Cisco.com

Cisco 지능형 인프라 보안 솔루션

2004년 10월 20일

Cisco Systems Korea
한현철(harryhan@cisco.com)

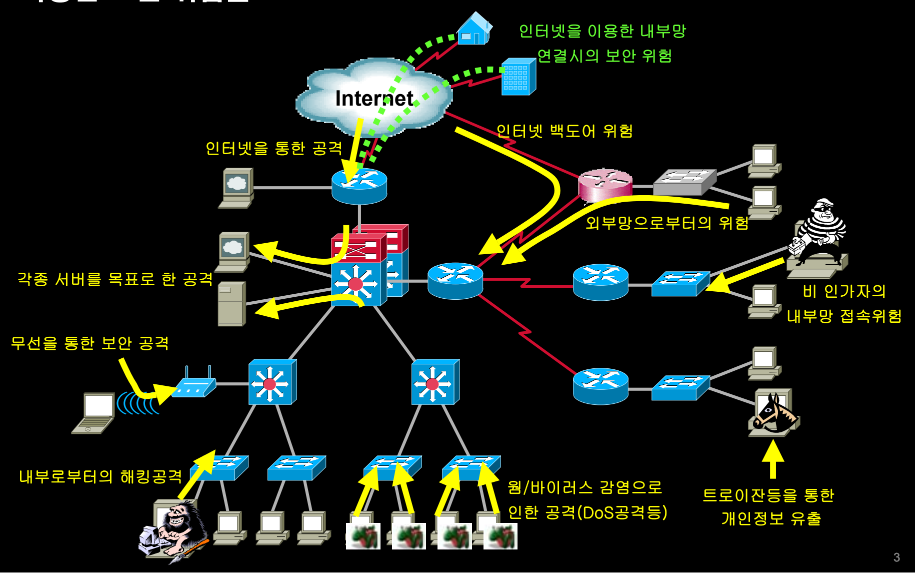
목 차

Cisco.com

Cisco Security 솔루션 개요

Cisco.com

❑ 다양한 보안 위협들



Cisco Security 솔루션 개요

Cisco.com

❑ Security에 대한 새로운 대응전략

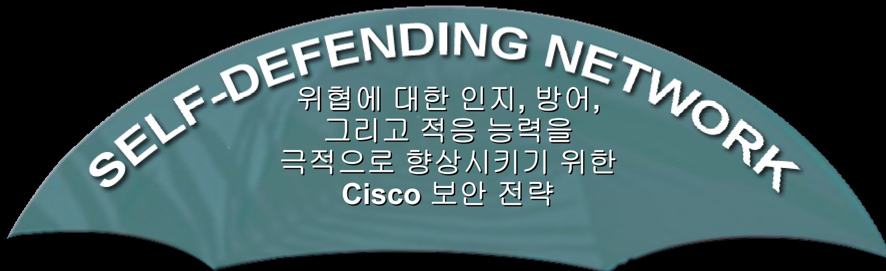
PAST		Need Now
Reactive	→	*Automated, Proactive*
Standalone	→	*Integrated Multiple Layers*
Product Support	→	*Network / End – Point system*

통합적인 시스템 차원의 접근

Cisco Security 솔루션 개요

Cisco.com

❑ SDN(Self Defending Network)



통합된 보안 솔루션

- Secure Connectivity
- Threat Defense
- Trust & Identity

지속적인 보안 기술 개발 및 혁신

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

시스템적인 보안 솔루션

- Endpoints + Networks + Policies
- Partnerships
- Services

Cisco Security 솔루션 개요

Cisco.com

❑ Cisco Integrated Security Portfolio

MANAGEMENT AND ANALYSIS	• Security management • Security policy, security event monitoring and analysis • Threat validation and investigation • Embedded device management				
COMPLETE COVERAGE	Protecting Desktops, Servers and Networks				
FLEXIBLE DEPLOYMENT	Security Appliances	Switches	Routers	Security Software	
SECURITY SERVICES	VPN / SSL	Firewall	IDS	Identity	Behavior
SECURE INFRASTRUC-TURE	Device Authentication, Port Level Security, Secure and Trusted Devices, Secure Access, Transport Security				

Advanced Security Services

PIX Appliance Firewall

PIX Appliance Firewall

Cisco.com

❑ PIX Appliance Firewall 개요

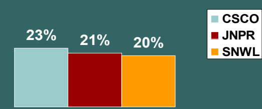
* ROBO : Remote Office Branch Office

PIX Appliance Firewall

Cisco.com

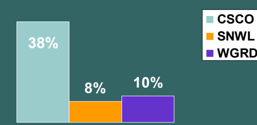
❑ Firewall 시장 점유율

Small Office / Home Office
($499 - $1,499 segment)



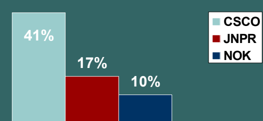
Marketshare leader:
Cisco PIX 501 Security Appliance

Remote Office / SMB
($1,500 - $9,999 segment)



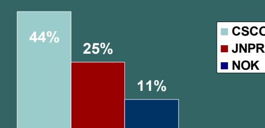
Marketshare leaders:
Cisco PIX 506E and 515E

Medium Enterprise
($10,000 - $30,000 segment)



Marketshare leader:
Cisco PIX 525 Security Appliance

Large Enterprise / Campus
(>$30,000 segment)



Marketshare leaders:
Cisco PIX 535 and FWSM

* Infonetics Q2 2004 Firewall / VPN Security Appliance Market Share Report, units by segment

PIX Appliance Firewall

Cisco.com

❑ Security Certifications

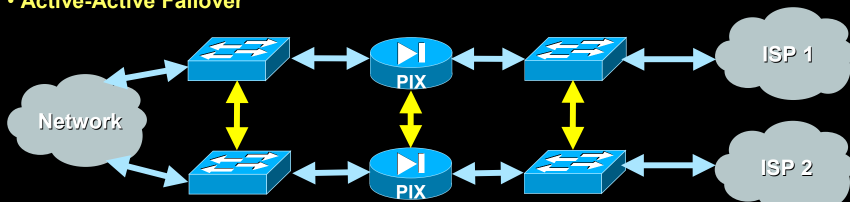
- **Common Criteria**
  - Current: EAL4, v6.2(2)
  - Future: EAL4+, v7.0(1)
- **FIPS 140**
  - Tentative: Level 2, v7.0(1)
- **ICSA Firewall 4.0, Corporate Category**
  - Current: v6.2(2) – PIX Family
  - Future: v6.3(4) – PIX Family
- **ICSA IPSec 1.0D**
  - Future: v6.3(4) – PIX Family

