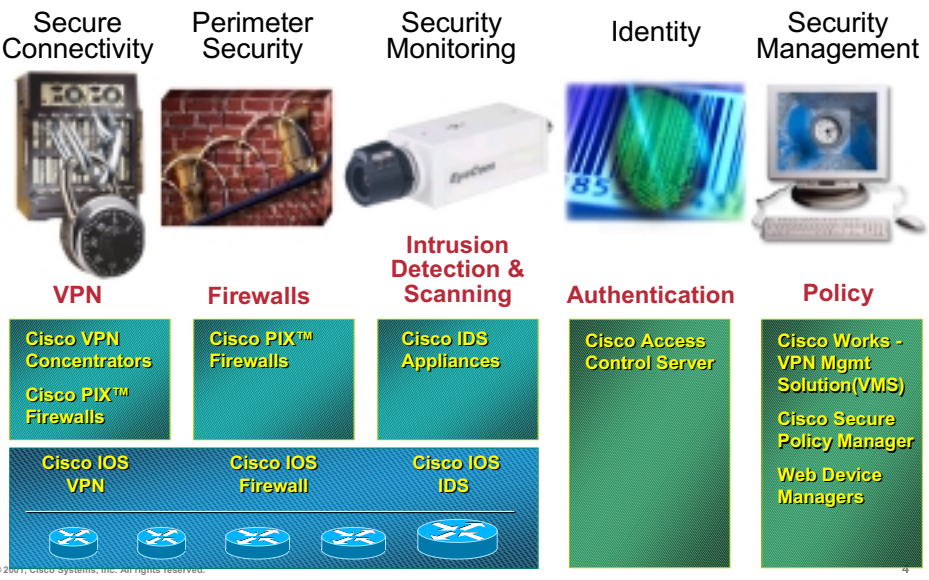
목차

Cisco.com

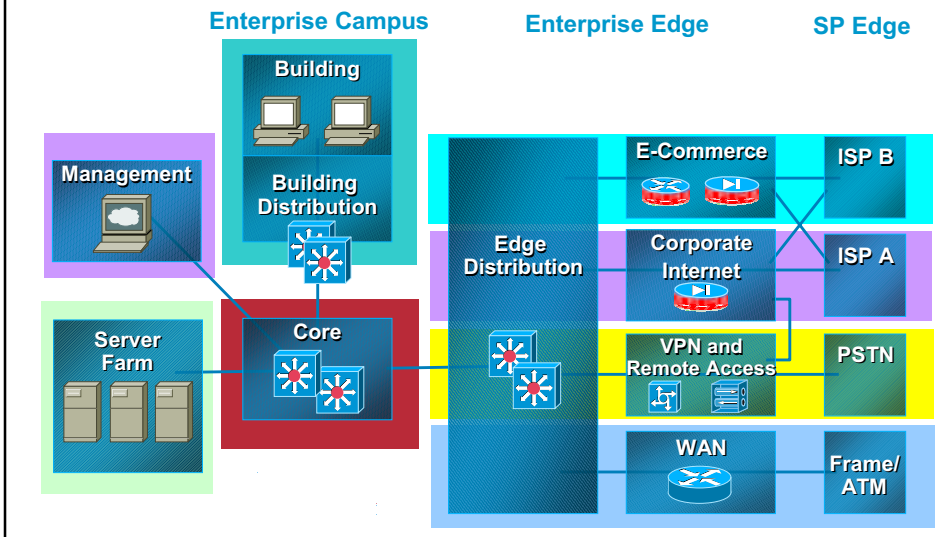
- **Cisco Security/VPN Solution 개요**
- **Product Update**
- **Network Security Design (VPN 중심)**

