McAfee Virtual Network Security Platform

Detección de amenazas y prevención de intrusiones completas para las redes en la nube

McAfee® Virtual Network Security Platform (McAfee vNSP) 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 rápidamente las sofisticadas amenazas dirigidas a las arquitecturas de la nube, de manera precisa y sencilla, para que las empresas puedan proteger las cargas de trabajo y garantizar el cumplimiento de las normativas con fiabilidad. Las tecnologías avanzadas incluyen detección sin firmas, emulación en línea y corrección de vulnerabilidades basada en firmas. Gracias a los flujos de trabajo simplificados, las flexibles opciones de integración y las sencillas licencias, las empresas pueden gestionar y escalar fácilmente su seguridad para satisfacer sus necesidades ahora y en el futuro.

Seguridad total para las nubes públicas

Las nubes públicas ofrecen comodidad, ahorro de costes 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 vNSP admite Amazon Web Services (AWS), Microsoft Azure y Oracle Cloud Infrastructure (OCI), los servicios de la nube pública líderes en la actualidad, por lo que ofrece visibilidad total de amenazas y protección de los datos a través de un gateway de Internet o de servidor a servidor (tráfico este-oeste).

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 y cargas de trabajo 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 las nubes privadas y públicas, así como en los centros de datos definidos por software (SDDC).

Ventajas principales

- Protección completa para nubes públicas y privadas (AWS, Azure y OCI)
- Protección verdadera del tráfico este-oeste
- Consola de administración centralizada para facilitar el control y la visibilidad
- Tecnologías de inspección avanzadas para protegerse frente a las amenazas conocidas y desconocidas
- Alta disponibilidad, recuperación ante desastres y equilibrio de carga, para mejorar el rendimiento
- Uso compartido de licencias en la nube, para disfrutar de flexibilidad en nubes públicas y privadas
- Integración con la cartera de soluciones de McAfee, para ofrecer seguridad del dispositivo a la nube
- Disponible en **AWS Marketplace**
- Disponible en **Azure Marketplace**

Síganos

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.

Agilidad en las nubes privadas

McAfee vNSP se integra perfectamente con las plataformas de nube privada más populares, como los entornos SDN basados en VMware NSX y OpenStack. McAfee vNSP 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 avanzadas

McAfee vNSP 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 vNSP incorpora varios motores de detección con firmas y sin firmas para evitar que el malware no deseado cause estragos en su red. Esta solución emplea varias 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 vNSP también identifica y bloquea 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 profundos de código estático (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. Además, McAfee ofrece soporte nativo para firmas Snort con el fin de detectar y proteger frente al malware.

Más información

- **Protección de sus redes virtuales Amazon Web Services**
- **Protección de sus redes virtuales Microsoft Azure**

Uso compartido de licencias de la nube, con flexibilidad

Las grandes empresas con frecuencia reparten su infraestructura y sus recursos de TI entre varias nubes y plataformas, ya sea para mantener la compatibilidad con aplicaciones heredadas, para reducir la dependencia de un solo proveedor, para mejorar la redundancia de sistemas o para ahorrar costes. 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 costes gracias al uso compartido de licencias para la nube, que permite a las empresas compartir sus licencias de McAfee vNSP en cualquier combinación de plataformas de nubes públicas y privadas. El uso compartido de licencias de la nube ofrece flexibilidad y 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 estén, sin tener que pasar por el largo proceso de adquisición de licencias completo.

Flujos de trabajo y análisis más sencillos

Las amenazas modernas pueden generar grandes volúmenes de alertas, que ponen a prueba la capacidad del operador de seguridad para priorizarlas y supervisarlas. Si la respuesta es demasiado lenta, las amenazas pueden entrar sin ser detectadas. McAfee vNSP incluye análisis avanzados y flujos de trabajo prácticos que correlacionan varias alertas de IPS en un solo evento, para que los administradores puedan identificar rápidamente la información relevante. Además, la integración con otras soluciones de seguridad de McAfee crea una verdadera plataforma de detección y mitigación de amenazas que llegan a través de la red, global y conectada.

Administración centralizada para obtener visibilidad y control en tiempo real

Con un solo dispositivo McAfee Network Security Manager es posible disfrutar de una administración centralizada y basada en la Web, para obtener visibilidad y control en tiempo real. La innovadora consola le proporciona el control de los datos en tiempo real a través de un solo panel. Ahora puede 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 entornos tradicionales o en la nube pública o privada. La intuitiva interfaz también se escala para gestionar los clústeres esenciales que están muy distribuidos.

