IMPLEMENTACIÓN Y ASEGURAMIENTO DE RED CON ENDIAN FIREWALL EN ENTORNO VIRTUALIZADO

Miguel David Saavedra Hamburger
e-mail: mdsaavedrah@unadvirtual.edu.co

RESUMEN: *Se implementó y configuró Endian Firewall Community en un entorno virtualizado con VirtualBox para asegurar una infraestructura de red segmentada en zonas LAN (Verde), DMZ (Naranja) y WAN (Roja, modo puente). Se establecieron reglas de firewall para controlar el tráfico saliente, inter-zona y de acceso al sistema, incluyendo el bloqueo de ICMP tipo 8. Se configuró NAT (SNAT para salida y DNAT/Port Forwarding para acceso WAN-DMZ a servicios HTTP/FTP). Adicionalmente, se implementó un Proxy HTTP no transparente en la zona LAN, con autenticación local basada en usuarios/grupos y filtrado de contenido mediante listas negras. Las pruebas funcionales validaron la correcta segmentación, el control de acceso, la redirección de puertos y el funcionamiento del proxy, demostrando la aplicación efectiva de conceptos de seguridad de red con herramientas open source.*

PALABRAS CLAVE: DMZ, Endian Firewall, Proxy HTTP, Seguridad de Red.

1 INTRODUCCIÓN

La seguridad de las redes informáticas es un pilar fundamental en la infraestructura tecnológica actual. La protección de los activos de información y la garantía de la continuidad operativa requieren la implementación de mecanismos robustos para controlar el acceso y mitigar amenazas. En este contexto, las soluciones de Gestión Unificada de Amenazas (UTM) basadas en software libre, como Endian Firewall Community (EFW), ofrecen una alternativa flexible y potente.

Este artículo presenta la implementación y configuración de EFW en un entorno virtualizado mediante Oracle VM VirtualBox. Se simuló una topología de red segmentada en tres zonas: una red local interna (LAN - GREEN), una zona desmilitarizada (DMZ - ORANGE) para servidores expuestos, y la conexión a la red externa (WAN - RED). El objetivo principal fue aplicar y validar diversas configuraciones de seguridad esenciales para proteger dicha infraestructura.

A lo largo del documento se describe el proceso de instalación y configuración base del firewall, el establecimiento de reglas de NAT (SNAT y DNAT), la implementación de políticas de firewall para controlar el tráfico saliente, inter-zona y de acceso al sistema (incluyendo el bloqueo ICMP), y la configuración de un proxy HTTP no transparente con autenticación y filtrado de contenido, cubriendo así las cinco temáticas clave del ejercicio propuesto.

2 METODOLOGÍA Y CONFIGURACIÓN DEL ENTORNO

El presente trabajo se desarrolló utilizando un enfoque práctico basado en la simulación de un entorno de red empresarial. Se empleó software de virtualización y sistemas operativos de código abierto para implementar y validar las configuraciones de seguridad propuestas.

El software principal utilizado incluyó Oracle VM VirtualBox (versión 7.1.8) como hipervisor, ejecutándose sobre un sistema anfitrión Windows 11. Como elemento central de seguridad, se instaló Endian Firewall Community (EFW) versión 3.3.2. Para simular los servidores y clientes internos, se utilizaron las distribuciones Ubuntu Server 24.04 LTS y Ubuntu Desktop 24.04 LTS, respectivamente.

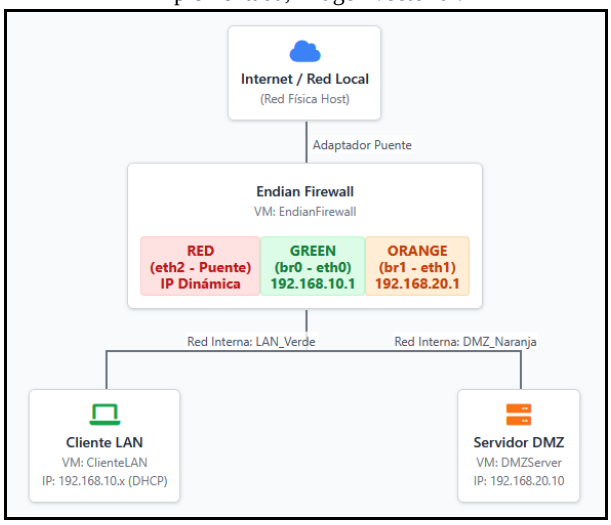
La topología de red virtual implementada en VirtualBox consistió en tres máquinas virtuales (VMs) principales: EndianFirewall, DMZServer (Ubuntu Server) y ClienteLAN (Ubuntu Desktop). Estas VMs se interconectaron a través del firewall EFW, el cual definió tres zonas de seguridad distintas:

- **Zona GREEN (LAN):** Representa la red local interna segura. Se configuró en el segmento de red 192.168.10.0/24, con la IP 192.168.10.1 asignada a la interfaz correspondiente del firewall (puente br0 sobre eth0). Se habilitó un servidor DHCP en esta zona. La VM ClienteLAN se conectó a esta zona.
- **Zona ORANGE (DMZ):** Representa la zona desmilitarizada para servidores con exposición controlada. Se configuró en el segmento 192.168.20.0/24, con la IP 192.168.20.1 asignada a la interfaz del firewall (puente br1 sobre eth1). La VM DMZServer se conectó a esta zona.

- **Zona RED (WAN):** Representa la conexión a la red externa (Internet). La interfaz correspondiente del firewall (eth2) se configuró en modo Adaptador Puente en VirtualBox, obteniendo una dirección IP dinámica de la red física local del anfitrión (ej. 192.168.1.8/24).

La comunicación entre las zonas GREEN y ORANGE se gestionó mediante Redes Internas de VirtualBox (LAN_Verde y DMZ_Naranja) conectadas a los adaptadores correspondientes del firewall y las VMs internas, asegurando el aislamiento inicial entre segmentos. Dicha topología se ilustra esquemáticamente en la Figura 1.

Figura 1. Diagrama simplificado de la topología de red implementada, imagen vectorial.



Fuente: Elaboración propia

Esta configuración de entorno proporcionó la base para la implementación y prueba de las diversas políticas de seguridad detalladas en las siguientes secciones.

3 IMPLEMENTACIÓN DE SEGURIDAD POR TEMÁTICAS

A continuación, se describen las configuraciones clave realizadas en el firewall Endian Community (EFW) y las máquinas virtuales de soporte, siguiendo las temáticas propuestas en la guía de aprendizaje.

4 INSTALACIÓN Y CONFIGURACIÓN BASE DE ENDIAN FIREWALL (TEMÁTICA 1)

El primer paso consistió en la instalación del sistema operativo EFW v3.3.2 en la máquina virtual EndianFirewall previamente creada en VirtualBox. Se siguió el asistente de instalación basado en texto, seleccionando el idioma inglés y aceptando las configuraciones por defecto para el particionamiento del disco virtual. Durante este proceso inicial, se configuró la dirección IP estática para la interfaz GREEN (eth0, conectada a la red interna LAN_Verde) como 192.168.10.1/24 (ver Figura 2).

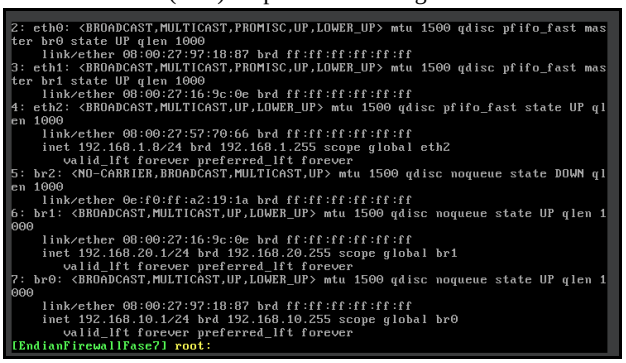
Figura 2. Configuración dentro de Endian Firewall de la instalación de la máquina virtual del interfaz GREEN.

Fuente: Captura de la máquina virtual

Tras la instalación base y el primer arranque, se accedió a la consola del sistema. Dado que no se solicitaron contraseñas durante la instalación, se utilizaron las opciones del menú para establecer credenciales conocidas para los usuarios root (administrador de consola) y admin (administrador web), utilizando la contraseña por defecto endian para realizar el cambio inicial.