네트워 보안 요소 별 시스코 솔루션

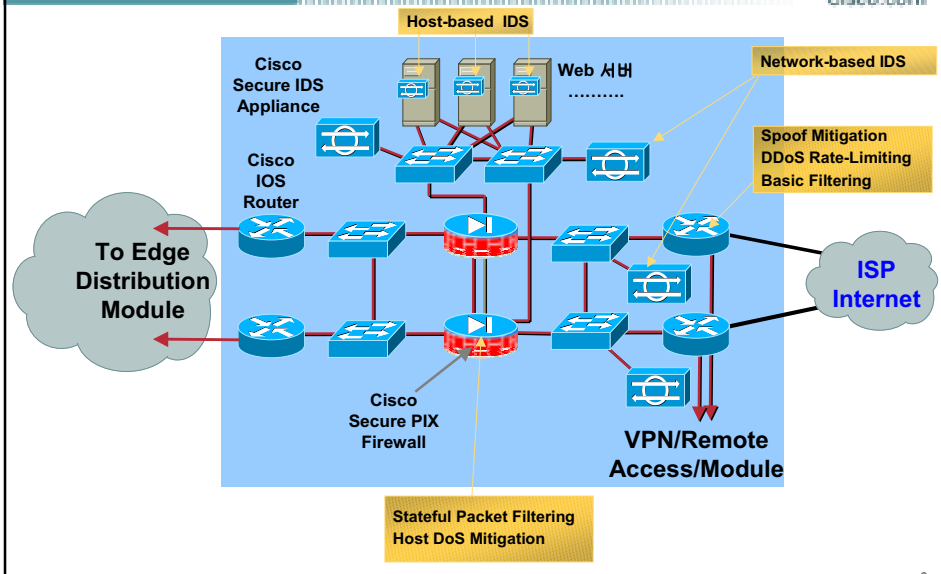
Cisco.com



일반적인 기업의 네트웍
Usually Modular/Hierarchical Design



기업의 인터넷 모듈

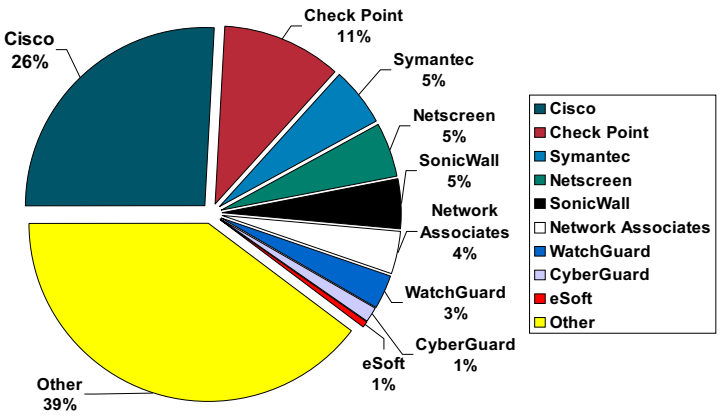


Cisco.com

Cisco in Market

전체 방화벽 시장 점유율
Q2CY01 - Infonetics Research

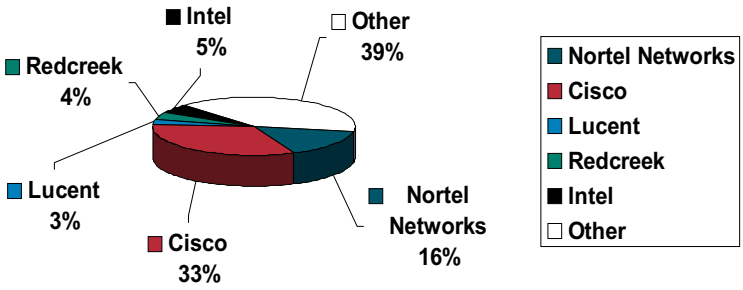
Cisco.com



Infonetics Research, August, 2001.
Based on $430.7M Worldwide Hardware & Software Firewall revenue.

VPN 전용 장비 시장 점유율
Q2CY01 - Synergy Research

Cisco.com

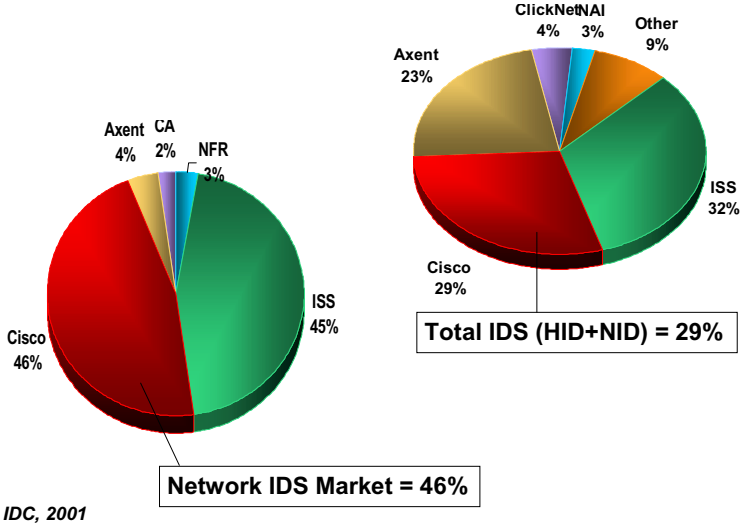


Synergy Research, August, 2001

- Cisco figure is assessed based on estimated revenues of Cisco VPN 3000 Concentrator and 7100 VPN Router
- CheckPoint/Nokia revenues were not included since figures for each respective company could not be distinguished by analyst firm.
- Based on $116.3M Total VPN Gateway revenue for Q2CY01.

침입탐지시스템 시장 점유율 - IDC

Cisco.com



Source: IDC, 2001

Cisco.com

Product Update
Firewall

Cisco Secure Firewall Solutions - PIX and Cisco IOS

Cisco.com

- **Cisco IOS firewall**
  - Embedded software solution
  - Provides Firewalling and IDS
- **Cisco Secure PIX firewall**
  - Firewall 전용 장비
  - VPN-Enabled
  - High-performance
  - Scalable
  - Stateful Fail-Over
  - Powerful inline IDS sensor (53)
  - Common Criteria EAL4 인증
  - K2인증 진행 중

Cisco PIX® 501 Firewall

NEW!

Cisco.com

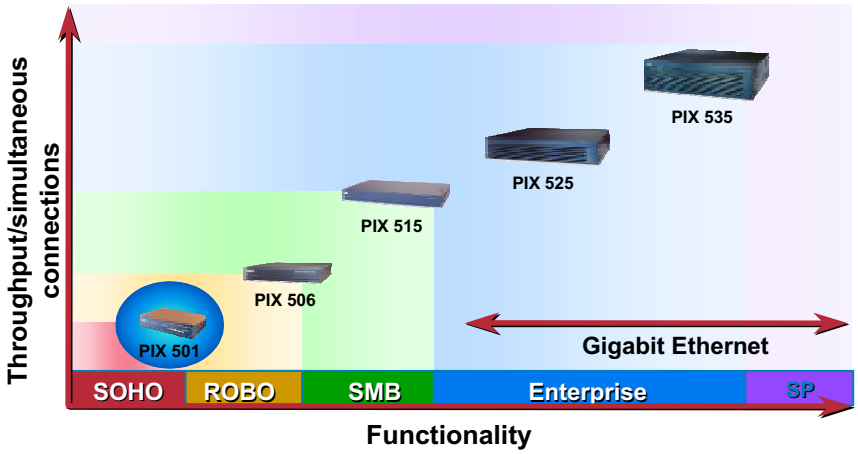
Front View

Rear View

- Intuitive LEDs display current status of all network ports, power and VPN tunnels
- Integrated security lock slot - improved physical security
- Console port - local PIX CLI access
- 10 BaseT port - outside interface
- Integrated 4-port 10/100 switch for inside "interface" with auto-sensing and auto-MDIX features

