

McAfee Network Security Platform

Optimización de la protección de la red con prevención de intrusiones de próxima generación

Ventajas principales

Prevención contra amenazas rápida y precisa

- Inspección del tráfico con mantenimiento de la información del estado de cada unidad ("stateful")
- Información anticipada sobre amenazas a través de McAfee GTI
- Malware, zero-day, DoS/DDoS, redes de bots

Rendimiento y disponibilidad

- Más de 10 Gbits/s
- Fiabilidad líder en el sector
- Conmutación en caso de error y protección de carga en caso de error

Visibilidad en toda la red

- Visibilidad de aplicaciones de próxima generación
- Detección de bots basada en el comportamiento
- Análisis de comportamiento de red basado en flujo

Administración centralizada de la seguridad

- Administración de la seguridad de la red escalable
- Integración con el software McAfee ePO
- Visibilidad de eventos de prevención de intrusiones en host, virus y spyware

Simplicidad de uso

- Bloqueo inteligente dinámico
- Correlación de amenazas
- Análisis de vulnerabilidades integrado

Inspección de entornos virtuales

- Inspección del tráfico entre máquinas virtuales
- Cuarentena de máquinas virtuales maliciosas
- Una consola para dispositivos físicos y virtuales

McAfee, el líder global en sistemas de prevención de intrusiones en la red (IPS, del inglés Intrusion Prevention System), proporciona niveles de seguridad nunca vistos y, al mismo tiempo, opciones de despliegue flexibles que facilitan la optimización de sus inversiones en red. Solo McAfee® Network Security Platform ofrece la mejor efectividad de seguridad en su categoría, rendimiento en línea escalable y controles IPS de próxima generación que eliminan las conjeturas en la administración de la seguridad. Unifique la administración de la seguridad en entornos físicos y virtuales, simplifique las operaciones de seguridad y proteja su empresa contra las últimas amenazas: malware, ataques de tipo zero-day, redes de bots, intentos de denegación de servicio (DoS) y ataques selectivos avanzados.

Protección líder de la industria

Deje que McAfee se ocupe de las tareas más difíciles de la seguridad de la red. Sin necesidad de más configuración, McAfee Network Security Platform ofrece mejor efectividad que la mayoría de las soluciones IPS de red tras realizar ajustes importantes. Con decenas de miles de sensores desplegados en todo el mundo, McAfee Network Security Platform es la solución de prevención de intrusiones en red más eficaz del sector. Ofrece cobertura contra malware, amenazas de tipo zero-day, ataques de denegación de servicio y redes de bots.

Rendimiento de varios gigabits

Disfrute de todas las ventajas: seguridad y alto rendimiento. McAfee Network Security Platform combina una arquitectura de inspección basada en protocolos, de un solo paso, con un hardware específico de categoría de operadora para conseguir en la práctica un rendimiento de análisis de más de 10 Gbits en un solo dispositivo. A diferencia de otras soluciones IPS en las que el rendimiento se deteriora en un 50% debido a un enfoque de que da prioridad a la seguridad frente al rendimiento, la arquitectura de McAfee Network Security Platform, de extremada eficacia, mantiene el rendimiento sea cual sea la configuración de la seguridad.

Información anticipada sobre amenazas

Mejore significativamente la efectividad de su seguridad con información anticipada sobre las amenazas. McAfee Network Security Platform incorpora McAfee Global Threat Intelligence™ (McAfee GTI™) para adecuar de manera dinámica la prevención en línea de los ataques tradicionales y los emergentes. McAfee GTI evalúa la reputación de las comunicaciones de la red basándose en

la reputación de miles de millones de datos de archivos, IP, URL, protocolos y geolocalización exclusivos procedentes de todo el mundo.

Conocimiento y control de las aplicaciones

Tome decisiones fundamentadas sobre las aplicaciones y los protocolos de su red. McAfee Network Security Platform es la primera y la única solución IPS que combina prevención avanzada de amenazas y conocimiento de las aplicaciones en un solo motor de decisión de seguridad. Nosotros comparamos la actividad de las amenazas con el uso de las aplicaciones, con visibilidad de más de 1.100 aplicaciones y protocolos de la capa 7 del modelo OSI, para que pueda decidir con fundamento qué aplicaciones pueden ejecutarse en su red.

Visibilidad de la red sin precedentes

Nunca antes ha podido disfrutar de una visión tan detallada de su red. Puede observar claramente el comportamiento de los sistemas, aplicaciones y usuarios, y detectar cualquier anomalía en la red. McAfee Network Security Platform amplía enormemente el ámbito de las soluciones de prevención de intrusiones en red tradicionales y, mediante el análisis de los flujos de datos de los conmutadores y enrutadores ubicados en distintos puntos en la empresa, identifica fácilmente las redes de bots y otras actividades maliciosas en toda la red.

