it white papers

Seguridad
para el centro de datos

vmware®

Junio 2016

Este es un documento producido por

www.ituser.es
www.itreseller.es

Accede a nuestras publicaciones digitales

CÓMO USAR ESTE DOCUMENTO

Con el fin de obtener la mejor experiencia de uso de esta revista, es **imprescindible** seguir estos sencillos pasos que te indicamos a continuación:

Paso 1. Asegúrate de disponer de las versiones más actualizadas de Adobe Reader y Flash Player. Si no las tienes instaladas, puedes descargarlas aquí:

Adobe Acrobat Reader y Adobe Flash Player

Paso 2. Accede al enlace de descarga y la publicación se abre en el visor del navegador.

Paso 3. Busca la opción guardar como que, dependiendo del navegador que utilices, podrá ser un icono o estar incluída en la barra de menú, y guarda la revista en la carpeta donde almacenes los documentos en tu equipo.

Paso 4. Accede a dicha carpeta y usa el botón derecho del ratón para hacer clic en el fichero de la revista.

Paso 5. Selecciona Adobe Reader como aplicación predeterminada para abrir este tipo de documentos.

Paso 6. Una vez abierta la revista, habilita la visualización a pantalla completa, y puedes iniciar la lectura de la revista con todas las capacidades interactivas disponibles.

Seguridad para el centro de datos

El centro de datos definido por software, si bien iba a ser asumido por las empresas por factores tales como la agilidad, la velocidad y la eficiencia, ha demostrado que ofrece posibilidades más allá de estas ventajas, y una de ellas, muy valiosa para las empresas en este momento es la seguridad.

El centro de datos definido por software es el futuro

Un centro de datos definido por software aprovecha las ventajas de la virtualización y automatización y las incorpora a la estructura de centro de datos completa. La capacidad de crear, tomar instantáneas, mover, eliminar y restaurar máquinas virtuales en el software mediante programación transformó el modelo operativo de los recursos informáticos para el departamento de TI. Ahora, el enfoque definido por software permite al departamento de TI crear, tomar instantáneas, mover, eliminar y restaurar mediante programación toda una estructura de centro de datos con recursos informáticos, de almacenamiento y de redes en el software. La automatización de los centros de datos, las TI de autoservicio y una transformación total del modelo operativo de red han resultado ser grandes ventajas de este enfoque.

La repercusión sobre la gestión de la seguridad del departamento de TI es mucho mayor que los cambios

que se deben aplicar a los recursos protegidos. El centro de datos definido por software brinda una plataforma que aborda intrínsecamente algunas restricciones arquitectónicas básicas relacionadas con el diseño de los centros de datos, las cuales han limitado la capacidad de actuación de los profesionales de seguridad durante décadas.

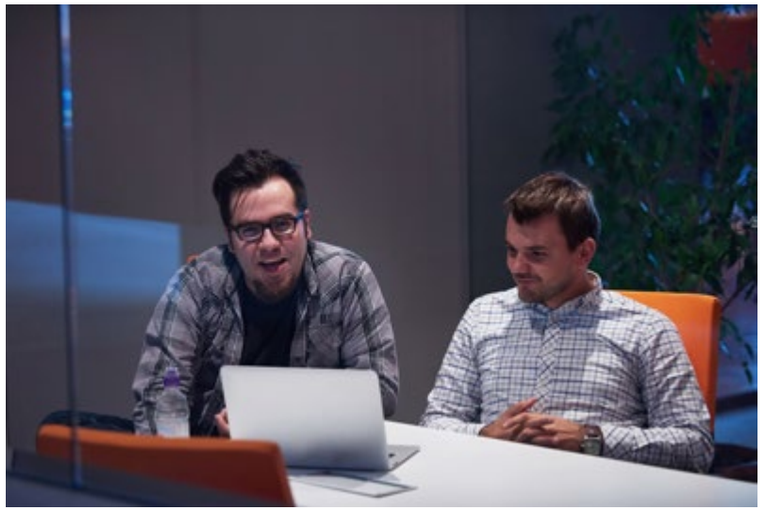
La capa de virtualización del centro de datos que utiliza brinda el espacio ideal para lograr tanto el contexto como el aislamiento adecuados con una aplicación ubicua. Los controles que actúan en la capa de virtualización del centro de datos hacen uso de la introspección segura del host, la capacidad de proporcionar un contexto de host de gran calidad sin usar agentes, mientras permanecen aislados en el hipervisor, protegidos ante los intentos de ataque.

