IMPLEMENTACIÓN ACADÉMICA DE UN FIREWALL PERIMETRAL BASADO EN GNU/LINUX ENDIAN

Jose Andres Orjuela Orjuela
jaorjuelao@unadvirtual.edu.co
Luz Ayda Morante Pinzón
lamorantep@unadvirtual.edu.co
Oscar Yesid Gordillo Ubaque
oygordillou@unadvirtual.edu.co
Yeiler Augusto Cortes Osorio
yacorteso@unadvirtual.edu.co

RESUMEN:*El presente artículo describe la implementación de una arquitectura perimetral de seguridad utilizando la distribución GNU/Linux Endian Firewall dentro de un entorno virtualizado con VirtualBox. Se desarrollaron cinco temáticas orientadas a la configuración de zonas de red (LAN, WAN y DMZ), reglas NAT, habilitación de servicios en la DMZ, políticas de control de acceso entre zonas y la implementación de un proxy HTTP con autenticación. Los resultados evidencian un entorno seguro y funcional que replica escenarios empresariales reales, permitiendo el acceso controlado a servicios web, FTP y políticas de filtrado de contenido en Internet.*

PALABRAS CLAVE: Endian Firewall, DMZ, NAT, Proxy, Network Security, VirtualBox, LAN, WAN.

1 INTRODUCCIÓN

La creciente necesidad de asegurar los entornos empresariales frente a amenazas externas e internas exige la implementación de soluciones perimetrales robustas. En este contexto, GNU/Linux Endian Firewall se presenta como una herramienta profesional que integra cortafuegos, NAT, proxy, zona desmilitarizada (DMZ), antivirus y servicios avanzados de red. Este trabajo tuvo como objetivo diseñar, implementar y validar un entorno de seguridad perimetral mediante cinco temáticas orientadas a simular un ecosistema corporativo que incluye zonas LAN, DMZ y WAN, acceso controlado a servicios y políticas de navegación segura. Cada temática fue implementada en un ambiente virtualizado basado en VirtualBox utilizando múltiples tarjetas de red y reglas específicas para la comunicación inter-zona.

El proyecto desarrollado busca poner en práctica los principios fundamentales de segmentación de red, filtrado de tráfico, traducción de direcciones (NAT), control de servicios y restricciones basadas en protocolos. Todo ello se lleva a cabo mediante pruebas funcionales, configuraciones técnicas y validaciones que demuestran el funcionamiento real del firewall.

Este artículo IEEE presenta de manera estructurada el proceso de instalación, configuración, validación y análisis de cada temática asignada, enfatizando el valor pedagógico de la virtualización y el aprendizaje práctico para el fortalecimiento de competencias en ciberseguridad, redes y administración de sistemas GNU/Linux.

2 JUSTIFICACIÓN

La implementación de un firewall perimetral constituye una necesidad esencial para cualquier organización que gestione datos, servicios en red o infraestructura de TI. La creciente frecuencia de ataques informáticos, el incremento de dispositivos conectados y la necesidad de segmentar redes internas justifican la adopción de arquitecturas seguras donde el flujo de tráfico sea controlado de forma efectiva.
El desarrollo de esta actividad en la UNAD permite al estudiante comprender no sólo los fundamentos teóricos de la seguridad perimetral, sino también interactuar con herramientas reales como Endian Firewall. Esta experiencia práctica fortalece competencias clave para el ejercicio profesional, tales como:

- Implementación de políticas de acceso.
- Administración de zonas perimetrales.
- Configuración de reglas NAT.
- Publicación y protección de servicios en la DMZ.
- Aplicación de restricciones por protocolo.
- Interpretación de logs y monitoreo del firewall.

La virtualización con VirtualBox refuerza el aprendizaje seguro, permitiendo al estudiante experimentar con tecnologías reales sin comprometer una infraestructura física.

3 MARCO TEÓRICO

La seguridad perimetral comprende el conjunto de tecnologías que protegen la infraestructura de red delimitando zonas con niveles de confianza diferenciados. Endian Firewall integra herramientas como IPTables, Squid y SquidGuard, soportando zonas Verde (LAN), Roja (WAN) y Naranja (DMZ).
Conceptos clave:

- DMZ: Zona de servidores expuestos parcialmente a Internet.

- NAT: Traducción de direcciones privadas a públicas para navegación externa.
- Proxy: Intermediario entre cliente e Internet que permite filtrado, autenticación y monitoreo.
- Reglas de firewall: Políticas que permiten o bloquean tráfico entre zonas basadas en puertos, protocolos y direcciones IP.
- VirtualBox: Plataforma de virtualización que permite emular topologías reales de red.

4 METODOLOGÍA

El desarrollo se realizó de forma individual en una máquina virtual utilizando VirtualBox, instalando Endian Firewall y configurando sus componentes.
Los pasos generales fueron:

1. Instalación del sistema Endian Firewall.
2. Configuración de interfaces para las zonas Verde, Roja y Naranja.
3. Configuración de NAT para navegación y publicación.
4. Creación de reglas de acceso inter-zona.
5. Habilitación de servicios HTTP/FTP en la DMZ.
6. Configuración de un proxy no transparente.
7. Validaciones finales con pruebas desde navegadores, ping y herramientas del firewall.

