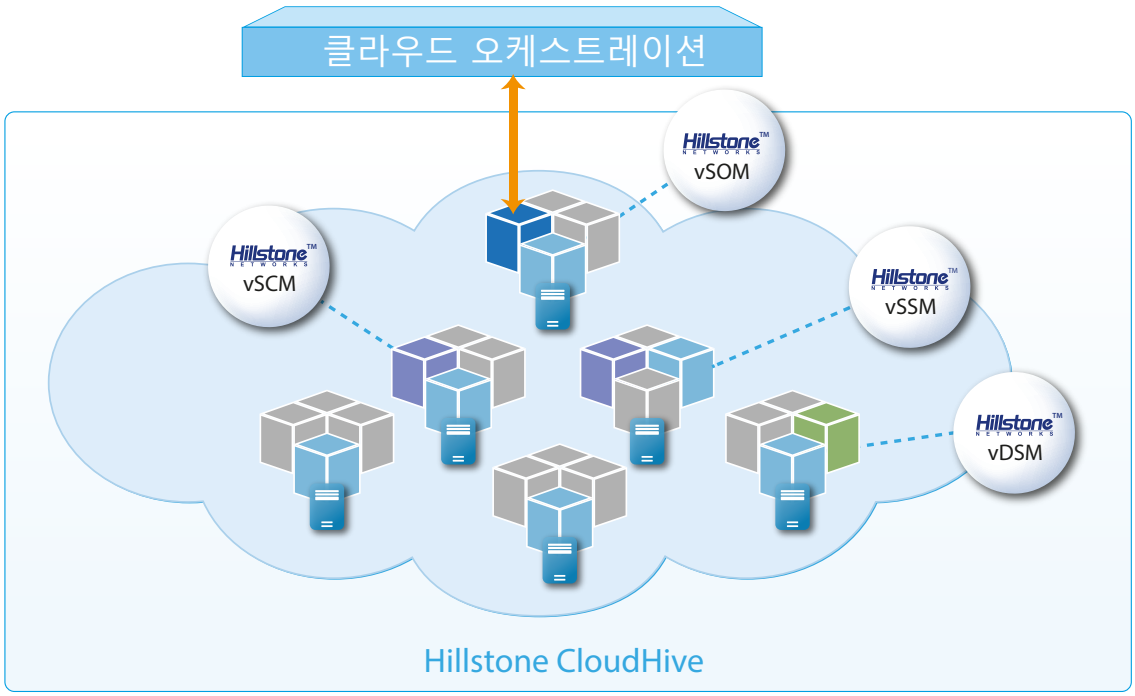
Hillstone CloudHive: 클라우드용 마이크로 세그먼테이션 솔루션

Hillstone CloudHive는 클라우드에 배포된 각각의 가상 머신을 보호하기 위해 마이크로 세그먼테이션 기술을 제공합니다. 횡방향 트래픽에 대한 포괄적인 파악 기능과 함께 가상 머신 간의 측면 공격을 막을 수 있는 완벽한 방어 기능을 제공합니다. 또한 CloudHive 보안 서비스는 중단 없이 쉽게 확장하여 비즈니스 요구사항을 충족할 수 있습니다.

Hillstone CloudHive는 하나로 함께 작동하는 4가지 유형의 가상 모듈로 구성되어 각 가상 머신에 완벽한 보안을 제공합니다.

- 클라우드 관리 플랫폼(CMP)과 통합 및 연결되는 가상 보안 오케스트레이션 모듈(vSOM)은 CloudHive 서비스의 수명 주기를 관리합니다.
- 가상 보안 제어 모듈(vSCM)은 정책의 구성과 배포를 지원하고 vSSM의 수명 주기도 관리하는 제어 패널입니다.
- 가상 보안 서비스 모듈(vSSM)은 물리적 서버에 가기 구축되어 마이크로 세그먼테이션을 구현하고 L2~L7 보안 서비스를 제공합니다.
- 가상 데이터 서비스 모듈(vDSM)은 CloudHive 로그를 외부 syslog 서버로 전달하는 모듈로, 필요할 경우에만 사용할 수 있습니다. 여러 모듈의 로드 밸런싱 구축을 통해 대량의 로그 전달을 지원합니다.



