IMPLEMENTANDO UN ENTORNO DE RED SEGURO CON ENDIAN EN GNU/LINUX

Lizeth Katerin Bernal Maldonado
lkbernalm@unadvirtual.edu.co
Duvan Camilo García Panqueva
dcgarciapan@unadvirtual.edu.co
Juan Pablo Barrios Ramirez
jpbarriosr@unadvirtual.edu.co
Geraldine Stefania Diaz Barreto
gsdiazb@unadvirtual.edu.co

RESUMEN: *El presente documento describe la instalación y configuración de Endian Firewall Community (EFW) como solución de seguridad perimetral en una red segmentada en tres zonas: zona LAN (verde), DMZ (naranja) y acceso a Internet (roja). Se implementan y prueban las cinco temáticas solicitadas: configuración de zonas y tarjetas de red, NAT, reglas de acceso a servicios en DMZ, políticas interzonales y proxy HTTP no transparente con autenticación y lista negra. Todo el desarrollo se realiza sobre máquinas virtuales en VirtualBox, garantizando la protección de servidores internos y el control de navegación de los usuarios de la red local.*

Abstract - This document describes the installation and configuration of Endian Firewall Community (EFW) as a perimeter security solution in a network segmented into three zones: LAN (green), DMZ (orange), and Internet access (red). The five required topics are implemented and tested: configuration of zones and network interfaces, NAT, access rules for DMZ services, inter-zone policies, and a non-transparent HTTP proxy with authentication and a blacklist. All implementation is carried out on virtual machines in VirtualBox, ensuring the protection of internal servers and effective control of web browsing for local network users.

PALABRAS CLAVE: DMZ, Endian Firewall, Firewall, NAT, Proxy no transparente, Seguridad perimetral, VirtualBox, Zonas de red.

1 INTRODUCCIÓN

En el marco de la Etapa 7 del Diplomado, se plantea la necesidad de proteger servidores internos (intranet) y controlar el acceso a Internet mediante una arquitectura de seguridad perimetral. Para ello se implementa Endian Firewall Community como plataforma unificada de seguridad que permite crear tres zonas de red:

Verde (GREEN): Red interna LAN
Naranja (ORANGE): Zona DMZ con servidores públicos
Roja (RED): Conexión a Internet (WAN simulada)

El objetivo principal es garantizar que los servicios críticos ubicados en la DMZ sean accesibles desde Internet y desde la LAN de forma controlada, mientras se bloquea tráfico no deseado y se implementa un proxy autenticado para el acceso a Internet de los usuarios internos.

2 METODOLOGÍA / DESARROLLO DE LA SOLUCIÓN

Se requiere proteger una red corporativa donde:

Los usuarios de la LAN necesitan acceso controlado a Internet.

Un servidor web y FTP en la DMZ debe ser accesible desde Internet y desde la LAN.

Se debe impedir el acceso directo no autorizado y bloquear sitios de entretenimiento.

Todo el tráfico saliente de la LAN debe pasar por proxy autenticado

COMPONENTES PRINCIPALES

A. Endian Firewall Community (EFW)

Endian Firewall es una distribución de GNU/Linux basada en CentOS diseñada específicamente como UTM (Unified Threat Management). Incluye firewall stateful, VPN, proxy con autenticación, antivirus, antispam, hotspot y múltiples zonas de seguridad. Su versión Community es gratuita y de código abierto.

B. Zonas de seguridad

GREEN: Red confiable (LAN interna)

ORANGE: DMZ – servidores accesibles desde fuera pero protegidos

RED: Interfaz expuesta a Internet

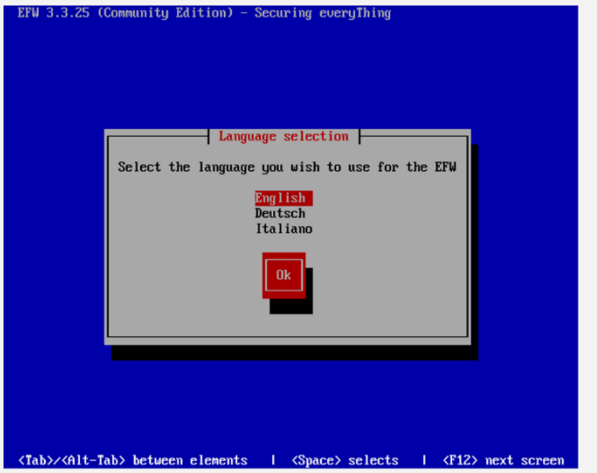
Esta separación permite aplicar políticas granulares de tráfico.

C. Proxy no transparente

Obliga a los clientes a configurar explícitamente el proxy en el navegador (puerto 8080 por defecto en Endian), permitiendo autenticación de usuarios y aplicación de políticas por grupo o usuario.

