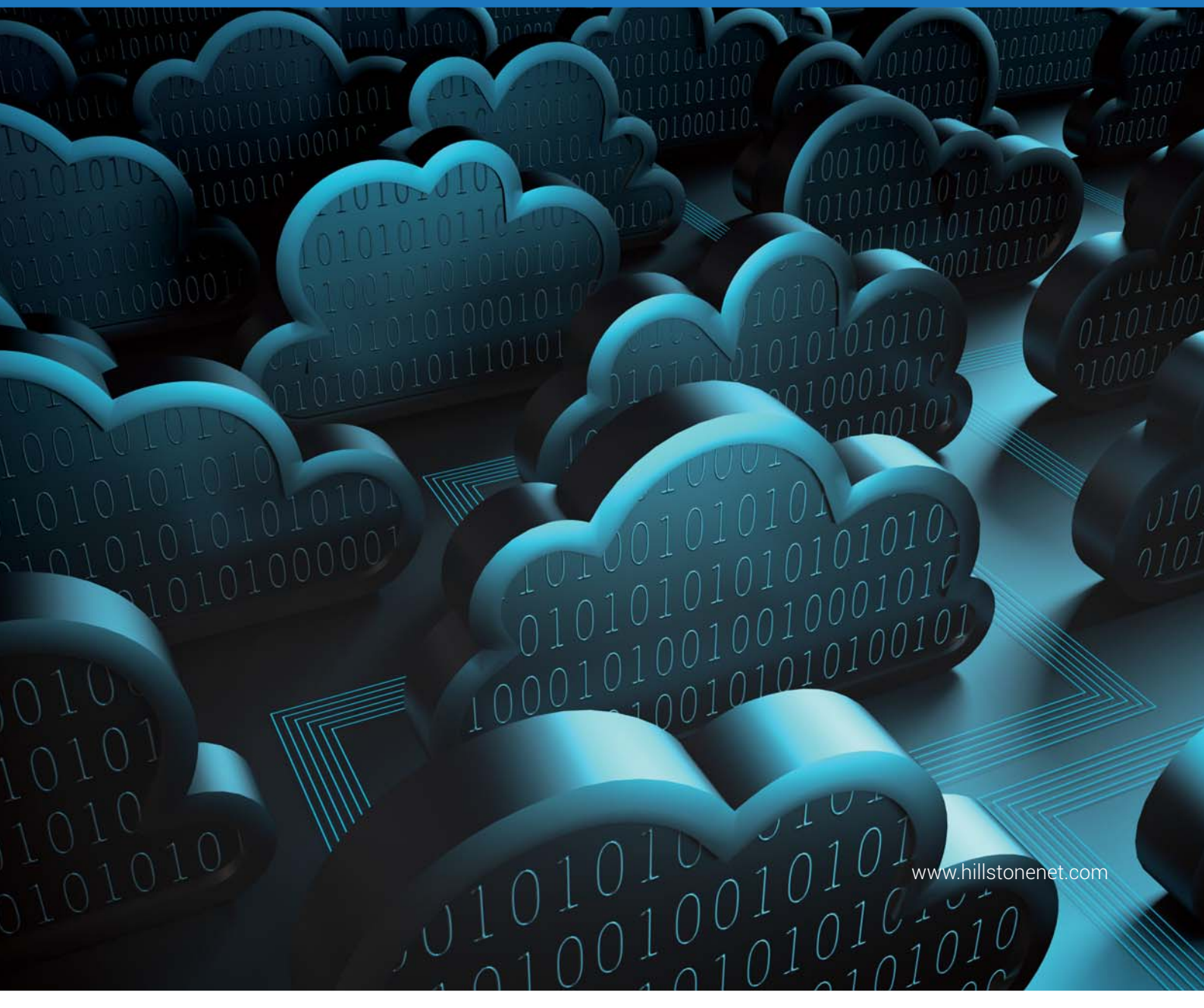
Hillstone™
NETWORKS

Hillstone CloudHive:

Micro-segmentación de Seguridad para Centros de Datos Virtualizados



Como los centros de datos han evolucionado desde lo físico a lo virtual, de empresarial a la nube, los problemas de seguridad que enfrentan han evolucionado también. Algunas de las tendencias que han cambiado la naturaleza de la seguridad del centro de datos incluyen:

Multi-Alquiler Los días de un centro de datos que servía a una sola organización se están desvaneciendo rápidamente. Hoy en día los centros de datos virtuales y aquellos en la nube, ya sean privados, públicos, comunitarios o híbridos, son más propensos a servir a varias organizaciones, filiales o departamentos. Los ejemplos incluyen las agencias gubernamentales, organizaciones de salud u otras entidades que comparten una sola nube comunitaria o cientos de organizaciones no relacionadas que se aprovechan de la infraestructura de la nube pública y sus aplicaciones.

Con el multi-alquiler, una organización puede ser atendida por varias máquinas virtuales y por aplicaciones que comparten no sólo el mismo centro de datos, sino los mismos servidores físicos con otros inquilinos. Para evitar filtraciones de datos y la propagación de malware de inquilino a inquilino, la infraestructura virtual de cada organización debe estar aislada y protegida de las otras organizaciones que comparten la misma nube, red o servidor.

Multi-nube El concepto de centro de datos como un lugar físico se ha desvanecido a medida que las organizaciones han ampliado su infraestructura y sus aplicaciones a través de organizaciones públicas, privadas, y de múltiples nubes. Hoy en día, incluso un solo proceso de negocio o aplicación puede depender de la infraestructura y los componentes que abarcan múltiples servicios en la nube y varios tipos de nubes.

Norte-Sur al Este-Oeste En los primeros días físicos del centro de datos en Internet, la seguridad trataba sobre todo de supervisar y asegurar el tráfico que entraba y salía de un perímetro bien definido de la red. Hoy en día, el tráfico de este a oeste entre máquinas virtuales, los servicios web y sus aplicaciones que comparten el mismo centro de datos y servidores físicos es igual o más común, no sólo entre los diferentes inquilinos, pero los servidores y componentes de una única aplicación compuesta u otros basados en la Web. Sin la protección adecuada, las amenazas a un servicio o componente Web pueden infectar fácilmente a los otros.

SDN y NFV Aunque la virtualización se trató por muchos años principalmente de servidores, aplicaciones y almacenamiento, hoy en día la red sev ha puesto al día, con hardware de red transformándose en redes virtuales y software definidos. Las redes basadas en software tienen ventajas obvias en términos de normalización, agilidad y movilidad. Desafortunadamente, las soluciones SDN y NFV de hoy en día a menudo se sigue poniendo al día con la robusta seguridad de hardware de red legado desarrollado durante décadas, seguridad que a menudo era difícil de configurar y de mantener.

Movilidad y Elasticidad La virtualización ha dado lugar a un centro de datos dinámico, infinitamente elástico, con datos móviles, máquinas virtuales, almacenamiento y despliegue de recursos en la red, con expansión, contratación y migración a voluntad. La protección de un entorno de centro de datos dinámico con tales soluciones, basadas en dispositivos fijos no es una estrategia viable. Es posible desviar todo el tráfico VM-a-VM y el tráfico inquilino a inquilino a través de una solución de seguridad fija. Sin embargo, una estrategia de este tipo es ineficiente, difícil de manejar y obliga a tener una latencia y rendimiento de las aplicaciones con impacto negativo, ralentizando el ritmo del negocio.

Lo que se Necesita para la Verdadera Seguridad el la Nube

El centro virtual de datos habilitado para la nube necesita una nueva estrategia de seguridad y la solución que pueda hacer frente a las demandas virtuales con un impacto mínimo en el rendimiento. Esta solución debe ofrecer las siguientes capacidades:

Una solución habilitada para ambiente virtual/nube Cualquier solución de seguridad debe ser virtual, flexible y elástica como la infraestructura a la que sirve. Debe ser consciente del hipervisor y capaz de insertarse profundamente en el entorno virtual, protegiendo las comunicaciones entre los recursos virtuales a su despliegue, crecimiento, reducción y migración a través del centro de datos. Debe integrarse perfectamente con las plataformas de gestión y orquestación virtual y en la nube como VMware vCenter y OpenStack, y con los hipervisores como ESXi, y debe ofrecer servicios API amigables en la nube, como una API RESTful para que se pueda asegurar la infraestructura y las aplicaciones en un entorno multi-nube.

