시스코 ASA5500 UTM 솔루션 웹 세미나

Cisco Korea
Yong-Ho Kim(yonghkim@cisco.com)

목차

- Why Cisco?
- 시스코 차세대 DDoS 솔루션
- 시스코 UTM 솔루션 – ASA 5500 Series
- Summary
- Q&A

Why Cisco?

용감했던 네덜란드 소년 이야기

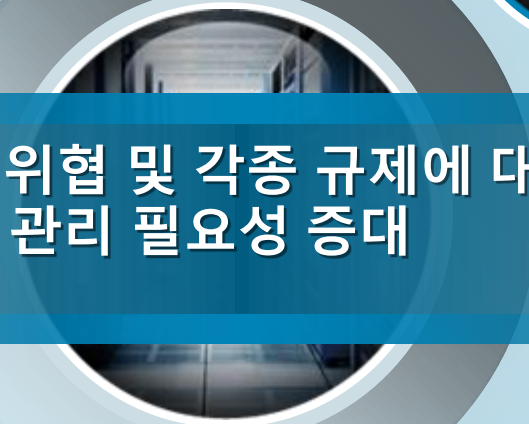
현실세계에서 벌어지고 있는 사태들…

- 대내외 서비스 중단 사태
- 내부자 불법 자료 유출
- 외부 데이터 노출
- 기업의 신뢰도 실추

IT 기반 보안 솔루션에 대한 요구 사항의 변화

규정 준수

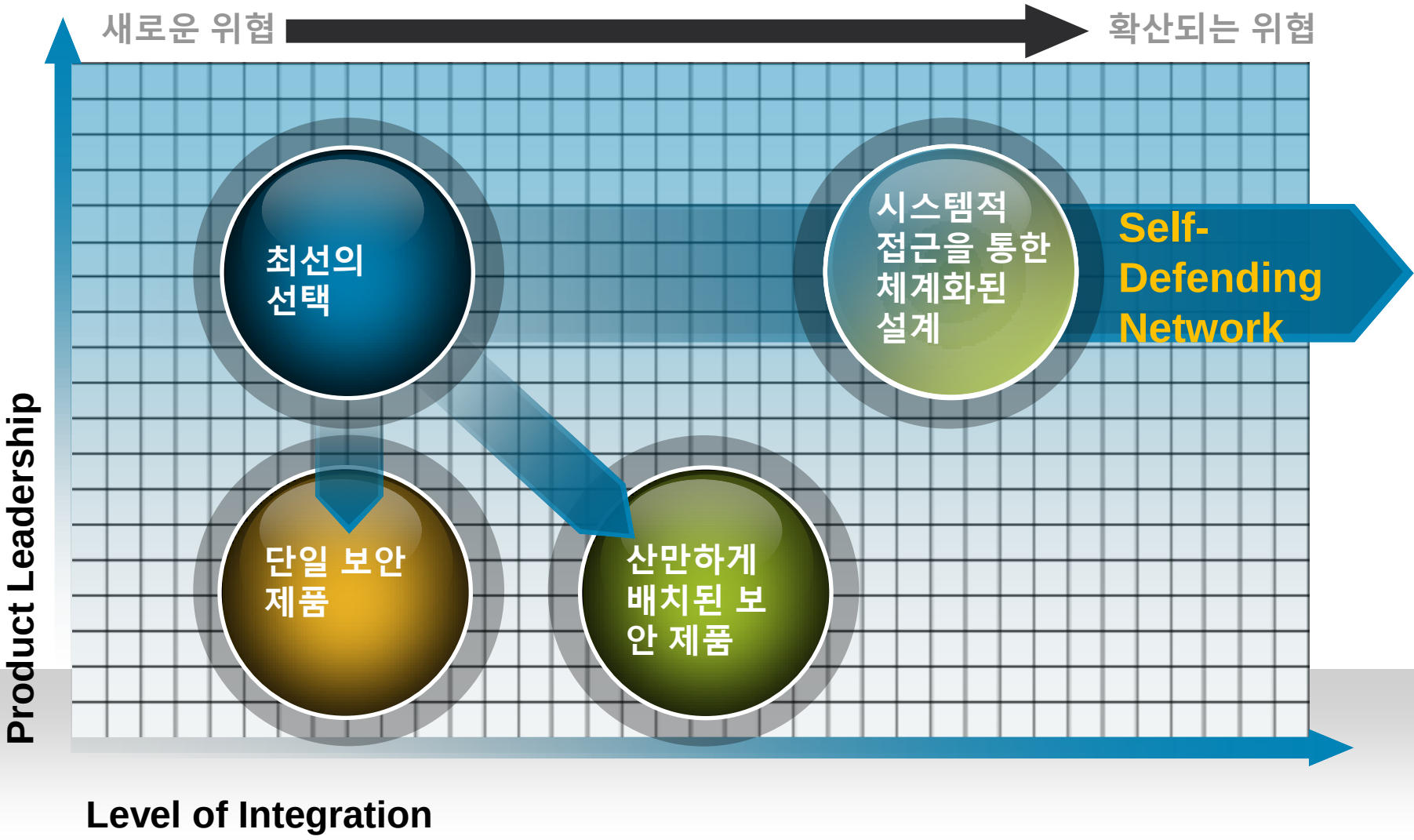
데이터 유출



다양해진 보안 위협 및 각종 규제에 대한 IT 기반의
시스템적 Risk 관리 필요성 증대

Malware
DDoS

시스템적 접근을 통한 체계적인 보안설계 필요성 증가



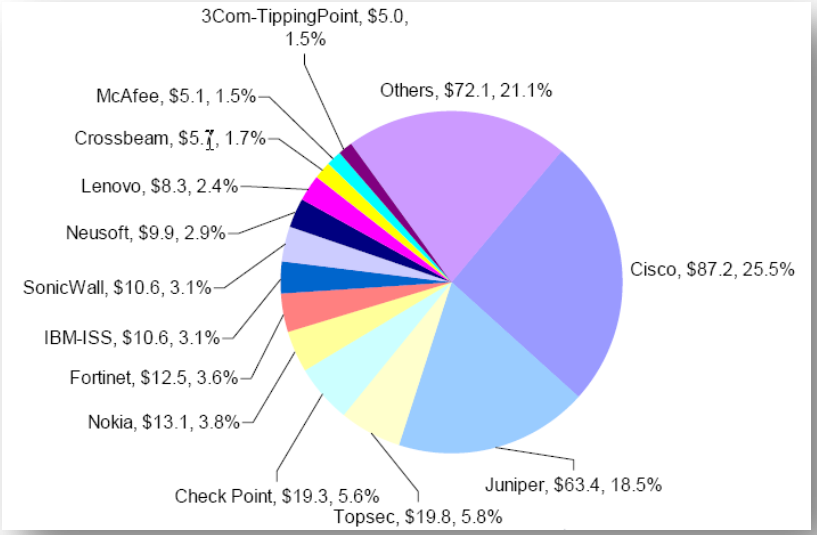
Cisco Self-Defending Network

- 기업의 보안 정책 또는 비즈니스 규정 준수 및 중요 자산에 대한 완벽한 보호
- IT관리자 또는 보안 담당자의 관리적 업무부담 감소 및 비용 절감
- IT 기반의 보안 및 규정 위배에 대한 철저한 대응

