시스코 보안 제품 업데이트

정 희 철
Cisco Systems Korea

Key Message

- **시스코 통합 보안 제품 : ASA, 6500/7600**
- **시스코 통합 보안 관리 제품 : CS-MARS**
- **End-to-End 보안 제품간 연동 : CSA, AVS (Application 보안)**

목 차

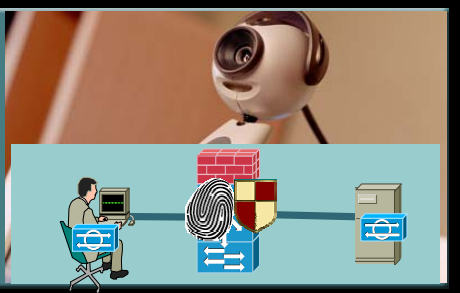
- 시스코 보안 전략
- 통합형 보안 신제품
  - 중소형 통합 보안 제품 :
    시스코 **ASA (Adaptive Security Appliances - SSL VPN,** 방화벽 **7.0, IPS)**
  - 대형 통합 보안 제품 : **Catalyst 6500** 과 보안 모듈
- 통합 보안 관리 신제품
  - **CS-MARS**
- 사용자 보안 제품 업데이트
  - **CSA (Cisco Security Agent)**
- 응용프로그램 관리/보안 제품
  - **AVS (Application Velocity System)**
- 결론
- 데모

시스코 보안 전략

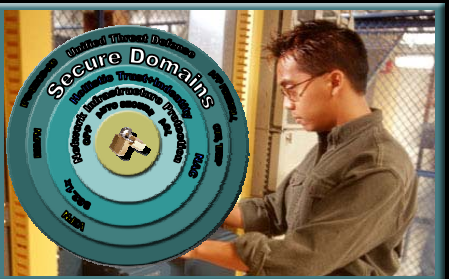
차세대 보안

1.단품 방식 → 통합 보안

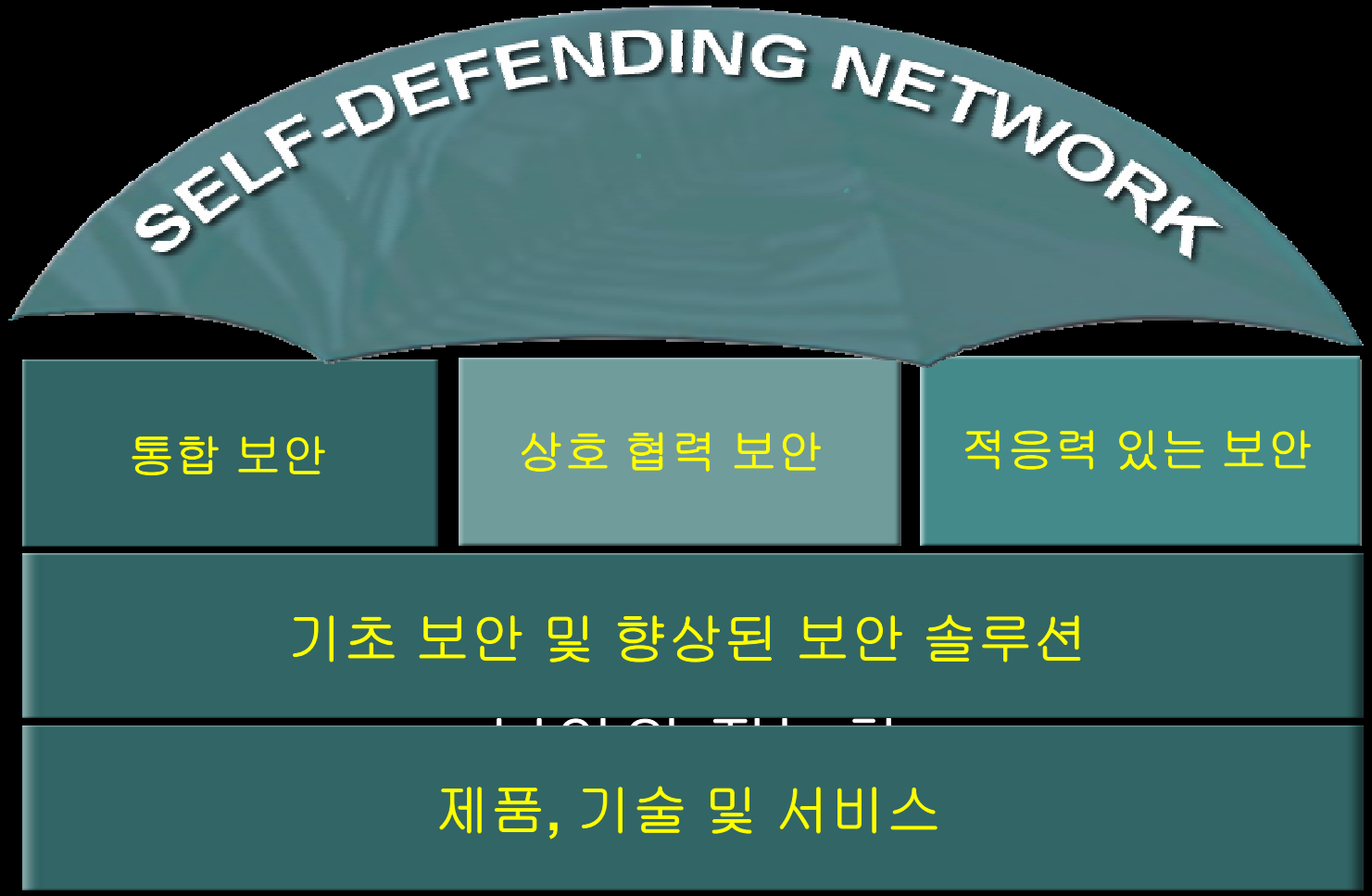
2. 개별적인 보안방식 → 상호 협력 보안



3. Virus 방어 → 적응력 있는 보안



Self-Defending Network
이것이 바로 시스코의 차별성 입니다.



2005년 시스코 보안 신제품 소개

Converged Security
Cisco ASA 5500
New!

ASA 7.0: "All-in-One" Security

Firewall
Cisco PIX
New!

PIX 7.0: Web, IM and P2P Security, Active/Active

Intrusion Prevention
Cisco IPS
New!

IPS 5.1: In-Line IPS, RR rating

Remote Access VPN
Cisco VPN 3000
New!

4.7: SSL VPN, CSD, Cache cleaner

Switch Security
Catalyst Engines
New!

Cat6k: Web VPN Module, IPSec SPA, DDoS Solutions, FWSM 2.3

Security Management
Cisco VMS/MARS
New!

Management: Security Auditor, VMS 2.3, MARS

Endpoint Security
Cisco Security Agent
New!

CSA 5.0: **한글 버전 지원**, Anti-Spyware, Trusted QoS

Application Security
AVS
New!

AVS: 응용프로그램 최적화 및 가속, 응용프로그램 보안

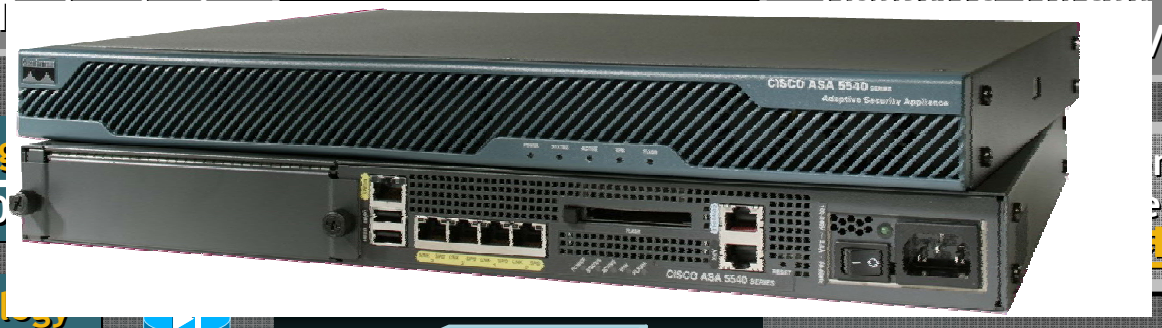
중소형 통합 보안 제품

- ASA (Adaptive Security Appliance)

시스코 ASA 5500 시리즈

시장에서 검증된 완벽한 보안 기술의 집합체

Market-Proven T



VPN Technolog
Cisco VPN 300

Firewall Technolo
Cisco PIX

IPS Technology
Cisco IPS

NW-AV Technology
Cisco IPS, Trend AV

Network Services
Cisco Networking

Adaptive Threat Defense
/PN"

n, Use
eb Control
보안

Malware/Content Defense,
Anomaly Detection
Anti-X 방어

Traffic/Admission Control,
Proactive Response
봉쇄 & 제어

안전한 "CLEAN VPN" 접속

시스코 ASA 5500 시리즈

Industry First! Scalable, Multi-Function, Feature Rich

어플리케이션 보안

- 멀티 레이어 방식의 패킷 및 트레픽 분석
- 향상된 기술을 이용한 어플리케이션 및 프로토콜 감시 서비스
- 네트워크 어플리케이션 제어
- 향상된 VoIP 및 멀티미디어 보안

Anti-X 방어

- 네트워크 방식의 웜 및 바이러스 방어
- Spyware, adware, malware 감지 및 제어
- 정확하고 신뢰성 있는 방어 기술
- 이벤트의 상관관계를 이용한 적극적인 방어 구현

봉쇄와 제어

- Layer 3 / 4 엑세스 컨트롤 서비스
- Stateful 패킷 감시
- 융통성 있는 정책 그룹 적용 (user, network, application)

"CLEAN VPN"

- Zero-touch, automatically updateable IPSec remote access
- 융통성 있고 안전한 SSL VPN 서비스
- QoS/routing-enabled site-to-site VPN
- Integrated threat mitigation protect against VPN-delivered threats

CISCO NETWORK SERVICES INTELLIGENCE

- Low Latency Support
- Support for Diverse Topologies
- Multicast Support
- Services Virtualization
- Network Segmentation & Partitioning
- Routing, Resiliency, Load-Balancing

시스코 ASA 5520/5540 적응 형 보안 장비

Product Tour

4개의 10/100/1000 Copper Gigabit 포트

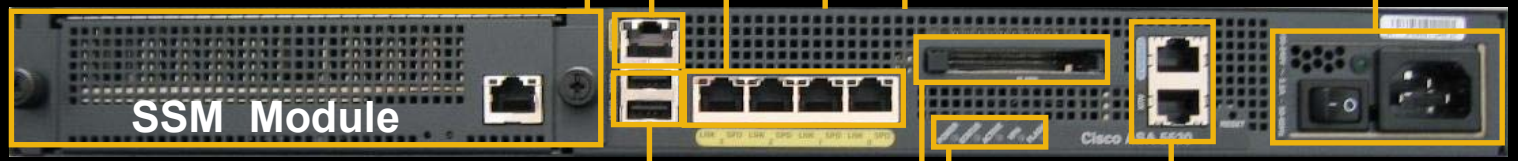
하나의 10/100 Out of Band Management 포트*

SSM Module - IPS 5.0 Out of Band - GE

Sleek, High Performance 1 Rack Unit (RU) Design

Diskless Architecture for High Reliability

Single Field Upgradeable AC or DC Power Supply



2개의 USB 2.0 포트 (Credentials, Failover, and more)

Int. / Ext. Compact Flash for Software, Config, and Logs

Console and AUX Ports

Five Status LEDs (Power, Status, Active, VPN, Flash)

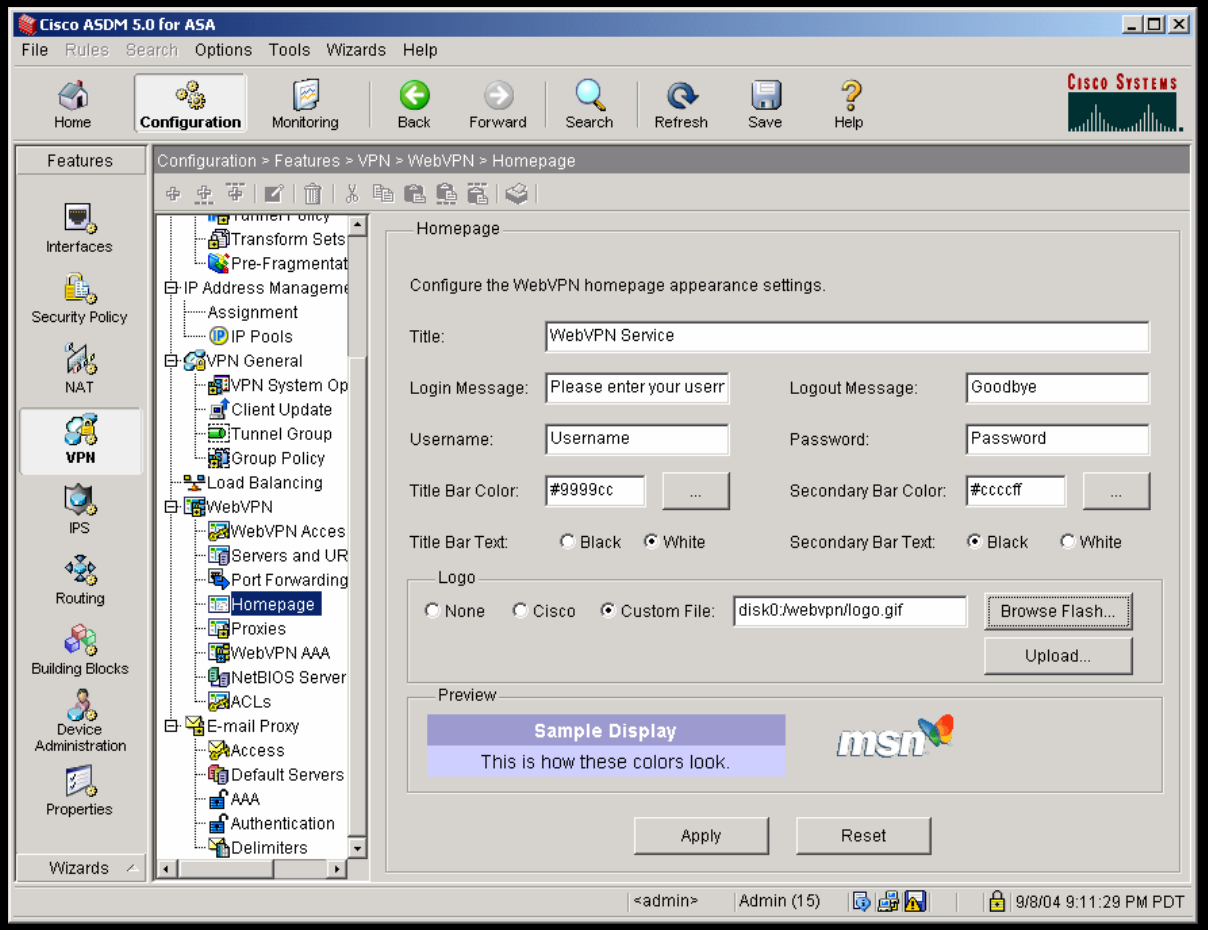
시스코 ASA 5500 제품 군

	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540
			
대상 고객	중소 기업	100~300인 규모의 중견 기업	대기업
IPSec VPN Web VPN	50/ 150* 50/ 150*	300/ 750* 300/ 750*	500/ 2000* / 5000** 500/ 1250* / 2500**
성능 방화벽 최대 성능 방화벽+IPS 최대 성능 IPSec VPN 최대 성능	 300 Mbps 150 Mbps 170 Mbps	 450 Mbps 375 Mbps 225 Mbps	 650 Mbps 450 Mbps 325 Mbps
기본 제공 서비스	방화벽, IPSec 과 SSL VPN, 그리고 A/S HA (업그레이드 필요.), 3 FE to 5 FE	5510과 서비스에 더하여 A/A 장애 복구, VPN Clustering, 4 GE + 1 FE	5520에 더하여 고성능과 더 높은 확장성 제공

