VMWARE NSX

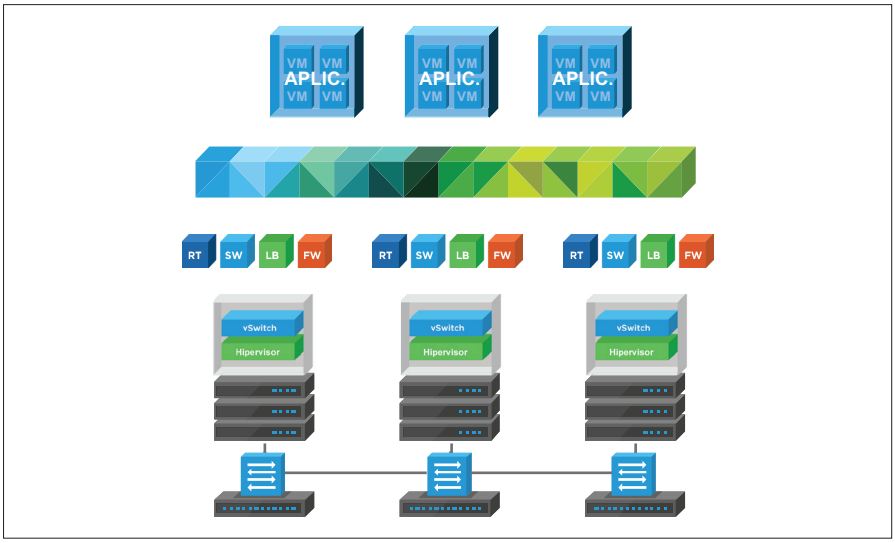
La plataforma de virtualización de redes

PRESENTACIÓN GENERAL

VMware NSX® es la plataforma de virtualización de redes para el centro de datos definido por software (Software-Defined Data Center, SDDC) que permite suministrar el modelo operacional de una máquina virtual para redes enteras. Con NSX, las funciones de red, incluidos los enrutamientos, las conmutaciones y la protección de firewall, están incorporadas en el hipervisor y distribuidas en el entorno. Gracias a esto, se crea un "hipervisor de red" que actúa como una plataforma para servicios y redes virtuales. De manera similar al modelo operacional de las máquinas virtuales, las redes virtuales se aprovisionan y administran programáticamente, independientemente del hardware subyacente. Mediante NSX, se reproduce el modelo de red completo en el software, lo que permite la creación y el aprovisionamiento en segundos de cualquier topología de red, desde redes simples hasta redes complejas de múltiples niveles. Los usuarios pueden crear múltiples redes virtuales con diversos requisitos y aprovechar una combinación de los servicios que se ofrecen mediante NSX para diseñar entornos inherentemente más seguros.

VENTAJAS CLAVE

- Suministro de microsegmentación y seguridad detallada para la carga de trabajo individual
- Reducción del tiempo de aprovisionamiento de redes de días a segundos y eficiencia operacional mejorada por medio de la automatización
- Movilidad de la carga de trabajo independiente de la topología de red física entre los centros de datos y dentro de ellos
- Seguridad mejorada y servicios de red avanzados por medio de una red de proveedores líderes de terceros



La virtualización de redes y el centro de datos definido por software

Con VMware NSX, se suministra un modelo operacional para redes completamente nuevo que se convierte en la base del centro de datos definido por software. Debido a que NSX permite diseñar redes en el software, los operadores del centro de datos pueden alcanzar niveles de agilidad, seguridad y rentabilidad que eran inalcanzables con las redes físicas. Mediante NSX se proporciona un conjunto completo de elementos y servicios de red lógicos que incluye switches lógicos, enrutamiento, protección de firewall, balanceo de carga, red privada virtual (Virtual Private Network, VPN), calidad de servicio (Quality of Service, QoS) y monitoreo. Estos servicios se aprovisionan en redes virtuales por medio de cualquier plataforma de administración de la nube, lo que permite aprovechar las interfaces de programación de aplicaciones (Application Programming Interface, API) de NSX. Las redes virtuales se implementan de manera no disruptiva en cualquier hardware de red existente.

