IMPLEMENTACIÓN DE ENDIAN UTM PARA LA GESTIÓN DE REGLAS DE TRÁFICO EN REDES LAN Y DMZ

Doly Lorena Salazar Cabra
e-mail: dlsalazarca@unadvirtual.edu.co
Yeiner Alcedis Ochoa Martinez
e-mail: yaochoama@unadvirtual.edu.co
Sandra Patricia Romero Cano
e-mail: spromeroc@unadvirtual.edu.co
Jerferson David Chaparro Gualteros
e-mail: jdchaparrog@unadvirtual.edu.co
Sandra Milena López Benavides
e-mail: smlopezben@unadvirtual.edu.co

RESUMEN: *Este informe presenta el proceso de instalación y configuración del sistema Endian UTM en un entorno virtualizado, con el objetivo de implementar reglas de acceso que permitan o restrinjan el tráfico de red entre zonas LAN, WAN y DMZ. Se realizaron pruebas de conectividad, configuración de reglas NAT y Port Forwarding, así como la verificación de logs, logrando una gestión efectiva del tráfico HTTP y FTP en una red corporativa simulada. Este procedimiento busca fortalecer la comprensión de arquitecturas de red seguras en entornos educativos y de pruebas.*

PALABRAS CLAVE:
Debian, DMZ, NAT, virtualización.

1 INTRODUCCIÓN

La seguridad en redes informáticas es un aspecto fundamental en la infraestructura tecnológica de cualquier organización. En el presente informe se describe el trabajo realizado por el grupo entorno a la instalación, configuración y prueba de la distribución Endian UTM como firewall perimetral. La actividad incluyó la creación de una máquina virtual, la configuración de múltiples interfaces de red (RED, GREEN y ORANGE), así como la implementación de reglas para controlar el tráfico entre zonas de red. Este ejercicio práctico refuerza los conocimientos adquiridos en administración de sistemas Linux y fortalece las capacidades técnicas para entornos empresariales.

2 DESARROLLO TEMATICAS

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

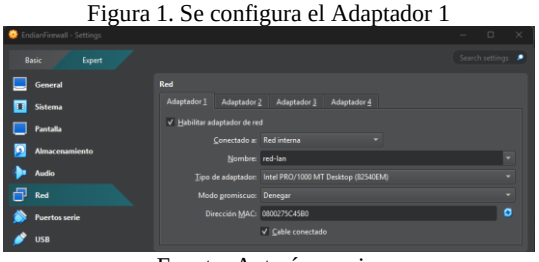
Para llevar a cabo la implementación práctica descrita en este estudio, fue necesario contar con una infraestructura de pruebas basada en software libre y herramientas de virtualización. El sistema anfitrión utilizado correspondió a las distribuciones Ubuntu 24.04.2 LTS y Ubuntu 24.10, seleccionadas por su estabilidad, compatibilidad con entornos de desarrollo y soporte comunitario. La virtualización se realizó mediante Oracle VirtualBox, en su versión 7.1.6, que permitió la creación y gestión de múltiples máquinas virtuales con distintas configuraciones de red. Como sistema operativo para el firewall perimetral, se empleó la imagen ISO de la distribución Endian Firewall Community 3.3.2, [1], una solución UTM de código abierto ampliamente reconocida por su facilidad de configuración, robustez y funcionalidades orientadas a la seguridad perimetral. Esta combinación de herramientas proporcionó un entorno flexible y controlado para llevar a cabo las pruebas de segmentación de red, configuración de interfaces y aplicación de políticas de seguridad.

Se configuran las tres interfaces de Red en VirtualBox.

- eth0 (GREEN): Modo Red interna, conectada a la LAN virtual.
- eth1(RED): Modo NAT, conecta a internet.
- eth2(ORANGE): Modo Red interna, conectada a servidores en la DMZ.

Las redes internas fueron definidas como GREEN: red-lan, ORANGE: red-dmz.

Figura 1. Se configura el Adaptador 1

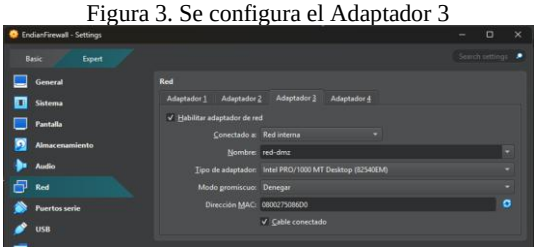


Fuente: Autoría propia.

Figura 2. Se configura el Adaptador 2

Fuente: Autoría propia.

Figura 3. Se configura el Adaptador 3

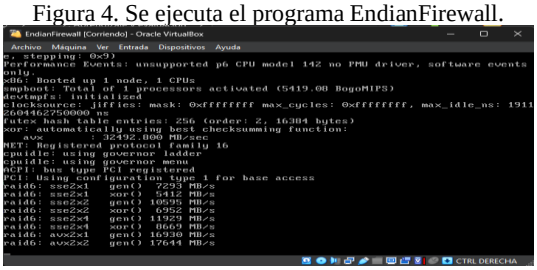


Fuente: Autoría propia.

La instalación de Endian fue realizada utilizando una imagen ISO montada como unidad de CD. El procedimiento incluyó la ejecución del instalador, la selección del idioma y la asignación de las interfaces de red:

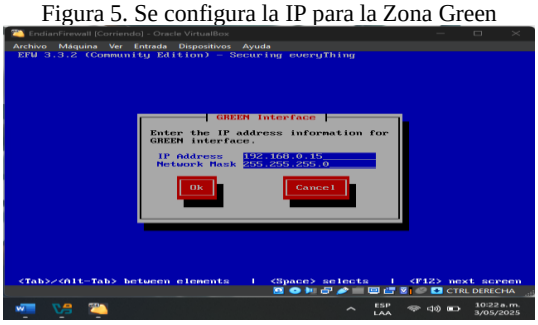
- GREEN eth0 192.168.0.15/24
- RED eth1 (DHCP automático)
- ORANGE eth2 192.168.1.10/24

Figura 4. Se ejecuta el programa EndianFirewall.



Fuente: Autoría propia.

