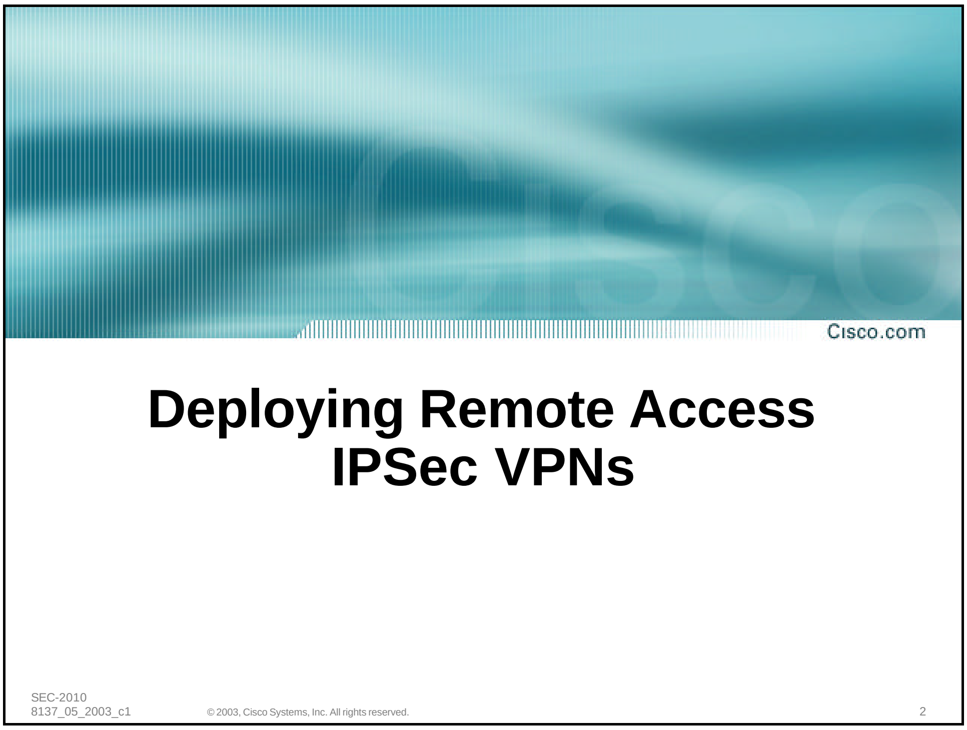
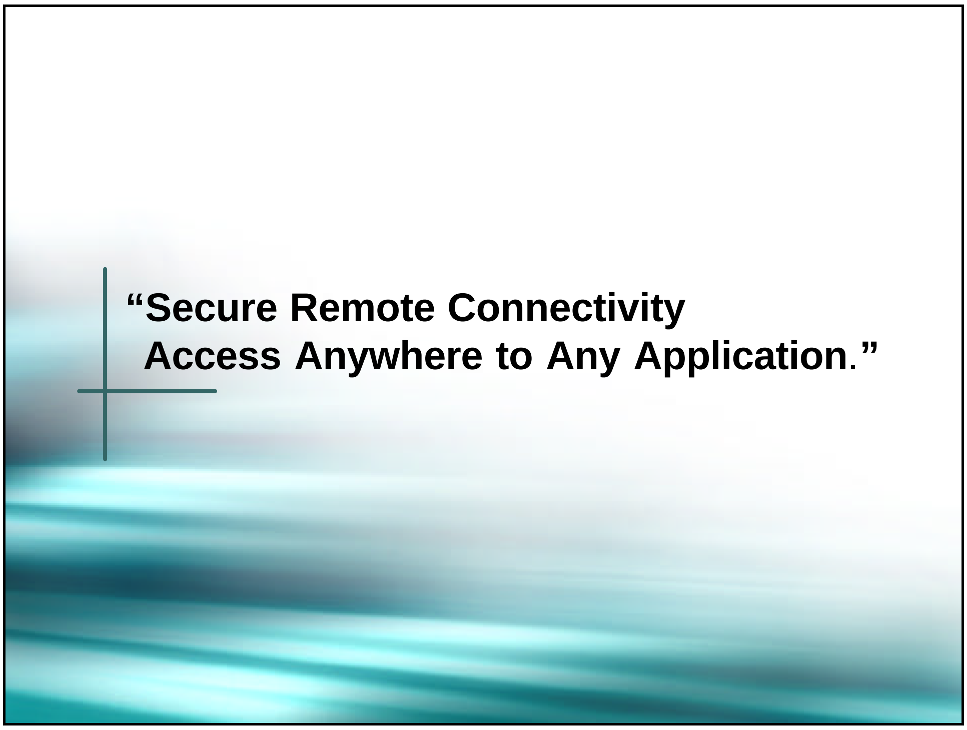
CISCO SYSTEMS

