CASO DE USO DEL PRODUCTO – **FEBRERO DE 2018**

CÓMO LAS EMPRESAS MEDIANAS PUEDEN SATISFACER LOS REQUISITOS DE CUMPLIMIENTO Y MEJORAR LA CIBERSEGURIDAD MEDIANTE EL USO DE MICROSEGMENTACIÓN

vmware®

Índice

Para los directores ejecutivos, pocos asuntos son más importantes que la ciberseguridad y el cumplimiento. A pesar de toda la publicidad y atención que reciben estos asuntos, las encuestas muestran que todavía queda mucho por hacer. Un estudio reciente de Fortinet demostró que casi la mitad de los profesionales expertos de TI creen que sus directivos y equipos de administración deben tomar más medidas para proteger la organización.[1]

Sin embargo, una gran cantidad de pequeñas y medianas empresas se enfrentan a una compleja dicotomía: tienen las mismas exigencias de seguridad y cumplimiento que las empresas más grandes de Fortune 500 pero muchos menos recursos para superar estos desafíos. Por lo tanto, es fundamental que elijan una estrategia de seguridad y cumplimiento que sea más eficiente y que haga valer la inversión más que las soluciones heredadas. La estrategia anterior que consistía en comprar distintos productos de seguridad y cumplimiento que resolvían distintos problemas no solo ya no funciona, sino que también suma complejidad y requiere contratar e invertir más dinero en personal para que monitoreen y administren el sistema.

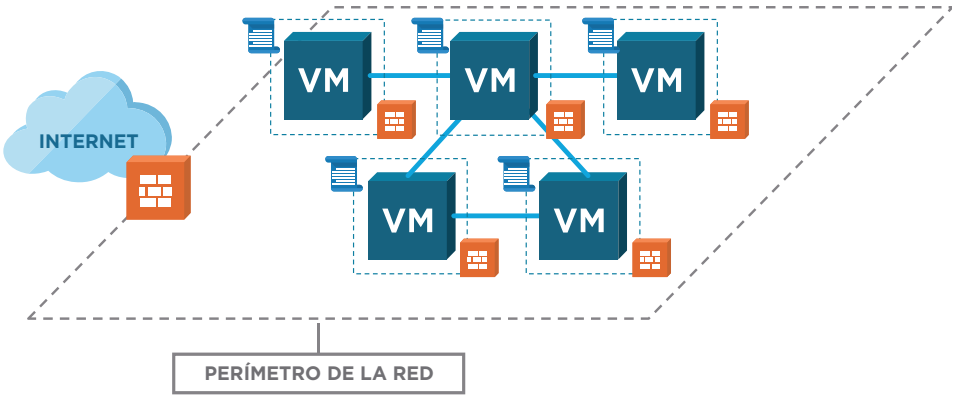
Para responder a la necesidad de mejorar la seguridad y el cumplimiento de manera más eficiente, muchas pequeñas y medianas empresas están evaluando y adoptando una tecnología de red virtual compatible con la microsegmentación, como VMware NSX. Esta tecnología proporciona una plataforma completamente segura que cumple con las normas y que ofrece muchas de las competencias necesarias para satisfacer las exigencias de hoy y de mañana. Es una estrategia básica que además de ser eficaz, es muy eficiente.

Una breve descripción general tecnológica

Aunque a simple vista parezca compleja, esta tecnología es simple y toma como punto de partida la virtualización de redes. VMware NSX separa el hardware de red y las conexiones subyacentes por medio de una plataforma de software de administración que es coherente en todos los aspectos de la red. Toda la complejidad de la red física se representa en la capa virtual de software. De esta manera, la administración y la operación de la red se simplifican y los administradores de red pueden ver toda la red, incluidos el tráfico y el rendimiento. Pero lo más importante es que esta tecnología le permite al equipo de TI proteger la red de forma básica e integral, ya que elimina distintos segmentos de red aislados que pueden crear puntos ciegos y representar un riesgo.

La microsegmentación toma como base la red virtual y le permite al equipo de TI proteger todas las aplicaciones por medio de la implementación de políticas de seguridad en el nivel más detallado de la aplicación: la carga de trabajo individual. Este método protege los recursos de TI que se encuentran dentro del firewall perimetral. Uno de los mayores problemas en la ciberdefensa de hoy en día es que una vez que los hackers atraviesan el firewall, son pocas las defensas que pueden impedir que accedan a las aplicaciones y a los datos más confidenciales. La microsegmentación protege la parte interna del perímetro; más específicamente, protege cada aplicación, base de datos o carga de trabajo.

