AhnLab

대기업과 데이터센터를 위한 차세대 방화벽

AhnLab XTG 2000, 5000, 10000, 20000

Why AhnLab XTG

초대용량 트래픽을 수용하는대기업 및 데이터센터 요구사항 맞춰 성능 극대화에 중점을 두고 설계된 **고성능 방화벽**

IPSec VPN과 SSL VPN 동시지원을 통해 본사-지사 및 기업-파트너 간 원격 접속을 위한 **안전한 VPN 네트워크 접속 환경 조성**

하나의 장비로 최대 255개 장비 구축의 효과를 내는 **가상 시스템 기능 제공**

안랩의 다양한 엔드포인트 보안 솔루션 연동을 통한 **엔드포인트-네트워크 통합 보안 구현**

ZTNA 기반의 안전한 접근 제어를 통해 **언제 어디서나 강력한 보안 제공**

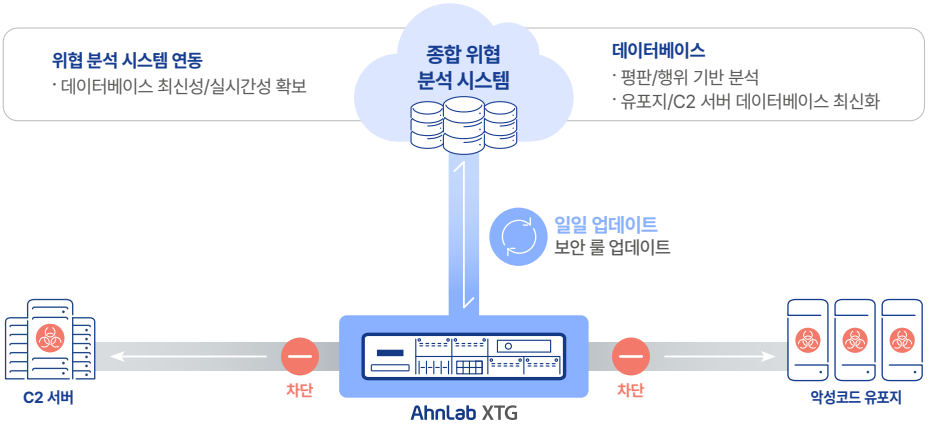
강력한 고성능 차세대 방화벽

대기업과 데이터센터는 초대용량 트래픽을 수용하며, 본사-지사, 기업-파트너 등 다양한 접속 사례에 대응하는 차세대 방화벽을 갖춰야 합니다. 이에 대해, AhnLab XTG는 탁월한 성능을 갖춘 4가지 하이엔드 라인업 (2000, 5000, 10000, 20000)을 제공합니다. AhnLab XTG는 강력한 방화벽 및 VPN 기능 뿐만 아니라, 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.

활용 사례 (Use Case)

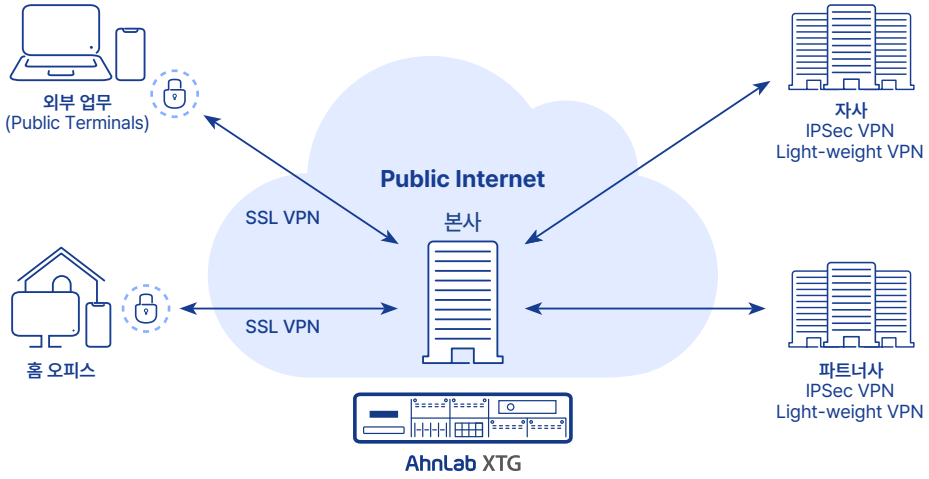
차세대 방화벽

- 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.



