“Implementación de un Firewall Endian en VirtualBox con configuración de zonas, NAT y proxy HTTP”

Luisa Fernanda Baquero
lfbaquerolo@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación práctica del firewall GNU/Linux Endian en un entorno de virtualización con VirtualBox, abarcando la configuración de redes por zonas (verde, roja y naranja), reglas NAT para traducción de direcciones, control de tráfico entre zonas, y establecimiento de un proxy HTTP no transparente con autenticación y políticas de filtrado de contenido. Se describen los resultados obtenidos a lo largo de cinco temáticas fundamentales, evidenciando el funcionamiento esperado de cada configuración.*

PALABRAS CLAVE: Endian, Firewall, VirtualBox, NAT, DMZ, Proxy, HTTP, Reglas de tráfico.

1 INTRODUCCIÓN

El uso de firewalls en entornos empresariales es crucial para el control y la seguridad del tráfico de red. En este contexto, Endian Firewall representa una solución basada en GNU/Linux que permite segmentar redes, aplicar políticas de seguridad y controlar servicios de forma eficiente. Este artículo detalla el proceso de configuración de Endian en VirtualBox, simulando un entorno de red con zonas diferenciadas y múltiples servicios.

2 DESARROLLO DE ACTIVIDADES

Instalación y configuración de la distribución GNU/Linux Endian (EFW), así mismo seleccionar una de las siguientes cinco (5) temáticas y darle solución bajo esta distribución.

2.1 INSTALACIÓN Y CONFIGURACIÓN DE LA DISTRIBUCIÓN GNU/LINUX ENDIAN (EFW)

Para llevar a cabo la implementación del firewall de código abierto Endian, se optó por realizar el proceso dentro de un entorno controlado utilizando VirtualBox, se descarga de la imagen ISO de Endian Firewall Community Edition desde su sitio oficial.

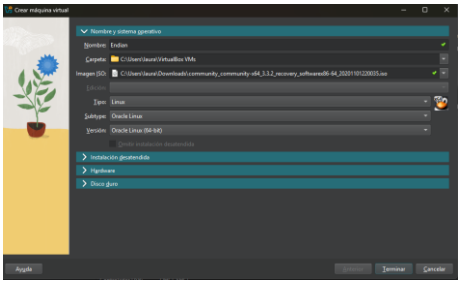

Figura 1 Configuración de la máquina Virtual en VirtualBox Endian

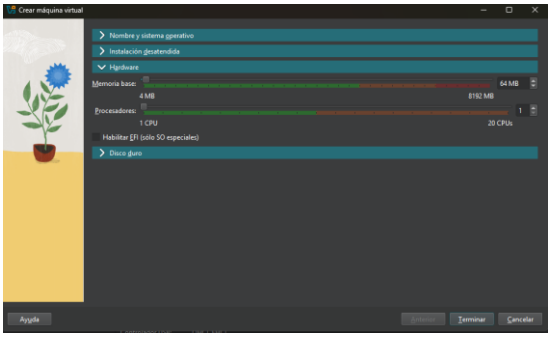

Figura 2 Configuración Hardware

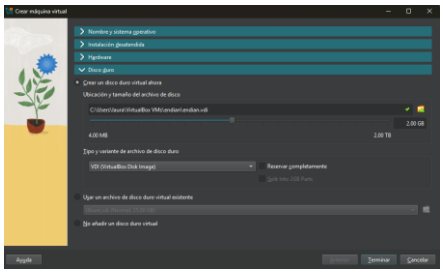

Figura 3 Configuración Disco Duro Virtual

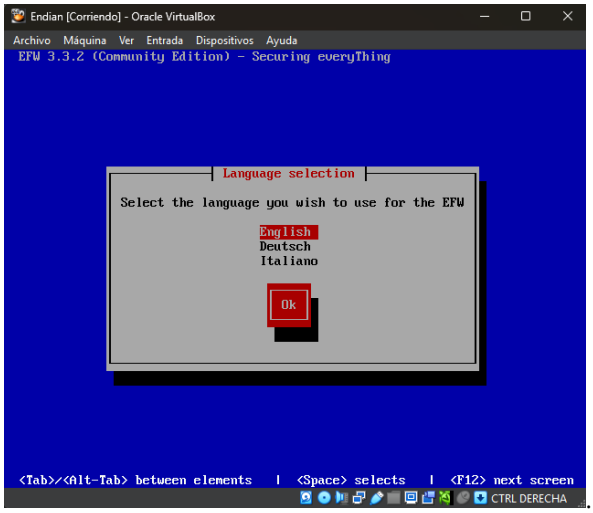

Figura 4 Instalación del Endian selección de idioma

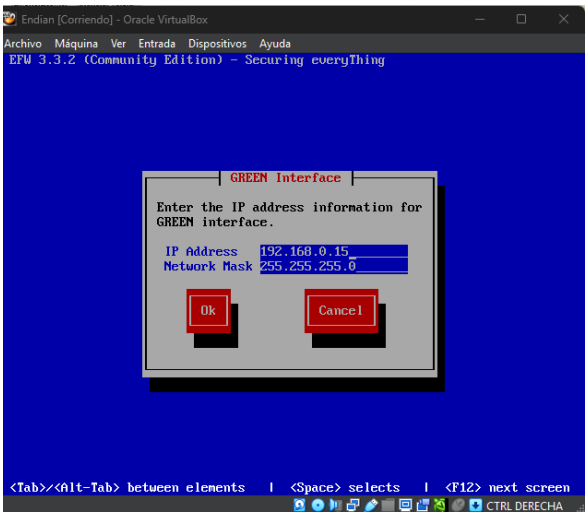

Figura 6 Instalación del Endian selección de la IP para la zona Verde 192.168.0.15

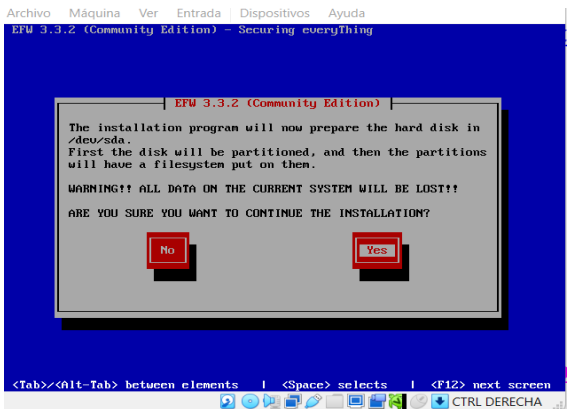

Figura 5 Instalación del Endian selección de la partición del Disco

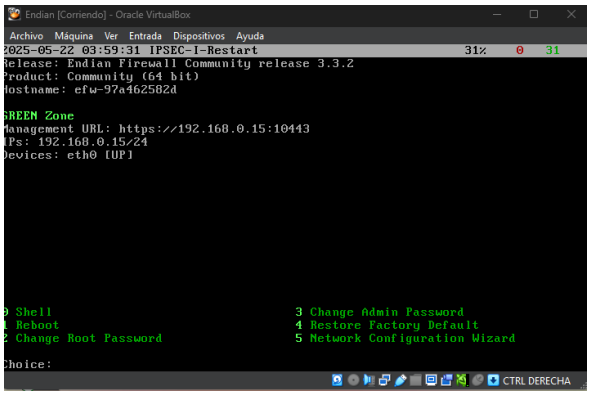

Figura 7 Instalación completa del Endian

2.2 DESARROLLO DE LAS TEMÁTICAS

Se dividieron las actividades entre los miembros del grupo. Cada integrante asumió una temática, realizó la instalación, configuración y prueba del servicio, documentando paso a paso el procedimiento y sus evidencias. Las máquinas virtuales fueron configuradas bajo red en modo puente para garantizar conectividad entre Windows y GNU/Linux.

