



**Facultad de Ciencias Empresariales**  
**Ingeniería en Tecnologías de la Información Empresarial**

## **Seguridad TICs**

# **Trabajo Práctico Final: Implementación de Endian Firewall Community**

**Tobías Emanuel González Vera**

**San Lorenzo, 2024**

# Tabla de Contenidos

<b>Introducción</b>	<b>4</b>
<b>Objetivo</b>	<b>5</b>
<b>Marco Teórico</b>	<b>5</b>
Conceptos clave	5
Firewall	5
Virtual Machines (VM)	5
Redes Virtuales (Virtual Networks)	5
Segmentación de Red (Network Segmentation)	6
Protocolos de Comunicación (Communication Protocols)	6
Gestión de Políticas de Seguridad (Security Policy Management):	6
Intrusion Detection System (IDS)	6
NAT (Network Address Translation)	6
DHCP (Dynamic Host Configuration Protocol):	6
Proxy Server:	7
DNS (Domain Name System):	7
Zonas de la estructura	7
Zona Naranja	7
Zona Verde	8
Zona Azul	8
Herramientas a utilizar	9
VMware Workstation	9
Kali Linux	9
Servidor Web Vulnerable	9
Endian Firewall Community	10
Windows 7 Ultimate x64	10
Interfaces de Red y Zonas	10
Interfaces	10
Conexión NAT (VMnet8 - NAT)	11
<b>Implementación del Sistema</b>	<b>13</b>
Estructura	13
Endian Firewall Community	13
Zona Naranja: DMZ (Demilitarized Zone)	14
Zona Verde: LAN (Red Interna)	14
Zona Azul: Usuarios Externos	14
Conexión y Flujo de Tráfico	14
Documentación del funcionamiento	15
Funcionamiento en forma independiente de las cuatro máquinas virtuales	15
Acceso a internet desde los navegadores con permisos (servidor web + zona verde)	19
Arquitectura con las direcciones de red utilizadas	20

Reglas Configuradas	21
Pruebas de Funcionamiento	23
<b>Conclusiones</b>	<b>32</b>
<b>Referencias</b>	<b>33</b>

# Introducción

La seguridad en Tecnologías de la Información y Comunicación (TICs) es esencial en un mundo donde la interconectividad y la dependencia de sistemas digitales son omnipresentes. Las amenazas ciberneticas evolucionan rápidamente, desafiando constantemente las medidas de protección de organizaciones y usuarios. En este contexto, los cortafuegos (firewalls) y los sistemas de detección de intrusiones (IDS) son vitales para mantener la integridad, confidencialidad y disponibilidad de la información.

Este trabajo se centra en la implementación del Endian Firewall Community en una red virtualizada, configurada con VMware Workstation. La red consta de tres zonas: Zona Verde (Red Interna), Zona Naranja (DMZ) y Zona Azul (Red de Invitados), cada una con una función específica y configuraciones de seguridad adaptadas a sus necesidades. Además, se integrarán herramientas como Kali Linux y un servidor web vulnerable para simular y analizar ataques, permitiendo evaluar la eficacia de las configuraciones de seguridad implementadas.

El objetivo principal es demostrar cómo un firewall bien configurado puede proteger una red compleja, identificando y mitigando posibles vulnerabilidades. A través de este proyecto, se busca proporcionar una comprensión práctica y detallada de las técnicas de seguridad en redes, destacando la importancia de una configuración adecuada y la vigilancia constante en un entorno de ciberseguridad.

# 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.

# 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 ciberneticas, 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**

**Interfaz:** eth2

**Dirección IP:** 192.167.9.11/24

**VMnet:** VMnet10

**Tipo:** Host-Only

**Sistema:** Servidor Web

#### **Descripción:**

- **Funcionalidad:** La Zona Naranja está destinada al servidor web vulnerable, utilizado para pruebas de penetración y evaluación de seguridad.
- **Configuración:** Asigna la interfaz eth2 del Endian Firewall con la dirección IP 192.167.9.11/24. Conéctalo a VMnet10.
- **Objetivo en el Proyecto:** Simular un entorno donde se pueden realizar ataques y análisis de vulnerabilidades en el servidor web, sin comprometer la seguridad de otras zonas de la red.

- **Uso en el Proyecto:** Realizar pruebas de seguridad y vulnerabilidades en el servidor web vulnerable.

## Zona Verde

**Interfaz:** eth1

**Dirección IP:** 192.168.9.10/24

**VMnet:** VMnet4

**Tipo:** Host-Only

**Sistema:** Windows 7

### Descripción:

- **Funcionalidad:** La Zona Verde se utiliza para la red interna segura, donde se encuentra la máquina con Windows 7.
- **Configuración:** Asigna la interfaz eth1 del Endian Firewall con la dirección IP 192.168.9.10/24. Conéctalo a VMnet4.
- **Objetivo en el Proyecto:** Proveer un entorno seguro para el sistema Windows 7 que permitirá monitorear el tráfico y realizar pruebas de comunicación segura.
- **Uso en el Proyecto:** Evaluar y asegurar la comunicación interna en la red.

## Zona Azul

**Interfaz:** eth3

**Dirección IP:** 192.169.9.15/24

**VMnet:** VMnet2

**Tipo:** Host-Only

**Sistema:** Kali Linux

### Descripción:

- **Funcionalidad:** La Zona Azul se dedica a las herramientas de prueba y análisis de seguridad, representadas por la máquina Kali Linux.
- **Configuración:** Asigna la interfaz eth3 del Endian Firewall con la dirección IP 192.169.9.15/24. Conéctalo a VMnet2.
- **Objetivo en el Proyecto:** Proporcionar un entorno seguro y aislado para llevar a cabo pruebas de penetración y análisis de seguridad utilizando Kali Linux.

- **Uso en el Proyecto:** Realizar pruebas de seguridad y ataques simulados desde Kali Linux hacia el servidor web y otras máquinas virtuales para evaluar la seguridad de la red.

## 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.

## Interfaces de Red y Zonas

### Interfaces

#### 1. eth0 - Zona Roja (VMnet0 - Bridged):

- **Descripción:** La interfaz `eth0` está configurada en modo "Bridged", lo que conecta directamente la VM con la red física del host.

- **Funcionalidad:** Permite que la VM obtenga una dirección IP en la misma red que la máquina host, facilitando la interacción con otros dispositivos en la red física.
  - **Uso:** Esta configuración es ideal para situaciones donde la VM necesita acceso directo a la red externa, como Internet.
2. **eth1 - Zona Verde (VMnet4 - Host-Only):**
- **Dirección IP:** 192.168.9.10/24
  - **Descripción:** La interfaz `eth1` se conecta a la red VMnet4 en modo "Host-Only".
  - **Funcionalidad:** Permite la comunicación entre la VM y el host, así como con otras VMs en la misma red aislada.
  - **Sistema:** Windows 7
  - **Uso:** Utilizada para pruebas y desarrollo en un entorno aislado sin acceso a la red externa.
3. **eth2 - Zona Naranja (VMnet10 - Host-Only):**
- **Dirección IP:** 192.167.9.11/24
  - **Descripción:** La interfaz `eth2` se conecta a la red VMnet10 en modo "Host-Only".
  - **Funcionalidad:** Permite la comunicación entre la VM y el host, así como con otras VMs en la misma red aislada.
  - **Sistema:** Servidor Web
  - **Uso:** Ideal para configurar un servidor web en un entorno controlado y seguro para pruebas de seguridad y desarrollo.
4. **eth3 - Zona Azul (VMnet2 - Host-Only):**
- **Dirección IP:** 192.169.9.15/24
  - **Descripción:** La interfaz `eth3` se conecta a la red VMnet2 en modo "Host-Only".
  - **Funcionalidad:** Permite la comunicación entre la VM y el host, así como con otras VMs en la misma red aislada.
  - **Sistema:** Kali Linux
  - **Uso:** Utilizada para pruebas de penetración y análisis de seguridad en un entorno aislado.

