INSTALACIÓN Y CONFIGURACIÓN DE ENDIAN COMO FIREWALL PARA PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

Maricel Silva Albarracín
e-mail: msilvaal@unadvirtual.edu.co

RESUMEN: *En el presente artículo se describe la implementación individual del firewall de código abierto Endian Firewall Community (EFW), edición 3.3.2. El despliegue se realizó mediante virtualización, estableciendo un esquema de seguridad basado en tres interfaces de red operativas: una zona de red externa (WAN), una red interna protegida (LAN) y una zona desmilitarizada (DMZ) para la exposición controlada de servicios.[1]*

PALABRAS CLAVE: Endian, Firewall, DMZ, Red

ABSTRACT: *This article describes the individual implementation of the Open-Source firewall Endian Firewall Community (EFW), version 3.3.2. The deployment was carried out using virtualization, establishing a security scheme based on three operational network interfaces: an external network zone (WAN), a protected internal network (LAN), and a delimitarized zone (DMZ) for controlled service exposure.[1]*

1 INTRODUCCIÓN

El presente articulo corresponde al desarrollo individual de la Temática de permitir servicios de la zona DMZ para la red, en la cual se configura el firewall Endian Firewall Community (EFW) versión 3.3.2, instalado sobre una máquina virtual en VirtualBox con tres interfaces de red: Zona Roja (WAN), Zona Verde (LAN) y Zona Naranja (DMZ). La configuración de las reglas de filtrado se realiza íntegramente desde la consola utilizando comandos iptables, cumpliendo con el requisito de la guía de no utilizar interfaces gráficas.

Se documentan los procedimientos técnicos ejecutados, las capturas de pantalla con evidencia de fecha y hora, y la verificación del bloqueo del protocolo ICMP, demostrando el cumplimiento de los objetivos planteados.[2]

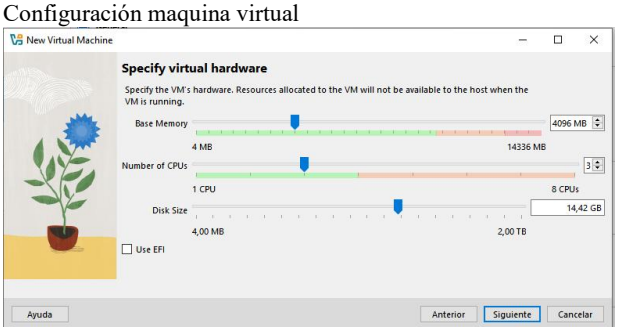
2 DESARROLLO DE LA TEMATICA

2.1 TEMATICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

La fase de implementación del entorno de red de prueba requiere la configuración de un hipervisor sobre el sistema anfitrión, para esto se seleccionó la plataforma de código abierto Oracle VM VirtualBox, el proceso de instalación del entorno se inició con la instalación siguiendo los parámetros de configuración de almacenamiento y asignación de recursos descritos en su manual de usuario oficial [3].

Se inicia con el descargue del sistema operativo Ubuntu en modo gráfico y modo consola (Desktop y Server) [4], de acuerdo con la tecnología que maneja el equipo, que para este caso corresponde a 64 bits. También se instaló Endian Firewall UTM 3.2 [5]. En la figura 1 se observa la configuración de la maquina virtual en VirtualBox, se asignaron 4096 MB de memoria RAM y 14,42 GB de disco duro, el tipo de sistema operativo seleccionado fue Red Hat (64-bit) para garantizar la compatiblidad con el kernel de endian .

