CONTROL DEL TRÁFICO HTTP Y FTP ENTRE LAN, DMZ Y WAN MEDIANTE REGLAS INTERZONA EN ENDIAN UTM

Johan Manuel Santana Cortes
johanmanuelsantana318@gmail.com

RESUMEN: La actividad que se desarrolla consiste en el ajuste y control de las reglas de acceso en la plataforma Endian Firewall (EFW) para poder gestionar el tráfico entre las diferentes zonas de red: Verde (LAN), Naranja (DMZ) y Roja (WAN/Internet). Se aplican reglas específicas de administración para aquellos protocolos HTTP y FTP, permitiendo la comunicación controlada entre la LAN y la DMZ y entre la DMZ (la parte desmilitarizada de la red) y la WAN ; la configuración se hace desde la web de Endian, a la cual se le han asignado correctamente las IPs y puertas de enlace de cada zona , además s de verificar la conectividad que al igual que se ha fundamentado mediante pruebas de ping, telnet y acceso a los servicios de web y FTP , Los resultados muestran que las reglas aplicadas aseguran que solamente se permitirá á el tráfico autorizado entre zonas y que el tráfico no definido se bloqueará. Esta actividad permite gestionar de forma práctica la gestión de la política de seguridad perimetral, además de la importancia que tiene segmentar la red para proteger aquellos recursos críticos en una organización.

PALABRAS CLAVE: Endian Firewall, FTP, WAN y HTTP.

1. INTRODUCCIÓN

En los entornos organizacionales actuales, la protección del perímetro de red se ha convertido en un componente esencial para garantizar la integridad, disponibilidad y confidencialidad de la información. La creciente exposición de servicios internos hacia la red pública y la necesidad de segmentar correctamente los dominios de seguridad hacen indispensable la implementación de arquitecturas robustas basadas en zonas diferenciadas como la LAN, la DMZ y la WAN. En este contexto, la presente actividad se orienta a la configuración y gestión de reglas de acceso utilizando la plataforma Endian Firewall (EFW), una solución UTM de código abierto diseñada para controlar, filtrar y asegurar el tráfico entre diferentes segmentos de red.

El propósito principal es comprender y aplicar políticas de acceso que permitan delimitar el comportamiento del tráfico entre zonas, implementando reglas específicas para los protocolos HTTP y FTP. Estas configuraciones permitirán habilitar de manera controlada la comunicación entre la zona Verde (usuarios internos), la zona Naranja (DMZ donde residen servicios web y bases de datos) y la zona Red (WAN o Internet). De esta manera, se busca reforzar las buenas prácticas en seguridad perimetral, garantizando que solo el tráfico autorizado circule entre segmentos críticos, a la vez que se simulan escenarios reales de operación y verificación de servicios bajo plataformas GNU/Linux.

2 DESCARGA, INSTALACIÓN Y CONFIGURACIÓN DE ENDIAN UTM, SERVIDOR UBUNTU Y CLIENTE LINUX MINT

2.1 CARACTERÍSTICAS GENERALES

El desarrollo de este laboratorio tiene como objetivo implementar una arquitectura de red segmentada, utilizando un firewall UTM con el fin de simular un entorno seguro de tipo empresarial. La segmentación se realiza mediante la creación de tres zonas de seguridad: VERDE (LAN), NARANJA (DMZ) y ROJA (Internet), lo cual permite aplicar políticas de control de acceso y aislamiento de servicios de forma efectiva. Este tipo de arquitectura es ampliamente recomendado en la administración de infraestructuras de red seguras [5].

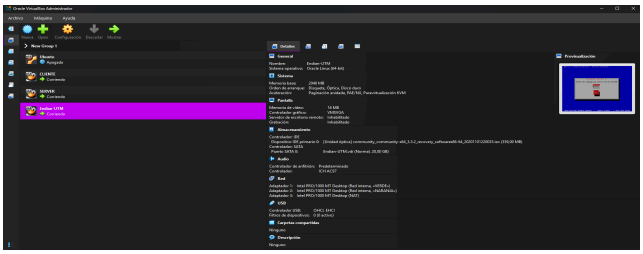
El entorno fue virtualizado mediante el uso de VirtualBox, lo cual permite simular escenarios reales de red de forma segura y controlada, sin afectar sistemas productivos reales [4].

