Implementación de Servicios de Seguridad Perimetral en GNU/Linux mediante Endian Firewall: NAT, DMZ, Reglas y Proxy

Fernando Andres Acosta
e-mail: faacosta@unadvirtual.edu.co
Daniel Felipe Lancheros Neuta
e-mail: dflancherosn@unadvirtual.edu.co
Stiven Arley Herrera Arguello
e-mail: saherreraar@unadvirtual.edu.co
Juan Carlos Cangrejo Rueda
e-mail: jccangrejor@unadvirtual.edu.co
Laura Daniela Paz SIlva
e-mail: ldpazs@unadvirtual.edu.co

RESUMEN: *Este artículo presenta el desarrollo colaborativo de las cinco temáticas definidas en la Etapa 7 del diplomado, orientadas a la administración y configuración de servicios en GNU/Linux con énfasis en seguridad perimetral. Las actividades incluyeron la instalación del firewall Endian, la configuración de servicios NAT, la habilitación de servicios en la DMZ, la aplicación de reglas de acceso interzonas y la implementación de un proxy HTTP con autenticación. Cada temática fue desarrollada por un integrante del grupo, documentando paso a paso los procedimientos realizados. Los resultados permiten evidenciar el fortalecimiento de habilidades en administración de servicios Linux, gestión de redes y configuración de seguridad perimetral.*

PALABRAS CLAVE: Endian Firewall, seguridad perimetral, GNU/Linux, redes LAN, DMZ.

1 INTRODUCCIÓN

La Etapa 7 del diplomado aborda la administración de servicios en GNU/Linux mediante el despliegue de un entorno seguro basado en Endian Firewall, ISPConfig y servicios complementarios. El trabajo grupal se divide en cinco temáticas independientes pero complementarias, encargadas de construir la estructura de seguridad perimetral: configuración inicial del firewall, NAT, DMZ, reglas de acceso interzonas y proxy HTTP.

Cada integrante desarrolla una temática específica con evidencia, análisis y resultados que permiten consolidar un ecosistema funcional de seguridad en red.

2 DESARROLLO DE LAS TEMÁTICAS

Temática 1: Configuración inicial de Endian Firewall

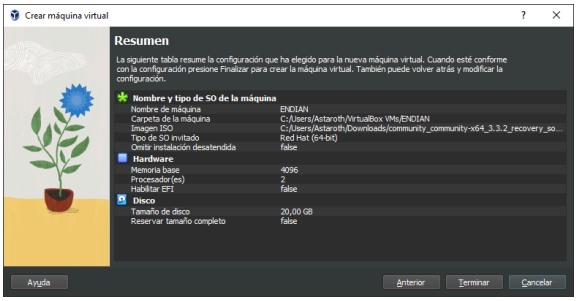
La Temática 1 corresponde a la implementación base del entorno de seguridad perimetral mediante la instalación y configuración inicial del Firewall Endian Community 3.3.2 en una máquina virtual. Este firewall constituye el núcleo del sistema de seguridad del proyecto, permitiendo gestionar zonas de red, enrutar tráfico y habilitar funciones esenciales como DMZ y políticas de acceso.

2.1.1 Creación de la Máquina Virtual en VirtualBox

Para la instalación del firewall se creó una máquina virtual en Oracle VirtualBox con los siguientes parámetros:

- Nombre: Endian
- Tipo: Linux
- Versión: Red Hat (64-bit)
- Memoria RAM: 4096 MB
- Procesadores: 2
- Disco duro virtual: 20 GB, asignación dinámica
- Imagen ISO: Endian Firewall Community 3.3.2

Fig. 1. *Resumen de configuración inicial de la máquina virtual Endian Firewall en VirtualBox.*



Fuente: Autoría Propia

La configuración inicial permitió garantizar recursos suficientes para soportar los servicios de red y el procesamiento de tráfico asociado a las zonas GREEN, ORANGE y RED. [3]

Mencione las figuras con la abreviatura: Fig. 2, a menos que sea al inicio de la oración.

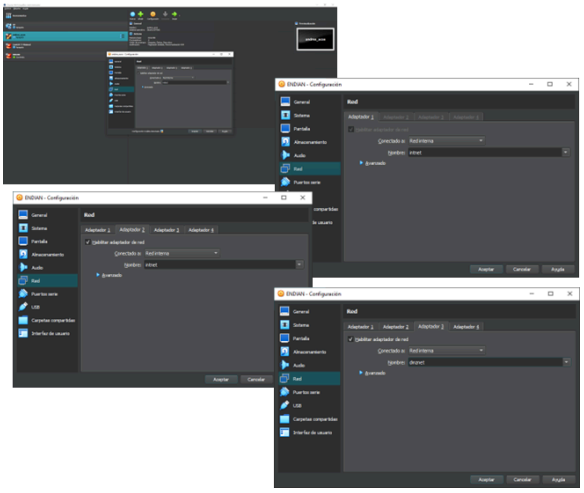
2.1.2 Configuración de Adaptadores de Red

Endian requiere, como mínimo, tres interfaces de red para implementar las zonas de seguridad. En VirtualBox se configuraron los adaptadores de la siguiente forma:

- **Adaptador1–GREEN(LAN):**
  Conectado a *Red interna* con nombre **intnet**, destinado a la red interna segura y a la administración del firewall.
- **Adaptador2–ORANGE(DMZ):**
  Conectado a *Red interna* con nombre **dmznet**, usado para alojar futuros servidores expuestos (HTTP/FTP).
- **Adaptador3–RED(WAN):**
  Configurado como *Adaptador puente*, permitiendo la conexión al router del host y salida a Internet.

Esta estructura garantiza aislamiento y segmentación entre las zonas de red. [2]

Fig. 2. *Configuración de los adaptadores de red en VirtualBox, asignando redes internas para la zona GREEN (intranet) y la zona ORANGE (DMZ).*



Fuente: Autoria Propia

2.1.3 Instalación del Sistema Endian Firewall 3.3.2 [1]

La instalación se inició a partir de la ISO cargada en la máquina virtual. Durante el proceso se ejecutaron los siguientes pasos:

1. Selección del idioma del instalador.
2. Confirmación del particionado del disco ("All data on /dev/sda will be lost").
3. Instalación automática de los paquetes del sistema.
4. Configuración inicial de la **zona GREEN** con la dirección:
   - **IP:** 192.168.0.15
   - **Máscara:** 255.255.255.0
5. Desactivación de consola serial (no requerida en entornos virtuales).
6. Finalización del instalador y reinicio del sistema.

