La microsegmentación del centro de datos

Una estrategia de centro de datos definido por el software para la estrategia de seguridad “*Zero Trust*”

CASO DE USO DEL PRODUCTO

vmware®

Índice

Resumen ejecutivo

El centro de datos definido por el software (SDDC, *Software-Defined Data Center*), a pesar de que se comprende en términos de arquitectura, está comenzando a mostrar sus ventajas más allá de la agilidad, velocidad y eficacia a medida que las organizaciones implementan y descubren otras áreas de mejora. Una de las áreas clave en la que las organizaciones que impulsan la implementación del centro de datos definido por el software es la seguridad.

Cuando las organizaciones de TI de las empresas y el sector público adoptan el centro de datos definido por el software y virtualizan el procesamiento, la red y el almacenamiento, automatizan el aprovisionamiento y reducen significativamente el tiempo de salida al mercado de las aplicaciones y los servicios de TI. También optimizan y eliminan el riesgo de los movimientos, las incorporaciones y los cambios en la infraestructura. Este nuevo modelo de operaciones tiene algunas ventajas adicionales. Los clientes que crearon su centro de datos definido por el software con la automatización y la seguridad incorporada de la plataforma de VMware NSX™ descubrieron, casualmente, algunas ventajas de seguridad significativas, en un momento en el que muchas organizaciones tratan de implementar en sus redes del centro de datos una estrategia cada vez más detallada de segmentación de red (p. ej., la arquitectura de red *Zero Trust* de Forrester Research), como respuesta al aumento del índice de atacantes que se mueven con libertad dentro del perímetro del centro de datos de las empresas. Estas estrategias se extienden a los controles de seguridad de grupos de recursos mucho más pequeños, normalmente, a un grupo pequeño de recursos virtualizados o máquinas virtuales (VM, *Virtual Machine*) individuales. Se cree que la microsegmentación es una estrategia de las mejores prácticas desde un punto de vista de seguridad, pero es difícil de aplicar en entornos tradicionales. Las capacidades inherentes de seguridad y automatización de la plataforma NSX hacen que la microsegmentación sea, por primera vez, operacionalmente viable en el centro de datos empresarial.

VMware NSX implementa tres modos de seguridad para redes del centro de datos: redes virtuales completamente aisladas, redes virtuales segmentadas (mediante el firewall nativo de la plataforma NSX, de alto rendimiento y completamente automatizado) y segmentación con servicios de seguridad avanzados con nuestros socios de seguridad. Los ejemplos de integración de socios incluyen Palo Alto Networks para la segmentación de red con firewalls de última generación o Rapid7 para el escaneo de vulnerabilidad.

En lo que respecta al negocio, la microsegmentación de red no solo es operacionalmente viable con VMware NSX, sino también rentable, ya que permite la implementación de controles de seguridad dentro de la red del centro de datos por una fracción del costo del hardware.

Muchos centros de datos grandes utilizan la seguridad como una de las primeras ventajas importantes del centro de datos definido por el software. En un futuro muy cercano, contar con un centro de datos más seguro será lo normal.

El centro de datos definido por el software es el futuro

Un centro de datos definido por el software constituye una estrategia de arquitectura para el diseño de centros de datos, que aprovecha un principio fundamental de la ciencia de la computación: la separación. Los sistemas operativos, los lenguajes de programación superiores, los protocolos de redes, y más recientemente, la virtualización de servidor, son todos ejemplos de separación, cuyas incorporaciones dieron como resultado ciclos importantes de innovación en el sector en los últimos 25 años. La introducción de una capa de separación permite que los sistemas y servicios sobre la capa de separación y debajo de ella funcionen e innoven de manera independiente, mientras mantienen rutas de comunicación acordadas y exponen servicios entre capas por medio de interfaces bien definidas. Cuando se usa una estrategia de centro de datos definido por el software se aplican los principios de separación para brindar una estructura completa de centro de datos en software y se desvincula el suministro de servicio de la infraestructura física subyacente. Esto permite que se utilice el hardware subyacente como depósitos generalizados de capacidad de almacenamiento, red y procesamiento, que puede combinarse, consumirse y reasignarse de forma programática, sin modificar el hardware.

