Integración de Firewalls en Sistemas GNU/Linux para la Gestión Segura de las redes

Jossea Germain Pérez Castro
e-mail: josuarestro@gmail.com
Hadder Enrique Saenz Rhenals
e-mail: haddersaenz@gmail.com
Andrés Ríos Orozco
e-mail: anrioco23@gmail.com
Duvian Andres Arango Sequeda
e-mail: arangosequeda123@gmail.com
Ian David Ramírez Moreno
e-mail: ianramirez084@gmail.com

RESUMEN: *El presente trabajo se enfoca en la implementación de medidas de seguridad orientadas a entornos GNU/Linux, con el propósito de fortalecer la protección de servidores y redes internas. Por tal motivo, se abordan aspectos fundamentales como la gestión de reglas de firewall, la segmentación de redes y la configuración de servicios esenciales en entornos seguros. De igual manera, durante el desarrollo de la actividad, se exploran estrategias de filtrado de tráfico, la implementación de NAT para asegurar la comunicación entre redes, y la restricción de accesos a nivel de protocolos y puertos, con el objetivo de reducir las vulnerabilidades. Además, se lleva a cabo la configuración de un proxy HTTP con autenticación de usuario, promoviendo así un entorno controlado en cuanto al acceso a la red.*

PALABRAS CLAVE: Filtrado de tráfico, firewall, reglas de acceso, seguridad perimetral

1 INTRODUCCIÓN

La seguridad perimetral es un componente esencial en el diseño de infraestructuras de red modernas. La segmentación de tráfico, el filtrado de paquetes y la administración de accesos entre zonas de red representan pilares clave para proteger recursos críticos. Las soluciones libres basadas en GNU/Linux, como Endian Firewall Community (EFW), ofrecen funcionalidades integradas que permiten implementar este tipo de esquemas con eficiencia y flexibilidad.

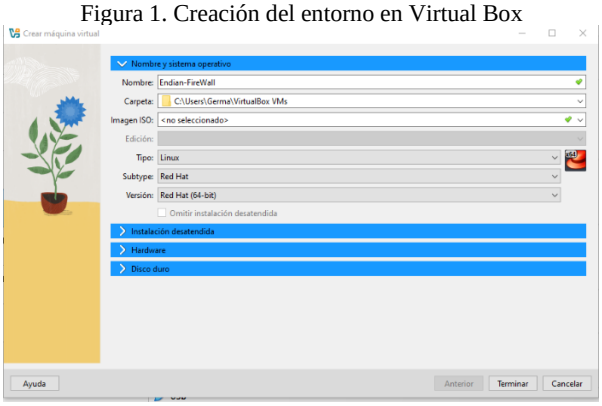
El presente artículo describe la construcción de un entorno virtualizado orientado a la seguridad perimetral, utilizando EFW como plataforma principal. Se desarrollaron cinco componentes técnicos interdependientes: la instalación y configuración de EFW con zonas LAN (verde), WAN (roja) y DMZ (naranja); la creación de reglas NAT; la habilitación y restricción de servicios desde la DMZ; la definición de políticas de acceso entre zonas; y la configuración de un proxy HTTP con autenticación. El documento detalla los procedimientos, configuraciones y resultados asociados a cada una de estas temáticas, con el objetivo de documentar una solución replicable en entornos GNU/Linux.

2 INSTALACIÓN Y CONFIGURACIÓN DE ENDIAN

Endian Firewall es una distribución GNU/LINUX creada con el propósito de ser una solución integral de seguridad en redes, contribuyendo con características avanzadas sobre firewall, tales como, filtrado de tráfico y administración de servicios. Otro aspecto importante para resaltar es acerca de su arquitectura, cuyo código es abierto, facilitando así, que la comunidad pueda contribuir en el avance y mejoramiento de infraestructuras empresariales y educativas, por medio de implementación de reglas de seguridad. En cuanto a sus características más reconocidas se encuentran, el uso de VPNs, configuración de proxy, herramientas de antivirus y antispam. Esta descripción la corrobora Iñaguazo Velepucha (2022) donde señala que “Endian incluye funcionalidades para configurar NAT, tráfico saliente, entre zonas, tráfico VPN y diagramas de Firewall; imágenes que muestran el tipo de tráfico interceptado” (p. 34). [4]

A continuación, se explica el proceso de instalación de Endian Firewall, usando VirtualBox como ambiente virtualizado de máquinas. Como primer paso, se debe crear el entorno de Endian en VirtualBox para, posteriormente, instalar la ISO del firewall, evitando así posibles errores durante la instalación. Es necesario especificar el tipo de sistema operativo, que en este caso es Linux, y en el subtipo, seleccionar Red Hat.

Figura 1. Creación del entorno en Virtual Box



Fuente: Autoría Propia

Se instala la ISO y se reinicia el entorno, este ya estará listo para proceder con la instalación de Endian Firewall. A continuación, se mostrarán una serie de pasos a seguir para que la instalación sea correcta.

Figura 2. Se elige utilizr todo el disco duro

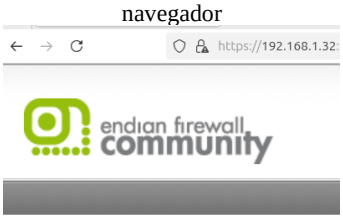
Fuente: Autoría Propia

Figura 3. especificar la IP a asignar en la “Green Zone”

Fuente: Autoría Propia

Se procede a configurar las tarjetas de red de Endian Firewall en el siguiente orden: Adaptador 1 – Red interna “Zona verde”, Adaptador 2 – Red interna “Zona Naranja” y Adapatador 3 – NAT. En cuanto al sistema operativo que se usará como escritorio, se debe configurar el Adaptador 1 como Red internat “Zona Verde” y el server como Adapatador 1 – Red interna “Zona Naranja”. Una vez configurado las tarjetas de red, se procede a configurar Endian FireWall desde el entorno gráfico en la “Zona Verde”

Figura 4. se accede con la IP “Zona Verde” desde un navegador

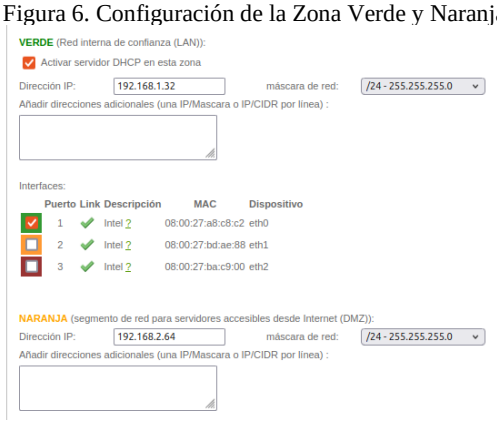


Fuente: Autoría Propia

Figura 5. Configuración de Endian Firewall

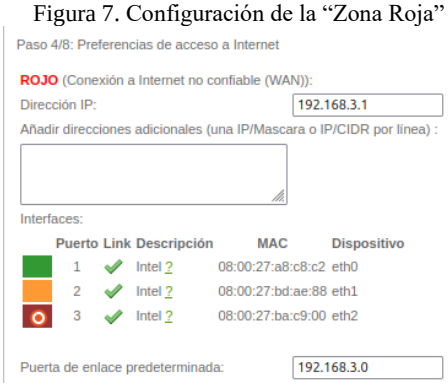
Fuente: Autoría Propia

Figura 6. Configuración de la Zona Verde y Naranja



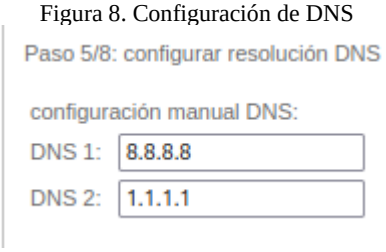
Fuente: Autoría Propia

Figura 7. Configuración de la “Zona Roja”



Fuente Autoría Propia

Figura 8. Configuración de DNS



Fuente Propia

Una vez se lleven a cabo los pasos anteriores, Endian ya quedará configurado.

