Implementación de un Firewall Multizona con Endian en VirtualBox: Configuración, NAT, Control de Tráfico y Proxy HTTP con Autenticación

Heidy Patricia Triana Rueda
hptrianar@unadvirtual.edu.co
Josè Antonio Cuta Gonzàlez
jacutag@unadvirtual.edu.co
Oscar Alfonso Nova Suarez
oanovas@unadvirtual.eedu.co
Angely Johanna Pineda Borda
ajpinedab@unadvirtual.edu.co
Sindy Yamile Romero Bernal
syromerob@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación y configuración de un firewall multizona utilizando Endian Firewall Community 3.3.2 en un entorno virtualizado con Oracle VirtualBox. Se diseñó una topología de red segmentada en tres zonas de seguridad: GREEN (LAN interna), ORANGE (DMZ) y RED (WAN), con el objetivo de aislar el tráfico, controlar el acceso entre segmentos y garantizar la seguridad mediante políticas de firewall y NAT. Adicionalmente, se implementó un proxy HTTP no transparente con Squid, incorporando listas negras de sitios web y autenticación de usuarios para un control granular del acceso a Internet. Los resultados confirman la efectividad de la configuración, validando la conectividad entre zonas, el funcionamiento de las reglas de filtrado y la administración centralizada a través de la interfaz web de Endian. Este trabajo demuestra la aplicabilidad de soluciones open-source en entornos educativos y profesionales para el despliegue de infraestructuras seguras y escalables.*

PALABRAS CLAVE: VirtualBox, Endian, seguridad, OpenSource, Proxy HTTP, restricción, protocolos.

INTRODUCCIÓN

La creciente complejidad de las redes modernas exige mecanismos robustos de seguridad que permitan aislar recursos críticos y controlar el flujo de tráfico entre diferentes segmentos. La segmentación de red, mediante el uso de firewalls multizona, se ha consolidado como una práctica fundamental para reducir la superficie de ataque y aplicar políticas de seguridad granulares.

Este artículo documenta el proceso completo de configuración de una instancia de Endian Firewall Community 3.3.2 en un entorno virtualizado con Oracle VirtualBox. El objetivo principal fue establecer una arquitectura de tres zonas: GREEN para red interna confiable, ORANGE para servicios expuestos (DMZ) y RED para conexión a Internet. La implementación incluyó configuración de interfaces, asignación de direcciones IP, políticas de NAT y validación de conectividad bidireccional.

El trabajo se desarrolló como parte de los requisitos académicos de la Universidad Nacional Abierta y a Distancia (UNAD), demostrando la aplicabilidad de soluciones de código abierto para la implementación de infraestructuras de red seguras.

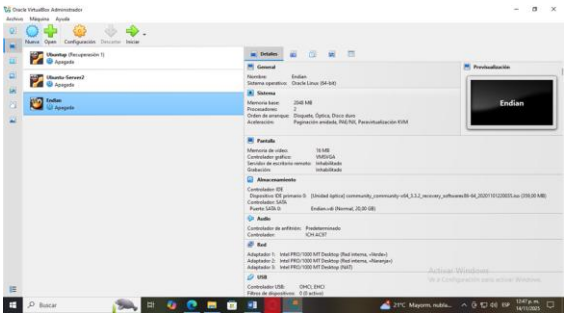
I. TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO.

1. METODOLOGÍA Y TOPOLOGÍA DE RED

Se diseñó una topología de red segmentada en tres zonas de seguridad (Fig. 1), donde el firewall Endian actúa como dispositivo central de conectividad y control:

- **Zona GREEN (eth0)**: Red interna confiable con rango 192.168.2.20/24
- **Zona ORANGE (eth2)**: DMZ para servidores con rango 192.168.1.20/24
- **Zona RED (eth1)**: Conexión a Internet mediante NAT

Figura 1: Configuración inicial de la máquina virtual en VirtualBox para instalar Endian Firewall, Ubuntu desktop que es el cliente y Ubuntu server.



Fuente propia

1.2 HERRAMIENTAS Y TECNOLOGÍAS

- Endian Firewall Community 3.3.25: Firewall de código abierto
- Oracle VirtualBox 7.2: Plataforma de virtualización
- Ubuntu Desktop 24.04 LTS: Cliente en zona GREEN
- Ubuntu Server 24.04 LTS: Servidor en zona ORANGE

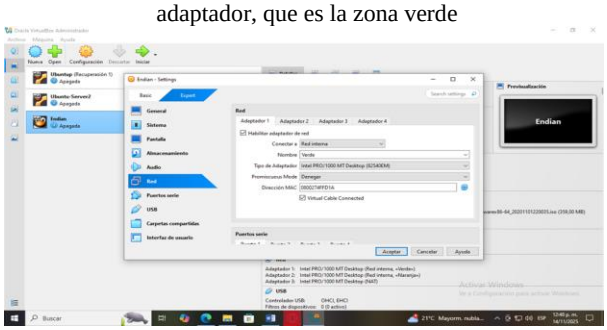
1.3 PROCESO DE CONFIGURACIÓN

1.3.1 CONFIGURACIÓN DE VIRTUALBOX

Se creó una máquina virtual para Endian Firewall con tres adaptadores de red

- Adaptador 1: Red interna "green" (Modo RED INTERNA)
- Adaptador 2: Red interna "orange" (Modo RED INTERNA)
- Adaptador 3: NAT (Conexión a Internet)

Figura 2: Configuramos el puerto de red con el primer adaptador, que es la zona verde



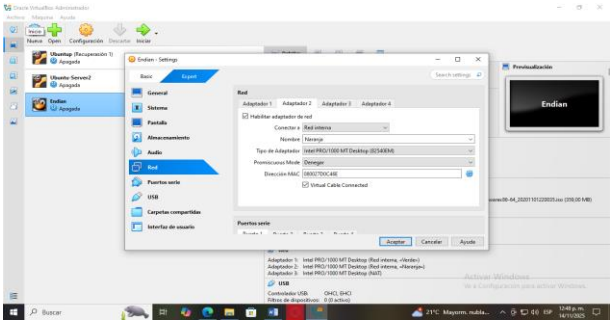
Fuente propia

1.3.2 INSTALACIÓN DE ENDIAN FIREWALL

El proceso de instalación inició con la carga de la imagen ISO de Endian Community 3.3.25 Durante la instalación se configuraron manualmente las interfaces de red:

- **eth0** asignada a zona GREEN con IP 192.168.2.20/24
- **eth1** asignada a zona ORANGE con IP 192.168.1.20/24
- **eth2** asignada a zona RED con DHCP

Figura 3: Configuramos el Segundo adaptador que va hacer la zona naranja.



