IMPLEMENTACIÓN DE PRACTICAS DE SEGURIDAD UTILIZANDO ENDIAN FIREWALL

Sebastian Ayala Gonzalez
sayalag@unadvirtual.edu.co

RESUMEN— *Es un hecho que el vertiginoso desarrollo tecnológico de las últimas dos décadas ha revolucionado las capacidades a nuestra disposición. Pero de igual manera, este panorama de innovación también ha propiciado un incremento y una mayor sofisticación de las amenazas cibernéticas, las cuales persiguen la vulneración de sistemas para eludir las medidas de seguridad, resultando en el acceso no autorizado o la explotación de información y activos digitales críticos.*

PALABRAS CLAVE— Endian Firewall, Seguridad de Red, UTM (Unified Threat Management), Segmentación de red, NAT (Network Address Translation), Reglas de firewall, Proxy HTTP.

1 INTRODUCCIÓN

Hoy en día, la interconexión es una realidad global, y nuestra dependencia de los dispositivos electrónicos crece constantemente para realizar múltiples tareas en la vida personal y profesional, como son el estudio, el trabajo, la salud o las finanzas, entre varias más. Esta situación ha llevado a que personas sin escrúpulos busquen afectar, mediante ataques, a quienes dependemos de la tecnología. Se podría afirmar que una gran parte de la población, de manera directa o indirecta, utiliza la tecnología en algún aspecto fundamental de su vida.

En este escenario, la seguridad informática se vuelve tan vital como la seguridad física, un tema con el que los gobernantes a menudo se identifican, especialmente durante campañas o al ejecutar sus planes. No obstante, y a diferencia de la lucha contra la inseguridad física, la protección digital no siempre recibe la misma consideración hasta que ocurre un incidente que nos impacta de forma personal.

A pesar de esto, es positivo que la seguridad de la información interese a muchas personas, más de lo que a veces se percibe. Esto ha llevado a la formación de comunidades que, con el tiempo, diseñan, implementan y mantienen sistemas de seguridad pensados para el uso comunitario –es decir, hechos por y para la comunidad–. Esta forma de trabajo se conoce como desarrollo de soluciones de Código Abierto (Open Source).

Existen numerosos sistemas de seguridad, pero este artículo se enfocará en Endian Firewall. Se analizará su funcionalidad de firewall como componente clave, ya que representa una primera línea de defensa fundamental contra ataques y ha evolucionado para incluir capacidades avanzadas, como las de Gestión Unificada de Amenazas (UTM, por sus siglas en inglés: Unified Threat Management).

2 CONFIGURACIÓN INICIAL DEL FIREWALL Y DIVISION DE ZONAS DE RED

2.1 OBJETIVO DE LA FASE

Como configuración inicial lo que se realiza, es la instalación de Endian en un entorno controlado, en este caso se realiza la instalación en el software Virtual Box, este proceso busca instalar Endian y posterior a esto configurarlo para poder tener la red distribuida en diferentes zonas que favorezcan la funcionalidad de los sistemas inmersos tanto en el servidor como en la red LAN y su interacción con demás miembros de la red.

2.2 CONCEPTOS CLAVE: DISTRIBUCIÓN DE RED Y SEGURIDAD PERIMETRAL

La zonificación de red es fundamental en el proceso de gestión de redes y seguridad, porque es la forma en que controlamos el acceso a nuestra red, ya sea desde dentro o desde fuera de ella. Así podemos definir e identificar el nivel de confianza y la exposición que tendrá un segmento específico. De esta manera, logramos controlar ciertos ataques; por ejemplo, algunos podrían llegar a la Zona Naranja (DMZ) sin alcanzar la Zona Verde (LAN) y comprometer activos digitales. Esto no significa que la Zona Naranja se descuide; al contrario, también debemos controlar quién accede a ella y, desde esta misma zona, a qué otros servicios o redes se puede conectar. Un ejemplo es permitir que los dispositivos en la Zona Naranja salgan a Internet usando principalmente protocolos y puertos considerados seguros, como HTTPS (usualmente sobre el puerto 443), y que el acceso entrante a estos dispositivos también se limite a puertos específicos y bien controlados.

2.3 ENDIAN FIREWALL COMO HERRAMIENTA

Endian es una herramienta que permite realizar configuraciones de seguridad que limiten perimetralmente la manera en como nuestros sistemas y dispositivos internos se conectan entre sí e incluso fuera de la red a lo que conocemos como zona roja. Endian es una solución que agrupa features de seguridad como firewall, vpn, antivirus, proxy, filtrado web

entre muchas más funcionalidades. Está basado en Linux lo cual ofrece una gran comunidad interna que colabora a la estabilidad y la robustez del sistema otro aspecto importante es que tiene base open source la cual es muy útil para un buen número de escenarios y también una capa Enterprise que puede hacer más sentido para empresas grandes que pueden necesitar soporte prioritario.

2.4 ENTORNO DE VIRTUALIZACIÓN: VIRTUALBOX

Dentro del proceso de aprendizaje y con ánimo de que con los mínimos recursos se pueda desarrollar la temática abordada en este artículo, se usará y podrá usar usted también un virtualizador de su preferencia, en el hilo conductor de este artículo usaremos VirtualBox, el cual entre sus bondades nos ofrece la capacidad de ejecutar diferentes sistemas operativos en una sola computadora, reduciendo los costos que una práctica como la que desarrollaremos en este artículo. También podemos realizar pruebas de concepto en entornos de red aislados.

2.5 IMPLEMENTACIÓN PASO A PASO

El objetivo será tener segmentada la red en las diferentes zonas verde, naranja y roja, y de esta manera evidenciar la correcta instalación.

Como primer paso se deberá ingresar a la página oficial de Endian, *Endian Firewall Community* (Endian, s.f.) para realizar la descarga de la imagen iso que contiene el sistema operativo junto con las herramientas que integran a Endian como solución.

