gestor de máquinas virtuales utilizamos el comando:

~$ **sudo** apt install qemu-kvm libvirt-daemon-system libvirt-clients bridge-utils virt-manager -y

Luego iniciamos el gestor con el comando:

~$ virt-manager

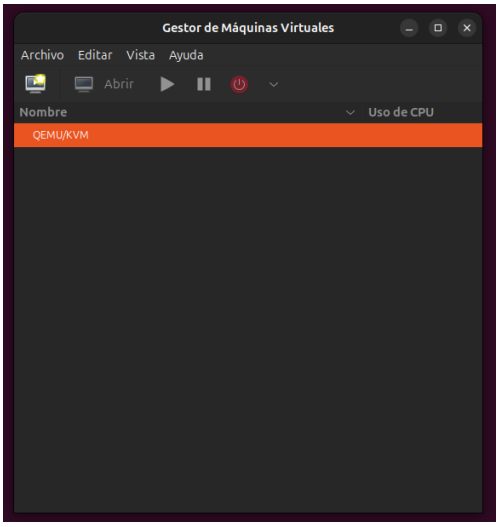


Figura 1. Interfaz gráfica gestor de máquinas virtuales

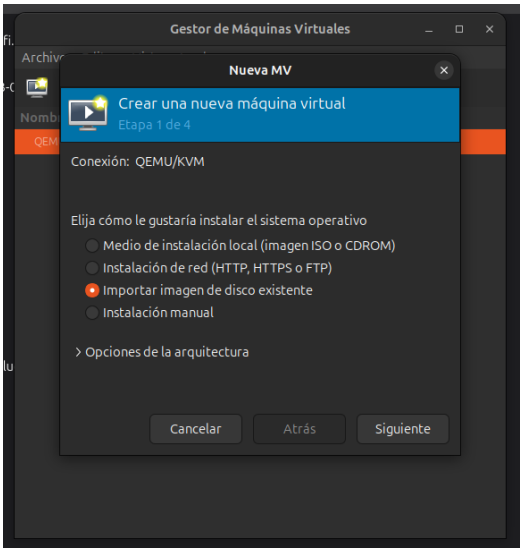


Figura 2. Creación de máquina virtual

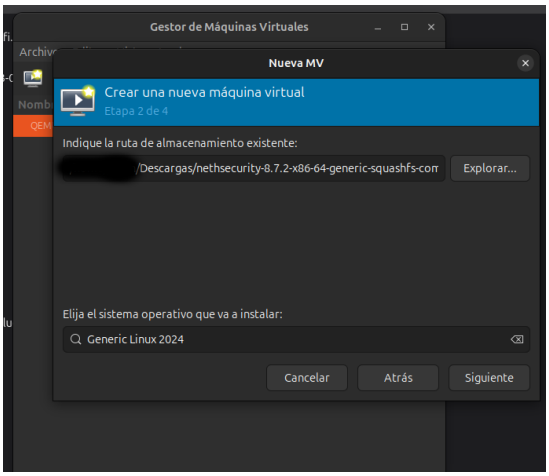


Figura 3. selección de archivo de imagen

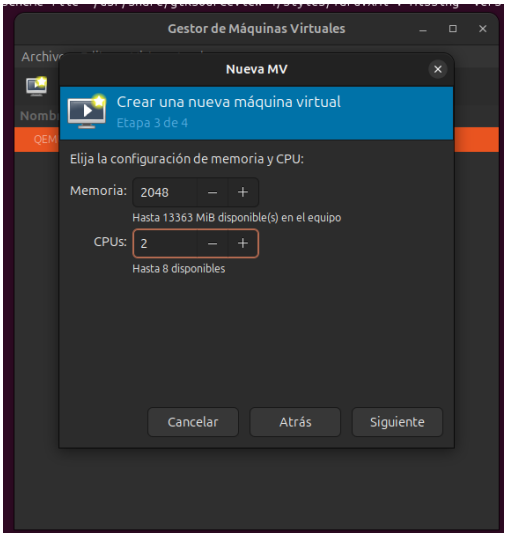


Figura 4. Memoria y CPUs

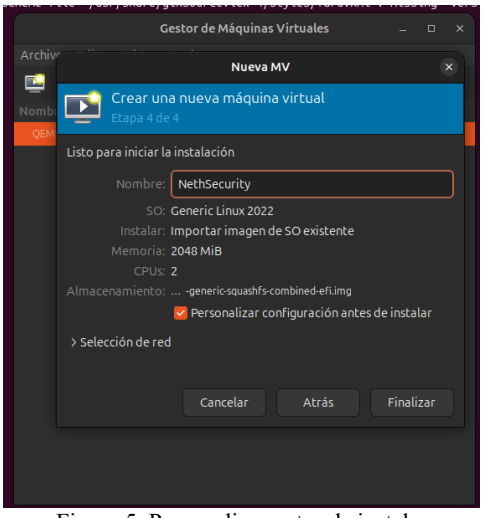


Figura 5. Personalizar antes de instalar

Se debe agregar una nueva interfaz de red para simular las dos redes a las que estará conectada la máquina virtual, una WAN que será conectada al modem de internet de nuestro proveedor

de acceso y que para el caso del laboratorio será la interfaz conectada en modo NAT (Fig.6) y una LAN que será la interfaz conectada en modo Bridge o puente a la red preparada para este laboratorio. (Fig. 7)

