ENDIAN FIREWALL COMO SOLUCION DE SEGURIDAD EN REDES EN UN ENTORNO VIRTUALIZADO

Edison Adrian Hoyos Pantoja
e-mail: eahoyosp@unadvirtual.edu.co
Cristian Andres Hoyos Pantoja
e-mail: cahoyospa@unadvirtual.edu.co
Jesus Alberto Montealegre Aquite
e-mail: jamontealegrea@unadvirtual.edu.co
Cristian Rafael Gomez Aguirre
e-mail: crgomezag@unadvirtual.edu.co

RESUMEN: *El presente artículo presenta el proceso de instalación, configuración y prueba de Endian Firewall Community como solución de seguridad para la protección de redes virtualizadas, usando VirtualBox se realizó un entorno simulado donde se definieron zonas de red específica para representar distintos niveles de seguridad, se configuraron reglas NAT, servicios como HTTP y FTP, así como un proxy no transparente con filtrado de contenido y autenticación, al final obtuvimos un correcto aislamiento y control del tráfico entre segmentos de red, evidenciando la capacidad de Endian para gestionar eficazmente el acceso y la protección de los recursos de la red.*

PALABRAS CLAVE: Endian, firewall, zona verde, zona naranja, máquina virtual, dirección IP.

ABSTRACT: *This article presents the installation, configuration and testing process of Endian Firewall Community as a security solution for the protection of virtualized networks, using VirtualBox a simulated environment was created where specific network zones were defined to represent different security levels, NAT rules were configured, services such as HTTP and FTP, as well as a non-transparent proxy with content filtering and authentication, in the end we obtained correct isolation and control of traffic between network segments, demonstrating Endian's ability to effectively manage access and protection of network resources.*

KEYWORDS: Endian, firewall, green zone, orange zone, virtual machine, IP address.

1 INTRODUCCIÓN

Actualmente la seguridad es un componente esencial en todo sistema informático, esta garantiza la integridad, confidencialidad y disponibilidad de los servicios dentro de una red, es por ello que las organizaciones tantos públicas como privadas requieren de soluciones que permitan proteger la infraestructura tecnológica frente amenazas internas y externas, es ahí donde los firewalls como Endian Firewall Community desempeñan un papel fundamental en la defensa de sistemas informáticos, al ofrecer una solución robusta en la gestión unificada de amenazas UTM.

El presente artículo describe el proceso de instalación, configuración y administración de Endian Firewall en un entorno virtualizado mediante VirtualBox, se abordarán aspectos desde la definición de zonas de red, configuración de adaptadores, asignación de direcciones IP, así como la definición de reglas NAT y políticas de filtros, se pretende simular un entorno de red seguro que permita el control granular del tráfico entre segmentos y la validación de servicios como HTTP, FTP, y proxy transparentes.

2 ENDIAN COMO FIREWALL

2.1 QUE ES ENDIAN

Endian Firewall Community es una distribución GNU/Linux especializada en seguridad de redes, que permite convertir un equipo estándar en un dispositivo de seguridad con gestión unificada de amenazas UTM [1].

Su principal característica es el firewall bidireccional incluido que permite controlar todo el tráfico de entrada y salida, así mismo Endian provee otras características como VPN, proxy transparente, filtro de contenido, gestión de múltiples zonas de red, entre otras.

2.2 REQUISITOS MINIMOS

Antes de iniciar la instalación el equipo o PC deberá cumplir con los siguientes requisitos del sistema:

CPU: compatible con Intel x86 (mínimo 500 MHz, recomendado 1 GHz)

RAM: 256 MB mínimo (512 MB recomendados)

Disco: Se requiere disco SCSI, SATA, SAS o IDE (mínimo 4 GB)

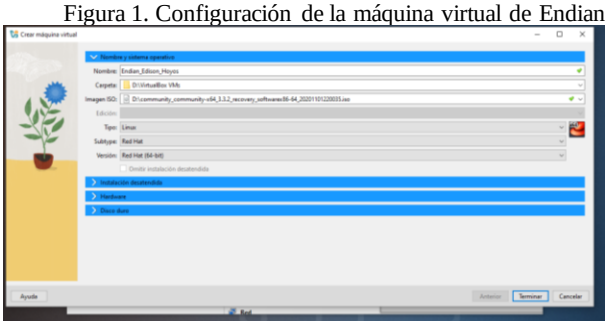
CD-ROM: Se requiere unidad de CDROM IDE, SCSI o USB para la instalación

Tarjetas de red: Se requieren al menos dos tarjetas Ethernet, una para la WAN/Internet y otra para la LAN[1].

2.3 INSTALACIÓN

El proceso de instalación de Endian comienza desde la descarga en el sitio oficial de Endian https://www.endian.com/en/community/, en este repositorio se descarga la herramienta en su forma ISO, posteriormente la ISO se carga en VirtualBox donde se ejecuta como una máquina virtual basada y configurada como RHEL, para poder instalar Endian y hacer su respectivo uso se configuró una máquina virtual: Fig. 1.

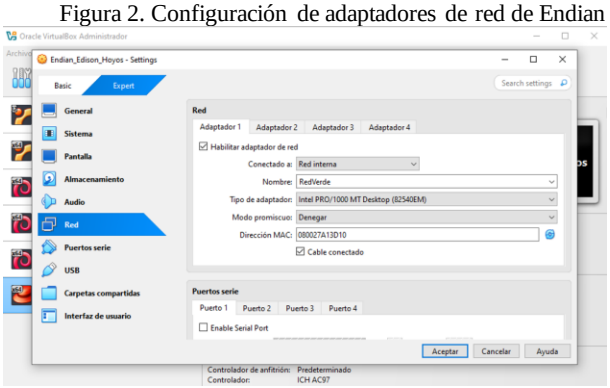
Figura 1. Configuración de la máquina virtual de Endian



Fuente. Autoría Propia

Después de configurar los aspectos necesarios de la máquina virtual se configuran los adaptadores de red, esto con el fin de definir que adaptadores debe tener y trabajar la red configurada desde Endian: Fig. 2, los adaptadores con los que debe contar la máquina virtual son tres, dos adaptadores configurados como red interna, uno para la zona verde y otro para la zona naranja, así como un adaptador configurado como NAT que permite establecer comunicación a través de internet u otra red WAN, los nombres de la red interna fueron definidos como RedVerde y RedNaranja, por ende estos mismos nombres se deben asignar a los adaptadores de red de las máquinas que estarán en la zona verde y naranja respectivamente.

