Cisco ASA 5500 Series Technical Briefing

Updated: Dec 2008

Cisco Korea

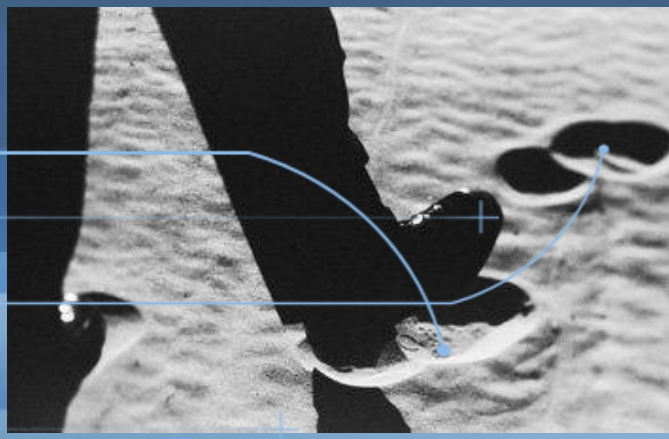
Solution SE Team

Yong-Ho Kim(yonghkim@cisco.com)

목차

- 새로운 시대의 요구사항
- Cisco ASA 5500 Series
- Cisco ASA 5500 Series 기술 상세 소개
  - 고속 및 대용량 서비스를 위한 기술
  - 안정적이고 유연한 설계를 위한 기술
  - 강력한 보안 기능을 위한 기술
  - 쉽고 효율적인 운영을 위한 기술
- Why Cisco ASA 5500 Series?
- Appendix
  - 모델별 비교 테이블
  - 주요 레퍼런스
  - CC 인증 및 국정원 정보보호 적합성 검토 현황

새로운 시대의 요구 사항



인터넷 환경 변화와 기업 보안 당면 과제

- 동시 접속 및 대용량의 멀티미디어 트래픽 처리
- 다양한 구성환경으로 인한 복잡성 증가 및 구성 제약
- 접점 별 혼합 및 새로운 보안 위협에의 신속한 대응 필요
- 운영대상 보안 장비의 증가에 대한 효율적 관리 필요

Cisco ASA 5500 Series

Approach as A system

Cisco ASA 5500 Series

IPSec or SSL VPN

방화벽

IPS or Anti-X

ASA 5500 Series의 4대 핵심 기술

고속 대용량 트래픽 처리 기술	• Real 10 Gbps Traffic 처리 • 경쟁사 대비 7.5배 이상의 고속 처리 – 15만 CPS • 최대 100,000 개의 IPSec / SSL VPN 동시 세션 처리
고 집적 네트워킹 기술	• 자원 독립적 가상방화벽 서비스 • Routed / Transparent 방화벽 구성 및 다양한 NAT 기술 적용 • 상태보존형 Active/Standby 및 Active/Active 고가용성 • Active / Standby Dual ISP 및 Redundant Interface
통합 위협 방어 기술	• 30개 이상의 Application Level Deep Packet Inspection • 방화벽 기반의 서비스거부 및 스캐닝 공격 탐지 및 자동 방어 • IPSec 및 SSL VPN 동시 지원 • 하드웨어 기반의 Cisco IPS 6.0 기능 ▪하드웨어 기반의 컨텐츠 보안 기능
ASDM 을 통한 One-Stop-Operation	• ASA의 모든 기능을 하나의 GUI 통합 • 방화벽 정책 관련 Event Correlation • 다양한 마법사 기능 및 유용한 툴

Cisco ASA 5500 Series 기술 상세 소개

- 고속 대용량 서비스를 위한 기술

Real 10 Gbps Traffic 처리

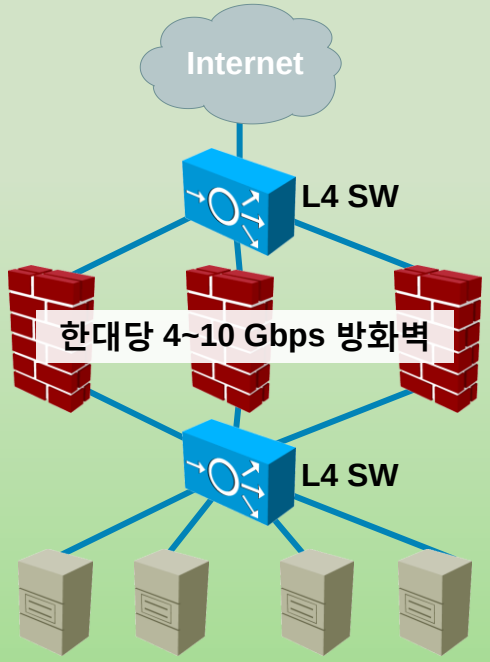
현재의 인터넷 트래픽

Web 1.0 텍스트기반 단방향 정보 전달 형 인터넷 서비스

Web 2.0 멀티미디어 기반 다중 대화형 인터넷 서비스

- 멀티미디어로 인한 **사용 대역폭(BPS) 급상승**
- **10~50배 이상의 초당 동시 연결(CPS)** 수 생성

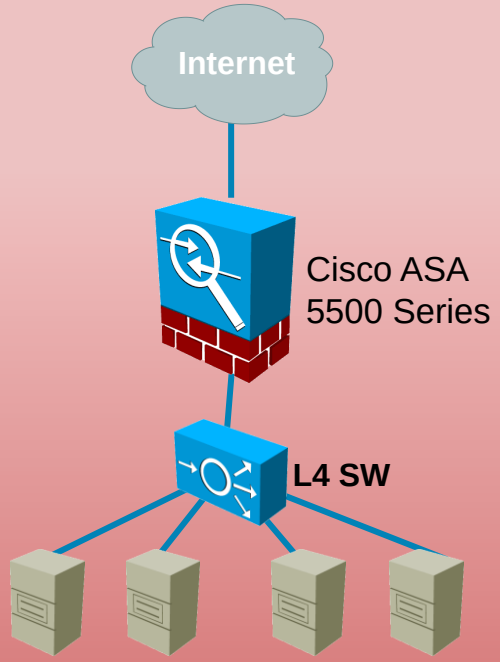
경쟁사 솔루션



- 단순히 대역폭 증가만 고려
- 낮은 CPS 그대로 유지

➔ 비용만 상승, 복잡한 구성 유지

Cisco ASA 솔루션

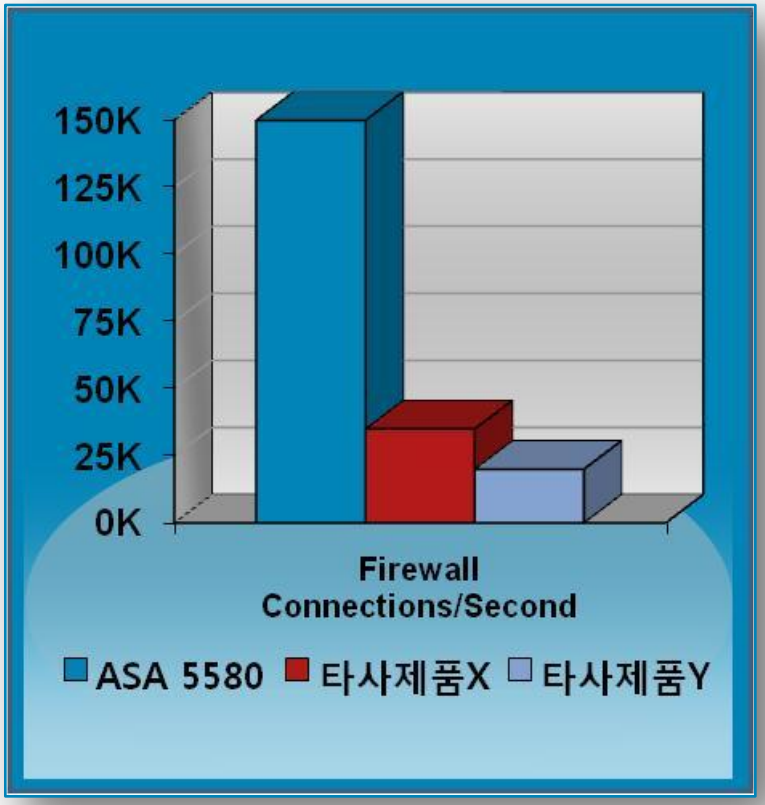


- 최대 16Gbps 의 고성능 지원
- 최대 15만 CPS 의 고속 처리

➔현실적인 인터넷 트래픽 처리 및 효율적인 구성

최대 15만 초당 동시 연결(CPS)