PIX Appliance Firewall

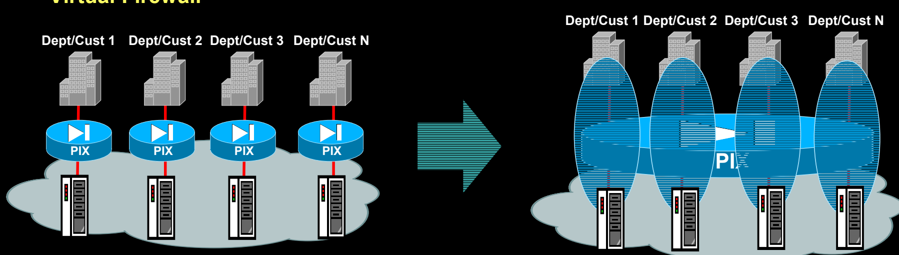
Cisco.com

❑ Cisco PIX v7.0의 특징

• Active-Active Failover



• Virtual Firewall

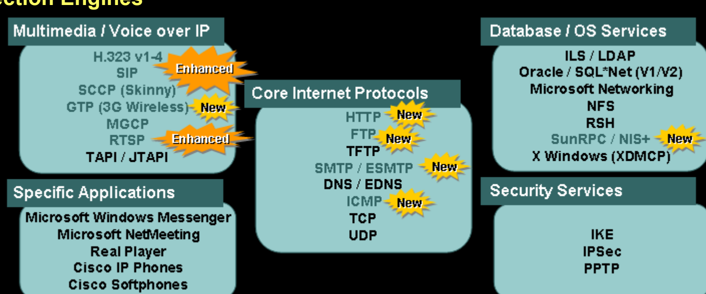


PIX Appliance Firewall

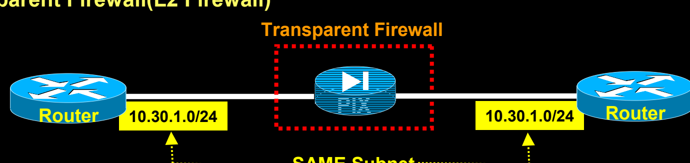
Cisco.com

❑ Cisco PIX v7.0의 특징(계속)

• Inspection Engines



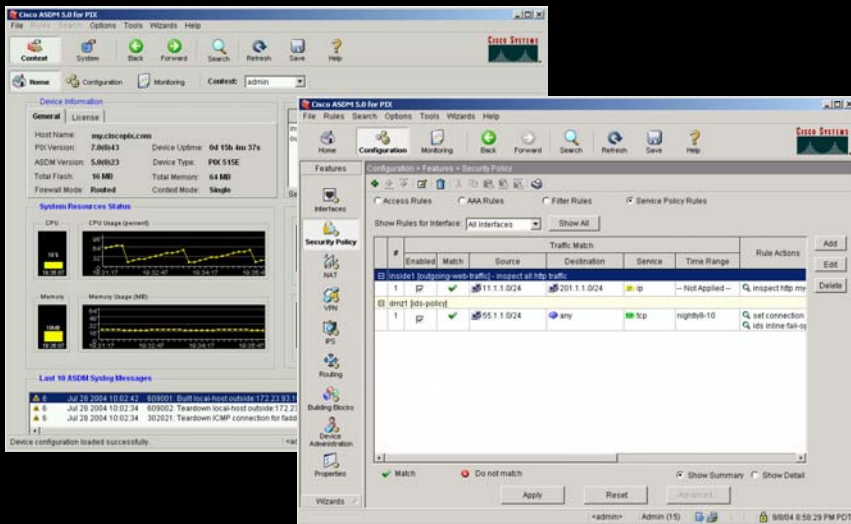
• Transparent Firewall(L2 Firewall)



PIX Appliance Firewall

Cisco.com

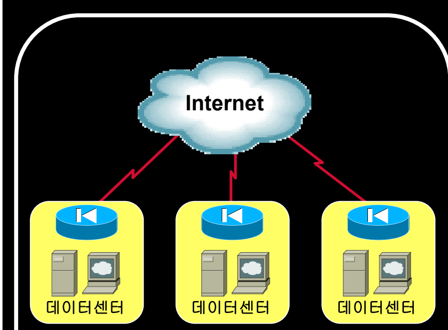
❑ ASDM(Adaptive Security Device Manager) 5.0



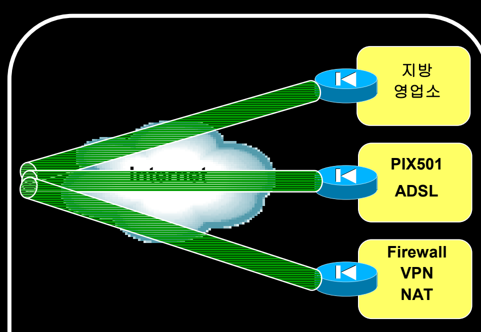
PIX Appliance Firewall

Cisco.com

❑ PIX Firewall 의 적용



[PIX F/W 을 이용한 서버팜 보안]



[PIX F/W 을 이용한 VPN구성]

IDS/IPS Appliance

IDS/IPS Appliance

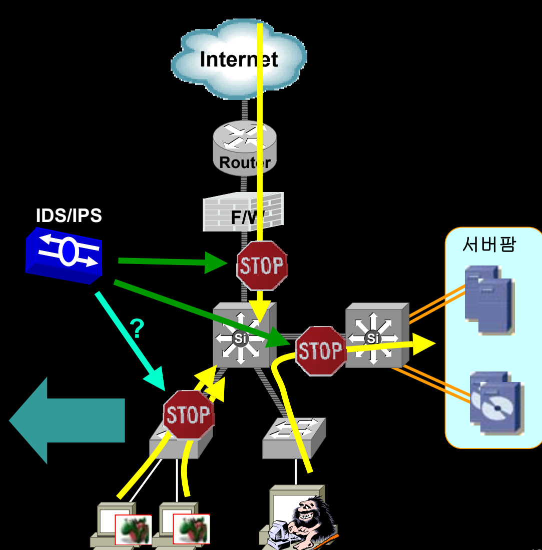
Cisco.com

❑ IDS/IPS 적용시 고려 사항

IDS/IPS는 해당 장비를
거쳐가는 Data에 대해서
차단 또는 탐지를 하므로
Design(구성)시
어떤 트래픽을 점검할것인지,
어느 지점에 설치것인지를
신중히 고려해야 함

- IDS/IPS와 네트웍장비간의 연동을 통한 차단(Shunning 기능)

- Host(PC, 서버)에서 발생되는 웜/바이러스등의 보안 위협에 대한 원천적인 위협 제거 (NAC,CSA)



IDS/IPS Appliance

Cisco.com

❑ Cisco IDS/IPS 개요

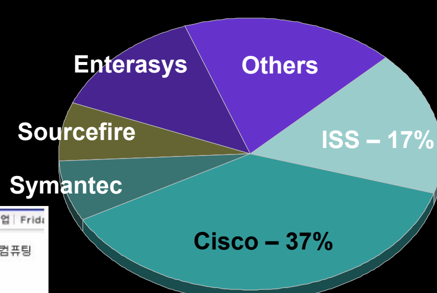
	Solution Breadth				
Network Sensor	4215	4235	4250	4250-XL	
Switch Sensor	IDSM-2				
Host Sensor	Security Agent - PC		Security Agent - Server		
Router Sensor	8xx	18xx	28xx	38xx	7xxx
Firewall Sensor	501	506E	515E	525	535
Investigation & Mgmt	Web UI Embedded Mgr	Threat Response	CiscoWorks VMS		

IDS/IPS Appliance

Cisco.com

❑ IDS/IPS 시장 점유율

- #1 Market share leader
- Cisco IDS is #1 with 37%, up 8% Q/Q,
- 20% Y/Y growth



Source: Infonetics 1Q2004

뉴 스 | 오늘의 뉴스 | 뉴스속보 | 종합 | 통신방송 | 컴퓨팅 | 콘텐츠 | 국제 | 경제과학 | 디지털산업 | Frid

Home > 컴퓨팅

"IDS 시장은 죽지 않았다"

침입방지시스템(IPS)이 보안 업계의 최대 화두로 부상한 가운데 침입탐지시스템(IDS)도 꾸준한 시장 수요를 유지하고 있어 귀추가 주목된다.

