Todo Firewall .com

¿Cómo seleccionar un Firewall de Nueva Generación (NGFW) para su empresa?

Guía técnica para un dimensionamiento correcto y una implementación exitosa que garantice seguridad, rendimiento y escalabilidad en su infraestructura de red.

PASO 1

Definición del escenario operativo

Antes de seleccionar un NGFW, es fundamental definir con precisión el contexto técnico donde será implementado. Un análisis detallado del entorno operativo permite identificar los requisitos reales de seguridad y rendimiento.

Variables clave a relevar

- Cantidad total de usuarios concurrentes y patrones de uso
- Dispositivos por usuario: PC, móviles, IoT y endpoints
- Sucursales o sitios remotos que requieren conectividad
- Accesos VPN (site-to-site y client VPN)
- Aplicaciones críticas: ERP, CRM, VoIP, servicios cloud
- Requerimientos de alta disponibilidad y continuidad

Punto crítico

Un dimensionamiento incorrecto impacta directamente en rendimiento, estabilidad y seguridad. Es esencial realizar un relevamiento exhaustivo antes de cualquier decisión de compra.

PASO 2

Dimensionamiento por usuarios y dispositivos

El NGFW debe ser capaz de manejar la carga actual y proyectada de su organización. Es fundamental considerar usuarios simultáneos (no totales), el crecimiento proyectado para los próximos 12–36 meses, la proporción entre tráfico interno y tráfico hacia Internet, así como los accesos remotos en modalidad de trabajo híbrido.

Usuarios Simultáneos

Calcular basándose en picos de uso real, no en el total de empleados

Crecimiento Proyectado

Planificar expansión de 12 a 36 meses con margen del 30-40%

Modalidades de Trabajo

Considerar accesos remotos, VPN y entornos híbridos

Regla práctica: Dimensionar siempre con margen de crecimiento mínimo del 30–40% para evitar obsolescencia prematura.

