빈틈없는 고성능 네트워크 보안

Secure with the pride

AXGATE Series

AXGATE

Security and Beyond

차세대 방화벽

AXGATE Series

AXGATE Series는 방화벽, VPN(IPsec/SSL), IPS, Anti-DDoS 및 Anti-Virus 등의 다양한 보안 기능을 제공하는 통합 보안 솔루션입니다. Multi Core 분산 처리 기술로 안정적인 고성능을 구현하며 대용량 네트워크 트래픽 처리 시에도 성능저하를 최소화 합니다. 다양한 제품 라인업으로 각 기업의 필요에 맞는 사양의 통합 보안 솔루션을 도입하실 수 있습니다.

AXGATE Series 특장점

논리적 가상화

논리적 가상화를 통해 한 대의 AXGATE 장비를 여러대의 방화벽/VPN과 같은 단위 별 독립적인 보안 서비스를 제공합니다.

NLB(네트워크 로드밸런싱), VPN

인터넷 구간의 다양한 회선을 수용하며, WAN의 대역폭을 통합하여 트래픽을 보장하는 기술로 엑스게이트는 dCube Bonding의 독자적인 기술로 지능적인 로드밸런싱을 통해 활용도를 극대화 합니다.

성능저하 없는 고성능 UTM

방화벽, VPN, IPS등의 다양한 보안 기능을 동시에 구동할 경우 발생 가능한 성능 저하를 최소화하기 위하여 제품 설계 단계부터 Multi Core에 최적화된 엔진을 개발하여 안정적인 고성능을 구현합니다.

사용자 인증 Zone 기반 보안정책

IP 주소가 아닌 사용자 계정을 기반으로 하여 접근을 제어하고 업무상 관련 있는 조직을 Zone 단위로 묶어 사용자 그룹별, 개인별로 차별화된 보안 정책을 적용하여 사용자 인증을 합니다.

