Prevención de intrusiones con Forcepoint Next-Gen Firewall

Forcepoint ofrece uno de los mejores sistemas de prevención de intrusiones (IPS) de la industria para proteger a las redes empresariales distribuidas en centrales de datos, oficinas, sucursales y en la nube.

Las soluciones de seguridad de redes de Forcepoint ofrecen uno de los sistemas de prevención de intrusiones más seguros de la industria. Con resultados de máximo nivel en pruebas independientes, Forcepoint Next-Gen Firewall puede desplegarse como un dispositivo IPS de capa 2 independiente o como parte de un firewall de última generación de capa 3 de capacidades completas en entornos físicos, virtuales y en la nube. Combate evasiones, vulnerabilidades y malware que los atacantes utilizan para penetrar y diseminarse por las redes empresariales.

Arquitectura única en términos de eficacia y velocidad

Forcepoint Next-Gen Firewall emplea un enfoque dinámico basado en el flujo para los procesos de inspección que va más allá de la mera inspección de paquetes. Reconstruye y analiza las cargas reales, combatiendo las técnicas de evasión que camuflan las vulnerabilidades y el malware.

Además, el descifrado granular de alta velocidad revela los ataques ocultos del tráfico SSL/TLS. Forcepoint analiza el flujo de cada carga, decodificando las distintas capas de protocolos para detectar anomalías o formatos incorrectos en configuraciones de protocolos, metadatos y encabezados.

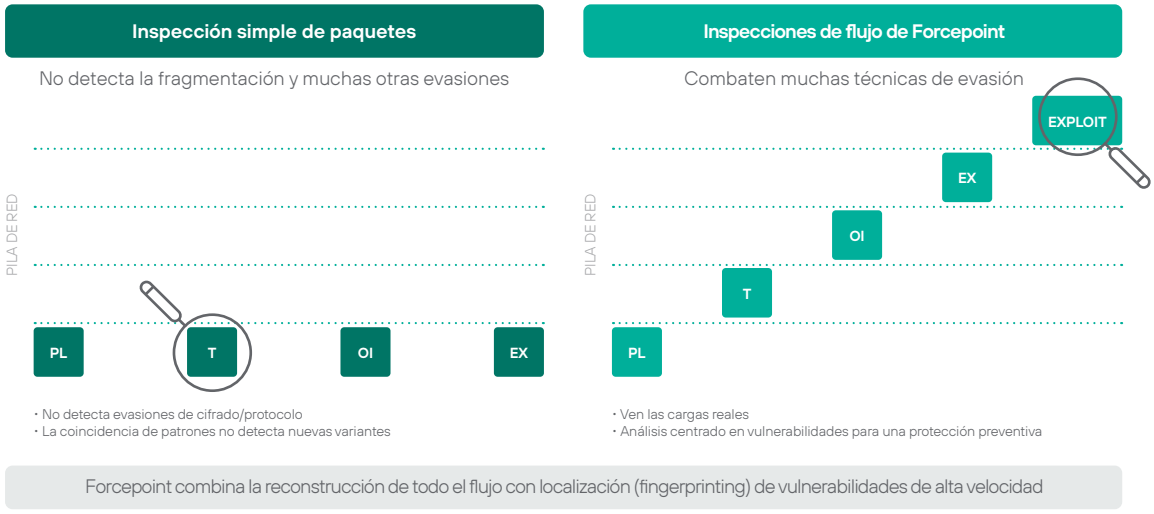
Forcepoint luego aplica técnicas avanzadas para examinar el contenido de las transmisiones a fin de detectar vulnerabilidades en diversos tipos de sistemas. A diferencia de los mecanismos basados en firmas con patrones detallados, el enfoque más sofisticado de Forcepoint permite identificar estos ataques con una única huella digital concisa. Se busca la coincidencia de estas huellas digitales por medio de un autómata finito determinista (DFA) de alta velocidad adaptado al contexto de cada protocolo, a fin de incorporar nuevas huellas prácticamente sin impacto en los recursos de la CPU.