ASIA/Global No1 보안 솔루션 벤더 = Cisco

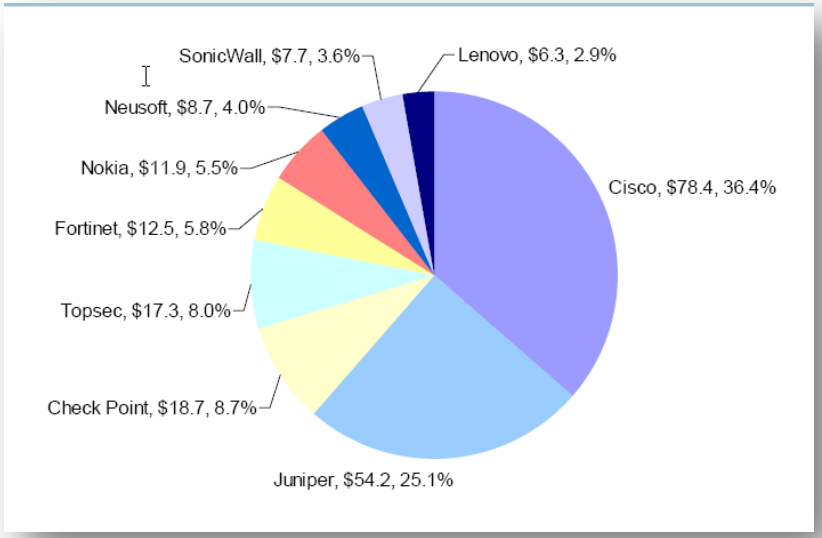
Network Security Market

- Firewall/IPSec VPN, SSL VPN, IDS/IPS 총괄
- Cisco No 1. 25.5 %



Firewall/IPSec VPN Market

- ASA 5500 Series, PIX 500 Series, IOS Based Firewall/VPN
- Cisco No 1. 36.4%



자료출처: Frost & Sullivan Executive Summary – APAC (excluding Japan) Network Security Market Q2 2008
단위 : Million $

시스코 UTM 솔루션
– ASA 5500 Series

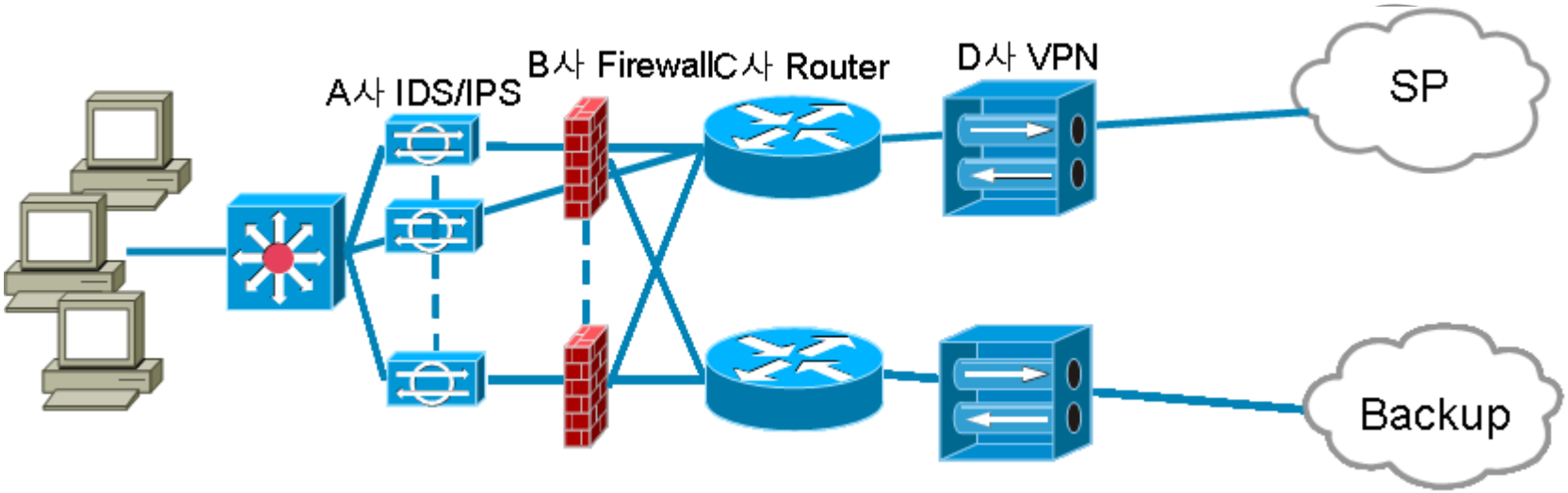
UTM 이란?

UTM = Unified Threat Management, 통합 위협 관리 솔루션

방화벽과 VPN, 침입방지, 바이러스 차단 등 여러 가지 보안 기능을 동시에 제공하는 네트워크 어플라이언스 장비

UTM의 필요성과 Cisco UTM 의 활용

- Cisco UTM – ASA 5500 Series의 활용



효과적인 기업의 보안방안은?

시스코 UTM – ASA 5500 Series

시장에서 입증된 기술기반 강력한 통합위협관리 솔루션 제공

시장에서 입증된 Cisco 보안솔루션

방화벽 기술
Cisco PIX

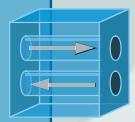
침입탐지/방지 기술
Cisco IPS

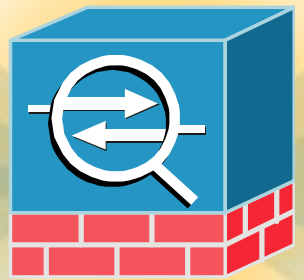
컨텐츠 보안 기술
Trend Micro

VPN 기술
Cisco VPN 3000

지능형 네트워크 기술
Cisco Network Services



새로운 보안위협 방어 및 안전한 보안연결

응용프로그램 감시 및 오용차단, 웹보안
어플리케이션 보안엔진

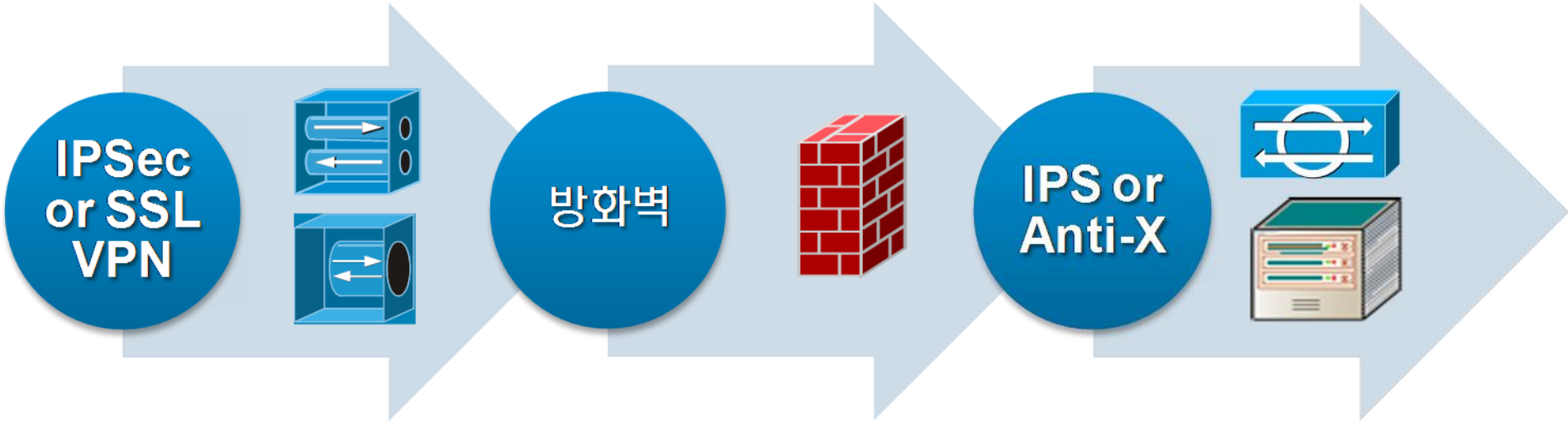
악성프로그램 및 컨텐츠 방어, 비정상 트래픽 차단
침입탐지/방지 및 컨텐츠 보안 엔진

트래픽 제어 및 접근통제
QoS 기술 및 NAC 연동

다양한 보안 연결
IPSec & SSL VPN

시스코 UTM – ASA 5500 Series

UTM 솔루션으로써의 Traffic Flow



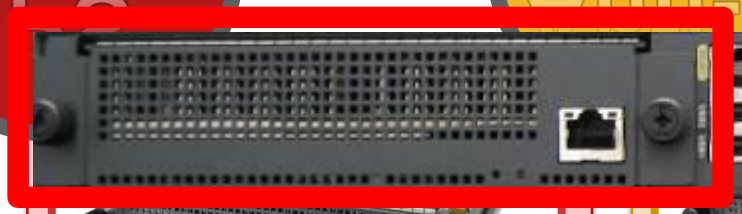
시스코 UTM 솔루션 – ASA 5500 Series

기능 확장 모듈(선택적 사양)

