IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD EN GNU/LINUX MEDIANTE ENDİAN

Jhon Mauricio Camargo Quintero
jmcamargoq@unadvirtual.edu.co
Juan Jesús González Espitia
jjgonzalezes@unadvirtual.edu.co
Chayanne Alfonso Sánchez García
casanchezgarcia@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación de medidas de seguridad en sistemas operativos GNU/Linux, con base en las buenas prácticas recomendadas para la protección de entornos de red LAN, WAN y DMZ. En el marco del diplomado en administración de sistemas operativos Open Source, se desarrollaron cinco temáticas clave: instalación y configuración de Endian Firewall (Endian, 2016), reglas de NAT (Endian, 2016), control de servicios en la zona DMZ (Endian, 2016), gestión del tráfico entre zonas de red y la implementación de un proxy HTTP con autenticación y políticas de acceso. Cada una de estas prácticas fue aplicada de forma colaborativa, simulando un entorno seguro y funcional. Se emplearon herramientas como VirtualBox (Oracle, 2020) y Ubuntu Server (Canonical Ltd., 2020) y la consola de Endian UTM, evidenciando el uso de comandos para el control y monitoreo de servicios.*

PALABRAS CLAVE: Endian Firewall, NAT, Proxy HTTP, Seguridad en Linux.

1 INTRODUCCIÓN

El uso de sistemas operativos basados en GNU/Linux ha crecido de manera significativa en entornos empresariales, educativos y personales debido a su estabilidad, flexibilidad y naturaleza de código abierto. Sin embargo, esta expansión también ha traído consigo nuevos desafíos en materia de seguridad informática (LaCroix, 2020). La protección de la información, el control de accesos y la correcta configuración de servicios son aspectos fundamentales para garantizar la integridad y confidencialidad de los sistemas. En este contexto, la presente investigación tiene como objetivo explorar e implementar buenas prácticas de seguridad en entornos GNU/Linux, aplicando herramientas como el endurecimiento del sistema, la gestión de usuarios y permisos, así como la utilización de mecanismos de detección de intrusos (Debian Project, 2023; LaCroix, 2020). A través de un enfoque práctico, se busca fortalecer los conocimientos del usuario sobre las medidas preventivas que contribuyen a mitigar vulnerabilidades y ataques frecuentes. Este artículo, enmarcado en las competencias del módulo, proporciona una guía estructurada y fundamentada para asegurar sistemas basados en Linux, resaltando su relevancia en la administración de tecnologías de la información seguras y eficientes.

2 ENDIAN

2.1 CARACTERÍSTICAS GENERALES

En primer lugar, se descargó la distribución de Endian UTM desde su sitio oficial y se instala en plataformas como VirtualBox o en hardware físico. Es compatible con arquitecturas x86.

Se utiliza el programa Oracle VM VirtualBox para la creación de una máquina virtual con las siguientes configuraciones:

- Tipo: Linux
- Versión: Oracle Linux (64 bit)
- Unidad óptica virtual: ISO

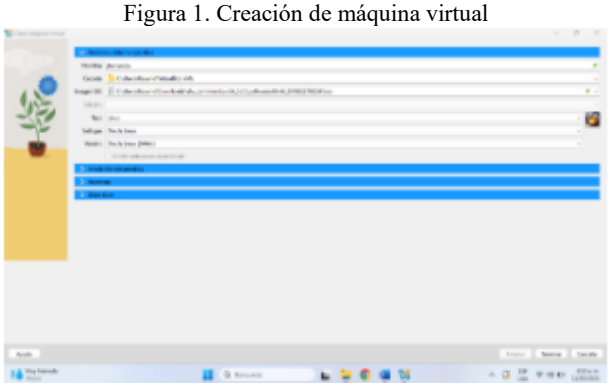
3 INSTALACIÓN Y CONFIGURACIÓN INICIAL DE ENDIAN FIREWALL

Esta sección describe los pasos fundamentales para la preparación del entorno virtual y la instalación básica de Endian Firewall, estableciendo la infraestructura necesaria para las configuraciones de seguridad subsiguientes.

