Hillstone CloudEdge:
차세대 가상 방화벽

Hillstone CloudEdge 차세대 가상 방화벽은 Hillstone Networks StoneOS 운영 체제에 내장되어 가상 머신으로 구축되며, 가상화 환경에서 고급 보안 서비스로 애플리케이션과 사용자를 보호합니다. 비즈니스를 완벽하게 보호하고 지속적으로 운영하기 위한 세분화된 애플리케이션 식별 및 제어, VPN, 침입 방지, 안티 바이러스, 공격 방어, 클라우드 샌드박스 등의 종합적인 보안 기능을 제공합니다. 퍼블릭/프라이빗 클라우드 고객 모두에게 가성비가 우수한 솔루션을 제공하며, 신속한 프로비저닝과 대규모 구축이 가능합니다.

주요 제품 정보

가상 환경과의 탁월한 호환성

가상 환경에서는 컴퓨팅과 스토리지, 데이터 리소스가 가상 머신에서 실행됩니다. Hillstone CloudEdge는 ESXi, KVM, Hyper-V, Xen 서버와 같은 주요 하이퍼바이저 기술을 지원하며, 가상 머신에 신속하게 구축하여 가상 네트워크 또는 가상화된 애플리케이션을 위한 고급 보안 서비스를 제공할 수 있습니다. CloudEdge는 가상 어플라이언스로 구축되어 물리적 방화벽의 한계를 극복할 수 있으며, 가상 네트워크 내 모든 트래픽을 검사하여 종방향 및 횡방향 트래픽을 보호합니다. 또한 사용자는 네트워크 토폴로지의 요구사항에 따라 유연하게 네트워크 리소스를 배포하고 관리할 수 있으므로 가상화의 이점이 극대화됩니다.

고급 보안 위협 방어 기능

CloudEdge는 Hillstone 차세대 방화벽(NGFW)과 기본적으로 동일한 기술을 사용하며 퍼블릭/프라이빗 클라우드 사용자의 네트워크 보안 요구사항을 모두 충족할 수 있습니다. Hillstone CloudEdge는 포트, 프로토콜 또는 우회 동작에 관계없이 웹 애플리케이션의 정교한 제어를 제공합니다. 애플리케이션과 사용자, 사용자 그룹에 대한 정책 기반 제어를 제공하는 동시에 고위험 애플리케이션과 연관된 잠재적인 보안 위협을 식별하여 방지합니다. 또한 여러 보안 엔진(AD, IPS, URL 필터링, 안티 바이러스, 클라우드 샌드박스 등)과 패킷 세부 정보를 공유하는 통합 보안 위협 탐지 엔진을 사용하므로 네트워크 지연 시간은 감소하는 반면 보안 효율성은 크게 향상됩니다.

주요 제품 정보 (계속되는)

클라우드 관리 플랫폼을 사용하는 가상화된 보안 관리

Hillstone CloudEdge는 클라우드 구축 환경의 독립 테넌트에 독자적인 보안 세그먼테이션과 정책 방어를 제공하며, 스냅샷 시스템에 기반한 즉각적인 복구를 구현할 수 있습니다. 가상 어플라이언스가 중단되거나 문제가 발생할 경우 저장된 구성을 가진 스냅샷을 사용하여 복구를 수행하고, 기존의 가상 머신 또는 새 가상 머신에서 새 가상 방화벽을 시작할 수 있습니다. CloudEdge 그래픽 관리 인터페이스의 쿼리 로깅 기능을 사용하여 네트워크 상태를 효과적으로 모니터링하고 추적할 수 있으며, 트래픽 및 보안 이벤트에 대한 실시간 세부 정보를 확인할 수 있는 보고서 기능도 제공합니다. 관리자는 이러한 툴이 제공하는 시각화된 정보를 통해 네트워크 작동 상태를 완벽하게 파악할 수 있으므로 운영 효율성이 향상됩니다.

