ETAPA 7 IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Integrante 1 (Juan Manuel González Santana)
e-mail: jmgonzalezsan@unadvirtual.edu.co
Integrante 2 (Valentina Useche Triana)
e-mail: vusechet@unadvirtual.edu.co
Integrante 3 (Juan Manuel Grisales Ortiz)
e-mail: jmgrisalesor@unadvirtual.edu.co
Integrante 4 (Luis Florentino Rodríguez Baquer)
e-mail: lfrodriguezbaq@unadvirtual.edu.co
Integrante 5 (Jose Alejandro Melo Arango)
e-mail: jameloa@unadvirtual.edu.co

RESUMEN: *El artículo trae el desarrollo colaborativo de una seguridad perimetral basada en GNU/Linux, el cual usó Endian Firewall (EFW). Esta idea busca la protección de servicios que la intranet (LAN) y la extranet (WAN) conforman y de una zona desmilitarizada (DMZ), cerciorándose de la confianza, la integridad y el estado activo de los servicios, las bases de datos y la aplicación web. Se montó una red con diferentes sectores con reglas para filtrar, traducción de direcciones de red (NAT), control de acceso entre zonas y servicio proxy con verificación. Cada parte la hicieron solo miembros del grupo y después la junta juntó todo. Se evidenció el empleo de una consola de comandos para manejar servicios. Los frutos muestran que Endian Firewall es eficaz para el sistema de seguridad perimetral del ambiente de negocio con aplicación libre.*

PALABRAS CLAVE: DMZ, Endian Firewall, GNU/Linux, NAT, seguridad perimetral.

1 INTRODUCCIÓN

La protección perimetral constituye uno de los elementos esenciales en la defensa de las infraestructuras de red contemporáneas. Una segmentación eficiente de las redes, la regulación del tráfico y la ejecución de políticas de acceso son estrategias que permiten disminuir los riesgos vinculados a accesos no autorizados y ataques externos. En este marco, Endian Firewall, como una solución UTM que opera en GNU/Linux, proporciona herramientas completas para la administración de la seguridad en redes LAN, WAN y DMZ. El presente documento detalla el desarrollo colaborativo de cinco temas enfocados en la implementación de una arquitectura segura, conforme a los lineamientos establecidos en la Etapa 7 del Programa de Diplomado en administración de sistemas operativos de Código Abierto.

2 DESCRIPCIÓN DE LA ACTIVIDAD Y METODOLOGÍA

La actividad grupal: La labor en grupo implicó la creación y ejecución de una solución de seguridad en el perímetro, utilizando Endian Firewall como el cortafuegos principal. Se estableció una infraestructura que incluía estaciones GNU/Linux en la red de área local, un firewall Endian conectado a la red de área extensa y un servidor GNU/Linux en la zona desmilitarizada que alberga servicios web y bases de datos. Cada miembro eligió un tema particular, lo desarrolló de manera individual a través de comandos en línea de comandos y registró pruebas con la fecha y hora de cada ejecución. Después, los resultados fueron consolidados en un único documento siguiendo el formato IEEE y se añadieron enlaces a los videos de presentación individual.

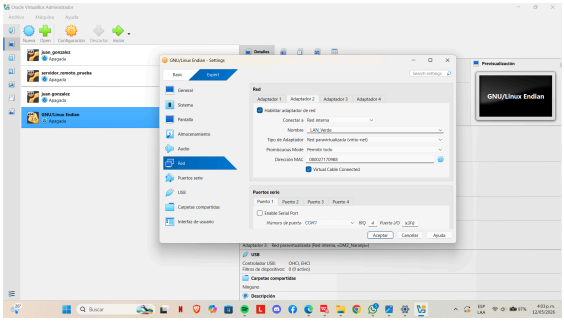
3 TEMÁTICAS DESARROLLADAS

3.1 Temática 1: Configuración de la instancia GNU/Linux Endian en VirtualBox

Producto esperado:Implementación de GNU/Linux Endian con las zonas verde, roja y naranja, así: Zona verde: red interna (LAN), Zona roja: acceso a internet(WAN) y Zona naranja: servidores (DMZ).

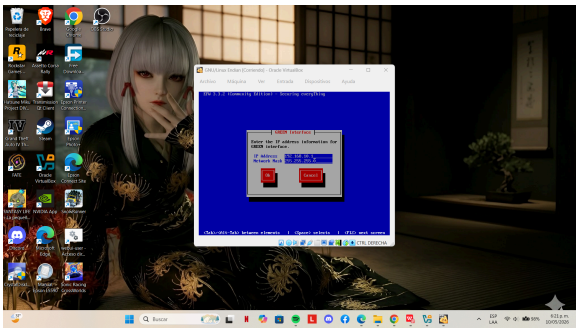
Configuración de la instancia GNU/Linux Endian en VirtualBox

Fig 1. Configuración de adaptadores de red en Oracle VirtualBox



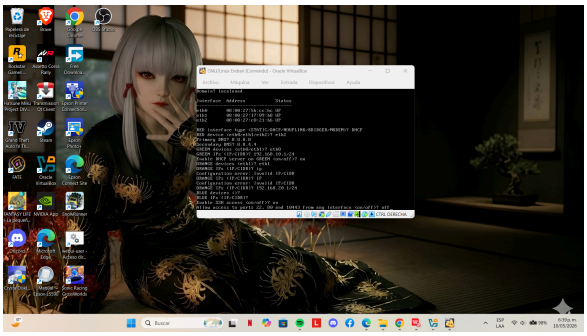
Nota. En la imagen se detalla la configuración de los tres adaptadores de red necesarios para la segmentación: el Adaptador 1 en modo Puente para la zona RED (WAN), el Adaptador 2 en Red Interna para la zona GREEN (LAN) y el Adaptador 3 en Red Interna para la zona ORANGE (DMZ).

Fig 2.Asignación de direccionamiento IP en la interfaz GREEN



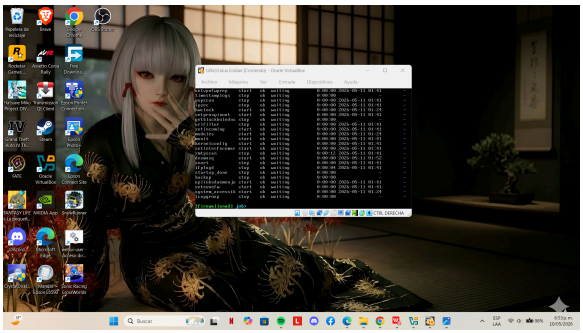
Nota. Se observa el proceso de configuración manual de la interfaz de red verde, donde se asigna la dirección IP estática 192.168.10.1 con máscara de subred 255.255.255.0, estableciendo así el gateway de la red de área local.

Fig 3.Resumen de configuración de interfaces de red



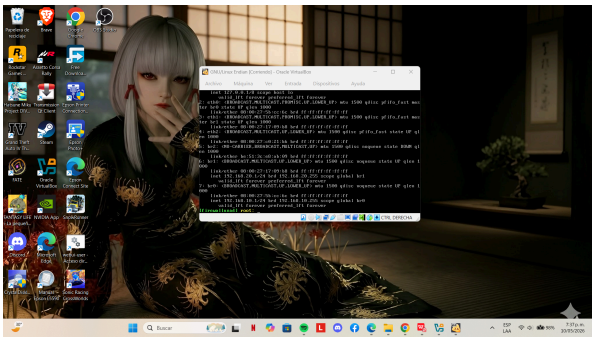
Nota. La captura muestra el resumen del asistente de configuración de Endian, validando el mapeo de los dispositivos físicos a las zonas lógicas: eth0 para GREEN, eth1 para ORANGE (con la IP 192.168.20.1) y eth2 para RED bajo el protocolo DHCP.

Fig 4.Validación de servicios del sistema mediante consola



Nota. Se evidencia el uso del comando de gestión de trabajos para verificar el estado operativo de los servicios críticos. Se confirma que módulos esenciales como dnsmasq y monit se encuentran en estado iniciado ("start") y correcto ("ok").

Fig 5 .Verificación de direccionamiento br0 y br1

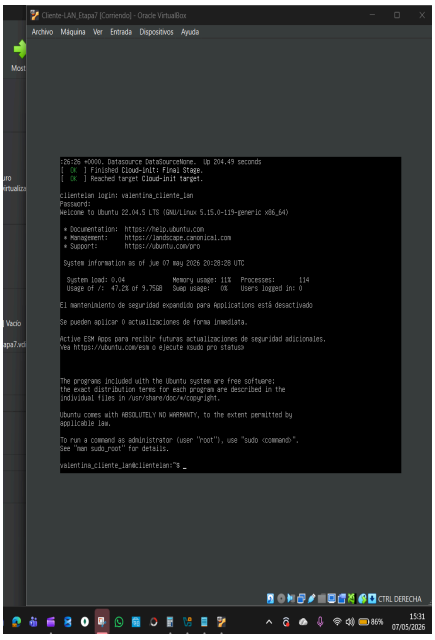


Nota. Mediante el comando de consola ip addr, se comprueba la correcta activación de los puentes de red br0 (192.168.10.1) y br1 (192.168.20.1), garantizando que el firewall está listo para gestionar el tráfico interzonas.

3.2 Temática 2: Configuración de NAT

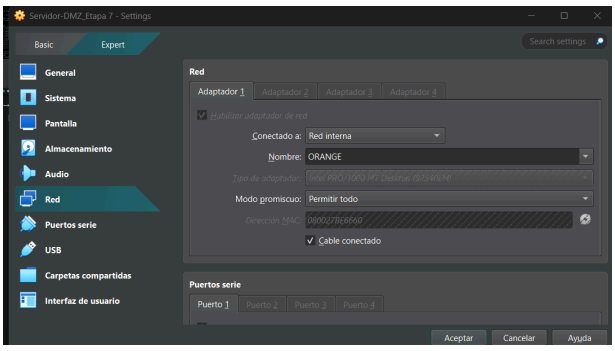
1. Configurar la regla de NAT (Network Address Translation / Traducción de Direcciones de Red), demostrando el establecimiento de la comunicación desde la LAN hacia la WAN (red simulada de Internet).

Fig . 6 Cliente de LAN preparado para pruebas de conexión a la WAN



Nota: En la imagen se observa el inicio de sesión del dispositivo cliente de LAN que opera con el sistema Ubuntu Server, el cual está configurado dentro de la red interna GREEN (192.168.10.0/24). Este dispositivo es empleado para llev ar a cabo pruebas de conexión a la red WAN, con el propósito de comprobar el correcto funcionamiento de la regla de NAT que facilita la conversión de direcciones desde la LAN hacia Internet a través del firewall Endian.