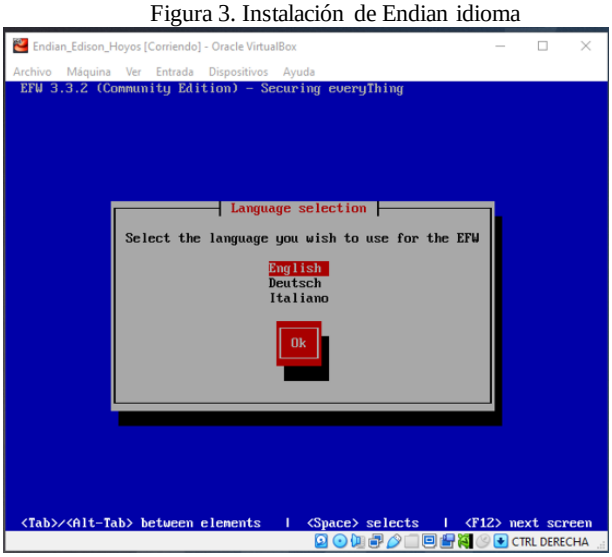
Figura 2. Configuración de adaptadores de red de Endian



Fuente. Autoría Propia

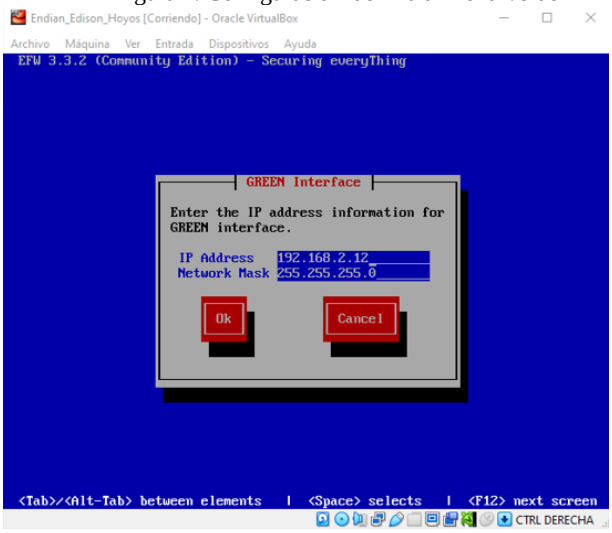
Con la configuración de la máquina virtual, se continúa a iniciar la instalación de Endian, al iniciar el sistema: Fig. 3, se solicita establecer un idioma, luego que se selecciona el idioma deseado, Endian solicita establecer una dirección IP que actuara como puerta predeterminada de la zona verde: Fig. 4, para esto se toma en cuenta lo especificado para las zonas de red de Endian: Fig. 5, establecida la dirección IP, Endian termina de instalarse, de forma que ya se encuentra listo para ser configurado desde su interfaz web.

Figura 3. Instalación de Endian idioma



Fuente. Autoría Propia

Figura 4. Configuración de Endian zona verde



Fuente. Autoría Propia

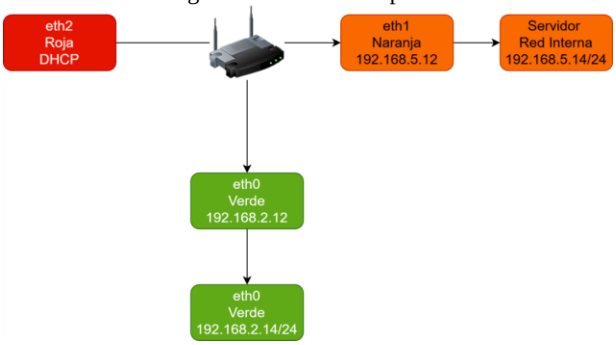
3 TEMATICA 1: CONFIGURACION DE INSTANCIAS DE ENDIAN

Cabe aclarar que todas las máquinas mencionadas en el presente artículo se ejecutaron mediante el software de virtualización VirtualBox, este no aborda la instalación de otras máquinas virtuales, sin embargo, se usaron dos máquinas virtuales adicionales para la simulación de la red una desktop que estará en el segmento de la zona verde, y otra máquina server que estará en el segmento de la zona naranja.

Antes de configurar las instancias se establecen las tres zonas de red, la zona roja destinada para la conexión WAN, la zona verde destinada para la red LAN y la zona naranja destinada para la zona DMZ, cada zona fue asignada a un adaptador de red específico, de esta forma se permite aislar

diferentes segmentos de red con distintos niveles de seguridad: Fig. 5.

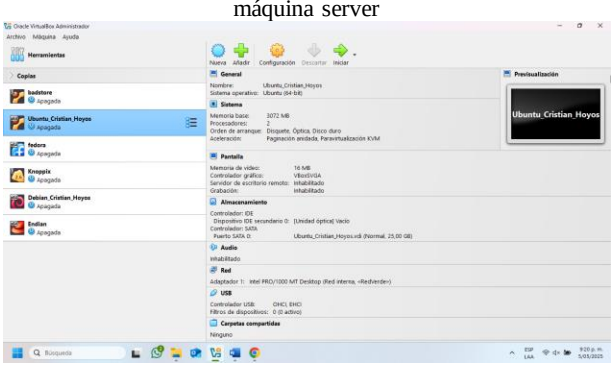
Figura 5. Zonas de red para Endian



Fuente. Autoría propia

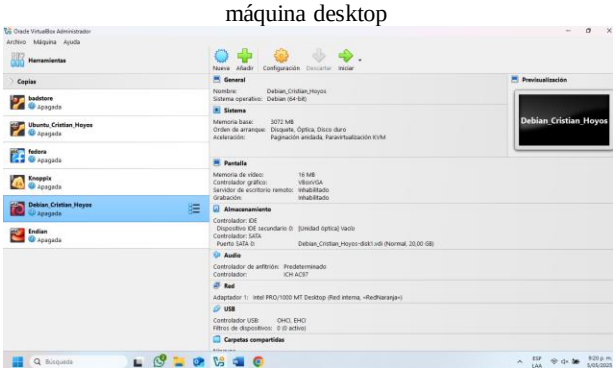
Definidos los segmentos de red para las zonas, se procedió a cambiar la configuración de los adaptadores de red de la máquina desktop y de la máquina server, desde la interfaz de VirtualBox, a adaptadores de red interna: Fig. 6 y 7, al cambiar los adaptadores a red interna se especifica también al tipo de red interna al que se destinaran estos.

