AhnLab
NETWORK PLUS

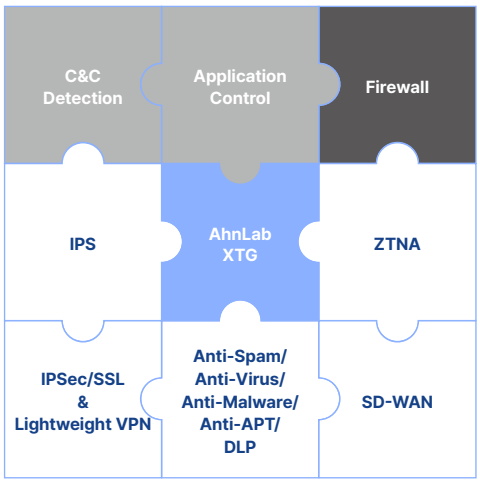
AhnLab XTG

차세대 방화벽 그 이상의 보안

XTG는 '방화벽/VPN 기반 고성능 네트워크 보안'과
'최신 보안 기능'을 겸비한 차세대 네트워크 보안 솔루션입니다.

제품 개요

AhnLab XTG는 AI 기반 차세대 네트워크 보안 솔루션으로, 복잡해지는 네트워크 환경과 고도화되는 사이버 위협에 효과적으로 대응할 수 있는 통합 보안 체계를 제공합니다.
또한 ZTNA(Zero Trust Network Access), Light-weight VPN, SD-WAN, 정책 기반 제어, IPS(Intrusion Prevention System), 애플리케이션 제어, URL 제어, C2 탐지 및 차단, 안티 스팸, 디도스 완화, DLP(Data Loss Prevention) 등 확장된 네트워크 보안 기능을 제공하여 더욱 안전한 비즈니스 환경을 구현합니다.



· 차별화된 차세대 네트워크 보안 플랫폼
- ZTNA 기반 제로트러스트 구축
- 지능적 트래픽 경로 최적화
- 사용자 및 디바이스 기반 정책 설정/제어
- 암호화된 트래픽 탐지
- 글로벌/국내 애플리케이션에 대한 심층 방어 기능

· 독보적인 위협 탐지 · 차단 기술
- AI기반 실시간 위협 탐지 및 차단
- 보안 위협 탐지에 특화된 다계층 멀티 엔진 구조
- 위협 인텔리전스 기반 차별화된 위협 탐지
- 인하우스 위협 분석 조직/인프라 보유

· 대용량 방화벽 처리 성능 보장
- 고도화된(Advanced) 하드웨어 플랫폼
- 고성능 멀티 코어 분배 기술

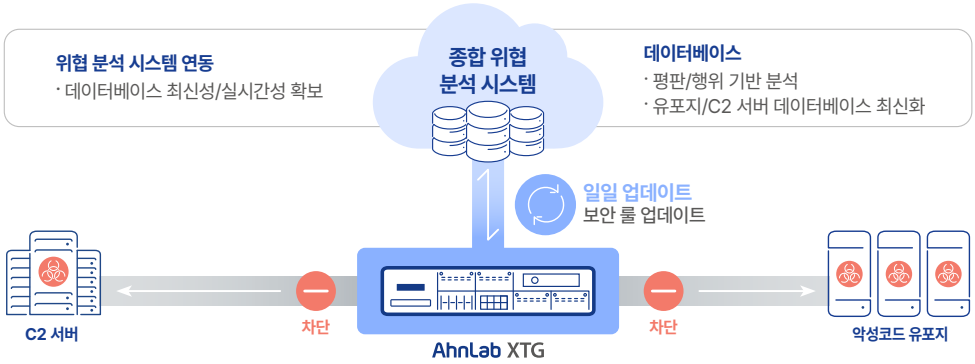
· 오랜 노하우가 축적된 사용자 인터페이스
- 정책 설정 · 관리 및 Seamless Flow 제공
- 드래그 앤 드롭(Drag & Drop) 방식의 유연한 인터페이스 제공

뛰어난 대용량 트래픽 처리의 **고성능 방화벽**	최신 활용 사례 기반 **차별화된 차세대 보안**
시장 요구사항이 철저히 반영된 **사용자 인터페이스**	독보적인 **위협 탐지 및 대응 능력**

