Cisco.com

기업 네트워크 End-to-End 보안

2004년 10월 20일

Cisco Systems Korea
정희철(hlchung@cisco.com)

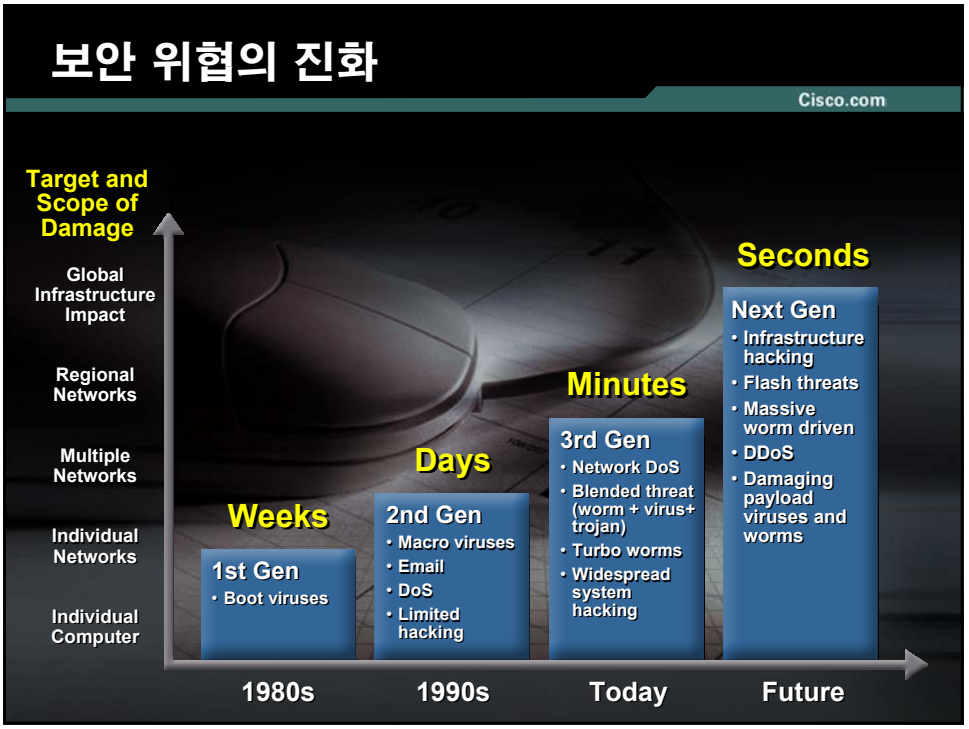
목 차

Cisco.com

네트워크 보안 동향

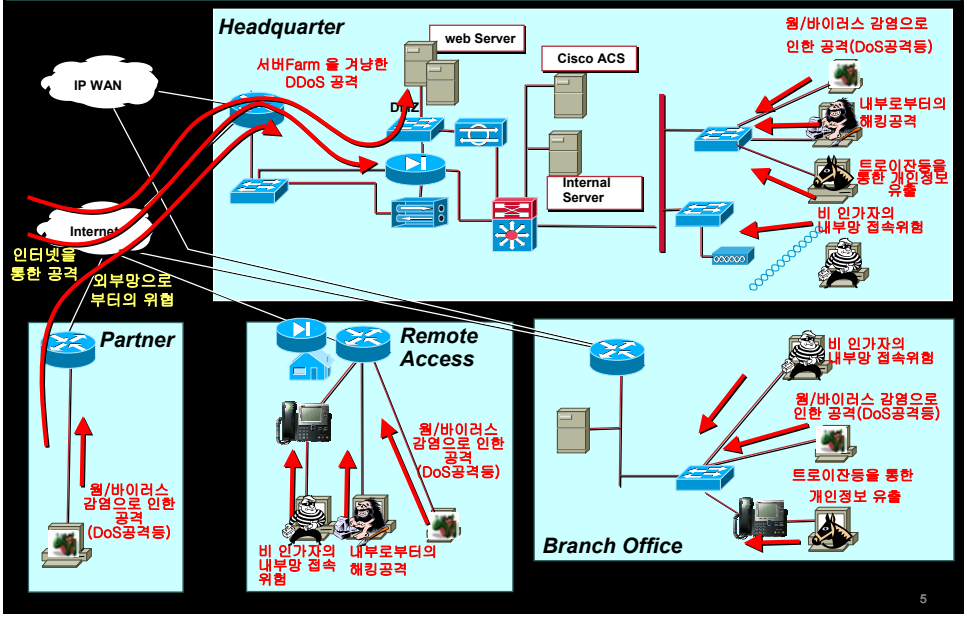
보안 위협의 진화

Cisco.com



기업 네트워크에서의 보안 위협 예

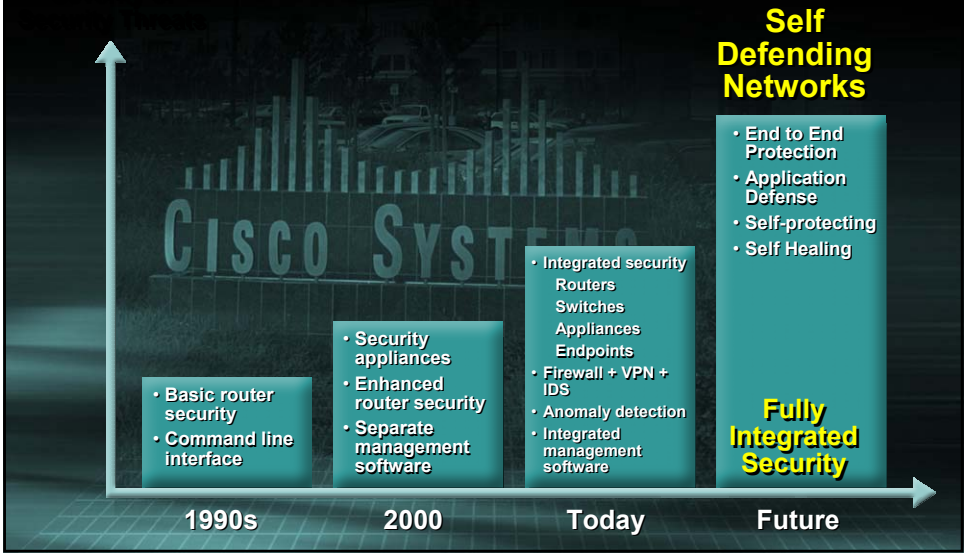
Cisco.com



5

시스코 보안 전략 – 자가 방어 네트워크

Cisco.com



End-to-end 네트워크 보안 전략

Cisco.com

SELF-DEFENDING NETWORK

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

통합된 보안 솔루션

- Trust & Identity
- Threat Defense
- Secure Connectivity

지속적인 보안 기술 혁신

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

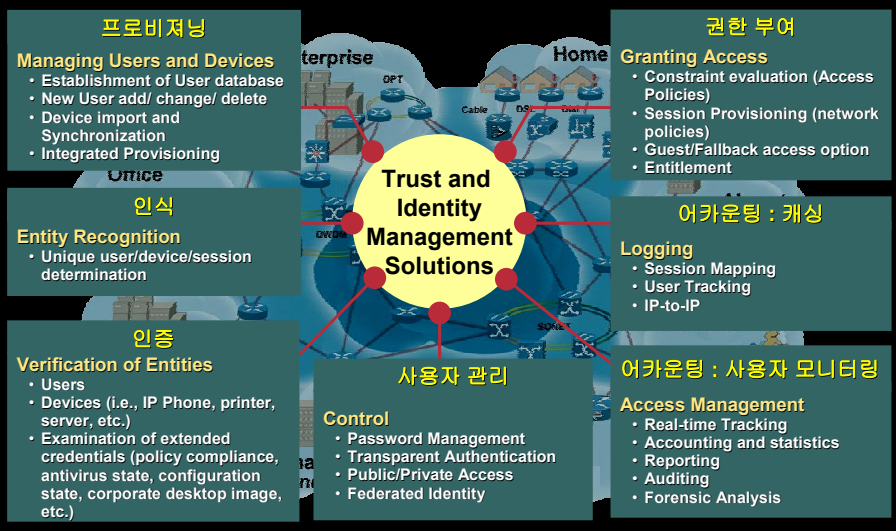
시스템적인 보안 솔루션

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

인증
- Trust and Identity

Trust and Identity 관리 솔루션

Cisco.com



프로비저닝

Managing Users and Devices
- Establishment of User database
- New User add/ change/ delete
- Device import and Synchronization
- Integrated Provisioning

인식

Entity Recognition
- Unique user/device/session determination

인증

Verification of Entities
- Users
- Devices (i.e., IP Phone, printer, server, etc.)
- Examination of extended credentials (policy compliance, antivirus state, configuration state, corporate desktop image, etc.)

사용자 관리

Control
- Password Management
- Transparent Authentication
- Public/Private Access
- Federated Identity

권한 부여

Granting Access
- Constraint evaluation (Access Policies)
- Session Provisioning (network policies)
- Guest/Fallback access option
- Entitlement

어카운팅 : 캐싱

Logging
- Session Mapping
- User Tracking
- IP-to-IP

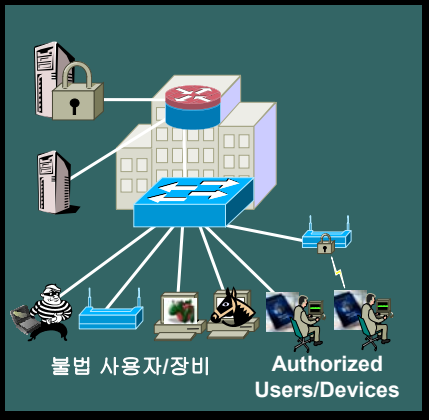
어카운팅 : 사용자 모니터링

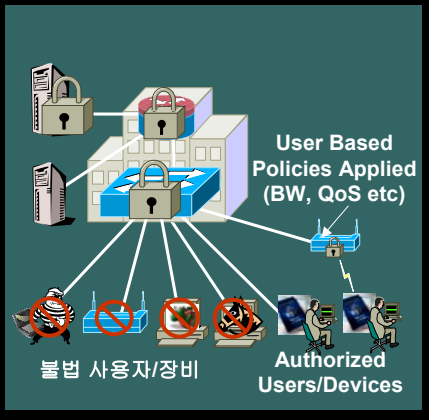
Access Management
- Real-time Tracking
- Accounting and statistics
- Reporting
- Auditing
- Forensic Analysis

9

인증 (Trust and Identity) 의 이해

Cisco.com





Identity-based Networking

Identifies the **user or device** on the network and ensures access to correct network resources

Network Access Control

Identifies the **posture (or compliance)** of the device to ensure the device can safely be admitted to the network without undue hazard

Trust and Identity 시스템 동작 방식

Cisco.com

1. **Who are you?** **802.1x** authenticates user in conjunction with ACS

2. **Are you healthy ?** Using **NAC**, the end-station and network can check whether the device has the correct virus software and protection.

