DISEÑO E IMPLEMENTACIÓN MULTI-ZONA CON ENDIAN FIREWALL PARA ENTORNOS VIRTUALIZADOS

Alejandro Forero Molano
aforeromo@unadvirtual.edu.co
Jhon Fredy Bermúdez López
jfbermudezl@unadvirtual.edu.co
José Argemiro Romero Suarez
jromerosu@unadvirtual.edu.co
Ricardo Emiro Corzo Rozo
recorzor@unadvirtual.edu.co

RESUMEN: *Este trabajo presenta la implementación de una infraestructura basada en GNU/Linux Endian dentro de un entorno virtualizado para establecer un modelo funcional de seguridad perimetral. Se configuraron las zonas Verde (LAN), Roja (WAN) y Naranja (DMZ), además de reglas de NAT que permiten comunicación controlada entre redes internas y externas. Se habilitaron y restringieron servicios como HTTP, FTP e ICMP según políticas definidas, verificando su funcionamiento mediante pruebas de conectividad y tráfico interzona. También se incorporó un Proxy HTTP no transparente con autenticación y listas negras para gestionar el acceso web desde la LAN. Los resultados demuestran una correcta segmentación de red, control de tráfico y aplicación de políticas de seguridad, evidenciando un entorno estable y administrado que refleja escenarios reales de protección de redes corporativas.*

PALABRAS CLAVE: Control de acceso, DMZ (Zona Desmilitarizada), Endian Firewall, NAT.

1 INTRODUCCIÓN

La implementación de infraestructuras seguras en entornos virtualizados se ha convertido en una necesidad fundamental para comprender el funcionamiento de los servicios de red y los mecanismos de protección perimetral. En este contexto, GNU/Linux Endian ofrece una plataforma robusta que permite simular escenarios reales de firewall, control de tráfico y segmentación de redes mediante el uso de zonas específicas como LAN, WAN y DMZ. Su integración en VirtualBox facilita el despliegue y la configuración de entornos de prueba sin comprometer sistemas reales.

En el desarrollo de esta práctica, se realiza la configuración integral de Endian, abarcando desde la estructura básica de red hasta la gestión avanzada de políticas de seguridad. Esto incluye la configuración de reglas NAT para permitir la comunicación controlada entre la red interna, la zona DMZ y la red externa simulada. Asimismo, se establecen permisos y restricciones para servicios esenciales como HTTP, FTP e ICMP, permitiendo validar el funcionamiento de cada política mediante pruebas directas de conectividad y monitoreo del tráfico interzona.

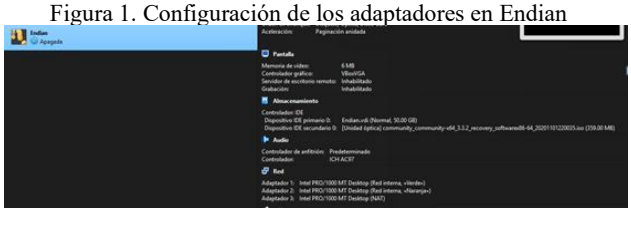
Finalmente, se implementa un Proxy HTTP no transparente con autenticación de usuarios y aplicación de listas negras, con el fin de gestionar de manera centralizada la navegación desde la LAN. Esta combinación de componentes permite comprender la importancia del control de acceso, la segmentación y la seguridad en redes corporativas, demostrando cómo un firewall perimetral puede proteger, administrar y monitorear el flujo de información dentro de una organización.

2 DESARROLLO DE CONTENIDOS

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

Para iniciar la práctica, se descarga la imagen de Endian Community desde su repositorio oficial y se preparan las máquinas virtuales necesarias en VirtualBox, incluyendo Ubuntu Desktop como cliente y Ubuntu Server para los servicios. Posteriormente, se configuran las interfaces de red del firewall, asignando la primera como red interna para la zona Verde (LAN), la segunda como otra red interna independiente destinada a la zona Naranja (DMZ) y la tercera como interfaz en modo NAT, que funciona como la zona Roja (WAN) y simula el acceso a Internet dentro del entorno virtual. [1]

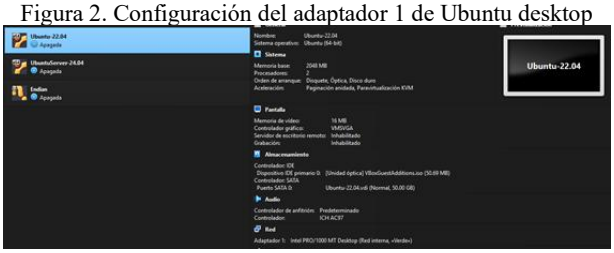
Figura 1. Configuración de los adaptadores en Endian



Fuente: Autoría Propia

En Ubuntu Desktop se configura el adaptador 1 como red interna, asignándolo a la zona Verde (LAN), permitiendo que el equipo funcione como cliente dentro del segmento principal de la red gestionada por Endian.

Figura 2. Configuración del adaptador 1 de Ubuntu desktop



Fuente: Autoría Propia

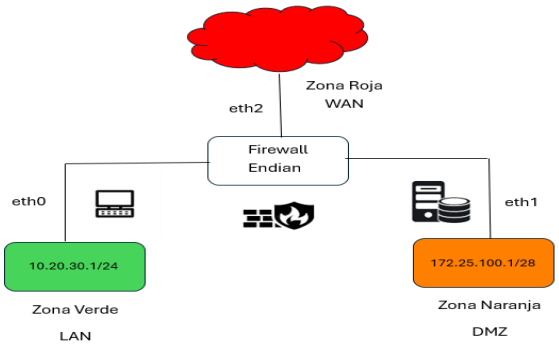
En Ubuntu Server se configura el adaptador 1 como red interna, asignándolo a la zona Naranja (DMZ) de modo que el servidor opere dentro del segmento destinado a servicios publicados y administrados por Endian.