3.1 PREPARACIÓN DE LA MÁQUINA VIRTUAL

Para la creación de la máquina virtual (MV) de Endian Firewall, se llevó a cabo la asignación de recursos computacionales esenciales para su correcto funcionamiento. Se configuraron la cantidad de memoria RAM, el número de procesadores (CPU) y el tamaño del disco duro. Aunque los valores numéricos exactos para estos recursos no se especifican en los materiales de referencia, se indica que fueron asignados de manera apropiada para el entorno simulado. La ausencia de valores específicos en los informes de los estudiantes no representa una deficiencia, sino que resalta un enfoque pedagógico particular. En este tipo de actividades formativas, el énfasis se coloca en el proceso de asignación de recursos y en la comprensión de la necesidad de cada componente (RAM para rendimiento, CPU para procesamiento, disco para almacenamiento), más que en la memorización de cantidades absolutas que pueden variar significativamente según el hardware disponible y los requisitos específicos de cada implementación. Esto fomenta una comprensión conceptual profunda y la capacidad de adaptar la configuración a diferentes escenarios.

Figura 1. Creación de máquina virtual



Fuente: Autoría Propia

Endian Firewall, al funcionar como un dispositivo de seguridad perimetral, requiere múltiples interfaces de red para segmentar y gestionar el tráfico de manera efectiva. Se configuraron tres adaptadores de red principales para establecer las diferentes zonas de seguridad:

- **Adaptador 1 (RED/WAN):** Este adaptador se configuró como un "adaptador puente" y se denominó "RED". Su función es conectar la máquina virtual a la red externa simulada, actuando como la interfaz hacia la WAN o Internet.

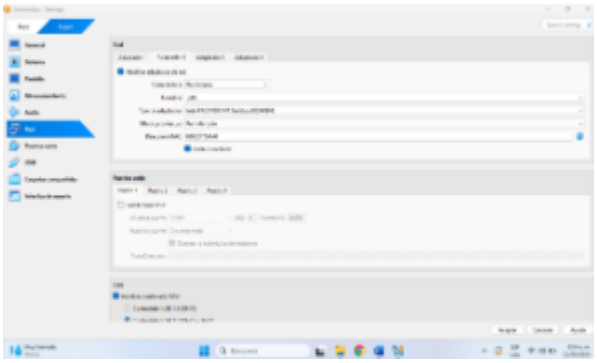
- **Adaptador 2 (GREEN/LAN):** Configurado como una "red interna" y denominado "LAN GREEN", este adaptador está destinado a la red local interna. Es la interfaz a través de la cual los dispositivos de la red interna se conectarán al firewall.

- **Adaptador 3 (DMZ ORANGE):** También configurado como una "red interna" y denominado "DMZ ORANGE", este adaptador se utiliza para la Zona Desmilitarizada. La DMZ es una subred que expone servicios públicos (como servidores web o FTP) a Internet de forma controlada, aislándolos de la red interna para añadir una capa de seguridad.

Figura 2. Adaptador 1 de red lo configurado como adaptador puente RED

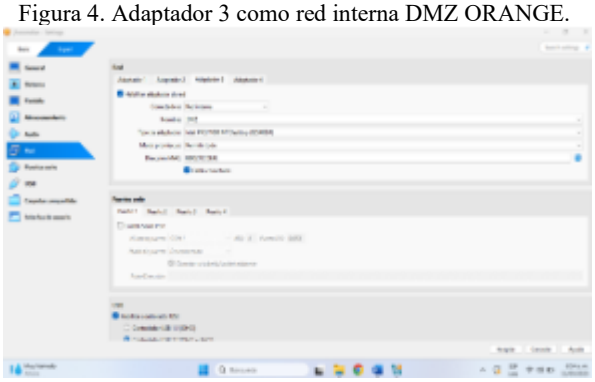
Fuente: Autoría Propia

Figura 3. Adaptador 2 como red interna LAN GREEN.



Fuente: Autoría Propia

Figura 4. Adaptador 3 como red interna DMZ ORANGE.



Fuente: Autoría Propia

La consistencia en la denominación de las zonas (RED, GREEN, ORANGE) y sus propósitos (WAN, LAN, DMZ) a lo largo de los diferentes documentos de los estudiantes sugiere la aplicación de una metodología de laboratorio o un currículo bien estructurado. Esta uniformidad en la arquitectura de red facilita que los estudiantes trabajen con un diseño común, lo que refuerza la comprensión de los principios de segmentación de red y seguridad perimetral de una manera estandarizada.