5 ACTIVIDAD GRUPAL

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

La seguridad es un componente fundamental durante la administración de redes, ya que esta permite controlar, filtrar y monitorear el tráfico de red que ingresa o sale en una organización.
Endian Firewall es una distribución de GNU/Linux la cual está diseñada con el fin de implementar soluciones de firewall, proxy, VPN y control de acceso de manera no centralizada.

En esta Temática se realiza la configuración de una instancia de Endian en virtualbox, también se realizará la configuración de sus tarjetas de red, segmentando la misma estableciendo las zonas principales del modelo de seguridad perimetral: WAN Rojo, LAN verde y DMZ naranja.

OBJETIVOS

El objetivo general es implementar una instancia funcional en de Endian en una máquina virtualBox, Segmentando la red adecuadamente.

Los objetivos específicos son:

- Configurar las tarjetas de red virtuales necesarias para la operación de Endian.
- Asignar cada interfaz física a una zona lógica (Roja, Verde y Naranja)
- Establecer la segmentación de red necesario para la realización de las demás temáticas del artículo.
- Validar el funcionamiento de cada zona mediante pruebas de red.
- Dejar la infraestructura establecida para poder continuar con el desarrollo de la actividad.

CONFIGURACIÓN DE LA RED

Para la instalación de Endian se establecieron tres interfaces desarrolladas de la siguiente manera:

- Interfaz: eth 0, Zona: Verde, redInterna - red_verde
- Interfaz: eth 1, Zona: Naranja, VirtualBox red: redInterna - Naranja_DMZ
- Interfaz: eth 2, Zona: Roja, VirtualBox red: DHCP

La Segmentación de red implementada para la actividad fue:

Zona Verde (LAN)

- Tipo de red: Red Interna
- propuesta: IP endian 192.168.10.5
- Destinado a clientes: 192.168.10.10

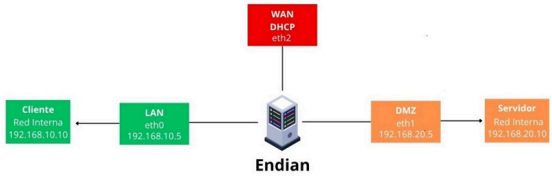
Zona Naranja (DMZ)

- Tipo de red: Red Interna
- propuesta: IP endian 192.168.20.5
- Destinado a servidores: 192.168.20.10

Zona Roja (WAN)

- Tipo de red: NAT
- Obtiene IP automáticamente
- proporciona la conexión a endian

Figura 1. Segmentación de redes



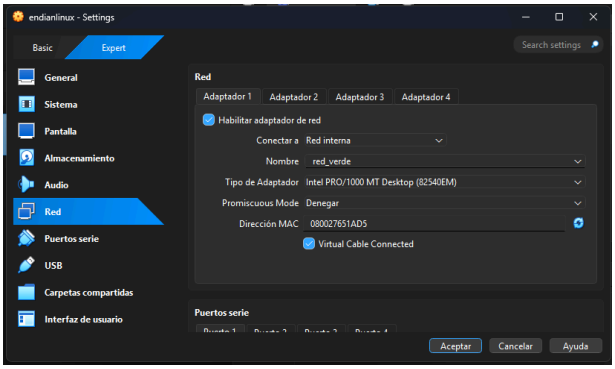
Fuente: Oscar Gordillo

Para la instalación de endian los pasos que se realizaron fueron:

Crear una máquina virtual a la cual se le asignó 2gb de memoria RAM, y 20 GB de disco duro. Posteriormente se asignaron 3 tarjetas de red en el adaptador 1, 2 y 3 configurándose de tal manera que el adaptador 1 conectará a

Red Interna, también se le asignó el nombre red_verde estableciendo que a esta tarjeta de red se conectaría la zona verde, de igual manera se hizo con el adaptador 2 a diferencia de que a este se le asignó el nombre de naranja_DMZ. Por último el adaptador 3 se configuró para conectar a NAT ya que este sería el asignado a la zona Roja.

Figura 2. Configuración adaptadores de red



Fuente: Oscar Gordillo

Después se procedió a:

- Cargar ISO de endian el la maquina virtual creada.
- Ejecutar la instalación básica de Endian, realizando la configuración básica como en otros Sistemas Operativos.
- Configurar las interfaces correspondientes a eth0, eth1 y eth1 en su respectiva zona.
- Definir las contraseñas de administración.
- Finalizar el proceso de instalación y acceder a la interfaz web de Endian para finalizar con la asignación de la zona naranja correspondiente a DMZ.