La posición ideal de la capa de virtualización del centro de datos, situada entre las aplicaciones y la infraestructura física y combinada con el aprovisionamiento y la gestión automatizados de redes y políticas de seguridad, un rendimiento integrado en el kernel, una aplicación distribuida y una capacidad con escalabilidad horizontal, está a punto de transformar por completo la seguridad de los centros de datos y permitir a los profesionales de seguridad de los centros de datos lograr niveles de seguridad que, en el pasado, eran inviables desde el punto de vista operativo.

Microsegmentación para proteger el centro de datos Clicar para ver el vídeo

Microsegmentación de la red

La estrategia de seguridad de red basada en el perímetro de los centros de datos empresariales ha demostrado ser insuficiente. Los ataques de hoy en día rompen esta defensa basada únicamente en el perímetro a través de los usuarios autorizados y, a continuación, se desplazan lateralmente por el perímetro del centro de datos de una carga de trabajo a otra sin apenas controles que bloqueen su propagación. Muchas de las infracciones que han salido a la luz recientemente son un claro ejemplo de ello: desde la suplantación de identidad o ingeniería social, hasta programas maliciosos, vulnerabilidades de seguridad, mando y control y libertad para realizar movimientos laterales por el centro de datos hasta que los atacantes encuentran lo que buscan para, posteriormente, realizar copias sin autorización.



La microsegmentación de la red del centro de datos puede ser de gran ayuda a la hora de limitar dicho movimiento lateral no autorizado, pero no es viable desde el punto de vista operativo en las redes de centros de datos tradicionales.

Los cortafuegos tanto tradicionales como los avanzados de nueva generación implementan controles como «cuellos de botella» físicos o virtuales en la red. El tráfico de carga de trabajo de las aplicaciones se dirige hacia estos puntos de control y, a continuación, se aplican las reglas para bloquear o permitir el tráfico de los paquetes. El enfoque de los cortafuegos tradicionales para lograr la microsegmentación se encuentra rápidamente con dos barreras operativas importantes: la

capacidad de rendimiento y la gestión de operaciones o cambios. La primera, relacionada con la capacidad, se puede superar a un cierto coste. Se puede adquirir la cantidad de cortafuegos físicos o virtuales suficiente como para proporcionar la capacidad necesaria para lograr la microsegmentación. Sin embargo, en el caso de las operaciones, el problema aumenta exponencialmente con el número de cargas de trabajo y la naturaleza cada vez más dinámica de los centros de datos actuales. Si hay que añadir, eliminar o modificar las reglas del cortafuegos, cada vez que se añade, se mueve

VMware NSX implementa tres modos de seguridad en las redes de los centros de datos: redes virtuales completamente aisladas, redes virtuales segmentadas y segmentación con servicios de seguridad avanzados

o se retira del servicio una nueva máquina virtual, la frecuencia de los cambios sobrecarga rápidamente las operaciones de TI. Es esta barrera la que ha supuesto el fin de los planes mejor trazados de la mayoría de los equipos de seguridad para lograr una microsegmentación completa o estrategia de «confianza cero».

El enfoque del centro de datos definido por software de VMware utiliza la plataforma de virtualización de red NSX para ofrecer grandes ventajas con respecto a los enfoques de seguridad de redes tradicionales, tales como el aprovisionamiento automatizado, movimientos, incorporaciones y cambios automatizados en las cargas de trabajo, la aplicación distribuida en todas las interfaces virtuales y cortafuegos en el kernel con escalabilidad horizontal, distribuidas por todos los hipervisores e integradas en la plataforma.

Rendimiento y automatización

Es importante señalar que el objetivo del rendimiento de cortafuegos que ofrece la plataforma NSX no es sustituir las plataformas de cortafuegos de hardware utilizadas para la defensa del perímetro. La capacidad de rendimiento de las plataformas de cortafuegos de hardware está diseñada para controlar el tráfico que fluye a través de cientos o miles de cargas de trabajo que entran o salen del perímetro del centro de datos.

La plataforma NSX ofrece un rendimiento de cortafuegos de 20 Gbps y admite más de 80 000 conexiones

Webinar: Seguridad intrínseca con VMware

Clicar para ver el vídeo

Introducción al laboratorio práctico de VMware NSX de Andrew Hald

Clicar para ver el vídeo

por segundo y host. Este rendimiento solo se aplica a las máquinas virtuales en el hipervisor y cabe señalar que, cada vez que se añade un host a la plataforma del SDDC, se suman otros 20 Gbps o capacidad de rendimiento.

