IMPLEMENTACIÓN DE UNA ARQUITECTURA DE SEGURIDAD PERIMETRAL CON ENDIAN FIREWALL EN ENTORNO VIRTUALIZADO

Santiago Fontecha Morales
sfontecham@unadvirtual.edu.co
Wilber Eulices Rincon Choconta
wi80rin295@unadvirtual.edu.co
Manuel Alejandro Amado Carmona
maamadoc@unadvirtual.edu.co
Edicson Lancheros Patino
elancherosp@unadvirtual.edu.co

RESUMEN: *En este trabajo se implementó y configuró una solución de seguridad perimetral utilizando la distribución GNU/Linux Endian Firewall (EFW) en un entorno virtualizado con VirtualBox. Se definieron tres zonas de red: LAN (verde), WAN (roja) y DMZ (naranja), y se aplicaron reglas de NAT, control de tráfico entre zonas, y políticas de proxy HTTP con autenticación de usuarios. Los procedimientos se ejecutaron mediante consola, validando la comunicación entre zonas y el bloqueo selectivo de servicios y sitios web. Los resultados demostraron una arquitectura segura y funcional, capaz de aislar servicios críticos y gestionar el tráfico de red de manera eficiente. Esta implementación provee un marco replicable para la protección de infraestructuras en entornos educativos y organizacionales.*

PALABRAS CLAVE: Seguridad perimetral, Endian Firewall, DMZ, NAT, Proxy HTTP, GNU/Linux.

1 INTRODUCCIÓN.

La frenética y exitosa búsqueda de vulnerabilidades que ejecutan constantemente los piratas informáticos revela con preocupación lo expuestos que se encuentran los sistemas informáticos a amenazas externas e internas, esto ha hecho de la seguridad perimetral un componente esencial en la protección de infraestructuras de red (Stallings, 2021). En entornos empresariales y académicos, la correcta segmentación de redes mediante el uso de firewalls y zonas desmilitarizadas (DMZ) se ha convertido en una práctica fundamental para aislar servicios críticos, como servidores web y bases de datos, del acceso no autorizado (Endian, 2016).

En este contexto, la distribución GNU/Linux Endian Firewall (EFW) se presenta como una solución de código abierto robusta y flexible, que permite implementar políticas de seguridad avanzadas, incluyendo traducción de direcciones de red (NAT), filtrado de tráfico entre zonas y configuración de proxis con autenticación (Oracle, 2020). Su integración en entornos virtualizados facilita la replicación de escenarios reales de red con un bajo costo operativo.

El presente artículo documenta el diseño, implementación y validación de una arquitectura segura basada en Endian EFW, desarrollada como parte de la etapa 7 del Diplomado de profundización en administración de sistemas Open Source. Se describen los procedimientos realizados para la configuración de zonas de red, reglas de NAT, control de servicios y políticas de proxy, con el fin de garantizar la confidencialidad, integridad y disponibilidad de los servicios internos y públicos.

2 CONFIGURACIÓN DE LA INSTANCIA DE GNU/LINUX ENDIAN EN VIRTUALBOX E INSTALACIÓN.

2.1 Descarga del Software Endian.

Se accedió al sitio oficial de Endian Firewall (EFW) en SourceForge (https://sourceforge.net/projects/efw/) mediante un navegador web, donde se descargó la imagen ISO correspondiente a la distribución.

2.2 Configuración del Hardware Virtual en VirtualBox.

Dentro de VirtualBox, se creó una nueva máquina virtual denominada “Endian”. Se asignaron los siguientes recursos:

- Memoria RAM: 2854 MB.
- Procesador: 3 núcleos.
- Disco duro virtual: 128 GB.

Se configuraron tres adaptadores de red:

- Adaptador 1: Red interna, denominada “verde”.
- Adaptador 2: Red interna, denominada “naranja”.
- Adaptador 3: Modo NAT.

Finalmente, se seleccionó la imagen ISO descargada y se inició la instalación del sistema operativo, eligiendo la opción “Linux Red Hat-based (64-bit)”.