Figura 6. Configuración de adaptadores de red para máquina server



Fuente. Autoría propia

Figura 7. Configuración de adaptadores de red para máquina desktop



Fuente. Autoría propia

Para este proceso es importante que los nombres de los adaptadores de red internas coincidan tanto en las máquinas desktop y server como en la máquina Endian.

Completada la configuración de los adaptadores de red se continúa cambiando las direcciones IPs de las máquinas desktop y server para que estén acordes en los segmentos de red que se han destinado para las zonas correspondientes.

Según la figura 5 la máquina server debe tener asignada la dirección IP 192.168.5.14/24, para determinar cuál es la IP actual se ejecuta el comando ip address el cual muestra que la IP es 169.254.5.68/24: Fig. 8, para realizar el cambio de la dirección IP actual de la máquina a la dirección IP de la zona naranja, se edita el archivo de configuración /etc/network/interfaces agregando al final las siguientes líneas:

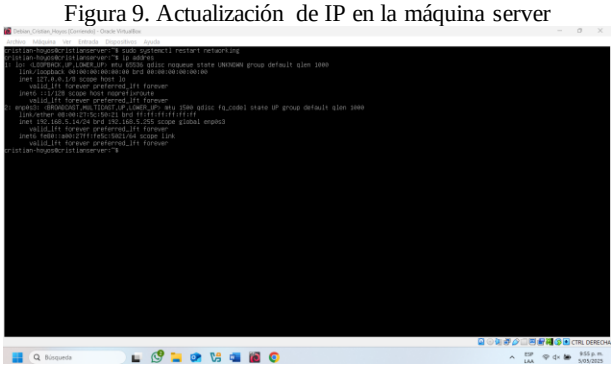
```
iface enp0s3 inet static
address 192.168.5.14
netmask 255.255.255.0
gateway 192.168.5.12
dns-nameservers 8.8.8.8 8.8.4.4
```

Figura 8. IP de la máquina Endian

Fuente. Autoría propia.

Es importante que al establecer el Gateway o la puerta de enlace predeterminada esta esté apuntando hacia la máquina Endian por el adaptador de la zona naranja la cual se definió como 192.168.5.12, de lo contrario la máquina server no podrá tener conexión, seguidamente de haber guardado el archivo /etc/network/interfaces se debe reiniciar el servicio de red para ello un usuario con privilegios de administrador puede ejecutar el comando sudo systemctl restart networking, luego de que el servicio se reinicie nuevamente se consulta la dirección IP con el comando ip address y ahora deberá mostrar la dirección IP que hemos asignado: Fig. 9.

Figura 9. Actualización de IP en la máquina server

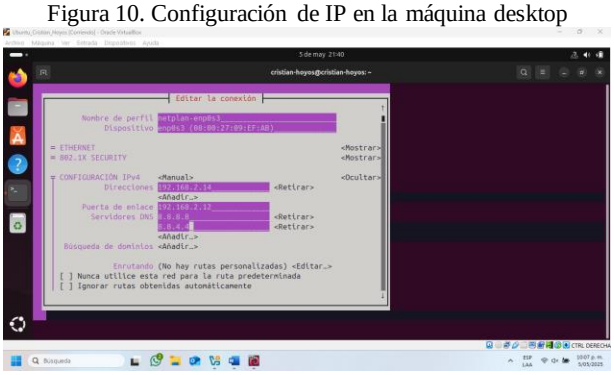


Fuente. Autoría Propia

Para la máquina desktop se puede hacer uso de la herramienta nmcli, la cual permite cambiar la dirección IP de un dispositivo Linux de manera más gráfica y sencilla, para acceder a esta herramienta se ejecuta el comando nmcli el cual

despliega una ventana por la cual se puede navegar entre distintas opciones para personalizar la configuración de red, para la máquina desktop se estableció la IP 192.168.2.14/24 e igual que la máquina server, la puerta de enlace predeterminada debe apuntar al adaptador de la máquina Endian de la zona verde mediante la dirección IP 192.168.2.12/24: Fig. 10.

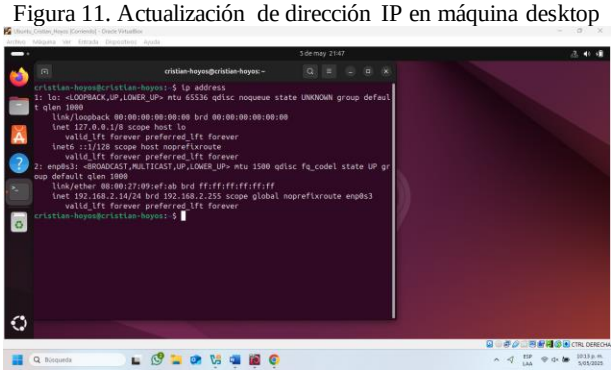
Figura 10. Configuración de IP en la máquina desktop



Fuente. Autoría Propia

Ya por último en esta parte se puede verificar la dirección IP asignada ejecutando el comando ip address: Fig. 11.

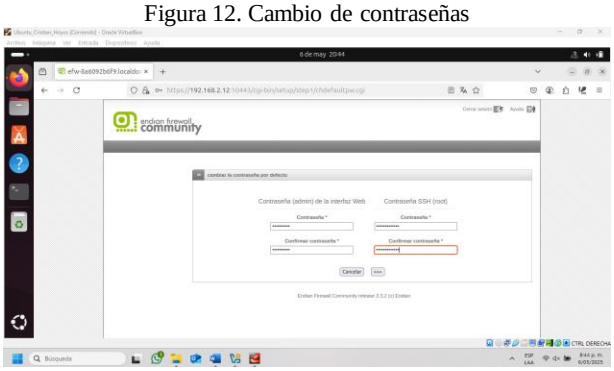
Figura 11. Actualización de dirección IP en máquina desktop



Fuente. Autoría Propia

Terminado de configurar las máquinas desktop y server ahora se continúa con la configuración de Endian desde su interfaz web, para ello se usó la máquina desktop que se encuentra en la zona verde, y el navegador de Firefox se ingresa a la dirección IP 192.168.2.12:10443, una vez cargada la interfaz se puede ver la bienvenida al firewall de Endian, inmediatamente después de esto el sistema pedirá que cambiemos la contraseña tanto para el usuario administrador de la interfaz web como para el usuario root: Fig. 12.

