Akamai

WHITE PAPER

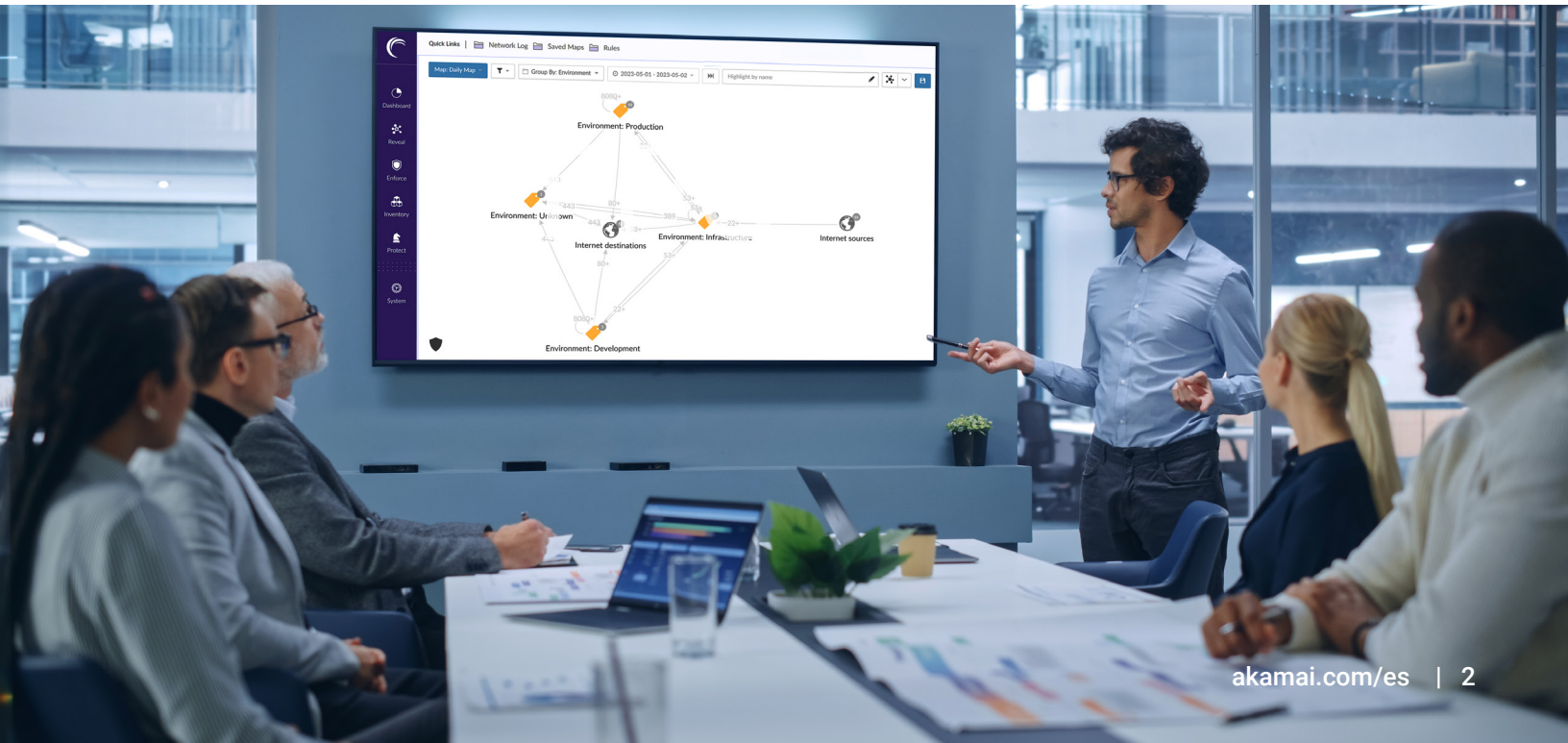
Segmentación definida por software para operadores de centros de datos

