Forcepoint Next Generation Firewall (NGFW)

La SD-WAN empresarial se une al número 1 de la seguridad de redes

Forcepoint NGFW es un firewall de última generación que combina redes rápidas y flexibles (SD-WAN y LAN) con seguridad líder en la industria para conectar y proteger a las personas y los datos que utilizan mediante redes empresariales diversas y en evolución. Forcepoint NGFW brinda seguridad, desempeño y operaciones coherentes en sistemas físicos, virtuales y en la nube. Está diseñado desde cero para ofrecer una alta disponibilidad y escalabilidad, así como administración centralizada con visibilidad completa de 360°.

Conectividad SD-WAN siempre disponible para empresas

Las empresas de hoy exigen soluciones de seguridad de redes totalmente resilientes. Forcepoint NGFW incorpora escalabilidad y disponibilidad altas en todos los niveles:

- **Agrupamiento (clustering) mixto activo-activo.** Se pueden agrupar hasta 16 nodos de distintos modelos ejecutando distintas versiones. Esto brinda un desempeño y una resiliencia de redes superior, y posibilita la seguridad, como la inspección profunda de paquetes y VPN.
- **Actualizaciones de software y de políticas sin complicaciones.** La disponibilidad líder de la industria de Forcepoint permite que las actualizaciones de políticas (e incluso las de software) se trasladen de manera fluida a un clúster sin interrumpir el servicio.
- **Agrupamiento (clustering) de redes SD-WAN.** Amplía la cobertura de alta disponibilidad a las conexiones de red y VPN. Combina la seguridad ininterrumpida con la capacidad de sacar ventaja de las conexiones de banda ancha locales a fin de complementar o reemplazar líneas rentadas costosas, como las de MPLS.

Los clientes que se cambian a Forcepoint NGFW informan una disminución del 86 % en ataques cibernéticos, un 53 % menos de carga sobre el departamento de TI y una reducción del 70 % en el tiempo de mantenimiento.*

Sígale el ritmo a las necesidades de seguridad cambiantes

Un software central unificado a través del cual Forcepoint NGFW desempeña diversos roles de seguridad, desde firewall/VPN a sistema de prevención de intrusiones (IPS) a firewall de capa 2, en entornos empresariales dinámicos. Los firewall Forcepoint NGFW pueden desplegarse de diversas formas (p. ej., dispositivos físicos, virtuales, en la nube) y todos se administran desde una sola consola.

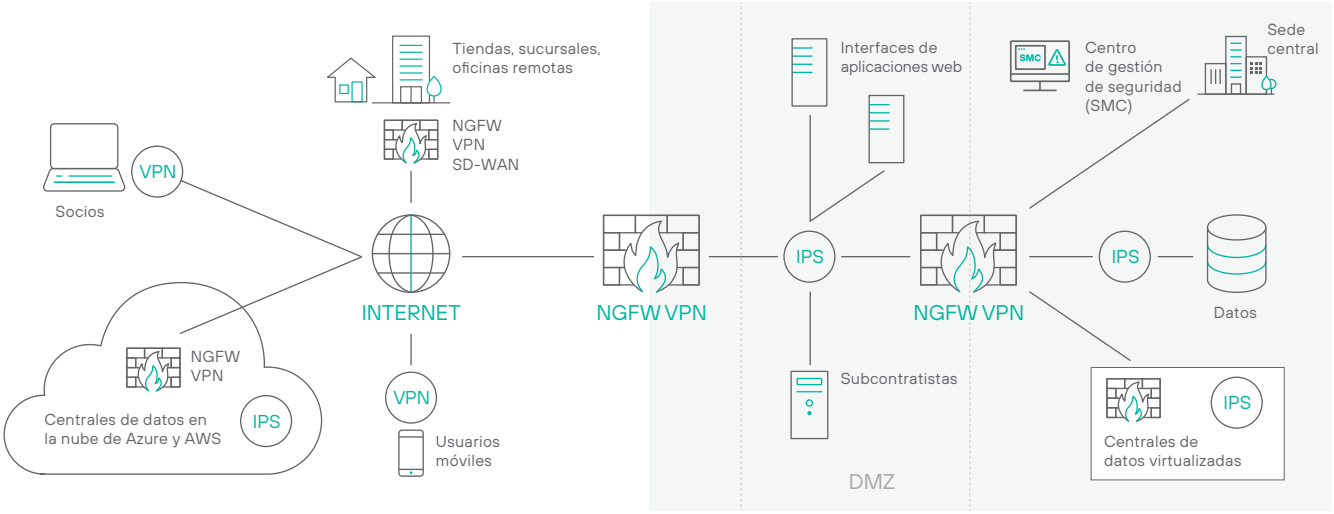
Forcepoint personaliza de manera única el control de acceso y la inspección profunda a cada conexión para brindar desempeño y seguridad superiores. Combina control granular de aplicaciones, defensas de sistema de prevención de intrusiones (IPS), control de red privada virtual (VPN) incorporado y proxies de aplicaciones de misión crítica en un diseño eficaz, ampliable y sumamente escalable. Nuestras tecnologías antievasión poderosas decodifican y normalizan el tráfico de la red antes de la inspección y a través de todas las capas de protocolos para exponer y bloquear los métodos de ataque más avanzados.

