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

Oscar Eduardo Cruz oecruz@unadvirtual.edu.co
Armando Romero Sua aromeros0@unadvirtual.edu.co
Wilson Eladio Velásquez Guerrero wevelasquezg@unadvirtual.edu.co
Carlos Alberto Avendaño Buitrago Ca79ave621@unadvirtual.edu.co
Edward Laiton Zarate elaitonz@unadvirtual.edu.co

RESUMEN: *Este artículo evidencia la configuración e implementación de una instancia para GNU/Linux Endian en una máquina Virtual ejecutada desde VirtualBox. Se mencionan uno a uno los pasos para establecer adecuadamente las tarjetas de red en las zonas verde (LAN), roja (WAN) y naranja (DMZ), aplicando la segmentación seleccionada por el grupo de trabajo entregando una solución efectiva para los tres entornos, en donde Endian utilizado como un firewall filtra cada una de las conexiones y regula el tráfico de entrada y salida de los datos, evitando así que cualquier equipo o tráfico malicioso pueda acceder al servidor y sus unidades dependientes o estaciones de trabajo. El resultado de esta configuración es un entorno de Linux seguro en donde todo lo que se ingresa y todo lo que sale de la red es filtrado por Endian en su función de firewall.*

PALABRAS CLAVE: Endian, Firewall, Segmentación, DMZ.

1. INTRODUCCIÓN

La presente práctica aborda el diseño e implementación de una arquitectura de red segura en un entorno virtualizado, tomando como eje central el uso de Endian Firewall como solución perimetral basada en GNU/Linux. Para ello, se construyó una infraestructura segmentada en tres zonas bien definidas: zona verde (LAN), destinada a los clientes internos; zona naranja (DMZ), reservada para los servidores expuestos; y zona roja (WAN), correspondiente al acceso a Internet. Esta segmentación no solo responde a un criterio lógico de organización, sino que se orienta a establecer distintos niveles de confianza y protección, permitiendo aplicar políticas de seguridad diferenciadas según el rol y la criticidad de cada segmento de red.

Sobre esta base, se integraron máquinas virtuales con sistemas Ubuntu y Debian Server para la prestación de servicios como HTTP y FTP, ubicando el servidor en la DMZ y los clientes en la LAN, de manera que todo el tráfico entre zonas fuese gestionado y controlado a través de Endian. La configuración de reglas de firewall, filtrado de tráfico, NAT y port forwarding permitió simular escenarios reales de publicación de servicios hacia Internet, al tiempo que se restringían y supervisaban los flujos de datos entre redes internas y externas. Adicionalmente, se aplicaron medidas específicas como el bloqueo de ICMP para aumentar la discreción del servidor y dificultar su identificación directa dentro de la red.

Como complemento a la función del firewall, se implementó un proxy HTTP en modo no transparente, orientado al control del tráfico saliente desde la red interna hacia Internet. La exigencia de autenticación previa para los usuarios, junto con el uso de listas negras de dominios, permitió reforzar la trazabilidad de las conexiones y aplicar restricciones de acceso a determinados contenidos, sin afectar la operatividad general de los servicios. Este enfoque evidenció cómo el proxy y el firewall pueden trabajar de forma conjunta para fortalecer la seguridad perimetral, combinando control de acceso, filtrado de contenidos y registro detallado de la actividad.

En conjunto, el trabajo integra tanto los fundamentos teóricos de la segmentación de redes, las zonas de seguridad, las políticas de acceso y el uso de NAT, como su aplicación práctica en un entorno virtualizado que emula condiciones propias de redes empresariales. La experiencia permitió a los participantes afianzar conocimientos sobre diseño seguro de infraestructuras, configuración de firewalls y proxies, y gestión centralizada de la seguridad, ofreciendo una visión integral de las herramientas y buenas prácticas necesarias para proteger servicios y recursos en organizaciones modernas.

2. INSTALACIÓN GNU/LINUX ENDIAN

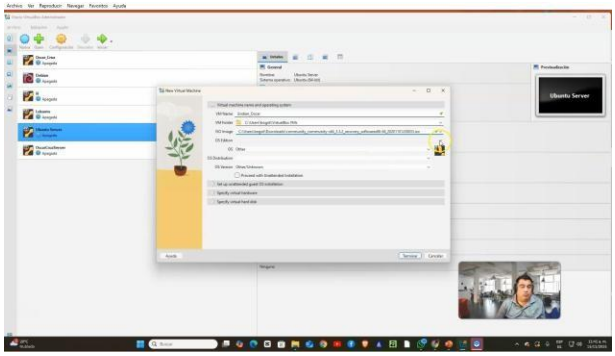
2.1 Requisitos Previos

Como parte inicial de la instalación de Endian existen requisitos base que son fundamentales para la implementación de la solución:

- Máquina virtual (VirtualBox)
- Imagen .iso de sistema Endian
- Computador que cumpla con los requisitos mínimos de Hardware.
- Otras distribuciones instaladas, como Linux Ubuntu y Ubuntu server.

A continuación, se presenta la creación de la Máquina virtual con especificaciones base y características en sus adaptadores de red.

Figura 1 Creación de Máquina Virtual 8Gb de RAM y128mb de Video, en ella se instalará Endian.

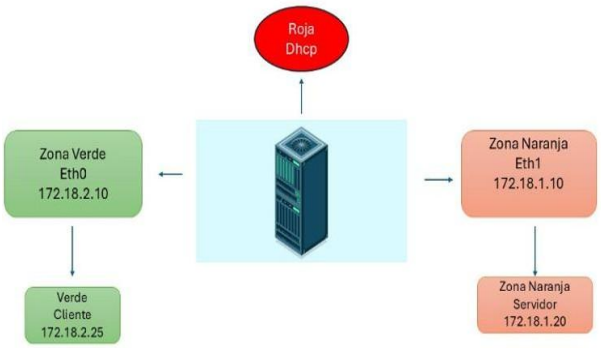


Fuente: Autoría Propia

2.2 Configuración de Adaptadores de red

Para que el cliente Ubuntu y el servidor puedan lograr conexión dentro del Firewall creado por Endian, se hace necesario establecer una segmentación y que los adaptadores de red estén configurados con los siguientes parámetros

Figura 2 Segmentación Establecida

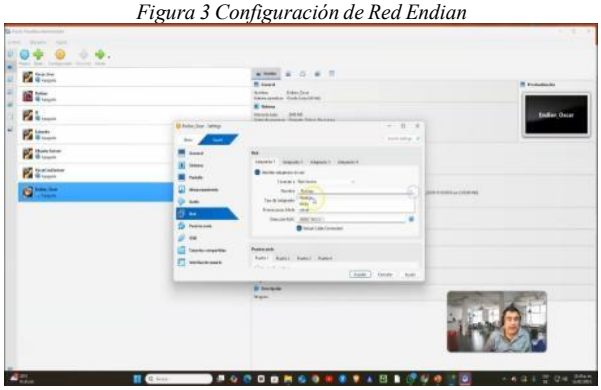


Fuente: Autoría Propia

Se establecen tres adaptadores:

- Adaptador 1 en red interna y nombre de segmentación Verde,
- Adaptador 2 red interna y nombre de segmentación Naranja
- Adaptador 3 en NAT para que allí funcione Rojo (Conexión a Internet.)

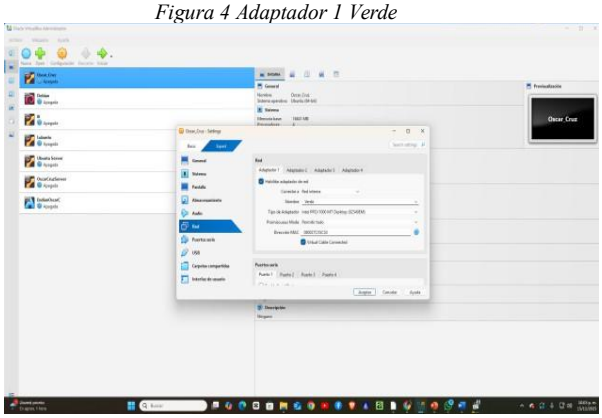
Figura 3 Configuración de Red Endian



Fuente: Autoría Propia.

Aquí se habilita el Adaptador 1 y se establece "Conectado a: Red interna", seleccionando como Nombre de red "VERDE". Esto hace que el cliente Ubuntu quede conectado al mismo segmento interno GREEN que el adaptador correspondiente del firewall Endian. Gracias a esta configuración, cualquier tráfico de este cliente hacia otras redes (por ejemplo, Internet o la DMZ/ORANGE) deberá pasar obligatoriamente por el firewall, cumpliendo con el objetivo de segmentación y control de acceso dentro del entorno virtual.

