DOCUMENTO TÉCNICO, **JUNIO DE 2020**

Protección del centro de datos en solo cuatro pasos

vmware®

Introducción

Durante mucho tiempo, las empresas han delegado la interminable lucha contra los ciberataques en los cortafuegos perimetrales tradicionales, que impiden que los ciberdelincuentes accedan a sus objetivos del centro de datos. Ante la vulnerabilidad patente a la queda expuesta el perímetro hoy en día, las empresas se apresuran a mejorar la situación de seguridad en sus redes corporativas.

Sin embargo, en un contexto de aplicaciones modernas y distribuidas y de cargas de trabajo cada vez más dinámicas, proteger todo o casi todo el tráfico este-oeste (esto es, el interno) siempre ha parecido una tarea demasiado compleja, cara y laboriosa para los centros de datos existentes, e incluso para los nuevos. Sin duda, esa percepción resulta acertada en el caso de las organizaciones que intentan proteger el tráfico este-oeste empleando cortafuegos perimetrales tradicionales basados en dispositivos a modo de cortafuegos internos.

No obstante, existe una alternativa sencilla, rápida y rentable. Los *cortafuegos internos distribuidos con escalabilidad horizontal* están diseñados específicamente para supervisar y proteger el tráfico este-oeste. Por eso, son la solución de seguridad idónea para los centros de datos y las cargas de trabajo actuales, ya que eliminan la complejidad, los gastos excesivos y las limitaciones de escalabilidad y flexibilidad que caracterizan a los cortafuegos perimetrales tradicionales.

Los cortafuegos internos distribuidos, como el *cortafuegos definido por servicio de VMware NSX*, impiden el desplazamiento lateral y, de ese modo, mejoran la seguridad de las cargas de trabajo modernas. Como está distribuido, es fácil de utilizar y cuenta con reconocimiento de aplicaciones, el cortafuegos definido por servicio optimiza y automatiza gran parte de la planificación, la implementación, la configuración y la gestión de los cortafuegos internos, además de las funciones y las políticas detalladas en las que estos se basan.

Con todo, cada vez que se adopta una solución nueva, los equipos de seguridad deben dedicar tiempo y esfuerzo para aprender a utilizar esa tecnología de manera eficaz y a implementarla en el entorno de la organización. En este documento técnico presentamos un enfoque de cuatro pasos que permite a las organizaciones aprovechar rápidamente las ventajas del cortafuegos definido por servicio y, con el tiempo, extender su uso a todo el centro de datos.

Seguridad que supera los desafíos actuales

Tanto los directores de seguridad de la información como sus equipos de seguridad afrontan cada vez más desafíos a la hora de proteger la empresa contra los ciberataques. He aquí algunos de ellos:

- El campo de batalla contra las ciberamenazas se ha trasladado al interior del centro de datos.
- Los equipos tienen poca o ninguna visibilidad del tráfico este-oeste.
- Las amenazas que logran traspasar el perímetro se pueden desplazar lateralmente junto con el tráfico permitido dentro del centro de datos, sin apenas obstáculos que lo impidan.
- Los modelos de teletrabajo y la infraestructura de escritorios virtuales (VDI) permiten que el tráfico entre directamente en el centro de datos, con lo que las cargas de trabajo que se ejecutan en él quedan expuestas a las amenazas.

Las soluciones tradicionales de seguridad basadas en dispositivos carecen de la eficacia necesaria para ofrecer visibilidad de todo el tráfico este-oeste, proteger el tráfico e impedir el desplazamiento lateral de las amenazas. Por ese motivo, las empresas están recurriendo al cortafuegos definido por servicio de VMware. Este cortafuegos interno distribuido protege todo el tráfico este-oeste con un enfoque de seguridad que es intrínseco a la infraestructura, lo cual simplifica drásticamente el modelo de implementación. Si desea obtener más información sobre los problemas que tienen los controles tradicionales de seguridad de la red para proteger las cargas de trabajo modernas, lea el documento técnico *Cinco requisitos esenciales para usar cortafuegos internos en el centro de datos*.

Gracias al cortafuegos definido por servicio, los equipos de seguridad pueden proteger la marca de las amenazas internas y minimizar los daños ocasionados por los ciberataques que logran penetrar el perímetro de red tradicional. Esta solución incluye un *cortafuegos distribuido*, un *sistema de detección y prevención de intrusiones (IDS/IPS)* y técnicas de análisis mediante *NSX Intelligence* (consulte la figura 1).

