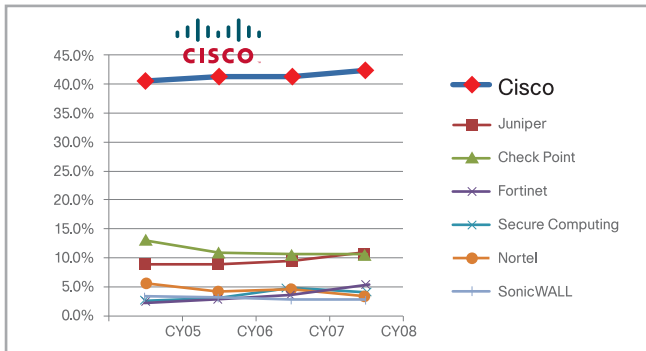


업계 최강의 통합 방화벽 솔루션, Cisco ASA 5500 시리즈

Cisco ASA 5500 Series의 경쟁우위적 기능 소개

제품소개

Cisco ASA5500 시리즈는 지난 십수년간 지속적으로 발전시켜 **최고의 안정성**을 자랑하고 있는 OS를 기반으로 방화벽과 IPSec VPN 서비스를 기본 제공하며, 라이선스 기반의 SSL VPN과 H/W 기반의 침입방지 또는 콘텐츠 보안 모듈을 탑재할 수 있는 통합 위협 관리 솔루션입니다.

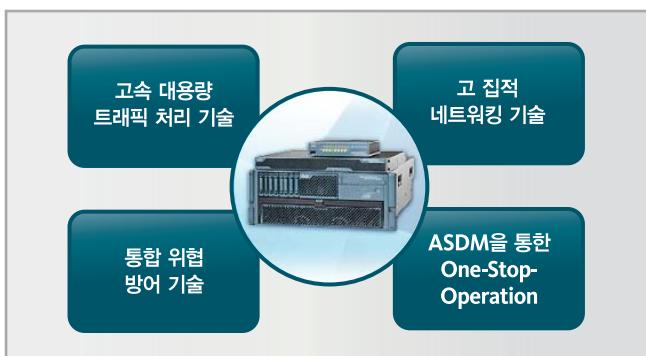


〈그림 1-1 지난 4년간 전세계 Integrated Security Appliance 시장 점유율의 변화. 출처: Infonetics〉

Cisco ASA5500 Series는 기업이 당면한 혼합된 보안 위협 및 제로 데이 위협에 대해 **하나의 시스템적 보안 처리**를 수행함으로써 효율적이고 완벽하게 기업 네트워크를 보호할 수 있습니다.

제품의 특징점(경쟁우위 기능들)

Cisco ASA 5500 시리즈가 가지고 있는 4가지 핵심 기술은 대형 포털 서비스 또는 대형 기업의 고속 대용량 서비스를 위한 **고속 대용량 트래픽 처리 기술**, 안정적이고 유연한 설계를 위한 **고 집적 네트워킹 기술**, 기업이 직면한 다양한 보안 위협에 대한 강력한 통합 보안 기능을 제공하는 **통합 위협 방어 기술**, 이런 다양한 기능들에 대해 쉽고 효율적인 운영이 가능하도록 Built-in 되어 있는 ASA의 GUI 관리툴로서 제공되는 ASDM을 이용한 One-Stop-Operation 기술로 나누어 질 수 있습니다.



〈그림 1-2 Cisco ASA 5500 Series 4대 핵심 기술〉

→ 고속 대용량 트래픽 처리기술

기본적으로 방화벽에 있어서 고대역폭의 지원도 요즘과 같은 대용량의 멀티미디어 트래픽을 지원함에 있어서 빼 놓을 수 없는 요소이지만, 다양한 광고와 다수의 대화형 웹 응용프로그램을 하나의 웹 페이지에서 모두 보여 주는 현재와 같은 Web 2.0 시대에 있어서 더욱 더 중요한 부분이 바로 초당 신규 연결 요청 처리 속도(CPS: Connection Per Second)입니다.