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

La configuración inicial de un sistema de seguridad perimetral requiere la instalación y puesta en marcha de un firewall capaz de segmentar el tráfico en múltiples zonas de red. Endian Firewall Community (EFW), una distribución basada en GNU/Linux, permite gestionar estas zonas desde una interfaz gráfica accesible vía navegador, además de ofrecer herramientas robustas para control de tráfico, NAT, proxy y filtrado de paquetes [3].

Para esta implementación se utilizó Oracle VirtualBox, que facilita la simulación de entornos de red complejos mediante la creación de adaptadores virtuales [8]. Se creó una máquina virtual con tres interfaces de red, distribuidas así:

- eth0: Zona roja (WAN), conectada al adaptador puente.
- eth1: Zona verde (LAN), configurada como red interna.
- eth2: Zona naranja (DMZ), también configurada como red interna en un segmento distinto.

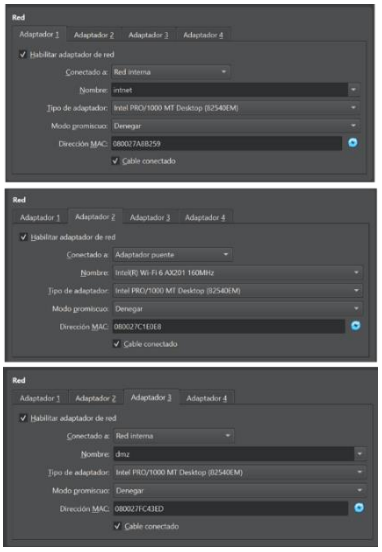
Durante la instalación, se montó la imagen ISO de Endian (v3.3.2), y se definieron los parámetros básicos: idioma, zona horaria, contraseña de administración, y asignación de IPs estáticas. La zona verde fue configurada con la dirección 192.168.10.1/27, la roja con 192.168.1.2/24 y la naranja con 192.168.20.65/27. Las direcciones fueron definidas de acuerdo con las buenas prácticas de segmentación de red para garantizar aislamiento y control entre zonas [6].

Tras finalizar la instalación, se accedió a la interfaz de administración web desde la IP de la zona verde. Desde allí se validaron los estados de las interfaces, la asignación de roles por zona y la conectividad de cada segmento. Este paso resultó fundamental para habilitar posteriormente las reglas de seguridad, NAT y servicios controlados en las zonas WAN y DMZ.

Además de la verificación por consola, se accedió al panel de administración web desde la IP de la zona verde: https://192.168.10.1:10443. Desde este entorno gráfico, se confirmaron los dispositivos de red activos y su asignación a las zonas correspondientes

Esta validación visual permite corroborar el estado operativo de cada interfaz, el tráfico por zona y la base sobre la cual se aplicarán las reglas de seguridad en las temáticas siguientes.

Figura 9. Configuración de adaptadores de red para Endian en VirtualBox

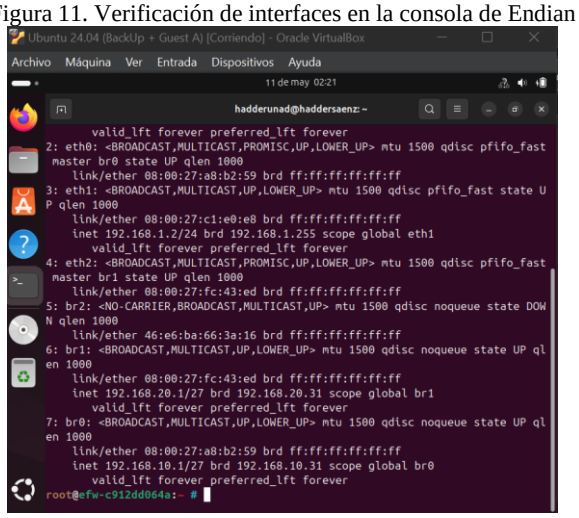


Fuente Autoría Propia

Figura 10. Interfaz web de Endian con zonas de red configuradas

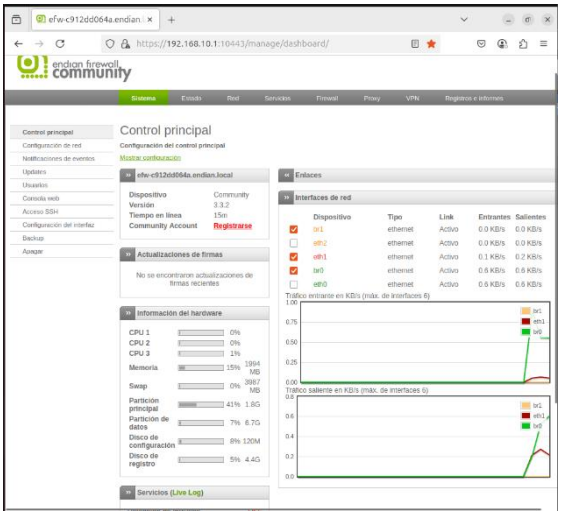
Fuente Autoría Propia

Figura 11. Verificación de interfaces en la consola de Endian



Fuente Autoría Propia

Figura 12. Interfaz de administración de Endian con resumen de interfaces activas



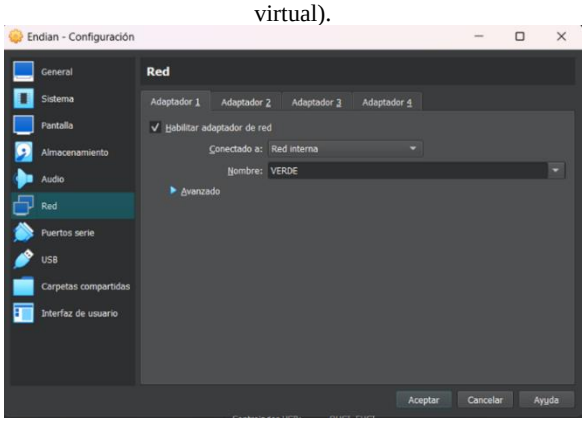
Fuente Autoría Propia

4 TEMÁTICA 2: Configuración NAT

En el contexto la administración y la seguridad de redes, la traducción de direcciones de red NAT, o Network Address Translation, se destaca como una de las herramientas más utilizadas para facilitar la conectividad entre redes privadas y públicas, al mismo tiempo que otorga una capa básica de seguridad. NAT permite que múltiples dispositivos dentro de una red local (LAN) compartan una única dirección IP pública al acceder a recursos externos, optimizando el uso del espacio de direcciones IPv4 y ocultando la topología interna de la red [5].

En la práctica, se configuraron reglas NAT utilizando el software Endian Firewall, virtualizando tres máquinas para representar las zonas WAN, LAN y DMZ. Esta infraestructura permitió simular un entorno real, logrando establecer correctamente la comunicación entre las zonas mediante NAT y reenvío de puertos, garantizando tanto el acceso a servicios desde Internet como la salida segura desde la red interna.

Figura 13: Configuración adaptador red Endian (Maquina virtual).