Figura 1. Sitio oficial de Endian Firewall

. Fuente: Autoría Propia

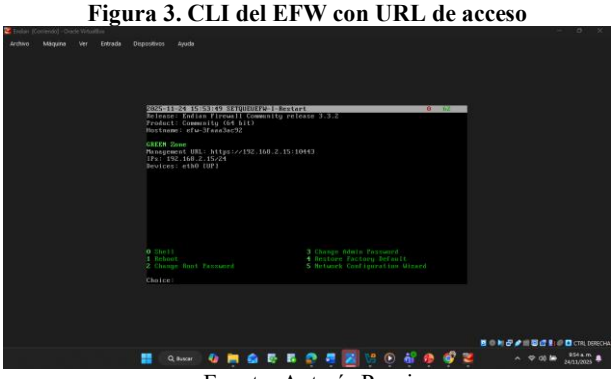
Figura 2. Configuración del Hardware Virtual

. Fuente: Autoría Propia

2.3 Instalación y Configuración Inicial de Endian.

Tras iniciar la máquina virtual, se siguió el asistente de instalación. Se seleccionó el idioma preferido y se confirmó la preparación del disco duro, aceptando la advertencia sobre la pérdida de datos. Se habilitó la conexión remota vía cable multipuerto y se asignó la dirección IPv4 192.168.2.15 con máscara 255.255.255.0 para la tarjeta de la zona verde. Al finalizar, el sistema proporcionó las direcciones de acceso a la interfaz web administrativa.

Figura 3. CLI del EFW con URL de acceso



. Fuente: Autoría Propia

2.4 Configuración de las Zonas Roja, Verde y Naranja.

Zona Roja: Configurada automáticamente mediante el adaptador en modo NAT.

Zona Verde: Se conectó el adaptador de red de una máquina virtual con Ubuntu Desktop a la red interna "verde", la cual obtuvo dirección IP vía DHCP. El tráfico fue correctamente detectado por Endian.

Zona Naranja: (DMZ): Se accedió a la interfaz web de Endian desde un equipo en la zona verde. Tras superar la advertencia de seguridad, se establecieron las contraseñas de admin y root, y se verificó la configuración de las tres tarjetas de red. Se asignó a la zona naranja la IPv4 192.168.1.15/24 y se asignó el nombre "servidor-efw". Se aplicó la configuración con DNS automático.