Figura 3. Configuración del adaptador 1 de Ubuntu server

Fuente: Autoría Propia

La segmentación se realizó asignando la red 10.20.30.1/24 a la zona Verde para el Ubuntu Desktop, la red 172.25.100.1/28 a la zona Naranja para el Ubuntu Server y dejando la zona Roja en NAT para simular el acceso a Internet. Este esquema permite visualizar claramente cómo cada segmento mantiene su propia función dentro de la estructura administrada por Endian.

Figura 4. Diagrama de red para configurar Endian



Fuente: Autoría Propia

Al iniciar la instalación de Endian, se selecciona únicamente el idioma y se continúa con las opciones básicas de almacenamiento y preparación del sistema. Después, en la configuración de red, se asigna la dirección IP de la zona Verde, que será la interfaz principal de administración; por ejemplo, estableciéndola como 10.20.30.1/24, desde donde se ingresará luego a la consola web para completar el resto de la configuración. [2]

Figura 5. Configuración inicial de Endian

Fuente: Autoría Propia

Figura 6. Asignación de la IP de la zona verde

Fuente: Autoría Propia

En la pantalla inicial de Endian se visualizan las interfaces ya configuradas, mostrando claramente la zona Verde como interfaz de administración y la zona Roja conectada mediante NAT. Esta vista confirma que el sistema reconoce ambas zonas y que el firewall está listo para continuar con su ajuste.

Figura 7. Pantalla inicial con la zona verde y roja en Endian

Fuente: Autoría Propia

Para continuar con la configuración de Endian, desde el Ubuntu Desktop se abre el navegador y se ingresa la dirección correspondiente a la zona Verde para acceder a la consola web del firewall. El navegador muestra una advertencia debido al

certificado no seguro; se selecciona la opción avanzada y luego se confirma el acceso para continuar con la interfaz de administración de Endian.

Figura 8. Ingreso con la IP de la zona verde puerto 10443

Fuente: Autoría Propia

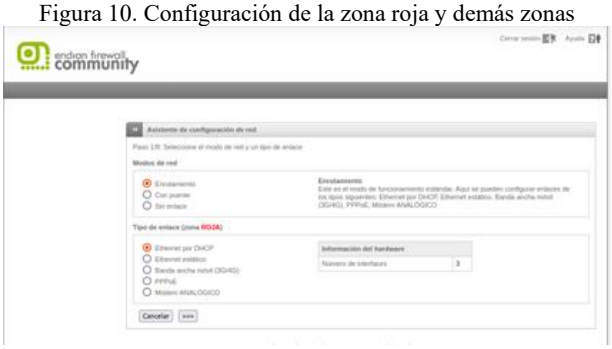
Al ingresar desde el navegador del Ubuntu Desktop a la dirección de la zona Verde, se carga la pantalla inicial del firewall Endian, donde se presenta la interfaz web de administración lista para continuar con la configuración del sistema.

Figura 9. Pantalla de inicio del firewall Endian

Fuente: Autoría Propia

En la interfaz inicial se indica que deben completarse ocho pasos de configuración, mostrando que el acceso a Internet se realizará en modo de enrutamiento mediante un enlace Ethernet por DHCP y que el sistema dispone de tres tarjetas de red para configurar. Al avanzar, se accede a la sección de la zona Roja, donde se habilita su conexión como interfaz hacia Internet y se confirman sus parámetros antes de continuar con el siguiente paso.

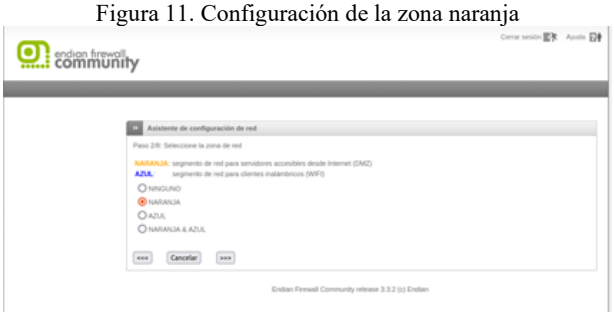
Figura 10. Configuración de la zona roja y demás zonas



Fuente: Autoría Propia

En la pantalla de configuración inicial de Endian se habilita la zona Naranja, asignando su interfaz correspondiente y dejando lista la DMZ para continuar con el proceso de configuración.

Figura 11. Configuración de la zona naranja



Fuente: Autoría Propia

En esta etapa se asignan las direcciones IP y la submáscara para cada segmento de red del firewall. La zona Verde se configura con la IP 10.20.30.1 y la máscara /24, mientras que la zona Naranja utiliza la IP 172.25.100.1 con máscara /28. Además, se definen los puertos físicos que ocupará cada interfaz en Endian, permitiendo que ambos segmentos queden correctamente estructurados y listos para su funcionamiento dentro del firewall.

Figura 12. Asignación de la IP y puertos de las zonas

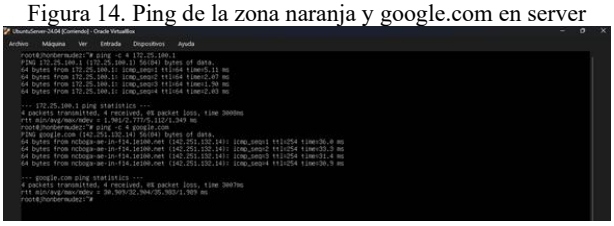
Fuente: Autoría Propia

En los pasos finales se deja la configuración por defecto hasta llegar al último apartado, donde Endian confirma que las direcciones asignadas para cada zona han sido guardadas correctamente. Para verificar el funcionamiento, se realizan pruebas de conectividad desde los equipos de la zona Verde y Naranja, comprobando que existe respuesta hacia destinos externos como google.com, confirmando así que la comunicación y la segmentación de red operan adecuadamente.

