VMWARE NSX DATA CENTER: MICROSEGMENTACIÓN CON RECONOCIMIENTO DEL CONTEXTO

Proteja la red frente a la propagación lateral de amenazas

Las aplicaciones modernas son complejas, distribuidas y dinámicas

Todas las organizaciones están buscando la mejor manera de gestionar su actividad en un mundo hiperconectado, en el que las aplicaciones y los datos son la savia de cualquier empresa. Las aplicaciones modernas se distribuyen en múltiples centros de datos y clouds, y se aplican hasta el perímetro del entorno.

La virtualización, junto con la aparición de conceptos como DevOps, contenedorización y microservicios, ha permitido crear y modificar aplicaciones más rápido que nunca. Mantener la seguridad es un desafío importante, dada la naturaleza distribuida de las aplicaciones modernas y la velocidad a la que cambian.

Las estrategias de seguridad tradicionales ya no son eficaces

La proliferación de aplicaciones hace que la seguridad de red tradicional centrada en el perímetro ya no sea suficiente para proteger los datos y las aplicaciones. Los atacantes han demostrado una y otra vez que pueden traspasar o eludir las medidas de seguridad del perímetro. Una vez dentro, se desplazan lateralmente sin obstáculos, de un servidor a otro, buscando información que robar o secuestrar.

En el mundo de las aplicaciones distribuidas modernas, los equipos de seguridad y de redes de TI suelen enfrentarse al reto de mantener políticas de seguridad distintas en diferentes partes del entorno, lo que genera carencias en la situación de seguridad global.

Seguridad coherente desde el centro de datos a la cloud y al perímetro

Con VMware NSX® Data Center se pueden definir políticas de seguridad de forma coherente en todo el entorno, independientemente del tipo de aplicación o de dónde se haya implementado. Las políticas se aplican en el nivel de las cargas de trabajo individuales. Esto permite la segmentación de cargas de trabajo que residen en el mismo host físico sin tener que establecer conexiones con el exterior a través de un cortafuegos físico o virtual. Este nivel de detalle de la seguridad se denomina microsegmentación.

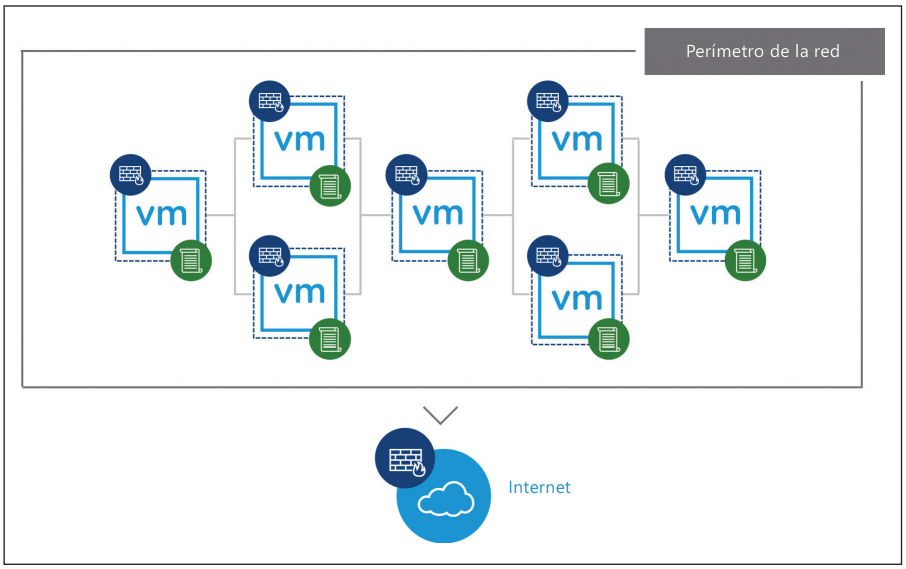

Figura 1. La microsegmentación se refiere a la aplicación de la política de seguridad de red en el nivel de carga de trabajo individual.

«Con el aumento del número de dispositivos de IdC, cuanto más segmentada esté la red, mejor... Esto evitará que las amenazas se muevan lateralmente dentro del centro de datos».

CHRISTOPHER FRENZ
DIRECTOR DE INFRAESTRUCTURA
INTERFAITH MEDICAL CENTER

CARACTERÍSTICAS DESTACADAS

- La naturaleza distribuida y dinámica de las aplicaciones modernas hace que la seguridad tradicional centrada en el perímetro sea insuficiente.
- VMware NSX Data Center habilita la microsegmentación para proteger las aplicaciones de la propagación lateral de las amenazas.
- La política de seguridad se define a partir del contexto de la aplicación y se aplica a la carga de trabajo individual.
- La seguridad se implementa de forma coherente desde el centro de datos a la cloud y al perímetro.