Una vez descargado Endian se procederá a realizar la instalación en VirtualBox, en donde el sistema con su interfaz visual intuitiva nos indicará con un botón que desde esta opción se puede crear una nueva máquina virtual. Procedemos a crear la máquina virtual y dentro de las variables requeridas al momento de crear una máquina virtual están las siguientes, nombre (identifica la máquina virtual que creas), carpeta (donde se almacenaran los recursos de tú máquina, archivos de configuración, etc), imagen iso. Solo con estas variables ya le decimos que cree la máquina virtual.

Una vez creada, y con creada no me refiero a funcional simplemente creada para inicializar lo que hacemos antes es ir a la configuración de esta máquina virtual en la sección de redes y configurar 3 adaptadores de red, uno llamado WAN que será un adaptador de tipo puente, otro adaptador de tipo LAN (nuestra zona verde) que será de tipo "Red interna" y el último que será el adaptador DMZ (Zona naranja) el cual será de tipo "Red interna". Debemos asegurarnos de que estén correctamente configurados y con la opción "Cable conectado" seleccionada para que tenga acceso a estos tres segmentos de red.

Ahora si es momento de encender la maquina virtual, en donde inicialmente lo que veremos serán unas pantallas de configuración que nos proporciona un asistente de configuración con preguntas de respuesta cerrada, así como idioma con sus opciones limitadas, entre las cuales se encuentran Ingles, italiano y alemán. Así como estas preguntas luego aparecerán mas preguntas dentro de las cuales están las siguientes, "Quiere reiniciar el equipo para propósito de instalación de EFW" (Así se refiere a Endian, *Endian Firewall Community* (Endian, s.f.)), también hay preguntas que nos preguntan si estamos seguros de realizar la instalación de EFW. Luego nos pide algo muy importante y es la dirección IP y la mascara de red para definir cual será la red verde y la IP en la cual funcionara Endian como se muestra en la Fig. 1. Interfaz de configuración de dirección IP y máscara de red para segmentación.

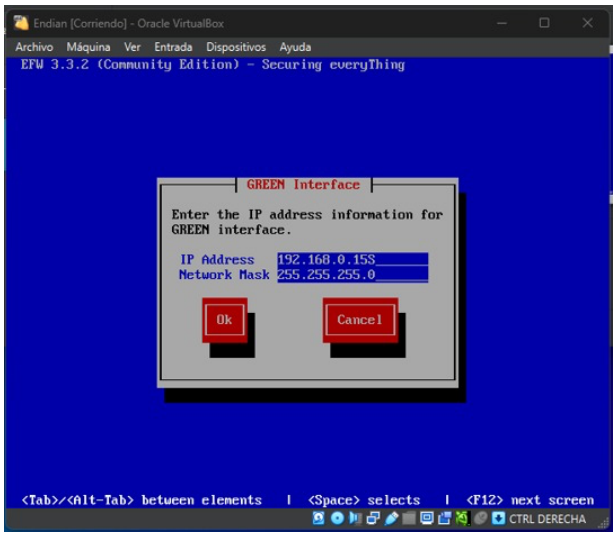

Fig. 1. Interfaz de configuración de dirección IP y máscara de red para segmentación.

Luego de esto empieza el proceso de instalación en segundo plano, instalando todo lo necesario para tener operativo el sistema. Una vez se termina la instalación podemos ver la consola de la maquina con la dirección IP asignada a Endian y el rango IP especificado para la zona verde (LAN). Fig. 2. Consola de Endian luego de instalación.

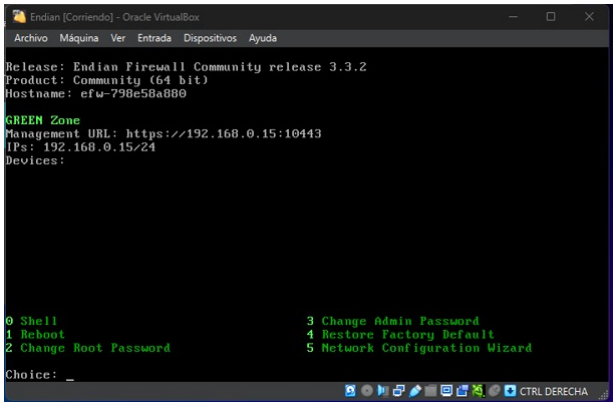

Fig. 2. Consola de Endian luego de instalación.

A continuación, como se muestra en la Fig. 2, se observa la consola de Endian después de la instalación. Desde aquí, se dispone de opciones para configurar el sistema. Lo que se hace es presionar la opción número 5, la cual permite realizar la segmentación de la red, siendo este el producto esperado de la fase que resta por configurar.

Una vez presionada la tecla 5, la consola despliega una interfaz con un formulario. En él se solicitan aspectos como: nombre de host (hostname), dominio, DNS primario, DNS secundario, y los rangos de direcciones IP para los segmentos de red Verde, Naranja y Azul. También se pregunta si se desea habilitar el acceso SSH y el servidor DHCP. Esto se puede observar en la Fig. 3.

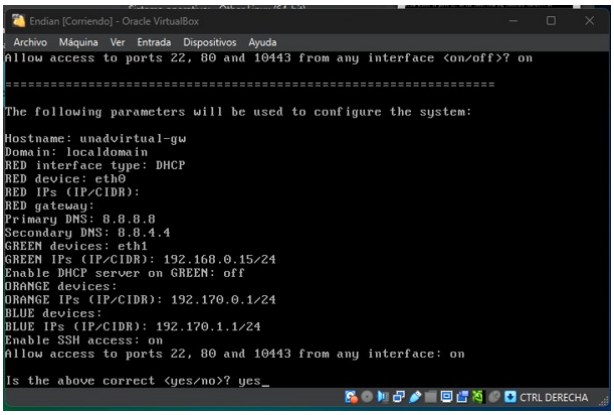

Fig. 3. Formulario de configuración inicial Endian.