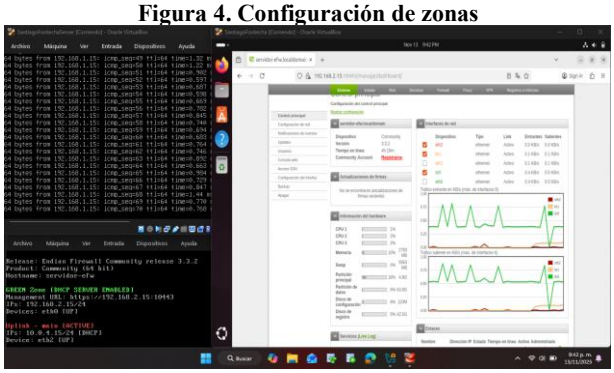
Para conectar un servidor a la zona naranja, se utilizó una máquina Ubuntu Server con su adaptador configurado en la red interna "naranja". Se editó el archivo NetPlan (/etc/netplan/xxxx.yaml) con la siguiente configuración:

```
network:
  version: 2
  ethernets:
    ens33:
      dhcp4: no
      addresses: [192.168.1.44/24]
      routes:
        - to: 0.0.0.0/0
          via: 192.168.1.15
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

Tras aplicar los cambios con sudo netplan apply, se verificó la conectividad mediante ping 192.168.1.15, confirmando la comunicación con el firewall.

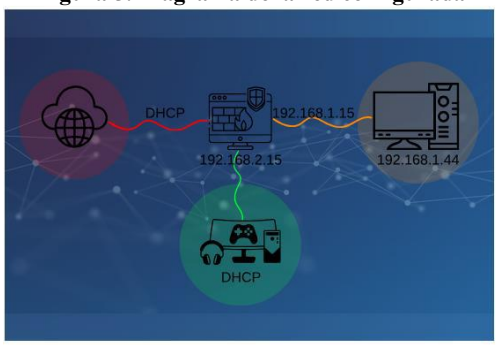
De este modo, se establecieron y verificaron las tres zonas de red propuestas: roja (WAN), verde (LAN) y naranja (DMZ).

Figura 4. Configuración de zonas



. Fuente: Autoría Propia

Figura 5. Diagrama de la red configurada



. Fuente: Autoría Propia

3 CONFIGURACIÓN DE REGLAS NAT PARA CONECTIVIDAD ENTRE ZONAS.

3.1 Establecimiento de Comunicación desde la LAN hacia la WAN.

La zona verde (LAN) se configuró con la subred definida por el grupo 192.168.2.0/24 la cual es administrada por el firewall Endian a través de la interfaz interna Verde. Para permitir que los desktops conectados en esta zona accedieran a la WAN (zona Roja) fue necesario implementar una regla de Source NAT (SNAT) haciendo uso de la funcionalidad de traducción automática de direcciones la cual fue provista por el firewall Endian. Esta regla asegura que el tráfico que se origina en la zona vede LAN sea enmascarado con la dirección IP de la zona roja (WAN) y así permitir la salida hacia internet de una manera controlada.

La configuración se realizó ingresando a la interfaz web del firewall Endian, en el módulo Firewall - Redirección de puertos/Nat - NAT fuente como se muestra en la **Figura 1**. En esta sección se definió como origen la subred 192.168.2.0/24 y como destino el enlace principal de la zona roja (enlace main). La opción "NAT a: Auto" permitió que Endian seleccionara la dirección adecuada para realizar el enmascaramiento. Una vez diligenciados los campos para esta regla, se procede a activarla y registrarla como "NAT de zona VERDE LAN hacia WAN zona ROJA". Seguido a la aplicación de la regla se validó la comunicación desde una máquina virtual con Ubuntu desktop hacia internet abriendo el navegador Mozilla Firefox y navegando por internet, adicional se realiza prueba de ping hacia dominio externo con resultados satisfactorios. Ambas pruebas confirmaron que el tráfico estaba siendo traducido por el firewall Endian y que la red LAN contaba con acceso exitoso a la zona roja WAN.