Figura 13. Ping de la zona verde y google.com en desktop

Fuente: Autoría Propia

Figura 14. Ping de la zona naranja y google.com en server



Fuente: Autoría Propia

En la pantalla principal de Endian se visualiza el panel de monitoreo, donde se observa el estado de las zonas Verde, Naranja y Roja. Allí se muestran sus interfaces activas, el tráfico que circula por cada una y el comportamiento general del firewall, permitiendo verificar en tiempo real la actividad y el funcionamiento de toda la red segmentada.

Figura 15. Pantalla del monitoreo de las zonas en Endian

Fuente: Autoría Propia

2.2 TEMÁTICA 2: CONFIGURACIÓN NAT.

El desarrollo de la configuración NAT (Network Address Translation) en el firewall Endian se basa en una arquitectura de red la cual esta segmentada por zona de colores.

Las zonas establecidas en la arquitectura de red trabajan son:

A) Zona roja (RED/WAN): es la que representa la red externa en donde el tráfico de datos es alto y de menor confiabilidad, normalmente su configuración precisa de una IP publica, en esta práctica de entorno virtual, la IP asignada es de naturaleza privada y se obtiene mediante DHCP en la configuración de Endian.
B) Zona verde (GREEN/LAN): es la que representa la red interna y es donde se encuentra los clientes, equipos de trabajo de las organizaciones
C) Zona naranja (ORANGE/DMZ): es la zona desmilitarizada y es donde se encuentran los servidores.

Una vez definida las zonas que conforman la arquitectura de red, se establece las subredes que identificaran o referenciaran cada zona:

Tabla 1. Arquitectura de la red.

Interfaz en Endian	Dirección IP (gateway)	Subred establecida	Rol de la zona
red (eth2)	10.0.4.15	10.0.4.0/24	wan
green (eth0)	10.20.30.1	10.20.30.0/24	lan/ cliente
orange (eth1)	172.25.100.1	172.25.100.0/28	dmz/ servidores

Fuente: Autoría Propia

La administración y manejo del tráfico de datos se llevará a cabo mediante la coordinación de las IP de origen (source) y destino (destination) a través de las funciones NAT en la interfaz del firewall de Endian, las cuales se detallarán a continuación.

La configuración de las reglas que permitirán la conexión de la zona verde (LAN/CLIENTE) y la zona naranja (DMZ/SERCIDORES) a la zona roja (WAN/INTERNET), se realizará a través de la interfaz de Endian. En donde se ingresa a la sección Firewall.

Para que la zona verde tenga comunicación con la zona roja, se realiza el siguiente proceso:

1. Se accede a la sección de firewall, posteriormente se ingresa a la sección de outgoing traffic (tráfico saliente).
2. Se accede a la opción de “add new rule” y se procede a crear la regla.
3. Se define en tipo de origen (type source) la zona verde.
4. Se define el tipo de destino (type Destination) se selecciona la zona roja.
5. Se especifica el tráfico seleccionando “any” en los servicios (service) y protocolos (protocol).
6. Se especifica las políticas (Policy) seleccionando “ALLOW wtih IPS”
7. Se crea la regla.

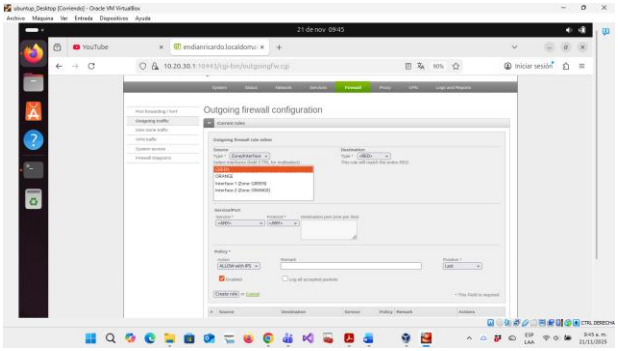
Como se observa en la tabla. 2 y la fig. 16.

Tabla 2. Regla 1: Acceso de la zona verde (LAN/CLIENTE) a la WAN

Característica	Valor de la configuración	Propósito
Source (origen)	Green	Determinar el segmento de red de origen para el flujo de datos.
Destination (Destino)	Red	Determinar el segmento de red de destino.
Services (servicios)	Any	Permite la comunicación a través de todos los puertos disponibles (80.443,21,25) etc.
Protocol (Protocolos)	any	Permite el uso de todos los protocolos de transporte para la comunicación (TCP, UDP, ICPM) etc.
Policiy (Políticas)	Allow with IPS	Permite la conexión y también implementa el sistema de prevención de instrucciones IPS.

Fuente: Autoría Propia

Figura 16. Regla 1: Acceso de la zona verde (LAN/CLIENTE) a la WAN



Fuente: Autoría Propia

Para que la zona naranja tenga comunicación con la zona roja, se realiza dos procesos:

El primero proceso es la creación de la siguiente regla:

1. Se accede a la sección de firewall, posteriormente se ingresa a la sección de outgoing traffic (tráfico saliente).
2. Se accede a la opción de “add new rule” y se procede a crear la regla.
3. Se define en tipo de origen (type source) la zona naranja.
4. Se define el tipo de destino (type Destination) se selecciona la zona roja.
5. Se especifica el tráfico seleccionando “any” en los servicios (service) y protocolos (protocol).
6. Se especifica las políticas (Policy) seleccionando “ALLOW wtih IPS”
7. Se crea la regla

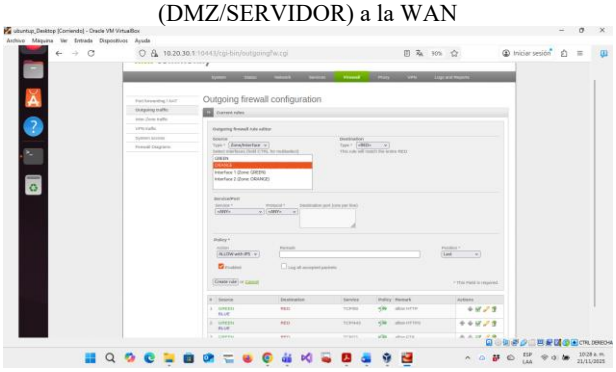
Como se observa en la tabla. 3 y la fig. 17.