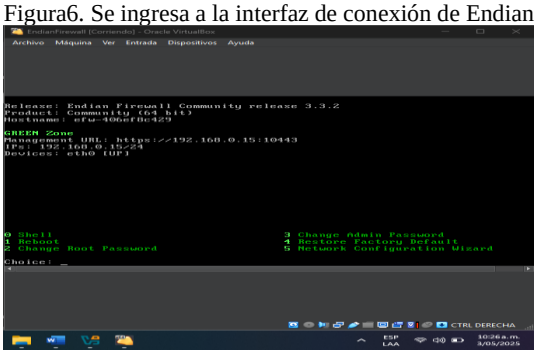
Figura 5. Se configura la IP para la Zona Green



Fuente: Autoría propia.

Una vez realizadas las configuraciones conforme a las instrucciones, Endian se reinicia y presenta la interfaz de conexión.

Figura6. Se ingresa a la interfaz de conexión de Endian



Fuente: Autoría propia

Desde otras máquinas virtuales conectadas a las redes LAN y DMZ se validó lo siguiente:

- Acceso a la interfaz web de Endian desde la zona GREEN.
- Conectividad por ping desde DMZ hacia la zona GREEN.
- Verificación de conexión a Internet en la zona GREEN.

Primero, se accede al sistema Ubuntu Desktop, donde se introduce la dirección IP correspondiente a la interfaz GREEN. Al hacerlo, se redirecciona a una página de advertencia de seguridad, la cual se acepta para continuar [2]. A continuación, se muestra la página de instalación de Endian, en la que se siguen los pasos y configuraciones establecidas. Finalizado el proceso, se accede a la página principal de Endian en la web, verificando así la conexión con la zona GREEN.

Figura 7. Se conecta a la Red-LAN en Ubuntu Desktop [3].

Fuente: Autoría propia.

Figura 8. Visualización de una página de advertencia en el entorno Ubuntu Desktop.

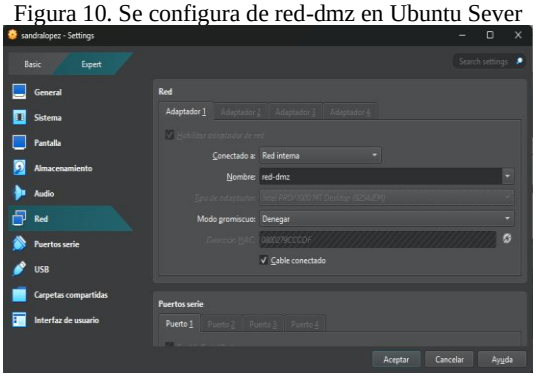
Fuente: Autoría propia.

Figura 9. Ingreso a la interfaz web de Endian

Fuente: Autoría propia.

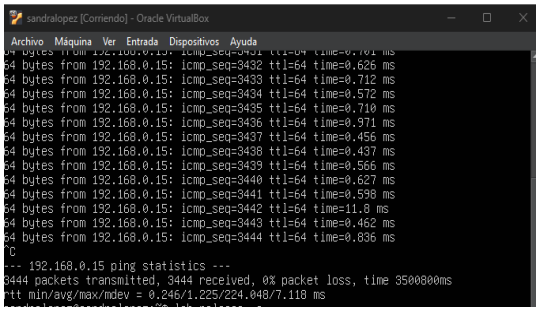
Para verificar la conectividad desde la zona DMZ hacia la zona GREEN, se accede a una máquina virtual ubicada en la DMZ y se ejecuta el comando ping dirigido a la dirección IP de la interfaz GREEN. Una respuesta exitosa confirma que existe comunicación entre ambas zonas.

Figura 10. Se configura de red-dmz en Ubuntu Sever



Fuente: Autoría propia.

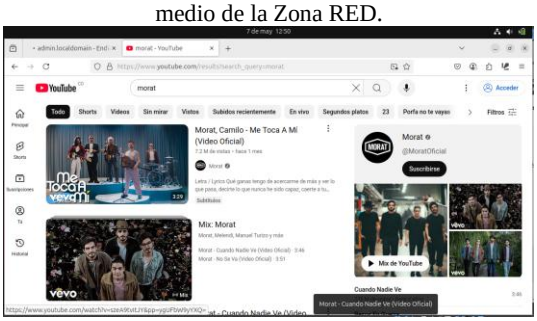
Figura 11. Se hace Ping desde Ubuntu Server a IP de la Zona Green



Fuente: Autoría propia.

Para verificar la conexión a Internet en la zona GREEN, se accede a Ubuntu Desktop donde esta conectada dicha zona y se abre un navegador web para acceder a un sitio externo. Si se obtiene respuesta o se carga la página, se confirma que hay acceso a Internet desde GREEN

Figura 12. Se conecta a internet desde Ubuntu Desktop por medio de la Zona RED.



Fuente: Autoría propia.

2.2 TEMÁTICA 2: CONFIGURACIÓN NAT

Se presenta la implementación y la configuración de las reglas NAT mediante el uso de Endian firewall en un entorno virtualziado conformado por tres zonas: Green (LAN), Orange (DMZ) y red (WAN). La configuración permite habilitar y demostrar la comunicación saliente desde la LAN y la DMZ hacia la red WAN simulada, así como el reenvío de puertos para el acceso a servicios alojados en la DMZ. Para la validación del entorno se utiliza Ubuntu Desktop como cliente en la zona Green y Ubuntu Server como servidor en la zona Orange, montados sobre máquinas virtuales.

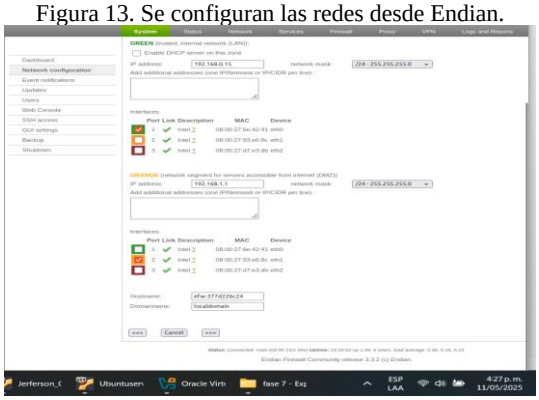
Para ello tenemos en cuenta la arquitectura de red.

- Ubuntu desktop: 192.168.0.15/24
- Ubuntu server: 192.168.1.0/24
- Endian: Dispositivo que conecta todas las zonas y configura las reglas NAT.
- Red WAN: Ip publica simulada.