구축 자동화 및 서비스 오케스트레이션

Hillstone CloudEdge는 클라우드 플랫폼의 요구사항을 충족할 수 있는 여러 통합 솔루션을 제공하며, 이미 여러 테스트 및 운영 클라우드 환경에 구축되어 다양한 산업군 및 고객의 요구사항을 지원하고 있습니다. Hillstone CloudEdge의 구축 자동화 및 라이센스 관리 기능을 사용하면 클라우드 관리자의 개입 없이 클라우드 사용자가 비즈니스 요구사항에 따라 직접 서비스를 수행하고 관리할 수 있습니다. 오케스트레이션 기능은 각 CloudEdge의 자동 구축 및 구성을 보장하고, 라이센스 관리 기능은 CloudEdge가 자동으로 작동 모드를 시작하도록 보장합니다. Hillstone CloudEdge REST API는 시스템 구성, 보안 정책 구성, 인터페이스 및 네트워크 구성을 지원하여 주요 클라우드 관리 플랫폼과 통합할 수 있습니다.

기능

네트워크 서비스
- 동적 라우팅(OSPF, BGP, RIPv2)
- 정적 및 정책 라우팅
- 애플리케이션별 라우팅 제어
- DHCP, NTP, DNS 서버 및 DNS 프록시 내장
- 탭 모드 - SPAN 포트 연결
- 인터페이스 모드: 스니퍼, 포트 통합, 루프백, VLANS (802.1Q 및 트렁킹)
- L2/L3 스위칭 및 라우팅
- 버추얼 와이어(Layer 1) 트랜트패어런트 인라인 구성

방화벽
- 작동 모드: NAT/라우팅, 트랜스패어런트(브릿지) 및 혼합 모드
- 정책 개체: 사전 정의, 사용자 정의 및 개체 그룹화
- 애플리케이션, 역할 및 지리적 위치 기반 보안 정책
- 애플리케이션 레벨 게이트웨이 및 세션 지원: MSRCP, PPTP, RAS, RSH, SIP, FTP, TFTP, HTTP, dcerpc, dns-tcp, dns-udp, H.245 0, H.245 1, H.323
- NAT 및 ALG 지원: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT, STUN
- NAT 구성: 정책별 및 중앙 NAT 테이블
- VoIP: SIP/H.323/SCCP NAT 통과, RTP 핀홀
- 글로벌 정책 관리 보기
- 보안 정책 중복 검사, 정책 그룹, 정책 구성 롤백
- 간편한 정책 배포를 위한 정책 도움이
- 정책 분석 및 유효하지 않은 정책 정리
- 포괄적인 DNS 정책
- 스케줄: 1회성 및 반복

침입 방지
- 프로토콜 비정상 탐지. 속도 기반 탐지, 사용자 정의 시그니처, 시그니처 업데이트의 수동/자동 푸시/풀, 통합 보안 위협 백과 사전
- IPS 동작: 디폴트, 모니터링, 차단, 만료 시간으로 리셋 (공격자 IP 또는 피해자 IP, 수신 인터페이스)
- 패킷 로깅 옵션
- 필터 기반 선택: 심각도, 대상, OS, 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

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

URL 필터링
- 플로우 기반 웹 필터링 검사
- URL, 웹 컨텐츠 및 MIME 헤더 기반 수동 정의 웹 필터링
- 클라우드 기반 실시간 분류 데이터베이스를 사용한 동적 웹 필터링: 64개 카테고리(그 중 8개는 보안 관련)로 분류된 1억, 4천만 개 이상의 URL
- 추가 웹 필터링 기능:
  - Java Applet, ActiveX 또는 쿠키 필터링
  - HTTP Post 차단
  - 로그 검색 키워드
  - 개인정보 보호를 위해 특정 카테고리의 암호화된 연결에 대한 검사 제외
- 웹 필터링 프로파일 재정의: 관리자가 사용자/그룹/IP에 임시로 서로 다른 프로파일을 지정 가능
- 웹 필터 로컬 카테고리 및 카테고리 등급 재정의

클라우드 샌드박스
- 분석을 위해 클라우드 샌드박스에 악성 파일 업로드
- 지원 프로토콜: HTTP/HTTPS, POP3, IMAP, SMTP, FTP 등
- 지원 파일 형식: PE, ZIP, RAR, Office, PDF, APK, JAR, SWF 등
- 파일 전송 방향 및 파일 크기 제어
- 악성 파일에 대한 완벽한 행위 분석 보고서 제공
- 글로벌 보안 위협 인텔리전스 공유, 실시간 보안 위협 차단
- 파일 업로드 없이 동작하는 탐지 전용 모드 지원

