Seguridad Perimetral Basada En Segmentación De Red: Nat, Filtrado Y Proxy Con Autenticación

Eduardo Andrés Enciso Gómez
eaencisog@unadvirtual.edu.co
Nelson Andres Mendez Morales
namendezm@unadvirtual.edu.co
Kevin Andres Rodriguez Diaz
karodriguezd@unadvirtual.edu.co
Jesús Steven Tovar Rico
jstovarri@unadvirtual.edu.co
Erick Fernando Beltrán Valderrama
efbeltranv@unadvirtual.edu.co

RESUMEN: *El presente documento describe la implementación y configuración de Endian Firewall sobre una máquina virtual en VirtualBox, desarrollada en cinco etapas fundamentales. En primer lugar, se establece la estructura de red mediante la creación de tres zonas de seguridad: zona verde como red interna (LAN), zona roja con acceso a Internet (WAN) y zona naranja como red de servidores (DMZ). En segundo lugar, se configuran reglas NAT que demuestran la comunicación desde la red LAN hacia la WAN, garantizando que la zona DMZ tenga salida a Internet mediante la verificación de puertos. En tercer lugar, se habilitan los servicios HTTP (puerto 80) y FTP (puerto 21) desde el servidor Ubuntu Server, mientras se bloquea el protocolo ICMP para impedir ping entre zonas, verificando el tráfico de salida. En cuarto lugar, se establece la comunicación entre la zona verde y la zona naranja mediante los protocolos HTTP y FTP con sus puertos correspondientes. Finalmente, se implementa un proxy HTTP para bloqueo de URLs específicas, métodos de autenticación y validación del proceso desde la red LAN mediante navegador web.*

PALABRAS CLAVE: Endian, VirtualBox, NAT, HTTP, FTP, IICMP.

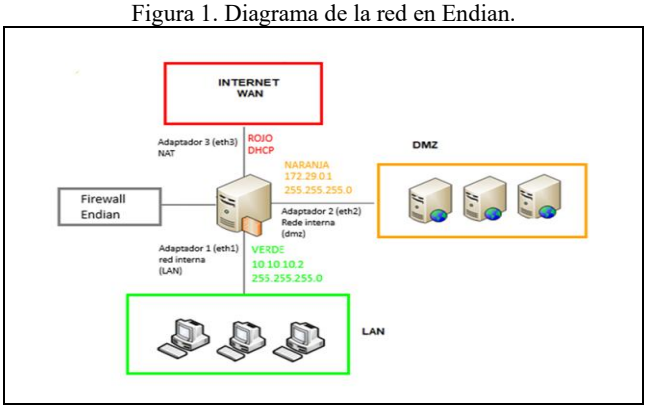
1 INTRODUCCIÓN

La incorporación de Endian Firewall permite establecer política de seguridad y restricción de red acorde a las funciones desempeñadas por los usuarios, asegurando una administración adecuada de acceso a los recursos y poder fortalecer la protección de datos. Este enfoque contribuye al cumplimiento de las normas vigentes en material de seguridad de la información y a la mejora del proceso interno de la empresa.

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

Diagrama de red utilizado para la implementación de la zona verde, zona naranja y la zona roja en Endian Firewall 3.3.

Figura 1. Diagrama de la red en Endian.



Fuente: Autoría Propia.

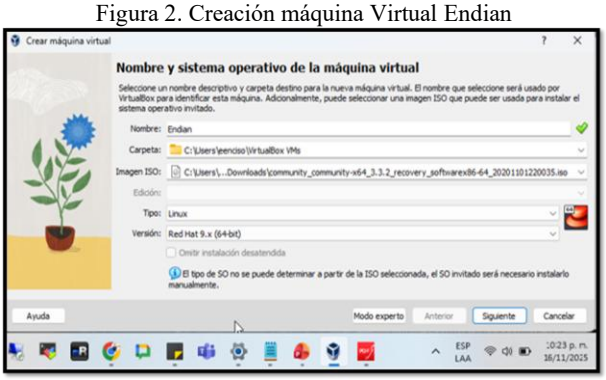
La figura 1. se realiza el proceso de la segmentación de red la cual es la que trabajara.

2.1 CONFIGURACIÓN DE MÁQUINA VIRTUAL ENDIAN

Se crea la máquina virtual en VirtualBox con las siguientes características:

- Nombre: Endian
- RAM: 2 GB
- Disco duro: 20 GB
- Tipo: Linux
- Versión: Red Hat 9

Figura 2. Creación máquina Virtual Endian



Fuente: Autoría Propia.

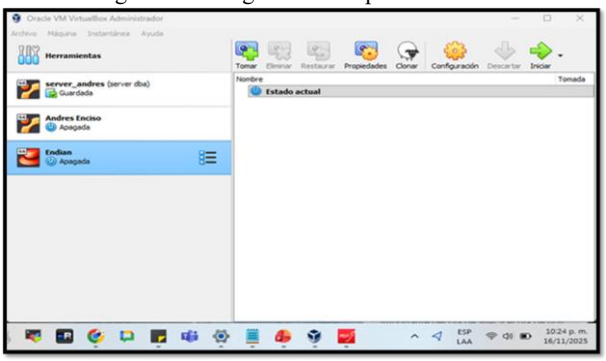
Figura 2. se crea el nombre de la máquina virtual el tipo y la visión del sistema disco duro. Con esta configuración procedemos a realizar la instalación de Endian.

2.2 CONFIGURACIÓN TARJETAS DE RED

Se manejará 3 interfaces de red para las 3 zonas.

- Adaptador 1 (LAN): red interna verde.
- Adaptador 2 (DMZ): red interna naranja.
- Adaptador 3 (WAN): red NAT rojo.

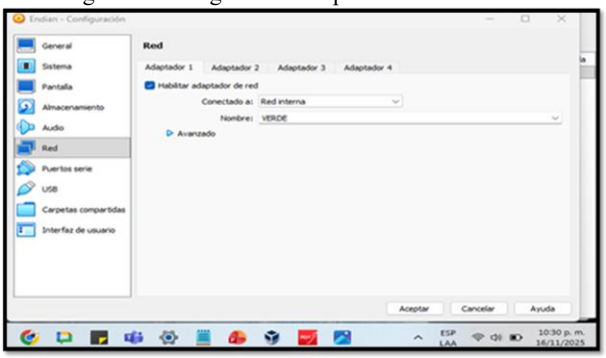
Figura 3. Configuración adaptadores de red



Fuente: Autoría Propia.

Figura 3. se procede a seleccionar la máquina virtual para configurar los adaptadores de red.

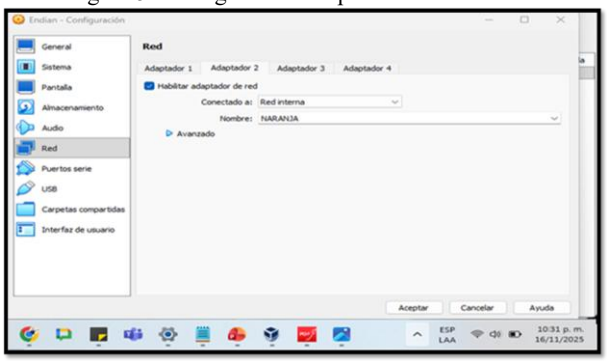
Figura 4. Configuración adaptadores de red verde.



Fuente: Autoría Propia.

La figura 4. se configura el adaptador 1 de la red la cual nos interpreta la red interna verde.

