Evaluación del rendimiento y la seguridad de los Next generation firewalls (NGFW)

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*—El entorno digitalizado y conectado de la actualidad ha dado lugar a un aumento constante de ciberataques sofisticados y frecuentes. Este paper explora la ciberseguridad en relación con los NGFW y su importancia en la protección contra amenazas avanzadas. Se presenta un caso de uso para evaluar el rendimiento y la seguridad de un servicio NGFW en un entorno de laboratorio, abordando aspectos técnicos de configuración y la automatización de pruebas con Python. El objetivo de este caso de uso es medir la capacidad del NGFW para detectar y mitigar amenazas, así como su impacto en el rendimiento de la red. Los resultados esperados incluyen la capacidad del NGFW para detectar y bloquear amenazas cibernéticas con éxito, sin un impacto significativo en el rendimiento de la red. Para tener una visión más clara de la eficacia y aplicabilidad de los NGFW en la lucha contra los ciberataques en entornos empresariales.**

***Abstract*—Today's digitized and connected environment has resulted in a steady increase in sophisticated and frequent cyber-attacks. This paper explores cybersecurity as it relates to NGFWs and their importance in protecting against advanced threats. A use case is presented to evaluate the performance and security of an NGFW service in a lab environment, addressing technical aspects of configuration and test automation with Python. The objective of this use case is to measure the NGFW's ability to detect and mitigate threats, as well as their impact on network performance. Expected results include the ability of NGFW to successfully detect and block cyber threats without significant impact on network performance. For a clearer picture of the effectiveness and applicability of NGFWs in combating cyber-attacks in enterprise environments.**

I. Introducción

Debido a que cada día contamos con un entorno cada vez más digitalizado y conectado, la ciberseguridad se ha convertido en un desafío de crecimiento continuo. Adicional a esto, el auge de la tecnología ha llevado a que organizaciones de todos los tamaños enfrenten una amenaza constante para la confidencialidad, integridad y disponibilidad de los activos de información dado que en la actualidad los ciberataques son más sofisticados y frecuentes.

La encuesta “Threat Mindset Survey 2022” patentada de SonicWall revela que el 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 han evolucionado significativamente en comparación con los firewalls tradicionales, que solían basarse en decisiones sobre datos según su origen y destino.

Aprovechando la base de conocimiento presentada anteriormente, exploraremos el ámbito de la ciberseguridad y su relación con los NGFW. Los firewalls de nueva generación se han destacado como una herramienta de tercera generación que desempeñan un papel fundamental en la estrategia de seguridad cibernética de las organizaciones. Su capacidad para detectar y bloquear ataques avanzados, como ransomware, phishing y malware cifrado, mediante una inspección profunda del tráfico, control de aplicaciones, prevención de instrucciones y acceso a la inteligencia de amenazas en la nube, los convierte en un componente crucial para salvaguardar la seguridad de las redes y sistemas en un entorno de constante evolución.

Para ilustrar la importancia y las capacidades de los NGFW, se planteará un caso de uso con un enfoque en la evaluación del rendimiento y la seguridad de un servicio NGFW en un entorno de laboratorio. Este caso de uso permitirá medir la capacidad del NGFW para detectar y mitigar amenazas, así como su impacto en el rendimiento de la red. Se explorarán los aspectos técnicos de su configuración y la automatización de pruebas con Python para obtener resultados precisos.

II. Metodología

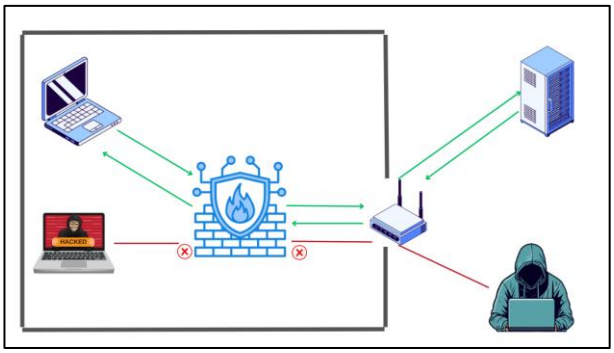

Fig. 1. Funcionamiento firewall [1]

2.1. Configuración del entorno de laboratorio

Para llevar a cabo la evaluación del rendimiento y la seguridad del servicio NGFW, se establecerá un entorno de laboratorio, en el que se configurarán dos máquinas virtuales (VM) que simularán un escenario de host protegido por el NGFW que nos permitirá evaluar la capacidad del NGFW para detectar y mitigar amenazas y un host de ataque desde el cual se generarán las pruebas de seguridad. Ambas máquinas estarán conectadas a una red virtual, lo que permitirá la realización de las pruebas y la recopilación de datos de manera controlada.

