



# Avance del Trabajo Práctico Final

Topic	Trabajo Práctico Final de Ciberseguridad:
Module	IT - Cibersecurity
Teacher,-s	Chrystian Ruiz Diaz
Student,-s	Tobías Emanuel González Vera
Career,-s	Ingeniería en Tecnologías de la Información Empresarial
Date	@July 9, 2024
Wochentage	Dienstag
Deadline	@July 11, 2024
Status	Sended
Attached files	<u><a href="#">Unidad_90_GuiaTrabajoPracticoFinal.pdf</a></u>

---

Objetivo

Introducción

Marco Teórico

Conceptos clave

Firewall

Virtual Machines (VM)

Redes Virtuales (Virtual Networks)

Segmentación de Red (Network Segmentation)

Protocolos de Comunicación (Communication Protocols)

**Gestión de Políticas de Seguridad (Security Policy Management):**

Intrusion Detection System (IDS)

NAT (Network Address Translation)

**DHCP (Dynamic Host Configuration Protocol):**

**Proxy Server:**

**DNS (Domain Name System):**

Zonas de la estructura

Zona Naranja

Zona Verde

Zona Azul

Herramientas a utilizar

**VMware Workstation**

**Kali Linux**

**Servidor Web Vulnerable**

**Endian Firewall Community**

**Windows 7 Ultimate x64**

Conexiones de Red

VMnet0 - Bridged:

VMnet1 - Host Only:

VMnet8 - NAT:

VMnet3-7, 9:

Implementación práctica

Proceso de implementación

**Paso 1: Preparación del Entorno**

**Paso 2: Configuración de la Red Virtual**

**Paso 3: Instalación y Configuración de Endian Firewall**

Pings

Funcionamiento en forma independiente de las cuatro máquinas virtuales

Acceso a internet desde los navegadores con permisos (servidor web + zona verde)

---

---

# **Objetivo**

Implementar una seguridad perimetral utilizando el firewall "Open Source" Endian Firewall Community (EFW) para proteger una red con tres zonas:

- Zona Naranja: Servidor web accesible desde Internet.
- Zona Verde: Zona segura (interna).
- Zona Azul: Conexiones de personas/empresas externas.

## **Introducción**

La seguridad de redes es esencial para proteger la integridad, confidencialidad y disponibilidad de los datos en cualquier organización. Este proyecto tiene como finalidad la implementación de un firewall perimetral utilizando Endian Firewall Community para segmentar la red en tres zonas distintas, ofreciendo diferentes niveles de seguridad y acceso.

## **Marco Teórico**

### **Conceptos clave**

#### **Firewall**

Un firewall es una solución de seguridad informática que se utiliza para controlar y monitorear el tráfico de red entrante y saliente basado en reglas de seguridad predeterminadas. Su principal objetivo es proteger las redes internas de accesos no autorizados, ataques y amenazas provenientes del exterior. Los firewalls pueden ser tanto hardware como software, y sus funcionalidades incluyen filtrado de paquetes, inspección de estado, y control de aplicaciones. Además, ayudan a prevenir ataques como el acceso no autorizado, malware, y otras amenazas cibernéticas, asegurando así la integridad, confidencialidad y disponibilidad de la información.

#### **Virtual Machines (VM)**

Las máquinas virtuales (VM) son entornos de computación virtualizados que emulan un sistema informático completo, permitiendo ejecutar múltiples sistemas operativos en una sola máquina física. Estas VMs funcionan mediante hipervisores, que gestionan y asignan los recursos del hardware físico a las máquinas virtuales. Las VMs son ampliamente utilizadas en desarrollo, pruebas, educación, y despliegues en producción debido a su flexibilidad, capacidad de aislamiento, y eficiencia en la utilización de recursos. Facilitan la simulación de diferentes entornos operativos y la implementación de redes virtuales complejas para propósitos educativos y de prueba.

## **Redes Virtuales (Virtual Networks)**

Las redes virtuales permiten la creación de subredes dentro de un entorno de virtualización. Cada red virtual puede ser configurada con diferentes políticas de seguridad y acceso, permitiendo la segmentación del tráfico y la simulación de redes complejas. En este proyecto, las redes virtuales serán fundamentales para establecer las zonas Naranja, Verde y Azul, y para controlar cómo se comunican las máquinas virtuales entre sí.

## **Segmentación de Red (Network Segmentation)**

La segmentación de red es la práctica de dividir una red en múltiples segmentos más pequeños o subredes, cada uno con sus propias políticas de seguridad y reglas de acceso. Esto mejora la seguridad al limitar la propagación de amenazas y facilita la gestión del tráfico. En el proyecto, la segmentación se implementará mediante las zonas de Endian Firewall para aislar y proteger diferentes partes de la red.

## **Protocolos de Comunicación (Communication Protocols)**

Los protocolos de comunicación son reglas y estándares que permiten a los dispositivos en una red intercambiar información. Protocolos como HTTP, HTTPS, y ICMP serán esenciales en este proyecto para probar la conectividad, la navegación web, y la capacidad de ping entre las diferentes zonas y máquinas virtuales. La configuración correcta de estos protocolos asegurará la funcionalidad y la seguridad de la red.

## **Gestión de Políticas de Seguridad (Security Policy Management):**

La gestión de políticas de seguridad implica la definición, implementación y monitoreo de reglas y procedimientos que aseguran la protección de la red y

los datos. Esto incluye el control de acceso, la configuración de firewalls, y la supervisión del cumplimiento de las políticas. En este proyecto, la gestión de políticas de seguridad será crucial para establecer y mantener las reglas que regulan el tráfico entre las diferentes zonas y para proteger los activos de la red contra amenazas internas y externas.