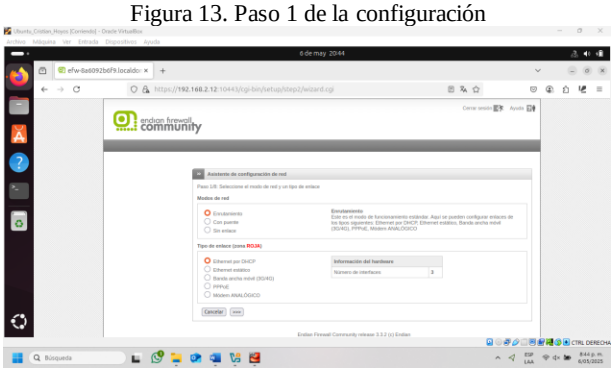
Figura 12. Cambio de contraseñas



Fuente. Autoría Propia

Luego de haber cambiado las contraseñas el sistema iniciara automáticamente la configuración de la red mediante ocho pasos, en el primer paso se establece el modo de la red en enrutamiento y el tipo de enlace para la zona roja en ethernet por DHCP: Fig. 13.

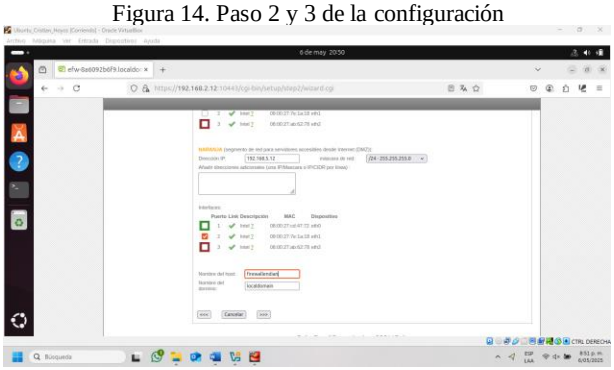
Figura 13. Paso 1 de la configuración



Fuente. Autoría Propia

Posterior a esto en el paso 2 se pedirá especificar qué tipo de zonas se va a configurar en la red, para este punto se selecciona configurar la zona naranja, esto debido a que durante la instalación ya se configuró la zona verde y en el paso anterior se especificó la configuración de la zona roja, luego de haber seleccionado la zona naranja en el paso 3 se deberá establecer el segmento de red para la zona naranja, en este punto se escribe la dirección IP 192.168.5.12 que se ha definido previamente: Fig. 5, y se selecciona el adaptador de red que se ha reservado para esto, así mismo en este punto también se puede cambiar el nombre del host y el nombre del dominio: Fig. 14.

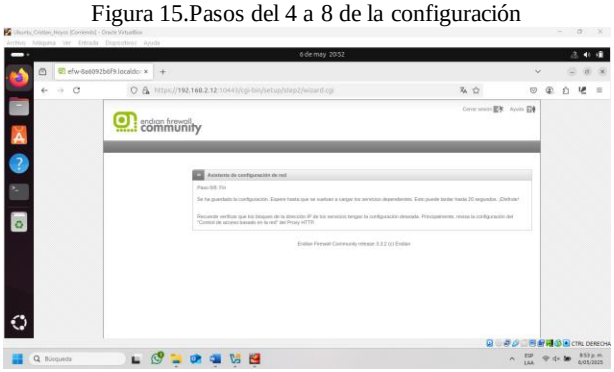
Figura 14. Paso 2 y 3 de la configuración



Fuente. Autoría Propia

Posteriormente en los pasos 4 a 8 se pueden configurar otras opciones para el firewall Endian, como el DNS y el correo electrónico administrativo por defecto, así mismo se puede confirmar las opciones que hemos definido antes de hacer algún cambio, y si todas las opciones ya se han configurado correctamente en el paso 7 se pueden aplicar la configuración y solo resta esperar a que se reinicien los servicios de Endian: Fig. 15.

Figura 15.Pasos del 4 a 8 de la configuración



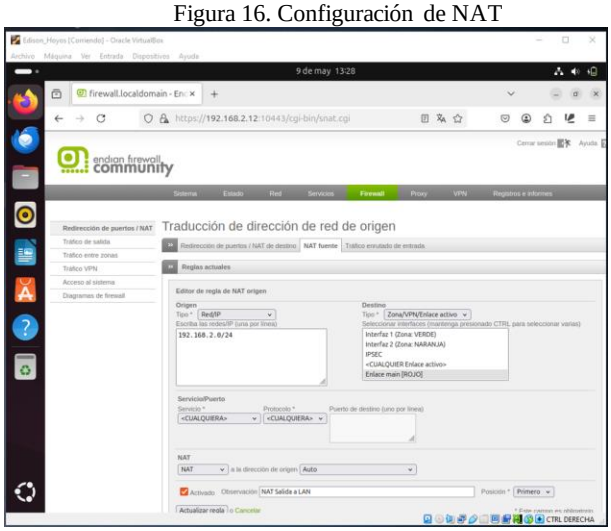
Fuente. Autoría Propia

Luego de que los servicios se hallan reiniciados el sistema pedirá que se inicie sección nuevamente, esta vez se deberá usar la contraseña que se definió durante el proceso.

