Tecnologías automatizadas de última generación en ciberseguridad: Next generation firewalls

Luisa Fernanda Bermudez Giron
Jorge David Sáenz Diaz
Karol Daniela Ladino Ladino

Universidad Escuela Colombiana de Ingeniería Julio Garavito

luisa.bermudez@mail.escuelaing.edu.co
jorge.saenz-d@mail.escuelaing.edu.co
karol.ladino@mail.escuelaing.edu.co

***Resumen*—En este paper discute la importancia de la ciberseguridad en el mundo actual y como los Next Generation Firewalls (NGFW) se han convertido en una pieza de vital importancia entre la amplia gama de estrategias de ciberseguridad. Se explica que son los NGFW, su capacidad de detección y bloqueo de ataques cibernéticos avanzados de diferentes tipos, añadiendo una capa de seguridad efectiva contra amenazas como el ransomware, phishing, malware cifrado, entre otras. Se compara con los firewalls tradicionales, destacando la ventaja de los NGFW frente a estos, ya que proveen la capacidad de inspeccionar el tráfico a un nivel más profundo, proporcionando servicios de seguridad tales como, el conocimiento y control de aplicaciones, la prevención de intrusiones y la inteligencia de amenazas. Finalmente, se concluye que hay muchos productos NGFW disponibles en el mercado que utilizan diferentes tecnologías para proporcionar esta capa de seguridad adaptada a las necesidades del usuario/organización.**

***Abstract*- This paper discusses the importance of cybersecurity in today's world and how Next Generation Firewalls (NGFWs) have become a vitally important part of a wide range of cybersecurity strategies. It explains what NGFWs are, their ability to detect and block advanced cyber attacks of different types, adding an effective layer of security against threats such as ransomware, phishing, encrypted malware, among others. It is compared to traditional firewalls, highlighting the advantage of NGFWs over them, as they provide the ability to inspect traffic at a deeper level, providing security services such as, application awareness and control, intrusion prevention and threat intelligence. Finally, it is concluded that there are many NGFW products available in the market that use different technologies to provide this layer of security tailored to the needs of the user/organization.**

I. Introducción

La ciberseguridad es un problema que ha ido creciendo cada día más debido a los avances de la tecnología, llevando así a que los ataques cibernéticos sean más sofisticados y constantes. Los Firewalls de Nueva Generación (NGFW) son una herramienta que sirve para salvaguardar la integridad y la privacidad de la información en las redes y sistemas de organizaciones pequeñas, medianas y grandes.

Los NGFW han evolucionado significativamente con respecto a los firewalls tradicionales. Si bien estos últimos bloquean o permiten los datos en función de hacia dónde van, de donde proceden y si forman parte o no de una conexión de red legítima; los NGFW inspeccionan los datos a un nivel más profundo para identificar y bloquear las amenazas que puedan estar ocultas en el tráfico con apariencia normal.

En la actualidad existen una gran variedad de productos NGFW disponibles en el mercado, los cuales son proveídos por fabricantes lideres como Fortinet, Cisco, Palo Alto, Networks, Check Point y Juniper. Cada uno de estos productos cuenta con tecnologías específicas para proporcionar un nivel de protección adaptado a las necesidades de cada organización.

II. Next Generation Firewalls

La encuesta “Threat Mindset Survey 2022” patentada de SonicWall da a conocer que existe una preocupación creciente en materia de ciberataques entre el 66% de las organizaciones encuestadas; ransomware lidera como el ataque cibernético más inquietante ya que el 91% de todos los clientes lo mencionaron como su mayor preocupación. El phishing y el spear-phishing (76%), así como el malware cifrado (66%), se han posicionado como las tres principales preocupaciones.

Para abordar las preocupaciones previamente mencionadas, muchas organizaciones están recurriendo a soluciones de ciberseguridad avanzadas, como los Firewalls de Nueva Generación (NGFW) los cuales se han convertido en una pieza fundamental de la estrategia de seguridad cibernética, ya que son capaces de detectar y bloquear ataques sofisticados, incluyendo ransomware, phishing y malware cifrado, proporcionando una defensa efectiva contra estas amenazas."

Un firewall de próxima generación (NGFW) es la tercera generación de firewalls que se puede implementar tanto en forma de hardware como de software y se destaca por su capacidad para detectar y bloquear ataques cibernéticos cada vez más avanzados mediante la aplicación de políticas de

seguridad en múltiples niveles, incluyendo la aplicación, el puerto y el protocolo.

En comparación con un firewall tradicional, que generalmente se limita a una inspección detallada del tráfico de red entrante y saliente, un NGFW va más allá. Integra características adicionales de vanguardia, como el reconocimiento y control de aplicaciones, lo que permite identificar y gestionar el uso de aplicaciones específicas en la red. Además, ofrece una prevención de intrusiones integrada, lo que significa que puede detectar y detener posibles amenazas antes de que comprometan la seguridad de la red.

