

**SEGURIDAD EN TIEMPO
REAL**

CÓMO UN NGFW MODERNO DETIENE AMENAZAS ANTES DE QUE LLEGUEN A TU RED



EBOOK



Introducción

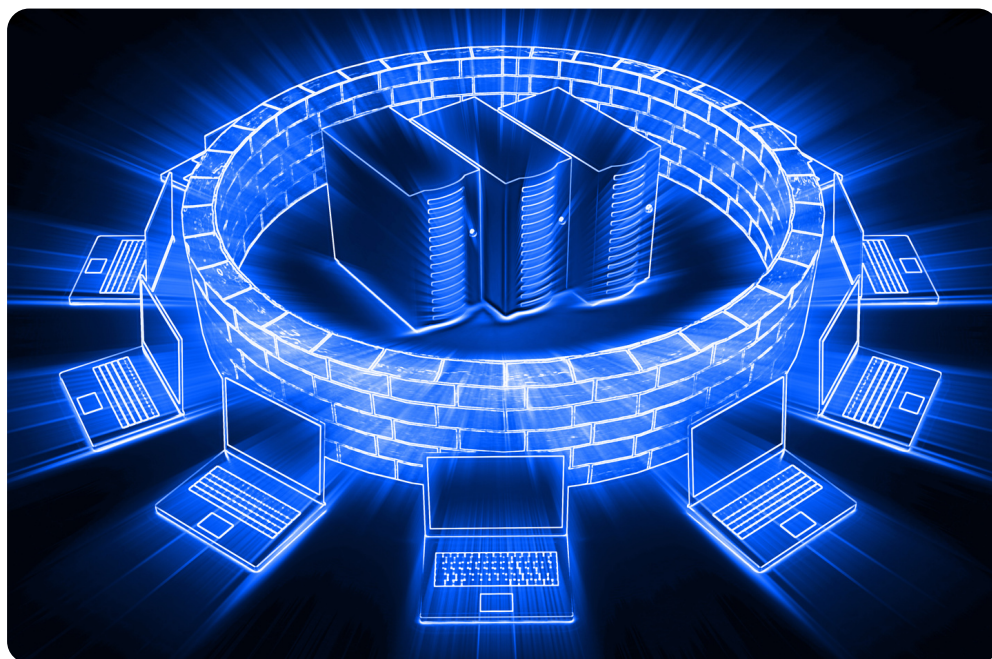
Las organizaciones industriales, logísticas y corporativas se enfrentan a un entorno digital donde las amenazas evolucionan más rápido que nunca. El crecimiento del trabajo remoto, los dispositivos IoT y la conectividad constante han ampliado la superficie de ataque. Frente a este escenario, un firewall tradicional ya no es suficiente. Es aquí donde entra en juego un Next Generation Firewall (NGFW): una solución avanzada que detiene ataques en tiempo real, antes de que afecten la operación.

¿Qué hace diferente a un NGFW moderno?

Un firewall de nueva generación no se limita a bloquear puertos. Integra inteligencia, visibilidad y capacidad de respuesta. Algunas características clave:

- **Inspección profunda de paquetes (DPI)** para analizar el contenido completo del tráfico.
- **Prevención de amenazas basada en inteligencia de amenazas** (Threat Intelligence), no solo detección.
- **Segmentación dinámica que** protege diferentes áreas de red según riesgo.
- **Desempeño eficiente aún en tráfico cifrado**, algo crucial en redes modernas.

Un NGFW como los de Check Point combina estos elementos con visibilidad centralizada, automatización y escalabilidad.



Escenarios reales de ataque y cómo un NGFW los detiene

Ataque por ransomware

Un empleado recibe un correo con un archivo malicioso. Un firewall tradicional lo deja pasar. Un NGFW lo envía a un sandbox en la nube donde se detecta el comportamiento malicioso antes de llegar al endpoint.

Dispositivo IoT comprometido

Un sensor de temperatura en la red OT comienza a enviar tráfico inusual. El NGFW detecta este comportamiento anómalo por análisis heurístico y lo bloquea sin afectar al resto de la operación.

Acceso desde ubicación sospechosa

Se intenta iniciar sesión desde un país con alto riesgo cibernético. El NGFW con geolocalización, reputación IP y políticas Zero Trust, bloquea automáticamente la conexión.

Beneficios tangibles para operaciones e IT

- Reducción en el tiempo de respuesta ante incidentes.
- Menos presión sobre el equipo de TI gracias a procesos automáticos.
- Mayor visibilidad, incluso del tráfico cifrado y de las aplicaciones en uso.
- Facilidad para cumplir con normativas como ISO 27001, CTPAT, NIST.
- Seguridad unificada para redes físicas, virtuales y en la nube.

Datos Claves

Las organizaciones que implementan un NGFW Moderno

94%

EDUCEN EL TIEMPO DE DETECCIÓN DE AMENAZAS A MENOS DE 24 HORAS

Las empresas de manufactura que no tenían un NGFW moderno

82%

SUFRIERON UN ATAQUE RANSOMWARE

Check Point bloquea más de

86 MIL MILLONES

AL DÍA MEDIANTE SU MOTOR DE THREATCLOUD

¿Por qué importa la inteligencia de amenazas en tiempo real?

Los ataques no esperan. Un NGFW moderno trabaja con fuentes actualizadas de amenazas globales (como ThreatCloud en el caso de Check Point), permitiendo bloquear vectores de ataque antes de que sean conocidos masivamente. Esta capacidad predictiva marca la diferencia entre prevenir o lamentar.

Casos de uso por industria

- **Logística y transporte:** Protección de CEDIS, flotillas conectadas y control de acceso remoto.
- **Manufactura:** Defensa de redes OT/IT sin detener la operación.
- **Retail y servicios:** Administración centralizada para múltiples sucursales.
- **Energía y puertos:** Segmentación crítica y cumplimiento con regulaciones internacionales.

Conclusión

Invertir en un NGFW moderno no es solo una mejora técnica: **es una estrategia de continuidad operativa y protección reputacional**. La ciberseguridad ya no es opcional; es el núcleo de una operación eficiente, conectada y confiable.

¿Quieres conocer cómo está tu red?

Solicita **una evaluación de seguridad** con nuestro equipo de ingenieros en Proyectos CSI. Analizamos tu infraestructura, detectamos vulnerabilidades y te ayudamos a tomar decisiones con base técnica.



Escríbenos a ingenieria@Proyectoscsi.mx

Llámanos al 33 4170 8104

Visítanos en <https://proyectoscsi.mx>

Infórmate en blog.proyectoscsi.mx