Internet/VPN Case Study

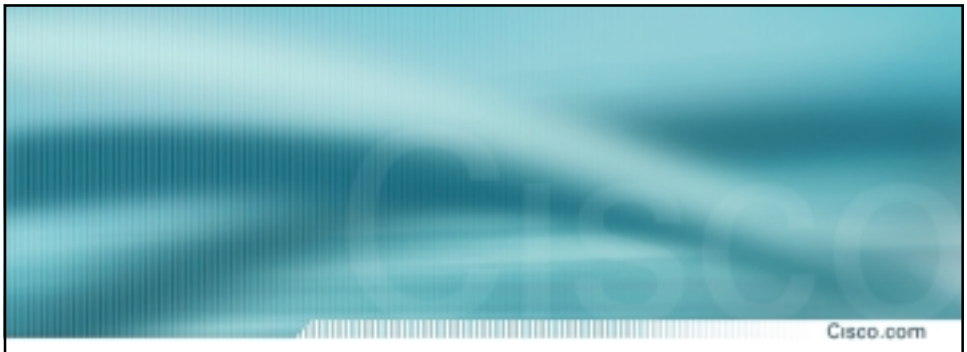
Cisco.com

박 승남
System Engineer, CCIE
Cisco Systems Korea

목 차

Cisco.com

- 기존 망 분석
- **Branch Internet/VPN** 방안
  - 적용기술 분석
  - **Router** 통합 **Solution**
  - 전용장비 **Solution**
  - 통신 사업자 **Solution**
- 적용사례분석

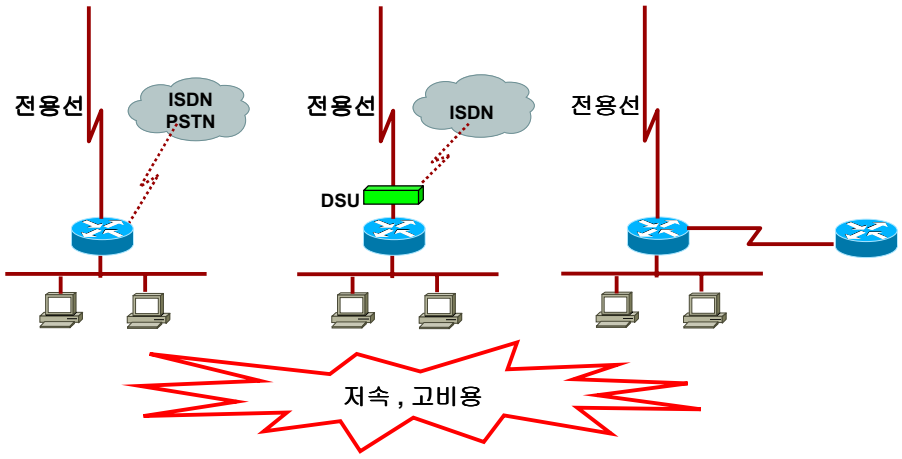


기존 망 분석

기존 백업망 분석

Cisco.com

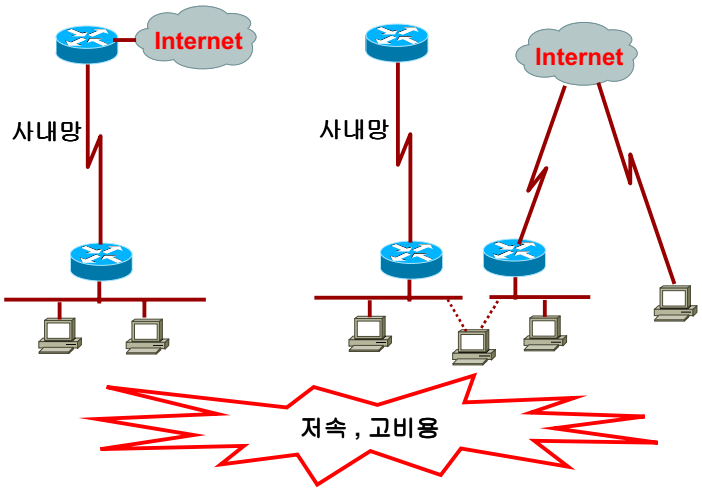
ISDN 또는 전화망 이용 | DSU에서 백업 | 인근 지점으로 백업



기존 Internet 접속방안 분석

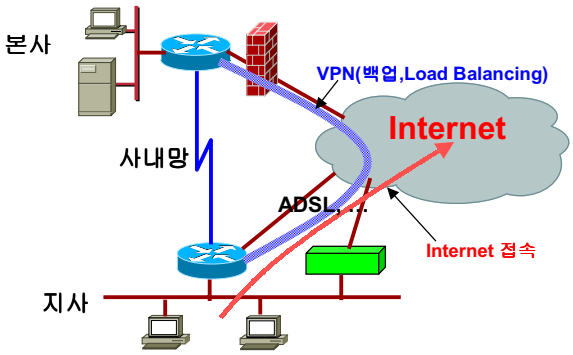
Cisco.com

사내망 이용 | 별도의 Internet망



백업과 Internet 접속을 위한 새 Solution ?