McAfee Network Security Manager también puede instalarse como instancia virtual en los servidores VMware ESX o en entornos AWS o Azure. McAfee vNSP admite AWS Identity and Access Management (IAM), por lo que permite a los administradores gestionar rápida y fácilmente el acceso a los servicios y recursos AWS en función de los permisos asignados a cada usuario y grupo.

Alta disponibilidad, recuperación ante desastres y equilibrio de carga

McAfee vNSP proporciona de forma automática control, protección y rendimiento ininterrumpidos, a través de varios métodos. McAfee Network Security Manager ofrece una gran disponibilidad mediante la supervisión proactiva del entorno. Si un controlador activo deja de estar disponible, McAfee Network Security Manager realiza automáticamente una conmutación por error a un controlador de reserva, para que no se interrumpan la visibilidad ni la seguridad. Además, se puede desplegar un McAfee Network Security Manager de reserva para la recuperación ante desastres en entornos AWS, Azure y OCI.

McAfee vNSP también ofrece una alta disponibilidad para sensores de IPS. Si un sensor deja de estar disponible, la función de escalación automática crea automáticamente un nuevo IPS virtual para proporcionar una protección continua impecable. Asimismo, si aumenta el tráfico de la red, el equilibrio de carga automático entre los sensores garantiza la optimización del rendimiento, y se pueden desplegar más sensores automáticamente para satisfacer el rendimiento exigido.

Seguridad integrada

Los ataques sofisticados no respetan los límites de los productos, y aprovecharán rápidamente cualquier brecha en la infraestructura, especialmente si se trata de productos de seguridad. McAfee vNSP es el único sistema de prevención de intrusiones (IPS) que se integra perfectamente en varios productos de seguridad, aprovechando con eficiencia datos y flujos de trabajo en distintas soluciones con el fin de proporcionar una seguridad y una protección excelentes, y una mejor rentabilidad. Estos son algunos ejemplos de la integración de las soluciones de seguridad de McAfee:

- **McAfee ePolicy Orchestrator® (McAfee ePO™):** visibilidad total de los endpoints para todos los eventos y alertas de IPS.
- **McAfee Endpoint Intelligence Agent:** combina las perspectivas 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:** inspección profunda para detectar amenazas evasivas.

- **McAfee Cloud Threat Detection:** un servicio que se integra en las soluciones de McAfee para detectar el malware avanzado.
- **McAfee Management for Optimized Virtual Environments (McAfee MOVE):** una solución antivirus para entornos virtuales.
- **Analizadores de vulnerabilidades de terceros:** análisis de riesgo y de hosts para los endpoints.

Funciones adicionales

Prevención de amenazas avanzadas

- Motor de emulación de McAfee Gateway Anti-Malware:
- Motor de emulación 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 control y mando

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 velocidad
- Inspección de entornos virtuales
- Prevención de denegación de servicio (DoS) y denegación de servicio distribuida (DDoS)
- Mejoras de lista blanca/lista negra para admitir Structured Threat Information eXpression (STIX)
- Detección basada en umbrales y en análisis heurístico
- Limitación de conexiones específicas de hosts
- Compatibilidad nativa con firmas Snort
- Detección basada en perfil con autoaprendizaje

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
Plataforma	VMware ESX 5.5/6.0/6.5	AWS Azure OCI VMware vSphere 6.5 y NSX 6.3
Modelo de sensor de IPS virtual	**IPS-VM600**	**IPS-VM600-VSS**
Tipo de despliegue de IPS virtual	Independiente	Distribuido
Compatibilidad con VMware NSX	No	Sí
Compatibilidad con AWS	No	Sí
Compatibilidad con Azure	No	Sí
Compatibilidad con OCI	No	Sí
Número de CPU lógicas	4	AWS 4, Azure 5
Memoria necesaria	6 GB	6 GB
Almacenamiento	8 GB	8 GB
Especificaciones del sensor virtual		
Rendimiento máximo	Hasta 1 Gbit/s	Hasta 1 Gbit/s
Número de pares de puertos de supervisión	3	1 (puerto de supervisión, no un par de puertos)
Interfaces virtuales (VIDS) por sensor	100	100
Perfiles de DoS	300	300
Puerto de administración	Sí	Sí
Puerto de respuesta	No	No
Modos de despliegue	Inspección entre máquinas virtuales, físico-máquina virtual, físico-físico, de puertos SPAN/en línea	

McAfee
Together is power.

Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas, Madrid, España
+34 91 347 85 00
www.mcafee.com/es