

VMware NSX

Logre que el entorno de TI avance al ritmo de la empresa

«La tecnología sigue avanzando a un ritmo sorprendente y promete grandes bonificaciones a las organizaciones capaces de tomar la iniciativa».

Doctor Bart Van Ark
Vicepresidente ejecutivo, director
economista y estratégico
The Conference Board

VMware NSX® es la plataforma de seguridad y virtualización de red que permite implementar la solución de red de nube de VMware con un enfoque de red definido por software que abarca centros de datos, nubes y marcos de aplicaciones. Con NSX, la red y la seguridad están más cerca de la aplicación, dondequiera que esta se ejecute, ya sea en máquinas virtuales, contenedores o servidores físicos. De forma parecida al modelo operativo de las máquinas virtuales, las redes se pueden implementar y gestionar de forma independiente del hardware subyacente. NSX reproduce todo el modelo de red mediante software, lo que permite crear e implementar cualquier topología de red, desde redes sencillas hasta redes complejas de varios niveles, en cuestión de segundos. Los usuarios pueden crear distintas redes virtuales con diferentes características. En su diseño de entornos más ágiles y seguros, pueden elegir entre los distintos servicios que se ofrecen a través de NSX o de un amplio ecosistema de integraciones de terceros, y que van desde cortafuegos de nueva generación hasta soluciones de gestión del rendimiento. A continuación, estos servicios pueden aplicarse a varios puntos de acceso dentro de las nubes y entre nubes.

La priorización de las necesidades de ciertas áreas tiene consecuencias

La velocidad y la agilidad, una seguridad sólida y la alta disponibilidad de las aplicaciones son prioridades clave para las organizaciones de TI. Las organizaciones dependen hasta tal punto de una infraestructura de aplicaciones sólida que, cada vez más, el entorno de TI representa la base que les permite innovar y triunfar en su transformación digital. Sin embargo, el acelerado ritmo de cambio general y en torno a las expectativas de TI altera constantemente la lista de prioridades, a menudo poniendo en peligro la prestación efectiva de los servicios.

Desgraciadamente, el equipo de TI se ve sometido a tensiones frecuentes por tener que contar con varias partes interesadas para satisfacer estas necesidades y, a menudo, se ve obligado a priorizar. Por ejemplo, la velocidad de distribución de una aplicación suele comprometer la seguridad debido a las grandes dificultades que su protección conlleva. A menudo, se asumen compromisos similares para la disponibilidad de las aplicaciones en los distintos entornos, lo que en la práctica hace al equipo de TI entrar en conflicto con el resto de la organización y viceversa.

A la larga, esta tensión y este compromiso constantes tienen consecuencias graves para el entorno de TI. De hecho, provoca graves deficiencias en varias áreas de responsabilidad: las organizaciones son incapaces de satisfacer las necesidades con rapidez, existen vulnerabilidades en el centro de datos y en los entornos de nube, y falta agilidad en general.

Ventajas principales

- Seguridad granular: evita la propagación lateral de amenazas en el entorno gracias a una política de seguridad microsegmentada para cargas de trabajo.
- Velocidad y agilidad: reduce el tiempo de aprovisionamiento de la red de días a segundos y mejora la eficiencia operativa gracias a la automatización.
- Políticas y operaciones coherentes: gestiona de forma coherente las políticas de red y seguridad, independientemente de la topología de la red física, en centros de datos, nubes públicas y privadas, y marcos de aplicaciones.

Aproveche el potencial de la infraestructura

La mayoría de las organizaciones ya han virtualizado los componentes informáticos de sus centros de datos. Muchas de ellas también han decidido virtualizar el almacenamiento, y más del 70 % ya han adoptado el almacenamiento definido por software o tienen previsto hacerlo.

Esta desvinculación de las funciones del hardware a favor de las del software permite a las organizaciones aprovisionar rápidamente componentes de aplicaciones, migrar sistemas virtuales entre centros de datos y automatizar procesos fundamentales. Si la conmutación, el enrutamiento, el balanceo de carga y el cortafuegos no se virtualizan, se desaprovecha el potencial del centro de datos definido por software.