Una de las características más valiosas de un NGFW es su capacidad para acceder a la inteligencia sobre amenazas proporcionada en la nube. Esto significa que puede estar al tanto de las últimas amenazas cibernéticas y adaptarse continuamente para defenderse contra ellas.

Pensemos en dos agencias de seguridad en aeropuertos. La primera (Firewall tradicional) comprueba que los pasajeros no estén en ninguna No-fly list, que sus identidades coincidan con lo que figura en sus billetes y que se dirijan a los destinos a los que presta servicio el aeropuerto. La segunda (NGFW), además de comprobar las No-fly list y demás, inspecciona lo que llevan los pasajeros, asegurándose de que no tengan artículos peligrosos o no permitidos. La primera agencia mantiene la seguridad de los aeropuertos frente a las amenazas obvias; la segunda también identifica las amenazas menos obvias [1].

A. ¿Cómo funciona un NFGW?

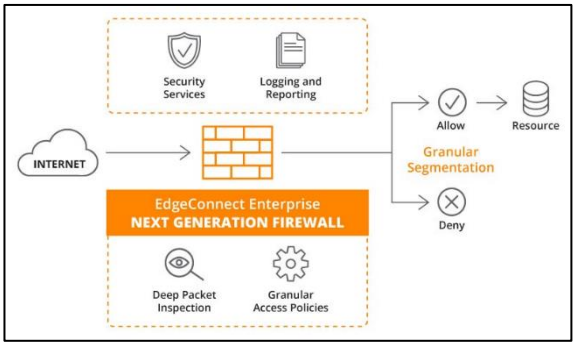

Fig. 1. Funcionamiento de un NGFW [2]

Un Firewall de nueva generación es como un guardián que se encuentra en la intersección entre la red interna de una organización y el internet, encargado de controlar el tráfico que ingresa y sale de la organización.

- El NGFW proporciona **servicios de seguridad** avanzados para proteger la red de una organización como la detección y prevención de amenazas, así como la aplicación de políticas de seguridad.
- También **registran y generan informes** detallados sobre el tráfico de red, las amenazas detectadas y las actividades relacionadas con la seguridad. Estos registros son esenciales para el monitoreo y la auditoría de la seguridad de la red.
- Por otro lado, los NGFW realizan una **inspección minuciosa de cada paquete** de datos que atraviesa la red. Esto implica analizar el contenido de los paquetes a nivel de aplicación, puerto y protocolo, lo que les permite identificar y bloquear amenazas más allá de la capa superficial.
- Así mismo, los NGFW permiten a las organizaciones establecer **políticas de acceso personalizadas** en las que se define quién tiene acceso a qué recursos y en qué condiciones.
- Los NGFW mejoran la seguridad al limitar el acceso entre diferentes partes de la red mediante la segmentación de esta en partes más pequeñas y así controlar el flujo de tráfico entre cada una de las partes.
- Basándose en las reglas de seguridad y las condiciones de acceso configuradas, los NGFW pueden **permitir o denegar** el acceso de usuarios o dispositivos a recursos específicos.

B. Funciones del NFGW

Un NGFW aparte de ofrecer las mismas funciones que un firewall normal, también proporciona una serie de funciones avanzadas como lo son:

- **Conocimiento de la VPN:** Un NGFW puede identificar el tráfico de VPN encriptado y permitir su paso, lo que mejora la seguridad de las comunicaciones seguras.
- **Conocimiento y Control de las Aplicaciones:** Los NGFW pueden analizar el tráfico en la capa de aplicación (capa 7) para identificar las aplicaciones en uso. Esto permite a los administradores bloquear aplicaciones potencialmente peligrosas y controlar el acceso a recursos específicos.
- **Prevención de Intrusiones:** Los NGFW incorporan sistemas de prevención de intrusiones (IPS) que detectan y bloquean amenazas conocidas y potenciales en el tráfico entrante.

  Los IPS utilizan varios métodos para proteger la red contra intrusiones como:
  - **Detección de firmas:** Escanear la información de los paquetes entrantes y compararla con amenazas conocidas.
  - **Detección estadística de anomalías:** Escanear el tráfico para detectar cambios inusuales en el comportamiento, en comparación con una base de referencia.
  - **Detección de análisis de protocolos de estado:** se centra en los protocolos de red en uso y los compara con el uso típico de los protocolos.

- **Inteligencia de Amenazas:** Los NGFW usan información sobre posibles ataques procedentes de fuentes externas

para mantenerse actualizados sobre potenciales amenazas en ciberseguridad y firmas de malware. También pueden bloquear direcciones IP maliciosas conocidas basadas en información de reputación de IP, en donde estas direcciones IP suelen proceder de ataques (especialmente de ataques de bots).