Mientras que las plataformas de gestión tales como vCenter le permiten a Informática configurar vLANs para segmentar los diferentes usuarios y máquinas virtuales, el proceso de configuración es manual y tedioso. Cualquier solución de seguridad virtual debe ser capaz de aislar el tráfico de forma rápida, sencilla y automatizada basada en la política y el cambio constante.

La visibilidad integral NS/EW Cuando la seguridad se centraba principalmente en el tráfico Norte-Sur dentro de la red de firewall físicos eran una solución viable. Una solución virtual, basada en la nube debe tener una visibilidad y una visión de todo el tráfico Norte-Sur y Este-Oeste entre los inquilinos y los servidores virtuales, incluyendo la red virtual, las máquinas virtuales, las

aplicaciones y la multi-nube. Se debe tener las herramientas para mostrar toda esa información de manera clara y llamar la atención sobre las anomalías y posibles problemas de seguridad en un formato que los haga fácil de detectar y abordar.

Escalabilidad y Movilidad El centro de datos virtual móvil, de alta elasticidad necesita una solución de seguridad altamente elástica, escalable y móvil que una las políticas a toda las máquinas virtuales, permaneciendo con cada una a medida que se despliega, se mueve y emigra, sin ningún impacto en el rendimiento de la seguridad o sobre la aplicación.

La seguridad multifunción L2-L7 A medida que el malware y las violaciones de datos se tornan cada vez más sofisticados, se ocultan mejor y son capaces de pasar por alto las soluciones de seguridad tradicionales. Han quedado atrás los días de la seguridad dirigida por una sola aplicación, herramienta o capacidad. Para que una solución de seguridad en la nube tenga éxito, debe aprovechar múltiples estrategias y capacidades de seguridad, incluyendo el control de acceso, la detección de aplicaciones y firewall, la prevención de intrusiones y la protección contra programas maliciosos. La solución debe ser capaz de hacer frente a todas estas capacidades con un impacto mínimo en el rendimiento.

Hillstone CloudHive

Hillstone CloudHive es una solución de seguridad avanzada, diseñada desde cero para las exigencias del centro de datos virtual, multiusuario y multi-nube habilitado. Gracias a la avanzada micro-segmentación y una API estándar de orquestación en la nube, CloudHive inserta sus capacidades de vigilancia y seguridad profunda y sin problemas en el entorno virtual. Supervisa y dirige todo el tráfico norte-sur y este-oeste para detectar, aislar y eliminar el malware, las violaciones de datos potenciales y otros problemas de seguridad antes de que puedan propagarse a través de las máquinas virtuales, los inquilinos y las redes virtuales.

CloudHive escala sus recursos de seguridad virtual de forma automática exactamente dónde y cuando se necesitan, vinculando y envolviendo todas las máquinas virtuales a medida que se despliegan, se mueven y emigran a través del centro de datos virtual y la multi-nube (Figura 1).

