Cisco Security Solution Overview

최 우 형

Cisco Systems Korea

목 차

- Cisco Security Vision
- End Point Security
- Network Infra Security
- Intelligent Security
- 통합 네트워크 보안
- Application Security
- Case Study

“ Cisco Security Vision “

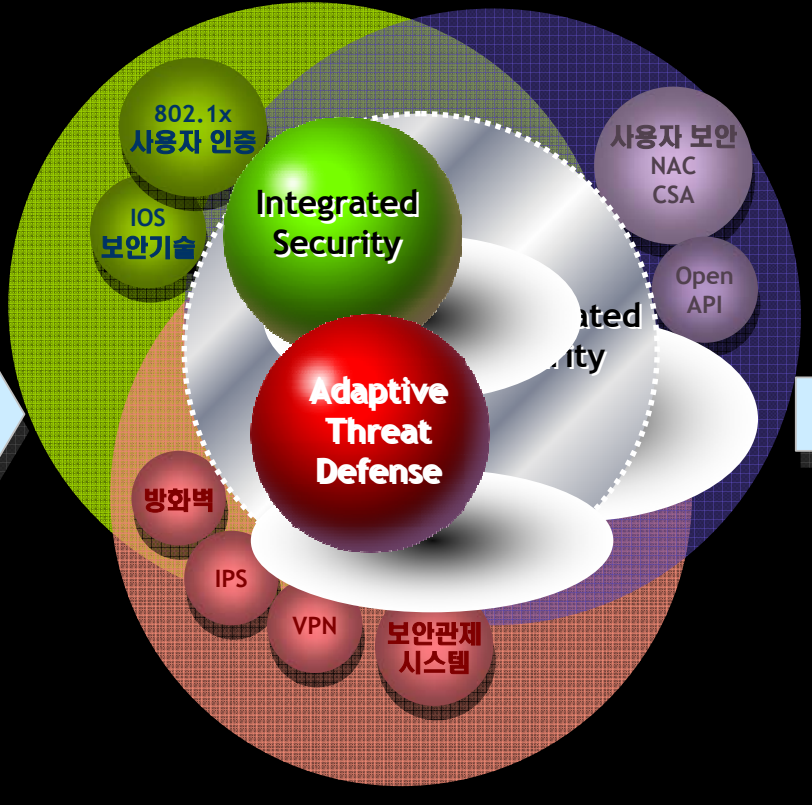
지금 겪고 있는 보안 문제 어떻게 해결하세요?

지금 겪고 있는 보안 문제 어떻게 해결하고 계십니까?

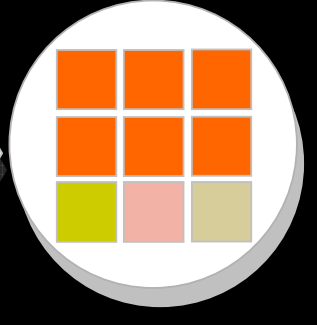
Cisco 보안 전략과 수행 방법

- 사용자 Patch 문제
- Zero Day Attack
- 사용자 인증 문제
- 네트워크 보안

Security Issue



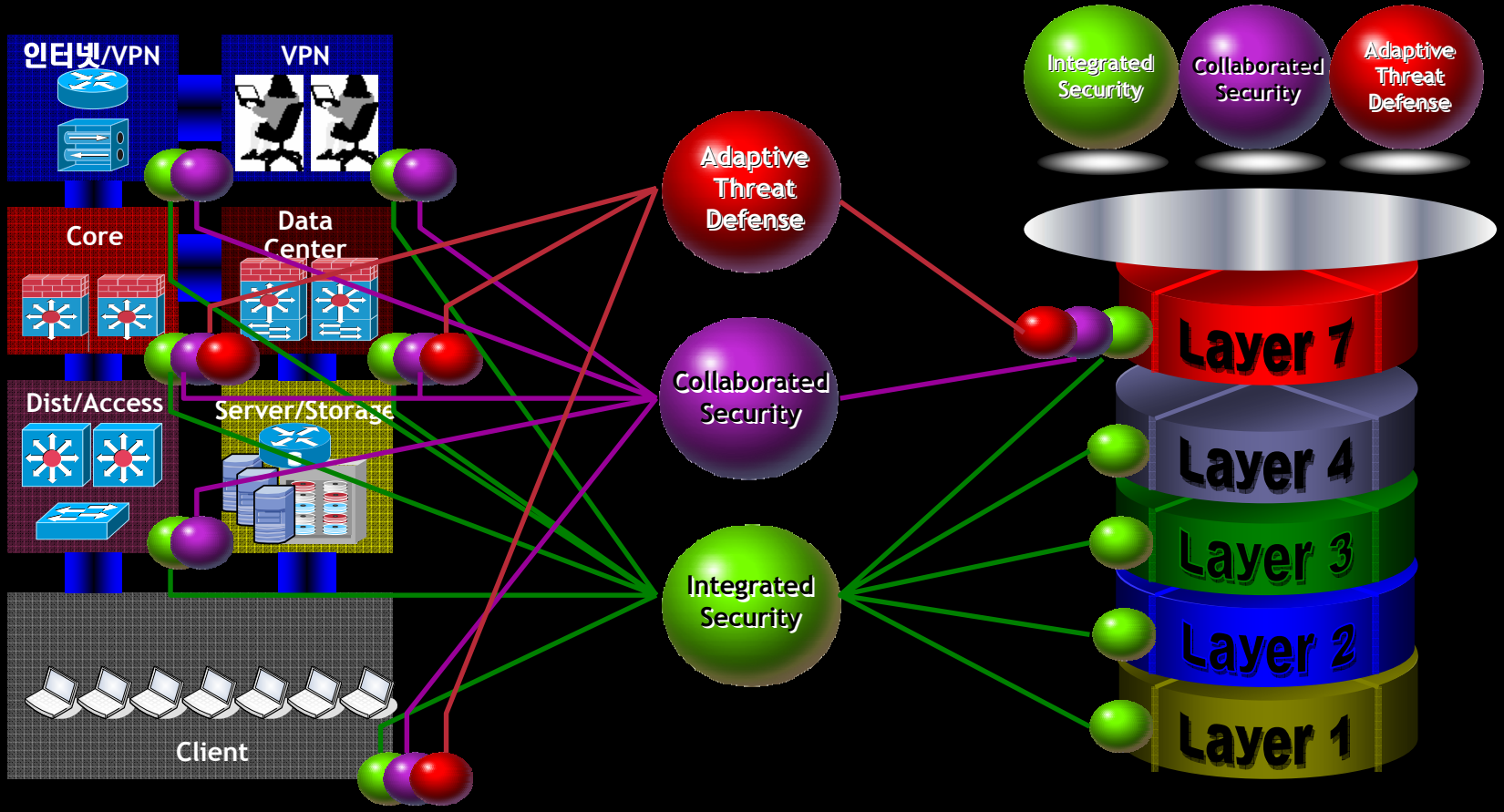
체계화된 보안 전략 수립



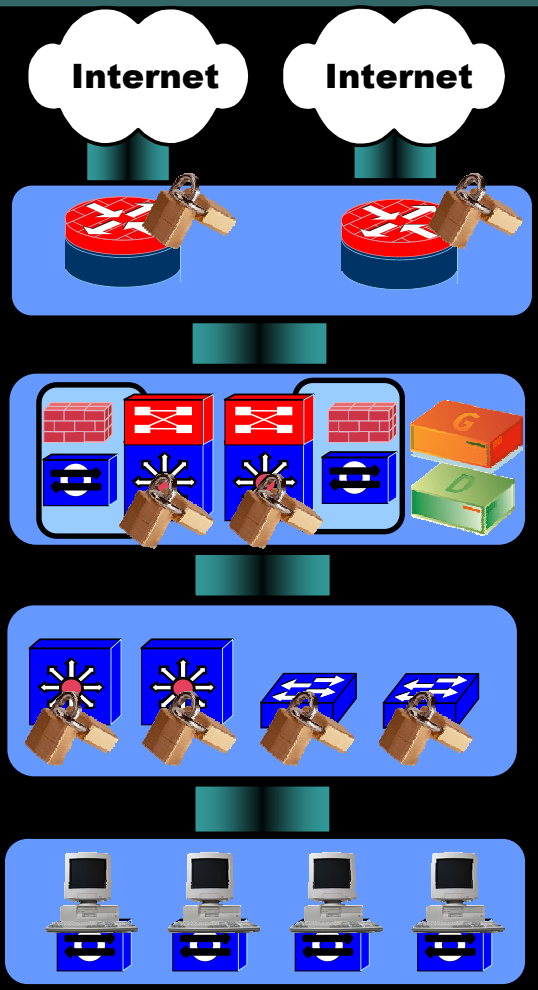
- 방화벽
- IPS
- VPN
- 보안관제
- App 보안

Cisco Security Vision

Cisco의 Security Depoly 전략 – 모든 영역에서 모든 레이어까지



Cisco Security Blueprints
– SDN (Self Defending Network) Evolution



SDN Phase III "Adaptive Threat Defense"

- 네트워크,어플리케이션 보호, 네트워크 전방위 위협 견제
- 좀 더 능동적 보안 기술 제공…
- 통합 보안 관리 운영을 통한 보안 기술 운영의 효율성 제공
- Deep Inspection 기반의 보안 구현

3

적응형 위협방어

SDN Phase II "Collaborative Security Systems"

- 상호 협력 기반의 보안 기술 제공
- End to End의 보안 청사진
- NAC, IBNS, SWAN

2

상호협력 보안기술

SDN Phase I "Integrated Security"

- 모든 네트워크 장비에 보안 기능을 탑재…
- 안전한 접속, 내/외부 위협으로 부터의 보호, 신뢰성 & 인증
- 네트워크 기반의 보호 기술

1

네트워크 장비기반 보안

Cisco Security Blueprints
- Solution Evolution

Converged Security
Cisco ASA 5500
New!

ASA 7.0: "All-in-One" 통합 네트워크 보안 장비

Firewall
Cisco PIX
New!

PIX 7.0: Application 기반 보안, Active/Active

Intrusion Prevention
Cisco IPS
New!

IPS 5.1: In-Line IPS, RR 기능을 통한 지능형 방어

Remote Access VPN
Cisco VPN 3000
New!

4.7: IPSec VPN, SSL VPN 동시 지원

Endpoint Security
Cisco Security Agent
New!

CSA 4.5: 알려지지 않은 공격 방어, 한글화 지원

Router Security
Cisco ISR Family
New!

ISR: 800, 1800, 2800, 3800

Switch Security
Catalyst Engines
New!

Cat6k: FWSM,IPSM,NAM,Web VPN,VPNSM,DDoS Guard

Application Security
AVS, ACE
New!

AVS: Application 방화벽

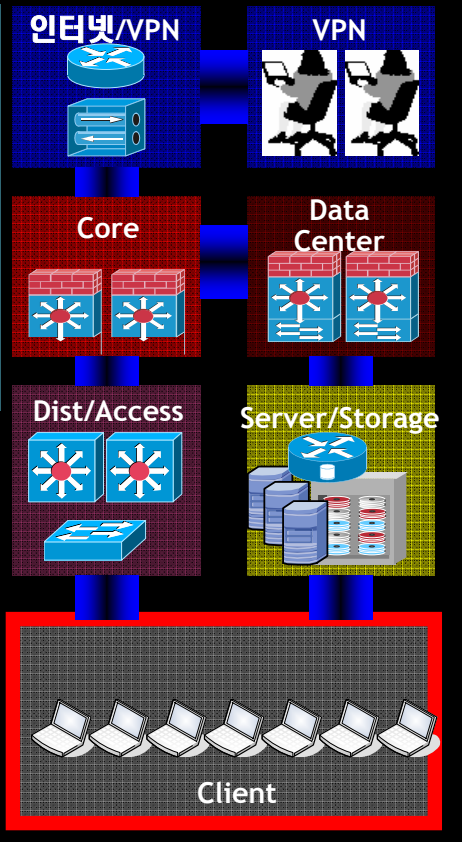
Security Management
Cisco VMS/MARS
New!

