IMPLEMENTACIÓN Y CONFIGURACIÓN DE UN FIREWALL GNU/LINUX ENDIAN PARA GESTIÓN DE SEGURIDAD EN REDES LAN, DMZ Y WAN

Ingrid Liliana Jiménez Vargas
iljimenezv@unadvirtual.edu.co
Holman Eduardo Rodriguez Agudelo
herodriguezag@unadvirtual.edu.co
Pedro Antonio Córdoba Martínez
pacordobam@unadvirtual.edu.co
María José Ladino Hernández
mjladinoh@unadvirtual.edu.co
Santiago Alberto Laverde Cepeda
salaverdec@unadvirtual.edu.co

RESUMEN: *Este artículo describe el proceso de implementación, configuración y validación de un firewall basado en GNU/Linux Endian dentro de un entorno virtualizado. El objetivo principal es fortalecer la comprensión de los servicios de seguridad perimetral mediante la creación de zonas de red (LAN, WAN y DMZ), la configuración de reglas de traducción de direcciones de red (NAT), la habilitación de servicios específicos en la zona DMZ, la gestión del tráfico interzonal y la implementación de un proxy HTTP con políticas avanzadas de autenticación.*
Se presentan cinco temáticas de trabajo que abarcan desde la instalación del sistema hasta la generación de políticas de acceso, permitiendo al estudiante comprender el comportamiento del tráfico en redes segmentadas y los mecanismos de control aplicados por un firewall perimetral tipo UTM (Unified Threat Management).

PALABRAS CLAVE: Endian Firewall, DMZ, NAT, Proxy HTTP, Seguridad Perimetral, Redes, Firewall UTM.

1 INTRODUCCIÓN

La seguridad perimetral constituye un componente esencial en la administración de redes modernas. Con el crecimiento de servicios digitales, las organizaciones requieren herramientas que permitan controlar el acceso, segmentar la red y supervisar el tráfico entre zonas de confianza diferenciadas.

Endian Firewall, una distribución GNU/Linux diseñada para operar como firewall UTM, ofrece funcionalidades como NAT, proxies, filtrado de tráfico, VPN, IDS/IPS y segmentación de redes mediante zonas Verde (LAN), Roja (WAN) y Naranja (DMZ).

El presente artículo documenta el proceso de instalación y configuración de Endian Firewall en un entorno VirtualBox, así como la aplicación de políticas de seguridad asociadas a NAT, servicios en DMZ, control del tráfico interzonal y autenticación mediante proxy web. Las actividades realizadas permiten comprender cómo se gestiona la comunicación entre segmentos de red y cómo se aplican las reglas de seguridad que garantizan un uso adecuado de los servicios.

2 MARCO TEÓRICO

2.1 SEGMENTACIÓN DE REDES: LAN, DMZ y WAN

La segmentación de red permite separar niveles de confianza. La zona LAN (verde) posee el mayor nivel de acceso; la DMZ (naranja) contiene servidores expuestos; y la WAN (roja) corresponde al acceso público.

2.2 NAT Y SEGURIDAD PERIMETRAL

NAT (Network Address Translation) traduce direcciones privadas a públicas y viceversa, permitiendo el acceso a Internet y la publicación de servicios en la DMZ mediante Port Forwarding.

2.3 PROXIES Y AUTENTICACIÓN

Un proxy HTTP no transparente actúa como intermediario entre el cliente y el servidor web. Puede aplicar políticas, filtrar contenido y requerir credenciales para acceder a Internet.

3 METODOLOGÍA

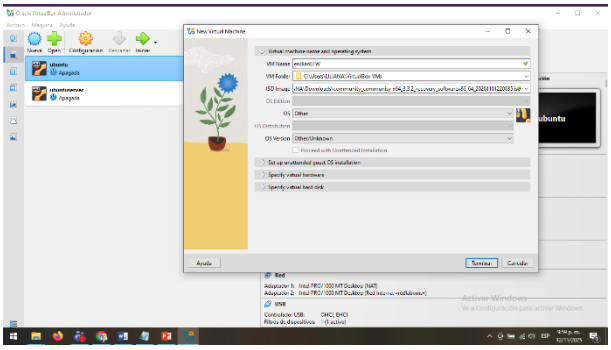
3.1 Temática 1: Configuración de la instancia para GNU/Linux Endian en VirtualBox (tarjetas de red) e instalación efectiva del mismo.

La segmentación de redes constituye una práctica fundamental en la implementación de arquitecturas de seguridad perimetral. Endian Firewall, basado en GNU/Linux, proporciona una solución robusta para la gestión de zonas de red diferenciadas, permitiendo establecer políticas de seguridad específicas para cada segmento.

Configuración de la Instancia de Endian en VirtualBox

Se descargó la imagen ISO de Endian Firewall desde el repositorio oficial en SourceForge: https://sourceforge.net/projects/efw/

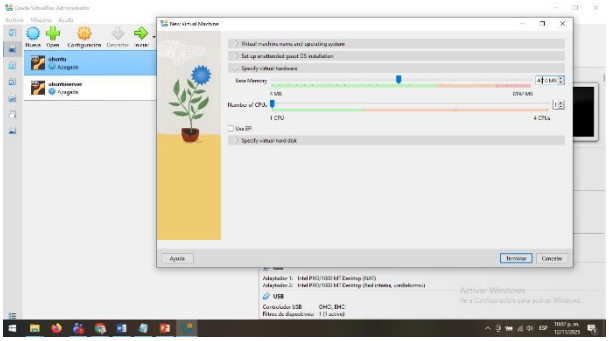
Una vez completada la descarga, se procedió a crear una nueva máquina virtual en VirtualBox. Se asignó un nombre a la máquina y se seleccionó el archivo ISO descargado previamente.



Fuente: Autoría Propia

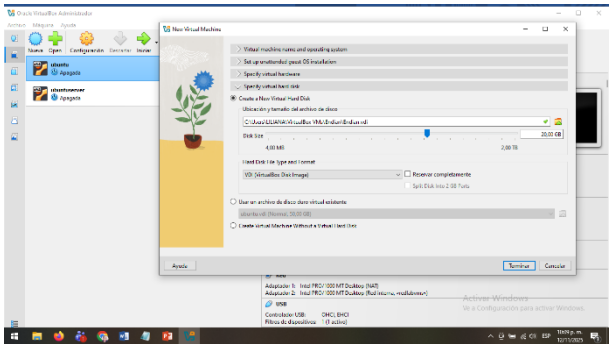
Especificaciones de Hardware

Se configuraron las especificaciones de hardware asignando 4010 MB de memoria RAM a la máquina virtual.



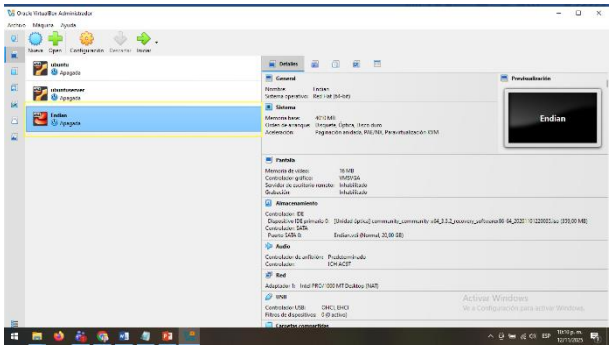
Fuente: Autoría Propia

Para el disco duro, se mantuvo la configuración recomendada por defecto.



Fuente: Autoría Propia

Una vez completada la configuración inicial, la nueva máquina virtual quedó creada y lista para configurar los adaptadores de red.

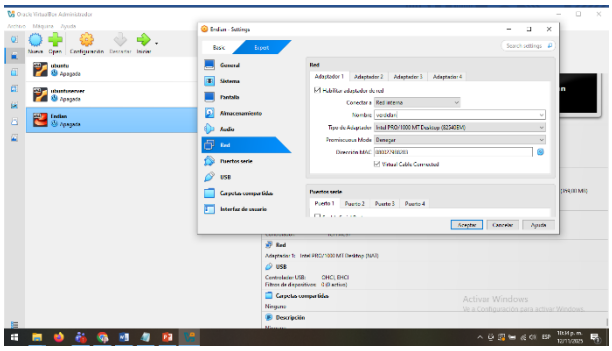


Fuente: Autoría Propia

Configuración de Adaptadores de Red

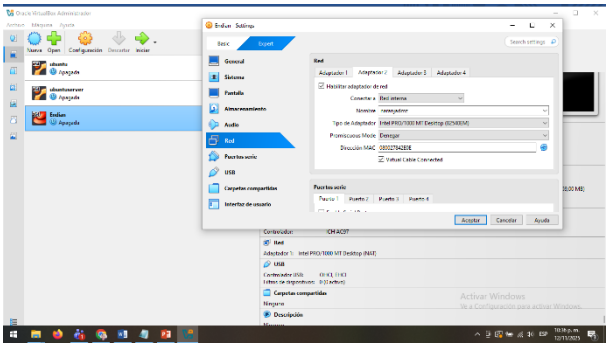
Se accedió a la configuración de la máquina virtual de Endian para establecer los tres adaptadores de red necesarios: Adaptador 1 - Zona Verde (GREEN/LAN):

Se configuró como red interna con el nombre "verderlan"



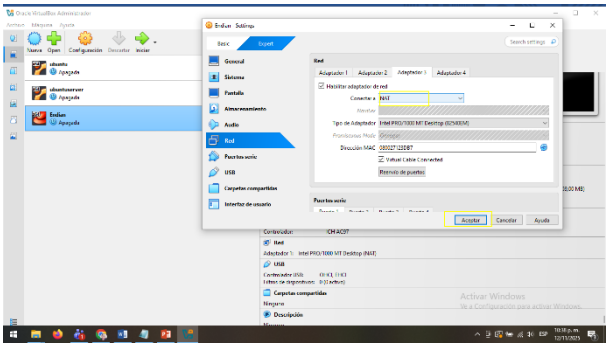
Fuente: Autoría Propia

Adaptador2 - Zona Naranja (ORANGE/DMZ):
Se configuró como red interna con el nombre "naranjadmz".



