LINUX: UN CAMINO Y UNA MIRADA HACIA EL MUNDO DE LA NUEVA GENERACIÓN EN INFORMACIÓN Y SEGURIDAD

Rafael Gustavo Guillen Mendoza
e-mail: rgguillenm@unadvirtual.edu.co
Luis Alberto De Los Reyes Movilla
e-mail: ladelosreyesm@unadvirtual.edu.co
Adrian Miguel Osorio Marsiglia
e-mail: amosorioma@unadvirtual.edu.co
Neftali Uscategui Perez
e-mail: nuscateguip@unadvirtual.edu.co
Bernardo Mejia Jimenez
e-mail: bmejiaj@unadvirtual.edu.co

RESUMEN**:** *Este artículo presenta la implementación de una solución de seguridad de red utilizando Endian UTM (Unified Threat Management) sobre un entorno virtualizado. A través de cinco temáticas, se configuraron zonas de red (GREEN, ORANGE y RED) para segmentar el tráfico y aplicar controles específicos. Además, se establecieron reglas de NAT para permitir la comunicación controlada entre zonas y hacia Internet. La configuración incluyó un proxy HTTP con autenticación y restricciones de acceso, así como una zona DMZ para alojar servicios expuestos de forma segura. Esta arquitectura permite aplicar políticas de seguridad diferenciadas, mejorar el control de tráfico y proteger la red interna frente a amenazas externas.*

PALABRAS CLAVE: Endian, Firewall, NAT, VirtualBox.

1 INTRODUCCIÓN

La seguridad perimetral en redes informáticas es fundamental para proteger los activos de información contra amenazas tanto internas como externas [1]. Una estrategia efectiva para lograr este objetivo es la implementación de sistemas UTM (Unified Threat Management) que combinan múltiples funciones de seguridad en un solo dispositivo, incluyendo firewall, sistema de detección/prevención de intrusiones, filtrado de contenido y proxies de aplicación.

En este trabajo se aborda la implementación de GNU/Linux Endian como solución UTM en un entorno virtualizado mediante Oracle VM VirtualBox, configurando diferentes zonas de seguridad e implementando políticas específicas para controlar el tráfico entre ellas. Esta aproximación permite demostrar cómo establecer una infraestructura segura y segmentada utilizando herramientas de código abierto.

2 INSTALACIÓN ENDIAN

2.1 CARACTERÍSTICAS GENERALES

En primer lugar, se descarga la distribución de Endian UTM desde su sitio oficial y se instala en plataformas como VirtualBox o en hardware físico. Es compatible con arquitecturas x86. Se utiliza el programa Oracle VM VirtualBox para la creación de una máquina virtual con las siguientes configuraciones:

- Tipo: Linux
- Versión: RedHat (64 bit)
- Unidad óptica virtual: ISO
- 3 interfaces de red.

2.2 INSTALACIÓN

Para la implementación del firewall Endian se procedió con la creación de una máquina virtual que permite simular las diferentes zonas de red: LAN (verde), DMZ (naranja) e Internet (roja).

Configuración de la máquina virtual

Inicialmente se procedió con la creación de una nueva máquina virtual en VirtualBox, asignándole un nombre representativo y seleccionando un sistema operativo Linux, tipo "RedHat (64-bit)", con una memoria RAM de al menos 2048 MB.

En cuanto al almacenamiento, se creó un disco duro virtual de tipo VDI con un tamaño dinámico y una capacidad mínima de 8 GB. Este espacio es suficiente para la instalación base de Endian y sus componentes esenciales.

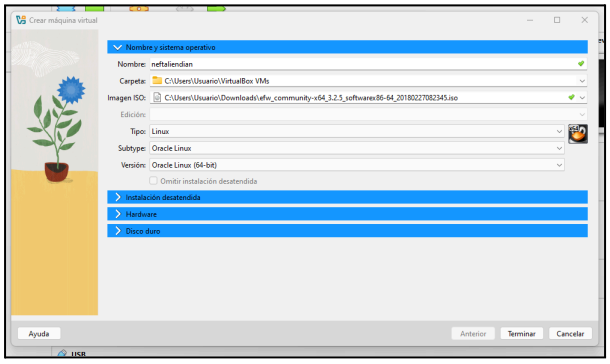

Figura 1. Creación de máquina virtual

Asignación de adaptadores de red

La configuración de red de la máquina virtual se ajustó para simular las tres zonas funcionales del firewall:

Adaptador 1 (RED o ROJA): Se puede configurar como Adaptador puente, simulando la red externa o acceso a Internet, o como adaptador NAT, obteniendo una IP dentro del conjunto de controladores que instala Virtual Box.

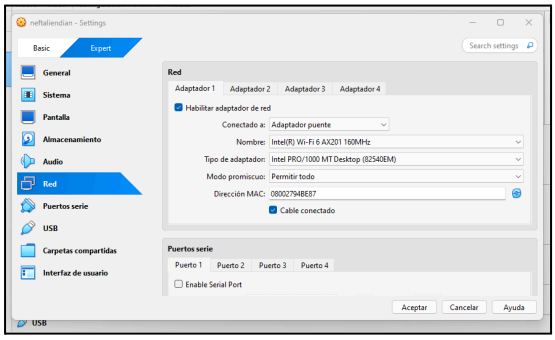

Figura 2. Configuración de adaptador puente 1.

Adaptador 2 (GREEN): Este se estableció como Red interna, representando la LAN. Se creó una red interna con nombre personalizado (GREEN o VERDE) para asegurar la comunicación entre máquinas virtuales conectadas a esta misma red.

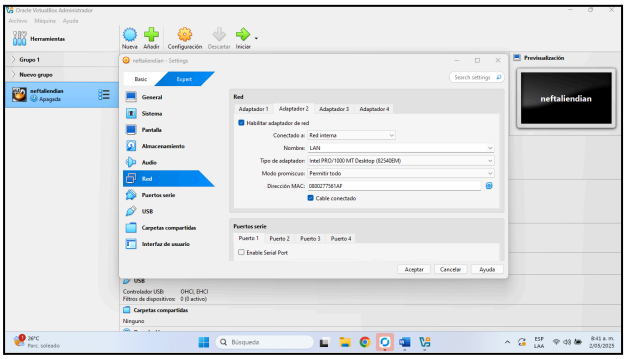

Figura 3. Configuración de adaptador puente 2.

