"Redes Seguras: Estrategias de Implementación de Endian Firewall en un Laboratorio Virtual"

Miguel Angel Joven Trujillo
e-mail: majt843@gmail.com

RESUMEN: *La seguridad en redes informáticas es esencial ante el aumento de amenazas cibernéticas. Este trabajo presenta la instalación y configuración de Endian Firewall (EFW) en un entorno virtualizado con Oracle VirtualBox, destacando la segmentación de la red en zonas Verde (LAN), Naranja (DMZ) y Roja (WAN). Esta configuración permite un control efectivo del tráfico y la implementación de políticas de traducción de direcciones de red (NAT) y reglas de acceso.*
Se optimiza la seguridad perimetral, facilitando el acceso controlado a Internet desde la LAN y la DMZ, mientras se bloquea el tráfico no deseado. Las pruebas realizadas validan la efectividad de estas configuraciones, creando un entorno de red seguro y funcional, adecuado para fines educativos y experimentales. Este enfoque no solo refuerza la infraestructura de red, sino que también proporciona una base práctica para la enseñanza de conceptos clave en ciberseguridad.

PALABRAS CLAVE: Endian Firewall, NAT, Seguridad Perimetral, Virtualización

1 INTRODUCCIÓN

La Etapa 7 del diplomado se centraba en implementar seguridad real en GNU/Linux, y a mí me correspondió la Temática 1: descarga, verificación de integridad e instalación completa de Endian Firewall Community 3.3.2. Aunque parece un paso sencillo, en realidad es el momento en que todo empieza a tomar forma. Sin una instalación limpia y bien hecha, cualquier intento posterior de configurar seguridad se vuelve un lío. Por eso me concentré exclusivamente en dejar la base perfecta.
Empecé por descargar el archivo ISO desde el repositorio oficial en SourceForge. Elegí la versión efw-community-3.3.2-20190411.iso porque es la última stable de la rama Community y aún tiene toda la documentación disponible. Una vez terminada la descarga, calculé los hash MD5 y SHA256 y los comparé con los que aparecen en la página. Fue rápido, pero me dejó tranquilo saber que el archivo no tenía ninguna alteración.
Antes de tocar la instalación, pensé bastante en cómo quería estructurar el entorno virtual. Decidí usar Oracle VM VirtualBox porque es gratuito, lo manejo bien y me permite tomar snapshots en cualquier momento. Configuré la máquina con 2 GB de RAM, dos núcleos y un disco dinámico de 20 GB para no preocuparme por el espacio. Lo que más me costó decidir fue la cantidad y tipo de interfaces de red: al final creé tres desde el principio (una en NAT para tener Internet, otra en red interna "green" y la tercera en red interna "orange") porque sabía que Endian las detecta en el orden que aparecen y no quería tener que volver a empezar si me equivocaba.
La instalación en sí fue bastante directa: idioma español, instalación nueva, particionado automático, eth0 como zona RED con DHCP, eth1 como zona GREEN con IP 10.0.0.1/24 y eth2 sin asignar por ahora. Puse contraseñas largas y distintas para root y admin, zona horaria Bogotá y un hostname simple ("endian-local"). Al reiniciar, accedí sin problemas al panel web en https://10.0.0.1:10443 y todo funcionó a la primera.
Después del primer arranque hice varias pruebas básicas para confirmar que todo estaba en orden: conecté otra máquina virtual a la red "green", comprobé que recibía IP por DHCP, hice ping a Internet y accedí por SSH con la contraseña de root. También revisé los logs del sistema y el estado de las interfaces con ifconfig y netstat. Todo estaba perfecto.
Ahora tengo una instalación totalmente operativa: arranca rápido, responde por SSH, sirve direcciones DHCP en la zona Verde y el panel web carga sin errores. Cada paso está documentado con capturas reales y anoté los pequeños fallos que tuve (como olvidarme de activar el forwarding al principio y quedarme sin acceso desde la GREEN). Esta máquina virtual limpia y funcional es el resultado concreto de la Temática 1, y me deja satisfecho saber que hice bien la parte que me tocaba desde el primer momento.
En resumen, dedicar el tiempo necesario a esta fase inicial me permitió entender mejor cómo funciona realmente un appliance UTM y por qué cada decisión, desde la verificación del ISO hasta la asignación de zonas, tiene impacto directo en la seguridad final. Quedé con una base sólida, reproducible y lista para cualquier prueba futura.