VALIDACIONES

Validación 1 - Estado del Firewall

Se valido el acceso web mediante el uso de la ip de la zona verde en este caso 192.168.10.5

Validación 2 - Conectividad de las zonas

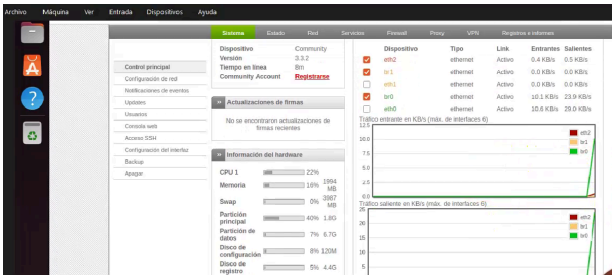
Se validó la conexión de la zona verde mediante la navegación desde endian hacia internet, de igual manera con la zona naranja se realizó mediante respuesta de ping hacia endian. Por último la zona de la zona roja se verificó mediante la ip asignada por el DHCP.

Validación 3 - Aislamiento entre zonas

Mediante esta validación se confirmó que la arquitectura de seguridad funciona correctamente teniendo en cuenta los siguientes puntos:

- LAN no accede directamente a DMZ sin algunas reglas.
- DMZ no accede a LAN.
- Solo Endian tiene contacto con cada una de las zonas establecidas.

Figura 3. Configuración endian desde web



Fuente: Oscar Gordillo

CONCLUSIONES

La instalación y configuración de Endian Firewall en virtualbox permite comprender la importancia de una adecuada segmentación de red dentro de un entorno seguro. También la separación de zonas WAN, LAN y DMZ facilitó la administración de tráfico de red, mejorando significativamente la protección de los recursos internos.

La configuración realizada garantizo una base estable para que los demás integrantes del grupo implementen servicios adicionales correspondientes a las demás temáticas. Con esta primera etapa se estableció una infraestructura sólida y lista para el desarrollo del resto de los puntos desarrollados a continuación.

5.2 TEMÁTICA 2: CONFIGURACIÓN NAT

La configuración de NAT (Network Address Translation) en Endian Firewall constituye uno de los pasos fundamentales para habilitar la comunicación entre las distintas zonas de la red —LAN (Zona Verde), DMZ (Zona Naranja) y WAN (Zona Roja)—. En esta temática se buscó garantizar que tanto la red interna (LAN) como los servidores ubicados en la DMZ pudieran acceder a Internet de manera segura.
El trabajo que se presenta a continuación está basado estrictamente en las acciones ejecutadas durante la implementación mediante un entorno virtual configurado en VirtualBox y documentado en el archivo de evidencia. Todo el procedimiento fue validado mediante pruebas de conectividad reales usando *ping*, acceso HTTP y revisión del tráfico en la consola del firewall.

OBJETIVOS

Los objetivos principales de esta temática fueron:

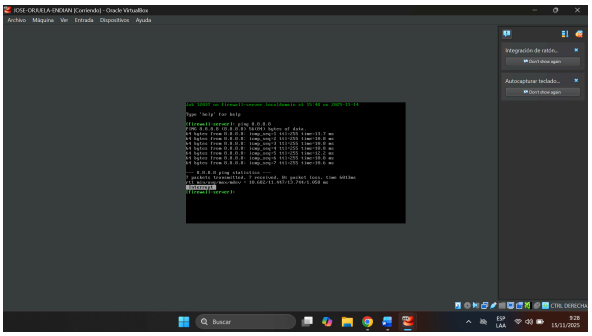
- Habilitar NAT para la LAN, permitiendo navegar desde la zona Verde hacia la zona Roja (Internet).

- Configurar NAT para la DMZ, permitiendo que los servidores ubicados en la zona Naranja puedan acceder a recursos externos.
- Crear reglas de NAT, con el fin de permitir los accesos de internet a LAN y DMZ
- Validar la funcionalidad del NAT mediante herramientas como *ping*, navegador web y registros del firewall.

VALIDACIÓN DE INTERNET DESDE ENDIAN

Antes de comenzar con la creación de reglas NAT, se verificó que la máquina Endian Firewall tuviera conectividad hacia Internet. Esto se realizó directamente desde la consola de Endian mediante el comando ping 8.8.8.8:

Figura 4. Prueba de red



Fuente: Jose Orjuela

El resultado fue positivo, confirmando que la interfaz Roja (WAN) del firewall sí tenía acceso a Internet. Esta validación es fundamental, ya que si la zona WAN no presenta conectividad, ninguna regla NAT podrá funcionar.

CONFIGURACIÓN NAT PARA LA LAN (ZONA VERDE)

- Acceso a la interfaz web de Endian

Desde la máquina Ubuntu Desktop (LAN), se ingresó al panel de administración de Endian Firewall a través del navegador web. Una vez dentro, se procedió al módulo:

- Creación de la regla NAT para la LAN

Tal como se documentó en el archivo, se diligenciaron los campos solicitados:

✔ Origen: Red/IP → 192.168.10.0

(Se usa .0 para abarcar toda la red LAN)

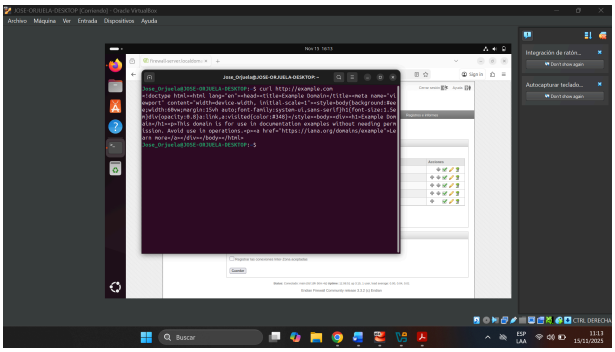
✔ Destino: Zona Roja (Enlace Main Rojo)

✔ Nat: Nat activado

Los demás parámetros se dejaron tal como estaban en el formulario.

