Forcepoint

Datasheet

Next Generation Firewall

Seguridad de Redes empresariales con capacidades de SD-WAN nativas

Beneficios clave

Conectividad SD-WAN siempre activa para empresas

Las empresas de hoy exigen soluciones de seguridad de redes totalmente resilientes. Forcepoint Next-Gen Firewall (NGFW) incorpora una alta escalabilidad y disponibilidad en todos los niveles.

- **Agrupación mixta activa-activa:** Se pueden agrupar hasta 16 nodos de diferentes modelos que ejecutan diferentes versiones. Esto proporciona un rendimiento y una resiliencia de red superiores, y permite la seguridad, como la inspección profunda de paquetes y las VPN.
- **Actualizaciones de políticas y software sin interrupciones:** La disponibilidad líder en el sector de Forcepoint permite que las actualizaciones de políticas (e incluso las actualizaciones de software) se envíen sin problemas a un clúster sin interrumpir el servicio.
- **Agrupación de redes de SD-WAN:** Amplía la cobertura de alta disponibilidad a las conexiones de red y VPN. Combina la seguridad continua con la capacidad de aprovechar las conexiones de banda ancha locales para complementar o reemplazar costosas líneas arrendadas como MPLS.

Forcepoint Next-Gen Firewall proporciona seguridad de red líder en el sector con conectividad SD-WAN rápida y flexible para conectar y proteger a las personas y los datos que utilizan en redes empresariales diversas y en evolución. Forcepoint NGFW ofrece seguridad, rendimiento y operaciones consistentes en sistemas físicos, virtuales y en la nube. Está diseñado desde cero para una alta disponibilidad y escalabilidad, junto con una administración centralizada y una visibilidad total de 360°.

Los clientes que se cambian a Forcepoint NGFW reportan una caída del 86 % en los ataques cibernéticos, un 53 % menos de carga de TI y un 70 % menos de tiempo de mantenimiento.*

Sígale el ritmo a las necesidades de seguridad cambiantes

Un núcleo de software unificado permite a Forcepoint manejar múltiples roles de seguridad, desde firewall/VPN y ZTNA Application Connector hasta el Sistema de Prevención de Intrusiones (IPS) y el firewall de capa 2, en entornos empresariales dinámicos. Forcepoint se puede implementar de diversas maneras (por ejemplo, dispositivos físicos, virtuales y en la nube), todo administrado desde una única consola.

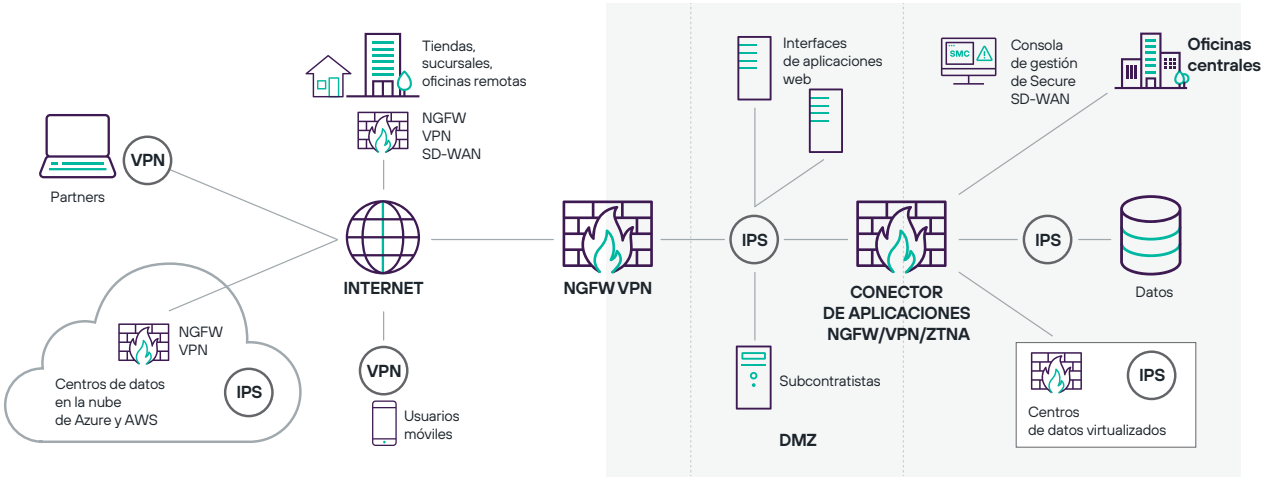
Forcepoint adapta de forma única el control de acceso y la inspección profunda para cada conexión para proporcionar un alto rendimiento y seguridad. Combina el control granular de aplicaciones, las defensas de IPS, el control integrado de redes privadas virtuales (VPN) y los proxies de aplicaciones de misión crítica en un diseño eficiente, extensible y altamente escalable. Nuestras poderosas tecnologías antievasión decodifican y normalizan el tráfico de red antes de la inspección y en todas las capas de protocolos para exponer y bloquear los métodos de ataque más avanzados.

Bloquee ataques de fuga de datos sofisticados

Grandes fugas de datos todavía afectan a empresas y organizaciones de todas las industrias. Combata esta amenaza con la protección contra la exfiltración en la capa de aplicación. Forcepoint permite o bloquea de forma selectiva y automática el tráfico de red que se origina en aplicaciones específicas en PC, computadoras portátiles, servidores, recursos compartidos y otros dispositivos de endpoint en función de datos contextuales de endpoint altamente granulares. Va más allá de los firewalls típicos para evitar los intentos de exfiltración de datos confidenciales de los endpoints a través de programas no autorizados, aplicaciones web, usuarios y canales de comunicación.