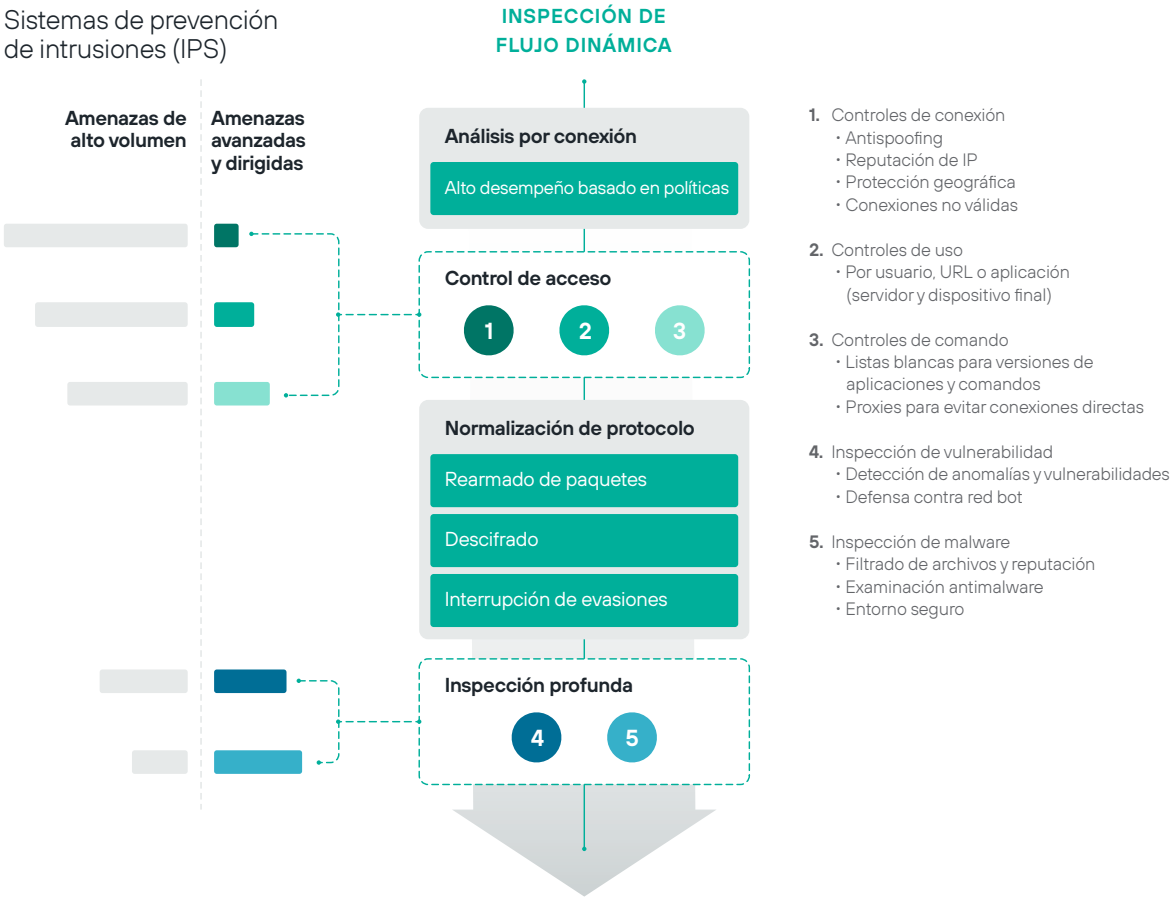
Actualizaciones continuas para mantenerse a la delantera de los atacantes

El equipo de investigación global de Forcepoint estudia constantemente fuentes de inteligencia sobre amenazas, informes de vulnerabilidad de diversos orígenes y distintos sistemas de prueba para analizar las explotaciones y vulnerabilidades. Se publican nuevas huellas digitales según resulte necesario por medio de nuestro servicio en la nube, y se descargan automáticamente a través de los sistemas de seguridad de redes de Forcepoint. Este enfoque proactivo brinda a los equipos de TI tiempo para estudiar los nuevos parches que se publican e implementar esfuerzos de corrección sin temor a sufrir un compromiso inmediato.

