IMPLEMENTACIÓN DE GNU/LINUX ENDIAN EN VIRTUALBOX CON ZONAS VERDE, ROJA Y NARANJA

Tania Julieth Álvarez Morales
e-mail: tjalvarezm@unadvirtual.edu.co
Maira Vannesa Robledo Angulo
e-mail: mvrobledoa@unadvirtual.edu.co
Christian Ernesto Lara Plazas
e-mail: celarap@unadvirtual.edu.co
Freddy Camilo Aldana Salas
e-mail: fcaldanas@unadvirtual.edu.co
Cristian Andrés Sevillano Molina
e-mail: casevillanom@unadvirtual.edu.co

RESUMEN: *En este trabajo se implementó un entorno de seguridad perimetral utilizando la distribución GNU/Linux Endian Firewall en VirtualBox, configurando tres zonas de red fundamentales: verde (LAN), naranja (DMZ) y roja (WAN). Cada zona fue asociada a un adaptador de red independiente, lo que permitió su segmentación y el control granular del tráfico. Se configuraron reglas de NAT para permitir la comunicación segura desde la LAN y la DMZ hacia Internet, además de establecer políticas de acceso mediante firewall y un proxy HTTP con autenticación. Se realizaron pruebas de conectividad entre las zonas y hacia servidores externos, validando el funcionamiento del enmascaramiento, la segmentación y las políticas de seguridad implementadas. Los resultados evidencian la importancia de la separación de redes, el control del tráfico perimetral y la administración centralizada mediante la consola web de Endian, preparando al estudiante para escenarios reales de gestión de firewalls en entornos corporativos.*

PALABRAS CLAVE: Endian Firewall, GNU/Linux, NAT, DMZ, Seguridad Perimetral, Virtualización, Proxy, Redes.

1 INTRODUCCIÓN

La seguridad en redes informáticas constituye un pilar fundamental para la protección de la información y la continuidad operativa de las organizaciones. En un entorno altamente interconectado, las amenazas externas e internas pueden comprometer la integridad, disponibilidad y confidencialidad de los datos, lo que hace indispensable la adopción de mecanismos de defensa robustos. Entre estas medidas, los firewalls perimetrales desempeñan un papel esencial al controlar el tráfico, segmentar redes y aplicar políticas que mitiguen riesgos y limitan la superficie de ataque. En este contexto, se seleccionó Endian Firewall, una distribución GNU/Linux especializada en seguridad perimetral, reconocida por su facilidad de administración y su capacidad para gestionar zonas de red diferenciadas mediante una consola web intuitiva. Su naturaleza libre, su arquitectura modular y su compatibilidad con entornos virtualizados como VirtualBox lo convierten en una herramienta adecuada para entornos educativos y escenarios prácticos de aprendizaje. El objetivo principal de esta práctica es implementar un firewall perimetral en VirtualBox, configurando tres zonas de red con roles claramente definidos:

- Zona Verde (LAN): red interna de usuarios, considerada de confianza.
- Zona Roja (WAN): salida hacia Internet, considerada no confiable.
- Zona Naranja (DMZ): espacio intermedio destinado a servidores que requieren acceso público controlado.

Esta segmentación permite simular un entorno real utilizado en organizaciones para proteger servicios críticos, como aplicaciones web y bases de datos. Asimismo, la práctica permite al estudiante comprender la importancia del diseño de red, la traducción de direcciones (NAT), el control del tráfico mediante reglas de firewall y la implementación de un proxy con políticas de autenticación, fortaleciendo sus competencias en seguridad informática bajo plataformas GNU/Linux.

2 DESARROLLO DE LAS TEMATICAS

2.1 INSTALACIÓN Y CONFIGURACIÓN DE ENDIAN FIREWALL

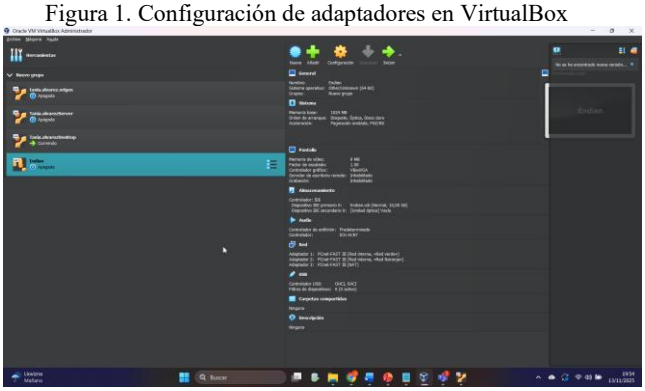
La práctica inició con la creación de una máquina virtual en Oracle VirtualBox destinada a la instalación de Endian Firewall Community Edition. Durante el proceso se particionó el disco, se generaron los sistemas de archivos y se instalaron los paquetes necesarios para el funcionamiento del firewall. Al finalizar la instalación, se asignó la dirección IP inicial a la interfaz verde (192.168.10.1/24), lo que permitió establecer comunicación con la red interna y habilitar el acceso a la consola web de administración. En VirtualBox se configuraron tres adaptadores de red con roles específicos:

- Zona verde (LAN): red interna con dirección 192.168.10.1/24, utilizada como gateway para los clientes.
- Zona naranja (DMZ): red interna con dirección 192.168.20.1/24, destinada a los servidores accesibles desde el exterior.

- Zona roja (WAN): adaptador en modo NAT, con dirección asignada por DHCP, encargado de la salida a Internet.

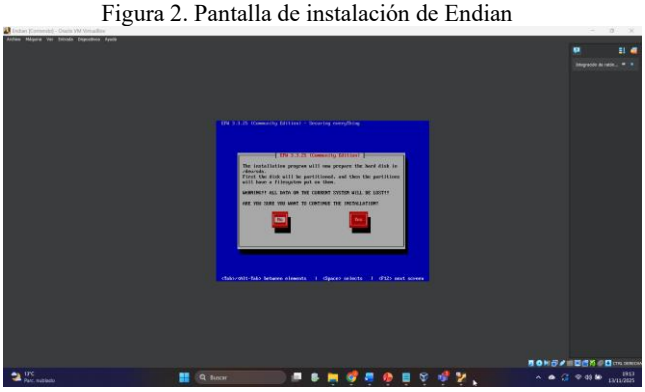
Con esta configuración se logró simular un entorno segmentado, donde cada zona cumple un rol de seguridad definido y facilita la aplicación de políticas diferenciadas. Adicionalmente, esta estructura permitió comprobar el funcionamiento del firewall bajo un entorno controlado y reproducible, garantizando la correcta separación del tráfico entre las distintas redes.