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

Implementación de GNU/Linux Endian con las zonas verde, roja y naranja, así: Zona verde: Red interna (LAN), Zona roja: Acceso a internet (WAN) y Zona naranja: Servidores (DMZ).

Se creó una regla de NAT de salida desde la zona verde hacia la roja para permitir a los clientes navegar en Internet. Se configuró en:

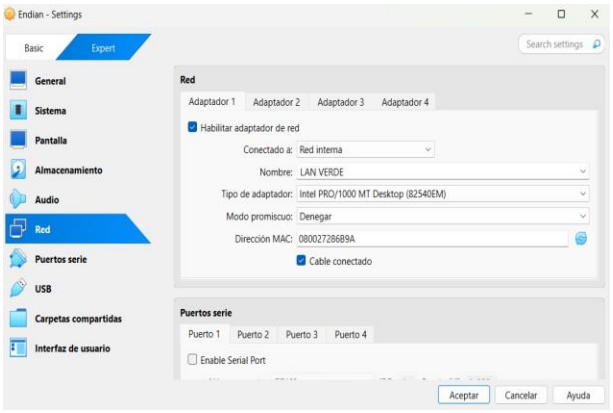

Figura 8 Configuración de los adaptadores Red en la máquina virtual de Endian – LAN Verde

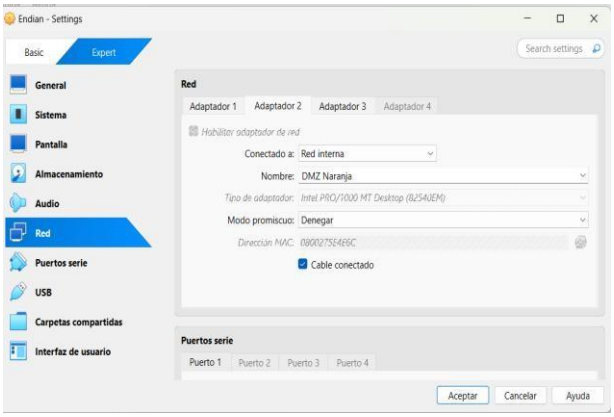

Figura 9 Configuración de los adaptadores de Red en la máquina virtual de Endian – DMZ – Naranja

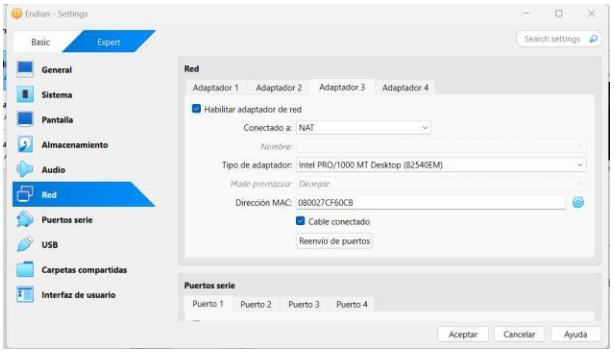

Figura 10 Configuración de los adaptadores de Red en la máquina virtual de Endian – WAN - Roja

Seguidamente en cada uno de las distribuciones se configuran los adaptadores a cada distribución.

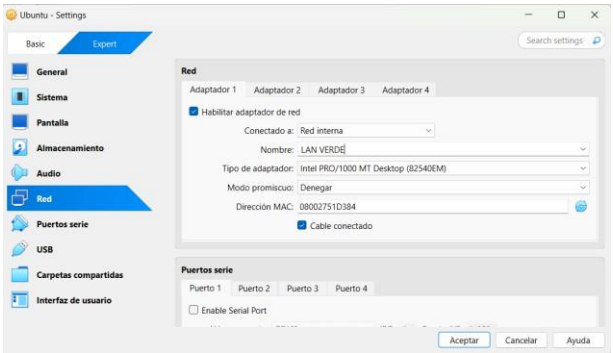

Figura 11 Configuración del adaptador de la Red en el UBUNTU

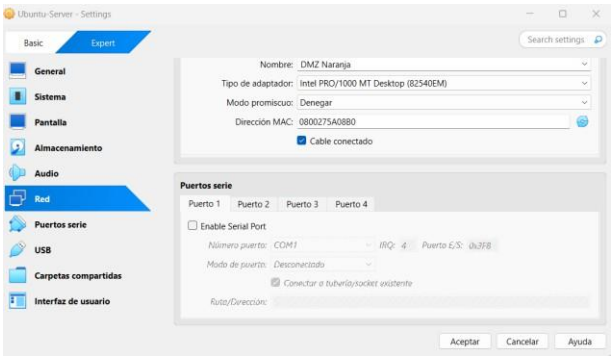

Figura 12 Configuración del adaptador de la Red en el UBUNTU Server

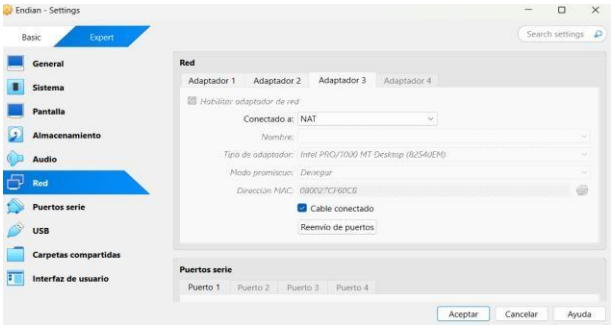

Figura 13 Configuración del adaptador de la Red Endian

Una vez realizado la instalación del Endian totalmente, en esta se realiza la configuración de la IP zona verde, la cual se le asigno la IP 192.168.3.20, esta configuración arroja una URL la cual debemos ingresar posteriormente para realizar la configuración mediante la interfaz web de Endian.

