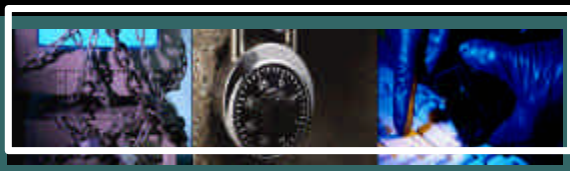
# 캠퍼스 네트워크 보안

**Cisco Systems Korea**
**Commercial Lob**
**System Engineer**

**최 우 형 (whchoi@cisco.com)**





## 캠퍼스 네트워크 보안

- 캠퍼스 네트워크 보안현재와 미래
- 캠퍼스 네트워크 라우터 보안
- 캠퍼스 네트워크 스위치 보안
- 시스코 캠퍼스 지능형 네트워크 보안
- 안전한 캠퍼스 네트워크를 꿈꾸며

# 캠퍼스 네트워크 보안 현재와 미래



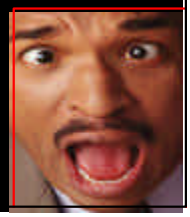
# 캠퍼스 네트워크 보안 사고 유형 속성별 특징

Cisco.com

| | | |
|---|---|---|
| 지역별 특성 |  | 대학(공대,기숙사), 기업(일반 근로자 근무지) 중심으로 광범위한 유해 트래픽 분포 |
| 구성원 특성 |  | 기숙사 구성원, 모바일 유저들에 대한 억제책 부족으로 인한 사고… |
| 사고 특성 |  | P2P로 인한 대역폭 점유<br>트로이 목마, DoS 공격으로 인한 영향 |
| 대처 특성 |  | 캠퍼스 특성상 억제 정책 부족…<br>구성원 관리 방안 부재… |

## 캠퍼스 네트워크 보안 사고 유형
## 유형별 특징

Worm
DDoS
Adware
음악파일 자료 공유
동영상 자료 공유
Virus
BHO
Spyware
Trojan
Bot Attack
Spam



## 캠퍼스 네트워크 보안 사고 유형
## 유형별 특징

| 유해 Traffic 발생 유형 | | | |
|---|---|---|---|
| | Virus<br>BHO<br>Spam<br>Spyware<br>Adware | Worm<br>DDoS<br>Trojan<br>Bot Attack | 음악파일 자료 공유<br>동영상 자료 공유 |
| 주 피해 시스템 | 일반 사용자 | 네트워크 장비, 보안 장비 | 보안 장비, 라우터 |
| 주요 증상 | PC 자원의 급격한 고갈 증상<br>인터넷 로딩 속도 현저히 저하 | 아상 패킷 발생으로 인한<br>네트워크,보안 장비 장애 | Session 폭주 → 시스템 Down<br>인터넷 대역폭 잠식 |
| 현재 대처 방안 | 사용자의 지속적인 백신 업데이트<br>꾸준한 OS 패치 | 보안장비 증설<br>기본 Packet Filtering | 대역폭 강제 억제 또는 사용금지 |

## 유해 Traffic의 올바른 이해
## P2P의 특징

Cisco.com

대역폭 잠식

pruna 파일구리

◆ 대역폭 점유 - 과도한 Traffic 사용 점유
◆ Proxy Server 로의 우회 기법, Port 변경을 통한 우회기법

Network 자원위협

soribada

Harness the power of 2000 electronic donkeys!

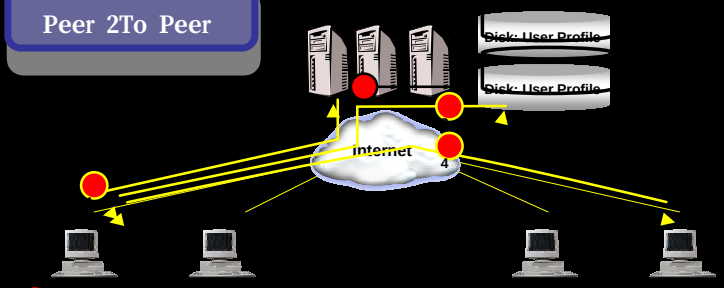
◆ 세션의 과도한 사용 – 보안 장비,Load분산 장비에 부하
◆ Proxy Server 로의 우회기법,Port변경을 통한 우회기법

7

## P2P에 대한 올바른 이해
## 중앙 서버 집중 방식 - 냅스터

Cisco.com

Peer 2To Peer

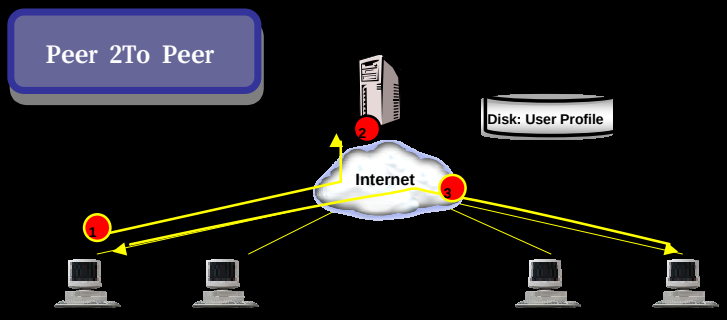



중앙 P2P Server로 사용자 인증 시도
자신의 Profile DB로 Upload – 자료 List 및 위치 등에 관한 정보 저장
원하는 자료 검색 시도 → 중앙 P2P Server 의 DB자료 검색 → 결과물을 사용자에게 전송
결과물을 가지고 있는 P2P사용자와 직접 접속 후 자료 로딩 시작

캠퍼스 인터넷 대역폭 잠식의 주원인 !!!

## P2P에 대한 올바른 이해
## Hybrid P2P 방식 - 소리바다

Cisco.com




1. 중앙 P2P Server로 사용자 인증 시도
2. 자신의 Profile DB로 Upload – 자료 List 및 위치 등에 관한 정보 저장
3. 원하는 자료 검색 시도 → 접속한 모든 사용자에게 검색 요청 → 응답 → 원하는 데이터 자료 로딩

보안장비 Session 과부하, NAT 부하, 부하 분산 장비 부하 원인 !!!



