# “FIREWALL”

Trabajo Preparatorio N°8

Laboratorio de Seguridad en Redes

Melanny Dávila
*Ingeniería en Telecomunicaciones*
*Facultad de Eléctrica y Eléctronica*
Quito, Ecuador
melanny.davila@epn.edu.ec

Alejandra Silva
*Ingeniería en Telecomunicaciones*
*Facultad de Eléctrica y Eléctronica*
Quito, Ecuador
alejandra.silva@epn.edu.ec

***Abstract*—A continuación, se hablará acerca de firewalls debido a que su importancia radica en que establecen una barrera entre las redes internas seguras y controladas en las que se puede confiar y las redes externas no confiables, como Internet.**

***Index Terms*—Firewall, tráfico, seguridad, NAT, NETinVM.**

## I. Introducción

Un firewall es un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide si permitir o bloquear tráfico específico según un conjunto definido de reglas de seguridad [1].

En su forma más básica, un firewall es esencialmente la barrera que se encuentra entre una red interna privada y la Internet pública. El objetivo principal de un cortafuegos es permitir la entrada de tráfico no amenazante y mantener fuera el tráfico peligroso.

A continuación se describirán los tipos de firewalls:

- **Filtrado de paquetes:** Una pequeña cantidad de datos se analiza y distribuye de acuerdo con los estándares del filtro.
- **Servicio de proxy:** Sistema de seguridad de red que protege mientras filtra mensajes en la capa de aplicación.
- **Firewall virtual:** Se implementa como un dispositivo virtual en una nube privada (VMware ESXi, Microsoft Hyper-V, KVM) o en una nube pública (AWS, Azure, Google, Oracle) para monitorear y asegurar el tráfico a través de redes físicas y virtuales.
- **Inspección estatal:** Filtrado dinámico de paquetes que monitorea las conexiones activas para determinar qué paquetes de red permitir a través del Firewall.
- **Cortafuegos de próxima generación (NGFW):** Firewall de inspección profunda de paquetes con inspección a nivel de aplicación [2].

## II. Objetivos

- Reforzar los conocimientos del alumno relativos a topologías de defensa de redes, el uso de cortafuegos y arquitecturas DMZ.
- Evaluar las reglas del firewall con respecto al tráfico permitido, descartado y rechazado.

## III. Cuestionario

*A. Revisar el marco teórico para la realización de la práctica.*

*B. Descargue NETinVM del siguiente enlace: https://informatica.uv.es/ carlos/docencia/netinvm/index.html*

A continuación, se presenta la pantalla principal de NETinVM.

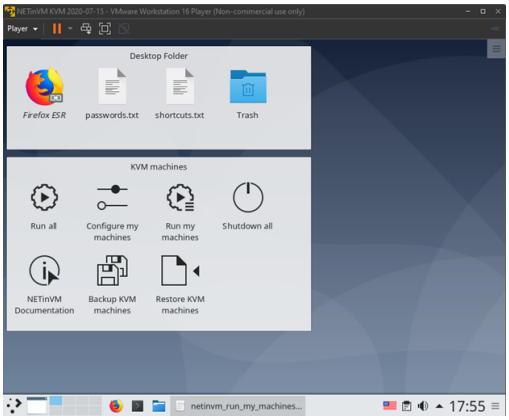


Fig. 1. Máquina NETinVM [1]

*C. Consultar el concepto de Destination NAT (DNAT) y en qué caso específico y práctico se utiliza.*

La NAT de destino se realiza en los paquetes entrantes cuando el cortafuegos traduce una dirección de destino a una dirección de destino diferente; por ejemplo, traduce una dirección de destino pública a una dirección de destino privada [4]. El NAT de destino también ofrece la opción de realizar el reenvío de puertos o la traducción de puertos.

La NAT de destino permite la traducción estática y dinámica:

- **IP estática:** Puede configurar una traducción estática uno a uno en varios formatos. Puede especificar que el paquete original tenga una única dirección IP de destino, un rango de direcciones IP o una máscara de red IP, siempre que el paquete traducido tenga el mismo formato y especifique la misma cantidad de direcciones IP. El

firewall traduce estáticamente una dirección de destino original a la misma dirección de destino traducida cada vez. Es decir, si hay más de una dirección de destino, el firewall traduce la primera dirección de destino configurada para el paquete original a la primera dirección de destino configurada para el paquete traducido, y traduce la segunda dirección de destino original configurada a la segunda dirección de destino traducida configurada. y así sucesivamente, utilizando siempre la misma traducción.

- **IP dinámica:** Le permite traducir la dirección de destino original a un host o servidor de destino que tiene una dirección IP dinámica , como un grupo de direcciones o un objeto de dirección que usa una máscara de red IP, rango de IP o FQDN, cualquiera de los cuales puede devolver múltiples direcciones de DNS. La IP dinámica (con distribución de sesiones) solo admite direcciones IPv4. La NAT de destino que usa una dirección IP dinámica es especialmente útil en implementaciones en la nube que usan direcciones IP dinámicas [3].

Un uso común de la NAT de destino es configurar varias reglas de NAT que asignan una única dirección de destino pública a varias direcciones de host de destino privadas asignadas a servidores o servicios. En este caso, los números de puerto de destino se utilizan para identificar los hosts de destino [4]. Por ejemplo:

- Reenvió de puertos: Puede traducir una dirección de destino publica y un número de puerto a una dirección de destino privada pero no mantiene le mismo número de puerto.
- Traducción de puertos: Puede traducir una dirección destino publica y un número de puerto a una dirección de destino privada y un número de puerto diferente, manteniendo así privado el numero de puerto real [4].

## REFERENCES


[1] “What Is a Firewall?”, Cisco. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html (accedido ago. 04, 2021).

[2] “What is a Firewall? The Different Types of Firewalls”, Check Point Software. https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/ (accedido ago. 04, 2021).

[3] Perez. C. , Perez. D. ”NETinVM”.(2020).https://informatica.uv.es/ carlos/docencia/netinvm/index.html. accedido (2021, Agos,4).

[4] ”NAT de destino”. (2021).https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/nat/source-nat-and-destination-nat/destination-nat. accedido (2021, Agos,4).