1 "Fortinet Survey Reveals Almost Half of IT Decision Makers Believe Board Members Still Do Not Treat Cybersecurity as a Top Priority" (Encuesta de Fortinet muestra que casi la mitad de los encargados de decisiones de TI creen que los directivos aún no consideran la ciberseguridad una prioridad), Fortinet, 9 de octubre de 2017



Cómo la microsegmentación resuelve los problemas de seguridad y cumplimiento

Los equipos de administración empresarial de hoy en día, especialmente los de pequeñas y medianas empresas, deben responder a numerosas y rigurosas exigencias de cumplimiento y seguridad. En pocas palabras, las organizaciones deben asegurar que toda información secreta permanezca secreta. La microsegmentación es la herramienta fundamental para alcanzar este objetivo.

Entre las principales ventajas de seguridad y cumplimiento que ofrece la microsegmentación, se encuentran las siguientes:

- **Separación de zonas:** un requisito fundamental de cumplimiento es la separación de "zonas" o la necesidad de restringir la comunicación entre las aplicaciones y los datos incluidos en las directivas de cumplimiento y las aplicaciones y los datos que no lo están. Algunas organizaciones creen que los sistemas principales están segmentados de forma física pero, con la expansión de la red y las incorporaciones imprevistas, muchas veces esto no es así y las organizaciones ya no garantizan el cumplimiento.
- **Eliminación de la estrategia "querer hacer lo imposible":** muchas organizaciones no pueden implementar seguridad y administrar el cumplimiento de forma eficaz centrándose solo en los sistemas más importantes. Por el contrario, intentan proteger o administrar todo con un único proceso de seguridad y cumplimiento. Pero este método casi nunca da resultado. En cambio, con la microsegmentación, los equipos de cumplimiento y de seguridad pueden centrarse en los sistemas más confidenciales y brindarles una mayor protección.
- **Menor impacto de infracciones cibernéticas:** la estrategia más antigua y menos eficaz de proteger el perímetro entre sistemas internos y externos es extremadamente defectuosa. Una vez que los hackers atraviesan las defensas, pueden acceder a todos los sistemas o datos. Pero gracias a la microsegmentación, las organizaciones protegen la parte interna del perímetro con defensas que pueden detener o interrumpir a un atacante que ha atravesado las defensas perimetrales.
- **Seguridad y cumplimiento de políticas coherentes:** gran parte de las directivas de cumplimiento requiere que los negocios creen y apliquen de forma coherente políticas adecuadas de seguridad y administración a fin de proteger los datos y las aplicaciones. Con una red altamente fragmentada, esta opción no es posible ni rentable. Con una red virtual con microsegmentación, las organizaciones pueden crear políticas y, además, garantizar que se implementen de forma coherente en toda la red. Asimismo, ahora también es posible modificar y optimizar con facilidad estas políticas a fin de satisfacer las nuevas demandas de cumplimiento o seguridad.

- **Posibilidad de aprovechar la computación en nube con mayor rapidez y menos riesgos:** la computación en nube ofrece nuevas competencias muy atractivas para los negocios. No obstante, si no se implementa la protección adecuada, el uso de la nube puede originar nuevos problemas de cumplimiento y seguridad. Las redes virtuales y la microsegmentación pueden proteger los recursos basados en la nube con las mismas defensas que se utilizan para proteger los recursos en las instalaciones. De esta manera, las organizaciones obtienen las ventajas de la nube sin ningún riesgo adicional.
- **Documentación de actividades de cumplimiento:** los equipos de cumplimiento suelen usar las políticas y los procesos que se definen para la microsegmentación a fin de comprobar que el sistema esté protegido. Comprobar que el negocio está implementando los procesos fundamentales para cumplir con las pautas normativas puede resultar problemático si la organización no tiene una solución coherente e integral, como la microsegmentación que se ejecuta en una plataforma de red virtual.

La virtualización de redes y la microsegmentación ofrecen ventajas más allá del cumplimiento

Este caso de uso de producto se enfoca en la funcionalidad de cumplimiento y seguridad en la virtualización de redes y la microsegmentación. Sin embargo, las organizaciones y sus equipos de TI gozan de ventajas adicionales sin costo o con un costo módico. Estas ventajas adicionales son importantes debido a que eliminan la necesidad de implementar soluciones tecnológicas alternativas de alto costo y mejoran los retornos de la inversión en redes virtuales y microsegmentación.

La más notable de estas funciones adicionales es la competencia de recuperación ante desastres que forma parte de la solución de red virtual. Con una red virtual, migrar cargas de trabajo desde una red que está experimentando tiempo fuera de servicio a otra que tiene un buen funcionamiento es un proceso rápido y fácil. Esta migración puede realizarse casi de forma "automática" a fin de asegurar que una interrupción en la red no genere mayores problemas. Esta resulta una función muy importante ya que las fallas de red son más frecuentes que antes debido a que se usan redes más antiguas que son complejas, frágiles y cuentan con poca documentación. Además, la complejidad de las redes más antiguas genera tiempos de recuperación más prolongados. Las redes virtuales, en cambio, son independientes del hardware, lo que le permite al negocio usar cualquier hardware de red subyacente e incluso modificarlo en otro momento.