Posteriormente, se ejecutó el Asistente de Configuración de Red (Opción 5 del menú) para verificar y completar los ajustes de red: se confirmó la IP de la zona GREEN, se habilitó el servidor DHCP para esta zona (asignando IPs en el rango 192.168.10.100-200), se asignó la interfaz eth1 (conectada a la red interna DMZ_Naranja) a la zona ORANGE y se estableció su IP estática como 192.168.20.1/24. La interfaz RED (eth2) se configuró inicialmente con DHCP (modo NAT en VirtualBox) y luego se cambió a modo Adaptador Puente, obteniendo una IP de la red física local (ej. 192.168.1.8/24). La configuración final de las interfaces activas (br0 para GREEN, br1 para ORANGE y eth2 para RED) se verificó mediante el comando ip a, como se muestra en la Figura 3.

Figura 3. Salida del comando ip a en la consola de Endian mostrando las IPs asignadas a las interfaces puente (br0, br1) y física (eth2) después de la configuración.

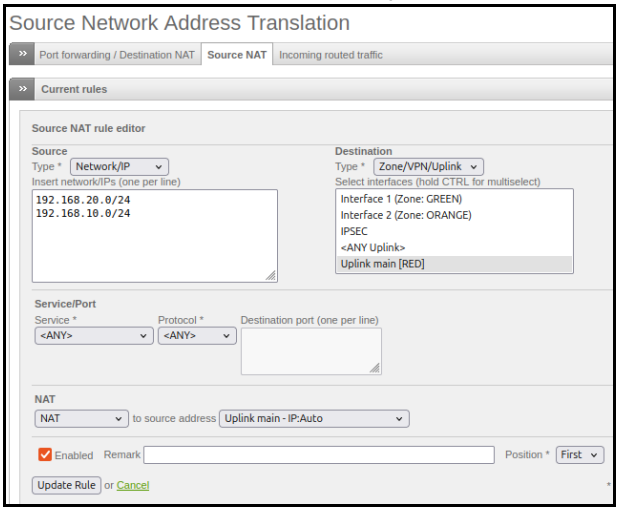


Fuente: Captura de la máquina virtual

5 CONFIGURACIÓN DE NAT Y FIREWALL (TEMÁTICAS 2 Y 3)

Una vez establecida la configuración base del firewall y las zonas, se procedió a configurar la Traducción de Direcciones de Red (NAT) y las reglas de firewall fundamentales. Para permitir el acceso a Internet desde las redes internas (GREEN y ORANGE), fue crucial crear una regla de Source NAT (SNAT). Esta regla, mostrada en la Figura 4, se configuró para traducir las direcciones IP de origen de las redes 192.168.10.0/24 y 192.168.20.0/24 utilizando la dirección IP de la interfaz de salida principal (RED/Uplink main).

Figura 4. Regla de Source NAT aplicada para permitir salida a Internet desde zonas GREEN y ORANGE.

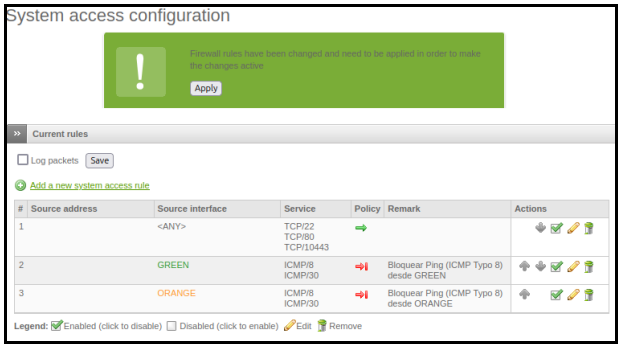


Fuente: Captura de la máquina virtual

Paralelamente, se definieron reglas de firewall para el tráfico saliente (Firewall -> Outgoing traffic), permitiendo explícitamente que el DMZServer (192.168.20.10) pudiera acceder a servicios esenciales en la zona RED, como DNS (TCP/UDP 53), HTTP (TCP 80) y HTTPS (TCP 443). Estas reglas fueron necesarias para resolver problemas iniciales de conectividad que impedían al servidor actualizar sus paquetes.