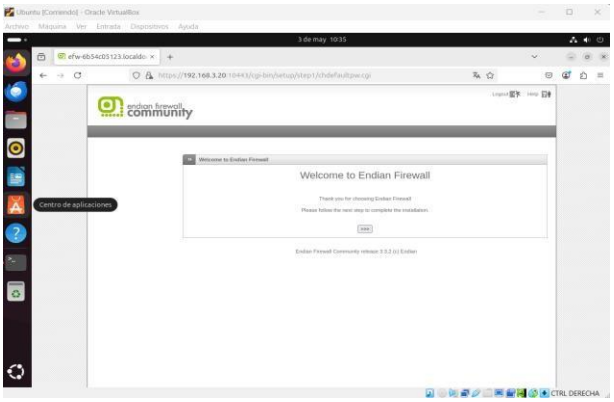

Figura 14 Ingreso a la configuración del Endian por panel mediante la IP https://192.168.3.20:10443

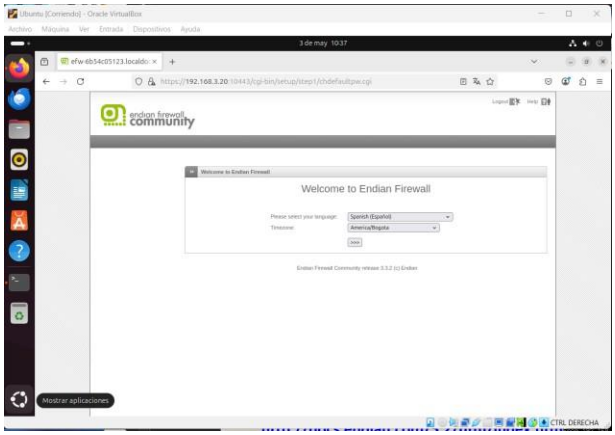

Figura 15 Selección de idioma y región

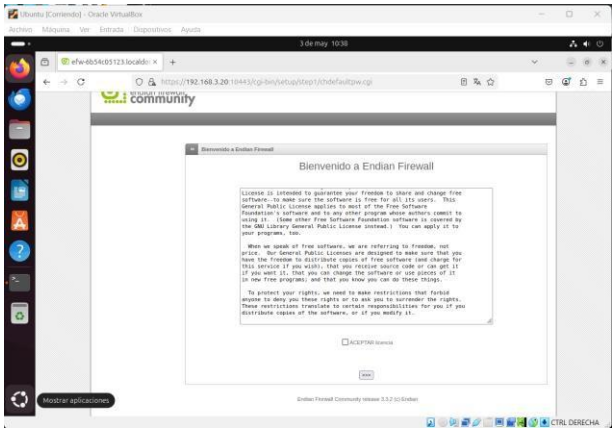

Figura 16 Aceptación de términos y condiciones.