Muchos de los centros de datos más grandes, ágiles y eficaces del mundo han probado la estrategia del centro de datos definido por el software, incluidos Google, Facebook y Amazon. En los últimos 10 años, estos operadores de grandes centros de datos diseñaron una capa de separación de centro de datos definido por el software en sus aplicaciones y plataformas personalizadas, lo que les permite automatizar prácticamente todos los aspectos de las operaciones del centro de datos, mientras se desvinculan completamente del hardware de almacenamiento, red y procesamiento subyacentes. Esta desvinculación reduce significativamente los gastos operacionales y de capital de su infraestructura física y les permite cumplir con los pedidos de servicio muchísimo más rápido que muchas organizaciones de TI de empresas.

En la actualidad, los departamentos de TI de las empresas pueden alcanzar el mismo nivel de agilidad y eficiencia que los grandes centros de datos en sus propios centros de datos, sin modificar su infraestructura de hardware existente.

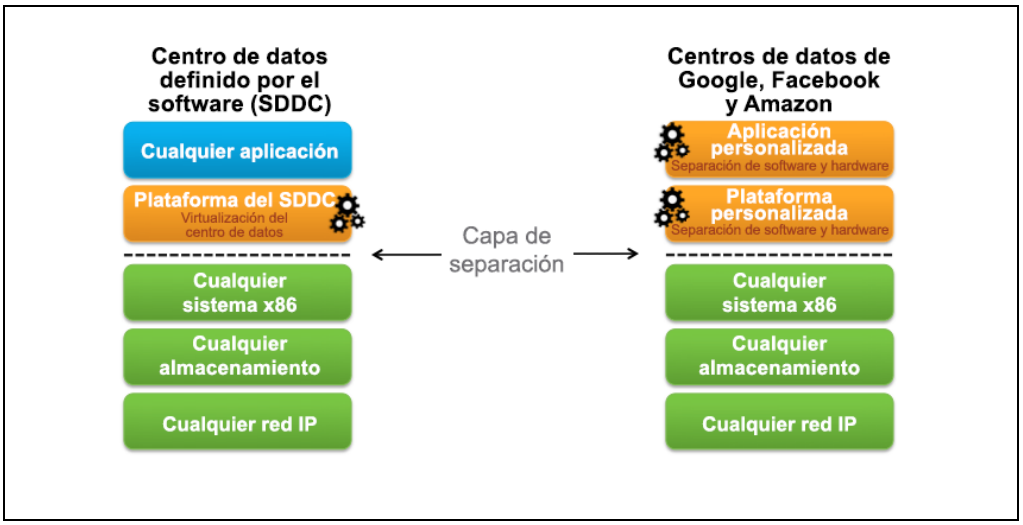

Figura 1: La inteligencia se desplazó al software para crear una capa de separación entre el software y la infraestructura física subyacente. Los grandes centros de datos han hecho esto durante décadas al incluir inteligencia en su software personalizado de aplicaciones o plataformas. Los centros de datos de las empresas de hoy pueden alcanzar el mismo nivel de desvinculación al aprovechar el software en la capa de virtualización del centro de datos.

VMware diseñó la capa de separación de centro de datos en su plataforma de virtualización de red NSX. La plataforma se basa en un controlador de sistema distribuido que se combina con un hipervisor tradicional y vSwitch para permitir que toda la estructura del centro de datos se reproduzca con precisión y sin interrupciones en el software, independientemente de la infraestructura física existente. La plataforma VMware NSX se probó en implementaciones de producción, algunas de más de tres años, y ahora se implementa en dos de los tres proveedores de servicios líderes del mundo, cuatro de las cinco empresas principales de servicios financieros del mundo y más de 100 centros de datos de clase empresarial en casi todos los sectores comerciales, incluidos los servicios de salud, manufactura, venta minorista, productos de consumo, bancario, seguros, transporte, gobierno local, federal y estatal e industria de la alta tecnología.