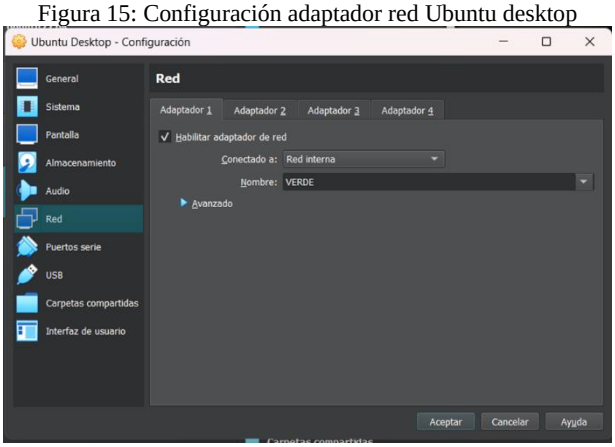


Fuente: Autoría propia

Figura 14: Configuración adaptador red Ubuntu Server

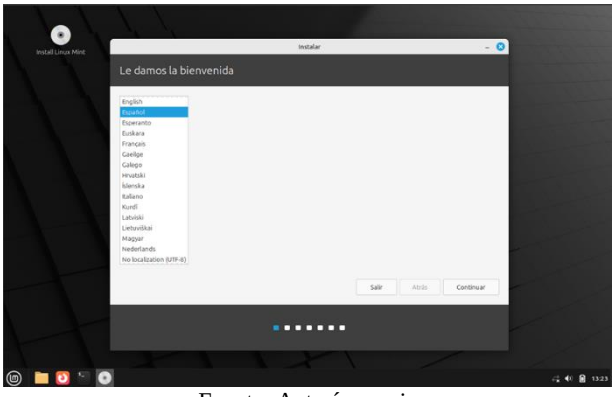
Fuente: Autoría propia

Figura 15: Configuración adaptador red Ubuntu desktop

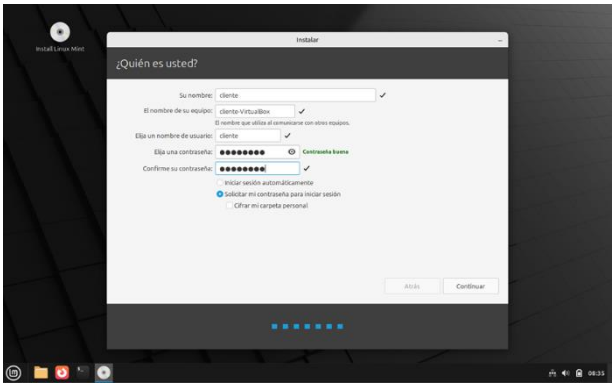


Fuente: Autoría propia

Una vez configuradas las redes de los diferentes dispositivos, se procede a configurar a instalar y configurar el linux mint, en el ubuntu de escritorio.

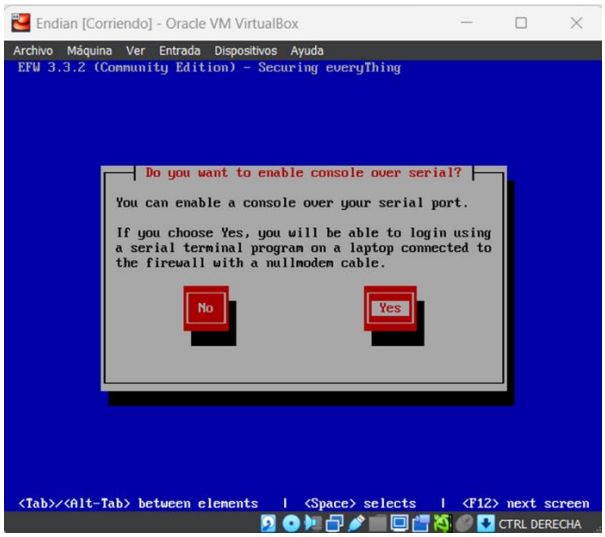


Fuente: Autoría propia



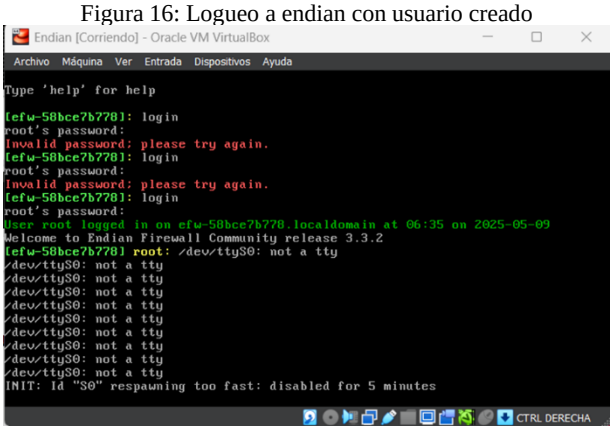
Fuente: Autoría propia

Mientras termina la instalacion del linux mint, se procede a intalar endian, y configurar la ip de la zona verde en el proceso de instalación, esto se hace para poder dar comunicacion en la zona de internet roja (DZM), y que no haya problemas para manipular el endian en la ip 192.168.2.15



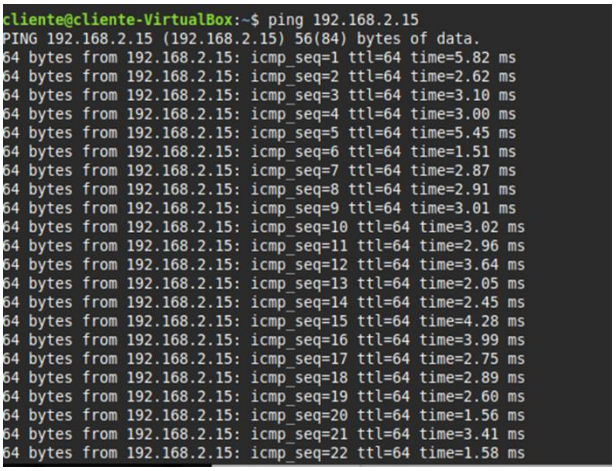
Fuente: Autoría propia

Figura 16: Logueo a endian con usuario creado



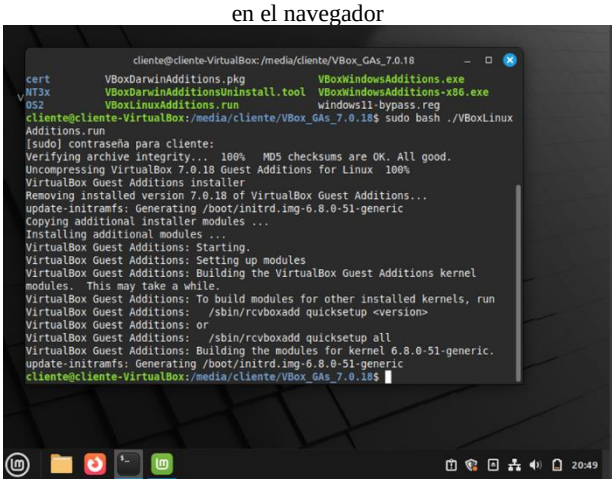
Fuente: Autoría Propia

Una vez finalizadas las instalaciones, se procede a realizar ping a la ip 192.168.2.15, esto con la finalidad de comprobar que si tenemos internet, gracias a las configuraciones del endian.