El procedimiento realizado permitió establecer la comunicación entre la LAN e internet garantizando que la salida desde la red interna dependiera y estuviera controlada por las politicas definidas en el firewall, cumpliendo así con los principios básicos de la segmentación y el control de tráfico en infraestructuras de red perimetrales.

3.2 Configuración de NAT para la Zona DMZ y Verificación de Reglas de Reenvío de Puertos.

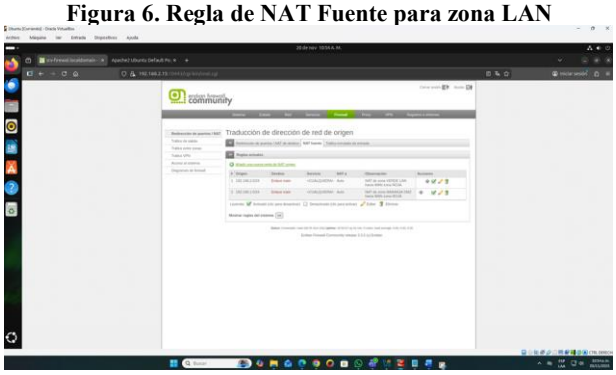
La zona naranja (DMZ) con la subnet definida 192.168.1.0/24 fue destinada para alojar servicios accesibles desde redes exteriores sin exponer directa y completa la red interna. En este escenario se usó un servidor Ubuntu con dirección IP estática 192.168.1.44 sobre la cual se configuró y habilitó un servicio web mediante Apache. Para otorgarle al servidor Ubuntu acceso controlado a la WAN, se implementó una regla NAT de salida equivalente a la utilizada en la zona verde LAN pero que solo se aplicó a la red DMZ.

En el firewall Endian, en la pestaña Firewall – NAT fuente y como se ilustra en la **Figura 2** se configuró el origen como 192.168.1.0/24 y el destino Enlace main, servicio "cualquiera" y NAT automático. Esto permitió que el servidor Ubuntu ubicado en la DMZ alcanzara los repositorios de paquetes de actualización e instalación de programas como en nuestro caso descargar e instalar Apache2.

Seguido del procedimiento anterior se configuró el reenvío de puertos (DNAT) como se evidencia en la **Figura 3** para permitir acceso HTTP desde la zona roja WAN hacia el servidor web alojado en la DMZ. En el menú NAT de destino se definió como la IP de entrada el enlace de la zona roja WAN, seleccionando el servicio HTTP (TCP/80) y traduciendo la solicitud a la dirección IP 192.168.1.44, puerto 80. La regla registrada como "Reenvío HTTP desde WAN hacia Ubuntu Server DMZ" permitió publicar de forma controlada un servicio web fuera de la red local. La verificación se realizó accediendo desde el navegador web Mozilla Firefox en el equipo Ubuntu desktop conectado a la zona verde LAN accediendo con la dirección IP de la interfaz WAN del firewall, obteniendo asi el mensaje por defecto de nuestro servicio web Apache lo que confirmó el correcto funcionamiento de esta regla DNAT. También se hizo una prueba de comunicación ICMP entre la DMZ y WAN con respuesta exitosa.

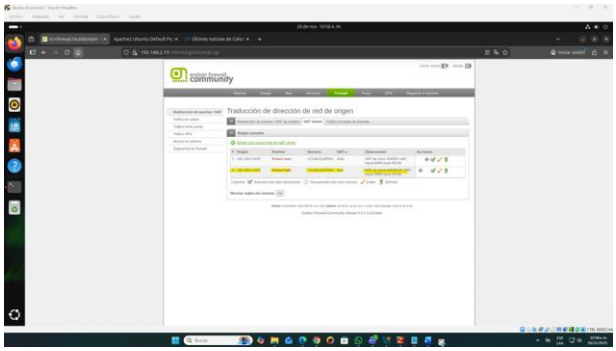
Con las configuraciones aplicadas anteriormente en Endian los servicios y red DMZ quedó correctamente integrado al esquema de seguridad del firewall Endian disponiendo una salida controlada hacia la zona roja WAN como la publicación selectiva de servicios hacia redes externas cumpliendo así con las buenas prácticas de aislamiento y exposición controlada de servidores.

Figura 6. Regla de NAT Fuente para zona LAN



. Fuente: Autoría Propia

Figura 7. Regla de NAT Fuente para zona DMZ