Lo cierto es que las organizaciones con arquitecturas de red basadas en el hardware no pueden igualar la velocidad, la agilidad ni la seguridad de las que implementan redes virtualizadas. El estado de la organización depende por completo del estado de la red.

Se necesita un enfoque esencialmente nuevo para la red del centro de datos, un enfoque que no exija concesiones entre velocidad y seguridad ni entre seguridad y agilidad. Para que el departamento de TI funcione sin concesiones, hay que reescribir las reglas del centro de datos que han estado impidiendo a las organizaciones aprovechar todo su potencial. Como ya han advertido miles de organizaciones, la virtualización de la red es el nuevo enfoque.

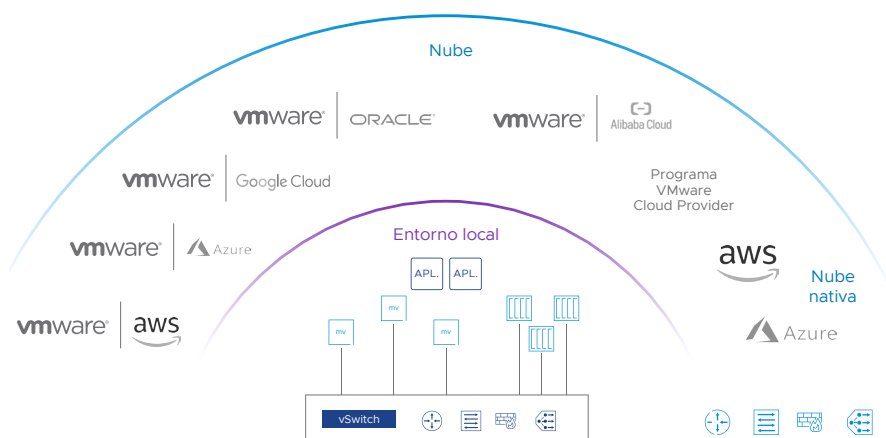


Figura 1: Red y seguridad coherentes con NSX

Al trasladar los servicios de red y seguridad a la capa de virtualización del centro de datos, la virtualización de la red permite al departamento de TI crear, almacenar, mover, eliminar y restaurar entornos de aplicaciones completos, y hacer instantáneas con la misma sencillez y velocidad que lo hacen ahora al crear máquinas virtuales. NSX amplía las políticas comunes de red y seguridad a entornos y marcos de aplicación heterogéneos, lo que permite disfrutar de estas ventajas en centros de datos, nubes privadas y públicas, y aplicaciones tradicionales y modernas. A su vez, esto fomenta niveles de seguridad y eficiencia que antes eran inviables desde el punto de vista operativo y financiero.

Características principales

- Cortafuegos distribuido con estado: permite disponer de funciones de cortafuegos con estado hasta la capa 7, integrado en el núcleo del hipervisor y distribuido por todo el entorno. Se integra directamente en entornos nativos de nube, nubes públicas nativas y hosts sin sistema operativo.
- Microsegmentación con reconocimiento de contexto: crea dinámicamente grupos y políticas de seguridad, y los actualiza automáticamente en función de numerosos atributos e información sobre aplicaciones de capa 7 para permitir una política de microsegmentación adaptable.
- Gestión de la nube: se integra de forma nativa con VMware vRealize® Suite, OpenStack, etc., y es totalmente compatible con Terraform Provider, los módulos Ansible y la integración con PowerShell.
- Integración con soluciones de terceros: mejora la seguridad y los servicios de red avanzados a través de un ecosistema de proveedores externos líderes.
- Soporte nativo de nube: admite un sistema empresarial de red y seguridad avanzadas en plataformas de contenedores, máquinas virtuales y hosts sin sistema operativo con visibilidad de la red de contenedores.
- NSX Intelligence™: reduce el tiempo necesario para identificar, analizar y aplicar políticas de segmentación de aplicaciones sin necesidad de implementar herramientas o agentes nuevos; simplifica las operaciones de seguridad mediante una seguridad intrínseca integrada en la infraestructura.
- NSX Distributed IDS/IPS™: es un motor de detección de amenazas avanzadas diseñado específicamente para detectar el desplazamiento lateral de las amenazas en el tráfico este-oeste a través de análisis distribuidos e integrados y una distribución de firma seleccionada.