현실화 된 동종업계 최고 성능 및 처리 속도

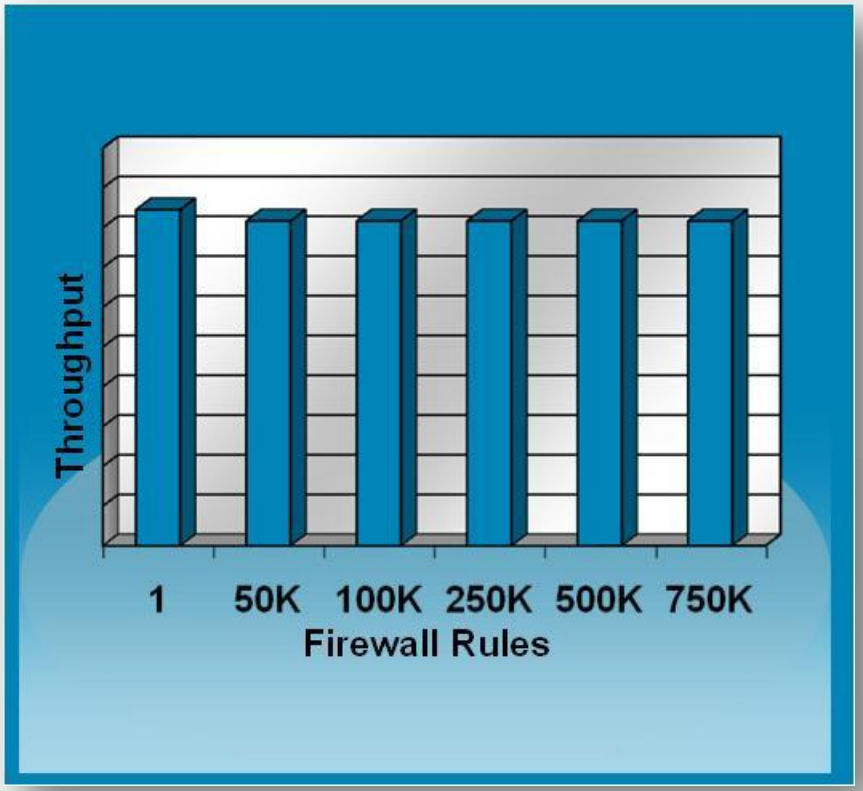


- 타사 대비 5~7 배 이상의 최대 15만 CPS 연결
- 대화형 다중 연결 구조의 인터넷 환경에 최적화

최대 75만개의 방화벽 정책

성능 영향 없는 대규모 방화벽 정책 적용

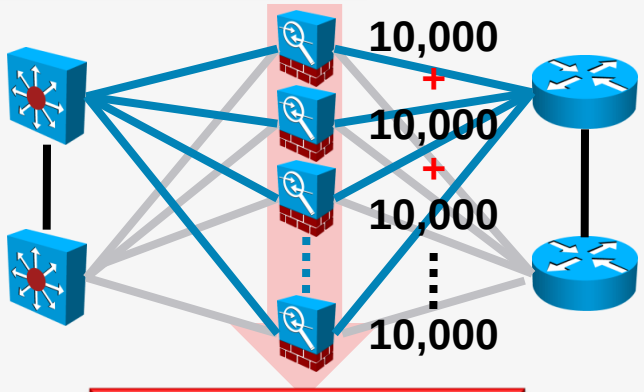
- 최대 75만개의 방화벽 정책 지원
- 성능에 전혀 영향 없이 적용 가능
- 대형 서비스 네트워크의 다양한 보안 정책 수용



최대100,000개의 IPSec/SSL VPN 동시세션처리

클러스터링 기술을 이용한 유연한 성능 확장

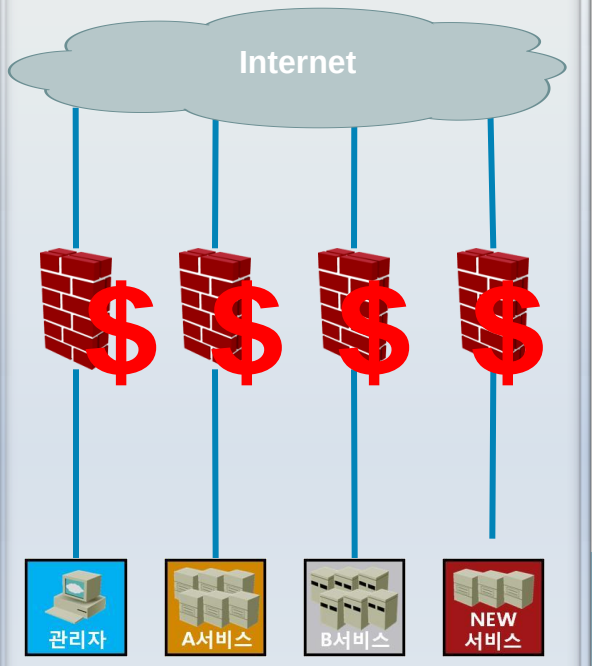
- 자체 로드밸런싱 기술을 이용, 추가적인 L4 스위치 불필요
- 플랫폼 구분 없이 클러스터링 가능
- 최대 10대까지 클러스터링