Funciones clave de NSX

Conmutación	Permite un overlay de la capa 2 lógica sobre extensiones en una estructura de conexión enrutada (capa 3, C3) dentro de los límites del centro de datos y entre ellos. Compatibilidad con overlays de redes basadas en LAN virtual extensible (Virtual eXtensible LAN, VXLAN).
Enrutamiento	Enrutamiento dinámico entre redes virtuales implementado de manera distribuida en el kernel del hipervisor, enrutamiento con escalabilidad horizontal y con conmutación de recuperación activo-activo mediante enrutadores físicos. Enrutamiento estático y enrutamiento dinámico compatibles con protocolos (OSPF, BGP).

Protección de firewall distribuida	Protección de firewall distribuida sin pérdida de estado, incorporada en el kernel del hipervisor para hasta 20 Gbps de capacidad de firewall por host hipervisor. Compatibilidad con Active Directory y monitoreo de actividad. Además, NSX también puede proporcionar capacidad de firewall de norte a sur por medio de NSX Edge™.
Balanceo de carga	Balanceador de carga C4–C7 con descarga y transferencia de capa de sockets seguros (Secure Socket Layer, SSL), comprobación del estado del servidor y reglas de aplicación para la programación y la manipulación de tráfico.
VPN	Capacidades de VPN de sitio a sitio y de acceso remoto, VPN no administrado para servicios de puerta de enlace de nube.
Puerta de enlace de NSX	Compatibilidad con conexión de VXLAN a VLAN para conexiones sin problemas a cargas de trabajo físicas. Esta capacidad es al mismo tiempo nativa de NSX y suministrada por switches de la parte superior del rack de una red de socios.
NSX API	API basada en RESTful para la integración a cualquier plataforma de administración de la nube o automatización personalizada.
Operaciones	Capacidades de operaciones nativas como la interfaz de línea de comando (Command Line Interface, CLI), Traceflow, el analizador de puerto de switch (Switch Port Analyzer, SPAN) y el protocolo de exportación de información de flujo (IP Flow Information Export, IPFIX) para solucionar problemas y monitorear la infraestructura de forma anticipativa. Integración con herramientas como VMware vRealize® Operations™ y vRealize Log Insight™ para técnicas avanzadas de análisis y solución de problemas. Gracias al Application Rule Manager (administrador de reglas de aplicaciones) y al Endpoint Monitoring (monitoreo de terminales) de NSX, se obtiene una visualización integral de los flujos de tráfico en la red hasta la capa 7. Esto permite que los equipos de aplicaciones identifiquen terminales dentro del centro de datos y entre centros de datos, y respondan mediante la creación de reglas de seguridad adecuadas.
Políticas de seguridad dinámica	El compositor de servicios de NSX permite la creación de grupos de seguridad dinámicos. Más allá de la dirección IP y MAC, la membresía de los grupos de seguridad se puede basar en objetos y etiquetas de VMware vCenter™, en el tipo de sistema operativo y en los roles de Active Directory para permitir una capacidad de cumplimiento de seguridad dinámica.
Administración de la nube	Integración nativa con vRealize Automation™ y OpenStack.
Integración de socios de terceros	Compatibilidad con la integración del plano de datos, el plano de control y la administración con socios de terceros en una gran variedad de categorías, como firewall de próxima generación, sistema de detección de intrusos (Intrusion Detection System, IDS) e instrucciones por segundo (Instructions Per Second, IPS), antivirus sin agentes, controladores de suministro de aplicaciones, conmutaciones, operaciones y visibilidad, seguridad avanzada y más.
Seguridad y redes de Cross vCenter	Extienda la seguridad y las redes en vCenter y a través de los límites del centro de datos independientemente de la topología física subyacente, lo que permite obtener capacidades como la recuperación ante desastres y los centros de datos activo-activo.
Administración de registros	Solucione problemas con mayor rapidez gracias a la visibilidad incorporada que ofrece vRealize Log Insight para NSX. Visualice tendencias de eventos, active alertas y mucho más, todo en tiempo real.