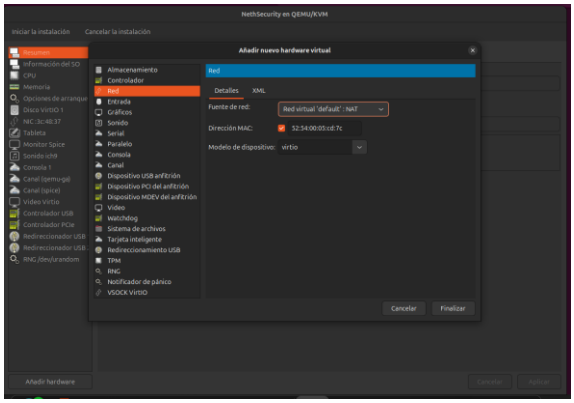


Figura 6. Agregar segunda tarjeta de red en modo NAT

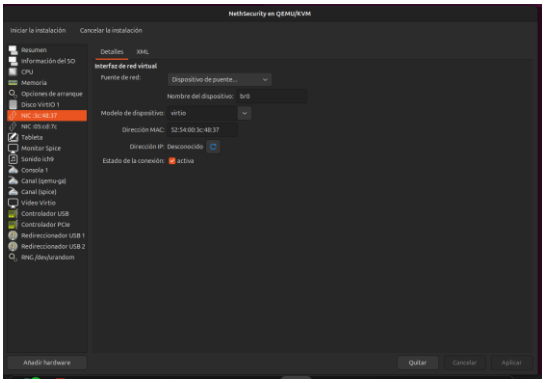


Figura 7. Primera tarjeta de red en modo Bridge

2.4 ARRANQUE DE LA PLATAFORMA EN EL ENTORNO VIRTUAL.

Al iniciar por primera vez la plataforma nethsecurity vamos a tener acceso por medio de la consola de comandos, en la Fig. 8 podemos ver cómo se puede seleccionar el arranque normal o el arranque seguro para solucionar problemas de sistema.

Una vez iniciado el sistema operativo, la plataforma quedará en modo de espera de interacción (Fig. 9) al presionar la tecla enter del teclado nos pide usuario para hacer login, la instalación inicial trae configurados por defecto los valores de usuario: root y contraseña: Nethesis,1234 al ingresar con estas credenciales podremos verificar los valores de dirección IP que han tomado las interfaces de red configuradas.

Usar el comando ifconfig para ver las direcciones IP de las diferentes interfaces de red (Fig. 11)

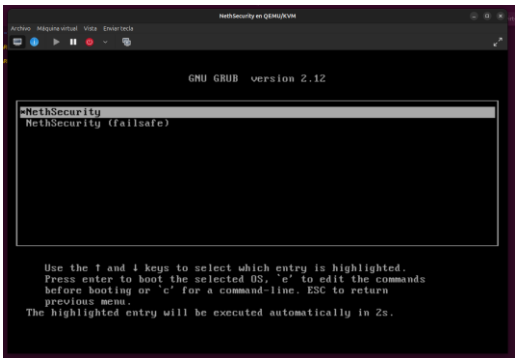


Figura 8. arranque del sistema GRUB

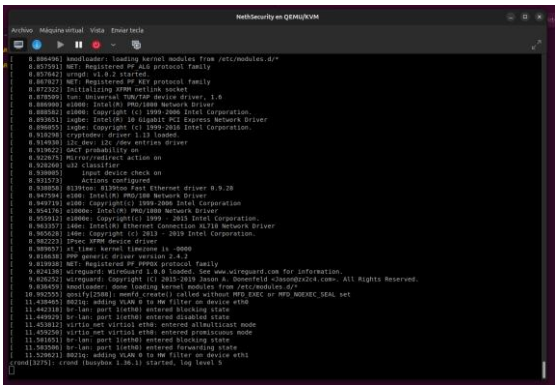


Figura 9. sistema en espera de interacción

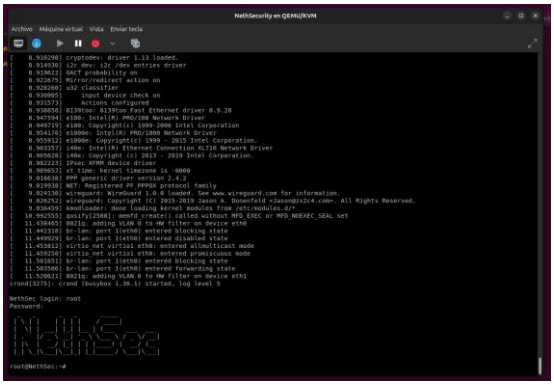


Figura 10. Sistema con usuario autenticado esperando comandos

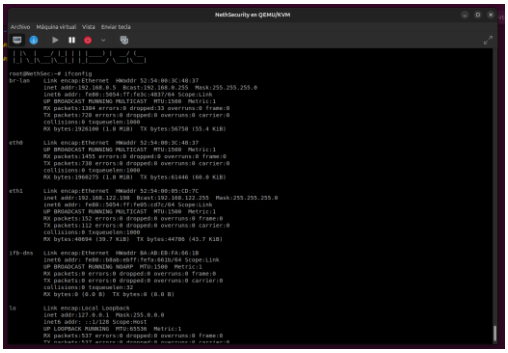


Figura 11. Comando ifconfig para verificar las IP que ha tomado el sistema

La interfaz en modo NAT (red WAN) en este caso tomó la dirección 192.168.122.198 y será la que nos de acceso a internet a través de la conexión a internet del host y la interfaz en modo bridge (red LAN) nos permitirá conectar con los demás dispositivos conectados a la red de ya que su direccionamiento coincide con las direcciones asignadas por DHCP a los demás equipos conectados al modem del proveedor de internet. En este caso la IP del servidor NethSecurity es 192.168.0.5

