엔터프라이즈 LAN/WAN 보안 구현 방안

한 현철

Cisco Systems Korea

- 전반적인 보안 솔루션에 관한 정리
- LAN/WAN 환경에서의 보안 솔루션 구현 방안
- Network과 Security와의 연관 관계

목 차

- 보안에 대한 고려 사항
- 네트워크 보안 정책
- 보안 기술별 고려 사항
- LAN 환경 보안 구현 모델
- WAN 환경 보안 구현 모델
- 결 론

보안에 대한 고려 사항

지속적으로 나타나는 보안 위협들

보안 위협 철학의 변화 : Fame to Profit, Less Noisy, More Sophisticated

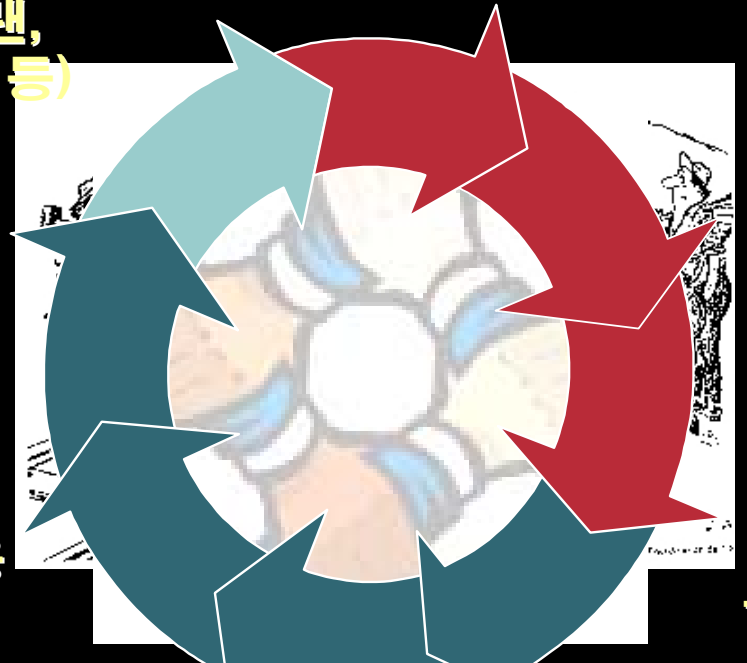
웜과 바이러스의 변화 : Bot-Net의 등장, Spy/Adware의 확산, 다양한 변종

DoS공격의 확대 : Distributed DoS공격의 확대, Application 레벨로의 확대

메세징 보안 위협 : Phishing & Pharming 위협, SPAM/SPIM 의 확산

Security Everywhere : Port Overloading 공격, Appliction 레이어 공격

보안 대응을 위한 고려 사항



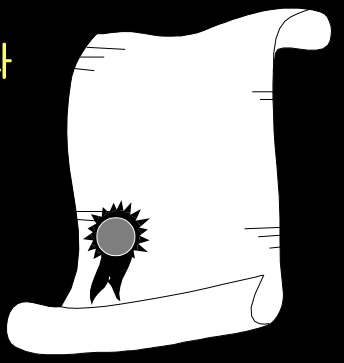
네트워크 보안 정책

네트워크 보안을 위한 지침들

1. Network 보안은 시스템이다.
2. 모든것은 Target(공격대상)이자 Weapon(공격무기)
3. 보호의 대상이 명확해야 한다.
4. 보안 기술에 대한 이해가 필요하다.
5. 100%는 없다.– 준비와 대응

"**Security Policy(**보안 정책)는 어떤 사람들이 조직의 기술이나 정보자산에 접근할 수 있는지, 그리고 그 사람들이 반드시 지켜야 하는 규정들을 집합한 공식적인 성명서이다.

RFC 2196, Site Security Handbook

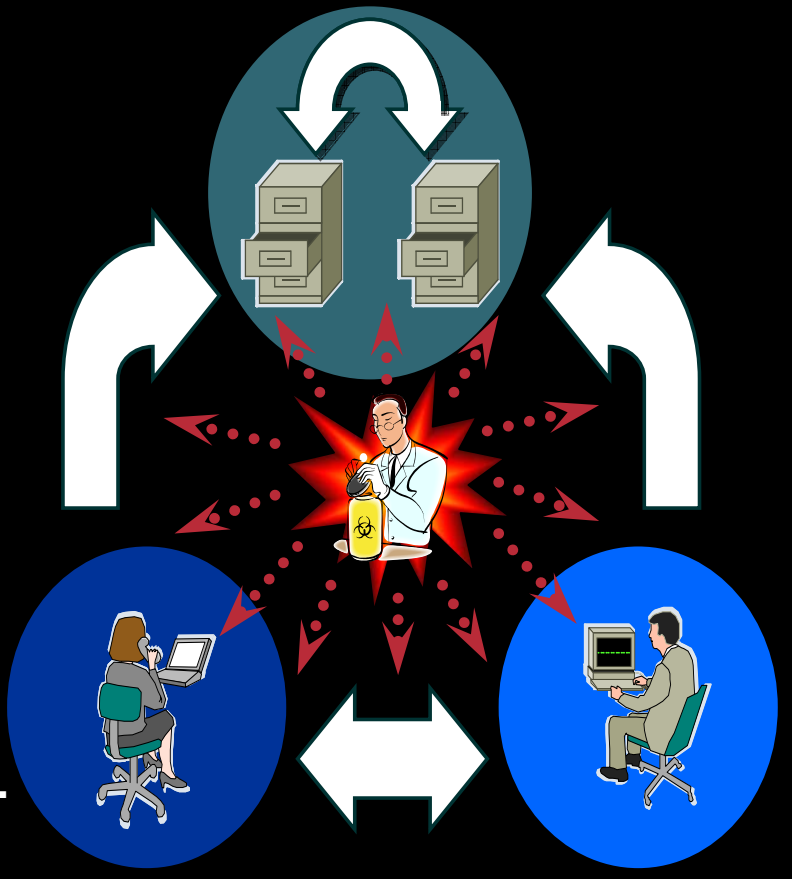


1. Network 보안은 시스템이다.

- **"Network Security = Firewall + AV"**
  이란 공식은 더 이상 일반론이 아니다.

- **"Network Security System"** 규정
  정보 자산에 대한 보안**(Security)**을
  제공하기 위해 상호 보완적인 방법으로
  작업하는, 네트워크와 연결된 장비들,
  기술들 그리고 최선의 연습들의 집합체
  출 처: **"Network Security Architectures"**

- 보안은 더 이상 개별적인 영역이 아니다.
  ; 내/외부 보안, 네트워크/서버/사용자 보안,
  유/무선 보안....



2. 모든것은 Target(공격대상)이자 Weapon(공격무기)

- 서버와 호스트들(단말기들)

  ; 보안 공격의 대상이자 공격을 위한 거점들

  - **Worm / DoS** 공격의 피해자이자 가해자
  - **DNS** 서버(**DNS**서비스 중단, **Pharming**)
  - **DHCP** 서버를 통한 공격(**IP**고갈, **DHCP Snooping**)

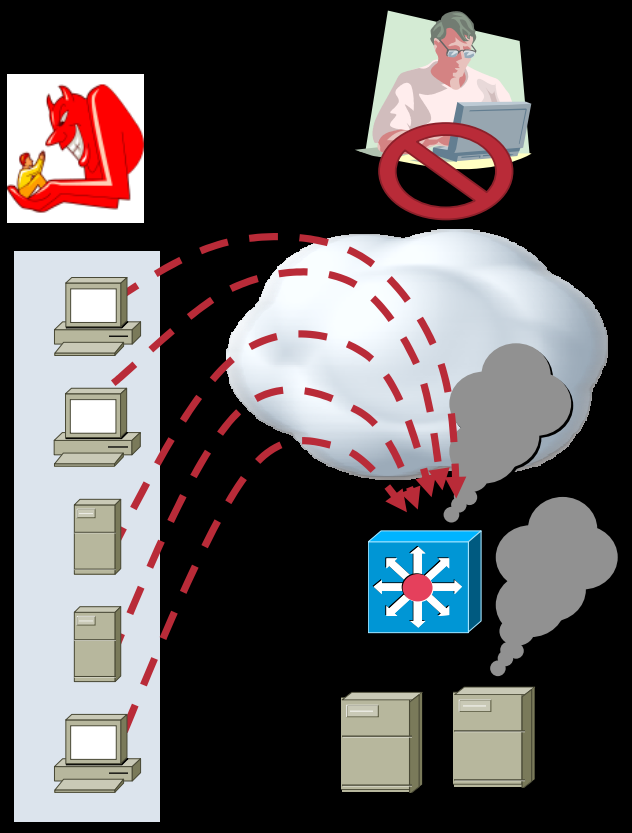
- 네트워크 장비들(라우터,스위치)

  ; 보안 공격의 통로이자 서비스 중단 공격

  (**DoS**공격)의 피해자들

  - 네트워크 장비 본연의 서비스 중단 **->** 업무 중단
  - 네트워크 **Capacity**의 고갈로 인한 비즈니스 중단
  - **Man-in-the-Middle** 공격을 통한 정보 유출

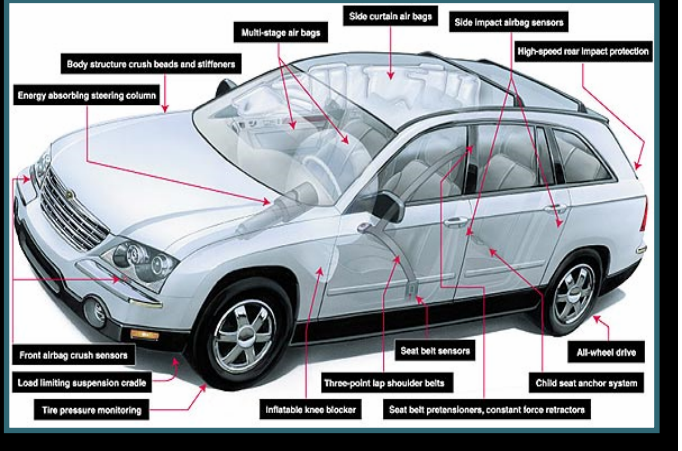
- **IT**전반에 대한 이해(예: **IT**서비스, 트래픽 흐름 등)가 요구



3. 보호의 대상이 명확해야 한다.

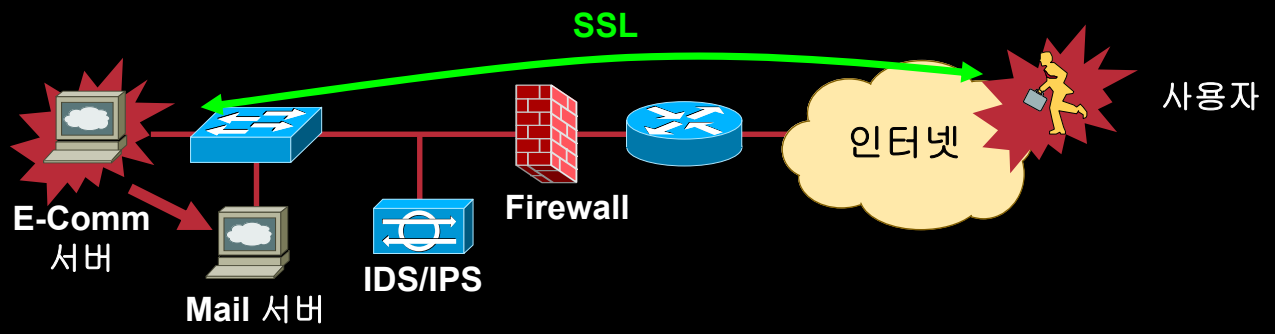
- 보안위협으로부터 무엇을 보호해야 하는가?
  - 어떤 보안 위협들이 있는가?(해킹, 서비스 중단)
  - 보호의 대상은 어떤것들인가?(정보, 서비스, 사용자, 시스템 리소스, 네트워크 리소스)
  - 보호하기 위한 사전 조치는 무엇인가?(정책, 교육, 보안 솔루션 구성)
  - 보안 위협에 대한 대응은 어떻게 할것인가? (모니터링, 조치 프로세스, 신규 솔루션 도입)

- 보안 도메인 구분 및 중요도의 규정
  - 인트라넷 **vs** 엑스트라넷 **vs** 인터넷
  - 내부용 서버 **vs** 엑스트라넷 서버 **vs** 공개용 서버
  - 서버 도메인 **vs** 사용자 도메인
  - 일반 사용자 **vs** 외부 사용자 **vs** 중요 사용자
  - **More…**



4. 보안 기술에 대한 이해가 필요하다.

- 어떤 보안 기술들을 어떻게 사용해야 하는가?
  - **Perimeter Security(경계선 보안)**
    : **Firewall, Access Control Lists, N/W Design(LAN, WAN 설계)**
  - **Application Level의 보안**
    : **Network IPS, HOST IPS, Anti-Virus**
  - **Secure Connectivity(암호화된 연결)**
    : **IPSec VPN, SSL VPN , 무선 랜 암호화**
  - 사용자 보안
    : 사용자 인증(**802.1x** 유/무선), 단말 인증(**NAC**), **N/W Design**(IP 라우팅, **VLAN**)
  - 내부 **Network Infra** 보안
    : 라우터/스위치 보안 기술들, (유해)트래픽 모니터링

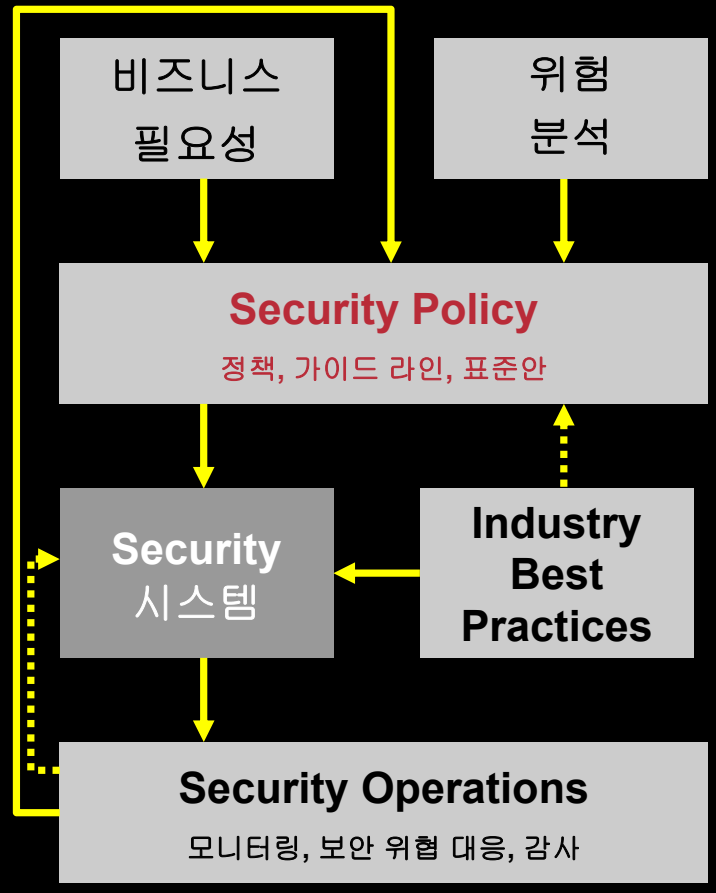


5. 100%는 없다. – 준비와 대응

- 보안은 **Risk Free**가 아닌 **Risk Reduce** 전략
- 알려진 보안 위협에 대한 준비 및 대응
- 알려지지 않은, 새로운 보안 위협에 대한 지속적인 관심 및 대응 방안 구현

