IMPLEMENTACIÓN PROTOCOLOS DE SEGURIDAD GNU/LINUX MEDIANTE ENDIAN

MIGUEL ANDRÉS OSORIO DIAZ
maosoriod@unadvirtual.edu.co
MARCOS ELIECER RODRIGUEZ CALDERÓN
merodriguezcal@unadvirtual.edu.co
JOSÉ GERMAN MORALES LÓPEZ
jgmoralesl@unadvirtual.edu.co
NICOLAS OTALORA TORRES
notalorat@unadvirtual.edu.co
LUIS ALBERTO BERMUDEZ ESCOBAR
labermudeze@unadvirtual.edu.co

RESUMEN: Este documento presenta la implementación y configuración integral de un firewall basado en Endian, detallando los procedimientos realizados para el establecimiento de políticas de seguridad perimetral. El trabajo incluyó la identificación de interfaces de red, verificación del estado del firewall, configuración de reglas de tráfico específicas para servicios HTTP y FTP, bloqueo de protocolos ICMP y la implementación de una arquitectura de red segmentada.

PALABRAS CLAVE: Endian, Firewall, WAN, LAN, protocolos, puertos, reglas, DMZ.

INTRODUCCIÓN: En el panorama actual de las redes de computadoras, la seguridad perimetral se ha convertido en un elemento fundamental para la protección de infraestructuras tecnológicas. Los firewall representan la primera línea de defensa en cualquier arquitectura de red moderna, actuando como barreras inteligentes que controlan el flujo de tráfico entre diferentes segmentos de red. La correcta configuración de estas herramientas es crucial para establecer políticas de seguridad efectivas que permitan el normal funcionamiento de los servicios mientras se mitigan potenciales amenazas.

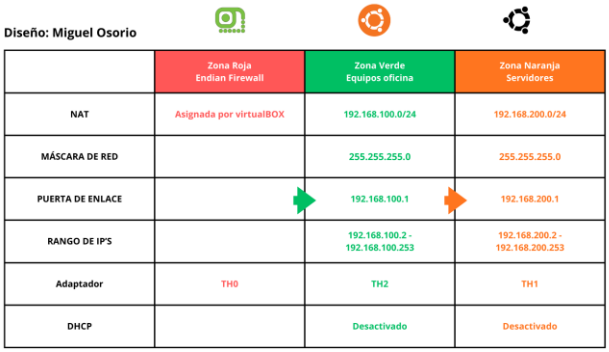
Este trabajo académico se centra en la implementación y configuración de un firewall basado en Endian, abordando los principios fundamentales de la seguridad de red. La creciente sofisticación de los ciberataques exige que los administradores de red comprendan no solo la teoría detrás de las políticas de seguridad, sino también su aplicación práctica en escenarios reales. A través de este proyecto, se explora la gestión integral de un firewall, desde su identificación inicial hasta la implementación de reglas específicas que balancean funcionalidad y protección

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

En esta fase abordaremos la configuración de una instancia de GNU/Linux Endian Firewall dentro de un entorno virtualizado utilizando VirtualBox, haciendo énfasis en la correcta asignación y gestión de las tarjetas de red. Endian es una solución de seguridad perimetral basada en Linux que permite segmentar y proteger redes mediante la implementación de distintas zonas. Para este proyecto se configuraron las tres zonas fundamentales: verde (LAN), destinada a la red interna; roja (WAN), encargada del acceso a internet; y naranja (DMZ), reservada para servidores expuestos. La implementación exitosa de estas zonas permite simular un entorno real de seguridad perimetral, comprender el flujo de tráfico entre redes y aplicar buenas prácticas en administración de sistemas y ciberseguridad

1.1 DISEÑO DE LA RED CON ENDIAN

Ilustración 1: arquitectura previamente diseñada para las zonas Verde (LAN), Roja y Naranaja (DMZ)

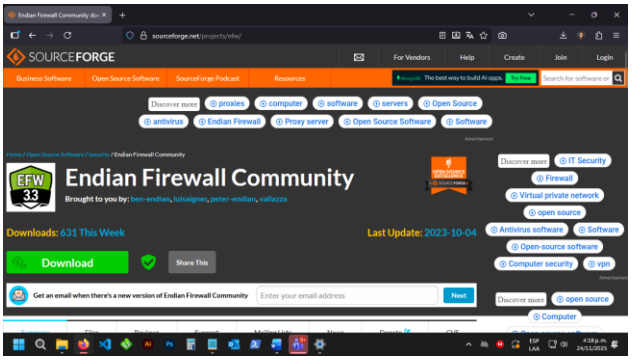


Fuente: autoría propia

1.2 CONFIGURACIÓN DE LA MAQUINA VIRTUAL CON ENDIAN

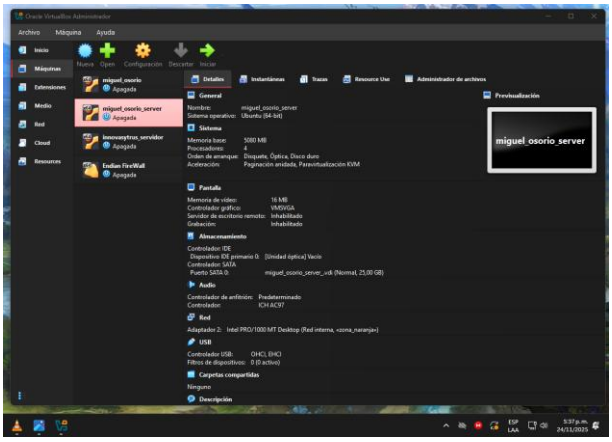
Descargamos la distribución Endian Firewall desde el sitio web oficial o directamente desde sourceforge. Usaremos VirtualBox para crear nuestra maquina virtual

Ilustración 2: descarga de Endian Firewall desde sourceforge



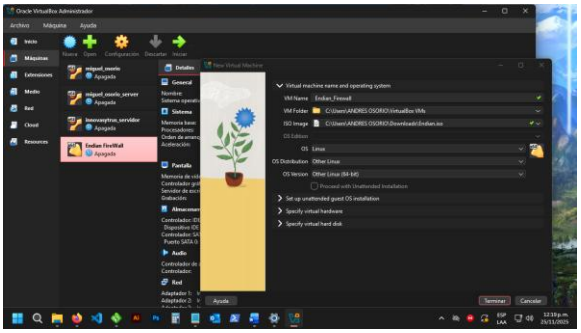
Fuente: autoría propia

Ilustración 3: VirtualBox y vamos a crear una nueva máquina virtual



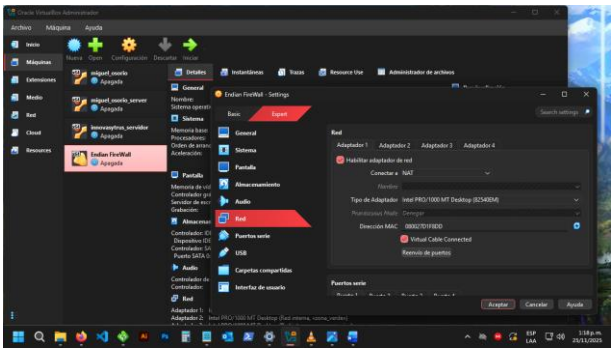
Fuente: autoría propia

Ilustración 4: Realizamos la configuración, eligiendo la imagen de disco que acabamos de descargar, seleccionamos Linux, luego other Linux para que funcione perfecto



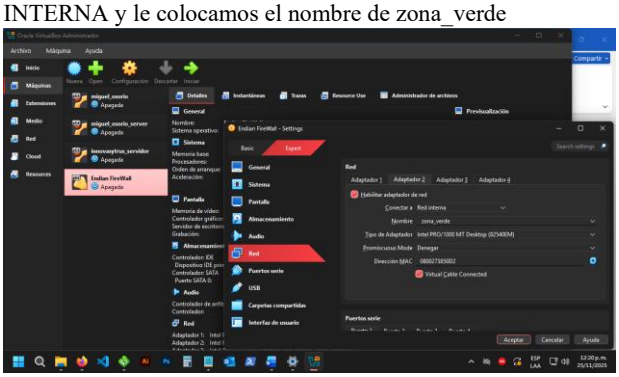
Fuente: autoría propia

Ilustración 5: Después de creado la MV vamos a configuración, luego en la opción RED y nos aseguramos que conectar A quede en NAT



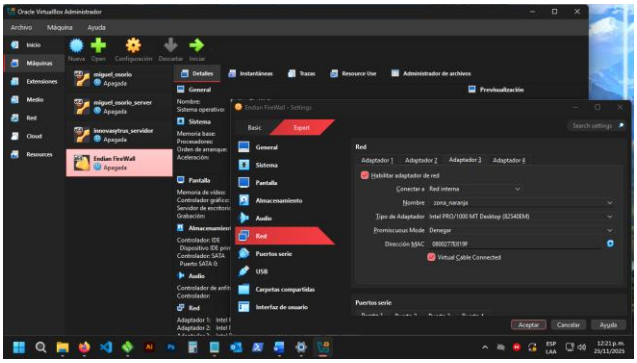
Fuente: autoría propia

Ilustración 6: dentro la misma opción de RED vamos a elegir la pestaña adaptador 2 y en Conectar a elegimos RED INTERNA y le colocamos el nombre de zona_verde