2.5 CONFIGURACIÓN A TRAVÉS DE LA INTERFAZ WEB DE NETHSECURITY

La url para la interfaz web de NethSecurity es https://[IP_DEL_SERVIDOR]:9090
Para el caso del laboratorio es: https://192.168.0.5:9090 al acceder a esta URL desde un navegador en cualquier equipo de la red LAN podremos ingresar, sin embargo debido a que no se han instalado certificados de seguridad válidos al ingresar por primera vez aparecerá una advertencia de seguridad en el navegador, se debe seleccionar omitir la advertencia y continuar al sitio (Fig. 12)

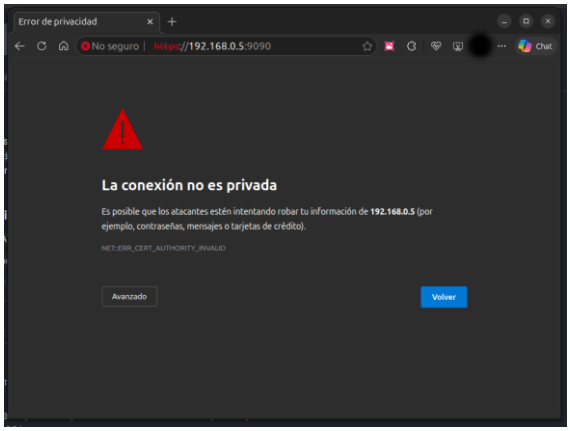


Figura 12. Advertencia de seguridad del navegador

Al avanzar se presentará la ventana de login de la plataforma NethSecurity, se deben usar los mismos datos de acceso que usamos al acceder por consola en la Figura 9. usuario: root y contraseña: Nethesis,1234 una vez ingresamos la plataforma nos va a dar un asistente de configuración inicial para cambiar la contraseña por defecto (Fig 15) configurar las opciones de acceso SSH (Fig.16) Habilitar el acceso a la interfaz web desde la red WAN, solo se habilita para configuración desde una ubicación remota (Fig. 17) acceso a través del puerto 443 (Fig. 18) .
Una vez terminado el asistente de configuración inicial, estaremos en la interfaz principal de la plataforma NethSecurity. (Fig. 20)

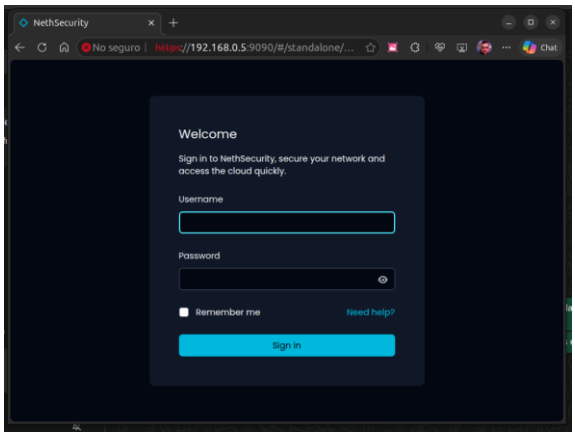


Figura 13. Página de Login del sistema.