Fuente: Autoría propia

Figura 17: Se ejecura el "VBox" para poder acceder al endian en el navegador



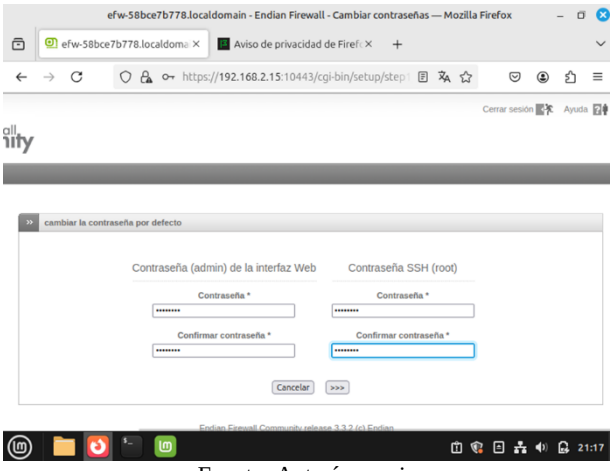
Fuente: Autoría propia

Figura 18: Se ingresa la ip 192.168.2.15:10443 para poder acceder al endian, es importante tener presente que debemos de acceder en la opcion de avanzado para continuar el proceso de instalación

Fuente: Autoría propia

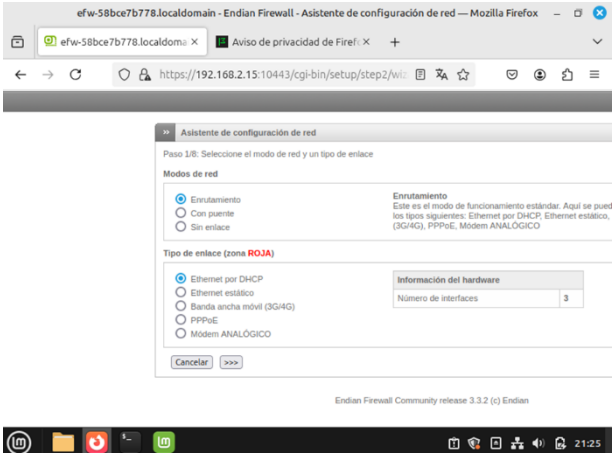
Figura 19: Instalación del endian y creación de cuenta

Fuente: Autoría propia

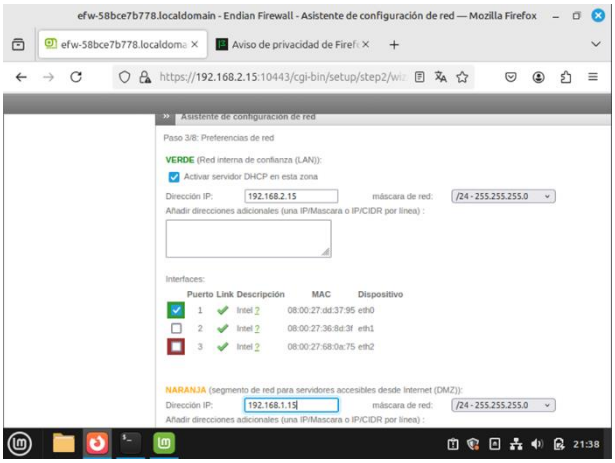


Fuente: Autoría propia

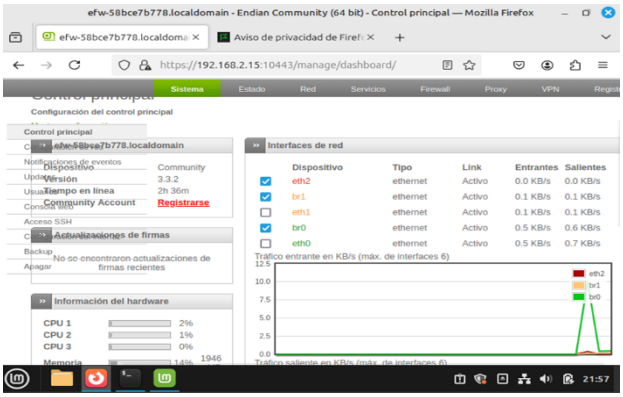
Figura 20: configuración hacia la zona naranja para la comunicación de la misma y manipulación de reglas desde el firewall



Fuente: Autoría propia



Fuente: Autoría propia



Fuente: Autoría propia

5 TEMÁTICA 3: Permitir servicios de la Zona DMZ para la red

La DMZ (zona desmilitarizada) es una red perimetral que protege la LAN (local-area-network) del tráfico no confiable, esta DMZ también es conocida como la zona naranja y se encuentra entre la internet publica y las redes privadas, agregando una capa adicional de seguridad para proteger los datos de las redes internas, utilizando firewall que permiten filtrar el tráfico.

El objetivo de DMZ, es permitir a una organización acceder a las redes no confiables, como lo es la internet y a su vez, garantizar la seguridad de la red privada o LAN. En la DMZ normalmente se almacenan los servicios y recursos externos como el DNS (Domain Name System), FTP (File Transference Protocol), correo, proxy, VoIP (Voice over Internet Protocol) y los servidores web [2]

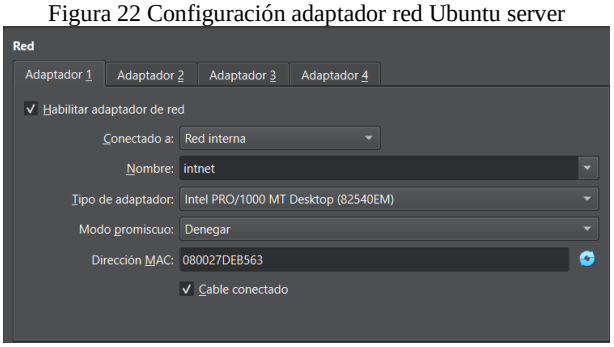
Durante el trabajo, se realizó uso del software de Endian firewall, sobre el cual se realiza la configuración para permitir los servicios DMZ a la red interna. En este proceso de configuración, debemos de ajustar los adaptadores red de las MV (Máquina Virtual) de acuerdo con los valores asignados en el adaptador de Endian (fig. 9, p.4).

Configuración de las MV para la red interna o LAN que se van a encontrar en la zona verde.

Figura 21 Configuración adaptador red Ubuntu server.

Fuente: Autoría Propia

Figura 22 Configuración adaptador red Ubuntu server



Fuente: Autoría Propia

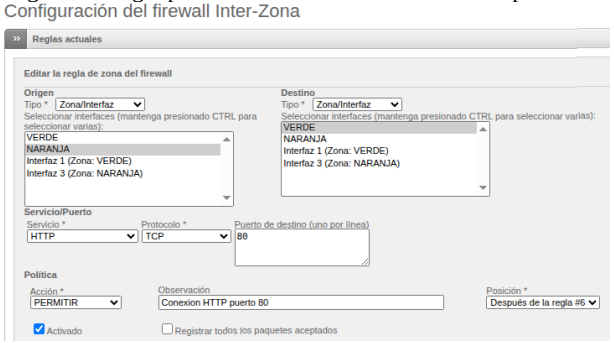
Configuración MV para la DMZ, la cual se encuentra en la zona naranja.

Figura 23 Configuración adaptador red Debian

Fuente: Autoría Propia

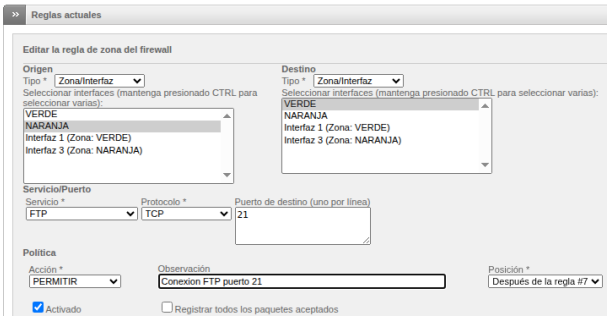
Realizada la configuración de los adaptadores de red, iniciamos las MV e ingresamos desde el Ubuntu desktop al apartado de administración de Endian firewall para permitir los servicios de HTTP (puerto 80) y FTP (puerto 21), para ello ingresamos al apartado de firewall > Tráfico entre zonas > nueva regla y se crea la regla para permitir la comunicación HTTP y FTP

Figura 24 Regla para funcionamiento servico HTTP puerto 80



Fuente: Autoría Propia

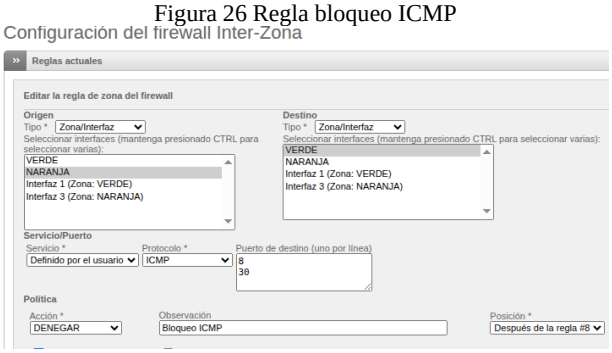
Figura 25 Regla para funcionamiento servico HTTP puerto 80



Fuente: Autoría Propia

Desde el mismo apartado de firewall > Tráfico entre zonas > nueva regla, procederemos a bloquear el protocolo de mensajes de Interter ICMP (es comúnmente utilizado por el comando ping).