3. **Where can you go?** Based on authentication, user is placed in correct workgroup or VLAN

4. **What service level to you receive?** The user can be put into a firewalled VPN or given specific QoS priority on the network

5. **What are you doing ?** Using the identity and location of the user, tracking and accounting can be better managed

인증
– 사용자 인증 **(802.1x)**

스위치의 Port Security

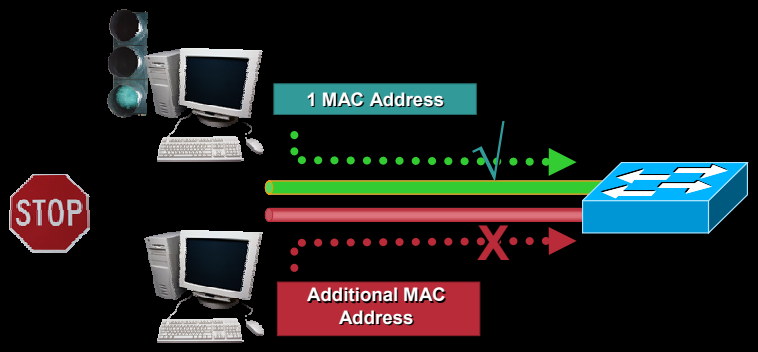
Cisco.com

What It Does:

Limits the number of MAC addresses that are able to connect to a switch and ensures only approved MAC addresses are able to access the switch.

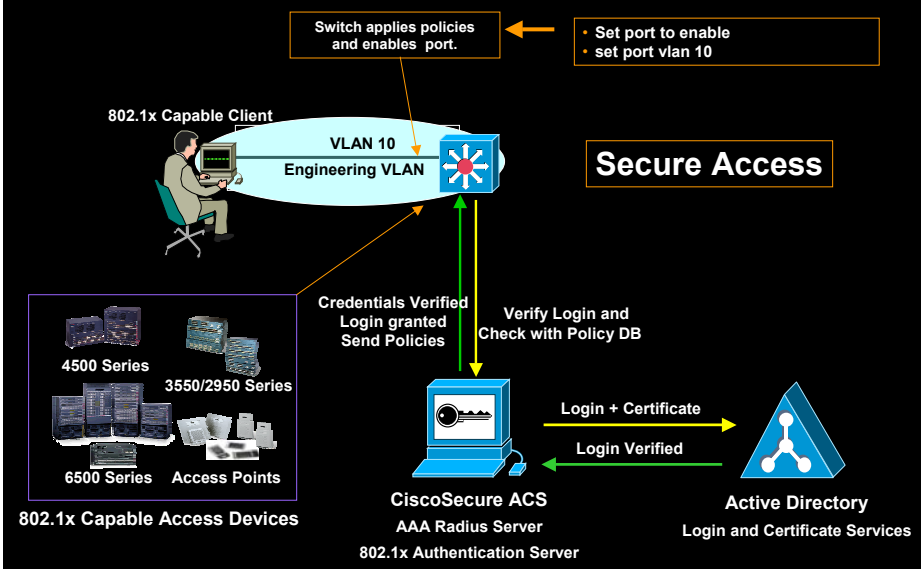
Benefit:

Ensures only approved users can log on to the network.



사용자 인증 기반의 네트워크 서비스

Cisco.com



사용자 ID에 기반한 자동 구성

Cisco.com

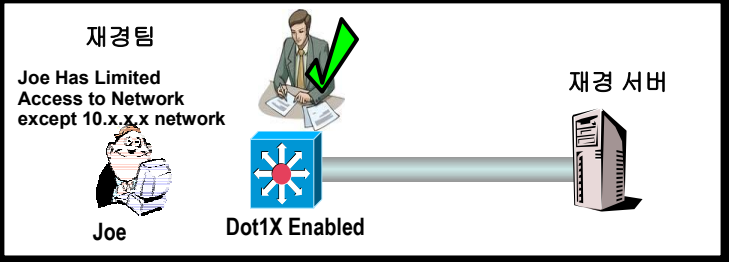
- **Extensions to 802.1x**
  - 802.1X with Dynamic VLANs
  - 802.1X with Port Security
  - 802.1X with VVID (IP Telephony)
  - 802.1X Guest VLANs
  - 802.1x and ACL / VACL propagation
  - 802.1X with ARP Inspection
  - 802.1X with DHCP
  - 802.1x and AutoQoS
  - 802.1x with Wake on LAN
  - 802.1x Accounting Enhancements
  - 802.1x - Authenticated Identity to Port Description Mapping
  - 802.1x - One-to-Many logical VLAN name to ID mapping
  - 802.1x – DNS Resolution for RADIUS Server

- Enhanced Admissions Control
- Greater flexibility and mobility for a stratified user community
- Enhanced User Productivity
- Lowered Operational Expenses
- Additional Security with converged VoIP networks

예) 802.1X with User ACLs

Cisco.com

Allows PACLs to be downloaded from Radius Server to control access on a per-user basis for duration of the session

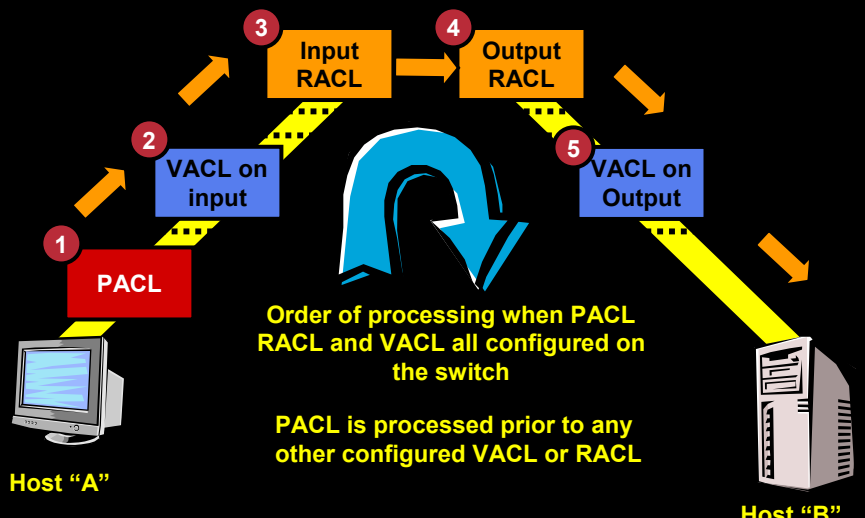


- In the case of Multiple Hosts mode, per-user ACL is disabled on the port
- Only Extended ACL format supported on RADIUS server
- Uses Vendor-Specific Attributes (VSAs) on RADIUS server and are passed to the Authenticator during the authentication process
- Port ACL - allows an IP and MAC access list to be applied to a L2 interface only in the input direction. A PACL is a L2 interface ACL.

ACL 비교

- **Router ACL**
  - **RACL -** can only be applied to a L3 interface, which could be either an SVI or a physical interface configured as a routed port. RACLs may be applied in either the input or output direction.
- **VLAN ACL**
  - **VACL -** can be applied to a VLAN and is always applied in both input and output directions.
- **Port ACL**
  - **PACL -** allows an IP and MAC access list to be applied to a L2 interface only in the input direction. A PACL is a L2 interface ACL.
- **CLI for PACLs**
  - Switch# (Config) interface fa0/1
  - Switch# (Config-if) ip access-group 101 in
  - Switch# (Config-if) mac access-group macacl1 in

Port기반의 ACLs (PACLs)

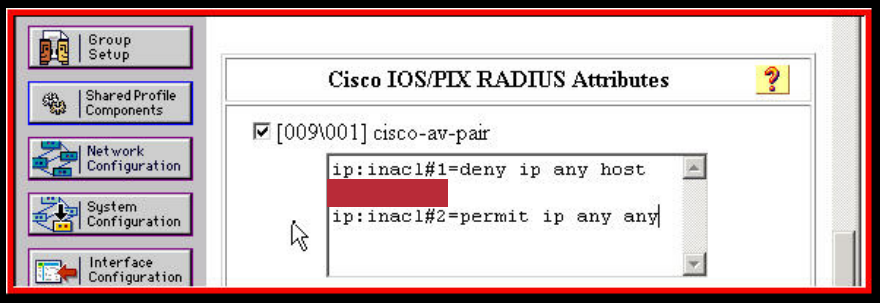


ACS 구성

Cisco.com

- **Modify applicable Cisco Secure Group (cont)**

  Configure the VSA for the Group. An example is below.



- In this example, we have an ACL that will deny access to a certain server.
- The ACL can be applied to allow it to be compliant to a customer's security policy.

ACL 할당 - 확인

Cisco.com

- **Working example from a Client:**

```
[root@id27 root]# ping 10.1.8.5
PING 10.1.8.5 (10.1.8.5) from 10.1.8.8 : 56(84) bytes of data.
Warning: time of day goes back, taking countermeasures.
64 bytes from 10.1.8.5: icmp_seq=0 ttl=128 time=458 usec
64 bytes from 10.1.8.5: icmp_seq=1 ttl=128 time=203 usec
64 bytes from 10.1.8.5: icmp_seq=2 ttl=128 time=195 usec

--- 10.1.8.5 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.195/0.285/0.458/0.122 ms
[root@id27 root]# ping 10.1.8.3
PING 10.1.8.3 (10.1.8.3) from 10.1.8.8 : 56(84) bytes of data.

--- 10.1.8.3 ping statistics ---
4 packets transmitted, 0 packets received,
```

- Notice the Client cannot access the denied server via the ACL, but can access other resources.

