



AXGATE 는 최근 DDoS, 웹 취약점을 이용한 공격 등 점점 다양화되고 집요해지는 보안 위협과 여러 어플리케이션 이용을 통한 내부 정보 유출의 위험 등 변화하는 네트워크 보안 환경에 대응하는 **새로운 개념의 고성능 통합 보안 솔루션**입니다.

엑스게이트 시리즈 기본 기능



NLB (네트워크 로드밸런싱)

인터넷 구간의 다양한 회선을 수용하며, WAN의 대역폭을 통합하여 트래픽을 보장하는 기술로 엑스게이트는 지능적인 로드밸런싱을 이용하여 회선 활용도를 극대화 합니다. (**엑스게이트만의 독자적인 Dcube Bonding 기술**)

방화벽(침입차단시스템)

Stateful Inspection 방식의 방화벽 기술 기반으로 패킷 필터링을 통해서 내/외부로 유입되는 트래픽 통제

IPS/DDoS 엔진을 통한 강력한 해킹방어

정확, 신속한 Signature 업데이트를 통해 패턴을 이용한 탐지 및 차단하고, 트래픽 정보를 기반으로 행위기반 탐지 및 차단을 통해 보안성을 강화합니다.

VPN (가상사설망)

안전한 IPSec VPN 및 암호화 SSL VPN으로 공중망을 이용하여 본/지사 간의 업무용 트래픽을 주고 받는 경로의 암호화를 통해 보호

엑스게이트 시리즈 특징점

사용자 인증 & 어플리케이션 제어

단순한 Port나 IP가 아닌 Application과 사용자를 구분하고 제어할 수 있는 새로운 개념의 통합 보안 솔루션

Zone기반 보안 정책

업무상 관련 있는 조직을 단위 Zone으로 묶어 차별화된 보안 정책 부여

가상화

방화벽을 논리적으로 가상화하여 현대의 AXGATE 장비를 이용하여 단위 별 독립적인 보안 서비스 제공

고성능 보장

FW, VPN, IPS, CF등의 다양한 보안 기능을 동시에 구동할 경우 발생 가능한 성능 저하를 최소화하기 위한 병렬처리 구조를 가짐

높은 편의성

- 대쉬보드 방식의 모니터링 환경 제공
- 다양한 통계 및 리포트 제공
- 정책 시뮬레이션 및 미사용 / 미참조 정책 조회 기능

엑스게이트 시리즈 보유 특허 현황

■ 사용자 인증을 통한 네트워크 자원 사용 제어 방법(FW)

웹 인증 화면을 통해 사용자를 인증하고 인증된 사용자 그룹별 정책을 적용하여 효율적으로 네트워크 자원 사용을 제어하는 기술

■ 서브트리를 활용한 퀴드트리 기반의 패킷 분류 방법(FW)

EAQT(영역분할사분트리)알고리즘을 이용한 빠른 패킷 분류를 실행하는 방법으로 퀴드트리에 별도의 서브트리를 구비하여 룰 정보가 루트노드로 편중되지 않고 별도의 해시 테이블이나 추가적인 퀴드트리를 이용하여 달성되도록 한 기술

■ DNS정보를 이용한 패킷 필터링 방법 및 방화벽 장치(FW)

고가의 DPI 기술이나 고비용의 프로세서를 사용하지 않고도 HTTPS의 암호화된 패킷에 대한 접근제어를 가능하게 하는 DNS정보를 이용한 패킷 필터링 기술

■ IP 채널 본딩을 통한 데이터 전송 방법(VPN)

인터넷에 연결된 다중 IP채널을 가상의 터널에 종속시켜 본딩하고, 이 때 각 IP채널에 대한 고효율의 로드밸런싱을 구현하며 데이터 전송 효율을 극대화 시키는 방법

엑스게이트 시리즈 상세정보

모델	장비사양
AXGATE 40	<ul style="list-style-type: none"> - CPU : 700MHz (Single Core) - RAM : 256M, USB Flash : 8G - Interface : 6Port 10/100BASE-T - Single Power
AXGATE 50	<ul style="list-style-type: none"> - CPU : MIPS 500MHz (Dual Core) - RAM : DDR2 1G, CF Card : 4G - Interface : 6Port 10/100/1000BASE-T - Single Power
AXGATE 80	<ul style="list-style-type: none"> - CPU : MIPS 700MHz (Dual Core) - RAM : DDR2 1G, CF Card : 2G - Interface : 6Port 10/100/1000BASE-T - Single Power

