Hillstone NETWORKS

Hillstone T-시리즈
지능형 차세대 방화벽

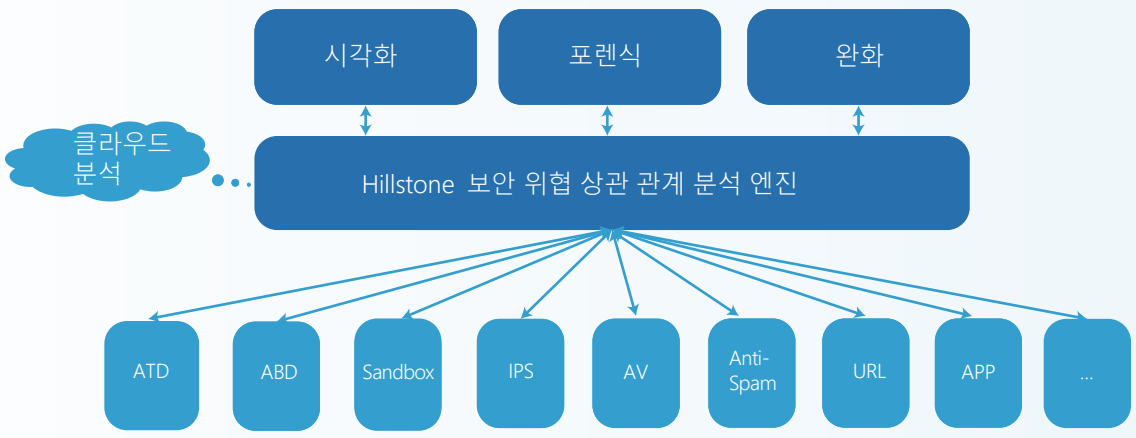
NSS LABS RECOMMENDED

ICSA labs CERTIFIED FIREWALL - CORPORATE

T1860 / T2860 / T3860 / T5060 / T5860

Hillstone T 시리즈 지능형 차세대 방화벽(iNGFW)은 세 가지 주요 기술을 사용하여 지속적인 보안 위협 방어를 제공합니다. 첫째, 특허받은 Hillstone 지능형 보안 위협 탐지(ATD) 엔진을 활용하는 통계 클러스터링을 사용하여 알려지지 않은 악성 코드를 탐지합니다. 둘째, Hillstone 비정상 행위 탐지(ABD) 엔진을 기반으로 하는 행위 분석을 사용하여 정상적이지 않은 네트워크 행위를 감지합니다. 마지막으로 ATD, ABD, 샌드박스, 기타 기존의 시그니처 기반 위협 탐지 기술 등 서로 다른 여러 엔진에서 탐지한 보안 위협 이벤트와 컨텍스트 정보의 연관성을 분석하여 지능형 보안 위협을 식별하기 위해 Hillstone 의 보안 위협 상관 관계 분석 엔진을 활용합니다.

Hillstone iNGFW는 심층적인 탐지 및 보안 위협 분석 기능을 사용하여 고객에게 각 호스트의 보안 위협 세부 정보는 물론, 네트워크의 위험 상태를 포괄적으로 파악할 수 있는 기능을 제공합니다. 또한 Hillstone iNGFW는 관리자가 공격의 근본 원인을 찾아 조사하는 데 필요한 다양한 툴과 경로로부터의 포렌식 정보를 제공합니다. 이와 함께 Hillstone iNGFW의 강력한 완화 기능은 관리자가 포렌식 데이터를 검사할 수 있는 시간을 벌어주어, 정확한 정보를 바탕으로 공격의 진위 여부를 판단하고 비즈니스 피해를 최소화할 수 있도록 합니다.



www.hillstonenet.kr
Phone: 1-800-889-9860

제품 주요 정보

알려지지 않은 악성 코드 탐지

Hillstone은 약 100만 개의 "알려진" 악성 코드 샘플을 분석한 독자 엔진을 구축했으며, 동작, 자산, 속성에 관한 여러 가지 복합적인 기준에 따라 그 특성별로 각 샘플을 분류했습니다. 운영 환경에서 새로운 악성 코드가 발견되면 이 코드 또한 분석을 거쳐 그 특성에 맞게 분류됩니다. 그런 다음 이미 분석된 악성 코드 샘플의 데이터베이스와 비교하며, 알려지지 않은 샘플이 알려진 샘플과 유사할수록 알려진 악성 코드 샘플의 변종임을 나타내는 지수가 높아집니다. "통계 클러스터링"이라고 하는 이 프로세스는 새로운 악성 코드를 정확하게 식별할 수 있는 방법을 제공합니다.

