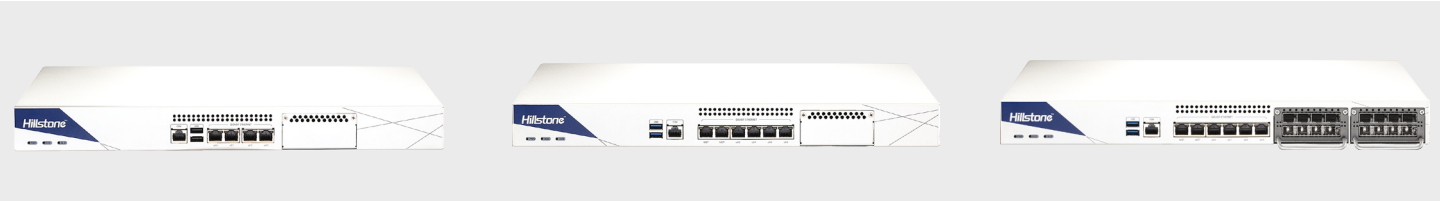
Hillstone S 시리즈 네트워크 침입 방지 시스템(NIPS)



보안 위협이 갈수록 공격적으로 진화함에 따라 여러 가지 네트워크 방어 기술이 빠르게 부상하고 있습니다. 이러한 다양한 기술 중에서 플랫폼이나 폼 팩터에 관계없이 가장 광범위하게 구축되는 솔루션 중 하나가 침입 방지 시스템(IPS)입니다.
Hillstone 네트워크 기반 IPS(NIPS) 어플라이언스는 인라인으로 작동하여 유선 속도로 심층 패킷 검사를 수행하고 모든 네트워크 트래픽의 검사 결과를 집계합니다. 또한 프로토콜 이상 분석, 시그니처 분석을 포함한 여러 방법론에 따라 보안 위협을 차단하기 위한 규칙을 적용합니다. Hillstone NIPS는 경계 솔루션으로 감지되지 않는 트래픽을 검사하기 위해 네트워크 내에 구축할 수 있으며, 시스템 운영에 영향을 미치지 않는 우수한 성능, 동급 최고의 방어 기능과 광범위하고 유연한 구축 시나리오를 제공하여 네트워크 보안 시스템의 필수 요소로 자리잡고 있습니다.

제품 주요 정보

성능 저하 없이 탁월한 보안 위협 방지 제공

Hillstone NIPS 플랫폼은 업계를 선도하는 기술 파트너와의 제휴를 통해 동급 최고의 시그니처를 갖춘 종합적인 고성능 검사 엔진을 탑재하고 있습니다. 따라서 낮은 총 소유비용(TCO)으로 최고 수준의 보안 위협 탐지율을 제공합니다. Hillstone IPS 엔진은 정적 취약점은 99.6%, 라이브 취약점은 98.325% 차단합니다(NSS Labs 보고서 자료).
Hillstone NIPS 플랫폼은 높은 처리량과 낮은 지연 시간, 최고의 가용성을 제공하여 네트워크 성능 저하 없이 효율적으로 보안 작업을 수행합니다. NIPS는 프로토콜 분석, 보안 위협 평판 기능과 함께 ARP 공격, Dos/DDoS 공격, 비정상 프로토콜, 악성 URL, 악성 코드, 웹 공격 등 Layer 2 ~ Layer 7의 보안 위협을 방어하는 여러 가지 기능을 결합하여 제공합니다.

특정 사용자 대상의 세분화된 보고 기능

Hillstone NIPS는 프로토콜, 애플리케이션, 사용자 및 컨텐츠를 바탕으로 포괄적으로 파악할 수 있는 기능을 제공합니다. 수백 개의 모바일 및 클라우드 애플리케이션을 비롯하여 3,000개 이상의 애플리케이션을 식별할 수 있습니다.
여러 소스에서 식별된 컨텍스트 정보를 하나로 취합하여 상황에 적합한 차단 결정을 내릴 수 있습니다.

강력하고 세분화된 보고 기능을 갖춘 Hillstone NIPS는 다양한 관점에서 네트워크 환경을 파악할 수 있도록 지원합니다.

