VMWARE NSX CLOUD

Redes y seguridad coherentes para aplicaciones que se ejecutan de forma nativa en clouds públicas

INFORMACIÓN BÁSICA

VMware NSX® Cloud ofrece unas redes y una seguridad coherentes para aplicaciones que se ejecutan de forma nativa en la cloud pública. NSX Cloud usa el mismo plano de gestión y el mismo plano de control que NSX Data Center, habilitando una sola solución de redes y seguridad desde el centro de datos privado hasta la cloud pública.

VENTAJAS PRINCIPALES

Las funciones de redes y de seguridad comunes en clouds públicas, como AWS y Azure, mejoran considerablemente la escalabilidad, el control y la visibilidad, con unos gastos operativos inferiores.

- Escalabilidad sencilla en redes virtuales, zonas de disponibilidad, regiones y clouds públicas.
- Control preciso de los servicios de redes y de seguridad que ofrece protección y estandarización a las aplicaciones.
- Visibilidad integral de las redes y de la seguridad que garantiza el buen estado y el cumplimiento de las aplicaciones en las clouds públicas.

PRECIOS

- Precios basados en suscripciones, con licencias temporales de 1 y 3 años.
- Se basan en el número de vCPU usadas por las cargas de trabajo activadas en la cloud pública, con independencia del número de redes virtuales (p. ej., VPC de AWS, VNet de Azure).
- No se requiere una licencia de NSX Data Center para casos de uso en la cloud únicamente.

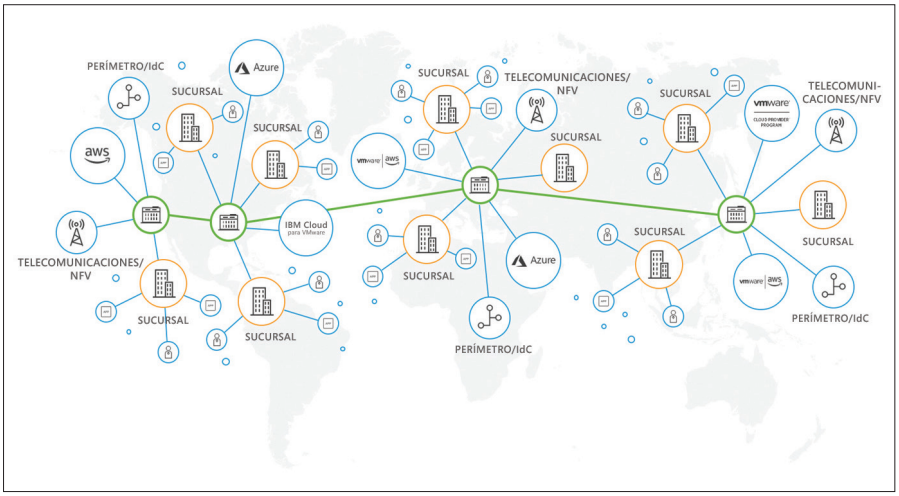

Figura 1: La red de la cloud virtual

Una red basada en los fundamentos de la cloud

VMware NSX Cloud ofrece redes y seguridad para las aplicaciones que se ejecutan de forma nativa en clouds públicas. Junto con la familia de productos VMware NSX, VMware NSX Cloud habilita una red de la cloud virtual, un enfoque definido por software de la red que se extiende a centros de datos, clouds, terminales y objetos.

Casos de uso

Seguridad uniforme en diversas clouds

NSX Cloud aplica una política en las cargas de trabajo que se ejecutan en múltiples clouds públicas. NSX Cloud usa el mismo plano de control y el mismo plano de datos que NSX Data Center, lo que permite una gestión integral de políticas en los centros de datos y en las clouds. La política se define una sola vez y se aplica a las cargas de trabajo en todas partes: en distintas redes virtuales de cloud, regiones, zonas de disponibilidad y múltiples proveedores de cloud. Las políticas de seguridad se aplican de forma dinámica a cada carga de trabajo en función de los atributos de la aplicación y las etiquetas definidas por el usuario. Incluso puede poner en cuarentena automáticamente las cargas de trabajo no autorizadas o en peligro si no cuentan con la política de seguridad de microsegmentación adecuada.

