IMPLEMENTACIÓN DE LA SEGURIDAD EN GNU/LINUX CON ENDIAN

Danid Mercedes Mora Botía
Cédula1052397929
Dmmora@unadvirtual.edu.co
Erika Milena Muñoz Castañeda
Cédula 1113334278
Emmunozcas@unadvirtual.edu.co
Nidia Yaneth Pardo Mozo
Cédula 46682102
nypardom@unadvirtual.edu.co

RESUMEN: *Desde un entorno de virtualización VirtualBox, se realiza la configuración de 3 máquinas virtuales Ubuntu Server, Ubuntu Desktop y Endian, donde se configuraron las redes desde Endian para poder generar una conexión entre las maquinas a través de la red NAT, en donde se divide las redes entre Desktop red verde y Server red Naranja para hacer conexión desde una IP estática, que será suministrada por Endian; al iniciar las máquinas virtuales se realiza la respectiva instalación, partiendo de una arquitectura de red suministrada en la temática 1, se llevará a cabo desde Endian Firewall Comunity y así generar comunicación entre NAT y DMZ, por tanto, la ingeniería de Sistemas, hace un importante aporte al conocimiento de los diferentes sistemas Open Source o software libre e ir a la vanguardia de las tecnologías ofreciendo a las empresas un sistema con eficacia, eficiencia en sus procesos, asegurando el activo principal "la información".*

PALABRAS CLAVE: *Endian, Firewall, NAT, DMZ, Red.*

INTRODUCCIÓN

Este articulo describe la configuración de las redes de GNU/Linux mediante Endian, especial para el uso de firewall, considerada una de las soluciones más eficientes para seguridad en comunidades empresariales; se retoman las temáticas de redes implementada sobre la máquina virtual VirtualBox, asegurando un ingreso óptimo a la topología de la red, desde Ubuntu Desktop y Ubuntu Server desde diferentes servidores con una IP estática. Así mismo, se pone en práctica mediante diferentes temáticas como son la configuración de la instancia para GNU/Linux Endian, la configuración NAT desde Endian, permitir Servicio desde la Zona Desmilitarizada (DMZ), reglas de acceso para permitir o denegar el tráfico e Implementar un Proxy HTTP con políticas de autenticación para navegación en Internet, donde estas 5 temáticas, ayudarán a comprender el uso demostrando el establecimiento de la comunicación desde la LAN hacia la WAN, demostrando el establecimiento de la comunicación de la Zona DMZ hacia la Internet, permitir los servicios HTTP y FTP desde el servidor Web bajo Ubuntu Server, Denegar el protocolo ICMP además de no permitir hacer ping en la red, comunicar la zona Verde con la zona Naranja, con el protocolo HTTP y FTP con sus respectivos puertos y finalmente crear un perfil y establecer una lista negra bloqueando sitios.

1 SOLUCIÓN A LA SEGUIRDAD PERIMETRAL MEDIANTE ENDIAN

1.1 CARACTERISTICAS

Para garantizar la protección de los servidores que conforman la intranet (LAN) / extranet (WAN), donde se requiere delimitarlos a través de una zona DMZ y así garantizar la seguridad e integridad de las bases de datos y aplicaciones bajo plataformas GNU/Linux.

2 TEMÁTICA 1

2.1 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX

En la implementación del sistema GNU/Linux Endian en VirtualBox, fue necesario realizar una configuración adecuada de la instancia para garantizar el funcionamiento correcto del firewall y la segmentación de la red. (Endian, s.f.) El proceso comenzó con la creación de una máquina virtual, seleccionando el sistema operativo Linux y asignando los recursos básicos como memoria RAM, disco duro virtual y la carga del archivo ISO de Endian para proceder con su instalación. (Oracle s.f.)

Figura 1. Descarga Endian

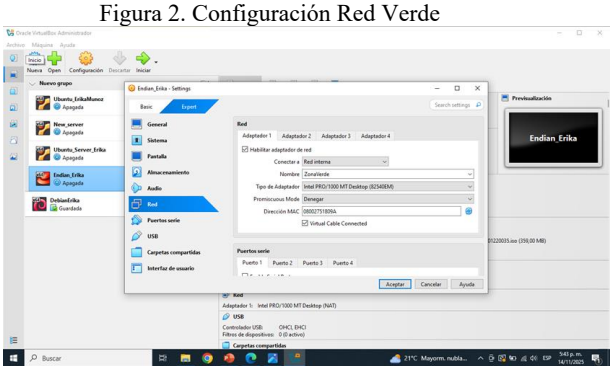
Fuente: Autoría Propia

En la implementación del sistema GNU/Linux Endian en VirtualBox, se hizo la segmentación de red mediante la configuración de las tres zonas principales que utiliza este firewall: la zona roja, la zona verde y la zona naranja. (Nemeth et al.,2017) Para lograrlo, fue necesario crear una máquina

virtual y asignar tres adaptadores de red, cada uno con un propósito específico dentro de la estructura del sistema a continuación:

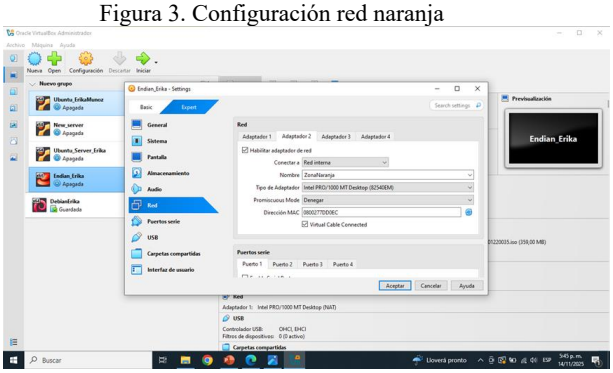
LAN eth0 192.168.2.15/24 MAC 08002751809A Zona verde: Red interna desktop DMZ eth1 192.168.1.15/24 MAC 0800277DD0EC Zona naranja: Servidores (DMZ). Server BRIDGE eth2 10.0.4.15/24 MAC 0800278D458D Zona roja: Acceso a internet (WAN) red NAT.

Figura 2. Configuración Red Verde



Fuente: Autoría Propia

Figura 3. Configuración red naranja



Fuente: Autoría Propia

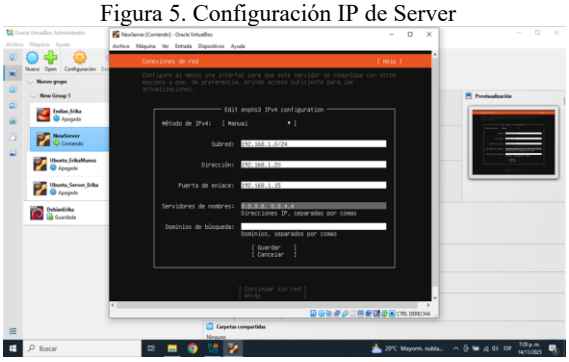
Figura 4. Configuración Red Roja

Fuente: Autoría Propia

En la implementación de GNU/Linux Endian en VirtualBox se realizó la segmentación de red configurando las zonas roja, verde y naranja. En la zona verde, el cliente usó la IP 192.168.2.15 y Endian 192.168.2.20. En la zona naranja se asignó la IP 192.168.1.15 a Endian y 192.168.1.20 al servidor. La zona roja quedó en NAT para el acceso a Internet. Así se completó la segmentación del sistema.

