GUÍA COMPLETA PARA CONFIGURAR ENDIAN EN VIRTUALBOX: IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Andres Eduardo Nuñez Muñoz
e-mail: aenunezm@unadvirtual.edu.co
Cesar Orlando Giraldo Ricaurte
e-mail: cogiraldor@unadvirtual.edu.co
Cristhian David Saldarriaga
e-mail: cdsaldarriaga@unadvirtual.edu.co
Maria Valentina Saac Montaño
e-mail: mvsaacm@unadvirtual.edu.co
Yurany Calvache Samboni
e-mail: ycalvaches@unadvirtual.edu.co

RESUMEN: *Este artículo presenta el diseño, implementación y verificación de una infraestructura de seguridad perimetral basada en Endian Firewall Community (EFW) desplegada sobre Oracle VirtualBox. Se describe un laboratorio de red virtualizado que replica un escenario corporativo real con tres zonas de seguridad diferenciadas: LAN (zona verde), DMZ (zona naranja) y WAN (zona roja). A lo largo de cinco temáticas progresivas se aborda la instalación y configuración del sistema UTM (Unified Threat Management), la configuración de NAT tanto de salida (SNAT/Masquerading) como de entrada (DNAT/Port Forwarding), el control granular del tráfico de salida con bloqueo de ICMP, la implementación de reglas de acceso inter-zona y finalmente el despliegue de un proxy HTTP no transparente con autenticación de usuarios, listas negras y registros de auditoría. Los resultados demuestran que la virtualización permite replicar fielmente escenarios de seguridad empresarial con recursos mínimos, y que Endian Firewall ofrece una plataforma robusta para la enseñanza y práctica de conceptos avanzados de seguridad de redes.*

PALABRAS CLAVE: DMZ, Endian Firewall, NAT, Seguridad perimetral.

ABSTRACT: This paper presents the design, implementation and verification of a perimeter security infrastructure based on Endian Firewall Community (EFW) deployed on Oracle VirtualBox. A virtualized network laboratory is described that replicates a real corporate scenario with three differentiated security zones: LAN (green zone), DMZ (orange zone) and WAN (red zone). Across five progressive topics, the article covers the installation and configuration of the UTM (Unified Threat Management) system, NAT configuration both outbound (SNAT/Masquerading) and inbound (DNAT/Port Forwarding), granular outbound traffic control with ICMP blocking, inter-zone access rule implementation, and finally the deployment of a non-transparent HTTP proxy with user authentication, blacklists and audit logs. Results demonstrate that virtualization faithfully replicates enterprise security scenarios with minimal resources, and that Endian Firewall provides a robust platform for teaching and practicing advanced network security concepts.

KEYWORDS: DMZ, Endian Firewall, NAT, Perimeter security.

1 INTRODUCCIÓN

La seguridad perimetral constituye uno de los pilares fundamentales en la arquitectura de redes empresariales modernas. La proliferación de amenazas cibernéticas, la complejidad de los entornos híbridos y la necesidad de cumplimiento normativo han elevado el rol de los sistemas de gestión unificada de amenazas (UTM) a un lugar central en la estrategia de protección de la información [1].

Endian Firewall Community (EFW) es una distribución GNU/Linux especializada en seguridad perimetral, derivada de IPCop y basada en Red Hat, que consolida en un único appliance las funciones de firewall con inspección de paquetes, proxy web, sistema de detección y prevención de intrusiones (IDS/IPS), soporte de redes privadas virtuales (VPN) y filtrado de contenido [2]. Su filosofía de segmentación por colores (verde, naranja, roja) permite implementar de forma didáctica y efectiva el modelo de zonas de confianza diferenciada que recomienda la industria.

El entorno virtualizado con Oracle VirtualBox ofrece una plataforma accesible para la enseñanza y práctica de estos conceptos, permitiendo reproducir con fidelidad la topología de redes corporativas sin requerir equipamiento físico especializado [3]. Esta aproximación pedagógica facilita la experimentación, el análisis de fallos y la comprensión profunda de los mecanismos de control de tráfico.

El presente artículo describe la implementación completa de un laboratorio de seguridad perimetral estructurado en cinco temáticas: (i) instalación y configuración del sistema Endian con sus tres interfaces de red, (ii) configuración de NAT para habilitar la comunicación entre zonas e Internet, (iii) control del tráfico de salida incluyendo el bloqueo de ICMP, (iv) implementación de reglas de acceso inter-zona basadas en el principio de mínimo privilegio, y (v) despliegue de un proxy HTTP no transparente con autenticación, perfiles de usuario y listas de bloqueo de contenido.

2 MARCO TEÓRICO

2.1 SISTEMAS UTM Y SEGMENTACIÓN DE RED

Los sistemas UTM (Unified Threat Management) integran múltiples funciones de seguridad en una única plataforma, reduciendo la complejidad operativa y los costos de gestión en comparación con soluciones distribuidas [4]. La segmentación de red mediante zonas de confianza diferenciada constituye la base arquitectónica de estos sistemas. En el modelo de Endian Firewall se definen tres zonas principales:

- **Zona Verde (LAN):** Red interna de confianza donde residen los equipos de usuarios finales. Posee el nivel más alto de privilegio y puede iniciar conexiones hacia las demás zonas sujeto a políticas.