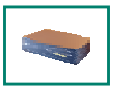
PIX Firewall Family Lineup

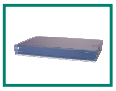
Cisco.com



PIX Firewall Product Line

GigE Enabled





Model	501	506	515-UR	525-UR	535-UR
Market	SOHO	ROBO	SMB	Enterprise	Ent.+, SP
Licensed Users	10 or 50	Unlimited	Unlimited	Unlimited	Unlimited
Max VPN Peers	5	25	2,000*	2,000*	2,000*
Size (RU)	< 1	1	1	2	3
Processor (MHz)	133	200	200	600	1 GHz
RAM (MB)	16	32	64	256	1 GB
Max. Interfaces	1 10BaseT + 4	2 10BaseT	6	8	10
Failover	No	No	Yes	Yes	Yes
Cleartext (Mbps)	10	20	145	320	1.7 Gbps
3DES (Mbps)	3	10	11	70*	95*

* Using a VPN Accelerator Card (VAC)

Cisco.com

Product Update
IDS & Scanning

Host vs. Network-Based IDS

Cisco.com

- Host-based : "Agent" software monitoring activity on hosts
- Network-based: Collects and analyzes data from the network

	장점	단점
Host-Based	• Can verify success or failure of attack • Generally not impacted by bandwidth or encryption • Understands host context and may be able to stop attack	• Impacts host resources • Operating system dependent • Scalability—Requires one agent per host
Network-Based	• Protects all hosts on monitored network • No host impact • Can detect network probes and denial of service attacks	• Switched environments pose challenges • Monitoring >100Mbps is currently challenging • Generally can't proactively stop attacks

Should View as Complementary!

Cisco IDS Host Sensor

Cisco.com

- Comprehensive protection for the server OS and server applications utilizing call interception techniques
- Sophisticated attack protection
  - OS and application attacks
  - Buffer Overflow attacks
  - Web server application attacks
  - SSL encrypted HTTP attacks
- Prevents access to server resources before any unauthorized activity occurs

Network-Based IDS Product Line Overview

Cisco.com

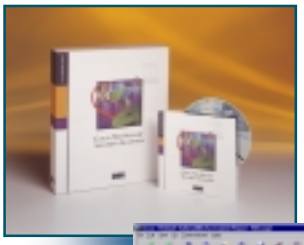
Model	4210	4230	C6000 IDSM
Size (RU)	1	4	1 slot
Processor (MHz)	566 (C)	Dual PIII-600	Custom
RAM (MB)	256	512	N/A
Performance (Mbps)	45	100	260
Response	Reset/Shun	Reset/Shun	Shun (v3.0)
Signature Coverage	Full	Full	Full

Cisco Secure Scanner

Cisco.com

Proactive, Preventative Security

- Helps manage risks
- Identifies security vulnerabilities
- Maps all active systems on a network
- Allows you to define and enforce security policies
- Windows or Solaris versions



Cisco.com

Product Update
Virtual Private Network

2가지 VPN 형태

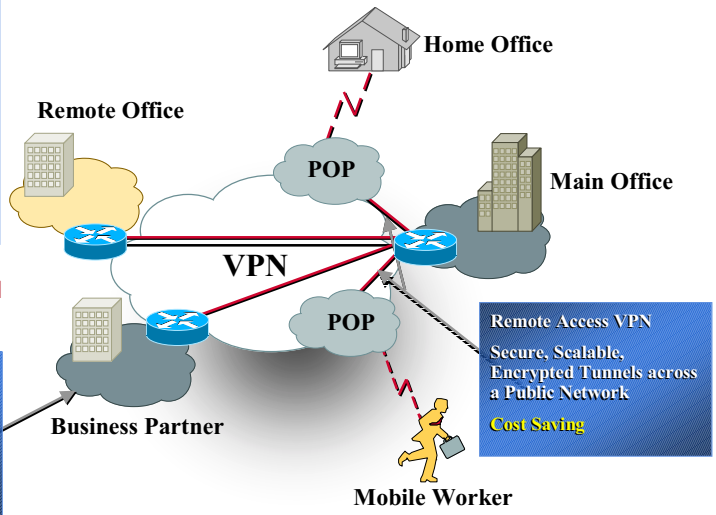
Cisco.com

Intranet VPN

Low Cost, Tunneled Connections with Rich VPN Services

Cost Saving and New Applications

Site-to-Site VPN



Extranet VPN

Extends WANs to Business Partners

New Applications and Business Models

Remote Access VPN

Secure, Scalable, Encrypted Tunnels across a Public Network

Cost Saving

Remote Access VPN

Cisco VPN 3000 Series

Cisco.com

Network Computing
EDITOR'S CHOICE

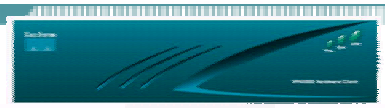
	3005	3015	3030	3060	3080
Number of Users	100	100	1500	5000	10,000
Encryption	SW	SW	HW	HW	HW
WAN Capability	Yes	Yes	Yes	Yes	Yes
Performance	4 Mb/s	4 Mb/s	50 Mb/s	100 Mb/s	100 Mb/s
Memory	32 MB	128 MB	128 MB	256 MB	256 MB
SEPs	0	0	1	2	4
Upgradable	No	Yes	Yes	Yes	N/A
Supports Dual PS	No	Yes	Yes	Yes	Yes
Redundancy	No	Yes	Yes	Yes	Yes
Site-to-Site Sessions	100	100	500	1000	1000