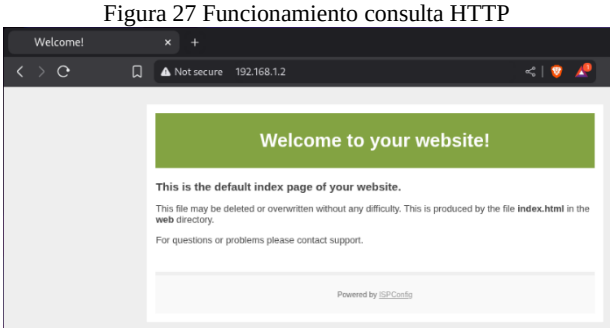
Figura 26 Regla bloqueo ICMP



Fuente: Autoría Propia

Teniendo encendida la MV de Ubuntu server (dentro de la zona verde) y la MV de Debian (en la zona naranja), procedemos a realizar las pruebas de la configuración realizada en Endian firewall. Desde el navegador web de Debian, apuntamos a la IP de Ubuntu server y agreamos el http:// dejando la ruta completa de http://192.168.1.2 el cual por defecto se encuentra funcionando por el puerto 80.

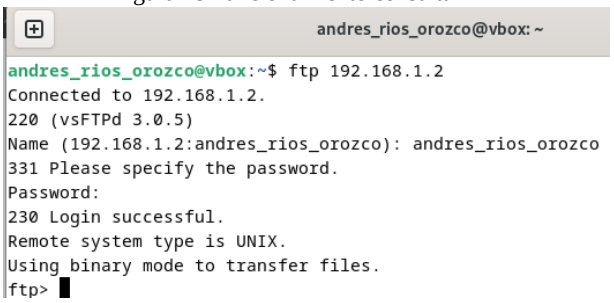
Figura 27 Funcionamiento consulta HTTP



Fuente: Autoría Propia

Para la prueba de ftp, se realiza desde una terminal y apuntamos a la misma dirección IP y accedemos con los datos de la maquina destino (en este caso es Ubuntu server)

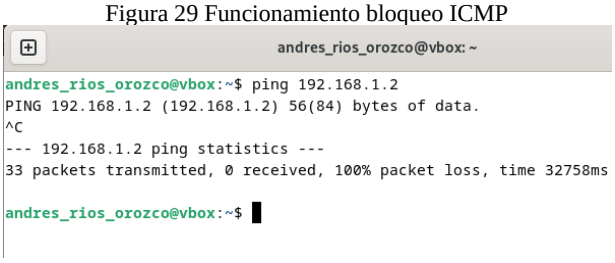
Figura 28 Funcionamiento consulta FTP



Fuente: Autoría Propia

Por último realizamos la validación del protocolo ICMP, para esto desde la terminal de Debian, ejecutamos el comando ping y apuntamos a la IP del Ubuntu server, en este caso no nos dara respuesta debido al bloquedo realizado en el Endian firewall

Figura 29 Funcionamiento bloqueo ICMP



Fuente: Autoría Propia

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

En el panorama de administración de redes y servidores GNU/LINUX, se vuelve esencial el manejo del tráfico de redes, debido a que es un aspecto clave para garantizar la seguridad y eficiencia de los diferentes entornos. Quiñones (2012) señala que “Mediante el análisis del tráfico, es posible descubrir cuellos de botella, medir la utilización del ancho de banda y generar gráficos de flujo de datos para optimizar el rendimiento de la red" **(**p.49) [9] haciendo énfasis en la importancia del tráfico de red como responsable de mejorar el rendimiento del servidor. De igual manera, León (2022) resalta que “La clasificación del tráfico es clave para la seguridad de la red, ya que facilita la detección de anomalías y la protección de recursos” (p.17). [7]

Teniendo en cuenta lo anterior, el desarrollo de la temática 4: Reglas de acceso para permitir o denegar el tráfico, tiene como objetivo la configuración de políticas que permitan o restrinjan la comunicación entre zonas de red, donde se garantiza el acceso a servicios relevantes y se reduce los riesgos de vulnerabilidades. En este contexto, se plantean diversos puntos a desarrollar, tales como la interconexión de la zona verde (LAN) con la zona naranja (DMZ) mediante protocolos específicos como HTTP y FTP, así como la regulación del tráfico entre la DMZ y la red externa (Internet). Además, se realizan pruebas para verificar la correcta implementación de las reglas de acceso, teniendo en cuenta una navegación controlada y restricciones en la comunicación entre servidores.

Esta temática también permite enfocarse en el diseño de una infraestructura segura y eficiente, en la cual las conexiones están definidas por distintos filtros de seguridad y niveles de accesibilidad. Es importante tener en cuenta que la configuración de estos filtros debe estar correctamente establecida para evitar posibles filtraciones de seguridad.

Con lo anteriormente mencionado, se procede a describir el desarrollo de la temática 4, a cargo del estudiante Jossea Germain Pérez Castro. Es importante mencionar, que los sistemas operativos utilizados fueron: Ubuntu Server para la zona Naranja, Ubuntu Desktop para la zona Verde y Endian Firewall para la zona Roja. En cuanto a los adaptadores de red y direcciones IP, la zona Verde utilizó el rango de IP 192.168.1.0/24, con la IP asignada 192.168.1.33. Por su parte, la zona Naranja empleó el rango 192.168.2.0/24, con la IP 192.168.2.65. Finalmente, la zona Roja trabajó con el rango 192.168.3.0/24 y se le asignó la IP 192.168.3.1. Todas las zonas usaron la máscara de red 255.255.255.0. Tanto la zona Verde como la zona Naranja fueron configuradas como redes internas, mientras que la zona Roja se configuró como red NAT y red interna.

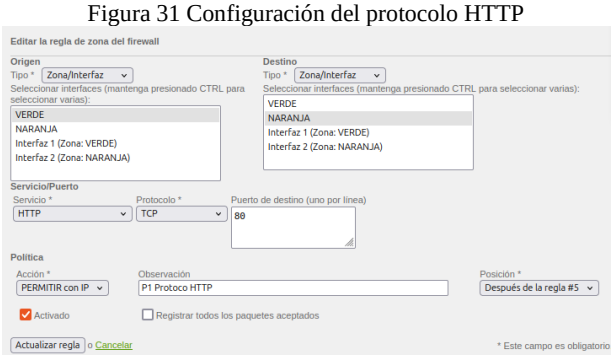
Una vez configurada las maquinas con los pasos anteriormente descritos, se accede a la interfaz de Endian FireWall a través de Ubuntu Desktop y haciendo uso de la IP de la zona verde. Una vez allí, se debe seleccionar la pestaña “Firewall” y el submenú “Tráfico entre zonas”

Figura 30 Seleccionar menú “Firewall” y submenú “Tráfico entre zonas”

Fuente: Autoría Propia

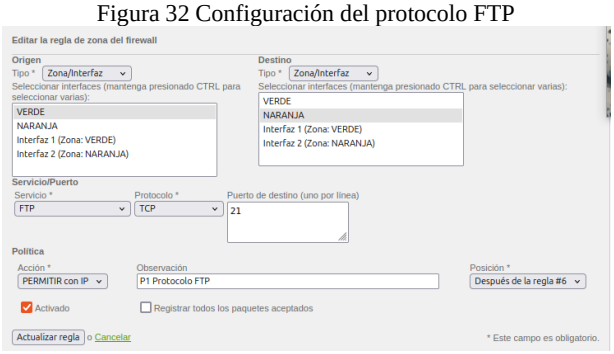
Se debe crear una nueva regla de firewall entre zonas para realizar la conexión entre la zona Verde y Naranja en los servicios FTP y HTTP.