- **Zona Naranja (DMZ — Demilitarized Zone):** Zona de acceso controlado donde se alojan los servidores que deben ser accesibles desde Internet (servidores web, FTP, correo). Actúa como buffer entre la red interna y el exterior, de modo que si un servidor de la DMZ es comprometido, el atacante no obtiene acceso directo a la LAN [5].

- **Zona Roja (WAN):** Representa la red externa no confiable, típicamente Internet.

2.2 NETWORK ADDRESS TRANSLATION (NAT)

NAT es un mecanismo que permite traducir las direcciones IP privadas de una red interna a una o más direcciones IP públicas para la comunicación con redes externas [6]. Sus variantes más relevantes en el contexto de este laboratorio son:

- **SNAT (Source NAT / Masquerading):** Modifica la dirección IP de origen de los paquetes que salen hacia la WAN, permitiendo que múltiples hosts internos compartan una única dirección IP pública. Es el mecanismo que habilita el acceso a Internet desde la LAN y la DMZ.

- **DNAT (Destination NAT / Port Forwarding):** Modifica la dirección IP de destino de los paquetes entrantes, redirigiendo el tráfico que llega a la IP pública del firewall hacia un servidor específico de la DMZ. Permite la publicación controlada de servicios internos.

2.3 CONTROL DE TRÁFICO CON IPTABLES

Linux implementa su subsistema de filtrado de paquetes a través de Netfilter, gestionado desde el espacio de usuario mediante la herramienta iptables [7]. Las cadenas principales relevantes para el laboratorio son:

- **FORWARD:** Procesa los paquetes que atraviesan el sistema (de una interfaz a otra), controlando el tráfico inter-zona.

- **PREROUTING:** Se aplica antes de la decisión de enrutamiento; aquí se configuran las reglas DNAT.

- **POSTROUTING:** Se aplica después de la decisión de enrutamiento; aquí se configuran las reglas SNAT/Masquerading.

El Protocolo de Mensajes de Control de Internet (ICMP) juega un papel especial en la seguridad de redes. Si bien es indispensable para diagnóstico (ping, traceroute), también puede ser explotado para reconocimiento de red, ataques de denegación de servicio y tunneling de datos [8]. El bloqueo selectivo de tipos ICMP (Tipo 8: Echo Request; Tipo 30: Traceroute) es una práctica recomendada para reducir la superficie de ataque.

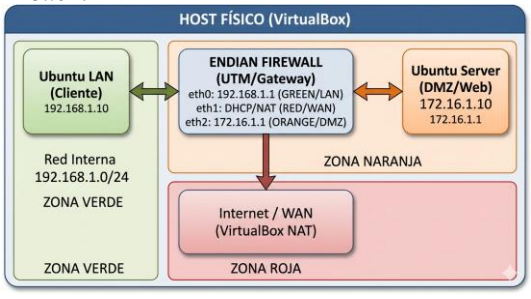
2.4 PROXY HTTP Y AUTENTICACIÓN

Un servidor proxy HTTP actúa como intermediario entre los clientes de una red y los servidores web en Internet. El proxy no transparente requiere que los clientes lo configuren explícitamente en sus aplicaciones, lo que permite implementar autenticación individual por usuario o grupo [9]. Squid es el motor de proxy utilizado por Endian Firewall, ampliamente reconocido por su robustez, soporte de listas de control de acceso (ACL) complejas, capacidad de caché y extensas opciones de registro (logging) [10].

3 TOPOLOGÍA SUGERIDA DEL LABORATORIO

La infraestructura virtualizada implementada en este laboratorio reproduce una topología de red corporativa de tres zonas sobre un único host físico con Oracle VirtualBox, tal como se ilustra en la Figura 1.

Figura 1.
Topología de red del laboratorio virtualizado con Endian Firewall.



Fuente: Autoría Propia.

4 METODOLOGÍA DE IMPLEMENTACIÓN

El laboratorio se desarrolló en cinco fases secuenciales y acumulativas, donde cada fase constituye un prerrequisito para la siguiente. Esta progresión permite verificar la correcta implementación de cada capa de seguridad de forma aislada antes de añadir complejidad.

4.1 TEMÁTICA 1: INSTALACIÓN Y CONFIGURACIÓN DE ENDIAN FIREWALL

1) Preparación del entorno VirtualBox

Antes de crear las máquinas virtuales, se configuraron dos redes host-only en VirtualBox para simular las zonas LAN y DMZ. Es crítico deshabilitar el servidor DHCP de VirtualBox en ambas redes, ya que Endian actuará como servidor DHCP para la zona LAN:

- **vboxnet0:** 192.168.2.0/24 (Zona Verde / LAN) — DHCP VirtualBox: DESHABILITADO.

- **vboxnet1:** 192.168.1.0/24 (Zona Naranja / DMZ) — DHCP VirtualBox: DESHABILITADO.