* VPN Plus 업그레이드 라이센스로 확장 가능

** VPN Premium 라이센스로 확장 가능

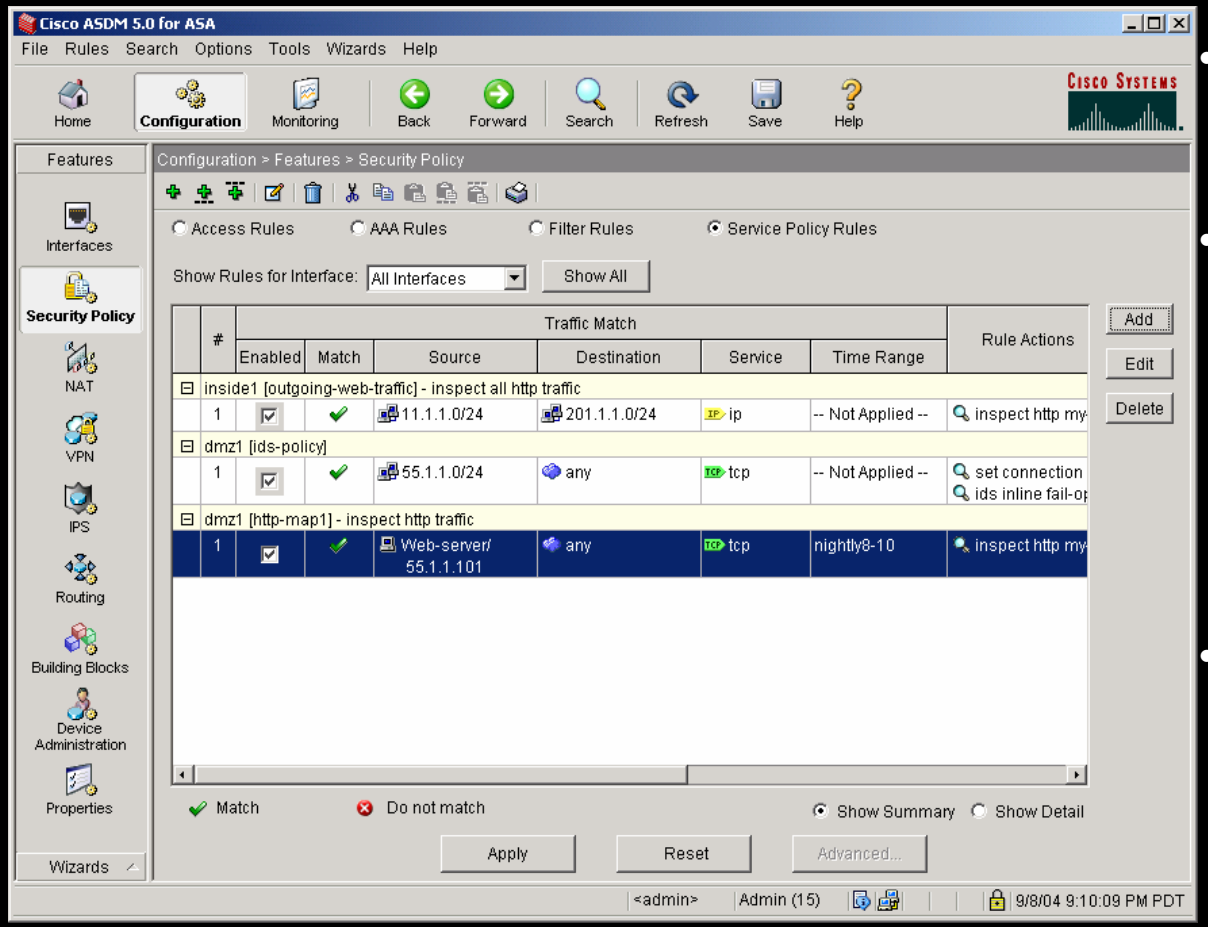
시스코 Adaptive Security Device Manager (ASDM)
VPN 관리 및 감시 기능



- Cisco ASDM v5.0
  - Remote access 및 site-to-site VPN 관리 및 모니터링
- Full configuration 지원
  - WebVPN
  - IPSec RA groups
  - S2S tunnels
  - AAA, DHCP, 등등
- 모니터링 지원
  - 가동 시간, 전송 바이트, 터널별 통계량
  - VPN 사용 추이

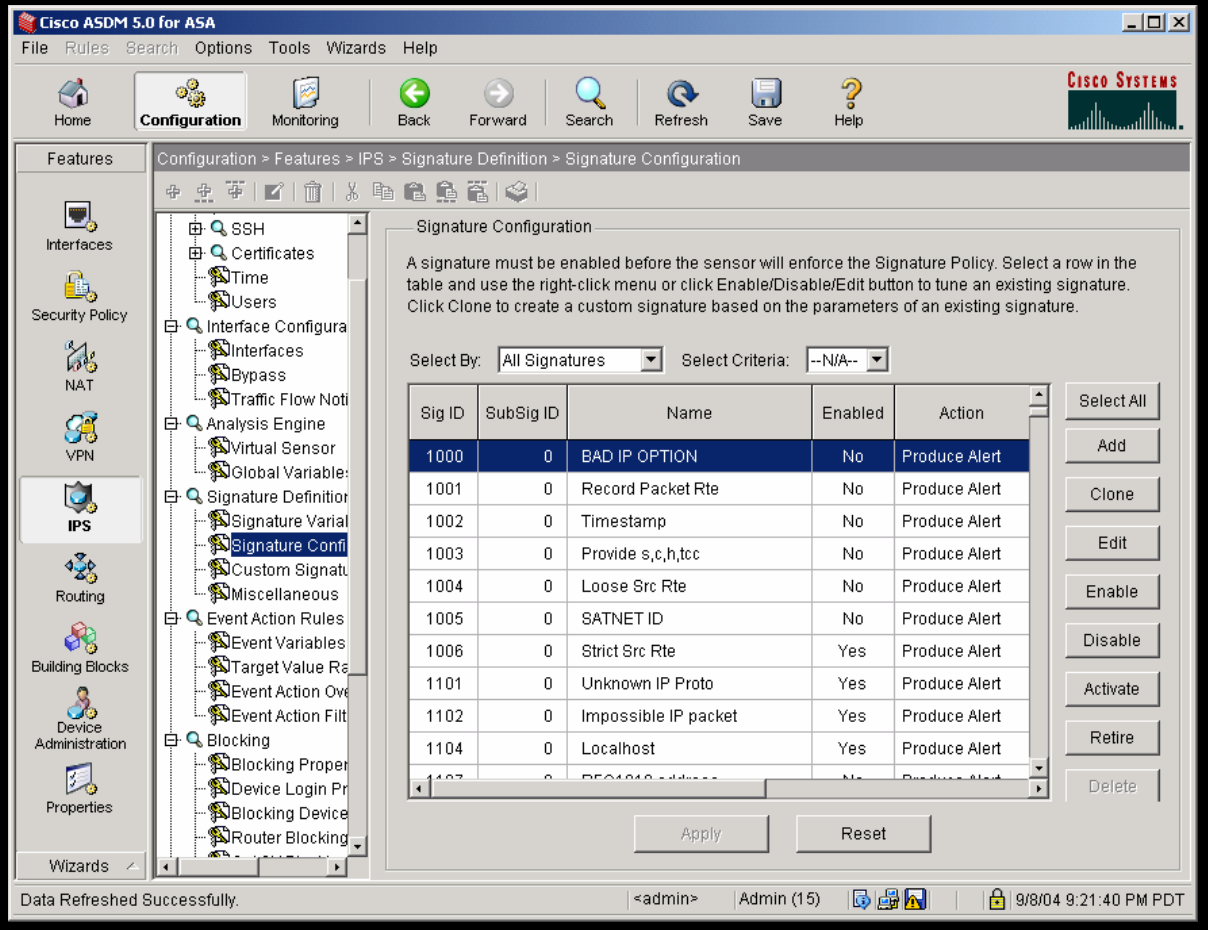
시스코 Adaptive Security Device Manager (ASDM)

방화벽 관리 및 제어 기능



- 시스코 ASDM v5.0
  - Firewall management and monitoring
- Full configuration 지원
  - Access control lists
  - Network 및 service object 그룹
  - Inspection Engines
  - NAT/PAT
  - AAA and more
- 모니터링 지원
  - Syslog (real-time)
  - 접속수
  - 성능 자료 및 기타

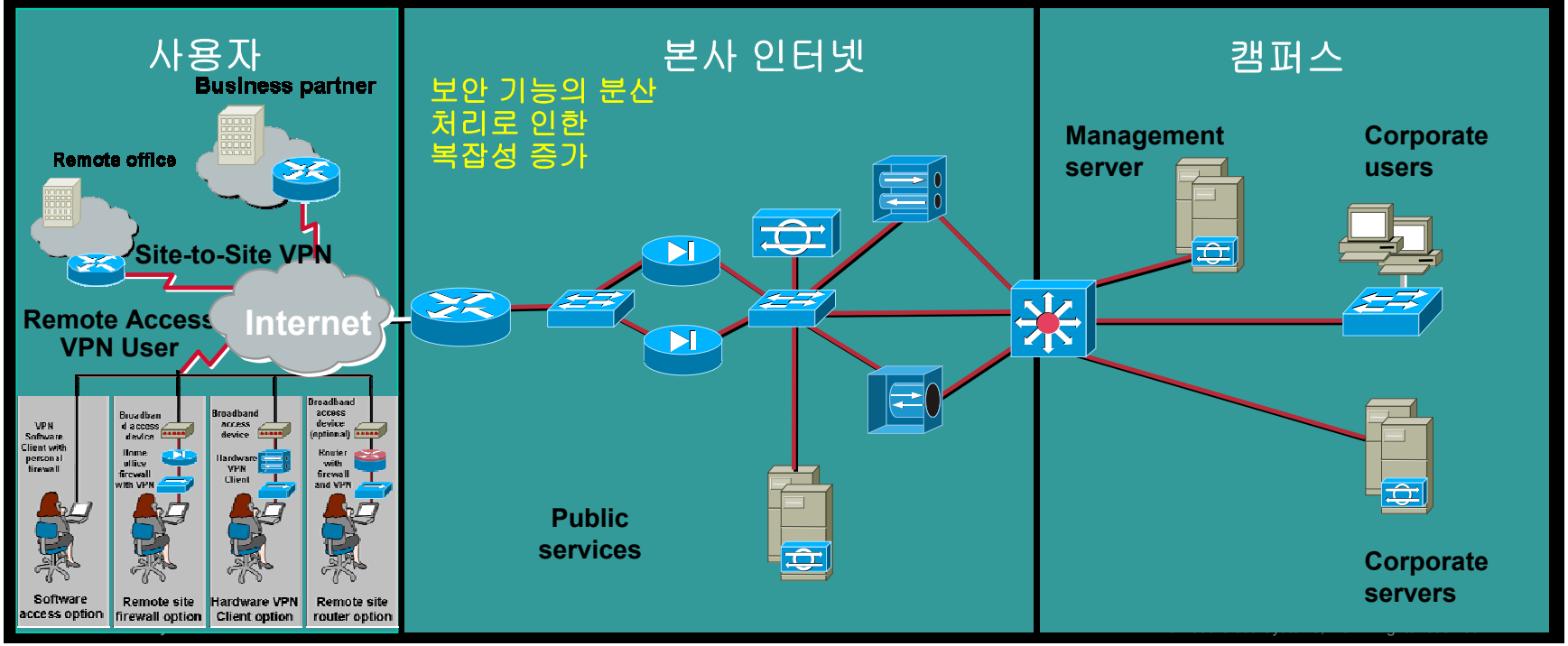
시스코 Adaptive Security Device Manager (ASDM)
IPS 관리 및 감시 기능



- **Cisco ASDM v5.0**
  - **IPS 관리 및 모니터링**
- **Full configuration지원**
  - **Engines**
  - **Signatures**
  - **Threat Risk Rating**
  - **IPS Actions 등등**
- 모니터링 지원
  - **Events**
  - **Diagnostic reports**
  - **Sensor statistics**

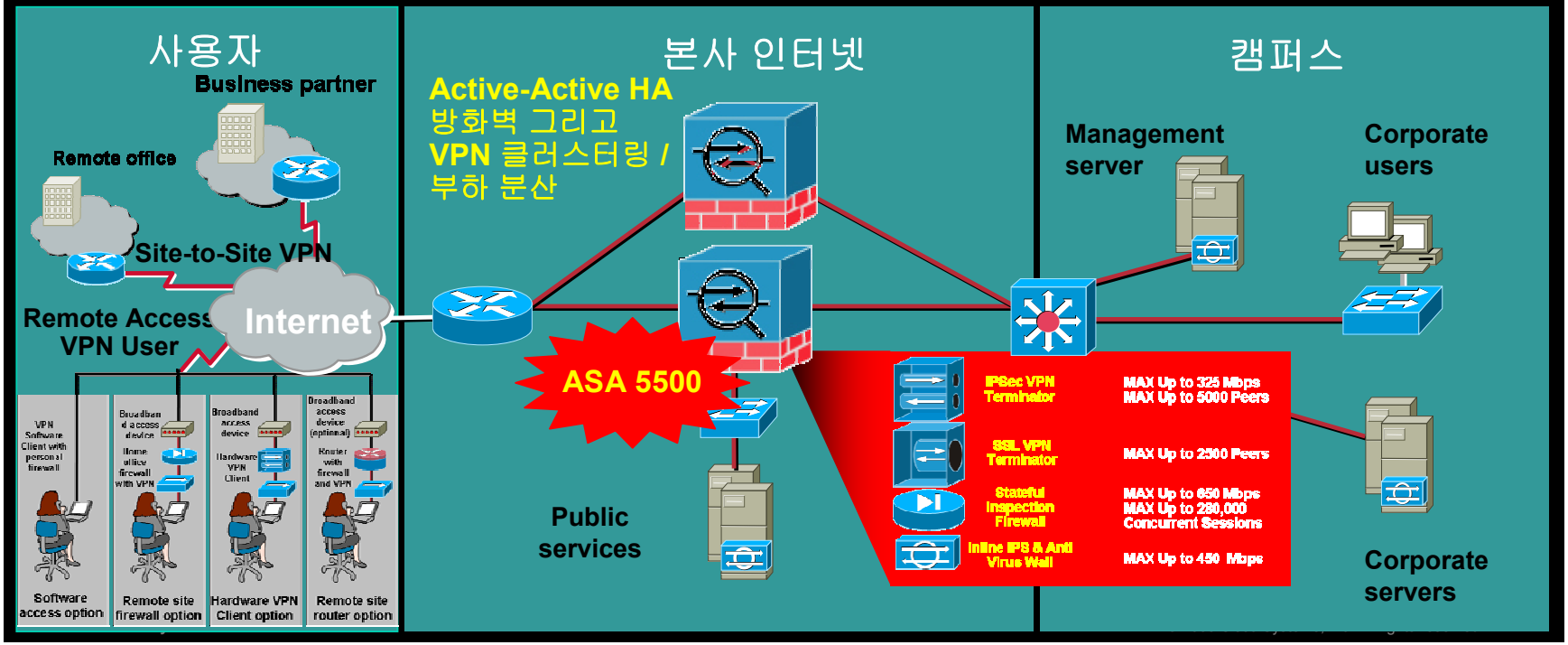
기존 보안 솔루션을 통한 네트워크 구성 예

- **Firewall, VPN, IDS/IPS** 을 개별적으로 구성
- 네트워크 구성 복잡 및 관리적 비용 과다



ASA 솔루션을 통한 네트워크 구성 예

- 기존 **Firewall, VPN, IDS/IPS** 를 단일 **Point** 로 구성하여 구성 단순화 및 관리적 비용 감소
- 추가 모듈 장착을 통한 다양한 부가 보안 기능 제공 **(Anti-virus, URL Filter** 등**)**
- **Active-Active HA** 및 **VPN Clustering** 및 **Load Balancing** 기능으로 **Service** 연속성 및 고 가용성 보장