III. Firewall Tradicional vs NGFW

TABLE I
Comparación entre firewalls

Capacidad	FW Tradicional	NGFW	Ventajas del NGFW
Inspección	Sin estado	Con estado	Mantener un seguimiento activo de las conexiones en curso, lo que significa que puede identificar y bloquear amenazas en tiempo real.
Visibilidad	Rudimentaria, solo capas inferiores del TCP/IP	Profunda, incluye todas las capas del TCP/IP	Inspeccionar el tráfico de las capas TCP/IP a un nivel detallado, lo que facilita la detección de amenazas que no se notan primera vista.
Servicios	Básico	Completo	Proporciona una amplia gama de servicios de seguridad, lo que incluye detección y prevención de intrusiones, filtrado de contenido, control de aplicaciones y más.
Protección	Limitada	Optimizada	Está diseñado para ofrecer una protección sólida y efectiva contra una variedad de amenazas cibernéticas.

Nota: La tabla presentada anteriormente de comparación de firewalls, ha sido adaptada para fines de esta investigación [3].

IV. Productos y Tecnologías

En la actualidad existen numerosos productos NGFW disponibles en el mercado que utilizan una variedad de tecnologías como inspección de contenido, protección contra amenazas avanzadas, inteligencia de amenazas y aprendizaje automático. Estos productos son proveídos por fabricantes lideres como Fortinet, Cisco, Palo Alto, Networks, Check Point y Juniper.

Algunos de estos productos son:

- **Juniper SRX Series:** brindan protección contra amenazas líder en la industria y han sido clasificados constantemente como el número 1 en eficacia en todas las pruebas durante los últimos cuatro años. Debido a esto Juniper recibió una calificación "AAA" en el Informe de firewall de red empresarial 2023 de CyberRatings, lo que demuestra una tasa de bloqueo de exploits del 99,9 % sin falsos positivos.

- **Fortinet FortiGate:** proporcionan protección contra amenazas y descifrados líderes en la industria a escala con una arquitectura ASIC personalizada. También ofrecen redes seguras con funciones integradas como SD-WAN, conmutación e inalámbrica, y 5G. Por esta razón, Fortinet logro un puntaje de eficacia de seguridad del 99,88 % en el Informe de firewall empresarial de CyberRatings 2023 con el El FortiGate 600F que recibió una calificación AAA.

- **Cisco Firepower:** es el primer NGFW centrado en las amenazas verdaderamente integrado del sector con administración unificada. Ofrece visibilidad y control de aplicaciones (AVC), IPS de última generación (NGIPS) opcional de Firepower, protección frente a malware avanzado (AMP) de Cisco y filtrado de URL. Cisco Firepower NGFW ofrece protección frente a amenazas avanzadas antes y después de un ataque, así como durante este.

Conclusión

Los Firewalls de Nueva Generación se han convertido en una herramienta importante utilizada por las organizaciones para proteger su información, debido a que estos tienen la capacidad de detectar y bloquear amenazas avanzadas gracias a la inspección profunda de paquetes, el control de aplicaciones en la red, la prevención de intrusiones y el acceso a la inteligencia de amenazas en la nube convirtiéndolo en un componente de seguridad muy completo.

Referencias

[1] [2023]. ¿Qué es un firewall de nueva generación (NGFW)?. Cloudflare. Disponible en: https://www.cloudflare.com/es-es/learning/security/what-is-next-generation-firewall-ngfw/

[2] [2023]. ¿Qué es un firewall de próxima generación (NGFW)?. Hewlett Packard Enterprise Development. Disponible en: https://www.arubanetworks.com/latam/faq/que-es-un-ngfw/

[3] [2023]. ¿Qué es un firewall de próxima generación (NGFW)?. Hewlett Packard Enterprise Development. Disponible en: https://www.arubanetworks.com/latam/faq/que-es-un-ngfw/

[4] [2023]. SONICWALL PRESENTA LOS DATOS DE SU ENCUESTA THREAT MINDSET SURVEY 2022. SonicWall. Disponible en: https://www.sonicwall.com/es-mx/news/sonicwall-presenta-los-datos-de-su-encuesta-threat-mindset-survey-2022/

[5] [2021,12,08]. NGFW: ¿Qué es el Next Generation Firewall?. International IT. Disponible en: https://www.internationalit.com/post/ngfw-que-es-el-next-generation-firewall?lang=es

[6] [2023]. What Is a Next-Generation Firewall?. Cisco. Disponible en: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html

[7] [2023]. SRX Series Firewalls. Juniper Networks. Disponible en: https://www.juniper.net/us/en/products/security/srx-series.html

[8] [2016]. Firewall de última generación Cisco Firepower. Cisco. Disponible en: https://www.cisco.com/c/dam/global/es_es/assets/pdf/c78-736661-00_cisco_firepower_next-generation_firewall_ds_v4a_es-eu.pdf

[9] [2023]. Next-Generation Firewall (NGFW). Fortinet. Disponible en: https://www.fortinet.com/lat/products/next-generation-firewall

[10] 2023. ¿Qué es un cortafuegos de próxima generación?. Zscaler. Disponible en: https://www.zscaler.es/resources/security-terms-glossary/what-is-next-generation-firewall#:~:text=Control%20de%20aplicaciones%3A%20los%20NGFW,que%20aumenta%20la%20visibilidad%20general