Management: CS-MARS를 통한 보안관제 구축

Security Systems
NAC/Clean Access
New!

NAC: NAC 기반의 End Point Security

End Point Security

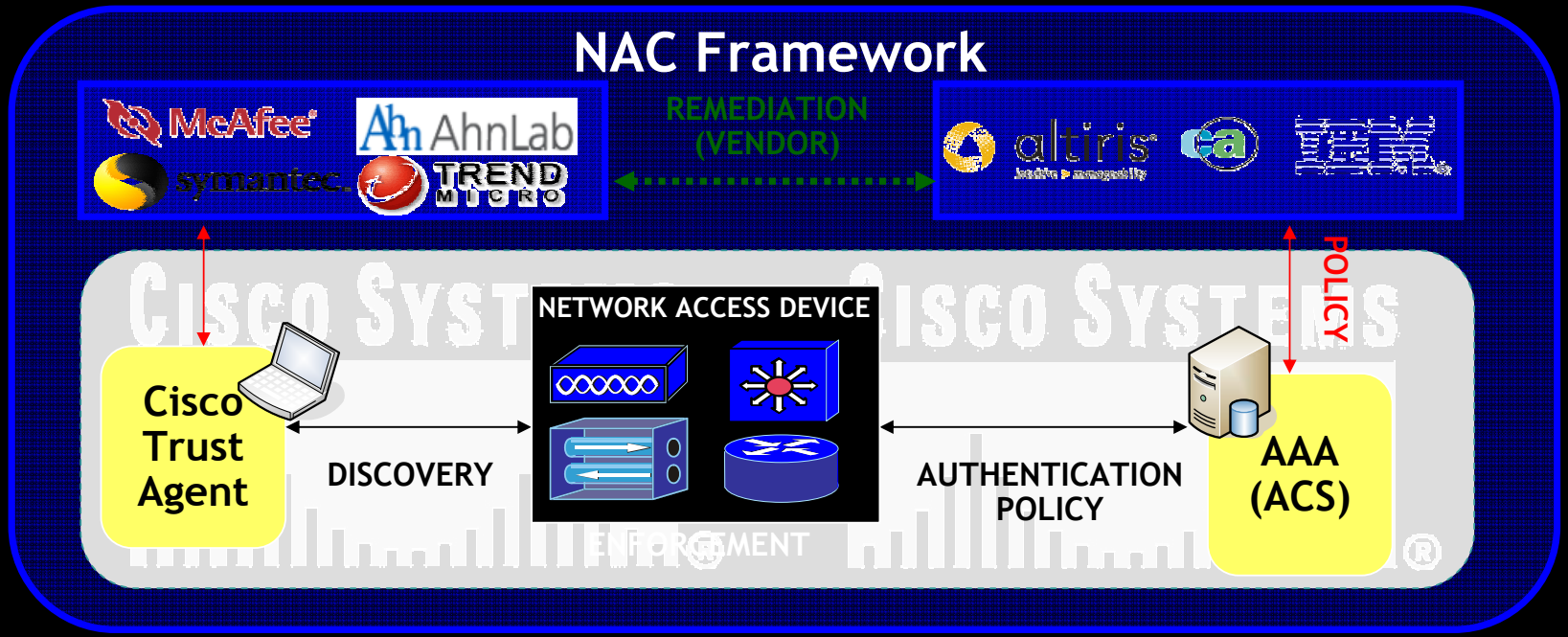


End Point Security
Cisco NAC을 통한 보안 건강성 유지

Collaborated Security

NAC(Network Admission Control)
- 모든 네트워크 자원의 인증과 보안 건강 상태를 점검하고 접근을 제어하는 기술

네트워크 접속 전 사용자 보안 상태 점검	사용자의 백신 패치 및 사용자 건강성 점검

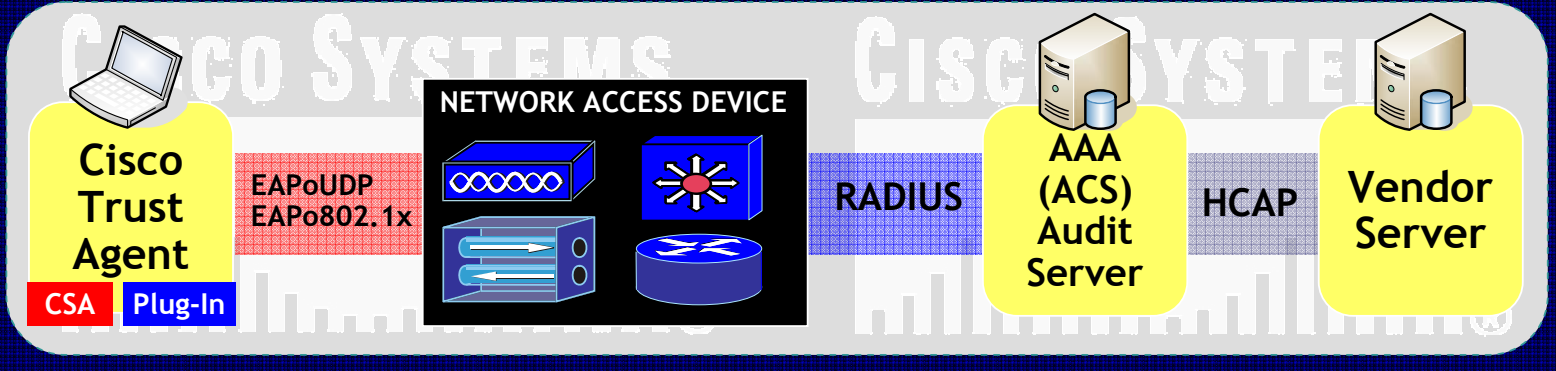


End Point Security
"Cisco NAC" 요소들의 논리적인 역할

Collaborated Security

Cisco NAC Logical Roles

NAC Framework



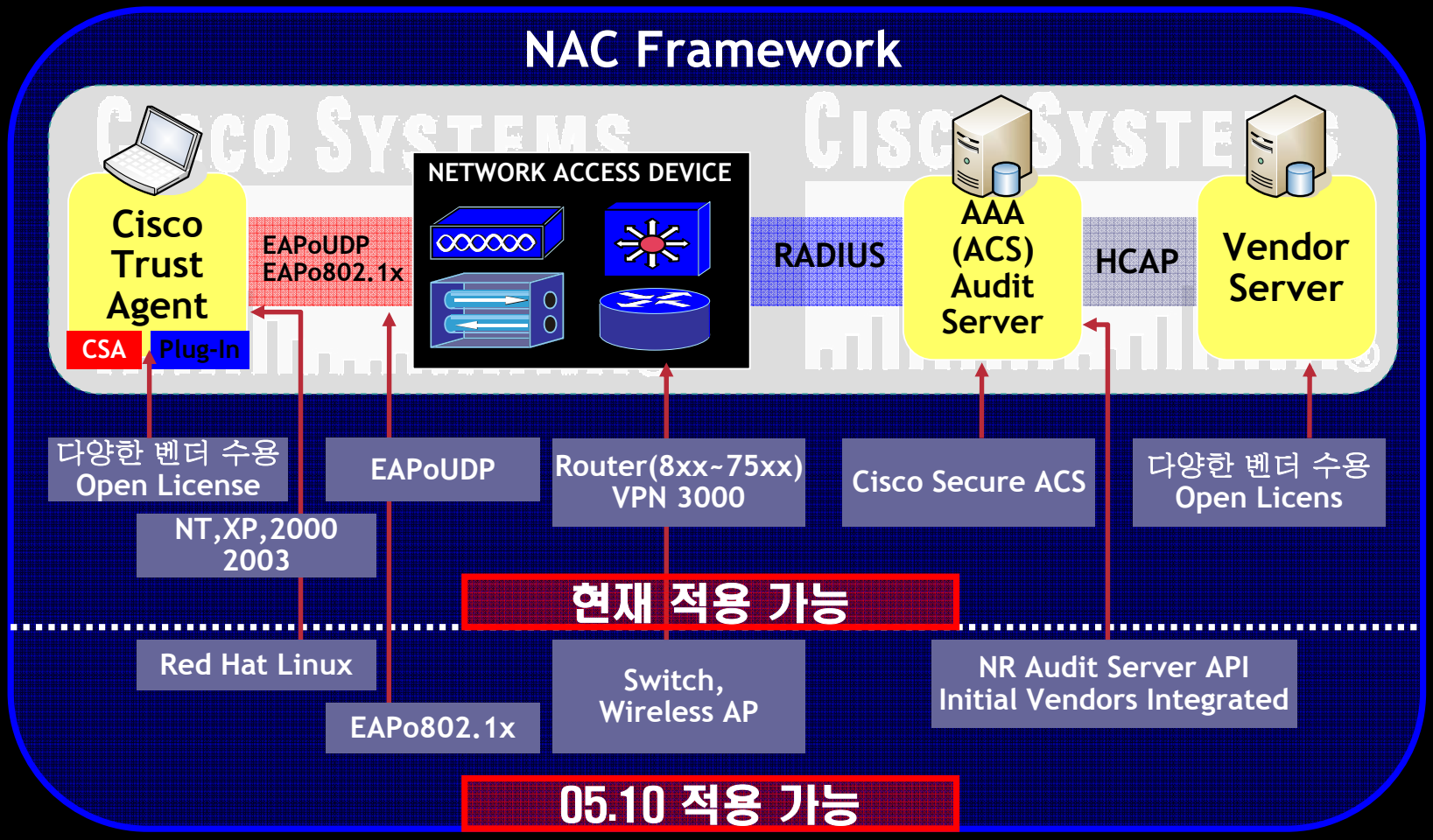
사용자
- 기본 인증에 대한 역할
- 관리 대상의 구분
- 보안 건강성 점검 대상

