SEGURIDAD PERIMETRAL CON SEGMENTACIÓN INTERNA: CONFIGURACIÓN NAT Y ACCESIBILIDAD DE SERVICIOS

Angie Tatiana Acevedo Moreno
e-mail: atacevedom@unadvirtual.edu.co
Dayana Vanessa Moreno Montañez
e-mail: dvmorenomo@unadvirtual.edu.co
Diego Ostos Cusba
e-mail: dostosc@unadvirtual.edu.co
Víctor Manuel Rodríguez Acero
e-mail: vmrodriguezac@unadvirtual.edu.co

RESUMEN: *El presente documento detalla la instalación, configuración e implementación de Endian Firewall sobre una máquina virtual en VirtualBox, ejecutándose en tres fases principales. En primer lugar, se realiza el despliegue del sistema operativo y la estructuración de la red mediante tres zonas de seguridad aisladas: la zona verde para la red interna (LAN), la zona roja con salida a Internet (WAN) y la zona naranja destinada a los servidores (DMZ). En segundo lugar, se configuran las reglas de traducción de direcciones de red (NAT) para permitir la comunicación bidireccional entre la LAN y la WAN, asegurando además el acceso a Internet de la DMZ mediante la verificación de puertos de enlace. Finalmente, se habilitan y exponen los servicios esenciales alojados en la zona DMZ hacia las demás zonas de la infraestructura, validando la conectividad y el correcto flujo de tráfico.*

PALABRAS CLAVE: DMZ, Endian, LAN, WAN.

1 INTRODUCCIÓN

La seguridad perimetral se ha convertido en un pilar fundamental para la protección de infraestructuras de red en entornos corporativos, especialmente cuando se requiere garantizar la integridad y confidencialidad de bases de datos y aplicaciones críticas alojadas en servidores. En este contexto, el presente artículo documenta la implementación de una solución de firewall basada en GNU/Linux Endian Firewall Community (EFW), configurada sobre máquinas virtuales en Oracle VirtualBox, con el objetivo de establecer una arquitectura de red segmentada en tres zonas diferenciadas: Zona Verde (LAN) para la red interna, Zona Roja (WAN) para el acceso a Internet, y Zona Naranja (DMZ) [3] para alojar servidores públicos como servidores web y bases de datos.

La metodología empleada abarca desde la descarga e instalación de Endian Firewall, la configuración de tres adaptadores de red con direccionamientos específicos (LAN: 192.168.0.0/24 con gateway 192.168.0.1; DMZ: 192.168.20.0/24 con gateway 192.168.20.1), hasta la verificación de conectividad y servicios mediante comandos en consola con registro de fecha y hora. Los resultados obtenidos demuestran una segmentación efectiva que permite aislar los servidores públicos de la red interna, reduciendo la superficie de ataque y estableciendo una base sólida para la implementación de políticas de filtrado, NAT y proxy en las temáticas subsiguientes [1].

2 DESARROLLO DE LA TEMÁTICA 1

2.1 INSTALACIÓN DE ENDIAN FIREWALL

La implementación de Endian Firewall Community versión 3.3.2 se realizó sobre Oracle VirtualBox, siguiendo el esquema de direccionamiento presentado en la Tabla 1.

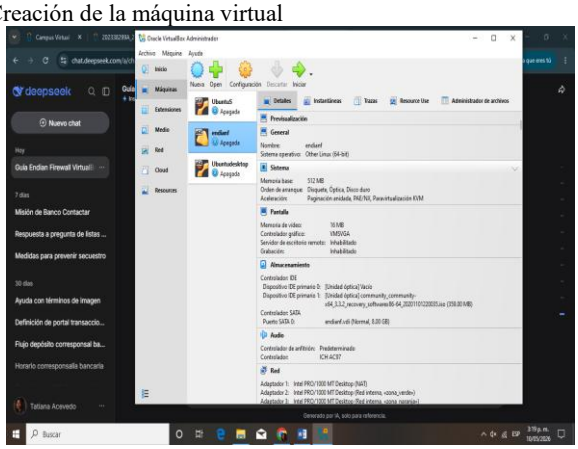
Para dar inicio a la implementación del firewall perimetral, se procedió con la adquisición de la imagen ISO correspondiente a la distribución Endian Firewall Community, específicamente la versión 3.3.2, la cual fue descargada directamente desde el repositorio oficial del proyecto. Posteriormente, se llevó a cabo el despliegue de este sistema operativo sobre una infraestructura virtualizada haciendo uso de Oracle VM VirtualBox como plataforma de virtualización.

2.2 CREACIÓN DE LA MÁQUINA VIRTUAL

Dentro del entorno de VirtualBox, se creó una nueva máquina virtual destinada a alojar el firewall, asignándole los siguientes recursos hardware:

- Denominación: Endian-Firewall
- Sistema base: Linux
- Variante: Red Hat (64-bit)
- Capacidad de memoria RAM: 2048 MB
- Almacenamiento: 20 GB en formato VDI con asignación dinámica.

Figura 1.
Creación de la máquina virtual



Fuente: Autoría Propia

En la figura 1 se observa el proceso de creación de una máquina virtual en el software VirtualBox, donde se configuran parámetros básicos como el nombre del sistema, tipo de sistema operativo, memoria RAM y almacenamiento.

2.3 CONFIGURACIÓN DE LOS INTERFACES DE RED

Durante el proceso de configuración del entorno virtual, se añadieron tres interfaces de red a la máquina virtual, cada una asociada a una zona de red específica según los requerimientos del proyecto. En la Tabla 1 se detalla la asignación realizada.

