

# Seguridad Perimetral



# Seguridad Perimetral

La evolución de la tecnología y la creciente demanda de seguridad han permitido que los sistemas de seguridad perimetral evolucionen para ofrecer una mayor confiabilidad a los usuarios tanto internos como externos sobre la transparencia y protección de su información para el acceso a diferentes servicios, hoy en día existen un sin número de personas que usan sus conocimientos y ética profesional de una forma incorrecta al ingresar a redes informáticas restringidas ocasionando pérdidas multimillonarias alrededor del mundo. La seguridad perimetral se ha convertido en un elemento clave que cada vez interesa valorar a más empresas, especialmente a aquellas que tienen presencia en el medio digital.

La seguridad perimetral es un método de defensa de las redes informáticas, el cual consiste en instalar equipos de comunicaciones (Firewall) en los que se establece las políticas de seguridad necesarias para su óptimo funcionamiento; estos equipos se los coloca entre la red externa y la red interna, permitiendo o denegando el acceso a los usuarios internos y externos a los diferentes servicios de la red.

## ¿Qué es un Firewall Perimetral?

Un firewall es aquel que se encarga de filtrar todos los paquetes de red que pasan por el y así tomar la decisión si dejar pasar el paquete o no, dependiendo si el paquete tiene contenido no deseado para la red.

El objetivo del Firewall perimetral es impedir que se realicen conexiones entre la red corporativa e Internet que estén fuera de la política de seguridad de la compañía, por tanto, estaríamos frente a la primera línea de defensa esencial de cualquier empresa relacionada al medio digital.

## NEXT GENERATION FIREWALL DE FORTINET

Presentamos la solución que nos permitirá garantizar la seguridad perimetral e integración con la seguridad de red: FortiGate, el Next generation firewall de Fortinet.

Ante nosotros tenemos un firewall de próxima generación (NGFW) y de alto rendimiento de protección frente a las amenazas y con visibilidad automatizada para detener los ataques. Al tratarse de un firewall de próxima generación, consigue filtrar el tráfico de la red y proteger a la empresa frente a amenazas externas. Con la diferencia de que posee unas capacidades de inspección mayores, para así identificar ataques, malwares y otras amenazas.

Reduce el costo y la complejidad consolidando capacidades de seguridad de empresas líder, como ser Inspección SSL, Filtrado Web, Control de Aplicaciones, y Sistema de Prevención de Intrusos (IPS), entre muchas características, para proveer visibilidad completa y proteger cualquier extremo de la red.

