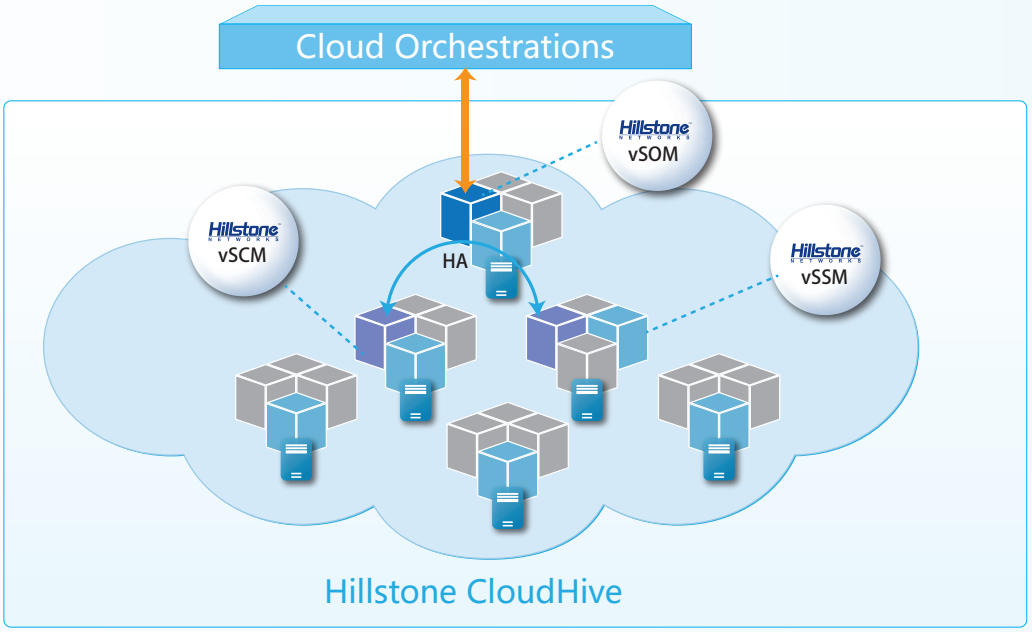
Hillstone CloudHive: Solución de Micro-segmentación para la Nube

Hillstone CloudHive ofrece tecnología de micro-segmentación para asegurar cada máquina virtual (VM) a implementar en la nube. Proporciona una visibilidad completa del tráfico Este-Oeste y ofrece protección completa para detener los ataques laterales entre máquinas virtuales. Además, el servicio de seguridad CloudHive se puede escalar fácilmente para satisfacer la demanda sin interrupción del negocio.

Hillstone CloudHive está compuesta de tres tipos de módulos virtuales que funcionan juntos como un único dispositivo para proporcionar completa seguridad para cada máquina virtual.

- El Módulo con Orquestación para la Seguridad Virtual (vSOM), integra y conecta las Plataformas de Administración desde la Nube (CMP), gestiona el ciclo de vida del servicio CloudHive.
- El Módulo de Servicios Virtuales de Seguridad (VSSM) se implementa en cada servidor físico para implementar su micro-segmentación y proporcionar servicios de seguridad L2-L7.
- El Módulo de Control Virtual de Seguridad (vSCM) es el panel de control, que permite la configuración y distribución de políticas, así como la gestión del ciclo de vida del vSSM.



www.hillstonenet.com
Phone: 1-800-889-9860

Detalles del Producto

- **Logra Visibilidad Incomparable del Tráfico en Vivo:**
  Todos los puntos de acceso para las máquinas virtuales pueden ser monitoreados para proporcionar visibilidad del tráfico, las aplicaciones y las amenazas relacionadas con cada máquina virtual, lo cual es la piedra angular para activar el control del tráfico Este-Oeste y su protección. La topología VM, la penetración del tráfico, la identificación de aplicaciones, así como las características de registros globales permiten a los proveedores de servicios en la nube (CSP) cumplir con los requisitos de auditoría y seguridad.
- **Reducen la Superficie de Ataque a Casi Cero**
  Cada Módulo de Servicios Virtuales de Seguridad CloudHive (vSSM) se implementa en un servidor físico, permitiendo micro-segmentación para la comunicación inter-VM. El tráfico Este-Oeste se asegura con los servicios de seguridad L2-L7, incluidas las funciones de firewall como límites normativos y de control de sesión, funciones de seguridad avanzadas como sistema de prevención de intrusiones (IPS) y Defensa contra Ataques (AD), así como el control de aplicaciones de granular. La mitigación en tiempo real también bloquea, impide o pone en cuarentena los ataques activos.
- **Se Escalona la Seguridad sin Esfuerzo por Medio de Orquestación Activa.**
  On-demand security services can be applied to any and all new workloads and VMs through the scalability of vSSM. The deployment of vSCM enables unified security policy configuration for each VM. CloudHive supports vMotion to ensure security services persist in the event the VM moves. Existing VM flows will not be interrupted by vMotion.
- **Mejora la Eficiencia Mientras Reduce los costos:**
  La implementación de CloudHive Capa 2 no tiene impacto en la topología de red existente. Reduce al mínimo el despliegue y la configuración de arriba, sin impactar al negocio y sin interrupción en la red. Además, facilita la ventaja de administrar un único dispositivo reduciendo los errores de funcionamiento y mejorando la eficiencia general. El coste total de propiedad también se reduce puesto que los servicios de seguridad CloudHive no necesitan ninguna actualización o ampliación de las actuales plataformas en la nube.