2.2 DESCARGA E INSTALACIÓN DE ENDIAN

Se descargó la Figura ISO oficial de Endian UTM desde el repositorio del fabricante. Posteriormente, se creó una máquina virtual en VirtualBox, asignando recursos de hardware como memoria RAM, almacenamiento y CPU de acuerdo con los requerimientos del sistema. Durante el proceso de instalación se configuraron parámetros básicos como idioma, distribución del teclado, zona horaria y particionamiento automático del disco.

La correcta asignación de recursos de hardware y la configuración inicial del sistema son fundamentales para el rendimiento del firewall, de acuerdo con las buenas prácticas descritas en la documentación técnica de Linux [1] y en el manual oficial de Endian [5].

Figura 1. Descarga de Endian



Fuente: Autoría Propia

PASO 2. CONFIGURACIÓN DE LA RED DE ENDIAN

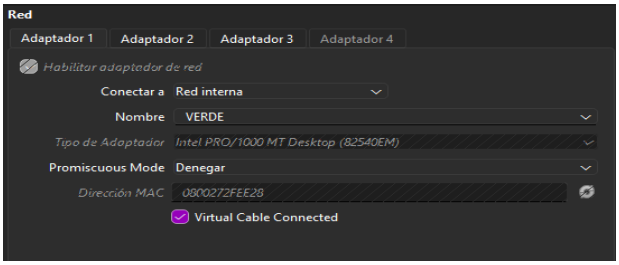
Se configuraron tres interfaces de red dentro de la máquina virtual de Endian, cada una asociada a una zona de seguridad distinta:

Tabla 2

Adaptador		Conectar a	Nombre	Dirección MAC
Adaptador 1	eth0	Red Interna	VERDE	0800272FEE28
Adaptador 2	eth1	Red Interna	NARANJA	080027CDBDF7
Adaptador 3	eth2	NAT	ROJO	080027B6C710

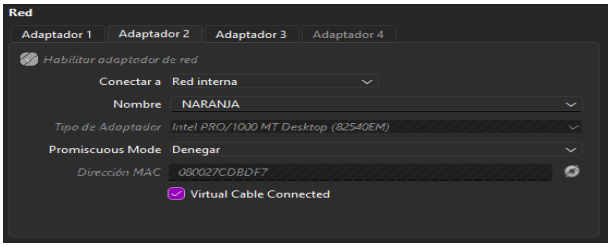
Esta separación de interfaces permite implementar políticas de seguridad diferenciadas y respalda el concepto de segmentación de red recomendado en los manuales de administración de sistemas Linux [3] y en la documentación oficial de Endian [5].:

Figura 2. Adaptador 1 — VERDE (LAN)



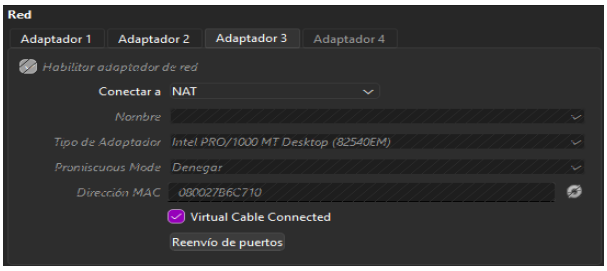
Fuente: Autoría Propia

Figura 3. Adaptador 1 — NARANJA (LAN)



Fuente: Autoría Propia

Figura 4. Adaptador 3 — NAT



Fuente: Autoría Propia

Para la configuración de la zona Verde, se usa el adaptador 1, como red interna. Para la zona Naranja se utiliza el adaptador 2 como red interna. Mientras que para el Adaptador 3, se usa como Red NAT.