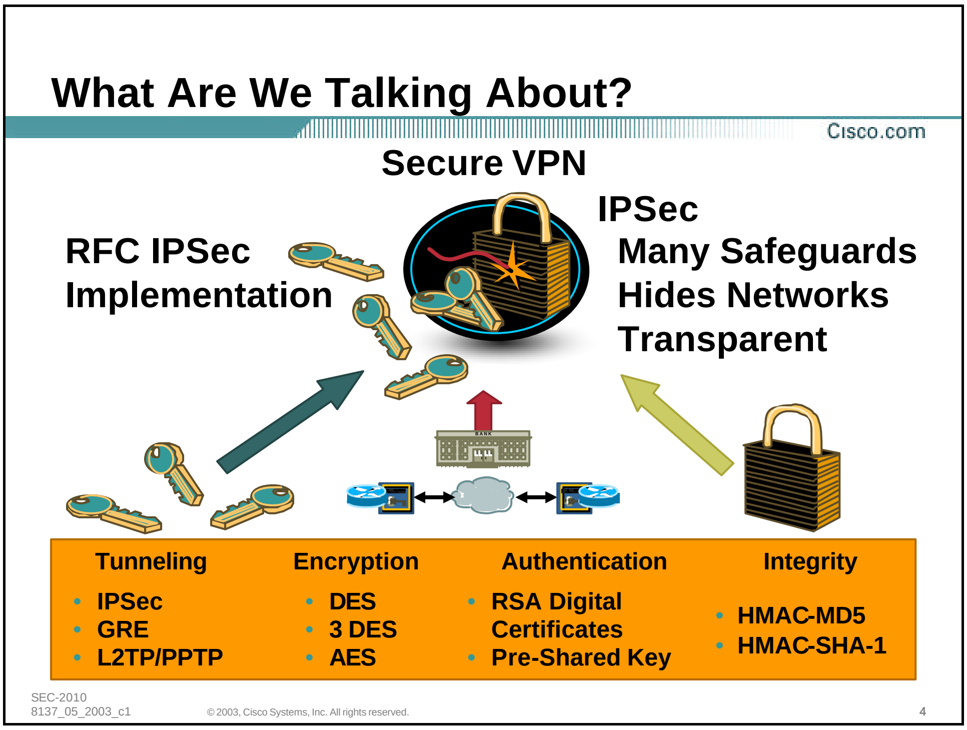


Cisco.com

Deploying Remote Access IPSec VPNs

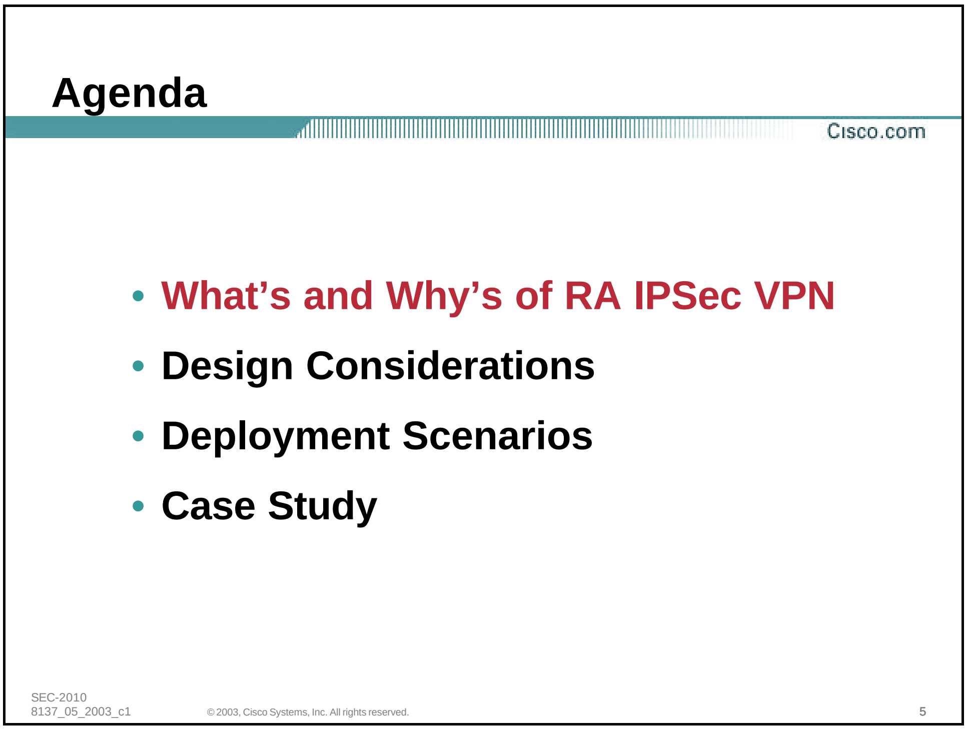


“Secure Remote Connectivity
Access Anywhere to Any Application.”