Cisco ASA 5500 Seires 기술 상세 소개
- 안정적이고 유연한 설계를 위한 기술

자원 독립적 가상방화벽 서비스

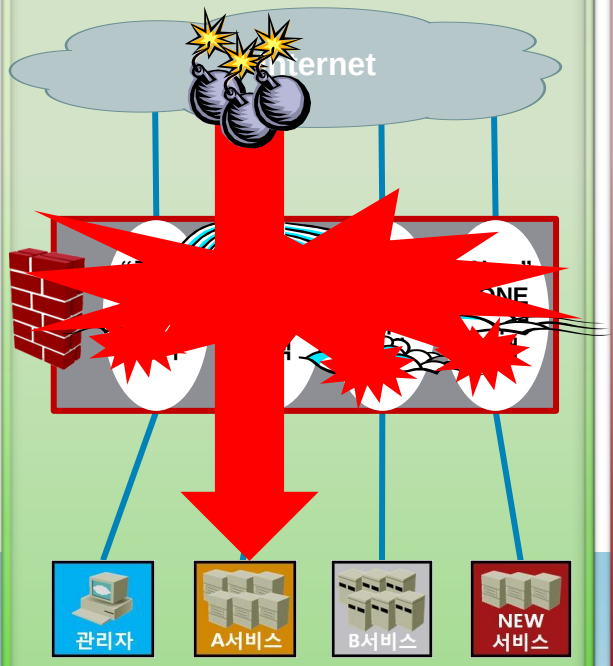
전통적인 서비스별 방화벽



서비스존 별 또는 목적별 H/W 기반의 독립방화벽 구성

➔ **비효율적 관리 부담 증가, 기하급수적 비용 상승**

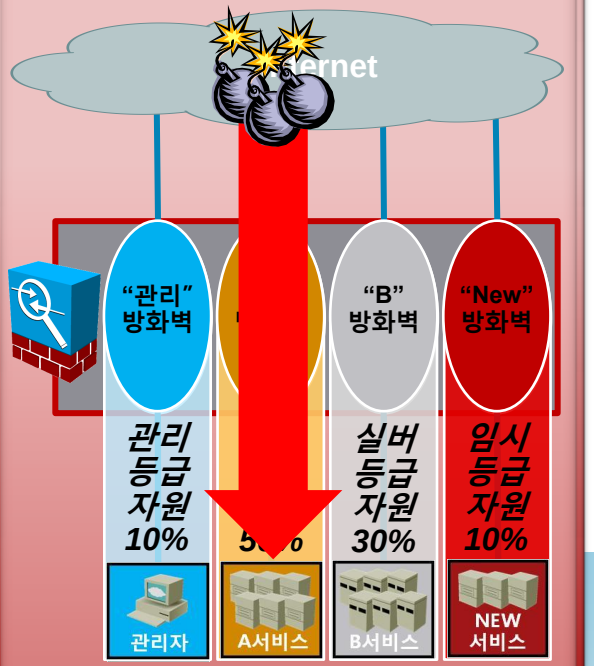
경쟁사 가상방화벽 기술



물리/논리적 인터페이스 페어링을 통한 서비스존 별 또는 목적별 방화벽 정책 구성

➔ **리소스 공유로 인한 전체 시스템 Fail 이슈**

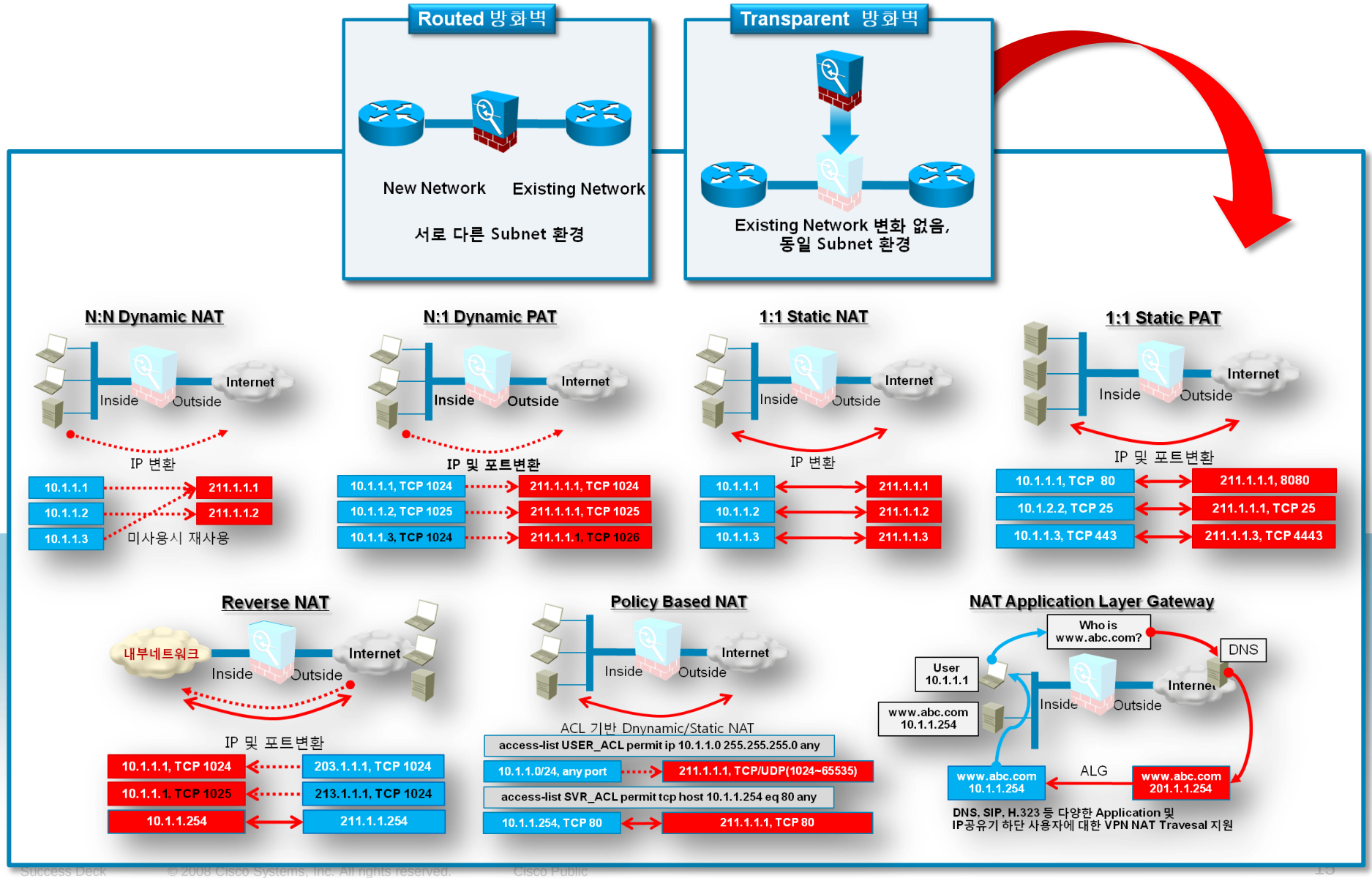
Cisco ASA 가상방화벽 기술



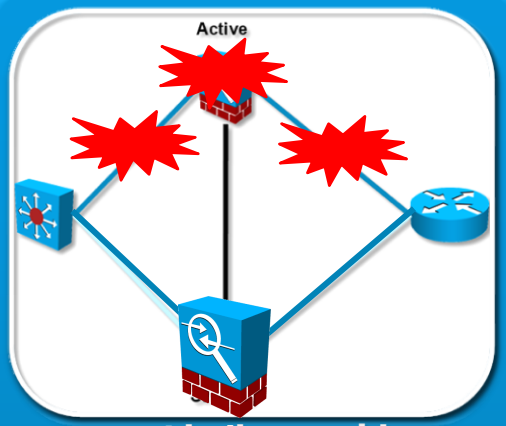
중요도별 자원 할당, 설정 및 방화벽 정책 등 완전히 독립된 논리적 가상방화벽

➔ **비용효율성 및 안정성 확보**

Routed / Transparent 방화벽 구성 및 다양한 NAT 기술 적용

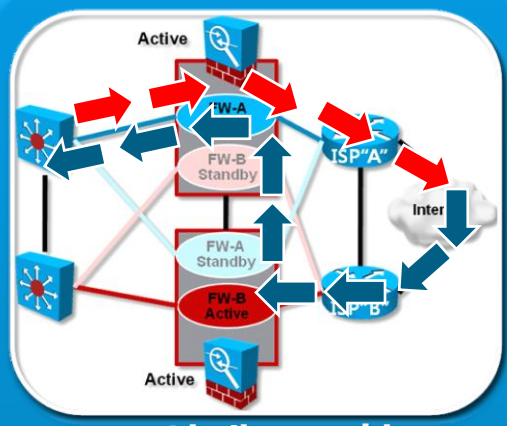


상태보존형 Active/Standby 및 Active/Active 고가용성



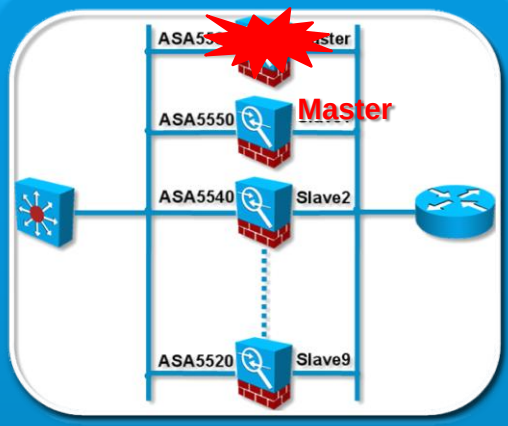
상태보존형 Active/Standby

- 방화벽 및 IPSec/SSL VPN 트래픽에 대한 상태보존형 고가용성 제공
- 모든 설정 및 상태 정보가 실시간으로 동기화됨



상태보존형 Active/Active

- 방화벽 트래픽에 대한 상태보존형 고가용성 제공
- 비대칭 라우팅 트래픽 처리 기능 지원
- 가상방화벽을 이용한 로드 공유



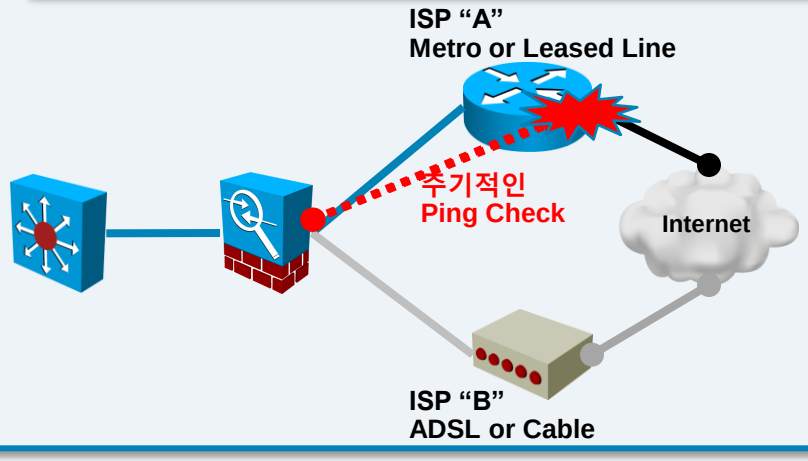
Active/Active 클러스터링

- IPSec/SSL VPN 트래픽에 대한 비상태 보존형 고가용성 제공
- 성능확장 능력 최대화
- 최대 10 대 이상의 동급 및 비동급 ASA 모델 클러스터링 가능

네트워크 환경별 유연한 고가용성 디자인

Active / Standby Dual ISP 및 Redundant Interface

Dual ISP 지원

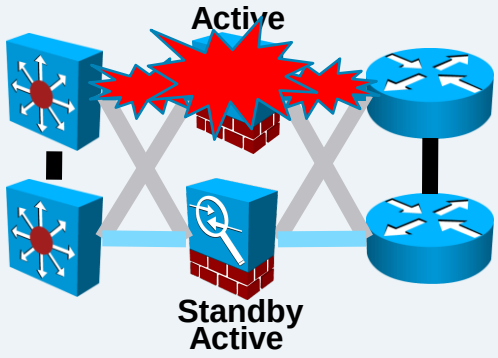


- Active / Standby 형태의 고가용성 제공
- IOS 기반의 SLA와 동일한 Interface 모니터링 기능 제공
- 긴급 상황을 위한 백업라인 체제에 적합
- Static Routing 과 연계