2.1.2 AJUSTE DE ADAPTADORES DE RED EN UBUNTU SERVER Y DESKTOP Y PREPARACIÓN DEL ENTORNO PARA EL INICIO DE ENDIAN FIREWALL

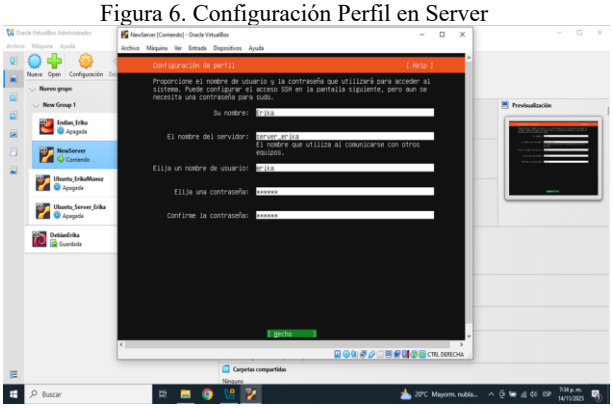
Figura 5. Configuración IP de Server



Fuente: Autoría Propia

Asignación y Establecimiento de la Dirección IP del Servidor, junto con la Adecuación y Organización de los adaptadores de red en Ubuntu Server y Ubuntu Desktop, como Fase Previa para la Puesta en Marcha, Inicialización y Operación del Sistema de Seguridad Endian Firewall. (Nemeth et al.,2017)

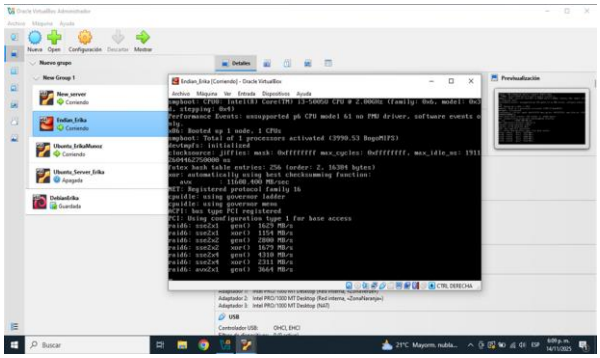
Figura 6. Configuración Perfil en Server



Fuente: Autoría Propia

Configuración del Perfil en el Servidor y Adecuación de los Parámetros de Red como Preparación para la Puesta en Marcha del Sistema Endian Firewall.

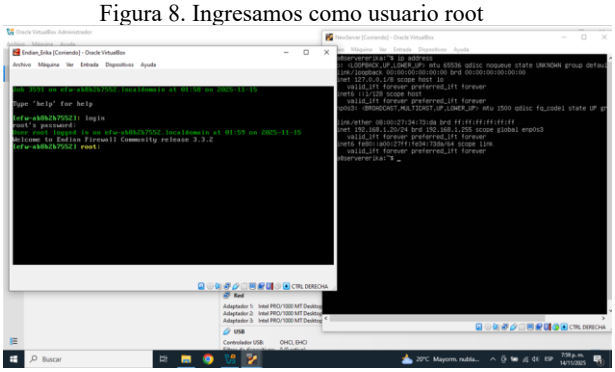
Figura 7. Inicio de Endian



Figu
Fuente: Autoría Propia

Proceso de Inicio del Sistema Endian Firewall y la Preparación Integral del Entorno de Red en el Servidor como Parte Fundamental de la Implementación del Esquema de Seguridad. (Endian, s.f.)

Figura 8. Ingresamos como usuario root

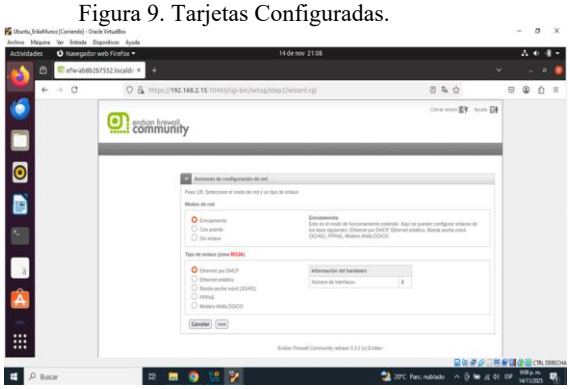


Fuente: Autoría Propia

Acciones Posteriores al Ingreso por el Shell en Endian Firewall al Verificar el Acceso como Usuario Root y Continuar con la Configuración Inicial.

2.1.3 INICIO DEL SISTEMA ENDIAN FIREWALL TRAS LA ACEPTACIÓN DE RIESGOS DE ACCESO E INGRESO EFECTIVO AL ENTORNO DE ADMINISTRACIÓN

Figura 9. Tarjetas Configuradas.



Fuente: Autoría Propia

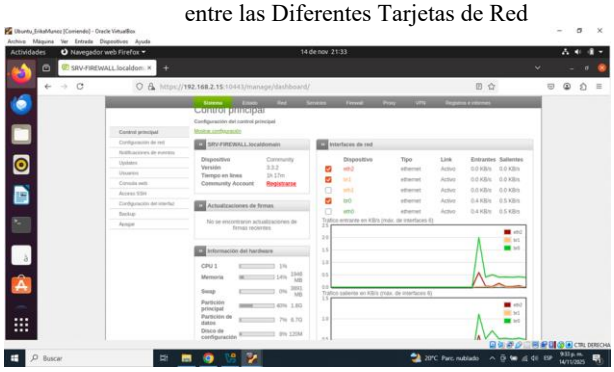
Visualización Detallada y Verificación Completa del Estado de las Tarjetas de Red Configuradas dentro del Entorno Operativo del Sistema Endian Firewall

Figura 10. Comunicación con la IP asignada

Fuente: Autoría Propia

Verificación y Establecimiento de la Comunicación Exitosa con la Dirección IP Asignada en el Entorno de Endian Firewall

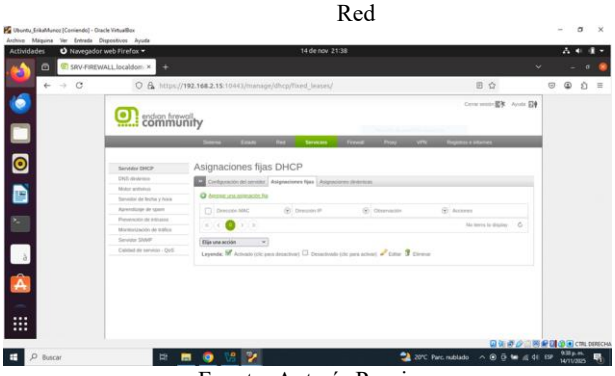
Figura 11. Visualización del Bridge Configurado entre las Diferentes Tarjetas de Red



Fuente: Autoría Propia

Visualización y Análisis de la Estructura de Bridge Implementada entre las Interfaces de Red en el Entorno de Endian Firewall. (Nemeth et al.,2017).