El aprovisionamiento y la capacidad de movimiento, incorporación y cambio automatizados permiten implantar las políticas de cortafuegos adecuadas a la hora de crear una carga de trabajo mediante programación. Dichas políticas siguen a la carga de trabajo cuando éstas se trasladan a cualquier ubicación del centro de datos o a otros centros de datos. Asimismo, si la aplicación se elimina por completo, las políticas de seguridad asociadas se eliminan del sistema igualmente. De esta forma, se elimina una importante barrera que ha impedido la presentación de una verdadera solución de microsegmentación viable.

Además, el ecosistema de partners de NSX también puede hacer uso de las funciones de distribución y automatización de la plataforma para que las empresas puedan aplicar una combinación de funcionalidades de distintos partners al vincular los servicios de seguridad avanzados y utilizar servicios diferentes en función de las condiciones de seguridad.

La combinación de rendimiento y automatización que ofrece la plataforma NSX permite diseñar e implementar una solución de microsegmentación viable desde el punto de vista operativo en todos los niveles hasta llegar a las distintas interfaces virtuales.

Seguridad nativa con tecnología NSX: aislamiento y segmentación

La plataforma VMware NSX proporciona de forma intrínseca tres niveles de seguridad a los centros de datos: aislamiento, segmentación y segmentación con servicios avanzados.

La combinación de rendimiento y automatización que ofrece la plataforma NSX permite diseñar e implementar una solución de microsegmentación viable desde el punto de vista operativo en todos los niveles hasta llegar a las distintas interfaces virtuales

El aislamiento es la base de la mayoría de los sistemas de seguridad de red, ya sea por motivos de conformidad o contención, o bien para evitar la interacción entre los entornos de desarrollo, prueba y producción. Mientras que el enrutamiento, las listas de control de acceso o las reglas de cortafuegos de los dispositivos físicos, con una configuración y un mantenimiento manuales, se han utilizado tradicionalmente para establecer y aplicar el aislamiento, éste y el entorno multicliente son inherentes a la virtualización de red. De forma predeterminada, las redes virtuales están aisladas de cualquier otra red virtual y de la red física subyacente, con lo que se aplica el principio de seguridad de mínimos privilegios. No es necesario el uso de subredes físicas, redes de área local virtuales, listas de control de acceso o reglas de cortafuegos para que sea posible el aislamiento. De nuevo, conviene señalar que no se requiere ninguna configuración. Las redes virtuales se crean de forma aislada y permanecen así a menos que se conecten entre sí expresamente.

Cualquier red virtual aislada puede estar formada por cargas de trabajo distribuidas por el centro de datos.

Protección de los CPD desde dentro con la Micro-Segmentación y VMware NSX

Clicar para ver el vídeo

El aprovisionamiento y la capacidad de movimiento, incorporación y cambio automatizados permiten implantar las políticas de cortafuegos adecuadas a la hora de crear una carga de trabajo mediante programación

Las cargas de trabajo de una misma red virtual pueden residir en el mismo hipervisor o en hipervisores diferentes. Es más, las cargas de trabajo de distintas redes virtuales pueden residir en el mismo hipervisor.

Las redes virtuales también están aisladas de la infraestructura física subyacente. Dado que el tráfico que se genera entre los hipervisores está encapsulado, los dispositivos de red físicos actúan en un espacio de direcciones totalmente diferente al de las cargas de trabajo conectadas a las redes virtuales.

Relacionada con el aislamiento, pero aplicada a una red virtual de múltiples niveles, se encuentra la segmentación. La segmentación de redes suele ser una función de un cortafuegos o enrutador físico diseñada para permitir o denegar el tráfico generado entre segmentos o niveles de una red.

Prepárate para la nueva regulación europea sobre los datos

Clicar para ver el vídeo

La segmentación de redes, al igual que el aislamiento, es una función básica de la plataforma de virtualización de red VMware NSX. Un entorno virtual puede admitir un entorno de red de múltiples niveles, lo que se traduce en múltiples segmentos de capa 2 con segmentación de la capa 3 o microsegmentación en un único segmento de capa 2 mediante el cortafuegos distribuido definido por las políticas de seguridad de las cargas de trabajo.

En una red virtual, los servicios de red (capa 2, capa 3, listas de control de acceso, cortafuegos y calidad de servicio, entre otros) aprovisionados con una carga de trabajo se crean y distribuyen mediante programación al conmutador virtual del hipervisor. Los servicios de red, incluidos el cortafuegos y la segmentación de la capa 3, se aplican en la interfaz virtual. Las comunicaciones de una red virtual no abandonan nunca el entorno virtual, por lo que se elimina la necesidad de configurar la segmentación de la red y realizar el mantenimiento correspondiente en redes o cortafuegos físicos.

