시스코 ADSL/VPN/Security Solution

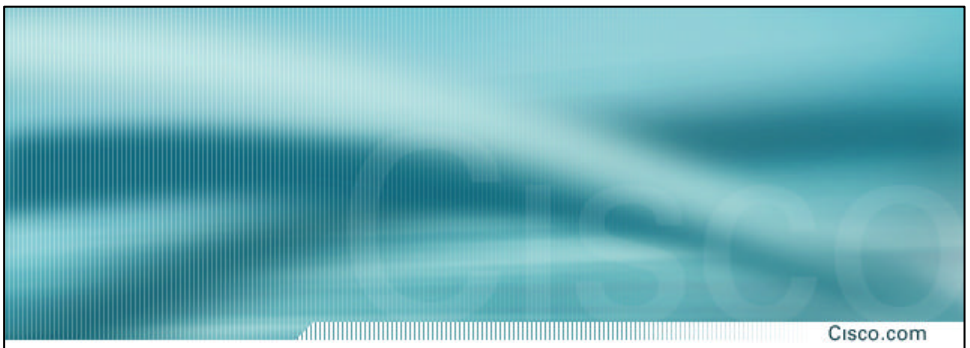
Cisco.com

정희철
System Engineer
Cisco Systems Korea

목차

Cisco.com

- VPN Solution
- ADSL Solution
- Remote Access VPN Solution
- Site-to-Site VPN Solution
  - Site-to-Site VPN 구성 방안
  - VPN 네트워크 디자인
  - Site-to-Site VPN 제품
- VPN Router 보안 강화 방안
- 평가 인증



VPN Solution

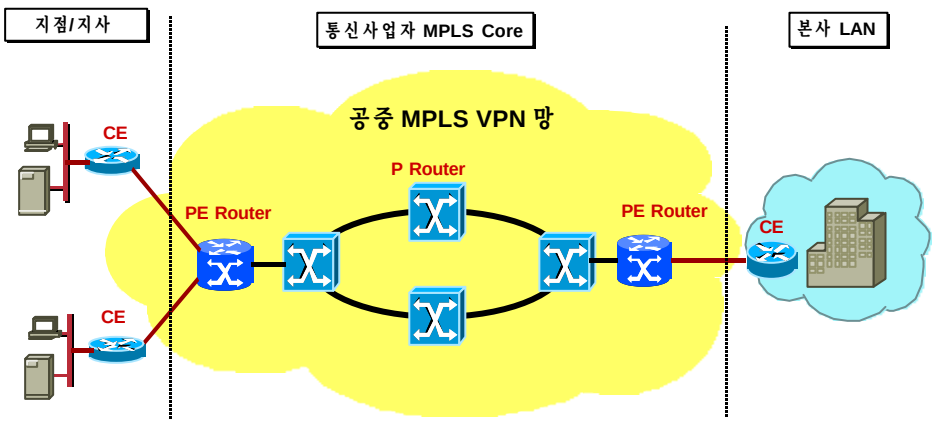
VPN Solution 분류

Cisco.com

- 서비스 Provider data delivery
  - L2 vs L3
  - PPP (tunnel)
  - Packet (IP, GRE, MPLS-VPN, IPSEC)
- 자체 구축 방안
  - IPSec을 이용한 VPN 구성

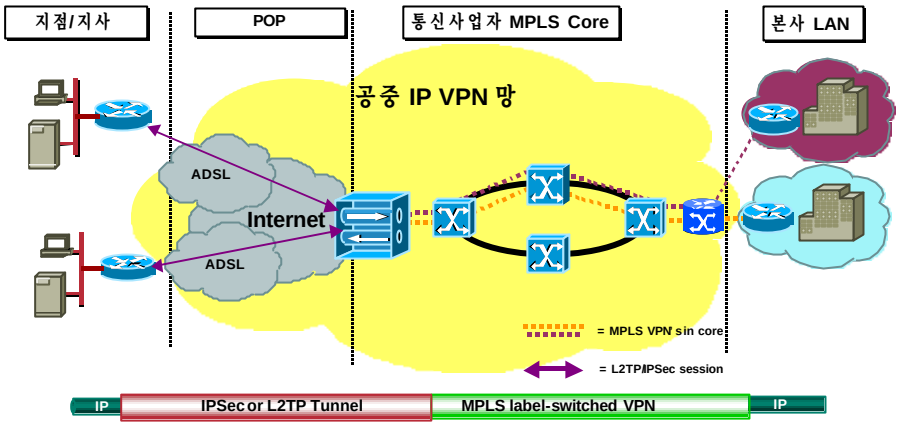
MPLS VPN

Cisco.com



MPLS VPN + L2TP/IPsec

Cisco.com



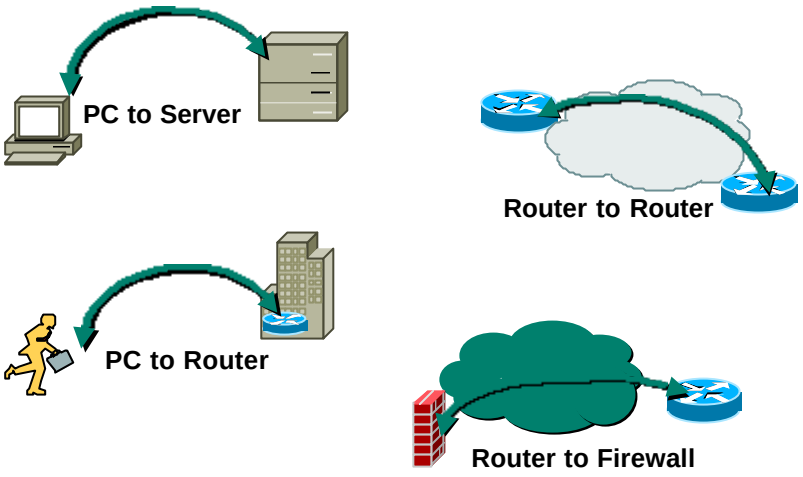
Site-to-Site and Remote Access VPNs

Cisco.com

- **Site-to-site**
  - Between two network entities
  - Trusted networks behind each entity
- **Remote access**
  - Central control of remote users
  - No trusted networks at remote location

IPsec VPN Implementation

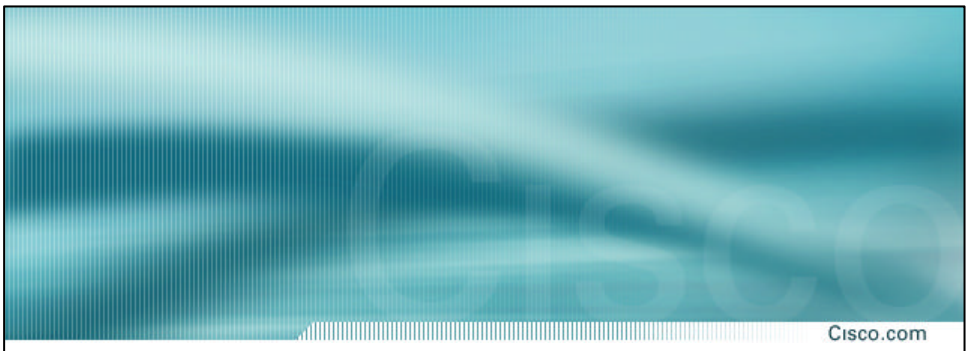
Cisco.com



Network-Based Implementation

Cisco.com

- **Routers**
  - All-purpose network device
- **Firewalls**
  - All-purpose security device
- **Dedicated devices**
  - Single purpose which stands by itself
- **Mixed environments**



ADSL Solution

DSL 기술 비교

DSL Service	Max. Data Rate Down/Uplink (bps)	Analog Voice Support	Max. Reach (km-feet)
VDSL–Very High Bit Rate	25M/1.6M or 8M/8M	Yes	.9–3,000
ADSL–Asymmetric	8M/1M	Yes	5.5–18,000
IDSL–ISDN DSL	144K/144K	No	5.5–18,000
SDSL–Symmetric	768K/768K	No	6.9–22,000
G.SHDSL	2.3M/2.3M.	No	8.15–26,000

Residential

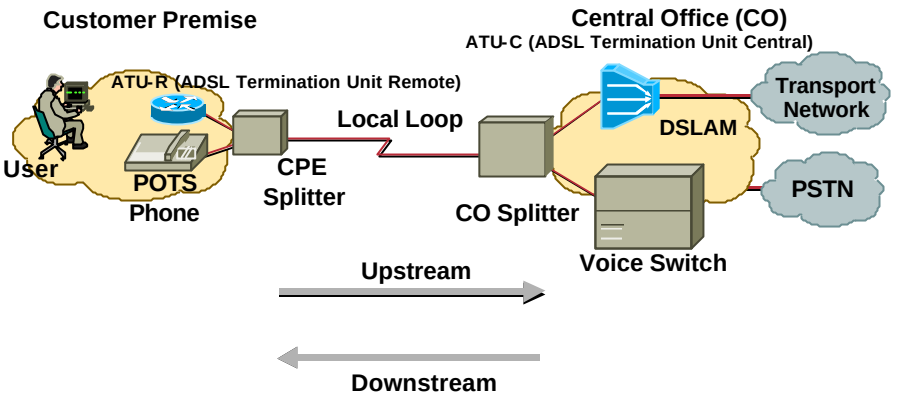
SOHO

Business

- Trade-off is reach vs. bandwidth
- Reach numbers imply “Clean Copper”
- Different layer 1 transmission technologies, need a common upper protocol layer to tie them together

ADSL Forum Reference Model

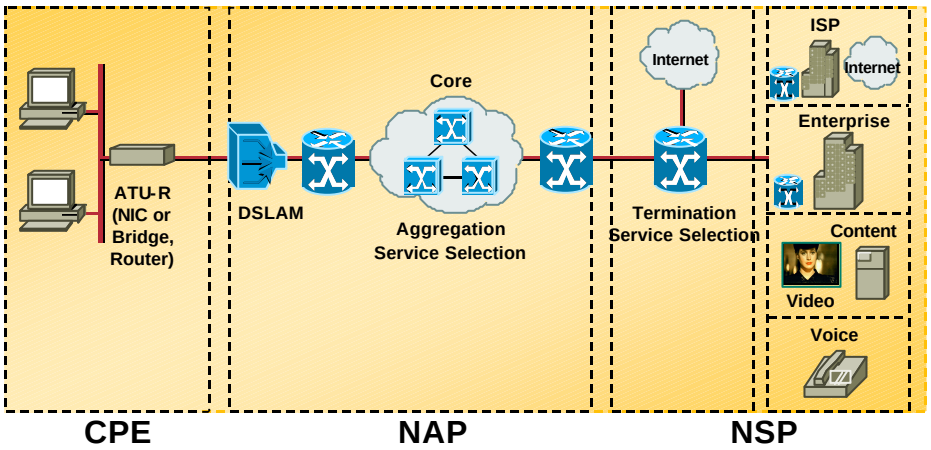
Cisco.com



Like Dial, Cable, Wireless, and T1, DSL Is a Transmission Technology

ADSL의 기능적 분류

Cisco.com



CPE —Customer Premise Equipment
NAP —Network Access Provider
NSP —Network Service Provider

IP over AAL5

Cisco.com

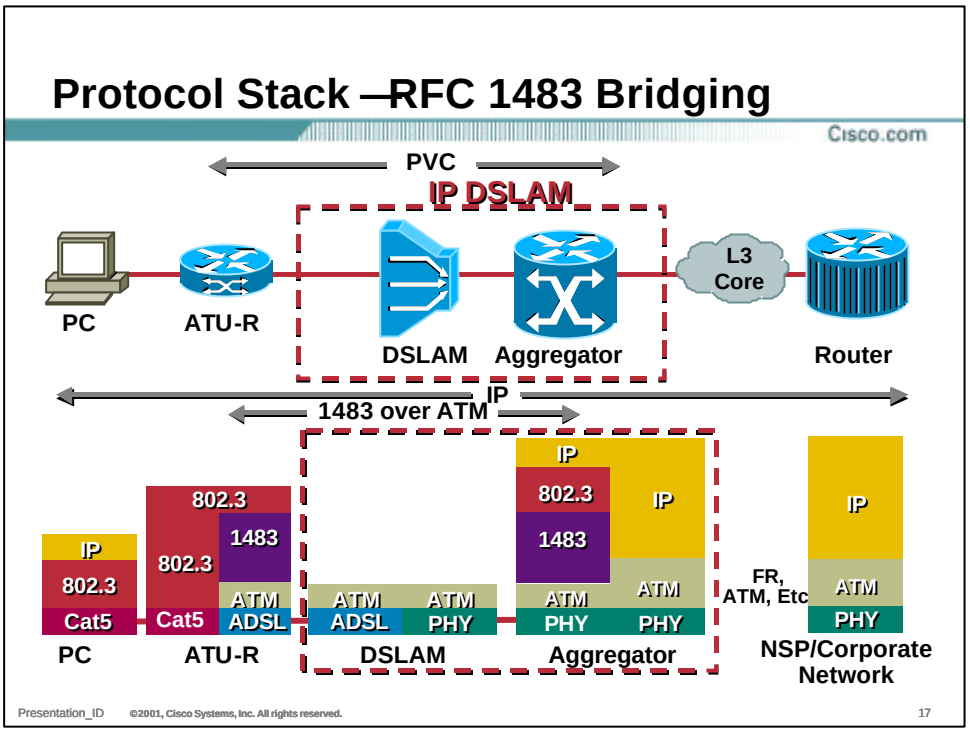
- Multiple methods exist for encapsulating IP packets in AAL5 PDUs (Protocol Data Units)
  - RFC 1483 (MPOA) bridging and routing (RFC 2684) – My IP (2개 이하)
  - PPP over ATM (RFC 2364) – Easy IP
  - PPP over Ethernet (RFC 2516) – Easy IP
  - RFC 1577 (classical IP over ATM) – Multi-IP (3개 이상)
- Different approaches yield different service offerings, architecture choices