중 략

이처럼 꾸준히 IDS 수요가 나오는 이유는 아직 IPS의 탐지 기능이 IDS를 따라가지 못하기 때문이다. 실제로 네트워크의 중간에 설치되는 IPS는 감시와 차단을 함께 하면서 적지 않은 병목현상을 일으킨다.

또 상당수의 IPS 업체가 기가비트 환경을 기원하는 제품을 출시했지만 24시간 서비스를 지속해야 하는 상당수의 공공기관과 기업의 경우 아직 불안감을 씻지 못하는 추세다. 따라서 네트워크에 부하를 주지 않는 IDS로 감시를 하고 전담 인력이 침입에 즉시 대응하는 체계를 만드는 것이다.

IDS/IPS Appliance

Cisco.com

❑ Security Certification

- Common Criteria
  - Current: IDS Protection Profile Compliant, v4.1 Sensor SW, 4200 Series and IDSM2
- ICSA IDS
  - Current: v4.x, 4235
  - Future: v5.xx
- NSS Group IDS
  - Current: v4.x, 4235 & 4250XL
  - Future: v5.0, IDSM2, 4240, 4255
- Neohapsis OSEC
  - Current: v4.1, 4250-XL
  - Future: v5.0, 4240, 4255

IDS/IPS Appliance

Cisco.com

❑ Cisco IPS Software v5.0

- Highlights
  - 악의적인 트래픽을 네트워크 상에서 차단하기 위해 인라인상에서의 침입방지 (Intrusion Prevention) 기능을 제공
- Timeframe
  - 베타 프로그램 시작 – October 2004
  - 출시 예정 – December 2004
- Platforms Supported
  - 기존 제품군 - 4215, 4235, 4250 (TX, SX & XL),IDSM2(5.1)
  - 새로운 제품군 - 4240, 4255
  - 기존 제품군중 IPS 기능 불가 – 4210

IDS/IPS Appliance

Cisco.com

❑ Cisco IPS 4240/4255 Appliance

- 4개의 10/100/1000 Copper Gigabit 포트
- One 10/100 Out of Band 관리 포트
- 추가적인 I/O를 위해 예약된 Slot
- 고성능의 1 RU Design의 섀시
- Three Thermal Zones with Heat Sensitive Fans
- Field에서 Upgrad 가능한 AC Power Supply

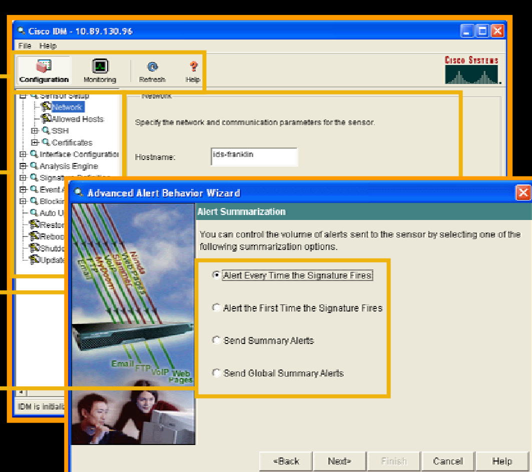
- 향후 확장 기능을 위한 2개의 USB 2.0 Ports (Failover, and more)
- Compact Flash for local storage (HD eliminated)
- 콘솔과 AUX Ports
- 상태 LEDs (Power, Status, Flash)

IDS/IPS Appliance

Cisco.com

❑ Cisco IPS Device Manager v5.0

- 주 화면에서 configuration(구성) 과 monitoring(모니터링) 화면사이에 쉬운 이동
- Configuration tasks 와 Work flow process 를 위한 직관력있는 계층적 View
- 센서 setup을 단순화 하기 위한 유용성의 강화
- signature customization 을 단순화 하기 위해 재 설계된 Signature Wizard



