IMPLEMENTACIÓN DE UNA ARQUITECTURA DE SEGURIDAD PERIMETRAL EN ENTORNOS VIRTUALIZADOS MEDIANTE GNU/LINUX ENDIAN, NAT, DMZ Y CONTROL DE ACCESO DE TRÁFICO

Angie Daniela Anacona Taque
e-mail: adanaconat@unadvirtual.edu.co
Diego Fernando Salazar Pulgarín
e-mail: dfsalazarpu@unadvirtual.edu.co
Luisa Fernanda Pérez Meza
e-mail: lfperezme@unadvirtual.edu.co
Rendell Ruiz Muñoz
e-mail: rruizmu@unadvirtual.edu.co
Victor Alfonso Casas Hernandez
e-mail: vacasash@unadvirtual.edu.co

RESUMEN: *En este documento se presenta el desarrollo de la Etapa 7 del diplomado, enfocada en la implementación de seguridad en GNU/Linux. Inicialmente, se abordan conceptos relacionados con la arquitectura del sistema, configuración de hardware, identificación de dispositivos y gestión de módulos del kernel. Posteriormente, se analiza el proceso de arranque del sistema, diferenciando el funcionamiento de BIOS y UEFI, así como el uso de gestores de arranque, parámetros del kernel e initramfs. También se estudian los niveles de ejecución en SysVinit y los objetivos en systemd mediante herramientas de administración de servicios. Finalmente, se documenta la instalación y configuración de Endian Firewall Community en un entorno virtualizado con VirtualBox, incluyendo la configuración de interfaces de red LAN, WAN y DMZ, la implementación inicial del firewall y el acceso al panel administrativo. Todo el proceso se encuentra respaldado mediante evidencias y capturas de pantalla que validan la implementación realizada.*

PALABRAS CLAVE**:** GNU/Linux, firewall, Endian, seguridad, virtualización.

1 INTRODUCCIÓN

En el recorrido que he realizado como estudiante del Diplomado de profundización en administración de sistemas operativos open source con certificación en Linux, me he encontrado con un desafío fundamental que todo administrador de sistemas enfrenta en la actualidad: garantizar la seguridad de la infraestructura tecnológica sin sacrificar la funcionalidad ni el rendimiento. Este documento presenta el desarrollo completo de la Etapa 7, titulada "Implementando Seguridad en GNU/Linux", donde integro los conocimientos adquiridos a lo largo del diplomado para construir una solución de seguridad perimetral funcional y bien documentada.

La motivación principal de este trabajo nace de una realidad ineludible en el mundo de la administración de sistemas: los entornos de producción requieren cada vez más medidas de protección robustas, y GNU/Linux, con su filosofía de código abierto y sus potentes herramientas de seguridad, se presenta como la plataforma ideal para implementar dichas medidas. A lo largo de este documento, abordo desde los fundamentos teóricos de la arquitectura del sistema y los procesos de arranque, hasta la implementación práctica de un firewall corporativo utilizando Endian Firewall Community en un entorno virtualizado con VirtualBox.

2 OBJETIVOS DEL PROYECTO

Objetivo General

Implementar y configurar un entorno de seguridad perimetral en un ambiente virtualizado mediante el uso del firewall Endian Firewall Community, aplicando mecanismos de segmentación de red, reglas NAT, control de tráfico, publicación de servicios HTTP y FTP, políticas de acceso Inter-Zona y autenticación mediante Proxy HTTP, con el fin de garantizar comunicaciones seguras entre las zonas LAN, DMZ y WAN y fortalecer los conocimientos relacionados con administración de redes y seguridad informática.

Objetivos Específicos

Configurar e implementar el firewall Endian Firewall Community en VirtualBox, estableciendo las zonas GREEN (LAN), ORANGE (DMZ) y RED (WAN) para segmentar adecuadamente la infraestructura de red.

Implementar y habilitar los servicios HTTP y FTP en un servidor Ubuntu Server ubicado en la zona DMZ, permitiendo el acceso controlado a los servicios publicados.

Configurar reglas de seguridad para denegar el protocolo ICMP y validar la restricción de respuestas ping dentro de la red mediante pruebas de conectividad.

Establecer reglas de acceso Inter-Zona que permitan o denieguen tráfico HTTP y FTP entre las zonas GREEN, ORANGE y RED, verificando el funcionamiento de las políticas de seguridad configuradas.

Realizar pruebas de conectividad y validación de servicios desde navegador web y herramientas de consola para comprobar la comunicación entre la LAN, la DMZ y la WAN.

Implementar un Proxy HTTP no transparente con autenticación por usuario y políticas de acceso, permitiendo controlar la navegación web mediante listas negras y restricciones de acceso a sitios específicos.

Verificar el funcionamiento de las políticas de autenticación y filtrado web desde la LAN mediante pruebas de navegación y control de acceso a portales bloqueados.

Analizar la importancia de la seguridad perimetral, la segmentación de red y el control de tráfico en la protección de infraestructuras tecnológicas empresariales.

3 METODOLOGIA

Para el desarrollo de la práctica se implementó un entorno virtualizado utilizando Oracle VM VirtualBox y el firewall Endian Firewall Community, configurando las zonas GREEN (LAN), ORANGE (DMZ) y RED (WAN). Inicialmente, se realizó la configuración de las interfaces de red y el direccionamiento IP correspondiente a cada segmento.

Posteriormente, se configuraron reglas NAT, políticas Inter-Zona y mecanismos de Port Forwarding para permitir y controlar la comunicación entre la LAN, la DMZ y la WAN mediante los protocolos HTTP y FTP. Asimismo, se instalaron y configuraron los servicios Apache y vsFTPd en Ubuntu Server ubicado en la DMZ, además de implementar restricciones de tráfico ICMP y políticas de acceso mediante Proxy HTTP con autenticación de usuarios.

Finalmente, se realizaron pruebas de conectividad y validación utilizando herramientas de consola y navegador web, permitiendo comprobar el funcionamiento de los servicios, las reglas de acceso y las políticas de seguridad configuradas en la infraestructura de red.

4 DESARROLLO TECNICO

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

DESCARGA DE LA IMAGEN ISO

Inicié el proceso descargando la imagen ISO de Endian Firewall Community desde el sitio oficial. Seleccioné la versión 3.3.2 para 64 bits, que es la más estable y compatible con mi hardware. Verifiqué el checksum y coincidió con el publicado en el sitio oficial, lo que me garantizó que la descarga fue exitosa y el archivo no estaba corrupto.

CREACIÓN DE LA MÁQUINA VIRTUAL

En VirtualBox, procedí a crear una nueva máquina virtual con las siguientes características: la nombré "Endian- Firewall-Casas" como identificador único con mi apellido; seleccioné tipo Linux porque Endian está basado en Linux; elegí la versión Linux 2.6/3.x/4.x (64-bit) por su compatibilidad con el kernel de Endian; asigné 2048 MB de RAM, que es el mínimo recomendado para un rendimiento óptimo; y configuré un disco duro de 20 GB en formato VDI dinámico, suficiente para almacenar logs y configuraciones futuras.

EL ACCESO A LA INTERFAZ WEB Y LA ADVERTENCIA DEL CERTIFICADO

Cuando intenté acceder por primera vez a la interfaz web de administración de Endian Firewall, mi navegador Chrome me mostró una pantalla que, confieso, me generó un momento de incertidumbre.