Figura 1. Configuración de adaptadores en VirtualBox



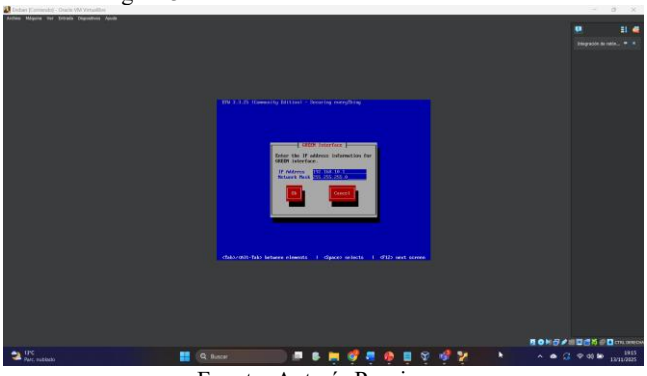
Fuente: Autoría Propia

Figura 2. Pantalla de instalación de Endian



Fuente: Autoría Propia

Figura 3. Pantalla de instalación de Endian



Fuente: Autoría Propia

La asignación precisa de direcciones IP y la configuración de los adaptadores fueron fundamentales para asegurar la comunicación entre zonas. Finalmente, esta base permitió continuar con la creación de reglas, pruebas de conectividad y validación del comportamiento esperado del sistema.

2.2 TEMÁTICA 1 – CONFIGURACIÓN Y VALIDACIÓN DE GNU/LINUX ENDIAN EN VIRTUALBOX

2.2.1 ENDIAN FIREWALL (MÁQUINA PRINCIPAL)

Configuración general: La máquina principal de Endian Firewall fue configurada con tres adaptadores de red en VirtualBox, cada uno asignado a una zona de seguridad específica:

- Verde (LAN): 192.168.10.1/24
- Naranja (DMZ): 192.168.20.1/24
- Roja (WAN): NAT/DHCP

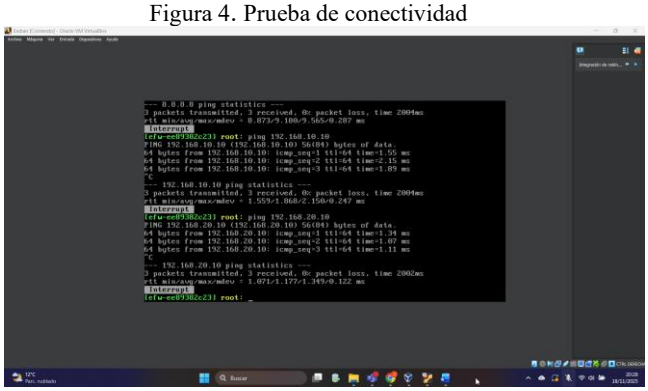
Verificación de interfaces y rutas: Se utilizó el comando ip a para comprobar que las interfaces br0 y br1 tenían asignadas correctamente sus direcciones IP, y que la interfaz eth2 recibió una IP dinámica desde el servidor DHCP de la WAN. Mediante ip route se confirmó la presencia de las rutas hacia las redes internas y la ruta por defecto apuntando al gateway de la zona roja.

Pruebas de conectividad:

- ping 8.8.8.8 → salida a Internet.
- ping 192.168.10.10 → comunicación con estación verde.
- ping 192.168.20.10 → comunicación con servidor en DMZ.

Resultado: El firewall gestionó correctamente el enrutamiento entre las tres zonas y hacia Internet, confirmando el funcionamiento adecuado de la segmentación de red y de la configuración aplicada.

Figura 4. Prueba de conectividad



Fuente: Autoría Propia

2.2.2 ESTACIÓN DE TRABAJO EN ZONA VERDE (DESKTOP GNU/LINUX)

- Configuración:
  IP estática: 192.168.10.10/24
  Gateway: 192.168.10.1
  DNS: 8.8.8.8 y 1.1.1.1

Configuración realizada en /etc/netplan/50-cloud-init.yaml.

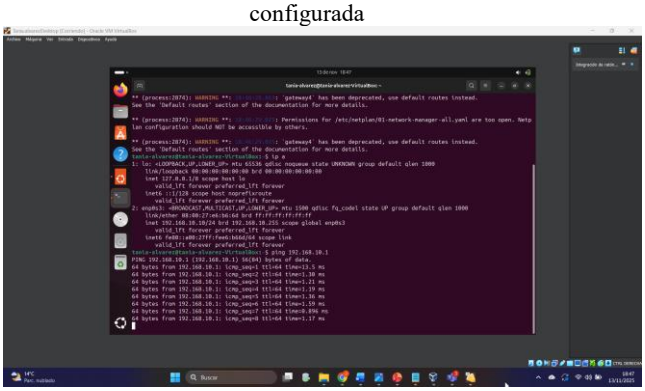
- Comprobaciones realizadas:
  Con ip a se verificó que la interfaz enp… tenía la IP correcta.
  Con ip route se confirmó la ruta por defecto hacia el gateway verde.
  Prueba de conectividad:
  ping 192.168.10.1 → comunicación con el firewall.
  Acceso a la consola web:
  en https://192.168.10.1:10443.
  Se aceptó el certificado auto firmado y se accedió al asistente de configuración.

Resultado: La estación verde se comunica con el firewall y permite administrar Endian desde la consola web.

