Cisco.com

사용자 보안 솔루션
(End Point Security Solution)

2004년 10월 20일

Cisco Systems Korea
최 우 제(wjchoi@cisco.com)

목 차

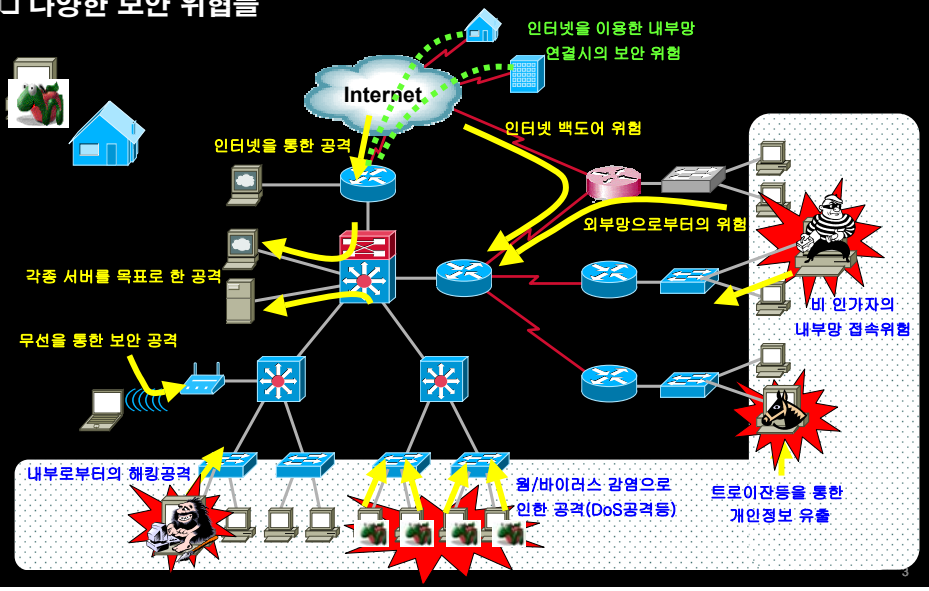
Cisco.com

- 오늘날의 사용자 보안
- Cisco의 사용자 보안 전략
- 사용자 인증 (IBNS)
- 사용자 호스트 보안상태 인증(NAC)
- 사용자 호스트 침입 차단(CSA)
- 데모: Cisco 사용자 보안 구현 예