VPN – 원격 접근

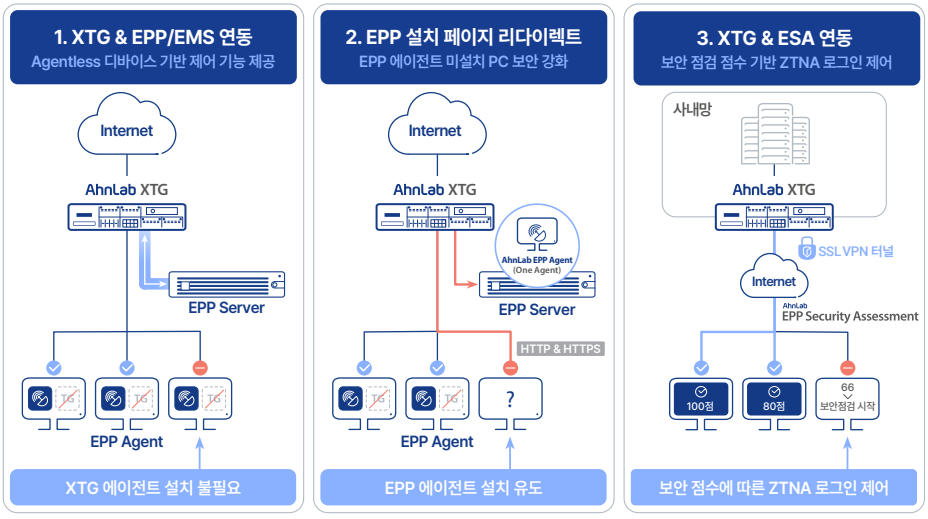
- IPSec VPN, SSL VPN, 그리고 Light-weight VPN을 동시 지원해 원격 접속, 본사-지사 접속의 보안을 강화합니다.
- Windows, Mac, Linux, Android, iOS 등 다양한 OS를 지원합니다.
- 모바일 전용 SSL VPN을 지원합니다.
- HA, 멀티라인 로드밸런싱 등의 기술을 통해 VPN 안정성 및 가용성을 극대화합니다.



EPP 연동

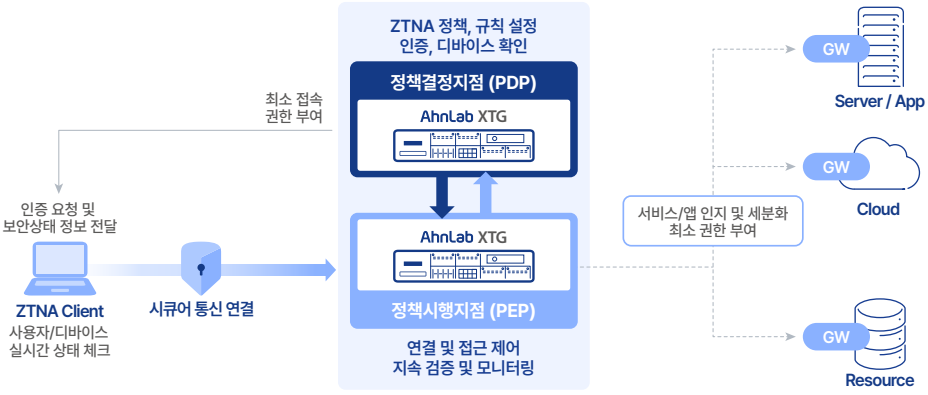
AhnLab XTG와 AhnLab EPP를 연동해 안전한 디바이스만 ZTNA 접속을 허용합니다.

- EPP 연동으로 XTG 에이전트 설치 없이 디바이스 기반 제어를 구현합니다.
- XTG를 통해 EPP 에이전트 설치를 유도합니다. (HTTP/HTTPS)
- ESA 보안 점검 점수를 기반으로 XTG의 ZTNA와 로그인을 제어합니다.