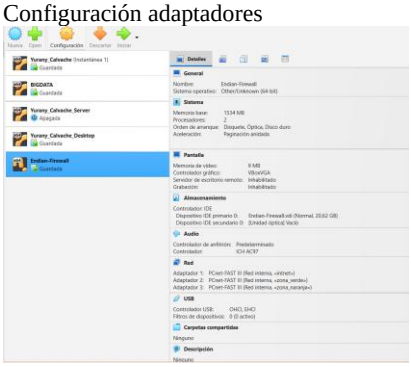
2) Configuración de la VM Endian Firewall

La máquina virtual de Endian requiere tres adaptadores de red configurados en el orden exacto mostrado a continuación, ya que el sistema detecta las interfaces según el índice del adaptador en VirtualBox:

- **Adaptador 1** → eth0 (GREEN/LAN): Red solo-anfitrión, vboxnet0
- **Adaptador 2** → eth1 (RED/WAN): NAT (para acceso a Internet desde el host)
- **Adaptador 3** → eth2 (ORANGE/DMZ): Red solo-anfitrión, vboxnet1

El orden incorrecto de los adaptadores es el error más común en esta fase: intercambiar la WAN con la LAN crearía un agujero de seguridad severo donde el tráfico externo no confiable sería tratado como tráfico interno.

Figura 2.
Configuración adaptadores



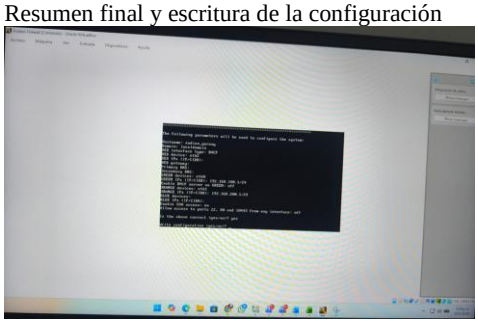
Fuente: Autoría Propia.

3) Proceso de instalación

La instalación se realiza desde la ISO de EFW Community 3.x, seleccionando particionado automático del disco virtual de 20 GB. Tras la instalación, el sistema solicita la configuración inicial de interfaces mediante un asistente en consola:

- **GREEN (eth0):** IP 192.168.2.15, Máscara 255.255.255.0
- **RED (eth1):** Tipo DHCP (VirtualBox NAT asigna 10.0.2.15)
- **ORANGE (eth2):** IP 192.168.1.15, Máscara 255.255.255.0

Figura 3.
Resumen final y escritura de la configuración



Fuente: Autoría Propia.

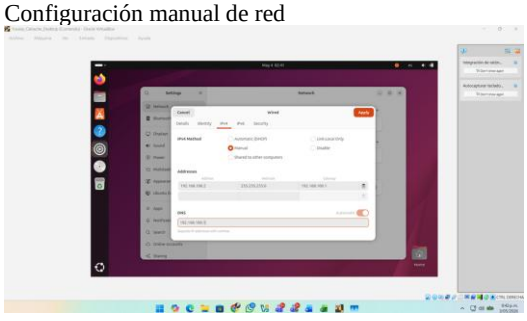
4) Configuración de los servidores en la DMZ

En Ubuntu Server DMZ se configuró una IP estática mediante Netplan y se instalaron los servicios web y FTP:

```
# /etc/netplan/00-installer-config.yaml
network:
  version: 2
  ethernets:
    enp0s3:
      addresses:
        - 192.168.1.20/24
      gateway4: 192.168.1.0
      nameservers:
        addresses: [8.8.8.8]
      dhcp4: false
```

```
sudo apt install apache2 vsftpd -y
sudo systemctl enable --now apache2 vsftpd
```

Figura 4.
Configuración manual de red



Fuente: Autoría Propia.

5) Verificación de la Temática 1

La validación se realizó comprobando la conectividad ICMP entre todas las zonas desde la consola de Endian y confirmando el acceso a la interfaz web de administración en https://192.168.1.1:10443 desde el cliente LAN.

Figura 5.
Panel de control principal de Endian Firewall

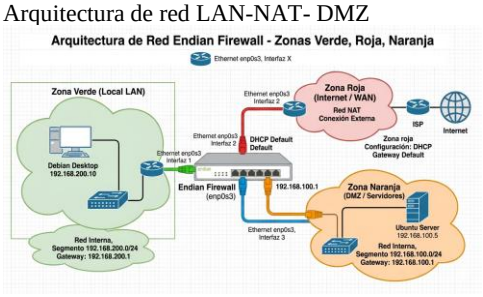
Fuente: Autoría Propia.

4.2 TEMÁTICA 2: CONFIGURACIÓN NAT

1) SNAT — NAT de Salida (Masquerading)

Se configuraron dos reglas de Outbound NAT en la interfaz web de Endian (Firewall → NAT) para habilitar el acceso a Internet desde ambas zonas internas:

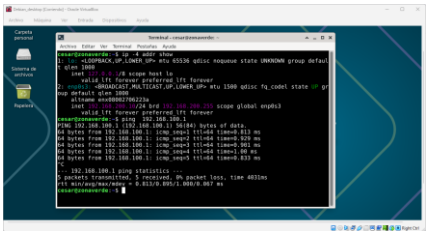
Figura 6.
Arquitectura de red LAN-NAT- DMZ



Fuente: Autoría Propia.

