VMware NSX for Horizon

INFORMACIÓN BÁSICA

VMware NSX™ for Horizon® aumenta la velocidad y la simplicidad de las redes de infraestructura VDI. En segundos, los administradores de TI pueden crear políticas que realicen el seguimiento dinámico de los escritorios virtuales, sin necesidad de llevar a cabo tareas de aprovisionamiento de redes que requieren mucho tiempo. Esta solución conjunta, que amplía las políticas de seguridad de los centros de datos a los escritorios y las aplicaciones, también ofrece una plataforma extensible que se integra con las soluciones de seguridad líderes del mercado.

VENTAJAS

- Se mejora la seguridad de los escritorios virtuales que se encuentran entre otras cargas de centros de datos.
- Se simplifica y se acelera la administración de políticas de seguridad y redes para los usuarios basándose en agrupaciones lógicas, funciones o etiquetas.
- Las políticas se conectan automáticamente a los escritorios en el momento de su creación para realizar un seguimiento de la máquina virtual con independencia de la infraestructura subyacente.
- Se integra con las soluciones líderes del mercado de servicios de seguridad de próxima generación, prevención de intrusiones, programas maliciosos y antivirus.

Redes y seguridad para aplicaciones y escritorios virtuales: rápido, fácil y extensible

Muchas organizaciones implementan la virtualización de escritorios y aplicaciones para mejorar la seguridad de la informática para clientes y ofrecer una mayor movilidad empresarial. Al centralizar los escritorios y las aplicaciones, se protegen los datos inactivos, se impide el acceso no autorizado a las aplicaciones y se proporciona una forma más eficaz de aplicar parches a imágenes, llevar a cabo su mantenimiento y actualizarlas.

No obstante, con la virtualización de escritorios y aplicaciones, pueden surgir nuevos problemas de seguridad detrás del cortafuegos del centro de datos (donde residen cientos o incluso miles de escritorios). Estos escritorios se encuentran muy cerca de otros usuarios y cargas de trabajo esenciales, lo que los hace mucho más vulnerables a los programas maliciosos y a otros ataques. Estos ataques pueden pasar del escritorio al servidor, lo que supone una gran superficie de ataque en el centro de datos. Este escenario de amenazas «este-oeste» es muy común y afecta a muchos clientes actualmente, especialmente a los que cuentan con instrucciones de seguridad y normativas estrictas.

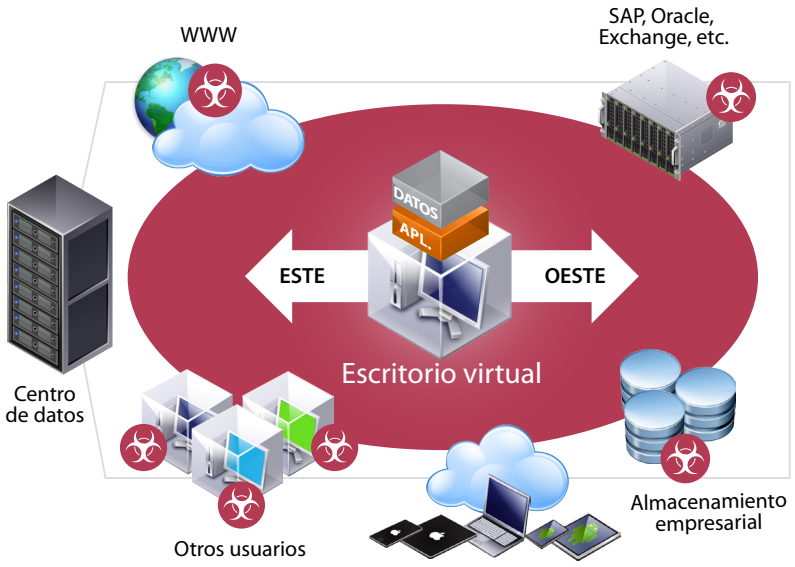

Figura 1: problemas de seguridad este-oeste en el centro de datos

Las organizaciones que desean administrar políticas de seguridad y redes que realicen un seguimiento constante de los usuarios y las cargas de trabajo también han realizado importantes inversiones en arquitecturas centradas en el hardware con elevados gastos de capital, de manejo complejo y adaptación lenta al entorno empresarial dinámico típico.

VMware NSX for Horizon

VMware NSX for Horizon protege de forma eficaz el tráfico este-oeste en el centro de datos, a la vez que garantiza que el departamento de TI pueda administrar de forma rápida y sencilla las políticas de seguridad y redes que realicen el seguimiento dinámico de las aplicaciones y los escritorios virtuales de los usuarios finales en las infraestructuras, los dispositivos y las ubicaciones.