Security Policy(보안 정책) 구성 및 구현

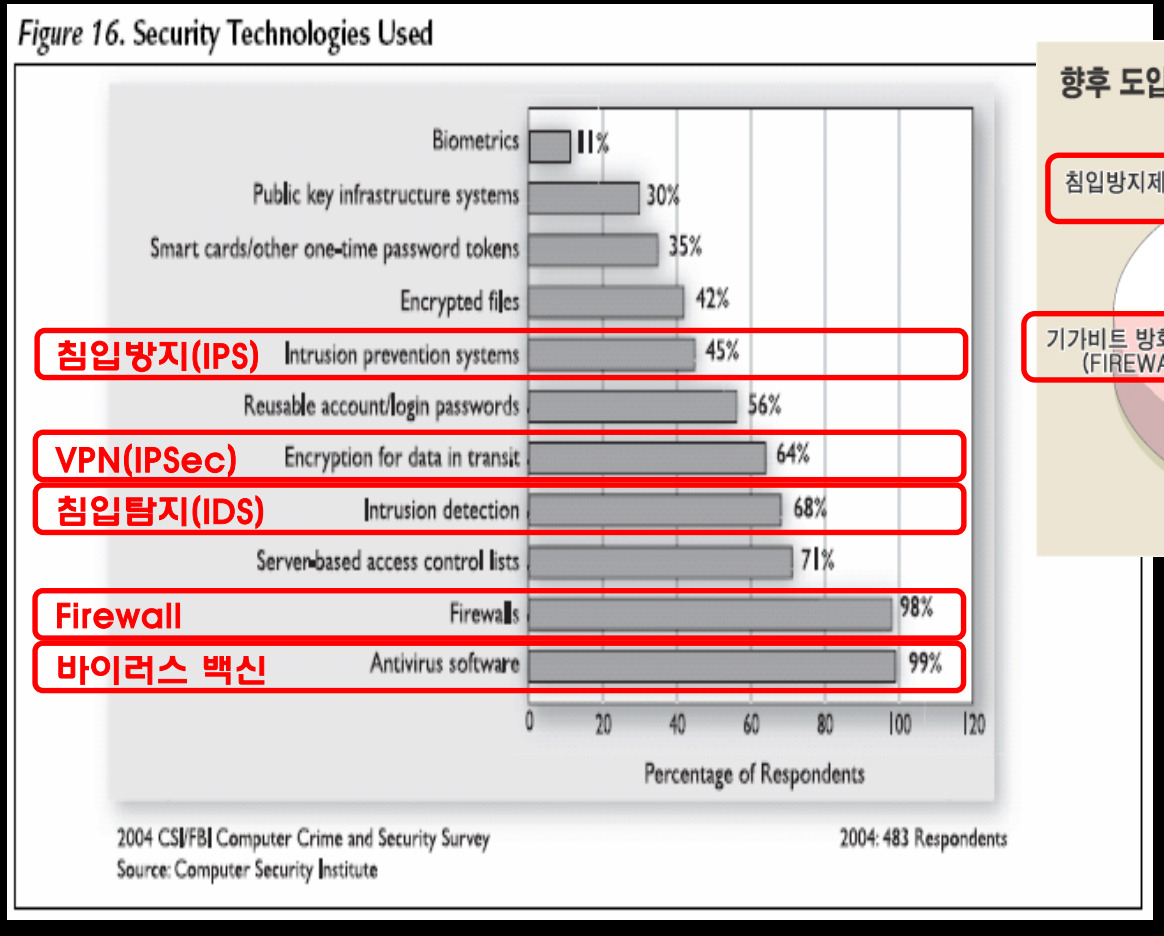
- 네트워크 사용 권한과 영역에 대한 규정
- 신원 증명 방법 및 인증 방법에 대한 규정
- 인터넷 사용 정책
- 내부 네트워크 접속 정책
- **Remote access** 정책
- 내부 사용자 보안 교육 및 정보 제공 방법
- 보안 사고 대응 방법에 대한 정책
- **More…**

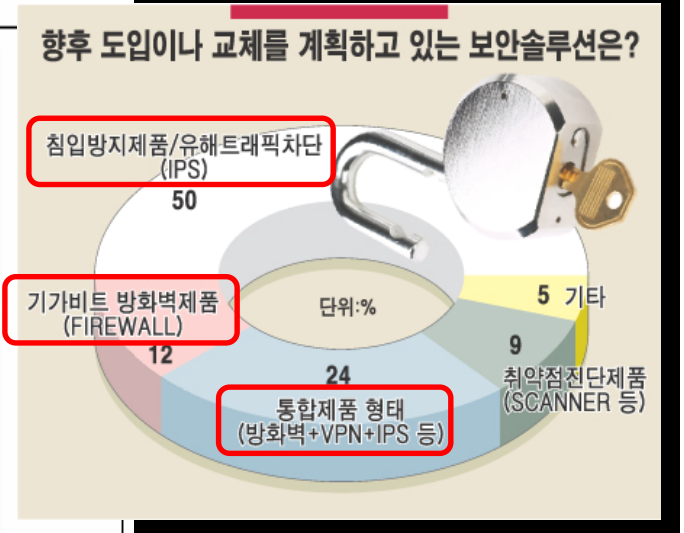


[Security System Cycle]

보안 기술별 고려 사항

현재 많이 사용되는 보안 기술들





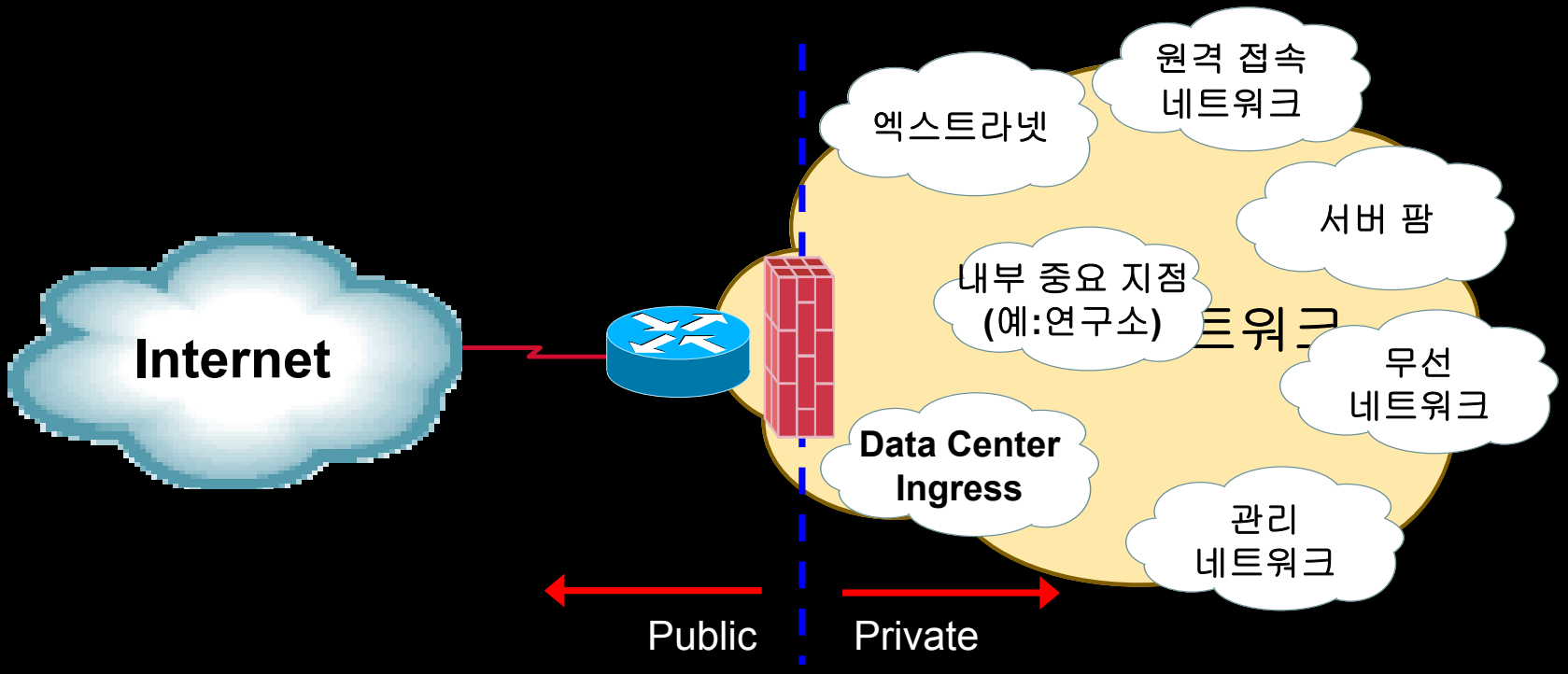
2004년 국내 IT관리자 대상 설문

출 처: **CSI/FBI 2004 Computer Crime and Security Survey**

1. Perimeter Security (경계선 보안)

F/W, ACL

- 보안 경계선에 대한 새로운 접근



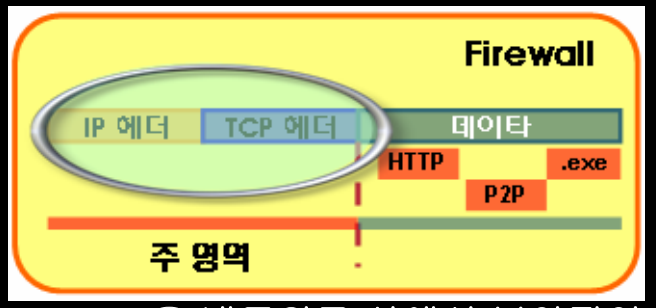
- 내부(**Private**)에서 발생하는 보안 위협들의 증가로 인해 내부 네트워크에서 보안적으로 경계가 강력하게 구분되어야 하는 곳은 **Firewall**(또는 **Access Control List**)이 적용될 수 있는
  모든 지점

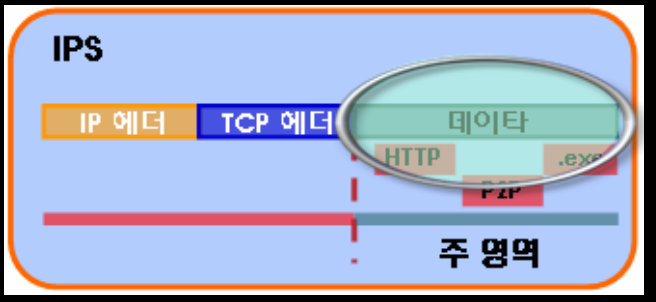
1. Perimeter Security (경계선 보안)

F/W, ACL

- **Firewall**에 관하여

  ✓ **IPS(Intrusion Prevention System)**에서 차단까지 되는데, 굳이 **Firewall**이?





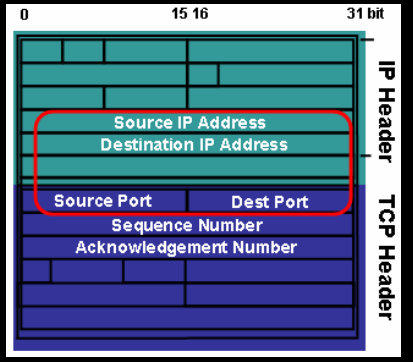
Firewall은 네트워크 상에서 보안적인 경계선을 만드는 것이 **1**차 목적

-> 접근 자체에 대한 보안 정책 구현시 요구

  ✓ 네트워크 내부에 보안이 필요한 경계선마다 **Firewall**을 모두 놓는다면?

- **Router/Switch**의 **ACL**
  (VACL, RACL, PACL,
  Time-based ACL, etc)

- **Firewall** 기술의 **Embeded**
  (Router IOS F/W,
  Switch FWSM 모듈 **etc)**

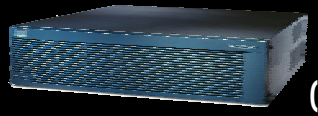
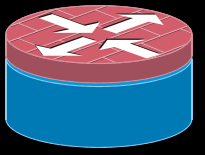
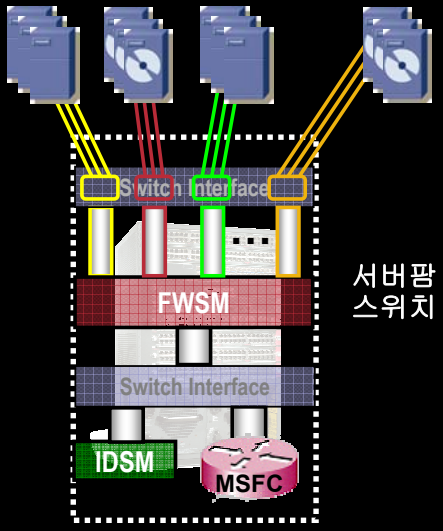
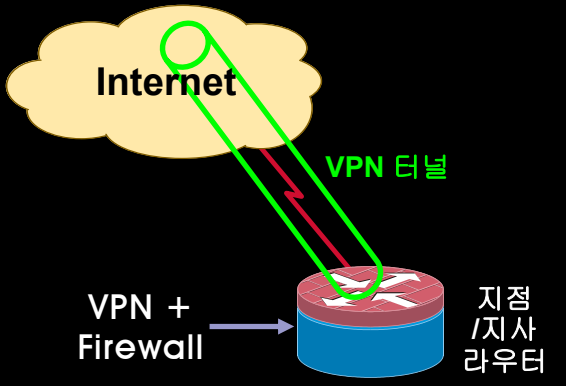


ACL

1. Perimeter Security (경계선 보안)

F/W, ACL

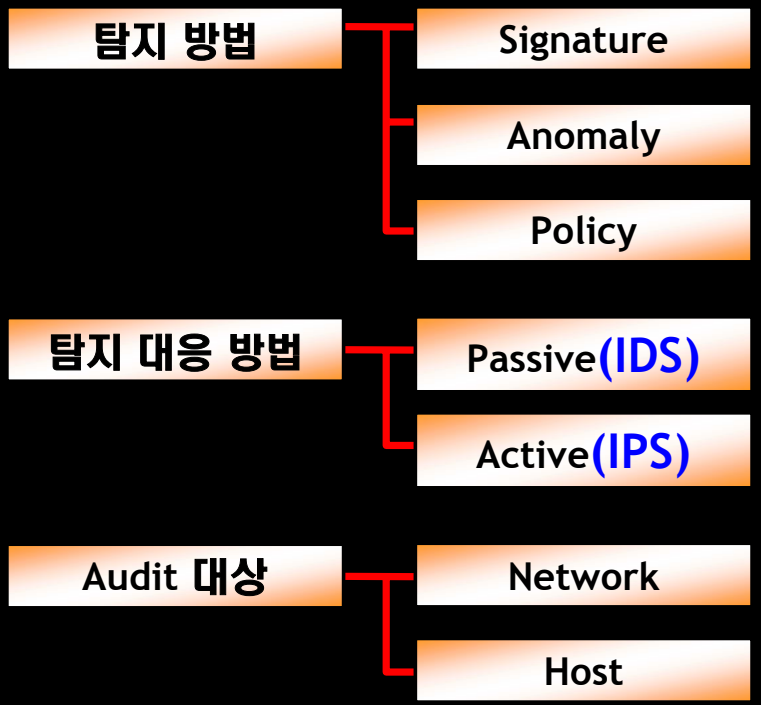
- **Cisco Firewall**의 종류

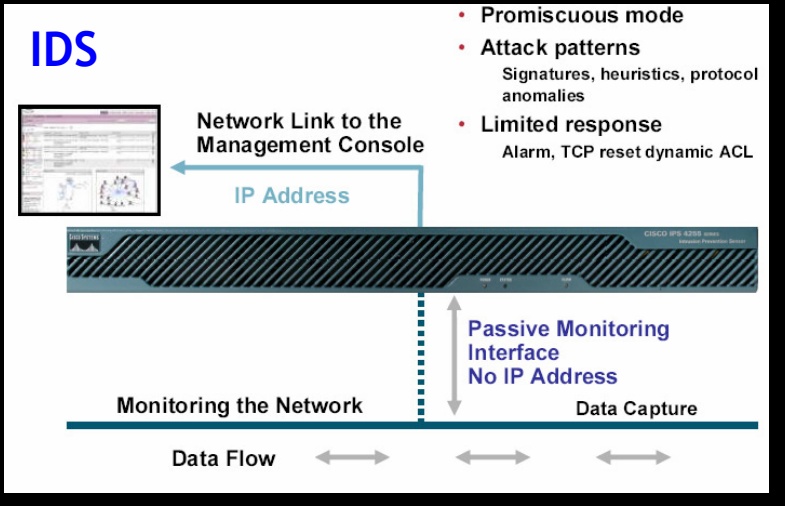
Appliance(Box형) 타입	Integrated(모듈형) 타입	Embeded(포함형) 타입
PIX F/W 	FWSM (w/Cat6500) 	IOS Firewall 
ASA 5500 	 서버팜 스위치	
Cat6503 (with Sup32 + FWSM) 		
 Sup32		