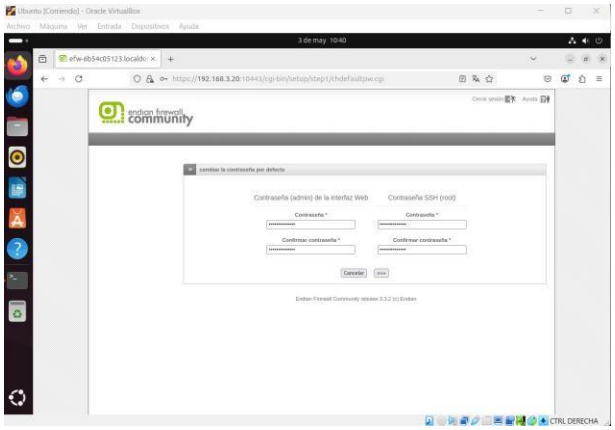

Figura 17 Configuración de contraseña del Root y de la interfaz Web

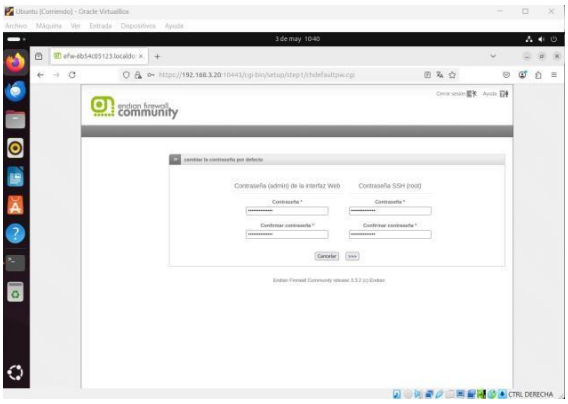

Figura 18 Enrutamiento y tipo de enlace de la zona Roja este caso DHCP

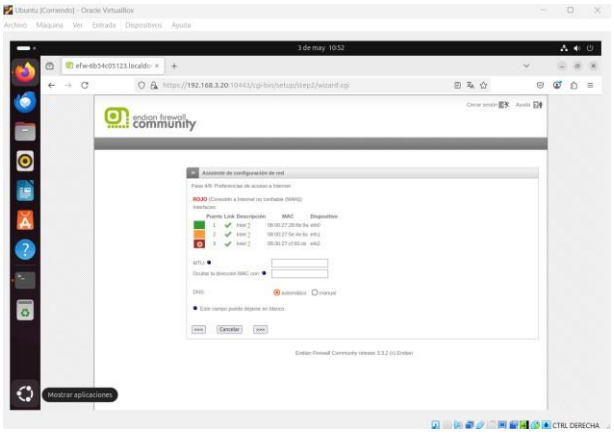

Figura 21 Configuración de la zona roja

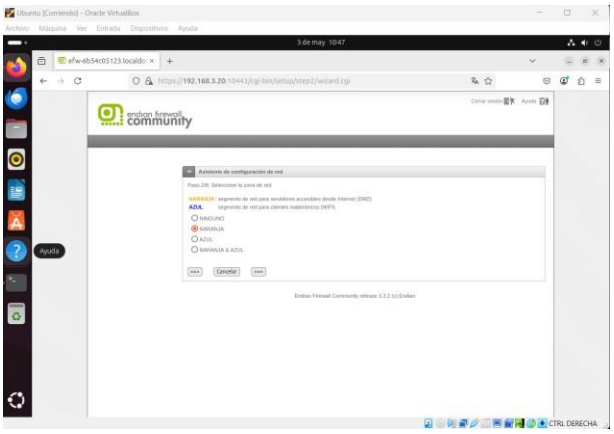

Figura 19 Selección de configuración de la zona Naranja DMZ

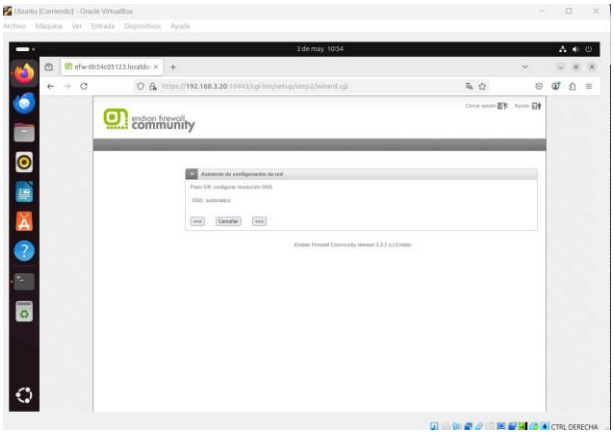

Figura 22 Configuración del DNS para este caso automático

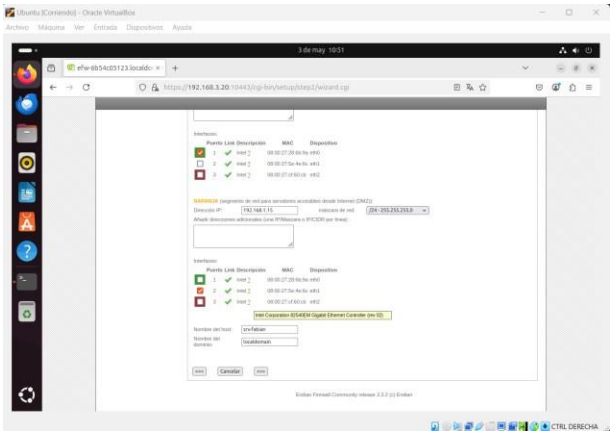

Figura 20 Configuración de la zona Naranja DMZ, IP y nombre del host

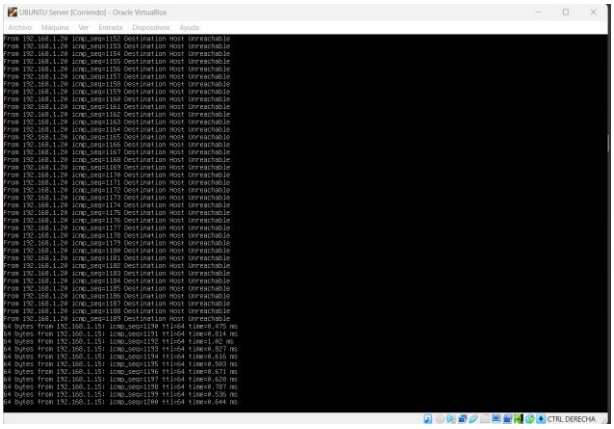

Figura 23 Comprobación del ping realizado desde el servidor

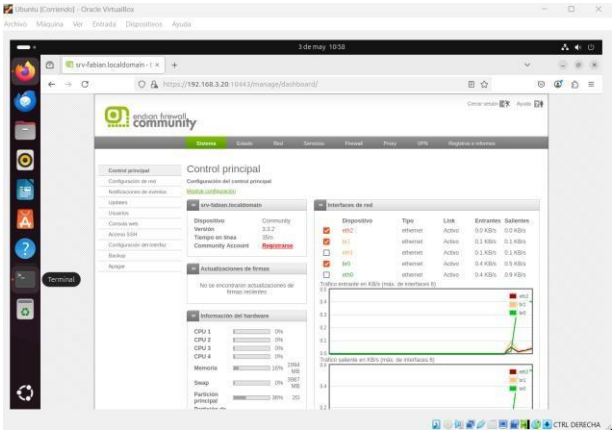

Figura 24 Visualización del comportamiento de la red

.

La implementación del firewall Endian en una máquina virtual a través de VirtualBox permitió simular un entorno de red segmentado, seguro y funcional, replicando el comportamiento de una infraestructura perimetral en entornos reales. El uso de zonas diferenciadas (verde, roja y naranja) facilitó la gestión del tráfico, el aislamiento de servicios y la creación de políticas de seguridad específicas para cada segmento.

2.2.2 TEMÁTICA 2 CONFIGURACIÓN NAT.

CONFIGURACIÓN NAT

Figura 25 Nat.

Configuración de NAT para LAN hacia WAN:

1. Acceder al dispositivo de red: Accede al router o dispositivo de red que actuará como gateway para la LAN.
2. Crear una regla de NAT: Crea una regla de NAT que traduzca las direcciones IP privadas de la LAN a una dirección IP pública.
3. Especificar la interfaz: Especifica la interfaz que se utilizará para la conexión a Internet (WAN).
4. Configurar la dirección IP pública: Configura la dirección IP pública que se utilizará para la traducción.
5. Guardar la configuración: Guarda la configuración para que se aplique.

Configuración de NAT para DMZ hacia Internet:

1. Crear una zona DMZ: Crea una zona DMZ (Demilitarized Zone) en el dispositivo de red.
2. Crear una regla de NAT: Crea una regla de NAT que traduzca las direcciones IP de la DMZ a una dirección IP pública.
3. Especificar la interfaz: Especifica la interfaz que se utilizará para la conexión a Internet.
4. Configurar la dirección IP pública: Configura la dirección IP pública que se utilizará para la traducción.
5. Guardar la configuración: Guarda la configuración para que se aplique.

Verificar la configuración de NAT:

1. Verificar la tabla de NAT: Verifica la tabla de NAT para asegurarte de que las reglas se hayan aplicado correctamente.
2. Probar la conectividad: Prueba la conectividad desde la LAN y la DMZ hacia la Internet para asegurarte de que la configuración de NAT esté funcionando correctamente.
3. Verificar la tabla de NAT: Verifica la tabla de NAT para asegurarte de que las reglas se hayan aplicado correctamente.
4. Probar la conectividad: Prueba la conectividad desde la LAN y la DMZ hacia la Internet para asegurarte de que la configuración de NAT esté funcionando correctamente.

Reenvío de puertos / NAT:

1. Crear una regla de re-envío de puertos: Crea una regla de re-envío de puertos que permita el tráfico entrante hacia un servidor o dispositivo específico en la LAN o DMZ.
2. Especificar el puerto: Especifica el puerto que se utilizará para el re-envío.
3. Especificar la dirección IP: Especifica la dirección IP del servidor o dispositivo que recibirá el tráfico.
4. Guardar la configuración: Guarda la configuración para que se aplique.

Ejemplo:

Tenemos un router con la siguiente configuración:

- Interfaz WAN: eth0 con dirección IP pública 200.100.50.25
- Interfaz LAN: eth1 con dirección IP privada 192.168.1.1
- Zona DMZ: eth2 con dirección IP privada 10.10.10.1

La configuración de NAT para la LAN hacia la WAN sería la siguiente:

- -Router(config)# ip nat inside source list 1 interface eth0 overload
- -Router(config)# ip nat inside source static tcp 192.168.1.100 80 200.100.50.25 80

La configuración de NAT para la DMZ hacia la Internet sería:

- -Router(config)# ip nat inside source list 2 interface eth0 overload
- -Router(config)# ip nat inside source static tcp 10.10.10.100 80 200.100.50.25 8080

Configuración de NAT para LAN hacia WAN:

Si tenemos un router con la siguiente configuración:

- Interfaz WAN (Internet): GigabitEthernet0/0 con dirección IP pública 200.100.50.25/24
- Interfaz LAN: GigabitEthernet0/1 con dirección IP privada 192.168.1.1/24
- Red LAN: 192.168.1.0/24

Queremos configurar NAT para que los dispositivos de la LAN puedan acceder a Internet. Para ello, crearemos una regla de NAT que traduzca las direcciones IP privadas de la LAN a la dirección IP pública de la interfaz WAN.