Configuración inicial de Endian, se accede al Ubuntu desktop por medio del navegador web, con la ip de la configuración de instalación que se da dentro de Endian. https://192.168.0.15:10443

Una vez completada la instalación del sistema, se accedió a la interfaz de configuración de Endian Firewall a través del navegador web. Desde esta interfaz, se procedió a la configuración de las tres zonas de red definidas por la arquitectura de seguridad: RED (WAN), GREEN (LAN) y ORANGE (DMZ). La interfaz correspondiente a la zona RED fue configurada para obtener su dirección IP de forma automática mediante el protocolo DHCP, permitiendo así la conexión con redes externas o proveedores de servicios de Internet. Por otro lado, se asignaron direcciones IP estáticas a las interfaces GREEN y ORANGE, correspondientes a la red local interna y a la zona desmilitarizada, respectivamente. Esta segmentación de red es fundamental para aplicar políticas de control de tráfico diferenciadas, garantizando un mayor nivel de seguridad y aislamiento entre los distintos entornos de red.

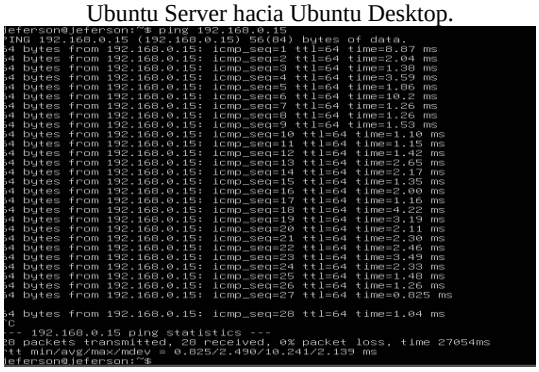
Figura 13. Se configuran las redes desde Endian.



Fuente: Autoría propia.

Se verifica la conectividad desde la zona DMZ hacia la zona Green mediante el uso de la herramienta *ping*, comprobando la comunicación entre el servidor Ubuntu (en la zona Orange/DMZ) y el cliente Ubuntu Desktop (en la zona Green/LAN).

Figura 14. Conectividad establecida desde la instancia de Ubuntu Server hacia Ubuntu Desktop.



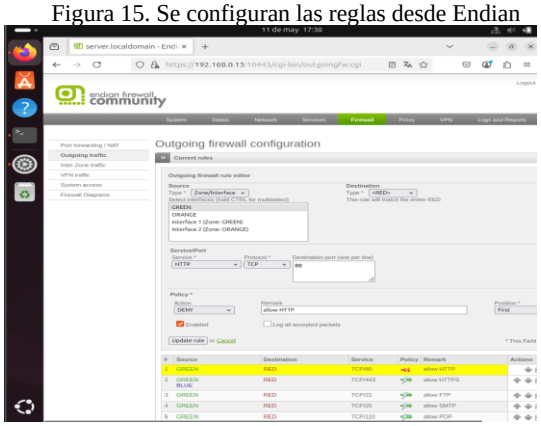
```
jeferson@jeferson:~$ ping 192.168.0.15
PING 192.168.0.15 (192.168.0.15) 56(84) bytes of data.
64 bytes from 192.168.0.15: icmp_seq=1 ttl=64 time=8.87 ms
64 bytes from 192.168.0.15: icmp_seq=2 ttl=64 time=2.04 ms
64 bytes from 192.168.0.15: icmp_seq=3 ttl=64 time=1.38 ms
64 bytes from 192.168.0.15: icmp_seq=4 ttl=64 time=3.59 ms
64 bytes from 192.168.0.15: icmp_seq=5 ttl=64 time=1.86 ms
64 bytes from 192.168.0.15: icmp_seq=6 ttl=64 time=10.2 ms
64 bytes from 192.168.0.15: icmp_seq=7 ttl=64 time=1.26 ms
64 bytes from 192.168.0.15: icmp_seq=8 ttl=64 time=1.26 ms
64 bytes from 192.168.0.15: icmp_seq=9 ttl=64 time=1.53 ms
64 bytes from 192.168.0.15: icmp_seq=10 ttl=64 time=1.10 ms
64 bytes from 192.168.0.15: icmp_seq=11 ttl=64 time=1.15 ms
64 bytes from 192.168.0.15: icmp_seq=12 ttl=64 time=1.42 ms
64 bytes from 192.168.0.15: icmp_seq=13 ttl=64 time=2.65 ms
64 bytes from 192.168.0.15: icmp_seq=14 ttl=64 time=2.17 ms
64 bytes from 192.168.0.15: icmp_seq=15 ttl=64 time=1.35 ms
64 bytes from 192.168.0.15: icmp_seq=16 ttl=64 time=2.00 ms
64 bytes from 192.168.0.15: icmp_seq=17 ttl=64 time=1.26 ms
64 bytes from 192.168.0.15: icmp_seq=18 ttl=64 time=4.22 ms
64 bytes from 192.168.0.15: icmp_seq=19 ttl=64 time=3.19 ms
64 bytes from 192.168.0.15: icmp_seq=20 ttl=64 time=2.11 ms
64 bytes from 192.168.0.15: icmp_seq=21 ttl=64 time=2.30 ms
64 bytes from 192.168.0.15: icmp_seq=22 ttl=64 time=2.46 ms
64 bytes from 192.168.0.15: icmp_seq=23 ttl=64 time=3.49 ms
64 bytes from 192.168.0.15: icmp_seq=24 ttl=64 time=2.33 ms
64 bytes from 192.168.0.15: icmp_seq=25 ttl=64 time=1.48 ms
64 bytes from 192.168.0.15: icmp_seq=26 ttl=64 time=1.26 ms
64 bytes from 192.168.0.15: icmp_seq=27 ttl=64 time=0.825 ms

64 bytes from 192.168.0.15: icmp_seq=28 ttl=64 time=1.04 ms
^C
--- 192.168.0.15 ping statistics ---
28 packets transmitted, 28 received, 0% packet loss, time 27054ms
rtt min/avg/max/mdev = 0.825/2.490/10.241/2.139 ms
jeferson@jeferson:~$
```

Fuente : Autoria propia.