Fig. 3. *Proceso de instalación inicial de Endian Firewall desde consola: selección de idioma, aprobación de preparación de disco e ingreso de dirección IP para la interfaz GREEN.*

Fuente: Autoría Propia

Al finalizar, el instalador presentó la URL de administración vía HTTPS:
https://192.168.0.15:10443

2.1.4 Configuración Inicial desde Consola

Tras el reinicio del sistema, Endian presentó un menú de administración local con opciones para cambiar contraseñas, reiniciar el sistema y ejecutar el asistente de configuración. Se verificó que la interfaz GREEN estuviera activa en la IP configurada y se procedió a realizar la configuración web desde un cliente Linux conectado a la misma red interna (intnet).

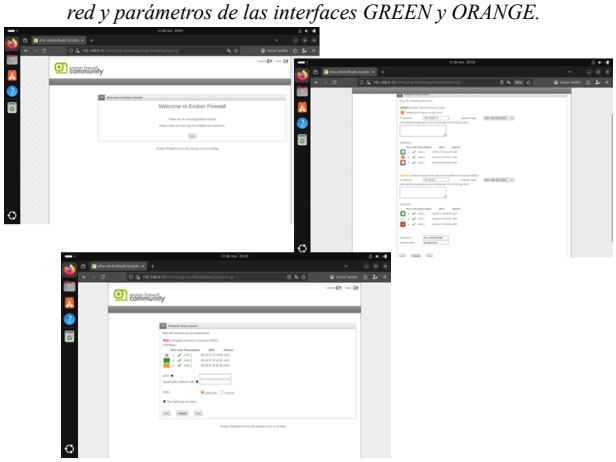
2.1.5 Configuración Web del Firewall

Desde el cliente Ubuntu Desktop se accedió a la interfaz web mediante conexión segura: https://192.168.0.15:10443

En el asistente de configuración se realizaron las siguientes acciones:

- Selección de idioma (**English**)
- Zona horaria (**America/Bogota**)
- Aceptación de licencia GPL
- Establecimiento de las contraseñas para **admin** y **root**
- Selección del modo de operación: **Routed**
- Activación de la zona **ORANGE**
- Asignación de interfaces:
  - GREEN → eth0
  - ORANGE → eth1
  - RED → eth2
- Configuración de la zona RED mediante DHCP automático
- DNS automático
- Aplicación de la configuración

Fig. 4. *Pantallas del asistente web de Endian Firewall, incluyendo aceptación de licencia, selección de idioma, configuración de zonas de red y parámetros de las interfaces GREEN y ORANGE.*



Fuente: Autoría Propia

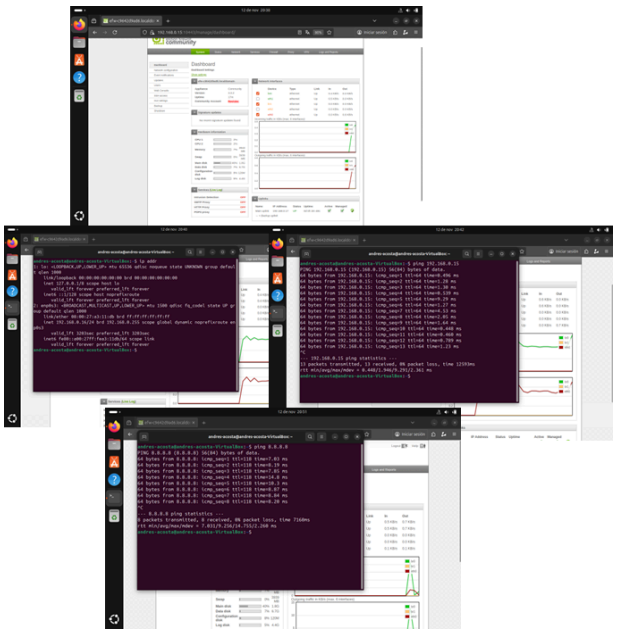
El asistente finalizó mostrando el mensaje:
“Your configuration has been saved… Enjoy!”

2.1.6 Verificación de Conectividad

Para validar la correcta configuración del firewall se ejecutaron pruebas desde el cliente Ubuntu:

1. Verificación de la dirección IP obtenida vía DHCP: ip addr - Se obtuvo una IP dentro del rango GREEN (192.168.0.x).
2. Prueba de conectividad hacia el firewall: ping 192.168.0.15 - Los paquetes fueron respondidos correctamente.
3. Prueba de salida a Internet a través de Endian: ping 8.8.8.8 - Se confirmó conectividad externa, validando la operación de la zona RED.
4. Acceso al Dashboard: Se ingresó nuevamente al portal web para visualizar el estado del sistema, interfaces y servicios.

Fig. 5. *Comprobación del funcionamiento del firewall: acceso al panel de administración, verificación de IP en Ubuntu Desktop y pruebas de conectividad interna y externa mediante comandos ip addr y ping.*



Fuente: Autoría Propia

2.1.7 Resultados de la Temática 1

La instalación y configuración de Endian Firewall permitió establecer la estructura perimetral inicial del proyecto. Se dejaron operativas las zonas:

- **GREEN:** LAN interna y administración
- **ORANGE:** Infraestructura DMZ
- **RED:** Acceso a Internet mediante DHCP

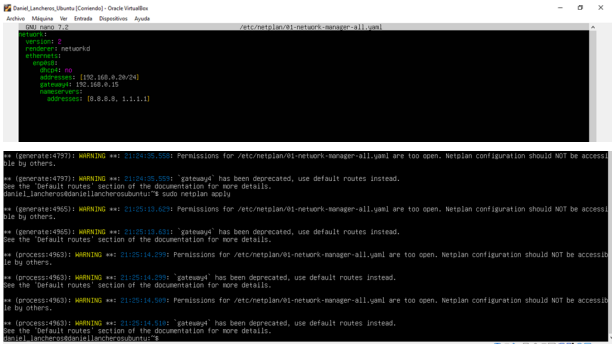
El firewall quedó completamente configurado y funcional, sirviendo como base para las siguientes temáticas del grupo (NAT, DMZ, reglas interzonas, proxy autenticado).