## **Intrusion Detection System (IDS)**

Un sistema de detección de intrusos (IDS) monitorea el tráfico de la red en busca de actividades sospechosas y posibles amenazas. Puede alertar a los administradores de red sobre ataques en curso o comportamientos inusuales. En el contexto de este proyecto, un IDS podría ser implementado en la zona Verde para detectar y responder a intentos de intrusión desde la zona Azul (donde se encuentra el servidor web vulnerable) o desde la red externa.

## **NAT (Network Address Translation)**

NAT es una técnica utilizada para modificar las direcciones IP en los paquetes de datos que pasan a través de un router o firewall. Permite que múltiples dispositivos en una red privada comparten una única dirección IP pública para acceder a internet. En este proyecto, NAT será crucial para permitir que las máquinas virtuales de las zonas internas accedan a recursos externos, manteniendo las direcciones IP privadas ocultas de la red pública.

## **DHCP (Dynamic Host Configuration Protocol):**

DHCP es un protocolo de red que permite a los dispositivos obtener automáticamente una dirección IP y otros parámetros de configuración de red, como la puerta de enlace predeterminada y los servidores DNS. En este proyecto, DHCP puede ser utilizado para simplificar la gestión de direcciones IP dentro de las diferentes zonas de la red, asegurando que cada dispositivo obtenga una configuración de red adecuada sin intervención manual.

## **Proxy Server:**

Un proxy server actúa como intermediario entre los clientes y los servidores web. Puede utilizarse para mejorar la seguridad, el rendimiento y la privacidad de la red. En tu proyecto, un servidor proxy puede ser implementado para controlar y monitorear el tráfico de internet, aplicar políticas de acceso y caché de contenido para mejorar la eficiencia de la red.

## **DNS (Domain Name System):**

DNS es un sistema que traduce nombres de dominio legibles por humanos (como [www.example.com](http://www.example.com)) en direcciones IP numéricas que las computadoras utilizan para comunicarse entre sí. En este proyecto, la configuración y gestión del DNS será crucial para asegurar que todos los dispositivos y servicios en la red puedan ser fácilmente accesibles mediante nombres de dominio, facilitando la administración y operación de la red.

## Zonas de la estructura

### Zona Naranja

- **Descripción:** La Zona Naranja en una estructura de red con Endian Firewall es típicamente la red que está conectada a Internet.
- **Funcionalidad:** Esta zona se utiliza para la conexión directa con la red externa, es decir, el acceso a Internet. Los dispositivos en esta zona son considerados externos.
- **Papel en el trabajo:** En este trabajo, la Zona Naranja se utilizará para conectar el Endian Firewall a Internet, permitiendo que las VMs accedan a servicios externos y que se realicen pruebas de acceso a recursos en línea.

### Zona Verde

- **Descripción:** La Zona Verde es la red interna segura donde residen los dispositivos y servidores de la red local.
- **Funcionalidad:** Esta zona está destinada a la red local interna (LAN), que debe estar protegida del acceso directo desde Internet.
- **Papel en el trabajo:** En este proyecto, la Zona Verde albergará las VMs que simulan la red interna, como Kali Linux y Windows 7, proporcionando un entorno seguro para el desarrollo y pruebas internas.

### Zona Azul

- **Descripción:** La Zona Azul es una red DMZ (zona desmilitarizada) donde se ubican los servicios que necesitan ser accesibles desde Internet pero que no deben tener acceso directo a la red interna.
- **Funcionalidad:** Utilizada para colocar servidores y servicios que deben ser accesibles desde la red externa, como servidores web, sin comprometer la seguridad de la red interna.

- **Papel en el trabajo:** En este trabajo, la Zona Azul se utilizará para alojar el servidor web vulnerable, permitiendo el acceso externo para pruebas de penetración y análisis de vulnerabilidades, manteniendo al mismo tiempo la red interna segura.

## Herramientas a utilizar

### VMware Workstation

VMWare Workstation es una herramienta de virtualización de escritorio que permite la creación, gestión y ejecución de múltiples máquinas virtuales en un solo sistema físico. Con VMWare Workstation, los usuarios pueden ejecutar diferentes sistemas operativos simultáneamente, facilitando el desarrollo, pruebas, y simulación de entornos complejos de red y software. Sus características avanzadas incluyen snapshots, que permiten capturar el estado de una VM en un momento específico, y networking configurables, que permiten la simulación de diversas topologías de red.

- **Papel en este trabajo:** VMware Workstation se utilizará como la plataforma de virtualización para crear y gestionar las máquinas virtuales necesarias para el proyecto. Permitirá la configuración de diferentes adaptadores de red para simular las distintas zonas (Naranja, Verde, Azul) y facilitará el aislamiento y la interacción de las VMs entre sí.

### Kali Linux

Kali Linux es una distribución de Linux basada en Debian, diseñada para la seguridad informática y el pentesting (pruebas de penetración). Incluye una amplia gama de herramientas preinstaladas para tareas como análisis de redes, pruebas de penetración, forense digital, y más. Kali Linux es utilizado por profesionales de seguridad y hackers éticos para identificar y mitigar vulnerabilidades en sistemas y redes. Su interfaz amigable y su conjunto de herramientas especializado lo hacen ideal para realizar auditorías de seguridad completas.

- **Papel en este trabajo:** Kali Linux se empleará como la máquina virtual en la Zona Verde para realizar pruebas de penetración y análisis de seguridad. Proporcionará las herramientas necesarias para evaluar las vulnerabilidades y la fortaleza de la configuración del Endian Firewall y otras VMs en la red.