Fuente propia

1.3.3 CONFIGURACIÓN DE ESTACIONES DE TRABAJO

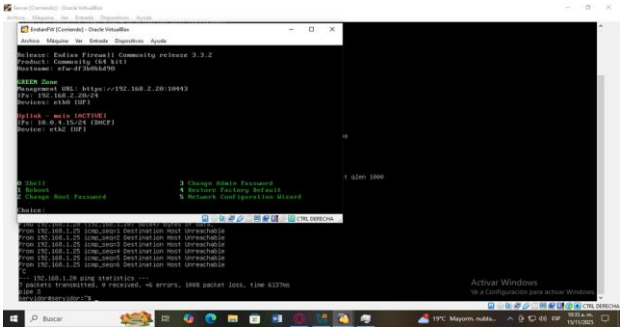
Ubuntu Desktop (Zona GREEN):

```
IP: 192.168.2.21/24
Gateway: 192.168.2.20
DNS: 8.8.8.8
                                    código
```

Ubuntu Server (Zona ORANGE):

```
IP: 192.168.1.25/24
Gateway: 192.168.1.20
DNS: 8.8.8.8
                                    código
```

Figura 4: Pantalla principal de endian, con la configuración establecida



Fuente propia

1.4 RESULTADOS Y VALIDACIÓN

1.4.1 PRUEBAS DE CONECTIVIDAD

Se ejecutaron pruebas exhaustivas de conectividad para validar la configuración:

Desde **Endian** Firewall:

- Ping a 8.8.8.8: EXITOSO
- Ping a google.com: EXITOSO
- Ping a Ubuntu Desktop (192.168.2.20): EXITOSO
- Ping a Ubuntu Server (192.168.1.20): EXITOSO

Desde **Ubuntu Desktop** (GREEN):

- Ping a gateway (192.168.2.20): EXITOSO
- Ping a 8.8.8.8: EXITOSO
- Navegación web: EXITOSO

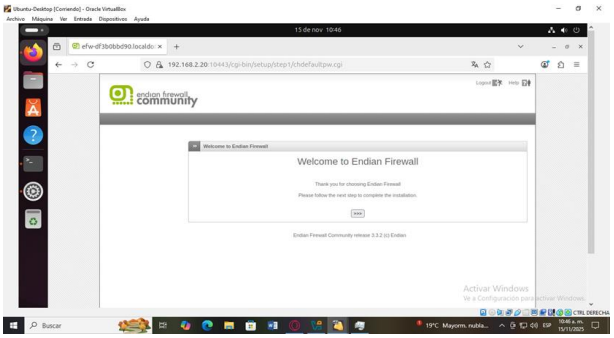
Desde **Ubuntu Server** (ORANGE):

- Ping a gateway (192.168.1.20): EXITOSO
- Ping a 8.8.8.8: EXITOSO
- Resolución DNS: EXITOSO

1.4.2 ACCESO A INTERFAZ DE ADMINISTRACIÓN

Se validó el acceso a la interfaz web de administración mediante HTTPS

Figura 5: Pantalla de bienvenida del instalador de Endian Firewall.



Fuente propia

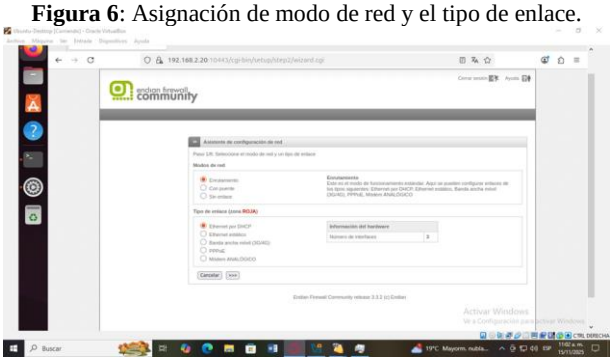
http://192.168.2.20 Dirección IP

1.5 CONFIGURACIÓN DE POLÍTICAS DE SEGURIDAD

Se implementaron políticas básicas de firewall

NAT de origen para tráfico de GREEN a RED

Figura 6: Asignación de modo de red y el tipo de enlace.



Fuente propia

Políticas restrictivas entre ORANGE y GREEN

Figura 7. Configuración de la dirección IP estática para la interfaz verde y Naranja.

Fuente propia

1.6 CONSIDERACIONES DE CIBERSEGURIDAD

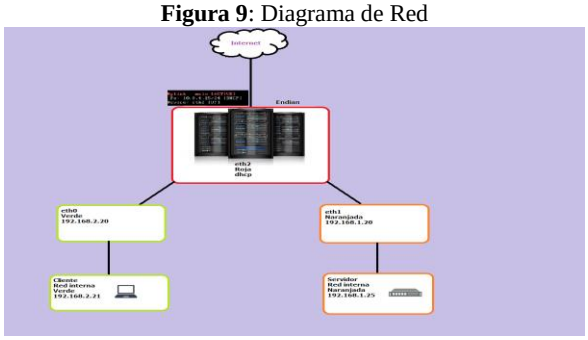
La implementación abordó principios fundamentales de seguridad:

Figura 8: Pantalla principal de Endian

Fuente propia

- **Segmentación de Red**: Aislamiento de dispositivos críticos en zonas separadas
- **Control de Acceso**: Políticas firewall entre zonas según principio de mínimo privilegio
- **Ocultamiento de Infraestructura**: Uso de NAT para ocultar IPs internas
- **Autenticación Fuerte**: Acceso administrativo con credenciales seguras vía HTTPS

Figura 9: Diagrama de Red



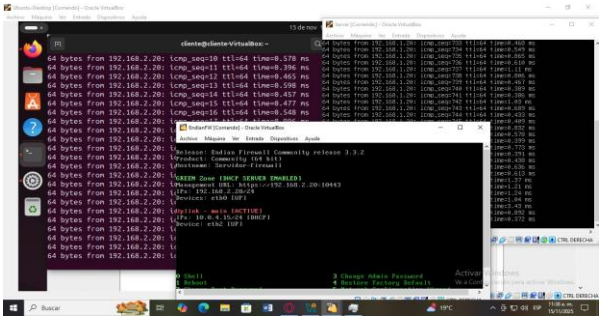
Fuente: Autoría propia

1.7 PROBLEMAS ENCONTRADOS Y SOLUCIONES

Durante la implementación se identificaron y resolvieron los siguientes inconvenientes:

- Problema 1: Falta de conectividad desde GREEN a Internet
  - ➢ Solución: Configuración de Source NAT (SNAT) en políticas firewall
- Problema 2: Error de resolución DNS en estaciones
  - ➢ Solución: Configuración manual de servidores DNS (8.8.8.8)
- Problema 3: Conectividad interrumpida entre zonas
  - ➢ Solución: Verificación de nombres de red interna en VirtualBox

Figura 10: Verificación de conectividad entre interfaces y acceso a internet



Fuente propia

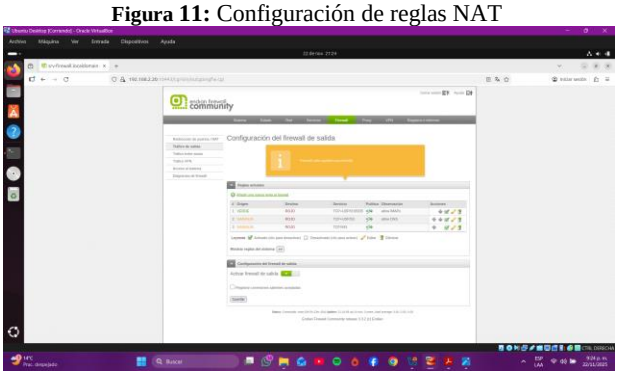
II. TEMÁTICA 2: CONFIGURACIÓN NAT.

Configurar la regla de NAT (Network Address Translation / Traducción de Direcciones de Red), demostrando el establecimiento de la comunicación desde la LAN hacia la WAN (Red simulada de Internet)

2.1 CONFIGURACION DE LA REGLA DE NAT

Teniendo en cuenta que la red roja (DNS/Internet simulada), red naranja (DMZ con Ubuntu servidor) y red verde (LAN con Ubuntu desktop), se realiza la configuración de las reglas, con el objetivo de permitir comunicación de la LAN hacia la WAN mediante NAT, permitir comunicación de la DMZ hacia la WAN mediante NAT y publicar servicios de la DMZ hacia la WAN mediante reglas de reenvío de puertos

Figura 11: Configuración de reglas NAT

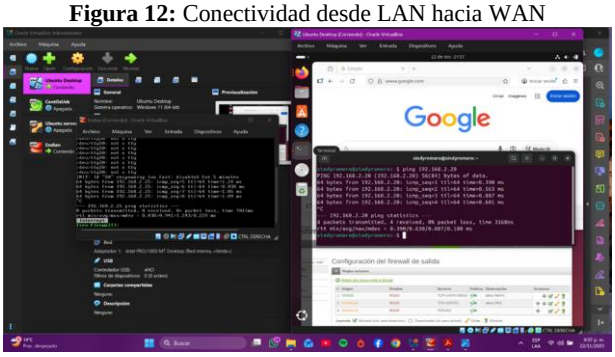


Fuente: Autoría propia

2.2 VERIFICACIÓN DE CONECTIVIDAD

Al realizar configuración de una regla al firewall, en la opción tráfico de salida, donde el origen es la zona verde (LAN) y el destino es zona roja (WAN), donde se puede observar que si hay conectividad, mediante navegación en Firefox desde LAN.

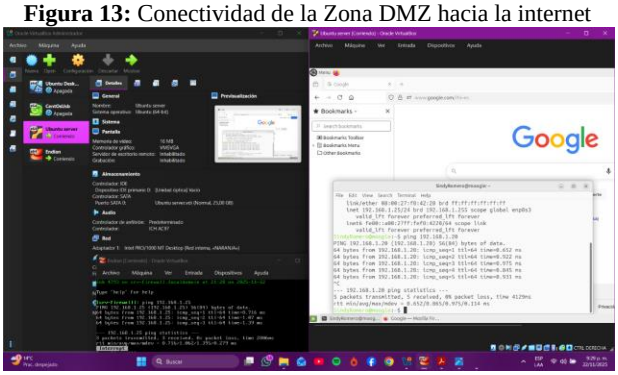
Figura 12: Conectividad desde LAN hacia WAN



Fuente: Autoría propia

Al configurar la regla de NAT, demostrando el establecimiento de la comunicación de la Zona DMZ hacia la Internet, donde se puede observar que si hay conectividad, mediante navegación en Firefox desde el servidor ubicado en DMZ

Figura 13: Conectividad de la Zona DMZ hacia la internet

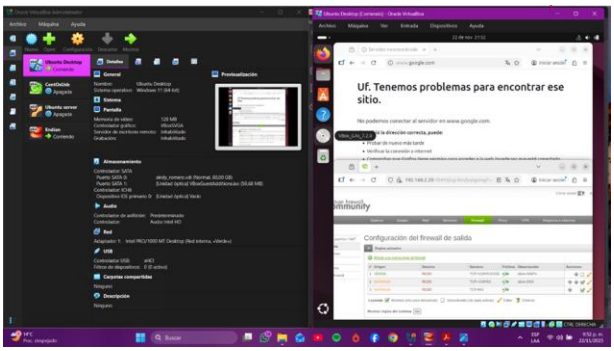


Fuente: Autoría propia

2.3 INHABILITACIÓN DE LAS REGLAS

Al inhabilitar las reglas de conectividad donde el origen es la zona verde (LAN) y el destino es zona roja (WAN), donde se puede observar que ya no se tiene acceso a la zona WAN, por consiguiente no hay navegación en Firefox.

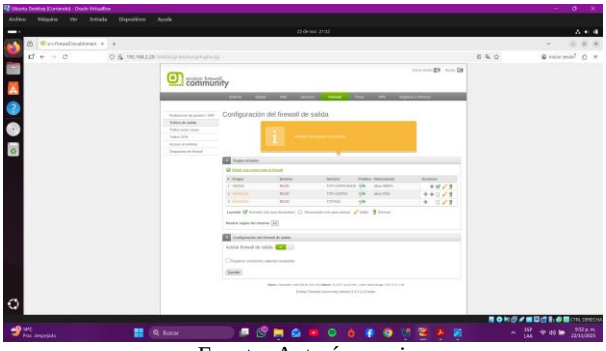
Figura 14: Inhabilitación regla desde LAN hacia WAN



Fuente: Autoría propia

Se realiza inhabilitación de la regla de conectividad de la Zona DMZ hacia la Internet.