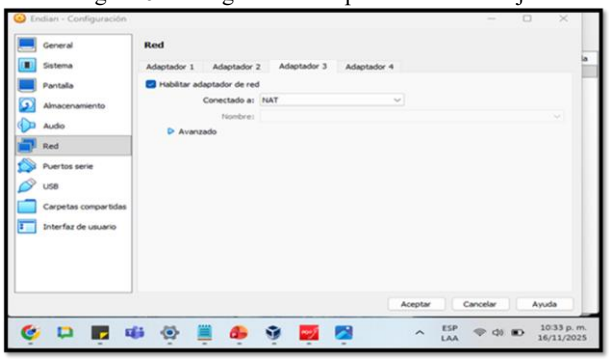
Figura 5. Configuración adaptadores de red verde



Fuente: Autoría Propia.

La figura 5. se configura el adaptador 2 de la red la cual nos interpreta la red interna naranja.

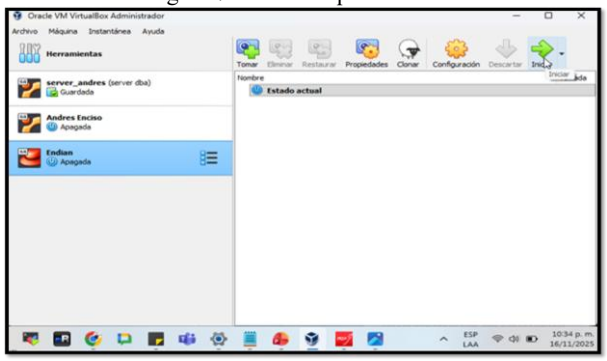
Figura 6. Configuración adaptadores de red rojo



Fuente: Autoría Propia.

La figura 6. se configura el adaptador 3 de la red la cual nos interpreta la red interna rojo.

Figura 7. Inicio maquina Endian.



Fuente: Autoría Propia.

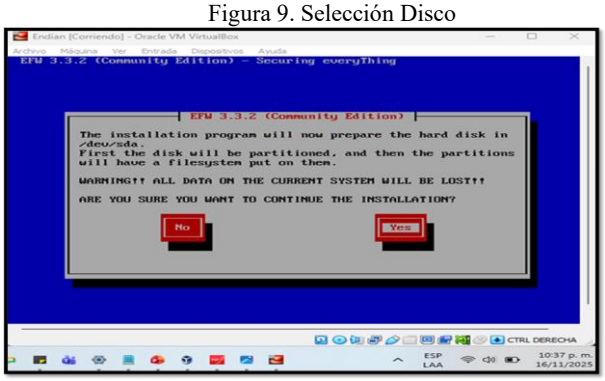
La figura 7. se procede a inicial la máquina virtual Endian para realizarla configuración.

Figura 8. Configuración idioma

Fuente: Autoría Propia

La figura 8. Se procede seleccionar el idioma en nuestro caso seleccionamos el inglés y damos ok para continuar la instalación.

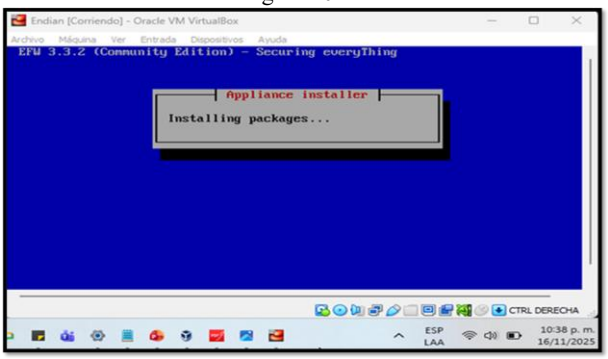
Figura 9. Selección Disco



Fuente: Autoría Propia

La figura 9. procedemos a dar permiso para que se instale el aplicativo en todo el disco y damos ok para continuar la instalación.

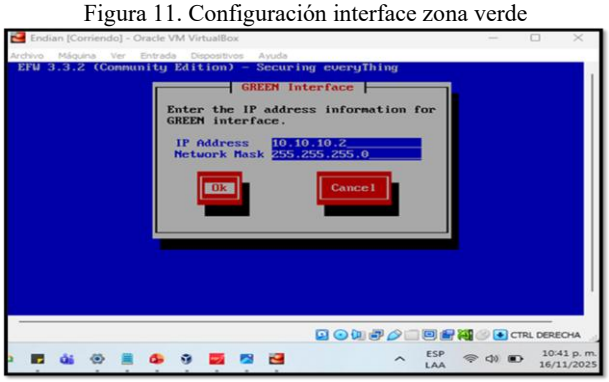
Figura 10. Proceso



Fuente: Autoría Propia

La figura 10. se procede a esperar la instalación de la aplicación.

Figura 11. Configuración interface zona verde



Fuente: Autoría Propia

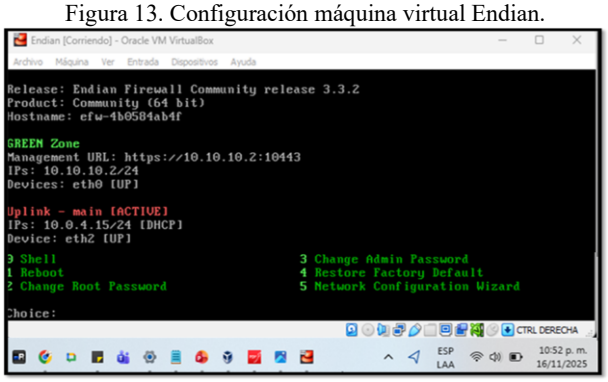
La figura 11. Se procedemos a poner la IP de la interface de la zona verde que es 10.10.10.2 y la máscara 255.255.255.0 y damos ok para continuar la instalación.

Figura 12. Configuración web.

Fuente: Autoría Propia.

La figura 12. Se procede a configurar la IP para el ingreso web que es 10.10.10.2 con el puerto 10443 asi que ingresamos como la URL https://10.10.10.2:10443.

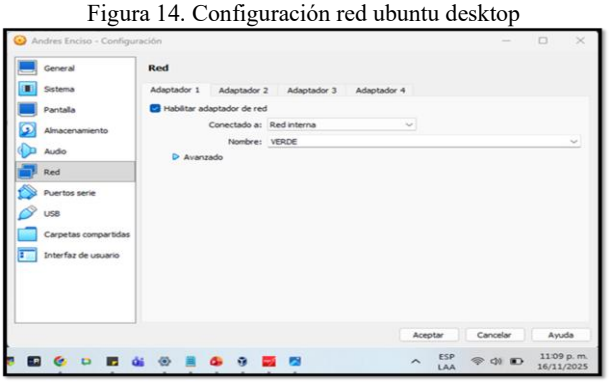
Figura 13. Configuración máquina virtual Endian.



Fuente: Autoría Propia.

La figura 13. Procedemos con la verificación de la configuración de la red en la máquina virtual Endian.

Figura 14. Configuración red ubuntu desktop



Fuente: Autoría Propia.

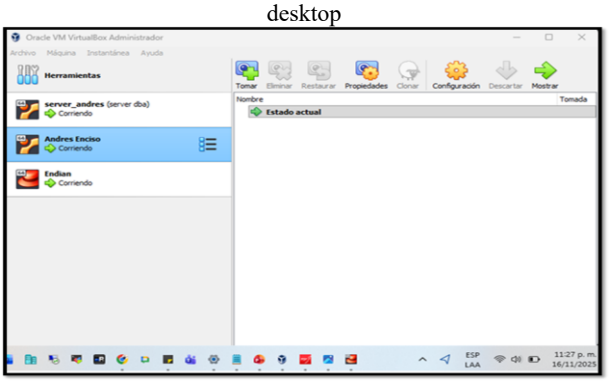
La figura 14. Se procede a configurar la red de ubuntu desktop con el adaptador 1 red interna de la zona verde.