Paso 1: Configurar la interfaz WAN:

- Router(config)# interface GigabitEthernet0/0
- Router(config-if)# ip address 200.100.50.25 255.255.255.0
- Router(config-if)# no shutdown

Paso 2: Configurar la interfaz LAN:

- Router(config)# interface GigabitEthernet0/1
- Router(config-if)# ip address 192.168.1.1 255.255.255.0

Paso 3: Crear una lista de acceso para la LAN

- Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255

Paso 4: Configurar la regla de NAT:

- Router(config)# ip nat inside source list 1 interface GigabitEthernet0/0 overload

Paso 5: Aplicar la regla de NAT a la interfaz LAN:

- Router(config)# interface GigabitEthernet0/1
- Router(config-if)# ip nat inside

Paso 6: Aplicar la regla de NAT a la interfaz WAN:

- Router(config)# interface GigabitEthernet0/0
- Router(config-if)# ip nat outside

Configuración de NAT para DMZ hacia Internet:

Si tenemos una zona DMZ con la siguiente configuración:

- Interfaz DMZ: GigabitEthernet0/2 con dirección IP privada 10.10.10.1/24
- Red DMZ: 10.10.10.0/24

Queremos configurar NAT para que los dispositivos de la DMZ puedan acceder a Internet. Para ello, crearemos una regla de NAT que traduzca las direcciones IP de la DMZ a la dirección IP pública de la interfaz WAN.

Paso 1: Configurar la interfaz DMZ:

- Router(config)# interface GigabitEthernet0/2
- Router(config-if)# ip address 10.10.10.1 255.255.255.0
- Router(config-if)# no shutdown

Paso 2: Crear una lista de acceso para la DMZ:

- Router(config)# access-list 2 permit 10.10.10.0 0.0.0.255

Paso 3: Configurar la regla de NAT:

- Router(config)# ip nat inside source list 2 interface GigabitEthernet0/0 overload

Paso 4: Aplicar la regla de NAT a la interfaz DMZ:

- Router(config)# interface GigabitEthernet0/2
- Router(config-if)# ip nat inside

Re-envío de puertos / NAT:

Si queremos permitir el acceso a un servidor web en la LAN con dirección IP 192.168.1.100 y puerto 80. Queremos que el tráfico entrante hacia la dirección IP pública 200.100.50.25 y puerto 80 sea re-enviado al servidor web.

- Router(config)# ip nat inside source static tcp 192.168.1.100 80 200.100.50.25 80

De esta manera, cuando alguien acceda a la dirección IP pública 200.100.50.25 y puerto 80, el tráfico será re-enviado al servidor web en la LAN con dirección IP 192.168.1.100 y puerto 80.

2.2.3 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

Paso1 : Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server.

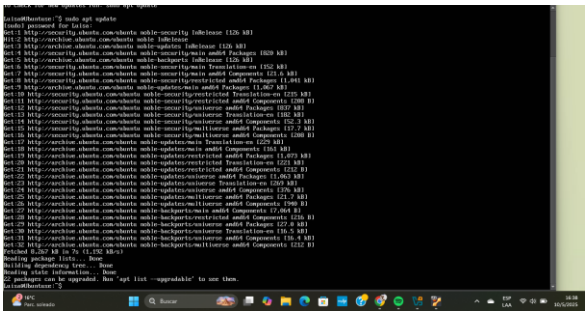

Figura 26 Asegurar que UFW este instalado y habilitado

Paso 2: Permitir HTTP y FTP

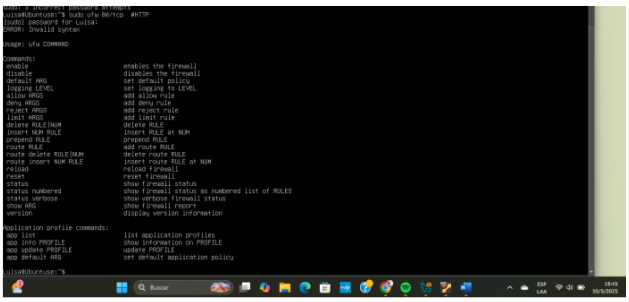

Figura 27 Permitir HTTP

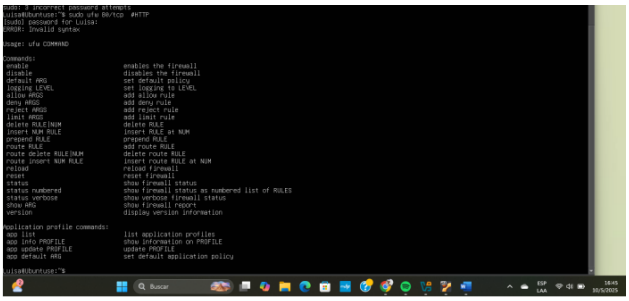

Figura 28 Permitir FTP

Paso 3: Bloquear ICMP (Ping) UFW no bloquea ICMP directamente, así que debemos editar una regla en el archivo de configuración: Se abre el archivo de configuración de UFW antes de que cargue las reglas:

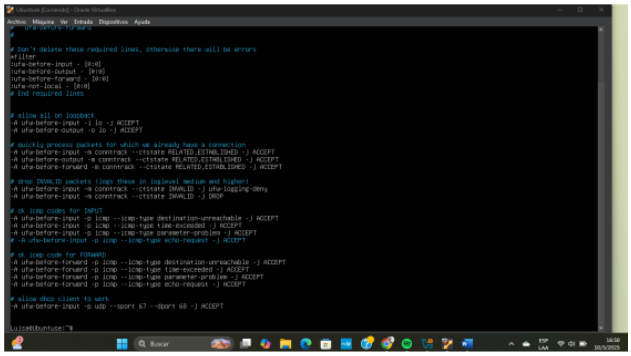

Figura 29 Bloquear ICMP (Ping)

Figura 30 Reiniciar el firewall

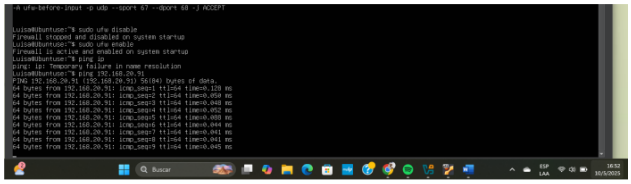

Figura 31 Verificar que ICMP está bloqueado

Paso 4:

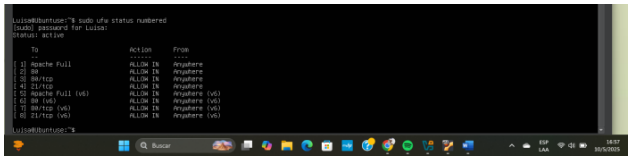

Figura 32 Ver reglas activas en UFW

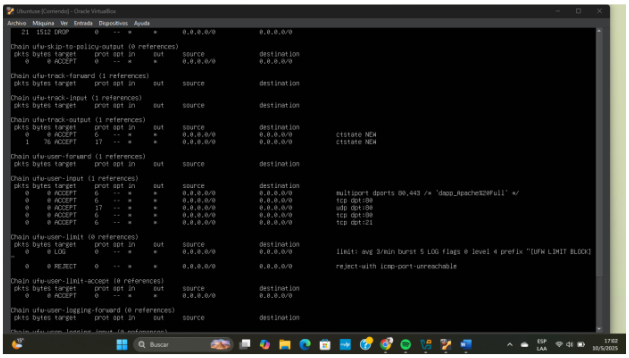

Figura 33 Ver reglas activas en UFW

Figura 36 Definir la segmentación de red para clientes inalámbricos

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

Las reglas de firewall en Endian Firewall que permiten el tráfico controlado entre zonas de red críticas (LAN, DMZ e Internet), asegurando comunicaciones seguras para servicios HTTP y FTP.