Fig. 7 Ajustes de la interfaz de red del Cliente LAN en VirtualBox (Zona VERDE)

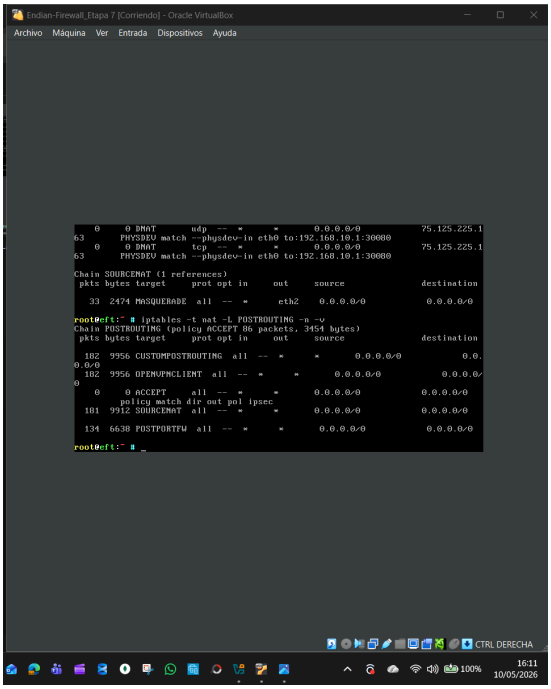


Nota. La imagen muestra cómo está configurada la red del Cliente LAN en Oracle VirtualBox, donde se puede ver que el adaptador de red está enlazado a una red interna llamada VERDE. Esto permite que el dispositivo se integre a la red LAN y que todo el tráfico que salga sea dirigido al firewall Endian para su conversión a través de NAT antes de acceder a la red WAN simulada.

Fig .8 Configuración de interfaces de red en Endian Firewall para usar NAT

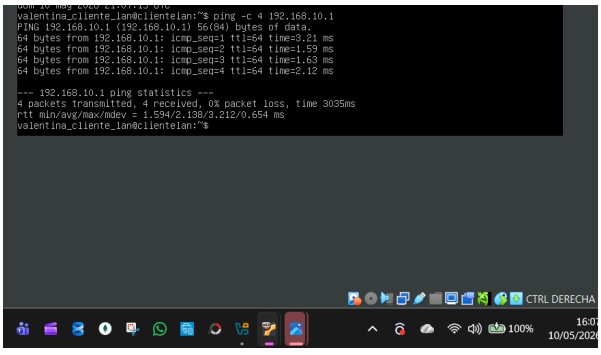
Nota: En la imagen se muestra el asistente de configuración de red del firewall Endian, donde se designan las interfaces adecuadas a las zonas RED (WAN), GREEN (LAN) y ORANGE (DMZ). Este ajuste es esencial para poner en práctica las reglas de traducción de dirección de red (NAT), ya que facilita la gestión y conversión del tráfico que se origi na en la red LAN hacia la red WAN, cumpliendo así con el primer objetivo de la Temática 2.

Fig 9. Revisión de reglas NAT vigentes en el Firewall Endian usando iptables



Nota: La imagen muestra el resultado del comando iptables -t nat -L -n -v ejecutado en el firewall Endian, donde se pueden ver las cadenas de traducción de direcciones de red (DNAT y POSTROUTING). En particular, se puede ver la implementación de reglas de origen (SNAT/MASQUERADE) que posibilitan el enmascaramiento del tráfico que sale de las redes internas hacia la red WAN. Esta revisión confirma que las reglas NAT configuradas para la comunicación desde la LAN y la zona DMZ hacia Internet están activas y funcionando, satisfaciendo los requerimientos estableci dos en la Temática 2.

Fig .10 Comprobación de la conexión entre el Cliente LAN y el gateway Endian (Zona VERDE)



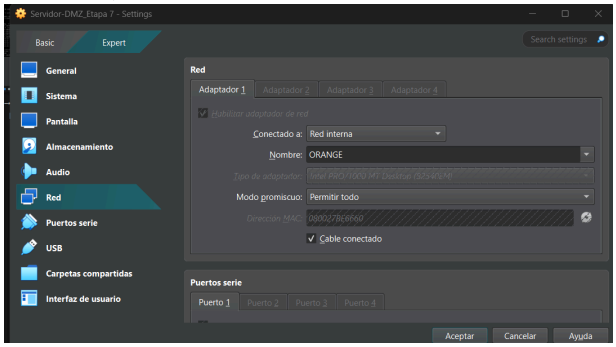
Nota: En la imagen se muestra la realización del comando ping desde el dispositivo Cliente LAN hacia la IP 192. 168. 10. 1, que es el gateway de la red VERDE que está en el firewall Endian. La recepción positiva de los paquetes ICMP demuestra que la comunicación en la red LAN es correcta, lo que es necesario para la implementación y verificación posteriores de las reglas NAT hacia la red WAN

2. Configurar la regla de NAT, demostrando el establecimiento de la comunicación de la Zona DMZ hacia Internet. Verificar en el reenvío de puertos/NAT la creación de las reglas.

Fig .11 Inicio de sesión y estado del Servidor DMZ en Ubuntu Server

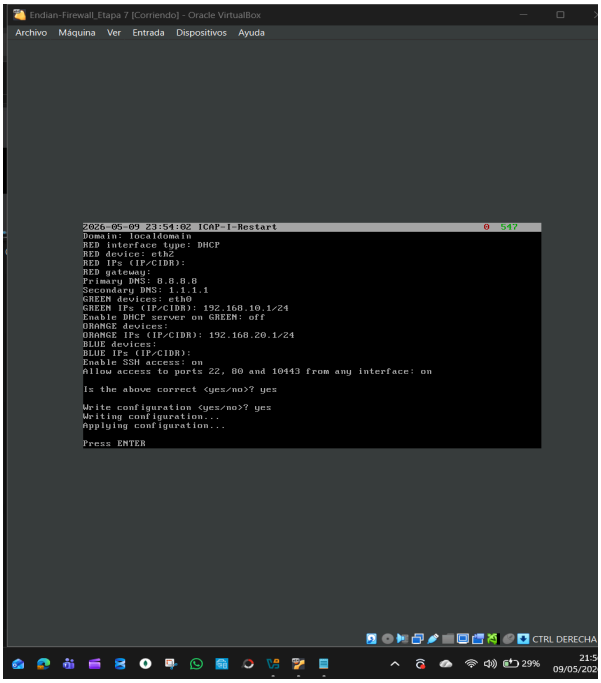
Nota. La imagen presenta el acceso al servidor DMZ usando el sistema operativo Ubuntu Server 22. 04 LTS, demostrando que el sistema se ha iniciado correctam ente y que el entorno está listo para comprobar la conectividad. Este dispositivo es p arte de la zona NARANJA (DMZ) y se empleará para validar la comunicación hacia la red WAN mediante las reglas de Traducción de Direcciones de Red (NAT) establecidas en el firewall Endian.

Fig ,12 Configuración de red del Servidor DMZ en Oracle VirtualBox (Zona NARANJA



Nota: La imagen muestra cómo se ha ajustado el adaptador de red del Servidor DMZ en Oracle VirtualBox, donde se puede ver la conexión a una red interna llamada NARANJA. Este ajuste permite que el servidor esté situado en la zona DMZ, asegurando que todo el tráfico que sale sea dirigido al firewall Endian para ser procesado a través de reglas NAT antes de llegar a la red WAN.

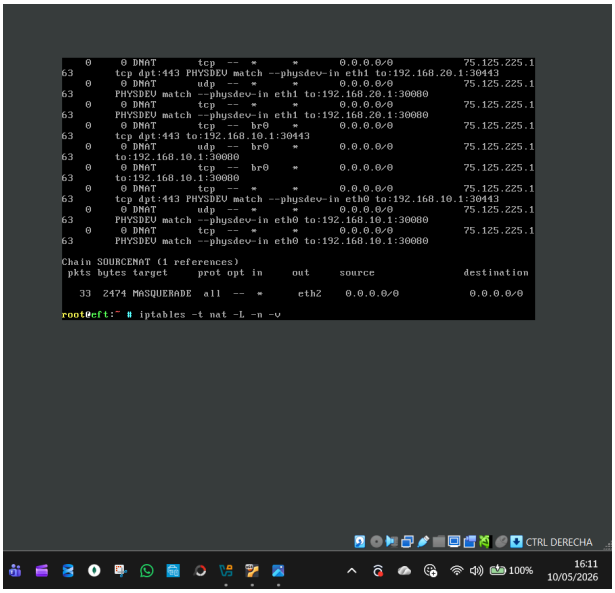
Fig .13 Configuración de las interfaces RED, GREEN y ORANGE en el cortafuegos Endian



Nota:

La imagen muestra cómo se aplica la configuración de red en el cortafuegos Endian a través del asistente de configuración. En este proceso se asignan las direcciones IP adecuadas a las zonas GREEN (LAN) y ORANGE (DMZ), y se configura la interfaz RED (WAN) utilizando DHCP. Esta configuración es fundamental para establecer las reglas de NAT que facilitan la comunicación desde la LAN y la DMZ hacia la red WAN, cumpliendo así con los objetivos definidos en la Temática 2.

Fig .14 Revisión de normas NAT y ocultación de tráfico en Endian Firewall



Nota:
La imagen muestra el resultado del comando iptables -t nat -L -n -v ejecutado en el firewall Endian, donde se pueden observar las cadenas de traducción de direcciones de red (DNAT, SOURCENAT y POSTROUTING). En particular, se puede ver la regla de tipo MASQUERADE, que posibilita la ocultación del tráfico que proviene de las redes internas hacia la red WAN. Esta revisión verifica que las reglas de NAT establecidas en Endian están activas y funcionando, lo que permite la salida controlada de la LAN y la DMZ hacia Internet, de acuerdo con los objetivos de la Temática 2.

Fig .15 Prueba de conexión desde el Servidor DMZ a la red WAN usando NAT

Nota: En la imagen se muestra la configuración temporal de las direcciones IP en el Servidor DMZ y la ejecución del comando ping a la dirección pública 8. 8. 8. 8. La recepción exitosa de las respuestas ICMP demuestra que el tráfico que proviene de la zona ORANGE (DMZ) puede acceder a la red WAN a través del firewall Endian, evidenciando que la regla de NAT que permite la comunicación de la DMZ a Internet está funcionando correctamente.