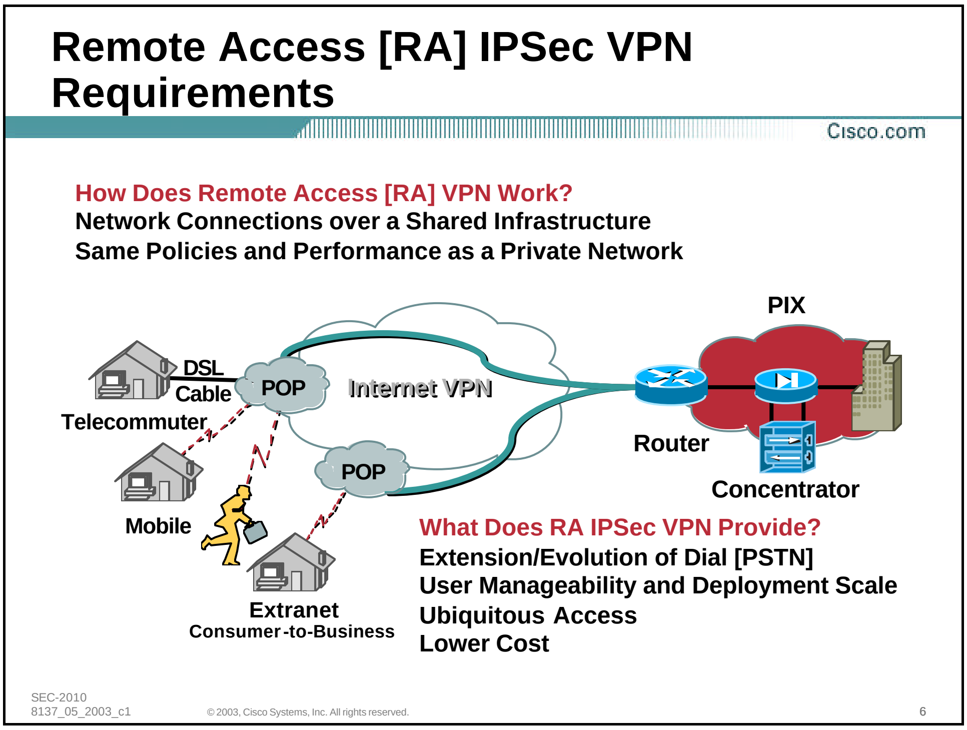
What Are We Talking About?

Tunneling	Encryption	Authentication	Integrity
• IPSec • GRE • L2TP/PPTP	• DES • 3 DES • AES	• RSA Digital Certificates • Pre-Shared Key	• HMAC-MD5 • HMAC-SHA-1



Agenda

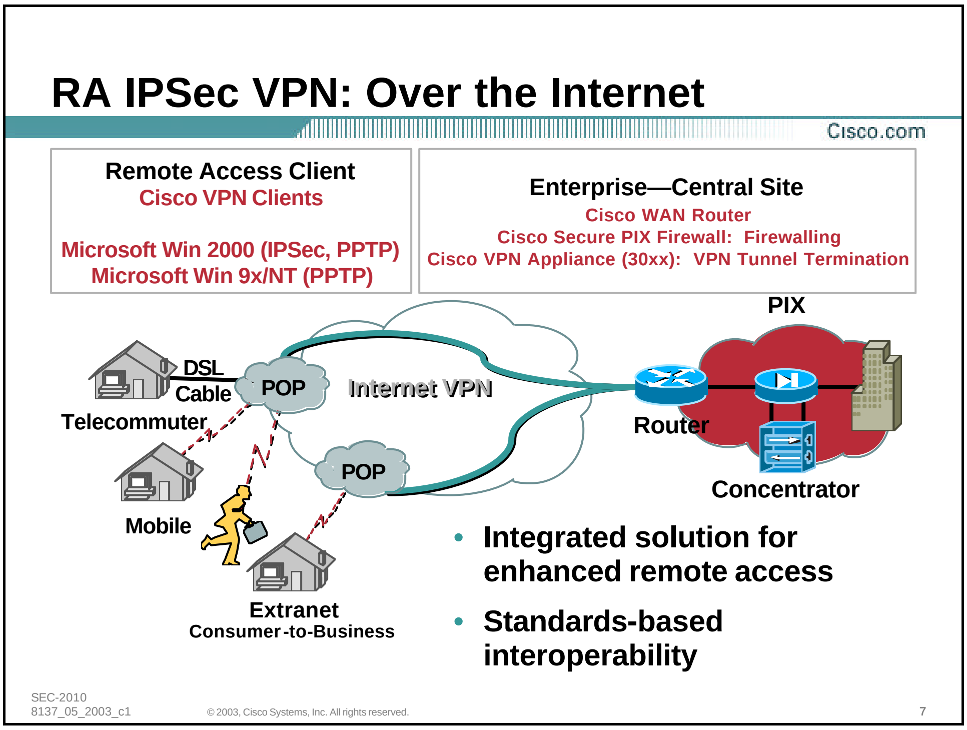
- What’s and Why’s of RA IPSec VPN
- Design Considerations
- Deployment Scenarios
- Case Study



Remote Access [RA] IPSec VPN Requirements

How Does Remote Access [RA] VPN Work?
Network Connections over a Shared Infrastructure
Same Policies and Performance as a Private Network

What Does RA IPSec VPN Provide?
Extension/Evolution of Dial [PSTN]
User Manageability and Deployment Scale
Ubiquitous Access
Lower Cost