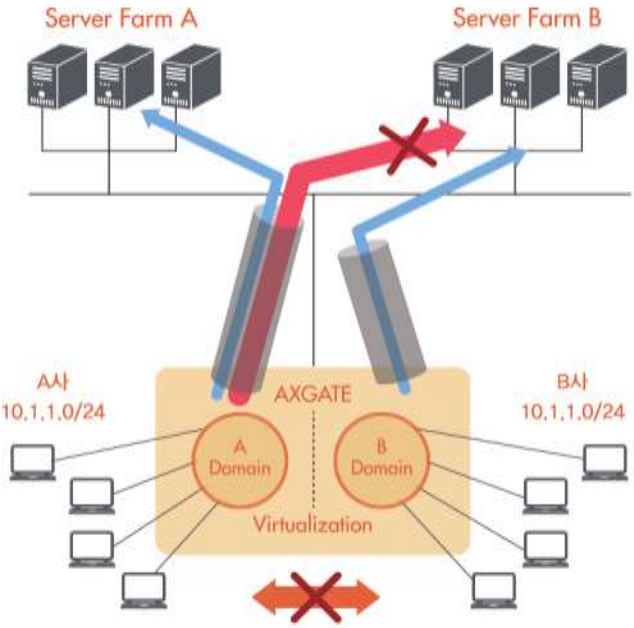
특허출원등록

- 사용자 인증을 통한 네트워크 자원 사용 제어 방법 (제 10-1387937 호)
  웹 인증 화면을 통해 사용자를 인증하고 인증된 사용자 그룹별 정책을 적용하여 효율적으로 네트워크 자원 사용을 제어하는 기술
- 서브트리를 활용한 쿼드트리 기반의 패킷 분류 방법 (제 10-1387942 호)
  EAQT(영역분할사분트리) 알고리즘을 이용한 빠른 패킷 분류를 실행하는 방법으로 쿼드트리에 별도의 서브트리를 구비하여 룰 정보가 루트노드로 편중되지 않고 별도의 해시 테이블이나 추가적인 쿼드트리를 이용하여 달성되도록 하는 기술
- DNS정보를 이용한 패킷 필터링 및 방화벽 장치 (제 10-1428999 호)
  고가의 DPI 기술이나 고비용의 프로세서를 사용하지 않고도 HTTPS의 암호화된 패킷에 접근제어를 가능하게 하는 DNS정보를 이용한 패킷 필터링 기술
- IP채널 본딩을 통한 데이터 전송 방법 (제 10-1404998 호)
  인터넷에 연결된 다중 IP 채널을 가상의 터널에 종속시켜 본딩 시 각 IP 채널에 대한 고효율의 로드밸런싱을 구현하고 데이터 전송 효율을 극대화 시키는 기술
- HA 환경에서의 패킷 처리 방법, 패킷 처리 장치 및 패킷 처리 시스템 (제 10-1836938 호)
  HA 환경에서 세션의 트래픽이 비대칭으로 서로 다른 장비에서 처리될 때 세션 동기화 패킷이 응답 패킷보다 늦게 처리되는 경우에도 응답 패킷이 차단되지 않고 정상 처리될 수 있도록 제어하는 기술
- 가상사설망을 통해 접속하는 기기를 차단하는 방법, 센터 장치 및 시스템 (제 10-1908428 호)
  무인지점의 부팅 시간과 센터와 연결된 터널의 접속 해제 시간 정보를 이용하여 장비도난에 대한 판단을 수행하고, 도난 장비 가능성이 있는 경우 터널 접속을 허용하지 않는 방법

주요기능

논리적 가상화 기능

방화벽과 VPN을 논리적으로 가상화하여 한대의 AXGATE 장비로 Virtual Domain 별 독립적인 방화벽, VPN 서비스를 제공합니다. 따라서 기존 내부 네트워크 환경의 변화 없이 적용이 가능하며, 확장성 확보, 가용성 증가, 관리편의성, 비용절감이 가능합니다.



* 한 대의 AXGATE 방화벽으로 독립적인 보안 기능

- Routing 및 방화벽 기능만이 아닌 VPN, NAT, IPS, Qos, Content Filter 등 AXGATE 의 모든 기능을 가상화 합니다.
- 한대의 물리적 장치에서 최대 250개의 Domain을 제공합니다.
- Super User 계정은 모든 Domain 의 설정 수정/삭제가 가능합니다.
- 각각의 Domain 관리자는 자신의 Domain을 제외한 다른 Domain으로는 접근/설정 변경/삭제가 불가능 합니다.
- CLI 및 GUI를 통한 가상화 관리가 가능합니다.

사용자 기반 접근 제어

IP 주소뿐만이 아닌 사용자 계정 (ID+Password) 정보를 통해 접근을 제어하고 사용자 그룹별, 개인별로 보안 정책을 차등 적용합니다.

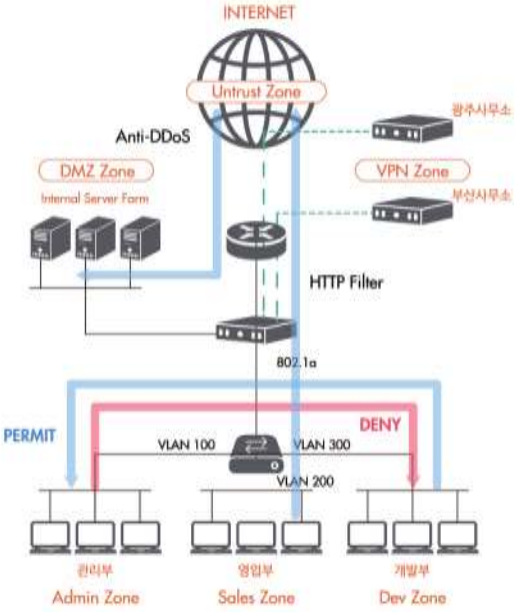
- 사용자 단말에 Agent 를 따로 설치할 필요 없이 Web을 통한 보안 인증을 지원하며, 사용자 별 이용트래픽, 공격 유형등의 통계를 지원합니다.
- 신뢰성 있는 3rd Party 인증을 통한 접근관리를 위해 Radius, LDAP, AD, MS-SQL, ORACLE, Local DB 등의 연동을 지원합니다.
- 고정 IP환경과 더불어 유동 IP를 사용하는 환경에서도 사용자 기반의 접근 제어가 가능합니다.