〈그림 1-3 초당 신규 연결 처리 속도 경쟁사 비교〉

Cisco ASA 5500 시리즈는 전 플랫폼에서 동급 경쟁사 장비 대비 2~7배 이상의 CPS 성능을 제공하며 최대 15만 CPS의 고속 처리 및 최대 16Gbps의 대용량 트래픽 처리를 지원합니다.

또한 장소, 시간에 구애 없는 사무환경의 확장이 중요한 만큼 Cisco ASA 5500 시리즈에서는 전 플랫폼이 IPSec VPN과 SSL VPN을 동시에 지원하며, 자체 로드밸런싱 및 클러스터링 기술을 통해 최대 100,000 동시 세션까지의 동시 연결이 가능합니다.



〈그림 1-4 IPSec/SSL VPN 클러스터링 기능 및 성능〉

IPSec VPN과 라이선스 추가만으로 가능한 SSL VPN의 동시 지원은 유일하게 Cisco ASA 5500 시리즈만이 제공하는 기능으로써 모빌리티 환경을 위한 암호화된 안전한 연결을 언제 어디서나 쉽고 간편하게 제공할 수 있습니다.

➔ 고 집적 네트워킹 기술 - 자원독립적 가상방화벽 기술

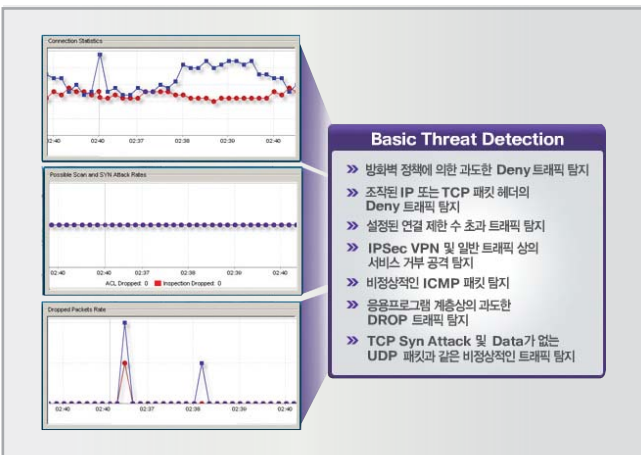
기업 네트워크에서 각 서비스존 또는 네트워크 자원 별로 개별 방화벽을 구축하여 발생하는 비용 및 비효율적 관리를 보완하기 위한 Cisco ASA 5500 시리즈의 가상방화벽 기술은 타 경쟁사 방화벽에서 지원하고 있는 몇가지 설정 및 정책에 대해서만 독립적인 관리가 되는 제한된 가상화 기술이 아니라 완전히 독립된 가상방화벽으로써, 각 가상방화벽에 대한 관리적 접근에서부터 가능한 시스템 자원의 한계에 대해서도 각 서비스 등급별로 완전하게 나눌 수 있어서, 특정한 서비스 네트워크에서의 과도한 자원 사용을 할지라도 해당 가상방화벽내의 네트워크로만 영향을 최소화하므로, 경쟁사 가상방화벽 기술과는 달리 비용 효과적 이면서도 최고의 안정성을 제공합니다.



〈그림 1-5 Cisco 자원 독립적 가상방화벽 vs 경쟁사 정책기반 가상 방화벽 기술 비교〉

➔ 통합위협 방어기술

Cisco ASA 5500 시리즈는 방화벽 대시보드를 통해 단순한 방화벽 정책 기반의 방어의 한계를 넘어서 방화벽기반의 공격성 비정상 트래픽 및 스캐닝 공격을 실시간으로 탐지 및 차단 할 수 있습니다.

