Configuración de la instancia para GNU/Linux Endian en Virtualbox (tarjetas de red) e instalación efectiva del mismo.

Jalil Danilo Aviles Pacheco
e-mail: jdavilesp@unadvirtual.edu.co

RESUMEN: *Implementar una instancia funcional del sistema Endian Firewall Community en un entorno virtualizado, configurando correctamente las zonas de red GREEN (LAN), ORANGE (DMZ) y RED (WAN), asegurando la segmentación de la red, conectividad y base para futuras configuraciones de seguridad.*

PALABRAS CLAVE: Endian Firewall

VirtualBox, Zonas de red, Zona GREEN, Zona ORANGE,
Zona RED.

1 INTRODUCCIÓN

Describir paso a paso el proceso de instalación, configuración, validación y puesta en marcha de una infraestructura de red basada en GNU/Linux Endian Firewall en VirtualBox. El objetivo fue lograr una segmentación segura de red mediante la implementación de tres zonas: GREEN (LAN), RED (WAN) y ORANGE (DMZ), garantizando salida a Internet, aislamiento de zonas y comunicación controlada entre ellas. Además, se abordaron aspectos fundamentales de ciberseguridad, considerando la importancia de proteger cada segmento y evitar accesos no autorizados.

2 FORMATO

Temática 1: Configuración de la instancia para GNU/Linux Endian en Virtualbox (tarjetas de red) e instalación efectiva del mismo.
Producto terminado:
Implementación de GNU/Linux Endian con las zonas verde, roja y naranja, así: Zona verde: Red interna (LAN), Zona roja: Acceso a internet (WAN) y Zona naranja: Servidores (DMZ).

Topología de Red

Se implementó la siguiente estructura:

- GREEN (eth0): Red interna - LAN (192.168.100.0/24)
- RED (eth1): Salida a Internet - NAT o Bridge (IP por DHCP)
- ORANGE (eth2): DMZ - Red aislada para servidores (192.168.20.0/24)
- Se utilizó una VM Ubuntu Desktop para la zona GREEN y una VM Ubuntu Server para ORANGE.

3 Proceso de configuración

3.1 Instalación de Endian

- Se descargó la ISO de Endian Community 3.3.2
- Se creó una VM con 3 adaptadores de red
- Adaptador 1: Red Interna (GREEN)
- Adaptador 2: NAT (RED)
- Adaptador 3: Red Interna (ORANGE)
- Se instaló Endian con configuración manual de zonas

Configuración de Ubuntu Desktop (zona GREEN)

- IP: 192.168.100.2
- Gateway: 192.168.100.1
- DNS: 8.8.8.8

Configuración de Ubuntu Server (zona ORANGE)

- IP: 192.168.20.10
- Gateway: 192.168.20.1
- DNS: 8.8.8.8

4 PRUEBAS Y VALIDACIONES

Desde Endian

- Ping 8.8.8.8
- Ping google.com
- Ping de Endian a Server
- Ping de Server a Endian

Desde Desktop (GREEN)

- ping 192.168.100.1
- ping 8.8.8.8
- ping google.com

Desde Server (ORANGE)

- ping 192.168.20.1
- ping 8.8.8.8
- ping google.com

5 ERRORES ENCONTRADOS Y SOLUCIONADOS

No respuesta a ping desde GREEN a Internet:

Solución: configurar NAT en Firewall → NAT → Source NAT (SNAT)
Revisar regla: GREEN → RED, SNAT habilitado

Error en DNS en Desktop:

- Solución: cambiar resolv.conf a nameserver 8.8.8.8

ORANGE sin conectividad:

- Revisión de nombre de Red Interna en VirtualBox
- Solución: asegurar coincidencia exacta de nombre de red entre Endian y Server

Gateway4 deprecated en Netplan:

- No afecta funcionamiento, se puede actualizar posteriormente usando "routes"

6 CONSIDERACIONES DE CIBERSEGURIDAD

Durante la implementación de la Temática 1, se aplicaron principios básicos de ciberseguridad en la arquitectura:

- Segmentación de red: aísla dispositivos críticos en GREEN, acceso controlado a servidores en ORANGE y salida segura por RED.
- Uso de NAT: oculta las IPs internas (GREEN y ORANGE) de redes externas.
- Políticas de firewall: se configuraron reglas explícitas para restringir tráfico entre zonas según necesidad.
- DNS seguro: uso de servidores confiables como 8.8.8.8, evitando resoluciones internas no deseadas.
- Verificación de logs y monitoreo: Endian provee herramientas que pueden activarse para detectar tráfico sospechoso.