Como evidencias se realizaron 3 pruebas garantizando la correcta configuración de las reglas Nat por lo tanto se realizó el envío de paquetes al DNS de google 8.8.8.8, google.com y adicional a ello de realizo un curl a http://example.com lo cual corresponde a una página de prueba obteniendo resultados exitosos como listar el contenido html de la respectiva página.

Figura 5. Pruebas configuración reglas



Fuente: Jose Orjuela

CONFIGURACIÓN NAT PARA DMZ

- Creación de regla NAT para la DMZ

Siguiendo los mismos pasos de la LAN, se creó una regla NAT adicional para permitir que la DMZ pudiera salir a Internet. En el formulario se diligenció:

✔ Origen: Red/IP → 192.168.20.0

(correspondiente a la subred DMZ)

✔ Destino: Zona Roja

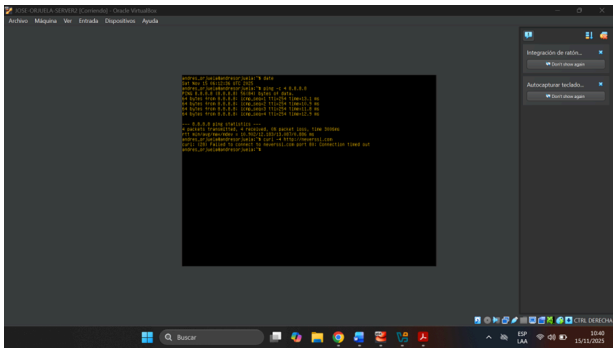
✔ Servicio: Cualquiera

✔ Nat: Nat Activado

Esto garantiza que cualquier servidor ubicado en la DMZ puedan realizar peticiones hacia Internet (actualizaciones, conexión a repositorios, consultas DNS, etc.).

Como evidencias se realizaron 2 pruebas para garantizar el correcto funcionamiento de la regla, se realizo un ping al DNS de google ping -c 4 8.8.8.8 los cual respondio de manera exitosa pero al momento de querer ingresar a una página externa como por ejemplo a http://neverssl.com no funciona esto debido a que se debe a debemos crear unas reglas en el tráfico de salida donde permitamos salida a HTTP, HTTPS y DNS.

Figura 6. Pruebas configuración reglas-Server



Fuente: Jose Orjuela

En el archivo se describe que para permitir la salida de Internet desde la DMZ hacia la WAN, fue necesario configurar reglas adicionales en:
Firewall → Tráfico de salida
Aquí se observó que la zona Verde (LAN) ya tenía reglas predeterminadas, pero la zona Naranja (DMZ) no contaba con ninguna.
Por lo tanto, se crearon tres reglas esenciales:

- ✔ Regla para permitir HTTP (puerto 80):

  Origen: Zona / Interfaz → NARANJA
  Destino: ROJO
  Servicio: HTTP
  Acción: Permitir

- ✔ Regla para permitir HTTPS (puerto 443)

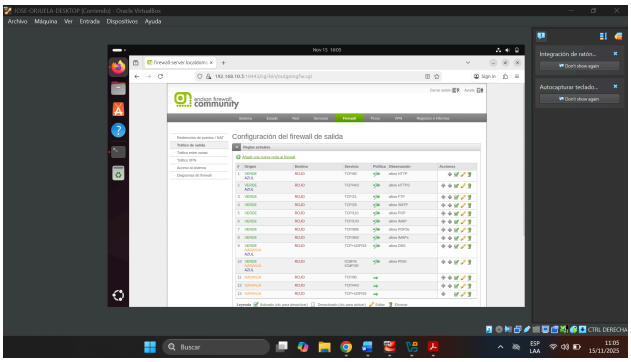
  Origen: NARANJA
  Destino: ROJO
  Servicio: HTTPS
  Acción: Permitir

- ✔ Regla para permitir DNS (puerto 53)

  Origen: NARANJA
  Destino: ROJO
  Servicio: DNS
  Acción: Permitir

Una vez creadas las reglas, estas quedaron visibles en la tabla de “Tráfico de salida”.