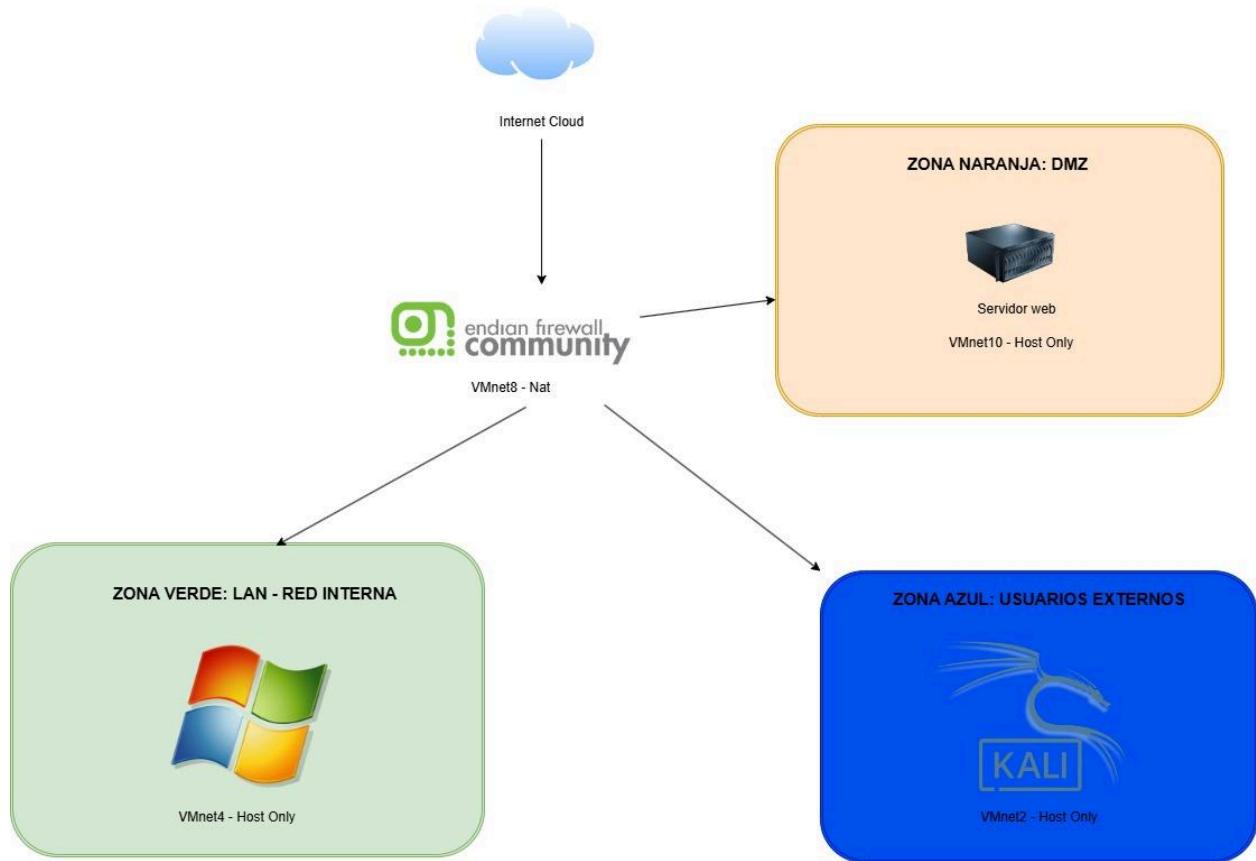
## Conexión NAT (VMnet8 - NAT)

- **Descripción:** VMnet8 está configurada en modo "NAT" (Network Address Translation).
- **Funcionalidad:** Permite que las VMs comparten la dirección IP del host para acceder a Internet, asignando direcciones IP dinámicas a las VMs.
- **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.
- **Sistema:** Endian Firewall
- **Nota:** El Endian Firewall utiliza esta configuración para gestionar y asegurar el tráfico de red de las otras VMs.

Esta configuración asegura que cada zona y tipo de conexión esté correctamente asignada y gestionada para cumplir con los requisitos de seguridad y funcionalidad en un entorno de red virtual.

# Implementación del Sistema

## Estructura



Esta estructura de red ilustra la implementación de Endian Firewall Community en una red segmentada en tres zonas distintas: Zona Naranja (DMZ), Zona Verde (LAN), y Zona Azul (Usuarios Externos). Cada una de estas zonas tiene un propósito específico y está configurada de manera que maximiza la seguridad y la eficiencia de la red. A continuación, se describe cada componente de la estructura en detalle:

### Endian Firewall Community

El Endian Firewall Community actúa como el núcleo de la red, gestionando el tráfico y aplicando políticas de seguridad entre las diferentes zonas. Está configurado para funcionar con VMnet8 en modo NAT, lo que permite la conexión a la Internet externa y la redirección de tráfico a las distintas zonas internas. El Endian Firewall se encarga de filtrar el tráfico, prevenir ataques y proporcionar una capa adicional de seguridad.

## **Zona Naranja: DMZ (Demilitarized Zone)**

La Zona Naranja es conocida como la DMZ y está diseñada para alojar servicios que deben ser accesibles desde la red externa (Internet), pero que requieren protección adicional. En este caso, la DMZ alberga un servidor web, que se encuentra en una red VMnet10 configurada como "Host Only". Esta configuración permite que el servidor web sea accesible tanto desde la red externa a través de políticas específicas del firewall, como desde la red interna, manteniendo una capa de aislamiento para prevenir accesos no autorizados directos a la LAN.

## **Zona Verde: LAN (Red Interna)**

La Zona Verde representa la LAN o red interna de la organización. En esta zona se encuentran los dispositivos internos, como las estaciones de trabajo y servidores que no necesitan ser accesibles desde el exterior. En el diagrama, esta zona contiene una máquina con Windows, que está conectada mediante VMnet4 configurada como "Host Only". Esta configuración asegura que los dispositivos en la LAN están protegidos y solo accesibles desde la DMZ y la zona de usuarios externos a través de las políticas de firewall bien definidas.

## **Zona Azul: Usuarios Externos**

La Zona Azul está destinada a usuarios externos que necesitan acceder a recursos internos de forma controlada. En esta implementación, se muestra un dispositivo con Kali Linux, el cual está conectado mediante VMnet2 configurada como "Host Only". Esta zona permite a los usuarios externos o dispositivos de prueba acceder a ciertos recursos de la red interna bajo políticas de seguridad estrictas, evitando comprometer la seguridad de la LAN.

## **Conexión y Flujo de Tráfico**

El tráfico entre estas zonas está controlado por el Endian Firewall, que aplica reglas específicas para permitir o denegar el acceso según la zona de origen y destino. Por ejemplo, el tráfico desde la Zona Naranja (servidor web) hacia la Zona Verde (LAN) puede estar restringido a ciertos tipos de servicios o protocolos. Asimismo, el acceso desde la Zona Azul (usuarios externos) a la Zona Verde (LAN) está controlado para asegurar que solo usuarios autorizados y bajo condiciones específicas puedan interactuar con los recursos internos.