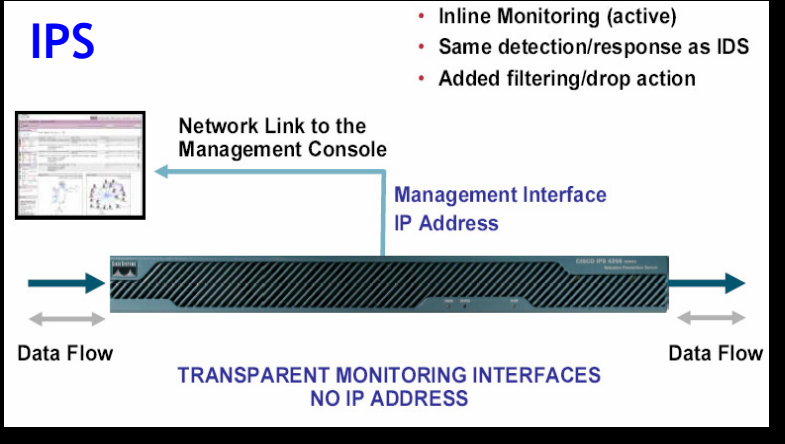
- 필요 성능, **Design(구성)**, 필요 포트수, 다른 기능과의 연계(다른 보안 기능과의 연계, 다른 서비스와의 연계 (예: 음성 서비스) ,관리 등을 고려하여 선택

2. Application Level의 보안

- IDS(Intrusion Detection System) / IPS(Intrusion Prevention System)



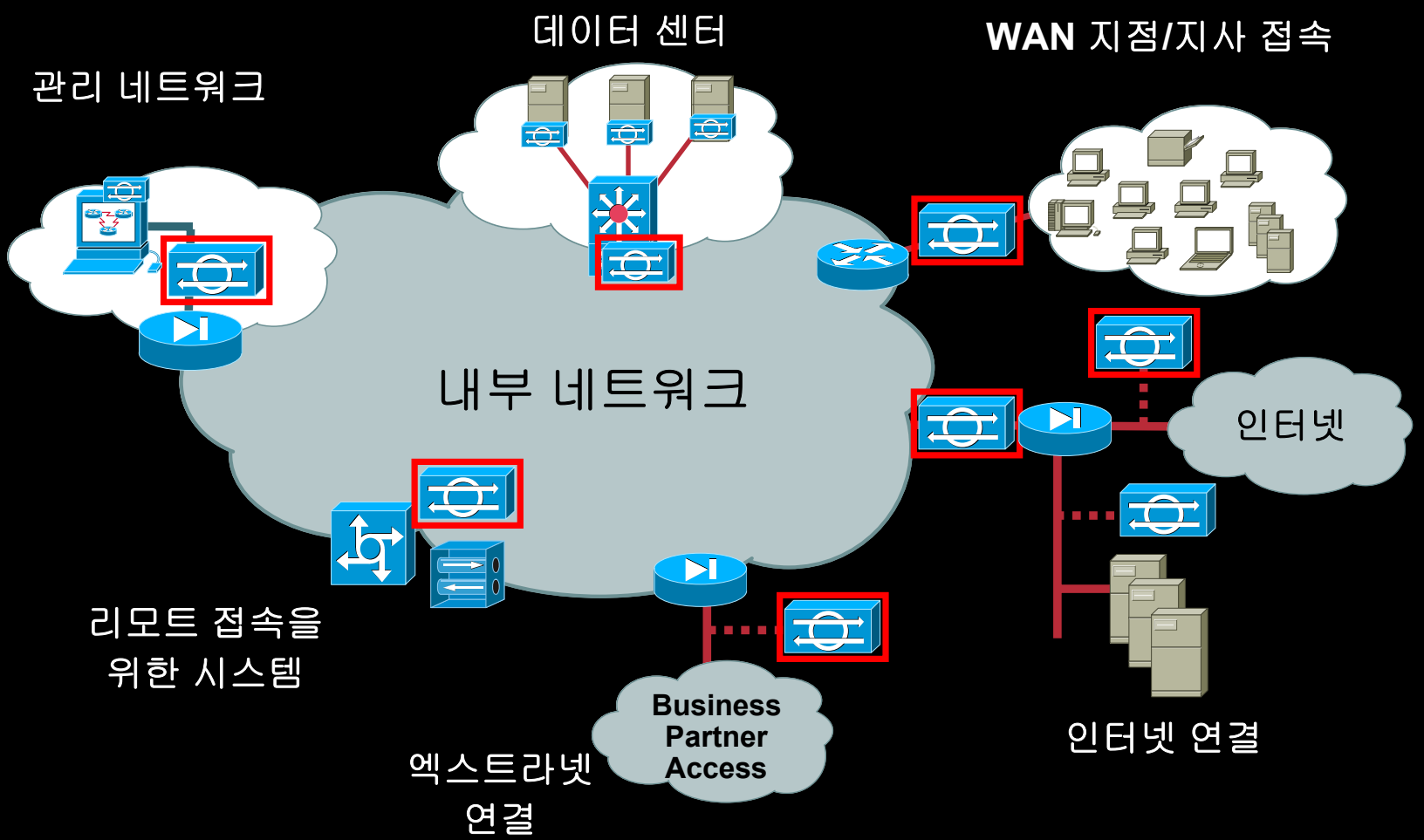




2. Application Level의 보안

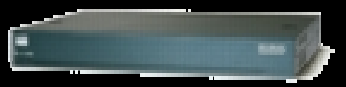
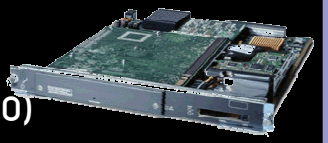
IDS / IPS

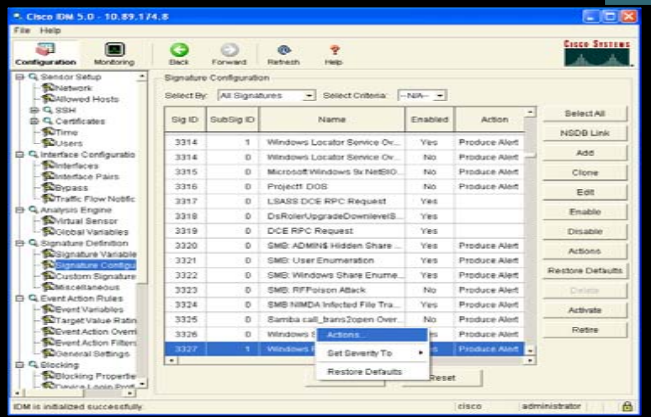
- **IDS/IPS** 구성시 고려 사항 – **Where are the Points ?**

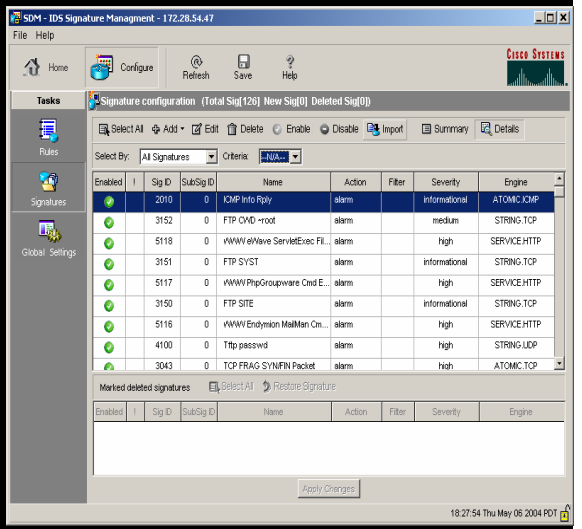


2. Application Level의 보안

- **Cisco IDS/IPS**의 종류

Appliance(Box형) 타입	Integrated(모듈형) 타입	Embeded(포함형) 타입
IPS 4200 	IPSM (w/Cat6500) 	IOS IPS 
ASA 5500 	Router IDS 모듈 	

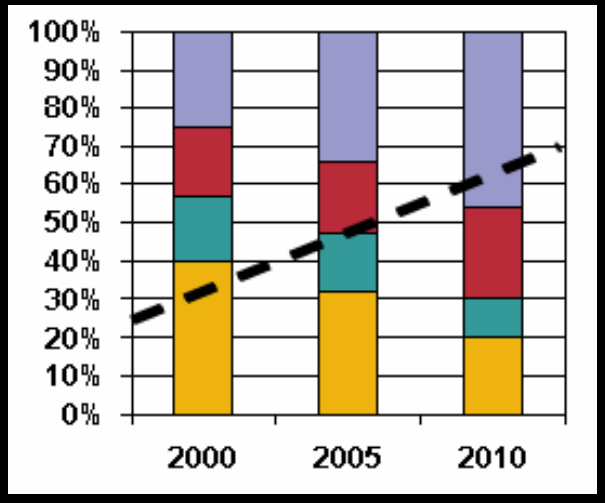




- 필요 성능, **Design(구성)**, 다른 기능과의 연계(다른 보안 기능과의 연계), 관리 등을 고려하여 선택

3. Secure Connectivity(암호화된 연결)

- **VPN(Virtual Private Network)** 의 개요



다른 시간, 다른 장소

같은 시간, 다른 장소

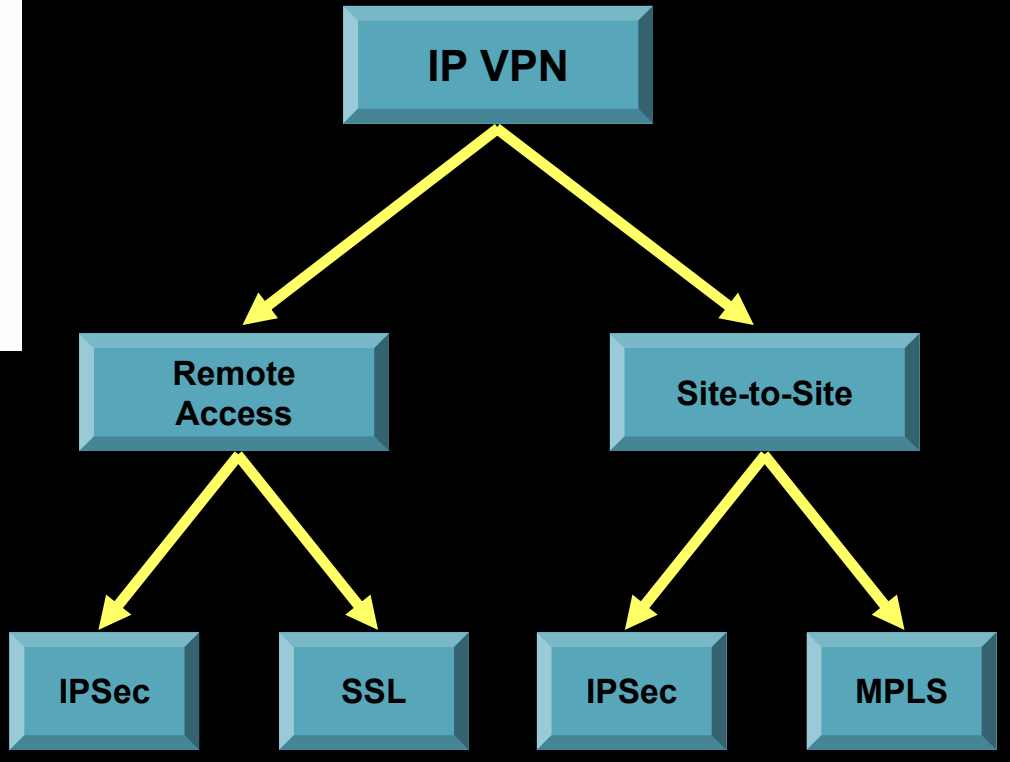
같은 시간, 같은 장소

혼자서 일함

다른 사람/조직과 같이 일하는 비율

The Change in How Work Is Done

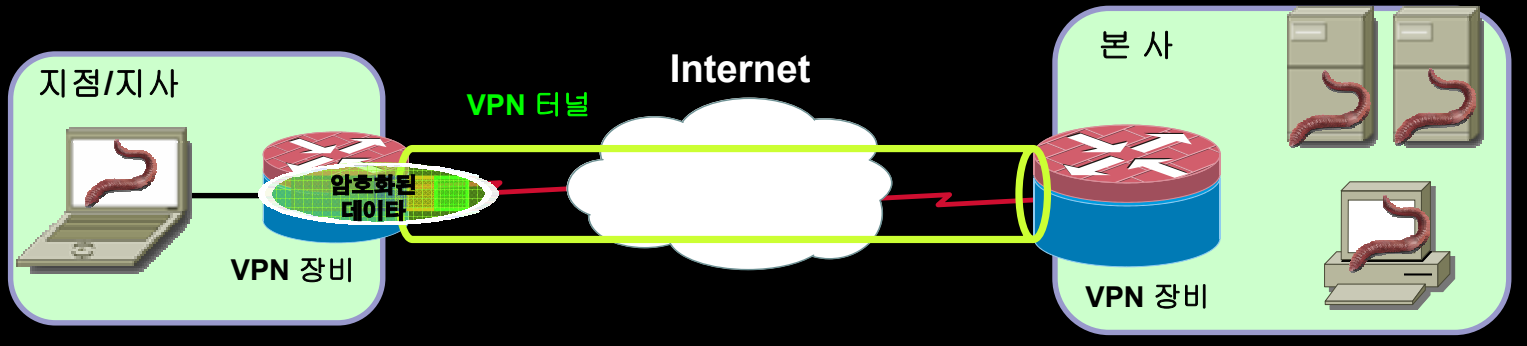
출 처: **Gartner** 그룹



3. Secure Connectivity(암호화된 연결)

- **VPN = Security ?**

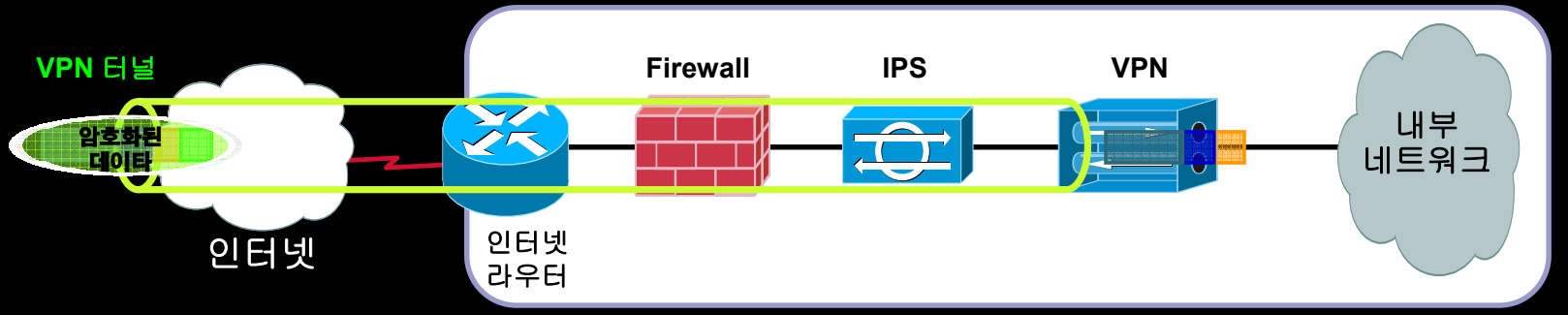
  ✓ 우리 지사는 **ADSL**을 이용한 **VPN**을 사용하는데 충분한 보안**(Security)**이 구현?