Tabla 1. Configuración de Adaptadores de Red de la Máquina Virtual Endian

Adaptador de Red	**Tipo de Red**	**Nombre de Zona**	**Propósito**
Adaptador 1	Puente	RED	WAN/Internet
Adaptador 2	Interna	LAN GEEN	LAN (Red Local
Adaptador 3	Interna	DMZ ORANGE	DMZ (Zona Desmilitarizada)

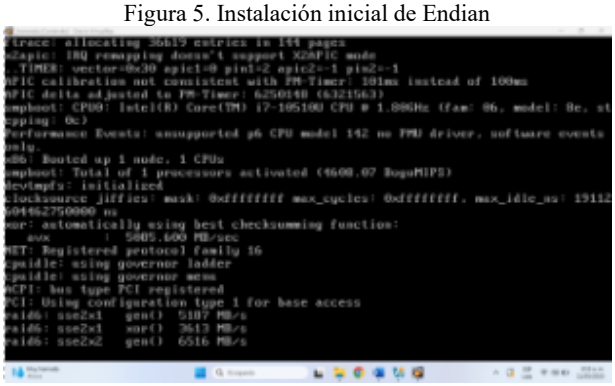
Fuente: Autoría Propia

3.2 PROCESO DE INSTALACIÓN DEL SISTEMA OPERATIVO ENDIAN

La instalación inicial de Endian Firewall se llevó a cabo directamente a través de la interfaz de la máquina virtual. Los pasos fundamentales para este proceso incluyeron:

- El inicio de la máquina virtual de Endian.
- La selección del idioma preferido para la instalación del sistema operativo.
- La confirmación explícita para que el instalador creara las particiones necesarias e instalara el sistema operativo en el disco virtual.
- La decisión de no habilitar el acceso al firewall a través de un puerto serial, una opción que no era requerida para los objetivos de esta implementación.
- El establecimiento de la dirección IP y la máscara de red para la interfaz GREEN, cuya configuración fue confirmada como exitosa, sentando las bases para la conectividad interna.

Figura 5. Instalación inicial de Endian



. Fuente: Autoría Propia

Figura 6. Instalación exitosa de endian

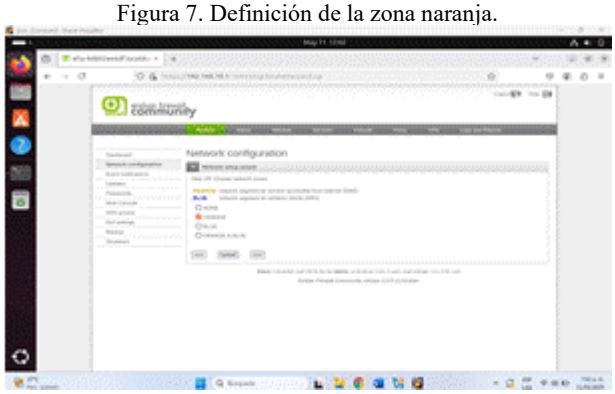
. Fuente: Autoría Propia

3.3 CONFIGURACIÓN DE ZONAS DE RED Y ACCESO WEB

Una vez completada la instalación básica, se procedió con la configuración detallada de las zonas de red y el acceso a la interfaz de gestión web de Endian Firewall, que es crucial para la administración posterior.

- **Configuración de Interfaces:** La interfaz RED (WAN) se configuró para obtener su dirección IP de forma dinámica mediante DHCP, lo que simula una conexión a un proveedor de servicios de Internet. Se confirmaron las direcciones IP estáticas para la interfaz GREEN (LAN) como 192.168.10.1 y para la interfaz ORANGE (DMZ) como 192.168.20.1, estableciendo los segmentos de red para cada zona. Además, se configuraron los servidores DNS 8.8.8.8 y 4.4.4.4 para la resolución de nombres de dominio.
- **Acceso a la Interfaz Web:** Con las zonas de red configuradas, se verificó el acceso a la interfaz web de Endian desde una máquina cliente (Ubuntu Desktop) previamente configurada. Esta máquina cliente se estableció con una dirección IP estática (192.168.10.20) dentro del segmento de la red LAN GREEN, asegurando que pudiera comunicarse con la interfaz de gestión del firewall. Tras ingresar las credenciales de inicio de sesión, se aplicaron los cambios de configuración pendientes, y el sistema mostró un mensaje de confirmación de aplicación exitosa, validando el acceso y la capacidad de gestión del firewall.