Estas medidas sientan la base para una arquitectura segura y escalable, reforzando buenas prácticas en laboratorios y entornos reales.

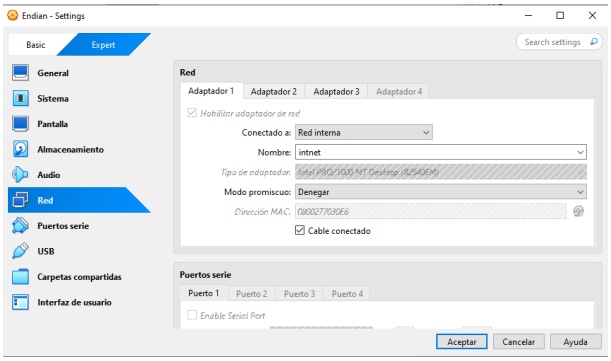
7 PRÁCTICA

La figura muestra la ventana de configuración de red de la máquina virtual Endian dentro de Oracle VirtualBox, específicamente en la sección de Adaptadores de Red. Aquí se establecen las interfaces de red necesarias para que Endian pueda conectar con las zonas GREEN, RED y ORANGE.

Configurar correctamente los tres adaptadores que permitirán que Endian gestione:

- La red local segura (GREEN),
- El acceso a Internet (RED),
- Y la red de servidores (ORANGE).

Figura 1 Configuración de adaptadores de red en Endian para conexión con desktop

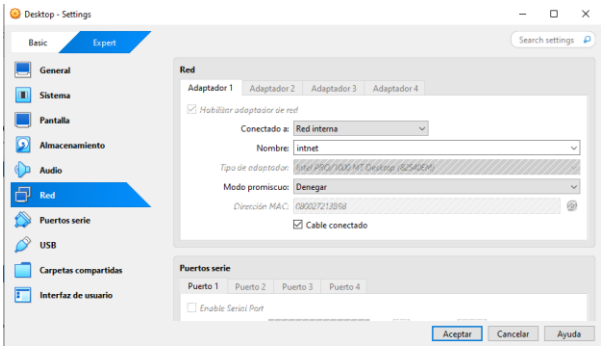


Fuente propia

Esta figura muestra la configuración de red en VirtualBox para la máquina virtual Ubuntu Desktop. Específicamente, se observa el Adaptador 1, que debe estar configurado en modo Red Interna para conectarse a la zona GREEN del firewall Endian.

Permitir que el Ubuntu Desktop se comunique directamente con la interfaz GREEN de Endian (por ejemplo, con IP 192.168.100.1), de modo que pueda acceder a la GUI de administración, salir a Internet si se habilita NAT, y representar una máquina cliente de la red LAN interna.

Figura 2 Configuración de adaptadores de red en Desktop para conexión con Endian

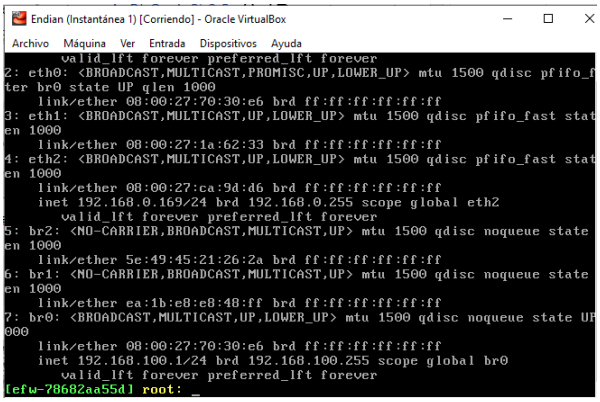


Fuente propia

La figura muestra la salida del comando ip a o ip addr show ejecutado desde la consola de Endian. Este comando permite visualizar el estado y la configuración de las interfaces de red del sistema.