Adicionalmente, como parte de la Temática 3, se implementó el bloqueo de solicitudes de ping dirigidas al propio firewall desde las redes internas. Esto se logró mediante la creación de reglas de acceso al sistema (Firewall -> System access) que denegaban específicamente el tráfico ICMP tipo 8 (Echo Request) originado en las zonas GREEN y ORANGE, como se observa en la Figura 5. Las pruebas posteriores confirmaron que el ping a las interfaces del firewall desde las VMs internas fallaba, validando la efectividad de estas reglas.

Figura 5. Reglas de acceso al sistema aplicadas para bloquear ICMP tipo 8 desde zonas GREEN y ORANGE.

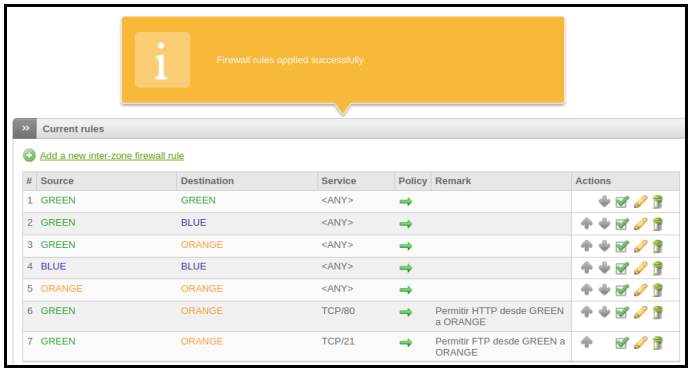


Fuente: Captura de la máquina virtual

6 CONTROL DE ACCESO INTER-ZONA Y WAN-DMZ (TEMÁTICA 4)

Para controlar el flujo de tráfico entre las zonas definidas y permitir el acceso controlado desde el exterior, se configuraron reglas Inter-Zona y de Redirección de Puertos (DNAT). Primero, se habilitó la comunicación desde la red interna GREEN hacia la DMZ ORANGE para los servicios HTTP y FTP, creando reglas específicas en la sección Firewall -> Inter-Zone traffic que permitían explícitamente este tráfico (ver Figura 6). Las pruebas posteriores desde el ClienteLAN hacia el DMZServer confirmaron el acceso exitoso a los servicios Apache y vsftpd.

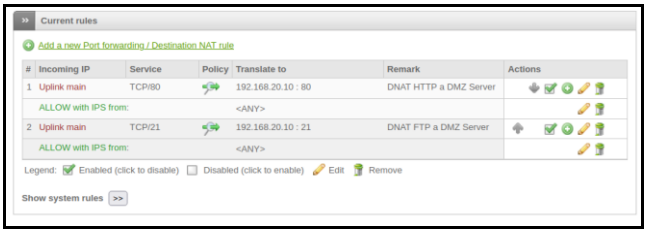
Figura 6. Reglas Inter-Zona aplicadas permitiendo HTTP y FTP desde GREEN hacia ORANGE.



Fuente: Captura de la máquina virtual

A continuación, para permitir el acceso a los servicios del DMZServer desde la red externa (WAN/RED), se configuró el Port Forwarding (DNAT) en la sección Firewall -> Port forwarding / NAT. Se crearon reglas para redirigir las solicitudes entrantes a la interfaz RED en los puertos TCP 80 (HTTP) y TCP 21 (FTP) hacia la dirección IP interna del DMZServer (192.168.20.10) en los puertos correspondientes, como se muestra en la Figura 7.

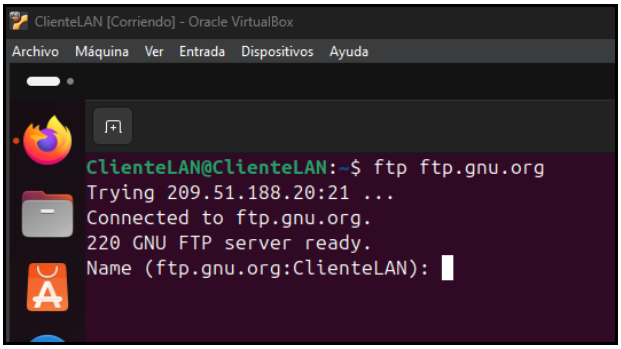
Figura 7. Reglas de Port Forwarding (DNAT) aplicadas para redirigir HTTP y FTP al DMZServer.