Adaptador 3 (ORANGE o NARANJA): También configurado como Red interna, corresponde a la zona DMZ, donde se alojarán los servidores públicos como HTTP y FTP

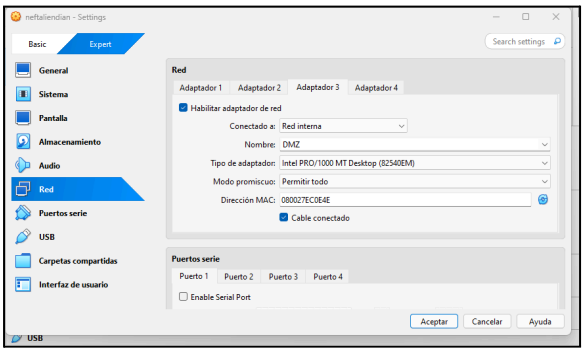

Figura 4. Configuración de adaptador puente 3.

Esta configuración permite que Endian actúe como intermediario y filtro entre estas zonas, controlando el tráfico según las políticas establecidas.

Instalación del sistema Endian

Una vez configurada la máquina virtual, se inició la instalación del sistema operativo Endian desde el archivo ISO previamente descargado. El instalador guiado permite seleccionar el idioma de preferencia y confirmar la creación automática de las particiones necesarias en el disco.

Durante el proceso, se deshabilitó el acceso al firewall mediante puerto serial (opción "No") al no ser requerido en este entorno virtualizado.

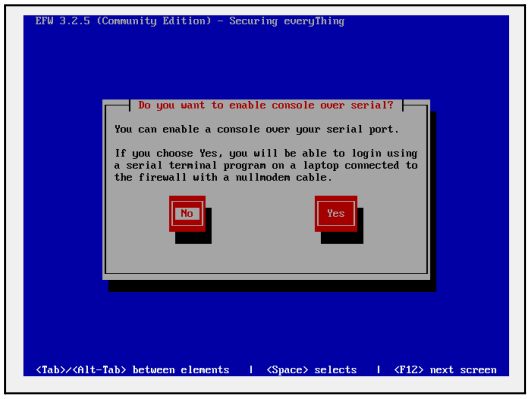

Figura 5. Negamos la habilitación de puerto serial.

Posteriormente, se solicitó la configuración de la red GREEN, especificando manualmente la dirección IP y la máscara de subred. Esta dirección será utilizada para acceder a la interfaz web de administración del firewall.

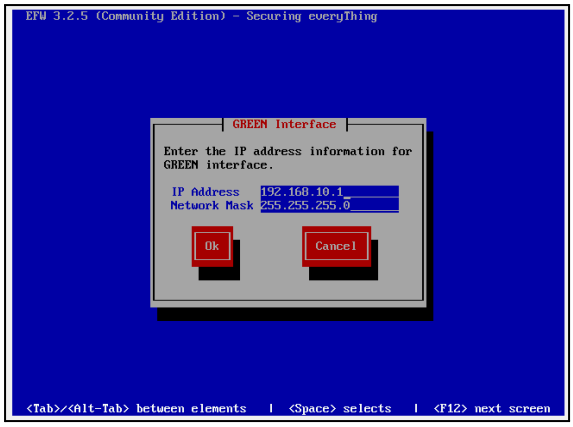

Figura 6. Establecimiento de ip GREEN.

Primer arranque y verificación

Una vez completada la instalación, se reinició la máquina virtual. Al finalizar el arranque, se presentó en pantalla la dirección IP asignada a la interfaz verde, confirmando que el sistema se encuentra activo y listo para su administración desde un navegador web de la LAN.

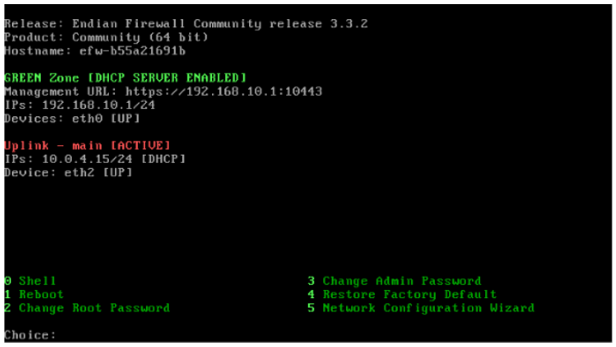

Figura 7. Evidencia de inicio de endian.

3 DESARROLLO TEMATICAS

3.1 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUAL BOX (TARJETA DE RED) E INSTALACIÓN EFECTIVA DEL MISMO.

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).

Se crea él diagrama de RED en zonas Endian, que se utilizará a para el desarrollo de todos los ejercicios, con su respectivas Zonas Roja (WAN), Zona Anaranjada (DMZ), Zona Verde (LAN), y el Firewall Endian que actúa como puente y escudo entre zonas.

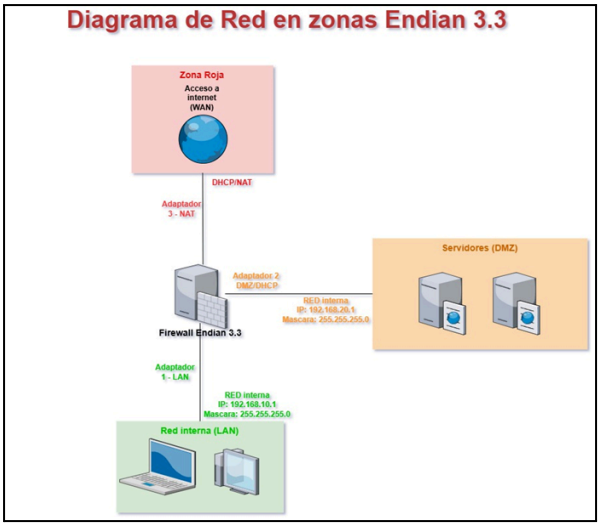

Figura 8. Diagrama de Red de endian.

Seguidamente se realiza la configuración de la RED de Ubuntu Server, aplicando la Zona naranja (DMZ), al igual que la RED para el equipo desktop, asignándole la zona verde (LAN).

Se prosigue con la configuración inicial del Endian ingresando por el navegador Web de preferencia, seguidamente se selecciona el idioma y la zona horaria para Endian, a través del desktop, y se aceptan los términos de la licencia GNU-GPL, y se procede con la asignación de las contraseñas de Endian, para el acceso por web, y para el SSH.