NSX permite al departamento de TI convertirse en el impulsor de la innovación en la organización y atender las solicitudes de las distintas partes interesadas simultáneamente en lugar de tratarlas como incompatibles. El departamento de TI no solo es capaz de proporcionar unos niveles de seguridad sin precedentes, sino que puede hacerlo a una velocidad acorde con el ritmo de la empresa.

Seguridad intrínseca

VMware NSX aprovecha la excepcional visibilidad de la composición de las aplicaciones (desde las comunicaciones de red hasta el comportamiento durante los procesos de las cargas de trabajo individuales) que obtiene gracias a su propia integración en el hipervisor y otros puntos de control nativos en los que se basan las aplicaciones. Esta visibilidad impulsa la creación automatizada de políticas de seguridad de la red basadas en la situación de seguridad prevista para la aplicación. De esta forma, la cantidad de tiempo que los equipos de TI, de seguridad de la información y de desarrollo de aplicaciones dedican a los ciclos de revisión de la seguridad disminuye.

También permite la ampliación y la aplicación de las políticas de seguridad en los entornos de múltiples centros de datos y de nube híbrida, y concede control omnipresente de las aplicaciones desarrolladas en máquinas virtuales, contenedores y servidores bare metal. NSX Intelligence proporciona visibilidad continua de todo el centro de datos, para así simplificar y automatizar radicalmente el proceso de puesta en funcionamiento de la microsegmentación.

NSX Distributed IDS/IPS ayuda a garantizar la conformidad fácilmente, crear zonas de seguridad virtuales y detectar el desplazamiento lateral de las amenazas en el tráfico este-oeste. NSX también obtiene mayor visibilidad y control de los servicios de seguridad de terceros, como cortafuegos de nueva generación, sistemas de prevención y detección de intrusiones (IDS/IPS) y herramientas antivirus, lo que incrementa su eficacia.

NSX hace que la seguridad pase de ser un proceso reactivo complementario al ciclo de vida de desarrollo de aplicaciones a un paso proactivo, integrado y automatizado del ciclo de vida. Las cargas de trabajo recién aprovisionadas heredan automáticamente las políticas de seguridad, que les acompañan durante todo su ciclo de vida. Cuando las cargas de trabajo se quedan obsoletas, lo mismo sucede con las políticas de seguridad. Esto evita que se acumulen políticas a lo largo del tiempo y simplifica la gestión.