Casos de uso

Seguridad

Gracias a NSX, las organizaciones pueden dividir de manera lógica el centro de datos en distintos segmentos de seguridad hasta el nivel de carga de trabajo individual, independientemente de la subred o red de área local virtual (Virtual LAN, VLAN) de la red de carga de trabajo. Por lo tanto, los equipos de TI pueden definir las políticas y los controles de seguridad para cada carga de trabajo, según los grupos de seguridad dinámicos. Esto garantiza respuestas inmediatas a las amenazas dentro del centro de datos y su aplicación en la máquina virtual individual. A diferencia de las redes tradicionales, si un atacante supera las defensas del perímetro del centro de datos, las amenazas no se pueden mover de forma lateral dentro del centro de datos.

Automatización

Con NSX se abordan los desafíos de aprovisionamiento prolongado de redes, errores de configuración y procesos costosos mediante la automatización de tareas arduas y propensas a errores. NSX permite crear redes en el software y eliminar los embotellamientos propios de las redes basadas en el hardware.

La integración nativa de NSX con plataformas de administración de la nube, como vRealize Automation u OpenStack, permite una mayor automatización.

Continuidad de las aplicaciones

Debido a que en NSX se extraen redes desde el hardware subyacente, las políticas de redes y seguridad están relacionadas con las cargas de trabajo asociadas. Las organizaciones pueden replicar fácilmente entornos de aplicaciones completos en centros de datos remotos para la recuperación ante desastres, migrarlos desde un centro de datos corporativo hasta otro o implementarlos en un entorno de nube híbrida. Todo esto se realiza en minutos, sin afectar el funcionamiento de las aplicaciones y sin tocar la red física.

Ediciones de VMware NSX

Las ofertas nuevas de NSX permiten que más clientes puedan cumplir los requisitos específicos de virtualización de red para comenzar el cambio hacia el centro de datos definido por software.

Standard

Para organizaciones que necesitan agilidad y automatización de la red

Advanced

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

Enterprise

Para organizaciones que necesitan la edición Advanced, más redes y seguridad en múltiples dominios

MÁS INFORMACIÓN

Para obtener más información, visite http://www.vmware.com/go/products/nsx.

Se pueden consultar los detalles adicionales sobre las funciones de asignación de licencias de las ediciones de NSX en https://kb.vmware.com/kb/2145269.

Para obtener información sobre todos los productos de VMware o para realizar una compra, llame al 877-4-VMWARE (fuera de Norteamérica, marque +1-650-427-5000), visite http://www.vmware.com/latam/products o busque un revendedor autorizado en línea.

	STANDARD	ADVANCED	ENTERPRISE
Conmutaciones y enrutamientos distribuidos	•	•	•
Firewall de NSX Edge	•	•	•
NAT	•	•	•
Conexión de C2 del software al entorno físico	•	•	•
Enrutamiento dinámico con ECMP (activo-activo)	•	•	•
Automatización regida por API	•	•	•
Integración con vRealize y OpenStack	•	•	•
Administración de registros con vRealize Log Insight para NSX	•	•	•
Automatización de las políticas de seguridad con vRealize		•	•
Balanceo de carga de NSX Edge		•	•
Protección de firewall distribuida		•	•
Integración con Active Directory		•	•
Monitoreo de la actividad del servidor		•	•
Inserción de servicios (integración de terceros)		•	•
Integración con VMware AirWatch®		•	•
Application Rule Manager		•	•
NSX a través de vCenter			•
Optimizaciones de NSX en múltiples sitios			•
VPN (IPSEC y SSL)			•
Puerta de enlace remota			•
Integración con los VTEP de hardware			•
Endpoint Monitoring			•

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel. 877-486-9273 Fax 650-427-5001 www.vmware.com/latam.