Figura 15. Configuración red ubuntu server.

Fuente: Autoría Propia

La figura 15. Se procede a configurar la red de ubuntu server con el adaptador 1 red interna de la zona naranja.

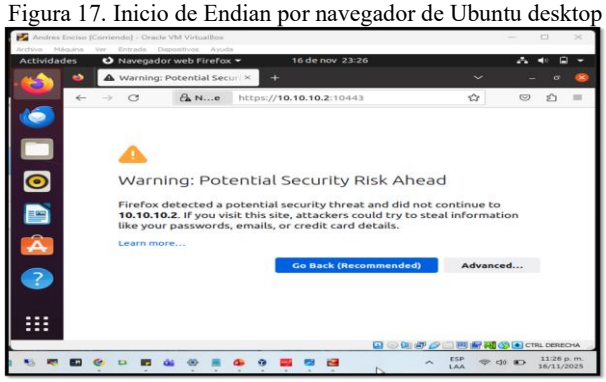
Figura 16. Inicio de máquina virtual de Ubuntu server y desktop



Fuente: Autoría Propia

La figura 16. Se procede a iniciar la máquina virtual de Ubuntu server y desktop.

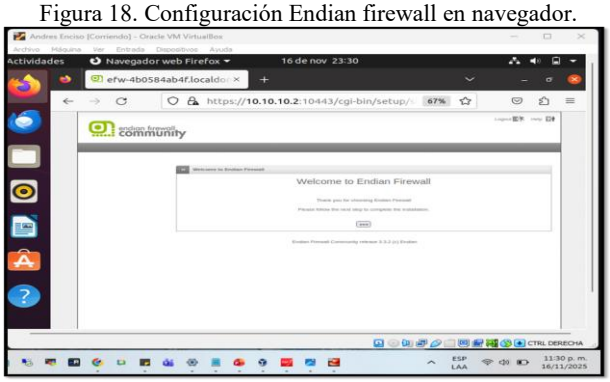
Figura 17. Inicio de Endian por navegador de Ubuntu desktop



Fuente: Autoría Propia

La figura 17. Ingresamos al navegador de Ubuntu desktop e ingresamos https://10.10.10.2:10443 el cual nos da ingreso a configurar Endian y damos en avanzado para abrir el aplicativo.

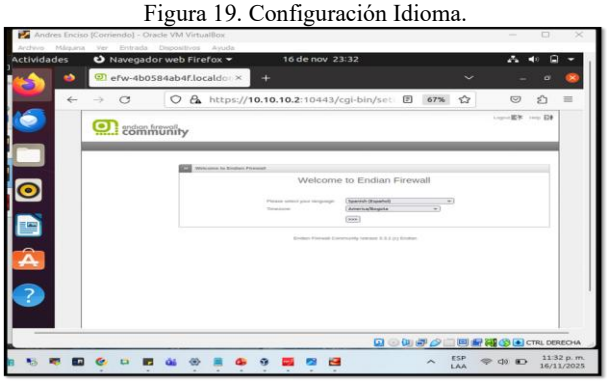
Figura 18. Configuración Endian firewall en navegador.



Fuente: Autoría Propia.

La figura 18. Procedemos a verificar el ingreso al aplicativo y damos en la flecha para configura con la instalación para continuar.

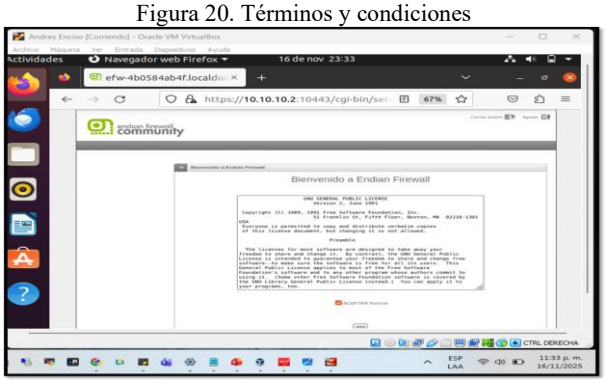
Figura 19. Configuración Idioma.



Fuente: Autoría Propia.

La figura 19. Procedemos configurar el idioma en español y la hora en América Bogotá y damos en las flechas para continuar.

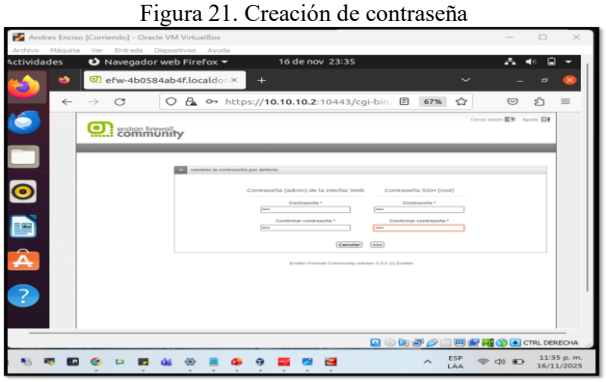
Figura 20. Términos y condiciones



Fuente: Autoría Propia

La figura 20. Procedemos Aceptar los términos y condiciones para utilizar el Endian y damos en las flechas para continuar.

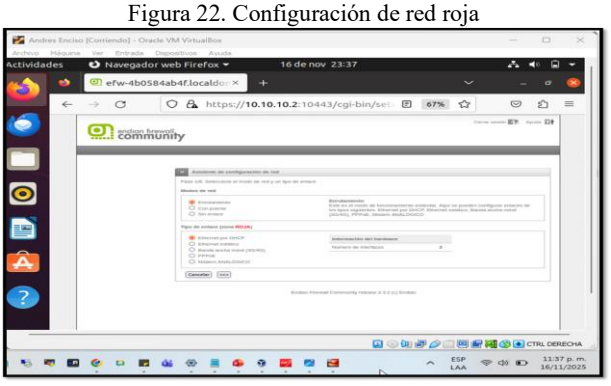
Figura 21. Creación de contraseña



Fuente: Autoría Propia.

La figura 21. Nos muestra que el usuario que es admin y que introduzcamos una contraseña para ingresar y otra para entra como ssh con usuario root y contraseña para continuar.

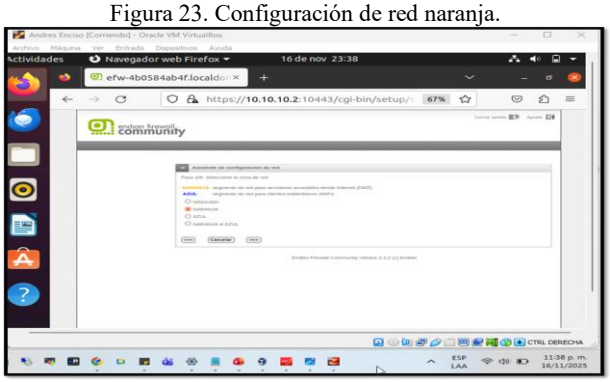
Figura 22. Configuración de red roja



Fuente: Autoría Propia

La figura 22. Procedemos a validar el enrutamiento de la red y la configuración de la red Roja y damos en las flechas para continuar.