Fuente: Autoría Propia

Adaptador 3 - Zona Roja (RED/WAN):
Se configuró en modo NAT sin nombre específico.

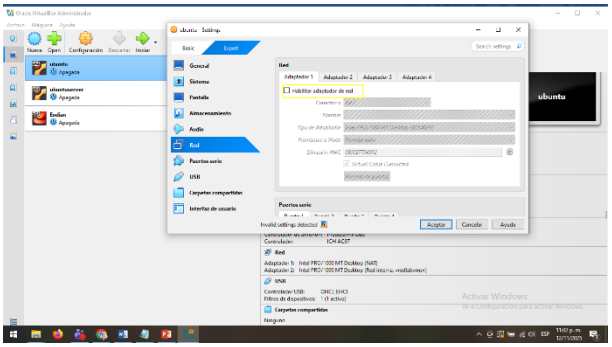


Fuente: Autoría Propia

Preparación de Máquinas Ubuntu

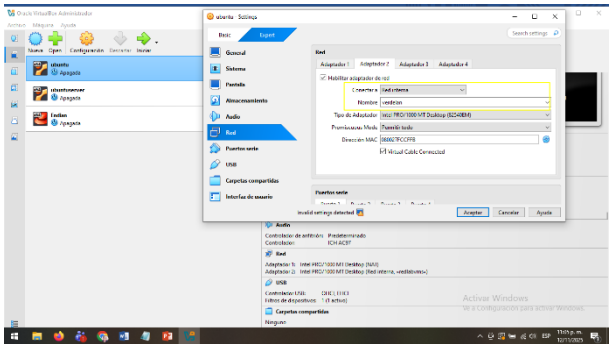
Ubuntu Desktop: Se inició la máquina Ubuntu Desktop y se ejecutó el comando apt update && apt upgrade para actualizar el sistema.

Posteriormente, se apagó la máquina para reconfigurar sus adaptadores de red. Se deshabilitó el Adaptador 1 y se habilitó el Adaptador 2.



Fuente: Autoría Propia

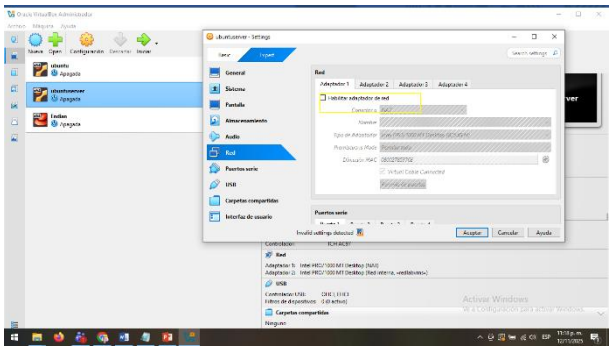
El Adaptador 2 se configuró como red interna con el nombre "verderlan" para conectarlo a la zona verde.



Fuente: Autoría Propia

Ubuntu Server: Se inició la máquina Ubuntu Server y se ejecutó sudo apt update && sudo apt upgrade.

Una vez actualizado el sistema, se apagó la máquina y se reconfiguró el adaptador de red. Se deshabilitó el Adaptador 1 y se configuró el Adaptador 2.

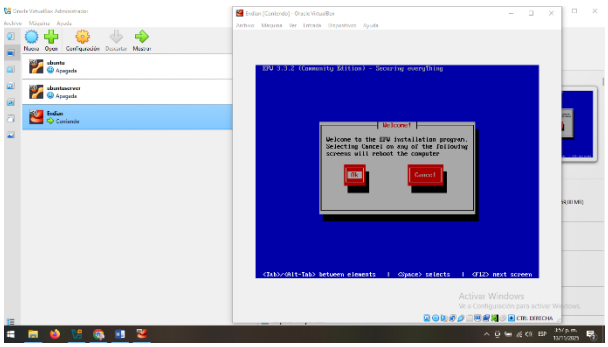


Fuente: Autoría Propia

El Adaptador 2 se configuró como red interna con el nombre "naranjadmz" para conectarlo a la zona DMZ.

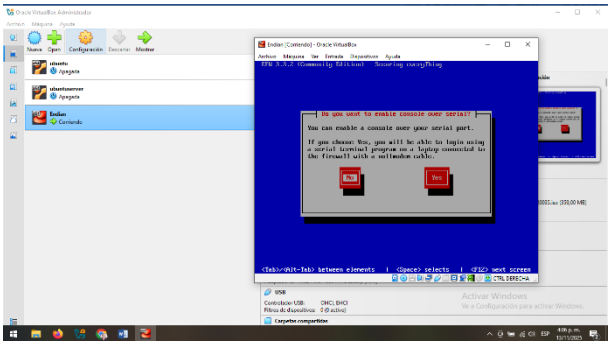
Proceso de Instalación Endian Firewall

Se inició la máquina virtual de Endian y se seleccionó el idioma. En la pantalla inicial se presionó Enter para confirmar.



Fuente: Autoría Propia

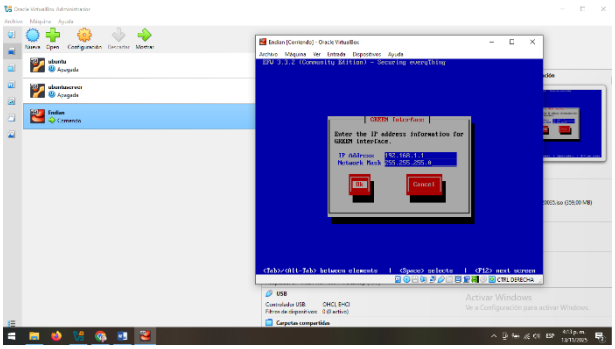
El sistema procedió a particionar el disco e instalar los paquetes necesarios. Durante el proceso se seleccionó "Yes" para continuar. La máquina se reinicia automáticamente.



Fuente: Autoría Propia

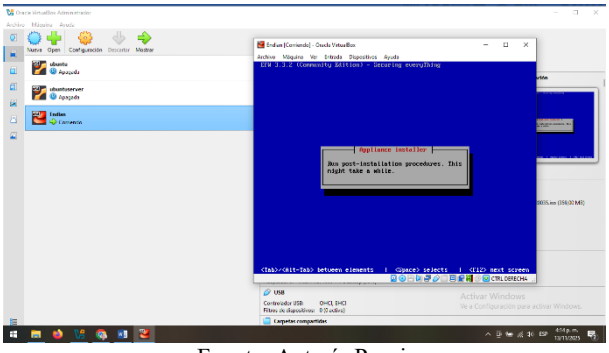
Configuración de la Interfaz Verde

En la siguiente ventana se configuró la dirección IP para la interfaz verde (GREEN): 192.168.1.1 con su máscara de red correspondiente.



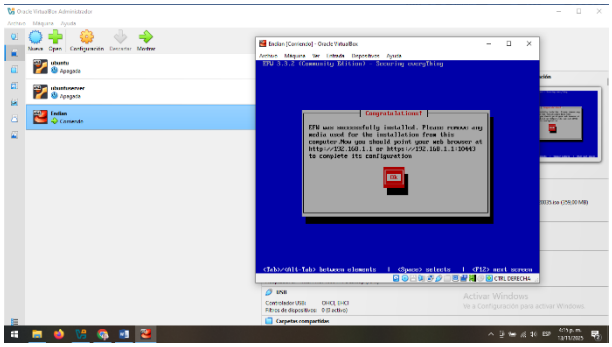
Fuente: Autoría Propia

El sistema continuó con la instalación durante algunos minutos.



Fuente: Autoría Propia

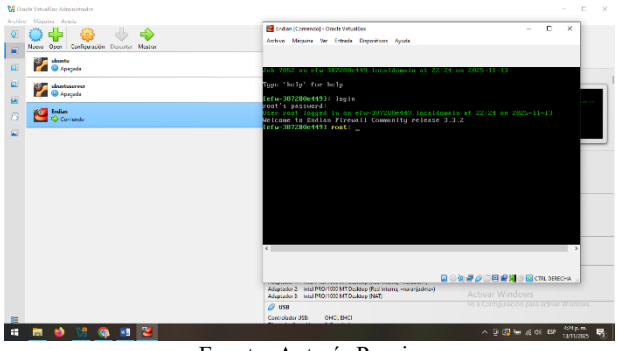
Al finalizar, apareció un mensaje confirmando que la instalación fue exitosa y que el sistema EFW estaba funcionando correctamente.