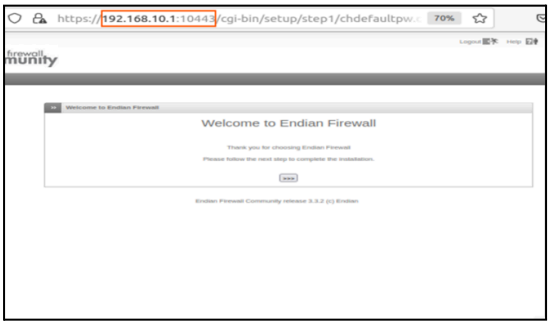

Figura 9. Configuración Inicial de Endian.

Se continua con el asistente de configuración de Red de cada zona, la zona Roja tiene un método de Red de enrutamiento y tiene un tipo de enlace DHCP, y contamos con tres interfaces.

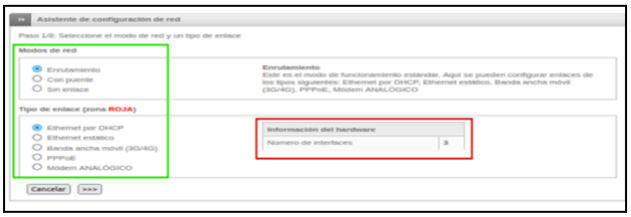

Figura 10. Configuración Inicial de Endian DHCP.

Se procede a configurar la zona naranja, asignándole la IP, establecida en el diagrama de RED.

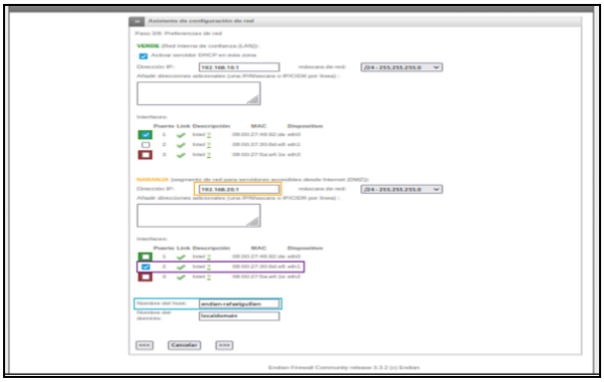

Figura 11. Configuración Inicial de Endian Red Naranja.

Se evidencian las 3 zonas activas, y se configura el DNS de forma automática. Al dar clic en siguiente se evidencia el mensaje de confirmación, guardado correctamente en Endian de las configuraciones.

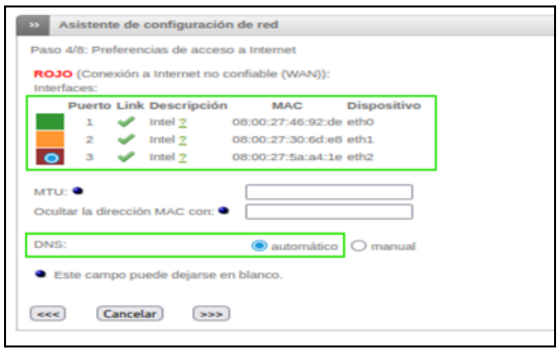

Figura 12. Configuración Inicial de Endian DNS.

Finalmente se ingresa al panel de control principal del Firewall Endian, después de ingresar el usuario y contraseña previamente establecidos.

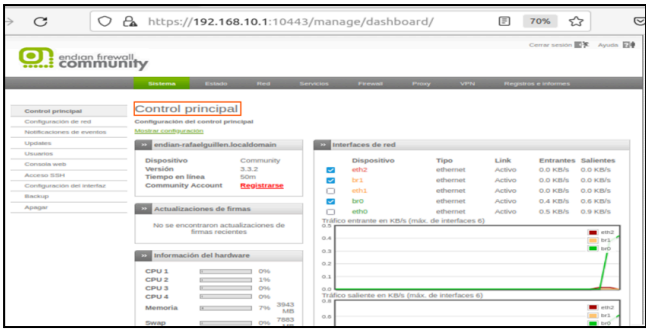

Figura 13. Panel de Control de Endian.

Seguidamente se le asigna una IP estática al Server, y se verifica la conexión entre el Server y Endian.

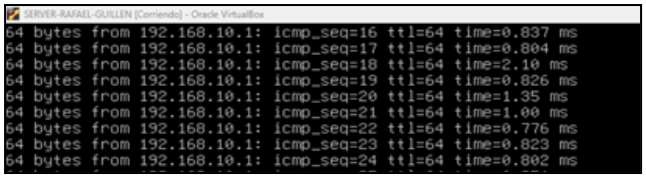

Figura 14. Conexión Server-Endian.

Finalmente se comprueba el acceso desde el desktop a la zona roja, esta validación se realiza confirmando el acceso a internet.

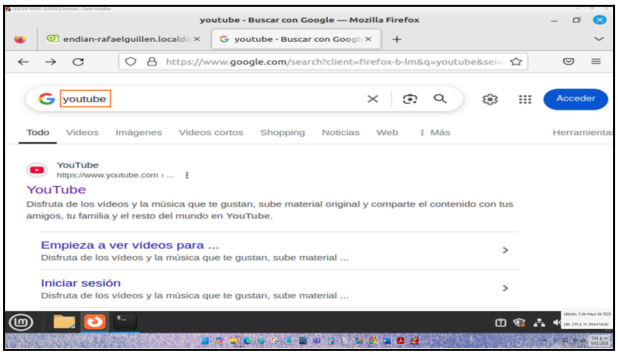

Figura 15. Conexión a Internet Desktop-Endian.

Se evidencia el funcionamiento de los tres ambientes ejecutándose simultáneamente.

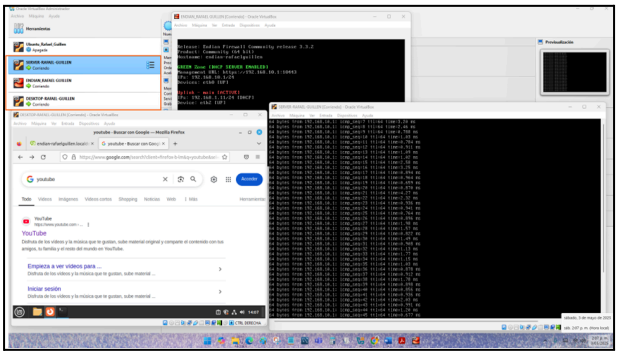

Figura 16. Funcionamiento Simultáneo.