Fuente: Captura de la máquina virtual

Las pruebas de validación realizadas desde la máquina anfitriona Windows 11 (simulando la WAN) hacia la IP externa de Endian (192.168.1.8) demostraron el correcto funcionamiento de estas redirecciones, logrando acceder tanto a la página web por defecto de Apache como al prompt de inicio de sesión del servidor FTP alojados en el DMZServer. Finalmente, se verificó la conectividad saliente FTP desde la LAN hacia Internet (ftp ftp.gnu.org), como se evidencia en la conexión mostrada en la Figura 8, confirmando el correcto funcionamiento del SNAT para esta zona.

Figura 8. Conexión FTP desde la máquina virtual ClienteLAN, a un FTP Externo



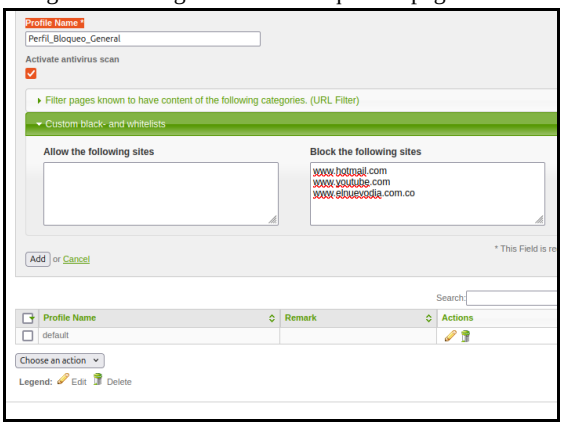
Fuente: Captura de la máquina virtual

7 IMPLEMENTACION DE PROXY HTTP NO TRANSPARENTE (TEMATICA 5)

Finalmente, se implementó un servidor Proxy HTTP en EFW para gestionar la navegación web de la zona GREEN. Se habilitó el servicio (Proxy -> HTTP) en modo no transparente, escuchando en el puerto TCP 8080. Se configuró la autenticación para utilizar la base de datos local de usuarios y grupos (NCSA).

Se creó un grupo denominado usuariosproxy y un usuario de prueba tematica5 (con contraseña 12345678) asignado a dicho grupo. Paralelamente, se definió un perfil de filtro web (Perfil_Bloqueo_General) que incluía una lista negra con los sitios www.hotmail.com, la URL específica de www.youtube.com y www.elnuevodia.com.co, cuya configuración se puede observar en la Figura 9.

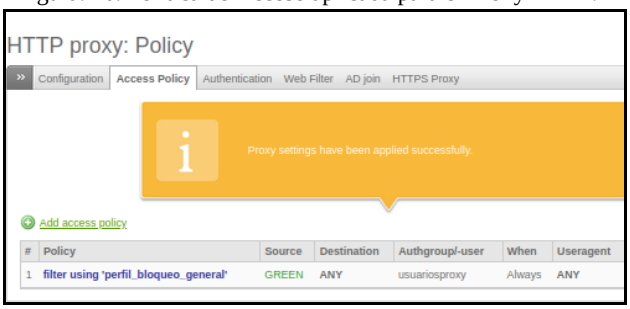
Figura 9. Configuración del bloqueo de páginas web.



Fuente: Captura de la máquina virtual

La configuración se completó mediante la creación de una Política de Acceso (Proxy -> HTTP -> Access Policy), mostrada en la Figura 10. Esta política especifica que el tráfico originado en la zona GREEN hacia cualquier destino debe pasar por autenticación basada en la pertenencia al grupo usuariosproxy y aplicar las reglas del filtro Perfil_Bloqueo_General, permitiendo el acceso si se cumplen las condiciones.

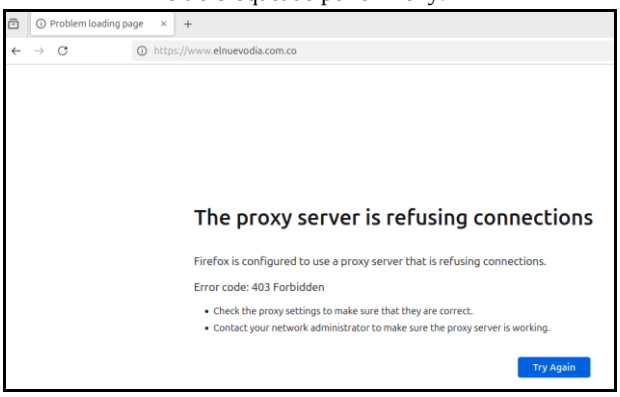
Figura. 10. Política de Acceso aplicada para el Proxy HTTP.