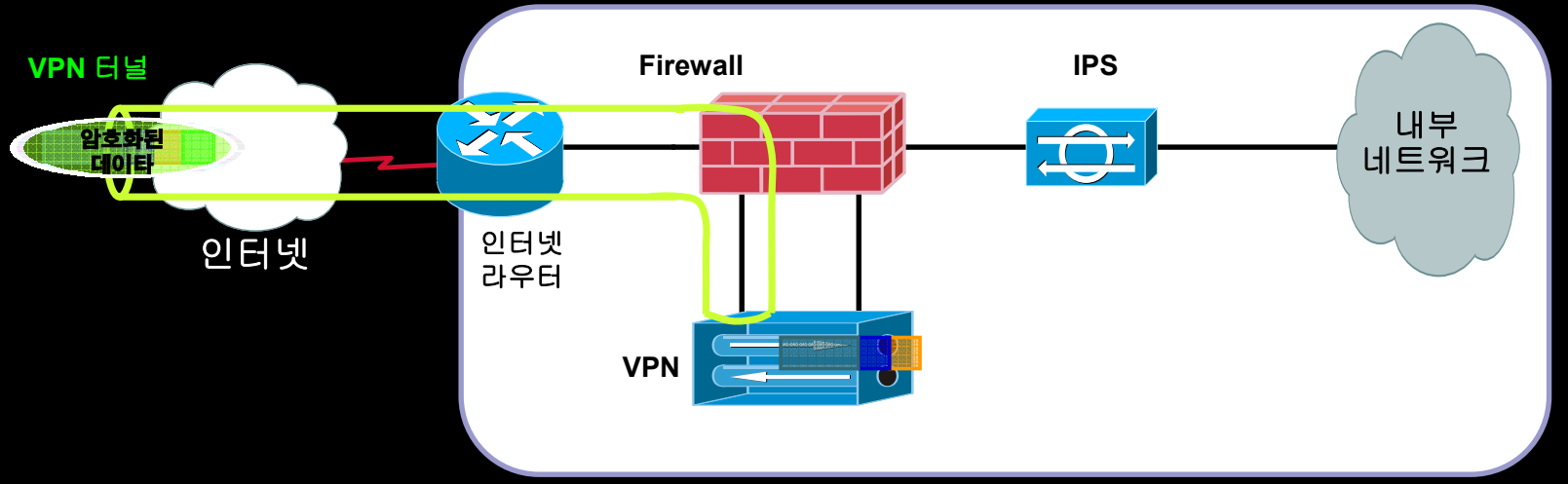


- **VPN**은 데이타의 기밀성**(Confidentiality)**을 제공(데이타의 중간 유출 위협 방지) 해주는 기술...
  그러므로 데이타의 보안**(Security)**은 다른 보안 요소와 함께 구현되어야 함.

3. Secure Connectivity(암호화된 연결)

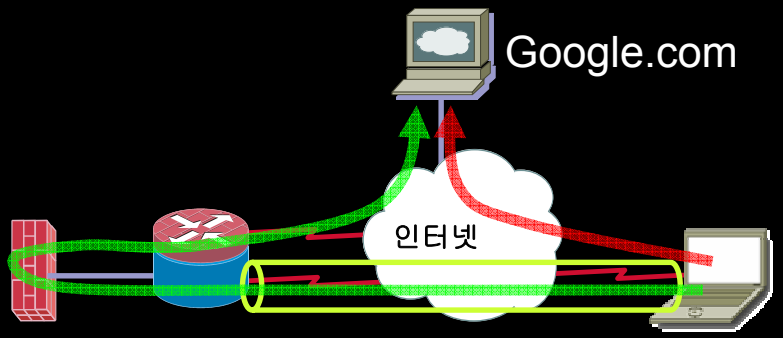
- **VPN**의 디자인
  - ✓ 그럼 다른 보안 요소와 어떻게 함께 구성되어야 효과적인가?





3. Secure Connectivity(암호화된 연결)

- **More ?**



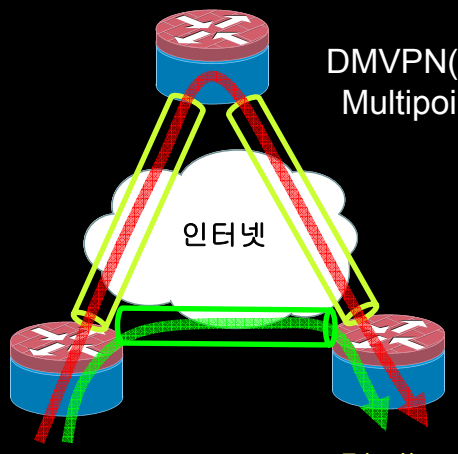
Split Tunneling

IPSec VPN or SSL VPN

Dedicated VPN Infrastructure

Integrated Routing Infrastructure

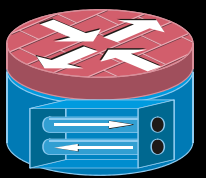
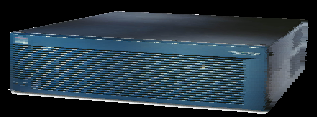
VPN 장비



Connectivity 형태
(Hub&Spoke or Full-Mesh)

3. Secure Connectivity(암호화된 연결)

- **Cisco VPN**의 종류

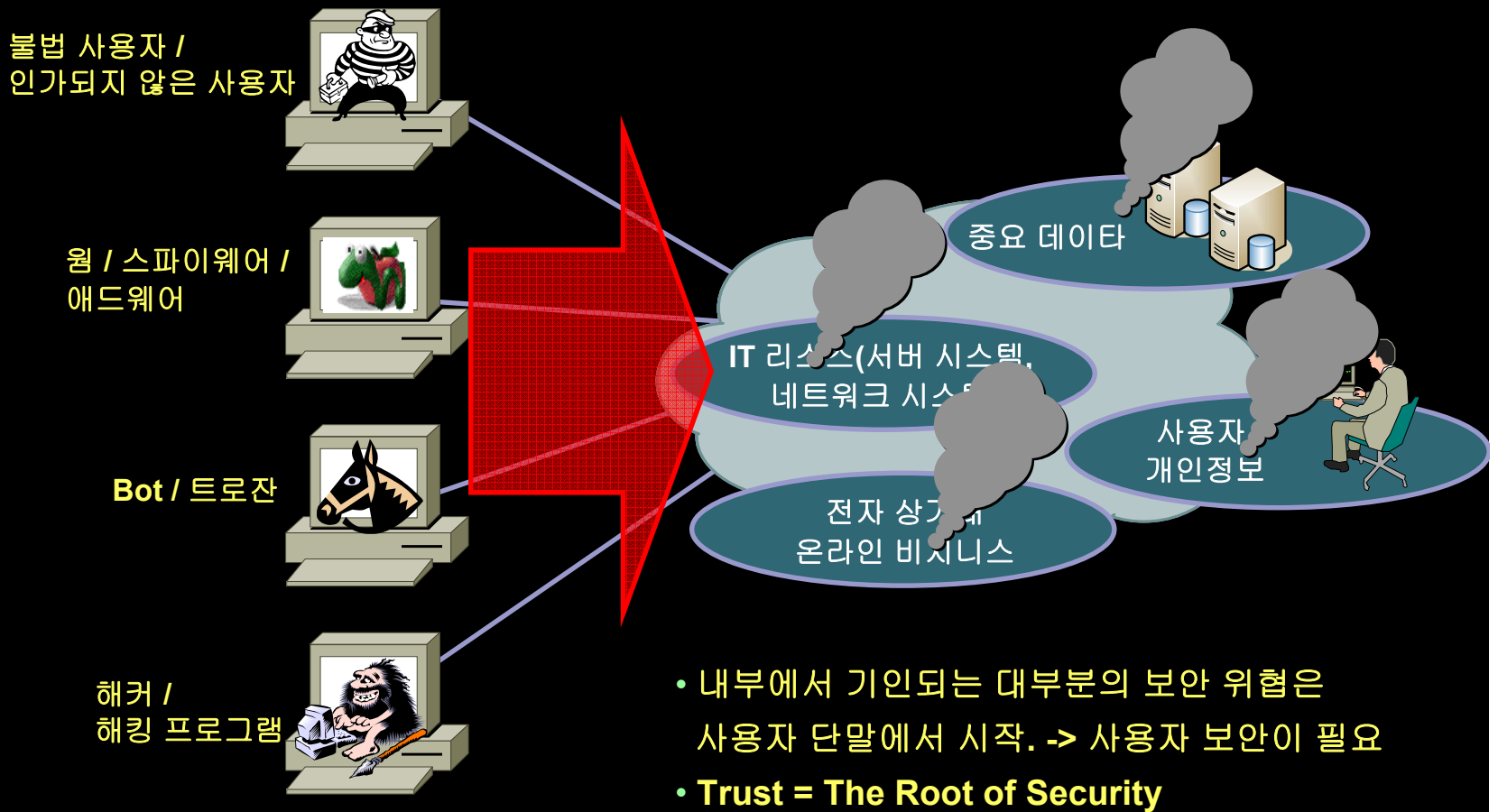
Appliance(Box형) 타입	Integrated(모듈형) 타입	Embeded(포함형) 타입
VPN 3000 	IPSec VPN모듈 	IOS VPN 
ASA 5500 	SSL VPN모듈 	
  IPSec VPN과 SSL VPN 동시지원	라우터 VPN 가속기 모듈 	VPN 가속기 모듈
PIX F/W 		

- 필요 성능, **Design(구성)**, 다른 기능과의 연계(다른 보안 기능과의 연계, 다른 서비스와의 연계 (예: 음성 서비스, 멀티캐스트를 통한 방송) 등을 고려하여 선택

4. 사용자 보안

802.1x / NAC / Host IPS

- 사용자 보안에 대한 새로운 접근

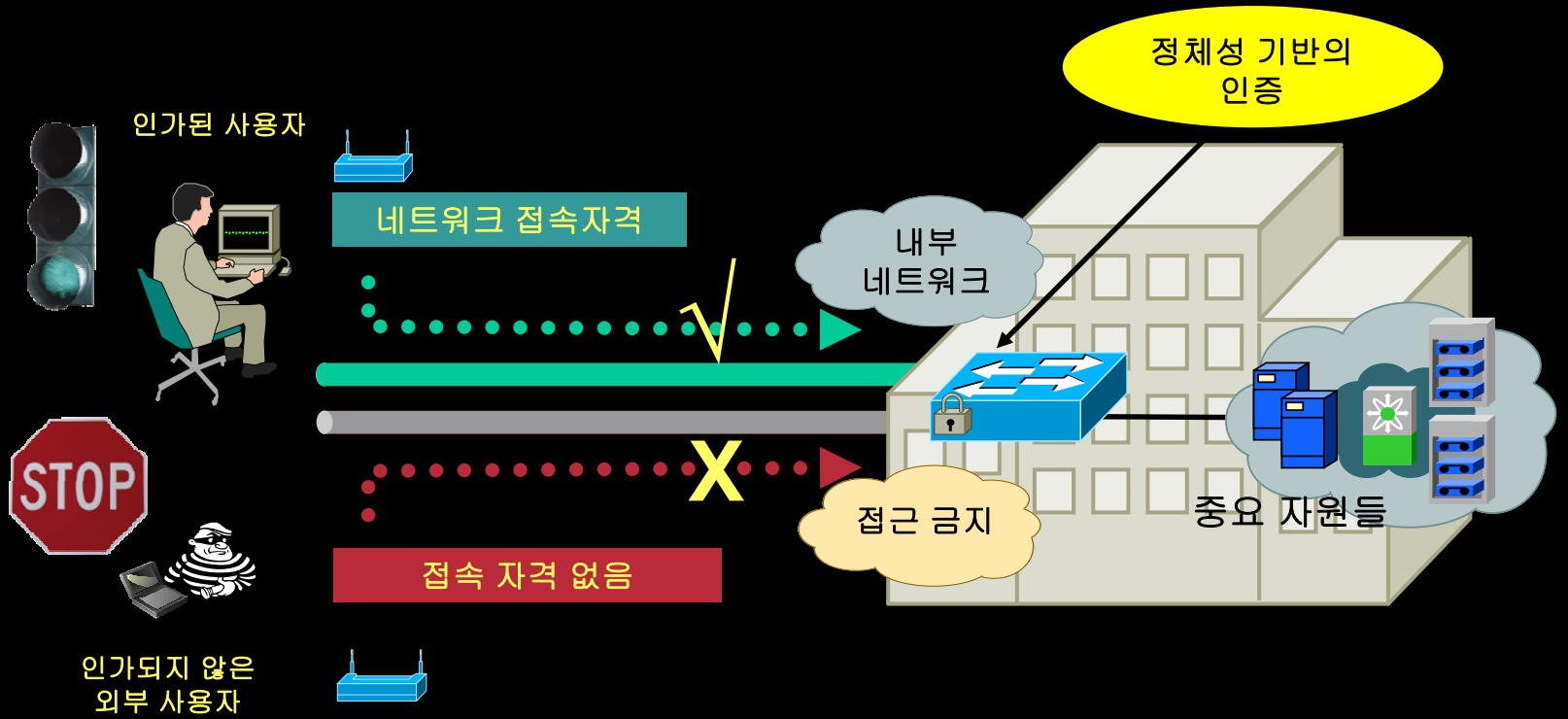


- 내부에서 기인되는 대부분의 보안 위협은 사용자 단말에서 시작. -> 사용자 보안이 필요
- **Trust = The Root of Security**

4. 사용자 보안

802.1x / NAC / Host IPS

- **802.1x** 기반의 사용자 인증**(IBNS; Identity Based Networking Services)**



- 내부 네트워크의 사용 여부에 대한 정책 규정 – 정규 사용자, 외부 사용자 (외주업체, 방문객등), 불법 사용자에 대한 네트워크 사용 여부 및 접속 권한등
- 무선 인증 및 유선 인증의 사용 여부에 대한 정책