오늘날 사용자 보안

Cisco.com

❑ 다양한 보안 위협들



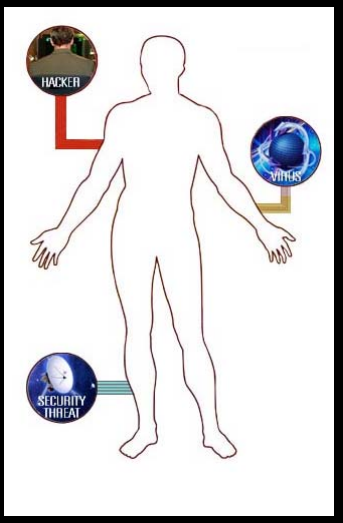
Cisco.com

Cisco 사용자 보안 전략

Cisco 사용자 보안 비전

인체와 같은 자가 면역 기능을 갖춘 네트워크

Self-Defending Network



자가 방어 네트워크 전략

SELF-DEFENDING NETWORK

위협에 대한 인지, 방어,
그리고 적응 능력을
극적으로 향상시키기 위한
Cisco 보안 전략

INTEGRATED SECURITY

- Secure Connectivity
- Threat Defense
- Trust & Identity

INDUSTRY COLLABORATION

- Endpoint Security
- Application Firewall
- SSL VPN
- Network Anomaly

SYSTEM LEVEL SOLUTION

- Dynamically identify, prevent, and respond to threats
- Endpoint + Network

자가 방어 네트워크를 위한 Cisco 사용자 보안

사용자 인증 - **IBNS**

사용자 호스트 상태 인증 – **NAC**

사용자 호스트 침입 차단 – **CSA**

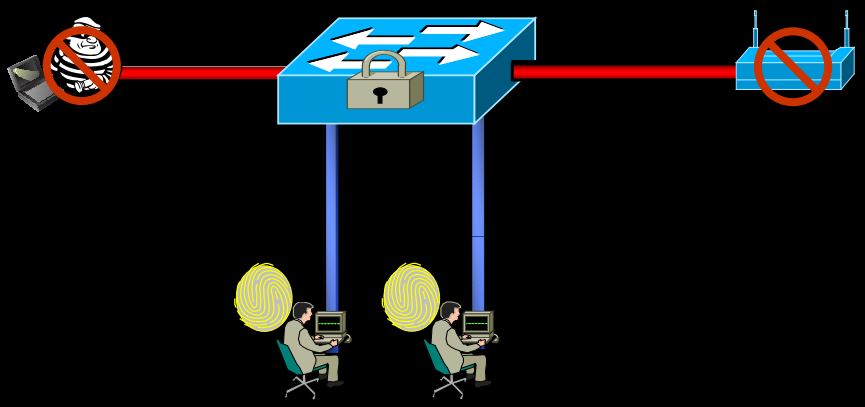
Cisco.com

사용자 인증 - IBNS
(Identity Based Networking Service)

시스코 사용자 인증 솔루션 -IBNS

Cisco.com

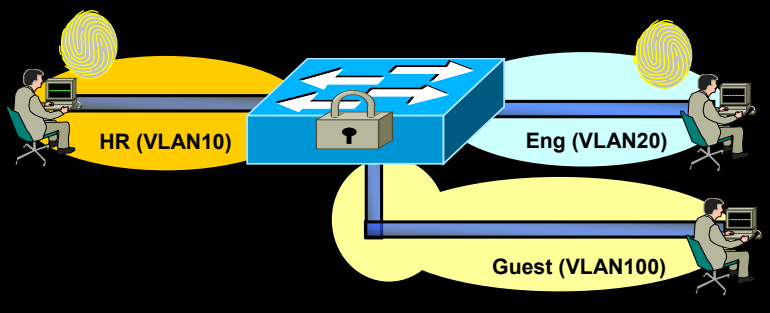
- ***802.1x기반의 IBNS*** **(Identity Based Networking Service)** 를 통해 사용자 인증을 통한 **Network** 접속 보안 서비스를 제공합니다.



IBNS 솔루션을 통한 사용자별 접속 제한 (VLAN)

Cisco.com

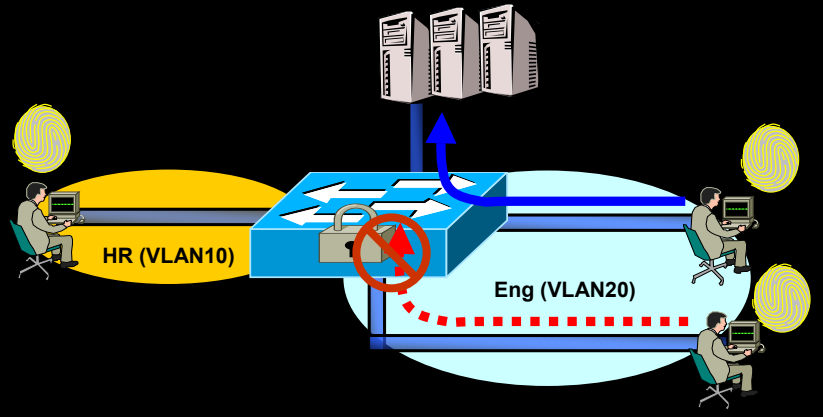
- 사용자별 **VLAN 할당**을 통해 사내 망에서의 접속 제한을 제공합니다.
- 인증을 받지 못한 사용자의 경우 **Guest VLAN할당**을 통한 제한적 접속을 제공할 수 있습니다.



IBNS 솔루션을 통한 사용자별 접속 제한(ACL)

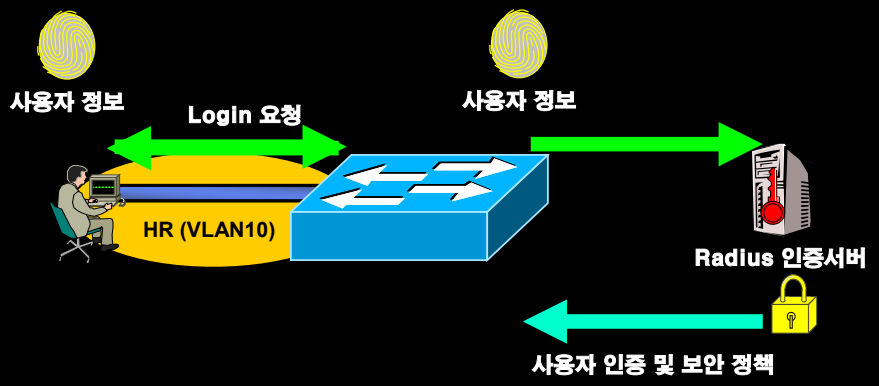
Cisco.com

- 사용자별 **Access Control (ACL)**적용을 통한 동일 **VLAN** 내에서의 접속 제한을 제공합니다.
- 사용자별 **QoS** 적용 가능.



