CONFIGURACION DE REGLAS DE ACCESO PARA COMUNICACIÓN SEGURA ENTRE ZONAS DE RED

John Alexander Arturo Quintero
e-mail: jaarturoq@unadvirtual.edu.co

RESUMEN: *La configuración adecuada de reglas de acceso es fundamental para garantizar la seguridad y funcionalidad de las redes de computadores. En este artículo, se presenta un enfoque sistemático para configurar reglas de acceso que permitan o denieguen tráfico entre diferentes zonas de red, específicamente entre la Zona Verde y la Zona Naranja con protocolos HTTP y FTP, y entre la Zona Internet y la Zona DMZ. Se detallan los pasos para crear reglas de acceso específicas, verificar el tráfico inter-zona y probar las directivas de acceso desde un navegador web. Los resultados obtenidos demuestran la importancia de una configuración precisa y la necesidad de una monitorización continua para asegurar la eficacia de las reglas de acceso frente a las cambiantes necesidades y amenazas…*

PALABRAS CLAVE: Reglas de acceso, seguridad de red, zonas de red, HTTP, FTP, DMZ.

Abstract: *Proper access rule configuration is essential to ensure the security and functionality of computer networks. This article presents a systematic approach to configuring access rules that allow or deny traffic between different network zones, specifically between the Green Zone and the Orange Zone with HTTP and FTP protocols, and between the Internet Zone and the DMZ. The steps to create specific access rules, verify inter-zone traffic, and test access directives from a web browser are detailed. The results obtained demonstrate the importance of precise configuration and the need for continuous monitoring to ensure the effectiveness of access rules against changing needs and threats.*

Keywords: *Access rules, network security, network zones, HTTP, FTP, DMZ.*

1 INTRODUCCIÓN

La seguridad de las redes de computadores es un aspecto fundamental en la era digital actual, donde la información y los servicios se encuentran cada vez más expuestos a amenazas y vulnerabilidades. La configuración adecuada de reglas de acceso es una de las medidas más efectivas para proteger las redes y garantizar la integridad y confidencialidad de los datos. En este contexto, la segmentación de redes en zonas con diferentes niveles de seguridad es una práctica común para aislar y proteger los activos más críticos.

Sin embargo, la comunicación entre estas zonas de red es necesaria para el funcionamiento adecuado de los servicios y aplicaciones. Por lo tanto, es crucial configurar reglas de acceso que permitan o denieguen tráfico entre las zonas de manera controlada y segura. En este artículo, se aborda el tema de la configuración de reglas de acceso para la comunicación segura entre zonas de red, específicamente entre la Zona Verde y la Zona Naranja con protocolos HTTP y FTP, y entre la Zona Internet y la Zona DMZ.

Se presentará un enfoque sistemático para crear reglas de acceso específicas, verificar el tráfico inter-zona y probar las directivas de acceso desde un navegador web. El objetivo es proporcionar una guía práctica para los administradores de redes y los profesionales de la seguridad para configurar reglas de acceso efectivas y seguras en entornos de red complejos.

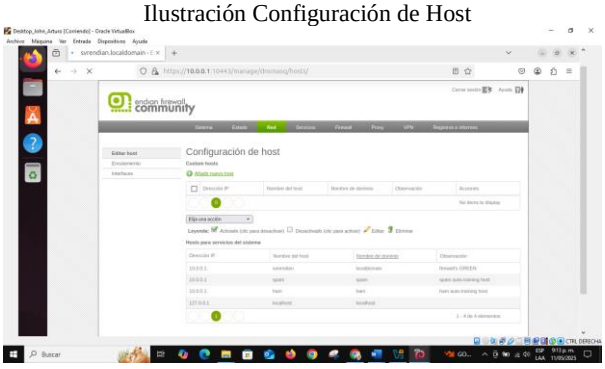
Estructura del artículo

El artículo se estructura de la siguiente manera:
Se presenta el enfoque sistemático para configurar reglas de acceso para la comunicación segura entre zonas de red.
Se detallan los pasos para crear reglas de acceso específicas para los protocolos HTTP y FTP entre la Zona Verde y la Zona Naranja, y entre la Zona Internet y la Zona DMZ.
Se describe la verificación del tráfico inter-zona y la prueba de las directivas de acceso desde un navegador web.
Se presentan los resultados y conclusiones obtenidos, destacando la importancia de una configuración precisa y la necesidad de una monitorización continua para asegurar la eficacia de las reglas de acceso.

