

# 시스코와 트렌드마이크로의 NAC을 위한 네트워크 시큐리티 솔루션



**Cisco Systems**

**Trend Micro**

**2006.8.31**



錦上添花

금

상

첨

화

# 목차

1. **ASA5500 Series Overview**
2. **CSC-SSM (Content Security and Control)의 세부 기능**
3. 사용자 보안 솔루션
4. 결론

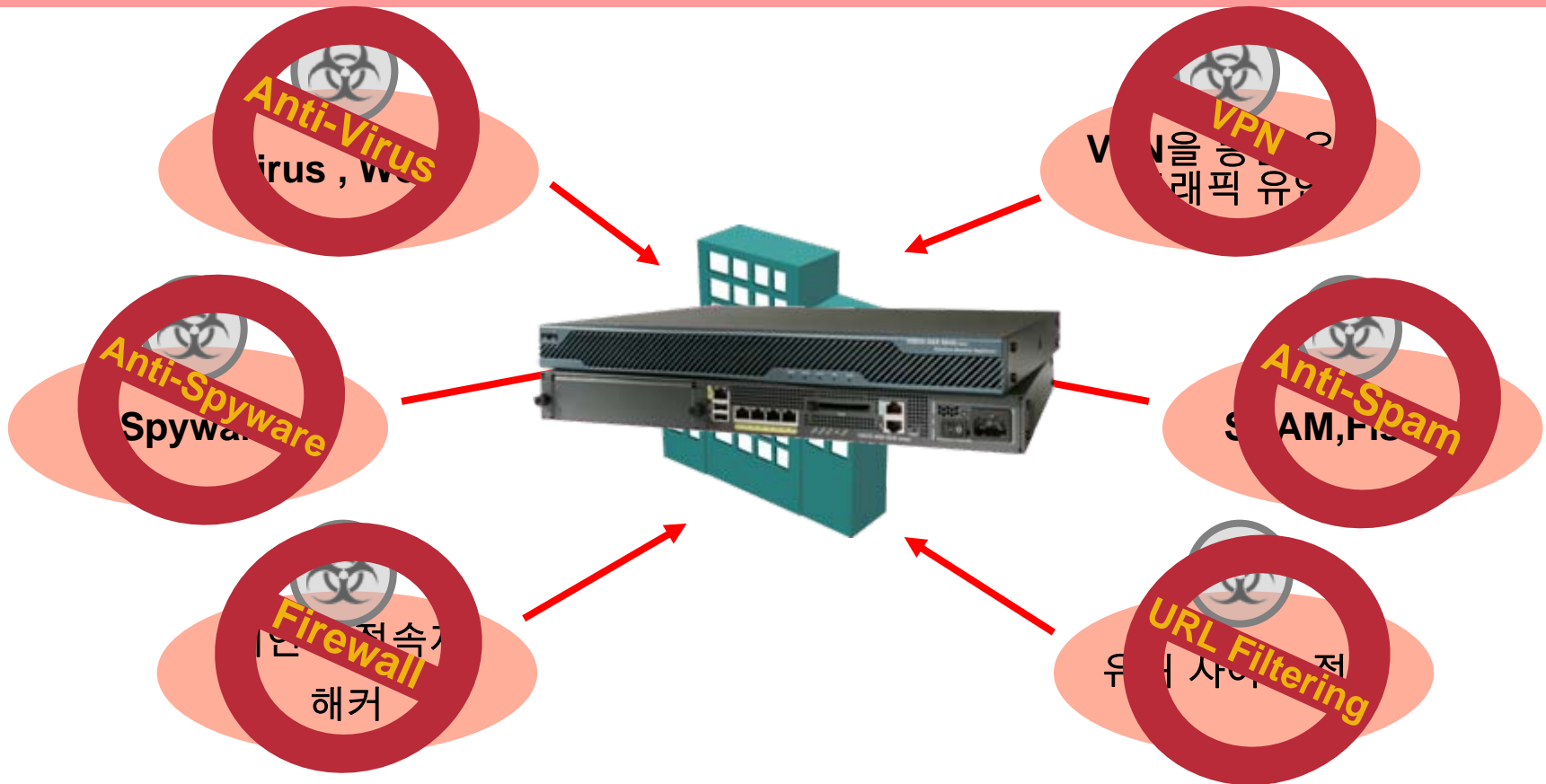


# ASA 5500 Series Overview

1

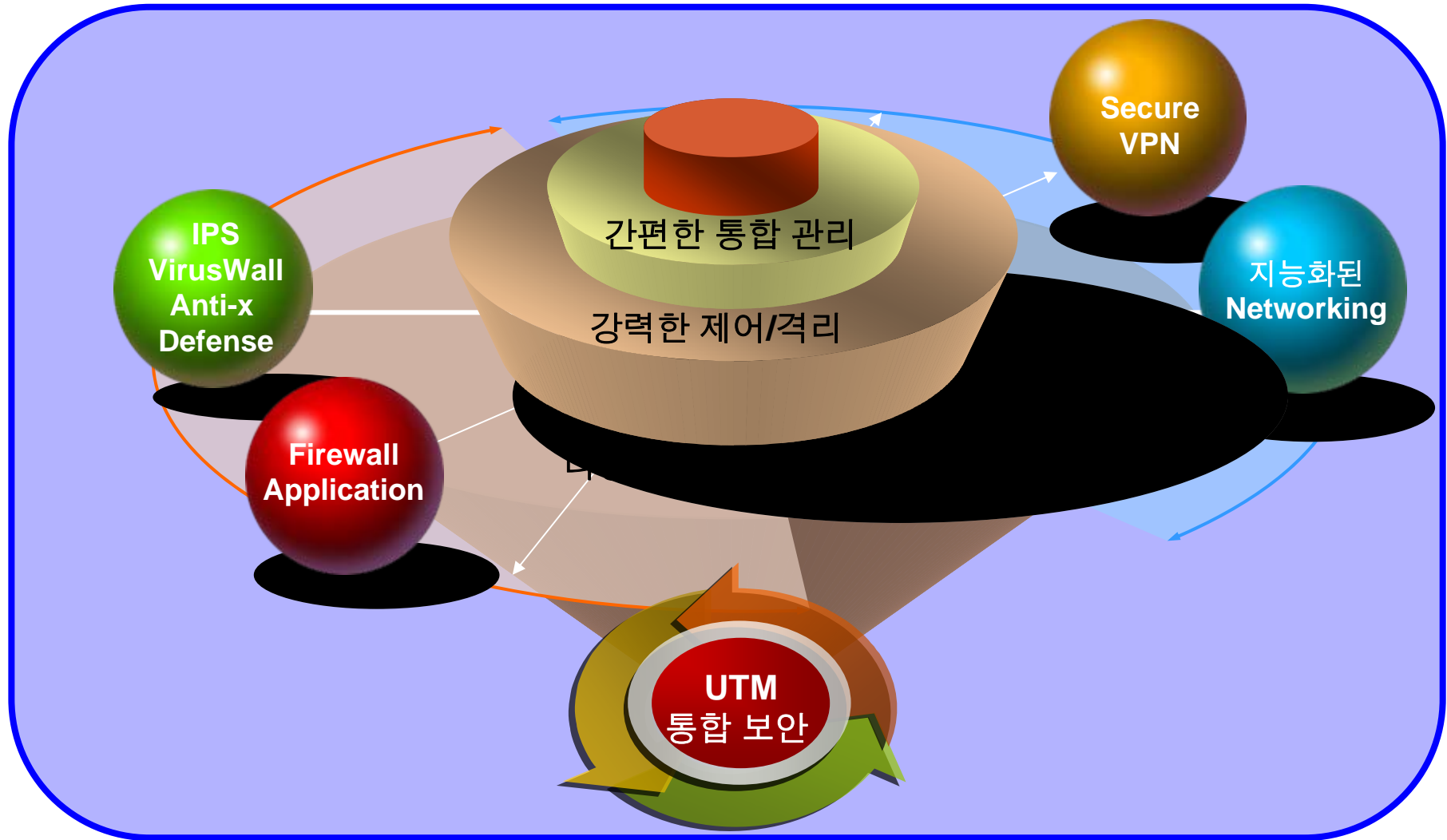
# 왜 통합 보안 장비 인가?