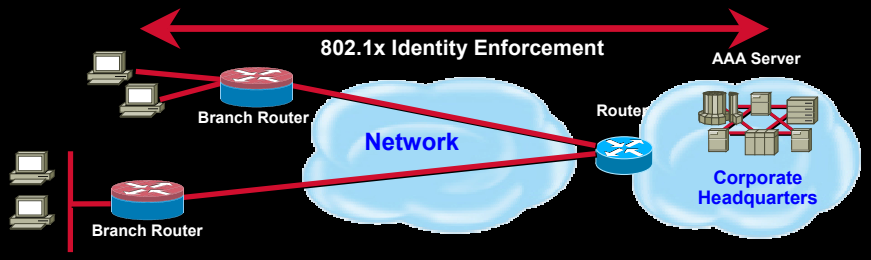
라우터 Ethernet 모듈의 802.1x 지원

Cisco.com

HWIC-ESW
4 and 9 port
Hi-Speed WAN Interface Card

NM-ESW
16 and 36 ports of 10/100 Ethernet

- Support for 802.1x Authentication
  - New 4 & 9 Port EtherSwitch HWIC and current 16 and 36 Port NM all Support 802.1x *AND* Power over Ethernet (POE)
  - All new router Ethernet ports also support 802.1x
- Survivable Remote User Authentication



21

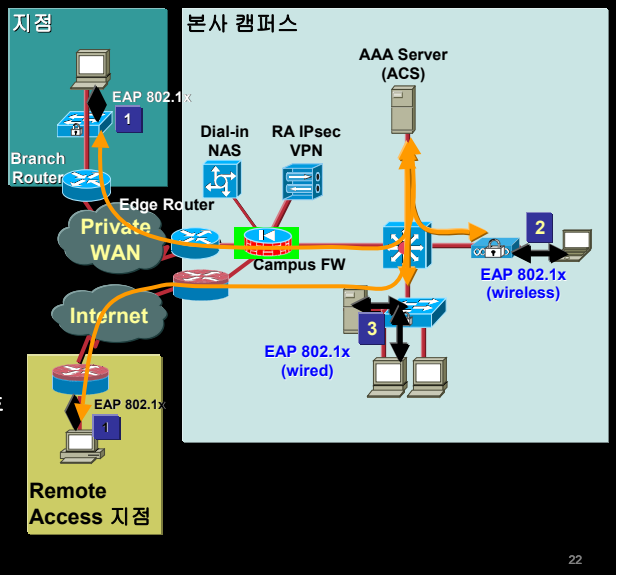
802.1x 적용 시나리오

Cisco.com

1: 지점 네트워크의 보호
정상적인 네트워크 접속을 위해서는 사용자 인증이 필요

2: 무선 캠퍼스 네트워크 보호
무선랜 접속을 위해서는 사용자 인증이 필요

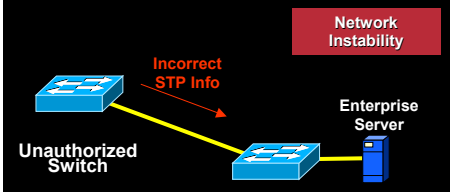
3: 캠퍼스 및 데이터 센터 접속 보호
LAN 접속을 위해서는 사용자 인증이 필요
VALN, ACL, QoS 적용



22

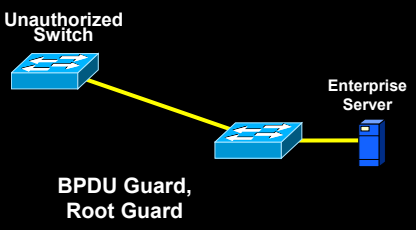
불법 스위치 설치 방지

Cisco.com



Problem:

- Rogue switches or routers can insert incorrect routing/STP info and inadvertently bring down the entire network

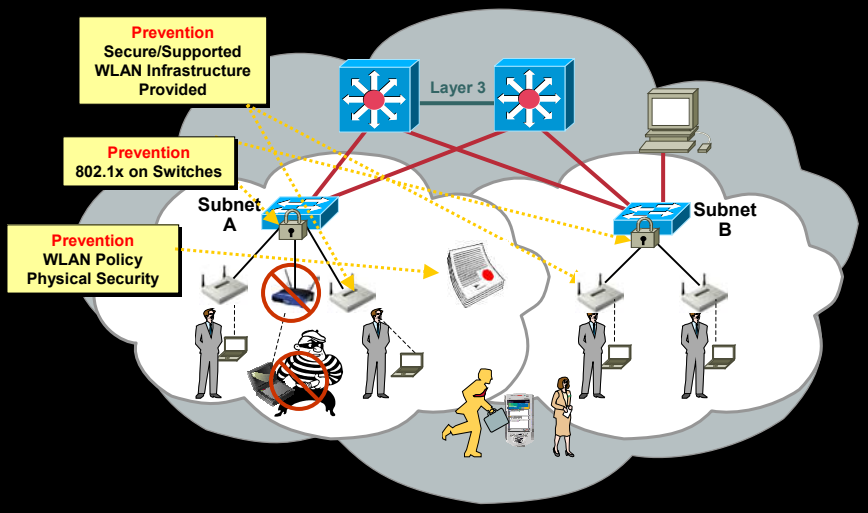


Solution:

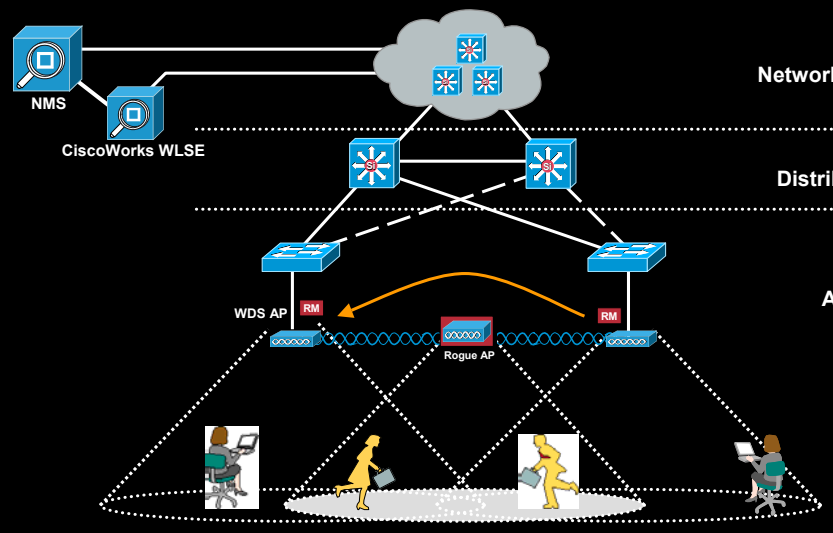
- Catalyst Switches support BPDU-Guard and authenticated routing updates: BPDU Guard, Root Guard, etc.

무선 : 불법 AP 설치 방지

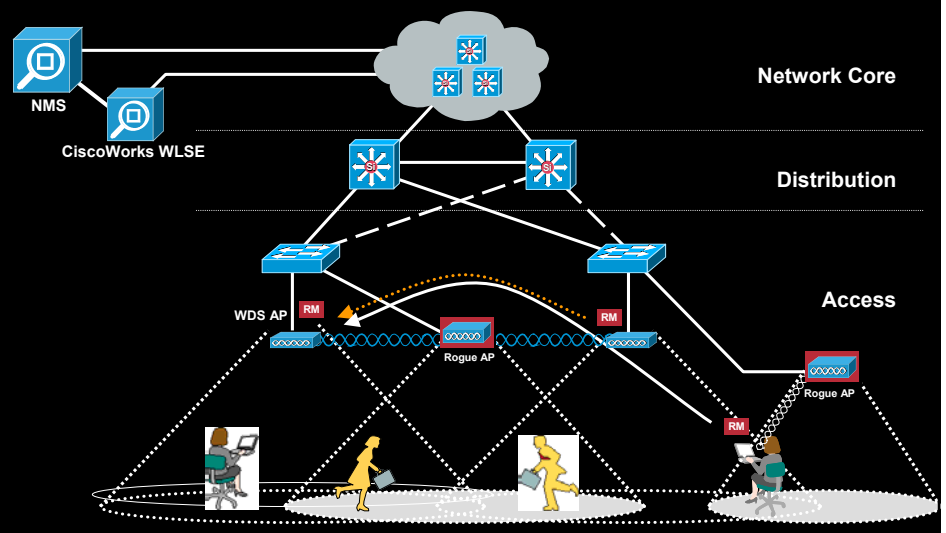
Cisco.com



무선 : 불법 AP 감지 – AP 스캐닝



무선 : 불법 AP 감지 – 클라이언트 스캐닝

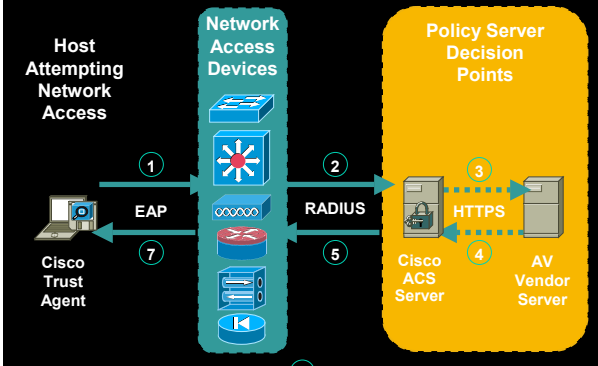


인증
– 사용자 호스트 상태 인증 (NAC)

시스코 NAC 솔루션

Cisco.com

NAC Solution: Leverage the network to intelligently enforce access privileges based on **endpoint security compliance**



1. Host Sends Credentials to Access Device using EAP (UDP or 802.1x)
2. Access Device forwards Credentials to Policy Server (ACS) using RADIUS
3. ACS Server authenticates ID and passes AV info to AV Vendors Servers
4. AV Vendors Servers respond with Compliance/Non-Compliance Message
5. Policy Server Responds to Access Device with Access Rights and VLAN assignment
6. Access Device accepts rights, enforces policy, and notifies client
7. **(Permit/Deny/Restrict/Quarantine)**

안철수연구소 symantec. TREND MICRO Network ASSOCIATES YOUR NETWORK. OUR BUSINESS.

