IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL EN GNU/LINUX MEDIANTE ENDIAN FIREWALL

Brahyam David Sánchez Montoya
e-mail: bdsanchezmo@unadvirtual.edu.co
Jhonny Castro Clavijo
e-mail: jcastrocla@unadvirtual.edu.co
Manuel Enrique Vega Ayala
e-mail: mevegaa@unadvirtual.edu.co

RESUMEN: *En este artículo se documenta la implementación de seguridad perimetral en sistemas GNU/Linux utilizando la distribución Endian Firewall Community. Se desarrollaron prácticas que incluyen la configuración inicial de redes y máquinas virtuales, la aplicación de reglas de Network Address Translation (NAT), y la creación de políticas de acceso en una zona desmilitarizada (DMZ). Los resultados evidencian la correcta segmentación de zonas (LAN, DMZ, WAN), la aplicación del principio de mínimo privilegio y la verificación de conectividad mediante protocolos HTTP y FTP, bloqueando tráfico ICMP. Estas configuraciones fortalecen la seguridad perimetral y consolidan competencias en administración de firewalls en entornos académicos.*

PALABRAS CLAVE: DMZ, Endian Firewall, NAT, Seguridad Perimetral

ABSTRACT: *This article documents the implementation of perimeter security in GNU/Linux systems using the Endian Firewall Community distribution. The practices developed include the initial configuration of networks and virtual machines, the application of Network Address Translation (NAT) rules, and the creation of access policies within a demilitarized zone (DMZ). The results demonstrate effective segmentation of zones (LAN, DMZ, WAN), the application of the principle of least privilege, and connectivity verification through HTTP and FTP protocols while blocking ICMP traffic. These configurations strengthen perimeter security and consolidate competencies in firewall administration within academic environments.*

KEYWORDS: DMZ, Endian Firewall, NAT, Perimeter Security

1 INTRODUCCIÓN

La seguridad perimetral en sistemas GNU/Linux es un componente esencial para proteger servicios críticos y garantizar la integridad de las aplicaciones [1][5]. En el marco del diplomado de profundización en administración de sistemas operativos Open Source, se desarrollaron prácticas orientadas a la configuración de Endian Firewall (EFW) como plataforma de seguridad [5].

Las temáticas abordadas incluyen:

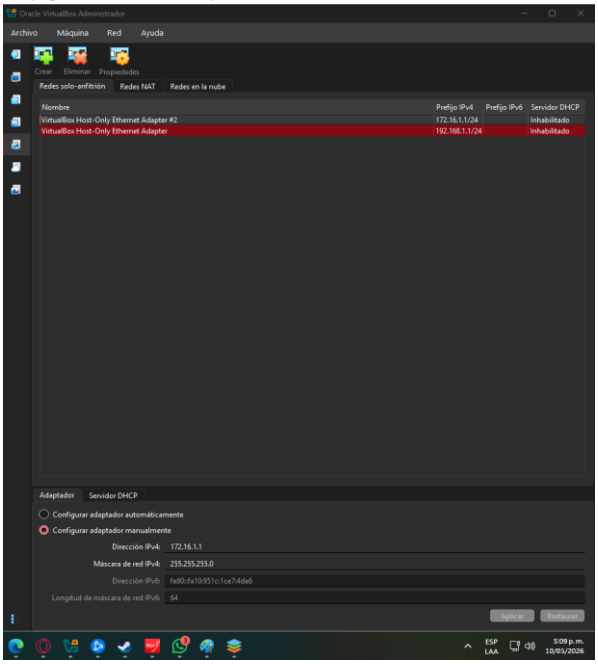
- Configuración inicial de redes y máquinas virtuales en VirtualBox [4].
- Implementación de reglas de **SNAT y DNAT** para permitir comunicación controlada entre zonas internas y externas [5].
- Aplicación de políticas de mínimo privilegio en la DMZ, habilitando únicamente servicios HTTP y FTP y bloqueando ICMP [1][5].
- Verificación de reglas mediante consola e interfaz gráfica, documentando evidencias de funcionamiento [1].

2 CONFIGURACIÓN DE GNU/LINUX ENDIAN EN VIRTUALBOX E INSTALACIÓN

Para garantizar la segmentación de red [4][5], se requiere la creación de dos redes de solo-anfitrión (Host-only) en VirtualBox que representarán las zonas aisladas: [4][5].

• Virtualbox Host-Only Ethernet Adapter (Zona GREEN/LAN): Red 192.168.1.1/24.
• Virtualbox Host-Only Ethernet Adapter#2 (Zona ORANGE/DMZ): Red 172.16.1.1/24.

Figura 1.
Configuración de interfaces de red



Fuente: Autoría Propia

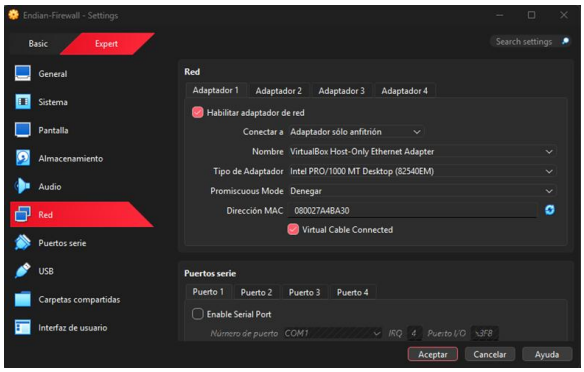
La figura 1 muestra la configuración de las redes Host-Only en VirtualBox utilizadas para la implementación de las zonas GREEN y ORANGE dentro de Endian Firewall Community. En la imagen se observan los adaptadores VirtualBox Host-Only Ethernet Adapter y VirtualBox Host-Only Ethernet Adapter #2, configurados con los prefijos IPv4 192.168.1.1/24 y 172.16.1.1/24 respectivamente. Asimismo, se evidencia que el servidor DHCP se encuentra deshabilitado, permitiendo una administración manual y controlada del direccionamiento IP dentro de la infraestructura virtualizada.

2.1 CONFIGURACIÓN DE LA MÁQUINA VIRTUAL ENDIAN

La correcta asignación de adaptadores es un requisito absoluto para la integridad de las zonas [1]. Se configuró la VM con los siguientes parámetros:

• Adaptador 1 (eth0): Conectado a Red de solo-anfitrión (Virtualbox Host-Only Ethernet Adapter). Representa la zona GREEN.

Figura 2.
Configuración de adaptador 1



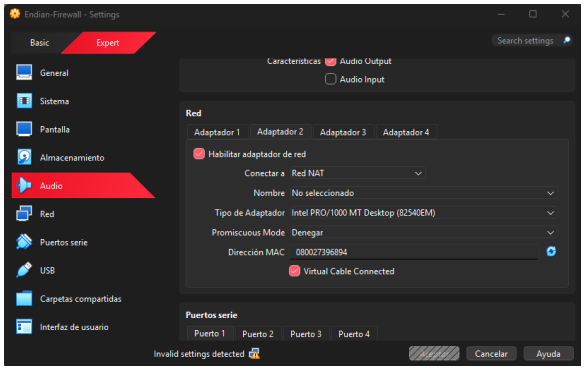
Fuente: Autoría Propia

La figura 2 presenta la configuración del primer adaptador de red de la máquina virtual Endian Firewall en VirtualBox. En esta sección se habilitó el adaptador de red utilizando el modo “Host-Only Ethernet Adapter”, el cual permite la comunicación interna dentro de la zona GREEN (LAN). Asimismo, se observa la selección del tipo de adaptador Intel PRO/1000 MT y la activación de la conexión mediante cable virtual, parámetros necesarios para garantizar la correcta comunicación entre los equipos virtualizados y el firewall implementado.

• Adaptador 2 (eth1): Conectado a NAT (VirtualBox). Representa la zona RED (Internet).

Se evidencia en las figuras 2, 3 y 4 la configuración de los adaptadores de red utilizada en la creación del servidor Endian para que pueda segmentar la red y cumplir su función.