다양한 위협으로 부터 강력한 보안 서비스 요구



# 통합 네트워크 보안이란 ?

## UTM (Unified Threat Management)



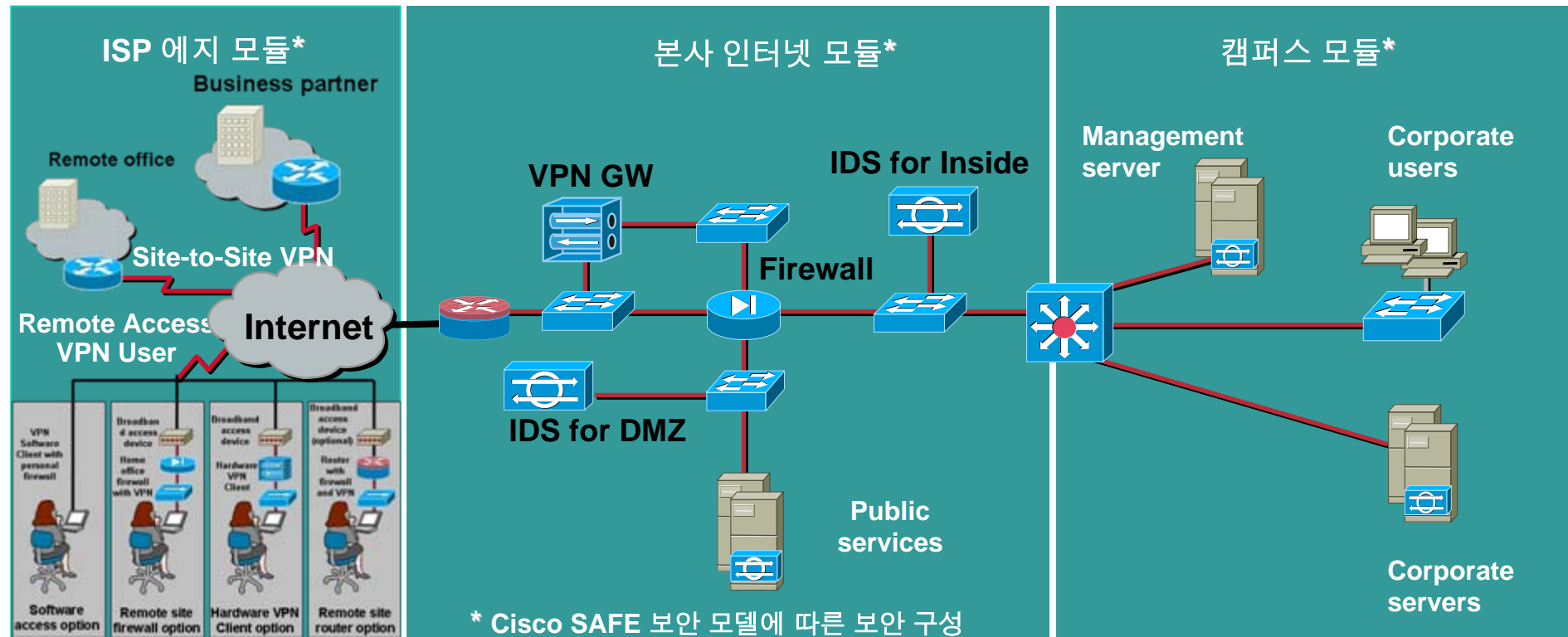
# 통합 네트워크 보안

## Cisco UTM Solution – ASA 5500



# 전형적인 기업 네트워크 보안구성

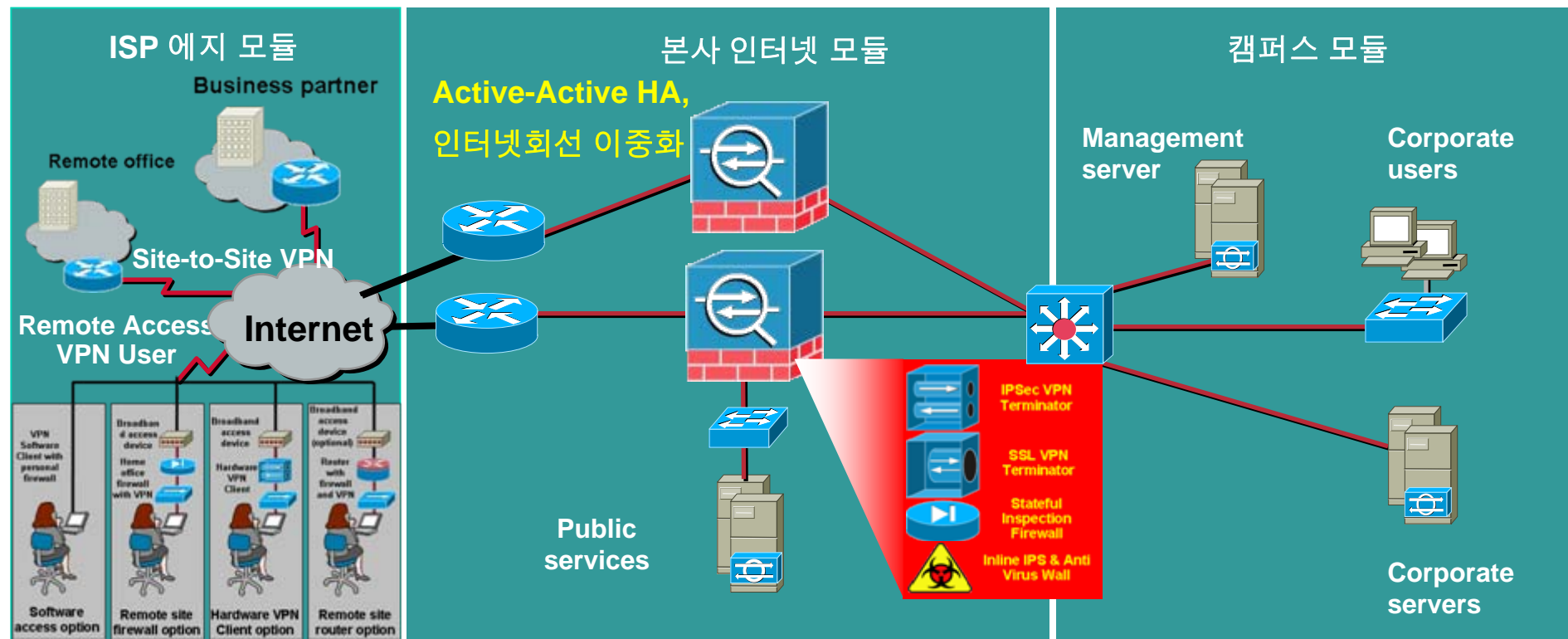
- **Gateway** 형태의 침입차단 시스템 단독 구성
- 각 서비스 **Network** 별 별도의 침입탐지시스템 구성
- **Remote Access VPN** 및 **Site-to-Site VPN** 을 위한 전용 **VPN** 장비 구성
  - ➔ 운영 비용의 증가
  - ➔ 관리 **Point Device** 증가로 인한 관리 효율 성 저하
  - ➔ 내부 사용자가 외부 **Internet** 또는 **Business Traffic** 유발 시 거쳐야 할 보안 **Device** 가 너무 많다!!