Bridging Implementation

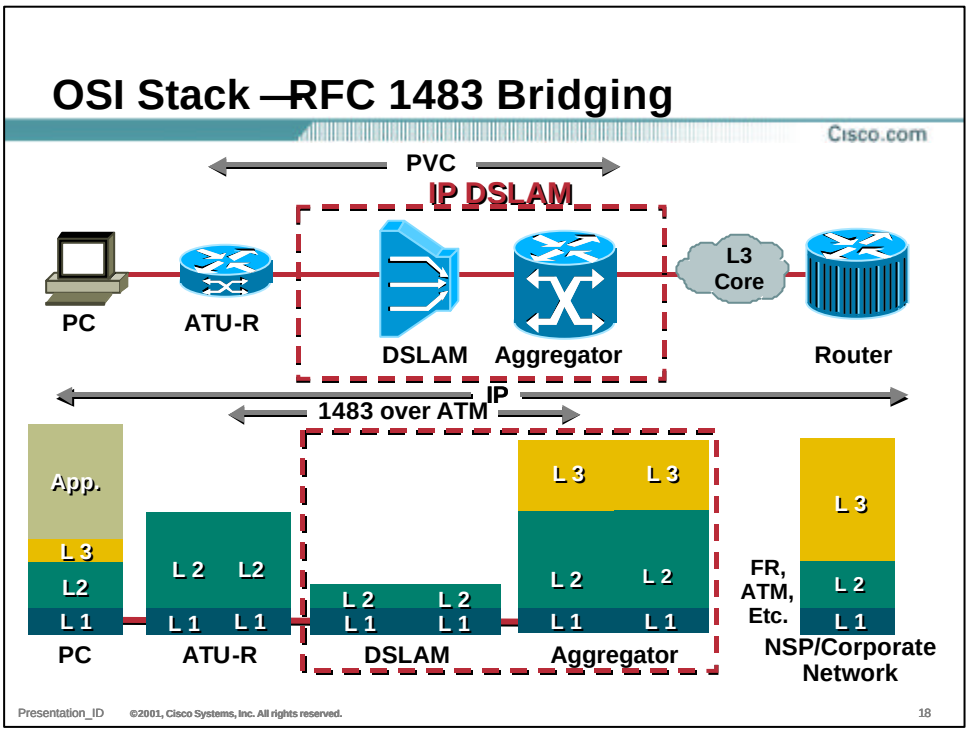
Cisco.com

- CPE—RFC 1483 (now RFC 2684) bridging
- Aggregation/termination
  - Integrated Routing Bridging (IRB)
  - Routed Bridge Encapsulation (RBE)
- Core
  - Usually ATM, if no aggregation used
  - With VC aggregation, typically IP or IP+ATM

Protocol Stack—RFC 1483 Bridging



OSI Stack—RFC 1483 Bridging



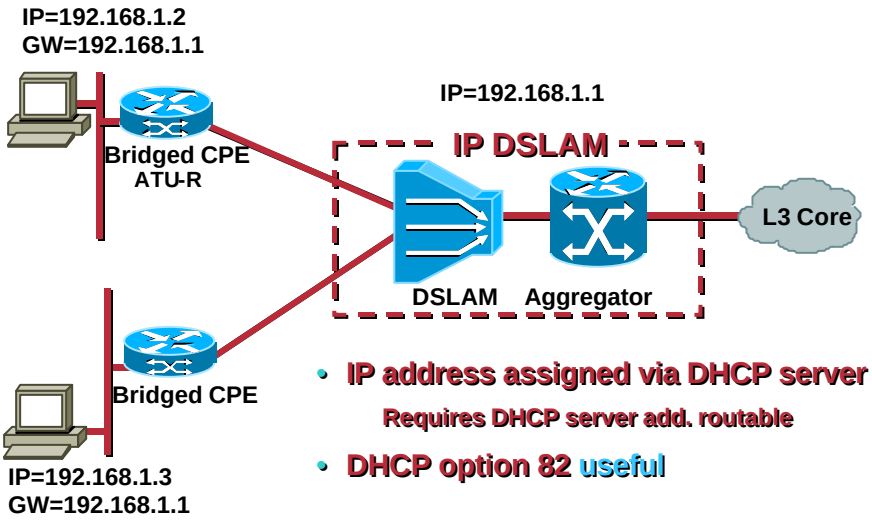
How Does RBE (Routed Bridge Encapsulation) Work?

Cisco.com

- Subscriber traffic is carried in a BPDU (Bridged Protocol Data Unit)
- The routed-bridge ATM interface treated as a routed interface;
- For packets originating from the subscriber end
  - Ethernet header is skipped
  - Packet forwarded based on Layer 3 information
- For packets destined to the subscriber end
  - Destination IP address is checked on the packet
  - Outbound interface is determined from routing table
  - ARP (Address Resolution Protocol) table is checked for the destination Mac address, if none found than ARP request sent out on the destination interface only

Typical RBE Architecture

Cisco.com



- IP address assigned via DHCP server
  - Requires DHCP server add. routable
- DHCP option 82 useful

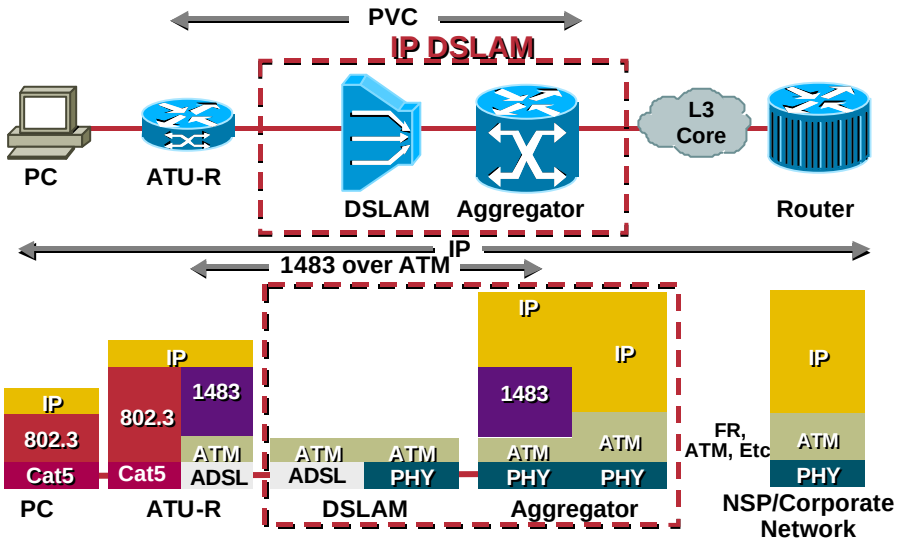
Routing Implementation

Cisco.com

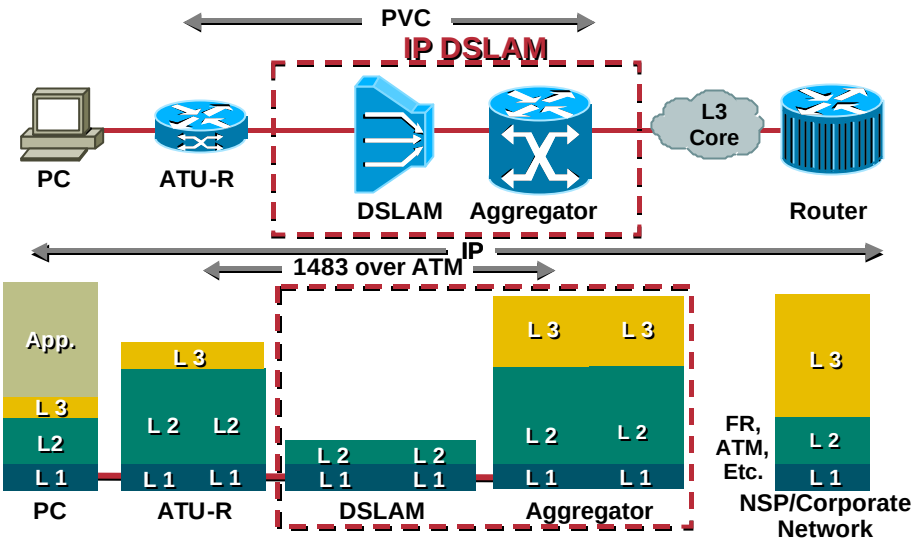
- **CPE**
  - CPE in routing mode, single or multiple subnet behind CPE
  - Routing protocol support
- **Aggregation**
  - Learns subscriber routes through routing protocol or static routes
- **Core**
  - Typically,IP or IP+ATM (MPLS/VPN)

Protocol Stack — RFC 1483 IP Routing

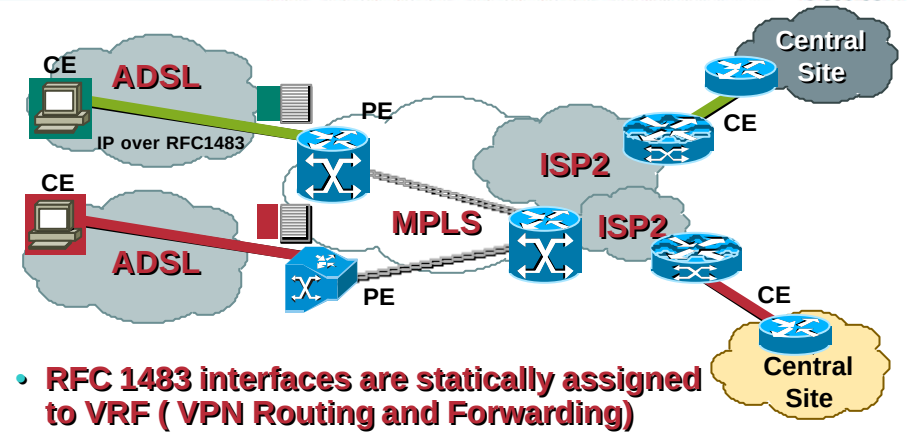
Cisco.com



OSI Stack —RFC 1483 Routing



RFC 1483 Routing



- RFC 1483 interfaces are statically assigned to VRF (VPN Routing and Forwarding)
- Can run RIP, BGP across upstream interfaces
- IP Address Assigned Via DHCP Server

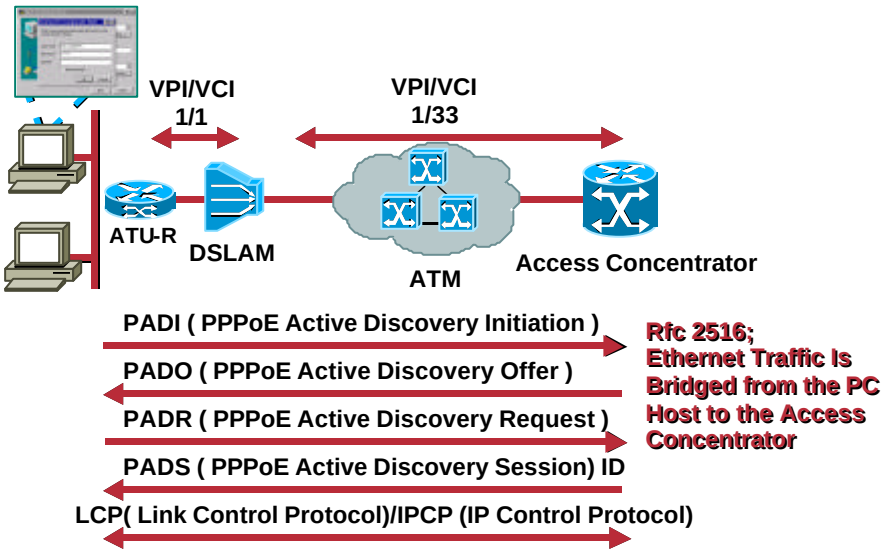
PPP (Point to Point Protocol) Implementation

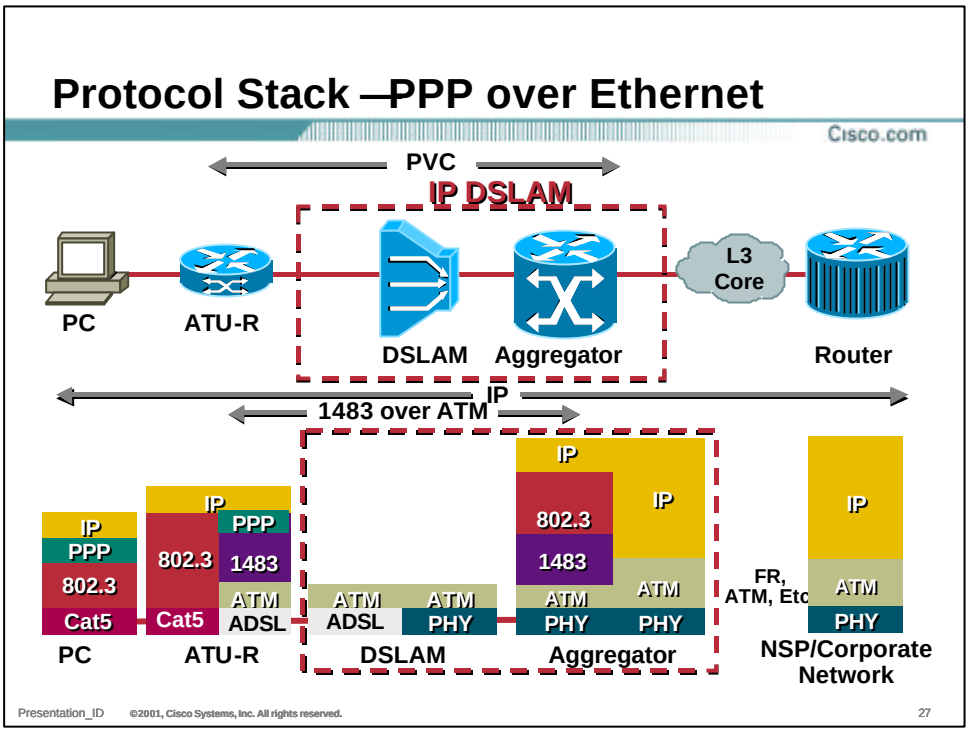
Cisco.com

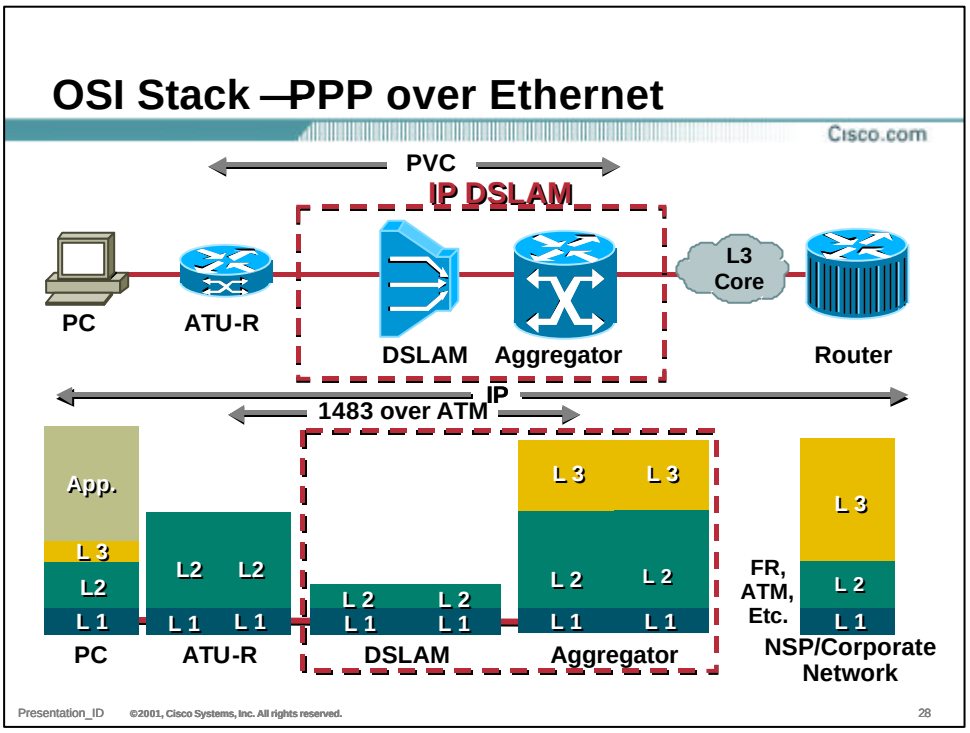
- **Three access methods from subscriber**
  - **PPPoA, PPPoE, L2TP client**
- **Aggregation**
  - **PPP sessions terminated**
  - **PPP sessions tunneled over to NSP**
- **Core**
  - **End–to–end ATM PVC, PPP terminated at NSP IP, ATM or IP+ATM; (L2TP, L2F, MPLS/VPN)**

How Does PPPoE Work?