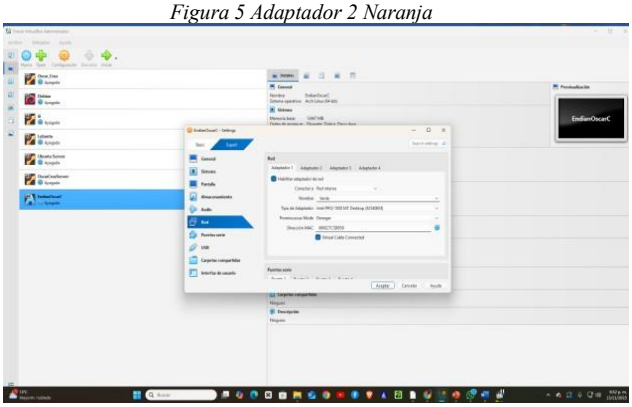
Figura 4 Adaptador 1 Verde



Fuente: Autoría propia

En este caso también se habilita el adaptador, pero se selecciona "Conectado a: NAT". Con esta elección, Endian utiliza la interfaz del host como puerta de salida hacia Internet, ya que el modo NAT de VirtualBox traduce el tráfico generado por el firewall hacia la red externa. Este adaptador se emplea como interfaz WAN del firewall: recibe una dirección IP del servicio NAT de VirtualBox y permite que las demás redes internas (GREEN/ORANGE) puedan acceder al exterior a través de las reglas de enrutamiento y de firewall que se definan en Endian.

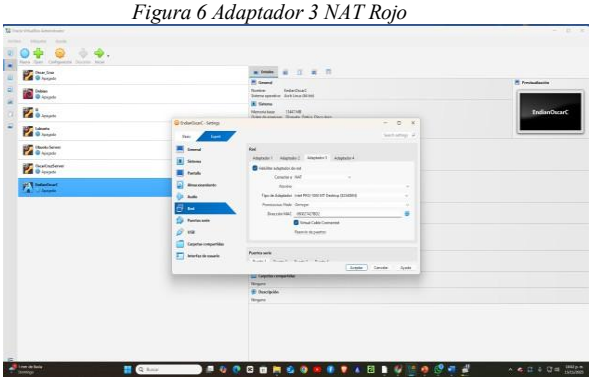
Figura 5 Adaptador 2 Naranja



Fuente: Autoría propia

Se procedió a configurar la Zona Roja (RED) del firewall Endian, correspondiente al enlace con la red externa o Internet. Para ello, se aprovechó el segundo adaptador de red de la máquina virtual *Endian*, previamente configurado en VirtualBox en modo NAT. Durante el asistente de configuración inicial de Endian, este adaptador se definió como interfaz RED/WAN, permitiendo que obtenga una dirección IP de manera dinámica a través del servicio DHCP ofrecido por el propio entorno de VirtualBox.

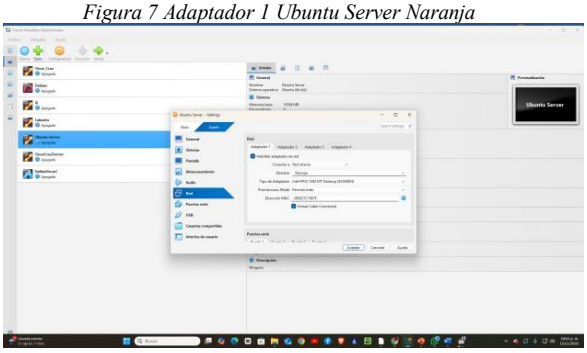
Figura 6 Adaptador 3 NAT Rojo



Fuente: Autoría propia

En cuanto a la Zona Naranja (ORANGE), se configuró como la DMZ del firewall Endian, destinada a alojar servicios que deben ser accesibles desde el exterior, pero sin exponer directamente la red interna de usuarios. Para ello, en VirtualBox se habilitó uno de los adaptadores de la máquina Endian en modo Red interna, asignándole el nombre lógico "ORANGE". Posteriormente, durante el asistente de configuración de Endian, este adaptador se declaró como interfaz ORANGE/DMZ, asignándole una dirección IP fija dentro de un segmento de red independiente del resto de zonas.

Figura 7 Adaptador 1 Ubuntu Server Naranja

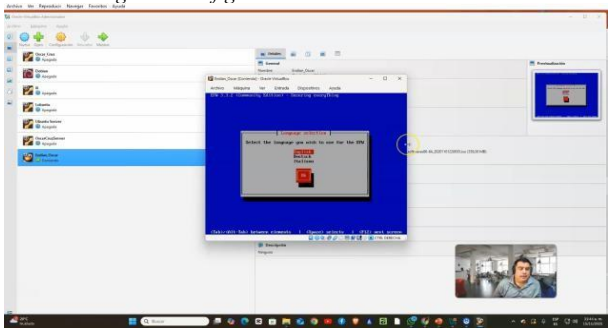


Fuente: Autoría propia

3. INSTALACIÓN DE ENDIAN

La Instalación de Endian inicia colocando la .iso en la máquina virtual creada, tras iniciar la maquina esta iniciará la instalación hasta un punto en donde solicitará configurar el idioma del sistema, en este caso el idioma más adecuado es Ingles puesto que español no está disponible para la distribución.

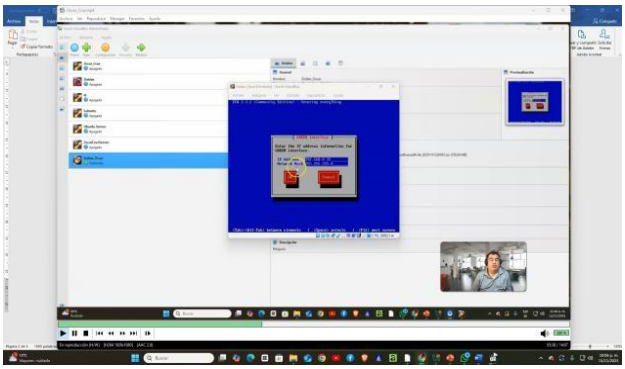
Figura 8 Configuración de Idioma en Endian



Fuente: Autoría Propia

Ahora se deberá establecer la IP correspondiente a la zona verde para nuestro Endian, que según nuestra segmentación es 172.18.2.10 (*Véase figura 2*)

Figura 9 Configurando IP de Endian

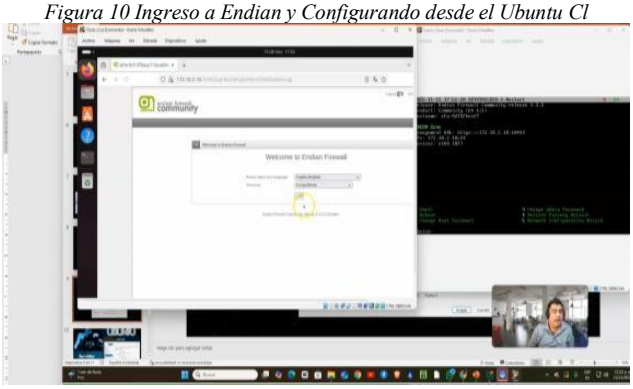


Fuente: Autoría Propia

Luego de ello se accede desde el cliente Ubuntu y su navegador usando la ip que se asignó con anterioridad en la segmentación

http://172.18.2.10 o https://172.18.2.10:10443

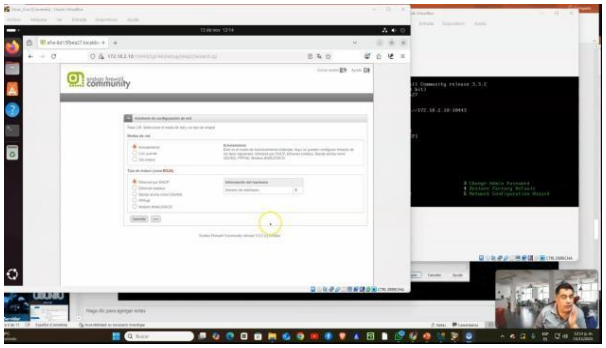
Figura 10 Ingreso a Endian y Configurando desde el Ubuntu Cl



Fuente: Autoría Propia

Ahora se observa que la Zona roja quedo establecida con las 3 interfaces de red que se configuraron en Endian.