시스코 ASA 5500 Summary

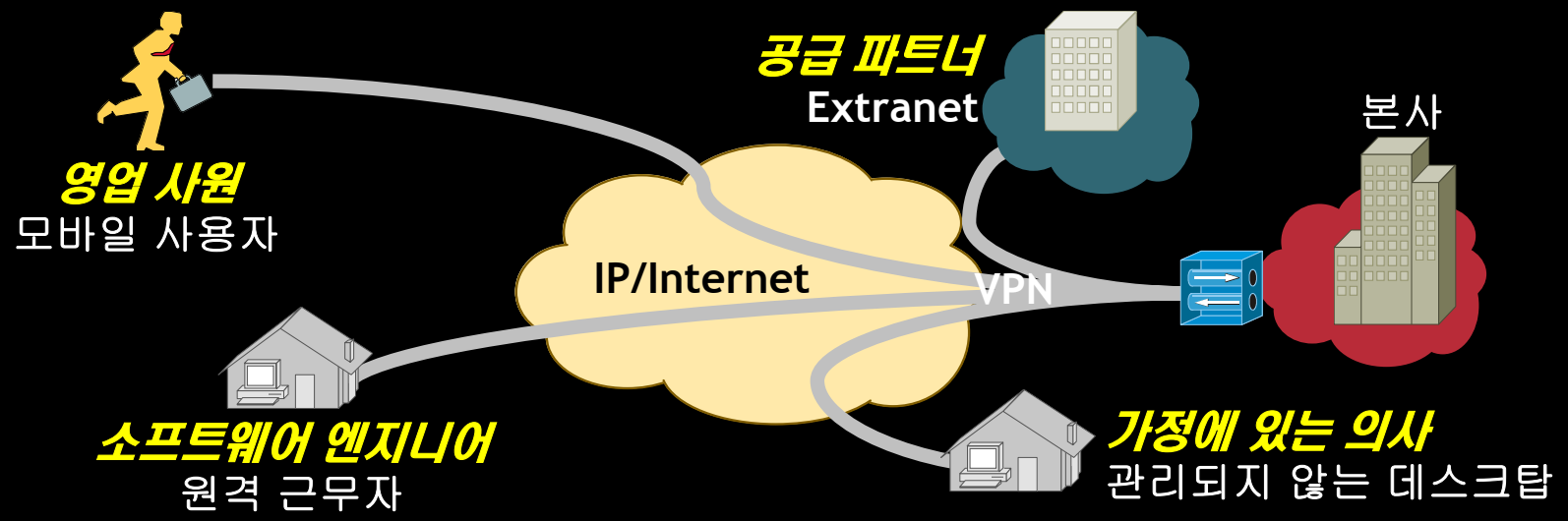
- **Cisco**의 **Market-Leading** 보안 기술을 하나의 장비로 통합
- 새로운 서비스 확장이 쉬운 구조
- 비용 효율적인 보안 서비스 전개
- 관리의 편의성

ASA 세부 기능

- SSL VPN

원격 접속에 대한 두가지 방안

Using "Best Fit" IPSec and SSL VPN Technologies



SSL VPN	IPSEC VPN
• **파트너** – 응용 프로그램 및 서버 이용이 제한적 , 엄격한 엑세스 제어 필요, 데스크탑 환경에 대한 통제 불가능, 방화벽 제어 • **의사** – 간헐적 접속, 이용 가능 응용프로그램이 아주 제한적, 데스크탑 소프트웨어에 대한 통제 없음	• **엔지니어** – 이용하고자 하는 서버 및 응용프로그램이, 고유의 응용프로그램, VoIP, 빈번한 접속, 장시간의 접속 시간 • **어카운트 매니저** – **다양한 응용프로그램**,, 기업에서 관리가능한 데스크탑환경에서 작업 수행

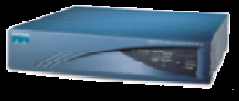
시스코 SSL VPN 장비

- **IPSec** 및 **SSL VPN** 통합 솔루션
- 다이나믹 로드 밸런싱 및 **VPN** 장비 클러스터링
- 다양한 사용자 인증 방법
- 통합 웹 기반 관리

Cisco ASA Series

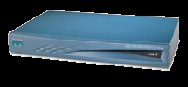
WebVPN Module for 6500/7600
~300Mbps, 8000 Users (4 blades Per Chassis – 32k users w/ 1.2 Gig of Throughput)

VPN 3030 Clusters
N x 500 = 1000s of SSL VPN Sessions



VPN 3030
500 SSL VPN Sessions

VPN 3020
200 SSL VPN Sessions

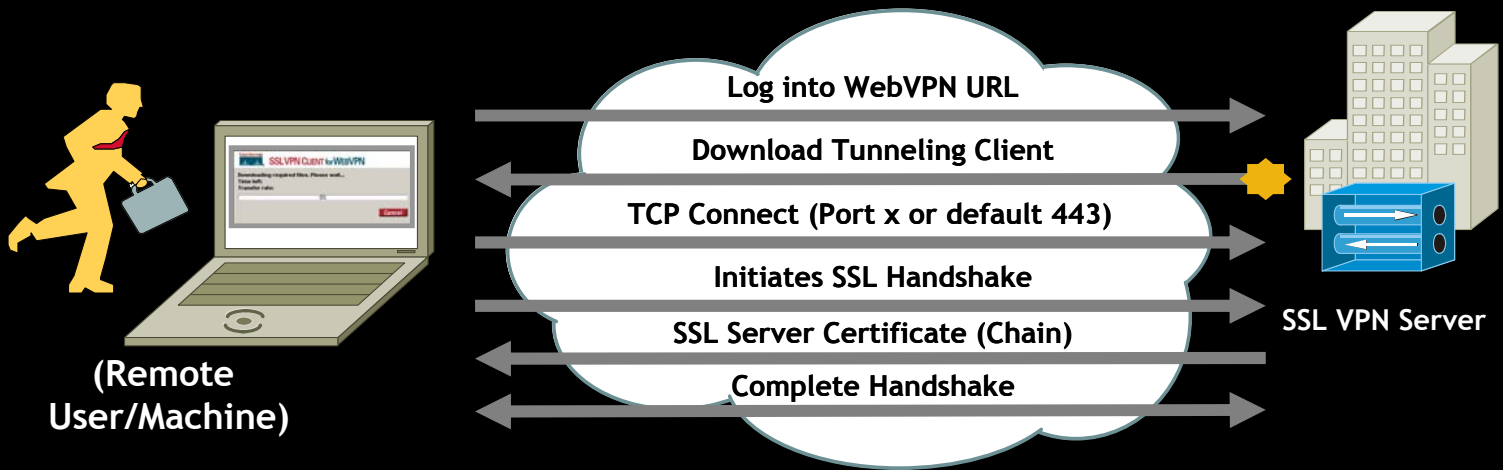


VPN 3005
50 SSL VPN Sessions

SOHO	ROBO	SMB	ENTERPRISE

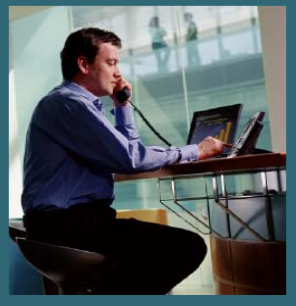
시스코 SSL VPN client 지원 방식은 ?

- 시스코 **SSL VPN Client** 지원 방식
  1. **Tunnel Mode : VPN Tunnel**
  2. **Clientless Mode : Web 기반의 접속**
  3. **Thin-Client Mode : Port-Forwarding**



Tunnel Mode 동작 방식

어떤 client 모델을 선택해야 하는가 ?



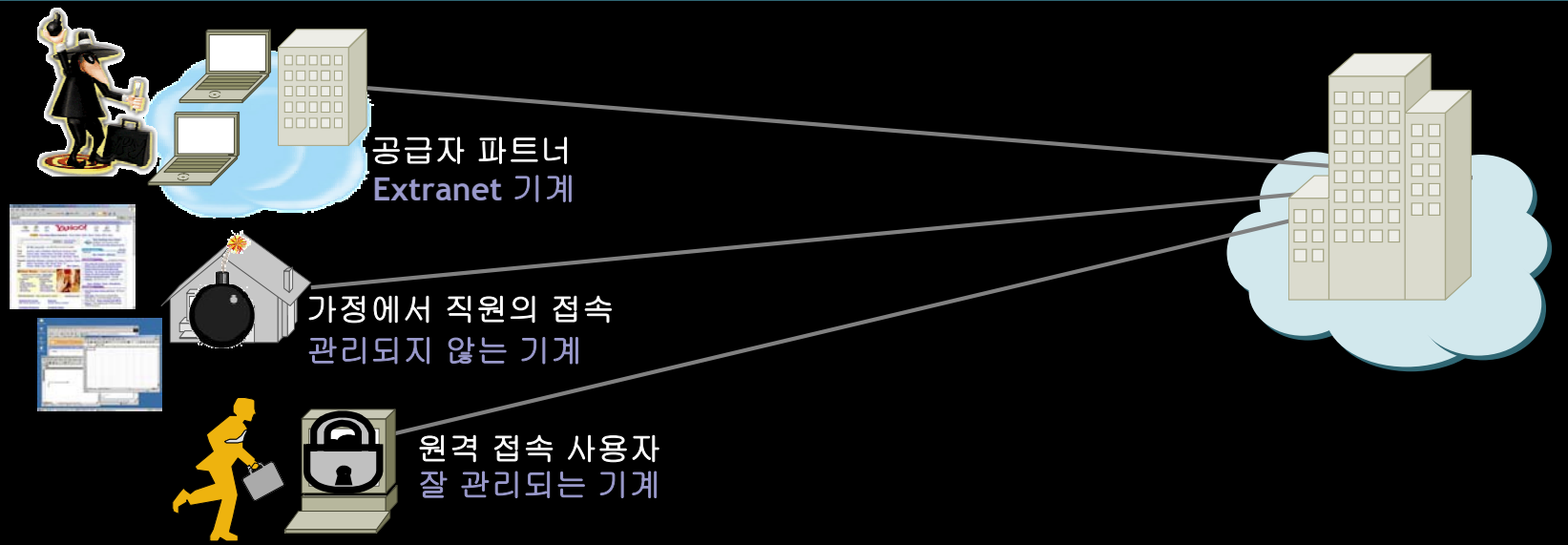
1. SSL VPN Tunneling Client
- 지속적인, "LAN과 같은" 네트워크 접속
- 어떤 응용프로그램의 접속도 가능
- 광범위한 응용프로그램 접속을 위한 최적의 옵션

2. Clientless, Web-Based Access
- Reverse 프락시 방화벽과 유사한 접속
- 웹 기반 응용프로그램 및 Citrix 접속
- 소프트웨어 다운로드 불필요
- 제한적인 웹 응용프로그램 접속과 관리불능의 데스크탑환경을 위한 최적의 옵션

3. Thin Client Port Forwarding
- Reverse proxy 방화벽과 유사한 접속 형태
- 웹, E-mail, 캘린더, IM 및 기타 여러 TCP 응용프로그램
- 조그만 자바 애플릿이 다이나믹하게 다운로드됨
- 제한적인 웹 및 클라이언트/서버 응용프로그램 및 관리하기 힘든 데스크탑의 환경을 위한 최적의 옵션

SSL VPN 이용 시 어떤 보안 문제가 있는가 ?

SSL VPN 사용은 또 다른 공격 포인트를 제공한다



SSL VPN 세션 사용 전 확인

- 누가 사용자 단말을 소유하고 있는 가 ?
- 단말 보안 상태는 : AV, 개인 방화벽 ?
- 현재 악성 프로그램 (malware)이 깔려 있는가 ?

SSL VPN 세션 사용 중 확인

- VPN 세션 데이터는 잘 보호되고 있는가 ?
- 입력한 패스워드는 잘 보호되고 있는가 ?
- 악성 프로그램 (malware) 이 수행되고 있는가?

SSL VPN 세션 사용 후 확인

- 브라우져가 인트라넷 웹페이지를 캐시하고 있는가 ?
- 브라우져가 패스워드를 저장하고 있는 가 ?
- 다운로드한 파일들이 계속 뒤에 남아 있는가 ?

보안 문제를 해결하기 위한 시스코 솔루션

Cisco Secure Desktop

접속전 사전 환경에 대한 평가:

- 접속 지점에 대한 평가 - 관리되는 데스크탑 ? 관리되지 않는 데스크탑 ?
- 보안 상태 평가 - AV 작동여부/업데이트, 개인 방화벽 작동 여부, malware존재 ?

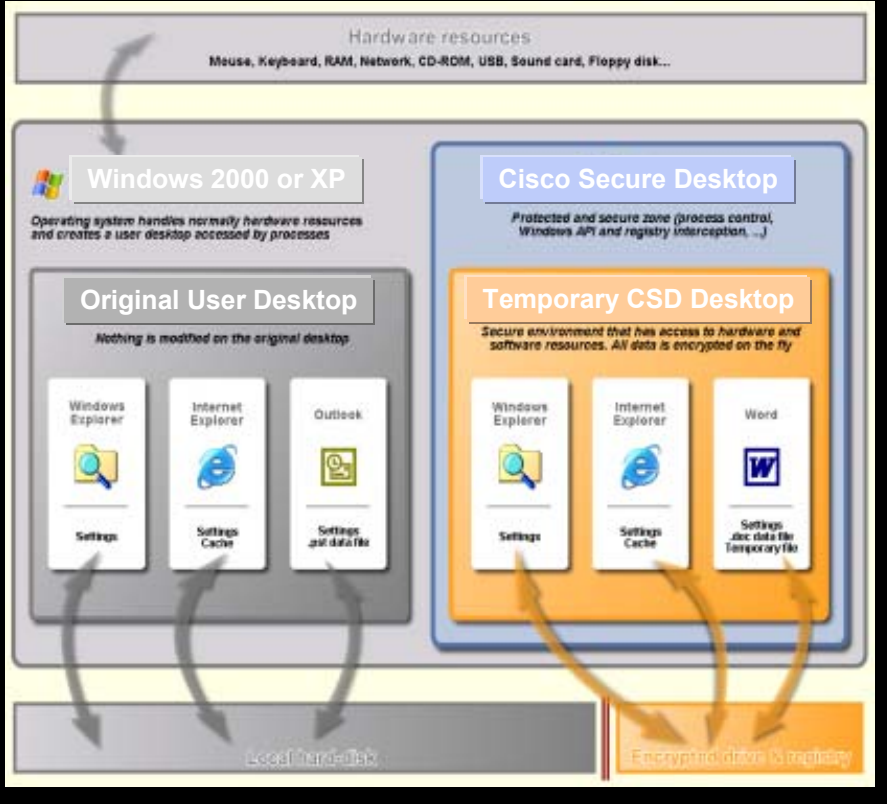
사용 중 완전한 세션 보호:

- Data sandbox and encryption protects every aspect of session
- 마이크로소프트 Malware 탐지 anti-spyware 소프트웨어

접속 후 세션 정보 Clean-Up:

- DoD 알고리즘을 이용한 암호화된 파티션 overwrite (삭제가 아님)
- 캐시, 히스토리 및 쿠키 overwrite
- 다운로드 파일 및 E-메일 첨부파일 overwrite
- Auto-complete 패스워드 overwrite