## 유해 Traffic의 올바른 이해
## 각종 침해 사고 Tool - 상반기 주요 악성 Code

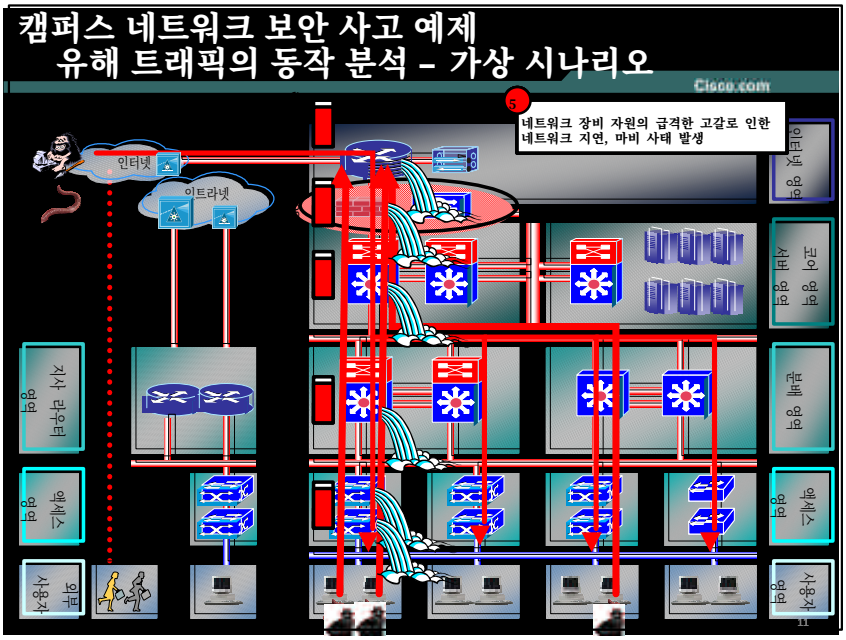
Cisco.com

1. Bagle
2. Netsky
3. Agobot
4. Blaster
5. Mydoom
6. Welchia

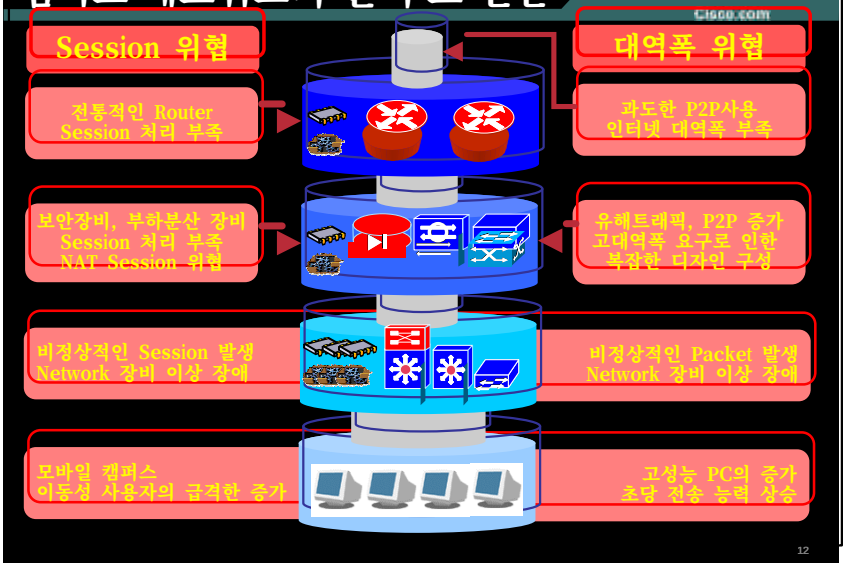
- Bagle – port 6667
- 변종 O – Port 2556
- 변종 P – port 81, 2556
- 변종 Q,R,S – 81, 2556
- 변종 X - 2535

- Port 135 – MS RPC
- Port 445 – SMB
- Port 139 – Netbios
- Port 25 – SMTP
- Port 554 – RTSP
- Port 1433 – SQL
- Port 80 – HTTP
- Port 901 – samba-swat
- Port 21 – FTP
- Port 110 – POP3

# 캠퍼스 네트워크 보안 사고 예제
## 유해 트래픽의 동작 분석 – 가상 시나리오




# 캠퍼스 네트워크의 현 주소 진단



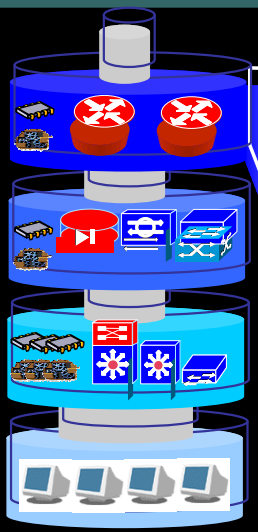
# 캠퍼스 네트워크 라우터 보안

Security Zone 외부에 구성되는 Router의 보안이 반드시 필요합니다 !!!



# 라우터 보안의 현재

Cisco.com



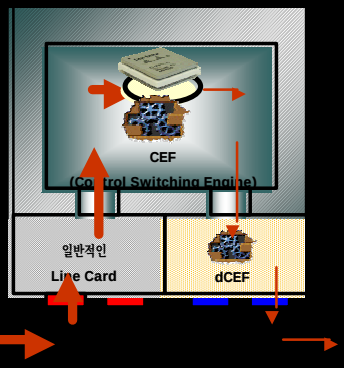
1. 비대칭 대역폭 구조
   유해 트래픽으로 인한 대역폭 부족 현상
   차별화된 트래픽 분류 필요성 대두
2. 라우터의 Security Zone 외부 설치 구성 일반화
   Metro Ethernet 등 다양한 인터넷 접속 구조
   발생으로 인한 Switch 대체 수요
   → 일반적 Switch로는 보안 기능 적용 불가
3. 라우터의 보안 기능성 요구 대두
   → 라우터 보안 모듈, 보안 IOS 등장.

❖ 내,외부로 부터의 위협에 견고히 견딜 수 있는
**지능형 라우터** 요구 !!!

# 라우터 CPU 보호를 위한 기술

Cisco.com

## Router 구조- CPP




CPP(Control Plane Policing)을 통한 유해 트래픽 제어 기법

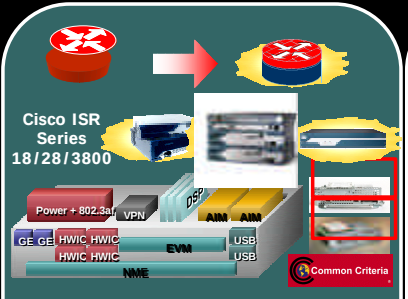
### CPP (Control Plane Policing) 구성 예제

```
##Access-list 작성##
Router(config)# access-list 141 permit icmp any any
                    port-unreachable

##Class-Map 작성##
Router(config)# class-map icmp-class
Router(config-cmap)# match access-group 141

##Policy-Map 작성##
Router(config)# policy-map control-plane-out-policy
Router(config-pmap)# class icmp-class
Router(config-pmap-c)#
          police rate 1500000 pps bc 500000 packets

##Control Plane 에 적용##
Router(config)# control-plane
Router(config-cp)# service-policy output
                        control-plane-policy
```



# 시스코 지능형 보안 라우터로의 진화

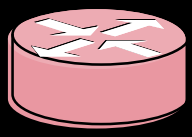
Cisco.com




1. 인증 기술 지원 – NAC(네트워크 허가 제어 기술) 802.1x 기반의 인증
2. 외부 위협으로 부터의 방어 기술 지원
   - IPS Module, 네트워크 분석 모듈(Netflow), IOS F.W
3. 안전한 접속 기술 – H.W 기반의 VPN 접속
4. 네트워크 기반 보호 기술
   - CPP(CPU 보호 기술), NBAR, Auto-Secure

# 캠퍼스 네트워크 라우터 운영 가이드

Cisco.com

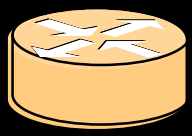


**1. 보안 가이드**

Access-list를 Compact 하게 사용 – Turbo ACL, ACL Summary
다양한 ACL 구현을 통한 유연한 정책을 구현 – Time,Reflect ACL
RFC 1918 Filtering, uRPF를 통한 변조된 IP Filtering
Netflow의 적극 활용 권고

**2. QoS 가이드**

Time ACL과의 연동을 통한 시간대별 유연한 QoS 구성 – CAR, CBWFQ
NBAR는 CPU 사용량에 따라서 적절하게 사용



**3. 성능 가이드**

Router의 용량의 백본 스위치에 준하는 용량으로 설계.
라우터 전위에 또 다른 네트워크 장비 설치 지양. – 성능 감소 우려…

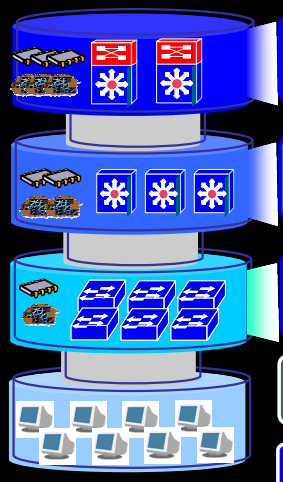


# 캠퍼스 네트워크 스위치 보안

내부 사용자의 공격에 대한 방어는 IDS/IPS로 모두 해결 할 수 없습니다.