* "Quantifying the Operational and Security Results of Switching to Forcepoint NGFW", R. Ayoub & 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 han convertido en expertos en penetrar en redes, aplicaciones, centros de datos y endpoints empresariales. Una vez dentro, roban propiedad intelectual, información de los clientes y otros datos confidenciales, lo que causa daños irreparables a las empresas y a sus respectivas reputaciones.

Las nuevas técnicas de ataque pueden evadir la detección por parte de los dispositivos de red de seguridad tradicionales, incluidos muchos firewalls de marca, yendo más allá de la simple transmisión de vulnerabilidades.

Las evasiones funcionan en múltiples niveles para camuflar las explotaciones y el malware, haciéndolos invisibles a la inspección tradicional de paquetes basada en firmas. Incluso los ataques que han estado bloqueados durante años pueden reempaquetarse con evasiones para comprometer los sistemas internos.

Forcepoint tiene un enfoque diferente. Nuestro motor de seguridad líder en el sector está diseñado para las tres etapas de la defensa de la red: para derrotar las evasiones, detectar la explotación de vulnerabilidades y detener el malware. Se puede implementar de forma transparente detrás de firewalls existentes para agregar protección sin interrupciones, o como un firewall corporativo, con todas las funciones para una seguridad todo en uno.

Además, Forcepoint proporciona un rápido descifrado del tráfico cifrado, incluidas las conexiones web HTTPS, combinado con controles de privacidad granulares que mantienen su empresa y sus usuarios seguros en un mundo que cambia rápidamente. Incluso puede limitar el acceso desde aplicaciones específicas de endpoint para bloquear dispositivos o evitar el uso de software vulnerable.

Resultados comerciales

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

Funcionalidades clave

- → Conectividad de SD-WAN a escala empresarial
- → Integración de SASE/SSE para la web, la nube y la seguridad de aplicaciones privadas
- → IPS integrado en defensas de evasión
- → Agrupamiento 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 de Sidewinder para aplicaciones de misión crítica
- → Contexto del usuario y del endpoint
- → Descifrado de alto rendimiento con controles de privacidad granulares
- → Permitir/bloquear por aplicación y versión del cliente
- → Monitoreo de la salud del sistema
- → Integración de CASB y seguridad web
- → Entornos seguros antimalware
- → Software unificado para implementaciones físicas,, AWS, Azure, y VMware
- → Menos exposición a nuevas vulnerabilidades mientras los equipos de TI se preparan para implementar nuevos parches
- → Menor costo total de propiedad (TCO) para la seguridad e infraestructura de redes

Especificaciones de Forcepoint NGFW

PLATAFORMAS	
Dispositivo físico	Múltiples opciones de equipos de hardware, desde instalaciones en sucursales hasta centros de datos
Infraestructura en la nube	Amazon Web Services, Microsoft Azure, Google, Oracle, IBM
Equipo virtual	Sistemas basados en x86 64-bit; VMware ESXi, VMware NSX, Microsoft Hyper-V, KVM y Nutanix AHV
Endpoint	Agente de contexto de endpoint (ECA), cliente VPN
Contextos virtuales	Hasta 250
Administración centralizada	Sistema de administración centralizada de nivel empresarial con capacidades de análisis de registros, monitoreo y elaboración 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 de múltiples capas e inspección profunda de flujo completo, defensa de evasión, detección de contextos dinámicos, gestión e inspección del tráfico específicos del protocolo, descifrado granular del tráfico SSL y TLS (TLS 1.2 y 1.3), detección de vulnerabilidades, impresión digital personalizada, reconocimiento, anti-botnet, correlación, registro del tráfico, protección DoS y DDoS, métodos de bloqueo, actualizaciones automáticas
Identificación de usuarios	Base de datos interna de usuarios, LDAP nativa, Microsoft Active Directory, RADIUS, TACACS+, Microsoft Exchange, certificados de cliente
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 › Agregación 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 relé 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, IGMP proxy › Enrutamiento en función de las aplicaciones
IPv6	IPv4/IPv6 de doble pila, NAT 44, NAT64, NAT66, ICMPv6, DNSv6, NAT, funciones completas de NGFW
Redireccionamiento de proxy	Redireccionamiento de protocolos HTTP, HTTPS, FTP, SMTP a Forcepoint o al servicio de inspección de contenido de terceros (CIS) en las instalaciones y en la nube
Protección geográfica	País o continente de origen/destino actualizado dinámicamente
Lista de direcciones IP	Categorías IP predefinidas o uso de listas de direcciones IP personalizadas o importadas
Filtrado de URL (Suscripción Separada)	Listas de URL personalizadas o importadas; admite QUIC y HTTP/3
Aplicaciones de endpoint:	nombre y versión de la aplicación
Aplicaciones de red	Más de 7400 aplicaciones de red y en la nube
Sidewinder Security Proxies	TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS

INTEGRACIÓN CON SASE	
Reenvío de tráfico web	Tunelización de GRE e IPsec a plataformas de Security Service Edge (SSE), como Forcepoint ONE
ZTNA Application Connector	Permite que las aplicaciones privadas en centros de datos internos se conecten a Zero Trust de Forcepoint ONE

SD-WAN	
Protocolos	IPsec y TLS
Site-to-Site VPN	› 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 ISP (retrasos, fluctuación de latencia, 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 un eficiente proceso de reducción de opciones 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*
Sandboxing de día cero	FForcepoint Advanced Malware Detection and Protection disponible como servicio en la nube y en las instalaciones

* El análisis antimalware local no está disponible con dispositivos 110/115.