IPS

Anti-X

Interface



Cisco ASA 5500 Series Advanced Inspection and Prevention Module (AIP SSM)

Cisco ASA 5500 Series Content Security and Control Module (CSC SSM)

Cisco ASA 5500 Series 4-Port GE Services Module (4GE SSM)

심층적인 보안 또는 네트워크 확장성 제공

시스코 UTM 솔루션 – ASA 5500 Series

침입탐지 및 방지 기능(IDS/IPS)

IPS

Cisco ASA 5500 Series Advanced Inspection and Prevention Module (AIP SSM)

플랫폼 별 최대 성능

AIP-SSM-10	AIP-SSM-20	AIP-SSM-40
▪ 150 Mbps with Cisco ASA 5510	▪ 375 Mbps with Cisco ASA 5520	▪ 450 Mbps with Cisco ASA 5520
▪ 225 Mbps with Cisco ASA 5520	▪ 450 Mbps with Cisco ASA 5540	▪ 650 Mbps with Cisco ASA 5540

주요 기능

다중 분석 기반 위협 방어

- 원 터치 침입방지 룰 최적화
- 비정상 트래픽 탐지 및 방어
- 어플리케이션 오용 및 남용 찬단
- Traffic Cleansing

Cisco IPS v6.0 기능 Full Integrated

시스코 UTM 솔루션 – ASA 5500 Series

컨텐츠 보안(Anti-X) 기능

Cisco ASA 5500 Series Content Security and Control Module (CSC SSM)

플랫폼 별 최대 사용자

CSC-SSM-10

- 50 User
- 100 User
- 250 User
- 500 User

CSC-SSM-20

- 500 User
- 750 User
- 1,000 User

주요 기능

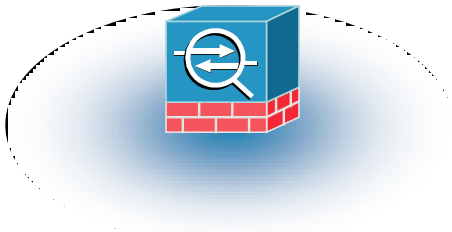
컨텐츠기반 Anti-X 기능 제공

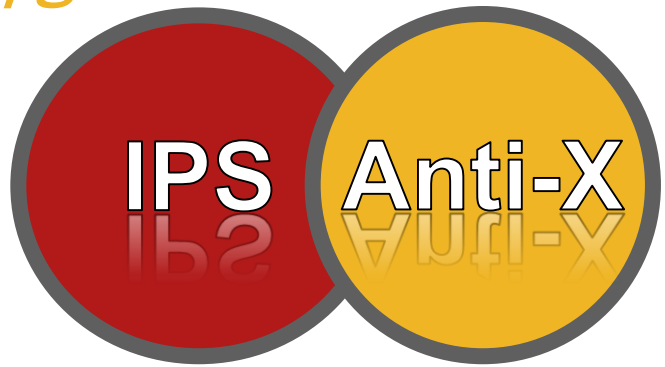
- 기본라이센스
  - –파일 기반 안티바이스 및 안티스파이웨어 기능
- 플러스 라이센스
  - –안티 스팸, 컨텐트필터링, 안티피싱, URL 필터링 및 블록킹

Trend Micro 의 최신 컨텐츠보안 엔진 통합

시스코 UTM 솔루션 – ASA 5500 Series

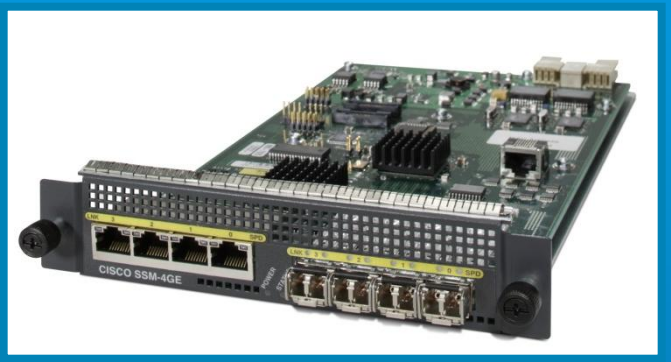
보안모듈 선택시 고려사항





Focus	네트워크 기반의 주요 **서버 보호**	사용자 컨텐츠 기반의 **사용자 보호**
Threats	네트워크 웜 확산, 해킹 시도, 백도어, 봇, 프로토콜 오용 및 남용 방어 트래픽 패턴 기반의 비정상적인 트래픽 방어	파일 기반의 바이러스, 스파이웨어 애드웨어, 그레이웨어 악성파일 방어 스팸, 피싱, 컨텐츠 보안, URL 필터링 및 블록킹
Markets	지사 및 중규모 기업	Commercial, 중소규모의 기업 및 지점
Pricing	대역폭 기반, 연간 서비스 라이센스 겡신 필요	사용자수 기반, 연간 서비스 라이센스 갱신 필요

시스코 UTM 솔루션 – ASA 5500 Series
확장 인터페이스 기능(4GE)



Cisco ASA 5500 Series 4-Port GE Services Module (4GE SSM)

주요 기능

유연한 네트워크 디자인

- **4개의 copper 10/100/1000 포트 및 4개의 SFP 포트 제공 총 4개의 Cooper와 Optic 기반의 포트 선택적 조합 가능**
- **ASA 5510, 5520, 5540 and 5550 장착 가능**

다양한 인터페이스 타입 제공

시스코 UTM 솔루션 – ASA 5500

Product Lineup

	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550
					
대상 시장	Teleworker / Branch Office / SMB	SMB and SME	Enterprise	Medium Enterprise	Large Enterprise
성능					
최대 방화벽 성능	150 Mbps	300 Mbps	450 Mbps	650 Mbps	1.2 Gbps
최대 방화벽 + IPS 성능	Future	300 Mbps	375 Mbps	450 Mbps	N/A
최대 IPSec VPN 성능	100 Mbps	170 Mbps	225 Mbps	325 Mbps	425 Mbps
최대 IPSec/SSL VPN Peers	25/25	250/250	750/750	5000/2500	5000/5000
Platform Capabilities					
최대 동시 연결 세션수	10,000/25,000	50,000/130,000	280,000	400,000	650,000
최대 초당 연결 세션수	3,000	6,000	9,000	20,000	28,000
Packets/Second (64 byte)	85,000	190,000	320,000	500,000	600,000
기본 인터페이스	8-port FE switch	5 FE	4 GE + 1 FE	4 GE + 1 FE	8 GE + 1 FE
VLANs 지원	3/20 (trunk)	50/100	150	200	250
고가용성 지원	Stateless A/S (Sec Plus)	A/A and A/S (Sec Plus)	A/A and A/S	A/A and A/S	A/A and A/S

ASDM v 6.1

ASDM 이란?

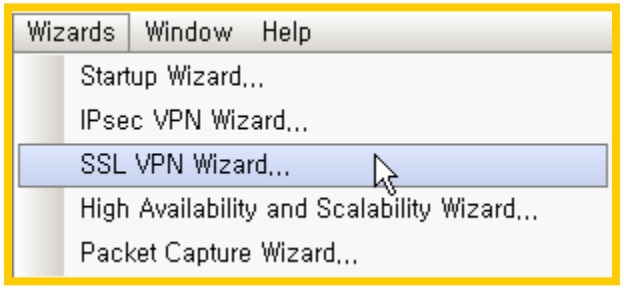
- Cisco의 FWSM 및 ASA 장비에 Built-in 된 GUI 기반의 관리 툴
- FWSM 용 ASDM과 ASA 용 ASDM은 기능과 버전이 조금씩 다르며 FWSM용의 경우 버전 끝에 “f” 가 붙음
  - FWSM 용 : FWSM 3.x 이후 부터 ASDM 6.x(x)f 버전 사용 가능
  - ASA 용 : ASA 7.x 이후 부터 ASDM 6.x(x) 버전 사용 가능