Figura 12. IP Fijas por MAC para Dispositivos de Red



Fuente: Autoría Propia

3 TEMATICA 2

3.1 CONFIGURACIÓN NAT.

Configurar la regla de NAT (Network Address Translation / Traducción de Direcciones de Red) permite la comunicación de varios dispositivos a través de una dirección IP pública, demostrando el establecimiento de la comunicación desde la LAN hacia la WAN (Red simulada de Internet). Este proceso se realiza comúnmente en routers o cortafuegos, que controlan y administran el tráfico entre redes internas y externas (Tanenbaum & Wetherall, 2011).

Según Cisco (s.f.), NAT facilita la traducción de direcciones privadas a direcciones públicas para permitir acceso a Internet desde la red local. Así mismo, la configuración de reglas NAT permite establecer la comunicación desde la Zona DMZ hacia Internet, traduciendo la red privada del dispositivo ubicado en dicha zona a una IP pública (Cisco, s.f.). Esto también permite implementar funciones de reenvío de puertos y la creación de reglas necesarias para publicar servicios hacia el exterior.

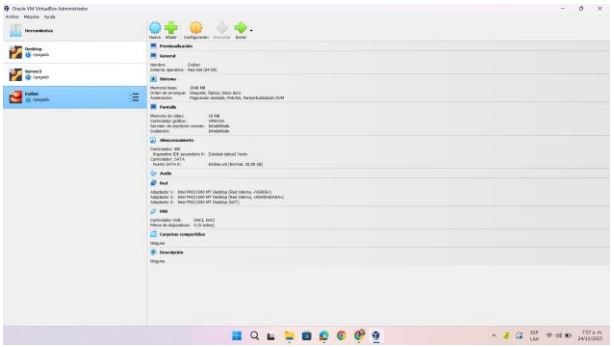
3.1.1 CONFIGURACIÓN DE LAS REDES EN GNU/LINUX ENDIAN

Para el desarrollo de la temática, se utilizó VirtualBox, instalando Ubuntu Server, Ubuntu Desktop y Endian Firewall 3.2. De acuerdo con Oracle (s.f.), VirtualBox permite crear adaptadores y redes internas que facilitan la simulación de entornos complejos. Desde Endian se realizó la actualización y configuración de las interfaces de red, que se gestionan según las zonas establecidas en el firewall (Endian, s.f.):

Adaptador 1: Red interna Verde (LAN)
Adaptador 2: Red interna Naranja (DMZ)
Adaptador 3: Red Roja mediante NAT (WAN)

La Red NAT utiliza conexiones a través del host para proporcionar salida a Internet, compartiendo la dirección IP del equipo físico y funcionando como puente hacia redes externas (Oracle, s.f.).

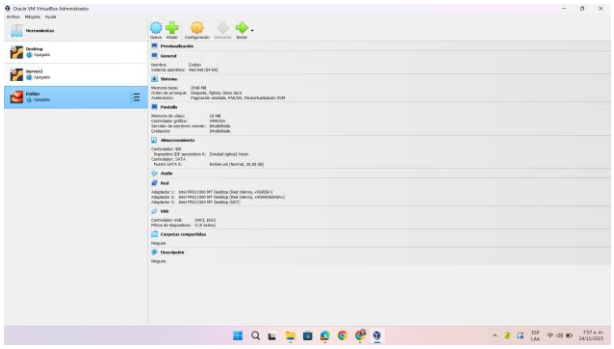
Figura 13. Configuración redes verde, naranja y NAT



Fuente: Autoría Propia

La red interna LAN, corresponde a la red interna destinada a los clientes. Conecta el router o firewall con los dispositivos del mismo segmento, permitiendo el intercambio de información local (Tanenbaum & Wetherall, 2011).
Interfaz: eth0
Dirección: 192.168.2.15/24
MAC: 08:00:27:62:19
Zona: Verde – Red interna del Desktop.

Figura 14. Configuración Red Verde.



Fuente: Autoría Propia

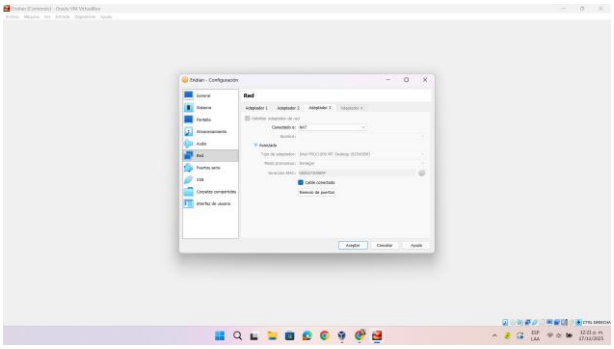
La red Naranja o DMZ (Zona Desmilitarizada) es el segmento donde se ubican servidores de acceso público, aislándolos de la red interna para evitar que un compromiso afecte otros segmentos (Tanenbaum & Wetherall, 2011).
Interfaz: eth1
Dirección: 192.168.1.15/24
MAC: 08:00:27:9B:BE:89
Zona: Naranja – Servidores Server2

Figura 15. Configuración red Naranja Server2 y verificación de MAC asignada.

Fuente: Autoría Propia

La red roja (WAN -NAT) o bridge es una interconexión entre máquinas virtuales que permite compartir el mismo dominio de broadcast y algunos servicios como DHCP (Nemeth et al., 2017). En el caso de Endian, esta zona representa la conexión hacia Internet:
Interfaz: eth2
Dirección: 10.0.4.15/24
MAC: 08:00:27:3C:B3:66
Zona: Roja – Acceso a Internet

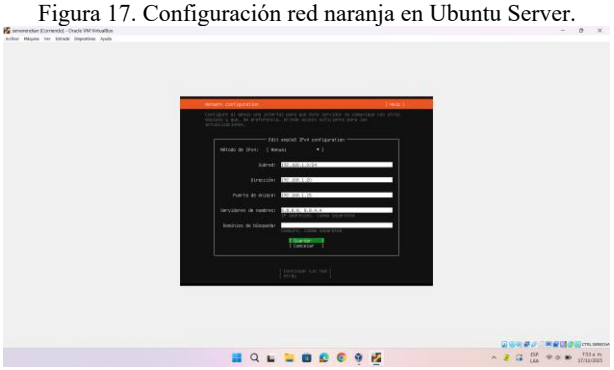
Figura 16. Configuración red NAT en Endian y verificación de MAC asignadas.



