IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL EN GNU/LINUX MEDIANTE FIREWALL ENDIAN EN ENTORNOS LAN, WAN Y DMZ

Helman Camilo Blanco Cárdenas
hcblancoc@unadvirtual.edu.co
Luis Alejandro Zamora Méndez
lazamorame@unadvirtual.edu.co
Eidher Alexander Cardozo Campos
eacardozoca@unadvirtual.edu.co
Brian Felipe Restrepo Salamanca
bfrestrepos@unadvirtual.edu.co

RESUMEN: *La seguridad perimetral es fundamental para proteger la infraestructura tecnológica en entornos empresariales con múltiples servicios y segmentos de red. Este artículo presenta la implementación de un esquema integral de seguridad utilizando Endian Firewall y sistemas GNU/Linux, con un enfoque práctico orientado al control del tráfico, la segmentación de redes y la gestión de accesos.*

El proyecto se desarrolló en un entorno virtualizado que incluyó las zonas LAN, DMZ y WAN, simulando un escenario real de administración de redes. Se abordaron cinco aspectos clave: instalación y configuración de Endian, uso de NAT, publicación segura de servicios en la DMZ, definición de reglas de acceso interzona y configuración de un proxy HTTP con autenticación y filtrado de contenidos. Los resultados evidencian una arquitectura robusta y replicable que fortalece la seguridad perimetral y la formación en administración de sistemas Open Source.

PALABRAS CLAVE: Arquitectura de red, Endian Firewall, GNU/Linux, Seguridad perimetral.

1 INTRODUCCIÓN

La seguridad perimetral constituye uno de los componentes esenciales para la protección de infraestructuras tecnológicas en entornos empresariales y académicos. En un escenario donde los ataques informáticos, accesos no autorizados y vulnerabilidades asociadas a redes no segmentadas representan amenazas crecientes, se hace indispensable la implementación de arquitecturas de seguridad que garanticen el aislamiento, control y monitoreo del tráfico entre diferentes zonas de red.

En este contexto, las distribuciones GNU/Linux han demostrado ser una solución sólida y confiable para la administración de servicios críticos y la implementación de herramientas de protección, gracias a su estabilidad, flexibilidad y naturaleza Open Source.

El presente trabajo se desarrolló en el marco de la Etapa 7 del Diplomado en Administración de Sistemas Operativos Open Source, cuyo objetivo principal consistió en la configuración e implementación de un entorno de seguridad perimetral utilizando la distribución Endian Firewall y servidores GNU/Linux. Para ello, se diseñó una arquitectura compuesta por tres zonas: la red Verde (LAN), destinada a dispositivos internos confiables; la red Roja (WAN), encargada de la conexión con Internet; y la red Naranja (DMZ), orientada a la exposición controlada de servicios web y FTP. Esta segmentación permitió recrear un escenario real de seguridad empresarial en el cual se aplicaron buenas prácticas de administración de redes y control de tráfico.

Durante la ejecución del proyecto se trabajó de manera colaborativa en cinco temáticas específicas: instalación y configuración de Endian, implementación de NAT para permitir la comunicación LAN/WAN y DMZ/WAN, publicación de servicios desde la DMZ, establecimiento de reglas de acceso interzona y la puesta en marcha de un proxy HTTP con autenticación y filtrado de contenidos.

Cada temática fue abordada desde la consola, cumpliendo estrictamente las políticas establecidas por la guía de aprendizaje, lo cual permitió reforzar competencias prácticas en administración de redes y servidores bajo entornos GNU/Linux.

Asimismo, se realizaron pruebas de conectividad, validación de reglas, análisis de tráfico, verificación de políticas y documentación detallada de cada proceso, lo que permitió obtener evidencia técnica replicable en diferentes contextos. La experiencia de trabajo grupal favoreció la integración de habilidades individuales orientadas hacia un mismo objetivo, fomentando la comunicación eficiente, la gestión del conocimiento y la solución colaborativa de incidentes y configuraciones.

Finalmente, este artículo presenta la totalidad del proceso de implementación desarrollado en cada temática, exponiendo la configuración aplicada, los resultados obtenidos y las conclusiones generales del equipo.

El propósito es ofrecer un documento técnico estructurado bajo los lineamientos IEEE que permita comprender la importancia de los mecanismos de seguridad perimetral y su aplicación práctica en infraestructuras basadas en GNU/Linux.

2 DESARROLLO DE LAS TEMÁTICAS

Tabla 1. Asignación de Roles y Temáticas.