2.Temática 4: Reglas de acceso para permitir o denegar el tráfico.

2.1 Paso 1: Configurar las interfaces de red

Ilustración Configuración de Host



Fuente: Autoría Propia

Ingresa al panel de administración de Endian y navega a Red > Interfaces.

Configura las interfaces de red para cada zona:

Zona Verde (LAN): IP 10.0.0.1, máscara 255.255.255.0.

Zona Naranja (DMZ): IP 172.16.0.1, máscara 255.255.255.240.

Zona Roja (WAN): Configura la interfaz para acceso a Internet.

2.2 Paso 2: Crear reglas de firewall

Crea una nueva regla para permitir la comunicación entre la zona Verde y la zona Naranja:

Nombre de la regla: Verde a Naranja HTTP y FTP.

Protocolo: TCP.

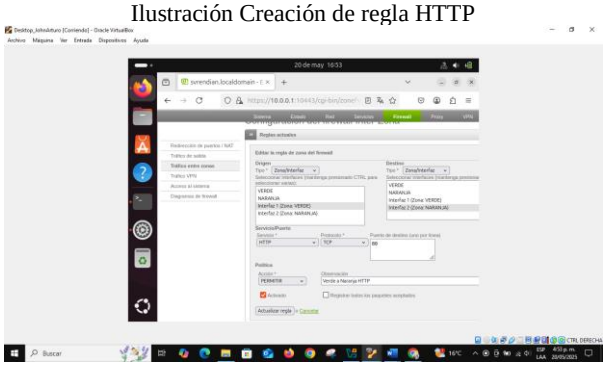
Puertos: 80 (HTTP) y 21 (FTP).

Origen: Zona Verde (LAN).

Destino: Zona Naranja (DMZ).

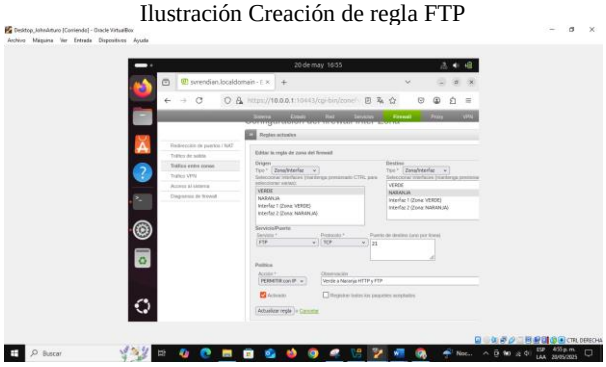
Acción: Permitir.

Ilustración Creación de regla HTTP



Fuente: Autoría Propia

Ilustración Creación de regla FTP



Fuente: Autoría Propia

Crea otra regla para permitir la comunicación entre la zona Internet y la zona DMZ:

Nombre de la regla: Internet a DMZ.

Protocolo: TCP.

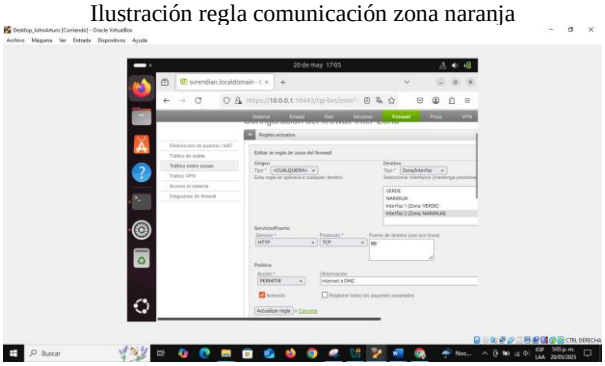
Puertos: 80 (HTTP).