Figura 5. Configuración de la interfaz zona verde

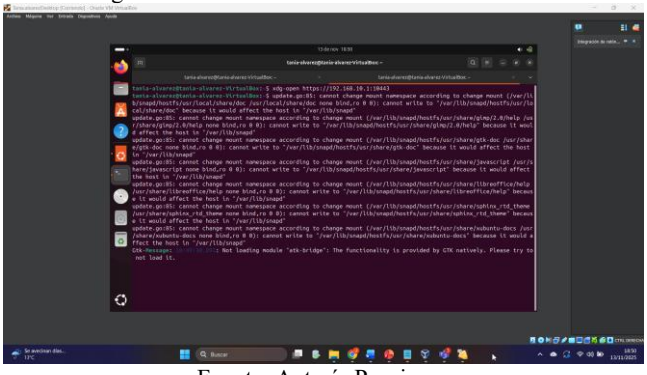
Fuente: Autoría Propia

Figura 6. Verificación de estación verde está correctamente configurada



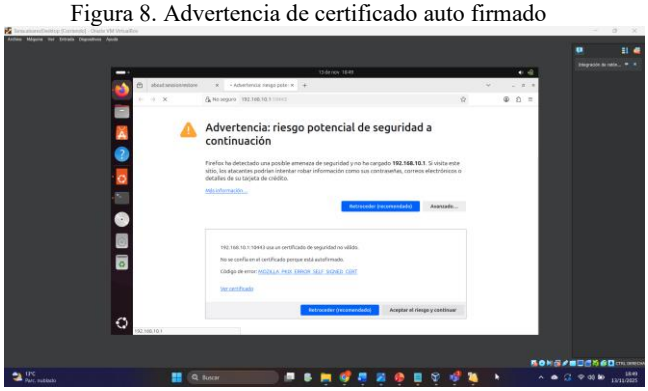
Fuente: Autoría Propia

Figura 7. Acceso a la consola web de Endian



Fuente: Autoría Propia

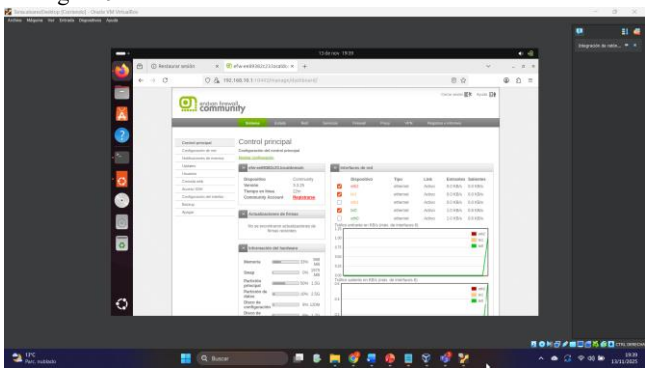
Figura 8. Advertencia de certificado auto firmado



Fuente: Autoría Propia

Además, una vez configurada la interfaz verde, se accedió al Dashboard web de Endian mediante la dirección https://192.168.10.1:10443. Desde esta consola gráfica fue posible visualizar el estado del sistema, administrar las interfaces, revisar los registros y aplicar las políticas de seguridad de forma centralizada. Este acceso facilitó la gestión del firewall y la validación continua de la configuración realizada.

Figura 9. Acceso a la consola web de Endian dashboard



Fuente: Autoría Propia

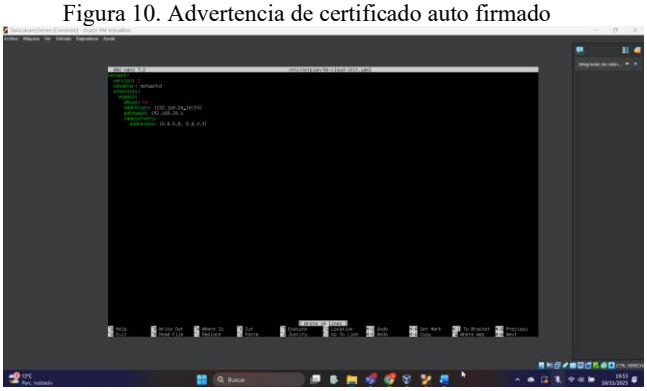
2.2.3 SERVIDOR EN ZONA NARANJA (DMZ)

- Configuración:
  IP estática: 192.168.20.10/24
  Gateway: 192.168.20.1
  DNS: 8.8.8.8 y 8.8.4.4
- Comprobaciones realizadas:
  Con ip a se verificó la IP asignada a la interfaz.
  Con ip route se confirmó la ruta por defecto hacia el gateway naranja.
  Prueba de conectividad:
  ping 192.168.20.1 → comunicación con el firewall.
  ping 8.8.8.8 → salida a Internet a través del firewall.
  Validación de servicio web:
  curl -I http://localhost → respuesta HTTP 200 OK.
  systemctl status apache2 → servicio Apache activo.

Resultado: La máquina ubicada en la zona naranja quedó correctamente configurada y logra comunicarse tanto con el firewall como con Internet. Además, mantiene operativos sus

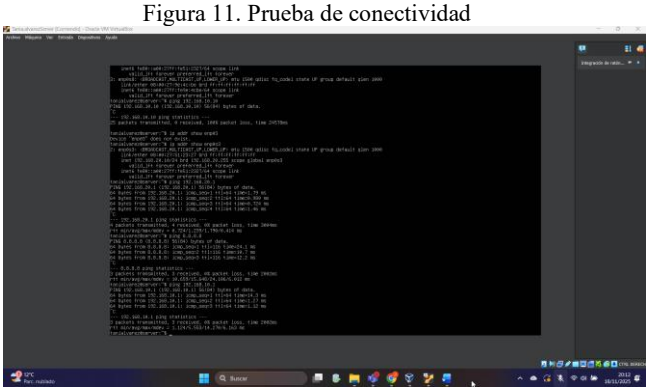
servicios internos, lo que confirma que la DMZ funciona de manera estable y aislada según lo previsto.

Figura 10. Advertencia de certificado auto firmado



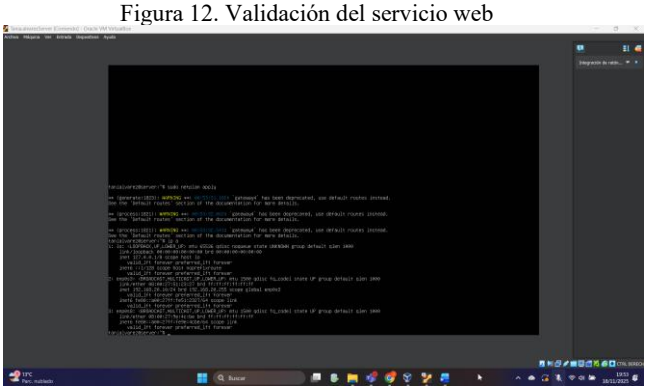
Fuente: Autoría Propia

Figura 11. Prueba de conectividad



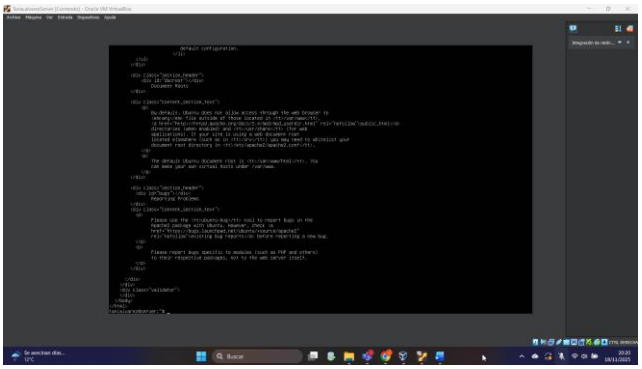
Fuente: Autoría Propia

Figura 12. Validación del servicio web



Fuente: Autoría Propia

Figura 13. Evidencia que el servidor DMZ ofrece servicios accesibles



Fuente: Autoría Propia

2.3 TEMÁTICA 2 – CONFIGURACIÓN NAT

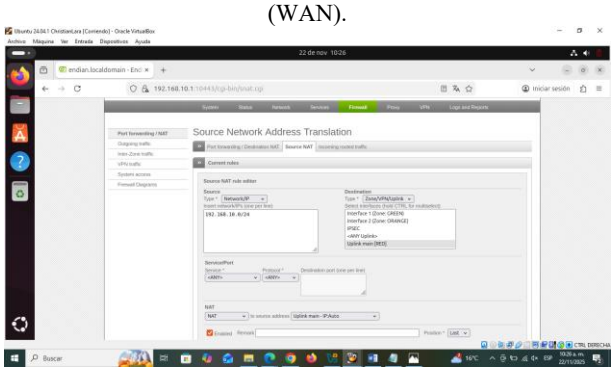
En esta sección se describe el proceso de configuración del servicio Network Address Translation (NAT) en Endian Firewall, con el fin de permitir la comunicación segura desde las zonas internas (verde y Naranja) hacia la zona externa (roja), correspondiente a Internet simulada.