El centro de datos definido por el software es más ágil, más flexible y más seguro

Una estrategia de centro de datos definido por el software toma las ventajas de la virtualización y automatización y las amplía para incorporar toda la estructura del centro de datos. La capacidad de snapshot y de crear, mover, eliminar y restaurar máquinas virtuales de forma programática en un software transformó el modelo operacional del procesamiento para TI. Ahora, una estrategia de centro de datos definido por el software permite que TI tenga snapshot, cree, mueva, elimine y restaure de forma programática toda una estructura de centro de datos de procesamiento, almacenamiento y red en un software. La automatización del centro de datos, la TI de autoservicio y la transformación completa del modelo operacional de red han probado ser grandes ventajas de la estrategia de centro de datos definido por el software. En las implementaciones, los líderes del negocio y la TI coinciden en que una estrategia de centro de datos definido por el software brinda diferencias que se pueden medir en ventajas de velocidad, agilidad y competitividad de la TI. Los líderes de las operaciones del departamento de TI se benefician rápidamente de la administración automatizada de cambios y la simplificación de la configuración y la administración del hardware subyacente. Tal vez, lo más importante es que la estrategia de SDDC impulsa la capacidad de los equipos de infraestructura y seguridad para alcanzar flexibilidad (diseñada para parecer y volverse un híbrido) y protección (utiliza hardware existente) de la inversión, mayor utilización y una seguridad nunca antes vista en el centro de datos. De hecho, la seguridad probó ser una de las aplicaciones más convincentes de la plataforma de centro de datos definido por el software.

El centro de datos definido por el software: un arma, no un objetivo

A primera vista, la mayoría de los profesionales de seguridad de red de TI verán las nuevas estrategias, como la del centro datos definido por el software, como si fuera un objetivo potencial. La realidad es que el impacto sobre la forma en la que TI trabaja con la seguridad es mucho mayor (y más positivo) que los cambios de lo que se necesita asegurar. En otras palabras, para los equipos de seguridad de TI, el centro de datos definido por el software es más bien un arma que un objetivo. En realidad, una estrategia de centro de datos definido por el software brinda una plataforma que aborda de forma inherente algunas limitaciones fundamentales de arquitectura en el diseño del centro de datos, lo cual ha limitado a los profesionales de seguridad durante décadas.

Piense en cómo se suele elegir entre contexto y aislamiento en las estrategias tradicionales de seguridad. Normalmente, para ganar contexto ubicamos los controles en sistema operativo anfitrión. Esta estrategia nos permite ver a qué aplicaciones y datos se accede y qué usuarios utilizan el sistema, lo que produce un buen contexto. Sin embargo, dado que el control se encuentra en el dominio de ataque, lo primero que hará el atacante será desactivar el control. Este es un mal sistema de aislamiento. Esta estrategia equivale a colocar los interruptores del sistema de alarma de una casa del lado de afuera. Una estrategia alternativa, que cambia contexto por aislamiento, coloca el control en la infraestructura física. Esta estrategia aísla el control del recurso que protege, pero tiene un mal contexto porque las direcciones, los puertos y los protocolos de TI son proxies muy malos para el contexto de los usuarios, las aplicaciones y las transacciones. Además, nunca se diseñó una capa de cumplimiento omnipresente en la infraestructura… hasta ahora.

La capa de virtualización del centro de datos que utiliza el SDDC brinda la ubicación perfecta para obtener el contexto y el aislamiento, junto con el cumplimiento omnipresente. Los controles que funcionan en la capa de virtualización del centro de datos aprovechan la introspección segura del anfitrión y la capacidad de brindar contexto de anfitrión sin agentes y de alta definición, mientras permanece aislado en el hipervisor, seguro del ataque que se lleva a cabo.