Figura 3.
Configuración de adaptador 2



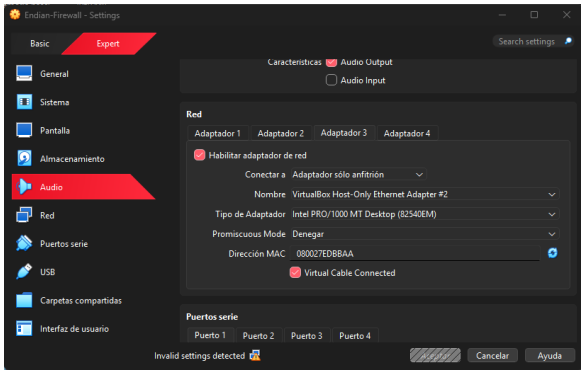
Fuente: Autoría Propia

La figura 3 muestra la configuración del segundo adaptador de red de la máquina virtual Endian Firewall dentro de VirtualBox. Este adaptador fue configurado en modo NAT, permitiendo el acceso de la máquina virtual hacia redes externas e Internet mediante la zona RED (WAN). Asimismo, se observa la utilización del adaptador Intel PRO/1000 MT Desktop y la habilitación de la conexión de red virtual, elementos fundamentales para garantizar la comunicación

saliente y la implementación de servicios de acceso externo dentro de la infraestructura

• Adaptador 3 (eth2): Conectado a Red de solo-anfitrión (Virtualbox Host-Only Ethernet Adapter#2). Representa la zona ORANGE.

Figura 4.
Configuración de adaptador 3



Fuente**:** Autoría Propia

La figura 4 presenta la configuración del tercer adaptador de red de la máquina virtual Endian Firewall en VirtualBox. Este adaptador fue conectado mediante la opción "Adaptador solo-anfitrión (Host-Only Adapter)", utilizando la interfaz Host-Only Ethernet Adapter para representar la zona ORANGE (DMZ). Asimismo, se evidencia la selección del adaptador Intel PRO/1000 MT Desktop y la conexión mediante cable virtual habilitado, permitiendo establecer una red aislada destinada a alojar servicios expuestos de manera controlada dentro de la infraestructura de seguridad perimetral.

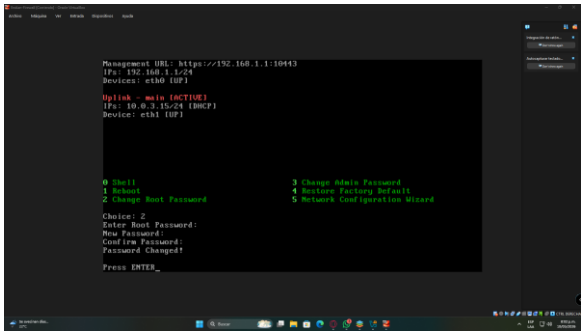
2.2 PROCESO DE INSTALACIÓN Y PRIMER ARRANQUE

Se inició la instalación desde la imagen ISO de Endian Firewall Community 3.x [5]. Durante el proceso de post-instalación en consola, se definieron los parámetros críticos de seguridad y red:

1. Asignación de contraseña para el usuario root y admin.
2. Configuración de la IP para la interfaz GREEN: 192.168.1.1/24.
3. Configuración de la interfaz RED vía DHCP [2][3].
4. Configuración de la IP para la interfaz ORANGE: 172.16.1.1/24.

Salida esperada en la consola de Endian
eth0: 192.168.1.1/24 (GREEN)
eth1: 10.0.2.15/24 (RED - IP de NAT de VirtualBox)
eth2: 172.16.1.1/24 (ORANGE)

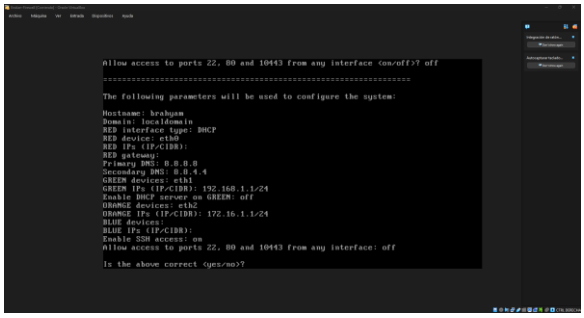
Figura 5.
Menú inicial Endian Firewall



Fuente: Autoría Propia

En la figura 5 se puede observar el menú inicial que se presenta cuando se termina la instalación de Endian, de las opciones que nos presenta en la figura 6 se puede observar el resultado de la ejecución de Network Configuration Wizard (Asistente de configuración de red)

Figura 6.
Ejecución del Network Configuration Wizard



Fuente: Autoría Propia

La figura 6 presenta la ejecución del asistente de configuración de red de Endian Firewall Community, herramienta utilizada para definir los parámetros principales de comunicación y segmentación de la infraestructura virtualizada. En esta sección se configuraron las interfaces RED, GREEN y ORANGE, asignando direccionamiento IP, método de obtención de red y parámetros DNS necesarios para el funcionamiento del firewall. Asimismo, se observa la configuración de la interfaz RED mediante DHCP y la asignación manual de direcciones para las zonas GREEN y ORANGE, permitiendo establecer una separación lógica entre la red interna, la DMZ y el acceso externo. Estas configuraciones constituyen la base para la implementación de políticas de seguridad y control de tráfico dentro del entorno GNU/Linux.

2.3 CONFIGURACIÓN DE CLIENTES Y SERVIDORES UBUNTU

Se desplegaron instancias de Ubuntu configuradas mediante archivos Netplan [3][6] para validar la conectividad entre zonas.
Ubuntu Cliente (LAN) - /etc/netplan/01-netcfg.yaml:

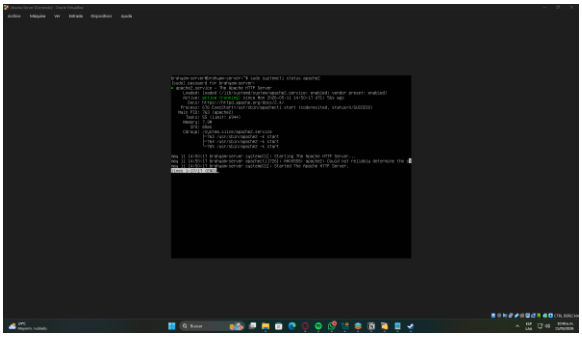
```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s8:
      addresses: [192.168.1.20/24]
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

Ubuntu Servidor (DMZ) - /etc/netplan/01-netcfg.yaml:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s8:
      addresses: [172.16.1.10/24]
      gateway4: 172.16.1.1
      nameservers:
        addresses: [8.8.8.8]
```

Se instalaron los servicios Apache y vsftpd en el servidor DMZ [6][10] y se completó el wizard en https://192.168.1.1:10443 [5].

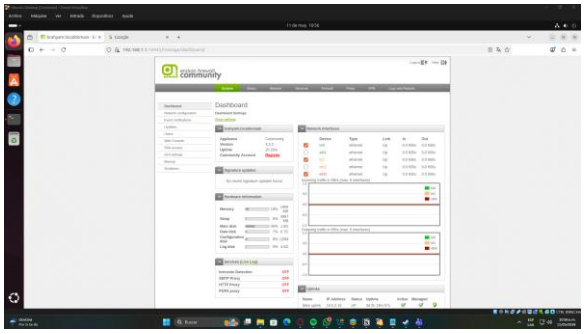
Figura 7.
Verificación del estado del servidor Apache



Fuente: Autoría Propia

La figura 7 muestra la verificación del estado del servicio Apache2 ejecutada desde la terminal del servidor Ubuntu ubicado en la zona DMZ. Mediante el comando `systemctl status apache2` se comprobó que el servicio web se encontraba activo y en ejecución correctamente, permitiendo validar el funcionamiento del servidor HTTP dentro de la infraestructura implementada. Asimismo, la salida de la consola evidencia que el servicio fue iniciado exitosamente por el sistema y que los procesos asociados al servidor web permanecen operativos. Esta validación resulta fundamental para garantizar la disponibilidad de los servicios publicados en la DMZ y comprobar el correcto funcionamiento de las reglas de acceso y traducción NAT configuradas en Endian Firewall Community.