Características del Producto

Control de Aplicaciones

- Más de 3.000 aplicaciones que se pueden filtrar por nombre, categoría, subcategoría, tecnología y por riesgo
- Cada aplicación contiene una descripción, sus factores de riesgo, dependencias, puertos típicos utilizados, y las URL de referencia adicionales
- Acciones: bloqueo, reinicio de la sesión, monitoreo, modulación del tráfico
- Actualización en tiempo real de la base de datos de aplicaciones

Visibilidad

- Descubrimiento automático de activos en a nube: redes y máquinas virtuales
- Visualización de la topología de red virtual, máquinas virtuales y tráfico
- Profunda comprensión y seguimiento a todo el tráfico entre máquinas virtuales
- Opciones de visualización personalizadas: Ordenar, filtrar por consulta, ampliar / reducir.
- Soporte a Registros: registros de sesión, registros de amenazas y del sistema

Firewall

- Control de acceso de Capa 2 y Capa 7
- VM y control de acceso basado en la red
- Tabla de secuencias basada en control de acceso
- Gateway por Capa de Aplicación (ALG por su sigla en inglés)
- Límite de la sesión: Nueva sesión / Sesión simultánea

IPS

- Más de 8.000 firmas, incluyendo firmas personalizadas
- Configuraciones de Prevención predefinidas
- Detección de anomalías de protocolo: HTTP, IMAP, POP, VoIP,NETBIOS etc. Especificaciones
- Actualización automática y manual de firmas
- Enciclopedia de amenazas integrada
- Acciones IPS: por defecto, monitoreo, bloqueo, reinicio con tiempo de caducidad
- Opción de registro de paquetes
- Selección basada en filtros: gravedad, destino, sistema operativo, aplicación oprotocolo
- Exención de IP de firmas IPS específicas
- Modo de detección IDS

Defensa contra Ataques

- Defensa contra ataques de paquetes malformados
- Defensa contra DoS/DDoS: Consulta de inundación DNS, SYNflood, etc.
- Defensa contra los ataques ARP

Anti-Virus

- 4 millones de firmas de virus, manual, actualización automática de firmas push o pull
- Antivirus basado en flujos: protocolos que incluyen HTTP, SMTP, POP3, IMAP, FTP/SFTP
- Escaneo de virus en archivos compreso

Alta Disponibilidad

- Separación de la administración, control y plano de servicios asegura la estabilidad del servicio
- vSOM "VM inestable" no afecta al servicio CloudHive
- vSCM se despliegan en pares (activos/pasivos) para proporcionar alta disponibilidad
- Un solo VSSM "VM inestable" no afecta al sistema, el tráfico de usuarios en la VM puede pasar por alto el vSSM,
- El vSCM puede reiniciar el sistema y reiniciar el servicio de seguridad de forma automática después de una caída de una "VM". después de una "VM inestable".
- Soporte para vMotion : la política de seguridad y de flujos de sesiones se sincroniza automáticamente a través de múltiples módulos
- Apoyo para la actualización de software de servicios (ISSU)

Escalabilidad y Automatización

- La vSSM se puede ampliar sin necesidad de interrumpir el servicio de seguridad, hasta 200 módulos vSSM
- Logra la configuración políticas basadas en las VM por medio del aprendizaje automático de los activos virtuales.
- Detecta las VM y su tráfico, y actualiza el cambio de IP de la VM automáticamente

Despliegue

- Apoya tanto al modo tapping como al transparente en línea
- Despliegue de L2 sin necesidad de cambiar la configuración de red
- Facilidad de implementación sin autorización root y sin ningún efecto al plug-in, minimizado a VM y al hipervisor.
- Enable or disable security service on VM or network through one click
- Support VSS/VDS, vSAN, NSX deployment
- Support 5G high speed with one vSSM module and VMXNET3 VM network card
- Support vCenter 5.0/5.1/5.5/6.0

Management

- Interface: RESTful API, CLI, WebUI
- Centralized and unified management through a single interface

Hypervisor Compatibility

- VMWARE vSphere 5.0/5.1/5.5/6.0

Especificaciones del producto

Cada vSOM requiere un mínimo de 2 vCPU, 2 GB de memoria y 2 GB de disco duro; Cada vSCM requiere un mínimo de 2 vCPU, 6 GB de memoria y 16 GB de disco duro; Cada vSSM requiere un mínimo de 2 vCPU, 4 GB de memoria y 4 GB de disco duro.

Especificación	Sistema CloudHive
Rendimiento Firewall (Máximo)	1 Tbps
Maximum Concurrent Sessions	340 millones
Nueas sesiones (HTTP)	6 millones
Rendimiento IPS (máximo)	200 Gbps
Escalabilidad vSSM (máxima)	200

Especificación	Cada vSSM
Rendimiento Firewall	5 Gbps
Máximo número de sesiones simultáneas	1.7 millones
Nuevas Sesiones (HTTP)	30,000
Rendiemiento IPS	1 Gbps

A menos que se especifique lo contrario, todo el rendimiento, la capacidad y funcionalidad se basan en StoneOS 5.5R1. Los resultados pueden variar en función de la versión y de la implementación del StoneOS®.