Figura 7. Definición de la zona naranja.



. Fuente: Autoría Propia

Figura 8. Confirmación de ip de red verde y naranja

. Fuente: Autoría Propia

4 TEMÁTICA 2: CONFIGURACIÓN NAT.

Producto esperado: 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). Configurar la regla de NAT, demostrando el establecimiento de la comunicación de la Zona DMZ hacia la Internet. Verificar en el reenvió de puertos / NAT, la creación de las reglas.

4.1 IMPLEMENTACIÓN DE REGLAS NAT PARA TRADUCCIÓN DE DIRECCIONES

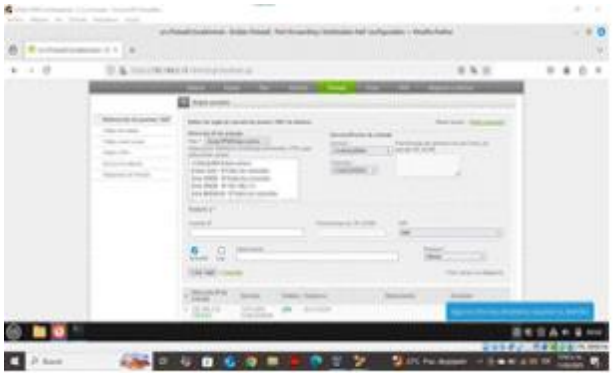
La configuración de NAT es un pilar fundamental en la seguridad de red, permitiendo que múltiples dispositivos en una red privada compartan una única dirección IP pública [5], y controlando el flujo de tráfico entre distintas zonas de red.

- **NAT para comunicación LAN hacia WAN:** Se implementó una regla de NAT específica para facilitar que el tráfico originado en la red LAN (zona GREEN) pudiera salir hacia la WAN (zona RED), simulando así el acceso a Internet. Esta configuración es crucial para permitir que los dispositivos internos de la red puedan iniciar y mantener conexiones con recursos externos.
- **NAT y reenvío de puertos para la Zona DMZ hacia Internet (HTTP, FTP):** Para posibilitar el acceso a servicios alojados en la DMZ (zona ORANGE) desde Internet (zona RED), se configuraron reglas de reenvío de puertos (Port Forwarding). Específicamente, se establecieron reglas para:
- Permitir el tráfico HTTP (puerto 80) desde la LAN hacia la DMZ.
- Permitir el tráfico HTTP (puerto 80) desde la RED (Internet) hacia la DMZ.
- Permitir el tráfico FTP (puerto 21) desde la RED (Internet) hacia la DMZ.
- Estas reglas de NAT son esenciales para asegurar que las solicitudes entrantes dirigidas a la dirección IP pública de Endian en puertos específicos sean correctamente redirigidas a los servidores correspondientes ubicados dentro de la DMZ, permitiendo la exposición controlada de servicios.

Figura 9. Creación de la regla de NAT, LAN hacia la WAN

. Fuente: Autoría Propia

Figura 9. Configurar la regla de NAT, demostrando el establecimiento de la comunicación de la Zona DMZ hacia la Internet.



Fuente: Autoría Propia

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

5.1 ESTABLECIMIENTO DE REGLAS DE FIREWALL PARA CONTROL DE TRÁFICO

Complementando las configuraciones de NAT, se establecieron reglas de firewall para controlar explícitamente el flujo de datos entre las distintas zonas de red. El propósito principal de estas reglas es asegurar que solo el tráfico autorizado circule por la red, mientras que el tráfico no deseado sea bloqueado de manera efectiva. Esta granularidad en el control es vital para mantener la integridad y la confidencialidad de los datos.

Figura 10. Configuración de la regla puerto 21

. Fuente: Autoría Propia

Figura 11. Configuración de regla puerto 80.

. Fuente: Autoría Propia

5.2 VERIFICACIÓN DE CONECTIVIDAD Y TRÁFICO

La verificación es una fase indispensable para confirmar la correcta implementación y el funcionamiento de las reglas de NAT y firewall.