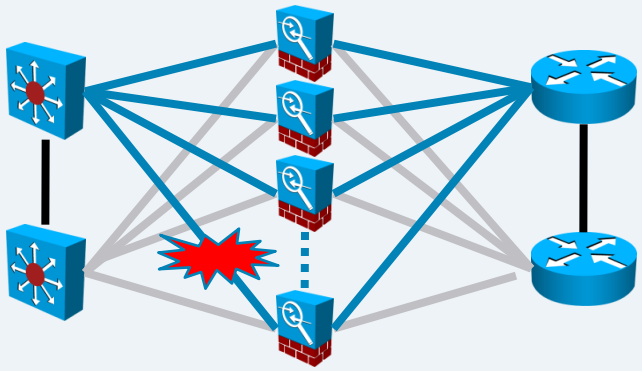
Redundant Interface

Basic Deployment

Full Meshed A/S Failover



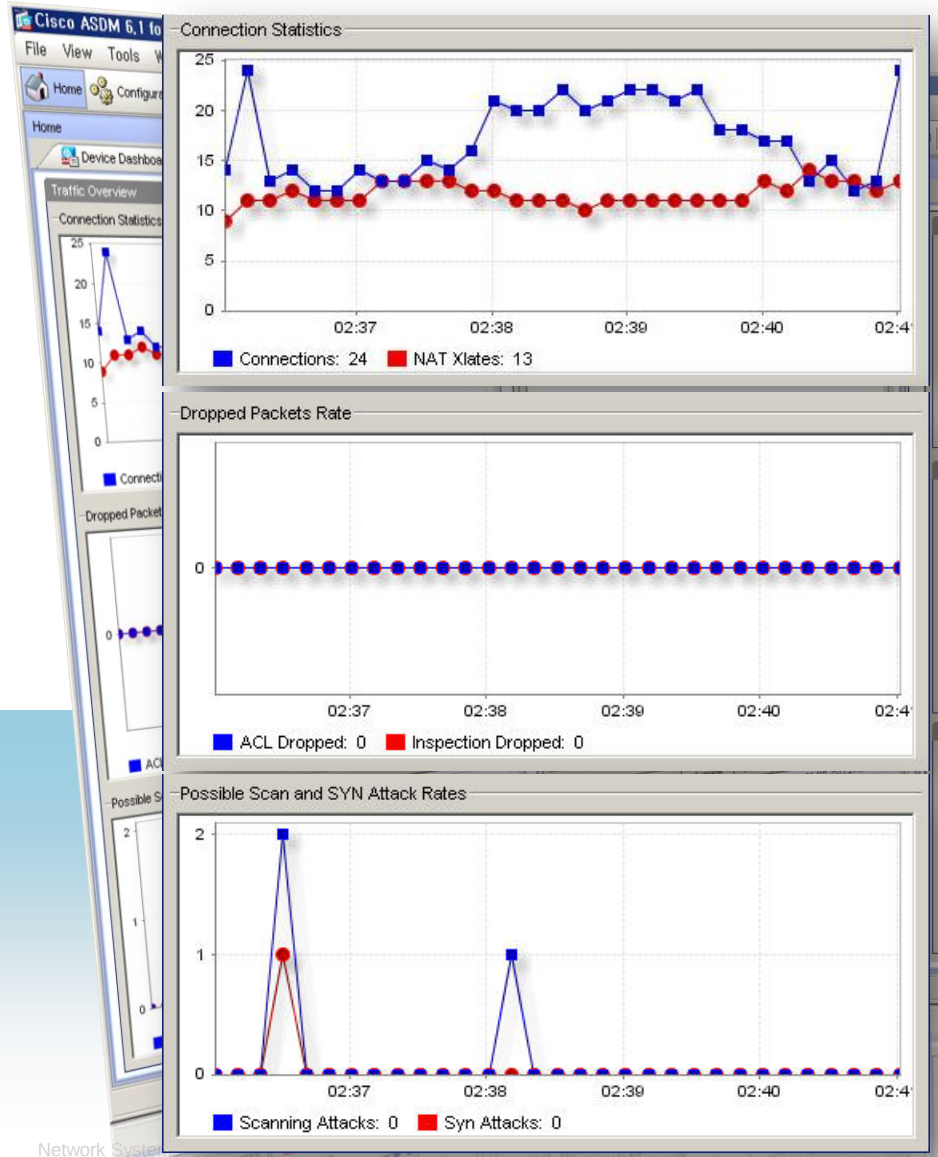
A/A Clustering Redundant Path



Cisco ASA 5500 Seires 기술 상세 소개

- 강력한 보안 기능을 위한 기술

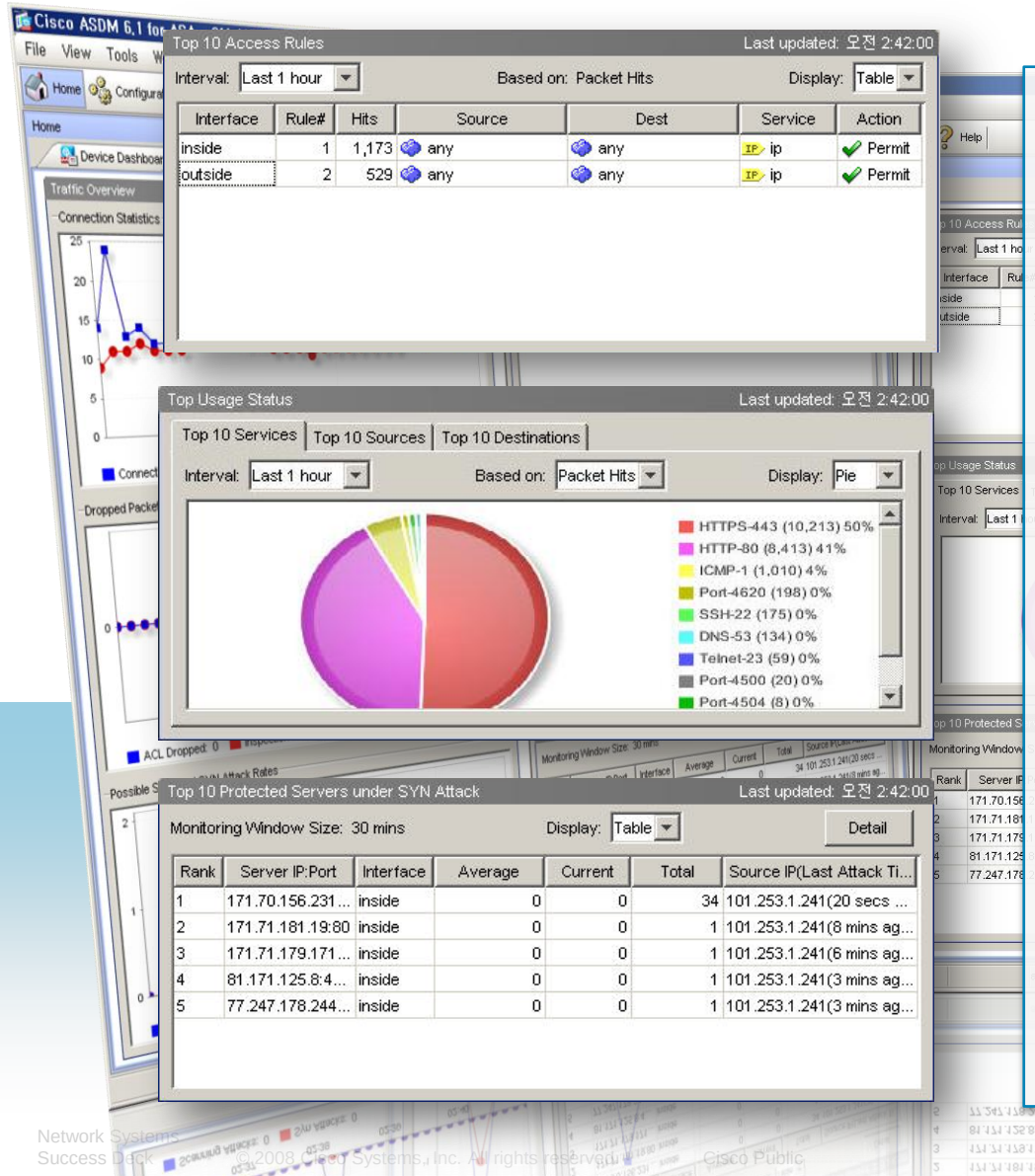
방화벽 기반의 서비스거부 및 스캐닝 공격 탐지 및 자동 방어(1/2)



Basic Threat Detection

- 방화벽 정책에 의한 과도한 Deny 트래픽 탐지
- 조작된 IP 또는 TCP 패킷 헤더의 Deny 트래픽 탐지
- 설정된 연결 제한 수 초과 트래픽 탐지
- IPSec VPN 및 일반 트래픽 상의 서비스 거부 공격 탐지
- 비정상적인 ICMP 패킷 탐지
- 응용프로그램 계층상의 과도한 Drop 트래픽 탐지
- TCP Syn Attack 및 Data가 없는 UDP 패킷과 같은 비정상적인 트래픽 탐지

방화벽 기반의 서비스거부 및 스캐닝 공격 탐지 및 자동 방어(2/2)