차세대 방화벽 기능

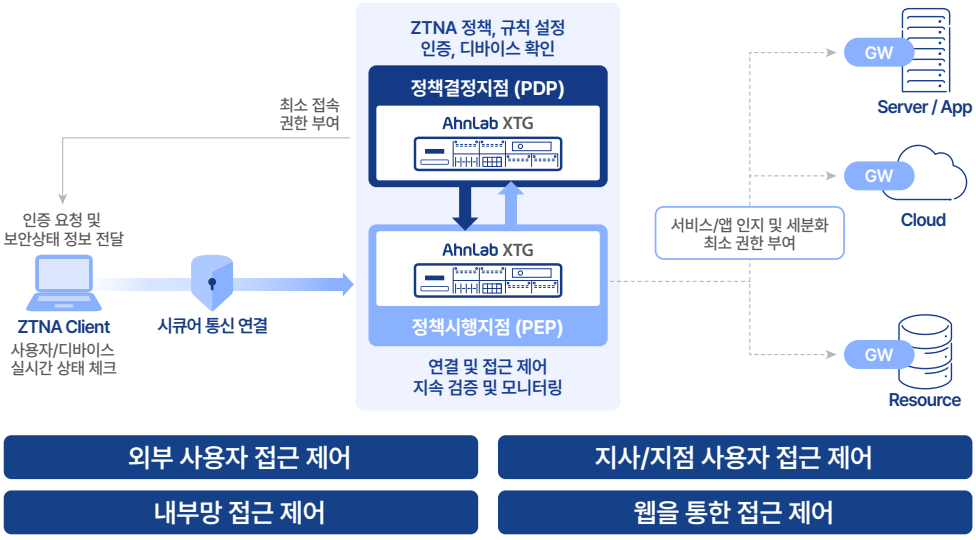
차세대 방화벽

인바운드 및 아웃바운드 트래픽을 사용자, 디바이스, IP, URL 등 다양한 속성에 따라 정교하게 허용 또는 차단합니다.
보안 관점에서 위험도가 높은 IP나 웹사이트를 실시간으로 차단하고, 외부에서 내부 중요 자산으로의 IP, 포트(Port) 접근을 제어해 랜섬웨어 등 악성코드 감염을 예방합니다.
자체 보유한 위협 분석 시스템과 C2 블랙리스트 데이터베이스를 기반으로 C2 서버 접속을 탐지 및 차단해 사이버 위협으로부터 비즈니스 환경을 보호합니다.



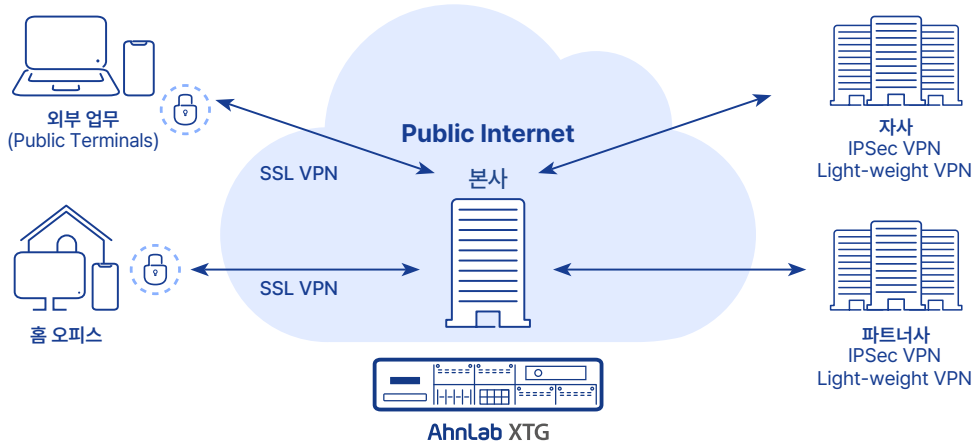
ZTNA 접근 제어

AhnLab XTG ZTNA는 네트워크 내부와 외부를 불문하고 모든 사용자와 디바이스의 신원을 철저히 검증하여 최소 권한 접근을 보장합니다.