## **Servidor Web Vulnerable**

Un servidor web vulnerable es una máquina configurada intencionalmente con debilidades de seguridad para fines educativos y de prueba. Este entorno permite a los estudiantes y profesionales de la seguridad practicar técnicas de hacking ético y pruebas de penetración en un entorno controlado. Los servidores web vulnerables se utilizan para simular escenarios de ataques reales, permitiendo a los usuarios identificar y explotar vulnerabilidades comunes, y aprender cómo proteger sistemas similares en entornos de producción.

- **Papel en este trabajo:** El servidor web vulnerable se ubicará en la Zona Azul para simular un entorno realista donde se puedan realizar pruebas de seguridad. Servirá como objetivo para los ataques de penetración desde Kali Linux y permitirá evaluar la efectividad de las reglas de firewall y las configuraciones de seguridad implementadas.

## **Endian Firewall Community**

Endian Firewall Community (EFW) es una solución de seguridad basada en Linux diseñada para convertir dispositivos de hardware en herramientas de Gestión Unificada de Amenazas (UTM). Este software de código abierto simplifica la protección de redes mediante la integración de funcionalidades como firewall, VPN, filtrado de contenidos, y detección de intrusiones en una única plataforma. EFW es ideal para pequeñas y medianas empresas que buscan una solución robusta y económica para proteger su infraestructura de red contra amenazas cibernéticas. La comunidad de Endian proporciona soporte y actualizaciones continuas, asegurando que el sistema esté siempre al día con las últimas amenazas y técnicas de defensa.

- **Papel en este trabajo:** Endian Firewall Community será el componente central de la configuración de seguridad de la red. Se utilizará para gestionar las conexiones entre las distintas zonas (Naranja, Verde, Azul) y para establecer y aplicar las reglas de acceso y seguridad que protegen la red interna y los servicios expuestos.

## **Windows 7 Ultimate x64**

Windows 7 Ultimate x64 es una versión de 64 bits del sistema operativo Windows 7, utilizada en entornos de prueba y desarrollo. Ejecutar Windows 7 en una máquina virtual permite a los usuarios experimentar con configuraciones de red, instalar software de prueba, y simular entornos de

usuario final sin afectar el sistema operativo principal. Esta VM es especialmente útil para realizar pruebas de compatibilidad y seguridad, así como para simular ataques y defensas en un entorno controlado.

- **Papel en este trabajo:** La máquina virtual con Windows 7 se ubicará en la Zona Verde para simular un entorno de usuario final típico. Permitirá realizar pruebas de acceso y navegación desde un sistema operativo de uso común, asegurando que las configuraciones de red y las reglas de seguridad permiten un uso funcional y seguro de los recursos de la red interna.

## Conexiones de Red

### VMnet0 - Bridged:

- **Descripción:** La configuración en modo "Bridged" conecta directamente la máquina virtual (VM) con la red física a la que está conectada la máquina host.
- **Funcionalidad:** Este modo permite que la VM tenga su propia dirección IP en la misma red que la máquina física, como si estuviera conectada directamente a la red física.
- **Uso:** Ideal para situaciones donde la VM necesita interactuar con otros dispositivos en la red física, como impresoras, servidores, o para ser accesible desde otros dispositivos en la misma red.

### VMnet1 - Host Only:

- **Descripción:** "Host Only" es una configuración de red donde la VM se conecta solo con el host y otras VMs en la misma configuración, sin acceso a Internet.
- **Funcionalidad:** Utiliza una interfaz virtual (VMnet1) creada por VMware, permitiendo la comunicación entre el host y las VMs en esta red aislada.
- **Uso:** Utilizado para entornos de prueba y desarrollo donde se necesita aislamiento de la red externa para simular redes privadas o para pruebas de seguridad sin riesgo de exposición.

### VMnet8 - NAT:

- **Descripción:** "NAT" (Network Address Translation) permite a las VMs compartir la dirección IP del host para acceder a Internet.
- **Funcionalidad:** Asigna direcciones IP dinámicas a las VMs, permitiéndoles salir a Internet utilizando la conexión del host, mientras mantiene las VMs ocultas detrás de la dirección IP del host.
- **Uso:** Ideal para situaciones donde las VMs necesitan acceso a Internet pero no requieren una dirección IP propia en la red física, proporcionando un nivel adicional de seguridad.

## VMnet3-7, 9:

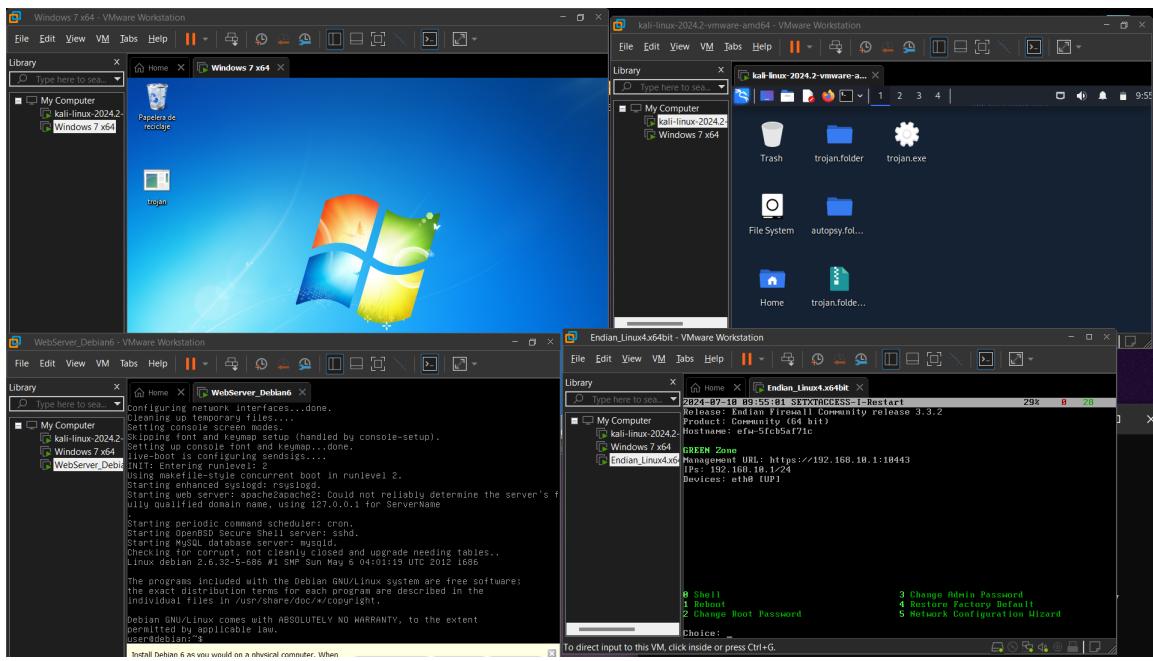
- **Descripción:** Estos son switches virtuales independientes que se pueden configurar para crear subredes entre múltiples VMs.
- **Funcionalidad:** Permiten la creación de redes privadas entre VMs, que pueden estar completamente aisladas de la red física y de otras redes virtuales.
- **Uso:** Utilizados para simular complejas topologías de red, realizar pruebas de múltiples segmentos de red, o para aislar ciertos grupos de VMs por motivos de seguridad o pruebas específicas.

