

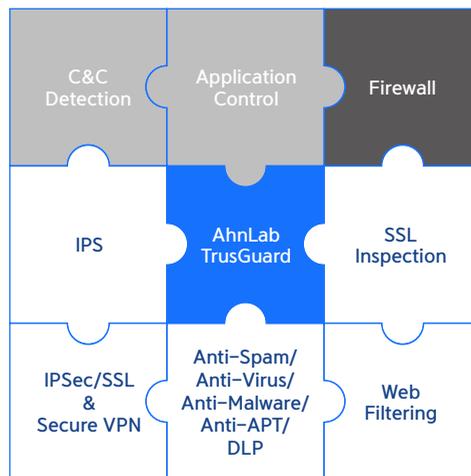
AhnLab TrusGuard

차세대 네트워크 보안 플랫폼의 기준!

TrusGuard는 진화하는 보안 위협으로부터 안전하게 조직을 보호할 수 있는 최적의 차세대 방화벽입니다.

제품 개요

철저한 시장 검증을 통해 기술력과 성능, 안정성을 인정받은 차세대 방화벽 AhnLab TrusGuard는 방화벽, IPS(Intrusion Prevention System), 애플리케이션 제어, VPN, C&C 탐지 및 차단, 안티바이러스, 안티스팸, DLP(Data Loss Prevention) 등 급변하는 비즈니스 요구사항을 반영한 제품입니다. 로우엔드 모델부터 데이터센터급 모델까지 다양한 제품 라인업을 갖추고 있는 TrusGuard는 기업 네트워크 환경에 맞춰 효율적으로 적용할 수 있습니다.



• 차별화된 차세대 네트워크 보안 플랫폼

- 글로벌/국내 애플리케이션에 대한 심층 방어 기능
- 사용자 및 디바이스 기반 정책 설정/제어
- 암호화된 트래픽 탐지
- Anti-APT 솔루션 (MDS) 연동 보안

• 독보적인 위협 탐지·차단 기술

- 보안 위협 탐지에 특화된 다계층 멀티 엔진 구조
- 보안 인텔리전스 기반 차별화된 위협 탐지
- 인하우스 위협 분석 조직/인프라 보유
- 최신 보안 위협 대응을 위한 실시간 위협 정보 반영