Fuente: autoría propia

Ilustración 7: Hacemos lo mismo en la pestaña del adaptador 3, Red Interna y como nombre zona_naranja, por último, pulsamos aceptar

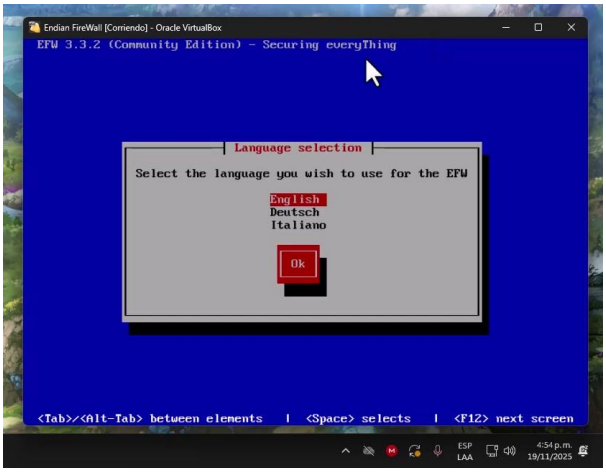


Fuente: autoría propia

1.3 INSTALACIÓN DE ENDIAN

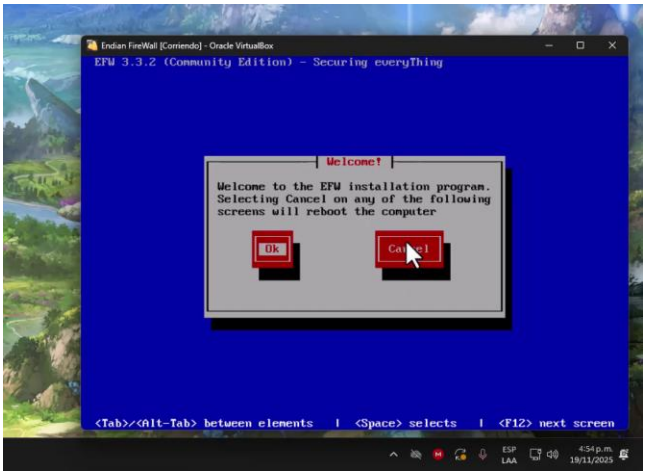
Instalar Endian por primera vez es bastante sencillo con los siguientes pasos se podrá levantar el firewall en nuestra red en pocos minutos

Ilustración 8: Ejecutamos la nueva máquina virtual creada. Tan pronto inicie nos mostrara las opciones de idiomas, elegiremos English



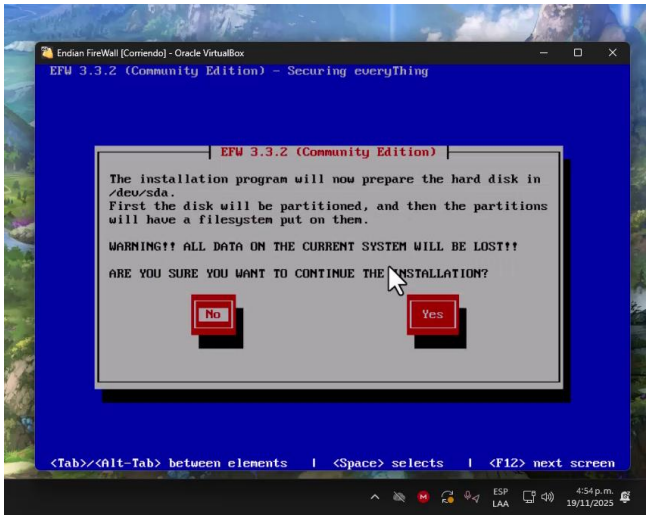
Fuente: autoría propia

Ilustración 9: Luego nos dará la bienvenida el instalador de Endian pulsamos OK



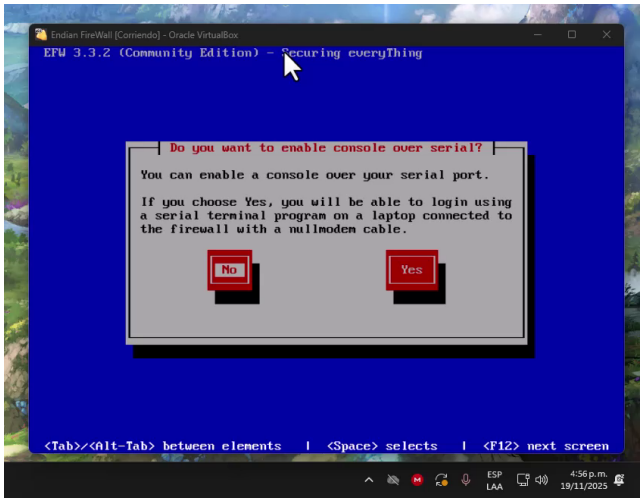
Fuente: autoría propia

Ilustración 10: Nos mostrara una advertencia de que el disco será formateado, pulsamos YES para continuar



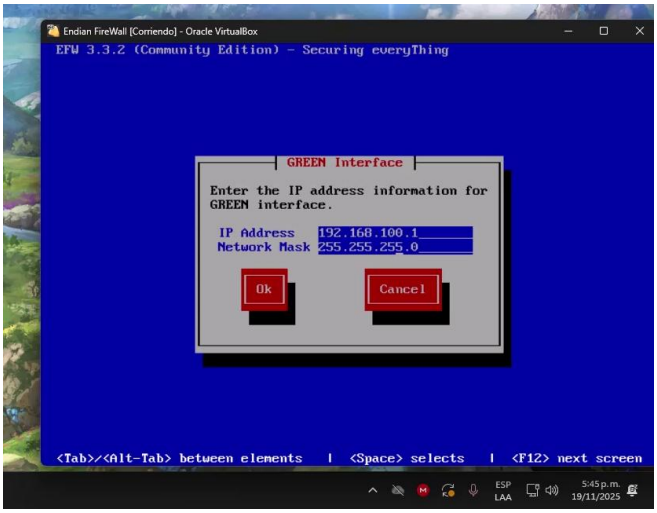
Fuente: autoría propia

Ilustración 11: Después de unos minutos nos mostrara esta opción de habilitar un puerto serial por consola por cual elegiremos No



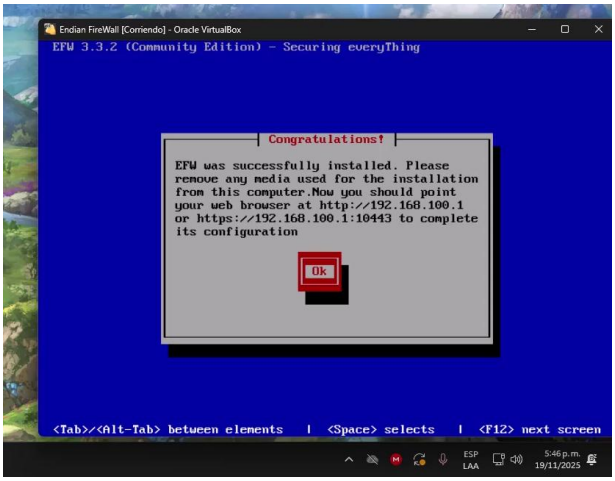
Fuente: autoría propia

Ilustración 12: luego de ellos nos pedirá ingresar la IP de la puerta de enlace de la Zona verde y la mascará de red. Estos datos están consignados en la tabla mostrada anteriormente



Fuente: autoría propia

Ilustración 13: Después de esto nos mostrara un mensaje de que Endian fue instalado correctamente mostrándonos la URL del administrador

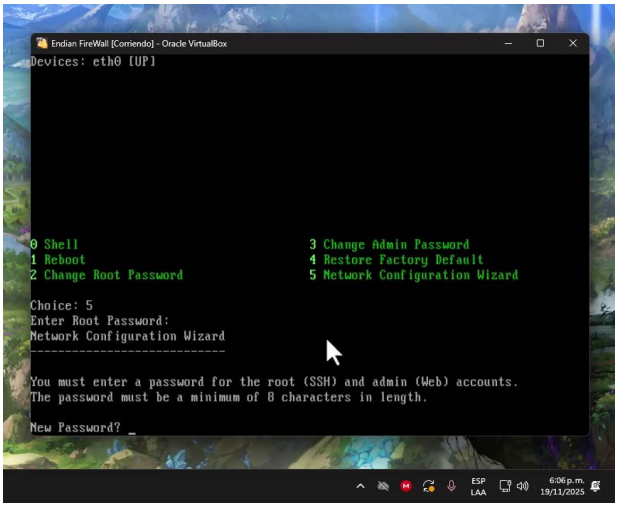


Fuente: autoría propia

1.4 CONFIGURACIÓN DE ENDIAN

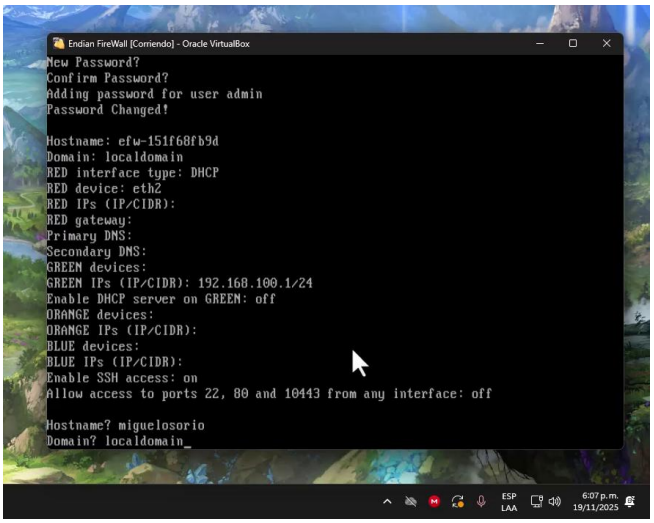
Después de la instalación haremos las primeras configuraciones para que los demás dispositivos se conecten correctamente con la RED

Ilustración 14: Luego de la instalación nos mostrara el menú de ENDIAN el cual vamos a elegir la opción 5: Asistente de configuración de Red. Nos pedirá que establezcamos una nueva contraseña para el administrador. La contraseña que esta por defecto es **endian**.