Rol	Estudiante				
Temática	Compilador	Evaluador	Entregas	Alertas	Revisar
Temática 1: Configuración de la instancia para GNU/Linux				Luis Alejandro Zamora	
Temática 2: Configuración NAT			Helenas Camilo Blanco		
Temática 3: Permitir servicios de la Zona DMZ para la red	Esther Alexander Cárdozo				
Temática 5: Implementar un Proxy HTTP (No transparente)					Brian Felipe Restrepo

Fuente: Autoría Propia

2.1 TEMATICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO.

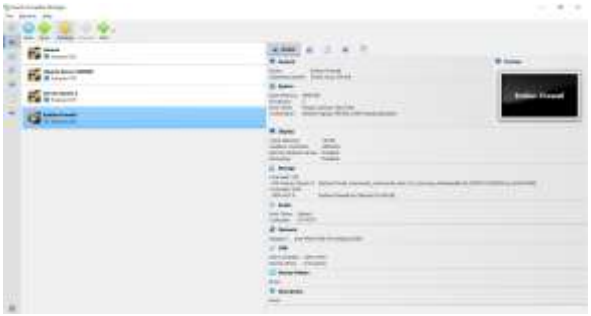
La implementación de firewalls perimetrales constituye una práctica fundamental en la protección y segmentación de redes. En esta actividad se configura el sistema GNU/Linux Endian Firewall en VirtualBox, cumpliendo los requerimientos de la Temática 1: instalación de la instancia, configuración de tarjetas de red y establecimiento de tres zonas de seguridad: VERDE (LAN), NARANJA (DMZ) y ROJA (WAN).

El objetivo es comprender la arquitectura básica de seguridad, validar la comunicación entre zonas y confirmar el funcionamiento correcto del firewall.

2.1.1 INSTALACIÓN DE ENDIAN FIREWALL

Se creó una máquina virtual en VirtualBox utilizando la imagen ISO de Endian Firewall Community. Durante la instalación se definió el esquema de red basado en tres adaptadores, cada uno correspondiente a una zona específica del firewall.

Figura 1. Configuración inicial de la máquina virtual Endian Firewall en VirtualBox

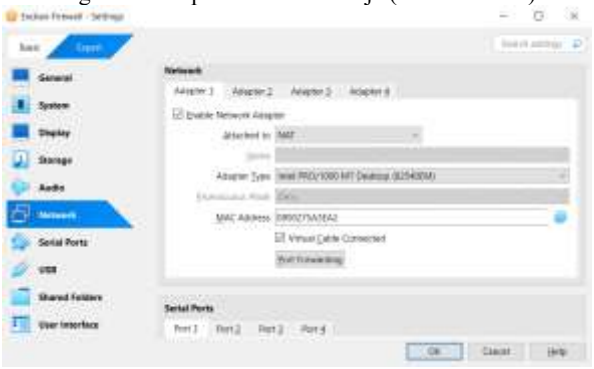


Fuente: Autoría Propia

2.1.2 CONFIGURACIÓN DE TARJETAS E INTERFACES

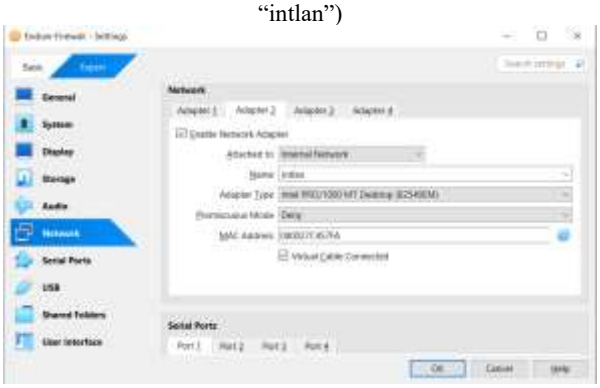
La asignación final de interfaces quedó de la siguiente manera:
• Zona VERDE (eth1): 192.168.10.1/24 — LAN interna.
• Zona NARANJA (eth0): 192.168.20.1/24 — DMZ para servidores.
• Zona ROJA (eth2): DHCP — conexión hacia Internet.
Esta configuración garantiza el aislamiento correcto entre zonas, cumpliendo la arquitectura estándar del modelo de seguridad Endian.

Figura 2. Adapter 1 → Zona Roja (WAN – NAT)



Fuente: Autoría Propia

Figura 3. Adapter 2 → Zona Verde (LAN – Internal Network "intlan")



Fuente: Autoría Propia

Figura 4. Adapter 3 → Zona Naranja (DMZ – Internal Network dmz")2.1

Fuente: Autoría Propia

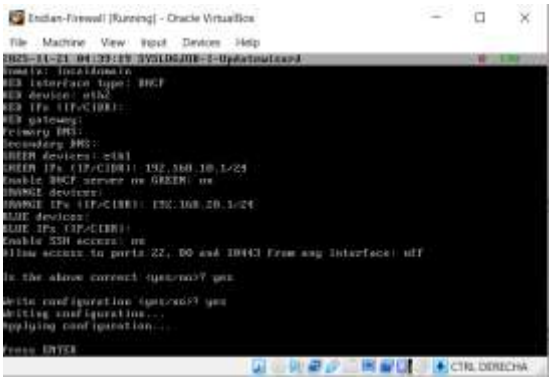
2.1.3 CONFIGURACIÓN DE INTERFACES EN EL WIZARD

Durante la ejecución del asistente se configuraron las interfaces así:

RED (Zona Roja): DHCP – eth2
GREEN (Zona Verde): eth1 – 192.168.10.1/24 (DHCP activo)

