# CONFIGURACIÓN DE SERVICIOS HTTP Y FTP EN UNA ZONA DMZ CON RESTRICCIONES ICMP UTILIZANDO ENDIAN FIREWALL.

Oscar Arley Cruz Herrera.
oacruzh@unadvirtual.edu.co

**RESUMEN:** *El presente trabajo describe la configuración de servicios HTTP y FTP en una zona DMZ mediante Endian Firewall en un entorno virtualizado. La implementación se realizó utilizando Ubuntu Server como servidor y VirtualBox como herramienta de virtualización. Se configuraron reglas de firewall para permitir el acceso a los servicios HTTP (puerto 80) y FTP (puerto 21) desde la red, garantizando la comunicación controlada entre las zonas configuradas. También, se aplicaron restricciones al protocolo ICMP mediante reglas de filtrado que impiden la respuesta a solicitudes de ping, fortaleciendo la seguridad de la infraestructura de red. Las pruebas de conectividad y monitoreo del tráfico permitieron verificar el correcto funcionamiento de las políticas implementadas y la creación de reglas de salida en el firewall. Los resultados obtenidos evidencian un adecuado control de acceso y segmentación de servicios en la zona DMZ.*

**PALABRAS CLAVE**: Endian Firewall, ICMP, HTTP, Seguridad perimetral.

# 1 INTRODUCCIÓN

La gestión de servicios en zonas desmilitarizadas o DMZ constituye un elemento esencial en la implementación de arquitecturas de red seguras, ya que permite la exposición controlada de servicios hacia redes externas sin comprometer la integridad de la red interna. En este contexto, el presente trabajo aborda la configuración de una DMZ utilizando Endian Firewall en un entorno virtualizado, enfocándose en la habilitación de servicios web y de transferencia de archivos.

Se implementa la exposición de servicios HTTP (puerto 80) y FTP (puerto 21) en un servidor Ubuntu ubicado en la zona naranja del DMZ, permitiendo su acceso desde la red interna bajo reglas de control definidas. Adicionalmente, se establecen políticas de seguridad para restringir el protocolo ICMP, con el fin de impedir respuestas a solicitudes de diagnóstico como ping, ayudando a reducir posibles vectores de reconocimiento en la red.

Por último, se validan las reglas configuradas mediante pruebas de conectividad y análisis del tráfico, evidenciando el correcto funcionamiento de las políticas de seguridad aplicadas en la zona DMZ.

# 2 MARCO TEÓRICO

## 2.1 ZONA DESMILITARIZADA (DMZ)

Es una subred o un segmento de red perimetral el cual actúa como un amortiguador o capa adicional de seguridad entre la red interna de confianza (LAN o Zona Verde) y una red externa no confiable, generalmente Internet [1][3]. El propósito principal es permitir que una organización ofrezca servicios públicos, como servidores web (HTTP), servidores de archivos (FTP) o servidores de correo, a usuarios externos, mientras el proveedor mantiene aislados y protegidos los recursos y datos sensibles de su red privada [8]. Para poder lograr este aislamiento, la DMZ se sitúa idealmente entre dos firewalls o en un segmento dedicado de un único firewall con múltiples interfaces, donde el primer firewall filtra el tráfico proveniente de Internet hacia la DMZ y un segundo firewall controla rigurosamente las comunicaciones desde la DMZ hacia la red interna [1].

## 2.2 PROTOCOLO ICMP

Es un protocolo fundamental de la capa de red de nivel 3 del modelo OSI, el cual es utilizado por los dispositivos de red, como routers y servidores, para comunicar errores en la transmisión de datos y realizar diagnósticos de conectividad [2][4]. A diferencia de protocolos orientados a conexión como TCP, ICMP opera de manera sin conexión, lo que significa que un dispositivo puede enviar un mensaje ICMP a otro sin necesidad de establecer una comunicación previa [7]. Su uso más conocido es a través de los comandos de diagnóstico ping y traceroute: el primero utiliza mensajes de "solicitud de eco" (tipo 8) y "respuesta de eco" (tipo 0) para verificar si un host remoto está activo y medir la latencia en la red, mientras que el segundo permite trazar la ruta que siguen los paquetes hasta su destino, identificando cada salto o router intermedio [2][4]. En el contexto de la seguridad de redes, aunque ICMP es una herramienta valiosa para el diagnóstico, también puede ser explotado maliciosamente en ataques de denegación de servicio (DDoS), como las inundaciones de ping o los ataques Smurf, por lo que es común que los administradores restrinjan o bloqueen selectivamente el tráfico ICMP en firewalls perimetrales [2][7].