3 CONFIGURACIÓN NAT (NETWORK ADDRESS TRANSLATION)

3.1 OBJETIVO DE LA FASE

Se espera con esta fase, poder establecer comunicación entre las diferentes zonas, mas específicamente se espera como resultado de esta sección 3, poder comunicar la red LAN hacia la WAN mejor conocida como zona roja o Internet, asi como también se espera poder conectarnos a internet desde la DMZ.

3.2 CONCEPTOS CLAVE: TRADUCCIÓN DE DIRECCIONES DE RED (NAT)

La traducción de direcciones de red es la manera como las redes pueden mapear direcciones IP de un segmento en otro, pudiendo así comunicar dispositivos conectados a diferentes esquemas de direccionamiento. Lo que hace NAT por debajo es modificar los encabezados de los paquetes que transitan en la red para ajustar la IP origen o destino de acuerdo con las reglas configuradas.

3.3 CONFIGURACIÓN DE NAT PARA LA ZONA VERDE (LAN) HACIA WAN

Endian además de una consola nos proporciona una interfaz visual con la cual podemos realizar labores de administración de manera intutiva, este panel de administración lo podemos ver en la Fig. 4. Interfaz visual de Endian.

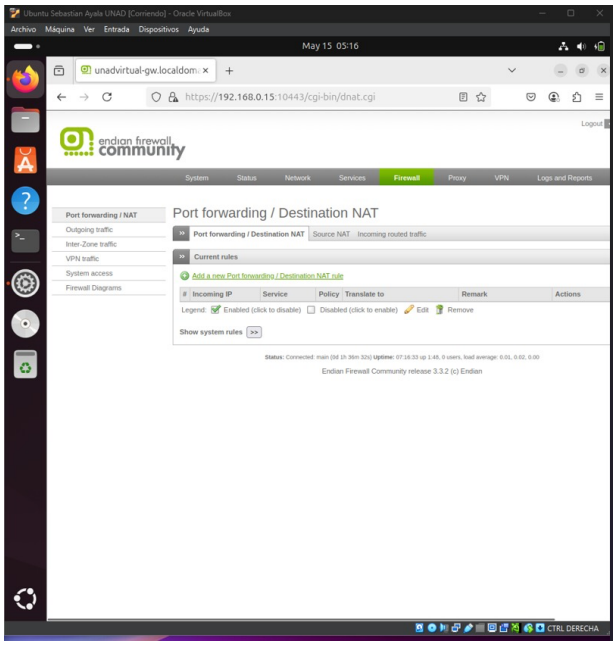

Fig. 4. Interfaz visual de Endian.

Luego de estar en la interfaz, nos dirigimos por medio de los menus a la sección llamada “Proxy” y dentro de la misma vamos a la sección llamada “Outgoing firewall configuration”. Allí encontraremos la sección de configuración donde crearemos las reglas que nos permitan acceder a internet desde la red LAN y tambien desde la red DMZ.

Crearemos una regla con dando en la opción “Add a new firewall rule” y nos pedirá información de la fuente y el destino, campos en los cuales vamos a seleccionar como destino la zona roja y como fuente en dos reglas diferentes seleccionaremos la red verde y la naranja respectivamente. En cuanto a puertos no realizaremos ninguna validación, permitiremos el trafica a internet por medio de cualquier puerto como se ve en la Fig. 5. Reglas firewall creadas.

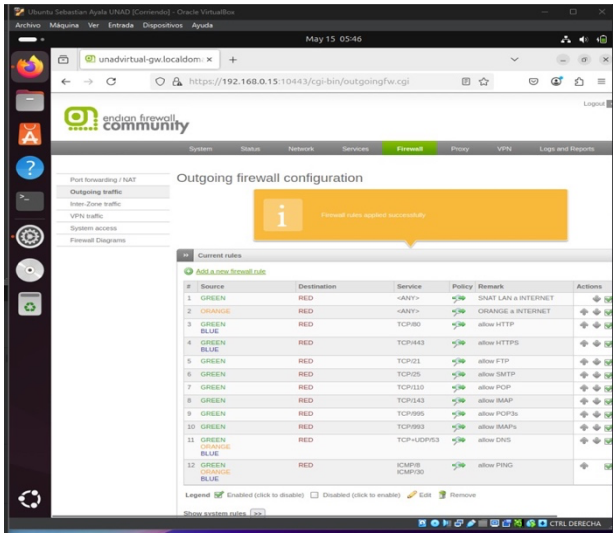

Fig. 5. Reglas firewall creadas.

Una vez las reglas están creadas probar el funcionamiento de estas es tan sencillo como realizar una búsqueda en el navegador de preferencia dentro de un dispositivo que este en el segmento de red verde, y como por lo general en la zona naranja están los servidores, lo que podemos hacer en este caso es realizar una sencilla actualización de paquetes, que para ejemplificación se usaría el comando “sudo apt update” en una maquina Ubuntu Server. Si lo anterior funciona correctamente, ya damos por bien configuradas las reglas firewall de salida.

4 ACCESIBILIDAD A LA ZONA DMZ DESDE LA RED

4.1 OBJETIVO DE LA FASE

Dentro de la jerga militar existe algo llamado zona DMZ o mas conocida como zona desmilitarizada, la cual esta compuesta por espacio compartido entre ambos bandos de una guerra, esto con el fin de no tener quizás un conflicto directo y tener algo de separación. En las redes no es muy diferente, básicamente es una zona la cual es usada por empresas que requieren proveer servicios a externos que los usan a través de internet (Zona roja), la idea principal de esto es que si los enemigos (Ciber delincuentes) realizan un ataque exitoso, no puedan comprometer las zonas seguras de nuestra red (Zona verde). El objetivo de nuestra fase es darle acceso a los dispositivos ubicados en internet para que accedan a nuestra DMZ con los puertos y reglas que nosotros por seguridad definamos.