# Implementación práctica

## Proceso de implementación

### Paso 1: Preparación del Entorno

- Descargar e instalar VMware Workstation.
- Crear y configurar las máquinas virtuales necesarias (Kali Linux, Windows 7, Endian Firewall, WebServer vulnerable).



## Paso 2: Configuración de la Red Virtual

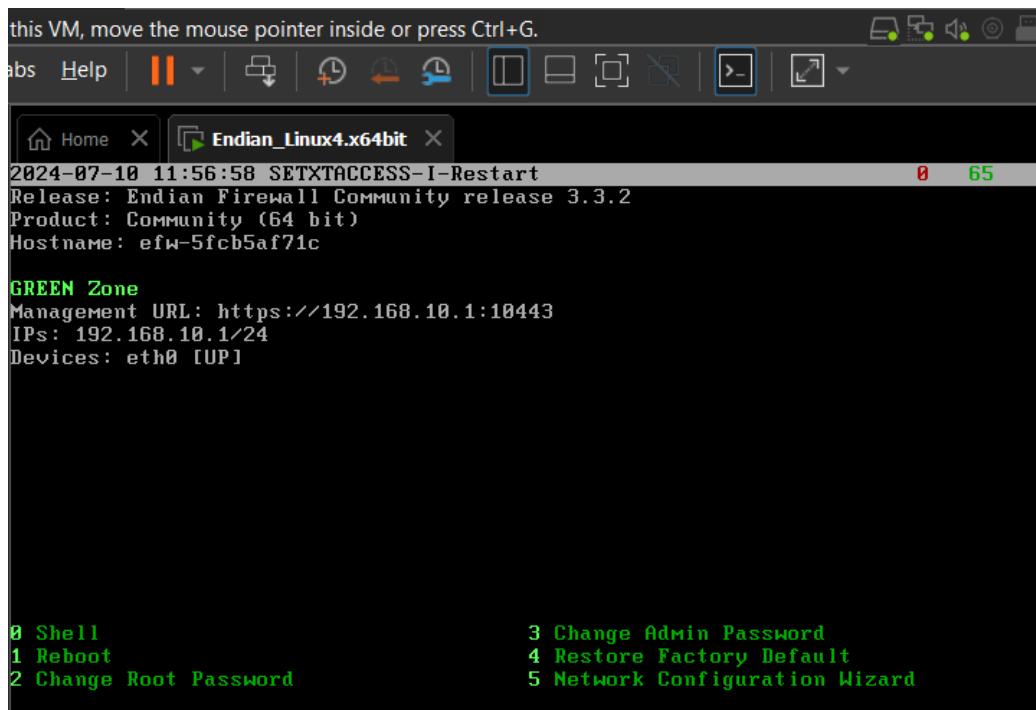
- Configurar las conexiones de red en VMware utilizando VMnet0, VMnet1, y VMnet8.
- Asegurar que las máquinas virtuales estén correctamente conectadas según las zonas (naranja, verde, azul).