주요기능

Zone 기반 보안 정책

Security Zone이란 단순한 IP Address Group이 아닌 실제 인터페이스를 Binding하는 인터페이스의 묶음으로, 사전에 정의된 Zone에 할당하여 Identity를 부여합니다. Security Zone 별 정책 설정으로 보안 룰의 추가,삭제,수정이 용이하며 불필요한 보안 모듈 적용으로 인한 성능저하를 방지합니다.

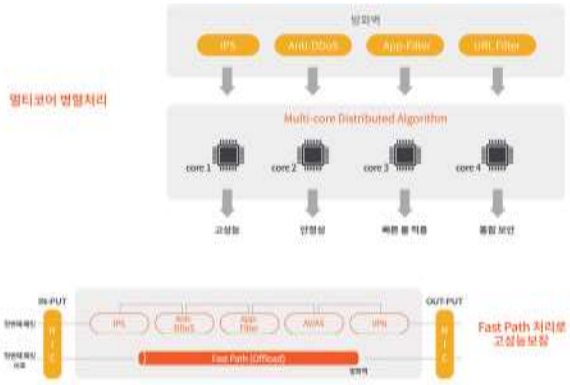
- Security Zone 별 개별 정책 / 로그 / 통계
- Contents Filter, IPS, Anti-DDoS, 방화벽 등의 보안 모듈을 Security Zone 별로 적용
- 불필요한 보안 모듈 적용으로 인한 성능 저하 방지
- Zone 간 세부 정책 설정으로 보안성 강화



Multi Core 병렬처리로 고성능 구현

개별 모듈의 병렬 처리로 여러 기능(방화벽, IPS, DDoS, SSL VPN, 어플리케이션 제어 등) 동시 구동시 성능저하를 최소화 합니다.

- 멀티코어에 최적화된 설계로 멀티코어 분산 알고리즘이 IDLE 없이 CPU Core를 활용하여 최대의 성능을 구현합니다.
- 첫 번째 패킷은 분석 과정을 통해 어떤 보안 모듈에서 처리할 지 판단하는 Slow Path로 처리하고, 두 번째 패킷부터는 선행된 패킷 처리를 참조하여 Fast Path (offload)에서 처리함으로써 Wired Speed에 가까운 성능을 구현합니다.



IPS

시그니처 기반 Rule 제공 및 사용자 정의 Rule을 지원함으로써 다양해지는 공격 유형에 대해 능동적으로 대처합니다. 지능화, 다양화되고 있는 외부 침입 공격을 다양하게 탐지, 차단하며 PCRE를 통해 변형된 공격 패턴을 감지합니다.

주요기능

어플리케이션 제어

단순한 Port 차단이 아닌 Application Level에서 탐지, 제어, 차단합니다. 업무 중요도가 낮은 어플리케이션에 대해서 Traffic과 Packet, Session을 제한합니다.

- 업무상 불필요한 사이트의 접속을 차단하여 악성코드, 웜 등을 유포하는 유해사이트를 차단
- 15개 이상의 상위 Category와 1100개 이상의 어플리케이션을 제어
- FTP, Telnet 업로드 및 다운로드 제어
- P2P, 웹하드 등에 접근 제어, 암호통신차단, 로그인 제어, 메일 제어, 파일 전송 차단 및 QoS 대역폭 제한

*메신저, 어플리케이션, P2P, 웹하드, SNS, 웹메일 차단

Web URL 필터링

업무 상 불필요한 사이트의 접속을 차단하며 악성코드, 웜 등을 유포하는 유해 사이트를 차단합니다.

- 방송통신위원회 SafeNet DB : 유해 사이트 DB연동 사이트 필터링 제공
- PICS (Platform for Internet Content Selection) : HTML 메타 태그에 포함된 내용 등급에 따른 필터링 제공
- Customized Category : 사이트 특징에 따른 사용자 정의 URL Group 필터링 제공

WEF (Web Editor Filtering)