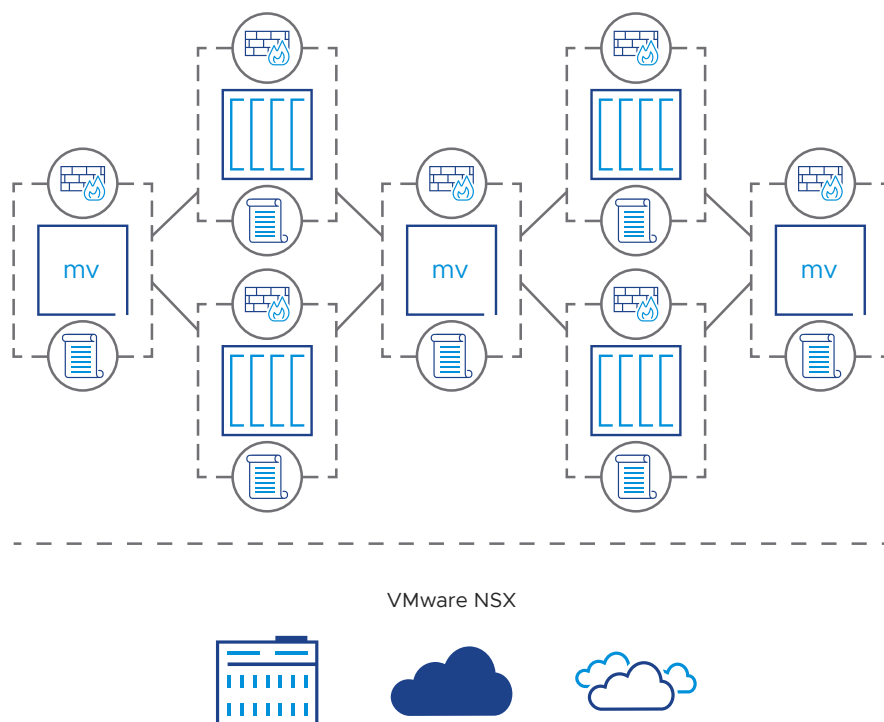


Figura 2: Aplicación de la seguridad en el centro de datos a nivel granular

Automatización

Mientras las organizaciones siguen creciendo de forma acelerada, la automatización de la red y la seguridad virtualizadas garantiza que los servicios y las aplicaciones se creen y distribuyan al ritmo de la empresa. Eliminar las tareas de aprovisionamiento de red manuales y propensas a errores mediante la automatización aumenta considerablemente la velocidad de distribución de las aplicaciones.

Si VMware NSX se combina con software de gestión de la nube (por ejemplo, VMware vRealize Automation Cloud™), puede gestionar el aprovisionamiento, la distribución, las operaciones y la retirada de las aplicaciones y la infraestructura de red y seguridad desde un panel de control centralizado. Al integrar el ciclo de vida de la red y la seguridad en el proceso mediante herramientas como Terraform y Ansible, VMware automatiza todas las operaciones de infraestructura y elimina el cuello de botella que suponen la red y la seguridad en el ciclo de vida de las aplicaciones.

La automatización de la red y seguridad tanto de las aplicaciones tradicionales (basadas en máquinas virtuales) como de las nuevas (basadas en contenedores) es posible gracias a la ampliación de las políticas comunes de red y seguridad en ambos marcos. Además, esto hace posible la distribución, la movilidad y la retirada automática de aplicaciones en los centros de datos locales, las nubes privadas y las nubes públicas.

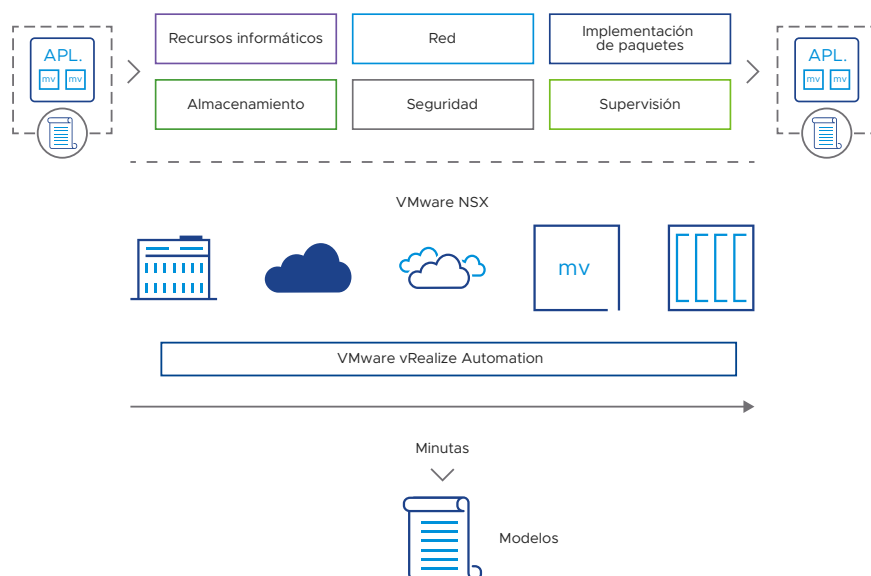


Figura 3: Implementaciones rápidas y repetibles gracias a red y seguridad automatizadas