Cisco S/W VPN Client

Cisco.com

- Connectivity between all clients and all Cisco central-site VPN gear
- Centralized push policy technology:
  - Simplifies user experience
  - Provides more control for companies
  - Reduces complexity of VPN deployments
- Cisco VPN concentrators/IOS routers/ PIX– Based
  - Includes non-Windows OS (Linux, Mac, Solaris)
- Substantial savings:
  - Reduced support expense
  - Consolidated hardware
  - Reduced administration in the central site at the central site

Cisco VPN 3002 H/W Client



New

Front

Basic 3002 without Switch

3002 unit with 8 Port 10/100 Switch

- Industry's first TRUE hardware client
  - Used in place of software client—it deploys like a client
- Simplifies deployment and manageability
- Scales to very large networks (tens of thousands of units)
- Includes two hardware versions:
  - Dual Ethernet
  - Ethernet with 8 port 10/100 Mbps AUTO-MDIX switch
- Widens number of VPN environments customers can implement, working alongside or independent of the software client

VPN-Enabled Broadband Routers

Cisco 806 Broadband Gateway Router

	806	827/804	905
Simultaneous Tunnels	50	50	50
Performance	384 kbps	384 kbps	6 Mbps
Hardware Acceleration	None	None	(built-in)
WAN Interfaces	Ethernet	DSL/ISDN	Cable
LAN Interfaces	4xEthernet	1xEthernet	4xEthernet

VPN-Enabled Broadband Routers

	1710	1720/1750	2611/2621	2611/2621	3620/3440
Simultaneous Tunnels	100	100	300	300	800
Performance(Mbps)	4	4	10/12	10/12	10/19
Hardware Acceleration	(Built-in)	VPN Module	AIM-VPN/BP	AIM-VPN/EP	NM-VPN/MP
WAN Interfaces	1xEthernet	(Varies)	(Varies)	(Varies)	(Varies)
LAN Interfaces	1xFE	1xFE	2xFE	2xFE	(Varies)

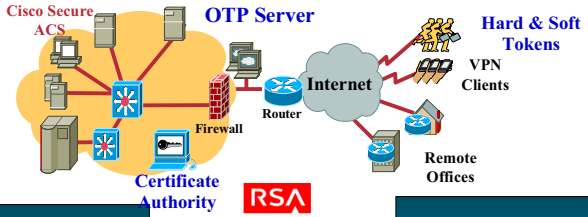
	3660	7120	7140	7140	7200
Simultaneous Tunnels	1,300	2,000	2,000	3,000	5,000
Performance(Mbps)	40	50	90	140	145
Hardware Acceleration	AIM-VPN/HP	ISM	ISM	ISM&ISA	SA-VAM
WAN Interfaces	(Varies)	(Varies)	(Varies)	(NONE)	(Varies)
LAN Interfaces	1xFE	2xFE	2xFE	2xFE	(Varies)

Product Update
Access Control Solution

Authentication, Authorization, and Accounting (AAA)

Unified control of user identity for the Enterprise

3000 VPN Concentrators, Cisco IOS Routers, PIX Firewalls



- Identity/Authentication
- Public Key Infrastructure
- Digital Certificates (x.509)
- Certificate Authorities
  - SCEP
- Public Key Exchange
  - RSA
  - DH

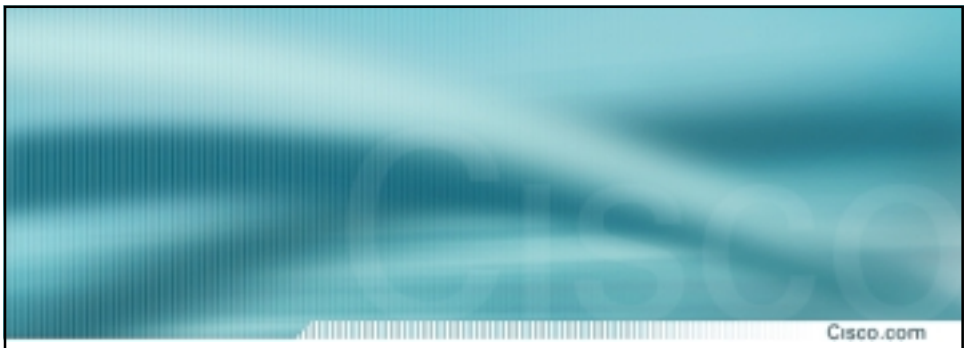
RSA SECURITY, VeriSign, Baltimore, Entrust, SECURE COMPUTING, Microsoft, CRYPTOCard

- Authentication Methods:
  - Passwords
  - One Time Passwords(OTP)
  - RADIUS
  - TACACS