Finalmente se evidencian las tres zonas en ejecución mediante el Firewall Endian.

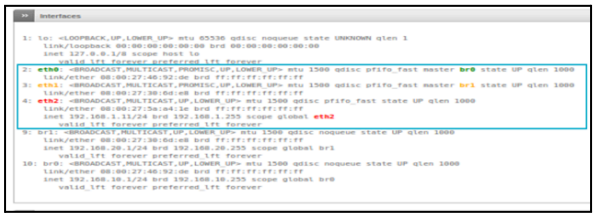

Figura 17. Tres Zonas en Ejecución Endian.

3.2 TEMÁTICA 2: CONFIGURACIÓN NAT

Producto esperado: Configurar la regla de NAT (Network Address Translation / Traducción de Direcciones de Red), demostrando el establecimiento de la comunicación desde la LAN hacia la WAN (Red simulada de Internet).

Configurar la regla de NAT, demostrando el establecimiento de la comunicación de la Zona DMZ hacia Internet. Verificar en el reenvío de puertos / NAT, la creación de las reglas.

Configuración de la VM con Endian.

Para el desarrollo de esta temática, se usará como referencia, el diagrama de red de la temática 1 (Figura 8).

Se agrega una VM de tipo Linux RedHat, con 3 tarjetas de red. Tal configuración es la misma indicada en el punto 2 (Instalación Endian) de este documento.

Para la zona GREEN, se utilizó una máquina virtual con Debian y entorno GNOME, la cual estará conectado al segmento de red 192.168.10.x. En la zona ORANGE, se desplegó un servidor Ubuntu Server con Apache2 instalado, la cual estará conectado al segmento de red 192.168.20.x. La red RED se configuró a través de la interfaz NAT de Endian OS, obteniendo una IP asignada automáticamente (en este caso 10.0.4.15). Esto permitirá que nuestra red local tenga conexión a Internet.

Desde la consola de administración de Endian se habilitaron los servicios DHCP (Figura 18) correspondientes y se configuraron las reglas de redireccionamiento de puertos, como se muestra en la Figura 18.

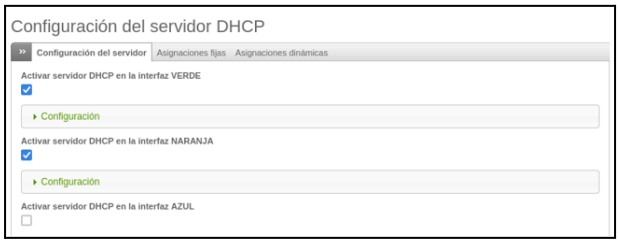

Figura 18. Configuración de DHCP en Endian.

La regla principal redirige el tráfico recibido desde la red RED (NAT) en el puerto 8080 hacia la IP del servidor Ubuntu en la zona ORANGE (192.168.20.2) por el puerto 80. Esto permite acceder a los servicios web ubicados en la DMZ desde redes externas o simuladas.

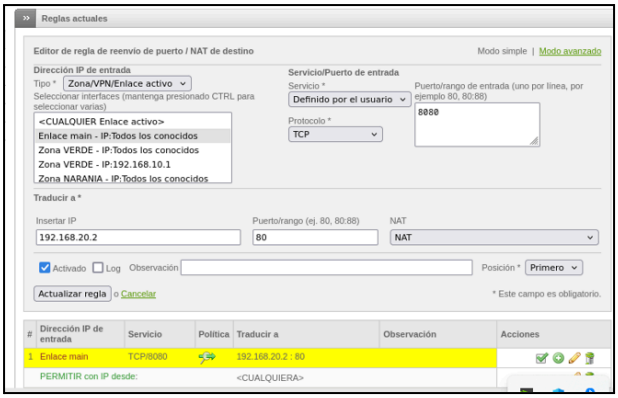

Figura 19. Configuración de la regla de redirección de puerto.

Como lo muestra la Figura 20, se verificó el funcionamiento accediendo desde un navegador web en la red GREEN a la IP de la interfaz NAT (10.0.4.15:8080), comprobando que el tráfico fue correctamente redireccionado al servidor web de la zona ORANGE. Este comportamiento valida la correcta implementación de las reglas NAT y de reenvío de puertos configuradas en Endian.

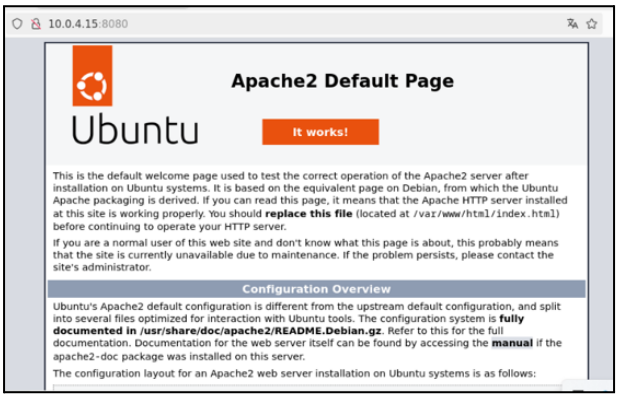

Figura 20. Redirección desde la red ROJA o WAN.

Así mismo se verifica que es posible acceder desde la red GREEN o VERDE hasta el host con Ubuntu Server (192.168.20.2) en zona NARANJA, como se muestra en la Figura 21.

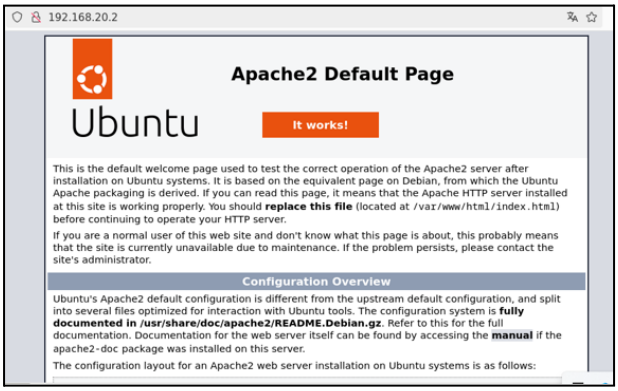

Figura 21. Redirección desde la red VERDE o LAN.