# ASA 5500를 이용한 네트워크 보안구성 1

## 기업 네트워크의 단순화 및 강력한 보안 네트워크 구성

- 기존 **Firewall, VPN, Anti-X** 을 통합 구성 → 종합 보안 기능 **100%** 지원
- 구성 단순화 및 관리적 비용 감소
- **Active-Active HA** 방화벽 구성 및,
- 인터넷 회선 이중화 구성으로 **Service** 연속성 및 고 가용성 보장 (비대칭 라우팅 기능 지원)



# ASA 5500를 이용한 네트워크 보안구성 2

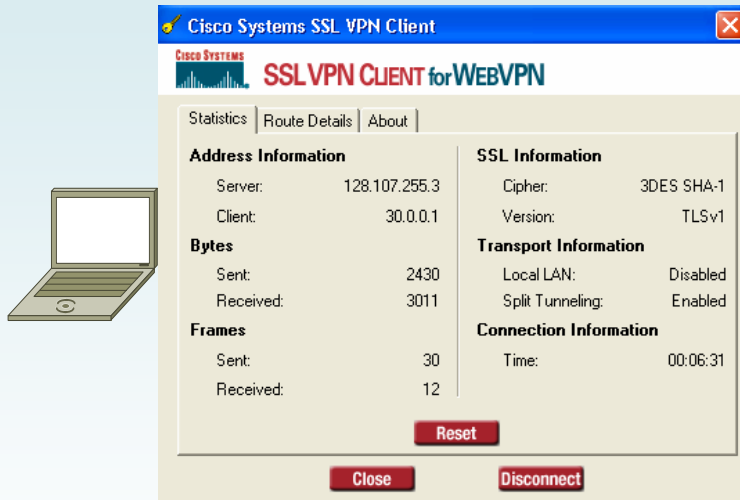
## IPSecVPN에서 SSLVPN까지 폭 넓게 대응

### SSLVPN 클라이언트

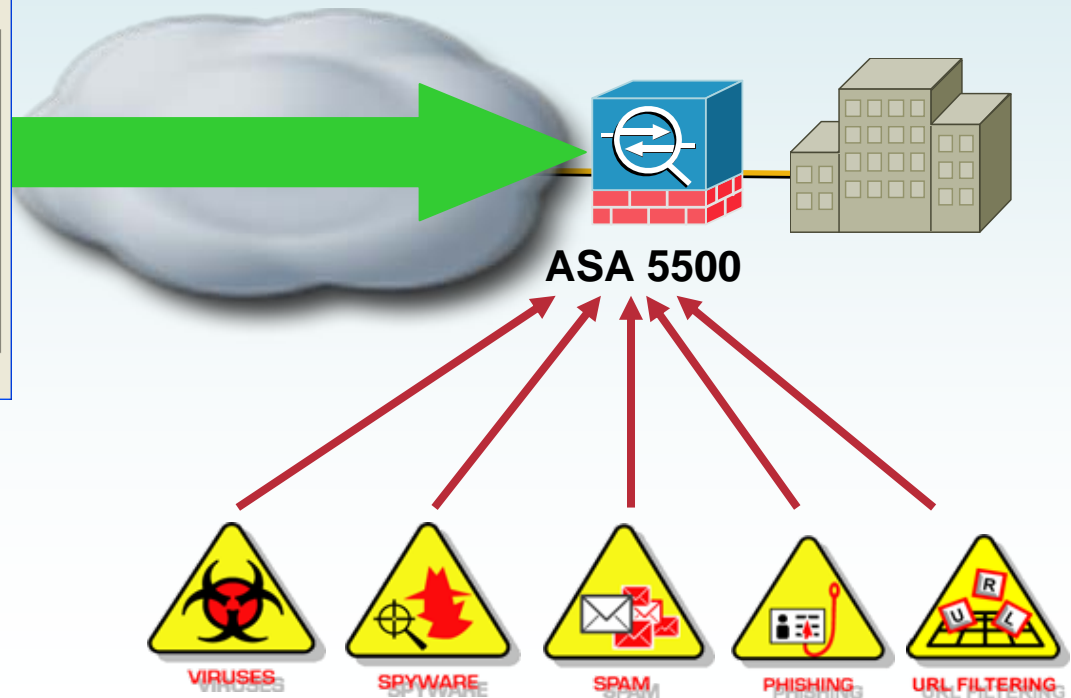
IPSec 클라이언트와 같은 기능 제공  
동시에 동적으로 클라이언트 설치

### VPN : 숨은 공격도 방어

SSL 내부의 트래픽에 FW 정책 또는 Anti-X  
정책을 설정함으로써 VPN 내부에 숨어있는  
위험 제어



포괄적인 차단:  
바이러스 차단  
스팸 메일 차단  
스파이웨어 차단  
피싱 차단



# Cisco ASA 5500 Series Anti-X Edition

광범위한 유해트래픽 제어 서비스

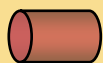
## THREAT TYPES



Unauthorized Access



Intrusions & Attacks



Insecure Comms.



Viruses

*New!*



Spyware



Malware



Phishing

Spam

허가되지 않은 URLs

Identity Theft

Offensive Content

## ASA 5500 with CSC-SSM



세밀한 정책 기반 제어

광범위한 유해 트래픽 차단

File 기반의 Inspection

Message 보안 통합

손쉬운 사용 관리

## PROTECTION

Resource & Information Access Protection

Hacker Protection

Client Protection

DDoS Protection

Protected Email Communication

Protected Web Browsing

Protected File Exchange

Unwanted Visitor Control

Audit & Regulatory Assistance

Non-work Related Web Sites

Identity Protection

# Cisco ASA 5500 Series Anti-X Edition

## Line-Up



### ASA 5510 and CSC-SSM



SME & Remote  
Office

300 Mbps  
500 (SSM-10)  
1000 (SSM-20)

Firewall, antivirus, anti-  
spyware, file blocking,  
IPSec VPN

Anti-spam, anti-  
phishing, URL  
blocking/filtering  
SSL VPN

### ASA 5520 and CSC-SSM



Remote Office

450 Mbps  
500 (SSM-10)  
1000 (SSM-20)

Firewall, antivirus, anti-  
spyware, file blocking,  
IPSec VPN

Anti-spam, anti-  
phishing, URL  
blocking/filtering  
SSL VPN

### CSC-SSM



SME & Remote  
Office

N/A  
500 (SSM-10)  
1000 (SSM-20)

Firewall, antivirus, anti-  
spyware, file blocking,  
IPSec VPN

Anti-spam, anti-  
phishing, URL  
blocking/filtering  
SSL VPN

Target Market

Max Firewall Performance  
Max Users

Base Platform  
Services

Optional Premium  
Services

# CSC-SSM (Content Security and Control)

## 라이선스 유형



VIRUSES



SPYWARE



SPAM



PHISHING



URL FILTERING

CSC-SSM 하드웨어	표준(Basic) 라이선스	옵션 (Plus)라이선스	
		사용자 업그레이드 (전체 사용자)	기능 업데이트
<b>ASA-SSM-CSC-10-K9=</b>	<ul style="list-style-type: none"> <li>• 50 사용자라이선스</li> <li>• 바이러스 차단, 스파이웨어 차단, 파일 차단</li> </ul>	<ul style="list-style-type: none"> <li>• 100 사용자</li> <li>• 250 사용자</li> <li>• 500 사용자</li> </ul>	<b>Plus</b> 라이선스-스팸 메일 차단, 피싱 차단, <b>URL</b> 차단/필터링, 콘텐츠 제어
<b>ASA-SSM-CSC-20-K9=</b>	<ul style="list-style-type: none"> <li>• 500 사용자라이선스</li> <li>• 바이러스 차단, 스파이웨어 차단, 파일 차단</li> </ul>	<ul style="list-style-type: none"> <li>• 750 사용자</li> <li>• 1000 사용자</li> </ul>	<b>Plus</b> 라이선스-스팸 메일 차단, 피싱 차단, <b>URL</b> 차단 / 필터링, 콘텐츠 제어

