Hillstone X-Series Data Center Firewall X10800

X10800

전면

후

탁월한 성능과 안정성, 확장성을 갖춘 Hillstone X10800 데이터 센터 방화벽은 고속 서비스 공급업체와 대기업, 통신업체에 적합하며 높은 처리량, 뛰어난 동시 연결 및 신규 세션 기능을 갖춘 방화벽을 완벽하게 구현하는 혁신적인 완전 분산 아키텍처 기반의 제품입니다. 또한 Hillstone X10800은 대용량 가상 방화벽을 지원하여 가상 환경에 유연한 보안 서비스를 제공하는 것은 물론이고 애플리케이션 식별, 트래픽 관리, 침입 방지, 공격 방지 등의 기능으로 데이터 센터 네트워크의 완벽한 보안을 보장합니다.

제품 주요 정보

탄력적인 보안 아키텍처 기반의 뛰어난 성능

트래픽이 폭발적으로 증가하고 있는 데이터 센터 방화벽에는 높은 트래픽과 대규모 동시 사용자 액세스를 처리하는 강력한 기능과 함께 사용자 활동의 급격한 증가에 효과적으로 대처할 수 있는 능력이 필요합니다. 따라서 데이터 센터 방화벽은 높은 처리량뿐만 아니라 매우 높은 동시 연결 및 신규 세션 처리 기능을 갖춰야 합니다.

Hillstone X10800 데이터 센터 방화벽은 혁신적인 완전 분산 아키텍처를 사용하여 서비스 모듈(SSM) 및 인터페이스 모듈(IOM)에서 지능형 트래픽 분산 알고리즘을 통해 서비스 트래픽의 고속 분산 처리를 구현합니다.

특허받은 리소스 관리 알고리즘을 통해 분산형 멀티 코어 프로세서 플랫폼의 잠재력을 충분히 발휘할 수 있으므로 방화벽 동시 연결 및 초당 신규 세션의 성능이 더욱 향상되며 시스템 성능의 완전한 선형 확장이 가능합니다. X10800 데이터 센터 방화벽은 처리량이 최대 1Tbps에 달하며 최대 1천만 건의 초당 신규 세션, 최대 4억 8천만 건의 동시 연결을 처리할 수 있습니다. 이 장치는 최대 44개의 100GE 인터페이스와 88개의 10G 인터페이스 또는 22개의 40GE 인터페이스와 132개의 10G 인터페이스의 확장을 제공합니다. 또한 패킷 전달 지연이 10us 이내이므로 데이터 센터의 실시간 서비스 전달 수요를 충분히 충족할 수 있습니다.

통신 사업자급 안정성

X10800 데이터 센터 방화벽의 하드웨어와 소프트웨어는 99.999%의 통신 사업자급 안정성을 제공합니다. Active/Active 또는 Active/Passive 모드 이중 구축 솔루션을 지원하여 단일 장애가 발생해도 무중단 서비스가 보장됩니다. 전체 시스템은 모듈식 설계를 사용하여 제어 모듈 중복성, 서비스 모듈 중복성, 인터페이스 모듈 중복성, 스위칭 모듈 중복성을 지원하며 모든 모듈은 핫 스왑이 가능합니다.

X10800 데이터 센터 방화벽은 멀티모드 및 싱글모드 광 바이패스 모듈을 지원합니다. 전원 꺼짐 등 특수한 상황이 될 경우 시스템이 바이패스 모드에서 동작하여 무중단 비즈니스 운영을 보장합니다. 또한 전원 중복성, 팬 중복성 및 그 밖의 주요 구성 요소를 제공하여 신뢰성을 보장합니다.

트윈 모드 HA로 이중 데이터 센터의 비대칭 트래픽 문제를 해결합니다. 방화벽 트윈 모드는 매우 안정적인 네트워크 모드로, 이중 장치 백업을 기반으로 구축됩니다. 2개의 데이터 센터에 Active/Passive 방화벽 2세트가 전용 데이터 링크 및 제어 링크를 통해 연결되며, 장치 2세트에서 세션 정보 및 구성 정보가 서로 동기화됩니다.