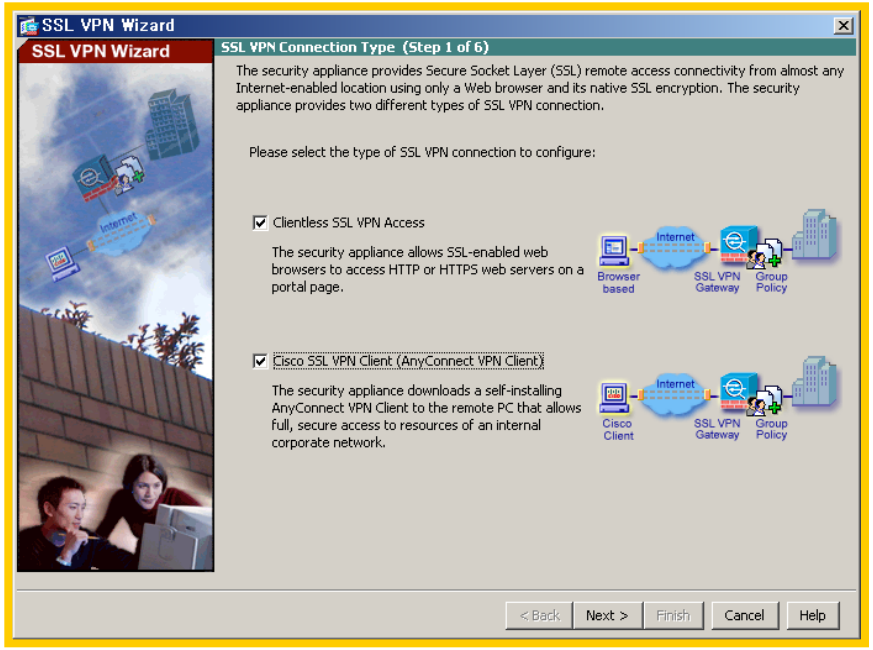
ASDM v6.1 주요 기능 소개

다양한 Wizard 기능 제공

- 직관적인 그림 및 설명과 함께 간편하고 쉽게 완성할 수 있음
- Startup, IPSec VPN, SSL VPN , HA 구성, Packet Capture 5가지에 대한 Wizard 제공

(단, FWSM의 경우 Startup Wizard 만 지원)

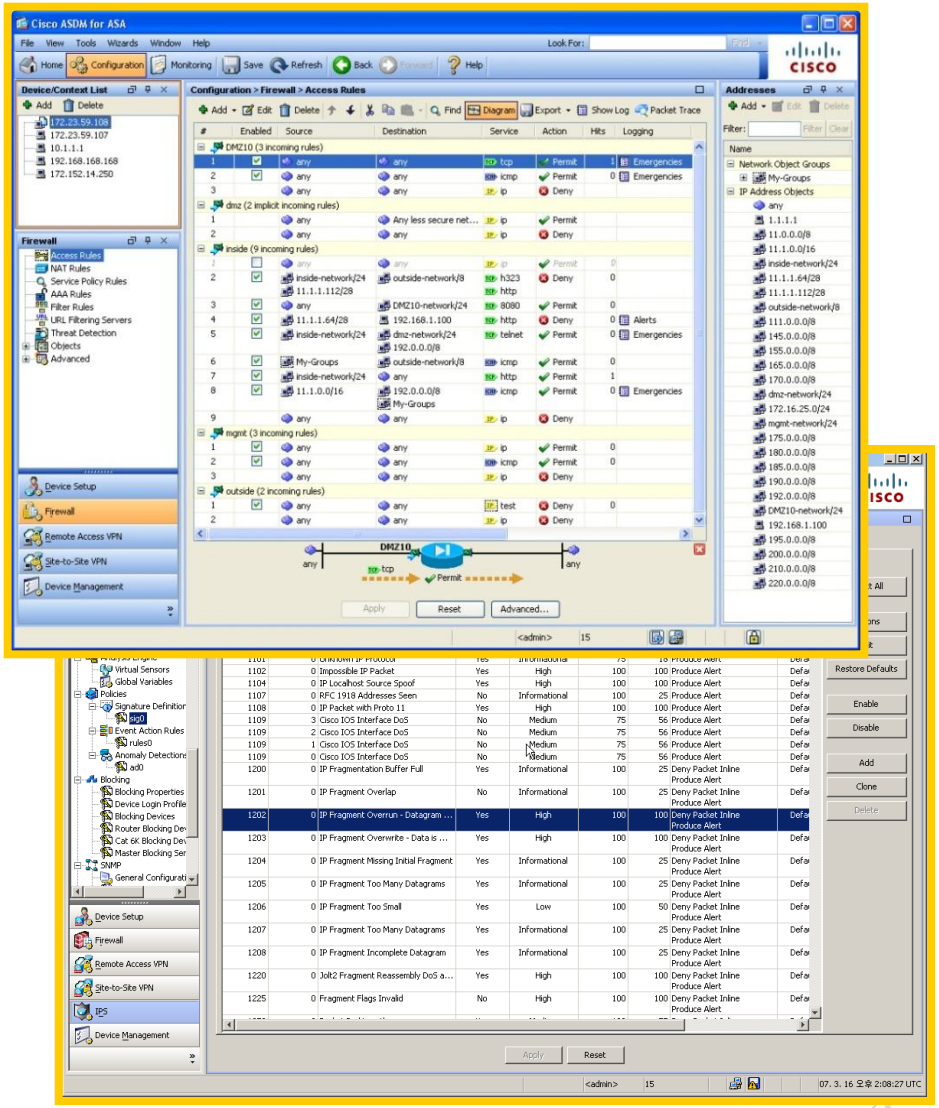




ASDM v6.1 주요 기능 소개

직관적인 보안 정책 설정

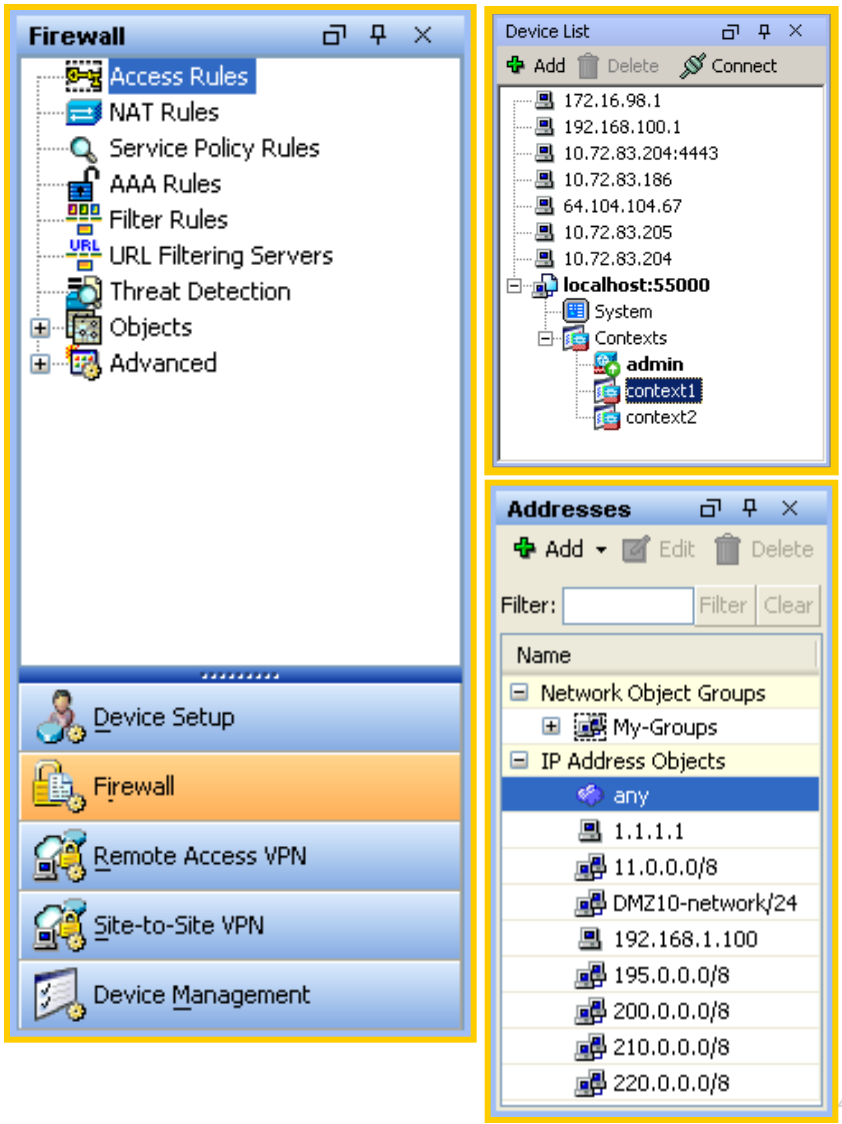
- 각 오브젝트에 대한 Copy&Pase, Drag&Drop등 간편하게 작성 가능
- Diagram을 통한 적용되는 정책의 방향성을 직관성있게 제시
- 방화벽 정책테이블 내에서 각 정책별 Hit Count 에 대한 실시간 업데이트 기능 제공
- IPSec/SSL VPN, IPS 및 Anti-X에 대한 모든 설정을 하나의 GUI 로 가능