• 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

다양한 최신 보안 위협에 대한
차별화된 차세대 보안

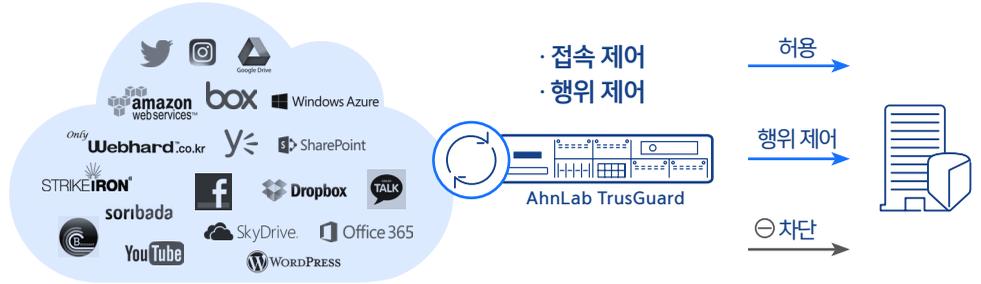
시장 요구사항이 철저히 반영된
사용자 인터페이스

독보적인
위협 탐지 및 대응 능력

차세대 방화벽 기능

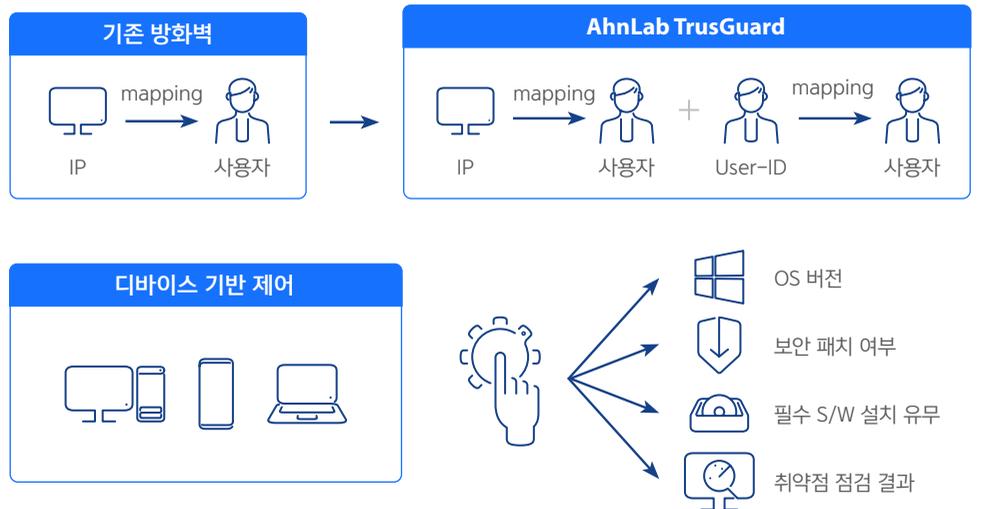
애플리케이션 제어

TrusGuard는 차세대 보안 기술인 애플리케이션 제어(Application Control) 기능을 탑재해 P2P, 웹하드, 메신저(Instant Messenger), SNS 등 수 천 개의 글로벌 및 국내 애플리케이션에 대해 실시간 분석 및 차단·허용·행위 제어가 가능합니다. 특히 국내 환경에 특화된 주요 애플리케이션에 대한 독보적인 대응 능력을 제공합니다. 또한 식별이 불가능한 알려지지 않은(Unknown) 애플리케이션 인지를 통해 허용된 애플리케이션에 대한 통신만 가능하게 하여 보안성이 높아집니다.



사용자 & 디바이스 기반 제어

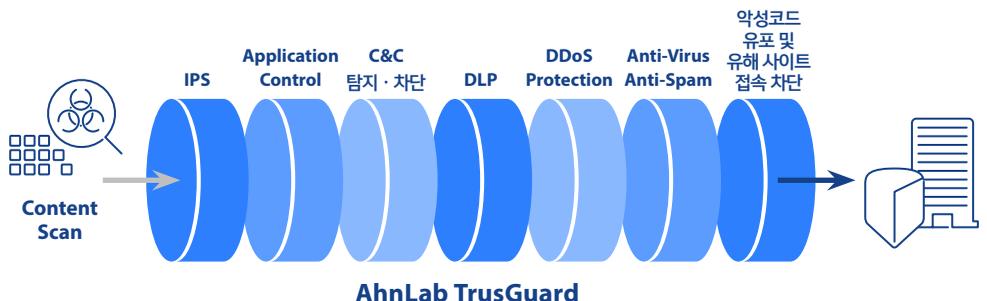
IP 주소를 기반으로 사용자를 식별하는 방식과 함께 사용자 ID 기반의 사용자 구분 및 행위 제어 기능을 제공해 효율적인 내부 보안 관리와 신속한 보안 위협 대응이 가능합니다. 또한 디바이스 상태 정보를 인지하여 OS 버전, 보안 패치 여부, 필수 SW 설치 유무, 취약점 점검 결과 등에 따라 네트워크 접근을 제어할 수 있습니다.