Figura 8.
Interfaz gráfica de configuración de Endian



Fuente**:** Autoría Propia

La figura 8 presenta la interfaz gráfica de administración de Endian Firewall Community, accesible mediante navegador web a través de la URL de gestión configurada durante el proceso de instalación. Desde este panel centralizado es posible administrar las políticas de seguridad, reglas de firewall, configuración de red, servicios y monitoreo del sistema. Asimismo, la interfaz permite gestionar de manera visual las zonas GREEN, ORANGE y RED, facilitando la implementación de reglas NAT, control de tráfico y políticas de acceso entre segmentos de red. El uso de esta plataforma gráfica simplifica las tareas de administración y fortalece la gestión de seguridad perimetral dentro del entorno GNU/Linux virtualizado.

3 CONFIGURACIÓN NAT (NETWORK ADDRESS TRANSLATION)

3.1 IMPLEMENTACIÓN DE SNAT (OUTBOUND NAT)

Se configuraron reglas Outbound NAT para permitir el tráfico desde las zonas internas hacia la RED pública [5].

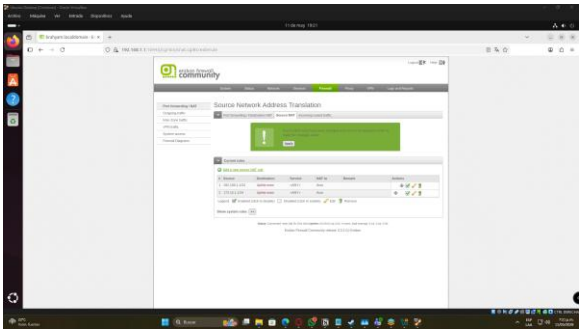
Tabla 1.
Configuración NAT

Origen	Destino	Servicio	Tipo de NAT
GREEN (192.168.1.0/24)	Interfaz RED	ANY	MASQUERADE
ORANGE (172.16.1.0/24)	Interfaz RED	ANY	MASQUERADE

Fuente: Autoría Propia

Como se observa en la figura 9 se configuran las reglas de port forwarding / NAT (Network Address Translation).

Figura 9.
Configuración de redireccionamiento



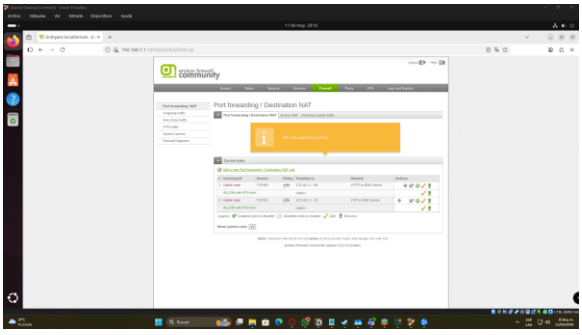
Fuente: Autoría Propia

La figura 9 muestra la sección de configuración de Source Network Address Translation (SNAT) dentro de la interfaz gráfica de Endian Firewall Community. En esta sección se implementaron las reglas de traducción de direcciones necesarias para permitir la salida de tráfico desde las zonas internas hacia redes externas mediante el proceso de enmascaramiento (MASQUERADE). Estas configuraciones permiten ocultar las direcciones IP privadas de la infraestructura interna y utilizar la dirección pública asignada a la interfaz RED para establecer comunicación con Internet. Asimismo, la implementación de reglas NAT contribuye a mejorar la seguridad perimetral al controlar y administrar el flujo de tráfico entre las diferentes zonas de red definidas en la infraestructura virtualizada.

3.2 IMPLEMENTACIÓN DE DNAT (PORT FORWARDING)

Se establecieron reglas de reenvío de puertos (Port Forwarding) desde la interfaz RED hacia el servidor DMZ (172.16.1.10) para los puertos 80 (HTTP) y 21 (FTP) [5].

Figura 10.
Configuración DNAT port forwarding



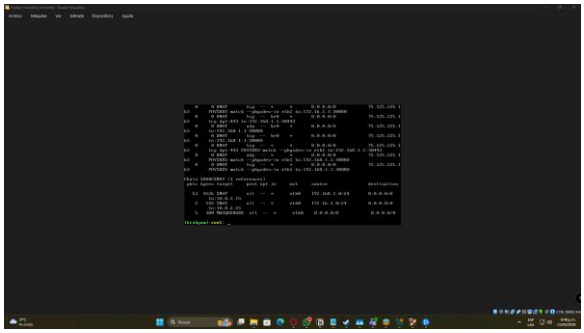
Fuente: Autoría Propia

La figura 10 presenta la configuración de reglas de Destination Network Address Translation (DNAT) y Port Forwarding en Endian Firewall Community. En esta sección se definieron las políticas de redireccionamiento de puertos desde la interfaz RED hacia el servidor ubicado en la zona DMZ, permitiendo el acceso controlado a los servicios HTTP y FTP. Asimismo, las reglas configuradas posibilitan que las solicitudes provenientes de redes externas sean dirigidas hacia la dirección IP interna del servidor alojado en la DMZ, manteniendo la segmentación y el control de tráfico dentro de la infraestructura. Estas configuraciones resultan fundamentales para publicar servicios hacia Internet de manera segura, limitando únicamente el acceso a los puertos autorizados dentro de la política de seguridad perimetral implementada.

3.3 VERIFICACIÓN MEDIANTE IPTABLES

La verificación de las reglas se realizó en la consola de Endian mediante el comando de inspección de la tabla NAT [1][8][9]: iptables -t nat -L -n -v
Se identificaron las cadenas PREROUTING (para DNAT) y POSTROUTING (para MASQUERADE) como los puntos críticos de manipulación de paquetes.

Figura 11.
Resultado de iptables



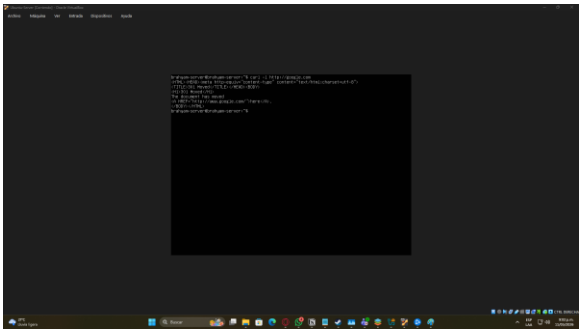
Fuente: Autoría Propia

La figura 11 presenta el resultado de la verificación de reglas NAT ejecutada mediante el comando `iptables -t nat -L -n -v` en la consola de Endian Firewall Community. En la salida del sistema se observan las cadenas y reglas encargadas de administrar los procesos de traducción de direcciones, incluyendo configuraciones SNAT, DNAT y MASQUERADE aplicadas sobre las interfaces de red del firewall. Asimismo, se evidencia el redireccionamiento de tráfico hacia direcciones IP internas y la utilización de reglas de enmascaramiento para permitir la comunicación de las zonas GREEN y ORANGE hacia redes externas. La verificación de estas políticas permitió confirmar el correcto funcionamiento de las configuraciones NAT implementadas dentro de la infraestructura virtualizada y validar el control del tráfico entre las diferentes zonas de seguridad.

3.4 PRUEBAS DE FUNCIONAMIENTO

Se validó la salida a Internet desde el cliente LAN mediante curl -I http://google.com y desde el servidor DMZ mediante curl ifconfig.me.

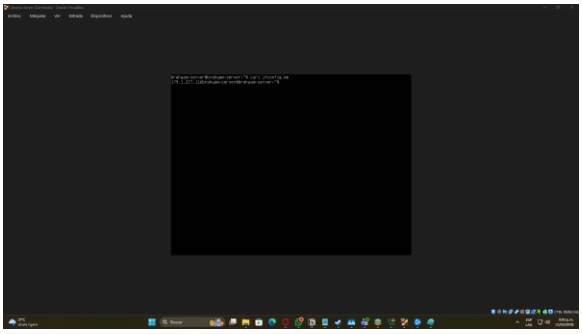
Figura 12.
Verificación de protocolo HTTP



Fuente: Autoría Propia

La figura muestra la ejecución del comando curl -I http://google.com desde un host en la zona GREEN (LAN) del Endian Firewall, obteniendo una respuesta HTTP/1.1 301 Moved Permanently con redirección hacia https://www.google.com. Esta prueba verifica el correcto funcionamiento del proxy HTTP (Squid) configurado en Endian y las reglas de masquerading (SNAT) en la tabla nat de iptables, que traducen el tráfico saliente desde LAN hacia la interfaz RED (WAN). La configuración habilita el forwarding stateful entre zonas GREEN y RED, permitiendo el acceso controlado a Internet sin exposición directa de los hosts internos. Desde el punto de vista de la seguridad perimetral, esta validación confirma que el firewall aplica las políticas de acceso definidas, registra la actividad en logs y previene fugas de tráfico no autorizado, manteniendo el equilibrio entre conectividad y protección.