Verificar que las interfaces de red en Endian estén activas, correctamente asignadas a sus zonas (GREEN, RED, ORANGE) y con direcciones IP válidas para establecer comunicación con otras máquinas de la red virtual.

Figura 3 IP de Endian



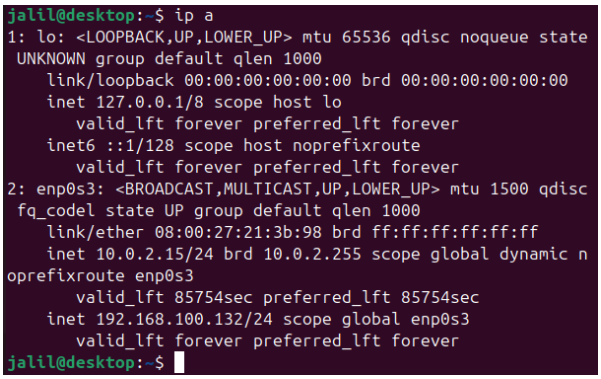
Fuente propia

La figura muestra la salida del comando ip a ejecutado desde la consola de Ubuntu Desktop, que está conectado a la zona GREEN del firewall Endian.

Validar que el Ubuntu Desktop se encuentra correctamente configurado dentro

del rango IP de la zona GREEN (192.168.100.0/24) y que tiene asignada una IP funcional para establecer conexión con Endian y eventualmente con Internet.

Figura 4 IP de Desktop

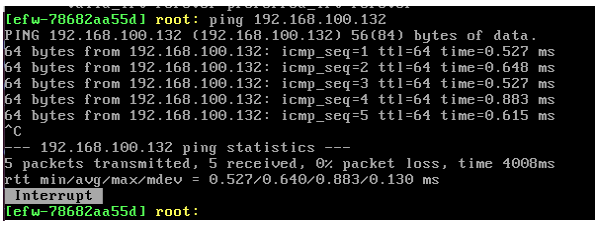


Fuente propia

Esta figura muestra el resultado de ejecutar el comando PING desde la consola de Endian (root@efw) hacia la IP estática del Ubuntu Desktop, ubicada en la zona GREEN.

Verificar la conectividad entre Endian y el cliente Ubuntu Desktop dentro de la misma subred (GREEN). Esto confirma que la configuración de red de ambas máquinas es correcta y que no existen bloqueos o errores de enrutamiento en la zona LAN.

Figura 5 Ping de Endian a Desktop

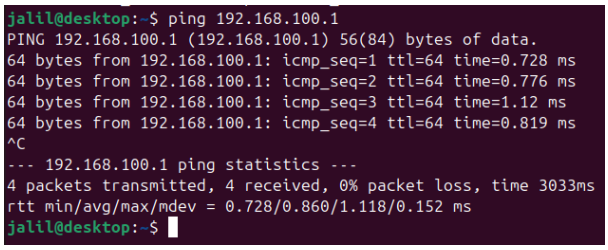


Fuente propia

La figura muestra el resultado del comando ping ejecutado desde la consola del Ubuntu Desktop hacia la interfaz GREEN del firewall Endian, cuya IP es 192.168.100.1.

Confirmar que el cliente en la red GREEN (Ubuntu Desktop) puede comunicarse con el firewall Endian, estableciendo así que la conectividad LAN funciona correctamente y que no hay barreras que impidan el flujo de paquetes en esa subred.

Figura 6 Ping de desktop a Endian

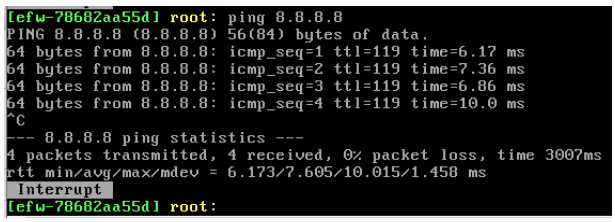


Fuente propia

La figura muestra la ejecución del comando ping realizado desde la consola de Endian Firewall Community, usualmente desde el entorno root@efw, con el objetivo de probar la conectividad hacia el exterior (Internet), usando una IP pública del servicio DNS de Google.