Temática 2: Configuración NAT

2.2.1 Configuración de NAT LAN → WAN:

En esta etapa se configuró la zona **GREEN** (LAN) en el Firewall Endian y se conectó un cliente Ubuntu.

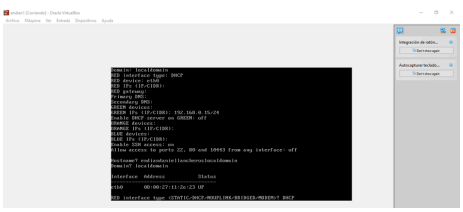
Configuración en Endian (Servidor): Se definió la interfaz eth1 como zona GREEN con la dirección IP estática 192.168.0.15/24. El servicio DHCP se habilitó en esta zona para la gestión de clientes, y el sistema habilitó automáticamente el NAT entre la zona GREEN y RED.



Configuración en Ubuntu (Cliente): Se editó el archivo de configuración de red (Netplan) asignando una IP estática 192.168.0.24 dentro del segmento de la LAN, apuntando como puerta de enlace (gateway) a la IP del Endian (192.168.0.15).

2.2.2 Configuración de NAT DMZ → WAN

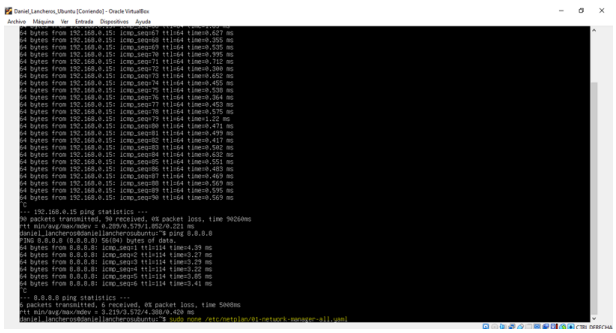
Interfaz RED (WAN): La interfaz de red externa fue configurada en modo DHCP (RED: Interface type DHCP), lo que permite que el Firewall reciba una dirección IP de la red proveedora (simulada en VirtualBox) para salir a Internet.



Mecanismo NAT: El Endian Firewall estableció la regla de enmascaramiento (Source NAT) de forma automática al detectar las zonas, permitiendo que el tráfico generado en las redes internas (LAN/DMZ) salga hacia la WAN utilizando la IP de la interfaz RED.

2.2.3 Verificación de reglas aplicadas

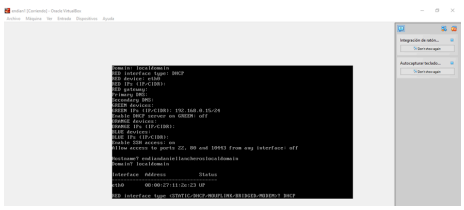
Estado de Interfaces: La consola muestra las interfaces activas con sus respectivas direcciones:



RED: Dispositivo eth0 (Uplink/WAN) activo vía DHCP.

GREEN: Dispositivo eth1 (LAN) activo con IP 192.168.0.15.

Regla NAT: El sistema confirma explícitamente en el log de configuración: "NAT entre GREEN = RED habilitado automáticamente".



2.2.4 Pruebas de conectividad

Se realizaron pruebas de conectividad (ping) desde la máquina cliente (Ubuntu) para validar el funcionamiento del NAT y la resolución DNS.

```
daniel_lancheros@daniellancherosubuntu:~$ 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=114 time=4.36 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=4.27 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=3.31 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=3.28 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=114 time=2.71 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=114 time=3.36 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=114 time=3.57 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6011ms
rtt min/avg/max/mdev = 2.708/3.551/4.364/0.542 ms
daniel_lancheros@daniellancherosubuntu:~$
```

Conectividad Interna (LAN): Se realizó un ping exitoso al Gateway (Endian) en la dirección 192.168.0.15, confirmando comunicación con el firewall.

```
daniel_lancheros@daniellancherosubuntu:~$ ping 192.168.0.15
PING 192.168.0.15 (192.168.0.15) 56(84) bytes of data.
64 bytes from 192.168.0.15: icmp_seq=1 ttl=64 time=1.38 ms
64 bytes from 192.168.0.15: icmp_seq=2 ttl=64 time=0.508 ms
64 bytes from 192.168.0.15: icmp_seq=3 ttl=64 time=0.493 ms
64 bytes from 192.168.0.15: icmp_seq=4 ttl=64 time=0.470 ms
^C
--- 192.168.0.15 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3070ms
rtt min/avg/max/mdev = 0.470/0.713/1.382/0.386 ms
daniel_lancheros@daniellancherosubuntu:~$
```

Conectividad Externa (Internet): Se realizó un ping exitoso al dominio google.com.

```
daniel_lancheros@daniellancherosubuntu:~$ ping google.com
PING google.com (172.217.162.142) 56(84) bytes of data.
64 bytes from gru14s19-in-f14.1e100.net (172.217.162.142): icmp_seq=1 ttl=114 time=3.44 ms
64 bytes from gru14s19-in-f14.1e100.net (172.217.162.142): icmp_seq=2 ttl=114 time=3.25 ms
64 bytes from gru14s19-in-f14.1e100.net (172.217.162.142): icmp_seq=3 ttl=114 time=3.05 ms
64 bytes from gru14s19-in-f14.1e100.net (172.217.162.142): icmp_seq=4 ttl=114 time=2.87 ms
64 bytes from gru14s19-in-f14.1e100.net (172.217.162.142): icmp_seq=5 ttl=114 time=2.61 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 2.607/3.042/3.439/0.290 ms
daniel_lancheros@daniellancherosubuntu:~$
```

Resultado: El sistema resolvió el dominio correctamente y recibió respuesta de los paquetes (0% packet loss), lo que confirma que el NAT está traduciendo las direcciones internas correctamente hacia Internet y el servicio DNS está operativo.