**CSC-SSM**는 위 2가지 라이선스로 제공되며, 각기 다른 기능을 지원합니다.

# 각 AIP-SSM 의 포지셔닝



## IPS Edition (AIP-SSM)

- 중규모 엔터프라이즈 사이트  
Large number of users  
Up to 450 Mbps
- 서버 보호와 **Critical** 자원 보호
- Stops network worms, hacking attempts, trojans, bots, zombies, and covert channel communication



## Anti-X Edition (CSC-SSM)

- 소규모, 중규모, 원격지 사무실의 엔터프라이즈 사이트  
Up to 1000 users  
Up to 120 Mbps
- Client 보호와 Internet Edge 보호
- Stops viruses, spyware / adware / grayware, malicious files, spam, phishing, and inappropriate URLs / content



## CSC-SSM (Content Security and Control)의 세부 기능

# 2

# CSC-SSM의 주요 기능

1 . 메일 보안

➡ **SMTP POP3**

2 . 웹 보안

➡ **HTTP**

3 . 파일 전송 보안

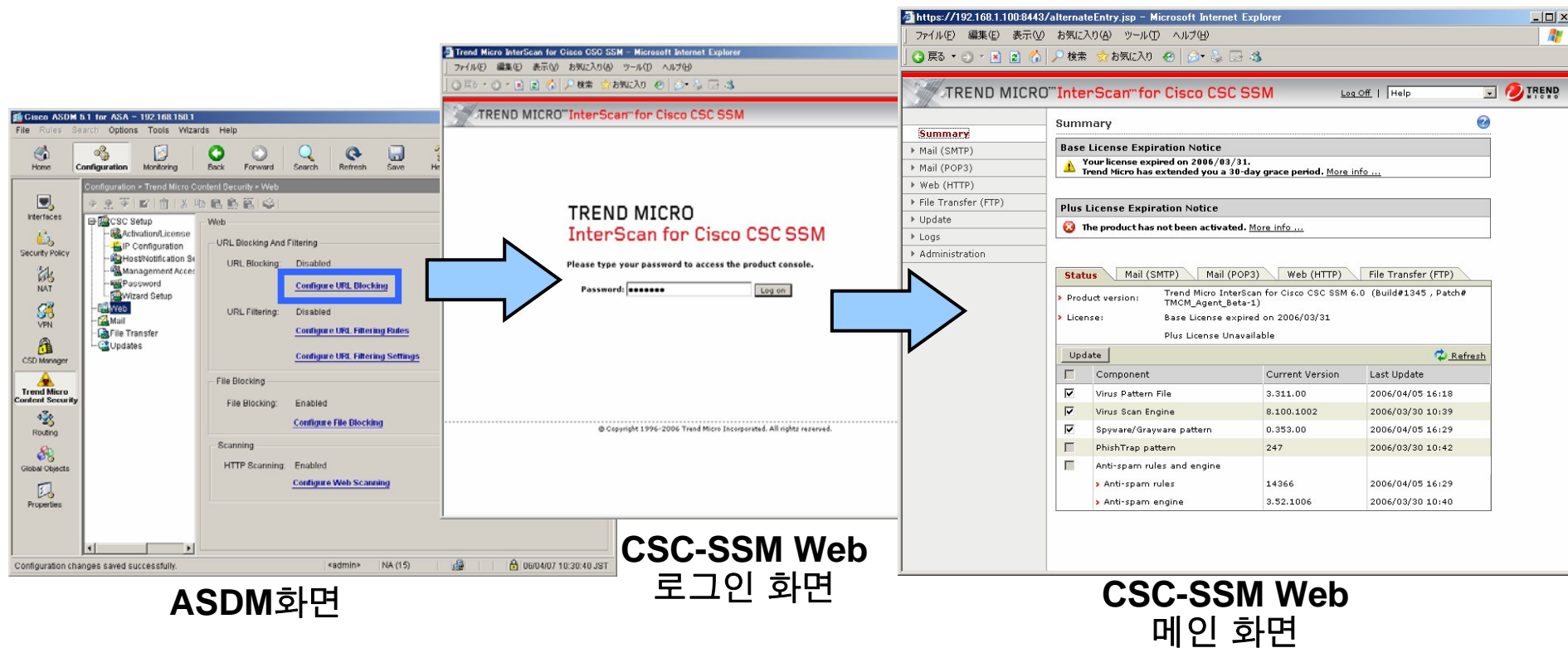
➡ **FTP**

4 . 통합관리

➡ **Trend Micro  
Control manager3.5**

# CSC-SSM 관리 콘솔

ASDM을 이용한 간편한 이동 및 효율적인 관리 통합 기능 제공



# CSC-SSM 관리콘솔(Cont'd)

## 모든 설정 및 Anti-X 정책 설정 가능

The screenshot displays the Trend Micro InterScan for Cisco CSC SSM management console. The interface includes a left sidebar with a 'Summary' menu and a main content area. The 'Summary' menu is highlighted with a blue box. The main content area shows a 'Summary' section with license expiration notices and a 'Status' section with a table of components and their update status. A blue box highlights the 'Status' section.

**Summary**

- Mail (SMTP)
- Mail (POP3)
- Web (HTTP)
- File Transfer (FTP)
- Update
- Logs
- Administration

**Summary**

**Base License Expiration Notice**

⚠ Your license expired on 2006/03/31. Trend Micro has extended you a 30-day grace period. [More info ...](#)

**Plus License Expiration Notice**

❌ The product has not been activated. [More info ...](#)

**Status**

Product version: Trend Micro InterScan for Cisco CSC SSM 6.0 (Build#1345, Patch# TCMC\_Agent\_Beta-1)

License: Base License expired on 2006/03/31

Plus License Unavailable

**Update** [Refresh](#)

<input type="checkbox"/>	Component	Current Version	Last Update
<input checked="" type="checkbox"/>	Virus Pattern File	3.311.00	2006/04/05 16:18
<input checked="" type="checkbox"/>	Virus Scan Engine	8.100.1002	2006/03/30 10:39
<input checked="" type="checkbox"/>	Spyware/Grayware pattern	0.353.00	2006/04/05 16:29
<input type="checkbox"/>	PhishTrap pattern	247	2006/03/30 10:42
<input type="checkbox"/>	Anti-spam rules and engine		
	➤ Anti-spam rules	14366	2006/04/05 16:29
	➤ Anti-spam engine	3.52.1006	2006/03/30 10:40

- 요약
- Mail(SMTP)
  - 바이러스 검사 설정
  - 스팸 메일
  - 콘텐츠 필터 설정
  - SMTP설정
- Mail(POP3)
  - 바이러스 검사 설정
  - 스팸 메일
  - 콘텐츠 필터 설정
- Web(HTTP)
  - VirusScan설정
  - 파일 차단 설정
  - URL 차단 설정
  - URL필터링 설정
- FTP
  - VirusScan 설정
  - 파일 차단 설정
- 업데이트
  - 매뉴얼
  - 스케줄
  - Proxy설정
- 로그
- 관리
  - 암호 설정
  - 인증 설정

# 1. 메일 보안 기능 – 기본 및 옵션

1 . 메일 보안

2 . 웹 보안

3 . 파일전송 보안

4. 통합관리

## 메일에 첨부된 바이러스 파일 검사

- **Scan POP3, SMTP**
- **Cleaning 서비스 수행**
- **Compressed files / attachment 탐지**
- **Fully featured configuration options**
  - user Flag , notify admin
  - 검역 기능 수행

## Anti-Spam

- **Spam 위협별 Setting (High/Med/Low)**
- **Approved/blocked senders**
- **Flag/delete option**

## Content Filtering

- **Message size**
- **Subject & body filters**
- **첨부 파일 이름이나 종류에 의한 filters**



# 1. 메일 보안 기능 - 검사 대상 설정

TREND MICRO™ InterScan™ for Cisco CSC SSM

Log Off | Help

Summary

▼ Mail (SMTP)

Scanning

Incoming

Outgoing

Anti-spam

Content Filtering

Incoming

Outgoing

Configuration

► Mail (POP3)

► Web (HTTP)

► File Transfer (FTP)

► Update

► Logs

► Administration

## SMTP Incoming Message Scan

Target Action Notification

SMTP Incoming Message Scan **Enabled** Disable

### Default Scanning

Select a method:

☐ All scannable files

☒ IntelliScan: uses "true file type" identification

☐ Specified file extensions...

