IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Duberney Betancur Calle
dbetancurc@unadvirtual.edu.co
Cristian Geovanny Rodas Ballesteros
cgrodasb@unadvirtual.edu.co
Luis David Hurtado Serna
ldhurtados@unadvirtual.edu.co
Daniela Rojas Baena
drojasbae@unadvirtual.edu.co
Juan Sebastián Rave Parra
jsravep@unadvirtual.edu.co

RESUMEN: *La actividad descrita en este artículo contiene la implementación de una arquitectura de seguridad perimetral utilizando Endian Firewall Community sobre entornos de virtualización como KVM o VirtualBox. El proyecto se centra en la segmentación lógica de la red en tres zonas de seguridad: WAN (roja) LAN (verde), DMZ (Naranaja). Además, se abarca la configuración de interfaces virtuales, la aplicación de reglas de traducción de direcciones (NAT) y el filtrado de paquetes para permitir servicios específicos como HTTP y FTP, restringiendo protocolos vulnerables como ICMP. También se implementa un Proxy HTTP con autenticación y listas de control de acceso (ACL) para gestionar y asegurar la navegación web de los usuarios. Con los resultados obtenidos se demuestra la eficacia y viabilidad de integrar soluciones UTM (Unified Threat Management) de open source para garantizar la integridad, confidencialidad y disponibilidad de los recursos en un entorno corporativo simulado.*

PALABRAS CLAVE: Endian Firewall, redes, seguridad perimetral, zonas.

1 INTRODUCCIÓN

En el ámbito de la administración de sistemas, la protección de la infraestructura de red es esencial para garantizar la integridad, confidencialidad y disponibilidad de la información; Este artículo describe la implementación técnica de una solución de seguridad perimetral basada en Endian Firewall Community, desplegada sobre entornos virtualizados. El proyecto se centra en el diseño de una topología de red segmentada en tres zonas estratégicas: Zona Verde (LAN), Zona Naranja (DMZ) y Zona Roja (WAN), estableciendo fronteras de confianza claras, según los tipos de usuarios o recursos, sean internos o externos.

El desarrollo abarca la configuración de interfaces de red, la aplicación de reglas de Traducción de Direcciones de Red (NAT) y el filtrado de paquetes para permitir servicios críticos mientras se restringen protocolos vulnerables como ICMP. También, se detalla la implementación de un Proxy HTTP con mecanismos de autenticación y listas de control de acceso (ACL). Por medio de estas configuraciones, se puede validar la capacidad de las soluciones de código abierto para gestionar eficazmente la seguridad, la disponibilidad y el control de navegación en un entorno corporativo simulado.

2 CONCEPTOS PREELIMINARES

Para una mejor comprensión de la arquitectura implementada, es necesario definir los componentes lógicos y físicos que hacen parte de la protección perimetral.

- Firewall: De acuerdo con Forninet, es un dispositivo o software de seguridad de red que monitorea y filtra el tráfico entrante y saliente de la red, basado en un conjunto de reglas de seguridad para permitir o denegar paquetes de datos. [1]
- Red virtual: Según RedHat, sobre la creación de redes en máquinas virtuales, se puede decir que es cuando una red física se divide lógicamente en varios segmentos. En virtualización, como en este caso, se usa un switch de software (vswitch) que permite a las VMs comunicarse entre sí y con redes externas, aplicando aislamiento y políticas de tráfico. [2]
- NIC o Tarjetas de Red: De acuerdo con Lenovo, es un componente de hardware o su emulación virtual cuando se usan máquinas virtuales para conectar un equipo a una red. Cuentan con una dirección MAC única, que permite la identificación en la Capa 2 además de la transmisión y recepción de tramas de datos. [3]
- Zonas de Seguridad: Siguiendo lo que propone Endian en su documentación, son usadas en contexto de firewalls y hacen referencia a una agrupación lógica de una o más interfaces de red (físicas o virtuales) que tienen un nivel similar de confianza de seguridad. Las reglas del firewall se aplican al tráfico que cruce los límites que hay entre estas zonas, por ejemplo, de LAN a DMZ o de WAN a LAN). [4]
- Endian Firewall Community: Es el núcleo de la seguridad perimetral de este proyecto, que es una distribución de seguridad de código abierto basada en Linux que transforma un sistema (físico o virtual) en un dispositivo de Gestión Unificada de Amenazas o UTM (Unified Threat Management). Opera bajo el concepto de "Inspección de Estado de Paquetes" (Stateful Packet Inspection) integrando múltiples servicios de seguridad en una sola plataforma, tales como firewall, VPN, filtrado web, antivirus, antispam y gestión de ancho de banda,

todo esto permite la implementación flexible de zonas de seguridad (Roja, Verde, Naranja y Azul) para segmentar redes corporativas de manera más eficiente [5].

3 DESARROLLO DE TEMÁTICAS

3.1 TEMÁTICA 1: CONFIGURACIÓN E INSTALACIÓN DE ENDIAN.

Producto esperado: 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).

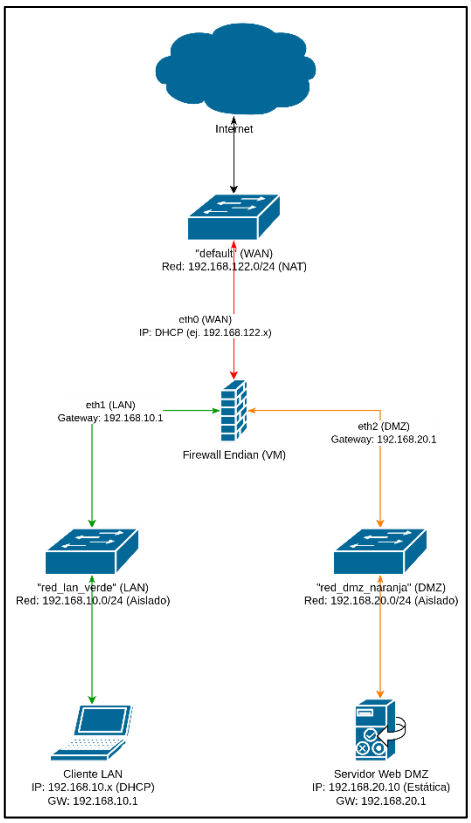
En esta primera fase se abordó la implementación del núcleo de seguridad de la red, abarcando temas desde el diseño de la topología lógica hasta la instalación efectiva del sistema operativo Endian Firewall y su segmentación en zonas de seguridad.

3.1.1. DISEÑO DE LA TOPOLOGÍA DE RED

El primer paso es la segmentación en tres zonas (Verde, Roja y Naranja), se diseñó una arquitectura de red virtualizada, entendiendo la topología de red como lo indica IBM, es la forma como los nodos y conexiones de una red se organizan física y lógicamente [6], tal como se presenta en la Fig. 1.

Figura 1. Topología de red implementada por zonas

.



Fuente: Autoría propia (Duberney Betancur)

Además, basados en dicha topología se definieron tres conmutadores virtuales (vSwitches) para aislar el tráfico, de la siguiente manera:

- Zona Roja (WAN): Interfaz conectada a la red default (NAT) del hipervisor (192.168.122.0/24), simulando el acceso a Internet.
- Zona Verde (LAN): Red aislada (red_lan_verde) con segmento 192.168.10.0/24, destinada a las estaciones de trabajo internas.
- Zona Naranja (DMZ): Red aislada (red_dmz_naranja) con segmento 192.168.20.0/24, exclusiva para servidores públicos.

3.1.2. ASIGNACIÓN DE RECURSOS DE HARDWARE PARA MÁQUINA VIRTUAL

Se desplegó una máquina virtual con recursos dedicados (CPU, RAM, Almacenamiento), y antes de la instalación se asignaron tres tarjetas de red virtuales (vNICs). Para garantizar la correcta asociación durante la instalación, se documentaron las direcciones MAC de cada interfaz, vinculando eth0 a la WAN, eth1 a la LAN y eth2 a la DMZ, como lo muestra la tabla 1.

Tabla 1. Resumen de interfaces de red a utilizar

Zona	MAC	Interfaz
Roja	52:54:00:8d:ed:51	eth0
Verde	52:54:00:3a:61:5a	eth1
Naranja	52:54:00:0a:84:36	eth2

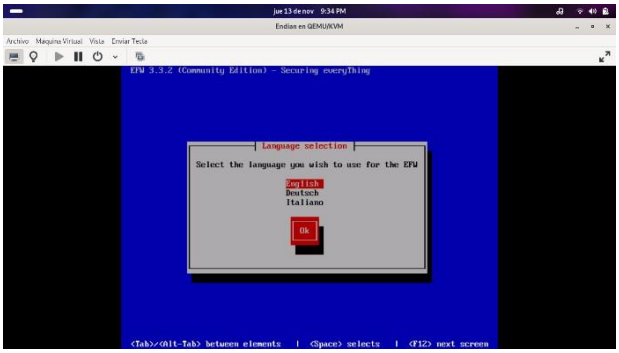
Fuente: Autoría propia (Duberney Betancur)

3.1.3. PROCESO DE INSTALACIÓN DE ENDIAN

Una vez se realizaron las configuraciones previas, se realizó la instalación del sistema usando la imagen ISO de Endian Firewall Community 3.3.2, el proceso siguió un flujo de configuración básico a través del instalador basado en texto:

Algunos de los pasos fueron el arranque de la instancia creada y la selección de idioma inglés para la interfaz del sistema (Fig. 2).

Figura 2. Instalación de Endian

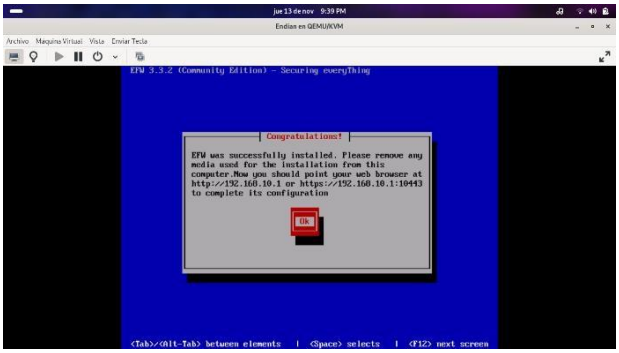


Fuente: Autoría propia (Duberney Betancur)

Otros pasos importantes fueron el particionamiento, en este caso, el instalador preparó el disco virtual, creando las particiones necesarias para el sistema (/), los registros (/var/log) y la configuración (/var/efw), además pidió la dirección IP de la zona verde, por lo tanto, se le indicó la correspondiente. 192.168.10.0.