Fuente: Autoría Propia

Figura 8. Regla de NAT de destino (DNAT) para HTTP

Fuente: Autoría Propia

4 GESTIÓN DE SERVICIOS Y CONTROL DE ACCESO EN LA ZONA DMZ.

4.1 Habilitación de Servicios HTTP y FTP desde Ubuntu Server.

El servidor ubicado en la zona DMZ fue configurado con el sistema operativo Ubuntu Server 22.04, cumpliendo la función de ofrecer servicios controlados de acceso HTTP y FTP.

Para su implementación, se estableció la comunicación entre el servidor DMZ y el firewall Endian Community 3.3.2, configurando las reglas correspondientes de tráfico de salida.

En la interfaz de gestión de Endian (https://192.168.2.15:10443), se crearon las reglas con los siguientes parámetros:

Origen: Zona NARANJA (DMZ).

Destino: Zona ROJA (Internet).

Puertos habilitados: TCP/80 (HTTP) y TCP/21 (FTP).

Acción: Permitir (ACCEPT).

Una vez aplicadas las reglas, se realizaron las pruebas de conectividad desde el Ubuntu Server. Para el servicio HTTP, se ejecutó el comando:

curl -I http://example.com

El resultado obtenido fue un código de estado HTTP/1.1 200 OK, confirmando la correcta habilitación del servicio.

De igual manera, se verificó la conectividad FTP mediante:

ftp ftp.dlptest.com

El ingreso exitoso con credenciales de prueba evidenció la correcta salida del tráfico por el puerto 21, cumpliendo con los requerimientos del laboratorio.

4.2 Bloqueo del Protocolo ICMP y Verificación de Reglas de Tráfico de Salida

Posteriormente, se configuró una política de restricción para bloquear el tráfico ICMP desde la zona DMZ hacia la red ROJA, con el propósito de evitar respuestas de ping hacia direcciones externas y comprobar la efectividad del control del firewall.

Los parámetros aplicados fueron:

Origen: Zona NARANJA (DMZ).

Destino: Zona ROJA (Internet).

Protocolo: ICMP.

Acción: Denegar (DROP).

Una vez aplicada la política, se ejecutó la prueba desde el Ubuntu Server:

ping -c 4 8.8.8.8

El resultado obtenido fue:

Destination Net Unreachable

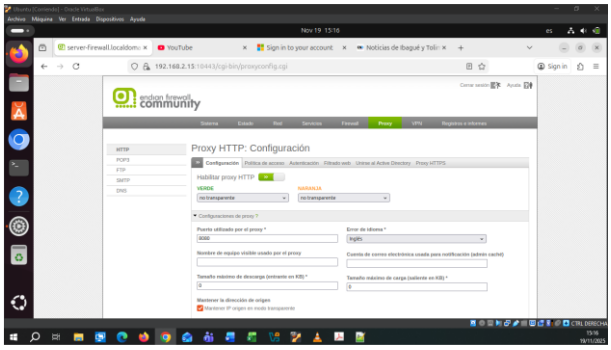
100% packet loss

Esto confirma que las reglas de filtrado se aplicaron correctamente, bloqueando la comunicación ICMP hacia Internet.

5 IMPLEMENTACIÓN DE PROXY HTTP CON AUTENTICACIÓN Y POLÍTICAS DE FILTRADO

Después de la instalación del firewall Endian se procede a ingresar a la pestaña proxy donde se habilitará como tal el proxy http como se evidencia en la Figura 9 desde el navegador web

Figura 9. Pantalla configuración proxy



Fuente: Autoría Propia

5.1 Creación de Lista Negra y Perfil de Restricción de Acceso

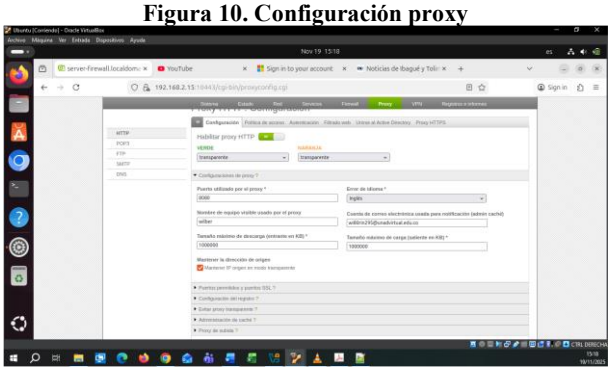
