ENDIAN FIREWALL COMO SOLUCIÓN UTM: CONFIGURACIÓN DE ZONAS, NAT, FILTRADO DE SERVICIOS Y PROXY HTTP EN AMBIENTE VIRTUALIZADO

Alfonso González Posso
e-mail: agonzalezpo@unadvirtual.edu.co
Natalia Herrera Jara
e-mail: nherreraj@unadvirtual.edu.co
Jeison Alexander Castro Maestre
e-mail: jacastromae@unadvirtual.edu.co
Richard Duverney Rodriguez Corba
email:rdrodriguezcor@unadvirtual.edu.co
Jenny Rocio Castillo Castillo
email:jrcastilloc@unadvirtual.edu.co

RESUMEN: *Este trabajo presenta la implementación y configuración de Endian Firewall en VirtualBox, un firewall UTM de código abierto basado en GNU/Linux. Se configura una arquitectura de seguridad con tres zonas diferenciadas (verde, naranja y roja), implementando NAT para conectividad, reglas de firewall para control de tráfico inter-zonas, servicios HTTP/FTP con bloqueo ICMP, y un proxy HTTP no transparente con autenticación y filtrado de contenido. Se valida la funcionalidad de cada componente mediante pruebas de conectividad y acceso a servicios.*

PALABRAS CLAVE: Firewall, Endian, Segmentación de red, NAT, Proxy HTTP, Autenticación.

1 INTRODUCCIÓN

La seguridad en redes se ha convertido en un factor crítico en la infraestructura de tecnología de información de cualquier organización. Con la proliferación de amenazas cibernéticas y la creciente sofisticación de ataques dirigidos, implementar mecanismos robustos de defensa perimetral es esencial. Endian Firewall es una solución Unified Threat Management (UTM) de código abierto basada en GNU/Linux que integra múltiples capas de seguridad: firewall stateful, traducción de direcciones de red (NAT), servicios de proxy, detección de intrusiones y filtrado de contenido. Este trabajo presenta la implementación práctica de Endian Firewall en un entorno virtualizado, demostrando cómo configurar una arquitectura de red segmentada en tres zonas de seguridad diferenciadas y aplicar políticas de control granular de tráfico.

2 MARCO TEÓRICO

2.1 CONCEPTOS FUNDAMENTALES

La segmentación de redes es la práctica de dividir una red de área local en múltiples subredes, cada una actuando como su propio pequeño segmento de red. Esta estrategia proporciona:

- Reducción de riesgo: Limita el movimiento lateral de amenazas
- Control de tráfico: Permite políticas específicas por zona
- Aislamiento de servicios: Para usuarios de servidores críticos
- Cumplimiento normativo: Facilita auditorías de seguridad

2.1.1 ZONA DE SEGURIDAD EN LAS REDES

Las zonas de seguridad son agrupaciones lógicas de redes con el mismo nivel de confianza y requisitos de seguridad similares. En la arquitectura de tres zonas:

- Zona verde (LAN – local area network) que es una red interna confiable donde residen los usuarios finales y dispositivos de la organización. Se caracteriza por:
  - Acceso controlado a través de credenciales
  - Conexiones físicas dentro de instalaciones
  - Confianza media-alta
  - Requisito de aislamiento de zonas externas
- Zona naranja (DMZ – Demilitarized Zone) que es una zona intermedia desmilitarizada donde se ubican servidores que requieren acceso desde la zona roja (Internet) pero no deben comprometer la zona verde. Sus características incluyen:
  - Accesibilidad controlada desde Internet
  - Aislamiento completo de la LAN
  - Confianza baja-media
  - Acceso selectivo a Internet
- Zona roja (WAN – Wide Area Network)

Representa Internet, la red no confiable externa. Se define por:

- Acceso ilimitado e impredecible
- Origen de múltiples amenazas
- Confianza mínima
- Filtrado exhaustivo requerido

2.1.2 FIREWALL Y SUS FUNCIONES

Un firewall es un dispositivo o software que monitorea y controla el tráfico de red entrante y saliente basado en reglas de seguridad predeterminadas. Las funciones principales incluyen:

- **Filtrado de paquetes:** Análisis de cabeceras IP y puertos
- **Traducción de direcciones (NAT):** Enmascaramiento de direcciones IP internas
- **Inspección de estados (Stateful Inspection):** Seguimiento de conexiones activas
- **Protección perimetral:** Barrera entre redes confiables y no confiables

2.1.3 ENDIAN FIREWALL

Endian Firewall es una distribución de GNU/Linux especializada en seguridad perimetral. Características principales:

- **Código abierto:** Basado en Linux, permite modificaciones y auditoría
- **Multifunción:** Integra firewall, NAT, VPN, proxy, IDS y más
- **Interfaz web:** Panel de administración centralizado
- **Estable:** Versión Community Edition gratuita y completa
- **Arquitectura modular:** Permite habilitar solo servicios necesarios

2.1.4 VIRTUALIZACIÓN CON VIRTUALBOX

VirtualBox es un hipervisor de tipo 2 (hosted hypervisor) que permite ejecutar múltiples máquinas virtuales en un host. Su relevancia para este proyecto:

- **Flexibilidad:** Crear entornos de prueba sin hardware adicional
- **Aislamiento:** Las VMs no interfieren entre sí
- **Redes internas:** Crear redes de prueba aisladas del host
- **Accesibilidad:** Software de código abierto y gratuito

2.2 TEMATICA 1: CONFIGURACIÓN DE INSTANCIA GNU/LINUX ENDIAN FIREWALL EN VIRTUALBOX E INSTALACIÓN EFECTIVA

2.2.1 DISEÑO EXPERIMENTAL

La implementación sigue una metodología de cascada (waterfall) con las siguientes fases:

- **Planificación:** Definición de requisitos y arquitectura
- **Preparación:** Instalación de software base
- **Configuración:** Implementación del entorno de red
- **Validación:** Pruebas de funcionalidad
- **Documentación:** Registro de resultados

Como requisitos del sistema debemos tener un hardware mínimo y recomendamos los siguientes componentes:

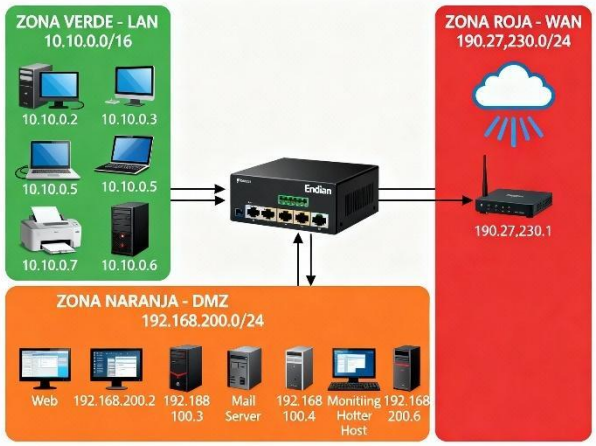
- **Procesador**: Intel i5 o equivalente con tecnología de virtualización habilitada
- **RAM**: 8 GB (4 GB para VirtualBox, 2-4 GB para Endian, 2 GB para cliente)
- **Almacenamiento**: 50 GB libre (10 GB para host, 20 GB para Endian, 10 GB para cliente)
- **Conectividad**: Acceso a Internet

Y como software requerido mínimo proponemos estos componentes:

- VirtualBox 6.1 o superior
- ISO de Endian Firewall Community Edition (descargable gratuitamente)
- Imagen de SO cliente (Ubuntu 20.04 LTS o similar)
- Herramientas de diagnóstico (ping, tracert, navegadores web)

2.2.2 ARQUITECTURA DE IMPLEMENTACIÓN

Figura 1. Arquitectura de implementación

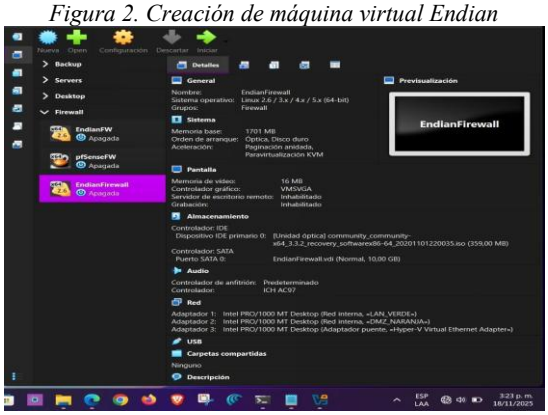


Fuente: Autoría Propia.

En nuestro equipo determinamos una infraestructura en Firewall Endian UTM. Como se ve en la figura 1. Y vamos a explicar el procedimiento paso a paso de nuestra infraestructura.

2.2.3 FASE 1: CONFIGURACIÓN DE VIRTUALBOX

Figura 2. Creación de máquina virtual Endian



Fuente: Autoría Propia.