VPN 3000 Concentrators

VPN 3000 Concentrators

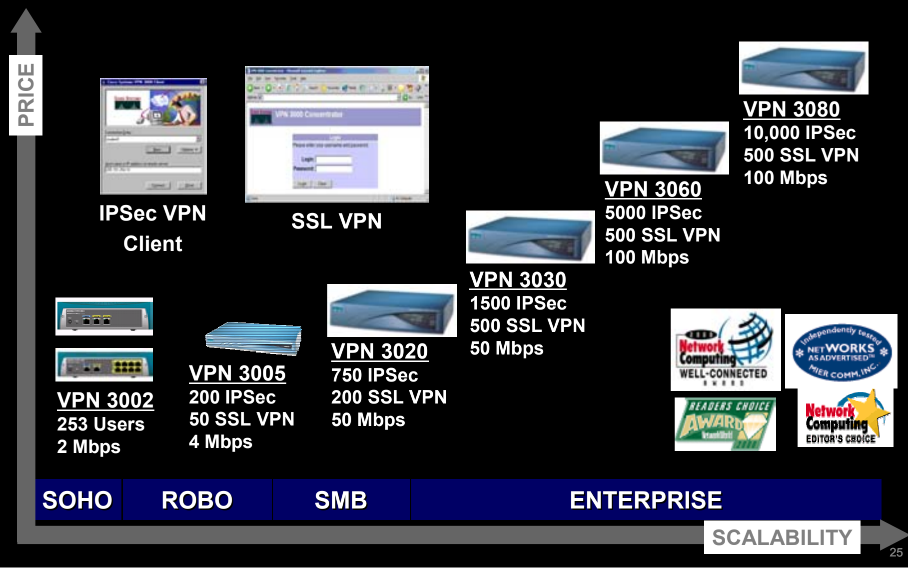
Cisco.com

❑ **VPN 솔루션의 필요성**

VPN 3000 Concentrators

Cisco.com

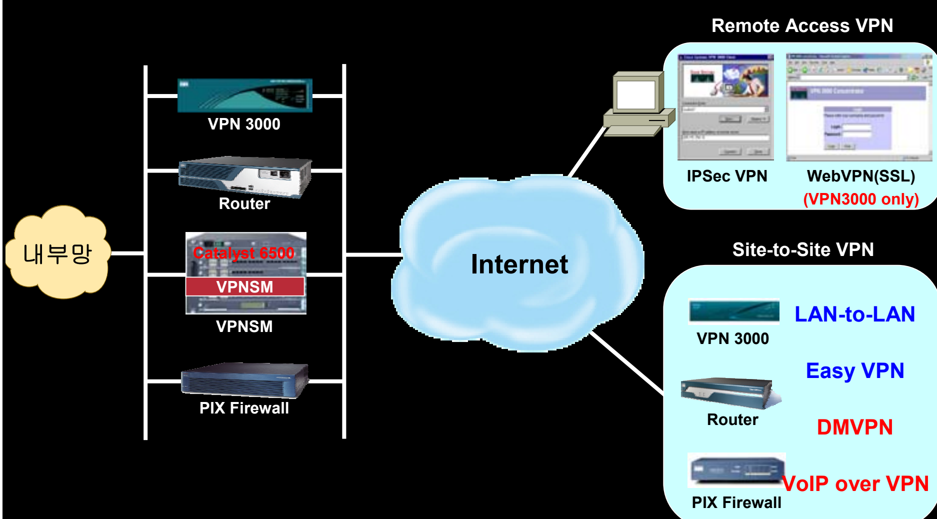
❑ VPN 3000 Concentrators 개요



VPN 3000 Concentrators

Cisco.com

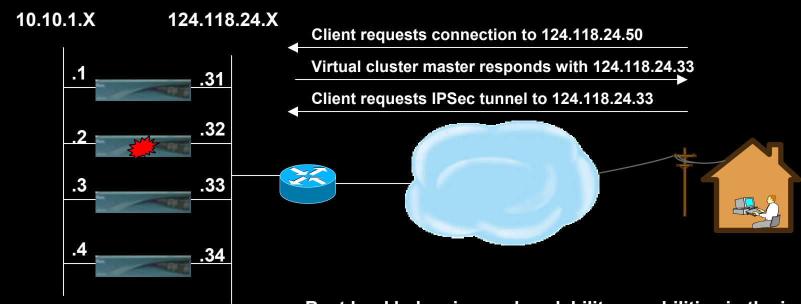
❑ Cisco VPN 솔루션의 다양성



VPN 3000 Concentrators

Cisco.com

❑ VPN 3000 Loadbalancing – Virtual Clustering



Virtual Cluster IP Address = 124.118.24.50

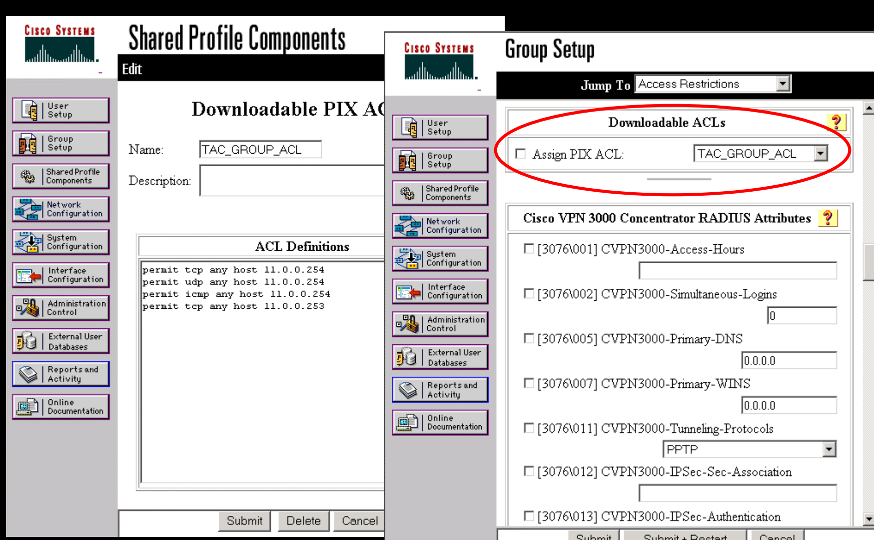
=Virtual Cluster Master

- Best load balancing and scalability capabilities in the industry
- New price action allows for price effective "clusters"
- Internal redundancy/scalability is good but clustering is superior

VPN 3000 Concentrators

Cisco.com

❑ Downloadable ACL



VPN 3000 Concentrators

Cisco.com

❑ WebVPN(SSL VPN)

- Web page access (HTTP/HTTPS)
- Remote e-mail access
  - POP, IMAP, SMTP, OWA, Outlook, Notes, iNotes, etc
- File access on enterprise servers
  - Windows CIFS file shares via Web Interface
- Flexible login options customizable for diverse user communities
  - Group based access control
  - Support for all enterprise authentication mechanisms
- Port forwarding
  - Access to thick client TCP-based applications
- Web-based management
  - Full-featured configuration and monitoring for WebVPN via VPN 3000 Device Manager

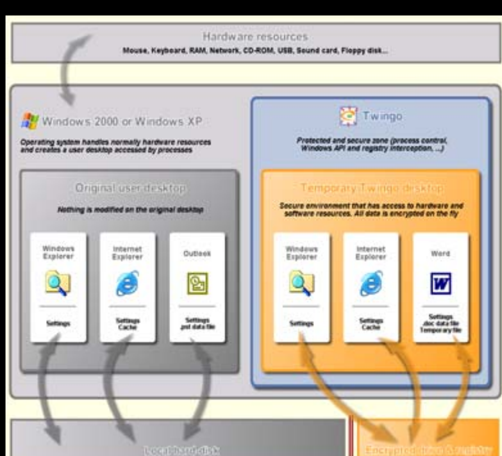
ALL SSL VPN FEATURES INCLUDED IN BASE PRICING— NO SPECIAL LICENSES!

VPN 3000 Concentrators

Cisco.com

❑ Cisco Secure Desktop(Twingo)

SSL VPN의 Endpoint Security 강화를 위해....



THE TECHNOLOGY:
VIRTUAL SECURE DESKTOP

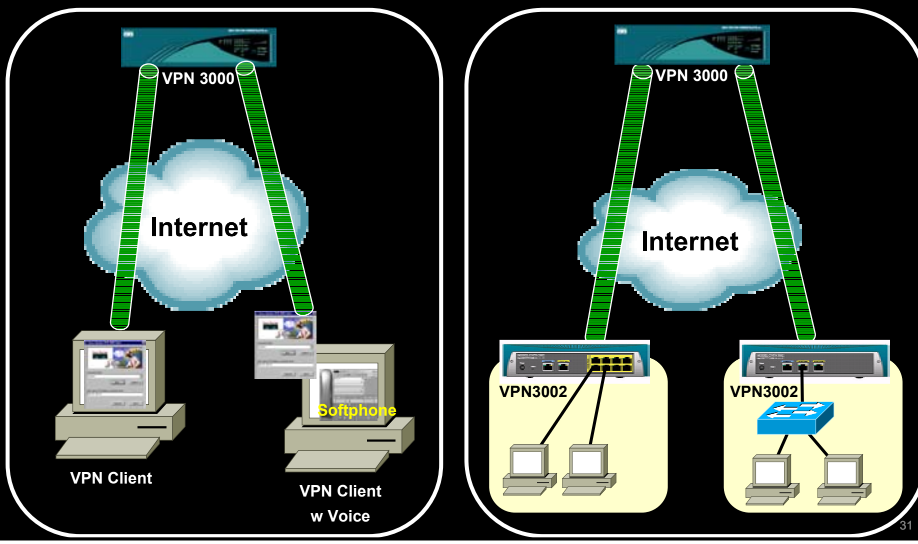
Removes sensitive security information (cookies, browser cache/history, e-mail file attachments, etc.) related to an SSL VPN connection at the close of the session.

