

# Foro Evaluado#3

---

SEGURIDAD DE REDES [SDR 404]

Profesor: William Vladimir Alvarado Campos

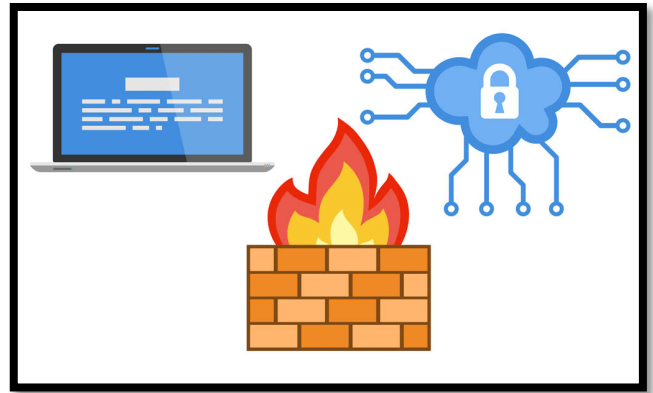
## INTEGRANTES

Miguel Angel Barahona Garcia.....BG191322

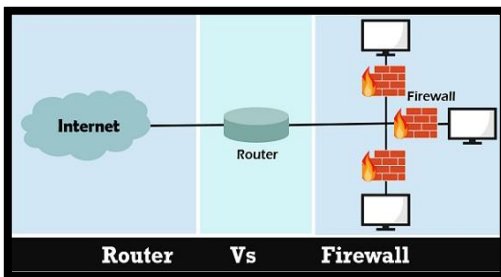
José Manuel Orellana Gutiérrez.....OG160906

## 1- ¿Cuáles son las ventajas que se tienen entre las soluciones de NGFW vs los Firewall clásicos?

1. Tiene un mejor control y una vista más detallada de las aplicaciones dentro de la red.
2. Tiene soporte y apoyo con el sistema de prevención de intrusos.
3. Tiene soporte con:
  - A. NAT (Network Address Translation o Traducción de direcciones de red).
  - B. Servicios de reputación e identidad.
  - C. VPN (Virtual Private Network o Red privada virtual).
4. Sus capas de trabajo rondan desde la capa 2 hasta la capa 7.
5. Los informes son más específicos, ya que nos brinda toda la información sobre los paquetes que se mueven dentro de la red.
6. Contiene mayor capacidad de alcance y de eliminación contra los malware y virus.
7. Su proceso de prevención de amenazas es antes, durante y después de cualquier amenaza.



## 2- Ante los avances que representan estas tecnologías, ¿Considera realmente necesario utilizar tecnologías tradicionales como los routers, por ejemplo, para brindar conectividad a la red?



**Respuesta:** En la actualidad, utilizar routers siempre es necesario, debido que es una buena herramienta para conexiones entre dispositivos, a pesar de que un firewall de nueva generación te brinda la función de leer los paquetes entrantes y su contenido, los routers nos brindan una mejor estabilidad en la red y a su topología, y un mejor manejo a

la hora de que las tramas transiten en la red. Los routers siempre son esenciales, y también depende mucho de la seguridad que se tenga dentro de la red, ya que si es una muy pequeña y con pocos dispositivos, tener un router no es tan necesario, pero si es para una red de una empresa, un router siempre es esencial, por lo que se ha estado mencionando anteriormente.

**3- En lo relacionado a los costos económicos de los mismos, ¿Considera usted que una solución "open source" o incluso "libre" puede llegar a competir con soluciones de renombre como Palo alto o Check Point?**

**Respuesta:** En mi opinión depende mucho de la red que se necesita proteger, más allá de que al utilizar un firewall de "open source" es más económico y no conlleva gastos de licencia, esto puede llegar a jugar en contra, debido que al ser de código libre, no pueden ser tan efectivos, al momento de proteger contra amenazas más peligrosas de lo común. Decir que puede llegar a competir contra firewall de empresas como Palo Alto, es una idea errónea y la única manera de pensar que un firewall de "open source" puede ser mejor que un firewall de las empresas mencionadas, sería en el ámbito económico, ya que si es para un equipo de un estudiante normal, un firewall "open source", es una buena opción, ya que no necesita de mayor conocimiento en protección de red y no genera gastos, pero si ya es para una empresa, que tiene demasiados datos, y tiene mucho flujo de información entre su red, lo más seguro es invertir un poco y comprar una licencia de firewall de empresas como Palo Alto o Check Point.