Verificar que Endian tiene salida a Internet a través de su interfaz RED, lo que permite actuar como puerta de enlace (gateway) para otras zonas (como GREEN o ORANGE) que dependan de él para conectarse al exterior mediante NAT.

Figura 7 Salida de Endian a internet Ping 8.8.8.8



Fuente propia

Esta figura muestra la ejecución del comando ping desde la consola de Endian, con

el fin de verificar la resolución DNS y conectividad hacia Internet mediante nombres de dominio.

Confirmar que Endian no solo tiene conectividad IP hacia Internet, sino que también puede resolver nombres de dominio usando un servidor DNS confiable (como el de Google).

Figura 8 Ping a google desde Endian

```
[endian]: ping google.com
PING google.com (142.250.218.78) 56(84) bytes of data.
64 bytes from ncboga-aa-in-f14.1e100.net (142.250.218.78): icmp_seq=2 ttl=118
me=44.6 ms
64 bytes from ncboga-aa-in-f14.1e100.net (142.250.218.78): icmp_seq=3 ttl=118
me=40.2 ms
64 bytes from ncboga-aa-in-f14.1e100.net (142.250.218.78): icmp_seq=4 ttl=118
me=45.3 ms
64 bytes from gru06s61-in-f14.1e100.net (142.250.218.78): icmp_seq=5 ttl=118 t
e=46.6 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4012ms
rtt min/avg/max/mdev = 40.231/44.199/46.624/2.413 ms
 Interrupt
[endian]: _
```

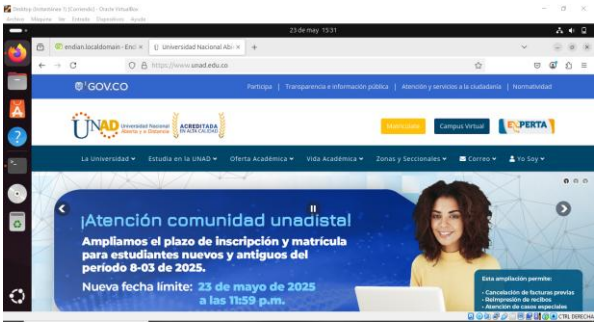
Fuente propia

La figura muestra una ventana del navegador en Ubuntu Desktop, que ha accedido exitosamente al sitio oficial de la Universidad Nacional Abierta y a Distancia (UNAD) mediante la URL https://www.unad.edu.co.

Validar que el cliente conectado a la zona GREEN del firewall Endian (Ubuntu Desktop) tiene acceso a Internet completo, incluyendo:

- Conectividad IP
- Resolución de nombres de dominio (DNS)
- Acceso a servicios HTTPS

Figura 9 Salida a internet desde desktop

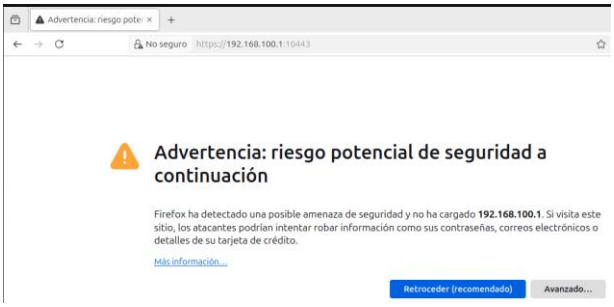


Fuente propia

La figura muestra el navegador Firefox en Ubuntu Desktop intentando acceder a la interfaz gráfica de administración (GUI) de Endian a través de la dirección: https://192.168.100.1:10443 El navegador lanza una advertencia de seguridad por certificado no confiable (self-signed).