### Compressed File Handling

Action on password-protected files: ☒ Deliver ☐ Delete

Do not scan compressed file if:

Decompressed file count exceeds: 200 (1-400)

Size of a decompressed file exceeds: 20 (1-30)MB

Number of layers of compression exceeds: 3 (2-20)

Size of decompressed files is "x" times the size of compressed file: 100 (2-200)

Action on unscanned compressed files: ☒ Deliver ☐ Delete

### Scan for Spyware/Grayware

☒ Select all

☒ Spyware

☒ Adware

☒ Dialers

☒ Joke Programs

☒ Hacking Tools

☒ Remote Access Tools

☒ Password Cracking Applications

☒ Others

Save Cancel

① 검사 대상 설정 관리 탭

검사 대상 파일 설정

암호화 파일 처리 설정

파일 크기/형식별 처리 설정

스파이웨어의 검사 설정

# 1.메일 보안 기능 – 감염파일 처리설정

TREND MICRO™ InterScan™ for Cisco CSC SSM

Log Off | Help

TREND MICRO

SMTP Incoming Message Scan

Target Action Notification

**For Messages with Virus/Malware Detection**

☒ Clean detected files before delivering the message

If undetectable: Delete

☐ Deliver message without detected attachment.

☐ Deliver message with detected attachment (not recommended)

**For Spyware/Grayware Detections**

☒ Allow spyware/grayware files to be delivered

☐ Delete spyware/grayware files

Save Cancel

Summary

▼ Mail (SMTP)

Scanning

Incoming

Outgoing

Anti-spam

Content Filtering

Incoming

Outgoing

Configuration

► Mail (POP3)

► Web (HTTP)

► File Transfer (FTP)

► Update

► Logs

► Administration

②감염파일 처리 설정 템

바이러스 감염파일 처리방법 설정

스파이웨어웨어 처리 방법 설정

# 1. 메일 보안 기능 - 감염시 경고 설정

## ③ 감염시 경고 설정 템

TREND MICRO™ InterScan™ for Cisco CSC SSM Log Off | Help

Summary

▼ Mail (SMTP)

Scanning

Incoming

Outgoing

Anti-spam

Content Filtering

Incoming

Outgoing

Configuration

► Mail (POP3)

► Web (HTTP)

► File Transfer (FTP)

► Update

► Logs

► Administration

SMTP Incoming Message Scan

Target Action Notification

Email Notifications

When a security risk is detected in an incoming message, the following notifications will be sent via email:

☐ Administrator A security risk was detected in an incoming SMTP message from %SENDER% to %RCPTS% titled %SUBJECT%.

☐ Sender A security risk was detected in a message you attempted to send, titled %SUBJECT%. The message may not be delivered to the recipient, %RCPTS%. We suggest scanning your computer for security risks.

☐ Recipient Warning - security risk was detected in a recent message addressed to you titled %SUBJECT% from %SENDER%. If the security risk cannot be removed, the message may not be delivered.

Inline Notifications

The following comments will be inserted in all scanned incoming messages and viewable by recipients:

☐ Risk free message This message has been scanned by the InterScan for CSC SSM and found to be free of known security risks.

☒ Message with security risk %VIRUSNAME% was detected in the file (%FILENAME%). The following action has been taken: %ACTION%

Save Cancel

발송대상별 경고메일 내용

메일본문에 삽입할 경고 내용

## 2.웹 보안 기능 – 기본 기능

1 . 메일보안

2 . 웹 보안

3 . 파일 전송 보안

4. 통합 관리

### 웹 액세스 시 바이러스 검사

- 바이러스 발견 시 브라우저 상에 임의로 메시지 표시
- 발견 시 감염 파일의 바이러스 제거 / 감염파일 삭제 중에서 원하는 처리 방식 선택 가능



### 파일 차단

- 특정 파일 유형의 다운로드 제한
- 차단 시 웹 브라우저 상에 표시하는 통지 메시지 편집 가능
- 관리자에 대한 통지 유무 및 통지 내용 설정 가능



### 스파이웨어 차단

- 스파이웨어나 조크 프로그램을 탐지 및 삭제

## 2.웹 보안 기능 – 옵션 기능

1 . 메일보안

2 . 웹 보안

3 . 파일 전송 보안

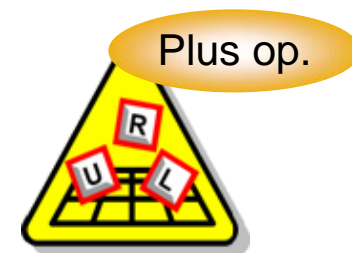
4. 통합 관리

### URL 필터링

- TrendLabs online database 활용
- 10 categories (pornography, violence, etc., etc.)
- 특정 시간,기간 동안 **Block** 또는 허용할 **URL** 지정
- **exception URL list** 에 대한 **Import** 기능

### URL 블로킹

- “**Black list**” 설정을 통한 차단 설정
- **URL list** 에 대한 **Import** 기능
- “**white list**”을 이용한 예외 설정



### 피싱 차단

- 알려진 **phishing, spyware, malicious site**들에 대한 **URL Block**

## 2. 웹 보안 기능 – URL 블로킹 설정

1. 제품 소개

2. 웹 보안

3. 파일 전송 보안

4. 설정 관리

TREND MICRO™ InterScan™ for Cisco CSC SSM

Log Off | Help

Summary

Mail (SMTP)

Mail (POP3)

Web (HTTP)

Scanning

File Blocking

URL Blocking

URL Filtering

Filtering Rules

Settings

File Transfer (FTP)

Update

Logs

Administration

URL Blocking

Via Local List | Via Pattern File (PhishTrap) | Notification

URL Blocking: Enabled Disable

URLs to Block

Match: www.example.com

Web site (example: 'xxx.com' matches all URLs starting with 'xxx.com')

URL keyword (example: 'yyy' string matches all URLs containing 'yyy')

Subsite/Path address (exact-match, example: zzz.com/file matches only 'zzz.com/file')

Block Do Not Block

Import block list and exceptions: 参照... Import

Block List

Users are never allowed to access URLs included in this list.

www.example.com\*

Remove Remove All

Block List Exceptions

Access to these URLs is always allowed.

Remove Remove All

Save Cancel

① Web(HTTP) 메뉴에서 URL Blocking 선택

② 액세스를 차단하려는 URL 등록

③ 등록 실행

④ 등록 결과

⑤ 설정 반영

## 2. 웹 보안 기능 – URL 블로킹 설정 (Cont'd.)

### URL 차단 정책에 의한 차단시 브라우저 경고 설정

TREND MICRO™ InterScan™ for Cisco CSC SSM

Log Off | Help

URL Blocking

Via Local List | Via Pattern File (PhishTrap) | **Notification**

**User Notification**

Display the following message in the user's browser when a blocked URL is accessed:

The URL you are attempting to access has been blocked. Organization policy does not allow access to this activity.