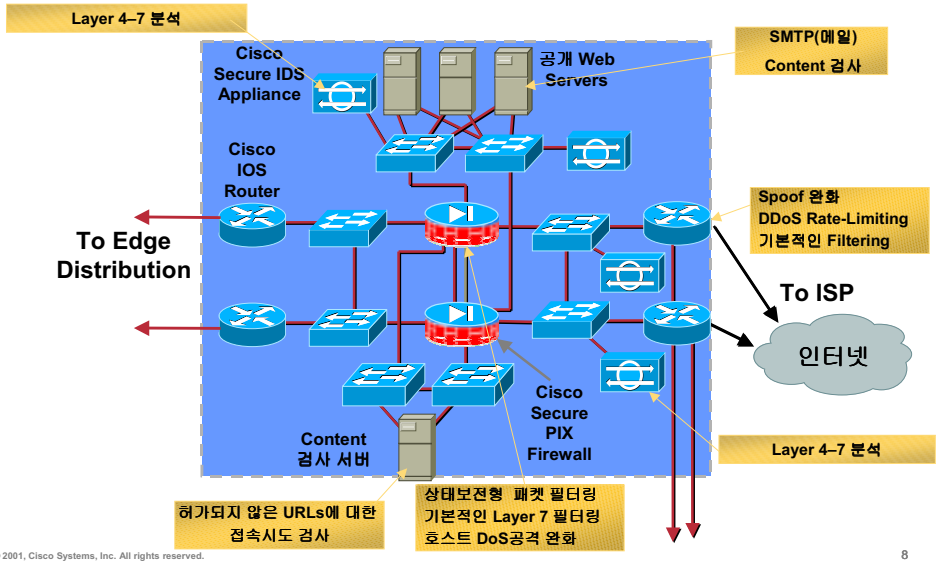
Cisco.com



높은 대역폭, 경제성 ⟺ 관리, 보안의 어려움

보안을 고려한 인터넷접속 구성 예

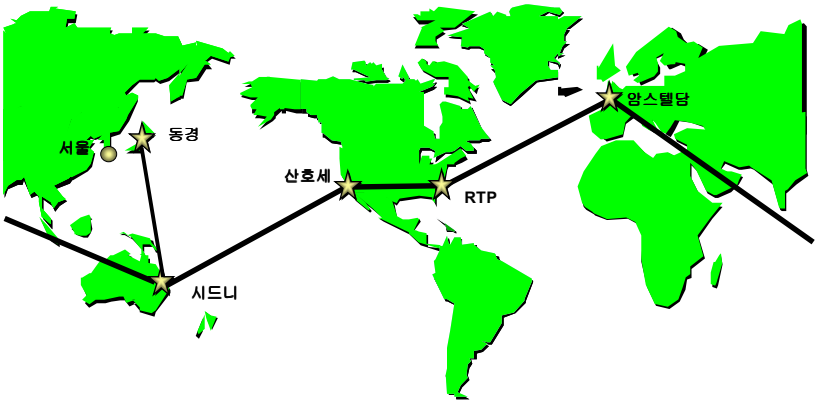
Cisco.com



다국적 기업의 Internet망

Cisco.com

- 거대 다국적 기업의 대규모 망에서도 Internet 접속은 최소로 구성 하여 관리와 보안유지
  - Cisco(미국 산호세/RTP, 유럽 암스텔담, 호주 시드니, 일본 동경),
  - IBM, HP, … 수개 이내의 Internet 접속point 보유



Cisco.com

Branch Internet/VPN 구성방안

- 적용기술 분석

Internet 접속 방법

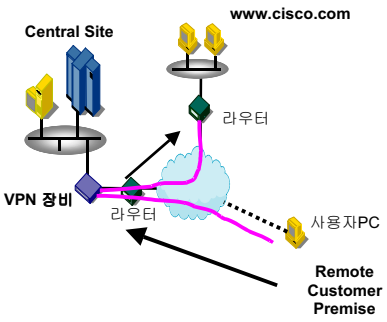
Cisco.com

항목	적용유형
적용보안 기술	Access-list only Access-list + VPN(VPN only) Fire-wall + VPN(split tunnel 지원) Fire wall + VPN + IDS
장비 통합 측면	단일장비 : Router에 ADSL카드 장착, S/W로 보안적용 복합장비 : Router, VPN, F/W,IDS, ADSL을 별도 장비로 구성
회선구성방식	전용선+ADSL, ADSL 1회선, ADSL2회선, ADSL+Dialup(PSTN/ISDN)
IP 주소	고정 IP : IPoA, RBE(Routed Bridged Encapsulation)방식. 보안, Management 유리 유동 IP : 비용절감, 보안 Management 취약
Tunneling	IPSec : 다양한 IP service 지원 불가능 GRE over IPSec : IP Multicasting 지원(Dynamic routing, Multi-media, 방송…)