Tabla 1.
Asignación de adaptadores de red por zona

Adaptador	Tipo de conexión	Zona asignada	Función
Adaptador 1	NAT	WAN (Roja)	Salida a Internet
Adaptador 2	Red Interna	LAN (Verde)	Red de trabajo interna
Adaptador 3	Red Interna	DMZ (Naranja)	Servidores públicos

Fuente: Autoría Propia

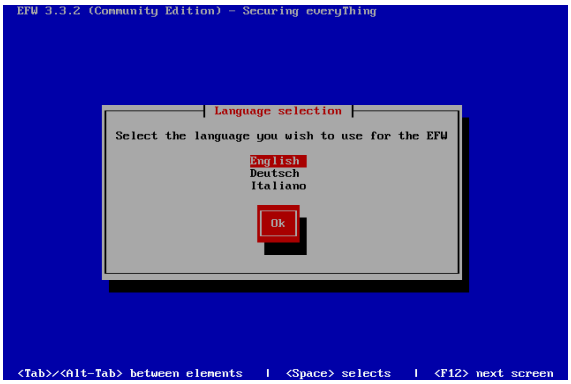
2.4 CONFIGURACIÓN DE ENDIAN

El sistema Endian se ejecuta por defecto en modo consola, aunque también permite su administración mediante una interfaz gráfica web, accesible desde cualquier dispositivo conectado a la red mediante la dirección IP asignada durante la instalación. Con el sistema Endian en funcionamiento, se procede con la configuración inicial accediendo a la dirección web correspondiente. En esta etapa, se selecciona el idioma de la interfaz gráfica y se aceptan los términos y condiciones de la licencia ofrecidos por Endian. Se asignan las contraseñas para la administración del firewall. El modo de red seleccionado es Enrutamiento, un modo de funcionamiento estándar en el firewall. En cuanto a la zona ROJA, se configura el enlace mediante asignación DHCP.

Una vez seleccionado el enlace y modo de red, se procede a seleccionar la zona NARANJA, la cual representa el segmento de red para servidores accesibles desde internet (DMZ). En el siguiente paso, dentro del apartado de preferencias de red, se configuran las zonas VERDE (LAN) y NARANJA (DMZ), asignando a cada una una dirección IP, una máscara de red y su interfaz correspondiente. Siguiendo con la configuración, se llega al apartado de preferencia de acceso a internet, correspondiente a la zona ROJA (WAN). Hasta este punto, ya se ha configurado lo más importante del sistema Endian. Ahora se procede a definir la configuración del DNS en modo automático. Opcionalmente, se puede configurar un correo electrónico administrativo. Para finalizar, se aceptan y aplican las configuraciones realizadas.

Una vez finalizada la configuración del sistema Endian, se inicia sesión con las credenciales del usuario administrador para ingresar a la interfaz principal de control, donde se muestra información relevante como las interfaces de red, información de hardware, versión del sistema, tiempo en línea, entre otros. Se verifica que toda la red esté correctamente configurada y funcionando.

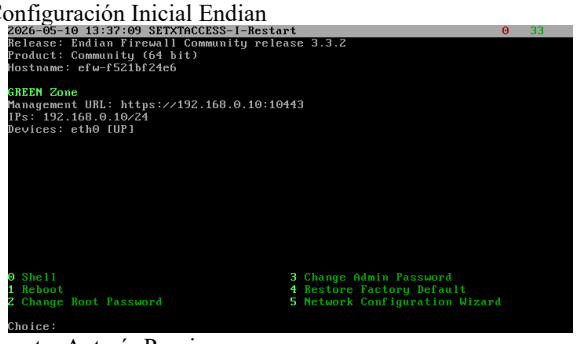
Figura 2.
Proceso de Instalación Endian



Fuente: Autoría Propia

La Figura 2 muestra la etapa inicial de instalación de Endian dentro de la máquina virtual, específicamente la selección del idioma de configuración. Este procedimiento permite definir las preferencias básicas del sistema antes de continuar con la instalación y configuración de los servicios de red y seguridad.

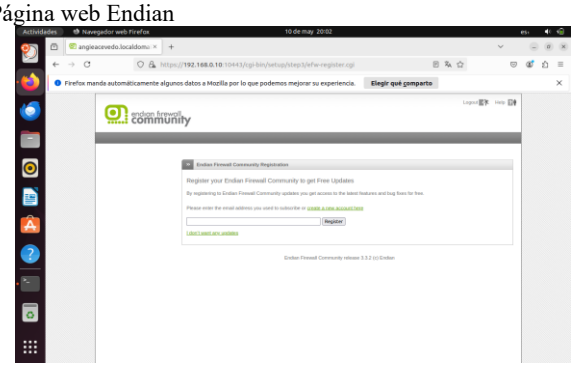
Figura 3.
Configuración Inicial Endian



Fuente: Autoría Propia

En la figura 3 se presenta la interfaz de configuración inicial del sistema operativo Endian Firewall Community Edition una vez finalizada su instalación. En esta etapa se visualizan las opciones principales de administración, como acceso a la consola, reinicio del sistema, cambio de contraseñas y configuración de red. Además, se muestra la dirección IP asignada al servidor y la URL de administración web, elementos necesarios para gestionar y monitorear los servicios de seguridad y red del sistema.

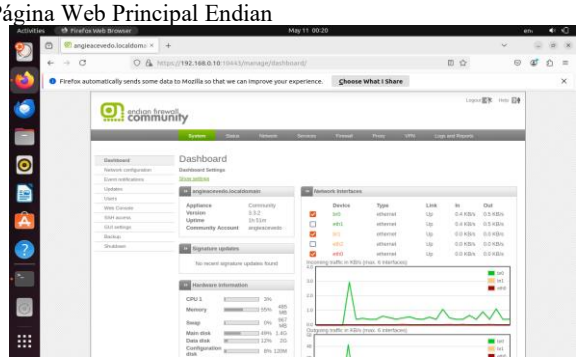
Figura 4.
Página web Endian



Fuente: Autoría Propia

La Figura 4 muestra la interfaz web de administración de Endian Firewall, accesible mediante un navegador web dentro del entorno Linux. Desde esta plataforma se pueden realizar tareas de configuración, supervisión y control de los servicios de red y seguridad, permitiendo administrar el firewall de forma remota, centralizada y eficiente.