보안 정책 집행자
- 정책 위반에 대한 제어 구성

보안 정책 결정자
- AAA 기능 수행
- 교정 치료 서비스
- Agentless 시스템에 대한 감사

End Point Security
"Cisco NAC" Logical Components

Collaborated Security



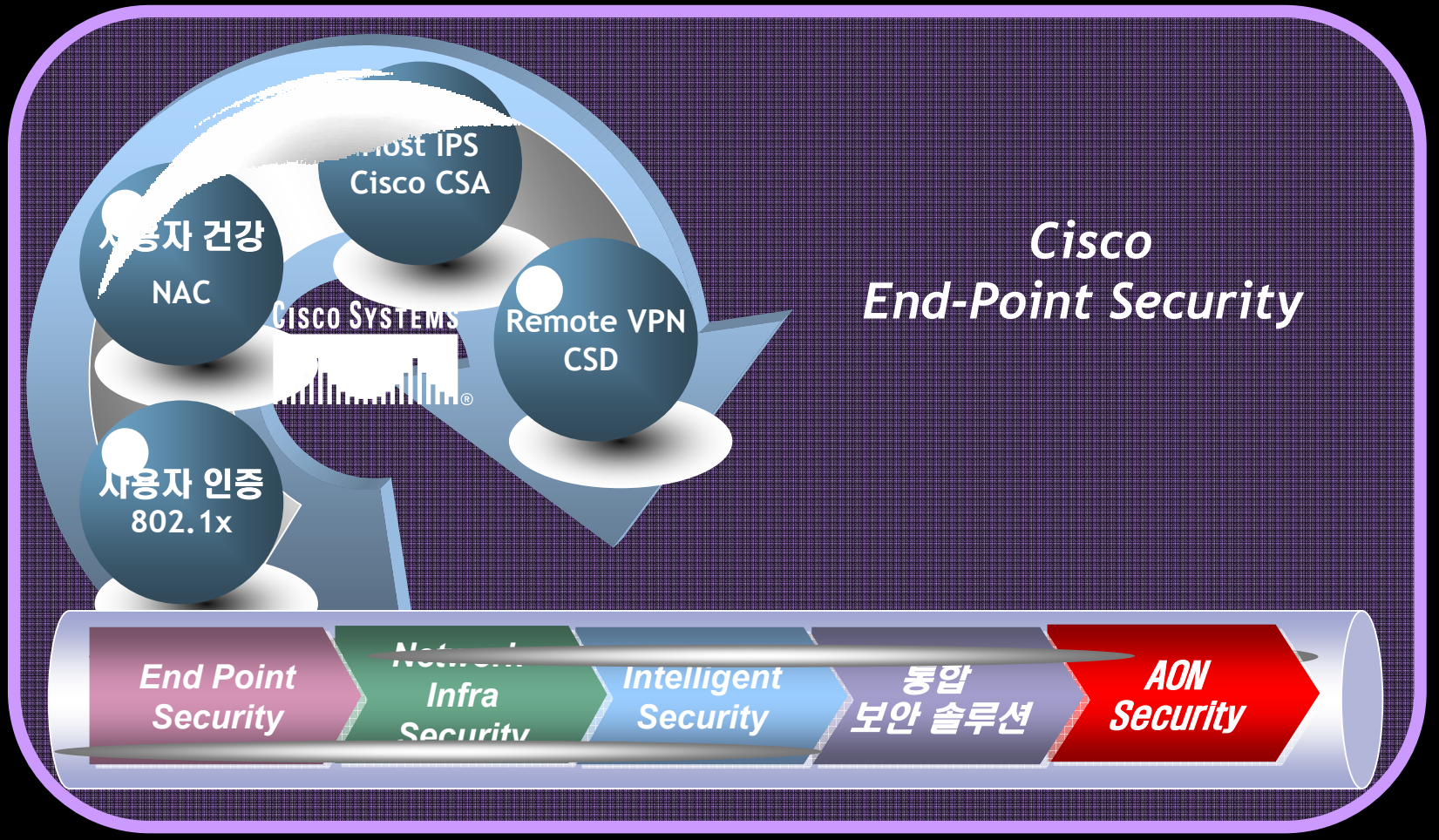
End Point Security
인프라 환경에 맞게 지금 바로 적용이 가능 !!!

Collaborated Security

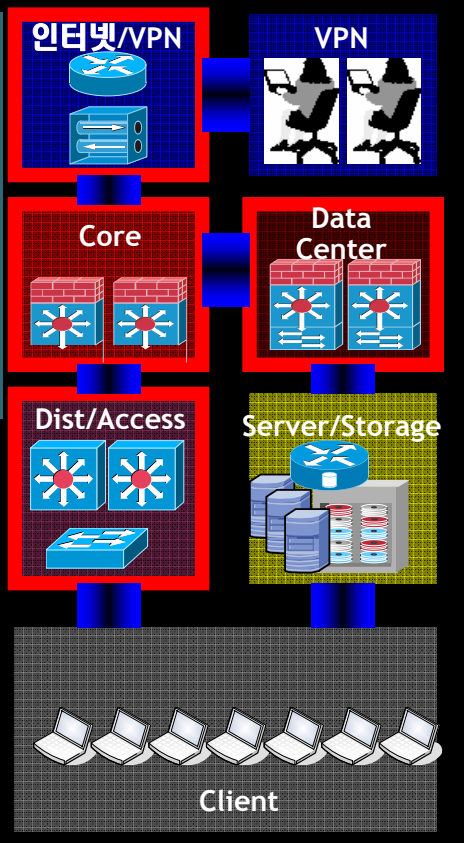
L2 ~L3 환경, 802.1x 환경 등 조합을 통한 적용 가능

Feature	NAC-L2-802.1x	NAC-L2-IP	NAC-L3-IP
Trigger mechanism	Data Link Up	DHCP or ARP	Forwarded Packet
Machine Identity	●		
User 인증 요구	●		
Posture	●	●	●
VLAN 할당	●		
URL-Redirection		●	●
Downloadable ACLs	6500-only (Port 기반 ACL)	●	●
Posture 상태 질의		●	●
802.1x Posture Change	●		