## Paso 3: Instalación y Configuración de Endian Firewall

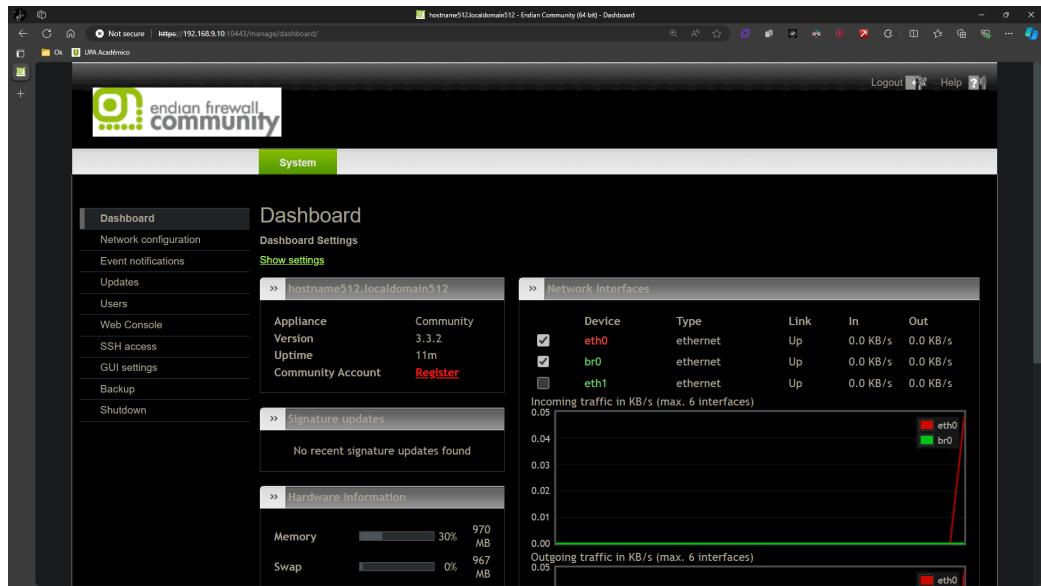
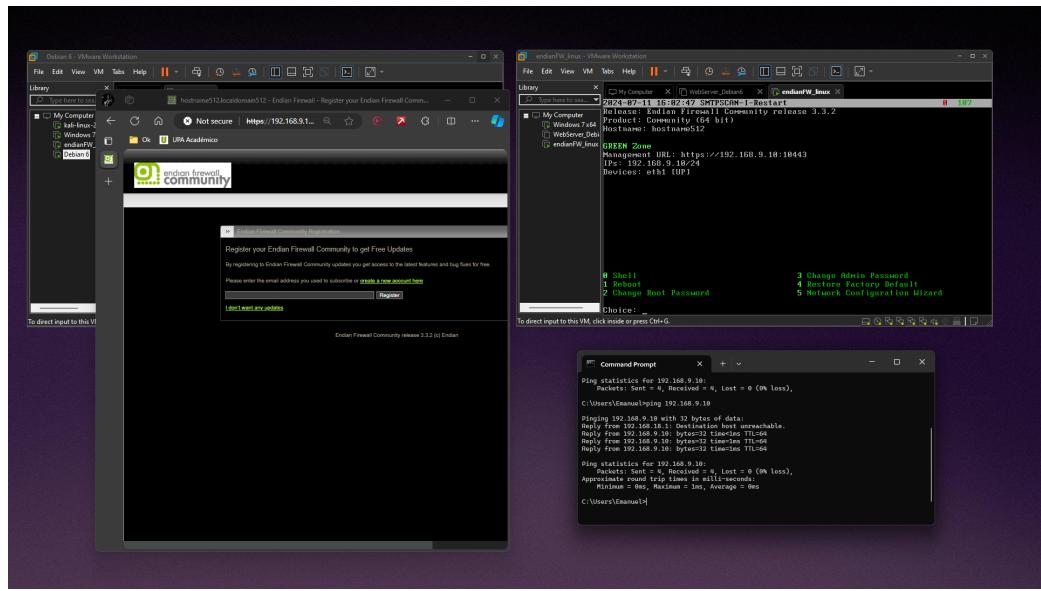
- Montar la VM de Endian Firewall.
  - Instalación:**
    - Descargar e instalar/montar la VM de Endian Firewall Community desde Endian.

The screenshot shows the Endian Firewall Community website. At the top, there's a navigation bar with links like 'Community', 'Overview', 'Features', 'Comparison', 'Download' (which is highlighted), and 'Get Help'. Below the navigation, there's a section for 'Endian Firewall Community' with a logo and a brief description: 'Free Open Source UTM Solution for Home use'. It mentions that Endian Firewall Community (EFW) is a turn-key network security software product dedicated to home users. There are three main product cards: 'Endian UTM' (IT Cybersecurity), 'Endian 4i' (OT Cybersecurity), and 'Endian Switchboard'. Each card has a brief description and a list of available solutions: Hardware Lösung, Virtuelle Lösung, and Software Lösung. Buttons for 'Weiterlesen' (Read more) are at the bottom of each card. A 'Free Download' button is located at the bottom left of the main content area.