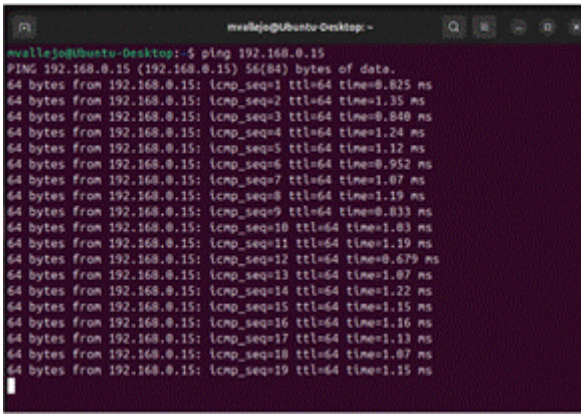

Figura 34 Verificar la conectividad de red hacia el host 192.168.0.1 mediante el comando ping

Figura 37 Asistente de configuración inicial para definir los parámetros de red para las zonas verde (LAN) y Naranja (DMZ).

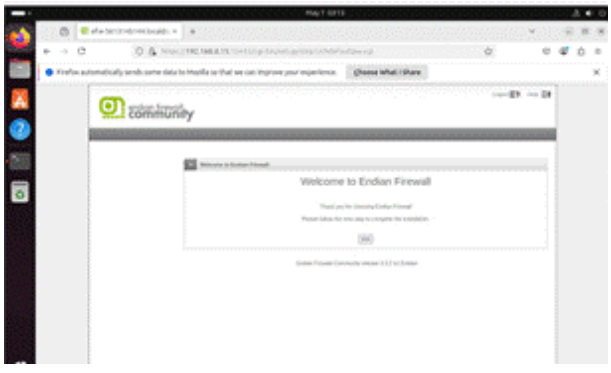

Figura 35 Endian Firewall, para comenzar con la configuración y administración

Figura 38 Asistente de configuración inicial, Configurado correctamente.

.

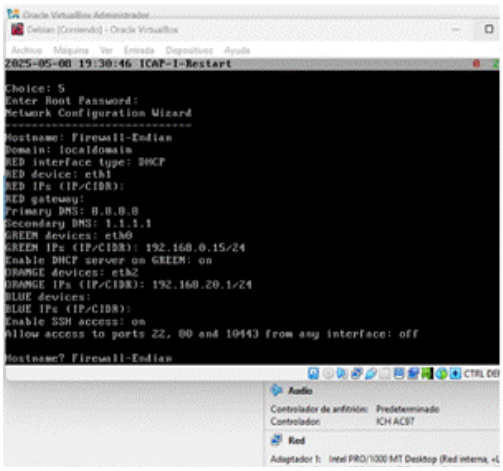

Imagen 39 Configuración la red para el firewall

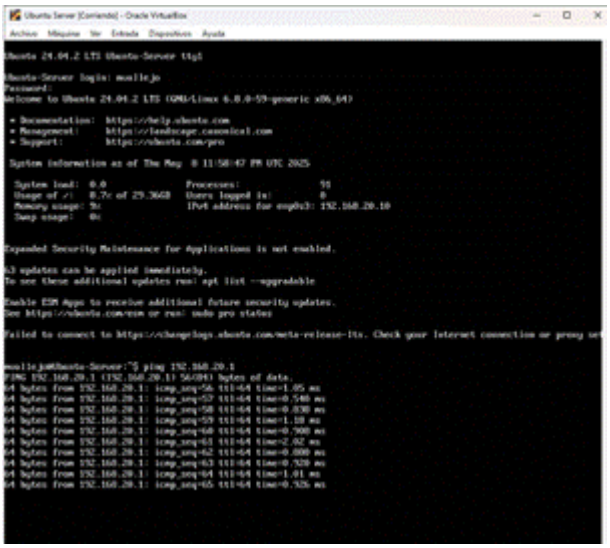

Figura 40 Monitoreo el estado del sistema y su conectividad.

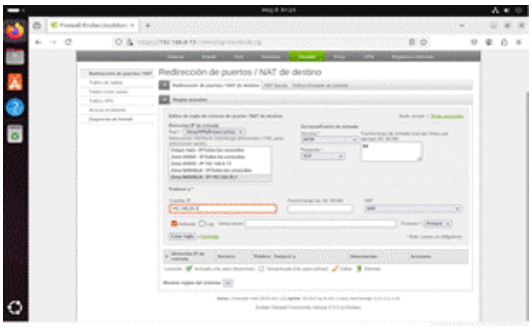

Figura 41 Configurar NAT de destino (redirección de puertos)

Figura 42 Configurando reglas para manejar tráfico entrante hacia servidores internos.

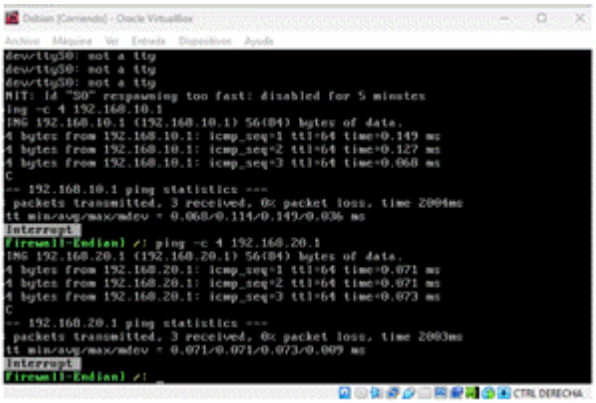

Figura 43 Probando la conexión de la red.