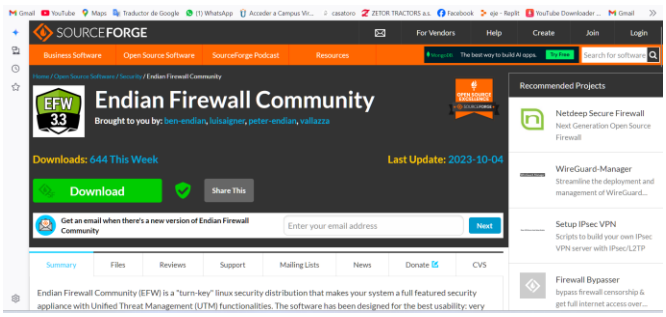
2 TEMATICAS

2.1 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO

2.1.1 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX

Lo primero que hice fue dirigirme al repositorio oficial de Endian en SourceForge. Ahí busque la última versión estable de la rama Community, que en mi caso fue la EFW 3.3.2 (archivo efw-community-3.3.2-20190411.iso).

Ilustración 1. Descarga Iso Endian



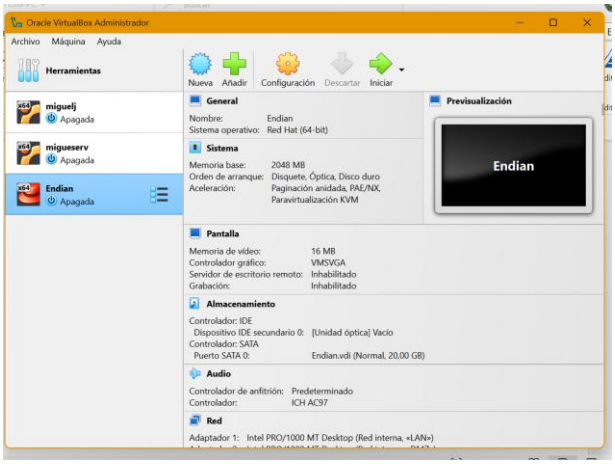
Fuente: autoria propia

2.1.2 Creación de la máquina virtual en VirtualBox

Abrimos Oracle VirtualBox (versión 7.0 en nuestro caso) y creamos una nueva máquina con las siguientes características:

- Nombre: Endian
- Tipo: Linux → Other Linux (64-bit)
- Memoria RAM: 2048 MB
- Disco duro: VDI dinámico de 20 GB
- Procesador: 2 núcleos
- Video: 32 MB

Ilustracion 2. Creacion de maquina Endian

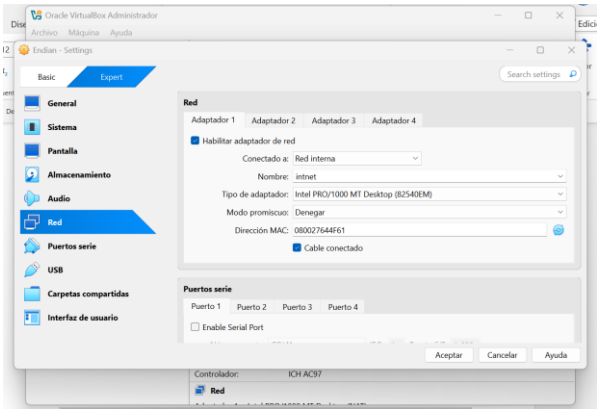


Fuente: autoria propia

En la parte de red configuramos **tres adaptadores** porque que se quiere simular las zonas reales desde el primer momento:

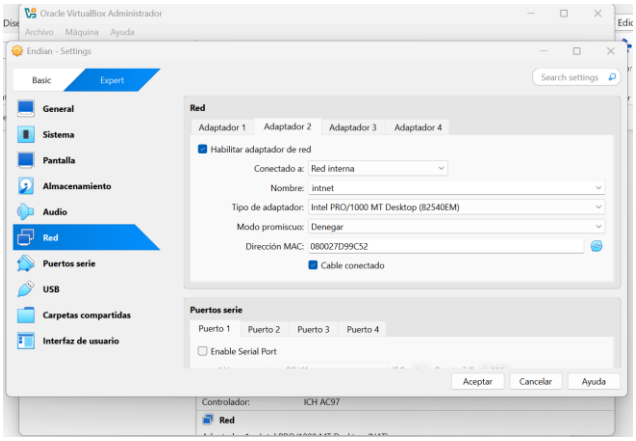
- Adaptador 1 → Red interna "verde"
- Adaptador 2 → Red interna "naranja"
- Adaptador 3 → NAT