La posición ideal de la capa de virtualización del centro de datos entre la infraestructura física y de las aplicaciones, junto con el aprovisionamiento y la administración automatizada de políticas de red y seguridad, el rendimiento incorporado de kernel, el cumplimiento distribuido y la capacidad de escalabilidad horizontal, están a punto de transformar completamente la seguridad del centro de datos y de permitir a los profesionales de seguridad de centros de datos alcanzar niveles de seguridad que antes eran operacionalmente imposibles.

El comienzo de la verdadera red del centro de datos microsegmentado

La estrategia de seguridad de red centrada en el perímetro para centros de datos empresariales demostró ser inadecuada. Los ataques modernos aprovechan la vulnerabilidad de seguridad que exhibe la defensa exclusivamente perimetral para filtrarse junto con usuarios autorizados y moverse lateralmente dentro del perímetro del centro de datos de una carga de trabajo a otra, sin que exista un control suficiente que bloquee la propagación. Muchas de las filtraciones públicas recientes son

ejemplos de esto, como la suplantación de identidad específica o la ingeniería social. Estas prácticas tienen como resultado el ingreso de malware, el aprovechamiento de una vulnerabilidad de seguridad, la obtención del comando y el control, y el movimiento lateral incontenible dentro del centro de datos que les permite a los atacantes encontrar lo que buscan y extraerlo.

La microsegmentación de la red del centro de datos puede ser de gran ayuda para limitar este movimiento lateral no autorizado, pero no ha sido factible desde el punto de vista operacional en las redes tradicionales de centros de datos. ¿Por qué?

Los firewalls tradicionales, e incluso los de última generación, implementan controles como conexiones entre nodos físicas o virtuales en la red. Se dirige un tráfico de carga de trabajo de aplicación para que pasen a través de estos puntos de control, se hacen cumplir las reglas y se bloquea o permite el paso a los paquetes. El uso de la estrategia de firewall tradicional para alcanzar la microsegmentación se encuentra rápidamente con dos obstáculos operacionales: la capacidad de tasa de transferencia y la administración de operaciones o cambios. La primera, la capacidad, se puede superar si se paga el precio. Se pueden comprar suficientes firewalls físicos o virtuales para brindar la capacidad que se necesita y alcanzar la microsegmentación. Sin embargo, la segunda, las operaciones, aumenta exponencialmente con el número de cargas de trabajo y la naturaleza cada vez más dinámica de los centros de datos de la actualidad. Si se necesitan agregar, eliminar o modificar manualmente reglas de firewall cada vez que se agrega, mueve o retira una máquina virtual, la tasa de cambios sobrepasa rápidamente las operaciones de TI. Este obstáculo ha destruido la mayoría de los mejores planes de los equipos de seguridad para concretar una estrategia integral de microsegmentación o “*Zero Trust*”.

Una estrategia de centro de datos definido por el software de VMware aprovecha la plataforma de virtualización de red NSX para ofrecer varias ventajas significativas, en comparación con las estrategias tradicionales de seguridad de red: aprovisionamiento automatizado, tareas automatizadas para mover, agregar y cambiar cargas de trabajo, cumplimiento distribuido en todas las interfaces virtuales y rendimiento de firewall en el kernel, de escalabilidad horizontal, distribuido a todos los hipervisores e incorporado a la plataforma.

Rendimiento

Es importante remarcar que el rendimiento del firewall que ofrece la plataforma NSX no se diseñó para reemplazar las plataformas de firewall de hardware que se utilizan para defender la totalidad del perímetro. La capacidad de rendimiento de las plataformas de firewall de hardware se diseñó para controlar el tráfico de cientos a miles de cargas de trabajo que entran o salen del perímetro del centro de datos.