## 2.3 REGLAS DE FILTRADO

Son las que constituyen el mecanismo fundamental mediante el cual un firewall controla todo el tráfico de red que intenta atravesar sus interfaces, permitiendo o denegando paquetes según un conjunto predefinido de condiciones [5][6]. Estas reglas operan bajo el principio de evaluación secuencial, lo que significa que los paquetes se comparan con cada regla en un orden específico por lo general de arriba a abajo, y la primera regla que coincida con las características del paquete determina la acción a aplicar, ya sea permitir, denegar o en algunos casos, solicitar una acción al usuario [5][9]. Un firewall de filtrado de paquetes, como el implementado en Endian, inspecciona las cabeceras de los paquetes a nivel de red y transporte, lo que le permite tomar decisiones rápidas y eficientes sin necesidad de analizar el contenido completo de cada paquete [6]. Una lección crítica en la administración de firewalls es la importancia del orden de las reglas: las reglas

más específicas deben colocarse al principio de la tabla, antes que las reglas genéricas, para garantizar que se evalúen correctamente [5][9]. La correcta implementación de reglas de filtrado permite aplicar el principio de "mínimo privilegio", donde un servidor en la DMZ solo tiene permitido el tráfico estrictamente necesario para su funcionamiento como HTTP y FTP, mientras que todo el resto del tráfico incluyendo ICMP permanece bloqueado [6][8].

# 3 IMPLEMENTACIÓN

## 3.1 INFRAESTRUCTURA DE RED

La infraestructura propuesta para el desarrollo del laboratorio se presenta en la Tabla 1, en la cual se detalla la configuración de la red, especificando los tipos de adaptadores de red, interfaces y las direcciones IP asignadas a cada zona de seguridad.

*Tabla 1.*
Direccionamiento IP.

| Zona | Interfaz / Adaptador | Dispositivo | Dirección IP |
|---|---|---|---|
| LAN (Verde) | eth0 / Red interna | Ubuntu Desktop | 192.168.0.0 |
| DMZ (Naranja) | eth1 / Red interna | Ubuntu Server | 192.168.20.0 |
| WAN (Roja) | eth2 / NAT | Endian Firewall | DHCP/NAT |

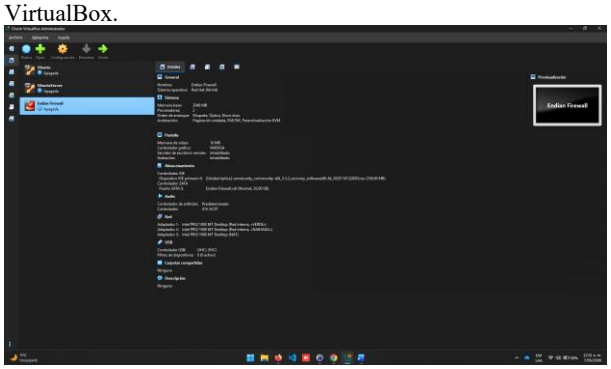
Nota. El esquema de direccionamiento IP define la segmentación de zonas en Endian Firewall para la aplicación de políticas de seguridad entre WAN, LAN y DMZ.

## 3.2 CONFIGURACIÓN DE MÁQUINA VIRTUAL Y ASIGNACIÓN DE ADAPTADORES DE RED

Se realizó la creación de una máquina virtual en VirtualBox, en la cual se cargó la imagen ISO de Endian Firewall Community versión 3.3.2. Posteriormente, se configuraron tres adaptadores de red con el objetivo de establecer la segmentación de las zonas de seguridad.

El primer y segundo adaptador fueron configurados como red interna, asignando los nombres “Verde” y “Naranja”, correspondientes a las zonas LAN y DMZ, respectivamente. El tercer adaptador fue configurado en modo NAT, permitiendo la salida hacia Internet a través de la red del host, como se observa en la Figura 1.