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

La segmentación de redes mediante zonas como LAN, DMZ y WAN permite establecer niveles diferenciados de seguridad, donde cada zona está sujeta a políticas específicas de acceso. En entornos corporativos, es común aislar los servidores accesibles desde Internet –como los servidores web y FTP– en una zona DMZ. Esta arquitectura permite proteger la red interna (LAN) de posibles ataques, al tiempo que garantiza la prestación de ciertos servicios hacia el exterior. La configuración de estas políticas recae en los dispositivos firewall, los cuales definen el tipo de tráfico permitido entre zonas

El objetivo de la implementación es permitir los servicio HTTP (puerto 80) y FTP (puerto 21) desde un servidor web basado en Ubuntu Server, así como denegar el protocolo ICMP (tipo 8 y tipo 30), bloqueando la funcionalidad de ping dentro de la red. Para validar esta configuración, se realizan pruebas desde la consola, verificando la ausencia de respuesta al comando ping, asi como la creacion y aplicacion efectiva de las reglas de tráfico saliente

El primer paso consiste en acceder a la interfaz de administración web del cortafuegos Endian Firewall, la cual se encuentra disponible a través de un navegador utilizando la dirección IP asignada al firewall, en nuestro caso https://192.168.0.15. Una vez dentro, se procede a autenticar al usuario utilizando las credenciales administrativas configuradas previamente. Este entorno web proporciona acceso a todas las funciones del firewall, incluyendo la gestión de zonas de red, reglas de tráfico y servicios.

Desde el módulo de Firewall > Reglas se procede a crear políticas explícitas que permitan el acceso desde la red roja (internet) hacia los servicios alojados en la DMZ.

1. **Regla para HTTP:** Se configura una regla que permita el tráfico TCP desde cualquier origen hacia la dirección IP del servidor web en la DMZ, por el puerto 80, como muestra la Figura 22. Esta regla permite que usuarios externos accedan al servicio web público.

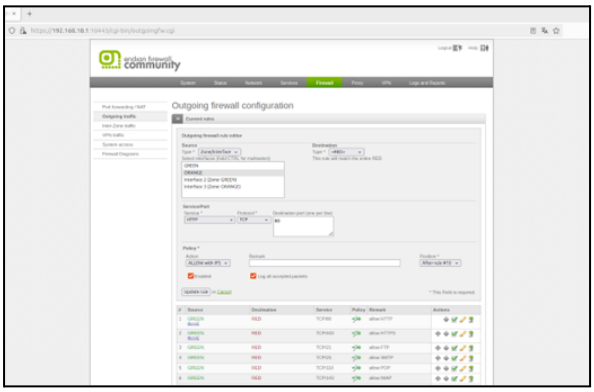

Figura 22. Creación de regla para HTTP

2. **Regla para FTP:** De forma análoga, se crea una regla para permitir el tráfico TCP por el puerto 21 destinado al servidor FTP, como muestra la Figura 23. Es importante tener en cuenta que FTP requiere configuraciones adicionales para los puertos pasivos si se utiliza en modo pasivo.

Figura 23. Creación de regla para FTP

Como medida de seguridad, se implementó una política que niega explícitamente el tráfico ICMP —protocolo utilizado para realizar solicitudes de eco (ping)— desde la zona verde (LAN) hacia la DMZ o hacia otras zonas, como se muestra en la Figura 24. Esta configuración se realizó desde la sección Firewall > Reglas, mediante una política de denegación específica para el protocolo ICMP. De este modo, se mitigan posibles intentos de reconocimiento o escaneo de red por parte de usuarios internos.

Figura 24. Política para bloqueo de tráfico ICMP

Las pruebas de conectividad mostraron que la segmentación y las reglas por zona funcionan correctamente. Se evidenció que el orden de las reglas en Endian es fundamental, ya que una regla de ALLOW mal posicionada podría sobrescribir una denegación deseada.

Además, para comprobar la efectividad de la regla de bloqueo ICMP, se realizó una prueba de ping desde el servidor Ubuntu en la zona DMZ hacia el servidor DNS público 8.8.8.8. El resultado fue una pérdida del 100% de los paquetes transmitidos, confirmando que el tráfico ICMP está siendo correctamente filtrado por la regla del firewall. La Figura 25 muestra la captura de dicha prueba:

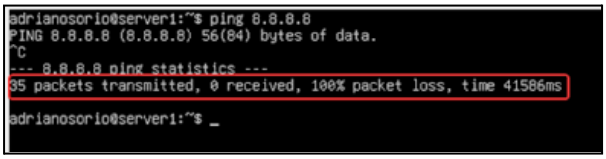

Figura 25. Prueba de bloqueo de ICMP (ping fallido)

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

Producto esperado: Configuración de reglas de acceso en un firewall para controlar el tráfico, permitiendo servicios legítimos y bloqueando el no deseado. Incluye definir políticas de seguridad, configurar reglas por puerto y protocolo, usar NAT para redirección de tráfico, verificar registros y realizar pruebas de conectividad para asegurar su efectividad y seguridad.

La correcta configuración de reglas de acceso en un firewall es fundamental para garantizar la seguridad de una red. En esta fase del proyecto, se implementaron las reglas necesarias en Endian Firewall con el fin de permitir servicios esenciales y bloquear accesos no deseados, estableciendo un control granular del tráfico entre las zonas GREEN (LAN), ORANGE (DMZ) y RED (WAN).

La configuración inició con el acceso a la interfaz gráfica del firewall mediante autenticación con usuario y contraseña, como se muestra en la Figura 26. Luego, se procedió a configurar la zona RED (WAN) en modo DHCP para obtener automáticamente su dirección IP. Se definieron las interfaces de red para las tres zonas: GREEN (192.168.10.1), ORANGE (192.168.20.1) y RED (por DHCP), estableciendo las bases de conectividad necesarias entre las diferentes redes simuladas.

