RESUMEN DE LA SOLUCIÓN

La Generación de la Nube: Una Tormenta Perfecta de Desafíos de Seguridad

Symantec™

Introducción

A medida que la adopción de la nube se acelera y todos nos acostumbramos a la simplicidad, flexibilidad y ventajas de costos del modelo en la nube, no debemos perder de vista un aspecto fundamental: La Seguridad para la Generación de la Nube no es nada sencillo.

El crecimiento explosivo en la cantidad de usuarios móviles, aplicaciones en la nube, oficinas remotas y requisitos de cumplimiento, acompañada de una serie de amenazas emergentes de seguridad, ha creado una tormenta perfecta de complejidad que está desafiando a su límite a los equipos de seguridad y las operaciones de red.

La verdad es que los modelos de seguridad heredados no funcionan bien para la Generación de la Nube. Los enfoques tradicionales de backhauling para la seguridad de la red – que envían el tráfico de Internet desde instalaciones remotas y usuarios móviles a través del centro de datos corporativo, donde se aplican las políticas de seguridad y cumplimiento de datos – están desactualizados, son lentos e ineficientes.

Lo que se necesita es un enfoque más simple, optimizado y más completo centrado en algunos conceptos clave:

Vaya más allá de los principios básicos de seguridad de aplicaciones web y en la nube

Muchas organizaciones confían en gateways web seguros (SWG) para realizar las funciones básicas de seguridad web y en la nube: filtrado de URL, aplicación de políticas de uso, flujo seguro de datos a aplicaciones web y en la nube y escaneo y orquestación del tráfico cifrado.

Sin embargo, la Generación de la Nube requiere mucha más funcionalidad de sus SWG.

Al considerar un SWG basado en la nube, busque un servicio que:

- Inspeccione de forma selectiva el tráfico cifrado SSL / TLS para escanear con precisión el contenido en busca de malware
- Utilice técnicas avanzadas, como el aislamiento de la web, para bloquear amenazas y ataques de phishing dirigidos a los navegadores web de los empleados
- Escaneé el contenido con servicios de prevención de pérdida de datos (DLP) para evitar fugas de datos
- Proteja las aplicaciones en la nube mediante controles de seguridad de acceso a la nube (CASB) para proteger los datos que interactúan con las nubes públicas
- Se integre con la protección contra amenazas instalada en sus endpoints
- Dirija fácilmente el tráfico remoto a la seguridad en la nube a través de SD-WAN opcional y dispositivos similares

Symantec Web Security Service: Creado para la Generación de la Nube

Symantec Web Security Service ofrece un conjunto amplio de protección de amenazas y capacidades de seguridad desde la nube. Respaldado por una sólida infraestructura en la nube y la fuerza y el alcance de nuestra red global de inteligencia, Symantec Web Security Service protege sus datos confidenciales, en cualquier lugar. Symantec es líder en soluciones para la generación de la nube, y trabaja para garantizar que sus aplicaciones web y en la nube sean productivas, seguras y compatibles.

Administre el riesgo y mantenga el cumplimiento mientras migra a la nube

La gestión del riesgo regulatario presenta serios desafíos. Mantenerse en conformidad requiere visibilidad y control de los datos confidenciales, en cualquier lugar que residan. Esto es especialmente desafiante cuando los documentos se comparten fácilmente en las aplicaciones en la nube, algunas de las aplicaciones adoptadas directamente por los empleados que eludieron el proceso de aprobación de TI.

Las capacidades de Cloud Access Security Broker (CASB) ofrecen visibilidad de todas las aplicaciones en la nube utilizadas por sus empleados. Con esta visibilidad, puede tomar medidas para garantizar que el uso de la aplicación en la nube cumpla con las políticas de la compañía y que los datos confidenciales estén protegidos de forma adecuada.

Al considerar CASB, busque una solución que:

- Identifique con precisión las aplicaciones en la nube que utilizan sus empleados.
- Proporcione herramientas y datos para evaluar los riesgos del uso de estas aplicaciones en la nube.
- Controle el acceso a las aplicaciones en la nube por usuario, grupo, ubicación, etc.

Resuelva el dilema de rendimiento y costo

Multiprotocolo de conmutación por etiquetas (MPLS) es una técnica de transporte de datos para redes de alta velocidad. Los enlaces MPLS ofrecen un rendimiento que con frecuencia los convierte en la opción preferida para realizar el backhauling del tráfico de Internet de otras unidades a los centros de datos corporativos principales, donde se aplican políticas de seguridad y protección contra amenazas. Sin embargo, el backhauling de tráfico a través de enlaces MPLS, dado el crecimiento explosivo en el tráfico de aplicaciones web y en la nube, es un costo que está creciendo fuera de control.