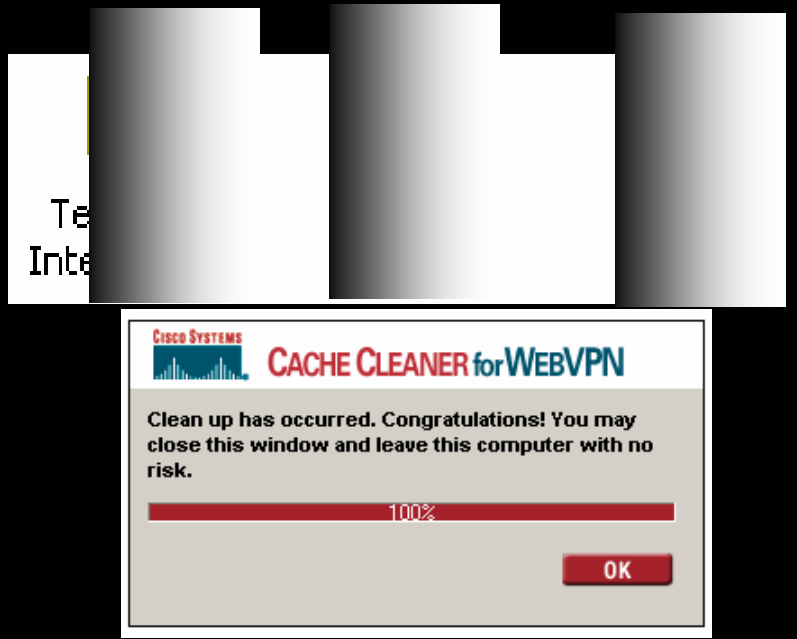
데스크탑 Guest Permissions으로 동작



보안 문제를 해결하기 위한 시스코 솔루션
캐시 클리너

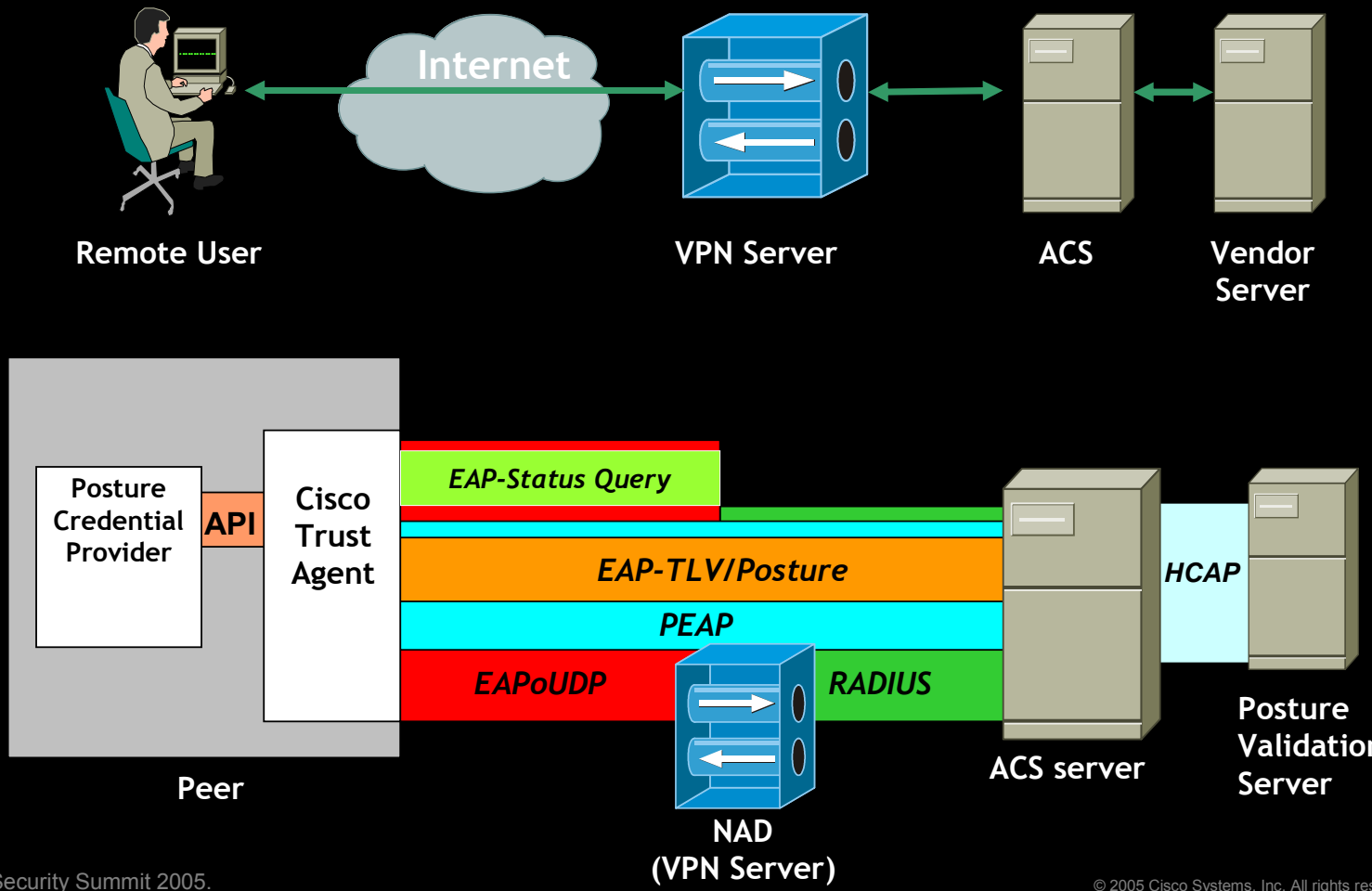
캐시 클리너는 세션 관련 정보 및 아래 정보를 제거해 줌:

- 쿠키 정보
- 히스토리 정보
- 캐시
- 패스워드



보안 문제를 해결하기 위한 시스코 솔루션

NAC 지원



ASA 세부 기능

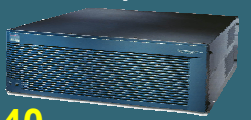
- Firewall

시스코 Firewall 장비
업계 최고의 보안 솔루션

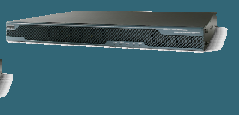
- 다양한 어플리케이션을 가진 상태 보존형(**Stateful**) **Firewall / Protocol** 검사기능
- 우수한 음성 및 멀티미디어 보안
- **Cost-Effective High Availability Solution**
- 웹방식의 편리한 사용 관리
- 강력한 원격 관리 옵션

Catalyst 6500 Firewall System
Up to 20 Gbps FW

PIX 535
1.7 Gbps FW



ASA 5540
650 Mbps FW



ASA 5520
450 Mbps FW

ASA 5510
300 Mbps FW

PIX 515E
190 Mbps FW

PIX 525
330 Mbps FW

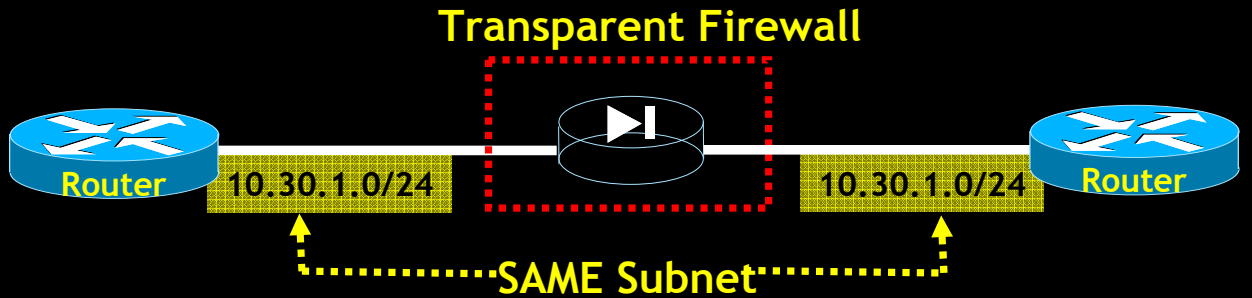
PIX 506E
100 Mbps FW

PIX 501
60 Mbps FW

SOHO | ROBO | SMB | Enterprise | Campus/SP

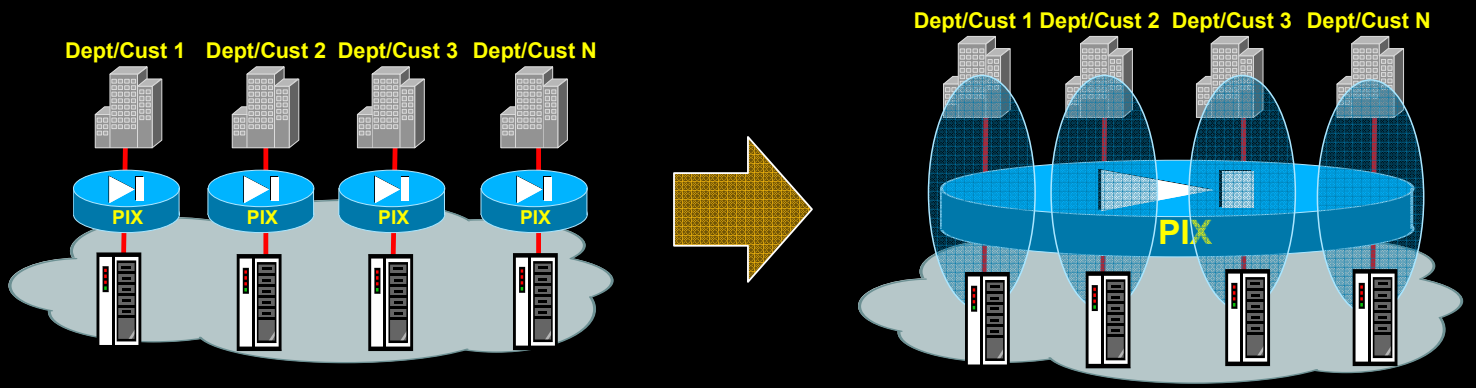
시스코 Firewall 특징

- ***Transparent firewall***



- L2~L7 까지의 모든 네트워크 레이어에 대해 L2에서 제어 가능

- ***Virtual Firewall***



- Firewall 의 논리적 분리로 운영 비용 절감 및 효율적 제어 가능

시스코 Firewall 특징
향상된 응용프로그램 및 프로토콜 Inspection

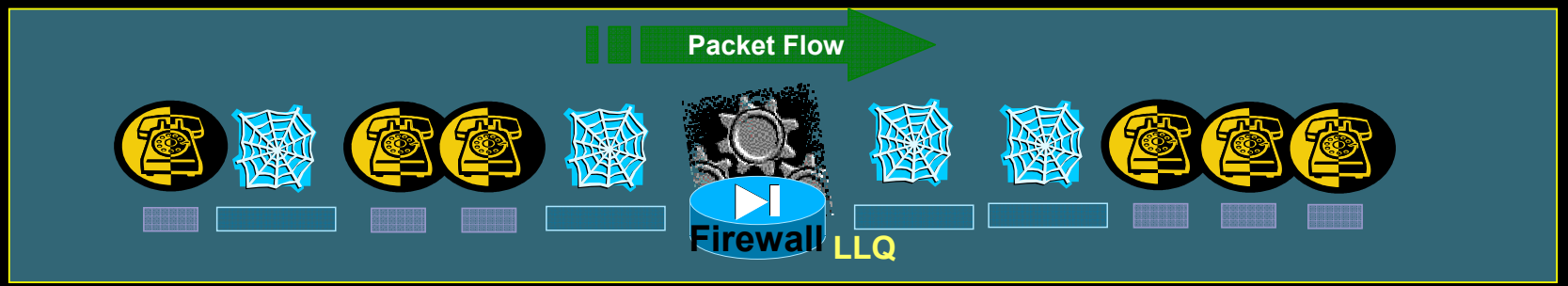
- **Inspection Engine Capabilities**

- Application Policy Enforcement
- Protocol Conformance Checking
- Protocol State Tracking
- Security Checks
- NAT / PAT Support
- Dynamic Port Allocation

- **Core Internet Protocols**
  - Web Inspection Engine : 인스턴트 메시징, MIME type filtering
  - FTP Inspection Engine : Put / Get / Dele등의 제어
  - ICMP Inspection Engine : Stateful tracking of ICMP traffic
- **Multimedia / Voice over IP**
  - H.323 v1-4, SIP, SCCP (Skinny), GTP (3G Wireless), MGCP, RTSP, TAPI / JTAPI
- **Specific Applications**
  - Cisco IP Phones, Cisco Softphones
  - Microsoft Windows Messenger, Microsoft NetMeeting, Real Player
- **Database / OS Services**
  - ILS / LDAP, Oracle / SQL*Net (V1/V2), Microsoft Networking, NFS, RSH, SunRPC /NIS+, X Windows (XDMCP)

시스코 Firewall 특징
VoIP 및 QoS 지원

H.323	MGCP	RTSP	SCCP	SIP	TAPI / JTAPI
NAT/PAT	NAT/PAT	NAT	NAT/PAT	NAT/PAT	NAT/PAT
Version1-4	v0.1/v1.0	TCP	TCP	UDP/TCP	TCP
Fragmentation and Segmentation Support					



Conc. Calls

PIX			ASA
515	525	535	5540
250	1500	3000	6000+

VoIP performance through the PIX / ASA

시스코 Firewall 요약

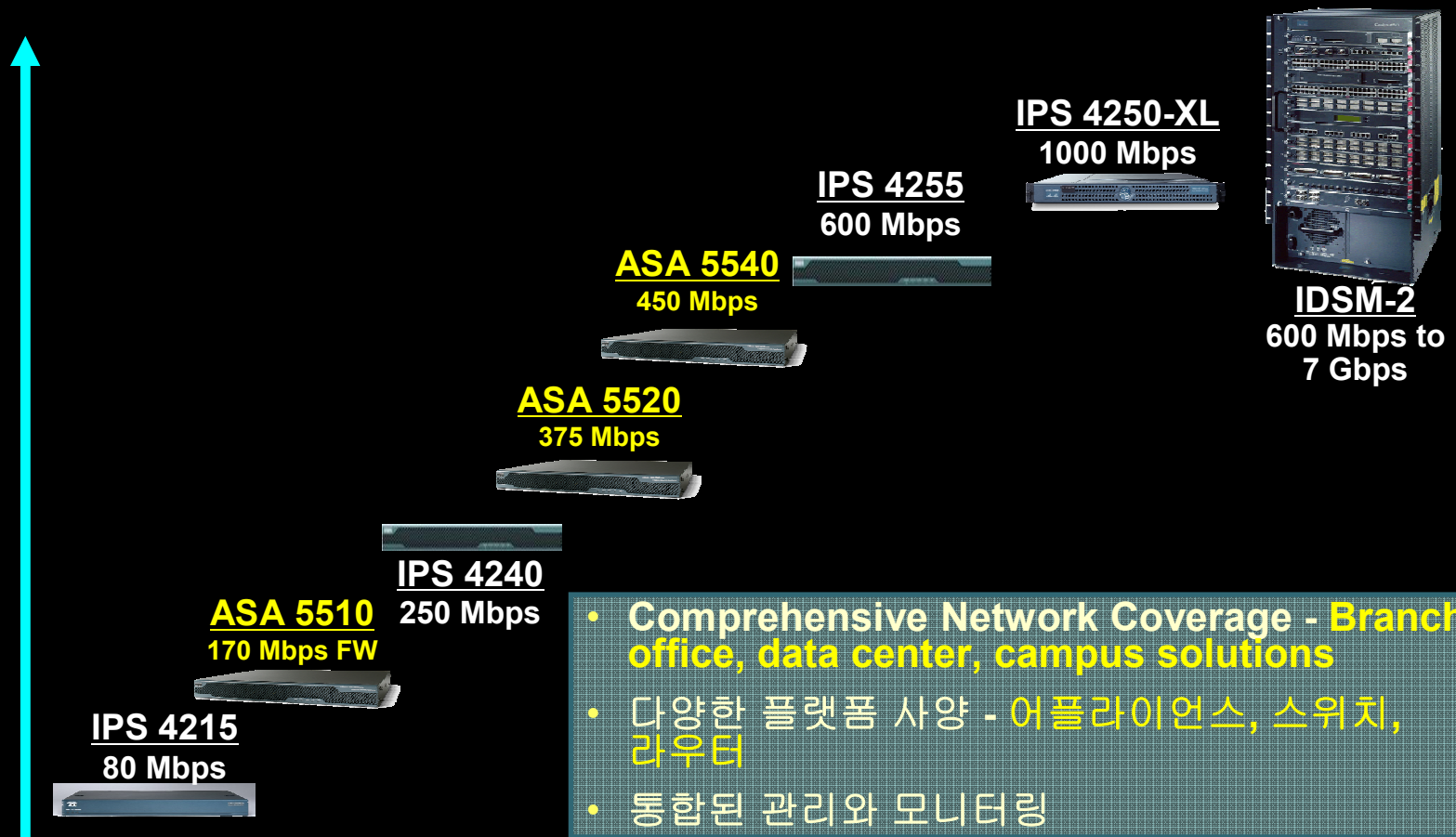
- **Transparent Firewall** 및 **Virtual Firewall** 지원으로 다양한 환경 적용 가능
- **L7** 응용프로그램에 대한 통제 가능 **(Web, FTP, ICMP …)**
- **VoIP** 등 다양한 멀티 미디어 프로토콜 지원
- **QoS** 지원으로 멀티 미디어 데이터의 효율적 전송 가능
- 다양하고 편리한 구현 옵션