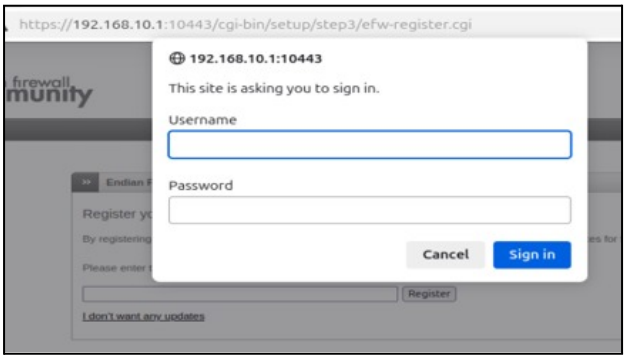

Figura 26. Autenticación de usuario y contraseña Endian

Una vez establecidas las zonas, se crearon reglas de Port Forwarding (NAT) para permitir el tráfico HTTP (puerto 80) y FTP (puerto 21) como se muestra en la Figura 27 y 28, desde la zona GREEN hacia la zona ORANGE. Estas reglas garantizan que los clientes en la LAN puedan acceder a los servicios web y FTP ofrecidos por un servidor ubicado en la DMZ. Del mismo modo, se configuraron reglas que permiten el acceso desde la RED (Internet simulada) hacia la zona ORANGE para los mismos servicios.

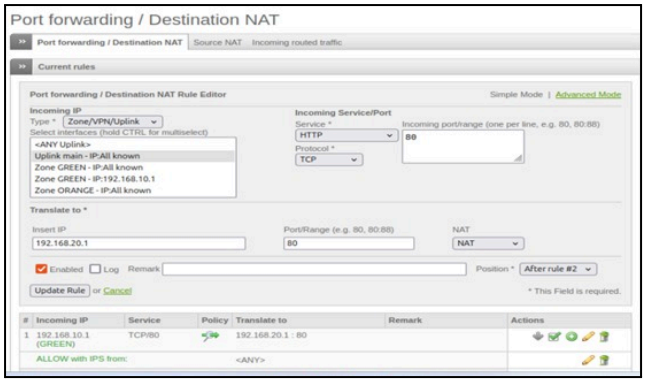

Figura 27. Configuración de regla puerto 80.

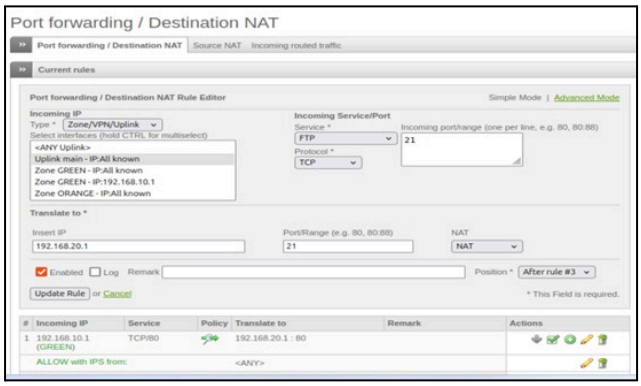

Figura 28. Configuración de regla puerto 21.

Cada una de estas reglas fue verificada mediante el monitoreo de los registros del firewall en tiempo real, como se muestra en la Figura 29. Observando que el tráfico fue aceptado correctamente y redirigido al servidor en la DMZ. Esta etapa confirmó que los paquetes eran procesados conforme a las políticas establecidas, lo cual valida la eficacia de las configuraciones implementadas.

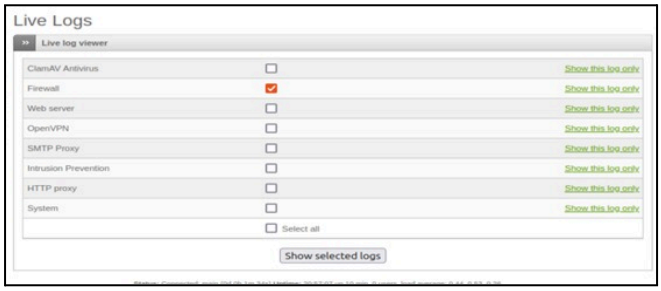

Figura 29. Verificación de logs.

Adicionalmente, se verificó el acceso del servicio HTTP desde LAN a WAN y desde WAN a DMZ, como se muestra en la Figura 30.

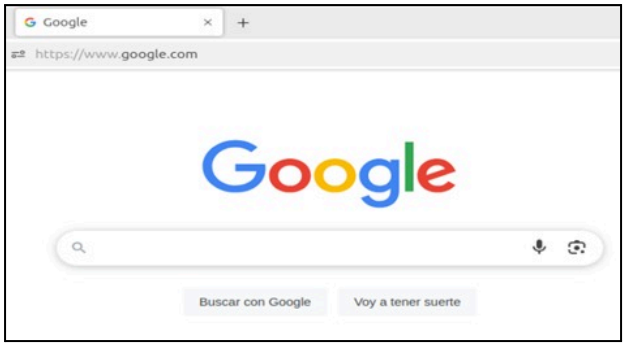

Figura 30. Tráfico HTTP desde la LAN hacia la WAN.

Finalmente, la configuración se consolidó aplicando y guardando todas las reglas, asegurando la persistencia de los cambios tras reinicios del sistema. Esta temática demuestra la capacidad de Endian para implementar políticas de seguridad robustas mediante reglas de acceso personalizadas, fortaleciendo la defensa perimetral de una red segmentada.

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

Producto esperado: El producto esperado consiste en crear un perfil y establecer una lista negra que bloquee los sitios www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Además, se debe implementar la autenticación por usuario, creando un usuario y asignándole a un grupo, estableciendo una política de acceso y vinculando esta política con el perfil creado. Finalmente, se debe probar el acceso a los sitios bloqueados desde la LAN utilizando un navegador web.

Como se muestra en la Figura 31, se creó un usuario desde el módulo de autenticación de Endian UTM, lo cual permite establecer identidades únicas para los dispositivos o personas que acceden a la red interna. Esta funcionalidad es esencial para implementar políticas de control de acceso basadas en autenticación, ya que cada usuario puede asociarse a reglas específicas de navegación, filtros de contenido o niveles diferenciados de privilegio.

Más allá de habilitar el inicio de sesión, la gestión de usuarios facilita una administración precisa y segura del tráfico dentro de la red. En entornos donde se requiere monitoreo, restricciones o auditoría por usuario como instituciones educativas o redes corporativa, esta capacidad garantiza un control individualizado, asegurando trazabilidad y cumplimiento de las políticas organizacionales establecidas

Figura 31. Creación de usuarios.

Como se muestra en la Figura 32, se creó un grupo denominado "neftali" y se asoció al usuario previamente registrado desde el módulo de gestión de usuarios de Endian. Esta acción permite estructurar el control de acceso a la red agrupando usuarios según perfiles comunes. En este caso, al integrar al usuario administrador en dicho grupo, se habilita la aplicación centralizada de políticas de navegación específicas, como autenticación obligatoria, restricciones horarias o filtros de contenido.