En la figura 6, validamos la ip estática asignada con el comando ip -4 addr show y posteriormente validamos las comunicaciones desde el servidor zona verde (192.168.200.10) hacia la red zona naranja (192.168.100.1), con el comando ping 192.168.100.1 y se evidencia que no se pierde ningún paquete.

Figura 7.
Validación comunicación entre redes



Fuente: Autoría Propia.

2) DNAT — NAT de Entrada (Port Forwarding)

Para publicar los servicios del servidor DMZ hacia Internet, se configuraron reglas de Inbound NAT (Firewall → Port Forwarding):

Tabla 1.
Reglas de NAT

Adaptador	Tipo de Red	Nombre red	Ethernet enp0s3	Ip	Gateway
1	Red Interna	Zona verde	**Debian desktop** 192.168.2.0/24	192.168.200.10	192.168.200.1
2	NAT	Zona roja	**Endian** DHCP	Default	Default
3	Red Interna	Zona naranja	**Ubuntu server** 192.168.1.0/24	192.168.100.5	192.168.100.1

Nota. Esta tabla muestra la configuración de las zonas, adaptadores e IP utilizadas en el laboratorio virtualizado con Endian Firewall. Fuente. Autoría Propia.

El panel administrativo de Endian refleja estas reglas como entradas DNAT que redirigen el tráfico de los puertos 80, 21, 22 hacia la IP del servidor en la DMZ.

Figura 8.
Creación reglas de Nateo entre redes

Fuente: Autoría Propia

4.3 TEMÁTICA 3: PERMITIR SERVICIOS DMZ Y DENEGAR ICMP

Esta fase aplica el principio de mínimo privilegio al tráfico de salida de la DMZ: el servidor web solo necesita HTTP y FTP para comunicarse hacia Internet; cualquier otro tipo de tráfico, especialmente ICMP, debe ser bloqueado.

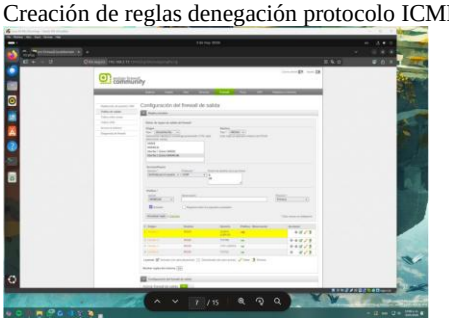
1) Justificación del bloqueo de ICMP

El protocolo ICMP, aunque útil para diagnóstico de red, puede ser explotado de múltiples formas [8]:

- **Reconocimiento:** Descubrir hosts activos y topología de red mediante ping sweeps.
- **DoS:** Ataques de inundación ICMP (ping flood) contra servicios críticos.
- **Tunneling:** Exfiltración de datos encubierta dentro de paquetes ICMP (herramientas como ptunnel).

Los tipos ICMP críticos a bloquear son el Tipo 8 (Echo Request, origen del ping) y el Tipo 30 (Traceroute, usado para mapeo de rutas).

Figura 9.
Creación de reglas denegación protocolo ICMP



Fuente: Autoría Propia.

2) Reglas configuradas en Outbound Traffic

El orden de procesamiento de reglas es determinante; las restricciones deben preceder a los permisos, a diferentes servicios (ftp, ssh, entre otros) y puertos (21, 22, 80, 10443, entre otros), desde la zona naranja DMZ, como se detallan en la tabla 2

Tabla 2.
Reglas de tráfico de salida — Zona DMZ

Origen	Destino	Protocolo	Puerto /Tipo	Acción	Comentario
Orange	Any	ICMP	Tipo 8 (Echo Req.)	DROP	Bloquear ping saliente
Orange	Any	ICMP	Tipo 30 (Traceroute)	DROP	Bloquear traceroute
Orange	Any	TCP	80 (HTTP)	ACCEPT	Permitir HTTP
Orange	Any	TCP	21 (FTP)	ACCEPT	Permitir FTP

Nota. Esta tabla muestra las reglas de tráfico de salida configuradas para la zona DMZ en Endian Firewall. Fuente. Autoría Propia.

Figura 10.
Reglas de salida

Fuente: Autoría Propia.

3) Implementación por consola con iptables

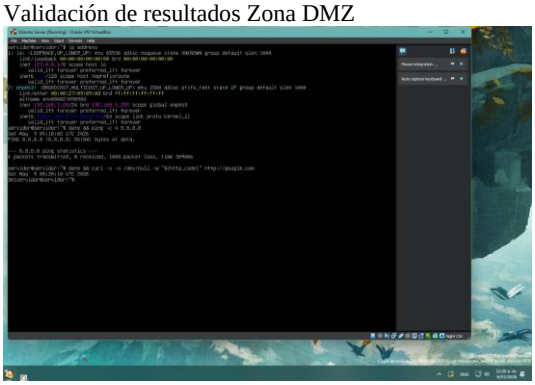
Cuando la interfaz web no permite granularidad por tipo ICMP, las reglas se pueden insertar directamente:

```
# Bloquear ICMP Echo Request desde DMZ

iptables -I FORWARD -s 192.168.1.0/24 -p icmp --icmp-type 8 -j DROP

# Bloquear ICMP Traceroute desde DMZ

iptables -I FORWARD -s 192.168.1.0/24 -p icmp --icmp-type 30 -j DROP
```

4) Verificación

```
# Desde Ubuntu-Server-DMZ — debe fallar:

ping -c 4 8.8.8.8

# Resultado esperado: 100% packet loss

# Desde Ubuntu-Server-DMZ — debe funcionar:

curl -I http://google.com

# Resultado esperado: HTTP/1.1 301
```

Figura 11.
Validación de resultados Zona DMZ



Fuente: Autoría Propia.