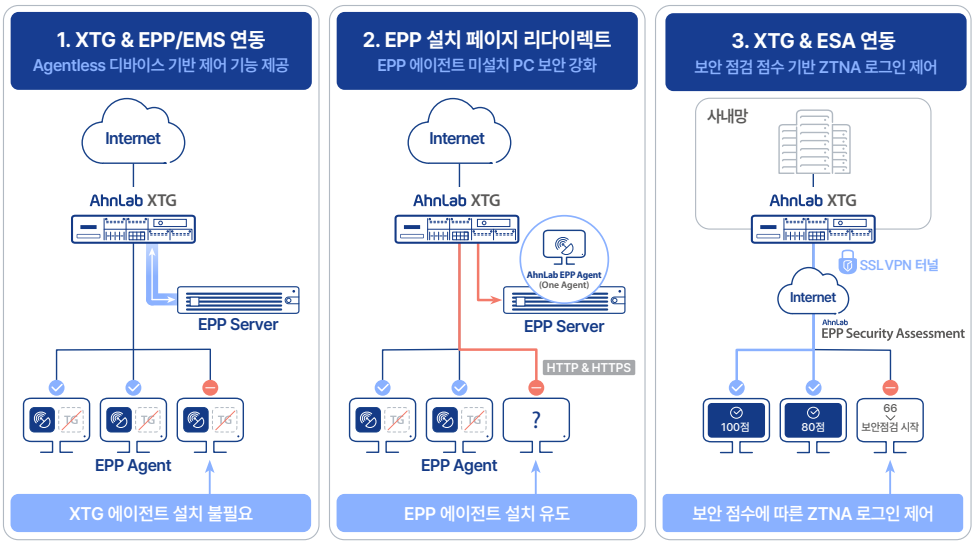
VPN – 원격 접근

IPSec VPN, SSL VPN, 그리고 Light-weight VPN을 동시 지원해 원격 접속, 본사-지사 접속의 보안을 강화합니다.
Windows, Mac, Linux, Android, iOS 등 다양한 OS를 지원하며 모바일 전용 SSL VPN을 지원합니다.
HA, 멀티라인 로드밸런싱 등의 기술을 통해 VPN 안정성 및 가용성을 극대화합니다.



EPP 연동

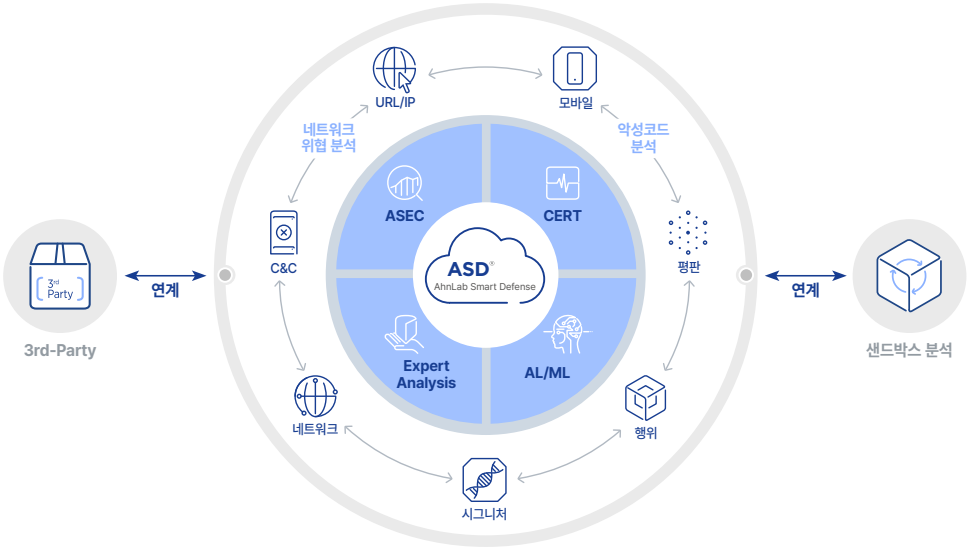
AhnLab XTG와 AhnLab EPP를 연동해 안전한 디바이스만 VPN 접속을 허용합니다.
EPP 연동으로 XTG 에이전트 설치 없이 디바이스 기반 제어를 구현합니다.
XTG를 통해 EPP 에이전트 설치를 유도합니다. (HTTP/HTTPS)
ESA 보안 점검 점수를 기반으로 XTG의 SSL VPN과 로그인을 제어합니다.



안랩 보안 인프라

안랩의 기술력과 노하우가 축적된 AhnLab XTG

안랩 제품 및 서비스의 기반인 AhnLab Smart Defense (ASD)는 URL/IP, C2, 모바일, 네트워크, 행위, 시그니처, 평판 정보 등을 종합 분석해 신종 위협 탐지와 대응 역량을 강화합니다. AhnLab XTG는 이러한 안랩의 기반 기술과 인프라를 바탕으로 최신 시그니처, 취약점, 평판 정보, C2 정보를 적용해 고객을 최신 네트워크 위협으로부터 보호합니다.