Split Tunneling기능

Cisco.com

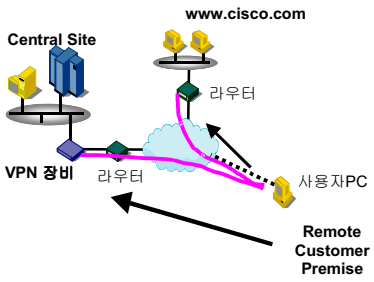
Split Tunneling을 사용하지 않는 경우



- 원격사용자 PC와 외부간 모든 트래픽이 터널을 경유
- 사용자의 모든 접속 Destination은 중앙에서 통제

=> 높은 수준의 보안성 제공

Split Tunneling을 사용하는 경우



- 원격사용자 PC는 2개의 Path를 가짐
- Secure Path(Tunnel) : 사용자 PC ~ 회사 네트웍
- Clear text path : 사용자 PC ~ 인터넷 사이트

⇒ 편리성, 잠재적인 보안취약성

Firewall이란?

Cisco.com

- 네트웍상의 특정지점에서 보안정책을 수행하는 하드웨어와 소프트웨어의 집합
- 외곽보안(Perimeter Security)을 담당하는 장비
- 내부에서 외부, 외부에서 내부로 가는 양방향의 네트웍 트래픽을 검사하여, 사전에 정의된 보안정책을 준수하는 인증된 트래픽만을 통과시킴

종류 : Access-list에 의한 Packet filter , Proxy Server, Stateful Packet Filter

Cisco.com

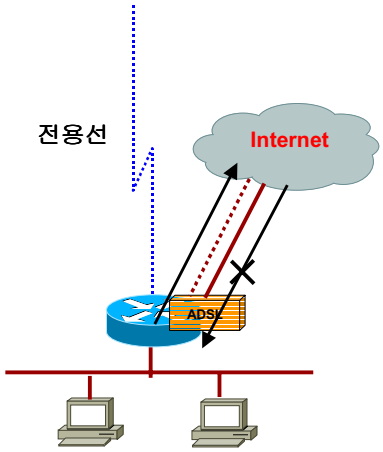
Branch Internet/VPN
구성방안

-Router 통합 Solution

Internet/VPN 방안 1-1

Cisco.com

Router를 이용한 단일 장비 구성 - Access list only



- 구성: 라우터의 Access-list로 Packet Filter 하여 Internet 접속은 Outbound WEB 만 허용, 외부로부터의 다른 모든 접속은 차단

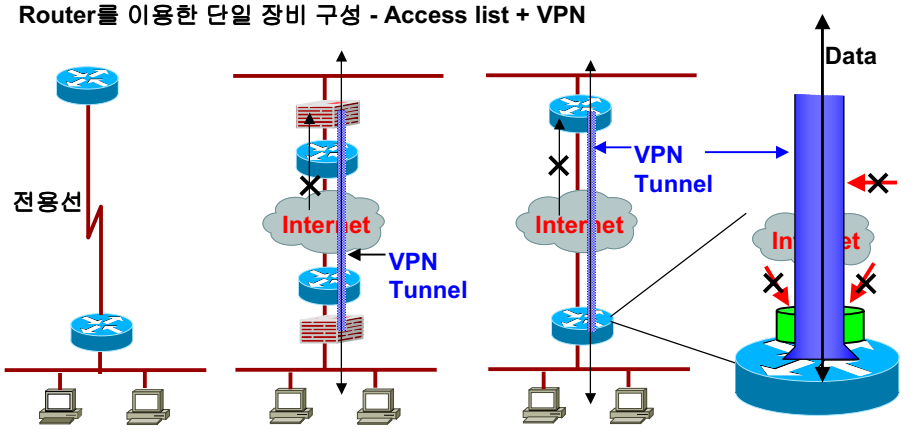
-장비: 라우터의 기본 S/W에 ADSL 카드장착

-적용 : 지사에 Client만 존재하고, 본사를 Internet을 통하여 접속하는 경우

Internet/VPN 방안 1-2

Cisco.com

Router를 이용한 단일 장비 구성 - Access list + VPN



전용선 연결

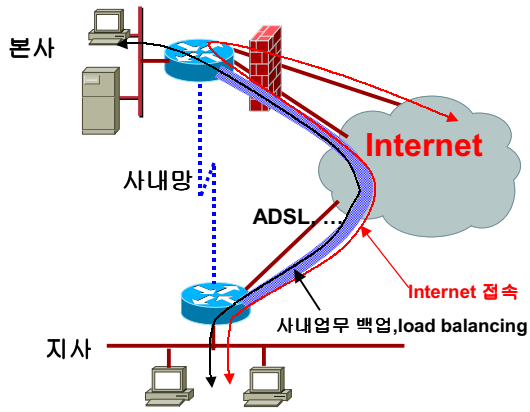
F/W VPN 연결

VPN 연결

라우터 ADLS 포트에 IPSec 이외의 모든 Traffic 을 filtering하여 VPN을 통해서만 통신이 가능하게 함

Internet/VPN 방안 1-2

Router를 이용한 단일 장비 구성 - Access list + VPN



-구성: 라우터의 Access-list로 Packet Filter하여 VPN을 통해서만 통신. 사내망의 백업및 업무분담으로 VPN 이용.
Internet은 VPN을 통하여 본사의 F/W을 통하여 접속