ASDM v6.1 주요 기능 소개

편리한 사용자 정의 판넬

- MS 아웃룩 Look&Feel의 익숙한 인터페이스 제공
- 각 기능별 판넬들을 고정, 숨기기 및 없애기 가능
- 특히 Device List 판넬에서 관리대상 Device 또는 가상 방화벽에 대한 연결을 ASDM 추가 실행없이 쉽게 전환 가능

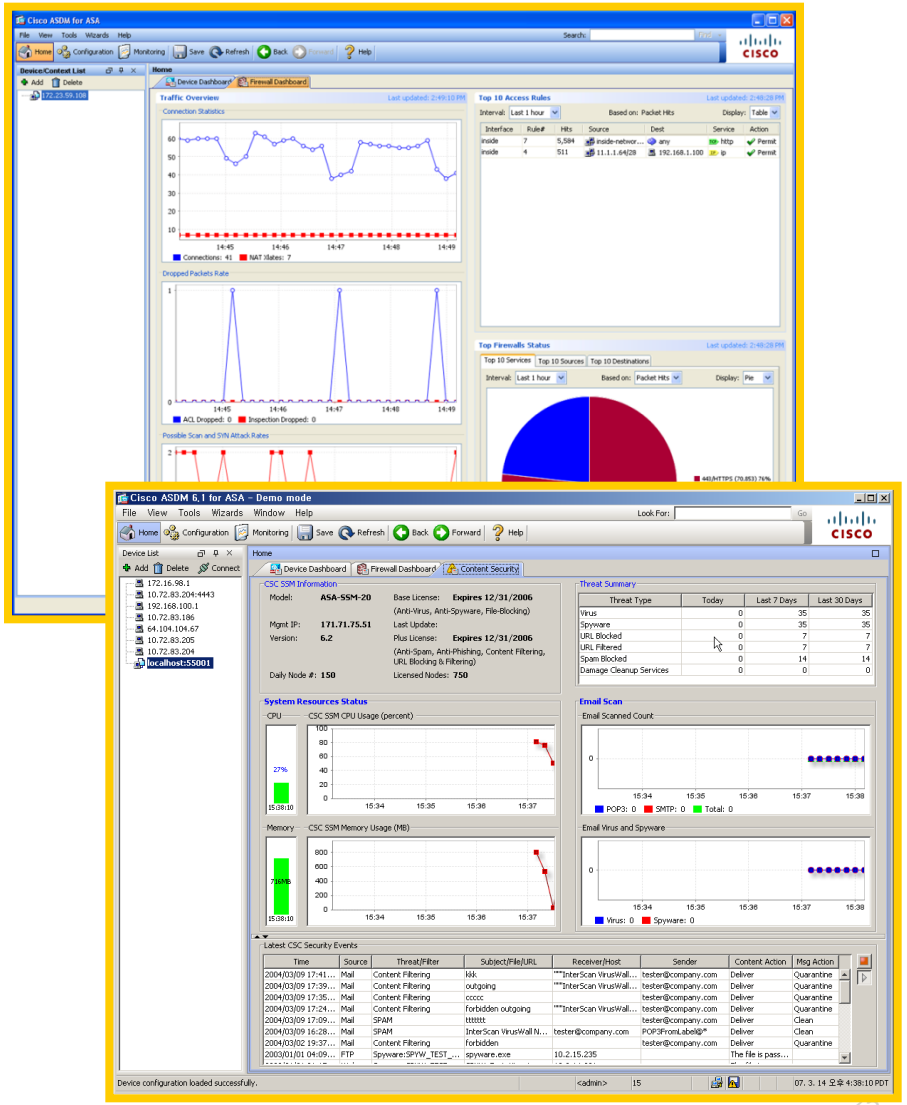


ASDM v6.1 주요 기능 소개

Security Dashboards

- Firewall, IPS, Anti-X 에 대한 Dashboard 제공
- 각각의 기능에 대한 실시간 리소스 사용 통계 그래프 및 상태 표시

(단, ASA에서만 지원함)

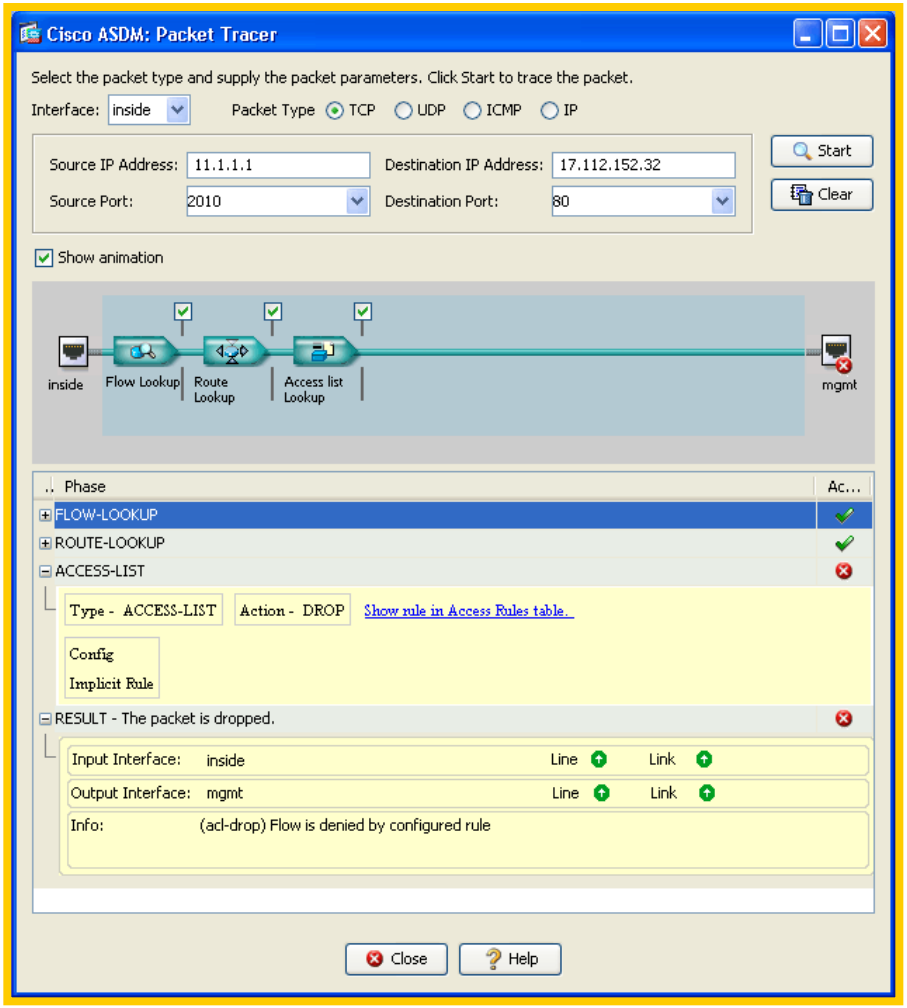


ASDM v6.1 주요 기능 소개

Packet Tracer

- 사용자가 입력한 세션에 대한 보안 기능 적용 유무를 가상으로 시뮬레이션
- 현재 동작 중인 Config 를 기반으로 어떠한 보안기능(L2, L3 Network 설정, Firewall 정책, IPS 모듈 정책, Anti-X 모듈정책 등)에 의해 허용/차단되는 지를 미리 확인할 수 있음