4 TEMATICA 2: CONFIGURACIÓN DE REGLA NAT

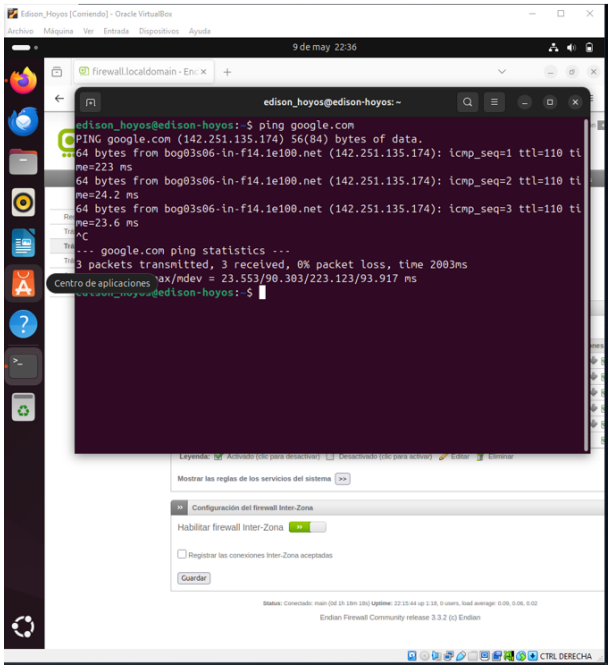
Una vez configurado Endian, al igual que las máquinas virtuales de las zonas, verde y naranja, se procedió a crear algunas reglas NAT, en el firewall Endian, esto se realizó con el fin de poder tener acceso desde la red LAN hacia la WAN, para entender esto de mejor modo, se recalca que la red LAN hace parte de la zona verde, y la red WAN es la zona roja: Fig. 5, se establece que la dirección IP de la zona verde es 192.168.2.12/24, por ende la LAN de esta red abarca desde el host 0 hasta el 254, de este modo se creó una regla NAT: Fig. 16, que indica que la red completa 192.168.2.0/24 puede tener acceso a la zona roja, de este modo al hacer ping desde la zona verdad que es la máquina Ubuntu hacia Google.com este arroja una conexión: Fig. 17.

Figura 16. Configuración de NAT



Fuente. Autoría Propia

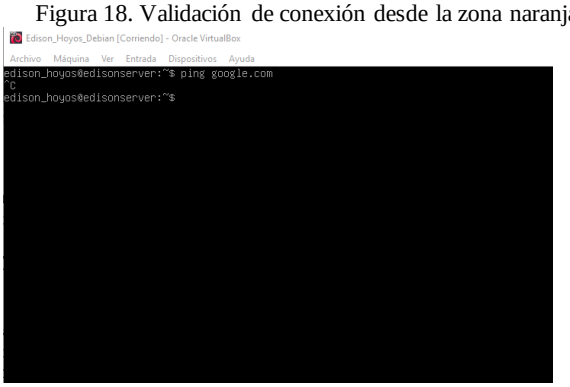
Figura 17. Demostración de conexión entre LAN y WAN



Fuente: Autoría Propia

Una vez que se verificó la conexión entre la LAN y WAN, se procedió a configurar y validar la conexión entre la zona desmilitarizada (zona naranja) hacia la WAN (zona roja), para ello se intentó realizar una conexión a google.com a través del comando ping desde la máquina Debian Server que está en la zona naranja: Fig. 18, el cual arroja que no existe comunicación a internet desde esta red.

Figura 18. Validación de conexión desde la zona naranja



Fuente. Autoría Propia

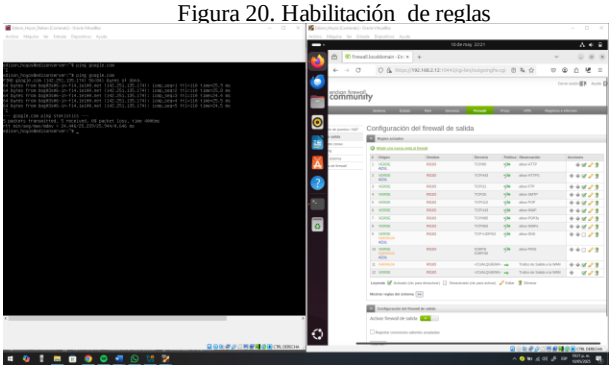
Para configurar y administrar esto se hizo uso de las reglas del firewall de Endian: Fig. 19, en Endian se tienen configuras por defecto varias reglas, algunas habilitas y otras deshabilitadas, para demostrar el funcionamiento de las reglas y su administración se dejó deshabilitadas las reglas 9 y 10. Fig. 19, al realizar esto solo se encuentra habilitada la comunicación de la zona verde con la zona roja, es por esto que el ping realizado tuvo existo: Fig. 17, dado que la regla se encuentra habilitada, ahora si se habilita la regla 11 y se vuelve a realizar ping a Google.com debería haber tráfico de paquetes.

Figura 19. Configuración de tráfico de salida

Fuente. Autoría Propia

En la figura 20, se aprecia del lado derecho que la regla 11 se encuentra activa y del lado izquierdo que existe tráfico de paquetes hacia Google.com, de este modo se comprobó que la zona naranja tiene acceso a internet y el uso de las reglas NAT desde Endian.

Figura 20. Habilitación de reglas

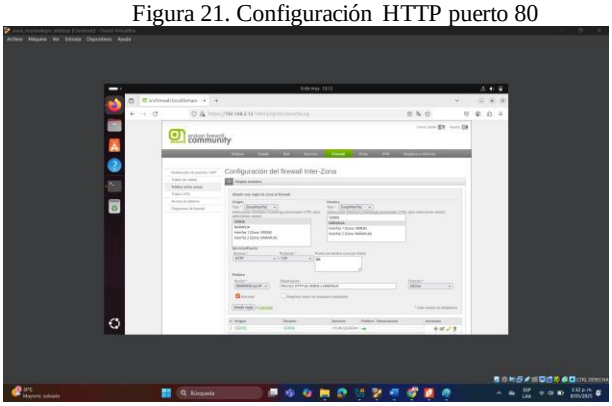


Fuente. Autoría Propia

5 TEMACTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

En la interfaz web de Endian específicamente en la sección tráfico entre zonas, se crea una regla para permitir el acceso HTTP desde la zona origen verde hasta la zona destino naranjada, se define el puerto 80 y se agrega la regla, una vez agregada se aplican los cambios: Fig. 21.