-장비: 라우터에 VPN이 추가된 S/W와 ADSL 카드장착

-적용 : 모든 지점/지사에 적용가능

-관리의 단순화, 보안

-Cisco GRE tunnel 사용시,
IP Multi-casting,
Dynamic Routing지원

IOS Firewall

Cisco IOS™

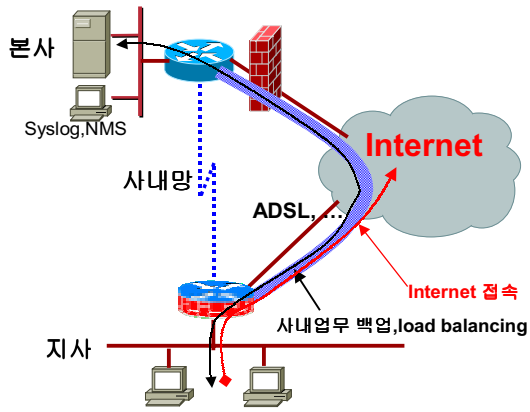
- **Integrated Security solution**
  - Combines Firewall and Routing into one platform
  - Combines Firewall features, Access lists and NAT(Network Address Translation) feature
  - Easy add on for existing network
- **No New hardware required** – Support Cisco 800, 900,1400,1600,1700,2500,2600,3600,7100,7200 and 7500 routers and Catalyst Switch with IOS
- **Firewall Feature Overview**
  - CBAC(Context Based Access Control)
  - Intrusion Detection(59 Signatures)
  - Authentication Proxy
  - Denial of Service Detection and Prevention
  - Dynamic Port Mapping
  - Real Time Alerts & Aduit Trail
  - Etc.

[Data Sheet]
http://wwwin.cisco.com/cmc/cc/pd/iosw/ioft/iofwft/prodlit/fire_ds.htm

[Technical Document]
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/fw3600.htm
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/index.htm

Internet/VPN 방안 1-3

Router를 이용한 단일 장비 구성 – Fire wall + VPN + IDS



-구성: 라우터의 IOS fire wall과 VPN을 이용하여, 사내망의 백업및 업무분담으로 VPN 이용, Internet은 Split Tunnel로 Internet 을 직접 접속