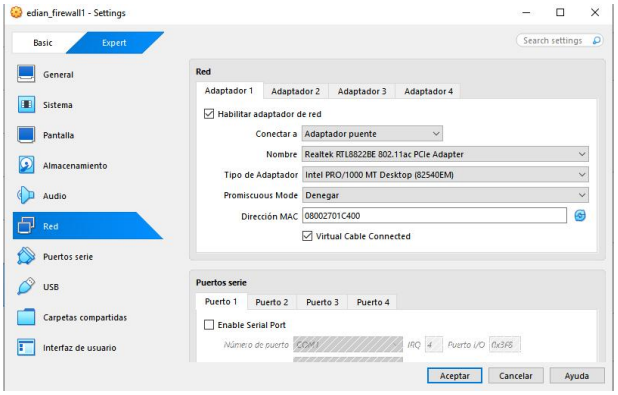
Figura 1.
Configuración maquina virtual



Fuente: Autoría Propia

En la figura 2 se evidencia la configuración del adaptador 1 correspondiente a la zona red (WAN). Se seleccionó el modo adaptador puente sobre la interfaz de red Realtek del equipo anfitrión, esta configuración permite que el firewall obtenga una dirección IP directamente de la red local facilitando el acceso a Internet para la zona LAN y DMZ

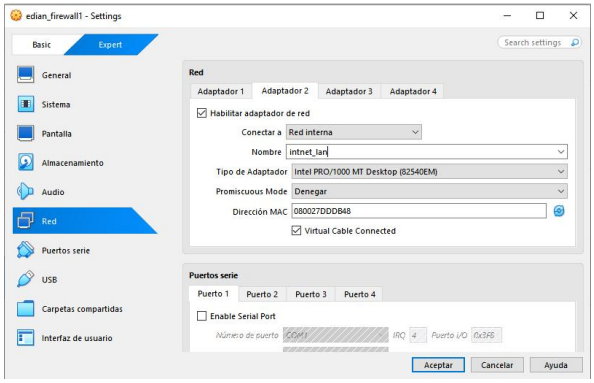
Figura 2.
Configuración adaptador 1 WAN



Fuente: Autoría propia

Para la configuración del adaptador 2 destinado a la zona Green (LAN) como muestra la Figura 3 se eligió este tipo de red interna con el nombre de intnet_lan lo que crea una red aislada entre la maquina virtual Endian y los futuros clientes de la red interna.

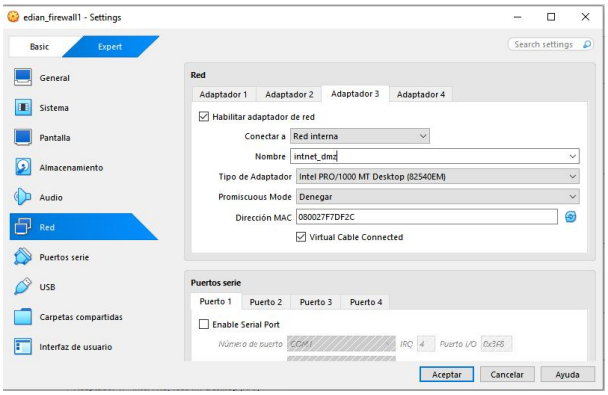
Figura 3.
Configuración adaptador 2 LAN



Fuente: Autoría propia

La figura 4 muestra la configuración del adaptador 3 correspondiente a la zona Orange (DMZ) al igual que LAN se utilizó una red interna con el nombre intnet_dmz, esta red aislada aloja los servicios Web y FTP que serán accesibles desde Internet.

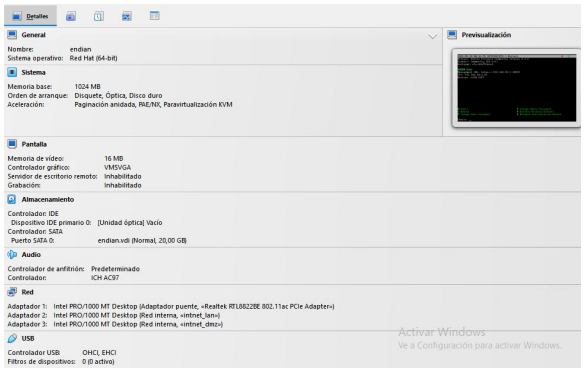
Figura 4.
Configuración adaptador 3 DMZ



Fuente: Autoría propia

Posteriormente se presenta un resumen completo de la configuración de la maquina virtual como se evidencia en la Figura 5, en esta etapa de verificación se confirman parámetros establecidos para garantizar el rendimiento optimo del sistema operativo basado en la arquitectura Red Hat (64-bit), el aprovisionamiento de recursos que incluye una memoria de 4 GB, la asignación de 3 procesadores. Un aspecto importante en este despliegue es la presencia de 3 adaptadores de red configurados, la red interna LAN, la conexión externa (WAN) y la zona desmilitarizada (DMZ); también se valida la habilitación del controlador USB 2.0 para la compatibilidad de periféricos y la gestión local de almacenamiento físico en caso de contingencias.