Figura 5.
Página Web Principal Endian



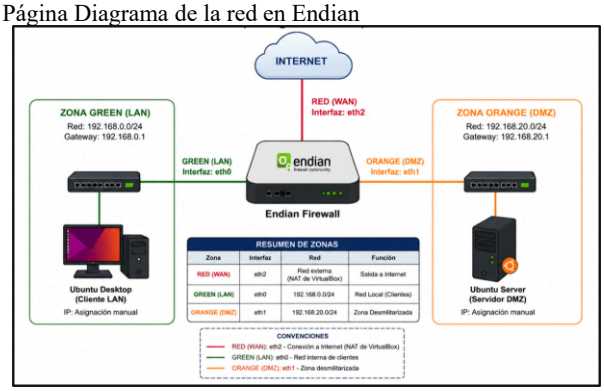
Fuente: Autoría Propia

La Figura 5 permite identificar la distribución gráfica y organización de la interfaz de Endian Firewall, destacando el uso de paneles, menús y secciones informativas que facilitan la interacción del usuario con la plataforma. Además, se observa una estructura visual diseñada para brindar acceso rápido y ordenado a las diferentes funciones del sistema.

3 DESARROLLO DE LA TEMÁTICA 2: CONFIGURACIÓN NAT.

La figura 6 representa la segmentación propuesta para proceder con la configuración NAT. En donde se definen las zonas verde, naranja y roja. Las respectivas IP según aplique a la red y Gateway correspondientes.

Figura 6.
Página Diagrama de la red en Endian



Fuente: Autoría Propia

3.1 CONFIGURACIÓN DE LAS ZONAS

La cohesión técnica del diseño se detalla en la Tabla 2, donde se especifican los segmentos de direccionamiento IP e identificadores de puerta de enlace (gateway) para cada zona. Esta estructuración garantiza que el tráfico proveniente de la zona externa (RED) sea rigurosamente filtrado antes de interactuar con los recursos críticos de la organización, aislando de manera preventiva la zona de servidores (ORANGE) de la red de usuarios locales (GREEN). Se definieron los siguientes segmentos según las zonas correspondientes:

Tabla 2.
Características de configuración de zonas

Zona	Red	Gateway
GREEN	192.168.0.0/24	192.168.0.1
ORANGE	192.168.20.0/24	192.168.20.1
RED	DHCP (VB)	Dinámico

Nota. Esta tabla muestra las interfaces según su configuración.
Fuente. Autoría Propia

3.2 CONFIGURACIÓN NAT LAN (GREEN) A WAN

La zona verde representa la confianza máxima. Se configuró una máquina Ubuntu Desktop para actuar como cliente. Para lograr la salida a WAN, se verificó la regla de enmascaramiento automática en Endian. El NAT de origen

(SNAT) permite que el tráfico generado en el segmento 192.168.0.0/24 llegue a la zona RED con la IP pública asignada. Se efectúa configuración del enmascaramiento de red para permitir que el Ubuntu Desktop en la zona GREEN acceda a la red externa. La validación se realiza mediante pruebas de conectividad (ping) a servidores DNS externos, confirmando que la traducción de direcciones se ejecuta correctamente en la interfaz RED de Endian. La figura 7 comprueba la configuración correspondiente, la cual se establece como GREEN Zone con URL: https://192.168.0.1:10443. Devices: eth0

Figura 7.
Máquina Virtual Endian con la configuración Zona Verde

Fuente: Autoría Propia

3.3 CONFIGURACIÓN NAT DMZ (ORANGE) A INTERNET

La zona naranja (192.168.20.0/24) alberga el Ubuntu Server. A diferencia de la zona GREEN, las políticas de seguridad de Endian son restrictivas por defecto para la DMZ. Se procedió a crear una regla de tráfico saliente permitiendo el protocolo TCP para los puertos 80 y 443, necesaria para la actualización de repositorios. Se configuró el enmascaramiento de red para permitir que el Ubuntu Desktop en la zona GREEN acceda a la red externa. La validación se realizó mediante pruebas de conectividad (ping) a servidores DNS externos, confirmando que la traducción de direcciones se ejecuta correctamente en la interfaz RED de Endian.

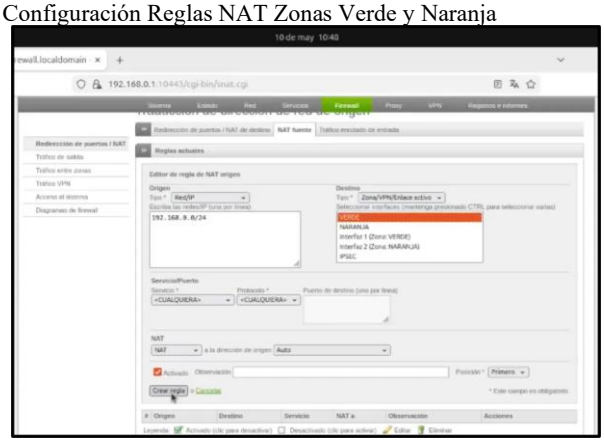
Esta configuración se realiza desde el ambiente gráfico de Endian. Para esto, se ingresa desde un navegador en Ubuntu Desktop ingresando la dirección: http://192.168.0.1:10443/. Se accede con las credenciales creadas (usuario y contraseña) y desde el módulo Configuración de red se procede a configurar la red ORANGE con las redes establecidas anteriormente. La fig.8 evidencia el módulo correspondiente para la configuración de la Zona Naranja.

Figura 8.
Configuración Zona Naranja

Fuente: Autoría Propia

Una vez configuradas las zonas se procede con la configuración desde el ambiente gráfico. Menú Firewall, opción NAT fuente, se indican las reglas y las redes aplicables. La Figura 9 evidencia el módulo correspondiente para aplicar la configuración.

Figura 9.
Configuración Reglas NAT Zonas Verde y Naranja



Fuente: Autoría Propia

3.4 CONFIGURACIÓN REENVÍO DE PUERTOS CREACIÓN DE LAS REGLAS NAT

Se verificó la creación automática de reglas NAT, observando políticas activas dentro del panel administrativo de Endian.

La segmentación de zonas (GREEN, ORANGE, RED) constituyen un método eficaz para mitigar riesgos. Incluso si un servidor en la DMZ fuese comprometido, las reglas configuradas impedirían el desplazamiento lateral hacia la red privada de confianza.

Desde el módulo Firewall y la opción NAT fuente del panel administrativo de Endian se procede a revisar que las reglas hayan sido creadas y estén activas.