독보적인 위협 탐지·대응

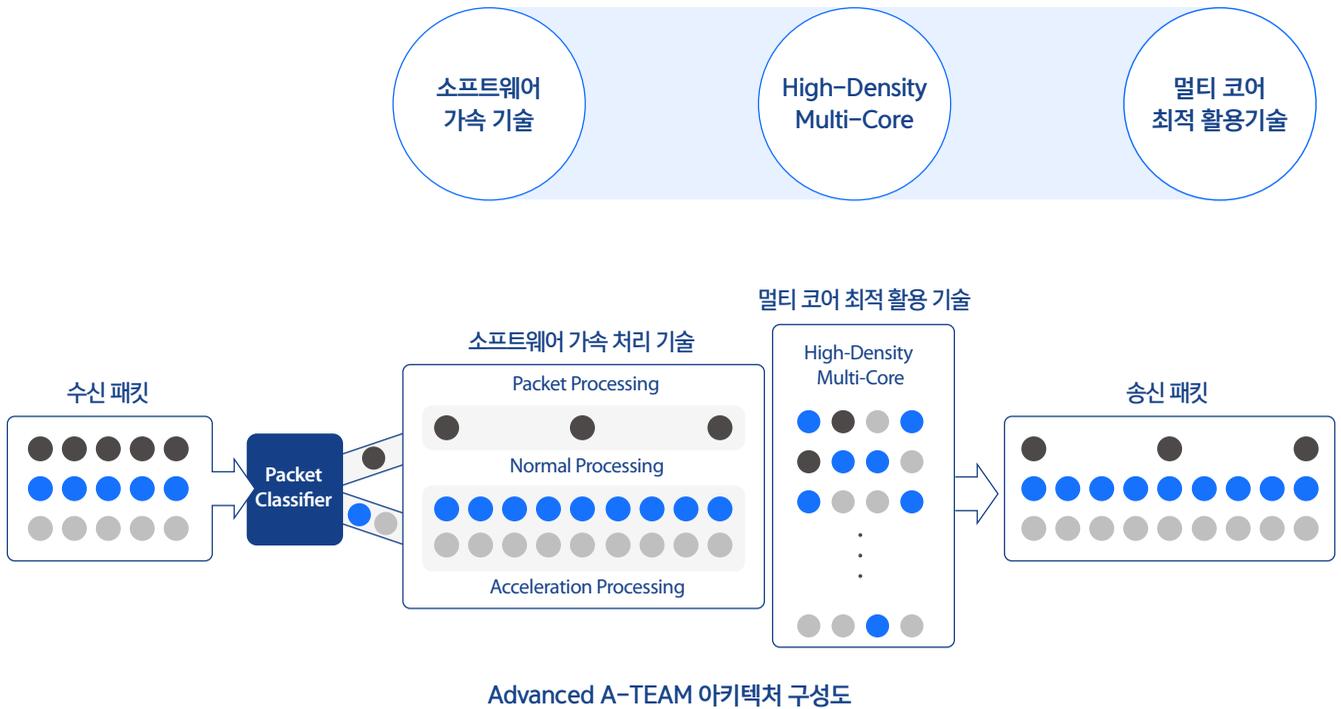
안랩의 독자적인 보안 위협 대응 체계를 기반으로 한 TrusGuard는 기업 내부로 유입되는 콘텐츠를 실시간으로 검사해 제로데이(Zero-Day) 공격 및 알려지지 않은 위협에 대한 선제적인 방어를 제공합니다.

위협 탐지에 특화된 다계층 멀티 엔진 구조	최신 보안 위협 대응을 위한 실시간 위협 정보 반영
보안 인텔리전스 탑재 (C&C 탐지/ 악성코드 유포 사이트 탐지/ 위협탐지 필터)	제로데이 공격 및 알려지지 않은 공격 대응



강력한 성능

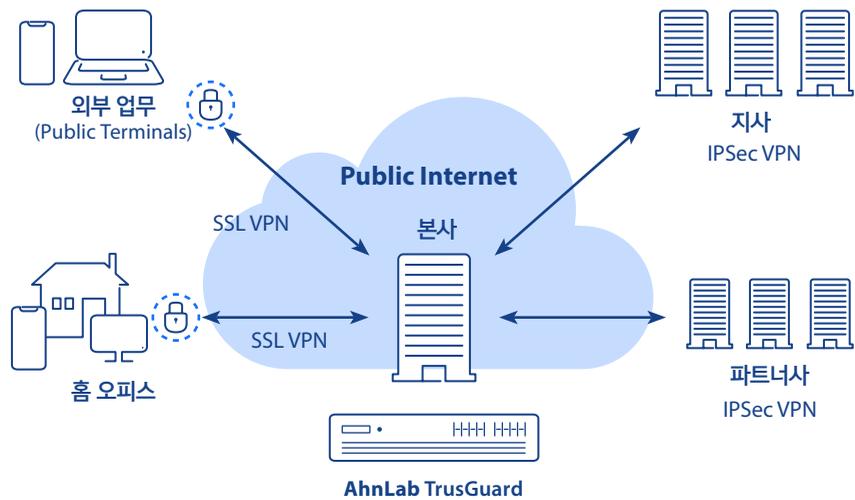
TrusGuard는 안랩이 자체 개발한 'Advanced A-TEAM' 아키텍처를 기반으로 **방화벽 처리 성능을 극대화**하였습니다. Advanced A-TEAM은 일반적인 패킷 처리 속도 대비 몇 배 이상의 처리 속도를 가능케 하는 아키텍처 기술로, 멀티 코어 최적 활용 기술과 소프트웨어 가속 처리 기술로 구성되어 있습니다.