시스코 IBNS 솔루션 구성

Cisco.com



시스코 사용자 인증 솔루션 -IBNS

- **IEEE 802.1X 표준 기반**의 사용자 인증을 제공합니다.
- **Window XP**에선 기본적으로 지원합니다.
- 기존 **Cisco** 스위치 **Infra**를 통해 적용 가능합니다.
  - **Catalyst 2950**
  - **Catalyst 3550/3750**
  - **Catalyst 4500**
  - **Catalyst 6500**

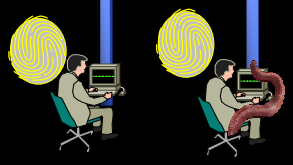
사용자 호스트 상태 인증 - NAC (Network Admission Control)

사용자 인증만으로 충분한가?

Cisco.com

- 사용자는 인증되었다 하더라도 호스트 자체에 대한 신뢰성을 검증할 수 없습니다.

사용자 인증과 Worm/Virus 방어는 별개입니다!!

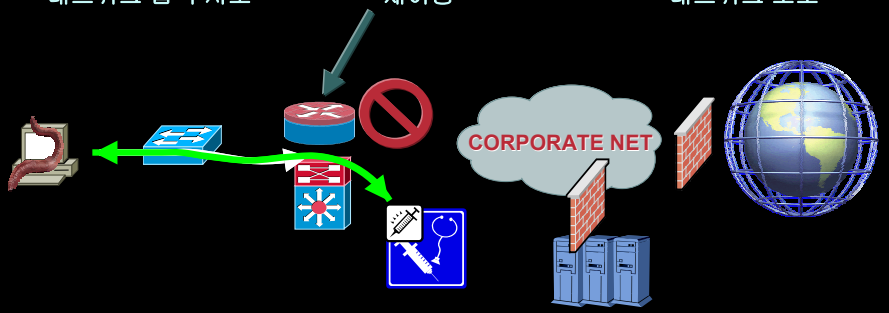


사용자 호스트 상태 인증 솔루션 -NAC

Cisco.com

- **NAC (Network Admission Control)을 통해 사용자 호스트의 상태에 따라 지능적으로 네트워크 접속을 통제할 수 있는 솔루션 입니다.**

1. 적절치 않은 Host의 네트워크 접속 시도
2. 검역/치료 지역으로 재이동
3. 감염을 차단하고 네트워크 보호

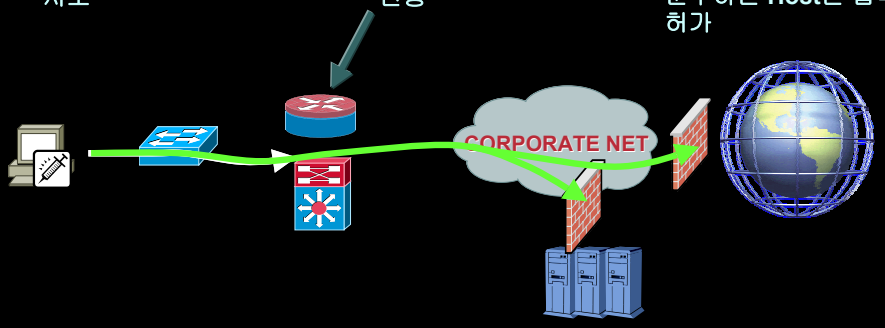


사용자 호스트 상태 인증 솔루션 -NAC

Cisco.com

- **NAC (Network Admission Control)을 통해 사용자 호스트의 상태에 따라 지능적으로 네트워크 접속을 통제할 수 있는 솔루션 입니다.**