- 비즈니스 시스템 관리자, 보안 관리자 또는 CIO나 임원 등 각 사용자에 따라 고유한 템플릿을 사용합니다.
- 위험을 명확하게 파악하여 올바른 결정을 내릴 수 있도록 보안, 시스템 위험, 네트워크 보안 위협, 트래픽 등의 여러 기준에 따라 체계적인 보안 위협 컨텐츠를 제공합니다.

간편한 구축 및 중앙 집중식 관리

Hillstone NIPS는 단순한 구축 및 관리로 오버헤드를 최소화합니다. 보안 요구사항을 충족하고 최적의 네트워크 연결을 보장하기 위해 다음과 같은 구축 모드가 지원됩니다.

제품 주요 정보 (계속되는)

• 능동적 방어(침입 방지 모드), 실시간모니터링 및 차단
• 수동적 탐지(침입 탐지 모드), 실시간모니터링 및 경고

Hillstone NIPS는 Hillstone 보안 관리 플랫폼(HSM)을 사용하여 관리할 수 있습니다. 관리자는 네트워크 간 통합 관리 정책을 사용하여 서로 다른 지사 또는 위치에 배포된 NIPS 장치를 한 곳에서 등록, 모니터링, 업그레이드할 수 있어 효율성이 극대화됩니다.

기능

침입 방지
- 8,000개 이상의 시그니처, 프로토콜 이상 탐지. 속도 기반 탐지, 사용자 정의 시그니처, 시그니처 업데이트의 수동/자동 푸시/풀, 통합 보안 위협 백과 사전
- IPS 작업: 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

위협 상관 분석
- 알려지지 않은 위협, 비정상적인 동작 및 잠재적인 위협 또는 공격을 발견하기위한 응용 프로그램 동작 간의 상관 관계
- 클라우드에서 매일 자동 업데이트되는 다차원 상관 규칙,

지능형 보안 위협 탐지
- 행위 기반의 지능형 악성 코드 탐지
- 바이러스, 웜, 트로이 목마, 오버플로우 등 2,000개 이상의 알려지거나알려지지 않은 악성 코드 제품군 탐지
- 악성 코드 행위 모델 데이터베이스 실시간 온라인 업데이트

비정상 행위 탐지
- 기본 L3-L7 트래픽 기반 행위 모델링을 통해 HTTP 스캐닝, Spider, SPAM, SSH/FTP의 취약한 암호와 같은 비정상 네트워크 행위 감지
- DDoS 탐지(Flood, Sockstress, zip of death, reflect, DNS query, SSL DDos, 애플리케이션 DDoS 등)
- 알려지지 않은 애플리케이션에 대한 암호화된 터널링 트래픽 검사 지원
- 비정상 행위 모델 데이터베이스의 실시간 온라인 업데이트

안티 바이러스
- 1,300만 개 이상의 AV 시그니처
- 플로우 기반 안티 바이러스: HTTP, SMTP, POP3, IMAP, FTP/SFTP 등의 프로토콜
- 압축 파일 바이러스 검사 지원

공격 방어
- 비정상적인 프로토콜 공격 방어
- SYN Flood, DNS 쿼리 Flood 방어를 포함한 Anti-DoS/DDoS
- ARP 공격 방어

URL 필터링
- 플로우 기반 웹 필터링 검사
- URL, 웹 컨텐츠 및 MIME 헤더를 기반으로 수동으로 정의된 웹 필터링
- 클라우드 기반 실시간 분류 데이터베이스-64 개 카테고리(8 개는 보안 관련)를 가진 1억 4천만 개 이상의 URL-를 사용한 동적 웹 필터링:
- 추가 웹 필터링 기능:
  - Java 애플릿, ActiveX, 쿠키 필터링
  - HTTP POST 차단
  - 검색 키워드 기록
  - 개인 정보 보호를 위해 특정 카테고리에서 암호화된 연결 검사 제외
- 웹 필터링 프로파일 재정의: 관리자가 사용자/그룹/IP에 임시로 서로 다른 프로파일을 지정 가능
- 웹 필터 로컬 카테고리 및 카테고리 등급 재정의

안티 스팸
- 실시간 스팸 분류 및 예방
- 확인된 스팸, 의심되는 스팸, 벌크 스팸, 유효한 벌크
- 메시지의 언어, 형식 또는 내용에 관계없는 보호
- SMTP 및 POP3 이메일 프로토콜 모두 지원
- 인바운드, 아웃바운드 탐지
- 신뢰할 수 있는 도메인/이메일주소로부터의 이메일을 허용하는 화이트리스트
- 사용자 정의 블랙리스트