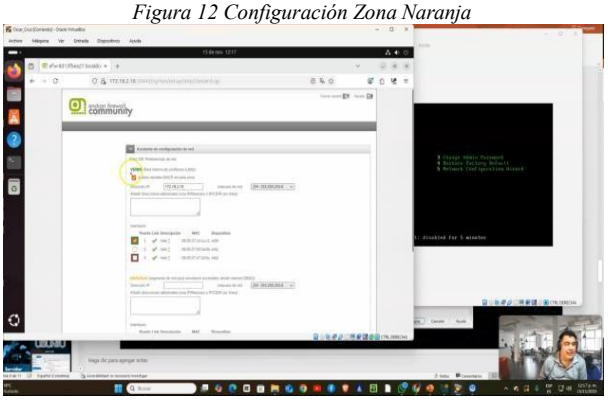
Figura 11 Zona Roja



Fuente: Autoría Propia

Cuando se avanza al siguiente entorno preguntará que zona se va a configurar y allí seleccionara la zona naranja, asignando la ip ya definida en la segmentación (*Véase figura 2*) 172.18.1.10

Figura 12 Configuración Zona Naranja



Fuente: Autoría Propia

TEMÁTICA 2 CONFIGURACIÓN NAT Y SEGMENTACIÓN DE RED

La Temática 2 del proyecto, permitió configurar y aplicar las reglas NAT dentro de la plataforma Endian Firewall, la base inicial corresponde a la segmentación de red propuesta para las zonas Verde, Naranja y Roja.

Como objetivo principal es la necesidad de permitir la salida controlada de tráfico desde las redes internas (LAN y DMZ) hacia la red externa (WAN), garantizando conectividad sin comprometer la seguridad perimetral; Para lograr este objetivo, se implementaron reglas de NAT fuente (Source NAT).

1. ENDIAN EJECUTANDO ADAPTADORES CONFIGURADOS

Figura 13 Interfaces de red.

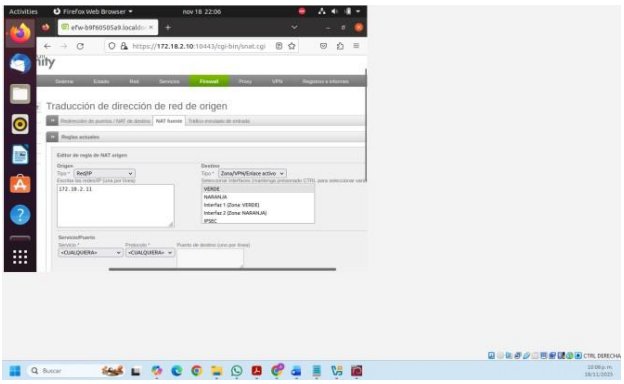
Fuente: Autoría Propia

2. CONFIGURACIÓN DE REGLAS NAT DESDE LAN HACIA WAN

Se creó una regla SNAT para permitir que el cliente Ubuntu (172.18.2.11) acceda a Internet. La IP de origen fue traducida por la IP pública simulada del firewall.

Origen: Zona Verde (LAN), su destino: Zona Roja (WAN), el servicio acceder: ALL para este caso también nuestra dirección IP de origen: 172.18.2.11 y la dirección IP de destino: 10.0.4.15 (IP simulada de Internet) con un único objetivo de permitir tráfico.

Figura 14 Configuración Regla NAT desde LAN a WAN.



Fuente: Autoría Propia

3. PRUEBAS DE FUNCIONALIDAD NAT DESDE LAN HACIA WAN

Con el objetivo de validar la regla SNAT configurada en el firewall Endian, se realizaron pruebas de conectividad desde el cliente Ubuntu (IP: 172.18.2.11), ubicado en la Zona Verde (LAN), hacia una IP simulada de internet (10.0.4.15) en la Zona Roja (WAN).

La regla permite traducir la IP de origen por la IP pública simulada del firewall, habilitando el acceso a servicios externos.
ping -c 4 10.0.4.15 con el propósito de confirmar que el tráfico es redirigido correctamente por la regla SNAT.

ping -c 4 www.google.com con el propósito de confirmar que el cliente puede resolver nombres de dominio y salir a internet a través del firewall.

Figura 15 Pruebas de Funcionalidad desde LAN a WAN.

Fuente: Autoría Propia

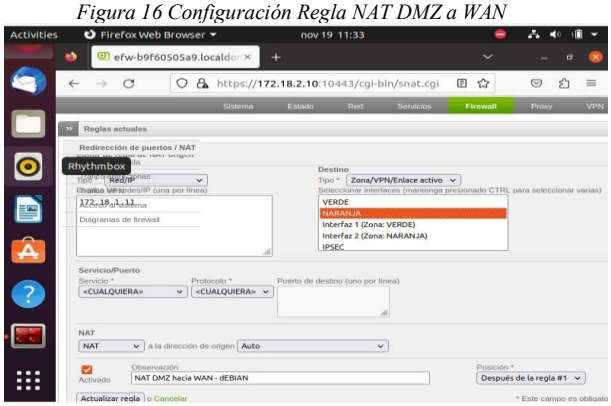
4. CONFIGURACIÓN DE REGLAS NAT DESDE DMZ HACIA WAN

Se configuró una regla similar para el servidor Debian (172.18.1.11), permitiendo su salida hacia la red externa.

Origen: Zona Naranja (DMZ) con destino: Zona Roja (WAN), el servicio acceder: ALL; nuestra dirección IP de origen: 172.18.1.11 (IP del servidor Debian) y nuestra

dirección IP de destino: 10.0.4.15 (IP simulada de Internet) con un único objetivo de permitir tráfico.

Figura 16 Configuración Regla NAT DMZ a WAN



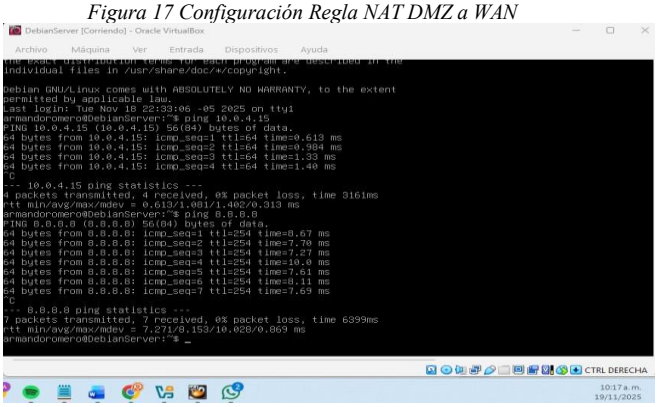
Fuente: Autoría Propia

5. PRUEBAS DE FUNCIONALIDAD NAT DESDE DMZ HACIA WAN

Con el objetivo de validar la regla SNAT configurada en el firewall Endian se ejecuta un ping -c 4 10.0.4.15 con el propósito de confirmar que el tráfico desde la DMZ es redirigido correctamente por la regla SNAT.

Desde el Servidor Debian CURL http://10.0.4.15 con el propósito de confirmar que el servidor puede establecer conexiones HTTP hacia la IP simulada.

Figura 17 Configuración Regla NAT DMZ a WAN



Fuente: Autoría Propia

6. VERIFICACIÓN DE CONECTIVIDAD

Se ejecutaron pruebas de conectividad mediante ping (ICMP) desde Ubuntu y Debian hacia el firewall y hacia direcciones externas, confirmando la funcionalidad de las reglas NAT.

7. IMPORTANCIA DE LAS REGLAS NAT

La configuración adecuada de las reglas NAT fuente (SNAT) en Endian Firewall es esencial para permitir que los dispositivos internos accedan a recursos externos sin exponer sus direcciones IP privadas.

Además, se verificó la efectividad de estas reglas desde las terminales de los clientes, como se evidenció en sesiones con usuarios como:

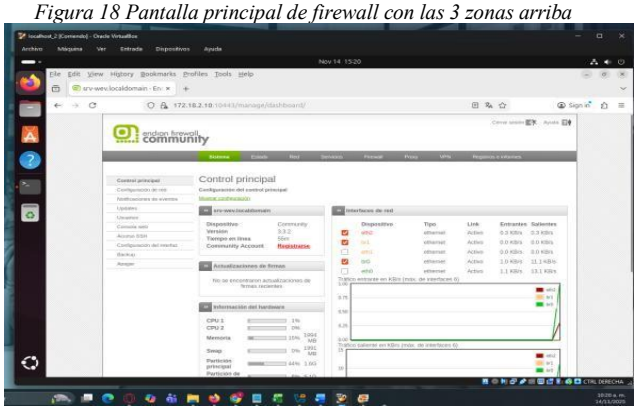
armandoromero@ubuntu:~$ ping 8.8.8.8

Estas pruebas confirmaron que el tráfico saliente fue correctamente enmascarado y redirigido por el firewall.