봇넷 C&C 방지
- C&C 연결 모니터링을 통한 인트라넷 봇넷 호스트 발견 및 봇넷과 랜섬웨어 등의 추가 지능형 보안 위협 차단
- 봇넷 서버 주소 정기 업데이트
- C&C IP 및 도메인 방지
- TCP, HTTP 및 DNS 트래픽 탐지 지원
- IP 및 도메인 화이트리스트

IP 평판
- 봇넷 호스트, 스패머, 토르 노드, 손상된 호스트 및 무차별 대입 공격 등 위험한 IP의 트래픽 식별 및 필터링
- 다양한 유형의 위험한 IP 트래픽에 대한 로깅, 패

기능 (계속되는)

킷 버리기 또는 차단
- 정기 IP 평판 시그니처 데이터베이스 업그레이드

엔드포인트 식별
- 엔드포인트 IP, 엔드포인트 수, 온라인 시간, 오프라인 시간 및 온라인 지속기간 식별 지원
- Windows, iOS, 안드로이드를 포함한 10개의 운영체제 지원
- IP, 엔드포인트 수, 제어 정책 및 상태 등을 기반으로 한 쿼리 지원
- Layer 3 전반에 걸쳐 액세스된 엔드포인트 수 식별 및 오버런 IP의 간섭, 로깅 지원
- 사용자 정의 간섭 동작 후 페이지 리디렉션
- 오버런 IP에 대한 차단 동작 지원

데이터 보안
- 파일 유형 기반 파일 전송 제어
- 파일 프로토콜 식별(HTTP, FTP, SMTP 및 POP3 포함)
- 100개 이상의 파일 유형에 대한 파일 서명 및 접미사 식별
- HTTP-GET, HTTP-POST, FTP 및 SMTP 프로토콜에 대한 컨텐츠 필터링
- IM 식별 및 네트워크 행위 감사

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, 추가 참조용 URL이 포함됨
- 동작: 차단, 세션 재설정, 모니터링, 트래픽 형상화
- 클라우드의 애플리케이션 식별 및 제어
- 위험 카테고리 및 특성을 포함하여 클라우드에서 실행되는 애플리케이션에 대한 다차원 모니터링 및 통계 제공

QoS
- IP/사용자 기준 최대/보장 대역폭 터널
- 보호 도메인, 인터페이스, 주소, 사용자/사용자 그룹, 서버/서버 그룹, 애플리케이션/애플리케이션 그룹, TOS, VLAN 기준 터널 할당
- 시간 또는 우선 순위별 대역폭 할당 또는 동일한 대역폭 공유
- 서비스 유형(TOS) 및 DiffServ 지원
- 우선 순위별 잔여 대역폭 할당
- IP당 최대 동시 연결 수
- URL 카테고리 기반 대역폭 할당
- 사용자 또는 IP 액세스 지연을 통한 대역폭 제한
- 자동 만료 정리 및 사용자 사용 트래픽에 대한 수동 정리

서버 로드 밸런싱
- 가중 해시, 가중 최소 연결 및 가중 라운드 로빈
- 세션 방어, 세션 지속 및 세션 상태 모니터링
- 서버 상태 검사, 세션 모니터링 및 세션 방어

링크 로드밸런싱
- 양방향 링크 로드 밸런싱
- 아웃바운드 링크 로드 밸런싱: 정책 기반 라우팅, ECMP 및 가중, 내장 ISP 라우팅, 동적 감지 포함
- 인바운드 링크 로드 밸런싱: SmartDNS 및 동적 감지 지원
- 대역폭, 지연 시간, 지터, 연결성, 애플리케이션 등에 기반한 자동 링크 스위칭
- ARP, PING 및 DNS를 사용한 링크 상태 검사