ORANGE (Zona Naranja): eth0 – 192.168.20.1/24
Habilitación de SSH: ON

Figura 5. Configuración final de las zonas RED, GREEN y ORANGE en Endian Firewall

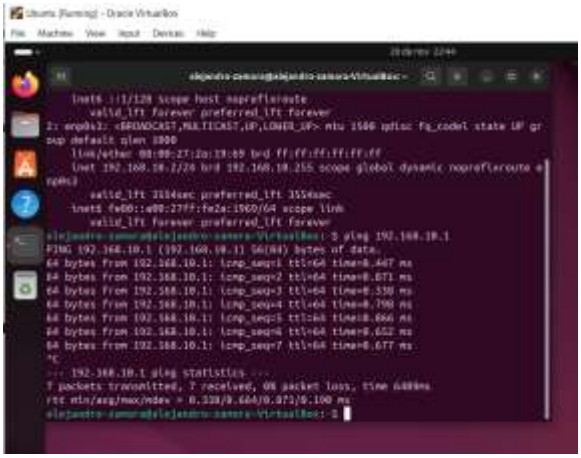


Fuente: Autoría Propia

2.1.4 VALIDACIÓN DE CONECTIVIDAD

Para validar el funcionamiento, se implementó una máquina Ubuntu conectada a la zona VERDE. El cliente obtuvo la IP 192.168.10.2 mediante DHCP. Se realizaron pruebas exitosas de conectividad hacia el firewall (ping a 192.168.10.1) y acceso a la interfaz web mediante HTTPS en el puerto 10443.

Figura 6. Prueba de conectividad entre Ubuntu y la zona verde del firewall Endian



Fuente: Autoría Propia

Figura 7. Pantalla de registro inicial de Endian Firewall Community

Fuente: Autoría Propia

2.2 TEMATICA 2: CONFIGURACIÓN NAT

Se implementaron reglas NAT para permitir el acceso a Internet desde la red LAN y desde la DMZ.

- **NAT LAN → WAN** utilizando *MASQUERADE*.
- **NAT DMZ → WAN** restringido por subred.
- Pruebas realizadas mediante ping, curl y verificaciones de tabla NAT.

Esta temática permitió validar el funcionamiento del firewall como puente seguro entre redes internas y externas.

La segunda temática del proyecto se centró en la configuración de la traducción de direcciones de red (NAT, por sus siglas en inglés), un mecanismo fundamental para permitir que múltiples dispositivos internos accedan a recursos externos utilizando una sola dirección IP pública o una interfaz de salida a Internet. En el contexto del firewall Endian, NAT constituye una herramienta indispensable para gestionar la comunicación entre las zonas internas (LAN y DMZ) y la zona externa (WAN), garantizando seguridad, eficiencia y control del tráfico.

Tabla 2. Arquitectura Requerida.

Zona	Maquina	Función	IP Recomendada
LAN (Verde)	Ubuntu Desktop	Cliente interno	192.168.10.10
FIREWALL	Ubuntu Server / Endian	Router + NAT	LAN: 192.168.10.1 / DMZ: 192.168.20.1 / WAN: DHCP
DMZ (Naranja)	Ubuntu Server Web	Servidor web/ftp	192.168.20.10

Fuente: Autoría Propia

El objetivo principal de esta temática fue habilitar el tráfico desde la red Verde (LAN) hacia la red Roja (WAN) y desde la red Naranja (DMZ) hacia la WAN, asegurando que ambas zonas pudieran acceder a Internet a través del firewall. Este proceso

incluyó la verificación de tablas de traducción, pruebas de conectividad, monitoreo del flujo de paquetes y validación de las reglas autogeneradas por Endian.

2.2.1 CONCEPTOS FUNDAMENTALES DE NAT APLICADOS EN EL FIREWALL

Dentro de la arquitectura configurada, la LAN (192.168.10.0/24) y la DMZ (192.168.20.0/24) son redes privadas que requieren traducción de direcciones para comunicarse con Internet. La interfaz Roja, por su parte, recibe su dirección IP mediante DHCP, representando la red externa.

Endian utiliza principalmente dos tipos de NAT:

SNAT/MASQUERADE:
Traduce direcciones privadas en una única IP de salida. Es el mecanismo principal utilizado para permitir navegación desde LAN o DMZ hacia Internet.
DNAT/Port Forwarding:
Redirige conexiones entrantes desde la WAN hacia servidores ubicados en la DMZ.
Este mecanismo se trabaja en la Temática 3.

Durante esta temática se trabajó esencialmente con SNAT, específicamente mediante la opción **MASQUERADE**, diseñada para interfaces configuradas por DHCP.