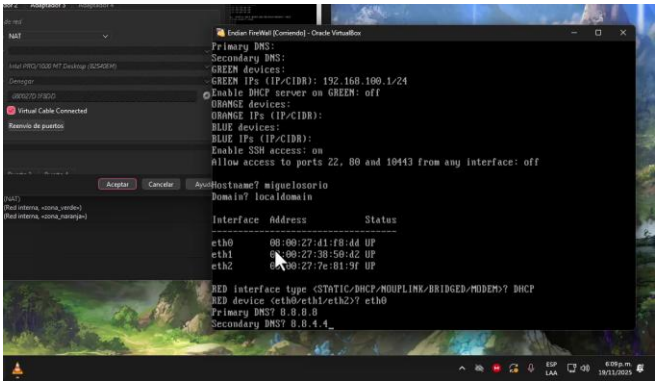
Fuente: autoría propia

Ilustración 15: Endian nos preguntara el nombre del hostname que le asignaremos a nuestro firewall, en el cual pondremos una a gusto, y un domain dejaremos por defecto como localdomain



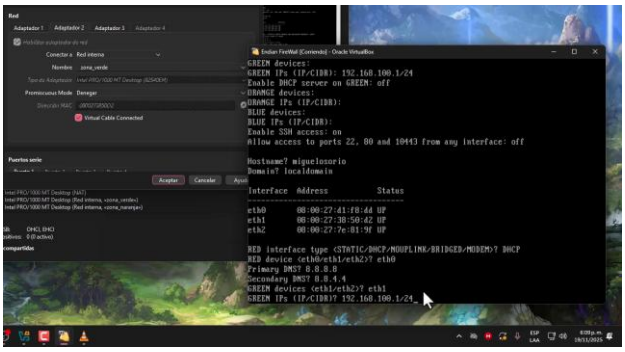
Fuente: autoría propia

Ilustración 16: Luego de ello nos pedira la configuración de la zona roja (WAN) primero nos preguntara que tipo de interfaz es a lo que elegiremos DCHP. Que dispositivo elegiremos, entonces comparamos la tabla con la Direccion MAC de el adaptador 1 de la MV del firewall de ENDIAN. Para nuestro ejemplo es eth0. Lo siguiente que elegiremos son los DNS primarios y secundarios que para el caso usaremos los de GOOGLE.



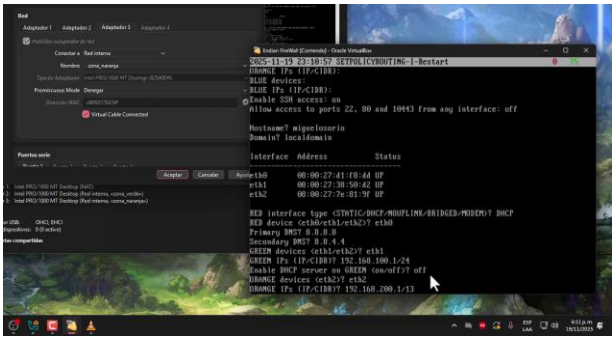
Fuente: autoría propia

Ilustración 17: Repetimos lo mismo para la Zona verde. Green Device ahora es eth1 ya que es la misma dirección MAC que el adaptador 2, y usaremos la puerta de enlace que esta se rellena automáticamente



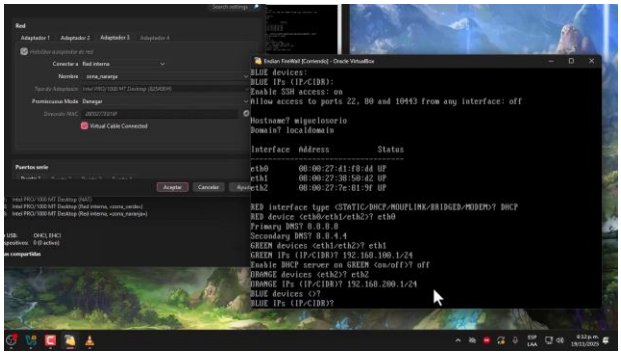
Fuente: autoría propia

Ilustración 18: Nuevamente repetimos para la zona naranja, usando eth2 como device ya que es el ultimo que queda para elegir. Usamos la IP de la puerta de enlace para la misma zona que fue establecida previamente en el diseño de la red.



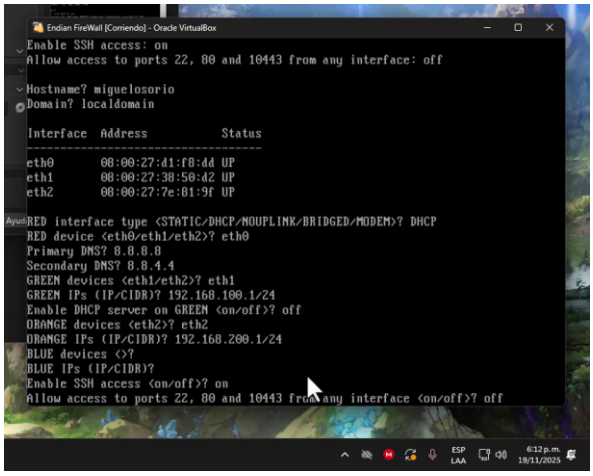
Fuente: autoría propia

Ilustración 19: Luego se pide configurar la zona azul. Blue Devices lo cual en est



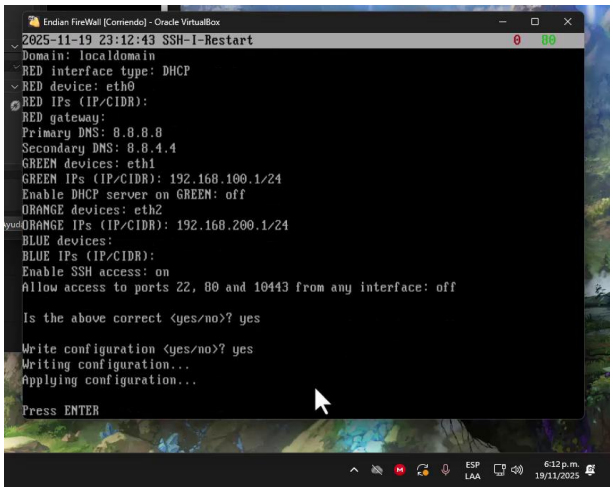
Fuente: autoría propia

Ilustración 20: luego de establecer las zonas, nos preguntara si deseamos activar el acceso SSH por lo que pondremos ON. Y también nos preguntara si dejamos los puertos 22, 80 y 10443 para cualquier interfaz, a lo que elegiremos off



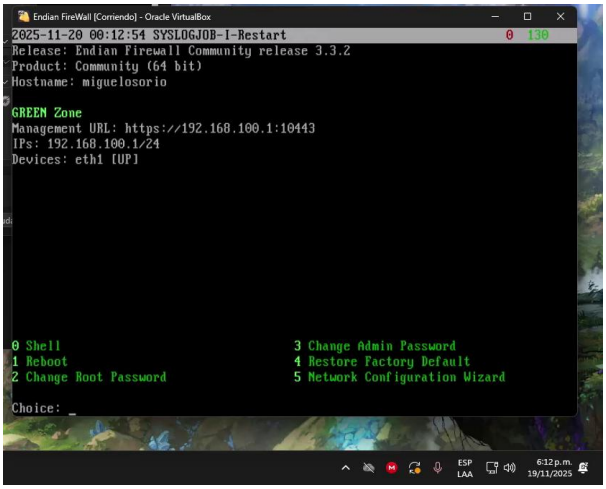
Fuente: autor

Ilustración 21: Por ultimo nos preguntara que si toda la configuración esta correcta, por lo que pondremos yes y luego nos preguntara que si escribimos la configuración, igualmente elegimos yes. Endian escribirá y aplicará la configuración y al finalizar deberemos pulsar ENTER.



Fuente: autoría propia

Ilustración 22: Endian reestablecerá los servicios y con eso ya se podrá iniciar a configurar los demás dispositivos en la red.