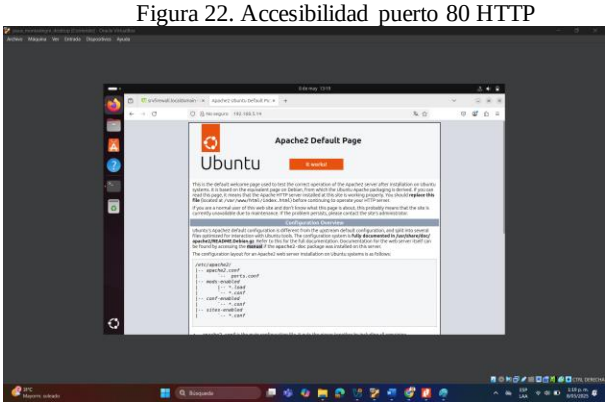
Figura 21. Configuración HTTP puerto 80



Fuente: Autoría Propia

Se verifica la funcionalidad de acceso al puerto 80 por el servicio HTTP por medio de la dirección http://192.168.514 en el navegador de Ubuntu Desktop, se visualiza la accesibilidad por este puerto accediendo a la interfaz web apache2, otra manera de probar la funcionalidad es con http://google.com: Fig. 22.

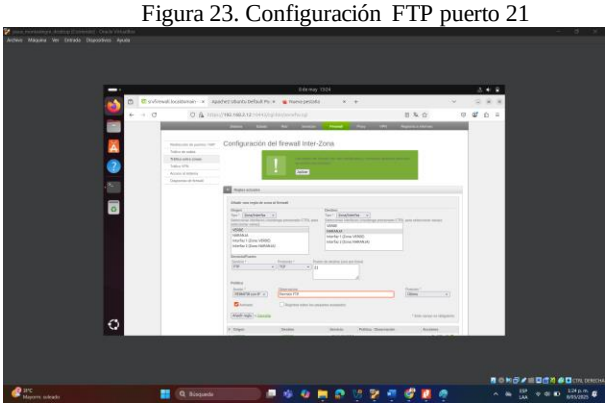
Figura 22. Accesibilidad puerto 80 HTTP



Fuente: Autoría Propia

Ahora para permitir el servicio FTP por el puerto 21 nuevamente desde la interfaz web de Endian, en la sección de tráfico entre zonas se crea una regla con el servicio FTP del puerto 21, una vez agregada la regla, se aplican los cambios realizados: Fig. 23.

Figura 23. Configuración FTP puerto 21



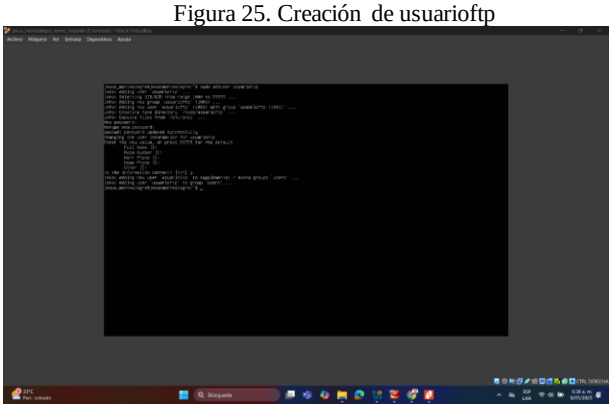
Fuente: Autoría Propia

Para probar el funcionamiento del FTP, en Ubuntu Server se instaló un servidor vsftpd: Fig. 24, finalizada la instalación se creó un usuario llamado usuarioftp, se asignó una contraseña y el resto de información se dejó por defecto: Fig. 25.

Figura 24. Instalación servidor de FTP

Fuente: Autoría Propia

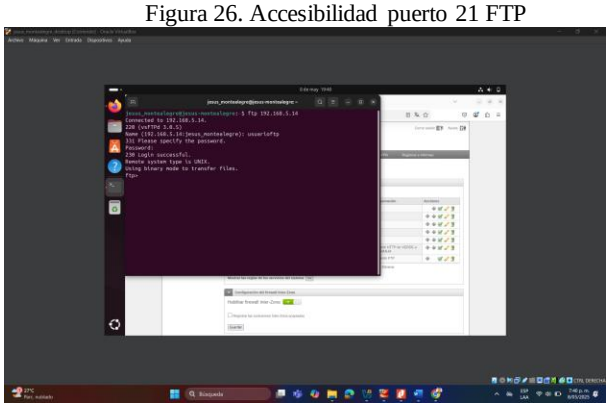
Figura 25. Creación de usuarioftp



Fuente: Autoría Propia

Se accedió a la terminal de Ubuntu Desktop, y se digitó el comando ftp 192.168.5.14 logrando establecer una conexión para el servidor: Fig. 26.

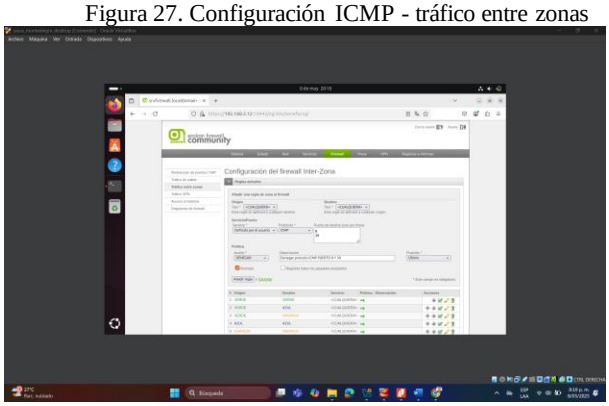
Figura 26. Accesibilidad puerto 21 FTP



Fuente: Autoría Propia

Ahora para denegar el protocolo ICMP por el puerto 8 y 30 desde la interfaz web de Endian se crean dos reglas, la primera en la sección tráfico entre zonas donde va de un origen cualquiera a un destino cualquiera y se seleccionó el servicio ICMP por el puerto 8 y 30, para la acción se escogió denegar: Fig. 27, por la sección de tráfico de salida se creó una regla para denegar el ping que se realiza hacía la WAN inicia desde un origen cualquiera y llega a un destino rojo por el puerto 8 y 30 teniendo la acción de denegar: Fig. 28.