Figura 10.
Verificación Reglas NAT Zonas Verde y Naranja

Fuente: Autoría Propia

La capacidad de definir políticas diferenciales para las zonas GREEN y ORANGE permite un equilibrio entre la libertad de navegación del usuario final y la exposición controlada de servicios críticos. [7].

Tabla 3.
Resultados configuración de Zonas

Prueba de Conectividad	Origen	Destino	Recurso
ICMP Ping1	GREEN	WAN	NAT
ICMP Ping1t	ORANGE	WAN	Regla Out

Fuente. Autoría Propia

La validación demostró una salida a Internet exitosa desde ambas zonas, registrando cero pérdidas de paquetes y latencias óptimas. Asimismo, los tiempos de respuesta inferiores a un milisegundo hacia la puerta de enlace local ratifican el correcto funcionamiento de las interfaces de red configuradas [2].

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

4.1 CONFIGURACIÓN DE RED Y ADAPTADORES

Para segmentar la red en zonas (Verde/LAN, Naranja/DMZ y Roja/Internet), se habilitaron tres adaptadores de red en la máquina virtual. El Adaptador 3, por ejemplo, se configuró como "Red interna" bajo el nombre DMZ_ZONA_NARANJA. Mediante el comando ip addr, se verificó que la interfaz enp0s3 tiene asignada la IP 192.168.0.14/24 [5].

4.1.1 COMUNICACIÓN ZONA VERDE A NARANJA (HTTP Y FTP)

Se establecieron reglas para permitir que la zona local (Verde) acceda a la zona de servidores (Naranja).

Comando: sudo ufw allow from 192.168.0.0/24 to any proto tcp port 80,21.

Validación de servicios: Se confirmó que tanto el servidor web Apache2 como el servidor de archivos vsftpd están en estado active (running) [6].

4.1.2 COMUNICACIÓN INTERNET (WAN) A DMZ

Se habilitó el acceso público al servidor web ubicado en la DMZ para que sea alcanzable desde cualquier origen en Internet.

Comando: sudo ufw allow proto tcp from any to any port 80.

4.1.3 VERIFICACIÓN DE REGLAS CREADAS

Mediante el comando sudo ufw status verbose, se comprobó la creación exitosa de las políticas. La salida muestra que los puertos 80 (HTTP) y 21 (FTP) están permitidos desde la red 192.168.0.0/24, y el puerto 80 está abierto para cualquier origen (Anywhere).

4.1.4 PRUEBAS DE DIRECTIVAS (INGRESO DE SERVICIOS)

Se realizaron pruebas de conectividad mediante herramientas de consola (curl y telnet) para validar el flujo de tráfico inter-zona:

LAN a DMZ (HTTP): Ejecutando curl -I http://localhost se obtuvo una respuesta 302 Found, confirmando el acceso al servidor Apache local.

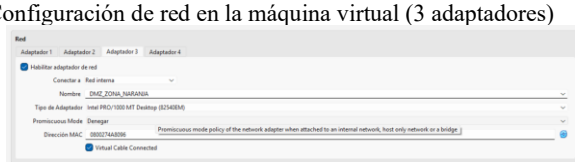
LAN a WAN (HTTP): Se validó la salida a Internet desde la LAN accediendo a Google con éxito (HTTP/1.1 200 OK).

DMZ a WAN (HTTP): Se probó la conectividad desde el servidor hacia el exterior mediante Ubuntu.com, recibiendo un código 301 Moved Permanently.

WAN a DMZ (HTTP): Al habilitar el puerto 80 para cualquier origen, se obtuvo una respuesta satisfactoria del servicio Apache.

WAN a DMZ (FTP): Se utilizó telnet localhost 21 para verificar el puerto de enlace, obteniendo una conexión exitosa con el banner 220 (vsFTPd 3.0.5), lo que demuestra que el servicio es accesible.

Figura 11.
Configuración de red en la máquina virtual (3 adaptadores)



Fuente: Autoría Propia

Se inicia con la configuración de red desde la máquina virtual.

Figura 12.
Configuración de red en la máquina virtual

Fuente: Autoría Propia

En la Figura 12 se observa la ejecución del comando ip addr en la consola del sistema operativo cliente. La salida en pantalla permite comprobar el estado de las interfaces de red configuradas.

Figura 13.
Comunicación Zona Verde a Naranja (HTTP y FTP)

```
vboxuser@DAYANAMORENO04:~$ sudo ufw allow from 192.168.0.0/24 to any proto tcp port 80,21
Skipping adding existing rule
vboxuser@DAYANAMORENO04:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2026-05-12 04:36:22 UTC; 43min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 646 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 771 (apache2)
      Tasks: 7 (limit: 7864)
     Memory: 55.0M
        CPU: 1.206s
     CGroup: /system.slice/apache2.service
             ├─ 771 /usr/sbin/apache2 -k start
             ├─ 789 /usr/sbin/apache2 -k start
             ├─ 790 /usr/sbin/apache2 -k start
             ├─ 791 /usr/sbin/apache2 -k start
             ├─ 792 /usr/sbin/apache2 -k start
             ├─ 793 /usr/sbin/apache2 -k start
             └─25692 /usr/sbin/apache2 -k start
```

Fuente: Autoría Propia

Para segmentar la red en zonas (Verde/LAN, Naranja/DMZ y Roja/Internet), se habilitaron tres adaptadores de red en la máquina virtual. El Adaptador 3, por ejemplo, se configuró como "Red interna" bajo el nombre DMZ_ZONA_NARANJA. Mediante el comando ip addr, se verificó que la interfaz enp0s3 tiene asignada la IP 192.168.0.14/24.

Figura 14.
Comunicación Zona Verde a Naranja

```
vboxuser@DAYANAMORENO04:~$ sudo systemctl start vsftpd
sudo systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2026-05-12 05:55:08 UTC; 5s ago
   Main PID: 27079 (vsftpd)
      Tasks: 1 (limit: 7864)
     Memory: 852.0K
        CPU: 12ms
     CGroup: /system.slice/vsftpd.service
             └─27079 /usr/sbin/vsftpd /etc/vsftpd.conf

May 12 05:55:08 DAYANAMORENO04 systemd[1]: Starting vsftpd FTP server...
May 12 05:55:08 DAYANAMORENO04 systemd[1]: Started vsftpd FTP server.
vboxuser@DAYANAMORENO04:~$
```

Fuente: Autoría Propia

WAN a DMZ (FTP): Se utilizó telnet localhost 21 para verificar el puerto de enlace, obteniendo una conexión exitosa con el banner 220 (vsFTPd 3.0.5), lo que demuestra que el servicio es accesible.