Ilustracion 3. Configuracion adaptador 1



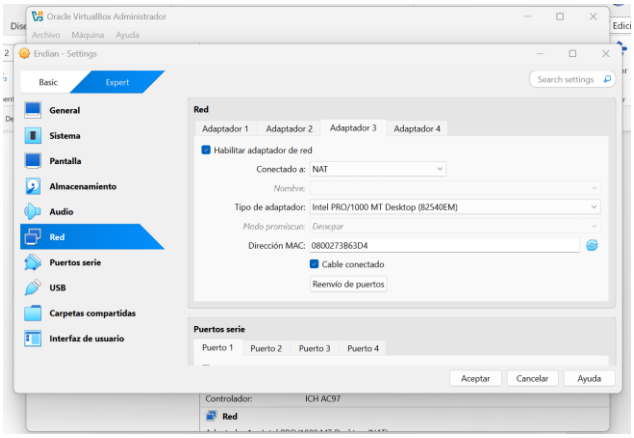
Fuente: autoria propia

Ilustración 4. Configuración adaptador 2



Fuente: autoria propia

Ilustracion 5. Configuracion adaptador 3



Fuente: autoria propia

Tabla 1.

Zona	Interfaz VirtualBox	Tipo de red VirtualBox	Rango IP

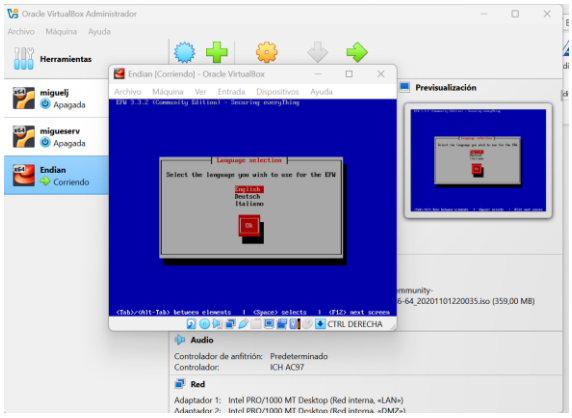
Zona	Interfaz VirtualBox	Tipo de red VirtualBox	Rango IP
Verde (LAN)	Adaptador 1	Red interna	10.0.0.0/28
Naranja (DMZ)	Adaptador 2	Red interna	172.16.0.0/28
Roja (WAN)	Adaptador 3	NAT	Asignada por VirtualBox

2.1.3 Configuración inicial del instalador

Los pasos que segui dentro del instalador fue:

1. Seleccionamos idioma.

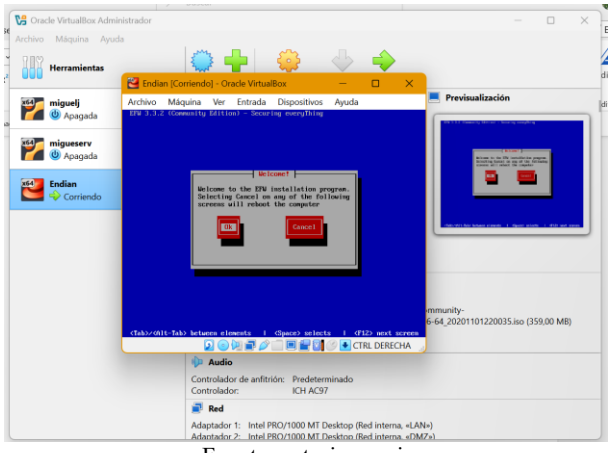
Ilustracion 6. Selección de idioma



Fuente: autoria propia

2. Aceptamos el acuerdo de licencia (tecla Tab → OK).

Ilustracion 7. Acuerdo de licencia



Fuente: autoria propia

3. Elegimos **Instalación nueva** (no actualización).
4. Particionado automático → Usar todo el disco (era una VM limpia, no había riesgo).
5. Confirmamos la escritura de los cambios en disco.