2.2.2 ACTIVACIÓN DEL NAT PARA LA LAN HACIA LA WAN

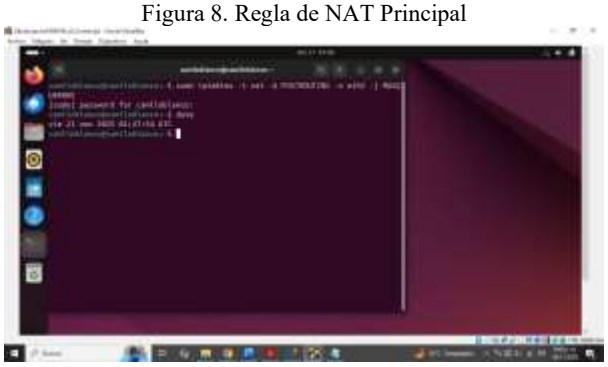
Una vez configurada la conectividad básica de la Temática 1, se procedió a validar el enrutamiento entre las redes. Para permitir que los equipos de la LAN accedieran a Internet, Endian generó automáticamente reglas NAT basadas en la activación del módulo "Allow outbound traffic" en la zona Verde.

Este procedimiento se verificó mediante:

- Revisión de la tabla NAT en el firewall.
- Pruebas de navegación desde el cliente Ubuntu Desktop.
- Comprobación de asignación de gateway hacia la interfaz Green (192.168.10.1).
- Pruebas con ping, curl, traceroute y nslookup.

La tabla NAT mostró la creación de reglas MASQUERADE dirigidas desde la subred 192.168.10.0/24 hacia la interfaz Red, lo que confirmó que el tráfico de la LAN estaba siendo traducido correctamente.

Figura 8. Regla de NAT Principal



Fuente: Autoría Propia

2.2.3 ACTIVACIÓN DEL NAT PARA LA DMZ HACIA LA WAN

Posteriormente, se trabajó con la red DMZ, cuyo propósito es servir como zona de semi-confianza donde residen servidores expuestos, como el servidor web y el servidor FTP configurados en la Temática 3. Para que estos servidores pudieran obtener actualizaciones, resolver dominios o interactuar con servicios externos, se activó el NAT para la zona Naranja.

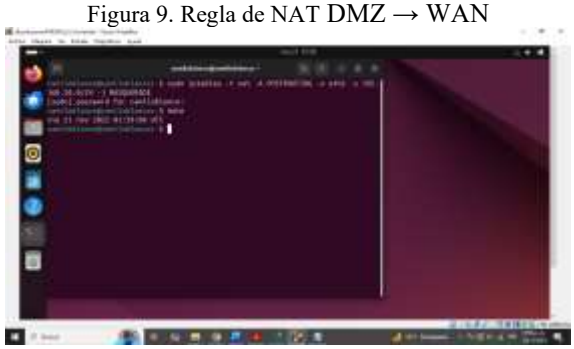
Esta configuración no se activa automáticamente, por lo que fue necesario habilitar manualmente las políticas correspondientes en el panel de firewall. Se generaron reglas SNAT que permitían que las direcciones 192.168.20.0/24 fueran traducidas por la interfaz Red hacia Internet.

Posteriormente, se realizaron pruebas desde el servidor web alojado en la DMZ, verificando:

- Resolución DNS (dig, nslookup).
- Conexiones HTTP y HTTPS de salida (curl hacia repositorios oficiales).
- Comprobación del gateway asignado (192.168.20.1).

Una vez validadas estas pruebas, se confirmó el correcto funcionamiento del NAT para la DMZ.

Figura 9. Regla de NAT DMZ → WAN



Fuente: Autoría Propia

2.2.4 VERIFICACIÓN DE LAS REGLAS NAT Y FUNCIONAMIENTO DEL REENVÍO

la verificación técnica fue un componente esencial de esta temática. Se revisaron las siguientes áreas:

Tabla NAT del firewall

Se observaron entradas de tipo:

- POSTROUTING - MASQUERADE - eth2
- SNAT -o red0 -s 192.168.10.0/24
- SNAT -o red0 -s 192.168.20.0/24

Estas reglas evidenciaron la traducción activa para ambas subredes internas.

Monitoreo de tráfico

Desde el panel de Endian se analizó:

- Cantidad de conexiones NAT en tiempo real.
- Dirección fuente y puerto traducido.
- Dirección externa asignada.

Pruebas desde las máquinas internas

Desde LAN y DMZ se realizaron comandos como:

- ping 8.8.8.8
- curl http://google.com
- traceroute 8.8.4.4

Estas pruebas confirmaron que el tráfico salía correctamente del firewall y retornaba a las interfaces internas.

Figura 10. Verificación Reglas en el Firewall

Fuente: Autoría Propia

2.2.5 IMPORTANCIA DEL NAT DENTRO DEL ESQUEMA DE SEGURIDAD

La correcta implementación de NAT es clave para el funcionamiento de toda la arquitectura del proyecto, puesto que:

- Asegura que las redes privadas puedan comunicarse con Internet sin exponer sus direcciones reales.
- Actúa como un primer nivel de seguridad ocultando la topología interna.
- Permite controlar qué zonas pueden o no tener salida hacia la WAN.
- Facilita la aplicación posterior de reglas de firewall y proxy.
- Evita que los servidores de la DMZ queden expuestos directamente, mitigando riesgos.