Fuente: autoría propia

2 Configuración NAT

En proceso y desarrollo de estrategias eficaces para la seguridad de las redes, la configuración NAT (Network Addres Translation / Traducción de Direcciones de Redes), brinda una solución eficaz a esta problemática, mediante el uso de Endian (firewall), se garantiza que las distintas zonas tanto la red interna (LAN), como la zona desmilitarizada (DMZ) tengan acceso seguro a internet (red WAN) sin poner en peligro la seguridad de las distintas zonas, esto gracias a una administración eficaz de las reglas de seguridad.

2.1 ARQUITECTURA DE RED

Tabla 1

Zona	Interfaz VirtualBox	Tipo de Red VirtualBox	Rango IP
Verde (LAN)	Adaptador 2	Red Interna	192.168.100.2/24
Naranja (DMZ)	Adaptador 3	Red interna	192.168.200.2/24
Roja (WAN)	Adaptador 1	Red NAT	10.0.2.15/24

Fuente: autoría propia

2.2 FUNDAMENTOS DE LA RED NAT

La red NAT permite que dispositivos conectados a una red privada, puedan compartir una única conexión a internet por medio de una IP publica, esto permite que Endian por medio de una IP distinta a la que comparten las zonas que la componen puede salir a internet (WAN), generando conexión a los dispositivos conectados a él, pero ocultando la dirección real de ellos ante la WAN.

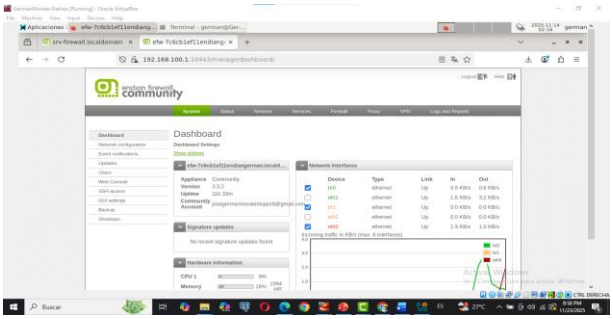
2.3 REENVIO DE PUERTOS

Este servicio permite un acceso de manera limitada a las redes LAN internas desde la WAN, el reenvió de puertos permite el tráfico especifico según lo requiera cada máquina, concediendo así permisos o no mediante la aplicación de protocoles de red implementados en reglas creadas por el usuario, o usando unas ya predeterminadas si así lo requiere la situación a resolver, el firewall funciona como una especie de enrutador que envía cada petición al servidor interno que fue preparado para ello.

2.4 CONFIGRUACION DE REGLAS

Este función ayuda a restringir u otorgar permisos a los servidores, mediante el uso de Endian podemos crear reglas de firewall, lo primero a llevar a cabo es elegir la zona u zonas en cuestión a quienes deseamos que se apliquen dichos cambios, después seleccionamos el servicio o puerto que deseamos aplicar bien sea HTTP, FTP, IMAC entre muchos, posteriormente elegimos el protocolo UDP, TCP, GRE entre otras opciones, por ultimo elegimos el tipo de política y guardamos los cambios para que nuestra regla sea agregada al listado de reglas ya existentes.

Ilustración 23: Dashboard Endian



Fuente: autoría propia

Ilustración 24: Creación de Reglas

Fuente: autoría propia

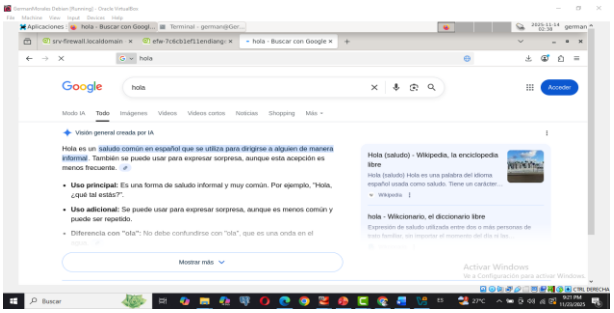
Ilustración 25: Creación servicios y protocolos

Fuente: autoría propia

2.5 COMUNICACIÓN DE LA ZONA NARANJA A INTERNET

La comunicación a internet por medio de un servidor es de vital importancia, así que la restricción en las reglas no debería impedir el acceso a internet, dado que muchos de estos servidores alojan servicios que deben estar expuestos fuera de la red segura, tales como servicios FTP, HTTPS entre muchos otros, por tal motivo el garantizar la conexión a la zona WAN es de carácter prioritario.

Ilustración 26: conexión a internet

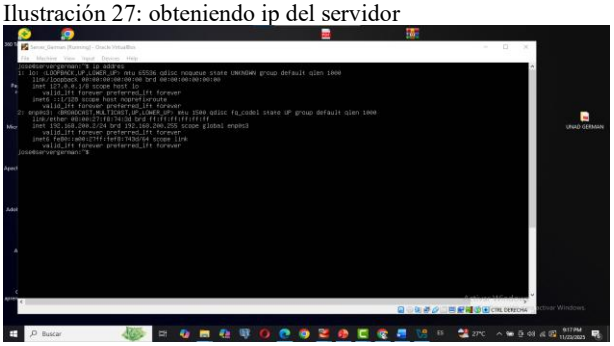


Fuente: autoría propia

2.6 VERIFICACION DE LA CONEXIÓN ENTRE EQUIPOS DE LA ZONA

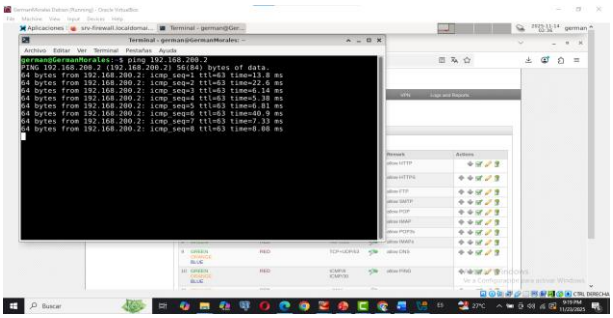
Así como es de vital importancia la comunicación de los equipos a internet, también se hace necesario una comunicación fluida entre los equipos de las zonas existentes, una manera eficaz de saber si hay comunicación es mediante el envió de paquetes, obtenemos la ip de un equipo por medio del comando ip addres y le hacemos un ping desde otro equipo para verificar el reenvió de paquetes es válido.

Ilustración 27: obteniendo ip del servidor



Fuente: autoría propia

Ilustración 28: generando ping para envío de paquetes



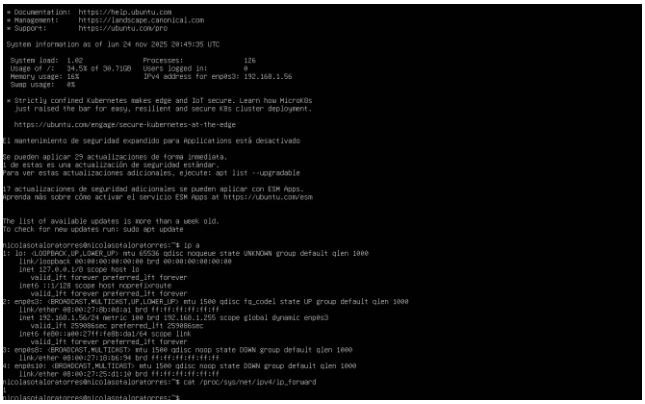
Fuente: autoría propia

3 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

El propósito de esta práctica fue configurar un servidor en DMZ que permitiera las solicitudes HTTP y FTP provenientes de la LAN, mientras se aplicaban políticas de bloqueo al tráfico ICMP para evitar respuestas a comandos de ping.

3.1 IDENTIFICAR LA INTERFAZ DE RED

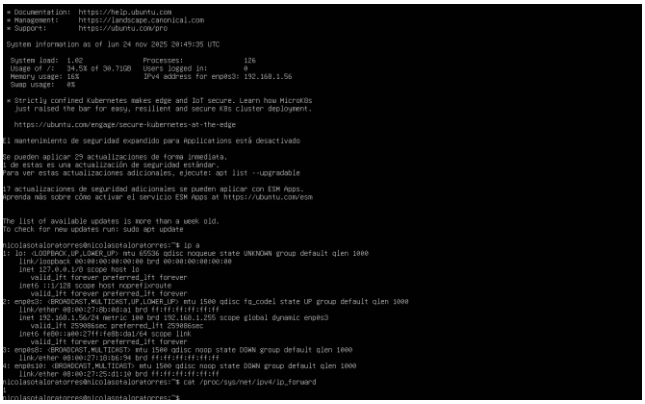
Ilustración 29: Para poder identificar la interfaz de red ingresamos el comando ip a el cual nos generará una lista, en dicha lista buscaremos nuestra ip la cual es 192.168.1.56/24



Fuente: autoría propia

3.2 VERIFICAR SI EL SERVIDOR ACTÚA COMO FIREWALL

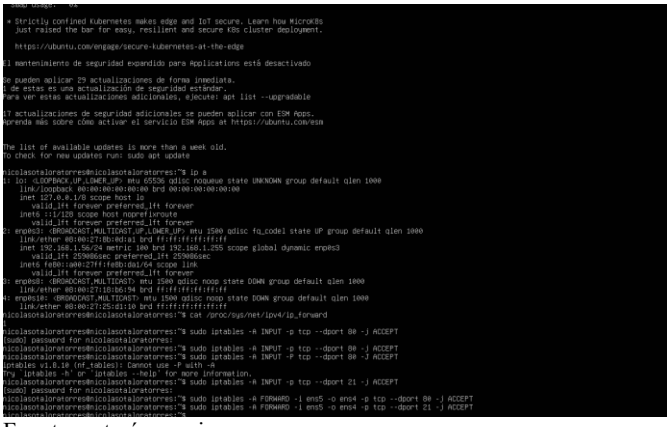
Ilustración 30: Para verificarlo debemos hacerlo con el mismo comando ip a, esto lo sabremos mirando el número de interfaces activas, si tiene 1 sola interfaz entonces no es firewall, pero si tiene 2 o más entonces si es firewall, en el caso de que sea firewall verificaremos que tenga habilitado el reenvío de paquetes con el comando cat /proc/sys/net/ipv4/ip_forward, al activarlo nos podrá dar dos resultados 0 el reenvío de paquetes está desactivado y 1 el reenvío de paquetes está activado.