La dirección que escribí fue https://192.168.1.200:10443, que corresponde a la IP que configuré para la Zona Verde de mi firewall. En lugar de ver el panel de control que esperaba, el navegador me recibió con un mensaje en rojo que decía "La conexión no es privada". Al principio, mi reacción fue preguntarme si había cometido algún error durante la instalación. Sin embargo, recordé lo que habíamos estudiado sobre certificados SSL en el curso.

Endian Firewall genera un certificado auto firmado durante su instalación, y los navegadores modernos como Chrome están programados para desconfiar de este tipo de certificados porque no fueron emitidos por una autoridad certificadora reconocida a nivel mundial.

Lo que esta imagen representó para mí fue el momento en que la teoría se encontró con la práctica. Entendí que no se trataba de un problema de seguridad real, sino de una medida de precaución del navegador. La comunicación entre mi computadora y el firewall seguía siendo cifrada y segura; simplemente faltaba que una entidad externa validara la identidad del certificado.

Para continuar con mi trabajo, hice clic en el botón "Avanzado" y luego en el enlace que me permitió acceder al sitio de todos modos. Esta captura fue importante para mí informe porque documentó que logré llegar hasta este punto de la instalación, confirmó que la IP 192.168.1.200 quedó correctamente configurada, y demostró que el servicio HTTPS de Endian está funcionando en el puerto 10443.

Al expandir las opciones adicionales, el navegador me mostró información más detallada sobre por qué estaba bloqueando el acceso. El mensaje decía: "Este servidor no ha podido probar que su dominio es 192.168.1.200, el sistema operativo de tu ordenador no confía en su certificado de seguridad". Leí con atención cada palabra porque quería entender exactamente qué estaba pasando antes de tomar la decisión de continuar.

Esta pantalla representó para mí el momento crucial donde debía tomar una decisión informada. El navegador me estaba dando todas las herramientas para entender el riesgo y, al final, me presentaba la opción con un enlace que decía "Acceder

a 192.168.1.200 (sitio no seguro)". No era que el sitio fuera realmente inseguro, sino que el navegador no podía garantizar su seguridad por la falta de un certificado validado externamente

.

Antes de hacer clic, me detuve un momento a pensar en lo que había aprendido en el curso sobre certificados digitales. Entendí que los certificados autoformados como el que genera Endian son perfectamente válidos para entornos de prueba y aprendizaje, aunque los navegadores comerciales muestren este tipo de advertencias. Con esa claridad mental, hice clic en el enlace para continuar.

LA PANTALLA DE BIENVENIDA

Después de hacer clic en el enlace para acceder al sitio a pesar de la advertencia del certificado, finalmente apareció la pantalla que tanto esperaba ver. La imagen mostró la página de bienvenida de Endian Firewall Community, con su característico fondo oscuro y el logotipo de la plataforma en la parte superior. En el centro de la pantalla, un mensaje me daba la bienvenida con un tono amable y profesional.

Confieso que en ese momento sentí una gran satisfacción. Después de todos los pasos que había seguido — descargar el ISO, crear la máquina virtual en VirtualBox, configurar las tres interfaces de red, particionar el disco, establecer contraseñas y enfrentar la advertencia del certificado— finalmente estaba viendo la luz al final del túnel. En la parte inferior de la pantalla, pude identificar la versión que estaba instalando: Versión 3.3.2 de la comunidad de Endian Firewall.

Esto confirmó que había descargado la versión correcta y que el proceso de instalación se había completado exitosamente.

CONFIGURACIÓN DEL IDIOMA Y ZONA HORARIA

Después de hacer clic en el botón de continuar, el asistente de configuración me presentó una pantalla donde debía definir dos parámetros fundamentales para mi firewall: el idioma de la interfaz yla zona horaria en la que operaría el sistema. En el primer campo, el sistema ya había detectado automáticamente mi preferencia y mostraba "español (español)". Decidí verificar manualmente el desplegable para asegurarme de que no hubiera ninguna otra variante del español que pudiera afectar la visualización de fechas o formatos.

El segundo campo, la zona horaria, era especialmente importante para mí porque sé que los registros de logs, las marcas de tiempo en los eventos de seguridad y la programación de tareas automáticas dependen directamente de una configuración horaria precisa. En el desplegable, busqué y seleccioné "América/Bogotá", que corresponde a mi ubicación geográfica actual. Esta decisión no fue trivial para mí, ya que, en administración de sistemas, tener la hora correcta es fundamental para auditar eventos de seguridad y correlacionar incidentes.

ACEPTACIÓN DE LA LICENCIA GPL

Esta pantalla me presentó un momento de gran significado para mí, no solo como estudiante de sistemas, sino como usuario del software de código abierto. El asistente de configuración de Endian Firewall me mostró la GNU General Public License versión 2, el marco legal que protege la libertad del software que estaba a punto de utilizar.

Me tomé un momento para leer el preámbulo de la GPL, ese fragmento que siempre me ha parecido inspirador desde que comencé a estudiar software libre. Las palabras resonaron en mi mente: las licencias de la mayoría del software están diseñadas para quitarle la libertad de compartir y modificarlo, mientras que la GPL hace exactamente lo contrario: garantiza la libertad de compartir y modificar el software. Esta filosofía es precisamente la razón por la cual elegí trabajar con herramientas GNU/Linux para mi formación profesional.

CONFIGURACIÓN DE CONTRASEÑAS

Esta pantalla representó para mí uno de los momentos más críticos de todo el proceso de instalación. El asistente me presentaba la opción de cambiar la contraseña por defecto, y entendí de inmediato la importancia de este paso desde el punto de vista de la seguridad. Lo que veía en mi monitor era un formulario que me permitiría establecer dos contraseñas fundamentales para el funcionamiento de mi firewall: por un lado, la contraseña del administrador para la interfaz web, que sería la llave de acceso al panel gráfico desde donde administraría todas las configuraciones de seguridad; por otro lado, la contraseña SSH para el usuario root, que protegería el acceso por línea de comandos.

En ese momento recordé las palabras de mi profesor sobre la importancia de las contraseñas seguras. No podía caer en el error de usar contraseñas débiles o predecibles. Un firewall es el primer punto de defensa de toda la infraestructura de red, y si alguien lograra acceder a él, tendría el control total sobre el tráfico que pasa entre la LAN, la DMZ y la WAN.

Me tomé un momento para diseñar mis contraseñas. Decidí que ambas serían robustas, combinando mayúsculas, minúsculas, números y caracteres especiales. Las escribí en un cuaderno físico que tengo exclusivamente para registrar este tipo de información sensible, asegurándome de no perderlas ni exponerlas digitalmente

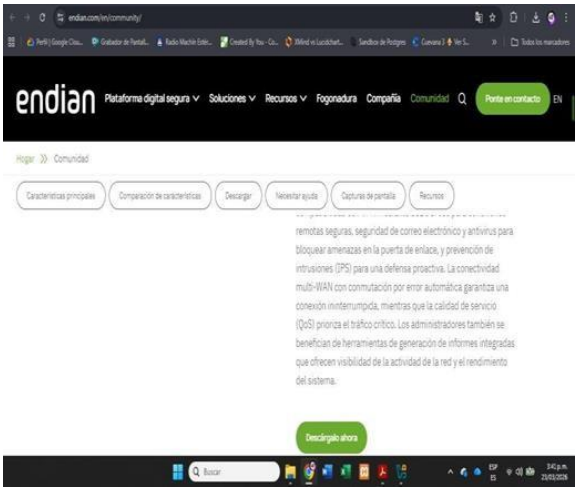
Tabla 1, características máquina virtual