Una vez finalizado el proceso, el asistente de instalación confirma que se ha realizado satisfactoriamente tras la copia de paquetes y la configuración del gestor de arranque, termina desplegando la pantalla de confirmación ("Congratulations!") que además indica la dirección URL de administración por defecto, con la IP que se le indicó y su respectivo puerto, y finalmente solicita el reinicio del sistema (Fig. 3).

Figura 3. Fin de instalación de Endian

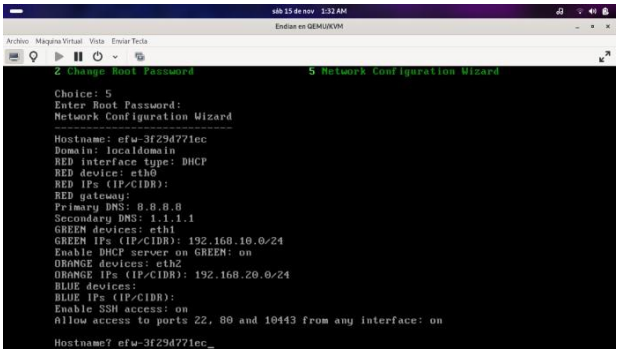


Fuente: Autoría propia (Duberney Betancur)

3.1.4 CONFIGURACIÓN DE INTERFACES Y ZONAS

Una vez reiniciado el sistema se procede a comprobar que todas las redes o zonas estén configuradas correctamente, por eso se accede al asistente por consola con la opción 5; en este caso faltaban asignar algunos roles a las interfaces de red, se hacen estos ajustes (Fig. 4):

Figura 4. Asistente de configuración de Endian

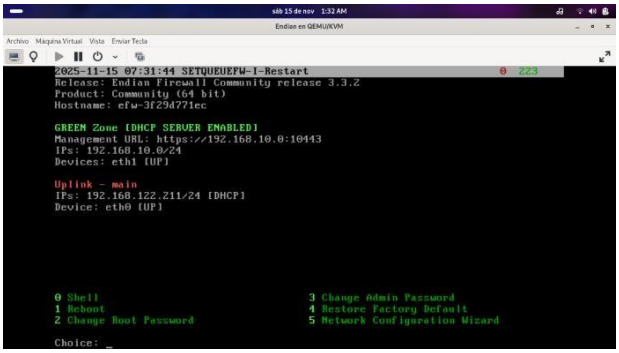


Fuente: Autoría propia (Duberney Betancur)

- La zona roja (eth0) se configuró en modo DHCP para recibir direccionamiento del ISP simulado.
- La zona verde (eth1) se estableció en DHCP en el rango 192.168.10.0, para que asigne las IP a los equipos de esta zona.
- La zona naranja (eth2) se definió en la subred 192.168.20.0 para la zona DMZ.
- Se habilitó el acceso administrativo desde la zona verde, para permitir la gestión remota y validar la operatividad de las tres zonas.

Una vez realizados estos pasos y reiniciado la máquina virtual de Endian, debe aparecer activa también la zona roja en la interfaz de Endian (Fig. 5), y se puede preceder al acceso desde el equipo cliente para las demás configuraciones.

Figura 5. Interfaz de Endian en máquina virtual

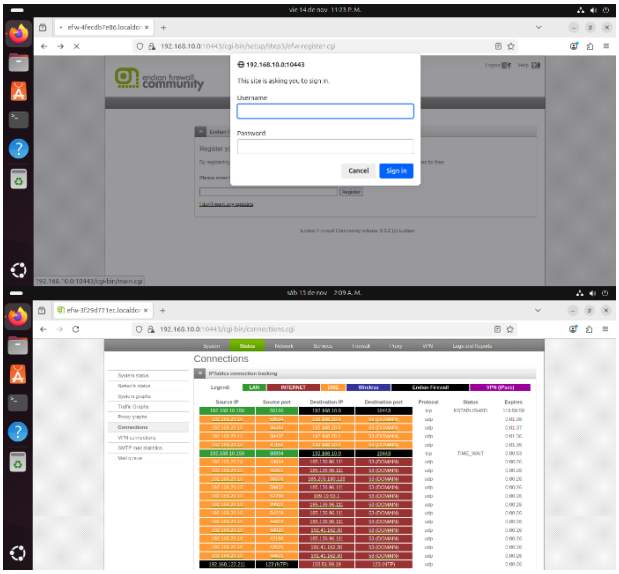


Fuente: Autoría propia (Duberney Betancur)

3.1.5 ACCESO DESDE CLIENTE

Se comprueba finalmente que todo ha quedado instalado y configurado adecuadamente al ingresar desde el navegador del equipo cliente a la URL 192.168.10.1:10443 y se visualizan la pantalla de inicio de sesión, pantalla principal, estado de la red con los respectivos colores de las zonas (Fig. 6), con lo cual se puede continuar con las demás configuraciones que se verán a continuación.

Figura 6. Interfaz de Endian desde cliente



Fuente: Autoría propia (Duberney Betancur)

3.2 TEMÁTICA 2: CONFIGURACIÓN NAT.

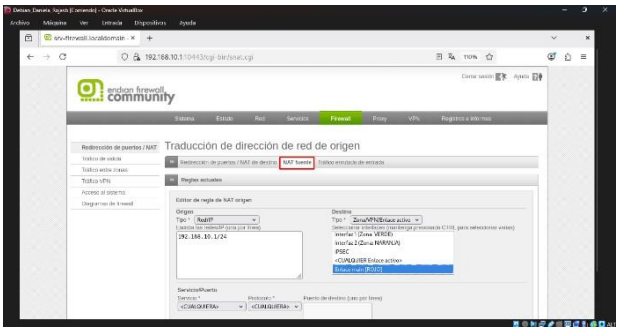
Producto esperado: Consiste en la configuración de las reglas de NAT (Network Address Translation), demostrando el establecimiento de la comunicación tanto desde la LAN hacia la WAN (red simulada de Internet) como desde la zona DMZ hacia la Internet, incluyendo la verificación del reenvío de puertos y la correcta creación de las reglas correspondientes.

Lo primero entender que NAT, como lo indica IETF, hace referencia al mecanismo que permite a diferentes dispositivos de una red privada acceder a Internet utilizando una única dirección IP pública, al modificar los encabezados de los paquetes [7].

Una vez instalado el sistema y configuradas las zonas de red (verde para LAN, naranja para a DMZ y roja para WAN), se procedió a configurar las reglas de NAT (Network Address Translation). El objetivo de esta configuración fue demostrar el correcto establecimiento de la comunicación tanto desde la red LAN hacia la red WAN (simulando el acceso a Internet), como desde la zona DMZ hacia la WAN, garantizando así que el tráfico generado en cada zona pudiera ser traducido y enrutado adecuadamente hacia su destino externo.

La configuración se realizó desde la pestaña "NAT fuente" dentro del módulo de Firewall, permitiendo establecer una regla que traduce el tráfico generado en la zona verde (LAN) cuando se dirige hacia la zona roja (WAN).

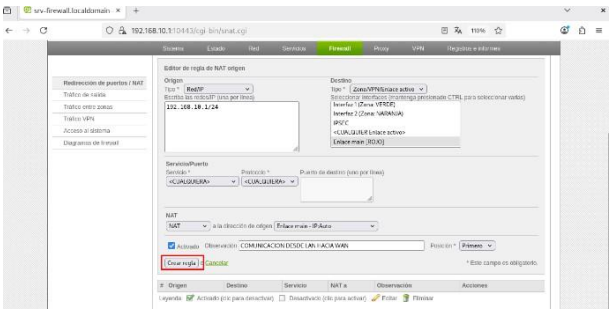
Figura 7. Configuración NAT fuente zona verde.



Fuente: Autoría propia (Daniela Rojas)

En esta configuración se creó una regla de NAT Fuente (SNAT) en el firewall Endian con el fin de permitir que los equipos de la red LAN accedan correctamente a la red WAN. Para ello, se especificó como origen la red interna 192.168.10.1/24 y como destino la interfaz roja (WAN), de modo que todo el tráfico saliente desde la LAN sea traducido utilizando la IP asignada al firewall en dicha interfaz. Esta traducción es esencial para que las direcciones privadas de la red local puedan comunicarse con redes externas, además de proporcionar enmascaramiento, mayor seguridad y un control centralizado del tráfico que abandona la infraestructura interna.

Figura 8. Creación de regla NAT zona verde



Fuente: Autoría propia (Daniela Rojas)

Se verifica la creación de la nueva regla y posteriormente se aplican los cambios para que la configuración quede activa y comience a operar dentro del firewall.

Figura 9. Aplicación de la regla zona verde

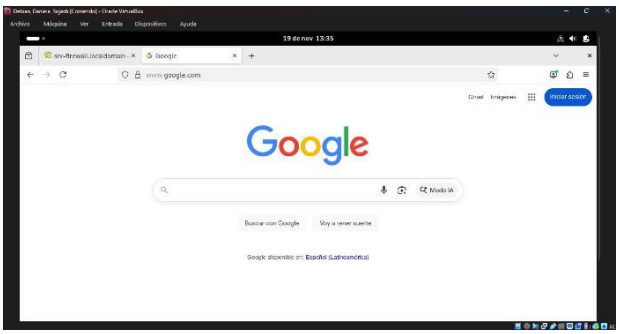
Fuente: Autoría propia (Daniela Rojas)

Para comprobar el funcionamiento de esta regla, se realizaron pruebas de conectividad desde un cliente ubicado en la LAN, utilizando comandos de ping y verificando además el acceso mediante navegación web, confirmando así que el tráfico se traducía y enrutaba correctamente hacia la red WAN.

