FICHA TÉCNICA

McAfee Virtual Network Security Platform

Detección de amenazas completa para las redes en la nube

McAfee® Virtual Network Security Platform es una completa solución de prevención de intrusiones (IPS) y amenazas en la red diseñada para las necesidades específicas de las nubes privadas y públicas. Esta solución descubre y bloquea las sofisticadas amenazas dirigidas a las arquitecturas de la nube de manera precisa y sencilla, para que las empresas puedan garantizar el cumplimiento de las normativas y disfrutar de una nube segura. Las tecnologías avanzadas incluyen detección sin firmas, emulación en línea, parches de vulnerabilidades basados en firmas, y compatibilidad con Amazon Web Services (AWS) y virtualización de la red. Con flujos de datos simplificados, numerosas opciones de integración y sencillas opciones de licencias, las empresas pueden gestionar y adaptar fácilmente su seguridad en las arquitecturas en la nube más complejas.

Protección total para la nube pública con tecnología de seguridad avanzada

Las nubes públicas ofrecen comodidad, ahorro de costos y la oportunidad de trasladar los gastos de infraestructura a un modelo de gastos de explotación. Pero, por otra parte, también introducen un nuevo nivel de riesgo, ya que un agresor podría aprovechar una vulnerabilidad de un software accesible para el público, para penetrar en la nube y filtrar información confidencial, o exponer datos de clientes de forma accidental a otros arrendatarios que utilicen el mismo servicio. McAfee Virtual Network Security Platform es compatible con AWS —el servicio en la nube pública líder en la actualidad— que ofrece una visibilidad total de los datos que pasan por un gateway de Internet y también del tráfico este-oeste, para detectar posibles amenazas. Este servicio permite garantizar de nuevo el cumplimiento de las normativas de seguridad y la visibilidad de amenazas en las arquitecturas de nube pública, con una plataforma de prevención de intrusiones (IPS) que ofrece inspección real del tráfico este-oeste.

Ventajas principales

Prevención de amenazas avanzadas inigualable

- Análisis antimalware avanzado y sin firmas
- Protección frente a secuencias de comandos entre sitios e inyección SQL
- Detección avanzada de redes de bots y devoluciones de llamadas de malware
- Análisis basado en el comportamiento y protección frente a ataques DDoS
- Integración con McAfee Advanced Threat Defense
- Despliegue de sistemas de detección de intrusiones (IDS) y de prevención de intrusiones (IPS)
- Solución VMware ESX-McAfee Virtual Network Security Platform siempre activa

Protección de entornos virtualizados

Las empresas adoptan con rapidez las infraestructuras de TI virtualizadas —como las nubes privadas y públicas— en las que los servidores físicos pueden alojar simultáneamente varias máquinas virtuales e incluso cargas de trabajo completas virtualizadas. La comunicación entre máquinas virtuales resultante, junto a la migración, replicación y copia de seguridad inmediatas de estas cargas de trabajo incrementan significativamente el tráfico este-oeste dentro de la nube privada y pública, así como en los centros de datos definidos por software (SDDC). Además, con la flexibilidad que ofrece la virtualización de la red, este creciente flujo de tráfico se hace dinámico e imprevisible, lo que aumenta el caos. Para estar a la altura, las soluciones de seguridad deben ser flexibles y escalables, y lo que es más importante, deben funcionar perfectamente con las plataformas de red definidas por software (SDN) que organizan estas máquinas virtuales y cargas de trabajo, que suelen tener una duración limitada.

Mejora de la agilidad en las nubes privadas

Diseñada para satisfacer las necesidades de protección de los entornos virtualizados, McAfee Virtual Network Security Platform se integra completamente con plataformas de nube privada conocidas, como los entornos SDN basados en VMware NSX y OpenStack. De hecho, McAfee Virtual Network Security Platform es la única solución IPS virtual y dedicada que está certificada para funcionar con VMware NSX. La microsegmentación de las máquinas virtuales y la inspección profunda del tráfico este-oeste se mantienen automáticamente en los entornos virtualizados, incluso con cargas de trabajo que se generan, migran y dan de baja con gran rapidez.