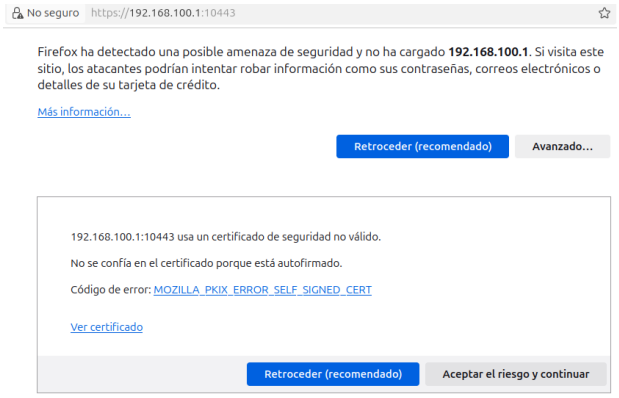
Verificar que la GUI de Endian es accesible desde la zona GREEN, que el servicio web seguro está funcionando correctamente en el puerto 10443 (HTTPS), y que se puede continuar con la administración del sistema desde un cliente interno.

Figura 10 Acceso a Endian por GUI https://192.168.100.1:10443



Fuente propia

Figura 11 Acceso a Endian por GUI https://192.168.100.1:10443



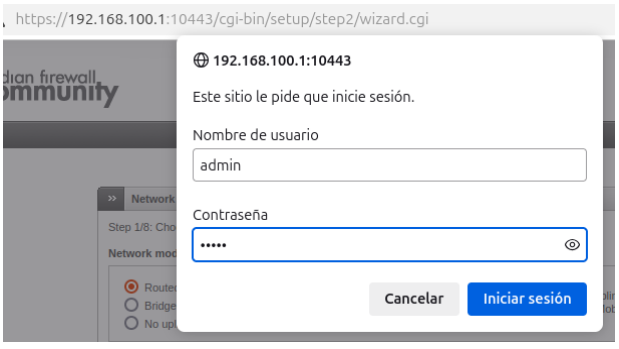
Fuente propia

La imagen muestra la ventana emergente de autenticación del navegador al intentar acceder a la interfaz web segura (GUI) de Endian. Se observa la solicitud de credenciales con los campos:

- Nombre de usuario: admin
- Contraseña: oculta por seguridad

Verificar que el servicio web de Endian no solo está en ejecución, sino que exige autenticación segura para ingresar a la interfaz de administración, lo cual refuerza el principio de control de acceso.

Figura 12 Acceso a Endian por GUI https://192.168.100.1:10443

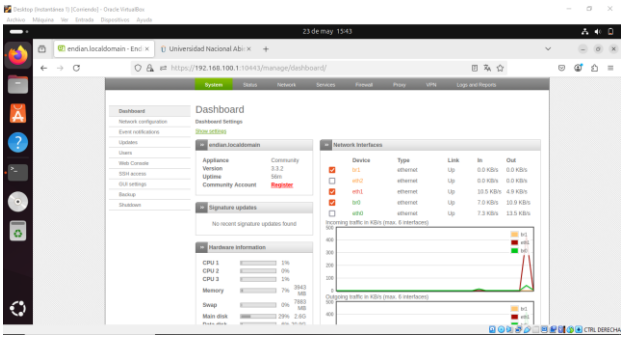


Fuente propia

La imagen muestra el panel de control (Dashboard) de la interfaz gráfica de Endian Firewall, accesible desde el navegador web de Ubuntu Desktop. El usuario ha superado la autenticación y ahora visualiza el entorno de administración completo.

Validar el acceso exitoso al entorno de gestión de Endian, comprobando que los servicios están levantados y que el firewall puede ser administrado remotamente desde la zona GREEN, en un entorno seguro vía HTTPS.