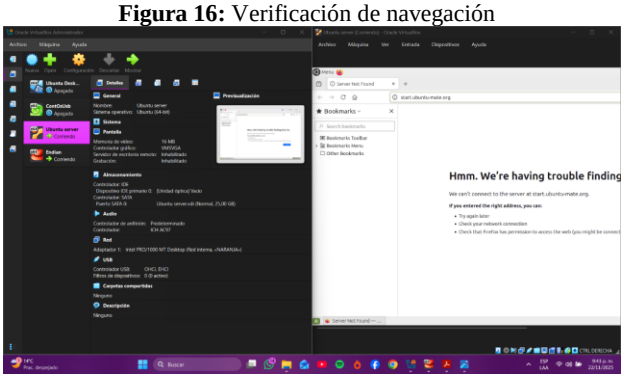
Figura 15: Inhabilitación de la regla de conectividad zona DMZ hacia internet



Fuente: Autoría propia

Se puede observar que no hay acceso a internet, mediante la navegación en Firefox

Figura 16: Verificación de navegación



Fuente: Autoría propia

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

3. PROCEDIMIENTO

- Configuración de VirtualBox [1] e instalación de Ubuntu Desktop y Ubuntu Server.
- Realizar la instalación del cortafuego Endian [2]**.**
- Definir los parámetros para configurar las máquinas y permitir la conexión entre ellas [3].
- Instalación de servicio Apache2, verificar protocolo HTTP [6] (puerto 80) y vsftpd para FTP (puerto 21).
- Denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red.
- Verificar en el tráfico de salida, la creación de las reglas.

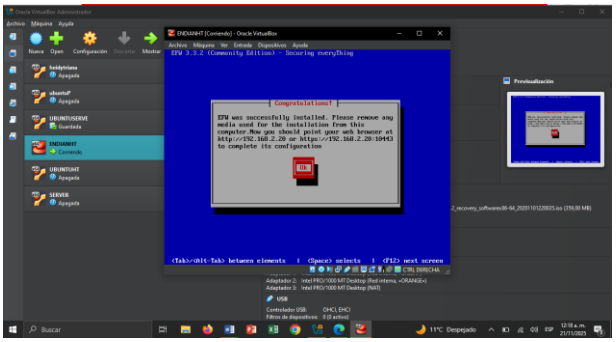
3.1 PARAMETROS DEL SISTEMA

Para la implementación del sistema se establecieron unas instancias específicas con el fin de vincular de manera eficiente la respuesta del servidor, cuando sea requerido, para esto se utilizó como herramienta principal el sistema Endian, designado características determinadas a cada adaptador de red, así:

- **Adaptador 1: GREEN** Red interna **rango** 192.168.2.20/24
- **Adaptador 2: ORANGE** Red interna DMZ (servidor) **rango** 192.168.1.20/24
- **Adaptador 3: RED** Conexión a Internet mediante Network Address Translation – NAT.

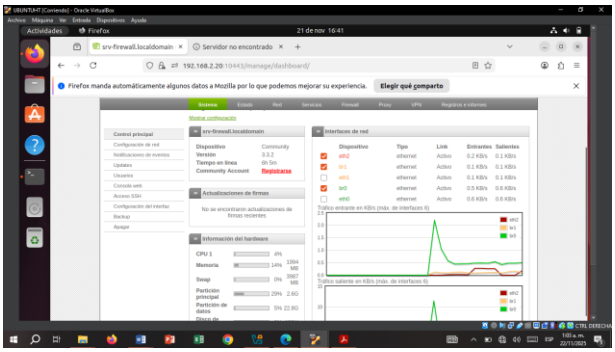
3.2 DESARROLLO TEMÁTICA

Figura 17. Se realiza la instalación de Endian, definiendo idioma y la IP de conexión (192.168.2.20).



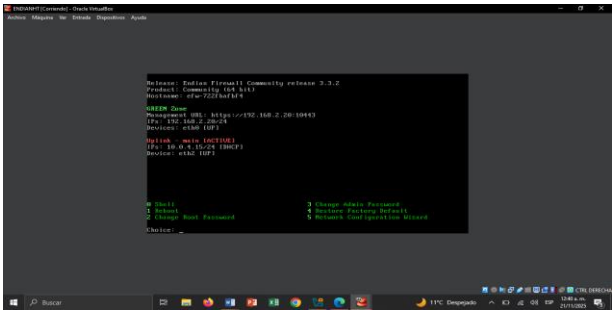
Fuente: Autoría propia

Figura 18. Terminada la instalación nos dirigimos al buscador de Ubuntu desktop (Firefox) e ingresamos a la IP que se ha determinado para la Configuración de Endian (192.168.2.20).



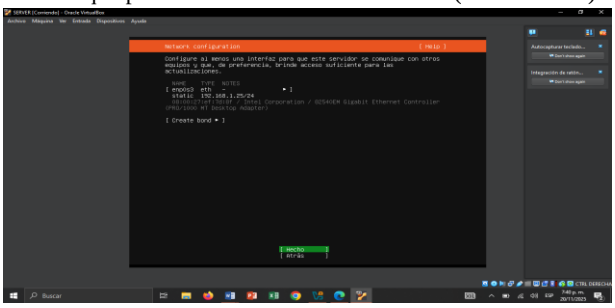
Fuente: Autoría propia

Figura 19. Al ingresar al entorno de Endian, se puede evidenciar la terminal que muestra la conexión del adaptador (GREEE) y la red.



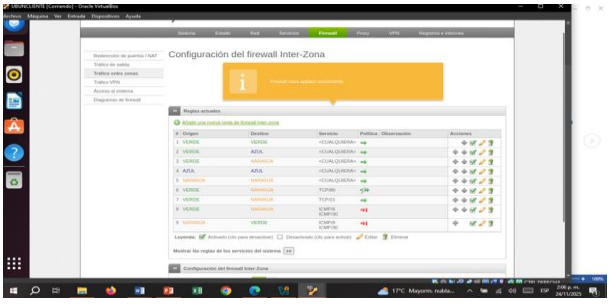
Fuente: Autoría propia

Figura 20. En este punto se establece la configuración IP estática que para este caso establecimos como (192.168.1.25)



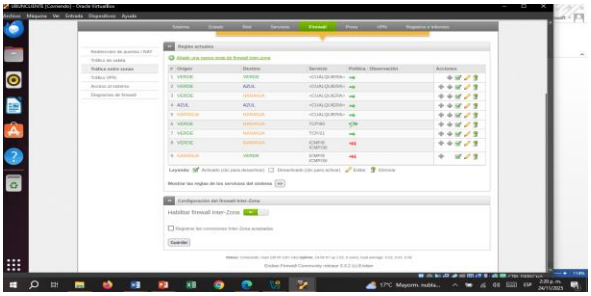
Fuente: Autoría propia

Figura 21. Verificar protocolo HTTP [6] (puerto 80) y vsftpd para FTP (puerto 21).