Se establecieron reglas para permitir que la zona local (Verde) acceda a la zona de servidores (Naranja). Se comprueba la conexión exitosa, con acceso al servicio, permitiendo el acceso entre la zona verde y la zona naranja.

Figura 15.
Comunicación Internet (WAN) a DMZ

```
Tue May 12 05:02:39 AM UTC 2026
vboxuser@DAYANAMORENO04:~$ sudo ufw allow proto tcp from any to any port 80
date
Rules updated
Rules updated (v6)
Tue May 12 05:04:15 AM UTC 2026
vboxuser@DAYANAMORENO04:~$
```

Fuente: Autoría Propia

WAN a DMZ (HTTP): Al habilitar el puerto 80 para cualquier origen, se obtuvo una respuesta satisfactoria del servicio Apache.

Se habilitó el acceso público al servidor web ubicado en la DMZ para que sea alcanzable desde cualquier origen en Internet.

Figura 16.
Verificar las Reglas Creadas

```
vboxuser@DAYANAMORENO04:~$ sudo ufw status verbose
[sudo] password for vboxuser:
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
21,80/tcp                  ALLOW IN    192.168.0.0/24
80/tcp                     ALLOW IN    Anywhere
22/tcp                     ALLOW IN    Anywhere
80/tcp (v6)                ALLOW IN    Anywhere (v6)
22/tcp (v6)                ALLOW IN    Anywhere (v6)

vboxuser@DAYANAMORENO04:~$
```

Fuente: Autoría Propia

Mediante el comando sudo ufw status verbose, se comprobó la creación exitosa de las políticas. La salida muestra que los puertos 80 (HTTP) y 21 (FTP) están permitidos desde la red 192.168.0.0/24, y el puerto 80 está abierto para cualquier origen (Anywhere).

Mediante el comando sudo ufw status verbose, se comprobó la creación exitosa de las políticas. La salida muestra que los puertos 80 (HTTP) y 21 (FTP) están permitidos desde la red 192.168.0.0/24, y el puerto 80 está abierto para cualquier origen (Anywhere).

Figura 17.
Ingreso HTTP desde LAN a DMZ

```
Tue May 12 05:07:57 AM UTC 2026
vboxuser@DAYANAMORENO04:~$ curl -I http://localhost
HTTP/1.0 302 Found
Date: Tue, 12 May 2026 05:10:17 GMT
Server: Apache/2.4.52 (Ubuntu)
Location: http://192.168.0.15/index.php?
Connection: close
Content-Type: text/html; charset=utf-8

vboxuser@DAYANAMORENO04:~$
```

Fuente: Autoría Propia

LAN a DMZ (HTTP): Ejecutando curl -I http://localhost se obtuvo una respuesta 302 Found, confirmando el acceso al servidor Apache local.

Figura 18.
Ingreso HTTP desde LAN a WAN (Internet)

```
vboxuser@DAYANAMORENO04:~$ curl -I http://www.google.com
HTTP/1.1 200 OK
Content-Type: text/html; charset=ISO-8859-1
Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-uNGQ4ipRUN8S2QvXZmiBdQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Date: Tue, 12 May 2026 05:12:23 GMT
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Expires: Tue, 12 May 2026 05:12:23 GMT
Cache-Control: private
Set-Cookie: AEC=AaJma5tSQX1mA6mHlE_nyHSq1qT5AiA3J02imC7QOH8mQou22huAxhmyNA; expires=Sun, 08-Nov-2026 05:12:23 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax
Set-Cookie: NID=531=PqPWuycoQpCnXLaYXHZoEFxxvluAucxwX880cxz_JC6BFeFmRgFvcLOrNevqDtzz9TpH7j7cbS3xHo2n_Hl6DmTJD2_4L2zzPH8MIHuWztbBAZCovAuIWnVyIZiIBnKlpsHhyDJktnFY6EhocgmgkO8nIa8RNpFkGoc7SnDTe8K9erSVSmlq99BL7-T63bRyS_hW59JAdKPRZn0lnKFo; expires=Wed, 11-Nov-2026 05:12:23 GMT; path=/; domain=.google.com; HttpOnly
Transfer-Encoding: chunked

vboxuser@DAYANAMORENO04:~$
```

Fuente: Autoría Propia

LAN a WAN (HTTP): Se validó la salida a Internet desde la LAN accediendo a Google con éxito (HTTP/1.1 200 OK).

Figura 19.
Comunicación DMZ a WAN

```
vboxuser@DAYANAMORENO04:~$ curl -I http://www.ubuntu.com
HTTP/1.1 301 Moved Permanently
content-length: 0
location: https://www.ubuntu.com/

vboxuser@DAYANAMORENO04:~$
```

Fuente: Autoría Propia

Se validó el ingreso desde la zona WAN hacia la DMZ al habilitar el puerto 80 (HTTP) para cualquier origen (Anywhere) y verificar la respuesta del servidor mediante la herramienta curl, obteniendo una respuesta satisfactoria del servicio Apache.

La implementación de la plataforma de seguridad basada en la lógica de GNU/Linux Endian permitió establecer una arquitectura de red robusta y segmentada, garantizando la protección perimetral mediante la delimitación clara de zonas de confianza: Verde (LAN), Naranja (DMZ) y Roja (Internet). A través de la administración por línea de comandos, se configuraron y validaron reglas de acceso granulares para los protocolos HTTP y FTP, asegurando que los servicios críticos alojados en la zona Naranja sean accesibles de forma segura tanto para los usuarios internos como externos, según las directivas establecidas.

Finalmente, las pruebas de conectividad inter-zona realizadas con herramientas como curl y telnet certifican que el cortafuegos no solo filtra el tráfico correctamente, sino que mantiene la alta disponibilidad de los servicios, cumpliendo con los estándares de seguridad exigidos para la administración de sistemas operativos Open Source.