2.3.1 CONFIGURACIÓN DE NAT PARA (ZONA VERDE (LAN INTERNA) - ZONA ROJA (WAN))

Para permitir que los equipos de la red LAN (zona verde) establezcan comunicación hacia la red simulada de Internet (zona roja). Entonces, se ingresó al menú Firewall Port Forwarding / NAT y en la sección Source NAT se creó una nueva regla y la regla se configuró con los siguientes parámetros:

- Source: 192.168.10.0/24
- Destination: Uplink main RED
- Service: ANY
- NAT Type: Uplink main – IP: Auto

Figura 14. Configuración de NAT para habilitar la comunicación de zona verde (LAN interna) hacia la zona roja (WAN).

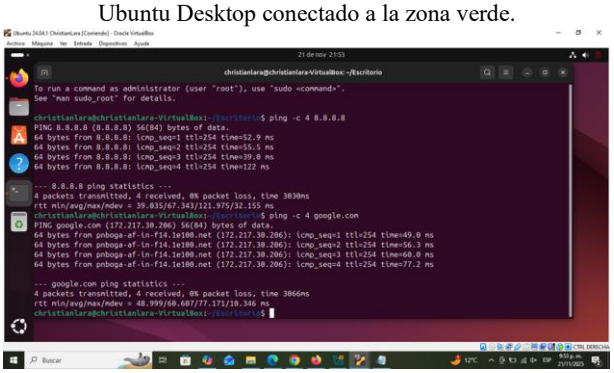


Fuente: Autoría propia

Al Seleccionar NAT to Source Address - uplink main-ip:auto, lo cual indica que Endian usará automáticamente su IP de la zona RED para enmascarar a los dispositivos internos. Seguidamente, se habilitó la regla y se aplicaron los cambios. Como resultado, los equipos de la LAN pudieron comunicarse

correctamente con la red WAN simulada, confirmando el funcionamiento del NAT para tráfico saliente.

Figura 15. Prueba de conectividad exitosa desde el equipo Ubuntu Desktop conectado a la zona verde.



Fuente: Autoría propia

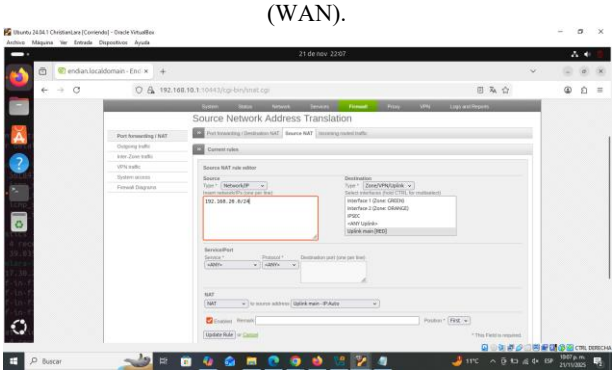
Ambas pruebas fueron exitosas, lo que confirma que la LAN interna tiene acceso a Internet, que las reglas de salida configuradas en el firewall están funcionando correctamente y que el proceso de NAT está enmascarando las direcciones IP privadas de la red verde, utilizando automáticamente la IP de la zona roja como dirección de salida.

2.3.2 CONFIGURACIÓN DE NAT PARA (ZONA VERDE (LAN INTERNA) - ZONA ROJA (WAN))

Para permitir la comunicación de los servidores ubicados en la zona DMZ (zona naranja) hacia la red WAN/Internet, se creó una regla de NAT adicional con las siguientes características:

- Source: 192.168.20.0/24
- Destination: Uplink main RED
- Service: ANY
- NAT Type: Uplink main – IP: Auto

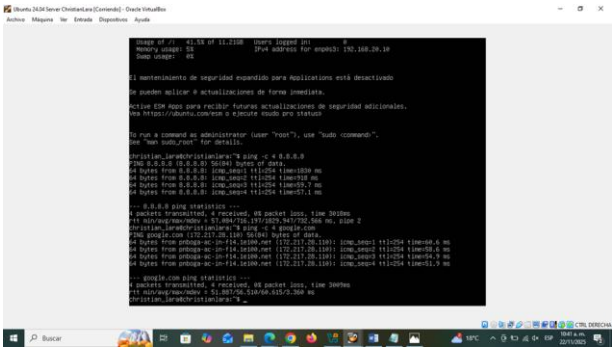
Figura 16. Configuración de NAT para habilitar la comunicación de la zona naranja (DMZ) hacia la zona roja (WAN).



Fuente: Autoría propia

Desde el equipo Ubuntu Server (zona naranja) se realizaron las siguientes pruebas

Figura 17. Prueba de conectividad exitosa desde el equipo Ubuntu Server conectado a la zona naranja



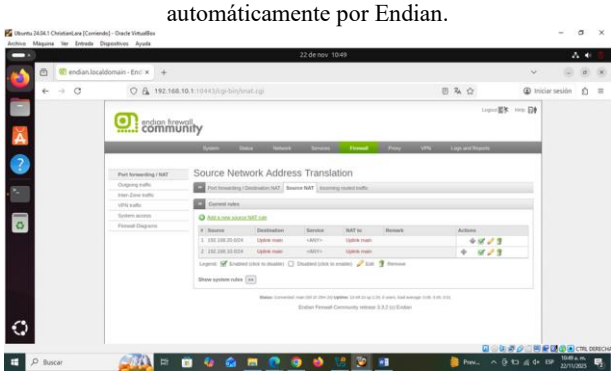
Fuente: Autoría propia

Los resultados fueron exitosos, demostrando que la zona naranja puede comunicarse correctamente con Internet, que la regla NAT está traduciendo adecuadamente las direcciones provenientes de la DMZ y que el firewall permite el tráfico desde la zona naranja hacia la zona roja sin restricciones para los servicios autorizados.

2.3.3 VERIFICACIÓN DE REGLAS NAT EN ENDIAN

En el menú Firewall - Port forwarding / NAT, se verificó la existencia y correcto funcionamiento de las reglas NAT generadas para permitir la salida de tráfico desde las zonas verde y naranja hacia la WAN. Las reglas están activadas y aplicadas.

Figura 18. Verificación de las reglas NAT generadas automáticamente por Endian.



Fuente: Autoría propia

Esto confirma que el proceso de NAT funciona correctamente en ambas zonas.

