VMWARE NSX

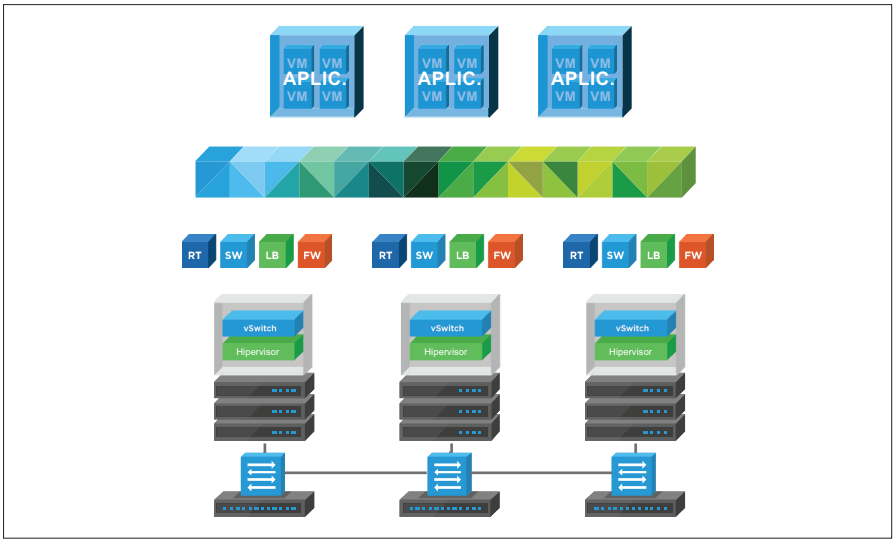
La plataforma de seguridad y virtualización de redes

PRESENTACIÓN GENERAL

VMware NSX® es la plataforma de seguridad y 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. De este modo, se crea eficazmente un "hipervisor de red" que actúa como una plataforma para servicios de seguridad y redes virtuales. De manera similar al modelo operacional de las máquinas virtuales, las redes virtuales se aprovisionan y administran de manera programática, 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



Virtualización de redes, seguridad y SDDC

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, entre los que se incluyen 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 instancias de NSX API. Las redes virtuales se implementan de manera no disruptiva en cualquier hardware de red existente.

Funciones clave de NSX

Conmutación	Permite extensiones de overlay de la capa 2 lógica 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 realizado de manera distribuida en el kernel del hipervisor, enrutamiento con escalabilidad horizontal y con conmutación de recuperación activo-activo, mediante enrutadores físicos. Compatibilidad con protocolos de enrutamiento estático y enrutamiento dinámico (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 administrada para servicios de puerta de enlace de nube.
Puerta de enlace de NSX	Compatibilidad con conexión de VXLAN a VLAN para conexiones a cargas de trabajo físicas sin problemas. Esta capacidad es nativa de NSX y es suministrada por switches de la parte superior del rack de un socio de la red.
NSX API	API basada en RESTful para la integración en cualquier plataforma de administración de la nube o automatización personalizada.
Operaciones	Capacidades de operaciones nativas como la interfaz de línea de comando central (Command Line Interface, CLI), Traceflow, el analizador de puerto de switch (Switch Port Analyzer, SPAN) y la exportación de información de flujo de protocolo de Internet (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 a Application Rule Manager (Administrador de reglas de aplicaciones) y a Endpoint Monitoring (Monitoreo de terminales) de NSX, se obtiene una visualización integral de los flujos de tráfico de 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.
Microsegmentación con reconocimiento del contexto	Con NSX, es posible crear grupos de seguridad dinámicos y políticas asociadas en función de factores que van más allá de la dirección de protocolo de Internet (Internet Protocol, IP) y la dirección de control de acceso a medios (Media Access Control, MAC), incluidos los objetos y las etiquetas de VMware vCenter™, el tipo de sistema operativo e información sobre las aplicaciones de capa 7, para permitir la microsegmentación basada en el contexto de la aplicación. Las políticas basadas en la identidad que usan información de inicio de sesión de máquinas virtuales (Virtual Machine, VM), de Active Directory y de la integración de administración de dispositivos móviles permiten la seguridad basada en el usuario, lo que incluye seguridad en el nivel de la sesión en entornos remotos y de escritorios virtuales.
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 a través de 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 recuperación ante desastres y centros de datos activo-activo.
Administración de registros	Solucione problemas con mayor rapidez gracias a la visibilidad incorporada que ofrece vRealize Log Insight for NSX. Visualice tendencias de eventos, active alertas y mucho más, todo en tiempo real.

Casos de uso

Seguridad

NSX les 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, independientemente de la subred o red de área local virtual (Virtual LAN, VLAN) de la red de la 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 del aprovisionamiento prolongado de redes, los errores de configuración y los procesos costosos mediante la automatización de tareas arduas y propensas a errores. NSX permite crear redes en el software y eliminar los cuellos de botella 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 separan las redes del 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

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

Sucursales y oficinas remotas

Para organizaciones que desean virtualizar y proteger aplicaciones en sucursales u oficinas remotas

MÁS INFORMACIÓN

Para obtener más información, visite www.vmware.com/go/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 www.vmware.com/latam/products o busque un revendedor autorizado en línea.

	STANDARD	ADVANCED	ENTERPRISE	SUCURSALES Y OFICINAS REMOTAS
Conmutación distribuida	•	•	•	•*
Enrutamiento distribuido	•	•	•	
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 for NSX	•	•	•	•
Automatización de las políticas de seguridad con vRealize		•	•	•
Balanceo de carga de NSX Edge		•	•	•
Firewall distribuido (incluida la 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			•	
Monitoreo de terminales			•	
Firewall distribuido con capa 7			•	

*Respaldado por VLAN

vmware®

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

N.º de elemento: 117478wf-vmw-fy18q4-sddc-launch-ds-nsx-a4-web
1/18