La plataforma de virtualización de red VMware NSX básica posee características de cortafuegos de inspección con estado fundamentales para aplicar la segmentación en redes virtuales. En algunos entornos, es necesario el uso de funciones de seguridad de red más avanzadas. En estos casos, los clientes pueden utilizar la plataforma para distribuir, activar y aplicar servicios de seguridad de red avanzados en un entorno de red virtualizado. La plataforma NSX distribuye los servicios de red en el conmutador virtual para formar un canal de servicios lógico aplicado al tráfico de la red virtual. Los servicios de red de terceros se pueden insertar en el canal lógico, lo que permite utilizar los servicios físicos o virtuales en el propio canal.

Otra ventaja importante del enfoque NSX es la capacidad de crear políticas que utilizan la inserción de servicios, la vinculación y la dirección del tráfico de NSX para gestionar la ejecución de los servicios en el canal de servicios lógico en función de los resultados de otros servicios, lo que permite coordinar servicios de seguridad de red de distintos proveedores que, de otra forma, no guardarían relación alguna.

El valor de la seguridad

Tal y como nos explican Moisés Navarro, business Strategist de VMware, “la compañía lleva muchos años trabajando alrededor de la racionalización, la agilidad, la automatización… y siempre incorporando capacidades de robustez, gobierno, control. Tanto en lo que respecta a los centros de datos como a los entornos de usuario (fijos o móviles, físicos o virtualizados). Por lo tanto, desde el primer momento hemos venido persiguiendo esa securización de entornos y cargas de trabajo. Ahora, gracias a las plataformas definidas por software, hemos visto que podemos llegar de manera

mucho más directa y mucho más intensa a cuestiones clave para los responsables de seguridad. Y en todo esto es clave el concepto de micro-segmentación que habilita VMware".

Como elemento diferencial de esta propuesta "destacaría la capacidad de implementar un modelo de confianza cero (Zero Trust model) apoyado por la micro-segmentación, que aplica el control perimetral a cada elemento de infraestructura que queremos proteger. A día de hoy, la aproximación más habitual es definir islas, las cuales se intentan blindar perimetralmente, metiendo dentro los recursos que se quieren proteger. El riesgo de seguir exclusivamente una aproximación perimetral es que, una vez roto el perímetro, expandir el ataque es demasiado sencillo. Con la micro-segmentación, lo que lograríamos en primera instancia es que, una vez comprometido un recurso, no sirva como trampolín obvio de ataque a otros recursos. Para ello ofrecemos nuestras tecnologías y servicios profesionales, junto con los de nuestra amplísima red de socios, tanto tecnológicos de cara a ofrecer soluciones, como en el área de servicios profesionales, de cara a llevar estos modelos a la realidad del cliente".

La aproximación seguida por VMware para seguridad "sigue el patrón propuesto en nuestro modelo de software-defined business: una política corporativa desplegada por un motor unificado actuando sobre toda plataforma y todo destino donde estén presentes las cargas de trabajo y los procesos de negocio de ese cliente. De esta manera, se consigue un modelo de seguridad intrínseca y se logra una mayor homogeneidad, ya que no hablamos de una seguridad para el centro de datos diferente de una seguridad para nube pública, al igual que no hablamos del motor de seguridad que un cliente despliega en sus plataformas desacoplado del motor de seguridad que pueda usar para gestionar los recursos alojados en plataformas de terceros".

Pensando en el desarrollo de esta estrategia, "por un lado, de manera muy clara, continuar trabajando codo con codo con el ecosistema. Y eso nos permitirá potenciar nuestras soluciones y, algo muy importante, su aplicabilidad en entornos muy diversos. Esta expansión es crucial ya que hoy vemos claramente cómo nuestros clientes trabajan en entornos multi-cloud: nubes propias y muchas nubes de terceros. Vemos cómo trabajan en entornos multi-contexto: centros de datos, clouds, usuarios, dispositivos, containers... Vemos que deben enfrentarse al reto del cifrado en entornos dispersos, por eso trabajamos sobre la base del cifrado de red distribuido (Distributed Network Encryption), que permite al cliente decidir qué debe cifrarse dentro y fuera de su Centro de Datos. Y toda esta explosión de plataformas y servicios que usarán nuestros clientes irá a más, por lo que queremos estar ahí para ayudarles a securizar de manera viable y solvente todo ese entorno tan variado y tan variable".

Enlaces relacionados

- Microsegmentación dentro y fuera del centro de datos
- VMware NSX para multi-hipervisor: guía de diseño para la virtualización de la red
- VMware NSX