# 캠퍼스 스위치 보안 기능 구현

Cisco.com



- uRPF 기법을 통한 IP 변조 방지 정책
- QoS를 통한 대역폭 강제 조절 정책
- DHCP 서버의 보호
- CPU Rate Limit을 통한 장비의 보호

- DAI,IP source Guard 기법을 통한 IP변조 방지
- QoS를 통한 대역폭 강제 조절
- DHCP 서버의 보호
- 다양한 ACL 정책 적용

- Port Security – MAC addres 유일 강제 억제
- VACL을 통한 동일 Subnet 간의 특정 포트 차단 정책

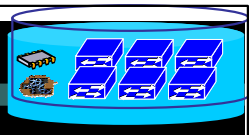
CIST 제공

(Catalyst Integrity Security Toolkit)

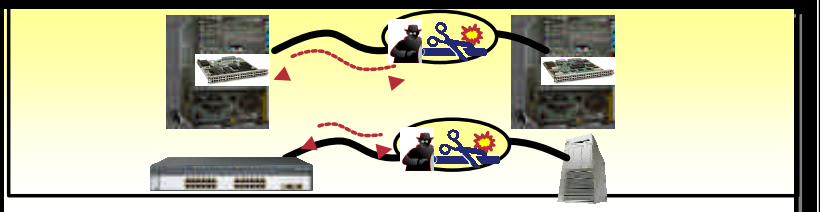
Dynamic ARP Inspection | DHCP Snooping | IP Source Guard

19

# 캠퍼스 네트워크 스위치 보안
# TDR을 통한 UTP Cable 단절 사고 대처



TDR (Time Delay Reflectometer) 기능



캠퍼스 내 잦은 전기, 시설 공사로 인한 UTP Cable 단절 사고 대비
TDR 기능을 통한 Cable 단절에 대한 빠른 대처 가능 !!!

20


캠퍼스 스위치 보안 기능 구현
MAC filtering – 공격자 Filtering 기술
공격자 MAC 제어 기술 :
Mac Filtering 기술/ Port Security
STOP
-특정 MAC Filtering 기술-
x.4444 MAC Filtering 설정
-Port 당 최대 MAC 숫자 정의-
Maximum xx 개
21

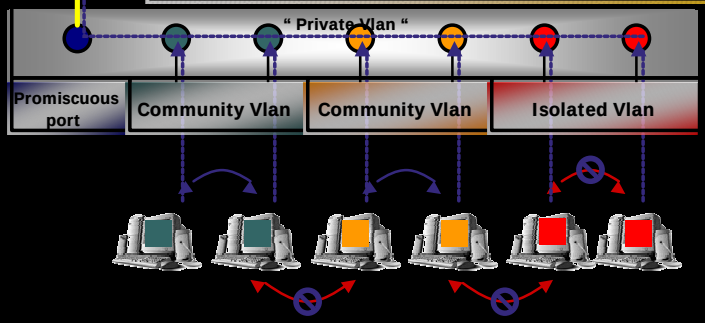

캠퍼스 스위치 보안 기능 구현
Multi/Broadcast Flooding 방어
Multi/Broadcast Flooding 제어 기술 : Storm Control - IOS
M
Uni/Multi/Broadcast억제
(B/W 대비 Percent 비율)
대량의 Multicast, Broadcast 전송시 제어 대책에 필수 !!!
22

# 캠퍼스 스위치 보안 기능 구현
## PVLAN – Snooping 방지 대책

Snooping 방지 : Private Vlan

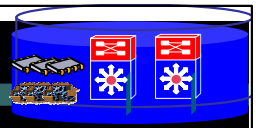
Private Vlan : 동일 Vlan 내부에서의 불필요한 Traffic 제어

1. Community Vlan : C-vlan 간 Host만 통신이 가능
2. Isolated Vlan : I-Vlan 간 Host도 통신 불가
3. Promiscuous Port : 모든 Pvlan Host는 P-port를 통한 외부 통신 가능

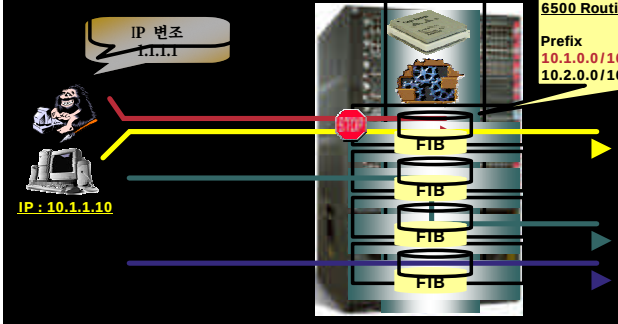





# 캠퍼스 스위치 보안 기능 구현
## uRPF – IP 변조 방지



IP 변조 방지 기능 : uRPF(Unicast Reverse Path Forwarding)



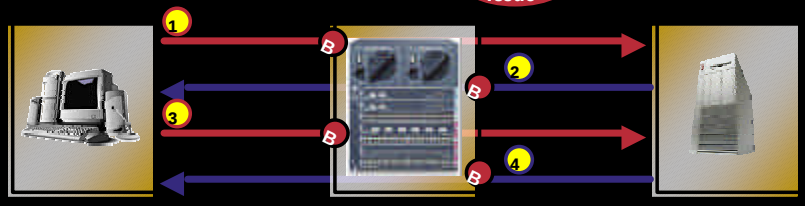

6500 Routing Table (FIB)

| Prefix | Next Hop | Interface |
|---|---|---|
| 10.1.0.0/16 | 10.1.1.1 | gig 1/1 |
| 10.2.0.0/16 | 10.2.1.1 | gig 1/2 |

# 캠퍼스 스위치 보안 기능 구현
## DHCP 위협 요소...

### DHCP 동작 원리의 이해

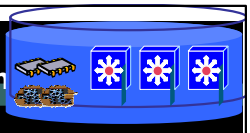
Broadcast Issue




1. IP Lease Request → DHCP Discover 메시지를 Broadcast 형식으로 뿌린다.
2. IP Lease Offer → DHCP Discover 메시지를 받은 서버는 응답을 Discover Offer 메시지로 Broadcast 응답한다. (Client MAC,할당될 IP 주소, 서브넷, Lease 기간, Server 식별자 IP 포함)
3. IP Lease Selection → DHCP Request로 서버에게 Broadcast 응답( Server 식별자 IP, Client IP 포함)
4. IP Lease Ack → DHCP Request 받은 서버는 DHCP ACK 를 Broadcast 발송



# 캠퍼스 스위치 보안 기능 구현
## DHCP Request Flooding – DHCP Snoopin



### DHCP request Flooding 공격 방어 : DHCP snooping rate Limit 기능

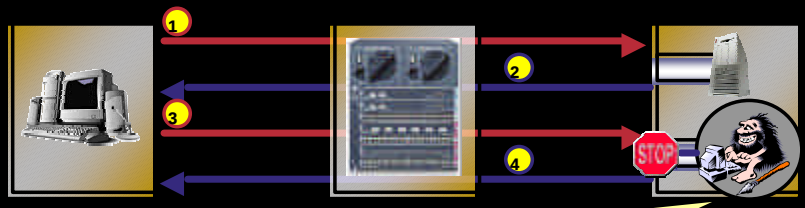

DHCP Scope Size 전체에 IP 할당을 요청하여, DHCP Server 과부하 발생 시킴

- DHCP Request Flooding 공격 방어 구성 예제.

```
Switch(config)# ip dhcp snooping      → DHCP Snooping enable
Switch(config)# ip dhcp snooping vlan 10    → DHCP Snooping 적용 Vlan 정의
Switch(config-if)# ip dhcp snooping limit rate 100(pps)   → DHCP Request 허용 수치 제한
```