33

ASA 세부 기능

- IPS

시스코 IPS 장비

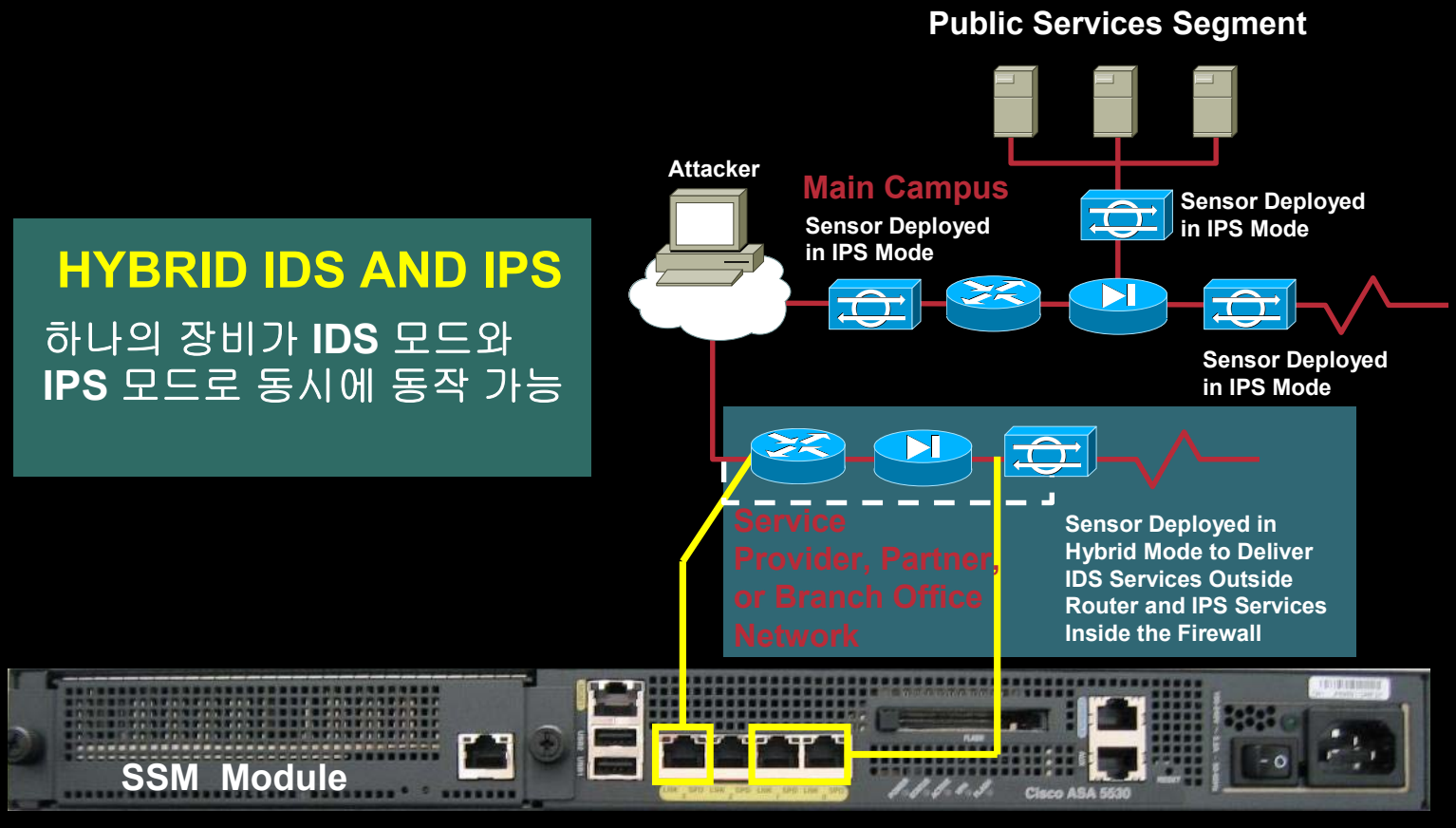


- Comprehensive Network Coverage - Branch office, data center, campus solutions
- 다양한 플랫폼 사양 - 어플라이언스, 스위치, 라우터
- 통합된 관리와 모니터링

IDS/IPS 의 편리한 옵션

HYBRID IDS AND IPS

하나의 장비가 **IDS** 모드와
IPS 모드로 동시에 동작 가능



시스코 IPS 의 가용성

Configurable* SW Bypass Mechanism delivering High Availability to IPS deployment

***Bypass can be configured in Auto / Manual Modes**

시스코 IPS 의 정확한 차단 기술
Risk Rating

이벤트 심각성 — 이 공격이 얼마나 심각한 문제인가?

+

시그니처 충실도 — 시그니처가 얼마나 정확한가?

+

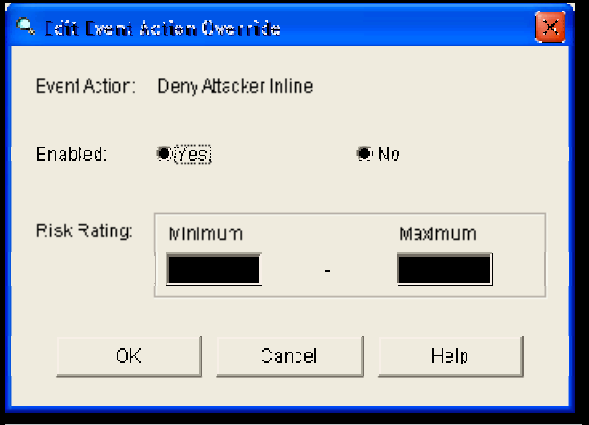
공격 연관성 — 공격 당하는 호스트와 연관되는 공격인가?

+

대상의 중요성 — 대상 호스트가 얼마나 중요한 장비인가?

위험 지수 → **Drives Mitigation Policy**

공격의 심각성과 함께 비즈니스에 미치는 영향까지를 고려한 결정



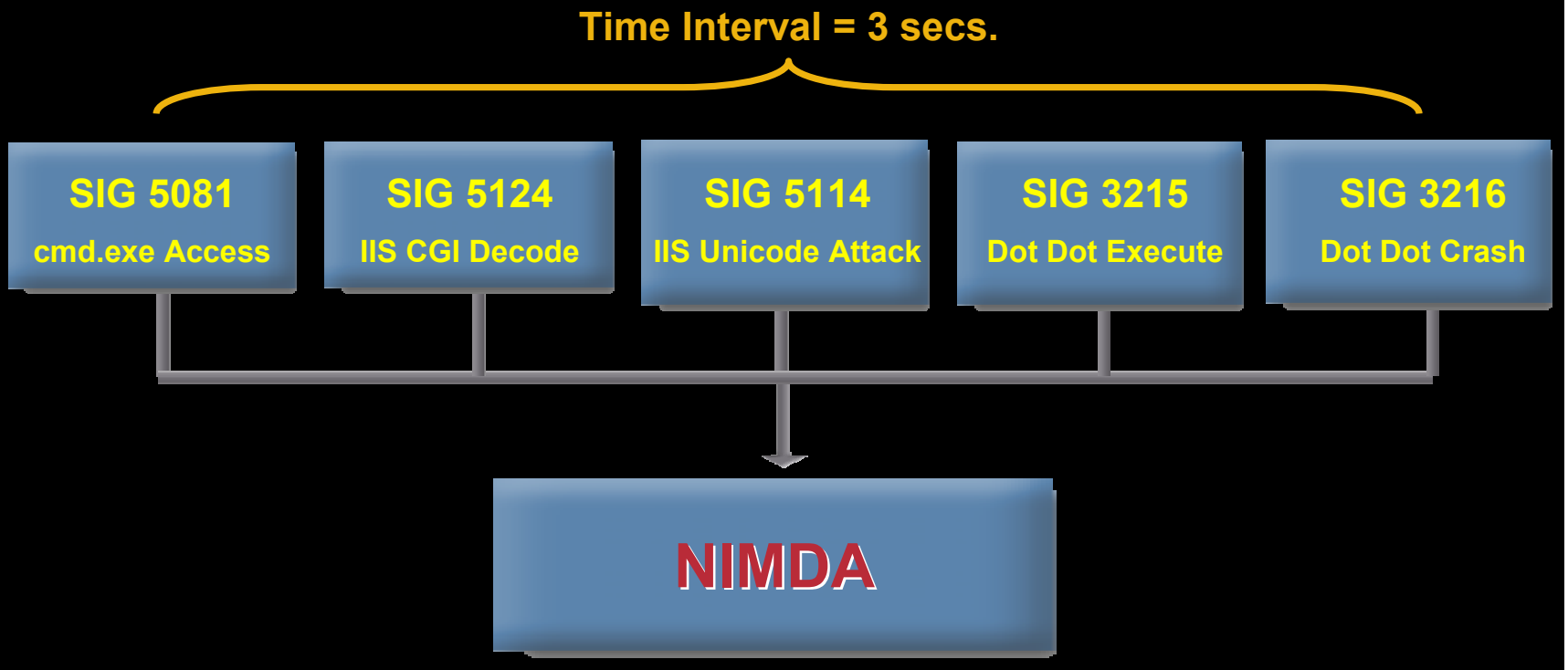
Customizable Risk Rating Thresholds :

0 < RR < 35	Alarm
35 < RR < 85	Alarm & Log Packets
85 < RR < 100	Drop Packet

시스코 IPS 의 정확한 차단 기술

MEG (Meta Event Generator)를 통한 장비 내의 이벤트 상호 연동

만약 **SIG IDs 5081, 5124, 5114, 3215 & 3216** 이벤트가 **3**초 간격 이내에 발생된다면, **MEG**로 **"Nimda"**이벤트가 발생



시스코 IPS 요약

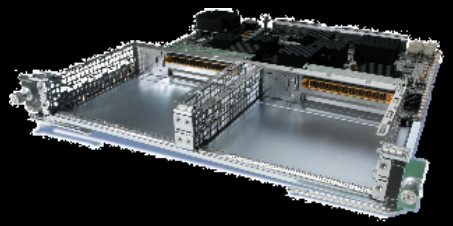
- 다양하고 정확한 위협 분석 기술 적용 **(Risk Rating, MEG)**
- 네트워크와의 완벽한 상호연계
- 다양하고 편리한 구현 옵션

대형 통합 보안 장비

- Catalyst 6500 과 보안 서비스 모듈

시스코 **Catalyst 6500** 보안 서비스 모듈

IPSec VPN SPA



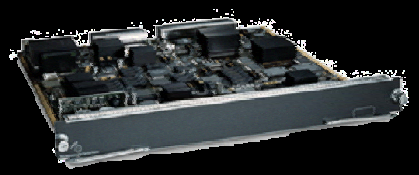
Services SPA Carrier Module

SSL VPN Module

Firewall Services Module (FWSM)

Cisco Catalyst 6500 Series

Intrusion Detection Module (IDSM2)



VPN Services Module (VPNSM)

SSL Module (SSL)

Network Analysis Module (NAM2)

6500 IPSec VPN Services SPA(Shared Port Adapter)

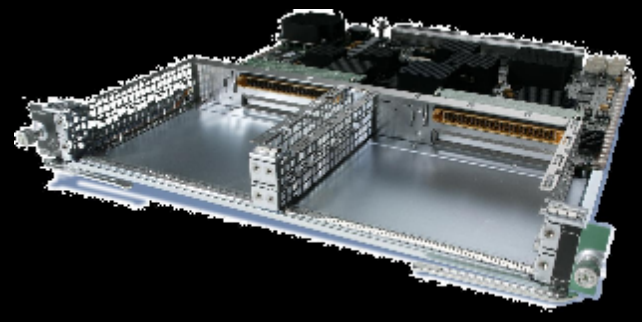
성능 및 Features

- Up to 2.5 Gbps AES (1.7 Gbps IMIX) per blade
- Up to 10 IPSec VPN SPA per platform (25 Gbps or 5 Mpps)
- Up to 8,000 IPSec Tunnels, up to 65 Tunnels/second
- DES, 3DES, and AES (128, 192, 256-bit key sizes)
- Jumbo Frame support

Integrated Platform Strengths

- SIP/SPA form factor
- Support with Sup720
- Support with Sup32 – target Q3CY05

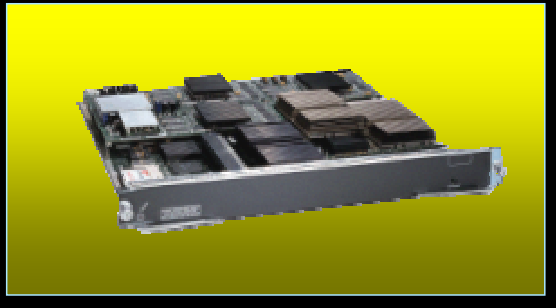
IPSec VPN SPA



Services SPA Carrier Module

6500 Web VPN Services Module

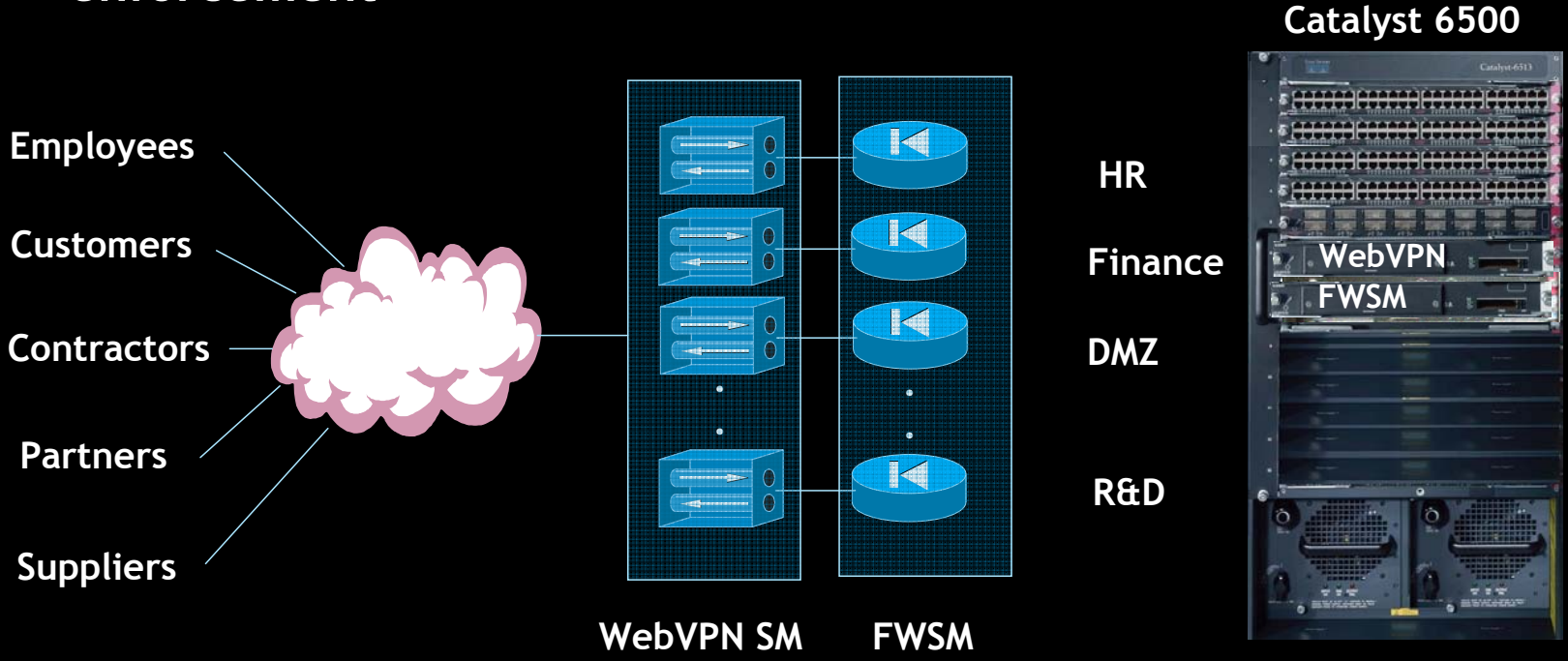
- 대규모 사업장을 위한 확장성
  - 모듈당 **8000** 사용자 지원
  - 스위치당 **32,000** 사용자 지원
- **Virtualized SSL VPN Service** 지원
  - **64 Contexts per module, 256 per switch**



Scale / Performance	
SSL Connections per Module	8,000
SSL Sessions per Module	32,000
Throughput per Module	300 Mbps
Setup Rate	1000/Sec
Modules per Chassis	4
Max SSL Connections per Chassis	32,000