Figura 10. Comunicación a internet desde LAN consola

Fuente: Autoría propia (Daniela Rojas)

Figura 11. Comunicación a internet desde LAN Navegación Web

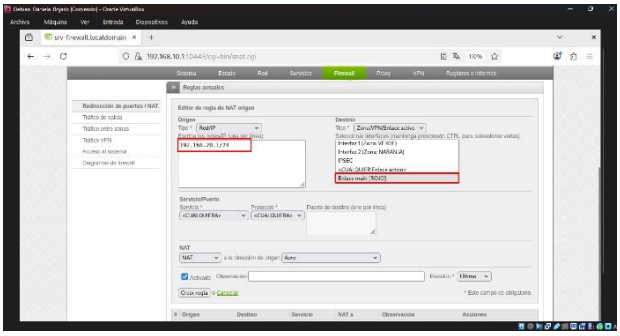


Fuente: Autoría propia (Daniela Rojas)

Para la comunicación desde la DMZ (zona naranja) hacia la WAN y garantizar que los servicios publicados tengan acceso a Internet, se creó una segunda regla de NAT Masquerading específica para dicha interfaz. Esta configuración permite mantener debidamente segmentados los dominios de red, asegurando que el tráfico de la DMZ salga hacia la WAN sin exponer directamente la infraestructura interna, preservando así la seguridad y el control sobre los flujos de información.

Se crea la regla para permitir el acceso a Internet utilizando la opción "NAT de fuente", configurando el enmascaramiento necesario para que el tráfico saliente desde la red interna pueda ser correctamente dirigido hacia la WAN.

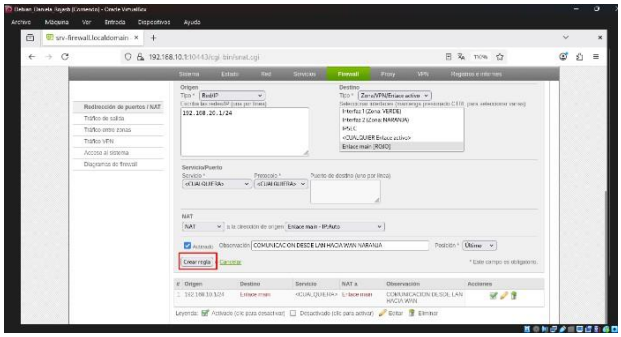
Figura 12. Configuración NAT fuente zona naranja



Fuente: Autoría propia (Daniela Rojas)

Se confirma la creación de la regla una vez verificados y validados todos los parámetros configurados, asegurando que la definición sea correcta antes de su aplicación.

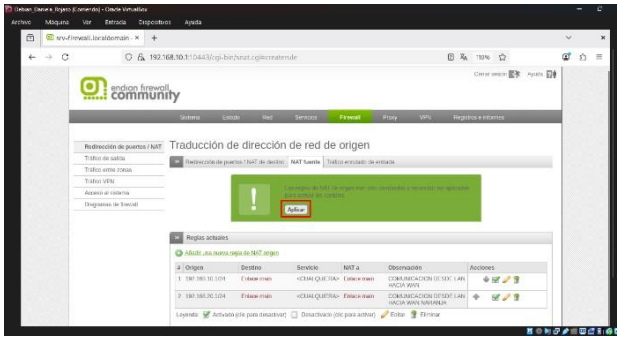
Figura 13. Creación de regla NAT zona naranja



Fuente: Autoría propia (Daniela Rojas)

Aplicación de los cambios para la nueva regla.

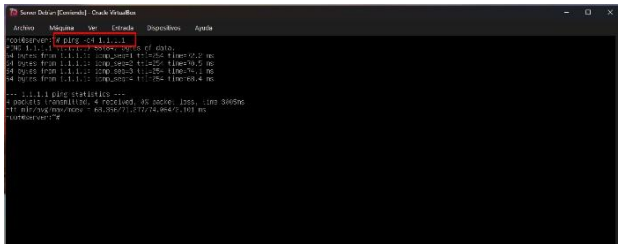
Figura 14. Aplicación de nueva regla para zona DMZ



Fuente: Autoría propia (Daniela Rojas)

Se realiza la comprobación de la conectividad a Internet desde el servidor ubicado en la zona naranja (DMZ), verificando que la regla configurada permita el acceso externo de manera correcta.

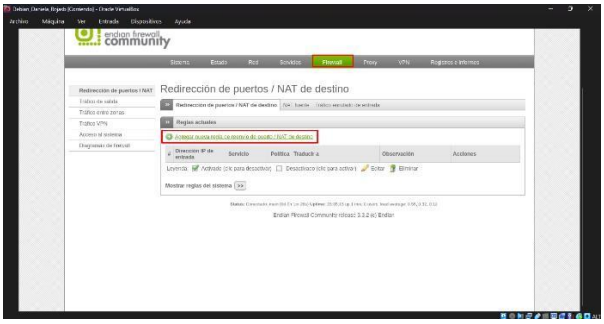
Figura 15. Comunicación a internet desde DMZ consola



Fuente: Autoría propia (Daniela Rojas)

Por medio de la opción "Redirección de puertos / NAT de destino" se crea una nueva regla que permite redirigir el tráfico entrante hacia un servicio o equipo específico dentro de la red interna.

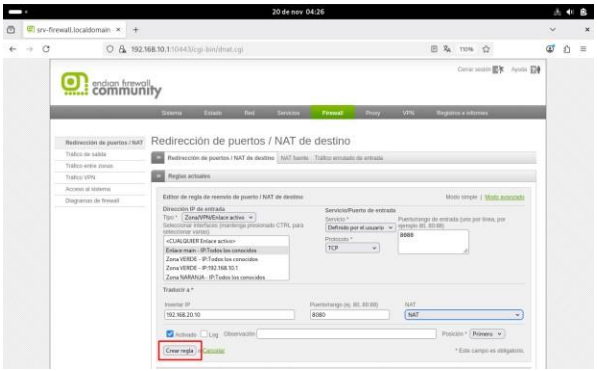
Figura 16. Regla Redirección de puertos / NAT de destino



Fuente: Autoría propia (Daniela Rojas)

En esta sección del firewall se configuró una regla de redirección de puertos (NAT de destino), seleccionando como origen la interfaz correspondiente a la zona naranja (DMZ), con el fin de permitir el acceso externo a los servicios alojados en dicha zona. Para ello, se definió el tipo de entrada, el servicio o puerto involucrado y la acción de traducción necesaria.

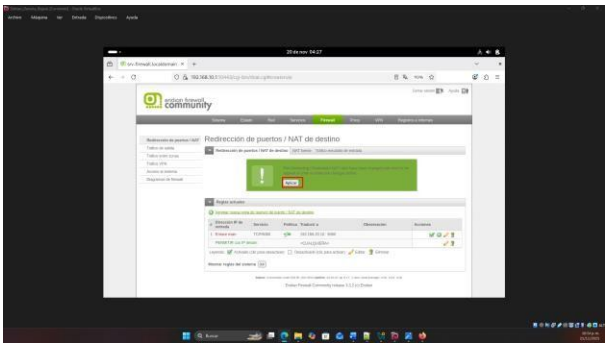
Figura 17. Creación de regla para puertos



Fuente: Autoría propia (Daniela Rojas)

Una vez establecidos todos los parámetros, se procedió a crear la regla y aplicarla, habilitándola para que el tráfico entrante hacia la IP pública o interfaz definida sea correctamente redirigido hacia el servidor interno ubicado en la DMZ. Esta configuración tiene como finalidad exponer de forma controlada y segura los servicios internos hacia el exterior, garantizando que solo el tráfico permitido llegue al destino adecuado.

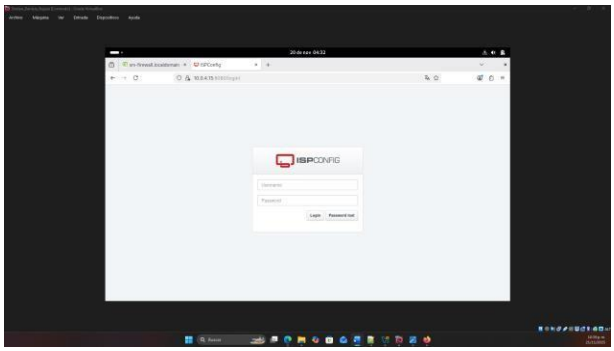
Figura 18. Aplicación de regla para redirección de puertos



Fuente: Autoría propia (Daniela Rojas)

El servidor configurado respondió correctamente después de aplicar únicamente la regla principal de redirección de puertos (NAT de destino). Gracias a esta configuración, el acceso externo se estableció sin inconvenientes, permitiendo que el servicio alojado en la zona Naranja se visualizara desde el navegador de forma estable y segura. Este resultado confirma que el Endian gestionó el reenvío de puertos de manera efectiva, garantizando la disponibilidad del servicio publicado.

Figura 19. Comprobación de servicio de zona naranja



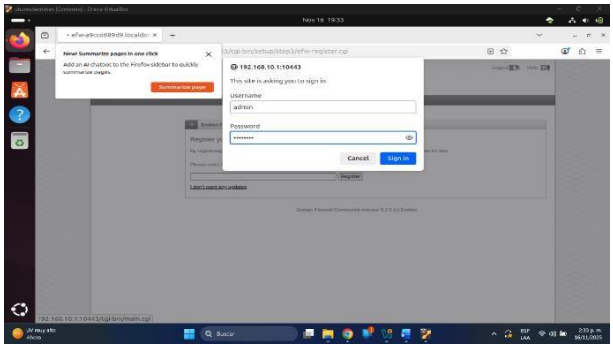
Fuente: Autoría propia (Daniela Rojas)

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

Producto esperado: El producto esperado es habilitar los servicios HTTP y FTP en el servidor web bajo Ubuntu Server permitiendo el acceso a los puertos 80 y 21 desde la zona DMZ. Además, se debe denegar el protocolo ICMP bloqueando los puertos 8 y 30 para evitar respuestas de ping en la red. Finalmente, se debe verificar en el tráfico de salida la creación de las reglas de firewall implementadas.

En primer lugar, es importante comprender algunos conceptos clave de este punto como son las ACL o reglas de firewall, que Fortinet define como instrucciones lógicas que permiten o deniegan el tráfico de red según criterios específicos como la IP de origen, destino y el puerto del servicio [8], y el protocolo ICMP, como señala IETF, pertenece a la capa de red y permite enviar mensajes de error y diagnósticos entre dispositivos, es la base de herramientas de verificación de conectividad como el comando el comando ping [9].