Cisco.com

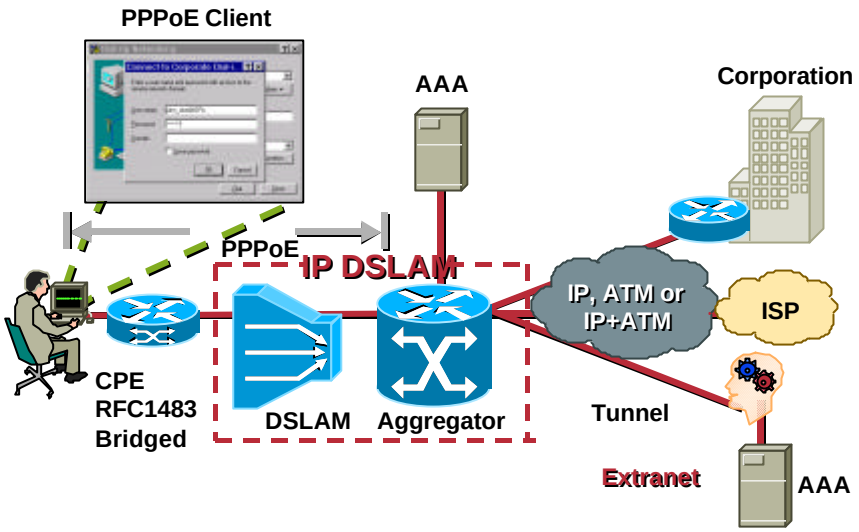






Typical PPPoE Architecture

Cisco.com



PPPoE IP Address Management

Cisco.com

- **Same as PPP in dial mode**
  - Address can be assigned to host by NAP (Network Access Provider) if session terminated, or by NSP (Network Service Provider) if tunneled
- **IP addresses assigned by RADIUS**
  - Local or proxy
- **IP address assigned from pool**
  - Local or from radius
- **The Ethernet NIC on PC does not need an IP address to start the PPPoE session**

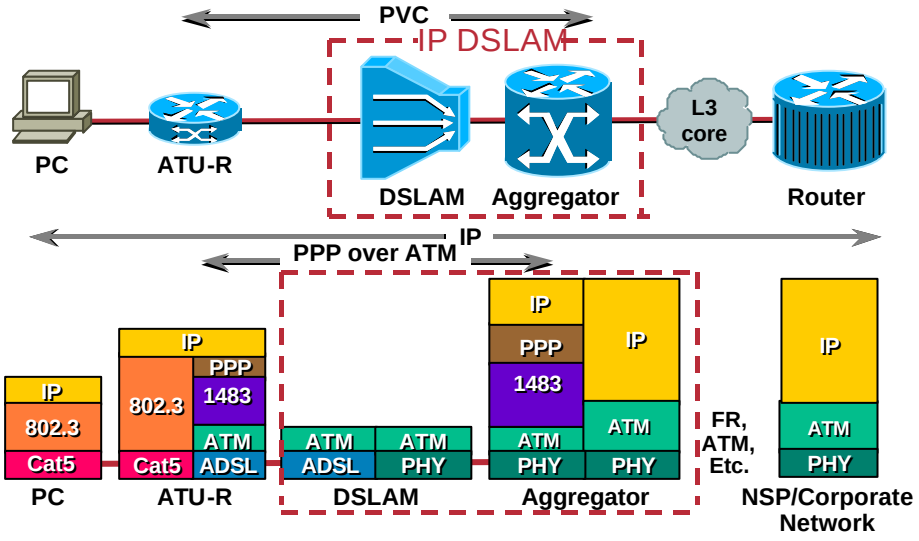
How Does PPPoA Work?

Cisco.com

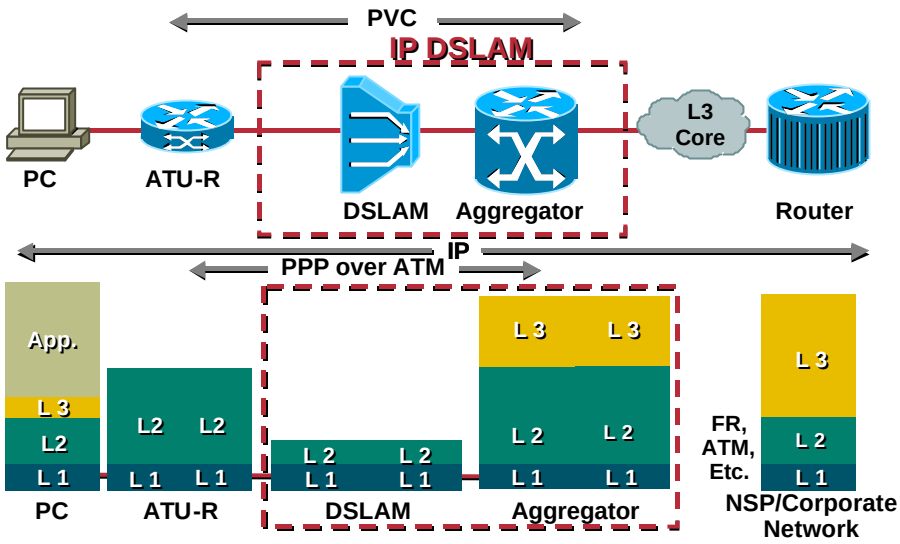
- Based on RFC 2364 (PPP over AAL5)
  - VC multiplexed PPP, LLC (Link Layer Control) encapsulated PPP
- CPE and aggregation goes through;
  - LCP (Link Control Protocol) negotiation
  - Authentication phase
  - IPCP (IP Control Protocol)
- Aggregation configured with virtual template
  - Brings up the virtual access interface
  - Assigns IP address to the CPE via local pool, dhcp, local radius or proxy radius
  - Establishes a 32-bit host route

Protocol Stack — PPP over ATM

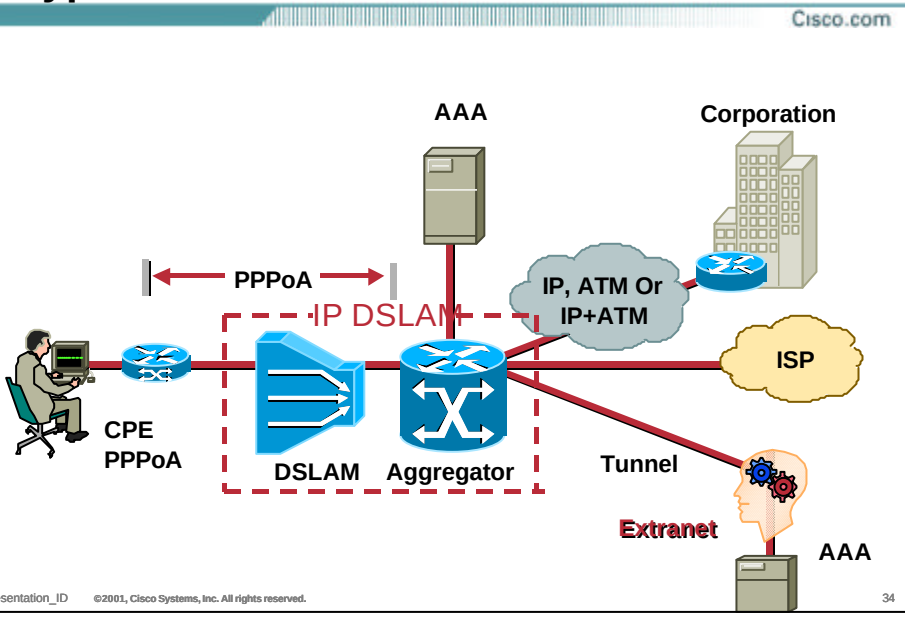
Cisco.com



OSI Stack—PPP over ATM



Typical PPPoA Architecture



PPPoA IP Address Management

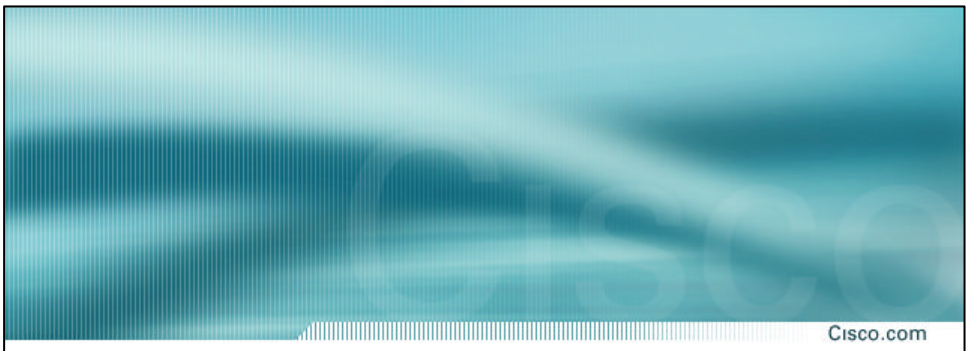
Cisco.com

- CPE is smarter and more complex
  - CPE can do Protocol Address Translation (PAT)/DHCP, to conserve IP address
  - IP address gets assigned to CPE
  - IP subnet feature, prevents NAT (Network Address Translation)
- PPPoA sessions can be terminated on NAP (Network Access Provider) or tunneled out using L2x
  - If terminated IP address provided by NAP
  - If tunneled, by the LNS (L2TP Network Server)
- IP address allocation same as PPPoE

Subscriber Connection Summary

Cisco.com

- Subscriber devices are
  - LAN attached
    - Bridge CPE: RFC1483 Ethernet over ATM
    - Router CPE: RFC1483 IP over ATM, PPPoA
  - PPP attached
    - Bridged CPE: PPPoE, L2TP
- Rapid, easy provisioning is key



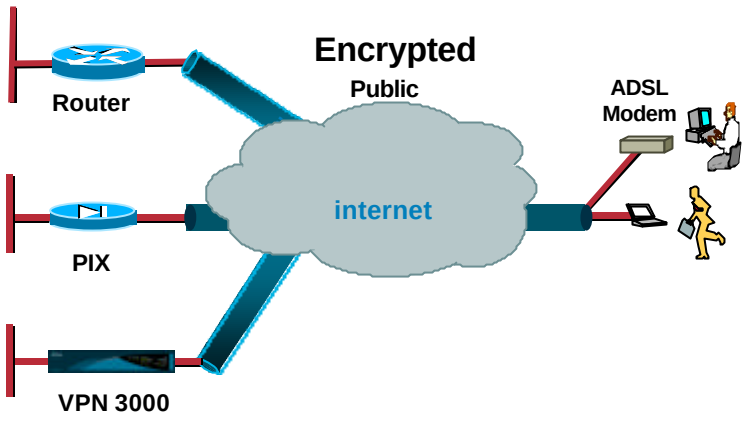
Remote Access VPN Solution

목차

- Remote Access VPN Solution
- 디자인 고려 사항
  - Redundancy
  - Load Balancing
  - Remote Access VPN + Firewall
  - VPN 장비의 위치 선정
- Cisco VPN 3000 Series Products

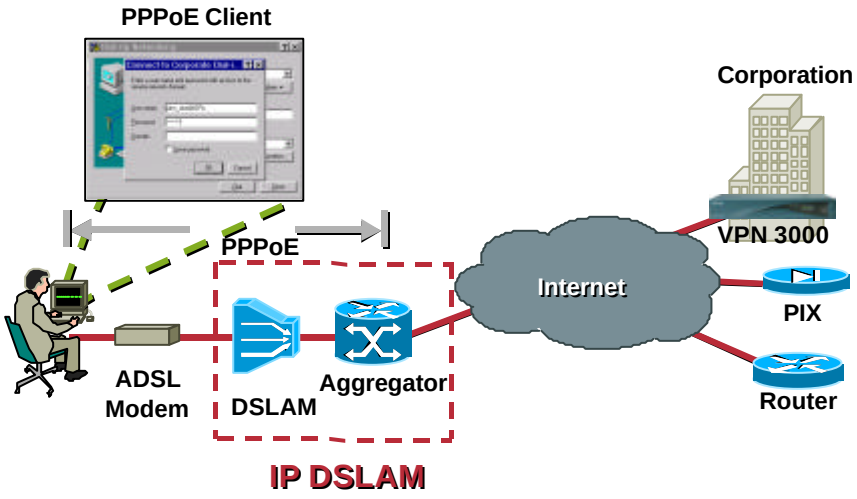
Remote Access 장비와 PC Client

Cisco.com



PPPoE(or PPPoA) 를 이용한 Remote Access VPN 접속

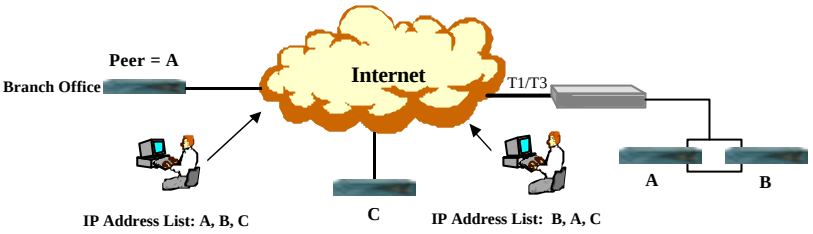
Cisco.com



Redundancy

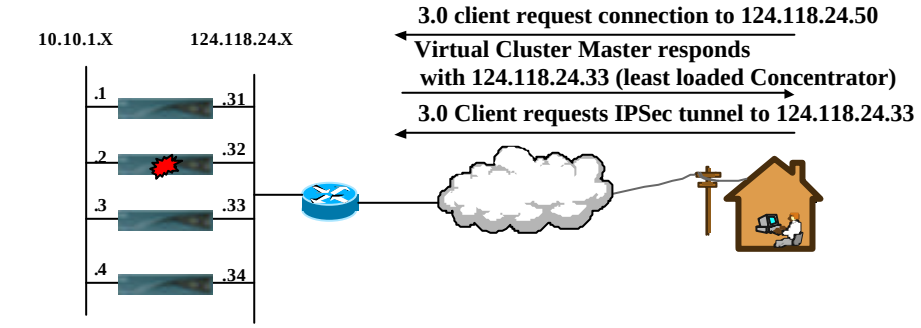
Cisco.com

- **Remote Access**
  - Multiple IP Addresses in the IPSec client
- **Redundant Platform**
  - Virtual Router Redundancy Protocol (VRRP)
    - Automatic Recovery
    - Same IP Addresses, MAC Addresses