Fuente: Autoría Propia

Al configurar la máquina virtual Server, se asignó una dirección estática dentro de la subred 192.168.1.0/24, utilizando como puerta de enlace la dirección 192.168.1.15 correspondiente a la red Naranja. Los servidores DNS utilizados fueron 8.8.8.8 y 8.8.4.4, los cuales, según Google (s.f.), mejoran la velocidad y confiabilidad en la resolución de nombres.

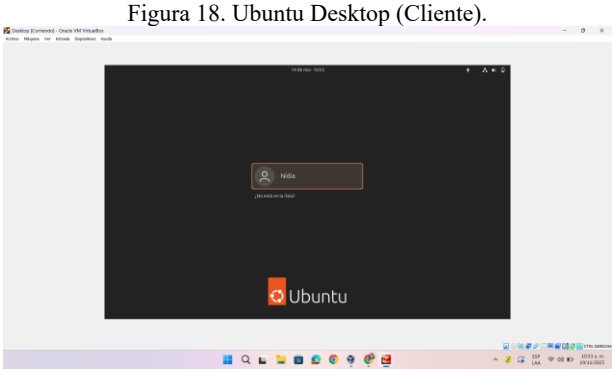
Figura 17. Configuración red naranja en Ubuntu Server.



Fuente: Autoría Propia

El cliente (Ubuntu Desktop) se conecta a través de Endian, lo que protege la red de amenazas externas e internas mediante herramientas de administración remota y control de tráfico (Nemeth et al., 2017). Esto facilita la gestión desde cualquier lugar y permite trabajar en un entorno seguro.

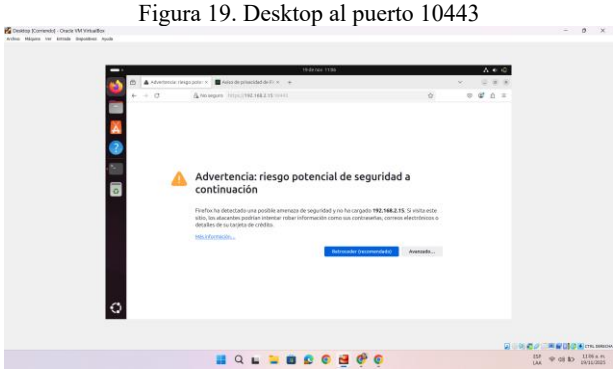
Figura 18. Ubuntu Desktop (Cliente).



Fuente: Autoría Propia

Para acceder a Endian, se ingresa mediante el puerto 192.168.2.15:10443, el cual utiliza un canal SSL alternativo para evitar conflictos con la configuración principal (Endian, s.f.).

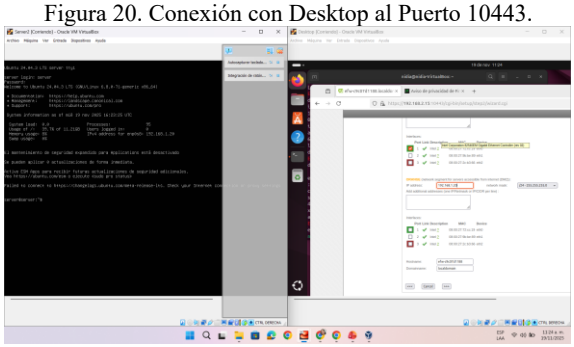
Figura 19. Desktop al puerto 10443



Fuente: Autoría Propia

Después de completar la configuración en Endian, se procede a verificar desde el Server la dirección IP asignada en la red Naranja y validar la MAC correspondiente en la zona Orange, garantizando la correcta asociación de las interfaces (Nemeth et al., 2017).

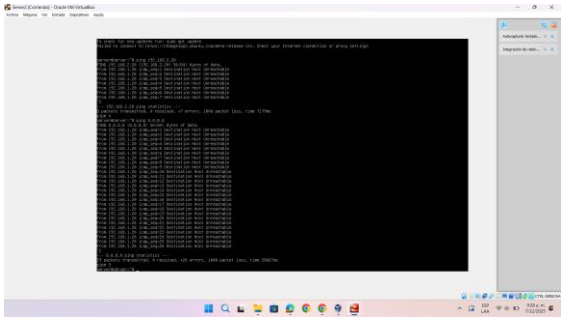
Figura 20. Conexión con Desktop al Puerto 10443.



Fuente: Autoría Propia

La comunicación ping permite verificar la conectividad entre el equipo local y un destino remoto, este evalúa si existe comunicación a nivel de red. En este caso el Desktop dentro de la red LAN puede comunicarse correctamente con el servidor público 8.8.8.8 el cual pertenece al servicio DNS de Google.

Figura 21. Ping de comunicación A Desktop y 8.8.8.8



Fuente: Autoría Propia

4 TEMÁTICA 3

4.1 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

DMZ (Demilitarezed Zone) es una zona intermedia diseñada para alojar servicios que deben ser accesibles desde el exterior, entre ellos los servidores web, DNS, FTP o correo. El sistema por defecto tiene esta zona aislada tanto de internet como la red interna con el fin de reducir los riesgos de seguridad. Permitir que la DMZ entregue servicios hacia LAN requiere reglas específicas que controlen este tráfico de manera estricta (López & García, 2022).

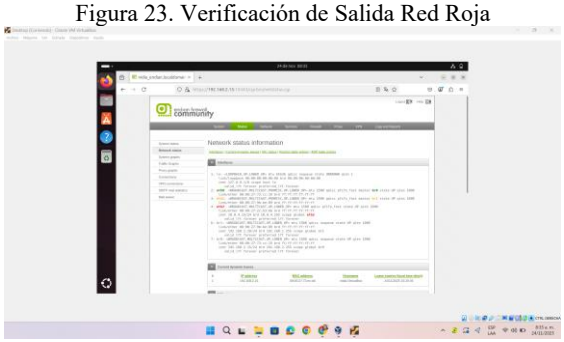
Para iniciar Sesión se utiliza la administración de Endian Firewall, ingresando a l interfaz web por el puerto 10443, desde allí se gestionan las políticas de reglas NAT, la configuración de la DMZ, proxy HTTP, VPN, monitoreo de tráfico y los servicios críticos del sistema. Según la documentación técnica del fabricante (Endian,2023)