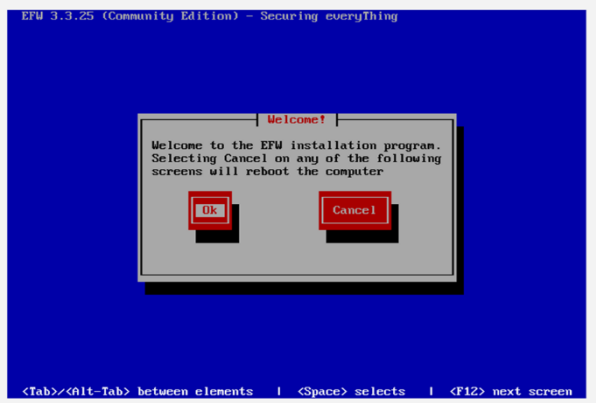
3 INSTALACIÓN DE ENDIAN

Figura 1.1 Configuración de lenguaje



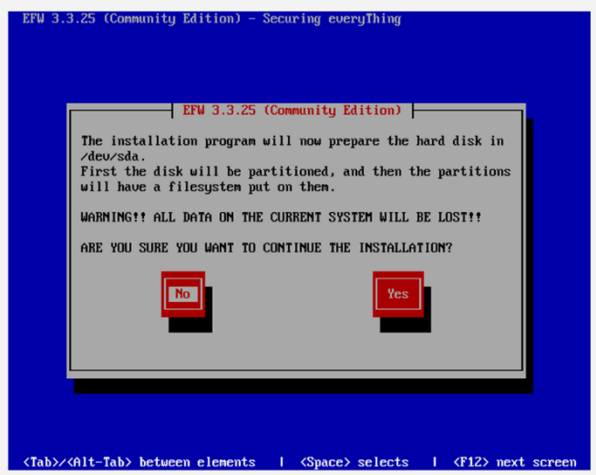
Fuente: Autoría Propia

Figura 1.2 Pasos iniciales de instalación



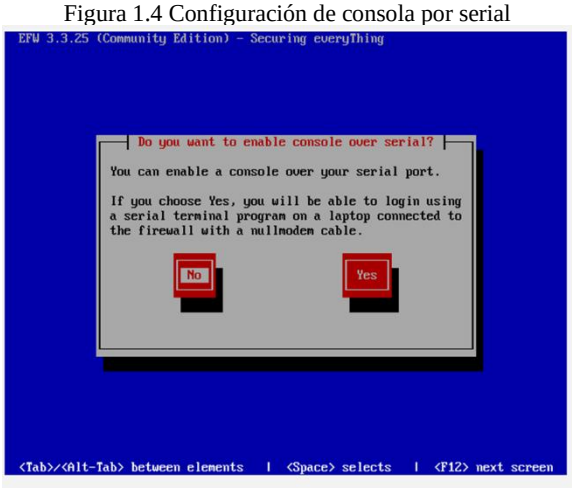
Fuente: Autoría Propia

Figura 1.3 Configuración de discos



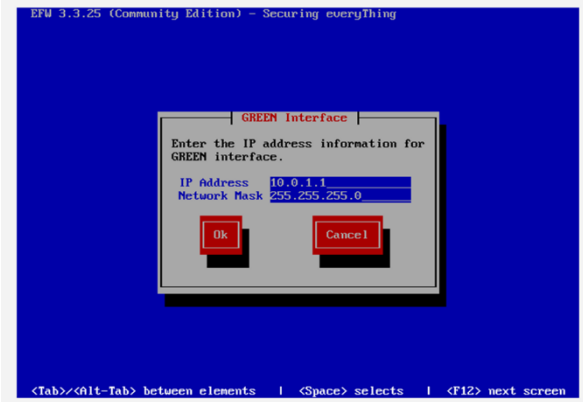
Fuente: Autoría Propia

Figura 1.4 Configuración de consola por serial



Fuente: Autoría Propia

Figura 1.5 Definición IP para zona GREEN



Fuente: Autoría Propia

Figura 1.6 Finalización de instalación

Fuente: Autoría Propia

4 DESARROLLO DE LAS TEMÁTICAS

Temática 1 – Configuración de Endian Firewall en VirtualBox e instalación con tres zonas
Para la implementación del entorno seguro se creó la infraestructura base compuesta por tres máquinas virtuales: Endian Firewall, Ubuntu Server y Linux Mint, cada una cumpliendo un rol dentro de las zonas GREEN, ORANGE y RED. La configuración inicial consistió en definir correctamente las tarjetas de red en VirtualBox para garantizar la segmentación de la red y el funcionamiento esperado del firewall.

1. Configuración de máquinas virtuales
   Se prepararon las siguientes máquinas:

Endian Firewall 3.3.2
Configurada con tres adaptadores de red:
- eth0 – GREEN (Red interna LAN)
- eth1 – ORANGE (Red interna DMZ)
- eth2 – RED (Adaptador puente simulando Internet)

Linux Mint (Cliente)
Conectada únicamente a la zona GREEN, verificando su conexión y obtención de IP.

Ubuntu Server (Servidor DMZ)
- Conectado a la zona ORANGE
- IP estática asignada para pruebas de conectividad y servicios.

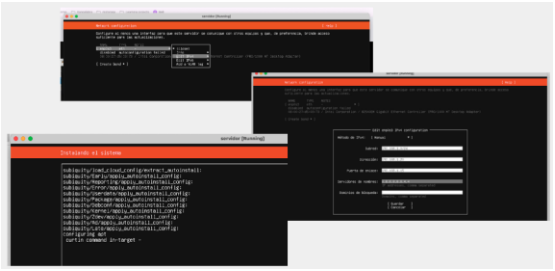
Figura 1.7 Configuración de las tarjetas de red

Fuente: Autoria Propia

2. Carga de imágenes ISO e instalación
   Se agregó el ISO correspondiente en cada máquina virtual y se procedió a instalar:
   - **Linux Mint** como estación de trabajo en la zona GREEN.
   - **Ubuntu Server** como servidor en DMZ.
   - **Endian Firewall,** configurando durante la instalación sus tres zonas de red.

Cada máquina virtual se verificó para asegurar que estuviera operativa antes de configurar Endian.

Figura 1.8 Instalación de Ubuntu server

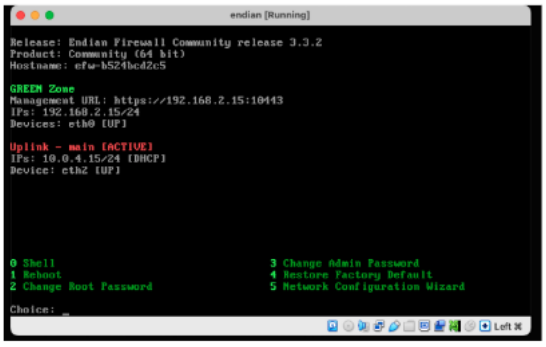


Fuente: Autoría Propia

Figura 1.9 Instalación de Linux Mint

Fuente: Autoría Propia

Figura 1.10 Instalación de Linux Mint



Fuente: Autoría Propia

3. Configuración de las zonas en Endian
   Durante la instalación de Endian se definieron las tarjetas de red:

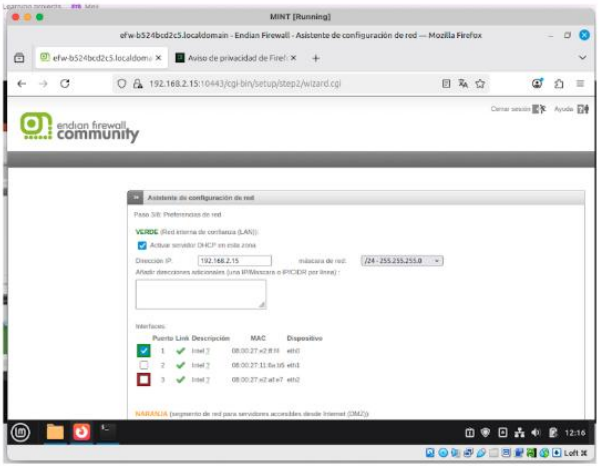
Zona GREEN (LAN interna)
- Puerta de enlace del firewall: 192.168.2.15
- Permite navegación y administración interna.

Zona ORANGE (DMZ)
- Segmento donde se ubica el servidor Ubuntu.
- Configuración de IP manual durante la instalación.

Zona RED (Internet/WAN)
- Configurada con adaptador puente para simular salida real a Internet.
- Se validó conectividad mediante pruebas de ping externas.

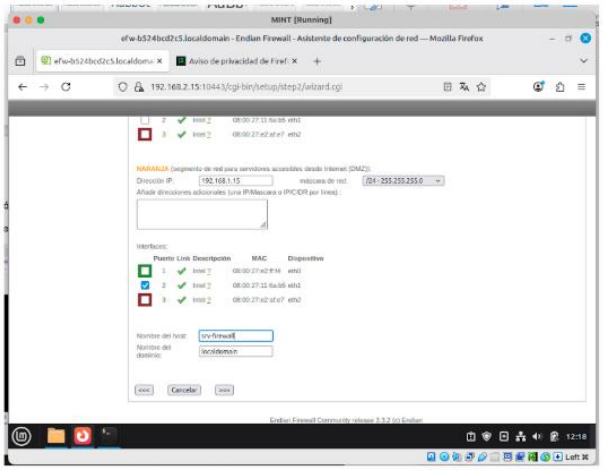
Tras definir cada zona, Endian ejecutó su asistente de configuración, habilitando servicios base como DHCP en la zona GREEN y confirmando el correcto levantamiento del firewall.