Figura 27. Configuración ICMP - tráfico entre zonas



Fuente: Autoría Propia

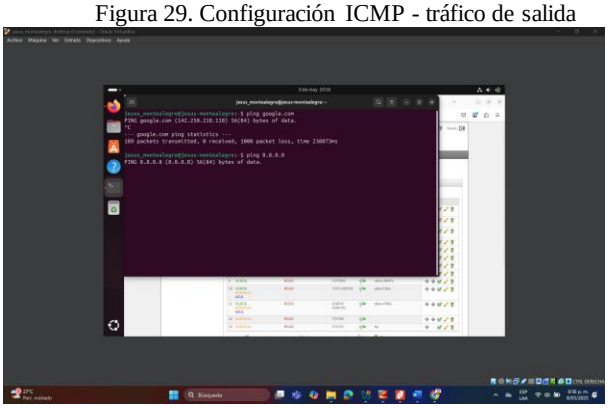
Figura 28. Configuración ICMP - tráfico de salida

Fuente: Autoría Propia

Desde Ubuntu Desktop se ingresó a la terminal y se ejecutaron los comandos ping google.com y ping 8.8.8.8. y se

confirmó que en ambos casos no se obtuvo respuesta de la red: Fig. 29.

Figura 29. Configuración ICMP - tráfico de salida



Fuente: Autoría Propia

6 TEMATICA 4: IMPLEMENTACION DE UN PROXY HTTP NO TRANSPARENTE

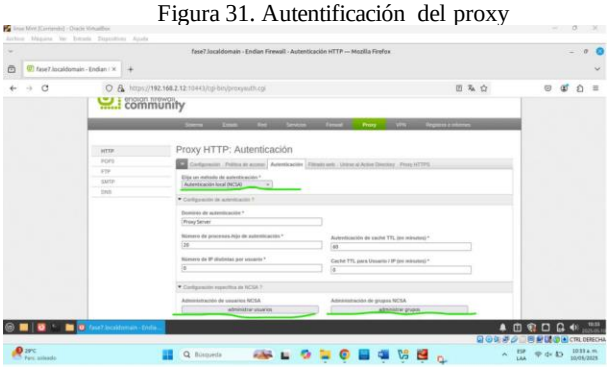
En la sección web de Endian de Proxy se habilitó el proxy, de igual manera se configuró con un proxy no transparente en el puerto 8080 para las redes verde y naranja: Fig. 30.

Figura 30. Configuración del proxy

Fuente. Autoría Propia

Para poder configurar la autentificación del proxy se creó un usuario llamado fase7 y un grupo llamado 24, para el cual se estableció una contraseña: Fig. 31.

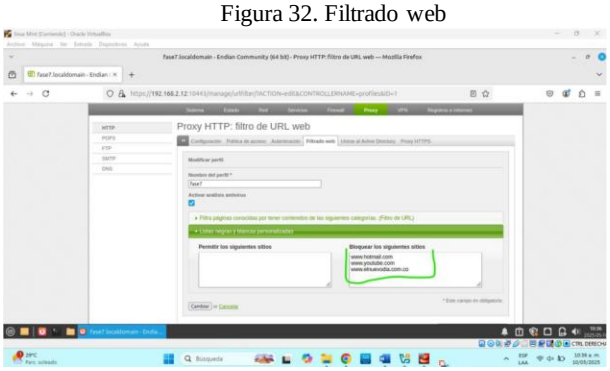
Figura 31. Autentificación del proxy



Fuente. Autoría Propia

Gracias a que se creó un usuario, se configuró el perfil de este para habilitar la lista negra de las páginas web a las cuales se les denegó el acceso entre estas están www.hotmail.com, www.youtube.com, www.elnuevodia.com.co: Fig. 32.

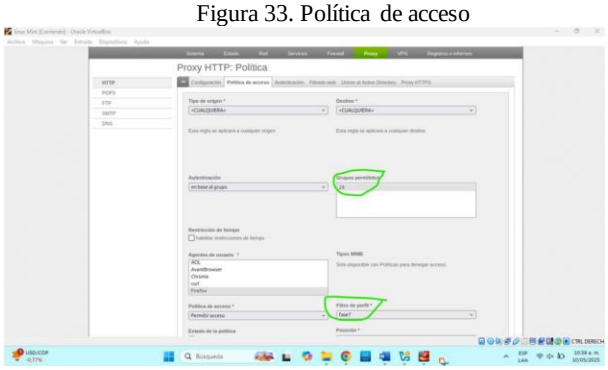
Figura 32. Filtrado web



Fuente: Autoría Propia

Una vez se aplicó el filtro web para denegar el acceso a las páginas web, se configura la política de acceso: Fig. 33, al grupo 24 y al usuario fase 7 creados.

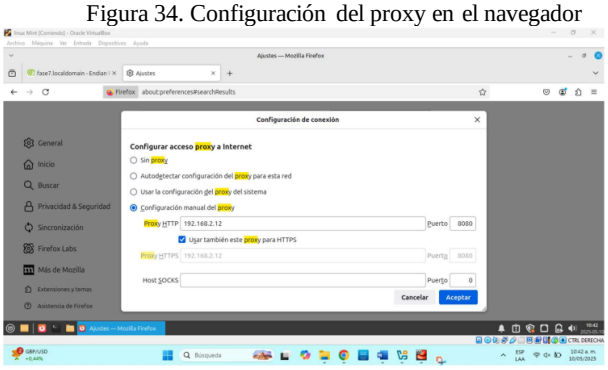
Figura 33. Política de acceso



Fuente. Autoría Propia

Finalizada la configuración desde Endian del proxy se procedió a habilitar en el navegador, la dirección 192.168.2.12 con el puerto 8080: Fig. 34, esta configuración se aplicó en el navegador Firefox de la zona verde.