제품과 서비스의 근간을 이루는 기술력

안랩은 위협 분석과 침해 대응을 통해 30여 년간 축적한 방대한 보안 데이터를 기반으로 AI 보안 플랫폼 AhnLab AI PLUS를 운영하고 있습니다. 차별화된 보안 데이터를 학습한 안랩의 AI는 위협 탐지와 대응 역량을 고도화하고, 보안 운영의 생산성 혁신을 지원합니다.

상세기능

카테고리	기능	설명
네트워크	인터페이스	· Bridge/Aggregation/VLAN/VXLAN/VRF 지원
	운영모드	· Router/Bridge 모드 지원
	라우팅 프로토콜	· Static/Dynamic/Multicasting 프로토콜 및 라우팅 시뮬레이터 지원
	DHCP	· Client/Server/Relay 지원
	SD-WAN	· 애플리케이션/서비스 경로 최적화, 네트워크 품질 모니터링, 로드밸런싱 등 지원
차세대 방화벽	High Availability (HA)	· Active-Standby, Active-Active 지원
	동기화	· 관리자 설정, 로그 설정, 정책 동기화 지원
	동적 정보 동기화	· 사용자 및 FQDN IP 수집 정보를 다른 XTG 장비에 동기화 지원
	객체	· 클라우드 연동 기능 지원 · 국가 객체를 제공해 국가 기반 방화벽 정책 수립 지원
	QoS	· 정책 별 최소 대역폭 보장 및 최대 대역폭 제한 설정 지원
	접근 차단 (Blacklist)	· IPv4/IPv6 차단 관리 · L3/L4 프로토콜 이상 검사 지원 · 접근 차단 파일 내 IP 중복 검사 도구 지원
	정책 예외 (Whitelist)	· IPv4/IPv6 예외 정책 관리 기능 지원
	중복 객체 검사	· 중복 객체 및 참조 객체 검사 지원 · 선택된 정책별 중복 여부 검사
	정책 검사	· 중복 정책 필터링, 가상 패킷 정책 유효성 검사 지원
	NAT	· Static/Dynamic/Policy based NAT 등 지원
	사용자 인증	· 써드 파티 표준 인증 서버 연동 인증 지원 (RADIUS/LDAP/AD/TACACS+/MS-SQL 등)
	정책 설정 및 제어	· IP/MAC, 사용자, 디바이스 설정 및 제어 지원
	ZTNA	· 사용자 및 디바이스 신원을 기반으로 애플리케이션 및 리소스 별 접근 제어 지원 · Agent 및 Agentless ZTNA 지원
	가상 패킷 검색	· 가상 패킷을 통한 NFGW 정책의 전체 패킷 처리 시뮬레이터 지원
IPSec VPN	구성	· Hub & Spoke, Mesh
	DMVPN	· Hub & Spoke 구성에서 허브 설정 변경 없이 동적으로 Hub-Spoke 간 IPSec VPN 터널 생성 · Spoke 간 통신 시 동적으로 터널 생성 지원
	알고리즘	· 다양한 암호화 알고리즘 지원 (AES/SEED/ARIA/LEA/HIGHT 등)
	HA	· 본사 VPN 이중화 (Active-Standby, Active-Active) 지원
	로드밸런싱	· 다양한 인터넷 멀티 회선 로드밸런싱 기능 지원
	장애 복구	· DPD 검사 및 DR 연결 지원
SSL VPN	지원 환경	· Windows, Mac, Linux, Android, iOS 등 지원
	사용자 인증	· 써드 파티 표준 인증 서버 연동 인증 지원 (RADIUS/LDAP/AD/DBMS/OTP/FIDO/SMS 등)
	알고리즘	· 다양한 암호화 알고리즘 지원 (AES/SEED/ARIA/LEA/HIGHT 등)
	엔드포인트 연계 보안	· 엔드포인트 보안 연동 - 접속 PC 사전/사후 보안 기능 지원
	HA	· Active-Standby, Active-Active 구성 지원
	지원 기기	· 모바일 기기 (핸드폰/패드) 및 임베디드 단말 (라우터)
Light-weight VPN	HA	· 본사 VPN 이중화 (Active-Standby, Active-Active) 지원
	구성	· Gateway-to-Gateway
	장비 차단 목록	· 중앙 장비에서 특정 지점 장비 차단 목록 지원