Posteriormente, se configuró una regla de firewall que permite el acceso a Internet desde la red local (GREEN). Esta regla tiene como objetivo habilitar la navegación web para los dispositivos conectados a la red interna, garantizando al mismo tiempo que el tráfico saliente esté controlado por las políticas de seguridad establecidas. Para ello, se definió una política de acceso que autoriza el tráfico saliente desde la zona GREEN hacia la zona RED (WAN), especificando los protocolos necesarios, como HTTP y HTTPS. Esta configuración representa una de las reglas fundamentales en un entorno de red segmentado, ya que permite la conectividad hacia el exterior sin comprometer la integridad de las zonas internas de la red.

Figura 15. Se configuran las reglas desde Endian



Fuente : Autoria propia.

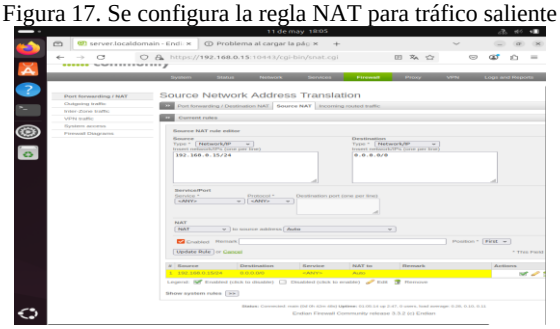
A continuación, se configura una regla de tráfico saliente que define los destinos permitidos. En este caso, se especifican tres direcciones IP correspondientes a servidores de Google. En los campos de servicio y protocolo se selecciona HTTP y TCP, respectivamente. Finalmente, se establece la acción *Allow* para permitir todo el tráfico HTTP sobre el protocolo TCP hacia los servidores especificados desde la red local.

Figura 16. Se configuran las reglas de tráfico.

Fuente: Autoría propia.

Se agrega una nueva regla de NAT que permite que todo el tráfico saliente desde las redes internas utilice la dirección IP de la interfaz de salida como dirección de origen. En esta configuración, se especifica la dirección IP de la zona Green como origen y se define la dirección de destino como 0.0.0.0/0, lo cual habilita el acceso a cualquier destino en Internet.

Figura 17. Se configura la regla NAT para tráfico saliente



Fuente: Autoría propia.

Es posible visualizar todas las configuraciones y reglas establecidas para NAT, así como verificar el acceso a Internet. Posteriormente, se reinicia la máquina virtual con el fin de validar la correcta activación de los servicios.

Figura 18. Listado de configuraciones y reglas para NAT

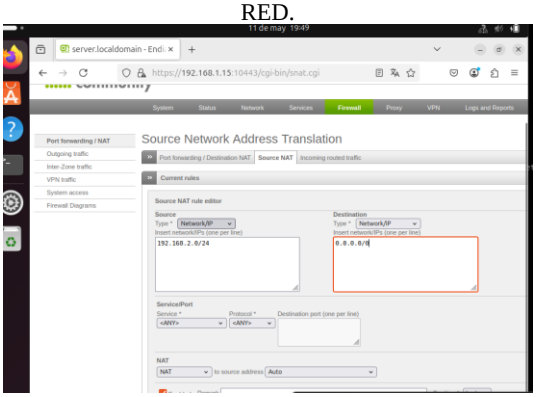
Fuente: Autoría propia.

Después de reiniciar la máquina, se confirmó el acceso a Internet. Se configura la regla de NAT para establecer la comunicación desde la zona DMZ hacia Internet. Para ello, en la sección de Reenvío de Puertos / NAT, se define una ruta de salida desde la zona ORANGE hacia la dirección 0.0.0.0, correspondiente al acceso a Internet.

Figura 19. Acceso a internet desde Ubuntu Desktop

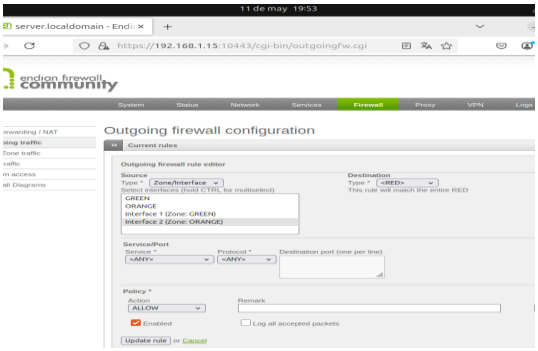
Fuente: Autoría propia.

Figura 20. Regla NAT configurada para permitir el enrutamiento del tráfico desde la zona DMZ hacia la zona RED.



Fuente: Autoría propia.

Figura 21. Regla NAT aplicada para habilitar la comunicación desde la zona DMZ hacia la zona RED.



Fuente: Autoría propia.

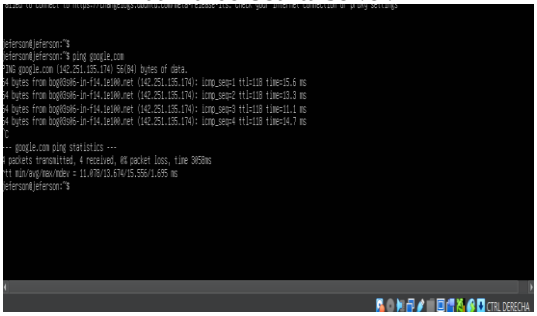
Configuración de una regla de tráfico saliente que permite a la zona ORANGE establecer conexión con la red y acceder a todos sus servicios.

Figura 22. Establecimiento de conexión desde la zona ORANGE hacia la zona RED.

Fuente: Autoría propia.

Se verifica que el servidor Ubuntu en la zona ORANGE realiza correctamente ping hacia la zona RED, así como hacia Internet. La salida hacia la red WAN se realiza a través de la regla configurada, la cual permite el acceso desde la zona ORANGE a cualquier servicio externo.

Figura 23. Acceso a Internet desde la zona ORANGE utilizando Ubuntu Server.



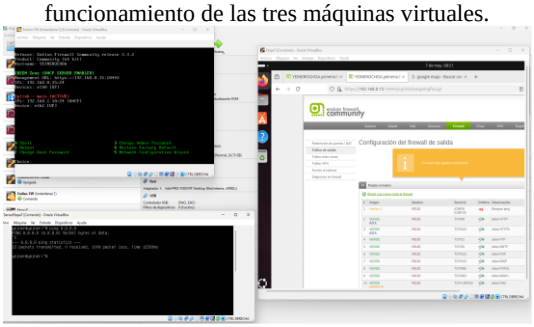
Fuente: Autoría propia.