Figura 34. Configuración del proxy en el navegador

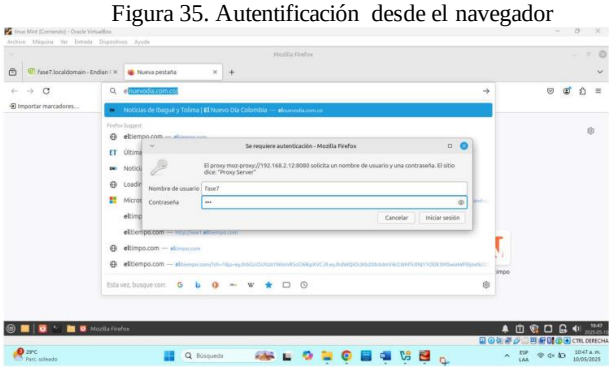


Fuente. Autoría Propia

En la figura 34 al dar clic en aceptar, el navegador solicita autentificarse para aplicar la configuración del proxy

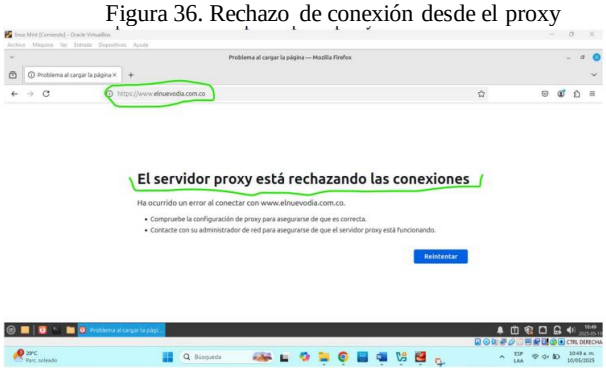
de Endian: Fig. 35, después de la autentificación, se ingresó a las páginas de la lista negra configuradas: Fig. 32, y se observa cómo se denegó el tráfico hacia el sitio web, con esto se demostró que el proxy está configurado y rechazando conexiones de la lista negra: Fig. 36.

Figura 35. Autentificación desde el navegador



Fuente. Autoría Propia

Figura 36. Rechazo de conexión desde el proxy



Fuente. Autoría Propia

7 CONCLUSIONES

7.1 TEMATICA 1

La configuración inicial de la instancia de Endian Firewall en un entorno virtualizado permitió establecer una red segmentada bajo principios de seguridad por capas, gracias a la configuración de los adaptadores de red y la definición de las distintas zonas como la verde para la red LAN, la naranja para la zona DMZ y la roja para la red WAN, se constituyó una base para un entorno controlado y seguro que facilita la administración eficiente del tráfico interzonal.

7.2 TEMATICA 2

Con la configuración de las zonas y la asignación de los adaptadores de red específicos se pudieron aplicar reglas NAT que permiten aislar y controlar el tráfico entre diferentes partes de la red, reduciendo la superficie de ataque y facilitando la administración de reglas de acceso y servicios.

La creación y habilitación de reglas NAT y de firewall en Endian permite controlar el acceso entre las zonas, habilitando o restringiendo servicios como HTTP y FTP según las necesidades de la organización.

7.3 TEMATICA 3

Endian Firewall Community, basado en GNU/Linux, permite transformar un equipo estándar en un dispositivo de seguridad con gestión unificada de amenazas (UTM). Su firewall bidireccional, junto a funciones como VPN, proxy, filtro de contenido y la gestión de múltiples zonas de red, lo hacen adecuado para proteger infraestructuras tecnológicas frente a amenazas internas y externas.

7.4 TEMATICA 4

La validación práctica mediante pruebas de conexión HTTP, FTP y uso de proxy no transparente demostró que Endian permite una administración eficiente de los servicios, control de acceso web y aplicación de filtros por ende estas configuraciones refuerzan la importancia de integrar soluciones de firewall avanzadas en entornos de red para fortalecer la ciberseguridad organizacional.

8 REFERENCIAS

[1] Geier, E. (2021, 12 marzo). *Endian Firewall, router & server set up*. ServerWatch. https://www.serverwatch.com/guides/setting-up-an-open-source-server-firewall-and-router-on-endian-part-1/?utm

[2] *Guía de escritorio de Ubuntu*. (2023). Ubuntu Documentation. https://help.ubuntu.com/20.04/ubuntu-help/index.html

[3] *Guía Debian GNU/Linux de instalación*. (2023). Debian. https://www.debian.org/releases/stable/amd64/index.es.html

[4] *Endian UTM 3.2 Reference Manual*. (2016). Endian. http://docs.endian.com/3.2/utm/index.html

[5] LaCroix, J. (2020). *Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server*. Packt Publishing. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[6] *21.3. Comandos nmcli frecuentes*. (s. f.). Red Hat Documentation. https://docs.redhat.com/es/documentation/red_hat_enterprise_linux/8/html/system_design_guide/ref-frequent-nmcli-commands_getting-started-with-nmcli

[7] *Oracle VirtualBox: User Guide for Release 7.1*. (2020). VirtualBox. https://www.virtualbox.org/manual/

[8] *DHCP Administrative Web Page*. (2016). Endian. https://docs.endian.com/archive/2.1/efw.services.dhcp.html

[9] *DNAT (Port Forward) - Basic Setup*. (2016). Endian. https://help.endian.com/hc/en-us/articles/218144268-DNAT-Port-Forward-Basic-Setup

[10] theNET. (s. f.). *¿Qué es una WAN? | WAN vs. LAN*. CLOUDFLARE. https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-wan/

[11] Das, P. K., & Deka, G. C. (Eds.). (2018). *Design and use of virtualization technology in cloud computing*. IGI Global. https://doi.org/10.4018/978-1-5225-2785-5

[12] *Configuring DMZ*. (s. f.). Recuperado 22 de mayo de 2025, de https://www.cisco.com/c/dam/assets/sol/sb/isa500_emulator/help/guide/ad1681599.html

[13] Gagliardo, D., Lechner, R., Sondermann, M., Vallazza, R., Warasin, P., & Graffer, C. (2006, 24 mayo). *Endian Firewall Administrators Guide*. Recuperado 22 de mayo de 2025, de https://docs.endian.com/archive/2.1/efw.system.network_configuration.html

[14] IBM. (2021, 14 abril). *Crear reglas de NAT*. Recuperado 22 de mayo de 2025, de https://www.ibm.com/docs/es/i/7.3.0?topic=rules-creating-nat

[15] Walton, A. (2018, 15 febrero). *Configuración de la NAT: Ejemplos y Comandos - CCNA desde Cero*. CCNA Desde Cero. https://ccnadesdecero.es/configuracion-nat-estatica-dinamica-pat/