Bloquee ataques de fuga de datos sofisticados

Las fugas de datos grandes siguen afectando a las empresas y organizaciones en todas las industrias. Ahora puede contraatacar con protección contra la exfiltración en la capa de las aplicaciones. Los firewall Forcepoint NGFW colocan el tráfico de la red que se origina de aplicaciones específicas en computadoras de escritorio y portátiles, servidores, sistemas de intercambio de archivos y otros dispositivos finales en una lista blanca o una lista negra de manera selectiva y automática basándose en datos contextuales de los dispositivos finales altamente granulares. Van más allá que los firewalls típicos para evitar los intentos de exfiltración de datos confidenciales de los dispositivos finales mediante canales de comunicación, usuarios, aplicaciones web y programas no autorizados.

* "Cuantificación de los resultados operativos y de seguridad al pasar a Forcepoint NGFW", R. Ayoub y M. Marden, IDC Research, mayo de 2017.

Una plataforma con muchas opciones de despliegue, todo administrado desde una sola consola



Protección sin igual

Los atacantes se convirtieron en expertos en penetrar dispositivos finales, centrales de datos, aplicaciones y redes empresariales. Una vez que acceden, roban propiedad intelectual, información de clientes y otros datos confidenciales, lo que causa daños irreparables a las empresas y su reputación.

Las nuevas técnicas de ataque pueden evadir la detección de dispositivos de seguridad de redes tradicionales, lo que incluye muchos firewalls de marcas reconocidas, más allá de la simple transmisión de explotaciones de vulnerabilidades.

Las evasiones funcionan a distintos niveles para camuflar las vulnerabilidades y el malware, haciendo que pasen inadvertidas para la inspección de paquetes basada en firmas tradicional. Gracias a las evasiones, incluso pueden volverse a empaquetar ataques antiguos que habían sido bloqueados durante años para comprometer a los sistemas internos.

Forcepoint NGFW adopta un enfoque diferente. Nuestro motor de seguridad líder en la industria está diseñado para las tres etapas de la defensa de redes: combatir evasiones, detectar vulnerabilidades y detener malware. Puede desplegarse de forma transparente detrás de firewalls existentes para añadir protección sin causar interrupciones, o como un NGFW de capacidades completas para una seguridad todo en uno.

Además, Forcepoint NGFW brinda descifrado rápido de tráfico cifrado, lo que incluye conexiones web de HTTPS, combinado con controles de privacidad granulares que mantienen a su empresa y sus usuarios seguros en un mundo que cambia rápidamente. Incluso puede limitar el acceso desde aplicaciones de dispositivo final específicas para bloquear dispositivos o evitar el uso de software vulnerable.

Resultados comerciales

- → Implementación más rápida de sucursales, nubes o centrales de datos
- → Menos tiempo de inactividad
- → Mayor seguridad sin interrupciones
- → Menos fugas
- → Menor exposición a nuevas vulnerabilidades mientras los equipos de TI se preparan para desplegar nuevos parches
- → Menor costo total de propiedad (TCO) para la seguridad e infraestructura de redes

Características clave

- → Conectividad de SD-WAN a escala empresarial
- → IPS integrado en defensas antievasión
- → Agrupamiento (clustering) de dispositivos y redes de alta disponibilidad
- → Actualizaciones automáticas con cero tiempo de inactividad
- → Administración centralizada impulsada por políticas
- → Visibilidad 360° interactiva y accionable
- → Proxies de seguridad Sidewinder para aplicaciones de misión crítica
- → Contexto de usuarios y dispositivos finales centrado en las personas
- → Descifrado de alto desempeño con controles de privacidad granulares
- → Uso de listas blancas/listas negras según la aplicación del cliente y versión
- → Integración de CASB y seguridad web
- → Entornos seguros antimalware
- → Software unificado para despliegues físicos, de AWS, Azure, VMware

Especificaciones de Forcepoint Next Generation Firewall (NGFW)