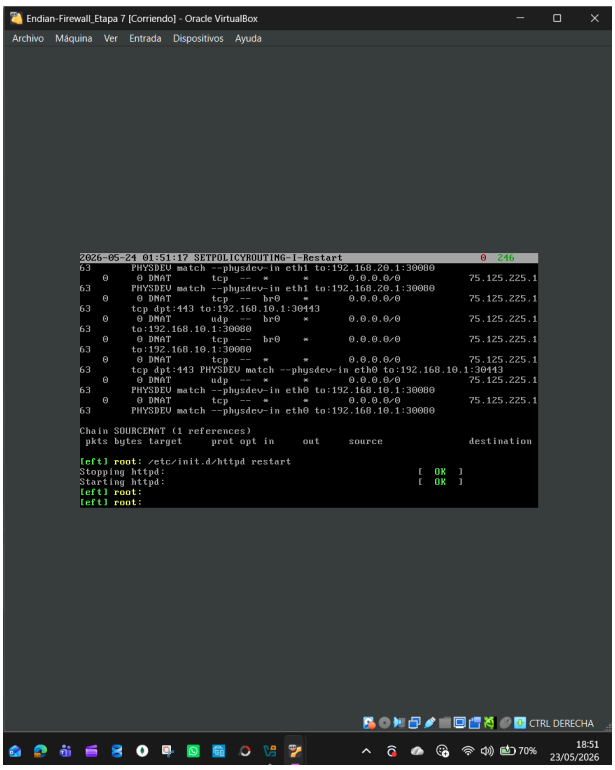
Fig . 16 Revisión *de la conectividad, desde el equipo Cliente-LAN hasta la WAN, se llevó a cabo a través de pruebas ICMP y consulta de DNS usando google.com.*

Nota. Se implementó el NAT de direcciones en Endian Firewall; con esto se permitió al cliente de la LAN 192.168.10.0/24 poder comunicarse con la WAN simulada. La verificación se efectuó por medio de pruebas ICMP hacia la IP pública 8.8.8.8 y DNS usando google.com.

Fig .17.Validación de conectividad, desde el servidor Ubuntu Server dentro de la DMZ, hacia Internet, empleando ICMP y DNS.

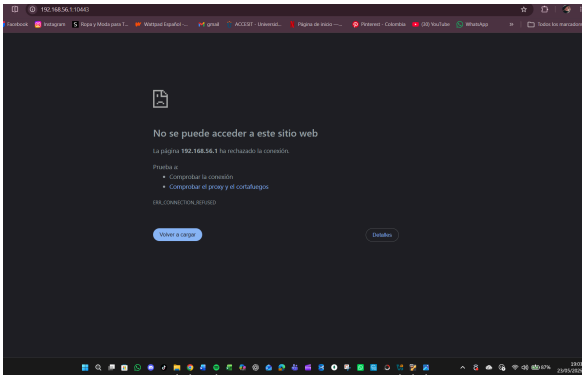
Nota.. Se aplicó una regla NAT para la DMZ 192. 168. 20. 0/24, esto daba acceso vigilado a Internet. La conexión la probamos con ICMP y la resolución DNS desde el Ubuntu Server de la DMZ.

Fig. 18. Se observa la revisión de las políticas NAT y la traducción de direcciones que estaban configuradas en el Endian Firewall por medio de reglas DNAT y MASQUERADE desde la consola de administración.



Nota. En las últimas pruebas surgieron problemas con el acceso a la interfaz web del Endian Firewall desde el host Windows por causa de la virtualización de red en VirtualBox. A pesar de eso, fue confirmado el funcionamiento de las políticas NAT usando reglas DNAT y MASQUERADE vistas desde la consola root del firewall, verificando la interconexión entre las zonas GREEN, ORANGE, RED y la WAN simulada

Fig. 19. Un intento de ingresar a la interfaz web de administración de Endian Firewall a través del puerto 10443, partiendo de una máquina Windows.



Nota. Se intentó acceder a la interfaz de administración web del Endian Firewall con la dirección https://192. 168. 56. 1:10443 en las pruebas finales; no obstante, el navegador mandó el mensaje "ERR_CONNECTION_REFUSED". Esto se debe a restricciones de virtualización y a la comunicación de las

interfaces en VirtualBox. Aun así, la administración y la validación del firewall fueron ejecutadas bien desde la consola root de Endian, verificando cómo trabajan las políticas NAT con reglas DNAT y MASQUERADE, y también la comunicación entre zonas GREEN, ORANGE, RED y la WAN simulada.

3.3 Temática 3: Publicación de servicios en la DMZ

1. Configuración de red en VirtualBox

Inicialmente se realizó la configuración de las interfaces de red en las máquinas virtuales dentro de Oracle VM VirtualBox, estableciendo la distribución de zonas solicitada en la guía de actividades.

La máquina virtual correspondiente a Endian Firewall fue configurada con tres adaptadores de red:

*Fig 20.*Adaptador 1 → RED (WAN) mediante NAT.

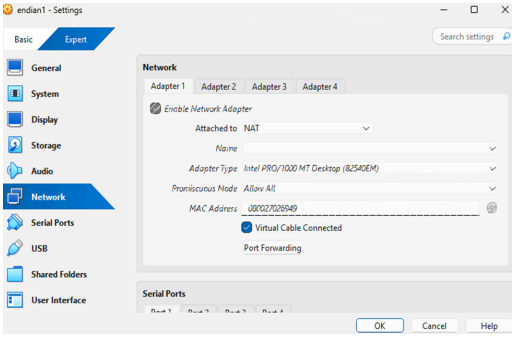


*Fig 21.*Adaptador 2 → GREEN (LAN) mediante red interna con nombre LAN.

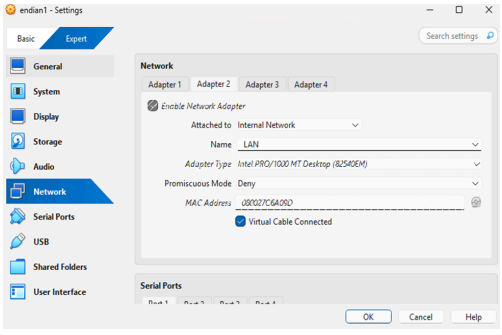
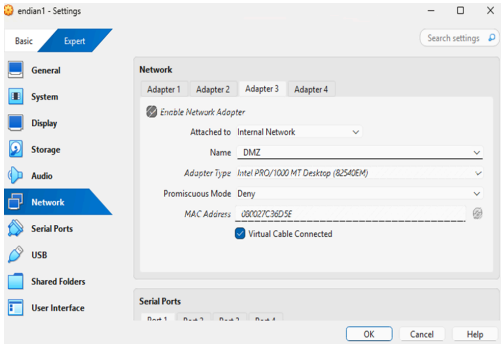


Fig .22 Adaptador 3 → ORANGE (DMZ) mediante red interna con nombre DMZ.



Así mismo, se configuró la máquina Ubuntu Cliente conectada a la red LAN y la máquina Ubuntu Server conectada a la red DMZ

2. Instalación y configuración de Endian Firewall

Posteriormente se realizó la instalación de Endian Firewall Community utilizando la imagen ISO correspondiente.

Durante la configuración inicial se asignaron las interfaces de red de la siguiente manera:
Después se configuraron las direcciones IP para cada zona de red.

Configuración GREEN (LAN)

IP: 192.168.10.1

Máscara: 255.255.255.0

Configuración ORANGE (DMZ)

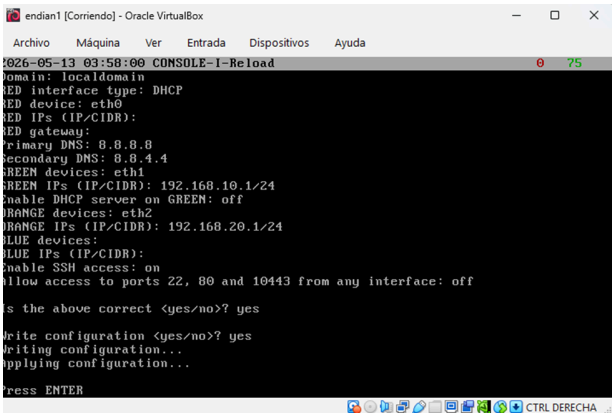
IP: 192.168.20.1

Máscara: 255.255.255.0

Configuración RED (WAN)

DHCP automático

Fig .23 Instalación inicial de Endian Firewall Community.



Nota. La imagen presenta el proceso de instalación de Endian Firewall Community en VirtualBox, incluyendo la detección de interfaces y el inicio del asistente de configuración.

3. CONFIGURACIÓN IP UBUNTU CLIENTE (LAN)

En la máquina Ubuntu Cliente se configuró una dirección IP estática perteneciente a la red GREEN.

Para ello se editó el archivo de configuración de Netplan mediante el siguiente comando:

sudo nano /etc/netplan/00-installer-config.yaml

Se agregó la siguiente configuración:

network:

version: 2

ethernets:

enp0s3:

dhcp4: no

addresses:

- 192.168.10.10/24

Routes:

To: default

via: 192.168.10.1

nameservers:

addresses:

- 8.8.8.8

- 8.8.4.4

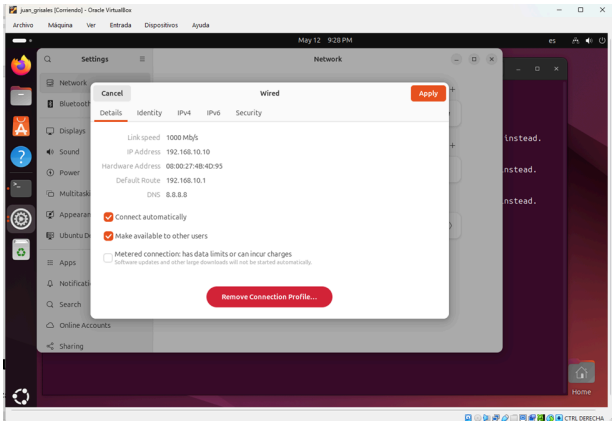
Posteriormente se aplicaron los cambios:

sudo netplan apply

Finalmente se verificó la configuración IP:

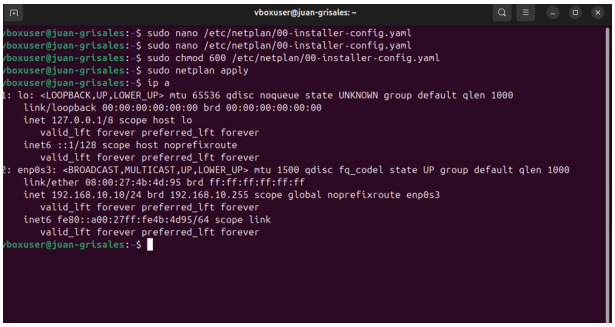
ip a

Fig .24 Asignación de interfaces RED, GREEN y ORANGE.



Nota. Configuración de las interfaces de red del firewall Endian, asignando las zonas WAN, LAN y DMZ según los requerimientos de la práctica.

Fig .25 Configuración IP del cliente Ubuntu en la red GREEN.



Nota. Asignación de dirección IP estática al Ubuntu Cliente mediante Netplan dentro de la red LAN GREEN.

4. Configuración IP Ubuntu Server (DMZ)

Posteriormente se configuró la dirección IP estática del servidor ubicado en la zona DMZ.