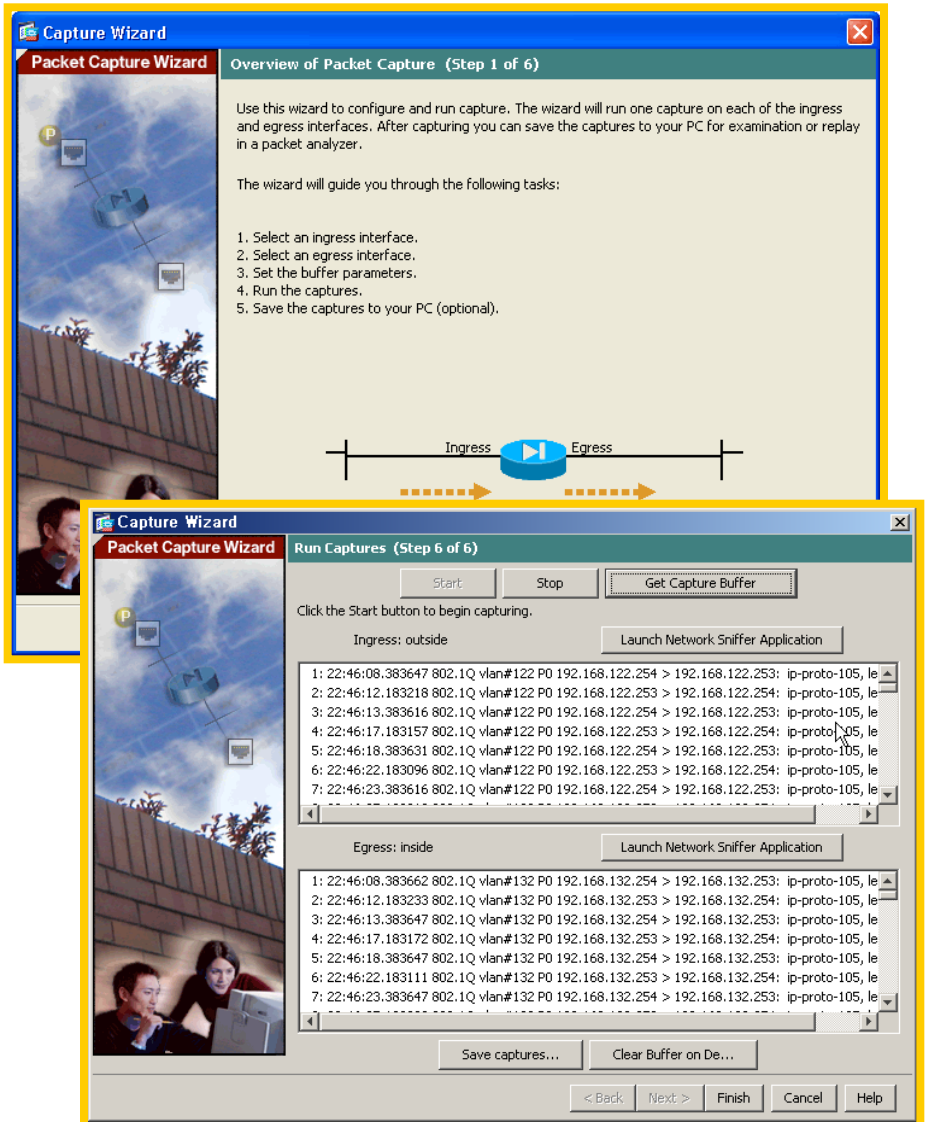
(단, ASA에서만 지원함)



ASDM v6.1 주요 기능 소개

Packet Capture Wizard

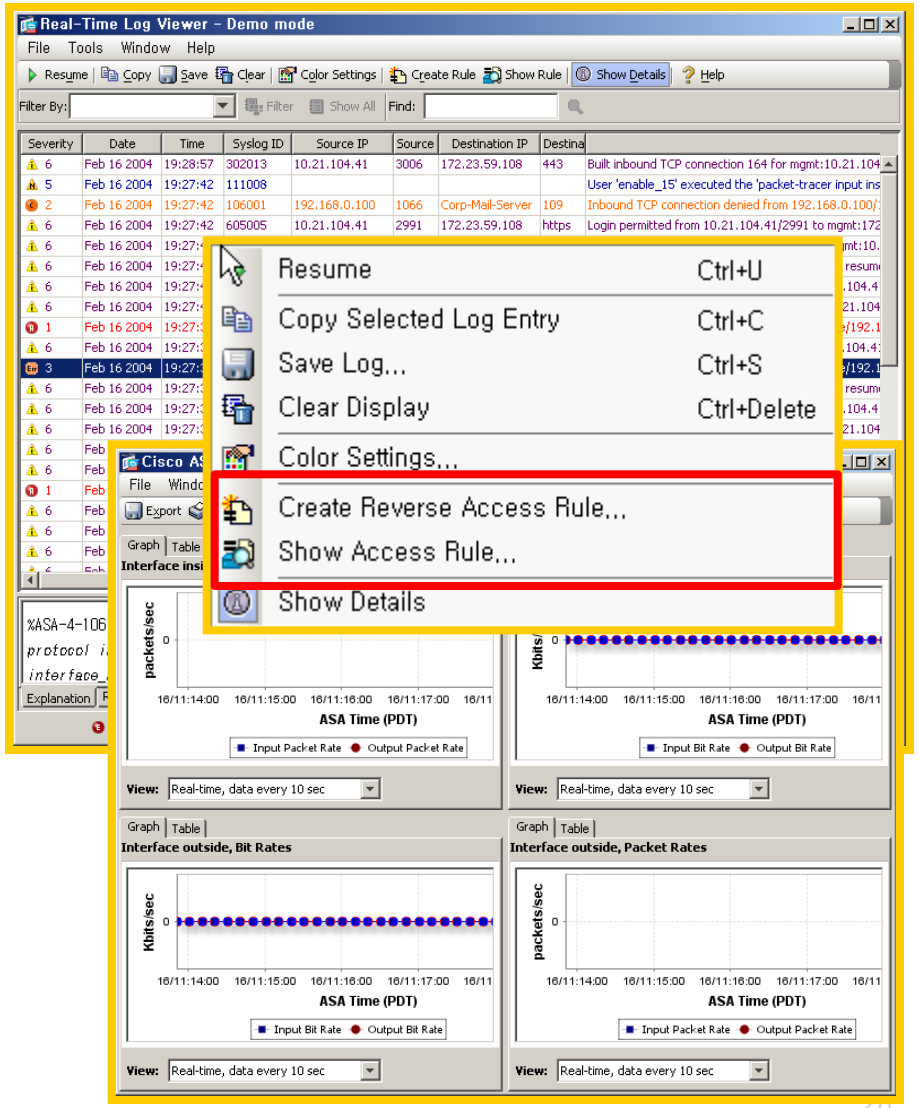
- ASA에 트래픽이 도달한 시점 부터 Law Level 의 패킷 캡처링 기능 지원
- ACL에 의한 특정 세션 지정 캡처 및 Real-Time View 기능 지원
- Law Level Data를 전문으로 분석하는 툴을 지정할 경우 자동 실행 지원



ASDM v6.1 주요 기능 소개

강력한 실시간 모니터링

- 실시간 Syslog 모니터링 및 각 기능 사용 통계 그래프 기능
- 실시간 Syslog 모니터링시 One-Click 차단 또는 해당 룰 수정 기능 제공



ASDM 데모 모드란?

ASDM 데모 모드란?