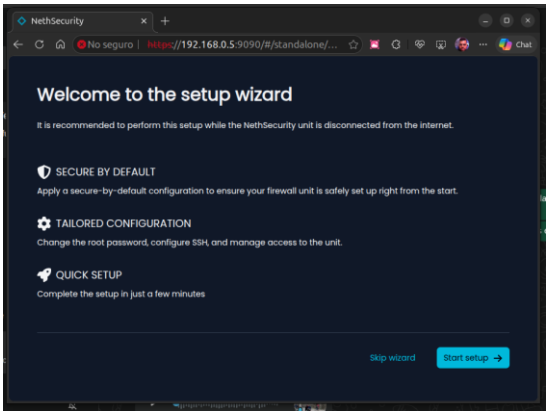


Figura 14. Setup wizard

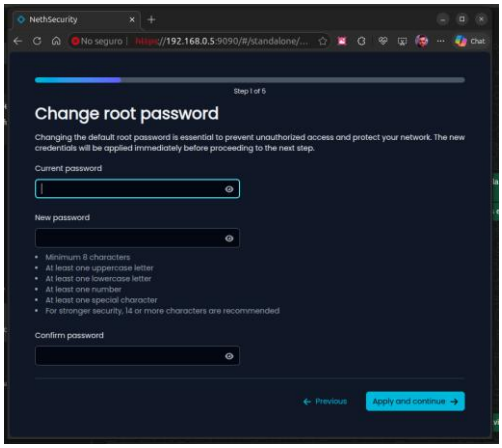


Figura 15. cambiar el password por defecto

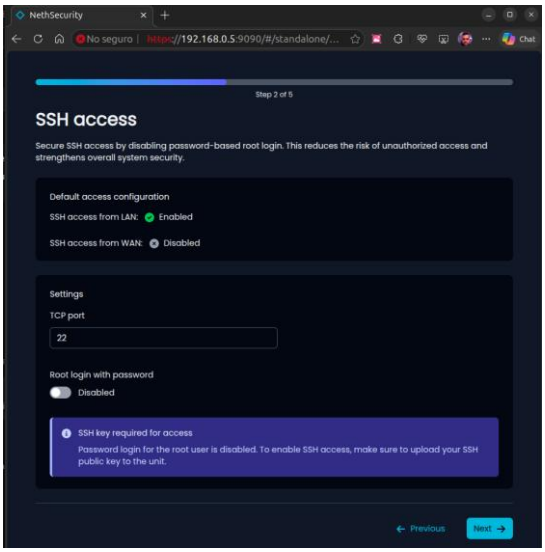


Figura 16. configurar acceso SSH

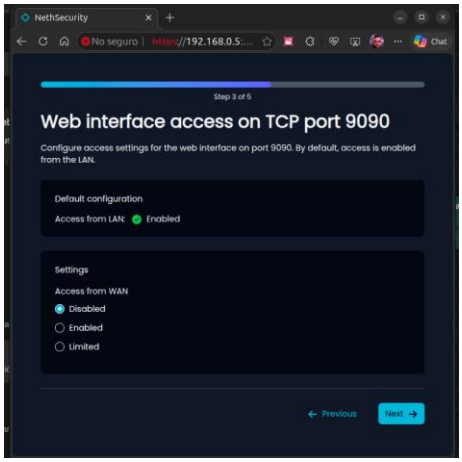


Figura 17. Acceso a la interfaz Web

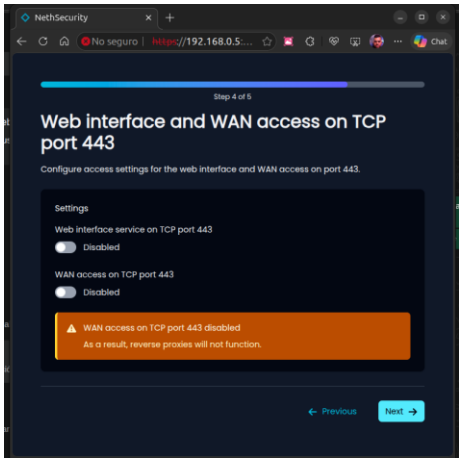


Figura 18. Acceso en puerto 443

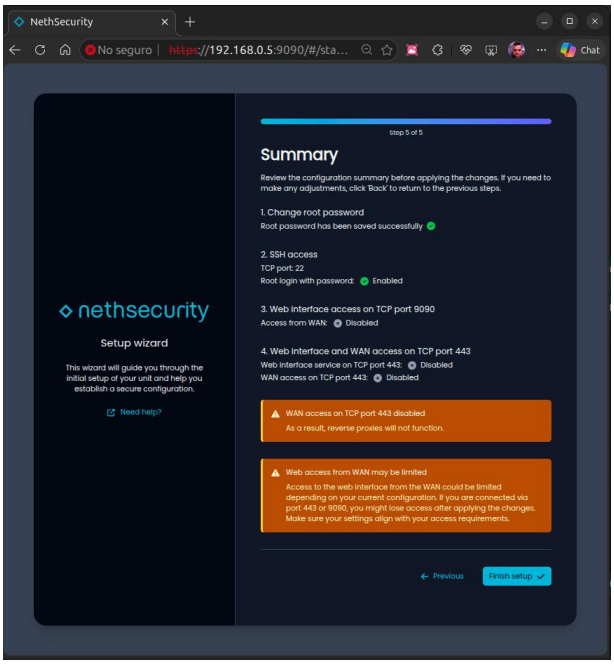


Figura 19. Resumen

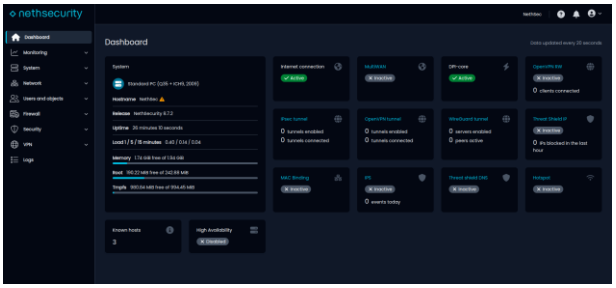


Figura 20. Interfaz principal

La Interfaz gráfica de NethSecurity nos permite configurar las diferentes funciones habilitadas para la plataforma, para habilitar el servicio de OpenVPN es necesario crear un usuario que va a identificar a cada cliente al que le vamos a dar acceso a la red VPN.