TEMÁTICA 3 PERMITIR SERVICIOS DE LA ZONA DMZ

Como parte de la actividad de seguridad implementada en la infraestructura de red por medio del firewall Endian, se realizó la configuración de servicios dentro de una zona desmilitarizada (DMZ). Esta zona permite exponer de manera controlada ciertos servicios hacia la red interna y, en algunos casos, hacia el exterior, minimizando el riesgo hacia los servidores de la intranet.

Figura 18 Pantalla principal de firewall con las 3 zonas arriba



Fuente: Autoría Propia

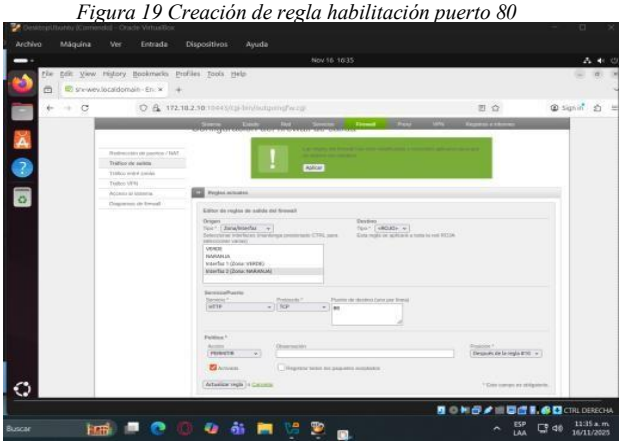
Se realizó la habilitación de servicios HTTP y FTP en un servidor Ubuntu Server ubicado en la DMZ, así como la restricción del protocolo ICMP para evitar respuestas de ping desde la red.

Se habilitan los Servicios HTTP (Puerto 80) y FTP (Puerto 21)

Se configuró un servidor Ubuntu Server con el fin de permitir el acceso a los servicios HTTP y FTP. Para ello, se definieron reglas específicas en el firewall, permitiendo únicamente el tráfico entrante en los puertos 80 y 21.

Se crea la regla para permitir la salida http puerto 80

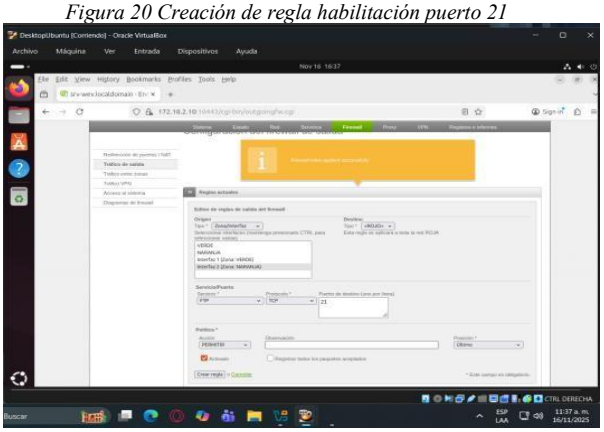
Figura 19 Creación de regla habilitación puerto 80



Fuente: Autoría Propia

Se crea la regla para permitir la salida ftp puerto 21

Figura 20 Creación de regla habilitación puerto 21



Fuente: Autoría Propia

1. RESULTADOS OBSERVADOS

El servidor Web respondió correctamente a peticiones HTTP, evidenciando la correcta apertura del puerto 80 realizando consulta por medio de código para verificar que el puerto se encontraba abierto.

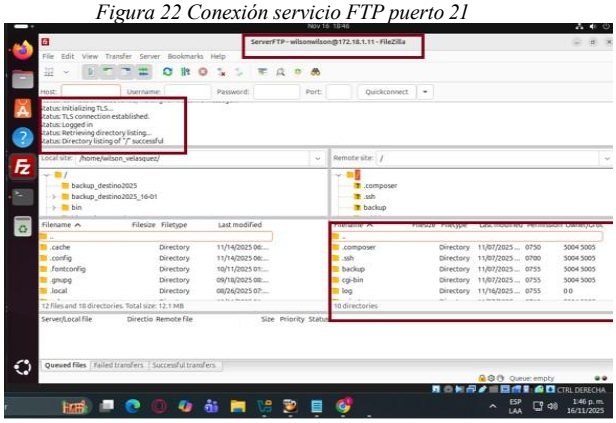
Figura 21 Puerto 80 habilitado

Fuente: Autoría Propia

La conexión al servicio FTP fue exitosa, validando que el puerto 21 se encuentra habilitado y accesible desde la DMZ.

Las pruebas de conexión realizadas desde el Ubuntu Desktop con el cliente FileZilla confirmaron que el tráfico permitido coincide con las reglas configuradas en el firewall Endian.

Figura 22 Conexión servicio FTP puerto 21



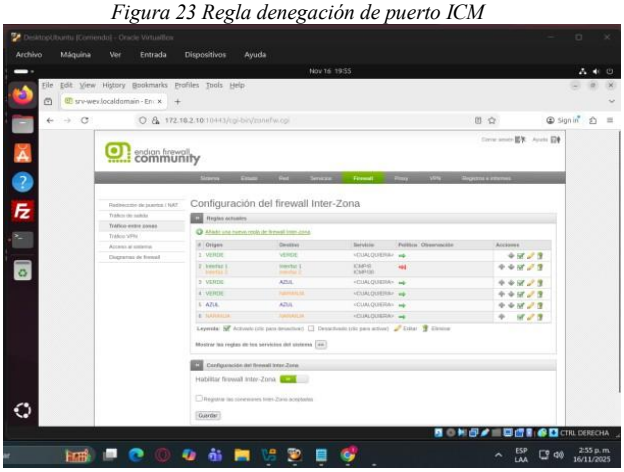
Fuente: Autoría Propia

Los registros del firewall mostraron la creación y activación de las reglas para ambos puertos, lo cual garantiza la trazabilidad y control del servicio.

2. RESTRICCIÓN DEL PROTOCOLO ICMP (PING)

Como medida adicional de seguridad, se configuraron reglas para denegar el protocolo ICMP, realizando el bloqueo de los puertos 8 y 30. Esto impide que los equipos de la red puedan utilizar el comando ping para descubrir o diagnosticar el servidor en la DMZ.

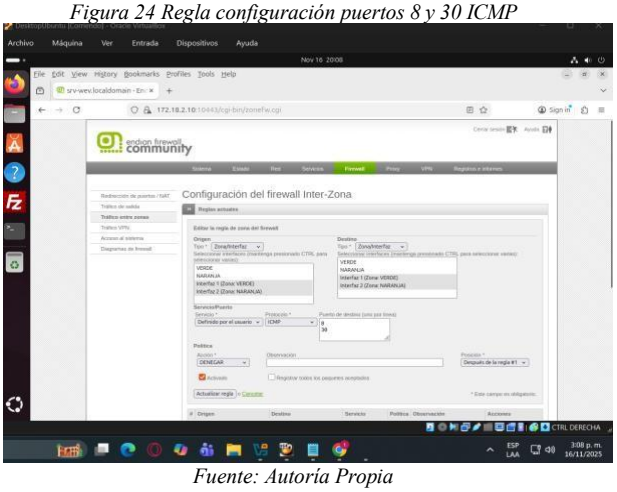
Figura 23 Regla denegación de puerto ICM



Fuente: Autoría Propia

Se define la regla inter-zona del firewall Endian, seleccionando como origen la red interna de usuarios (Zona VERDE) y como destino la red de servidores (Zona NARANJA/DMZ). Con ello se establece explícitamente qué tráfico puede salir desde la LAN hacia la DMZ, evitando que la comunicación entre zonas quede abierta por defecto. Esta segmentación permite que solo el tráfico autorizado llegue a los servicios publicados en la zona naranja, manteniendo aislada la red de usuarios frente a posibles compromisos en los servidores.

Figura 24 Regla configuración puertos 8 y 30 ICMP

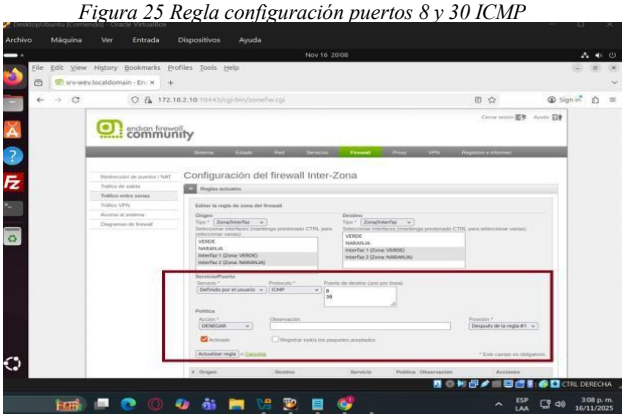


Fuente: Autoría Propia

Se detalla la política aplicada a la regla, donde se especifican los puertos o servicios permitidos, se define la acción "Aceptar" y se habilita el registro de eventos. De esta manera, no se habilita un acceso general entre zonas, sino que se limita el tráfico a los servicios estrictamente necesarios y, además, se genera un log que permite auditar y comprobar el comportamiento del firewall. Esto refuerza el control sobre

las comunicaciones entre la red VERDE y la DMZ, alineándolo con los objetivos de seguridad del diseño.