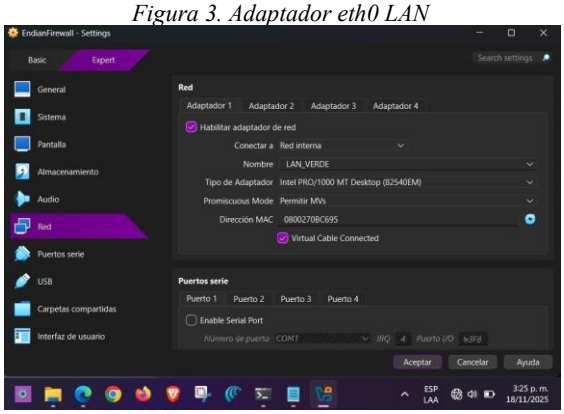
Creación de los requisitos previos y montaje de la iso Endian para su instalación y puesta en marcha en VirtualBox.

2.2.4 FASE 2: CONFIGURACIÓN DE REDES

Se crean tres redes en VirtualBox

-

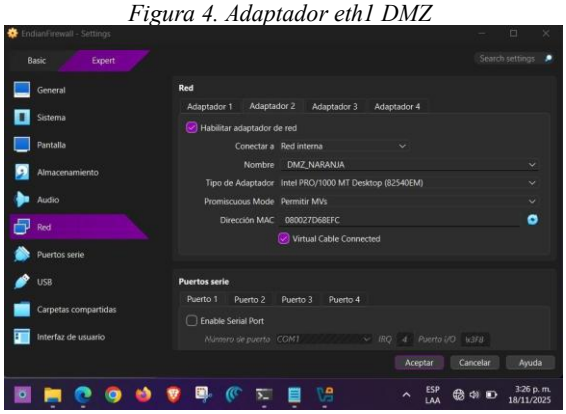
Figura 3. Adaptador eth0 LAN



Fuente: Autoría Propia.

Configuración de adaptador eth0 en VirtualBox como red interna y en nombre se le agrega LAN_VERDE para mayor claridad.

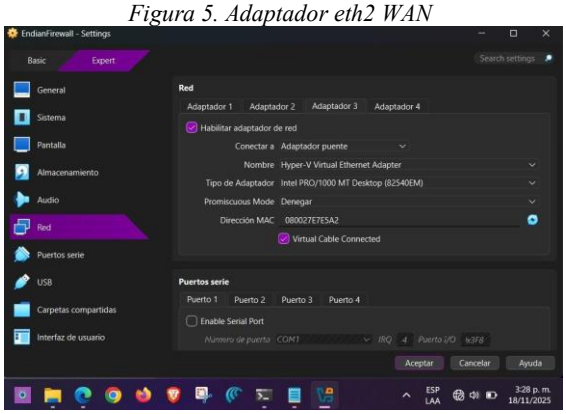
Figura 4. Adaptador eth1 DMZ



Fuente: Autoría Propia.

Configuración de adaptador eth1 en VirtualBox como red interna y en nombre se le agrega DZM_NARANJA para mayor claridad.

Figura 5. Adaptador eth2 WAN

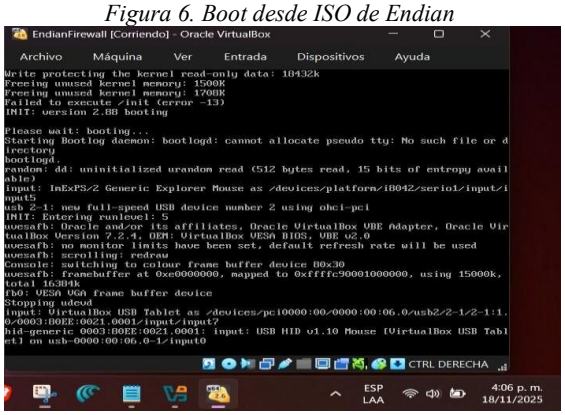


Fuente: Autoría Propia.

Configuración de adaptador eth2 en VirtualBox como adaptador puente que para este caso será las veces de nuestro proveedor de internet ISP por el cual vamos a salir a navegar, seria nuestra IP pública.

2.2.5 FASE 3: INSTALACIÓN DE ENDIAN FIREWALL

Figura 6. Boot desde ISO de Endian



Fuente: Autoría Propia.

Proceso de carga de la iso Endian para su instalación.

Figura 7. Seleccionar lenguaje

Fuente: Autoría Propia.

Se selecciona lenguaje por el cual el equipo va a reconocer la distribución del teclado.

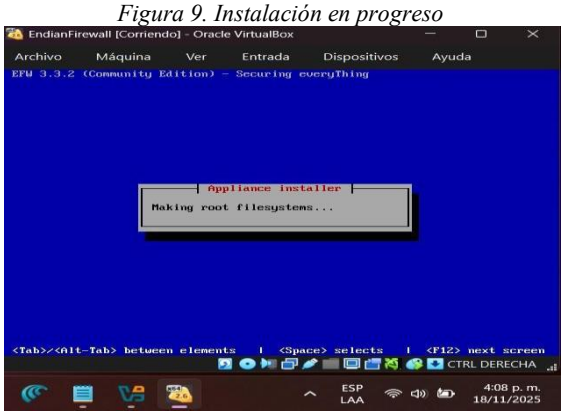
Figura 8. Aceptar particionado automático

Fuente: Autoría Propia.

-

Proceso de selección para aceptar las particiones de forma automática propuesta por Endian.

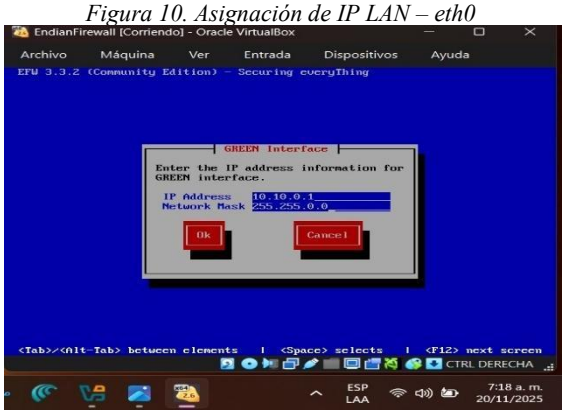
Figura 9. Instalación en progreso



Fuente: Autoría Propia.

Instalando máquina, realizando particionado e instalación de las aplicaciones o núcleo de Endian.

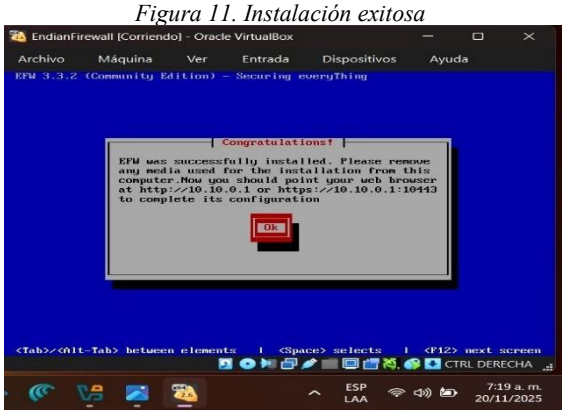
Figura 10. Asignación de IP LAN – eth0



Fuente: Autoría Propia.

Asignación manual de la IP red Verde o eth0 por la cual nos vamos a poder conectar a Endian.

Figura 11. Instalación exitosa

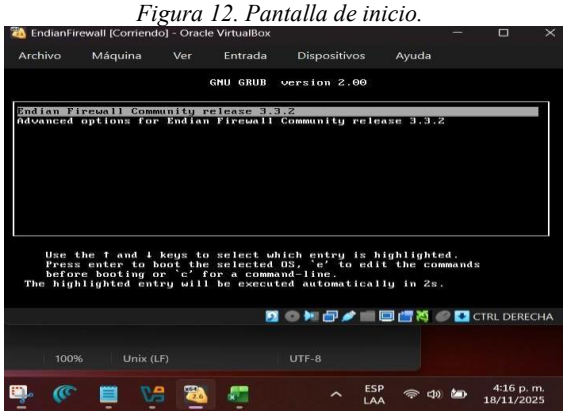


Fuente: Autoría Propia.

-

Notificación de instalación exitosa y nos muestra la IP para conectarnos vis web o por su interfaz web (GUI).

Figura 12. Pantalla de inicio.

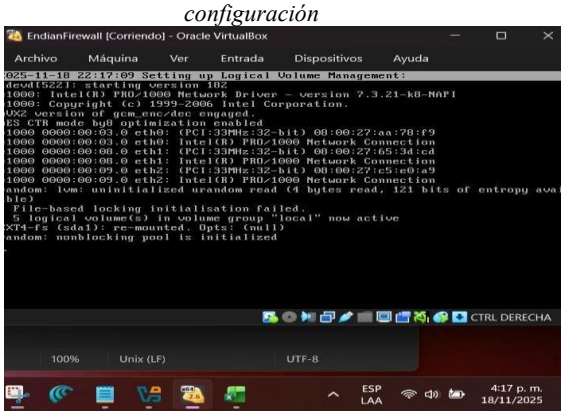


Fuente: Autoría Propia.