ZTNA 접근 제어

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



외부 사용자 접근 제어

SSL VPN 접속 시, 사용자 신원 확인 및 디바이스 상태 점검을 통해 외부 디바이스 내부 리소스 접근 제어 지원

지사/지점 사용자 접근 제어

IPSec 터널링을 통해 본사에 접속하는 지사/지점 사용자 신원 확인 및 디바이스 상태 체크를 통한 접근 제어

내부망 접근 제어

사용자 인증 및 디바이스 상태 체크를 통해 내부망에서 내부 리소스에 접속하는 단말에 대한 접근 제어 지원

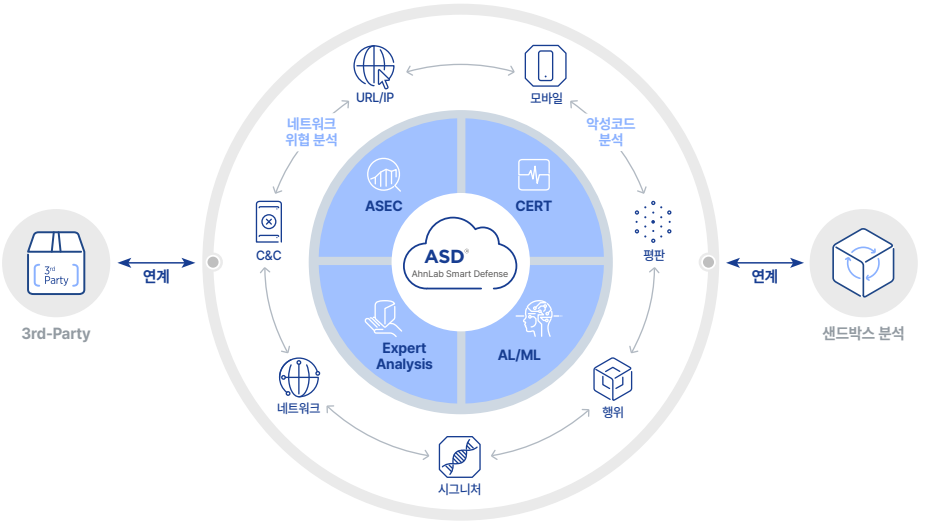
웹을 통한 접근 제어

Agentless 환경에서 HTTPS를 기반으로 암호화 채널을 생성하여 웹을 통한 접속에 대한 접근 제어 지원

백엔드 인프라

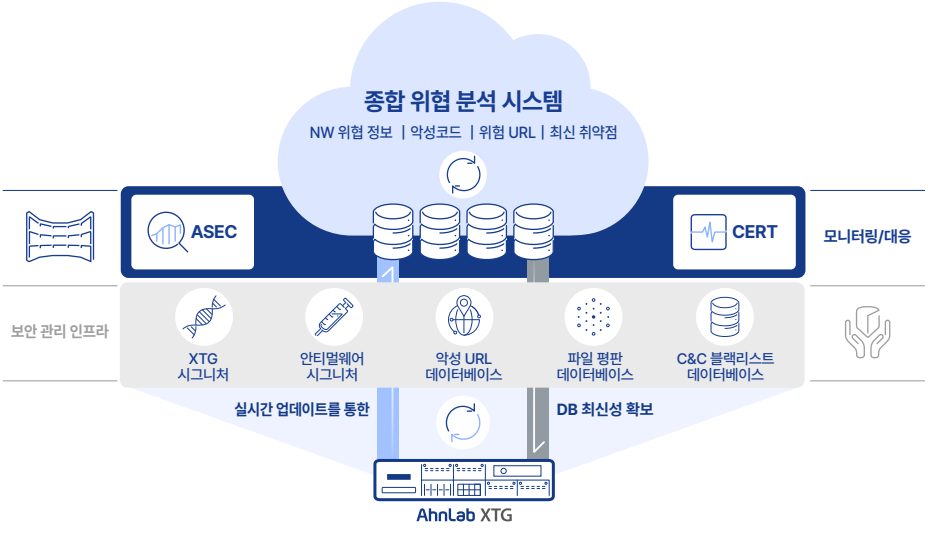
제품과 서비스의 근간을 이루는 기술력

안랩 제품 및 서비스의 근간에는 수 십년 간 축적된 기술력과 노하우가 반영된 클라우드 기반 엔진 'AhnLab Smart Defense (ASD)'가 있습니다. ASD 엔진은 URL/IP, C2, 모바일, 네트워크, 행위, 시그니처, 평판 정보에 대한 분석 기술을 복합적으로 적용해 신종 위협에 대한 다차원적인 탐지 및 대응을 구현합니다. 여기에, AI와 머신러닝 등의 기술과 위협 분석 전문가들의 역량이 더해져 차별화된 인프라를 구성합니다. 이러한 기반 기술은 안랩의 모든 제품과 서비스에 적용되어 전체적인 위협 탐지, 분석 및 대응 역량을 강화합니다.