Control preciso de las redes de cloud

VMware NSX Cloud se ha diseñado para entornos de cloud pública nativa, como Amazon (AWS) y Microsoft Azure. NSX Cloud complementa los servicios nativos de estos proveedores de cloud pública. Con NSX Cloud puede seguir utilizando la infraestructura y los servicios de aplicaciones del proveedor de cloud pública para cargas de trabajo sin limitaciones (p. ej., AWS ELB/Azure Load Balancer, AWS Route53/Azure DNS, AWS Direct Connect/Azure ExpressRoute y Amazon RDS/Azure Database). La gestión de la implementación y la configuración se puede automatizar por medio de solicitudes de API de REST usando las herramientas de automatización que ya tiene.

PARA OBTENER MÁS INFORMACIÓN O ADQUIRIR PRODUCTOS DE VMWARE,

LLAME AL NÚMERO DE TELÉFONO
+34 914125000 (si no está en España, marque el 877-4-VMWARE si se encuentra en Norteamérica o el +1 6504275000 desde el resto del mundo),

VISITE
www.vmware.com/es/products/nsx-cloud.html o http://www.vmware.com/es/products para buscar en Internet un distribuidor autorizado.

Visibilidad y control operativo integrales

VMware NSX Cloud proporciona interfaces y protocolos estándar para acceder a los datos de redes y de seguridad que necesita obtener de sus redes de cloud. La información sobre flujos, paquetes y eventos está disponible a través de IPFIX, Traceflow, Port Mirroring y Syslog. Estos datos los pueden utilizar sus herramientas de operaciones locales, y se pueden emplear para obtener una visibilidad en profundidad e integral de las supervisiones, la solución de problemas y las auditorías. Son datos de operaciones de gran riqueza, útiles para reducir drásticamente el tiempo necesario para detectar y solucionar los problemas de conectividad de red, rendimiento y seguridad en toda la implementación de cloud híbrida, incluidas las aplicaciones locales y en la cloud pública.

Características principales

Redes y seguridad multicloud en varios sitios: NSX Cloud ofrece funcionalidades de redes y de seguridad para terminales en múltiples clouds, y se integra con NSX Data Center para proporcionar gestión de las redes y la seguridad en clouds y centros de datos.

Microsegmentación: control sobre el tráfico este-oeste entre cargas de trabajo de aplicaciones que se ejecutan de forma nativa en las clouds públicas.

Grupos de seguridad: los grupos y las reglas de seguridad se pueden definir basándose en estructuras de políticas con riqueza de información como el nombre de instancia, el tipo de sistema operativo, el ID de AMI y las etiquetas definidas por el usuario.

Política dinámica: la política de seguridad se aplica automáticamente en función de atributos de instancia y de etiquetas definidas por el usuario. Las políticas siguen automáticamente a las instancias cuando estas se mueven dentro de las clouds y entre clouds.

Instancias en cuarentena: ponga en cuarentena las cargas de trabajo no autorizadas o vulnerables que se ejecuten en la cloud pública sin seguridad de microsegmentación. Las instancias en cuarentena no pueden comunicarse en la red de la cloud.

Arquitectura distribuida: la arquitectura de cortafuegos distribuida de NSX Cloud elimina los saltos de red y el tráfico adicionales gracias a que las políticas se aplican en la interfaz de red virtual de cada instancia, en lugar de enrutarse a través de un cortafuegos externo.

Cortafuegos perimetral: NSX Cloud incluye un cortafuegos con estado que filtra el tráfico norte-sur entre instancias, en redes virtuales y la Internet pública.

API RESTful: API RESTful y herramientas de automatización para implementar y configurar de forma programada la infraestructura de redes y seguridad según las necesidades.

Plantillas: utilice las herramientas de automatización y coordinación existentes para crear plantillas de aplicación estandarizadas y simplificar la prestación y la gestión de servicios de redes y seguridad en clouds públicas.

Visibilidad del tráfico este-oeste: utilice las herramientas de operaciones posteriores para obtener visibilidad del tráfico este-oeste dentro de las VPC y entre ellas.

Registro de seguridad: visibilidad y auditoría en tiempo real de eventos de seguridad como permisos y denegaciones o incidentes de cuarentena. Envíe información de eventos de seguridad a un servidor Syslog o SIEM.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
C/ Rafael Botí, 26 · 2.ª planta, 28023 Madrid, España. Tel. +34 914125000 Fax +34 914125001 www.vmware.com/es

N.º artículo: 149451wf-vmw-q2fy19-sddc-launch-ds-nsx-cld-a4
6/18