Figura 13.
Resultado de curl ifconfig.me



Fuente: Autoría Propia

La figura muestra la ejecución del comando curl ifconfig.me desde un host en la zona GREEN (LAN), devolviendo la IP pública 179.1.227.116 de la interfaz RED (WAN). Esta prueba verifica el correcto funcionamiento del masquerading (SNAT) en la tabla nat de iptables configurado en Endian Firewall. La configuración habilita el forwarding stateful entre GREEN y RED, ocultando las direcciones privadas de la LAN. Desde el punto de vista de la seguridad perimetral, confirma el ocultamiento efectivo de la topología interna y el correcto enrutamiento del tráfico saliente.

4 CONFIGURACIÓN DEL FIREWALL

4.1 REQUISITOS PREVIOS

Para el desarrollo de la práctica fue necesario contar con los siguientes elementos previamente configurados:
• Temáticas 1 y 2 completadas correctamente.
• Servidor Ubuntu-Server-DMZ con dirección IP 172.16.1.10.
• Servicios Apache2 y vsftpd instalados y activos.
• Acceso a la interfaz web de administración de Endian Firewall.
• Cliente Ubuntu-LAN-Cliente para las pruebas de conectividad.

4.2 CONFIGURACIÓN DE OUTBOUND TRAFFIC

Figura 14.
Interfaz principal de Endian Community Firewall y verificación de política DROP

Fuente: Autoría propia.

La figura presenta el dashboard de la interfaz web de Endian Community Firewall, donde se accede a la sección Firewall → Outbound Traffic para verificar la política predeterminada configurada en modo DROP [5]. Esta configuración asegura que todo el tráfico saliente desde las zonas DMZ, LAN o BLUE sea denegado por defecto, permitiendo únicamente las conexiones explícitamente autorizadas. La verificación confirma la aplicación correcta del modelo stateful del firewall basado en iptables, reforzando la seguridad perimetral mediante el principio de menor privilegio. El impacto es una mayor protección contra fugas de tráfico no autorizado y ataques desde el interior hacia el exterior.

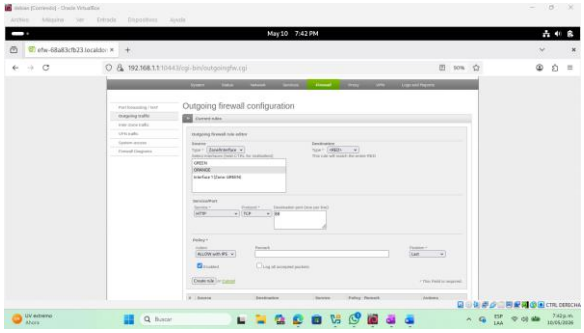
4.3 REGLA PARA PERMITIR HTTP

Se creó una regla de tráfico saliente para permitir conexiones HTTP desde el servidor ubicado en la DMZ hacia internet utilizando el protocolo TCP y el puerto 80 [5].

Parámetros configurados:
• Source Zone: ORANGE
• Source IP: 172.16.1.10/32
• Destination Zone: RED
• Protocol: TCP
• Destination Port: 80

• Action: ACCEPT

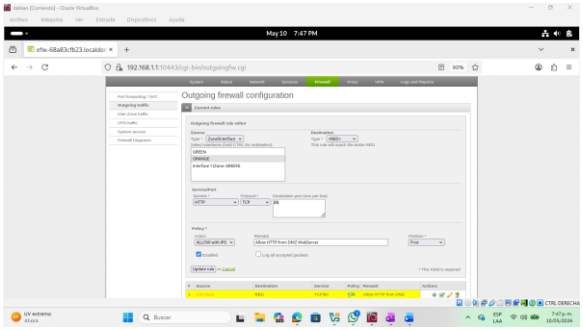
Figura 15.
Configuración de regla Outbound para permitir HTTP desde la DMZ.



Fuente: Autoría Propia

La figura muestra la sección Outgoing Firewall Configuration de Endian Community Firewall, donde se creó una regla específica que permite tráfico HTTP (puerto 80) desde la zona DMZ (ORANGE) hacia cualquier destino en Internet [5]. Se observa la configuración con Source = DMZ, Destination = Any, Service = HTTP y Action = ACCEPT. Esta regla se aplica sobre la política predeterminada DROP, permitiendo únicamente el tráfico explícitamente autorizado. Desde el punto de vista de la seguridad perimetral, esta configuración mantiene el principio de menor privilegio al controlar de forma granular el tráfico saliente desde servidores expuestos en DMZ.

Figura 16.
Regla HTTP habilitada en el firewall Endian.



Fuente: Autoría propia.

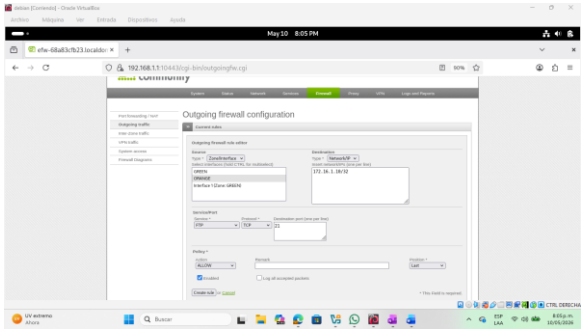
La figura muestra la regla outbound configurada en Endian Community Firewall para permitir tráfico HTTP (puerto 80) desde la zona DMZ hacia cualquier destino en Internet [5]. Se observa la regla activa con Source = DMZ, Destination = Any, Service = HTTP y Action = ACCEPT. Esta configuración opera sobre la política predeterminada DROP, permitiendo únicamente el tráfico explícitamente autorizado. Desde el punto de vista de la seguridad perimetral, la regla mantiene el principio de menor privilegio al controlar granularmente el tráfico saliente desde servidores en DMZ.

4.4 REGLA PARA PERMITIR FTP

Posteriormente se configuró una regla para permitir el tráfico FTP desde el servidor DMZ hacia internet utilizando el puerto 21 [5].

Parámetros configurados:
• Source Zone: ORANGE
• Source IP: 172.16.1.10/32
• Destination Zone: RED
• Protocol: TCP
• Destination Port: 21
• Action: ACCEPT

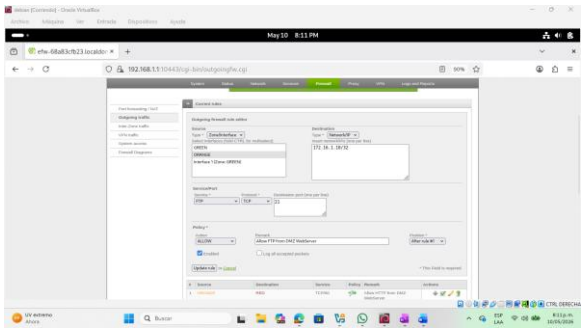
Figura 17.
Configuración de regla Outbound para permitir FTP desde la DMZ.



Fuente**:** Autoría propia.

La figura muestra la configuración de una regla outbound en Endian Community Firewall para permitir tráfico FTP (puerto 21/TCP) desde el servidor ubicado en la zona DMZ (ORANGE, IP 172.16.1.10) hacia Internet [5]. Se observan los parámetros específicos: Source Zone = ORANGE, Source IP = 172.16.1.10/32, Destination Zone = RED, Protocol = TCP, Destination Port = 21 y Action = ACCEPT. Esta regla se aplica sobre la política predeterminada DROP, garantizando que solo el tráfico explícitamente autorizado sea permitido. Desde el punto de vista de la seguridad perimetral, esta configuración demuestra la aplicación del principio de menor privilegio, permitiendo únicamente el servicio necesario desde la DMZ sin exponer el servidor a tráfico entrante no solicitado, fortaleciendo así el control granular del firewall basado en iptables.

Figura 18.
Regla FTP habilitada correctamente en el firewall.



Fuente: Autoría propia.