Figura 25 Regla configuración puertos 8 y 30 ICMP

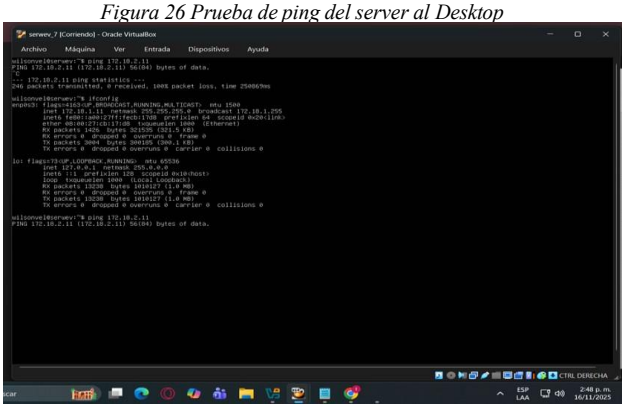


Fuente: Autoría Propia

3. RESULTADOS OBSERVADOS

Al realizar pruebas desde una consola hacia la IP del servidor en la DMZ, el comando ping no obtuvo respuesta, confirmando que los paquetes ICMP fueron bloqueados correctamente.

Figura 26 Prueba de ping del server al Desktop



Fuente: Autoría Propia

El firewall registró intentos de salida ICMP, pero estos fueron descartados de acuerdo con las reglas implementadas.

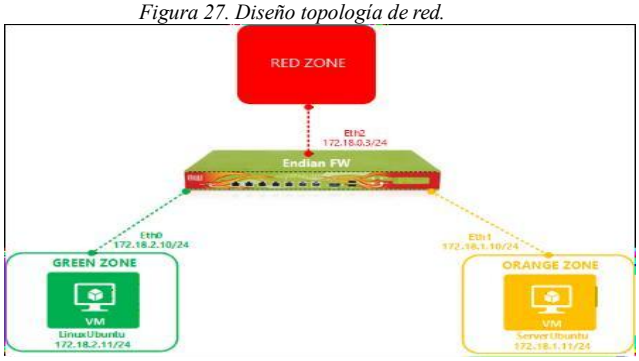
La no respuesta al ping incrementa la dificultad para que las personas no autorizadas identifiquen el servidor mediante técnicas de enumeración o escaneo básico.

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

La Temática 4 se desarrolló mediante la implementación de una topología de red que incluyó zonas de red diferenciadas (verde, naranja y roja), segmentadas de acuerdo con los servicios alojados en cada una. En la zona verde se implementó un servidor Desktop Linux como cliente, en la zona naranja se desplegó un servidor Ubuntu destinado a la publicación de servicios. Endian Firewall se estableció como un nodo central de filtrado de tráfico entre las zonas, aprovechando sus capacidades avanzadas para la gestión de reglas de tráfico, políticas de acceso y traducción de direcciones (NAT).

Para facilitar la comprensión en la fig. No 31 se presenta la topología de red implementada.

Figura 27. Diseño topología de red.



Fuente: Autoría Propia

4.1 COMUNICACIÓN ZONA VERDE - NARANJA PROTOCOLOS HTTP Y FTP

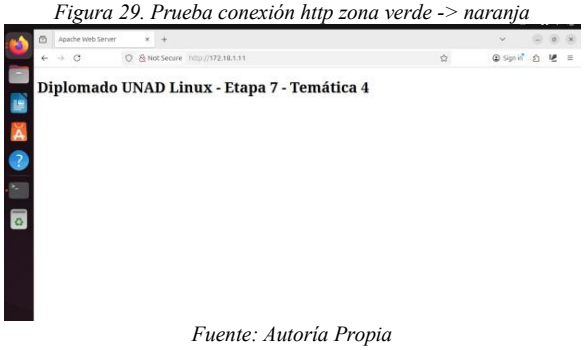
Para habilitar la comunicación entre las zonas verde y naranja, se accedió al portal de administración de Endian FW y en la sección de configuración de tráfico Inter-Zona, se editó la regla No. 2 con el fin de permitir el tráfico HTTP únicamente.

Figura 28. Ajuste configuración regla No. 2

Fuente: Autoría Propia

Para validar el funcionamiento de la regla configurada, se ejecutó una prueba de acceso desde la máquina virtual Ubuntu Linux con dirección IP 172.18.2.11, ubicada en la zona verde (LAN), hacia el servicio HTTP publicado por el servidor Ubuntu con dirección IP 172.18.1.11, alojado en la zona naranja (DMZ).

Figura 29. Prueba conexión http zona verde -> naranja



Fuente: Autoría Propia

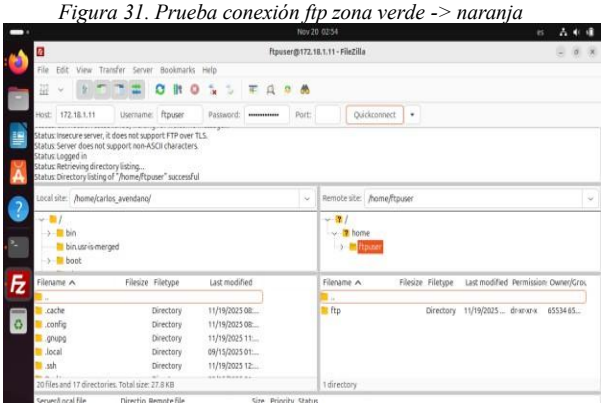
Se definió la regla No. 3 en el firewall con el propósito de habilitar la comunicación hacia el servicio FTP ubicado en la zona DMZ (naranja) desde la zona Internet (roja).

Figura 30. Creación regla No.3 permitir FTP

Fuente: Autoría Propia

Para validar el funcionamiento de la regla No.3, se ejecutó una prueba de acceso desde la máquina virtual Ubuntu Linux con dirección IP 172.18.2.11, ubicada en la zona verde (LAN), hacia el servicio FTP mediante el cliente FileZilla. La conexión se estableció apuntando al servidor Ubuntu con dirección IP 172.18.1.11, alojado en la zona naranja (DMZ).

Figura 31. Prueba conexión ftp zona verde -> naranja



Fuente: Autoría Propia

4.2 COMUNICAR LA ZONA INTERNET CON LA ZONA DMZ

Para permitir la comunicación entre la zona Internet (roja) y la zona DMZ (naranja), se accedió al portal de administración de Endian FW y en la sección de configuración del firewall, se definió la regla No.1 tipo "Port forwarding / NAT). Esta regla permitió el redireccionamiento del tráfico entrante en el puerto HTTP hacia el servidor ubicado en la zona DMZ.

Figura 32. Creación regla NAT para el servicio HTTP

Fuente: Autoría Propia.

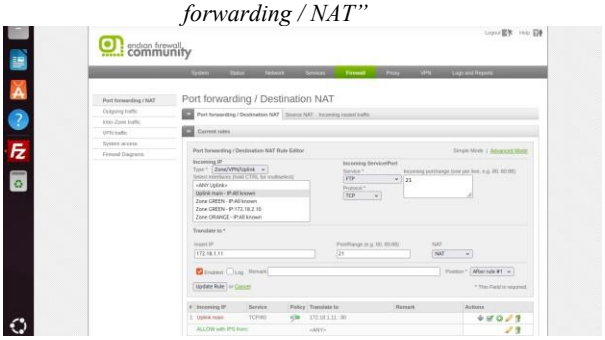
Dado que el servicio FTP se pública mediante una regla de traducción de direcciones de red (NAT), resulta necesario configurar el servidor FTP para que admita conexiones en modo pasivo. Esta configuración se implementa agregando las siguientes líneas al archivo de configuración /etc/vsftpd.conf

Figura 33. Configuración modo pasivo servicio FTP

Fuente: Autoría Propia

Se definió una segunda regla de firewall para habilitar el acceso desde la zona Internet (roja) hacia la zona DMZ (naranja) a través del puerto de conexión TCP 21, correspondiente al servicio FTP.