En la sección “Users and Objects” enviamos a agregar un usuario, la ventana de creación de usuario se despliega de forma lateral a la derecha de la pantalla y solo pide poner el usuario y contraseña, la contraseña debe cumplir los criterios de complejidad establecidos, como mínimo 8 caracteres, una letra mayúscula y una minúscula, un número y un carácter especial (Fig. 22)

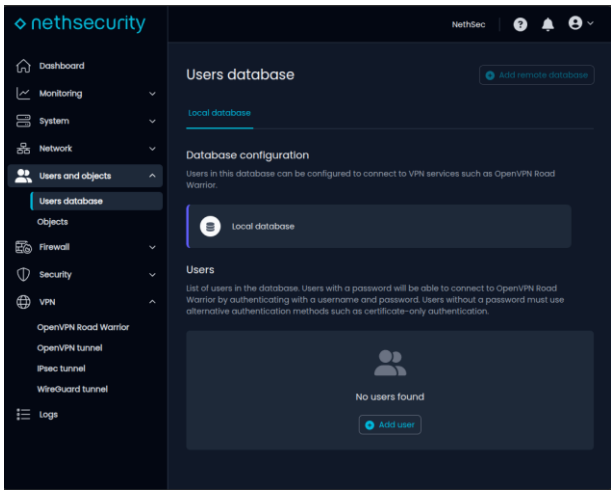


Figura 21. Creación de Usuario

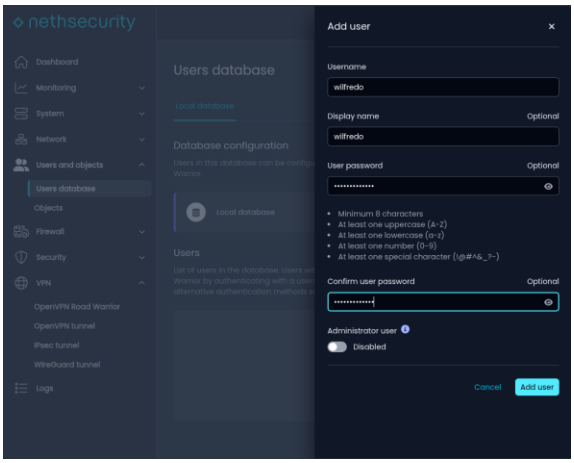


Figura 22. Creación de usuario 2

Luego de crear el usuario, vamos a la sección de VPN en el menú lateral izquierdo donde se maneja la configuración de OpenVPN Road Warrior (servidor VPN), OpenVPN tunnel, IPsec tunnel y Wireguard Tunnel.

Para los efectos de este artículo vamos a crear un servidor VPN en la sección OpenVPN Road Warrior, al crearlo nos va a solicitar la siguiente información, como se ve en la figura 24.
Nombre de servidor: laboratorio1
User database: local database (usuarios creados en el sistema)
Hay un selector que le permite crear una cuenta para cada usuario creado en el sistema (en el paso anterior)
El modo de autenticación tiene 3 opciones:
Certificado, solo usará el archivo de configuración que contiene el certificado generado para cada usuario
Usuario y password: el usuario deberá hacer login con usuario y password
Usuario, password y certificado,
Usuario y OTP (Password de un solo uso generado por el sistema.
Ver Figura 23

Los rangos de IP dinámicos configurados determinarán las IP asignadas a los clientes al momento de realizar la conexión.

Se debe asignar una IP de acceso o nombre de host para acceder al servidor VPN, para el caso utilizaremos la IP asignada por el DHCP, en caso de un servidor publicado en internet, debe usarse o la IP pública o el nombre de dominio asociado a la IP donde se encuentra el servidor.
Ver Figura 24.