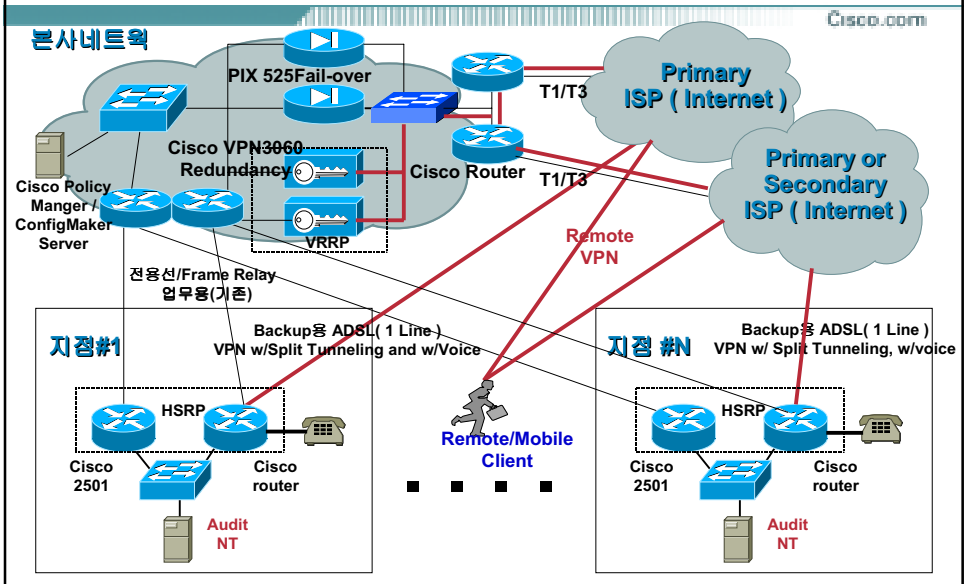
-장비: 라우터의 VPN,F/W이 추가된 S/W와 ADSL 카드장착

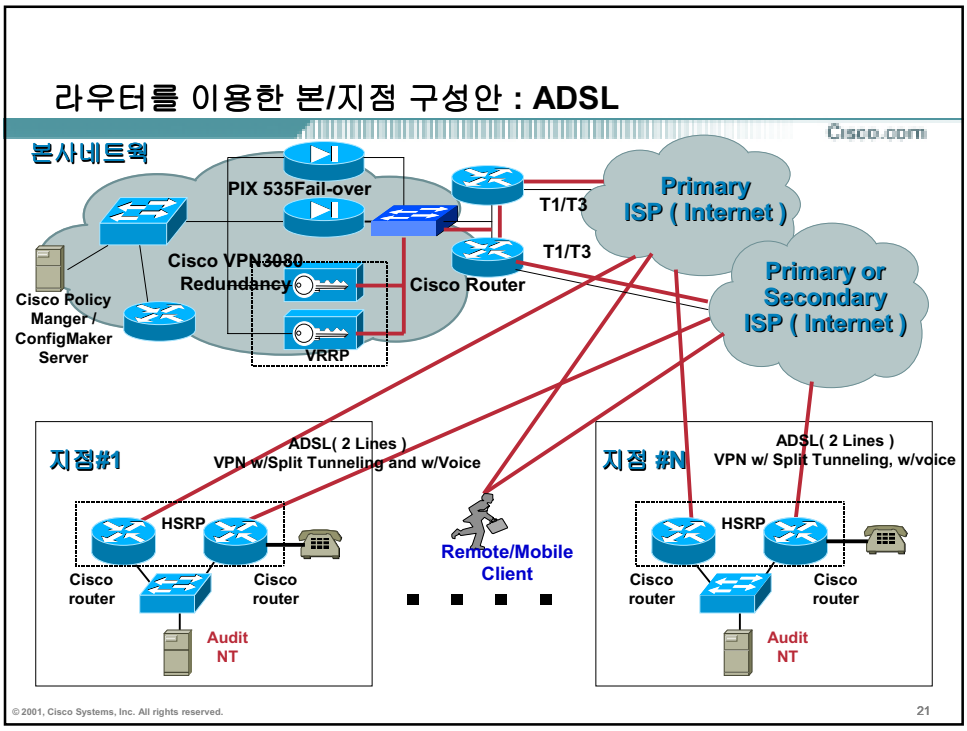
-적용 : 모든 지점/지사에 적용가능

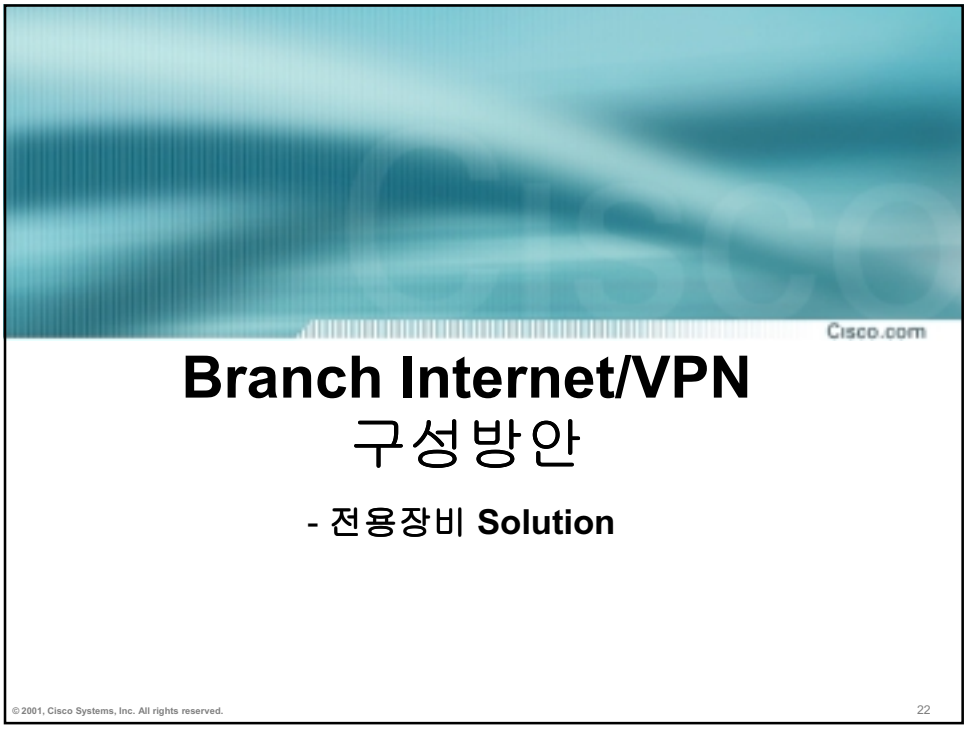
-완벽한 보안과 효율적인 성능개선

-관리 point 증가

라우터를 이용한 본/지점 구성안 : 전용선 + ADSL



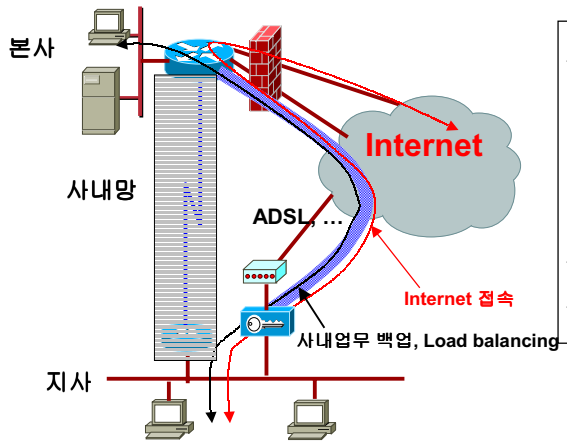




Internet/VPN 방안 2-1

Cisco.com

전용장비를 이용한 복수 장비 구성 – Access list + VPN



-구성: VPN 3000의 Access-list로 Packet Filter하여 VPN을 통해서만 통신, 또는 PIX를 이용한 VPN tunnel 구성. 사내망의 백업 및 업무분담으로 VPN 이용. Internet은 VPN을 통하여 본사의 F/W을 통하여 접속