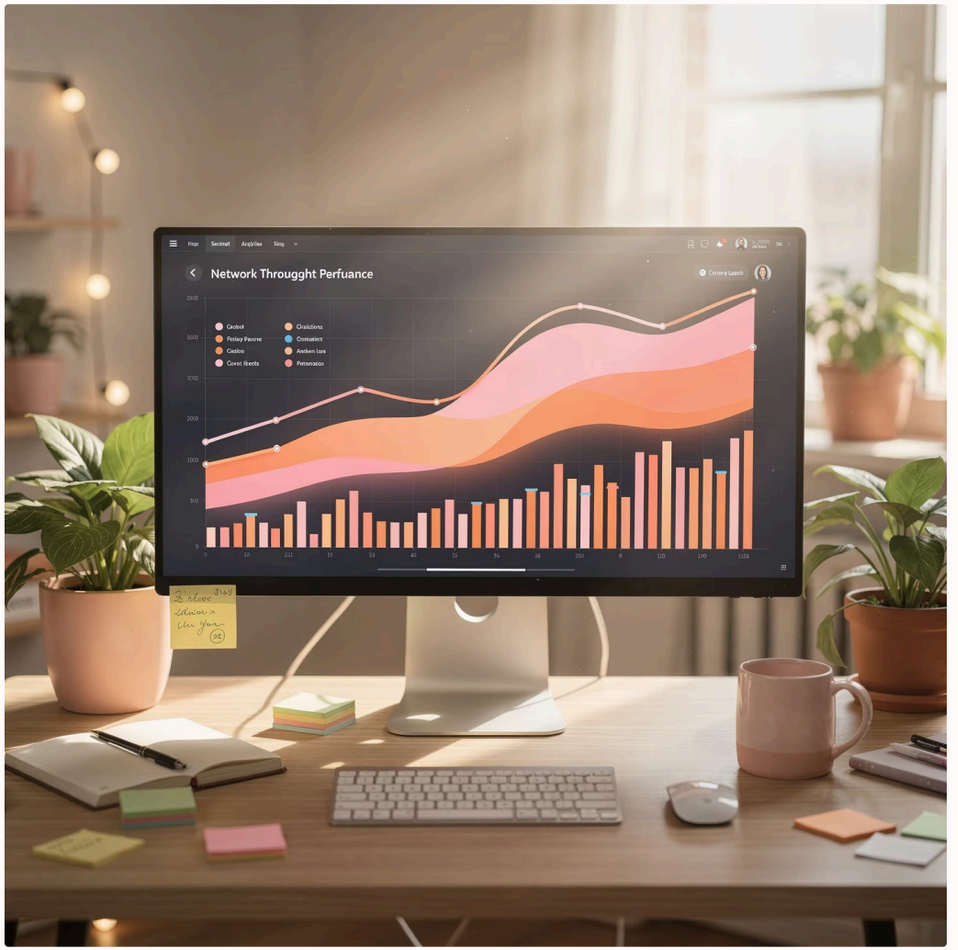
PASO 3

Análisis de tráfico y throughput real

No basta con evaluar el throughput nominal que proporcionan los fabricantes en sus especificaciones técnicas. La realidad operativa es significativamente diferente cuando todas las funciones de seguridad están activas.

Factores críticos a considerar

- Throughput con todas las funciones de seguridad activas simultáneamente
- Inspección SSL/TLS habilitada en todo el tráfico
- Predominancia de tráfico cifrado en la actualidad
- Conexiones concurrentes máximas soportadas
- Sessions per second (SPS) en condiciones reales



Dato importante: El throughput real suele ser 30–60% menor al teórico sin inspección. Siempre solicite pruebas con todas las funciones activas.

PASO 4

Inspección profunda y carga de procesamiento

Las funciones avanzadas de un NGFW consumen recursos significativos de CPU y memoria. Es fundamental comprender el impacto de cada función de seguridad en el rendimiento global del sistema.

Deep Packet Inspection (DPI)

Análisis profundo del contenido de cada paquete en tiempo real

IPS en Modo Prevención

Sistema de prevención de intrusiones activo bloqueando amenazas

Antivirus en Flujo

Detección de malware en tráfico de red en tiempo real

Control de Aplicaciones

Identificación y gestión granular de aplicaciones empresariales

Filtrado Web

Categorización y bloqueo de contenido web por políticas

Sandboxing

Análisis de archivos sospechosos en entorno aislado

Verificar: Capacidad del hardware, aceleración por ASIC/NP y el impacto específico de SSL Inspection en el rendimiento.

PASO 5

Tráfico cifrado y SSL Inspection

Desafío actual

Más del 80% del tráfico actual en redes empresariales está cifrado mediante SSL/TLS. Sin capacidad de inspección, el firewall opera prácticamente a ciegas ante amenazas ocultas en conexiones cifradas.

Capacidades necesarias

- SSL Inspection para tráfico inbound y outbound
- Políticas diferenciadas por usuario y aplicación
- Exclusiones configurables para privacidad y compliance
- Gestión segura de certificados y PKI
- Rendimiento sostenido con inspección activa

Punto crítico: SSL Inspection es uno de los principales puntos de fallo en equipos subdimensionados. Verificar rendimiento real con esta función habilitada.

PASO 6

VPN y conectividad segura remota

Túneles Site-to-Site

Cantidad de túneles IPsec necesarios entre oficinas y datacenter

VPN SSL Concurrente

Usuarios remotos simultáneos con acceso VPN cliente

Throughput VPN Real

Rendimiento efectivo con cifrado y tráfico productivo simultáneo

Autenticación Robusta

Integración con LDAP, Active Directory y MFA para Zero Trust

El rendimiento VPN debe medirse en simultáneo con tráfico productivo, no en condiciones de laboratorio aisladas.

PASO 7

Alta disponibilidad y arquitectura resiliente

Para entornos críticos donde la continuidad operativa es esencial, la alta disponibilidad no es opcional. Una arquitectura resiliente garantiza que las operaciones continúen sin interrupción ante fallos de hardware o problemas de conectividad.