4.4 TEMÁTICA 4: REGLAS DE ACCESO INTER-ZONA

Las reglas inter-zona definen la matriz de comunicación entre las zonas de seguridad, implementando el modelo de confianza diferenciada que fundamenta el diseño de la DMZ.

1) Matriz de tráfico permitido

Tabla 3.
Matriz de acceso Inter-Zona

Origen / Destino	LAN (GREEN)	DMZ (ORANGE)	WAN (RED)
lan (green)	—	http (80), ftp (21)	http (80), ftp (21)
dmz (orange)	bloqueado ✗	—	http (80), ftp (21)
wan (red)	bloqueado ✗	http (80), ftp (21)	—

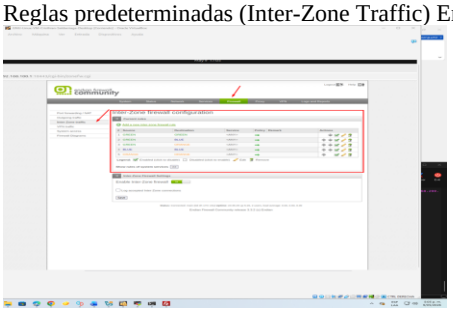
Nota. Esta tabla presenta la matriz de acceso y comunicación permitida entre las zonas LAN, DMZ y WAN configuradas en Endian Firewall. Fuente. Autoría Propia.

Esta matriz implementa los siguientes principios de seguridad:

- La DMZ nunca puede iniciar conexiones hacia la LAN (contención de intrusiones).
- Internet nunca puede alcanzar la LAN directamente.
- Internet puede acceder a la DMZ únicamente en los puertos de servicio explícitamente habilitados.

2) Reglas configuradas en Endian (Inter-Zone Traffic)

Figura 12.
Reglas predeterminadas (Inter-Zone Traffic) Endian



Fuente: Autoría Propia.

Primero, notamos que la regla de la Zona Verde a la Naranja permite cualquier servicio (ANY). Esto no es un error, es una decisión de diseño basada en la confianza, como la Zona Verde es nuestra red interna segura, el Endian le otorga permiso total para administrar y consumir cualquier recurso que necesitemos del servidor en la DMZ, es decir confiamos en nuestra propia red para que use el servidor como quiera.

Tabla 4.
Reglas de acceso Inter-Zona implementadas

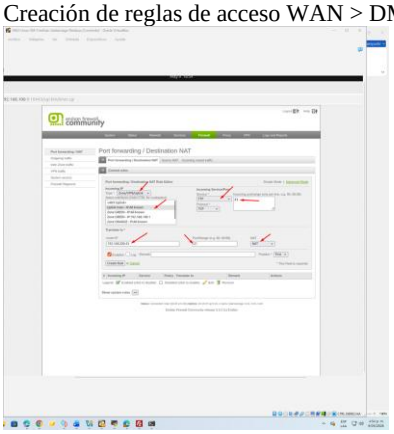
Zona Origen	Zona Destino	Protocolo	Puerto	Acción	Comentario
green	orange	tcp	80	accept	lan → dmz http
green	orange	tcp	21	accept	lan → dmz ftp
red	orange	tcp	80	accept	wan → dmz http
red	orange	tcp	21	accept	wan → dmz ftp
green	red	tcp	80	accept	lan → wan http
green	red	tcp	21	accept	lan → wan ftp
orange	red	tcp	80	accept	dmz → wan http
orange	red	tcp	21	accept	dmz → wan ftp

Nota. Esta tabla muestra las reglas de acceso inter-zona configuradas en Endian Firewall para permitir el tráfico HTTP y FTP entre las zonas LAN, DMZ y WAN. Fuente. Autoría Propia.

3) Verificación de acceso al server 22 desde la WAN hacia la DMZ

Para formalizar el acceso al servicio de transferencia de archivos, utilicé el formulario de edición de reglas de Port Forwarding en el Endian. Como se observa en la configuración, define que cualquier petición entrante por la interfaz Uplink main dirigida al puerto 21 (FTP) sea redirigida mediante una regla de DNAT hacia la dirección IP interna 192.168.200.43.

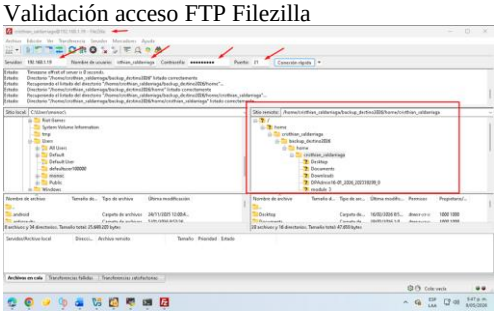
Figura 13.
Creación de reglas de acceso WAN > DMZ vía web



Fuente: Autoría Propia.