Figura 13 Acceso a Endian por GUI https://192.168.100.1:10443



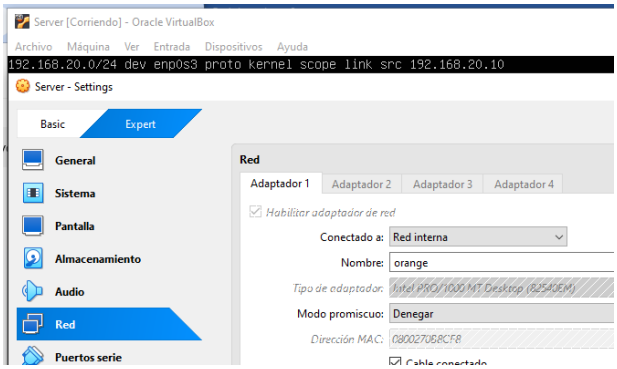
Fuente propia

La figura muestra la configuración de red de la máquina virtual Ubuntu Server, dentro de Oracle VirtualBox, enfocada en el Adaptador 1. Este adaptador está configurado para conectarse a una Red Interna con el nombre orange, que representa la zona ORANGE (DMZ) del firewall Endian.

En la parte superior, también se observa la salida de una instrucción en consola, donde se especifica la IP 192.168.20.10, correspondiente a este servidor.

Permitir que el servidor (en este caso Ubuntu Server) se conecte a la zona ORANGE de Endian, la cual representa una red aislada para servidores expuestos (por ejemplo, servicios web, FTP, correo, etc.) dentro de un entorno controlado y segmentado.

Figura 14 Configuración del adaptador del server



Fuente propia

La imagen muestra la salida del comando ping ejecutado desde el Ubuntu Server que se encuentra en la zona ORANGE del firewall Endian. Esta prueba tiene como objetivo verificar la conectividad IP a Internet desde un servidor aislado, a través del firewall.

Comprobar que el servidor en la zona ORANGE (DMZ) puede alcanzar Internet mediante el servicio de NAT configurado en Endian, lo que demuestra que la política de salida ORANGE → RED está activa y funcional.

Figura 15 Ping al 8.8.8.8 desde el server

```
jalil@server:~$ 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=118 time=64.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=50.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=45.6 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=43.8 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=118 time=43.1 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 5 received, 16.6667% packet loss, time 5140ms
rtt min/avg/max/mdev = 43.128/49.588/64.744/8.020 ms
jalil@server:~$
```

Fuente propia

La imagen muestra el resultado del comando ping -c 4 192.168.20.1 ejecutado desde la terminal del Ubuntu Server, el cual se encuentra en la zona ORANGE (DMZ), hacia la IP de la interfaz ORANGE de Endian.

Verificar la comunicación interna entre el servidor y Endian dentro de la misma red segmentada ORANGE (192.168.20.0/24). Esta prueba asegura que:

- La interfaz ORANGE de Endian está activa.
- El gateway configurado en el servidor es válido.
- No existen errores de red entre ambos extremos.

Figura 16 Ping a la Zona Orange

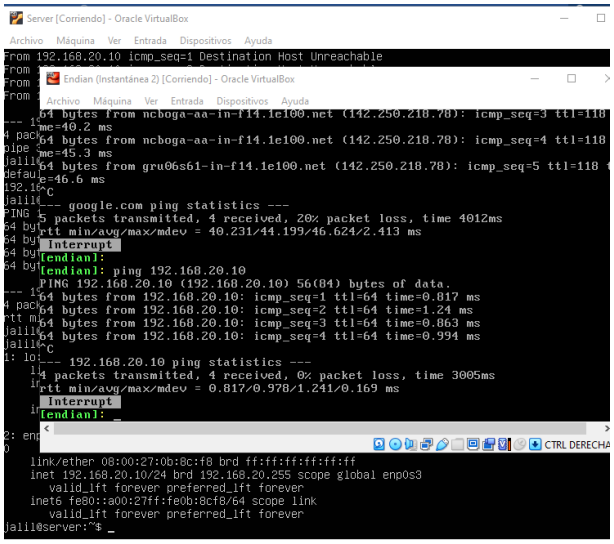
```
jalil@server:~$ ping -c 4 192.168.20.1
PING 192.168.20.1 (192.168.20.1) 56(84) bytes of data.
64 bytes from 192.168.20.1: icmp_seq=1 ttl=64 time=1.29 ms
64 bytes from 192.168.20.1: icmp_seq=2 ttl=64 time=1.15 ms
64 bytes from 192.168.20.1: icmp_seq=3 ttl=64 time=0.886 ms
64 bytes from 192.168.20.1: icmp_seq=4 ttl=64 time=1.11 ms

--- 192.168.20.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3028ms
rtt min/avg/max/mdev = 0.886/1.110/1.292/0.145 ms
```

Fuente propia

La imagen contiene varias ventanas superpuestas, destacando una consola del firewall Endian intentando hacer ping a la IP del Ubuntu Server (192.168.20.10), así como la consola del Server, que también muestra sus interfaces activas (br0, enp0s3).