Configuración en Clúster

Implementación activo/pasivo o activo/activo según necesidades de rendimiento y presupuesto

Sincronización de Sesiones

Estado de conexiones replicado entre nodos para continuidad transparente

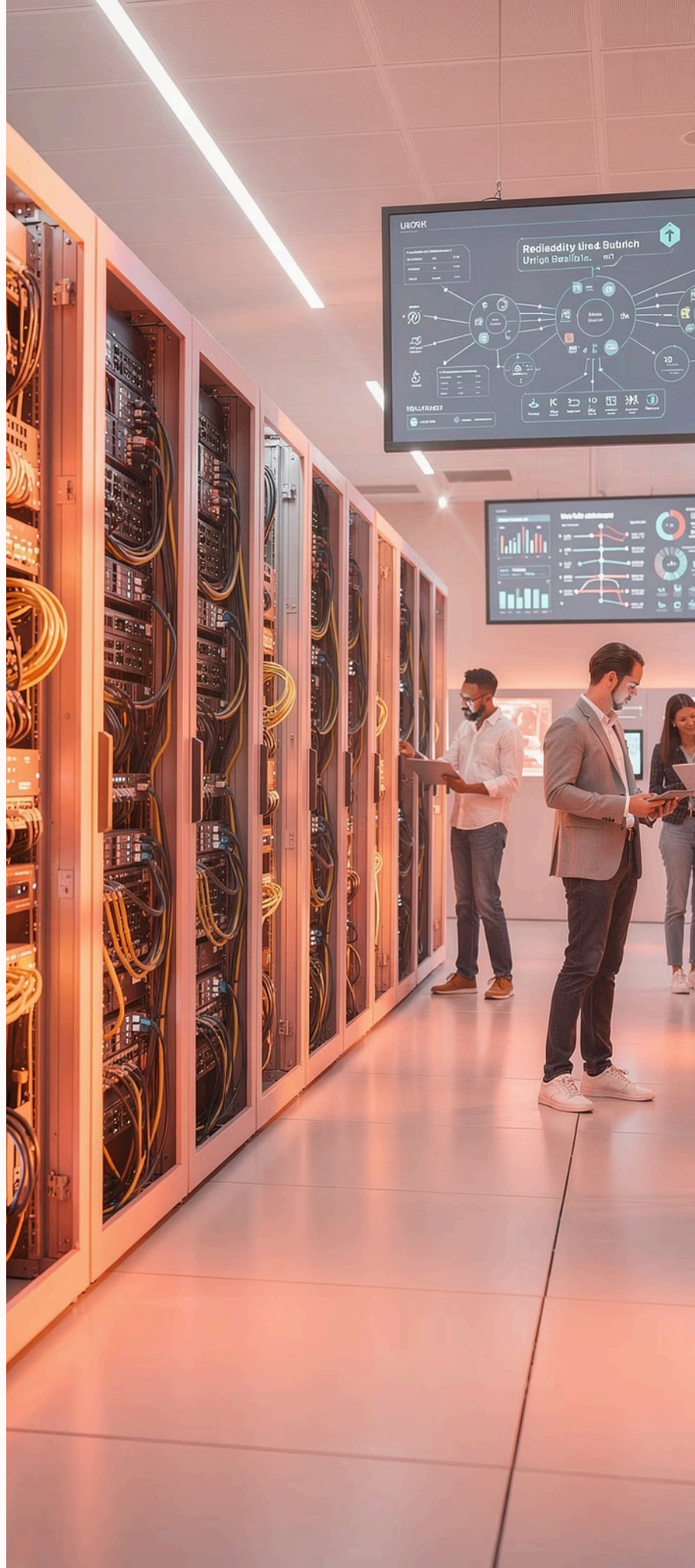
Failover Automático

Conmutación sin pérdida de tráfico ni interrupción de servicios críticos

Redundancia WAN

Múltiples enlaces de salida para garantizar conectividad continua a Internet

La alta disponibilidad impacta directamente en el dimensionamiento final y debe considerarse desde la fase de diseño inicial.