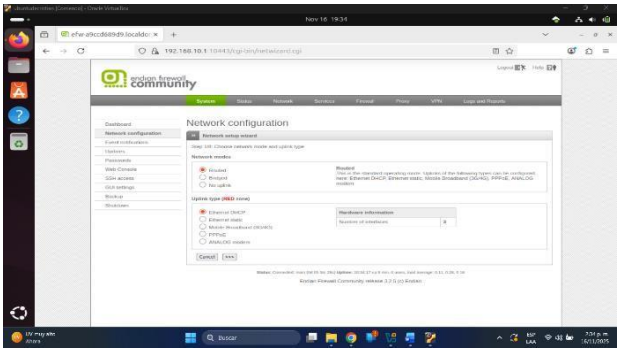
Figura 20. Autenticación de usuario y contraseña Endian.



Fuente: Autoría propia (Cristian)

Desde desktop accedemos a Endian por medio de https://192.168.10.1:10443 y nos logueamos.

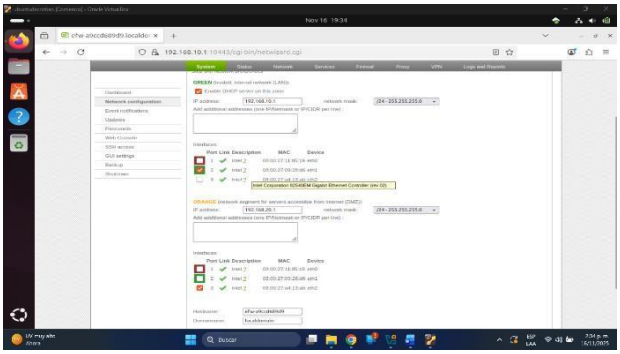
Figura 21. Configuración de RED en modo DHCP.



Fuente: Autoría propia (Cristian)

Confirmamos la configuración de RED (WAN).

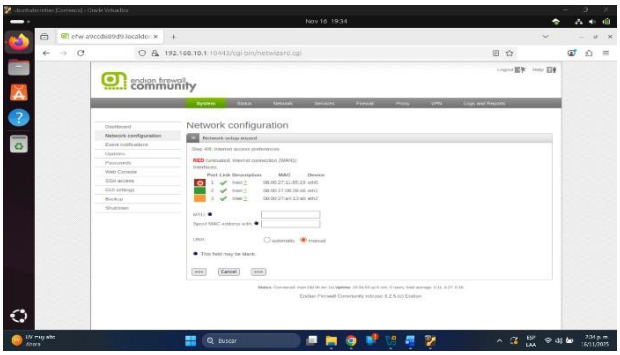
Figura 22. Confirmación de ip de GREEN y ORANGE



Fuente: Autoría propia (Cristian)

Confirmamos la configuración de GREEN y ORANGE con sus respectivas ip.

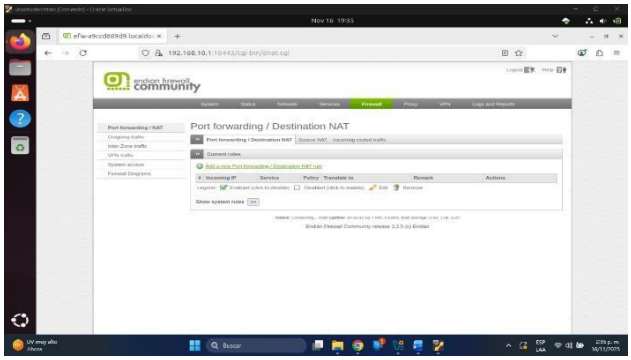
Figura 23. Confirmación de configuración de RED en DHCP.



Fuente: Autoría propia (Cristian)

Confirmamos eth0 para RED.

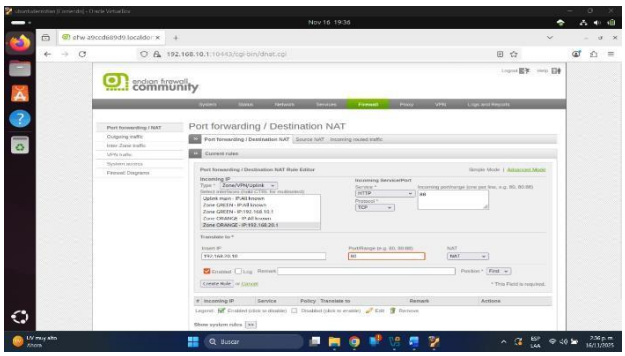
Figura 24. Ingresamos al modulo firewall.



Fuente: Autoría propia (Cristian)

Nos dirigimos al modulo de firewall y le damos en botón de añadir una nueva regla.

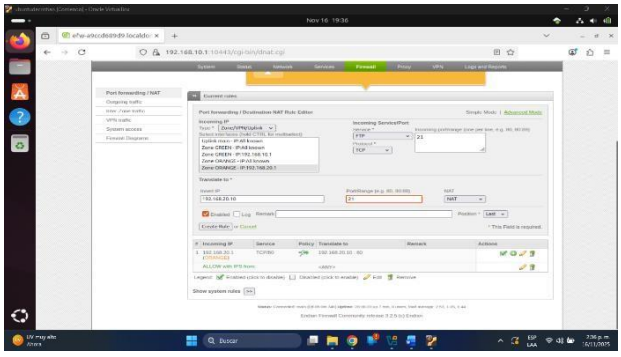
Figura 25. Configuracion de reglas puerto 80.



Fuente: Autoría propia (Cristian)

Configuración de port forwarding en Endian Firewall para permitir el tráfico HTTP (puerto 80) hacia el servidor Ubuntu en la zona DMZ con la IP 192.168.20.100.

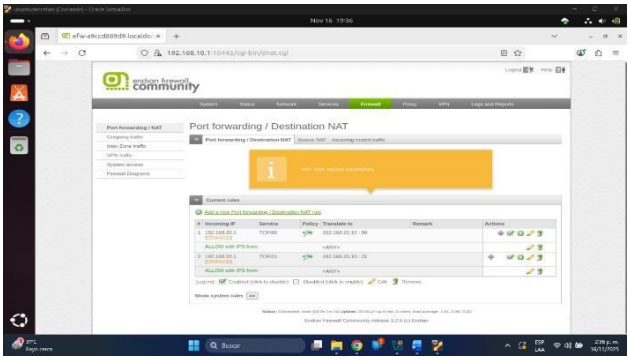
Figura 26. Configuracion de regla puerto 21.



Fuente: Autoría propia (Cristian)

Configuración de port forwarding para permitir el tráfico FTP (puerto 21) hacia el servidor Ubuntu en la zona DMZ con la IP 192.168.20.100.

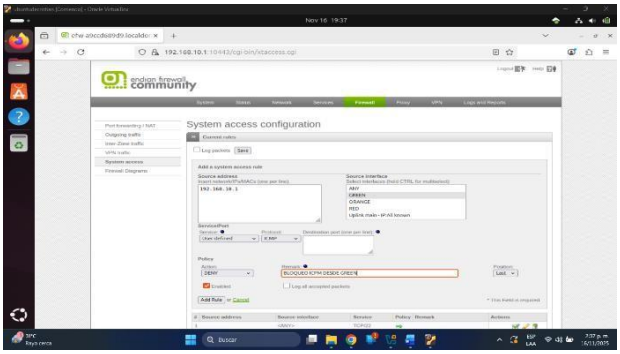
Figura 27. Visualizacion de reglas creadas.



Fuente: Autoría propia (Cristian)

Reglas creadas correctamente.

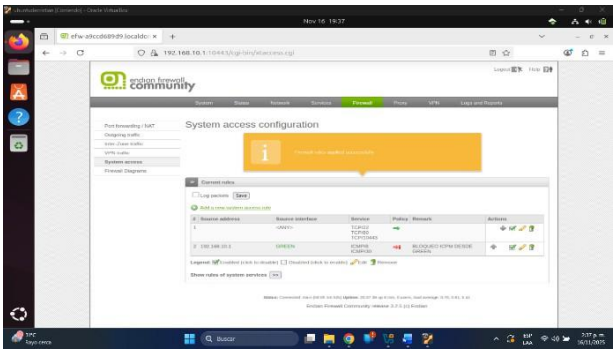
Figura 28. Configuracion de bloqueo para ICMP.



Fuente: Autoría propia (Cristian)

Regla de firewall en Endian Firewall para bloquear el tráfico ICMP desde la IP 192.168.10.1 en la interfaz GREEN (DMZ), con acción de denegar el tráfico. La regla está habilitada y aplicada.

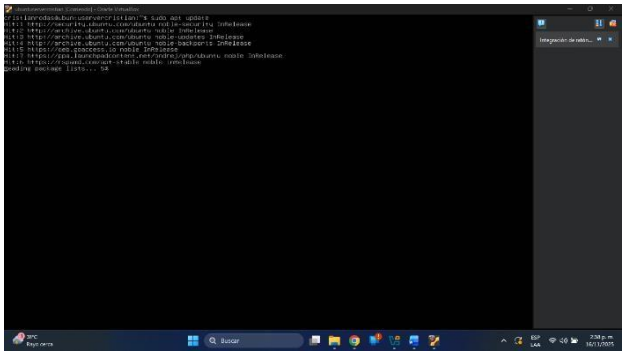
Figura 29. Visualizacion de bloqueo.



Fuente: Autoría propia (Cristian)

Bloqueo creado.

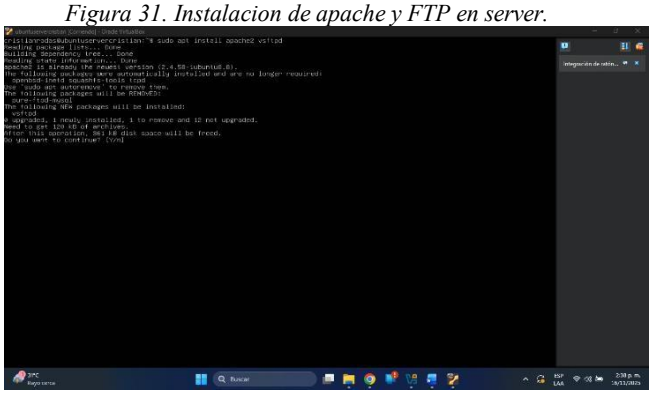
Figura 30. Actualizacion de paquetes en server.