Se validó el ingreso del servicio FTP desde la zona WAN hacia la DMZ utilizando el cliente FileZilla. Al configurar la conexión hacia la IP pública del firewall (192.168.1.19), se confirmó que la regla de Port Forwarding creada previamente redirige correctamente el tráfico hacia el servidor interno. La sesión exitosa en FileZilla, que permite visualizar la estructura de directorios del servidor, es la evidencia final de que el servicio de transferencia de archivos está correctamente publicado y accesible para usuarios externos bajo los parámetros de seguridad establecidos.

Figura 14.
Validación acceso FTP Filezilla



Fuente: Autoría Propia.

4) Verificación de acceso DMZ hacia WAN

Para habilitar la salida, es necesario asegurar que la zona ORANGE esté incluida como origen en las reglas de permitir HTTP (80) y HTTPS (443), ya que actualmente el firewall solo autoriza estas salidas para la zona GREEN.

Figura 15.
Creación de reglas de acceso DMZ > WAN

Fuente: Autoría Propia.

Figura 16.
Validación acceso con curl hacia google.com

Fuente: Autoría Propia.

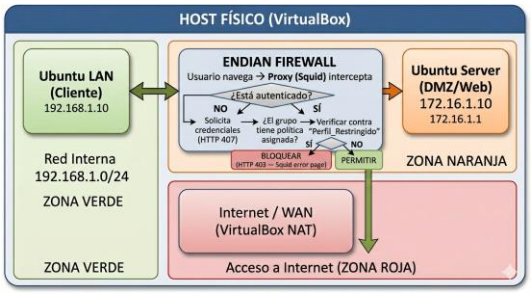
Se puede observar el resultado positivo de una prueba de conectividad realizada mediante el comando curl. Este hito no es casualidad; es el resultado directo de la correcta implementación de las reglas de tráfico en el firewall Endian, permitiendo la salida desde la Zona Naranja (DMZ) hacia la Red Externa (RED/Internet).

4.5 TEMÁTICA 5: PROXY HTTP NO TRANSPARENTE CON AUTENTICACIÓN

1) Arquitectura del proxy

Endian Firewall integra Squid como motor de proxy. La configuración no transparente requiere que el usuario configure explícitamente el proxy.

Figura 17.
Topología de red de los hosts



Fuente: Autoría Propia.

2) Configuración del proxy en Endian

En Proxy → HTTP de la interfaz web:

- **Enable HTTP proxy:** ACTIVADO
- **Transparent on GREEN:** DESACTIVADO (crucial para proxy no transparente)
- **Proxy port:** 8080
- **Log all queries:** ACTIVADO

3) Lista negra de dominios

Se creó un perfil de filtrado "Perfil_Restringido" con los siguientes dominios bloqueados, incluyendo variantes de subdominio para garantizar un bloqueo efectivo:

Tabla 5.
Dominios en lista negra

Dominio	Razón del Bloqueo
www.hotmail.com / hotmail.com / live.com / outlook.com	Webmail — distracción / fuga de información
www.youtube.com / youtube.com / googlevideo.com / ytimg.com	Streaming de video — consumo de ancho de banda
www.elnuevodia.com.co / elnuevodia.com.co	Sitio de noticias — control de contenido

Nota. Esta tabla presenta los dominios configurados en la lista negra del proxy HTTP y las razones de su bloqueo en la red.
Fuente. Autoría Propia.

Es importante notar que YouTube utiliza múltiples dominios para servir su contenido (googlevideo.com para video, ytimg.com para miniaturas), por lo que el bloqueo efectivo requiere incluir todos los dominios auxiliares.

4) Gestión de usuarios desde consola

Crear archivo de contraseñas y agregar usuario: htpasswd -c /etc/squid/passwd estudiante1

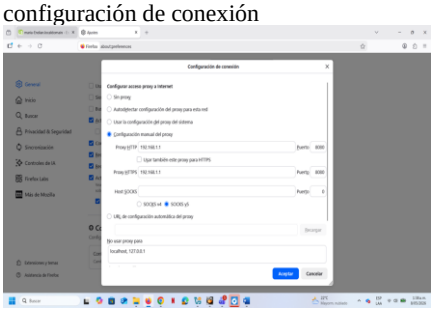
Agregar usuarios adicionales (sin -c para no sobreescribir):
htpasswd /etc/squid/passwd estudiante2

Verificar estado del servicio Squid:
date && /etc/init.d/squid status.

Monitorear accesos en tiempo real:
tail -f /var/log/squid/access.log.

5) Configuración del navegador en el cliente LAN

Figura 18.
Configuración de proxy en el navegador Firefox: configuración de conexión



Fuente: Autoría Propia.

En esta imagen, se presenta la configuración del proxy en el navegador Firefox. Dentro de Configurar Proxy, se seleccionó la opción de configuración manual de proxy y se ingresó la IP 192.168.1.1 con el puerto 8080 en el proxy HTTP y HTTPS. Además, en la opción No usar proxy para, se ingresó localhost y 127.0.0.1. Para guardar los cambios, se dio clic en el botón Aceptar. Este paso es importante para un proxy no transparente, ya que permite que el proxy configurado en Endian funcione en el navegador. Sin esta configuración, ni la autenticación ni el bloqueo de las páginas funcionarían correctamente.