This protects from exploitation of such information for host network or system penetration.

VPN 3000 Concentrators

Cisco.com

❑ VPN 3000 Concentrator의 적용

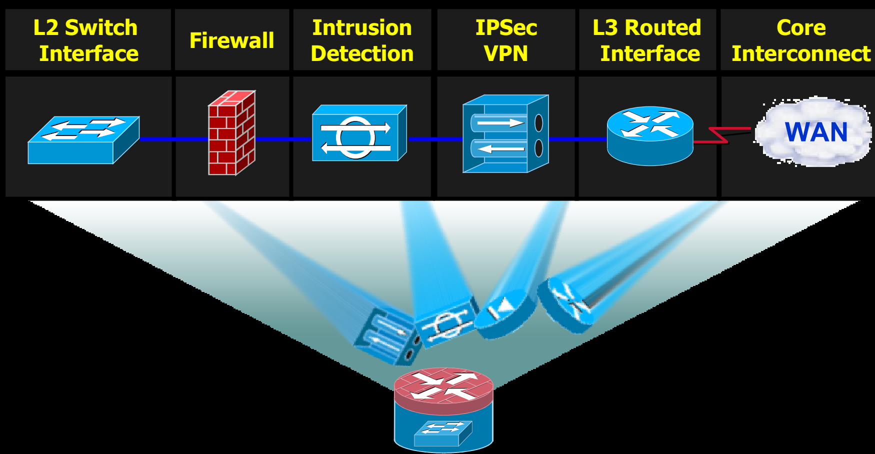


IOS Security

IOS Security

Cisco.com

❑ IOS Security 개요

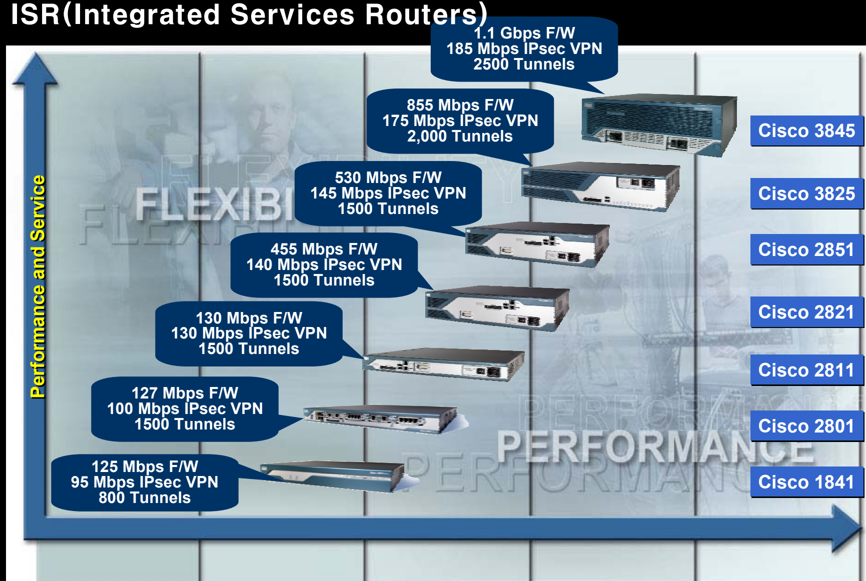


Cisco IOS Security Router
VPN + Firewall + IDS + Advanced
Security Service + IP Routing

IOS Security

Cisco.com

❑ ISR(Integrated Services Routers)



IOS Security

Cisco.com

❑ High-End Routers

7200	7300	7600
		
5000 IPSec Tunnels 260 Mbps IPSec	5000 IPSec Tunnels 370 Mbps IPSec	8000 IPSec Tunnels 1.9 Gbps IPSec per VPNSM

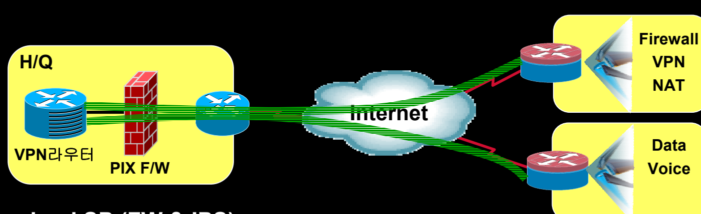
- Versatile, high-performance, modular, multiprotocol platforms that enable flexible and scalable deployments for Enterprise and Service provider environments.

- MPLS and IPSec VPN support

IOS Security

Cisco.com

❑ IOS Firewall



- Marriott Hotels
- Albertson's
- MasterCard
- XB Networks, Netherland SP (FW & IPS)
- Experio Solutions (PIX & IOS)
- Polo Ralph Lauren
- Germanos retail project 350 remote sites using c1760
- National Registry Land office, 60 remote sites
- Spanish northern region local Government) 200 routers
- Departament d'Educació. Generalitat de Catalunya
- Universitat de Girona (UDG) on aC7200 (Spain)

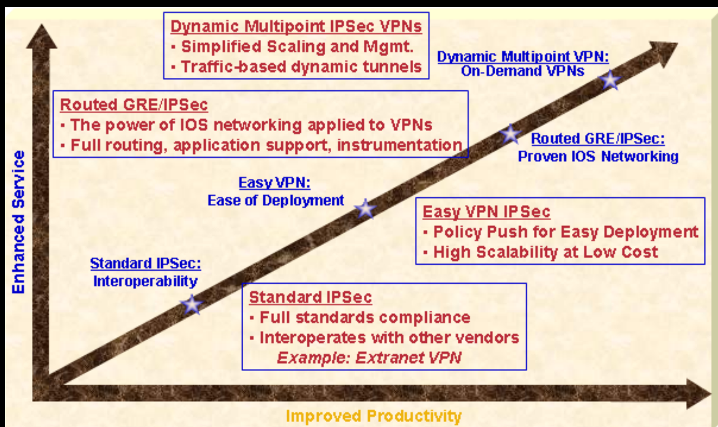
ICSA labs CERTIFIED www.ICSALabs.com Firewall