Temática 3: Habilitación de servicios en la DMZ

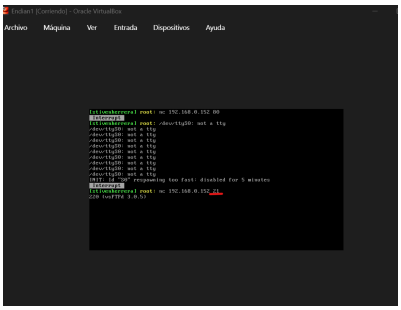
2.3.1 Configuración del servidor Web/FTP en la DMZ

La temática 3 corresponde al desarrollo y validación de permisos HTTP y FTP mediante puertos específicos dentro de una red en específico.

El documento establece la arquitectura lógica, definiendo al servidor Ubuntu con la IP 192.168.0.152 para alojar los servicios FTP y Web.

Validación de servicios activos: Antes de configurar el firewall, se verifica que los puertos están escuchando mediante el comando Netcat desde Endian:

- Web: nc 192.168.0.152 80.
- FTP: nc 192.168.0.152 21.



2.3.2 Permitir servicios HTTP y FTP.

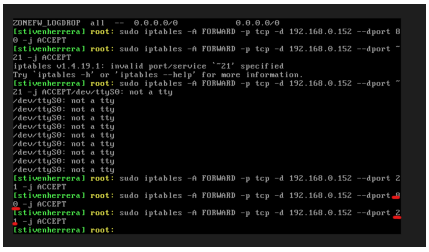
Para permitir el tráfico hacia el servidor Ubuntu (192.168.0.152), se ejecutan las siguientes reglas de iptables en la consola de Endian:

Habilitar HTTP (Puerto 80):

- sudo iptables -A FORWARD -i eth1 -p tcp -d 192.168.0.152 --dport 80 -j ACCEPT

Habilitar FTP (Puerto 21):

- sudo iptables -A FORWARD -p tcp -d 192.168.0.152 --dport 21 -j ACCEPT



2.3.3 Bloqueo de ICMP desde la DMZ

El objetivo es denegar el protocolo ICMP para evitar respuestas a ping. Se configuran las siguientes reglas de rechazo (DROP):

Bloquear paso de ICMP (Forward):

- sudo iptables -A FORWARD -p icmp --icmp-type echo-request -j DROP

Bloquear salida ICMP desde el propio Endian:

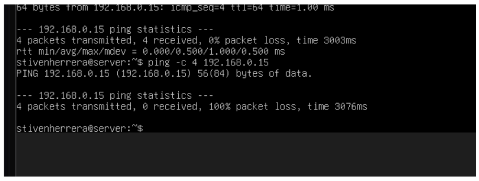
- sudo iptables -A OUTPUT -p icmp --icmp-type echo-request -j DROP

2.3.4 Comprobación mediante clientes LAN

Para validar que las reglas de bloqueo funcionan correctamente:

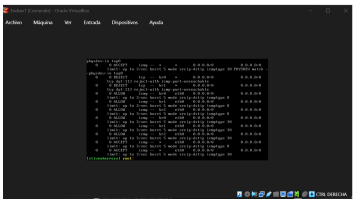
Prueba de Ping: Desde una máquina cliente (o el servidor Ubuntu), se ejecuta ping 192.168.0.15. El resultado debe mostrar paquetes transmitidos pero ninguno recibido (100% packet loss).

Desde el equipo LAN.



Verificación de reglas: En la consola de Endian, se comprueba que las reglas estén activas y contando tráfico con el comando:

sudo iptables -L -v -n | grep "icmp".



Temática 4: Reglas de acceso interzonas

El control de acceso al tráfico de red es un componente de suma importancia en la arquitectura de seguridad perimetral. En esta sección, se describe la metodología empleada para configurar y validar las reglas de filtrado dentro del cortafuegos, con el objetivo de establecer políticas de comunicación específicas entre las zonas de red internas (VERDE y NARANJA) y la red externa (ROJO/WAN), siguiendo las directivas de la práctica colaborativa. La configuración se realizó sobre una plataforma Unified Threat Management (UTM) [10].

2.4.1 Configuración de acceso controlado entre zonas

El primer objetivo de configuración fue establecer una comunicación estricta y controlada entre la Zona Verde (LAN de estaciones de trabajo, VERDE) y la Zona Naranja (Red de Servidores, NARANJA/DMZ). Antes de implementar las reglas específicas, se procedió a eliminar la política predeterminada que permitía cualquier servicio entre estas zonas, reforzando el principio de mínimo privilegio.

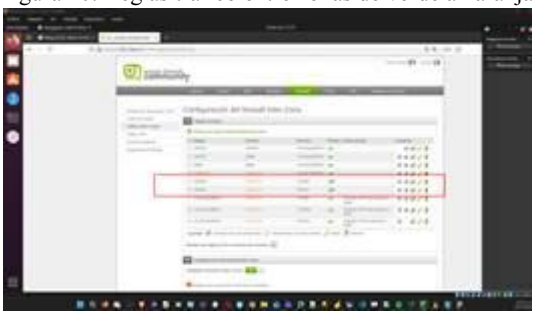
Posteriormente, se crearon dos reglas de tráfico inter-zona (o Inter-Zone Traffic) para autorizar únicamente los servicios necesarios:

- Servicio HTTP: Se estableció una regla para permitir el tráfico con protocolo TCP y puerto 80, con origen en la Zona Verde y destino en la Zona Naranja.

- Servicio FTP: Similarmente, se configuró una regla que autoriza el tráfico para el Protocolo de Transferencia de Archivos (FTP) con protocolo TCP y puerto 21, también con origen verde y destino naranja.

La eliminación de la política permisiva y la posterior creación de las reglas específicas de HTTP y FTP son pasos indispensables para garantizar que solo el tráfico esencial y conocido pueda fluir entre la LAN interna y la DMZ.

Figura 20. Reglas tráfico entre zonas de verde a naranja



Fuente: Autoría propia

2.4.2 Exposición controlada de servicios a la red externa

El siguiente paso consistió en habilitar la comunicación entre la Zona Roja (WAN/Internet) y la Zona Naranja (DMZ), con el propósito de exponer selectivamente los servicios alojados en el servidor de la DMZ (IP 172.16.0.10) hacia Internet. Esta configuración requiere la implementación de tres tipos de reglas: Redirección de Puertos (NAT), Tráfico Inter-Zona y Trafico de salida.