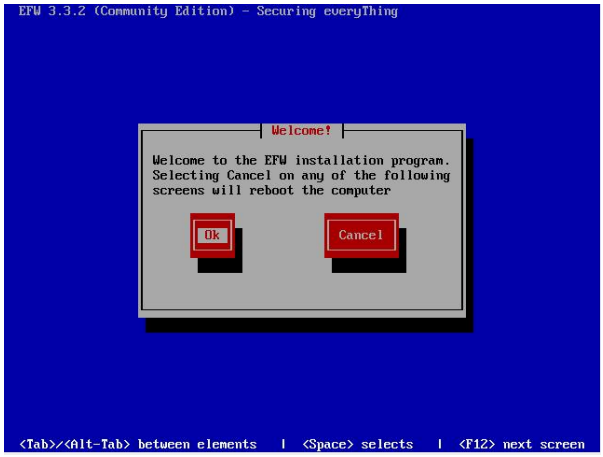
Figura 5.
Configuración maquina virtual a trabajar



Fuente: Autoría propia

Como se evidencia en la figura 6 la interfaz presenta la pantalla de bienvenida del instalador de Endian Firewall, en este punto el sistema confirma que ha detectado el disco para la instalación, al confirmar la acción mediante la selección del comando OK, dando inicio al proceso automatizado de particionamiento de disco y formato del sistema. Con este paso se establece la estructura necesaria para la posterior carga de los módulos de red y servicios de seguridad del Firewall.

Figura 6.
Instalación de Endian

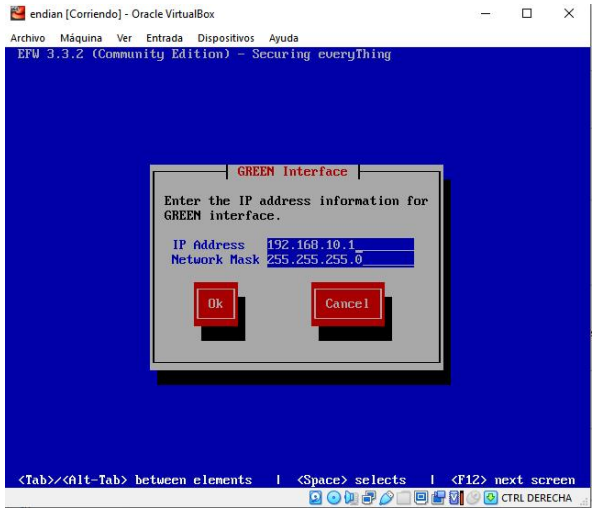


Fuente: Autoría Propia

Como se observa en la figura 7 se procedió con la modificación de la dirección IP predeterminada de la interfaz de administración, asignado el valor 192.168.10.1 Esta modificación responde a una estrategia de segmentación y estandarización del segmento de la red de área local LAN. Al reconfigurar este parámetro el Endian Firewall se establece

como la puerta de enlace predeterminada de la subred interna, permitiendo centralizar el enrutamiento y aplicar las políticas de seguridad y filtrado de paquetes sobre todo el trafico saliente de los hosts locales antes de interactuar con la zona DMZ o la red externa (WAN).