NAC 적용 시나리오

Cisco.com

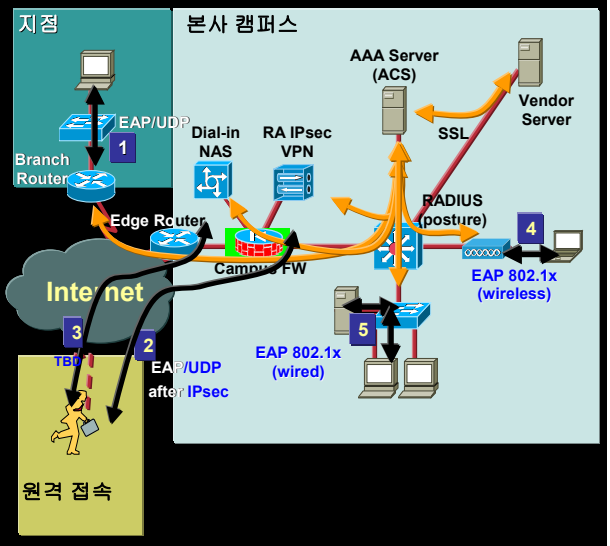
1: 지점 네트워크 접속 준수
- Enforce on L3 router and firewall

2: 원격 접속 준수
- Extension of “Are You There”

3: 다이얼 인 접속 준수

4: 무선 네트워크 보호
- Quarantine with ACLs/VLANS
- Extension of 802.1x

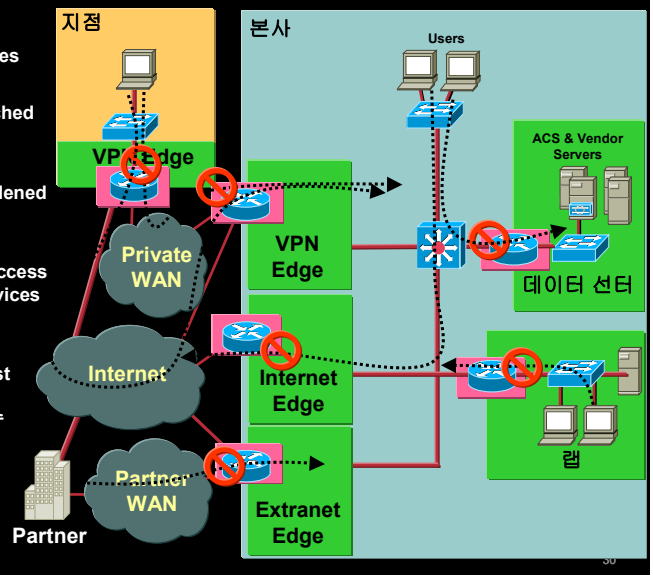
5: 캠퍼스 접속 및 데이터 센터 접속 준수
- Quarantine with ACLs/ VLANS
- Extension of wired 802.1x



Router 기반의 적용 시나리오

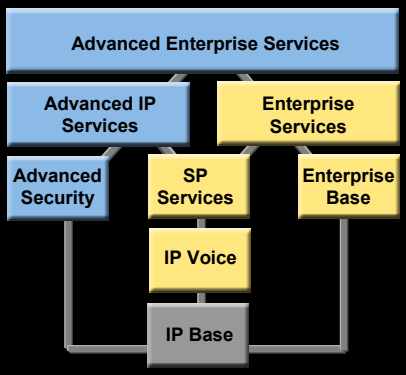
Cisco.com

- 지점 접속 준수
  - Focus first on less trusted/managed offices
- 엑스트라넷 접속 준수
  - Partner hosts are patched and comply
- 인터넷 접속 준수
  - Ensure hosts are hardened prior to browsing
- 랩 네트워크 접속 준수
  - Production network access only for compliant devices
- 데이터 센터 보호
  - Devices accessing protected servers must comply
- 원격 접속 & 무선 접속 준수 (not shown)
  - Mobile & remote compliance
  - Put router behind RA VPN, dialup, & WAP



라우터 NAC 지원 사양

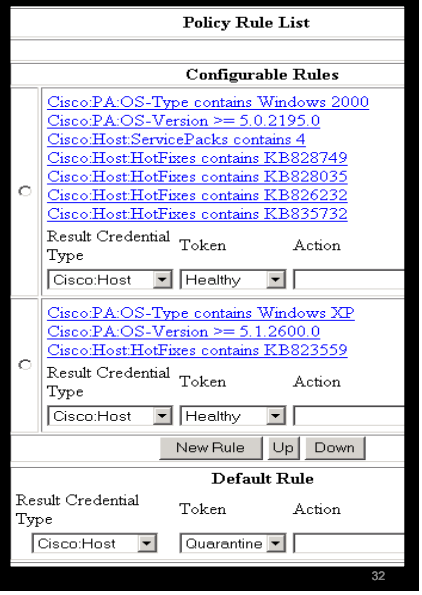
- **NAC support available in 12.3(8)T3 IOS images with Security**
  - Advanced Security , Advanced Services, and Advanced Enterprise images
  - * Yes—older platforms with NAC support only in the Classic IOS FW Feature Sets in 12.3T, these Routers do not have the Advanced newer images in 12.3T



Cisco 18xx, 28xx, 38xx	Yes
Cisco 72xx	Yes *
Cisco 37xx	Yes
Cisco 3640, 3660-ENT Series	Yes *
Cisco 2600XM, 2691	Yes
Cisco 1701,1711, 1712, 1721, 1751, 1751-V, 1760	Yes
Cisco 83x	Yes *
Cisco 74xx, 73xx, 71xx	TBD
Cisco 5xxx	TBD
Cisco 4500	No
Cisco 3660-CO Series	No
Cisco 3620	No
Cisco 2600 non-XM Models	No
Cisco 1750, 1720, 1710	No

시스코 Secure ACS의 NAC 지원

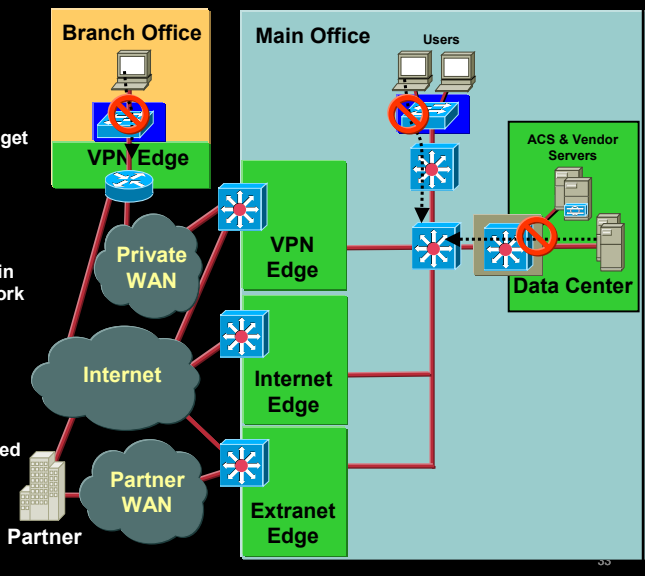
- Policy decision point for NAC in version 3.3
- Obtain credentials from endpoint
  - Establish secure communication channel with CTA
  - Request and receive application (& OS) credentials
- Perform AAA on credentials
  - Authenticate each set of credentials
    - Each evaluated by ACS or vendor server (e.g. CSA in ACS, OfficeScan by TMCM)
  - ACS determines authorization rights
    - Lowest rights of all authentication results (Healthy + Checkup = Checkup)
  - Exception list based on MAC & IP addresses
  - Audit log (collected by CiscoWorks SIMS)
- Send authorization rules to router, feedback to endpoint
  - Dynamic ACL and optional URL redirection
  - Per application notifications possible on endpoint, user feedback too
  - Based on vendor application, feedback may trigger remediation



Switch LAN 적용 시나리오

Future

- 사용자 접속 LAN 보호
  - User hosts, and others, must comply in order to get normal LAN access
- 서버 LAN 보호
  - All servers must comply in order to get normal network access, even to the LAN
- 무선랜/ 공유 매체 보호 (not shown)
  - Protect hosts using shared media on a port
  - Hubs & WAP scenarios



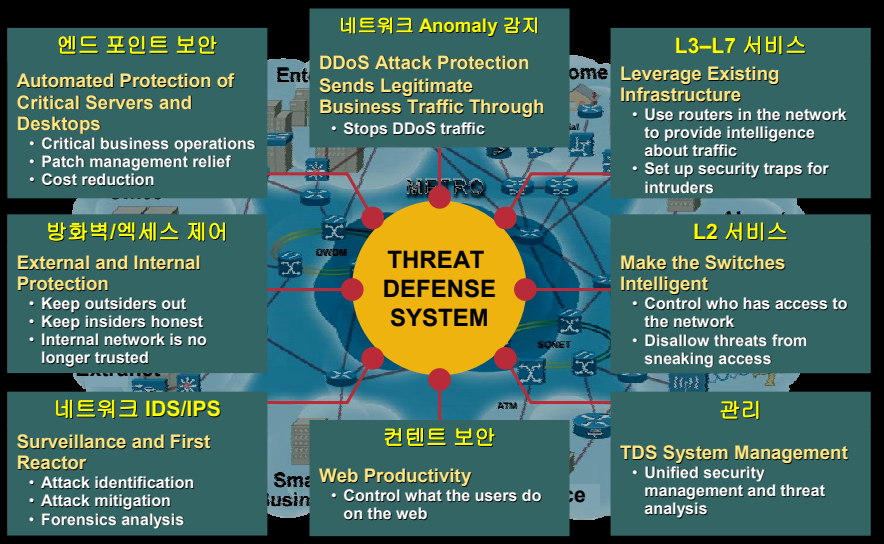
33

위협 방어
– Threat Defense

34

중요 비즈니스 자산의 보호

Cisco.com



35

위협 방어 - 목차

Cisco.com

- 사용자 위협 방어
  - **CSA** 솔루션
- 백본 및 지점 네트워크 위협 방어
  - 트래픽 감지/분석
  - 방어 적용
- 내,외부 네트워크으로부터의 방어
  - 외부 침입 차단/ 방어 (**Firewall/ IDS,IPS**)
  - **DDoS** 방어

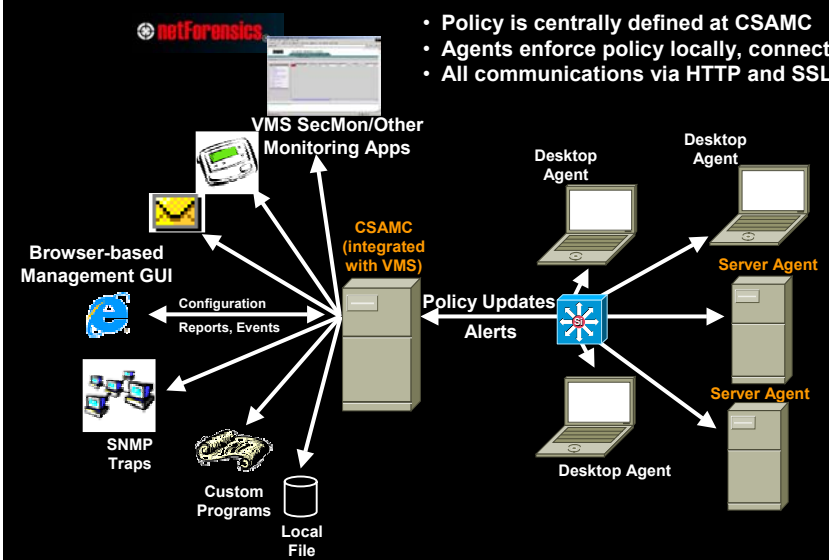
36

위협 방어
– 사용자 위협 방어 (CSA)