다양한 포렌식 분석

Hillstone은 공격을 시각화하고 분석하기 위한 새로운 방법을 제공합니다. 잠재적 악성 코드에 의해 수행되는 모든 동작은 자동으로 "킬 체인" 내의 단계와 연결됩니다. 이 과정에서 다양한 포렌식 정보가 함께 제공되어 보안 분석가가 공격의 시작 시점과 공격의 심각도, 사용된 방법을 파악할 수 있습니다. Hillstone은 또한 syslog 및 트래픽 로그에 추가하여 관리자에게 다양한 부가 정보를 제공할 수 있는 패킷 캡처 파일을 제공합니다. 이와 함께 방문한 웹사이트, 사용된 애플리케이션, 애플리케이션의 위험 수준과 같은 사용자 데이터를 통해 공격에 악용된 취약점을 파악할 수 있습니다. 가장 중요한 것은 Hillstone은 방화벽 통과를 야기한 방화벽 정책을 정확하게 식별한다는 것입니다.

비정상 행위 감지

각 월/일/시별로 정상적인 네트워크 트래픽 상태를 파악하여 네트워크 동작이 계산된 임계치를 초과할 경우 경고를 표시합니다. 50차원 이상의 배열을 사용하여 L4-L7 계층의 일반 네트워크 트래픽을 계산하는데, 이를 "행위 모델링"이라고 합니다. 또한 악성 동작을 더욱 정확하고 확실하게 식별할 수 있도록 실제 해킹 툴을 사용한 훈련도 수행하고 있습니다. 이러한 방법을 통해 오탐지를 방지하고 사용자에게 공격을 막을 수 있는 여러 기회를 제공합니다.

사전 예방적 완화

Hillstone에는 공격을 막기 위해 정책을 변경하는 기능 외에도 몇 가지 자동 완화 기능이 내장되어 있습니다. 이러한 기능은 의심스러운 행위가 감지되면 자동으로 공격을 차단하거나 둔화시키는 사전 정의된 템플릿으로 구성됩니다. 관리자는 템플릿을 수정하여 공격자가 이용할 수 있는 대역폭이나 세션 수를 제한할 수 있습니다. 또한 공격 유형과 심각도 수준에 따라 네트워크 리소스에 지정한 제약 조건을 조정할 수 있습니다. 공격의 심각도와 공격 지수가 높을 경우 모든 네트워크 리소스를 완전히 차단하는 완화 조치를 취할 수 있습니다. 템플릿이 없거나 활성화되지 않은 경우에는 관리자가 신속하게 해당 이벤트에 대한 임시 완화 조치를 설정할 수 있습니다.

기능

보안 위협 상관 관계 분석
- 알려지지 않은 보안 위협, 비정상 행위 및 애플리케이션 행위 간의 상관 관계를 분석하여 잠재적 위협 또는 공격 발견
- 클라우드에서 매일 자동 업데이트되는 다중 차원의 상관 관계 규칙

지능형 보안 위협 탐지
- 행위 기반의 지능형 악성 코드 탐지
- 바이러스, 웜, 트로이 목마, 오버플로우 등 2,000개 이상의 알려지거나 알려지지 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
- DGA(Domain Generation Algorithm)를 사용한 C&C 공격 탐지
- 비정상 행위 모델 데이터베이스의 실시간 온라인 업데이트

보안 위협 파악 및 완화
- 네트워크 위험 지수, 중요 자산 및 호스트 위험 상태, 호스트 및 보안 위협의 위험 심각도 및 확실성
- 각 호스트에 대한 보안 위협 이벤트의 킬 체인 매핑
- 보안 위협 분석, 기술 자료, 기록 및 PCAP를 포함한 보안 위협 포렌식
- 완화 규칙의 사전 정의 및 사용자 정의

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
- 버추어 와이어(Layer 1) 트랜스패어런트 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
- 스케줄: 1회성 및 반복

침입 방지
- 프로토콜 이상 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

안티 스팸
- 실시간 스팸 분류 및 방지
- 확인된 스팸, 의심되는 스팸, 대량 스팸, 유효 대량 스팸
- 메시지의 언어, 형식 또는 내용에 관계없이 방어
- SMTP 및 POP3 이메일 프로토콜 모두 지원
- 인바운드 및 아웃바운드 탐지
- 신뢰할 수 있는 도메인의 이메일을 허용하는 화이트리스트

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

IP 평판
• 글로벌 IP 평가 데이터베이스에 기반한 봇넷 서버 IP 차단

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

엔드포인트 식별
• 엔드포인트 IP, 엔드포인트 수, 온라인 시간, 오프라인 시간 및 온라인 지속 기간 식별 지원
• 10개 운영 체제 지원
• IP 및 엔드포인트 수 기반 쿼리 지원

데이터 보안
• 파일 유형 기반 파일 전송 제어
• 파일 프로토콜 식별(HTTP, FTP, SMTP 및 POP3 포함)
• 100개 이상의 파일 유형에 대한 파일 시그니처 및 접미사 식별
• 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 리셋, 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

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

링크 로드 밸런싱
• 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 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
• 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 모드의 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

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 및 ND 공격 방어

VSYS
• 각 VSYS에 대한 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/Active 및 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

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
• 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

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 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, 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 정의된 보고서: 보안, 플로우 및 네트워크 보고서 형식
• 사용자 정의 보고 기능
• 이메일 및 FTP를 통한 PDF 형식 보고서 전송