- **Pruebas de Ping y Acceso a Servicios:** Se llevaron a cabo pruebas de conectividad exhaustivas, incluyendo la ejecución de comandos ping desde el cliente hacia el servidor y viceversa. Los resultados de estas pruebas confirmaron que las reglas de NAT habían sido configuradas correctamente, permitiendo el acceso bidireccional entre la LAN y la WAN, y entre la DMZ y la Internet simulada.
- **Análisis de Logs del Firewall:** Para una verificación más detallada, se supervisaron los registros de tráfico del firewall en tiempo real. Este monitoreo permitió confirmar el acceso a los servicios HTTP y FTP, y verificar que el tráfico se gestionaba de manera adecuada, sin bloqueos inesperados. Sin embargo, a pesar de las observaciones iniciales de "configuraciones exitosas" y "tráfico gestionado sin bloqueos", un análisis más profundo de los registros de tráfico reveló que algunas conexiones fueron rechazadas. Esta aparente contradicción subraya la complejidad inherente a la configuración de firewalls y NAT en entornos reales o simulados. Indica que una verificación inicial puede no capturar todos los escenarios posibles, o que se requiere un ajuste fino continuo de las reglas. Esto pone de manifiesto que la seguridad de red no es una tarea estática, sino un proceso iterativo que demanda una configuración, prueba y refinamiento constantes para adaptarse a las dinámicas del tráfico y las necesidades de seguridad.

Figura 12. Verificación de logs

. Fuente: Autoría Propia

Figura 13. Verificación de tráfico exitoso.

. Fuente: Autoría Propia

Tabla 2. Resumen de Reglas NAT y Reenvío de Puertos Implementadas

Origen	Destino	Protocolo	Puerto Original	Puerto Destino (DMZ)
Lan	Wan	Cualquiera	N/A	N/A
Lan	Dmz	Tcp	80 (Http)	80
Lan	Dmz	Tcp	21 (Ftp)	21
Red	Dmz	Tcp	80 (Http)	80
Red	Dmz	Tcp	21 (Ftp)	21

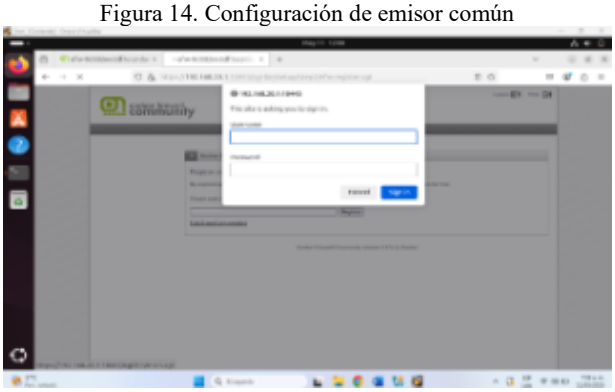
Fuente: Autoría Propia

6 TEMATICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

Esta sección explora la segmentación de la red y la implementación de servicios de seguridad avanzados, como el

proxy y el filtrado de contenido, utilizando las capacidades de Endian Firewall.

Figura 14. Configuración de emisor común



. Fuente: Autoría Propia

6.1 DISEÑO Y CONFIGURACIÓN DE SEGMENTOS DE RED (LAN Y DMZ)

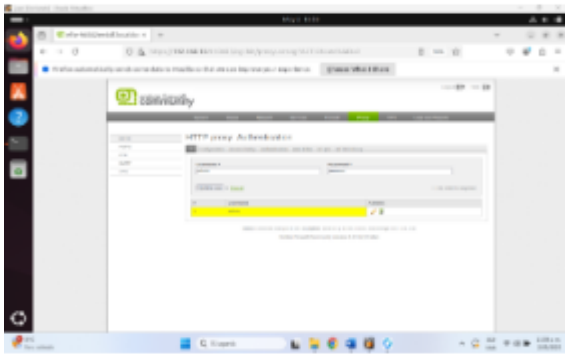
La segmentación de red constituye una estrategia fundamental para mejorar la seguridad, al permitir el aislamiento de diferentes tipos de tráfico y recursos. Se configuraron las interfaces de Endian Firewall para establecer una segregación clara entre las redes LAN (GREEN) y DMZ (ORANGE), garantizando una separación efectiva y una mayor protección.