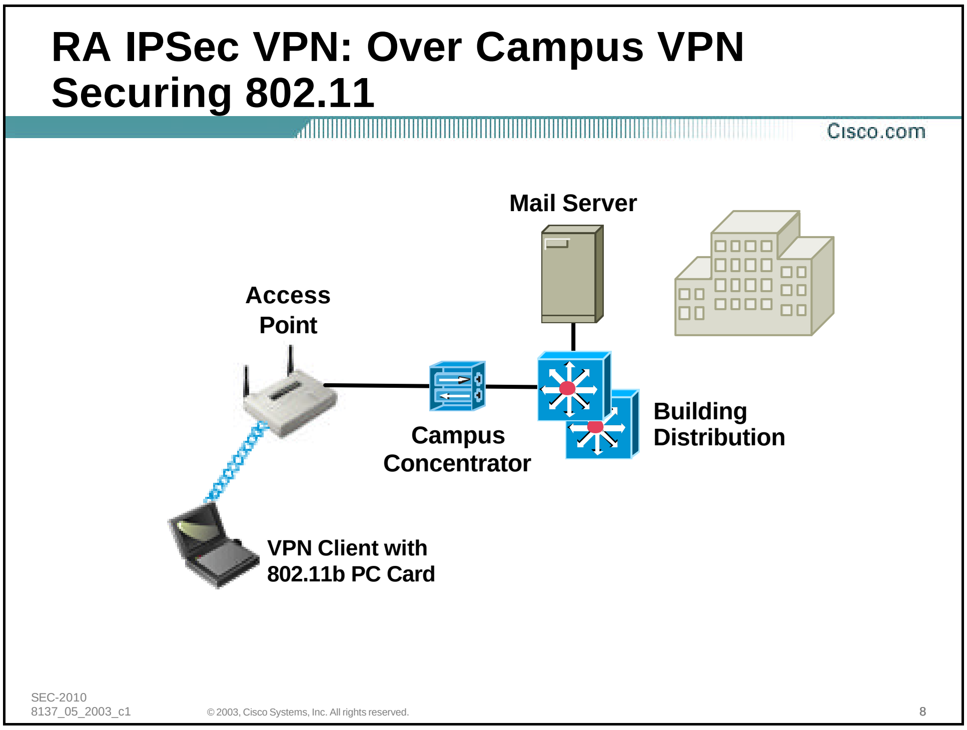
RA IPSec VPN: Over the Internet

Remote Access Client
Cisco VPN Clients

Microsoft Win 2000 (IPSec, PPTP)
Microsoft Win 9x/NT (PPTP)

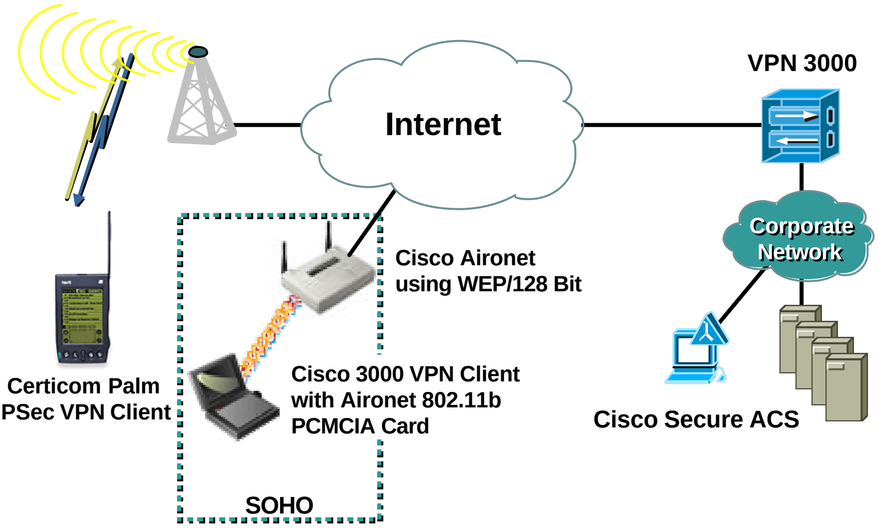
Enterprise—Central Site
Cisco WAN Router
Cisco Secure PIX Firewall: Firewalling
Cisco VPN Appliance (30xx): VPN Tunnel Termination

- Integrated solution for enhanced remote access
- Standards-based interoperability



RA IPSec VPN: Over Campus VPN Securing 802.11

RA IPSec VPN: Wireless Access VPN Securing Wireless ISP Access



Internet

VPN 3000

Corporate Network

Cisco Aironet using WEP/128 Bit

Certicom Palm IPSec VPN Client

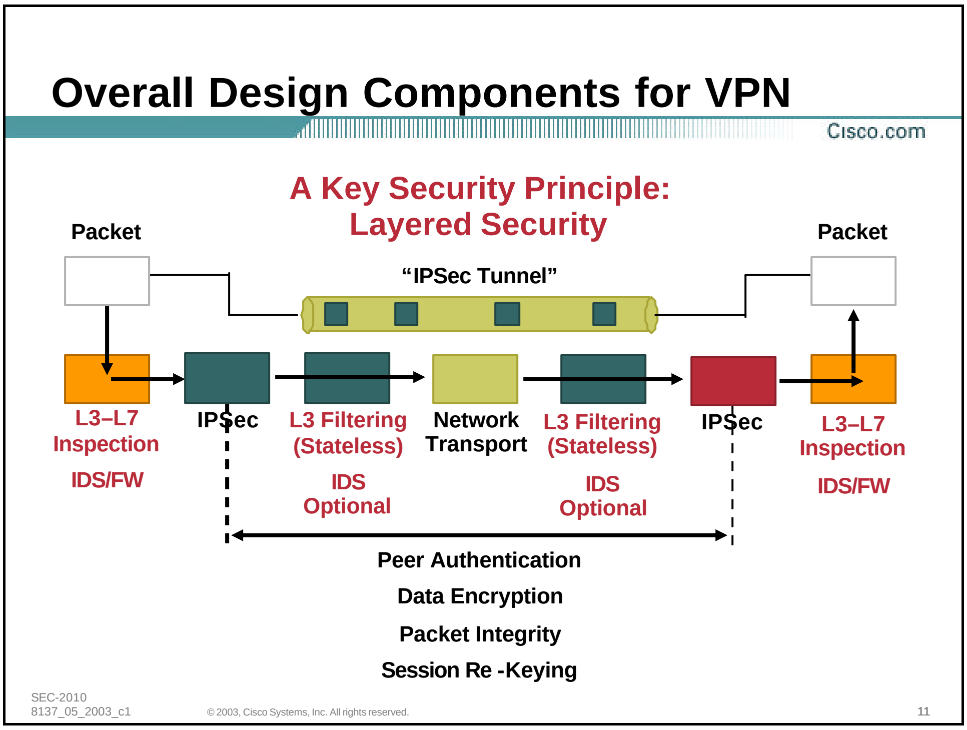
Cisco 3000 VPN Client with Aironet 802.11b PCMCIA Card