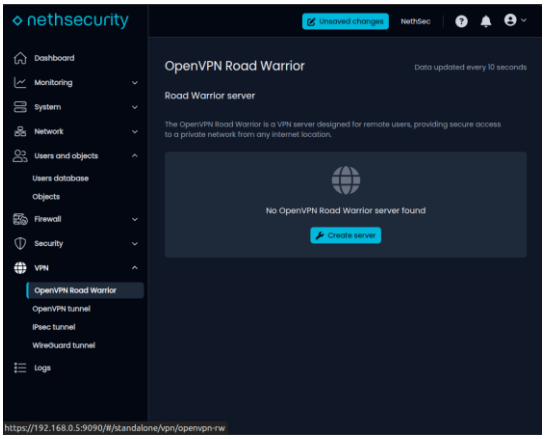


Figura 23. Creación Servidor OpenVPN Road Warrior

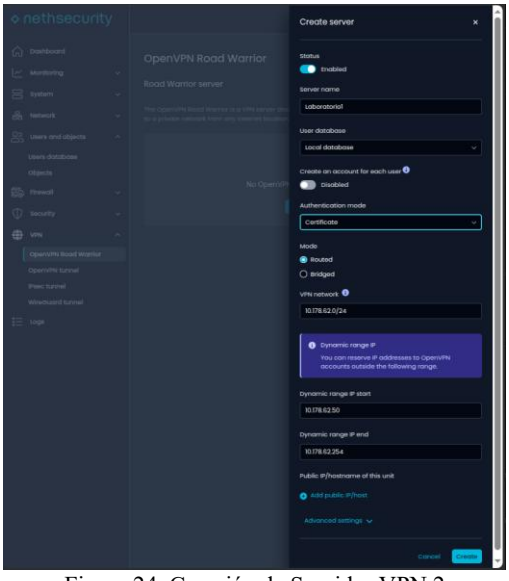


Figura 24. Creación de Servidor VPN 2

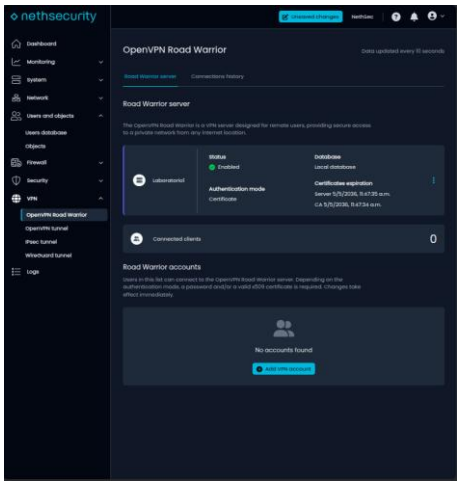


Figura 25. Servidor creado

Una vez creado el servidor se procede a crear la cuenta VPN, si no se ha chequeado la opción de crear un usuario en la figura 24, al crear el usuario permite seleccionar dentro de los usuarios del sistema, asignar opcionalmente una IP reservada y configurar los días de expiración del certificado, por defecto este valor está en 3650. Ver Figura 26.

Una vez asociado/creado el usuario VPN se debe descargar el archivo de configuración, este archivo de configuración contiene los datos de configuración necesarios para crear el perfil en la aplicación OpenVPN connect. Ver Figura 28.

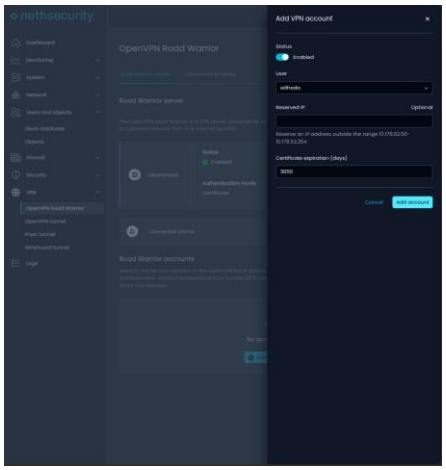


Figura 26. Asociar usuario a VPN

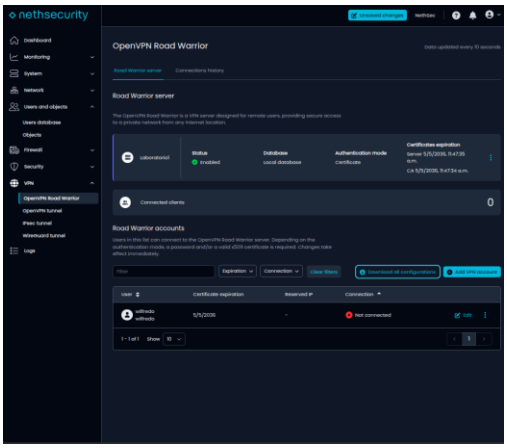


Figura 27. Descargar Archivo de configuración

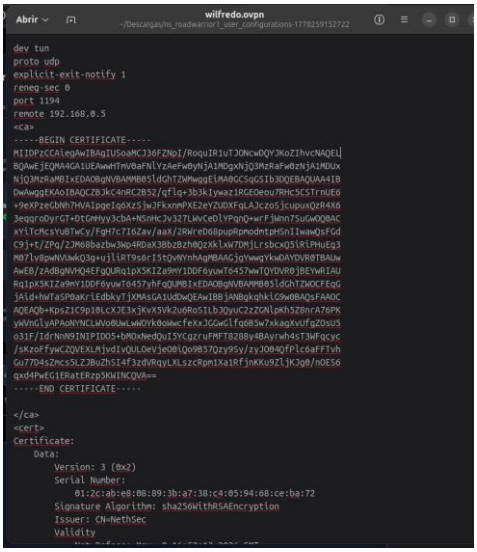


Figura 28. Archivo de configuración

2.6 CONFIGURACIÓN DEL CLIENTE VPN OPENVPN CONNECT (WINDOWS)

En entornos windows se utilizan clientes de conexión para acceder al servidor VPN, OpenVPN connect es la aplicación requerida y se puede descargar de la url https://openvpn.net/client/ aquí se descarga un archivo .msi que permite instalar la aplicación a través de un asistente de forma rápida. Ver figuras 29 a 33.

