Hillstone T 시리즈 지능형 차세대 방화벽

T1860 / T2860 / T3860
T5060 / T5860

Hillstone T 시리즈 지능형 차세대 방화벽(iNGFW)은 지속적으로 네트워크를 모니터링하는 애플리케이션 인식 방화벽입니다. 모든 운영 체제와 기기, 브라우저에서 보안 공격을 식별할 수 있습니다. 공격의 모든 단계에 대해 세부적으로 파악하여 정보를 제공하며 몇 분 또는 몇 초 내로 보안 침해를 탐지할 수 있습니다. 보안 위험도를 기준으로 호스트의 우선 순위를 지정하며 보안 위협에 대한 배경 정보를 제공합니다. 보안 관리자는 패킷 캡처 등을 포함하여 공격을 세부 분류하여 모든 보안 위협 정보를 분석할 수 있습니다.

Hillstone T 시리즈는 높은 수준의 보안, 향상된 파악 기능, 지속적인 네트워크 가동 시간이 필요한 중대 기업용으로 개발되었습니다.

Product Highlights

지속적인 보안 위협 방어

Hillstone T 시리즈 지능형 차세대 방화벽(iNGFW)은 세 가지 주요 기술을 사용하여 지속적인 보안 위협 방어를 제공합니다. 첫째, 통계적 클러스터링을 사용하여 거의 실시간으로 보안 침해를 감지합니다. 보안 위험도를 기준으로 호스트의 우선 순위를 지정하며 보안 공격에 대한 배경 정보를 제공합니다. 둘째, 동작 분석을 사용하여 이상 네트워크 동작을 감지합니다. 공격 킬 체인의 모든 단계를 파악하여 정보를 제공하며 사용자가 다양한 방식으로 공격을 차단할 수 있도록 지원합니다. T 시리즈는 위협 상관 관계 분석을 활용하여 사이버 보안 침해에 대한 전체 킬 체인을 표시할 뿐만 아니라 위험한 호스트의 현재 단계를 식별함으로써 공격의 피해 범위를 파악할 수 있습니다. 또한 포렌식 분석을 제공하여 공격의 근본 원인을 분석할 수 있습니다. 이를 통해 관리자는 정책을 수정하여 네트워크에서 향후 이와 유사한 침입을 방지할 수 있습니다.

통계적 클러스터링

Hillstone T 시리즈는 초기 감염 이후 이를 감지하기까지의 무방비 상태를 방지하기 위해 독점 기술인 통계적 클러스터링 알고리즘을 적용하여 알려진 악성 코드의 변종을 신속하게 감지합니다. 이미

Highlight

밝혀진 서명 검색 대신 악성 코드의 동작을 분석하고 알려진 악성 코드와 깊이 연관된 반복되는 동작의 조합을 검사합니다. 유사성이 확인되면 시스템은 경고를 전송하고 패킷 캡처를 비롯하여 악성 코드에 대한 완벽한 설명을 제공합니다. 또한 신뢰 수준 및 심각도 수준을 제공하여 관리자가 문제 해결 조치를 취할 수 있도록 합니다.

동작 분석

Hillstone T 시리즈는 공격의 모든 단계를 파악할 수 있는 정보는 제공합니다. 기계 학습을 사용하여 정상 네트워크 활동의 기준선을 설정하고 빅데이터 분석 및 수학적 모델링을 사용하여 킬 체인의 각 단계별 공격을 나타내는 비정상적인 네트워크 동작을 감지합니다. 직관적인 대시보드에 표시되는 이 정보는 사용자에게 공격을 차단할 수 있는 여러 기회를 제공합니다. 여러 가지 완화 기술이 디스플레이에 내장되어 관리자가 이상 트래픽을 조사할 동안 신속하게 잠재적 손실을 제한할 수 있습니다

포렌식 분석

Hillstone T 시리즈는 관리자가 공격의 근본 원인을 파악하는 데 도움이 되는 다양한 증거를 제공합니다. 보고서와 로그가 초기 손상 이후 데이터 유출까지 공격의 진행 단계에 대한 감사 추적을 제공합니다. 호스트는 보안 위험 및 지정된 위험 요소를 기준으로 우선 순위가 정해집니다. 각 공격의 자세한 설명과 신뢰도, 패킷 캡처와 함께 위험 요소에 관련된 보안 위협을 검사할 수 있습니다.