VPN

(Virtual Private Network)

TrusGuard는 IPSec / SSL VPN 기능을 동시에 지원해 언제, 어디서나 안전한 네트워크 접속을 구현합니다. 또한 IPS 및 애플리케이션 제어를 기반으로 VPN 터널을 통한 악성코드 확산을 강력하게 통제합니다.



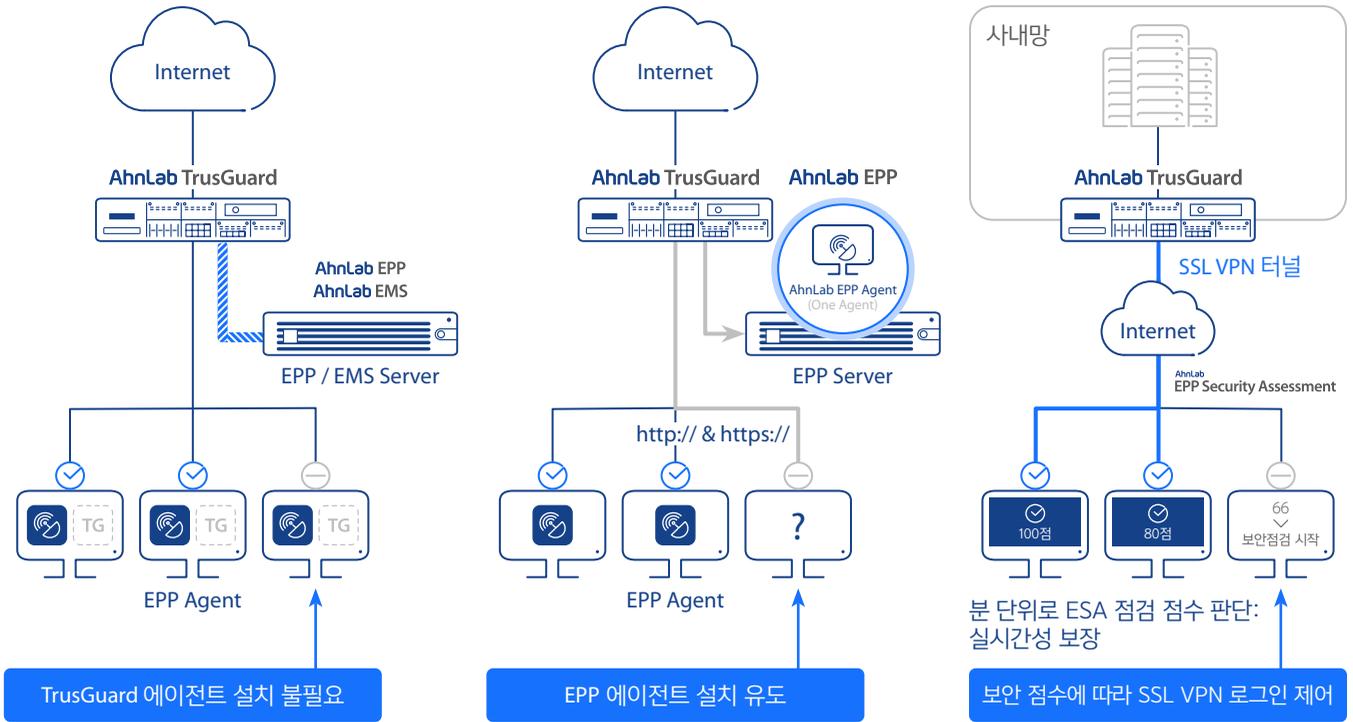
- 안정성
- 보안성

- ✓ IPSec / SSL VPN 기능 동시 지원
- ✓ 모바일 전용 SSL VPN 지원
- ✓ 다양한 클라이언트 지원 (Windows, Mac, Linux 등)
- ✓ 지점 / 지사 보안을 통한 강력한 통합 보안