4.2 CONCEPTOS CLAVE: POLITICAS DE FIREWALL

Una política es una norma que regula el comportamiento en un contexto determinado. Pensemos, por ejemplo, en las reglas que ponen unos padres para la hora de llegada a casa de su hijo. Si vive con ellos, es habitual que establezcan un horario: en días hábiles, no podrá entrar después de las 10:00 p.m.; en cambio, durante fines de semana o festivos, el acceso estará permitido hasta las 2:00 a.m., siempre que no se supere ese límite. De modo similar funcionan las políticas de firewall: definimos reglas explícitas para permitir o denegar el acceso a nuestros recursos digitales.

4.3 CONFIGURACIÓN DE NAT PARA LA ZONA VERDE (LAN) HACIA WAN

Para poder definir las reglas claras con las cuales agentes externos van a acceder nuestros servicios dentro de la DMZ debemos en la interfaz visual de Endian ir al menú “Firewall” en el cual encontraremos una sección llamada “Port forwarding” en donde podremos crear las reglas de acceso desde internet a nuestra DMZ. Como primer paso lo que hacemos es dar clic en “Add a new Port forwarding / Destination NAT rule” aquí se nos pide proveer la zona fuente de la cual vamos a recibir el tráfico, como el objetivo es que el tráfico llegue desde internet vamos a seleccionar la zona roja, luego le indicamos que queremos exponer el puerto 80 el cual es de uso común para servicios HTTP mediante el protocolo TCP. También debemos proporcionarle la IP a la cual será redireccionado el tráfico una vez llegue. Aquí le especificamos la dirección IP del dispositivo dentro de la DMZ desde el cual vamos a resolver las peticiones. También lo que haremos será crear la regla para permitir que entren peticiones desde el puerto 21 comúnmente usado para el protocolo FTP.

Luego de esto lo que haremos será crear una regla, pero en lugar de permitir, lo que haremos será denegar, ¿denegar que? Denegar la entrada de tráfico a los puertos 8 y 30 que son comúnmente usados cuando un servidor quiere saber si puede establecer comunicación con una IP especifica, esto puede ser usado como un hook (gancho) para pescar IP’s que están expuestas y posterior a esto realizar ataques que puedan comprometer activos digitales sensibles. La configuración anterior la podemos ver en la Fig. 6. Reglas de redirección.

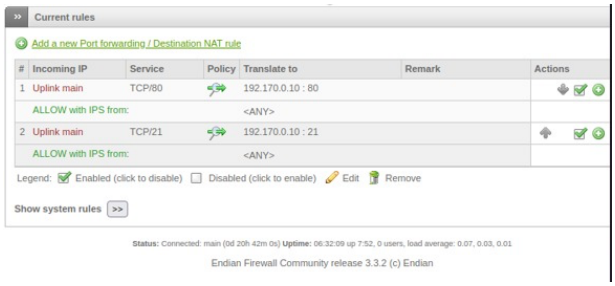

Fig. 6. Reglas de redirección.

El proceso para realizar las pruebas de funcionamiento se lleva a cabo desde una maquina que no este dentro de la red, y con la red nos referimos a que no este dentro de la DMZ y opcionalmente podemos probar incluso desde la zona roja. La prueba se realiza accediendo a la IP publica asignada a Endian para que esta a su vez redireccione las peticiones, también se puede realizar desde la IP privada pero solo funcionara dentro de la red. La anterior configuración deniega de manera correcta las conexiones que se quieren establecer usando el protocolo ICMP como se observa en la Fig. 7. Resultado de peticiones mediante el protocolo ICMP.

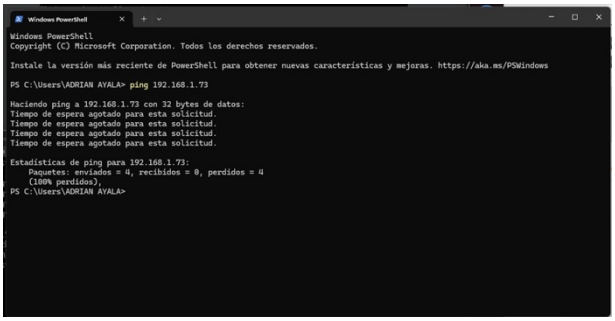

Fig. 7. Resultado de peticiones mediante el protocolo ICMP.

Para probar que el puerto 21 y el puerto 80 esten permitiendo que las conexiones alcancen su destino final (Servidor en la red DMZ) se hace un proceso similiar, con la característica de que la prueba HTTP se puede hacer desde un navegador web y la prueba de FTP la realizaremos con un

comando de consola llamado muy intuitivamente “ftp” donde podemos establecer una conexión con un servidor e interactuar usando comandos con el fin de realizar transferencias de archivos locales hacia el servidor remoto. En este caso solo estableceremos la conexión como lo muestran Fig. 8. Resultado de conexión FTP. Y Fig. 9. Resultado de conexión vía HTTP.

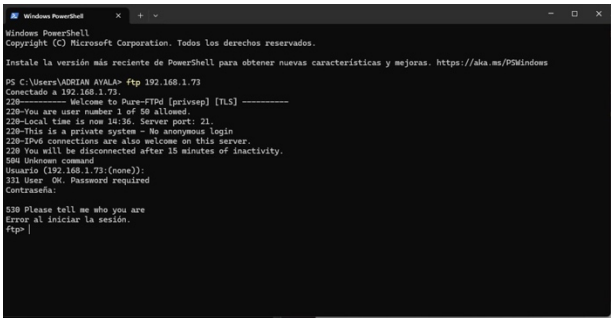

Fig. 8. Resultado de conexión FTP.