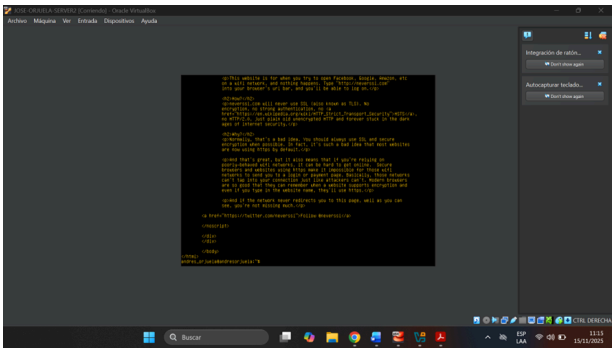
Figura 7. Visualización reglas-tráfico de salida



Fuente: Jose Orjuela

Se realiza nuevamente la prueba en la consola de ubuntu server mediante el comando curl http://neverssl.com y como resultado obtenemos acceso al HTML que hace parte de dicha página.

Figura 8. Visualización desde Ubuntu server



Fuente: Jose Orjuela

VALIDACIONES DE FUNCIONAMIENTO

Las validaciones de funcionamiento realizadas durante la configuración de NAT se basaron en pruebas directas desde cada una de las zonas involucradas: Zona Verde (LAN) y Zona Naranja (DMZ). Estas validaciones permitieron comprobar que las reglas NAT y las reglas de tráfico de salida creadas en Endian Firewall funcionarán según lo esperado. A continuación, se describen las pruebas realizadas y los resultados obtenidos.

CONCLUSIONES

La configuración NAT en Endian Firewall funcionó correctamente, permitiendo que tanto la LAN como la DMZ obtuvieron acceso a Internet mediante reglas de

enmascaramiento aplicadas de forma independiente para cada zona.

La LAN demostró conectividad completa luego de aplicar su regla NAT, logrando comunicación, resolución DNS y acceso HTTP a dominios públicos; validado mediante pruebas de ping y carga de páginas web.

En el caso de la DMZ, se evidenció que NAT por sí solo no era suficiente, ya que los servicios de salida (HTTP, HTTPS, DNS) se encontraban bloqueados. Esto demostró la importancia del filtrado de tráfico dentro del firewall.
Una vez creadas las reglas específicas de salida para la zona Naranja, la DMZ obtuvo acceso total a Internet, logrando resolver dominios y acceder a sitios web externos, lo cual confirma el funcionamiento adecuado de las reglas configuradas.

La práctica permitió comprender cómo Endian Firewall controla el tráfico de manera independiente en cada zona, reforzando el concepto de segmentación de red y seguridad perimetral.

Finalmente, la temática permitió validar que una arquitectura bien segmentada con reglas NAT apropiadas garantiza un entorno seguro, controlado y funcional, replicando el comportamiento esperado en redes corporativas reales.

5.3 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

Esta temática plantea la necesidad de controlar los servicios expuestos en la Zona Naranja (DMZ) y administrar cuidadosamente las políticas de tráfico entre zonas usando Endian Firewall. En un entorno real, la DMZ funciona como una zona intermedia donde se alojan servicios que pueden ser consultados desde la red interna o desde Internet, pero sin exponer directamente los recursos internos ubicados en la LAN.

El propósito principal de esta temática fue habilitar los servicios HTTP (puerto 80) y FTP (puerto 21) desde la LAN hacia la DMZ y, simultáneamente, bloquear el protocolo ICMP para impedir cualquier tipo de reconocimiento entre zonas. Estas actividades permiten emular escenarios reales de seguridad perimetral utilizados por empresas, proveedores de hosting, centros de datos y redes corporativas donde se requiere limitar la visibilidad de los servidores sin impedir totalmente el acceso a los servicios esenciales

OBJETIVOS

- Configurar un servidor Ubuntu dentro de la DMZ para ofrecer servicios HTTP (Apache) y FTP (vsftpd), garantizando su correcta instalación y disponibilidad.
- Establecer reglas de acceso en Endian Firewall que permitan el tráfico HTTP y FTP desde la zona LAN hacia la DMZ, siguiendo políticas de mínimo privilegio.
- Implementar una regla de bloqueo del protocolo ICMP con el fin de evitar el reconocimiento de hosts entre la LAN y la DMZ, reforzando la seguridad y el aislamiento perimetral.
- Validar la accesibilidad de los servicios HTTP y FTP mediante pruebas de conexión desde equipos ubicados en la red LAN.
- Verificar la efectividad del bloqueo de ICMP, comprobando la imposibilidad de realizar ping hacia el servidor DMZ desde la LAN.
- Analizar el comportamiento del firewall ante los flujos de tráfico permitidos y bloqueados, evaluando los resultados frente a la arquitectura de seguridad planteada.
- Documentar la configuración aplicada y las pruebas realizadas, generando evidencia técnica del funcionamiento real de los servicios y las políticas de acceso configuradas.

CONFIGURACIÓN SERVICIOS EN EL SERVIDOR DMZ

El objetivo de habilitar servicios específicos alojados en la zona Naranja (DMZ) y establecer restricciones de seguridad entre zonas mediante reglas del firewall. Esta sección describe paso a paso las configuraciones realizadas en el servidor Ubuntu ubicado en la DMZ y en el panel administrativo de Endian Firewall, siguiendo un enfoque sistemático y orientado a las mejores prácticas de seguridad perimetral.