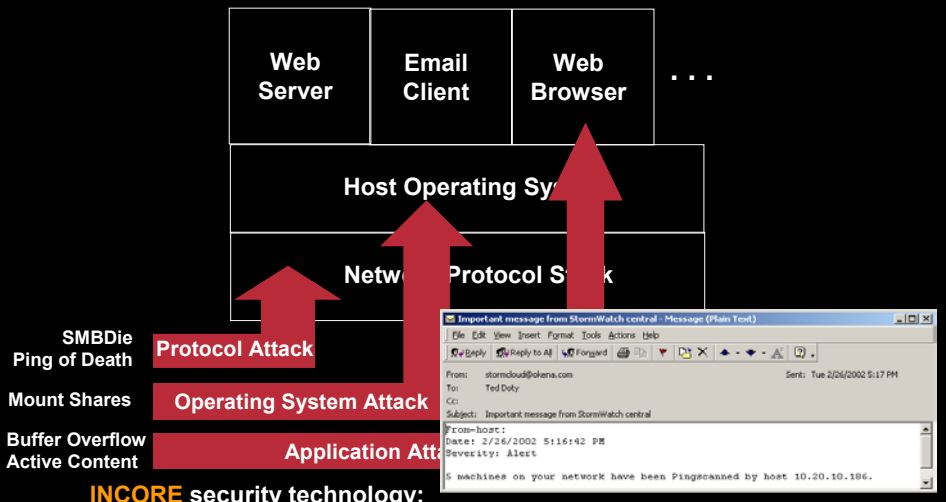
엔드 포인트 보안 : CSA 솔루션

Cisco.com

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



Behavior Control Protects End Points



INCORE security technology:

- **IN**tercept Operating System calls caused by application behavior
- **CO**rrelate system calls to ensure accuracy
- **R**ules **E**ngine is customizable to adapt to local environment

CSA DayZero ScoreCard

CSA successfully blocked the following known attacks with a default installation

- Partial List -

- Mydoom
- W32.Blaster
- Fizzer
- Bugbear
- Sobig.E
- SQL Slammer
- Sircam.A
- WebDav Vulnerability
- Code Red
- Nimda

위협 방어

– 백본 및 지점 네트워크 위협 방어

DoS 공격 감지 : CPU Load 분석

Cisco.com

```
router>sh proc cpu
CPU utilization for five seconds: A%/B%; one
  minute: C%; five minutes: D%
```

CPU total utilisation

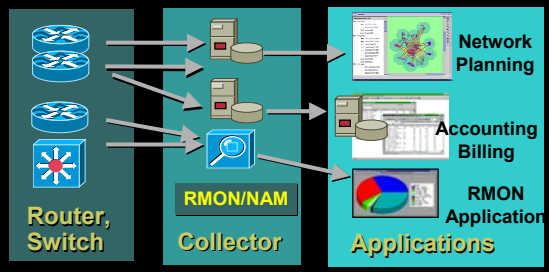
CPU at interrupt level

- If A>>B (CPU too busy)
  - Switching problems:
    - Cache misses: If flow not in cache, ask CPU! (sh int switching)
    - DoS: spoofed addresses -> many cache misses
  - Packet from/to router:
    - Routing, ARP, ICMP, SNMP, console, telnet, vty,
    - Watch out: Too many ICMP could come from a route null0
    - use no ip unreachables or ICMP Unreachable Rate-Limit
  - Packets with options (could be DoS)
- CPU / Memory Threshold Notification
  - Generates an SNMP trap message when a predefined threshold of CPU/Memory usage is crossed

NetFlow를 통한 Traffic 감지

Cisco.com

Defined by seven unique keys:
- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 3 protocol type
- TOS byte (DSCP)
- Input logical interface (ifIndex)



- Enable at the interface level on a Cisco router:
  - `router(config-if)# ip route-cache flow`
- To view flow data locally on a device:
  - `router # show ip cache flow`
- Netflow 지원 장비

43

show ip cache verbose flow

Cisco.com

```
router_A#sh ip cache verbose flow
IP packet size distribution (23597 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  1323 active, 2773 inactive, 23533 added
  151644 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
```

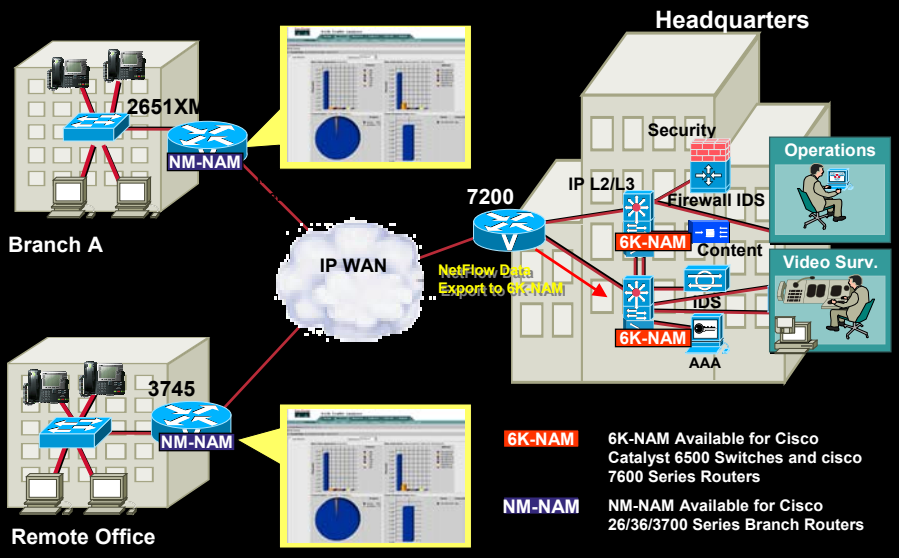
Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
TCP-other	22210	3.1	1	1440	3.1	0.0	12.9
Total:	22210	3.1	1	1440	3.1	0.0	12.9

SrcIf Port	Msk	AS	SrcIPaddress	DstIf Port	Msk	AS	DstIPaddress NextHop	Pr	TOS	Flgs	Pkts B/Pk	Active
Et0/0			216.120.112.114	Se0/0			192.168.1.1	06	00	10		1
5FA7	/0	0		0007	/0	0	0.0.0.0				1440	0.0
Et0/0			175.182.253.65	Se0/0			192.168.1.1	06	00	10		1

44

NAM 을 이용한 Netflow 데이터 수집 및 분석

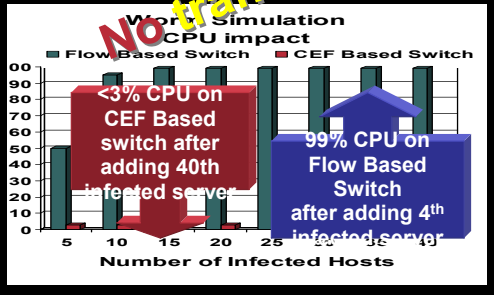
Cisco.com

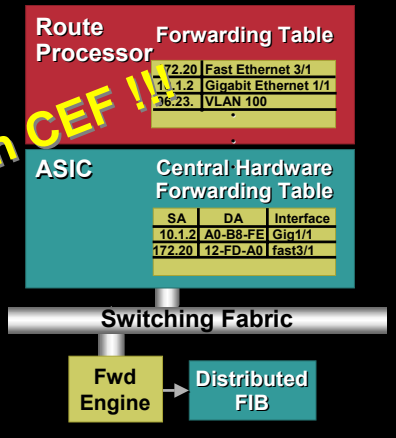


DoS 방어 : 시스코 CEF 스위칭

Cisco.com

- Forwarding table calculated based on routing table entries, not traffic flows
- CEF uses a longest match lookup on prefix/mask, not an exact match

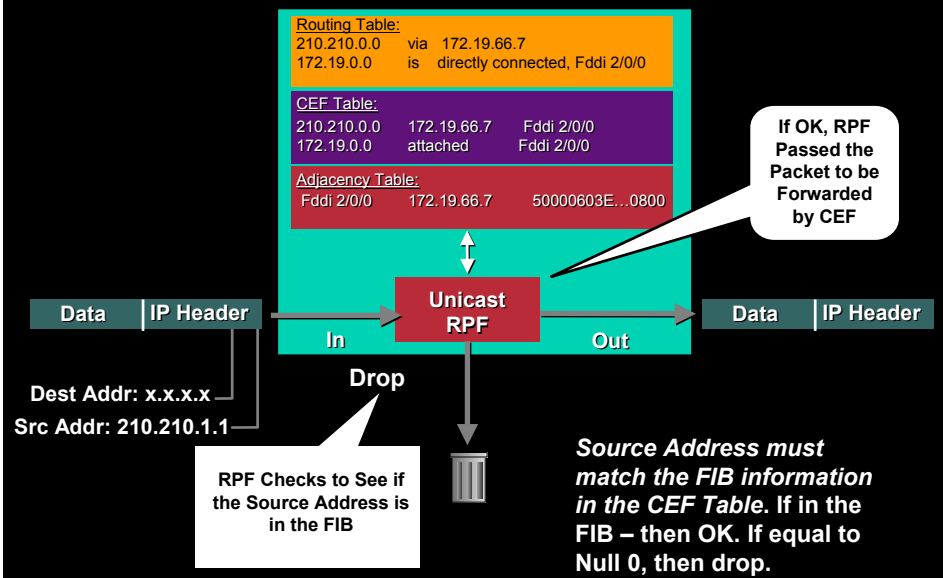




* CEF : Cisco Express Forwarding

CEF Unicast RPF

Cisco.com

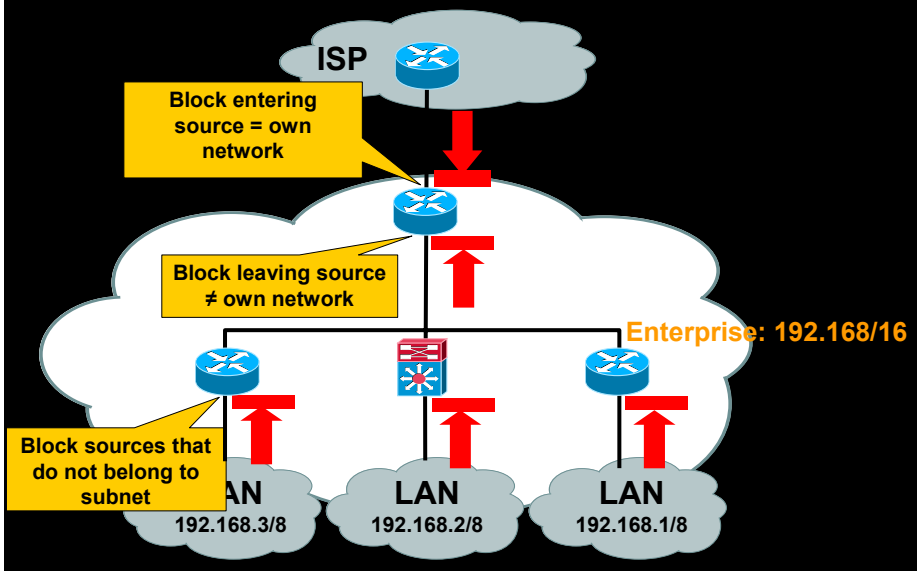


Source Address must match the FIB information in the CEF Table. **If in the FIB – then OK. If equal to Null 0, then drop.**