Se implementaron tres reglas de Redirección de Puertos (NAT) para traducir el tráfico entrante a la interfaz WAN (IP 10.0.2.3) del cortafuegos hacia la dirección IP privada del

servidor en la DMZ (172.16.0.10). Estas reglas se activaron para cualquier enlace activo (ANY) en el cortafuegos:

- Redirección HTTP: Tráfico TCP en puerto 80, traducido al servidor 172.16.0.10.
- Redirección HTTPS: Tráfico TCP en puerto 443, traducido al servidor 172.16.0.10.
- Redirección FTP: Tráfico TCP en puerto 21, traducido al servidor 172.16.0.10.

La regla de redirección para HTTP es fundamental, ya que permite que los clientes externos accedan al servidor web utilizando la dirección pública del firewall [11]

Figura 21. Creación de reglas de redirección de puertos

Fuente: Autoría propia

Las reglas NAT solo modifican la dirección IP de destino; por lo tanto, es necesario un segundo conjunto de reglas de Tráfico Inter-Zona que autoricen explícitamente el flujo del tráfico de la Zona Roja hacia la Zona Naranja (destino 172.16.0.10) para los mismos servicios (HTTP, HTTPS, FTP).

Figura 22. Reglas tráfico entre zonas de rojo a naranja

Fuente: Autoría propia

2.4.3 Verificación de la configuración y resultados

Una vez implementadas todas las reglas, se procedió a la verificación del tráfico inter-zona. Endian permitió visualizar las reglas activas tanto para la comunicación VERDE - NARANJA como para ROJO - NARANJA, confirmando que la política de seguridad se encontraba correctamente cargada y en vigor.

Para validar la efectividad de las directivas configuradas, se realizaron una serie de pruebas de acceso utilizando un navegador web y herramientas de línea de comandos, simulando escenarios de tráfico interno y externo, la cuales fueron exitosas. Los resultados obtenidos para cada directiva se detallan a continuación.

Tabla 1. Pruebas de acceso HTTP

Pruebas Servicio HTTP	Origen > Destino	Tipo
LAN > DMZ	Cliente (192.168.0.16) > Server3 (172.16.0.10)	Navegador Web
LAN > WAN	Cliente (192.168.0.16) > Internet (Google)	Navegador Web
DMZ > WAN	Server3 (172.16.0.10) > Internet (Google)	Terminal curl http://google.com
WAN > DMZ	Máquina 'WAN' (10.0.2.15) IP Firewall (10.0.2.3) > Server3 (172.16.0.10)	Navegador Web

Fuente: Autoría propia

Tabla 2. Pruebas de acceso FTP

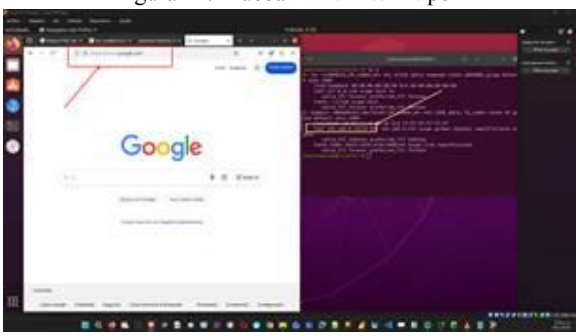
Pruebas Servicio FTP	Origen > Destino	Tipo
LAN > WAN	Cliente (192.168.0.16) > Servidor FTP Externo (Maquina 'WAN' 10.0.2.15)	Terminal fpt 10.0.2.15
WAN > DMZ	Máquina 'WAN' (10.0.2.15) IP Firewall (10.0.2.3) > Server3 (172.16.0.10)	Terminal fpt 10.0.2.3