2.4 TEMÁTICA 3 – PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

2.4.1 PERMITIR LOS SERVICIOS HTTP (PUERTO 80) Y FTP (PUERTO 21) DESDE EL SERVIDOR WEB BAJO UBUNTU SERVER.

Se definieron tres segmentos de red:

- LAN (192.168.10.0/24): Red interna de usuarios.
- DMZ (192.168.20.0/24): Red desmilitarizada con servicios públicos.

- SERVIDOR (192.168.20.10): Host en DMZ con servicios HTTP y FTP.

Se desarrollaron reglas de firewall aplicando los siguientes principios:

- Principio de menor privilegio: Solo se permite el tráfico necesario.
- Segmentación lógica: Separación entre redes de usuarios y servicios.
- Denegación por defecto: Todo tráfico no explícitamente permitido es bloqueado.

Figura 19. Creación de regla

Fuente: Autoría Propia

Ir a:

Firewall → Port Forwarding → New rule

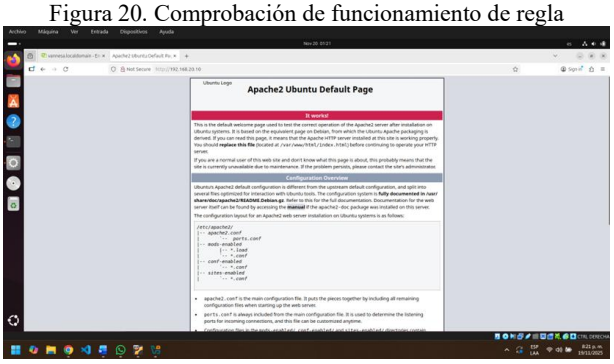
Regla 1: Permitir HTTP (80)

- Source: DMZ
- Service: HTTP (80)
- Destination: DMZ → 192.168.20.10
- Action: ACCEPT

Regla 2: Permitir FTP (21)

- Source: DMZ
- Service: FTP (21)
- Destination: DMZ → 192.168.20.10
- Action: ACCEPT
- Guardar y aplicar.

Figura 20. Comprobación de funcionamiento de regla



Fuente: Autoría Propia

En la consola para probar que quedar bien se digita un curl http://localhost tanto en el desktop como en el server lo redigira a la página de apache comprobando que si quedaron habilitados los puertos 80 y 21

2.4.2 DENEGAR EL PROTOCOLO ICMP (PUERTO 8 Y PUERTO 30)

Ahora para crear las reglas de bloqueo realice los siguientes pasos.

Firewall → Outgoing / Rule list (o Packets filtering)

Crear regla:

- Nombre: Block_ICMP_echo_request
- From: LAN,DMZ (o 192.168.10.0/24, 192.168.20.0/24)
- To: any (o dentro de las redes)
- Protocol: ICMP
- ICMP Type: echo-request (8)
- Action: DROP
- Guardar.

Crear otra regla:

- Nombre: Block_ICMP_echo_reply
- Same as above, ICMP Type: echo-reply (0)
- Action: DROP
- Guardar y aplicar.

Figura 21. Creación de regla Bloqueo

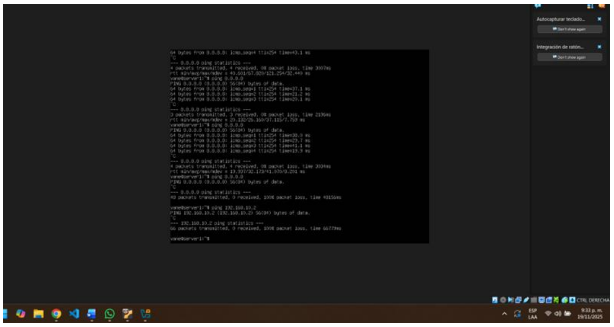
Fuente: Autoría Propia

2.4.2 PROBAR A TRAVÉS DE UNA CONSOLA O TERMINAL LA NO RESPUESTA DEL COMANDO PING HACIA UNA IP DE LA RED

Para pobrar que el bloqueo quedo efectivo se realiza el ping en el server a la IP 192.168.20.1 y muestra Destination Host Unreachable

Request timed out

Figura 22. Prueba de negación en server

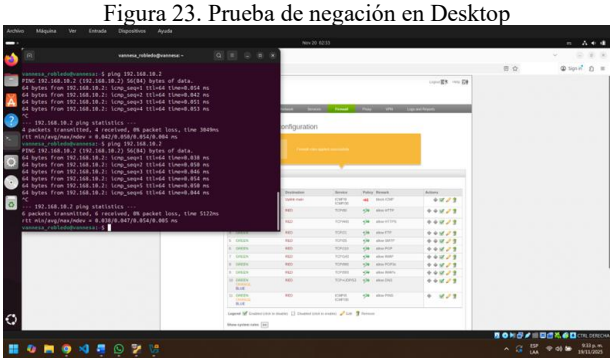


Fuente: Autoría Propia

Para pobrar que el bloqueo quedo efectivo se realiza el ping en el desktop a la IP 192.168.20.1 y muestra Destination Host Unreachable

Request timed out.

Figura 23. Prueba de negación en Desktop



Fuente: Autoría Propia

2.5 TEMÁTICA 4 - REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO.

En esta actividad se realizará la configuración de reglas de acceso en Endian Firewall con el fin de controlar el tráfico entre las diferentes zonas de la red: Verde (LAN), Naranja (DMZ) y Roja (WAN). El objetivo principal es permitir únicamente los servicios necesarios como HTTP y FTP garantizando una comunicación segura y ordenada entre estas áreas.

A través de la creación, verificación y prueba de estas reglas, se comprenderá cómo Endian gestiona el filtrado interzonal y cómo estas políticas fortalecen la seguridad perimetral dentro de una infraestructura de red.

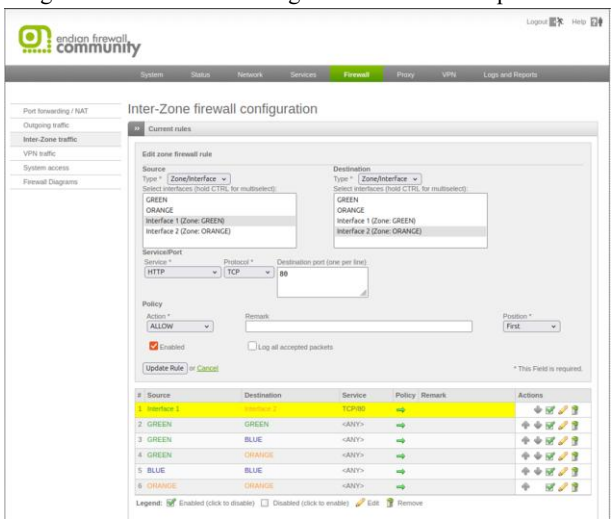
2.5.1 CONFIGURACIÓN DE COMUNICACIÓN EN HTTP DE LA ZONA VERDE A LA ZONA NARANJA

Para configurar el firewall para que el tráfico proveniente de la zona Verde pueda llegar a la zona Naranja, específicamente habilitando los puertos correspondientes de HTTP, realice los siguientes pasos:

Firewall - Inter-Zone traffic / Rule list

- Type: Zone/Interface
- Source: Green
- To: Orange
- Service: HTTP
- Protocol: TCP
- Port: 80
- Policy/Action: Allow
- Agregar la regla.