Fuente: Autoría propia (Cristian)

Se actualizan paquetes.

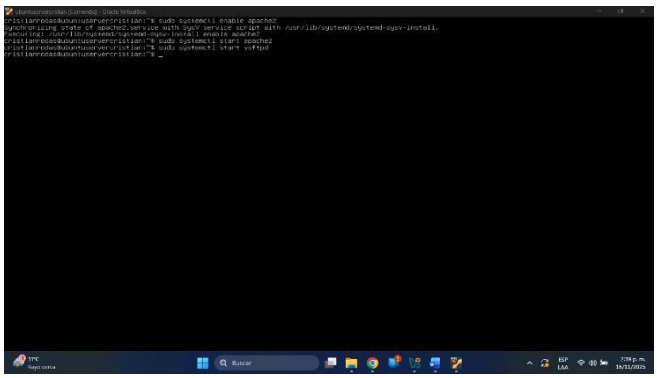
Figura 31. Instalacion de apache y FTP en server.



Fuente: Autoría propia (Cristian)

Instalación de Apache y FTP en Ubuntu Server

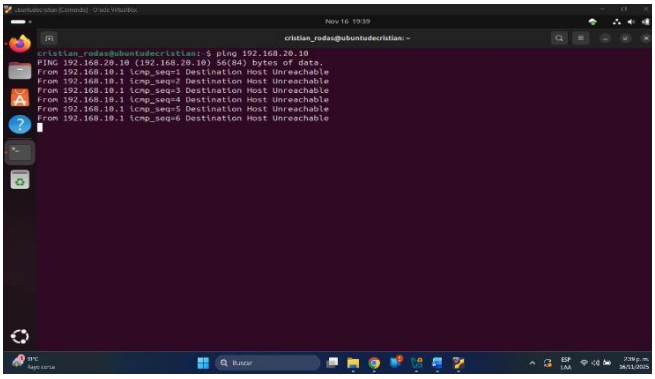
Figura 32. Configuracion de servicios en server



Fuente: Autoría propia (Cristian)

Instalación de Apache y FTP en Ubuntu Server: Configuración de servicios HTTP y FTP.

Figura 33. Bloqueo a ICMP exitosamente.



Fuente: Autoría propia (Cristian)

El ping a la dirección IP de la red DMZ está siendo bloqueado, mostrando "Destination Host Unreachable", lo que indica que la regla para bloquear ICMP está funcionando correctamente.

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

Producto esperado: Se deben comunicar la zona Verde y la zona Naranja utilizando los protocolos HTTP y FTP con sus respectivos puertos, así como establecer comunicación entre la zona Internet y la zona DMZ; además, es necesario verificar en el tráfico interzona la creación de las reglas correspondientes y, finalmente, probar desde un navegador web las siguientes directivas: el acceso HTTP desde la LAN hacia la DMZ y hacia la WAN, el acceso HTTP desde la DMZ hacia la WAN y desde la WAN hacia la DMZ, así como el acceso FTP desde la LAN hacia la WAN y desde la WAN hacia la DMZ.

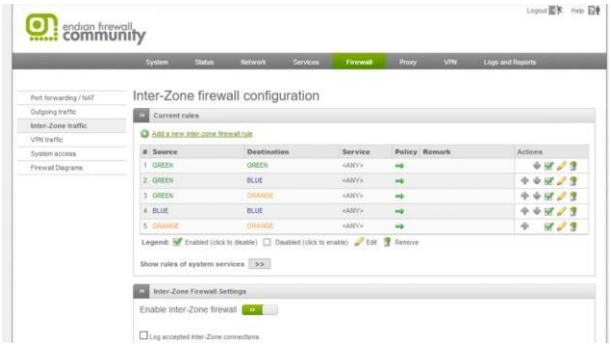
También es importante conocer qué es HTTP, que como lo señala RFC, es el protocolo estándar para la transmisión de información en la web, permite los navegadores solicitar y visualizar páginas web desde los servidores, comúnmente opera en el puerto 80 [10], por otro lado el protocolo FTP que según IETF, está optimizado exclusivamente para la transferencia de archivos entre un cliente y un servidor, utilizando comumnente el puerto 21. [11]

3.4.1 COMUNICAR LA ZONA VERDE CON LA ZONA NARANJA CON EL PROTOCOLO HTTP Y FTP CON SUS RESPECTIVOS PUERTOS.

GREEN → ORANGE solo HTTP y FTP. Aquí procedí a crear las reglas necesarias para permitir únicamente los servicios HTTP (y FTP desde la zona GREEN hacia la zona ORANGE.

Para ello añadí dos reglas nuevas especificando como Source = GREEN, Destination = ORANGE y seleccionando cada servicio correspondiente. Finalmente habilité ambas reglas y verifiqué que quedaran visibles y activas en la lista de "Current rules", asegurando así que la LAN pueda acceder únicamente a esos servicios del servidor ubicado en la DMZ.

Figura 37. Configuracion de reglas

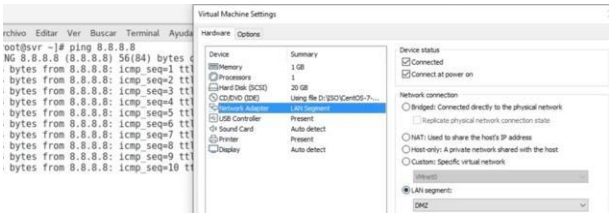


Fuente: Autoría propia (Juan Rave)

Para verificar hare un ping desde el DMZ configuré la tarjeta de red de la máquina virtual para dejarla dentro del segmento correspondiente a la zona ORANGE (DMZ). Esto me permite que el servidor de la DMZ quede totalmente aislado de la red GREEN, pero al mismo tiempo pueda aplicar las reglas Inter-Zone que voy a crear después en Endian.

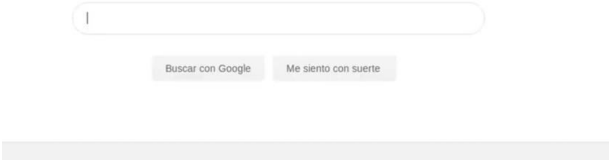
Verifiqué que la interfaz estuviera conectada y asignada al segmento correcto, asegurándome así de que la comunicación entre GREEN y ORANGE funcioné únicamente a través del firewall, tal como exige la temática 4 para el control del tráfico HTTP y FTP.

Figura 38. Acceso DMZ y ping



Fuente: Autoría propia (Juan Rave)

Figura 39. Acceso a internet con las reglas

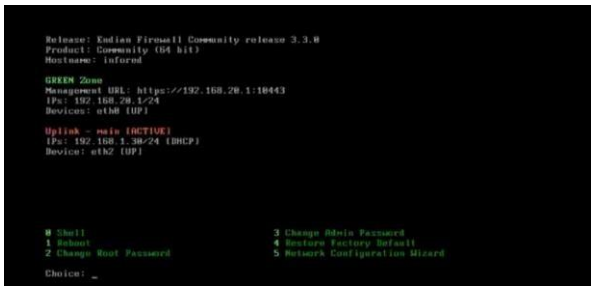


Fuente: Autoría propia (Juan Rave)

3.4.2 COMUNICAR LA ZONA INTERNET CON LA ZONA DMZ.

Confirmé la configuración de las zonas en Endian: la interfaz GREEN quedó en la red, mientras que la interfaz RED obtuvo su dirección por DHCP desde Internet. Con esto verifiqué que el firewall ya reconoce correctamente la red interna y la salida WAN, lo cual es indispensable para crear las reglas de DNAT y publicar los servicios de la DMZ hacia la zona RED.

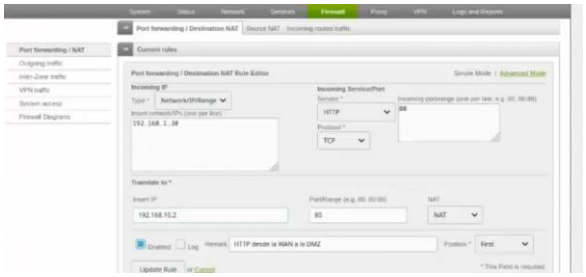
Figura 40. Configuracion de zonas



Fuente: Autoría propia (Juan Rave)

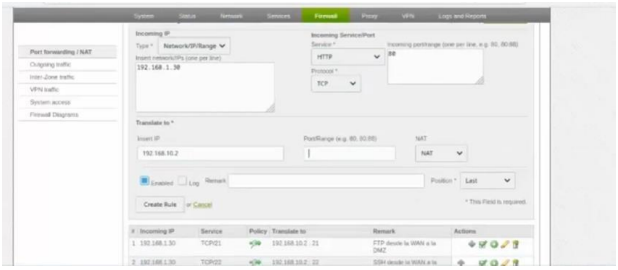
Creo una regla de Port forwarding Destination NAT para publicar mi servidor web de la DMZ hacia Internet. En la sección Incoming IP indico la IP de la interfaz RED del firewall y, en Incoming Service/Port, selecciono el servicio HTTP con el puerto TCP. Luego, en Translate to, escribo la IP de mi servidor web en la DMZ (ORANGE) y también el puerto 80, de forma que todo el tráfico HTTP que llegue desde la WAN al firewall sea redirigido automáticamente a ese servidor.

Figura 41. Acceso Port forwarding Destination NAT



Fuente: Autoría propia (Juan Rave)

Figura 42. Reglas HTTP y FTP



Fuente: Autoría propia (Juan Rave)

Creé reglas que toman las conexiones que llegan desde Internet HTTP y FTP y las traducen en la zona naranja (DMZ), agregando además una regla para el puerto 22 SHH. De esta forma, cualquier acceso HTTP, FTP o SSH desde la WAN se redirige de forma controlada al servidor DMZ, cumpliendo el requisito de comunicar Internet con la zona DMZ mediante DNAT.

Figura 43 HTTP y FTP .