Figura 22. Ingreso al Admin de Endian

Fuente: Autoría Propia

Al realizar la verificación de la red roja es esencial para confirmar la correcta conectividad del firewall, revisando el Status, según los parámetros asociados a cada interfaz. De acuerdo con Hernández y Castillo (2022), se presentan los detalles de la dirección, la máscara y la puerta de enlace, la presencia de la IP válida indica que Endian ha establecido comunicación con el proveedor de Internet (Pérez & Jimenez,2021)

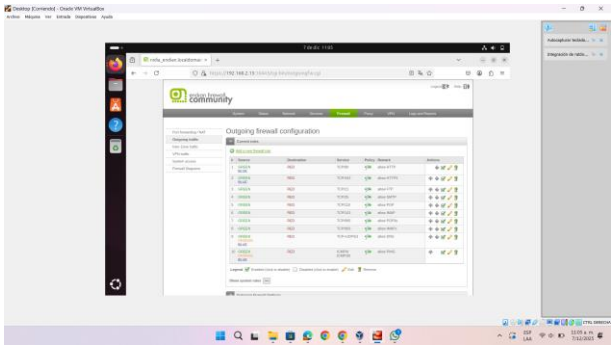
Figura 23. Verificación de Salida Red Roja



Fuente: Autoría Propia

La configuración de Outgoing firewall en Endian, hace la función de controlar todas las conexiones salientes desde las zonas internas hacia la red externa, Según Endian Tecnologies (2023) desde donde se instalan los servicios estrictamente necesarios para evitar las fugas de información o conexiones no autorizadas (Ramos & Ortega,2022).

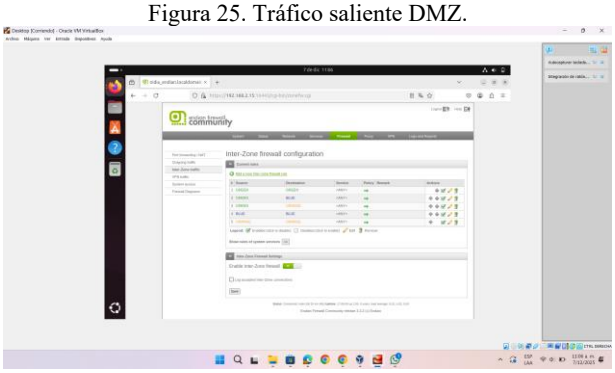
Figura 24. Identificacion Outgoing Firewall.



Fuente: Autoría Propia.

Se realiza la configuración del tráfico saliente lo cual consiste en permitir que la red Verde acceda a Internet por puertos estándar como 80 y 443 donde la red DMZ.

Figura 25. Tráfico saliente DMZ.



Fuente: Autoría Propia

Se realiza el pin a la red verde y la conexion 8.8.8.8 de g

Figura 26. Ping de Acceso a la red.

Fuente: Autoría Propia

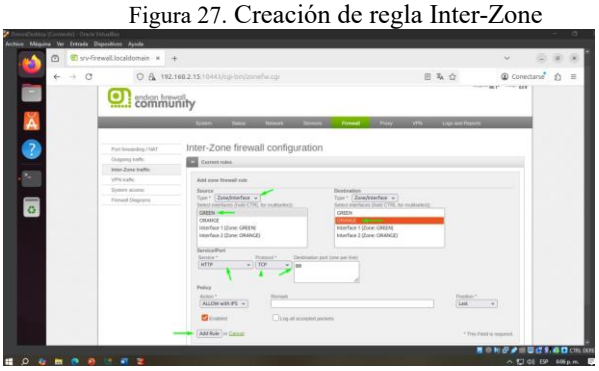
5. TEMÁTICA 4

5.1 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO.

Son directivas que controlan el tráfico de red que puede entrar o salir de un sistema o red. (Tanenbaum & Wetherall, 2011). Así mismo, se pueden implementar en dispositivos de red como firewalls, routers y sistemas operativos, usando herramientas como iptables para el caso de Linux o firewalls, integrados en soluciones de seguridad. (Nemeth et al.,2017).

Para comunicar la zona verde con la zona naranja mediante el protocolo HTTP y FTP se deben crear las siguientes reglas desde inter-zone indicando la salida en Green y destino Orange con servicio HTTP y puerto 80.(Endian, s.f.)

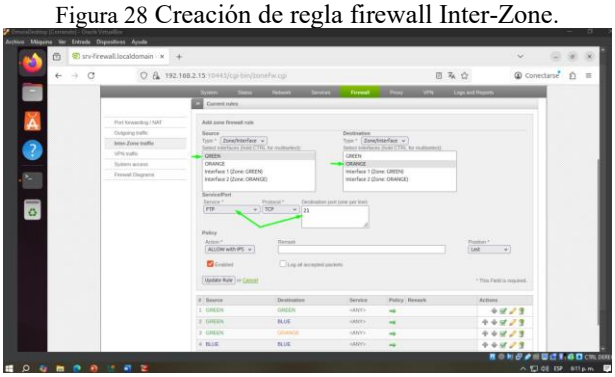
Figura 27. Creación de regla Inter-Zone



Fuente: Autoría Propia

Igualmente, para el FTP se cambia el servicio y se configura el puerto 21.

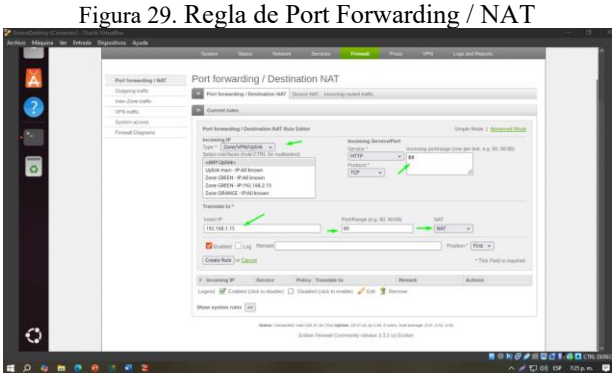
Figura 28 Creación de regla firewall Inter-Zone.



Fuente: Autoría Propia

Luego se requiere comunicar la zona de internet con la zona DMZ en la cual se crea una regla en Port Forwarding para redirigir el tráfico de internet como zona uplink (Intenert) en servicio HTTP puerto 80 con destino la ip del DMZ o zona naranja en el server configurado. (Cisco, s.f.; Nemeth et al.,2017).