Fuente: autoría propia

3.3 PERMITIR TRÁFICO HTTP Y FTP HACIA UN SERVIDOR EN LA DMZ

Ilustración 31: Ahora debemos Permitir tráfico HTTP (Puerto 80) y Permitir tráfico FTP (Puerto 21), abriendo únicamente los puertos necesarios que son el 80 y 21.



Fuente: autoría propia

Permitir HTTP (80)
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

Permitir FTP (21)
sudo iptables -A INPUT -p tcp --dport 21 -j ACCEPT

El tráfico viene desde otra red
sudo iptables -A FORWARD -i ens5 -o ens4 -p tcp --dport 80 -j ACCEPT
sudo iptables -A FORWARD -i ens5 -o ens4 -p tcp --dport 21 -j ACCEPT

3.4 BLOQUEAR ICMP (PING)

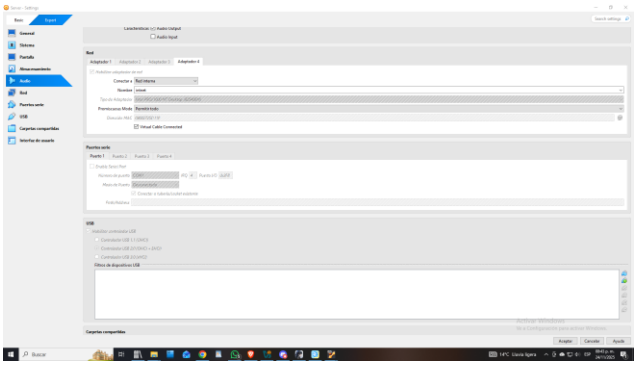
Procedemos a bloquear el ICMP, para evitar ataque o posibles visitantes.

Bloquear solicitud de ping
sudo iptables -A INPUT -p icmp --icmp-type 8 -j DROP
sudo iptables -A FORWARD -p icmp --icmp-type 8 -j DROP

Bloquear respuesta de ping (tipo 0):.
sudo iptables -A INPUT -p icmp --icmp-type 0 -j DROP
sudo iptables -A FORWARD -p icmp --icmp-type 0 -j DROP

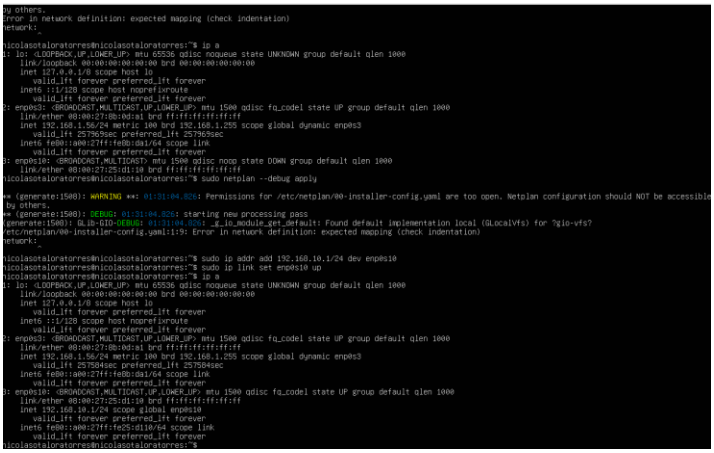
3.5 CONFIGURAMOS LAS REDES Y LAS IP

Ilustración 32: En virtualBox, entramos a configuración-redes: adaptador 1 y adaptador 4, uno con adaptador puente y el otro con red interna.



Fuente: autoría propia

Ilustración 33: Configuramos la Ip manualmente con el comando sudo ip **addr add 192.168.10.1/24 dev enp0s10,** activamos **interfaz sudo ip link set enp0s10** up y **ip a**



Fuente: autoría propia

3.6 COMPROBAR QUE FUNCIONA

Ilustración 34: Ingresamos desde el navegador a http://192.168.10.1

Fuente: autoría propia

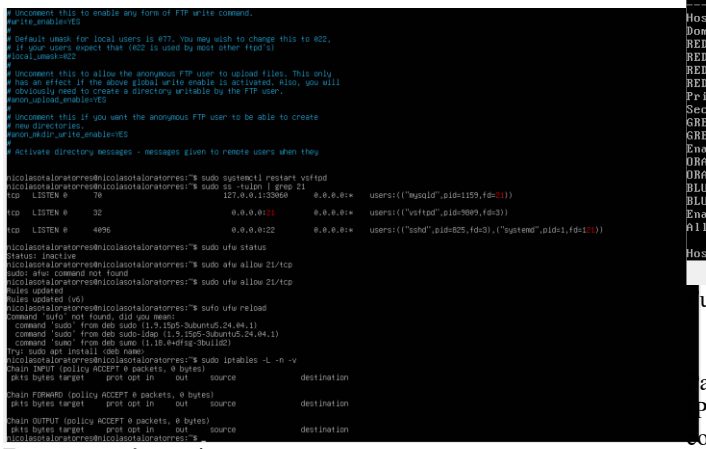
3.7 DEMOSTRAR QUE EL PING ESTÁ BLOQUEADO

Ilustración 35: Hacemos ping a 192.168.10.1

Fuente: autoría propia

3.8 REGLAS DEL FIREWALL

Ilustración 36: Ingresamos el comando sudo iptables -L -n -v

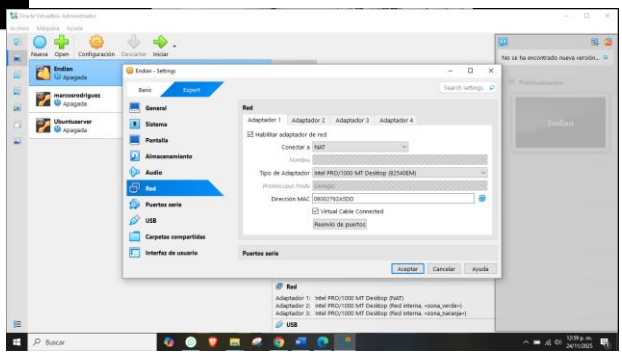


Fuente: autoría propia

REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO.

Para el desarrollo de esta etapa, es necesario descargar e stalar el Endian y configurar en sus puertos de red, el aptador 1 en NAT, con el fin de brindar y recibir el acceso a terne a través de él, el adaptador 2 debe ser puesta en la red terna, la cual designaremos como zona_verde y el adaptador dentro de la red interna, lo designaremos como na_naranja.

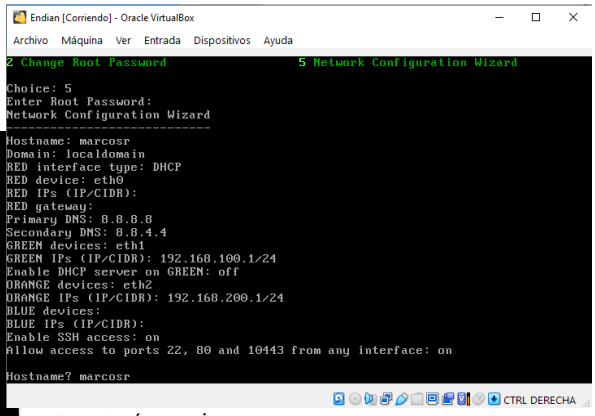
stración 36: configuración de adaptadores



Fuente: autoría propia

Posterior a la configuración de los adaptadores, se procede a ingresa a Endian y realizr la configuración de los puertos eth0, eth1 y eth2 respectivamente, se han seleccionado las IP asignadas a cada uno de ellos como se estableció en el trabajo colaborativo con las fases anteriores.

Ilustración 37: configuración de ips

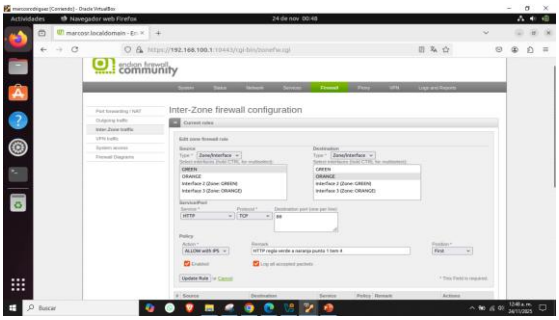


uente: autoría propia

aso seguido, se ingresa en el navegados de Ubuntu desktop la P configurada para la zona verde y adicionando el puerto de onexión 10443, ingresando como http://192.168.100.1:10443, se debe ingresar usuario y contraseña, anteriormente definidos, y a continuación, se selecciona el menú de firewall, luego Inter-zone traffic, y se adiciona una nueva regla para poder ingresar a establecer los requisitos de conexión utilizando

HTTP como se muestra en la imagen a continuación y se selecciona el puerto 80.