Cisco Secure ACS

SOHO

Agenda

- What’s and Why’s of RA IPSec VPN
- Design Considerations
- Deployment Scenarios
- Case Study



Overall Design Components for VPN

Cisco.com

A Key Security Principle:
Layered Security

Packet

Packet

"IPSec Tunnel"

L3–L7 Inspection

IDS/FW

IPSec

L3 Filtering (Stateless)

IDS Optional

Network Transport

L3 Filtering (Stateless)

IDS Optional

IPSec

L3–L7 Inspection

IDS/FW

Peer Authentication

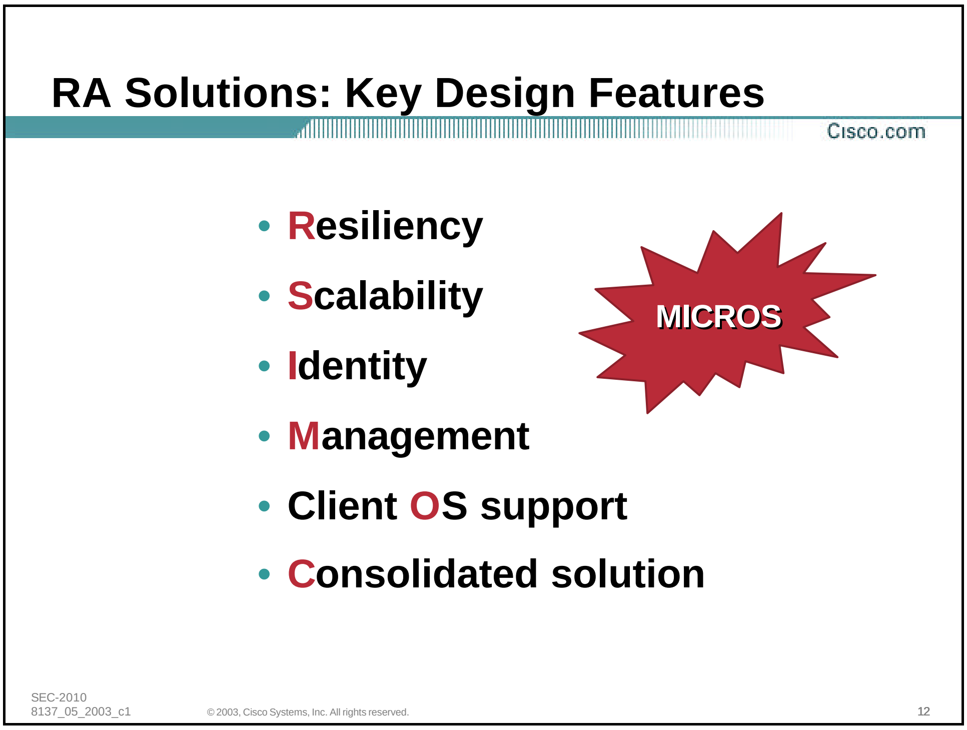
Data Encryption

Packet Integrity

Session Re -Keying

SEC-2010
8137_05_2003_c1

© 2003, Cisco Systems, Inc. All rights reserved.