Fuente: Autoría propia (Juan Rave)

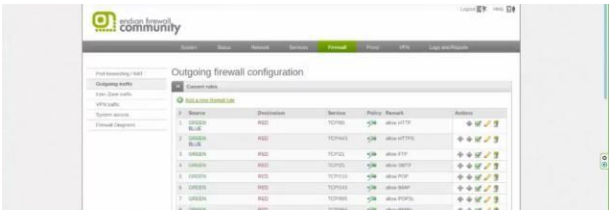
Se crea la regla que publica los servicios del servidor en la DMZ. En la regla seleccioné como destino la zona ORANGE y habilité la opción de NAT, de modo que todo el tráfico que llegue desde Internet (zona RED) sea redirigido hacia mi servidor de la DM.

Figura 44. Publicacion servicios DMZ

Fuente: Autoría propia (Juan Rave)

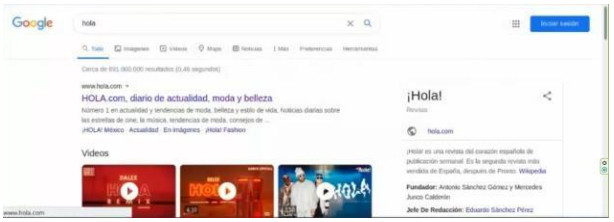
Outgoing traffic de Endian para definir las reglas de salida hacia Internet. estoy configurando las políticas que permiten que el tráfico desde las zonas internas pueda ir a la zona RED, autorizando servicios como HTTP (TCP/80), HTTPS y FTP TCP. Con estas reglas preparo el acceso de la LAN y de la DMZ hacia Internet, dejando registrado qué protocolos están permitidos para la comunicación hacia la WAN.

Figura 45. Outgoing traffic de Endian



Fuente: Autoría propia (Juan Rave)

Figura 46. Prueba de acceso a internet



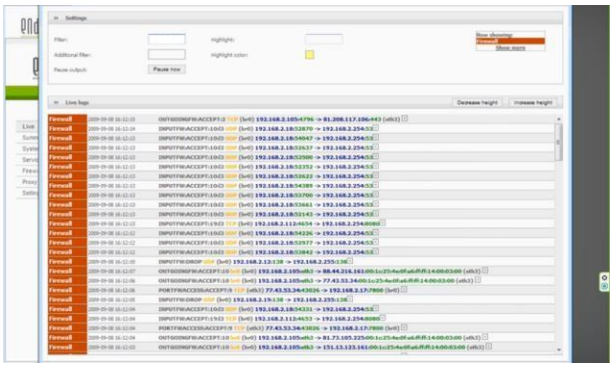
Fuente: Autoría propia (Juan Rave)

3.4.3 VERIFICAR EN EL TRÁFICO INTER - ZONA, LA CREACIÓN DE LAS REGLAS.

Ahora pues ingreso al módulo de Logs & Reports del firewall y abro Live logs para comprobar que las reglas de acceso entre zonas están funcionando.

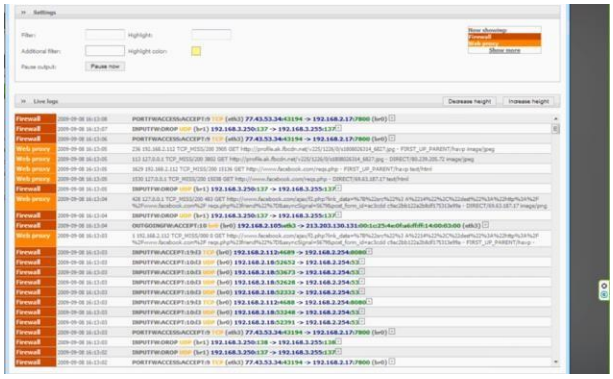
El tiempo real las entradas donde el firewall registra el tráfico ACCEPT y DROP, incluyendo la fecha y hora, el tipo de regla tráfico saliente o Inter-Zone y las IP de origen y destino. Al generar tráfico HTTP y FTP desde la zona verde hacia la zona naranja, verifico que aparecen líneas de registro correspondientes a mis reglas creadas, lo que me confirma que el firewall está aplicando correctamente la política definida para la Temática 4.

Figura 47. Logs



Fuente: Autoría propia (Juan Rave)

Figura 48. Logs UDP



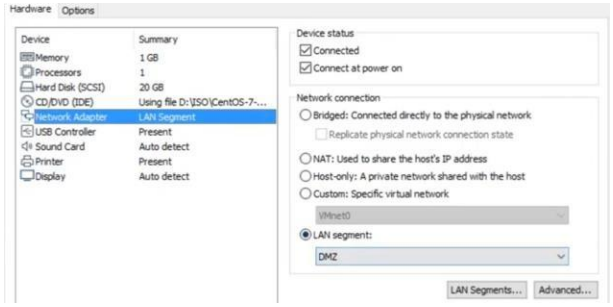
Fuente: Autoría propia (Juan Rave)

3.4.4 PROBAR DESDE UN NAVEGADOR WEB, LAS SIGUIENTES DIRECTIVAS: EL INGRESO DEL SERVICIO HTTP DESDE LA LAN HACIA LA ZONA DMZ.

Se había testeado en el 1er punto. Ya había configurado la tarjeta de red de la máquina virtual para que quede en el segmento LAN DMZ, de modo que pueda actuar como servidor dentro de la zona naranja y estar conectada al firewall Endian, desde una estación de trabajo en la zona verde (LAN).

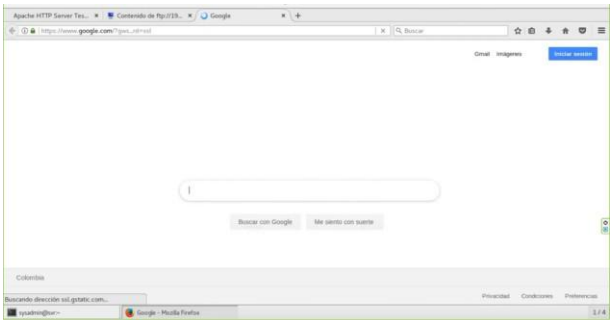
Se abre el navegador Firefox y accedí por HTTP al servidor web de la DMZ, comprobando que la comunicación GREEN → ORANGE funciona correctamente gracias a la regla Inter-Zone que creé previamente.

Figura 49. Red en DMZ



Fuente: Autoría propia (Juan Rave)

Figura 50. Acceso a internet con DMZ



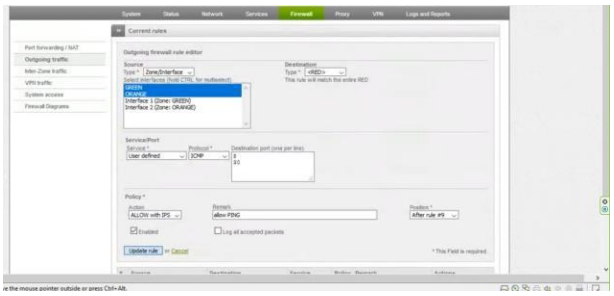
Fuente: Autoría propia (Juan Rave)

3.4.5 EL INGRESO DEL SERVICIO HTTP DESDE LA LAN HACIA LA WAN.

Cree todas las reglas de salida desde mi red interna hacia Internet. Selecciono como origen las zonas GREEN (LAN) y ORANGE (DMZ), y como destino toda la zona RED, que representa la conexión a la WAN.

Para permitir la navegación web desde la LAN hacia Internet configuro el servicio HTTP con protocolo TCP y puerto de destino 80, dejando la acción en ALLOW with IPS y la regla habilitada. De esta forma estoy autorizando el tráfico HTTP desde la red interna hacia la WAN, cumpliendo con la prueba "HTTP LAN → WAN (GREEN → RED)" de la temática 4. Permitimos el ping hacia DMZ para permitir el tráfico de salida.

Figura 51. Acceso a internet mediante las reglas



Fuente: Autoría propia (Juan Rave)

También que pueda ir a internet por cualquier servicio y protocolo.

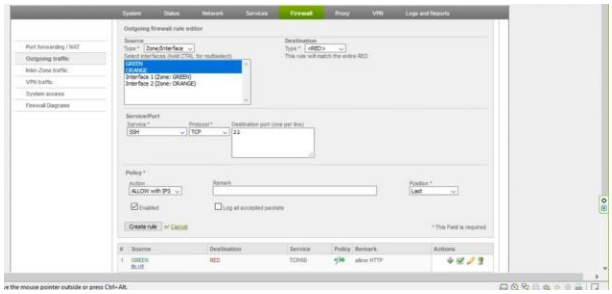
Figura 52. Configuracion HTTP

Fuente: Autoría propia (Juan Rave)

3.4.6 EL INGRESO DEL SERVICIO HTTP DESDE LA ZONA DMZ HACIA LA WAN.

Outgoing traffic cree una regla de tráfico saliente desde mis zonas internas GREEN y ORANGE hacia la zona RED (Internet). Para ello seleccioné como origen las interfaces GREEN y ORANGE, como destino la zona RED y elegí el servicio SSH con protocolo TCP y puerto 22, dejando la acción en ALLOW with IPS y la opción Enabled marcada.

Figura 53. Configuracion ICMP

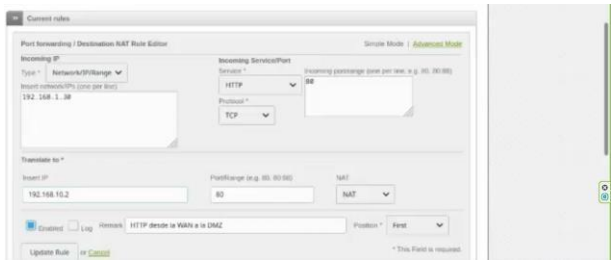


Fuente: Autoría propia (Juan Rave)

3.4.7 El ingreso del servicio HTTP desde la WAN hacia la zona DMZ.

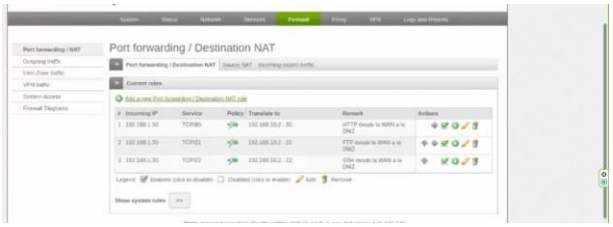
Se configuro en el paso 2, creé la regla para publicar mi servidor web de la DMZ hacia Internet. Especifico como IP de entrada la dirección pública de la WAN y como servicio selecciono HTTP/TCP, de forma que todo el tráfico que llegue por ese puerto se traduzca (DNAT) hacia la IP del servidor de la DMZ. En la tabla de reglas se ve cómo dejé configurado el acceso HTTP, FTP y SSH desde la WAN a la DMZ, lo que permite que los equipos externos puedan llegar a esos servicios del servidor ubicado en la zona naranja.