SSL VPN – Security Service Convergence

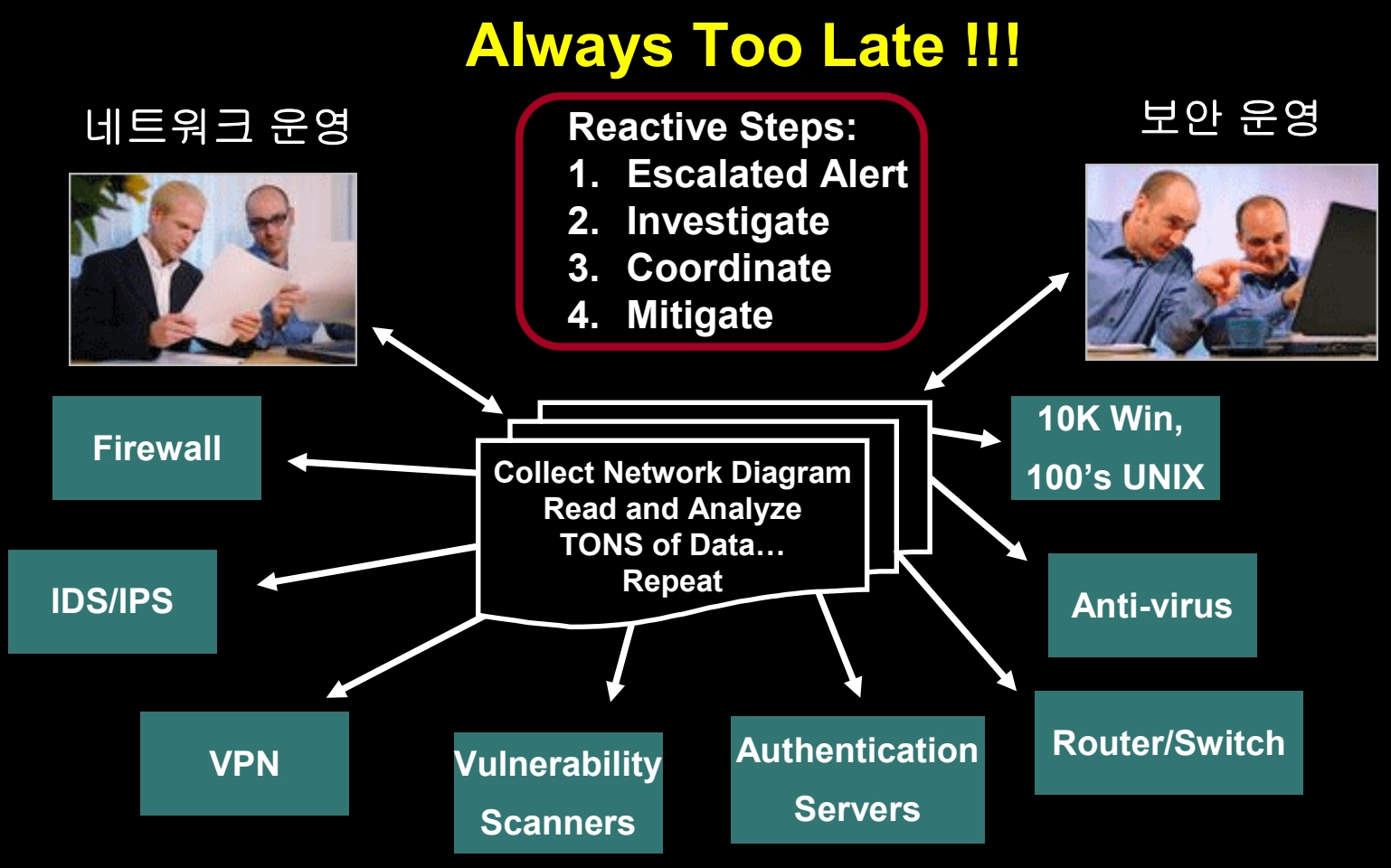
- Virtual SSL VPN Contexts mapped to Virtual Firewall Contexts
- Integrates remote access with corporate policy enforcement



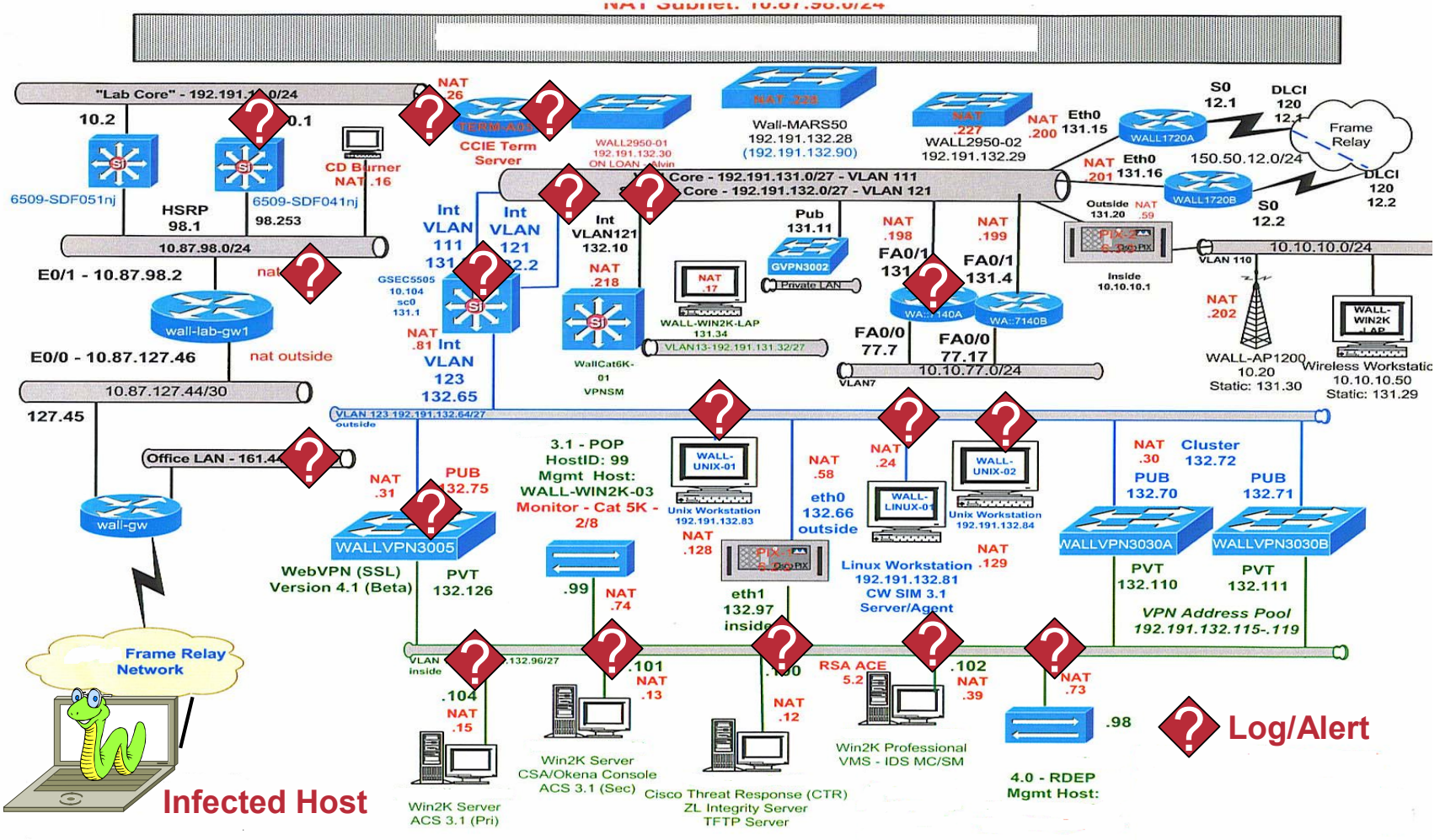
통합 보안 관리 제품

- CS-MARS (Monitoring, Analysis, and Response System)

보안 운영 시스템의 대응



Defense-In-Depth = 복잡합니다!!



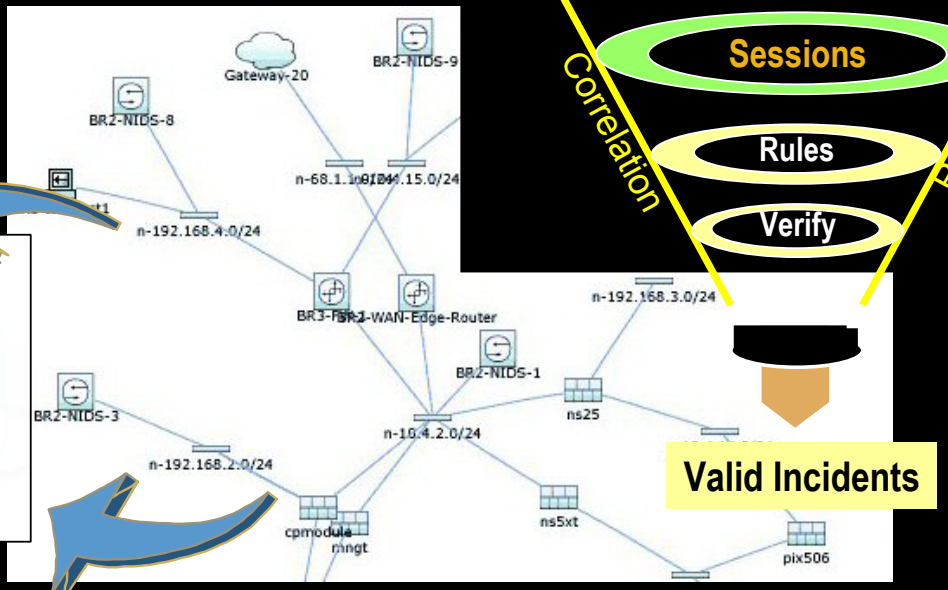
Firewall Log : 이 결과를 어떻게 활용 하겠습니까?

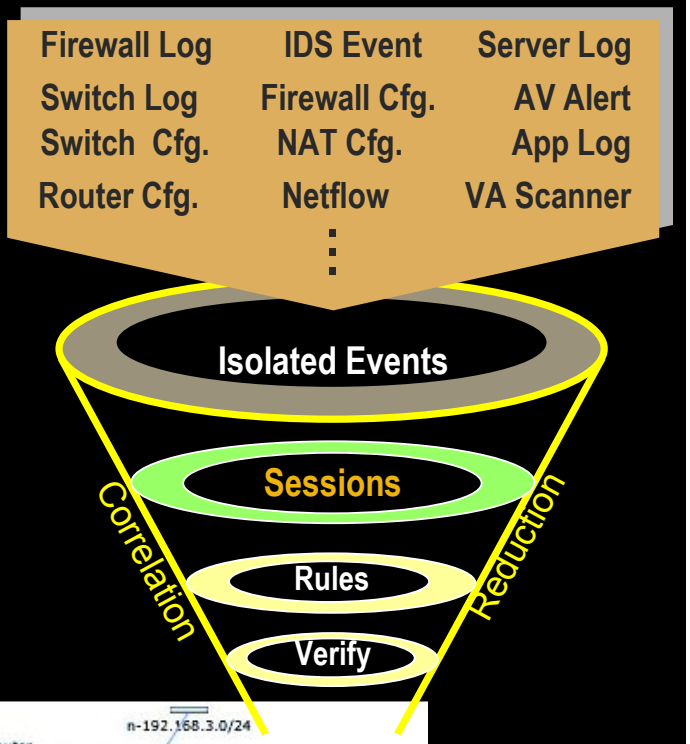
Telnet 192.168.1.1

```
302013: Built outbound TCP connection 207 for outside:198.133.219.25/80 (198.133.219.25/80) to inside:192.168.1.3/1606 (67.82.22
.18/1182)
305011: Built dynamic TCP translation from inside:192.168.1.3/1607 to outside:67.82.225.18/1183
302013: Built outbound TCP connection 208 for outside:198.133.219.25/80 (198.133.219.25/80) to inside:192.168.1.3/1607 (67.82.22
.18/1183)
304001: 192.168.1.3 Accessed URL 198.133.219.25:/favicon.ico
304001: 192.168.1.3 Accessed URL 198.133.219.25:/swa/j/cisco_detect.js
302014: Teardown TCP connection 207 for outside:198.133.219.25/80 to inside:192.168.1.3/1606 duration 0:00:01 bytes 5919 TCP Res
t-I
106015: Deny TCP (no connection) from 198.133.219.25/80 to 67.82.225.18/1182 flags ACK  on interface outside
106015: Deny TCP (no connection) from 192.168.1.3/1606 to 198.133.219.25/80 flags RST  on interface inside
106015: Deny TCP (no connection) from 198.133.219.25/80 to 67.82.225.18/1182 flags ACK  on interface outside
106015: Deny TCP (no connection) from 198.133.219.25/80 to 67.82.225.18/1182 flags ACK  on interface outside
302014: Teardown TCP connection 206 for outside:198.133.219.25/80 to inside:192.168.1.3/1602 duration 0:00:01 bytes 53445 TCP FI
s
305012: Teardown dynamic TCP translation from inside:192.168.1.3/1427 to outside:67.82.225.18/1142 duration 0:00:35
305011: Built dynamic TCP translation from inside:192.168.1.3/1610 to outside:67.82.225.18/1184
302013: Built outbound TCP connection 209 for outside:198.133.219.25/80 (198.133.219.25/80) to inside:192.168.1.3/1610 (67.82.22
.18/1184)
Jesus-Christ# sh log
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Standby logging: disabled
    Console logging: level informational, 919 messages logged
    Monitor logging: disabled
    Buffer logging: level informational, 915 messages logged
    Trap logging: disabled
    History logging: disabled
nslation from inside:192.168.1.3/1618 to outside:67.82.225.18/1052
305011: Built dynamic UDP translation from inside:192.168.1.3/29 to outside:67.82.225.18/42
302015: Built outbound UDP connection 210 for outside:167.206.3.158/53 (167.206.3.158/53) to inside:192.168.1.3/29 (67.82.225.18
42)
302016: Teardown UDP connection 210 for outside:167.206.3.158/53 to inside:192.168.1.3/1618 duration 0:00:01 bytes 158
305011: Built dynamic TCP translation from inside:192.168.1.3/1619 to outside:67.82.225.18/1185
302013: Built outbound TCP connection 211 for outside:64.154.80.250/80 (64.154.80.250/80) to inside:192.168.1.3/1619 (67.82.225.
8/1185)
304001: 192.168.1.3 Accessed URL 64.154.80.250:/HG?hc=we69&hb=DM5401281KAA%3BDM54012890CV&cd=1&hv=6&n=/Cisco.com+Public&con=&vc
=/%3B/Public&bn=Netscape&ce=y&ss=1024*768&sc=32&sv=13&cmp=&gp=&dcmp=&cy=u&hp=u&ln=en-US&cp=null&fnl=&pec=&vpc=090101r&vjs=090101
07r&seg=*;1&epg=n&ja=y&dt=5&zo=240&lm=0&cv=&gn=&ld=&la=&c1=&c2=&c3=&c4=&customerid=&ra=&rf=bookmark&pl=CDT%20Plug-in%3AQuickTime
20Plug-in%205.0.1%3AQuickTime%20Plug-in%205.0.1%3AQuickTime%20Plug-in%205.0.1%3AQuickTime%20Plug-in%205.0.1%3AQuickTime%20Plug-
%205.0.1%3AMozilla%20Default%20Plug-in%3AShockwave%20Flash%3AMicrosoft%AE%20DRM%3AMicrosoft%AE%20DRM%3AMetaStream%203%20Plugin%3
Java%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AHP%20Peripheral%20Interrogator%3AWindows%20
edia%20Player%20Plug-in%20Dynamic%20Link%20Library%3AAdobe%20Acrobat%3A&tt=auto_pos
305011: Built dynamic TCP translation from inside:192.168.1.3/1620 to outside:67.82.225.18/1186
302013: Built outbound TCP connection 212 for outside:64.154.80.250/80 (64.154.80.250/80) to inside:192.168.1.3/1620 (67.82.225.
8/1186)
305012: Teardown dynamic UDP translation from inside:192.168.1.3/1454 to outside:67.82.225.18/1040 duration 0:00:31
305012: Teardown dynamic UDP translation from inside:192.168.1.3/17 to outside:67.82.225.18/30 duration 0:00:31
302014: Teardown TCP connection 211 for outside:64.154.80.250/80 to inside:192.168.1.3/1619 duration 0:00:01 bytes 2652 TCP FINs
304001: 192.168.1.3 Accessed URL 64.154.80.250:/HGct?hc=we69&hb=DM5401281KAA%3BDM54012890CV&cd=1&hv=6&n=/Cisco.com+Public&con=&v
on=/%3B/Public&bn=Netscape&ce=y&ss=1024*768&sc=32&sv=13&cmp=&gp=&dcmp=&cy=u&hp=u&ln=en-US&cp=null&fnl=&pec=&vpc=090101r&vjs=0901
1.07r&seg=*;1&epg=n&ja=y&dt=5&zo=240&lm=0&cv=&gn=&ld=&la=&c1=&c2=&c3=&c4=&customerid=&ra=&rf=bookmark&pl=CDT%20Plug-in%3AQuickT
e%20Plug-in%205.0.1%3AQuickTime%20Plug-in%205.0.1%3AQuickTime%20Plug-in%205.0.1%3AQuickTime%20Plug-in%205.0.1%3AQuickTime%20Plug
in%205.0.1%3AMozilla%20Default%20Plug-in%3AShockwave%20Flash%3AMicrosoft%AE%20DRM%3AMicrosoft%AE%20DRM%3AMetaStream%203%20Plugin
3AJava%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AJava%20Plug-in%3AHP%20Peripheral%20Interrogator%3AWindows%
0Media%20Player%20Plug-in%20Dynamic%20Link%20Library%3AAdobe%20Acrobat%3A&tt=auto_pos
305012: Teardown dynamic UDP translation from inside:192.168.1.3/1462 to outside:67.82.225.18/1041 duration 0:00:31
305012: Teardown dynamic UDP translation from inside:192.168.1.3/18 to outside:67.82.225.18/31 duration 0:00:31
305012: Teardown dynamic UDP translation from inside:192.168.1.3/1463 to outside:67.82.225.18/1042 duration 0:00:31
305012: Teardown dynamic UDP translation from inside:192.168.1.3/19 to outside:67.82.225.18/32 duration 0:00:31
```