Validar que el firewall Endian puede comunicarse correctamente con el servidor ubicado en la zona ORANGE (DMZ), usando su interfaz de red correspondiente (br2 con IP 192.168.20.1).

Figura 17 Ping del Endian al Server



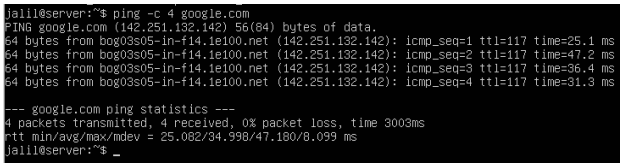
Fuente propia

La imagen muestra la ejecución del comando:
ping -c 4 google.com desde la terminal del Ubuntu Server conectado a la zona ORANGE (DMZ), con el objetivo de comprobar si el servidor puede resolver nombres de dominio a direcciones IP y alcanzar servicios externos a través del firewall Endian.

Validar que el servidor:

- Puede resolver correctamente nombres de dominio mediante DNS.
- Tiene salida a Internet.
- Recibe respuestas desde el exterior (servicio completo de red operando).

Figura 18 Verificación de salida a DNS desde el server



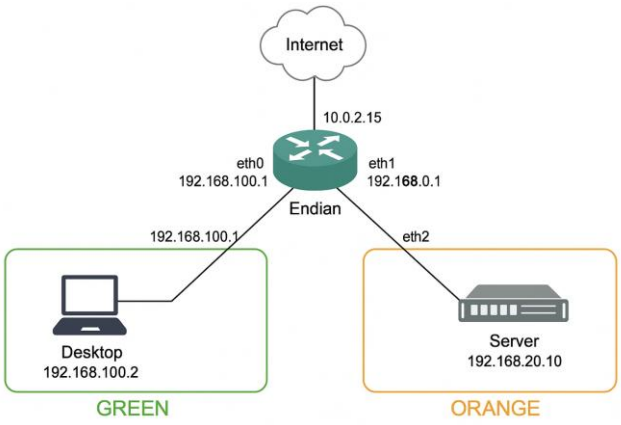
Fuente propia

El diagrama representa gráficamente la topología lógica del entorno implementado, segmentado por zonas y gestionado por el firewall Endian. Se observan tres interfaces de red conectadas a diferentes zonas:

- eth0 – GREEN (LAN) → conectada al Desktop 192.168.100.2
- eth1 – RED (WAN) → conectada a Internet (10.0.2.15)
- eth2 – ORANGE (DMZ) → conectada al Server 192.168.20.10

Visualizar de forma clara la arquitectura de red establecida, mostrando cómo Endian actúa como núcleo de segmentación y control de tráfico entre las zonas GREEN, ORANGE y RED.

Figura 18 Diagrama de Red



Fuente propia

8 Conclusiones.

La configuración manual de zonas en Endian requiere atención a detalle, especialmente en redes virtuales.

La configuración de NAT y políticas de firewall es esencial para permitir salida a Internet.

Las pruebas con ping y resolv.conf fueron claves para validar conectividad y DNS.

La experiencia fortaleció la comprensión de la segmentación de red, aislamiento, y principios fundamentales de ciberseguridad.

9 RECOMENDACIONES

Nombrar cuidadosamente las redes internas en VirtualBox para evitar errores de conectividad.

Documentar las IPs y adaptadores para cada zona desde el inicio.

Habilitar logging en el firewall de Endian para depurar problemas futuros.