엔드포인트 솔루션 연동

안랩의 엔드포인트 솔루션과의 연동을 통한 다양한 기능을 제공합니다.

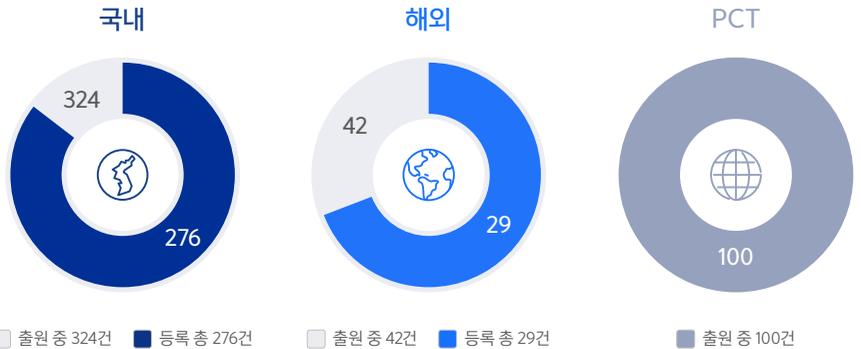
- 1) **AhnLab EPP/ EMS 연동**으로 TrusGuard의 Agent 설치없이 디바이스 기반 제어가 가능합니다.
- 2) **AhnLab EPP Agent 설치 유도**를 TrusGuard에서 제공 가능합니다. (http, https)
- 3) **AhnLab ESA 보안 점검 점수** 기반으로 TrusGuard의 SSL VPN 로그인 제어가 가능합니다.



인증 및 특허 현황

안랩의 독자적인 네트워크 기술 및 노하우가 적용된 TrusGuard는 국내 방화벽 제품 중 최초로 글로벌 시장 조사 기관 가트너의 '매직퀵드런트 엔터프라이즈 네트워크 방화벽' 부문에 5년 연속(2014~2018) 등재되는 등 세계적으로 기술력을 인정받고 있습니다.

[2022년 2월 누적 기준]



Gartner는 연구 간행물에서 다른 벤더 또는 제품, 서비스는 인증하지 않으며 기술 사용자에게 최상급 등급을 받은 벤더만을 선정하도록 권하지 않는다. Gartner 연구 간행물은 Gartner의 연구조직의 의견으로 구성되며 어떤 사실에 대한 증명서로 해석되지 말아야 한다. Gartner는 특정 용도에 대한 상품성 또는 적합성 보증을 포함하여 연구와 관련하여 어떠한 암묵적 또는 명시적인 보증을 주장하지 않는다.