Load Balancing – "Virtual Clustering"

Cisco.com

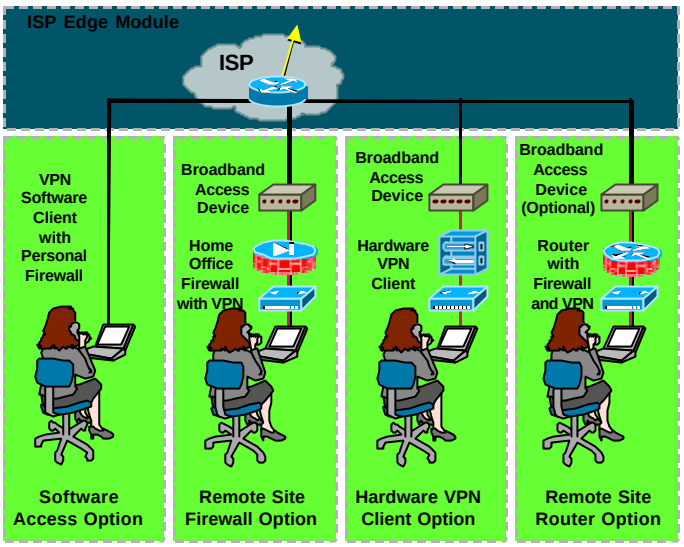


Virtual Cluster IP address = 124.118.24.50

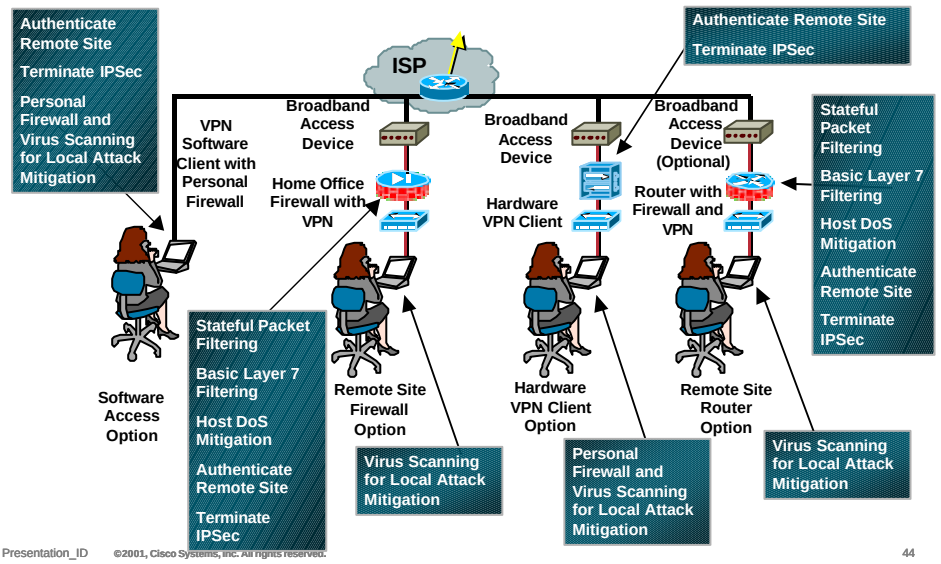
Virtual Cluster Master

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

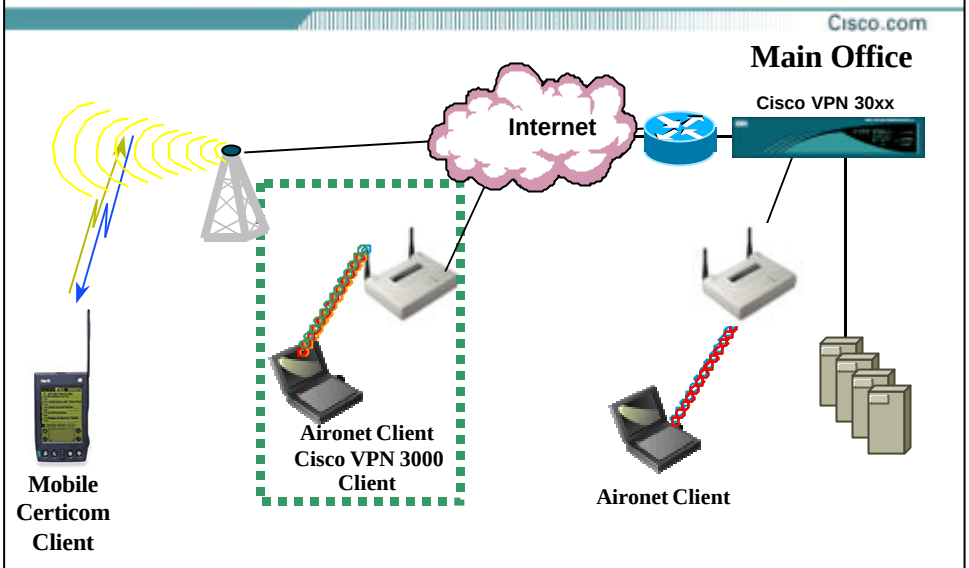
Remote Access VPN – SAFE Design



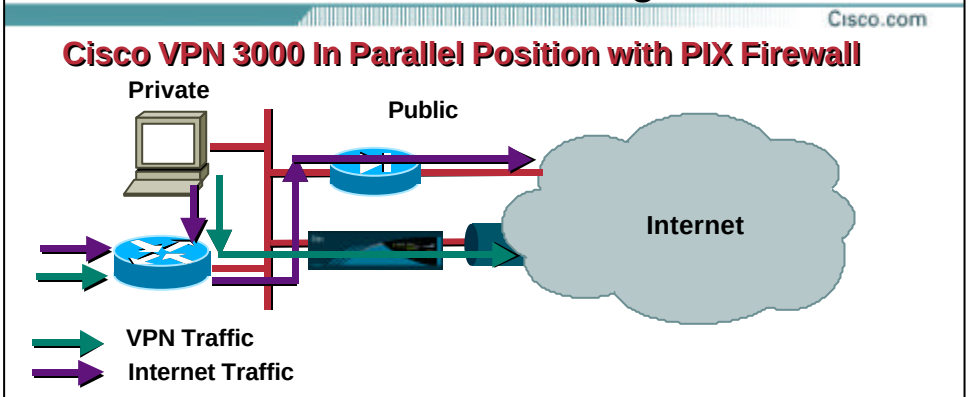
Remote-User Design Attack Mitigation Roles



Remote Access Wireless VPN



VPN 3000 위치에 따른 Routing Issues -1

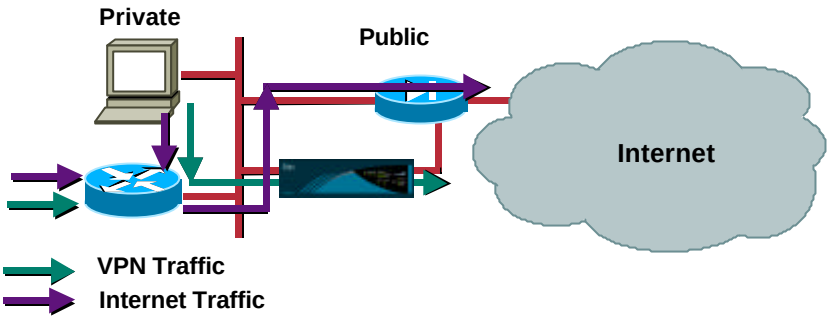


- PIX doesn' t redirect packets, use the router as host' s default gateway
- Router has a specific route for VPN traffic and the gateway of last resort is the PIX
- Router is Configured as tunnel default gateway on VPN 3000 Concentrator

VPN 3000 위치에 따른 Routing Issues - 2

Cisco.com

Cisco VPN 3000 behind PIX Firewall



VPN Traffic
Internet Traffic

- Better design. VPN 3000 concentrator protected by stateful firewall.
- Make sure that the PIX has holes for VPN traffic

Cisco.com

Remote Access VPN Products

Cisco VPN 3000 Series

Cisco.com

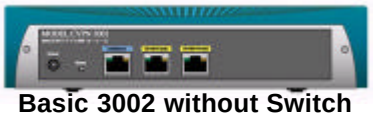
Network Computing EDITOR'S CHOICE

	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 VPN 3002 Hardware Client Physical Features

Cisco.com

Front



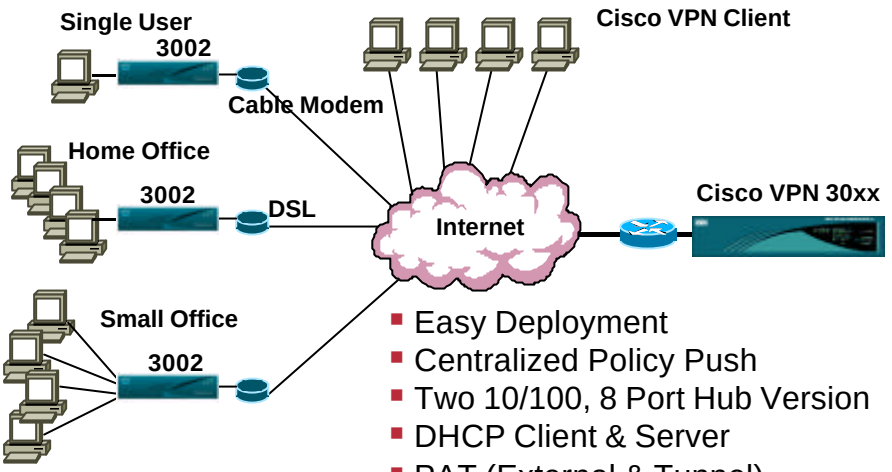
Basic 3002 without Switch

3002 unit with 8 Port 10/100 Switch

- 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

Cisco VPN 3002
Hardware VPN Client

Cisco.com



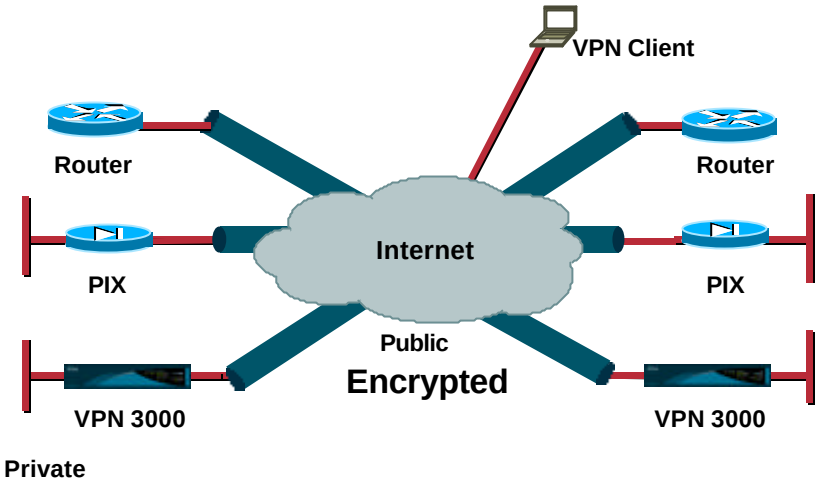
- Easy Deployment
- Centralized Policy Push
- Two 10/100, 8 Port Hub Version
- DHCP Client & Server
- PAT (External & Tunnel)
- Client & Network Extension modes

Cisco.com

Site-to-Site VPN Solution

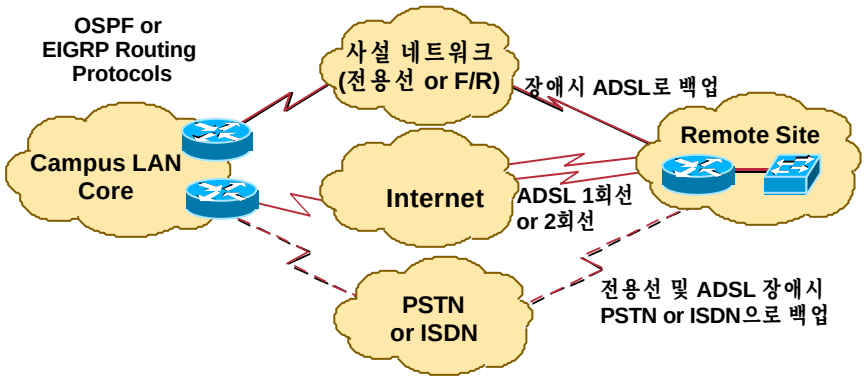
VPN 장비별 Layout

Cisco.com



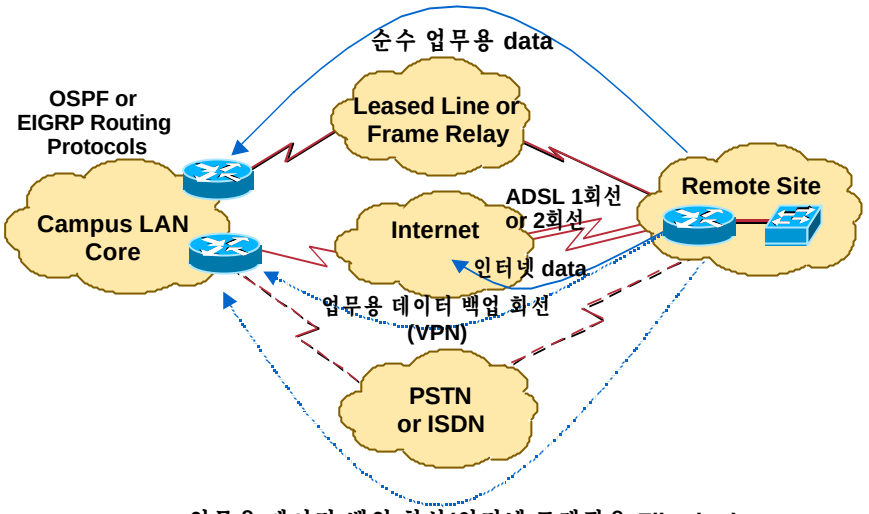
단순 Backup (GRE, IPSec)