Cisco Secure ACS v2.6

- Easy-to-use Web GUI
- Full RADIUS & TACACS+ user and administrator access control
- High performance (500+ auths per sec)
- Supports LDAP, NDS, ODBC datastores
- Scalable- data replication and redundancy services
- Full accounting and user reporting features

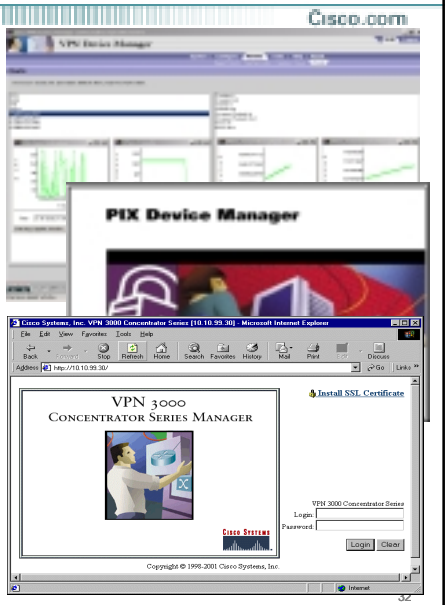
Wireless Support



Product Update
Security and VPN Management

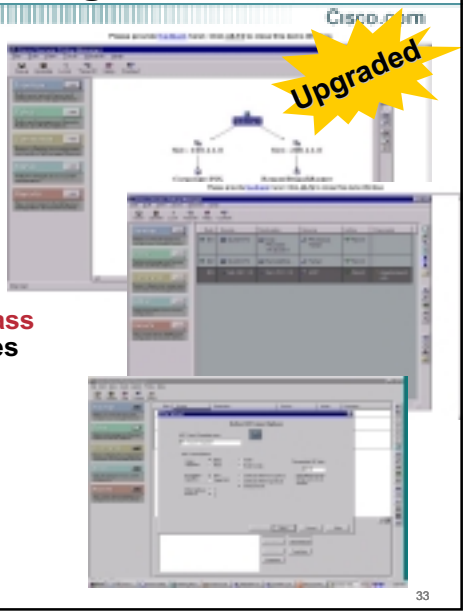
Cisco Device Manager

- VPN Device Manager (VDM)
  - Web-based VPN site-to-site VPN
  - Supports 7100, 7200
  - Tunnel throughput/ Errors/ VPN performance
- PIX Device Manager (PDM)
  - Web-based configuration and monitoring application
  - SSL access for single device management
- VPN 3000 Concentrator Manager
  - Web based monitoring, administration, & configuration
  - Supports remote access and site-to-site VPN
  - SSL for security of mgmt traffic
  - Supports the VPN 3002 H/W Client, 3005, 3015,3030, 3060, 3080



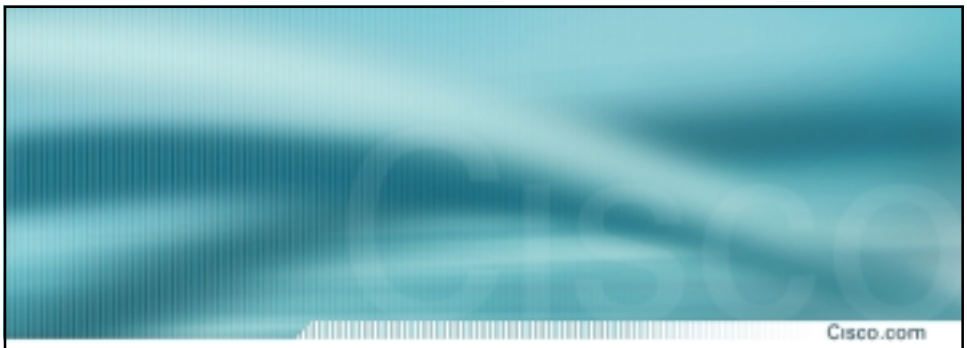
Cisco Secure Policy Manager - CSPM v3.0

- Centrally manages policies that support configurations of Cisco security products
- Defines appropriate policies for networks
- Centralized mgmt. Alleviates mass configurations of several devices
- Basic auditing tools to alert sys. admin of network events
- Implement at central site on the internal network



VPN/Security Management Solution(VMS)

- Integrated solution for VPN & Security Management
  - VPN / Firewall / Network-based IDS /Host-based IDS
- Includes IDS Host Sensor 2.0.1
- New version of CSPM 3.0
- New version of VPN Monitor 1.1
  - Now supports 1700, 2600, and 3600