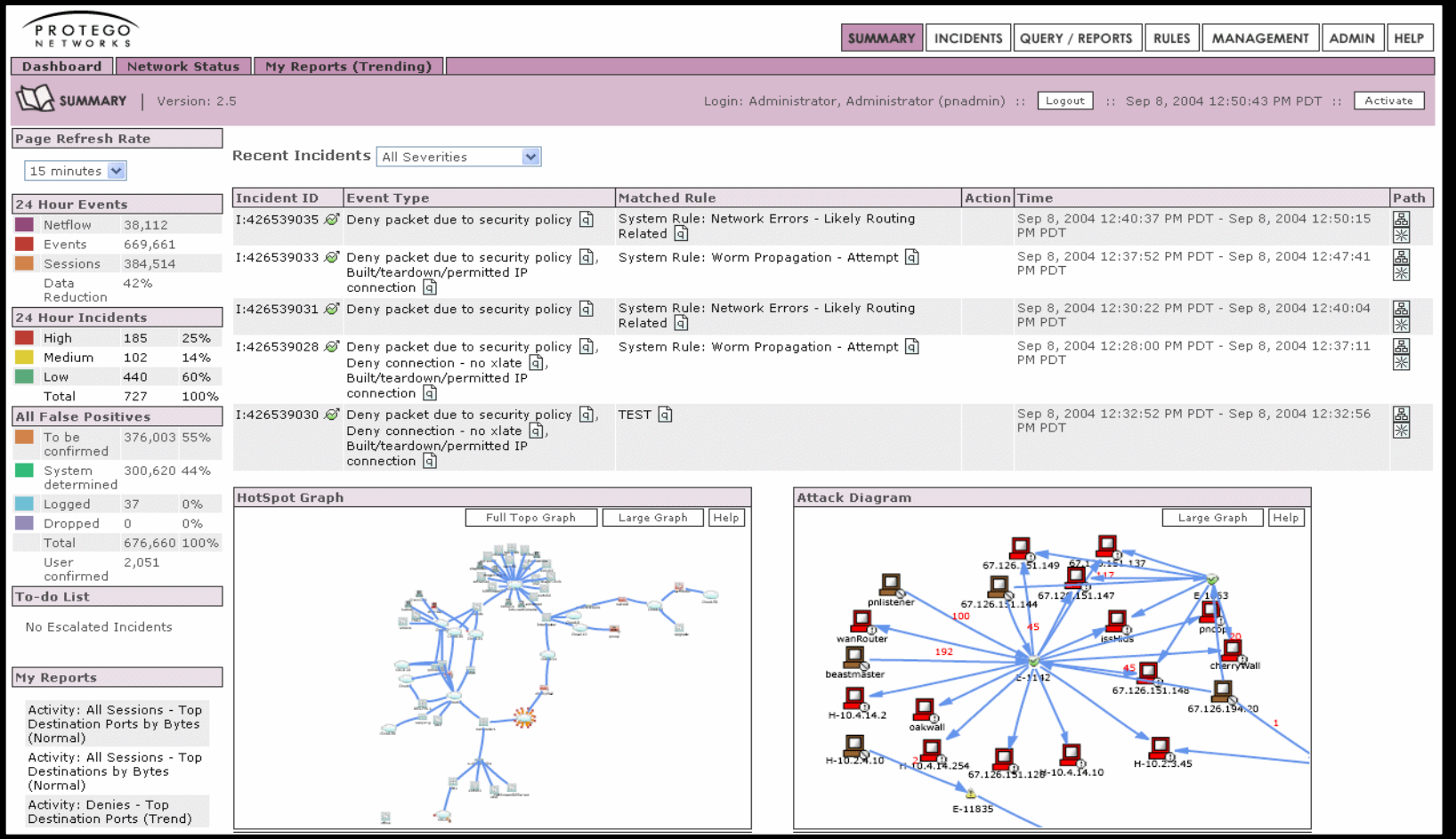
CS-MARS: "문제의 핵심을 파악하고 있습니다"

- 네트워크 지능성
  - 토플로지, 트레픽 플로우,
  - 장비구성, 장비 제어
- **ContextCorrelation™**
  - 이벤트의 연관성 분석, 이벤트를 분류하고 중복되는 부분 삭제,
  - 사건을 정확히 정의함



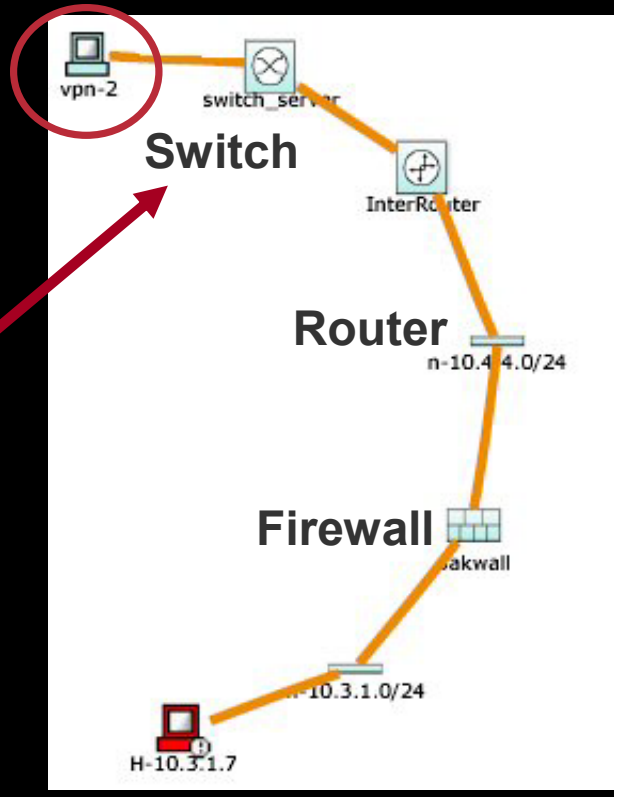


CS-MARS "이벤트 분석 & 네트워크 맵 제공"



CS-MARS 공격 PC가 연결된 스위치 포트 차단

- 해당 네트워크 인프라 내에서의 통제 기능 사용
  - **Layer 2/3 공격 경로의 가시화**
  - **공격 차단 적용 장비의 선택**
  - **정확한 차단 명령어 제공**



Enforcement Device: **switch_server**, Suggested

Enforcement Device Information

Device	Type	Manager	Children	Log To	Collects From	Info
switch_server	Cisco Switch-IOS 12.2	Protego Networks MARS 1.0 on pnvalis		N/A		

Interface Information

Direction	IP Address	Interface Name	DNS Name	MAC Address	MAC Update Time

Recommended Policy/Command

```
configure t
interface FastEthernet0/4
  no ip address
  shutdown
```

Push Cancel

CS-MARS "알기 쉬운 보고서 제공"

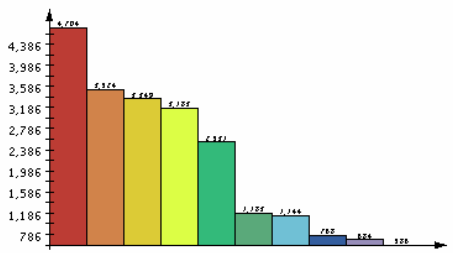
Report: Activity: Denies - Top Destination Ports Sep 8, 2004 1:07:45 PM PDT

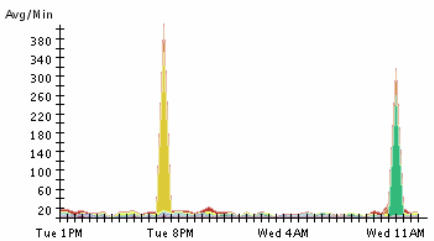
Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Activity: Denies - Top Destination Ports	*Every hour*	*Normal*	None	*Event type: AttacksProtected, FirewallPolicyViolation/ACL, Query Type: Destination Ports ranked by Sessions Time: 1dd:0hh:0mm:0ss*	This report ranks the destination ports to which attacks have been targetted but denied.	Finished: Sep 8, 2004 1:07:43 PM PDT	Sep 8, 2004 1:07:39 PM PDT	Sep 7, 2004 1:07:39 PM PDT - Sep 8, 2004 1:07:39 PM PDT

Report type: Destination Ports ranked by Sessions, 1dd:0hh:0mm:0ss

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Reported User
ANY	ANY	ANY	AttacksProtected, FirewallPolicyViolation/ACL	ANY	ANY	CA	None	ANY	ANY	ANY

Keywords: [None]





Rank		Count (# of sessions)	Raw Destination Port
	1	4704	445
	2	3524	80
	3	3349	26686
	4	3183	135
	5	2531	47683
	6	1183	1026
	7	1144	0
	8	768	139
	9	684	9898

CS-MARS 제품군

CS-MARS Model	20	50	100e	100	200	Global Controller
Events/Sec	500	1,000	3,000	5,000	10,000	N/A
NetFlow Flows/Sec	15,000	25,000	75,000	150,000	300,000	N/A
RAID Storage	120GB	120GB	750GB	750GB	1TB	1TB
Rack Size	1 RU	1 RU	3 RU	3 RU	4 RU	4 RU




- Installation takes minutes
- NO JRE Conflicts
- Raid 1+0
- Oracle Embedded - No DBA Needed

- Agent-less Event Collection
- Layer 2/3 Network Topology and Mitigation
  - NetFlow
  - Drill down to MAC addresses

CS-MARS 지원 장비 리스트

- *Networking*
  - Cisco IOS 11.x and 12.x, Catalyst OS 6.x
  - NetFlow v5/v7
  - NAC ACS 3.x
  - Extreme Extremeware 6.x
- *Firewall/VPN*
  - Cisco PIX 6.x, IOS Firewall, FWSM 1.x & 2.2, VPN Concentrator 4.0
  - CheckPoint Firewall-1 NG FPx, VPN-1
  - NetScreen Firewall 4.x, 5.x
  - Nokia Firewall
- *IDS/IPS*
  - Cisco NIDS 3.x & 4.x, IDSM 3.x & 4.x
  - Enterasys Dragon NIDS 6.x
  - ISS RealSecure Network Sensor 6.5, 7.0
  - Snort NIDS 2.x
  - McAfee Intrushield NIDS 1.x
  - NetScreen IDP 2.x
  - Symantec ManHunt 3.x
- *Vulnerability Assessment*
  - eEye REM 1.x
  - Foundstone FoundScan 3.x
- *Host Security*
  - Cisco Security Agent (CSA) 4.x
  - McAfee Entercept 2.5, 4.x
  - ISS RealSecure Host Sensor 6.5, 7.0
  - Symantec AnitVirus 9.x
- *Host Log*
  - Windows NT, 2000, 2003 (agent and agent-less)
  - Solaris
  - Linux
- *Syslog*
  - Universal device support
- *Applications*
  - Web servers (IIS, iPlanet, Apache)
  - Oracle 9i, 10i database audit logs
  - Network Appliance NetCache

시스코 CS-MARS Summary

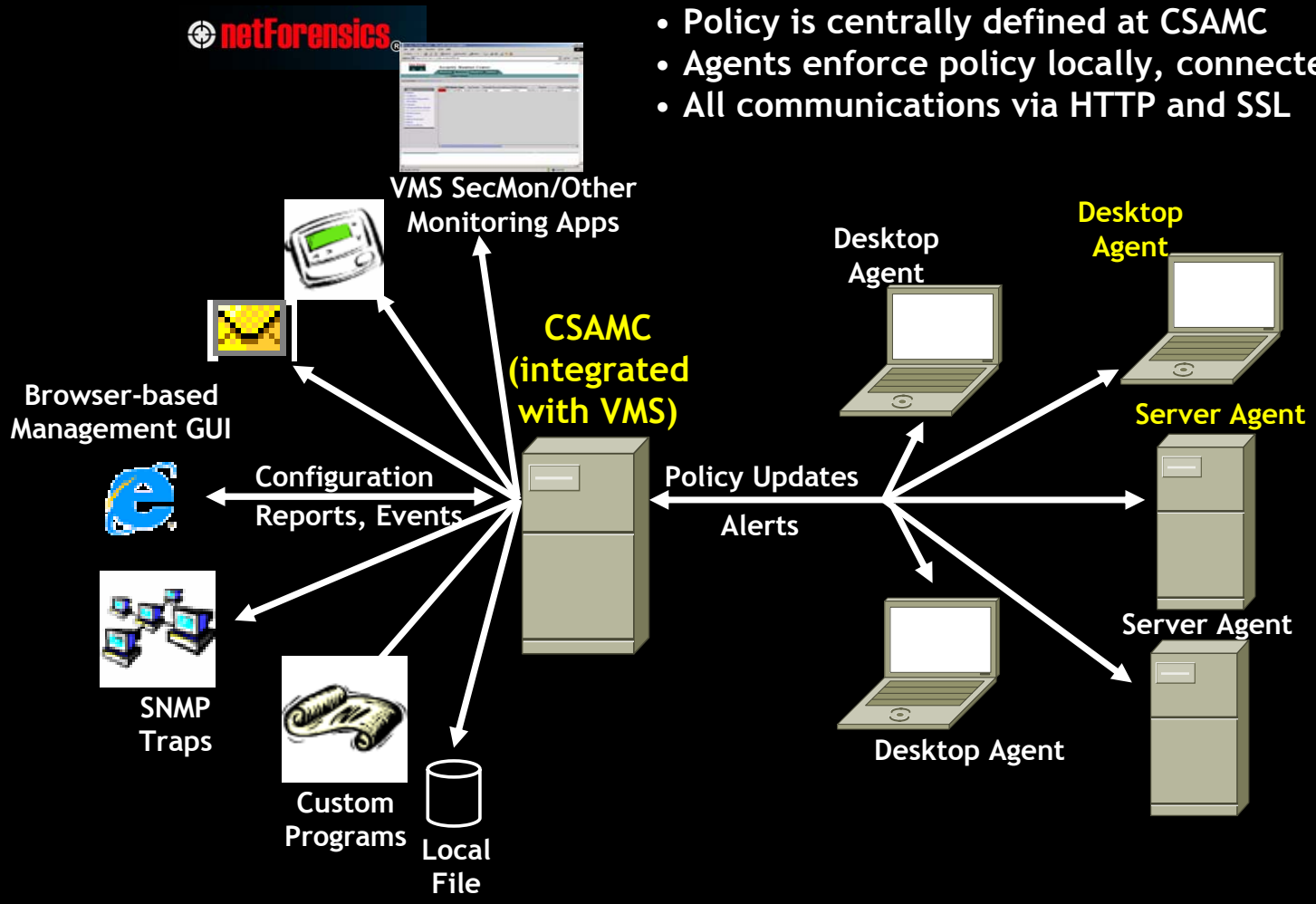
- 네트워크 전체에 지능적인 상호 연계
- 다양한 이벤트 분석을 통한 명확한 사건 정의
- 그래픽을 이용한 공격 경로 분석
- 지능적인 방어 방안 자동 제공
- 편리한 관리, 최고의 성능