Se editó el archivo Netplan:

sudo nano /etc/netplan/00-installer-config.yaml

Configurando:

network:

version: 2

ethernets:

enp0s3:

dhcp4: no

addresses:

- 192.168.20.10/24

gateway4: 192.168.20.1

nameservers:

addresses:

- 8.8.8.8

Después se aplicaron los cambios:

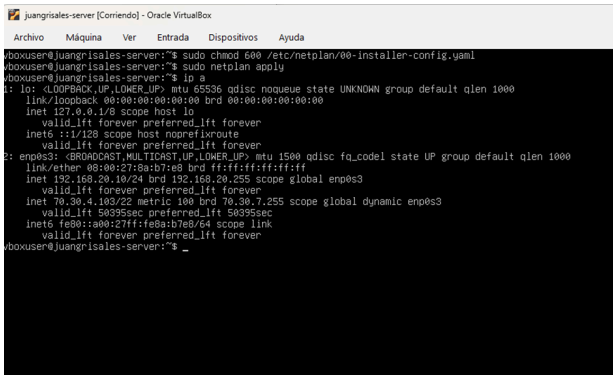
sudo netplan apply

Y se verificó la dirección IP:

ip a

Evidencia:

Fig .26 Configuración IP del servidor Ubuntu en la red ORANGE.



Nota. Configuración de la dirección IP estática del Ubuntu Server en la zona DMZ utilizando Netplan.

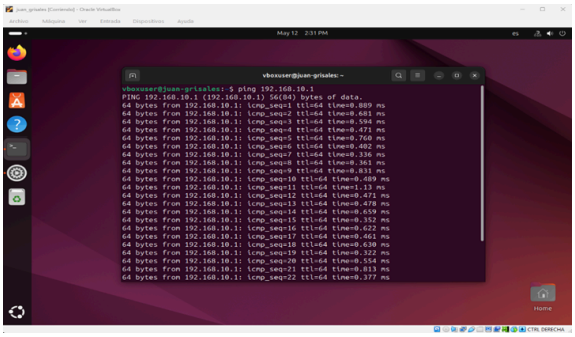
5. Verificación de conectividad

Una vez configuradas las direcciones IP, se realizaron pruebas de conectividad entre las zonas de red.

Desde Ubuntu Cliente se verificó conectividad con la puerta de enlace GREEN:

ping 192.168.10.1

Fig .27 Verificación de conectividad con la puerta de enlace GREEN.

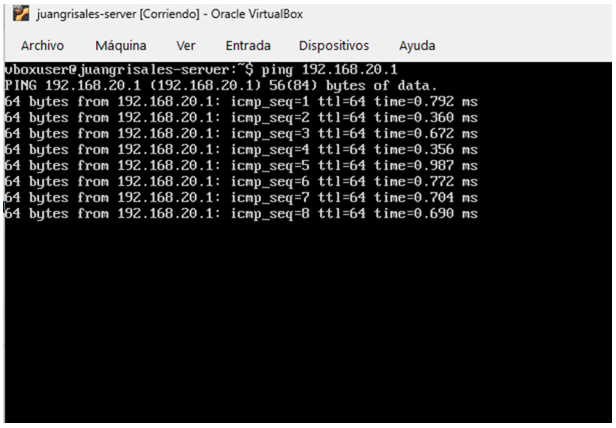


Nota. Validación de conectividad entre Ubuntu Cliente y Endian Firewall mediante pruebas ICMP hacia la interfaz GREEN.

Desde Ubuntu Server se verificó conectividad con la puerta de enlace ORANGE:

ping 192.168.20.1

Fig .28 Verificación de conectividad con la puerta de enlace ORANGE.



Nota. Comprobación de comunicación entre Ubuntu Server y la interfaz ORANGE configurada en Endian Firewall.

6. Instalación del servicio HTTP Apache

Con el fin de habilitar el servicio HTTP solicitado en la guía, se instaló el servidor web Apache en Ubuntu Server.

Primero se actualizaron los paquetes del sistema:

sudo apt update

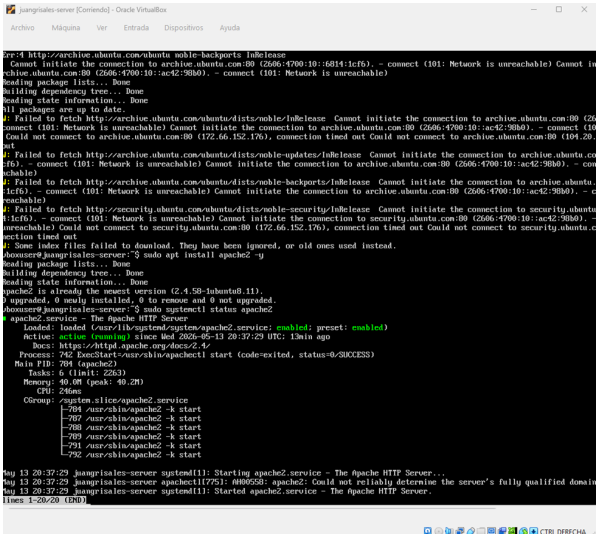
Posteriormente se instaló Apache:

sudo apt install apache2 -y

Después se verificó el estado del servicio:

sudo systemctl status apache2

Fig .29. Estado del servicio Apache2.



Nota. Verificación del funcionamiento del servicio Apache2 mediante el comando systemctl status en Ubuntu Server.

Se realizaron pruebas de administración del servicio:

Detener servicio

sudo systemctl stop apache2

Iniciar servicio

sudo systemctl start apache2

Reiniciar servicio

sudo systemctl restart apache2

Fig .30. Administración del servicio Apache2.

Nota. Ejecución de comandos para detener, iniciar y reiniciar el servicio Apache2 en Ubuntu Server.

7. Instalación del servicio FTP

Seguidamente se instaló el servicio FTP mediante VSFTPD.

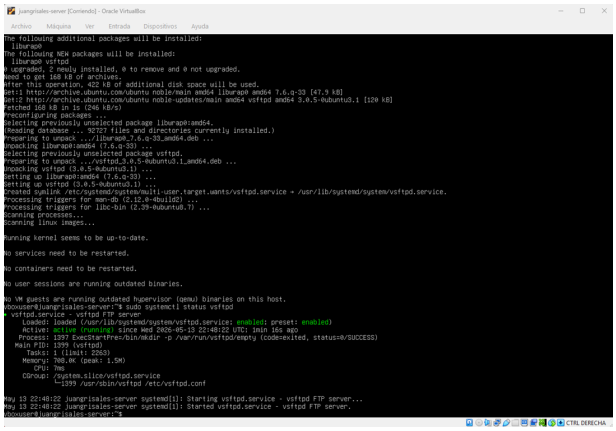
La instalación se realizó ejecutando:

sudo apt install vsftpd -y

Posteriormente se verificó el estado del servicio:

sudo systemctl status vsftpd

Fig .31. Estado del servicio VSFTPD.



Nota. Verificación del estado operativo del servicio FTP VSFTPD utilizando comandos administrativos en Ubuntu Server.

También se realizaron pruebas administrativas del servicio.

Detener servicio

sudo systemctl stop vsftpd

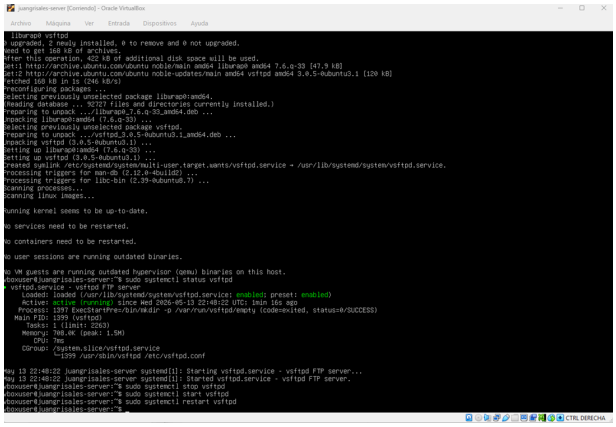
Iniciar servicio

sudo systemctl start vsftpd

Reiniciar servicio

sudo systemctl restart vsftpd

Fig .32 Administración del servicio VSFTPD.



Nota. Validación del inicio, detención y reinicio del servicio FTP VSFTPD desde la consola Linux.

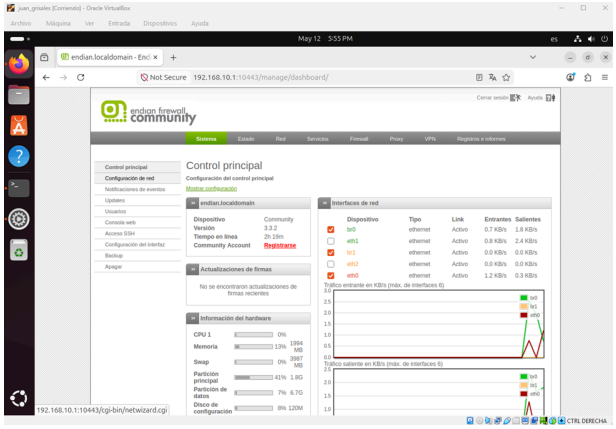
8. Acceso a la consola web de Endian

Desde Ubuntu Cliente se accedió a la interfaz web administrativa de Endian Firewall mediante la siguiente dirección:

https://192.168.10.1:10443

Se aceptó el certificado de seguridad y posteriormente se ingresó con las credenciales configuradas.

Fig .33. Acceso a la consola web de Endian Firewall.



Nota. Acceso exitoso a la interfaz administrativa web de Endian Firewall desde Ubuntu Cliente mediante HTTPS.

9. Creación de reglas HTTP y FTP

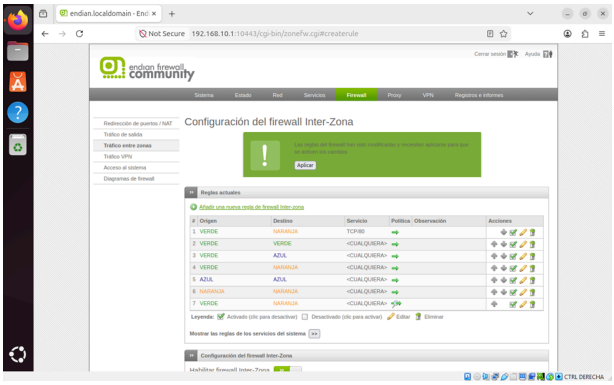
Dentro de Endian Firewall se ingresó a:

Firewall → Inter-Zone Traffic

Se creó una regla que permitió el tráfico HTTP desde la zona GREEN hacia la zona ORANGE.

Campo	Configuración
Source Zone	GREEN
Destination Zone	ORANGE
Service	HTTP
Action	ACCEPT

Fig .34. Regla HTTP entre GREEN y ORANGE.