PLATAFORMAS	
Dispositivo físico	Múltiples opciones de dispositivos de hardware, que van desde instalaciones en sucursales a centrales de datos
Infraestructura en la nube	Amazon Web Services, Microsoft Azure, Google, Oracle, IBM
Dispositivo virtual	Sistemas x86 de 64 bits; VMware ESXi, VMware NSX, Microsoft Hyper-V, KVM y Nutanix AHV
Dispositivo final	Agente de contexto de dispositivo final (ECA), cliente VPN
Contextos virtuales	Hasta 250
Administración centralizada	Sistema de administración centralizada a nivel empresarial con capacidades de análisis de registro, monitoreo y generación de informes *Consulte la hoja de datos de Forcepoint Security Management Center para obtener más información.*
CARACTERÍSTICAS DEL FIREWALL	
Inspección profunda de paquetes	Normalización del tráfico multicapa/Inspección profunda de todo el flujo, defensa antievasión, contexto dinámico Detección, inspección/manejo del tráfico específico según el protocolo, descifrado granular del tráfico SSL/TLS (tanto TLS 1.2 y 1.3), detección de explotación de vulnerabilidades, localización (fingerprinting) personalizada, reconocimiento, defensa contra red bot, correlación, registro del tráfico, protección contra DoS/DDoS, métodos de bloqueo, actualizaciones automáticas
Identificación de usuarios	Base de datos de usuarios interna, LDAP nativo, Microsoft Active Directory, RADIUS, TACACS+, Microsoft Exchange, certificados de clientes
Alta disponibilidad	› Agrupamiento (clustering) de firewall activo-activo/activo-en espera de hasta 16 nodos › SD-WAN › Conmutación por error con estado (incluye conexiones de VPN) › Equilibrio de carga de servidor › Agregado de enlaces (802.3ad) › Detección de falla de enlace
Asignación de dirección IP	› IPv4 estática, DHCP, PPPoA, PPPoE, IPv6 estática, SLAAC, DHCPv6 › Servicios: Servidor DHCP para IPv4 y retransmisión DHCP para IPv4 e IPv6
Enrutamiento	› Rutas IPv4 e IPv6 estáticas, enrutamiento basado en políticas, enrutamiento multidifusión estático › Enrutamiento dinámico: RIPv2, RIPng, OSPFv2, OSPFv3, BGP, MP-BGP, BFD, PIM-SM, PIM-SSM, proxy IGMP › Enrutamiento en función de las aplicaciones
IPv6	IPv4/IPv6 de doble pila, NAT64, ICMPv6, DNSv6, NAT, funciones completas de NGFW
Redireccionamiento de proxy	Redireccionamiento de protocolos HTTP, HTTPS, FTP, SMTP a Forcepoint o servicio de inspección del contenido (CIS) de terceros en las instalaciones o en la nube
Protección geográfica	País o continente de origen/destino actualizado dinámicamente
Lista Dirección IP	Categorías IP predefinidas o uso de listas de direcciones IP personalizadas o importadas
Filtrado de URL (Suscripción aparte)	Listas de URL personalizadas o importadas
Aplicaciones de dispositivos finales	Nombre y versión de la aplicación
Aplicaciones de red	Más de 7400 aplicaciones de red y en la nube
Proxies de seguridad Sidewinder	TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS

SD-WAN	
Protocolos	IPsec y TLS
VPN de sitio a sitio	› VPN basada en políticas y rutas › Topologías radiales, de malla completa, de malla parcial e híbridas › Selección dinámica de varios enlaces de ISP › Intercambio de cargas, activo/en espera, agregado de enlaces › Monitoreo en vivo y generación de informes sobre la calidad de los enlaces de los ISP (retrasos, vibración, pérdida de paquetes)
Acceso remoto	› Cliente Forcepoint VPN para Microsoft Windows, Android y Mac OS › Cualquier cliente IPsec estándar › Alta disponibilidad con conmutación por error automática › Verificaciones de seguridad del cliente › Acceso al portal VPN de TLS
DETECCIÓN DE MALWARE AVANZADO Y CONTROL DE ARCHIVOS	
Protocolos	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
Filtrado de archivos	Filtrado de archivos basado en políticas con proceso de selección eficiente. Más de 200 tipos de archivos admitidos en 19 categorías de archivos
Reputación de archivos	Verificación y bloqueo de reputación de malware basado en la nube de alta velocidad
Antivirus	Motor de detección de antivirus local*
Entornos seguros de día cero	Forcepoint Advanced Malware Detection está disponible como servicio en las instalaciones y en la nube

* La examinación antimalware local no está disponible con los dispositivos de 110/115.