Fuente: Autoría propia

Figura 22. Denegar protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red.



Fuente: Autoría propia

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

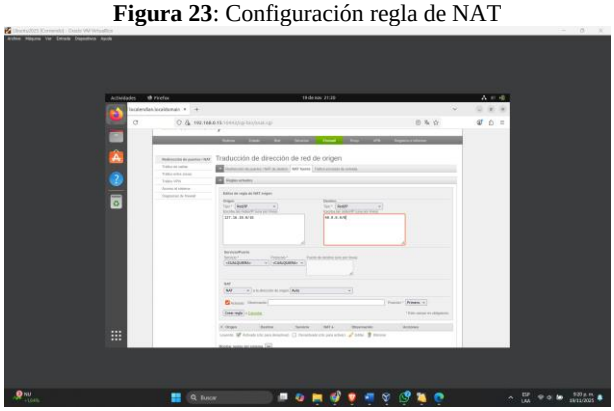
Basándose en la configuración definida en la Temática 1, se establecieron las siguientes zonas de red, gestionadas mediante el firewall Endian:

- Zona Verde (LAN): Administrada por el firewall. Contiene los equipos de los usuarios internos.
- Zona Naranja (Servidor): Reservada para servicios internos de uso público.
- Zona DMZ (zona desmilitarizada): Aloja servicios que pueden ser accedidos desde el exterior de la red.
- Zona WAN (Internet): Canal de comunicación con Internet.

4.1 REGLAS DE COMUNICACIÓN ENTRE ZONAS

Lo primero es configurar la regla de NAT, la cual nos traduce la comunicación desde la LAN a la WAN

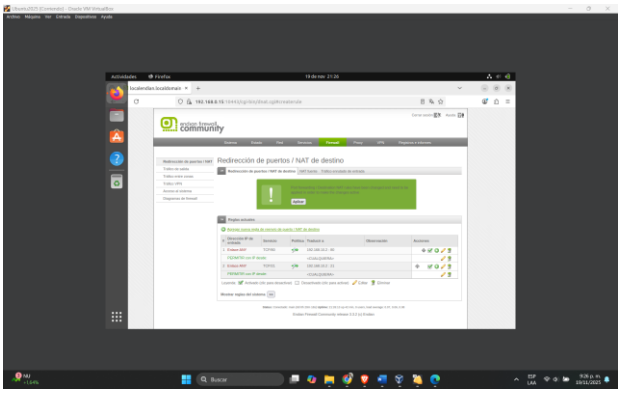
Figura 23: Configuración regla de NAT



Fuente: Autoría propia

Procedemos a evidenciar que las reglas de NAT se creen correctamente

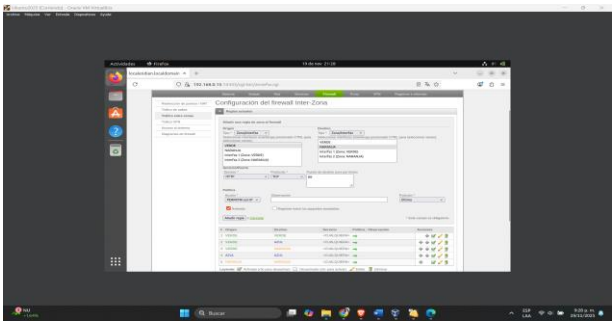
Figura 24: Reglas de NAT



Fuente: Autoría propia

Agregamos la regla inter-zona especificando de la VERDE a la NARANJA con el protocolo HTTP

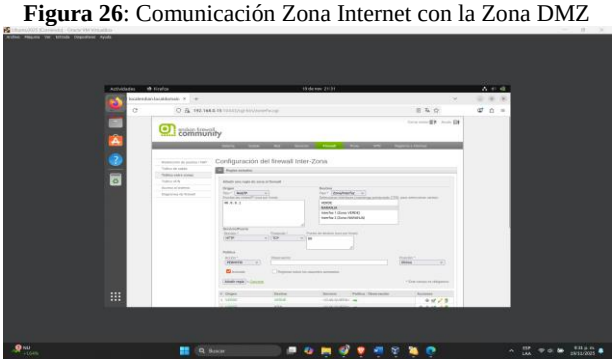
Figura 25: Comunicación Zona Verde con Zona Naranja mediante HTTP



Fuente: Autoría propia

Agregamos la regla inter-zona especificando de la VERDE a la NARANJA con el protocolo FTP. Comunicar la zona Internet con la zona DMZ.

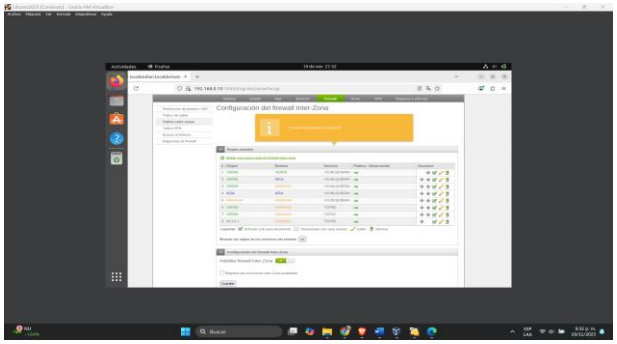
Figura 26: Comunicación Zona Internet con la Zona DMZ



Fuente: Autoría propia

Verificamos en el tráfico Inter - Zona, la creación de las reglas.

Figura 27: Creación de reglas



Fuente: Autoría propia

4.2 VERIFICACIÓN Y PRUEBAS

Validación de reglas inter-zona: Para confirmar que las reglas fueron aplicadas correctamente, se monitoreó el tráfico en el módulo de administración del firewall. Las reglas creadas permitieron la comunicación deseada entre zonas, de forma controlada y segura.

Pruebas de acceso desde el navegador web: Se realizaron pruebas de navegación desde equipos ubicados en distintas zonas para validar el acceso permitido por las reglas configuradas. Los resultados fueron los siguientes:

El ingreso del servicio HTTP desde la LAN hacia la zona DMZ. El ingreso del servicio HTTP desde la LAN hacia la WAN.