2.2. Despliegue y configuración del NGFW

El servicio NGFW se implementará y configurará en una de las máquinas virtuales, en este caso sería la que va a actuar como host protegido. Para esto se seguirán las mejores prácticas de configuración para garantizar una seguridad efectiva.

2.3. Generación de trafico de prueba

Se utilizarán herramientas de generación de tráfico, para estos escenarios de red. Esto incluirá pruebas de intrusión, escaneo de puertos, tráfico de malware y otros tipos de amenazas comunes. La generación de este tráfico se llevará a cabo desde el host de ataque con el propósito de evaluar la efectividad del NGFW en la detección y bloqueo de dichas amenazas.

2.4. Evaluación de la capacidad de detección y bloqueo

Se medirá la capacidad del NGFW para detectar y bloquear las amenazas generadas en el tráfico de prueba. Se registrarán las tasas de detección y bloqueo, así como los posibles falsos positivos. Los resultados obtenidos en esta evaluación nos permitirán determinar la eficacia del NGFW en la protección contra amenazas cibernéticas.

2.5. Evaluación del rendimiento

Se medirá el impacto del NGFW en el rendimiento de la red, incluyendo la latencia, el ancho de banda y la utilización de recursos de la máquina virtual en la que se encuentra implementado. Esta evaluación nos brindara información sobre la influencia del NGFW en la operatividad de la red.

2.6. Automatización de pruebas con Python

Se desarrollarán scripts en Python para automatizar la ejecución de las pruebas, la recopilación de datos y la generación de informes.

2.7. Análisis de resultados

Luego de realizar las pruebas, se analizarán los resultados de estas para evaluar la efectividad del NGFW en términos de detección, bloqueo y rendimiento.

III. Resultados esperados

- El NGFW debe ser capaz de detectar y bloquear las amenazas cibernéticas con una alta tasa de éxito.
- El NGFW no debe tener un impacto significativo en el rendimiento de la red.

IV. Conclusiones y Discusión

El paper concluirá con una discusión detallada sobre los resultados obtenidos en el experimento. Se analizará el rendimiento y la seguridad del servicio NGFW, así como las implicaciones prácticas de su uso en entornos empresariales. Los hallazgos de este experimento proporcionarán una visión clara sobre la eficacia y la aplicabilidad de los NGFW en la protección contra las crecientes amenazas cibernéticas en la actualidad.

Referencias

[1] Incibe. [2020,06,02]. Firewall tradicional, UTM o NGFW. Diferencias, similitudes y cuál elegir según tus necesidades. Incibe. Disponible en: https://www.incibe.es/empresas/blog/firewall-tradicional-utm-o-ngfw-diferencias-similitudes-y-cual-elegir-segun

[2] [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/

[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]. ¿Qué es un firewall de próxima generación (NGFW)?. Hewlett Packard Enterprise Development. Disponible en: https://www.arubanetworks.com/latam/faq/que-es-un-ngfw/
[5] [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/
[6] [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
[7] [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
[8] [2020]. Next Generation Firewall, y los impactos en la seguridad corporativa.Ostec. Disponible en: https://ostec.blog/es/seguridad-perimetral/next-generation-firewall/?cn-reloaded=1
[9] [2023]. Casos de uso del Next-Generation Firewall. Fortinet. Disponible en: https://www.fortinet.com/lat/products/next-generation-firewall/use-case
[10] Canalejo, L. [2023,09,28]. Configurar Firewall seguro en la Nube - ¡Guía Fácil y Rápida!. Linkedin. Disponible en: https://www.linkedin.com/pulse/configurar-firewall-seguro-en-la-nube-gu%C3%ADa-f%C3%A1cil-y-r%C3%A1pida-canalejo/?originalSubdomain=es
[11] Bermudez, LF. Sáenz, JD. Ladino, KD. [2023]. Tecnologías automatizadas de última generación en ciberseguridad: Next generation firewalls.