VMware NSX: La plataforma para la virtualización de la red

La virtualización de red y el centro de datos definido por software (SDDC)

VMware NSX ofrece un modelo operativo totalmente nuevo para la red que conforma la base del centro de datos definido por software. Dado que NSX crea redes en el software, los operadores del centro de datos pueden lograr unos niveles de agilidad, seguridad y economía que antes eran imposibles con las redes físicas. NSX ofrece todo un conjunto de elementos y servicios de red lógicos, como conmutadores lógicos, enrutadores, cortafuegos, equilibrio de carga, VPN, calidad de servicio (QoS) y supervisión. Estos servicios se implementan en redes virtuales mediante cualquier plataforma de gestión de la cloud que aproveche las API de NSX. Las redes virtuales se implementan sin interrupciones en cualquier hardware de red existente.

INFORMACIÓN BÁSICA

VMware NSX® es una plataforma de virtualización de red para el centro de datos definido por software (SDDC) que ofrece el modelo operativo de una máquina virtual para redes completas. Con NSX, las funciones de red, incluida la conmutación, el

enrutamiento y los cortafuegos están integradas en el hipervisor y distribuidas en el entorno. Esto crea de manera eficaz un «hipervisor de red» que sirve de plataforma para los servicios y redes virtuales. De forma parecida al modelo operativo de las máquinas virtuales, las redes virtuales se implementan mediante

programación y se gestionan de forma independiente al hardware subyacente. NSX reproduce todo el modelo de red en software, lo que permite la creación

y la implementación de cualquier topología de red, desde redes sencillas hasta redes complejas de varios niveles, en cuestión de segundos. Los usuarios pueden crear varias redes virtuales con diversos requisitos, aprovechando una combinación de los servicios

PRINCIPALES VENTAJAS

- **Microsegmentación y seguridad detallada proporcionada a la carga de trabajo individual**
- **Menor tiempo de implementación de la red, de días a segundos, además de mejor eficiencia operativa a través de la automatización**
- **Movilidad de la carga de trabajo independiente de la topología de la red física en los centros de datos y entre ellos**
- **Mayor seguridad y servicios de red avanzados a través de un ecosistema formado por los principales proveedores**

CARACTERÍSTICAS PRINCIPALES

Conmutación	Permite las extensiones de superposición de capa 2 lógicas en una estructura enrutada (capa 3) dentro y a través de los límites del centro de datos. Compatibilidad con superposiciones de redes basadas en VXLAN.
Enrutamiento	Enrutamiento dinámico entre redes virtuales realizado de una manera distribuida en el kernel del hipervisor, enrutamiento de escalabilidad horizontal con conmutación por error activa-activa con enrutadores físicos. Compatibilidad con protocolos de enrutamiento estático y dinámico (OSPF, BGP).
Cortafuegos distribuido	Cortafuegos con estado distribuido, incorporado en el kernel del hipervisor para hasta 20 Gbps de capacidad de cortafuegos por host de hipervisor. Compatible con Active Directory y supervisión de actividad. Asimismo, NSX también puede proporcionar funciones de cortafuegos de norte a sur a través de NSX Edge™.
Equilibrio de carga	Equilibrador de carga de capas de 4 a 7 con descarga y traspaso de SSL, comprobación del estado del servidor y reglas de aplicaciones para programación y manipulación del tráfico.
VPN	Funciones VPN de acceso remoto y de sitio a sitio, VPN no gestionado para servicios de puerta de enlace de la cloud.
Puerta de enlace de NSX	Compatibilidad de conexión entre VXLAN y VLAN para una conexión perfecta con las cargas de trabajo del entorno físico. Esta función es nativa de NSX y la ofrecen los conmutadores de la parte superior del rack desde un partner del ecosistema.

www.inycom.es
info@inycom.es
+34 902 995 820

API de NSX	API de RESTful para la integración en cualquier plataforma de gestión de la cloud o automatización personalizada.
Operaciones	Funciones de operaciones nativas, como CLI central, Traceflow, SPAN e IPFIX para la solución de problemas y la supervisión proactiva de la infraestructura. Integración con herramientas como VMware vRealize® Operations™ y vRealize Log Insight™ para técnicas de análisis y solución de problemas avanzadas.
Política de seguridad dinámica	NSX Service Composer permite la creación de grupos de seguridad dinámicos. Más allá de la dirección IP y MAC, la pertenencia a grupos de seguridad se puede basar en etiquetas y objetos de VMware vCenter™, el tipo de sistema operativo y las funciones de Active Directory para habilitar una función de aplicación de seguridad dinámica.
Gestión de la cloud	Integración nativa con vRealize Automation™ y OpenStack.
Integración con otros partners	Soporte de la integración de la gestión, el plano de control y de datos con otros partners en una gran variedad de categorías, como cortafuegos de nueva generación, sistema de prevención y detección de intrusiones (IDS/IPS), antivirus sin agente, controladores de despliegue de aplicaciones, conmutación, operaciones y visibilidad, seguridad avanzada, entre otros.
Redes y seguridad más allá de vCenter	Amplíe las redes y la seguridad más allá de los límites de vCenter y el centro de datos, con independencia de la topología física, lo que permite funciones como la recuperación ante desastres y los centros de datos activo-activo.
Gestión de registros	Ayude a resolver problemas más rápidamente con la mayor visibilidad de vRealize Log Insight para NSX. Visualice tendencias de eventos, active alertas, etc., todo ello en tiempo real.

AUTOMATIZACIÓN

NSX soluciona los problemas derivados del tiempo que se tarda en implementar la red, además de los errores de configuración y los costosos procesos al automatizar tareas muy laboriosas y que son susceptibles a errores. NSX crea redes en el software, lo que elimina los cuellos de botella asociados a las redes basadas en hardware.

La integración nativa de NSX con las plataformas de gestión de la cloud, como vRealize Automation u OpenStack, permiten una mayor automatización.

CONTINUIDAD DE LAS APLICACIONES

Dado que NSX abstrae la red del hardware subyacente, las políticas de red y seguridad están conectadas a sus cargas de trabajo asociadas. Las organizaciones pueden replicar fácilmente entornos de aplicaciones completos en centros de datos remotos para la recuperación ante desastres, trasladarlos de un centro de datos corporativo a otro o desplegarlos en un entorno de cloud híbrida, todo en cuestión de minutos y sin interrumpir las aplicaciones ni tocar la red física.

EDICIONES DE VMWARE NSX

Las nuevas soluciones de NSX permiten que más clientes satisfagan sus requisitos específicos de virtualización de red para emprender su viaje al centro de datos definido por software.

- **Standard**

Para organizaciones que necesitan agilidad y automatización de la red

- **Advanced**

Para organizaciones que necesitan la versión Standard, además de un centro de datos fundamentalmente más seguro con microsegmentación

- **Enterprise**

Para organizaciones que necesitan la versión Advanced, más redes y seguridad en varios dominios

AUTOMATIZACIÓN

- **Standard**

NSX permite a las organizaciones dividir de manera lógica el centro de datos en distintos segmentos de seguridad hasta el nivel de la carga de trabajo individual, con independencia de la subred o VLAN de la red de la carga de trabajo. Luego, los equipos de TI pueden definir políticas de seguridad y controles para cada carga de trabajo con base en grupos de seguridad dinámicos, lo que garantiza respuestas inmediatas a las amenazas internas del centro de datos y la exigencia del cumplimiento hasta el nivel de máquina virtual individual.

A diferencia de las redes tradicionales, si un atacante traspasa las defensas perimetrales del centro de datos, las amenazas no se pueden mover lateralmente en el centro de datos.