최고의 가상 방화벽 기술

가상화 기술은 데이터 센터에서 점점 더 광범위하게 사용되고 있습니다. X10800 데이터 센터 방화벽은 데이터 센터의 가상화 요구사항에 맞춰 하나의 물리적 방화벽을 1천 개 이상의 가상 방화벽으로 논리적으로 나눌 수 있어 대규모 데이터 센터에 적합한 가상 방화벽 지원 기능을 제공합니다. 또한 사용자가 CPU와 세션을 비롯하여 정책 및 포트 등의 개수와 같은 실제 비즈니스 조건을 기반으로 각각의 가상 방화벽에 대해 리소스를 동적으로 설정할 수 있으므로 가상 환경의 서비스 트래픽에 유연하게 변경 사항을 적용할 수 있습니다. X10800 데이터 센터 방화벽의 각 가상 방화벽 시스템은 독립된 시스템 리소스를 갖추고 있을 뿐 아니라 다양한 서비스 또는 사용자에 대해 독립된 보안 관리 플레인을 제공할 수 있도록 개별적으로 세분화하여 관리할 수 있습니다.

세분화된 애플리케이션 제어 및 종합 보안

X10800 데이터 센터 방화벽은 고급 심층 애플리케이션 식별 기술을 사용하여 프로토콜 기능, 행위 특성, 상관 관계 분석을 기반으로 수백 가지 모바일 애플리케이션과 암호화된 P2P 애플리케이션 등의 수많은 네트워크 애플리케이션을 정확하게 식별하며 정교하고 유연한 애플리케이션 보안 제어 기능을 제공합니다.

또한 X10800 데이터 센터 방화벽은 심층 애플리케이션 식별, 프로토콜 탐지, 공격 원칙 분석을 기반으로 침입 방지 기술을 제공합니다. 트로이 목마, 웜, 스파이웨어, 취약점 공격과 같은 보안 위협을 효과적으로 탐지하고 공격을 피하며 사용자에게 L2~L7 네트워크 보안 기능을 제공합니다. 그중 웹 보호 기능은 웹 서버의 심층 보안 방어 요구사항을 충족하며 봇넷 필터링 기능으로는 내부 호스트가 감염되지 않도록 보호할 수 있습니다.

X10800 데이터 센터 방화벽은 수천만 개의 URL 시그니처 라이브러리에 대한 URL 필터링을 지원하며, 관리자가 웹 검색 액세스 제어 기능을 간편하게 구현하고 악성 URL의 보안 위협 침투를 방지할 수 있도록 도움을 줍니다.

X10800 데이터 센터 방화벽의 지능형 대역폭 관리는 심층 애플리케이션 식별 및 사용자 식별을 기반으로 합니다. 서비스 애플리케이션 우선 순위와 결합된 X10800 데이터 센터 방화벽은 정책을 기반으로 2개 계층, 8개 레벨의 세분화된 트래픽 제어 기능을 구현하고 탄력적인 QoS 기능을 제공할 수 있습니다. 세션 제한, 정책, 라우팅, 링크 로드 밸런싱, 서버 로드 밸런싱 등의 기능과 함께, 더욱 유연한 트래픽 관리 솔루션을 제공합니다.

강력한 네트워크 적응성

X10800 데이터 센터 방화벽은 듀얼 스택, 터널, DNS64/NAT64 및 그 밖의 전환 기술 등 차세대 인터넷 배치 기술을 완벽하게 지원합니다. 또한 외부 네트워크 주소의 고정 포트 블록을 인트라넷 주소에 정적으로 매핑하도록 지원하는 충분히 안정된 NAT444 기능을 갖추고 있습니다. 세션과 사용자를 기반으로 로그를 생성할 수 있어 간편하게 추적할 수 있습니다. Full-cone NAT, 포트 멀티플렉싱 등 향상된 NAT 기능으로 현재의 ISP 네트워크에 대한 요구사항을 완벽하게 충족하며 사용자 네트워크 구축 비용을 절감할 수 있습니다.

X10800 데이터 센터 방화벽은 표준 IPSec VPN 기능을 완벽하게 지원하고 3세대 SSL VPN을 통합하여 사용자에게 고성능, 대용량의 완벽한 VPN 솔루션을 제공합니다. 그와 동시에, 고유한 플러그 앤 플레이 VPN으로 구성 및 유지 관리 문제를 크게 간소화하며 사용자에게 편리한 원격 보안 액세스 서비스를 제공합니다.