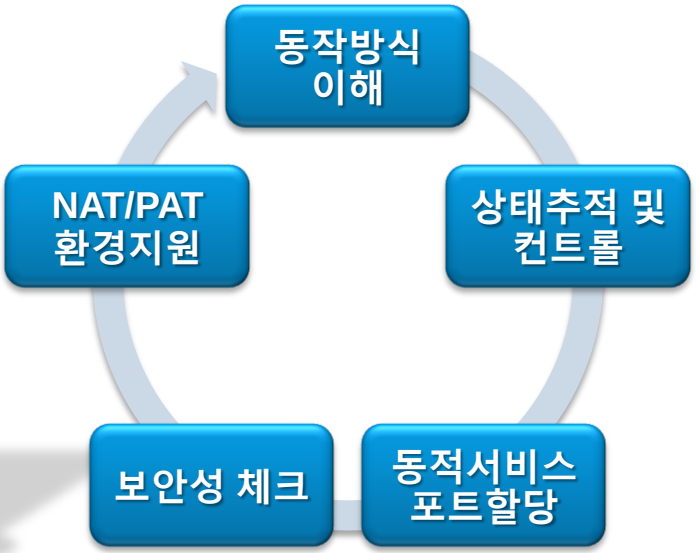
다양한 통계 기반 탐지

- **Top 10 Access Rule** ➔ 매칭되는 수가 많은 상위 10 개 방화벽 정책 리스트
- **Top Usage Status** ➔ BPS 또는 PPS 기반의 가장 많은 트래픽을 사용하는 상위 10개 항목별 리스트
  - Top 10 Service
  - Top 10 Source
  - Top 10 Destination
- **Top 10 Protected Server under Syn Attack** ➔ 설정된 Syn Attack 보호 서버중 공격을 가장 많이 받고 있는 상위 10개 서버 리스트

30개 이상의 Application Level Deep Packet Inspection Engine

- SIP
- SCCP (Skinny)
- H.323 v1–4
- GTP (3G Mobile Wireless
- MGCP
- TRP/RTCP/RTSP
- TAPI/JTAPI

Unified Communications



- Microsoft Windows Messenger
- Microsoft NetMeeting
- Real Player
- Cisco IP Phones
- Cisco Softphones

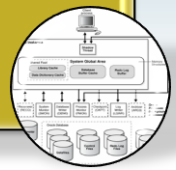
Specific Applications

- HTTP
- FTP
- TFTP
- SMTP/ESMTP
- DNS/EDNS
- ICMP
- TCP,UDP

Core Internet Protocols

- ILS/LDAP
- Oracle/SQL*Net (V1/V2)
- Microsoft RPC/DCE RPC
- Microsoft Networking
- NFS, RSH
- SunRPC/NIS+
- X Windows (XDMCP)

Database/OS Services



- IKE
- IPSec
- PPTP

Security Services

IPSec 및 SSL VPN 동시 지원(1/2)

Any Application

Latency 등 속도에 민감한 음성 및 비디오 데이터 전송 최적화, 업계 최초의 **DTLS(신SSL VPN** 기술) 적용

Any Endpoint

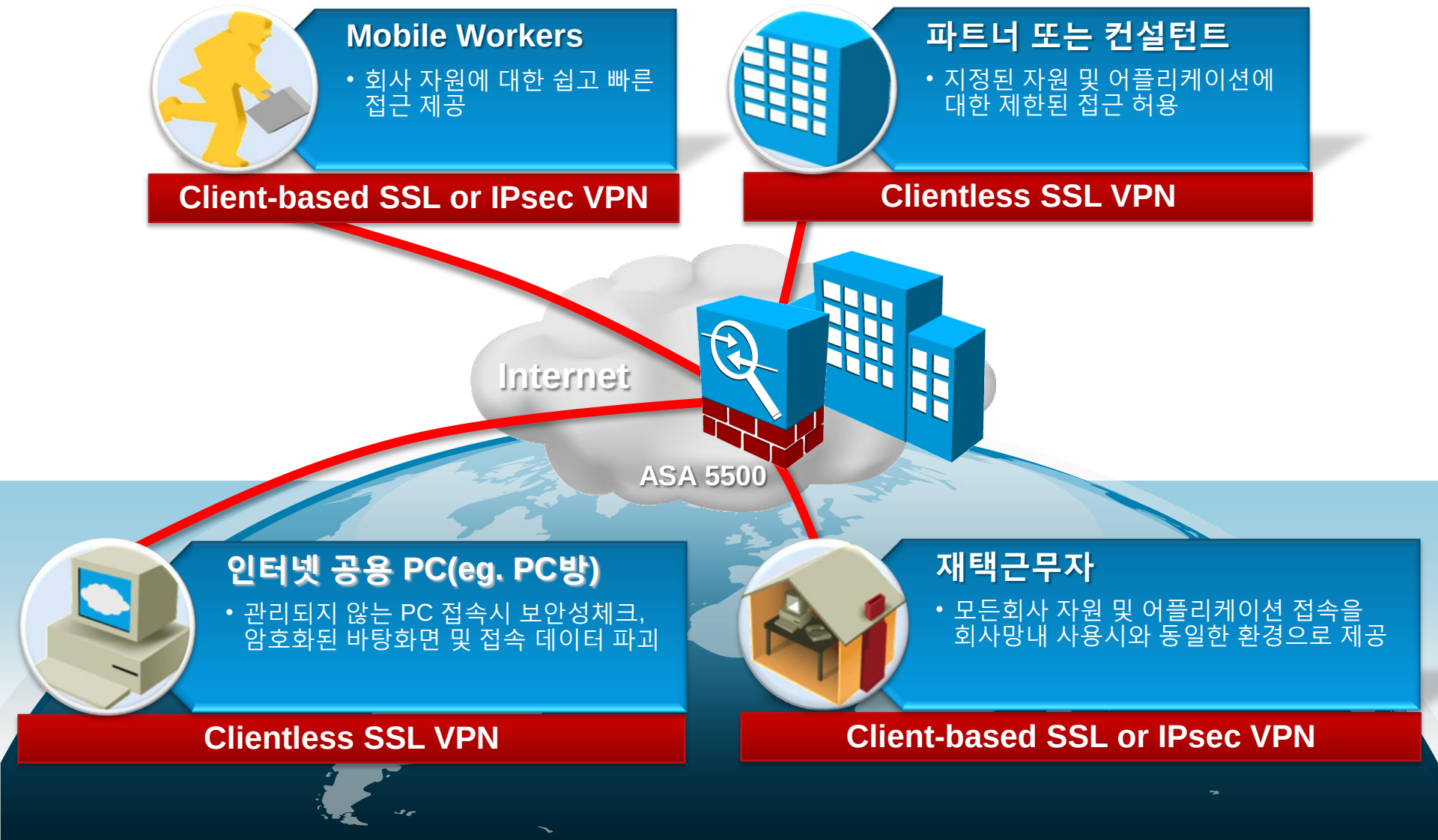
Windows, Mac OS, Linux, 스마트폰(브라우징)

Any Policy

접속자의 소속에 따른 다양한 사용자 및 그룹별 세밀한 보안 정책 적용

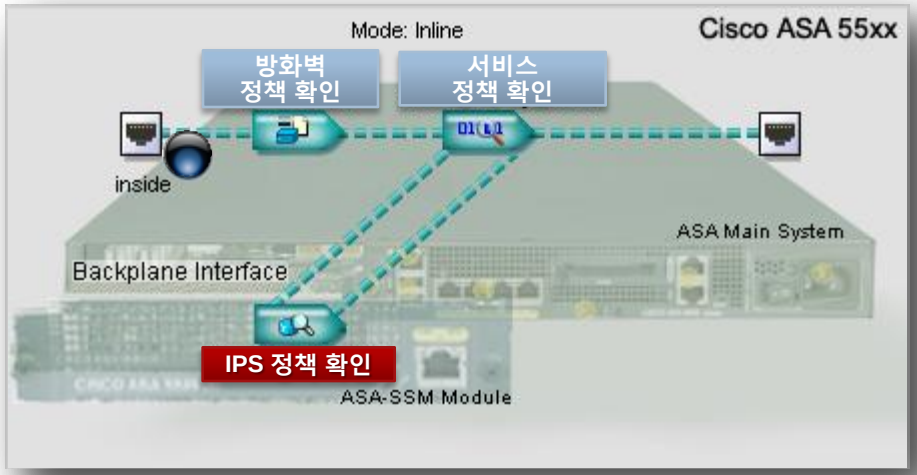
언제 어디서나 간편하고 안전하게 업무 공간 확장

IPSec 및 SSL VPN 동시 지원(2/2)



하드웨어 기반의 Cisco IPS 6.0 기능

AIP-SSM-10/20/40



- Cisco IPS 6.0 S//W의 모든 기능을 동일하게 지원
- **AIP-SSM-10**
  ➔ 150Mbps ~ 250Mbps
- **AIP-SSM-20**
  ➔ 375Mbps ~ 450Mbps
- **AIP-SSM-40**
  ➔ 450Mbps ~ 650Mbps