- **Asignación de Direcciones IP y Rangos:** La red LAN (GREEN) fue configurada con el segmento de red 192.168.10.0/24, donde Endian Firewall actuaba como la puerta de enlace con la dirección 192.168.10.1. Por su parte, la red DMZ (ORANGE) se estableció con el segmento 192.168.20.0/24, con Endian operando en la dirección 192.168.20.1. Para la interacción dentro de la red interna, una máquina cliente (Ubuntu Desktop) en la LAN se configuró con una dirección IP estática de 192.168.10.6/24.

Figura 15. Confirmamos RED DHCP.

. Fuente: Autoría Propia

Figura 16. Creación de usuarios.



. Fuente: Autoría Propia

6.2 ACTIVACIÓN Y GESTIÓN DE SERVICIOS DE RED

Para optimizar la gestión y el funcionamiento de la red interna, se activaron servicios esenciales que facilitan la administración y mejoran la experiencia del usuario.

- Configuración del Servicio DHCP para la Red LAN: Se configuró el servicio DHCP (Dynamic Host Configuration Protocol) en Endian Firewall para la red LAN (GREEN). Esta implementación permite la asignación automática de direcciones IP a los dispositivos cliente que se conectan a este segmento, lo que simplifica enormemente la administración de la red y asegura que todas las zonas sean accesibles de acuerdo con las políticas de seguridad establecidas

Figura 17. Confirmación de configuración de RED en DHCP.

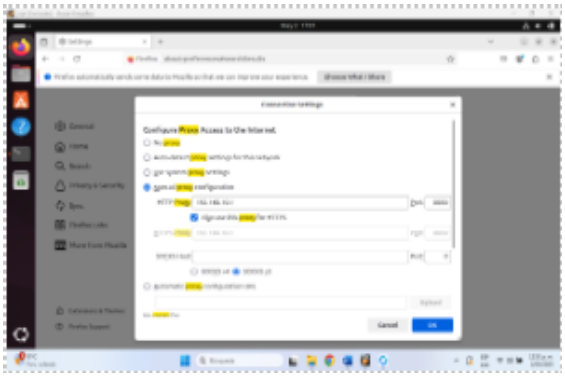
. Fuente: Autoría Propia

6.3 IMPLEMENTACIÓN DE PROXY Y FILTRADO DE CONTENIDO WEB

El servicio de proxy, junto con el filtrado de contenido, representa una herramienta crucial para controlar y monitorear el acceso a Internet, lo que se traduce en mejoras significativas tanto en la seguridad como en la productividad de la red.

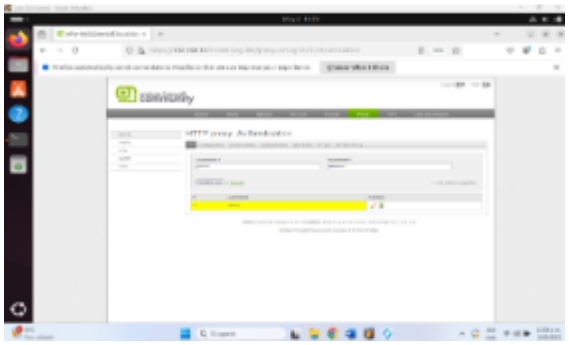
- **Habilitación del Servicio de Proxy:** El servicio de proxy se habilitó en Endian Firewall. Para que los clientes pudieran utilizarlo, se configuraron manualmente los navegadores (por ejemplo, Firefox) para que apuntaran a la dirección IP de Endian en la interfaz GREEN (192.168.10.1) como servidor proxy tanto para el tráfico HTTP como para HTTPS.
- **Creación de Usuarios y Grupos para Autenticación:** Se procedió a la creación de un usuario en el módulo de autenticación de Endian Firewall, el cual fue posteriormente asociado a un grupo específico (por ejemplo, el grupo "juan" con el usuario "admin"). La integración de la autenticación de usuario con el servicio de proxy y el filtrado de contenido añade una capa de seguridad y control más allá del simple filtrado de URLs. Esta funcionalidad permite no solo determinar qué contenido es accesible, sino también registrar y controlar quién accede a la red y bajo qué políticas. Esto representa un avance hacia una gestión de seguridad más granular y responsable, alineándose con principios de auditoría y control de acceso en entornos empresariales. Permite la implementación de políticas de acceso diferenciadas para distintos usuarios o departamentos, optimizando el control de acceso y la rendición de cuentas.
- **Configuración de Políticas de Acceso y Listas Negras de Sitios Web:** Se implementó un filtro de contenido específico, denominado "lista negra" (blacklist), con el objetivo de bloquear el acceso a sitios web predefinidos. En los ejemplos prácticos, se incluyeron www.hotmail.com, www.youtube.com y www.elnuevodia.com.co en esta lista. Adicionalmente, se creó una política de acceso que vinculaba al usuario "admin" con esta regla de filtrado, asegurando que las restricciones se aplicaran a usuarios específicos.
- **Verificación del Filtrado de Contenido:** Para validar la efectividad del filtro de contenido, se realizaron pruebas de acceso desde el cliente configurado con el proxy. Al intentar navegar a los sitios web incluidos en la "lista negra", los intentos resultaron en solicitudes de autenticación y, posteriormente, en mensajes de bloqueo, confirmando que la política de filtrado operaba según lo previsto y que el acceso a los sitios prohibidos estaba efectivamente restringido (Oracle, 2020).