정교한 애플리케이션 제어

Hillstone T 시리즈 방화벽은 포트, 프로토콜, 회피 동작에 관계없이 웹 애플리케이션에 대한 정교한 제어를 제공합니다. 애플리케이션과 사용자, 사용자 그룹에 대한 정책 기반 제어를 제공하면서 고위험 애플리케이션과 관련된 잠재적인 위협을 식별하고 방지할 수 있습니다. 부적절하거나 악성인 애플리케이션을 제한하거나 차단하면서 미션 크리티컬 애플리케이션의 대역폭을 보장하는 정책을 정의할 수 있습니다. 이름과 카테고리, 하위 카테고리, 기술 및 위험을 기준으로 애플리케이션을 분류할 수 있습니다. 이러한 분류를 하나 이상 사용하여 정책을 생성하고 선택된 사용자와 그룹에 허용할 애플리케이션을 세부 조정할 수 있습니다. 또한 특정 시간대와 애플리케이션 특성을 기준으로 사용자/그룹에 대해 정책 기반 라우팅 및 대역폭 관리 정책을 생성할 수 있습니다. 이와 함께 사용자/그룹, 시간대 및 기타 기준에 따라 애플리케이션 내 특정 기능(예: 게임, 파일 공유)을 차단하거나 대역폭을 관리할 수 있습니다.

네트워크 위험 지수

Hillstone의 특허 받은 네트워크 위험 지수는 네트워크의 상태를 수치로 평가합니다. 보안 위협 정보와 호스트 위험 상태를 사용하여 네트워크의 현재 위험도를 계산합니다. 네트워크 가용성, 위험 요소 및 진행 중인 보안 위협에 대한 다차원 실시간 평가를 제공합니다. 직관적인 대시보드를 통해 IT 팀에서 적시에 보안 정책을 조정하여 보안 위험을 완화하고 네트워크 가동시간을 유지할 수 있습니다.

우수한 사용자 환경

Hillstone의 지능형 차세대 방화벽은 네트워크 애플리케이션, 네트워크 트래픽, 사용자 및 그룹, 대역폭 활용도, 악성 활동, 비정상적인 동작, 위험 요소, 진행 중인 위협 및 기타 여러 네트워크 및 보안 속성에 대한 파악 기능과 제어 기능을 제공합니다. 모니터링, 보고, 기록, 프로비저닝 및 운영 관리를 위한 다양한 도구 또한 사용할 수 있습니다

Features

Network Services
- 동적 라우팅(OSPF, BGP, RIPv2)
- 정적 및 정책 라우팅
- 애플리케이션별 라우팅 제어
- 내장 DHCP, NTP, DNS 서버 및 DNS 프록시
- 탭 모드 – SPAN 포트 접속
- IPv6 지원: IPv6를 통한 관리, IPv6 라우팅 프로토콜, IPv6 터널링, IPv6 로깅 및 HA
- 인터페이스 모드: 스니퍼, 포트 통합, 루프백, VLANS(802.1Q 및 트렁킹)
- L2/L3 스위칭 및 라우팅
- 가상 유선(Layer 1) 투명 인라인 배포

Firewall
- 작동 모드: NAT/라우팅, 투명(브릿지) 및 혼합 모드
- 정책 개체: 사전 정의, 사용자 정의 및 개체 그룹화
- 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 지원: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT, STUN
- NAT 구성: 정책별 및 중앙 NAT 표
- VoIP: SIP/H.323/SCCP NAT 통과, RTP 핀 홀링
- 글로벌 정책 관리 보기
- 일정: 1회성 및 반복
- QoS 트래픽 형상화:
  - 최대/보장 대역폭 터널 또는 IP/사용자 기준
  - 보안 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 차등 서비스(DiffServ) 지원
  - 우선 순위별 잔여 대역폭 할당
  - IP당 최대 동시 연결
- 가상 방화벽: 최대 250개의 vSYS 로드 밸런싱 방화벽
- 로드 밸런싱:
  - 가중 해시, 가중 최소 연결 및 가중 라운드 로빈
  - 세션 보호, 세션 지속 및 세션 상태 모니터링
  - 양방향 링크 로드 밸런싱
  - 정책 기반 라우팅, ECMP 및 가중, 내장 ISP 라우팅, 동적 감지 포함 아웃바운드 링크 로드 밸런싱