네트웍 보안 설계
VPN 중심

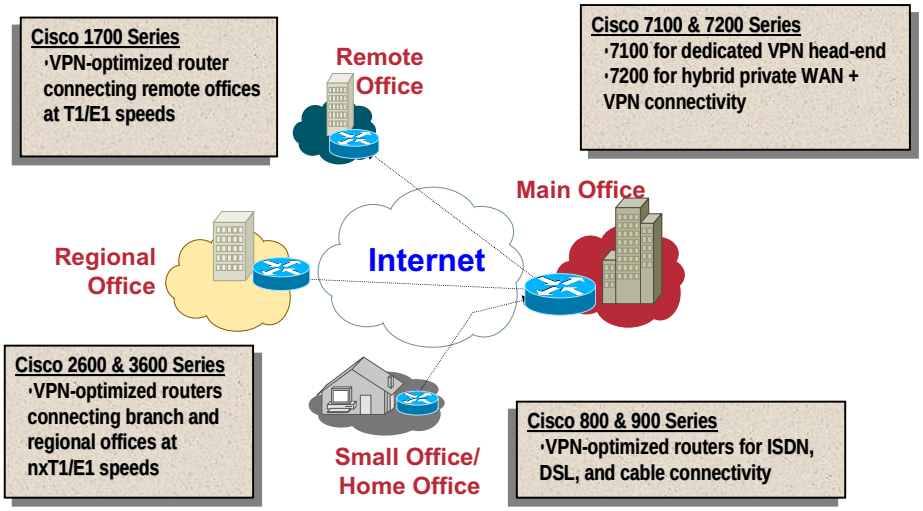
VPN Design 고려사항

Cisco.com

- Performance/Scalability
  - PIX-Based/Router-Based/Concentrator/Mixed VPN
  - Routing : Static / Dynamic Routing(Router-based)
- Network Topology
  - Point-to-point : Natural for encryption
  - Hub and spoke : 90% hub ⊂ spoke; 10% spoke ⊂ spoke
  - Full-mesh : > 50% Spoke ⊂ Spoke
- Redundancy/Fail-Over
- Manageability
- Quality of Service (VoIP)

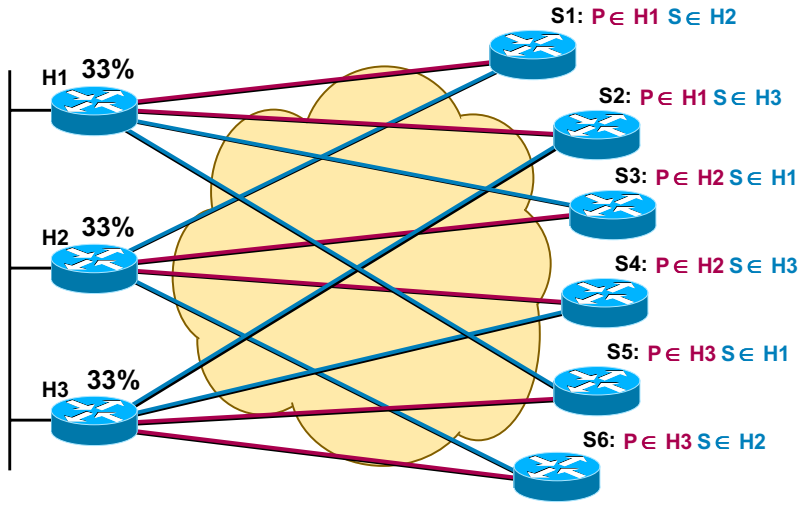
Case 1 - Site-to-Site VPN Design Based on VPN enabled-Router

Cisco.com

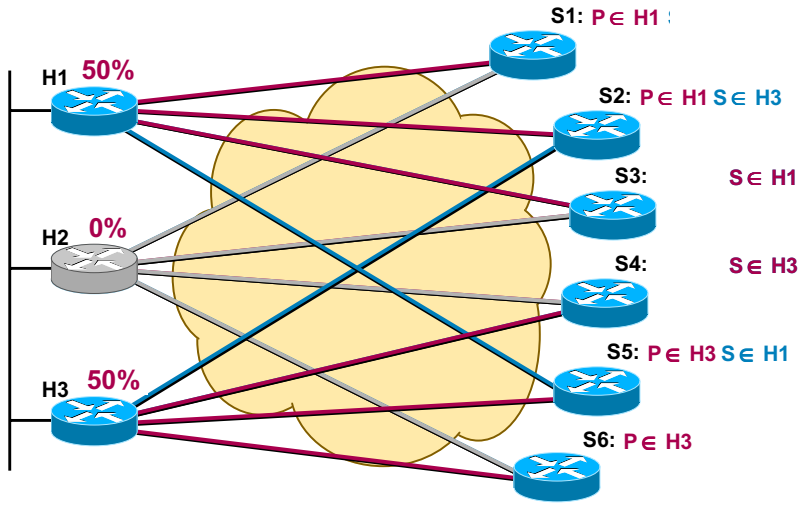


Case 1.1 - Redundant Hub-Spoke Site-to-Site VPN (Initial)

Cisco.com

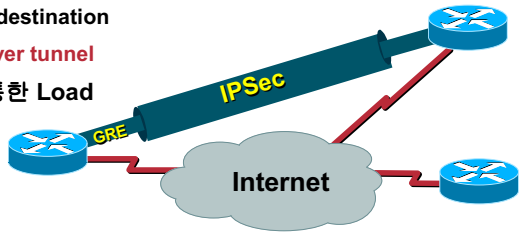


Case 1.1 - Redundant Hub-Spoke Site-to-Site VPN (After Fail)