2.3 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

Se trabajó con tres máquinas virtuales: un servidor Ubuntu (DMZ), un cliente Desktop (LAN) y Endian Firewall (controlador central). Las interfaces fueron configuradas como sigue: Verde (192.168.0.0/24), Naranja (172.16.0.0/24) y Roja (Internet, modo puente). En Endian se habilitó Masquerading para permitir salida desde la zona Naranja y se aplicaron reglas de firewall para permitir los puertos 80 (HTTP) y 21 (FTP) desde la DMZ hacia la zona ROJA.

Adicionalmente, se bloqueó el protocolo ICMP (echo-request) creando una regla de denegación específica. En el servidor Ubuntu se instaló el servicio vsftpd y se comprobó el acceso desde el cliente Desktop por medio de conexión FTP. Asimismo, se validó el acceso web desde la DMZ mediante el navegador y se ejecutó un ping a 8.8.8.8 para comprobar el bloqueo.

Figura 24. La imagen muestra simultáneamente el funcionamiento de las tres máquinas virtuales.



Fuente: Autoría propia.

La imagen muestra simultáneamente el funcionamiento de las tres máquinas virtuales implicadas en la implementación del escenario de seguridad con Endian Firewall:

En la parte superior izquierda se observa la consola de la máquina Endian-FW, donde se confirma que las interfaces de red están correctamente activadas: la interfaz verde (LAN) con IP 192.168.0.15 y la interfaz roja (WAN) con IP dinámica en el segmento 10.0.2.0/24.

En la parte inferior se encuentra la terminal del servidor en la zona DMZ (NARANJA), ejecutando un ping hacia 8.8.8.8, el cual falla, demostrando que la regla de denegación ICMP está funcionando correctamente.

A la derecha se visualiza la interfaz web del firewall Endian desde el cliente Desktop, específicamente en la sección de reglas de salida, donde se aplicaron y activaron múltiples reglas para permitir servicios (HTTP, HTTPS, DNS, FTP, etc.) y denegar ICMP desde NARANJA, tal como exige la guía.

Figura 25. Prueba de ping fallida desde la zona DMZ.

Fuente: Autoría propia

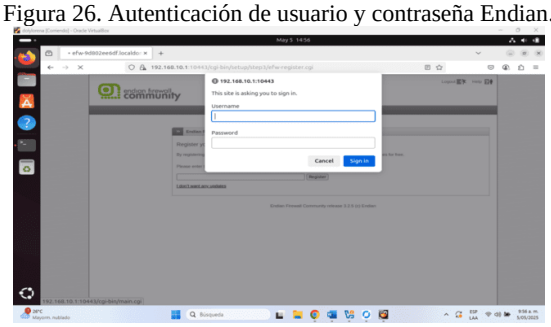
Muestra que el bloqueo ping funciona correctamente.

2.4 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO.

Como producto de la actividad, se estableció la configuración de reglas de acceso en el firewall con el objetivo de ejercer un control preciso sobre el tráfico de red. Este proceso incluyó la definición de políticas de seguridad orientadas a permitir únicamente servicios legítimos y a bloquear aquellos considerados no deseados o potencialmente peligrosos. Las reglas fueron especificadas según puertos y protocolos, con el fin de aplicar un filtrado detallado del tráfico entre zonas. Se incorporó el uso de traducción de direcciones de red (NAT) para la redirección adecuada del tráfico hacia servicios internos. Además, se llevó a cabo la verificación del funcionamiento mediante el análisis de registros del sistema y la ejecución de pruebas de conectividad, asegurando con ello la efectividad y robustez de las medidas implementadas.

Al acceder a la interfaz de administración, se solicita un nombre de usuario y una contraseña. Una vez ingresadas las credenciales correspondientes, se procede a iniciar sesión mediante la opción Sign In.

Figura 26. Autenticación de usuario y contraseña Endian.



Fuente: Autoría propia.

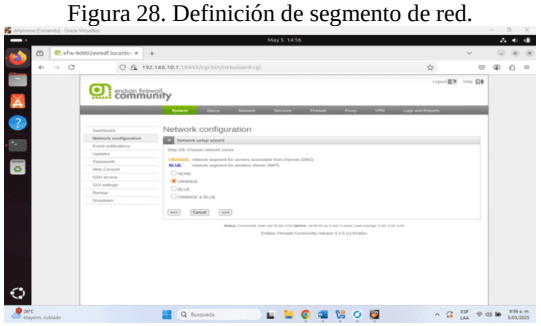
Desde el módulo Network Configuration, se configura la interfaz RED con asignación automática mediante DHCP.

Figura 27. Configuración de RED en modo DHCP.

Fuente: Autoría propia.

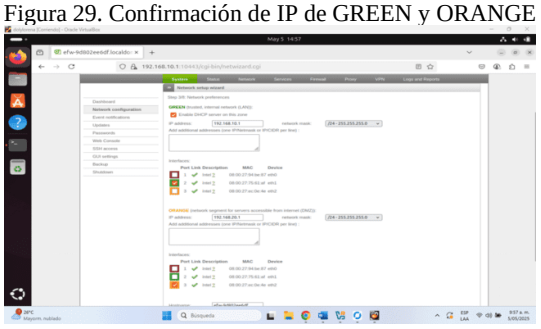
En esta etapa, se configuró el tipo de red correspondiente a cada una de las zonas del firewall. Se seleccionó la interfaz ORANGE para definir el segmento de red destinado a la zona desmilitarizada (DMZ), permitiendo así la exposición controlada de servicios hacia Internet sin comprometer la seguridad de la red interna. Se confirman las IP de GREEN 192.168.10.1 y ORANGE 192.168.20.1.

Figura 28. Definición de segmento de red.



Fuente: Autoría propia.