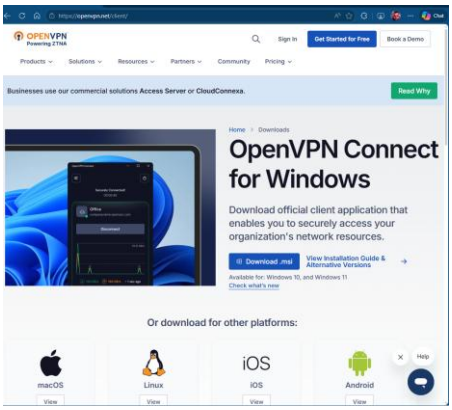


Figura 29. Sitio de descarga de Cliente VPN

Figura 30. Instalación de OpenVPN Connect

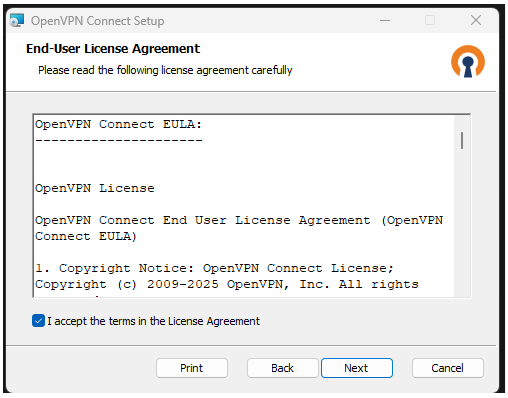


Figura 31. Aceptar términos de licencia OpenVPN Connect

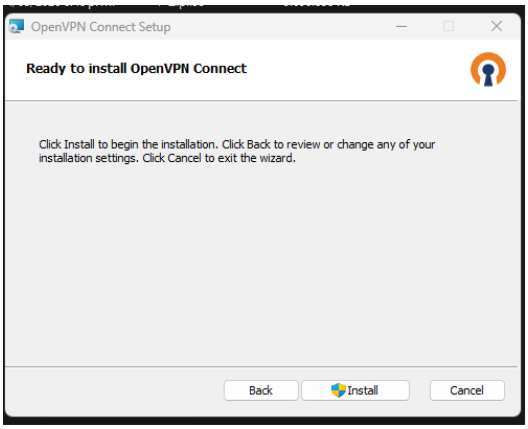


Figura 32. Iniciar la instalación de OpenVPN Connect

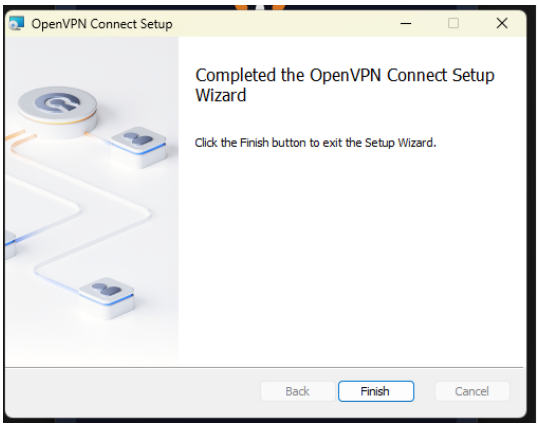


Figura 33. Finalizar la instalación de OpenVPN Connect

Una vez realizada la instalación, al abrir la aplicación aparece un diálogo para aceptar los términos y condiciones de uso de la aplicación. Fig34

En la figura 35 se púede observar la interfaz básica de la aplicación donde podemos crear el perfil de conexión para poder acceder a la red VPN, se realiza la carga del archivo de configuración generado por el servidor y esto crea automáticamente el perfil, como se observa en la figura 38

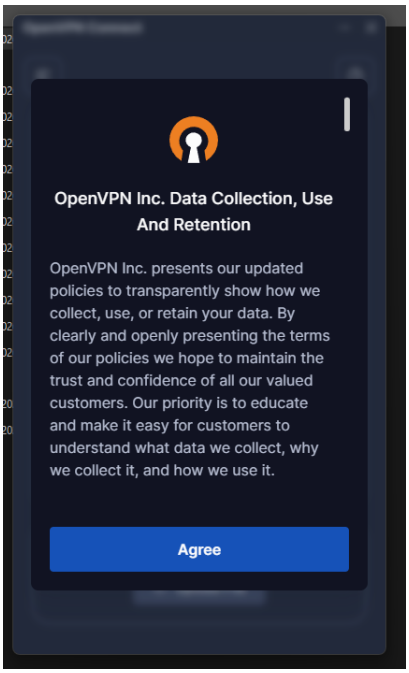


Figura 34. Terminos Aplicación OpenVPN Connect

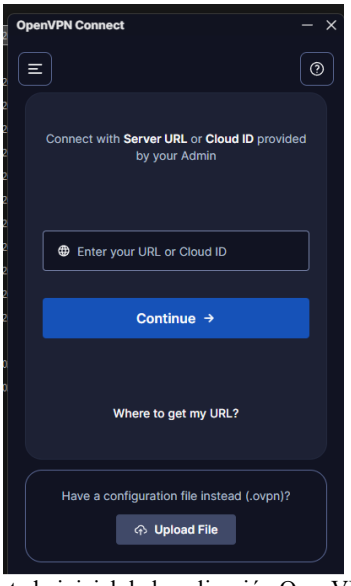


Figura 35. Estado inicial de la aplicación OpenVPN Connect

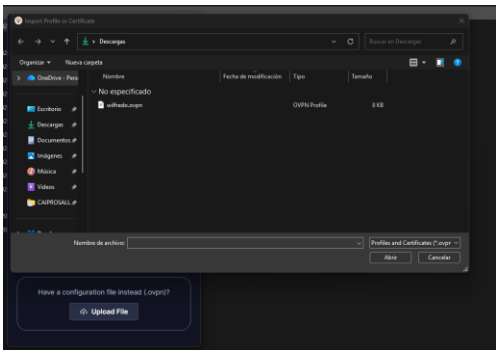


Figura 36. Seleccionar el archivo de configuración generado por OpenVPN Road Warrior en el paso indicado en la figura 26.

