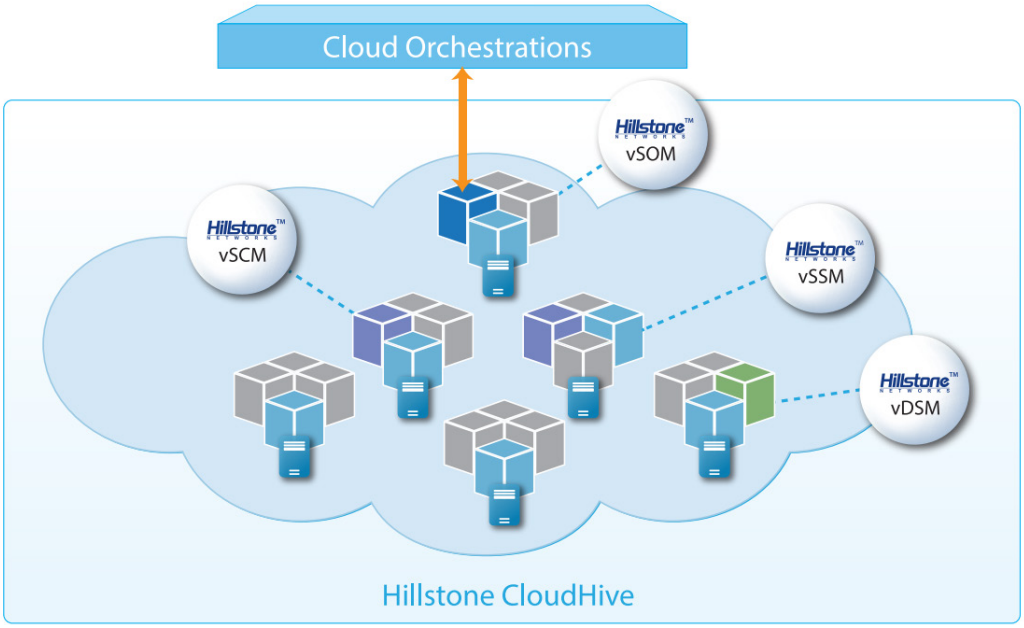
Hillstone CloudHive

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.

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. La implementación de capa 3 es compatible con VMware vSphere, que ofrece escalabilidad y flexibilidad para cumplir con diferentes requisitos de red ahora y en el futuro. 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.

Monitoreo en Tiempo Real para el Desempeño del Servicio

CloudHive se sumerge profundamente en el entorno de la nube para crear la primera línea de seguridad y defensa para máquinas virtuales , datos y aplicaciones críticos que residen en ellas. Debido a que los intercambios de información entre varios sistemas y servicios empresariales en el entorno de la nube son complejas, CloudHive proporciona una gestión del rendimiento de la red desde un punto de vista empresarial. CloudHive descubre y define automáticamente las dependencias de servicio tanto dentro como fuera del centro de datos, y establece una relación de referencia entre los servicios de una empresa determinada. Luego monitorea el retraso y la fluctuación de fase de cada servicio y la pérdida de paquetes de cada red, junto con el análisis de la utilización del CPU y memoria de la máquina virtual. Por lo tanto, CloudHive proporciona un monitoreo completo de las cadenas de servicios en términos de calidad de servicio, calidad de red y recursos informáticos, brindando una capacidad rápida de solución de problemas con análisis de datos avanzado.

Características

Control de Aplicaciones
- Más de 4,000 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
- Administración de grupos de activos virtuales, sincronización automática / información de agrupación manual de activos
- Visualización de topología de red virtual, máquinas virtuales, tráfico, plan definido por el usuario y diferentes colores para clasificaciones de nivel de amenaza
- 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

Monitoreo de Rendimiento de Servicios
- Supervisión de la calidad del rendimiento del servicio en la nube, incluida la utilización de recursos, la calidad de la red y los servicios.
- Consulta de datos con punto de monitoreo flexible e intervalo
- Topología automática de la cadena de servicios que presentan las comunicaciones internas y externas de los servicios en la nube.
- Proyección de pantalla para una visión global

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
- Control de acceso basado en nombres de dominio
- Control de acceso basado en geolocalización/IP
- Gateway por Capa de Aplicación (ALG por su sigla en inglés)
- Límite de la sesión: Nueva sesión / Sesión simultánea
- Admite detección, filtrado y alarma para archivos de protocolos HTTP, FTP, SMTP, SMB

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

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
- Admite la configuración de lista blanca