Aun así, el rendimiento y la capacidad del firewall de la plataforma NSX es muy impresionante. La plataforma NSX brinda 20 Gbps de tasa de transferencia de firewall y es compatible con más de 80 000 conexiones por segundo, por anfitrión. Este rendimiento solo se aplica a las máquinas virtuales en su hipervisor, y cada vez que se agrega otro anfitrión a la plataforma de centro de datos definido por el software, se agregan otros 20 Gbps o capacidad de tasa de transferencia.

Automatización

La tareas para mover, agregar y cambiar cargas de trabajo y el aprovisionamiento automatizados permiten que se aprovisionen las políticas de firewall correctas cuando se crea una carga de trabajo de manera programática. Además, esas políticas siguen la carga de trabajo a medida que se mueve a cualquier parte dentro del centro de datos o entre los centros de datos. Y, si alguna vez se elimina la aplicación, también se eliminan del sistema las políticas de seguridad. Esto elimina la barrera principal, que hizo que sea imposible el suministro de una solución verdadera de microsegmentación.

Además, la red de socios de NSX también puede aprovechar las capacidades de distribución y automatización de la plataforma de centro de datos definido por el software o NSX para permitir que las empresas apliquen una combinación de diferentes capacidades de socio uniendo servicios avanzados de seguridad y cumpliendo diferentes servicios según la situación de seguridad. Por ejemplo, se puede aprovisionar una carga de trabajo con políticas de firewall estándares, lo que permite o limita el acceso a otros tipos de cargas de trabajo. La misma política también puede definir que si se detecta una vulnerabilidad en la carga de trabajo durante el curso de un escaneo normal de vulnerabilidad, se aplique una política de firewall más restringida, que solo permite el acceso a la carga de trabajo por parte de las herramientas que corrigen las vulnerabilidades. Todo está automatizado, siempre en funcionamiento y sin intervención del usuario.

La combinación de rendimiento y automatización que brinda la plataforma NSX permite que se diseñe e implemente una microsegmentación operacionalmente factible en todas las interfaces virtuales.

Seguridad nativa en el centro de datos definido por el software con tecnología de NSX: aislamiento y segmentación

La plataforma VMware NSX brinda de manera inherente tres niveles de seguridad en los centros de datos: aislamiento, segmentación y segmentación con servicios avanzados.

Aislamiento

El aislamiento es la base de casi toda la seguridad de red, ya sea para cumplir, contener o simplemente mantener los entornos de desarrollo, pruebas y producción en interacción. Mientras que las reglas de enrutamiento, listas de control de acceso (ACL, *Access Control List*) o firewall en los dispositivos físicos que se configuran y mantienen de modo manual se han utilizado tradicionalmente para establecer y garantizar el aislamiento, dicho aislamiento y la modalidad multicliente son inherentes a la virtualización de red. Las redes virtuales se aíslan de cualquier otra red virtual y de la red física subyacente por defecto, lo que genera un principio de seguridad de menor privilegio. No se necesitan subredes físicas, redes de área local virtuales (VLAN, *Virtual Local Area Network*), ACL ni reglas de firewall para habilitar este aislamiento. Vale la pena repetirlo… *NO se requieren configuraciones*. Las redes virtuales se crean en aislamiento y permanecen aisladas, a menos que se conecten específicamente.

Cualquier red virtual aislada puede formarse con cargas de trabajo distribuidas en cualquier parte del centro de datos. Las cargas de trabajo de la misma red virtual pueden residir en el mismo hipervisor o en hipervisores separados. Además, en el mismo hipervisor pueden residir cargas de trabajo de varias redes virtuales aisladas. Este es un ejemplo muy útil: el aislamiento entre las redes virtuales permite superponer direcciones IP, lo que posibilita tener redes virtuales de desarrollo, prueba y producción aisladas, cada una con versiones de aplicaciones diferentes, pero con las mismas direcciones IP y todas funcionando al mismo tiempo, en la misma infraestructura física subyacente.