Cisco.com



업무용 과 인터넷 Data 분산 및 Backup

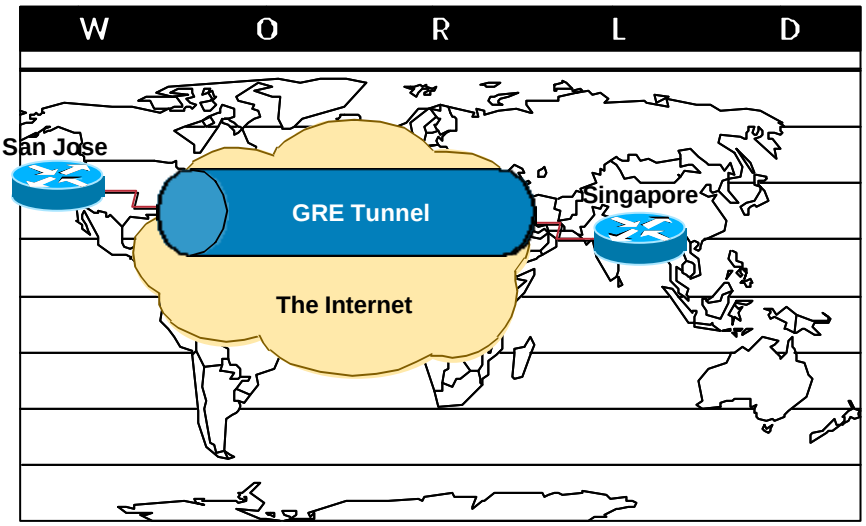
Cisco.com



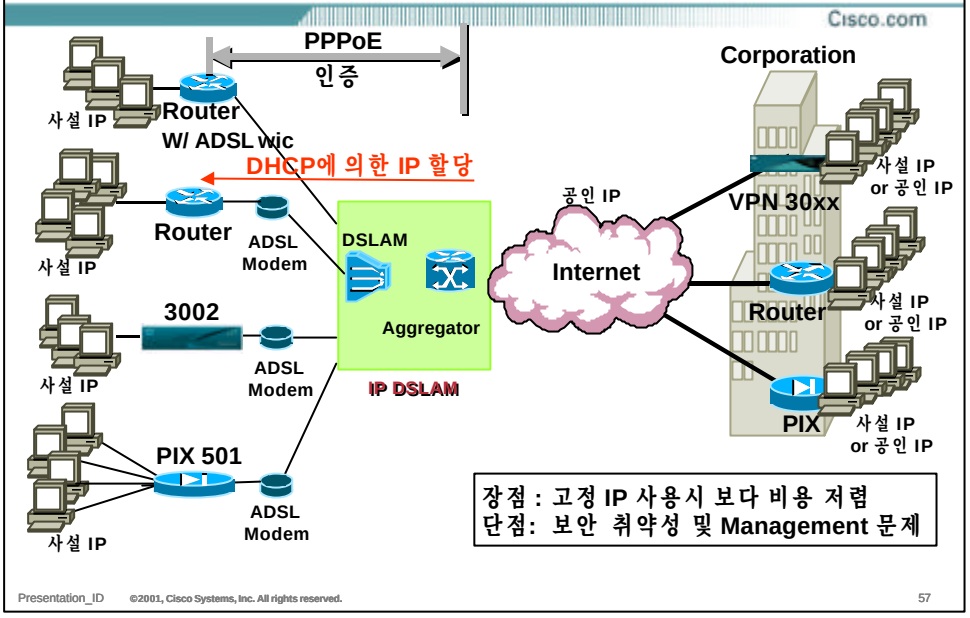
업무용 데이터 백업 회선(인터넷 트래픽은 Filtering)

Site-to-Site VPN Example

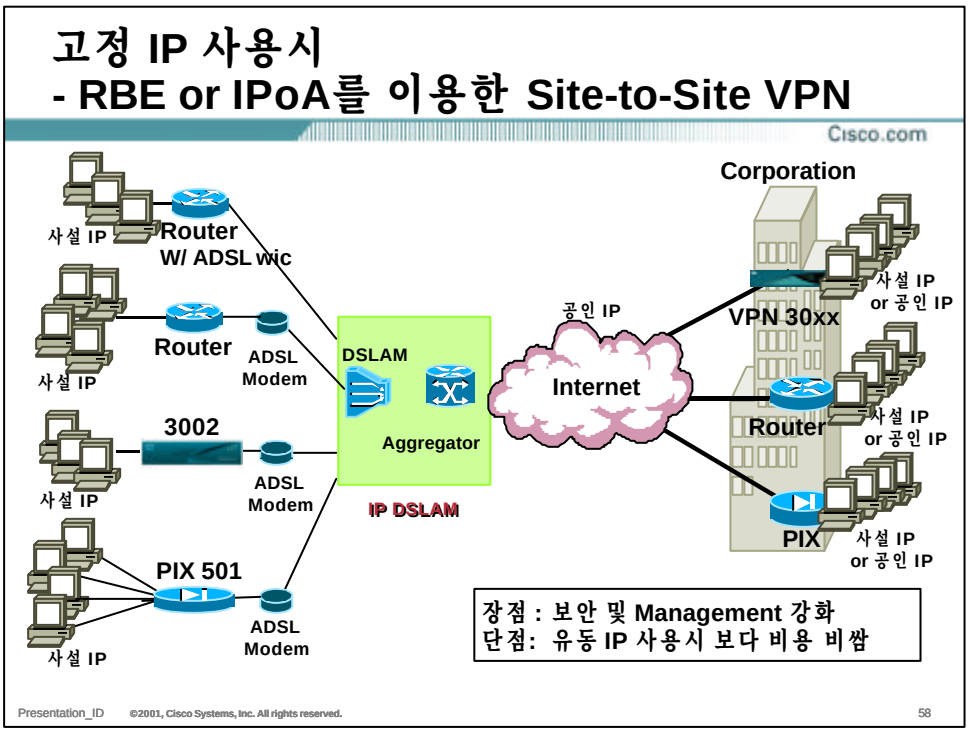
Cisco.com



DHCP에 의한 유동 IP 사용시
- PPPoE를 이용한 Site-to-Site VPN

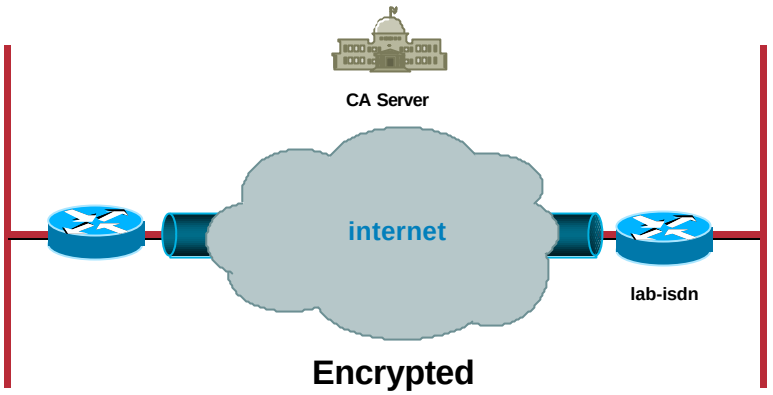


고정 IP 사용시
- RBE or IPoA를 이용한 Site-to-Site VPN



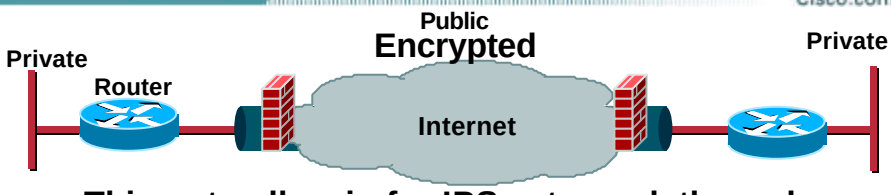
CA config

Cisco.com



Firewall in the Middle

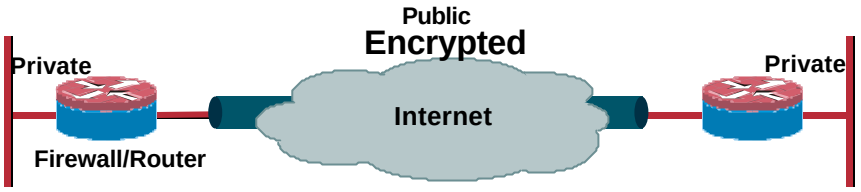
Cisco.com



- Things to allow in for IPSec to work through a firewall:
- Firewall in the middle of the tunnel:
  - ESP or/and AH
  - UDP port 500 (ISAKMP)
  - For IPSec through NAT in VPN 3000, open UDP ports configured on concentrator
  - For NAT transparency mode in VPN 5000, open TCP with source port 500 and destination port 80

Firewall on IPSec Endpoint

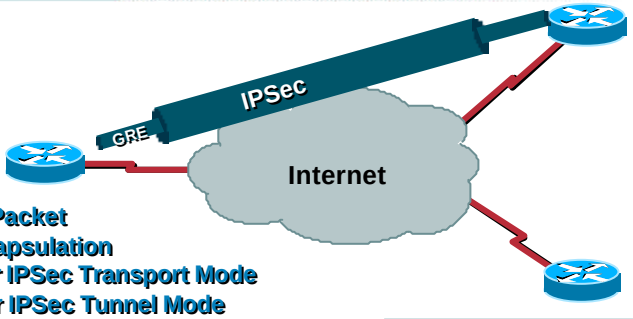
Cisco.com



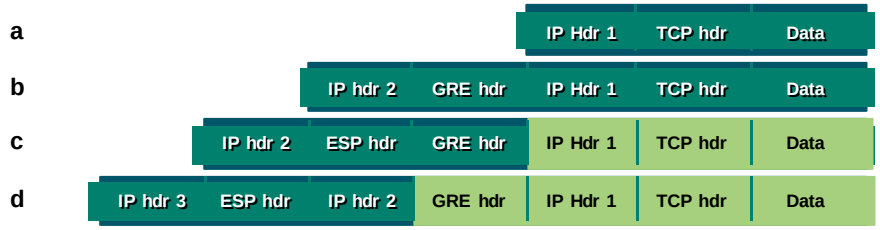
- **Firewall on the IPSec endpoint router:**
  - Esp or/and AH
  - UDP port 500
  - Decrypted packet IP addresses (incoming access group is applied twice)
- **Firewall on the IPSec endpoint PIX:**
  - Sysopt connection permit-IPSec
  - (Note: No conduits needed)

GRE over IPSec

Cisco.com



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



GRE Over IPSec - Configuration

Cisco.com

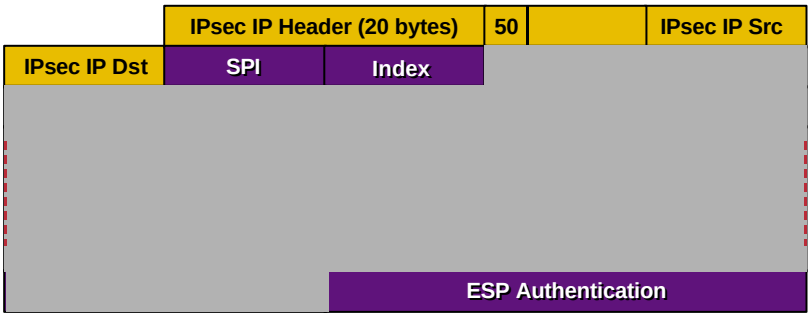
- Apply crypto map on both the tunnel interfaces and the physical interfaces
- Specify GRE traffic as IPSec interesting traffic.

  access-list 101 permit gre host 200.1.1.1 host 150.1.1.1
- Static or dynamic routing is needed to send VPN traffic to the GRE tunnel before it gets encrypted.