Prevención de amenazas inigualable

McAfee Virtual Network Security Platform se basa en una arquitectura de inspección de próxima generación diseñada para llevar a cabo inspecciones exhaustivas del tráfico de red virtual. Utiliza una combinación de tecnologías de inspección avanzadas, como el análisis de todos los protocolos, la reputación de amenazas, el análisis de comportamientos y el análisis de malware avanzado, para detectar y prevenir tanto los ataques de red conocidos como los desconocidos (zero-day).

Ninguna tecnología de detección de malware es capaz de prevenir todos los ataques por sí sola, razón por la cual McAfee Virtual Network Security Platform incorpora varios motores de detección con firmas y sin firmas para evitar que el malware no deseado cause estragos en sus nubes. Esta solución ofrece numerosas tecnologías de inspección, como la emulación en línea de navegadores, y archivos JavaScript y Adobe, la detección de devoluciones de llamadas de redes de bots y malware, la detección de ataques DDoS basada en comportamientos, y la protección frente a ataques avanzados, como secuencias de comandos entre sitios e inyección SQL. McAfee Virtual Network Security Platform también puede identificar y bloquear hasta los archivos más ocultos gracias a su integración con McAfee Advanced Threat Defense, que somete a los archivos a profundos análisis de comportamiento. McAfee Advanced Threat Defense combina análisis de código estático en profundidad (con entornos aislados para malware), y aprendizaje automático para incrementar la detección de amenazas de tipo zero-day, como las que emplean técnicas de evasión y el ransomware.

Arquitectura preparada para la nube

- Una licencia permite compartir el resultado en cualquier combinación de nubes públicas y privadas.
- El innovador enfoque de la inspección de AWS ofrece protección del tráfico este-oeste real en la nube pública.
- Las opciones de organización que ofrecen los entornos SDN basados en VMware NSX y OpenStack permiten la microsegmentación automatizada y la inspección del tráfico entre cargas de trabajo de la nube privada.
- Panel compatible con máquinas virtuales con función de cuarentena disponible con la integración de VMware.
- Una sola consola centralizada para la administración de sensores físicos y virtuales, in situ y en la nube.

Simplificación con uso compartido de licencias para la nube

En la actualidad, muchas empresas reparten su infraestructura y sus recursos de TI entre varias nubes y plataformas, ya sea para mantener la compatibilidad con aplicaciones heredadas, o para reducir la dependencia de un solo proveedor o la redundancia de sistemas, o bien para ahorrar costos. Adquirir licencias de soluciones de seguridad para entornos virtualizados puede resultar complicado y caro, ya que la mayoría de los proveedores exigen licencias diferentes para las nubes privadas y públicas, y para las distintas plataformas SDN.

McAfee simplifica la adquisición de licencias y reduce los costos gracias al uso compartido de licencias para la nube, un nuevo concepto que permite a los clientes compartir su licencia de McAfee Virtual Network Security Platform en cualquier combinación de plataformas de nubes públicas y privadas. Además, mejora la seguridad, ya que permite a los administradores ofrecer rápidamente protección del tráfico este-oeste y microsegmentación en cargas de trabajo virtuales dondequiera que esté, sin tener que pasar por el largo proceso de adquisición completo.

Flujos de trabajo y análisis más sencillos

Descubra y bloquee las amenazas más sofisticadas con facilidad. McAfee Virtual Network Security Platform incluye análisis avanzados e integraciones con otras soluciones de seguridad para crear una plataforma de detección y mitigación de amenazas para redes verdaderamente global y conectada.