1. Host의 네트워크 접속 시도
2. Host의 보안 상태 인증
3. 설정된 보안 기준을 준수하는 Host는 접속 허가



시스코 NAC 솔루션의 구성

Cisco.com

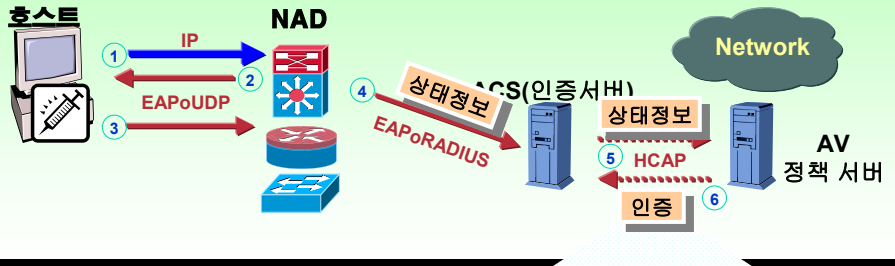
Network

Anti Virus

- Anti-Virus
  - AV software name
  - Software version
  - Scan engine version
  - DAT/pattern file version
  - AV enabled or not
  - On-access scan enabled
  - DAT/pattern file release date
- Other Software
  - Varies by vendor
  - E.g. SYMC SCS 2.0 includes FW & HIDS

시스코 NAC 솔루션의 구성

Cisco.com

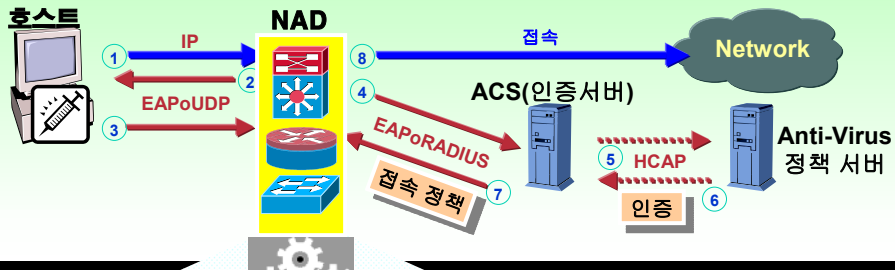


보안 상태 인증

- Health
- Checkup
- Unknown
- Quarantine(검역)

시스코 NAC 솔루션의 구성

Cisco.com



접속 정책 (ACL/URL Redirect)

- Healthy:전체 네트워크 접속 허용
- Checkup/Quarantine(검역):
  URL Redirect를 통한 검역
  서버로 이동
- Unknown: CTA download
  서버로 Redirect

시스코 NAC 솔루션은…

Cisco.com

Multi Partner Program

TREND MICRO

symantec.

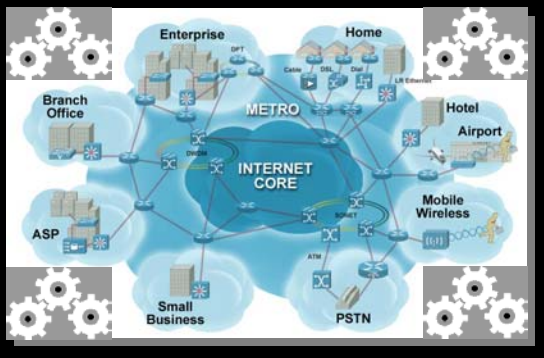
McAfee

Ahn 안철수연구소

시스코 NAC 솔루션은…

Cisco.com

사용자 호스트 보안 상태에 따라 네트워크에서의 보안 정책 적용



시스코 NAC 솔루션은...

Cisco.com

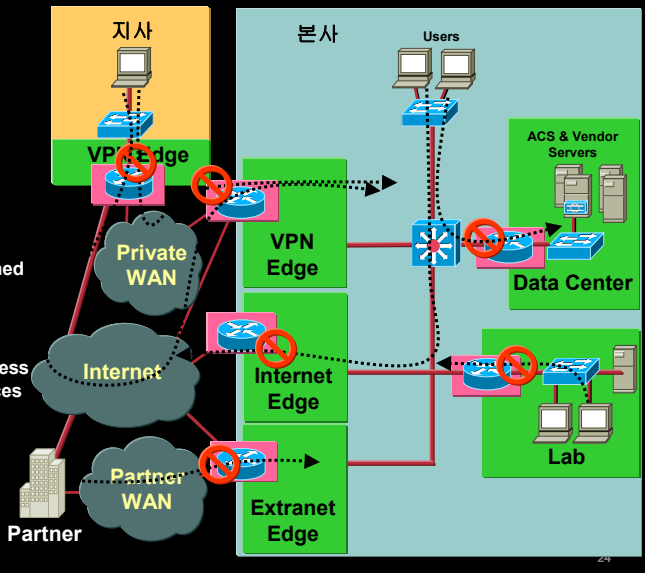
기존 Cisco Network 인프라 활용

NOW	CY2005
Cisco 18xx, 28xx, 38xx	Catalyst 6500
Cisco 72xx	Catalyst 4000/4500
Cisco 37xx	Catalyst 3550/3750
Cisco 3640, 3660-ENT Series	Catalyst 2950
Cisco 2600XM, 2691	Catalyst 2955/2970
Cisco 1701,1711, 1712, 1721, 1751, 1751-V, 1760	VPN 3000
Cisco 83x	IOS Switch