Network Infra Security
Cisco의 End-Point Security



Network Infra Security



Network Infra Security
Router 기반의 보안 구성

Integrated Security

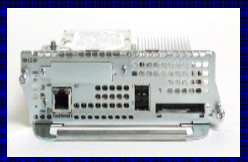
Adaptive Threat Defense

Router CPU 보호 기술 - CPP
공격 발생시 라우터 CPU를 보호, CPU 과부하를 방지 하는 기술 제공

Router 통합 내장형 IPS Module
- Router 기반 자동 Blocking



자사 병원 네트워크(인터넷,WAN) 현황 분석
- 인터넷,외부 전용선 사용량 현황 정밀 분석 기능



고성능 인터넷 라우터 구성 - Cisco 7600 Router

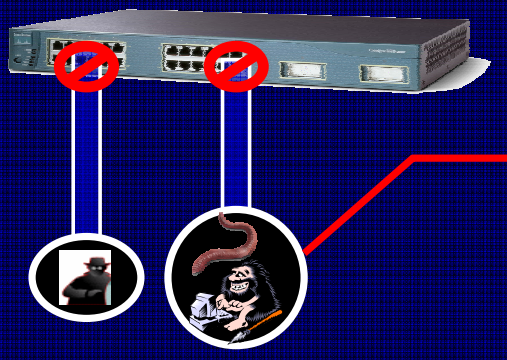
통합 보안 Router - Cisco ISR Series

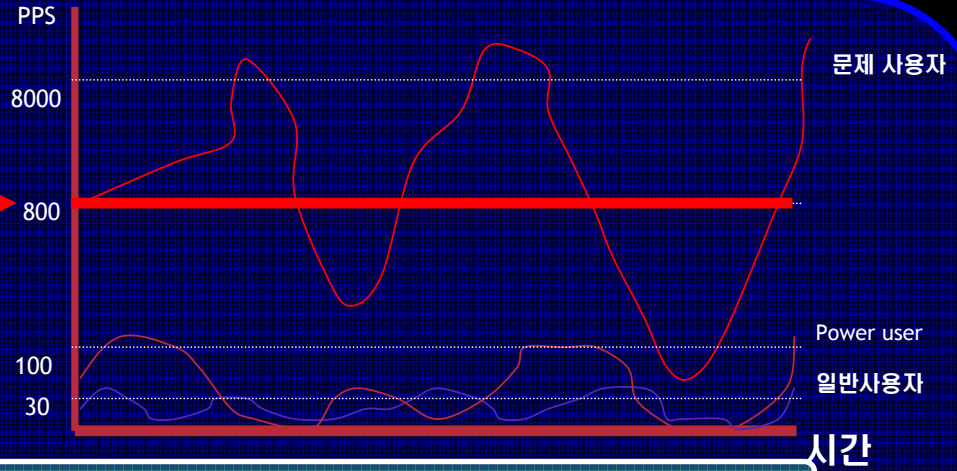
Cisco IOS 기반 Firewall / IPS 구현

Network Infra Security
Access-Switch 기반의 보안 전략 강화

Integrated Security

Access Switch의 Semi-IPS 기능 활성화





❖ *Semi IPS Switch 탄생 - Storm Control PPS Limit 기능 !!!*

Storm Control PPS 기능 Enable

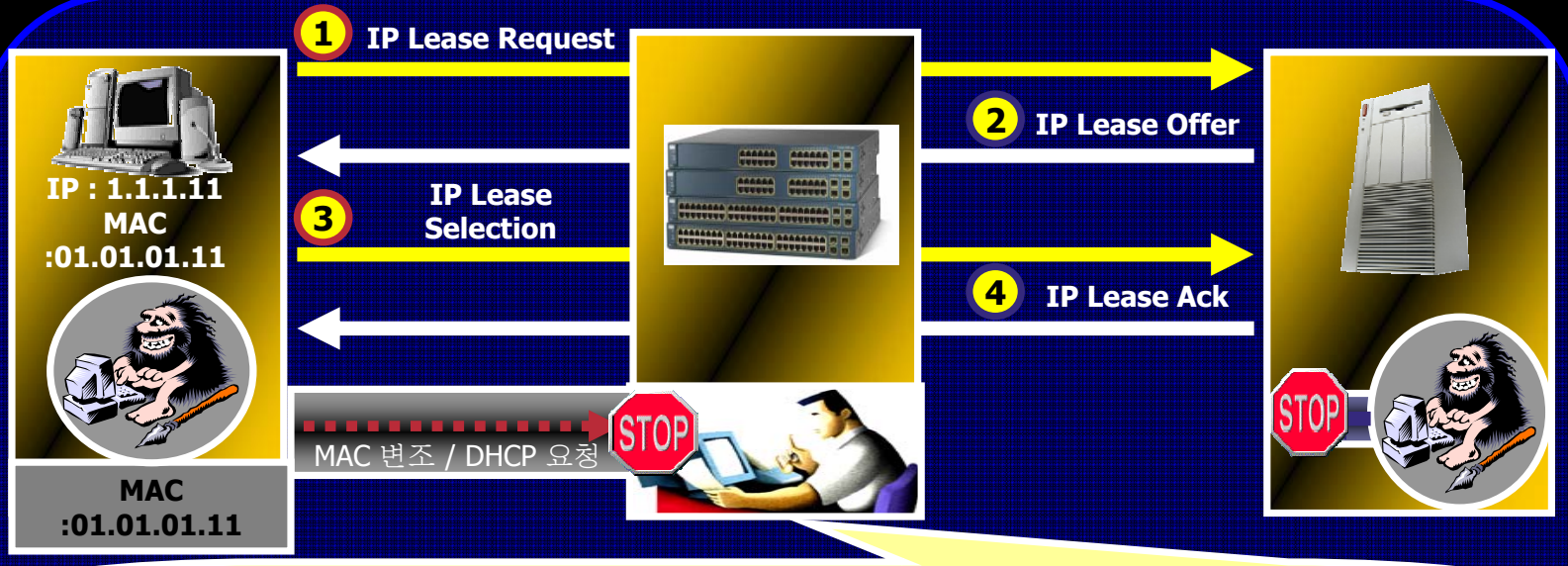
Action : 800 PPS 이상 일 경우

- *SNMP Trap Log*
- *Blocking* → *자동 Forwarding*
- *Shutdown* → *수동 Enable*

Network Infra Security
동적 IP 환경에서의 강력한 보안 구현

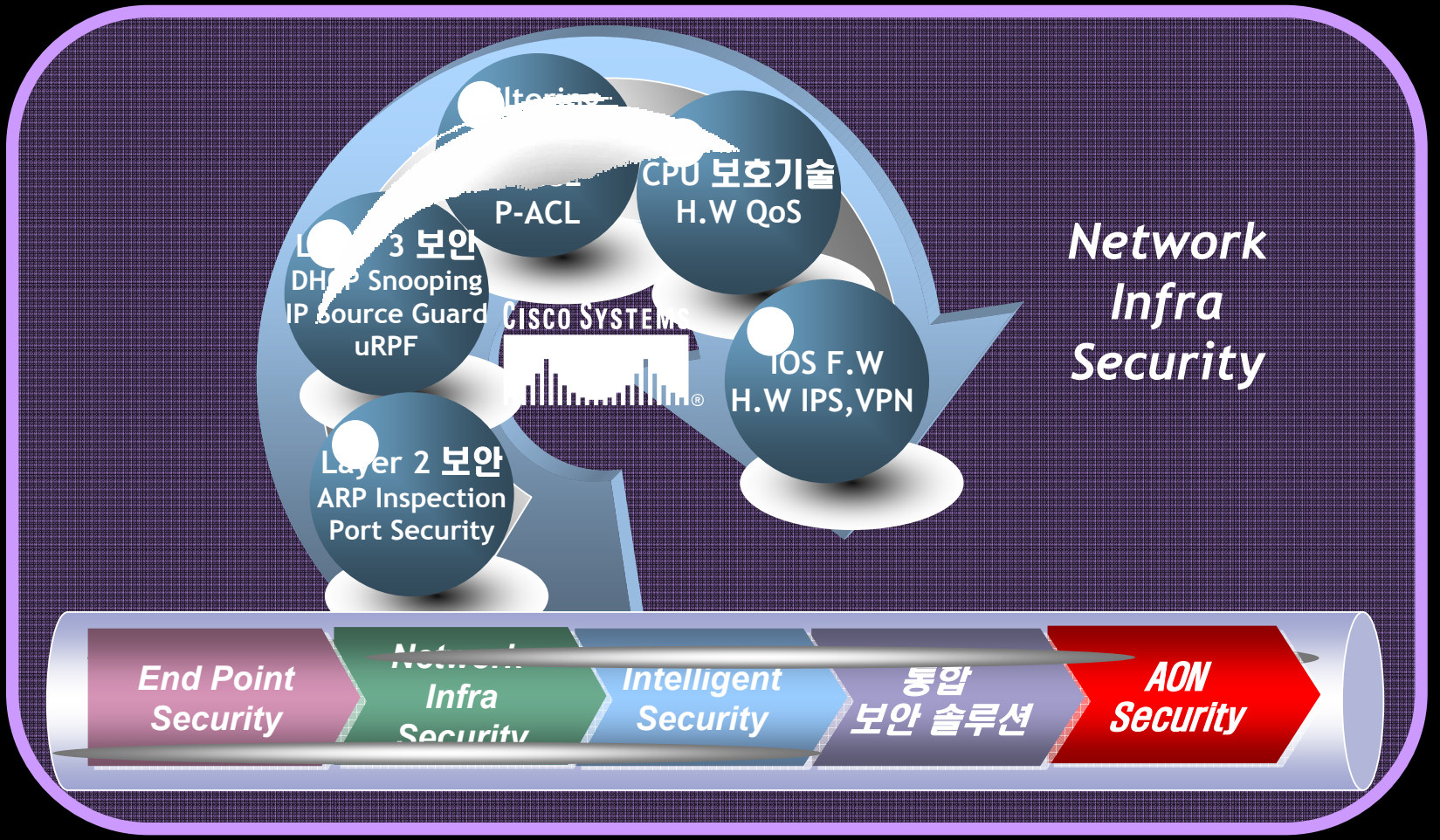
Integrated Security

DHCP 기반의 강력한 보안 기능 구현

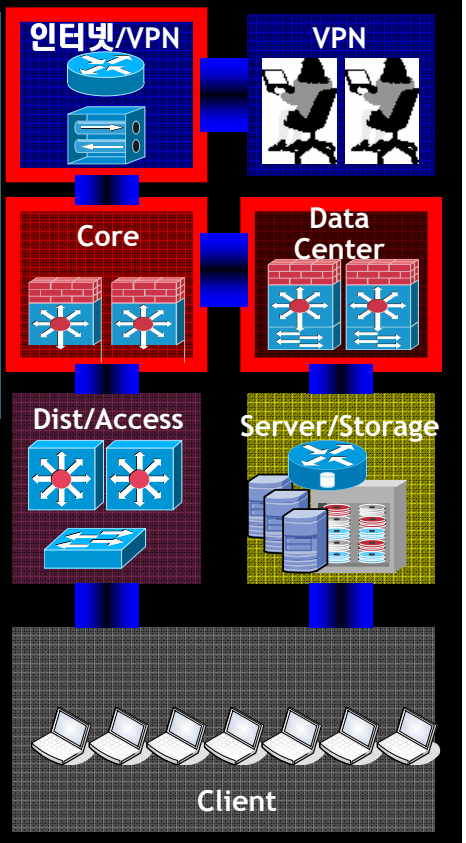


1. DHCP Snooping 기능 - 잘못된 DHCP 서버로 인해 네트워크가 이상동작 방지
2. DHCP 환경 기반의 IP 제어 - IP 변조 방지 및 Static IP 설정 Host 사용 금지 기능
3. DHCP 환경 기반 Man in the Middle Attack 방어 기능 - ID,PWD 도용 기능 방지

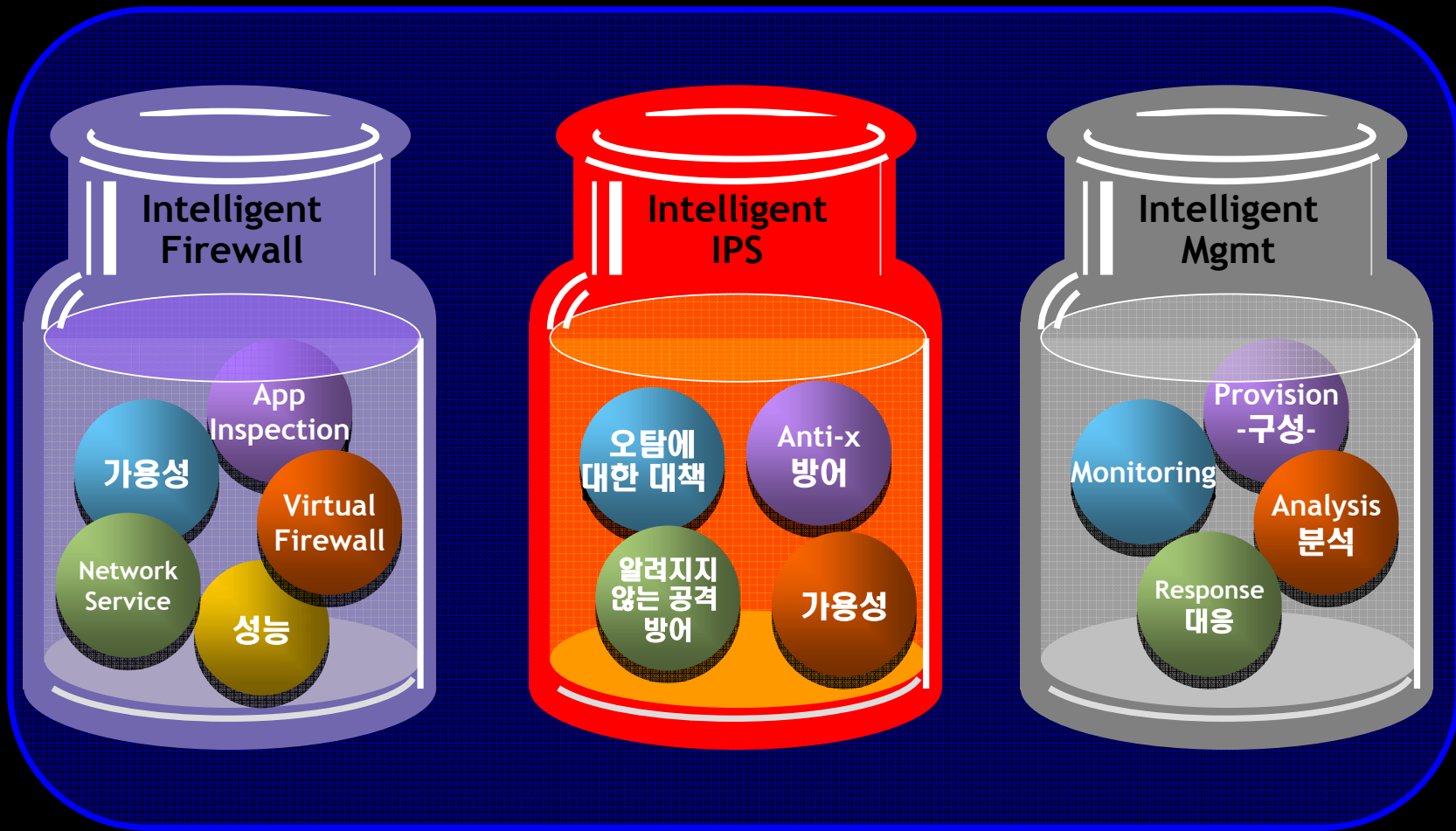
Network Infra Security
Cisco의 Network Infra Security



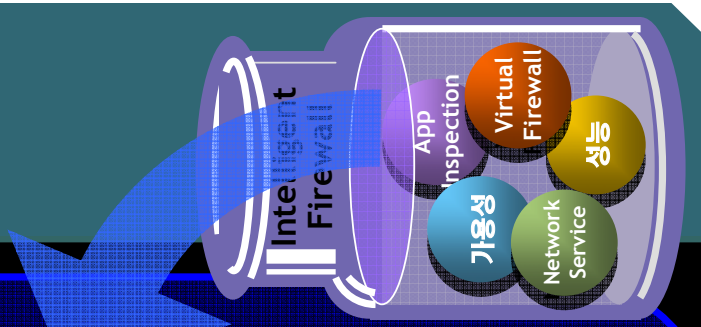
Intelligent Security



Intelligent Security

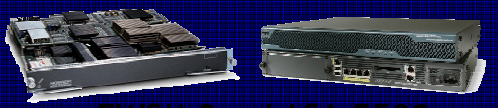


Intelligent Security
Cisco 지능형 방화벽

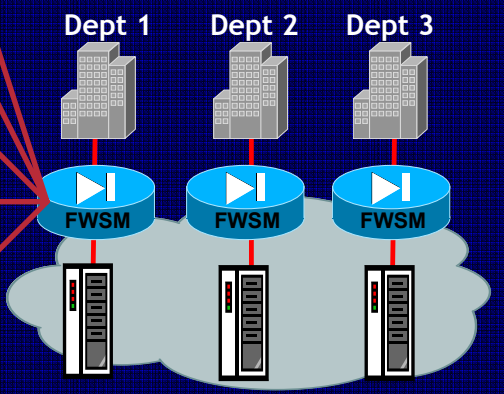


	Cisco Firewall 기술
Application Inspection	• Inspection Engine 수행 능력의 증가 • Web Traffic Inspection Service
가용성	•Active / Active Stateful Failover 구현
Virtual F.W	•논리적인 방화벽 구성 - 보안 정책의 유연성 •VRF-Aware 를 통한 MPLS 지원
Network Service	• 가용성 극대화를 위한 OSPF 지원 • QoS 지원 - Policing , LLQ
성능	• Service Module Type의 5.5Gbps 지원

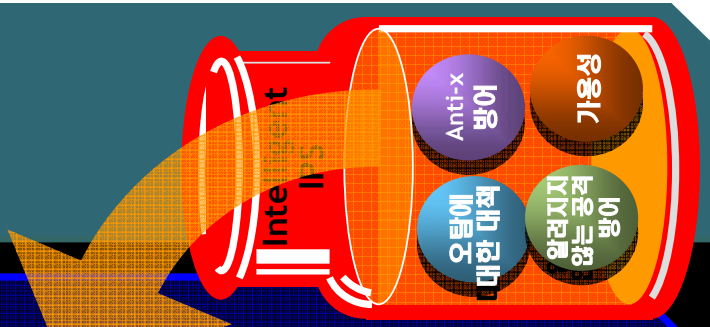
Cisco F.W Product



FWSM 3.x / ASA 5500



Intelligent Security
Cisco 지능형 IPS



Anti-X Defense

오탐에 대한 대책

가용성

알려지지 않은 공격 방어

Cisco IPS 기술

- Spyware/Adware,Virus,Worm, App Abuse
- Deny Attacker 방어 - 정교한 방어 기법 New!