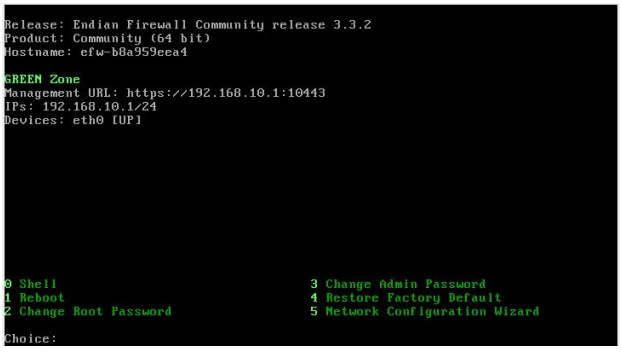
Figura 7.
Dirección IP y Network Mask



Fuente: Autoría propia

Como se muestra en la figura 8 se despliega el menú principal de la consola Endian Firewall una vez finalizada la secuencia de arranque inicial después de la instalación. En esta interfaz el sistema confirma que la zona GREEN se encuentra completamente operativa bajo la dirección IP 192.168.10.1 Asimismo, se valida que el servicio de aprovisionamiento y configuración remota esta disponible a través del puerto seguro 10443 mediante el protocolo HTTPS.

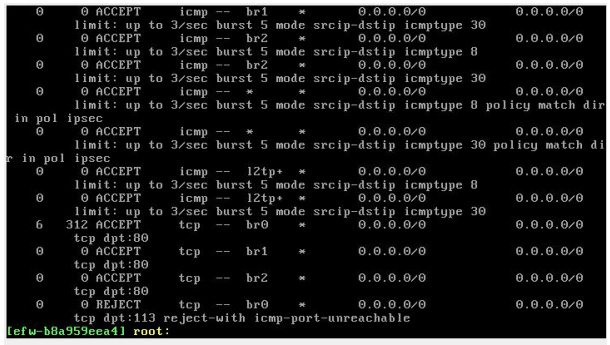
Figura 8.
Zona verde



Fuente: Autoría propia

En la figura 9 se presentan las reglas del firewall configuradas mediante el comando iptables, especificamente se observa la declaración de reglas con politica de aceptación (ACCEPT) dirigidas al trafico saliente desde la interfaz fisica eth2 asociada a la zona DMZ hacia la interfaz eth0 asignada como el enlace de salida hacia la red externa (WAN). Estas reglas habilitan la comunicación a través de los puertos 80 (HTTP) y 21 (FPT) permitiendo de forma controlada que los servidores alojados en el segmento DMZ inicien conexiones hacia el exterior para tareas de administración como actualización de paquetes de software.

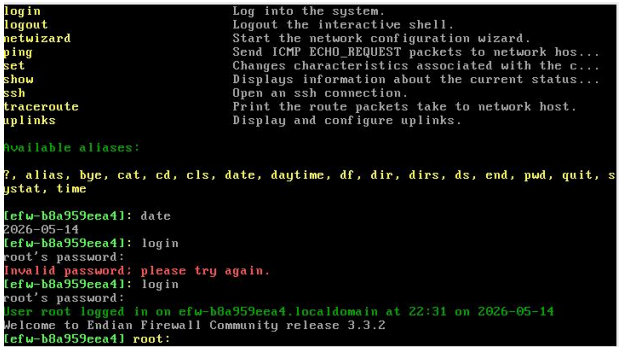
Figura 9.
Actualización puertos



Fuente: Autoría propia

En la figura 10 se documenta el proceso de autenticación en la consola de linea de comandos de Endian, la captura evidencia el mecanismo de control de acceso, donde se ejecuta el proceso de inicio (login), seguido del usuario root y la validación de la contraseña configurada previamente. Este acceso directo por consola resulta indispensable para la auditoría de registros en tiempo real, el diagnostico físico de las interfaces de red y la manipulación avanzada de las tablas de enrrutamiento que no están expuestas en la interfaz gráfica.