Sin NAT, la DMZ no podría actualizar paquetes, la LAN no tendría acceso a recursos externos y el firewall sería incapaz de actuar como gateway.

2.3 TEMATICA 3: PERMITIR SERVICIOS DESDE DMZ

Se configuró la publicación de servicios web (HTTP – puerto 80) y FTP (puerto 21) desde la DMZ hacia la LAN y la WAN.

Adicionalmente, se configuró la denegación del protocolo ICMP para evitar el uso de ping como método de reconocimiento de red.

Se verificó el funcionamiento mediante:

- Acceso a páginas web alojadas en la DMZ.
- Transferencias FTP entre zonas.
- Bloqueo del ICMP desde la LAN y DMZ.

Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server. Denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red.

Probar a través de una consola o terminal la no respuesta del comando ping hacia una IP de la red. Verificar en el tráfico de salida, la creación de las reglas.

2.3.1 INSTALACIÓN Y CONFIGURACIÓN DE ENDIAN

Se realiza la instalación y configuración de Endian firewall en un entorno virtualizado para esto se utilizó la versión 3.3.2 descarga de la imagen ISO desde el sitio oficial en SourceForge (https://sourceforge.net/projects/efw).

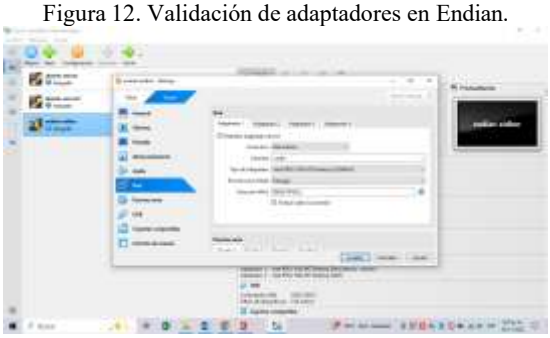
De esta forma se procede con la configuración de la máquina en la herramienta de VirtualBox.

Figura 11. Configuración máquina virtual Endian.

Fuente. Autoría Propia.

Antes de realizar con el proceso de instalación de la máquina se realizó la configuración de los adaptadores de red que se utilizaran en el proceso para esto se tuvieron presentes las zonas roja, verde y naranja en el cual se validaron en el proceso de instalación.

Figura 12. Validación de adaptadores en Endian.



Fuente. Autoría Propia.

Una vez realizadas dichas configuraciones se proceden con las validaciones de instalación del Endian en el cual se instala en idioma inglés, se procede con las configuraciones y particiones del disco duro de esta forma se procede con aceptar dichos procesos.

Se procede a realizar la validación de permitir el acceso a los servicios HTTP mediante los puertos 80 y FTP por el puerto 21 esto mediante el servidor Web estas configuraciones se realizan mediante la opción de Firewall en el tráfico entre zonas.

Esta validación se realiza mediante la creación de una nueva regla en el cual se seleccionará la zona naranja de origen y el destino la zona verde esto para el servicio HTTP con el protocolo TCP para el puerto 80 y de esta forma se permite.

Figura 13. Particiones del disco en Endian.

Fuente. Autoría Propia.

Se realiza las configuraciones de la IP de la zona verde que este caso hace referencia a la máquina que tiene asignado el cliente el cual es el Desktop el cual se le asigno la IP 192.168.0.15/24 con una máscara de red 255.255.255.0 de esta forma se estará configurando la primera zona que necesita para el proceso del Endian.

Figura 14. Validación de la Ip de zona verde Desktop.

Fuente. Autoría Propia.

De esta forma se obtiene la URL de acceso para la parte gráfica de la configuración del Endian esto quedando de esta forma http://192.168.0.15:40443 esto haciendo referencia a la zona verde configurada anteriormente y procedido se da Ok para confirmar dichas configuraciones necesarias para el proceso y utilización del servicio Endian.

Figura 15. Validación de URL de acceso Endian

Fuente. Autoría Propia.

Mediante este proceso inicial se obtienen las configuraciones de la zona verde y roja que en este caso la IP se obtiene de manera automática por DHCP: 10.0.3.15/24.

Figura 16. Configuraciones de zona verde y roja

Fuente. Autoría Propia.

Se accede a la URL asignada mediante el equipo Desktop el cual este está configurado por medio del adaptador verde validado en la máquina de Endian esta máquina tiene la IP 192.168.0.15 el cual se ingresa por medio del navegador y obtenemos respuesta de manera correcta esto con el fin de realizar las respectivas configuraciones de acceso desde la interfaz gráfica.

Figura 17. Configuraciones previas del proceso Endian

Fuente. Autoría Propia.

Una vez realiza el proceso de configuraciones iniciales se procede a validar las configuraciones de red en el cual este queda por medio del enrutamiento esto mediante la conexión DHCP se le da siguiente y se procede con la configuración del adaptador red faltante en este caso la zona naranja el cual cumple la función del servidor DMZ esto validado mediante

la IP 192.168.0.15/24 y la máscara de red 255.255.255.0 de igual forma se permite visualizar las tarjetas de red de cada uno de los adaptadores configurados.