AIP-SSM

- 서비스 정책에 의한 트래픽 선별
- **Inline Mode** : 인라인상으로 공격트래픽 탐지 및 차단
- **Promiscuous Mode:** Passive 형태로 공격트래픽 탐지 및 방화벽 정책 삽입으로 차단

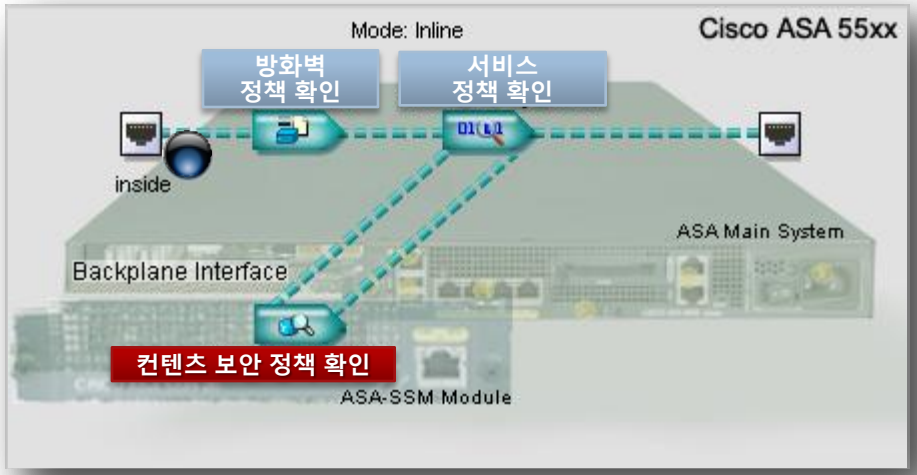
동작방식

- **Anomaly Detection :** 학습기반 비정상(웜확산) 트래픽 탐지 및 차단
- **One-Stop-Prevention :** 실시간 이벤트 연동 즉시 차단
- **Risk Rating** : 오탐 최소화 자동설정 기능
- **쉽고 간편한 관리**
- **직관적인 모니터링**

주요기능

하드웨어 기반의 컨텐츠 보안 기능

CSC-SSM-10/20



CSC-SSM

- 트렌트마이크로사의 최신 컨텐츠 보안 엔진
- **CSC-SSM-10**
  ➔ 100,250,500 Users
- **CSC-SSM-20**
  ➔ 750, 1000 Users

동작방식

- 서비스 정책에 의한 트래픽 선별
- **Pattern Matching Engine**
  :정책기반 탐지 및 차단
- **Heuristic Engine**:학습기반 탐지 및 차단
- **Email Reputation Service**
  :신뢰도 DB 기반 탐지 및 차단

주요기능

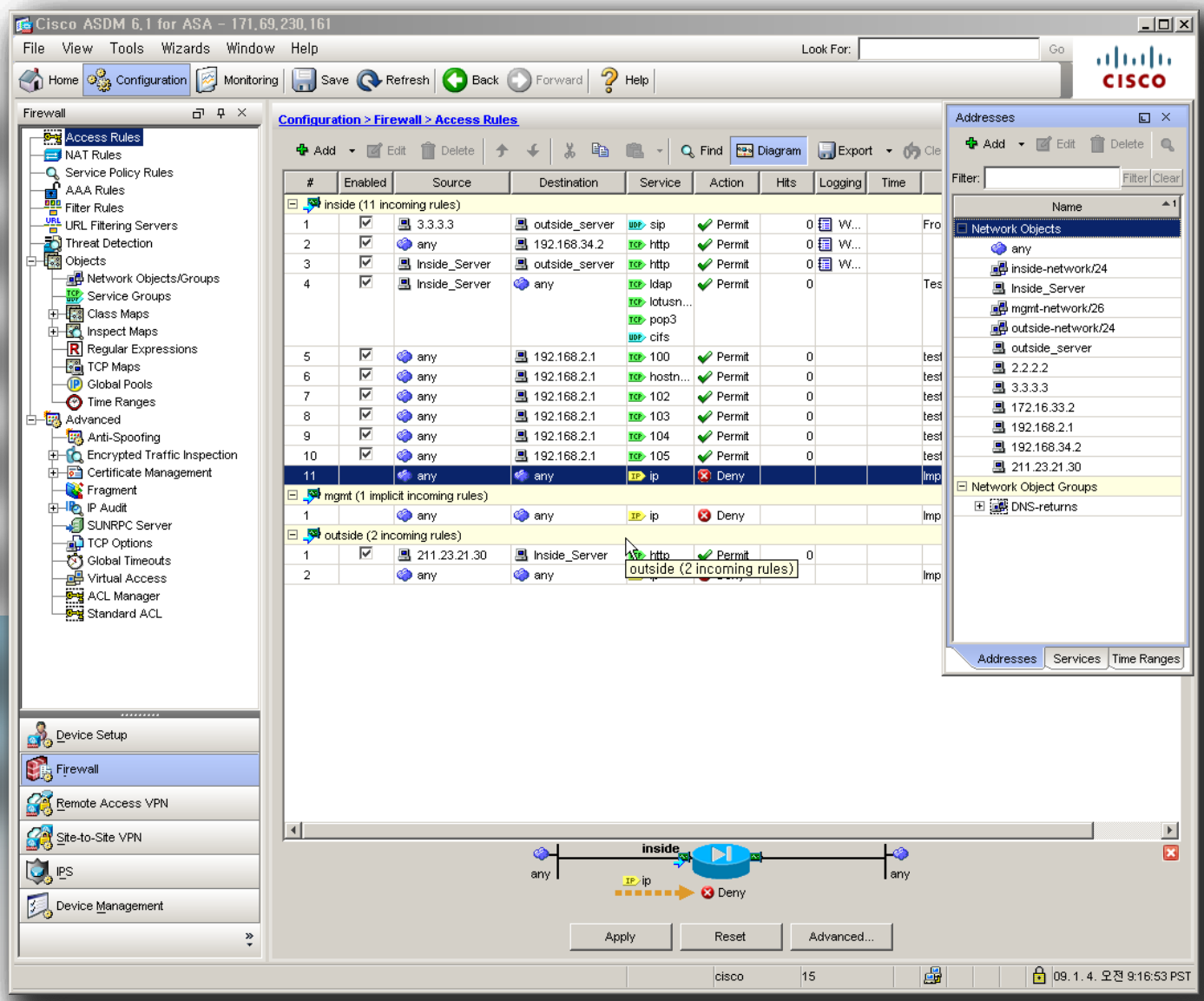
- **Base License**
  - 파일 기반 안티바이러스 및 악성코드 탐지 및 차단
  - 안티 스파이웨어
- **Plus License**
  - 안티스팸 및 안티피싱
  - 컨텐트 필터링
  - URL 블록킹 및 필터링