Configuración	Valor asignado	Justificación
Nombre	Endian-Firewall-Casas	Identificador único con mi apellido
Tipo	Linux	Endian está basado en Linux
Versión	Linux 2.6/3.x/4.x (64-bit)	Compatible con el kernel de Endian

RAM	2048 MB	Mínimo recomendado para rendimiento óptimo
Disco duro	20 GB VDI	Suficiente para logs y configuraciones

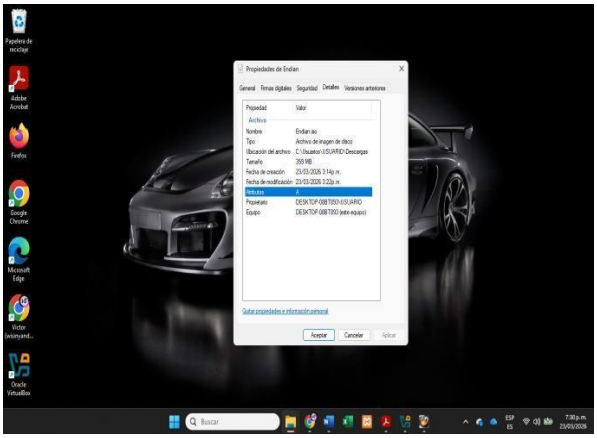
Fuente: Autoría Propia

Figura 1. Descargando endian



Fuente: Autoría propia

Figura 2, instalando endian



Fuente: Autoría propia

4.1.2 TEMÁTICA 2: CONFIGURACIÓN NAT

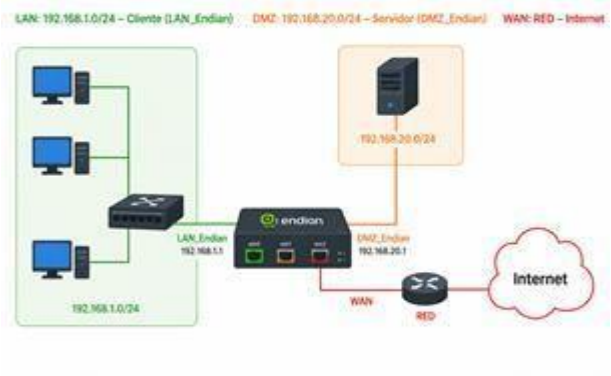
La infraestructura de red implementada estuvo compuesta por tres segmentos principales administrados mediante Endian Firewall Community:

- RED (WAN): conexión hacia Internet.
- GREEN (LAN): red interna donde se ubicó Ubuntu Cliente.
- ORANGE (DMZ): zona desmilitarizada donde se configuró Ubuntu Server.

La segmentación permitió aislar los servicios públicos de la red interna, aplicando políticas de seguridad independientes para cada zona.

La máquina Ubuntu Cliente fue configurada dentro de la red interna LAN_Endian utilizando direccionamiento privado 192.168.0.0/24, mientras que Ubuntu Server fue conectado a la red ORANGE para la publicación controlada de servicios HTTP.

Figura 1. Topología de Red Endian Firewall



Fuente: Autoría propia

CONFIGURACIÓN DE NAT EN ENDIAN FIREWALL

Se realizó la configuración del mecanismo NAT en Endian Firewall con el fin de permitir que las redes internas GREEN y ORANGE pudieran acceder a Internet mediante la interfaz RED. Endian implementó automáticamente una regla de Source NAT (Masquerading), permitiendo ocultar las direcciones privadas internas y traducirlas hacia la dirección pública de salida WAN.

Adicionalmente, se configuraron reglas de Destination NAT (Port Forwarding) para publicar servicios HTTP alojados en el servidor Ubuntu ubicado en la DMZ.

CONFIGURACIÓN UBUNTU CLIENTE

El Ubuntu Cliente fue configurado en VirtualBox utilizando un adaptador de red interna denominado LAN_Endian. Posteriormente se verificó la configuración IP mediante el comando:

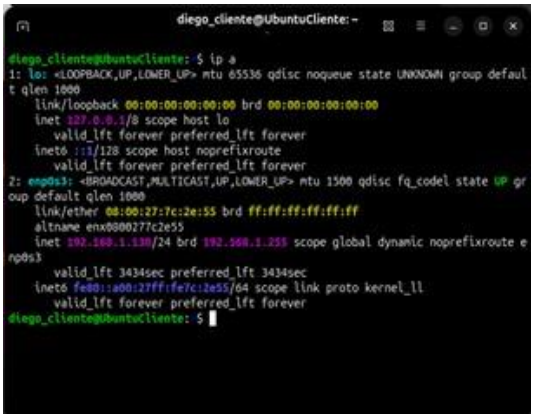
ip a

También se validó la puerta de enlace predeterminada utilizando:

ip route

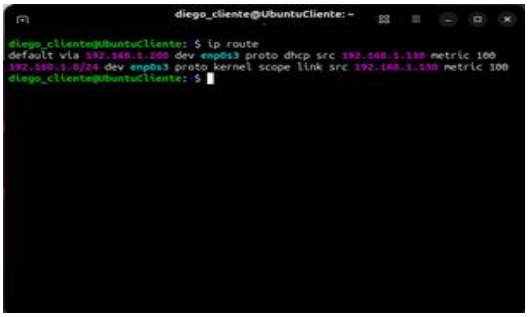
Las pruebas de conectividad realizadas hacia Internet permitieron confirmar el correcto funcionamiento del NAT configurado en Endian Firewall.

Figura 2. Ip a Cliente



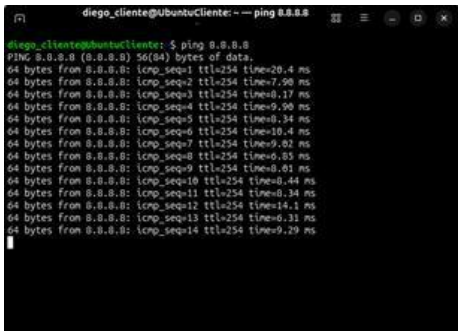
Fuente: Autoría propia

Figura 3. Ip route Cliente



Fuente: Autoría Propia

Figura 4. ping 8.8.8.8 Cliente



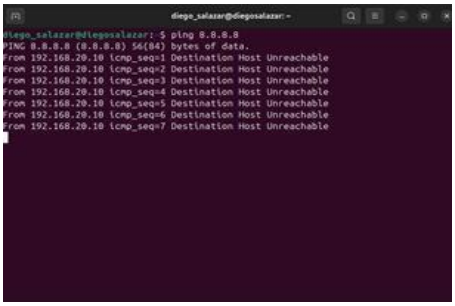
Fuente: Autoria propia

CONFIGURACIÓN UBUNTU SERVER DMZ

El Ubuntu Server fue ubicado dentro de la zona ORANGE (DMZ) con el propósito de alojar servicios accesibles desde otras redes. La configuración IP y la puerta de enlace fueron verificadas mediante los comandos ip a e ip route.