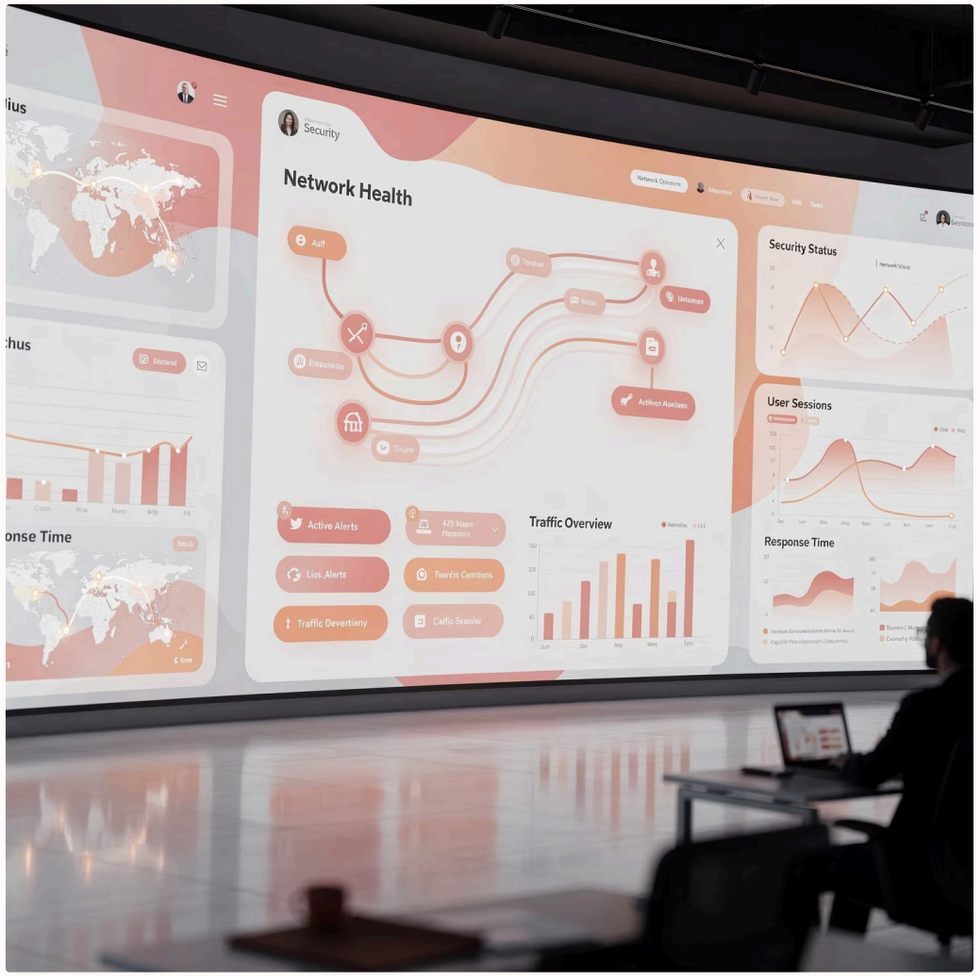


Gestión, monitoreo y visibilidad operativa

Capacidades esenciales de gestión

Un NGFW empresarial debe proporcionar visibilidad completa y herramientas de gestión centralizadas que faciliten la operación y el mantenimiento.

- Consola centralizada (local o cloud) para gestión unificada
- Logs detallados de todo el tráfico y eventos de seguridad
- Integración nativa con plataformas SIEM
- Sistema de alertas proactivas ante amenazas
- Reportes personalizables de uso, amenazas y compliance
- Dashboard en tiempo real con métricas clave



Considerar: Mayor nivel de log implica mayor consumo de recursos de almacenamiento y procesamiento. Dimensionar adecuadamente.

Selección integral: más allá del hardware

Licenciamiento Completo

IPS, antivirus, filtrado web, control de apps, cloud management y reporting. Un hardware potente sin licencias activas no es un NGFW completo.

Escalabilidad Futura

Capacidad de upgrade de licencias, soporte de nuevas versiones, integración cloud (AWS, Azure, M365) y roadmap tecnológico del fabricante.

Arquitectura Integral

Pensar el firewall como plataforma de seguridad, no como equipo aislado. Considerar integración SD-WAN y evolución hacia SASE.

La selección de un NGFW no es solo una compra, es una decisión de arquitectura

En TodoFirewall ayudamos a relevar su escenario real, dimensionar correctamente, seleccionar la tecnología adecuada e implementar y mantener su NGFW para garantizar seguridad, rendimiento y ROI a largo plazo.

Solicitar consultoría **Más información**