# 캠퍼스 스위치 보안 기능 구현
## DHCP Request Flooding – DHCP Snoopin

DHCP Server 위조 공격 방어 : DHCP snooping Trust 기능




DHCP Request 에 대해, 공격자가 거짓된 정보를 전달함…

❖ DHCP Request Flooding 공격 방어 구성 예제.

```
Switch(config)# ip dhcp snooping        → DHCP Snooping enable
Switch(config)# ip dhcp snooping vlan 10    → DHCP Snooping 적용 Vlan 정의
Switch(config-if)# ip dhcp snooping trust→ DHCP discover, request 등 메시지를 해당 Port만 수용
```



# 캠퍼스 스위치 보안 기능 구현
## MAC 변조 방지 기능 – Dynamic ARP Inspection

DHCP Snooping을 통한 MAC 변조 방지 기능 – ARP Inspection


DHCP Snooping 을 통해 기록된 정보 조회…

| MacAddress | IpAddress | Lease(sec) | Type | VLAN | Interface |
|---|---|---|---|---|---|
| 01.01.01.11 | 1.1.1.11 | 4995 | dhcp-snooping | 1 | FastEthernet3/4 |

# 캠퍼스 스위치 보안 기능 구현
# IP 변조 방지 기능 – IP Source Guard

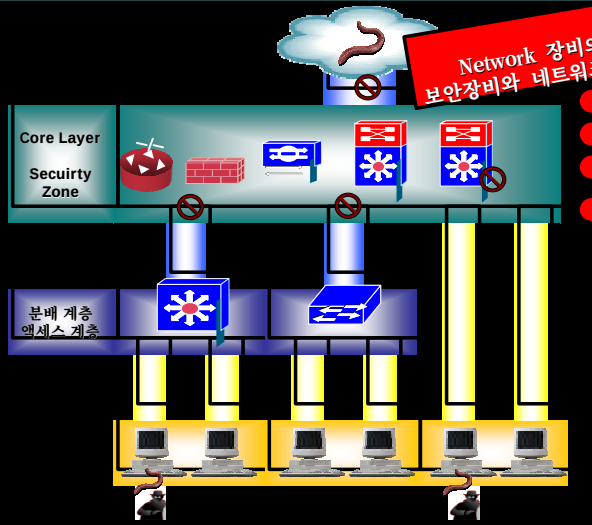
DHCP Snooping을 통한 IP 변조 방지 기능 – IP Source Guard


DHCP Snooping 을 통해 기록된 정보 조회…

| MacAddress | IpAddress | Lease(sec) | Type | VLAN | Interface |
|---|---|---|---|---|---|
| 01..01.01.11 | 1.1.1.11 | 4995 | dhcp-snooping | 1 | FastEthernet3/4 |



# 특정 Port를 통한 Worm 전이 과정의 이해



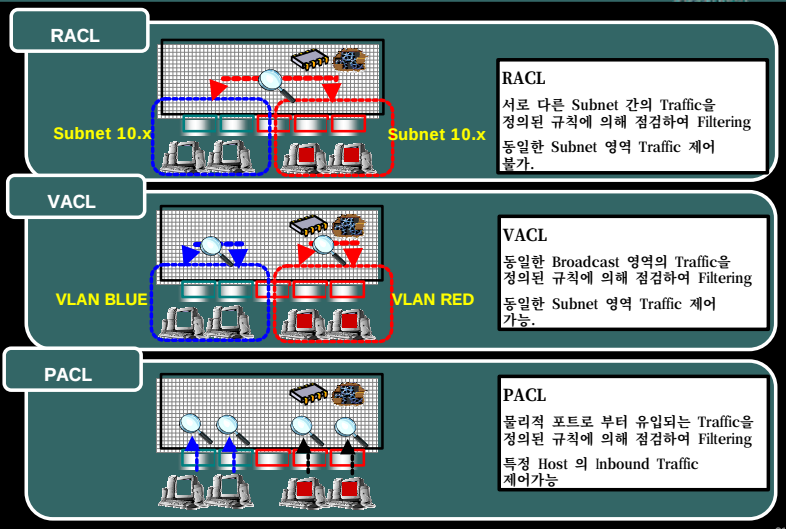

Network 장비의 보안 기능 요구
보안장비와 네트워크 장비간의 연동 요구

- Internet을 통한 웜 유입
- 내부 감염자를 통한 Worm 전이
- 웜 전이 방지를 위한 ACL 작성을 통한 Service port 차단
- 할당 Vlan/Broadcasting Domain 에서의 지속적인 전이 현상 …

같은 Subnet/Vlan 에서 퍼지는 Worm을 막을 수 있는 방법이 없다…

# 캠퍼스 스위치 보안 기능 구현
## ACL 의 이해

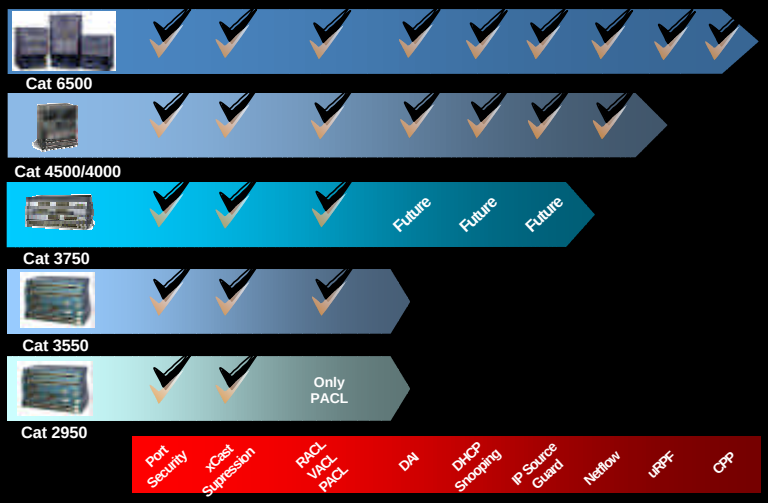
Cisco.com




31

# Catalyst Security Function Matrix
## 시스코 스위치 제품군 별 보안 기능

Cisco.com



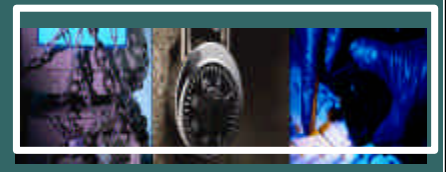

32

# Cisco Catalyst Switch 보안 구성
## 위협요소에 대한 시스코 스위치의 방어 전략

Cisco.com

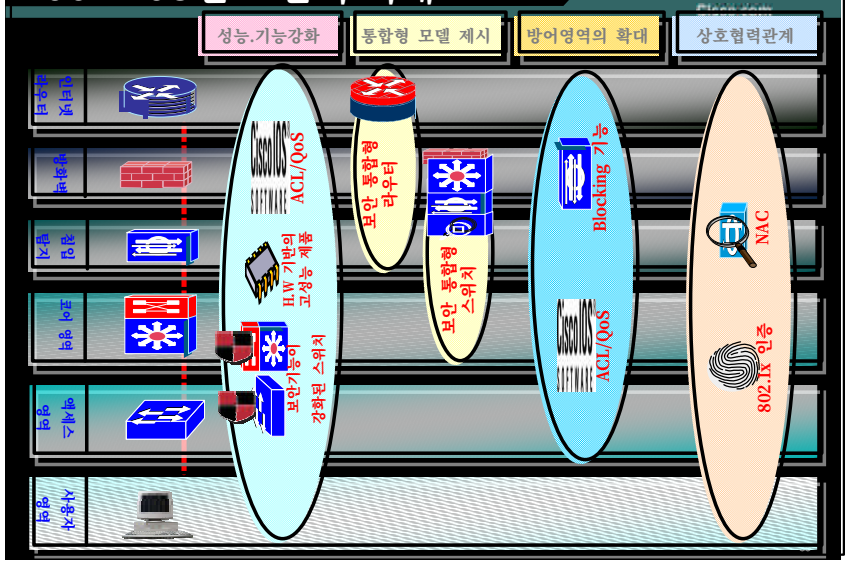

33

# 시스코
# 캠퍼스 네트워크
# 지능형 보안



End to End의 통합 지능형 보안 네트워크 만이 안전한 네크워크를 만들 수 있습니다.