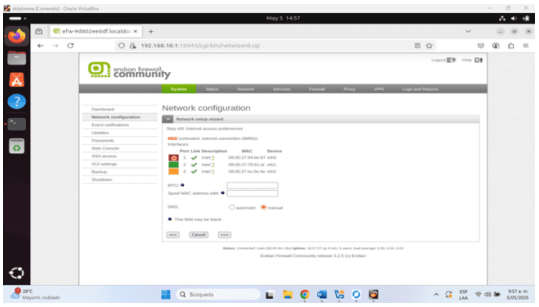
Figura 29. Confirmación de IP de GREEN y ORANGE



Fuente: Autoría propia.

De manera similar, se confirmó la configuración de la interfaz RED para obtener su dirección IP mediante el protocolo DHCP, lo cual permite la conectividad automática con redes externas o proveedores de servicios de Internet.

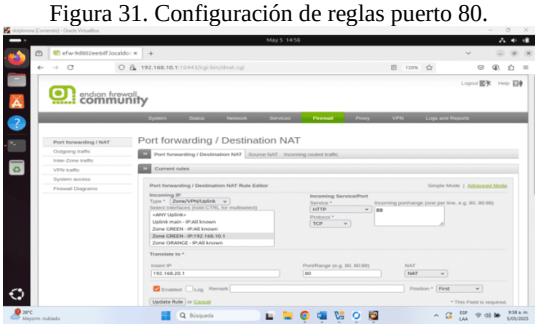
Figura 30. Confirmación de configuración de RED en DHCP.



Fuente: Autoría propia.

Configuración de reglas de Port Forwarding para permitir tráfico HTTP (puerto 80) desde la LAN hacia la DMZ en un firewall Endian.

Figura 31. Configuración de reglas puerto 80.

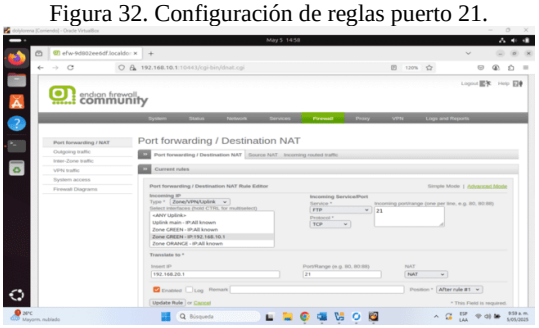


Fuente: Autoría propia

Configuración de reglas de Port Forwarding para permitir tráfico FTP (puerto 21) desde la LAN hacia la DMZ en un firewall Endian.

Reglas NAT aplicadas para permitir el tráfico HTTP (puerto 80) y FTP (puerto 21) hacia la IP interna en la zona DMZ.

Figura 32. Configuración de reglas puerto 21.



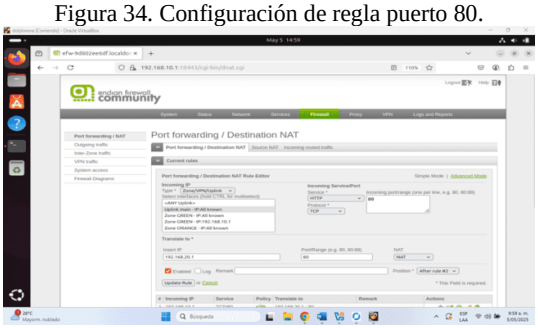
Fuente: Autoría propia.

Figura 33. Reglas guardadas y aplicadas.

Fuente: Autoría propia.

Reglas NAT aplicadas para permitir el tráfico HTTP (puerto 80) y FTP (puerto 21) hacia la IP interna en la zona DMZ. Configuración de reglas de Port Forwarding para permitir tráfico HTTP (puerto 80) desde la RED hacia la DMZ en un firewall Endian.

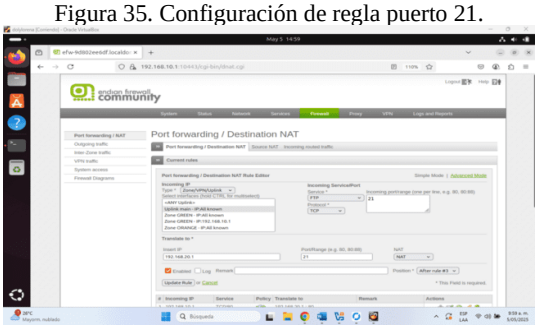
Figura 34. Configuración de regla puerto 80.



Fuente: Autoría propia.

Configuración de reglas de Port Forwarding para permitir tráfico HTTP (puerto 21) desde la RED hacia la DMZ en un firewall Endian.

Figura 35. Configuración de regla puerto 21.



Fuente: Autoría propia.

Reglas NAT aplicadas para permitir el tráfico HTTP (puerto 80) y FTP (puerto 21) hacia la IP interna en la zona DMZ.

Figura 36. Reglas guardadas y aplicadas.

Fuente: Autoría propia.

Se realizó la verificación en tiempo real de los registros (logs) del firewall para monitorear el tráfico y validar el acceso a los servicios HTTP y FTP. Este monitoreo permitió comprobar la correcta aplicación de las reglas de seguridad configuradas, asegurando que el tráfico legítimo fuera permitido mientras se detectaban y bloqueaban posibles accesos no autorizados.

Figura 37. Verificación de logs.

Fuente: Autoría propia.

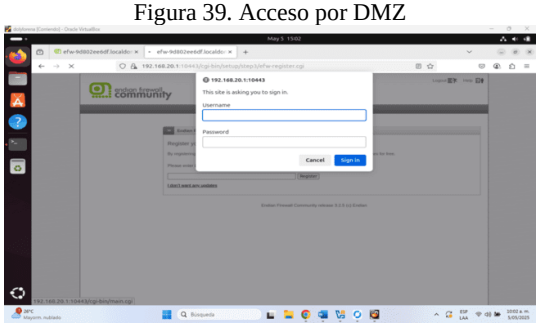
De manera correcta se evidencia que se configuraron correctamente las reglas de NAT y Firewall para permitir el acceso HTTP desde la LAN hacia la WAN. Tras aplicar las reglas, se verificó que el tráfico HTTP se estaba gestionando adecuadamente sin bloqueos, lo que indica que las configuraciones fueron exitosas.

Figura 38. Verificación de tráfico exitoso

Fuente: Autoría propia.