Figura 24. Creación de la regla Inter-Zone traffic por HTTP



Fuente: Autoría Propia

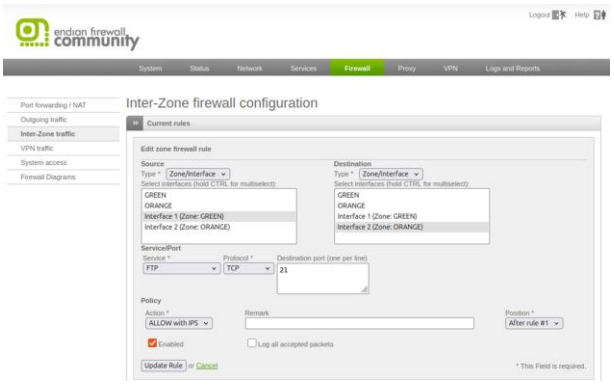
2.5.2 CONFIGURACIÓN DE COMUNICACIÓN EN FTP DE LA ZONA VERDE A LA ZONA NARANJA

Una vez creada esta regla, se procede con la creación de la siguiente que es la comunicación de la zona Verde con la zona Naranja a través del servicio FTP. Se realiza con los siguientes pasos:

Firewall→ Inter-Zone traffic / Rule list

- Type: Zone/Interface
- Source: Green
- To: Orange
- Service: FTP
- Protocol: TCP
- Port: 21
- Policy/Action: Allow
- Agregar la regla.

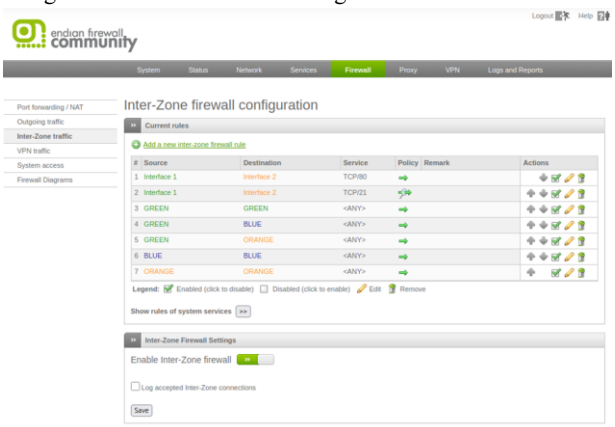
Figura 25. Creación de la regla Inter-Zone traffic por FTP



Fuente: Autoría Propia

Ahora se comprueba que ambas reglas hayan sido creadas correctamente y que estén listadas en la configuración del tráfico:

Figura 26. Revisión de ambas reglas creadas exitosamente.

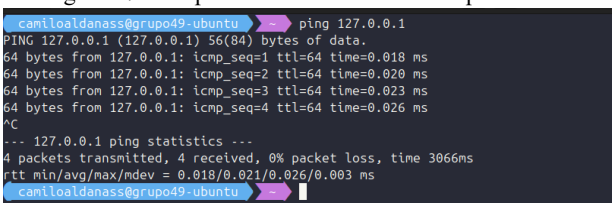


Fuente: Autoría Propia

2.5.3 COMPROBACIÓN DE COMUNICACIÓN ENTRE ZONAS POR HTTP A TRAVÉS DE UN PING

Ahora se confirma que haya comunicación y que la transferencia de datos a través del servicio HTTP sea posible entre la zona Verde con la zona Naranja a través de un ping a la IP 127.0.0.1:

Figura 27. Comprobación de comunicación por HTTP.



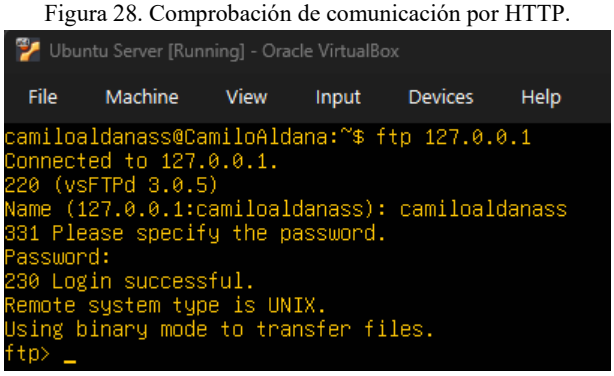
Fuente: Autoría Propia

Podemos comprobar que la comunicación por HTTP existe, ya que el ping fue exitoso y hubo transferencia de datos entre zonas.

2.5.3 COMPROBACIÓN DE COMUNICACIÓN ENTRE ZONAS POR FTP

Para la comprobación de la comunicación a través del servicio FTP, se utiliza un equipo diferente y se conecta a través del comando ftp en la consola junto con la IP destino (ftp 127.0.0.1). Una vez ingresado el comando mencionado, si existe la comunicación se solicitará el usuario y contraseña del administrador creado en Endian Firewall. Si no hay comunicación, se producirá un error mencionando que la red no se encuentra disponible.

Figura 28. Comprobación de comunicación por HTTP.



Fuente: Autoría Propia

Podemos confirmar que la comunicación fue exitosa una vez ingresado el usuario y contraseña correcto.

2.6 TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

2.6.1 CONFIGURACIÓN INICIAL DE RED - ENDIAN FIREWALL

Figura 29. Configuración inicial de red - endian firewall

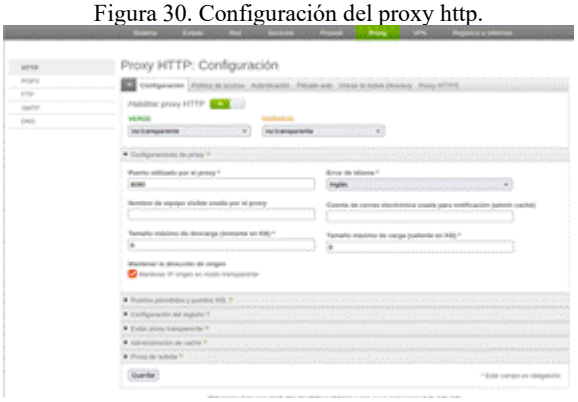
Fuente: Autoría Propia

La implementación del proxy HTTP requiere una configuración previa de las interfaces de red del firewall Endian. Como se observa en la Figura [X], durante el asistente de configuración se establecieron tres zonas de seguridad claramente diferenciadas: GREEN (red interna o LAN), ORANGE (zona desmilitarizada o DMZ) y RED (interfaz hacia Internet).