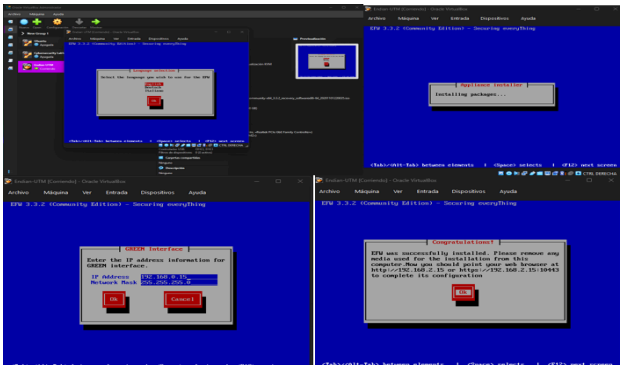
Esta configuración permite aislar los segmentos de red y controlar el tráfico entre ellos mediante reglas de firewall, tal como lo recomienda la literatura sobre redes seguras.

3. PROCESO DE INSTALACIÓN DE ENDIAN

Durante este paso se ejecutó el asistente de instalación de Endian, donde se configuró el nombre del equipo (hostname), las direcciones IP estáticas para cada interfaz y la contraseña del usuario administrador. Adicionalmente, se habilitó el acceso a la interfaz web de administración a través del protocolo HTTPS.

La administración remota a través de interfaces seguras es una práctica recomendada en la documentación oficial de Endian UTM [5].

Figura 5. Proceso de instalación de Endian



Fuente: Autoría Propia

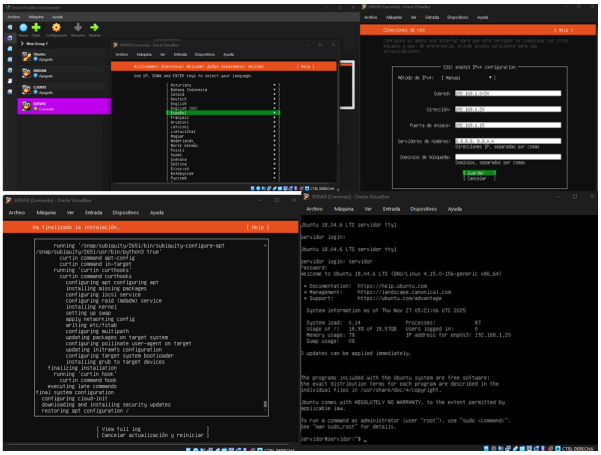
Se completó la instalación iniciando el asistente, configurando el hostname, la contraseña del usuario

administrador y la dirección IP de cada interfaz. El sistema quedó accesible mediante su interfaz web segura por HTTPS.

2.3 PROCESO DE DESCARGA E INSTALACIÓN DEL SERVIDOR

Se descargó la Figura ISO Ubuntu 15.04.6 Live Server y se creó una máquina virtual dedicada al servidor, ubicada en la zona NARANJA (DMZ). Durante la instalación se configuraron los parámetros regionales, los usuarios del sistema y la estructura de particiones.

Figura 6. Instalación de “Ubuntu 15.4.-live Server”



Fuente: Autoría Propia

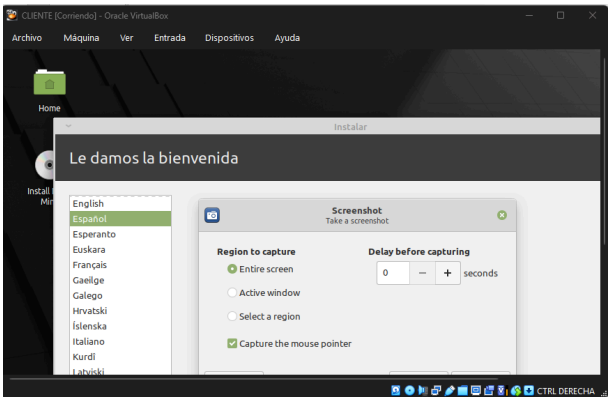
Posteriormente, se asignó una dirección IP estática para garantizar la estabilidad de la comunicación con el firewall. Las configuraciones de red y administración básica del sistema se realizaron siguiendo las recomendaciones oficiales de Canonical [2].