## Sitio web de Endian para descargar el Endian Firewall Community

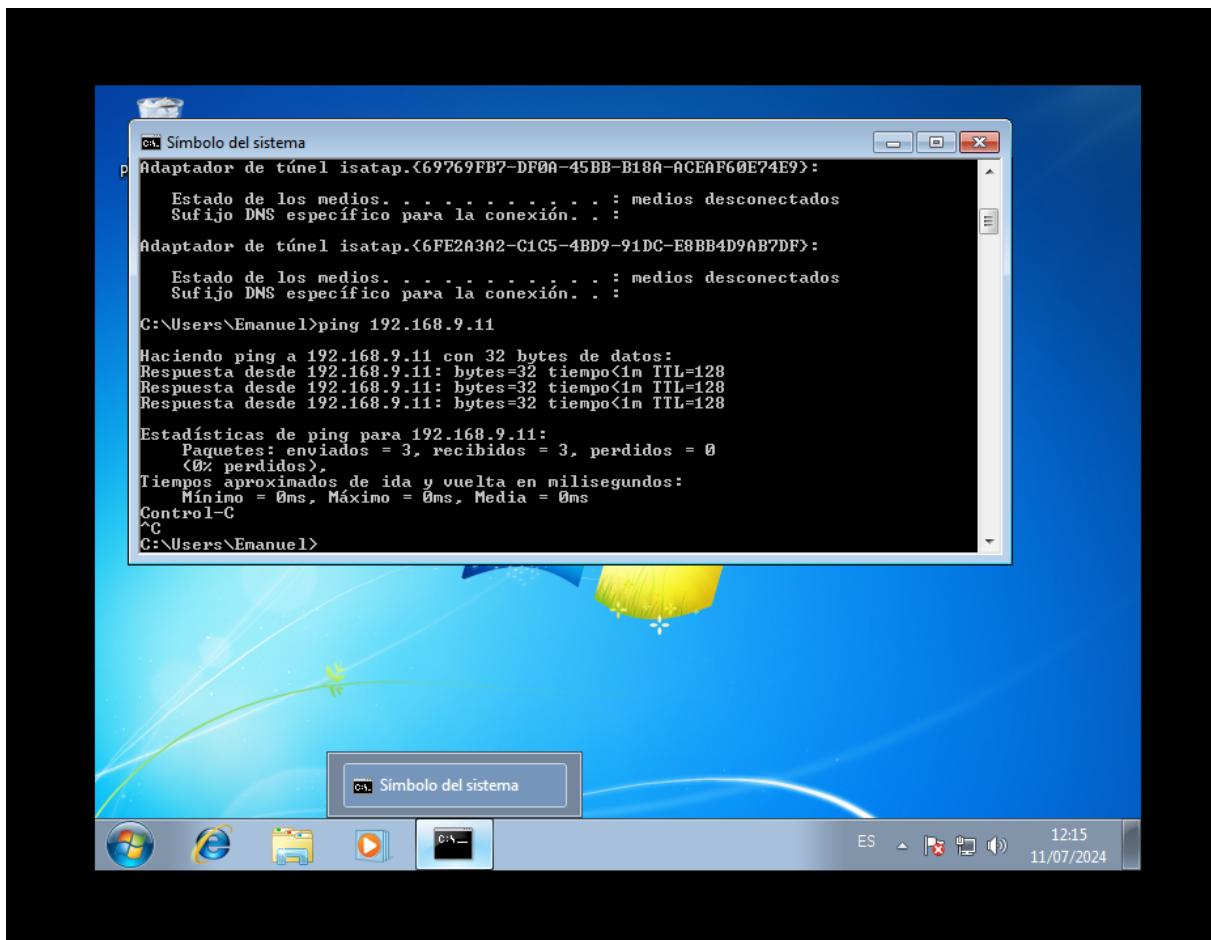


Endian instalado e inicialmente configurado



## Pings

Ping desde Windows 7



Ping desde Enbian

```
[hostname512]: ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=24.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=26.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=24.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=21.1 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=21.2 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=128 time=23.5 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5012ms
rtt min/avg/max/mdev = 21.126/23.440/26.452/1.836 ms
Interrupt
[hostname512]: ping 192.168.88.131
PING 192.168.88.131 (192.168.88.131) 56(84) bytes of data.
64 bytes from 192.168.88.131: icmp_seq=1 ttl=64 time=1.90 ms
64 bytes from 192.168.88.131: icmp_seq=2 ttl=64 time=1.43 ms
64 bytes from 192.168.88.131: icmp_seq=3 ttl=64 time=1.00 ms
64 bytes from 192.168.88.131: icmp_seq=4 ttl=64 time=0.732 ms
^C
--- 192.168.88.131 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.732/1.268/1.905/0.447 ms
Interrupt
[hostname512]:
```

To direct input to this VM, click inside or press Ctrl+G.

## Funcionamiento en forma independiente de las cuatro máquinas virtuales

Enbian Firewall a Envían Firewall

Ip: 192.168.9.10/24 (el .9 es por los últimos dígitos de mi número de documento "09")

```
Home X | endianFW_linux X

64 bytes from 8.8.8.8: icmp_seq=22 ttl=128 time=20.7 ms
64 bytes from 8.8.8.8: icmp_seq=23 ttl=128 time=21.3 ms
64 bytes from 8.8.8.8: icmp_seq=24 ttl=128 time=21.2 ms
64 bytes from 8.8.8.8: icmp_seq=25 ttl=128 time=23.4 ms
64 bytes from 8.8.8.8: icmp_seq=26 ttl=128 time=24.9 ms
64 bytes from 8.8.8.8: icmp_seq=27 ttl=128 time=21.4 ms

--- 8.8.8.8 ping statistics ---
27 packets transmitted, 27 received, 0% packet loss, time 26799ms
rtt min/avg/max/mdev = 20.679/21.669/24.986/0.887 ms
Interrupt
[hostname512]: ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=24.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=26.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=24.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=21.1 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=21.2 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=128 time=23.5 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5012ms
rtt min/avg/max/mdev = 21.126/23.440/26.452/1.836 ms
Interrupt
[hostname512]: _
```

Enbian Firewall a Kali Linux

Ip: 192.168.88.131

```
[hostname512]: ping 192.168.88.131
PING 192.168.88.131 (192.168.88.131) 56(84) bytes of data.
64 bytes from 192.168.88.131: icmp_seq=1 ttl=64 time=1.90 ms
64 bytes from 192.168.88.131: icmp_seq=2 ttl=64 time=1.43 ms
64 bytes from 192.168.88.131: icmp_seq=3 ttl=64 time=1.00 ms
64 bytes from 192.168.88.131: icmp_seq=4 ttl=64 time=0.732 ms
^C
--- 192.168.88.131 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.732/1.268/1.905/0.447 ms
Interrupt
[hostname512]: _
```

Enbian Firewall al Servidor web

Ip: 192.167.9.11

```
[hostname512]: ping 192.167.9.11
PING 192.167.9.11 (192.167.9.11) 56(84) bytes of data.
64 bytes from 192.167.9.11: icmp_seq=1 ttl=64 time=0.039 ms
64 bytes from 192.167.9.11: icmp_seq=2 ttl=64 time=0.098 ms
64 bytes from 192.167.9.11: icmp_seq=3 ttl=64 time=0.127 ms
^C
--- 192.167.9.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.039/0.088/0.127/0.036 ms
Interrupt
```