Figura 1.
Configuración de adaptadores de red en máquina virtual VirtualBox.

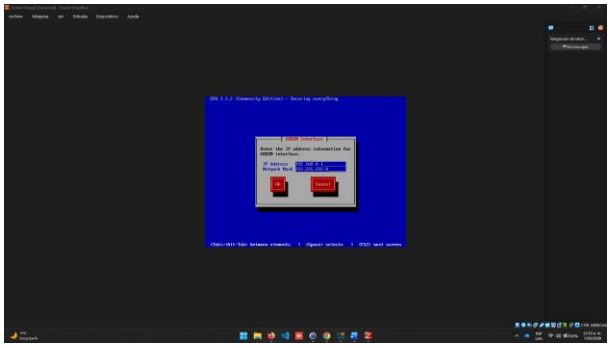


Fuente: Autoría Propia.

## 3.3 CONFIGURACIÓN INICIAL DEL SISTEMA ENDIAN FIREWALL

Se inicia la máquina virtual con Endian Firewall y se procede con el proceso de instalación, siguiendo las instrucciones del asistente hasta la asignación de la dirección IP correspondiente a la zona Verde. En esta etapa se configura la dirección 192.168.0.1 para la interfaz LAN, como se observa en la Figura 2.

Figura 2.
Configuración de la interfaz de la zona Verde (LAN) en Endian Firewall

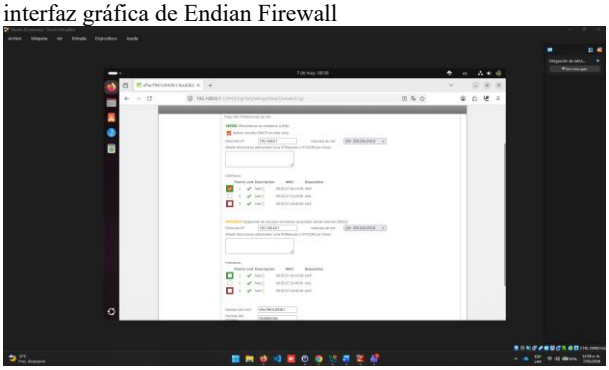


Fuente: Autoría Propia.

Finalizada la instalación, se accede al entorno gráfico de administración de Endian desde un equipo cliente mediante un navegador web, utilizando la dirección https://192.168.0.1:10443. Para este acceso, fue necesario ajustar el adaptador de red de la máquina virtual en modo red interna, asegurando que coincidiera con la configuración establecida previamente en la zona “Verde”.

En esta fase, el sistema solicita completar la configuración inicial, donde se define la zona Naranja asignando la dirección IP 192.168.20.10, correspondiente al servidor Ubuntu ubicado en la DMZ. Este proceso se evidencia en la Figura 3.

Figura 3. Configuración de la zona Naranja (DMZ) desde la interfaz gráfica de Endian Firewall



Fuente: Autoría Propia.

## 3.4 CONFIGURACIÓN DE REGLAS DE FILTRADO EN ENDIAN.

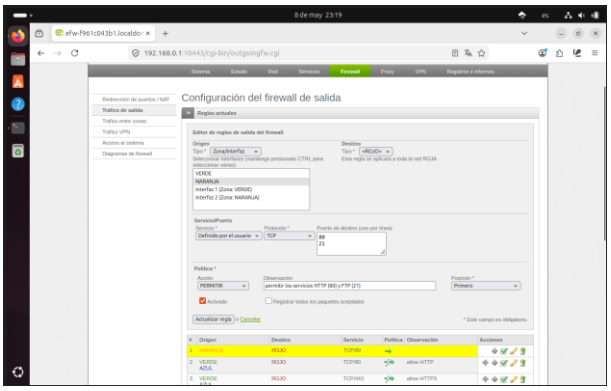
Para el desarrollo de la temática 3, fue necesario configurar en VirtualBox el adaptador de red en modo red interna, asignándole el nombre “Naranja”, correspondiente a la zona DMZ. Adicionalmente, se realizó la instalación de los servicios Apache2 y VSFTPD en el servidor Ubuntu, habilitando los protocolos HTTP y FTP, también se realiza la verificación que estos servicios se encontraran activos para el desarrollo de las pruebas.

