Forcepoint

Datasheet

Forcepoint ONE Firewall

Asegura todo el tráfico de Internet y protégelo de ataques diseñados para explotar sitios vulnerables de las sucursales.

Beneficios clave

Proporcionado como un servicio

- Distribuye, actualiza e implementa nuevas políticas y firmas de seguridad en tiempo real.
- Implementa el escalado automático (ascendente o descendente) en una arquitectura moderna de nube, impulsado por el uso real.
- Reduce los costos y cambia de una infraestructura de altos gastos de capital (CapEx) a la ahorrativa arquitectura de nube de costos operativos (OpEx).

Aumenta la seguridad con capacidades de IPS líderes de la industria

- Observa los signos de advertencia temprana de posibles actividades maliciosas, incluyendo amenazas de día cero y ransomware.
- Protégete contra ataques de negación de servicio (DoS). Identifica intrusiones conocidas o sospechadas, incluidos los ataques de shellcode.
- Evita los ataques de SSL diseñados para explotar vulnerabilidades destinadas a filtrar información confidencial.

Dashboards administrativos e informes

- Detecta rápidamente las amenazas con dashboards administrativos e informes personalizados, y obtén información sobre los usuarios o grupos que enfrentan ataques con más frecuencia.
- Reduce el riesgo mediante una fácil identificación de tendencias y patrones de amenazas.
- Simplifica la investigación de incidentes cuando únicamente ves los eventos asociados con un incidente específico.

La transformación digital ha llegado: Los datos y las aplicaciones residen en la nube, y los usuarios acceden a los recursos desde cualquier lugar mediante el uso de dispositivos tanto administrados como no administrados. Sin embargo, las organizaciones distribuidas todavía dependen de firewalls heredados para proteger sus redes. Los ciberdelincuentes están conscientes de esto y constantemente están elaborando formas de atacar el eslabón más débil de la cadena, que a menudo se encuentra en el sitio de la sucursal.

Protege los sitios de las sucursales y las oficinas remotas con Forcepoint ONE Firewall. Garantiza una visibilidad, seguridad y control completos de todo el tráfico de Internet, con el fin de eliminar los puntos ciegos de las redes. Ten paz mental cuando sabes que tu red está protegida por las funciones de IPS de precisión de detección y protección de evasión líderes de la industria contra amenazas avanzadas, incluidos los ataques de día cero.

Inspección completa del tráfico

Forcepoint ONE Firewall ofrece capacidades de inspección de tráfico para proteger contra ataques destinados a exponer sitios vulnerables de sucursales y remotos que operan con firewalls heredados. Junto con Forcepoint ONE SWG, Forcepoint ONE Firewall garantiza que todos los puertos y protocolos sean inspeccionados. Protege y controla todo tu tráfico de Internet para mitigar las brechas de seguridad y proteger contra ataques no convencionales dirigidos a puertos.

Gestión granular de políticas

Forcepoint ONE Firewall ofrece a los administradores capacidades de gestión granular de políticas para aumentar la seguridad general. Los administradores pueden especificar reglas en función del usuario(s) y grupo(s), el servicio que rige la regla de la política y la acción que se debe tomar cuando se activa la regla de la política. Los administradores también pueden reorganizar la prioridad de cada una de las políticas y asignar una política predeterminada para ser utilizada en ausencia de otras políticas. Con el control de políticas de cinco tuplas, los administradores pueden establecer fácilmente reglas en función del protocolo, las direcciones IP de origen y destino, y los puertos de origen y destino, lo que permite un control preciso sobre la seguridad de redes y el tráfico. Este nivel de precisión permite a las organizaciones establecer reglas detalladas que garanticen que solo se produzcan comunicaciones autorizadas y seguras.

Despliegue y gestión de la nube

A diferencia de los firewalls de dispositivos físicos más comunes, costosos y difíciles de mantener, Forcepoint ONE Firewall "se proporciona como un servicio". Esta solución basada en SaaS permite a las organizaciones reducir o eliminar los costos de infraestructura y gastos generales asociados con la adquisición, el despliegue y el mantenimiento de firewalls físicos tradicionales en cada sucursal. Mediante la administración central, los administradores pueden distribuir e implementar rápidamente las últimas actualizaciones de seguridad y firmas en tiempo real, lo que mejora la seguridad general y reduce el riesgo de fugas de datos.