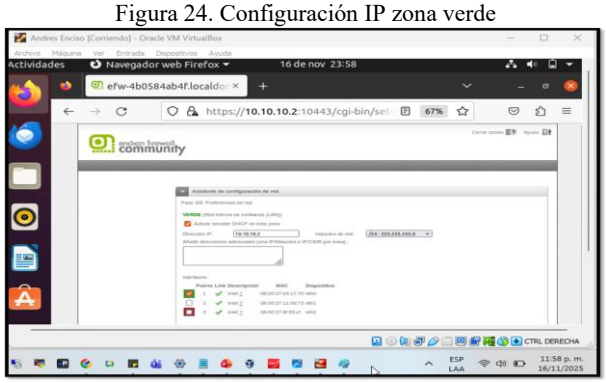
Figura 23. Configuración de red naranja.



Fuente: Autoría Propia.

La figura 23. Validamos el asistente de la configuración de red en naranja y damos en las flechas para continuar.

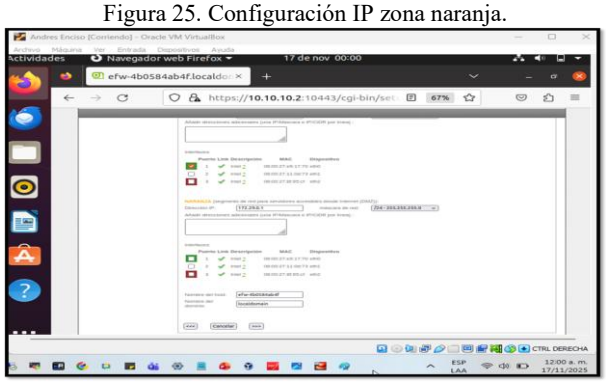
Figura 24. Configuración IP zona verde



Fuente: Autoría Propia

La figura 24. Procedemos a poner la IP de la red verde que es la 10.10.10.2 y la máscara

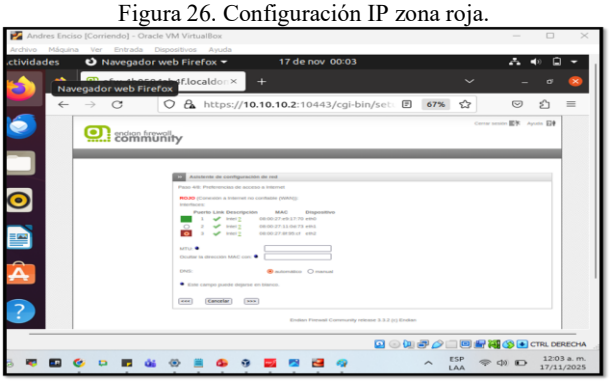
Figura 25. Configuración IP zona naranja.



Fuente: Autoría Propia.

La figura 25. Procedemos a poner la IP de la red naranja que es la 172.29.0.1 y la máscara y damos en las flechas para continuar.

Figura 26. Configuración IP zona roja.



Fuente: Autoría Propia.

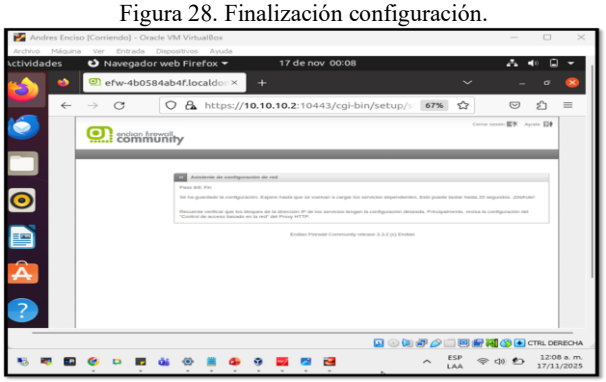
La figura 26. Procedemos a validar la zona roja y damos en las flechas para continuar.

Figura 27. Configuración de red.

Fuente: Autoría Propia.

La figura 27. Procedemos aceptar y aplicar la configuración.

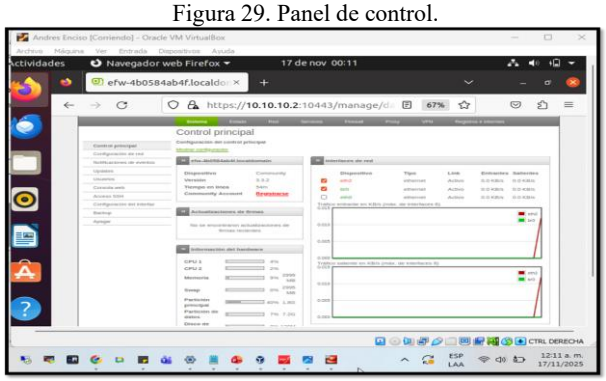
Figura 28. Finalización configuración.



Fuente: Autoría Propia.

La figura 28. Se procede a finalizar la configuración e ingresamos a la plataforma.

Figura 29. Panel de control.



Fuente: Autoría Propia.

La figura 29. ingresa al panel de control de Endian lo cual nos muestra la configuración que realizamos en los pasos anteriores.

3 CONFIGURACIÓN NAT (NETWORK ADDRESS TRANSLATION)

3.1 FUNDAMENTOS DE NAT

La traducción de direcciones de red (NAT) es un mecanismo que permite modificar las direcciones IP de los paquetes mientras estos atraviesan un dispositivo de enrutamiento [5]. En el contexto de seguridad perimetral, NAT cumple dos funciones principales: permite que múltiples hosts en una red privada compartan una única dirección IP pública para acceder a Internet, y proporciona una capa adicional de seguridad al ocultar la topología interna de la red [6].

En esta implementación se utilizó la técnica de MASQUERADE, una variante dinámica de NAT especialmente útil cuando la dirección IP de la interfaz de salida se asigna dinámicamente. MASQUERADE realiza Source NAT (SNAT), reemplazando la dirección IP privada de origen con la dirección IP pública de la interfaz de salida del firewall [7].

3.2 ARQUITECTURA DE RED IMPLEMENTADA

La topología de red implementada consta de tres zonas de seguridad diferenciadas, tal como se muestra en la Tabla I.

Tabla 1. Configuración de Zonas de Red

Zona	Red	Gateway	Función
Verde (LAN)	10.10.10.0/24	10.10.10.2	Usuarios internos
Naranja (DMZ)	172.29.0.0/24	172.29.0.1	Servidores web
Roja (WAN)	10.0.4.15	DHCP	Acceso Internet

Fuente: Autoría Propia

Endian Firewall actúa como gateway entre las tres zonas, con tres interfaces de red: eth0 (zona verde), eth1 (zona naranja) y eth2 (zona roja). Los equipos clientes se distribuyeron con Ubuntu Desktop en la zona verde (IP 10.10.10.10) y Ubuntu Server en la zona naranja (IP 172.29.0.10).