Figura 10.
Interfaz linea de comandos

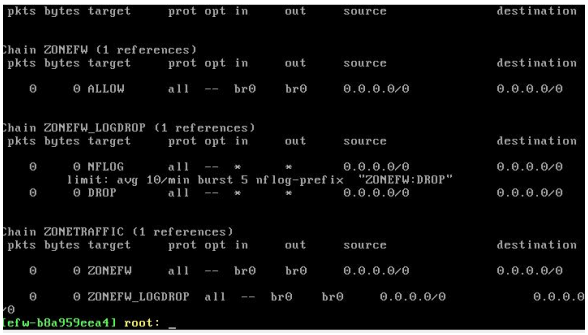


Fuente: Autoria propia

En la figura 11 se evidencia la salida del comando: iptables -L -v - n en la consola del sistema, herramienta fundamental para la auditoría y verificación del plano de datos en tiempo real; enlista todas las reglas de firewall activas en el sistema, se pueden identificar las cadenas personalizadas del endian (zone fw, zonefw_logdrop, zonetraffic) que gestionan el trafico entre zonas. Esta verificacion es crucial para

confirmar que las reglas de permitir HTTP / FTP y denegar ICMP se hayan aplicado correctamente.

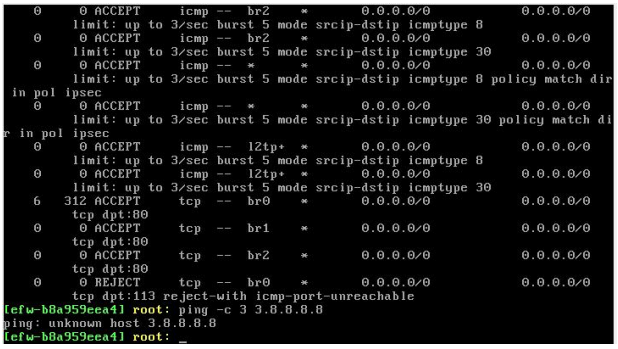
Figura 11.
Salida del comando



Fuente: Autoría Propia

Con el propósito de verificar la efectividad de las directivas de seguridad aplicadas sobre el trafico de diagnostico, se ejecutó una prueba de conectividad mediante el comando ping 8.8.8.8 desde la interfaz de linea de comandos. Como se observa en la figura 12 el intento de comunicación hacia el direccionamiento IP externo no produce replica alguna por parte del destino, registrando de forma concluyente un 100% de perdida de paquetes, lo que confirma que el protocolo ICMP ha sido denegado correctamente.

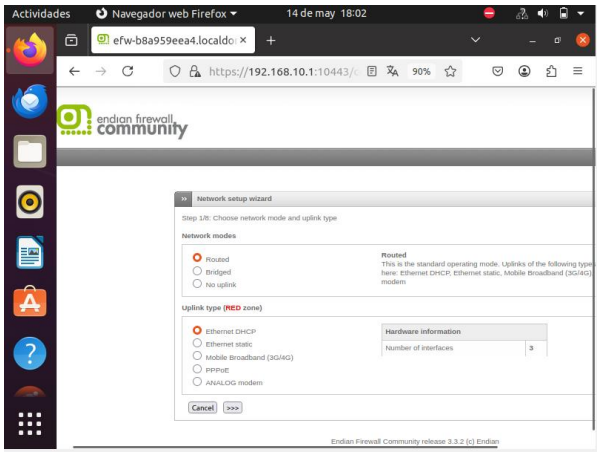
Figura 12.
Negación ping en red



Fuente: Autoria propia

A continuación, en la figura 13 se ilustra la etapa inicial del asistente de configuración de red, al cual se accedió a través de la interfaz gráfica de usuario https://192.168.10.1:10443 En esta pantalla se selecciona el modo routed (NAT) y el tipo de UPLINK Ethernet DHCP para la zona red. Durante esta secuencia el sistema de Endian Firewall validó la correspondencia del hardware virtual, detectando correctamente las 3 interfaces de red configuradas en VirtualBox, las cuales servirán como la base física para la segmentación de las zonas LAN, WAN y DMZ.