## Enbian Firewall a Windows 7

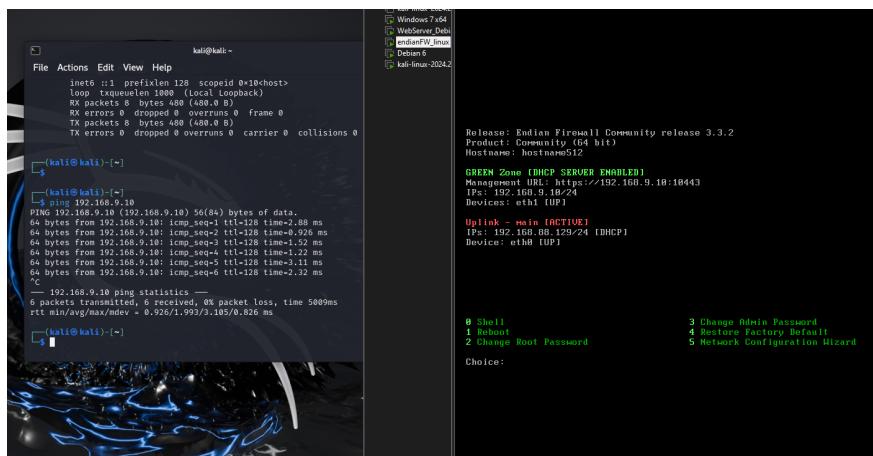
Ip: 192.168.9.11

```
Job 5655 on hostname512.localdomain512 at 22:15 on 2024-07-11
Type 'help' for help

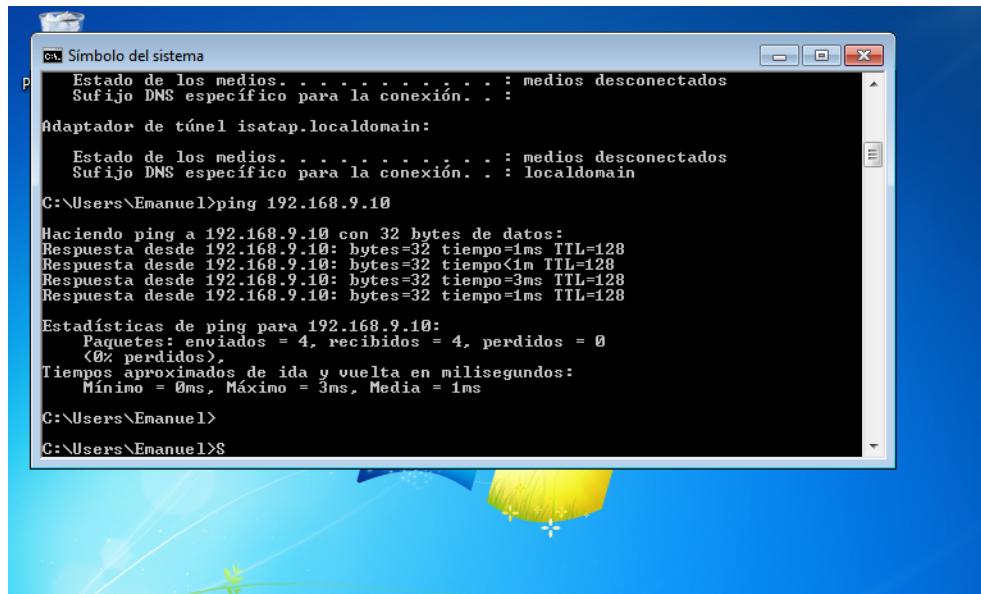
[hostname512]: ping 192.168.88.128
PING 192.168.88.128 (192.168.88.128) 56(84) bytes of data.
```