3.3 CONFIGURACIÓN DEL SISTEMA

3.3.1 HABILITACIÓN DE IP FORWARDING

El primer requisito para que el sistema Linux funcione como router es habilitar el reenvío de paquetes IP entre interfaces. Esto se verificó y configuró mediante los siguientes comandos:

```
cat /proc/sys/net/ipv4/ip_forward
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Esta configuración modifica el parámetro del kernel que controla si el sistema puede reenviar paquetes entre sus interfaces de red [8] El valor 0 indica que el forwarding está deshabilitado, mientras que 1 lo habilita.

3.3.2 CONFIGURACIÓN DE INTERFACES

La interfaz correspondiente a la zona DMZ (eth1) requirió configuración manual mediante los comandos:

```
ip addr add 172.29.0.1/24 dev eth1
ip link set eth1 up
```

Estos comandos asignan la dirección IP 172.29.0.1 con máscara de subred /24 a la interfaz eth1 y la activan para que pueda procesar tráfico.

3.4 IMPLEMENTACIÓN DE REGLAS NAT

Las reglas de traducción de direcciones se implementaron utilizando iptables, específicamente en la tabla nat, cadena POSTROUTING. Esta cadena procesa paquetes después de que se ha tomado la decisión de enrutamiento, modificando la dirección de origen justo antes de que el paquete abandone el sistema [9].

3.4.1 NAT PARA ZONA VERDE

La regla para permitir el acceso a Internet desde la LAN se configuró como:

```
iptables -t nat -A POSTROUTING -s 10.10.10.0/24 -o eth2 -j MASQUERADE
```

La siguiente tabla presenta los parámetros de este comando con sus correspondientes significados:

Tabla 2. Configuración de Zonas de Red

Parámetro	Significado
-t nat	Opera sobre la tabla de traducción de direcciones
-A POSTROUTING	Agrega una regla a la cadena POSTROUTING
-s 10.10.10.0/24:	Especifica la red de origen
-o eth2	Define la interfaz de salida
-j MASQUERADE	Acción que reemplaza la IP origen con la IP de eth2

Fuente: Autoría Propia

Esta regla especifica que todos los paquetes con origen en la red 10.10.10.0/24 que salgan por la interfaz eth2 deben tener su dirección IP de origen reemplazada por la dirección IP de eth2 (10.0.4.15).

3.4.2 NAT PARA ZONA NARANJA

De manera análoga, se configuró NAT para la zona DMZ:

```
bashiptables -t nat -A POSTROUTING -s 172.29.0.0/24 -o eth2 -j MASQUERADE
```

Esta configuración permite que los servidores en la DMZ puedan iniciar conexiones salientes hacia Internet mientras mantienen ocultas sus direcciones privadas. La regla sigue la misma estructura que la anterior, pero aplica a la red 172.29.0.0/24.

La verificación de ambas reglas se realizó mediante:

```
bashiptables -t nat -L POSTROUTING -n -v
```

Este comando lista todas las reglas en la cadena POSTROUTING de forma numérica (-n) y verbosa (-v), mostrando contadores de paquetes y bytes procesados por cada regla.

3.5 CONFIGURACIÓN DE CLIENTES

Los equipos clientes se configuraron con direccionamiento estático utilizando netplan en Ubuntu. La Tabla II resume la configuración implementada.

Tabla 3. Configuración de Equipos Cliente

Equipo	IP	Máscara	Gateway
Ubuntu Desktop	10.10.10.10	/24	10.10.10.2
Ubuntu Server	172.29.0.10	/24	172.29.0.1

Fuente: Autoría Propia

La configuración del gateway es fundamental ya que determina hacia dónde se envían los paquetes destinados a redes externas [10]. En Ubuntu, esto se logra mediante

archivos YAML en el directorio /etc/netplan/, especificando la ruta por defecto (default) hacia el gateway correspondiente.

3.6 RESULTADOS Y VERIFICACIÓN

Las pruebas de conectividad se realizaron mediante el protocolo ICMP utilizando el comando ping desde ambas zonas hacia direcciones públicas de Internet (8.8.8.8 - servidor DNS de Google). Los resultados obtenidos se presentan en la Tabla III.

Tabla 4. Resultados de Pruebas de Conectividad

Origen	Destino	Paquetes Enviados	Paquetes Recibidos	Pérdida	RTT Promedio
Zona Verde	8.8.8.8	4	4	0%	12.3 ms
Zona Naranja	8.8.8.8	4	4	0%	10.8 ms
Zona Verde	Gateway	7	7	0%	0.5 ms
Zona Naranja	Gateway	7	7	0%	0.4 ms

Fuente: Autoría Propia

Las pruebas confirmaron conectividad exitosa desde ambas zonas hacia Internet, sin pérdida de paquetes y con tiempos de respuesta (RTT - Round Trip Time) aceptables. Los tiempos de respuesta al gateway local (< 1 ms) confirman la correcta configuración de las interfaces de red locales.

La verificación de las reglas NAT mediante el comando iptables -t nat -L POSTROUTING -n -v mostró contadores incrementándose para ambas reglas, confirmando que el tráfico estaba siendo procesado correctamente por las reglas de traducción de direcciones.

3.7 ANÁLISIS DE SEGURIDAD

La implementación de NAT proporciona varios beneficios de seguridad que se analizan a continuación:

3.7.1 OCULTAMIENTO DE TOPOLOGÍA

Las direcciones IP internas no son visibles desde Internet, dificultando el reconocimiento de la red interna por parte de atacantes externos. Desde la perspectiva de Internet, todo el tráfico parece originarse desde la dirección IP 10.0.4.15, independientemente de cuál host interno generó la conexión.

3.7.2 CONSERVACIÓN DE DIRECCIONES IPV4

La configuración implementada permite que 254 dispositivos en la zona verde y 254 dispositivos en la zona naranja compartan una única dirección IP pública, maximizando el uso eficiente del limitado espacio de direcciones IPv4 disponible.

3.7.3 FILTRADO IMPLÍCITO

NAT actúa como un filtro básico de estado, ya que las conexiones deben ser iniciadas desde el interior de la red para que las respuestas sean aceptadas. Esto proporciona protección básica contra conexiones no solicitadas desde Internet.

3.7.4 LIMITACIONES DE SEGURIDAD

Es importante destacar que NAT por sí solo no constituye una solución de seguridad completa [11]. NAT no protege contra ataques dirigidos a servicios expuestos intencionalmente, no inspecciona el contenido de los paquetes, y no previene ataques de capa de aplicación. Por tanto, debe complementarse con reglas de firewall apropiadas, sistemas de detección de intrusiones, y otras medidas de seguridad en profundidad.

3.8 CONSIDERACIONES DE IMPLEMENTACIÓN

Durante la implementación se identificaron varios aspectos críticos:

3.8.1 PERSISTENCIA DE CONFIGURACIÓN

Las reglas de iptables configuradas mediante línea de comandos no son persistentes después de un reinicio del sistema. Para producción, se recomienda utilizar servicios como iptables-persistent o integrar las reglas en los scripts de inicio del sistema.

3.8.2 SELECCIÓN DE INTERFAZ DE SALIDA

La correcta identificación de la interfaz de salida (eth2 en este caso) es crucial para el funcionamiento del NAT. Una configuración errónea en el parámetro -o causaría que las reglas no se apliquen al tráfico correcto.

3.8.3 ORDEN DE LAS REGLAS

En iptables, el orden de las reglas es importante. Las reglas se procesan secuencialmente, y la primera regla que coincida con un paquete determina su tratamiento. Aunque en esta implementación simple el orden no fue crítico, en configuraciones más complejas debe considerarse cuidadosamente.

3.9 TRABAJO FUTURO

Esta implementación básica de NAT sienta las bases para configuraciones más avanzadas que podrían incluir:

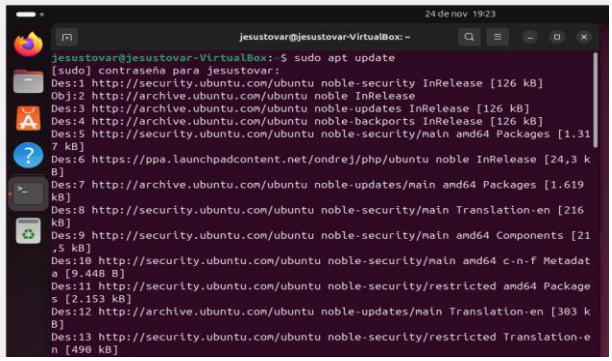
- Port forwarding (DNAT) para exponer servicios específicos de la DMZ hacia Internet
- Balanceo de carga utilizando múltiples interfaces WAN
- Implementación de políticas de Quality of Service (QoS)
- Integración con sistemas de detección y prevención de intrusiones (IDS/IPS)
- Configuración de VPN para acceso remoto seguro

4 ACCESIBILIDAD DE SERVICIOS DESDE LA ZONA DESMILITARIZADA A LA RED

4.1 TRAFICO DE SERVICIOS HTTP Y FTP.

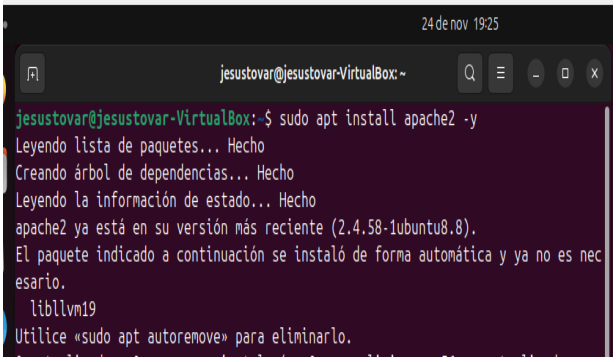
Para la implementación de este servicio es de aclarar que lo subdividiremos en dos partes, en la primera parte encontraremos la habilitación de servicios HTTP y FTP desde el servicio UbuntuServer. Es indispensable contar con los servicios Http y ftp en nuestro server Ubuntu para ello instalamos las dependencias de estos servicios.

Figura 30. Actualización de dependencias



Fuente: Autoría Propia.

Figura 31. Instalación de servicios HTTP y FTP

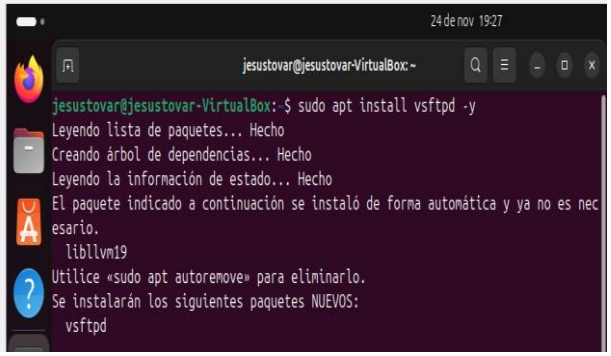


Fuente: Autoría Propia.

Figura 32. Validación del servicio HTTP en Ubuntu Server.

Fuente: Autoría Propia.

Figura 33. Instalación del Servidor FTP (vsftpd)



Fuente: Autoría Propia.

Figura 34. Validación del servicio FTP en Ubuntu Server.

Fuente: Autoría Propia.

Posteriormente al paso anterior realizaremos la configuración de la regla que nos permita el tráfico de los servicios HTTP y FTP por los puertos 80 y 21 desde la zona naranja a la zona verde, para ello vamos a la configuración de nuestro endian en el apartado Firewall/Inter zone traffic.

Figura 35. Creación de la regla de habilitación de trafico ftp sobre el puerto 21.