2.4 PROCESO DE DESCARGA E INSTALACIÓN DEL CLIENTE

Se descargó la Figura ISO de Linux Mint 20.2 de 64 bits y se creó una máquina virtual que fue configurada dentro de la zona VERDE. Durante el proceso de instalación se configuraron los usuarios, el entorno gráfico y las opciones regionales del sistema.

La configuración de red del cliente fue realizada asignando una IP estática para asegurar la correcta comunicación con Endian y con el servidor de la DMZ, siguiendo las buenas prácticas de administración de sistemas tipo Debian [3].

Figura 7. Instalación de Linux Mint



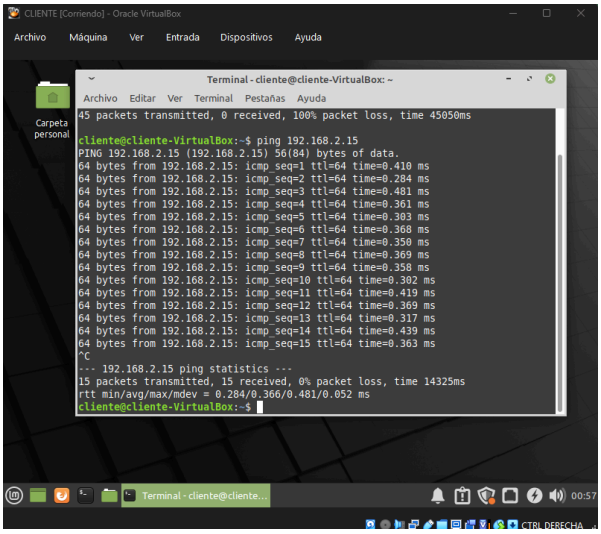
Fuente: Autoría Propia

2.5 PRUEBA DE CONECTIVIDAD CON EL SERVIDOR 192.168.2.15

Una vez configurados todos los equipos, se realizaron pruebas de conectividad utilizando comandos de red básicos como: ping 192.168.2.15

La recepción de respuestas exitosas confirmó la correcta configuración de las interfaces de red. Estas pruebas son fundamentales en los procesos de diagnóstico de redes en sistemas Linux [1].

Figura 8. Prueba de Conectividad con el Servidor 192.168.2.15



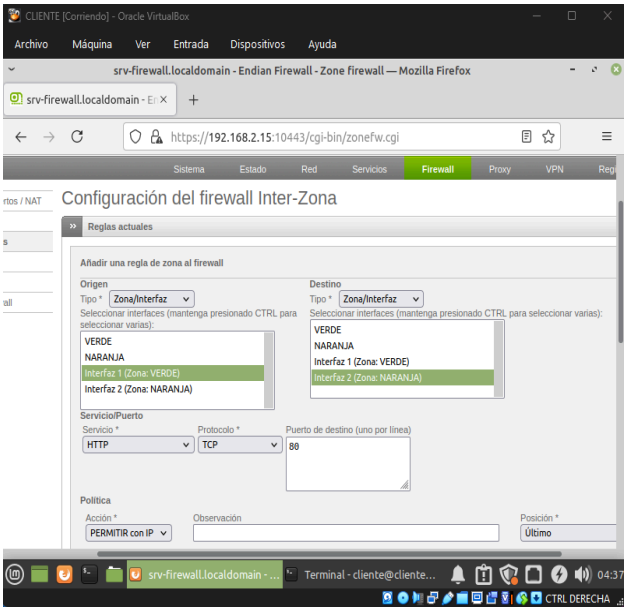
Fuente: Autoría Propia

3. COMUNICAR LA ZONA VERDE CON LA ZONA NARANJA CON EL PROTOCOLO HTTP Y FTP CON SUS RESPECTIVOS PUERTOS.

3.1 ACCEDER A LA INTERFAZ WEB DE ENDIAN

Desde el Cliente VERDE se accedió a la interfaz de administración de Endian mediante HTTPS, permitiendo la gestión centralizada de las reglas de seguridad. Esta funcionalidad está documentada en el manual oficial de Endian[5].