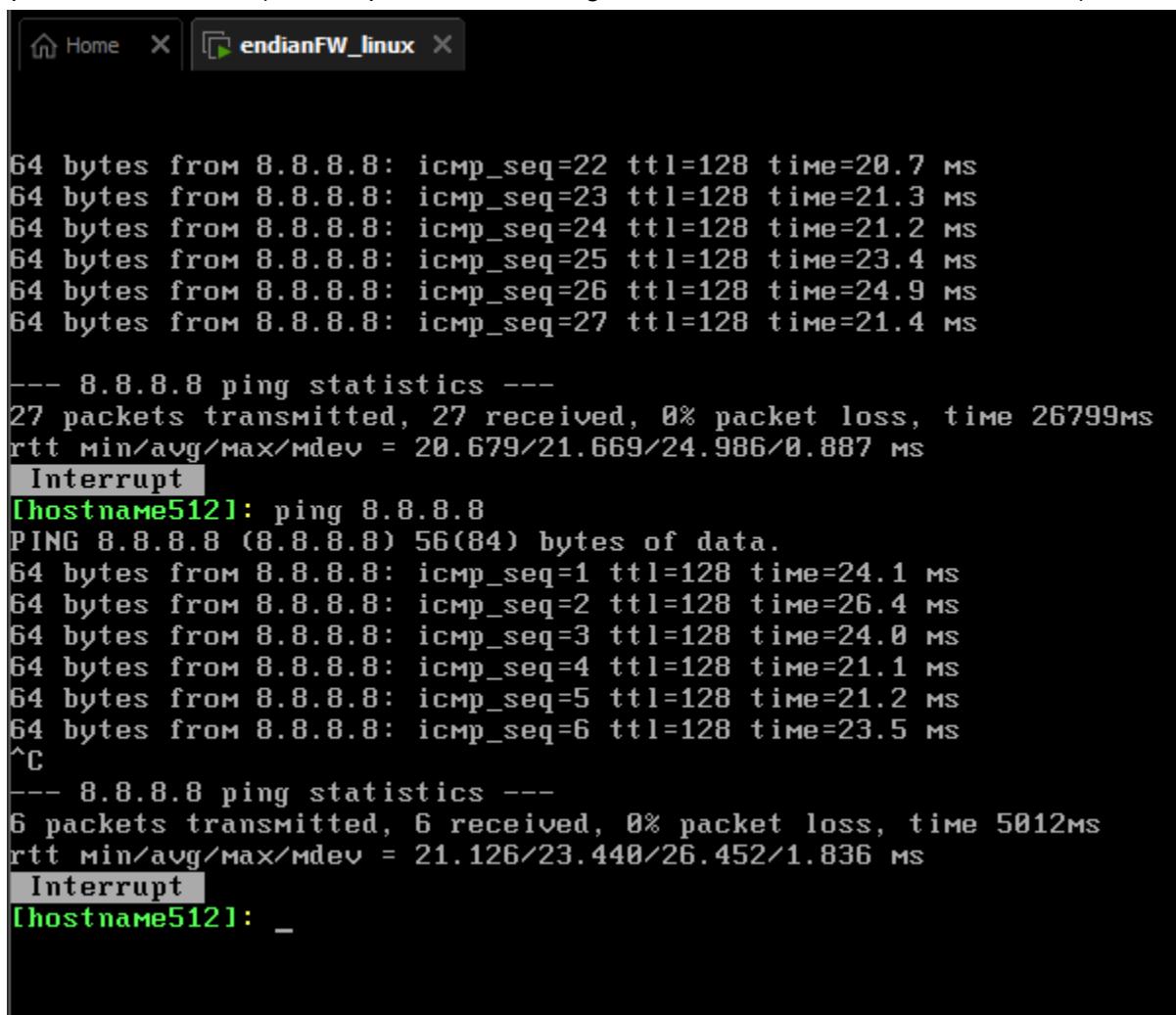
Esta configuración proporciona una estructura de red segmentada y segura, que no solo protege los activos internos de la organización sino que también asegura que los servicios que necesitan ser accesibles desde el exterior están adecuadamente aislados y protegidos.

## Documentación del funcionamiento

Funcionamiento en forma independiente de las cuatro máquinas virtuales

Enbian Firewall a Envian Firewall

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



```
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
```

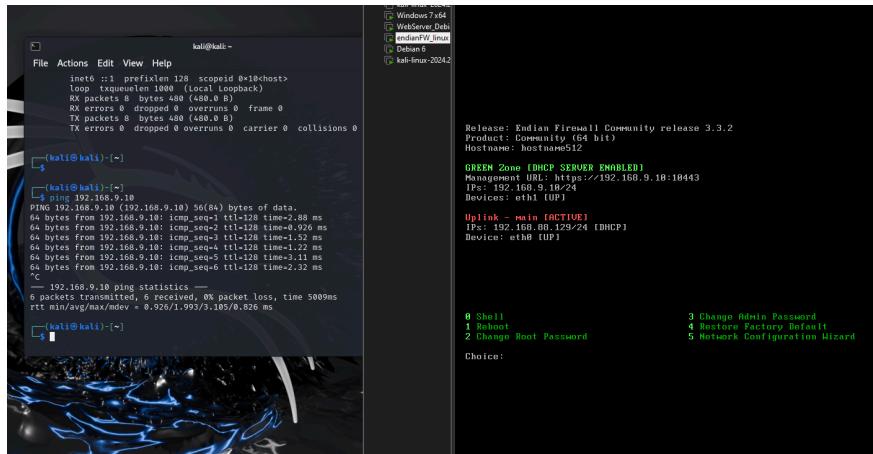
Enbian Firewall a Windows 7  
Ip: 192.168.9.11