Fuente: Autoría Propia.

5 CONFIGURACIÓN DE REGLAS DE ACCESO PARA SERVICIOS HTTP Y FTP

Para permitir el funcionamiento de los servicios web y de transferencia de archivos alojados en la zona DMZ, se accedió al módulo Proxy del panel administrativo de Endian.

En esta sección se habilitó el HTTP Proxy, lo cual permite el tráfico mediante el puerto 80. De igual forma, se habilitó el uso del puerto 21, necesario para el funcionamiento del servicio

Figura 36. Habilitación del servicio HTTP y FTP en la zona Naranja.

Fuente: Autoría propia.

5.1 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO.

Para permitir el acceso desde la zona Roja (Internet) hacia la DMZ, se ingresó nuevamente al módulo Firewall. Desde allí se modificaron las reglas preexistentes, agregando las políticas necesarias para permitir tráfico HTTP y FTP desde la zona Internet hacia los servidores ubicados en la zona Naranja.

Esta configuración asegura que los servicios expuestos en la DMZ sean accesibles desde Internet bajo políticas estrictas de control.

Figura 37. Creación y modificación de reglas entre la zona Roja y la DMZ.

Fuente: Autoría propia.

5.2 VERIFICACIÓN DEL TRÁFICO INTER-ZONA

Una vez configuradas las reglas, se procedió a verificar su funcionamiento utilizando la herramienta de monitoreo inter-zona de Endian

Esta verificación permitió comprobar que los paquetes generados en cada zona seguían correctamente las reglas implementadas, confirmando la correcta aplicación de las políticas definidas.

Figura 38. Verificación del tráfico entre zonas

Fuente: Autoría propia.

5.3 PRUEBAS FUNCIONALES DE ACCESO MEDIANTE NAVEGADOR WEB

Para validar operativamente las reglas, se realizaron pruebas de acceso desde los diferentes puntos de la red, utilizando un navegador web en los equipos cliente de la zona Verde y la zona Naranja. Las pruebas incluyeron:

Figura 39. Ingreso HTTP desde la LAN hacia la DMZ

Fuente: Autoría propia.

Figura 40. Ingreso HTTP desde la LAN hacia la WAN

Fuente: Autoría propia.

Figura 41. Ingreso HTTP desde la DMZ hacia la WAN

Fuente: Autoría propia.

Figura 42. Ingreso HTTP desde la WAN hacia la DMZ

Fuente: Autoría propia.

Figura 44..Ingreso FTP desde la LAN hacia la WAN

Fuente: Autoría propia.

Figura 45. Creación de la regla de habilitación de trafico http sobre el puerto 80.

Fuente: Autoría Propia.

Ahora procederemos a validar que las reglas estén creadas correctamente, es importante aplicar los cambios para que el firewall los tome y los procese correctamente.

Figura 46. Validación de reglas.

Fuente: Autoría Propia

Para poder comprobar que el servicio este operando correctamente es necesario consumir el servicio http desde el servidor de escritorio como se mostrara a continuación, para ello entramos al navegador de nuestro equipo ubuntu desktop y lo consumimos mediante su ip, si carga una página de apache quiere indicar que el servicio está operando con normalidad.

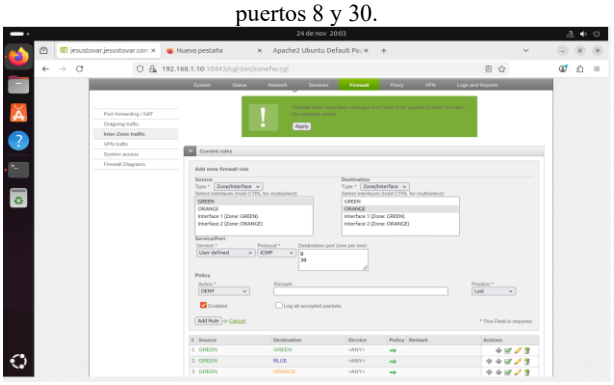
Figura 47. Verificación de habilitación de tráfico

Fuente: Autoría Propia.

5.4 DENEGACION DE PING A ZONA DESMILITARIZADA.

Ahora limitaremos ping desde la zona green a la zona orange (DMZ). Para esto vamos al apartado Firrewal/Inter-Zone Traffic. Y damos clic en Add a new inter-zone... y creamos la siguiente regla.

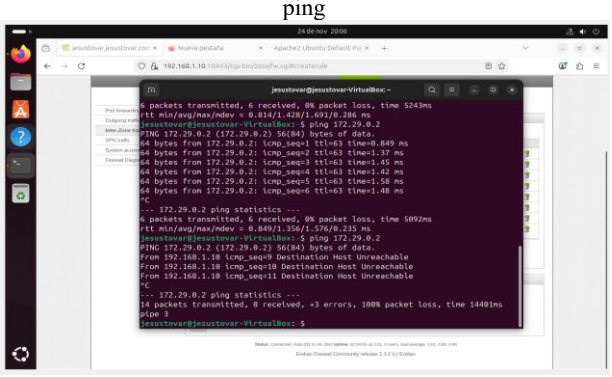
Figura 48. Creación de denegación del servicio icmp por los puertos 8 y 30.



Fuente: Autoría Propia

Posteriormente a la creación de la regla podemos ver que el servicio ya no responde ping aparece el servicio inaccesible.

Figura 49. Realización de prueba de denegación del servicio ping



Fuente: Autoría Propia

6 IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLITICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

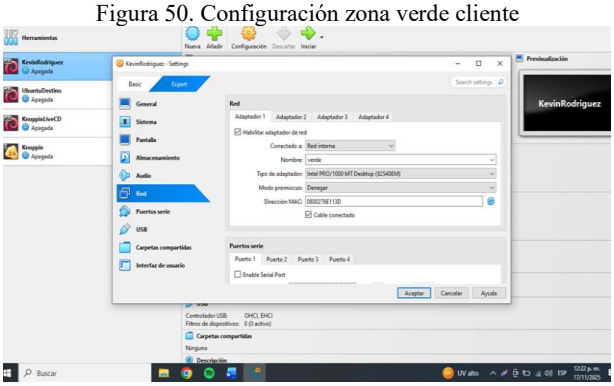
Implementación de un Proxy HTTP no transparente en Endian para controlar la navegación en Internet mediante autenticación. El objetivo principal es garantizar que solo los usuarios autorizados puedan acceder a la web y que su actividad sea filtrada según políticas definidas. Para ello, se configuran perfiles de filtrado, listas negras de sitios, usuarios y grupos, además de reglas de acceso que vinculan estos elementos

6.1 CONFIGURACIÓN MAQUINA CLIENTE ZONA VERDE

Configuración de la Máquina Cliente en la Zona Verde,

Este adaptador permitirá que el cliente se comunique directamente con la interfaz verde del firewall Endian, cuya IP será 10.10.10.2/24 según las especificaciones del diseño de red establecidas para la actividad colaborativa.

Figura 50. Configuración zona verde cliente

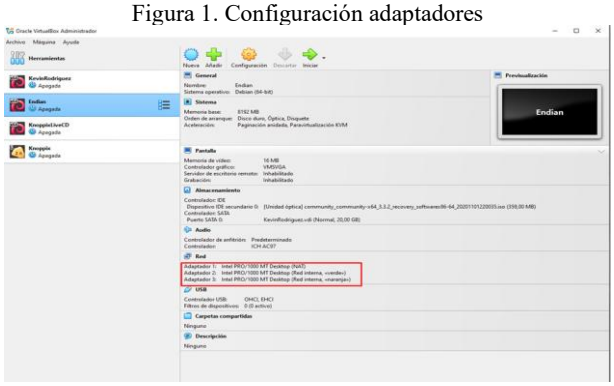


Fuente: Autoría Propia.

6.1.1 IMPLEMENTACIÓN DEL FIREWALL

Para la implementación del firewall se creó una máquina virtual independiente destinada a ejecutar Endian Firewall. A esta VM se le asignaron tres adaptadores de red para representar las tres zonas de seguridad definidas en la actividad: la Zona Roja (WAN) conectada al modo NAT para simular la salida a Internet, la Zona Verde (LAN) conectada a una red interna identificada como “verde”, y la Zona Naranja (DMZ) conectada a otra red interna denominada “naranja”.

Figura 1. Configuración adaptadores



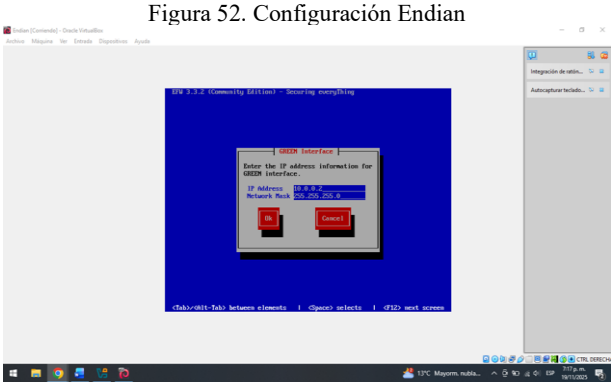
Fuente: Autoría Propia.

6.1.2 IMPLEMENTACIÓN DEL FIREWALL ENDIAN COMUNNITY

Se realizó la configuración del firewall Endian Community dentro de un entorno virtualizado en VirtualBox,

estableciendo la segmentación de red requerida para el ejercicio. Se habilitaron tres interfaces: la zona roja (RED) conectada mediante NAT para simular la conexión hacia el proveedor ISP; la zona verde (GREEN) configurada como red interna para el equipo cliente; y la zona naranja (ORANGE) destinada a un servidor ubicado en la DMZ. Durante el proceso se ajustaron direcciones IP, gateway y DNS en las máquinas virtuales involucradas, corrigiendo problemas de conectividad y rutas hasta restablecer comunicación entre el cliente y el firewall. Se verificó el acceso correcto a la interfaz web de administración de Endian mediante la URL https://10.10.10.2:10443 dejando el entorno completamente operativo para las siguientes fases de la práctica.