# 2004~05년 보안의 미래

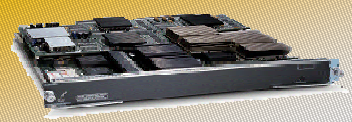



# 캠퍼스 지능형 방화벽 모듈

7600Router / Catalyst 6500 방화벽 모듈

모듈당 5Gbps – 최대 20Gbps 대용량 방화벽

Cisco FWSM Module 기능 및 성능



Performance

- PIX 6.0 base Feature Set (some feature of 6.2 )
- High Performance Firewall, targeted OC48 or 5GB (aggregated)
- Concurrent connections : 1M
- 3 Million pps

FWSM

- 100K new connections/sec for HTTP, DNS and enhanced SMTP
- 100 VLAN 지원
- LAN failover active/standby
- Dynamic Routing i.e. OSPF
- 단일 샤시 내 multiple blades 지원
- 128K Rule Set 지원
- No IDS Signatures
- Supported on Native IOS and CatOS ( IOS12.1(13)E / Cat OS 7.5(1))
- Classic 32G bus/Fabric 256G bus

# 캠퍼스 지능형 방화벽 모듈 소개

Cisco.com

*Version 1.1.3*

Active X Blocking
Cut Through proxy
DNS Guard
Failover
Flood Defender
Flood Guard
Fragmentation Guard
Fragmentation virtual reassembly
FTP and URL Logging
Support Multimedia protocols
Mail Guard
NAT/PAT
NETBIOS over IP
Radius Authorisation
SSH
TCP Intercept
URL Filtering…

*Version 2.2*

Policy NAT 지원
Bidirectional NAT 지원

H.323 v3,4 지원
MGCP 지원

ACL Syslog 지원
Outbound ACL 지원

DHCP Relay 지원

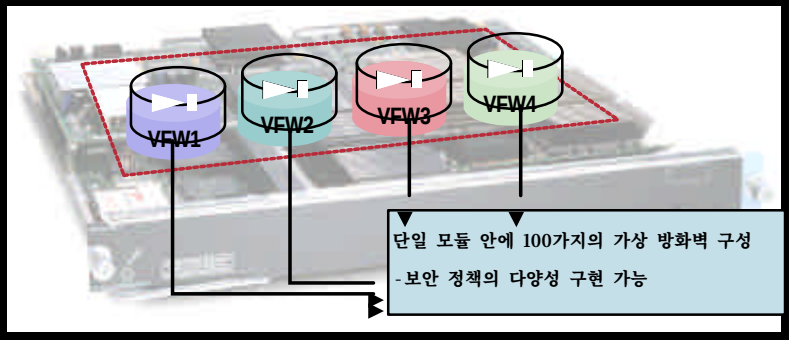
SNMP를 통한 CPU Monitoring
Interface Monitoring

Virtual Firewall 지원
Transparent/Stealth F.W 지원

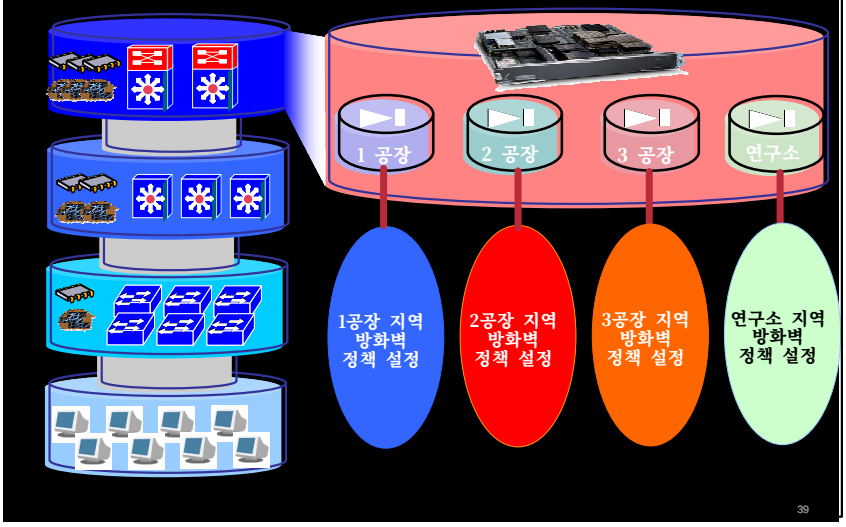


# 캠퍼스 지능형 방화벽 모듈
# – 방화벽 모듈을 통한 캠퍼스 구성 방법

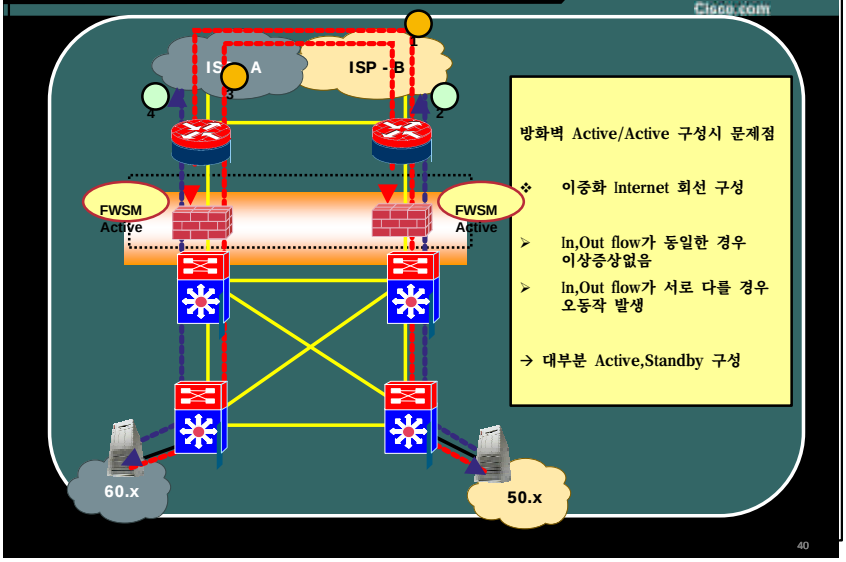
Cisco.com



## 캠퍼스 지능형 방화벽 모듈 구성 예 – 가상방화벽 구성

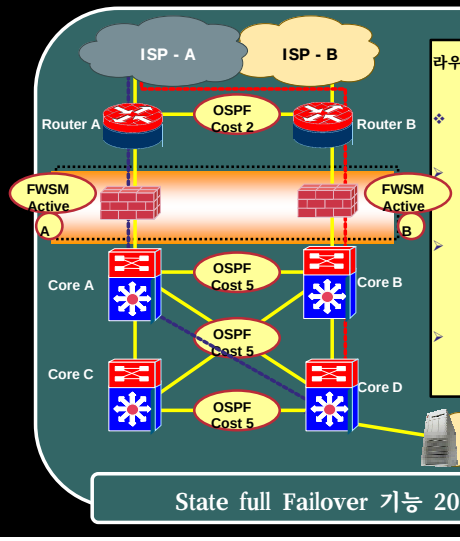



## 캠퍼스 지능형 방화벽 모듈 FWSM Active/Active 구성 시 문제점



# 캠퍼스 지능형 방화벽 모듈
# FWSM Active/Active Routing 구성 방안

Cisco.com




라우팅을 통한 Active/Active 구성 방법

- FWSM – OSPF 구동 가능
- OSPF Cost 변경을 통한 Active/Active 구성 가능
- Failover – 10Sec 이내 가능
  OSPF Hello Time 조정 시 Failover Time 단축 가능
- 주의 !!! – Routing Active/Active 구성 시 State full Failover 불가.