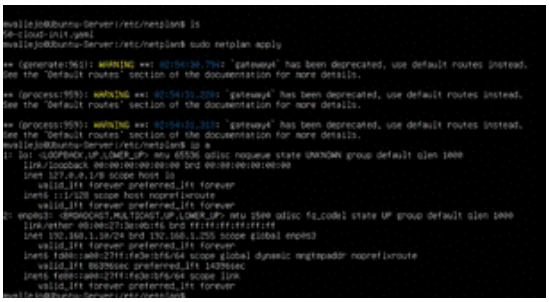

Figura 44 Configurar la red en Ubuntu Server

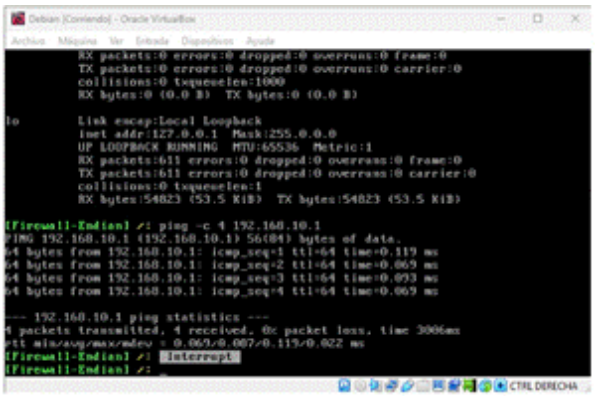

Figura 45 Monitoreando la red y validando conectividad desde el firewall Endian.

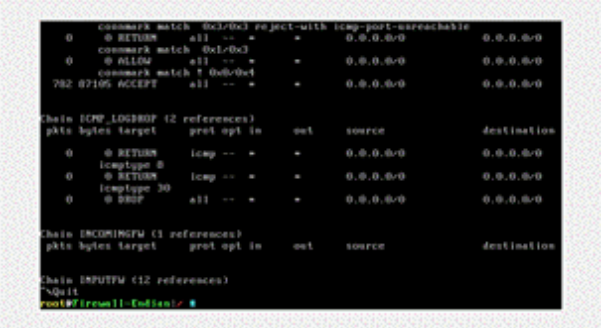

Imagen 46 Monitoreando la red y validando conectividad.

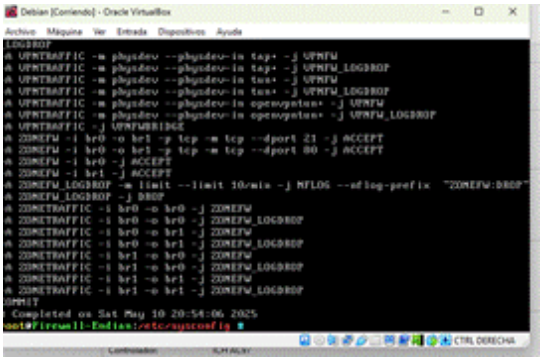

Figura 47 Validación de las reglas de filtrado de un Firewall Endian, tráfico VPN , Comunicación entre zonas (LAN - DMZ), Registro de tráfico bloqueado para seguridad.

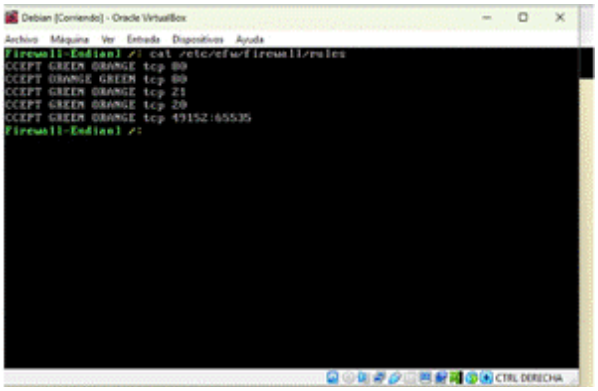

Figura 48 Se evidencia el firewall configurado, Permitir HTTP y FTP entre la LAN GREEN y la DMZ -ORANGE.

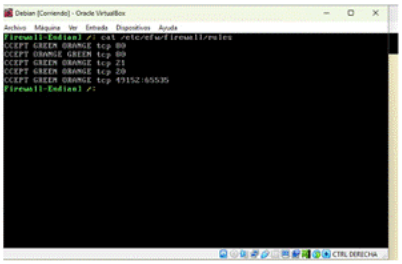

Figura 48 Se evidencia el firewall configurado, Permitir HTTP y FTP entre la LAN GREEN y la DMZ -ORANGE.

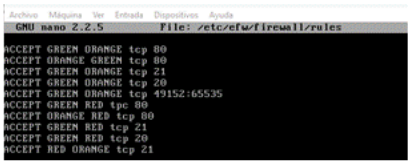

Figura 49 Evidencia donde Permite HTTP y FTP entre la LAN GREEN y la DMZ -ORANGE.

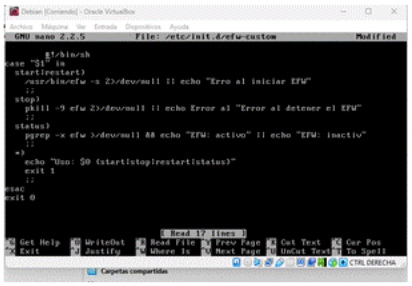

Figura 50 Se crea un script de inicio para gestionar el servicio efw (Endian Firewall).

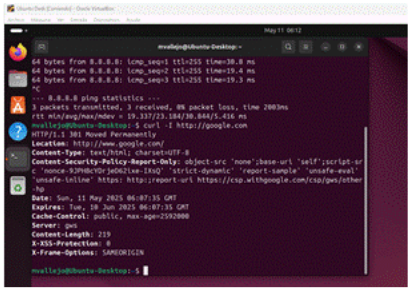

Figura 51 Ingreso del servicio HTTP desde la zona DMZ hacia la WAN

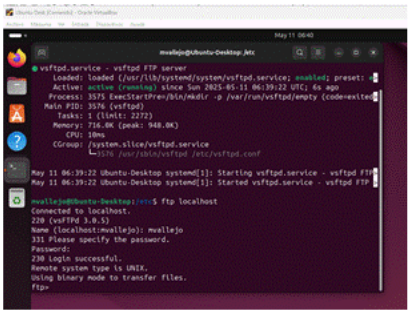

Figura 52 Comunicar la zona Verde con la zona Naranja usando FTP, el puerto 21 está en funcionamiento

En las reglas de acceso en endian firewall nos permite conectar de forma segura las zonas LAN, DMZ y WAN, siguiendo mejores prácticas de seguridad perimetral. La segmentación adecuada reduce el riesgo de ataques transversales, también permitiendo que las reglas específicas para HTTP/FTP permiten comunicaciones necesarias mientras se bloquea tráfico no autorizado.

2.2.5 TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

La implementación practica de un proxy HTTP no transparente utilizando el firewall Endian Community para aplicar navegación autenticada y filtrado de contenido en una red de área local (LAN). El estudio detalla el proceso de configuración, incluyendo la creación de un perfil de navegación asociado a una lista negra de sitios web específicos (www.hotmail.com , www.youtube.com y www.elnuevodia.com.co).