Figura 54. Configuracion TCP



Fuente: Autoría propia (Juan Rave)

Figura 55. Configuracion NAT

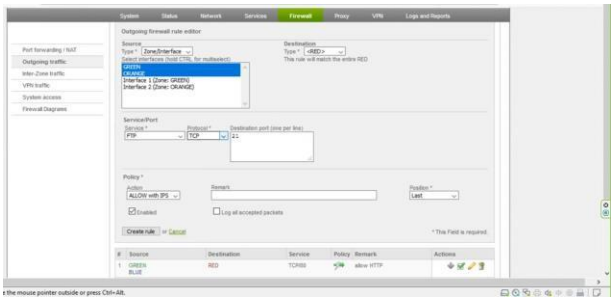


Fuente: Autoría propia (Juan Rave)

3.4.8 EL INGRESO DEL SERVICIO FTP DESDE LA LAN HACIA LA WAN.

Para crear la regla que permite que mi LAN pueda usar FTP hacia Internet. Se eligio como Source el tipo Zone/Interface y marqué la zona GREEN (y ORANGE para que la DMZ también salga), como Destination seleccioné RED para que la regla aplique hacia la WAN, y en Service/Port escogí el servicio FTP, protocolo TCP también configuré la Policy en ALLOW with IPS, dejé la regla y con Create rule habilité oficialmente el tráfico FTP desde la LAN hacia la WAN.

Figura 56. Configuracion FTP

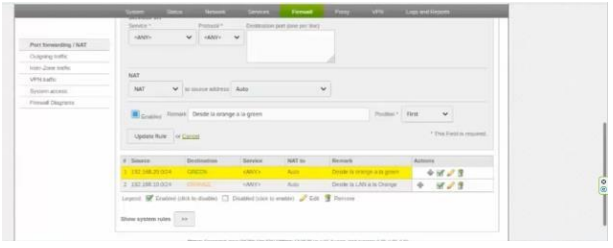


Fuente: Autoría propia (Juan Rave)

3.4.9 EL INGRESO DEL SERVICIO FTP DESDE LA WAN HACIA LA ZONA DMZ.

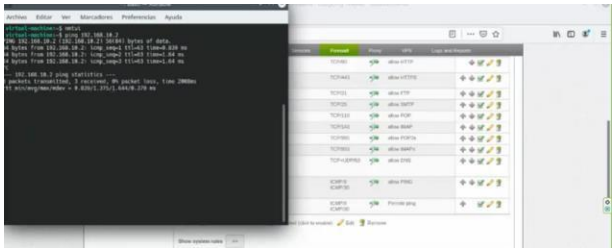
Creando la traducción entre mis redes internas. zona ORANGE/DMZ y destino GREEN, indicando en el campo Remark “Desde la orange a la green”. Con esta regla, todo el tráfico que salga desde la red hacia la red verde se traducirá usando NAT (modo Auto), lo que me permite controlar y registrar cómo se comunican los equipos de la DMZ con los de la LAN, como parte de las pruebas de acceso entre zonas de la Temática 4.

Figura 57. Configuración exitosa



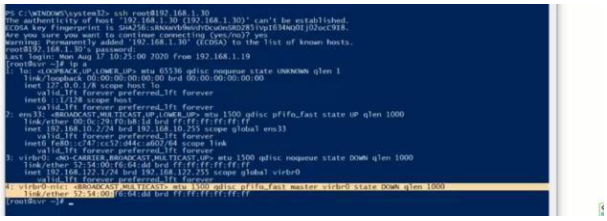
Fuente: Autoría propia (Juan Rave)

Figura 58. Prubas/ping



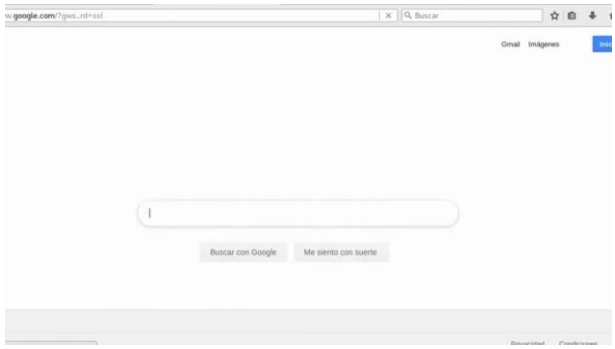
Fuente: Autoría propia (Juan Rave)

Figura 59. Pruebas ping



Fuente: Autoría propia (Juan Rave)

Figura 60. Acceso a internet exitoso



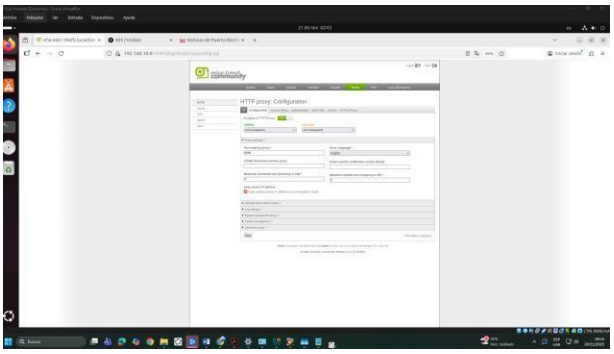
Fuente: Autoría propia (Juan Rave)

3.5 TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLITICAS DE AUTENTICACION PARA NAVEGACION EN INTERNET.

Producto esperado: Consiste en implementar un Proxy HTTP no transparente en Endian Firewall configurando un perfil de filtrado con una lista negra que bloquee el acceso a los sitios web www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Además, se debe habilitar autenticación por usuario, creando un usuario y asociándolo a un grupo, vinculando tanto el perfil de filtrado como la política de autenticación a la política de acceso. Finalmente, es necesario realizar pruebas desde la red LAN mediante un navegador web para comprobar que los portales incluidos en la lista negra son bloqueados correctamente.

Para comprender este paso, es importante tener claro lo que es un Proxy, que, según Fortinet, actúa como un intermediario entre usuarios y la web, intercepta el tráfico para aplicar filtros de seguridad, controlar el acceso a sitios restringidos y puede mejorar la velocidad usando almacenamiento en caché [12].

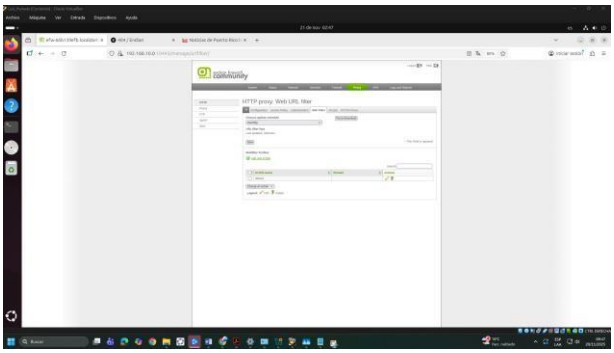
Figura 61. Proxy HTTP Habilitado



Fuente: Autoría propia (Luis Hurtado)

Ingreso a Web Filter y creacion de nuevo perfil

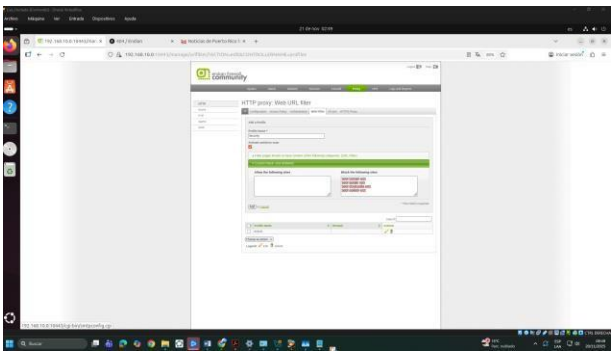
Figura 62. Creacion de perfil



Fuente propia (Luis Hurtado)

Bloqueo de paginas hotmail, google y elnuevodia.

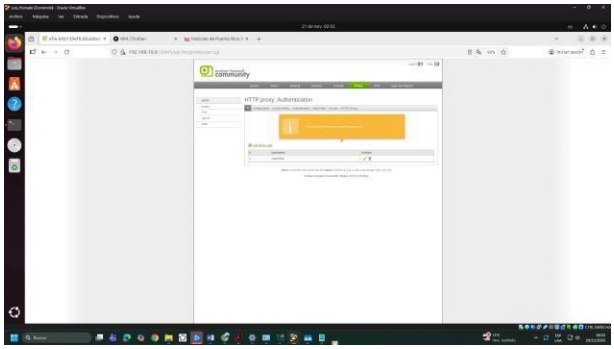
Figura 63. Bloqueo de URL



Fuente: Autoría propia (Luis Hurtado)

Ingreso a Autenticacion, en administracion de usuarios, creamos u nuevo usuario y asignamos contraseña

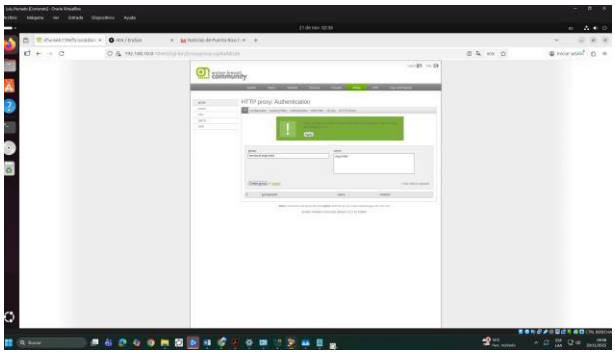
Figura 64. Usuario creado exitosamente.



Fuente: Autoría propia (Luis Hurtado)

Administramos los grupos y creamos un nuevo grupo y no vinculamos al usuario creado en la figura 28.