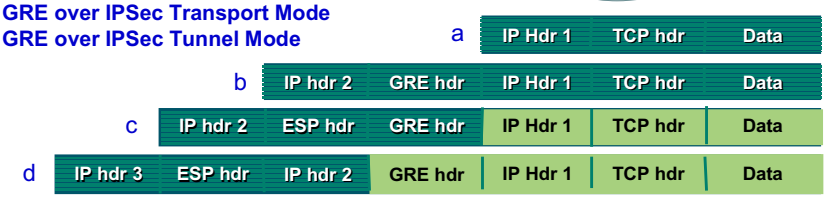


Case 1.2 - Dynamic Routing using GRE over IPSec

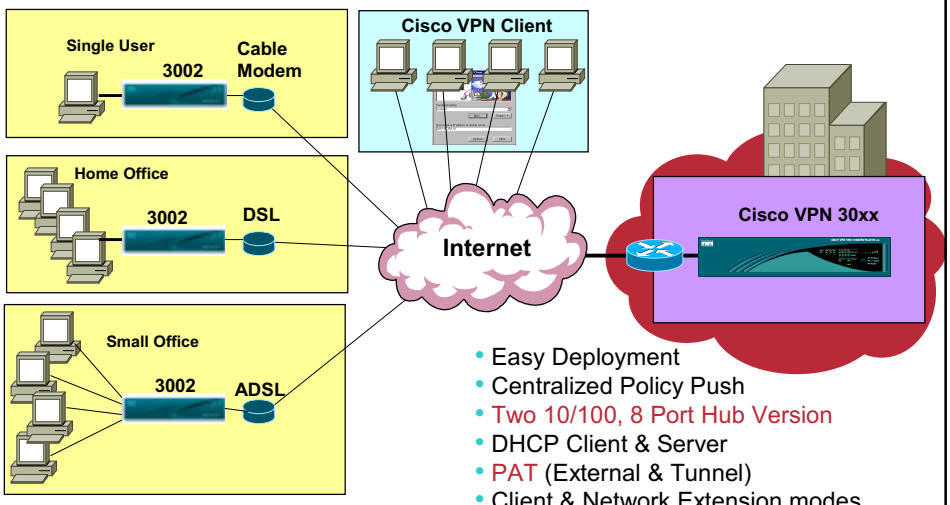
- Generic Routing Encapsulation(RFC 1701)
  - Multicast, Multiprotocol, …
  - Implemented using a virtual interface
  - Point-to-point - static tunnel destination
  - Can run a routing protocol over tunnel
- Dynamic Routing Protocol을 통한 Load Balancing 및 Backup



a. Original Packet
b. GRE Encapsulation
c. GRE over IPSec Transport Mode
d. GRE over IPSec Tunnel Mode

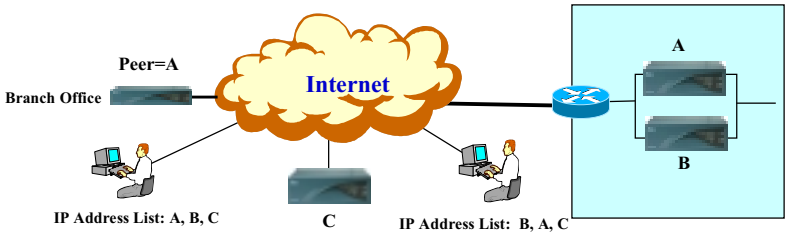


Case 2 - Remote Access VPN
Cisco VPN Concentrator & Client



- Easy Deployment
- Centralized Policy Push
- Two 10/100, 8 Port Hub Version
- DHCP Client & Server
- PAT (External & Tunnel)
- Client & Network Extension modes

Case 2.1 - Remote Access VPN
Concentrator Redundancy

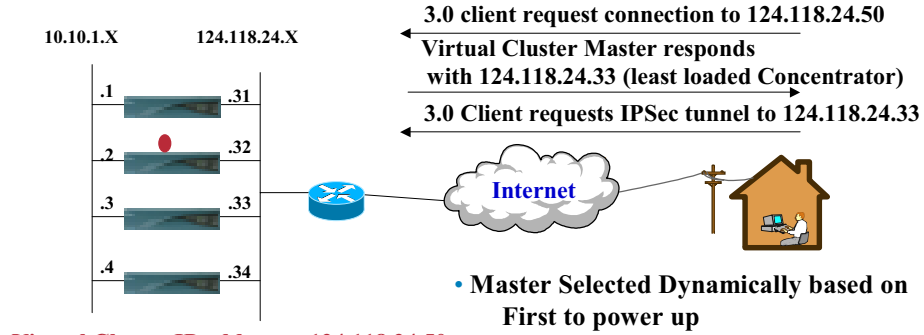


- **Remote Access**
  - **Multiple IP Addresses in the IPSec client**
- **Redundant Platform**
  - **Redundant Power Supplies, Redundant Fans**
  - **Hot Swap & Redundant SEP Modules**
  - **Virtual Router Redundancy Protocol (VRRP)**

Case 2.2 - Remote Access VPN
VPN Concentrator Load Balancing

Cisco.com

"Virtual Clustering"



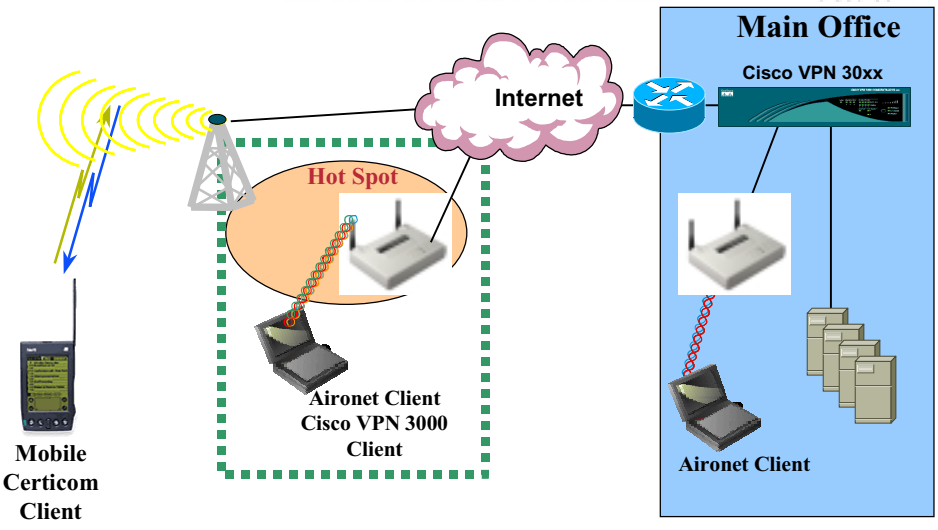
Virtual Cluster IP address = 124.118.24.50