- Risk Rating을 통한 정밀 방어 시스템 구축

- In-line Vlan 지원 New!
- S.W Bypass 기능 구현 - 엔진 장애 시 우회

- Host IPS 구현을 통한 Unknown Attack 방어
- Guard Solution을 통한 DDoS 방어 구현
- Rate Limit 기능 지원 - Flood Attack 방어 New!

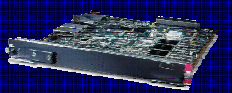
Cisco IPS Product

	Traditional IPS	Cisco IPS 5.1
Manually Investigate	Manually Investigate	Manually Investigate
Automated Mitigation	Automated Mitigation	Automated Mitigation

Cisco ISR
IOS IPS, IPSM

Cisco IPS
4200

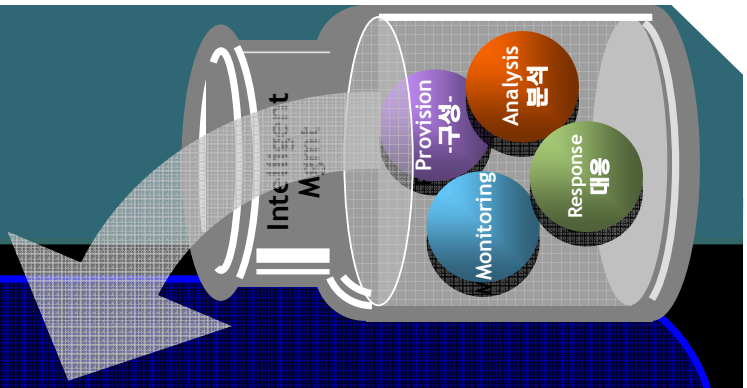
Cisco IPSM II



Cisco
DDoS Guard

Host IPS
CSA 4.5

Intelligent Security
Cisco Management Solution



	Cisco Mgmt 기술	
Provisioning	• Integrated Device Manger – ASDM,PDM… • 빠른 Setup 과 config 변경	Integrated Device Managers
Monitoring	• Router,Switch,Appliances,endpoint 구성을 위한 솔루션	CSM
Response	•Security Mitigation & Monitoring Solution •Attack 경로 보고 / 강제 억제 가능	CS-MARS / CICS
Analysis	• NSA ,CIS, SAFE 기반 보안 config 관련 Predefine	Cisco Security Auditor

Intelligent Security
지능형 보안 관제 시스템 구축 - CICS를 통한 사전 방어 시스템

유해트래픽 사전 방어 시스템 제공 !!!

Outbreak & threat 정보 제공
- 위협 등급
- 상세 정보 제공
- 위협 내용과 영향
- 권고 OPACL

정책 설정
- 수동 설정 또는 자동 Config Loading
- 장비별 또는 Group 별 제어
- OPACL 수정 또는 권고 사항 Push

Trend Micro LAB

OPACL

OPSig

Cisco Incident Control Server

OPACL

OPSig

Catalyst

Catalyst 6500 IPS Blade

ASA 5500 IPS Blade

IPS 4200 Series

Router

Router IPS in Software

PIX

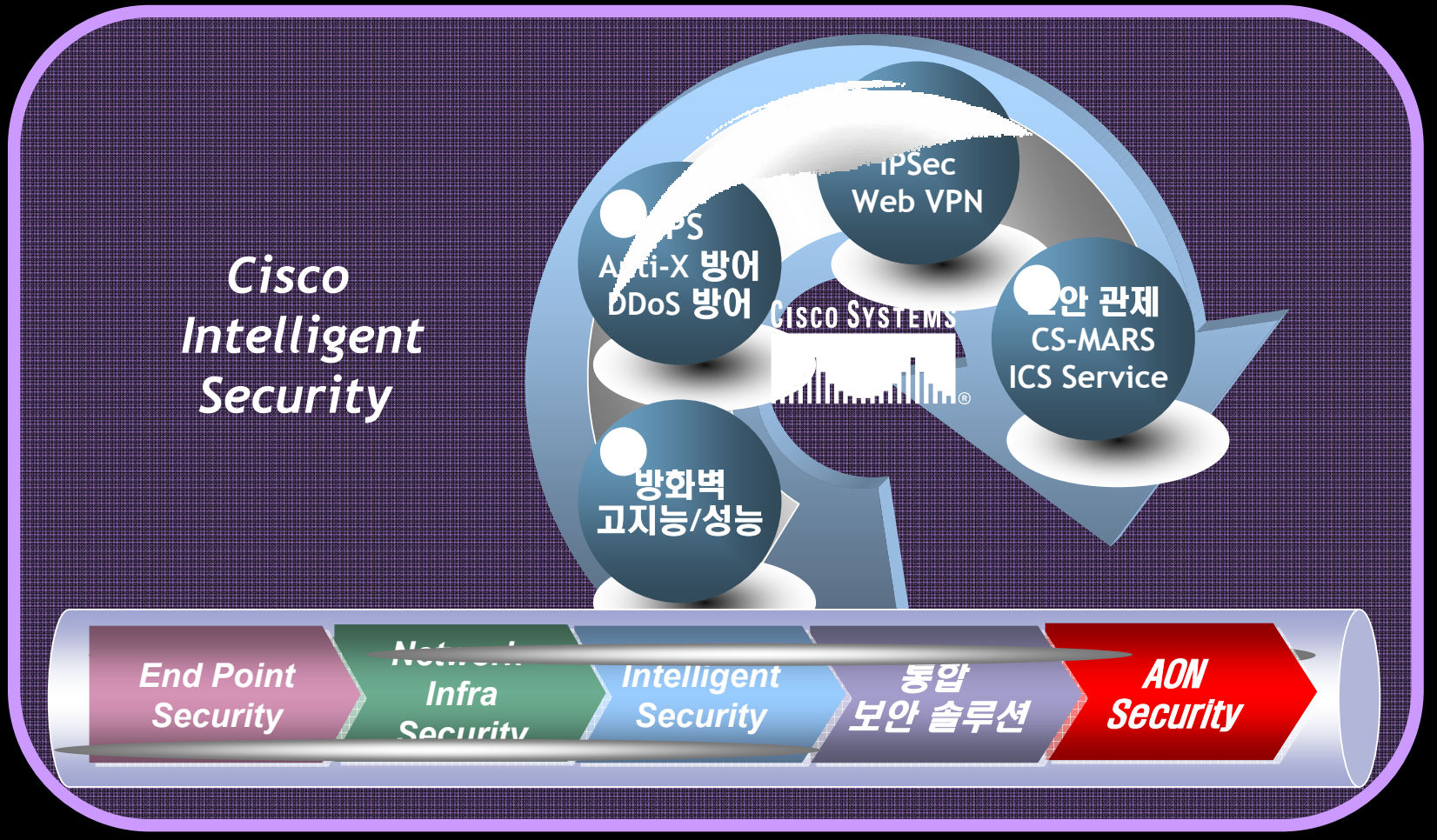
Malware Outbreak 발생 !!

t=0

최대 30분 이내 OPACL 전송

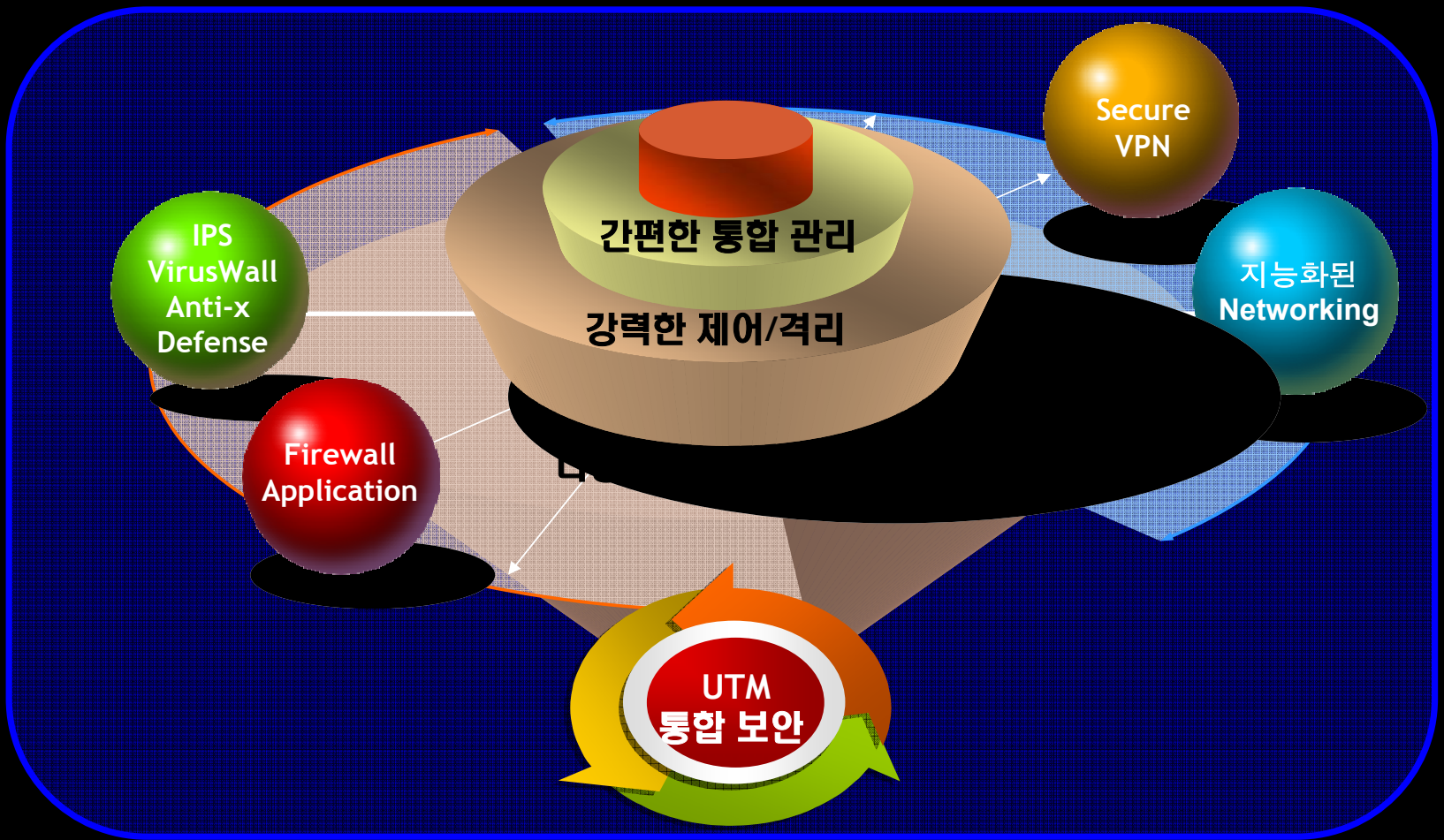
최대 120분 이내 OPSig 전송

Intelligent Security
Cisco의 Intelligent Security



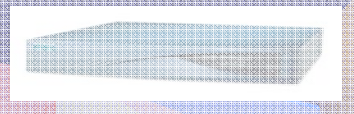
통합 보안

통합 네트워크 보안이란 ?
UTM (Unified Threat Management)