Después, se realizó la configuración de reglas de filtrado en el módulo Firewall - Tráfico de salida en el entorno gráfico de Endian, dado que este módulo controla las conexiones iniciadas desde las zonas internas hacia redes externas.

### 3.4.1 PERMISO PARA SERVICIOS HTTP (PUERTO 80) Y FTP (PUERTO 21).

Se creó una única regla en el módulo Firewall - Tráfico de salida que agrupa ambos servicios. En la configuración de la regla, se seleccionó como origen la zona NARANJA mediante el tipo “Zona/Interfaz”, y como destino la zona ROJA, mediante tipo “ROJO”. Para el servicio, se seleccionó la opción “Definido por el usuario” con protocolo TCP, donde se especifica en el campo “Puerto de destino” los valores 80 y 21, cada uno en una línea independiente. La acción configurada fue Permitir, En observación se dejó una descripción de la regla, la posición se estableció como Primero para garantizar su evaluación temprana en la cadena de filtrado, y el estado se dejó como Activo, como se visualiza en la figura 4.

Figura 4.
Configuración de regla para permitir servicios HTTP y FTP.




Fuente: Autoría Propia.

Las pruebas de conectividad se ejecutaron desde el servidor Ubuntu con dirección 192.168.20.10 utilizando los siguientes comandos.

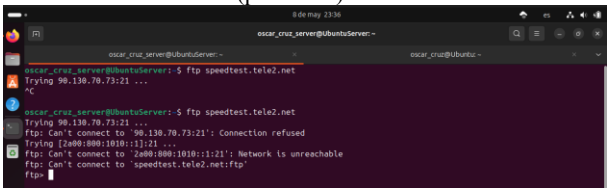
Para las pruebas del servicio HTTP se utilizó el comando “curl -4 -I http://www.google.com” donde el resultado que arrojo después de activar la regla es HTTP/1.1 200 OK, antes de que se creara la regla se quedaba colgado sin dar conexión, como se evidencia en la figura 5.

Figura 5.
Pruebas de servico HTTP (puerto 80).


Fuente: Autoría Propia.

Para las pruebas del servicio FTP se utilizó el comando “ftp speedtest.tele2.net”, donde el resultado después de activar la regla es “Connected to speedtest.tele2.net”. Antes de crear la regla al ejecutar el comando se queda en “Trying” sin generar alguna conexión, como se visualiza en la figura 6.

Figura 6.
Pruebas de servico FTP (puerto 21).

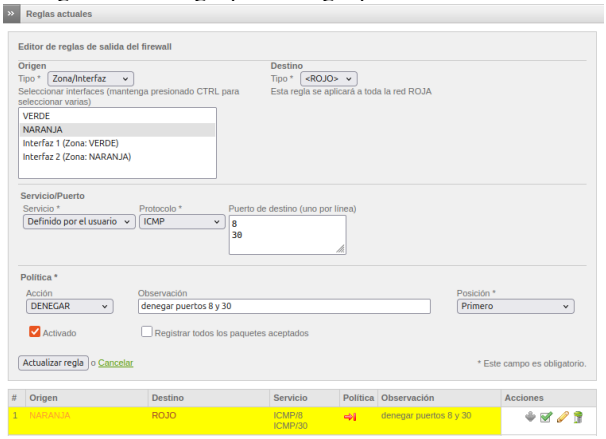



Fuente: Autoría Propia.

### 3.4.2 DENEGACIÓN DEL PROTOCOLO ICMP

Para bloquear el comando ping desde la zona naranja, se configuró una regla adicional en Firewall - Tráfico de salida. En esta regla, se definió como origen la zona NARANJA y como destino la zona ROJO. El servicio seleccionado fue "Definido por el usuario" con protocolo ICMP, donde se especifica en el campo "Puerto de destino" los valores 8 y 30. La acción se configuró como Denegar, y se asignó la posición Primero, de modo que esta regla se evalúe antes que la regla de permitir, garantizando así que los paquetes ICMP sean bloqueados antes de que cualquier regla más permisiva pueda autorizarlos, como se visualiza en la figura 7.

Figura 7.
Configuración de regla para denegar protocolos ICMP.




Fuente: Autoría Propia.