주요 기능

네트워크	Firewall	IPSec VPN
Route 모드/Bridge 모드	Stateful Inspection	Hub&Spoke/Star/Mesh
Static/Policy based 라우팅	HA 구성(A-A/A-S without L4)	다양한 암호 및 해시 알고리즘 지원
Dynamic 라우팅(RIP/OSPF/BGP/RRP)	정책/세션 동기화	센터 VPN 이중화(A-A/A-S)
멀티캐스트 라우팅(PIM-SM/ IGMP)	QoS(최소 보장/최대 제한)	멀티라인 로드밸런싱 지원
Port Aggregation/ VLAN 지원	블랙리스트 필터링	DPD/PFS/Replay 공격 방어
DHCP Server/Client/Relay	화이트리스트 정책(정책예외)	SSL VPN
SNMP	중복 객체 및 중복 정책 필터링	Gateway-to-Client
IPv4 및 IPv6 Dual Stack	다양한 정책 유효성 검증	2 Factor 인증(ID/PW + 인증서)
IPv6 라우팅/IPv6 Transition	다양한 NAT 지원(Static/Dynamic/Policy based NAT 등)	엔드포인트 보안 연동 (접속 PC 사전/사후 보안 기능)
VoIP 통신 지원(H.323/SIP)	인증서 연동 사용자 인증(LDAP 등)	다양한 환경의 SSL VPN 지원 (Windows, Mac, Linux, Android, iOS 등)
IPS	프록시(proxy) 기반 제어	임베디드 단말 연동 SSL VPN 지원
Pre-defined 시그니처(7,000여 개)	정책별 세션 제어	FIDO 연동 지원
일일(daily) 시그니처 정기 업데이트	IP-Mac 필터링/IPv6 필터링	구글 OTP 자체 제공
제로데이 공격 방어(ACCESS/MAPP)	사용자 및 디바이스 기반 정책 설정/제어	Anti-Spam
시그니처 기반/Anomaly 기반	가상 시스템 지원	전용 스팸(Spam) 엔진
취약점 기반 공격 차단 (Web/OS/Network/Application)	정책/객체 자동 생성	RBL/사용자 정의 필터링
악성코드 기반 공격 차단 (Worm/Bot/Trojan/Downloader 등)	가상 패킷 정책 유효성 검사	Spam Quarantine(특정 메일 계정)
Zone 기반 정책 적용	C&C 탐지 / 차단	Anti-APT
Application Control	클라우드 기반 C&C 서버 접속 탐지 및 차단	자사 APT 보안 솔루션(AhnLab MDS) 연동
글로벌/국내 애플리케이션 탐지 및 차단	Unknown 악성 의심 파일/PUP 내부 유입 탐지	의심 파일 동작 분석 기능
애플리케이션별 세부 행위 제어	DDoS 공격 차단	악성 추정 URL 차단 기능
Unknown 애플리케이션 제어 지원	UDP/ICMP/TCP Flooding	데이터 유출방지 (DLP)
NAC	Spoofed TCP Attack	내부 정보 유출 방지
엔드포인트 안티바이러스 솔루션(V3) 연동	HTTP 취약점 공격	본문, 첨부파일, 확장자 차단
PC 백신 제어 에이전트 설치 탐지/제어	CC Attack	모니터링/로그
악성코드 감염 PC 탐지/제어	웹 필터링	내장형 HDD/로그 저장
EPP 연동을 통한 디바이스 기반 제어 (Agnatless)	방송통신심의위원회 유해사이트 DB	위젯 방식의 대시보드/연관 분석
EPP 에이전트 리다이렉트 기능 제공	자체 악성코드 유로 사이트 DB	트래픽 통합 로그/Custom 보고서
ESA 취약성 점검 기반의 SSL VPN 접속 제어	Global Categorized URL DB	관리 기능
SSL Inspection	Anti-Virus	다단계 관리자 권한
암호화된 트래픽 검사	자체 엔진(V3)	웹 기반의 HTTPS 접속
지역기반 차단	자체 시그니처 제작 역량/조직	Open API 제공
특정 국가 및 대륙별 차단	첨부파일/압축파일 검사	[AIPS 연동] 탐지 IP 블랙리스트 등록
	이메일에 첨부된 악성코드 사전방역	
	패킷 기반 Malware 고속 탐지	

제품 사양 (Specification)

SMB/중견기업 및 지사(Branch Office)용

구분	TrusGuard 40B	TrusGuard 50B	TrusGuard 70B	TrusGuard 100B	TrusGuard 200E	TrusGuard 400C
CPU	2 Core	4 Core	4 Core	8 Core	8 Core	4 Core
RAM	4GB	8GB	8GB	8GB	8GB	8GB
System Storage	4GB	4GB	4GB	4GB	SSD 32GB	SSD 64GB
Log Storage	-	SATADOM 120GB (Option)	SATADOM 120GB (Option)	HDD 1TB or SSD 240GB/960GB	HDD 2TB	HDD 2TB/4TB or SSD 960GB/1.92TB
NIC	1GC	8	8	8	6	9 (Mgmt 포함)
	1GF	-	-	-	4	8
	10GF	-	-	-	-	-
FW	4G	6G	8G	10G	14G	20G
IPS	-	1.5G	2.5G	3.5G	8G	8G
VPN	1G	1.2G	1.4G	1.6G	3.5G	4G
VPN Tunnel	2,500	5,000	5,000	10,000	30,000	30,000