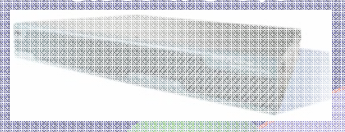


통합 네트워크 보안
Cisco UTM Solution - ASA 5500

Cisco VPN 4.7



Cisco IPS 5.0



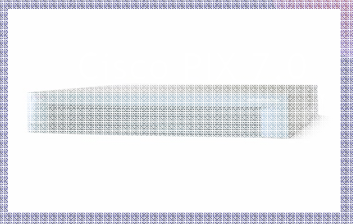
Secure
VPN

IPS
VirusWall
Anti-x
Defense

지능화된
Networking

Firewall
Application

Cisco PIX 7.0



The Cisco ASA 5500 Series

UTM
통합 보안

통합 네트워크 보안
Cisco UTM Solution - Cisco 통합 보안 스위치

통합 네트워크 보안 솔루션
Cisco ASA 5500과 통합 보안 스위치의 적절한 배치

Adaptive Threat Defense

대형 기업,공공,교육: 통합 네트워크 보안 장비

효과적인 비용 투자와 통합 보안 기능 구현:

- 통합 네트워크 보안 장비를 통한 관리 및 정책 구현
- 통합 OS를 통한 보안 정책 구현의 복잡도 감소 가능
- 간편한 운영 및 장애 처리
- 간편한 설치 가능
- IT 관련 관리자의 훈련 용이

중소규모 기업: 통합 네트워크 보안 장비

투자 대비 효과적인 보안 구현:

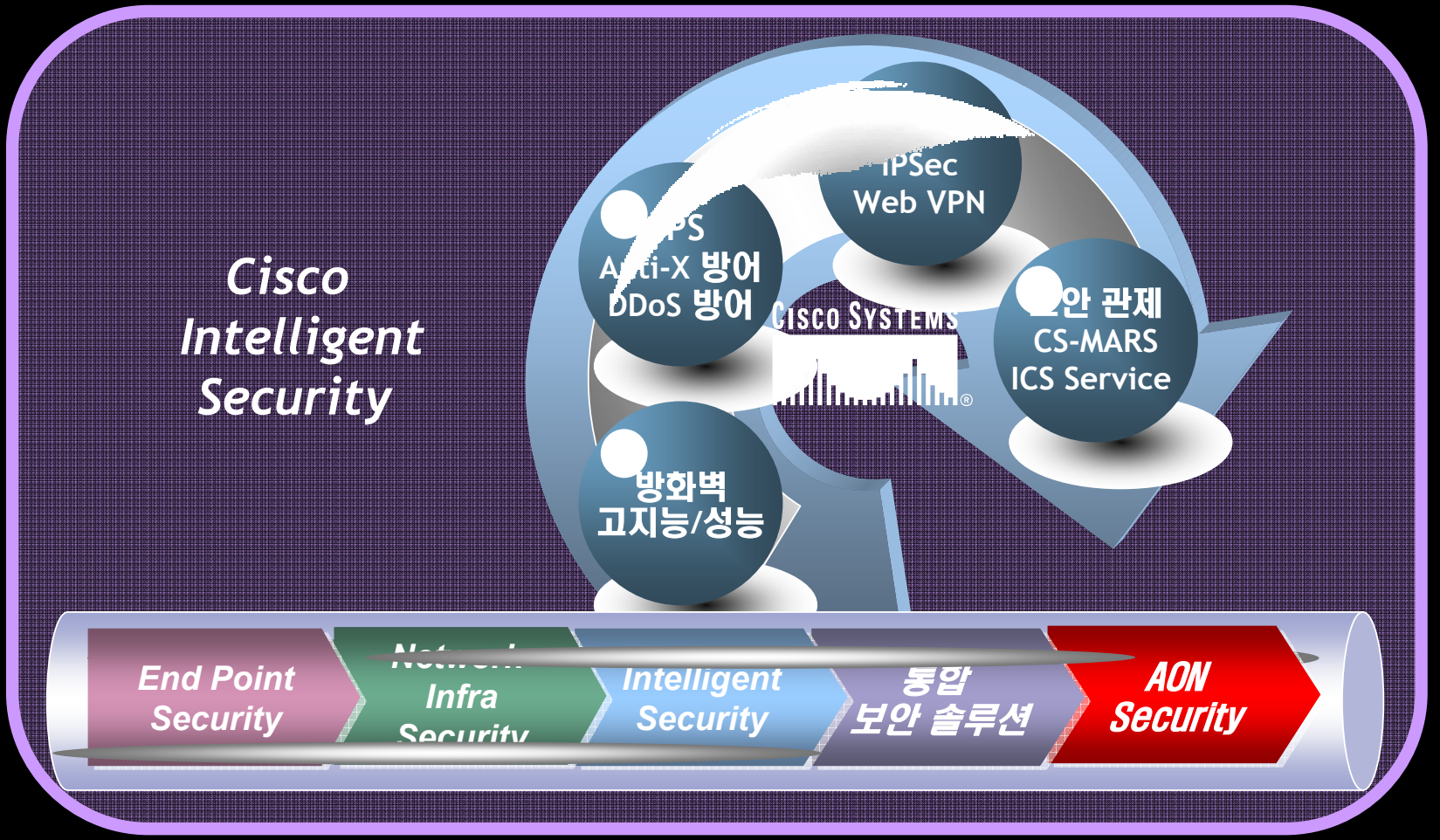
- 중소기업을 위한 효율적인 보안 정책 구현
- 관리의 복잡도 감소
- 성능 저하 없이 새로운 보안 정책 구현

Service Provider: 다양한 서비스

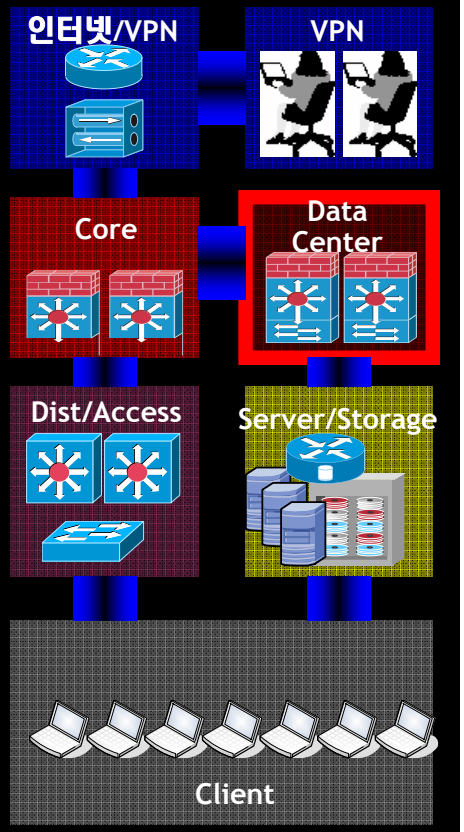
투자 대비 효과적 보안 구현:

- management, monitoring, provisioning 통합
- 새로운 장비 추가 없이 새로운 기능 구현 및 Provisioning
- 관리자의 훈련용이

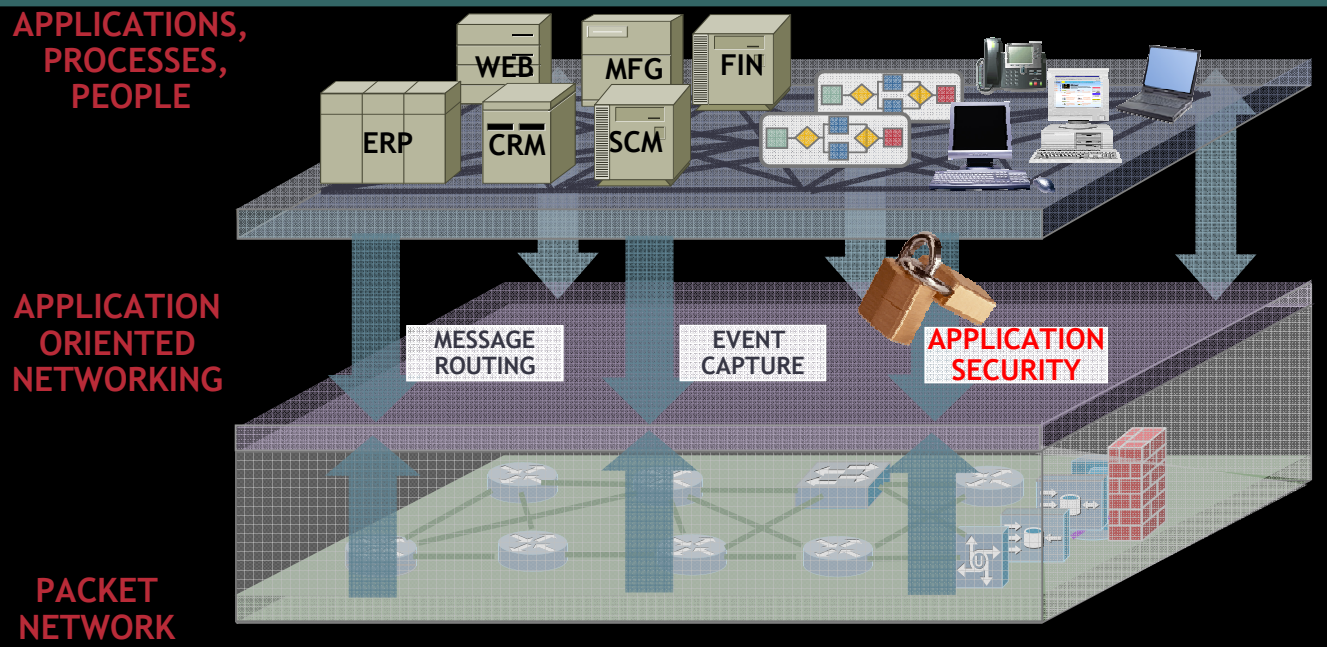
Intelligent Security
Cisco의 Intelligent Security



Application Security



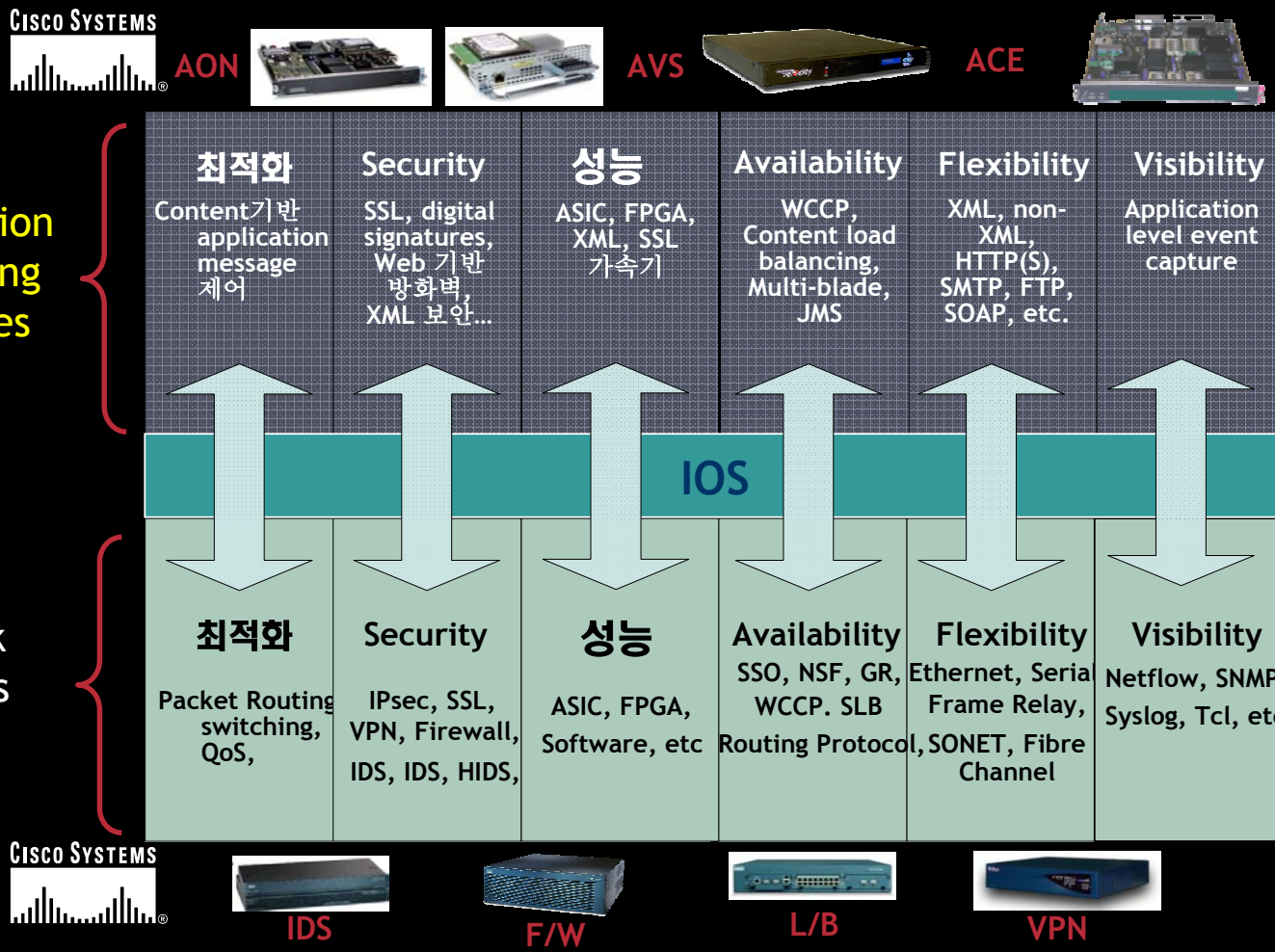
AON = 'Network for Applications'