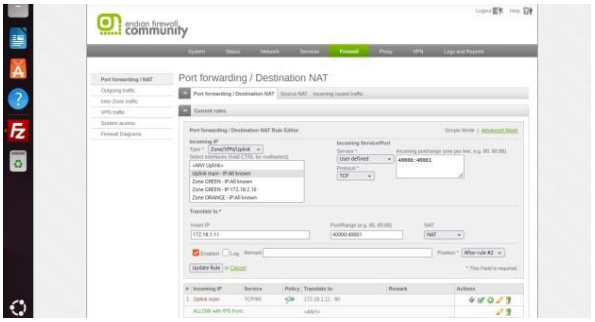
Figura 34. Creación y configuración regla No. 2 tipo "Port forwarding / NAT"



Fuente: Autoría Propia

Se definió la regla No. 3 en el firewall con el objetivo de habilitar el tráfico de transferencia de datos correspondiente al servicio FTP, mediante el rango de puerto 40000-40001.

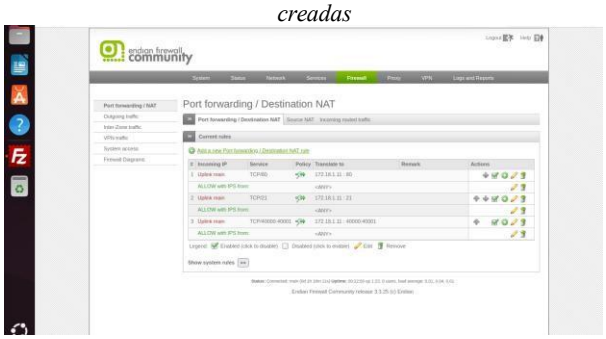
Figura 35. Creación y configuración regla No. 3 tipo "Port forwarding / NAT



Fuente: Autoría Propia

En la figura siguiente se valida la creación de las reglas tipo "Port forwarding / NAT" configuradas en el firewall.

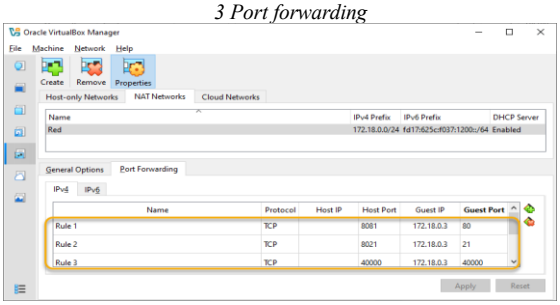
Figura 36. Validación reglas tipo "Port forwarding /NAT" creadas



Fuente: Autoría Propia

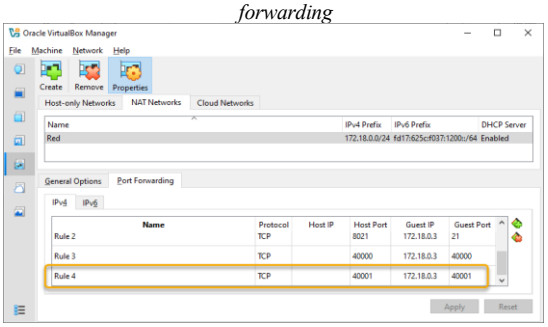
Finalmente, en la red NAT configurada en las propiedades de VirtualBox se definieron cuatro reglas de "Port forwarding" que mantienen correspondencia con las reglas previamente creadas en Endian Firewall.

Figura 37. VirtualBox Network Properties – Reglas 1, 2 y 3 Port forwarding



Fuente: Autoría Propia

Figura 38. VirtualBox Network Properties – Regla 4 Port forwarding



Fuente: Autoría Propia

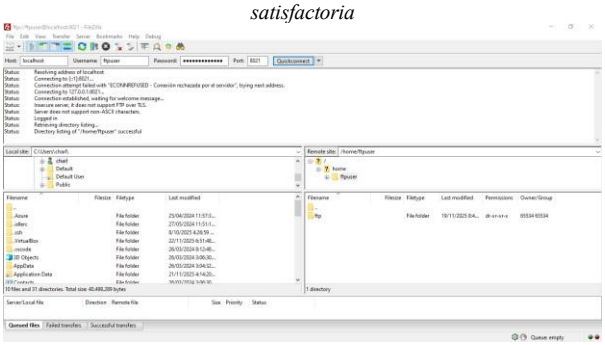
Se ejecutó la prueba a nivel de la capa de aplicación mediante un explorador web, estableciendo una conexión al puerto 8081 del equipo local. La petición fue redirigida a través de la regla de "Port forwarding /NAT" hacia el servidor Ubuntu con dirección IP 172.18.1.11, utilizando el puerto 80 correspondiente al servicio HTTP.

Figura 39. Prueba HTTP a nivel de la capa de aplicación satisfactoria

Fuente: Autoría Propia

Se ejecuto la prueba para el servicio FTP a nivel de la capa de aplicación utilizando el cliente FileZilla. La conexión se estableció al puerto 8021 del equipo local, y la petición fue redirigida mediante la regla de "Port forwarding /NAT" hacia el servidor Ubuntu con dirección IP 172.18.1.11, empleando el puerto 21 correspondiente al servicio FTP.

Figura 40. Prueba FTP a nivel de la capa de aplicación satisfactoria

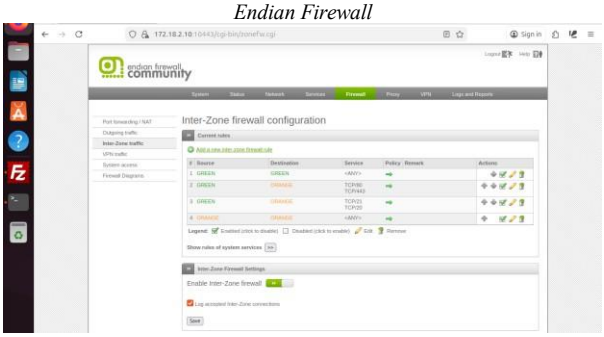


Fuente: Autoría Propia

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

En la fig. 40 se presentan las reglas creadas para el tráfico Interzonal requerido para las actividades correspondientes a la temática 4.

Figura 41. Reglas de tráfico Inter-Zona configuradas en Endian Firewall



Fuente: Autoría Propia

4.4 PROBAR DESDE UN NAVEGADOR WEB LAS SIGUIENTES DIRECTIVAS

4.4.1 EL INGRESO DEL SERVICIO HTTP DESDE LA LAN HACIA LA ZONA DMZ

Desde el cliente Linux con dirección IP 172.18.2.11, ubicado en la zona verde (LAN), se probó la conexión HTTP hacia el servidor Ubuntu con dirección IP 172.18.1.11, alojado en la zona naranja (DMZ). La validación se realizó mediante un navegador web, observándose que la conexión se estableció de manera satisfactoria.

Figura 42. Validación de la conexión HTTP desde la zona verde hacia el servidor en la zona DMZ.

Fuente: Autoría Propia

4.4.2 EL INGRESO DEL SERVICIO HTTP DESDE LA RED LAN HACIA LA RED WAN

Para la validación de estas pruebas se definieron dos reglas de tráfico saliente desde la zona verde hacia la zona roja. La regla No.1 habilito el tráfico HTTP, mientras que la regla No.2 permitió el tráfico HTTPS.

Figura 43. Creación de reglas tipo "Tráfico saliente" para las conexiones HTTP y HTTPS desde la zona verde hacia la zona WAN.

Fuente: Autoría Propia

Desde el cliente Linux con dirección IP 172.18.2.11, ubicado en la zona verde (LAN), se probó la conexión HTTP hacia el sitio web www.eltiempo.com, alojado en la zona Internet (WAN). La validación se realizó mediante un navegador web, observándose que la conexión se estableció de manera satisfactoria.

Figura 44. Prueba de conexión HTTP hacia la zona WAN

Fuente: Autoría Propia

4.4.3 EL INGRESO DEL SERVICIO HTTP DESDE LA ZONA DMZ HACIA LA ZONA WAN

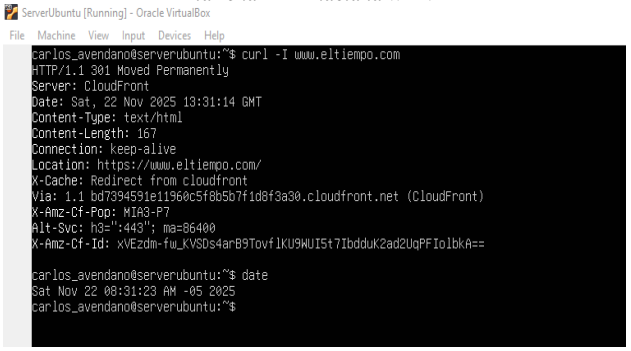
Para la ejecución de estas pruebas se modificaron las reglas de tráfico saliente No.1 y No.2 creadas previamente, incorporando la zona naranja (DMZ) como origen de tráfico.