Ya instalado Endian nos muestra su pantalla de inicio o carga de Endian UTM Core.

2.2.6 FASE 4: CONFIGURACIÓN INICIAL DE ENDIAN

Figura 13. El asistente detecta las interfaces y solicita configuración



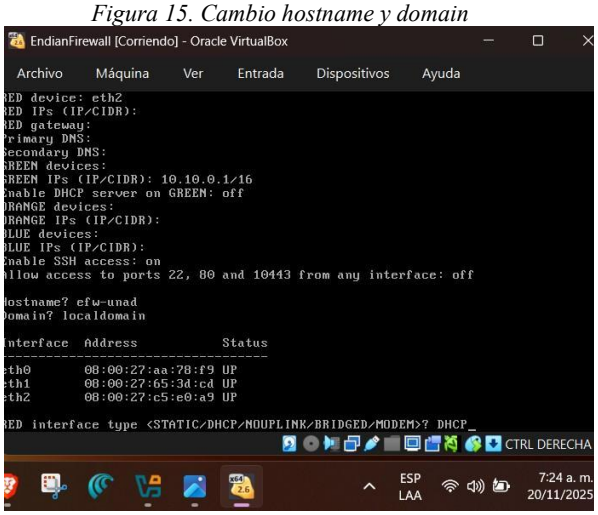
Fuente: Autoría Propia.

Figura 14. Cambio password user root

Fuente: Autoría Propia.

Proceso de campo de clave para user root y admin, los cuales se realizan de forma exitosa desde la terminal o por su interfaz web.

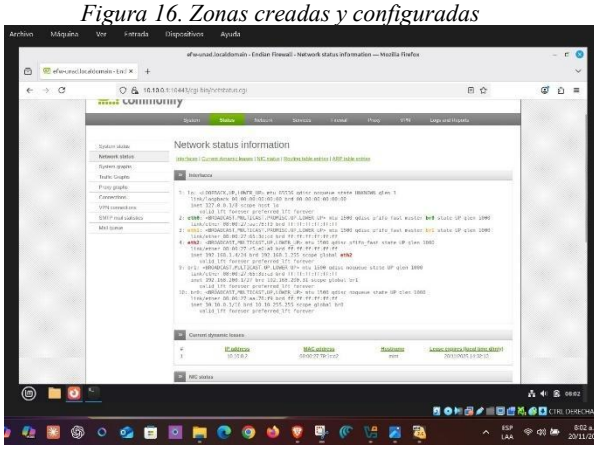
Figura 15. Cambio hostname y domain



Fuente: Autoría Propia.

Proceso de campo de hostname y domain, los cuales se realizan de forma exitosa desde la terminal o por su interfaz web.

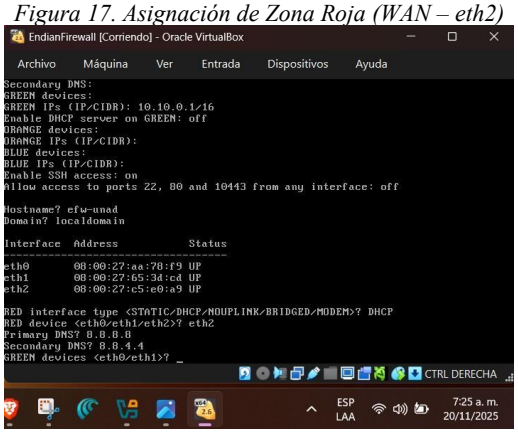
Figura 16. Zonas creadas y configuradas



Fuente: Autoría Propia.

Correcta implementación de las configuraciones de las zonas VERDE, NARANJA y WAN.

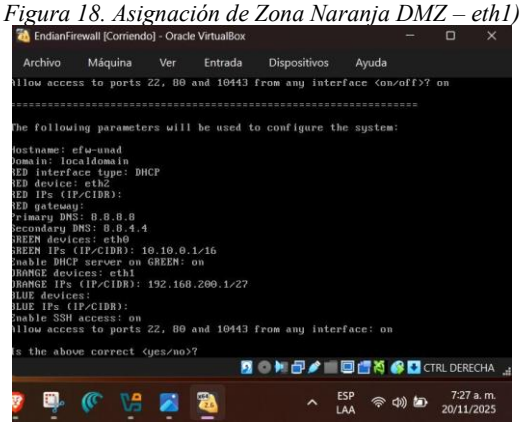
Figura 17. Asignación de Zona Roja (WAN – eth2)



Fuente: Autoría Propia.

Proceso de asignación de la zona WAN adaptador eth2 y su configuración para poder salir a internet.

Figura 18. Asignación de Zona Naranja DMZ – eth1)



Fuente: Autoría Propia.

Proceso de asignación de la zona DMZ adaptador eth1 y su configuración para poder tener un control total y segmentar la red.

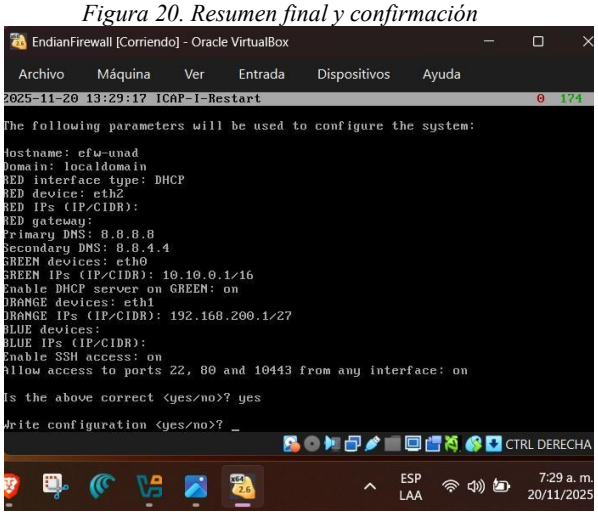
Figura 19. Asignación de Zona Verde (LAN – eth0)

Fuente: Autoría Propia.

-

Proceso de asignación de la zona LAN adaptador eth0 y su configuración para poder tener un control total y segmentar la red local.

Figura 20. Resumen final y confirmación

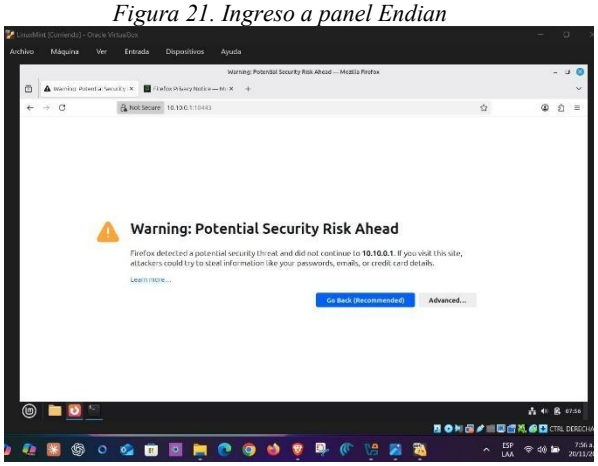


Fuente: Autoría Propia.

Resumen y confirmación de la configuración los cuales aceptamos y escribimos para poder ingresar a la interfaz web de Endian.

2.2.7 FASE 5: CONFIGURACIÓN Y SERVICIOS

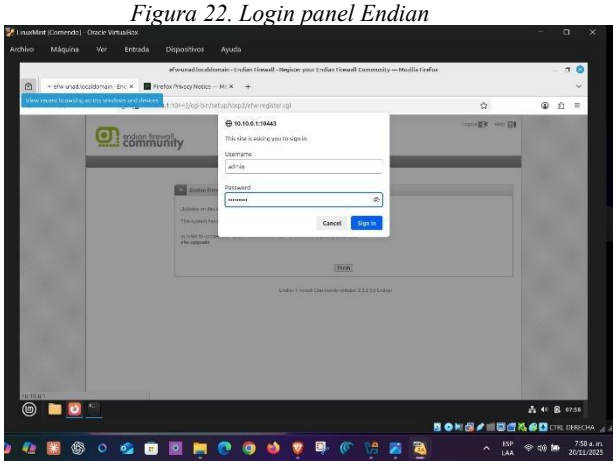
Figura 21. Ingreso a panel Endian



Fuente: Autoría Propia.

Ingresamos a su interfaz web o panal de administración web, la cual muestra una advertencia porque el certificado no es 100% comprobado, los cuales debemos aceptar y continuar.

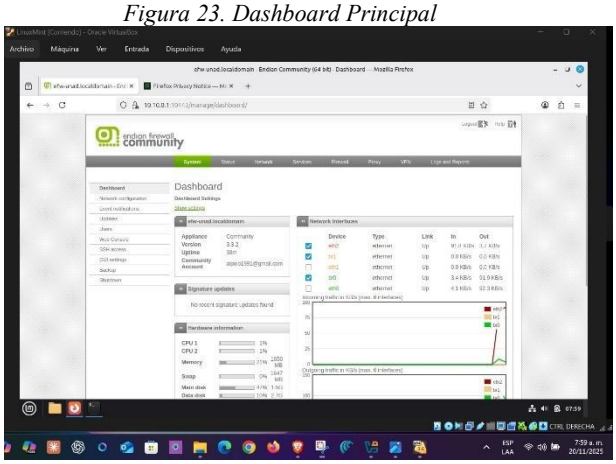
Figura 22. Login panel Endian



Fuente: Autoría Propia.