Para la zona GREEN se configuró la dirección IP 192.168.10.10 con máscara de red /24 (255.255.255.0), activando el servidor DHCP para asignar automáticamente direcciones IP a los clientes de la red interna. De manera similar, la zona ORANGE se configuró con la dirección IP 192.168.20.10 y máscara /24, también con servicio DHCP habilitado para los servidores ubicados en la DMZ.

2.6.2 CONFIGURACIÓN DEL PROXY HTTP NO TRANSPARENTE

Figura 30. Configuración del proxy http.



Fuente: Autoría Propia

El Proxy HTTP es un servidor intermediario que controla el acceso a Internet actuando como punto de filtrado entre los usuarios de la red local y los sitios web externos. A diferencia de otros servicios de filtrado que operan a nivel de red, el proxy HTTP trabaja en la capa de aplicación, permitiendo un control granular sobre el contenido web accedido por los usuarios.

Para este laboratorio se configuró el proxy en modo no transparente, lo que implica que cada cliente debe configurar manualmente su navegador para utilizar el servicio. Esta decisión de diseño, aunque requiere configuración adicional en cada equipo, ofrece ventajas significativas en términos de autenticación y control de acceso por usuario.

El proxy se habilitó tanto para la zona GREEN como para la zona ORANGE, utilizando el puerto 8080 como punto de escucha estándar para las conexiones HTTP.

2.6.3 CONFIGURACIÓN DE AUTENTICACIÓN DE USUARIOS

Se realiza la configuración de autenticación de usuarios en la ventana de proxy y se hace la implementación de esta.

Figura 31. Autenticación de usuarios

Fuente: Autoría Propia

La autenticación de usuarios constituye un componente esencial en la implementación de políticas de acceso diferenciadas. Para este laboratorio se seleccionó el método de autenticación local NCSA (National Center for Supercomputing Applications), que permite crear y gestionar credenciales directamente en el firewall sin necesidad de infraestructura externa como servidores LDAP o Active Directory. Se configuró un dominio de autenticación denominado "Proxy Server", nombre que aparece en la ventana de solicitud de credenciales cuando los usuarios intentan navegar. Los parámetros de concurrencia se establecieron para controlar el número de procesos hijos de autenticación y limitar el número de direcciones IP distintas por usuario, evitando así el uso compartido no autorizado de credenciales entre múltiples dispositivos. Mediante las herramientas de administración integradas, se creó un grupo denominado "Listanegra" al cual se asoció un usuario de prueba.

2.6.4 CREACIÓN DE PERFIL DE FILTRADO WEB (LISTA NEGRA)

Figura 32. Evidencia que el servidor DMZ ofrece servicios accesibles

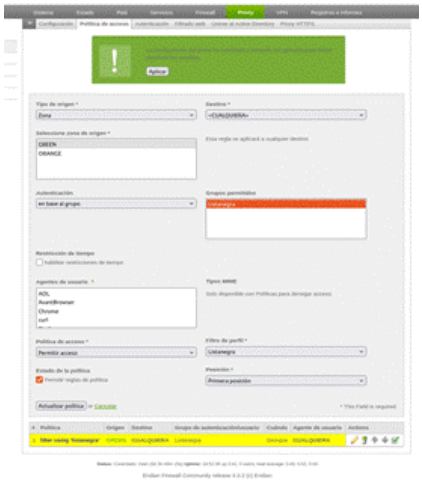
Fuente: Autoría Propia

El sistema de filtrado web de Endian permite crear perfiles personalizados que definen qué sitios están permitidos o bloqueados para grupos específicos de usuarios, se creó un perfil denominado "Listanegra" con el análisis antivirus activado para proporcionar una capa adicional de seguridad. En la sección de listas negras y blancas personalizadas, se

agregaron tres dominios específicos al campo "Bloquear los siguientes sitios": www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. El sistema de filtrado opera mediante comparación de dominios completos, por lo que bloquea tanto el dominio principal como todos sus subdominios asociados. Es importante destacar que el campo "Permitir los siguientes sitios" se dejó vacío, estableciendo así una política por defecto donde todos los sitios están permitidos excepto aquellos explícitamente bloqueados en la lista negra.

2.6.5 CONFIGURACIÓN DE POLÍTICA DE ACCESO

Figura 33. Evidencia que el servidor DMZ ofrece servicios accesibles



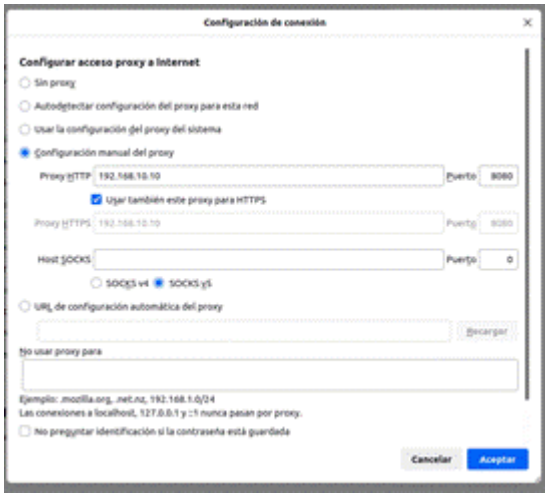
Fuente: Autoría Propia

Las políticas de acceso son el mecanismo mediante el cual se vinculan los usuarios o grupos con los perfiles de filtrado previamente configurados. En la interfaz de configuración de políticas, se establecieron los siguientes parámetros: tipo de origen "Zona" con las redes GREEN y ORANGE seleccionadas, destino configurado como "CUALQUIERA" para aplicar la política a todos los sitios web, y método de autenticación "en base al grupo" vinculado al grupo "Listanegra" creado anteriormente.

Los agentes de usuario especificados (AOL, AvantBrowser, Chrome, curl) determinan desde qué navegadores web se aplicará la política, permitiendo un control adicional sobre los métodos de acceso. La política de acceso se configuró como "Permitir acceso" con el filtro de perfil "Listanegra" aplicado, lo que significa que el grupo tiene permiso para navegar, pero con las restricciones de la lista negra activas. La posición de la política se estableció en "Primera posición" para asegurar que sea evaluada antes que cualquier otra regla, y se activó la casilla "Permitir reglas de política" para hacerla efectiva inmediatamente.