Figura 29. Regla de Port Forwarding / NAT



Fuente: Autoría Propia

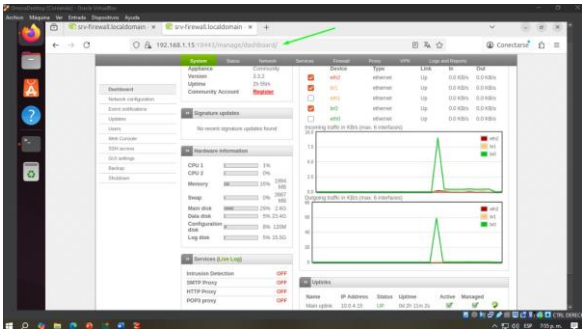
Para verificar el tráfico inter – zona y la creación de reglas, las podemos visualizar desde el panel de inter – zone en el menú de Firewall.(Endian, s.f.).

Figura 30. Trafico de Red

Fuente: Autoría Propia

Luego se verifica el servicio HTTP desde la LAN hacia la zona DMZ ingresando a la IP de la DMZ zona naranja, en el desktop o zona verde.

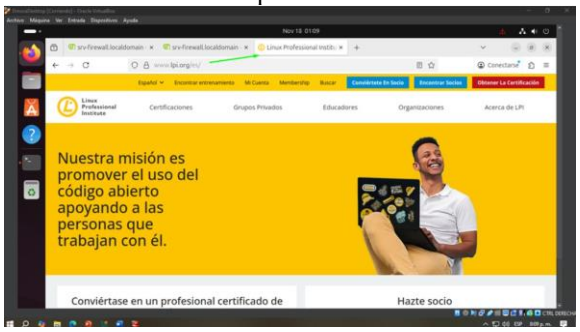
Figura 31. “Dashboard del servidor firewall



Fuente: Autoría Propia

Continuamos validando el servicio HTTP desde la LAN hacia la WAN ingresando la url de una página publica en el navegador de la zona verde en este caso el desktop, si la página carga, quiere decir que el tráfico funciona.. (Nemeth et al.,2017)

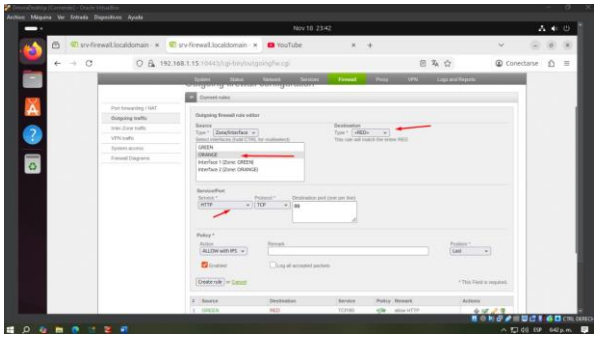
Figura 32. Prueba de navegación: tráfico permitido



Fuente: Autoría Propia

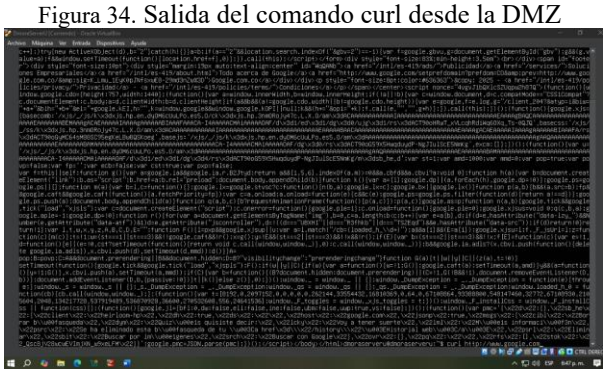
Para la configuración del servicio HTTP desde la zona DMZ hacia la WAN se crea la regla en outgoing traffic con zona naranja y destino RED y puerto 80, se valida agregando el comando curl y la dirección que se requiere en el DMZ del server.(Google,s.f.).

Figura 33. Regla de tráfico saliente desde la DMZ



Fuente: Autoría Propia

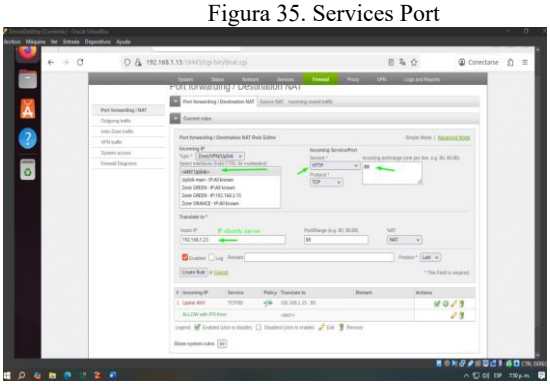
Figura 34. Salida del comando curl desde la DMZ



Fuente: Autoría Propia

Para el servicio HTTP desde la WAN hacia la zona DMZ se crea una regla Port Forwarding con salida ANY Uplink y destino la zona naranja asociando la ip de ubuntu server en el puerto 80. La verificacion se hace con el comando curl desde el servidos en la DMZ (Nemeth et al.,2017)

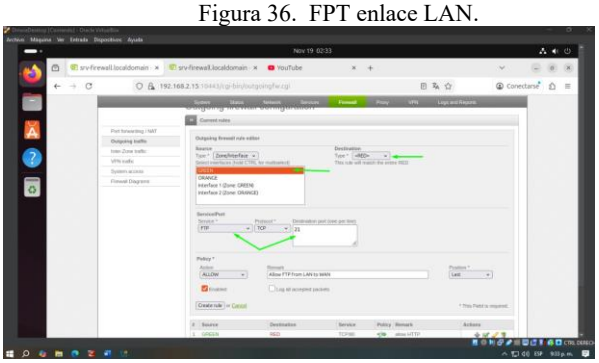
Figura 35. Services Port



Fuente: Autoría Propia

Para el servicio FTP desde LAN hacia la WAN , se crea regla de zone/interface Green y destino RED en servicio FTP y puerto 21. (IETF,s.f.).

Figura 36. FPT enlace LAN.



Fuente: Autoría Propia

Para el servicio FTP desde la WAN hacia la zona DMZ se crea regla en Port Forwarding con salida ANY Uplink y servicio FTP puerto 21 con destino a zona naranja la cual es la IP configurada en el server. (Nemeth et al.,2017)

Figura 37. Regla de Port Forwarding configurada para HTTP

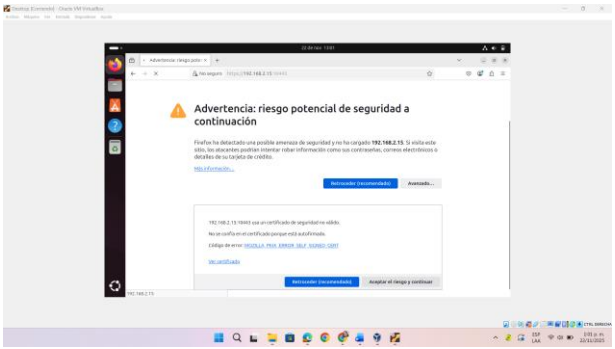
Fuente: Autoría Propia

6. TEMATICA 5

5.1 IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

La implementación de un proxy HTTP no transparente permite ejercer control detallado sobre quién accede a Internet y qué recursos puede utilizar, gracias a mecanismos de autenticación y políticas de acceso que refuerzan la seguridad de la red al bloquear tráfico no autorizado y mitigar riesgos externos, tal como lo señalan enfoques fundamentales de administración y seguridad de redes (Tanenbaum & Wetherall, 2011; Stallings, 2020).