Ya aceptando la advertencia, continuamos y nos pide ingresar user y password, los cuales configuramos anterior mente.

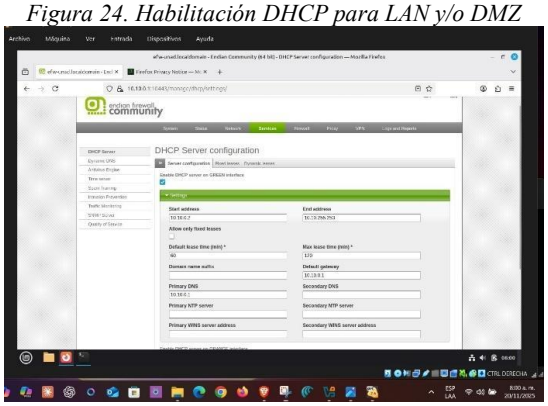
Figura 23. Dashboard Principal



Fuente: Autoría Propia.

Pantalla de inicio principal donde realizamos todas nuestras configuraciones en Endian Firewall, ten en cuenta que también se puede realizar por terminal.

Figura 24. Habilitación DHCP para LAN y/o DMZ



Fuente: Autoría Propia.

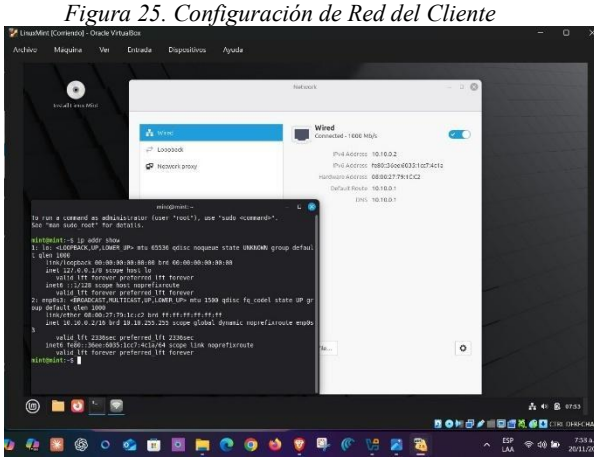
-

En la configuración inicial se realiza o habilita servidor DHCP el cual confirmamos y se encuentran correctamente configurado y funcional, cabe recalcar que también se puede habilitar para la zonas naranja y azul.

2.2.8 FASE 6: VALIDACIÓN Y PRUEBAS

Desde máquina cliente en zona verde:

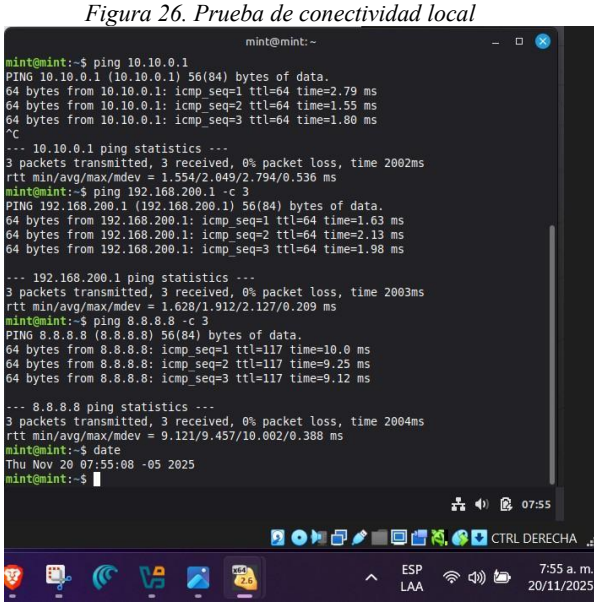
Figura 25. Configuración de Red del Cliente



Fuente: Autoría Propia.

Nos conectamos desde nuestro pc cliente a la red LAN y validamos la IP asignada por Endian, las cuales se encuentran dentro de lo establecido.

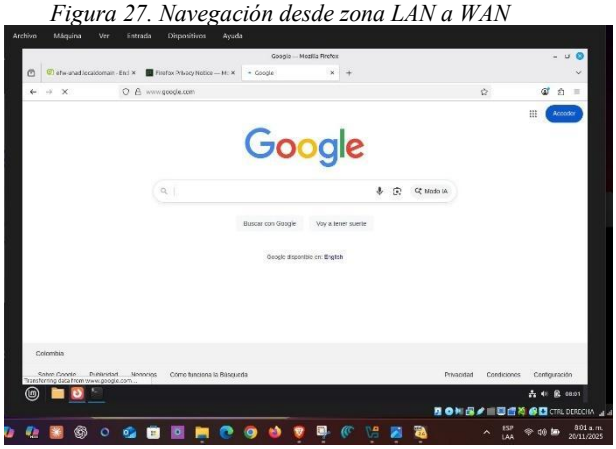
Figura 26. Prueba de conectividad local



Fuente: Autoría Propia.

Se realizan pruebas de conectividad por medio de la terminal realizando ping desde el pc cliente a las diferentes zonas configuradas en Endian, somo se observa tenemos respuesta las cuales están funcionando correctamente.

Figura 27. Navegación desde zona LAN a WAN



Fuente: Autoría Propia.

Validamos salida a internet desde nuestro pc cliente conectado a la red/zona LAN de Endian.

Figura 28. Segmentación de IP por zonas

Fuente: Autoría Propia.

Distribución de IP por zonas para mayor performance y administración, los cuales nos brinda un total control.

2.3 TEMÁTICA 2 – CONFIGURACIÓN NAT

2.3.1 FUNDAMENTOS TEÓRICOS Y ARQUITECTURA DE RED

El diseño de seguridad perimetral implementa tres zonas de confianza mediante GNU / Linux Endian Firewall 3.3.2. La segmentación de basa en el framework netfilter del kernel de Linux, donde los iptables actúa como interfaz de configuración para la manipulación de paquetes en las cadenas PREROUTING, POSTROUTING Y FORWARD.

2.3.2 PRINCIPIOS DE SEGMENTACIÓN DE RED EN ENDIAN UTM

Endian firewall 3.3.2 es una distribucción UTM (Unified Threat Management) la cual está basada en Linux, que orquesta netfilter a través de un sistema de plantillas de configuración, pero que permite la intervención directa en iptables para reglas avanzadas; por consiguiente, la arquitectura implementa tres zonas de confianza mediante la asignación de interfaces al framework netfilter del kernel Linux: Zona Verde (LAN interna), Zona Naranja (DMZ) y Zona Roja (WAN). A diferencia de firewalls de alto nivel (firewalld, ufw), trabajar directamente con iptables en Endian ofrece control granular sobre la cadena PREROUTING, FORWARD Y POSTROUTING, sin abstracciones que oculten el flujo de paquetes.

Nota: Este trabajo no utiliza framework de gestión (firewalld, nftables, ufw). Todas las reglas se insertan a través de iptables en modo consola, con el fin de garantizar la

-

trazabilidad forense, además de la comprensión del procesamiento de los paquetes.

2.3.3 DISEÑO EXPERIMENTAL DE TOPOLOGÍA

La arquitectura de máquinas virtuales en virtualbox. Debemos tener en cuenta que el siguiente escenario aísla el perímetro en red NAT/Red Interna de VirtualBox, evitando puentes entre interfaces físicas.

Figura 29: tabla de distribución de las zonas en el Endian Firewall

Función	Sistema Operativo	Interfaz	IP/Zona	Servicio de Validación
Firewall UTM	Endian Firewall 3.3.2	eth0	10.10.0.1/16 (Zona Verde)	iptables, conntrack
		eth1	192.168.200.1/24 (Zona Naranja)	
		eth2	10.0.4.15/24 (Zona Roja)	
Cliente LAN	Ubuntu Desktop 24.04	enp0s3	10.10.0.2/16	ping, curl, netcat
Servidor DMZ	Ubuntu Server 24.04	enp0s3	192.168.200.2/24	nginx(puerto 80), tcpdump
Pruebas WAN	Linux Mint 21.3	enp0s3	10.255.0.15/24	curl, netcat, tcpdump

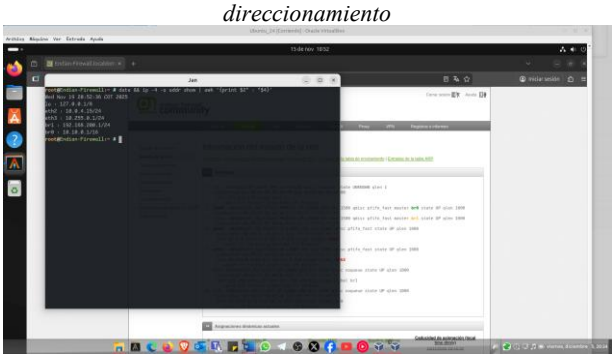
Fuente: Autoría Propia.