라우터 기반의 NAC 적용 시나리오

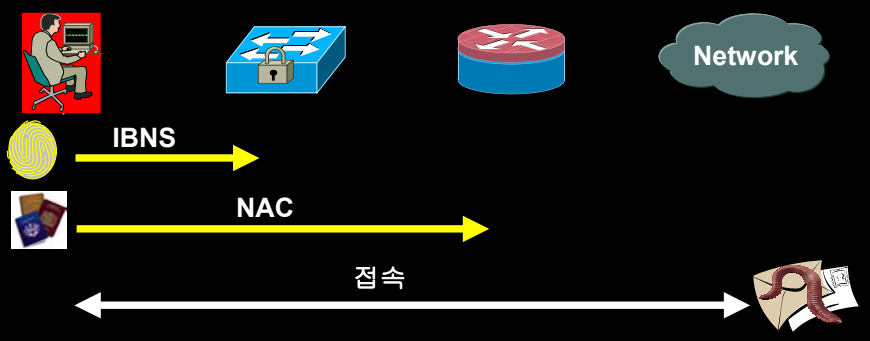
Cisco.com

- 지방 사무소
  - Focus first on less trusted/managed offices
- 익스트라넷
  - Partner hosts are patched and comply
- 인터넷
  - Ensure hosts are hardened prior to browsing
- 랩 환경
  - Production network access only for compliant devices
- 데이터 센터 보호
  - Devices accessing protected servers must comply



사용자 호스트 침입 차단 – CSA (Cisco Secure Agent)

사용자 인증, 장비 상태 인증 그리고…

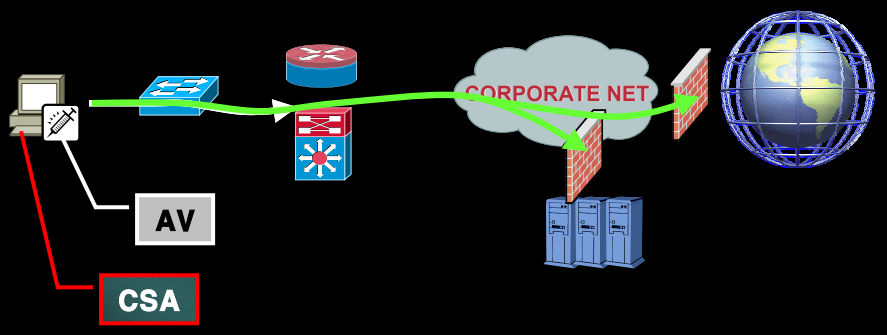


- 인증된 사용자가
- 적절한 보안 상태의 End Device로
- 적절한 네트워크에 접속한 후에,
- 합법적 경로 (ex: email attached)로 유입된 신종 Attack (Day-Zero Attack, 즉 기존 백신이 치료할 수 없는 공격)은 어떻게 방어할 수 있을까요?