Se ingresa mediante el navegador web a la opción proxy y en la pestaña configuración se realizan ajustes para la zona naranja y la zona verde, agregando el puerto por el cuan se ingresará al proxy que en esta ocasión es el 8080, se muestra en que idioma se muestran los errores, el nombre del equipo que es visible para los usuarios, al igual que el correo electrónico donde llegaran las notificaciones de acceso o solicitud de permisos. Ver Figura 10

Se validan los puertos permitidos desde el cliente como mediante SSL, se habilitan los registros, el agente del usuario, y el filtro de contenido y se procede a guardar la configuración. Ver Figura 11

Se ingresa al administrador de cache y se ajustan los tamaños en megas para la memoria, cache y se coloca una página web donde no se ponga cache, para este informe se utilizó la página www.google.com. Se procede a guardar y aplicar los cambios realizados.

Dentro de la opción proxy se ingresa a la pestaña filtrado web donde se agregaran los sitios restringidos, se crea un perfil dentro del mismo y en la opción de bloquear los siguientes sitios se colocan los que fueron solicitados para esta actividad que son www.hotmail.com, www.youtube.com y www.elnuevodia.com.co se da guardar y aplicar . Ver Figura 12

Figura 10. Configuración proxy

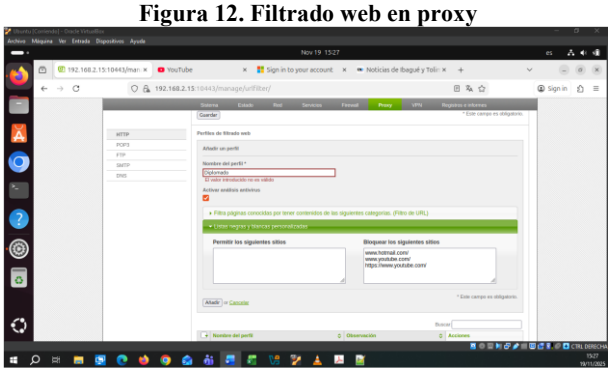


Fuente: Autoría Propia

Figura 11. Validación puertos proxy

Fuente: Autoría Propia

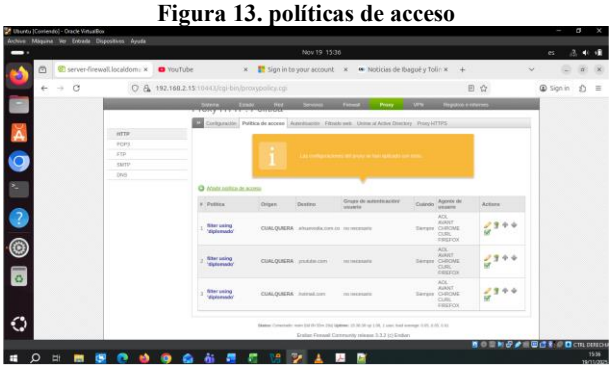
Figura 12. Filtrado web en proxy



Fuente: Autoría Propia

Posterior a ello se procede en la pestaña de proxy a ingresar a la pestaña política de acceso, añadimos una nueva política por cada uno de los sitios web donde se realiza restricción de acceso, dentro del cual seleccionamos cualquier tipo de origen, en el destino seleccionamos dominio, y en los agentes de usuarios agregamos los nombres de los navegadores seleccionando uno o varios dependiendo las restricciones o programas que tenga el equipo que va a acceder a las páginas creadas en las listas negras, aplicamos y guardamos, ver figura 13

Figura 13. políticas de acceso

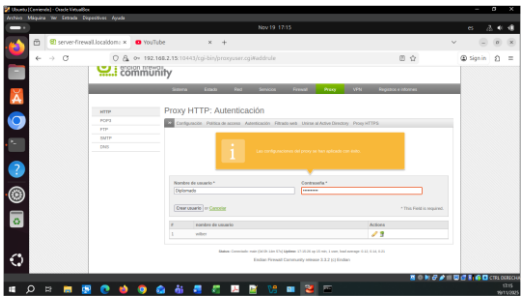


Fuente: Autoría Propia

5.2 Configuración de Autenticación por Usuario y Asociación a Políticas

Se procede a ingresa dentro del proxy a la pestaña de autenticación y se crean los usuarios junto con sus contraseñas los cuales van a ser utilizados para el acceso a las páginas previamente restringidas. Dentro de este módulo se debe crear un usuario junto con una contraseña segura, la cual será solicitada en el momento del acceso a las paginas Hotmail.com, youtube.com y elnuevodia.com.co. Ver figura 14

Figura 14. Creación usuarios de acceso



Fuente: Autoría Propia

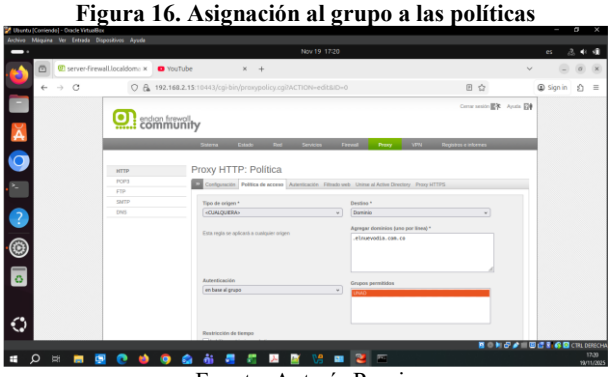
Dentro de la pestaña de autenticación procedemos a crear un grupo con los usuarios a los cuales va dirigida la política creada, esto debido a como se explicaba anteriormente cada área debe tener ciertos permisos hacia ciertos lugares de navegación para ser más eficiente el trabajo. Ver Figura 15.