No más amenazas de día cero y contenido no deseado

Los productos de seguridad de redes de Forcepoint también ofrecen múltiples capas de defensa contra ataques previamente desconocidos y contenido no deseado. Los archivos que se transmiten son sometidos a un análisis de reputación y malware riguroso, y es posible detectar las nuevas amenazas, como los ataques de día cero, con nuestra tecnología de entorno seguro de avanzada. Forcepoint es una de las empresas pioneras en la categorización y el filtrado de sitios web y contenido. Gracias a nuestros dispositivos IPS y firewalls, resulta más sencillo para las organizaciones cumplir las reglamentaciones que afectan el lugar de trabajo, limitar la exposición de los datos personales y evitar que los usuarios ingresen a sitios web con contenido peligroso en primer lugar.





Resiliencia de falla de apertura

Los dispositivos de Forcepoint admiten diversas tarjetas de red modulares, incluso interfaces de falla de apertura que mantienen el tráfico en movimiento incluso cuando el firewall de última generación pierde potencia.

Protección que mantiene a su organización en funcionamiento

Cada día, los atacantes mejoran sus tácticas para penetrar dispositivos finales, centrales de datos, aplicaciones y redes empresariales. Una vez que acceden, pueden robar propiedad intelectual, información de clientes y otros datos confidenciales, lo que causa daños irreparables a su confianza y reputación.

Los ataques a través de Internet van más allá de la simple transmisión de explotaciones de vulnerabilidades. Cada vez más, se emplean nuevas técnicas para evadir la detección por medio de dispositivos de seguridad de redes tradicionales, incluso muchos firewalls de marcas reconocidas.

Estas 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 utilizar repentinamente ataques antiguos que habían sido bloqueados durante años para comprometer a los sistemas internos.

Forcepoint adopta un enfoque diferente. Nuestro motor de IPS 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 parte de nuestro Next-Gen Firewall de capacidades completas para una seguridad todo en uno.

Todos los productos de seguridad de redes de Forcepoint se actualizan constantemente, se administran de manera central y permiten compartir con fluidez políticas de seguridad y paneles en toda la red. Con Forcepoint, podrá proteger a su organización, de manera confiable, constante y eficiente, en todas sus centrales de datos, redes de oficina, sucursales o entornos de red.

Resultados

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

Características clave

- Despliegue como IPS de capa 2, firewall de última generación de capa 2 o como parte de un firewall de última generación de capa 3
- Sistema de detección de intrusiones (IDS) y sistema de prevención de intrusiones (IPS) combinados que ofrecen protección y defensa
- Inspección de flujos que analiza las cargas reales
- Defensas contra evasiones de vanguardia
- Descifrado de alta velocidad con controles de privacidad granulares
- Detección de uso indebido y anomalías en protocolos
- Detección de explotaciones y malware a través de DFA de alta velocidad
- Detección de denegación de servicio (DoS)
- Defensas antibot
- Entornos seguros de día cero en dispositivos en la nuble o en las instalaciones
- Filtrado de URL líder en la industria
- Interfaces de red de falla de apertura modulares para dispositivos
- Capacidades y desempeño unificado en cada despliegue
- Administración centralizada basada en políticas
- Actualizaciones rápidas sin tiempo de inactividad

Especificaciones de Forcepoint Next-Gen Firewall

PLATAFORMAS ADMITIDAS	
Dispositivos	Múltiples series de dispositivos modulares para el despliegue en centrales de datos, bordes de redes y sucursales
Infraestructura en la nube	Amazon Web Services, Microsoft Azure
Dispositivo virtual	Sistemas x86 de 64 bits; VMware ESXi, VMware NSX, Microsoft Hyper-V y entorno virtualizado con KVM
Modos de despliegue	IPS independiente (capa 2, con módulos de interfaz de falla de apertura opcionales), parte de NGFW (capa 3)
Contexto virtual	Virtualización para separar los contextos lógicos con diferentes interfaces y políticas