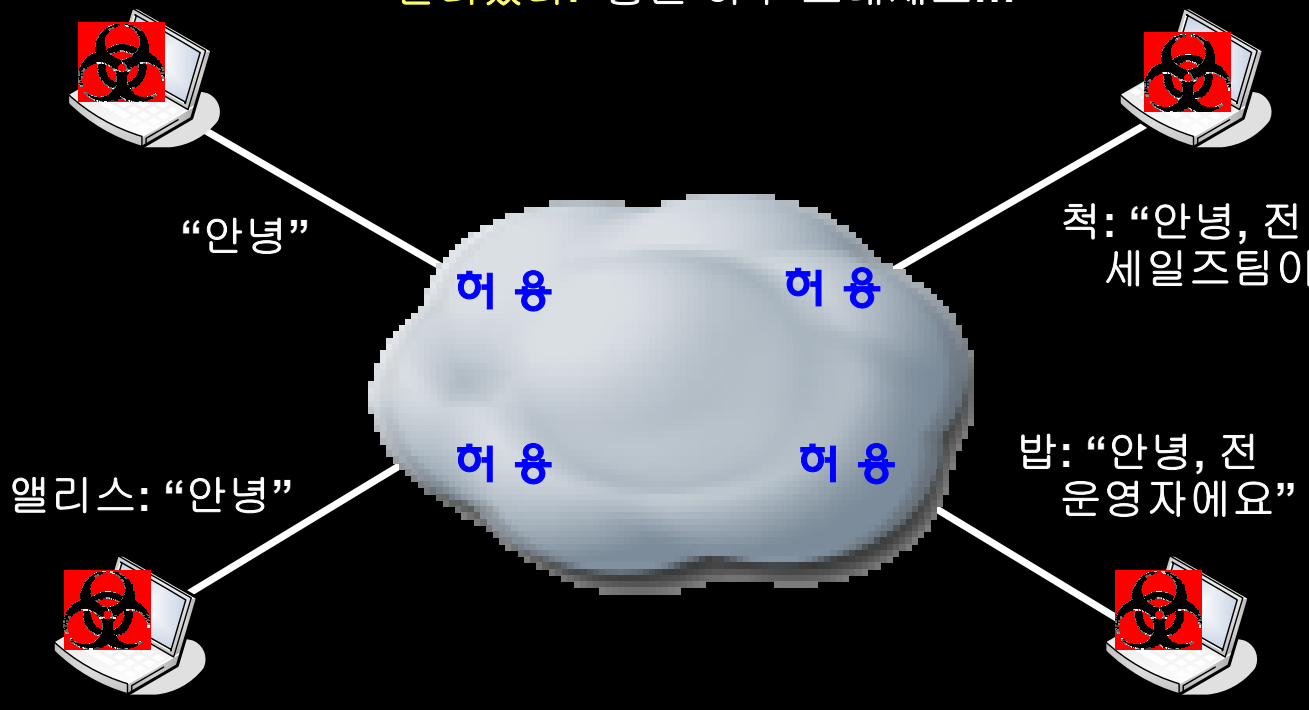
4. 사용자 보안

802.1x / NAC / Host IPS



- 단말기에 대한 인증 – **NAC(Network Admission Control)**

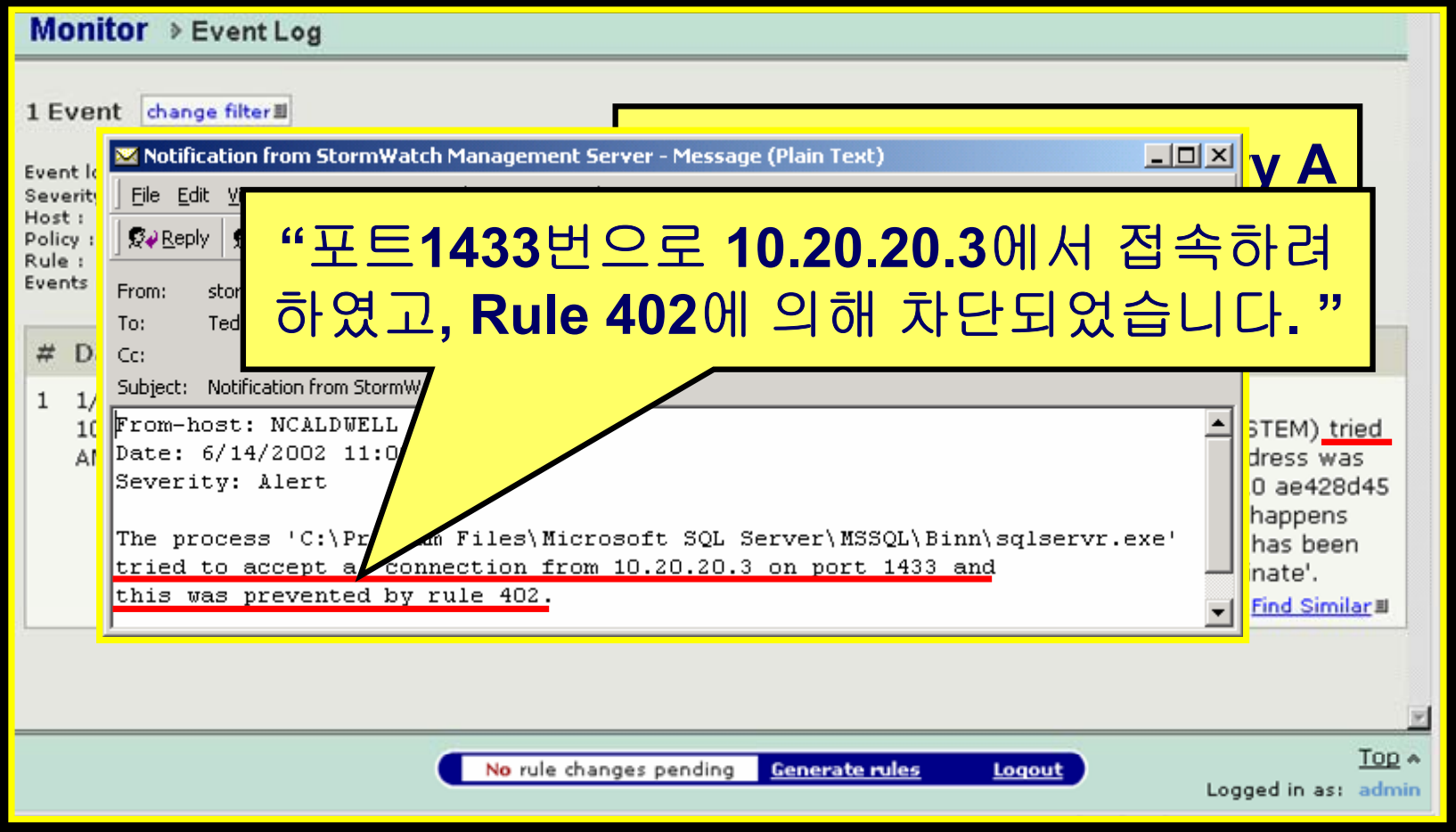
척은 **unpatched Windows 2000 system**을 이용하고 **Gigabit Ethernet**으로 연결되 있으며, 척의 **PC엔 Worm**이 깔려있다. 좋은 하루 보내세요...



4. 사용자 보안

802.1x / NAC / Host IPS

- 새로운 공격 / 단말기 대상의 **Application** 레벨 공격 차단 – **Host IPS(CSA)**



5. 내부 Network Infra 보안

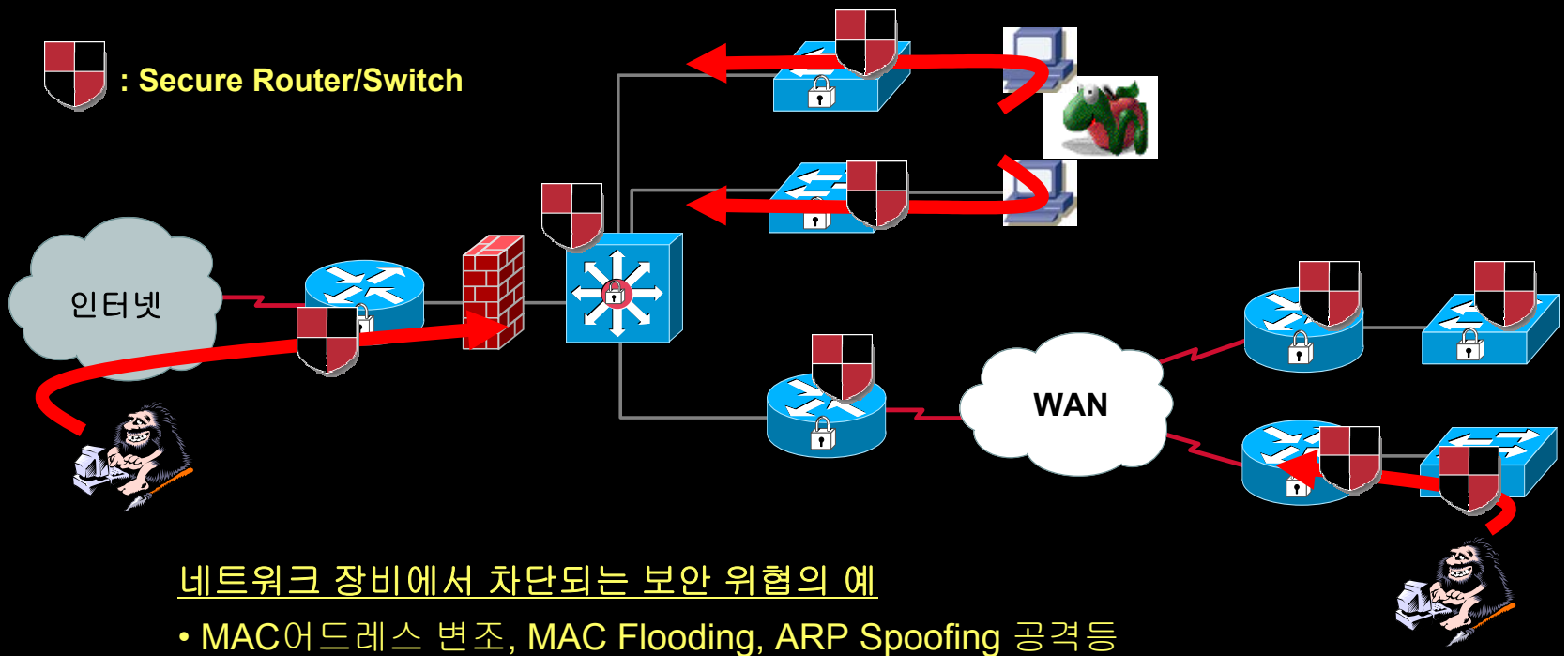
Router / Switch

- 네트워크 장비에 가해지는 또는 경유하는 보안 공격의 영향들

5. 내부 Network Infra 보안

Router / Switch


• 네트워크 장비에 가해지는 또는 경유하는 보안 공격의 영향들



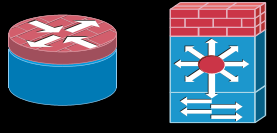
네트워크 장비에서 차단되는 보안 위협의 예

- MAC어드레스 변조, MAC Flooding, ARP Spoofing 공격등
- IP어드레스 변조, Scanning, ICMP Flooding 공격, DHCP 공격등
- TCP Syn Flooding, UDP Flooding 공격, Broadcast Storm 공격등
- 사용 Port가 알려진 Worm, 바이러스등의 악성 코드

5. 내부 Network Infra 보안

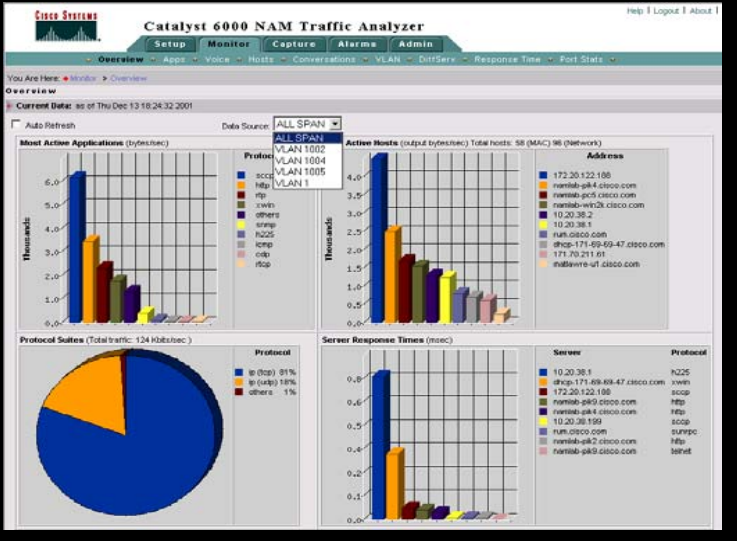
Router / Switch


- 네트워크 관리의 확장 – 트래픽 모니터링 **(Netflow, NAM)**
  - 우리 네트워크상에 어떤 트래픽들이 돌아다니나?
  - 우리 네트워크를 사용하는 트래픽의 분포는 어떤가?
  - 혹시 웜이나 바이러스와 관련된 유해 트래픽은 돌아다니지 않는가?
  - 혹시 부적절한 트래픽(**P2P**, 음란 동영상…)은 돌아다지니 않는가?
  - 어떤 사용자가 유해 또는 부적절한 트래픽을 사용하고 있는가?
  - **More**



