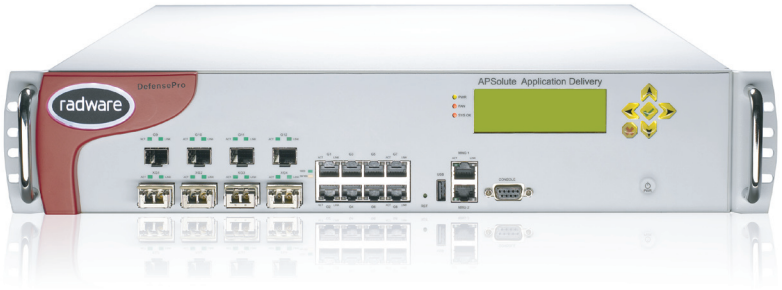
www.kornicglory.co.kr

Smart Business.



Radware DefensePro

No.1 in Anti-DoS & IPS

Anti-DoS

Anti-DoS 솔루션은 언제 발생할지 모르는 DDoS 공격에 대응하기 위해 반드시 필요한 기본적인 보안 솔루션으로 자리잡았습니다. Anti-DoS 솔루션은 내부로 유입 되는 트래픽의 성격 및 트랜잭션,커넥션에 대한 다양한 정보를 학습한 후에 비정상적인 형태의 공격 트래픽, 혹은 비정상적인 서비스 요청이 발생하는 경우 관리자의 개입없이 이를 능동적으로 즉시 차단시켜줄 수 있어야 하며, 이러한 공격 차단 과정에서 정상적인 트래픽이 막히는 오탐(False – positive) 이 없어야 합니다.
즉,실제 서비스 트래픽은 100% 정상적으로 통과시켜야 합니다.

DefensePro

라드웨어의 디펜스프로는 멀티코어 ASIC 기반의 고성능 하드웨어를 통해 멀티 기가 트래픽의 처리 능력을 제공하고 행동 기반으로 동작하는 BDoS(Behavior DoS) 엔진을 통해 네트워크 기반의 DDoS 공격을 완벽하게 차단함과 동시에 Mitigator 엔진을 탑재하여 HTTP, SIP 과 같은 애플리케이션 기반의 플러딩 공격도 완벽히 차단하는 전세계 보안시장의 대표적인 Anti-DoS 솔루션입니다.

radware

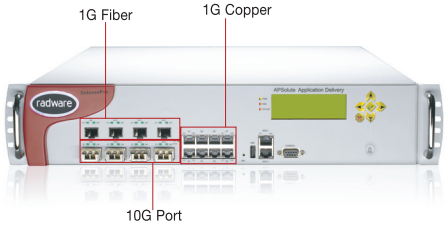
KORNIC GLORY

KORNIC GLORY

Why DefensePro?

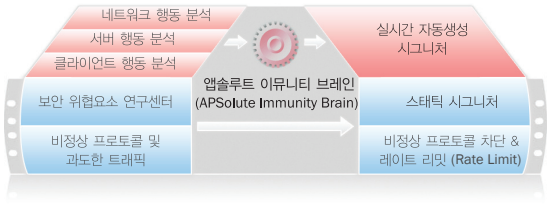
1. 강력한 처리 성능

ASIC 기반의전용 하드웨어를 통해 업계 최고인 12Gbps이상의 공격 차단 성능을 제공하며, 멀티포트의 10GE 및 1G 인터페이스를 지원합니다.



2. 완벽한 DDoS 공격 차단 능력

행동 분석 기반의 공격 차단 엔진을 통하여 실시간으로 시그니처를 자동 생성하여 DDoS 공격의유입을 즉각 차단시켜줍니다. 또한 이미 알려진 형태의 공격은 정기적으로 업데이트되는 스태틱 시그니처를 통하여 효과적으로 차단시켜줍니다.