INSPECCIÓN	
Normalización del tráfico multicapa / Inspección profunda de todo el flujo	› Reconstruye y analiza las cargas reales para garantizar la integridad de los flujos de datos › Descarta los segmentos de nivel inferior duplicados que podrían llevar a ambigüedades durante el rearmado
Defensas contra evasiones	Detiene fragmentos desordenados, segmentos superpuestos, manipulación de protocolos, ofuscación y trucos de codificación
Detección de contexto dinámico	Protocolo, aplicación, tipo de archivo
Inspección/ manejo del tráfico específico según el protocolo	Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IP-in-IP, encapsulación IPv6, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, MSRPC, datagrama de NetBIOS, OPC Classic, OPC UA, Oracle SQL Net, POP3, POP3S, RSH, RSTP, SIP, SMTP, SSH, SunRPC, NBT, SCCP, SMB, SMB2, SIP, proxy TCP, TFTP, inspección integrada en proxy de seguridad Sidewinder
Descifrado granular del tráfico SSL/TLS	› Descifrado de alto desempeño para flujos de servidores y clientes HTTPS › Controles centrados en políticas para proteger la privacidad de los usuarios y limitar la exposición de las organizaciones a los datos personales › Verificaciones de validez de certificados TLS y lista de excepción basada en certificados de nombres de dominio
Detección de explotación de vulnerabilidades	› Independiente de protocolos, cualquier protocolo TCP/UDP con detección y protección contra evasiones › Soporte para integraciones de firmas Snort que permite personalizar y mejorar la postura de seguridad general › Enfoque de huellas sofisticado que elimina la necesidad de múltiples firmas › Motor de coincidencia por medio de un autómata finito determinista (DFA) de alta velocidad que maneja las nuevas firmas con rapidez › Actualización constante de huellas de Forcepoint
Localización (Fingerprinting) personalizada	› Coincidencia de huellas independiente del protocolo › Lenguaje regular de huellas basado en expresiones con soporte de aplicaciones personalizadas
Reconocimiento	Examinación de TCP/UDP/ICMP, detección de exploración lenta y sigilosa en IPv4 e IPv6
Defensa contra red bot	› Detección basada en descifrado y análisis de secuencia de longitud de mensaje › Categorización de URL de actualización automática para bloquear o advertir a los usuarios respecto de sitios de red bot
Correlación	Correlación local, correlación de servidor de registro
Protección DoS/DDoS	› Detección de descobrde de SYN/UD con límite de conexiones concurrentes, compresión de registros basada en la interfaz › Protección contra métodos de solicitud HTTP lentos, límite de conexión medio abierta › Separación del plano de control y el plano de datos
Métodos de bloqueo	Bloqueo directo, restablecimiento de conexión, uso de listas negras (locales y distribuidas), respuesta HTML, redireccionamiento HTTP
Registro del tráfico	Registro del tráfico automático/extractos de situaciones de uso indebido
Actualizaciones automáticas	› Actualizaciones dinámicas continuas a través de Forcepoint Security Management Center (SMC) › Actualiza los parches virtuales y brinda detección y prevención contra amenazas emergentes

Especificaciones de Forcepoint Next-Gen Firewall, continuación

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
Examinación de antivirus de archivos	Motor de detección de antivirus local*
Entornos seguros de día cero	Forcepoint Advanced Malware Detection disponible para Forcepoint NGFW como un servicio en la nube, en las instalaciones o incluso aislado similar al que utilizan Forcepoint Web Security, Forcepoint Email Security y Forcepoint CASB

FILTRADO DE URL	
Categorización de URL	Impulsada por Forcepoint ThreatSeeker Intelligence, la misma solución que utilizan Forcepoint Web Security y Forcepoint Email Security
Actualizaciones automáticas	Actualización constante a medida que se analizan nuevos sitios
Aplicación de políticas de acceso basado en categorías	Filtrado de URL para Forcepoint NGFW disponible como complemento mediante suscripción

ADMINISTRACIÓN Y MONITOREO	
Interfaces de administración	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)
Monitoreo de SNMP	SNMPv1, SNMPv2c y SNMPv3
Captura de tráfico	tcpdump de la consola, captura remota mediante Forcepoint Security Management Center
Comunicación de administración de alta seguridad	Seguridad de 256 bits para la comunicación de administración de motores
Certificaciones de seguridad	Criterios Comunes (CC) Perfil de protección de dispositivos de red (NDPP) con Firewall con filtrado del tráfico con estado con paquete extendido (Extended Package Stateful Traffic Filter Firewall), certificación de cifrado FIPS 140-2, CSPN por ANSSI, certificación de seguridad de primer nivel de USGv6
Agente de contexto de dispositivo final	Colocación en listas blancas/listas negras a las aplicaciones del cliente que se ejecutan en los host y dispositivos de usuario final. Evita que los archivos no confiables establezcan conexiones salientes y permite ejecutar controles granulares que se adaptan a las necesidades de su organización.

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