클라우드 샌드박스
- HTTP/HTTPS, POP3, IMAP, SMTP 및 FTP를 포함한 프로토콜 지원
- PE, ZIP, RAR, Office, PDF, APK, JAR 및 SWF를 포함한 파일 형식 지원
- 파일 전송 방향 및 파일 크기 제어
- 글로벌 위협 인텔리전스 공유, 실시간 위협 차단

봇넷 C&C 예방
- C&C 연결을 모니터링하여 인트라넷의 봇넷 호스트를 찾고 봇넷 및 랜섬웨어와 같은 추가 고급 위협을 차단
- 봇넷 서버 주소를 정기적으로 업데이트
- C&C IP 및 도메인 예방
- TCP, HTTP 및 DNS 트래픽 감지 지원
- IP 및 도메인 화이트리스트

IP 평판
- 봇넷 호스트, 스패머, Tor 노드, 침해된 호스트 및 무차별 대입 공격과 같은 위험한 IP로부터의 트래픽을 식별하고 필터링
- 다양한 유형의 위험한 IP 트래픽에 대한 로깅, 패킷 드롭 또는 차단
- 정기적 인 IP 평판 시그니쳐 데이터베이스 업그레이드

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
- 작업: 차단, 모니터링
- 위험 카테고리 및 특성을 포함하여 클라우드에서 실행되는 애플리케이션에 다차원 모니터링 및 통계 제공

QoS
- 최대 또는 대역폭 보장 터널, IP/사용자 기준
- 보안 도메인, 인터페이스, 주소, 사용자/사용자 그룹, 서버/서버 그룹, 응용 프로그램/앱 그룹, TOS, VLAN을 기반으로 한 터널 할당
- 시간, 우선 순위 또는 동일 대역폭 공유에 따라 할당되는 대역폭
- TOS 및 DiffServ 지원
- 남은 대역폭의 우선 순위 할당
- IP 당 최대 동시 연결
- URL 카테고리에 따른 대역폭 할당
- 사용자 또는 IP에 대한 액세스를 지연시켜 대역폭 제한

기능 (계속되는)

IPv6
- IPv6, IPv6 로깅 및 HA에 대한 관리
- IPv6 터널링, DNS64 / NAT64 등
- IPv6 라우팅 프로토콜, 정적 라우팅, 정책 라우팅, ISIS, RIPng, OSPFv3 및 BGP4+
- IPS, 애플리케이션 식별, 안티 바이러스, 액세스 제어, ND 공격 방어

VSYS
- 각 VSYS에 시스템 리소스 할당
- CPU 가상화
- 비 루트 VSYS 지원 방화벽, IPSec VPN, SSL VPN, IPS, URL 필터링
- VSYS 모니터링 및 통계

HA
- 이중 하트비트 인터페이스
- Active/Passive 및 Peer Mode
- 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

손쉽게 파악할 수 있는 관리 기능
- 관리 액세스: HTTP/HTTPS, SSH, telnet, 콘솔
- 중앙 집중식 관리: Hillstone Security Manager(HSM), 웹 서비스 API
- 이중 인증: 사용자 이름/비밀번호, HTTPS 인증서 파일
- 시스템 통합: SNMP, syslog, 제휴 파트너쉽
- 빠른 구축: USB 자동 설치, 로컬 및 원격 스크립트 실행
- 동적 실시간 대시보드 상태 및 상세 모니터링 위젯
- 스토리지 장치 관리: 스토리지 공간 임계값 사용자 정의 및 경고, 오래된 데이터 오버레이, 기록 중지
- 언어 지원: 영어

로그 & 보고서
- 로그 위치: 로컬 메모리 및 스토리지, 다중 syslog 서버 및 다중 Hillstone Security Audit(HSA) 플랫폼
- HSA로의 지정 스케쥴 배치 로그 업로드를 통한 암호화된 로깅 및 로그 무결성 지원
- TCP 옵션(RFC 3195)을 사용한 안정적인 로깅
- 상세 트래픽 로그: 전달, 위반 세션, 로컬 트래픽, 유효하지 않은 패킷
- 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
- 특정 사용자 대상의 세분화된 보고 기능
  - HA 관리/임원용 보기
  - 비즈니스 시스템 소유자 보기
  - 네트워크 보안 관리자 보기