Justificación de servicios: nginx en DMZ permite probar DNAT HTTP real con respuesta del servidor web. Netcat (nc) en nodos cliente/WAN valida conectividad TCP sin capa de aplicación, lo que aísla problemas de NAT de errores de servicio.

2.3.4 IMPLEMENTACIÓN DE SNAT PARA ZONA VERDE (LAN - WAN)

Validación previa con el fin de evitar errores que invaliden reglas NAT:

Figura 30: Verificación en vivo de interfaces y direccionamiento



Fuente: Autoría propia.

Propósito de seguridad: El timestamp (date) asegura la trazabilidad forense. El filtrado awk expone IPs asignadas, reduciendo la superficie de información sensible en auditorias.

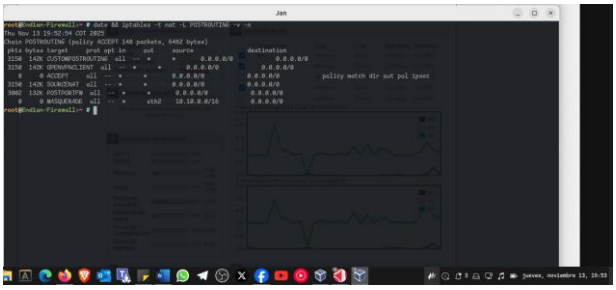
2.3.5 REGLA SNAT PARA OCULTACIÓN DE RED PRIVADA

Figura 31: Creación de regla POSROUTING para LAN-WAN

-

Fuente: Autoría propia.

Figura 32: Verificación de la regla creada



Fuente: Autoría propia.

Explicación detallada (Modo consola directo)

- -t nat: Tabla de traducción. A diferencia de firewalld, que oculta esta separación, usar iptables directamente expone que NAT y filtrado son procesos independientes, lo que optimiza el rendimiento.

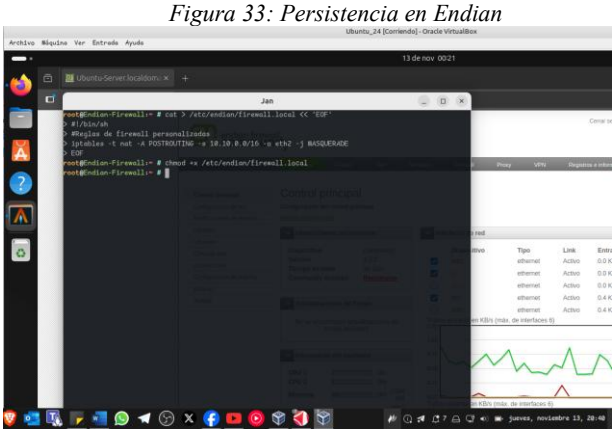
- -A POSTROUTING: Añade cadena a POSTROUTING. Endian genera reglas en /etc/shorewall/rules, pero insertar manualmente permite precedencia exacta y depuración sin sobrescritura por la GUI.

- -s 10.10.0.0/16: Fuente LAN. Si se usara una máscara de /24, ocultaría fallos de diseño. La máscara de /16 documenta la intensión de la escalabilidad.

- -o eth2: Crítico en Endian. La interfaz de red enp0s3 es la única con gateway. Omitir la opción -o, aplicaría NAT incluso al tráfico LAN-DMZ, rompiendo logs de conexión en el servidor DMZ al ocultar IPs de origen.

- -j MASQUERADE: Propósito de seguridad. MASQUERADE consulta IP de eth0 dinamicamente. Si Endian obtiene por IPCP WAN, la traducción persiste sin reconfiguración, evitando outages causados por scripts de Endian que asumen IP estática.

Figura 33: Persistencia en Endian



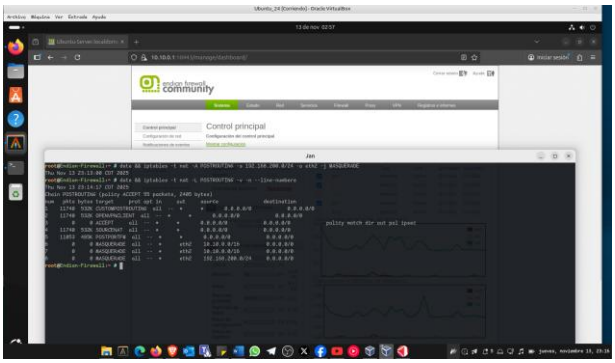
Fuente: Autoría propia.

Propósito: /etc/endian/firewall.local ejecuta después de que Endia carga reglas GUI. Esto garantiza que reglas manualmente debuggeadas no sean sobrescritas por actualizaciones del sistema. chmod +x es obligatorio: reglas sin permisos son ignoradas silenciosamente, creando falsa sensación de seguridad.

2.3.6 IMPLEMENTACIÓN DE SNAT PARA ZONA NARANJA (DMZ-WAN)

Segregación intencional de Zonas: esta regla replica la lógica LAN pero para DMZ.

Figura 34: Segregación intencional de Zonas



Fuente: Autoría propia.

Crítico: No hay NAT entre DMZ y LAN. Si el servidor DMZ (192.168.200.2) accede a 10.10.0.0, el firewall ve la IP real, permitiendo:

- Logs forenses detallados: Se sabe exactamente qué host DMZ atacó LAN.
- Políticas FORWARD específicas: iptables -A FORWARD -s 192.168.200.2 -d 10.10.0.0/16 -p tcp –dport 443 -j ACCEPT permite solo HTTPS a LAN.
- Sin NAT: La IP origen se mantiene, imposible conMASQUERADE global.

2.3.7 IMPLEMENTACIÓN DE DNAT: PUBLICACIÓN CONTROLADA DE SERVICIOS

Para realizar una redirección de puertos http (WAN-DMZ) debemos tener en cuenta los siguientes criterios de seguridad

- -i eth2: Imprescindible. Limita a tráfico WAN. En Endian, si se omite, usuarios LAN podrían acceder a http://10.10.0.1:8080 y ser redirigidos al servidor DMZ, violando segregación y creando vector de ataque lateral.

- --dport 8080: Principio de reducción de superficie de ataque. Publicar en puerto no estándar (8080) reduce escaneos de bots. No es seguridad por oscuridad, sino filtro de ruido. Nginx en DMZ sigue escuchando en puerto 80, simplificando su configuración.

- --to-destination 192.168.200.2:8080: Separación de exposición pública de configuración interna. El firewall expone 8080; nginx no necesita cambios.

-

Propósito de seguridad: DNAT solo traduce; no filtra. Sin regla FORWARD, el paquete bloquea por política DROP, pero el log muestra IP traducida (192.168.200.2), no IP WAN de origen. La regla explícita permite logging detallado con –log-prefix “DNAT-HTTP: ” para identificar IPs atacantes reales en intentos de explotación de Nginx.

2.3.8 CONFIGURACIÓN DE NODO WAN SIMULADA (Linux Mint)

Configuración estática en /etc/network/interfaces
auto enp0s3
iface enp0s3 inet static
address 10.255.0.10
netmask 255.255.255.0
gateway 10.255.0.1
dns-nameservers 8.8.8.8 8.8.4.4

Propósito de seguridad: La IP 10.255.0.10 simula un atacante externo. Usar red RFC1918 aísla el laboratorio de internet real, evitando filtrado accidental de paquetes. Gateway 10.255.0.1 es la IP es la IP virtual que el firewall usa para simular un router ISP.

- curl: Valida respuestas HTTP real en nginx (encabezados, códigos 200).

- netcat-openbsd: Versión BSD, permite -zv con timeout más preciso que GNU netcat.

- tcpdump: Captura tráfico en interfaz física para validar traducción.

2.3.9 VALIDACIÓN DE CONECTIVIDAD CON NETCAT

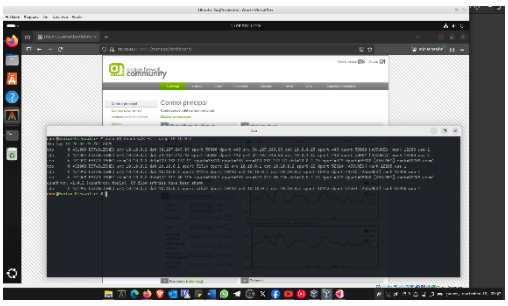
Desde Linux Mint (WAN):

$$date \;\&\&\; nc - zv - w\ 3\ 10.255.0.1\ 8080 \qquad (1)$$

Ventajas de netcat: -zv realiza TCP handshake sin enviar datos de aplicación. Si la conexión falla, descarta problemas de nginx y aísla fallo en NAT o FORWARD. Es la herramienta preferida para validar capa de transporte sin interferencia de capa de aplicación.

2.3.10 VERIFICACIÓN FORENSE DE CONEXIONES NAT

Figura 35: Validación de traducción snat



Fuente: Autoría propia.