La funcionalidad de agrupar usuarios simplifica la administración de reglas dentro del proxy HTTP, ya que evita configuraciones individuales y garantiza coherencia en la aplicación de normativas internas de uso de red.

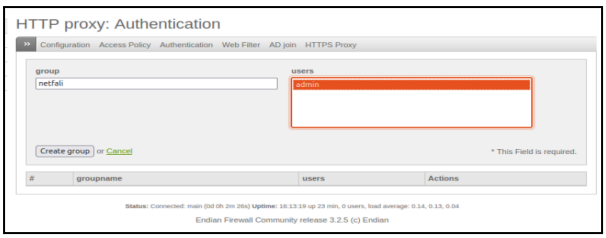

Figura 32. Creación de grupo.

Como se muestra en la Figura 33, dentro del módulo de configuración de Endian UTM se habilitó el servicio de proxy HTTP activando la opción "Enable HTTP Proxy", asignando el puerto 8080 y seleccionando el modo no transparente. Esta configuración obliga a que los dispositivos cliente configuren manualmente el proxy en sus navegadores para poder acceder a Internet.

El modo no transparente brinda mayor control sobre el tráfico saliente, ya que permite aplicar autenticación por usuario, filtros de contenido personalizados y políticas de navegación detalladas. Al no reenviar automáticamente las solicitudes HTTP, se asegura que solo los usuarios autorizados y correctamente configurados accedan a la red externa bajo las condiciones definidas por el administrador.

.

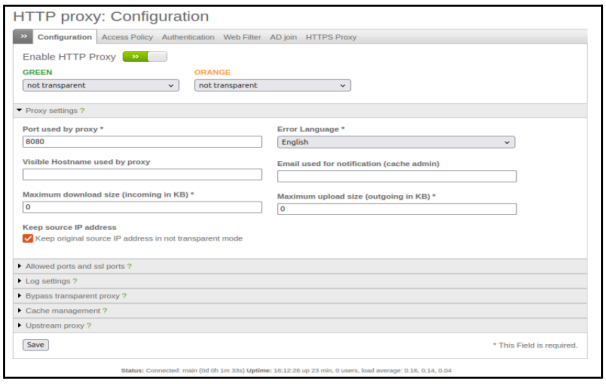

Figura 33. Habilitación de proxy y modo no transparente

Durante la configuración del control de acceso por contenidos, se procedió a crear un filtro personalizado que permitirá bloquear sitios no deseados dentro de la red. En la Figura 34 se evidencia la creación del filtro denominado "listanegra" en el módulo del proxy HTTP, en el cual se incluyeron los dominios www.hotmail.com, www.youtube.com y www.elnuevodia.com.co para restringir su acceso desde la zona GREEN.

Esta herramienta resulta clave para establecer barreras específicas frente a páginas que no se alinean con los objetivos de uso de la red. La implementación de listas negras permite aplicar políticas preventivas frente a contenidos distractores o potencialmente inseguros, fortaleciendo el control que ejerce el firewall sobre la navegación de los usuarios.

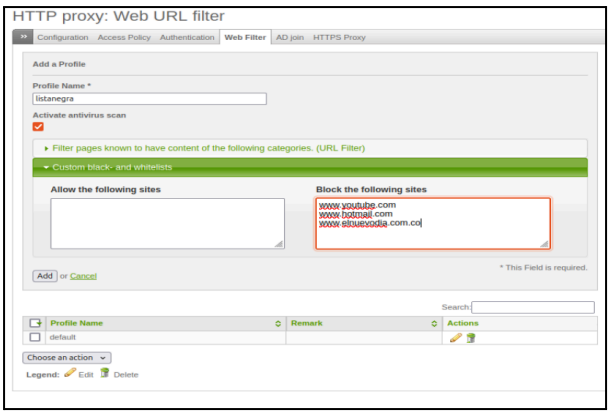

Figura 34. Creación de lista negra.

Luego de definir los filtros de contenido, fue necesario establecer una política de acceso que determinará a qué usuarios se aplicarían dichas restricciones. En la Figura 35 se observa la creación de una política en el proxy HTTP, en la cual se asocia el usuario "admin" al filtro previamente creado llamado "listanegra".

Esta política actúa como una regla de control que vincula usuarios o grupos con determinadas condiciones de navegación. A través de ella, Endian aplica automáticamente el filtrado configurado cada vez que el usuario autenticado intenta acceder a la web. Además, se completaron otros campos de configuración, como el tipo de acceso, el método de autenticación y el perfil de acción, garantizando una gestión precisa y personalizada del tráfico saliente desde la red LAN.

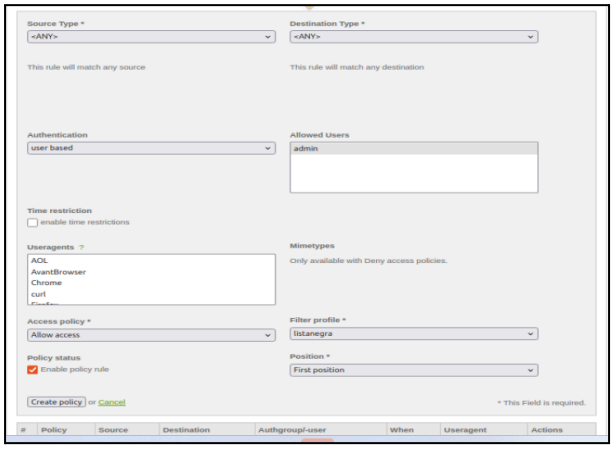

Figura 35. Aplicación de políticas de acceso.

Para que el proxy HTTP configurado en Endian funcione correctamente en los equipos cliente, es necesario ajustar manualmente la configuración del navegador. En la Figura 36 se aprecia la modificación de los parámetros de red en Firefox, donde se especifica el uso del proxy con la dirección IP 192.168.10.1 y el puerto previamente definido (8080).

Además, se habilitó la opción para utilizar el mismo proxy en conexiones HTTPS, lo que permite que todo el tráfico web tanto en protocolos HTTP como HTTP sea redirigido a través de Endian. Esta configuración asegura que las políticas de autenticación y filtrado aplicadas en el proxy se ejecuten de forma efectiva cada vez que el usuario accede a Internet desde el navegador.