통계와 모니터링
- 응용 프로그램, URL, 위협 이벤트 통계 및 모니터링
- 실시간 트래픽 통계 및 분석
- 동시 세션, CPU, 메모리 및 온도와 같은 시스템 정보
- iQOS 트래픽 통계 및 모니터링, 링크 상태 모니터링
- Netflow(v9.0)를 통한 트래픽 정보 수집 및 전달 지원
- 클라우드 기반 위협 인텔리전스 푸시 서비스

CloudView
- 클라우드 기반 보안 모니터링
- 웹 또는 모바일 애플리케이션에서 24/7 액세스
- 장치 상태, 트래픽 및 위협 모니터링
- 클라우드 기반 로그 보존 및 보고

제품 사양

	S600	S1060	S1560	S2160	S2660	S3560	S3860	S5560
IPS Throughput (1)	1 Gbps	3 Gbps	4 Gbps	10 Gbps	14 Gbps	16 Gbps	21 Gbps	50 Gbps
Maximum Concurrent Connections (TCP) (2)	0.6 Million	1 Million	1 Million	2 Million	2 Million	4 Million	4 Million	8 Million
New connections per second (TCP) (3)	9,000	35,000	41,000	92,000	120,000	150,000	200,000	485,000
Stoneshield	N/A	N/A	Yes	N/A	Yes	N/A	Yes	Yes
Storage	1T	1T	1T	1T	1T	1T	1T	1T
Form Factor	1U	1U	1U	1U	1U	2U	2U	2U
Management Ports	2 x USB Port, 1X Consle Port	2 x USB Port, 1X Consle Port	2 x USB Port, 1X Consle Port	2×USB Port 2× MGT 1× Consle Port	2×USB Port 2×MGT 1× Consle Port	2×USB Port 2×MGT 1× Consle Port	2×USB Port 2×MGT 1× Consle Port	2×USB Port 2×MGT 1× Consle Port
Fixed I/O Ports	4 x GE	4 x GE	4 x GE	4 x GE	4 x GE	6 x GE	6 x GE	N/A
Available Slots for Extension Modules	1 x Generic Slot	1 x Generic Slot	1 x Generic Slot	2 x Generic Slot	2 x Generic Slot	2 x Generic Slot	2 x Generic Slot	4 x Generic Slot
Expansion Module Option	IOC-S-4GE-B-L IOC-S-4SFP-L	IOC-S-4GE-B-L IOC-S-4SFP-L	IOC-S-4GE-B-L IOC-S-4SFP-L	IOC-S-4GE-B IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP IOC-S-4GE-4SFP IOC-S-4SFP-B IOC-S-2SFP+ IOC-S-2SFP+-B IOC-S-4SFP+, IOC-S-4SFP+-B	IOC-S-4GE-B IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP IOC-S-4GE-4SFP IOC-S-4SFP-B IOC-S-2SFP+ IOC-S-2SFP+-B IOC-S-4SFP+, IOC-S-4SFP+-B	IOC-S-4GE-B IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP IOC-S-4GE-4SFP IOC-S-4SFP-B IOC-S-2SFP+ IOC-S-2SFP+-B IOC-S-4SFP+, IOC-S-4SFP+-B	IOC-S-4GE-B IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP IOC-S-4GE-4SFP IOC-S-4SFP-B IOC-S-2SFP+ IOC-S-2SFP+-B IOC-S-4SFP+, IOC-S-4SFP+-B	IOC-S-4GE-B-H IOC-S-4SFP-H IOC-S-8GE-B-H IOC-S-8SFP-H IOC-S-4SFP-B-H IOC-S-2SFP+-H IOC-S-4SFP+-H IOC-S-2SFP+-B-H IOC-S-4GE-4SFP-H
Latency	<100 μs	<100 μs	<100 μs	<100 μs	<100 μs	<100 μs	<100 μs	<100 μs
Bypass Support (Default/Max.)	4/8	4/8	4/8	4/20	4/20	6/22	6/22	0/32
Power Supply	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz
Maximum Power Consumption	1 x 60W	1 x 60W	1 x 60W	250W Redundancy 1 + 1	250W Redundancy 1 + 1	350W Redundancy 1 + 1	350W Redundancy 1 + 1	350W Redundancy 1 + 1
Dimension (W×D×H, mm)	16.9 ×11.8×1.7 in (430×300×44mm)	16.9 ×11.8×1.7 in (430×300×44mm)	16.9 ×11.8×1.7 in (430×300×44mm)	16.9 ×11.8×1.7 in (430×300×44mm)	16.9 ×11.8×1.7 in (430×300×44mm)	16.9×19.7×3.5 in (430×500×88mm)	16.9×19.7×3.5 in (430×500×88mm)	16.9×19.7×3.5 in (430×500×88mm)
Weight	14.3 lb (6.5kg)	14.3 lb (6.5kg)	14.3 lb (6.5kg)	22.0 lb (10kg)	22.0 lb (10kg)	35.3 lb (16kg)	35.3 lb (16kg)	35.3 lb (16kg)
Temperature	32-104 F (0-40 °C)	32-104 F (0-40 °C)	32-104 F (0-40 °C)	32-104 F (0-40 °C)	32-104 F (0-40 °C)	32-104 F (0-40 °C)	32-104 F (0-40 °C)	32-104 F (0-40 °C)
Relative Humidity	5-85% (no dew)	5-85% (no dew)	5-85% (no dew)	5-85% (no dew)	5-85% (no dew)	5-85% (no dew)	5-85% (no dew)	5-85% (no dew)