State full Failover 기능 2005년 1월 제공 !!!

41

# 캠퍼스 지능형 침입차단 모듈

Cisco.com


7600Router /Catalyst 6500 침입방지 모듈

침입발생시 시스코 IOS 탑재 장비와 연동 방어

❖Switch IPS – IDSM2

◆실시간 침입 탐지 감시
◆폭넓은 침입 탐지 인식 및 감시
◆확장된 침입 탐지 유형
◆다중 VLAN 탐지 기능
◆32Gb bus/ Fabric 과의 연동 구조
◆Switch 성능 저하 없는 monitoring
◆Passive Monitoring
◆Transparent Operation
◆IDSM 관리를 위한 SSL기반의 IDM 지원
◆Event 분석을 위한 IEV 지원
◆라우터,스위치,방화벽 제품 군과의 연동
◆Cat OS 7.5(1)/IOS 12.1(19)E 이상 지원

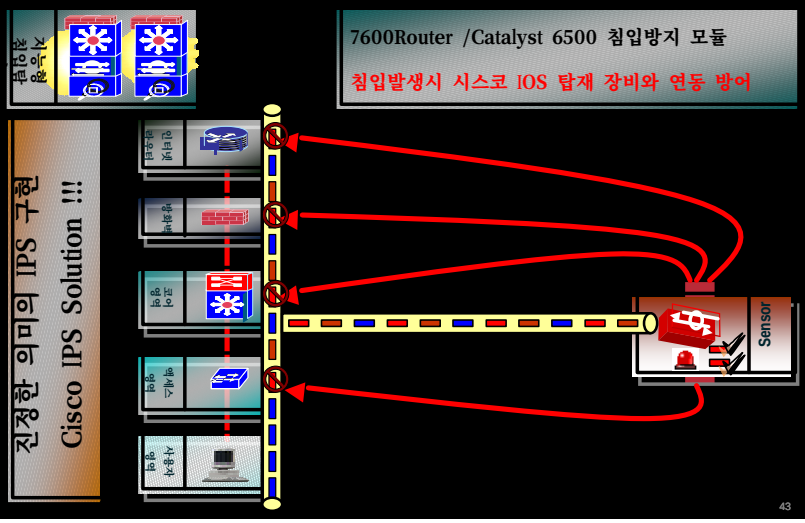
❖강력한 성능

◆ 600Mbps 높은 성능
◆ 5000 cps(초당 TCP 처리 수)
◆ HTTP Transaction 5000 TPS
◆ 동시 접속 수 최대 500,000 개

42

## 캠퍼스 지능형 침입차단 모듈
## 네트워크 장비와 연동이 가능한 지능형 침입탐지

Cisco.com




43

## Cisco IDS의 Signature 대폭 강화 !!!

Cisco.com

Trend Micro와 Cisco의 심도깊은 Signature 제공

| | Cisco | | Trend Micro |
|---|---|---|---|
| Core Focus | Worms | + | Viruses |
| Signature Type | Vulnerability | | Exploit |
| Nature of Threat | Slow Mutation | | Rapid Mutation |
| Examples | Code Red, Nimda | | Bagle, Netsky |

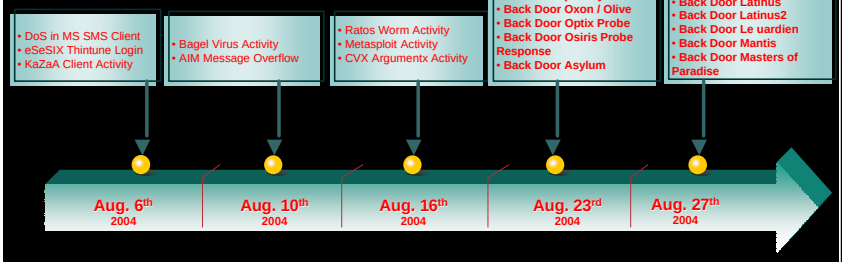
44

# Cisco IDS의 고지능 변화

Cisco.com

백신회사와의 상호협력관계

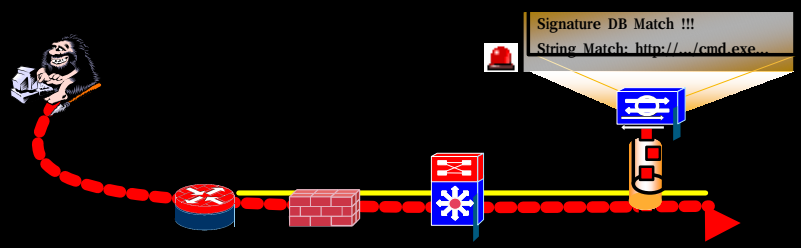
Cisco IDS → Cisco IPS→
Cisco Virus Wall 진화






# IDS의 새로운 Trend
# 기존 IDS 동작 방식 – Signature Based

Cisco.com




String Match: http get … ./cmd.exe… . 를 통한 유해 Traffic 유입

Signature (Misused) Based IDS

◆ Capture 된 Packet과 알려진 Attack, Worm, Virus, 취약점 등으로 이미 정의된 Signature DB와 비교하여 유해 트래픽을 검출하는 방식

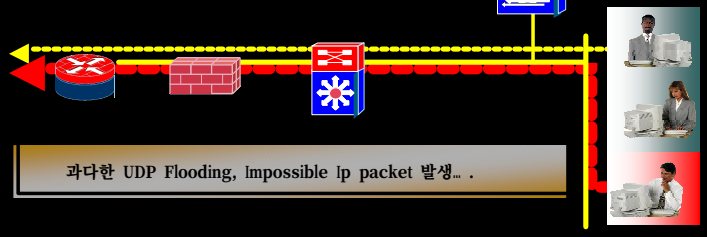
◆ 가장 대표적인 방식으로 현재 IDS 방식의 대부분이 이 방식을 기본으로 하고 있음.

# IDS의 새로운 Trend
# 시장에서 요구되어지는 Anomaly Based IPS

Cisco.com

시장에서 점점 더 요구되어지는
Anomaly Detection IDS

예상치 않은 과다 UDP Packet 유입
정의 되지 않은 IP Packet 유입



과다한 UDP Flooding, Impossible Ip packet 발생… .

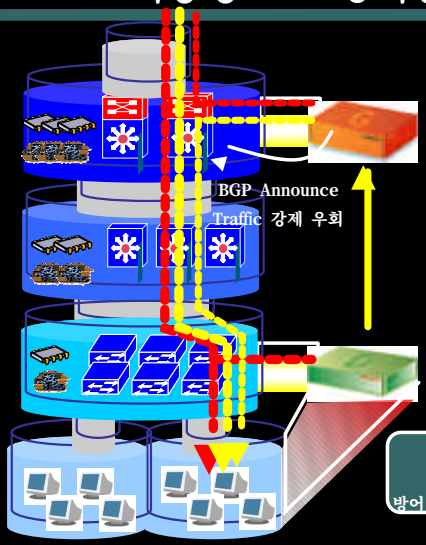
**Anomaly Based IDS**

- ◆ Statistical vs non-Statistical : 정상적인 Traffic에 대한 상황과 비정상적인 상황에 대한 능동적인 대처 가능
- ◆ 정의 되지 않은 공격 유형에 대한 능동적 탐지 수행