Fuente: Captura de la máquina virtual

Tras configurar el navegador Firefox del ClienteLAN para usar manualmente el proxy (192.168.10.1:8080), las pruebas de funcionamiento fueron exitosas: al intentar acceder a cualquier sitio, se solicitó la autenticación; introduciendo las credenciales de tematica5, se permitió el acceso a sitios no bloqueados (como google.com); e intentar acceder a los sitios de la lista negra resultó en una página de acceso denegado (Error 403) servida por el proxy, como se ilustra en la Figura 11.

Figura. 11. Página de error mostrada al intentar acceder a un sitio bloqueado por el Proxy.



Fuente: Captura de la máquina virtual

8 CONCLUSIONES

La implementación práctica de las cinco temáticas propuestas permitió validar la configuración de un entorno de red seguro utilizando Endian Firewall Community (EFW) en VirtualBox. Se logró establecer una segmentación efectiva mediante las zonas GREEN, ORANGE y RED, configurando las interfaces de red y el direccionamiento IP correspondiente. La configuración de reglas de firewall fue exitosa en varios niveles: se gestionó el tráfico saliente permitiendo servicios esenciales (DNS, HTTP, HTTPS) desde la DMZ, se controló el acceso al sistema bloqueando el protocolo ICMP tipo 8 desde las redes internas, y se definieron reglas Inter-Zona para permitir selectivamente el tráfico HTTP y FTP entre la LAN y la DMZ.

La implementación de Network Address Translation (NAT) fue crucial. Se configuró Source NAT (SNAT) para posibilitar la salida a Internet de las redes internas y Destination NAT (DNAT) o Port Forwarding para redirigir el tráfico externo HTTP y FTP hacia el servidor ubicado en la DMZ. La fase de troubleshooting inicial, que requirió cambiar la interfaz RED de modo NAT a modo Puente en VirtualBox, subrayó la importancia de verificar la conectividad a nivel del propio firewall y adaptar la configuración a las particularidades del entorno de virtualización.

Finalmente, la configuración de un Proxy HTTP no transparente demostró la capacidad de implementar controles de acceso a nivel de aplicación, requiriendo autenticación basada en usuarios y grupos locales (NCSA) y aplicando filtrado de contenido mediante listas negras, validando así un mecanismo adicional de seguridad para la navegación web desde la red interna.

En conjunto, el ejercicio permitió consolidar habilidades en la administración de sistemas GNU/Linux enfocados en seguridad, demostrando la viabilidad y efectividad de soluciones UTM open source como Endian Firewall para proteger infraestructuras de red.

9 REFERENCIAS

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

[2] Cervelión, Á. J. (2023). Instalación Nagios Core 4.4 en Ubuntu 22.04 [OVI]. Repositorio UNAD. https://repository.unad.edu.co/handle/10596/54230

[3] Debian. (2023). Manual administrador Debian 12.5.0. Debian. https://www.debian.org/releases/stable/amd64/index.es.html

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

[5] LaCroix, J. (2020). Mastering Ubuntu Server. Packt Pub. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[6] Linux Pro. Inst. (2022). LPI LPIC-1 Exam 101 (T. 102): Comandos GNU/Unix. https://learning.lpi.org/es/learning-materials/101-500/102/

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

[8] Gaikwad, D.P., & Chandane, M.M. (2015). Open-source firewalls performance in virtualization. *Proc. ICCICT*. https://doi.org/10.1109/ICCICT.2015.7045666

[9] Sharma, S., & Singh, S. (2016). Open-source firewalls survey & security issues. *Int. J. Comput. Sci. Inf. Technol.*, *7*(1), 409-12. https://www.researchgate.net/publication/304562924

[10] Islam, R., Ema, R.R., & Synthee, S.S. (2018). Software firewall study: Windows vs Linux. *Proc. ICAEEE*. https://www.researchgate.net/publication/324985984