VMware NSX para Horizon

PRESENTACIÓN GENERAL

VMware NSX™ para Horizon® brinda velocidad y simplicidad a las redes de infraestructuras de escritorio virtual (VDI, *Virtual Desktop Infrastructure*). En cuestión de segundos, los administradores de TI pueden crear políticas que sigan dinámicamente a los escritorios virtuales, sin la necesidad de un aprovisionamiento de red que demande mucho tiempo. Al extender las políticas de seguridad desde el centro de datos al escritorio y a la aplicación, esta solución conjunta también proporciona una plataforma extensible que se integra con soluciones de seguridad líderes del sector.

VENTAJAS

- Aumente la seguridad para escritorios virtuales que se encuentran en cargas de trabajo de otros centros de datos.
- Simplifique y acelere la administración de redes y políticas de seguridad para usuarios según el agrupamiento lógico, el rol o la etiqueta.
- Añada políticas automáticamente al escritorio a medida que se crea, que sigan a la máquina virtual, independientemente de la infraestructura subyacente.
- Realice la integración con soluciones líderes del sector para obtener servicios de antivirus, malware, prevención de intrusiones y de seguridad de próxima generación.

Redes y seguridad para escritorios virtuales y aplicaciones: rápidas, simples y extensibles

Muchas organizaciones implementan la virtualización de aplicaciones y escritorios para mejorar la seguridad de la computación del cliente y brindar una mayor movilidad empresarial. La centralización de escritorios y aplicaciones protege los datos estáticos, previene el acceso no autorizado a aplicaciones y brinda una manera más eficiente para aplicar parches, y mantener y actualizar imágenes.

Sin embargo, con la virtualización de aplicaciones y escritorios, pueden surgir nuevas preocupaciones relacionadas con la seguridad detrás del firewall del centro de datos, donde residen cientos o, incluso, miles de escritorios. Estos escritorios están cerca de otros usuarios y cargas de trabajo de misión crítica, lo que los hace mucho más susceptibles al malware y a otros ataques. Estos ataques pueden moverse del escritorio al servidor y, así, exponer una superficie de ataque grande dentro del centro de datos. Esta situación de amenaza "de este a oeste" es común y afecta a muchos clientes en la actualidad, particularmente a aquellos con directivas estrictas de cumplimiento normativo y seguridad.

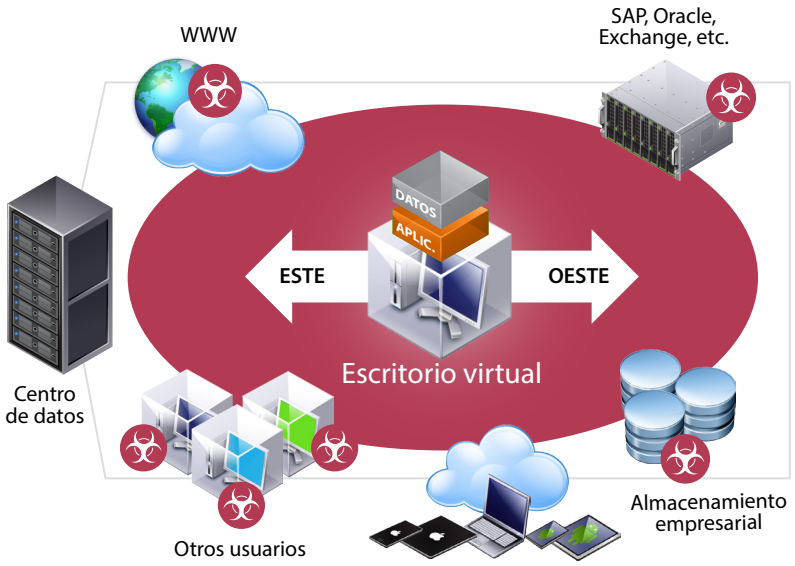

Figura 1: Inquietudes de seguridad de este a oeste dentro del centro de datos

Las organizaciones que buscan administrar redes y políticas de seguridad que siguen de manera permanente a usuarios y cargas de trabajo, también han realizado tradicionalmente una inversión importante en una arquitectura centrada en el hardware, la cual tiene gastos altos de capital, es compleja de manejar y lenta para adaptarse al entorno dinámico y típico del negocio.