Save Cancel

① Notification 태그 선택

② 표시할 문장 입력

③ 설정 반영

## 2. 웹 보안 기능 – URL 필터링 설정

URL Categories		URL Filtering Exceptions		Schedule		Re-classify URL	
Move Selected Sub-categories to: --Select one--		<input type="button" value="Move"/>					
Sub-category	Company Prohibited Sites	Non-work Related	Research Topics	Business Function Related	Customer Defined	Others	
<input type="checkbox"/> Illegal Drugs	X						
<input type="checkbox"/> Violence/Hate/Racism	X						
<input type="checkbox"/> Nudity	X						
<input type="checkbox"/> Intimate Apparel/Swimsuit	X						
<input type="checkbox"/> Sex Education	X						
<input type="checkbox"/> Pornography	X						
<input type="checkbox"/> Adult/Mature Content	X						
<input type="checkbox"/> Alcohol/Tobacco						X	
<input type="checkbox"/> Illegal/Questionable						X	
<input type="checkbox"/> Gambling		X					
<input type="checkbox"/> Weapons						X	
<input type="checkbox"/> Abortion						X	
<input type="checkbox"/> Arts/Entertainment		X					
<input type="checkbox"/> Business/Economy			X				
<input type="checkbox"/> Cult/Occult						X	
<input type="checkbox"/> Education		X					
<input type="checkbox"/> Cultural Institutions		X					

- 업무와 무관한 URL에 대한 액세스 제한

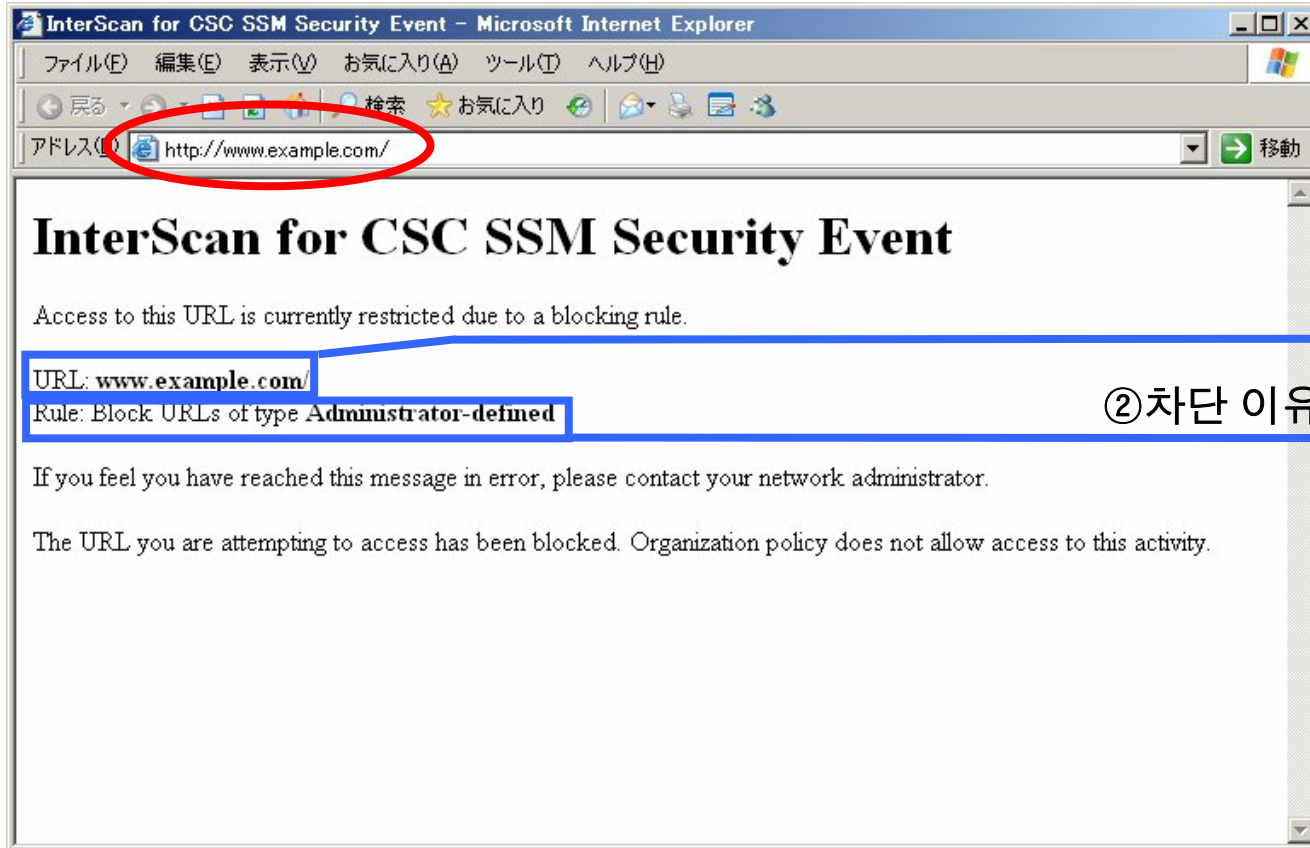
- 제한 URL은 카테고리별로 설정

- 그룹별, 시간별, 요일별 등의 속성으로 제한 카테고리 변경 가능

- URL 목록은 트렌드마이크로가 수시로 변경함

- 개별 블랙리스트, 화이트리스트의 설정 가능

## 2. 웹 보안 기능 – URL 차단시 경고 화면



① 차단된 URL

② 차단 이유(관리자에 의해 금지됨)

# 3.파일 전송 보안

1 . 메일보안

2 . 웹 보안

3 . 파일 전송 보안

4. 통합관리

## 파일 전송 시 바이러스 검사 실시

- 바이러스 발견 시 **FTP** 클라이언트 상에서 임의 메시지 표시 및 통지
- 바이러스 발견 시 관리자에게 통지 메일을 발송 가능
- 발견 시 감염 파일의 바이러스 제거 / 감염파일 삭제 중에서 원하는 처리 방식 선택 가능



## 파일 차단

- 특정 파일 유형의 다운로드 제한
- 차단 시 **FTP** 클라이언트 상에 표시할 통지 메시지 편집 가능
- 관리자에 대한 통지 유무 및 통지 내용 설정가능



## 스파이웨어 차단

- 스파이웨어나 죠크 프로그램을 탐지 및 삭제



# 4.중앙 관리 기능

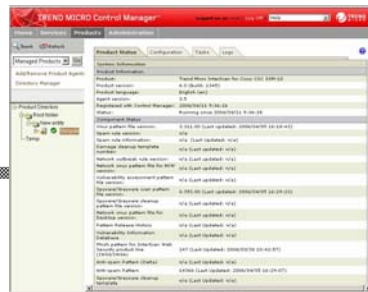
별도 라이선스

## CSC-SSM의 통합관리

- Trend Micro Control Manager 3.5를 이용한 CSC-SSM 관리 통합
  - 다수의 CSC-SSM에 대한 관리 통합
  - 각종 패턴의 파일, 검색 엔진 송신
  - 로그인 관리 통합, 보고 기능
  - 감염 클라이언트 치료DCS