47

Unicast RPF – 기업 네트워크에서의 IP 주소 변조 방어

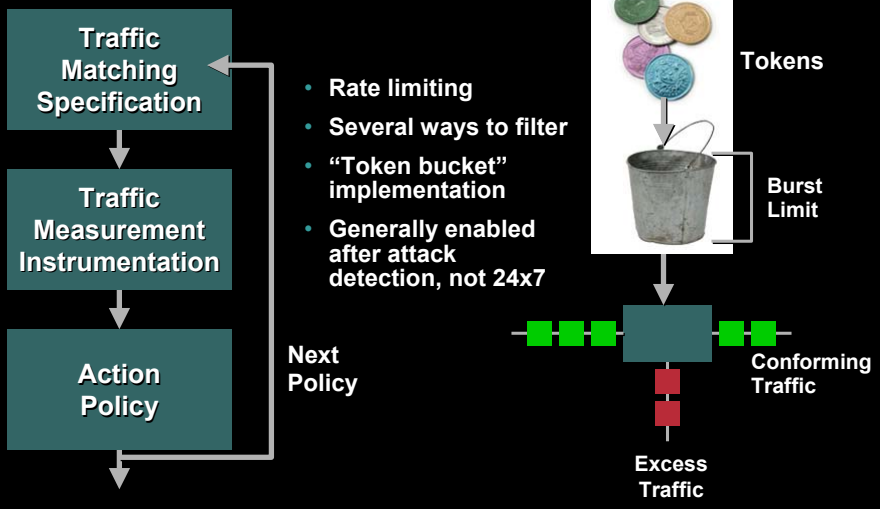
Cisco.com



48

트래픽 제어 - Committed Access Rate

Cisco.com



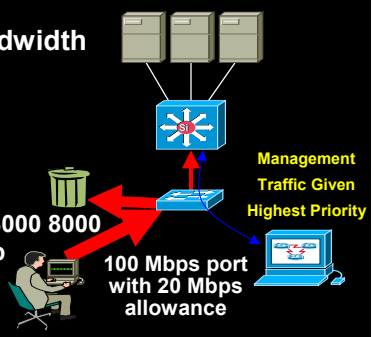
DoS 방어를 위한 CAR Rate Limiting

Cisco.com

- CAR allows network managers to set bandwidth thresholds for users and by traffic type.

- Limit outbound ping to 256 Kbps

```
interface xy
     rate-limit output access-group 102 256000 8000 8000
     conform-action transmit exceed-action drop
!
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

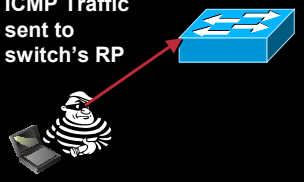


- Limit inbound TCP SYN packets to 8 Kbps

