VMware NSX Cloud

Redes y seguridad de nube híbrida en nubes privadas y públicas

INFORMACIÓN BÁSICA

VMware NSX Cloud™ ofrece redes y seguridad uniformes para aplicaciones que se ejecutan de forma nativa en la nube pública. NSX Cloud usa los mismos planos de gestión y de control que VMware NSX® Data Center mediante una sola solución de red y seguridad desde el centro de datos privado hasta la nube pública.

VENTAJAS PRINCIPALES

Los sistemas de red y seguridad comunes en nubes públicas, como AWS y Azure, mejoran considerablemente la escalabilidad, el control y la visibilidad, además de reducir los gastos operativos:

- Flexibilidad de implementación mediante estructuras de NSX o estructuras nativas de la nube pública
- Escalabilidad sencilla en redes virtuales, zonas de disponibilidad, regiones y nubes públicas
- Control preciso de los servicios de red y de seguridad que ofrece protección y estandarización a las aplicaciones
- Visibilidad integral de la red y la seguridad que garantiza el correcto funcionamiento y la conformidad de las aplicaciones en las nubes públicas

PRECIOS

- Los precios se basan en un modelo de suscripciones, con licencias temporales de uno y tres años de duración.
- Varían en función de las vCPU que se utilizan según las cargas de trabajo activas en la nube pública, con independencia del número de redes virtuales, como AWS Virtual Private Cloud (VPC) y Azure Virtual Network (VNet).
- No se requiere una licencia de NSX Data Center para casos de uso exclusivos de la nube.
- Consulte la guía de productos de VMware para obtener más información sobre la portabilidad de las licencias de NSX Data Center Enterprise Plus a NSX Cloud.

Una red basada en los fundamentos de la nube

VMware NSX Cloud ofrece red y seguridad para las aplicaciones que se ejecutan de forma nativa en nubes públicas. Junto con la familia de productos VMware NSX, VMware NSX Cloud hace posible una red de nube virtual, un enfoque de red definido por software que abarca centros de datos, nubes, terminales y objetos.

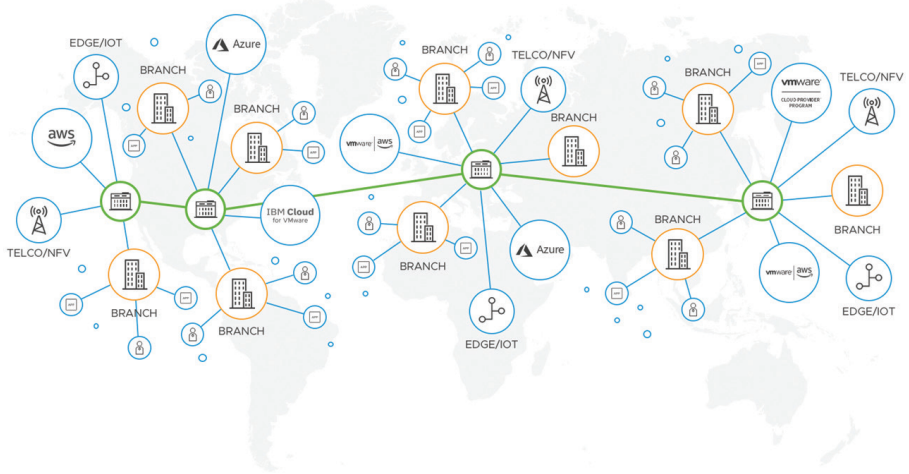

FIGURA 1: La red de nube virtual.

Casos de uso

Seguridad uniforme en diversas nubes

NSX Cloud establece una política para las cargas de trabajo que se ejecutan en varias nubes públicas y en centros de datos locales. La política se define una sola vez y se aplica a las cargas de trabajo en todas partes: en distintas redes virtuales de nube, regiones, zonas de disponibilidad y múltiples proveedores de nube. 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. NSX Cloud admite la inserción de servicios norte-sur, lo cual permite redirigir un determinado tipo de tráfico a dispositivos de seguridad de terceros para contar con una protección avanzada.

Control preciso de las redes de nube

VMware NSX Cloud se ha diseñado para entornos nativos de nube pública, como Amazon (AWS) y Microsoft Azure, incluidos los de AWS GovCloud (EE.UU.) y Azure Government. NSX Cloud complementa los servicios nativos de estos proveedores de nube pública. Con NSX Cloud, puede seguir utilizando la infraestructura y los servicios de aplicaciones del proveedor de nube pública para cargas de trabajo sin limitaciones (p. ej., AWS ELB/Azure Load Balancer, AWS Route 53/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. NSX Cloud también admite la consolidación de puertas de enlace en tránsito a la VPC o VNet. Esto simplifica las operaciones y permite usar servicios integrados, como la VPN de sitio a sitio, además de servicios de tránsito o perímetro de terceros.