Figura 45. Modificación de reglas No.1 y No.2 incorporando la zona naranja como origen.

Fuente: Autoría Propia

Debido a que el servidor ubicado en la zona naranja (DMZ) no dispone de entorno gráfico, la validación se realizó mediante una ventana de terminal utilizando la utilidad curl.

Figura 46. Prueba de conexión HTTP satisfactoria mediante curl desde la zona DMZ hacia la WAN

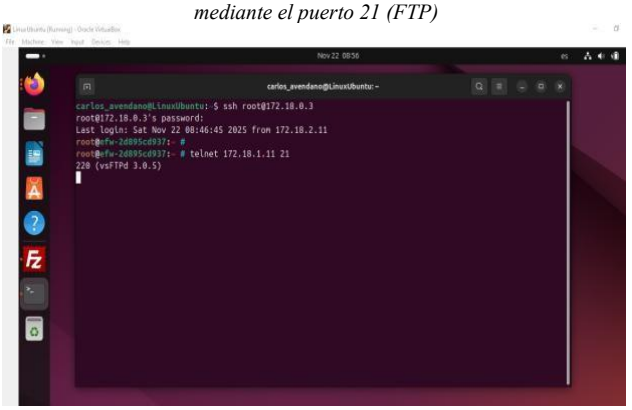


Fuente: Autoría Propia

4.4.4 EL INGRESO DEL SERVICIO FTP DESDE LA ZONA WAN HACIA LA ZONA DMZ

Dado que en la zona roja (WAN) únicamente se dispone de la máquina virtual con Endian Firewall, la validación se realizó estableciendo una conexión SSH desde la máquina virtual desktop Linux Ubuntu con dirección IP 172.18.2.11, hacia el servidor Endian Firewall con dirección IP 172.18.0.3. Posteriormente, desde esta sesión remota en la máquina virtual Endian Firewall se ejecutó una prueba utilizando la utilidad telnet al puerto 21 del servidor FTP alojado en la máquina virtual Ubuntu Server (172.18.1.11).

Figura 47. Prueba de conexión satisfactoria en sentido WAN -> DMZ mediante el puerto 21 (FTP)



Fuente: Autoría Propia

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

5.1 CONTEXTO DE LA SEGURIDAD PERIMETRAL Y USO DE ENDIAN COMO FIREWALL

La Temática 5 se desarrolló en el marco de la Etapa 7, orientada al fortalecimiento de la seguridad perimetral en un entorno basado en GNU/Linux. Para ello se utilizó Endian Firewall Community como dispositivo central, configurado con zonas de red como GREEN (LAN interna) y RED (salida a Internet), de modo que todo el tráfico HTTP de la red local pasará por un punto de control único. En este escenario de laboratorio se simuló el funcionamiento de una red organizacional donde la navegación hacia Internet debe ser regulada mediante políticas de acceso y filtrado de contenido.

Figura 48. Esquema de la topología de red.

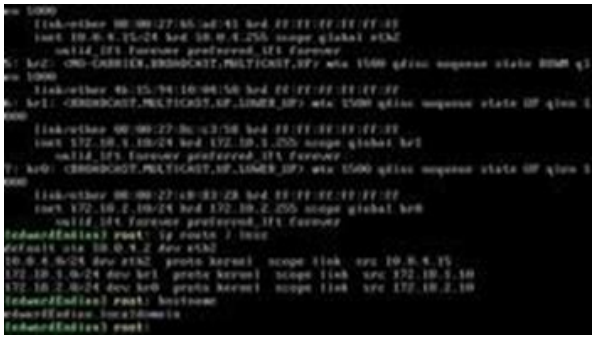
Autoría propia.

5.2 CONFIGURACIÓN DE LAS ZONAS DE RED Y DEL SERVICIO DHCP

A continuación, se revisa y ajusta la asignación de las interfaces físicas a las zonas lógicas GREEN, RED y ORANGE. La interfaz correspondiente a la LAN se asoció a GREEN, la de salida a Internet a RED y una tercera a ORANGE como segmento adicional. Sobre la zona GREEN se definió el segmento de red privada y se habilitó el servidor DHCP, configurando el rango de direcciones, la puerta de enlace y el servidor DNS apuntando al propio Endian.

Con esta configuración, los equipos conectados a la LAN quedaron en capacidad de obtener automáticamente sus parámetros de red y utilizar al firewall como punto de salida hacia el exterior. Fig. (48)

Figura 49. Zonas de red y servicio DHCP. Autoría propia



Fuente: Autoría Propia

5.3 PRUEBAS DE CONECTIVIDAD DESDE LA ESTACIÓN UBUNTU

Una vez configuradas las zonas, se encendió la estación de trabajo Ubuntu conectada a la red GREEN. Desde el gestor de redes se comprobó que el equipo había recibido correctamente la dirección IP, la máscara, la puerta de enlace y el DNS a través de DHCP.

Luego se realizaron pruebas de conectividad mediante ping hacia la dirección de Endian y hacia destinos externos, verificando que el tráfico se enruta a través del firewall. Fig.50.

Figura. 50. Resultados de los pings al servidor

Fuente: Autoría Propia

Finalmente, se accedió a la interfaz web de administración de Endian desde el navegador de Ubuntu, utilizando el protocolo HTTPS y las credenciales de administrador. Esta comprobación confirmó que el cliente de la LAN podía comunicarse con el dispositivo y que el entorno estaba listo para la configuración del proxy HTTP. Fig. 51.

Fig. 51. Acceso a server Endian desde el escritorio del cliente.

Fuente: Autoría Propia

5.4 HABILITACIÓN DEL PROXY HTTP EN MODO NO TRANSPARENTE

Con la conectividad validada, se ingresó al módulo de configuración del proxy HTTP en la interfaz de Endian. En esta sección se activó el servicio y se seleccionó el modo no transparente, de forma que los clientes debieran especificar manualmente el uso del proxy en su navegador. Se definió el puerto de escucha (8080) y se indicó que las zonas autorizadas para utilizar el servicio serían, principalmente, GREEN y, en caso necesario, ORANGE.

Tras guardar los cambios, el sistema comenzó a escuchar peticiones HTTP en el puerto configurado, quedando preparado para recibir las conexiones provenientes de los equipos de la red interna. *Fig. 52.*

Figura. 52. Configuración del proxy HTTP

Fuente: Autoría Propia

5.5 CREACIÓN DEL PERFIL DE FILTRADO Y DEFINICIÓN DE LA LISTA NEGRA

El siguiente paso consistió en crear un perfil de filtrado específico para el tráfico HTTP. Desde el módulo de Web Filter se generó un nuevo perfil, en el cual se habilitó la inspección del contenido y se activaron las opciones de análisis de tráfico. En la sección destinada a listas negras se añadieron de forma explícita los dominios www.hotmail.com, www.youtube.com y www.elnuevodia.com.co, tal como lo indicaba la guía.

Estos sitios quedaron registrados para ser bloqueados cuando el perfil se aplicará a una política de acceso, asegurando que los intentos de conexión hacia ellos fueran rechazados por el proxy. *Fig. 53.*

Figura. 53. Creación perfil para filtrado HTTP

Fuente: Autoría Propia

5.6 ASOCIACIÓN DEL PERFIL DE FILTRADO A LA POLITICA DE ACCESO

Una vez definido el perfil, se pasó a configurar la política de acceso del proxy HTTP. En el módulo correspondiente se editó la política encargada de gestionar el tráfico desde la zona GREEN. Como origen se seleccionó la zona interna y como acción principal se estableció permitir el acceso, pero condicionando la navegación al uso del perfil de filtrado creado anteriormente.

Al guardar la política, todo el tráfico HTTP que salía de la LAN a través del proxy quedó sometido a la lista negra, de manera que los dominios configurados debían ser bloqueados de forma automática durante las pruebas de navegación. Fig. 54.