# Cisco 지능형 DoS 방지용 Anomaly IPS

Cisco.com




공격 성향의 Traffic에 대한 감사 수행

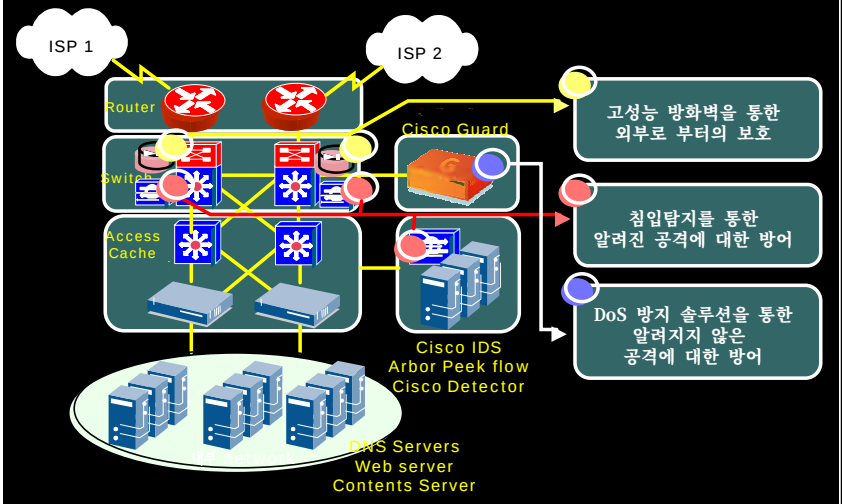
Guard=DDoS Mitigation 을 위한 통보

특정 구역에 대한 모니터링
> DDoS Detection

불특정 다수의 외부로 부터의 공격에
방어 솔루션 제공 – 국내 포털 사이트, 서버팜 보호

# 캠퍼스 네트워크의 심도깊은 보안 디자인
## - F.W , IDS, DoS 방지 솔루션

Cisco.com



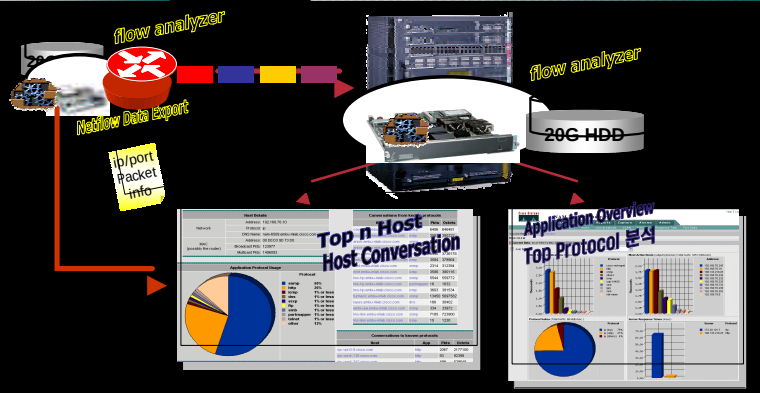



# 캠퍼스 지능형 분석 모듈

Cisco.com

7600Router /Catalyst 6500 네트워크 분석 모듈

Traffic 정밀 분석, 리포팅 제공



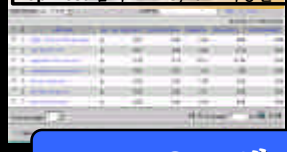
# 캠퍼스 지능형 분석 모듈

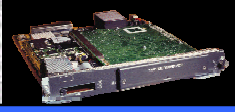
Cisco.com


7600Router /Catalyst 6500 네트워크 분석 모듈

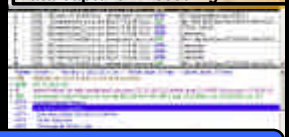
Traffic 정밀 분석, 리포팅 제공

Top Host 탐지 – PPS,B/W 사용률





Data Capture - Decoding



**New S.W 발표 – URL별 분석 기능 제공 !!!**

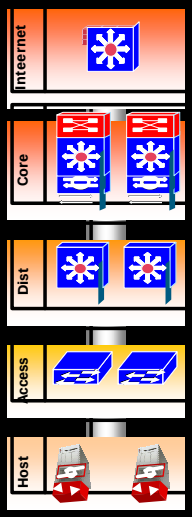
Top Application 탐지
– PPS,B/W 사용률

- Router Netflow Exporting
- 다양한 Reporting 기능
- Interface 상세 분석 기능
- Alarm 기능

51

# Service Module Case Study 1

## 7600 보안 라우터 + 6500 구성 : FWSM 1 set + IDSM 2set




Product : Cisco 7600 Router + FWSM
Internet BGP Router 전용
- FWSM Module 을 통한 고성능 방화벽 구축
- 외부로 부터의 공격자 방어 용도

Product : Cisco 6500 Switch + IDSM 2
내부 Backbone Switch 전용
- 내부 사용자 Monitoring 및 외부로 부터 웜 감염 검사
- 침입자,공격자 발견시 7600FWSM,Backbone Switch 내부 Dist Switch,Access Switch 자동 방어

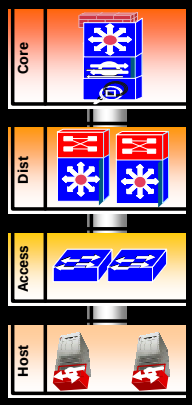
MAC 변조 방지, MAC Flooding 방어, 다양한 ACL 구성
IP 변조 방지 기술,
QoS를 통한 효과적인 Traffic 제어 기술 적용

52

# Service Module Case Study 2

## 7600보안 라우터 구성 - FWSM / IDSM / NAM 1set

Cisco.com




Product : Cisco 7600 Router + FWSM + IDSM2 + NAM 2
Internet BGP Router / Backbone Switch 겸용
•FWSM Module 을 통한 고성능 방화벽 구축
- 외부로 부터의 공격자 방어 용도
•IDSM Module을 통한 ServerFarm,내부 사용자 감시, 웜 방어
- Cisco 장비와 유기적 연동을 통한 방어 시스템 구축
•NAM Module을 통한 Traffic 변동 추이 조사
- Master Plane 작성
- Trouble Shooting 도구 활용
- Application, 사용률 분포도 조사

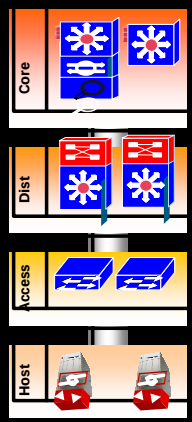
MAC 변조 방지, MAC Flooding 방어, 다양한 ACL 구성
IP 변조 방지 기술,
QoS를 통한 효과적인 Traffic 제어 기술 적용



# Service Module Case Study 3

## Failover - FWSM 2 set + IDSM 1set + NAM 1set

Cisco.com



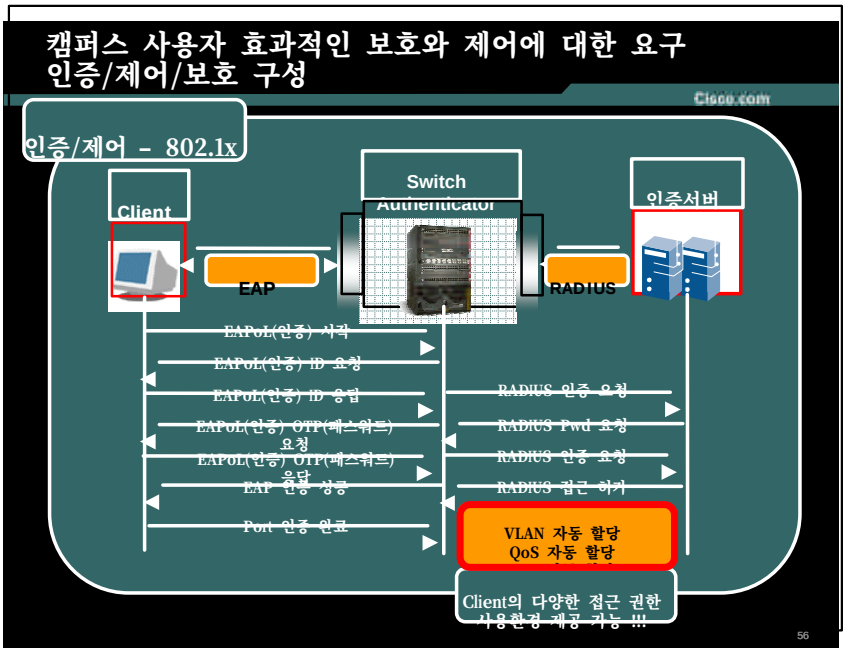

Product : Cisco 6500 + FWSM + IDSM2 + NAM 2
Internet BGP Router / Backbone Switch 겸용
•FWSM Module 을 통한 고성능 방화벽 구축
- 외부로 부터의 공격자 방어 용도
- 장애를 대비한 FWSM Failover 구성