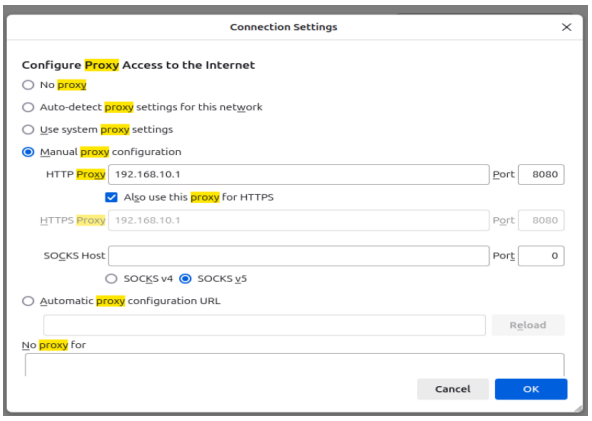

Figura 36. Configuración de proxy en firefox.

Como parte de la validación del funcionamiento del proxy HTTP con autenticación y filtrado de contenidos, se realizaron pruebas de acceso desde un navegador configurado. Al intentar ingresar al sitio www.hotmail.com, el sistema solicitó autenticación mediante usuario y contraseña, tal como se aprecia en la Figura 37. Esta solicitud confirma que el proxy está operando en modo no transparente con autenticación obligatoria, controlando el acceso en función del usuario registrado.

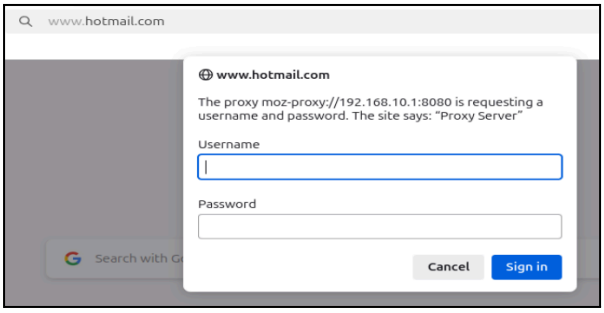

Figura 37. Autenticación de usuario y contraseña.

Una vez autenticados, se intentó acceder a los sitios previamente incluidos en la lista negra configurada en Endian. En las Figuras 38, 39 y 40 se evidencia el resultado del intento de conexión a www.hotmail.com, www.youtube.com y www.elnuevodia.com.co, respectivamente. En todos los casos, el sistema devuelve un mensaje de "acceso denegado", lo que indica que la política de filtrado se aplicó correctamente al usuario autenticado.

Estas pruebas demuestran que el proxy no sólo valida la identidad del usuario, sino que también ejecuta de manera efectiva las restricciones establecidas en las políticas de acceso, cumpliendo el objetivo de controlar y monitorear el tráfico saliente desde la red interna.

Se puede observar en las siguientes imágenes, (Figura 38 - 40) el funcionamiento del proxy, y como este nuestra los mensajes de acceso denegado en cada una de las URLs configuradas.

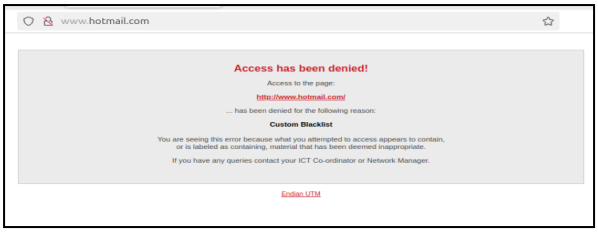

Figura 38. Acceso denegado de www.hotmail.com

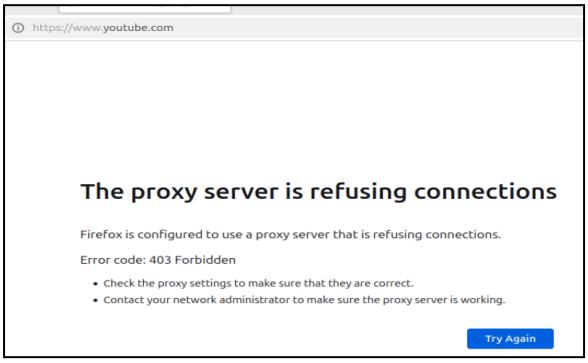

Figura 39. Acceso denegado a www.youtube.com

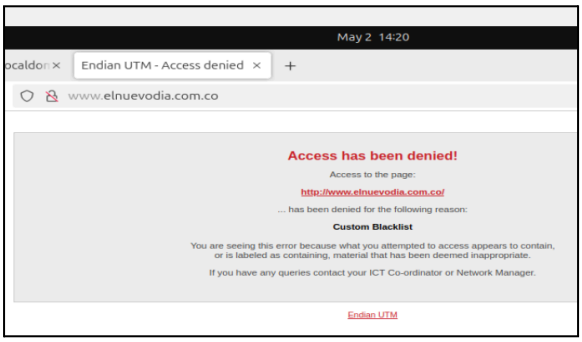

Figura 40. Acceso denegado a www.elnuevodia.com.co

4 CONCLUSIONES

La implementación de un sistema de seguridad perimetral basado en GNU/Linux Endian UTM ha demostrado ser una solución efectiva para la segmentación de redes en entornos virtuales. Este enfoque permite:

Una segmentación efectiva: La configuración de zonas de color (verde, roja y naranja) facilita la separación lógica de redes con diferentes niveles de confianza, mejorando significativamente lapostura de seguridad.

Mejor control de acceso: La implementación del proxy HTTP no transparente con autenticación de usuarios permite establecer políticas granulares de navegación, restringiendo el acceso a sitios web específicos y manteniendo un registro de la actividad de los usuarios.

Protección de servicios: La configuración de una zona desmilitarizada (DMZ) proporciona un nivel adicional de seguridad para los servidores que requieren exposición limitada a redes externas.

Flexibilidad y escalabilidad: La virtualización del firewall facilita la implementación, prueba y escalabilidad de la solución sin requerir hardware dedicado, lo que resulta especialmente útil en entornos de laboratorio y desarrollo.

Esta implementación sienta las bases para desarrollar configuraciones más complejas que pueden incluir sistemas de detección de intrusiones, VPN y otras funcionalidades avanzadas de seguridad, adaptándose a los requerimientos específicos de organizaciones de diferentes tamaños y complejidades.

5 REFERENCIAS

[1] Hubbard, B. (2022, julio 25). ¿Qué es la seguridad perimetral informática? Invgate.com. https://blog.invgate.com/es/seguridad-perimetral-informatica