Figura 31 Configuración del protocolo HTTP



Fuente: Autoría Propia

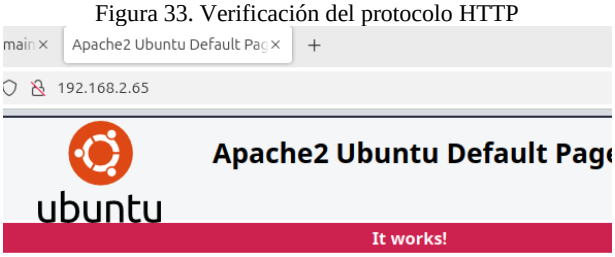
Figura 32 Configuración del protocolo FTP



Fuente: Autoría Propia

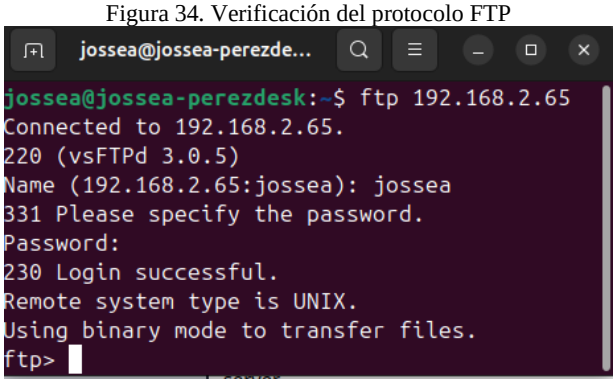
Cuando se configuran ambos protocolos, FTP y HTTP, es necesario verificar su correcto funcionamiento. Para el protocolo HTTP, se comprueba accediendo a la Zona Verde a través del navegador, utilizando la IP asignada al servidor. Previamente, debe instalarse el servicio Apache2 en el servidor para llevar a cabo esta prueba. En cuanto a la verificación del protocolo FTP, esta debe realizarse por medio de una conexión desde la terminal de la Zona Verde hacia la Zona Naranja, utilizando la IP del servidor.

Figura 33. Verificación del protocolo HTTP



Fuente: Autoría Propia

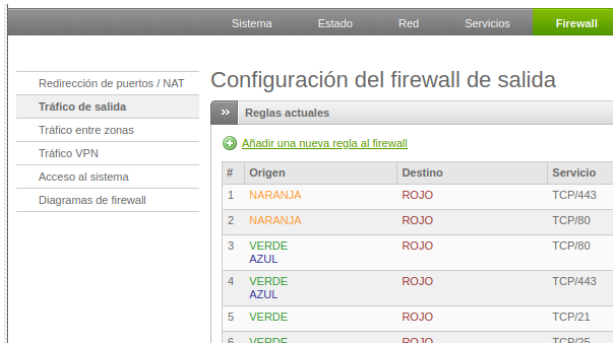
Figura 34. Verificación del protocolo FTP



Fuente: Autoría Propia

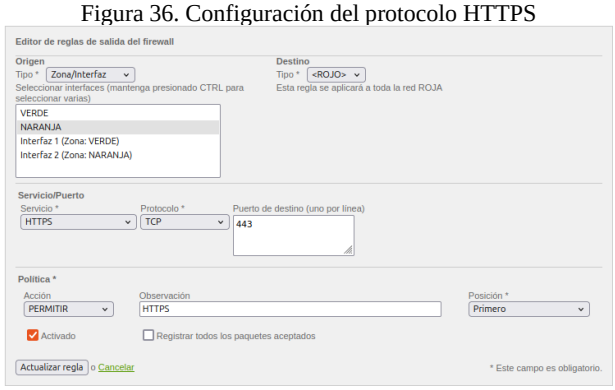
A continuación, se describe el proceso para comunicar la zona internet con la zona DMZ, con el objetivo de brindarle internet al servidor. En la misma pestaña Firewall , se accede al submenú Tráfico de salida. Allí, se añade una nueva regla al firewall, en la que se va a tener en cuenta los protocolos HTTP, HTTPS, PING y DNS. Pues estos protocolos son necesarios para comunicar la zona internet a la zona DMZ

Figura 35. Acceder al menú firewall y al submenú Tráfico de salida



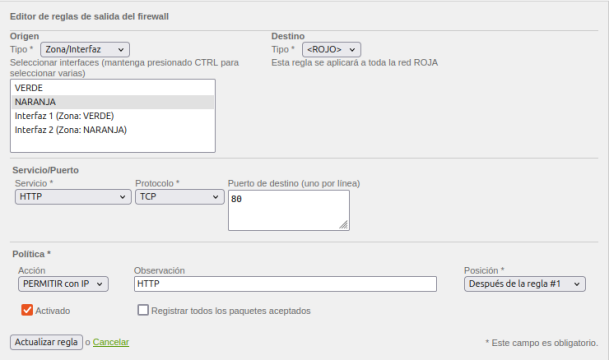
Fuente: Autoría Propia

Figura 36. Configuración del protocolo HTTPS



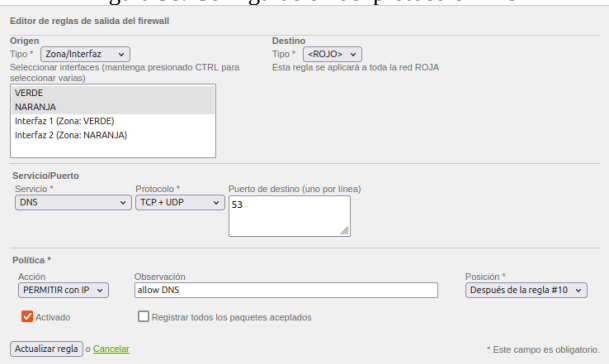
Fuente: Autoría Propia

Figura 37. Configuración del protocolo HTTP



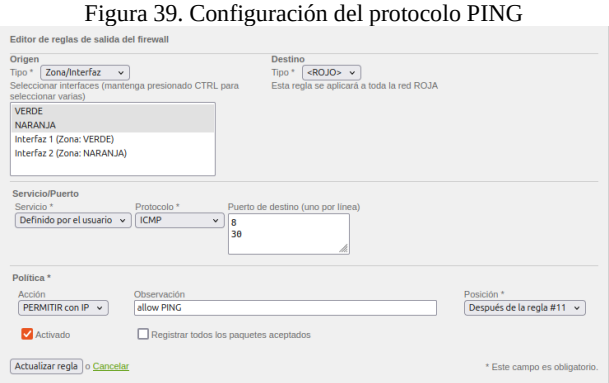
Fuente: Autoría Propia

Figura 38. Configuración del protocolo DNS



Fuente: Autoría Propia

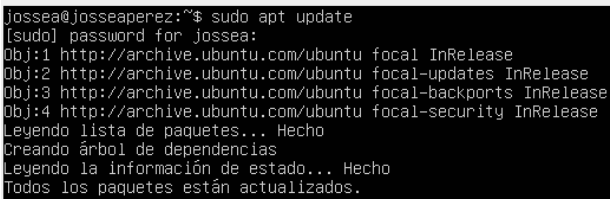
Figura 39. Configuración del protocolo PING



Fuente: Autoría Propia

Para comprobar que se configuró correctamente el tráfico de salida hacía la zona DMZ, se realiza una update en el servidor con el comando: sudo apt update. El servidor debe conectarse al servidor de Ubuntu para bajar las librerías y actualizar el sistema.