La figura muestra la regla outbound configurada y habilitada en Endian Community Firewall para permitir tráfico

FTP (puerto 21/TCP) desde la zona DMZ (ORANGE) hacia el destino 172.16.1.18/32 [5]. Se observa la configuración con Source Zone = ORANGE, Service = FTP, Protocol = TCP, Action = ALLOW y el remark "Allow FTP from DMZ WebServer". Esta regla opera sobre la política predeterminada DROP, permitiendo únicamente el tráfico explícitamente autorizado. Desde el punto de vista de la seguridad perimetral, confirma el control granular del firewall basado en iptables y la aplicación efectiva del principio de menor privilegio para servicios específicos en la DMZ.

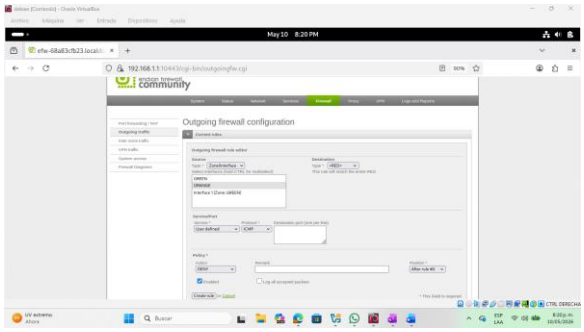
4.5 REGLAS PARA DENEGAR ICMP

Con el propósito de impedir tareas de reconocimiento de red se implementaron dos reglas de denegación para tráfico ICMP [1][5].

4.5.1 BLOQUEO ICMP ECHO REQUEST

La primera regla fue creada para bloquear solicitudes ICMP Echo Request (Tipo 8), utilizadas comúnmente por el comando ping.

Figura 19.
Regla DENY para ICMP Echo Request desde la zona ORANGE hacia RED



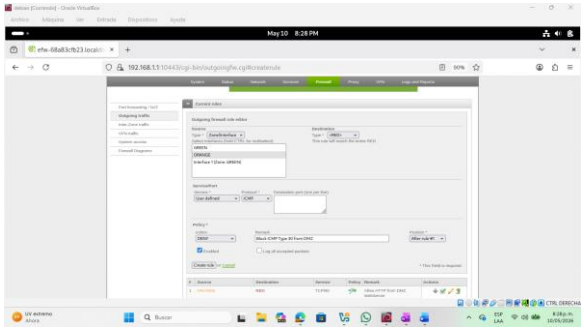
Fuente: Autoría propia.

La figura muestra la configuración de una regla outbound en Endian Community Firewall para denegar tráfico ICMP Echo Request (Tipo 8) desde la zona DMZ (ORANGE) hacia la interfaz RED (WAN) [5]. Se observa la creación de la regla con Source Zone = ORANGE, Service = ICMP Echo Request, Action = DENY y la política predeterminada DROP. Esta regla tiene como propósito impedir tareas de reconocimiento de red mediante el comando ping. Desde el punto de vista de la seguridad perimetral, reduce la superficie de ataque al evitar que servidores expuestos en DMZ revelen información sobre la topología de red y posibles hosts activos.

4.5.2 BLOQUEO ICMP TIPO 30

La segunda regla se configuró para bloquear paquetes ICMP Tipo 30 asociados a operaciones de traceroute.

Figura 20.
Regla DENY para ICMP Tipo 30 desde la zona ORANGE hacia RED.



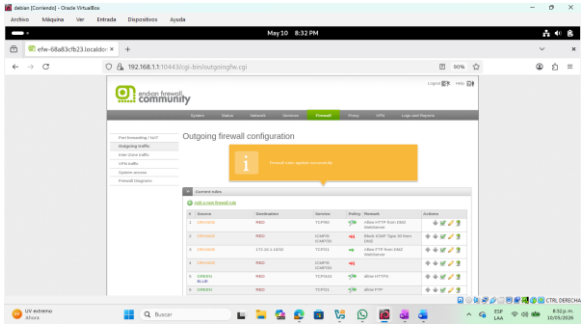
Fuente: Autoría propia.

La figura muestra la configuración de una regla outbound en Endian Community Firewall para denegar tráfico ICMP Tipo 30 desde la zona DMZ (ORANGE) hacia la interfaz RED (WAN) [5]. Se observa la definición de Source Zone = ORANGE, Service = ICMP Tipo 30 y Action = DENY. Esta regla complementa el bloqueo de ICMP Echo Request con el fin de impedir técnicas avanzadas de reconocimiento de red como traceroute. Desde el punto de vista de la seguridad perimetral, reduce la exposición de información sobre la topología de red y limita la capacidad de los atacantes para mapear la infraestructura interna.

4.6 APLICACIÓN DE CAMBIOS

Después de configurar todas las reglas del firewall se procedió a aplicar los cambios mediante el botón "Apply Changes" de la interfaz de administración de Endian.

Figura 21.
Mensaje de confirmación de aplicación exitosa de reglas del firewall.



Fuente: Autoría propia.

La figura muestra el mensaje de confirmación "Rules have been applied successfully" tras aplicar las reglas configuradas en la sección Outgoing Firewall de Endian Community Firewall [5]. Se observa la interfaz que indica que las modificaciones (incluyendo reglas de ALLOW para HTTP/FTP e ICMP DENY) han sido cargadas correctamente en el motor de iptables subyacente. Esta verificación asegura que las políticas de seguridad perimetral definidas están activas y operativas. Desde el punto de vista técnico, confirma la correcta traducción de las reglas gráficas a cadenas

FORWARD y NAT del firewall, garantizando el control efectivo del tráfico entre zonas DMZ y RED.

5 VERIFICACIONES REALIZADAS

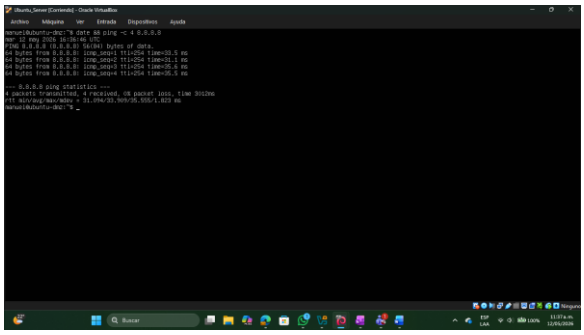
5.1 VERIFICACIÓN DE BLOQUEO ICMP

Desde el servidor Ubuntu-Server-DMZ se ejecutó el siguiente comando:

date && ping -c 4 8.8.8.8

El resultado mostró pérdida total de paquetes, confirmando que las reglas de denegación ICMP estaban funcionando correctamente. [1].

Figura 22.
Resultado de prueba ping desde la DMZ con 100% packet loss.



Fuente: Autoría propia.

La figura muestra la ejecución del comando ping 8.8.8.8 desde el servidor en la zona DMZ (ORANGE), obteniendo un resultado de 100% packet loss tras enviar 4 paquetes ICMP Echo Request. Esta prueba verifica el correcto funcionamiento de las reglas DENY configuradas en Endian Community Firewall para bloquear tráfico ICMP saliente [5]. Se confirma que las reglas para ICMP Echo Request (Tipo 8) y Tipo 30 están operativas, impidiendo el tráfico de diagnóstico. Desde el punto de vista de la seguridad perimetral, esta validación demuestra la efectividad del control de reconnaissance attacks, ocultando la presencia y topología de la DMZ hacia Internet.

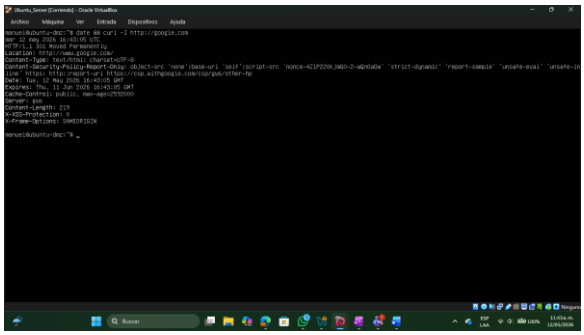
5.2 VERIFICACIÓN DE ACCESO HTTP

Desde el servidor Ubuntu-Server-DMZ se verificó el acceso HTTP permitido ejecutando el siguiente comando:

date && curl -I http://google.com

El resultado devolvió una respuesta HTTP exitosa (HTTP/1.1 301 OK), confirmando que el tráfico por el puerto 80 está correctamente autorizado [7].