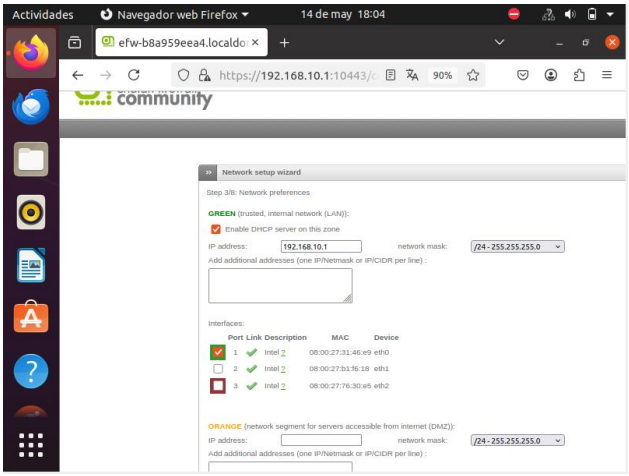
Figura 13.
Acceder a interfaz Web



Fuente: Autoría propia

En la figura 14 se documenta la fase de aprovisionamiento y asignación de interfaces dentro del asistente de configuración en la Web, este paso permite asignar las interfaces físicas (eth0, eth1 y eth2) a las zonas lógicas (RED, GREEN, ORANGE)

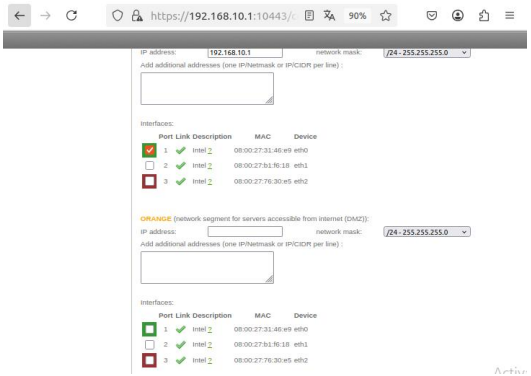
Figura 14.
Acceder a interfaz Web



Fuente: Autoría propia

En la figura 15 se presenta la configuración detallada de las zonas GREEN (LAN) y ORANGE (DMZ), para la GREEN se asignó la IP 192.168.10.1/24 con servidor DHCP habilitado mientras que para la ORANGE se reservó la IP 192.168.20.1/24 para los servidores Web y FTP, esta segmentación permite que los servidores en DMZ sean accesibles desde Internet sin comprometer la seguridad de la red interna.

Figura 15.
Asistente de configuración de red



Fuente: Autoría propia

Con el desarrollo de la temática de permitir servicios de la zona DMZ para la red se evidencia la ejecución de los servicios HTTP (puerto 80) y FPT (puerto 21) desde el servidor Web bajo Ubuntu Server , así como la denegación del protocolo ICMP para no permitir hacer ping en la red.

3 CONCLUSIONES

1. El uso de iptables en Endian Firewall permite un control granular del tráfico de red, diferenciando entre servicios permitidos (HTTP y FTP) y denegados (ICMP), lo que facilita la implementación de políticas de seguridad perimetral.

2. El bloqueo total del protocolo ICMP mediante reglas DROP en las cadenas INPUT, FORWARD y OUTPUT fortalece la seguridad de la red al impedir que atacantes realicen escaneos básicos de reconocimiento mediante el comando ping.

4 REFERENCIAS

[1] Universidad Nacional Abierta y a Distancia (UNAD), "Guía de aprendizaje - Etapa 7 - Implementando Seguridad en GNU/Linux," en Diplomado de profundización en administración de sistemas operativos open source con certificación en Linux, 2026. [En línea]. Disponible en: https://campus151.unad.edu.co/ses62/mod/resource/view.php?id=4464

[2] Free Software Foundation (2016). Software Libre y educación. El sistema operativo GNU. http://www.gnu.org/education/education.html

[3] Oracle, Manual de usuario VirtualBox, VirtualBox documentation,2020. [En línea]. Disponible en: https://www.virtualbox.org/manual/

[4] Canonical, Guía del Ubuntu desktop 20.04 LTS, Help Ubuntu, 2023. [En línea]. Disponible en: https://help.ubuntu.com/

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