```
interface xy
     rate-limit input access-group 103 8000  8000 8000
          conform-action transmit exceed-action drop
!
access-list 103 permit tcp any any syn
```

Control Plane Rate Limiting

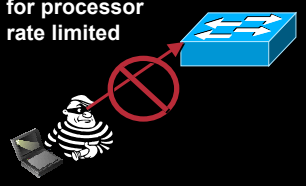
100 Mbps of ICMP Traffic sent to switch's RP



Problem:

- DoS Attacks at infrastructure devices generate rogue IP traffic streams destined to the Route Processor at very high data rates.
- Affects routing protocols, STP updates, which in turn severely affect network stability

Traffic bound for processor rate limited



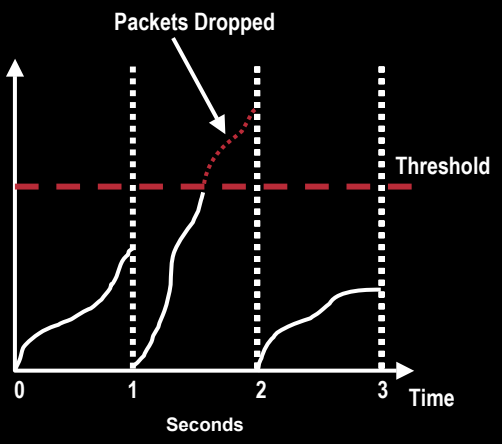
Solution:

Route Processor Rate Limiting provides hardware-based mechanism for limiting traffic destined to RP, including:

- Ingress/Egress ACLs
- CEF Receive and Glean
- ICMP Redirects/Unreachable
- TTL Failure
- CEF No Route
- RPF Failure
- VACL Logging

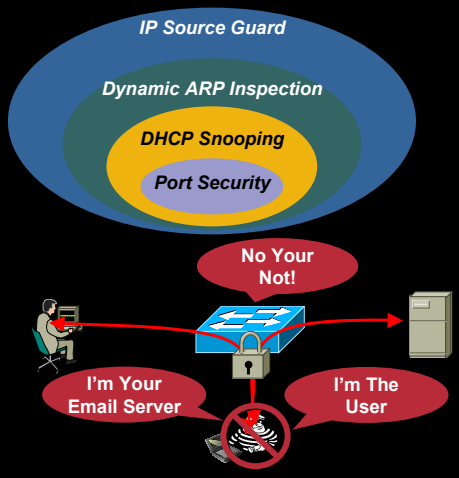
Broadcast Suppression for Storm Control

- Storm Control is also known as Broadcast suppression
- Able to limit the volume of broadcast, multicast and/or unicast traffic
- Protect the network from intentional and unintentional flood attacks i.e. STP loop
- Limit the combined rate of broadcast & multicast traffic to normal peak loads



Layer 2 내부 공격으로부터의 방어

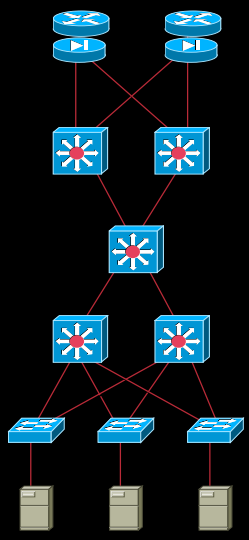
Cisco.com



Attack	Switch Feature
MAC Address Flooding	Port Security
DHCP Rogue Server for Default Gateway Interception	DHCP Snooping
ARP Spoofing or ARP Poisoning	Dynamic ARP Inspection
IP Spoofing	IP Source Guard

Anti-Spoof and Filtering 응용

Cisco.com



Perimeter: uRPF, RFC 1918 and 2827, Bogon filtering

Distribution: uRPF, L3 filtering (network isolation, watchdog and unused network screening)

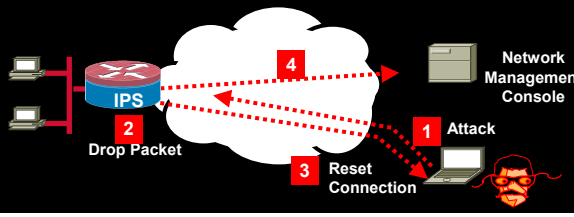
Distribution: as above

Access: ARP inspection, 802.1x and EAP authentication, PVLANs, Port Security , DHCP Snooping, IP Source Guard

Cisco IOS Intrusion Prevention (IPS)

Cisco.com

- IPS in a router – *inline* ability to mitigate network attacks:
  - DROP packet, RESET connection, send ALARM
- Wide range of attack/worm signatures supported – 740+
- Use it for inline intrusion prevention and event notification
- Dynamically load attack signatures to the router
- Integrates technology from Cisco IDS Sensor families
  - Cisco IDS 4200 Series Appliances, Catalyst 6500 IDS Module, Network Module IDS appliance (NM-CIDS)



Cisco IOS 와 NM-CE를 이용한 컨텐츠 보안

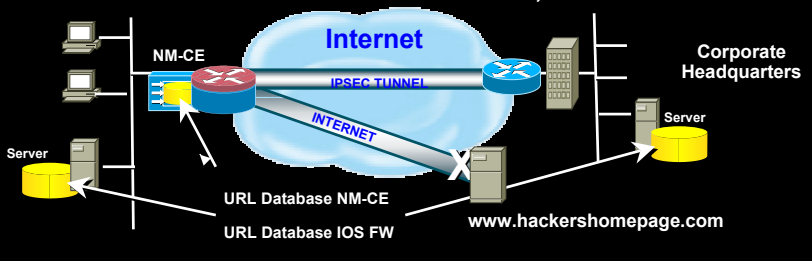
Cisco.com

Cisco IOS URL Filtering

- Integrated with Cisco IOS Firewall
- Supports Websense and N2H2 Web filtering clients
- Works with external Websense and N2H2 servers
- Static “good” list / “bad” list URL filtering in IOS

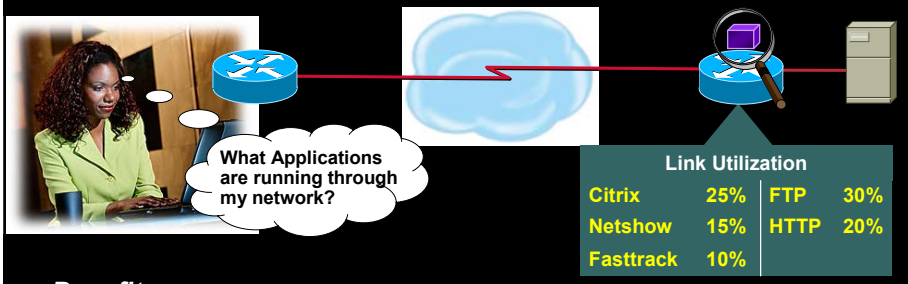
Content Engine Network Module

- Internet Proxy Cache
- URL Filtering Application Server
- Pre-loaded OEM Websense and Smartfilter filtering applications
- Enforces Application Use Policy
- Traffic logging and reporting
- Anti-Virus Gateway (ICAP) to scan, clean, and cache Web content



Network-based Application Recognition (NBAR)

Cisco.com



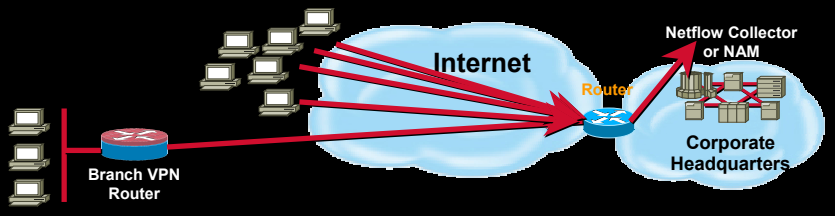
Benefits:

- Helps identify worms and other attacks by tracking Layer 4-7 applications and protocols
  - Stateful & deep packet inspection
  - Use SDM for Graphical display of application traffic analysis
- Protocol Discovery analyzes application traffic patterns in real time and provides statistics
- Now supports more than 98 protocols and applications

엑스트라 넷 : DDoS 공격시 IOS 를 이용한 네트워크 인프라 보호 예

Cisco.com

Control Plane Policing	Protects access to control plane, even during DDoS attacks. Monitors packets, increases infrastructure reliability, and availability
Netflow monitoring	Provides early warning while visibility on traffic flows help you optimize network availability
Out-of-band management	Ensures access despite DoS attacks, or congestion
Network-based Application Recognition (NBAR)	Helps identify worms and other attacks by tracking Layer 4-7 applications and protocols
Role-based CLI Access	Provides partitioned, non-hierarchical, access to CLI commands for secure, logical separation of router users (eg. NetOps and SecOps)

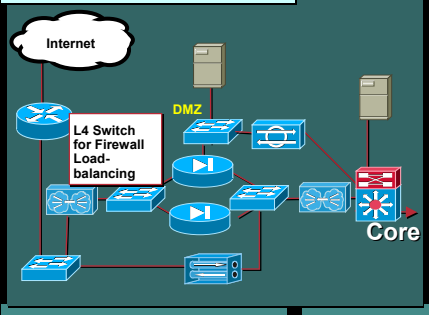


위협 방어
– 내.외부 네트워크으로부터의 위협 방어

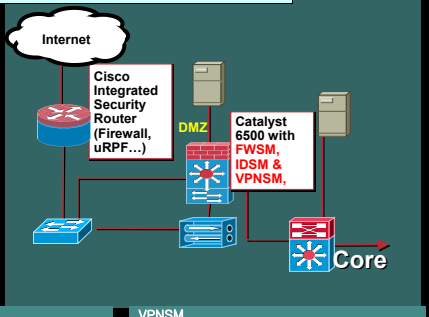
외부 침입 차단/방어

Cisco.com

기존 인터넷 디자인



변경 인터넷 디자인



FWSM
- ❑PIX OS(Secure OS) 기반의 운영
- ❑ 5Gbps 이상의 고성능 처리속도
- ❑ 250 개 VLAN(Firewall Interface) 제공
- ❑ GUI 기반의 손쉬운 관리(FDM)
- ❑ Dynamic Routing (RIP,OSPF) 지원
- ❑ 사시 내부 최대 4장 까지 구성 가능 (최대 20Gbps지원)
- ❑ 동시 접속수 1,000,000개
- ❑ 초당 접속 처리수 100,000 session
- ❑ Packet Forwarding 속도 : 3Million pps
- ❑ 128,000 개 정책 구현 가능

IDSM
- ❑ 실시간 침입 탐지 감시
- ❑ 다중 VLAN 탐지 기능
- ❑ 600Mbps 의 고성능
- ❑ 5,000 cps(초당 TCP처리수)
- ❑ Switch 성능 저하 없는 모니터링 (Passive monitoring)
- ❑ 라우터, 스위치, 방화벽 제품군과의 연동을 통한 In-line Filtering 제공
- ❑ IDSM관리를 위한 SSL기반의 IDM 지원
- ❑ Event분석을 위한 IEV 지원

VPNSM
- ❑ 모듈당 1.9 Gbps (3DES 기준)의 고성능
- ❑ 샤시당 최대 8개의 VPNSM 지원가능 (14Gbps or 5 Mpps)
- ❑ 8,000개의 IPSec Tunnels 제공
- ❑ Site-to-Site and EzVPN Remote Access
- ❑ IPSec Stateful Failover
- ❑ Hardware accelation of both IPSec & GRE
- ❑ Compatible with all Cisco VPN Products
- ❑ Support with both Sup2/MSFC2 and Sup720

안전한 통신
- Secure Connectivity

모든 가능한 접근 방법의 Secure Connectivity

Cisco.com

지점

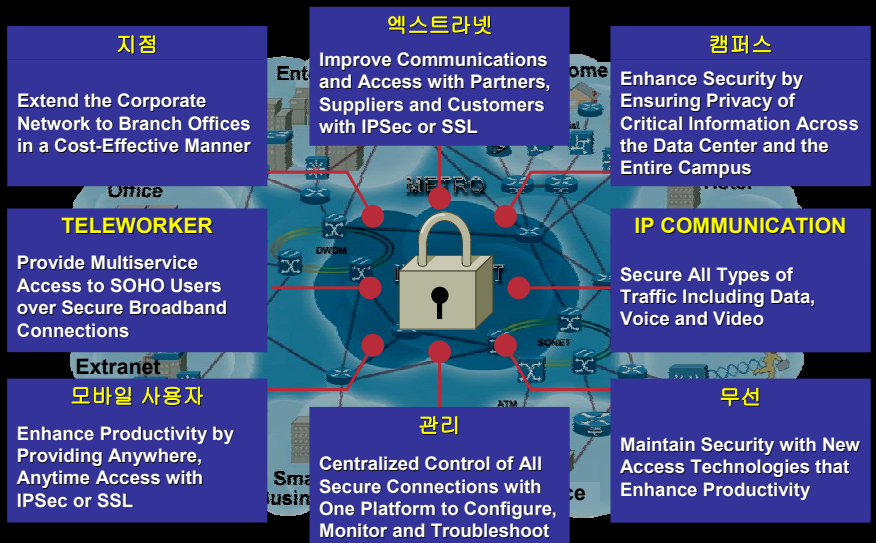
Extend the Corporate Network to Branch Offices in a Cost-Effective Manner

엑스트라넷

Improve Communications and Access with Partners, Suppliers and Customers with IPSec or SSL

캠퍼스

Enhance Security by Ensuring Privacy of Critical Information Across the Data Center and the Entire Campus



TELEWORKER

Provide Multiservice Access to SOHO Users over Secure Broadband Connections

IP COMMUNICATION

Secure All Types of Traffic Including Data, Voice and Video

모바일 사용자

Enhance Productivity by Providing Anywhere, Anytime Access with IPSec or SSL

관리

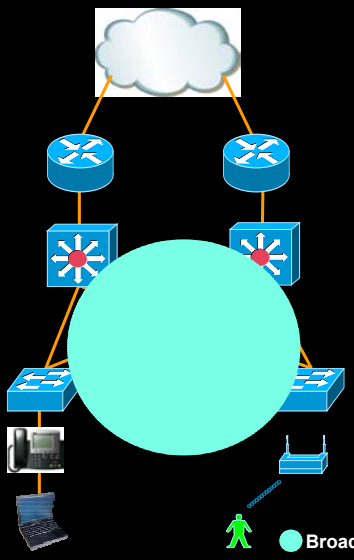
Centralized Control of All Secure Connections with One Platform to Configure, Monitor and Troubleshoot

무선

Maintain Security with New Access Technologies that Enhance Productivity

캠퍼스 : Virtual LANs – 논리적 분리

Cisco.com

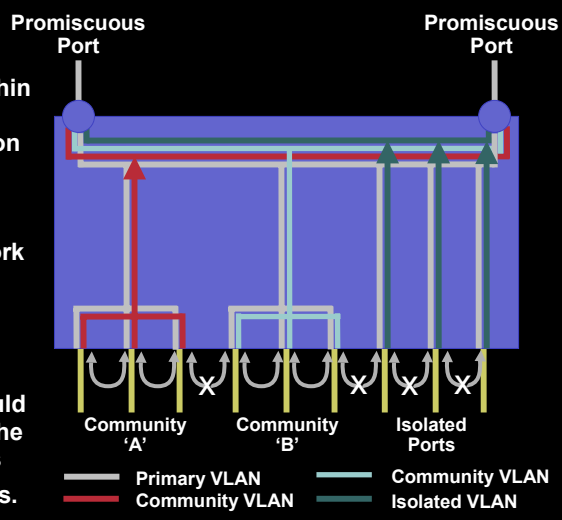


- **What VLANs do:**
  - Provides isolation at Layer 2 of different broadcast domains. VLANs provide a very basic level of security to preventing cross-VLAN hopping and snooping
- **Benefit:**
  - Network manager can create small Layer 2 domains for simple connectivity and addressing, which map into the Layer 3 routed network for campus/enterprise-wide scalability

캠퍼스 : Private VLANs

Cisco.com

- **What it Does:**
  - Sets up "sub-VLANs" within a master VLAN, where the hosts in a private VLANs on given segment can only communicate with default gateway— NOT other hosts on network that reside in different Private VLANs
- **Benefit:**
  - Compromised device could not infect others. Solves the problem of isolating users without wasting IP subnets.



엑스트라넷 : Web VPN(SSL VPN) 및 IPSec VPN

Cisco.com

Deployment Flexibility = Comprehensive Solutions

Web VPN(SSL VPN)

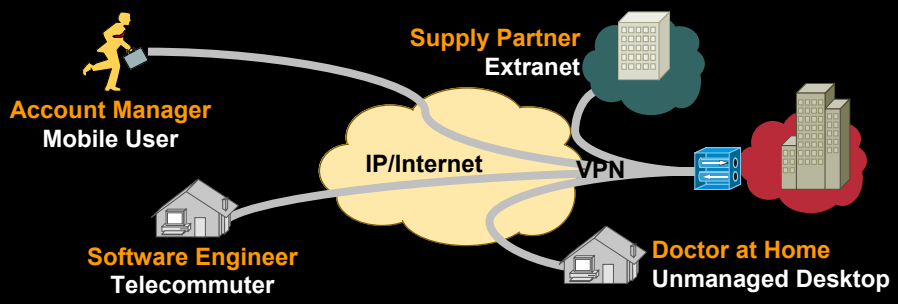
- Anywhere access to a specific application set using a web browser
  - All applications accessed through browser portal
  - Easy firewall traversal
  - Enables extranets/B2B commerce
- Client/server support requires application specific applets

IPSec VPN

- Robust remote access extending all applications available in the office to remote users
  - All applications, all traffic types
  - Client software allows for application transparency
- Maximum functionality for managed computers
- Robust voice/video convergence

엑스트라넷 : IPSec 및 SSL(Web) VPN 이용 방안

Cisco.com

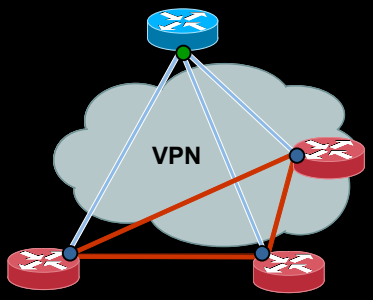


Web VPN(SSL VPN)	IPSEC VPN
• PARTNER — Few apps/servers, tight access control, no control over desktop software environment, firewall traversal • DOCTOR — Occasional access, few apps, no desktop software control	• ENGINEER — Many servers/apps, needs native app formats, VoIP, frequent access, long connect times • ACCOUNT MANAGER — Diverse apps, home-grown apps, always works from enterprise-managed desktop

엑스트라넷 : Dynamic Multipoint VPN (DMVPN)

Cisco.com

Secure Meshed Tunnels Automatically!



Spoke A

= DMVPN Tunnels
= Traditional Static Tunnels
= Static Known IP Addresses
= Dynamic Unknown IP Addresses

Spoke A needs to contact Spoke B:

V3PN Call

PC Contact to a Server

- Learns real address of Spoke B via NHRP, OSPF or EIGRP (routing features)
- IPSec VPN tunnel to Spoke B is dynamically built over mGRE interface

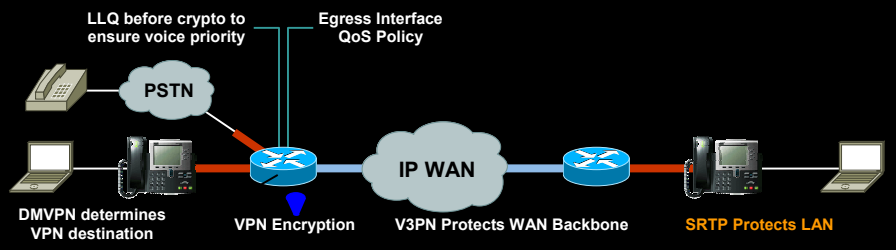
Benefits:

- Full Meshed connectivity with configuration simplicity of hub and spoke
- Preserves (central) bandwidth, minimizes latency
- Support for dynamically addressed spokes
- Zero touch configuration for addition of new spokes in the DMVPN

Secure Toll Quality IP Telephony Using DMVPN & V3PN

Cisco.com

Communications problem solved though network intelligence and a systems approach managed though policies



Requirements

- Mesh configuration, hub & spoke simplicity
- Wire-speed encryption
- Voice / video prioritization
- Bandwidth conservation
- Concurrent services VPN
- Secure RTP

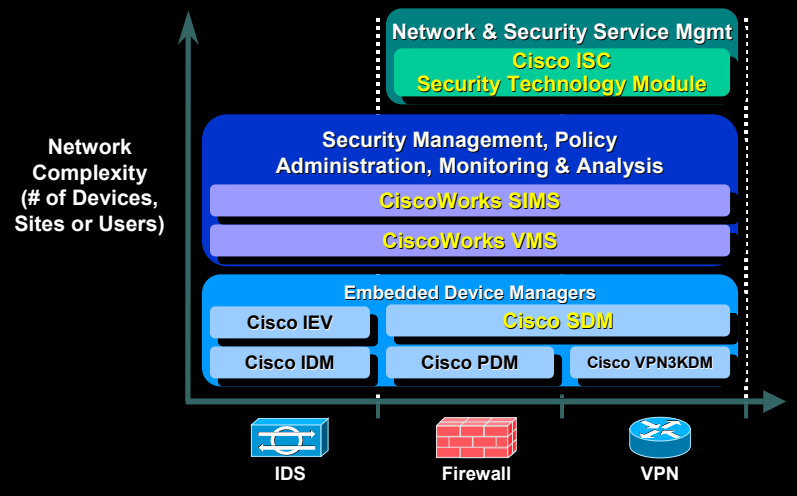
Benefits

- Ease of management, configuration
- Traffic throughput with encryption
- Toll quality, jitter-free voice and video
- DMVPN sets up tunnel when needed
- WAN hacker security, lower costs
- LAN hacker security

보안 관리

시스코 보안 관리 제품

Cisco.com



Auto Secure

12.3 and 12.3T

Cisco.com

- "One Touch" Device Lockdown that quickly and easily eliminates many potential security threats
- Management Plane Security