카테고리	기능	설명
가상시스템	지원 방식	· MAC VLAN 방식을 통한 최대 논리적 가상화 지원
	HA	· 가상 시스템 HA 지원
	통신	· Veth 인터페이스를 사용하여 가상시스템 간 통신 지원
	관리	· 가상 시스템을 통한 프라이빗 클라우드, SDN, NFV 관리 지원
IPS	시그니처	· 약 10,000개 이상의 시그니처 지원
	시그니처 업데이트	· 정기 시그니처 패턴 자동 업데이트 지원
	탐지/차단	· 시그니처/Anomaly/취약점/악성코드 기반 탐지 및 차단 지원
	시그니처 관리	· 사용자 정의 패턴/Snort Rule(PCRE 패턴) 관리 기능 지원
디도스 방어	공격 차단	· UDP/ICMP/TCP Flooding, Spoofed TCP 공격, HTTP 취약점 공격 차단 지원
어플리케이션 제어	애플리케이션 지원	· 약 3,000여개 애플리케이션 및 사용자 정의 애플리케이션에 대한 위협 탐지 및 차단 지원
	제어	· 애플리케이션 사용자 접속과 로그인, 세부 Function 제어, Unknown 애플리케이션 제어 지원
C2 탐지/차단	탐지	· 클라우드 기반 C2 서버 접속, Unknown 악성 의심파일, PUP 내부 유입 탐지
	차단	· 자체 보유 Blacklist 데이터베이스 기반 C2 서버 접속 차단
안티 멀웨어	엔진	· 자체 엔진 지원
	탐지/차단	· Stream-based 안티멀웨어 엔진을 기반으로 멀웨어 고속 탐지/차단
	시그니처 업데이트	· 최신 시그니처 대응을 위해 1일 2회 시그니처 업데이트 지원
	멀웨어 검사	· HTTP/SMTP/POP3/FTP 등 다양한 프로토콜 및 압축파일에 대한 멀웨어 검사
안티 스팸	엔진	· 국제적으로 공인된 스팸 엔진 지원
	필터링	· RBL (Real-time Blacklist)와 사용자 정의 키워드 기반 필터링
	차단	· 특정 시간 당 일정 개수 이상 메일 혹은 특정 메일 계정 차단
DLP	제어	· 내부 정보 외부 유출 및 파일 유형과 콘텐츠 별 제어
	탐치/차단	· 개인정보와 키워드에 대한 패턴 탐지 및 차단
위협 탐지 필터	데이터베이스	· 자체 악성코드 유포 사이트 DB, 방송통신심의위원회 유해사이트 DB 및 Global Categorized URL DB 지원
자사 제품 연동	연동 제품	· V3, EPP, MDS, AIPS, DPX, ASTx, ESA, TMS, AIPS 등 연동 지원
기타	SSL Inspection	· 암호화된 트래픽 검사
	모니터링/로그	· 로그 스토리지: 내장형 HDD/로그 저장
		· 대시보드: 위젯 방식의 대시보드 및 연관 분석
		· 콘텐츠: 트래픽 통합 로그 및 Custom 보고서
	차단	· GeoIP: 특정 국가 및 대륙별 차단
	관리	· 권한: 다단계 관리자 권한
		· 접속: 웹 기반 HTTPS 접속
		· 연동: Open API

제품사양

중소기업용

카테고리	40	50	70	100
Certification				
CC인증	EAL4FW+VPN(국내)			
IPv6인증	IPv6ReadyLogoPhase-2(Router)			
전자파인증	KC			
Physical				
Processor	2Core/1.8Ghz	4Core/1.3Ghz	4Core/2.4Ghz	8Core/2.4Ghz
Memory	8GB	8GB	8GB	8GB
System Storage	eMMC9.6GB	eMMC9.6GB	eMMC9.6GB	M.2SSD512GB
Log Storage	-	-	-	HDD2TB
Form Factor	Desktop	19"RackMount/1U	19"RackMount/1U	19"RackMount/1U
Dimension (WxHxD mm)	220×44×194.5	438×44×194	438×44×194	430×44×340
Power (External Power Supply)	40WSingle	65WSingle	65WSingle	100WSingle
Operating Temperature	0~40°C			
Storage Temperature	-20~70°C			
Interface				
Slot	-	-	-	1
10/100/1000 Base-T	8	8	8	기본6 / 최대10
1G Base-X	-	-	-	기본4 / 최대8
Bypass	지원			
SystemPerformance				
Max Concurrent Sessions (CC)	1,000,000	1,500,000	2,000,000	3,500,000
Connection Per Second (CPS)	35,000	50,000	50,000	200,000
Firewall Throughput (UDP)	4G	6G	8G	12G
Firewall Throughput (UDP 64B)	1G	1.5G	2G	3G
VPN Throughput	1G	1.2G	1.4G	1.9G
VPN 터널 수	2,500	5,000	5,000	20,000
ZTNA 최대 동시 접속 가능 디바이스 수	50	100	200	300
SSL VPN 동시 접속 가능 세션 수	500	1,000	1,000	1,000