제품 주요 정보

독보적인 실시간 트래픽 파악 기능

횡방향 트래픽을 제어하고 방어하기 위해서는 가상 머신의 모든 액세스 포인트를 모니터링하여 가상 머신 또는 포트 그룹과 관련된 트래픽과 애플리케이션, 보안 위협을 완벽하게 파악하는 기능이 필요합니다. Hillstone CloudHive는 특정 기간 동안 새로운 트래픽과 애플리케이션을 모니터링하고 시각화하여 가상 네트워크의 미세한 변화를 표시할 수 있습니다. 가상 머신 토폴로지, 트래픽 통찰력, 애플리케이션 식별은 물론, 포괄적인 로그 기능까지 제공하여 클라우드 서비스 공급업체(CSP)가 규정 준수 및 보안 감사 요구사항을 충족할 수 있습니다.

공격 대상이 거의 0으로 감소

각 CloudHive Virtual Security Service Module(vSSM)은 물리적 서버에 구축되므로 가상 머신 간 또는 네트워크 간 통신의 마이크로 세그먼테이션이 가능합니다. 정책 제어, 세션 제한과 같은 방화벽 기능, 침입 방지 시스템(IPS), 안티 바이러스, 공격 방어(AD)와 같은 고급 보안 기능은 물론, 정교한 애플리케이션 제어까지 포함한 L2-L7 보안 서비스를 사용하여 횡방향 트래픽을 보호합니다. 또한 실시간 완화를 통해 진행 중인 공격을 차단, 지연 또는 격리합니다.

능동적인 오케스트레이션을 통해 간편하게 보안 확장

CloudHive는 VMware 및 Openstack과 같은 주요 가상화 플랫폼과 원활하게 통합되며, NSX 통합을 통한 VMware 지원 인증을 받았습니다. vSSM을 확장하여 필요에 따라 모든 새로운 업무를 수행하는 가상 머신에 보안 서비스를 적용할 수 있습니다. vSCM을 구축하면 각 가상 머신에 대해 통합 보안 정책을 구성할 수 있습니다. CloudHive는 가상 머신의 이동 시에도 보안 서비스를 지속적으로 적용하는 vMotion을 지원합니다. vMotion은 기존 가상 머신의 플로우에 영향을 주지 않습니다.

비용을 절감하며 효율성 향상

CloudHive의 Layer 2 기반의 구축은 기존 네트워크 토폴로지에 영향을 주지 않습니다. 고유한 구성 최적화 툴과 기능을 사용하여 구축 및 구성의 오버헤드를 최소화하고 비즈니스에 영향을 주거나 네트워크 중단이 발생하지 않습니다. 또한 단일 어플라이언스의 장점인 편리한 관리로 인해 운영 오류가 감소하고 전반적인 효율성이 향상됩니다. CloudHive 보안 서비스는 기존 클라우드 플랫폼을 업그레이드하거나 확장할 필요가 없어 총 소유비용도 감소합니다.

서비스 성능 실시간 모니터링

CloudHive는 클라우드 환경을 심층적으로 분석하여 가상 머신과 가상 머신 내부의 중요한 데이터 및 애플리케이션에 대한 첫 번째 보안 및 방어 라인을 구축합니다. 클라우드 환경에서 다양한 비즈니스 시스템과 서비스 간의 상호관계는 복잡하기 때문에 CloudHive는 비즈니스 관점에서 네트워크 성능 관리를 제공합니다. CloudHive는 데이터 센터 내부 및 외부에서 서비스 종속성을 자동으로 감지하고 정의하며 지정된 비즈니스 서비스 간의 참조 관계를 설정합니다. 그런 다음 각 서비스의 지연시간 및 지터, 각 네트워크의 패킷 손실, 가상 시스템 CPU 및 메모리의 사용률을 모니터링합니다. 따라서 CloudHive는 서비스 품질, 네트워크 품질 및 컴퓨팅 리소스 측면에서 서비스 체인을 완벽하게 모니터링하고 고급 데이터 분석을 통해 신속한 문제 해결 기능을 제공합니다.