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

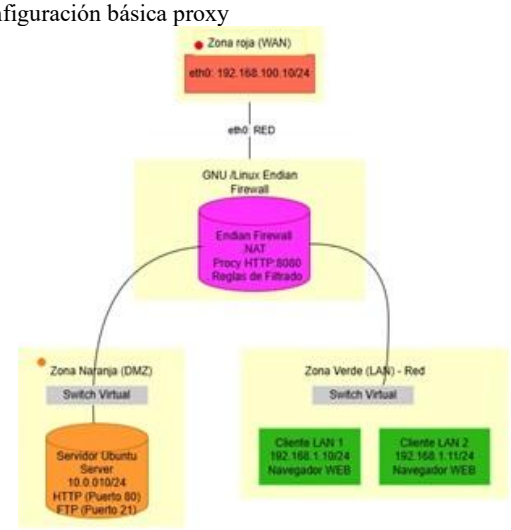
5.1 PROCEDIMIENTO DE CONFIGURACIÓN PROXY

El primer paso consiste en activar el servicio de proxy en la interfaz web de Endian (accesible mediante https://192.168.0.1/24).

1. Navegar a Proxy -> HTTP en el menú principal
2. Activar el servicio con Enable HTTP Proxy.
3. En la sección de zonas, configurar la Zona Verde (LAN), con la opción de “authentication required” o “no authentication”, en este caso se selecciona “authentication required”.
4. Importante: Desmarcar la opción “transparent on zone” para la zona Verde, ya que la autenticación no funciona correctamente en modo transparente.
5. Configurar el puerto de escucha del proxy (por defecto 8080). Este puerto deberá ser configurado en los navegadores del cliente Ubuntu.
6. Se establecen los parámetros adicionales según las necesidades: tamaño máximo de archivos, idioma de mensajes de error, etc.

La figura 20 muestra la configuración básica del proxy en la interfaz Web de Endian, donde se aprecia la selección del puerto 8080 y la habilitación para la zona Verde sin modo transparente.

Figura 20.
Configuración básica proxy



Fuente: Curso de redes cisco. Esquema de conexión de de Endian, definiendo las IPs en cada una de las zonas.

5.2 CONFIGURACIÓN DEL PERFIL DE FILTRADO CON LISTA NEGRA

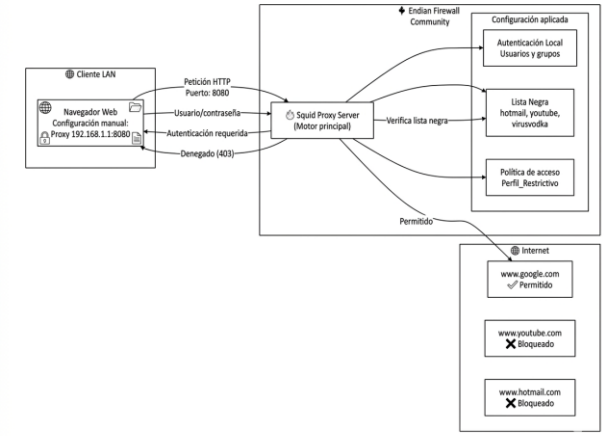
Para bloquear los sitios web especificados, se debe crear un perfil de filtrado de contenido:

1. En la sección Proxy a HTTP, acceder a la pestaña “Web Filter Profiles”.
2. Se crea un nuevo perfil haciendo clic en “Create new Profile” y asignarle un nombre especifico (Perfil restricción).
3. En la sección “Custom blacklist”, agregar los dominios a bloquear, uno por línea [9].
   www.hotmail.com
   www.youtube.com
   www.elnuevodia.com.co
4. Se puede configurar listas blancas (whitelist) si requiere establecer excepciones.
5. Habilitar opcionalmente el antivirus HTTP para análisis de contenido descargado.
6. Guardar el perfil con “Update Profile” y luego “Apply changes”.

Se aclara que las listas negras personalizadas solo aceptan nombres de dominio completo, no URLs completas con path. El bloque aplica solicitudes HTTP; para HTTPS se requeriría configuración adicional del proxy HTTPS.

La figura 21 muestra la creación del perfil de filtrado con la lista negra de dominios.

Figura 21.
Creación perfil filtrado lista negra



Fuente: Panel de control de microservicios

5.3 CONFIGURACIÓN DEL PERFIL DE FILTRADO CON LISTA NEGRA

Para la autenticación por usuario, se utiliza la base de datos locales de Endian:

1. Navegar a Users --> Users.

2. Crear un nuevo usuario haciendo clic en “Create new user”.

3. Completar los campos requeridos:
   - Username: diegostos
   - Password y Confirm password: se establece una contraseña segura.
   - Groups: asignar el usuario a un grupo (se puede crear uno nuevo como “Proxys_Users” desde Users --> Groups).

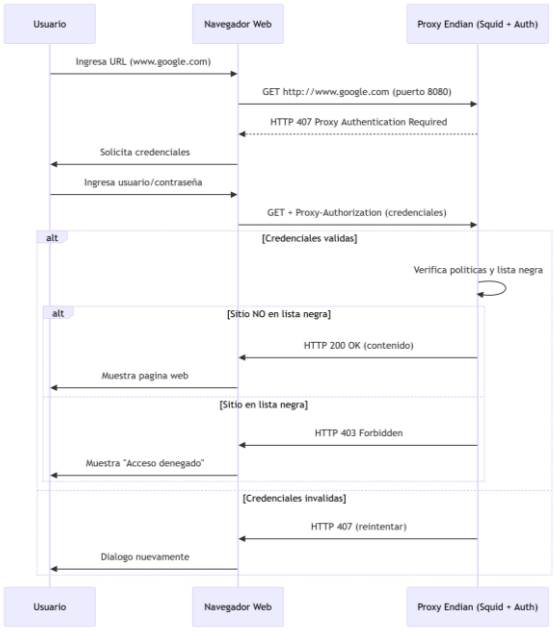
4. En la creación del grupo, se pueden definir permisos básicos, aunque en esto la política del proxy se gestionan independientemente.