Fuente: Autoría Propia

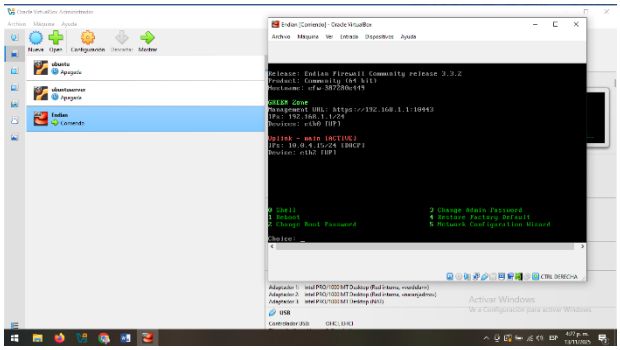
Configuración Inicial del Sistema

Tras el reinicio, se presionó la tecla 0 para acceder al sistema. Se ingresaron las credenciales predeterminadas: usuario "login" y contraseña "endian".



Fuente: Autoría Propia

"exit" para salir del Shell. El sistema mostró la configuración actual donde se confirmó que la zona verde quedó configurada con la IP 192.168.1.1/24, y la zona roja (NAT) obtuvo automáticamente la IP 10.0.4.15/24 mediante DHCP.

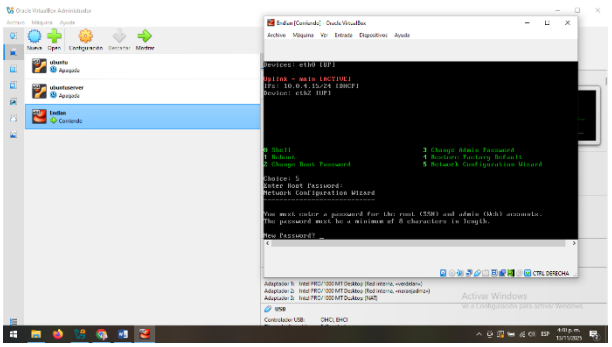


Fuente: Autoría Propia

Configuración de Contraseña y Zonas

Se seleccionó la opción 5 del menú principal e ingresó la contraseña actual "endian". El sistema solicitó establecer una nueva contraseña de administración.

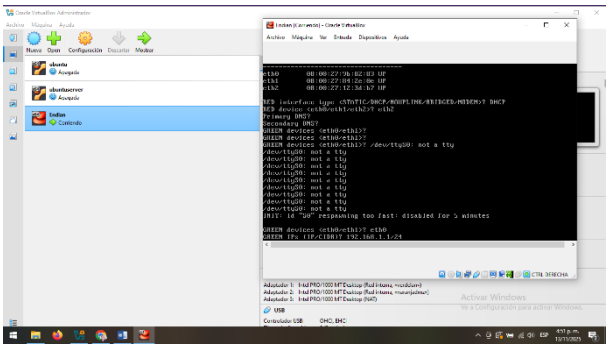
Se estableció la nueva contraseña: 1q2w3e$r



Fuente: Autoría Propia

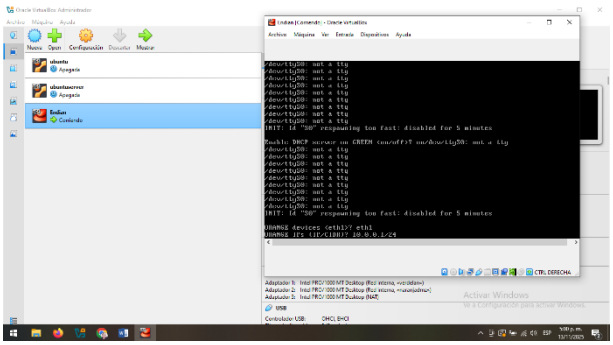
El sistema tomó algunos valores de configuración por defecto.

Cuando el sistema solicitó "GREEN devices <eth0/eth1>?", se escribió eth0. A continuación, se confirmó la IP para la zona verde: 192.168.1.1/24.



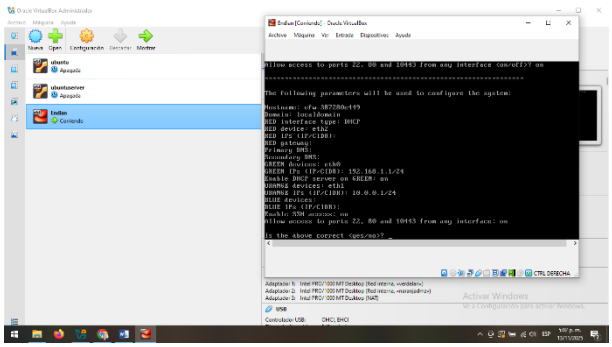
Fuente: Autoría Propia

Para la zona naranja, ¿cuándo solicitó “ORANGE devices <eth1>?", se escribió eth1 y se asignó manualmente la IP 10.0.0.1/24.



Fuente: Autoría Propia

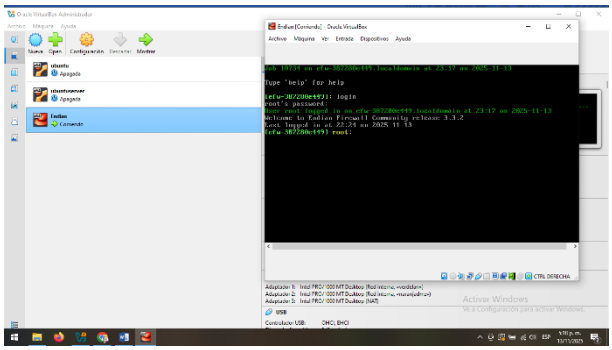
Cuando solicitó "BLUE devices", se presionó Enter sin asignar ningún valor. Finalmente, se mostró la configuración completa y se escribió "yes" para confirmar.



Fuente: Autoría Propia

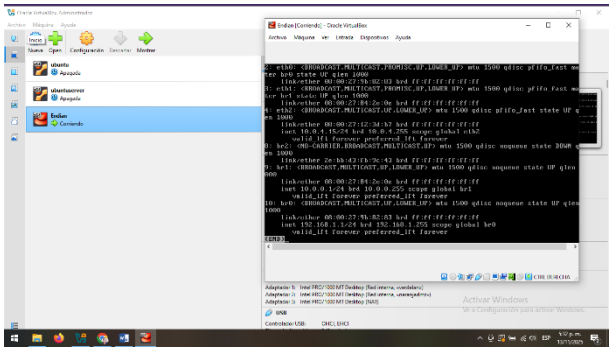
Validación de la Configuración de Endian

Para verificar la configuración, se seleccionó la opción 0 del menú para acceder al Shell. Se ingresaron las credenciales: usuario "login" y la contraseña configurada previamente (1q2w3e$r), lo que permitió acceder con privilegios de administrador (root).



Fuente: Autoría Propia

Se ejecutó el comando ip a | less para verificar la configuración de red. Se confirmó que Endian creó correctamente los bridges br0, br1 y br2 para gestionar las diferentes zonas.



Fuente: Autoría Propia

Configuración final de zonas:

Zona	Interfaz	Ip
GREEN (LAN)	br0	192.168.1.1
ORANGE (DMZ)	br1	10.0.0.1/24
RED (WAN)	eth2	10.0.4.15/24

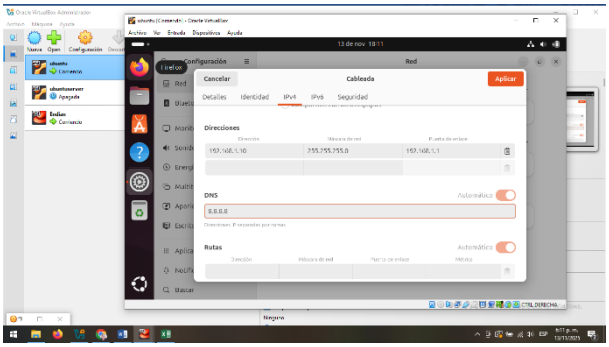
Configuración de Ubuntu Desktop (Zona Verde)

Esta máquina se conecta a través de la red 192.168.1.0/24, por lo que requiere configuración manual de red.

Se inició la máquina Ubuntu Desktop y se verificó que detectara la red cableada configurada. Se hizo clic en el ícono de configuración.

En la pestaña IPv4 se estableció el modo manual con los siguientes parámetros

Dirección: 192.168.1.10
Máscara de red: 255.255.255.0
Puerta de enlace: 192.168.1.1
DNS: 8.8.8.8



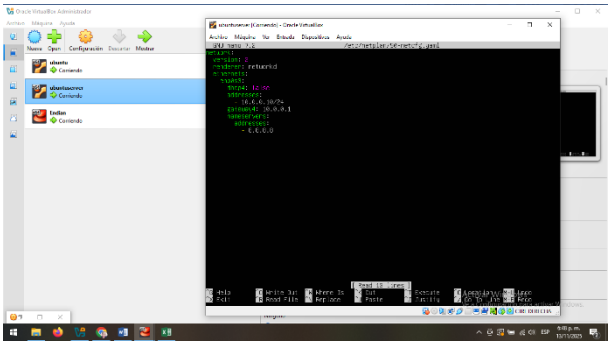
Fuente: Autoría Propia

Se abrió una terminal y se ejecutó un ping a la zona verde de Endian (192.168.1.1) para verificar la conectividad.

Configuración de Ubuntu Server (Zona Naranja)

Esta máquina se conecta a la DMZ con la red 10.0.0.0/24.

Se inició la máquina y se editó el archivo de configuración de red con el comando sudo nano /etc/netplan/*.yaml



Fuente: Autoría Propia

Se aplicó la configuración ejecutando sudo netplan apply.