안랩의 기술력과 노하우가 축적된 AhnLab XTG

이처럼 위협 탐지, 분석 및 대응에 특화된 기술력과 인프라는 AhnLab XTG에도 적용되어 있습니다. AhnLab XTG는 자사 인프라를 기반으로 최신 시그니처, 취약점, 평판 정보, C2 정보 등을 적용해 고객들을 최신 네트워크 위협으로부터 안전하게 보호합니다.



주요 기능

차세대 방화벽

AhnLab XTG는 외부 위협으로부터 내부 네트워크를 보호하는 차세대 방화벽의 본질에 충실합니다. 사용자와 디바이스 기반 정책 생성뿐만 아니라 정책의 차단, 허용 및 거절 여부도 선택할 수 있습니다. 또한, 클라우드 연동 객체 및 국가 기반 객체를 제공하여 가시성 높은 정책 제어를 지원하며, 사용자 객체를 활용한 SSL VPN 사용자 접근 제어도 가능합니다. 생성된 정책에 대해 다양한 방식으로 유효성을 검증할 수 있으며, 중복된 객체와 정책에 대한 필터링도 가능합니다. L4 스위치 없이도 HA(High Availability) 구성이 가능하고, 정책 및 세션 동기화를 통해 장비에 장애가 발생한 경우에도 중단 없이 안정적인 서비스를 제공할 수 있도록 합니다.

IPSec VPN

표준 프로토콜을 지원하며 다양한 암호화 및 해시 알고리즘을 바탕으로 IPSec VPN을 제공합니다. 고성능 HA(High Availability) 기술을 기반으로 안정적인 VPN 서비스를 제공하며, 본사와 지사 모두에 이중화 구성을 지원합니다. 또한, IPS 연동을 통해 VPN 터널을 통한 악성코드 유포 및 확산을 방지합니다. 인터페이스 수만큼 멀티라인 로드밸런싱을 지원해 트래픽을 효율적으로 분배하고 지사 대역폭을 확장해 VPN 네트워크 가용성을 극대화합니다. 또한, Dynamic Access 기능을 제공하여 Hub & Spoke 구성에서 허브의 설정 변경 없이 동적으로 Hub-Spoke 간 IPSec VPN 터널 생성이 가능합니다. Spoke 간 통신 시에도 동적으로 터널을 생성해 탁월한 관리 편의성을 제공합니다.

SSL VPN

SSL VPN은 SSL 표준 프로토콜을 기반으로 Full Tunnel 방식의 Gateway-to-Client 접속을 지원합니다. 스마트폰, 태블릿 등 모바일 기기와 임베디드 장치에서 SSL VPN 연결이 가능하며, 3rd Party 표준 인증 서버와 연동해 다양한 사용자 인증 방식(ID/PW + 인증서 기반 2차 인증 및 FIDO 인증)을 제공합니다. 또한, Windows, Mac, Linux 등 여러 클라이언트 OS를 지원하며, SSL VPN 사용자 및 SSL VPN 복호화 트래픽에 대한 접근 제어를 제공하여 보안성을 강화합니다. 추가로, Active-Active 구성을 통해 접속 장비에 장애가 발생하더라도 VPN 재연결 없이 지속적으로 서비스를 이용할 수 있습니다.

Light-weight VPN

AhnLab XTG의 Light-weight VPN(LW VPN)은 WireGuard 프로토콜 기반 경량 VPN입니다. Gateway to Gateway 방식을 지원하며, 기존 VPN 대비 빠르고 효율적인 연결을 제공합니다. 최신 암호화 알고리즘을 적용해 보안성을 강화하면서도, 가벼운 프로토콜 구조로 낮은 리소스 사용과 빠른 속도를 보장합니다. 설정이 간단해 키 페어만으로 손쉽게 VPN을 구축할 수 있으며, IP 변경과 같은 네트워크 변경 시에도 빠르게 재연결되어 안정적인 접속이 가능합니다. 또한 UDP 기반 전송 기법을 사용해 방화벽과 NAT 환경에서도 원활하게 동작합니다. 복잡한 설정 없이 고성능 VPN을 구현할 수 있어, 기업이나 다양한 환경에서도 효율적인 원격 접속 솔루션으로 활용할 수 있습니다.