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

CloudSandbox
- Carga de archivos maliciosos en la zona de pruebas de la nube para su análisis
- Admite varios tipos de archivos, incluidos PE, APK, JAR, MS-Office, PDF, SWF, RAR, ZIP, Script
- Admite protocolos que incluyen HTTP, POP3, IMAP4, SMTP, FTP, SMB
- Proporciona un informe de análisis de comportamiento completo para archivos maliciosos
- Admite la administración de listas de confianza/amenazas

Filtrado de Contenido
- Control de acceso a la página web basado en IP, VM, atributos de grupo de servicio
- Admite más de 60 categorías, decenas de millones de firmas de URL, categorías de URL personalizables
- Actualización en tiempo real de la base de datos de firmas URL

Despliegue
- Admite tanto el modo de tapping como el modo transparente en línea
- Implementación en L2 e implementación en L3 (solo VMware vSphere)
- 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

Alta Disponibilidad
- vSOM "Caída de máquina virtual" no afecta el servicio CloudHive
- vSOM se puede implementar en pares (activo / pasivo) para proporcionar alta disponibilidad
- 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

Management
- Interfaz: RESTful API, CLI, WebUI
- Arquitectura distribuida, gestión centralizada y unificada a través de una única interfaz
- El vSOM admite la copia de seguridad periódica de la configuración global y la entrega a través de FTP/SMTP
- 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/Active Directory/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.
- Soporta el autoaprendizaje / agrupamiento / convergencia de políticas, eliminación de duplicaciones y conteo de visitas
- Compatible completamente con IPv6, admite actualización de IPv4 a IPv6
- 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
- Importar / exportar archivos de políticas y configuración

Compatibilidad de Virtualización

- VMware vSphere 5.0/5.1/5.5/6.0/6.5/7.0
- VMware NSX 6.2/6.3/6.4
- Plataforma VMware Horizon VDI
- FusionCompute 6.5.1/8.0.x/8.1.x

Especificaciones del Producto

Module	Description	System Resource	Module #
vSOM	Módulo de orquestación de seguridad virtual	2*vCPU, 6GB Memory, 60GB Hard Disk	Compatible con alta disponibilidad
vSCM	Virtual Security Control Module	2*vCPU, 8GB Memory, 17GB Hard Disk	1 Min., 2 Recommended
vSSM (Tipico)	Virtual Security Service Module 02	2*vCPU, 6GB Memory, 5GB Hard Disk	200 Max.
vSSM (Avanzado)	Virtual Security Service Module 04	4*vCPU, 10GB Memory, 5GB Hard Disk	Cuando se implementa en modo Jumbo Frame, el requisito de memoria aumentará en 2G sobre la base original.
vDSM	Módulo de servicio de datos virtuales	2*vCPU, 6GB Memory, 5GB Hard Disk	Optional, multiple mode supported

Sistema CloudHive	vSSM 02	vSSM 04
Firewall Throughput (Maximum)	1 Tbps	1 Tbps
Maximum Concurrent Sessions	340 Million	680 Million
New Sessions/s (HTTP)	6 Million	10 Million
IPS Throughput (Maximum)	300 Gbps	1 Tbps
AV Throughput (Maximum)	300 Gbps	1 Tbps
vSSM Scalability (Maximum)	200	200

vSSM individual	vSSM 02	vSSM 04
Firewall Throughput [1]	5 Gbps	5 Gbps
Firewall Throughput (NSX) [2]	16 Gbps	16 Gbps
Maximum Concurrent Sessions	1.7 Million	3.4 Million
New Sessions/s (HTTP)	30,000	50,000
IPS Throughput [3]	1.5 Gbps	5 Gbps
AV Throughput [4]	1.5 Gbps	5 Gbps

NOTAS:

(1) Todos los datos de rendimiento se obtuvieron en un Dell R720, VMware, entorno VDS;

(2) Todos los datos de rendimiento se obtuvieron en un Dell R720, VMware(6.0U2), NSX(v6.4), entorno VDS;

(3) Los datos de rendimiento IPS se obtuvieron bajo detección de tráfico HTTP bidireccional con todas las reglas IPS activadas;

(4) Los datos de rendimiento de AV se obtuvieron en el tráfico HTTP con archivos adjuntos de 512 KB

A menos que se especifique lo contrario, todo el rendimiento, la capacidad y la funcionalidad se basan en StoneOS 5.5R3. Los resultados reales pueden variar debido a las versiones del software CloudHive y al entorno de implementación.

Version: EX-08.01-CloudHive-V2.9-0922-SP-01