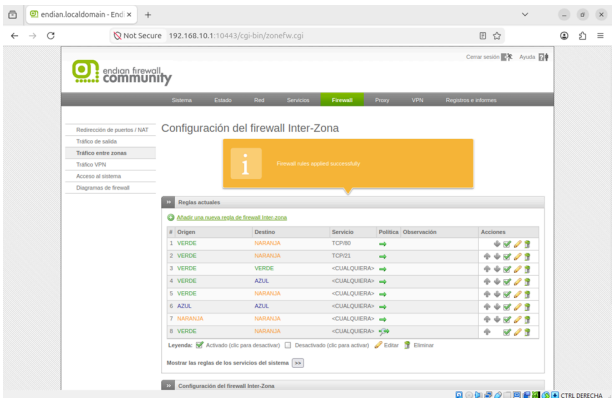


Nota. Configuración de regla de firewall que permite tráfico HTTP desde la red GREEN hacia la zona ORANGE.

Posteriormente se creó la regla para permitir tráfico FTP.

Campo	Configuración
Source Zone	GREEN
Destination Zone	ORANGE
Service	FTP
Action	ACCEPT

Fig .35. Regla FTP entre GREEN y ORANGE.



Nota. Creación de regla de firewall para permitir tráfico FTP desde la red LAN hacia la DMZ.

10. Bloqueo del protocolo ICMP

Con el objetivo de impedir respuestas de ping dentro de la red, se creó una regla de denegación ICMP.

La configuración se realizó en:

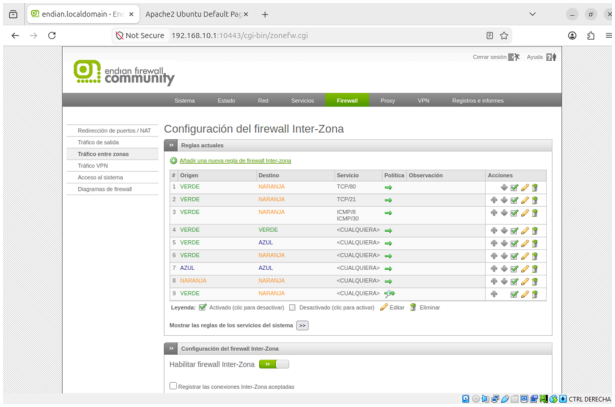
Firewall → Inter-Zone Traffic

Configurando:

Campo	Configuración
Source Zone	GREEN
Destination Zone	ORANGE
Service	ICMP
Action	DROP

Evidencia:

Fig .36. Regla de bloqueo ICMP.



Nota. Política de seguridad configurada para bloquear tráfico ICMP entre las zonas GREEN y ORANGE.

11. Prueba del servicio HTTP

Desde Ubuntu Cliente se realizó una prueba de acceso HTTP hacia el servidor ubicado en la zona DMZ mediante el navegador web.

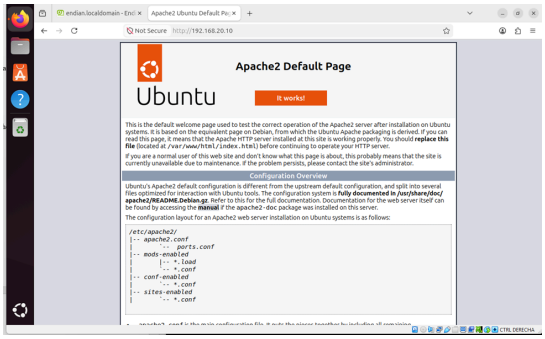
Se ingresó la siguiente dirección:

http://192.168.20.10

Visualizando correctamente la página predeterminada de Apache.

Evidencia:

Fig .37. Prueba de acceso HTTP desde Ubuntu Cliente.



Nota. Validación de acceso al servidor Apache alojado en la zona DMZ desde el navegador web del cliente Ubuntu.

12. Prueba del servicio FTP

Posteriormente se instaló el cliente FTP en Ubuntu Cliente:

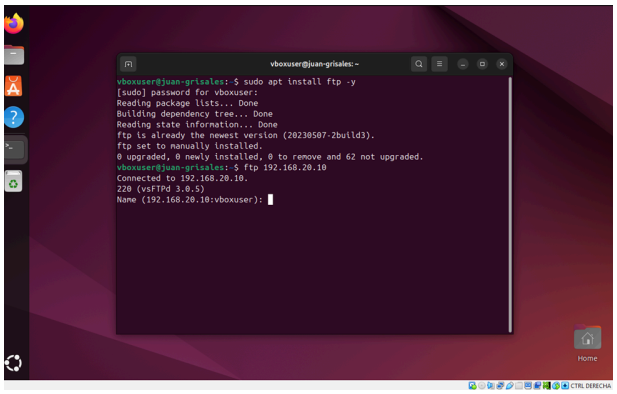
sudo apt install ftp

Luego se realizó la conexión FTP hacia el servidor DMZ:

ftp 192.168.20.10

La conexión se realizó satisfactoriamente.

Fig .38. Prueba de conexión FTP.



Nota. Verificación de acceso FTP desde Ubuntu Cliente hacia Ubuntu Server utilizando el protocolo FTP.

14. Verificación del bloqueo ICMP

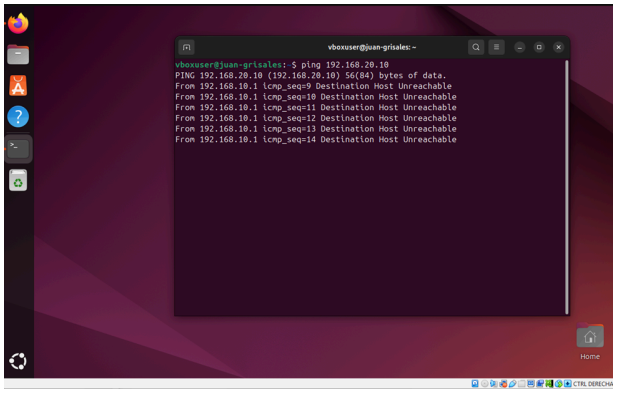
Finalmente se comprobó el funcionamiento de la regla de bloqueo ICMP realizando una prueba de ping desde Ubuntu Cliente hacia Ubuntu Server.

ping 192.168.20.10

El servidor no respondió a las solicitudes ICMP, validando correctamente la política de seguridad implementada.

Evidencia:

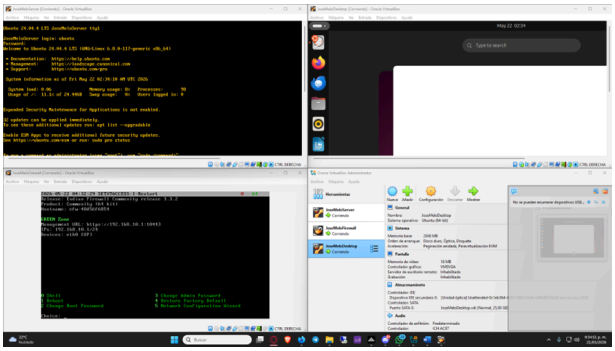
Fig .39, Validación del bloqueo ICMP.



Nota. Comprobación de funcionamiento de la regla de denegación ICMP implementada en Endian Firewall.

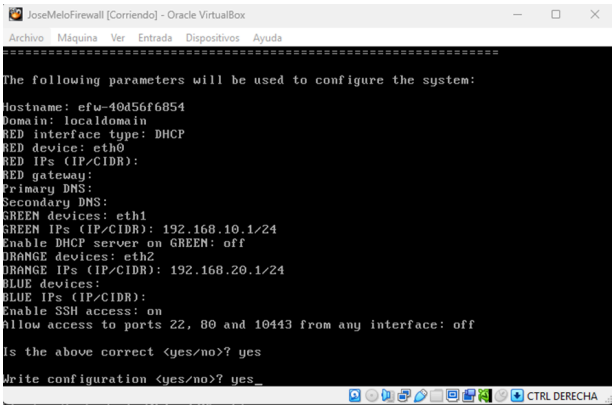
3.4 Temática 4: Reglas de acceso para permitir o denegar el tráfico.

Fig .40 Despliegue de la infraestructura de red en VirtualBox



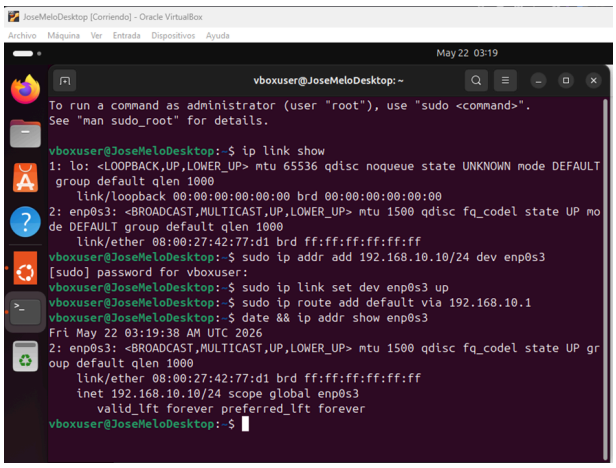
Nota. La imagen presenta las tres máquinas virtuales inicializadas en el hipervisor VirtualBox: Endian Firewall Appliance, Ubuntu Server (DMZ) y Ubuntu Desktop (LAN). Se demuestra que el entorno de virtualización se encuentra activo y con los recursos de hardware dispuestos para iniciar las pruebas de comunicación perimetral.

Fig .41 Asignación de interfaces y direccionamiento IP en Endian Firewall



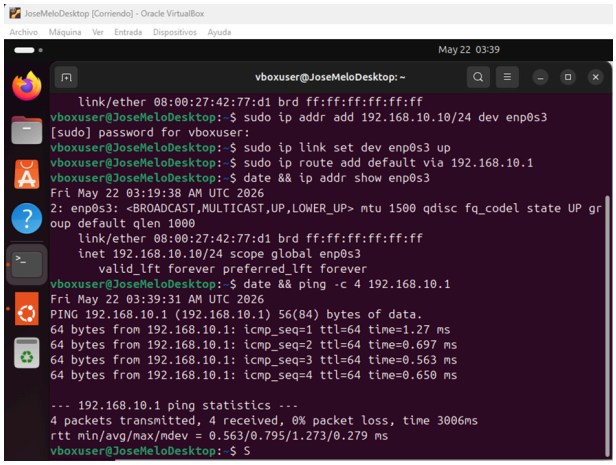
Nota. La imagen presenta el asistente de red (Network Wizard) en la consola de administración de Endian, donde se definen de manera estricta las direcciones IP para la zona VERDE (LAN) y la zona NARANJA (DMZ), asociando correctamente cada segmento de red a sus respectivos dispositivos de red virtuales (*devices*).