사용자 호스트 침입 차단 - CSA

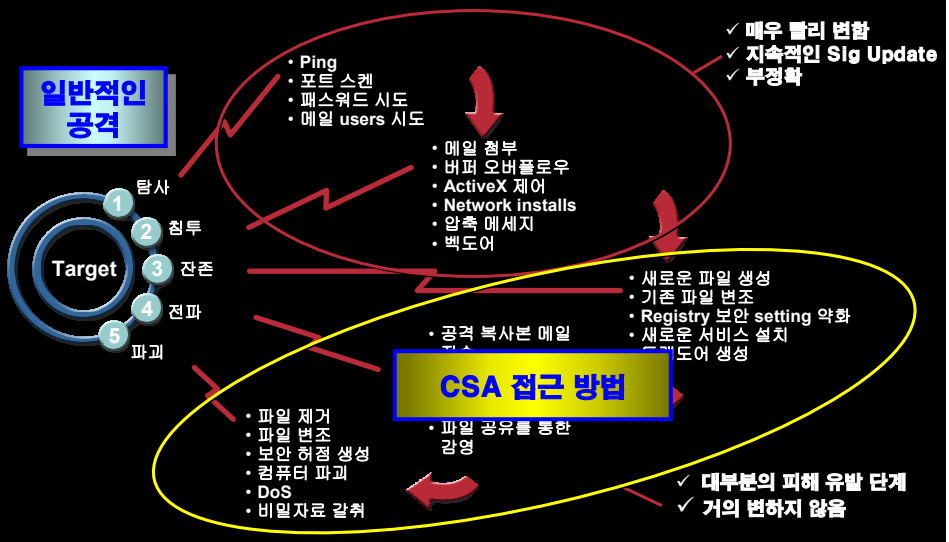
Cisco.com

- **CSA** (Cisco Security Agent)는 호스트나 서버에서의 유해 활동을 **행위 기반 기술로** 차단해주는 보안 Agent입니다.



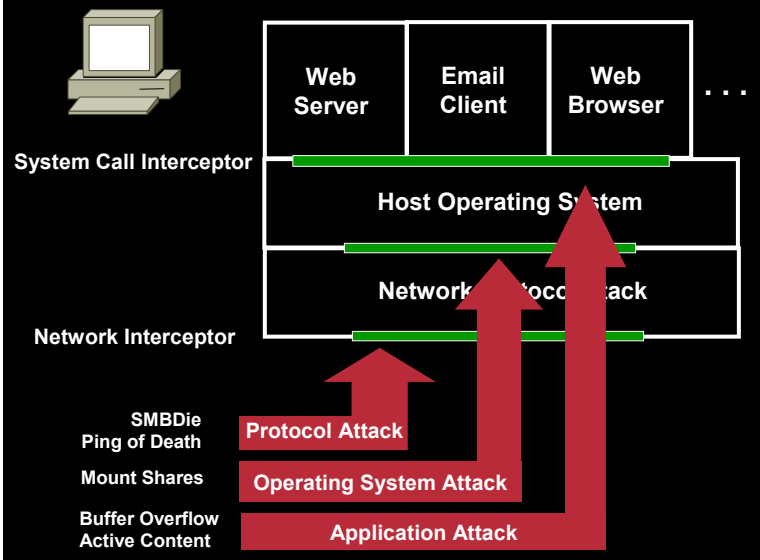
CSA 의 행위 기반의 공격 차단 원리

Cisco.com



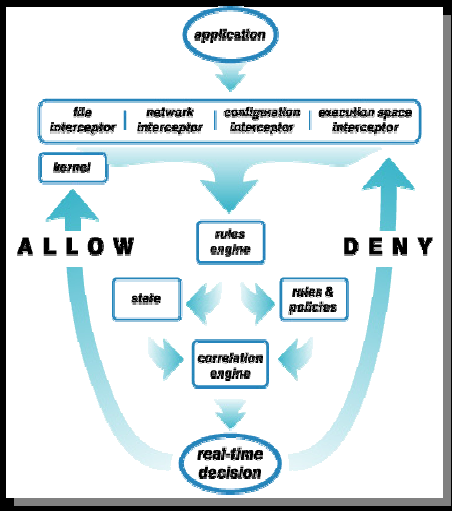
CSA (Cisco Security Agent)

Cisco.com



CSA (Cisco Security Agent)