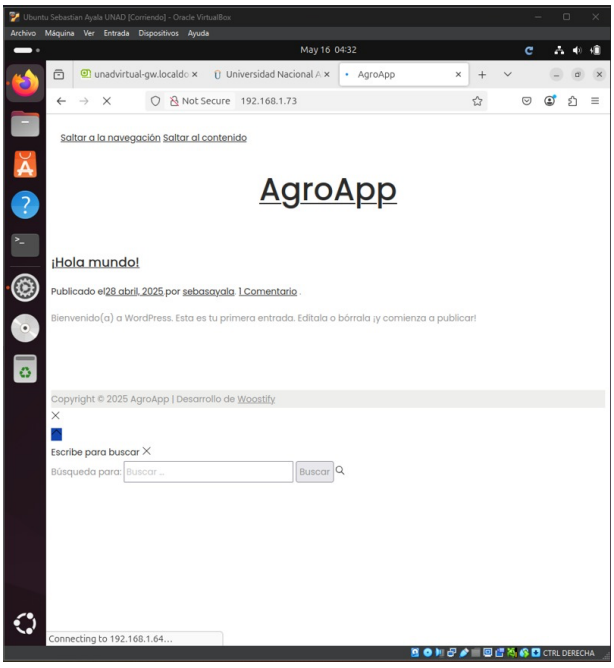

Fig. 9. Resultado de conexión vía HTTP.

5 ACCESIBILIDAD ENTRE LAS ZONAS DE LA RED

5.1 OBJETIVO DE LA FASE

La necesidad de que los dispositivos electrónicos estén interconectados es algo que ha hecho que los primeros esfuerzos de la ingeniería estuvieran en ello. Con el fin de poder crear dispositivos que hicieran tareas especificas y que conectados con otros dispositivos formaran una red que permitiera dividir tareas complejas y que fueran abordadas por diferentes dispositivos o zonas de red. En esta fase lo que haremos será complementar el trabajo que hasta ahora llevamos, en el cual hemos creado y definido reglas de acceso a nuestros dispositivos de una zona DMZ para que cualquier dispositivo en internet pueda acceder al recurso siempre y cuando cumpla con las reglas establecidas. Complementaremos el trabajo permitiendo que también las zonas de nuestra red se puedan conectar entre sí, pudiendo tener trafico entre ellas sin la necesidad de salir a internet, lo cual es una muy buena practica de seguridad y de rendimiento ya que no se requiere el mismo ancho de banda para ir a consumir un servicio a través de internet que consumirlo directamente aprovechando que esta en nuestra red.

5.2 CONCEPTOS CLAVE: POLITICAS DE FIREWALL INTER-ZONA

En una arquitectura de red segmentada como la que estamos abordando en este articulo el firewall no solo se limita a actuar como barrera contra amenazas externas, sino que también funciona como un actor que semaforiza la manera en como se distribuye el trafico interno. Endian sigue el principio de mínimo privilegio, razón por la cual la comunicación directa entre las diferentes zonas por lo general esta restringida, es decir así las diferentes zonas estén conectadas al mismo firewall no pueden intercambiar datos entre sí.

5.3 CONFIGURACIÓN DE REGLAS DE ACCESO

Nuestra arquitectura de red esta compuesta por 3 zonas definidas, la zona verde, naranja y roja. Lo que realizaremos será configurar una serie de reglas que permitirán la interconexión de estas zonas con limites claros establecidos.

Dentro de Endian lo que haremos será ir a la sección llamada “Firewall” en donde encontraremos una entrada llamada “Inter-Zone traffic”, allí habilitaremos la configuración customizada de comunicación inter-zona. La idea es crear dos reglas sencillas que nos permitan comunicarnos desde la zona verde a la zona naranja para poder establecer comunicación usando el protocolo HTTP y el protocolo FTP cada uno usando su puerto habitual el 80 y 21 respectivamente. Este proceso se puede ver como queda configurado en la Fig. 10. Reglas de conexión inter-zona.

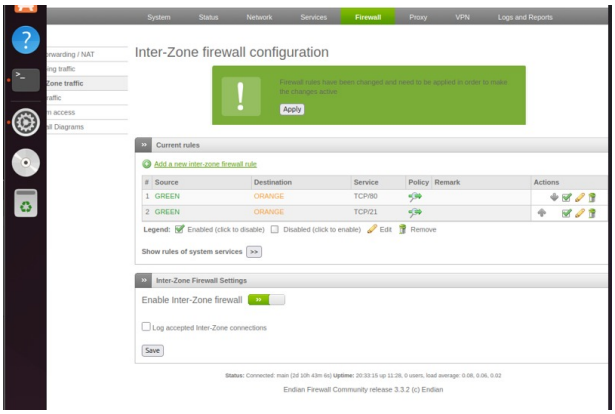

Fig. 10. Reglas de conexión inter-zona.

Debido a que queremos que comunicar la zona roja con la zona DMZ lo que vamos a hacer es crear reglas dentro del apartado Firewall > Port forwarding / NAT > Incoming routed traffic. Para la creación de las reglas lo que necesitamos es saber cual es el origen de la petición, cual es el destino, el servicio que se va a afectar en la regla y si la política permite lo anteriormente descrito o lo deniega. Y luego de realizar esta configuración las reglas quedan como lo muestra la Fig. 11. Reglas de trafico entrante.

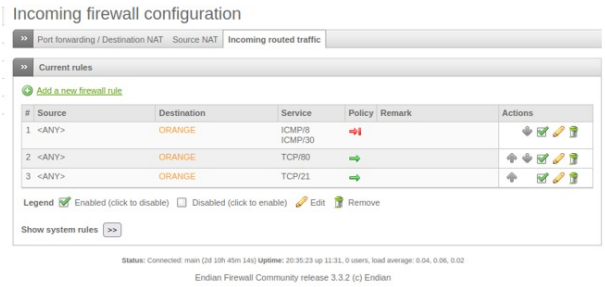

Fig. 11. Reglas de trafico entrante.