Propósito de seguridad: conntrack muestra conexión bidireccional mantenida por netfilter.

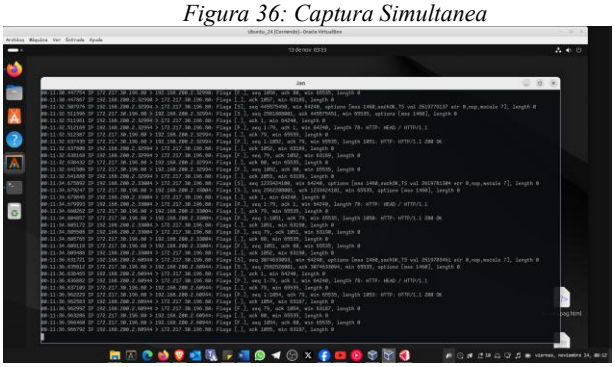
- Debugging: Si la traducción falla, la tabla está vacía, indicando problema en POSTROUTING.

- Auditoría: Detecta conexiones anómalas (host interno a puerto 25 = posible malware spam).

- Statefulnesss: ASSURED indica tráfico de retorno reconocido, evitando filtrado de respuestas legítimas.

2.3.11 CAPTURA SIMULTÁNEA PARA DNAT HTTP

Figura 36: Captura Simultanea

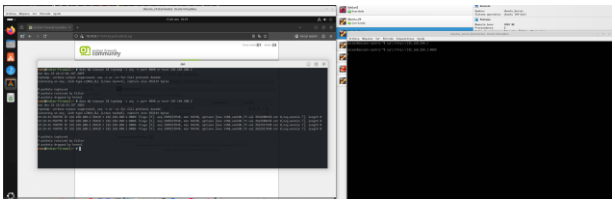


Fuente: Autoría propia.

Figura 37: Captura de tráfico en nodo 1 WAN prueba

Fuente: Autoría propia.

Figura 38: Captura de tráfico en nodo 2 WAN prueba



Fuente: Autoría propia.

Funcionamiento forense:

- En WAN: tcpdump debe mostrar 10.255.0.10 → 10.255.0.1:8080 Si no hay tráfico, problema de enrutamiento previo al firewall.

-

- En Firewall: tcpdump -i any -n debe mostrar traducción: 10.255.0.10 → 192.168.200.2:80. Ausencia de traducción = falla PREROUTING. Presencia de RST o ICMP Port Unreachable = problema FORDWARE o nginx caído.

Propósito de seguridad: Captura simultánea válida que DNAT no expone IPs internas. Si tcpdump en WAN mostrara 192.,168.200.2, habría fuga de información (IP spoofing interno visible desde el exterior).

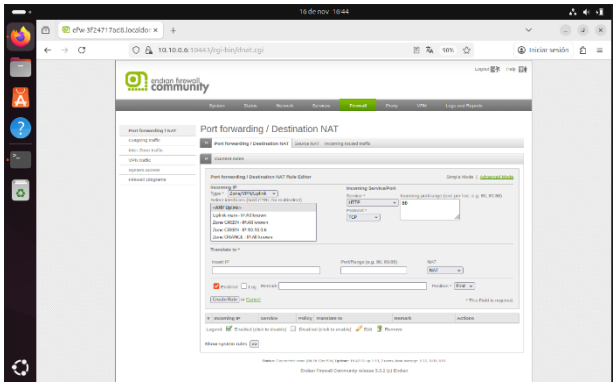
2.4 TEMÁTICA 3 - PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

2.4.1 PERMITIR LOS SERVICIOS HTTP (PUERTO 80) Y FTP (PUERTO 21)

En el ámbito de la seguridad informática, una de las estrategias más utilizadas es la implementación de una DMZ (Zona Desmilitarizada), que actúa como una barrera adicional entre la red interna (LAN) y el exterior (Internet). La DMZ permite exponer servicios públicos, como servidores web y FTP, sin comprometer la seguridad de la red interna, ya que los accesos y las reglas de comunicación se gestionan de manera estricta y controlada.

Su función principal es alojar servicios que deben ser accesibles desde Internet, como páginas web, servidores de correo electrónico, o servidores FTP. Al ubicar estos servicios en la DMZ, se reduce el riesgo de que un atacante que comprometa uno de estos servidores pueda acceder directamente a la red interna, donde se encuentran los recursos más sensibles.

Figura 39: Configuración de puertos en Endian para el servicio HTTP.

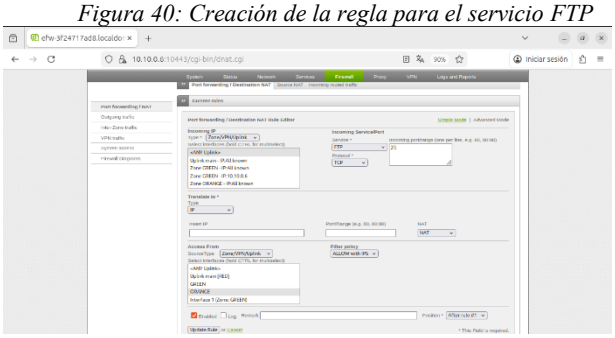


Fuente: Autoría propia

Por eso usamos Endian Firewall, una solución robusta y flexible para la gestión de reglas de seguridad en redes. En este escenario, contamos con dos redes principales: la red verde (interna) y la red naranja (DMZ), además de la red roja (Internet). Y tenemos tres máquinas virtuales: un servidor Ubuntu (DMZ), un cliente Desktop (LAN) y Endian Firewall (controlador central).

El primer paso es ingresar a Endian como en la figura 1 lo puedes encontrar en la opción Firewall y buscamos la opción Port Forwarding / Destination NAT y creamos una regla para permitir el servicio HTTP con el Protocolo TCP en el puerto 80, como en la figura 1 permitimos que el protocolo se permita desde cualquier red (Verde, Naranja o roja) para que toda nuestra infraestructura tenga acceso a internet.

Figura 40: Creación de la regla para el servicio FTP



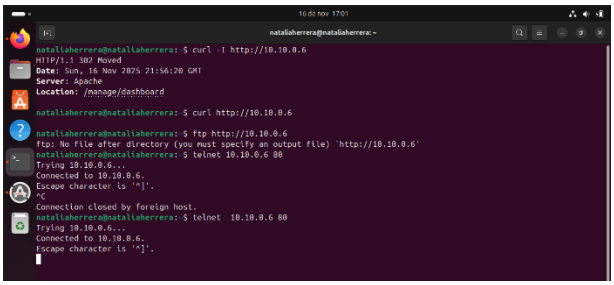
Fuente: Autoría propia.

Realizamos lo mismo para el servicio FTP, creamos una regla nueva en nuestro Endian en la configuración de puertos. En la red que la va a utilizar usaremos cualquiera y luego en servicio seleccionaremos el FTP con el protocolo TCP a través del puerto 21 como en la figura 40.

Limitar los servicios expuestos es una medida clave para reducir la superficie de ataque y facilitar el monitoreo de la red.

Para comprobar que la red quedo configurada correctamente validamos desde la terminal telnet 10.0.0.6 80 para validar la conexión al servicio HTTP en el puerto 80 en el servidor. Como responde que está conectado correctamente quiere decir que la regla fue configurada correctamente como se ve en la figura 3. Para comprobar lo mismo con el servicio FTP usamos el mismo comando pero con el puerto 21 y debe también tener la misma respuesta para comprobar que podamos tener la conexión correcta.

Figura 41: Comprobación de los puertos desde la red verde.



Fuente: Autoría propia.

Una vez finalizada la configuración de los puertos para los servicios HTTP y FTP, se logra centralizar el acceso web y la transferencia de archivos en servidores ubicados en zonas aisladas. Esta medida contribuye significativamente a reducir la superficie de ataque, facilita el cumplimiento de las políticas de segmentación de la red y optimiza el monitoreo de la infraestructura. En conjunto, esta estrategia no solo refuerza la protección de los sistemas, sino que también garantiza la prestación de servicios confiables sin poner en riesgo la integridad de la red interna.

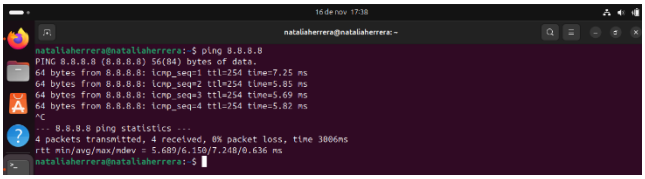
2.4.2 DENEGAR EL PROTOCOLO ICMP (PUERTO 8 Y PUERTO 30) PARA NO PERMITIR HACER PING EN LA RED.

El protocolo ICMP (Internet Control Message Protocol) se utiliza comúnmente para realizar pruebas de conectividad, como el comando “ping”. Sin embargo, ICMP también puede ser explotado en ataques de red, como el smurf o el ping flood, que buscan saturar la red con paquetes ICMP y provocar denegaciones de servicio.