```
Router# auto secure
            --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of the router but it will not make
router absolutely secure from all security attacks ***

All the configuration done as part of AutoSecure will be shown here. For more details of
why and how this configuration is useful, and any possible side effects, please refer to
Cisco documentation of AutoSecure.
......
Securing Management plane services..
Disabling service finger
Disabling udp & tcp small servers
Enabling service password encryption
......
Securing Forwarding plane services..
Enabling CEF (it might have more memory requirements on some low end platforms)
Configuring the named acls for Ingress filtering
autosec_iana_reserved_block:This block may subject to change by iana and for updated list
visit www.iana.org/assignments/ipv4-address-space.
......
```

e global services that could be

ten necessary global services (e.g.

e interface services that could be

rices

uter performance under SYN attacks

ation) to mitigate SYN-flood attacks

le interfaces for firewall images

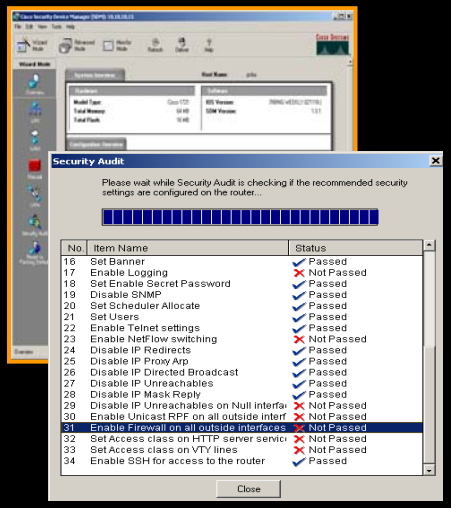
pp packets with obviously spoofed IP

packets with obviously illegal IP source

Security Device Manager (SDM) 2.0

Cisco.com

Integrated Management of Router Services – Routing, Switching, Security, QoS



- New Security Features
  - Inline IPS with Dynamic Signature update and signature customization
  - Role-Based Router Access
  - Easy VPN Server and AAA
  - Digital Certificates for IPSec VPNs
- New Wizards for non-experts
  - QoS Policy and NBAR
- New Troubleshooting tools
  - VPN, WAN connection
- Major UI Improvements - Router Services Dashboard, Task-based Navigation
- Real-Time and Graphical router and network resource monitoring

요약

Self-Defending Network 의 적용

Cisco.com

End Point Posture Enforcement
Network Admission Control, Identity Based Services

Network Device Protection
Control Plane Policing, CEF, Port Security, Broadcast Suppression BPDU Guard

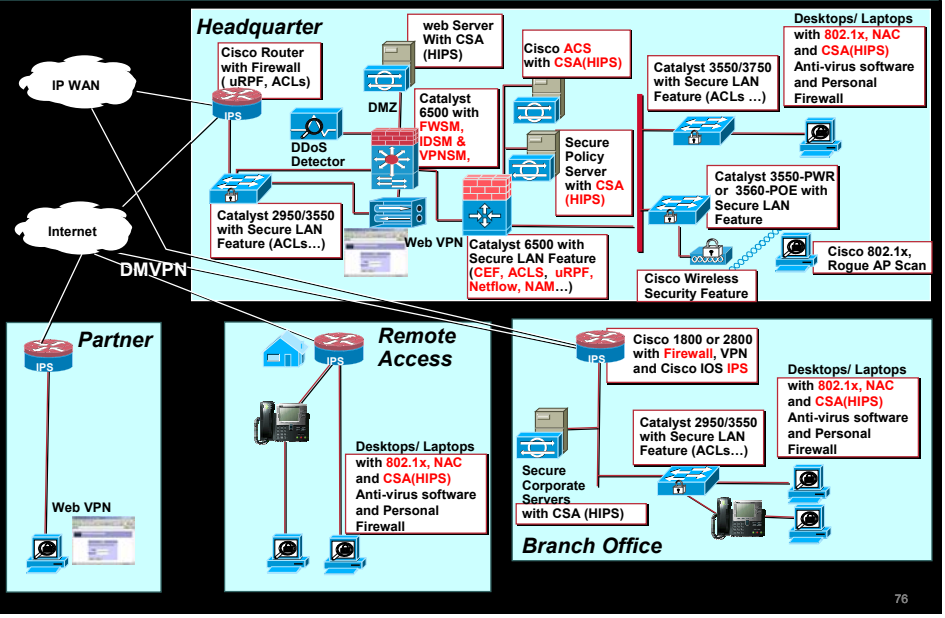
Dynamic/ Secure Connectivity
VLANs and Secure VPNs

Dynamic Communication Between Elements
DHCP Snooping, Dynamic ARP inspection, IP Source Guard

Automated Threat Response
Cisco Security Agent

기업 End-to-end 보안 네트워크 구조

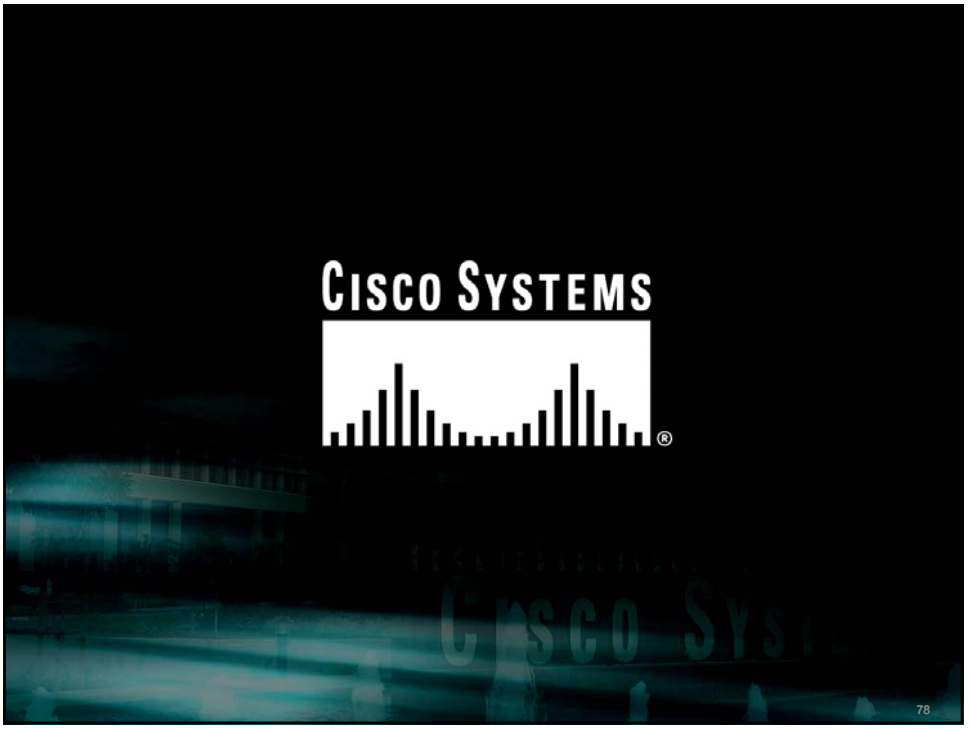
Cisco.com



76

Q and A

77


CISCO SYSTEMS