Las amenazas modernas pueden generar grandes volúmenes de alertas, que ponen a prueba la capacidad del operador de seguridad para priorizarlas y supervisarlas. Si no se correlacionan a tiempo, algunas amenazas reales pueden pasar desapercibidas. Los análisis avanzados y los flujos de trabajo prácticos de McAfee Virtual Network Security Platform, configurados de fábrica, correlacionan varias alertas de IPS para convertirlas en un solo evento, lo que permite a los administradores obviar los datos superfluos e ir directamente a la información relevante y práctica.

Administración centralizada con control en tiempo real de datos en tiempo real

Con un solo dispositivo McAfee Network Security Manager es posible disfrutar de una administración centralizada y basada en la Web, con una facilidad de uso incomparable. Su consola avanzada y su interfaz gráfica de usuario perfeccionada le permitirán controlar los datos en tiempo real. Ahora podrá gestionar, configurar y supervisar fácilmente todos los dispositivos McAfee Network Security Platform, virtuales o físicos, así como los dispositivos McAfee Network Threat Behavior Analysis, en sus recursos tradicionales o en la nube pública o privada, desde una sola consola. La intuitiva interfaz de administración basada en la Web permite abordar todo tipo de despliegues, ya se trate de dispositivos individuales o de clústeres esenciales y ampliamente distribuidos. Además, McAfee Network Security Manager puede instalarse como instancia virtual en los servidores VMware ESX y en AWS.

Administración de seguridad inteligente

- La consola gestiona los sensores in situ y en la nube.
- Priorización y correlación de alertas inteligente
- Paneles robustos de investigación de malware
- Flujos de trabajo de investigación preconfigurados
- Administración basada en la Web escalable

Visibilidad y control

- Identificación de aplicaciones
- Identificación de usuarios
- Identificación de dispositivos
- Estado de seguridad de todas las máquinas virtuales de AWS

Alta disponibilidad y recuperación ante desastres

McAfee Network Security Manager actúa como mediador entre los controladores y elige uno que estará activo y el otro, para que actúe de reserva. Cuando el controlador activo deja de estar disponible, se activa el controlador de reserva. De esta forma, se ofrece una alta disponibilidad de controladores para despliegues de AWS, con un mecanismo de conmutación en caso de error que garantiza que siempre haya un controlador activo y disponible. Además, un McAfee Network Security Manager de reserva facilita la recuperación ante desastres para entornos AWS.

McAfee Virtual Network Security Platform ofrece gran disponibilidad con Manager Disaster Recovery (MDR), alta disponibilidad de controladores y las funciones de autoadaptación del sensor de IPS virtual. De esta forma, McAfee Virtual Network Security Platform funciona siempre de forma ininterrumpida. La solución MDR ofrece un segundo administrador, que reemplaza al principal cuando está fuera de servicio. Gracias al par de controladores de alta disponibilidad, siempre hay uno de los controladores activo y disponible, por lo que la red nunca está inactiva. La función de autoadaptación de los sensores de IPS virtuales crea un nuevo sensor de IPS virtual, cuando se detiene una instancia del sensor. Así se efectúa un equilibrio de carga cuando hay un incremento en el tráfico de la red.

Arquitectura de defensa unificada

Los ataques sofisticados no respetan los límites de los productos, aprovechando cualquier brecha en la infraestructura, especialmente si se trata de productos de seguridad. McAfee Virtual Network Security Platform es la única solución IPS que se integra con distintos productos de seguridad, y emplea datos y flujos de trabajo para cerrar dichas brechas, lo que redunda en un incremento de la rentabilidad y una reducción del costo total de propiedad. Entre otros productos se integra con:

- **Software McAfee ePolicy Orchestrator® (McAfee ePO™):** visibilidad total de los endpoints para todos los eventos y alertas de IPS
- **McAfee Endpoint Intelligence Agent:** combina la perspectiva de la red y de los endpoints para detener las fugas de datos.
- **McAfee Enterprise Security Manager:** amplio uso compartido de datos y cuarentena de IPS para alertas de IPS.
- **McAfee Threat Intelligence Exchange:** aprendizaje compartido en distintos tipos de dispositivos.
- **McAfee Global Threat Intelligence:** el servicio de reputación más grande y activo del mundo.
- **McAfee Network Threat Behavior Analysis:** visibilidad ampliada y fiable de toda la red.
- **McAfee Virtual Advanced Threat Defense**
- **McAfee Cloud Threat Detection**
- **McAfee Management for Optimized Virtual Environments (McAfee MOVE)**
- **Analizadores de vulnerabilidades de terceros:** análisis de riesgo y hosts para los endpoints.