Common Criteria

IOS Security

Cisco.com

- IOS VPN



IOS Security

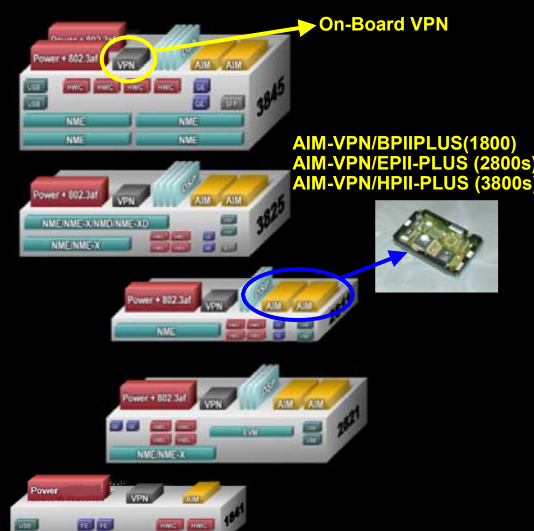
Cisco.com

- IOS VPN – Hardware Encryption module

ISR 3800

ISR 2800

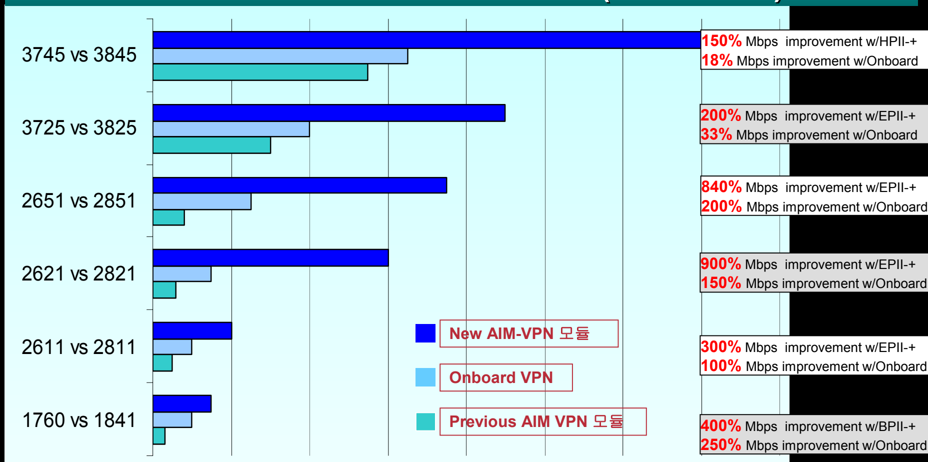
ISR 1800



IOS Security

❑ IOS Security Performance

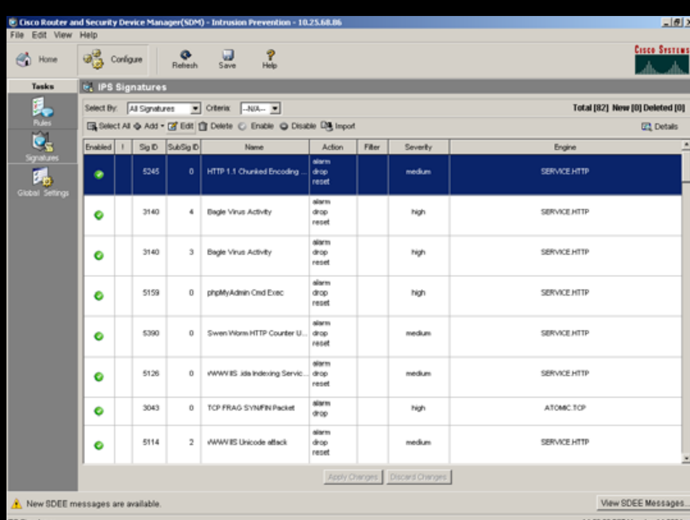
FW + IDS + VPN with 256 AES (IMIX traffic)



IOS Security

Cisco.com

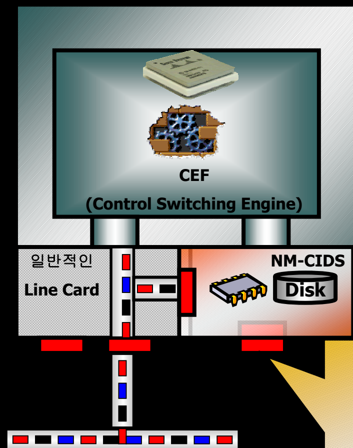
❑ IOS IDS/IPS



IOS Security

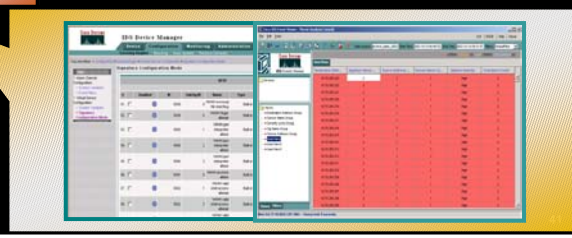
Cisco.com

❑ IOS IDS/IPS Module(NM-CIDS)



Cisco Router IDS Module

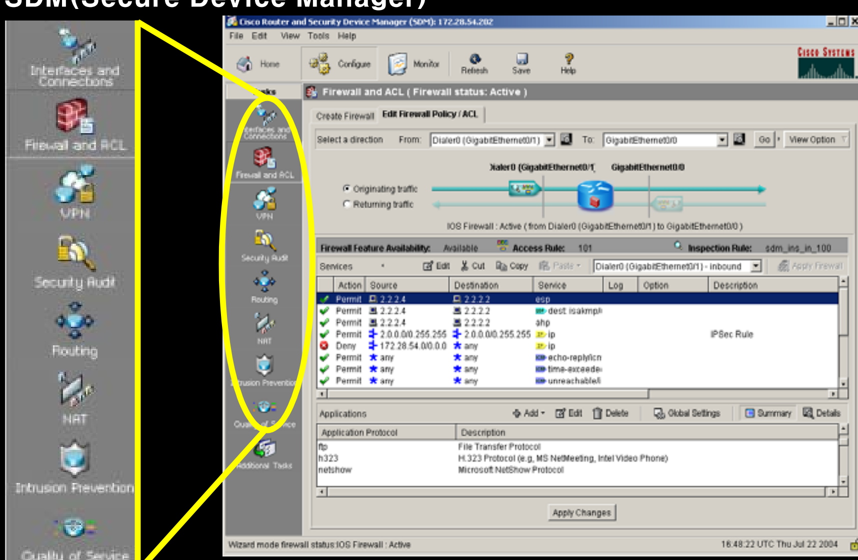
- Performance – 45Mbps
- Interface – Onboard FastEthernet 1port 지원
- Logging – 20 GB HDD
- Remote 관리 기능 지원(SSL 기반)
- GRE 암호화 Traffic 분석 기능 제공
- 유해 Traffic – Router 기반의 자동 Blocking 기능



IOS Security

Cisco.com

❑ SDM(Secure Device Manager)



Catalyst 6500 Security Service Modules

43

Catalyst 6500 Security Service Modules

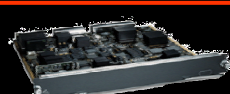
Cisco.com

❑ Catalyst 6500 Service Module 개요


Firewall Services Module (FWSM)

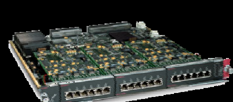

Intrusion Detection Module (IDSM2)


Content Switching Module (CSM)


VPN Services Module (VPNSM)

Integrated
High Performance
Right Position


Network Analysis Module (NAM2)


Communications Media Module (CMM))


Content Services Gateway (CSG)