RA Solutions: Key Design Features

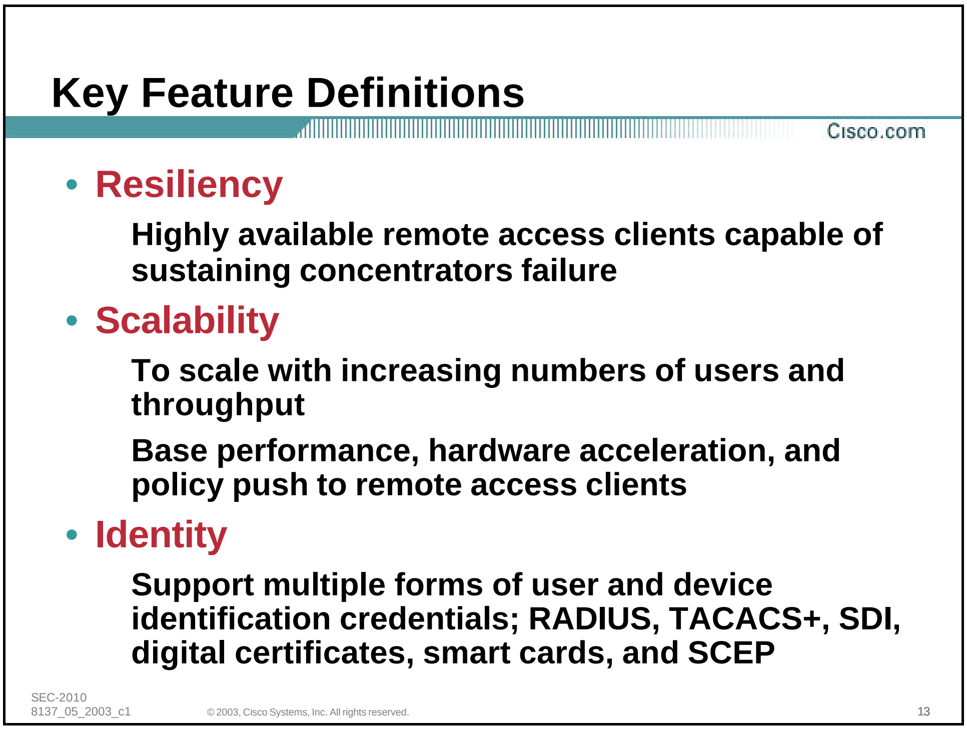
Cisco.com

- Resiliency
- Scalability
- Identity
- Management
- Client OS support
- Consolidated solution

MICROS

SEC-2010
8137_05_2003_c1

© 2003, Cisco Systems, Inc. All rights reserved.



Key Feature Definitions

- Resiliency

  Highly available remote access clients capable of sustaining concentrators failure

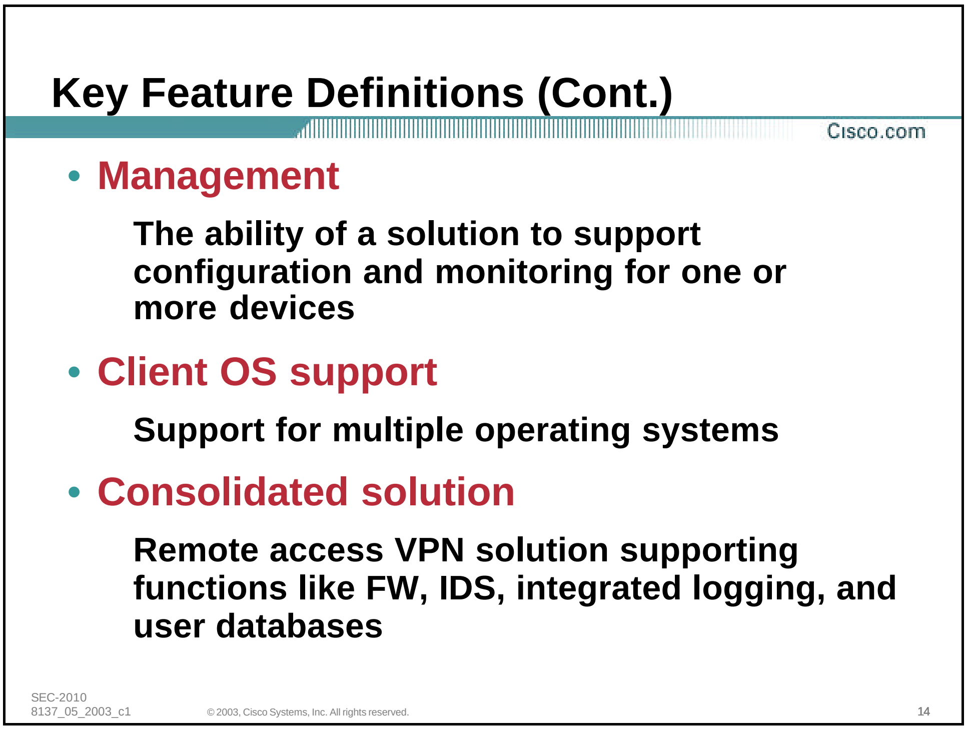
- Scalability

  To scale with increasing numbers of users and throughput

  Base performance, hardware acceleration, and policy push to remote access clients

- Identity

  Support multiple forms of user and device identification credentials; RADIUS, TACACS+, SDI, digital certificates, smart cards, and SCEP



Key Feature Definitions (Cont.)