Resolución de Problemas de Conectividad

Al intentar hacer ping a 10.0.0.1, no se estableció conexión inicialmente. Para resolver este problema, se apagó la máquina y se modificó la configuración del adaptador en VirtualBox:

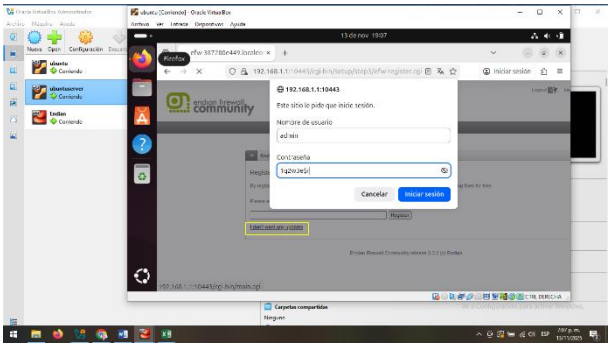
Se habilitó el Adaptador 1 y se configuró como red interna con el nombre "naranjadmz" y Se deshabilitó el Adaptador 2.

Tras reiniciar la máquina con esta nueva configuración, se ejecutó nuevamente el ping a 10.0.0.1, confirmando que la conexión con la zona naranja funcionaba correctamente.

Acceso al Panel de Administración de Endian

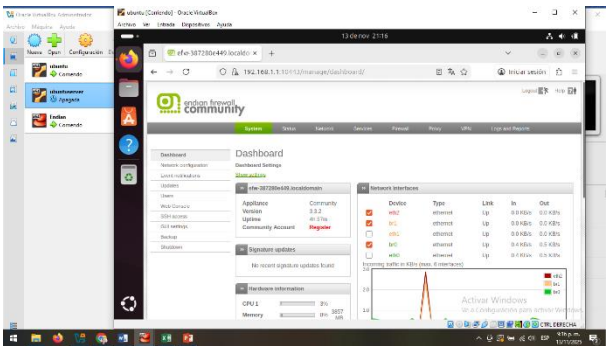
Desde Ubuntu Desktop se abrió un navegador web y se ingresó a la URL: https://192.168.1.1:10443

Al acceder, se hizo clic en "No quiero ninguna actualización". Posteriormente apareció una pantalla de login donde se ingresaron las credenciales: usuario "admin" y contraseña "1q2w3e$r" (configurada durante la instalación), finalmente se hizo clic en iniciar sesión.



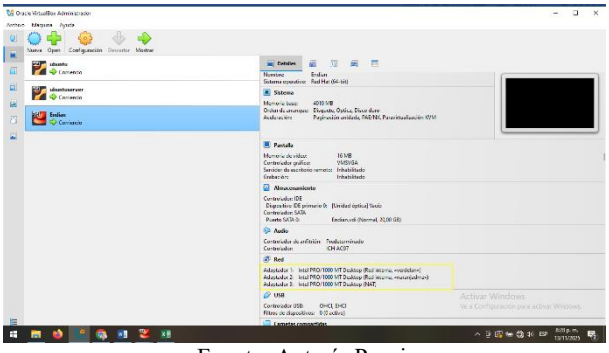
Fuente: Autoría Propia

Se accedió exitosamente al panel principal de administración de Endian.



Fuente: Autoría Propia

A continuación, en el panel muestra la configuración completa de red de Endian Firewall.



Fuente: Autoría Propia

3.2 Temática 2: Configuración NAT.

Previamente configurada la **Temática 1**, continuamos con el desarrollo de la temática seleccionada.

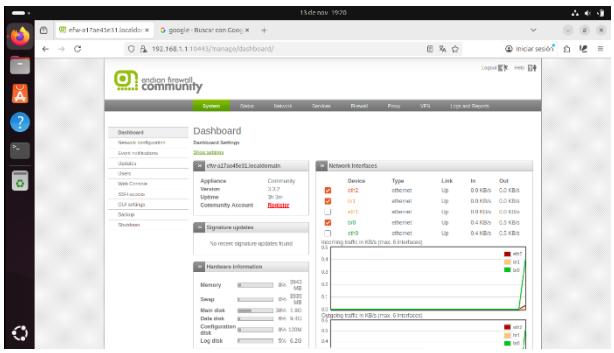
Ubuntu Desktop (LAN)

Inicio la máquina de Ubuntu Desktop, Accedo al navegador y escribo la siguiente dirección **URL** para entrar al panel web de **Endian**. **https://192.168.1.1:10443**

Damos clic en el enlace **I don't want any updates**

Probablemente nos pide iniciar sesión entonces el usuario admin y el password que configuramos anteriormente.

Si no nos pide credenciales nos carga inmediatamente el **Dashboard** del panel web de **Endian**.



Fuente: Autoría Propia

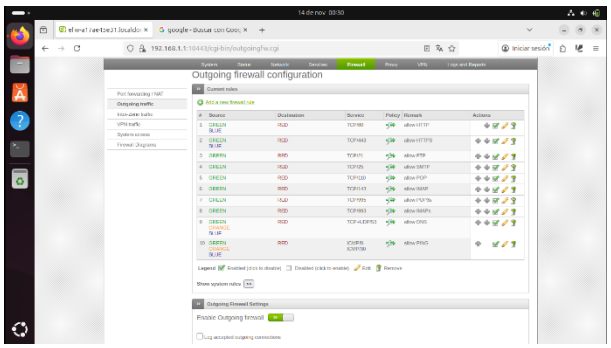
Voy a Habilitar NAT para la LAN (GREEN – RED)

En el panel de Endian voy a **Firewall – Outgoing traffic**

Voy a habilitar las filas que tengo, ya que cada fila permite activar o desactivar el tráfico saliente.

Buscamos y verificamos que las filas que digan **GREEN – RED** estén habilitadas. Sino están habilitadas, las habilitamos y guardamos los cambios.

Cada fila permite activar o desactivar el tráfico saliente.

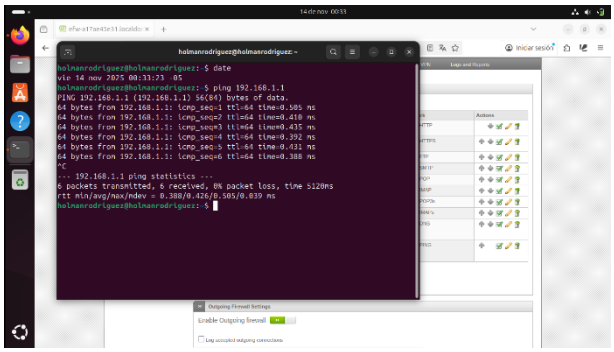


Fuente: Autoría Propia

Ahora voy a probar desde **Ubuntu Desktop (LAN)**

Voy a ejecutar los siguientes comandos.

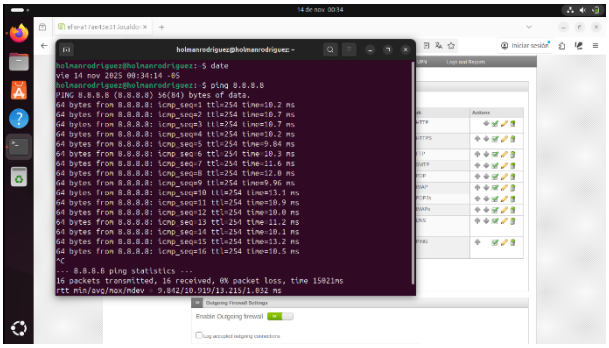
date
ping 192.168.1.1



Fuente: Autoría Propia

Ping establecido correctamente a **192.168.1.1**

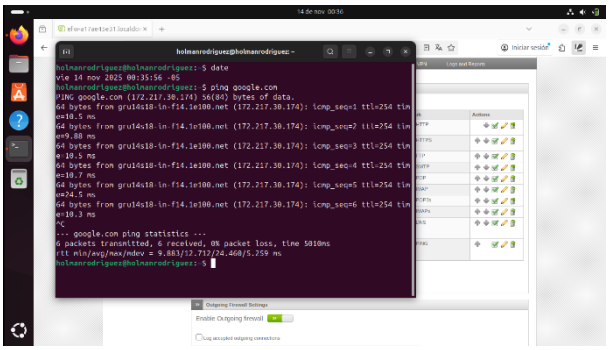
ping 8.8.8.8



Fuente: Autoría Propia

Ping establecido correctamente a **8.8.8.8**

ping google.com



Fuente: Autoría Propia

Ping establecido correctamente a **google.com**. **NAT** para **LAN** funciona correctamente.

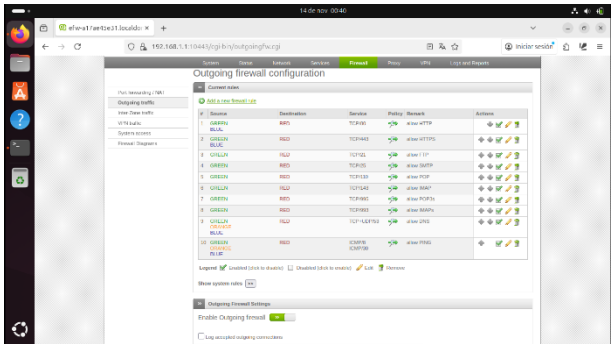
Configuración de NAT para DMZ (ORANGE – RED)

En el panel de Endian voy a **Firewall – Outgoing traffic**

Voy habilitar las filas que tengo, ya que cada fila permite activar o desactivar el tráfico saliente.

Buscamos y verificamos que las filas que digan **ORANGE – RED** estén habilitadas. Sino están habilitadas, las habilitamos y guardamos los cambios.

Esto permite que los servidores de la **DMZ** salgan al Internet simulado.