SD-WAN

지능형 트래픽 제어와 보안을 결합해 네트워크를 최적화할 수 있는 SD-WAN(Software-Defined WAN) 기능을 제공합니다. 네트워크 품질을 실시간으로 확인하여 자동으로 최상의 품질을 가진 회선으로 패킷을 전송하고, 애플리케이션 별 최적의 경로를 선택해 성능을 극대화합니다. 암호화된 터널링과 방화벽 기능을 결합해 보안성을 유지하면서 안전한 데이터 전송을 보장합니다. 클라우드 및 온프레미스 환경을 모두 지원하여 유연한 네트워크 구성이 가능하며, 지점 간 안정적인 연결과 성능 보장이 필요한 기업에 최적화된 솔루션을 제공합니다.

ZTNA

AhnLab XTG의 ZTNA(Zero Trust Network Access)는 제로 트러스트(Zero Trust)의 기본 원칙인 '항시 검증/최소 권한 접근'을 기반으로 안전한 네트워크 접근을 보장합니다. 사용자와 기기의 신원과 보안 상태를 지속적으로 확인하여 검증된 사용자만 애플리케이션 및 네트워크 리소스에 접근할 수 있도록 합니다. IP 기반 접근 통제를 벗어나 애플리케이션 단위의 세분화된 보안 정책을 적용할 수 있어, 보다 안전한 원격 접속이 가능합니다. 또한, ZTNA SWG 설정을 통해 터널링 구성이 어려운 환경에서 웹브라우저를 통한 원격 접속 환경도 구성할 수 있습니다. ZTNA를 통해 보다 강력하고 유연한 보안 접근 제어를 제공하여 기업의 보안 수준을 높이는데 기여합니다.

IPS

네트워크에 인입되는 다양한 유해 트래픽을 시그니처 및 행위 규칙을 기반으로 탐지하고 차단하는 IPS 기능을 제공합니다. 네트워크, OS, 애플리케이션의 취약점을 악용한 해킹 공격에 대응하기 위해 10,000개 이상의 취약점 공격 탐지 및 제어 시그니처를 제공합니다. 또한, 최신 및 zero-day 공격에 신속하게 대응할 수 있도록 일일 정기 시그니처 패턴 자동 업데이트를 지원합니다. 이를 통해 프로토콜 및 애플리케이션 취약점을 악용한 네트워크 침입을 효과적으로 탐지해 차단할 수 있습니다.

애플리케이션 제어

네트워크 내 다양한 애플리케이션 트래픽을 분석 및 제어하는 애플리케이션 제어 기능을 제공합니다. 이를 통해, 3천 개 이상의 애플리케이션에 대한 실시간 분석, 차단, 허용 및 세부 행위 제어가 가능합니다. 또한, 알려지지 않은 애플리케이션도 식별 및 제어할 수 있습니다. 사용자 정의 규칙을 추가해 네트워크 환경에 맞게 관리할 수 있고, 애플리케이션 매핑 기능을 활용하면 특정 트래픽을 더 손쉽게 제어해 보안을 강화할 수 있습니다.

DLP

AhnLab XTG는 데이터 유출 방지(DLP) 엔진을 활용해 개인정보, 내부 문서 등 중요정보가 외부로 유출되지 않도록 첨부파일 유형 분류 및 문서 내 콘텐츠 검사(동적 콘텐츠 분석)를 수행합니다. 이를 통해, 내부 자산 유출 방지는 물론 콘텐츠 가시성까지 확보할 수 있습니다.

디도스 공격 완화

자체 개발한 엔진을 기반으로 비정상 트래픽이나 과도한 서비스 요청으로 인해 발생하는 DoS 및 DDoS 공격을 방어합니다. TCP 및 HTTP 인증 방식을 사용하여 정상 트래픽과 비정상 디도스 트래픽을 구분하며, IP 스푸핑을 이용한 비정상 트래픽 기반 디도스 공격도 효과적으로 차단합니다.