Origen: Zona Roja (WAN).

Destino: Zona Naranja (DMZ).

Acción: Permitir.

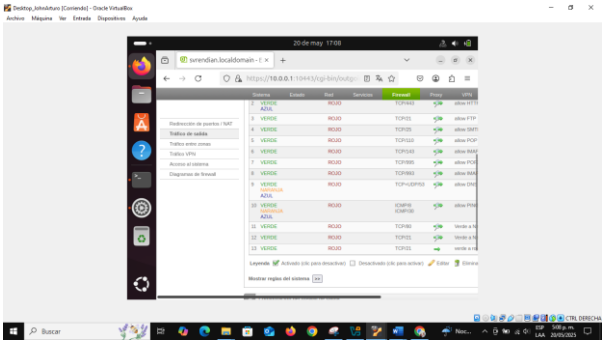
Ilustración regla comunicación zona naranja



2.3 Paso 3: Verificar el tráfico Inter-Zona

Navega a Seguridad > Firewall > Registros.

Ilustración tráfico de salida



Fuente: Autoría Propia

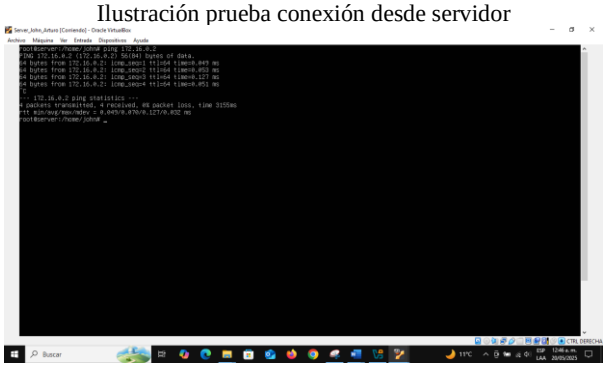
Una vez creadas las reglas de firewall en Endian, es fundamental aplicarlas correctamente para que surtan efecto en la red. Después de definir las reglas para permitir o denegar el tráfico entre las zonas (Verde, Naranja, DMZ y WAN) para los servicios HTTP y FTP, se deben guardar y aplicar los cambios en la configuración del firewall. Esto asegura que las reglas se activen y comiencen a controlar el tráfico según lo especificado. Con las reglas aplicadas, el firewall estará en capacidad de gestionar adecuadamente las conexiones entre las diferentes zonas de la red. Ahora, el siguiente paso es verificar el tráfico inter-zonas para confirmar que las reglas funcionan según lo esperado.

Verifica que las reglas estén funcionando correctamente y que se permita el tráfico entre las zonas según sea necesario.

Ilustración ping desde Desktop

Fuente: Autoría Propia

Ilustración prueba conexión desde servidor



Fuente: Autoría Propia

2.4 Paso 4: Probar las directivas

Desde un navegador web en la zona Verde (LAN), intenta acceder a un servidor web en la zona Naranja (DMZ) utilizando la dirección IP 172.16.0.1.

Ilustración ping 172.16.0.1

Fuente: Autoría Propia

Protocolo ftp, se realiza la verificación de conectividad utilizando el comando ping en un desktop

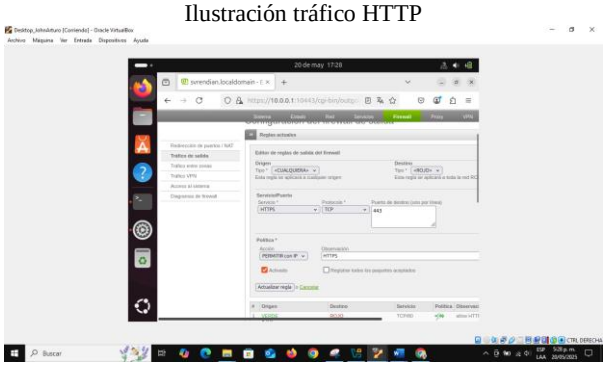
Ilustración ping FTP

Fuente: Autoría Propia

Ping desde la maquina en la LAN hacia la DMZ, puede comunicarse con el servidor en la DMZ y que el tráfico ICMP está permitido entre las dos zonas.