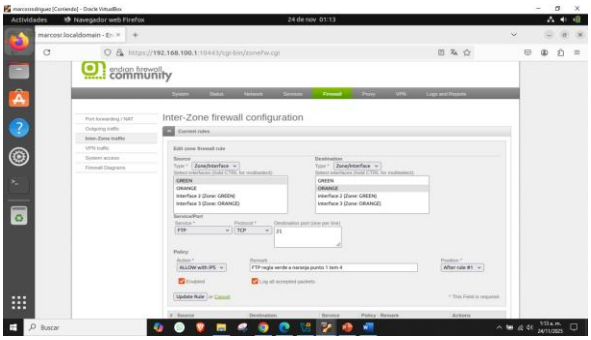
Ilustración 38: comunicación zona verde - naranja



Fuente: autoría propia

Se agrega una nueva regla y en esta se configura el servicio FTP y el puerto se selecciona el 21. Esto con el objetivo de vincular la zona_verde con la zona_naranja y que se establezca el enlace.

Ilustración 39: configuración zona verde-naranja ftp

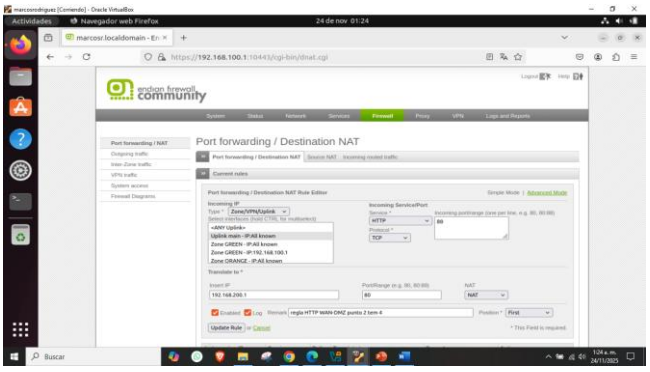


Fuente: autoría propia

4.1 COMUNICAR LA ZONA INTERNET CON LA ZONA DMZ

Acto seguido, se procede a ingresar en la pestaña de Port Forwarding/NAT, aquí se configura una nueva regla seleccionando Uplink main – IP ALL knuwn, seleccionamos el protocolo HTTP y el puerto 80.

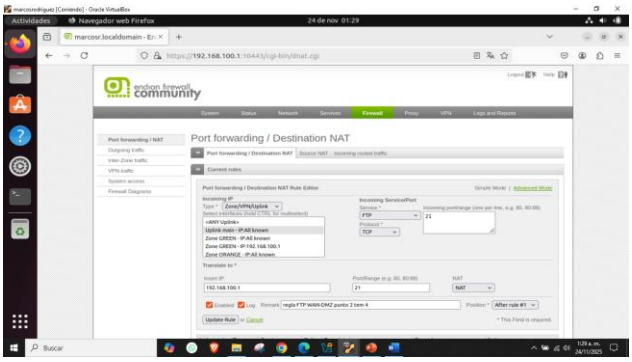
Ilustración 40: internet con la zona DMZ



Fuente: autoría propia

Para establecer la siguiente regla necesaria, únicamente modificamos el protocolo FTP y hacemos uso del puerto 21. Con estas configuraciones estamos comunicando la Zona Internet con la Zona DMZ.

Ilustración 41: internet con la zona FTP



Fuente: autoría propia

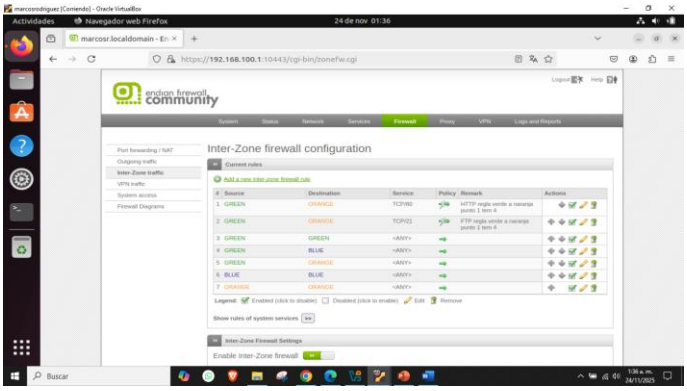
4.2 VERIFICAR EN EL TRÁFICO INTER-ZONA, LA CREACIÓN DE LAS REGLAS.

En las siguientes capturas de pantalla, se logra evidenciar que fueron creadas la reglas y que se establece es tráfico Inter-Zona con el cual se realizará el control de seguridad.

Se revisó la creación de las reglas en el firewall y se comprobó que estuvieran siendo aplicadas correctamente. Esto incluyó:

- Validar que solo los puertos autorizados estuvieran habilitados.
- Comprobar que el tráfico no permitido fuera bloqueado.
- Consultar registros (logs) para asegurarse de que el firewall estuviera actuando según lo configurado.

Ilustración 42: tráfico Inter-Zona, la creación de las reglas.



Fuente: autoría propia

4.3 PROBAR DESDE UN NAVEGADOR WEB, LAS SIGUIENTES DIRECTIVAS:

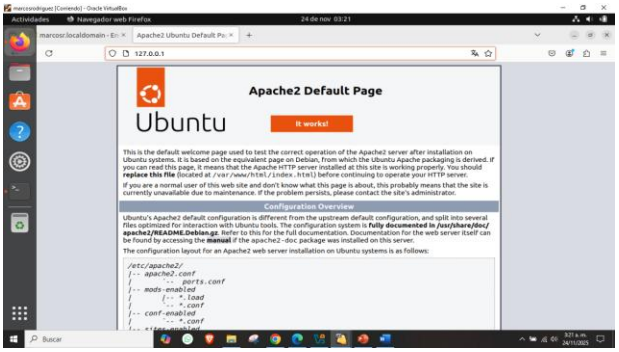
Para confirmar el correcto funcionamiento de todas las configuraciones, se realizaron distintas pruebas de acceso, entre ellas. Cada prueba permitió validar que las reglas fueran efectivas, confirmando que solo se podía acceder a los servicios desde las zonas permitidas y que la segmentación de la red funcionaba adecuadamente.

El ingreso del servicio HTTP desde la LAN hacia la zona DMZ.

En esta prueba se validó que los equipos ubicados en la **zona Verde (LAN)** pudieran acceder al servidor web alojado en la **zona Naranja (DMZ)** mediante el protocolo **HTTP (puerto 80)**.

- Se creó una regla de firewall que permitiera tráfico desde la red 192.168.100.1 (LAN) hacia la subred de la DMZ.
- El tráfico permitido estaba limitado exclusivamente al puerto **80/TCP**.
- Desde un navegador en la LAN se ingresó a la IP del servidor web de la DMZ.
- Se confirmó que el servidor respondió correctamente y la regla quedó registrada en el tráfico inter-zona.

Ilustración 43: servicio HTTP desde la LAN hacia la zona DMZ



Fuente: autoría propia

El acceso fue exitoso, confirmando que la DMZ está accesible desde la LAN, lo cual es típico cuando los usuarios internos necesitan consultar servicios corporativos alojados en una zona intermedia y controlada.

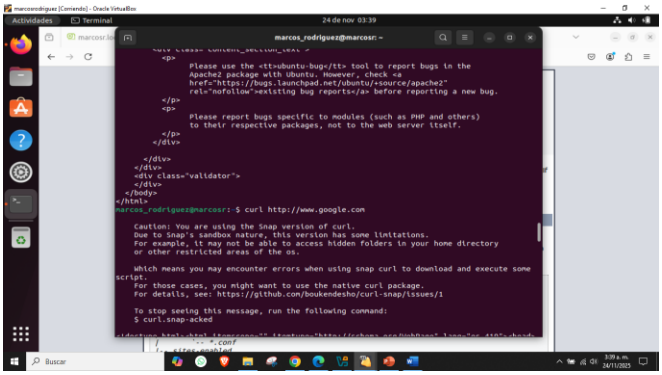
El ingreso del servicio HTTP desde la LAN hacia la WAN.

Esta prueba se enfocó en confirmar que los usuarios internos de la LAN tuvieran acceso normal a sitios web de Internet mediante HTTP.

¿Qué se realizó?

- Se habilitó una regla que permitiera tráfico HTTP desde la LAN hacia direcciones públicas.
- Se realizó una prueba ingresando a una página web externa (por ejemplo http://www.google.com).
- Se verificó en las tablas del firewall que el tráfico se estaba enroutando correctamente como salida a la WAN.

Ilustración 44: servicio HTTP desde la LAN hacia la WAN



Fuente: autoría propia

El acceso a Internet funcionó sin restricciones adicionales, lo que demuestra que la política de salida desde la LAN hacia la WAN está operativa y correctamente controlada por el firewall.