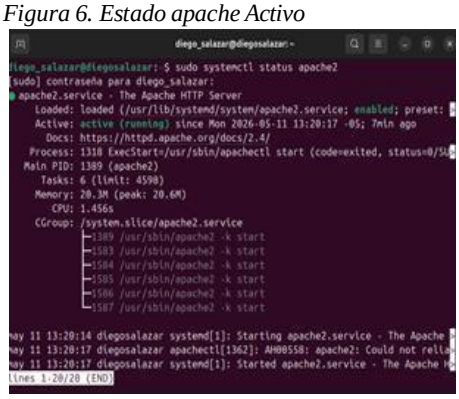
Durante las pruebas iniciales de conectividad se comprobó que Endian Firewall bloquea por defecto el tráfico saliente desde la DMZ, comportamiento coherente con las políticas de seguridad perimetral. Posteriormente se habilitaron reglas específicas para permitir el acceso controlado a servicios HTTP mediante Destination NAT.

Figura 5. Ping Fallido 8.8.8.8 Serve



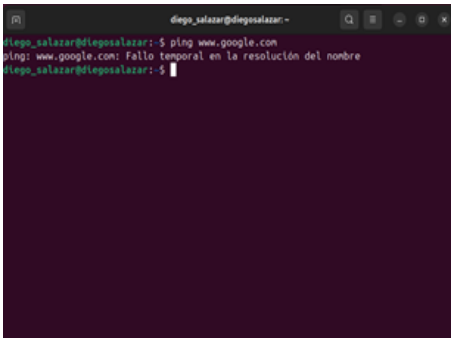
Fuente: Autoria propia

Figura 6. Estado apache Activo



Fuente: Autoría propia

Figura 7. Ping DNS Fallido



Fuente: Autoria propia

VERIFICACIÓN DESDE EL PANEL WEB ENDIAN

La administración del firewall se realizó desde el panel web de Endian mediante acceso HTTPS desde un equipo ubicado en la red GREEN.

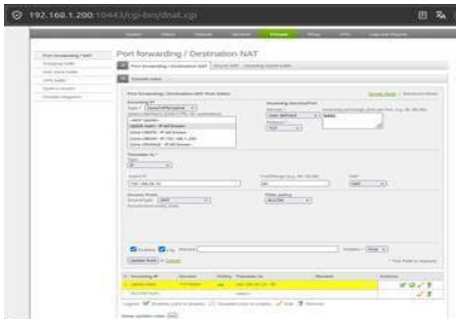
Desde el Dashboard se verificó el estado activo de las interfaces GREEN, ORANGE y RED, así como el tráfico entrante y saliente generado durante las pruebas de conectividad.

También se validó la presencia de reglas automáticas de Source NAT (Masquerading) y reglas manuales de redirección de puertos para la publicación de servicios en la DMZ.

Figura 8. Dashboard Endian

Fuente: Autoria propia

Figura 9. Reglas Firewall



Fuente: Autoria propia

Figura 10. Reglas Nat

Fuente: Autoría propia

RELACIÓN ENTRE ENDIAN, UBUNTU CLIENTE Y UBUNTU SERVER

En la infraestructura implementada, Endian Firewall Community actúa como el núcleo de seguridad y control de la red, mientras que Ubuntu Cliente y Ubuntu Server cumplen roles específicos dentro de zonas diferenciadas.

El Ubuntu Cliente se ubica en la zona LAN (GREEN) y representa a los usuarios internos de la red. Desde este equipo se realizan las tareas de administración, navegación web y pruebas de conectividad. Todo el tráfico generado por el cliente pasa obligatoriamente por Endian, que decide si se permite, bloquea o redirige según las reglas de firewall, NAT y proxy configuradas.

El Ubuntu Server se encuentra en la zona DMZ (ORANGE) y aloja servicios públicos como HTTP (Apache) y FTP (vsftpd). Esta zona intermedia permite que dichos servicios sean accesibles desde la red interna o desde Internet, sin exponer directamente la LAN. Endian controla el acceso a este servidor mediante reglas inter-zona y técnicas de DNAT (Port Forwarding), reduciendo el riesgo de que una posible vulneración del servidor afecte a la red interna.

El Endian Firewall interconecta y aísla ambas máquinas mediante la segmentación en zonas de seguridad (GREEN, ORANGE y RED). Además, aplica NAT de salida, filtrado de tráfico, bloqueo de protocolos como ICMP, y un proxy HTTP con autenticación, garantizando que toda la comunicación entre Ubuntu Cliente, Ubuntu Server e Internet sea segura, controlada y registrada.

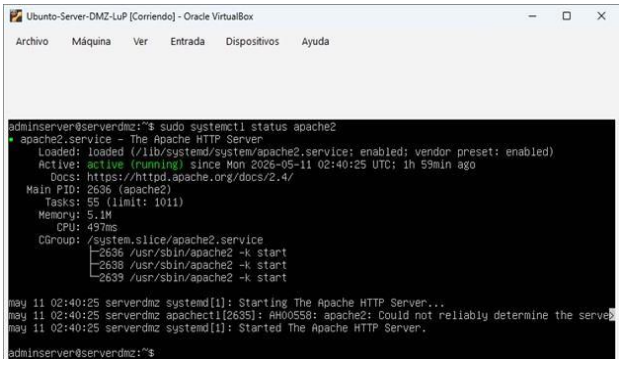
El conjunto, esta arquitectura simula un entorno corporativo real, donde los usuarios, los servidores y el acceso a Internet están protegidos mediante políticas claras de seguridad perimetral.

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

Previo a la implementación de las reglas de firewall, se realizó la validación del estado inicial del servidor Ubuntu Server ubicado en la zona DMZ. Esta validación tuvo como propósito confirmar que los servicios requeridos para la temática se encontraban correctamente instalados y en ejecución.

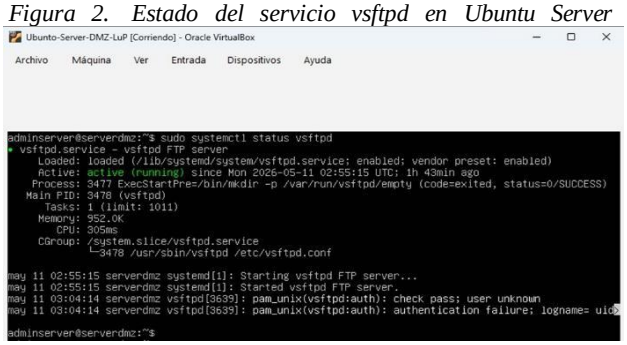
En el servidor DMZ se verificó el estado de los servicios Apache (HTTP) y VSFTPD (FTP), asegurando que ambos estuvieran activos antes de permitir el acceso desde otras zonas de red.

Figura 1. Estado del servicio Apache2 en Ubuntu Server



Fuente: Autoría propia

Figura 2. Estado del servicio vsftpd en Ubuntu Server



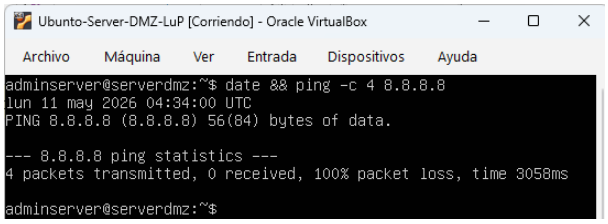
Fuente: Autoría propia

CONFIGURACIÓN DE SERVICIOS EN EL SERVIDOR DMZ

El servidor Ubuntu Server ubicado en la zona DMZ fue configurado para ofrecer los servicios HTTP y FTP. El servicio HTTP fue implementado mediante Apache, escuchando en el puerto estándar 80, mientras que el servicio FTP fue habilitado utilizando VSFTPD sobre el puerto 21. Para el acceso FTP se creó un usuario local exclusivo del servidor, garantizando que la autenticación se realice únicamente contra usuarios del sistema DMZ.