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) 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 트래버설, RTP 핀홀
- 글로벌 정책 관리 보기
- 보안 정책 중복 검사, 정책 그룹, 정책 구성 롤백
- 포괄적인 DNS 정책
- 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 세션

플러딩(소스/목적지)에 대한 임계값 설정을 통한 IPv4 및 IPv6 속도 기반 DoS 방어
- 바이패스 인터페이스를 사용한 액티브 바이패스
- 사전 정의된 방지 구성

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

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, 패킷 버리기 또는 차단
- 정기 IP 평판 시그니처 데이터베이스 업그레이드

엔드포인트 식별 및 제어
- 엔드포인트 IP, 엔드포인트 수, 온라인 시간, 오프라인 시간 및 온라인 지속기간 식별 지원
- 10개 운영 시스템 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

애플리케이션 제어
- 이름, 카테고리, 하위 카테고리, 기술 및 위험을 기준으로 3,000개 이상의 애플리케이션 필터링
- 각 애플리케이션 정보에는 설명, 위험 요소, 종속성, 일반적인 사용 포트 및 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, 플리케이션/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

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 탐지 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, 완전 메시, 부챗살, 이중 터널, 투명 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, URL 필터링, 액세스 제어, 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

High Availability
- 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

트윈 모드 HA
- 여러 장치 간 고가용성 모드
- 다중 HA 구축 모드
- 여러 장치 간 구성 및 세션 동기화

사용자 및 장치 식별
- 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 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
- HAS로의 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 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

제품 사양

Specification	SG-6000-X10800
	
FW 처리량(최대)	1 Tbps
IPSec 처리량(최대)	300 Gbps
동시 세션(최대)	4억 8,000만
초당 신규 세션	1,000만
IPS 처리량(최대)	400 Gbps
확장 모듈	SSM-300, QSM-300, IOM-P40-300, IOM-P100-300, SWM-300, SCM-300
최대 인터페이스	최대 11×2 40GE+11×12 10GE 또는 최대 11×4 100GE+11×8 10GE
최대 전력 소비	4400W, N+M(1), 이중 핫 스왑 전력 공급
전력 공급	AC 100-240 V (50/60H z), DC -40 ~ -72V
관리 인터페이스	콘솔 포트 1개, AUX 포트 1개, MGT 관리 1, USB 2.0 포트 1개(단일 SCM-300 모듈)
네트워크 인터페이스	2기가비트 광학 인터페이스(HA 인터페이스 2개, 단일 SCM-300 모듈)
확장 모듈 슬롯	범용 확장 슬롯 12개, 시스템 제어 모듈 확장 슬롯 2개, 스위칭 모듈 확장 슬롯 2개
크기(가로 x 세로 x 높이)	18U 17.3× 31.4× 25 in (440× 797× 635 mm)
무게	253 lb (114.75 KG)
규제 준수 및 인증서	CE, CB, FCC, UL/cUL, ROHS, IEC/EN61000-4-5 전원 서지 보호, ISO 9001:2015, ISO 14001:2015, CVE 호환, IPv6 지원, ICSA 방화벽

모듈 옵션

이름	IOM-P40-300	IOM-P100-300	SSM-300
			
설명	40GE, 10GE 인터페이스 모듈	100GE, 10GE 인터페이스 모듈	보안 서비스 모듈
네트워크 인터페이스	QSFP+ 40GE 인터페이스 2개, SFP+ 10Gb 인터페이스 12개, QSFP+ 및 SFP+ 모듈 없음	QSFP28 100GE 인터페이스 4개, SFP+ 10Gb 인터페이스 8개, QSFP28 및 SFP+ 모듈 없음	해당되지 않음
슬롯	범용 확장 슬롯 1개 사용	범용 확장 슬롯 1개 사용	범용 확장 슬롯 1개 사용
무게	12.45 lb (5.65 kg)	12.67 lb (5.75 kg)	12.56 lb (5.70 kg)

이름	SCM-300	SWM-300	QSM-300
			
설명	서비스 제어 관리 모듈	스위칭 모듈	QoS 서비스 모듈
슬롯	시스템 제어 모듈 확장 슬롯 1개 사용	스위칭 모듈 확장 슬롯 1개 사용	범용 확장 슬롯 1개 사용
무게	7.6 lb (3.45 kg)	7.05 lb (3.20 kg)	12.56 lb (5.70 kg)

달리 명시되지 않는 한 모든 성능, 용량 및 기능 정보는 StoneOS5.5R6 기준입니다. 결과는 StoneOS® 버전 및 구축 환경에 따라 달라질 수 있습니다.

참고: (1) AC 전원 기반의 전부하 운영에는 AC 전원 모듈이 3개 이상, DC 전원 기반의 전부하 운영에는 DC 전원 모듈이 4개 이상 필요합니다.

버전: EX-08.01-DCFW10800-5.5R6-0818-KR-01