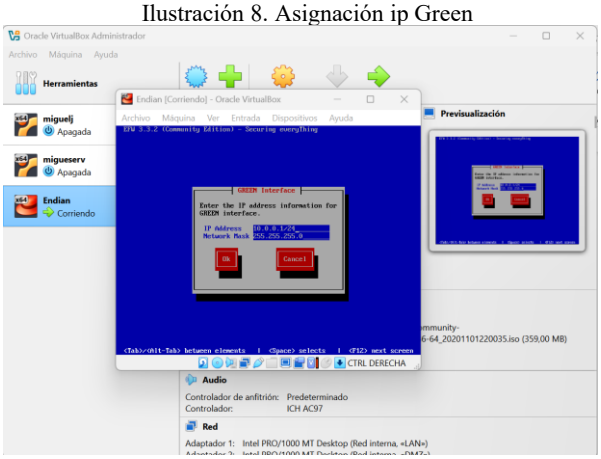
El sistema copia los archivos en unos 4-5 minutos.

2.1.4 Configuración de red – Asignación de zonas

Esta es la parte más importante y donde realmente empieza la magia de Endian:

La asignamos como GREEN: 10.0.0.1

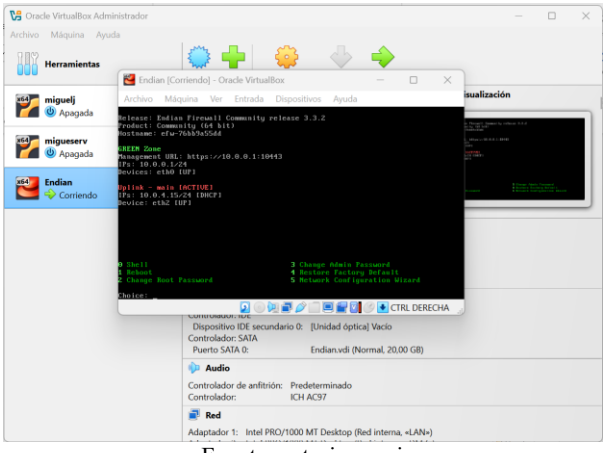
Ilustración 8. Asignación ip Green



Fuente: autoria propia

Luego de esto, el sistema se encarga de finalizar la instalacion para luego abrir en Endian.

Ilustracion 9. Asignaciones ip zona green y red



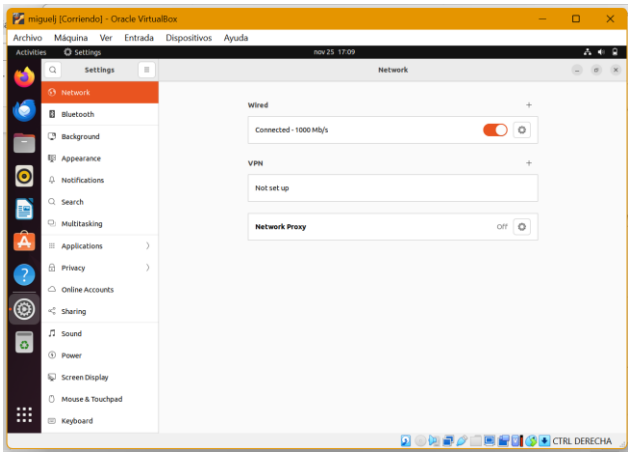
Fuente: autoria propia

Donde en la imagen anterior podemos ver y verificar que se asigno correctamente la ip para la zona verde y que de igual manera para la zona roja virtual box asigno una ip.

2.1.5 Configuración destokp

luego de estos pasos vamos a la maquina virtual a la cual vamos a usar para la zona verde, que en mi caso voy a usar el Ubuntu destokp, se realiza la configuración de la ip para que coincida con la asignada em Endian.