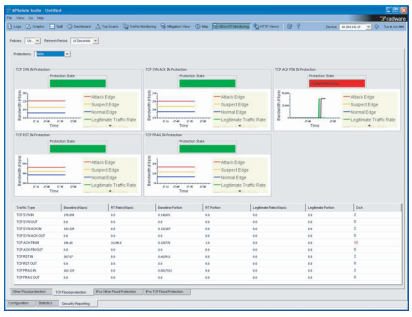


3. 심플한 구성 지원

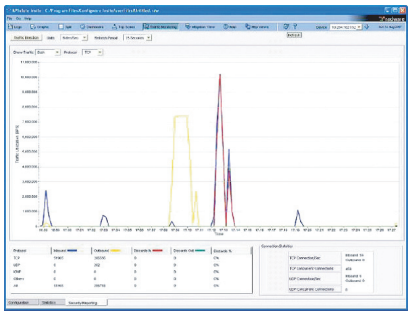
Anti-DoS 솔루션의 도입을 위해 기존 네트워크의 구성을 변경할 필요가 없습니다. 기존 네트워크 구성에 DefensePro 제품을 투명(Transparent)하게 추가하면 됩니다.

4. 손쉬운 설정과 관리

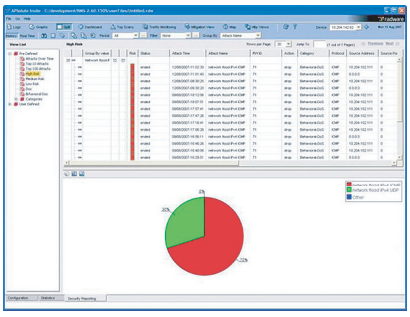
GUI기반의 관리툴인 APSolute Insite Security 를 통하여 직관적이고 편리한 관리 인터페이스를 제공합니다. 단 몇 분만에 모든 설정이 가능하며 유입되고 차단되는 공격의 정보를 실시간으로 모니터링 및 리포팅 할 수 있습니다.



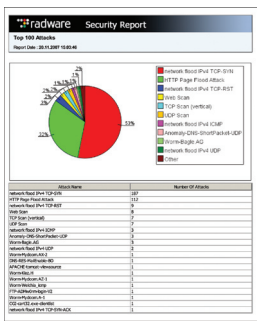
DDoS 공격 트래픽 통계 테이블

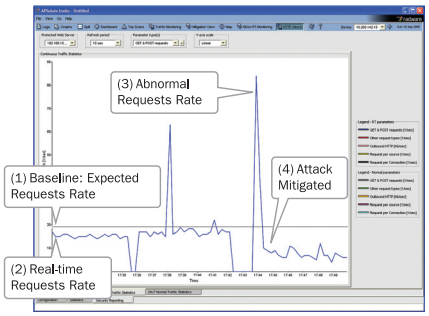


트래픽 모니터링 뷰 화면



실시간 공격 차단상태 모니터링 화면





HTTP 플러딩, SIP 플러딩과 같이 최근 부상하고 있는 신종 애플리케이션 기반 DDoS공격에 대한 대비책은 물론, Brute-Force와 같은 서버 대상의 공격 차단 및 Worm의 전파 침투 행위를 근본적으로 방지하는 Anti-Scanning 기능도 포괄적으로 제공됩니다.

차단된 DDoS 공격에 대한 명확한 차단 정비 및 Footprint 정보를 제시함으로써, 보안 관리자는 공격정보에 대한 내용을 정확히 확인할 수 있습니다.

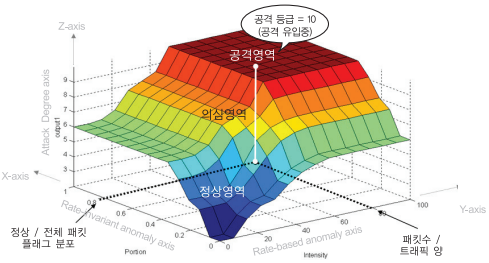
FEATURES

스스로 학습하고 즉시 방어하는 DDoS 보안 솔루션

디펜스프로의 행동기반(Behavior Based) 및 자가학습(Self Learning)메커니즘은 악의적인 네트워크 트래픽 패턴을 능동적으로 분석합니다. 공격이 유입되면 디펜스프로는 공격 고유의 행동과 습성을 찾아내고 이를 차단하기 위한 필터를 스스로 만들어낸 뒤 즉각 이에 적절한 차단 대응을 수행합니다. 또한 폐쇄형 피드백(Closed Feedback) 메커니즘은 필터링 영역을 동적으로 수정해주어 유입되는 공격을 계속적으로 찾아내고 위험성을 내포한 어떠한 정교한 공격이 유입되더라도 이를 효과적으로 차단합니다.