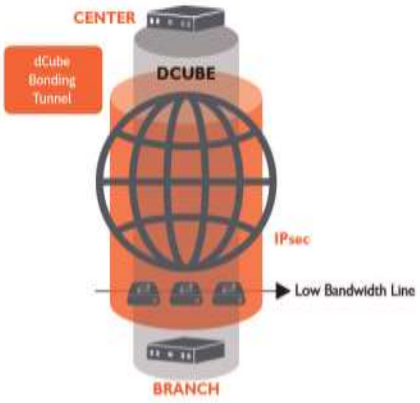
특성화된 기능 WEF (Web Editor Filtering) 으로 웹 브라우저, 웹 사이트 및 SNS에 댓글/이메일/파일 업로드 등의 행위를 차단합니다. 각종 커뮤니티 게시판에 글을 올리거나 댓글을 남기는 행위를 제한하는 기능으로 업무 이외의 활동을 제약함으로써 업무 집중력을 강화합니다. 공공기관의 경우 공무원들의 커뮤니티 및 SNS 댓글 쓰기를 통제하고 제한함으로써 정치적 중립의무를 위반하는 행위를 방지할 수 있습니다.

- 웹 메일 쓰기를 제한하여 사내 정보 외부 유출 사전 방지
- 파일 업로드 차단과 병행 시 효율적인 보안 적용이 가능함
- 커뮤니티 차단 가능 사이트 - 국내 Top 500 사이트 차단
  Alexa (http://www.alexa.com/topsites/countries/KR)
  랭키닷컴 (http://www.rankey.com/rank/rank_site_all.php)

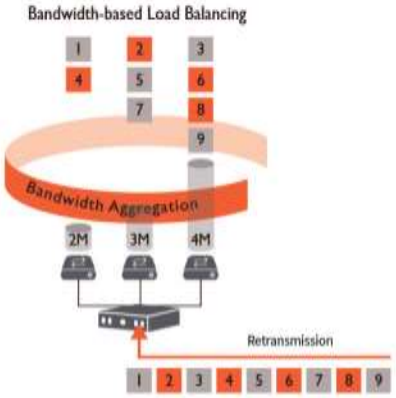
주요기능

IPsec VPN

엑스게이트의 독자적인 기술인 dCube 기술 (특허보유)은 IPsec VPN과 연동하여 안정성 높은 고 대역폭의 암호화된 채널을 제공하는 WAN Channel Bonding Algorithm으로 IPsec 암호화를 통해 보안성을 강화합니다.



*IPsec 암호화를 통한 보완성 강화



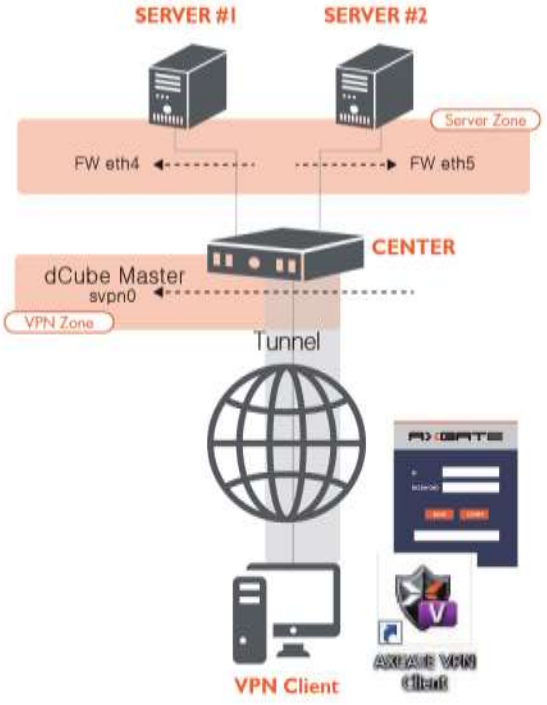
*회선 대역폭 자동감지를 통한 트래픽 부하 분산

도입 이점	저비용	지역적, 비용적인 문제로 인해 저속의 xDSL회선을 사용하는 경우 회선을 다중화 구성하여 회선 속도 향상
	고가용성	VPN Tunnel이 여러 개의 회선으로 구성됨으로써 회선 장애가 발생하더라도 실시간으로 Fail-over됨 회선 Fail-over시 Session유지 보장
특징	Bandwidth-based Load-balancing	회선의 Band width를 자동으로 감지하여 Traffic의 부하를 동적으로 분산처리하고 흐름 제어 수행
	Loss Control	Loss 패킷을 재전송하여 통신 지연 및 에러를 보정해주는 기술

SSL VPN

엑스게이트는 IPsec VPN 및 SSL VPN 기능을 동시에 지원합니다. 언제, 어디서나 안전한 내부 네트워크 접속을 구현합니다.