  - SmartDNS 및 동적 감지 지원 인바운드 링크 로드 밸런싱
  - 대역폭 및 지연 시간 기준 자동 링크 스위칭
  - ARP, PING 및 DNS의 링크 상태 검사
- IP 주소 위치 정보 기준 액세스 제어
- 반복 및 이중 방화벽 규칙 조사

VPN
- IPSec VPN:
  - IPSEC 1단계 모드: 공격적 주 ID 보호 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 통과 활성화 유지 빈도
  - 1단계/2단계 제안 암호화: DES, 3DES, AES128, AES192, AES256
  - 1단계/2단계 제안 인증: MD5, SHA1, SHA256, SHA384, SHA512
  - 1단계/2단계 Diffie-Hellman 지원: 1,2,5
  - XAuth as server 모드 및 다이얼업 사용자용
  - 죽은 피어 감지
  - 재생 감지
  - 2단계 SA용 자동키 활성화 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, 완전 메시, 부챗살, 이중 터널, 투명 모드의 VPN 종료
- 동일한 사용자 이름을 사용한 동시 로그인을 방지하는 1회 로그인
- SSL 포털 통시 사용자 제한
- 클라이언트 데이터를 암호화하여 애플리케이션 서버로 전송하는 SSL VPN 포트 포워딩 모듈
- iOS, Android 및 Windows XP/Vista(64비트 Windows OS 포함) 기반 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

User and Device Identity
- 로컬 사용자 데이터베이스
- 원격 사용자 인증: TACACS+,LDAP, Radius, Active Directory
- 싱글사인온: Windows AD
- 이중 인증: 타사 지원, 물리적 및 SMS의 통합 토큰 서버
- 사용자 및 기기 기반 정책

IPS
- 7,000개 이상의 서명, 프로토콜 이상 탐지, 속도 기반 탐지, 사용자 정의 서명, 서명 업데이트의 수동/자동 푸시/풀, 통합 보안 위협 백과 사전
- IPS 작업: 기본, 모니터링, 차단, 만료 시간으로 차단 (공격자 IP 또는 피해자 IP, 수신 인터페이스)
- 패킷 로깅 옵션
- 필터 기반 선택: 심각도, 대상, OS, 애플리케이션 또는 프로토콜
- 특정 IPS 서명에서 IP 면제
- IDS 스니퍼 모드
- IPv4 및 IPv6 속도 기반 DoS 보호 및 TCP Syn flood에 대한 임계값 설정, TCP/UDP/SCTP 포트 검사, ICMP 스위프, TCP/UDP/SCIP/ICMP session flooding(소스/목적지)
- 우회 인터페이스의 활성 우회
- 방어 구성의 사전 정의 템플릿 제공
- 사전 정의 방지 구성