Otra competencia que forma parte de las redes virtuales es el balanceo de cargas de red. Es fundamental que una organización pueda identificar y remediar aquellas situaciones en las que un segmento de red está sobrecargado y perjudica el rendimiento de las aplicaciones o de los sitios web. Algunos negocios compran productos adicionales para realizar esta tarea. Sin embargo, con una solución de red virtual, no es necesario incurrir en estos gastos. Además, con el balanceo de cargas que ofrece la red virtual, las operaciones son más eficientes, lo que permite ahorrar tiempo y, posiblemente, reducir el personal.

Por último, la red virtual es una plataforma que simplifica las operaciones y reduce los gastos operacionales (Operating Expenses, OpEx). La red virtual proporciona una consola de administración única para todos los segmentos de red, lo que elimina la necesidad de administrar distintas partes de la red con distintas herramientas. Gracias a esto, los administradores de red pueden ahorrar mucho tiempo de trabajo. Además de estas ventajas, la red virtual también proporciona una plataforma común que facilita la integración de los equipos de operaciones de sistemas, operaciones de seguridad y operaciones de red. Debido a que utilizan las mismas herramientas, pueden trabajar juntos sin problemas y con mayor eficiencia, y pueden enfocarse en prioridades empresariales reales en lugar de centrarse en cuestiones administrativas.

Las redes virtuales y la microsegmentación tienen un gran valor particularmente para las empresas medianas

Las pequeñas y medianas empresas tienen las mismas exigencias que las empresas más grandes de Fortune 500 pero muchos menos recursos. Como resultado, tienen que elegir soluciones tecnológicas que sean más eficientes de poseer, operar y modificar. La virtualización de redes y la seguridad con microsegmentación responden a estos desafíos.

La microsegmentación es una solución de ciberseguridad moderna y de última generación diseñada para mitigar muchas de las nuevas ciberamenazas a las que se enfrentan las organizaciones. Y, a diferencia de muchos otros productos de seguridad, la microsegmentación es tan simple que las organizaciones no tienen que invertir grandes sumas de dinero en personal de seguridad de TI o contratar a las pocas personas que están familiarizadas con la última tecnología. Implementar y operar redes virtuales con microsegmentación no es un proceso difícil ni lento.

Otra ventaja de las redes virtuales relacionada con la rentabilidad es que proporcionan una solución para otros requisitos de TI sin que sea necesario invertir más dinero. Adquirir las funciones de recuperación ante desastres y balanceo de cargas prácticamente de forma gratuita puede ayudar a las empresas a ahorrar una gran cantidad de dinero que puede invertirse en otras áreas.

Muchas de las empresas pequeñas tienen poco personal de TI. Las redes virtuales eliminan las tareas redundantes que se deben realizar para administrar segmentos de red o instalaciones individuales, ya que proporciona una única consola con un único conjunto de actividades de administración. Esto reduce la cantidad de tareas operacionales que se deben realizar y disminuye la exigencia que reciben los administradores de red, por lo que las organizaciones pueden lograr más objetivos con la misma cantidad de personal. También se aumenta la eficiencia del personal y se ahorra tiempo debido a que se mejoran la colaboración y la comunicación entre los equipos de seguridad, redes y centro de datos. Una red virtual ofrece una plataforma coherente que los tres equipos pueden usar y también funciona como una base de coordinación para los proyectos en los que los tres equipos deben trabajar juntos.

Por último, la red virtual les permite a los negocios aprovechar los aspectos económicos y la agilidad de la computación en nube con mayor rapidez y seguridad. De hecho, las redes virtuales facilitan la adopción de servicios de computación en nube, ya sean públicos o híbridos, en comparación con la mayoría de las implementaciones de red heredadas. Las redes virtuales fomentan la agilidad y la velocidad en vez de inhibirlas.

Conclusiones e información clave

A medida que el alcance y las exigencias de las directivas de cumplimiento y de la protección mediante ciberseguridad aumentan casi diariamente, las empresas deben asegurarse de cumplir los requisitos necesarios. Sin embargo, la estrategia heredada que consiste en comprar distintos productos que cumplen una única función a fin de satisfacer estas demandas ya no es la adecuada. A raíz del costo, la complejidad y la posibilidad de vulnerabilidades ocultas que implica la estrategia heredada es necesario cambiar la manera de pensar.

Las estrategias modernas como el uso de redes virtuales y la tecnología de microsegmentación representan un método optimizado y más eficiente para responder a estos requisitos. Si desea obtener más información sobre esta importante solución de seguridad y cumplimiento, puede consultar los siguientes recursos:

- The Total Economic Impact™ of VMware NSX (informe sobre el impacto económico total de VMware NSX)
- Micro-segmentation for dummies, 2nd edition

Estos recursos le ayudarán a comprender mejor y comenzar a implementar redes virtuales y microsegmentación.

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