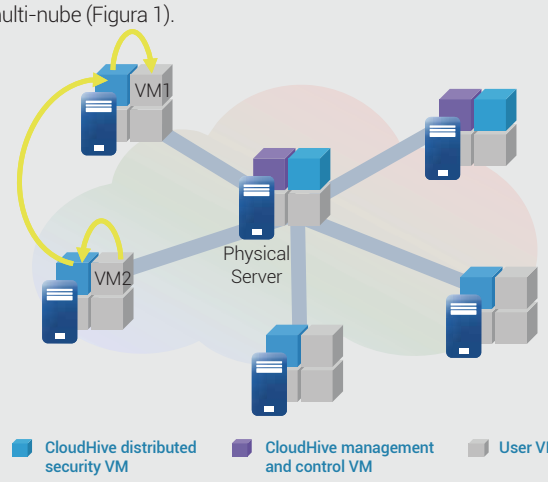


Figure 1: Hillstone CloudHive Distributed Components

El descubrimiento de activos de CloudHive crea un mapa visual de todos los recursos del centro de datos y multi-nube automáticamente, incluyendo las redes virtuales, las máquinas virtuales (VM), y todas las conexiones entre ellas. Su capacidad de mapeo le presenta a Informática vistas completas de todos los flujos de tráfico de las aplicaciones, los tipos de tráfico y las amenazas potenciales a todas las máquinas virtuales. La estrecha integración con las plataformas de orquestación en la nube existentes, tales como VMware vCenter y OpenStack asegura rica visibilidad, en tiempo real y contextual en la multi-nube y permite que los recursos de seguridad que crecen y decrecen al lado de los recursos virtuales se puedan asegurar.

Los componentes de CloudHive son todos basados en software y en las VM. Para distribuir y escalar el servicio de seguridad de una manera flexible con un impacto mínimo en el rendimiento, la arquitectura CloudHive, que se muestra en la Figura 2, separa la funcionalidad de seguridad en tres planos diferentes.

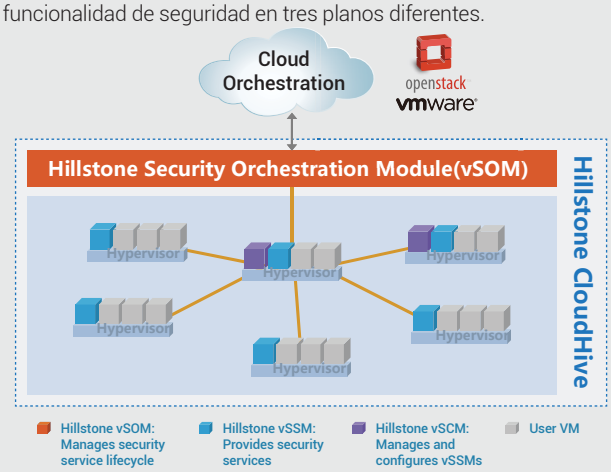


Figure 2: Hillstone CloudHive Architecture

El plano de servicio de seguridad está representado por los Módulos de Servicio de Seguridad virtual de CloudHive (vSSM). CloudHive despliega de vSSM en cada servidor físico para hacer cumplir la política de seguridad avanzada de L2-7, administrar sesiones y escalar elásticamente a través de todos los servidores de las VM.

El plano de control, representado por los Módulos de Control de Seguridad virtual de CloudHive (vSCM), actúa como el administrador de configuración de seguridad central, proporcionando interfaces de gestión (interfaz de usuario, la CLI o RestAPI) para configurar y supervisar el servicio de seguridad virtual y gestionar la configuración de la política de seguridad y el ciclo de vida de todos los vSSM. El plano de control también recopila y registra todos los datos de seguridad y de tráfico.

El plano de gestión, representado por los Módulos de Orquestación de Seguridad virtual de CloudHive (vSOM), integra e interactúa con la nube de orquestación y administración de herramientas de terceros para gestionar el ciclo de vida útil de todo el sistema CloudHive, incluyendo la instalación del sistema y cómo iniciar, detener y eliminar todos los componentes.

Beneficios CloudHive

Esta arquitectura de tres niveles tiene varios beneficios:

Escalabilidad y Movilidad Al separar la gestión, el control y el despliegue de seguridad, cada función puede escalar independientemente de las demás, aplicando el nivel preciso a cada recurso, exactamente donde se necesita. Dado que todos los servicios son elásticos y distribuidos en todo el entorno virtual, siempre estarán cerca de los recursos virtuales que protegen. Esto les permite aplicar el cumplimiento de políticas, sin los cuellos de botella que entorpesen el rendimiento con latencia e impactando el desempeño. CloudHive puede solicitar los servicios de seguridad en demanda a cualquiera y todas las nuevas cargas de trabajo y a las máquinas virtuales. La implementación de vSCM unifica la configuración de la política de seguridad a través de la multi-nube.