Redes multinube

NSX y NSX Cloud™ ofrecen un modelo de red y seguridad unificadas en muchas ubicaciones, eliminan la configuración manual de la red y logran un alto nivel de eficiencia operativa gracias a la automatización de la red. Las políticas de red y seguridad permanecen con cada carga de trabajo durante toda su vida útil, lo que simplifica la política y la gestión en entornos híbridos y multinube. NSX Federation permite la gestión centralizada de políticas en distintas ubicaciones (locales y en la nube), lo que ofrece sencillez operativa y una aplicación coherente en todas las nubes.

De esta forma, las organizaciones pueden migrar máquinas virtuales o centros de datos completos de una ubicación a otra con un tiempo de inactividad de las aplicaciones mínimo o inexistente. El resultado es que las organizaciones pueden acelerar la recuperación durante las migraciones planificadas y las interrupciones imprevistas. Con un modelo de red y seguridad que abarca entornos heterogéneos, las organizaciones también pueden utilizar los recursos de distintos centros de datos físicos para que funcionen como una sola nube privada. Esta forma de agrupación de recursos con centros de datos activo-activo se denomina «agrupación de varios centros de datos» o «creación de depósitos autónomos de recursos compartidos».

Esta combinación ofrece movilidad de aplicaciones segura y eficaz, facilitando la migración de las cargas de trabajo a la nube o desde ella y entre sitios físicos. NSX y NSX Cloud extienden a la nube o a otros sitios la misma plataforma de red y seguridad virtualizada que las organizaciones de TI utilizan en su infraestructura, lo que brinda un proceso de migración rápido y con poca interacción.

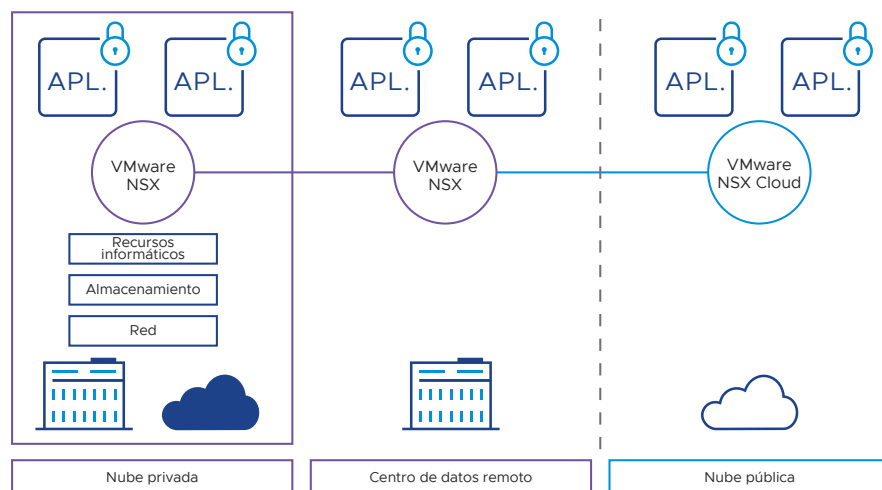


Figura 4: Disfrute de una red y seguridad coherentes en varias ubicaciones y nubes, y mitigue la repercusión de las interrupciones al mismo tiempo.

Red y seguridad para aplicaciones modernas

VMware NSX se integra con nuevas plataformas de aplicaciones para ofrecer funciones de red y seguridad (como balanceo de carga, cortafuegos, conmutación y enrutamiento) solo mediante software y para utilizarse en modelos de infraestructura como código basados en API.