Figura 9. Instalación de Linux Mint



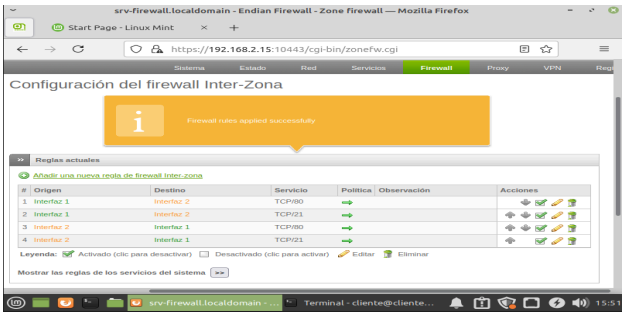
Fuente: Autoría Propia

3.2 CREAR REGLA DE FIREWALL: VERDE → NARANJA

Se configuraron reglas de firewall para permitir exclusivamente tráfico HTTP (puerto 80) y FTP (puerto 21) desde la zona VERDE hacia la zona NARANJA. Este tipo de control de tráfico se basa en los principios de administración segura de sistemas descritos en documentación técnica de Linux [3] y Endian [5].

1. Se va al menú Firewall → Tráfico entre Zonas
2. Selecciona la zona de origen: VERDE
3. Selecciona la zona de destino: NARANJA
4. Configura la regla
5. Se guarda la regla y aplica cambios.

Figura 10. Regla de firewall creada



Fuente: Autoría Propia

3.3 VERIFICAR CONECTIVIDAD HTTP Y FTP

Desde el Cliente VERDE se ejecutaron los siguientes comandos: curl http://192.168.1.20; ftp 192.168.1.20

Estas pruebas confirmaron la correcta aplicación de las reglas configuradas y la funcionalidad de los servicios habilitados. El uso de herramientas de diagnóstico de red está documentado en la formación LPI [1].

4. COMUNICAR LA ZONA INTERNET CON LA ZONA DMZ

Permitir que la zona ROJA / Internet se comunique con la zona NARANJA / DMZ. Esto normalmente se hace para servicios públicos alojados en la DMZ, como HTTP o FTP. Importante: solo abrir los puertos necesarios para seguridad.

4.1 CREAR REGLA DE FIREWALL: ROJA → NARANJA

Se configuró una regla de firewall con: Zona origen: ROJA; Zona destino: NARANJA y Servicios: HTTP (80) y FTP (21)

Figura 11. Regla de firewall creada

Fuente: Autoría Propia

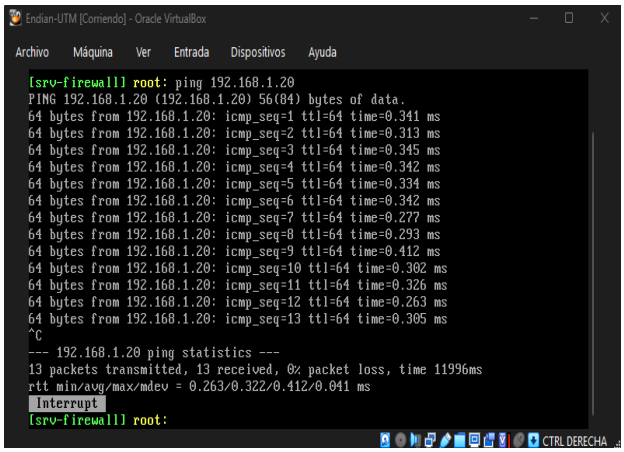
4.2 VERIFICAR CONECTIVIDAD DESDE INTERNET (ROJA)

Se realizaron pruebas utilizando:

ping 192.168.1.20
telnet 192.168.1.20 80
telnet 192.168.1.20 21

Las conexiones exitosas confirmaron la correcta exposición de los servicios, conforme a la documentación de Endian [5].