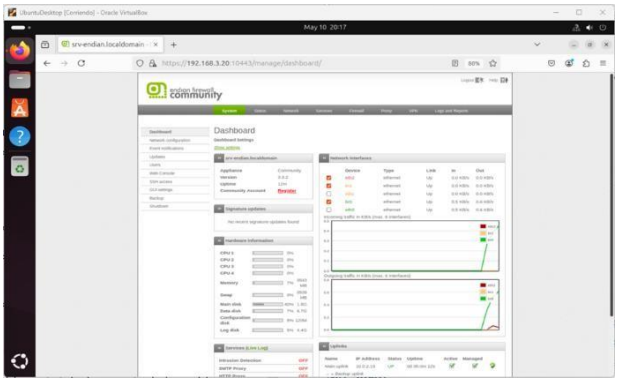

Figura 53 Accediendo al dashboard

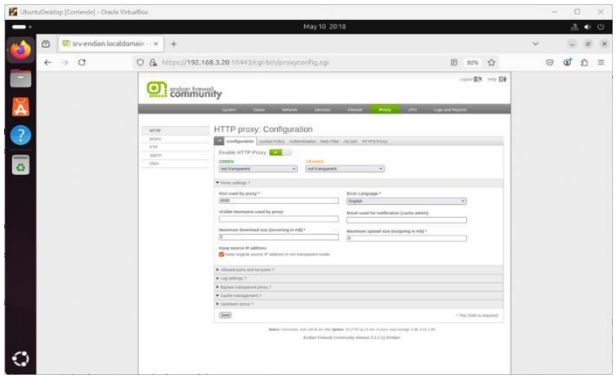

Figura 54 Habilitando el Proxy HTTP

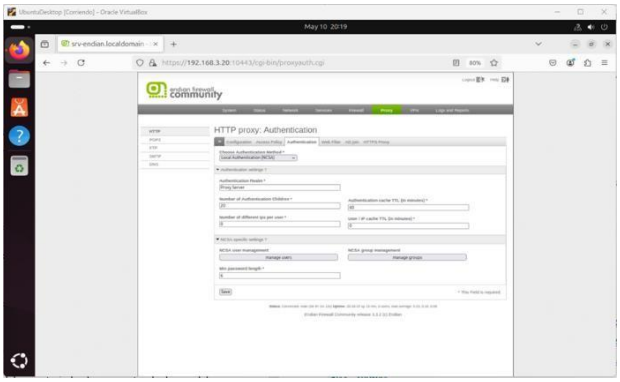

Figura 55 Habilitando autenticación local

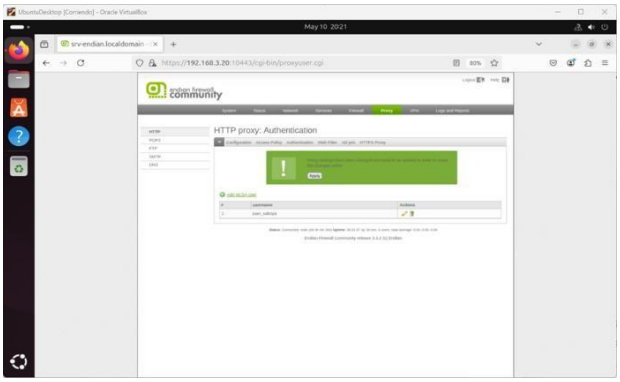

Figura 56 Creando Usuarios

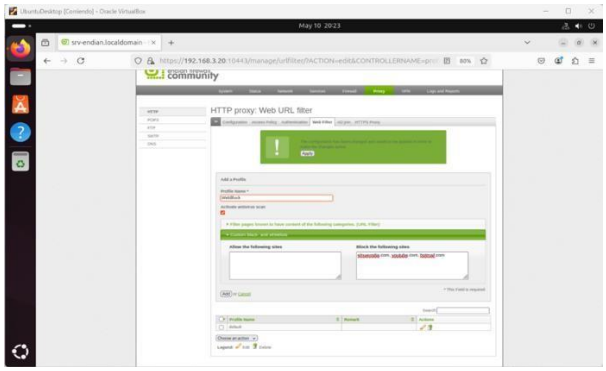

Figura 57 Creando la lista de bloquedo.

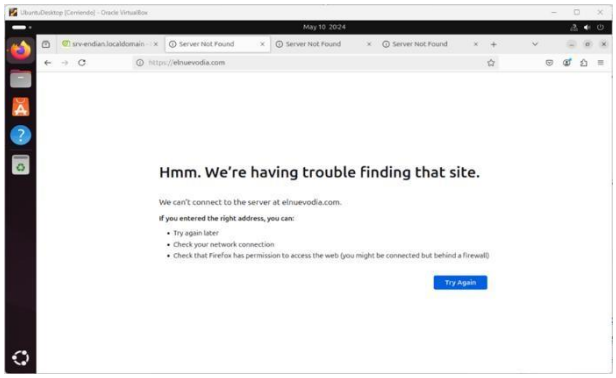

Figura 58 Bloqueando elnuevodia.com

Endian emerge como una solución robusta y flexible para implementar un control de acceso a internet granular y seguro mediante un proxy HTTP no transparente con autenticación y listas negras.

3. RECONOCIMIENTOS

Deseo expresar mi agradecimiento a la **Universidad Nacional Abierta y a Distancia**, por brindar el espacio académico y los recursos tecnológicos necesarios para el desarrollo de este proyecto. Asimismo, se agradece la orientación del tutor **Martin Camilo Cancelado Ruiz** , quien con su guía y acompañamiento permitió que cada integrante del grupo lograra avanzar en el proceso de migración e implementación de servicios bajo GNU/Linux Ubuntu Server.

4. CONCLUSIONES

La implementación de GNU/Linux Endian en un entorno virtual permitió simular un firewall funcional, segmentar una red por zonas, configurar NAT y establecer políticas de seguridad entre zonas. La integración del proxy con autenticación y filtrado de contenido refuerza el control administrativo sobre el uso de Internet. Esta práctica ofrece una base sólida para la administración de redes seguras en entornos corporativos.

5 . REFERENCIAS

[1] Endian Firewall Community, “Documentation,” [Online]. Available: https://www.endian.com/community

[2] Oracle Corporation, “VirtualBox User Manual,” [Online]. Available: https://www.virtualbox.org/manual/UserManual.html

[3] Ubuntu, “Ubuntu Server Documentation,” [Online]. Available: https://ubuntu.com/server/docs

[4] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 8th ed., Pearson, 2021.

[5] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed., Pearson, 2017.

[6] M. Thomas and K. Newby, *Mastering Proxmox*, 3rd ed., Packt Publishing, 2020. [Cap. sobre DMZ y firewall virtual]

[7] R. Perlman, C. Kaufman, and M. Speciner, *Network Security: Private Communication in a Public World*, 2nd ed., Prentice Hall, 2002.

[8] The Linux Foundation, “Linux Network Administration Guide,” [Online]. Available: https://tldp.org/LDP/nag2/index.html

[9] Mozilla, “Configuring Proxy Settings in Mozilla Firefox,” [Online]. Available: https://support.mozilla.org/en-US/kb/connection-settings-firefox

[10] M. Jang, *Linux Firewalls: Enhancing Security with nftables and Beyond*, 4th ed., Apress, 2021.