**Parte 2: Desarrolle una investigación de sobre mejores firewalls en el mercado**

Marca de Firewall	Check Point, Next Generation Firewall (NGFW)	
Características que apoya la confidencialidad	Características que apoyan la disponibilidad	Características que apoyan la integridad
Licencia de por vida, con excepciones de contrato y/o hardware adquirido.	Alta demanda del servicio	Haber demostrado su eficacia contra los ciberataques de nivel 5.
Check Point tiene el derecho de revisar, borrar o restringir ciertos programas del sistema operativo.	Se adapta en mayor parte a las necesidades de los consumidores.	Alto grado de customización, personalización de acuerdo al agrado/necesidad de la empresa/usuario.
Check Point tiene el derecho de revisar, descryptar, trafico encriptado y re-encriptarlo para ser enviado al servidor.		

Marca de Firewall	Cisco, Adaptive Security Appliance (ASA) with NGFW	
Características que apoya la confidencialidad	Características que apoyan la disponibilidad	Características que apoyan la integridad
Cisco recolecta información no limitada a solo sistemas operativos para su próxima revisión.	El precio por su desarrollo, calidad y desempeño es bastante accesible.	Flexibilidad en la personalización de las características del producto.
Los productos son de libre uso una vez adquiridos.	Mejora los resultados de los procesos de negocios y la relación de los clientes con los servicios.	Alto rango de escalabilidad.
	Marca reconocida.	Visibilidad y control de las acciones en la red.

Marca de Firewall	FortiNet, FortiGate NGFW	
Características que apoya la confidencialidad	Características que apoyan la disponibilidad	Características que apoyan la integridad
FortiNet concede al contratante acceso administrativos otorgándole un ID y password para su usuario.	Precio realmente accesible	Es fácil de hacer trabajar una vez adquirido el producto/servicio
El contratante autoriza la recopilación y uso de información sobre el producto.	Buena demanda de producto por su desempeño.	Facilidad para poder monitorear los paquetes en la red.
		Fácil de integrar con servicios de antivirus y VPNs

Marca de Firewall	Juniper Network, NGFW	
Características que apoya la confidencialidad	Características que apoyan la disponibilidad	Características que apoyan la integridad
Restringe el acceso a sitios en la lista negra del producto.	Demanda regular por su protección en contra de malware.	Flexibilidad y facilidad otorgada por el CLI (Command Line Interface) del producto.
El producto otorga el mantenimiento de la red al consumidor.	Demanda por su flexibilidad y facilidad de uso en un entorno controlado.	Regulación del tráfico permitido en la red.

- **Bibliografía Adicional**

Next Generation Firewall (NGFW). (2020, 1 noviembre). Check Point Software.  
<https://www.checkpoint.com/products/next-generation-firewall/>

Software License Agreement & Hardware Warranty. (2020, 21 febrero). Check Point Software.  
<https://www.checkpoint.com/support-services/software-license-agreement-limited-hardware-warranty/>

Cisco ASA 5500-X with FirePOWER Services. (2020, 11 noviembre). Cisco.  
<https://www.cisco.com/c/en/us/products/security/asa-firepower-services/index.html>

Gartner, Inc. (2020). Cisco ASA review in Network Firewall. Gartner.  
<https://www.gartner.com/reviews/market/network-firewalls/vendor/cisco/product/cisco-asa/review/view/3426772>

Next-Generation Firewall Services. (2020). Juniper Networks.  
<https://www.juniper.net/us/en/products-services/security/next-generation-firewall-services/>