En Firefox: Preferencias → Configuración de red → Configuración manual de proxy

- **HTTP Proxy:** 192.168.1.1 / Puerto: 8080.
- **HTTPS Proxy:** 192.168.1.1 / Puerto: 8080.
- **Sin proxy para**: localhost, 127.0.0.1.

6) Interpretación de los logs de Squid

El archivo /var/log/squid/access.log registra cada transacción con información de auditoría completa:

Acceso denegado (lista negra):
1714389600 192.168.1.10 TCP_DENIED/403 GET http://www.youtube.com/ - HIER_NONE/-

Figura 19.
Ingreso a sitio bloqueado Hotmail

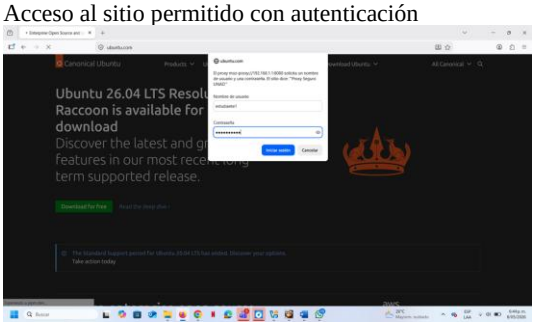
Fuente: Autoría Propia

En esta imagen, se presenta la prueba de acceso con autenticación. En este caso, después de ingresar el usuario y contraseña. Ingresó correctamente a la página de Ubuntu.

Acceso permitido con autenticación:
1714389605 192.168.1.10 TCP_MISS/200 GET http://www.ubuntu.com/ estudiante1 HIER_DIRECT/91.189.91.42

El campo estudiante1 en la segunda entrada confirma que la autenticación está funcionando correctamente y permite la trazabilidad de la actividad por usuario individual.

Figura 20.
Acceso al sitio permitido con autenticación



Fuente: Autoría Propia

En esta imagen, se presenta la prueba de acceso con autenticación. En este caso, se ingresó a la página de Ubuntu mediante el enlace http://www.ubuntu.com. Se ingresó el usuario y contraseña configurados en Endian y se dio clic en Iniciar sesión.

Figura 21.
Ingreso a la página después de la autenticación

Fuente: Autoría Propia

En esta imagen, se presenta la prueba de acceso con autenticación. En este caso, después de ingresar el usuario y contraseña. Ingresó correctamente a la página de Ubuntu.

5 RESULTADOS Y DISCUSIÓN

5.1 VERIFICACIÓN INTEGRAL DEL SISTEMA

La Tabla 6 resume los resultados de las pruebas de verificación ejecutadas al completar las cinco fases de implementación:

Tabla 6.
Resultados de verificación del laboratorio

Prueba	Escenario	Resultado Esperado	Resultado Obtenido
1	LAN → DMZ (HTTP, puerto 80)	200 OK	PASS
2	LAN → WAN (HTTP, Google)	200/301 OK	PASS
3	DMZ → WAN (HTTP)	200 OK	PASS
4	WAN → DMZ (HTTP, DNAT)	200 OK	PASS
5	DMZ → Any (ICMP ping)	100% packet loss	PASS
6	WAN → LAN (cualquier tráfico)	Bloqueado	PASS
7	DMZ → LAN (cualquier tráfico)	Bloqueado	PASS
8	Proxy: acceso con autenticación	Página carga tras credenciales	PASS
9	Proxy: hotmail.com (lista negra)	Página de error Squid	PASS
10	Proxy: youtube.com (lista negra)	Página de error Squid	PASS
11	LAN → DMZ (FTP, puerto 21)	Login exitoso	PASS
12	NAT Masquerade LAN→WAN	IP origen = eth1 Endian	PASS

Nota. Esta tabla muestra los resultados de verificación de las configuraciones implementadas en el laboratorio con Endian Firewall. Fuente. Autoría Propia.

5.2 ANÁLISIS DE ERRORES COMUNES

Durante la implementación se identificaron los errores más frecuentes y sus correcciones:

1) Orden de adaptadores de red en VirtualBox: La asignación incorrecta del tipo de red (NAT vs Host-Only) a los adaptadores produce que Endian asigne las zonas de confianza incorrectamente, exponiendo la LAN como WAN o viceversa. La verificación mediante ip addr show en la consola de Endian es el mecanismo de detección inmediata.

2) DHCP de VirtualBox habilitado en redes Host-Only: Genera conflictos con el servidor DHCP de Endian, produciendo asignaciones de IP inconsistentes en los clientes. La solución es deshabilitar el DHCP de VirtualBox antes de iniciar las VMs.

3) Orden de reglas en el firewall: Una regla ACCEPT genérica posicionada antes de las reglas DROP hace que estas últimas nunca se evalúen. El principio es: las reglas más restrictivas y específicas primero.

4) Proxy no transparente sin configuración en el navegador: Si el usuario no configura el proxy manualmente, el tráfico no pasa por Squid y el filtrado y la autenticación no tienen efecto. Esta es la diferencia arquitectónica fundamental con el proxy transparente.