Para las pruebas del protocolo ICMP se utilizó el comando "ping 8.8.8.8", donde el resultado después de crear la regla es "100% packet loss". Antes de crear la regla permitía la conexión sin perder paquetes, como se evidencia en la figura 8.

Figura 8.
Pruebas de servico ICMP (puerto 8 y 30).


Fuente: Autoría Propia.

### 3.4.3 VALIDACIÓN DEL ORDEN DE LAS REGLAS

Finalmente, se verificó la jerarquía de las reglas configuradas en el módulo Firewall - Tráfico de salida. La tabla de reglas quedó estructurada de la siguiente manera: en la primera posición se ubicó la regla correspondiente al protocolo ICMP con acción Denegar; en la segunda posición se ubicó la regla para los servicios HTTP (puerto 80) y FTP (puerto 21) con acción Permitir. Este orden garantiza que los paquetes de ping sean denegados antes de que cualquier regla de permitir pueda evaluarlos, mientras que el tráfico legítimo de HTTP y FTP es aceptado al coincidir con sus respectivas reglas posteriores, como se evidencia en la figura 9.

Figura 9.
Tabla de reglas completa en Tráfico de salida.


Fuente: Autoría Propia.

## 4 CONCLUSIONES

La conclusión para la temática 3, permitió comprender de manera práctica el funcionamiento de un firewall perimetral y la implementación de una zona DMZ mediante Endian, logrando configurar exitosamente el permiso de tráfico HTTP (puerto 80) y FTP (puerto 21) desde la zona naranja hacia Internet, así como la denegación del protocolo ICMP para bloquear el comando ping. Durante el desarrollo se presentaron dificultades como la resolución de nombres mediante IPv6, la cual se solucionó forzando el uso de IPv4 con el flag -4 en el comando curl; y el orden de evaluación de las reglas, que se corrigió ubicando la regla ICMP en la primera posición de la tabla y las reglas HTTP y FTP en posiciones posteriores. Estas dificultades permitieron afianzar conceptos fundamentales como la segmentación de red, la diferencia entre tráfico entre zonas y tráfico de salida, y la importancia de la jerarquía en las políticas de filtrado.

## 5 REFERENCIAS


[1] Fortinet, "¿Qué es una red DMZ y por qué la usaría?" Fortinet Cyberglossary. [Online]. Available: https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz

[2] Fortinet, "¿Qué es ICMP (Protocolo de control de mensajes de Internet)?" Fortinet Cyberglossary. [Online]. Available: https://www.fortinet.com/lat/resources/cyberglossary/internet-control-message-protocol-icmp

[3] J. Ocampos, "Zona Desmilitarizada (DMZ)," jorgeocampos.blog, Jul. 2024. [Online]. Available: https://jorgeocampos.blog/2024/07/09/zona_desmilitarizada_dmz/

[4] Amazon Web Services, "¿Qué es ICMP? Explicación del protocolo ICMP," AWS What Is. [Online]. Available: https://aws.amazon.com/es/what-is/icmp/

[5] ESET, "Reglas de firewall," *ESET Endpoint Security Help*, version 10.1. [Online]. Available: https://help.eset.com/ees/10.1/es-CL/idh_dialog_epfw_app_tree_rules_page.html

[6] Palo Alto Networks, "¿Qué es un firewall de filtrado de paquetes?" *Palo Alto Networks Cyberpedia*. [Online]. Available: https://www.paloaltonetworks.lat/cyberpedia/what-is-a-packet-filtering-firewall

[7] Cloudflare, "¿Qué es el ICMP? | Protocolo ICMP," Cloudflare Learning Center. [Online]. Available: https://www.cloudflare.com/es-es/learning/ddos/glossary/internet-control-message-protocol-icmp/
[8] AI Multiple, "Zona Desmilitarizada (DMZ): Ejemplos y Arquitectura," aimultiple.com. [Online]. Available: https://aimultiple.com/es/dmz
[9] TVC Ingeniería, "Cómo funcionan las reglas de filtrado del firewall," *foro.tvc.mx*, Mar. 2026. [Online]. Available: https://foro.tvc.mx/docs/como-funcionan-las-reglas-de-la-politica-de-balanceo-de-carga-en-firewall-1