Una vez configurado esto, debemos realizar la validación de que las reglas están funcionando de manera correcta, esto se puede hacer para el caso de conexión de zona verde con zona naranja realizando una petición HTTP desde un dispositivo conectado a la zona verde apuntando a la dirección IP privada que tiene nuestro servidor que reposa en la zona naranja (DMZ), ¿Por qué la IP privada? Básicamente porque nosotros estamos estableciendo que la comunicación debe estar a el mismo nivel entre ambas zonas, es decir que tanto la zona verde como la zona naranja al interactuar actúen como si estuvieran dentro del una misma "zona". Ver Fig. 12. Petición HTTP a servidor en zona DMZ.

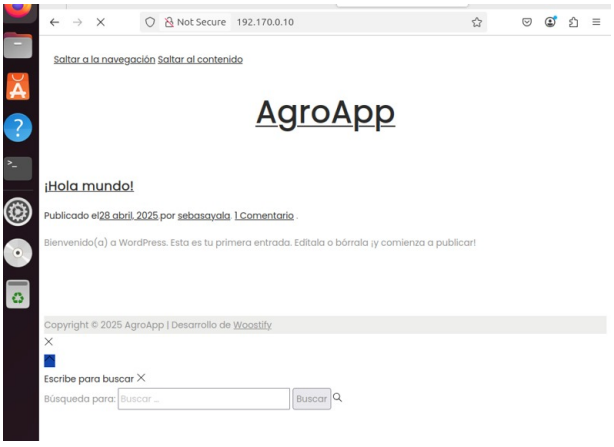

Fig. 12. Petición HTTP a servidor en zona DMZ.

No es muy diferente la prueba para comprobar acceso desde la zona roja a la zona naranja, aquí al contrario que con la prueba de conexión inter-zona no se necesita saber la dirección IP privada ya que la comunicación se debería realizar a través de la IP publica de Endian y debería estar en la capacidad de enrutar el trafico y de poder identificar si es una petición aceptable de acuerdo con las reglas configuradas en esta etapa y en etapas anteriores que complementan esta. La petición entonces se hará usando la IP publica de Endian. Revisar Fig. 13. Petición HTTP a servidor en DMZ a través de Endian Firewall desde zona roja.

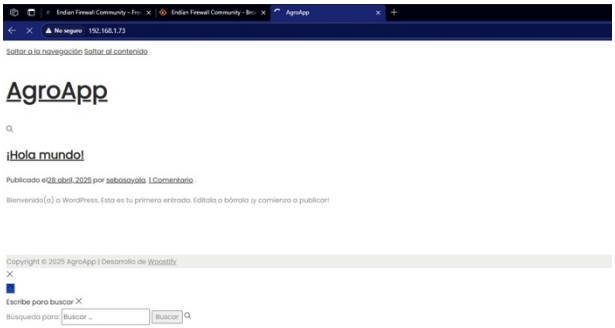

Fig. 13. Petición HTTP a servidor en DMZ a través de Endian Firewall desde zona roja.

Para el caso de el puerto 21 que comúnmente es usado por el protocolo FTP la prueba no varia mucho, simplemente se usa "ftp" para mediante consola establecer conexión. Revisar Fig. 14. Establecimiento de conexión FTP desde zona roja a zona naranja.

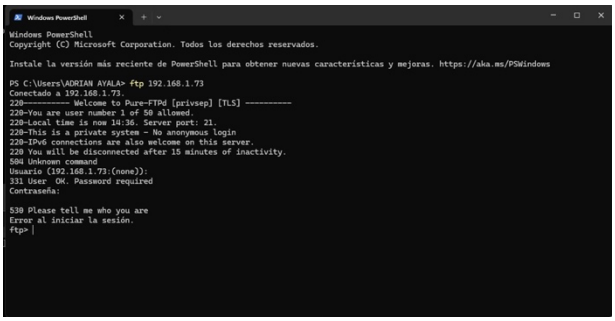

Fig. 14. Establecimiento de conexión FTP desde zona roja a zona naranja.

6 IMPLEMENTACIÓN DE PROXY HTTP: NAVEGACIÓN SEGURA EN INTERNET

6.1 OBJETIVO DE LA FASE

Desde el punto de vista técnico, la navegación en internet puede considerarse una actividad que en su mayoría de veces se realiza de manera adecuada y segura. Sin embargo, como hemos abordado desde el inicio de este articulo, existen personas que siempre están a la espera de poder realizar maniobras que puedan comprometer información personal o de empresas para beneficio propio. Es por esto por lo que muchas escuelas, empresas y entidades de diversos tipos optan por la utilización de un sistema de seguridad con proxy incluido para una navegación segura y de esta manera proteger los activos digitales y mejor aun en el caso de un colegio poder proteger a lo menores de acceder a sitios que podrían ser poco seguros para ellos y que podrían vulnerar sus derechos como lo son las redes sociales. Veremos como podemos implementar un proxy de

navegación y como restringir paginas, que para efectos de practicas serán paginas seguras, pero que en un entorno real esta acción podría hacer la diferencia al momento de recibir ataques.

6.2 CONCEPTOS CLAVE: LISTA NEGRA

Imaginemos que vivimos en un conjunto residencial en donde la portería que es donde suelen estar los vigilantes es el proxy de navegación, su misión es evitar que a tu casa lleguen personas no deseadas o que simplemente no quieres que entren en un momento especifico a tu casa. Una lista negra no es mas que una serie de instrucciones que le das a los vigilantes (Proxy) para que sepa a que personas debe dejar entrar y a que personas no. En este caso lo que se especifica en las listas negras son sitios web, dominios y hasta rangos de direcciones IP que no queremos que sean parte de nuestra navegación.