FIGURA 1: Arquitectura del cortafuegos definido por servicio de VMware NSX

Cuatro pasos para proteger el centro de datos

La implementación de un nuevo enfoque o solución de seguridad requiere una mayor dedicación y entrega por parte de los equipos de seguridad, ya de por sí abrumados por su carga de trabajo. Por ese motivo, aunque proteger el tráfico este-oeste es más fácil y rápido con un cortafuegos interno distribuido, en la mayoría de las organizaciones sigue siendo preferible el enfoque iterativo por fases para mejorar la seguridad del centro de datos.

Aparte de no abrumar a los equipos de seguridad con una iniciativa de gran envergadura, dividir la implementación de los cortafuegos internos en proyectos más pequeños también reporta otra ventaja: les permite acreditar el éxito muy pronto y demostrar el valor del enfoque a las partes interesadas internas. Además, se pueden basar en su experiencia para extender el uso del cortafuegos interno distribuido, de modo que sus progresos favorezcan la madurez, la rapidez y la confianza de la organización.

Si bien existen distintos enfoques, algunos clientes de VMware han seguido los cuatro pasos siguientes (consulte la figura 2) para empezar por lo básico y, con el tiempo, ir reforzando de forma continua las defensas de su centro de datos:

1. Principiante: macrosegmentar la red.
2. Iniciado: proteger las aplicaciones esenciales.
3. Intermedio: obtener visibilidad de otras aplicaciones y protegerlas.
4. Avanzado: proteger todas las aplicaciones.

FIGURA 2: Enfoque de cuatro pasos para proteger el centro de datos

Para obtener más información sobre cómo proteger el entorno de VDI, lea la descripción de la solución *Service-defined Firewall for Virtual Desktops*.

Principiante: macrosegmentar la red

Para muchas organizaciones, el primer paso para proteger el tráfico este-oeste es el más difícil. El motivo es que macrosegmentar la red con cortafuegos tradicionales basados en dispositivos ha demostrado ser una tarea laboriosa, compleja e inflexible, aparte de costosa.

En cambio, los *cortafuegos internos distribuidos* simplifican la arquitectura de seguridad y aceleran la rentabilidad, por lo que resulta más fácil implementar la macrosegmentación para mejorar la seguridad del tráfico este-oeste. También ofrecen más flexibilidad, pues se adaptan fácilmente a los cambios en los requisitos de red y seguridad a medida que la empresa evoluciona.

Gracias al cortafuegos definido por servicio, el equipo de seguridad puede empezar a aplicar la *segmentación de red* para aislar entornos concretos, como los de desarrollo y producción, y protegerlos de los demás. Así se impide de manera inmediata que los atacantes y los usuarios internos malintencionados se desplacen lateralmente entre esos entornos.

Objetivo

El objetivo consiste en implementar el cortafuegos definido por servicio para proteger los segmentos de la red mediante la creación de zonas de seguridad virtuales. Al macrosegmentar los entornos, el equipo de seguridad mejora el enfoque general de seguridad del centro de datos, ya que impide el desplazamiento lateral entre zonas.

Caso de uso típico

Según la estructura empresarial y los casos de uso, el equipo de seguridad se suele decantar por segmentar los entornos que no se deben comunicar directamente entre sí. Algunos ejemplos son las distintas unidades de negocio, los entornos de partners o los entornos de desarrollo y de producción.

Ventajas

- Permite demostrar a las partes interesadas internas de la empresa los buenos resultados que ofrece un enfoque adecuado de cortafuegos internos.
- Impide que los atacantes se desplacen de una zona a otra para limitar a una sola los daños en caso de que un ataque fructifique.
- Ofrece una solución más flexible en comparación con los cortafuegos tradicionales basados en dispositivos, por lo que resulta más sencillo ampliar el número de zonas según las necesidades.

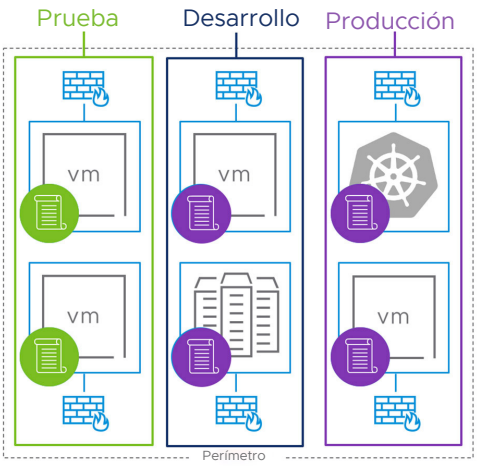

FIGURA 3: Segmentación de la red

Iniciado: proteger las aplicaciones esenciales

Por lo general, el siguiente paso para proteger el centro de datos consiste en pasar de la macrosegmentación a la *microsegmentación*. En este paso, el equipo de seguridad define y aplica controles más detallados que lleguen hasta las cargas de trabajo.