Figura 1.11 Configuración zona verde



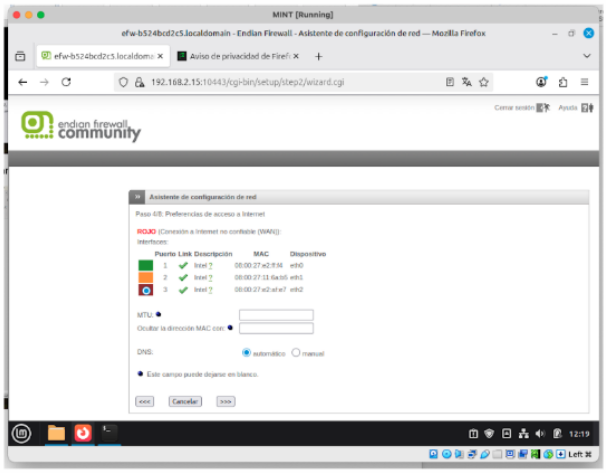
Fuente: Autoría Propia

Figura 1.12 Configuración zona naranja



Fuente: Autoría Propia

Figura 1.13 Configuración zona roja



Fuente: Autoría Propia

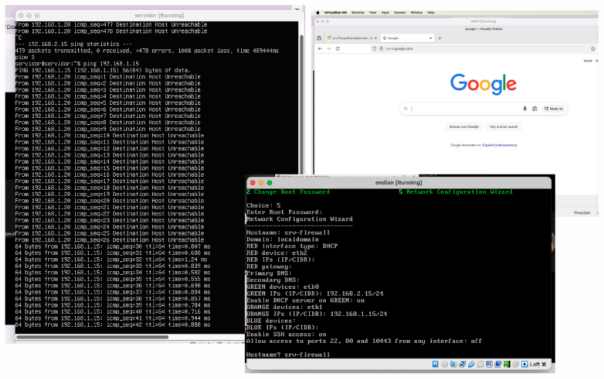
4. Validación de conectividad

Una vez instaladas las máquinas y configuradas las zonas:

- Se comprobó la conexión en la zona GREEN desde el cliente Linux Mint.
- Se verificó la conectividad en la zona ORANGE desde Ubuntu Server.
- Se validó la salida a Internet desde Endian mediante comandos de diagnóstico.
- Se confirmó que las tres zonas estaban correctamente segmentadas y operativas.

Esta configuración inicial permitió establecer la arquitectura fundamental sobre la cual se desarrollaron las temáticas posteriores como NAT, reglas interzonales y proxy.

Figura 1.14 Configuración zona roja



Fuente: Autoría Propia

Temática 2 – Configuración de NAT

En NAT:

LAN → Internet: Source NAT (masquerading) desde GREEN hacia RED.

DMZ → Internet: Source NAT desde ORANGE hacia RED.

También se habilita el reenvío de puertos (Port Forwarding) para HTTP y FTP desde RED hacia el servidor DMZ.

CONFIGURACION DE NAT

Se crean las máquinas virtuales Endian y Ubuntu Server, configurando sus redes respectivamente. Se implementa una arquitectura de tres zonas (WAN, LAN, DMZ) en las máquinas virtuales con el esquema de direccionamiento correspondiente.

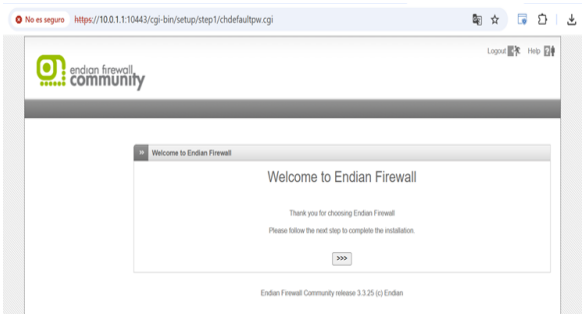
Figura 2.1 Definición de zonas

Adaptador EFW	Conexión VirtualBox	Zona/Color	Función	IP (Planificada)
Adaptador 1	**Solo Anfitrión**	**GREEN (LAN)**	Interfaz de Gestión	`10.0.1.1`
Adaptador 2	**Adaptador Puente**	**RED (WAN)**	Acceso a Internet Simulada	`192.168.1.100` (de rango de tu red física)
Adaptador 3	**Red Interna** (DMZ_ORANGE)	**ORANGE (DMZ)**	DMZ	`10.0.2.1`

Fuente: Autoría Propia

Se ingresa a la dirección IP configurada en Endian, permitiendo el acceso al firewall desde el navegador.

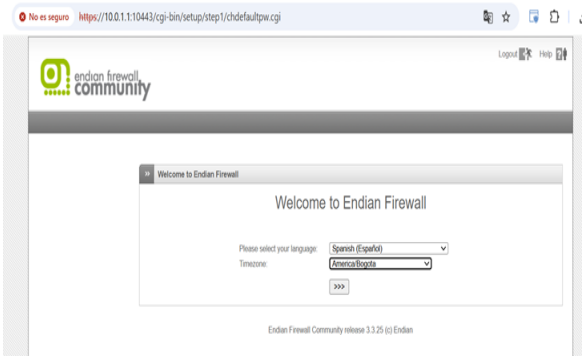
Figura 2.2 Ingreso Endian



Fuente: Autoría Propia

Se procede a configurar el idioma.

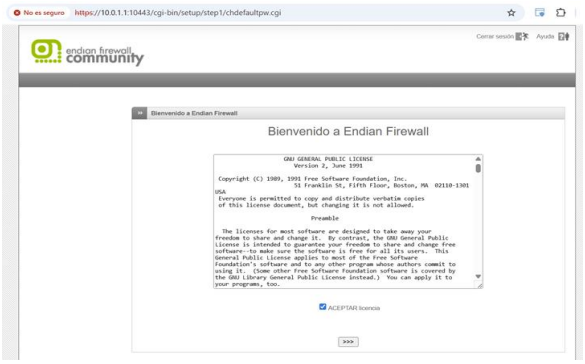
Figura 2.3 Ingreso de credenciales



Fuente: Autoría Propia

El sistema da la bienvenida y solicita aceptar la licencia.

Figura 2.4 Pantalla de ingreso Endian



Fuente: Autoría Propia

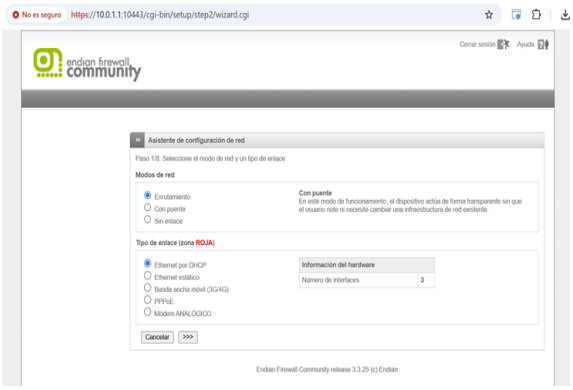
Se configuran las contraseñas del usuario *admin* y del usuario *root*, asignándose en ambos casos la clave

Figura 2.5 Creación de credenciales

Fuente: Autoría Propia

Se configura la red, específicamente el adaptador 2 correspondiente a la zona RED.