VPN
- IPSec VPN:
  - IPSEC 1단계 모드: 어그레시브 모드와 메인 ID 방어 모드
  - 피어 허용 옵션: 모든 ID, 특정 ID, 다이얼업 사용자 그룹의 ID
  - IKEv1 및 IKEv2 지원(RFC 4306)
  - 인증 방법: 인증서 및 사전 공유 키
  - IKE 모드 구성 지원(서버 또는 클라이언트)
  - IPSEC를 통한 DHCP
  - 구성 가능한 IKE 암호화 키 만료일, NAT 트래버설 활성화 유지 빈도
  - 1단계/2단계 제안 암호 알고리즘: DES, 3DES, AES128, AES192, AES256
  - 1단계/2단계 제안 인증 알고리즘: MD5, SHA1, SHA256, SHA384, SHA512
  - 1단계/2단계 Diffie-Hellman 지원: 1,2,5
  - 서버 모드로와 다이얼업 사용자를 위한 XAuth,
  - 동작 중지 피어 감지
  - 리플레이 감지
  - 2단계 SA를 위한 자동키 keep-alive 유지
- IPSEC VPN 영역 지원: 사용자 그룹과 연관된 다중 사용자 지정 SSL VPN 로그인 허용(URL 경로, 디자인)
- IPSEC VPN 구성 옵션: 경로 기반 또는 정책 기반
- IPSEC VPN 구축 모드: 게이트웨이 간, 풀 메시, 부챗살, 이중 터널, 트랜스패어런트 모드에서 VPN 종료
- 동일한 사용자 이름을 사용한 동시 로그인을 방지하는 1회 로그인
- SSL 포털 동시 사용자 제한
- 클라이언트 데이터를 암호화하여 애플리케이션 서버로 전송하는 SSL VPN 포트 포워딩 모듈
- iOS, Android 및 Windows XP/Vista(64비트 Windows OS 포함) 용 클라이언트 지원
- SSL 터널 연결에 앞서 호스트 무결성 확인 및 OS 검사 수행
- 포털별 MAC 호스트 확인
- SSL VPN 세션을 종료하기 전 캐시 지우기 옵션
- L2TP 클라이언트 및 서버 모드, IPSEC를 통한 L2TP, IPSEC를 통한 GRE
- IPSEC 및 SSL VPN 연결 보기 및 관리
- PnPVPN

HA
- 이중 하트비트 인터페이스
- Active/Passive
- 독립 실행형 세션 동기화
- HA 예약 관리 인터페이스
- 페일오버:
  - 포트, 로컬 및 원격 링크 모니터링
  - 상태 인식 페일오버
  - 1초 미만의 페일오버
  - 장애 통지
- 구축 옵션:
  - 링크 애그리게이션 HA
  - 풀 메시 HA
  - 지리적으로 분산된 HA

트윈 모드 HA
- 여러 장치 간의 고 가용성 모드
- 다중 HA 배포 모드
- 여러 장치 간의 구성 및 세션 동기화

SSL 복호화
- SSL 암호화 트래픽 애플리케이션 식별
- SSL 암호화 트래픽 IPS 활성화 지원
- SSL 암호화 트래픽 안티 바이러스 활성화 지원
- SSL 암호화 트래픽 URL 필터링 지원
- SSL 암호화 트래픽 화이트리스트
- SSL 프록시 오프로드 모드

사용자 및 장치 식별
- 로컬 사용자 데이터베이스
- 원격 사용자 인증: TACACS+, LDAP, Radius, Active Directory
- 싱글사인온: Windows AD
- 이중 인증: 타사 제품 지원, 물리적 및 SMS를 통한 통합 토큰 서버
- 사용자 및 장치 기반 정책
- AD 및 LDAP 기반 사용자 그룹 동기화
- 802.1X, SSO 프록시 지원
- WebAuth 페이지 사용자 정의
- 인터페이스 기반 인증
- 에이전트 없는 ADSSO(AD 폴링)
- SSO 모니터링 기반 인증 동기화 사용
- MAC 기반 사용자 인증 지원

관리
- 관리 액세스: HTTP/HTTPS, SSH, telnet, 콘솔
- 중앙 집중식 관리: Hillstone Security Manager(HSM), 웹 서비스 API
- 시스템 통합: SNMP, syslog, 제휴 파트너쉽
- 빠른 구축: USB 자동 설치, 로컬 및 원격 스크립트 실행
- 동적 실시간 대시보드 상태 및 상세 모니터링 위젯
- 언어 지원: 영어

로그 & 보고서
- 로그 위치: 로컬 메모리 및 스토리지(해당될 경우), 다중 syslog 서버 및 다중 Hillstone Security Audit(HSA) 플랫폼
- HSA로의 지정 스케줄 배치 로그 업로드를 통한 암호화된 로깅 및 로그 무결성 지원