IPsec Tunnel Mode

Cisco.com

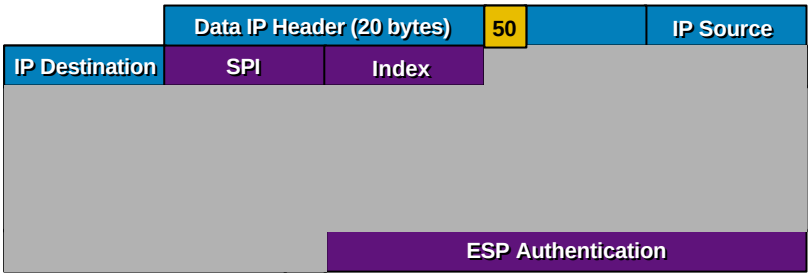
- Data IP traffic through IPsec peers
- Inner IP packet completely encrypted



IPsec Transport Mode

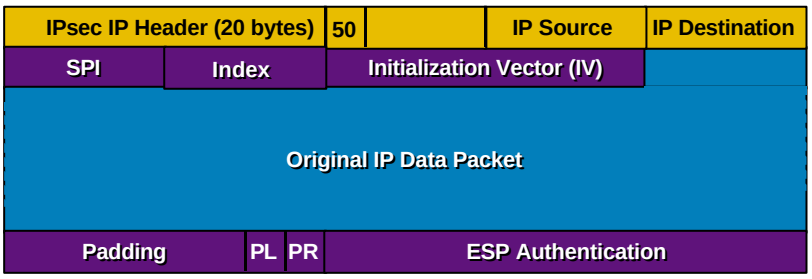
Cisco.com

- Data IP traffic between IPsec peers
- Reduced packet overhead
- Some of data IP header visible



MTU Issue - ESP IPsec Packet

Cisco.com

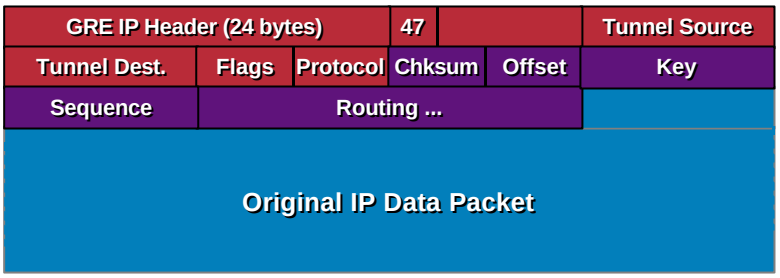


IPsec packet size = (Original IP Packet size +8+8+2) + 20+4+4+12
Max Original packet size = (IPsec packet size) - (20+4+4+12)-(8+2+1)

Examples:
IPsec packet size = (1445 + 18) + 40 = 1456 + 40 = 1496
IPsec packet size = (1446 + 18) + 40 = 1464 + 40 = 1504
Max Original packet size = (1500) - 40 – 11 = 1496 - 51 = 1445

GRE Tunnel Packet

Cisco.com



Flags = Checksum, Routing, Key, Sequence, Strict Source Route, Version
Protocol = Ethernet Protocol Type
Optional Fields
Checksum, Source Route Offset, Tunnel Key,
Packet Sequence Number, Source Routing Entries

IPsec + GRE Combined

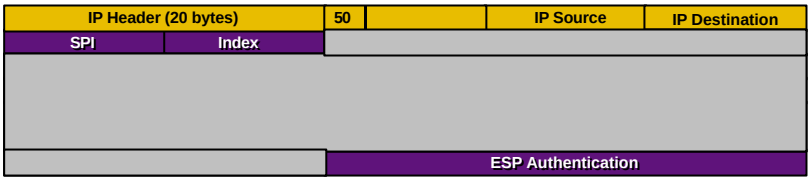
Cisco.com

- IPsec + GRE packets
  - Tunnel versus transport mode IPsec
- MTU Issues
  - Fragmentation
  - Path MTU discovery
- Switching mode
  - GRE Point-to-point – CEF switched

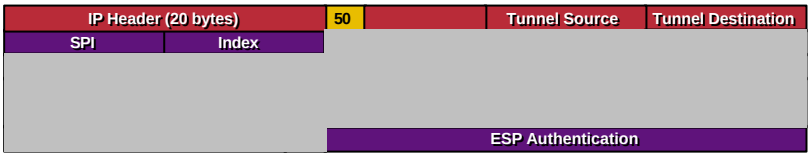
IPsec + GRE Packets

Cisco.com

IPsec Tunnel Mode + GRE



IPsec Transport Mode + GRE



IPsec + GRE Fragmentation

Cisco.com

- **Fragmentation**
  - GRE fragments **before** encapsulation
  - IPsec fragments **after** encryption
  - Can get **double** fragmentation
    - Reassembly by IPsec peer and end host
- **Set GRE interface IP MTU**
  - IPsec transport mode ‘ ip mtu 1440’
  - IPsec tunnel mode ‘ ip mtu 1420’

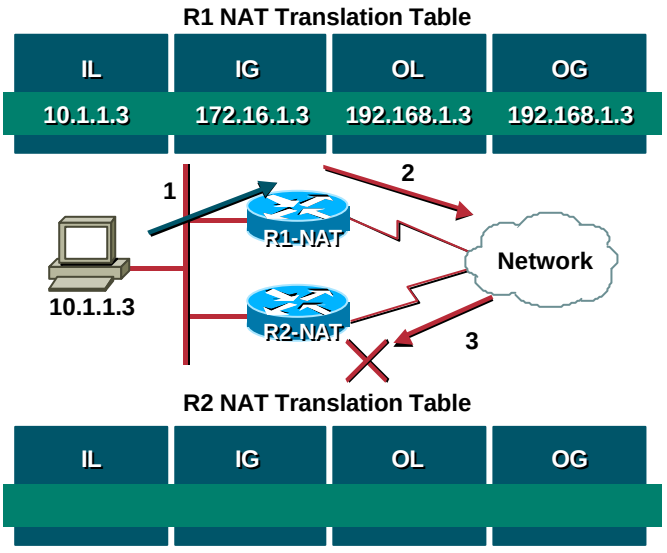
Stateful NAT - Future

Cisco.com

- Projected to be in the 12.2.4T code
- Platform independent
- Supports many peers
- Works in a HSRP environment for true fault tolerance

Without SNAT —the Problem

Cisco.com

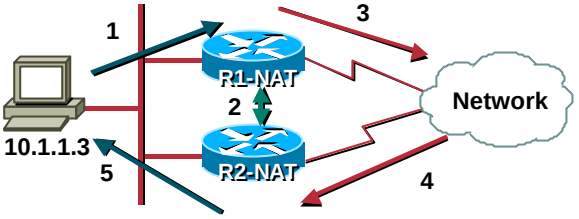


With SNAT —The Solution

Cisco.com

R1 NAT Translation Table

	IL	IG	OL	OG
1*	10.1.1.3	172.16.1.3	192.168.1.3	192.168.1.3



R2 NAT Translation Table

	IL	IG	OL	OG
2*	10.1.1.3	172.16.1.3	192.168.1.3	192.168.1.3

Cisco.com

VPN 네트워크 디자인

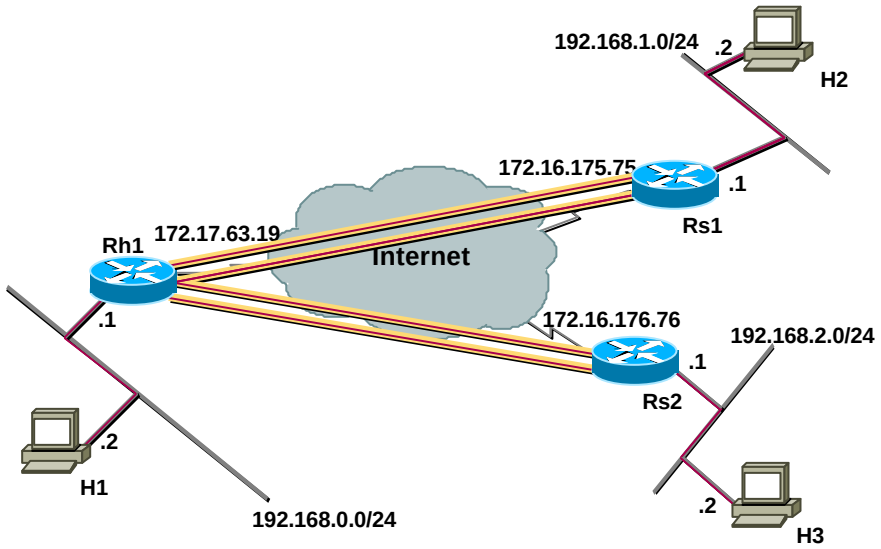
VPN Network Design

Cisco.com

- **Point-to-point**
  - Natural for encryption
- **IPSec Hub and spoke**
  - Small to medium static VPN
  - Traffic: hub spoke, spoke spoke
- **IPSec + GRE Hub and spoke**
- **Full-mesh**
  - Small Network

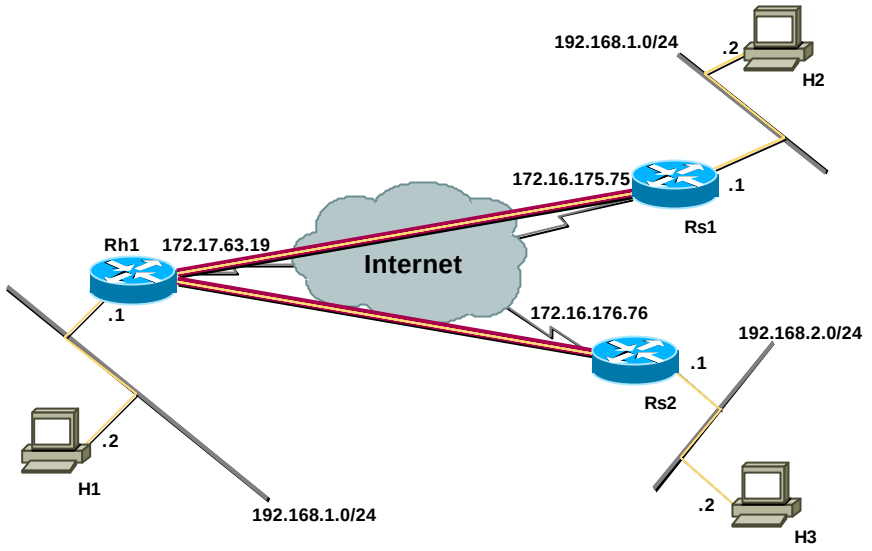
IPsec Hub and Spoke

Cisco.com



IPsec + GRE Hub and Spoke Network

Cisco.com



IPsec + GRE Hub and Spoke

Cisco.com

- **Dynamic routing—GRE tunnel**
  - **Redundant hub design**
- **Network changes/additions**
  - **No change in ACLs**
  - **Add configuration on hub and new spoke**
- **Controls split-tunneling on spokes**
- **GRE tunnel destinations**
  - **Statically configured on hub and spokes**
- **IPsec peers**
  - **Statically configured on spokes**
  - **Dynamic on hub - Reduces hub configuration lines**

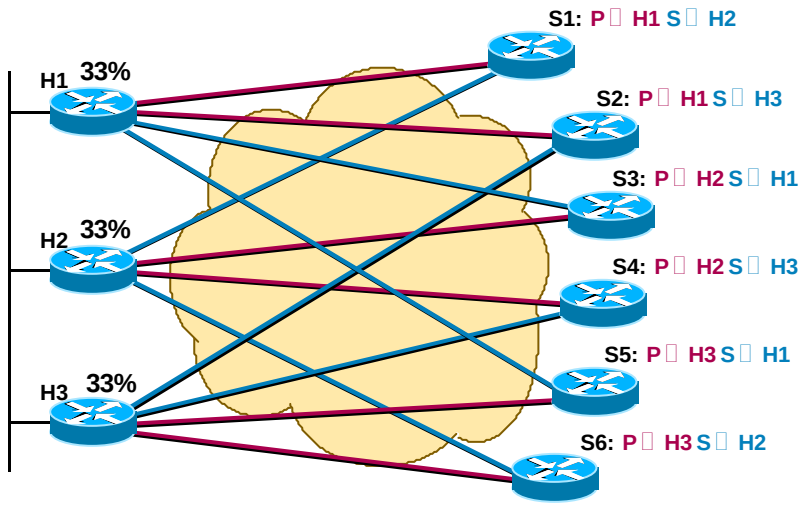
Redundant Hubs

Cisco.com

- Network: multi-hub and spoke
  - Traffic: hub spoke, spoke spoke
- Redundancy and fail over
  - Two tunnels from each spoke
  - Dynamic routing selects tunnel to use
- Load reduction on hubs
  - Distribute tunnels evenly across hubs

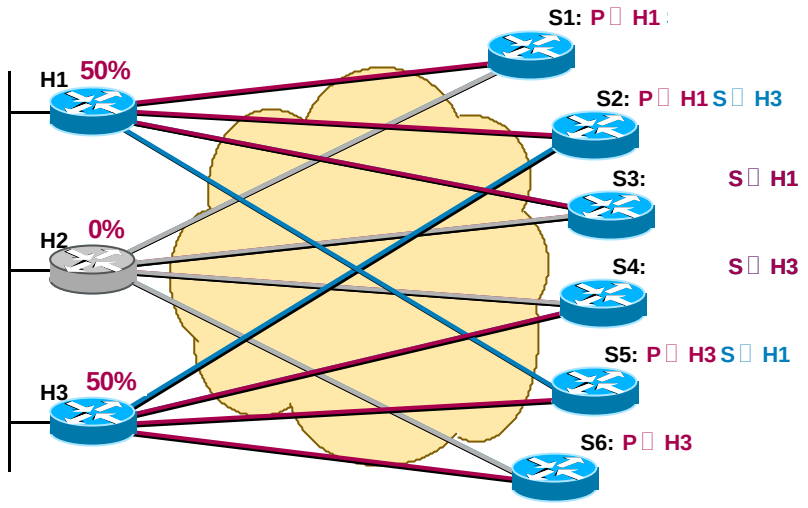
Redundant Hubs in Action Initial Build

Cisco.com



Redundant Hubs in Action After Failure

Cisco.com



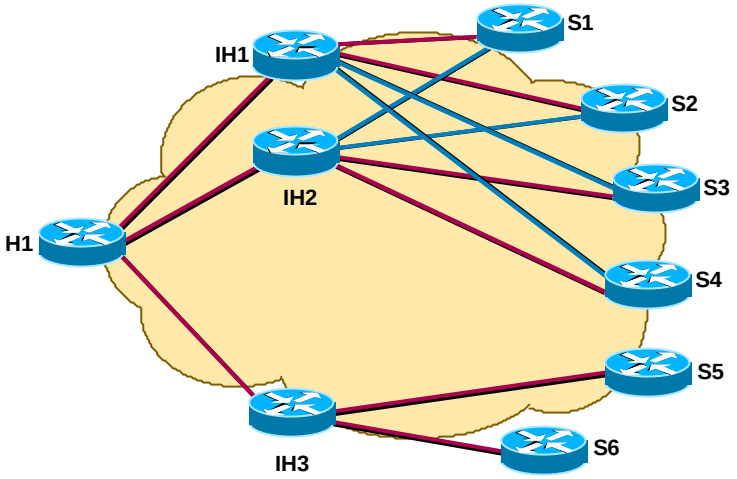
Tiered Hub Design

Cisco.com

- Repeat single or redundant hub design in layers
- Each layer of spoke routers are hub routers for next layer
  - Each tier requires another encrypt/decrypt of data traffic
- Scaling, redundancy and failover similar to redundant hub design

Tiered Design: Example

Cisco.com



Cisco.com

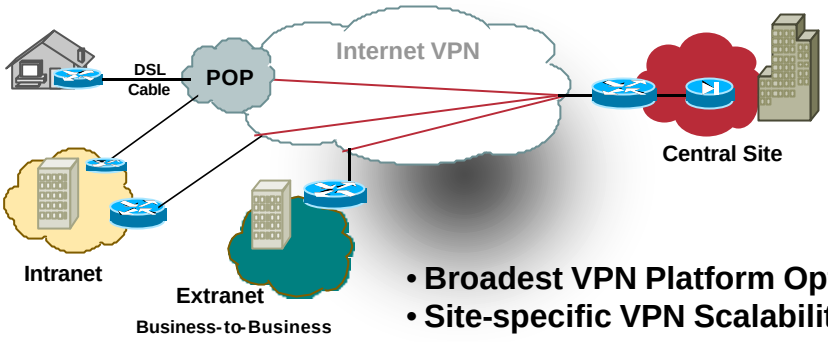
Site-to-Site VPN Products

Site-to-Site VPNs

Cisco.com

Access CPE - Remote Site
Cisco VPN-Optimized Routers
Cisco Broadband Routers

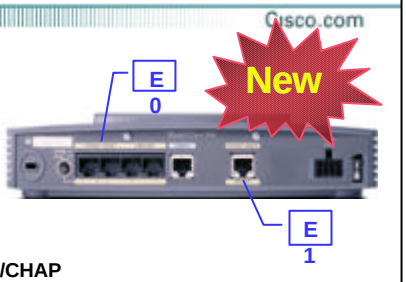
Enterprise - Central Site
Cisco VPN Routers: Routing + VPN
Cisco Secure PIX Firewall: Firewalling