- ASDM 을 Local PC 내에서 가상으로 실행되는 형태로,
- FWSM이나 ASA 장비를 연결하지 않고 연습 또는 기능의 확인 등을 목적으로 실행해볼 수 있음
- 데모 모드에서 수정 또는 새로이 생성한 설정은 저장 되지 않음
- 실행 가능한 데모 모드는 설치하는 버전에 따라 달라질 수 있음

ASDM Demo 설치를 위한 시스템 요구 사항

Operating System	Version	Browser
Microsoft Windows	Windows Vista Windows 2003 Server Windows XP Windows 2000 (Service Pack 4)	Internet Explorer 6.0 or 7.0 with Sun Java SE Plug-in 1.4.2, 5.0 (1.5.0), or 6.0 Firefox 1.5 or 2.0 with Java SE Plug-in 1.4.2, 5.0 (1.5.0), or 6.0
Apple MacIntosh	Apple MacIntosh OS X	Firefox 1.5 or 2.0 or Safari 2.0 with Java SE Plug-in 1.4.2, 5.0 (1.5.0), or 6.0
Linux	Red Hat Desktop, Red Hat Enterprise Linux WS version 4 running GNOME or KDE	Firefox 1.5 or 2.0 with Java SE Plug-in 1.4.2, 5.0 (1.5.0), or 6.0

ASDM Demo Mode 기능 소개

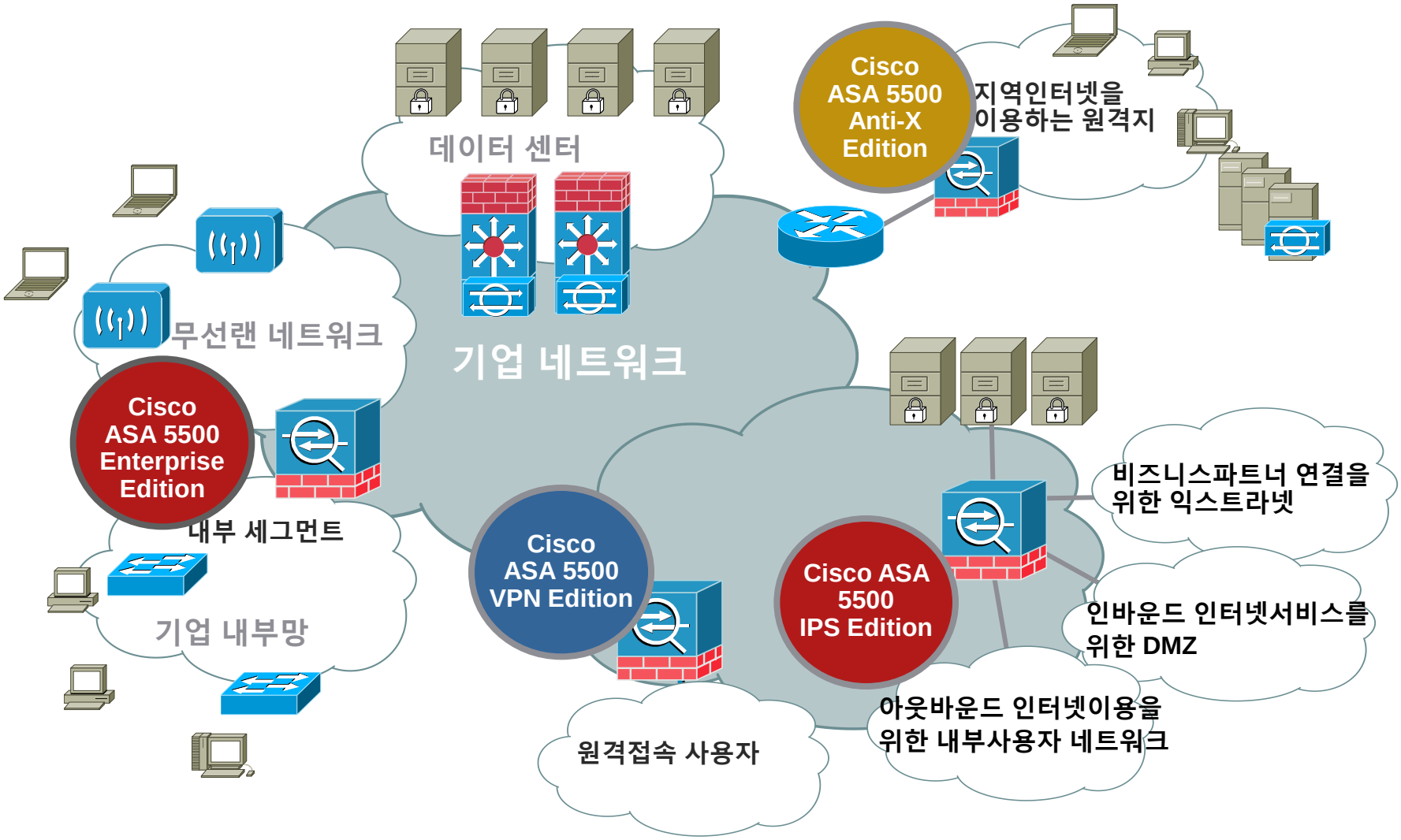
데모모드에서 지원 가능한 기능

- ASDM 등록 정보 및 자체 기능 데모
- ASA 또는 FWSM 의 설정 및 모니터링에 대한 대부분의 기능 데모
- IPS 모듈(AIP-SSM) 및 Anti-X 모듈(CSC-SSM) 설정 및 모니터링에 대한 대부분의 기능 데모 (FWSM제외)
- 가상의 로그 데이터를 랜덤하게 생성하여 Real-Time Syslog 모니터링 데모

데모 모드에서 제한된 기능

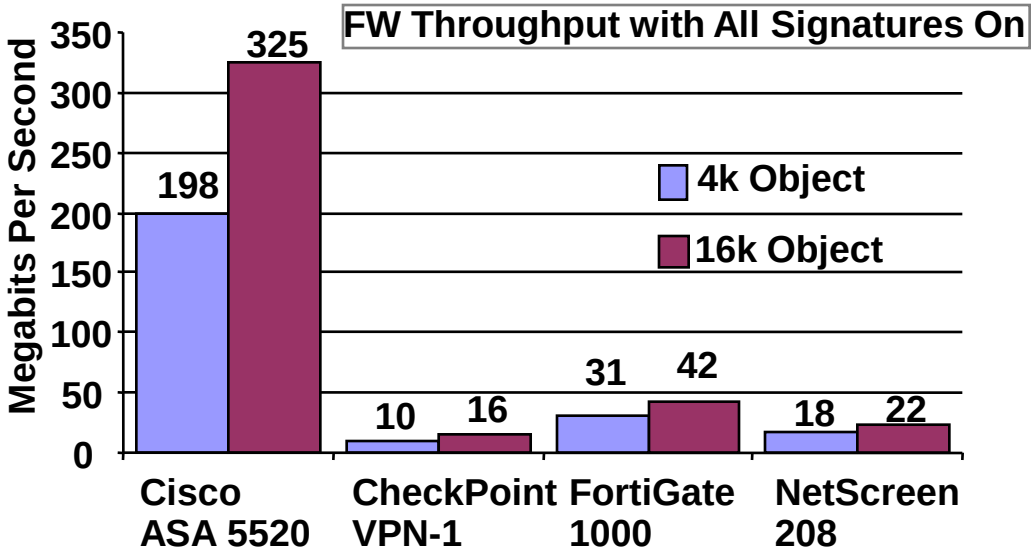
- 데모모드상에서 변경 또는 생성한 설정 저장 기능
- ASA 또는 FWSM에 대한 파일 및 디스크 관련 운영 기능
- Admin 권한 이외의 권한 사용자 운영 기능(예: Monitor Only, Read Only)
- File menu 상의 다음 기능
  - Save Running Configuration to Flash
  - Save Running Configuration to TFTP Server
  - Save Running Configuration to Standby Unit
  - Save Internal Log Buffer to Flash
  - Clear Internal Log Buffer
- Tools menu상의 다음 기능
  - Command Line Interface
  - Ping
  - File Management
  - Update Software
  - File Transfer
  - Upload image from Local PC
  - System Reload
- Toolbar/Status bar > Save
- Configuration > Interface > Edit Interface > Renew DHCP Lease
- Configuring a standby device after failover

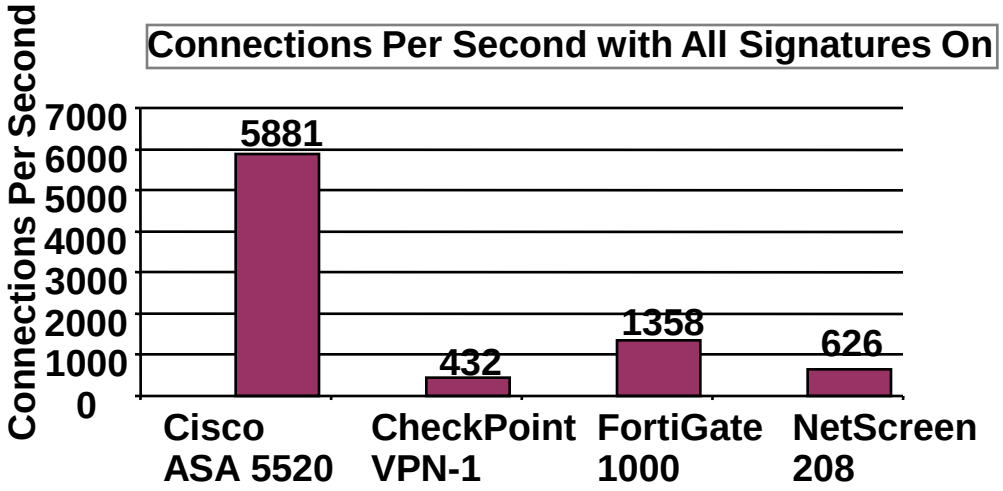
시스코 UTM – ASA 5500 Series 의 구성



Why Cisco UTM – ASA 5500 Series?