Dado que cada vez más aplicaciones se basan en contenedores y arquitecturas de microservicios, es necesario conectar y proteger estas nuevas aplicaciones hasta que alcancen el nivel de carga de trabajo individual. NSX trata los contenedores y los microservicios como ciudadanos de primera, igual que cualquier otra carga de trabajo o terminal, incluida la capacidad de integrar una red de capa 3. Puede crear de forma nativa una red de contenedor a contenedor, así como microsegmentar hasta el nivel de contenedor individual, lo que permite la microsegmentación de microservicios con políticas que siguen a las cargas de trabajo a medida que se aprovisionan, cambian, migran y retiran.

NSX se integra con múltiples plataformas de coordinación de aplicaciones y contenedores, hipervisores y entornos de nube pública. Así mismo, se integra en todas las plataformas de aplicaciones para aportar un sistema de red y seguridad ágil e inherente a las nuevas aplicaciones en desarrollo.

Más información

Para obtener más información, consulte los siguientes recursos:

- [Página del producto VMware NSX](#)
- [Ficha de VMware NSX](#)
- [Descripción de la solución VMware NSX Intelligence](#)
- [Página del producto VMware NSX Distributed IDS/IPS](#)

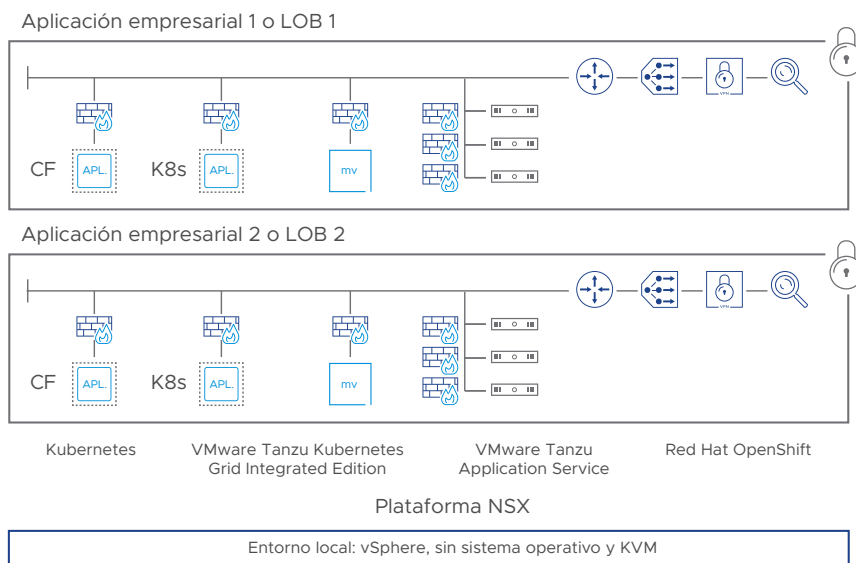


Figura 5: Aporte un sistema de red y seguridad avanzado para cargas de trabajo contenedorizadas en marcos de aplicaciones, plataformas, sitios y nubes.

Acelere el valor empresarial hoy y prepare el terreno para el futuro

Las organizaciones que han implementado NSX ven cómo se convierte rápidamente en el factor que define el éxito de sus organizaciones de TI y en una pieza clave de la infraestructura de sus centros de datos y sus estrategias multinube. Hoy en día, miles de clientes de NSX consiguen acelerar el aporte de valor a su organización distribuyendo algunas de sus aplicaciones más delicadas y esenciales en redes virtuales rápidas, ágiles y seguras, de una forma que jamás sería posible en redes tradicionales basadas en hardware.

Esta evolución del sistema de red y seguridad permite a los clientes de NSX disfrutar de ventajas considerables e inmediatas, y elimina las arduas y laboriosas tareas que antes ocupaban gran parte del ancho de banda de la organización. Esto, a su vez, da a estas organizaciones la libertad de utilizar estrategias organizativas mejoradas a la hora de planificar tanto el futuro de la organización como las funciones necesarias para que el departamento de TI respalde esa visión.