Fuente: Autoría propia

Figura 23. Prueba LAN > DMZ por HTTP

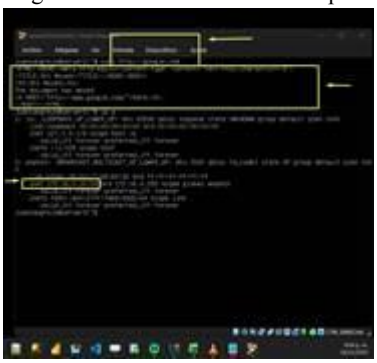
Fuente: Autoría propia

Figura 24. Prueba LAN > WAN por HTTP



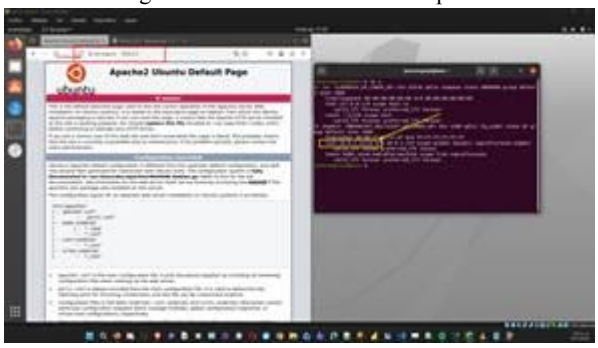
Fuente: Autoría propia

Figura 25. Prueba DMZ > WAN por HTTP



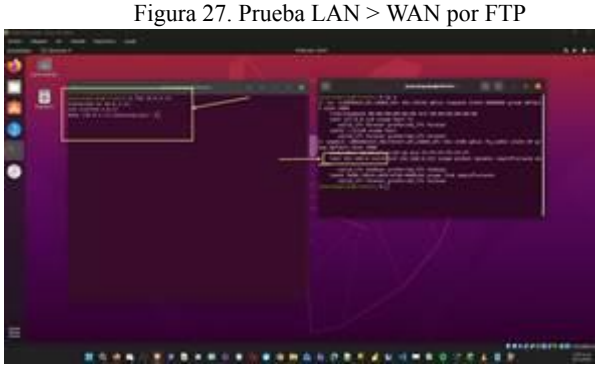
Fuente: Autoría propia

Figura 26. Prueba WAN > DMZ por HTTP



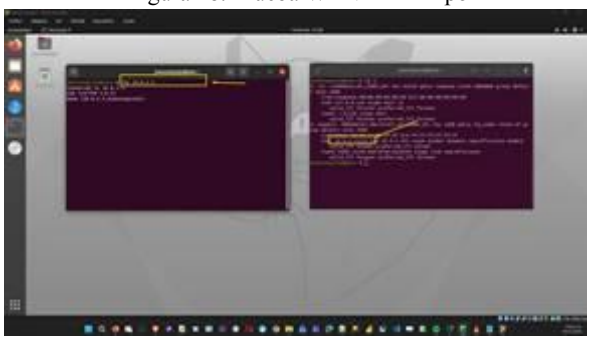
Fuente: Autoría propia

Figura 27. Prueba LAN > WAN por FTP



Fuente: Autoría propia

Figura 28. Prueba WAN > DMZ por FTP



Fuente: Autoría propia

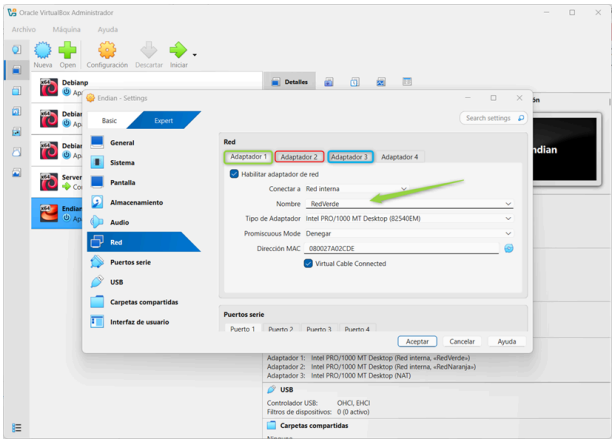
2.5 Temática 5: Implementación de Proxy HTTP

2.5.1 Creación del perfil, lista negra y autenticación (www.hotmail.com, youtube.com, etc.)

1. Instalación y configuración de Endian Firewall

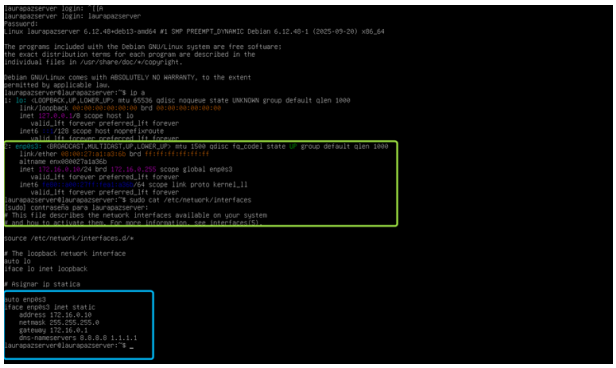
Se instalaron los 3 adaptadores de red:

- **Adaptador 1 (RedVerde)**: Conectado a los desktops.
- **Adaptador 2 (RedNaranja)**: Conectado al servidor.
- **Adaptador 3 (Red NAT)**: Para acceso a Internet.



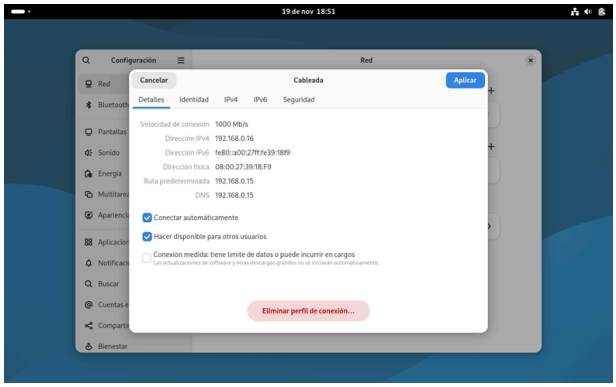
Se asignaron las IP según la información de la temática 1.

Asignación de Ip al Servidor



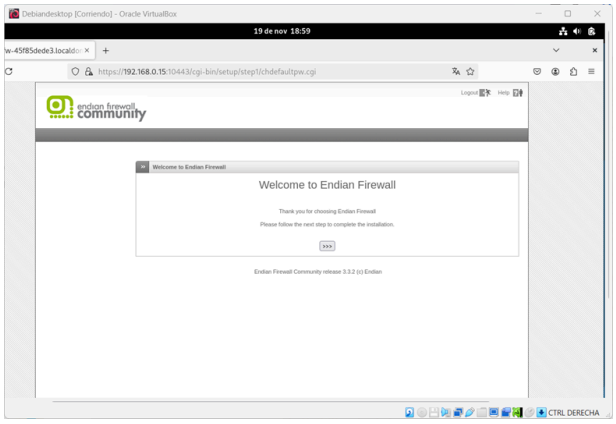
Fuente: Autoría propia

Asignación de Ip al Desktop



Fuente: Autoría propia

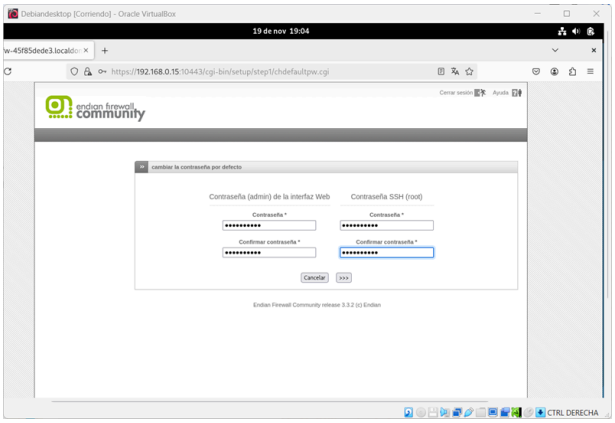
La IP verde fue configurada y verificada, asegurando la navegación desde los desktops hacia el servidor.



Fuente: Autoría propia

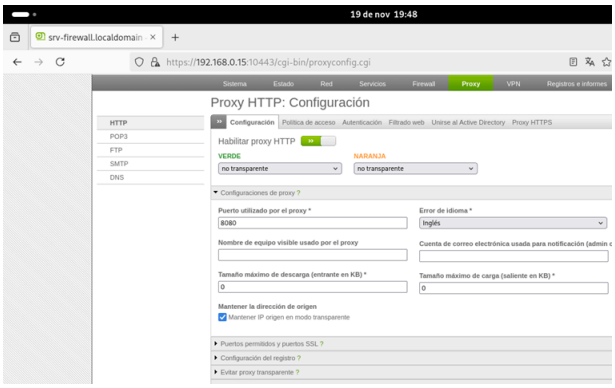
2. Configuración de proxy y firewall

Se inició sesión en Endian con la contraseña: Laura123**



Fuente: Autoría propia

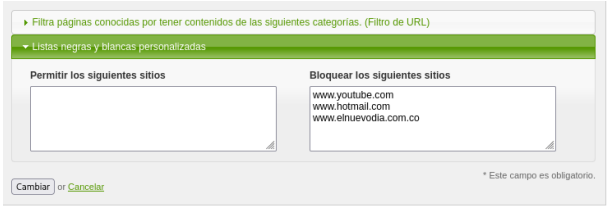
Se activó el **proxy no transparente** para controlar el tráfico web.