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

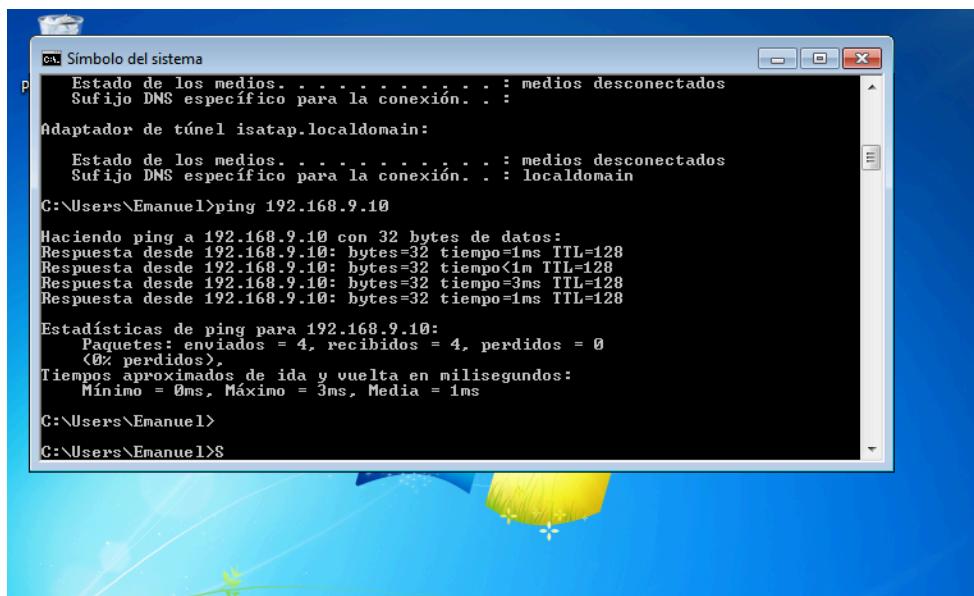
[hostname512]: ping 192.168.88.128
PING 192.168.88.128 (192.168.88.128) 56(84) bytes of data.
```

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

- Kali Linux



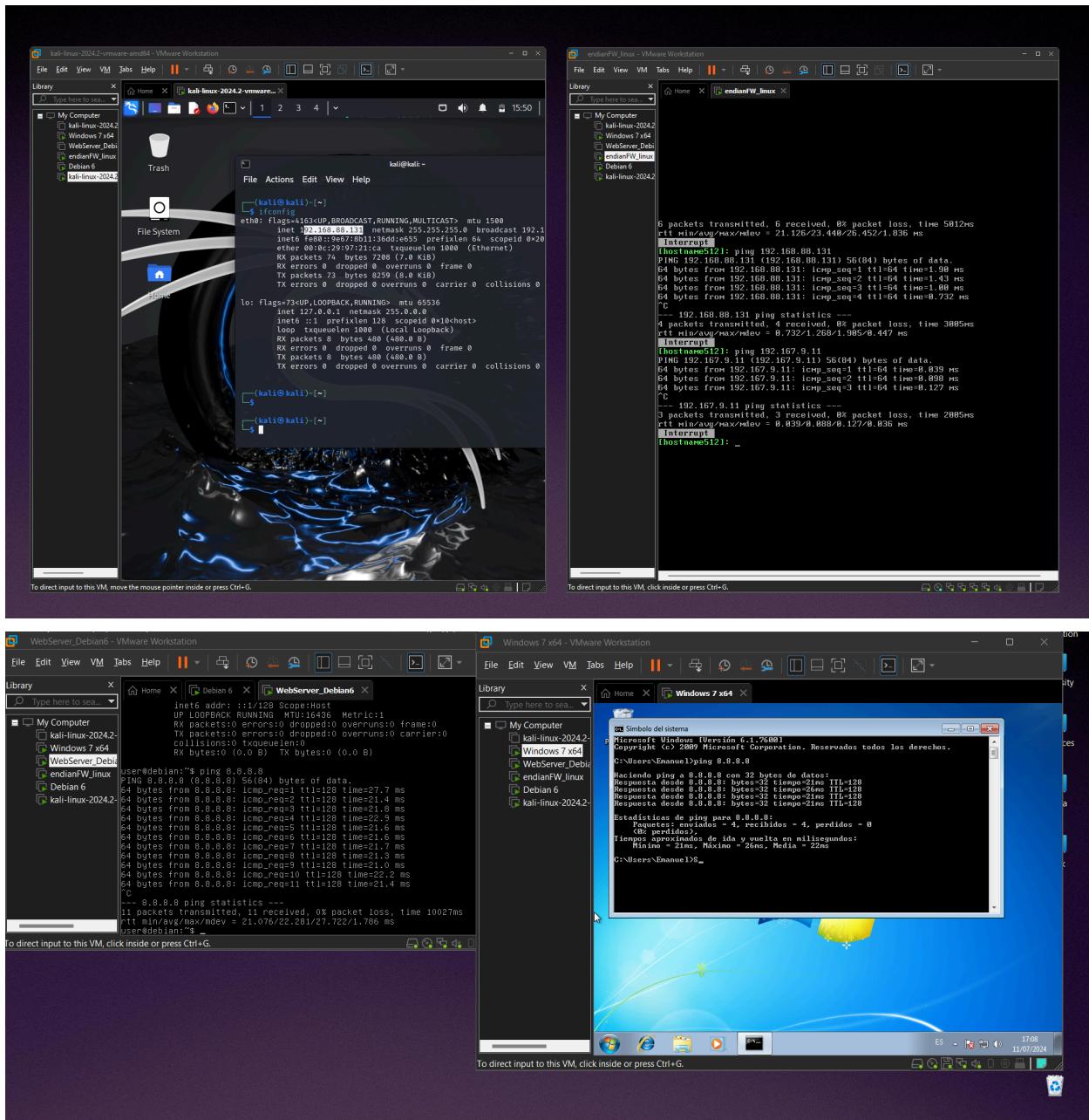
- Windows 7



- 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



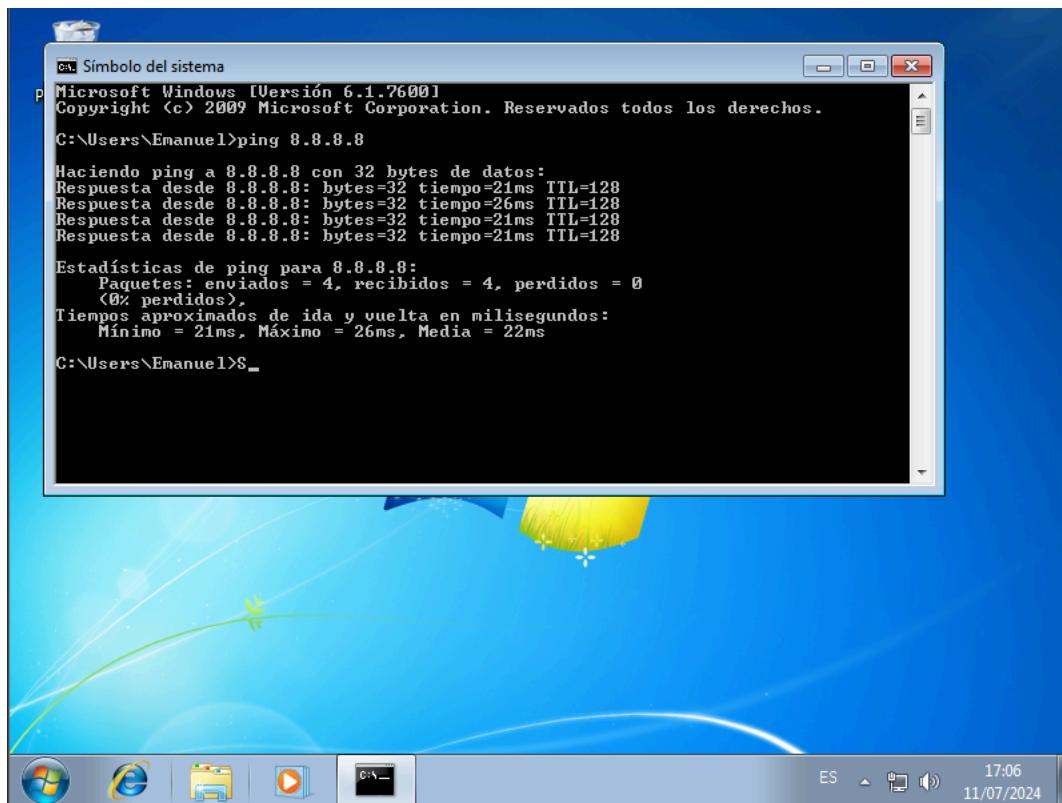
## Acceso a internet desde los navegadores con permisos (servidor web + zona verde)

### 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)

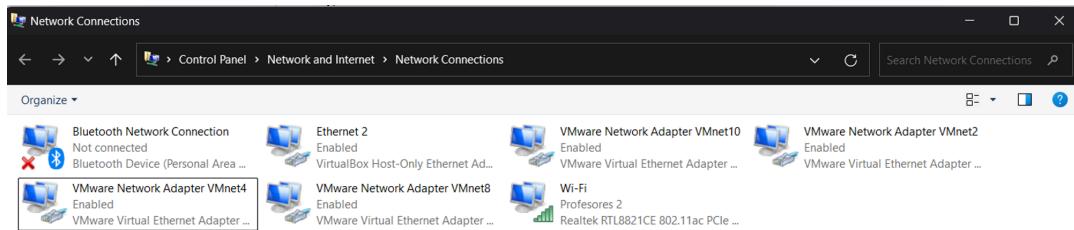
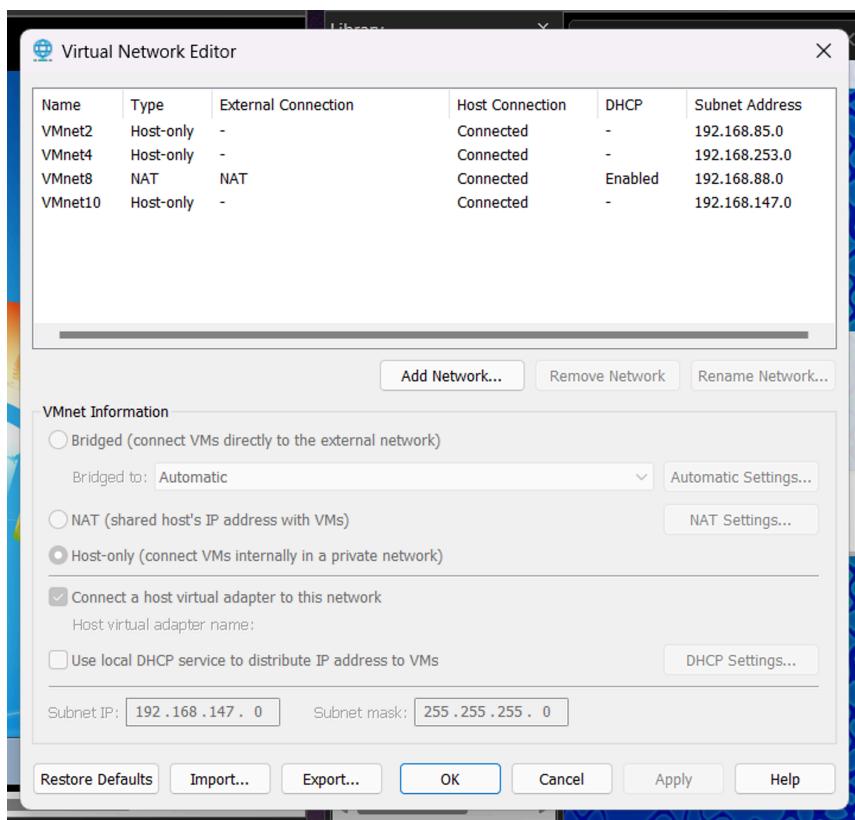
user@debian:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_req=1 ttl=128 time=27.7 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=128 time=21.4 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=128 time=21.8 ms
64 bytes from 8.8.8.8: icmp_req=4 ttl=128 time=22.9 ms
64 bytes 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)



## Arquitectura con las direcciones de red utilizadas

Interfaz	Dirección IP	Zona	VMnet	Tipo	Sistema
eth0		Roja			
eth1	192.168.9.10/24	Verde	VMnet4	Host-Only	Windows 7
eth2	192.167.9.11/24	Naranja	VMnet10	Host-Only	Servidor Web
eth3	192.169.9.15/24	Azul	VMnet2	Host-Only	Kali Linux
			VMnet8	NAT	Endian Firewall



# Reglas Configuradas

## Port forwarding / Destination NAT

Port forwarding / NAT

Outgoing traffic  
Inter-Zone traffic  
VPN traffic  
System access  
Firewall Diagrams

### Port forwarding / Destination NAT

Port forwarding / Destination NAT    Source NAT - Incoming routed traffic

Add a new Port forwarding / Destination NAT rule

#	Incoming IP	Service	Policy	Translate to	Remark	Actions
---	-------------	---------	--------	--------------	--------	---------

Legend:  Enabled (click to disable)  Disabled (click to enable) Edit Remove

Show system rules >>

Status: Connected: main (0d 0h 49m 14s) Uptime: 22:22:24 up 49 min, 1 user, load average: 0.00, 0.00, 0.00  
Endian Firewall Community release 3.3.2 (c) Endian

## Outgoing firewall configuration

### Outgoing firewall configuration

Current rules

Add a new firewall rule

#	Source	Destination	Service	Policy	Remark	Actions
1	GREEN	RED	TCP/80			
2	BLUE	RED	TCP/80			
3	ORANGE	RED	TCP/80			
4	GREEN	RED	TCP/443			
5	BLUE	RED	TCP/443			
6	ORANGE	RED	TCP/443			
7	ORANGE	RED	ICMP/8 ICMP/30			
8	BLUE	RED	ICMP/8 ICMP/30			
9	GREEN	RED	ICMP/8 ICMP/30			

Legend  Enabled (click to disable)  Disabled (click to enable) Edit Remove