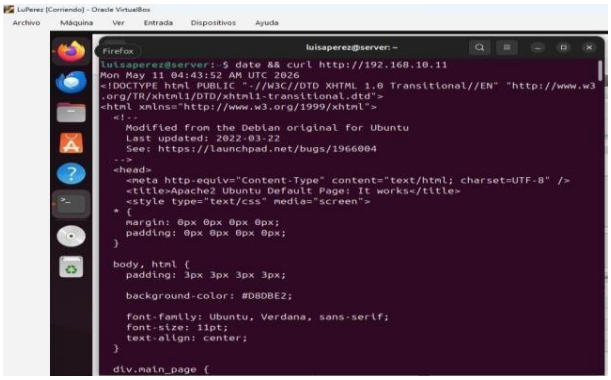
Esta configuración permite que el servidor actúe como un host de servicios públicos controlados, sin otorgar accesos innecesarios a otras capas de la red.

Figura 3. Bloqueo de tráfico ICMP desde la DMZ hacia Internet



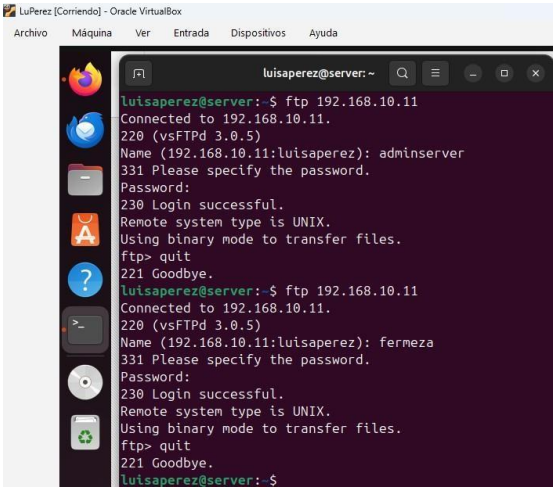
Fuente: Autoría propia

Figura 4. Acceso al servicio HTTP desde la LAN hacia la DMZ



Fuente: Autoria propia

Figura 5. Acceso al servicio FTP desde la LAN hacia la DMZ



Fuente: Autoría propia

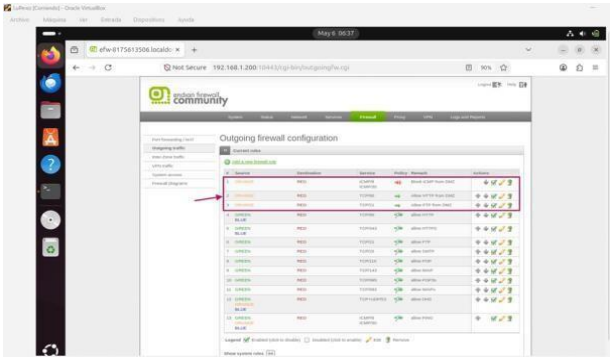
IMPLEMENTACIÓN DE REGLAS DE FIREWALL EN ENDIAN

Para controlar el tráfico de red, se configuraron reglas específicas en GNU/Linux Endian, diferenciando el tráfico saliente hacia Internet (Outgoing traffic) del tráfico entre zonas (Inter-Zone traffic).

- En el tráfico saliente desde la zona DMZ hacia Internet se implementaron las siguientes políticas:
- Bloqueo del protocolo ICMP desde la zona ORANGE hacia la zona RED.
- Permiso del tráfico HTTP (TCP/80) desde la zona ORANGE hacia la zona RED.
- Permiso del tráfico FTP (TCP/21) desde la zona ORANGE hacia la zona RED.

Estas reglas aseguran que el servidor DMZ pueda ofrecer servicios hacia el exterior sin permitir mecanismos de diagnóstico basados en ICMP.

Figura 6. Reglas activas de firewall para tráfico saliente desde DMZ y LAN en Endian Firewall



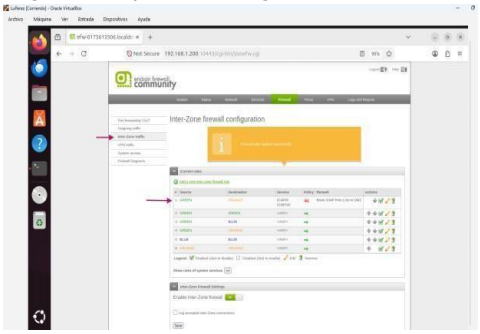
Fuente: Autoria Propia

BLOQUEO DE ICMP ENTRE ZONAS

Adicionalmente, se implementó una regla de firewall de tipo Inter-Zone traffic para bloquear el tráfico ICMP originado desde la red LAN (zona GREEN) hacia la zona DMZ (zona ORANGE). Esta medida evita que los equipos de la LAN puedan identificar o mapear el servidor DMZ mediante solicitudes de ping, reforzando la política de seguridad.

La regla fue configurada con acción de denegación y posicionada como prioridad alta para garantizar su correcta aplicación.

Figura 7. Definición de regla ICMP en Inter-Zone traffic



Fuente: Autoria propia

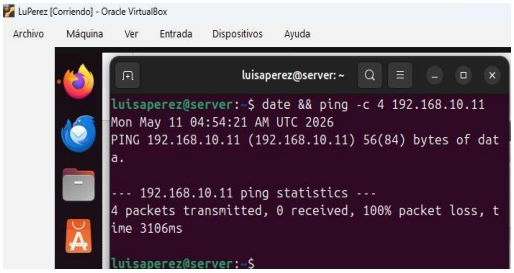
VALIDACIÓN DE LAS REGLAS DE SEGURIDAD APLICADAS

Para validar la correcta implementación de las reglas dfirewall, se realizaron pruebas de conectividad desde la red LAN hacia el servidor DMZ y desde el propio servidor DMZ hacia Internet.

Desde la red LAN se comprobó que el acceso al servicio HTTP y FTP del servidor DMZ es exitoso, evidenciando que los puertos 80 y 21 se encuentran correctamente habilitados. En contraste, los intentos de comunicación mediante ICMP desde la LAN hacia la DMZ no obtuvieron respuesta, confirmando el bloqueo del protocolo.

De igual manera, desde el servidor DMZ se ejecutaron pruebas ICMP hacia Internet, las cuales fueron bloqueadas de acuerdo con las reglas definidas, mientras que otros servicios continuaron funcionando de forma normal.

Figura 8. Bloqueo de tráfico ICMP desde la LAN hacia la DMZ



Fuente: Autoria propia

4.1.4 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

Para el desarrollo de la práctica se utilizó un entorno virtualizado mediante VirtualBox, implementando máquinas Ubuntu y el firewall Endian Firewall Community.

La infraestructura fue dividida en tres zonas de red:

- Zona GREEN (LAN): 192.168.1.200/24
- Zona ORANGE (DMZ): 192.168.2.1/24
- Zona RED (WAN): conexión externa

Inicialmente se configuraron las interfaces de red y el direccionamiento IP correspondiente a cada segmento. Posteriormente se instalaron y configuraron los servicios Apache y vsFTPd en la máquina Ubuntu Server ubicada en la DMZ.