Cisco ASA 5500 Seires 기술 상세 소개

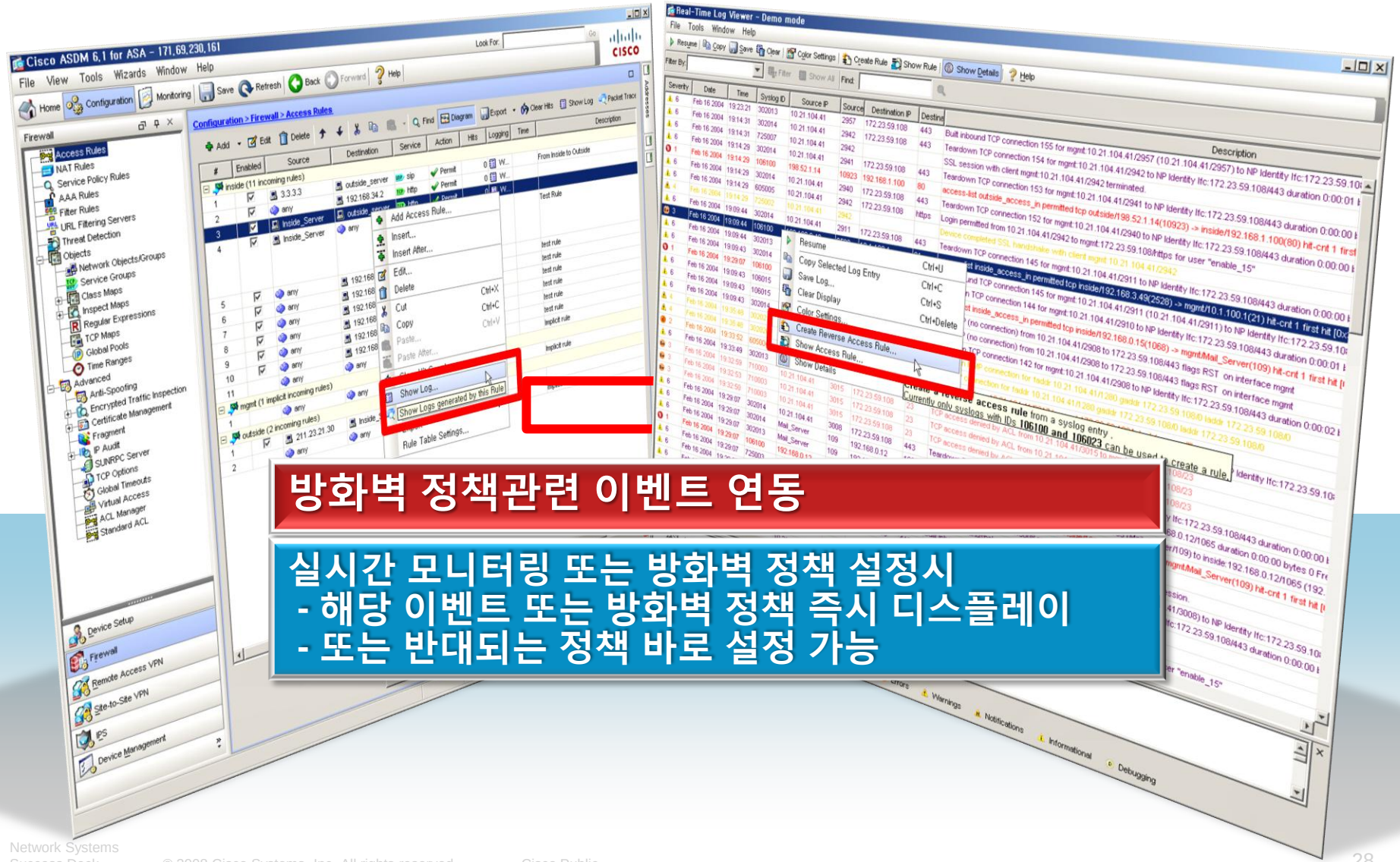
- 쉽고 효율적인 운영을 위한 기술

ASA의 모든 기능을 하나의 GUI 통합

- Device Setup
- Device Management
- Firewall
- Remote Access VPN
- Site-to-Site VPN
- IPS
- Trend Micro Content Security

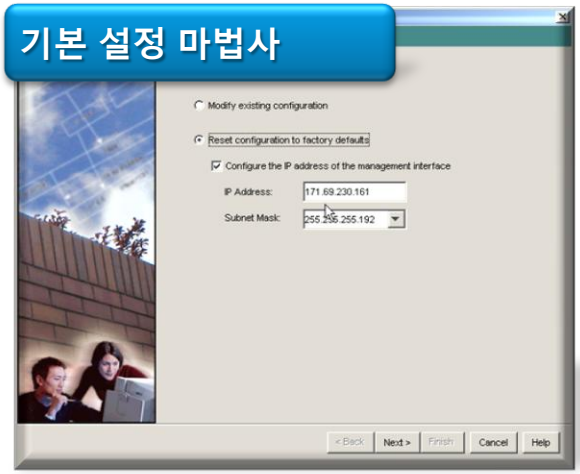


방화벽 정책 관련 Event Correlation

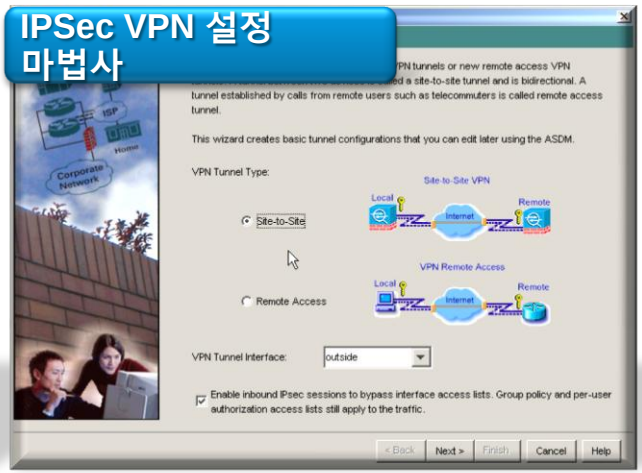


다양한 마법사 및 유용한 툴

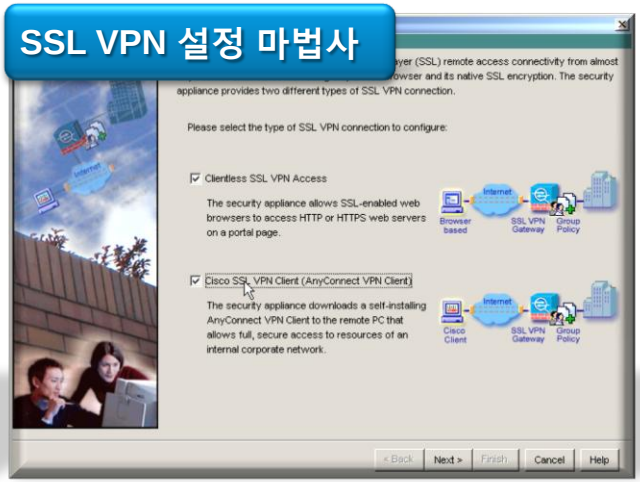
기본 설정 마법사



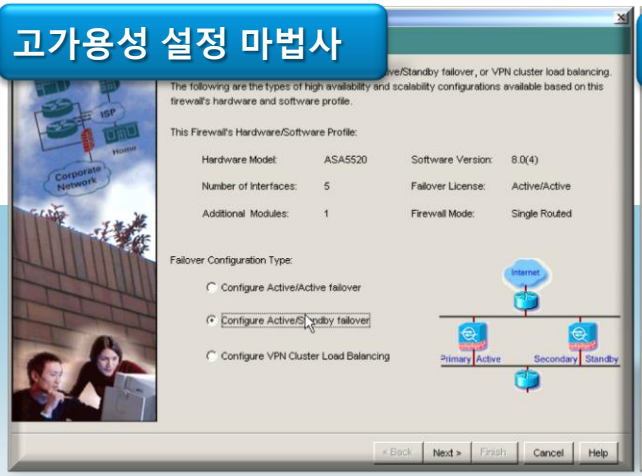
IPSec VPN 설정 마법사



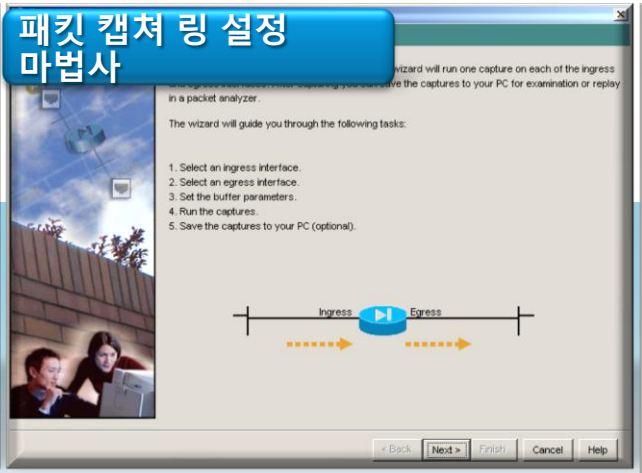
SSL VPN 설정 마법사



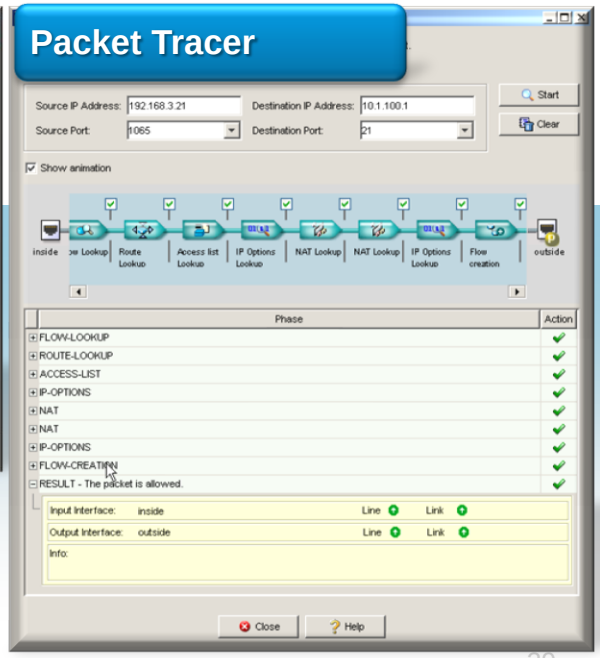
고가용성 설정 마법사



패킷 캡쳐 링 설정 마법사



Packet Tracer



Why Cisco ASA 5500 Series?

Why Cisco ASA 5500 Series?