복합 DDoS 공격 방어 기능

디펜스프로는 알려진 공격 및 알려지지 않은 신종 제로데이 공격을 차단시켜 줍니다. 디펜스프로는 Buffer Overflow, Ping of Death, Land Attack과 같이 단일 패킷 혹은 복수개의 패킷을 사용하는 DDoS 공격을 차단해주며 행동기반으로 동작하는 BDOS(Behavior DoS) 엔진을 통해 알려지지 않은 DDoS 공격을 차단 시킵니다. 차단할 수 있는 DDoS 공격은 제품 상세 규격 테이블을 참조하시기 바랍니다.



능동형 탐지 엔진 (Behavior DoS Engine)

디펜스프로는 악의적인 공격을 차단하기 위한 능동형 탐지 엔진을 채택하고 있습니다.
이 엔진은 유입되는 공격 트래픽에 대하여 빠르고 정확한 분류 및 제어를 수행하며 특히 DDoS 공격에 대하여 탁월한 차단능력을 제공합니다.

애플리케이션 스캐닝 및 사전 탐색 공격 방어 기능

해커들은 공격을 하기 전에 네트워크상의 공격 대상 서버에 열려 있는 애플리케이션주소 및 포트를 검사합니다. 디펜스프로는 이러한 스캐닝과 같은 사전 공격 활동을 감지 / 차단하여 공격의 여지를 적극적으로 제거시켜줍니다.

HTTP DDoS 공격 방어 기능

디펜스프로는 정상적인 웹서버 접속을 가장하여 무차별적인 웹 접속 트래픽을 일으켜 서버와 네트워크를 마비시키는 공격인 HTTP 플러딩에 대한 차단을 능동적으로 수행합니다. 통상 해커들은 HTTP BOT이나 HTTP Page Flooder 프로그램을 이용, 반복적으로 많은 양의 웹 접속을 일으켜 서버의 자원을 고갈시키고 서비스를 다운시키는데, 디펜스프로는 능동적인 분석/차단 메커니즘을 사용하는 HTTP Mitigator 기능을 통하여 HTTP 플러딩 공격을 완벽히 차단시켜줍니다.

SIP DDoS 공격 방어 기능

디펜스프로는VoIP가 사용하는 SIP 프로토콜에 대하여 시장에서 가장 정교한 보안기능을 제공하는 제품입니다. 디펜스프로는 SIP 서버, 프록시, 소프트폰에 이르는 다양한 SIP 장치를 DDoS 및 기타 악의적인 공격으로부터 안전하게 보호해 줍니다.

서버 크래킹 공격 방어 기능

디펜스프로는 능동형 감지 / 차단 메커니즘을 애플리케이션 레벨로 확장시켰습니다. 서버 크래킹 차단기능은 HTTP, FTP, POP, IMAP, SIP, MS-SQL 서버에 대한 크래킹은 물론, Brute-Force 공격, 사전(Dictionary) 공격, HTTP 취약점 스캐닝, SIP Spoofed Invite Floods, SIP Spoofed Register Floods를 비롯한 다양한 크래킹에 대한 차단을 능동적으로 수행합니다.

IPv6 주소 기반 DDoS 공격 방어 기능

디펜스프로는 최근 유/무선 통신사업자에서 요구가 증가되고 있는 IPv6를 지원합니다. 이것은 단순히 IPv6 패킷 플로우를 지원하는 것 뿐만 아니라 IPv6에 대한 완벽한 DDoS 공격 차단 기능을 의미하고 있습니다. 예를 들자면, IPv6를 통해 유입되는 공격의 스캐닝, 차단은 물론, 보고서 작성까지 지원하고 있습니다.