Luego se procedió a crear reglas Inter-Zona y políticas NAT en el firewall con el propósito de permitir la comunicación HTTP y FTP entre las diferentes zonas. Finalmente, se realizaron pruebas de conectividad utilizando comandos de consola y navegador web.

COMUNICACIÓN GREEN HACIA ORANGE MEDIANTE HTTP Y FTP

Se crearon reglas de firewall Inter-Zona permitiendo el tráfico desde la zona GREEN hacia la zona ORANGE mediante los protocolos HTTP y FTP.

Las reglas configuradas fueron:

- GREEN → ORANGE → TCP/80 → ALLOW
- GREEN → ORANGE → TCP/21 → ALLOW

Estas reglas permitieron habilitar el acceso al servidor Apache y al servidor FTP ubicados en la DMZ.

Figura 1. Configuración de reglas en el tráfico inter- zonas en Endian Firewall
Fuente: Autoría propia

COMUNICACIÓN WAN HACIA DMZ

Se configuraron reglas NAT y Port Forwarding con el objetivo de publicar servicios desde la DMZ hacia la WAN. Para ello, el firewall redirigió las conexiones entrantes hacia el servidor ubicado en la IP 192.168.2.10.

La regla NAT implementada permitió redirigir el puerto TCP/8080 del firewall hacia el puerto TCP/80 del servidor Apache ubicado en la DMZ.

Figura 2. Configuración de reglas en el tráfico Port forwarding /NAT en Endian Firewall

Fuente: Autoria propia

VERIFICACIÓN DE REGLAS INTER-ZONA

Posteriormente se verificó la correcta creación de las reglas Inter-Zona en el firewall Endian Firewall Community, evidenciando la habilitación de los servicios HTTP y FTP entre las diferentes zonas de red.

Las reglas visualizadas fueron:

- GREEN → ORANGE → TCP/80 → ALLOW
- GREEN → ORANGE → TCP/21 → ALLOW

Figura 3. Validación de las reglas configuradas en el módulo "Inter-Zone Traffic" de Endian Firewall

Fuente: Autoria propia

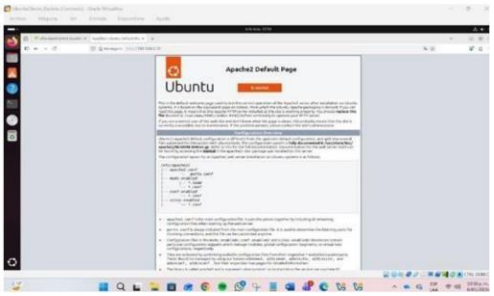
PRUEBA HTTP DESDE LAN HACIA DMZ

Desde Ubuntu Cliente se ejecutó el comando:

curl http://192.168.2.10

Como resultado se obtuvo la respuesta HTTP, correspondiente a la página predeterminada de Apache, validando el correcto funcionamiento del servicio web.

Figura 4. Prueba de acceso HTTP



Fuente: Autoría propia

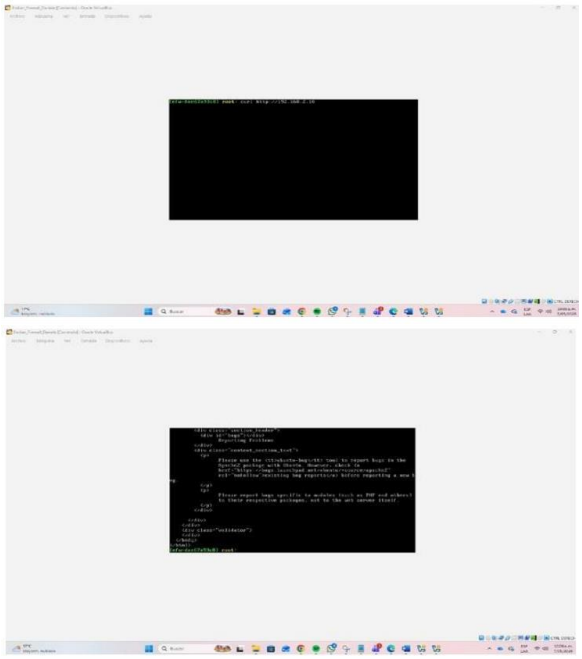
PRUEBA HTTP DESDE WAN HACIA DMZ

Desde la consola del firewall Endian se ejecutó:

curl http://192.168.2.10

La respuesta obtenida evidenció el correcto funcionamiento de la publicación del servicio HTTP mediante NAT.

Figura 5. Prueba de conectividad desde la consola de Endian Firewall



Fuente: Autoría propia

PRUEBA FTP DESDE WAN HACIA DMZ

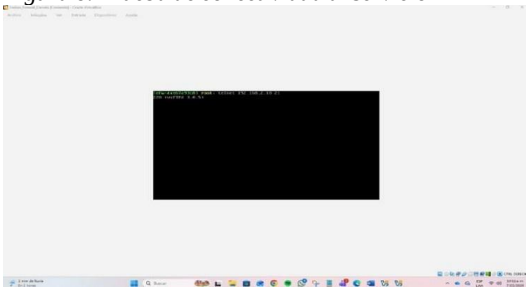
Se realizó una prueba de conectividad al puerto TCP/21 utilizando herramientas de consola, obteniendo respuesta exitosa del servicio vsFTPd.

La respuesta presentada fue:

220 (vsFTPd 3.0.5)

Lo anterior permitió validar el funcionamiento del servicio FTP y la comunicación entre la WAN y la DMZ.

Figura 6. Prueba de conectividad al servicio FTP



Fuente: Autoría propia

Las pruebas realizadas permitieron comprobar el funcionamiento correcto de las reglas de acceso implementadas en el firewall Endian Firewall Community. La comunicación entre las zonas GREEN, ORANGE y RED fue validada exitosamente mediante los protocolos HTTP y FTP.

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

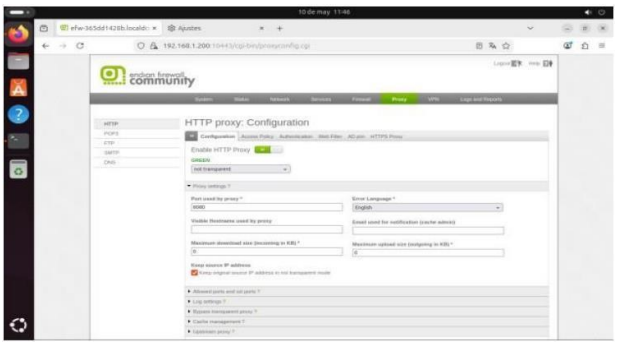
El control del acceso a internet en redes corporativas y académicas constituye una necesidad de seguridad real. Un proxy HTTP no transparente actúa como intermediario entre los clientes internos e internet, requiriendo configuración manual en el navegador y autenticación previa, lo que permite al administrador definir con precisión quién navega, hacia dónde y cuándo.

Endian Firewall Community (EFW) es una distribución GNU/Linux especializada en gestión unificada de amenazas (UTM) que integra en una sola plataforma firewall de inspección de estado, proxy HTTP/HTTPS con Squid, VPN, filtrado de contenido web y antivirus. Su modelo de zonas de color (GREEN/LAN, RED/WAN, ORANGE/DMZ) facilita la segmentación del tráfico de red

CONFIGURACIÓN DEL PROXY Y AUTENTICACIÓN

En Proxy → HTTP → Configuration se activó el switch "Enable HTTP Proxy" y se configuró el modo "not transparent" en GREEN con puerto 8080. Esta configuración exige que cada cliente configure manualmente el proxy en su navegador para que el tráfico sea interceptado y autenticado

Figura 1. Proxy HTTP en modo no transparente puerto 8080



Fuente: Autoría propia

PERFIL DE LISTA NEGRA - BLACKLISTRRM

En la pestaña Web Filter se creó el perfil "BlacklistRRM". En la sección "Block the following sites" se ingresaron los tres dominios requeridos

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

y grupos de usuarios, permitiendo niveles de restricción diferenciados por perfil.