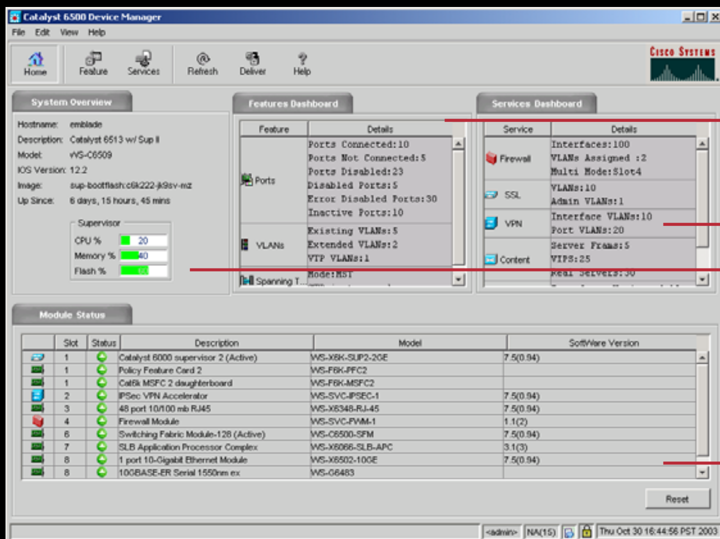

SSL Module (SSL)

44

Catalyst 6500 Security Service Modules

Cisco.com

❑ CVDM(CiscoView Device Manager)



Layer 2/3 Switching Dashboard

Layer 4-7 Services Dashboard

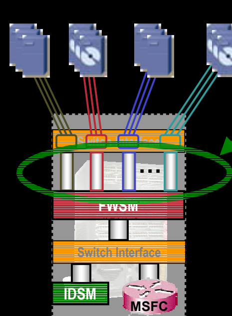
System Overview

Slot-by-Slot Switch Status Dashboard

Catalyst 6500 Security Service Modules

Cisco.com

❑ FWSM(Firewall Service Module)



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
- ❑ 샤시 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

Catalyst 6500 Security Service Modules

❑ IDSM-2

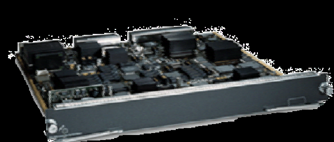
IDSM-2

- ❑ 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

Catalyst 6500 Security Service Modules

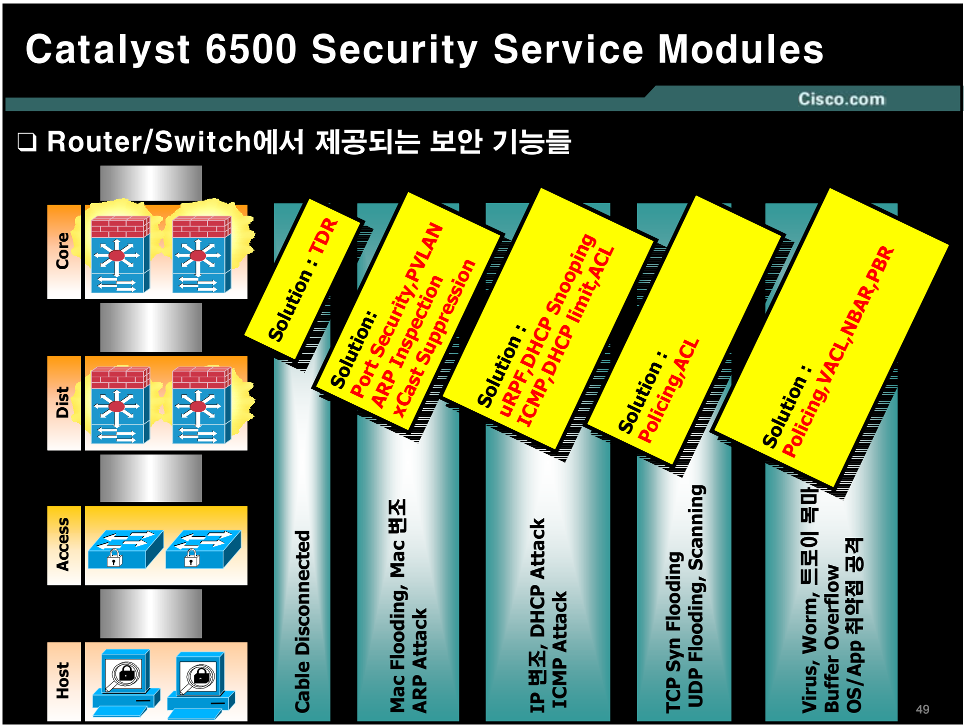
Cisco.com

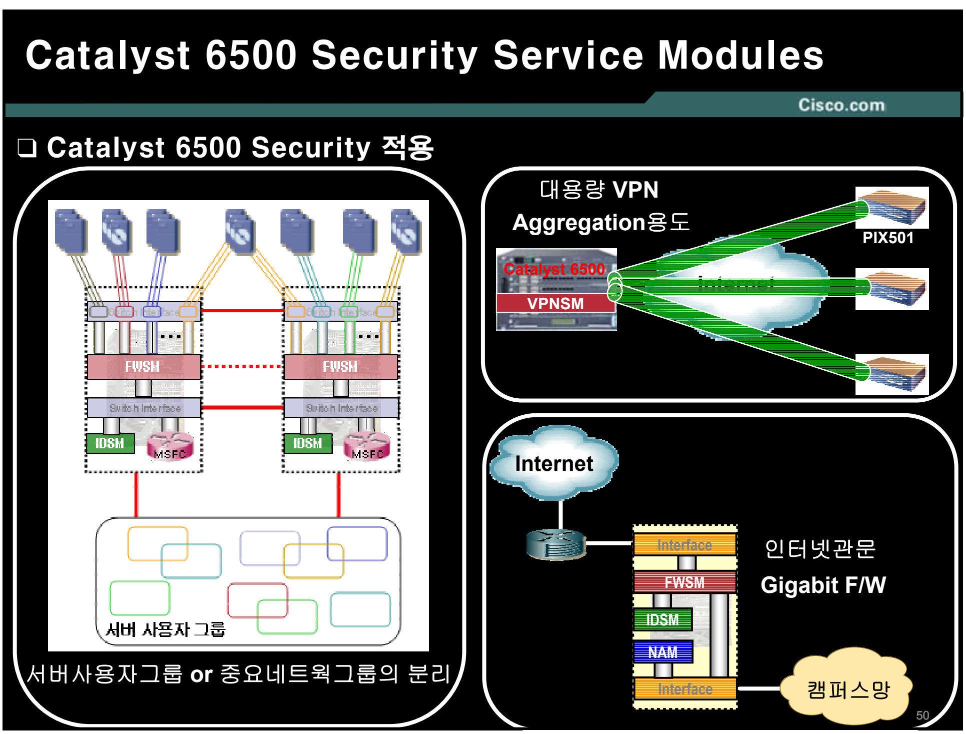
❑ VPNSM



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


Catalyst 6500 Security Service Modules
Cisco.com
❑ Router/Switch에서 제공되는 보안 기능들
Core
Dist
Access
Host
Solution : TDR
Cable Disconnected
Solution:
Port Security,PVLAN
ARP Inspection
xCast Suppression
Mac Flooding, Mac 변조
ARP Attack
Solution :
uRPF,DHCP Snooping
ICMP,DHCP limit,ACL
IP 변조, DHCP Attack
ICMP Attack
Solution :
Policing,ACL
TCP Syn Flooding
UDP Flooding, Scanning
Solution :
Policing,VACL,NBAR,PBR
Virus, Worm, 트로이 목마
Buffer Overflow
OS/App 취약점 공격
49