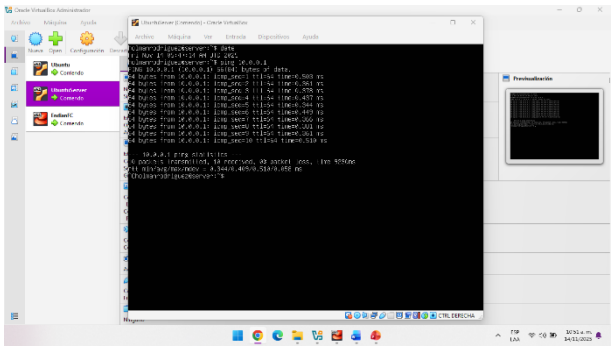


Fuente: Autoría Propia

Ahora voy a probar desde el **Ubuntu Server DMZ**

Ejecuto los siguientes comandos.

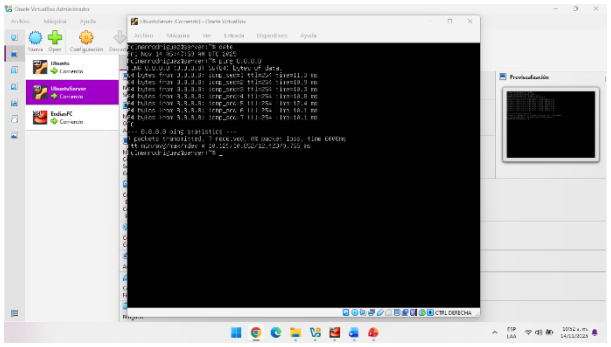
date
ping 10.0.0.1



Fuente: Autoría Propia

Ping establecido correctamente a **10.0.0.1**

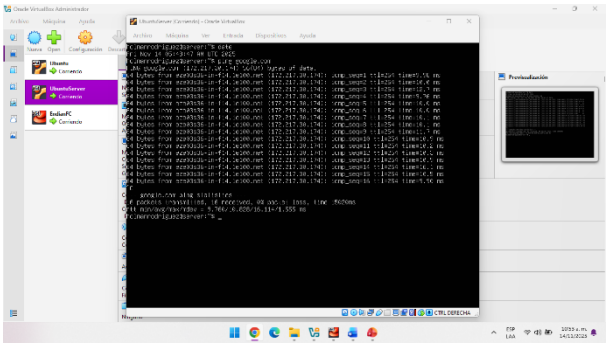
ping 8.8.8.8



Fuente: Autoría Propia

Ping establecido correctamente a **8.8.8.8**

ping google.com



Fuente: Autoría Propia

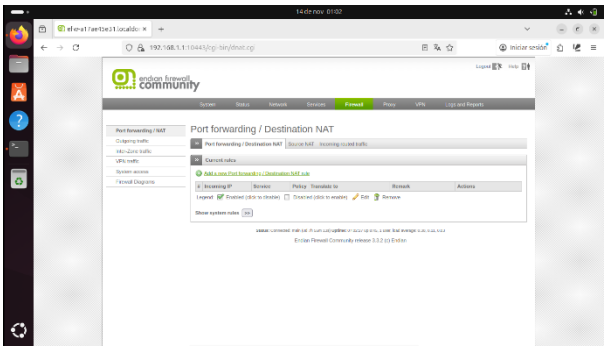
Ping establecido correctamente a **google.com**. **NAT** para **DMZ** funciona correctamente.

Ahora vamos a crear la regla de reenvío de puertos.

Port Forwarding / NAT

En Ubuntu Desktop voy al portal web de Endian

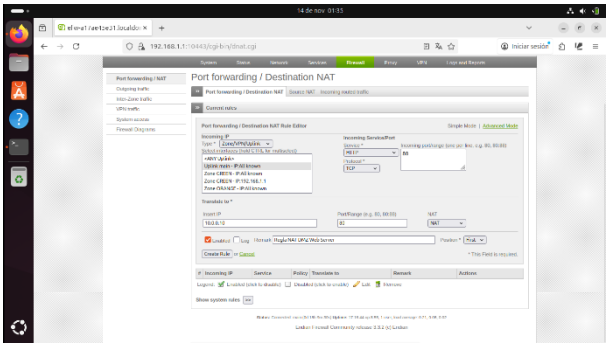
Voy a **Firewall → Port forwarding / NAT**



Fuente: Autoría Propia

Voy a agregar una nueva regla en **Add a new Port forwarding / Destination NAT rule**

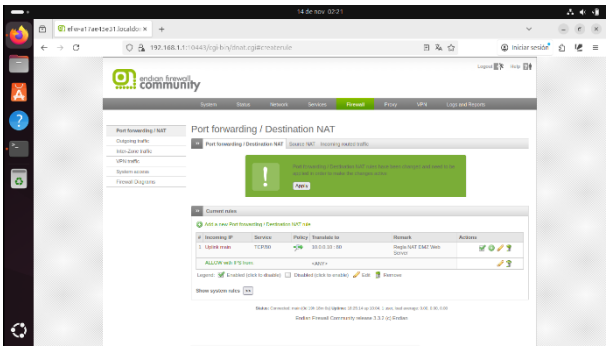
Modificamos los campos con la siguiente información.



Fuente: Autoría Propia

Type	Uplink main – IP:All known
Service	HTTP
Protocol	TCP
Incoming port/range	80
Insert IP	10.0.0.10
Port/Range	80
NAT	NAT
Enabled	True
Remark	Regla NAT DMZ Web Server
Position	First

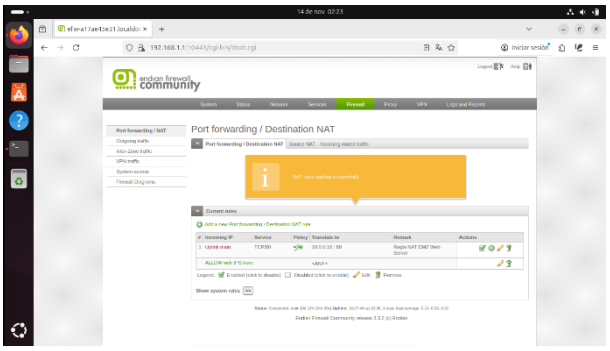
Al dar clic en el botón Crear regla nos muestra la siguiente ventana.



Fuente: Autoría Propia

Nos dice "Las reglas de reenvío de puertos NAT de destino se han modificado y deben aplicarse para que los cambios surtan efecto"

Damos clic en el botón **Apply**



Fuente: Autoría Propia

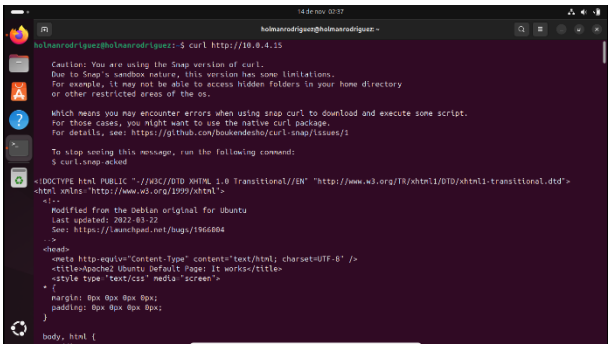
Las reglas NAT han sido aplicadas correctamente. Podemos ver el registro creado con la nueva regla que configuramos.

Ahora voy a validar la regla **Port Forwarding** desde **LAN**

En **Ubuntu Desktop**

Voy a probar acceso al servidor web a través del Endian

Ejecutar en **Ubuntu Desktop** el siguiente comando curl **http://10.0.4.15**



Fuente: Autoría Propia

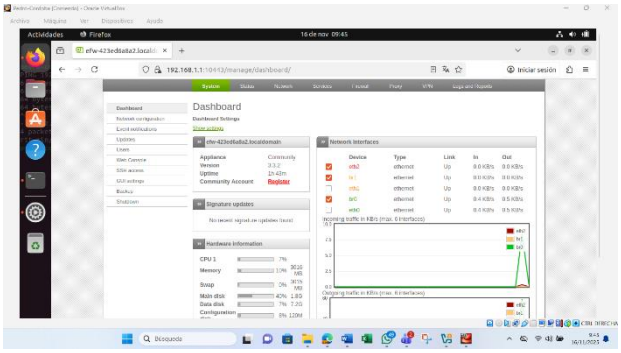
Como podemos ver nos aparece la página de **Apache del Ubuntu Server (HTML).**

Si esto pasa **NAT / Port forwarding** está funcionando correctamente.

3.3 Temática 3: Permitir servicios de la Zona DMZ para la red.

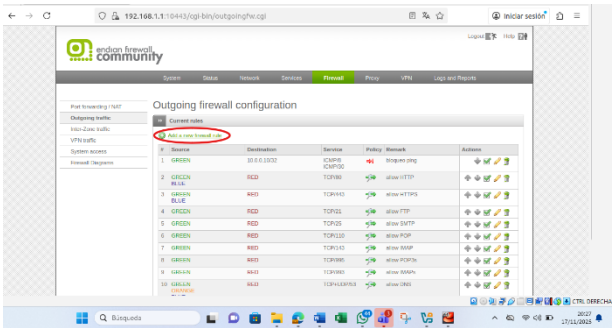
Configurar el firewall Endian para permitir el acceso a los servicios HTTP (puerto 80) y FTP (puerto 21) desde la zona GREEN hacia el servidor ubicado en la zona DMZ (ORANGE), y bloquear el protocolo ICMP para evitar diagnósticos mediante ping

Se inicia la máquina virtual de Ubuntu Desktop, para acceder desde el navegador al Dashboard de Endian con la información Generada anteriormente.