Figura 12. ping 192.168.1.20 # Servidor DMZ



Fuente: Autoría Propia

telnet 192.168.1.20 80 # HTTP
telnet 192.168.1.20 21 # FTP

Si telnet conecta, la regla está funcionando, si ping falla, es normal: ICMP puede estar bloqueado por defecto.

Resultado: ROJA puede acceder a HTTP y FTP del Servidor DMZ; ROJA no puede ver otras máquinas internas (VERDE) si no hay reglas adicionales; Ping ICMP puede estar bloqueado hasta que agregues una regla ICMP opcional.

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

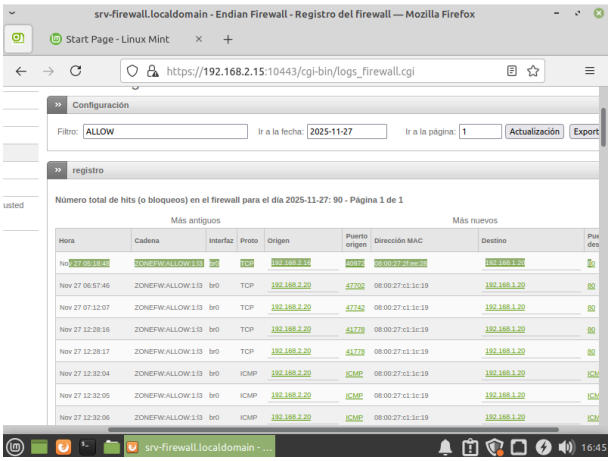
Objetivo: Comprobar que las reglas VERDE ↔ NARANJA y ROJA ↔ NARANJA están aplicadas correctamente.

Revisar que el tráfico permitido pase y el no permitido sea bloqueado.

5.1 HERRAMIENTAS DE VERIFICACIÓN EN ENDIAN

Endian tiene varias formas de monitorear el tráfico: Firewall Logs (Registros): Se ingresa por Registros e Informes → Firewall. Se Filtra por source zone / destination zone y puerto (HTTP=80, FTP=21), fecha etc. Se Verifica que los paquetes permitidos aparecen como ACCEPT.

Figura 13. Logs de Firewall

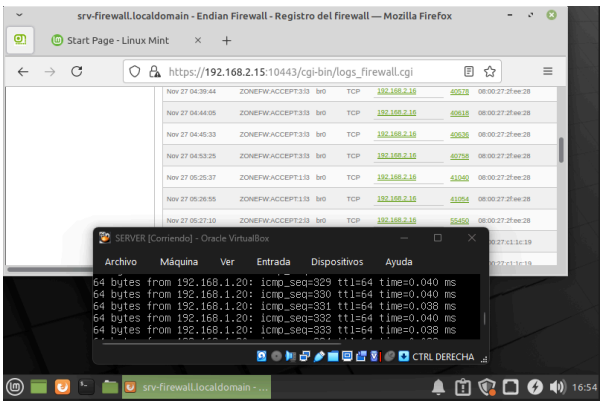


Fuente: Autoría Propia

Menú: Firewall → Connection Table. Observa conexiones activas entre Cliente, Servidor y ROJA. Esto muestra tráfico actual y puertos abiertos.

Ping / Telnet desde las VMs
Desde Cliente VERDE:
ping 192.168.1.20 # Servidor DMZ (ICMP)
telnet 192.168.1.20 80 # HTTP
telnet 192.168.1.20 21 # FTP

Figura 14. Logs de Firewall



Fuente: Autoría Propia

Nota: Ping ICMP puede estar bloqueado por defecto si no hay regla ICMP.