Catalyst 6500 Security Service Modules
Cisco.com
❑ Catalyst 6500 Security 적용
FWSM
FWSM
IDSM
MSFC
IDSM
MSFC
서버 사용자 그룹
서버사용자그룹 or 중요네트웍그룹의 분리
대용량 VPN
Aggregation용도
Catalyst 6500
VPNSM
Internet
PIX501
Internet
Interface
FWSM
IDSM
NAM
Interface
인터넷관문
Gigabit F/W
캠퍼스망
50

DDoS Prevention System

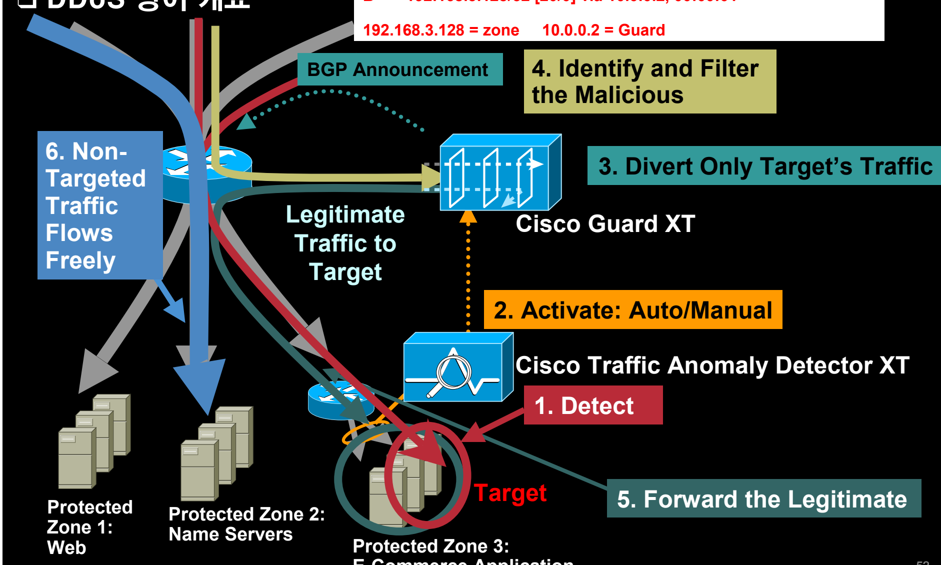
DDoS Prevention System

Cisco.com

❑ DDoS 방어 개요

```
O    192.168.3.0/24 [110/2] via 10.0.0.3, 2d11h, GigabitEthernet2
B    192.168.3.128/32 [20/0] via 10.0.0.2, 00:00:01

192.168.3.128 = zone     10.0.0.2 = Guard
```



DDoS Prevention System

Cisco.com

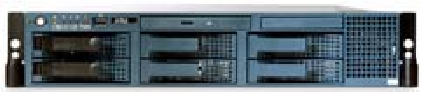
❑ Riverhead 제품군

Cisco Guard XT 5650

Attack *analysis & mitigation*

Diverts traffic flows for *on-demand scrubbing*

Cisco Traffic Anomaly Detector XT 5600



Attack *detection* to support on-demand, shared scrubbing

Monitors *copy of traffic*

Common Features

- Two Gigabit interfaces – MMF or GE-TX
- Two management interfaces
- Dual Xeon control plane, Broadcom Sibyte data plane
- Redundant power, RAID 1 dual drives

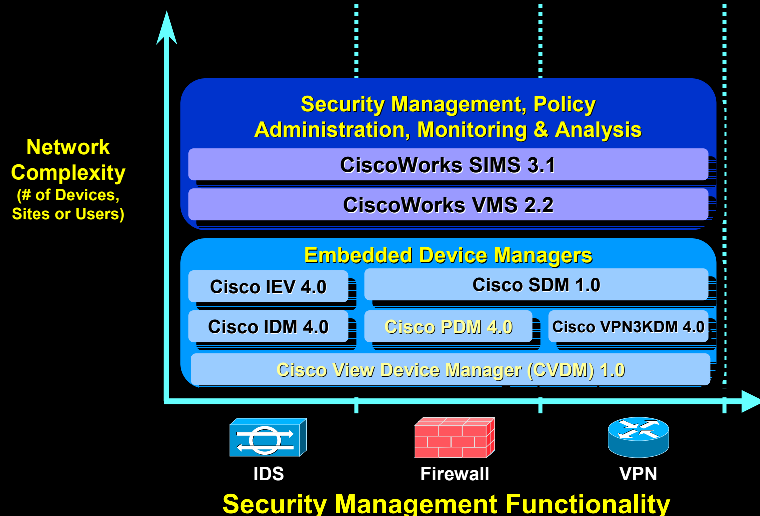
Guard / Detector SP Versions (4Q CY 04 FCS)

- dual SMF interfaces
- DC power and NEBS server

Security Management Solution

Security Management Solution

❑ **Security Management Portfolio**



Summary

Summary

Cisco.com

❑ Cisco Infra Security Solutions

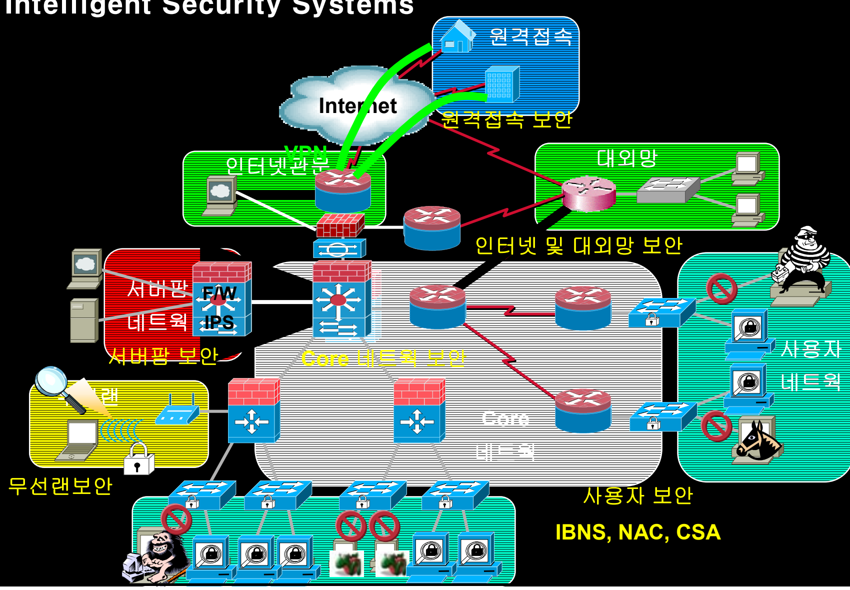
	Firewall	VPN	IDS/IPS
PIX	Yes	Yes	Yes(100개)
VPN 3000	Yes(Personal F/W)	Yes	No
Router	Yes(IOS)	Yes(IOS,H/W 모듈)	Yes(IOS,H/W 모듈)
Switch	Yes(FWSM)	Yes(VPNSM)	Yes(IDSM)

* Router/Switch의 경우엔 다양한 Enhanced Security 기능들(L3 보안, L2 보안 등)이 추가되어 있음

Summary

Cisco.com

❑ Intelligent Security Systems



Cisco Systems