5. Guardar el usuario “Save”.

5.4 HABILITACIÓN DEL PROXY HTTP EN MODO NO TRANSPARENTE

El primer paso consiste en activar el servicio de proxy en la interfaz web de Endian (accesible mediante https:10.10.10.1:10443). Según la documentación oficial, el proxy HTTP de Endian utiliza Squid como motor de caché y filtrado.

Figura 22.
Configuración de autenticación local



Fuente: Referencia de CISCO. Gráfico generado por mermaid

Muestra el diagrama de conexión de un usuario y la validación que realiza el Proxy.

5.5 CREACIÓN DE POLÍTICA DE ACCESO

La política de acceso está relacionada el perfil de filtrado con el/los usuarios autenticados:

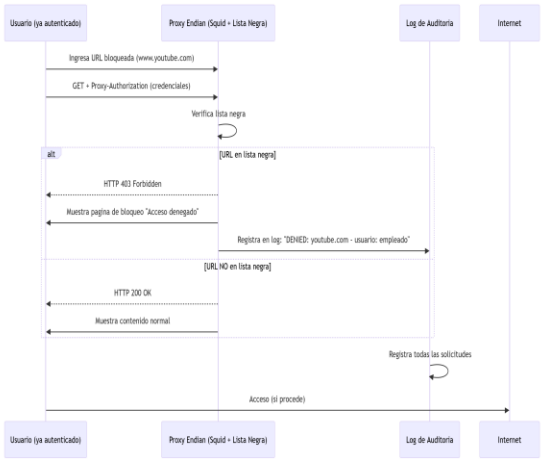
1. En Proxy ---> HTTP, acceder a la pestaña “Access Policies”.

2. Crear una nueva política con “Create new policy”.

3. Configurar los parámetros:
   - Source zone GREEN (LAN)
   - Authentication: Seleccionar “user based” o “group based” según se desee aplicar la política por usuario individual o por grupo.
   - Allowed users/groups: seleccionar el usuario “usuario_proxy” o el grupo “Proxy_Users” creado anteriormente.
   - Access Policy: Allow Access (política permitida).
   - Web Filter profile: Se selecciona el perfil “Perfil_Restrictivo” que se creó en el paso 2.
   - Time restrictions: opcional, permite restringir acceso por franjas horarias.

4. Guardar la política con “Create Policy” y luego “Apply changes”.

Figura 23.
Creación de la política de acceso vinculando el perfil de lista negra con un usuario autenticado.

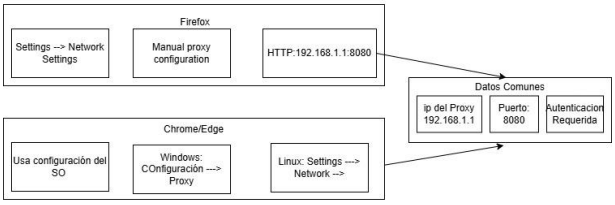


Fuente: referencia cisco. Gráfico generado por mermaid

Leyenda del log:

- TCP_DENIEN/403 --> Solicitud denegada con código 403.
- HIER/NONE/ ---> No se contactó servidor externo.
- text/html ---> Página de error enviada al navegador.

Figura 24.
Configuración manual del proxy HTTP no transparente en el navegador web.



Fuente: referencia cisco. Gráfico generado por mermaid.

En la siguiente tabla se muestra (según la guía solicita que sea no transparente), la diferencia entre lo solicitado y cuál es la configuración general de la red.

Tabla 4.
Configuración de Red

Modo de proxy	**¿Configuración manual?**	**¿Autenticación?**	**¿Cuándo se usa?**
Transparente	No necesaria	Generalmente no	Redes públicas, escuelas
No transparente	Requerida	Si, obligatoria	Entornos corporativos, SOHO

Fuente: autoría propia

El proxy transparente intercepta automáticamente el tráfico HTTP sin que el usuario o el navegador necesiten configuración alguna. El firewall redirige el tráfico del puerto 80 (HTTP) hacia el proxy sin que el cliente lo note.

Funcionamiento:

Usuario ---> [Puerto 80] --> Firewall ---> [Redirige] --> Proxy ----> Internet (no sabe que hay un proxy).

¿Configuración manual? -necesaria.

- El usuario no necesita hacer nada en su navegador.

- El administrador configura la redirección en el firewall (reglas de iptables o redirección de puertos).

- El tráfico HTTP es capturado y redirigido al proxy de forma forzada.

¿Autenticación? a Redes Públicas, escuelas

Ventajas del modo Transparente:

- Sin esfuerzo para el usuario: No hay que configurar nada en los navegadores.

- Imposible de evadir: El usuario no puede “saltarse” el proxy cambiando la configuración de su navegador.

- Ideal para redes con muchos usuarios visitantes: no se requiere crear cuentas.

Tabla 5.
Comparativa técnica en profundidad

Característica	Proxy Transparente	Proxy No Transparente
RFC / Estándar	No estándar (implementación propietaria)	RFC 7230 (HTTP/1.1)
Puerto típico	80 (HTTP), 443 (HTTPS con interceptación)	8080, 3128, 8000
Método HTTP utilizado	GET / POST normales	GET con URL completa (esquema incluido)
Interceptación	Por capa 3/4 (iptables, redirección)	Por capa 7 (aplicación)
Configuración cliente	Automática (redirección forzada)	Manual o WPAD
Autenticación	Portal cautivo (capa 7 con redirección)	HTTP 407 nativo del navegador
Soporte HTTPS	Requiere inspección SSL (MITM)	Túnel CONNECT (no inspecciona contenido)
Logs por usuario	No disponible (solo IP)	Disponible (nombre de usuario)
Evasión por usuario	Difícil (la redirección es obligatoria)	Fácil (deshabilitando el proxy)
Complejidad configuración	Baja (solo en firewall)	Media (cliente + servidor)

Fuente: Autoría propia.

Se muestra la forma como el usuario interactúa con el proxy y los pasos que se deben cumplir en su totalidad.

Configuración del modo transparente en Endian.