가상 시스템

가상 시스템 기능은 물리적인 방화벽 내에서 별도 관리할 수 있는 독립된 가상 인스턴스를 생성해 사용할 수 있도록 합니다. 관리자는 각 가상 시스템의 정책과 객체를 관리할 수 있고, AhnLab XTG가 제공하는 모든 기능을 최대 255개 인스턴스로 세분화해 사용 및 관리할 수 있습니다.

Anti-Malware

전 세계적으로 검증된 안랩의 안티멀웨어 엔진을 기반으로 멀웨어 필터링 기능을 제공합니다. 자체 개발한 스트림 기반 안티멀웨어 엔진을 통해 사용자는 이메일, 웹사이트, FTP 전송 파일의 악성코드 감염 여부를 신속하게 확인할 수 있습니다.

Anti-Spam

AhnLab XTG는 국제적으로 공인된 강력한 스팸 엔진을 적용해 SMTP/POP3를 통한 알려지지 않은 멀웨어를 사전에 차단합니다. 사용자는 SMTP/POP3 트래픽에서 스팸 메일을 탐지하는 조건과 처리 방법을 설정하고, 안티 스팸 기능을 활용해 발신 IP와 이메일 주소를 관리할 수 있습니다. 또한, 이메일 제목이나 본문에 특정 키워드가 포함되어 있는지 여부를 탐지하는 키워드 관리 기능도 제공합니다.

디바이스 제어

AhnLab EPP 등 엔드포인트 디바이스 연동 서버와 통신해 다수 단말 정보를 실시간으로 확인할 수 있습니다. 수집된 정보는 디바이스 제어를 위해 AhnLab EPP Security Assessment(ESA) 에이전트 속성값과 연계하여 보다 정교한 점검 및 제어가 가능합니다. 이 밖에, 단말 OS 버전, 보안 패치 적용 여부, 필수 소프트웨어 설치 상태, 취약점 점검 결과 등을 기반으로 네트워크 접근까지 제어할 수 있습니다.

기능 구성

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
	DA (Dynamic Access)	· 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
애플리케이션 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

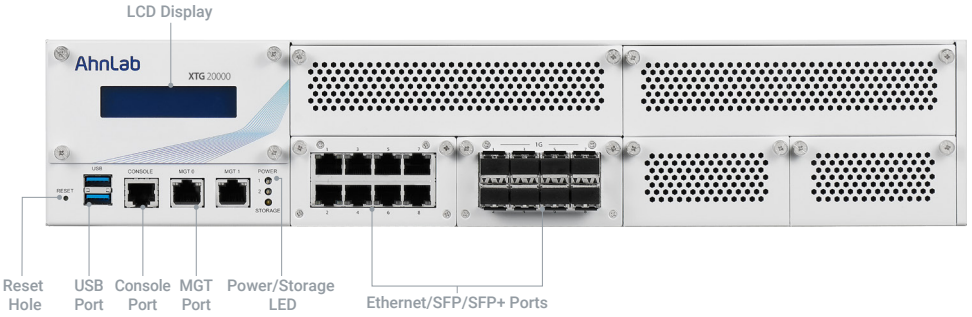
시스템 성능 및 하드웨어 사양

카테고리	2000	5000	10000	20000
Certification				
IPv6 인증	IPv6 Ready Logo Phase-2 (Router)			
전자파 인증	KC			
Physical				
Processor	8 Core/3.2Ghz (1 each)	12 Core/2.4Ghz (2 each)	16 Core/2.8Ghz (2 each)	32 Core/2.8Ghz (2 each)
Memory	32GB	64GB	64GB	256GB
System Storage	M.2 SSD 512GB			
Log Storage	SSD 2TB			
Form Factor	19" Rack Mount/2U			
Dimension (WxHxD mm)	438×88×602			
Power (External Power Supply)	550W Redundant	550W Redundant	1300W Redundant	1300W Redundant
Operating Temperature	0~40°C			
Storage Temperature	-20~70°C			
Interface				
Slot	4	8	8	8
10/100/1000 Base-T	기본 8 / 최대 32	기본 8 / 최대 48	기본 8 / 최대 48	기본 8 / 최대 48
1G Base-X	기본 8 / 최대 32	기본 8 / 최대 48	기본 8 / 최대 48	기본 8 / 최대 48
10G Base-X	기본 0 / 최대 12	기본 4 / 최대 28	기본 4 / 최대 28	기본 4 / 최대 28
40G Base-X	-	기본 0 / 최대 8	기본 0 / 최대 12	기본 0 / 최대 12
100G Base-X	-	-	기본 0 / 최대 2	기본 0 / 최대 4
Bypass	지원			
System Performance				
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
IPS Throughput (최대 성능)	20G	30G	50G	70G
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