Visibilidad y control integrales de las operaciones

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 nube. La información sobre flujos, paquetes y eventos está disponible a través de IPFIX, Traceflow, Port Mirroring y Syslog. Las herramientas de operaciones locales pueden usar estos datos, que también sirven para obtener una visibilidad en profundidad e integral para la supervisión, 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 nube híbrida, incluidas las aplicaciones locales y en la nube pública. NSX Cloud proporciona una visibilidad granular de las cargas de trabajo de la nube pública en todas las VPC o VNet y completas funciones de búsqueda y filtrado para facilitar la gestión, además de la posibilidad de elegir qué cargas de trabajo se gestionan con NSX.

Características principales

Modo de aplicación de NSX: use las herramientas de NSX para aplicar políticas de red y seguridad uniformes a las cargas de trabajo locales y las nativas de nube pública.

Modo de aplicación de la nube: use las infraestructuras de un proveedor de nube pública para aplicar políticas de red y seguridad uniformes a las cargas de trabajo locales y las nativas de nube pública.

Detección y protección de terminales de servicios nativos de nube pública: permita la detección y la protección de terminales de servicios nativos de nube pública, además de máquinas virtuales e instancias de Amazon EC2.

Seguridad y red multinube y multisitio: incorpore prestaciones de red y seguridad para terminales en varias nubes, e integre NSX Data Center para permitir la gestión de la red y de la seguridad en nubes y centros de datos.

Cortafuegos distribuido de capa 7: tome el control del tráfico este-oeste entre cargas de trabajo de aplicaciones que se ejecutan de forma nativa en nubes públicas con un cortafuegos con estado que abarca hasta la capa 7 (inclusión distribuida en listas blancas de nombres de dominio totalmente cualificados e identificación de aplicaciones). Esto permite aplicar políticas de seguridad a todas las máquinas virtuales y servicios nativos de nubes públicas. NSX Cloud también proporciona microsegmentación de los escritorios virtuales implementados mediante VMware Horizon® Cloud on Azure.

Desvinculación enriquecida con fines de definición de la política de seguridad: defina reglas y grupos de seguridad en función de estructuras de políticas enriquecidas, como el nombre de instancia, el tipo de sistema operativo, el identificador de imagen de máquina de Amazon y etiquetas definidas por el usuario.

Política dinámica: aplique la política de seguridad automáticamente en función de los atributos de la instancia y las etiquetas definidas por el usuario. Las políticas siguen automáticamente a las instancias cuando estas se desplazan dentro de una nube y de una nube a otra.

Instancias en cuarentena: ponga en cuarentena las cargas de trabajo no autorizadas o vulnerables que se ejecuten en la nube pública sin seguridad de microsegmentación. Las instancias en cuarentena no pueden comunicarse en la red de nube, lo que ofrece varias capas de seguridad.

Inserción de servicios: aplique un enrutamiento selectivo y basado en políticas del tráfico norte-sur a un dispositivo cortafuegos de nueva generación de un partner externo.

VPN de sitio a sitio: use una VPN de IPsec integrada y de ancho de banda alto que ofrece una conectividad segura a los centros de datos locales o entre varias regiones.

PARA OBTENER MÁS INFORMACIÓN O ADQUIRIR PRODUCTOS DE VMWARE, llame al +34 914125000 en España (marque el 877-4-VMWARE si se encuentra en Norteamérica o el +1-650-427-5000 desde el resto del mundo), visite vmware.com/es/products/nsx-cloud o vmware.com/es/products, o bien busque en Internet a un distribuidor autorizado.

Arquitectura distribuida: elimine el tráfico y los saltos de red adicionales con la arquitectura de cortafuegos distribuido de NSX Cloud, que aplica políticas en la interfaz de red virtual de cada instancia, en lugar de enrutarlas a través de un cortafuegos externo.

Puerta de enlace compartida en tránsito a una VPC o VNet: aumente la compatibilidad para la consolidación de puertas de enlace en tránsito a las VPC o VNet, lo que simplifica la administración, acelera la incorporación de VPC o VNet de recursos informáticos y permite insertar servicios de terceros.

Cortafuegos perimetral: use el cortafuegos con estado que filtra el tráfico norte-sur entre instancias en redes virtuales y el Internet público.

API basadas en REST: implemente y configure mediante programación la infraestructura de red y seguridad según las necesidades mediante API basadas en REST y herramientas de automatización.

Creación de plantillas: utilice las herramientas de automatización y coordinación de las que ya dispone para crear plantillas de aplicación estandarizadas y simplificar la prestación y la gestión de servicios de red y seguridad en nubes 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: obtenga 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.

Compatibilidad con AWS GovCloud (EE.UU.) y Azure Government: amplíe las prestaciones de red y seguridad de NSX a regiones de AWS GovCloud (EE.UU.), y cuente con un punto de control y gestión central para todas las cargas de trabajo alojadas localmente, en una nube de AWS y en regiones de AWS GovCloud (EE.UU.). De igual manera, NSX Cloud también es compatible con Azure Government.

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.es