Show system rules >>

## Inter-Zone firewall configuration

>> Current rules

[+ Add a new inter-zone firewall rule](#)

#	Source	Destination	Service	Policy	Remark	Actions
1	GREEN	GREEN	<ANY>	→		
2	GREEN	BLUE	<ANY>	→		
3	GREEN	ORANGE	<ANY>	→		
4	BLUE	BLUE	<ANY>	→		
5	BLUE	GREEN	<ANY>	→		
6	BLUE	ORANGE	<ANY>	→		
7	ORANGE	ORANGE	<ANY>	→		

Legend: Enabled (click to disable) Disabled (click to enable) Edit Remove

Show rules of system services >>

## VPN firewall configuration

Port forwarding / NAT

Outgoing traffic

Inter-Zone traffic

**VPN traffic**

System access

Firewall Diagrams

## VPN firewall configuration

>> VPN Firewall Settings

Enable VPN firewall

Use the switch above to enable the VPN firewall.  
The VPN firewall gives the ability to globally DENY VPN traffic and explicitly configure VPN firewall rules.

Status: Connected: main (0d 0h 51m 54s) Uptime: 22:25:04 up 52 min, 1 user, load average: 0.00, 0.00, 0.00  
Endian Firewall Community release 3.3.2 (c) Endian

## System access configuration

Port forwarding / NAT

Outgoing traffic

Inter-Zone traffic

**System access**

Firewall Diagrams

## System access configuration

>> Current rules

Log packets

[+ Add a new system access rule](#)

#	Source address	Source interface	Service	Policy	Remark	Actions
1	<ANY>		TCP/22 TCP/80 TCP/10443	→		

Legend: Enabled (click to disable) Disabled (click to enable) Edit Remove

Show rules of system services >>

Status: Connected: main (0d 0h 52m 14s) Uptime: 22:25:24 up 52 min, 1 user, load average: 0.07, 0.02, 0.00  
Endian Firewall Community release 3.3.2 (c) Endian

## Pruebas de Funcionamiento

Conforme indicado en el ítem “Funcionamiento del Sistema”

Configurar las reglas para darle acceso a internet (ICMP y navegación libre http, https, etc) a todas las zonas (Blue, Orange, Green).

The screenshot shows a firewall rule configuration interface with the following details:

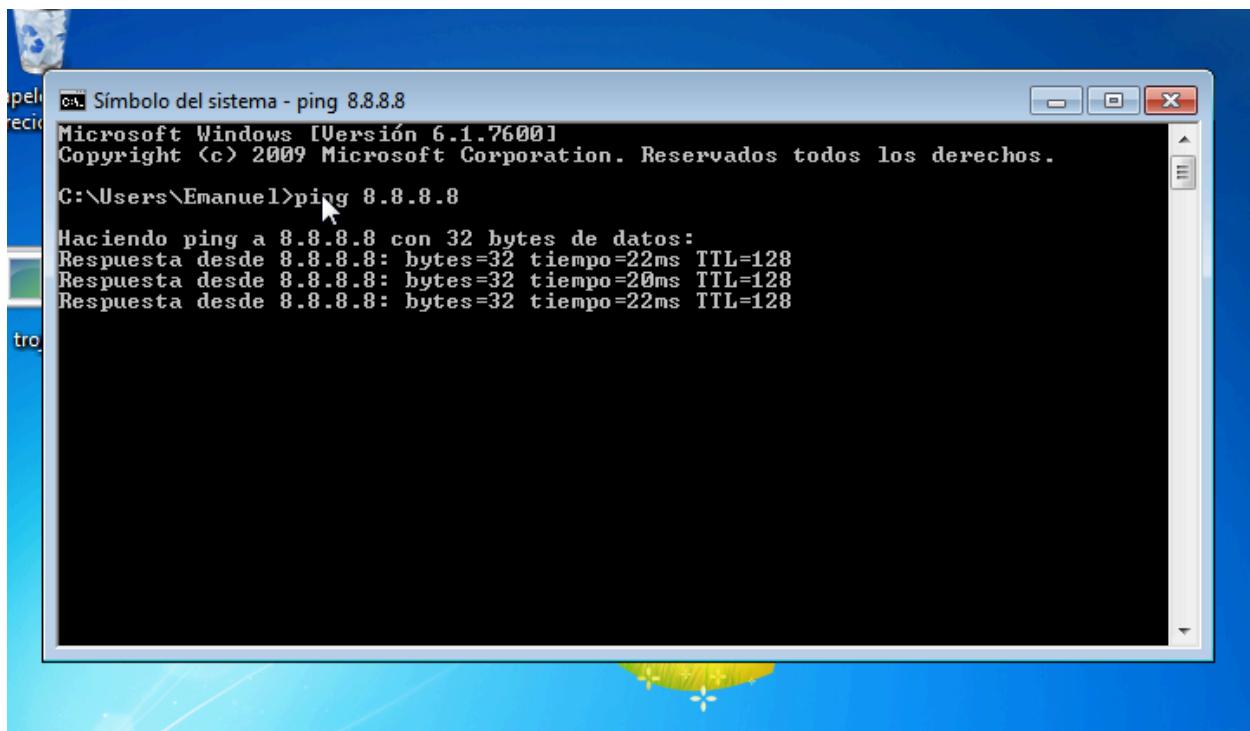
#	Source	Destination	Service	Policy	Remark	Actions
1	GREEN	RED	TCP/80	Allow		
2	BLUE	RED	TCP/80	Allow		
3	ORANGE	RED	TCP/80	Allow		
4	GREEN	RED	TCP/443	Allow		
5	BLUE	RED	TCP/443	Allow		
6	ORANGE	RED	TCP/443	Allow		

Legend: Enabled (click to disable) Disabled (click to enable) Edit Remove

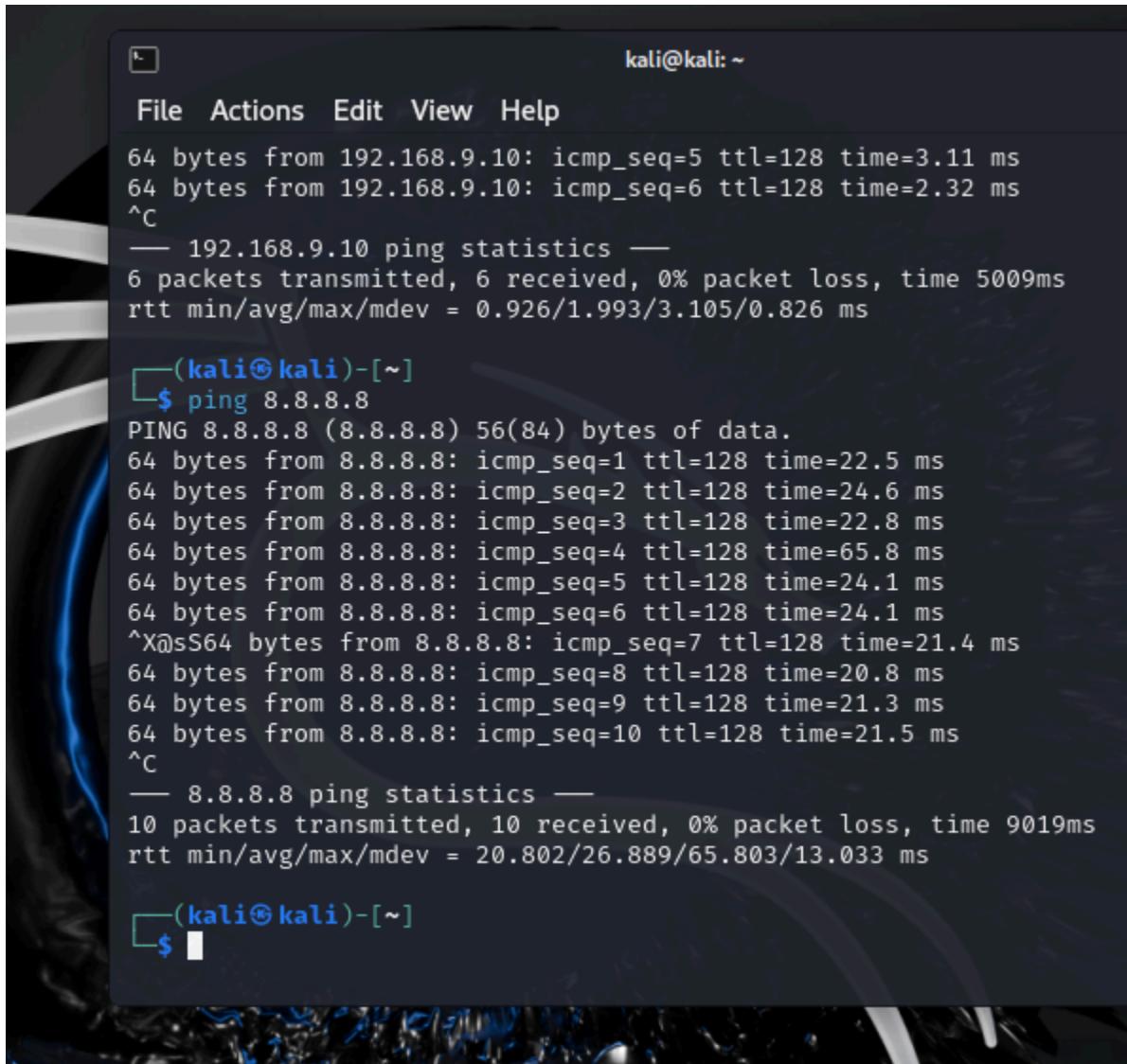
Show system rules >>

Pruebas de ping 8.8.8.8, tracert 8.8.8.8 (windows) o traceroute 8.8.8.8 (linux) y navegación http, https.

ping Windows 7



ping Linux