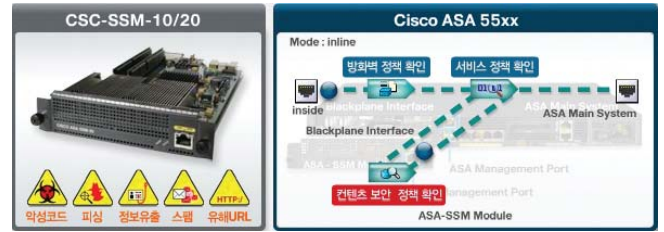


〈그림 1-6 Cisco ASA 5500 시리즈 방화벽 기반 위협탐지 및 차단 기능〉

또한 H/W 기반의 침입방지 또는 컨테츠 보안 모듈을 선택적으로 탑재하여 방화벽 정책에서 허용된 트래픽 일지라도 오염되거나 비정상적인 행위를 유발할 수 있는 트래픽을 차단하며, S/W기반으로 처리하는 경쟁사 솔루션과 달리 각 ASA 플랫폼이 낼 수 있는 최대 방화벽 성능을 보장할 수 있습니다.



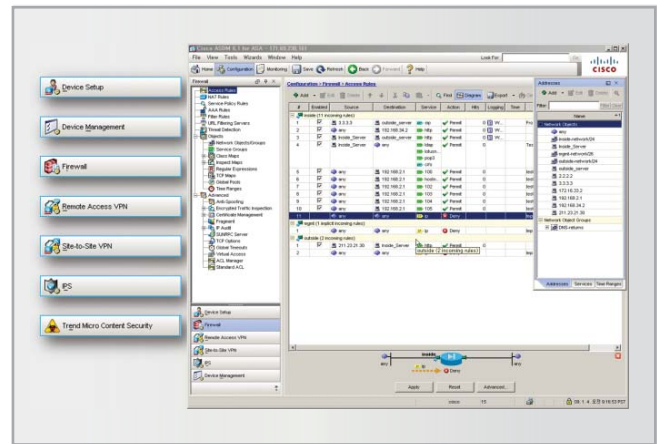
〈그림 1-7 Cisco ASA 5500 Series 침입방지모듈〉



〈그림 1-8 Cisco ASA 5500 Series 콘텐츠보안모듈〉

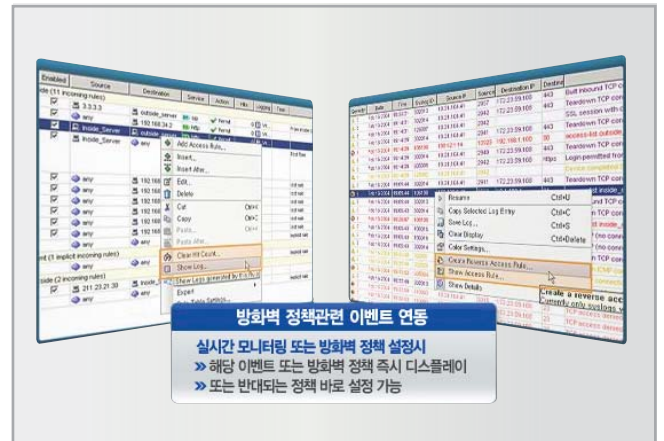
➔ ASDM을 통한 One-Stop Operation 기술

Cisco ASA 5500 시리즈 전 플랫폼에 무상으로 제공되는 GUI 타입의 관리인터페이스인 ASDM은 기본 설정에서 부터 각각의 통합 위협 관리 기능까지 하나의 GUI안에서 모두 설정 및 운영이 가능합니다. 특히 방화벽 정책 부분에서는 해당 GUI안에서의 Drag & Drop, Copy & Paste 와 같은 세세한 부분까지 신경을 썼으며, 적용되는 정책의 방향성과 적용 지점을 다이어그램으로 가시화 하여 운영자의 직관성을 높여 줍니다.