Figura 23.
Resultado exitoso del comando curl -I desde el servidor DMZ.



Fuente: Autoría propia.

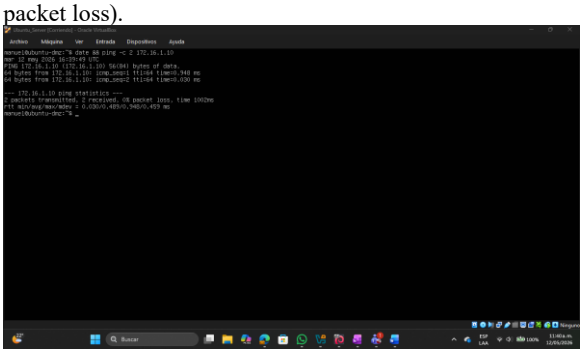
5.3 VERIFICACIÓN DESDE CLIENTE LAN

Desde el equipo Ubuntu-LAN-Cliente se ejecutó el siguiente comando para verificar el comportamiento de la política:

date && ping -c 2 172.16.1.10

El resultado mostró 100% packet loss, validando el correcto funcionamiento de las reglas aplicadas.

Figura 24.
Resultado de ping desde LAN hacia el servidor DMZ (100% packet loss).



Fuente: Autoría propia.

La figura muestra la ejecución del comando ping desde un host en la zona GREEN (LAN) hacia el servidor en la zona DMZ (ORANGE), resultando en 100% packet loss. Esta prueba verifica que las reglas de firewall configuradas en Endian Community Firewall bloquean correctamente el tráfico ICMP entre zonas GREEN y ORANGE [5]. La configuración mantiene la política de segmentación perimetral, impidiendo el movimiento lateral entre redes internas y la DMZ. Desde el punto de vista de la seguridad, esta validación refuerza la defensa en profundidad al evitar que un compromiso en LAN pueda alcanzar servidores expuestos en DMZ.

5.4 RESUMEN DE VERIFICACIONES CON MARCA DE TIEMPO:

Tabla 2.

Verificación incluye marca de tiempo

Verificación	Comando ejecutado	Fecha y hora registrada	Resultado
1	date && ping -c 4 8.8.8.8	mar 12 may 2026 11:37 am	100% packet loss
2	date && curl -I http://google.com	mar 12 may 2026 11:43 am	HTTP/1.1 301 OK
3	date && ping -c 2 172.16.1.10	mar 12 may 2026 11:40 am	100% packet loss

Fuente: Autoría propia.

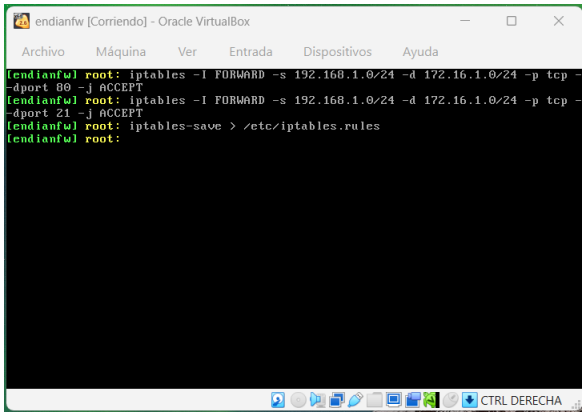
6 REGLAS DE ACCESO ENTRE ZONAS

La cuarta temática se centró en la creación de reglas de acceso entre LAN, DMZ y WAN, esta se implementa mediante la ejecución de comandos iptables y la interfaz gráfica de endian [1][5].

6.1 COMUNICACIÓN LAN → DMZ MEDIANTE HTTP Y FTP.

Figura 25.

Configuración de reglas mediante comando iptables.

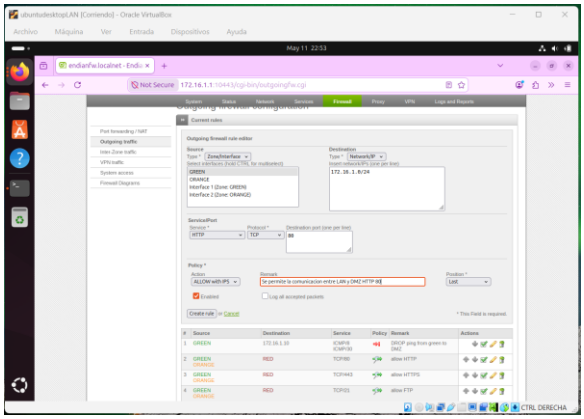


Fuente: Autoría propia.

La figura muestra la ejecución de comandos iptables directamente en la consola de Endian Community Firewall para crear reglas en la cadena FORWARD que permiten tráfico TCP desde la zona LAN (192.168.1.0/24) hacia la zona DMZ (172.16.1.0/24) por los puertos 80 (HTTP) y 21 (FTP) [5][9]. Estas reglas complementan las configuraciones gráficas del Outbound Firewall y garantizan la comunicación controlada entre ambas zonas de confianza. La configuración se realiza sobre el motor stateful de iptables, manteniendo el seguimiento de conexiones (conntrack). Desde el punto de vista de la seguridad perimetral, esta implementación permite el acceso necesario desde LAN a servicios en DMZ bajo el principio de menor privilegio, evitando exposición innecesaria.

Figura 26.

Creación de reglas mediante interfaz gráfica endian



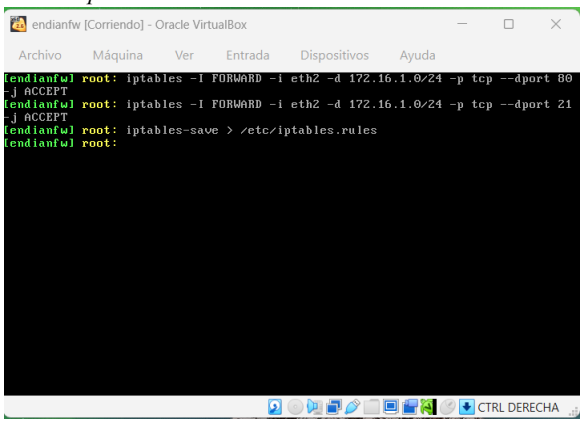
Fuente: Autoría propia.

La figura muestra la interfaz web de Endian Community Firewall en la sección de creación de una nueva regla Outbound Traffic. Se configuró una regla con origen en la zona ORANGE (DMZ), destino en la zona RED (WAN), protocolo TCP y acción ACCEPT [5]. Esta regla permite el tráfico controlado desde servidores en DMZ hacia Internet, operando sobre la política predeterminada DROP. Desde el punto de vista de la seguridad perimetral, la configuración gráfica facilita la aplicación del principio de menor privilegio, permitiendo únicamente el tráfico necesario mientras mantiene el control granular basado en iptables.

6.2 COMUNICACIÓN WAN → DMZ CON REDIRECCIONAMIENTO DE PUERTOS 80 Y 21.

Figura 27.

Configuración de reglas de redireccionamiento mediante comando iptables

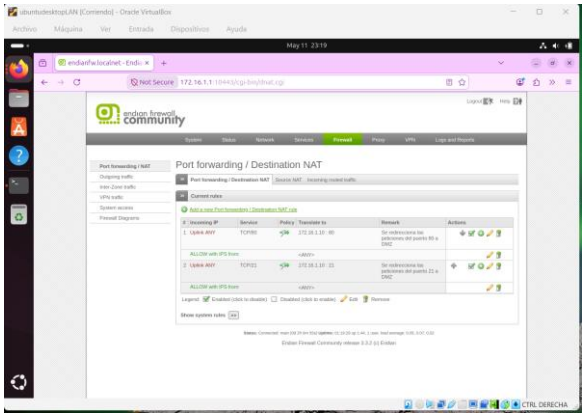


Fuente: Autoría propia.

La figura muestra la ejecución de comandos iptables en la consola de Endian Community Firewall para configurar reglas de redireccionamiento DNAT [5]. Se crearon reglas en las cadenas PREROUTING (tabla nat) y FORWARD que permiten tráfico entrante desde la zona WAN (RED) hacia la

zona DMZ (ORANGE) en los puertos 80 (HTTP) y 21 (FTP). Esta configuración habilita la publicación controlada de servicios desde la DMZ hacia Internet. Desde el punto de vista de la seguridad perimetral, el uso de DNAT junto con políticas restrictivas mantiene el principio de menor privilegio y reduce la exposición directa de los servidores.