El equipo de seguridad selecciona un número reducido de aplicaciones esenciales para el negocio que se conocen perfectamente. Entonces, las aísla y las protege con más controles de seguridad para evitar el acceso no autorizado, las vulneraciones de datos y otros tipos de ataques.

Los controles detallados de seguridad que se aplican a dichas aplicaciones se pueden mejorar aún más con funciones *IDS/IPS* para detectar los patrones de tráfico que pueden indicar ataques. Aunque es posible aislar aplicaciones con algunas soluciones diseñadas expresamente para la microsegmentación, estas no incluyen funciones IDS/IPS, que resultan imprescindibles para cumplir ciertas normativas, como la Ley de Transferibilidad y Responsabilidad de Seguros Médicos (HIPAA) y la Norma de Seguridad de Datos para el Sector de las Tarjetas de Pago (PCI DSS).

Para obtener más información sobre la visibilidad, lea el documento técnico *Ponga en marcha fácilmente la microsegmentación mediante NSX Intelligence*.

Objetivo

El objetivo consiste en usar la microsegmentación para aislar y proteger una aplicación esencial o varias. Con este objetivo, se aplican controles de seguridad por capas específicos de esas aplicaciones y se impide el desplazamiento lateral de los atacantes, tanto para entrar en el segmento donde se ejecutan como para salir de él.

Caso de uso típico

Al sopesar qué aplicación esencial debe ser la primera a la que aplicar la microsegmentación, las organizaciones suelen elegir el entorno de VDI u otras aplicaciones esenciales como los servicios compartidos; por ejemplo, los servidores DNS o de Active Directory. El entorno de VDI mejora la facilidad de gestión, los costes y la protección de datos de los escritorios de los usuarios, pero también expone la infraestructura del centro de datos a amenazas que se derivan de las infracciones de seguridad de los propios usuarios. Sin embargo, gracias al cortafuegos definido por servicio, el equipo de seguridad puede aislar las zonas destinadas a los escritorios para que queden separadas de los activos confidenciales del centro de datos. La funcionalidad de VMware NSX Distributed IDS/IPS complementa este cortafuegos con más funciones de inspección del tráfico para controlar las amenazas, además del acceso. De ese modo, se facilita el enfoque de seguridad por capas.

Ventajas

- Reduce la superficie de ataque aislando las aplicaciones esenciales de otros activos del centro de datos.
- Mitiga el desplazamiento lateral desde fuera del segmento.
- Activa en las aplicaciones confidenciales controles de acceso específicos de los usuarios y de las aplicaciones.
- Detecta amenazas avanzadas gracias a las funciones IDS/IPS.

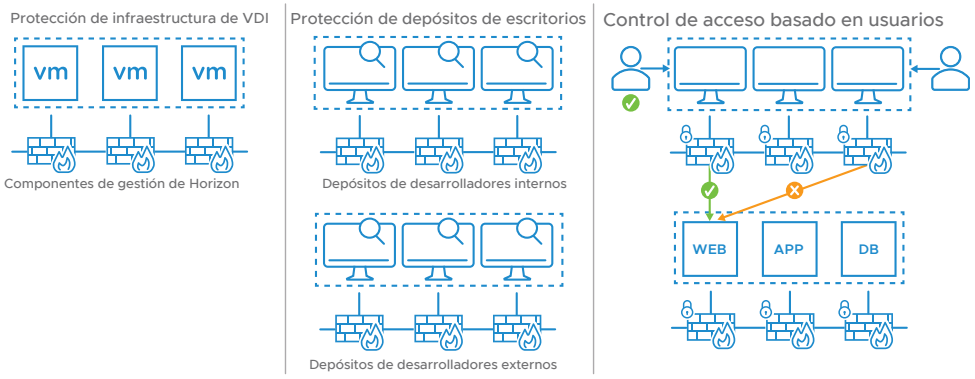

FIGURA 4: Protección de entornos de VDI

Intermedio: obtener visibilidad de otras aplicaciones y protegerlas

Una vez que el equipo de seguridad ha adquirido cierta experiencia en el uso del cortafuegos interno distribuido, puede extender la supervisión y la protección del tráfico este-oeste a otras cargas de trabajo esenciales o importantes del centro de datos.