Figura 38. Ingreso al puerto 10443 Proxy de Endian



Fuente: Autoría Propia

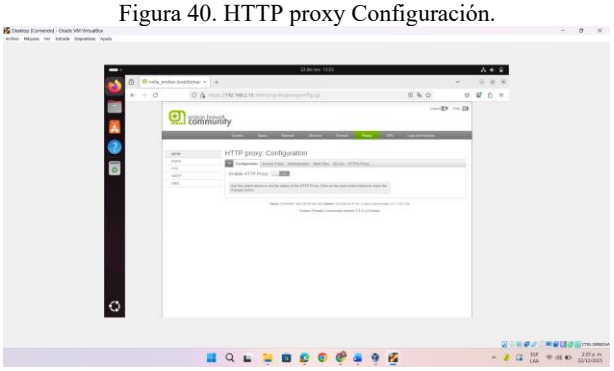
El uso de un proxy también posibilita almacenar en caché contenido web, reduciendo la carga del tráfico en la red y optimizando la velocidad de acceso, una práctica recomendada para mejorar el rendimiento en infraestructuras empresariales (Kurose & Ross, 2021). Desde Endian se pueden crear grupos de acceso específicos para cada área de una empresa, lo cual facilita la gestión eficiente de permisos y restricciones (Easttom, 2019). se aprecia el ingreso al puerto 10443, desde donde se administra el módulo de proxy.

Figura 39. Plataforma de Endian Firewall Proxy

Fuente: Autoría Propia

En el entorno del HTTP Proxy, se encuentran opciones como configuración general, acceso público, autenticación, filtrado web, unión a Active Directory y manejo de tráfico HTTPS, funciones diseñadas para aumentar la seguridad en la navegación corporativa (Williams, 2021).

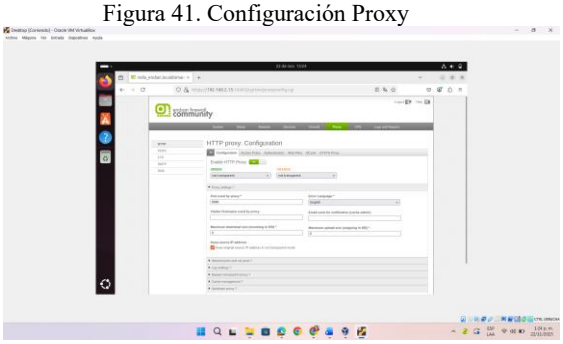
Figura 40. HTTP proxy Configuración.



Fuente: Autoría Propia

En la configuración estándar, el puerto verde se establece como no transparente, al igual que el puerto naranja, utilizando el puerto 8080 como canal de comunicación.

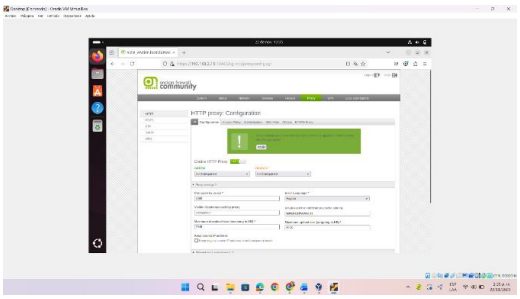
Figura 41. Configuración Proxy



Fuente: Autoría Propia

La activación de políticas como Web URL Filter permite aplicar criterios de control sobre los sitios visitados, fortaleciendo la protección frente a contenido malicioso o inapropiado, en concordancia con buenas prácticas de gestión de seguridad (Andress, 2019).

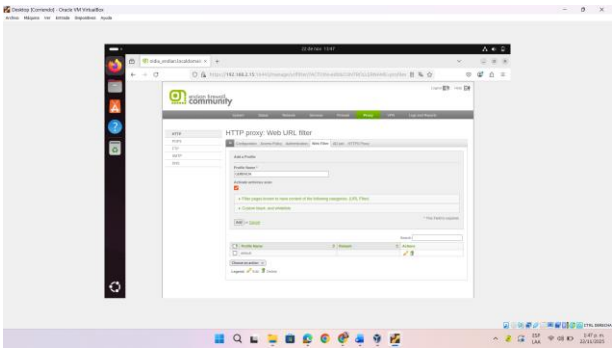
Figura 42. Activación de la configuración



Fuente: Autoría Propia

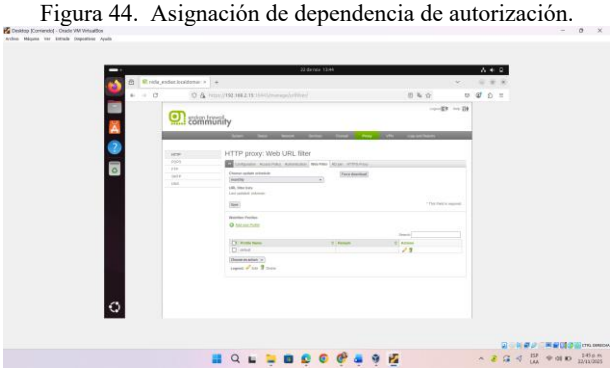
Asimismo, la asignación de autorizaciones y direcciones en listas negras permite cumplir con normativas de seguridad y evitar la propagación de programas malignos dentro de la red (Chapple & Seidl, 2021).

Figura 43. Activación de la Web URL Filter.



Fuente: Autoría Propia

Figura 44. Asignación de dependencia de autorización.



Fuente: Autoría Propia.

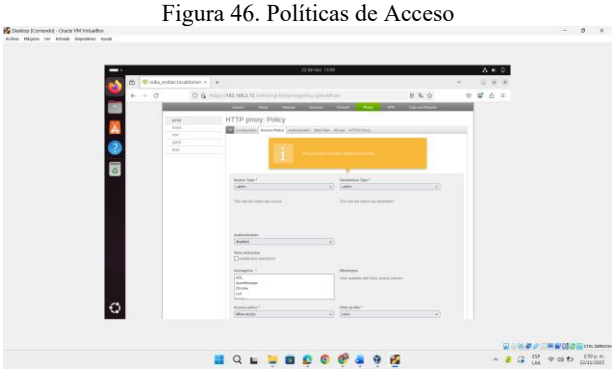
Se presenta la visualización de la lista blanca y lista negra, donde se especifican los dominios permitidos y aquellos restringidos para cada grupo. Este tipo de filtrado es considerado una de las medidas más efectivas para limitar la exposición de los usuarios a contenido no autorizado y reforzar las políticas corporativas, tal como afirman Scarfone y Hoffman (2009).