Tabla 3. Regla 1: Acceso de la zona verde (DMZ/SERVIDOR) a la WAN

Característica	Valor de la configuración	Propósito
Source (origen)	Orange	Determinar el segmento de red de origen para el flujo de datos.
Destination (Destino)	Red	Determinar el segmento de red de destino.
Services (servicios)	Any	Permite la comunicación a través de todos los puertos disponibles.
Protocol (Protocolos)	any	Permite el uso de todos los protocolos de transporte para la comunicación (TCP, UDP, ICPM) etc.
Policiy (Políticas)	Allow with IPS	Permite la conexión y también implementa el sistema de prevención de instrucciones IPS.

Fuente: Autoría Propia

Figura 17. Regla 1: Acceso de la zona verde (DMZ/SERVIDOR) a la WAN



Fuente: Autoría Propia

El segundo proceso es la creación de la siguiente regla:

1. Se accede a la sección de firewall, posteriormente se ingresa a la sección de port forwarding /NAT traffic (reenvío de puertos).
2. Se accede a la opción de “add new Port forwarding / Destination NAT rule” y se procede a crear la regla.
3. Se define en tipo de zona (type Zone/VPN/Uplink) la zona naranja.
4. Se especifica el servicio o puerto de comunicación “any” en los servicios (service) y protocolos (protocol).
5. Se crea la regla.

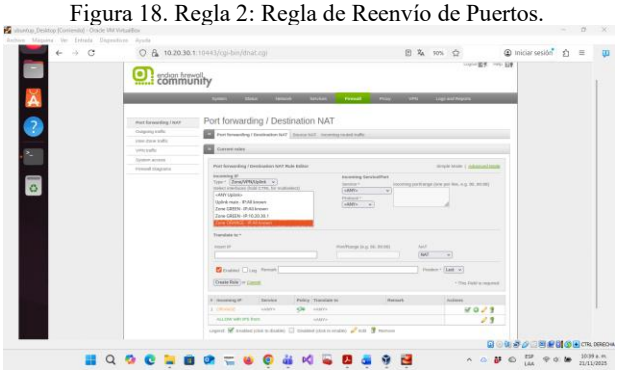
Como se observa en la tabla. 4 y la fig. 18.

Tabla 4. Regla 2: Regla de Reenvío de Puertos.

Característica	Valor de la configuración	Propósito
Incoming IP Type (origen)	Orange – ip all known	Determina la regla al tráfico entrante destinado a cualquier IP que este conocida dentro de la red naranja.
Incoming Service/Port	Red	Logra interceptar todos los puertos y servicios que llegan al DMZ (HTTP, HTTPS, SSH) etc.
Protocol (Protocolos)	Any	Logra interceptar todos los protocolos que llegan al DMZ (TCP, UDP, ICPM) etc.
Policiy (Políticas)	Allow with IPS	Permite el tráfico si las reglas del firewall lo permiten.

Fuente: Autoría Propia

Figura 18. Regla 2: Regla de Reenvío de Puertos.

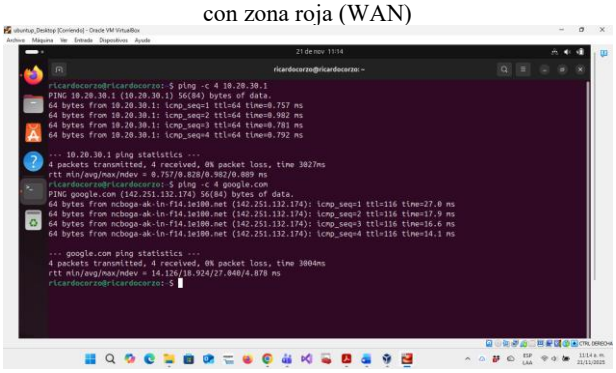


Fuente: Autoría Propia

La etapa final de la temática de configuración NAT es verificar que las reglas establecidas en la interfaz del firewall Endian están aplicando correctamente.

Primero se realiza la verificación y comprobación de la zona verde (LAN/CLIENTE) con la red roja (WAN) ejecutando el comando ping -c 4 a la ip de la zona que es 10.20.30.1 y a la página de Google.com.

Figura 19. Verificación conexión zona verde (LAN/CLIENTE) con zona roja (WAN)



Fuente: Autoría Propia

Posteriormente se realiza la verificación y comprobación de la zona naranja (DMZ/SERVIDOR) con la red roja (WAN) ejecutando el comando ping -c 4 a la IP de la zona que es 172.25.100.1 y a la página de Google.com

Figura 20. Verificación conexión zona naranja (DMZ/SERVIDOR) con zona roja (WAN)

Fuente: Autoría Propia

2.3 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

En esta temática se realizará la configuración de los servicios http (puerto 80) y ftp (puerto 21) desde el servidor web bajo Ubuntu server. además, se denegará el protocolo ICMP tanto en el puerto 8 como en el puerto 30, con el fin de no permitir hacer ping en la red. [3] todo esto será probado y confirmado haciendo uso de servicios establecidos en los puertos indicados y la terminal de los distintos sistemas.