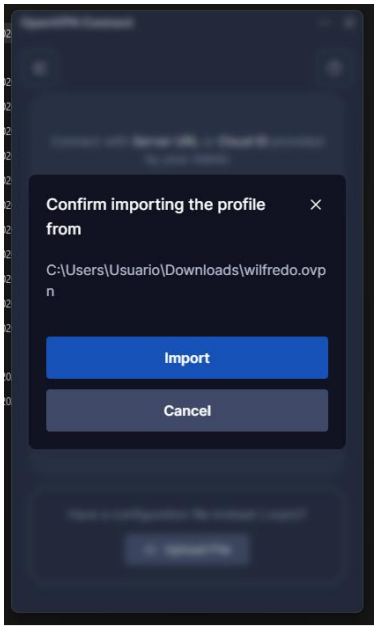


Figura 37. Confirmar la importación del archivo de configuración

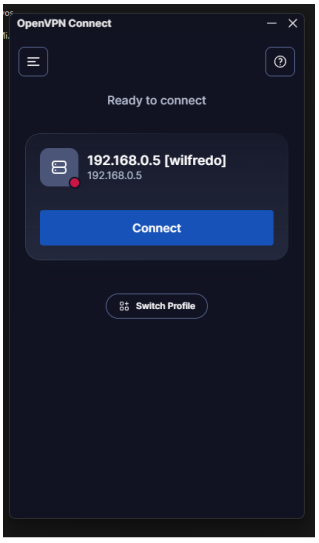
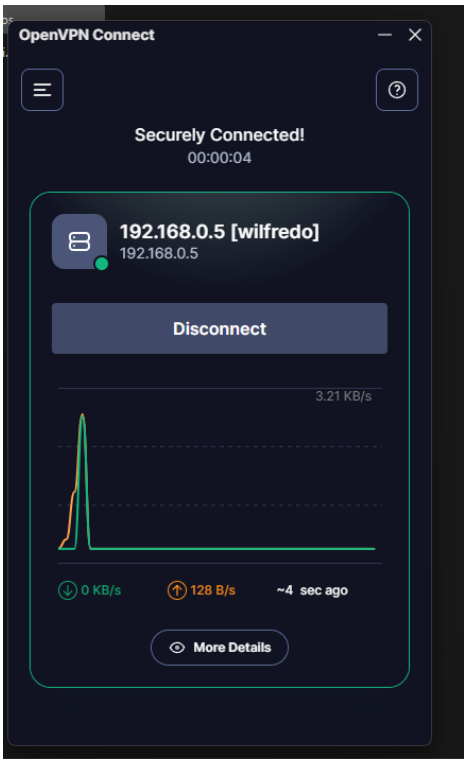


Figura 38. Perfil creado con el archivo .ovpn

Finalmente en la figura 39 vemos como se realiza la conexión exitosa al servidor VPN y en la figura 40 vemos el estado conectado del cliente en la interfaz gráfica del servidor.

A partir de este momento, el computador del cliente puede acceder a la red configurada por el servidor VPN y de esta forma utilizar los servicios configurados por el administrador.



3 CONCLUSIONES.

El desarrollo del presente trabajo permitió comprobar la viabilidad de implementar entornos de ciberseguridad funcionales utilizando exclusivamente herramientas de código abierto y recursos de hardware convencionales. La integración de Ubuntu Linux como sistema anfitrión, QEMU/KVM como plataforma de virtualización y NethSecurity como solución de firewall demostró ser una alternativa adecuada para la simulación de arquitecturas empresariales.

Durante el desarrollo de las actividades se evidenció la importancia del manejo de perfiles de seguridad asociados a usuarios que acceden a los servicios de red del entorno empresarial para un control adecuado de los mismos. Una red que tiene control sobre los servicios publicados en internet tendrá menos riesgos de sufrir ataques que comprometan la información de la empresa.

Cada usuario es responsable del uso que se le da a su acceso de forma que también es indispensable configurar dentro de la VPN unos límites que disminuyan la capacidad de una pérdida de información en caso de que el usuario por ejemplo pierda su equipo de trabajo remoto y este sea usado como punto de ataque.

Las VPN permiten configurar acceso a recursos de forma controlada, dentro de los servicios de seguridad perimetral se debe tener una segmentación avanzada, un monitoreo continuo del tráfico y unas políticas claras de acceso remoto seguro, de esta forma NethSecurity será la mejor opción dentro de las utilidades openSource para la seguridad de la empresa.

4 REFERENCIAS

[1] System requirements — NethSecurity documentation. (s. f.). https://docs.nethsecurity.org/en/latest/system_requirements.html

[2] Download — NethSecurity documentation. (s. f.). https://docs.nethsecurity.org/en/latest/download.html

[3] OpenVPN Connect - VPN for your operating system | OpenVPN. (s. f.). OpenVPN. https://openvpn.net/client/

[4] OpenVPN Connect User Guide. (s. f.). https://openvpn.net/connect-docs/user-guide.html

[5] QEMU's documentation — QEMU documentation. (s. f.). https://www.qemu.org/docs/master/.

[6] Ubuntu documentation. (s. f.). https://docs.ubuntu.com/