〈그림 1-9 ASDM 정책관리 화면〉

또한 방화벽 정책에 의해 발생하는 보안 이벤트에 대해서 간단한 마우스 조작만으로 쉽게 관련 보안 이벤트 필터링 및 관련 보안 정책 즉시 적용 기능을 제공하여 관리의 효율성을 극대화합니다.



〈그림 1-10 ASDM 정책관련 이벤트 연동 기술〉

장비정보	ASA 5505 Base / Security Plus	ASA 5520	ASA 5540	ASA 5550	ASA 5580-20	FWSM	ASA 5580-40
Device Image							
Product Part Number	ASA5505-BUN-K9 ASA5505-SEC-BUN-K9	ASA5520-BUN-K9	ASA5540-BUN-K9	ASA5550-BUN-K9	ASA5580-20-BUN-K9	WS-SVC-FWSM-K9	ASA5580-40-BUN-K9
Device Type	Appliance	Appliance	Appliance	Appliance	Appliance	Service Module	Appliance
제품 적용 산업군	SMB	소형 기업군	중소형 기업군	N/A	N/A	Catalyst 6500 / Cisco 7600	N/A
성능							
병화버 최대 성능	150 Mbps	450 Mbps	650 Mbps	12 Gbps	5 Gbps (real-world HTTP), 10 Gbps (jumbo frames)	55 Gbps	10 Gbps (real-world HTTP), 20 Gbps (jumbo frames)
병화버 최대 연속 세션	10,000 / 25,000	50,000 / 130,000	400,000	650,000	1,000,000	100,000,000	2,000,000
병화버 초당 커넥션 처리수	4,000	12,000	25,000	36,000	90,000	100,000	150,000
병화버 최대 패킷 처리 성능	85,000	190,000	500,000	600,000	2,500,000	2,800,000	4,000,000
VPN 성능	100 Mbps	170 Mbps	325 Mbps	425 Mbps	1 Gbps	N/A	1 Gbps
최대 VPN Session 지원	107/25	250	750	5000	10000	N/A	10000
최대 SSL VPN 접속 지원	25	250	2,500	5000	10,000	N/A	10,000
기본 SSL VPN 사용 지원	2	2	2	2	2	N/A	2
메모리 / 인터페이스							
Memory	256 MB	512 MB	1 GB	4 GB	8 GB	1 GB	12 GB
기본 System Flash 지원	64 MB	64 MB	64 MB	64 MB	1 GB	20MB	1 GB
물리적 포트 제공	8 port 10/100 switch (2개 PoE Port 제공)	4개 10/100/1000, 1개 10/100	4개 10/100/1000, 1개 10/100	8개 10/100/1000 4개 SFP & 1개 10/100	2개 10/100/1000 Management	관리용 (Catalyst 6500, Cisco 7600 모든 Interface 사용 가능)	2개 10/100/1000 Management
확장 물리적 포트 제공	N/A	4개 10/100/1000 & 4 SFP (4GE SSM)	4개 10/100/1000 & 4 SFP (4GE SSM)	N/A	4-10/100/1000 (with ASA5580-4GE-CU) 4 GE SR LC (with ASA5580-4GE-FI) 2 10GE SR LC (with ASA5580-2X10GE-SR)	제일 많은 (Catalyst 6500, Cisco 7600 모든 Interface 사용 가능)	4-10/100/1000 (with ASA5580-4GE-CU) 4 GE SR LC (with ASA5580-4GE-FI) 2 10GE SR LC (with ASA5580-2X10GE-SR)
최대 지원 VLAN Interface	3 (Trunk disabled) /20 (Trunk enabled)	50 /100	200	250	100 (향후 250 개 지원 예정)	1000	100 (향후 250 개 지원 예정)
확장 옵션							
SSC/SSM/IC Expansion	1개 SSC Card 지원	1개 SSM Module 지원	1개 SSM Module 지원	N/A	6개 인터페이스 카드 지원	N/A	6개 인터페이스 카드 지원
SSC/SSM/ICs supported	SSC 지원 예정	CSC SSM, AP SSM, 4GE SSM Yes (AP SSM)	CSC SSM, AP SSM, 4GE SSM Yes (AP SSM)	N/A	4-10/100/1000, 4GE SR LC, 2-10GE SR LC	N/A	4-10/100/1000, 4GE SR LC, 2-10GE SR LC
Intrusion Prevention	N/A	Yes (AP SSM)	Yes (AP SSM)	N/A	N/A	N/A	N/A
Firewall+IPS 성능	N/A	225 Mbps (AP SSM-H0) 375 Mbps (AP SSM-20) 450Mbps (with AP SSM-40)	500 Mbps (AP SSM-20) 650 Mbps (AP SSM-40)	N/A	N/A	N/A	N/A
바이러스 및 지민 (anti-virus, antispysware, file blocking)	N/A	Yes (CSC SSM)	Yes (CSC SSM)	N/A	N/A	N/A	N/A
바이러스 및 회대 지원 User 수	N/A	500 (CSC-SSM-H0) 1000 (CSC-SSM-20)	500 (CSC-SSM-H0) 1000 (CSC-SSM-20)	N/A	N/A	N/A	N/A
바이러스 및 회대 지원	N/A	Anti-spam, anti-phishing, URL filtering	Anti-spam, anti-phishing, URL filtering	N/A	N/A	N/A	N/A
기타 사항							
Software Version	8.0	8.0	8.0	8.0	8.1	4.0.2	8.1
L7 병화버 기능 지원	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bridge Mode & Routed Mode 병화버 지원 여부	Yes	Yes	Yes	Yes	Yes	Yes	Yes
기상병화버 지원 (기본제공/최대)	N/A	기본은 제공하지 않음 기본 3개/최대 5개	기본 3개/최대 50개	기본 3개/최대 50개	기본 3개/최대 50개	기본 3개/최대 250개	기본 3개/최대 50개
GTP/GPRS inspection 지원	N/A	N/A	Yes	Yes	Yes	Yes	Yes
이중화 구성 지원	N/A	Security Plus Active/Standby	Active/Active Active/Standby	Active/Active Active/Standby	Active/Active Active/Standby	Active/Active Active/Standby	Active/Active Active/Standby
SSL and Psec VPN services	Yes	Yes	Yes	Yes	Yes	N/A	Yes
VPN clustering and load balancing	N/A	기본은 제공하지 않음 Yes	Yes	Yes	Yes	N/A	Yes