El plano de control CloudHive aprovecha la arquitectura distribuida de Hillstone, la sensibilización vMotion y una tecnología patentada de distribución de sesión de flujo para mantener el estado las máquinas virtuales a medida que crecen, se disminuyen y se mueven por la multi-nube sin ningún tipo de interrupción o retraso al servicio de seguridad.

La función de visibilidad integral de CloudHive con descubrimiento activo construye una presentación global de las redes de máquinas virtuales en la nube y del tráfico de red virtual de forma automática, mostrando todo el tráfico entrante y saliente y resaltando las rutas de comunicación, los tipos de tráfico y las tendencias en cada ruta. CloudHive también ofrece visibilidad y control en vivo de la topología de las VM, de este a oeste y del tráfico de norte a sur, las aplicaciones y los ataques inter-VM. La visualización integral y la función de registro de CloudHive permiten a las empresas y proveedores de servicios cloud (CSP) satisfacer todos los requerimientos de cumplimiento, auditoría de seguridad, revisión de políticas y análisis de vulnerabilidad por amenaza y su remediación.

La seguridad multifunción L2-7 de CloudHive protege a todo el tráfico hacia las VM y el tráfico inter-VM con servicios de seguridad L2-L7, incluidas las funciones de firewall tales como los límites normativos y de control de sesión, la prevención de intrusiones, la Defensa contra Ataques y los Anti-Virus, y el control de grano fino para aplicaciones. Los bloques de mitigación en tiempo real, impiden o pone en cuarentena los ataques activos. Las vSSM aseguran todo el tráfico dirigido a las VM, tanto norte-sur como este-oeste, lo que permite el 100% de cobertura para seguridad del tráfico y cero superficie de ataque.

El bajo costo total de comprar los servicios de seguridad de CloudHive no requieren una actualización de NSX de VMware y no tienen ningún impacto en la topología de red existente. Su facilidad de gestión exige pocos recursos de informática, reduce los errores de manejo y mejora la eficiencia global.

CloudHive instala los componentes de una manera no disruptiva, lo que permite agregar o quitar los servicios de seguridad simplemente añadiendo y eliminando del servicio a las máquinas virtuales (vSSMs) distribuidas por los servidores físicos.

Informática se puede beneficiar de cualquiera de los dos modos de implementación de CloudHive para asegurar un despliegue transparente. El modo TAP, que supervisa el tráfico a través de la creación de espejos, es completamente no-intrusivo pero no ofrece ninguna aplicación de políticas. Puede servir como un primer paso viable para dotar a informática de visibilidad profunda de los recursos de la red y los flujos de tráfico a través del descubrimiento de activos, el monitoreo de tráfico VM, y los registros. El modo transparente (o modo en línea) puede luego utilizarse como una etapa posterior después de inspeccionar el tráfico y hacer cumplir las políticas de seguridad.

La nube virtual proporciona una serie de nuevos desafíos de seguridad que no existen en el entorno legado de centro de datos físicos. La solución virtual de seguridad distribuida de Hillstone CloudHive proporciona activos en la nube sin precedentes y visibilidad del tráfico, reduciendo a casi cero la superficie de amenaza a centro de datos, y ofrece la flexibilidad de despliegue dinámico, elasticidad, integración de orquestación, eficiencia empresarial y la rentabilidad que requieren los entornos de nube virtual de hoy.

Mediante la inserción e integración profunda y sin problemas de componentes en el entorno virtual, Hillstone CloudHive permite seguridad en la nube que sea robusta, dinámica, eficaz y escalable y no-intrusa.

Cómo contactar a Hillstone Networks

America: +1-408-508-6750 | SEA: +65-6678-7660

Europa: +420-721-125-070 | MEA: +971-4557-1493

Email: inquiry@Hillstonenet.com