Al guardar y aplicar los grupos y vincular los usuarios al mismo, se procede a ir nuevamente a la pestaña políticas de acceso y en la opción de autenticación cambiamos la opción a en base al grupo y en el recuadro donde dice grupos permitidos, agregamos el grupo creado previamente, esta tarea se debe realizar con cada una de las restricciones creadas para cada uno de los sitios previamente incluidos dentro de las listas. Ver figura 16 y 17

Figura 15. Asignación al grupo de usuarios

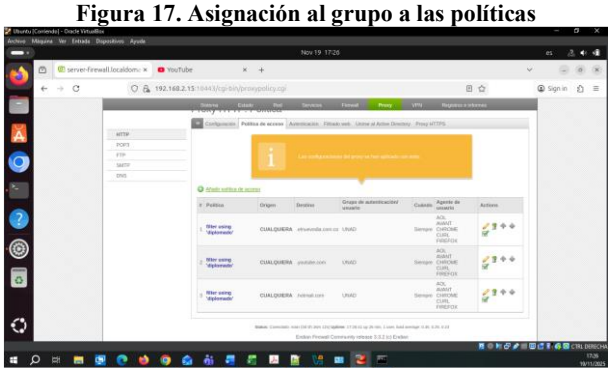
Fuente: Autoría Propia

Figura 16. Asignación al grupo a las políticas



Fuente: Autoría Propia

Figura 17. Asignación al grupo a las políticas



Fuente: Autoría Propia

Por último, si el servidor tiene vinculación con el directorio activo de la empresa o políticas de LDAP, automáticamente tomara los grupos que este tenga y le asignara los permisos respectivos de navegación

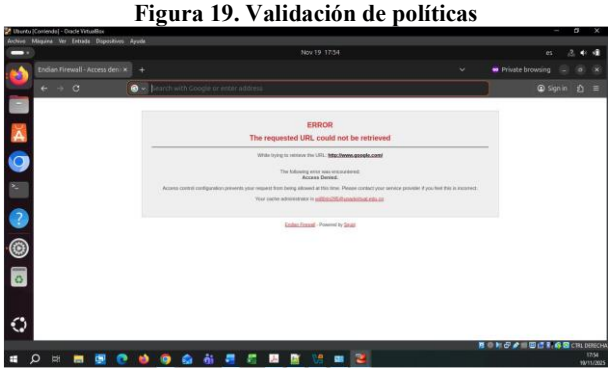
5.3 Validación del Bloqueo de Acceso desde la LAN a Sitios Restringidos

Finalmente, después de realizada y aplicada la configuración, se procede a acceder desde el navegador web a los sitios restringidos, donde como se parametrizo anteriormente se solicitará el usuario y clave para poder ingresar a los mismos, en caso tal informará que el usuario, o la calve están erróneas o que no se tiene los permisos correspondientes. Ver Figura 18, 19, 20 y 21

Figura 18. Validación de políticas

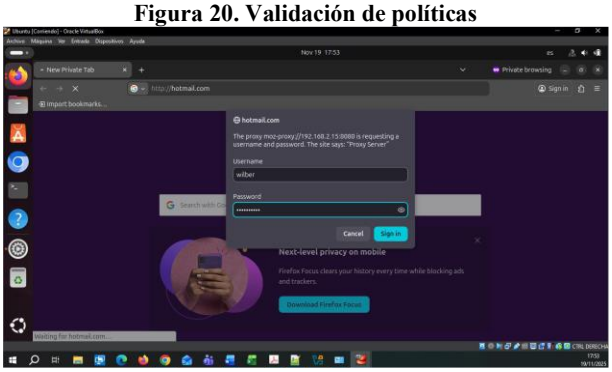
Fuente: Autoría Propia

Figura 19. Validación de políticas



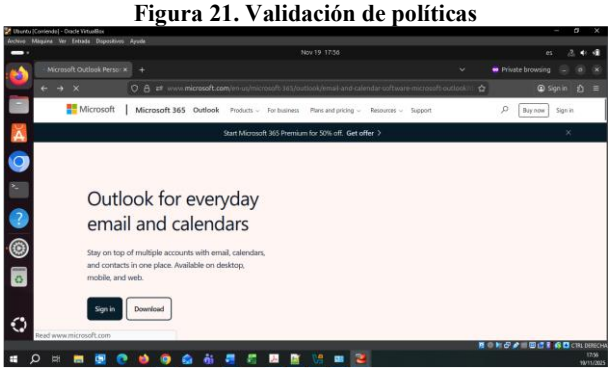
Fuente: Autoría Propia

Figura 20. Validación de políticas



Fuente: Autoría Propia

Figura 21. Validación de políticas



Fuente: Autoría Propia

6 CONCLUSIONES

La implementación de Endian Firewall (EFW) en un entorno virtualizado con VirtualBox demostró ser una solución efectiva para la segmentación de red y la seguridad perimetral. A través de la configuración de tres zonas diferenciadas —verde (LAN), naranja (DMZ) y roja (WAN)— se logró aislar servicios críticos y controlar el tráfico entre segmentos de red de manera granular.

La correcta configuración de reglas de NAT permitió la comunicación bidireccional entre la LAN y la WAN, así como el acceso controlado a servicios alojados en la DMZ. Adicionalmente, la implementación de un proxy HTTP con autenticación y políticas de filtrado facilitó el bloqueo selectivo de sitios web, mejorando el control sobre el uso de la red interna.