Una vez instalados los servicios en la DMZ, se procedió a configurar las reglas que permitirían el acceso desde la LAN hacia los servicios HTTP y FTP ubicados en la zona Naranja. Todas las reglas se aplicaron mediante el módulo:

Firewall - Tráfico de salida

- Permitir tráfico HTTP desde la LAN hacia la DMZ
  Se creó una regla con los siguientes parámetros:
  - ✔ Origen: Zona Verde (LAN)
  - ✔ Destino: Zona Naranja (DMZ)
  - ✔ Servicio: HTTP (puerto 80/TCP)
  - ✔ Acción: Permitir

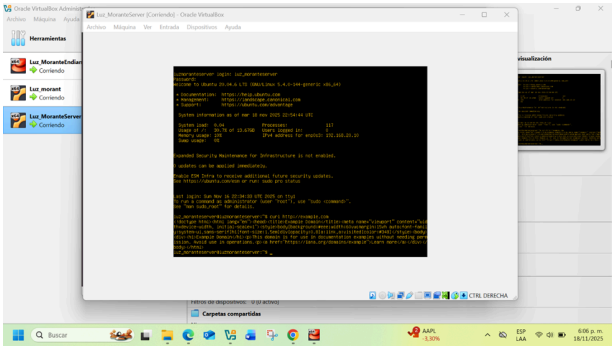
  Esta regla habilitó el acceso al servidor Apache desde cualquier equipo ubicado en la red interna, permitiendo la visualización de páginas web alojadas en la DMZ.

- Permitir tráfico FTP desde la LAN hacia la DMZ
  Se estableció una segunda regla con la siguiente configuración:
  - ✔ Origen: Zona Verde
  - ✔ Destino: Zona Naranja
  - ✔ Servicio: FTP (puerto 21/TCP)
  - ✔ Acción: Permitir

Esta acción garantizó que los equipos de la LAN pudieran conectarse al servidor FTP de la DMZ para realizar transferencias de archivos.

Se procedieron a realizar las respectivas pruebas en ubuntu server accediendo a una página que presente enlace http como por ejemplo curl http://example.com se visualiza cargue de contenido en HTML.

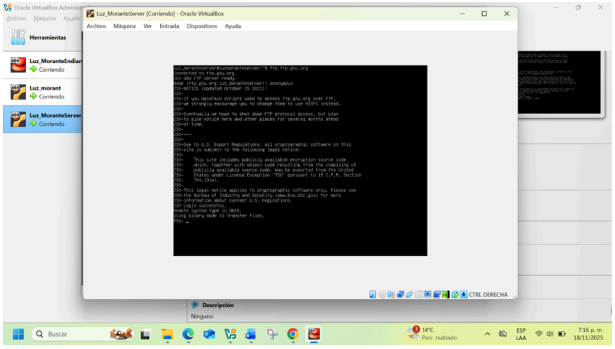
Figura 9. Verificación http



Fuente: Luz Morante

Adicionalmente se realizaron pruebas por medio del ftp mediante el comando ftp ftp.gnu.org como resultamos obtenemos el ingreso de un usuario y en tal caso una contraseña para acceder a su contenido

Figura 10. Verificación ftp



Fuente: Luz Morante

VALIDACIONES

Una vez instalado Apache en el servidor Ubuntu de la DMZ y creada la regla de acceso para HTTP en Endian Firewall, se procedió a validar si un equipo ubicado en la Zona Verde (LAN) podía ingresar al servidor web.

El firewall permitió únicamente el tráfico por el puerto 21 (FTP), lo que evidencia que la regla configurada fue efectiva. La DMZ queda accesible solo para el servicio FTP sin exponer otros puertos, reforzando la seguridad del entorno.

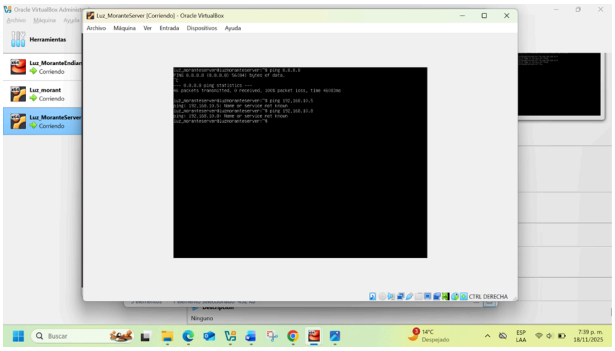
Este comportamiento indica que la regla configurada en Endian:

Origen: Zona Verde
Destino: Zona Naranja
Servicio: ICMP
Acción: Denegar

Este tipo de bloqueo evita ataques de reconocimiento (escaneos, barridos de red) y es una práctica común en seguridad perimetral.

En medio de los resultados, se realiza ping al DNS de google a la LAN y a al equipo de ubuntu desktop lo cual no presenta respuestas.