2.3.2 CONFIGURACIÓN DE ZONAS EN EL SERVIDOR

Figura 18. Configuración zona naranja servidor

Fuente. Autoría Propia

De esta forma se permitirá visualizar cada una de las configuraciones de adaptadores de red la zona roja es la conexión a internet esto validado mediante el tipo NAT.

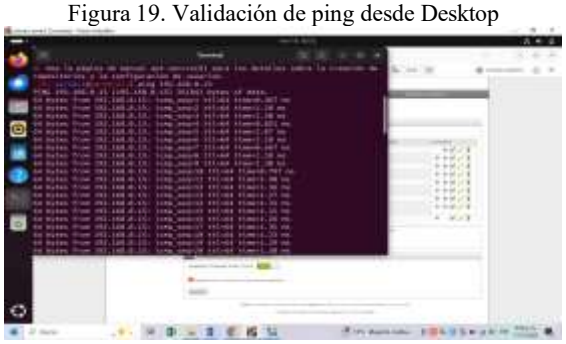
Se aceptan las configuraciones necesarias y se permitirá acceder de manera exitosa a las configuraciones del Endian en el cual podemos observar las previas configuraciones de las diferentes zonas de red.

Cada una de las validaciones realizadas permitirá acceder de manera correcta a las máquinas configuradas en este caso el Desktop y server que se tendrán en cuenta para este proceso se realizan las previas validaciones de acceso y ping en cada una de las máquinas esto con el fin de que en cada una esté tomando su Ip correspondiente. Se deben realizar configuraciones previas de las validaciones de los DNS en este caso se adicionan los accesos de Google.

De esta forma se definió el nombre del host en este caso se deja svr-firewall y el nombre del dominio localdomain de esta manera se permiten visualizar de manera correcta los tres adaptadores.

2.3.3 VALIDACIÓN DE PING DESDE DESKTOP Y SERVER DMZ

Figura 19. Validación de ping desde Desktop



Fuente. Autoría Propia.

Figura 20. Validación de ping desde Server DMZ

Fuente. Autoría Propia.

2.3.4 REALIZACIÓN DEL PERMISO DE SERVICIO FTP PARA EL PROTOCOLO TCP

Para la realización del permiso de servicio FTP para el protocolo TCP mediante el puerto 21 esto para la zona naranja como origen y verde destino.

Figura 21. Ingreso de la regla de servicio HTTP puerto 80

Fuente. Autoría Propia.

Figura 22. Ingreso de regla de servicio FTP puerto 21

Fuente. Autoría Propia.

Se realiza la configuración de la denegación del protocolo ICMP para los puertos 80 y 30 el cual no se permitirá realizar ping en el cual se procede a realizar la creación de la nueva regla en el cual se deja validado desde el origen como zona verde y destino naranja realizando la denegación del protocolo de esta manera si se realiza ping desde el equipo de Desktop no se permite realizar ninguna petición de ping a la Ip 192.168.0.15 una vez realiza estas configuraciones de creaciones de reglas se debe aplicar los cambios para que se ve han reflejados.

Figura 23. Creación de regla para denegación de protocolo ICMP

Fuente. Autoría Propia.

2.4 TEMATICA 5: IMPLEMENTACIÓN DE PROXY HTTP

Se configuró un proxy HTTP no transparente en Endian con:

Lista negra que bloquea sitios como:

www.hotmail.com
www.youtube.com
www.elnuevodia.com.co

- Autenticación por usuarios y grupos.
- Asociación del usuario con políticas de navegación.
- Pruebas de acceso desde la LAN con resultados de bloqueo correctos.

Esta temática reforzó conocimientos sobre control de acceso, monitoreo y auditoría de navegación.

2.4.1 PARAMETRIZACIÓN DE LA MÁQUINA DE ENDIAN

Se parametrizo la maquina con la imagen iso de Endian a la cual se le dio poca capacidad ya que sus necesidades de recursos son muy bajas.

Figura 24. Parametrización

Fuente. Autoría Propia.

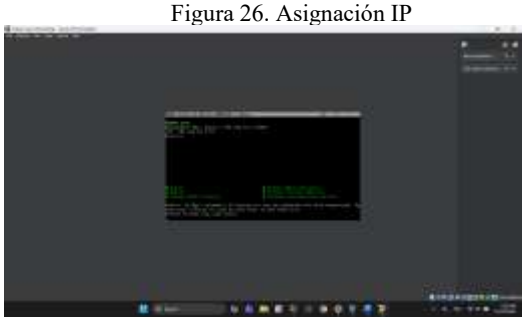
Directamente desde Endian se procede a realizar todos los procesos de parametrización para iniciar la máquina.

Figura 25. Inicio máquina virtual

Fuente. Autoría Propia.

Una vez iniciada la maquina y dentro de ella se procedió a asignar una ip y tipos de conexiones por zonas, para este ejercicio se cuadro la 192.168.0.15

Figura 26. Asignación IP



Fuente. Autoría Propia.