Trend Micro Control Manager



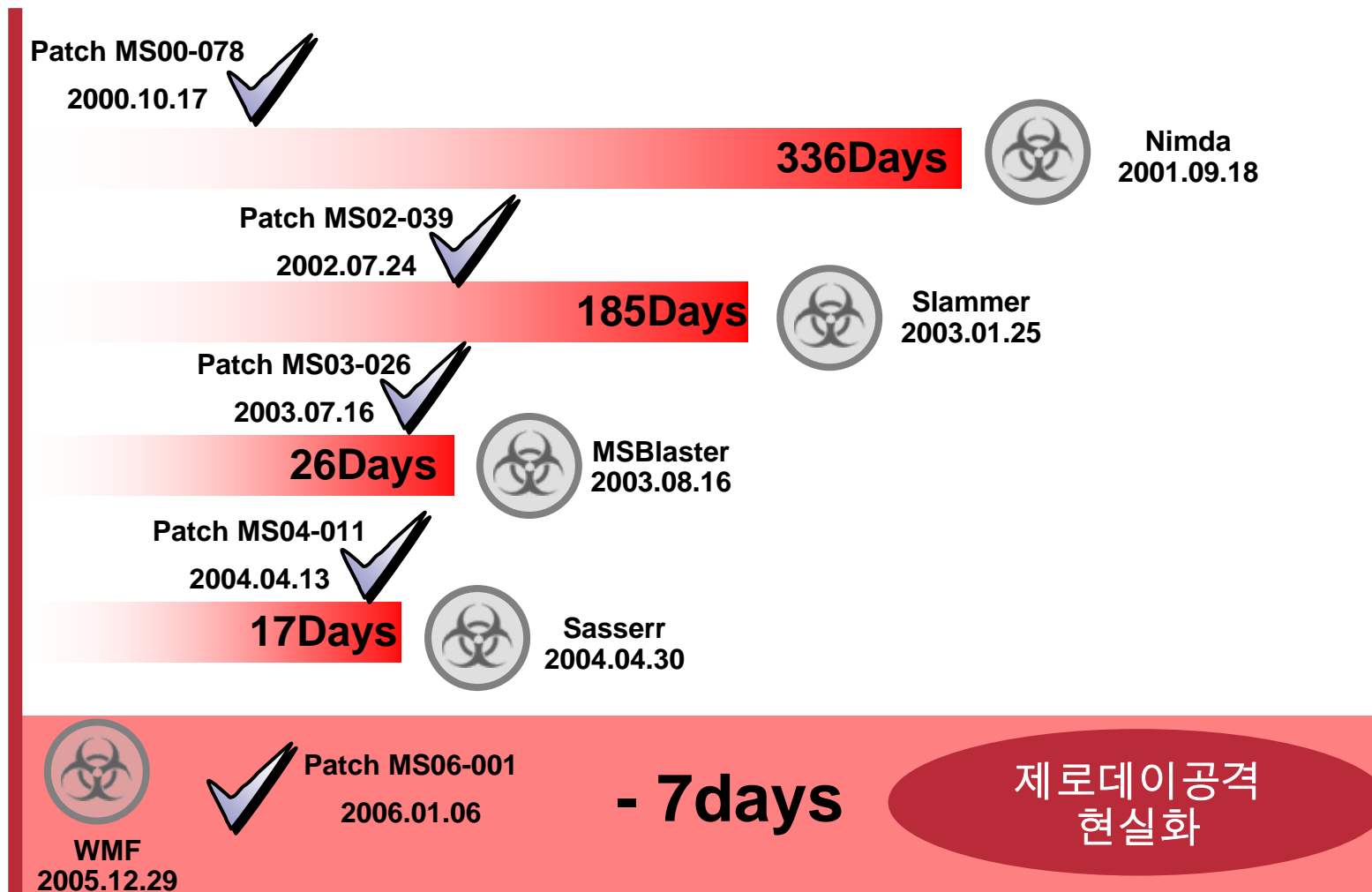
트렌드마이크로의 바이러스 백신 제품들



## 사용자 보안 솔루션

# 3

# Zero Day 공격의 위협 변화



# 트렌드마이크로의 NAC 차단 제품

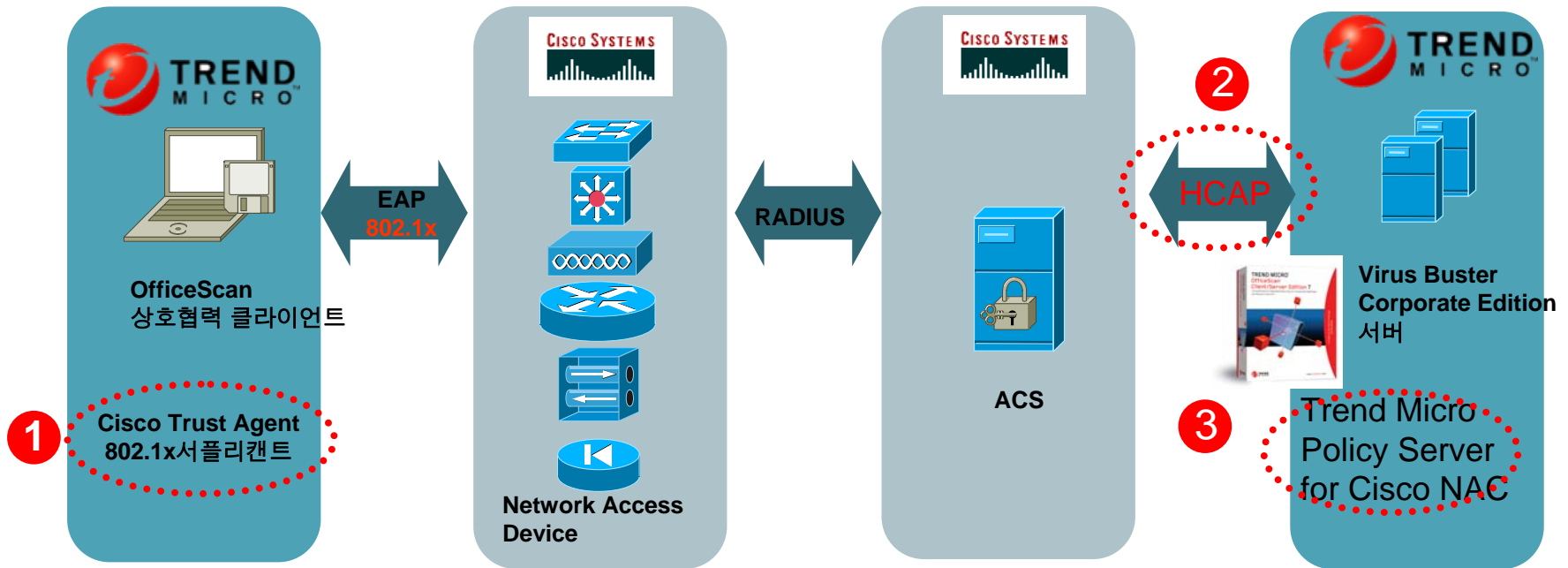
## Trend Micro Office Scan Client/Server Edition 7

- CTA Ver2.0 포함
- Cisco의 802.1x Supplicant 포함
- Office Scan Policy 서버에서 CTA, Supplicant로 전달 가능
- 퍼스널 방화벽 기능 ( Advanced Edition )
- Winny탐지 기능 ( Advanced Edition )

*NAC Ready!*



# 시스코와 트렌드마이크로의 완벽한 NAC호환성



## 1 OfficeScan Client/Server Edition Client와 CTA 연동

- OfficeScan Client/Server Edition Client의 모든 상태 정보를 CTA에서 모두 인식 및 전달 가능
- 802.1x Supplicant도 제품에 연동