Netflow기술

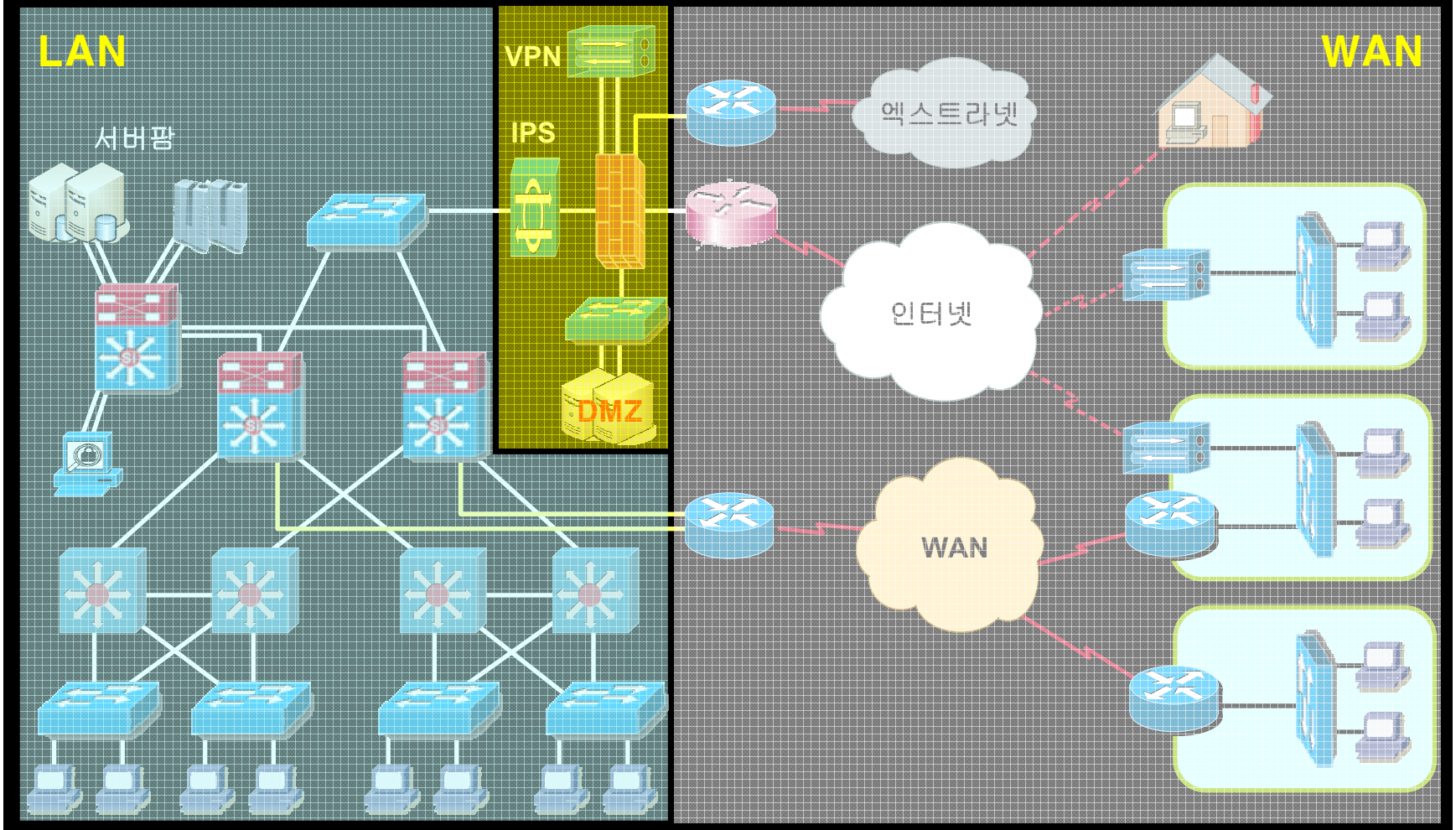
NAM



LAN 환경 보안 구현 모델

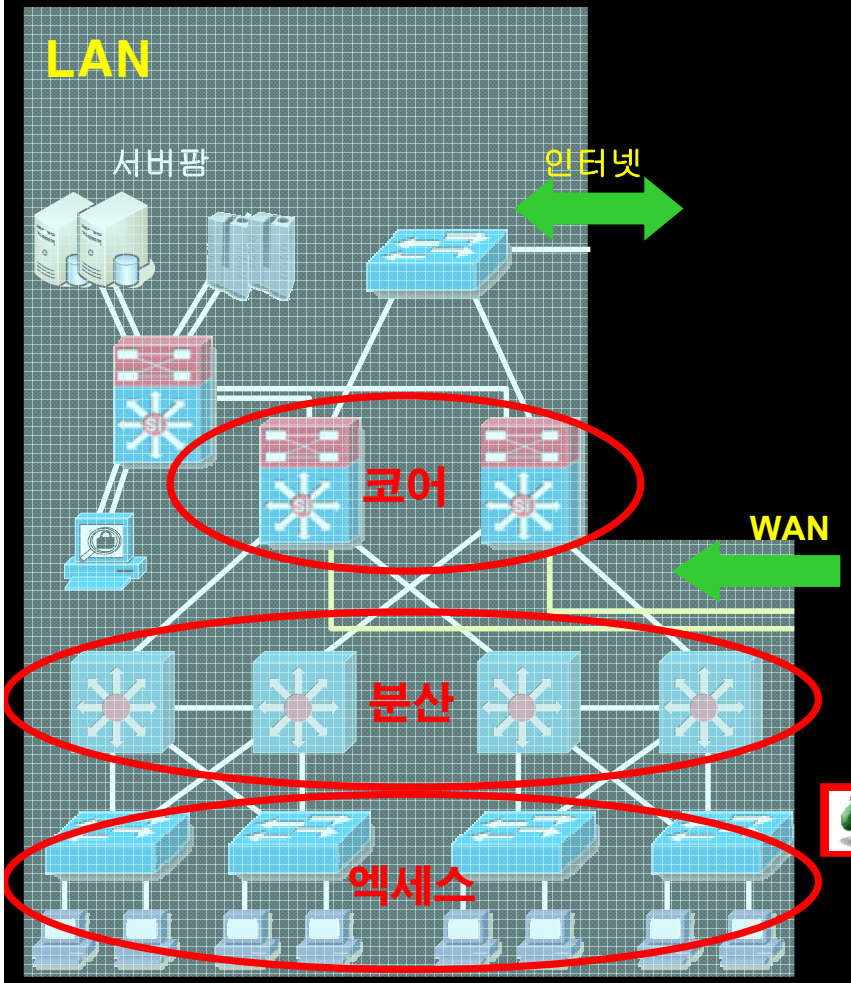
일반적인 네트워크 구성도

- 네트워크 도메인의 구분

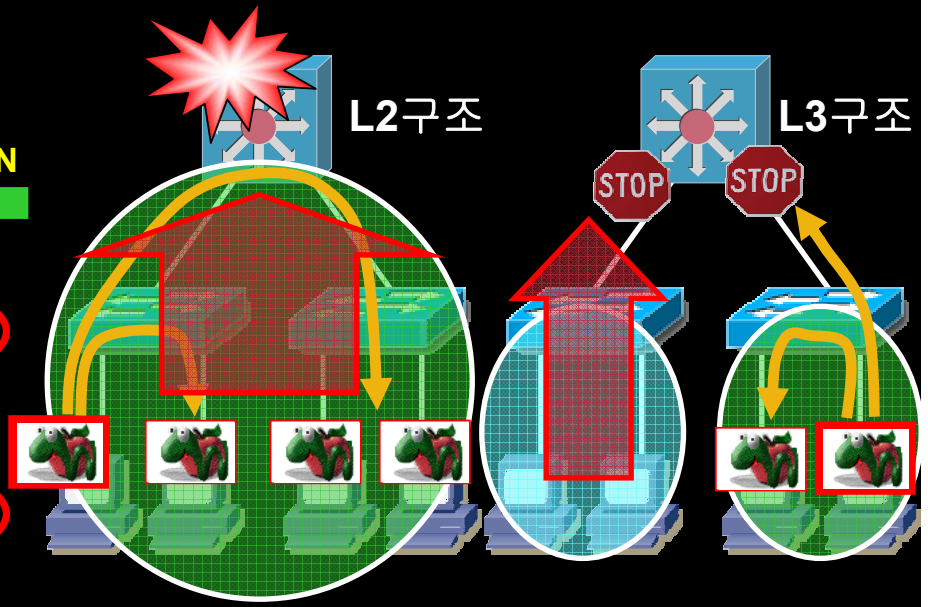


1. LAN 보안의 출발점 – 네트워크에 대한 이해

- 계층적 구조로 **Design** 되 있는가?

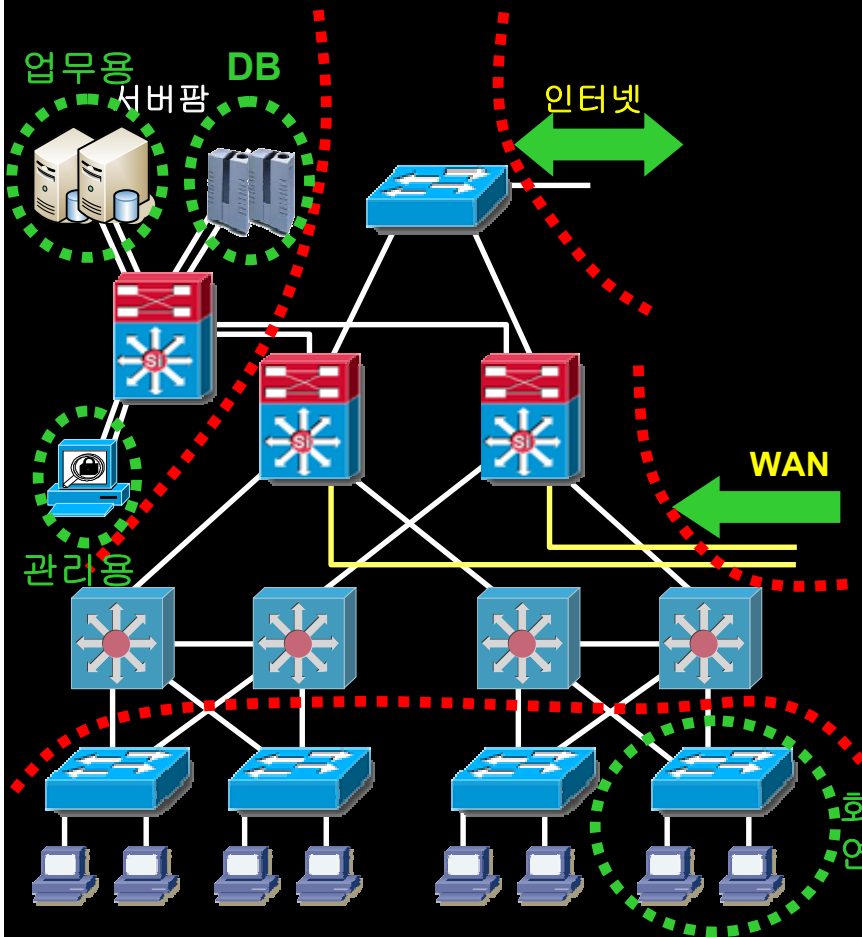


- 코어 / 분산 / 액세스 계층 설계시 각 계층에서 요구되는 보안 정책에 대한 기술 적용이 유리
- **L2** 구조보다는 **L3** 구조로 설계시 보안 위협에 대한 기술 적용이나 대응이 유리

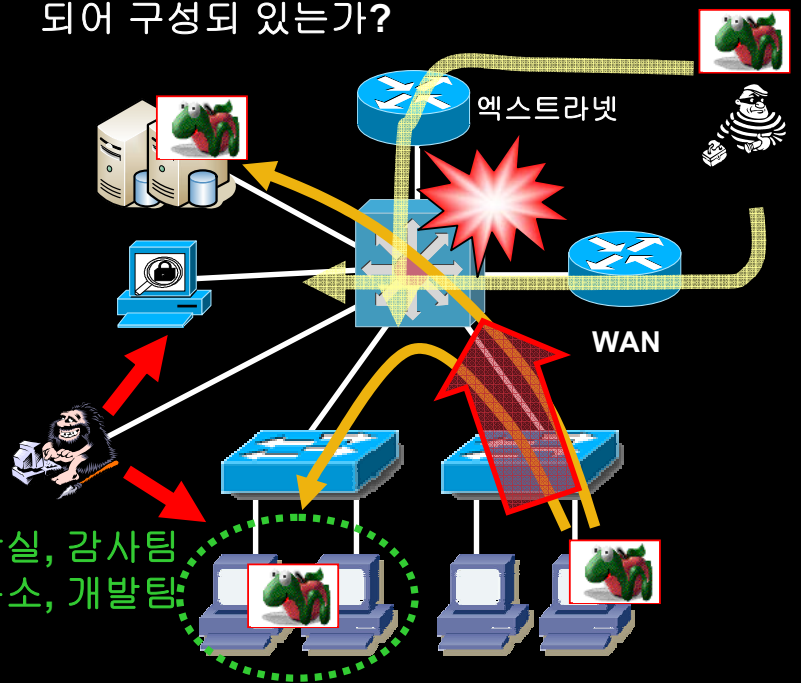


1. LAN 보안의 출발점 – 네트워크에 대한 이해

- **Segmentation**은 잘 되어 있는가?

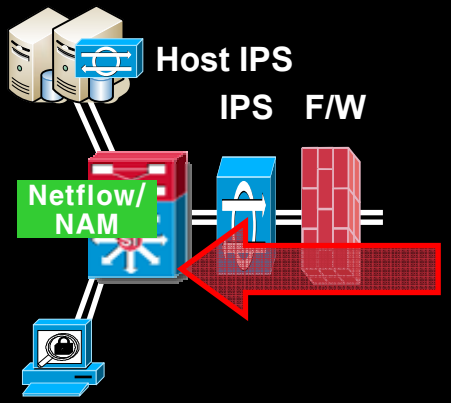


- 사용 용도 / 트래픽의 흐름 / 중요성 등에 따른 도메인들의 구분이 잘 정의 되어 있는가?
- 그러한 도메인들이 네트워크상에서도 잘 분류 되어 구성되 있는가?

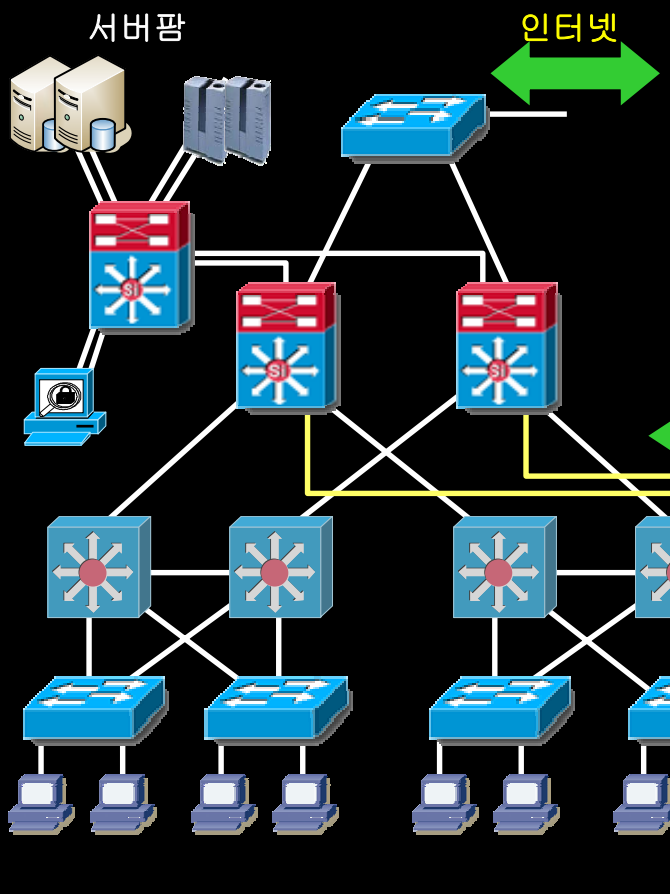


2. Perimeter(경계) 보안의 적용

- 경계 보안 적용의 요소들



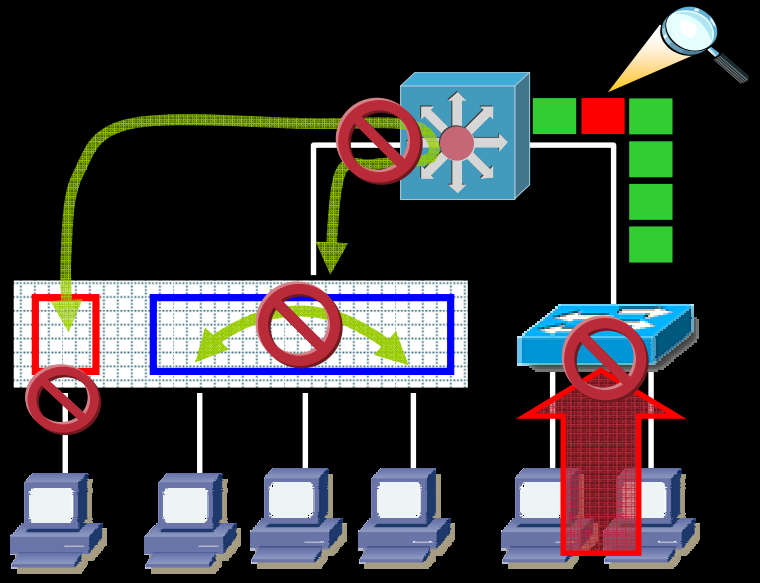
- 내부에서 기인하는 보안 위협들로 부터 서버팜을 보호하기 위한 경계선 구성 및 애플리케이션 보안
- 서버 사용에 대한 트래픽 감시 및 분석을 위해 트래픽 모니터링 동시 구현 **(Cat 6500 Netflow, NAM/ Cat 4500 Netflow)**