Proxy ---> HTTP ---> Zona Verde ----> Marcar “transparent on zone””

- El firewall redirige todo el tráfico del puerto 80 desde la LAN hacia Squid.

- No se requiere configuración en navegadores.

- Las opciones de autenticación quedan deshabilitadas o no funcionan correctamente.

Configuración del modo no transparente en Endian:

Proxy --> HTTP ---> Zona Verde ---> Seleccionar “authentication required”

Proxy ---> HTTP --> Zona Verde ----> DESMARCAR “transparent on zone”

- El proxy escucha en el puerto 8080

- Cada navegador debe configurarse con IP 192.168.0.1 y puerto 8080.

- El usuario debe autenticarse antes de navegar.

6 CONCLUSIONES

Temática 1. La implementación de Endian Firewall Community sobre Oracle VM VirtualBox permitió desarrollar un entorno de red virtualizado capaz de simular de manera eficiente una arquitectura de seguridad perimetral basada en la segmentación de zonas Verde (LAN), Roja (WAN) y Naranja (DMZ), evidenciando la importancia de la administración y control del tráfico de red en infraestructuras modernas. Mediante esta configuración fue posible comprender el funcionamiento de las políticas de filtrado, traducción de direcciones NAT, control de acceso y aislamiento de servicios expuestos al exterior, garantizando una mayor protección para la red interna frente a amenazas provenientes de Internet. Asimismo, la implementación demostró que el uso de tecnologías de virtualización constituye una alternativa flexible, escalable y de bajo costo para el diseño y validación de escenarios de ciberseguridad, permitiendo realizar pruebas, ajustes y monitoreo sin afectar entornos físicos reales. En conjunto, el desarrollo de este proyecto fortaleció competencias relacionadas con la administración de redes GNU/Linux, virtualización, segmentación de infraestructura y seguridad informática, concluyendo que la integración de Endian con máquinas virtuales representa una solución eficaz para fines académicos, de investigación y de entrenamiento en entornos de redes seguras [4].

Temática 2. El dominio de la configuración NAT y la segmentación de zonas (GREEN, ORANGE, RED) son competencias críticas, demostrando ser métodos eficaces para mitigar riesgos. El desarrollo de esta temática permitió diferenciar el enmascaramiento saliente del reenvío de puertos entrante y comprender su impacto en la seguridad del perímetro; evidenciando que, incluso si un servidor en la DMZ fuese comprometido, las reglas de firewall impedirían el desplazamiento lateral hacia la red privada de confianza.

La conclusión para la temática 4, permitió comprender de manera práctica el funcionamiento de un firewall perimetral y la implementación de una zona DMZ mediante Endian, logrando configurar exitosamente el permiso de tráfico HTTP (puerto 80) y FTP (puerto 21) desde la zona naranja hacia Internet, así como la denegación del protocolo ICMP para bloquear el comando ping. Durante el desarrollo se presentaron dificultades como la resolución de nombres mediante IPv6, la cual se soluciona forzando el uso de IPv4 con el flag -4 en el comando curl; y el orden de evaluación de las reglas, que se corrigió ubicando la regla ICMP en la primera posición de la tabla y las reglas HTTP y FTP en posiciones posteriores. Estas dificultades permitieron afianzar conceptos fundamentales como la segmentación de red, la diferencia entre tráfico entre zonas y tráfico de salida, y la importancia de la jerarquía en las políticas de filtrado.

La conclusión temática 5, - La segmentación en zonas (LAN, WAN, DMZ) constituye un pilar fundamental para la aplicación del principio de mínimo privilegio. Al aislar físicamente (a nivel lógico) los clientes internos (Zona Verde), los servidores públicos (Zona Naranja) y el acceso a Internet (Zona Roja), se logró controlar granular mente el tráfico. Las reglas de firewall implementadas permitieron únicamente las comunicaciones estrictamente necesarias: salida a Internet desde LAN y DMZ vía NAT, y acceso específico desde LAN hacia servicios HTTP/FTP en la DMZ. La denegación explícita del protocolo ICMP entre zonas, por ejemplo, evita ataques de reconocimiento de red como ping sweeps, reduciendo la superficie de ataque [8].

7 REFERENCIAS

[1] Fortinet, "¿Qué es una red DMZ y por qué la usaría?" Fortinet Cyberglossary. [Online]. Available: https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz..

[2] Fortinet, "¿Qué es ICMP (Protocolo de control de mensajes de Internet)?" Fortinet Cyberglossary. [Online]. Available: https://www.fortinet.com/lat/resources/cyberglossary/internet-control-message-protocol-icmp.

[3] J. Ocampos, "Zona Desmilitarizada (DMZ)," jorgeocampos.blog, Jul. 2024. [Online]. Available: https://jorgeocampos.blog/2024/07/09/zona_desmilitarizada_dmz/

[4] Amazon Web Services, "¿Qué es ICMP? Explicación del protocolo ICMP," AWS What Is. [Online]. Available: https://aws.amazon.com/es/what-is/icmp/.

[5] ESET, "Reglas de firewall," ESET Endpoint Security Help, version 10.1. [Online]. Available: https://help.eset.com/ees/10.1/es-CL/idh_dialog_epfw_app_tree_rules_page.html.

[6] Palo Alto Networks, "¿Qué es un firewall de filtrado de paquetes?" Palo Alto Networks Cyberpedia. [Online]. Available: https://www.paloaltonetworks.lat/cyberpedia/what-is-a-packet-filtering-firewall.

[7] Cloudflare, "¿Qué es el ICMP? | Protocolo ICMP," Cloudflare Learning Center. [Online]. Available: https://www.cloudflare.com/es-es/learning/ddos/glossary/internet-control-message-protocol-icmp/.

[8] AI Multiple, "Zona Desmilitarizada (DMZ): Ejemplos y Arquitectura," aimultiple.com. [Online]. Available: https://aimultiple.com/es/dmz.
[9] TVC Ingeniería, "Cómo funcionan las reglas de filtrado del firewall," foro.tvc.mx, Mar. 2026. [Online]. Available: https://foro.tvc.mx/docs/como-funcionan-las-reglas-de-la-politica-de-balanceo-de-carga-en-firewall-1.