네티크루즈사 LogSee for Cisco Security Product (CSP)

제품 소개

정보관리솔루션 전문 공급사인 네티크루즈사(www.netcruz.co.kr)의 LogSee for CSP 제품(NLM Series)은 Cisco ASA / FWSM 전용 로그 분석솔루션으로서 All-in-One 형태의 통합로그 관리시스템입니다. Cisco ASA 및 FWSM의 로그에 대한 Filter Pack 번들링 및 기술지원을 포함하고 있으며, 네티크루즈사 LogSee만의 특화된 Intelligent Log Search 엔진을 기본 탑재하여 최소한의 비용으로 효과적인 로그 관리 및 고속 검색기능을 제공할 수 있어 기업 보안 운영의 효율성을 높여 드릴 것입니다.

주요 특징

▶ 초간편 설치

편리한 Wizard기능으로 간단히 모든 설치가 완료됩니다. ASA, FWSM에 대해 추가 설정이 필요하지 않으며, 로그 유형이 변경되더라도 사용자가 직접 인덱싱, 정형화 설정을 변경할 수 있어 지속적으로 로그 수집 및 분석이 가능하도록 지원합니다.

▶ 자동 Device 인식

로그 발생 대상 장비를 자동으로 인식하여 대상 장비들을 일일이 등록하는 관리자의 수고를 덜어 줍니다.