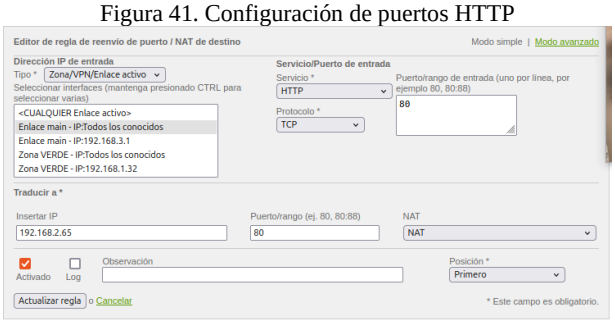
Figura 40. Verificación del acceso de internet a la zona DMZ



Fuente: Autoría Propia

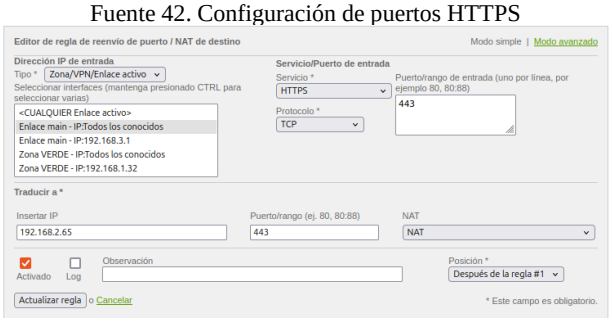
Se debe comprobar la conexión WAN, es decir la zona roja que tenga acceso a internet y pueda redirigir paginas hacía el servidor, comprobando de esta manera el ingreso HTTP a la zona DMZ. En la pestaña firewall, se seleccione el submenú redirección de puertos / NAT, con el propósito de configurar la redirección de puertos de la zona WAN hacía la zona DMZ.

Figura 41. Configuración de puertos HTTP



Fuente: Autoría Propia

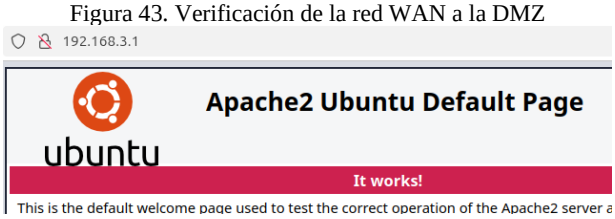
Fuente 42. Configuración de puertos HTTPS



Fuente: Autoría Propia

Al momento de comprobar la conexión WAN hacía el servidor DMZ, se debe tener en cuenta que se accede por medio de la IP de la zona Roja. Si la zona roja tiene acceso a internet, debe redirigir a la página de ejemplo de apache2 que está guardada en el servidor

Figura 43. Verificación de la red WAN a la DMZ



Fuente: Autoría propia

De esta manera, se configura Endian Firewall para permitir o denegar el tráfico en sus diferentes zonas. Lo que permite tener un mejor control de la seguridad, mejorar el rendimiento del servidor y evitar daños en la infraestructura del servidor.

7 TEMÁTICA 5: Implementar un Proxy HTTP (No transparente) con políticas de autenticación para navegación en Internet.

En el ámbito de la administración de redes y la seguridad informática, la implementación de un Proxy HTTP no transparente con políticas de autenticación se ha consolidado como una estrategia esencial para controlar el acceso a Internet y reforzar la seguridad organizacional. Este tipo de proxy requiere que los usuarios configuren explícitamente sus navegadores para acceder a los recursos web, lo que permite una gestión más detallada de las políticas de acceso y autenticación.La presente implementación se llevó a cabo utilizando Endian Firewall Community (EFW), configurando tres zonas de red: roja, naranja y verde. Antes de detallar el proceso, se definen los conceptos fundamentales para comprender adecuadamente la configuración realizada.

Proxy HTTP No Transparente: La configuración inicial de un proxy no transparente puede ser más compleja, pero en última instancia proporciona un servicio de proxy mucho más potente y flexible. El spyware y los gusanos que utilizan la web para transmitirse podrían no funcionar debido a que se desconoce la configuración del proxy [10].

Autenticación en el Proxy: permite configurar el método de autenticación que utiliza el servidor proxy y determina cómo validar los equipos cliente al acceder a los proxis. Por defecto, el campo de autenticación de proxy está desactivado y debe activarse para crear nuevas políticas para usuarios o grupos.

Como parte integral del proceso de implementación del proxy HTTP no transparente con políticas de autenticación, se establece una serie de actividades concretas cuyo objetivo es validar tanto la funcionalidad del servidor proxy como la correcta aplicación de las políticas de acceso definidas. Estas actividades se enfocan en la creación de perfiles de usuario, establecimiento de listas de bloqueo (listas negras) de sitios web, aplicación de políticas de autenticación y verificación desde un entorno LAN mediante navegación web. A continuación, se detallan los componentes específicos que conforman el producto esperado:

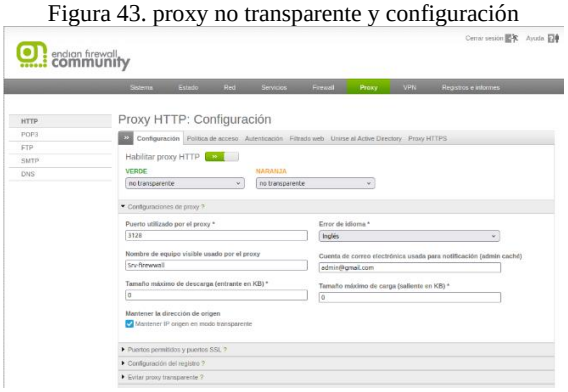
Como primer paso, se crea un perfil de control de acceso que actúe como base para la implementación de restricciones en la navegación. Este perfil está diseñado para bloquear explícitamente el acceso a una serie de dominios considerados no permitidos dentro del entorno organizacional. En este caso particular, la lista negra está compuesta por los siguientes sitios:
www.hotmail.com, www.youtube.com ,
www.elnuevodia.com.co

El segundo componente del producto esperado contempla la activación de un sistema de autenticación basado en usuarios individuales. Se procede a la creación de una cuenta de usuario a través del sistema de autenticación del proxy (como puede ser NCSA en el caso de Squid o mediante integración con LDAP o Active Directory). El usuario creado es asociado a un grupo específico, con el fin de establecer políticas de acceso diferenciadas por rol o nivel de privilegio

Finalmente, se ejecuta una prueba funcional que consiste en verificar, desde una estación de trabajo conectada a la red LAN, el cumplimiento efectivo de las políticas de bloqueo establecidas.

Se accedió a la interfaz gráfica de Endian desde la red verde, utilizando la dirección IP asignada y las credenciales del usuario administrador (admin). Al ingresar por primera vez, fue necesario habilitar manualmente la opción de proxy y esperar la recarga automática de la página. En accesos posteriores, el sistema muestra las redes previamente configuradas y una casilla para seleccionar el tipo de proxy. En este caso, se eligió el modo "proxy no transparente". A continuación, se visualizaron parámetros de configuración como el puerto, idioma, nombre del proxy y correo electrónico. Para esta implementación, se modificó el puerto a 3128 y se ajustaron algunos otros campos básicos, sin intervenir en las configuraciones avanzadas.