Threat Protection
- 보안 침해 감지
  - 거의 실시간으로 보안 침해 감지(수초/수분)
  - 유사 공격의 악성 코드에 대한 상세 설명 및 심각도
  - 확실한 증거를 제공하는 Pcap 파일 및 로그 파일
  - 공격의 확실성을 제공하는 신뢰도
  - 알려지지 않은 애플리케이션의 암호화된 터널링 트래픽의 검사 지원
- 네트워크 동작 분석
  - L3-L7 기준 트래픽과 실시간 트래픽의 비교로 이상 네트워크 동작 감지
  - 내장 완화 기술(세션 제한, 대역폭 제한 및 차단 등)
  - 기준, 상부 및 하부 임계값과 비교한 이상 동작의 그래픽 표시
  - Slow Drip DDoS 검사
- 누적 호스트 지수 기준 네트워크의 보안 위험도를 수치로 평가하는 Network Risk Index
- 공격 심각도, 감지 방법 및 신뢰도 기준 호스트 보안 위험도를 평가하는 Host Risk Index
- DGA 기반 C&C 검사
- 킬 체인 상의 위험한 호스트에 대한 시각적 정보 제공
- 130만 개 이상의 안티 바이러스 서명
- 봇넷 서버 IP 차단 및 글로벌 IP 평가 데이터베이스
- 플로우 기반 안티 바이러스: HTTP, SMTP, POP3, IMAP, FTP/SFTP 등의 프로토콜
- 플로우 기반 웹 필터링 검사
- URL, 웹 컨텐츠 및 MIME 헤더 기반 수동 정의 웹 필터링
- 동적 웹 필터링 및 클라우드 기반 실시간 분류 데이터베이스: 1억 4천만 개 이상의 URL 및 64개의 카테고리(그 중 8개는 보안 관련)
- 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 면제
- 웹 필터링 프로필 재정의: 관리자가 임시로 사용자/그룹/IP에 서로 다른 프로필을 지정 가능
- 웹 필터 로컬 카테고리 및 카테고리 등급 재정의
- 프록시 회피 방지: 프록시 사이트 카테고리 차단, 도메인과 IP 주소로 URL 평가, 캐시 및 번역 사이트의 리디렉션 차단, 프록시 회피 애플리케이션 차단, 프록시 동작 차단(IPS)

Application Control
- 이름, 카테고리, 하위 카테고리, 기술 및 위험을 기준으로 3,000개 이상의 애플리케이션 필터링
- 각 애플리케이션에는 설명, 위험 요소, 의존도, 일반적으로 사용하는 포트, 추가 참조용 URL이 포함됨
- 작업: 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

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

Administration
- 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
- 사용자 OS 및 웹 브라우저 식별 및 모니터링

Logs & Reporting
- 로깅 장비: 로컬 메모리 및 스토리지(해당될 경우), 다중 syslog 서버 및 다중 Hillstone Security Audit(HSA) 플랫폼
- HSA 지정 일정 배치 로그 업로드의 암호화된 로깅 및 로그 무결성
- 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 확인 옵션
- 간단 트래픽 로그 형식 옵션

SSL Decryption
- SSL 암호화 트래픽 검사
- SSL 암호화 트래픽을 위한 IPS 활성화 지원
- SSL 암호화 트래픽을 위한 안티 바이러스 활성화 지원
- https 암호화 트래픽을 위한 URL 필터링 지원

Product Specification

Specification	SG-6000-T1860	SG-6000-T2860	SG-6000-T3860	SG-6000-T5060	SG-6000-T5860
					