Para permitir el tráfico del servicio http puerto 80. es necesario crear una regla dentro del firewall, desde la pestaña redireccionamiento de puertos/NAT de destino. la cual es la encargada de controlar el trafico de puertos dentro de las distintas zonas.

Se debe iniciar seleccionando la opción para agregar una nueva regla, una vez dentro de ella se desplegarán varias opciones necesarias para su configuración las cuales se configuran tal y como se describe en la tabla 5.

Tabla 5. Regla 1: Regla http puerto 80

Opción	Configuración	complemento
Dirección IP de entrada	Zona/VPN/Enlace activo	Enlace main-ip todos los conocidos
Servicio/ puerta de entrada	Servicio: HTTP Protocolo: TCP	Puerto:80
Insertar IP	172.25.100.10	Rango de puerto: 80 NAT: NAT

Fuente: Autoría Propia

Donde la opción insertar IP equivale a la IP asignada al servidor en el cual se correrá el servicio por el puerto 80, luego de configurar estos valores se da clic en guardar y aplicar. debe quedar una regla igual a la fig. 21.

Figura 21. Confirmación Creación Regla http

Fuente: Autoría Propia

Con la regla creada en la columna acciones es necesario validar que está se encuentre chuleada, asi se verifica que la regla esta activa. para validar su funcionamiento se utilizará un servicio apache que esta corriendo en el puerto 80 con una página de Moodle, dentro del servidor alojado en la zona naranja.

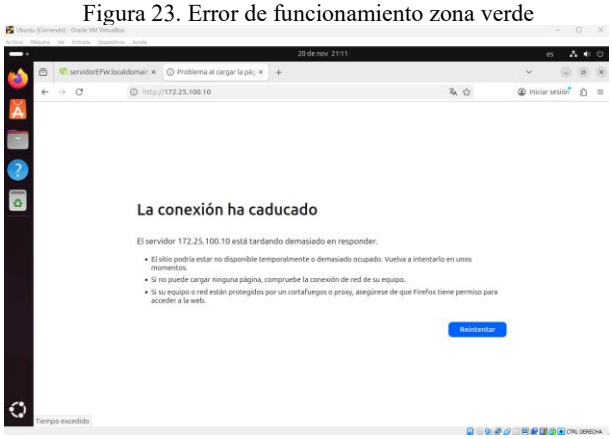
A este se accederá desde un equipo cliente con so Ubuntu ubicado en la zona verde de la red. Fig. 22 como la regla esta activa (chuleada) el equipo cliente podrá acceder sin problema

Figura 22. Validación de funcionamiento zona verde

Fuente: Autoría Propia

Para confirmar que es debido a esta regla que se permite el acceso en el panel administrador de Endian se desactiva la regla (desmarcar) y se intenta acceder nuevamente fig. 23. Se puede evidenciar como el acceso no esta permitido y la pagina no carga caducando su tiempo de espera.

Figura 23. Error de funcionamiento zona verde



Fuente: Autoría Propia

Para permitir la transferencia ftp en el puerto 21 se realiza un proceso muy similar al ejecutado anteriormente, ya que el permiso es manejado de la misma forma el cambio más importante será el servicio habilitado cambiando su valor de http a ftp.

Como primer paso se debe crear una nueva regla haciendo clic en el botón agregar nueva regla una vez dentro de la página de creación se configuran las opciones tal y como se describe en la tabla 6.

Tabla 6. Regla 2: Regla ftp puerto 21

Opción	Configuración	complemento
Dirección IP de entrada	Zona/VPN/Enlace activo	Enlace main-ip todos los conocidos
Servicio/ puerta de entrada	Servicio: FTP Protocolo: TCP	Puerto:21
Insertar IP	172.25.100.10	Rango de puerto: 21 NAT: NAT

Fuente: Autoría Propia

Donde la opción insertar IP equivale a la IP asignada al servidor en el cual se correrá el servicio por el puerto 21, luego de configurar estos valores se da clic en guardar y aplicar. deben quedar dos reglas igual a la fig. 24.

Figura 24. Confirmación Creación Regla ftp

Fuente: Autoría Propia

Una vez creada la regla, para validar su funcionamiento se realizará una prueba a través de la aplicación FileZilla. la cual permite la transferencia de archivos por ftp, En la zona naranja se encontrará en ejecución la aplicación del servidor de filezilla y en la zona verde se encontrará en ejecución la aplicación cliente. [4]

Para realizar la conexión y validar el funcionamiento es necesario rellenar los campos solicitados por FileZilla con los datos del servidor Ubuntu ubicado en la zona naranja. cabe resaltar que el campo usuario y contraseña son los del usuario del servidor y no del equipo cliente tabla 7.

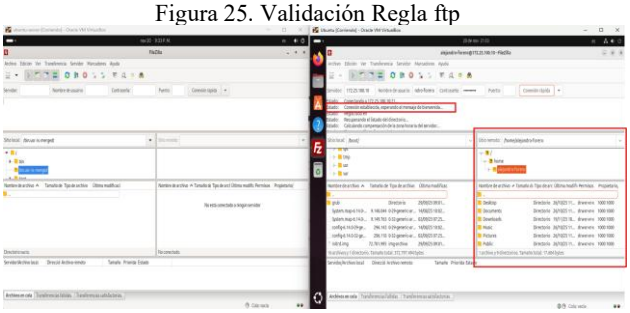
Tabla 7. Campos FileZilla

servidor	Nombre de usuario	Contraseña	puerto
Ip:172.25.100.10	Alejandro-forero	*********	21

Fuente: Autoría Propia

Como la regla esta activa (chuleada) el equipo cliente podrá acceder sin problema y el programa notificara que la conexión fue establecida mostrando los archivos disponibles dentro del servidor tal y como se evidencia en la fig 25. Del lado derecho el equipo cliente y el izquierdo el servidor.