Cisco.com

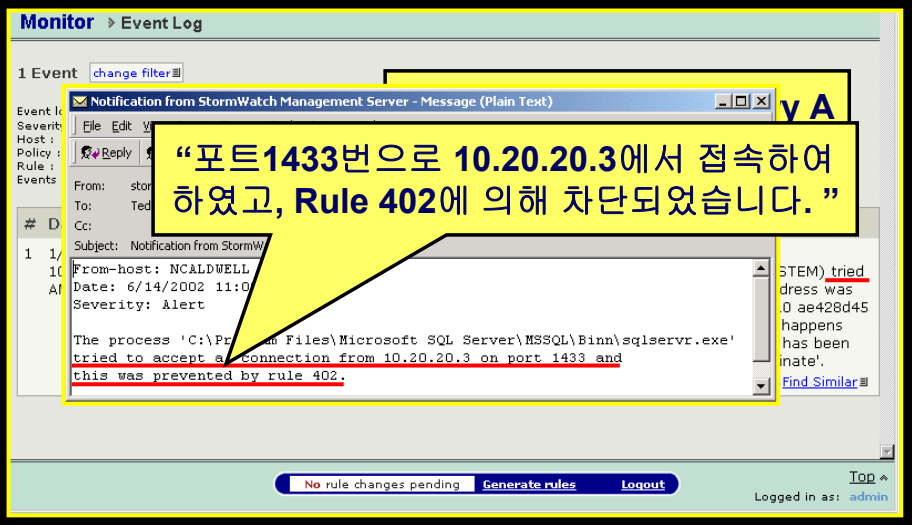


INCORE security technology

- **IN**tercept OS calls
- **CO**rrelate system calls
- **R**ules **E**ngine

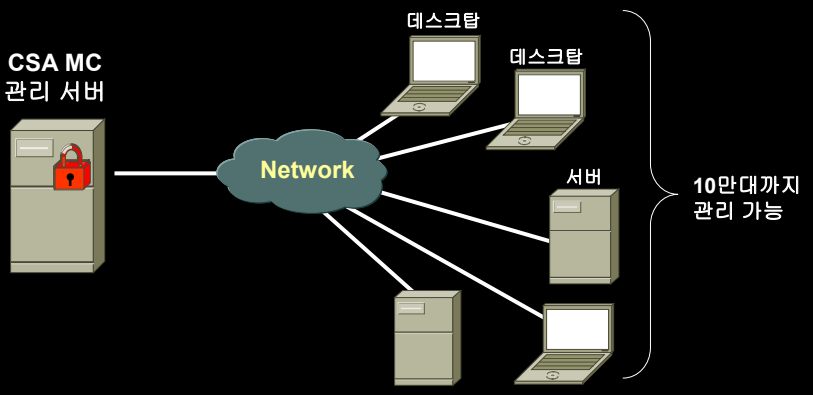
CSA 작동 예: Slammer 방어

Cisco.com



CSA 구성과 상호 연동

Cisco.com



CSA MC 지원 플랫폼: Window 2000 서버

CSA Agent 지원 플랫폼: NT, Win2K, XP, XP SP2, Win 2003 서버,Solaris 2.8
Win Cluster*,Redhat Enterprise Linux3.0* XP Home edition*

*주: CSA4.5기반으로 Dec,CY04에서 지원

CSA의 장점

Cisco.com

기존 호스트 방어 솔루션	Cisco Security Agent는...
Unknown공격 방어 한계	Unknown 공격 방어 가능
지속적인 Signature Update 필요	Zero Update
개별 방어 제품별 개별 관리 필요	All in One 과 자동 중앙 관리 HIPS+FW+OS lockdown