- Management

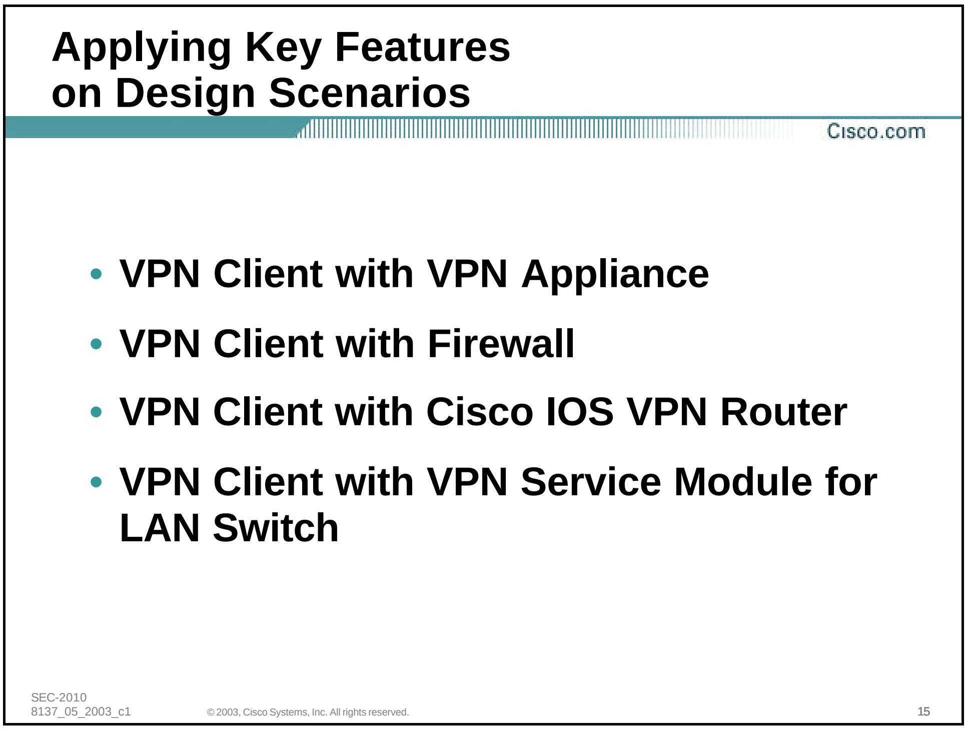
  The ability of a solution to support configuration and monitoring for one or more devices

- Client OS support

  Support for multiple operating systems

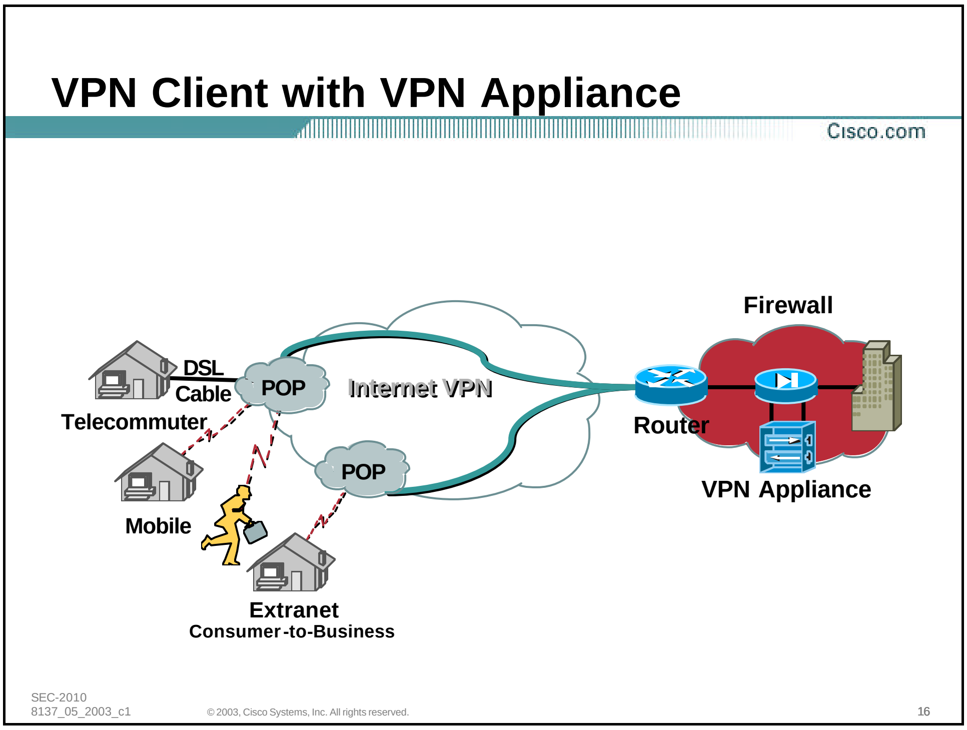
- Consolidated solution

  Remote access VPN solution supporting functions like FW, IDS, integrated logging, and user databases