중견기업용

카테고리	300	500	1000
Certification			
CC인증	EAL4 FW+VPN (국내)		
IPv6인증	IPv6 Ready Logo Phase-2 (Router)		
전자파인증	KC		
Physical			
Processor	6 Core/3.7Ghz (1each)	8 Core/3.8Ghz (1each)	12 Core/3.7Ghz (1each)
Memory	8GB	16GB	16GB
System Storage	M.2 SSD 512GB		
Log Storage	HDD 2TB		
Form Factor	19" Rack Mount/1U		
Dimension (WxHxD mm)	438×44×525		
Power (External Power Supply)	350W Single	350W Redundant	350W Redundant
Operating Temperature	0~40°C		
Storage Temperature	-20~70°C		
Interface			
Slot	4	4	4
10/100/1000 Base-T	기본8 / 최대32	기본8 / 최대32	기본8 / 최대32
1G Base-X	기본8 / 최대32	기본8 / 최대32	기본8 / 최대32
10G Base-X	-	기본0 / 최대8	기본0 / 최대8
40G Base-X	-	-	-
100G Base-X	-	-	-
Bypass	지원		
SystemPerformance			
Max Concurrent Sessions (CC)	5,000,000	8,000,000	10,000,000
Connection Per Second (CPS)	300,000	500,000	600,000
Firewall Throughput (UDP)	20G	40G	60G
Firewall Throughput (UDP 64B)	6G	8G	8G
VPN Throughput	8G	10G	12G
VPN 터널 수	30,000	40,000	40,000
ZTNA 최대 동시 접속 가능 디바이스 수	500	1,000	2,000
SSL VPN 동시 접속 가능 세션 수	2,000	3,000	4,000

대기업 및 데이터센터용

카테고리	2000	5000	10000	20000
Certification				
CC인증	EAL4FW+VPN(국내)			
IPv6인증	IPv6ReadyLogoPhase-2(Router)			
전자파인증	KC			
Physical				
Processor	8Core/3.2Ghz (1each)	12Core/2.4Ghz (2each)	16Core/2.8Ghz (2each)	32Core/2.8Ghz (2each)
Memory	32GB	64GB	64GB	256GB
System Storage	M.2SSD512GB			
Log Storage	SSD2TB			
Form Factor	19"RackMount/2U			
Dimension (WxHxD mm)	438×88×602			
Power (External Power Supply)	550WRedundant	550WRedundant	1300WRedundant	1300WRedundant
Operating Temperature	0~40°C			
Storage Temperature	-20~70°C			
Interface				
Slot	4	8	8	8
10/100/1000 Base-T	기본8 / 최대32	기본8 / 최대64	기본8 / 최대64	기본8 / 최대64
1G Base-X	기본8 / 최대32	기본8 / 최대64	기본8 / 최대64	기본8 / 최대64
10G Base-X	기본0 / 최대12	기본0 / 최대32	기본0 / 최대32	기본0 / 최대32
40G Base-X	-	기본0 / 최대8	기본0 / 최대12	기본0 / 최대16
100G Base-X	-	-	기본0 / 최대2	기본0 / 최대4
Bypass	지원			
SystemPerformance				
Max Concurrent Sessions (CC)	20,000,000	30,000,000	40,000,000	60,000,000
Connection Per Second (CPS)	850,000	1,000,000	1,300,000	1,500,000
Firewall Throughput (UDP)	100G	180G	240G	320G
Firewall Throughput (UDP 64B)	10G	25G	35G	60G
VPN Throughput	13G	15G	19G	38G
VPN 터널 수	40,000	50,000	60,000	100,000
ZTNA 최대 동시 접속 가능 디바이스 수	2,500	5,000	7,500	10,000
SSL VPN 동시 접속 가능 세션 수	5,000	10,000	15,000	20,000

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901

AhnLab