CSA와 Anti-Virus는 상호 보완적

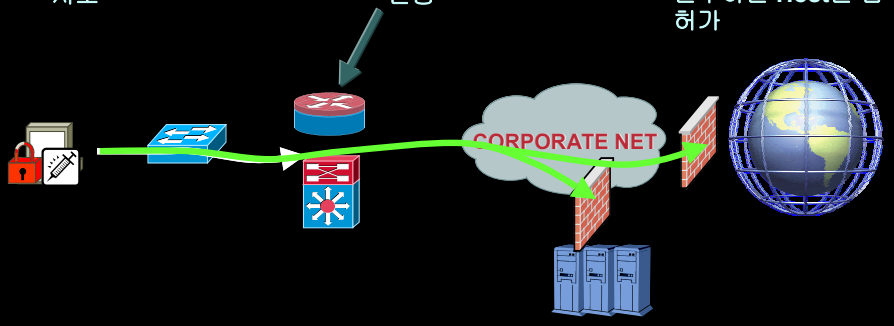
Cisco.com

	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	

시스코 NAC + CSA 솔루션의 구성

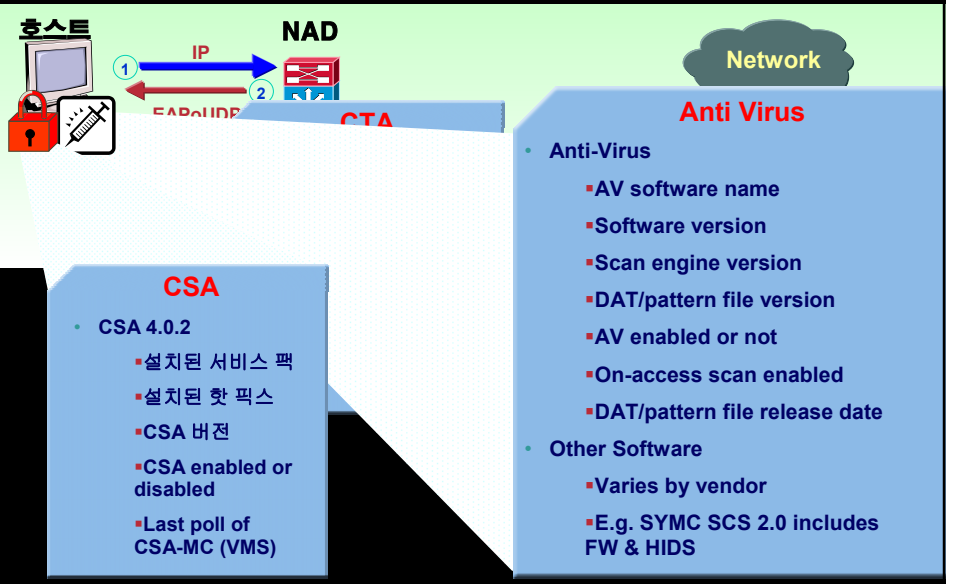
Cisco.com

1. Host의 네트워크 접속 시도
2. Host의 보안 상태 인증
3. 설정된 보안 기준을 준수하는 Host는 접속 허가

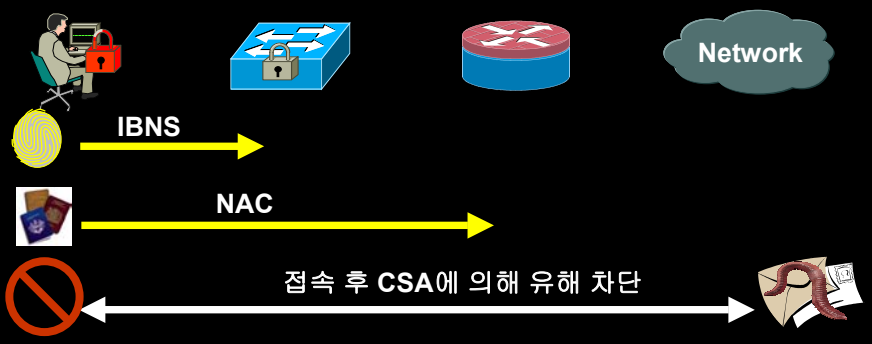


시스코 NAC + CSA 솔루션의 구성

Cisco.com



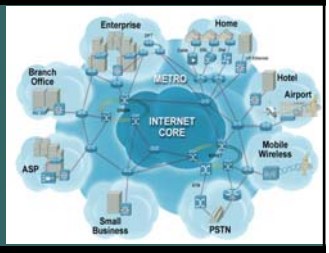
시스코 사용자 보안 Summary



Cisco 사용자 보안 솔루션은:

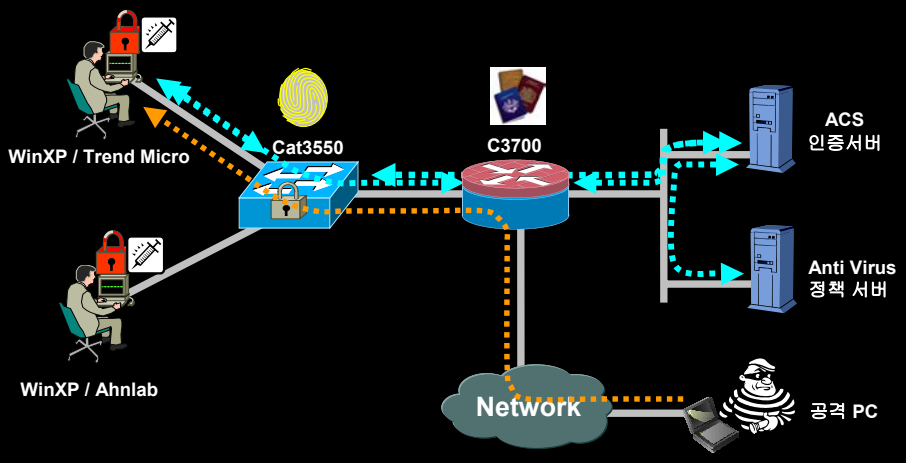
- **인증된 사용자와**
- **적절한 보안 상태의 사용자 호스트로 허용된 네트워크만 접속하며,**
- **행위 기반의 보안 Agent로 Day-Zero Attack까지 효율적으로 방어 관리 할 수 있는 솔루션입니다.**

DEMO



시스코 사용자 보안 데모 구성

Cisco.com



CISCO SYSTEMS