Fig .42 Configuración de red estática en el cliente GNU/Linux Ubuntu Desktop



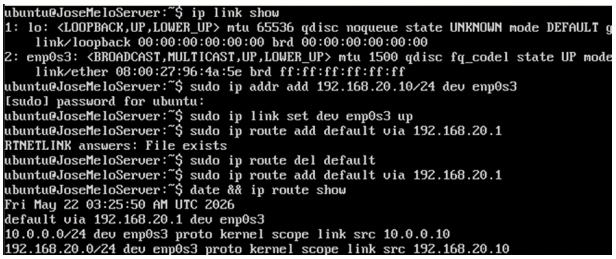
Nota. La imagen presenta la asignación manual de la dirección IP dentro del segmento de la zona VERDE (LAN) en el cliente Ubuntu Desktop. Esta configuración establece el enlace lógico y el direccionamiento necesario para utilizar el cortafuegos Endian como puerta de enlace predeterminada de la red interna.

Fig .43 Verificación de conectividad ICMP desde el cliente LAN hacia Endian



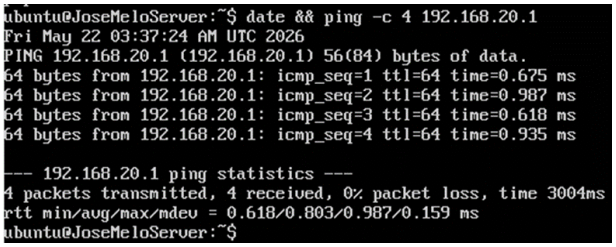
Nota. La imagen presenta la ejecución del comando ping desde la terminal de Ubuntu Desktop hacia la interfaz de la zona VERDE de Endian, demostrando una transmisión de paquetes exitosa y libre de pérdidas, lo que valida el correcto acoplamiento en la capa de enlace de datos.

Fig .44 Configuración de la interfaz de red en el servidor de la zona DMZ



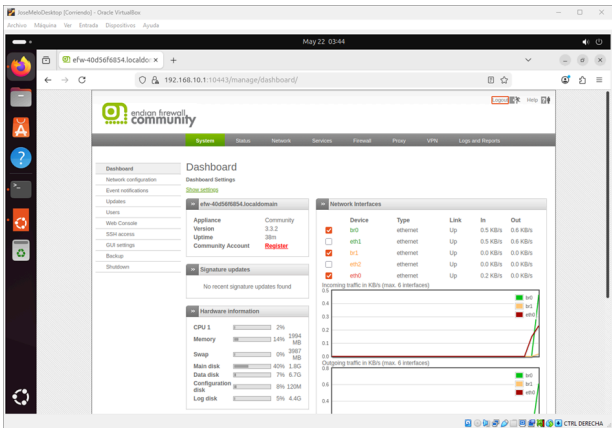
Nota. La imagen presenta la declaración manual de la dirección IP correspondiente a la subred de la zona NARANJA (DMZ) en la interfaz del Ubuntu Server, permitiendo que el servidor establezca un canal de comunicación directo y aislado hacia el firewall perimetral.

Fig .45 Verificación de enlace y respuesta ICMP en la zona DMZ



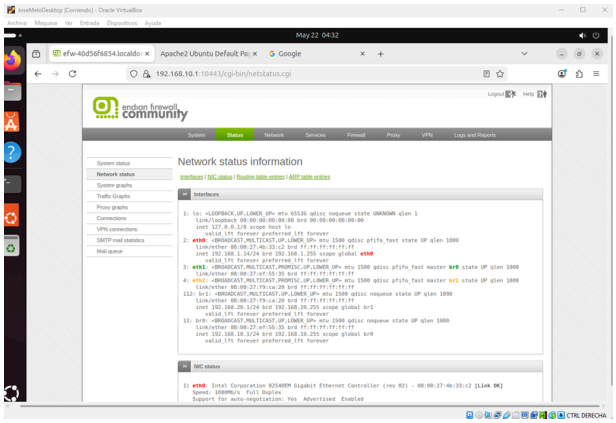
Nota. La imagen presenta la comprobación de conectividad mediante comandos de red en la consola de Ubuntu Server hacia la IP de la zona NARANJA de Endian. El intercambio exitoso de paquetes confirma que la tarjeta de red virtual responde de forma óptima dentro de su respectivo switch lógico.

Fig .46 Acceso seguro a la interfaz web de administración de Endian UTM



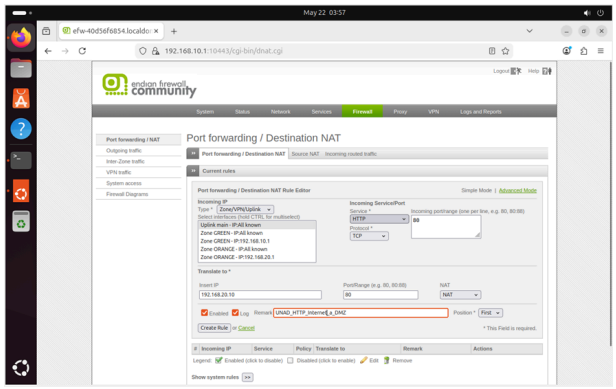
Nota. La imagen presenta el ingreso al panel gráfico de gestión de Endian Firewall desde el navegador web de Ubuntu Desktop, utilizando el protocolo HTTPS a través de la dirección IP de la zona VERDE en el puerto 10443, autenticando las credenciales del rol de administrador.

Fig .47 Panel de control y estado general de las interfaces de red (Network Status)



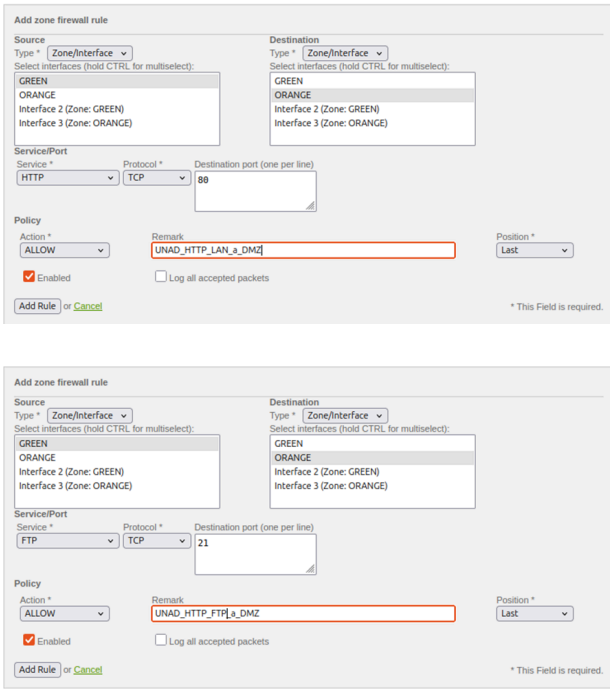
Nota. La imagen presenta el tablero principal (*Dashboard*) de Endian, evidenciando el estado operativo y las direcciones IP asignadas a cada una de las zonas de seguridad perimetral configuradas: VERDE (LAN), NARANJA (DMZ) y ROJA (WAN/Internet).

Fig .48 Parametrización de políticas de acceso y reglas de tráfico interzona



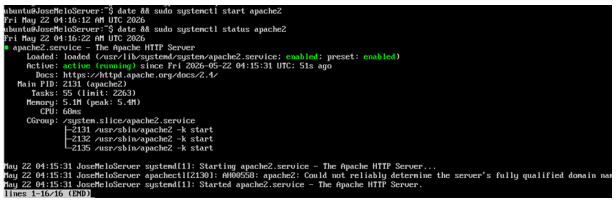
Nota. La imagen presenta el desarrollo de la Temática 4 mediante la creación y adición de reglas específicas de filtrado de paquetes en el cortafuegos. Estas políticas granulares permiten segmentar de manera estricta los puertos y protocolos autorizados para las fases de testeo de la guía.

Fig .49 Despliegue y verificación del servicio web HTTP Apache en el servidor DMZ



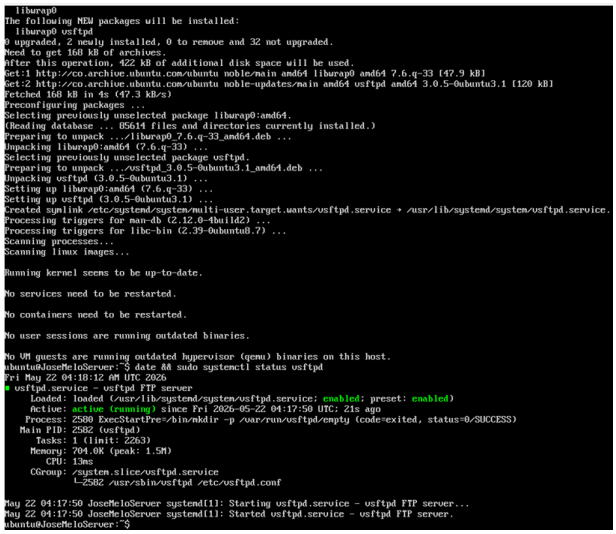
Nota. La imagen presenta el estado de ejecución del servicio web Apache2 dentro de la consola del Ubuntu Server. Se demuestra mediante comandos del sistema que el demonio se encuentra activo y escuchando en el puerto 80 para responder a las solicitudes entrantes.

Fig .50 Instalación y auditoría del demonio FTP en el entorno de la DMZ



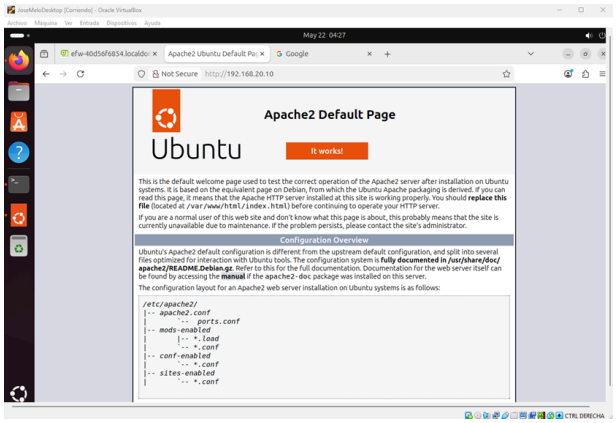
Nota. La imagen presenta el proceso de aprovisionamiento del servidor FTP (vsftpd) en el Ubuntu Server, validando el correcto despliegue del protocolo de transferencia de archivos en el puerto 21 para la ejecución de las directivas de seguridad estipuladas.