Seguridad según el contexto

Adopte una postura más agresiva con respecto a la seguridad de su red sin aumentar el riesgo de falsos positivos. McAfee compara los datos de varias fuentes —McAfee GTI, análisis de vulnerabilidades, comportamiento de aplicaciones y de sistemas— con el fin de identificar de



McAfee Network Security Platform le permite:

Proteger su negocio

- Prevención de ataques y reducción del tiempo de inactividad
- Protección de sus datos y su infraestructura
- Cumplimiento de exigencias de normativas

Proteger sus sistemas

- Protección proactiva para sistemas sin parches
- Protección proactiva contra ataques de tipo zero-day
- Prevención de intrusiones según el contexto

Proteger su red

- Visibilidad y control de aplicaciones
- Limitación versátil de flujos de tráfico
- Limitación de conexiones específicas de hosts

Proteger su inversión en seguridad

- Ethernet nativa de 10 gigabits
- Hardware para redes
- Durabilidad líder del sector

manera fiable los ataques a la red y, en muchos casos, prevenir de forma automática la actividad maliciosa. Por ejemplo, un evento de "sólo alerta" de baja fiabilidad puede pasar automáticamente a evento de "bloqueo" de alta fiabilidad gracias a la correlación en tiempo real de una definición de ataque basado en firma con la reputación de la IP de origen de la amenaza.

Control de acceso incorporado

Añada el software opcional de control de acceso a la red (NAC) y convierta su McAfee Network Security Platform en un dispositivo NAC, que ofrece control previo y posterior a la admisión, control de acceso basado en la identidad, así como cuarentena de host y directivas de acceso aplicables.

Administración de la seguridad integrada

Saque el máximo partido a su inversión en seguridad con gestión de riesgos y seguridad integrada. McAfee Network Security Platform se integra con el software McAfee® ePolicy Orchestrator® (McAfee ePO™) para ofrecer a su organización una visión consolidada de los riesgos y el cumplimiento de normativas en toda la empresa, con evaluaciones actualizadísimas de la infraestructura sometida a riesgos basadas en las vulnerabilidades de los sistemas, la protección de la red y los niveles de seguridad de los endpoints.

Todos los dispositivos McAfee Network Security Platform ofrecen las siguientes funciones:

Prevención de intrusiones avanzada

- Inspección del tráfico con mantenimiento de la información del estado de cada unidad ("stateful") (desfragmentación de IP y remontaje del tráfico TCP)
- Detección de anomalías
- Detección basada en firmas (definida por McAfee, definida por el usuario, de código abierto)
- Detección basada en reputación (McAfee GTI)
- Detección heurística de bots
- Correlación de ataques
- Detección de protocolos de la capa 7
- Cuarentena para hosts
- Protección avanzada contra evasiones

Prevención contra denegación de servicio (DoS) y denegación de servicio distribuida (DDoS)

- Detección basada en umbrales y en análisis heurístico
- Limitación de conexiones
- Detección basada en perfiles, autoaprendizaje

Visibilidad de la red

- Visibilidad de las aplicaciones
- Información del sistema
- Correlación de vulnerabilidades

- Alertas de intrusiones en host
- Inspección de entornos virtuales
- Captura de paquetes para integración en análisis forense
- Análisis de comportamiento basados en flujo (a través de NTBA)

Controles diferenciados

- Controles de aplicaciones y aplicaciones secundarias
- Reglas de listas de control de acceso basadas en geolocalización
- Limitación de conexiones
- Cuarentena para hosts (a través de IPS o NAC)
- Control del acceso basado en identidad
- Control de acceso basado en el estado del sistema

McAfee GTI

- Reputación de archivos
- Reputación de IP
- Reputación de aplicaciones y protocolos
- Geolocalización

Opciones de gran disponibilidad

- Conmutación en caso de error con información de estado
- Protección de carga en caso de error externa (activa y pasiva)
- Protección de carga en caso de error integrada (sólo para puertos de cobre)

Encapsulado de protocolos (tunneling)

- IPv6
- Túneles V4-in-V4, V4-in-V6, V6-in-V4 y V6-in-V6
- MPLS
- GRE
- VLAN doble Q-in-Q

McAfee Network Security Manager

- Administración continua
- Decenas de plantillas de directivas de seguridad IPS predefinidas
- Hasta 1.000 directivas IPS virtuales (en determinados modelos)
- Autenticación de usuarios integrada (Radius, LDAP y TACACS)
- Conmutación en caso de error y recuperación automáticas
- Recuperación de los datos de configuración críticos en caso de desastre
- Administración jerárquica para el control de directivas centralizado

Soluciones integradas

- Software McAfee ePolicy Orchestrator
- McAfee Network Threat Behavior Analysis
- McAfee Network Access Control (complemento de software)
- McAfee Network Threat Response
- McAfee Vulnerability Manager
- Análisis forense de terceros