외부기관에 의해 공인된 타사대비 성능 우수성





테스트 환경

- 방화벽 + 인라인 IPS Full 기능 적용
- 방화벽 및 IPS 통과 성능 테스트

테스트 결과

- 최대 6배 이상의 Throughput 성능
- 최대 3배 이상의 VPN Throughput 성능
- 최대 4배 이상의 초당 연결 개수

Full Report:
http://www.miercom.com/dl.html?fid=20050914&type=report

Why Cisco UTM – ASA 5500 Series?

차별화된 CC인증 기반의 방화벽 기능 기본 지원

- 같은 등급의 CC인증이라 할지라도 내부적인 주요 기능 항목에 대한 차별성이 존재

	Cisco ASA / PIX v7.0.6	Check Point NGX R60	Juniper ScreenOS v5.4	Fortinet FortiOS v2.8 CC
SIP	☑	☒	☒	☒
SCCP (Skinny)	☑	☒	☒	☒
H.323	☑	☒	☒	☒
MGCP	☑	☒	☒	☒
CTIQBE TAPI/JTAPI	☑	☒	☒	☒
GTP	☑	☒	☒	☒

	Cisco ASA / PIX v7.0.6	Check Point NGX R60	Juniper ScreenOS v5.4	Fortinet FortiOS v2.8 CC
평가 등급	EAL4+	EAL4	EAL4	EAL4+
Protection Profile	AppFW / Medium	Custom	Packet / Low	Packet / Low
Routed Mode	☑	☑	☑	☑
Transparent Mode	☑	☒	☑	☑
Virtual Firewalls	☑	☒	☒	☒
Physical & VLAN-based Interfaces	☑	☑	☒	☒
Local Management	☑	☑	☑	☑
Secure Remote Management	☑	☑	☒	☒
HTTP	☑	☑	☒	☒
FTP	☑	☑	☒	☒
SMTP	☑	☑	☒	☒
Telnet	☑	☑	☒	☒
DNS	☑	☒	☒	☒
ILS / LDAP	☑	☒	☒	☒
TCP	☑	☒	☒	☒
UDP	☑	☒	☒	☒
ICMP	☑	☒	☒	☒

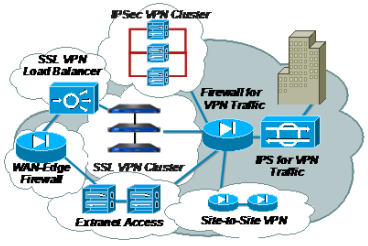
Why Cisco UTM – ASA 5500 Series?

비용효과적인 SSL/IPSec VPN 동시 지원 , 그리고 가장 안전한 VPN

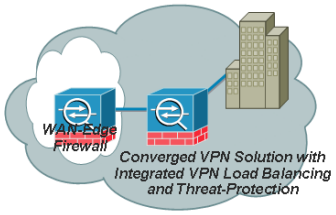
- The Most COST-EFFECTIVE ASA VPN
- The Most Secure Cisco ASA VPN

SSL VPN + IPSec VPN(무상) 기능 동시 지원

The Most COST-EFFECTIVE Cisco ASA VPN



Typical SSL VPN Deployment



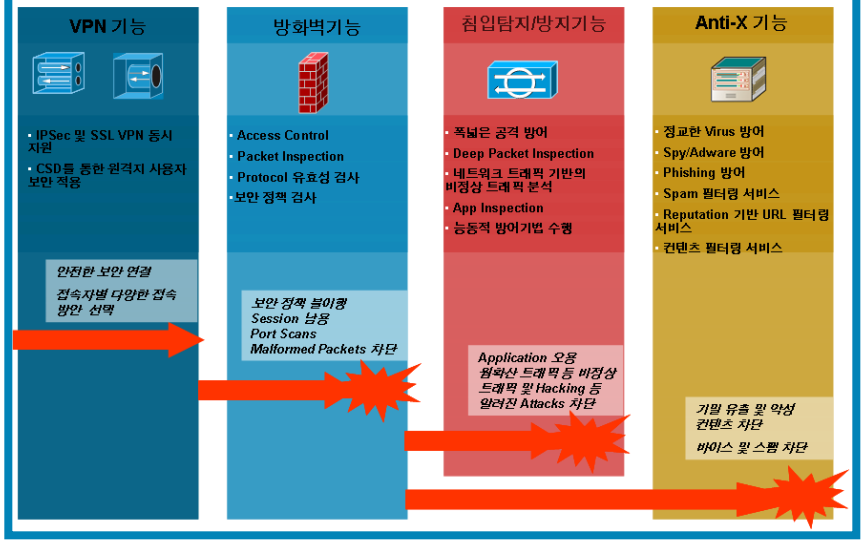
Cisco SSL VPN Deployment:
VPN Network 확장 및 보안성 강화로 인해 요구되어지는 장비 최소화

ASA VPN Solution Delivers:

- 통합 VPN 서비스 제공 – remote access(Ipsec,SSL), extranet and site-to-site VPN
- 모든 VPN 트래픽에 대한 방화벽/IPS 을 통한 통합 보안 위협 관리 제공
- 자체 로드밸런싱 기능으로 VPN 네트웍에 대한 저비용의 확장성 및 고가용성 제공
- 쉬운 운영을 통한 단독/통합 관리 솔루션 제공

SSL VPN + 방화벽 및 IPS, Anti-X 기능 선택 제공

The Most Secure Cisco ASA VPN



Why Cisco UTM – ASA 5500 Series?

Global Market Share #1, 국내 주요 그룹사 및 ISP 가 선택한 UTM!!

Vertical	References
Manufacture	SAMSUNG, LG전자, LG화학, 한진중공업, DOOSAN, posco, ISU 이수화학, KUMHO TIRES, 아시아나IDT, BMW Korea
Finances	MIRAE ASSET 미래에셋, 우리투자증권, E*TRADE, 나눔 Lotto, 키움증권 NO.1 ONLINE KIWOOM SECURITIES
Communications	KT, KTF, SK telecom, SK 브로드밴드, LG데이콤
Governments	Dynamic BUSAN, 이천시, Jeju 제주시, 한국전력공사
Portal & Game	Daum, AUCTION, NCSOFT, neowiz, CJ 인터넷, GRAVITY
ETC	HYUNDAI ENGINEERING & CONSTRUCTION CO.,LTD., 대우건설, 한림대학교의료원, 부산대학교병원, 부산대학교 PUSAN NATIONAL UNIVERSITY, 명지대학교 MYONGJI UNIVERSITY, LOTTE.com, Home plus 삼성 TESCO

참고 URL

- ASA 용 ASDM 관련 링크
  - ASDM 6.1(5) Release Note

    http://www.cisco.com/en/US/docs/security/asdm/6_1/release/notes/rn615.html
  - ASDM Configuraiton Guide, version 6.1

    http://www.cisco.com/en/US/docs/security/asdm/6_1/user/guide/usergd.html
- FWSM용 ASDM 관련 링크
  - ASDM Configuration Guide, version 6.1F

    http://www.cisco.com/en/US/docs/security/asdm/6_1f/user/guide/usrguide.html