INFRAESTRUCTURA E INSTALACIÓN

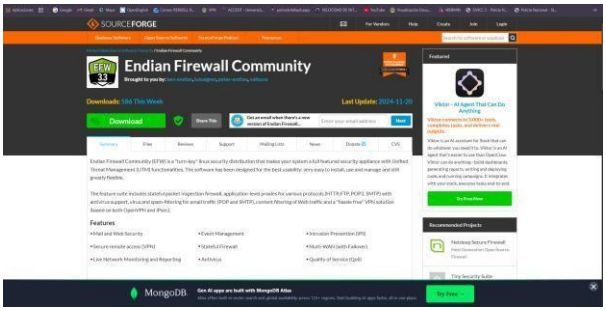
El entorno virtualizado en VirtualBox comprende dos VMs conectadas por la red interna "redproxy":

- VM Endian Firewall
- Adaptador 1: NAT (WAN/RED)
- Adaptador 2: Red interna redproxy (LAN/GREEN: 192.168.1.200/24)
- VM Cliente Ubuntu — Adaptador: Red interna redproxy (IP: 192.168.1.50/24)

El proxy HTTP opera en el puerto 8080 de la interfaz GREEN en modo no transparente

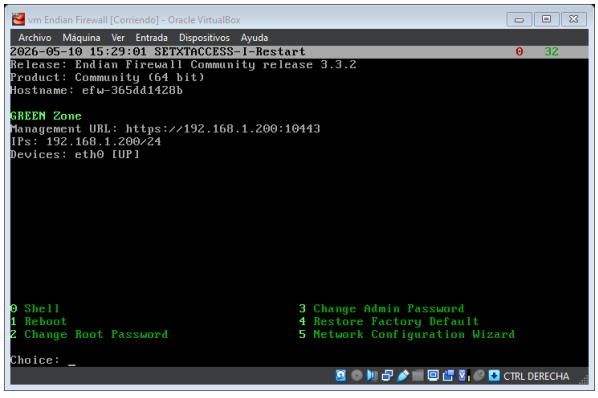
Se descargó el ISO de EFW 3.3.2 desde SourceForge (359 MB). La VM fue configurada con Linux Red Hat 64-bit, 1024 MB RAM y 20 GB de disco. Tras la instalación, el sistema arrancó con la consola de administración mostrando la zona GREEN activa y la URL de gestión https://192.168.1.200:10443

Figura 2. Descarga del ISO de Endian Firewall Community 3.3.2



Fuente: Autoría propia

Figura 3. Consola de Endian: GREEN Zone en 192.168.1.200



Fuente: Autoría propia

ACCESO INTERFAZ

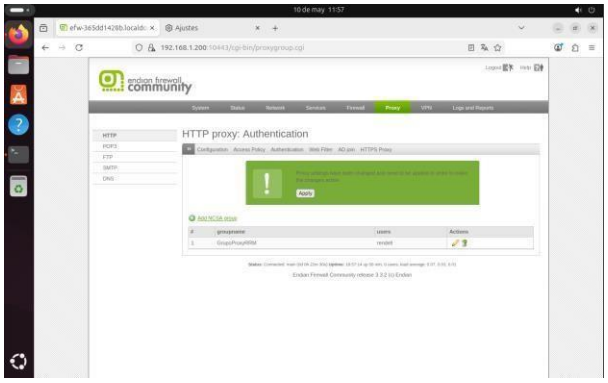
Desde el cliente Ubuntu se accedió a https://192.168.1.200:10443. Se aceptó el certificado auto firmado, se omitió el registro de la comunidad y se ingresaron las credenciales del administrador, accediendo al Dashboard de Endian Firewall Community 3.3.2.

Figura 4. Perfil BlacklistRRM con lista negra configurada
Fuente: Autoría propia

USUARIO, GRUPO Y POLÍTICA DE ACCESO

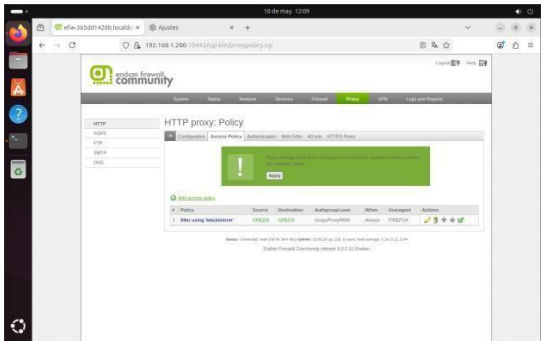
En Proxy → HTTP → Authentication se creó el usuario "rendell" y el grupo "GrupoProxyRRM", asociando el usuario al grupo. En la pestaña Access Policy se configuró la política "filter using blacklistrrm" vinculando: fuente GREEN, grupo GrupoProxyRRM y perfil BlacklistRRM, activa siempre.

Figura 5. Usuario "rendell" asociado al grupo "GrupoProxyRRM"



Fuente: Autoría propia

Figura 6. Política de acceso vinculando BlacklistRRM y GrupoProxyRRM

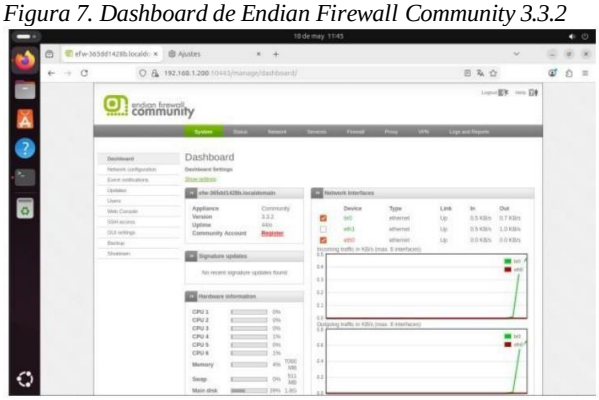


Fuente: Autoría propia

PRUEBAS DESDE LAN

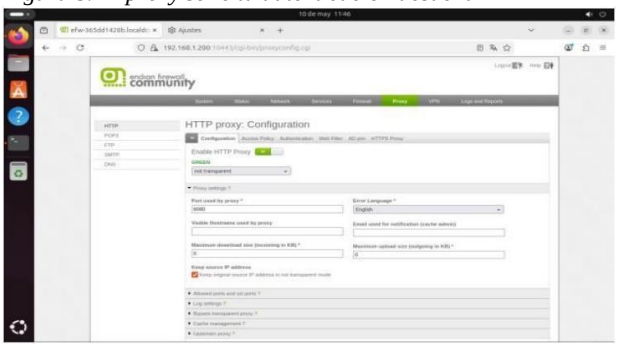
Con el proxy configurado en Firefox (192.168.1.200:8080), al acceder a cualquier sitio HTTP el proxy presentó el diálogo de autenticación. Esto confirma la operación no transparente y la política de autenticación activa para todos los usuarios de la LAN.