인터페이스

2000, 5000, 10000, 20000

전면 패널



#	카테고리	설명
1	LCD Display	LCD 화면을 이용하여 현재 상태를 표시합니다. 장비가 부팅되면 제품명/저작권 화면에서 PSU 화면까지 상태 정보를 갱신하여 표시해 줍니다.
2	Reset Hole	핀으로 해당 부분을 누르면 장비를 다시 시작합니다.
3	USB Port	USB 포트는 비활성화되어 있습니다.
4	Console Port	장비와 관리자용 컴퓨터를 시리얼 케이블로 연결하는 포트입니다. 관리자는 연결한 다음, CLI 명령어를 사용할 수 있습니다.
5	MGT Port	장비의 관리자 웹 화면 접속을 위해 제공하는 포트입니다.
6	Status LED	전원, Storage 상태를 표시합니다.
7	Ethernet/SFP Port	**이더넷(RJ45) 포트:** CAT5, CAT 5e 또는 CAT 6 케이블을 사용할 수 있으며, 10/100/1000Mbps 접속을 지원합니다. **광(SFP/SFP+) 포트:** 광 타입의 기가 비트 접속을 지원합니다.

후면 패널

#	카테고리	설명
1	Power Switch	전원 스위치를 누르면 장비가 구동됩니다. 운용 중인 장비의 전원 스위치를 길게 누르면 전원이 차단되고 장비가 강제 종료됩니다.
2	Power Supply	장비의 전원을 연결합니다.

주문 정보 (Ordering Information)

Product	Description
AhnLab XTG 2000	RJ45*8, SFP*8, MGT (RJ45)*2, Console*1, Interface Slots*8, Redundant Power
AhnLab XTG 5000	RJ45*8, SFP*8, MGT (RJ45)*2, Console*1, Interface Slots*8, Redundant Power
AhnLab XTG 10000	RJ45*8, SFP*8, MGT (RJ45)*2, Console*1, Interface Slots*8, Redundant Power
AhnLab XTG 20000	RJ45*8, SFP*8, MGT (RJ45)*2, Console*1, Interface Slots*8, Redundant Power

NIC Module	Description
1G Copper 8 Port	1GbE Copper (RJ45) 8 Port LAN Module with 2 Bypass Pairs
1G Fiber 4 Port	1GbE Fiber (SFP) 4 Port LAN Module
1G Fiber 8 Port	1GbE Fiber (SFP) 8 Port LAN Module
1G Fiber 2 Port Bypass	1GbE Fiber (SFP) 2 Port LAN Module with Bypass
1G Fiber 4 Port Bypass	1GbE Fiber (SFP) 4 Port LAN Module with Bypass
10G Fiber 4 Port	10G Fiber (SFP+) 4 Port LAN Module
10G Fiber 2 Port Bypass	10G Fiber (SFP+) 2 Port LAN Module with Bypass
10G Fiber 4 Port Bypass	10G Fiber (SFP+) 4 Port LAN Module with Bypass
40G Fiber 2 Port*	40G Fiber (QSFP+) 2 Port LAN Module
40G Fiber 2 Port Bypass*	40G Fiber (QSFP+) 2 Port/2 Slot LAN Module with Bypass
100G Fiber 2 Port**	100G Fiber (QSFP28) 2 Port/2 Slot LAN Module
100G Fiber 2 Port Bypass**	100G Fiber (QSFP28) 2 Port/2 Slot LAN Module with Bypass

※ NIC 모듈은 사용 가능한 인터페이스 슬롯이 있는 경우에만 주문할 수 있습니다.
* 40G NIC 모듈은 AhnLab XTG 5000/10000/20000에서만 사용할 수 있습니다.
** 100G NIC 모듈은 AhnLab XTG 10000/20000에서만 사용할 수 있습니다.