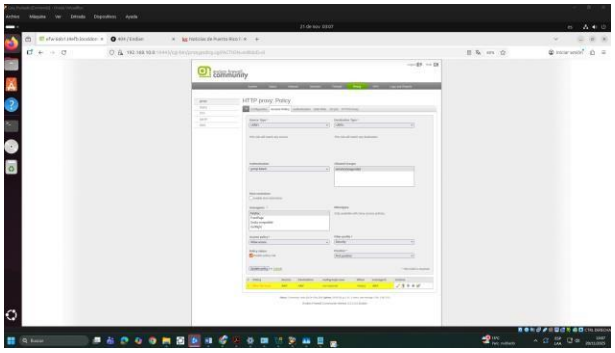
Figura 65. Grupo creado exitosamente.



Fuente: Autoría propia (Luis Hurtado)

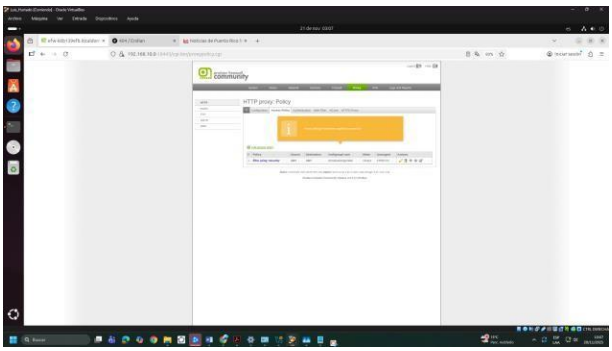
Accedemos a la política de acceso y la configuramos con el grupo que creamos, es decir “Tematica5seguridad” y configuramos también el perfil “Security”, seleccionamos el navegador donde se aplicara la politica y damos clic en actualizar política.

Figura 66. Configuracion de la Política de acceso.



Fuente: Autoría propia (Luis Hurtado)

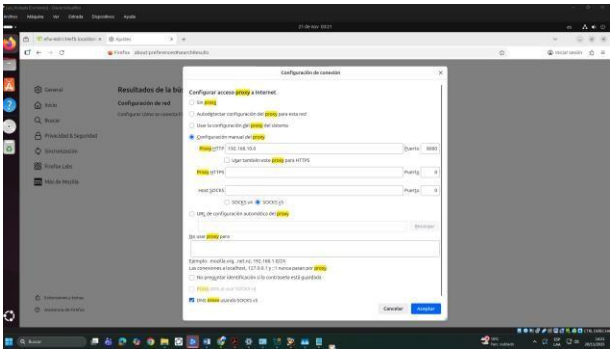
Figura 67. Politica configurada exitosamente.



Fuente: Autoría propia (Luis Hurtado)

Configuración del proxy en el navegador de manera manual y digitamos la IP Verde para que reconozca la politica creada.

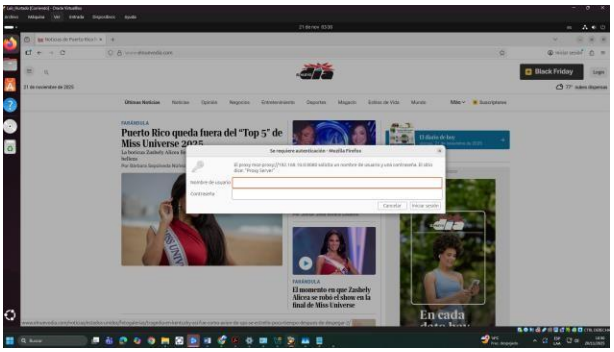
Figura 68. Política configurada exitosamente.



Fuente: Autoría propia (Luis Hurtado)

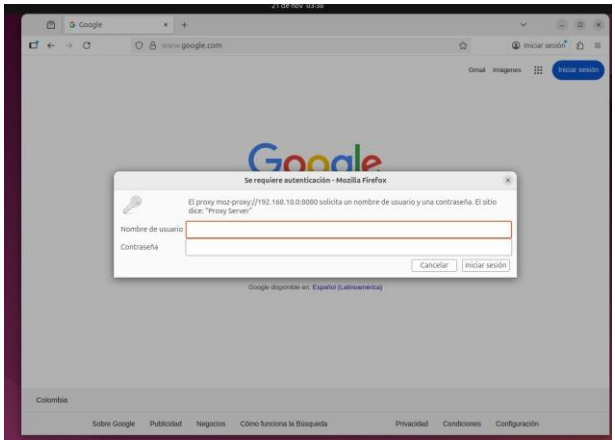
Probando la política en el sitio www.elnuevodia.com

Figura 69. Solicita autenticacion para navegar en el sitio.



Fuente: Autoría propia (Luis Hurtado)

Figura 70. Solicita autenticacion para navegar en el sitio.



Fuente: Autoría propia (Luis Hurtado)

4 CONCLUSIONES

Gracias a la comprensión de los conceptos preliminares y la adecuada implementación de una arquitectura de seguridad perimetral fue posible pasar de la fundamentación teórica de firewalls y zonas de seguridad a una implementación técnica en entornos virtualizados. Se pudo comprobar que la segmentación estricta del tráfico entre las zonas WAN, LAN y DMZ es viable mediante el uso de conmutadores virtuales aislados y la instalación efectiva de Endian Firewall, con lo cual se verificó no solo la compatibilidad del hardware virtualizado, sino que también se habilitó la gestión centralizada del flujo de datos organizacional, por tanto se pudo apreciar cómo desde un entorno de virtualizado se puede dimensionar e implementar una infraestructura jerárquica y segura aplicable a múltiples entornos.

A partir del análisis de la configuración y las reglas NAT en Endian Firewall, se puede concluir que este mecanismo es fundamental para permitir la comunicación segura entre la red interna y el Internet. La traducción de direcciones (NAT) no solo oculta las IP privadas detrás de una dirección pública, sino que también controla qué servicios pueden ser accesibles desde el exterior. Esto garantiza que los equipos internos naveguen sin exponer su identidad real y que solo los puertos autorizados sean redirigidos a servidores específicos dentro de la red. En términos prácticos, comprender estas reglas nos permite administrar mejor la seguridad, evitar accesos no deseados y asegurar que el tráfico fluya correctamente según las necesidades de la organización. En general, aprender a interpretar y configurar NAT nos da una visión más clara de cómo se construye y protege una infraestructura de red moderna.

Las pruebas de conectividad HTTP y FTP evidenciaron la importancia de revisar detalladamente las reglas de firewall y NAT para asegurar la disponibilidad de los servicios. Los registros mostraron conexiones rechazadas, lo que señala la necesidad de ajustar algunas reglas. Una configuración adecuada de interfaces y servicios optimiza el acceso y fortalece la seguridad de la red al evitar bloqueos innecesarios.

Mediante la configuración de reglas de reenvío de puertos (Port Forwarding), se logró exponer de manera controlada los servicios HTTP y FTP alojados en la zona naranja (DMZ) hacia la red externa, manteniendo un estricto aislamiento respecto a la red corporativa (LAN). Este despliegue demostró que se puede garantizar la disponibilidad y accesibilidad de servicios públicos sin comprometer la confidencialidad e integridad de la infraestructura interna, haciendo visibles los principios de defensa estricta.

La implementación del Proxy HTTP no transparente en Endian Firewall permitieron establecer un control efectivo sobre la navegación en la red LAN mediante mecanismos de autenticación y filtrado de contenido. La configuración del perfil con lista negra y su asociación a una política de autenticación por usuario garantizó que solo los usuarios autorizados pudieran acceder a Internet y que los sitios web definidos como restringidos fueran bloqueados correctamente. Las pruebas realizadas desde el equipo cliente evidenciaron que el sistema solicita credenciales antes de permitir la navegación y que los dominios indicados fueron denegados de forma exitosa, esta práctica demuestra la importancia del uso de proxies como herramienta de gestión de seguridad y políticas de acceso en entornos corporativos.

5 REFERENCIAS

[1] Endian. (s.f.). *Endian Firewall Community: The Open Source UTM*. Recuperado el 21 de noviembre de 2025, de https://www.endian.com/community/

[2] Endian, "Getting started," en *Endian UTM 3.2 Reference Manual*. Consultado: Nov. 21, 2025. [En línea]. Disponible: https://docs.endian.com/3.2/utm/first.html#the-zones

[3] Fortinet, "¿Qué es un firewall? Definición y tipos de firewall," *Fortinet Cyberglossary*. Consultado: Nov. 21, 2025. [En línea]. Disponible: https://www.fortinet.com/lat/resources/cyberglossary/firewall

[4] Fortinet, "What Is a Network Access Control List (ACL)?," *Fortinet Cyberglossary.* Consultado: Nov. 23, 2025. [En línea]. Disponible: https://www.fortinet.com/resources/cyberglossary/network-access-control-list

[5] Fortinet, "What is HTTP Proxy?," *Fortinet Cyberglossary*. Consultado: Nov. 23, 2025. [En línea]. Disponible: https://www.fortinet.com/uk/resources/cyberglossary/http-proxy

[6] IBM, *"Topología de red"* Ibm.com, Jan. 31, 2024. https://www.ibm.com/mx-es/think/topics/network-topology

[7] J. Postel and J. Reynolds, "File Transfer Protocol (FTP)," *IETF RFC 959*, Oct. 1985. [En línea]. Disponible: https://datatracker.ietf.org/doc/html/rfc959

[8] J. Postel, "Internet Control Message Protocol," *IETF RFC 792*, Sep. 1981. [En línea]. Disponible: https://datatracker.ietf.org/doc/html/rfc792

[9] Lenovo Colombia, "¿Qué es una NIC? ¿Para qué funciona?," *Glosario Lenovo*. Consultado: Nov. 21, 2025. [En línea]. Disponible: https://www.lenovo.com/co/es/glosario/nic/

[10] P. Srisuresh and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations," *IETF RFC 2663*, Aug. 1999. [En línea]. Disponible: https://datatracker.ietf.org/doc/html/rfc2663

[11] Red Hat, "Chapter 17. Configuring virtual machine network connections," en *Configuring and managing virtualization - Red Hat Enterprise Linux 9*. Consultado: Nov. 21, 2025. [En línea]. Disponible: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/configuring_and_managing_virtualization/configuring-virtual-machine-network-connections_configuring-and-managing-virtualization

[12] R. Fielding, M. Nottingham, and J. Reschke, "HTTP Semantics," *IETF RFC 9110*, Jun. 2022. [En línea]. Disponible: https://www.rfc-editor.org/rfc/rfc9110.html