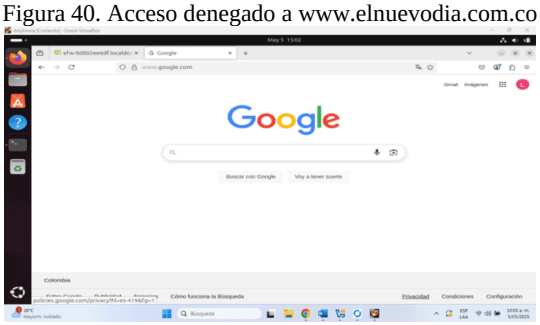
Se asigna la dirección IP 192.168.20.1 a la zona DMZ y se verifica la conexión exitosa. De igual forma, se verifica la conexión HTTP desde la LAN hacia la WAN.

Figura 39. Acceso por DMZ



Fuente: Autoría propia

Figura 40. Acceso denegado a www.elnuevodia.com.co



Fuente: Autoría propia.

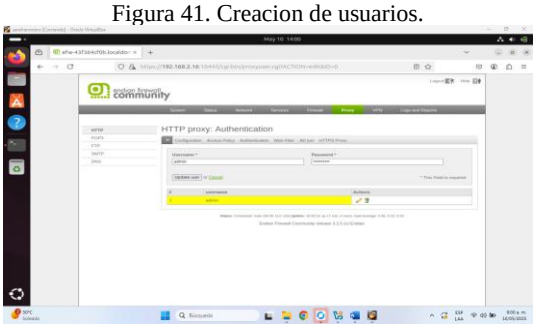
2.5 TEMATICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

Se configuró un perfil de filtrado de contenido junto con una lista negra destinada a bloquear el acceso a sitios web específicos, entre ellos www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Para reforzar el control de acceso, se implementó un mecanismo de autenticación basado en credenciales, que incluyó la creación de un usuario, su asignación a un grupo determinado y la definición de una política de acceso vinculada al perfil configurado. La efectividad de esta configuración fue verificada mediante pruebas realizadas desde un equipo ubicado en la red LAN, utilizando un navegador web para intentar acceder a los sitios restringidos, confirmando así la correcta aplicación de las políticas establecidas.

Para acceder al sistema, se requiere autenticación mediante el ingreso de un nombre de usuario y una contraseña. Una vez ingresadas las credenciales, se procede a iniciar sesión seleccionando la opción Sign In. A continuación, se accede al módulo de Network Configuration, desde donde se realiza la configuración de las interfaces de red del firewall.La interfaz RED fue configurada para obtener su dirección IP mediante el protocolo DHCP, permitiendo la conexión automatizada con redes externas. En esta etapa, también se definieron los tipos de red correspondientes a cada zona del firewall. La interfaz ORANGE fue seleccionada para representar la zona desmilitarizada (DMZ), permitiendo la exposición controlada de servicios hacia Internet. Finalmente, se confirmaron las direcciones IP asignadas a las interfaces internas: GREEN con la dirección IP 192.168.2.16 y ORANGE con la dirección IP 192.168.1.16.

En el módulo de autenticación del sistema, se procedió a la creación de un nuevo usuario con el fin de establecer un control de acceso basado en credenciales. Este procedimiento incluyó la definición de un identificador de usuario, la asignación de una contraseña segura y su vinculación a un grupo específico de políticas de acceso. Esta configuración permite gestionar de manera centralizada los permisos y restricciones asociados a la navegación desde la red local, facilitando la implementación de perfiles personalizados y el cumplimiento de las políticas de seguridad establecidas.

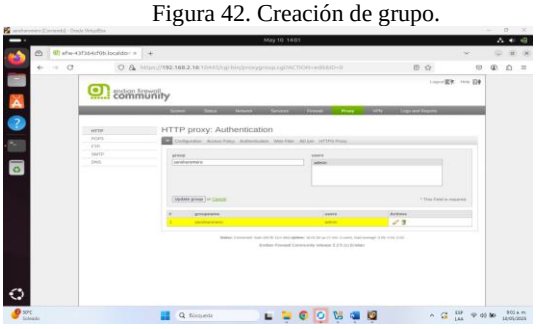
Figura 41. Creacion de usuarios.



Fuente: Autoría propia.

Se creó un grupo de autenticación denominado sandraromero, con el propósito de centralizar y gestionar políticas de acceso específicas para los usuarios pertenecientes a dicha categoría. Posteriormente, se asoció el usuario admin a este grupo, permitiendo que las restricciones y permisos definidos para el grupo sean aplicados automáticamente al usuario. Esta práctica facilita la administración de privilegios dentro del sistema, promoviendo una gestión más eficiente y segura del acceso a los recursos de red.

Figura 42. Creación de grupo.



Fuente: Autoría propia.

Se procedió a habilitar el servicio de proxy dentro del sistema de gestión del firewall. Esta acción permite canalizar y controlar el tráfico web saliente desde la red interna, facilitando la aplicación de políticas de filtrado de

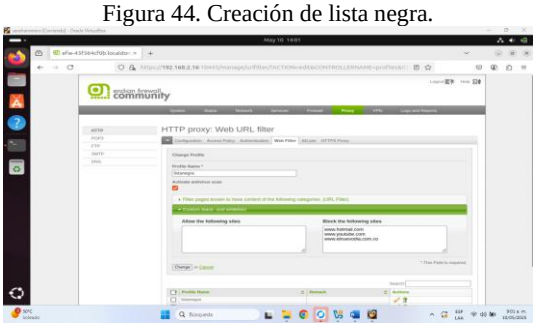
contenido, autenticación de usuarios y registro detallado de accesos. La activación del proxy es una medida fundamental para reforzar la seguridad perimetral, ya que actúa como intermediario entre los dispositivos de la red local y los servicios externos, mejorando el control y la visibilidad del tráfico de datos.

Figura 43. Habilitación de proxy y modo no transparente.

Fuente: Autoría propia.

Se crea un nuevo filtro denominado listanegra, en el cual se bloquean las páginas www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Finalmente, se aplican y guardan los cambios realizados.

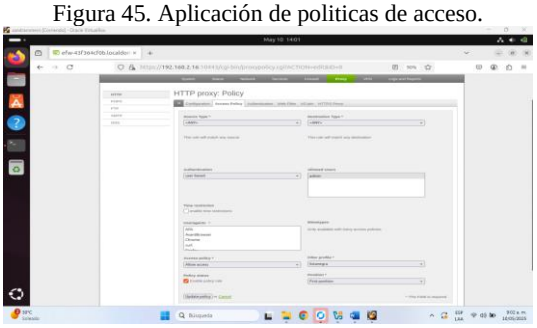
Figura 44. Creación de lista negra.