Fig .51 Petición HTTP local desde la zona VERDE hacia el Servidor DMZ



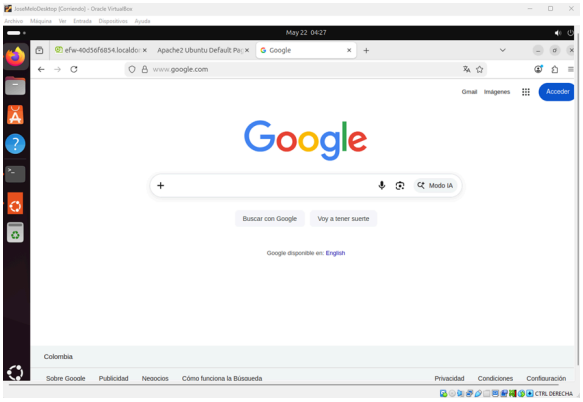
Nota. La imagen presenta la navegación y el consumo exitoso del servicio web del servidor (192.168.20.10) desde el cliente ubicado en la LAN, evidenciando que el cortafuegos Endian procesa y permite el tráfico interzona según las reglas previamente establecidas.

Fig .52 Comprobación de navegación externa y salida a Internet desde la LAN



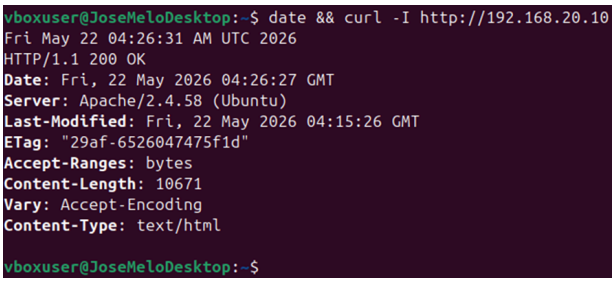
Nota. La imagen muestra el acceso a redes externas globales a través del navegador del cliente Ubuntu Desktop, lo que valida que el enrutamiento de salida y la regla NAT en la zona VERDE resuelven las solicitudes hacia la zona ROJA sin interrupciones.

Fig .53 Diagnóstico por consola de peticiones HTTP (curl) en el cliente de la LAN



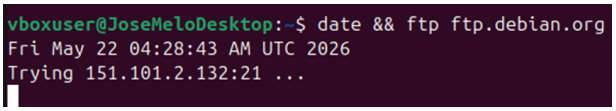
Nota. La imagen presenta el uso de la herramienta de línea de comandos curl en la terminal de Ubuntu Desktop. Se observa la obtención exitosa de las cabeceras HTTP del servidor de la DMZ, registrando la fecha y hora exactas del procedimiento mediante el comando date.

Fig .54 Evidencia de conexión interactiva mediante el protocolo FTP desde la LAN



Nota. La imagen presenta la traza de conexión en consola desde el Ubuntu Desktop hacia un servidor FTP externo, demostrando el saludo inicial del protocolo y la apertura correcta del canal de control de datos a través del firewall.

Fig .55 Verificación de conectividad WAN y resolución DNS en el Servidor DMZ



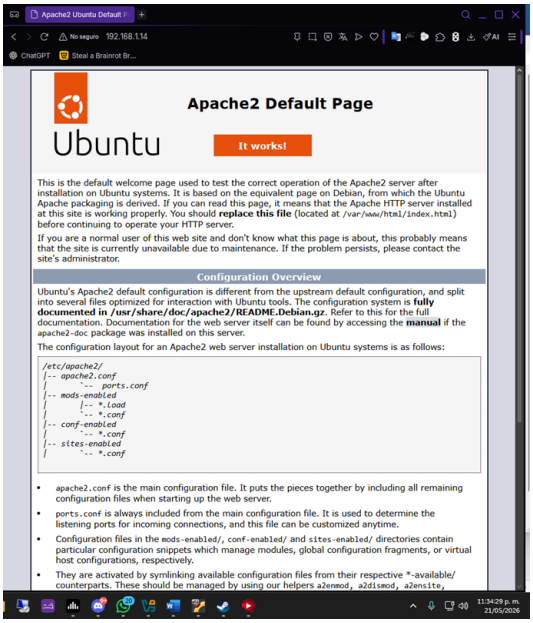
Nota. La imagen presenta la salida a internet del Ubuntu Server (DMZ) por medio de comandos de diagnóstico de red, confirmando que las políticas de tráfico saliente (*Outgoing*

Traffic) procesan correctamente las peticiones de los repositorios hacia el exterior.

Fig .56 Acceso externo al Servidor DMZ mediante técnicas de Port Forwarding

Nota. La imagen presenta la conexión exitosa desde el navegador web de la máquina física anfitriona (simulando un usuario en Internet) apuntando a la IP de la zona ROJA de Endian, demostrando que la regla de traducción de destino (DNAT) redirige el tráfico HTTP al puerto 80 del servidor interno.

Fig .57 Auditoría de seguridad perimetral y denegación del protocolo FTP externo



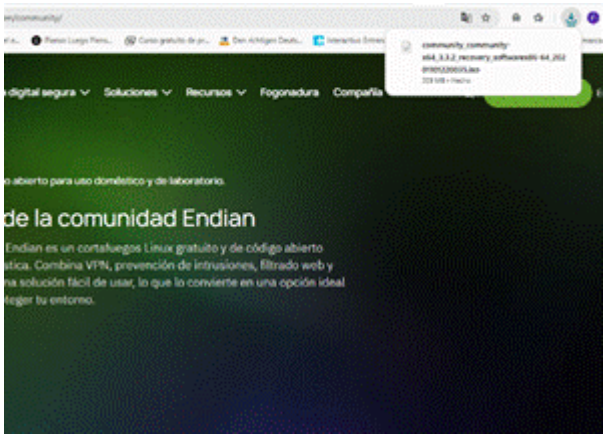
Nota. La imagen presenta el intento de conexión FTP desde la máquina física externa hacia la IP de la zona ROJA del firewall. Se observa que la solicitud se interrumpe y entra en estado de tiempo de espera agotado, validando la efectividad de la política de seguridad que restringe accesos no autorizados desde la WAN.

1.1 Temática 5: Implementación de Proxy HTTP con autenticación

I. Adquisición y despliegue base del firewall

El desarrollo del proyecto perimetral comenzó con la fase de aprovisionamiento lógico de la herramienta de seguridad. Para asegurar la integridad del sistema operativo, se accedió al repositorio oficial de la comunidad Endian para efectuar la descarga de la imagen ISO correspondiente a la versión Appliance Community, estableciendo la base del software de código abierto que actuará como pasarela de comunicación de la infraestructura corporativa.

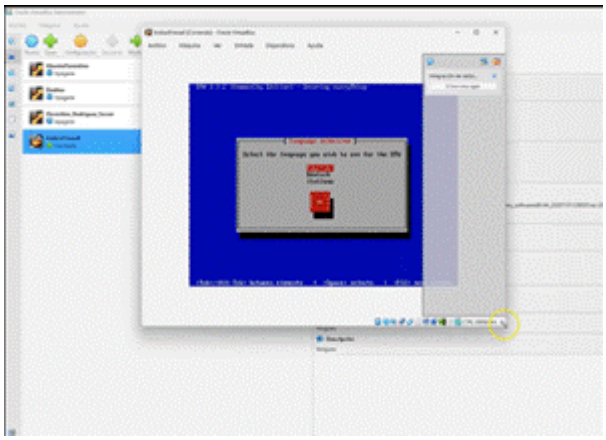
Fig .58 Descarga de la imagen ISO de Endian Firewall Community.



Nota. Obtención del instalador oficial del sistema operativo desde el portal de la comunidad para su despliegue virtual.

Una vez montada la imagen en el hipervisor, se inicializó el asistente de instalación en modo consola. El entorno requiere de manera prioritaria la interacción con el operador para la selección del idioma base del sistema de archivos, procediendo posteriormente con la destrucción lógica, el formateo y el particionado automatizado del disco duro virtual asignado.

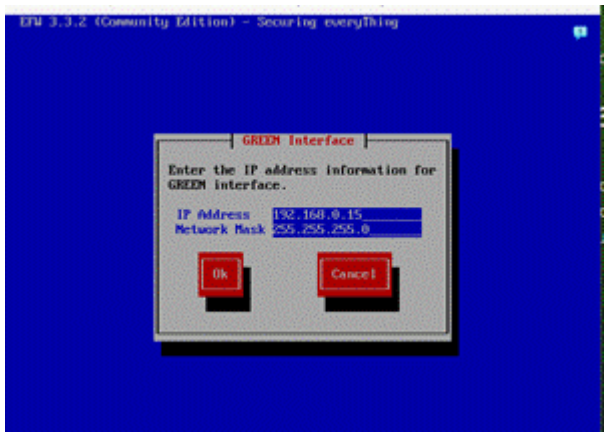
Fig .59 Selección de idioma en el instalador base de Endian UTM.



Nota. Interfaz de comandos inicial para la configuración regional y preparación del medio de almacenamiento.

Con el sistema base instalado, el asistente solicita la parametrización de la interfaz correspondiente a la red local interna (zona GREEN). Se procedió a ingresar de forma manual la dirección de red estática 192.168.0.15 junto con una máscara de subred de 24 bits (255.255.255.0), estableciendo así el punto de enlace obligatorio y la dirección de la puerta de enlace para todas las estaciones de trabajo de la LAN

Fig .60 Configuración manual de los parámetros de red de la interfaz GREEN.



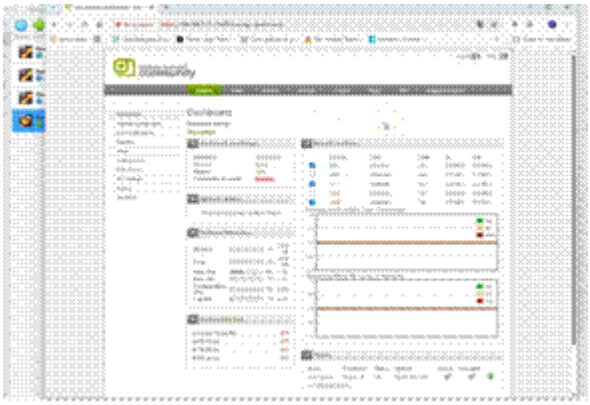
Nota. Asignación estática de la dirección IP perimetral para el gobierno de la subred interna a través de la CLI.

II. Gestión remota e implementación de autenticación local

Consolidado el direccionamiento físico y el primer arranque del cortafuegos, la administración se traslada a la interfaz gráfica de usuario (GUI). Se estableció una sesión de red remota mediante un navegador comercial utilizando el protocolo seguro HTTPS en el puerto no estándar 10443. Al autenticar el perfil de administración, el Dashboard principal del sistema despliega el

estado de salud de la máquina, validando la asignación del direccionamiento de las tarjetas de red y los consumos de memoria.

