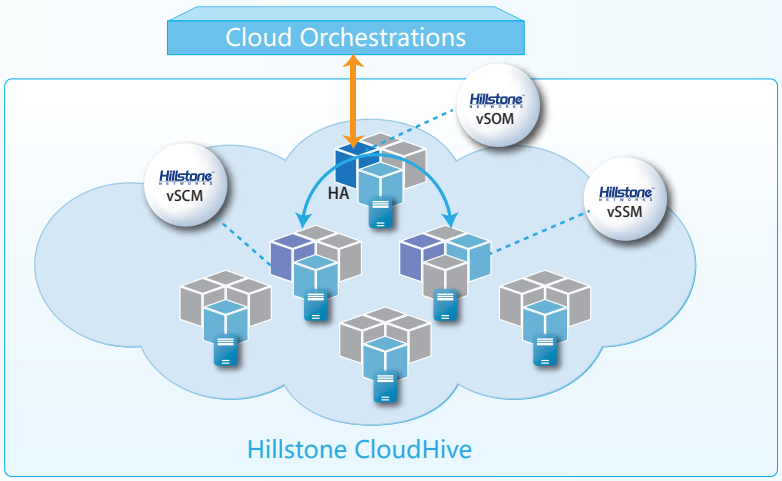
Hillstone CloudHive: Solución de Micro-segmentación para la Nube

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 las cuatro 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.
- El módulo de servicio de datos virtuales (vDSM) es un módulo de reenvío de logs opcional que reenvía los registros de CloudHive a los servidores de syslog externos. Es compatible con el reenvío masivo de registros a través de la implementación de equilibrio de carga de múltiples módulos.



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.

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

- **Se Escalona la Seguridad sin Esfuerzo por Medio de Orquestación Activa**

  CloudHive se integra perfectamente con las principales plataformas de virtualización, incluidas VMWARE y Openstack, y tiene el certificado VMWARE Ready con la integración de NSX. Los servicios de seguridad bajo demanda se pueden aplicar a todas y cada una de las nuevas cargas de trabajo y máquinas virtuales a través de la escalabilidad de vSSM. La implementación de vSCM permite la configuración unificada de la política de seguridad para cada máquina virtual. CloudHive es compatible con vMotion para garantizar que los servicios de seguridad continúen en caso de que la VM se mueva. VMotion no interrumpirá los flujos de VM existentes.

- **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 virtuales: redes y máquinas virtuales
- Monitor dinámico de activos virtuales, actualización automática/manual de la libreta de direcciones VM/IP/MAC
- Visualización de la topología de red virtual, máquinas virtuales y tráfico
- Profundo conocimiento y supervisión de todo el tráfico entre máquinas virtuales o grupos de puertos
- Clasificación del tráfico, aplicaciones y amenazas, desglosa la información relacionada.
- 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
- Control de acceso basado en cuenta AD
- 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

Prevención de Intrusiones

- Acciones de IPS: predeterminadas, monitoreo, bloqueo, reinicio (IP de los atacantes o IP de la víctima, interfaz entrante) con tiempo de caducidad
- Detección de anomalías de protocolo, detección basada en tasas, firmas personalizadas, actualizaciones de firmas automáticas manuales o automáticas, enciclopedia de amenazas integrada
- Opción de registro de paquetes
- Selección basada en filtros: severidad, destino, sistema operativo, aplicación o protocolo
- Exención de IP de firmas específicas del IPS
- Modo de husmeo IDS
- Protección DoS basada en IPv4 e IPv6 con configuración de umbral contra inundación TCP Syn, exploración de puertos TCP/UDP/SCTP, barrido ICMP, inundación de sesión TCP/UDP/SCIP/ICMP (fuente/destino)
- Bypass activo con interfaces de bypass
- Prevención de configuración predefinida

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

- Actualización de firmas automática y manual
- Antivirus basado en flujos: protocolos que incluyen HTTP, SMTP, POP3, IMAP, FTP/SFTP
- Escaneo de virus comprimidos