5) Bloqueo incompleto de YouTube: YouTube sirve contenido desde múltiples dominios (googlevideo.com, ytimg.com). Bloquear únicamente youtube.com resulta en que el sitio es accesible parcialmente. El bloqueo efectivo requiere incluir todos los dominios auxiliares en la lista negra.

5.3 CONSIDERACIONES DE SEGURIDAD ADICIONALES

El laboratorio implementado representa una configuración funcional pero no exhaustiva. En un entorno de producción se deben considerar adicionalmente:

- **SSL Inspection (SSL Bumping):** El proxy HTTP estándar no puede inspeccionar el contenido de conexiones HTTPS (puerto 443). YouTube y la mayoría de servicios modernos usan exclusivamente HTTPS, lo que requiere configuración adicional de SSL Bumping en Squid con un certificado raíz de confianza.

- **Módulo nf_conntrack_ftp:** FTP en modo activo requiere la carga explícita de este módulo del kernel para que el seguimiento de conexiones (connection tracking) funcione correctamente con el protocolo.

- **Persistencia de reglas iptables:** Las reglas configuradas manualmente por consola se pierden al reiniciar el sistema. En Endian, la persistencia se gestiona principalmente desde la interfaz web, que regenera el conjunto de reglas al iniciar.

6 CONCLUSIONES

Este trabajo ha presentado la implementación completa de una infraestructura de seguridad perimetral basada en Endian Firewall Community sobre un entorno virtualizado con VirtualBox. Las conclusiones principales son:

1. La virtualización es viable para la enseñanza de seguridad de redes: El laboratorio demuestra que VirtualBox permite reproducir fielmente topologías de red corporativas de tres zonas con recursos de hardware convencionales, facilitando la experimentación sin riesgo sobre infraestructura crítica real.

2. La segmentación por zonas de confianza es la base de la seguridad perimetral: La correcta separación en zonas

verde, naranja y roja, con políticas de acceso diferenciadas, limita eficazmente el radio de acción de un atacante que logre comprometer un servidor en la DMZ, impidiéndole el acceso directo a la red interna.

3. El principio de mínimo privilegio debe aplicarse a todas las zonas: Limitar el tráfico de salida de la DMZ exclusivamente a los protocolos necesarios para su función (HTTP y FTP) y bloquear ICMP reduce significativamente la superficie de ataque y las posibilidades de reconocimiento y exfiltración.

4. El proxy no transparente con autenticación aporta trazabilidad y control granular: A diferencia del proxy transparente, el modelo no transparente permite identificar individualmente cada usuario que accede a Internet, facilitando la auditoría, la aplicación de políticas por grupo y la investigación de incidentes.

5. El orden de las reglas de firewall es crítico: La secuencia de evaluación de las reglas determina el comportamiento efectivo del sistema. Las reglas restrictivas deben preceder a las permisivas, y la verificación mediante contadores de iptables permite confirmar que el tráfico sigue los caminos esperados.

Como trabajo futuro se propone la integración del módulo IDS/IPS de Endian (basado en Snort/Suricata) para detección de amenazas en tiempo real, la configuración de VPN para acceso remoto seguro y la implementación de SSL Inspection para extender el filtrado de contenido a las comunicaciones HTTPS.

7 REFERENCIAS

A. Daya, "Network Security: History, Importance, and Future," University of Florida Department of Electrical and Computer Engineering, 2013.

Endian GmbH, "Endian Firewall Community Documentation," Endian.com, 2023. [Online]. Disponible en: https://www.endian.com/community/

Oracle Corporation, "Oracle VM VirtualBox User Manual," Oracle VirtualBox, versión 6.1, 2021. [Online]. Disponible en: https://www.virtualbox.org/manual/

E. Messmer, "UTM Products Offer Comprehensive Security," Network World, 2009.

W. Stallings y L. Brown, Computer Security: Principles and Practice, 4th ed. Pearson, 2018, pp. 742–780.

K. Egevang y P. Francis, "The IP Network Address Translator (NAT)," RFC 1631, Internet Engineering Task Force (IETF), mayo 1994.

H. Welte y P. Russel, "The netfilter.org project," netfilter.org, 2012. [Online]. Disponible en: https://www.netfilter.org/

J. Postel, "Internet Control Message Protocol," RFC 792, USC/Information Sciences Institute, septiembre 1981.

R. Fielding et al., "Hypertext Transfer Protocol — HTTP/1.1," RFC 2616, IETF, junio 1999.

D. Wessels, Squid: The Definitive Guide. O'Reilly Media, 2004.

M. Rash, Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort. No Starch Press, 2007.

W. R. Cheswick, S. M. Bellovin y A. D. Rubin, Firewalls and Internet Security: Repelling the Wily Hacker, 2nd ed. Addison-Wesley, 2003.

T. Limoncelli, C. Hogan y S. Chalup, The Practice of System and Network Administration, 3rd ed. Addison-Wesley, 2016.

National Institute of Standards and Technology (NIST), "Guidelines on Firewalls and Firewall Policy," Special Publication 800-41 Rev. 1, septiembre 2009.

Canonical Ltd., "Ubuntu Server Guide — Network Configuration," Ubuntu Documentation, 2023. [Online]. Disponible en: https://ubuntu.com/server/docs/network-configuration