Figura 45. Asignación de Direcciones de Acceso Lista Negra.

Fuente: Autoría Propia

Ayuda a cumplir con las políticas de seguridad como las regulaciones de acceso, propagación de programa maligno. se observa la configuración de la dependencia o grupo que será autorizado, y en la Imagen 7 se confirma nuevamente la aplicación de la configuración realizada.

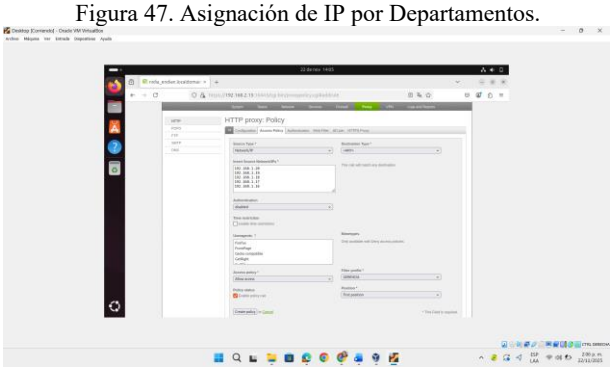
Figura 46. Políticas de Acceso



Fuente: Autoría Propia

Para las empresas resulta indispensable que cada departamento cuente con accesos diferenciados; mediante el proxy es posible gestionar estos permisos asignando direcciones IP autorizadas para determinadas URL, lo que garantiza un control segmentado y alineado con la estructura organizacional (Cole, 2022).

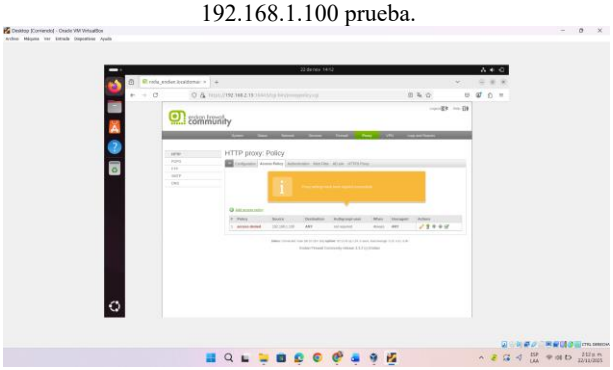
Figura 47. Asignación de IP por Departamentos.



Fuente: Autoría Propia

Finalmente, la aplicación de reglas de acceso personalizadas permite validar y restringir conexiones específicas, fortaleciendo la administración interna de los recursos web disponibles en la compañía (Peltier, 2016). haciendo un recurso de prueba, demostrándose cómo el sistema impide la conexión desde la política definida

Figura 48. Aplicación de reglas de acceso a la URL 192.168.1.100 prueba.



Fuente: Autoría Propia

6. CONCLUSIONES

La implementación de los servicios DHCP, DNS, FTP y SSH permitió evidenciar la importancia de una infraestructura de red correctamente configurada para garantizar un funcionamiento estable y seguro. DHCP automatiza la distribución de direcciones IP, optimizando la administración; DNS facilita la resolución de nombres, mejorando la accesibilidad a los recursos; FTP asegura la transferencia eficiente de archivos entre equipos; y SSH brinda un acceso remoto confiable para la gestión del servidor. En conjunto, estos servicios fortalecen el desempeño de la red, aumentan la productividad y permiten una administración centralizada y profesional del entorno GNU/Linux.

Se reconocen los elementos de la configuración de Endian con cada una de sus características, como una herramienta ágil y efectiva al momento de realizar la conexión entre el Servidor, Desktop y Endian. Así mismo, se realizó la respectiva conexión por la Red NAT y la Red DMZ identificando todas sus características y así poder ofrecer seguridad integral a las redes empresariales mediante la segmentación y control de las redes.

Se atienden de manera acertada las configuraciones que permiten que el proxy HTTP funcione como un mecanismo integral de control y seguridad, generando una seguridad en la eficiencia del tráfico y el cumplimiento de las políticas internas de una organización T desde una perspectiva amplia se llevó a cabo este articulo implementando de manera acertada el manejo de Endian como sistema de seguridad integral para cualquier empresa, y como profesionales en Ingeniería, poder ofrecer una asesoría en servicios de redes a través de máquinas virtuales.

7. REFERENCIAS

[1] Andrés, J. (2019). Cybersecurity: The Beginner's Guide. Pearson.

[2] Cisco. (s.f.). NAT: Network Address Translation. Cisco Documentation. https://www.cisco.com/c/en/us/tech/ip/nat/index.html

[3] Cisco Systems, Introduction to Proxy Services and Network Access Control, 2023.

[4] Endian. (s.f.). Endian Firewall 3.2 documentation. Endian Docs. https://docs.endian.com/3.2/

[5]Google. (s.f.). Public DNS documentation. https://developers.google.com/speed/public-dns

[6] Chapple, M., & Seidl, J. (2021). CompTIA Security+ Guide to Network Security Fundamentals. Cengage Learning.

[7] Cole, E. (2022). Network Security Bible. Wiley.

[8] Endian, HTTP Proxy Configuration Guide, Endian UTM 5.1 Documentation, 2024.

[9] Fortinet, Advanced Proxy Deployment and Authentication Policies, 2023.

[10] Endian, “HTTPS Proxy and URL Filtering Configuration,” Endian Knowledge Base, 2024.

Easttom, C. (2019). Network Defense and Countermeasures. Pearson.

[11] Kurose, J., & Ross, K. (2021). Computer Networking: A Top-Down Approach. Pearson.

[12] Nemeth, E., Snyder, G., Hein, T., Whaley, B., & Mackin, D. (2017). UNIX and Linux system administration handbook (5th ed.). Pearson.

[13]Oracle. (s.f.). VirtualBox User Manual. Oracle Documentation. https://www.virtualbox.org/manual/

[14] Palo Alto Networks, Enterprise Web Access Control and ecure Browsing, 2024.

[15] Peltier, T. (2016). Information Security Policies, Procedures, and Standards. Auerbach Publications.

[16] Stallings, W. (2020). Network Security Essentials. Pearson.

[17] Squid Cache, “Squid: Optimising Web Delivery,” 2024. Disponible en: https://www.squid-cache.org

[18] Sophos, Web Filtering and Policy Enforcement in Corporate Networks, 2024.

[19] Tanenbaum, A., & Wetherall, D. (2011). Computer Networks. Prentice Hall.

[20] Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer networks (5th ed.). Pearson.

[21] Williams, R. (2021). Practical Network Automation. Packt Publishing.