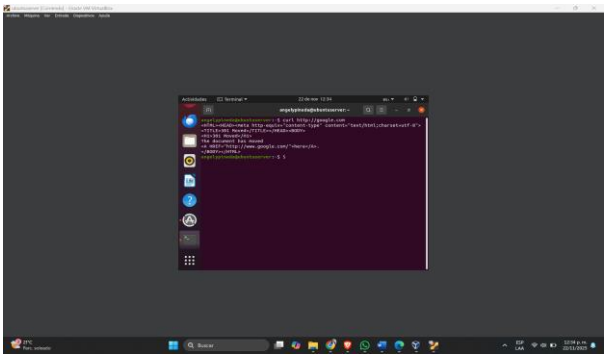
El ingreso del servicio HTTP desde la LAN hacia la WAN.

Figura 28: Prueba del servicio HTTP desde la LAN

Fuente: Autoría propia

El ingreso del servicio HTTP desde la zona DMZ hacia la WAN. El ingreso del servicio HTTP desde la WAN hacia la zona DMZ. El ingreso del servicio FTP desde la LAN hacia la WAN.

Figura 29: Prueba del servicio HTTP desde la zona DMZ



Fuente: Autoría propia

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

5.1. METODOLOGÍA DE IMPLEMENTACIÓN

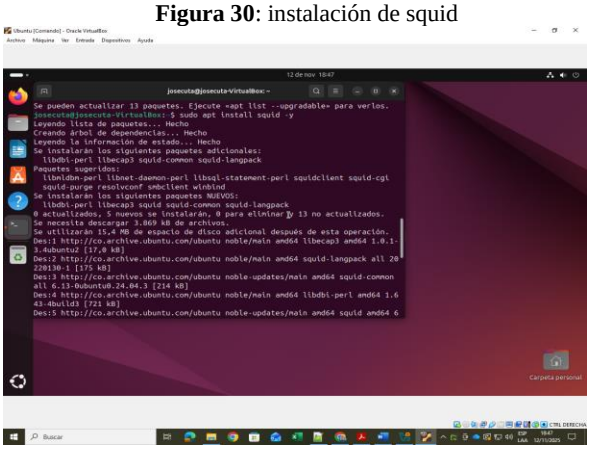
La metodología se centró en la instalación secuencial y la configuración del servidor Squid y sus políticas asociadas.

5.2 INSTALACIÓN Y VERIFICACIÓN DE SQUID

El proceso comenzó con la instalación del software Squid:

Bash
sudo apt install squid -y

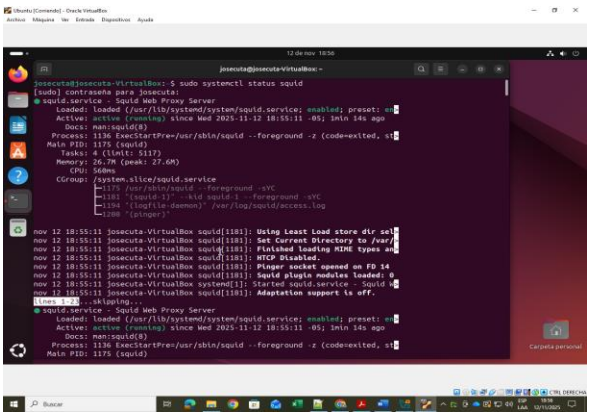
Figura 30: instalación de squid



Fuente: Autoría propia

Posteriormente, se verificó que el servicio estuviera cargado y en estado activo (active (running)) utilizando systemctl.

Figura 31: verificación de programa.



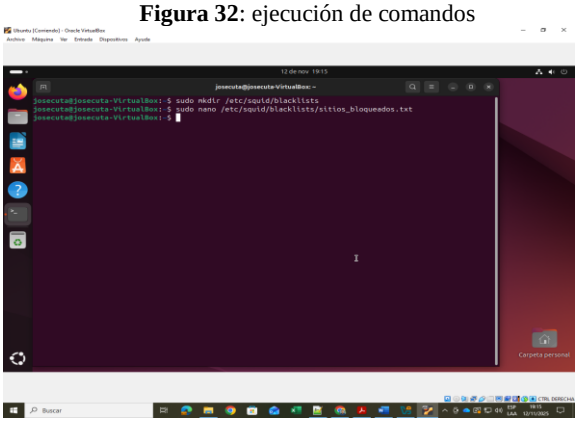
Fuente: Autoría propia

5.3 CREACIÓN Y CONFIGURACIÓN DE LA LISTA NEGRA

Se procedió a crear el directorio para las listas negras y el archivo de sitios a bloquear:

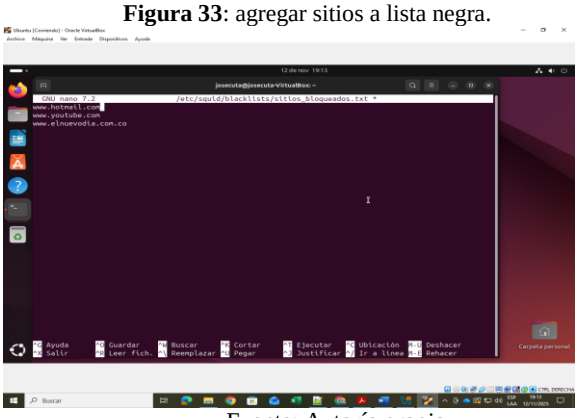
Bash
sudo mkdir /etc/squid/blacklists
sudo nano /etc/squid/blacklists/sitios_bloqueados.txt

Figura 32: ejecución de comandos



Fuente: Autoría propia

Figura 33: agregar sitios a lista negra.

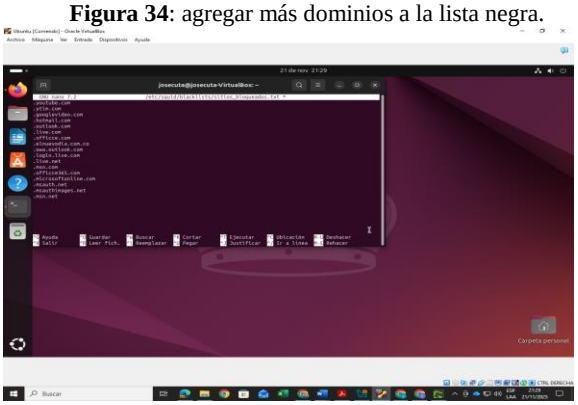


Fuente: Autoría propia

La lista inicial incluyó: www.hotmail.com, www.youtube.com, www.elnuevodia.com.co. Tras las pruebas

funcionales, se encontró que el dominio de Hotmail/Outlook requería la adición de múltiples subdominios asociados (.live.com, .outlook.com, .office365.com) para un bloqueo efectivo.

Figura 34: agregar más dominios a la lista negra.