모듈 옵션

Module	**IOC-S-4GE-B-L**	**IOC-S-4SFP-L**	**IOC-S-4GE-B**	**IOC-S-4SFP**	**IOC-S-8GE-B**	**IOC-S-8SFP**	**IOC-S-4GE-4SFP**
I/O Ports	4 x GE By Pass Ports	4 x SFP Ports	4×GE Bypass Ports	4×SFP Ports	8×GE Bypass Ports	8×SFP Ports	4×GE and 4×SFP Ports
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)
Weight	0.22 lb (0.1kg)	0.22 lb (0.1kg)	0.33 lb (0.15kg)	0.33 lb (0.15kg)	0.55 lb (0.25kg)	0.55 lb (0.25kg)	0.55 lb (0.25kg)

Module	**IOC-S-2SFP+**	**IOC-S-4SFP+**	**IOC-S-4SFP-B**	**IOC-S-2SFP+-B**	**IOC-S-4SFP+-B**	**IOC-S-4GE-B-H**	**IOC-S-4GE-4SFP-H**
I/O Ports	2×SFP+ Ports	4×SFP+ Ports	4×SFP Bypass Ports	2×SFP+ Bypass Ports	4×SFP+ Bypass Ports	4×GE Bypass Ports	4×GE and 4×SFP Ports
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)
Weight	0.33 lb (0.15kg)	0.44 lb (0.2kg)	0.88 lb (0.4kg)	0.88 lb (0.4kg)	0.88 lb (0.4kg)	0.33 lb (0.15kg)	0.55 lb (0.25kg)

Module	**IOC-S-8GE-B-H**	**IOC-S-8SFP-H**	**IOC-S-4SFP-H**	**IOC-S-2SFP+-H**	**IOC-S-4SFP+-H**	**IOC-S-4SFP-B-H**	**IOC-S-2SFP+-B-H**
I/O Ports	8×GE Bypass Ports	8×SFP Ports	4×SFP Ports	2×SFP+ Ports	4×SFP+ Ports	4×SFP Bypass Ports	2×SFP+ Bypass Ports
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)
Weight	0.55 lb (0.25kg)	0.55 lb (0.25kg)	0.33 lb (0.15kg)	0.33 lb (0.15kg)	0.44 lb (0.2kg)	0.88 lb (0.4kg)	0.88 lb (0.4kg)

참고:

(1) IPS 처리량 데이터는 모든 IPS 규칙을 설정한 상태에서 양방향 HTTP 트래픽 감지를 통해 측정되었습니다.

(2) 최대 동시 연결 수는 TCP 트래픽을 사용하여 측정되었습니다. 최대 동시 연결 수를 확장하려면 AEL 라이센스가 필요합니다.

(3) 새 세션 수는 TCP 트래픽을 사용하여 측정되었습니다.

달리 명시되지 않는 한 모든 성능, 용량 및 기능 정보는 StoneOS5.5R3 기준입니다. 결과는 StoneOS® 버전 및 구축 환경에 따라 달라질 수 있습니다.

www.HillstoneNet.kr

버전: EX-08.01-NIPS-V3.4-0120-KR-01