Regla firewall de salida, permitirá el tráfico HTTP desde la zona LAN hacia Internet.

Ilustración tráfico HTTP



Fuente: Autoría Propia

3. CONCLUSIONES

3.1 Temática 4: Reglas de acceso para permitir o denegar el tráfico.

La implementación de Endian Firewall ha permitido establecer una comunicación efectiva entre diferentes zonas de red, específicamente entre la zona Verde y la zona Naranja, utilizando los protocolos HTTP y FTP con sus respectivos puertos. Esta capacidad resalta la efectividad de Endian para controlar y gestionar el tráfico entre las distintas áreas de la red.

Además, se configuró exitosamente el acceso desde la zona de Internet a la zona DMZ, garantizando que los usuarios externos puedan acceder de manera segura a los servicios ofrecidos en esta área. La verificación del tráfico inter-zona ha demostrado que las reglas de seguridad están funcionando adecuadamente, permitiendo únicamente el tráfico autorizado, lo que refuerza la integridad de las políticas de seguridad implementadas.

4. REFERENCIAS

[1] Endian Team. (s.f.). *Endian Firewall Community (Versión 3.3.2) [Software de código abierto]*. SourceForge. https://sourceforge.net/projects/efw/

[2] *Outbound NAT | PFSense Documentation*. (s. f.). https://docs.netgate.com/pfsense/en/latest/nat/outbound.html

[3] *Port forwarding / NAT — Endian UTM 3.2 Reference Manual*. (s. f.). https://docs.endian.com/3.2/utm/firewall/dnat.html

[4] Endian UTM 3.0 Reference Manual. (s.f.). The Firewall Menu. Recuperado de https://docs.endian.com/3.0/en/utmfw.html

[5] Configuración de reglas de firewall. (s.f.). En Endian UTM 3.0 Reference Manual. Recuperado de https://docs.endian.com/3.0/en/utmfw-configure-rules.html

[6] Inter-Zone Traffic. (s.f.). En Endian UTM 3.0 Reference Manual. Recuperado de https://docs.endian.com/3.0/en/utmfw-interzone-traffic.html

[7] Port Forwarding / NAT. (s.f.). En Endian UTM 3.0 Reference Manual. Recuperado de https://docs.endian.com/3.0/en/utmfw-port-forwarding-nat.html

[8] Configuración de reglas de seguridad. (s.f.). En Endian UTM 3.0 Reference Manual. Recuperado de https://docs.endian.com/3.0/en/utmfw-security-rules.html

[9] Application Firewall. (s.f.). En Endian UTM 3.0 Reference Manual. Recuperado de https://docs.endian.com/3.0/en/utmfw-application-firewall.html

[10] nDPI. (s.f.). En Endian UTM 3.0 Reference Manual. Recuperado de https://docs.endian.com/3.0/en/utmfw-ndpi.html

[11] Endian UTM Appliance. (s.f.). En Endian UTM 3.0 Reference Manual. Recuperado de https://docs.endian.com/3.0/en/utmfw-appliance.html

[12] Guía de configuración de Endian UTM. (2022). Recuperado de https://www.endian.com/wp-content/uploads/2022/07/Endian-UTM-Configuration-Guide.pdf

[13] Manual de usuario de Endian UTM. (2022). Recuperado de https://www.endian.com/wp-content/uploads/2022/07/Endian-UTM-User-Manual.pdf

[14] Reglas de firewall en Endian UTM. (2020). Recuperado de https://www.it-connect.fr/configurer-les-regles-de-firewall-sur-endian-utm/

[15] Configuración de reglas de red en Endian UTM. (2019). Recuperado de https://www.admin-en-ligne.fr/configurer-les-regles-reseau-sur-endian-utm/