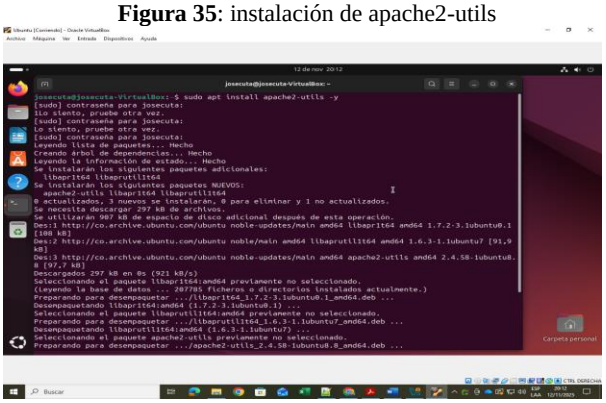
Fuente: Autoría propia

5.4 IMPLEMENTACIÓN DE LA AUTENTICACIÓN

La autenticación por usuario se habilitó instalando las utilidades de Apache:

Bash
sudo apt install apache2-utils -y

Figura 35: instalación de apache2-utils

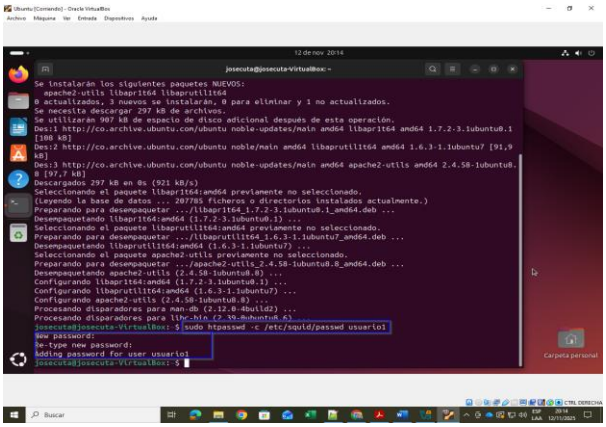


Fuente: Autoría propia

Luego, se creó el archivo de contraseñas y el usuario usuario1:

Bash
sudo htpasswd -c /etc/squid/passwd usuario1

Figura 36: creación de suario1 y asignación de contraseña



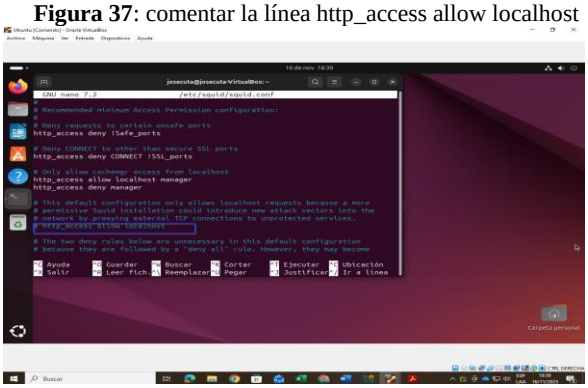
Fuente: Autoría propia

Se configuró el módulo de autenticación básica y la ruta del archivo de contraseñas dentro de squid.conf.

5.5 AJUSTE DE POLÍTICAS ACL EN SQUID

Para asegurar que las reglas de bloqueo se aplicaran a los clientes de la LAN (y no solo al tráfico saliente), se debió comentar la regla de acceso local por defecto: Bash
http_access allow localhost

Figura 37: comentar la línea http_access allow localhost



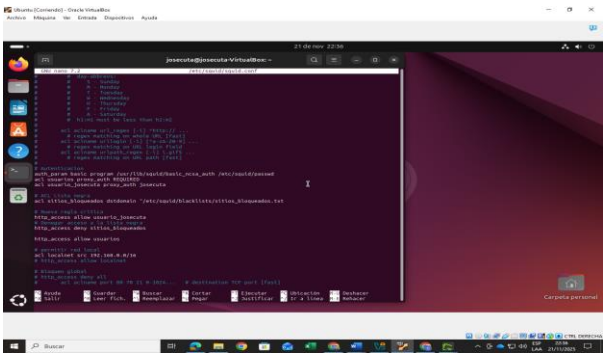
Fuente: Autoría propia

Finalmente, las políticas ACL fueron ajustadas para permitir el acceso al usuario josecuta y denegar el acceso a la lista negra para otros usuarios autenticados, logrando el control de acceso diferencial:

acl sitios_bloqueados dstdomain
"/etc/squid/blacklists/sitios_bloqueados.txt"
acl usuario_josecuta proxy_auth josecuta
http_access allow usuario_josecuta
http_access deny sitios_bloqueados
http_access allow authenticated

El servicio fue reiniciado para aplicar todos los cambios.

Figura 38: ajuste en las reglas.



5.6 RESULTADOS Y VERIFICACIÓN

La validación funcional se realizó configurando el navegador cliente (Firefox) para apuntar manualmente al servidor proxy (127.0.0.1:3128).

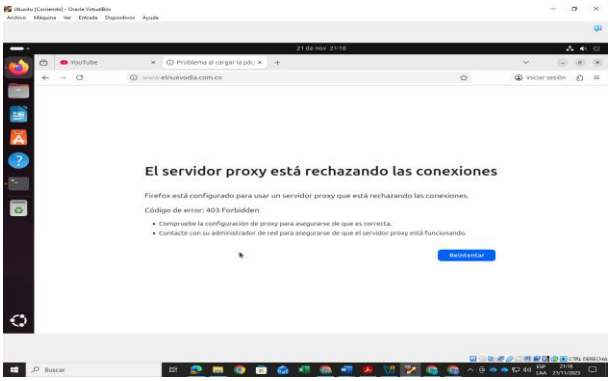
5.7 PRUEBA DE BLOQUEO (*USUARIO1*)

Al intentar acceder con las credenciales de usuario1, el proxy solicitó la autenticación. Tras ingresar las credenciales, se verificó el bloqueo exitoso a los sitios de la lista negra:

- **YouTube**: Bloqueado ("No hay conexión a Internet").
- **El Nuevo Día**: Bloqueado ("El servidor proxy está rechazando las conexiones - 403 Forbidden").
- **Outlook/Hotmail**: Bloqueado ("El servidor proxy está rechazando las conexiones - 403 Forbidden").