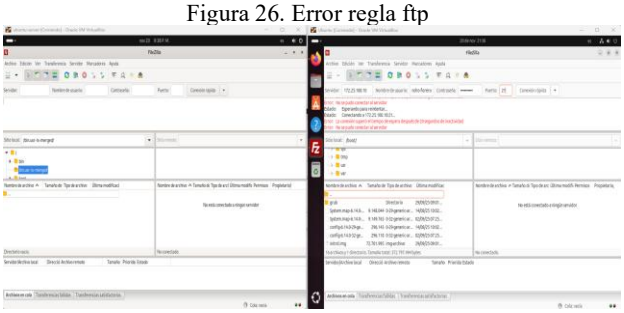
Figura 25. Validación Regla ftp



Fuente: Autoría Propia

Con el fin de confirmar que es debido a esta regla que se permite el acceso en el panel administrador de Endian se desactiva la regla (desmarcar) y se intenta acceder nuevamente fig. 26. Se puede evidenciar como el acceso no está permitido y el programa no puede encontrar el servidor caducando su tiempo de espera y notificando el servidor inaccesible.

Figura 26. Error regla ftp



Fuente: Autoría Propia

Para denegar el tráfico de ping en la red, se debe aplicar una configuración en el tráfico entre zonas. para el protocolo ICMP en el puerto 8 y puerto 30 esta regla, aunque es similar a las creadas anteriormente varia a que zonas y desde donde se aplica

Para la creación de esta regla es necesario acceder al panel de configuración Endian y dentro de la pestaña firewall seleccionar la opción trafico entre zonas. Una vez dentro se debe dar clic en el botón Añadir una nueva regla de firewall inter-zona [5]

Dentro de la página de creación de regla se desplegarán varias opciones entre ellas destaca el origen y el destino, como la idea es denegar el ping en toda la red el origen y el destino serán las dos zonas disponibles (verde y naranja). los demás campos son muy similares a los de los servicios permitidos anteriormente.

Para la configuración de esta regla se deben llenar todos los campos disponibles con los valores indicados en la tabla 8.

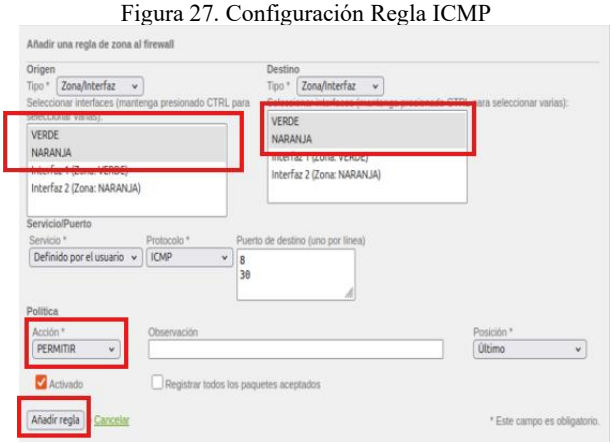
Tabla 8. Regla 3: Configuración Regla ICMP

Opción	Configuración	complemento
origen	Zona / Interfaz	VERDE NARANJA
Destino	Zona / Interfaz	VERDE NARANJA
Servicio/puerto	Servicio: definido por el usuario Protocolo: ICMP	8 30
Política / acción	PERMITIR	Observación (en blanco/ descripción de la regla)

Fuente: Autoría Propia

Esta configuración puede ser un poco más larga y confusa dentro de los puntos importantes se encuentra seleccionar las zonas de origen y destino manteniendo oprimida la tecla ctrl, las opciones seleccionadas quedaran de color gris a diferencia del resto. otro punto importante es dar enter luego de digitar cada puerto además de seleccionar permitir y no permitir con IP, para una guía mas grafica revisar la fig 27.

Figura 27. Configuración Regla ICMP

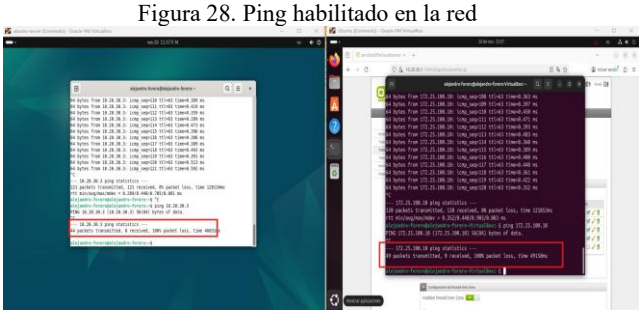


Fuente: Autoría Propia

Con la creación de la regla realizada, el ping entre la red será permitido siempre y cuando esta esté activa. para validar su funcionamiento se deberá realizar un ping desde la terminal del equipo cliente hacia el servidor Ubuntu (zona verde a zona naranja) y viceversa con la regla habilitada.

Primero se validan las direcciones IP de los distintos hosts abriendo una terminal y ejecutando el comando ifconfig y una vez validada la IP de cada host se ejecuta el comando ping en los dos equipos la respuesta de los quipos debe ser muchos paquetes transmitidos, y recibidos tal y como se detalla en la fig 28.