## De las máquinas virtuales a Endian Flrewall (Ip: 192.168.9.10)

- Kali Linux



- Windows 7

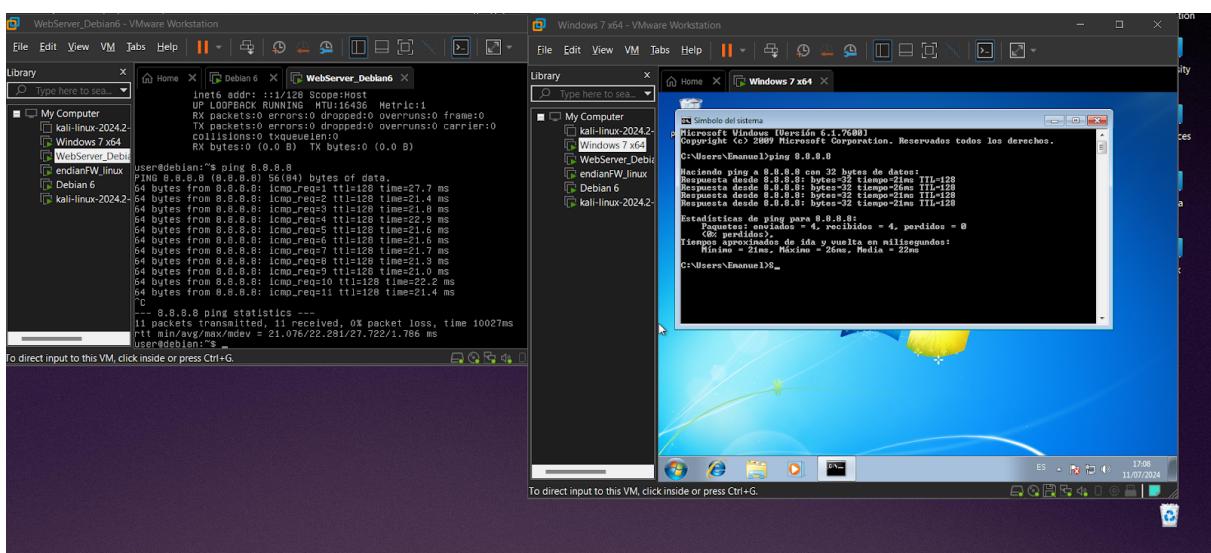
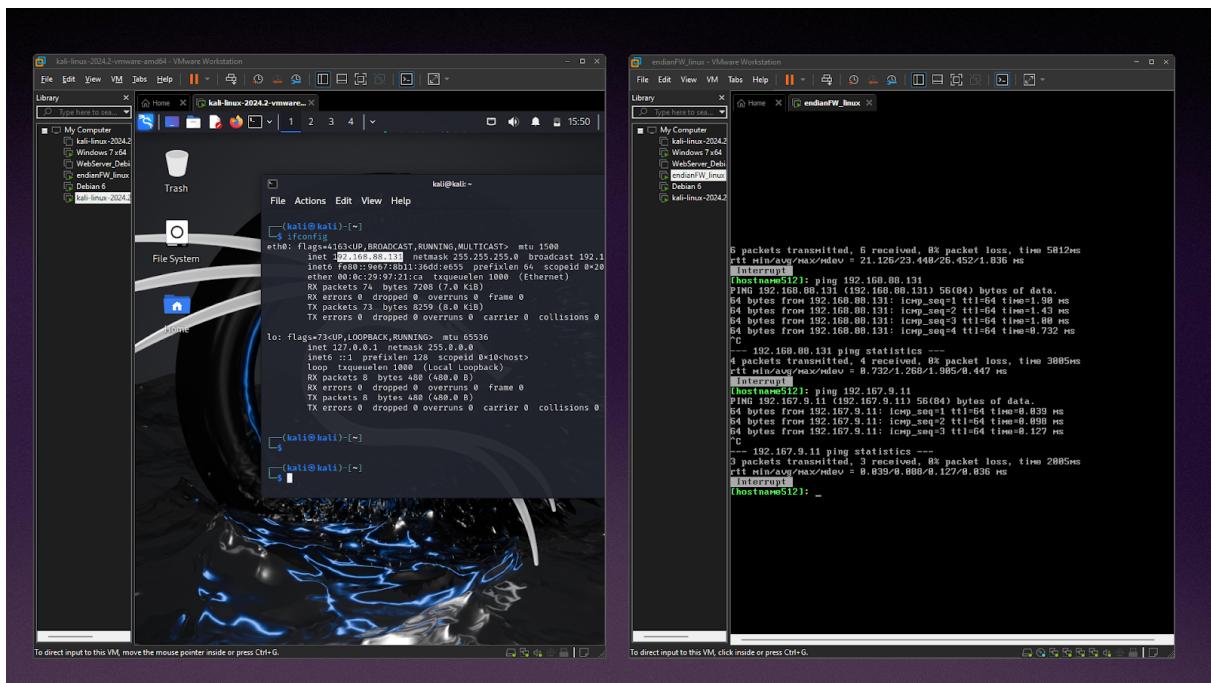


- Servidor Web

```

l
--- 8.8.8.8 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10027ms
rtt min/avg/max/mdev = 21.076/22.281/27.722/1.786 ms
User@debian:~$ ping 192.168.9.10
PING 192.168.9.10 (192.168.9.10) 56(84) bytes of data.
64 bytes from 192.168.9.10: icmp_req=1 ttl=128 time=6.22 ms
64 bytes from 192.168.9.10: icmp_req=2 ttl=128 time=0.806 ms
64 bytes from 192.168.9.10: icmp_req=3 ttl=128 time=1.82 ms
64 bytes from 192.168.9.10: icmp_req=4 ttl=128 time=1.27 ms
64 bytes from 192.168.9.10: icmp_req=5 ttl=128 time=1.56 ms
64 bytes from 192.168.9.10: icmp_req=6 ttl=128 time=1.05 ms
64 bytes from 192.168.9.10: icmp_req=7 ttl=128 time=1.42 ms
64 bytes from 192.168.9.10: icmp_req=8 ttl=128 time=0.935 ms
64 bytes from 192.168.9.10: icmp_req=9 ttl=128 time=0.909 ms
^C
--- 192.168.9.10 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8020ms
rtt min/avg/max/mdev = 0.806/1.779/6.225/1.603 ms
User@debian:~$
```

Las 4 máquinas virtuales trabajando en simultáneo



## Acceso a internet desde los navegadores con permisos (servidor web + zona verde)

Servidor web

```

inet6 addr: ::1/128 Scope:Host
  UP LOOPBACK RUNNING MTU:16436 Metric:1
  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:0
  RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

user@debian:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_req=1 ttl=128 time=27.7 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=128 time=21.4 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=128 time=21.8 ms
64 bytes from 8.8.8.8: icmp_req=4 ttl=128 time=22.9 ms
64 bytes from 8.8.8.8: icmp_req=5 ttl=128 time=21.6 ms
64 bytes from 8.8.8.8: icmp_req=6 ttl=128 time=21.6 ms
64 bytes from 8.8.8.8: icmp_req=7 ttl=128 time=21.7 ms
64 bytes from 8.8.8.8: icmp_req=8 ttl=128 time=21.3 ms
64 bytes from 8.8.8.8: icmp_req=9 ttl=128 time=21.0 ms
64 bytes from 8.8.8.8: icmp_req=10 ttl=128 time=22.2 ms
64 bytes from 8.8.8.8: icmp_req=11 ttl=128 time=21.4 ms
^C
--- 8.8.8.8 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10027ms
rtt min/avg/max/mdev = 21.076/22.281/27.722/1.786 ms
user@debian:~$
```

## Windows 7 (zona verde)