웜 전파 방지 기능

디펜스프로는 랜덤 혹은 수도-랜덤(Pseudo-Random) 확산 기법을 사용, 더욱 강력한 자가 확산 기능을 가진 신종 웜(Worm)의 활동을 감지하고 이를 차단시켜줍니다. 이 차단기술은 디펜스프로가 지원하는 BDOS엔진의 퍼지로직 알고리즘이 사용자 트래픽의 행동분석 및 차단 의사결정 메커니즘을 바탕으로 하고 있으며 패턴 없이도 웜 공격을 차단할 수 있는 제로데이 공격 방어 솔루션입니다.

SSL 암호화 DDoS 공격 방어 기능

해커들의 공격 방법은 나날이 지능화되고 있습니다. SSL 암호화 공격도 이 중 하나인데, SSL 트래픽 자체가 암호화된 형태이기 때문에 트래픽의 분석과 차단이 매우 어려운 것이 사실입니다. 하지만 라드웨어의 AppXcel™ 제품을 디펜스프로와 연동하면 SSL로 암호화되어 유입되는 공격도 완벽히 차단할 수 있습니다. 클라이언트의 SSL터널이 클라이언트에서 서버로 생성될 때 디펜스프로는 AppXcel™ 로 트래픽을 복사해주며 AppXcel은 암호화된 트래픽을 복호화시켜 디펜스프로가 검사를 수행할 수 있게끔 처리합니다. 한편, 디펜스프로는 공격 혹은 의심스러운 트래픽이 발견될 때 실시간으로 해당 세션을 단절시켜줍니다.

보안 업데이트

라드웨어는 24x7 체제로 운영하는 글로벌 보안 운영센터(SOC)에서 고객들에게 보안 업데이트 서비스(SUS, Security Update Service)를 제공합니다. 보안 업데이트를 통해 주간(Weekly) 보안 업데이트 및 수시 보안 업데이트가 자동적으로 고객들에게 제공되며 고객들은 새로운 공격 시그니처 필터를 통해 신종 공격으로 인한 피해를 예방할 수 있습니다.