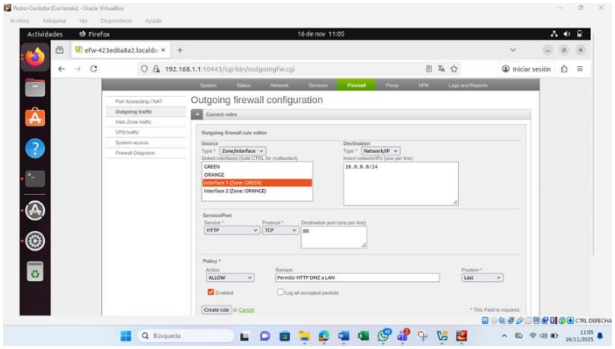
Fuente: Autoría Propia

Se procede a configurar las reglas. Siguiendo la ruta Firewall → Outgoing Traffic → Add a new rule



Fuente: Autoría Propia

Se crea la regla para permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server.

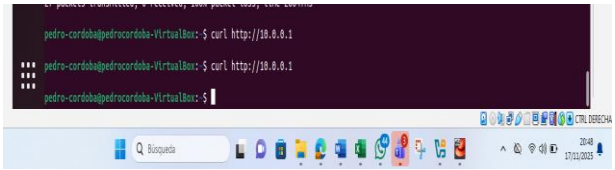


Fuente: Autoría Propia

Luego de terminar la configuración y establecer la regla se guarda y crea la nueva regla, a continuación, saldrá el siguiente cuadro de dialogo donde se debe seleccionar apply para que los cambios se apliquen.

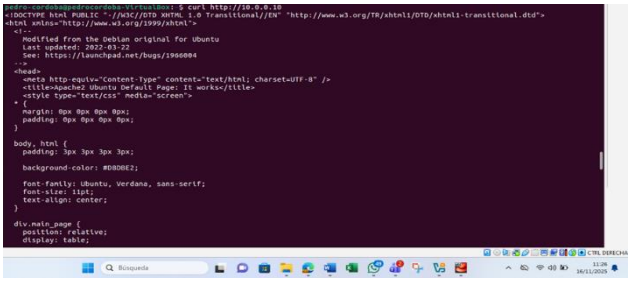
Fuente: Autoría Propia

Antes de guardar y aplicar las reglas verificamos con algunos comandos las reglas creadas.
Verificar con el comando curl http://10.0.0.10 donde se ve reflejado que no hay respuesta alguna antes de activar la regla.



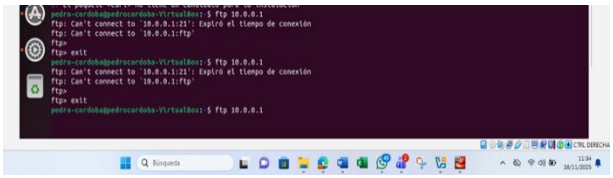
Fuente: Autoría Propia

Nuevamente se verifica con el comando curl http://10.0.0.10 se verá reflejado que se aplicó la regla y hay respuesta positiva enseñando el, índex de server.



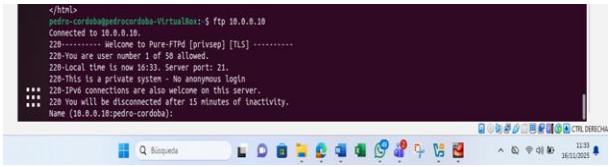
Fuente: Autoría Propia

Esto es lo que debe aparecer antes de crear la regla para permitir los servicios FTP (Puerto 21), no se obtiene respuesta mediante el comando ftp 10.0.0.10.



Fuente: Autoría Propia

Aplicando la regla ejecutamos el comando ftp 10.0.0.10.

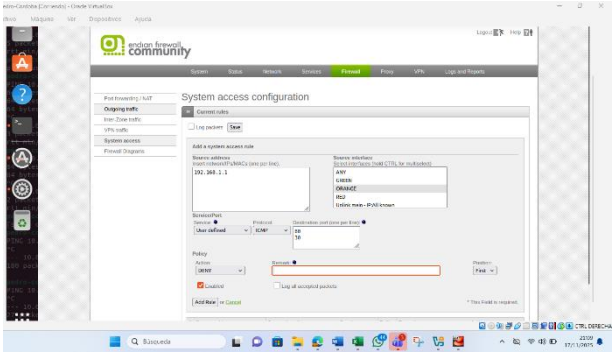


Fuente: Autoría Propia

Continuamos con Denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red.

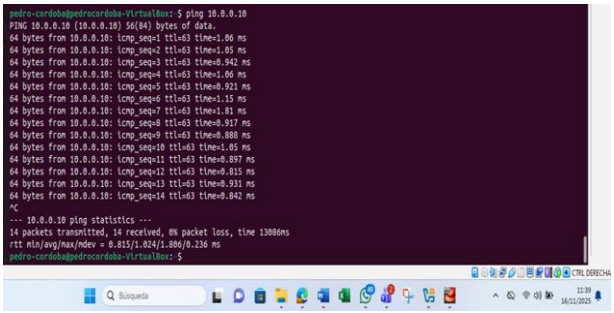
Creamos la nueva regla teniendo en cuenta que Endian muestra ICMP/8 y ICMP/30 automáticamente, pero no permite bloquear por tipo. La regla debe bloquear todo el protocolo ICMP, sin especificar puertos.

para estos seguimos la en la página de endian Ruta: Firewall → System Access → Add new system access rule



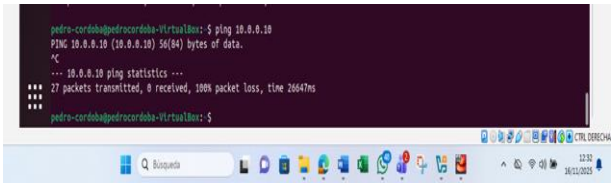
Fuente: Autoría Propia

Verificamos que este realizando ping antes de ejecutar la nueva regla mediante el comando ping 10.0.0.10 desde Ubuntu desktop a server (Naranja)



Fuente: Autoría Propia

Verificamos que ya no realice ping después de ejecutar la nueva regla mediante el comando ping 10.0.0.10 desde Ubuntu desktop (Green) a server (Naranja)



Fuente: Autoría Propia

Se configuraron reglas en Endian Firewall para permitir el acceso a los servicios HTTP y FTP desde la zona GREEN hacia el servidor en la zona DMZ (ORANGE), y se bloqueó el protocolo ICMP para evitar diagnósticos mediante ping. Las pruebas técnicas confirmaron que los servicios funcionan correctamente y que el tráfico ICMP fue bloqueado, cumpliendo con los objetivos de la temática 3.

3.4 Temática 4: Reglas de acceso para permitir o denegar el tráfico.

En esta temática se configuraron las reglas necesarias en Endian Firewall para permitir y denegar tráfico entre las zonas GREEN (LAN), ORANGE (DMZ) y RED (WAN), garantizando un control perimetral adecuado según los servicios autorizados.

Configuración de reglas GREEN → ORANGE (HTTP y FTP)

Se accedió al panel web de Endian en la ruta: Firewall → Inter-Zone Traffic → Add a new inter-zone rule

Se crearon las siguientes reglas:

Regla 1 – HTTP (puerto 80)

Source zone: GREEN

Destination zone: ORANGE

Service: HTTP (TCP/80)

Policy: Allow

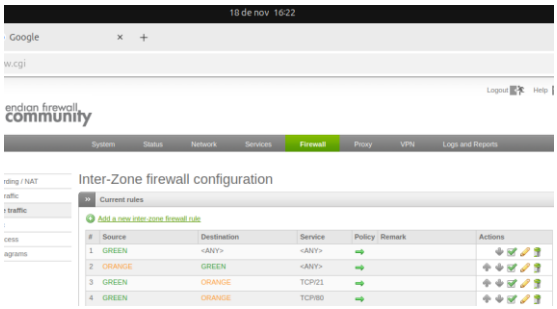
Regla 2 – FTP (puerto 21)

Source zone: GREEN

Destination zone: ORANGE

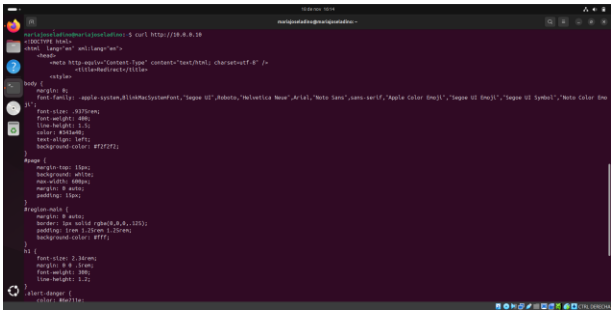
Service: FTP (TCP/21)

Policy: Allow



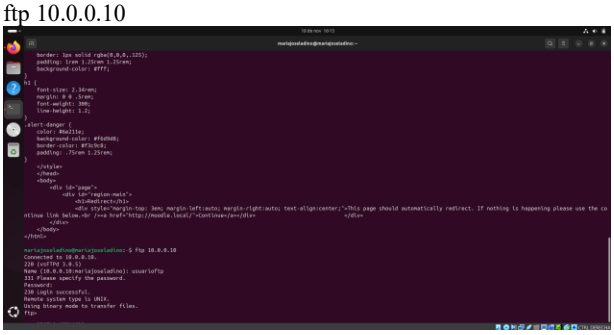
Tras crear ambas reglas, se aplicaron los cambios. Las pruebas desde Ubuntu Desktop mediante:

curl http://10.0.0.10



Fuente: Autoría Propia

ftp 10.0.0.10



Fuente: Autoría Propia

confirmaron la comunicación correcta hacia el servidor DMZ.
Comunicación RED → ORANGE (Acceso desde Internet simulado)