FW Throughput	8Gbps	10Gbps	20Gbps	25Gbps	40Gbps
IPS Throughput(1)	3Gbps	4Gbps	8Gbps	12Gbps	18Gbps
AV Throughput(2)	1.6Gbps	2Gbps	6Gbps	6.5Gbps	9.5Gbps
IPSec Thoughtput(3)	3Gbps	3.8Gbps	12Gbps	15Gbps	28Gbps
New Sessions/ sec(HTTP)	80K	100K	250K	300K	450K
IPSec Tunnel Number	6,000	10,000	20,000	20,000	20,000
Maximum SSL VPN Users	4,000	6,000	10,000	10,000	10,000
Maximum Concurrent Sessions	1.5M	3M	4M	5M	6M
Integrated I/O	6 × GE, 4 × SFP	6 × GE(1 pair bypass port), 4 × SFP, 2 × SFP+	2 × GE, 4 × SFP	2 × GE, 4 × SFP	2 × GE, 4 × SFP
Maximum I/O	26 × GE	26 × GE, 2 × 10GE	22 × GE, 4 × 10GE	38 × GE, 8 × 10GE	38 × GE, 8 × 10GE
Expansion Modules	2 × Generic Slot	2 × Generic Slot	2 × Generic Slot	4 × Generic Slot	4 × Generic Slot
Expansion Module Option	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-2XFP-Lite-M	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-4XFP, IOC-8SFP+, IOC-4SFP+, IOC-2XFP-Lite-M(only supported at Slot-3/4) ,	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-4XFP, IOC-8SFP+, IOC-4SFP+, IOC-2XFP-Lite-M (only supported at Slot-3/4)
Management Ports	1 × Concole Port, 1 × HA, 1 × MGT, 1 × USB 2.0, 1 × AUX Port	1 × Concole Port, 1 × HA, 1 × MGT, 1 × USB 2.0, 1 × AUX Port	1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT	1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT	1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT
Maximum Power Consumption	1 × 150w Redundancy 1 + 1	1 × 150w Redundancy 1 + 1	2 × 450W Redundancy 1 + 1	2 × 450W Redundancy 1 + 1	2 × 450W Redundancy 1 + 1
Storage	500G HDD	500G HDD	80G SSD, 500G HDD or 1T HDD	120G SSD, 500G HDD or 1T HDD	120G SSD, 500G HDD or 1T HDD
Power Supply	AC 100~240V 50/60Hz DC -40~-60V	AC 100~240V 50/60Hz DC -40~-60V	AC 100-240V 50/60Hz DC -40 ~ -60V	AC 100-240V 50/60Hz DC -40 ~ -60V	AC 100-240V 50/60Hz DC -40 ~ -60V
Dimension (W × D × H)	1U 17.2 × 14.4 × 1.7 in (436 × 366 × 44 mm)	1U 17.2 × 14.4 × 1.7 in (436 × 366 × 44 mm)	2 U 17.3 × 20.5 × 3.5 in (440 × 520 × 88 mm)	2 U 17.3 × 20.5 × 3.5 in (440 × 520 × 88 mm)	2 U 17.3 × 20.5 × 3.5 in (440 × 520 × 88 mm)
Weight	12.3 lb (5.6KG)	12.3 lb (5.6KG)	34.2 lb (15.5KG)	34.8 lb (15.8 KG)	34.8 lb (15.8 KG)
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)
Relative Humidity	10-95%	10-95%	10-95%	10-95%	10-95%

Specification	IOC-8GE-M	IOC-8SFP-M	IOC-4GE-B-M	IOC-2XFP-Lite-M
				
Name	8GE Extension Module	8SFP Extension Module	4GE Bypass Extension Module	2XFP Extension Module
I/O Ports	8 × GE	8 × SFP, SFP module not included	4 × GE Bypass (2 pair bypass ports)	2 × XFP, XFP module not included
Dimension	½ U (Occupies 1 generic slot)	½ U (Occupies 1 generic slot)	½ U (Occupies 1 generic slot)	½ U (Occupies 1 generic slot)
Weight	1.8 lb (0.8kg)	2.0 lb (0.9kg)	1.8 lb (0.8kg)	2.0 lb (0.9kg)

Specification	IOC-4XFP	IOC-8SFP+	IOC-4SFP+
			
Name	4XFP Extension Module	8SFP+ Extension Module	4SFP+ Extension Module
I/O Ports	4 × XFP, XFP module not included	8 × SFP+, SFP+ module not included	4 × SFP+, SFP+ module not included
Dimension	1 U (Occupies 2 generic slots)	1 U (Occupies 2 generic slots)	1 U (Occupies 2 generic slots)
Weight	2.0 lb (0.9kg)	1.5 lb (0.7kg)	1.5 lb (0.7kg)

(1) IPS Throughput data is obtained under 1M-byte-payload HTTP traffic with test of 32K-byte scanning.
(2) AV Throughput data is obtained under 1M-byte-payload HTTP traffic with file attachment.
(3) IPSec Throughput data is obtained under Preshare Key AES256+SHA-1 configuration and 1400-byte packet size packet .

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS 5.5R2. Results may vary based on StoneOS® version and deployment.

hillstone@kltec.kr | 1800-8773