기능

애플리케이션 제어
- 이름, 카테고리, 하위 카테고리, 기술 및 위험을 기준으로 3,000개 이상의 애플리케이션 필터링
- 각 애플리케이션 정보에는 설명, 위험 요소, 종속성, 일반적으로 사용하는 포트 및 추가 참조용 URL이 포함됨
- 동작: 차단, 세션 리셋, 모니터링, 트래픽 형상화
- 실시간 애플리케이션 데이터베이스 업그레이드

파악 기능
- 가상 자산 자동 검색: 네트워크 및 가상 머신
- 동적 가상 자산 모니터링, 가상 머신/IP/MAC 주소록 자동/수동 업데이트
- 가상 자산 그룹 관리, 자산 그룹화 정보 자동/수동 동기화
- 가상 머신 또는 포트 그룹 간의 모든 트래픽에 대한 심층적인 통찰력과 모니터링
- 트래픽, 애플리케이션 및 보안 위협의 순위 평가, 관련 세부 정보 제공
- 시각화 사용자 정의 옵션: 정렬, 조회, 필터링 확대/축소,
- 로그 지원: 세션 로그, 보안 위협 및 시스템 로그

서비스 성능 모니터
- 리소스 활용, 네트워크 품질 및 서비스를 포함한 다차원 클라우드 서비스 성능 품질 모니터링
- 유연한 모니터링 지점 및 시간 간격으로 모니터링 데이터 쿼리
- 클라우드 서비스의 내부 및 외부 통신을 나타내는 자동 서비스 체인 토폴로지
- 전체 개요를 보기 위한 스크린 캐스팅

방화벽
- Layer 2~Layer 7 액세스 제어
- 가상 머신 및 포트 그룹 기반 액세스 제어
- AD 계정 기반 액세스 제어
- 시간 테이블 기반 액세스 제어
- 애플리케이션 계층 게이트웨이(ALG)
- 세션 제한: 새 세션/동시 세션

공격 방어
- 비정상 프로토콜 공격 방어
- Anti-DoS/DDoS(SYN Flood, DNS Query Flood 방어 포함)
- ARP 공격 방어
- 포트 검사 탐지 및 방어

침입 방지
- IPS 동작: 디폴트, 모니터링, 차단, 만료 시간으로 리셋(공격자 IP 또는 피해자 IP, 수신 인터페이스)
- 프로토콜 이상 탐지, 속도 기반 탐지, 사용자 정의 시그니처, 시그니처 업데이트의 수동/자동 푸시/풀, 통합 보안 위협 백과 사전
- 패킷 로깅 옵션
- 필터링 기반 선택: 심각도, 대상, 운영 체제, 애플리케이션 또는 프로토콜
- 특정 IPS 시그니처에서 IP 제외
- IDS 스니퍼 모드
- TCP Syn flood, TCP/UDP/SCTP 포트 검사, ICMP 스위프, TCP/UDP/SCIP/ICMP session flooding (소스/목적지)에 대한 임계값 설정을 통한 IPv4 및 IPv6 속도 기반 DoS 방어
- 바이패스 인터페이스를 사용한 액티브 바이패스
- 사전 정의된 방지 구성

안티 바이러스
- 시그니처 업데이트의 수동/자동 푸시/풀
- 플로우 기반 안티 바이러스: HTTP, SMTP, POP3, IMAP, FTP/SFTP 등의 프로토콜
- 압축 파일 바이러스 검사

URL 필터링
- IP, VM, 서비스 그룹 속성을 기반으로 하는 웹 페이지 액세스 제어
- 60 개 이상의 범주, 수천만 개의 URL 시그니처, 사용자 정의 가능한 URL 카테고리 지원
- URL 시그니처 데이터베이스의 실시간 업데이트

구축
- 태핑 모드 및 트랜스패어런트 인라인 모드 모두 지원
- 네트워크 구성 변경이 필요 없는 L2 구축
- 루트 권한 및 플러그인이 필요 없는 간편한 구축으로 가상 머신과 하이퍼바이저에 미치는 영향 최소화
- vSSM은 보안 서비스 중단 없이 최대 200개의 vSSM 모듈까지 확장 가능
- 가상 자산에 대한 자동 학습을 통해 가상 머신 기반 정책 구성 가능
- 가상 머신의 상태(가동 또는 중지) 탐지 및 가상 머신 IP 변경 자동 업데이트
- 클릭 한 번으로 가상 머신 또는 포트 그룹에 보안 서비스 설정 또는 해제
- VMware VSS/VDS, vSAN 구축 지원
- Openstack OVS 구축 지원