```
kali㉿kali: ~
File Actions Edit View Help
64 bytes from 192.168.9.10: icmp_seq=5 ttl=128 time=3.11 ms
64 bytes from 192.168.9.10: icmp_seq=6 ttl=128 time=2.32 ms
^C
— 192.168.9.10 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 0.926/1.993/3.105/0.826 ms

└─(kali㉿kali)-[~]
└$ 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=22.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=24.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=22.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=65.8 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=24.1 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=128 time=24.1 ms
^X@ssS64 bytes from 8.8.8.8: icmp_seq=7 ttl=128 time=21.4 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=128 time=20.8 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=128 time=21.3 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=128 time=21.5 ms
^C
— 8.8.8.8 ping statistics —
10 packets transmitted, 10 received, 0% packet loss, time 9019ms
rtt min/avg/max/mdev = 20.802/26.889/65.803/13.033 ms

└─(kali㉿kali)-[~]
└$
```

ping Debian

```
Home X | Debian 6 X | WebServer_Debian6 X
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=0.985 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:~$ 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=24.8 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=128 time=21.8 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=128 time=22.3 ms
64 bytes from 8.8.8.8: icmp_req=4 ttl=128 time=31.4 ms
64 bytes from 8.8.8.8: icmp_req=5 ttl=128 time=23.0 ms
64 bytes from 8.8.8.8: icmp_req=6 ttl=128 time=21.2 ms
64 bytes from 8.8.8.8: icmp_req=7 ttl=128 time=21.6 ms
64 bytes from 8.8.8.8: icmp_req=8 ttl=128 time=21.7 ms
64 bytes from 8.8.8.8: icmp_req=9 ttl=128 time=23.2 ms
64 bytes from 8.8.8.8: icmp_req=10 ttl=128 time=25.3 ms
64 bytes from 8.8.8.8: icmp_req=11 ttl=128 time=21.7 ms
64 bytes from 8.8.8.8: icmp_req=12 ttl=128 time=21.0 ms
64 bytes from 8.8.8.8: icmp_req=13 ttl=128 time=22.2 ms

```

Click inside or press Ctrl+G.

Tracert Windows

```
Símbolo del sistema - tracert 8.8.8.8
Microsoft Windows [Versión 6.1.7600]
Copyright © 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Emanuel>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=22ms TTL=128
Respuesta desde 8.8.8.8: bytes=32 tiempo=20ms TTL=128
Respuesta desde 8.8.8.8: bytes=32 tiempo=22ms TTL=128
Respuesta desde 8.8.8.8: bytes=32 tiempo=21ms TTL=128

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 20ms, Máximo = 22ms, Media = 21ms

C:\Users\Emanuel>tracert 8.8.8.8

Traza a la dirección dns.google [8.8.8.8]
sobre un máximo de 30 saltos:

 1 <1 ms <1 ms <1 ms
```

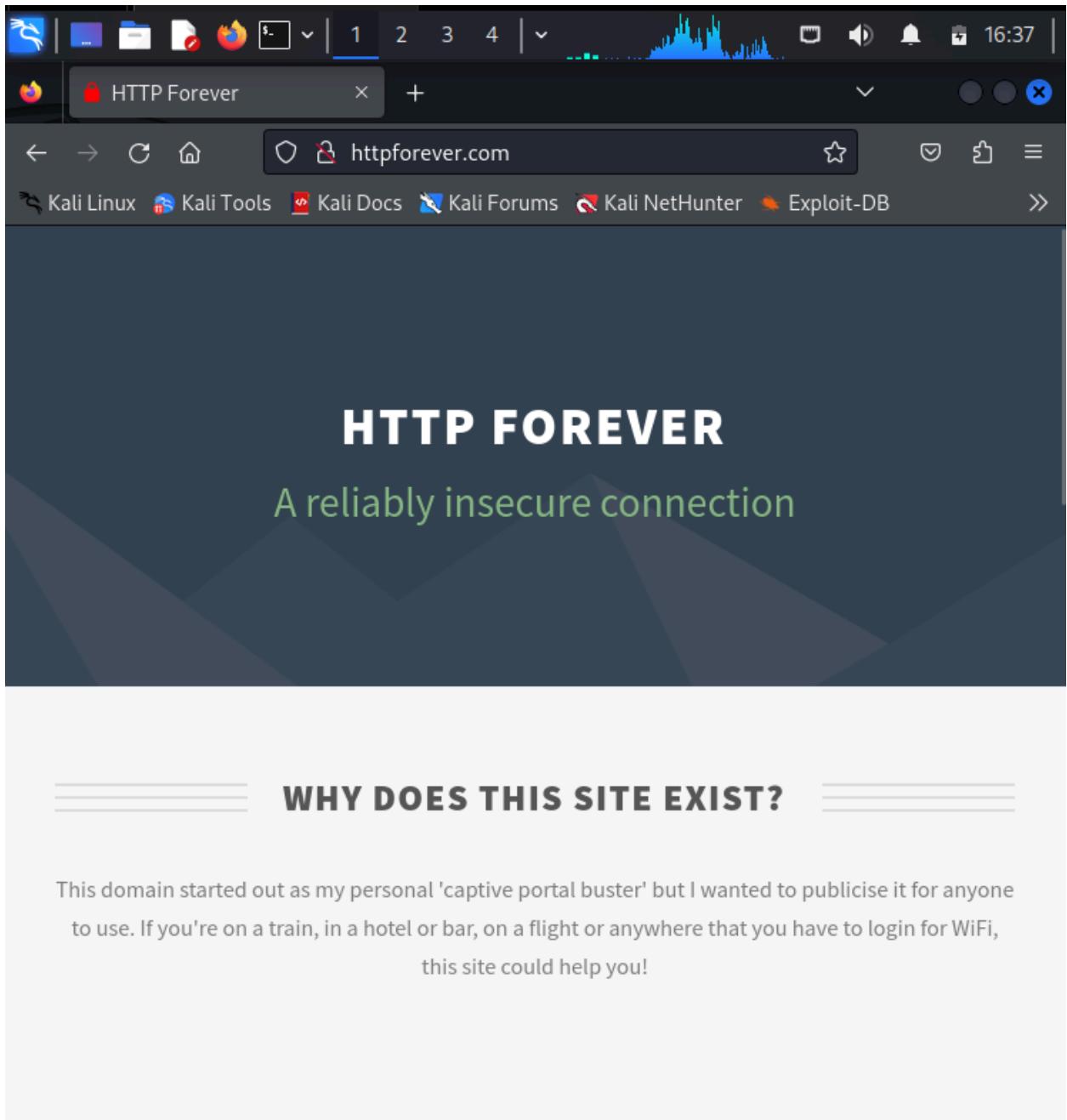
Traceroute Linux

```
kali@kali: ~
File Actions Edit View Help
^X@sS64 bytes from 8.8.8.8: icmp_seq=7 ttl=128 time=21.4 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=128 time=20.8 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=128 time=21.3 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=128 time=21.5 ms
^C
— 8.8.8.8 ping statistics —
10 packets transmitted, 10 received, 0% packet loss, time 9019ms
rtt min/avg/max/mdev = 20.802/26.889/65.803/13.033 ms

└─(kali㉿kali)-[~]
└─$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  192.168.88.2 (192.168.88.2)  0.644 ms  0.545 ms  0.504 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * ^C

└─(kali㉿kali)-[~]
└─$
```

Http Linux



Https Linux

A screenshot of a Firefox browser window. The address bar shows the URL <https://www.investing.com>. The page header includes the Investing.com logo, a 'Get 50% Off' button, and a search bar. Below the header is a navigation menu with links like 'United States', 'Major Indices', 'Indices Futures', 'Real Time Commodities', 'Webinars', 'Bitcoin', and 'E'. A yellow banner at the bottom of the page features a 'Premium AI-powered Stock Picks from InvestingPro Now up to 50% Off' offer with a 'CLAIM SALE' button.



## Stock Market Today: Nasdaq tumbles despite soft CPI data, Nvidia falls 5.6%

Investing.com- US stocks fell Thursday, despite cooling inflation data pointed to a slowing in the...



Tesla closes 8.4% on report it will delay robotaxi unveiling



September rate cut incoming: Wall Street reacts to a soft CPI print



Online Travel: 2Q24 Earnings Preview

Performing a TLS handshake to script.hotjar.com...

Configurar las reglas para dar acceso a internet ICMP solo a la zona Orange y Blue.

The screenshot shows a list of firewall rules under the heading "Current rules". The legend indicates that a green checkmark means "Enabled (click to disable)" and a grey square means "Disabled (click to enable)". The "Edit" icon is a pencil, and the "Remove" icon is a trash can.

#	Source	Destination	Service	Policy	Remark	Actions				
1	GREEN	RED	TCP/80	→						
2	BLUE	RED	TCP/80	→						
3	ORANGE	RED	TCP/80	→						
4	GREEN	RED	TCP/443	→						
5	BLUE	RED	TCP/443	→						
6	ORANGE	RED	TCP/443	→						
7	ORANGE	RED	ICMP/8 ICMP/30	→						
8	BLUE	RED	ICMP/8 ICMP/30	→						

Legend Enabled (click to disable) Disabled (click to enable) Edit Remove

Show system rules >>

Para la zona Green navegación habilitada http y https y bloqueo ICMP para la zona green.

This screenshot shows a single ICMP rule for zone GREEN. The rule number is 9, source is GREEN, destination is RED, service is ICMP/8 ICMP/30, and policy is →|. The legend indicates that a red double-headed arrow means "Enabled (click to disable)" and a grey square means "Disabled (click to enable)".

#	Source	Destination	Service	Policy
9	GREEN	RED	ICMP/8 ICMP/30	→

The screenshot shows a list of firewall rules under the heading "Current rules". The legend indicates that a green checkmark means "Enabled (click to disable)" and a grey square means "Disabled (click to enable)". The "Edit" icon is a pencil, and the "Remove" icon is a trash can.

#	Source	Destination	Service	Policy	Remark	Actions				
1	GREEN	RED	TCP/80	→						
2	BLUE	RED	TCP/80	→						
3	ORANGE	RED	TCP/80	→						
4	GREEN	RED	TCP/443	→						
5	BLUE	RED	TCP/443	→						
6	ORANGE	RED	TCP/443	→						
7	ORANGE	RED	ICMP/8 ICMP/30	→						
8	BLUE	RED	ICMP/8 ICMP/30	→						
9	GREEN	RED	ICMP/8 ICMP/30	→						

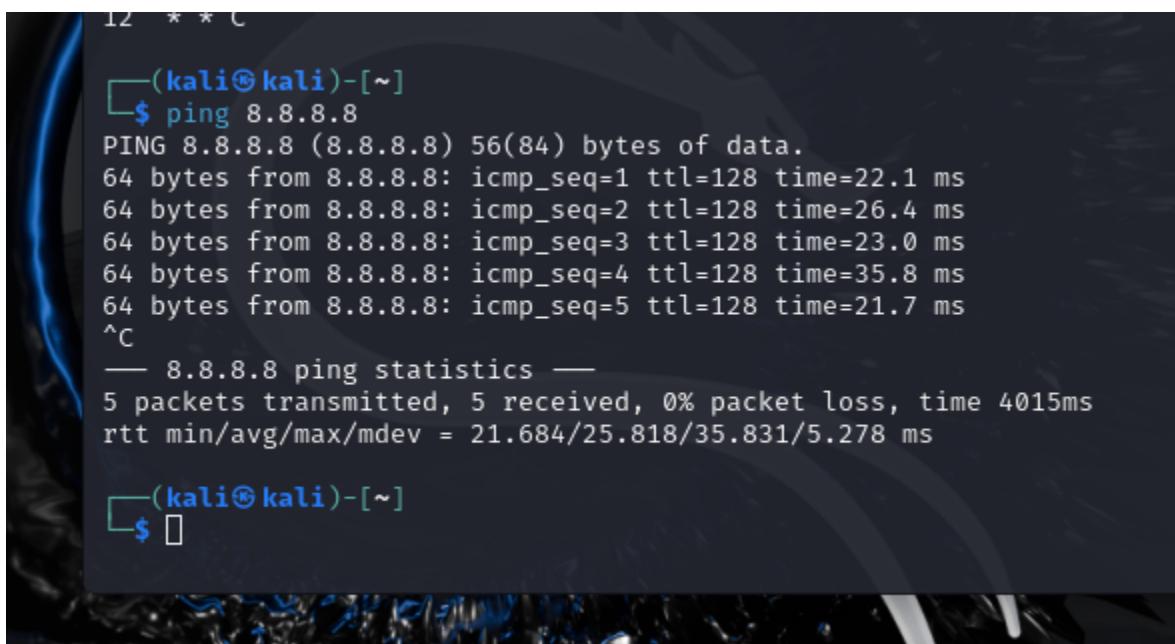
Legend Enabled (click to disable) Disabled (click to enable) Edit Remove

Show system rules >>

Windows bloqueado a ICMP

```
Haciendo ping a 8.8.8.8 con 32 bytes de datos:  
Tiempo de espera agotado para esta solicitud.  
  