사용자 보안 제품

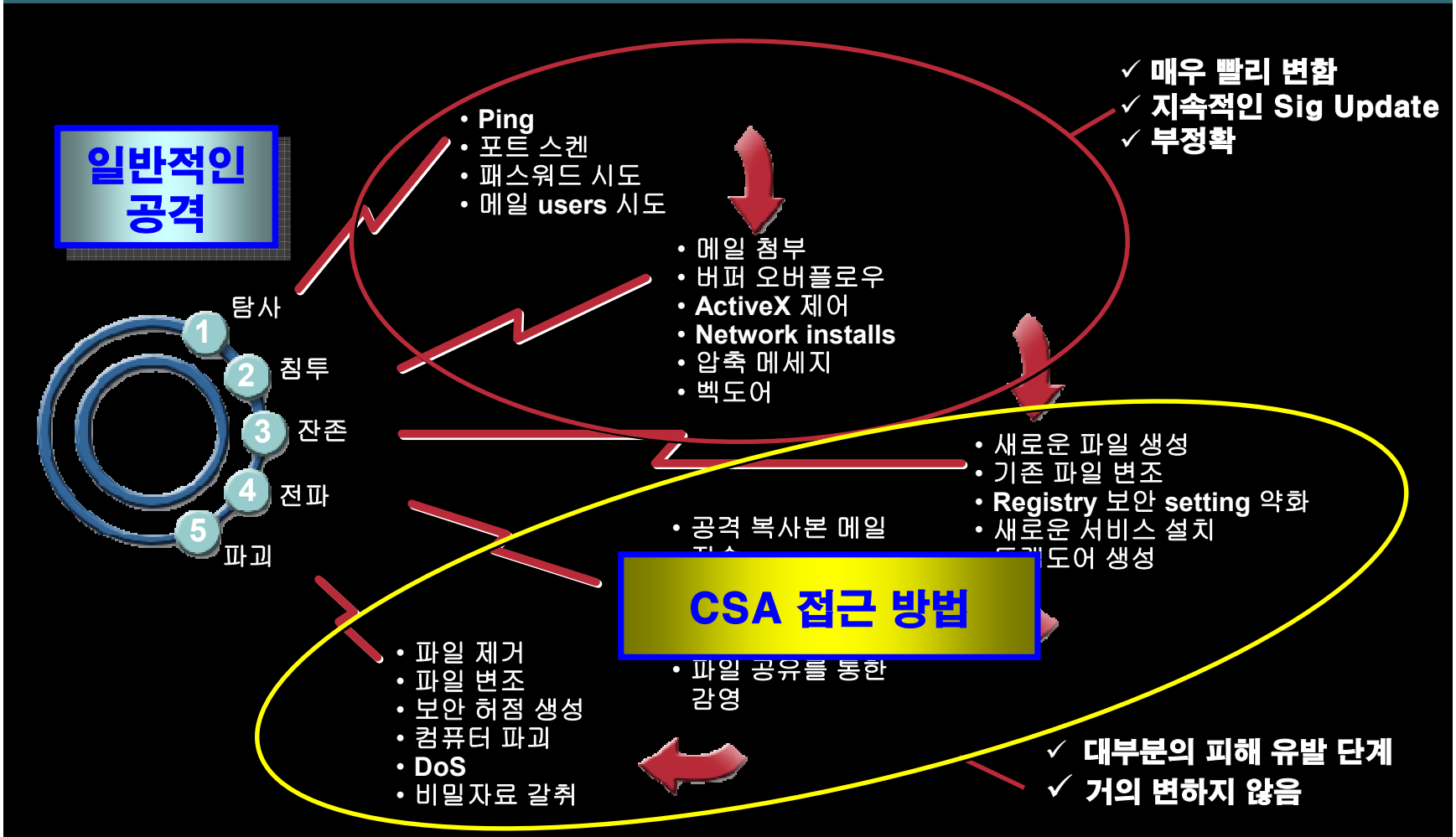
- Cisco Security Agent

CSA Architecture

- Policy is centrally defined at CSAMC
- Agents enforce policy locally, connected or not
- All communications via HTTP and SSL



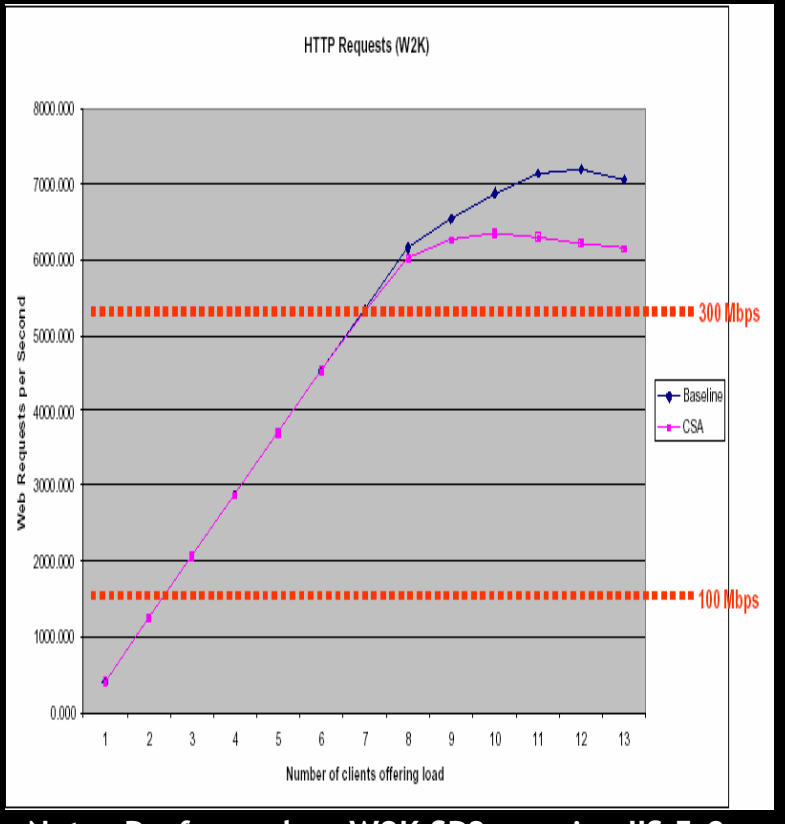
CSA 의 행위 기반의 공격 차단 원리



성능

- **Windows CPU 사용: 1-5%**
- **메모리 사용: 7-10MB, up to 20**
- **네트워크에 대한 영향:**
  - **Policy download: 35-70k**
  - **Event: ~3k**
  - **Poll: ~2.5k**
  - **Polling Interval change: ~3k**
  - **Software Update: varies**

Transactions per Second



Note: Performed on W2K SP3 running IIS 5.0. Single 2Ghz P4 CPU, 1Gbps NIC, non-hyperthreaded, 533Mhz system bus.

향상된 호스트 보호
스파이웨어, 강화된 NAC 연동

스파이웨어
- 스파이웨어의 설치/작동 차단
- 스캐닝 또는 시그니쳐 불필요
- 강력한 관리와 보고 기능
- **All-in-One 호스트 Agent**

동적으로 정책 결정
- 장비의 **NAC/Security** 상태
- 사용자 로그인 정보
- 장비의 위치

CSA Agent 한국어 지원

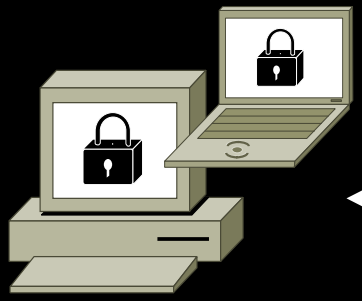
Windows 2000, Windows XP, Windows 2003 only

호스트 시스템 검사
- 단말에 설치된 모든 응용 프로그램에 대한 정보 수집
  - 응용프로그램 이름,버젼
- 핫픽스, 서비스팩 정보
- **NAC 지원 시스코 Trust Agent 포함**

호스트 상태 정보 + 위협 차단 으로
통합된 호스트 보호 제공

CSA 5.0 - Trusted QoS Solution

Cisco Security Agent

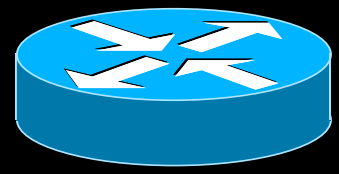


보안 레퍼런스 포인트
- Differentiated Service (DSCP) 을 설정 (QoS marking : Softphone, ERP, P2P)

Network Device - Access

Network Admission Control - 사용자 단말 상태를 확인 점검하여 비인가된 응용프로그램의 DCSP 설정 제거

Network Device - Routing



우선 순위에 따른 대역폭 할당

- CSA 와 NAC의 통합으로 QoS 신뢰성 제고 -> 단말에 대한 관리 및 필터링
- 여러 가지 DoS 상황에 대한 대처로 가용성 증대
- 모든 응용프로그램에 대해 CSA를 통한 QoS Marking 제공으로 주요 프로그램에 대해 따로 응용프로그램을 수정할 필요가 없음

CSA 요약

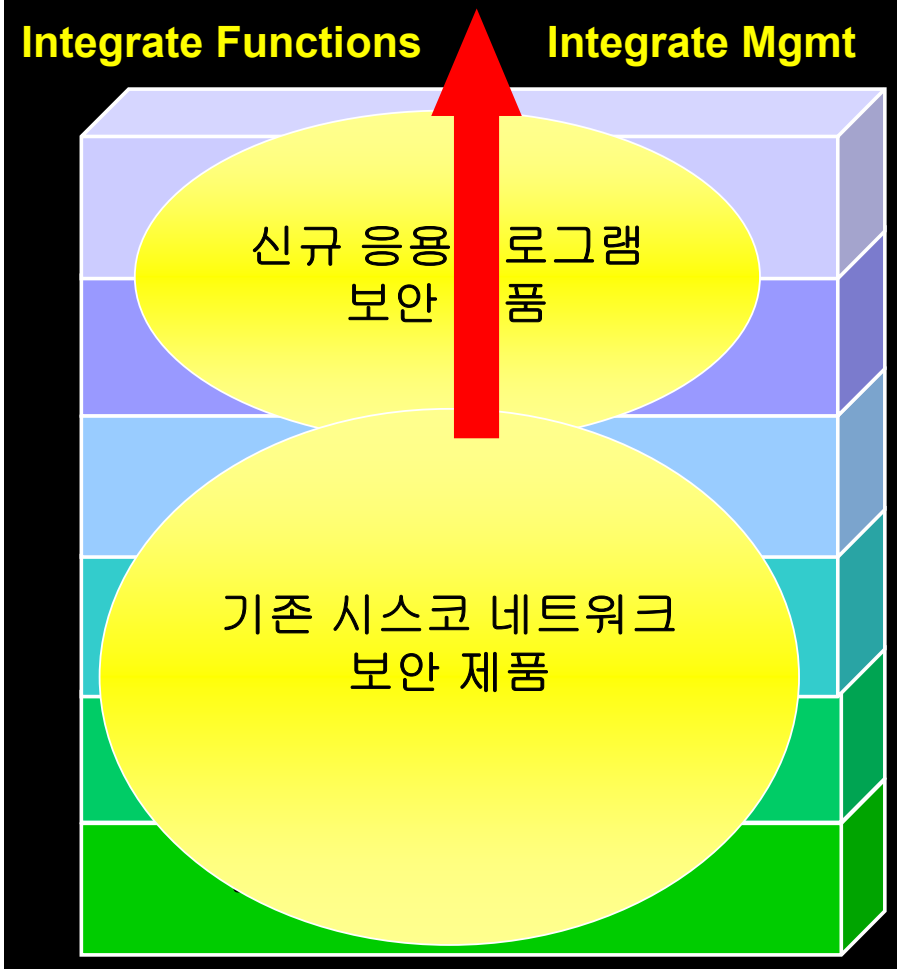
- **CSA** 는 피해가 발생하기 전에 사전에 방지
- **CSA**의 상관관계 분석에 의한 공격 범위 최소화
- **CSA** 행위 기반에 대한 인식 능력으로 **IT** 인프라의 효율적 사용 가능

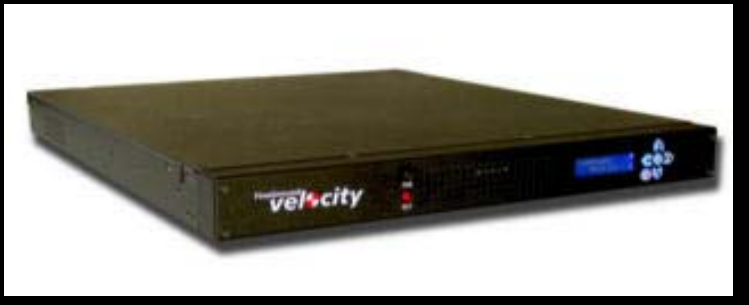
  -> CSA의 사용으로 **P2P,** 음악 파일의 다운로드 인스턴트 메시징 서비스 이용**, USB** 메모리의 사용 통제 등이 가능
- **CSA** 와 시스코 **NAC, QoS** 솔루션의 통합으로 다양한 보안 기능 구현

응용프로그램 관리/보안 제품

- AVS (Application Velocity System)

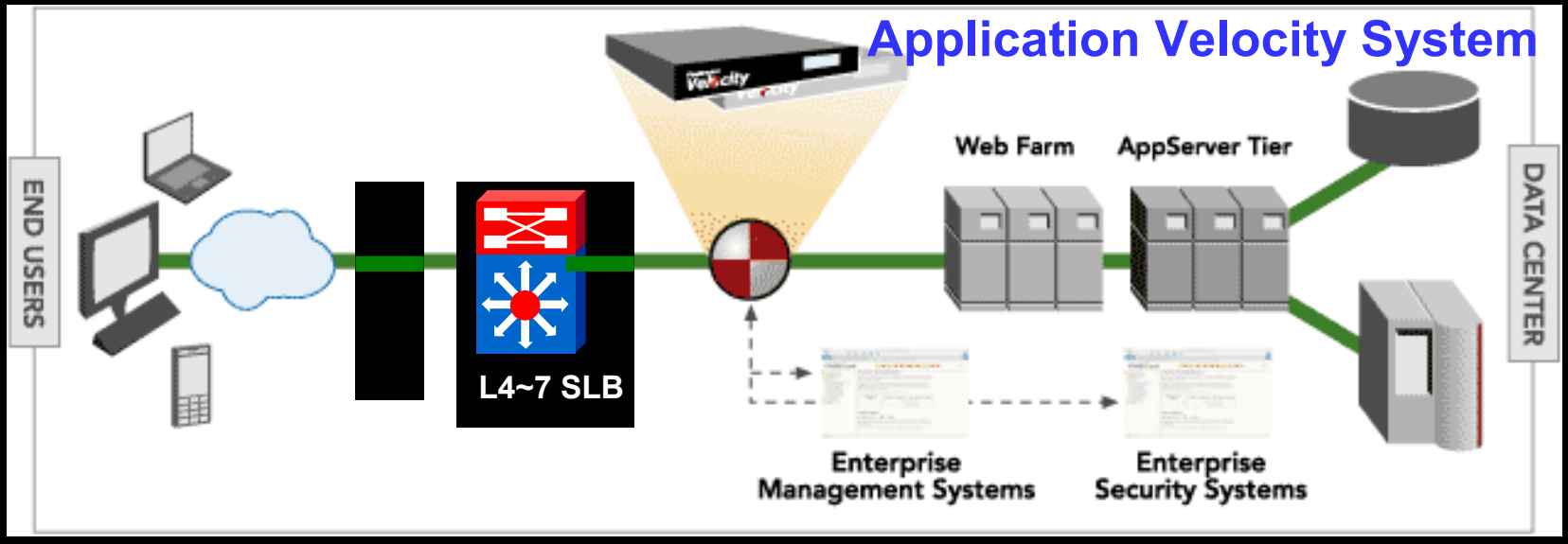
Cisco AVS 3100





- 응용프로그램 가속
- 응용프로그램 최적화
- 서버 부하 감소 – 서버 효율
- 응용프로그램 모니터링
- 응용프로그램 방화벽

응용프로그램 가속



- **AVS** 장비는 **2**가지 구성으로 적용 가능 :
  - **"Inline" :** 확장성 및 **Failover** 를 위한 내부 클러스터링
  - **"Out of band" :** 인프라를 관리하기 위한 **Layer 4-7 SLB**
    - 시스코 **L4** 스위치로 입증된 구성 환경
    - **AVS**는 **SLB** 장비에 대한 또 다른 웹서버로 인식

AVS 3100 Technology Advantage

Functional Areas	Standard Features	AVS-only Features
가속- 네트워크 지연 관리		▪ Request aggregation/Browser cache management ▪ Browser TCP multiplexing ▪ PDF download optimization ▪ Response redirection control
최적화-대역폭 절감	▪ Gzip/DEFLATE compression	▪ Delta encoding ▪ Dynamic browser caching ▪ Dynamic image optimization (JPG, GIF, PNG)* ▪ Flexible processing rules
서버 부하 감소 - 서버 효율	▪ TCP connection multiplexing ▪ SSL offload and acceleration ▪ Static caching	▪ Configurable dynamic caching ▪ Load-based caching ▪ Lazy request evaluation ▪ Single sign-on optimizations ▪ XML merging/transformation
모니터 - 응용프로그램 QoS	▪ Logging ▪ System health checking	▪ End-to-end response time monitoring ▪ Business transactions capability ▪ First-line service triage
응용프로그램 보안	▪ Rules-based definitions and capability	▪ Out-of-the-box Layer-7 protections ▪ Policy-based implementation ▪ Comprehensive exception handling & monitoring
관리 / 통합	▪ SNMP access and control	▪ Application delivery dashboard ▪ Service-level integration with BMC, HP, etc.

결론

보안제품도 시스코입니다.

- 통합 보안 제품
  - 시스코는 단품 방식의 제품이 아닌 통합 보안 제품을 제공하고 있습니다.
- 상호 연동
  - 시스코는 보안 장비간 상호 연동으로 보안 위협에 대해 가장 효율적으로 대처하고 있습니다.
- 통합 관리
  - 시스코는 보안 제품을 보다 효율적으로 통합 관리할 수 있는 솔루션을 제공하고 있습니다.
- **End-to-End**
  - 시스코는 네트워크에서 어플리케이션까지 망라하는 보안 솔루션을 제공하고 있습니다.