Figura 28.
Creación de regla redireccionamiento puerto 80 y 21 a DMZ.

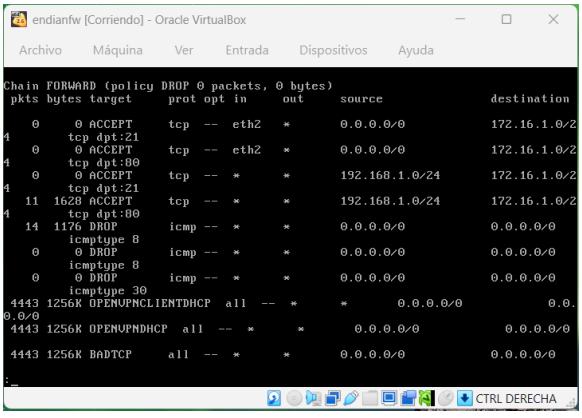


Fuente: Autoría propia.

La figura muestra la sección Port Forwarding / Destination NAT de la interfaz gráfica de Endian Community Firewall. Se configuraron reglas de redireccionamiento DNAT para los puertos 80 (HTTP) y 21 (FTP) desde la zona WAN (RED) hacia el servidor ubicado en la zona DMZ con dirección IP 172.16.1.10 [5]. Estas reglas se aplican en las cadenas PREROUTING (tabla nat) y FORWARD de iptables. Desde el punto de vista de la seguridad perimetral, permiten la publicación controlada de servicios hacia Internet manteniendo el principio de menor privilegio y la segmentación entre zonas.

6.3 LA VERIFICACIÓN SE REALIZÓ CON IPTABLES -L -N -V, CONFIRMANDO REGLAS ACTIVAS Y DENEGACIONES CORRECTAS.

Figura 29.
Resultado del comando iptables -L -n -v | less

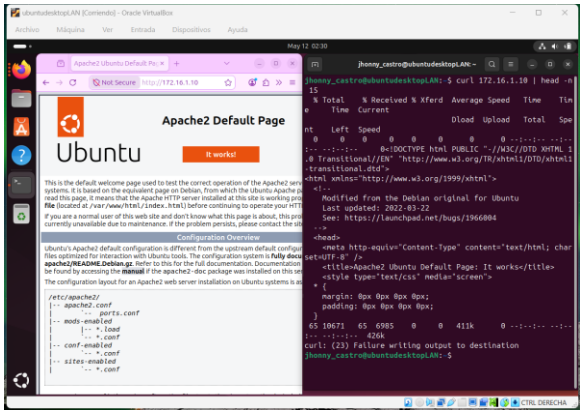


Fuente: Autoría propia.

La figura muestra el resultado del comando iptables -L -n -v | less ejecutado en la consola de Endian Community Firewall, donde se listan las reglas activas en las cadenas INPUT, FORWARD y OUTPUT [5]. Se observan claramente las políticas configuradas previamente, incluyendo reglas ACCEPT para tráfico autorizado (HTTP, FTP) y DROP para conexiones no permitidas entre las zonas LAN (GREEN), DMZ (ORANGE) y WAN (RED). Esta verificación confirma que las reglas definidas tanto gráficamente como mediante comandos se encuentran cargadas y operativas en el kernel. Desde el punto de vista de la seguridad perimetral, valida el correcto funcionamiento del firewall stateful y el cumplimiento de la política de denegación por defecto.

6.4 HTTP DESDE LAN → DMZ

Figura 30.
Verificación de comunicación HTTP desde LAN a DMZ

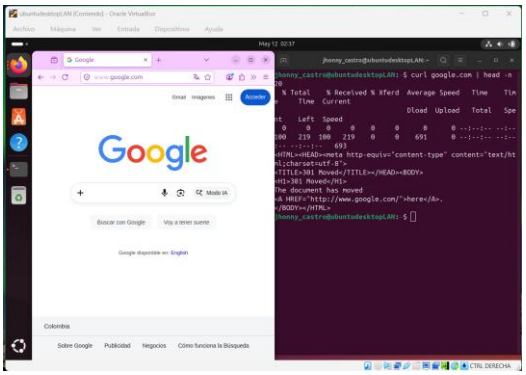


Fuente: Autoría propia.

La figura muestra el resultado del comando iptables -L -n -v | less ejecutado en la consola de Endian Community Firewall, donde se verifican las reglas activas en las cadenas INPUT, FORWARD y OUTPUT [5]. Se observan las reglas ACCEPT configuradas para permitir tráfico HTTP (puerto 80) desde la zona LAN (GREEN) hacia la zona DMZ (ORANGE), junto con las políticas DROP por defecto. Esta verificación confirma que las reglas de forwarding están operativas y que la comunicación entre ambas zonas se encuentra correctamente habilitada. Desde el punto de vista de la seguridad perimetral, valida el control granular del tráfico y el cumplimiento del principio de menor privilegio entre las zonas internas.

6.5 HTTP DESDE LAN → WAN

Figura 31.
Verificación de comunicación HTTP desde LAN a WAN



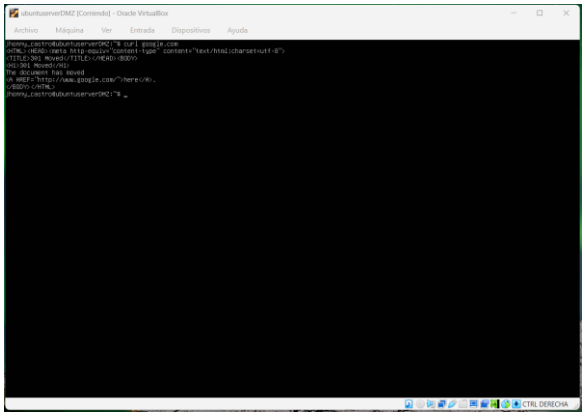
Fuente: Autoría propia.

La figura muestra la verificación exitosa de comunicación HTTP desde un cliente en la zona LAN (GREEN) hacia Internet (WAN). En la ventana izquierda se observa un navegador accediendo correctamente a la página de Google, mientras que en la ventana derecha se aprecia la salida del comando curl -I google.com con respuesta HTTP/1.1 200 OK [5]. Esta prueba confirma el correcto funcionamiento de las reglas de forwarding y masquerading (SNAT) configuradas en Endian Community Firewall. Desde el punto de vista de la seguridad perimetral, valida que el tráfico saliente autorizado fluye correctamente mientras se mantiene la política de denegación por defecto para conexiones no permitidas.

6.6 HTTP DESDE DMZ → WAN

Figura 32.

Verificación de comunicación HTTP desde DMZ a WAN

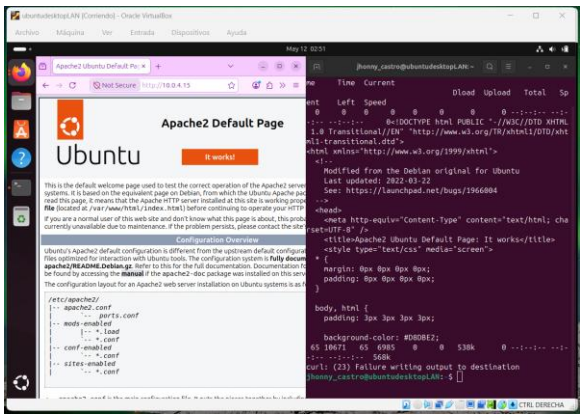


Fuente: Autoría propia.

La figura muestra la verificación de conectividad HTTP desde un servidor en la zona DMZ (ORANGE) hacia Internet (WAN) mediante los comandos curl -I -v. Se observa el acceso exitoso tanto al gateway local (172.16.1.1) como a un sitio externo (www.cisco.com), obteniendo respuestas HTTP/1.1 200 OK y redirecciones correctas [5]. Esta prueba confirma el correcto funcionamiento de las reglas outbound configuradas en Endian Community Firewall junto con el masquerading (SNAT). Desde el punto de vista de la seguridad perimetral, valida que el tráfico saliente autorizado desde la DMZ fluye correctamente mientras se mantiene la política de denegación por defecto para el resto de las conexiones.