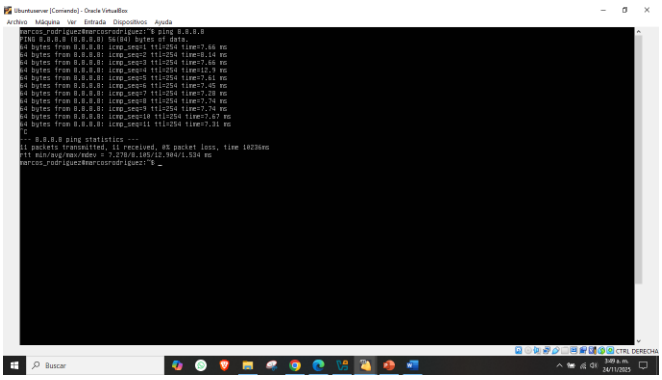
El ingreso del servicio HTTP desde la zona DMZ hacia la WAN.

En este punto se comprobó que los servidores ubicados en la **DMZ** pudieran realizar solicitudes hacia Internet. Esto suele ser necesario para actualizaciones, descargas de paquetes o sincronización de servicios.

¿Qué se realizó?

- Se creó una regla que permitiera tráfico saliente desde la DMZ hacia la WAN por el puerto HTTP.
- Desde el servidor o equipo en la DMZ se intentó ingresar a una página web pública.
- Se monitorearon las reglas activas para confirmar que el tráfico era permitido y registrado.

Ilustración 45: servicio HTTP desde la zona DMZ hacia la WAN



Fuente: autoría propia

La DMZ pudo acceder a recursos HTTP externos, manteniendo un flujo controlado y evitando accesos entrantes no autorizados.

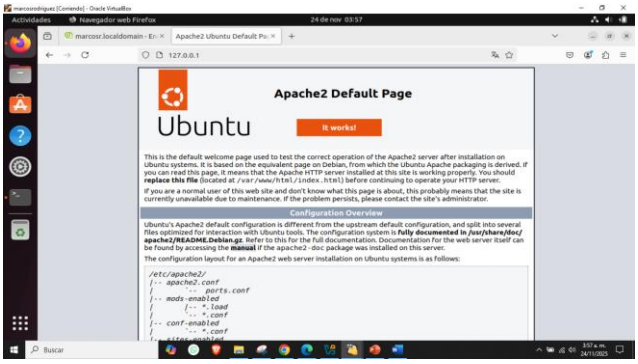
El ingreso del servicio HTTP desde la WAN hacia la zona DMZ.

Este es uno de los escenarios de seguridad más importantes, ya que implica publicar un servicio al público externo.

¿Qué se realizó?

- Se configuró una regla de **entrada** desde cualquier dirección pública hacia la IP del servidor web en la DMZ.
- Se limitó estrictamente al puerto **80/TCP**, evitando exponer otros servicios.
- Se realizó la prueba intentando acceder desde una máquina simulada en Internet.

Ilustración 46: servicio HTTP desde la WAN hacia la zona DMZ



Fuente: autoría propia

El servidor web fue accesible desde Internet, confirmando que los servicios alojados en la DMZ se encuentran publicados correctamente mientras se mantiene una capa de protección que evita el acceso directo a la LAN.

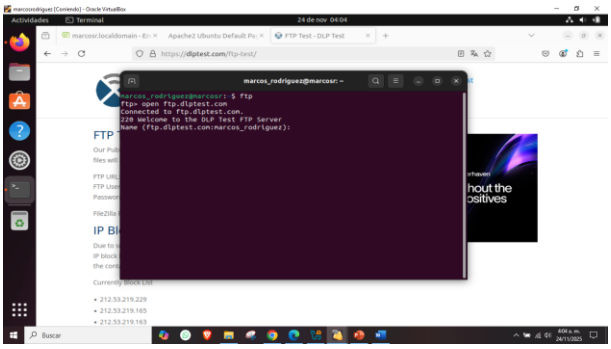
El ingreso del servicio FTP desde la LAN hacia la WAN.

Finalmente, se verificó la conectividad del protocolo **FTP** desde usuarios internos hacia servidores externos en Internet.

¿Qué se realizó?

- Se creó una regla para permitir tráfico FTP desde la LAN hacia Internet (puertos 20 y 21 TCP).
- Desde un cliente FTP local se intentó establecer una conexión con un servidor público.
- Se verificó en el firewall que las conexiones se estaban estableciendo correctamente.

Ilustración 47: servicio FTP desde la LAN hacia la WAN



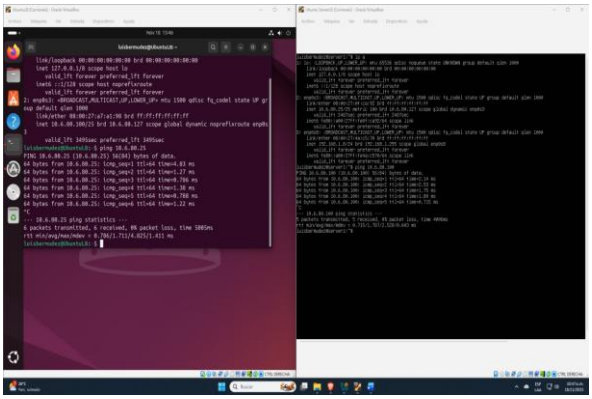
Fuente: autoría propia

El servicio funcionó correctamente, mostrando que la LAN tiene acceso controlado a servicios FTP externos, útil para transferir archivos a sitios remotos cuando es necesario.

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

Escriba su texto en Times News Roman de 9 Pts, espacio simple. No utilice el doble espaciamiento. Todos los párrafos deberán iniciar con una sangría de 0.75 cm en el primer renglón

Ilustración 48: Verifica conectividad entre cliente y servidor

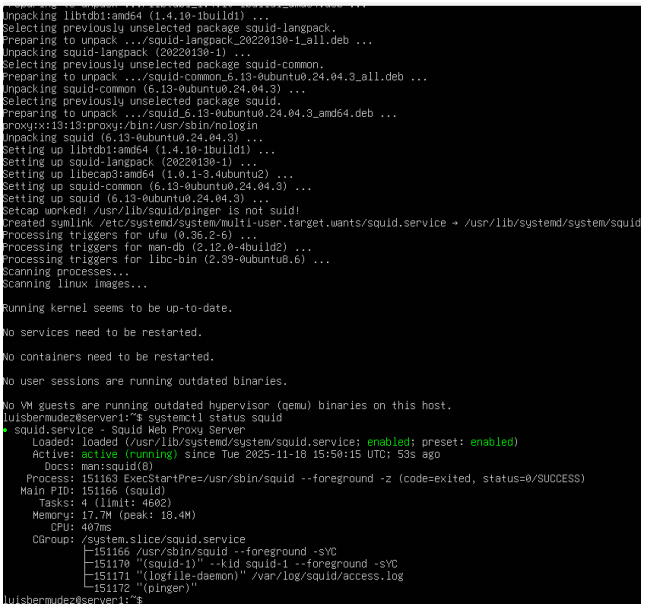


Fuente: autoría propia

5.1 INSTALACIÓN DEL SERVIDOR PROXY SQUID

Ilustración 49: Realizamos los siguientes comandos para realizar un update al sistema e instalamos squid:

sudo apt update
sudo apt install squid -y

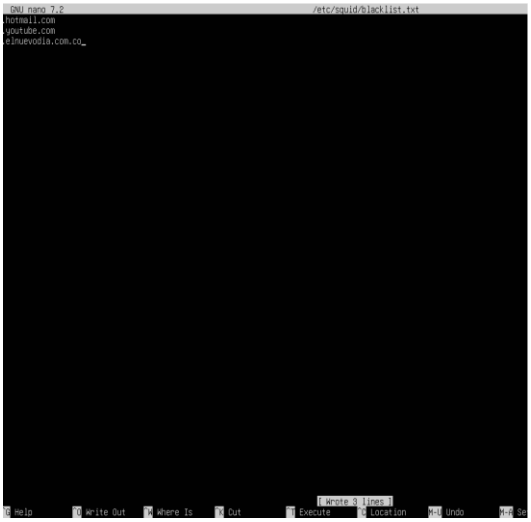


Fuente: autoría propia

Luego validamos que este activo con el comando systemctl status squid

5.2 CREAR LISTA NEGRA DE SITIOS BLOQUEADOS

Ilustración 50: Creamos el archivo: sudo nano /etc/squid/blacklist.txt

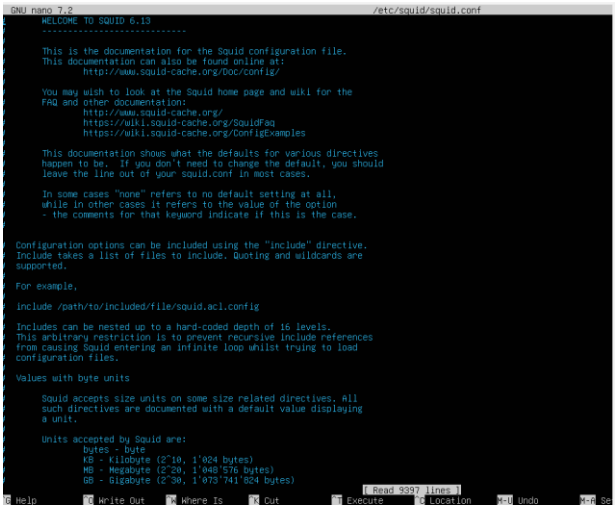


Fuente: autoría propia

Guardamos los cambios bloqueando los enlaces:
.hotmail.com
.youtube.com
.elnuevodia.com.co