Figura 7. Dashboard de Endian Firewall Community 3.3.2



Fuente: Autoría propia

Figura 8. El proxy solicita autenticación desde la LAN

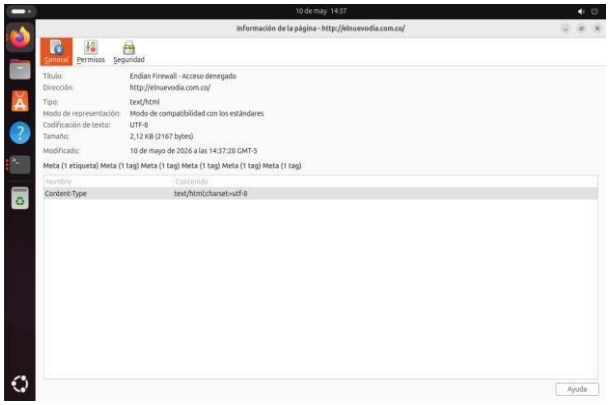


Fuente: Autoría propia

BLOQUEO DE SITIOS EN LISTA NEGRA

Tras autenticarse con el usuario rendell, el acceso a http://elnuevodia.com.co retornó la página "Endian Firewall - Acceso denegado", validando el bloqueo por lista negra. Para hotmail.com y youtube.com el bloqueo HTTP fue efectivo; el tráfico HTTPS requiere SSL Bump para inspección completa.

Figura 9. "Endian Firewall - Acceso denegado" — elnuevodia.com.co



Fuente: Autoría propia

5 CONCLUSIONES.

La implementación de Endian Firewall Community en un entorno virtualizado permitió comprender la importancia de la seguridad perimetral y la segmentación de redes dentro de infraestructuras GNU/Linux. La configuración de las zonas Verde (LAN), Roja (WAN) y Naranja (DMZ) facilitó el entendimiento del funcionamiento de un firewall y del control del tráfico entre diferentes segmentos de red. Asimismo, la configuración de tarjetas de red en Oracle VM VirtualBox y el acceso al panel administrativo permitieron fortalecer conocimientos relacionados con administración de sistemas, virtualización y conectividad. El desarrollo práctico de la actividad evidenció la relevancia de una adecuada configuración de interfaces y políticas de red para garantizar comunicaciones seguras y controladas en entornos empresariales.

La configuración de reglas NAT en Endian Firewall Community permitió establecer correctamente la comunicación entre la LAN y la WAN, así como la salida a Internet desde la zona DMZ, evidenciando el funcionamiento de la traducción de direcciones de red en entornos segmentados. La implementación de mecanismos de Port Forwarding facilitó la publicación controlada de servicios internos sin exponer directamente la red privada, fortaleciendo la seguridad perimetral y el control del tráfico. Asimismo, la verificación de las reglas NAT permitió comprender la importancia de la administración centralizada de las comunicaciones y el papel del firewall como intermediario entre las redes internas y externas.

El desarrollo de la Temática 3 permitió evidenciar la importancia del control del tráfico de salida dentro de un entorno de seguridad perimetral implementado mediante Endian Firewall Community. A través de la configuración de reglas de firewall, fue posible habilitar correctamente los servicios HTTP y FTP desde la zona DMZ, garantizando la disponibilidad controlada de los servicios publicados en Ubuntu Server.

Asimismo, la denegación del protocolo ICMP permitió restringir respuestas de reconocimiento de red mediante pruebas de ping, fortaleciendo la protección de la infraestructura frente a posibles procesos de escaneo y detección de dispositivos. La verificación de las reglas en el tráfico de salida permitió validar el funcionamiento de las políticas configuradas y comprender la importancia de aplicar mecanismos de control basados en el principio de mínimo privilegio para reducir riesgos y fortalecer la seguridad de la red.

La implementación de reglas de acceso en Endian Firewall Community permitió controlar de manera eficiente el tráfico entre las zonas GREEN (LAN), ORANGE (DMZ) y RED (WAN), garantizando comunicaciones seguras y administradas dentro de la infraestructura de red. La configuración de políticas Inter-Zona y reglas NAT facilitó la habilitación controlada de los servicios HTTP y FTP, permitiendo validar la comunicación entre la LAN, la DMZ y la WAN mediante pruebas exitosas de conectividad.

Asimismo, la publicación de servicios en la DMZ evidenció la importancia de utilizar zonas desmilitarizadas para alojar servicios accesibles desde Internet sin comprometer directamente la seguridad de la red interna. Las pruebas realizadas mediante navegador web y herramientas de consola como curl, ftp y telnet permitieron comprobar el correcto funcionamiento de los servicios Apache y vsFTPd, así como la efectividad de las reglas configuradas en el firewall.

La verificación del tráfico Inter-Zona permitió evidenciar el funcionamiento adecuado de las políticas de acceso implementadas y la importancia de administrar el tráfico de red mediante reglas específicas basadas en protocolos, puertos y zonas de seguridad.

La implementación del Proxy HTTP no transparente en Endian Firewall Community permitió establecer mecanismos de control y monitoreo de la navegación web dentro de la red LAN mediante herramientas de código abierto y una administración centralizada desde la interfaz del firewall. La configuración de políticas de autenticación por usuario y grupo permitió restringir el acceso a contenidos específicos, aplicando listas negras para bloquear dominios definidos dentro de la infraestructura de red.

Asimismo, la correcta asignación de las interfaces a las zonas GREEN y RED fue fundamental para garantizar el funcionamiento adecuado del proxy y el control del tráfico HTTP. Las pruebas realizadas desde la LAN evidenciaron el correcto funcionamiento de las políticas de acceso y filtrado web implementadas.

El desarrollo integral de las diferentes temáticas permitió fortalecer los conocimientos relacionados con seguridad perimetral, segmentación de redes, configuración de servicios, políticas NAT, control de tráfico y administración de firewalls en entornos GNU/Linux. La implementación práctica de cada uno de los componentes evidenció la importancia de aplicar mecanismos de protección y control de acceso para garantizar comunicaciones seguras y una adecuada administración de infraestructuras tecnológicas empresariales.

6 REFERENCIAS

[1] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed. Pearson Education, 2018.

[2] W. R. Stevens, B. Fenner y A. M. Rudoff, *UNIX Network Programming*, 3rd ed. Upper Saddle River, NJ: Addison-Wesley, 2004.

[3] Jay LaCroix, *Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server*. Birmingham, UK: Packt Publishing, 2020.

[4] Debian Project, *Debian Administrator Manual*. Debian Documentation, 2023. [En línea]. Disponible en: https://www.debian.org/doc/

[5] Canonical, "Ubuntu Server Networking," Ubuntu Documentation, 2024. [En línea]. Disponible en: https://ubuntu.com/server/docs/networking

[6] Endian Firewall Community, "Endian Firewall Documentation," 2024. [En línea]. Disponible en: https://www.endian.com/community/

[7] Oracle Corporation, "Oracle VM VirtualBox User Manual," 2020. [En línea]. Disponible en: https://www.virtualbox.org/manual/

[8] Linux Professional Institute, “Linux Essentials,” LPI Learning Materials, 2022. [En línea]. Disponible en: https://learning.lpi.org/

[9] Squid Project, “Squid Proxy Cache,” 2024. [En línea]. Disponible en: http://www.squid-cache.org/

[10] OpenSSH Project, “OpenSSH Documentation,” 2024. [En línea]. Disponible en: https://www.openssh.com/manual.html