6.3 MANOS A LA OBRA: IMPLEMENTACIÓN DE PROXY PARA NAVEGACIÓN WEB

Con la finalidad de restringir el acceso a sitios que puedan ser inseguros o que potencialmente vayan en contra de políticas de negocio de una empresa lo que vamos a hacer es implementar en la red un proxy que ayude a que toda petición realizada por un dispositivo dentro de la red verde pase primero por la evaluación de las reglas definidas para una navegación segura.

Para realizar la creación de estas reglas primero debemos entrar a la sección llamada “Proxy” en donde a su vez tenemos que ingresar a la sección “HTTP” ya que lo queremos hacer es configurar es un proxy para navegación web. Allí encontraremos un togggle que nos permitirá habilitar el uso del “HTTP proxy”. Una vez pulsado ese toggle, lo que haremos será seleccionar que para la zona verde el proxy será no transparente. Adicional proporcionaremos el puerto el cual será usado por el proxy. Véase la Fig. 15. Configuración inicial del proxy HTTP.

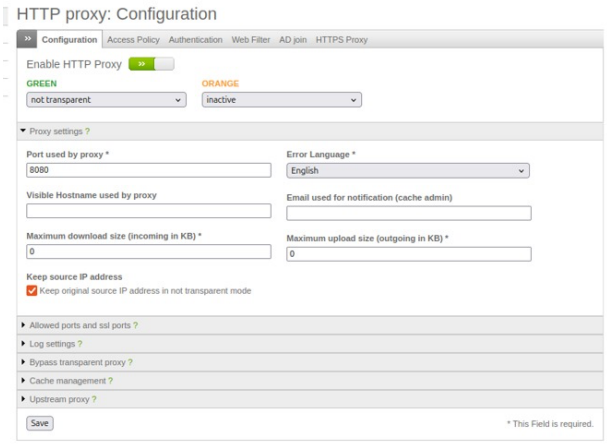

Fig. 15. Configuración inicial del proxy HTTP.

Posterior a esto se procede con la creación de un grupo de usuarios que servirá para agrupar los usuarios y que estas agrupaciones puedan tener configuraciones en común, facilitando de esta manera el mantenimiento de las reglas, en diferentes niveles de acceso si es requerido. Para la creación del grupo de usuarios y los usuarios solo es requerido el nombre para el grupo y para los usuarios bastara solo con asignar un nombre de usuario y una contraseña. Revisar Fig. 16. Creación de usuario. Revisar Fig. 17. Creación de grupo de usuarios.

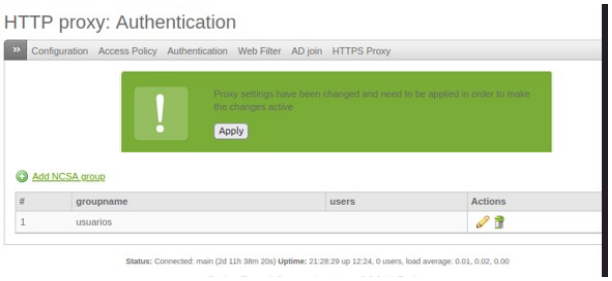

Fig. 16. Creación de usuario.

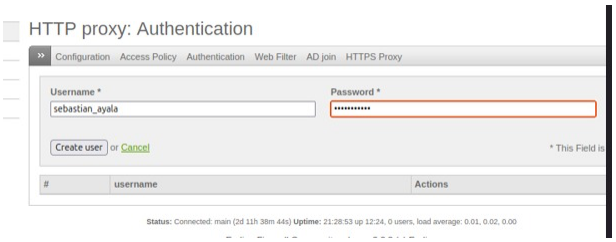

Fig. 17. Creación de grupo de usuarios.

Una vez que tenemos el grupo y el/los usuarios creados, procedemos a crear una lista negra que definirá los sitios a los cuales no podremos acceder por seguridad. Entramos en la sección Proxy > HTTP > Web Filter y allí encontraremos una función que nos permitirá crear la lista negra. En la lista negra podemos especificar un nombre para la misma así como activar proceccion de virus con la opción “Activate antivirus scan”, y luego si podremos especificar los sitios a los cuales no se podrá acceder; esta parte se puede hacer de dos maneras, una es agregando los sitios (Dominio, rangos IP, etc) o seleccionando categorías administradas por Endian que cuando por ejemplo detecten que se esta accediendo a un sitio categorizado como sitio de drogas entonces sea bloqueado de manera inmediata. En nuestro caso lo que haremos será simplemente colocar los dominios de los sitios que queremos bloquear. Véase la Fig. 18. Creación de la lista negra.

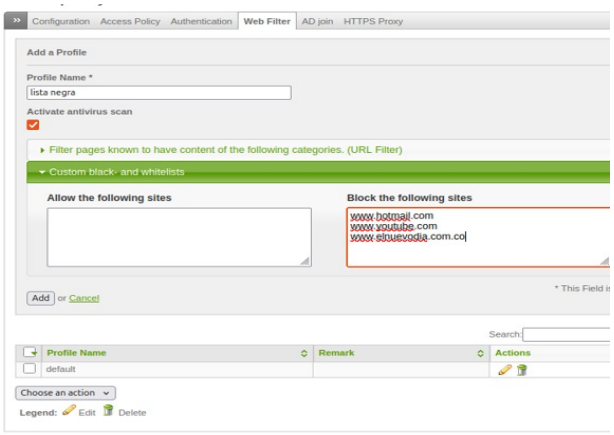

Fig. 18. Creación de la lista negra.