Para los operadores de centros de datos multiinquilino, la segmentación de los entornos informáticos no solo es importante, sino que es esencial para su modelo operativo. En primer lugar, necesitan separar su propia infraestructura de los entornos de sus clientes y compartir ciertos recursos a la vez que impiden el acceso a otros. En segundo lugar, deben evitar la "contaminación cruzada" entre los respectivos entornos de sus clientes, ya sea accidental o malintencionada. Esto implica evitar que las filtraciones exitosas o las infecciones de malware se propaguen del entorno de un cliente a los de otros. Por último, en lo que respecta a las aplicaciones operativas propias, se requiere un buen nivel de separación para limitar el impacto de una posible filtración. Si analizamos más a fondo las redes operativas de los proveedores de centros de datos, existen tres escenarios en los que la segmentación, si se logra de forma eficiente, puede mejorar significativamente la estrategia de seguridad y reducir los costes:

1. **Separación de las redes operativas** (DCIM, BMS, etc.) de la red empresarial (los sistemas internos del proveedor, que incluyen la facturación) y las redes de los clientes

2. **Reducción del riesgo de movimiento lateral dentro de la red operativa**, que cuenta con muchos sistemas a los que es difícil aplicar parches y genera riesgos si no se segmenta correctamente

3. **Creación de una conectividad eficaz y segura entre las redes orientadas al cliente**, como DMZ, donde se encuentra el portal personalizado, que necesita un acceso seguro a los datos desde las redes operativas (por ejemplo, para leer el estado de alimentación) y las redes empresariales (para leer la información de facturación)



En la actualidad, esto se gestiona mediante estructuras de red muy complejas, lentas de implementar e ineficientes, VLAN, redes provisionales, etc. Al implementar una solución definida por software que no dependa de configuraciones de red complejas, se reducirán significativamente los costes y se podrá controlar la conectividad de una forma más estricta y robusta.

Por otro lado, los clientes tienen dificultades para implementar y mantener un nivel profundo de segmentación en sus aplicaciones (alojadas o locales). Esto supone una importante oportunidad para que los operadores de centros de datos empleen su experiencia, herramientas y modelos operativos internos relativos a la segmentación para ofrecer servicios gestionados a sus clientes y crear un flujo de ingresos muy atractivo en torno a una práctica de segmentación. Además, gracias a la capacidad de extender las políticas de seguridad a las instalaciones del cliente con la metodología, las herramientas y los procesos adecuados, el operador podrá obtener acceso a las aplicaciones no alojadas y visibilidad de las mismas, lo que puede ayudar a acelerar su migración segura al centro de datos alojado y resulta ventajoso para el negocio principal.

Equifax: el peor de los casos

Si se está preguntando "qué es lo peor que podría suceder" con una segmentación del entorno débil, ineficaz o inexistente, la conocida filtración de Equifax en 2017 es un buen ejemplo histórico. La filtración tuvo como consecuencia la exposición de datos personales altamente confidenciales de 143 millones de estadounidenses. Según la investigación de la Oficina de Rendición de Cuentas del Gobierno de EE. UU. (GAO), los atacantes accedieron inicialmente al portal de resolución de disputas de clientes de la gigantesca agencia de crédito aprovechándose de una vulnerabilidad, conocida como CVE 2017-5638, en el entorno web Apache Struts. Una vez dentro, pudieron moverse libremente por los sistemas de la empresa durante 76 días. El informe de la GAO atribuyó esta libertad de movimiento lateral a la falta de segmentación, que permitió un acceso fácil y a voluntad a las bases de datos, una superficie de ataque prácticamente ilimitada.

La cuestión es cómo lograr este tipo de segmentación de la manera más eficaz, eficiente y económica. Históricamente, los operadores han dependido de firewalls tradicionales o VLAN para separar los entornos dentro de una arquitectura multiinquilino o multiusuario. Sin embargo, la implementación y el mantenimiento de dichas medidas suele ser un proceso arduo, muy manual, laborioso y costoso. Y, por si fuera poco, estas técnicas no son herméticas en absoluto y pueden dejar expuesta un área sustancial de superficie de ataque. La eficacia de las soluciones diseñadas para la defensa perimetral es especialmente problemática en el centro de datos, sobre todo porque la mayoría de estos entornos incluyen una amplia variedad de máquinas virtuales, hipervisores, contenedores e incluso componentes de nube, y las cargas de trabajo se activan y desactivan de forma dinámica y automática. Otro apunte importante es que la segmentación con VLAN requiere tiempo de inactividad de las aplicaciones, lo que para los controles operativos críticos puede ser un obstáculo insalvable.