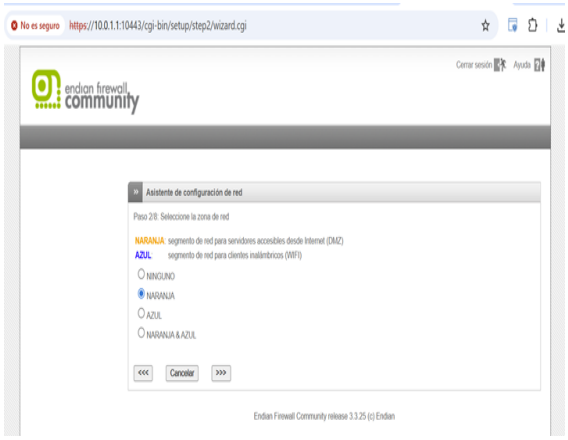
Figura 2.6 Configuración inicial de zonas



Fuente: Autoría Propia

Se configura el adaptador 2 de la zona ORANGE.

Figura 2.7 Elección de zonas a crear



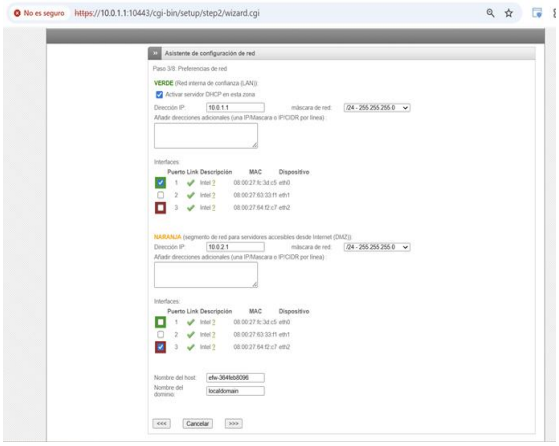
Fuente: Autoría Propia

Se configura el adaptador 1 perteneciente a la zona GREEN.

Se activa el servidor DHCP en esta zona, asignando la IP 10.0.1.1 con máscara 255.255.255.0 (/24).

las interfaces en el puerto 1 (zona GREEN) del adaptador, la zona ORANGE en el adaptador 3, asignando la IP indicada y la misma máscara. Después se configura el adaptador 2 (zona RED).

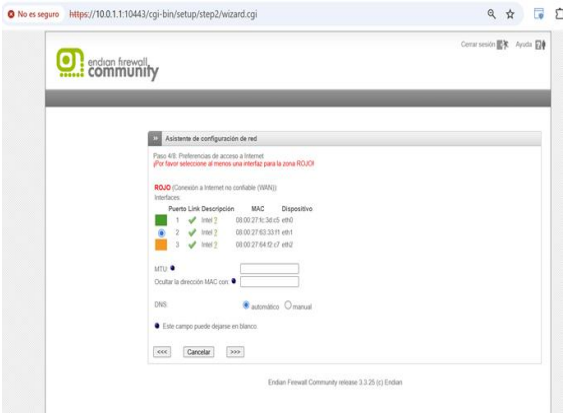
Figura 2.8 Definición de zona GREEN y ORANGE



Fuente: Autoría Propia

Después se configura el puerto dos en la zona red que es el adaptador 2 y se le da en siguiente

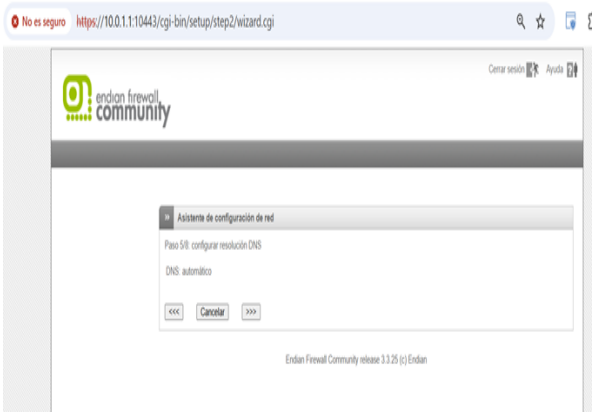
Figura 2.9 Definición de zona RED



Fuente: Autoría Propia

Se procede a configurar la resolución DNS.

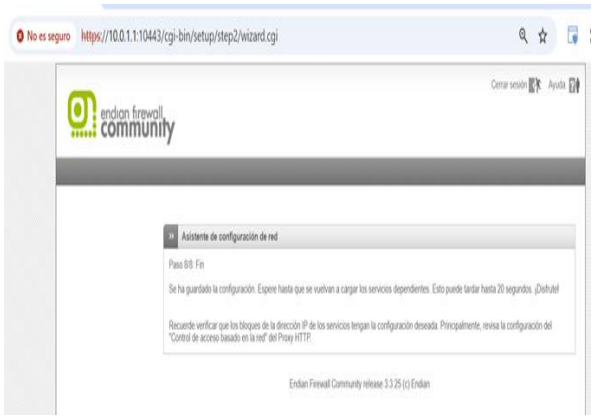
Figura 2.10 Definición de DNS



Fuente: Autoría Propia

El sistema indica que la configuración ha sido cargada y solicita esperar mientras se activan los servicios dependientes.

Figura 2.11 Finalización de configuración zonas



Fuente: Autoría Propia

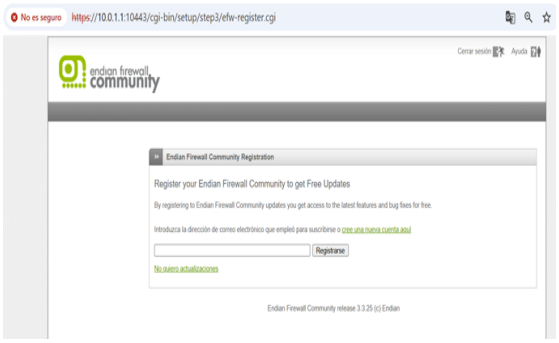
Una vez cargados, se inicia sesión con el usuario *admin* y la contraseña asignada (bigdata).

Figura 2.12 Inicio de sesión Endian

Fuente: Autoría Propia

Configuración de la tarjeta de red DMZ en Ubuntu Server: red interna DMZ_ORANGE y que posee la IP estática 10.0.2.15, para el enrutamiento y DNAT. El adaptador 1 está conectado a la red interna DMZ_ORANGE**,** Se muestra la opción para registrarse a las actualizaciones de la comunidad; se selecciona No quiero

Figura 2.13 Pantalla de recepción Endian

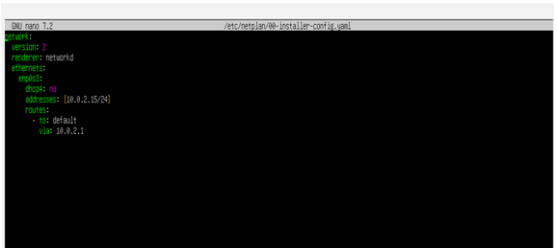


Fuente: Autoría Propia

Luego, en Ubuntu Server, se accede al archivo de configuración mediante: sudo nano /etc/netplan/00-installer-config.yaml

Se aplica la configuración de Netplan, mostrando la IP 10.0.2.15/24 activa en la interfaz enp0s3.