Exportar la VM Endian funcional como plantilla para futuros proyectos.

10 REFERENCIAS

[1] A, D. (s.f.). *ubunlog.com*. Obtenido de https://ubunlog.com/boxy-svg-editor-svg-snap/

[2] CreativeCommons. (s.f.). *wiki.creativecommons.org*. Obtenido de https://wiki.creativecommons.org/wiki/Es:Licencias_y_ejemplos#Atribuci.C3.B3n_CC_BY

[3] danscourses. (2019). Obtenido de https://www.youtube.com/watch?v=JqeRyoXJCxE&t=248s

[4] Endian. (s.f.). Obtenido de https://docs.endian.com/archive/2.1/efw.system.network_configuration.html???

[5] Endian. (s.f.). Obtenido de https://docs.endian.com/archive/2.1/efw.firewall.introduction.html

[6] Endian. (s.f.). *docs.endian.com/*. Obtenido de https://docs.endian.com/6.6/utm/firewall.html#inter-zone-traffic

[7] Endian. (s.f.). *help.endian.com*. Obtenido de https://help.endian.com/hc/en-us/articles/218144918-Network-Configuration-Wizard-Part-2-of-3

[8] Geek, M. T. (2018). Obtenido de https://www.youtube.com/watch?v=36VEmithaWs

[9] GNU. (2022). *www.gnu.org*. Obtenido de https://www.gnu.org/education/education.html

[10] GNU.org. (s.f.). *gnu.org*. Obtenido de https://www.gnu.org/philosophy/philosophy.es.html#:~:text=En%20concreto%2C%20el%20software%20libre,(3)%20distribuir%20versiones%20modificadas.

[11] GNU.org. (s.f.). *gnu.org*. Obtenido de https://www.gnu.org/philosophy/categories.es.html

[12] GNU.org. (s.f.). *gnu.org*. Obtenido de https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html

[13] InfoRed. (2018). Obtenido de https://www.youtube.com/watch?v=zOa1q1n7kU0

[14] InfoRed. (2018). Obtenido de https://www.youtube.com/watch?v=mAz0hJIEioc

[15] InfoRed. (2019). Obtenido de https://www.youtube.com/watch?v=XK0QdHYk6pg

[16] InfoRed. (2019). Obtenido de https://www.youtube.com/watch?v=rZtrqVI9Y7c

[17] Open Source Iniciative. (s.f.). *opensource.org*. Obtenido de https://opensource.org/license/bsd-2-clause

[18] Red Hat. (3 de 10 de 2021). *redhat.com*. Obtenido de https://www.redhat.com/es/topics/openstack?sc_cid=7015Y0000048RsyQAE&gad_source=1&gclid=CjwKCAiAt4C-BhBcEiwA8Kp0CU8IZkAQtMQF4d228KwBSJavOWNaPZYygDTTYhbJlt967nZd-cP4oxoCWoAQAvD_BwE

[19] Red Hat. (3 de 1 de 2023). *redhat.com*. Obtenido de https://www.redhat.com/es/topics/linux/whats-the-best-linux-distro-for-you

[20] Red Hat. (3 de 1 de 2023). *redhat.com*. Obtenido de https://www.redhat.com/es/topics/linux/what-is-linux

[21] Red Hat. (s.f.). *docs.redhat.com*. Obtenido de https://docs.redhat.com/es/documentation/red_hat_enterprise_linux/8/html/packaging_and_distributing_software/getting-started-with-rpm-packaging

[22] Red Hat. (s.f.). *docs.redhat.com*. Obtenido de https://docs.redhat.com/es/documentation/red_hat_enterprise_linux/6/html/installation_guide/apcs02#idm140338567937184

[23] Rodríguez, J. (2023). Obtenido de https://www.youtube.com/watch?v=Dw5maQE98oI

[24] UBUNTU. (s.f.). */help.ubuntu.com*. Obtenido de https://help.ubuntu.com/20.04/ubuntu-help/getting-started.html.es

[25] UBUNTU. (s.f.). *ubuntu.com/*. Obtenido de https://ubuntu.com/openstack/what-is-openstack