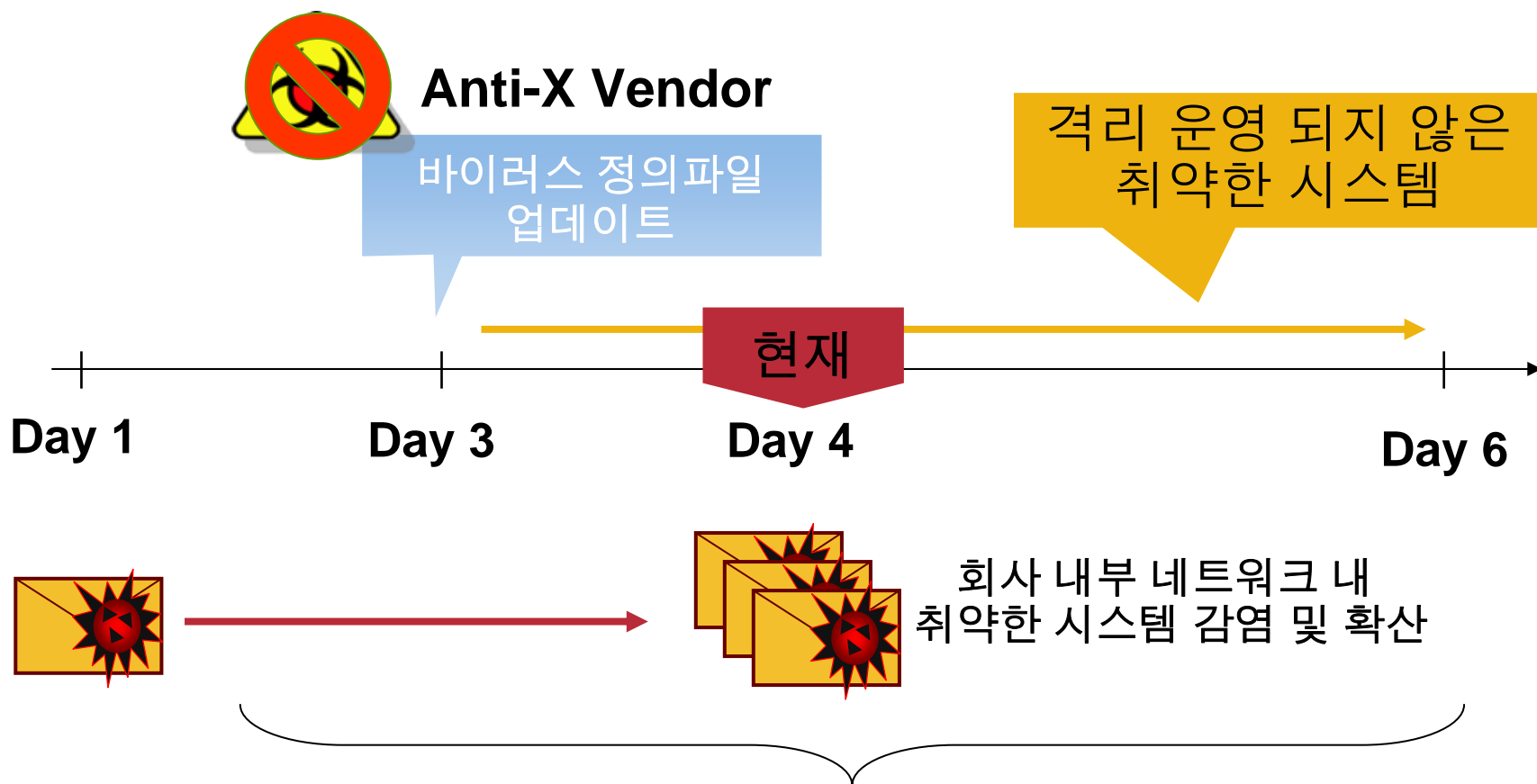
## 2 HCAP을 정식으로 지원

- ACS와 OfficeScan Client/Server Edition Server간의 실시간 정보 전달 및 연동

## 3 Trend Micro Policy Server for Cisco NAC

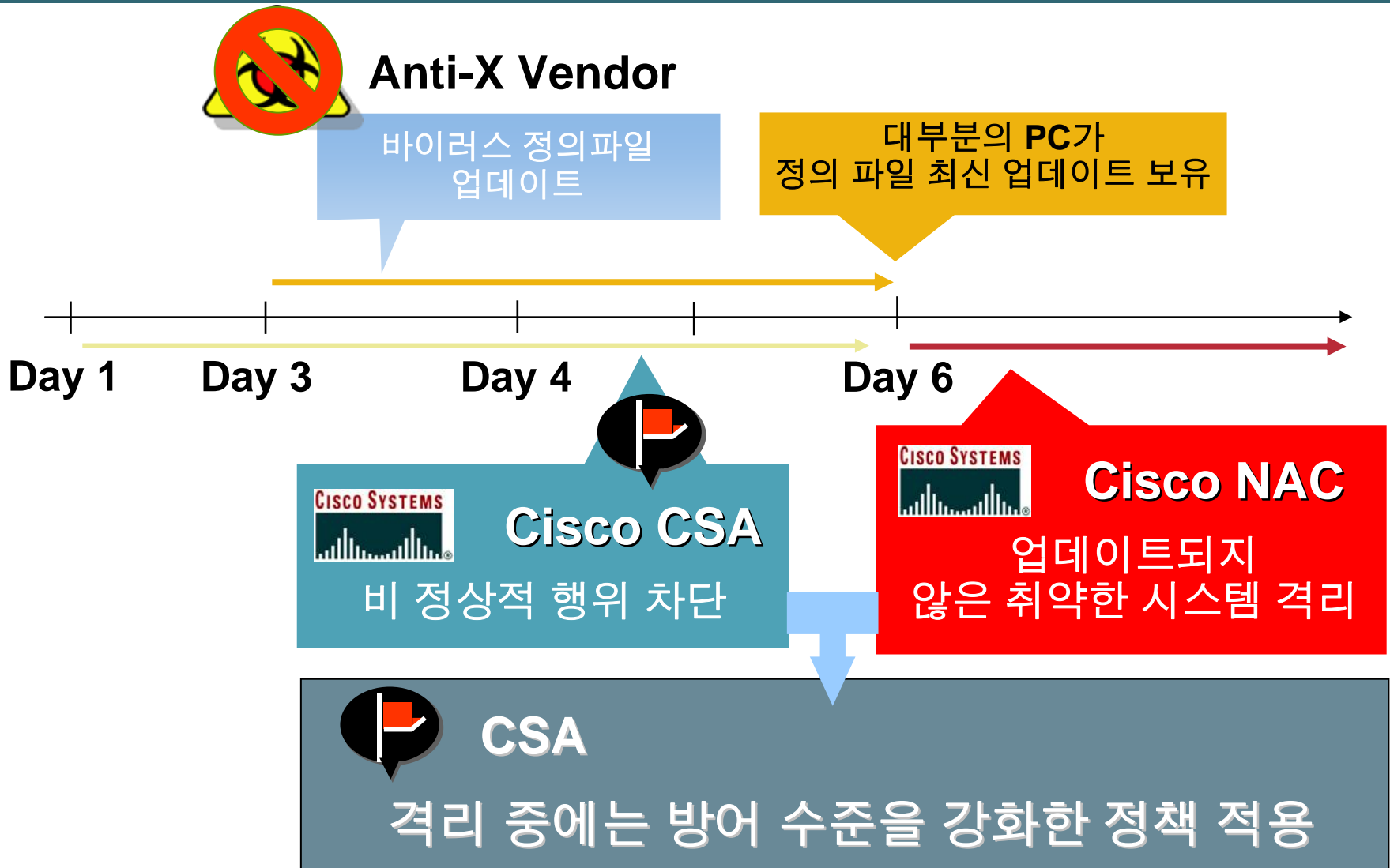
- GUI에 의한 정책 관리를 통해 보다 용이한 NAC 도입, 정책 관리 · 운영 실현

# 취약한 사용자 보안 환경



제로 공격에 대항할 수 있는 **CSA, IPS**의 연동 필요

# Cisco NAC 과 CSA 의 연동



# Cisco CSA의 접근 방법



# CSA와 Anti-Virus는 상호 보완적

	CSA	Anti-Virus
Malicious Code Protection		
Stop Known Virus/Worm Propagation	X	X
Stop Unknown Virus/Worm Propagation	X	
Scan/Detect Infected Files		X
“Clean” Infected Files		X
Identify Viruses/Worms by Name		X
No Signature Updates Required	X	
Distributed Firewall Functionality	X	
Operating System Lockdown	X	
Correlates Events Across Endpoints	X	



결론

4

# 결론



錦上添花



**Global Network Infra Security 최강자 → Cisco Systems**

**Global Contents Security & 사용자 보안 리더 → Trend Micro**

**Collaboration Technology 의 절정체 → ASA 5500 & CSC-SSM**

# CISCO SYSTEMS