Basado en tecnología confiable de IPS líder de la industria

Forcepoint ONE Firewall va más allá de abordar los problemas comunes de red; también identifica y mitiga rápidamente las amenazas cibernéticas avanzadas. Desde la detección de ataques de negación de servicio (DoS) hasta la visibilidad de ataques de SSL (como Heartbleed), ayuda a los administradores a protegerse de ataques a servidores sin parches e infraestructuras que no reciben mantenimiento. Los signos de alerta tempranos de una violación de la red son críticos para mitigar la infiltración y evitar cualquier control externo y no autorizado de los recursos internos y su consecuente filtración de datos. Es por eso que Forcepoint ONE Firewall detecta el tráfico anómalo y de botnets, ambos indicadores tempranos de posibles actividades maliciosas, incluidas las amenazas de día cero.

Capacidades avanzadas de informe para la tomada de decisiones informadas

Forcepoint ONE Firewall proporciona varias capacidades de generación de informes y dashboards informativos para garantizar que los administradores estén al tanto de la información crítica necesaria para tomar las decisiones correctas. Ofrece gráficos de series temporales para ver las tendencias y los patrones de las amenazas, de modo que los administradores puedan tomar medidas de manera proactiva y evitar intrusiones repetidas. Forcepoint ONE Firewall también ofrece la capacidad de ver eventos relacionados en el registro, a modo de simplificar la investigación de incidentes cuando solo se ven los eventos asociados con un incidente seleccionado. Los administradores pueden generar informes detallados en función de las amenazas identificadas, incluidas las amenazas conocidas y las de día cero detectadas en descargas o cargas, junto con información sobre los usuarios o grupos que las encontraron con más frecuencia.

PLATAFORMAS	
Administración centralizada	Sistema de administración centralizada a nivel empresarial con capacidades de análisis de registro, monitoreo y generación de informes Consulta el datasheet de Forcepoint Security Management Center para obtener más información.
FUNCIONES DE NETWORK SECURITY	
Control de políticas de 5 tuplas	Creación de políticas en función de los usuarios o grupos, sitios de origen o listas de direcciones IP, dominios de destino o listas de direcciones IP, puertas de origen y destino, y protocolos
Servicios y protocolos de red preconfigurados	Cientos de protocolos predefinidos y agentes de protocolo
Protocolos definidos por el usuario	Creación de protocolos definidos por el usuario para gobernar el comportamiento de la aplicación interna
INSPECCIÓN DEL TRÁFICO	
Integración de Forcepoint ONE SWG	Integración con Forcepoint ONE SWG para proteger la web
DNS	Prevención amenazas de DNS e implementación de protocolos para evitar ataques maliciosos a través de consultas de DNS
CAPACIDADES DE IPS Y PREVENCIÓN DE AMENAZAS	
Inspección profunda de paquetes	Inspección del comportamiento de los metadatos de los paquetes y el protocolo en busca de patrones de firmas de tráfico sospechosos
Amplio catálogo de situaciones de amenazas	Protección contra decenas de miles de situaciones de amenazas que se actualizan continuamente a través de la nube
Protección contra amenazas basada en categoría	Optimización de la detección de amenazas y simplificación de la gestión de configuraciones
Detección basada en anomalías	Aprovisionamiento de señales de alerta temprana sobre posibles actividades maliciosas, incluidas las amenazas de día cero, mediante la observación del tráfico antes y después de los ataques
Signature-based Detection	Identificación de aplicaciones, protocolos y servicios desde la huella digital
Protección contra DoS	Protección de la red mediante la identificación de ataques de negación de servicio, detección de amenazas que intentan bloquear servidores sin parches y protección de infraestructuras que no reciben mantenimiento
Ataques de divulgación	Visibilidad de ataques de amenazas de SSL (como Heartbleed), diseñados para explotar vulnerabilidades en servidores que podrían filtrar información confidencial, como palabras clave, claves de cifrado, nombres de usuario, código fuente, directorios, configuración y contenido de archivos
Protección contra botnets	Detección de tráfico de botnets (un indicador de que la red ha sido comprometida) y prevención de exfiltración de datos por parte de algún control externo y no autorizado de los recursos internos
Malware o antivirus	Detección y prevención de amenazas de servicios que se sabe que demuestran comportamientos maliciosos o indeseables, incluyendo spyware, adware y malware
Violaciones del protocolo	Implementación estricta del cumplimiento de una variedad de protocolos, incluidos TCP, HTTP, DNS y otros
Sondeos	Prevención de actividades de escaneo diseñadas para recopilar inteligencia e identificar vulnerabilidades
Enrutamiento malicioso	Ataques que intentan hacer un uso indebido de los protocolos de red para evitar o pasar los filtros de seguridad