- ID/Password 방식
- MAC Address 고정 기능
- VPN GW 사용자 별 접속 정책 설정
- VPN Client 계정 기반 세션 로그
- 연결 상태 체크, 알람 기능
- 연결 실패 시 자동 재접속(사용자 정의)
- 설치 파일 배포, Web 기반 배포
- PC, Mobile 등의 다양한 단말기기 지원 (Window, Android, iOS 환경 지원)
- iOS는 App Store에 등록된 자체 개발 클라이언트 프로그램 제공 및 설치 가능



상세 기능

방화벽

- Security Zone별 개별 정책 적용 및 로그, 통계 관리 기능 제공
- 장비 인터페이스(물리적)별 Security Zone 설정 제공
- Role-based 사용자 인증 정책을 통한 사용자 제어 방식의 방화벽 시스템 구현 (특허 보유 제 10-1387937 호)
- 별도의 에이전트 설치가 필요 없는 Agent-less 사용자 인증 기능 구현
- 가상 패킷 시뮬레이션을 이용한 정책 검사 기능 지원
- 미 참조, 미 사용 보안 정책 및 객체 검색 기능 제공
- 중복 정책 검색 기능 지원
- Stateful Inspection 방식의 방화벽 시스템 구현
- 패킷 필터링 및 IP/Port에 따른 필터링 기능 제공
- MAC 필터링
- 다양한 네트워크 주소 변환 기능지원 (SNAT, DNAT, LSNAT, Net-NAT, IPv6-to-IPv6, NAT64 등)
- DNAT위한 Proxy-arp 기능
- 다양한 정적 정책 기반 및 동적 라우팅(STATIC, RIP, OSPF 등) 기능 지원
- Radius, LDAP, AD, MS-SQL, ORACLE, Local DB등과 연동하여 사용자 기반 보안정책 수립으로 보안성 강화
- 사용자 그룹 및 방화벽 정책 기반 라우팅 기능 지원
- VLAN별 필터링 규칙 설정 기능 지원
- 보안정책(Rule) 수와 관계없이 일정한 성능 유지 (특허 보유 제 10-1387942 호)
- 추가 장비 없이 다양한 HA 구성이 가능
- 네트워크 구성에 변경 없이 Bridge 모드 지원
- Zone별, 사용자별 통계정보(트래픽량, 세션량, 서비스별 등) 제공
- Split DNS 서비스 제공
- 세션 제한 / 세션 affinity 기능
- FQDN 객체지원

VPN

- 표준 IPsec Protocol 지원 및 IKE v1, v2를 모두 지원
- IKE Diffie-Hellman Group 1, 2, 5, 14, 15, 16, 17, 18, 22, 23, 24
- 3DES, AES(128, 192, 256), SEED, ARIA(128, 192, 256)등 암호화 알고리즘 지원
- SHA1, SHA-256, SHA-384, SHA-512 등의 무결성 알고리즘 지원
- NAT-Traversal 및 Dead Peer Detection 기능 지원
- Multi-tunnel 지원을 통해 L4 switch 없이 Active-Active 구성 가능
- Bandwidth-based Load-balancing
- WAN Channel Bonding Algorithm 지원 (다중 회선 사용시 회선 Bonding 기능 지원) : dCube Bonding (특허 보유 제 10-1404998 호)
- 전송 중 발생하는 Loss 트래픽 감시 및 해당 패킷 수신 후 재전송 기능 지원
- 터널링 패킷 Flow Control
- L2 Bridge VPN 기능
- 클라이언트 프로그램을 통한 SSL VPN 기능 지원 (Gateway to Client VPN)
- VPN 클라이언트 계정 기반 세션 로그
- VPN 무인 지점 장비 도난 시 연결 차단 기능 (특허 보유 제 10-1908428 호)

가상화

- Virtual Domain 지원
- 물리적/논리적 다양한 Interface의 선택적 Virtual Domain에 할당 기능
- 도메인별 상호 독립적인 Static, Dynamic(OSPF) Routing 제공