6.7 HTTP DESDE WAN → DMZ

Figura 33.
Verificación de comunicación HTTP desde WAN a DMZ

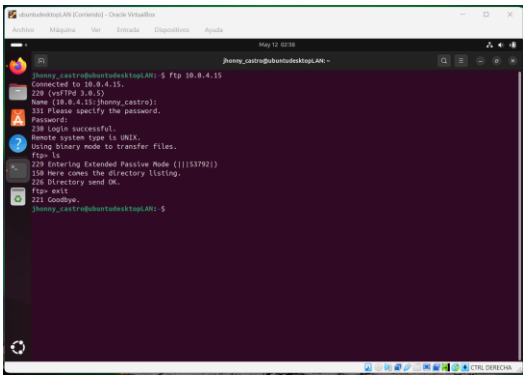


Fuente**:** Autoría propia.

La figura presenta la prueba de conectividad HTTP entrante desde la WAN hacia la DMZ. Mediante un navegador externo se accedió a la IP pública del firewall, mostrando correctamente la página por defecto de Apache2 (“It works!”) [5]. Esta verificación confirma que las reglas de Destination NAT (DNAT) y forwarding configuradas en Endian Community Firewall permiten el tráfico entrante desde RED hacia el servidor web en ORANGE. Desde el punto de vista de la seguridad perimetral, demuestra el correcto funcionamiento de la publicación controlada de servicios manteniendo la segmentación y el principio de menor privilegio.

6.8 FTP DESDE WAN → DMZ

Figura 34.
Verificación de comunicación FTP desde WAN a DMZ

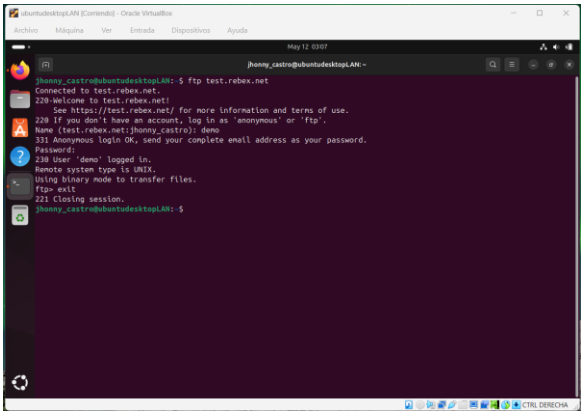


Fuente: Autoría propia.

La figura presenta la prueba de conectividad FTP entrante desde la WAN hacia la DMZ. Mediante un cliente FTP externo se estableció conexión exitosa al servidor en la zona DMZ (IP 10.0.4.15), logrando autenticación, modo pasivo y listado de directorio [5]. Esta verificación confirma que las reglas de Destination NAT (DNAT), port forwarding y forwarding configuradas en Endian Community Firewall permiten correctamente el tráfico por el puerto 21 desde RED hacia ORANGE. Desde el punto de vista de la seguridad perimetral, demuestra la publicación controlada del servicio FTP manteniendo el principio de menor privilegio y la segmentación entre zonas.

6.9 FTP DESDE LAN → WAN

Figura 35.
Verificación de comunicación FTP desde LAN a WAN

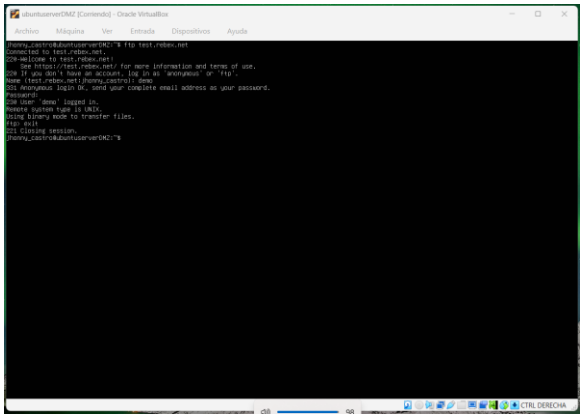


Fuente: Autoría propia.

La figura presenta la prueba de conectividad FTP saliente desde la zona LAN (GREEN) hacia Internet (WAN). Mediante el comando ftp test.rebex.net se estableció una conexión exitosa a un servidor público de prueba, logrando autenticación con la cuenta demo, modo de transferencia y cierre de sesión correcto [5]. Esta verificación confirma que las reglas outbound y masquerading (SNAT) configuradas en Endian Community Firewall permiten el tráfico FTP desde la LAN hacia RED. Desde el punto de vista de la seguridad perimetral, demuestra el control granular del tráfico saliente manteniendo la política de denegación por defecto para conexiones no autorizadas.

6.10 FTP DESDE DMZ → WAN

Figura 36.
Verificación de comunicación FTP desde DMZ a WAN



Fuente: Autoría propia.

La figura presenta la prueba de conectividad FTP saliente desde un servidor en la zona DMZ (ORANGE) hacia Internet (WAN). Mediante el comando ftp test.rebex.net se estableció una conexión exitosa utilizando la cuenta demo, completando correctamente la autenticación y el cierre de sesión [5]. Esta verificación confirma que las reglas outbound configuradas en Endian Community Firewall permiten el tráfico FTP desde la DMZ hacia RED. Desde el punto de vista de la seguridad perimetral, demuestra el control granular del tráfico saliente manteniendo la política de denegación por defecto para conexiones no autorizadas.

7 CONCLUSIONES.

La práctica de implementación de seguridad perimetral en GNU/Linux mediante Endian Firewall permitió validar la segmentación de zonas LAN, DMZ y WAN, aplicando el principio de mínimo privilegio en la gestión de servicios críticos. Las pruebas confirmaron la correcta aplicación de reglas NAT y políticas de firewall, garantizando conectividad controlada y ocultamiento de la topología interna frente a redes externas.

El despliegue de servicios HTTP y FTP en la DMZ evidenció la importancia de habilitar únicamente los protocolos necesarios, mientras se bloquean mecanismos de reconocimiento como ICMP. Esta configuración fortaleció la seguridad perimetral y demostró la efectividad del modelo stateful de iptables en la administración de tráfico.

La verificación mediante comandos y pruebas de conectividad consolidó competencias en administración de firewalls y resaltó la relevancia de documentar evidencias técnicas como parte del proceso académico. Sin embargo, se identificó la necesidad de mejorar la estructura del artículo, ajustando formato, referencias y equilibrio entre texto e imágenes para cumplir plenamente con los estándares IEEE.

Finalmente, se recomienda ampliar las pruebas hacia escenarios de alta disponibilidad y monitoreo avanzado, con el fin de consolidar un marco de seguridad perimetral más robusto y alineado con las mejores prácticas internacionales.

8 REFERENCIAS

[1] Linux Professional Institute. (2022). Tema 102: Comandos GNU y Unix. LPIC-1 Exam 101. Recuperado de https://learning.lpi.org/es/learning-materials/101-500/102/

[2] Canonical. (2023). Help Ubuntu. Ubuntu Documentation. Recuperado de https://help.ubuntu.com/

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

[4] Oracle Corporation. (2020). Oracle VM VirtualBox User Manual. VirtualBox Documentation. Recuperado de https://www.virtualbox.org/manual/

[5] Endian. (2016). Endian UTM 3.2 Reference Manual. Recuperado de http://docs.endian.com/3.2/utm/index.html

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

[7] Cervelión, Á. J. (2023). Instalación de Nagios Core 4.4 en Ubuntu 22.04 [Objeto Virtual de Información OVI]. Repositorio Institucional UNAD. Recuperado de https://repository.unad.edu.co/handle/10596/54230

[8] Hernandez, P. F., & Sánchez, J. (2022). Monitoreo y administración de sistemas Linux [Objeto Virtual de Información OVI]. Repositorio Institucional UNAD. Recuperado de https://repository.unad.edu.co/handle/10596/53211

[9] Jiménez, J. H. (2016). Shell Script para Bash [Objeto Virtual de Información OVI]. Repositorio Institucional UNAD. Recuperado de https://repository.unad.edu.co/handle/10596/9758

[10] Hernández, P. F., & Sánchez, J. (2022). *Servidores para administración remota y compartir recursos* [Objeto Virtual de Información OVI]. Repositorio Institucional UNAD. Recuperado de https://repository.unad.edu.co/handle/10596/53212