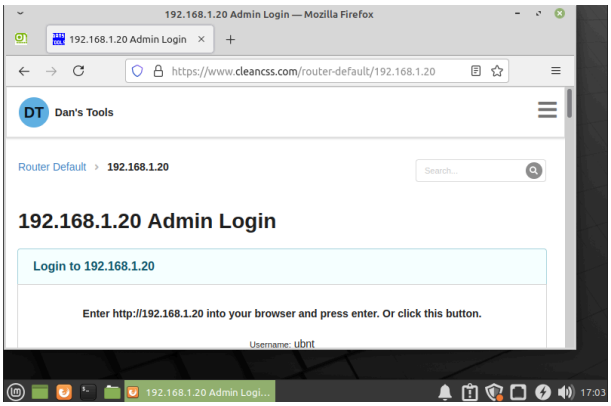
6 PROBAR DESDE UN NAVEGADOR WEB, LAS SIGUIENTES DIRECTIVAS

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

Objetivo: Comprobar que los servicios HTTP configurados en DMZ y WAN sean accesibles desde la LAN (Cliente VERDE). Validar que Endian está aplicando correctamente las reglas.

Ingreso HTTP desde la LAN → DMZ: Desde el Cliente VERDE, abre un navegador web (Chrome, Firefox, etc). Se ingresa la IP del Servidor DMZ (NARANJA) con HTTP: http://192.168.1.20

Figura 15. Ingreso HTTP desde la LAN → DMZ



Fuente: Autoría Propia

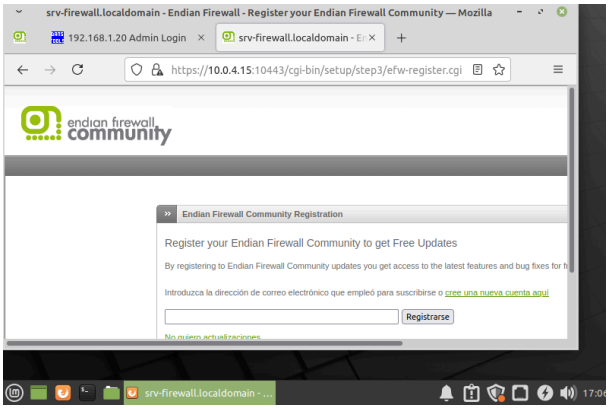
Página web servida por el Servidor NARANJA. Si funciona, significa que la regla VERDE → NARANJA para HTTP está activa y correcta.

Nota: Si el Servidor no tiene un servidor web activo, puedes instalar uno rápido:

Ingreso HTTP desde la LAN → WAN
Pasos:

1. Desde el Cliente VERDE, abre el navegador.
2. Ingresa cualquier dirección pública (o desde Endian, la IP de ROJA): http://10.0.4.15

Figura 16. Ingreso HTTP desde la LAN → WAN



Fuente: Autoría Propia

Ejemplo de prueba dentro de red: si Endian ROJA tiene acceso a Internet, intenta: http://www.google.com

Resultado: La página web se carga correctamente. Esto confirma que VERDE → WAN (ROJA) → Internet funciona vía Endian. Esto también permite ver si algún proxy de Endian está interfiriendo.

7. CONCLUSIONES

El desarrollo de la actividad fue capaz de aclarar de forma práctica los conceptos que rigen el control de tráfico interzona, a partir de llevar a cabo la configuración de la solución de seguridad Endian Firewall. Ha sido capaz de establecer reglas que permiten la comunicación e intercambio de los servicios HTTP y FTP entre la LAN, la DMZ y la WAN, pudiendo dejar que el tráfico interzonal ú nicamente pase si es el correcto. Las pruebas realizadas de Cliente y Servidor desde la zona de Internet han demostrado que las políticas de acceso funcionan correctamente, es decir, han demostrado que la seguridad perimetral se ha definido adecuadamente.

Además , se reitera la importancia de la correcta asignación de IPs y gateways , así como la realización de pruebas de conectividad antes de implementar la

política para simular lo más pronto un escenario real en producción . Contribuye a entender la segmentación de las redes y la administración de las políticas UTM, ya que se han visto cómo la configuración de las reglas interzona permite proteger los recursos críticos de la organización, garantizar la disponibilidad de los servicios y gestionar

8. REFERENCIAS

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

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

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

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

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