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

제품 사양

Specification	SG-6000-T1860	SG-6000-T2860	SG-6000-T3860	SG-6000-T5060	SG-6000-T5860
					
FW Throughput[1]	8Gbps	10Gbps	20Gbps	25Gbps	40Gbps
IPS Throughput[2]	3Gbps	4Gbps	8Gbps	12Gbps	18Gbps
AV Throughput[3]	1.6Gbps	2Gbps	6Gbps	7Gbps	10Gbps
IPSec Throughput[4]	3Gbps	3.8Gbps	12Gbps	15Gbps	28Gbps
IMIX Throughput[5]	1.6Gbps	2.1Gbps	8.2Gbps	10.9Gbps	17.4Gbps
NGFW Throughput[6]	1Gbps	1.5Gbps	5Gbps	8Gbps	12Gbps
Threat Protection Throughput[7]	600Mbps	900Mbps	2.5Gbps	4Gbps	6Gbps
New Sessions/s[8]	80K	100K	250K	300K	450K
Maximum Concurrent Sessions	1.5M	3M	4M	5M	6M
IPSec Tunnel Number	6,000	10,000	20,000	20,000	20,000
SSL VPN Users (Default/Max)	8/4,000	8/6,000	128/10,000	128/10,000	128/10,000
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	480G SSD (960G SSD Optional)	480G SSD (960G SSD Optional)	Dual Storage: 120G (480G or 960G SSD Optional) +480G SSD (960G SSD Optional)	Dual Storage: 120G (480G or 960G SSD Optional) +480G SSD (960G SSD Optional)	Dual Storage: 120G (480G or 960G SSD Optional) +1T HDD (960G SSD Optional)
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℃)	32-104 F (0-40℃)	32-104 F (0-40℃)	32-104 F (0-40℃)	32-104 F (0-40℃)
Relative Humidity	10-95%	10-95%	10-95%	10-95%	10-95%
Compliance and Certificate	CE, CB, FCC, UL/cUL, ROHS, IEC/EN61000-4-5 Power Surge Protection, ISO 9001:2015, ISO 14001:2015, CVE Compatibility, IPv6 Ready, ICSA Firewalls				

모듈 옵션

Specification	IOC-8GE-M	IOC-8SFP-M	IOC-4GE-B-M	IOC-2XFP-Lite-M	IOC-4XFP	IOC-4SFP+	IOC-8SFP+
							
Name	8GE Extension Module	8SFP Extension Module	4GE Bypass Extension Module	2XFP Extension Module	4XFP Extension Module	4SFP+ Extension Module	8SFP+ Extension Module
I/O Ports	8 x GE	8 x SFP, SFP module not included	4 x GE Bypass (2 pair bypass ports)	2 x XFP, XFP module not included	4 x XFP, XFP module not included	4 x SFP+, SFP+ module not included	8 x SFP+, SFP+ module not included
Dimension	½ U (Occupies 1 generic slots)	½ U (Occupies 1 generic slot)	½ U (Occupies 1 generic slot)	½ U (Occupies 1 generic slot)	1 U (Occupies 2 generic slots)	1 U (Occupies 2 generic slots)	1 U (Occupies 2 generic slots)
Weight	1.8 lb (0.8kg)	2.0 lb (0.9kg)	1.8 lb (0.8kg)	2.0 lb (0.9kg)	2.0 lb (0.9kg)	1.5 lb (0.7kg)	1.5 lb (0.7kg)

달리 명시되지 않는 한 모든 성능, 용량 및 기능 정보는 StoneOS5.5R5 기준입니다. 결과는 StoneOS® 버전 및 구축 환경에 따라 달라질 수 있습니다

참고: (1) FW 처리량 데이터는 1518바이트 패킷의 싱글 스택 UDP 트래픽을 사용하여 측정되었습니다. (2) IPS 처리량 데이터는 모든 IPS 규칙을 설정한 상태에서 양방향 HTTP 트래픽 감지를 통해 측정되었습니다. (3) AV 처리량 데이터는 첨부 파일을 포함한 HTTP 트래픽을 사용하여 측정되었습니다. (4) IPSec 처리량 데이터는 Preshare Key AES256+SHA-1 구성과 1400바이트 패킷을 사용하여 측정되었습니다. (5) IMIX 처리량 데이터는 UDP 트래픽 믹스(64바이트: 1518바이트=5:7:1)를 사용하여 측정되었습니다. (6) NGFW 처리량 데이터는 애플리케이션 제어 및 IPS를 설정한 상태에서 64K 바이트 HTTP 트래픽을 사용하여 측정되었습니다. (7) 보안 위협 방어 처리량 데이터는 애플리케이션 제어, IPS, AV, URL 필터링, ABD 및 ATD를 설정한 상태에서 64K 바이트 HTTP 트래픽을 사용하여 측정되었습니다. (8) 새 세션수/초는 TCP 트래픽을 사용하여 측정되었습니다.

Version :EX-08.01-iNGFW-5.5R5-1217-KR-02