Figura. 54. Política de acceso

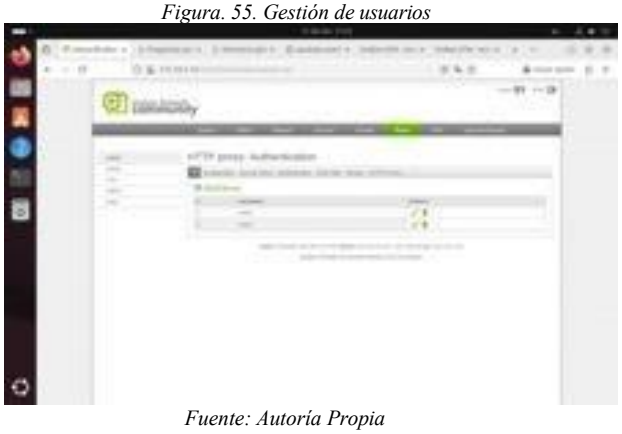
Fuente: Autoría Propia

5.7 CREACIÓN DE USUARIOS Y GRUPOS DE NAVEGACIÓN

Para incorporar la autenticación por credenciales, se crearon usuarios locales en la sección de Web Users de Endian. En esta base se añadieron cuentas específicas para la práctica, asignando a cada una un nombre de usuario y una contraseña, y habilitándolas para el uso del proxy HTTP.

Posteriormente, se organizaron estas cuentas en un grupo de navegación, lo que permitió gestionar de manera conjunta los permisos asociados al servicio. Esta estructura facilitó la aplicación de políticas basadas en grupo en lugar de trabajar usuario por usuario. Fig. 55.

Figura. 55. Gestión de usuarios



Fuente: Autoría Propia

5.8 CONFIGURACIÓN DE LA AUTENTICACIÓN BASADA EN USUARIOS

Con las cuentas ya definidas, se regresó a la política de acceso del proxy para habilitar la autenticación. En la misma política utilizada para la zona GREEN se activó la opción de autenticación y se seleccionó el modo basado en usuarios. A continuación, se indicó el grupo de navegación como conjunto autorizado para utilizar el servicio, manteniendo el perfil de filtrado con la lista negra.

De este modo, cualquier equipo de la LAN que intentara navegar a través del proxy debía autenticarse previamente y, una vez validado, quedaba sujeto a las restricciones establecidas en el perfil de filtrado. *Fig. 56.*

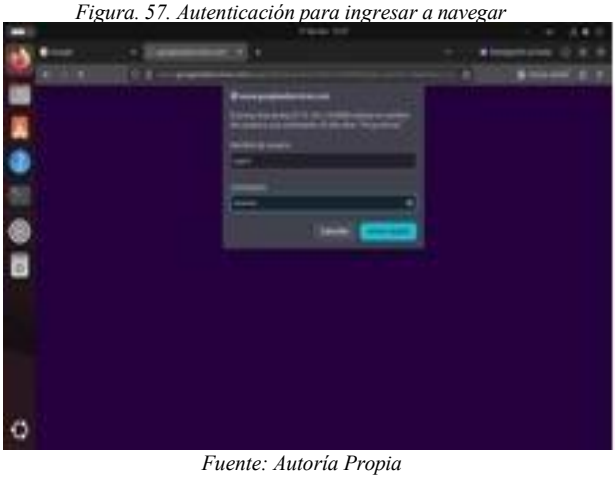
Figura. 56. Gestión de grupos

Fuente: Autoría Propia

5.9 PRUEBAS DE NAVEGACIÓN Y VERIFICACIÓN DE LAS POLITICAS

Finalmente, se realizaron las pruebas de funcionamiento desde la estación Ubuntu. En el navegador se configuró manualmente el uso del proxy, especificando la dirección IP de Endian y el puerto 8080. Al intentar acceder a cualquier sitio web, el navegador mostró una ventana solicitando usuario y contraseña, lo que confirmó que la autenticación se encontraba activa. *Fig. 57.*

Figura. 57. Autenticación para ingresar a navegar



Fuente: Autoría Propia

Tras ingresar con una de las cuentas creadas, se probó el acceso a páginas no incluidas en la lista negra, que cargaron con normalidad. Luego se intentó ingresar a www.hotmail.com, www.youtube.com y www.elnuevodia.com.co; en estos casos, el navegador presentó una página de error generada por el proxy, indicando que el acceso estaba bloqueado. Estas pruebas permitieron comprobar que el perfil de filtrado, la lista negra y la autenticación por usuario funcionaban de manera integrada según lo previsto. *Fig. 58.*

Figura. 58. Proxy bloqueando conexión a YouTube

Fuente: Autoría Propia

5.10 CUMPLIMIENTO DEL PRODUCTO ESPERADO

Al finalizar la actividad se verificó que cada uno de los componentes solicitados funcionara correctamente. El perfil de filtrado fue creado e incluyó la lista negra con los tres dominios establecidos, la cual quedó vinculada a la política de acceso del servicio proxy. La autenticación por usuario operó sin inconvenientes: el navegador solicita credenciales al intentar ingresar a recursos externos y permitió la navegación solo después de validar el usuario asignado al grupo configurado en el sistema. Desde la estación en la LAN se realizaron las pruebas requeridas. Los sitios incluidos en la lista negra fueron bloqueados de manera inmediata, mientras que las páginas no restringidas cargaron con normalidad una vez autenticado el usuario. Esto confirmó que el proxy actuaba como intermediario obligatorio y que aplicaba las reglas definidas en el perfil.

CONCLUSIONES.

La experiencia desarrollada a lo largo de las cinco temáticas permitió comprobar que la seguridad de una infraestructura de red no depende únicamente del sistema operativo, sino de cómo se diseñan e integran sus mecanismos de protección. En la Temática 1, la configuración de la instancia de Endian en VirtualBox y el ajuste de sus tarjetas de red sentaron las bases de todo el entorno, demostrando que una correcta planificación de interfaces y zonas es el punto de partida para cualquier esquema de seguridad sólido. Sin esta etapa inicial, el resto de servicios simplemente no tendrían un soporte coherente ni una segmentación clara.

A partir de esa estructura, la Temática 2 centrada en la

configuración de NAT evidenció la importancia de controlar la salida de la red hacia Internet, ocultando las direcciones internas y gestionando el tráfico a través de un punto único de salida. Sobre esta base, la Temática 3 abordó la publicación de servicios en la Zona Naranja (DMZ), mostrando cómo es posible ofrecer servicios accesibles desde el exterior sin exponer directamente la red de usuarios, gracias a la separación lógica entre segmentos y a la ubicación estratégica de los servidores.

La Temática 4, orientada a la definición de reglas de acceso entre zonas, reforzó el principio de mínimo privilegio: cada flujo de comunicación entre VERDE, NARANJA y ROJA debe estar justificado, delimitado y registrado. La creación de políticas específicas para permitir o denegar tráfico según origen, destino y servicio, convirtió al firewall en un verdadero orquestador de la seguridad, y no en un simple dispositivo de paso. Finalmente, la Temática 5 con la implementación de un Proxy HTTP no transparente con autenticación añadió una capa de control y trazabilidad sobre la navegación de los usuarios, integrando monitoreo, registro y responsabilidad en el uso de los recursos de Internet.

En conjunto, las cinco temáticas muestran un recorrido completo: desde la construcción de la infraestructura básica hasta la aplicación de políticas avanzadas de filtrado y control de acceso. El resultado es un entorno segmentado en Zonas Verde, Naranja y Roja, con servicios expuestos de forma controlada, tráfico interno protegido y uso de Internet regulado. Todo esto demuestra que, cuando se combina la robustez de GNU/Linux con herramientas como Endian y un diseño consciente de la arquitectura de red, es posible transformar un conjunto de máquinas virtuales en un laboratorio funcional de seguridad, perfectamente extrapolable a escenarios productivos reales.

BIBLIOGRAFÍA

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

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

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

LPI LPIC-1 Exam 101. (2022). *Tema 101: Determinar y configurar los ajustes de hardware*. Linux Professional Institute. https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

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

[1] Canonical, Guía del Ubuntu desktop 20.04 LTS. Ubuntu Documentation, 2023. [En línea]. Disponible en: https://help.ubuntu.com/20.04/ubuntu-help/index.html. [Accedido: 06-dic-2025].

[2] Debian, El manual del administrador de Debian 12.5.0. Proyecto Debian, 2023. [En línea]. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html. [Accedido: 06-dic-2025].

[3] Endian, Endian UTM 3.2: Manual de referencia. Endian, 2016. [En línea]. Disponible en: http://docs.endian.com/3.2/utm/index.html. [Accedido: 06-dic-2025].

[4] Linux Professional Institute, LPIC-1 Exam 101: Tema 101 – Determinar y configurar los ajustes de hardware. 2022. [En línea]. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/101/101.1/. [Accedido: 06-dic-2025].

[5] Oracle, Manual de usuario VirtualBox. Oracle VM VirtualBox, 2020. [En línea]. Disponible en: https://www.virtualbox.org/manual/. [Accedido: 06-dic-2025].