- Broadest VPN Platform Options
- Site-specific VPN Scalability
- Rich VPN Services in Cisco IOS Software

Cisco 806
Broadband Gateway Router

Cisco.com



- **Multi-User Access**
  - -4-Port Hub
  - -PPPoE client/server, DHCP client/server, unlimited users (20 recommended)
  - -Network Address Translation
- **Business-Class Security**
  - -Basic Security – NAT, Extended Access Lists, PAP/CHAP
  - -Enhanced Security – Stateful Inspection Firewall, Denial of Service detection and prevention, VPNs with IPSec DES/3DES
- **Manageability, Reliability, Scalability with Cisco IOS Software**
  - -Remote Monitoring, Troubleshooting, and s/w management
  - -Easy Set Up with web configuration tool
- **QoS and Traffic Management for Voice and Video Applications**
  - -Manage Multicast/video traffic
  - -Quality of Service for IP Phones* and other IP-based applications

VPN-Enabled Routers

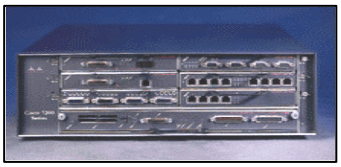
Cisco.com

	1700	2600	3620/40	3660	7200
Simultaneous Tunnels	100	300	800	2000	2000
Performance (Mbps)	2-3	6-8	12-15	24-30	60-90
Hardware Encryption	VPN Module	AIM	NM	AIM	ISA
WAN Interfaces	yes	yes	yes	yes	yes
LAN Interfaces	none	optional	optional	optional	optional

New 7200 VPN Bundles

Cisco.com

- **New 7200 VPN bundles:**
  - chassis / processor
  - I/O board
  - packet memory
  - flash memory
  - power supply
  - VAM VPN accelerator card
  - IOS IPSec 3DES software
  - DES bundles also available

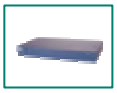


- **7204VXR400/VPNK9**
  - Base VPN Bundle for adding WAN
  - Cisco 7204 Router, NPE-400, I/O Board w/ Dual 10/100, AC, SA-VAM, IPSec 3DES
- **7204VXR400/T3VPNK9**
  - For High Bandwidth VPN Head-end
  - Cisco 7204 Router, NPE-400, I/O Board w/ Dual 10/100, PA-T3+, SA-VAM, AC, IPSec 3DES

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)

PIX 501 Deployments

Telecommuter / Day Extender

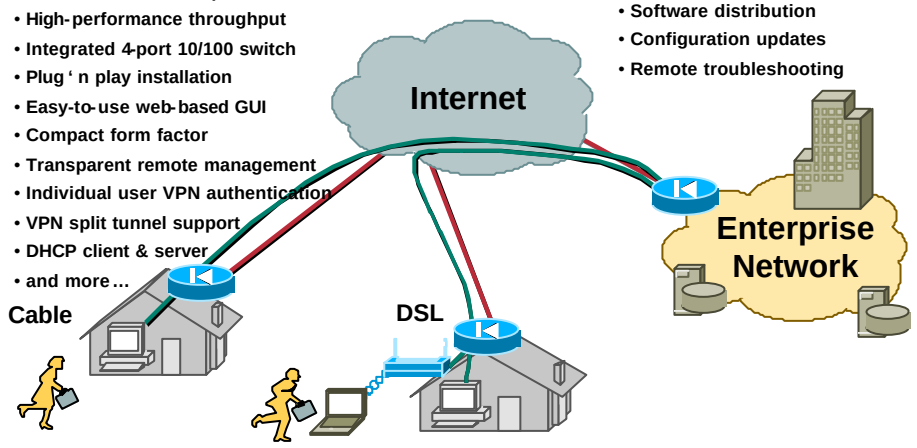
Cisco.com

PIX 501 Benefits

- Enterprise-class firewall security
- Integrated 3DES VPN
- Embedded intrusion protection
- High-performance throughput
- Integrated 4-port 10/100 switch
- Plug ' n play installation
- Easy-to-use web-based GUI
- Compact form factor
- Transparent remote management
- Individual user VPN authentication
- VPN split tunnel support
- DHCP client & server
- and more…

Administrative Benefits

- Scaleable "low touch" management
  - Provisioning
  - Software distribution
  - Configuration updates
  - Remote troubleshooting



PIX 501 Deployments
Remote Office/Small Business

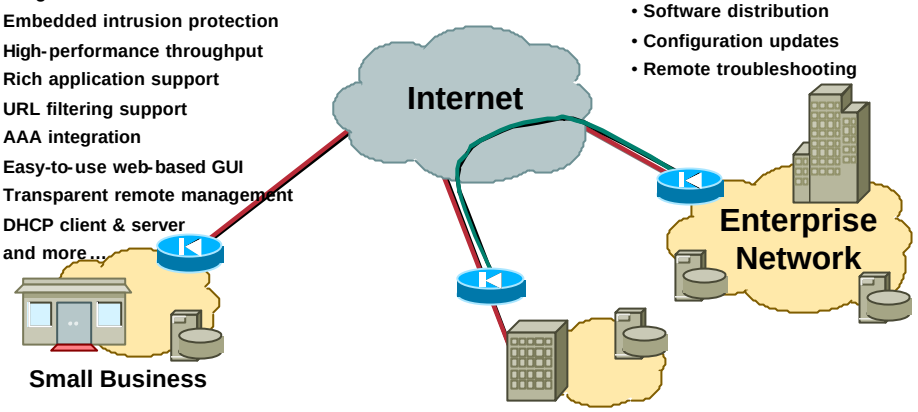
Cisco.com

PIX 501 Benefits

- Enterprise-class firewall security
- Supports up to 50 Users
- Integrated 3DES VPN
- Embedded intrusion protection
- High-performance throughput
- Rich application support
- URL filtering support
- AAA integration
- Easy-to-use web-based GUI
- Transparent remote management
- DHCP client & server
- and more…

Administrative Benefits

- Scaleable "low touch" management
  - Provisioning
  - Software distribution
  - Configuration updates
  - Remote troubleshooting



Cisco Dual Ethernet Security Platform Comparison

Cisco.com

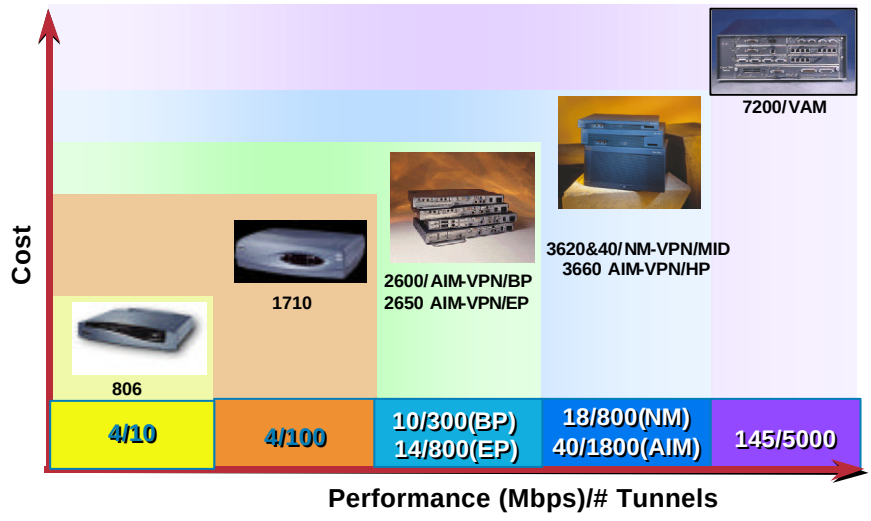
Product	PIX 501	PIX 506	VPN 3002	806
Physical Size (WxDxH")	6¼x5¼x1"	8¼x11.8x1.7"	8x6x2"	9¾x8½x2"
Inside Interface	4-FE Switch	10BaseT, Auto	1-FE or 8-FE Switch	4-10BaseT Hub
Outside Interface	10BaseT, Half	10BaseT, Auto	FE	10BaseT, Half
Clear-text (Mbps)	10	20	10	9
3DES (Mbps)	3	10	2.2	400 Kbps
Users	10 or 50	Unlimited	Unlimited	Unlimited, 20 sugg.
Concurrent VPN Tunnels	5 VPN Peers	25 VPN Peers	1	10
Stateful Firewall	Yes, PIX	Yes, PIX	No	Yes, IOS FW
Content Filtering	Yes, Java/ActiveX	Yes, Java/ActiveX	No	Yes, CBAC
URL Filtering	Yes, 3rd Party	Yes, 3rd Party	No	No
Intrusion Protection	Yes	Yes	No	No
AAA Support	Yes	Yes	Yes	Yes
NAT/PAT	Yes	Yes	Yes	Yes
Site-to-Site VPN	Yes	Yes	Network Ext Mode	Yes
VPN User Termination	Yes	Yes	No	Yes
VPN NAT Transparency	No	No	Yes	No
Individual User Auth	Yes, Cut-through Proxy	Yes, Cut-through Proxy	No (Q4)	Yes, Lock&Key
DHCP Client & Server	Yes (32 or 128 leases)	Yes (256 Leases)	Yes (253 Leases)	Yes (253 Leases)
PPPoE Support	Yes (V 6.2)	Yes (V 6.2)	Yes	Yes
SNMP & Syslog Support	Yes	Yes	Yes	Yes

Cisco.com

Cisco VPN Products Positioning

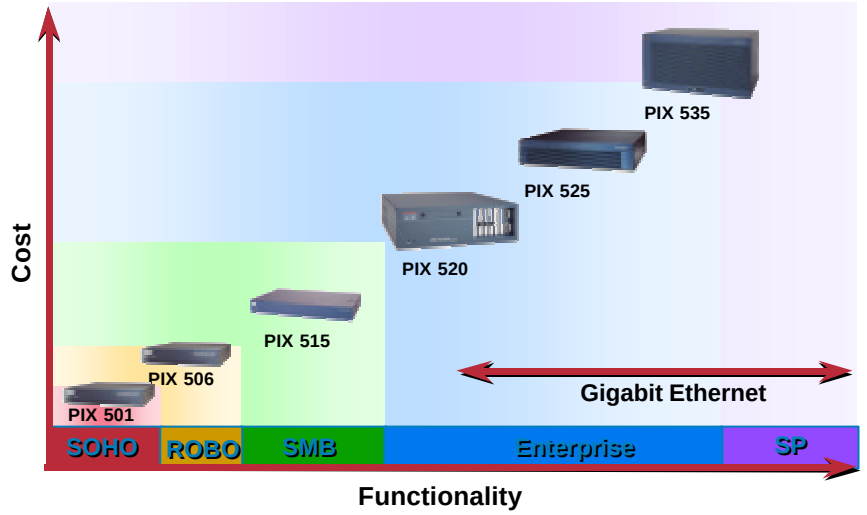
Cisco Secure VPN IOS Family

Cisco.com



PIX Firewall Family

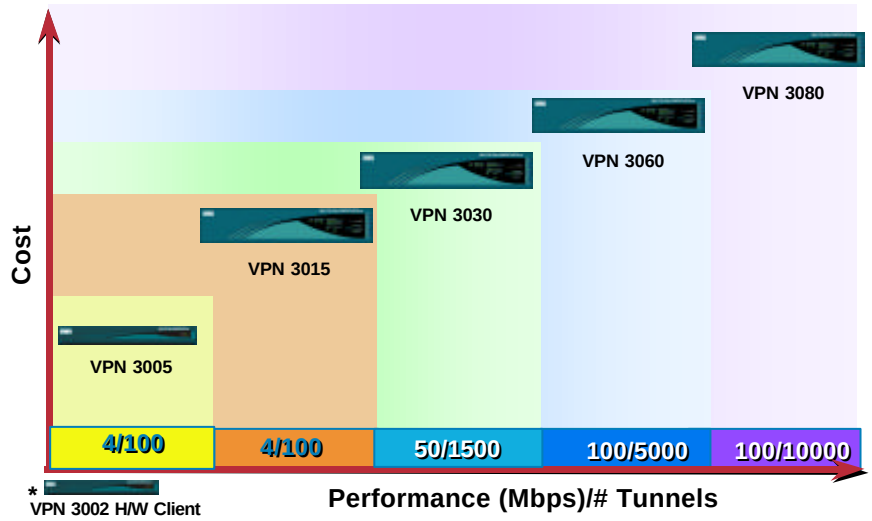
Cisco.com



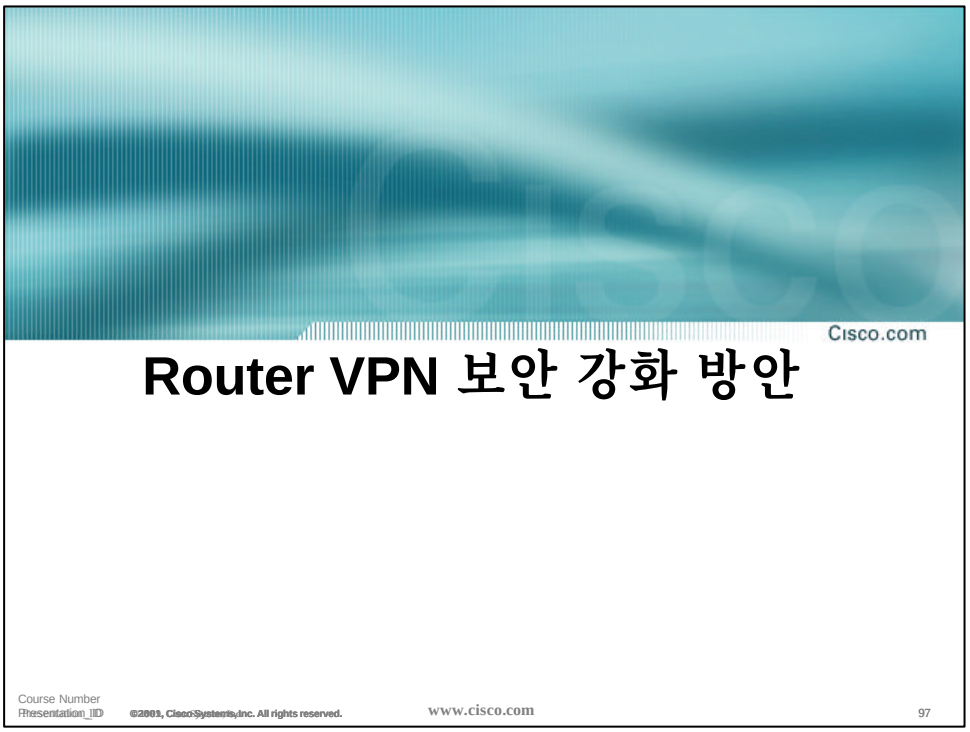
Presentation_ID ©2001, Cisco Systems, Inc. All rights reserved. 95