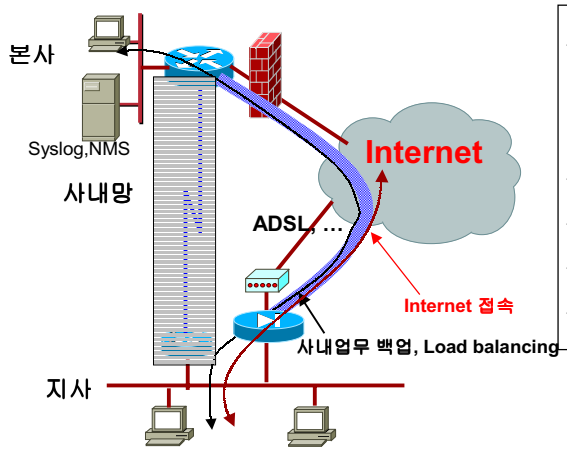
-장비: VPN 3000, ADSL Modem

-보안과 관리 용이

Internet/VPN 방안 2-2

Cisco.com

전용장비를 이용한 복수 장비 구성 – Firewall + VPN + IDS



-구성: PIX fire wall의 VPN기능을 이용하여, 사내망의 백업 및 업무분담으로 VPN 이용, Internet은 Split Tunnel로 Internet 을 직접 접속