Figura 17. Configuración de proxy en Firefox.



. Fuente: Autoría Propia

Figura 18. Creación de usuarios.



. Fuente: Autoría Propia

Figura 19. Creación de lista negra.

. Fuente: Autoría Propia

Figura 20. Verificación del Filtrado de Contenido

. Fuente: Autoría Propia

Tabla 3. Políticas de Filtrado de Contenido del Proxy

Nombre del Filtro	Sitios Web Bloqueados	Grupo Asociado	Resultado Esperado
Lista negra	www.hotmail.com	admin	Acceso Bloqueado
Lista negra	www.youtube.com	admin	Acceso Bloqueado
Lista negra	www.elnuevodia.co	admin	Acceso Bloqueado

Fuente: Autoría Propia

7 IMPLEMENTACIÓN DE VPNS Y ACCESO REMOTO SEGURO

La capacidad de establecer conexiones seguras a redes privadas a través de una red pública, como Internet, es fundamental en la administración de redes modernas. Las Redes Privadas Virtuales (VPNs) ofrecen una solución robusta para el acceso remoto seguro, y Endian Firewall proporciona herramientas integradas para su implementación.

7.1 CONFIGURACIÓN DE OPENVPN EN ENDIAN FIREWALL

OpenVPN es una solución de VPN de código abierto ampliamente utilizada por su flexibilidad y seguridad. En Endian Firewall, la configuración de OpenVPN implica varios pasos clave para establecer un servidor VPN y generar certificados para los clientes (OpenVPN Technologies Inc., 2024).

1. **Activación del Servicio OpenVPN:** Desde la interfaz de administración web de Endian, se navega a la sección de "VPN" y se activa el servicio OpenVPN. Esto inicializa los componentes necesarios para el servidor VPN.

2. **Configuración de Parámetros del Servidor:** Se definen los parámetros de la red VPN, incluyendo el rango de direcciones IP que se asignarán a los clientes VPN (e.g., 10.8.0.0/24), el puerto de escucha (usualmente UDP 1194), y los servidores DNS que los clientes utilizarán una vez conectados. Es crucial asegurar que el rango de IP de la VPN no se solape con las redes LAN o DMZ existentes.

3. **Generación de Certificados y Claves:** Endian Firewall facilita la creación de la Autoridad de Certificación (CA) interna, así como los certificados y claves para el servidor y los clientes VPN. Cada cliente remoto requerirá un certificado único para autenticarse con el servidor VPN.

7.2 CONFIGURACIÓN DE CLIENTES OPENVPN

Una vez que los certificados de cliente han sido generados en Endian Firewall, los usuarios remotos deben configurar sus clientes OpenVPN para conectarse al servidor.

1. **Descarga del Perfil de Cliente:** Endian Firewall permite descargar un archivo de configuración (.ovpn) que incluye el certificado del cliente, la clave privada y la configuración del servidor. Este archivo simplifica la configuración del cliente.

2. **Instalación del Cliente OpenVPN:** El usuario remoto debe instalar el software cliente de OpenVPN en su dispositivo (Windows, macOS, Linux, Android, iOS) (OpenVPN Technologies Inc., 2024).

3. **Importación del Perfil:** El archivo. ovpn descargado se importa al cliente OpenVPN. Esto configura automáticamente la conexión, incluyendo la dirección del servidor, los certificados y las claves necesarias.