HA
- vSOM "가상 머신 종료"가 CloudHive 서비스에 영향을 주지 않음
- 관리, 제어 및 서비스 플레인의 분리로 서비스 안정성 보장
- 고가용성을 제공하기 위해 vSCM은 이중(활성/비활성)으로 구축
- 단일 vSSM "가상 머신 중지"는 시스템에 영향을 주지 않으며 사용자 가상 머신 트래픽은 vSSM 바이패스 가능
- vSCM은 "가상 머신 중지" 후 자동으로 보안 서비스를 재부팅 및 재시작할 수 있음
- vMotion 지원: 여러 서비스 모듈 간 보안 정책 및 플로우 세션 자동 동기화
- 서비스 수행 중 소프트웨어 업그레이드(ISSU) 지원
- 신뢰할 수 있는 네트워크 관리 호스트 제어 및 로그인 시도 시간에 대한 제어 지원

관리
- 인터페이스: RESTful API, CLI, 웹 UI
- 분산 아키텍처, 단일 인터페이스를 통한 중앙 집중식 통합 관리
- vDSM을 통해 외부 syslog 서버로 로그 전달, 대량의 고속 로그 전달 지원
- 타사 Radius/TACACS+ 지원
- IP/포트/애플리케이션 기반 제어 및 가상 머신/포트 그룹 기반 제어 지원
- 정책 자가 학습, 정책 통합, 중복 제거 및 적중 횟수 파악 지원
- 정책 자체 학습/그룹화/수렴, 중복 제거 및 히트 카운트 지원
- IPv6 완벽 지원, IPv4에서 IPv6으로의 업그레이드 지원
- 파트너의 추가 자동화 개발 및 통합을 위해 RestAPI 제공
- SNMP 모니터링 및 SNMP 트랩 경보, NTP 지원
- 운영 및 관리의 분리를 위한 다중 계층 관리 모드
- 패키지 캡처 및 다운로드, 오류 발생 위치에 대한 환경 변화 진단

가상화 호환성
- VMware vSphere 5.0/5.1/5.5/6.0/6.5
- VMware NSX 6.2/6.3/6.4
- VMware Horizon VDI 플랫폼
- Openstack Mitaka(Openstack + KVM + OVS)

사양

Module	Description	System Resource	Module #
vSOM	가상 보안 오케스트레이션 모듈	2*vCPU, 2GB Memory, 12GB Hard Disk	1 Standard
vSCM	Virtual Security Control Module	2*vCPU, 6GB Memory, 17GB Hard Disk	1 Min., 2 Recommended
vSSM (표준)	Virtual Security Service Module 02	2*vCPU, 4GB Memory, 5GB Hard Disk	최대 200
vSSM (고급)	Virtual Security Service Module 04	4*vCPU, 8GB Memory, 5GB Hard Disk	점보 프레임 모드로 배포하면 메모리 요구 사항이 원래에서 2G 단위로 증가함.
vDSM	가상 데이터 서비스 모듈	2*vCPU, 4GB Memory, 5GB Hard Disk	Optional, multiple mode supported

CloudHive 시스템	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

개별 vSSM	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

참고:
(1) 모든 성능 데이터는 DellR720, VMware, VDS 환경에서 측정되었습니다.
(2) 모든 성능 데이터는 DellR720, VMware(6.0U2), NSX(v6.4), VDS 환경에서 측정되었습니다.
(3) IPS 처리량은 모든 IPS 규칙을 설정한 상태에서 양방향 HTTP 트래픽 감지를 통해 측정되었습니다.
(4) AV 처리량은 512K 첨부 파일을 포함한 HTTP 트래픽을 사용하여 측정되었습니다.
달리 명시되지 않는 한 모든 성능, 용량 및 기능은 StoneOS 5.5R3을 기반으로 합니다. 실제 결과는 CloudHive 소프트웨어 버전 및 배포 환경에 따라 다를 수 있습니다.

www.HillstoneNet.kr

버전: EX-08.01-CloudHive-V2.7.1-0520-KR-01