También se aíslan las redes virtuales de la infraestructura física subyacente. Dado que se encapsula el tráfico entre los hipervisores, los dispositivos de red física funcionan en un espacio de direcciones completamente diferente que las cargas de trabajo que están conectadas a las redes virtuales. Por ejemplo, una red virtual puede ser compatible con cargas de trabajo de aplicaciones IPv6 sobre una red física IPv4. Este aislamiento protege la infraestructura física subyacente de cualquier ataque posible que inicien las cargas de trabajo en cualquier red virtual. Nuevamente, todo esto es independiente de cualquier regla de VLAN, ACL o firewall que se requeriría tradicionalmente para crear este aislamiento.

Segmentación

La segmentación está relacionada con el aislamiento, pero se aplica dentro de la red virtual de múltiples niveles. Tradicionalmente, la segmentación de red es una función de un firewall o enrutador físico, que se diseñó para permitir o rechazar el tráfico entre segmentos o niveles de la red. Un ejemplo es la segmentación de tráfico entre un nivel web, un nivel de aplicaciones y un nivel de base de datos. Los procesos tradicionales para definir y configurar la segmentación llevan mucho tiempo y son muy propensos a los errores humanos, lo que da como resultado un gran porcentaje de brechas en la seguridad. La implementación requiere un nivel de conocimiento profundo y especializado en la sintaxis de configuración de dispositivos, en direcciones de red, puertos de aplicaciones y protocolos.

La plataforma de virtualización de redes fundamental VMware NSX brinda funciones básicas de firewall de inspección sin pérdida de estado para ofrecer segmentación dentro de las redes virtuales. Una red virtual puede ser compatible con un entorno de red de múltiples niveles, lo que implica múltiples segmentos L2 con segmentación L3 o microsegmentación en un solo segmento L2, que utiliza firewall distribuido y definido por políticas de seguridad de cargas de trabajo. Como en el ejemplo anterior, estas pueden representar un nivel web, un nivel de aplicaciones y un nivel de base de datos. Los firewalls físicos y las listas de controles de acceso ofrecen una función de segmentación probada, que cuenta con la confianza de los equipos de seguridad de red y los auditores de cumplimiento normativo. Sin embargo, la confianza en esta estrategia para los centros de datos en la nube se ha visto afectada, dado que hay cada vez más ataques, violaciones y tiempo fuera de servicio a causa del error humano en los procesos manuales de aprovisionamiento de seguridad de red y de administración de cambios.

En una red virtual, los servicios de red (L2, L3, ACL, Firewall, calidad de servicio, entre otros) que se aprovisionan con una carga de trabajo, se crean y distribuyen de manera programática al vSwitch del hipervisor. Los servicios de red, incluidos el firewall y la segmentación L3, se

garantizan en la interfaz virtual. La comunicación dentro de la red virtual nunca abandona el entorno virtual, lo que elimina la necesidad de configurar y mantener la segmentación de la red en el firewall o la red física.

Segmentación con inserción, unión y direccionamiento de tráfico de servicios de seguridad avanzados

La plataforma de virtualización de redes fundamental VMware NSX brinda funciones básicas de firewall de inspección sin pérdida de estado para ofrecer segmentación dentro de las redes virtuales. En algunos entornos, se necesitan capacidades de seguridad de red más avanzadas. En estos casos, los clientes pueden aprovechar la plataforma del centro de datos definido por el software para distribuir, habilitar y garantizar servicios avanzados de seguridad de red en un entorno de red virtualizada. La plataforma NSX distribuye servicios de red en el vSwitch para crear un proceso lógico de servicios que se aplique al tráfico de redes virtuales. Se pueden insertar servicios de red de terceros en este proceso lógico, lo que permite que se consuman los servicios físicos o virtuales dentro del proceso lógico.