Ahora si procederemos a crear una política de acceso para dejar completamente funcional el proxy de navegación. Esto lo hacemos entrando a Proxy > HTTP > Access Policy. Una vez en esta ruta lo que hacemos es crear una política, en donde debemos proporcionar información como la fuente del trafico, el destino, en base a que entidad se realizara la autenticación, en nuestro caso lo haremos con. Autenticación basada en grupo, entonces se nos pide cual es el grupo y por último proporcionar la lista negra para que la política evalué las configuraciones y permita o deniegue el acceso de acuerdo con la lista negra. Véase la Fig.19. Creación política de acceso proxy.

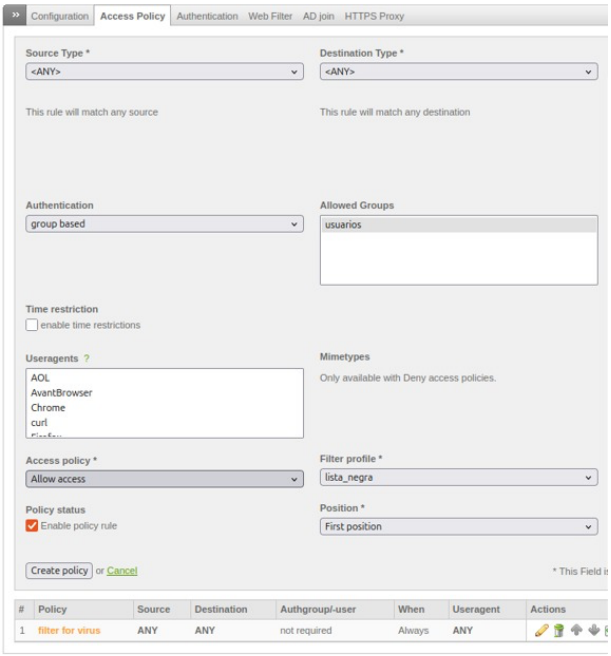

Fig. 19. Creación política de acceso proxy.

La prueba de esta configuración consta de realizar peticiones web a los dominios que explícitamente le indicamos a endian que bloqueara. Vease Fig. 20. Inicio de sesión usuario. Fig. 21. Intento de conexión a YouTube. Fig. 22. Intento de conexión a Hotmail.

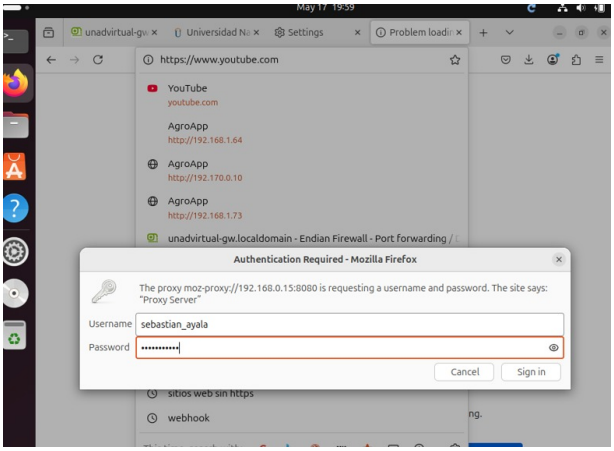

Fig. 20. Inicio de sesión usuario.

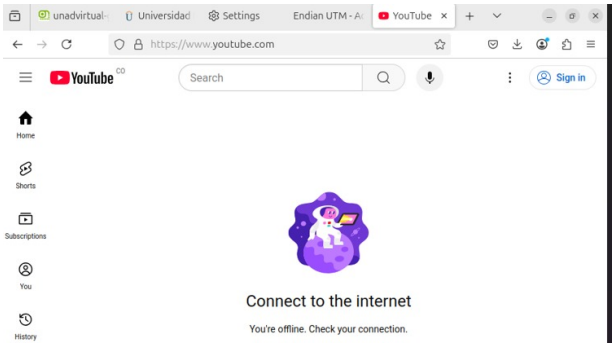

Fig. 21. Intento de conexión a YouTube.

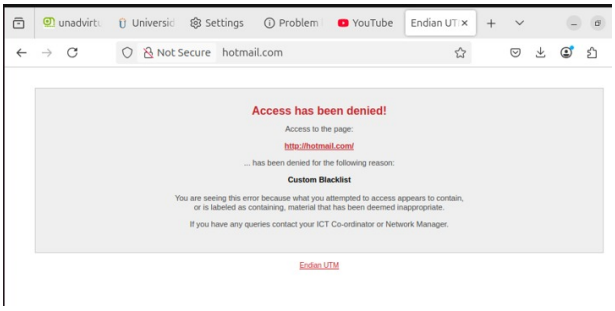

Fig. 22. Intento de conexión a Hotmail.

Con esto concluye las pruebas del proxy que ahora, servirá para que personas dentro de nuestra red, hagan un uso responsable de internet.

7 CONCLUSIONES

Llegar a este punto ha sido todo un reto para mi, sin embargo y pese al reto que significo fue un proceso lleno de aprendizaje. Mas que simples configuraciones técnicas de redes y seguridad he podido interiorizar temáticas que de otra manera no lo hubiese podido hacer.

Los objetivos planteados en las fases que abordamos se cumplieron, dando sentido ahora que se ve el resultado final a cada paso pequeño y que por mas insignificante que pareciera labraba el camino para una etapa posterior que daría sentido a todo el trabajo aquí hecho.

8 REFERENCIAS

[1] Endian Network. (s.f.). Endian UTM Documentation. Endian Community. Recuperado el 21 de mayo de 2025, de https://www.endian.com/community/
[2] Tanenbaum, A. S., & Wetherall, D. J. (2011). Redes de computadoras (5ª ed.). Pearson Educación.
[3] Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson.
[4] Oracle Corporation. (s.f.). Oracle VM VirtualBox User Manual. Oracle Corporation. Recuperado el 21 de mayo de 2025, de https://www.virtualbox.org/manual/UserManual.html