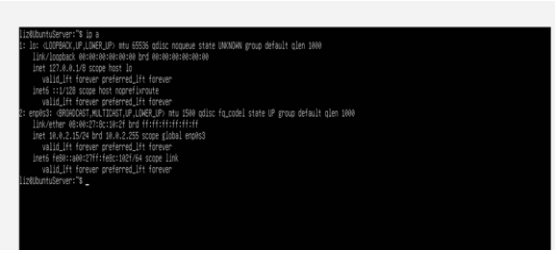
Figura 2.14 Configuración IP Manual



Fuente: Autoría Propia

Se visualiza la salida del comando ip a, confirmando las interfaces y direcciones asignadas.

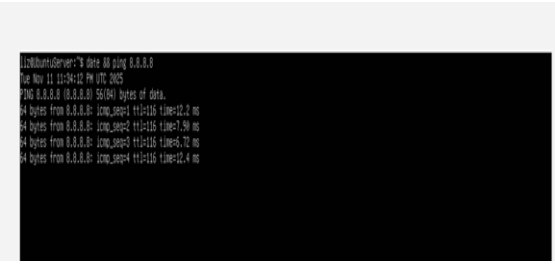
Figura 2.15 Verificación de IP asignada



Fuente: Autoría Propia

Se valida la conectividad mediante un ping hacia 8.8.8.8, confirmando salida a Internet.

Figura 2.16 Prueba de ping



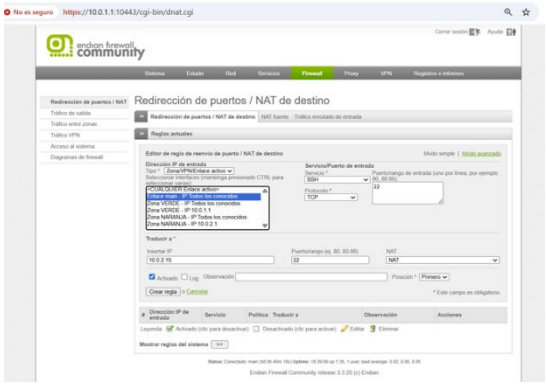
Fuente: Autoría Propia

Punto 2

Se configura el redireccionamiento de puertos/NAT destino:

Tipo: zona VPN (enlace activo)
Servicio: SSH
Puerto: 22
Protocolo: TCP
Interfaz: Enlace main – IP (todos los conocidos)
IP destino: 10.0.2.15, puerto 22
NAT: activado
Se crea la regla y se avanza.

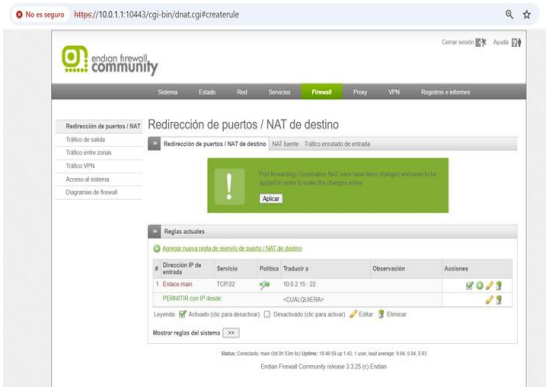
Figura 2.17 Configuración de NAT



Fuente: Autoría Propia

El sistema muestra una advertencia indicando que las reglas han sido modificadas y deben aplicarse los cambios. Se selecciona Aplicar.

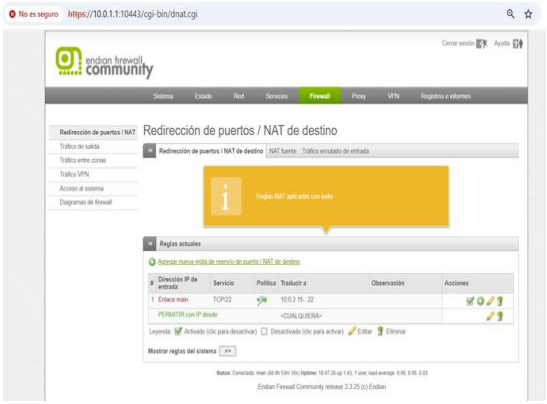
Figura 2.18 Resumen de NAT creada



Fuente: Autoría Propia

Posteriormente, se confirma que las reglas NAT fueron aplicadas exitosamente.

Figura 2.19 Regla de NAT aplicada



Fuente: Autoría Propia

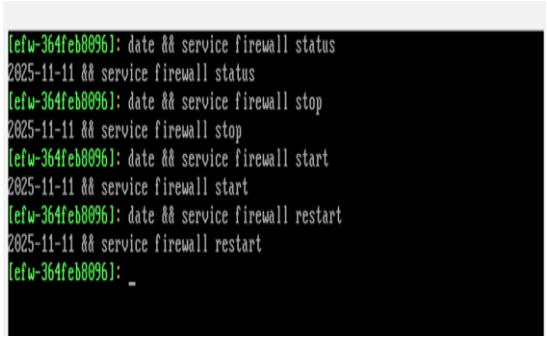
Finalmente se utilizan los siguientes comandos para Manejo de Servicios:

Tabla 1 Comados para manejo de servicios

Comando Ejecutado	Función
date && service firewall status	Verifica el estado del servicio de firewall
date && service firewall stop	Detiene el servicio de firewall.
date && service firewall start	Inicia el servicio de firewall.
date && service firewall restart	Reinicia el servicio de firewall.

Fuente: Autoría Propia

Figura 2.20 Pruebas de firewall



Fuente: Autoría Propia

Temática 4 – Reglas de acceso inter-zonas

Reglas en “Inter-Zone Traffic”:
GREEN → ORANGE: Permitir HTTP y FTP
ORANGE → RED: Permitir todo (porque luego se controla con proxy)
Se prueban todos los flujos con navegador y terminal para simular consumos http de navegador.

CONFIGURACION REGLAS DE TRAFICO INTERZONAS

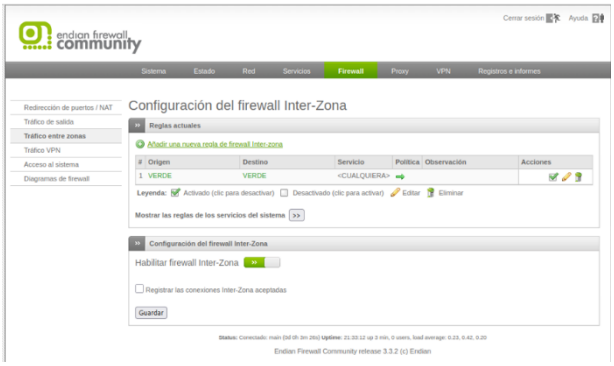
Configurada la red según la segmentación de la temática 1 se abre el apartado de firewall donde se configuran las reglas de acceso.