Por esta razón, una buena práctica de seguridad es bloquear el tráfico ICMP, especialmente entre la red interna y el exterior, para evitar que los atacantes puedan mapear la red, identificar dispositivos activos o lanzar ataques [1].

Desde nuestra máquina virtual Ubuntu Desktop primero comprobamos que podamos hacer ping a internet con el comando: ping 8.8.8.8 como la figura 42.

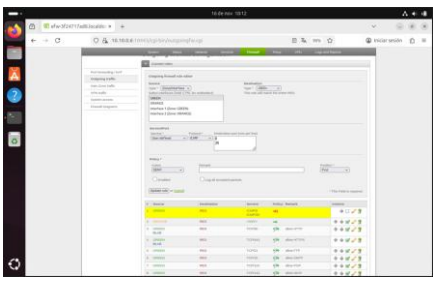
Figura 42: Ping a internet.



Fuente: Autoría propia.

Para llevar a cabo el bloqueo del protocolo ICMP, es necesario acceder al apartado de firewall y seleccionar la opción “Outgoing traffic”. A continuación, se crea una nueva regla en la que se establece la red verde como origen y la red roja como destino. En el campo de servicio, se selecciona la opción definida por el usuario, especificando el protocolo ICMP y configurando los puertos 8 y 30. La acción de la regla debe ser “denegar”, lo que impedirá la realización de pruebas de conectividad (ping) desde la red verde hacia la red roja.

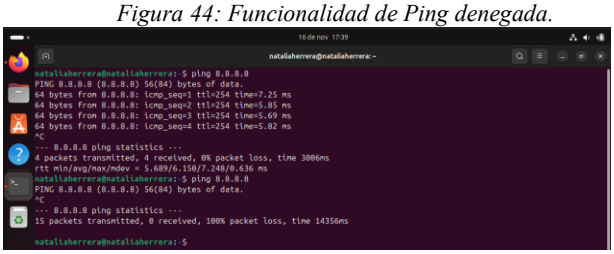
Figura 43: Configuración del servicio del servicio ICMP



Fuente: Autoría Propia.

De este modo, no será posible enviar paquetes ICMP mediante el comando ping desde el cliente (Ubuntu Server), evitando que posibles atacantes puedan utilizar esta funcionalidad para mapear la red y detectar dispositivos activos. Para comprobarlo realizamos el ping de nuevo y debe verse como en la figura 44.

Figura 44: Funcionalidad de Ping denegada.



Fuente: Autoría propia

La implementación de esta regla permite bloquear el protocolo ICMP dentro de la red, lo cual constituye una medida fundamental para fortalecer la seguridad y disminuir la superficie de ataque. El protocolo ICMP, comúnmente utilizado para realizar pruebas de conectividad mediante el comando ping, puede ser aprovechado por atacantes para mapear la red, identificar dispositivos activos y ejecutar ataques de denegación de servicio. Al restringir el tráfico ICMP hacia zonas críticas o hacia Internet, se evita la exposición innecesaria de información sobre la infraestructura y se mitigan los riesgos asociados a posibles ataques.

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

2.5.1 CONFIGURACIÓN DE REGLAS INTERZONAL

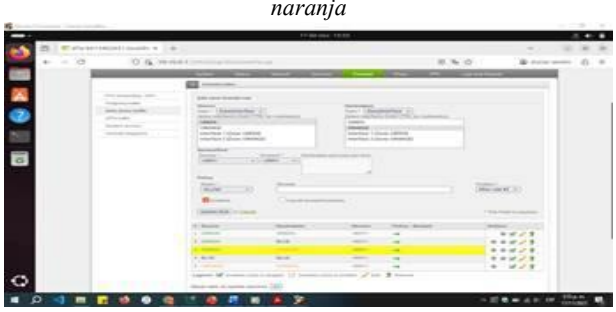
Se implementaron reglas de comunicación entre la zona verde y la zona naranja de forma controlada para servicios HTTP (puerto 80) y FTP (puerto 21), permitiendo únicamente tráfico requerido para el acceso a servidores ubicados en la DMZ.

Figura 45. Reglas establecidas por defecto

Fuente: Autoría propia.

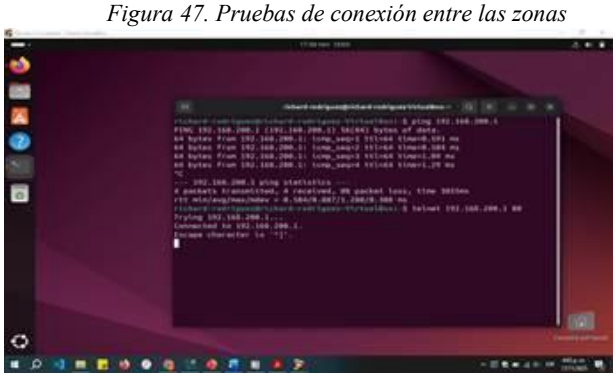
-

Figura 46. Configuración de regla zona Verde y la zona naranja



Fuente: Autoría propia.

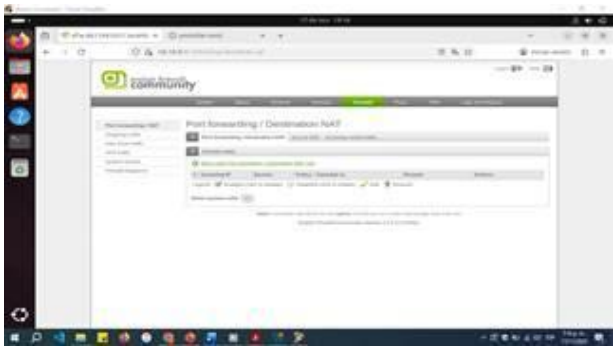
Figura 47. Pruebas de conexión entre las zonas



Fuente: Autoría propia.

A continuación, se accedió a la interfaz web de administración de Endian con el fin de configurar las reglas de firewall necesarias para permitir el tráfico requerido entre las zonas definidas.

Figura 48. Creación de usuario y grupo dentro del Firewall



Fuente: Autoría propia.

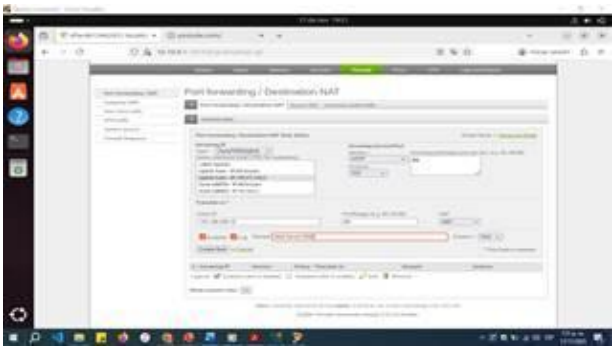
Se ingresó a la sección Firewall y posteriormente a la opción Port Forwarding / Destination NAT, con el propósito de crear las reglas necesarias para el direccionamiento de tráfico hacia los servicios configurados dentro del firewall.

Figura 49. Configuración de regla HTTP (Web Server)

Fuente: Autoría propia.

Se procedió a crear una regla que permita a los usuarios provenientes de Internet acceder a un servicio público alojado en la zona DMZ. Para ello, se configuró una dirección IP externa (190.27.230.2) y se definieron los servicios HTTP y FTP mediante los puertos 80 y 21, respectivamente, redireccionando el tráfico hacia el servidor interno ubicado en la DMZ con dirección IP 192.168.200.10.

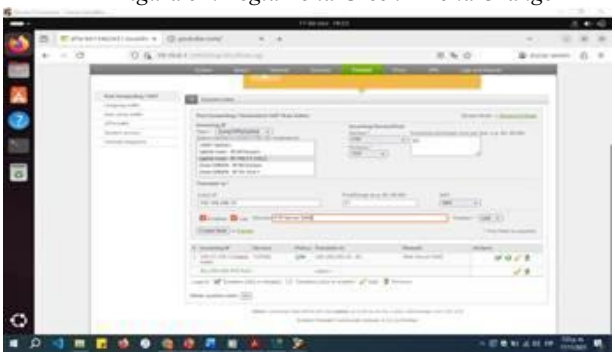
Figura 50. Regla Zona Red – Zona Orange



Fuente: Autoría propia.

De forma complementaria, se configuró una segunda regla que permite a los usuarios de la red interna (LAN) acceder a los servicios web y FTP alojados en la DMZ. Para ello, se estableció como dirección de origen la red 10.10.0.0 y como destino la red 192.168.200.0, habilitando los servicios HTTP y FTP mediante los puertos 80 y 21, respectivamente.

Figura 51. Regla Zona Green – Zona Orange



Fuente: Autoría propia.

-

Figura 52. Pruebas de conexión Servidor HTTP

Fuente: Autoría propia.

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

2.6.1 CREACIÓN DEL PERFIL DE BLOQUEO

Se configuró un perfil de filtrado dentro del proxy HTTP, bloqueando sitios mediante lista negra (Hotmail, YouTube y El Nuevo Día). Con ello, el firewall impidió el acceso al contenido especificado.