Figura 2: NSX for Horizon ofrece seguridad y redes de infraestructura VDI de forma rápida, sencilla y extensible

Con esta solución, las organizaciones disfrutan de seguridad y redes de infraestructura VDI rápidas y sencillas. En segundos, los administradores de TI pueden crear políticas que realicen el seguimiento dinámico de los escritorios virtuales, sin necesidad de llevar a cabo tareas de aprovisionamiento de redes que requieren mucho tiempo.

Esta solución, que extiende las políticas de seguridad del centro de datos a los escritorios y las aplicaciones, también ofrece una plataforma extensible que puede integrarse con el ecosistema de partners de seguridad líderes del mercado de VMware para ofrecer a los clientes una seguridad exhaustiva capaz de proteger todo el escritorio.

Funcionamiento

VMware NSX for Horizon mejora la seguridad de la virtualización de los escritorios y ayuda a hacer frente a las amenazas este-oeste al permitir que los administradores definan las políticas de forma centralizada. A continuación, esas políticas se distribuyen a la capa del hipervisor en todos los hosts de vSphere, y se conectan automáticamente a cada escritorio virtual en el momento de la creación del escritorio. Para proteger los escritorios virtuales y las cargas de trabajo adyacentes en el centro de datos, VMware NSX implementa la «microsegmentación», lo que ofrece a cada escritorio su propia defensa perimetral. Esta «seguridad envolvente» utiliza la capacidad de cortafuegos virtual distribuido de VMware NSX para controlar el tráfico entrante y saliente de cada máquina virtual, lo que elimina el tráfico no autorizado entre escritorios y cargas de trabajo adyacentes. Si un escritorio virtual pasa de un host al siguiente o se desplaza por el centro de datos, las políticas lo seguirán automáticamente.

Funciones y ventajas

VMware NSX for Horizon aumenta la velocidad y la simplicidad de las redes de infraestructura VDI con políticas de seguridad que realizan el seguimiento dinámico de los usuarios finales entre infraestructuras, dispositivos y ubicaciones.

Redes de infraestructura VDI rápidas y sencillas

Con VMware NSX for Horizon, los administradores pueden crear, modificar y gestionar las políticas de seguridad en todos sus escritorios virtuales con tan solo unos clics. Las políticas de seguridad pueden asignarse rápidamente a los grupos de usuarios para acelerar la integración de escritorios virtuales. Gracias a la capacidad para desplegar funciones de redes virtualizadas (como la conmutación, el enrutamiento, el uso de cortafuegos y el equilibrio de carga), los administradores pueden crear redes virtuales para la infraestructura VDI sin necesidad de sintaxis de configuración de hardware, ACL o VLAN complejas.

Políticas automatizadas que realizan el seguimiento dinámico de los usuarios finales y los escritorios

Los administradores pueden establecer políticas que se adaptan de forma dinámica al entorno informático de los usuarios finales, con servicios de seguridad de redes que se asignan a los usuarios basándose en funciones, agrupaciones lógicas, sistemas operativos de escritorio, etc. (con independencia de la infraestructura de red subyacente). Las políticas administradas de forma centralizada se conectan automáticamente a cada máquina virtual de escritorio en el momento de la creación del escritorio, por lo que las organizaciones pueden escalar con total tranquilidad, con una seguridad que realiza el seguimiento del escritorio virtual constantemente en el centro de datos.

Plataforma para la seguridad avanzada

VMware NSX ofrece una plataforma extensible que puede integrarse con las mejores prestaciones de un ecosistema reconocido de partners de seguridad. Al añadir servicios de forma dinámica, puede ampliarse la seguridad de los escritorios virtuales de los centros de datos a los escritorios y las aplicaciones. El ecosistema de partners, incluidos Trend Micro, Intel Security y Palo Alto Networks, ofrece soluciones para proteger el sistema operativo, el navegador, el correo electrónico, etc. (con servicios de seguridad de próxima generación, prevención de intrusiones, programas maliciosos y antivirus).

Más información

Para obtener más información sobre Horizon y VMware NSX, visite el sitio web de VMware y síganos en Twitter.

Recursos de VMware Horizon

Web: http://www.vmware.com/es/products/horizon-view

Blog: http://blogs.vmware.com/euc/

Twitter: @VMwareHorizon

Recursos de VMware NSX

Web: http://www.vmware.com/es/products/nsx/

Blog: http://blogs.vmware.com/networkvirtualization/

Twitter: @VMwareNSX

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, 2ª planta, 28023 Madrid, España. Tel. +34 914125000 Fax +34 914125001 www.vmware.es

N.º de artículo: VMW-SB-NSXNETWKSECUR-A4-20150401-WEB