VMware NSX para Horizon

VMware NSX para Horizon protege de manera eficaz el tráfico de este a oeste dentro del centro de datos y, a la vez, garantiza que TI puede administrar de manera rápida y fácil las redes y las políticas de seguridad que siguen dinámicamente a los escritorios virtuales y las aplicaciones de los usuarios finales en todos los dispositivos, las ubicaciones y la infraestructura.

Figura 2: NSX para Horizon ofrece seguridad y redes de VDI rápidas, simples y extensibles

Con esta solución, las organizaciones se benefician de la seguridad y de las redes de VDI rápidas y simples. En cuestión de segundos, los administradores de TI pueden crear políticas que sigan dinámicamente a los escritorios virtuales, sin la necesidad de un aprovisionamiento de red que demande mucho tiempo.

Al extender las políticas de seguridad desde el centro de datos hasta los escritorios y las aplicaciones, esta solución también proporciona una plataforma extensible que se integra con la red de VMware de socios de seguridad líderes del sector para proporcionarles a los clientes protección exhaustiva que proteja el escritorio completo.

Cómo funciona

VMware NSX para Horizon mejora la seguridad de la virtualización de escritorios y ayuda a abordar las amenazas del flujo este a oeste, ya que permite que los administradores definan las políticas de manera centralizada. Estas políticas luego se distribuyen a la capa del hipervisor dentro de cada anfitrión de vSphere y se añaden automáticamente a cada escritorio virtual apenas se crea. Para proteger los escritorios virtuales y las cargas de trabajo adyacentes dentro del centro de datos, VMware NSX implementa la "microsegmentación", lo que le da a cada escritorio su propia defensa de perímetro. Esta "seguridad lista para usar" utiliza la capacidad de protección de firewall virtual distribuida de VMware NSX para controlar el tráfico a cada máquina virtual y desde cada una de ellas, y así eliminar el acceso no autorizado entre escritorios y cargas de trabajo adyacentes. Si el escritorio virtual se mueve de un anfitrión a otro, o por el centro de datos, las políticas lo seguirán automáticamente.

Funciones y ventajas

VMware NSX para Horizon brinda velocidad y simplicidad a las redes de VDI con políticas de seguridad que siguen dinámicamente a los usuarios finales en los diferentes dispositivos, ubicaciones e infraestructuras.

Redes de VDI rápidas y simples

Con VMware NSX para Horizon, los administradores pueden crear, cambiar y administrar políticas de seguridad en todos los escritorios virtuales fácilmente con unos pocos clics. Las políticas de seguridad se pueden asignar rápidamente a grupos de usuarios para acelerar la incorporación de los escritorios virtuales. Al contar con la capacidad de implementar funciones de red virtualizadas (como conmutación, enrutamiento, protección de firewall y equilibrio de carga), los administradores pueden desarrollar redes virtuales para la VDI sin la necesidad de redes de área local (VLAN, *Virtual Local Area Network*), listas de controles de acceso (ACL, *Access Control List*) o sintaxis de configuración de hardware complejas.

Políticas automatizadas que siguen dinámicamente a los usuarios finales y escritorios

Los administradores pueden establecer políticas que se adapten dinámicamente al entorno de computación del usuario final, con servicios de seguridad de red que se mapeen al usuario según el rol, agrupamiento lógico, sistema operativo del escritorio y más, independientemente de la infraestructura de la red subyacente. Las políticas administradas de manera centralizada se añaden automáticamente a cada máquina virtual de escritorio apenas se crea, por lo que las organizaciones pueden escalar con confianza, ya que la seguridad sigue de manera permanente al escritorio virtual por todo el centro de datos.

Plataforma para la seguridad avanzada

VMware NSX ofrece una plataforma extensible que puede integrarse con las mejores capacidades de una red establecida de socios de seguridad. Al agregar servicios de manera dinámica, la seguridad del escritorio virtual se puede extender desde el centro de datos hasta el escritorio y las aplicaciones. Esta red de socios, incluidos Trend Micro, Intel Security y Palo Alto Networks, ofrece soluciones que protegen el sistema operativo, el explorador, el correo electrónico, entre otros, mediante los servicios de antivirus, malware, prevención de intrusiones y de seguridad de la próxima generación.

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/latam/products/horizon-view

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

Twitter: @VMwareHorizon

Recursos de VMware NSX

Web: http://www.vmware.com/latam/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/latam

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