Alta Disponibilidad

- vSOM "Caída de máquina virtual" no afecta el servicio CloudHive
- La separación de la gestión, el control y el plano de servicio garantizan la estabilidad del servicio
- vSCM se implementan en pares (activos/pasivos) para proporcionar alta disponibilidad
- Un solo vSSM "VM caída" no afecta el sistema; el tráfico de la VM del usuario puede eludir el vSSM
- vSCM puede reiniciar el sistema y reiniciar el servicio de seguridad de forma automática después de una caída de la "VM".
- Soporte para vMotion: la política de seguridad y las sesiones de flujo se sincronizan automáticamente en múltiples módulos de servicio
- Apoyo para la actualización de software de servicios (ISSU)
- Admite control de host de administrador de redes confiable y control sobre los tiempos de intento de inicio de sesión

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

- Admite tanto el modo de tapping como el modo transparente en línea
- Implementación de L2 sin la necesidad de cambios en la configuración de la red
- Facilidad de implementación sin autorización de root y cualquier complemento, efecto minimizado para las VM e hipervisor.
- El vSSM puede escalar sin interrumpir el servicio de seguridad, hasta 200 módulos vSSM
- Logre la configuración de políticas basada en las VM a través del aprendizaje automático de activos virtuales.
- Detecta el estado de la VM (arriba o abajo) y actualiza automáticamente el cambio de IP de la VM
- Habilite o deshabilite el servicio de seguridad en la VM o grupo de puertos con un solo clic
- Soporte VMware VSS/VDS, implementación de vSAN
- Soporte de implementación Openstack OVS

Management

- Interfaz: RESTful API, CLI, WebUI
- Arquitectura distribuida, gestión centralizada y unificada a través de una única interfaz
- El reenvío de registros a servidores de syslog externos a través de vDSM, admite el reenvío de registros masivos y de alta velocidad.
- Soporte para terceros Radius/TACACS +
- Soporte de control basado en IP/Puerto/App y control basado en grupo VM/Port
- Apoya el autoaprendizaje de políticas, la convergencia de políticas, la eliminación de duplicaciones y el conteo de aciertos.
- RestAPI se asociará para un mayor desarrollo e integración de la automatización
- Monitoreo de SNMP y alarma de trampa SNMP, compatibilidad con NTP.
- Modo de administración multicapa para la separación y administración de operaciones.
- Captura y descarga de paquetes, diagnóstico de cambio de entorno para localización de fallas

Compatibilidad de virtualización

- VMWARE vSphere 5.0/5.1/5.5/6.0/6.5
- VMWARE NSX 6.2/6.3/6.4
- Plataforma VMWARE Horizon VDI
- Openstack Mitaka (Openstack + KVM + OVS)

Especificaciones del producto

Módulo	Descripción	Recurso del Sistema	Módulo #
vSOM	Módulo de Gestión de Seguridad Virtual	2*vCPU, memoria de 2GB, disco duro de 12GB	1 Estándar
vSCM	VMódulo de Control de Seguridad Virtual	2*vCPU, memoria de 6GB, disco duro de 17GB	1 Min., 2 Recomendado
vSSM	Módulo de Servicio de Seguridad Virtual	2*vCPU, memoria de 4GB, disco duro de 5GB	200 Max.
vDSM	Módulo de Gestión de Seguridad Virtual	2*vCPU, memoria de 4GB, disco duro de 5GB	Opcional, modo múltiple compatible

Especificaciones	Sistema CloudHive
Rendimiento del Firewall (máximo)	1 Tbps
Máximo número de sesiones simultáneas	340 Million
Nuevas Sesiones/S (HTTP)	6 Million
Rendimiento IPS (máximo)	200 Gbps
Rendimiento AV (máximo)	200 Gbps
Escalabilidad vSSM (máxima)	200

Especificaciones	Cada vSSM
Rendimiento del Firewall (1)	5 Gbps
Máximo número de sesiones simultáneas	1.7 Million
Nuevas Sesiones/S (HTTP)	30,000
Rendimiento de IPS (2)	1 Gbps
Rendimiento de AV (3)	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®.

NOTAS: (1) Todos los datos de rendimiento se obtuvieron en un Dell R720, VMware, entorno VDS; (2) Los datos de rendimiento IPS se obtuvieron bajo detección de tráfico HTTP bidireccional con todas las reglas IPS activadas; (3) Los datos de rendimiento de AV se obtuvieron en el tráfico HTTP con archivos adjuntos de 512 KB