Figura 4.1 Sección firewall de Endian

Fuente: Autoría Propia

Para el primer escenario de reglas que permitan los protocolos HTTP y FTP entre la zona GREEN y zona ORANGE, se debe crear una regla nueva en el apartado de tráfico entre zonas.

Figura 4.2 reglas de tráfico entre zonas de firewall



Fuente: Autoría Propia

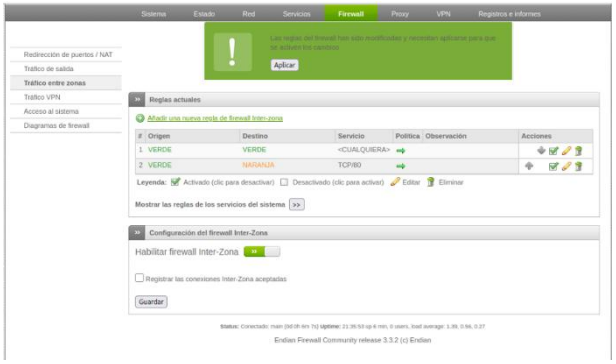
En la regla se debe definir la zona origen que en este caso será GREEN, la regla de destino que será ORANGE y en el servicio se seleccionará HTTP con acción permitir.

Figura 4.3 regla de tráfico HTTP

Fuente: Autoría Propia

Al finalizar se verá la regla creada en el listado donde detalla el origen, destino, servicio, sentido y estado de la regla. Para que empiece a tener validez la regla se deben aplicar los cambios en el pop-up emergente que aparece.

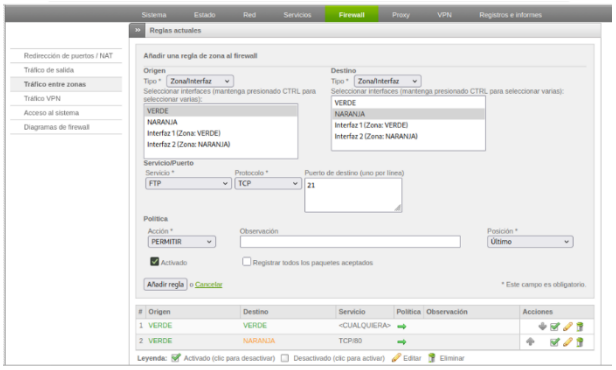
Figura 4.4 regla de tráfico HTTP



Fuente: Autoría Propia

Ahora para completar el primer escenario se debe crear la regla correspondiente al servicio FTP. Se debe crear la nueva regla cómo en los pasos anteriores cambiando solo en la parte de definición.

Figura 4.5 regla de tráfico FTP

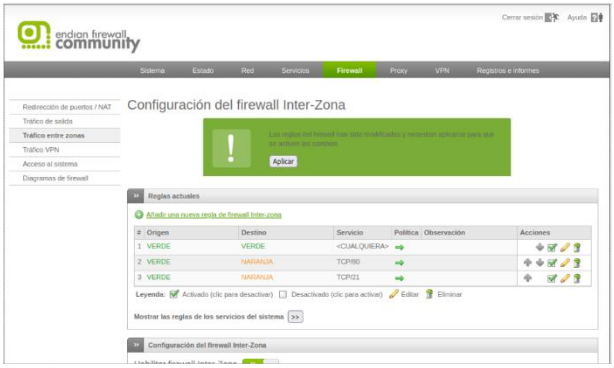


Fuente: Autoría Propia

Como se detalla en la figura 4.5 la regla se define muy parecida a la del protocolo HTTP solo cambia el servicio que se permite en la regla que en este caso es el FTP por el puerto 21. Al igual que con la regla anterior se deben aplicar los cambios

en el firewall para que se vean reflejados en los segmentos de red.

Figura 4.6 regla de tráfico FTP

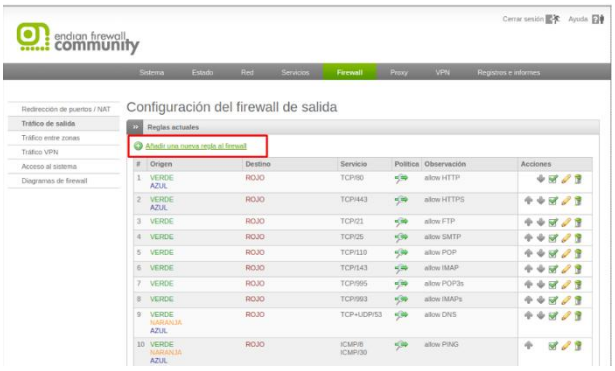


Fuente: Autoría Propia

CONFIGURACION REGLAS DE TRAFICO DE SALIDA

Ahora para continuar con las configuraciones planteadas, dentro de la sección de tráfico de salida se creará una nueva regla.

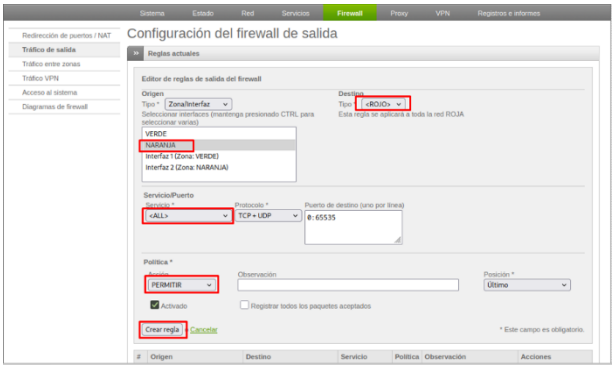
Figura 4.7 Reglas tráfico de salida



Fuente: Autoría Propia

En las reglas de trafico de salida se puede permitir el acceso desde cualquiera de las zonas controladas hacia la zona RED que es la que tiene exposición a internet. En el escenario a desarrollar crearemos una regla que permita acceso desde el origen zona ORANGE hacia el destino zona RED de todos los posibles servicios.

Figura 4.8 Regla tráfico de salida para todos los servicios



Fuente: Autoría Propia

Una vez creada la regla al igual que con las reglas de trafico entre zonas, se puede ver el listado de reglas existentes con el detalle de origen, destino, servicio, sentido y estado de la regla. Al igual que con las demás reglas se debe aplicar la configuración en el firewall para que esta se vea reflejada.