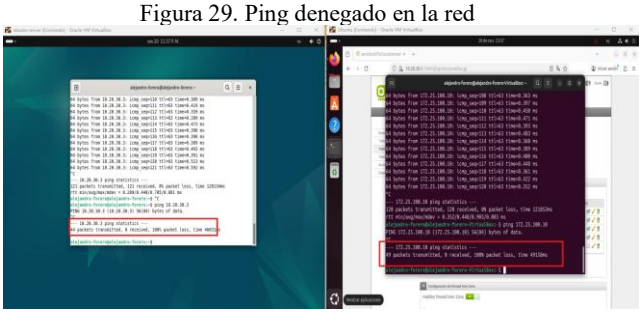
Figura 28. Ping habilitado en la red



Fuente: Autoría Propia

Para validar que debido a la regla el ping no es permitido en el panel de administración de Endian se deshabilita la regla (Desmarcar), y nuevamente se intenta realizar un ping entre los dos hosts como se puede evidenciar en la fig 29. el ping no obtiene respuesta y solo se evidencian muchos paquetes enviados y cero paquetes recibidos.

Figura 29. Ping denegado en la red



Fuente: Autoría Propia

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

El establecimiento de reglas de acceso para permitir o denegar el tráfico entre la zona Verde (LAN), la zona Naranja (DMZ) y la zona Roja (WAN), se realiza ingresando a la pestaña de Firewall en la interfaz web del servidor Endian,[6] como se puede observar en la siguiente figura.

Figura 30. Ingreso a la interfaz de Firewall en Endian firewall community

Fuente: Autoría Propia

Para realizar la comunicación interna entre la zona verde y la zona naranja mediante el protocolo HTTP y FTP con sus respectivos puertos, se debe ingresar a la pestaña de Trafico entre zonas y establecer una nueva regla de firewall Inter-zona. Como se aprecia a continuación en la figura 22.

Figura 31. Configuración de firewall Inter-zona

Fuente: Autoría Propia

Para establecer la comunicación entre zonas verde y naranja mediante el protocolo HTTP. Dar clic en añadir nueva regla, se despliega un menú de configuración el cual se diligencia de la siguiente forma:

Sección Origen, se selecciona Zona/Interfaz y la opción Verde.

Sección Destino, se selecciona Zona/Interfaz y la opción Naranja.

Sección Servicio/Puerto, se selecciona servicio HTTP, protocolo TCP y puerto de destino 80.

Sección Política, Acción, se selecciona permitir.

Sección observaciones, opcional se coloca el objetivo de la regla.

Seleccionar añadir regla.

Aplicar.

Figura 32. Tráfico HTTP zonas Verde y Naranja

Fuente: Autoria Propia

De igual forma, para realizar la comunicación entre la zona verde y la zona naranja mediante el protocolo FTP se deben seguir los siguientes pasos:

Al dar clic en añadir nueva regla, se despliega un menú de configuración la cual se diligencia de la siguiente forma:

Sección Origen, se selecciona Zona/Interfaz y la opción Verde.

Sección Destino, se selecciona Zona/Interfaz y la opción Naranja.

Sección Servicio/Puerto, se selecciona servicio FTP, protocolo TCP y puerto de destino 21.

Sección Política, Acción, se selecciona permitir.

Sección observaciones, opcional se coloca el objetivo de la regla.

Seleccionar añadir regla.

Aplicar.

Figura 33. Tráfico FTP zonas Verde y Naranja

Fuente: Autoria Propia

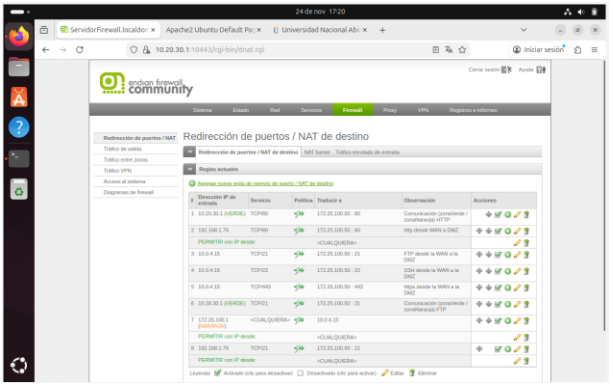
Realizada la configuración del tráfico entre zonas debe quedar la configuración de la siguiente forma como se muestra en la imagen.

Figura 34. Resultado de tráficos

Fuente: Autoria Propia

Ahora bien, para realizar la configuración de las reglas para comunicar la zona Roja de internet WAN con la zona Naranja DMZ, se ingresa a la seccion Firewall/Redireccion de puertos /NAT destino, allí establecer se debe crear una neva regla en la opcion “agregar una nueva regla de renvio de puertos/NAT de destino” como se muestra en la figura 35.

Figura 35. Configuración de reglas de comunicación de la WAN a la DMZ



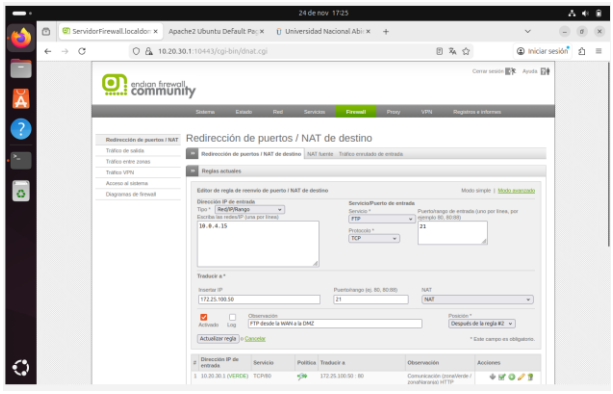
Fuente: Autoria Propia

Ya en el menu de configuración se procede a establecer los parametros para la comunicación de la zona roja WAN y la zona DMZ naranja estableciendo la traduccion de los paquetes de entrada entre el firwall y el servidor. Estos parametros se deben establecer de la siguiente forma:

Direccion IP de entrada:
Protocolo
Puerto
Traducir a (indicar la direccion IP, en este caso el servidor)

Como se establece en la siguiente figura

Figura 36. Establecimiento de parametros para la comunicación



Fuente: Autoria Propia

Para evidenciar el corrrecto funcionamiento de las reglas establecidas anteriormente se realizo una serie de pruebas donde se realizo la comunicación entre la zona LAN y la zona DMZ por medio del protocolo HTTP ingresando al explorador de la distribución ubuntu desktop, el cual estaba ubicado en la zona Verde LAN y se procedio acceder al servidor mediante la URL: http://172.25.100.50 , la cual dio como resultado la visualización de la pagina por defecto de Apache2, la cual se instalo previamente en el Servidor Ubuntu tal y como ilustra la imagen.