Figura 43. proxy no transparente y configuración



Fuente: Autoría propia

A continuación, se accedió a la pestaña de filtrado web, donde se procedió a la creación de un nuevo perfil. En este perfil, se incorporaron a la lista negra los sitios previamente definidos para ser bloqueados. Cabe destacar que, además de la lista personalizada, la plataforma ofrece la opción de aplicar filtros por categorías, lo cual permite adaptar el control de contenidos según las necesidades específicas de la organización.

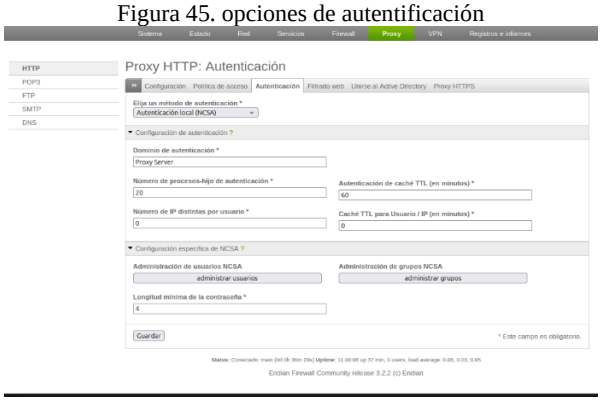
Figura 44. opción de filtrado web

Fuente: Autoría propia

El siguiente paso consistió en la creación del usuario y del grupo para el acceso mediante el proxy. Para ello, se ingresó a la sección de Autenticación, donde se seleccionó el método de autenticación local. Una vez definido este método, se accedió a la opción de administración de usuarios, desde

donde fue posible gestionar las cuentas necesarias para aplicar las políticas de acceso correspondientes.

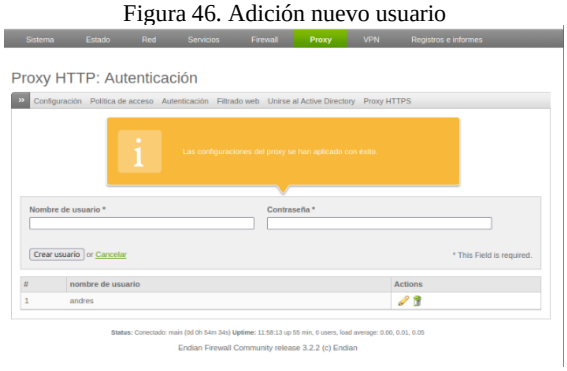
Figura 45. opciones de autentificación



Fuente: Autoría propia

Dentro de esta opción de administración de usuarios se escoge la opción de añadir nuevo, se solicita usuario y clave para el nuevo usuario. También se puede ber todos los usuarios que han sido creado y está la opción de editarlos en el cual podemos hacer cambio de contraseña

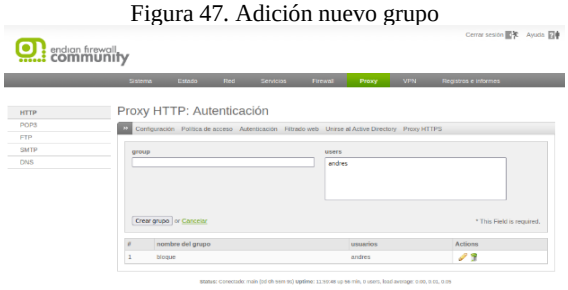
Figura 46. Adición nuevo usuario



Fuente: Autoría propia

Al acceder a la opción de administrar grupos, se presenta la posibilidad de listar todos los grupos creados. Esta funcionalidad permite asignar ciertos permisos a un conjunto de usuarios sin la necesidad de configurarlos individualmente, lo que optimiza el tiempo y la gestión. Durante la creación de un nuevo grupo, se habilita la opción de seleccionar los usuarios que formarán parte de él, para luego proceder a guardar la configuración.

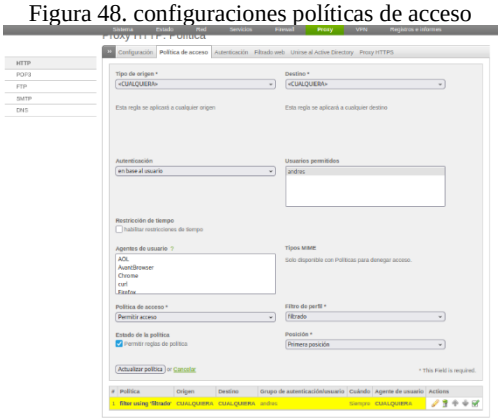
Figura 47. Adición nuevo grupo



Fuente: Autoría propia

Como parte de la configuración final, se procedió a la creación de una nueva política dentro de la pestaña de “Políticas de acceso” del módulo Proxy HTTP. En esta sección, se seleccionó la opción para añadir una nueva política, permitiendo definir múltiples parámetros de control. La política configurada fue aplicada a cualquier origen y destino, sin restricciones de tráfico, con la autenticación desactivada y sin limitaciones de tiempo. Se especificaron agentes de usuario como Chrome, Firefox y curl, sin aplicar filtros de perfil, y se posicionó la política en la primera posición con permisos activos, asociándola al usuario "andres"

Figura 48. configuraciones políticas de acceso



Fuente: Autoría propia

De esta manera se finaliza toda la configuración a nivel del proxy en Endian; sin embargo, aún queda un paso esencial para aplicar correctamente los cambios: la configuración del navegador. En este caso, se accedió a los ajustes del navegador Firefox, específicamente a la sección de configuración de red. Allí se seleccionó la opción de configuración manual del proxy y se ingresó la dirección IP del servidor Endian junto con el puerto 3120, previamente definido. Al intentar navegar, el sistema solicitó las credenciales de usuario y contraseña, las cuales ya habían sido creadas y asociadas en la política configurada anteriormente.

Figura 49. Proxy en firefox

Fuente: Autoría propia

Por último, se procedió a la verificación en los navegadores, comprobando que ninguno de los enlaces incluidos en la lista negra cargara correctamente, tal como se evidencia en las imágenes presentadas a continuación. De esta forma, se concluyó satisfactoriamente la implementación del proxy HTTP no transparente, confirmando el funcionamiento de las políticas de bloqueo y autenticación configuradas.

Figura 50. acceso a hotmail

Fuente: Autoría propia

8 REFERENCIAS

[1] ¿Qué es un firewall? (n.d.). Fortinet. Retrieved May 11, 2025, from https://www.fortinet.com/lat/resources/cyberglossary/firewall

[2] ¿Qué es una red DMZ y por qué la usaría? (n.d.). Fortinet. Retrieved May 24, 2025, from https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz

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

[4] Iñaguazo Velepucha, J. S. (2022). Estudio de Alternativas para la implementación de un Sistema Unificado de Seguridad Informática utilizando hardware de bajo costo y software libre (Bachelor's thesis, Quito: EPN, 2022.)

[5] Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson.

[6] LaCroix, J. (2020). Mastering Ubuntu Server: Gain expertise in the art of deploying, configuring, managing, and troubleshooting Ubuntu Server. Packt Publishing.

[7] León, D. A., Martínezq, J. G., Ardila, I. A., & Mosquera, D. J. (2022). Inteligencia artificial para el control de tráfico en redes de datos: Una Revisión. Entre Ciencia e Ingeniería, 16(31), 17-24.

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

[9] Quiñones, T. O. L., & Rey, L. C. (2012). Herramientas de monitorización y análisis del tráfico en redes de datos. Revista Telem@ tica. Vol, 11(2), 46-59.

[10] Using Transparent versus Non-Transparent Proxying. (n.d.). Help Centre. https://kb.smoothwall.com/hc/en-us/articles/360002033050-Using-Transparent-versus-Non-Transparent-Proxying