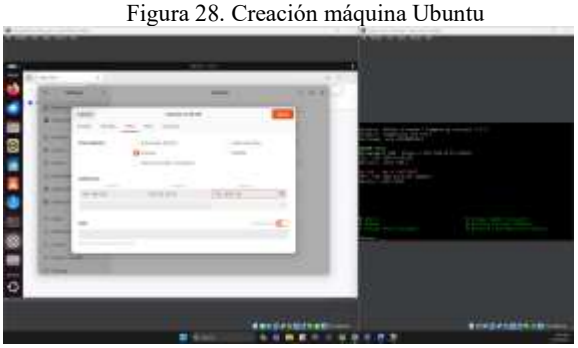
Figura 27. Configuración IP

Fuente. Autoría Propia

2.4.2 PARAMETRIZACIÓN DE LA MÁQUINA DE UBUNTU PARA LA RESTRICCIÓN DEL PROXY.

Una vez creada y configurada la máquina de Endian, se realizó un proceso de creación de una máquina de Ubuntu, a esta máquina se le asigno la ip 192.168.0.50 la cual fue conectada por conexión LAN con la máquina del Firewall de Endian.

Figura 28. Creación máquina Ubuntu

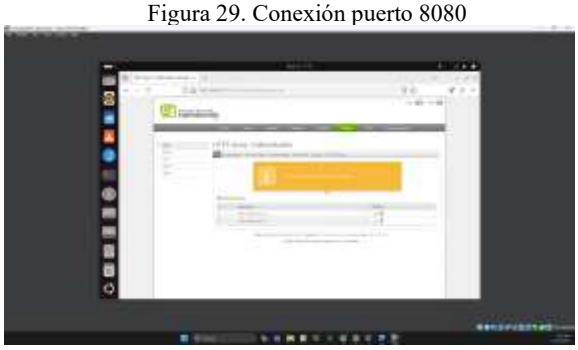


Fuente. Autoría Propia

2.4.3 ACCESO Y CONFIGURACIÓN DEL PROXY.

Una vez conectado, se accedió a la ip de Endian por el puerto 8080 y se colocaron clave y contraseña inicial, una vez dentro se activó la opción de proxy, en ella se cuadro una autenticación de usuarios, para el ejercicio fueron creados dos usuarios.

Figura 29. Conexión puerto 8080



Fuente. Autoría Propia.

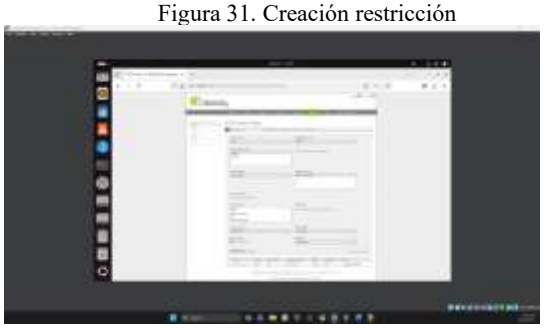
Tambien se creó un grupo para encerrar uno de los dos usuarios.

Figura 30. Creación grupo

Fuente. Autoría Propia.

Luego se creó la restricción de acceso de los usuarios a las páginas de www.hotmail.com, www.youtube.com y www.elnuevodia.com.co, estos entraron en la política de acceso del proxy que restringiría el acceso a los usuarios envueltos en el grupo creado, es decir el usuario 1.

Figura 31. Creación restricción



Fuente. Autoría Propia.

2.4.4 CONFIGURACIÓN DEL PROXY EN EL SERVIDOR UBUNTU.

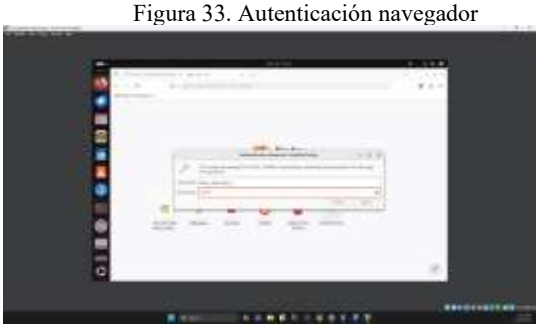
En la máquina de Ubuntu se colocó la restricción de proxy, allí se activó y se colocó la ip del Firewall y el número del puerto.

Figura 32. Creación firewall

Fuente. Autoría Propia.

Una vez configurado se confirmó que el navegador pidiera las credenciales de la cuenta o usuario que debía estar autenticado, se colocó para el ejemplo el usuario número 1.

Figura 33. Autenticación navegador



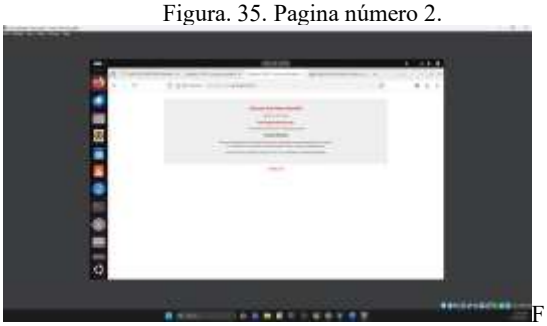
Fuente. Autoría Propia.