Para permitir el acceso desde la zona RED (WAN) hacia los servicios en la DMZ, se configuraron reglas de Port Forwarding / Destination NAT en: Firewall → Port forwarding / Destination NAT → Add new rule

Ejemplo de configuración para HTTP:

Source: RED

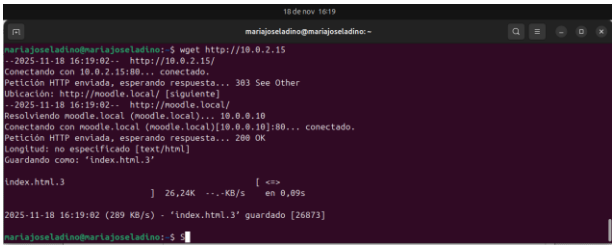
Destination: ORANGE

Service: HTTP (TCP/80)

Action: NAT / Port Forwarding

Insert IP: 10.0.0.10 (Servidor Web DMZ)

Aplicados los cambios, se probó el acceso desde la WAN usando:
wget http://10.0.2.15



Fuente: Autoría Propia

lo cual confirmó la correcta traducción de puertos.
Verificación en el módulo Inter-Zone Traffic

En el panel de Endian, se verificó que las reglas creadas aparecieran activas dentro del módulo Inter-Zone Traffic, validando que las políticas GREEN→ORANGE y RED→ORANGE se encontraban habilitadas.

Pruebas desde navegador Web

Se realizaron las siguientes pruebas:

HTTP desde LAN → DMZ: acceso exitoso al servidor web en 10.0.0.10.

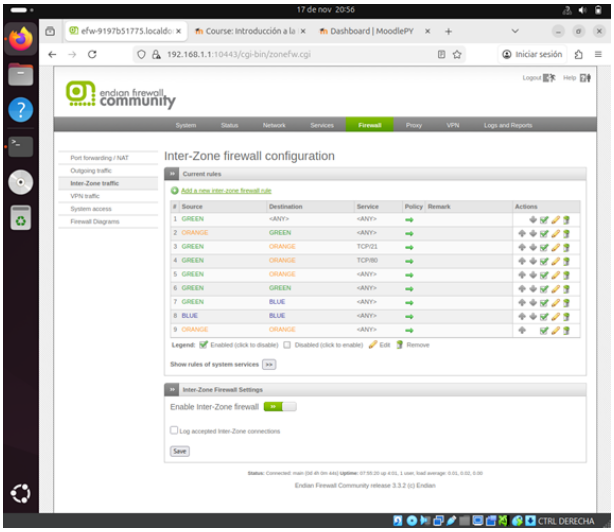
HTTP desde LAN → WAN: conectividad a Internet simulada validada mediante navegadores.

HTTP desde DMZ → WAN: servidor DMZ pudo acceder a Internet vía NAT.

HTTP desde WAN → DMZ: acceso correcto al servidor web mediante DNAT.

FTP desde LAN → WAN: conexión permitida según política configurada.

FTP desde WAN → DMZ: acceso permitido siguiendo la regla de NAT.



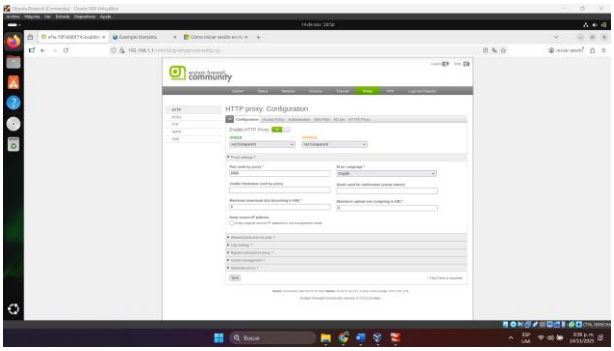
Fuente: Autoría Propia

Estas pruebas confirmaron que el firewall procesa adecuadamente las reglas de acceso entre zonas, respetando los servicios configurados.

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

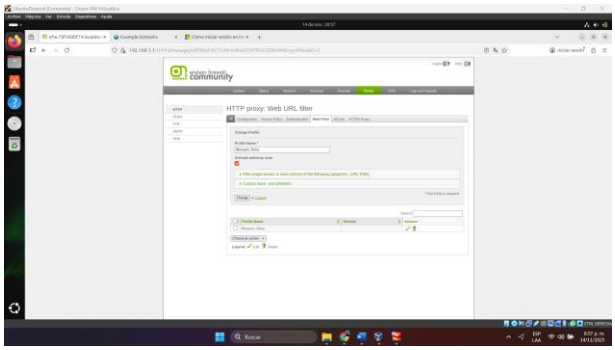
Después de configurar la temática 1, se realiza el paso a paso de la temática escogida.

Primero vamos a proxy y habilitamos el HTTP proxi; configuration y seleccionamos en la zona Green y Orange no transparent.



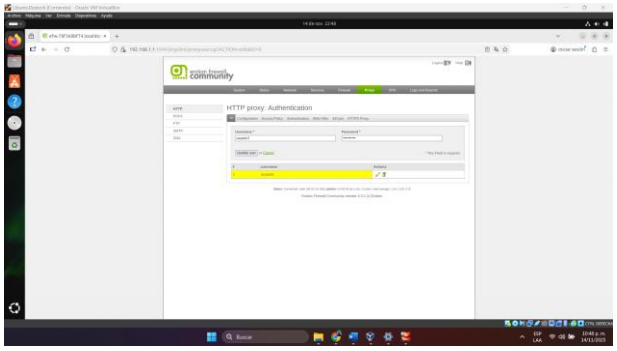
Fuente: Autoría Propia

Vamos a web filter y agregamos un nuevo perfil, colocamos Bloqueo_sitios como nombre y save para salvar el perfil.



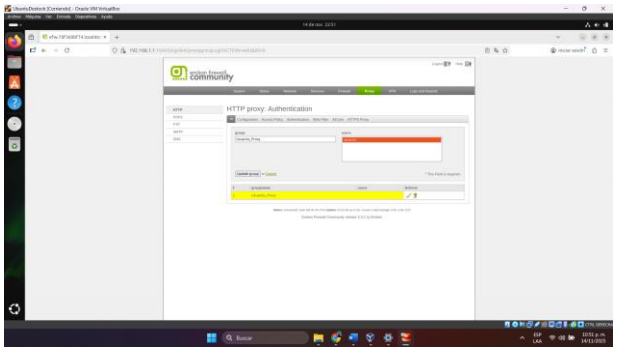
Fuente: Autoría Propia

Vamos a la pestaña autentificación y le damos a agregar un nuevo usuario, ingresamos el Username y el Password y guardar user.



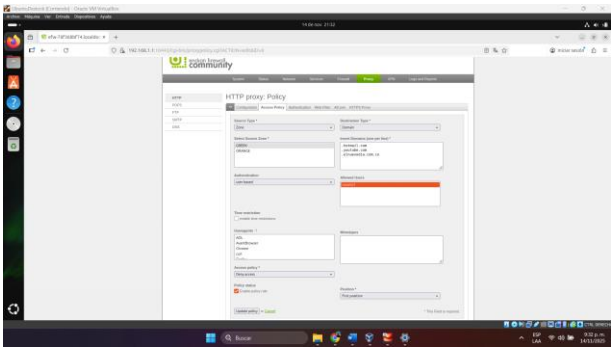
Fuente: Autoría Propia

En la pestaña autentificación buscamos manage group para crear el grupo de usuarios, le damos a add NCSA group y seleccionamos el usuario que creamos en la captura anterior luego le damos a guardar.



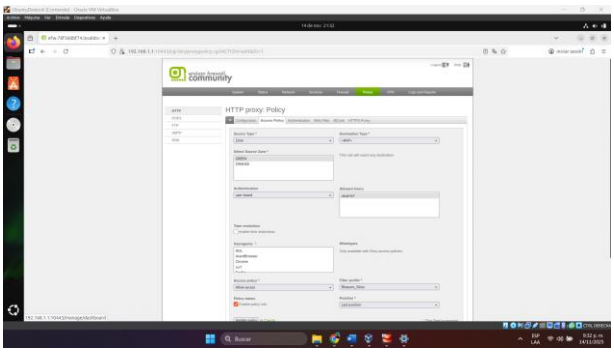
Fuente: Autoría Propia

Vamos a la pestaña Access policy y le damos a crear una nueva política de acceso, en esta seleccionamos la zona donde la vamos a realizar en mi caso quise hacerla para la zona verde y seleccionamos tipo de destinación la cual será dominio donde ingresamos los tres dominios que queremos colocar en nuestra lista negre: YouTube, Hotmail y elnuevodia en autentificación seleccionamos el usuario que creamos en autentificación, seleccionamos denegar acceso y le damos a guardar.