Cisco ASA 5500 Series Appliance

고속 대용량 트래픽 처리 기술
- Real 10 Gbps Traffic 처리
- 경쟁사 대비 7.5배 이상의 고속 처리 – 15만 CPS
- 최대 100,000 개의 IPSec / SSL VPN 동시 세션 처리

현실성 있는 고속 대용량 서비스

고 집적 네트워킹 기술
- 자원 독립적 가상방화벽 서비스
- Routed/TP 방화벽구성 및 다양한 NAT 기술
- 상태보존형 A/S 및 A/Active 고가용성
- A/S Dual ISP 및 Redundant Interface

최고의 안정성 및 유연한 구성

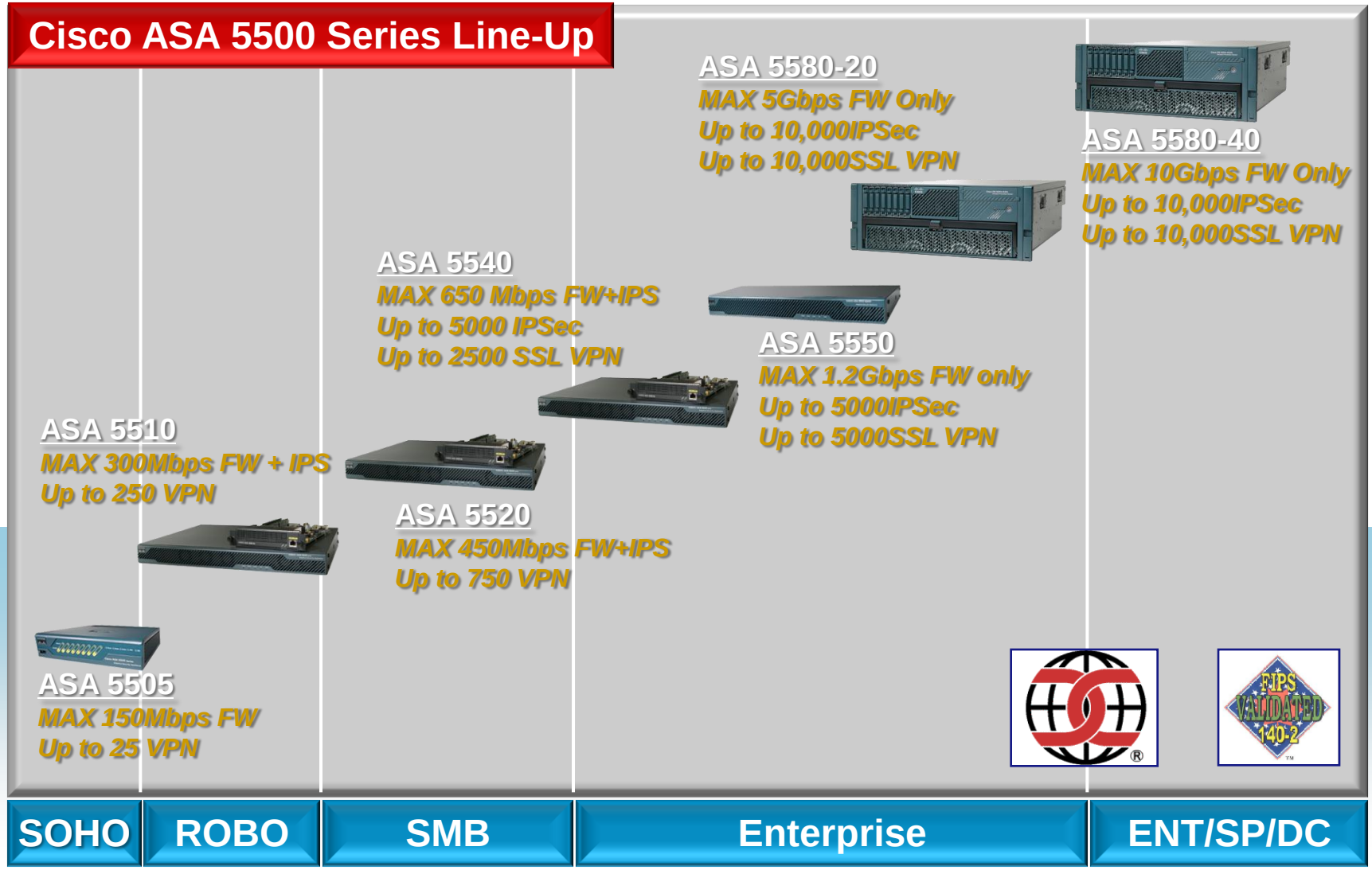
통합 위협 방어 기술
- L7 Deep Packet Inspection
- DoS 및 스캐닝 공격 탐지 및 자동 방어
- IPSec 및 SSL VPN 동시 지원
- H/W Based IPS or Contents 보안

강력한 통합보안 효과

ASDM을 통한 One-Stop-Operation
- ASA의 모든 기능을 하나의 GUI 통합
- 방화벽 정책 관련 Event Correlation
- 다양한 마법사 기능 및 유용한 툴

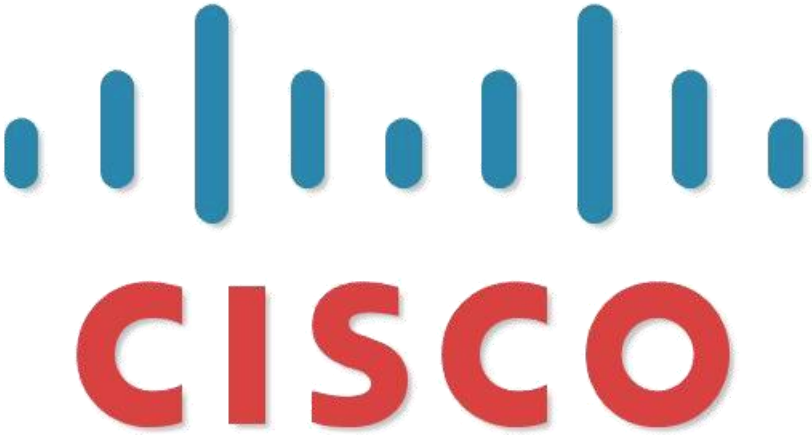
쉽고 효율적인 관리

모든 규모에 대한 풀 라인업



ASA 국내 주요 레퍼런스

Vertical	References
Manufacture	SAMSUNG, LG전자, LG화학, 한진중공업 HANJIN HEAVY INDUSTRIES & CONSTRUCTION, DOOSAN, posco, ISU 이수화학, KUMHO TIRES, 아시아나IDT, BMW Korea, BMW Sheer Driving Pleasure
Finances	MIRAE ASSET 미래에셋, 우리투자증권 WWW.WOORIINVM.COM, 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 KOREA ELECTRIC POWER CORPORATION
Portal & Game	DAUM, AUCTION an eBay company, NCSOFT, neowiz, CJ 인터넷, GRAVITY
ETC	HYUNDAI ENGINEERING & CONSTRUCTION CO.,LTD., 대우건설, 한림대학교의료원 HALLYM UNIVERSITY MEDICAL CENTER, PNUH 부산대학교병원 PUSAN NATIONAL UNIVERSITY HOSPITAL, 부산대학교 PUSAN NATIONAL UNIVERSITY, 명지대학교 MYONGJI UNIVERSITY, LOTTE.com, Home plus 삼성 TESCO


CISCO

Appendix

인터넷 Edge 에서 데이터 센터까지 High-End Market 대상 Lineup의 완결

네트워크 위치	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580-20 (New)	Cisco ASA 5580-40 (New)
				
	Internet Edge	Internet Edge / Campus	Campus / Data Center	Data Center
성능				
최대 파이어월 (Real-world HTTP)	500 Mbps	1 Gbps	5 Gbps	10 Gbps
최대 파이어월 (Jumbo-frame)	-	-	10 Gbps	20 Gbps
최대 파이어월 UDP 1400)	650 Mbps	1.2 Gbps	6.5 Gbps	14 Gbps
최대 IPSec VPN	325 Mbps	425 Mbps	1 Gbps	1Gbps
최대 IPSec/SSL VPN 동시 연결수	5000 / 2500	5000 / 5000	10,000 / 10,000	10,000 / 10,000
플랫폼별 상세				
최대 파이어월 동시연결수	400,000	650,000	1,000,000	2,000,000
최대 초당 동시 연결수	25,000	36,000	90,000	150,000
Packets/Second (64 byte)	500,000	600,000	2,500,000	4,000,000
Base I/O	4 GE + 1 FE	8 GE + 1 FE	2 Mgmt	2 Mgmt
Max I/O	8 GE + 1 FE	8 GE + 1 FE	24 GE / 12 10GE	24 GE / 12 10GE
최대 지원 VLAN 수	200	250	100 (250*)	100 (250*)
고가용성 기능	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S
최대 가상방화벽 수	50	50	50	50

* Supported in a re software release

Cisco ASA 5500 Series

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

차별화된 CC인증 기반의 방화벽 기능 기본 지원

- SSL/IPSec Remote Access VPN 사용자에 대한 기본 접근 통제 수단
- 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
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	☑	☒	☒	☒

	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	☑	☒	☒	☒