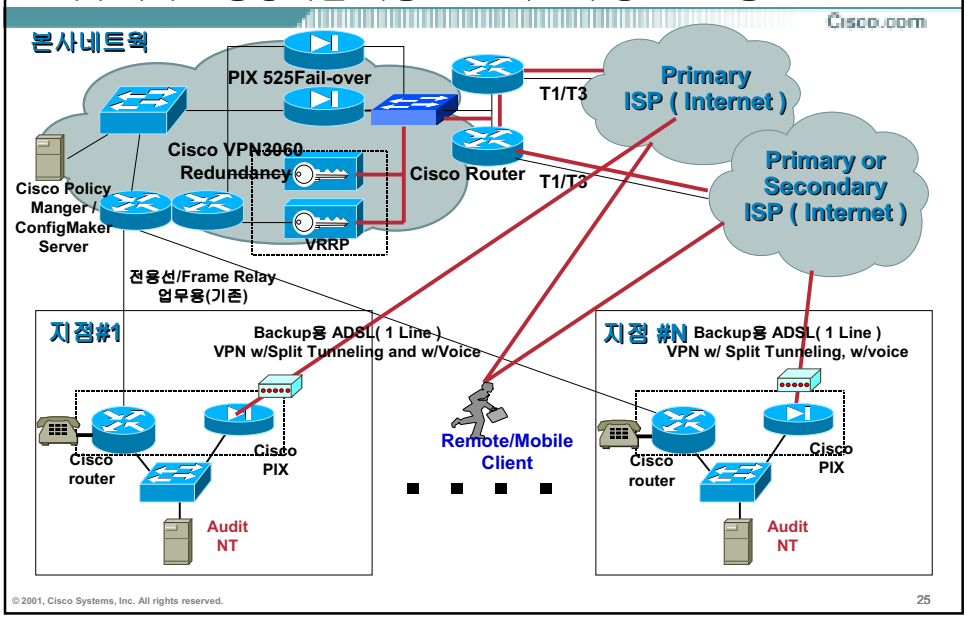
-장비: PIX(501), ADSL Modem

-적용 : 모든 지점/지사에 적용가능

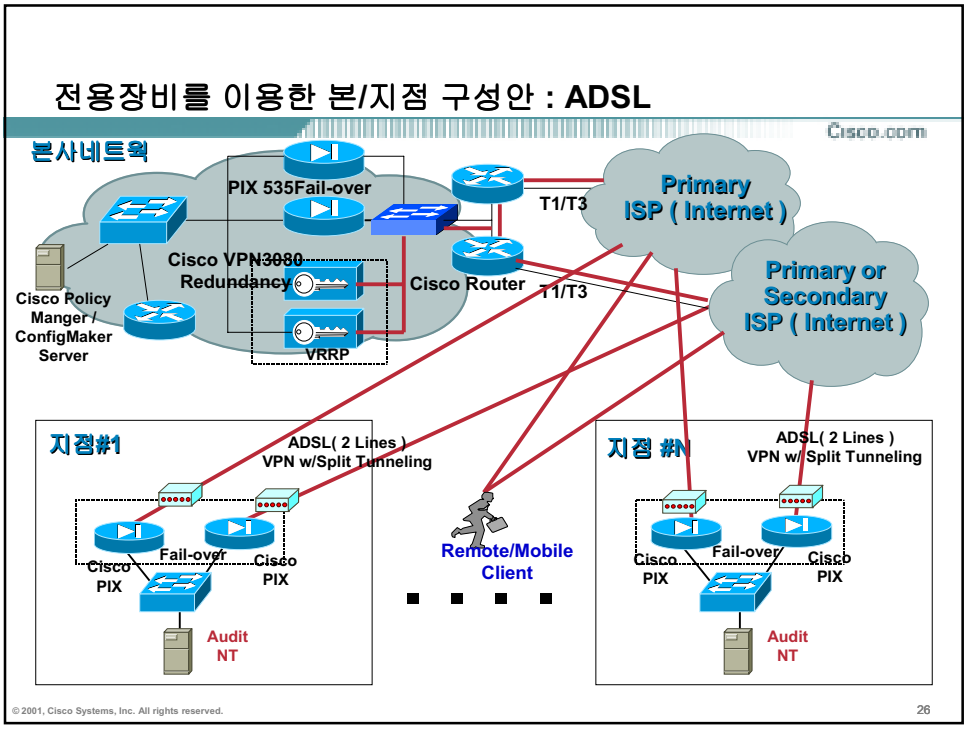
-완벽한 보안과 효율적인 성능개선

-관리 point 증가

라우터와 전용장비를 이용한 본/지점 구성안 : 전용선 + ADSL



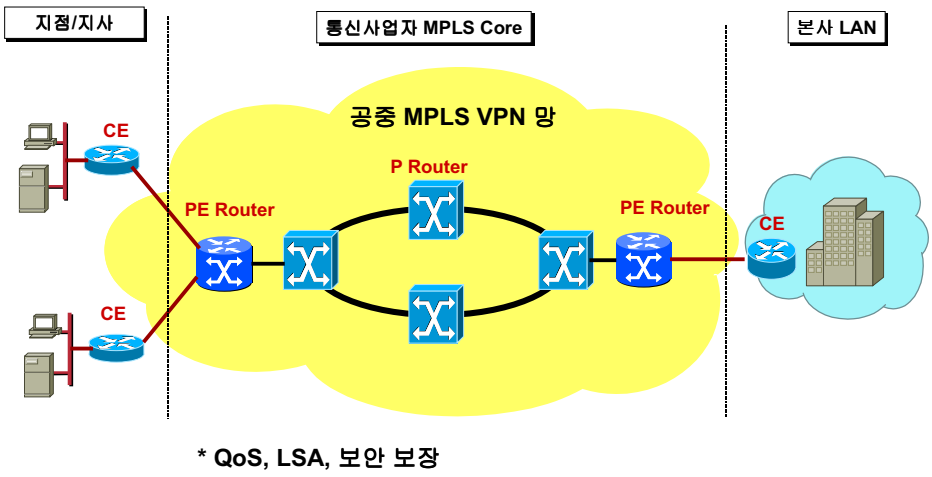
전용장비를 이용한 본/지점 구성안 : ADSL



Branch Internet/VPN
구성방안

-통신 사업자 **Solution**

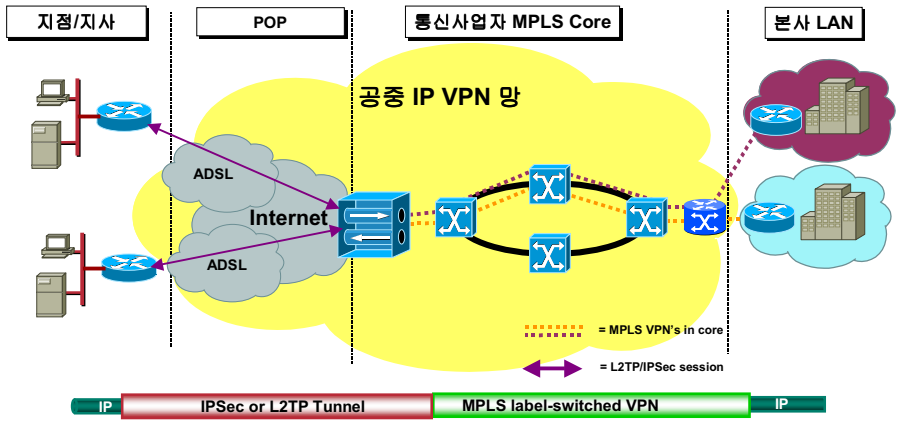
공중 VPN 분석 1 : MPLS VPN 망



* QoS, LSA, 보안 보장

공중 VPN 분석 2 : MPLS VPN + IP/ADSL망 (L2TP/IPsec)