Network의 차세대 진화 → Application Networking 진화

- Application message level 기반의 처리
- Application Message 의 Content, Context 의 이해 필요
- Infra의 큰 변화 없이 Application 처리 극대화

AON 기술의 확장
- Cisco's Intelligent Information Network

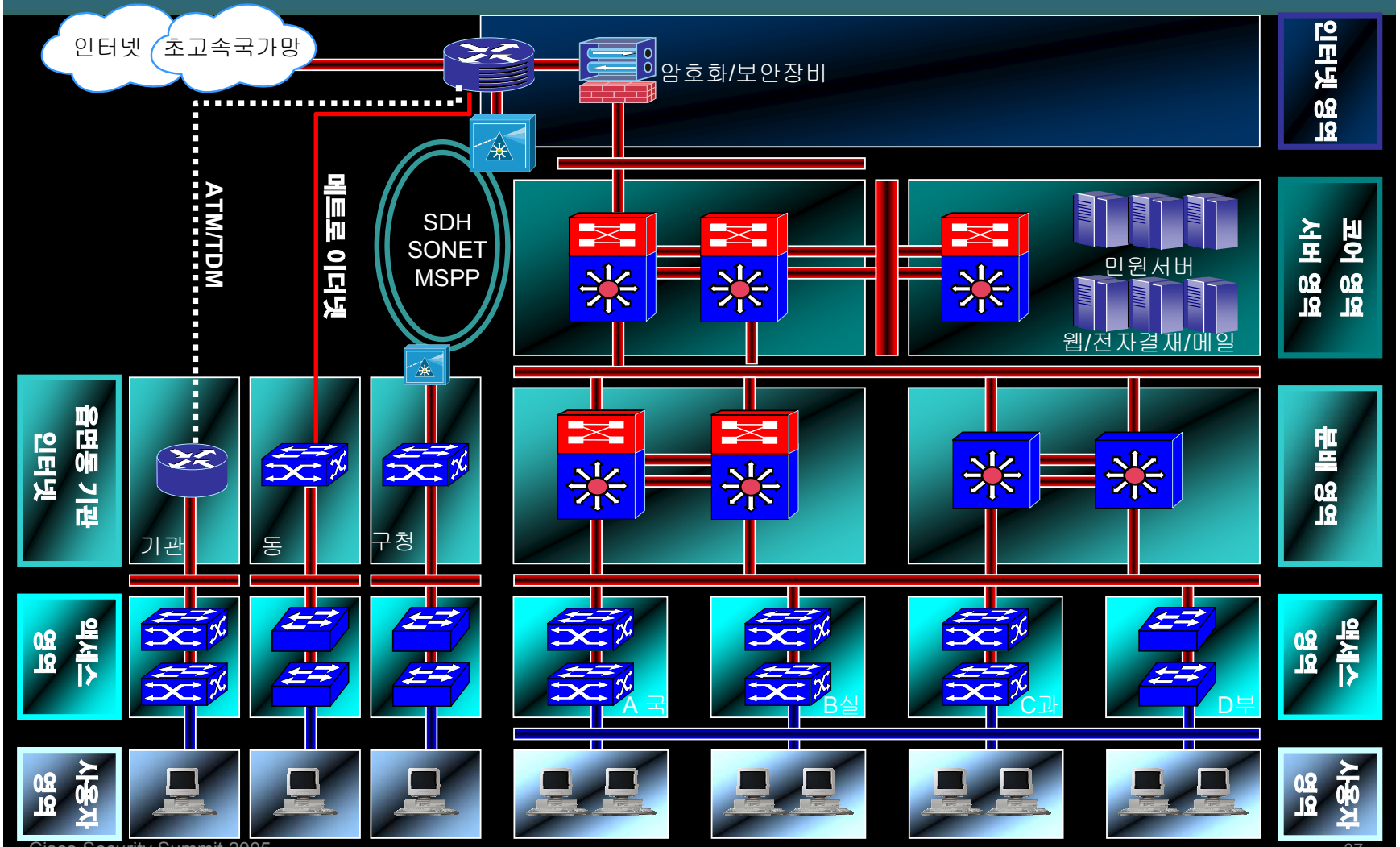


Application Security
Cisco의 Application Security

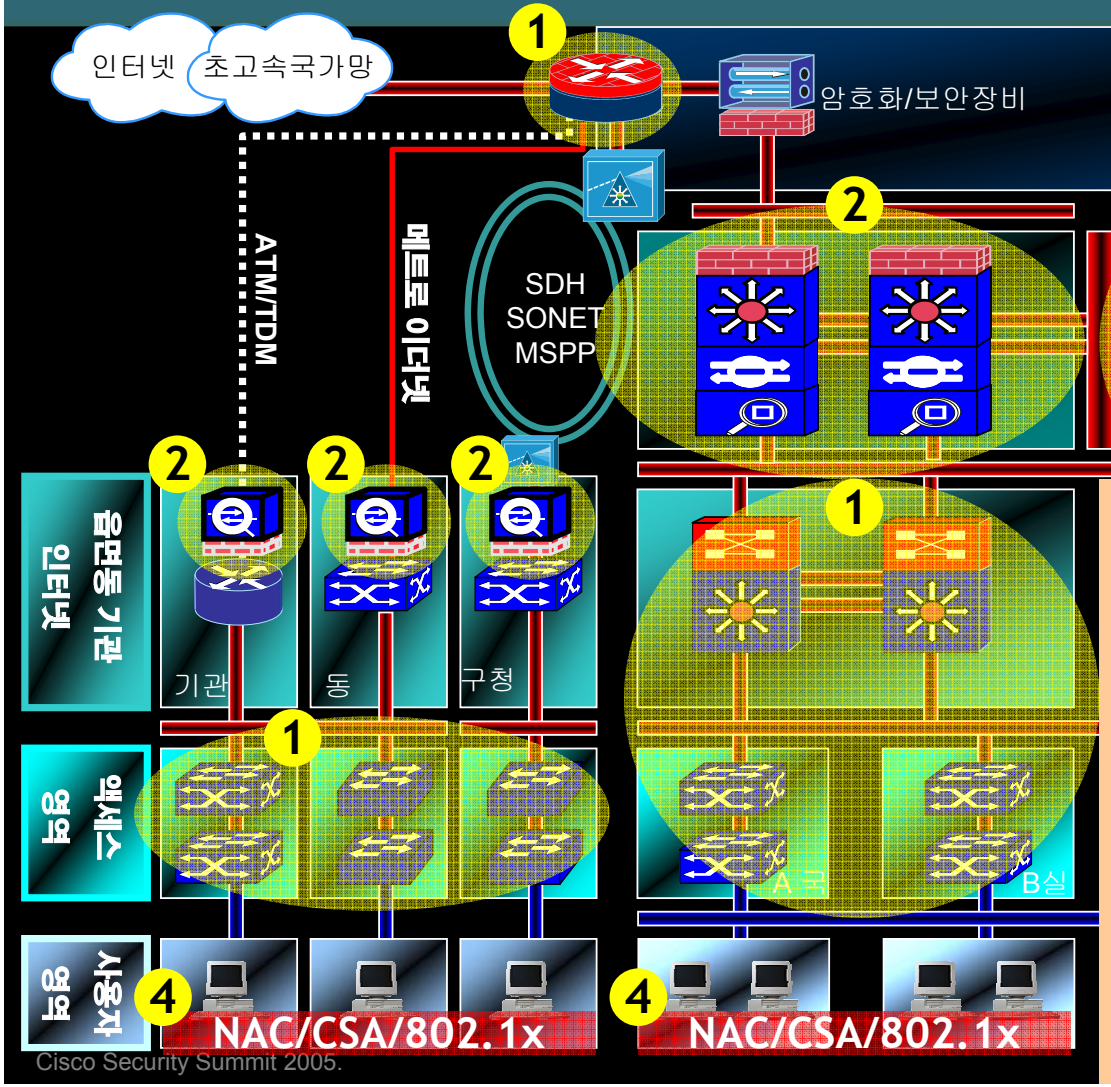
Cisco
AON Security 로의 진화

Cisco Security Design Case Study

전자정부 기관 네트워크 구성 예제

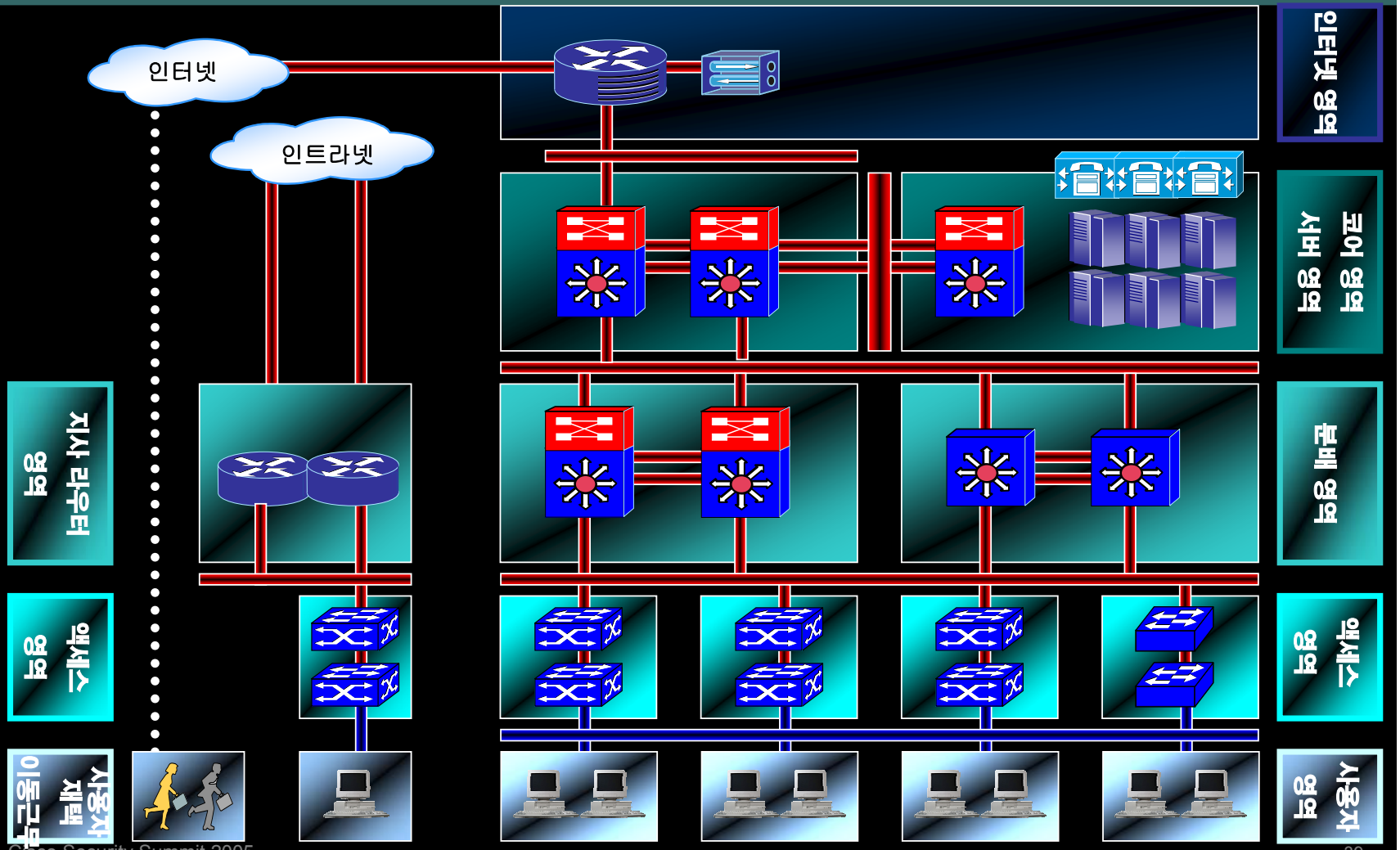


전자정부 기관 네트워크 보안 구성 예제

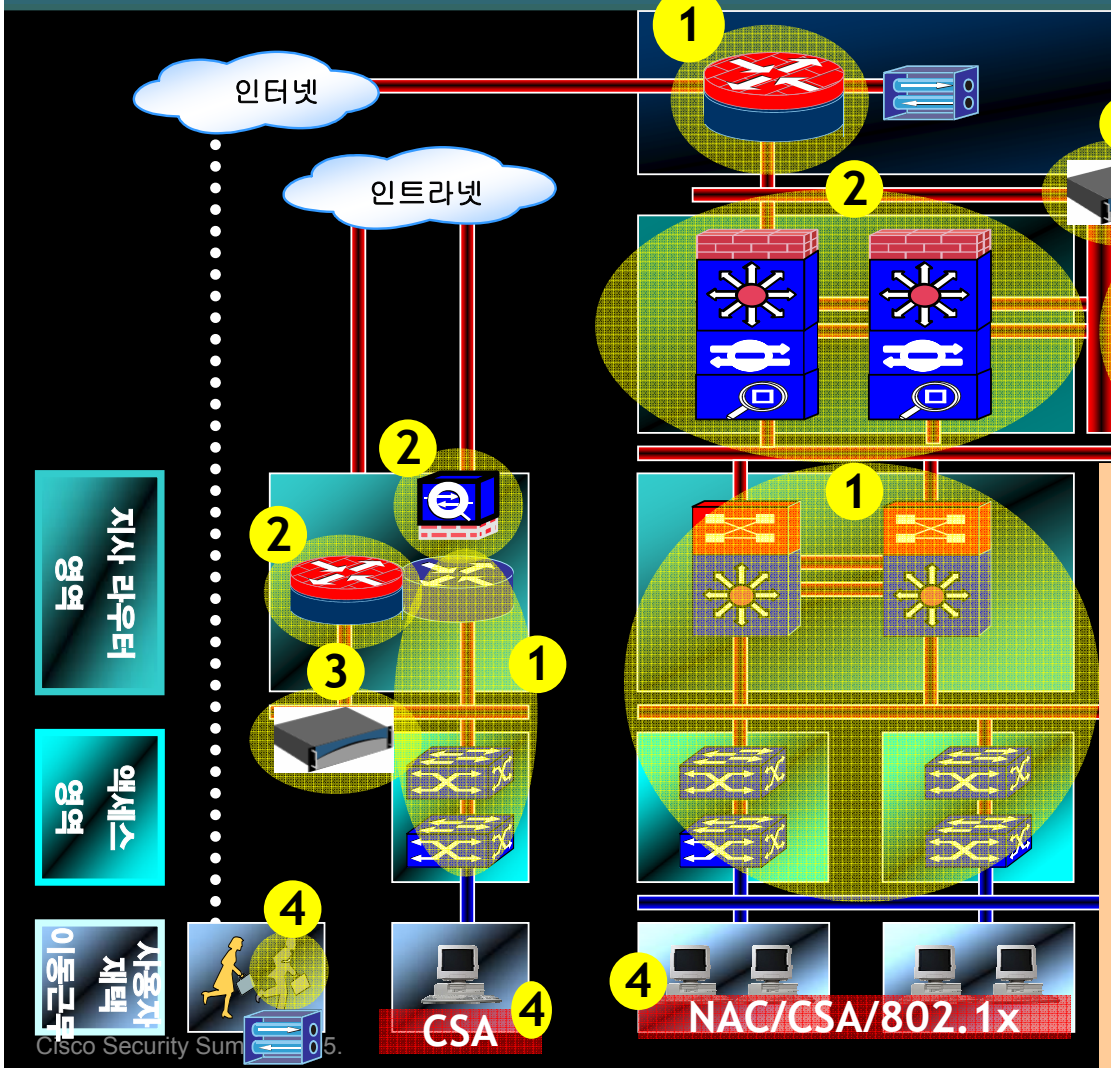


1. Network Infra 보안 구현
   – 기존 Router, Switch
2. Intelligent Security 구현 #1
   – 6500 통합 보안 스위치, ASA 5500
3. Intelligent Security 구현 #2
   – CS-MARS 보안 관제
4. End-Point Security
   – Cisco NAC & CSA & 802.1x
5. Application Security
   – AVS, ACE, AON 구축

기업 네트워크 구성 예제

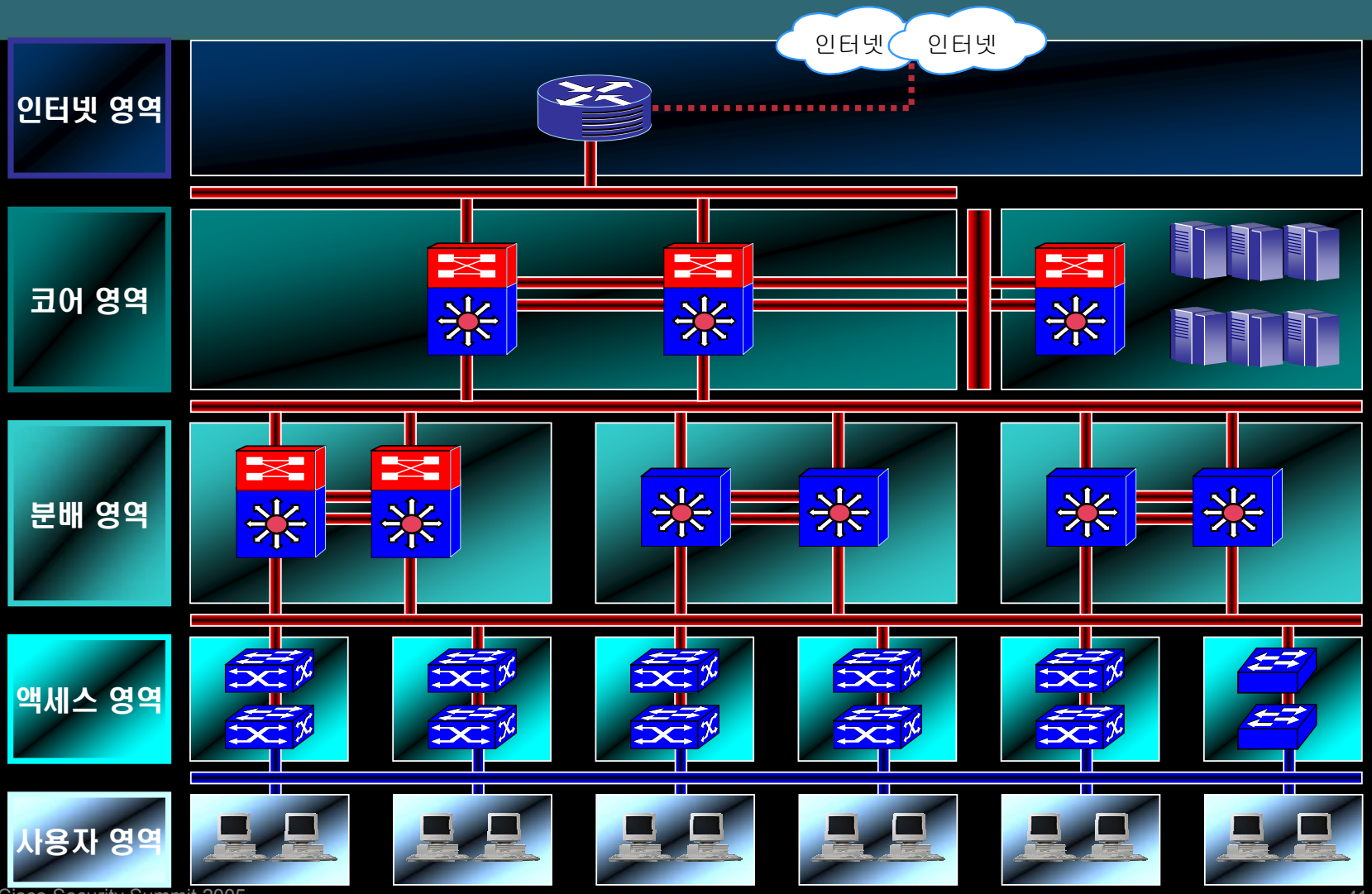