Estadísticas de ping para 8.8.8.8:  
Paquetes: enviados = 4, recibidos = 0, perdidos = 4  
(100% perdidos),
```

Kali LLinux habilitado

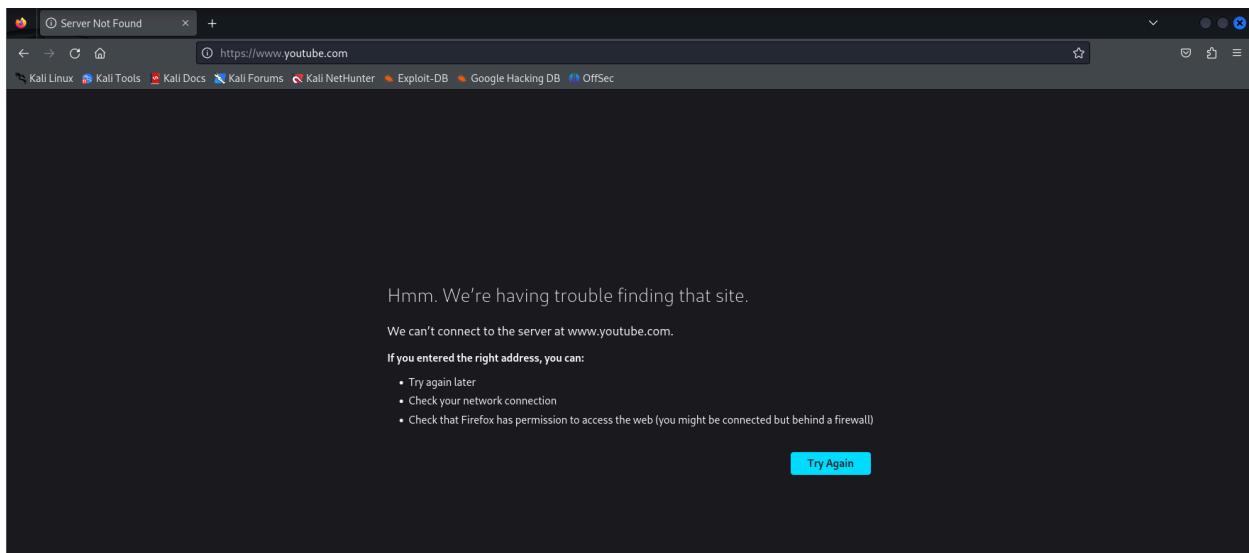


```
12 * * C  
└─(kali㉿kali)-[~]  
$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=22.1 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=26.4 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=23.0 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=35.8 ms  
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=21.7 ms  
^C  
— 8.8.8.8 ping statistics —  
5 packets transmitted, 5 received, 0% packet loss, time 4015ms  
rtt min/avg/max/mdev = 21.684/25.818/35.831/5.278 ms  
  
└─(kali㉿kali)-[~]  
$ ┌─
```

Debian habilitado

```
64 bytes from 8.8.8.8: icmp_req=8 ttl=128 time=21.7 ms
64 bytes from 8.8.8.8: icmp_req=9 ttl=128 time=23.2 ms
64 bytes from 8.8.8.8: icmp_req=10 ttl=128 time=25.3 ms
64 bytes from 8.8.8.8: icmp_req=11 ttl=128 time=21.7 ms
64 bytes from 8.8.8.8: icmp_req=12 ttl=128 time=21.0 ms
64 bytes from 8.8.8.8: icmp_req=13 ttl=128 time=22.2 ms
64 bytes from 8.8.8.8: icmp_req=14 ttl=128 time=35.2 ms
64 bytes from 8.8.8.8: icmp_req=15 ttl=128 time=21.6 ms
64 bytes from 8.8.8.8: icmp_req=16 ttl=128 time=21.6 ms
64 bytes from 8.8.8.8: icmp_req=17 ttl=128 time=22.1 ms
64 bytes from 8.8.8.8: icmp_req=18 ttl=128 time=26.0 ms
^C
--- 8.8.8.8 ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17065ms
rtt min/avg/max/mdev = 21.067/23.813/35.264/3.703 ms
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=23.0 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=128 time=22.0 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=128 time=21.2 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 21.243/22.125/23.066/0.764 ms
user@debian:~$
```

## Bloqueo http-https para Kali Linux



# Conclusiones

La implementación del Endian Firewall Community en un entorno de red virtualizado ha proporcionado una visión clara y práctica de las medidas de seguridad necesarias para proteger infraestructuras digitales. A lo largo del proyecto, se ha demostrado cómo un firewall bien configurado puede actuar como una barrera eficaz contra diversas amenazas ciberneticas, asegurando la integridad, confidencialidad y disponibilidad de los datos.

La configuración de las tres zonas de la red (Verde, Naranja y Azul) ha permitido una segmentación efectiva del tráfico, minimizando el riesgo de ataques internos y externos. La integración de herramientas como Kali Linux y un servidor web vulnerable ha sido crucial para simular escenarios de ataque y evaluar la respuesta del firewall y el IDS, proporcionando un contexto realista para la prueba y validación de las medidas de seguridad implementadas.

Los resultados obtenidos destacan la importancia de una configuración cuidadosa y la necesidad de una vigilancia constante en el campo de la ciberseguridad. La capacidad de detectar y mitigar amenazas en tiempo real es fundamental para mantener la seguridad en redes complejas y prevenir posibles brechas de seguridad. Este proyecto subraya la necesidad de formación continua y actualización de conocimientos en un campo tan dinámico como el de la seguridad TICs, donde las amenazas evolucionan constantemente.

La experiencia adquirida a través de este proyecto no solo refuerza los conceptos teóricos de la ciberseguridad, sino que también proporciona habilidades prácticas esenciales para enfrentar los desafíos actuales en la protección de redes e infraestructuras digitales.

# Referencias

## Fuentes en Línea:

- **Endian Firewall Community Documentation.** Recuperado de <https://www.endian.com/en/community/>
- **Kali Linux Official Documentation.** Recuperado de <https://www.kali.org/docs/>
- **VMware Workstation Documentation.** Recuperado de [https://www.vmware.com/support/pubs/ws\\_pubs.html](https://www.vmware.com/support/pubs/ws_pubs.html)
- **Microsoft. (2010).** Windows 7 Resource Kit. Recuperado de [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-7/ff633412\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-7/ff633412(v=ws.10))

## Artículos Académicos:

- **Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015).** Intrusion detection and Big Heterogeneous Data: a Survey. *Journal of Big Data*, 2(1), 3.
- **Axelsson, S. (2000).** Intrusion detection systems: A survey and taxonomy. *Technical Report*, Department of Computer Engineering, Chalmers University of Technology.

## Normas y Protocolos:

- **IETF (Internet Engineering Task Force).** (1981). *Transmission Control Protocol*. Recuperado de <https://tools.ietf.org/html/rfc793>
- **IETF. (1983).** *Domain names - implementation and specification*. Recuperado de <https://tools.ietf.org/html/rfc1035>

## Guías y Manuales Técnicos:

- **Cisco Systems.** (2021). *Cisco Networking Basics*. Recuperado de <https://www.cisco.com/c/en/us/support/docs/>
- **NIST (National Institute of Standards and Technology).** (2001). *An Introduction to Computer Security: The NIST Handbook*. Recuperado de <https://csrc.nist.gov/publications/detail/sp/800-12/archive/2001-10-19>

Para este proyecto, se ha tomado de base los materiales de lectura compartidos por el profesor Chrystian Ruiz Díaz dentro del módulo de Seguridad TICs 2024.