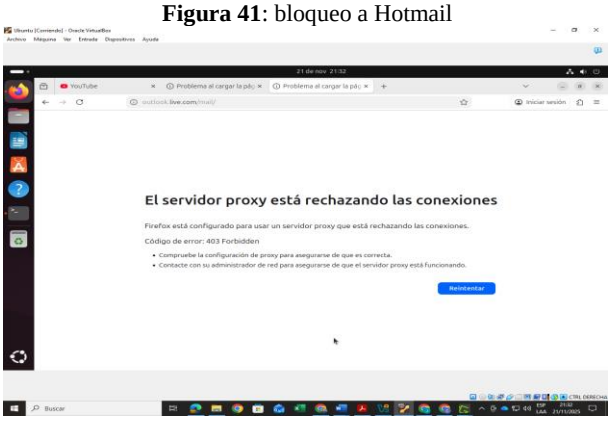
Figura 39: bloqueo acceso a YouTube

Figura 40: bloqueo a El nuevo día.



Fuente: Autoría propia

Figura 41: bloqueo a Hotmail



Fuente: Autoría propia

5.7.1 SITIOS NO BLOQUEADOS (Ej. Wikipedia): Acceso concedido.

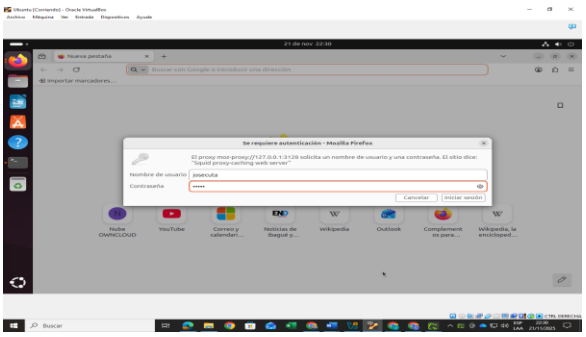
Figura 42: acceso a Wikipedia on usuario1

Fuente: Autoría propia

5.7.2 PRUEBA DE ACCESO DIFERENCIAL (*josecuta*)

Se probó el acceso con el usuario josecuta. Tras la autenticación, se confirmó que este usuario tenía acceso sin restricciones a los tres sitios bloqueados para usuario1, validando la efectividad de las reglas ACL basadas en la identidad del usuario.

Figura 43: acceso con usuario josecuta

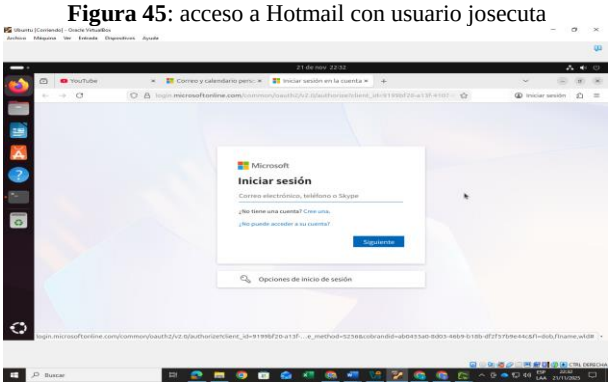


Fuente: Autoría propia

Figura 44: acceso a YouTube con usuario josecuta

Fuente: Autoría propia

Figura 45: acceso a Hotmail con usuario josecuta



Fuente: Autoría propia

Figura 46: acceso a El nuevo día con usuario josecuta

Fuente: Autoría propia

VI. RESULTADOS

1. Aislamiento efectivo entre zonas GREEN, ORANGE y RED
2. Conectividad controlada mediante políticas de firewall configuradas
3. Acceso a Internet seguro desde zonas internas mediante NAT
4. Administración centralizada mediante interfaz web segura
5. Se configuró la regla de NAT para la red verde (LAN hacia WAN), se configuró la regla de para la red naranja (DMZ hacia WAN).
6. Se verificó la salida de tráfico desde LAN y DMZ hacia la red roja (Internet simulada), obteniendo resultados de Comunicación LAN hacia WAN, (Ubuntu Desktop) logra conectividad hacia Internet simulada.
7. El servidor en la DMZ (Ubuntu Server) logró conectividad hacia Internet simulada.
8. La profundidad en el filtrado de URL al manejar servicios dinámicos como Hotmail/Outlook, donde la simple inclusión del dominio principal no es suficiente, requiriendo listar subdominios asociados.
9. La necesidad de ajustar las reglas de acceso por defecto (ej. http_access allow localhost) para que las políticas personalizadas surtan efecto en el servidor local.
10. La viabilidad del control de acceso diferencial en Squid, utilizando proxy_auth para vincular ACLs a usuarios específicos, lo que permite una administración granular de las políticas de navegación.
11.

VII. CONCLUSIONES

1. Se implementó exitosamente un firewall multizona con Endian en Oracle VirtualBox, logrando un aislamiento efectivo entre las zonas GREEN, ORANGE y RED, y permitiendo una administración centralizada mediante interfaz web.

2. La configuración de reglas de NAT y políticas de firewall permitió un control granular del tráfico entre zonas, garantizando la conectividad requerida y restringiendo accesos no autorizados.

3. La implementación de un proxy HTTP con Squid y autenticación de usuarios demostró ser efectiva para el control de acceso a Internet, permitiendo políticas diferenciadas por usuario y el bloqueo selectivo de sitios web.

4. Se identificaron desafíos técnicos, como la necesidad de incluir subdominios en las listas negras para un bloqueo efectivo de servicios dinámicos, y la importancia de ajustar las reglas por defecto de

Squid para aplicar correctamente las políticas personalizadas.

5. La solución presentada valida la viabilidad de utilizar herramientas open-source como Endian y Squid para desplegar infraestructuras de red seguras, escalables y de bajo costo, apropiadas tanto para entornos educativos como productivos.

.

REFERENCIAS

[1]. Oracle. (2020). *Manual de usuario VirtualBox.* Obtenido de https://www.virtualbox.org/manual/

[2]. Endian. (2016). *Endian UTM 3.2 Manual referencia. Endian.* . Obtenido de http://docs.endian.com/3.2/utm/index.html

[3]. giraldo, j. s. (2021). *VirtualBox con Endian 3.3.2, 3 Zonas_ Verde, Naranjada y Roja*. Obtenido de https://youtu.be/Dvht5wCPIrI

[4]. M. Z. Smith, "Firewall Policy Design and Implementation," in *IEEE Transactions on Network and Service Management*, vol. 16, no. 3, pp. 1124-1137, Sept. 2019.

[5] Endian Community Documentation, "Network Configuration Guide," Endian Ltd., 2023. [Online]. Available: https://docs.endian.com

[4] "Endian Firewall Community Edition," Endian Ltd., 2023. [Online]. Available: https://www.endian.com/community/