제품 기술 규격

사용목적		Anti-DoS 전용	Anti-DoS & IPS 동시 지원		
하드웨어 플랫폼		 ODS3 S1	 ODS3 S2	ODS2 S1/S2	 Mini DP(SP-1)
제품명		DP12414 DP8412 DP4412	DP8412 DP4412	DP3016 DP2016 DP1016	DP502 DP202 DP102
차단성능		12Gbps 8Gbps 4Gbps	8Gbps 4Gbps	4Gbps 2Gbps 1Gbps	500Mbps 200Mbps 100Mbps
성능 업그레이드 방법		라이센스 성능 업그레이드	라이센스 성능 업그레이드	라이센스 성능 업그레이드	라이센스 성능 업그레이드
메모리		8G	10G	6G	1G
포트	10GE Ports(XFP)	4	4	N/A	N/A
	1GE Ports(SFP)	4	4	4	N/A
	10 /100/1000Ports	8	8	12	2
	Management Ports	2	2	2	1
	USB port	지원	지원	지원	N/A
고가용성	Internal Bypass	Copper	Copper	Copper	Copper
	Power Supply	Dual	Dual	Single/Dual	Single
	Multi Segmentation	지원	지원	지원	N/A
세부 지원 기능	구성 지원	In-Line 및 Out-of-Path			
	다양한 차단 모드 지원	Report Only, Block, Reset Source, Reset Destination, Reset Bi-directional			
	네트워크 기반 DoS/DDoS 차단	TCP Flood, UDP Flood, DNS Query Flood, ICMP Flood, IGMP Flood, IP Fragment Flood 등 각종 네트워크(IPv4 & IPv6) 기반 Flood공격 차단			
	HTTP Flood 차단	반복적인 웹페이지 요청 공격 차단, 반복적인 검색어 공격 차단, 반복적인 URL/URI 공격 차단, Cache-Control 공격차단			
	Server-Cracking 공격 차단	Brute-force 및 dictionary공격 차단 : 메일서버(SMTP, POP3, IMAP), FTP 서버, SIP 서버, MS-SQL/MYSQL 서버 웹서버 취약점 스캔 공격 및 해킹 시도 공격차단 SIP Invite Flood 공격 차단, SIP Bye Flood 공격차단			
	Anomaly 공격 차단	L3-L4 Anomaly공격 차단, L4-L7 Application Stateful Inspection 기능 지원(TCP, ICMP, DNS, HTTP, HTTPS, SMTP, IMAP, POP3, FTP, SSH등) TCP Reassembly및 IP Defragmentation 지원			
	Scan 공격 차단	L3-L4 Horizontal/Vertical Scan 공격 차단, Fast/Slow Scan 공격 차단, Stealth Scan 공격 차단, Backdoor/Trojan Search 공격 차단, Ping Sweep공격 차단 등			
	Zero-Day 공격 차단	실시간 능동형 자동 필터 생성 기능(Source IP, Destination IP, Source Port, Destination Port, Packet ID, Packet size, TTL(Time to Live),Tos(Type of Service), IP Checksum, TCP Sequence Number, Tcp Checksum, TCP Flags, ICMP Checksum, UDP Checksum, ICMP Message Type, DNS Query, DNS Query ID, HTTP request 등의 정보조합)			
	NAT/Proxy 환경 지원	NAT/Proxy 환경(동일 Source IP)을 이용한 공격시, 정상트래픽과 공격트래픽을 분류하여 차단하는 스마트 매커니즘 지원			
	세션 제어 기능	프로토콜 및 서비스별 세션 제어기능 (Source Count, Target Count, Source+Target Count)			
	공격자 격리 기능	공격 의심 징후 포착시, 일정시간동안 공격자 격리(SrcIP, SrcIP+DestIP, SrcIP+DestPort, SrcIp+DestIP+DestPort, SrcOP+ DesIP+SrcPort+DestPort 조합)			
	예외 처리 기능	White List & Black List 기능 지원			
	Tunneling protocols	VLAN Tagging, L2TP, MPLS, GRE, GTP			
	경고 통보 기능	SNMP V1, 2C &3, Log File, Syslog, E-mail등			
	포렌직(Forensic) 기능	공격 차단 Footprint 정보 제공, 차단 로그 추출 기능 제공, 공격 패킷 검출 기능 제공, 공격 차단 레포트 기능 제공			
	관리 기능	SNMP V1, 2C, 3, HTTP, HTTPS, SSH, Telnet, Console			
	시그니처 기반 공격 차단 (IPS 패턴 업데이트)	N/A	Web application protection, Mail servers protection, FTP servers protection, DNS Vulnerabilities, SIP vulnerabilities, SNMP Vulnerabilities, Microsoft vulnerabilities, Worms and Viruses, Backdoors and Trojans, Cross-Site Scripting, SQL Injections, Spyware, LAN Protocol and Services Protection (RPC NetBIOS, Telnet etc.), Generic Payloads (Remote Execution, Shellcodes), Security updates service (SUS) – weekly updates and emergency updates. User-defined Attack Signatures.		

수상 및 인증 내역

Info Security Products Guide 2008 GLOBAL PRODUCT EXCELLENCE AWARDS CUSTOMER TRUST ★★★★★

美 Info Secuirty Products Guide에서 2008년/2009년 2년 연속 최고의 네트워크/애플리케이션 보안솔루션으로 선정

NSS Labs APPROVED

세계적인 보안솔루션 평가기관인 NSS Labs를 통해 Attack Mitigator 부분 인증 획득 (2008.4)
*Anti-DoS 제품 중 유일

RSTC Radware Security Training Center

"디도스 전문 보안교육센터" 인 라드웨어 보안교육센터(RSTC)를 통해 실무 중심의 디도스방어 기술 전수 및 최신 보안 트랜드 정보 제공

KORNIC GLORY
서울시 강남구 논현동 57-38 원영빌딩 5/6층
TEL 02_3476_4200 FAX 02_3476_4214
www.kornicglory.co.kr

radware
라드웨어 코리아(주) 서울시 강남구 역삼동 677-25 큰길타워 14층
(우)135-080 TEL 02)3452-1240 FAX 02)3452-2742
www.radware.com / www.radwarealteon.com