Todos los equipos de seguridad utilizan una combinación única de productos de seguridad de red para satisfacer las necesidades de su entorno. Toda la red de proveedores de soluciones de seguridad de VMware está aprovechando la plataforma VMware NSX. Los equipos de seguridad suelen tener dificultades para coordinar los servicios de seguridad de red de múltiples proveedores en relación con cada uno. Otra ventaja importante de la estrategia de NSX es su capacidad para diseñar políticas que aprovechan la inserción, la unión y el direccionamiento de servicios para dirigir la ejecución de estos en el proceso lógico de servicios según el resultado de otros servicios, lo que hace posible coordinar servicios de seguridad de red de múltiples proveedores que de otro modo no tendrían ninguna relación.

Por ejemplo, nuestra integración con Palo Alto Networks (vea aquí la publicación del blog) aprovecha la plataforma VMware NSX para distribuir el firewall de siguiente generación de la serie de máquinas virtuales de Palo Alto Networks, que hace que las funciones avanzadas estén disponibles localmente para cada hipervisor. Las políticas de seguridad de red, definidas por las cargas de trabajo de las aplicaciones aprovisionadas o trasladadas al hipervisor, se insertan en el proceso lógico de la red virtual. En el tiempo de ejecución, la inserción de servicios aprovecha la función disponible localmente del firewall de siguiente generación de Palo Alto Networks, que se estableció para proporcionar y garantizar los controles y las políticas basadas en el contenido, el usuario y la aplicación en la interfaz virtual de las cargas de trabajo.

Otro ejemplo incluye a nuestro socio Rapid7, que puede habilitar un escaneo automático y periódico de vulnerabilidad de las máquinas virtuales, y habilitar una política que pone automáticamente en cuarentena a las máquinas virtuales si no cumplen con ciertos estándares. Después de combinar esto con el firewall de última generación de Palo Alto Networks, pudimos lograr una cuarentena automática de cargas de trabajo vulnerables cuando fallaban los escaneos de vulnerabilidad de Rapid7, y el segmento en cuarentena podía quedar protegido con una política de firewall de siguiente generación de Palo Alto Networks que solo admitía herramientas de corrección de entrada y no de salida.

Costo

Una estrategia de centro de datos definido por el software que aprovecha VMware NSX no solo hace que la microsegmentación sea operacionalmente factible, también la hace rentable. Normalmente, los diseños de microsegmentación comienzan con el diseño de tráfico de este a oeste, para conectar entre nodos mediante firewalls físicos de gran capacidad. Como se menciona antes, esta estrategia es costosa y exigente operacionalmente, al punto de no ser factible en la mayoría de los entornos grandes. Normalmente, toda la plataforma NSX representa una fracción del costo de los firewalls físicos en estos diseños, y logra escalar horizontalmente de manera lineal a medida que los clientes agregan más cargas de trabajo.

Centros de datos más seguros: el software definido es la nueva regla

Aún se necesitarán los controles de seguridad de perímetro, pero ahora los controles internos de la red del centro de datos no solo son necesarios; por suerte, también son factibles. La plataforma de virtualización de red VMware NSX, como pilar clave de la arquitectura del centro de datos definido por el software, abrió las puertas a un nuevo modelo operacional para el equipo de seguridad en la infraestructura física que ya posee. No hace falta un hardware de redes nuevo. Virtualice el entorno del centro de datos que esté listo para virtualizar.

En este caso de uso se muestra solo una pequeña parte de las capacidades de seguridad que posibilitan la estrategia de centro de datos definido por el software y la plataforma de virtualización de red NSX. A medida que más y más centros de datos adoptan una arquitectura de centro de datos definido por el software, veremos surgir una amplia gama de soluciones y socios de VMware, que aprovecharán la posición única que ofrece la capa de virtualización del centro de datos definido por el software. Un conocimiento detallado de las máquinas virtuales y de los propietarios de procesos de aplicación, junto con eficacia operacional y de velocidad de aprovisionamiento automatizados, es la base de una nueva estrategia interesante para enfrentar desafíos antiguos en la seguridad de los centros de datos.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304, EE UU. Tel.: 877-486-9273. Fax: 650-427-5001. www.vmware.com/latam