•IDSM Module을 통한 ServerFarm,내부 사용자 감시, 웜 방어
- Cisco 장비와 유기적 연동을 통한 방어 시스템 구축

•NAM Module을 통한 Traffic 변동 추이 조사
- Master Plane 작성
- Trouble Shooting 도구 활용
- Application, 사용률 분포도 조사

MAC 변조 방지, MAC Flooding 방어, 다양한 ACL 구성
IP 변조 방지 기술,
QoS를 통한 효과적인 Traffic 제어 기술 적용


시스코 캠퍼스 지능형 모듈 요약
Cisco.com
IBM NP 4 GS3
5Gbps
방화벽 모듈
(FWSM)
Intel IXP
2Gbps
침입 방지 모듈
(IDSM2)
Intel IXP
1Gbps
네트워크 분석 모듈
(NAM2)
VPN Accelerator
2Gbps
VPN 모듈
(VPNSM)
SSL Accelerator
SSL Module (SSLM)
Gbps 급 이상의 고대역폭 확보
전용 NP를 통한 고성능 확보
55


캠퍼스 사용자 효과적인 보호와 제어에 대한 요구
인증/제어/보호 구성
Cisco.com
인증/제어 - 802.1x
Client
Switch
Authenticator
인증서버
EAP
RADIUS
EAPoL(인증) 시작
EAPoL(인증) ID 요청
EAPoL(인증) ID 응답
EAPoL(인증) OTP(패스워드) 요청
EAPoL(인증) OTP(패스워드) 응답
EAP 인증 성공
Port 인증 완료
RADIUS 인증 요청
RADIUS Pwd 요청
RADIUS 인증 승인
RADIUS 접근 허가
VLAN 자동 할당
QoS 자동 할당
Client의 다양한 접근 권한
사용환경 제공 가능 !!!
56

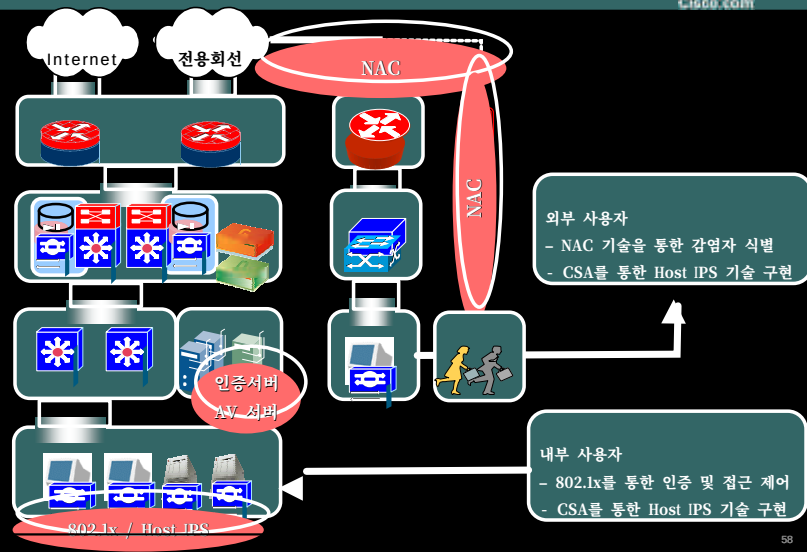
# 사용자 제어에 대한 요구
# Cisco NAC

Cisco.com

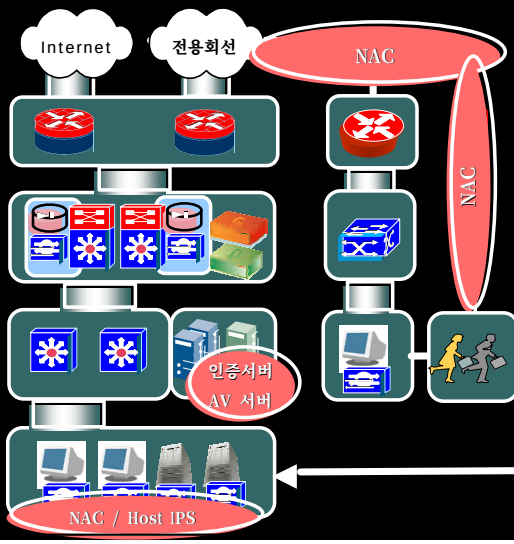



# 시스코 사용자 보호 기술
# 구성 예 – Phase I (현재)

Cisco.com

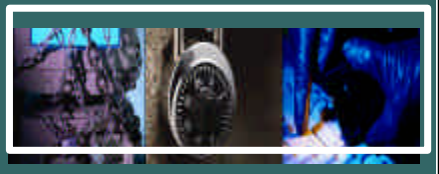


# 시스코 사용자 보호 기술
# 구성 예 – Phase II (2005년 Coming Soon)



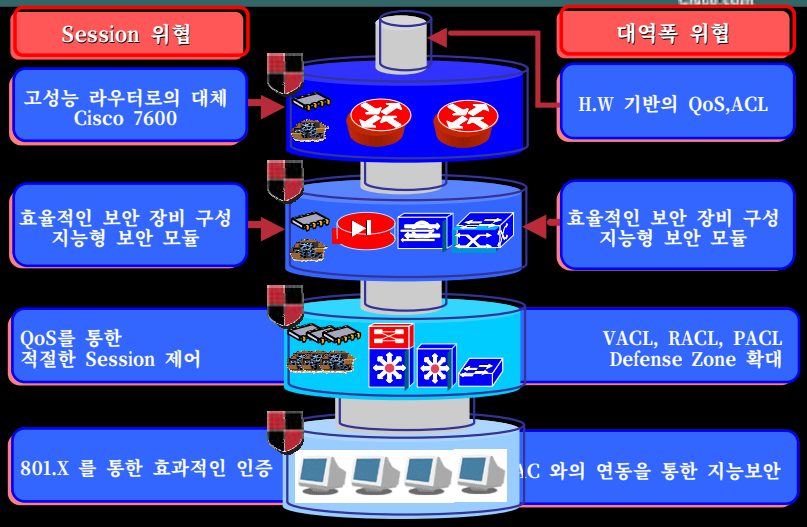



## 안전한
## 캠퍼스 네트워크
## 꿈꾸며...



# 시스코의 지능형 네트워크 보안 구성

Cisco.com




61

Cisco.com

1. 보다 안전한 Network Infra 구축을 위해 라우터 보안이 반드시 필요합니다.

2. Switch 보안 기술 구현을 통해 내부 사용자의 공격을 억제시킬 수 있습니다.

3. End to End의 지능형 보안 구현이 사용자에게 안전한 네트워크 환경을 만듭니다.

Cisco 통합 보안 라우터

Cisco 통합 보안 스위치

CISCO SYSTEMS

Cisco 지능형 보안 장비

사용자 보호 기술
802.1x / CSA / NAC

62

# 감사합니다.


# Q & A