Cabe destacar que todos los procedimientos se ejecutaron mediante consola, lo que refuerza las competencias administrativas en entornos GNU/Linux y garantiza la replicabilidad de la solución en escenarios reales. Esta experiencia evidencia la viabilidad de utilizar herramientas de código abierto como Endian para construir infraestructuras seguras, escalables y de bajo costo, apropiadas para entornos educativos y organizacionales que requieran balancear flexibilidad y protección.

La configuración de reglas NAT de salida permitió establecer la comunicación de manera controlada entre las zonas internas LAN y DMZ hacia la red WAN. La aplicación de NAT fuente garantizó que los dos segmentos de red pudieran alcanzar y acceder a servicios externos mediante el enmascaramiento sin comprometer la estructura de direccionamiento interno y los resultados demuestran que el firewall Endian gestiona y controla de una manera eficiente la traducción de direcciones y mantiene un flujo de tráfico estable entre las zonas segmentadas.

La implementación de reenvío de puertos hacia un servicio específico, en nuestro caso un servicio web ubicado en la DMZ evidenció la capacidad del firewall Endian para publicar servicios externos de manera segura sin comprometer la red interna cumpliendo con los principios de aislamiento de la DMZ. Esta configuración confirma la importancia de usar zonas diferenciadas y políticas de traducción como un mecanismo de control para el acceso y mitigar riesgos en infraestructuras sensibles.

Las ventajas de la utilización de un servidor proxy van desde una seguridad mejorada, para evitar intrusión de piratas informáticos, navegación, observación y vigilancia al detalle de para que no se permita la recopilación de datos específicos de, al igual que llevar el control de un IP especifica.

Evitar fuga de información o ingreso a sitios inapropiados que distraigan a los funcionarios de las labores para los cuales fueron contratados adicional de bloquear sitios donde se realice pérdida de tiempo acorde a las funciones de cada persona, ejemplo redes sociales para las personas de contabilidad o sistemas, y habilitar las mismas para las personas de comunicaciones, mercadeo y demás

7 REFERENCIAS

[1] Endian. (2016). *Endian UTM 3.2 Manual de referencia*. https://docs.endian.com/3.2/utm/first.html#conventions-used-in-this-document

[2] Oracle. (2020). *Manual de usuario de VirtualBox*. https://www.virtualbox.org/manual/topics/networkingdetails.html#networkingdetails

[3] Stallings, W. (2021). Network Security Essentials: Applications and Standards (7th ed.). Pearson. https://api.pageplace.de/preview/DT0400.9781292154916_A37747529/preview-9781292154916_A37747529.pdf

[4] E. H. Miller, *"A note on reflector arrays"*, IEEE Trans. Antennas Propagat., Aceptado para su publicación.

[5] *Control Toolbox* (6.0), User´s Guide, The Math Works, 2001, pp. 2-10-2-35.

[6] J. Jones. (2007, Febrero 6). Networks (2nd ed.) [En línea]. Disponible en: http://www.atm.com.