Fuente: Autoría propia.

Se crea una política de acceso en la que se asocia el usuario admin, se aprueba la regla denominada listanegra y se completan las configuraciones restantes.

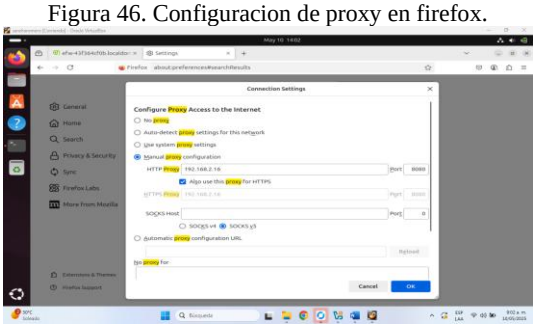
Figura 45. Aplicación de politicas de acceso.



Fuente: Autoría propia.

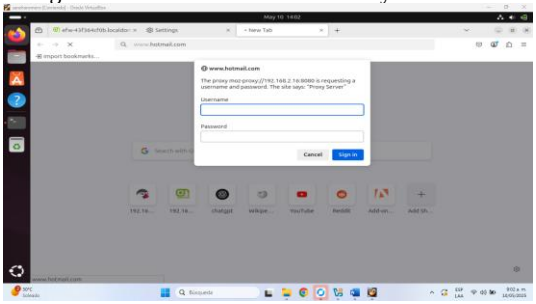
Se accede a la configuración de proxy en el navegador Firefox y se establece manualmente la dirección 192.168.10.1 como proxy. Asimismo, se configura el uso del mismo proxy para conexiones HTTPS [4]. Al intentar acceder a www.hotmail.com, se solicita autenticación de usuario.

Figura 46. Configuracion de proxy en firefox.



Fuente: Autoría propia.

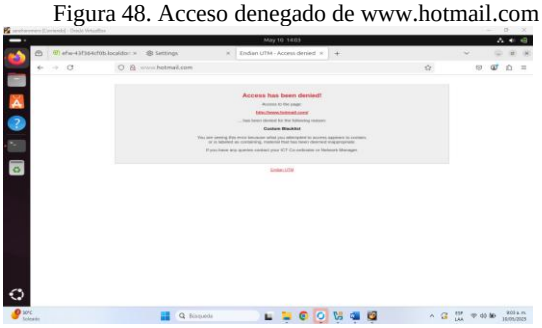
Figura 47. Autenticacion de usuario y contraseña.



Fuente: Autoría propia.

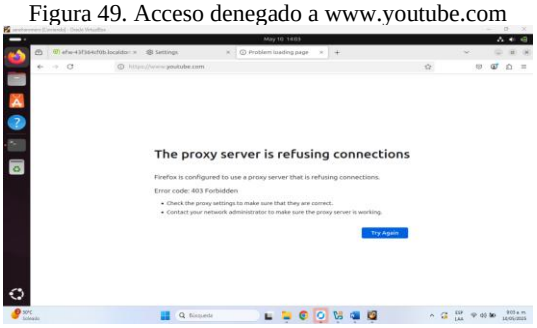
Una vez ingresadas correctamente las credenciales de autenticación, el sistema muestra un mensaje de confirmación que indica el acceso autorizado al servicio de navegación. Posteriormente, al intentar acceder al sitio web www.youtube.com desde un navegador en la red local, se presenta un mensaje de restricción generado por el sistema de filtrado de contenido, lo que confirma la aplicación exitosa de las políticas de bloqueo definidas previamente en la lista negra del proxy. Este comportamiento valida el funcionamiento del mecanismo de control de acceso basado en usuario y demuestra la efectividad de las configuraciones implementadas.

Figura 48. Acceso denegado de www.hotmail.com



Fuente: Autoría propia.

Figura 49. Acceso denegado a www.youtube.com



Fuente: Autoría propia.

Por último, al intentar acceder a www.elnuevodia.com.co, también se muestra el mismo mensaje.

Figura 50. Acceso denegado a www.elnuevodia.com.co

Fuente: Autoría propia.

3 CONCLUSIONES

La instalación y configuración de Endian UTM permitió comprobar su funcionalidad como una solución efectiva para la administración del tráfico de red. Mediante la aplicación de reglas de NAT y port forwarding, se logró controlar adecuadamente el acceso a los servicios HTTP y FTP, demostrando la versatilidad de esta herramienta en entornos de seguridad perimetral. El trabajo colaborativo facilitó la comprensión de conceptos clave como DMZ, red LAN y WAN, así como la importancia de registrar y analizar logs para garantizar la correcta operación del sistema. La actividad contribuyó significativamente al fortalecimiento de competencias en el manejo de sistemas operativos libres y software de virtualización.

La implementación de Endian Firewall en VirtualBox demuestra ser una solución didáctica y funcional para enseñar segmentación de redes y seguridad perimetral. La correcta configuración de tarjetas de red es fundamental para simular una topología realista, y permite ensayar políticas de firewall, NAT y DMZ sin riesgos en redes reales. Este enfoque es especialmente útil en programas de formación técnica y laboratorios remotos.

Las pruebas demostraron que el servidor en la zona DMZ pudo acceder a los servicios HTTP y FTP tal como se definió en las reglas. El protocolo ICMP fue correctamente bloqueado, como lo evidencia el mensaje "Destination Host Unreachable". El cliente en la zona Verde también tuvo acceso a los servicios del servidor. Se logró segmentar y controlar el tráfico entre zonas de forma eficaz y segura.

4 REFERENCIAS

[1] Endian (2016), Endian UTM 3.2 Manual referencia. Endian.
http://docs.endian.com/3.2/utm/index.html

[2] Canonical (2023). Guía del Ubuntu desktop 20.04 LTS. Help
Ubuntu. https://help.ubuntu.com/20.04/ubuntu-help/index.html
https://www.debian.org/releases/stable/amd64/index.es.html

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

[4] Mozilla. (n.d.). *Configurar un servidor proxy manualmente en Firefox*. Recuperado de https://support.mozilla.org/es/kb/configurar-un-servidor-proxy.