Figura 4.9 Regla tráfico de salida para todos los servicios

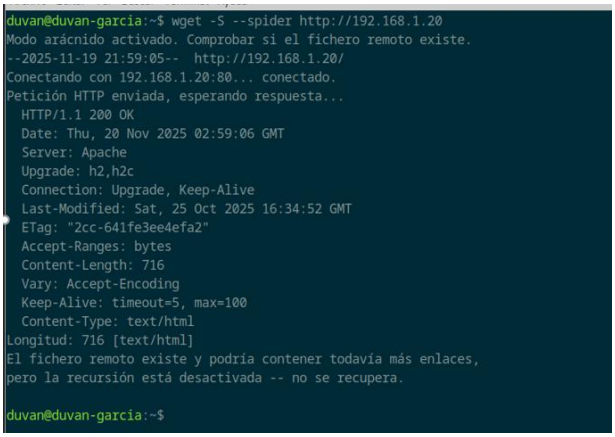
Fuente: Autoría Propia

VALIDACIÓN DE CONFIGURACIONES

1. GREEN → ORANGE: Permitir HTTP y FTP

Para evidenciar la funcionalidad de las reglas creadas se debe probar la conectividad entre las zonas. Primero se puede ver un ejemplo de conexión http desde un equipo Debian en la zona GREEN (192.168.2.20) hacia un servidor Linux en la zona ORANGE (192.168.1.20)

Figura 4.10 Prueba HTTP desde GREEN hacia ORANGE

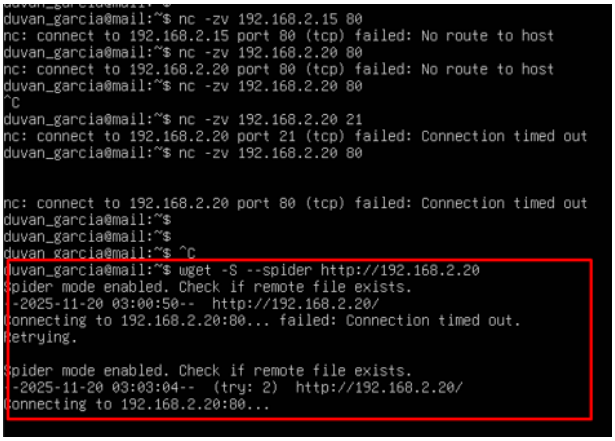


Fuente: Autoría Propia

En la figura 4.10 se puede ver cómo el comando wget retorna código HTTP 200 que significa exitoso.

Además, cómo la regla solo se creó en sentido desde zona GREEN hacía zona ORANGE en el momento de intentar una conexión de tráfico inverso, el resultado es fallido debido a que no se tiene esa conectividad permitida.

Figura 4.11 Prueba FTP desde GREEN hacia ORANGE



Fuente: Autoría Propia

Ahora para el escenario de FTP usando un comando distinto, se prueba la conectividad desde un equipo Debian en la zona GREEN (192.168.2.20) hacia un servidor Linux en la zona ORANGE (192.168.1.20).

Figura 4.12 Prueba FTP desde GREEN hacia ORANGE

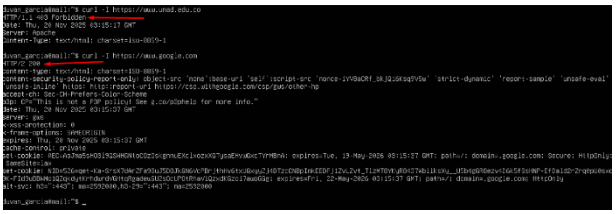
Fuente: Autoría Propia

En la figura 4.10 se puede ver cómo el comando nc en la segunda línea retorna la IP destino, el puerto, el protocolo del puerto y el estado de la conectividad.

2. ORANGE → RED: Permitir todo (porque luego se controla con proxy)

Para confirmar el tráfico hacia la zona RED, simplemente se debe realizar una prueba de uno de los servicios que usan internet. Para este escenario se realiza la prueba con un CURL hacia páginas de internet.

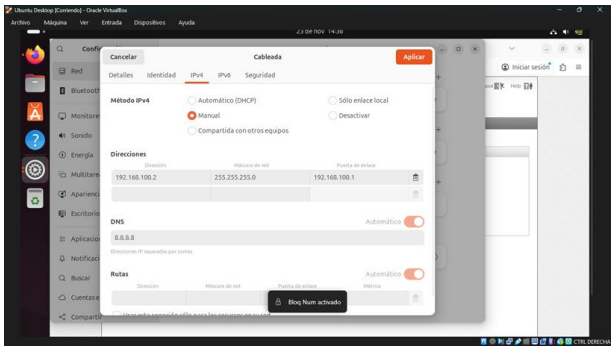
Figura 4.13 Prueba HTTPS desde ORANGE hacia RED



Fuente: Autoría Propia

Temática 5: Implementar un Proxy HTTP.

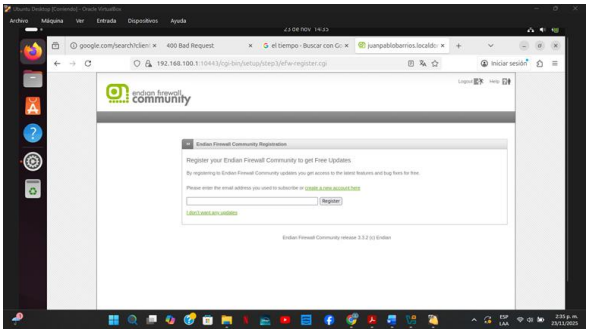
Figura 5.1 Ingreso a Ubuntu Desktop



Fuente: Autoría Propia

Se inicia sesión en Ubuntu Desktop y se configura la conexión de red en la opción IPv4, se escoge la opción manual se digita la puerta de enlace: 192.168.100.1 al igual que la máscara de red 255.255.255.0 y se asigna una IP dentro del rango de la puerta de enlace para el caso 192.168.100.2.

Figura 5.2 Ingreso al servidor Endian Firewall

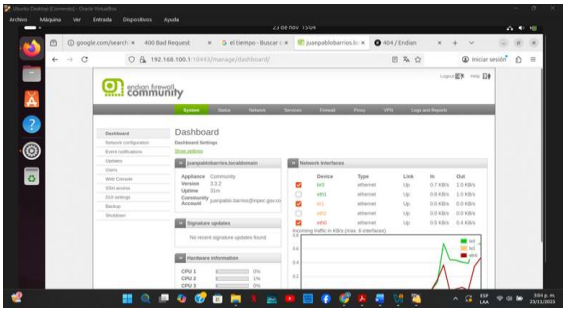


Fuente: Autoría Propia

Una vez finaliza se configura la red del sistema del Ubuntu desktop se abre el navegador predeterminado, para el ejemplo Mozilla Firefox. Digitamos la IP donde se encuentra

Endian firewall instalada y el número del puerto, para el caso: **192.168.100.1:10443**

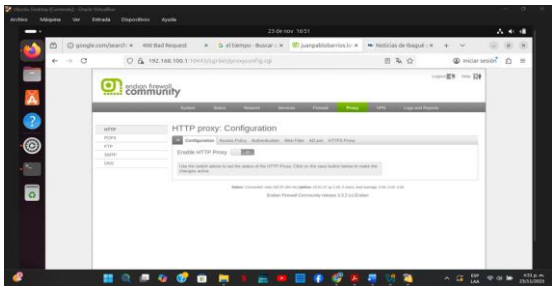
Figura 5.3 Ingreso interfaz gráfica Endian Firewall.