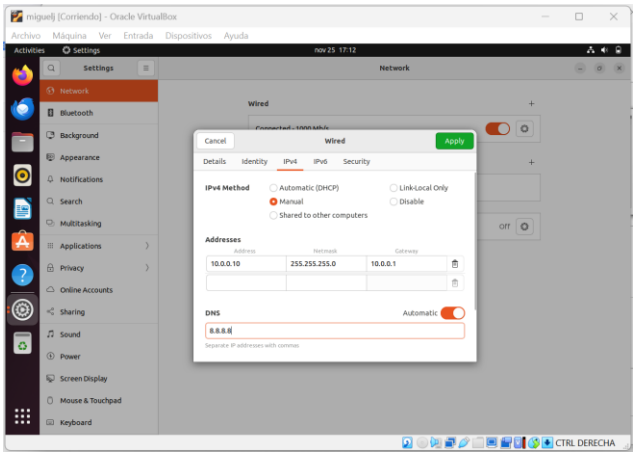
Ilustración 10. Configuraciones de Ubuntu



Fuente: autoria propia

Seguidamente realizamos la respectiva asigancion de la ip en ubuntu destokp.

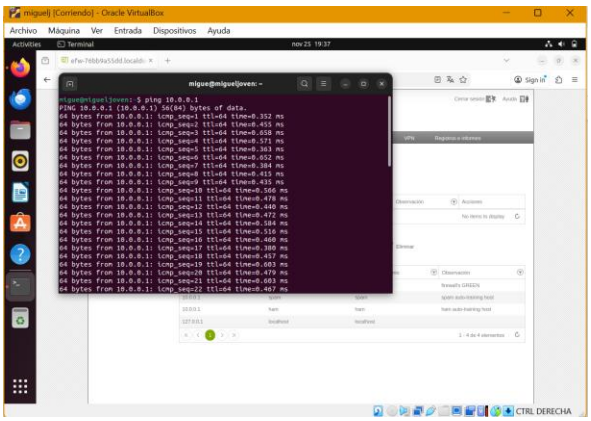
Ilustracion 11. Configuracion ip ubuntu



Fuente: autoria propia

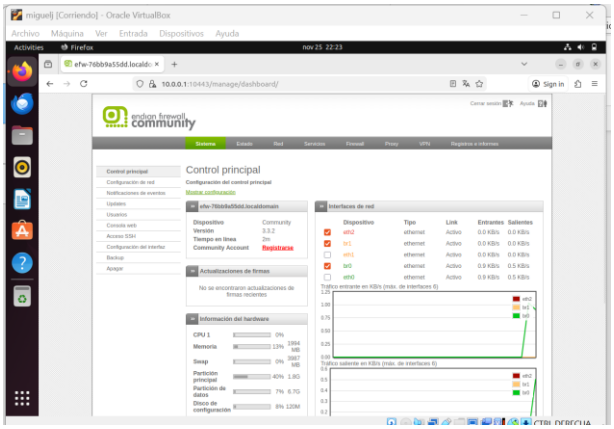
Y verificamos e ingresamos a la pagina web de endian a través del destokp para asi realizar la configuración de la zona naranja.

Ilustración 12. Ping desde Ubuntu destokp



Fuente: autoría propia

Ilustración 13. Consola administración Endian



Fuente: autoría propia

3. Conclusiones.

Antes de este trabajo, la mayoría de nosotros configurábamos servidores con una sola interfaz y "abriendo puertos" directamente. Después de implementar las zonas Verde, Naranja y Roja en Endian, comprendimos que la seguridad no empieza por la regla más restrictiva posible, sino por la arquitectura correcta. Tener claro qué servicios van en DMZ, cuáles nunca salen a Internet y cuáles necesitan acceso controlado desde afuera nos hizo repensar todas las topologías que habíamos hecho antes. Esa mentalidad de "segmentar primero, conectar después" es probablemente la lección más valiosa que nos llevamos.

El mayor cambio de mentalidad que me dejó este trabajo es que la seguridad no empieza por bloquear puertos al azar, sino por segmentar bien la red desde el principio. Antes abría el puerto 80 o 443 directamente en cualquier servidor y listo. Hoy entiendo que ningún servicio crítico debería estar nunca en zona Roja y que la DMZ (naranja) existe por una razón. Esa forma de pensar en "colores" antes de tocar cualquier regla me parece la lección más útil que me llevo para cualquier proyecto futuro, sea con Endian, pfSense o incluso con un simple servidor Ubuntu.

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] Jay LaCroix. (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

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