Además, el backhauling agrega una latencia significativa a las transacciones de aplicaciones web y en la nube, lo que resulta en velocidades lentas y una experiencia de usuario deficiente para los empleados de otras unidades, y una experiencia potencialmente peor para los trabajadores que utilizan dispositivos móviles.

Backhauling no es el único factor que contribuye al bajo rendimiento de la red. La inspección SSL, necesaria para tareas como el bloqueo de malware oculto en el tráfico cifrado, también agrega latencia. La interceptación y descifrado consumen bastante CPU y, cuando se realiza de forma ineficiente con un dispositivo inadecuado (piense en un firewall de próxima generación), impacta de forma negativa el rendimiento hasta en un 80% (según una **investigación de NSS Labs**).

Para concluir, la Generación de la Nube también presenta un conjunto único de problemas de rendimiento en los endpoints. A medida que los usuarios incrementan su acceso al contenido desde ubicaciones remotas con computadoras portátiles y teléfonos inteligentes, se necesitan más agentes para ampliar la seguridad a cada dispositivo conectado. Cada agente quiere una porción de la memoria del dispositivo; esto acaba acumulándose, perjudicando el rendimiento y reduciendo la velocidad de conectividad.

Es demasiado arriesgado brindarles a los usuarios acceso directo a la web y a la nube, ignorando la necesidad de seguridad de la información y la inspección para prevenir las amenazas. Sin embargo, la manera antigua, el backhauling del tráfico y el uso excesivo de la capacidad de agentes, es costoso, lento y no sostenible.

La nube ha creado una tormenta perfecta de desafíos. Afortunadamente, la nube también es el lugar donde puede encontrar las respuestas a sus inquietudes de rendimiento.

Vea cómo los servicios de seguridad entregados en la nube mejoran el rendimiento:

- Los servicios de seguridad entregados en la nube eliminan la necesidad de realizar un backhaul del tráfico para la aplicación de políticas de seguridad; tales servicios pueden ser accedidos directamente por sus empleados remotos, por lo que las políticas se aplican a medida que el tráfico va a las aplicaciones web y en la nube.
- Los servicios de seguridad en la nube que ofrecen capacidades preintegradas, como la prevención contra la pérdida de datos, sandbox, aislamiento y CASB, están diseñados para intercambiar datos entre sí de manera uniforme; la transferencia eficiente de datos con transferencias optimizadas representa menor latencia y una mejor experiencia del usuario.
- Del mismo modo, algunos servicios de seguridad en la nube están proyectados para inspeccionar con rapidez y eficiencia el tráfico cifrado SSL, proporcionando la protección que necesita con el rendimiento que exigen sus usuarios.

No todos los servicios de seguridad entregados en la nube mejoran el rendimiento con la misma eficiencia. Al evaluar servicios, busque aquellos alojados en una infraestructura de nube diseñada para la escalabilidad y el alto rendimiento. Asegúrese de que los servicios utilicen capacidades como el peering de contenido para mejorar la latencia con Office 365, por ejemplo, y la optimización de la ventana TCP para aumentar el rendimiento al mover archivos grandes de ida y vuelta con Box y otras aplicaciones de almacenamiento en la nube.

Administre sus políticas de seguridad de manera eficiente

Finalmente, a medida que los requisitos normativos y las exigencias corporativas evolucionan rápidamente, vale la pena tener una estructura flexible que le permita definir e implementar de forma rápida las políticas de seguridad. Asegúrese de migrar sus políticas locales existentes a su nueva seguridad entregada en la nube. Si posee un entorno de seguridad híbrido, local y en la nube, busque una administración unificada de políticas con el objetivo de que pueda definir políticas solo una vez y las envíe a todos sus gateways de seguridad, independientemente de dónde se encuentren.

Confíe en su solución de administración de políticas para:

- Simplificar la transición de su organización a la seguridad basada en la nube
- Crear y administrar políticas consistentes en todos los gateways
- Maximizar su inversión existente en la creación de políticas

Sobre a Symantec

Symantec Corporation (NASDAQ: SYMC) es líder mundial en soluciones de ciberseguridad y ayuda a las compañías, gobiernos e individuos a proteger sus datos más importantes en cualquier lugar. Compañías en todo el mundo buscan a Symantec para soluciones estratégicas e integradas para defenderse contra ataques sofisticados en endpoints, en la nube e infraestructura. De la misma forma, una comunidad global de más de 50 millones de personas y familias dependen de la suite de productos Norton y LifeLock de Symantec para proteger sus vidas digitales en casa y en todos sus dispositivos. Symantec opera una de las redes civiles de ciberinteligencia más grande del mundo, lo que le permite ver y proteger contra las amenazas más avanzadas. Para más información, visite **www.symantec.com** o síganos en **Facebook**, **Twitter** y **LinkedIn**.

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | +1 (800) 721 3934 | www.symantec.com

19B176756_SB_CLOUD_GEN_PERFECT_STORM_EN