Figura 53. Regla Zona Red – Zona Orange

Fuente: Autoría propia.

Se accedió a la sección de listas negras y blancas personalizadas, donde se habilitó la opción de bloqueo de sitios específicos. En este apartado se ingresaron las direcciones URL correspondientes a los portales que se requería restringir, y posteriormente se aplicaron los cambios para activar la política de filtrado.

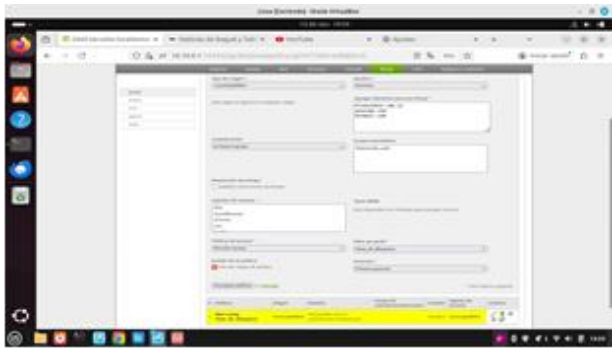
Una vez aplicados los cambios, el sistema confirmó correctamente la actualización de la configuración. Posteriormente, se ingresó a la pestaña de Políticas de acceso, donde se procedió a modificar la política previamente establecida con el fin de asociarla al perfil de filtrado configurado.

Figura 54. Políticas de acceso

Fuente: Autoría propia.

Dentro de la política seleccionada se accedió al apartado de Permisos de acceso, en el cual se habilitó la opción Permitir acceso con el objetivo de activar la configuración del filtro de permisos. Una vez visible dicha función, se seleccionó el perfil correspondiente a la lista de bloqueos previamente creada. Finalmente, se guardaron y aplicaron los cambios para que la política surtiera efecto en el proxy.

Figura 55. Configuración de permisos de acceso



Fuente: Autoría propia.

Una vez aplicados los cambios, se procedió a acceder nuevamente a los sitios previamente configurados en la lista de bloqueo, verificando que el sistema denegó correctamente el acceso a dichos portales, evidenciando la efectividad de la política aplicada en el proxy.

Figura 56. Acceso a página bloqueada

Fuente: Autoría propia.

-

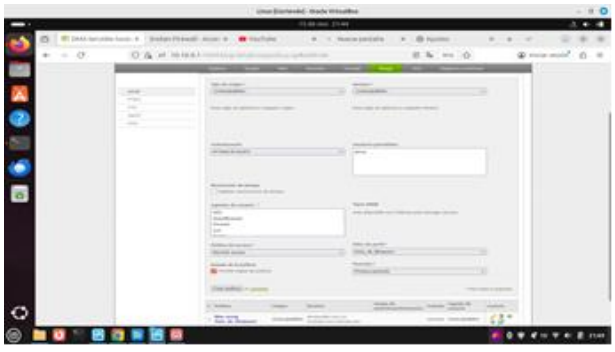
En la fase de autenticación por usuario, se procedió a crear una cuenta desde la sección de Proxy, asociándose posteriormente a un grupo específico. Para ello, se accedió a la pestaña Autenticación, ingresando a la opción de administración de usuarios mediante el módulo NCSA User Management. Una vez creado el usuario, este se vinculó al grupo correspondiente con el fin de aplicar la política de acceso definida previamente, relacionando así el perfil de filtrado con el esquema de autenticación del proxy.

Figura 57. Creación y asignación de grupo

Fuente: Autoría propia.

Se procedió a la creación del usuario ingresando al módulo de gestión NCSA, donde se especificaron el nombre de la cuenta y su contraseña. Una vez guardados los cambios, el usuario queda registrado correctamente en el sistema. Posteriormente, se configuró un grupo desde la opción Administración de grupos NCSA, asignándole un nombre y asociando a dicho grupo el usuario previamente creado, con el objetivo de aplicar sobre él las políticas de acceso establecidas.

Figura 58. Vinculación de usuario al grupo

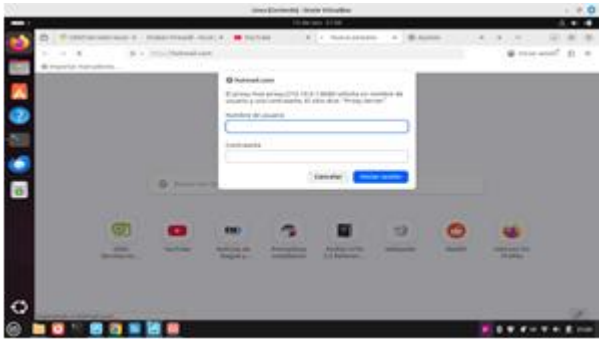


Fuente: Autoría propia.

A continuación, se accedió al apartado de Políticas de acceso, donde se creó una nueva política basada en autenticación por usuario, permitiendo así que el sistema aplicará los filtros únicamente a las cuentas previamente registradas. Dentro de esta política se vinculó el usuario creado, junto con el perfil de lista de bloqueo configurado anteriormente. Finalmente, al intentar acceder nuevamente a los sitios restringidos, el sistema solicita credenciales de inicio de

sesión, confirmando la correcta activación de la autenticación en el proxy.

Figura 59. Solicitud de permisos de ingreso a página bloqueada



Fuente: Autoría propia.

3 CONCLUSIONES

La instalación y configuración exitosa de Endian Firewall en VirtualBox permitió establecer una arquitectura segmentada en tres zonas de seguridad, asignando correctamente los adaptadores de red a sus respectivas interfaces (eth0 zona verde, eth1 zona naranja, eth2 zona roja). Esta configuración base garantiza el aislamiento lógico necesario para implementar políticas de seguridad perimetral efectivas [2].

Además, la configuración de servicios esenciales como DHCP y NAT, junto con reglas de firewall específicas, aseguraron la conectividad y seguridad entre zonas y hacia Internet, demostrando la viabilidad de una solución UTM basada en software libre para ambientes virtualizados [2].

La configuración de reglas NAT (Source NAT) permitió establecer la comunicación desde la zona verde y naranja hacia la zona roja (Internet), habilitando la traducción de direcciones IP privadas a públicas conforme a RFC 2663. Esto facilitó que dispositivos en redes privadas accedan a recursos externos manteniendo el aislamiento de direcciones internas [4].

La configuración selectiva de servicios en la zona DMZ permitió habilitar HTTP (puerto 80) y FTP (puerto 21) desde el servidor Ubuntu, mientras se bloqueó ICMP (puertos 8 y 30) para prevenir recon por ping. Esta granularidad en reglas de firewall implementa el principio de menor privilegio, permitiendo solo los servicios necesarios y denegando el resto [5].

La implementación de reglas inter-zona permitió comunicación controlada entre zonas verde y naranja para servicios HTTP/FTP, bloqueó acceso no autorizado desde la zona roja hacia la LAN, y limitó conexiones de la DMZ hacia Internet solo a puertos específicos. Las pruebas de navegación web validaron que las políticas de firewall se aplicaron correctamente, mejorando la postura de seguridad perimetral [2].

La implementación de un proxy HTTP no transparente con autenticación por usuario y lista negra de sitios (hotmail.com, youtube.com, elnuevodia.com.co) permitió centralizar el control de acceso web conforme a RFC 7235. El mecanismo de autenticación mediante credenciales de usuario asociadas a perfiles de filtrado proporciona auditoría y control granular de la navegación en Internet desde la LAN [6].

4 REFERENCIAS

[1] Azizov, D. (2020). Arquitectura DMZ Perimetral: una implementación corporativa.

[2] Endian Technologies, “Endian Firewall Community - Reference Manual,” Version 3.3, Endian.com, 2024. [Online]. Available: https://www.endian.com/community/

[3] Installing NGINX Open Source. (s/f). Nginx.com. Recuperado el 9 de diciembre de 2025, de http://docs.nginx.com/nginx/admin-guide/installing-nginx/installing-nginx-open-source/

[4] Internet Engineering Task Force (IETF), "Hypertext Transfer Protocol (HTTP/1.1) - Authentication," RFC 7235, 2014. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc7235

[5] Internet Engineering Task Force (IETF), "IP Network Address Translator (NAT) - Terminology and Considerations," RFC 2663, 1998. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc2663

[6] Muñoz, J. D. (2022, septiembre 28). iptables, un manual sencillo. PLEDIN 3.0. https://fp.josedomingo.org/seguridadgs/u03/iptables.html

[7] National Institute of Standards and Technology, “Guidelines on Firewalls and Firewall Policy,” NIST SP 800-41 Rev.1, Sep. 2009.

[8] NIST, "Recommendations on Blocking ICMP Traffic," RFC 4890, 2007. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4890

[9] Oracle Corporation, “Oracle® VM VirtualBox User Manual,” Version 7.0, Redwood Shores, CA, USA: Oracle, 2024.

[10] Practical Uses of nc(netcat) command in Linux. (2020, mayo 1). GeeksforGeeks. https://www.geeksforgeeks.org/linux-unix/practical-uses-of-ncnetcat-command-in-linux/

-