▶ 지능형 로그 검색 엔진 적용 시스템

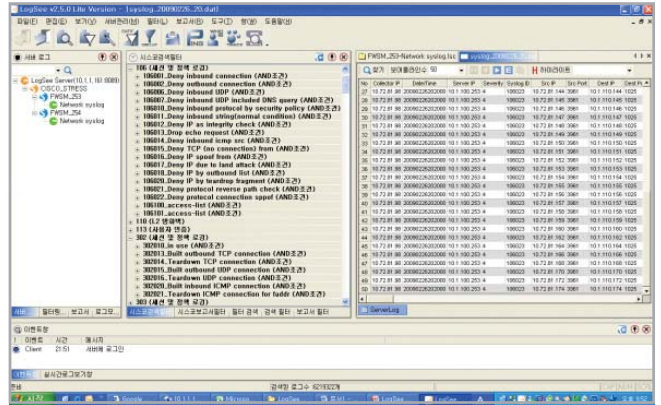
대용량 로그의 검색을 위한 Database의 단점을 극복하기 위하여 로그 전용 검색엔진(ILS)을 채용하였습니다. 장기간/대용량 로그에 대한 고속 검색, 이기종간 cross-text search, 백업데이터의 복구시 즉시 검색 기능을 제공합니다.



〈그림 2-1 LogSee Lite for CSP ILS엔진 실행화면〉

▶ Cisco 방화벽에 특화된 한글 Filter Pack 지원

Cisco 방화벽 로그는 타사보다 상세한 분류와 정보를 제공하고 있습니다. 따라서 LogSee Lite for CSP 는 시스템 레벨에서 특화된 한글 Filter Pack을 통해 Cisco ASA 및 FWSM의 로그를 쉽게 분석하도록 도와 줍니다.



〈그림 2-2 LogSee Lite for CSP 한글 Filter Pack〉

▶ Forensic 지원 시스템

로그 분석의 핫 이슈인 Forensic 프로세스를 수집부터 보관까지 적용함으로써, 이슈 발생시 Forensic기반의 보고서를 활용할 수 있습니다.

▶ 최소비용 Compliance 대응 시스템

Compliance이슈를 대응함에 있어, 고가의 타 제품과 달리 하나의 플랫폼에서 All-in-One 시스템으로 동작함으로써, 총 소요비용 절감 및 장애포인트를 최소화하며, 보관주기, 주기적 삭제, 백업 등 관리자의 필요 업무요건을 충족합니다.

▶ 상시감사 및 오남용 분석 기능

관리자는 상시적인 보고서 기반 분석 모니터링을 실행함으로써 비정상 패턴이나 데이터 증/감을 발견하고 IT infra 및 조직의 활동 감사를 할 수 있습니다.

제품 구성

Model	NLM-200	NLM-500
동작방식	Client / Server	
지원방식	Syslog (UDP)	
ILS engine	탑재	
지원 Cisco ASA 및 FWSM	ASA 5505, 5510, 5520	ASA 5540, 5550, FWSM
Devices	2 (Max 4)	2 (Max 4)
Max EPS	2,000	3,600

권장시스템 사양

Model	NLM-200	NLM-500
지원 OS	Windows Server 2003 이상	
CPU	1xIntel Core 2 Duo 2,6GHz 이상	1xZeon Core Duo 2,0GHz이상
RAM	2GB	2GB
Storage	1 x 160 GB	3 x 500 GB -- RAID0,5
Interfaces	1GE	2GE

네티크루즈사 담당자 및 연락처

	김한수 부장	Email	sales@netcruz.co.kr
Office	82-2-869-4123(Ext. 112)	M,P	010-3296-4369



www.cisco.com/kr
시스코 코리아 콜센터
시스코 코리아
Cisco Korea

080-808-8082
서울특별시 강남구 삼성 1동 아셈타워 5층 (135-798) Tel.02-3429-8000 Fax.02-3429-0851
5F ASEM Tower, Samsung 1-dong, Gangnam-gu, Seoul, Korea (135-798)