Figura 11. Verificación regla ICMP.- Denegar



Fuente: Luz Morante

CONCLUSIONES

- La configuración realizada en Endian Firewall permitió habilitar de manera segura los servicios HTTP y FTP alojados en la DMZ, demostrando la efectividad del control de tráfico inter-zona y el adecuado manejo de políticas basadas en puertos. Esto permitió que la zona LAN accediera únicamente a los servicios autorizados, cumpliendo con el principio de mínimo privilegio.
- El bloqueo del protocolo ICMP entre la LAN y la DMZ funcionó correctamente, impidiendo que los equipos internos pudieran detectar o mapear los servidores ubicados en la zona naranja. Esta característica fortalece la seguridad perimetral al reducir la superficie de exposición ante potenciales ataques de reconocimiento.
- Las pruebas de funcionamiento validaron el correcto enrutamiento y filtrado del tráfico, ya que el servidor Apache respondió de forma adecuada por el puerto 80, el servicio FTP permitió conexiones por el puerto 21 y las solicitudes ICMP fueron completamente descartadas. Esto evidencia que las reglas aplicadas en Endian fueron interpretadas y ejecutadas sin inconsistencias.
- La DMZ se comportó como una zona aislada pero accesible únicamente para los servicios específicos autorizados, replicando

el comportamiento esperado en entornos empresariales. Esta segmentación demuestra la importancia de separar los servicios expuestos al interior de redes protegidas para prevenir riesgos de seguridad.

- La implementación práctica permitió comprender de manera integral cómo un firewall controla y gestiona el tráfico entre zonas, reforzando conceptos fundamentales como la separación de redes, aperturas de puertos, servicios críticos, filtrado y políticas de denegación explícita. Esto aporta conocimientos esenciales para el diseño de infraestructuras seguras.
- Finalmente, la Temática 3 consolidó las habilidades del estudiante en el manejo de herramientas de seguridad perimetral, reglas firewall, servicios en DMZ y validación de tráfico, aportando un aprendizaje práctico directamente aplicable en escenarios reales de administración de redes y ciberseguridad.

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

En esta temática se trabajó la implementación de un Proxy HTTP en modo no transparente utilizando Endian Firewall, basados en máquinas virtuales de virtualbox. La finalidad principal es controlar la navegación en internet desde la red local (LAN), aplicando autenticación por usuario y restricciones basadas en perfiles de acceso. Con este tipo de configuración se busca que solo los usuarios autorizados puedan navegar y, adicional a esto, se establecer un control sobre las páginas permitidas y bloqueadas, reforzando la seguridad corporativa en la red.

Este escenario es muy común en redes donde se necesita auditar la navegación, limitar accesos a contenido no deseado, y llevar un registro de los usuarios que ingresan a Internet.

OBJETIVOS

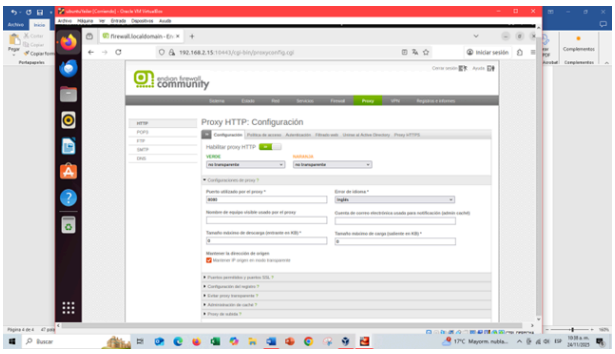
- Habilitar un Proxy HTTP en modo *no transparente*, de forma que los equipos de la LAN requieran configuración manual del proxy en el navegador.
- Crear usuarios y asignarlos a grupos para controlar su acceso mediante autenticación.
- Implementar un perfil con una lista negra de sitios web que no serán accesibles desde la red interna, para este escenario aplicamos la restricción a hotmail.com. youtube.com y elnuevodia.com.co
- Verificar el correcto funcionamiento de las políticas aplicadas, intentando acceder a las URLs restringidas.
- Generar evidencia del control de navegación y bloqueo aplicado a la lista negra.

CONFIGURACIÓN DE LA RED

Primero se habilitó el servicio Proxy desde el menú

Luego se configuró la opción **No transparente**, lo que implica que cada navegador de la LAN debe ser configurado con la dirección IP del Endian como proxy. Esto obliga a que todo usuario se autentique antes de navegar.

Figura 12. Habilitación Proxy

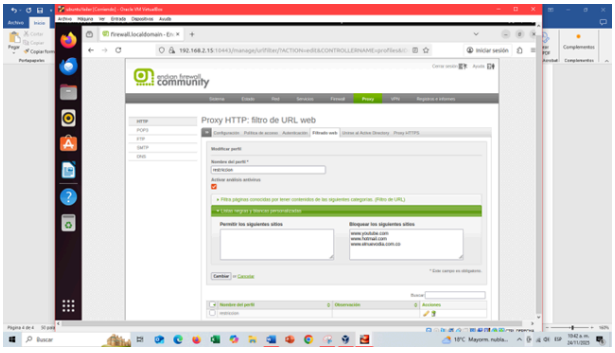


Fuente: Yeiler cortes

Se creó un nuevo perfil llamado usuario, donde se agregó la siguiente lista negra:

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

Figura 13.Creación de lista



Fuente: Yeiler cortes

Luego se realiza la configuración y las politicas deusuarios, esto para la autenticación interna, donde luego se relaciona:

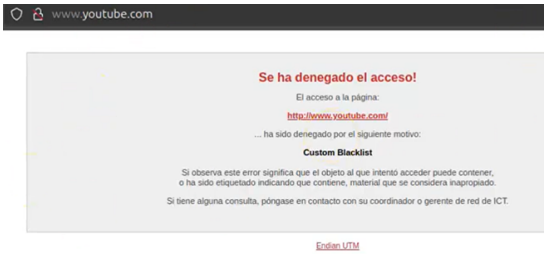
- ✔ origen
- ✔ grupo usuarios
- ✔ perfil
- ✔ autenticación obligatoria.