기업 네트워크 보안 구성 예제



1. Network Infra 보안 구현
   – 기존 Router, Switch
2. Intelligent Security 구현 #1
   – 6500 통합 보안 스위치, ASA 5500
3. Intelligent Security 구현 #2
   – CS-MARS 보안 관제
4. End-Point Security
   – NAC,CSA,802.1x,Web VPN
5. Application Security
   – AVS, ACE, AON 구축

캠퍼스 네트워크 구성도 예제



캠퍼스 네트워크 구성도 예제

1. Network Infra 보안 구현
   – 기존 Router, Switch
2. Intelligent Security 구현 #1
   – 6500 통합 보안 스위치, ASA 5500
3. Intelligent Security 구현 #2
   – CS-MARS 보안 관제
4. End-Point Security
   – NAC,CSA,802.1x,Web VPN
5. Application Security
   – AVS, ACE, AON 구축

Why Cisco Security ?

I. 네트워크 인프라 보호가 보안의 기본입니다.

Cisco SDN – Integrated Security

II. End Point의 보안에도 이제는 관심을 기울일 때 입니다.

Cisco SDN – Collaborated Security

III. 좀 더 지능적인 보안이 고객의 네트워크를 안심시킵니다.

Cisco SDN – Adaptive Threat Security

IV. 유비쿼터스 시대의 보안의 핵심은 모든 영역에서의 보안입니다.

Cisco End to End Security Solution