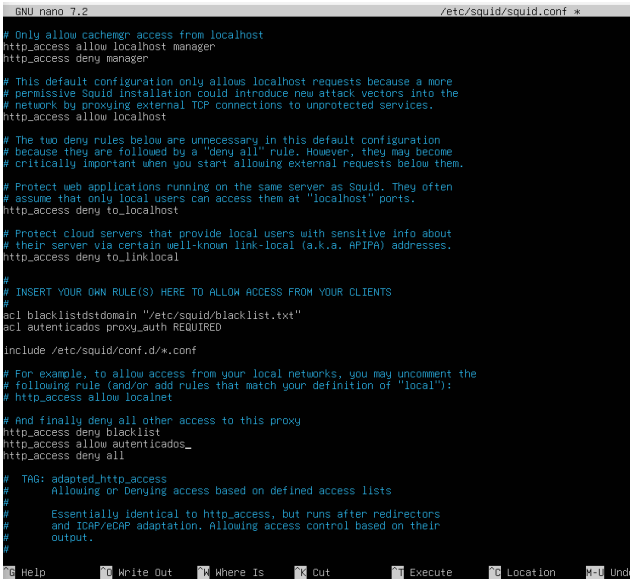
5.3 CONFIGURACIÓN DE SQUID

Ilustración 51: Editamos la configuración del archivo sudo nano /etc/squid/squid.conf



Fuente: autoría propia

Ilustración 52: Agregar (en la parte de ACL y http_access): acl blacklist dstdomain "/etc/squid/blacklist.txt" http_access deny blacklist



Fuente: autoría propia

http_access deny blacklist
http_access allow autenticados

MUY IMPORTANTE: debe ir antes del allow de autenticación.

5.4 CONFIGURACIÓN DE AUTENTICACIÓN POR USUARIO

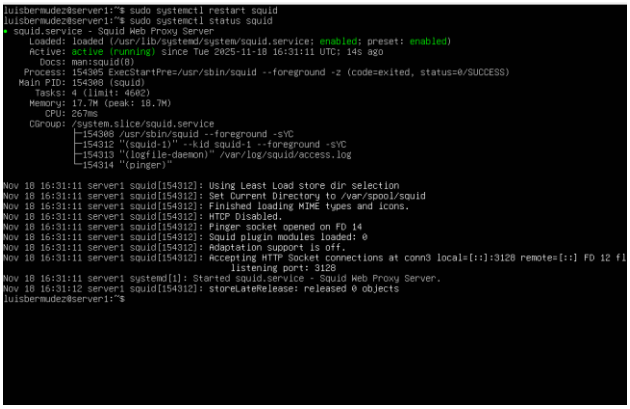
Instalar paquete para manejar contraseñas
sudo apt install apache2-utils -y

Crear archivo de credenciales
sudo htpasswd -c /etc/squid/users.list usuario1

Activar autenticación básica en Squid (squid.conf)

Agregamos estas líneas:
auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/users.list auth_param basic realm ProxyAuth
auth_param basic credentialsttl 2 hours

Ilustración 53: Reiniciamos los servicios de squid, nos debe dar nuevamente active



Fuente: autoría propia

5.5 CONFIGURACIÓN DEL NAVEGADOR DEL CLIENTE Y REALIZACIÓN DE PRUEBAS

Firefox → Configuración → Red → Configuración → Proxy manual: Al abrir cualquier sitio pedirá:

- usuario → usuario1
- contraseña → la que configuraste

Ilustración 54: Configuración en el navegador Cliente

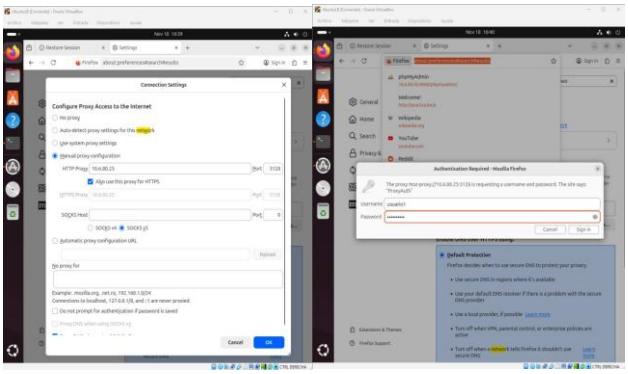
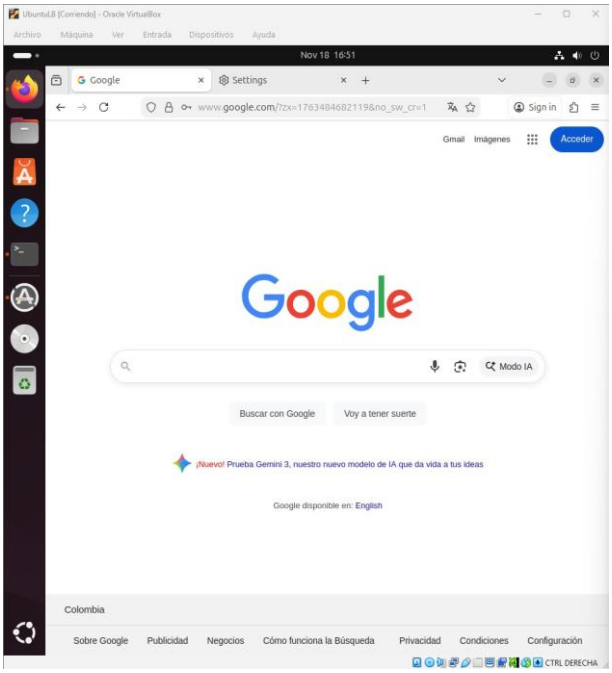
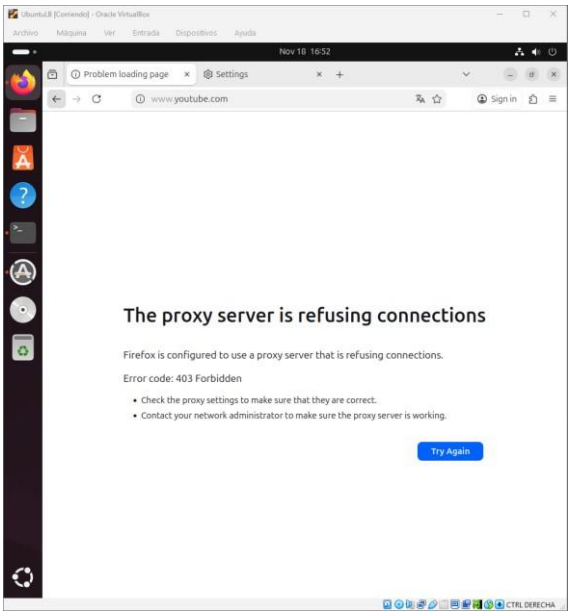

Fuente: autoría propia

Ilustración 55: Probando sitio permitido



Fuente: autoría propia

Ilustración 56: Sitios Bloqueados



Fuente: autoría propia

6 CONCLUSIONES

En la temática 1 se diseño la arquitectura de la red a trabajar con Endian y se delimito las zonas con las que se agrupo en ROJA para la WAN, VERDE para LAN y NARANJA para DMZ. A su vez se instalo y configuro Endian de forma correcta en al red

En la temática 2 La red NAT permite la comunicación segura de nuestras zonas, Endian es una herramienta poderosa que

permite establecer conexión o restringirla según sea la necesidad de un caso en concreto, pero esto no limita el potencial de nuestros equipos, dado que las reglas permiten una navegación segura y eficaz, aprovechando el uso de la WAN, pero sin exponer a la LAN a posibles intromisiones o daños por ataques maliciosos.

La clave de dicho porcentaje de éxito recae en la correcta administración y aplicación de las reglas en las distintas zonas que componen nuestra red.

En la temática 4 El haber implementado las reglas de firewall entre las zonas establecidas como LAN, DMZ y WAN, permitió poder establecer un entorno seguro y controlado, donde cada servicio funciona únicamente bajo las condiciones previstas y sin afectar servidores o datos de personas y equipos reales. Las pruebas realizadas demostraron que el diseño segmentado de la red cumple adecuadamente con los principios de seguridad en redes: aislamiento, control de accesos y monitoreo del tráfico, convirtiéndose en una herramienta de aprendizaje satisfactorio y que cumplió con los objetivos declarados.

La implementación de la Temática 3 permitió comprobar que la configuración de una DMZ aporta un nivel significativo de seguridad y control dentro de la infraestructura de red.

En la temática 5 se configuro un servidor Proxy llamado Squid el cual permite bloquear y permitir acceso a sitios dentro de la misma red, una forma de mantener seguro el mismo entorno.

7 REFERENCIAS

Cervelión, Á. J. (2023). Instalación de Nagios Core 4.4 en Ubuntu 22.04 . [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/54230

Jay LaCroix. (2020). Mastering Ubuntu Server : Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server . Packt Publishing. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b4195

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

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

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

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

LPI LPIC-1 Exam 101. (2022). Tema 102: Comandos GNU y Unix . https://learning.lpi.org/es/learning-materials/101-500/102/