Concurrent Session	1,000,000	1,500,000	2,000,000	3,000,000	3,500,000	5,000,000
Size(WxHxD)	220x44x194.5	430x44x193	430x44x193	430x44x340	430x44x340	430x44x460
Power	Single	Single	Single	Single	Single	Redundant

※ TrusGuard 40B 모델은 방화벽/IPSec VPN 기능만 제공합니다.
 ※ 성능 수치는 세부 환경 및 시스템 구성에 따라 달라질 수 있습니다.

엔터프라이즈/데이터센터 및 본사(Headquarter)용

구분	TrusGuard 500C	TrusGuard 2000B	TrusGuard 5000B	TrusGuard 10000B	TrusGuard 20000B
CPU	6 Core	8 Core	20 Core	32 Core	48 Core
RAM	16GB	16GB	64GB	64GB	256GB
System Storage	SSD 64GB	SSD 64GB	SSD 64GB	SSD 64GB	SSD 64GB
Log Storage	HDD 2TB/4TB or SSD 960GB/1.92TB	HDD 2TB/4TB or SSD 960GB/1.92TB (RAID-1/0)			
NIC	1GC	9 (Mgmt 포함)	10 (최대 34, Mgmt 포함)	10 (최대 50, Mgmt 포함)	10 (최대 50, Mgmt 포함)
	1GF	8	8 (최대 32)	8 (최대 48)	8 (최대 48)
	10GF	0 (최대 4)	0 (최대 12)	4 (최대 28)	4 (최대 28)
	40GF	-	-	0 (최대 8)	0 (최대 12)
	100GF	-	-	-	0 (최대 2)
FW	30G	60G	120G	200G	240G
IPS	12G	20G	30G	50G	70G
VPN	6G	10G	13G	19G	19G
VPN Tunnel	40,000	40,000	50,000	60,000	60,000
Concurrent Session	8,000,000	10,000,000	30,000,000	40,000,000	60,000,000
Size(WxHxD)	430x44x460	438x88x571	438x88x571	438x88x571	438x88x571
Power	Redundant	Redundant	Redundant	Redundant	Redundant

※ 성능 수치는 세부 환경 및 시스템 구성에 따라 달라질 수 있습니다.

Q-VPN용

구분	TrusGuard 2000BQ	TrusGuard 5000BQ	TrusGuard 10000BQ	TrusGuard 20000BQ
CPU	8 Core	20 Core	32 Core	48 Core
RAM	16GB	64GB	64GB	256GB
System Storage	SSD 64GB	SSD 64GB	SSD 64GB	SSD 64GB
Log Storage	HDD 2TB/4TB or SSD 960GB/1.92TB (RAID-1/0)			
NIC	1GC	10 (최대 34, Mgmt 포함)	10 (최대 50, Mgmt 포함)	10 (최대 50, Mgmt 포함)
	1GF	8 (최대 32)	8 (최대 48)	8 (최대 48)
	10GF	0 (최대 12)	4 (최대 28)	4 (최대 28)
	40GF	-	0 (최대 8)	0 (최대 12)
	100GF	-	-	0 (최대 2)
FW	60G	120G	200G	240G
IPS	20G	30G	50G	70G
VPN	별도문의			
QRNG	USB	USB	USB	USB
VPN Tunnel	40,000	50,000	60,000	60,000
Concurrent Session	10,000,000	30,000,000	40,000,000	60,000,000
Size(WxHxD)	438x88x571	438x88x571	438x88x571	438x88x571
Power	Redundant	Redundant	Redundant	Redundant

※ 성능 수치는 세부 환경 및 시스템 구성에 따라 달라질 수 있습니다.