VALIDACIONES

Al intentar navegar, el sistema solicitó autenticación del usuario configurado, lo cual confirma la correcta activación del proxy no transparente.

Al ingresar a **www.youtube.com** aparece un mensaje de bloqueo del proxy, con la denegación del acceso.

Figura 14. Evidencia de aplicación de permiso



Fuente: Yeiler cortes

Así mismo se ve con las demás páginas que fueron bloqueadas, Otras páginas como google.com o wikipedia.org cargan sin problema una vez autenticado el usuario

CONCLUSIONES

La implementación del proxy HTTP en modo no transparente permite un control efectivo sobre la navegación en la red LAN, ya que gracias al mecanismo de autenticación se puede identificar y gestionar a los usuarios que acceden a Internet, evitando el uso no autorizado y fortaleciendo las políticas de seguridad perimetral.

La creación del perfil con lista negra y su vinculación a una política de acceso demostró que es posible limitar páginas específicas sin afectar el funcionamiento general de la red.

6 CONCLUSIONES

- La implementación de Endian Firewall en VirtualBox permitió comprender de manera práctica la importancia de la segmentación de red para una arquitectura perimetral segura. La definición correcta de las zonas Verde, Roja y Naranja facilitó el control del tráfico y evidenció cómo el firewall actúa como punto central de gestión entre redes con distinto nivel de confianza. Esta temática dejó establecida una infraestructura sólida y funcional, necesaria para dar continuidad al resto de configuraciones del proyecto, demostrando que una instalación bien realizada es clave para garantizar estabilidad, aislamiento y seguridad.

- La configuración de NAT evidenció que la traducción de direcciones es fundamental para permitir que redes privadas accedan a Internet sin exponer sus direcciones internas. Gracias a las reglas aplicadas, tanto la LAN como la DMZ lograron conectividad externa mediante enmascaramiento, validando el funcionamiento adecuado del firewall. Esta temática permitió reforzar el entendimiento de cómo NAT, combinado con reglas de tráfico, garantiza navegación segura al mismo tiempo que mantiene el control centralizado sobre los flujos de red. Su correcta ejecución confirmó que la DMZ requiere políticas estrictas para no comprometer la seguridad general.

- La habilitación de HTTP y FTP desde la LAN hacia la DMZ funcionó de manera controlada, permitiendo validar servicios sin exponer otros puertos críticos. La regla de bloqueo ICMP evitó el reconocimiento entre zonas, reforzando el aislamiento del servidor y reduciendo la superficie de ataque. En conjunto, esta práctica confirmó la importancia del principio de mínimo privilegio y del uso selectivo de reglas para mantener la integridad de la DMZ.

- La implementación del proxy no transparente permitió comprender cómo controlar la navegación dentro de la LAN mediante autenticación y filtrado de contenido. Gracias al perfil con lista negra y políticas de usuario, se logró restringir el acceso a sitios específicos sin afectar la navegación general. La autenticación reforzó la trazabilidad del uso de Internet y mostró que el proxy es una herramienta eficaz para aplicar normas corporativas de navegación. Esta temática evidenció cómo la combinación de proxy, perfiles y grupos permite un control riguroso sobre el comportamiento de los usuarios en la red.

7 REFERENCIAS

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

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

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

Endian S.r.l., “Endian Firewall Community Documentation,” 2023. [Online]. Available: https://www.endian.com.

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

J. McCarty, Network Security Assessment: Know Your Network, 3rd ed. Sebastopol, CA: O'Reilly Media, 2021.
Cisco Systems, "DMZ Design Guide," Cisco Press, 2020. [Online]. Available: https://www.cisco.com

K. Beau, Practical Linux Security Cookbook, 3rd ed. Birmingham, U.K.: Packt Publishing, 2023.

LPI – Linux Professional Institute, "Linux Essentials Exam 010-160 Objectives," 2024. [Online]. Available: https://www.lpi.org

M. Cooper, Beginning Linux System Administration. Berkeley, CA: Apress, 2020.

Red Hat Inc., "Linux Security Guide," 2022. [Online]. Available: https://access.redhat.com/documentation/

Ubuntu Documentation Team, "Ubuntu Server Guide," Canonical Ltd., 2023. [Online]. Available: https://ubuntu.com/server/docs

W. Shotts, The Linux Command Line: A Complete Introduction, 2nd ed. San Francisco, CA: No Starch Press, 2019