- **WAN**을 통해 유입 가능한 웜,바이러스,스파이웨어등의 검색 및 차단
- 트래픽 모니터링 동시 구현 **(ISR Netflow, NAM)**
- 중요한 내부 영역에 대한 보안

3. 네트워크 인프라 보안의 적용

- 다양한 보안 위협에 대한 인프라의 대응
  - 통신(트래픽)에 대한 통제

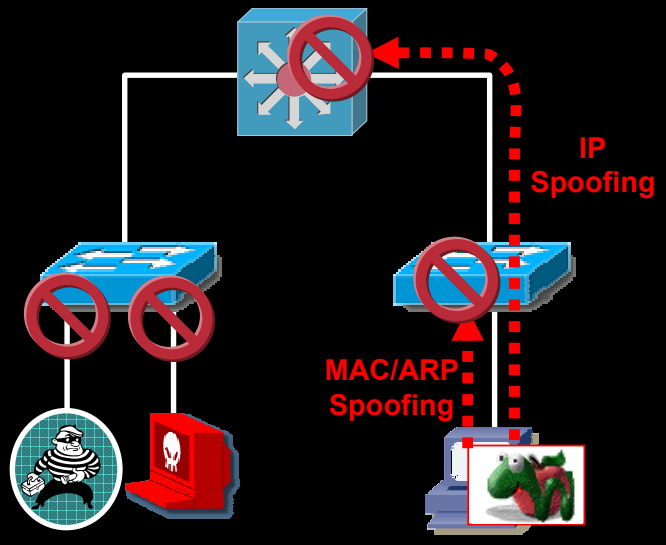


ACL 을 통한 통신(트래픽) 제어

과다한 트래픽에 대한 통제**(MAC,IP)**

QoS를 이용한 트래픽 통제 및 관리

  - 접근 및 **Spoofing** 공격에 대한 통제



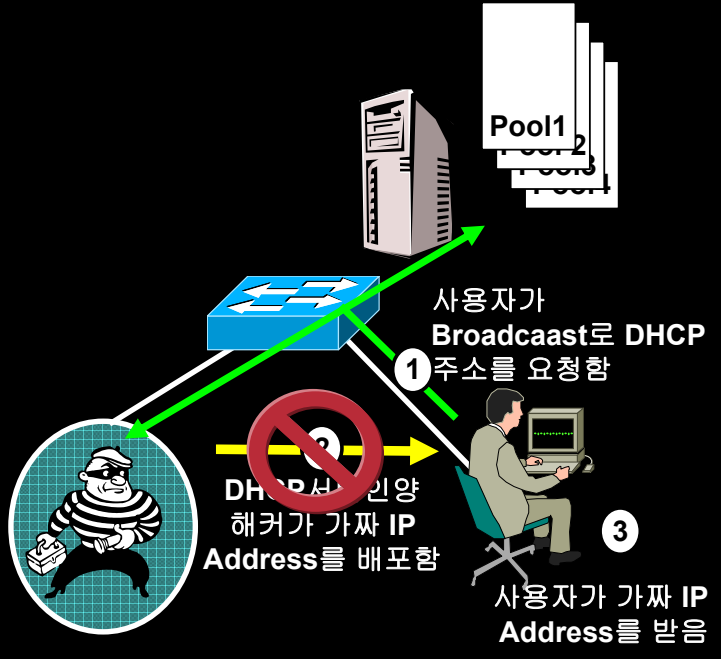
불법적인 사용자의 접근 통제 **(**사용자 인증**)**

Clean 하지 않은 단말 접근 통제**(**단말기 인증**)**

각종 위장**(Spoofing)** 공격에 대한 방어

3. 네트워크 인프라 보안의 적용

- 다양한 보안 위협에 대한 인프라의 대응
  - **Man-in-the-Middle** 공격 방지
  - **DHCP** 서비스에 대한 공격 방지



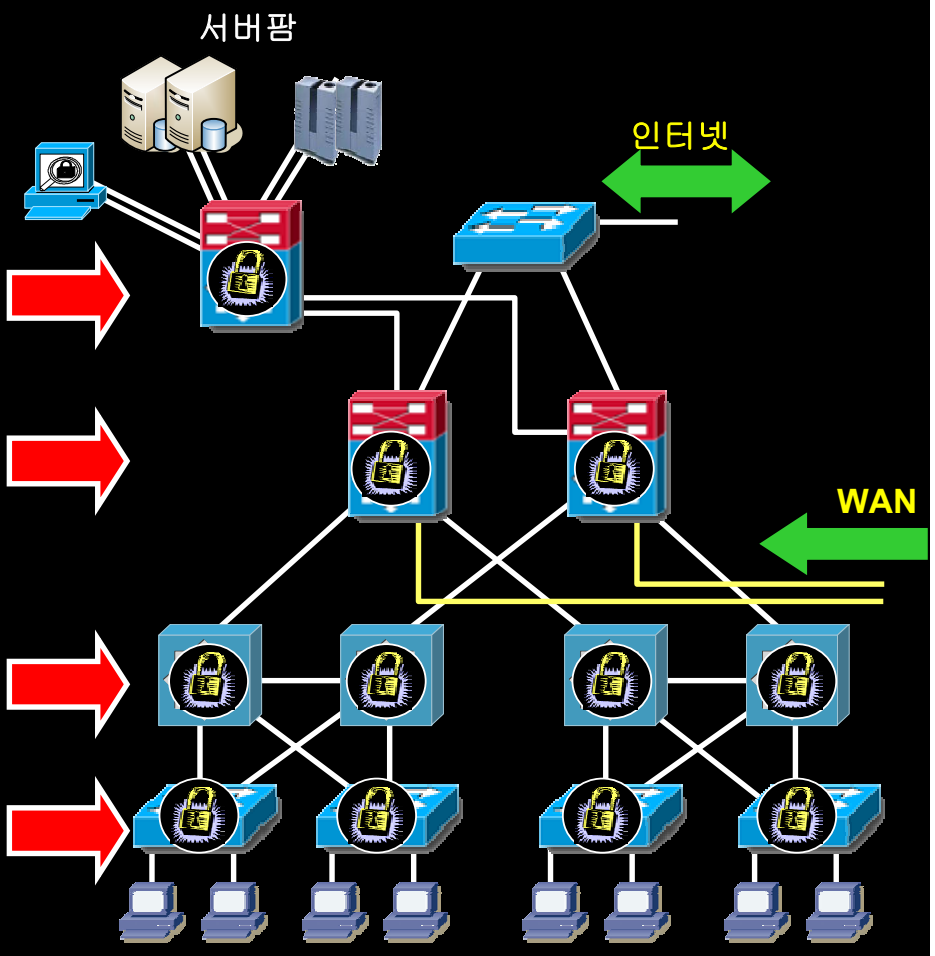
3. 네트워크 인프라 보안의 적용

- 네트워크 인프라의 역할 확장

- 분산 계층의 보안 역할 수행
- 동일 **VLAN**내의 서버들간의 통신 제어
- 서버 **VLAN** 간의 통신 제어

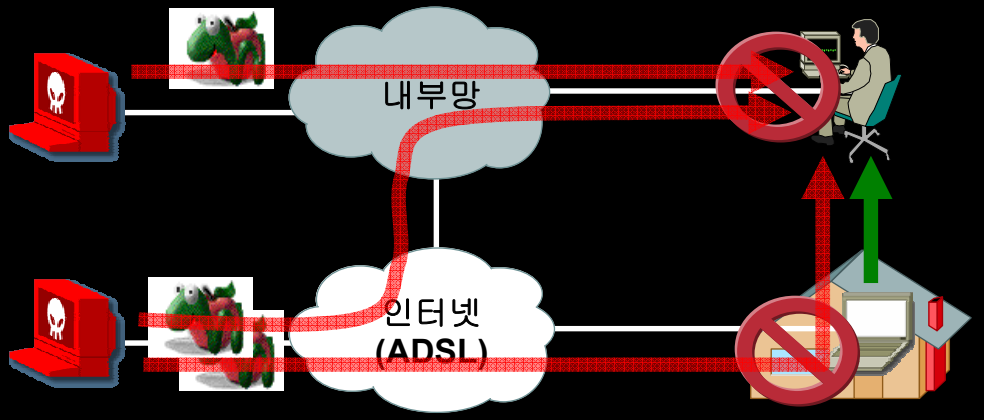
- 분산 계층간의 통신 및 트래픽 제어

- 액세스 / **VLAN** 간의 통신 및 트래픽 제어
- **IP** 변조 방어 및 **IP** 레벨의 통신제어
- **QoS**를 사용하는 보안 정책의 구현
- 각종 **Layer 2** 공격에 대한 방어
- 사용자 / 단말등에 대한 네트워크 접근 통제
- 포트/**VLAN**레벨의 통신 제어 및 단말에서 들어오는 트래픽 제어



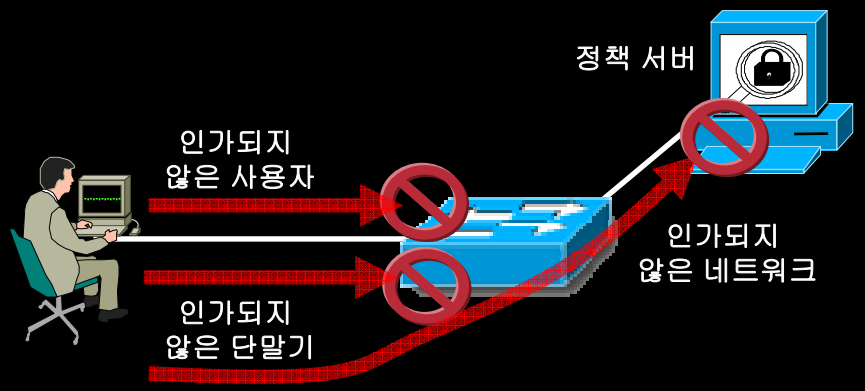
4. LAN 사용자 보안의 적용

- 사용자 보안의 구분
  - 사용자를 어떻게 보호할 것인가?



- 사용자 보안 정책은 사내망 사용시에만 해당되어선 안됨. (사용자 보안 교육도 필요)
- 기본적으로 **OS Patch** 및 **Anti-Virus**에 대한 주기적인 **Update** 필요
- **HOST IPS, Anti-Spyware/Adware** 솔루션의 구현 고려

  - 사용자로부터 어떻게 보호할 것인가?



- 사용자 단에서 발생할 수 있는 보안 위협에 대한 레벨을 구분하여 보안 솔루션 구현
- 네트워크 장비와의 연동을 통한 보안 구현 필요(네트워크를 보호하기 위한 정책)

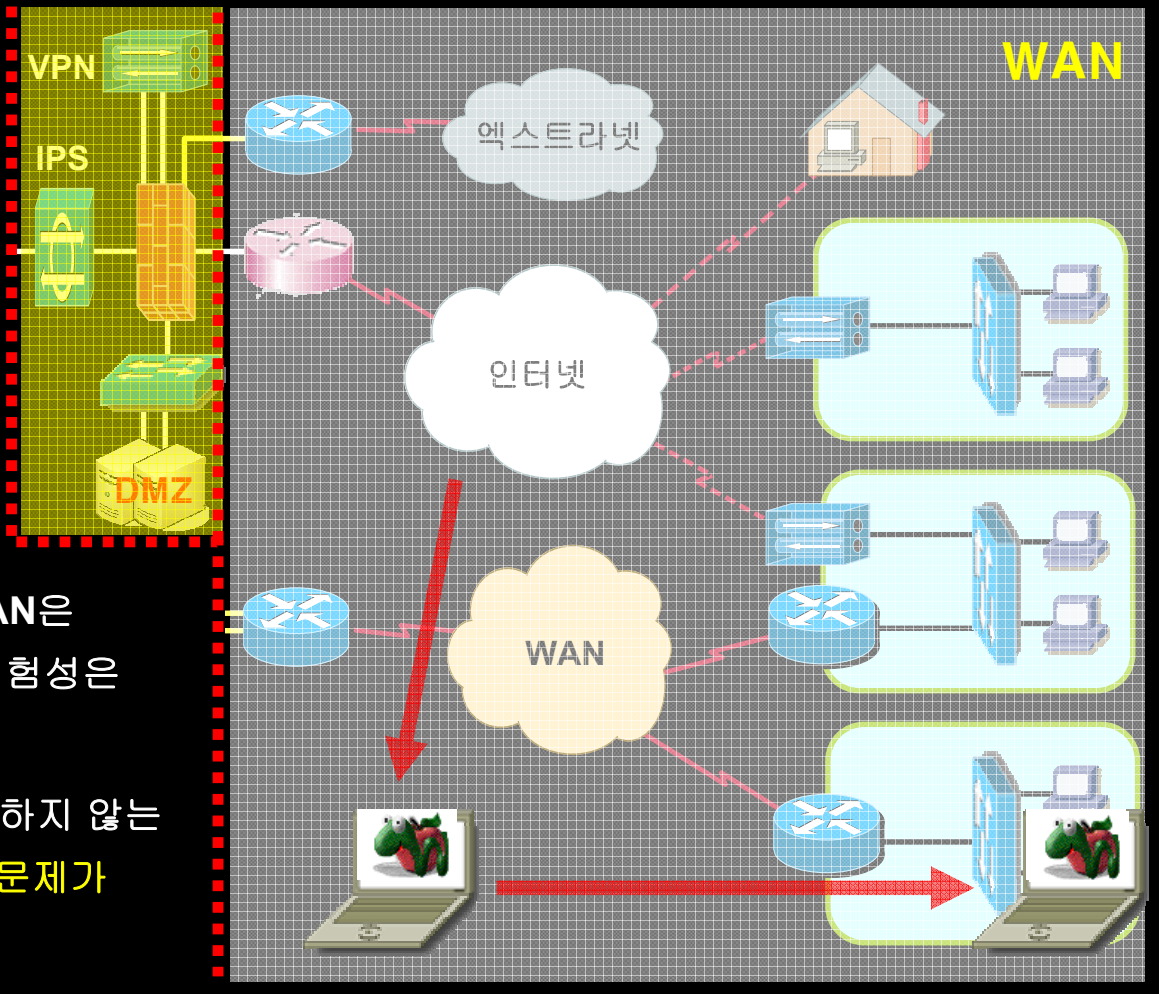
WAN 환경 보안 구현 모델

1. WAN 보안의 출발점 – 어디가 경계인가?

- **LAN**과 **WAN**은 보안을 위한 또 하나의 경계

전용선, ATM, F/R, PSTN, ISDN

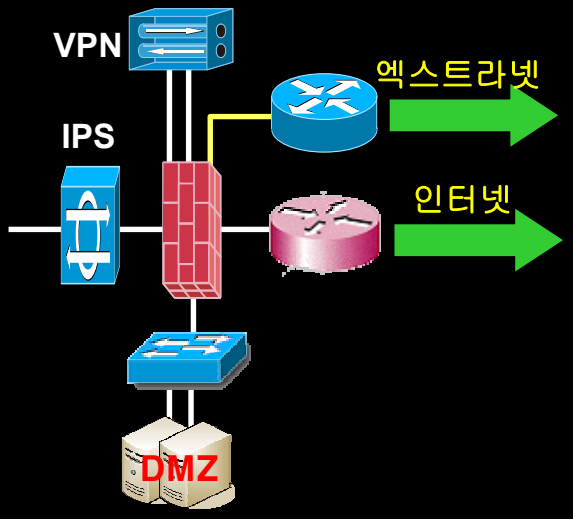
전용선, ATM, F/R, MPLS VPN, Metro Ethernet, ADSL/Cable(인터넷 VPN), PSTN



- 우리 네트워크와 연결된 **WAN**은 어떤 종류인가? 보안적인 위험성은 어떤가?
- 우리 **WAN**은 인터넷을 사용하지 않는 전용선인데 그래도 보안에 문제가 있나?