2.6.6 CONFIGURACIÓN DEL NAVEGADOR EN EL CLIENTE

Figura 34. Evidencia que el servidor DMZ ofrece servicios accesibles



Fuente: Autoría Propia

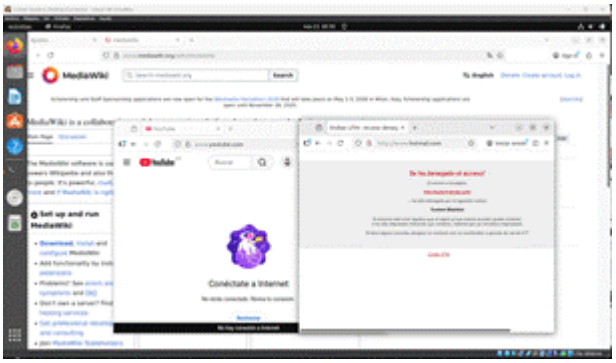
Para que el proxy HTTP no transparente funcione correctamente, es indispensable configurar el navegador web en cada equipo cliente de la red. Esta fue precisamente la razón por la cual inicialmente no se observaba el bloqueo de sitios: el navegador estaba conectándose directamente a Internet, evitando completamente el proxy y sus reglas de filtrado.

En el navegador Firefox del equipo cliente ubicado en la zona GREEN, se accedió a la configuración de red y se seleccionó "Configuración manual del proxy". Se ingresó la dirección IP del firewall Endian (192.168.10.10) en el campo "Proxy HTTP" y el puerto 8080 en el campo correspondiente. Crucialmente, se activó la opción "Usar también este proxy para HTTPS" para garantizar que tanto las conexiones HTTP como HTTPS pasen por el proxy y sean filtradas según las políticas establecidas.

En el campo "No usar proxy para" se eliminaron todas las excepciones predeterminadas, asegurando que absolutamente todo el tráfico web sea dirigido a través del servidor proxy.

2.6.7 VERIFICACIÓN DEL FUNCIONAMIENTO DEL PROXY

Figura 35. Evidencia que el servidor DMZ ofrece servicios accesibles



Fuente: Autoría Propia

Las pruebas de funcionamiento confirmaron la correcta implementación de todas las capas de la solución de proxy

HTTP con autenticación y filtrado. Como se evidencia en la Figura [X], se realizaron tres escenarios de prueba desde el equipo cliente en la zona GREEN.

En el primer escenario, al intentar acceder a www.youtube.com, el navegador mostró el mensaje "Conéctate a Internet - No estás conectado", indicando que el proxy está interceptando la solicitud y bloqueando efectivamente el acceso al sitio incluido en la lista negra. De manera similar, al intentar acceder a www.hotmail.com, apareció un mensaje explícito del firewall Endian indicando "Se ha denegado el acceso" con la justificación "Custom Blacklist", proporcionando retroalimentación clara al usuario sobre la razón del bloqueo.

El tercer escenario de prueba consistió en acceder a www.mediawiki.org, un sitio que no se encuentra en la lista negra. Este sitio cargó completamente sin restricciones, demostrando que el proxy permite el acceso normal a sitios no restringidos mientras mantiene el bloqueo selectivo de aquellos explícitamente prohibidos. Esta prueba final valida que la autenticación por grupo, la vinculación del perfil "Listanegra" con la política de acceso, y la configuración del navegador cliente están operando correctamente en conjunto, cumpliendo así con todos los objetivos planteados para la implementación del proxy HTTP no transparente con políticas de autenticación.

3 CONCLUSIONES

3.1 TEMÁTICA 1

La instalación y configuración de Endian Firewall en VirtualBox permitió segmentar la red en tres zonas (LAN, WAN y DMZ). Las comprobaciones realizadas en cada máquina confirmaron la correcta asignación de direcciones IP, la existencia de rutas adecuadas y la comunicación entre los segmentos. Además, se validó el acceso a la consola web y el funcionamiento de un servidor en la DMZ, demostrando la eficacia de la arquitectura implementada.

3.2 TEMATICA 2

La implementación de la Temática 2 permitió comprender de manera práctica el funcionamiento del NAT dentro de un entorno segmentado con Endian Firewall. A través de la configuración de las zonas GREEN, ORANGE y RED, fue posible validar cómo el firewall traduce las direcciones privadas de la LAN y la DMZ para permitir su salida a Internet de forma segura. Las pruebas realizadas —tanto de conectividad como de acceso a servicios— demostraron que las reglas de NAT se aplican correctamente, garantizando comunicación controlada entre las redes internas y externas. Esta práctica evidenció la importancia del NAT como mecanismo esencial para proteger las redes privadas y administrar el tráfico en arquitecturas orientadas a la seguridad perimetral.

3.3 TEMÁTICA 3

El desarrollo de reglas de firewall en GNU/Linux permite implementar políticas de seguridad claras y efectivas. La segmentación de red, combinada con el filtrado de paquetes, es una técnica esencial para proteger servicios críticos y limitar la exposición de sistemas internos. Esta experiencia refuerza la importancia del control de acceso en la administración de sistemas operativos abiertos.

3.4 TEMÁTICA 4

La configuración de reglas de acceso en Endian Firewall permitió controlar de manera segura la comunicación entre la LAN, la DMZ y la WAN. Al habilitar únicamente los servicios necesarios (HTTP y FTP), se garantizó un flujo de tráfico autorizado y una correcta segmentación de la red.
Este ejercicio mostró la importancia de aplicar políticas de filtrado adecuadas para proteger los servicios críticos y confirmó que Endian Firewall es una herramienta efectiva para fortalecer la seguridad perimetral en una infraestructura de red.

3.5 TEMATICA 5

La implementación del proxy HTTP no transparente con autenticación NCSA en Endian Firewall cumplió satisfactoriamente los objetivos planteados, permitiendo controlar el acceso a Internet mediante políticas diferenciadas por grupo de usuarios.

El sistema de filtrado mediante listas negras bloqueó efectivamente los sitios restringidos mientras mantuvo acceso a recursos permitidos, validando la precisión del mecanismo implementado.

4 REFERENCIAS

[1] Endian Firewall Community. (2025). Documentation. Disponible en: https://www.endian.com/community/

[2] UNAD. (2025). Guía de laboratorio de seguridad en GNU/Linux. Bogotá: Escuela de Ciencias Básicas, Tecnología e Ingeniería.

[3] Rash, M. (2007). Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort. No Starch Press.

[4] Srisuresh, P., & Egevang, K. (2001). RFC 3022: Traditional IP network address translator. Network Working Group.

[5] Gomes, J. R. D. F. (2023). Segurança de redes de computadores: um estudo sobre o Endian Firewall. https://repositorio.pucgoias.edu.br/jspui/handle/123456789/6739

[6] Hoyos Pantoja, E. A., Hoyos Pantoja, C. A., Montealegre Aquite, J. A., & Gomez Aguirre, C. R. Endian firewall como solución de seguridad en redes en un entorno virtualizado. https://repository.unad.edu.co/handle/10596/68800

[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=b881bf7 2-20a7-343c-94a8-f12e88b41952

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

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

[10] B. Hubert, "The Definitive Guide to Squid: The Web Proxy Cache", O'Reilly Media, 1st ed., pp. 23–57, 2005