Por todas estas razones, los operadores de entornos compartidos están considerando con más detenimiento las técnicas modernas de segmentación definidas por software, incluida la microsegmentación. Los avances en las tecnologías de microsegmentación la han convertido en una opción viable para todo tipo de empresas y, posiblemente, la opción idónea para lograr un modelo de seguridad Zero Trust. Igualmente importante, con las herramientas adecuadas y un poco de planificación cuidadosa, la microsegmentación no solo se puede implementar de forma más rápida y sencilla que los métodos mencionados anteriormente, sino que también es más fácil de gestionar y mantener. De hecho, pruebas recientes han demostrado que la microsegmentación es capaz de reducir el tiempo de implementación hasta 30 veces en comparación con la implementación de los firewalls tradicionales. Una ventaja adicional crucial: con la segmentación definida por software, no se requieren cambios en la red ni tiempo de inactividad de las aplicaciones. Este ahorro de tiempo y eficiencia se traduce en una reducción significativa de los costes a lo largo del ciclo de vida de implementación.

Los inconvenientes de los enfoques convencionales

Para comprender las ventajas de la segmentación definida por software o la microsegmentación, resulta útil, a efectos comparativos, analizar algunas de las desventajas y limitaciones de las técnicas estándar empleadas tanto en entornos locales como en la nube. Estas pueden incluir alguna combinación de firewalls físicos o virtualizados y configuraciones de red, como las VLAN. En general, estos métodos consumen muchos recursos y son trabajosos. La creación de políticas de seguridad es un proceso complejo. Las adiciones y modificaciones deben realizarse manualmente, lo que supone un lastre para la eficiencia operativa continua y aumenta el riesgo de vulnerabilidades.

Los firewalls internos, en particular, son caros y complejos de configurar. También interfieren con el flujo normal de tráfico, alterando patrones y creando conexiones tortuosas que, en última instancia, frenan el rendimiento del sistema. El sector se está dando cuenta de que los firewalls no están diseñados para efectuar la segmentación en el centro de datos. De hecho, algunos proveedores admitirán fácilmente que ese no es el sitio de los firewalls.

Uno de los desafíos más difíciles de superar al intentar introducir la segmentación en un entorno de producción existente y operativo es que los métodos tradicionales requieren tiempo de inactividad de las aplicaciones. Y el tiempo de inactividad es costoso. No solo eso, sino que solo puede tener lugar durante períodos de tiempo específicos y a menudo no es posible en absoluto.

Otro desafío destacable es que la creación de una segmentación interna requiere un buen conocimiento de las dependencias este-oeste de las aplicaciones. Y es muy poco frecuente que se disponga de esa información. Sin una forma sencilla de asignar las dependencias de las aplicaciones, es extremadamente difícil y arriesgado separar un entorno existente.

Motivos por los que la segmentación definida por software es más eficaz

Eficiencia operativa y una mejor estrategia de seguridad: la segmentación definida por software supera las ineficacias inherentes de las técnicas tradicionales y, lo que quizás es más importante, da lugar a una mayor seguridad para los entornos con varios usuarios. Como su nombre indica, la segmentación definida por software adopta el concepto de segmentación de red y lo implementa sin necesidad de modificar la infraestructura. Implica la creación de políticas de seguridad en torno a aplicaciones individuales o agrupadas de manera lógica, independientemente de dónde residan en el centro de datos híbrido. Estas políticas dictan qué aplicaciones pueden o no comunicarse entre sí: un verdadero enfoque Zero Trust.

Ausencia de cambios manuales y de tiempo de inactividad: la segmentación definida por software no requiere ningún cambio en la red ni la creación de VLAN, lo que se traduce en un ahorro operativo significativo. Tampoco requiere tiempo de inactividad de las aplicaciones ni cambios debido a la migración a una nueva VLAN. Y esto es importante. En lo que respecta a muchas aplicaciones para las que el tiempo de inactividad es muy caro o imposible, esta es la única forma de proporcionar esta medida de seguridad crucial.