IPS

- 5,000 여개 이상의 시그니처 기반 Rule 제공
- 시그니처 기반, 프로토콜 기반, 트래픽 기반 비정상 행위 탐지 및 차단
- Signature Action변경 가능(패턴, 패턴 그룹, 위험 등급)
- Snort 기반 Worm/Virus와 Backdoor, Web을 통한 Spyware, Malware 차단 시그니처 보유
- PCRE를 통한 다양한 형태의 외부 공격차단 가능
- 자체 IPS 및 Anti-Virus 시그니처 적용 정밀 탐지 및 차단 수행
- 실시간 패턴 및 정책 업데이트 기능 제공
- Stream 기반의 Anti-Virus 기능 제공
- Evasion Attack 탐지
- 사용자 정의 Rule 및 Snort Rule 형식 지원

Anti-DDoS

- TCP/UDP/ICMP/HTTP/DNS Flooding 공격 방어
- SIP Flooding 공격 방어, SCAN/SWEEP 공격 방어
- Protocal Anomaly, Traffic Anomaly 공격에 대한 차단 기능 제공
- Traffic Anomaly 자동 학습 기능 지원
- Black/White List를 통한 필터링 기능 지원

Anti-Virus

- 파일 기반 탐지
- FTP, HTTP, SMTP, POP3 지원

Anti-Spam

- 제목, 본문에 삽입된 키워드, 문장에 대한 필터링 기능
- PCRE기반 키워드 매칭
- 메일 사이즈, 수신자 수, 첨부파일 제한
- 메일 주소 기반 Black/White List
- RBL(Real-time Black List)기반 스팸 탐지 및 차단
- TAG/FORWARD 지원

애플리케이션 · 웹 필터링

- Kennel Level 패킷 처리 방식의 필터링 기법 구현
- 방송통신심의위원회 제공 SafeNet DB연동을 통한 유해사이트 차단 기능
- Web Editor Filtering기능 (커뮤니티, 포털, SNS, 웹메일 등의 댓글, 쓰기, 업로드 차단)
- 사용자 정의 URL 차단 기능 제공
- FTP 필터링 : 파일 업로드 및 다운로드 제어 기능 제공
- Telnet Command, 파일 업로드 및 다운로드 제어
- Anonymizer 서버 접속 차단
- IM(Instant Messenger), 인터넷 이메일, Game, P2P, SNS, Web-Hard 접근 제어
- 애플리케이션 단계별 제어(사용차단/파일전송차단/사용대역폭제한)
- Black/White List를 통한 필터링 기능 지원
- Proxy 서버 필터링
- Post Method 파일 첨부 금지 및 데이터 크기 제한
- URL 시뮬레이션 기능
- DNS Look Up Filtering (특허 보유 제 10-1428999 호)

Network

- Transparent, Router Mode
- Static, RIP, OSPF Routing
- Policy-based Routing/User-based Routing
- Multicast Routing(PIM-SM, PIM-DM, IGMP) 지원
- VRRP, IP Backup
- 802.1q VLAN
- 802.3ad Link Aggregation

IPv6

- IPv6 Firewall/IPS/Anti-DDoS/NAT/IPsec
- IPv6 Routing
- IPv4/IPv6 Transition (Dual Stack, NAT-PT, Tunneling, 6 to 4, ISATAP)
- IPv6 DHCP
- IPv6 RA(Router Advertisement)

Management

- Dashboard 형식의 모니터링
- 정책 import/export 기능
- 자동/수동 시그니처 업데이트
- 실시간 세션 검색
- CPS, BPS, PPS 정보 제공
- 백업 로그 viewer

HA

- Active-Active, Active-Standby
- 세션 끊김 없는 안정적인 Failover
- 세션 동기화/정책 동기화(자동, 수동)
- Virtual MAC 지원
- 패킷 스케쥴링 기능 (특허 보유 제 10-1836938 호)

QoS

- Rule 기반 대역폭 보장/제한 정책
- PPS 제어
- 우선 순위 지정

AXGATE
Security and Beyond

(주)엑스게이트
http://www.axgate.com
06183 서울특별시 강남구 영동대로 85길 13 (대치동 950-1 송석빌딩 5층)
Tel : 070-4034-6410 / Fax : 02-557-1778