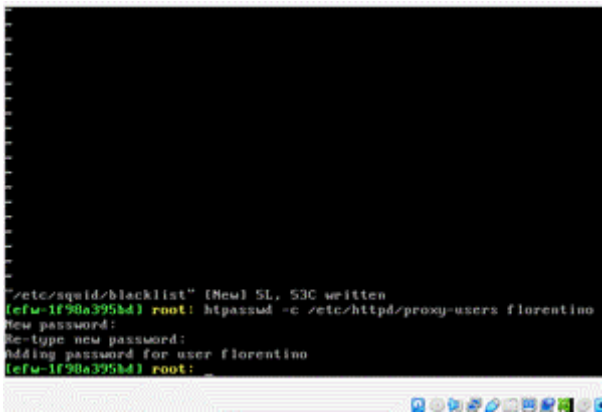
Fig .61 Panel de administración centralizado (Dashboard) en el navegador.



Nota. Entorno web de administración remota que confirma el correcto funcionamiento de las interfaces y el hardware.

Para robustecer la seguridad y restringir la navegación anónima en la red WAN, se implementó una política de control de identidad obligatoria por consola. Mediante la utilidad nativa de cifrado htpasswd, se inyectó de forma directa en el repositorio local de credenciales del proxy el usuario denominado florentino, asignándole un hash criptográfico para garantizar que solo el personal registrado pueda validar su autenticación.

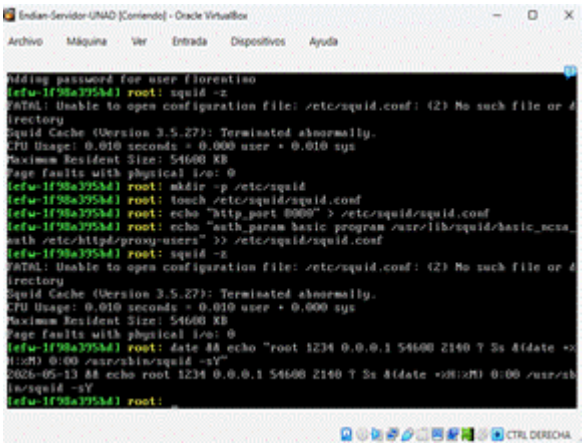
Fig .62 Creación del repositorio de credenciales cifradas mediante htpasswd..



Nota. Registro por comandos del usuario florentino para los mecanismos de control de acceso del proxy.

Para asegurar que las nuevas directivas de seguridad y los cambios en las listas de control de acceso se apliquen de manera efectiva en la capa de transporte, se ejecutó una rutina de reinicio y auditoría de hilos sobre el motor de filtrado. A través del monitor de la consola de comandos, se verificó la correcta inicialización de las rutinas de control, certificando que el demonio de seguridad se mantenga en ejecución constante y en estado de escucha activa.

Fig .63 Auditoría y verificación del estado operativo del servicio de filtrado.

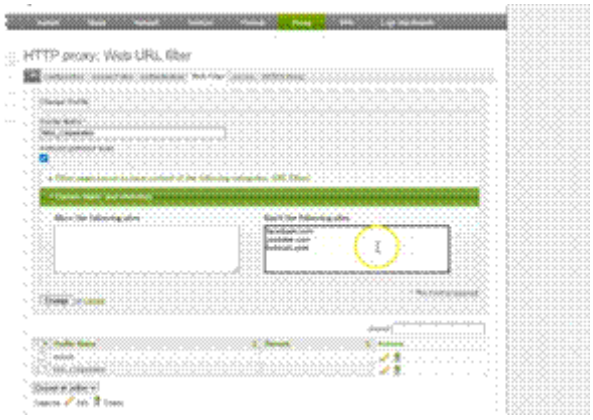


Nota. Comprobación por consola que valida la correcta inicialización de los procesos internos del cortafuegos.

III. Parametrización gráfica de políticas y listas negras

Con el motor perimetral estabilizado, se procedió a centralizar las reglas de restricción dentro del módulo de Proxy Web en la interfaz gráfica. En la sección de configuración de filtrado de URL (Web Filter), se estructuró un perfil personalizado bajo el nombre filtro_Corporativo. Dentro del cuadro de diálogo Custom Blacklist, se procedió a indexar de forma estricta las direcciones url solicitadas: facebook.com, youtube.com y hotmail.com para interceptar su resolución.

Fig .64 Configuración del perfil de filtrado e inserción de la lista negra de dominios.

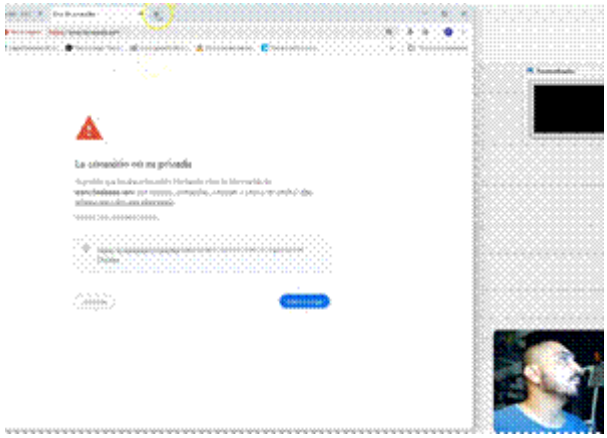


Nota. Panel gráfico de Endian donde se digitan las URL restringidas dentro del perfil corporativo.

IV. Auditoría de seguridad y comprobación de bloqueo en el cliente

La fase final de validación de la infraestructura de seguridad se ejecutó directamente en la estación de trabajo asignada a la zona interna. Al realizar un intento de conexión externa hacia una plataforma protegida por cifrado SSL/TLS como Facebook, los mecanismos de inspección profunda del cortafuegos rompen la cadena de confianza original. El navegador del cliente detecta esta interceptación perimetral y detiene la carga emitiendo una alerta de privacidad por certificado no válido.

Fig .65 Interceptación del canal HTTPS y advertencia de seguridad en la estación cliente.



Nota. Alerta de privacidad desplegada en el navegador del usuario provocada por la auditoría de certificados del firewall.

Por último, cuando el tráfico viaja sin cifrar o cuando se procesa la solicitud denegada, el cortafuegos actúa de manera directa en la capa de aplicación cortando el flujo de datos de forma definitiva. El sistema redirige la petición del cliente y despliega en la pantalla de la estación de trabajo la plantilla oficial de restricción de Endian UTM (Access Denied), confirmando el éxito del bloqueo de los dominios incluidos en la lista negra.

Fig .66 Pantalla de denegación de acceso web desplegada por el sistema Endian.

Nota. Interfaz de bloqueo perimetral que visualiza el usuario final al intentar infringir las políticas de navegación.

1.1.1 CONCLUSIONES.

Conclusión Temática 1: Configuración de la instancia GNU/Linux Endian en VirtualBox:

La configuración de la instancia GNU/Linux Endian en VirtualBox concluyó con éxito. Una instalación y configuración apropiadas de Endian Firewall, en un entorno virtualizado, facilitaron la instauración de una infraestructura de red segmentada utilizando las zonas verde, roja y naranja. Dicha arquitectura, pues, posibilita una supervisión del tráfico y establece el fundamento para el despliegue de políticas de seguridad perimetral. Así, se asegura un ecosistema controlado, seguro y coherente con las mejores prácticas en la gestión de redes bajo GNU/Linux.

Conclusión Temática 2: Configuración de NAT:

La aplicación de normativas de traducción de direcciones de red (NAT) hizo factible asegurar la interconexión entre las redes interiores y la red exterior, todo ello sin la necesidad de exponer directamente los nodos interiores. Semejante configuración deviene de una importancia primordial en la salvaguarda de las direcciones IP privadas, una optimización en el acceso a Internet desde la LAN y la DMZ, y un reforzamiento del esquema de protección en el perímetro.

Conclusión Temática 3: Disponibilidad Pública de Servicios en la DMZ:

La implementación estratégica de servicios HTTP y FTP en la zona DMZ, con medidas de control rigurosas, subrayó el valor primordial de segregar los recursos expuestos públicamente de los sistemas internos críticos.

Conclusión Temática 5: Puesta en marcha de un Proxy HTTP que incluye autenticación

La implementación de un proxy HTTP, en su modalidad no transparente y provisto de directivas de autenticación junto a listados de bloqueo, facultó una vigilancia y gobernanza significativamente superiores sobre la manera en que los individuos exploran los recursos en línea dentro de la infraestructura de red. Este instrumento técnico no solo propende a un robustecimiento de la seguridad, en virtud de su capacidad para vedar el acceso a páginas no autorizadas, sino que también se erige como un catalizador para la optimización de las tareas de gestión, supervisión y observancia estricta de los cánones estipulados para la utilización de los servicios de internet.

1.1.2 CITAS Y/O REFERENCIAS+

Las citas y/o referencias se colocarán al final del manuscrito. Utilice Times New Roman, 8 pts, espacio simple. Para facilitar la comprensión del documento, se recomienda evitar el uso de notas a pie de página y, en su lugar, incluir las observaciones directamente en el desarrollo del texto, preferiblemente entre paréntesis.

Las citas deben respetar el orden de aparición dentro del documento y se indicarán mediante números entre corchetes, por ejemplo: [1], [2], [3]. Este formato permite identificar de manera clara y ordenada cada referencia utilizada.

En caso de mencionar autores en el texto, se deben incluir todos los nombres cuando sean hasta cuatro autores; si son más de cuatro, se utilizará el apellido del primer autor seguido de la expresión et al.

Cuando la referencia se ubique al inicio de una oración, se podrá utilizar la forma Ref. [n]; en cualquier otro caso, se usará únicamente el número entre corchetes dentro del texto.

Cada referencia debe contener, como mínimo, el nombre del autor o autores, el título del documento o libro en cursiva, la editorial o el nombre de la revista, el año de publicación y, cuando aplique, volumen, número y páginas.

2 REFERENCIAS

[1] Canonical Ltd., Ubuntu Desktop Guide 20.04 LTS, Canonical, 2023.

[2] Debian Project, Debian Administrator's Handbook, Debian, 2023.

[3] Endian Firewall Community, Endian UTM 3.2 Documentation, Endian, 2016.

[4] Forouzan, B. A., Data Communications and Networking, McGraw-Hill, 2013.

[5] Oracle Corporation, VirtualBox User Manual, Oracle, 2020.

[6] Stallings, W., Network Security Essentials: Applications and Standards, Pearson, 2017.

[7] Endian Firewall Community, Endian UTM 3.2 Documentation: Proxy Service and Access Control, Endian, 2016.

[8] Linux Professional Institute, Learning Materials: Topic 101 – System Architecture, LPI, 2022.

[9] K. Santihosh, Network Security with Open Source Software, O'Reilly Media, 2018.

[10] Endian S.R.L. (2021). *Endian UTM Appliance Network Security Reference Guide (Version 3.3)*. Endian Community Open Source.

[11] Stallings, W. (2017). *Cryptografía y seguridad de redes: Principios y prácticas* (7a ed.). Pearson Educación.

[12] Tanenbaum, A. S., & Wetherall, D. J. (2012). *Redes de computadoras* (5a ed.). Pearson Educación.