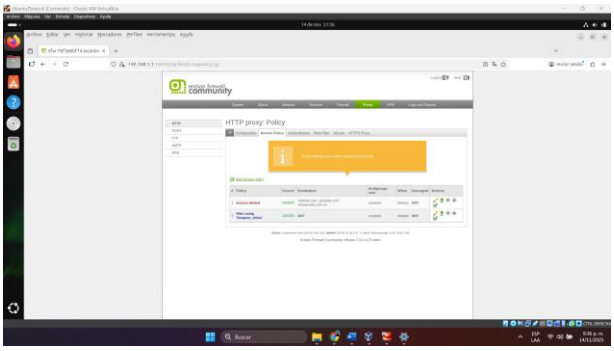
Fuente: Autoría Propia

Creamos una nueva política de acceso, le damos a crear política de acceso colocamos la zona que será verde en tipo de destino colocamos any, luego el usuario que creamos en autentificación en política de acceso colocamos permitir acceso, lo colocamos de segunda posición y le damos a guardar.



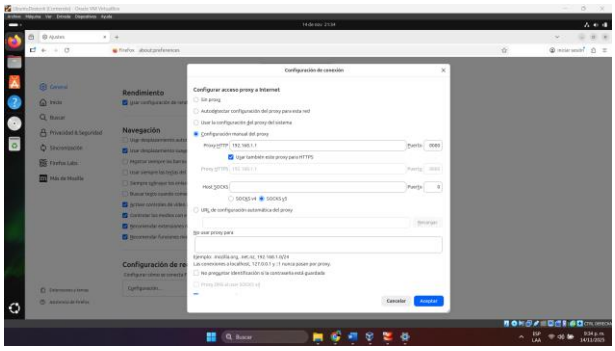
Fuente: Autoría Propia

Después nos saldrá una pestañita le damos a aplicar y esperamos a que se guarden los cambios y cómo podemos ver en la siguiente imagen salen nuestras políticas de acceso.



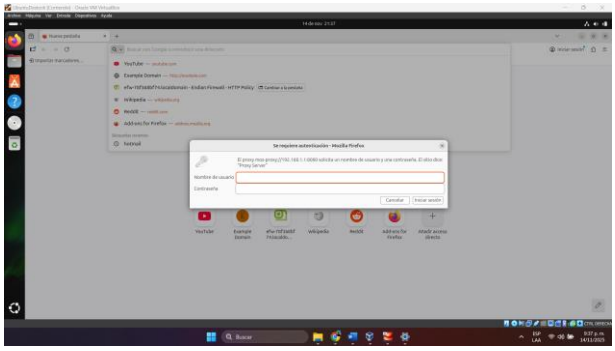
Fuente: Autoría Propia

Ahora en nuestro navegador nos vamos a ajustes, vamos hasta la parte de abajo y buscamos la configuración de red, seleccionamos la opción de configuración manual de proxy, colocamos nuestro proxy que es 192.168.1.1 en el puerto 8080 o el puerto que hallamos colocado en la configuración del proxi habilitamos la opción de usar también proxy para HTTPS y le damos a aceptar.

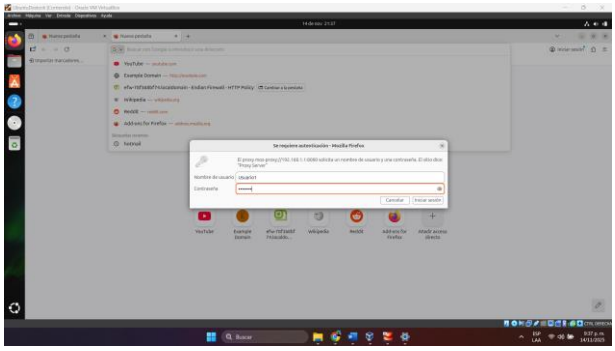


Fuente: Autoría Propia

Al volver a ingresar a nuestro navegador nos pedirá el usuario y contraseña que creamos en autentificación al momento de hacer cualquier opción en el navegador. Si la ingresamos podemos proseguir con lo que vamos a hacer.

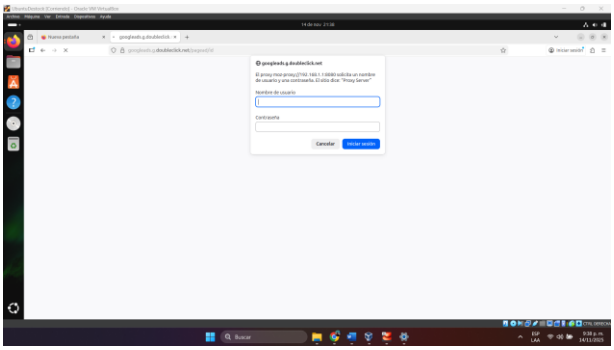


Fuente: Autoría Propia

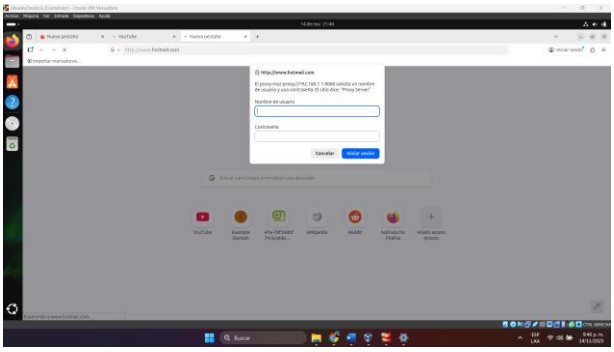


Fuente: Autoría Propia

Al ingresar a YouTube, Hotmail o el nuevo día nos pedirá la contraseña y usuario, pero no importa cuantas veces intentemos ingresar no nos lo va a permitir ya que el acceso está bloqueado y estos sitios están en la lista negra.

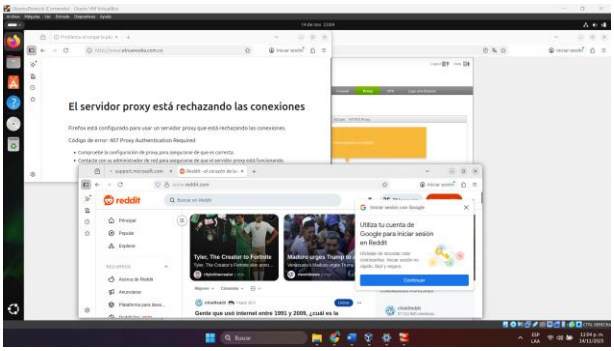


Fuente: Autoría Propia



Fuente: Autoría Propia

Pero si podremos ingresar a otras páginas que estén permitidas y no estén en la lista negra.



Fuente: Autoría Propia

4 RESULTADOS ESPERADOS POR TEMÁTICA

4.1 Temática 1: Configuración de la instancia para GNU/Linux Endian en VirtualBox (tarjetas de red) e instalación efectiva del mismo.

Instalación correcta de Endian.

Configuración de las zonas verde, roja y naranja.

Verificación del acceso vía interfaz web.

4.2 Temática 2: Configuración NAT.

Comunicación desde la LAN hacia Internet usando NAT Masquerading.

Traducción de puertos desde la WAN hacia los servicios en la DMZ.

Visualización de reglas generadas en Port Forwarding.

4.3 Temática 3: Permitir servicios de la Zona DMZ para la red.

Habilitación del servicio HTTP (puerto 80) y FTP (puerto 21) para clientes autorizados.

Bloqueo del protocolo ICMP para impedir ping entre zonas.

Evidencia de denegaciones en logs de tráfico.

4.4 Temática 4: Reglas de acceso para permitir o denegar el tráfico.

Comunicación permitida LAN → DMZ (HTTP/FTP).

Comunicación WAN → DMZ (según puertos autorizados).

Verificación en el módulo Inter-Zone Traffic.

Pruebas desde navegador web usando distintas combinaciones.

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

Creación de perfil y lista negra.

Configuración de usuario autenticado.

Aplicación de política de acceso vinculando lista negra y autenticación.

Pruebas desde LAN verificando bloqueo de:
hotmail.com
youtube.com
elnuevodia.com.co

5 CONCLUSIONES

La implementación de Endian Firewall permite comprender la importancia de la segmentación de redes y el manejo de políticas de seguridad perimetral.

Las reglas NAT habilitan el acceso controlado a Internet y la publicación segura de servicios en la zona DMZ.

El uso de reglas interzonales facilita el control del tráfico entre redes con distintos niveles de confianza.

La implementación del proxy HTTP con autenticación refuerza el control del acceso a Internet, permitiendo la creación de políticas centralizadas.

La experiencia práctica demuestra cómo los firewalls basados en GNU/Linux pueden operar como soluciones UTM completas y eficientes.

6 REFERENCIAS

[1] Endian Firewall Community. (2024). Endian Firewall Documentation. Recuperado de https://sourceforge.net/projects/efw/

[2] Oracle Corporation. (2024). Oracle VM VirtualBox User Manual.

[3] Endian S.r.l. (2023). Firewall and Network Address Translation (NAT) Configuration. Endian Documentation. https://docs.endian.com/

[4] Ziegler, R. (2019). Linux Firewalls: Enhancing Security with NFTables and Beyond (4th ed.). No Starch Press. (Capítulos sobre NAT, zonas de seguridad y DMZ)

[5] Cisco, “Network Address Translation: NAT Fundamentals,” Cisco Press, 2023.

[6] Stallings, W., *Foundations of Modern Networking: NAT and Security Concepts*, Pearson, 2022.

[7] Nemeth, E., Snyder, G., Hein, T., *Linux System Administration*, Addison-Wesley, 2018.

[8] Squid Proxy Project, “Squid: Optimising Web Delivery,” 2024. Disponible en: http://www.squid-cache.org