Especificaciones de McAfee Network Security Platform



Componentes de hardware del sensor	M-8000	M-6050	M-4050	M-3050	M-2950	M-2850/M-2750	M-1450	M-1250
Rendimiento								
Rendimiento en la práctica	10 Gbits/s	5 Gbits/s	3 Gbits/s	1,5 Gbits/s	1 Gbit/s	600 Mbits/s	200 Mbits/s	100 Mbits/s
Rendimiento máximo (paquetes UDP de 1.512 bytes)	Hasta 20 Gbits/s	Hasta 10 Gbits/s	Hasta 4 Gbits/s	Hasta 2,5 Gbits/s	Hasta 1 Gbit/s	Hasta 1 Gbit/s	Hasta 300 Mbits/s	Hasta 150 Mbits/s
Máximo de conexiones simultáneas	4.000.000	2.000.000	1.500.000	750.000	750.000	750.000 / 250.000	80.000	40.000
Nuevas conexiones por segundo	120.000	60.000	36.000	18.000	15.000	10.000	4.000	2.000
Rendimiento con descifrado SSL (basado en el 10% del tráfico SSL)	8,8 Gbits/s	4,4 Gbits/s	2,7 Gbits/s	1,3 Gbits/s	900 Mbits/s	550 Mbits/s	N/D	N/D
Máximo de flujo SSL	400.000	200.000	150.000	75.000	25.000	25.000	N/D	N/D
Claves SSL importadas	64	64	64	64	64	64	N/D	N/D
Perfiles								
Número de sistemas IPS virtuales	1.000	1.000	1.000	1.000	100	100	32	16
Máximo de perfiles de DoS	5.000	5.000	5.000	5.000	5.000	300	120	100
Reglas de ACL	1.000	1.000	1.000	1.000	1.000	400	100	50
Puertos								
Gigabit Ethernet, puertos de cobre fijos	—	—	—	—	8	8 / —	8	8
Gigabit Ethernet, puertos SFP	16	8	8	8	12	12 / 20	—	—
10-Gigabit Ethernet	12	8	4	4	—	—	—	—
Puertos de respuesta dedicados (GigE)	1	1	1	1	1	1	1	1
Puertos de administración dedicados (GigE)	1	1	1	1	1	1	1	1
Puertos con funciones de protección de carga en caso de error integradas	—	—	—	—	8	8 / —	8	8
Puertos de control para kits de protección de carga en caso de error externos	14	8	6	6	6	6 / 10	—	—
Características físicas								
Dimensiones	2 x 2RU montados en bastidor 42,54 cm (ancho) x 7,75 cm (alto) x 76,20 cm (fondo) cada uno	2RU montados en bastidor 42,54 cm (ancho) x 7,75 cm (alto) x 76,20 cm (fondo)	2RU montados en bastidor 42,54 cm (ancho) x 7,75 cm (alto) x 76,20 cm (fondo)	2RU montados en bastidor 42,54 cm (ancho) x 7,75 cm (alto) x 76,20 cm (fondo)	2RU montados en bastidor 40,34 cm (ancho) x 8,38 cm (alto) x 62,23 (fondo)	2RU montados en bastidor 40,34 cm (ancho) x 8,38 cm (alto) x 62,23 (fondo)	1RU montado en bastidor 44,12 cm (ancho) x 4,19 cm (alto) x 34,29 cm (fondo)	1RU montado en bastidor 44,12 cm (ancho) x 4,19 cm (alto) x 34,29 cm (fondo)
Peso	42,6 kg (21,3 cada unidad)	21,3 kg	21,3 kg	21,3 kg	18,1 kg	18,1 kg	5,4 kg	5,4 kg
Consumo eléctrico	900 W (450 W cada unidad)	450 W	450 W	450 W	450 W	450 W	120 W	120 W
Alimentación de CC disponible	Opcional	Opcional	Opcional	Opcional	Opcional	Opcional	No	No
Fuente de alimentación	100 - 240 V CA (50/60 Hz)							
Temperatura	De 0 a 35 °C (en funcionamiento) De -40 a 70 °C (sin funcionar)				De 0 a 40 °C (en funcionamiento) De -40 a 70 °C (sin funcionar)			
Humedad relativa (sin condensación)	En funcionamiento: de 10% a 90% Sin funcionar: de 5% a 95%							
Altitud	De 0 a 3.000 m							
Certificado de seguridad	UL 1950, CSA-C22.2 N° 950, EN-60950, IEC 950, EN 60825, IEC 60825, licencia 21CFR1040 CB e informe que cubre todas las desviaciones por país.							
Certificación EMI	FCC Parte 15, Clase A (CFR 47) (EE.UU.), ICES-003 Clase A (Canadá), EN55022 Clase A (Europa), CISPR22 Clase A (Internacional)							



McAfee, Inc.
6205 Blue Lagoon Drive
Suite 600
Miami, Florida 33126
U.S.A.
www.mcafee.com

McAfee, el logotipo de McAfee, McAfee Global Threat Intelligence, McAfee GTI, McAfee ePolicy Orchestrator y McAfee ePO son marcas comerciales registradas o marcas comerciales de McAfee, Inc. o de sus empresas filiales en EE. UU. y en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros. Los planes, especificaciones y descripciones de productos mencionados en este documento son únicamente a título informativo y están sujetos a cambios sin aviso previo; se ofrecen sin garantía de ningún tipo, ya sea explícita o implícita. Copyright © 2011 McAfee, Inc. Reservados todos los derechos.
37801ds_nsp_1011_fnl_ETMG