En el caso de las aplicaciones que no se conocen tan bien, el cortafuegos definido por servicio no solo ofrece visibilidad de todo el centro de datos al equipo de seguridad, sino que aplica el aprendizaje automático integrado para ayudarle a interpretar las aplicaciones y los flujos de tráfico. Además, mediante la detección automatizada de aplicaciones, le muestra un exhaustivo mapa con la topografía de las aplicaciones y, basándose en los flujos de tráfico observados, genera recomendaciones sobre políticas de seguridad automáticamente.

Objetivo

El objetivo consiste en aprovechar los conocimientos y la experiencia que ha adquirido el equipo en los dos primeros pasos, así como las prestaciones de visibilidad y automatización que integra el cortafuegos definido por servicio, para aislar y proteger más cargas de trabajo. De ese modo, se reduce la superficie de ataque y se refuerza la seguridad del centro de datos aún más.

Si desea ver el ejemplo de una organización que implementó el cortafuegos definido por servicio para garantizar la conformidad, lea el documento técnico *Cortafuegos interno: Cómo proteger mejor el tráfico este-oeste.*

Caso de uso típico

En este paso, los equipos de seguridad se suelen centrar en proteger aplicaciones importantes en las que cualquier interrupción o robo perjudicaría los resultados empresariales. Eso incluye aplicaciones que generan ingresos, tratan información confidencial de los clientes o la empresa, u ofrecen experiencias digitales relevantes a los clientes, además de otras que son esenciales para la actividad principal.

Ventajas

- Proporciona visibilidad de la topología de las aplicaciones con un mapa visual que se genera automáticamente y muestra tanto las aplicaciones como los flujos de tráfico, lo que elimina las conjeturas.
- Automatiza el proceso de identificación y aplicación de políticas de seguridad y, además, acelera la creación de políticas a partir de las recomendaciones generadas automáticamente.
- Reduce los puntos ciegos de seguridad aumentando la inspección del tráfico este-oeste para detectar y bloquear el desplazamiento lateral enseguida y, de ese modo, limitar los daños.

Avanzado: proteger todas las aplicaciones

A estas alturas del proceso, los equipos de seguridad están listos para proteger todas las aplicaciones del centro de datos con el cortafuegos definido por servicio. Así mitigan aún más los riesgos para la seguridad y, además, se preparan para proteger las cargas de trabajo nuevas y el tráfico en caso de que aumente. Por otra parte, facilitan el cumplimiento de requisitos normativos gracias a las funciones IDS/IPS del cortafuegos. Las organizaciones que antes usaban cortafuegos perimetrales basados en dispositivos como cortafuegos internos reducen costes al sustituirlos por este cortafuegos definido por servicio.

Objetivo

El objetivo consiste en extender la implementación del cortafuegos definido por servicio para que inspeccione y proteja el tráfico este-oeste de todo el centro de datos, además de aumentar las capas que protegen las cargas de trabajo confidenciales mediante las funciones IDS/IPS.

Caso de uso típico

Si bien el cortafuegos definido por servicio ya supervisa todo el tráfico este-oeste en este punto del proceso, los equipos de seguridad pueden implementar funciones avanzadas de detección y prevención de amenazas con IDS/IPS. De ese modo, se pueden cumplir las normativas relativas a las aplicaciones confidenciales, como la HIPAA o la PCI DSS, entre otras.

Ventajas

- Mejora la protección contra ciberataques de todas las cargas de trabajo del centro de datos.
- Reduce el coste y la complejidad, ya que no hace falta utilizar cortafuegos físicos ni dispositivos de IDS/IPS.
- Simplifica la implementación y la gestión de las funciones IDS/IPS en todas las cargas de trabajo.
- Facilita el cumplimiento normativo, al activar la inspección con IDS/IPS en las aplicaciones confidenciales.

Conclusión

Cuando las empresas toman medidas para proteger el tráfico y las cargas de trabajo del centro de datos contra los ciberataques, deben adoptar un enfoque adecuado de cortafuegos internos para proteger la marca de amenazas internas y minimizar los daños ocasionados por los ciberataques que logran vulnerar la seguridad del perímetro tradicional.

Si los equipos de seguridad se deciden por la estrategia en varios pasos, pueden usar el cortafuegos definido por servicio de VMware para mejorar la seguridad de forma continua a lo largo del tiempo, empezando por las zonas de seguridad virtuales y extendiendo luego su uso a todas las cargas de trabajo del centro de datos. Este cortafuegos protege todo el tráfico este-oeste con un enfoque de seguridad intrínseco a la infraestructura, lo cual simplifica drásticamente el modelo de implementación y permite que dichos equipos aceleren las operaciones de seguridad.

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 - 2.ª planta, 28023 Madrid, España. Tel. +34 914125000 Fax +34 914125001 www.vmware.es
N.º artículo: Securing the Data Center_062420 6/20