Por último, se intentó tener acceso a las páginas restringidas por el Proxy, confirmando que no se tienen el acceso a las páginas.

Figura. 34. Pagina número 1 www.hotmail.com.

Fuente. Autoría Propia.

Figura. 35. Pagina número 2.



Fuente. Autoría Propia.

Para el último caso hubo algo diferente y es que la url finalizaba en com.co, al ingresar la url se puso .com y permitió el acceso.

Figura. 36. Ingreso URL

Fuente. Autoría Propia.

Al colocar la url correcta denegó el acceso.

Figura. 37. Comprobación acceso

Fuente. Autoría Propia.

3 CONCLUSIONES

La implementación de Endian Firewall en VirtualBox permitió comprender la estructura de segmentación por zonas y los principios básicos del filtrado perimetral. La configuración de las zonas VERDE, NARANJA y ROJA se realizó correctamente, validando que el firewall administra las redes internas y externas de manera segura. Las pruebas de conectividad confirman que la arquitectura funciona según los requerimientos de la Temática 1.

La implementación de NAT permitió validar el funcionamiento del firewall como puerta de enlace segura entre redes privadas y redes externas. Al garantizar la salida controlada desde la LAN y la DMZ hacia la WAN, se comprobó la eficacia del mecanismo MASQUERADE para traducir direcciones privadas sin exponer la topología interna.

Las pruebas realizadas confirmaron que NAT es un componente fundamental de la infraestructura, ya que posibilita conectividad externa sin comprometer la seguridad del sistema.

El desarrollo de las cinco temáticas permitió al grupo comprender y aplicar de manera integral los

principios de seguridad perimetral y administración de redes bajo sistemas operativos GNU/Linux.

La utilización de Endian Firewall como herramienta central facilitó la implementación de una arquitectura funcional y segura, capaz de segmentar la red, controlar el tráfico y ofrecer servicios protegidos a través de la DMZ.

De igual forma, el trabajo práctico evidenció la importancia de combinar técnicas como NAT, DNAT, filtrado interzona, autenticación de proxy y restricciones de protocolo para crear un entorno seguro y alineado con las mejores prácticas de seguridad informática. Cada integrante del grupo aportó conocimiento técnico y soluciones que permitieron enriquecer el proceso de aprendizaje, promoviendo la colaboración y la toma de decisiones orientadas a la seguridad.

En conclusión, el proyecto demostró que la seguridad perimetral requiere una arquitectura bien diseñada, políticas estrictas y una correcta interacción entre servicios y mecanismos de protección.

La implementación de Endian Firewall, acompañada de servidores Linux configurados exclusivamente desde la terminal, permitió establecer un entorno seguro y funcional que refleja fielmente las necesidades de las organizaciones modernas.

La experiencia adquirida fortalece la capacidad de los participantes para administrar infraestructuras de red reales, aplicar controles de acceso efectivos y diseñar soluciones de seguridad coherentes con los desafíos actuales del entorno digital.

4 REFERENCIAS

[1] LPI LPIC-1 Exam 101. (2022). *Tema 101: Arquitectura del Sistema*. https://learning.lpi.org/es/learning-materials/101-500/101/

[2] LPI LPIC-1 Exam 101. (2022). *Tema 102: Instalación de Linux y gestión de paquete*s . https://learning.lpi.org/ es/learning -materials/101-500/102/

[3] Canonical (2023). *Guía del Ubuntu desktop 20.04 LTS . Help Ubuntu*. https://help.ubuntu.com/20.04/ubuntu - help/index.html

[4] Debian (2023). *El manual del administrador de Debian 12.5.0 .Debian*. https://www.debian.org/releases/stable/amd64/index.es.html

[5] Oracle (2020). *Manual de usuario VirtualBox*. VirtualBox . https://www.virtualbox.org/manual/

[6] Endian (2016), *Endian UTM 3.2 Manual referencia* . Endian. http://docs.endian.com/3.2/utm/index.html

[7] Jay LaCroix. (2020). Mastering Ubuntu Server : *Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server* . Packt Publishing. https://research-ebsco-com. bibliotecavirtual.unad.edu.co /linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[8] Stallings, W. (2020). *Network Security Essentials: Applications and Standards*. Pearson Education.

[9] Scarfone, K., & Hoffman, P. (2009). *Guidelines on Firewalls and Firewall Policy (SP 800-41 Rev.1)*. National Institute of Standards and Technology (NIST). https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final

[10] Behl, A., & Behl, K. (2017). *Cyberwar: The Next Threat to National Security and What to Do About It*. Oxford University Press.

[11] Red Hat. (2023). *Securing Networks with Firewalls and Packet Filtering*. Red Hat Documentation. https://access.redhat.com/documentation

[12] Pfaff, B., Davie, B., & Pettit, J. (2015). *The Architecture of Open Source Applications: Networking and Security*. Lulu Press.