Amplia visibilidad: además, las soluciones avanzadas de segmentación definida por software, diseñadas para hacer frente a los desafíos de la segmentación del tráfico de este a oeste, proporcionan una herramienta de visibilidad integrada que ayuda a identificar los límites de los segmentos y las dependencias de las aplicaciones. Esto se traduce en un proceso eficaz y acaba con los errores operativos al crear las políticas.

Automatización de políticas y controles: la segmentación definida por software también permite aplicar políticas de forma dinámica: a medida que las cargas de trabajo se activan o desactivan, se les asigna automáticamente la política correcta. Esto permite ahorrar una cantidad notable de recursos al eliminar la necesidad de movimientos, adiciones o cambios manuales.

Independencia de la infraestructura: una ventaja clave de la segmentación definida por software es que no depende de la infraestructura. La misma herramienta proporciona visibilidad y segmentación en cualquier infraestructura: bare metal, virtualizada, PaaS, nube, contenedores, etc. Todo en una vista unificada y con un único flujo de trabajo. Esto permite adoptar todo tipo de estándares de seguridad sin restricciones a la hora de elegir la infraestructura subyacente.

Mayores ingresos y relaciones más robustas: lo más importante es que esto supone una oportunidad crucial para los operadores de centros de datos. Mientras gestionan y proporcionan la segmentación interna, pueden aprovechar la formación, las herramientas y los procesos para ofrecer un servicio gestionado muy necesario a sus clientes, gestionando la segmentación no solo para las aplicaciones alojadas, sino también para las aplicaciones que están en las instalaciones del cliente o en la nube dentro de la misma herramienta, todo desde una vista unificada. Esto no solo da lugar a un potencial de ingresos adicional, sino que también crea una mayor dependencia del operador, lo que se traduce en relaciones más largas y mayores beneficios.

¿Por qué Akamai?

Para ofrecer estas ventajas, una solución de segmentación definida por software debe cumplir una serie de criterios esenciales. Debe permitir una visibilidad profunda a nivel de proceso de todas las aplicaciones que se ejecutan en el entorno informático y ofrecer la capacidad de asignar todos los flujos de datos que haya en ellas. La flexibilidad para etiquetar correctamente los activos para la creación de políticas y modificar las etiquetas sin operaciones manuales a medida que las cargas de trabajo se escalan automáticamente también es fundamental para una implementación y una gestión eficientes. Además, la solución debe ser independiente de la plataforma y la infraestructura. Las políticas deben ser capaces de seguir sus respectivas aplicaciones y funcionar de forma coherente en los distintos entornos. Por último, la solución debe permitir un modelo operativo automatizado y simplificado para la creación, gestión y aplicación de políticas.

Akamai Guardicore Segmentation es la única solución que cumple todos estos criterios. La segmentación definida por software es nuestra capacidad principal. La solución proporciona una visualización gráfica sin precedentes de todos los activos del entorno y de las dependencias entre ellos, ya sean bare metal, máquinas virtuales, nube pública, contenedores o dispositivos del Internet de las cosas (IoT). Esta visibilidad profunda acelera drásticamente el proceso de identificación, agrupación y creación de políticas de seguridad en torno a los microsegmentos de aplicaciones.

Para obtener más información, visite akamai.com/guardicore.

Akamai protege la experiencia de sus clientes, su personal, sus sistemas y sus datos, ayudándole a integrar la seguridad en todo lo que crea, dondequiera que lo cree o distribuya. La visibilidad de las amenazas globales que ofrece nuestra plataforma nos permite adaptar y desarrollar su estrategia de seguridad para integrar el enfoque Zero Trust, detener el ransomware, proteger las aplicaciones y las API o combatir los ataques DDoS, y le proporciona la confianza necesaria para innovar, crecer y transformar todo su entorno. Para obtener más información acerca de las soluciones de seguridad, informática y distribución de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en Twitter y LinkedIn. Publicado en junio de 2023.