Funciones adicionales

Prevención de amenazas avanzadas

- Motor de emulación de McAfee Gateway Anti-Malware
- Motor de emulación de JavaScript incrustado en archivos PDF (entorno aislado ligero)
- Motor de análisis de comportamiento de Adobe Flash
- Protección contra evasiones avanzadas

Protección frente a redes de bots y devoluciones de llamadas de malware

- Detección de devoluciones de llamadas a servidores de nombres de dominios (DNS)/algoritmos de generación de dominios (DGA), de flujo rápido
- "Sinkholing" de DNS
- Detección heurística de bots
- Correlación de varios ataques
- Base de datos de mando y control

Prevención de intrusiones avanzada

- Desfragmentación de IP y remontaje del tráfico TCP
- Firmas de McAfee, definidas por el usuario y de código abierto
- Cuarentena de hosts y limitación de flujos de tráfico
- Inspección de entornos virtuales
- Prevención de ataques de denegación de servicio (DoS) y denegación de servicio distribuidos (DDoS)
- Detección basada en umbrales y en análisis heurístico
- Limitación de conexiones basadas en hosts
- Autoaprendizaje, detección basada en perfiles

McAfee Global Threat Intelligence

- Reputación de archivos
- Reputación de IP
- Acceso limitado basado en la geolocalización
- Control de acceso basado en la dirección IP

FICHA TÉCNICA

	Tipo de sensor 1	Tipo de sensor 2	Tipo de sensor 3
Plataforma	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 NSX 6.3 AWS
Modelo de sensor de IPS virtual	**IPS-VM100**	**IPS-VM600**	**IPS-VM100-VSS**[1]
Tipo de despliegue de IPS virtual	Independiente	Independiente	Distribuido
Compatibilidad con VMware NSX	No	No	Sí
Compatibilidad con AWS	No	No	Sí
Número de núcleos lógicos de CPU[2]	3	4	3
Memoria necesaria[3]	4 GB	6 GB	5 GB
Especificaciones del sensor virtual			
Rendimiento máximo[4]	Hasta 500 Mbit/s	Hasta 1 Gbit/s	Hasta 500 Mbits/s
Conexiones simultáneas	200 000	600 000	200 000
Conexiones establecidas por segundo	6000	20 000	6000
Flujos UDP admitidos	39 168	254 208	39 168
Número de pares de puertos de supervisión	2	3	1[5]
Interfaces virtuales (VIDS) por sensor	32	100	32
Perfiles de DoS	100	300	100
Puerto de administración	Sí	Sí	Sí
Puerto de respuesta	Sí	Sí	No
Modos de despliegue	Inspección entre VM, inspección de máquina física a VM, inspección entre máquinas físicas, inspección de puertos SPAN		Inspección de VMware NSX en línea

1. Para uso solamente en entornos VMware NSX como servicio insertado.
2. Los requisitos de recursos de las máquinas virtuales pueden variar según la versión. Consulte la documentación de la versión de que se trate.
3. Ibid.
4. Medido con paquetes UDP de 1518 bytes en condiciones de prueba ideales.
5. Representación virtual de entrada y salida La inspección está muy relacionada con VMware NSX en la capa de kernel.

McAfee
Together is power.

Av. Paseo de la Reforma No.342 Piso 25
Colonia Juárez, México DF
C.P. 06600
+52-55-50890250
www.mcafee.com/mx