Fuente: Autoría propia

Se creó un **perfil de proxy** y se estableció una **lista negra** bloqueando los siguientes sitios:

- www.hotmail.com
- www.youtube.com
- www.elnuevodia.com.co



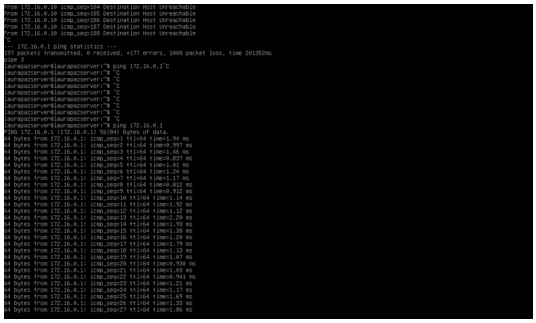
Fuente: Autoría propia

3. Autenticación

Se configuró la autenticación básica para los usuarios que utilicen el proxy, garantizando que solo los usuarios autorizados puedan navegar.

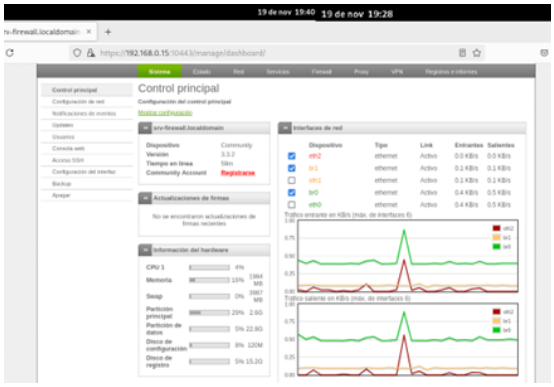
2.5.2 Configuración del usuario y grupo

- Se verificó que los desktops recibieron IP automáticamente desde Endian.
- Desde el servidor se configuró el adaptador 2 (Red Naranja) con IP: 172.16.0.1



Fuente: Autoría propia

- Se comprobó que los usuarios autorizados del grupo pudieran navegar correctamente mediante el proxy.
- Solo los usuarios autenticados y pertenecientes al grupo definido tienen acceso a Internet, respetando las restricciones de la lista negra.

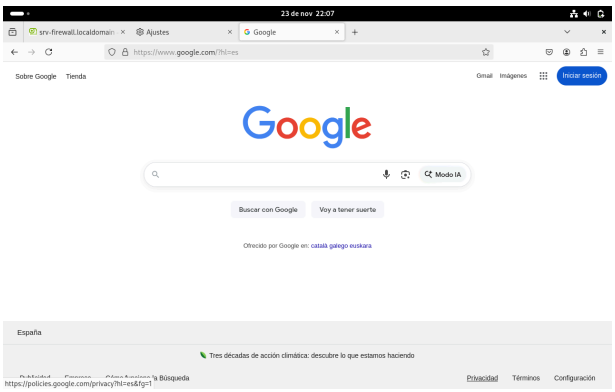


Fuente: Autoría propia

2.5.3 Pruebas de navegación con proxy

1. Prueba de acceso permitido

Se intentó navegar a sitios permitidos (por ejemplo: google.com) y el acceso fue exitoso.

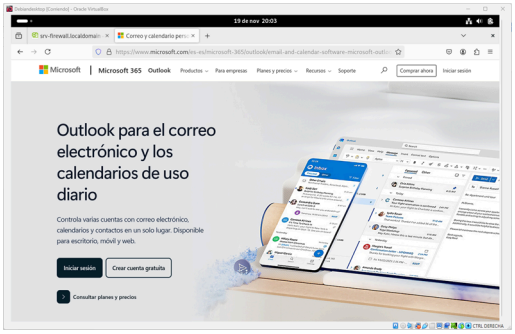


Fuente: Autoría propia

2. Prueba de lista negra

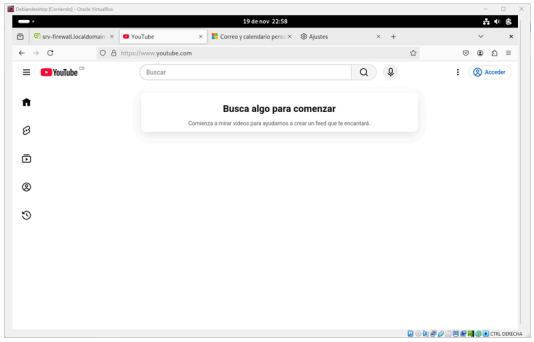
Se intentó acceder a:

- www.hotmail.com



Fuente: Autoría propia

- www.youtube.com

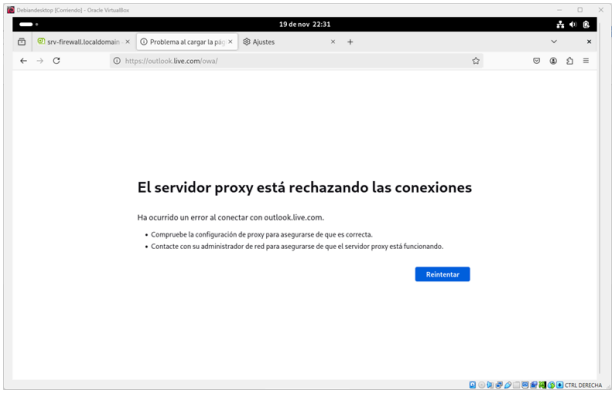


Fuente: Autoría propia

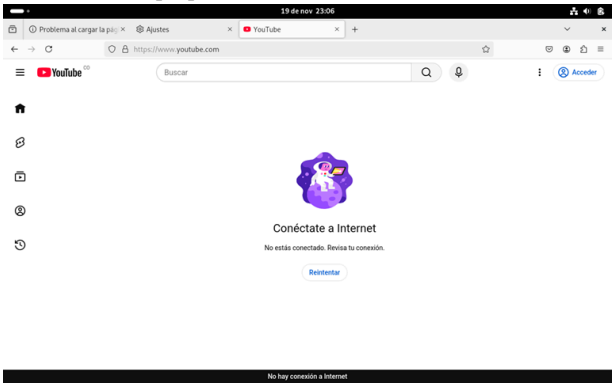
- www.elnuevodia.com.co

Fuente: Autoría propia

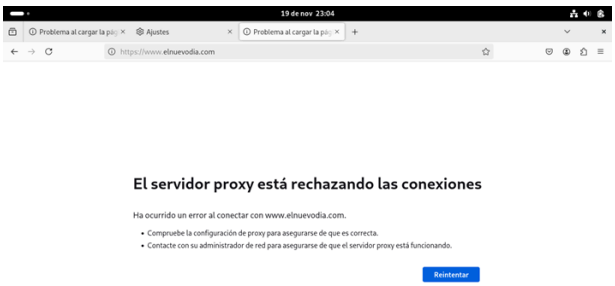
Todas las páginas fueron bloqueadas correctamente por el proxy.



Fuente: Autoría propia



Fuente: Autoría propia



Fuente: Autoría propia

1. Prueba de autenticación

- Se verificó que los usuarios debían ingresar usuario y contraseña para navegar.
- Solo los usuarios autorizados pudieron navegar mientras que los no autorizados fueron bloqueados.

2.1.8 Conclusiones.

Temática 1:La instalación y configuración inicial de Endian Firewall permitió habilitar correctamente las zonas GREEN, ORANGE y RED, estableciendo la estructura base de seguridad perimetral del proyecto. Las pruebas de conectividad confirmaron que el firewall enruta y protege el tráfico interno de manera adecuada. Esta temática proporcionó los fundamentos necesarios para que las siguientes actividades implementen NAT, DMZ, reglas de acceso y proxy dentro de un entorno GNU/Linux.

Temática 2: La práctica permitió configurar exitosamente el NAT en la distribución Endian Firewall, logrando establecer una comunicación segura y segmentada entre las zonas LAN, WAN y DMZ . Se verificó el correcto funcionamiento del NAT dinámico para permitir el acceso a Internet desde la red interna, así como la implementación de reglas de reenvío de puertos para publicar servicios de la DMZ sin comprometer la seguridad de la LAN . Este ejercicio validó la importancia de la segmentación de red y la administración de firewalls para proteger la infraestructura crítica en entornos corporativos.

Temática 3: El desarrollo de la Temática 3 me permitió comprender la importancia de la seguridad perimetral mediante la segmentación de la red en zonas (WAN, LAN y DMZ) utilizando Endian como pasarela central. A través de la configuración práctica con iptables, entendí cómo gestionar el tráfico de manera granular: habilitando servicios críticos como Web y FTP hacia el servidor, mientras fortalecer la defensa ocultando la topología de la red al bloquear protocolos de reconocimiento como ICMP (ping)

Temática 4: La implementación de las reglas de acceso demostró la capacidad de la plataforma UTM Endian, para aplicar políticas de seguridad granulares. Se logró migrar de una configuración permisiva a un modelo de "denegación por defecto" entre zonas, habilitando selectivamente los protocolos HTTP y FTP. Particularmente, la combinación de reglas de Port Redirection (NAT) y Inter-Zone Traffic fue exitosa al exponer los servicios de la DMZ hacia la WAN de manera

controlada, validando que el servidor puede ser accedido externamente (WAN a DMZ) y puede iniciar comunicación hacia el exterior (DMZ a WAN) solo para los servicios autorizados, lo cual es esencial para una postura de seguridad robusta.

2.1.9 CITAS Y/O REFERENCIAS

Las citas y/o referencias se colocarán al final del manuscrito. Utilice Times News Roman, 8 pts, espacio simple. Para ayudar a los lectores, evite notas a pie de página que incluyen las observaciones periféricas necesarias en el texto (dentro de paréntesis, si usted prefiere, como en esta oración). Las citas deberán de respetar el orden de aparición en las referencias.

Se colocarán entre corchetes Ej. [2].

Si es preciso mencionar los nombres de los autores deberán de aparecer todos los nombres exceptuando si el numero de éstos es más de cuatro, en tal caso se pondrá el nombre del primer autor y la leyenda ‘et al’.

Si la frase inicia citando la referencia entonces puede utilizar el formato Ref. [4], en otro caso utilice solo [4].

Las referencias electrónicas (URL) deben seguir el formato mostrado en [6].

3 REFERENCIAS

[1] Endian, *Endian Firewall Community Documentation*, Endian.com, 2020. [Online]. Available: https://docs.endian.com

[2] Oracle Corporation, *Oracle VM VirtualBox User Manual*, Oracle, 2023. [Online]. Available: https://www.virtualbox.org/manual

[3] Linux Professional Institute (LPI), *Linux Essentials Study Guide*, LPI, 2022. [Online]. Available: https://learning.lpi.org

[4] E. H. Miller, *“A note on reflector arrays”*, IEEE Trans. Antennas Propagat., Aceptado para su publicación.

[5] *Control Toolbox* (6.0), User´s Guide, The Math Works, 2001, pp. 2-10-2-35.

[6] J. Jones. (2007, Febrero 6). Networks (2nd ed.) [En línea]. Disponible en: http://www.atm.com.

[7] The Netfilter Project, The netfilter/iptables project homepage, Netfilter.org, 2025. [Online]. Available: https://www.netfilter.org/documentation/

[8] Canonical. (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. https://help.ubuntu.com/20.04/ubuntu-help/index.html

[9] Endian. (2020). Endian Firewall Community Edition [Software de cómputo]. https://www.endian.com/community/

[10] Endian, "Endian UTM 3.2 Manual referencia," 2016. [Online]. Disponible en: http://docs.endian.com/3.2/utm/index.html.

[11] W. R. Cheswick, S. M. Bellovin y R. L. R., Firewalls and Internet Security: Protecting Your Network, 2ª ed. Boston: Addison-Wesley Professional, 2003.