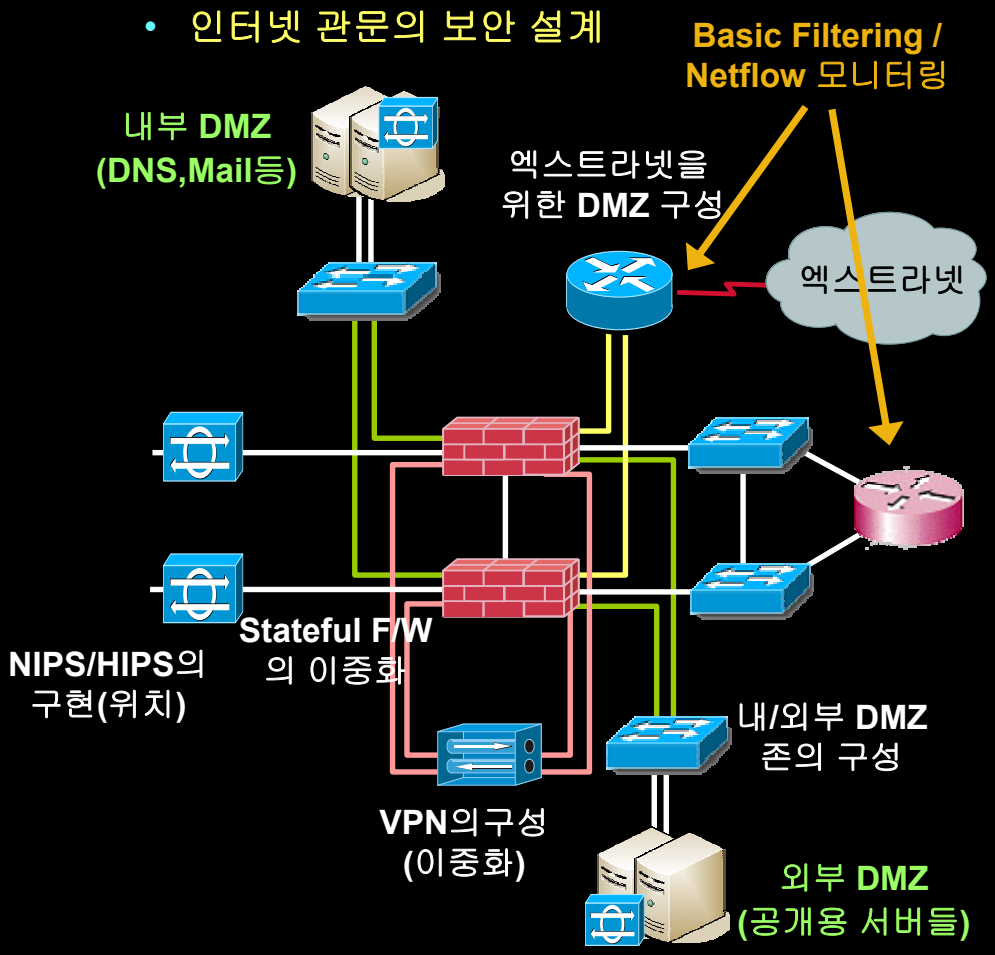
2. 대외망 경계 보안(인터넷 포함)

- 보안 구성 요소들



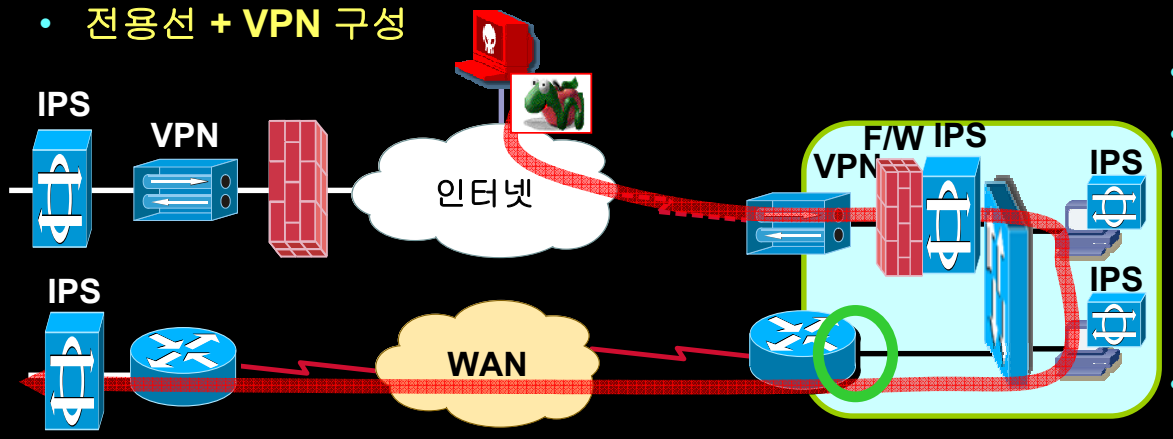
- 내부 **WAN** 관문 보안 설계

- 인터넷 관문의 보안 설계



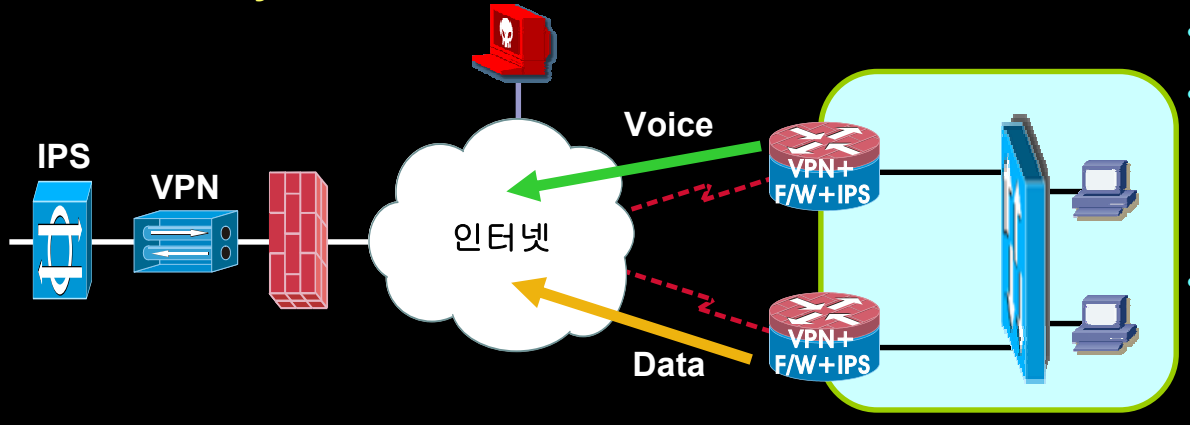
3. VPN의 구성

- **VPN(Site-to-Site의 경우) 구성 예**
  - **전용선 + VPN 구성**



  - **Split Tunneling 고려**
  - **Backdoor의 가능성 고려**
    - 리모트지역에 대한 보안
    - 단말기의 보안
    - **WAN 접점의 보안**
  - **VPN을 통한 Multi-Service 고려(예: Voice)**

  - **VPN Only 구성**

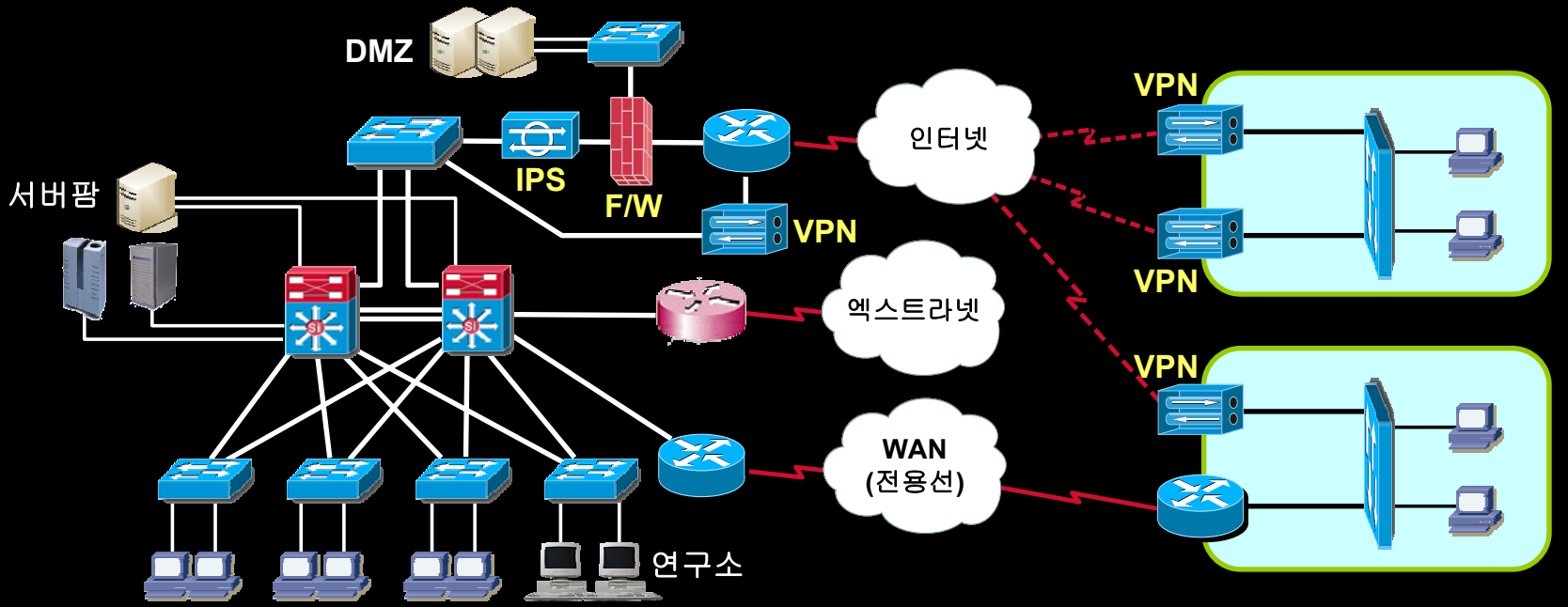


  - 상기 내용 포함
  - **WAN의 안정성 보장**
    - 회선 이중화
    - 장비 이중화
  - **일체형 Solutions**
    - **ISR(IPSec+F/W+IPS),**
    - **ASA 5500**

결 론

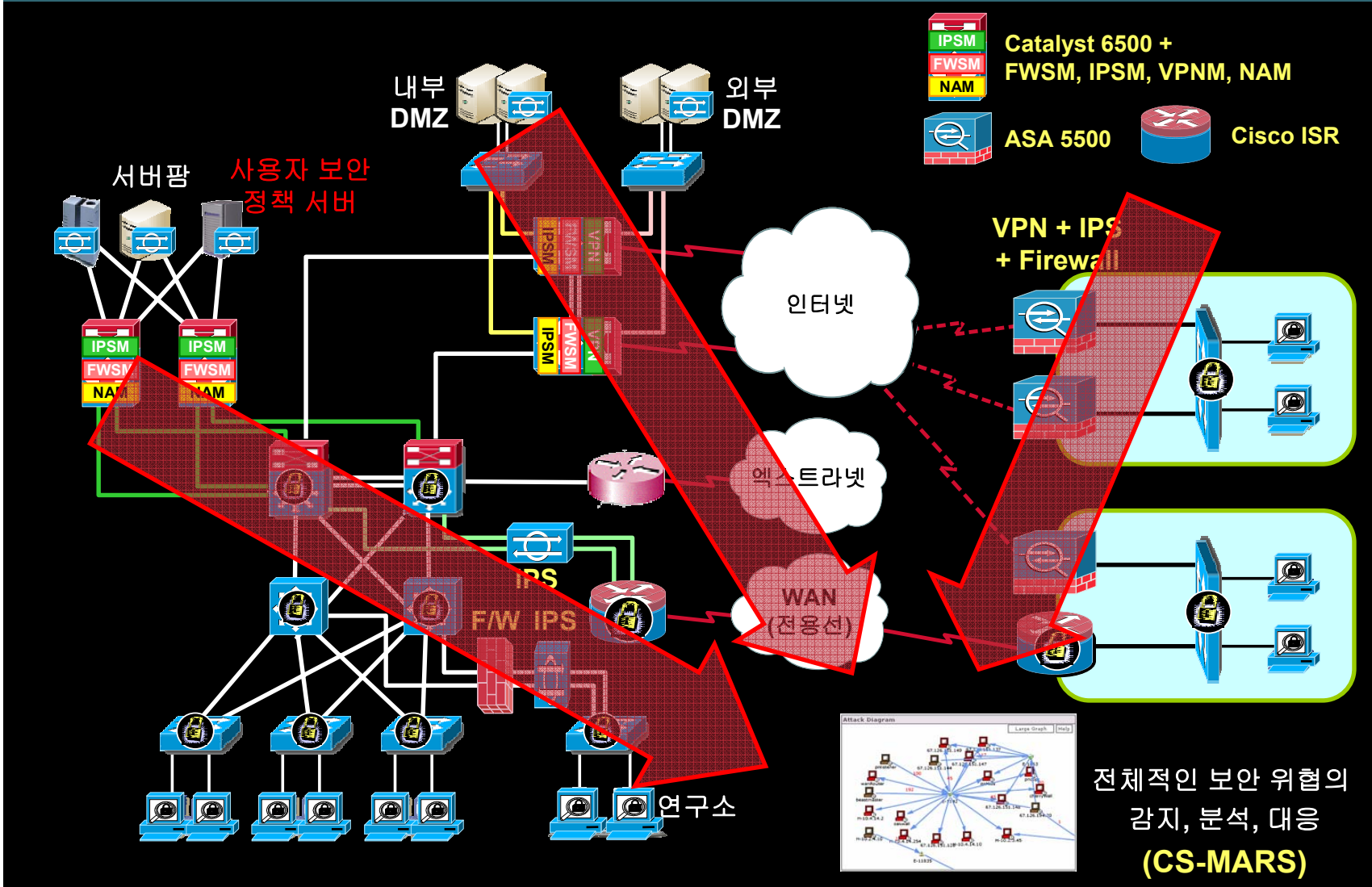
Case Study – Before

- LAN 백본 네트워크 : Layer 2 구조, 2-Tier구조, 접속 및 전달 위주, 도메인의 구분
- 서버 네트워크 : 백본에 직접 연결, 이중화,
- 인터넷 관문 : 이중화, VPN구성, DMZ구성
- WAN(엑스트라넷) 네트워크 : LAN 백본에 직접 연결, 접속 및 전달 위주,



- VPN 지역(지사) : 인터넷 관문 보안, Backdoor 제공 역할, 지사 LAN 보안
- 사용자 보안 : 바이러스 백신(사용자가 알아서 Update)

Case Study – After



효과적인 네트워크 보안을 위하여...

Business에 대한 이해가 필요합니다.

Security에 대한 이해가 필요합니다.

Network에 대한 이해가 필요합니다.