Fuente: Autoría Propia

La plataforma solicita que nos registremos con un correo e ingresamos usuario y contraseña (misma de la configuración de la distribución de Endian instalada en la otra máquina virtual) para el caso usuario :admin -contraseña:12345678

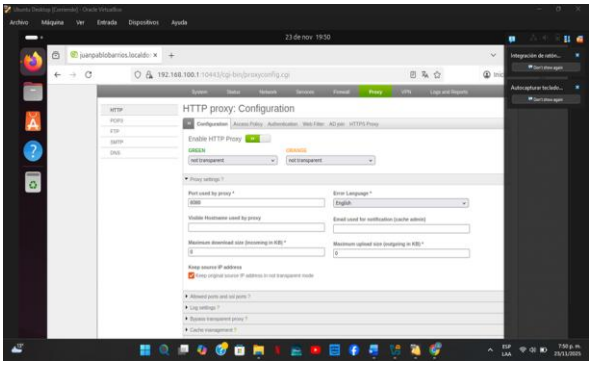
Figura 5.4 Configuración Proxy en la interfaz web.



Fuente: Autoría Propia

Se procede a configurar el proxy, lo primero habilitamos el proxy en la pestaña con el mismo nombre.

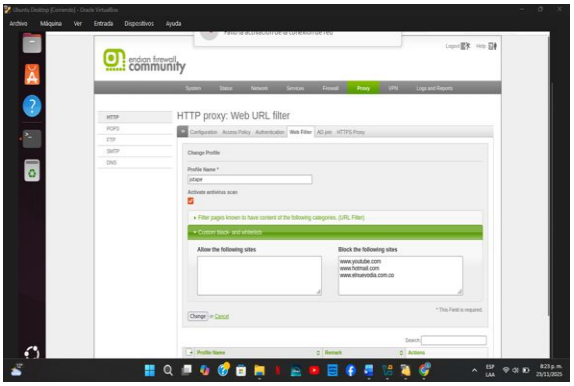
Figura 5.5 Configuración Proxy habilitado.



Fuente: Autoría Propia

En la zonas verde y naranja se selecciona la opción No transparente, *Se configura el puerto para el caso 8080, se escoge el idioma, las demás se pueden dejar por defecto*

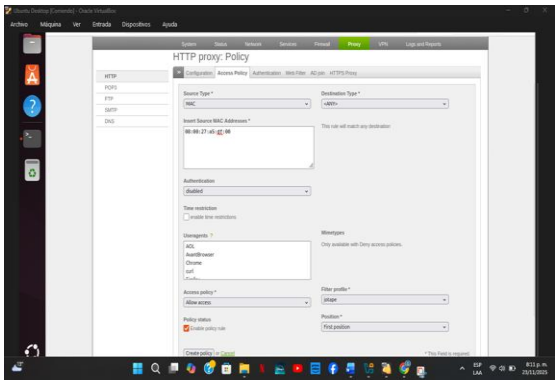
Figura 5.6 Creación de perfil para el filtrado del proxy.



Fuente: Autoría Propia

El sistema tiene creado por defecto un perfil, lo podemos editar, eliminar o crear uno nuevo. Se asigna nombre para que este se puede seleccionar en las diferentes configuraciones. Este espacio permite filtrar los sitios web por categorías, sin embargo, lo que vamos a efectuar es la creación de unas listas de sitios web no permitidos, (black lists). También se puede crear una lista de sitios web permitidos, (Whitelists)

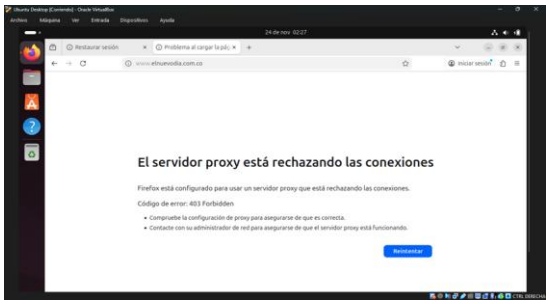
Figura 5.7 Creación de políticas de acceso.



Fuente: Autoría Propia

Por medio de la dirección MAC del equipo al cual se quiere restringir el acceso de un grupo de sitios web, en autentificación habilitamos la opción si queremos el destino puede ingresar con usuario y contraseña, en el perfil seleccionamos el efectuado anteriormente para el caso "jotape", denegamos o permitimos el acceso y luego creamos la política de acceso y aplicamos los cambios.

Figura 5.8 Validación de la restricción



Fuente: Autoría Propia

Una vez se efectúa lo configuración de restricciones en la interfaz de Endian , se habilita el proxy del navegador para generar la restricción en el sitio listado, se comprueba intentado ingresar a los sitios wew relacionados. El navegador debería mostrar una restricción de acceso.

5 CONCLUSIONES

La configuración inicial de la infraestructura en VirtualBox y la instalación de Endian Firewall permitieron establecer una base sólida para la segmentación de la red en sus tres zonas principales: GREEN, ORANGE y RED. Este proceso aseguró que cada máquina virtual cumpliera su rol dentro de la arquitectura planteada y que las interfaces de red funcionaran correctamente desde el inicio. Gracias a esta preparación, fue posible continuar con las etapas posteriores del proyecto, garantizando estabilidad, conectividad y una estructura adecuada para la implementación de reglas de seguridad, NAT y políticas de acceso.

La implementación de Endian Firewall Community en VirtualBox demostró ser una solución de seguridad robusta y efectiva para redes corporativas. La capacidad de configurar de manera eficiente las tres zonas de seguridad (Verde, Naranja y Roja), combinada con la aplicación de reglas de NAT y políticas interzonales, validó su potencial como una plataforma UTM (Unified Threat Management) gratuita y de código abierto.

La metodología de trabajo sobre máquinas virtuales en VirtualBox permitió la verificación práctica de todas las reglas de acceso y de NAT. Esto aseguró que las configuraciones de reenvío de puertos (para la DMZ) y las políticas Inter-Zona funcionaran según lo esperado, optimizando la gestión de riesgos y proporcionando un modelo escalable para una potencial implementación en un entorno de producción real.

Además, la implementación de un proxy HTTP no transparente con autenticación permitió ejercer un control fino sobre la navegación de los usuarios, aplicando listas negras y políticas por equipo. Este enfoque no solo mejora la seguridad, sino que también aporta herramientas de gestión y trazabilidad del uso de Internet en la organización.

6 REFERENCIAS

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

[5] Endian (2016), Endian UTM 3.2 Manual referencia. Endian. http://docs.endian.com/3.2/utm/index.html

[6] LPI Linux Essentials. (2022). Tema 5: Seguridad y sistema de permisos de archivos. https://learning.lpi.org/es/learning-materials/010-160/5/

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

[8] Hernández, P. F., & Sánchez, J. (2022). Monitoreo y administración de sistemas Linux. Repositorio UNAD. https://repository.unad.edu.co/handle/10596/53211

[9] Hernández, P. F., & Sánchez, J. (2022). Servidores para administración remota y compartir recursos. Repositorio UNAD. https://repository.unad.edu.co/handle/10596/53212

[10] Jiménez, J. H. (2016). Shell Script para Bash. Repositorio UNAD. https://repository.unad.edu.co/handle/10596/9758

[11] Free Software Foundation. (2016). Software Libre y educación. http://www.gnu.org/education/education.html

[12] Vargas, C. H. (2020). Implementando el entorno de trabajo GNU/Linux. Repositorio UNAD. https://repository.unad.edu.co/handle/10596/38598

[13] Hernández, P. F. (2022). Software Libre y Open Source. Repositorio UNAD. https://repository.unad.edu.co/handle/10596/53347