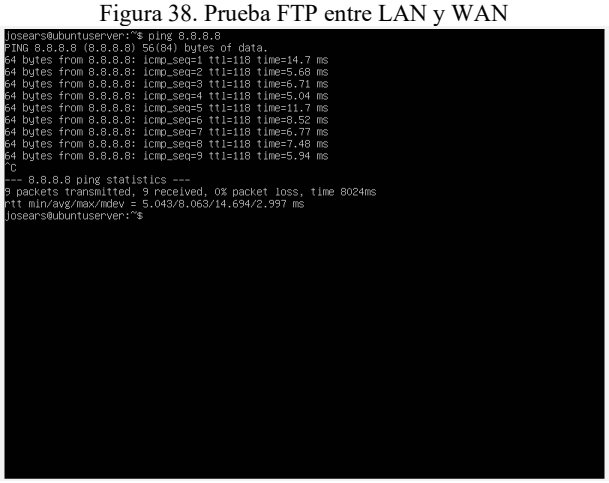
Figura 37. Comunicación HTTP zona LAN y DMZ

Fuente: Autoria Propia

De la misma forma se realizo la prueba con el protocolo FTP ingresando en el explorador la URL: ftp://172.25.100.50, dando como resultado un usuario FTP configurado previamente en el servidor. Asi mismo se realizaron las pruebas de conexión por medio de los protocolos HTTP Y FTP de la LAN a la WAN.

Ahora para revisar la conexión de la zona Naranja DMZ a la WAN se procedio a realizar un ping a los servidores de google desde la terminal del servidor

Figura 38. Prueba FTP entre LAN y WAN



Fuente: Autoria Propia

Y para la verificicación de ingreso del servicio HTTP desde la WAN hacia la zona DMZ. Se procedio a ingresar al explorador de Windows 11 la cual es la maquina anfitriona ubicada en la zona Roja WAN y escribir la URL del firewall el cual redirecciono al servidor gracias a la regla establecida anteriormente.

Figura 39. Comunicación HTTP entre WAN y DMZ

Fuente: Autoria Propia

Y por ultimo se procedio a verificar la comunicación entre la zona Roja y la zona DMZ mediante el protocolo FTP ingresando la URL del firewall de Indian el cual tradujo los paquetes y redirecciono al ubuntu server que como respuesta dio el ingreso a un usuario FTP previamente configurado.

Figura 40. Comuniacion FTP entre WAN y DMZ

Fuente: Autoria Propia

3 CONCLUSIONES

La configuración inicial de Endian permitió establecer correctamente la estructura de red fundamental mediante la asignación de las zonas Verde, Naranja y Roja dentro del entorno virtual, la definición de cada interfaz y su integración con los equipos Ubuntu aseguró una segmentación adecuada y una comunicación estable entre los componentes. Este proceso sentó las bases necesarias para continuar con las configuraciones avanzadas y garantizar un funcionamiento organizado y seguro del firewall.

La configuración NAT con su respectiva implementación y verificación de sus reglas demostró que es un procedimiento efectivo en el control y seguridad del flujo de tráfico que puede haber en una arquitectura de red segmentada en tres zonas, las cuales para la temática son (verde, naranja y roja). De esta manera se garantizó un acceso funcional y efectivo desde la zona verde (LAN/CLIENTE) y la red naranja (DMZ/SERVIDOR) a la red roja (WAN). El proceso de verificación demostró que la implementación y uso del firewall Endian proporciona no solo la segmentación de red apropiada, sino que además logra darle un equilibrio a la accesibilidad de los servicios en conjunto con la seguridad que requiere.

La denegación de servicios dentro de una red segmentada por zonas, tal y como la que se genero en el caso de estudio es parte fundamental, esto para impedir el acceso no autorizado a servicios específicos y así disminuir la vulnerabilidad de la red

Las reglas de acceso permiten controlar el flujo de tráfico de datos entre las diferentes zonas de la red, priorizando la seguridad entre las zonas naranja y verde, para de esta forma permitir, denegar o rechazar conexiones

4 REFERENCIAS

[1] Ben Endian Luisaigner, Peter Endian, Vallazza. (2023, abril 10). *Comunidad de firewall Endian*. Sourceforge. https://sourceforge.net/projects/efw/

[2] Koromicha. (2024, 25 julio). Install and Configure Endian Firewall on VirtualBox - kifarunix.com. kifarunix.com. https://kifarunix.com/install-and-configure-endian-firewall-on-virtualbox/

[3] Endian S.R.L., *Endian Firewall Community Documentation* (Online). [Año de consulta, ej., 2024]. [Online]. Available: https://www.endian.com/en/community/

[4] FileZilla - The free FTP solution. (s/f). Filezilla-project.org. Recuperado 2025, de https://filezilla-project.org/

[5] *Endian UTM 3.2 Reference Manual — Endian UTM 3.2 Reference Manual*. (s. f.). https://docs.endian.com/3.2/utm/index.html

[6] InfoRed (2019). Cómo Configurar Endian Paso a Paso Parte 3: https://www.youtube.com/watch?v=oeDawngVv6g&t=1331s