7.3 VERIFICACIÓN DEL ACCESO REMOTO SEGURO

Para asegurar que la conexión VPN funciona correctamente y que el acceso remoto es seguro, se realizan pruebas de conectividad y se monitorean los logs.

1. **Pruebas de Conectividad VPN:** Desde un cliente remoto, se inicia la conexión VPN. Una vez establecida, se realizan pruebas de ping y acceso a recursos internos (e.g., servidores en la LAN) para verificar que el tráfico se enruta correctamente a través del túnel VPN.

2. **Monitoreo de Logs de VPN:** En la interfaz de Endian Firewall, se revisan los logs del servicio OpenVPN para confirmar las conexiones exitosas de los clientes, detectar intentos de acceso no autorizados y diagnosticar posibles problemas de conexión. (Ubuntu Server, 2015).

La implementación de VPNs con Endian Firewall no solo proporciona un acceso remoto seguro, sino que también extiende las políticas de seguridad de la red interna a los usuarios que se conectan desde ubicaciones externas,

garantizando la confidencialidad e integridad de los datos en tránsito.

8 CONCLUSIONES

La implementación y configuración de Endian Firewall en un entorno virtualizado, detallada en este artículo, ha proporcionado una experiencia práctica invaluable para la comprensión profunda de la seguridad de red en sistemas GNU/Linux.

Se logró configurar con éxito la traducción de direcciones de red (NAT), facilitando la comunicación fluida desde la LAN hacia la WAN y el reenvío de puertos a la DMZ para servicios críticos como HTTP y FTP. Esta capacidad es fundamental para asegurar la conectividad y la exposición controlada de servicios a la red externa. La implementación de reglas de firewall y políticas de acceso, que incluyeron el filtrado de contenido web y la autenticación de usuarios [1], [4], permitió un control granular sobre el tráfico de red, demostrando la capacidad de Endian Firewall para aplicar directivas de seguridad complejas y adaptadas a las necesidades específicas de la red.

La segmentación de la red en zonas diferenciadas (LAN, WAN, DMZ) mediante Endian Firewall se confirmó como una estrategia altamente eficaz para aislar recursos y limitar el impacto de posibles brechas de seguridad. Las políticas de tráfico implementadas aseguran que solo las conexiones autorizadas puedan acceder a los recursos críticos, lo que fortalece significativamente la defensa frente a amenazas externas y optimiza el control del tráfico en toda la infraestructura de red.

La realización de estos ejercicios en un entorno simulado con Endian Firewall ha permitido consolidar los conocimientos teóricos y prácticos sobre la administración de sistemas operativos Open Source y la seguridad de red. La plataforma Endian facilita la experimentación con configuraciones de red complejas de manera segura y controlada, lo cual es esencial para el desarrollo de habilidades en ciberseguridad. La experiencia subraya la importancia de la revisión minuciosa de las reglas y la supervisión continua de los registros de tráfico para garantizar tanto la disponibilidad como la seguridad de los servicios en la red. Se reconoce que la configuración de seguridad es un proceso dinámico e iterativo de ajuste y mejora constante, donde la identificación y corrección de bloqueos inesperados son parte integral del ciclo de vida de la seguridad de red.

9 REFERENCIAS

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

[2] Canonical. (2023). Guía del Ubuntu desktop 20.04 LTS. https://help.ubuntu.com/20.04/ubuntu-help/index.html

[3] Oracle. (220). Manual de usuario VirtualBox. https://www.vrtualbox.org/manual/

[4] Debian. (2023). Manual del administrador de Debian 12.5.0. https://www.debian.org/releases/stable/amd64/index.es.html

[5] Canonical (2024). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. https://help.ubuntu.com/20.04/ubuntu help/index.html

[6] Debian (2024). El manual del administrador de Debian 12.5.0. Debian https://www.debian.org/releases/stable/amd64/in dex.es.html

[7] Jay LaCroix. (2020). Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting

[8] Debian. (2023). Manual del administrador de Debian 12.5.0. https://www.debian.org/releases/stable/amd64/index.es.html

[9] Ubuntu Server. Packt Publishing. https://research-ebsco com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b88 1bf72-20a7-343c 94a8-f12e88b41952

[10] Canonical. (2023). Guía del Ubuntu