Cisco.com



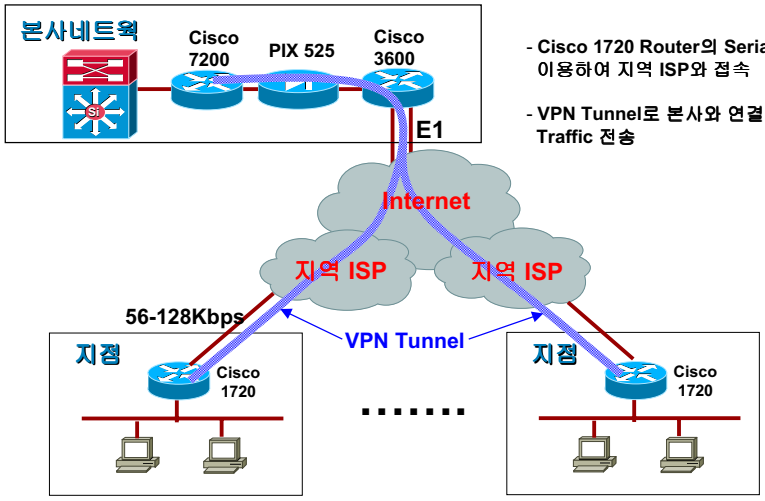
* 고속, QoS, LSA, 보안

Cisco.com

적용 사례 분석

사례 1 : 금융기관

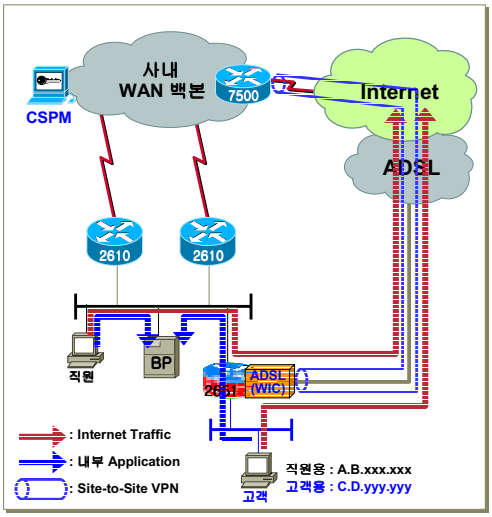
Cisco.com



- Cisco 1720 Router의 Serial port를 이용하여 지역 ISP와 접속
- VPN Tunnel로 본사와 연결하여 모든 Traffic 전송

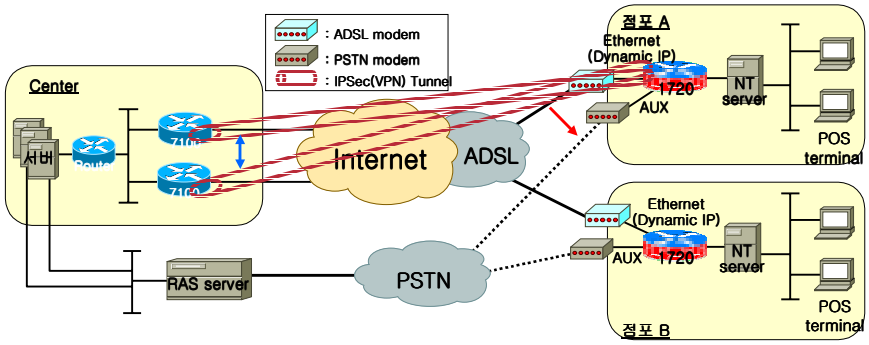
사례 2 : 금융기관

Cisco.com



- ❑ 고객 네트웍과 직원/사내 네트웍간 Segment분리를 통한 보안 강화
- ❑ ADSL을 이용한 지점단에서의 Internet Traffic의 분리
- ❑ ADSL interface와 직원 Ethernet interface에 Access -List적용 및 IOS F/W을 적용하여 보안 강화
- ❑ Routing Protocol적용을 통한 ADSL line down시 자동으로 전용선쪽으로 Backup되도록 구성
- ❑ 지점과 전산센터의 Router간 Site-to-Site VPN을 구성하여 전용선 Down시 Internet을 통한 Backup이 되도록 구성
- ❑ Router의 Security관련 Config(Access-list,NAT, Static정보, IOS F/W, VPN등)관리 및 Policy 관리를 위해 CSPM(Cisco Security Policy Manager) 적용

사례 3 : 유통업체



- Center의 7100 Router와 Remote의 1720 Router간 Site-to-Site VPN연결.
  (Center는 전용선으로 인터넷과 연결되고, Remote는 ADSL(유동 IP)로 연결)
- Center에 7100 2대를 구성하여 IPSec Tunnel간 Load Balancing 및 Failover구현.(↔)
- Remote의 ADSL line fail시 ISDN(또는 PSTN)으로 자동 Backup되도록 구성.(→)
- Remote 1720 Router에는 NAT, ACL, IOS F/W & IDS 적용.
- CSPM or VDM을 이용한 Management 구성.

CISCO SYSTEMS

EMPOWERING THE INTERNET GENERATION℠