기능 (계속되는)

- TCP 옵션(RFC 3195)을 사용한 안정적인 로깅
- 상세 트래픽 로그: 전달, 위반 세션, 로컬 트래픽, 유효하지 않은 패킷, URL 등
- 종합적인 이벤트 로그: 시스템 및 관리 작업 감사, 라우팅 및 네트워킹, VPN, 사용자 인증, WiFi 관련 이벤트
- IP 및 서비스 포트 이름 확장 옵션
- 간단 트래픽 로그 형식 옵션
- 3가지 사전 정의 보고서 형식: 보안, 플로우 및 네트워크 보고서
- 사용자 정의 보고 기능
- 이메일 및 FTP를 통한 PDF 형식 보고서 전송

통계와 모니터링

- 애플리케이션, URL, 보안 위협 이벤트 통계 및 모니터링
- 실시간 트래픽 통계 및 분석
- 동시 세션, CPU, 메모리 및 온도 등의 시스템 정보
- iQOS 트래픽 통계 및 모니터링, 링크 상태 모니터링
- Netflow(v9.0)를 통한 트래픽 정보 수집 및 전달 지원

라이센스 관리

- 자동 라이센스 활성화/비활성화
- 인터넷 액세스가 제공되는 퍼블릭 클라우드 또는 프라이빗 클라우드 사용자
- 장치를 사용한 라이센스 이동

CloudView

- 클라우드 기반 보안 모니터링
- 웹 또는 모바일 애플리케이션을 사용한 연중무휴 24시간 액세스
- 장치 상태, 트래픽 및 보안 위협 모니터링
- 클라우드 기반 로그 보존 및 보고서

REST API

- 로그인, 장치 모니터링
- 주소 테이블, 서비스 테이블, 애플리케이션 테이블
- 애플리케이션 정책, AV 정책, IPS 정책, DNAT/SNAT, 보안 정책
- 구성: 인터페이스 구성, 라우팅 구성, 영역 구성

가상화

- 하이퍼바이저: KVM, VMware ESXi, Xen, AMI (AWS), Hyper-V
- 퍼블릭 클라우드: AWS, Azure, AliCloud 등
- 클라우드 관리 플랫폼: Openstack Liberty 이상, VMware vCenter 5.5 이상 등
- Array AVX 시리즈 Network Functions Platform

사양

	VM01	VM02	VM04
Core (Min)	2	2	2
Memory (Min)	2G	4G	8G
Storage (Min)	4 Gbps	4 Gbps	4 Gbps
Network Interfaces	10	10	10
Firewall Throughput (vNIC/SR-IOV)	2 Gbps / 10 Gbps	4 Gbps / 20 Gbps	8 Gbps / 30 Gbps
IPS Throughput (vNIC/SR-IOV)	1 Gbps / 3 Gbps	2 Gbps / 5 Gbps	4 Gbps / 7 Gbps
AV Throughput (vNIC/SR-IOV)	800 Mbps / 1 Gbps	1.6 Gbps / 2 Gbps	3.2 Gbps / 4 Gbps
IPsec VPN Throughput (vNIC/SR-IOV)	200 Mbps / 400 Mbps	400 Mbps / 800 Mbps	800 Mbps / 2 Gbps
New Sessions / Second(vNIC/SR-IOV)	20,000 / 30,000	40,000 / 50,000	80,000 / 100,000
Maximum Concurrent Sessions	100,000	500,000	5 Million
IPSec VPN Tunnels (Max.)	100	500	10,000
SSL VPN Users (Max.)	100	500	2,000

참고:
상기 기재된 성능은 Del R720 서버(Intel(R) Xeon(R) CPU E5-2609 v2 @ 2.50GHz, 64GB 메모리, 2x 10 GE 인터페이스)와 StoneOS 5.5R5를 사용하여 측정되었습니다. 실제 성능은 StoneOS 버전, 네트워크 및 시스템 구성에 따라 달라질 수 있습니다.
달리 명시되지 않는 한 모든 성능, 용량 및 기능 데이터는 StoneOS5.5R6 기준입니다. 결과는 StoneOS® 버전 및 구축 환경에 따라 달라질 수 있습니다.

버전: EX-08.01-CloudEdge-5.5R7-0619-KR-01