



Sensor virtual de McAfee Network Security Platform

Sistema de prevención de intrusiones (IPS) de McAfee® para entornos virtuales

El sensor virtual de McAfee Network Security Platform es una completa y avanzada solución IPS preparada para las exigencias específicas de los entornos virtuales. Se trata de una solución de seguridad especialmente inteligente que detecta y bloquea amenazas sofisticadas en las redes virtuales con una velocidad, precisión y facilidad inigualables.

Ventajas principales

- Solución inteligente de prevención avanzada de intrusiones en la infraestructura, suministrada y utilizada como servicio basado en software.
- Elimina las barreras de implementación y arquitectura de las directivas de seguridad de red en entornos virtualizados.
- La integración con VMware NSX permite simplificar la administración y la mediación transparente.
- La integración con VMware crea un panel compatible con máquinas virtuales y con funciones de cuarentena.
- Administra el hardware físico y los sensores virtuales desde la misma plataforma de administración.

Protección de lo virtual

Las empresas están migrando a las infraestructuras de TI virtuales, como las nubes privadas y públicas, los centros de datos virtuales para servidores y las máquinas virtuales para clientes. Los requisitos de seguridad de las redes virtuales no suelen coincidir con los de las redes físicas.

Por ejemplo, supervisar el tráfico P2P y el control de acceso en una red virtual plantea sus propias dificultades. A causa de la arquitectura de red y de los requisitos de seguridad especiales, los productos de seguridad virtuales normalmente deben trascender las tareas de sus homólogos físicos. E incluso en las redes físicas pueden suponer un ahorro de costos y espacio.

McAfee Network Security Platform para entornos virtuales

El sensor virtual de McAfee Network Security Platform es una instancia virtual del software de esta plataforma que puede instalarse como máquina virtual en un host VMware ESX. Para desplegar un sensor virtual, no hace falta ningún hardware IPS de McAfee. Aunque está principalmente diseñado para proteger redes virtuales, también puede desplegarse para la seguridad de redes físicas.

Al igual que los sensores físicos, los sensores virtuales se pueden configurar y administrar con McAfee Network Security Manager. Este administrador puede instalarse en un servidor físico o en una máquina virtual. Además, es posible utilizar el mismo McAfee Network Security Manager para administrar sensores virtuales y físicos.

Los sensores virtuales son compatibles con la mayoría de las funciones que admite un sensor físico, pero, al contar con la ventaja añadida de ser virtuales, pueden desplegarse con rapidez para proteger varias arquitecturas de red, tanto virtuales como físicas.

Una defensa dual

El sensor virtual de McAfee Network Security Platform se integra con McAfee Advanced Threat Defense. Con un enfoque innovador y por capas, McAfee Advanced Threat Defense detecta hasta el malware actual más sigiloso de tipo zero-day. Esta solución combina firmas antivirus que no requieren intervención, información de reputación y emulación en tiempo real con análisis de código estático en profundidad y análisis dinámicos (en entornos aislados) con el fin de examinar el comportamiento real. Con todo ello se obtiene

la protección contra malware avanzado más sólida del mercado y se garantiza su efectividad, sin sacrificar el desempeño.

Una estrecha integración entre McAfee Advanced Threat Defense y los dispositivos de seguridad de la red, como McAfee Network Security Platform, permite actuar de manera inmediata cuando McAfee Advanced Threat Defense determina que un archivo es malicioso. Las soluciones de seguridad de red de McAfee bloquean inmediatamente cualquier otra copia de este archivo que entre a la red, sin necesidad de remitirla para su análisis. Además, McAfee Network Security Platform puede poner en cuarentena un host infectado para impedir que se propague la actividad maliciosa en la red.

Control en tiempo real de datos en tiempo real

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

	IPS-VM100	IPS-VM600	IPS-VM100-VSS ¹
Requisitos de la plataforma virtual			
VMware	<ul style="list-style-type: none"> • VMware ESX 5.0 • VMware ESX 5.1 • VMware ESX 5.5 • VMware ESX 6.0 		VMware ESXi5.5
Compatibilidad con NSX	No		Sí
Número de núcleos lógicos ²	Entre 3 y 4		3 (3 vCpu)
Memoria necesaria ³	Hasta 6 GB		5 GB
Especificaciones del sensor virtual			
Desempeño global ⁴	Hasta 500 Mbits/s	Hasta 1 Gbit/s	Hasta 700 Mbits/s
Desempeño máximo ⁵	Hasta 1 Gbit/s	Hasta 2 Gbit/s	Hasta 1 Gbit/s
Conexiones simultáneas	200 000	600 000	200 000
Conexiones establecidas por segundo	6000	20 000	6000
Flujos UDP admitidos	39 000	254 000	39 000
Número de pares de puertos de supervisión	2	3	1 ⁶
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 NSX en línea

1. Para uso solamente en entornos 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. El desempeño y las capacidades se midieron en condiciones de prueba ideales.
5. Medido con paquetes UDP de 1518 bytes en condiciones de prueba ideales.
6. Representación virtual de entrada y salida La inspección está muy relacionada con NSX en la capa de kernel.



McAfee. Part of Intel Security.

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