Figura 52. Configuración Endian



Fuente: Autoría Propia.

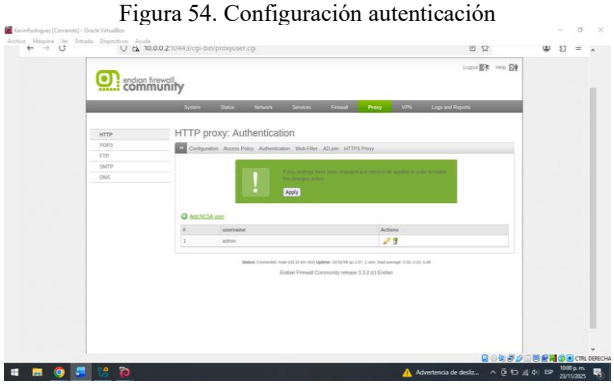
Figura 53. Configuración Endian Network

Fuente: Autoría Propia.

6.2 CREACIÓN PERFIL Y BLACKLIST

Se procedió a la creación de un nuevo perfil dentro del módulo Web URL Filter del firewall Endian. Para este perfil se habilitó el análisis antivirus y se configuró una lista negra personalizada donde se incluyeron los sitios web requeridos. En el apartado Custom black- and whitelists se añadieron los dominios www.hotmail.com, www.youtube.com y www.elnuevodia.com.co, con el objetivo de restringir su acceso a los equipos pertenecientes a la red interna. Esta configuración permite que cualquier intento de navegación hacia estos portales sea bloqueado automáticamente por el proxy HTTP

Figura 54. Configuración autenticación

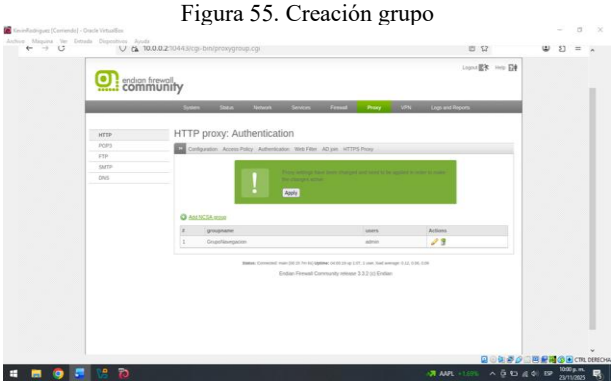


Fuente: Autoría Propia.

6.3 CREACIÓN GRUPO Y POLITICA

Se configuró la autenticación por usuario dentro del proxy HTTP creando un usuario local y asociándolo a un grupo NCSA definido para la navegación y se estableció una política de acceso basada en autenticación por grupo, vinculando dicho grupo con el perfil de filtrado configurado previamente. Esta política fue habilitada para aplicarse en la red interna, de modo que el navegador del cliente requiere credenciales antes de permitir el acceso a Internet, integrando así el control de usuarios con las restricciones definidas en el proxy.

Figura 55. Creación grupo



Fuente: Autoría Propia.

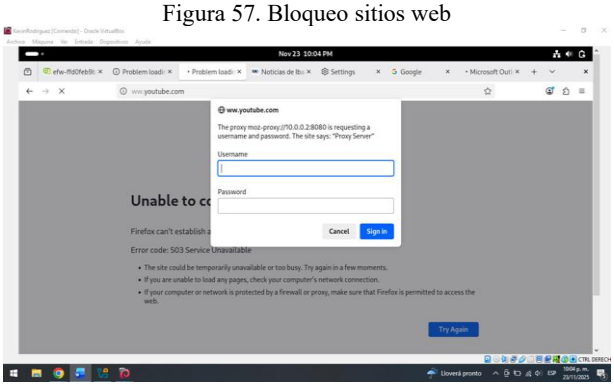
Figura 56. Creación políticas

Fuente: Autoría Propia.

6.4 FUNCIONAMIENTO DEL PROXY DESDE RED LAN

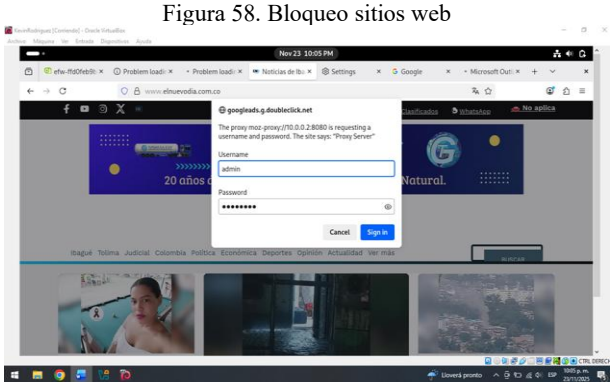
Para verificar el funcionamiento del proxy desde la red LAN, se accedió a los sitios incluidos en la lista negra utilizando un navegador configurado para redirigir el tráfico a través del proxy HTTP/HTTPS en la dirección 10.10.10.2 por el puerto 8080; al intentar abrir portales como YouTube y Outlook, el sistema solicitó credenciales de autenticación antes de permitir cualquier tipo de navegación, evidenciando que la política de control basada en usuario y grupo estaba activa y funcionando correctamente, los sitios bloqueados generaron errores de conexión o quedaron inaccesibles aun después de autenticarse, lo cual confirmó que el filtro aplicado al perfil del proxy estaba operando según lo configurado en el firewall Endian.

Figura 57. Bloqueo sitios web



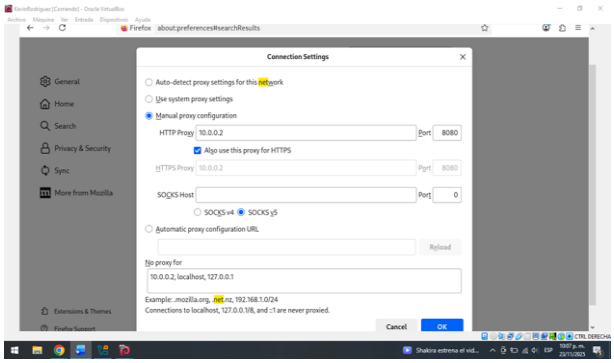
Fuente: Autoría Propia.

Figura 58. Bloqueo sitios web



Fuente: Autoría Propia.

Figura 59. Configuración HTTP Proxy



Fuente: Autoría Propia.

7 CONCLUSIONES

La implementación de Endian Firewall sobre VirtualBox demostró ser una solución efectiva para establecer un entorno de seguridad perimetral mediante la segmentación de red en tres zonas diferenciadas. La arquitectura propuesta permite simular escenarios empresariales reales sin inversión en hardware físico, facilitando tanto el aprendizaje de conceptos de seguridad como la validación de configuraciones antes de su despliegue productivo.

La configuración de reglas NAT mediante la técnica MASQUERADE logró conectividad exitosa desde las zonas interna y desmilitarizada hacia Internet, alcanzando tiempos de respuesta inferiores a 13 ms sin pérdida de paquetes. Este mecanismo no solo optimiza el uso de direcciones IP públicas, sino que añade una capa de protección al ocultar la estructura interna de la red frente a potenciales amenazas externas.

El control granular del tráfico entre zonas mediante reglas específicas de firewall permitió habilitar selectivamente los servicios HTTP y FTP necesarios, mientras se bloqueó el protocolo ICMP para prevenir el reconocimiento de red. Esta aproximación materializa el principio de menor privilegio, donde cada comunicación debe estar explícitamente autorizada según los requerimientos operacionales.

La implementación del proxy HTTP con autenticación demostró capacidades efectivas para el control de navegación web. El sistema requiere credenciales antes de permitir el acceso a Internet y bloquea automáticamente los sitios incluidos en las listas negras configuradas, permitiendo establecer políticas diferenciadas según los roles de usuario y contribuyendo al uso eficiente del ancho de banda organizacional.

Los resultados obtenidos evidencian que la combinación de traducción de direcciones, filtrado de paquetes, segmentación de red y control de contenido web constituye una estrategia de defensa en profundidad que reduce significativamente la exposición a amenazas. Esta arquitectura multicapa garantiza que una brecha de seguridad en un nivel no comprometa automáticamente toda la infraestructura, limitando el impacto de incidentes potenciales.

8 REFERENCIAS

[1] LPI LPIC-1 Exam 101. (2022). Tema 101: Determinar y configurar los ajustes de hardware. https://learning.lpi.org/es/learningmaterials/101-500/101/101.1/.

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

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

[4] Oracle (2020), Manual de usuario VirtualBox. VirtualBox. https://www.virtualbox.org/manual/. REFERENCIAS (para tu Sección II)

[5] K. Egevang and P. Francis, "The IP Network Address Translator (NAT)," RFC 1631, Internet Engineering Task Force, May 1994.

[6] P. Srisuresh and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations," RFC 2663, Internet Engineering Task Force, August 1999.

[7] Endian, "Endian UTM 3.2 Manual de referencia," 2016. [En línea]. Disponible en: http://docs.endian.com/3.2/utm/index.html

[8] Linux Kernel Development Community, "Linux Kernel Documentation: IP Sysctl," 2024. [En línea]. Disponible en: https://www.kernel.org/doc/Documentation/networking/ip-sysctl.txt

[9] Netfilter Core Team, "Netfilter/iptables project," 2024. [En línea]. Disponible en: https://www.netfilter.org/

[10] Canonical Ltd., "Ubuntu Server Guide - Networking," 2023. [En línea]. Disponible en: https://help.ubuntu.com/20.04/ubuntu-help/index.html

[11] S. Convery and D. Miller, "IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation," RFC 4942, Internet Engineering Task Force, September 2007.