Cisco Secure VPN 3K Family

Cisco.com



Presentation_ID ©2001, Cisco Systems, Inc. All rights reserved. 96



Benefits of Cisco IOS VPN

Cisco.com

- Routing across VPN - Using GRE
- Multi-protocol support across VPN - Using GRE
- Multicast across VPN - Using GRE
- QoS support for bandwidth optimization and voice quality
- Integrated voice features

  Though not all interoperate with voice today, they will soon
- Integrated WAN interfaces
- CiscoWorks 2000
- IOS CLI

Router Integrated Security Feature

Cisco.com

- Context Based Access Control
- Authentication proxy
  - AAA Server – TACACS+, RADIUS
  - OTP (One Time Password)
- Intrusion Detection

Access-Lists (ACLs)

Cisco.com

- Provide traffic filtering
- Implied “deny all’ at end
- Not configured is permit all
- Advanced access-lists:
  - reflexive access-lists
  - time-based access-lists

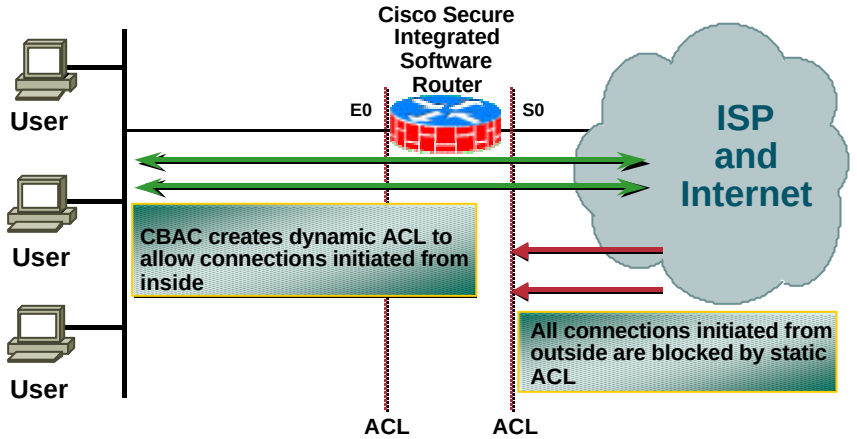
Context-Based Access Control (CBAC)

Cisco.com

- Packet inspection system based on connection states and payload
- Uses dynamic access-lists
- Works with IPSec and NAT
- Intercepts the packet after ACL check and routing setup
- For traffic passing through the router, not destined for it

How CBAC Works

Cisco.com



IOS Authentication Proxy

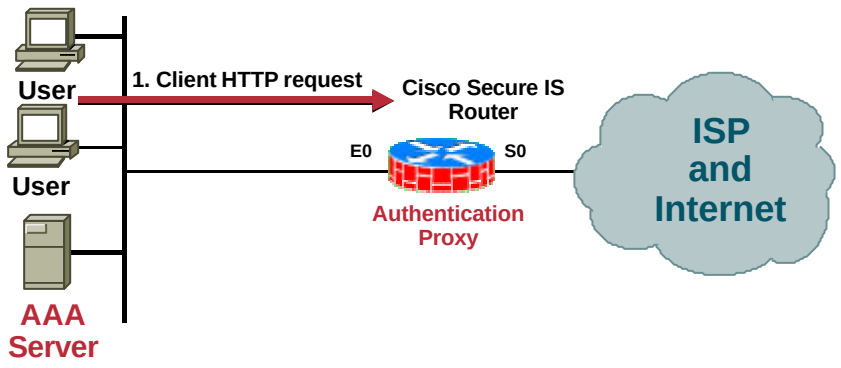
Cisco.com

- HTTP initiated
- Supports TACACS+ and Ascend and Livingston RADIUS
  - CiscoSecure supported
- Works with IPSec
- With CBAC, supports NAT
- Supports One Time Passwords (OTP) and strong authentication products that work with TACACS+ and RADIUS

How Proxy Works

Cisco.com

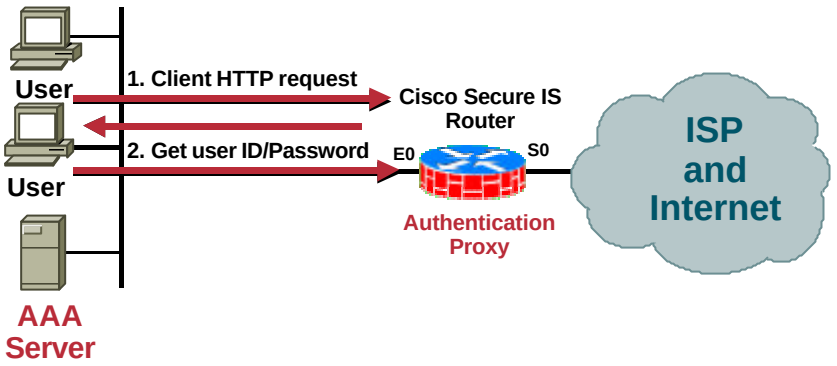
- Proxy intercepts client HTTP request: before input ACL; saves target URL



How Proxy Works

Cisco.com

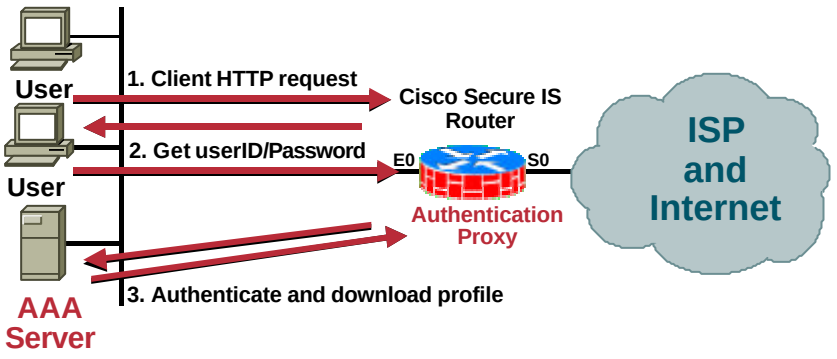
- Proxy replies to the client via HTML: gets user ID and password



How Proxy Works

Cisco.com

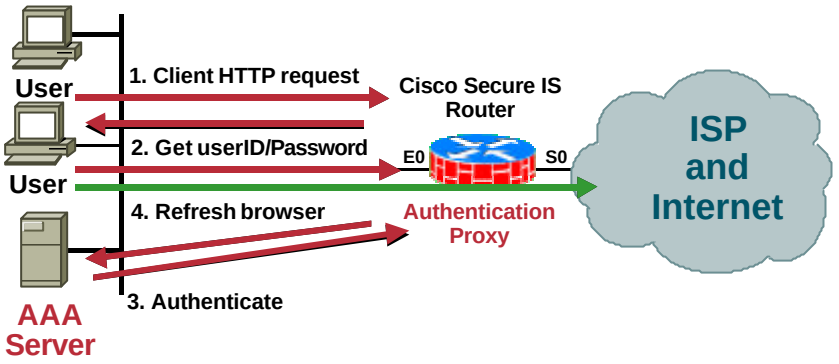
- Proxy authenticates with AAA server: downloads authorization profile; creates dynamic ACLs



How Proxy Works

Cisco.com

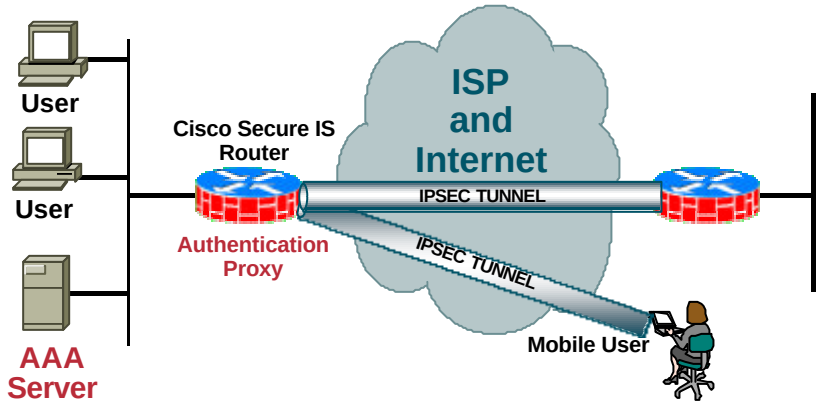
- **Proxy refreshes client's browser:**
  refreshes client's browser with saved target URL



Authentication Proxy with IPSec VPN

Cisco.com

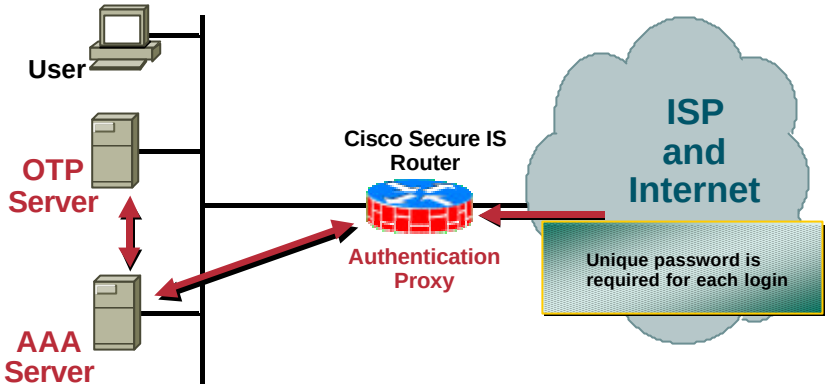
- **Firewall security at IPSec gateway**



Proxy with One-Time Password (OTP)

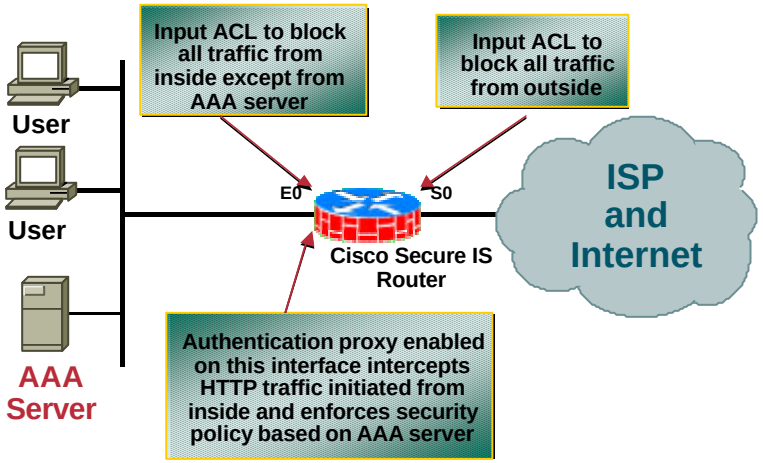
Cisco.com

- **Protection from password sniffing**



Outbound Authentication

Cisco.com



Cisco IOS IDS

Cisco.com

- On going monitoring of network traffic for security
- Matches network traffic against lists of signatures, which detects patterns of misuse
- Takes action upon detection

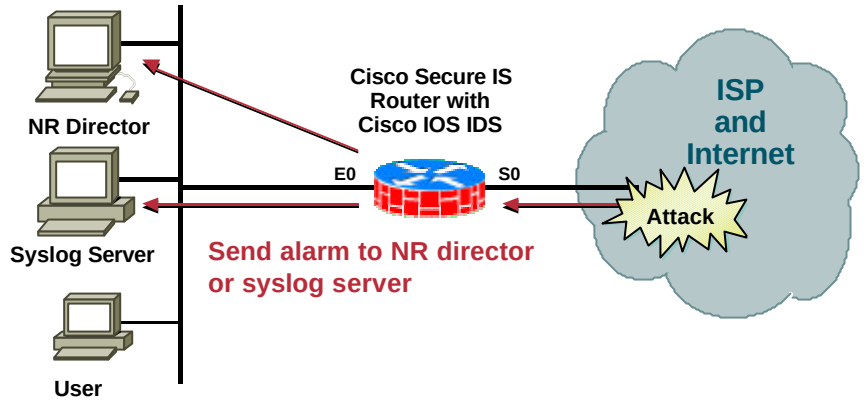
Cisco IOS IDS Actions

Cisco.com

- **Alarm**: sends alarm to NetRanger director, console or syslog server and forwards the packet
- **Drop**: drops the packet
- **Reset**: if TCP, sends packets with reset flag to both participants of the session and forwards the packet

Cisco Secure Integrated Software with Intrusion Detection

Cisco.com



Cisco.com

평가 인증

평가 기준 등급 비교

Cisco.com

•출처 : 한국 정보 보호 진흥원

미국			한국	국제		비고
TCSEC	FC		침입차단 시스템 평가 기준	Common Criteria		
	PP	보증				
D			K0	EAL0	부적절한 보증	
			K1(E)	EAL1	기능 시험	
C1			K2(E)	EAL2	구조 시험	
C2	CS-1	T1	K3(E)	EAL3	방법론적 시험과 점검	
B1	LP-1 CS-2 CS-3	T2 T2 T3	K4(E)	EAL4	방법론적 설계,시험 및 검토	PIX Firewall, IPSec VPN
B2	LP-2	T5	K5(E)	EAL5	준정형적 설계 및 시험	
B3	LP-3	T6	K6(E)	EAL6	준정형적 검증된 설계 및 시험	
A1	LP-4	T7	K7(E)	EAL7	정형적 검증	

• K4(E)인증 제품 및 현황은 http://www.kisa.or.kr/sysevaluation/menu2/sub3/index.html 참조

CISCO SYSTEMS

EMPOWERING THE INTERNET GENERATION℠