Virtual Cluster Master

- Master Selected Dynamically based on
  - First to power up
  - Priority (1 – 10)
  - Lowest IP address
- Supported by 3.0 Client only

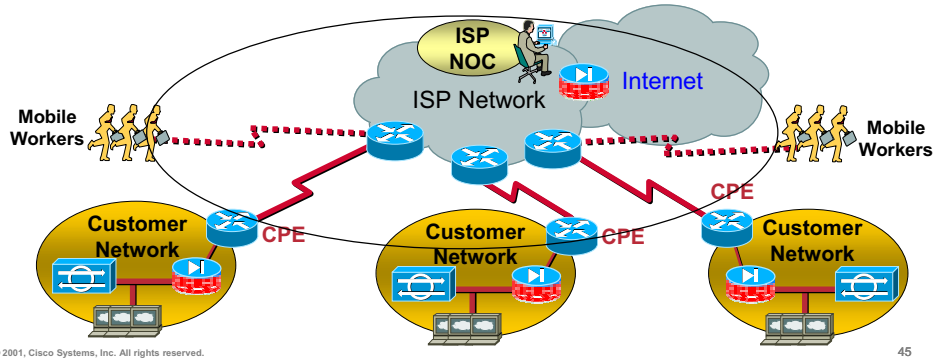
Case 2.3 - Remote Access Wireless VPN

Cisco.com

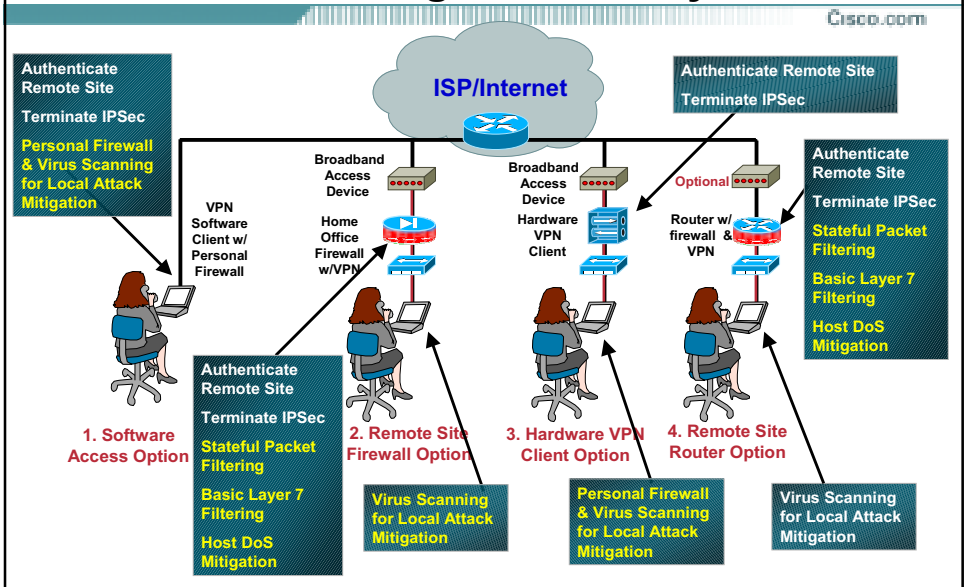


Case 3 - SP가 제공하는 VPN 서비스 이용

- "SP-provided VPN" 서비스 (MPLS / IP VPN)
  - Site-to-Site VPN / Remote Access VPN
  - Guaranteed 서비스 (SLA)
- SP가 네트웍 장비 관리/모니터링/리포팅 서비스를 제공
  - Traffic Filtering / Managed Firewall / Managed IDS



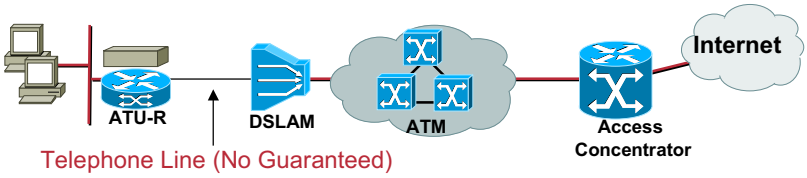
Remote Sites Design 시 Security 보완 사항



Cisco VPN support using ADSL

Cisco.com

서비스 제공업체 사용 Protocol	사용 IP	지원 제품
PPPoE	유동 IP (DHCP)	PIX (Ver. 6.2) VPN 3002 (Ver. 3.1) Router – ADSL 지원 IOS
PPPoA	유동 IP (DHCP)	Router – ADSL 지원 IOS
IPoA, RBE	고정 IP, Multi-IP	PIX / VPN 30XX / Router ALL



Why Cisco for Security?

Cisco.com

- No one knows your network or the Internet better
- Compatibility with the installed Cisco base (80% of the Internet)
- $$ savings from a single-vendor solution
- Excellent quality, standards-based development, and certified products
- Market-leading solutions, services, and support

******** Thank You ! *******