Los microsegmentos generados con NSX Data Center se definen y gestionan en el software, por lo que son ágiles y automatizables. A medida que las nuevas cargas de trabajo se implementan, heredan automáticamente las políticas de seguridad que permanecerán con cada carga de trabajo durante todo su ciclo de vida, con independencia de dónde se implementan o adónde se mueven.

Microsegmentación con reconocimiento del contexto, seguridad coordinada con las aplicaciones y los datos

La capacidad de definir políticas de seguridad según lo que realmente importa es tan esencial como implementar las políticas de manera uniforme. NSX Data Center desvincula la política de seguridad de atributos de red estáticos como la dirección IP, el puerto y el protocolo, y permite definir políticas a partir del reconocimiento del contexto de la aplicación y la infraestructura. Estos contextos incluyen los atributos de usuario y de identidad, los atributos de carga de trabajo (como el sistema operativo) o incluso los ámbitos de cumplimiento normativo.

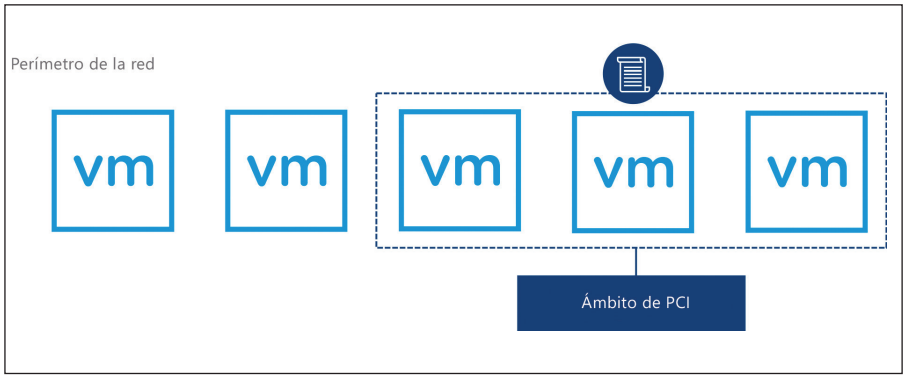

Figura 2. Los microsegmentos de NSX Data Center se pueden definir a partir de varios contextos distintos, como los ámbitos de cumplimiento normativo.

Gracias a la microsegmentación con reconocimiento del contexto que ofrece NSX Data Center, los equipos de seguridad cuentan con la flexibilidad que necesitan para proteger sus datos y aplicaciones basándose en los factores realmente importantes. Por ejemplo, se puede usar NSX Data Center para proteger una implementación de infraestructura de escritorios virtuales (VDI) aplicando una política de red según el contexto del usuario, hasta el nivel de la sesión de RDSH individual. O bien, se pueden aplicar políticas de seguridad a todas las cargas de trabajo que están incluidas en las normativas del sector de las tarjetas de pago (PCI), independientemente de si existen físicamente en el entorno.

Servicios de seguridad avanzados en el lugar y en el momento oportunos

NSX Data Center permite insertar servicios avanzados de seguridad de terceros en un microsegmento específico. En lugar de enrutar todo el tráfico de red a través de un dispositivo físico o virtual, como un cortafuegos de nueva generación (NGFW) o un sistema de detección de intrusiones (IDS) o de prevención de intrusiones (IPS), NSX Data Center puede dirigir tráfico específico dinámicamente en la capa de red virtual. Esto permite insertar los servicios de seguridad avanzados en los lugares adecuados y en el momento oportuno, para maximizar la eficiencia del tráfico de red y aumentar la eficacia de los servicios de seguridad en sí.

Visibilidad del tráfico de red en todo el entorno

El primer paso de la microsegmentación consiste en comprender cómo fluye el tráfico de red en la actualidad. VMware Network Insight™ proporciona una vista completa de todo el tráfico de red en el centro de datos, incluidos el tráfico de red física y el de red virtual. Tras analizar el tráfico de red, VMware Network Insight recomendará automáticamente políticas de microsegmentación que NSX Data Center puede utilizar en la implementación.

Empiece hoy mismo con una evaluación de red virtual gratuita para analizar el tráfico de red actual e iniciar la planificación del proyecto de microsegmentación. Para obtener más información, visite www.vmware.com/es/products/nsx/security.

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: 147939wf-vmw-q2fy19-sddc-launch-so-nsbu-context-aware-micro-seg-a4
5/18