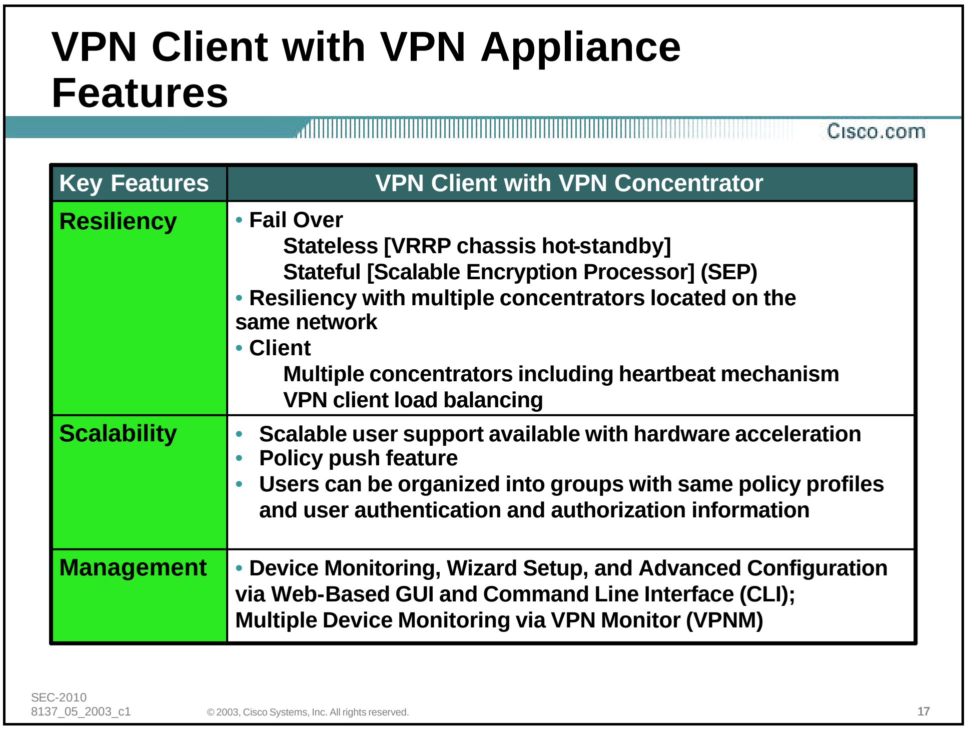


Applying Key Features on Design Scenarios

- VPN Client with VPN Appliance
- VPN Client with Firewall
- VPN Client with Cisco IOS VPN Router
- VPN Client with VPN Service Module for LAN Switch

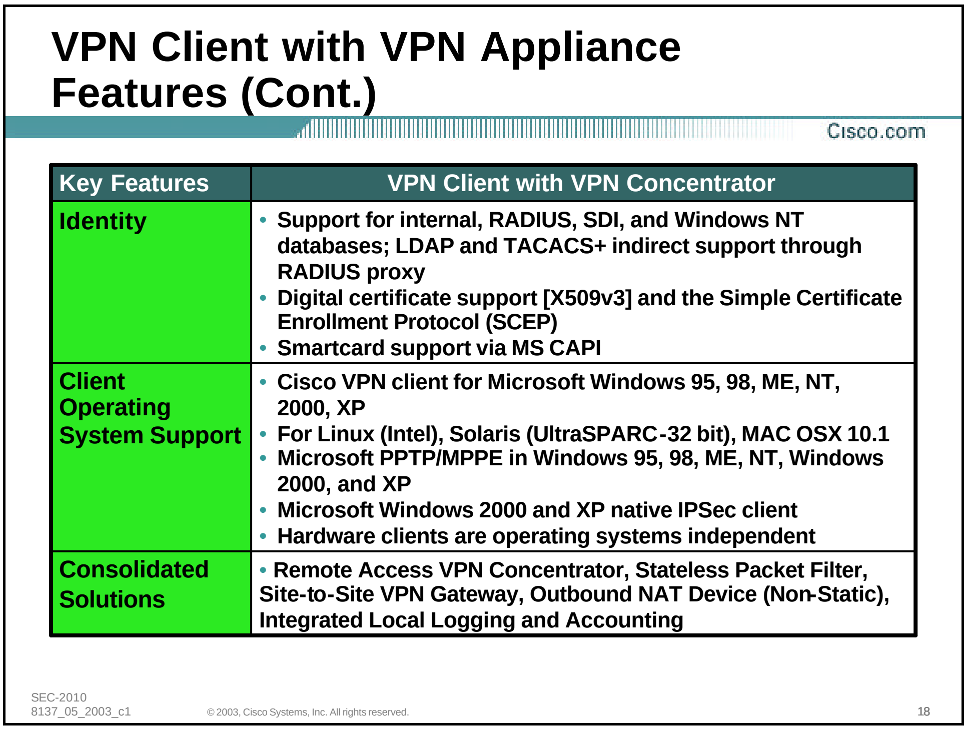


VPN Client with VPN Appliance



VPN Client with VPN Appliance Features

Key Features	VPN Client with VPN Concentrator
Resiliency	• Fail Over Stateless [VRRP chassis hot-standby] Stateful [Scalable Encryption Processor] (SEP) • Resiliency with multiple concentrators located on the same network • Client Multiple concentrators including heartbeat mechanism VPN client load balancing
Scalability	• Scalable user support available with hardware acceleration • Policy push feature • Users can be organized into groups with same policy profiles and user authentication and authorization information
Management	• Device Monitoring, Wizard Setup, and Advanced Configuration via Web-Based GUI and Command Line Interface (CLI); Multiple Device Monitoring via VPN Monitor (VPNM)



VPN Client with VPN Appliance Features (Cont.)

Key Features	VPN Client with VPN Concentrator
Identity	• Support for internal, RADIUS, SDI, and Windows NT databases; LDAP and TACACS+ indirect support through RADIUS proxy • Digital certificate support [X509v3] and the Simple Certificate Enrollment Protocol (SCEP) • Smartcard support via MS CAPI
Client Operating System Support	• Cisco VPN client for Microsoft Windows 95, 98, ME, NT, 2000, XP • For Linux (Intel), Solaris (UltraSPARC-32 bit), MAC OSX 10.1 • Microsoft PPTP/MPPE in Windows 95, 98, ME, NT, Windows 2000, and XP • Microsoft Windows 2000 and XP native IPSec client • Hardware clients are operating systems independent
Consolidated Solutions	• Remote Access VPN Concentrator, Stateless Packet Filter, Site-to-Site VPN Gateway, Outbound NAT Device (Non-Static), Integrated Local Logging and Accounting

VPN Client with VPN Appliance Features (Cont.)

Advantages

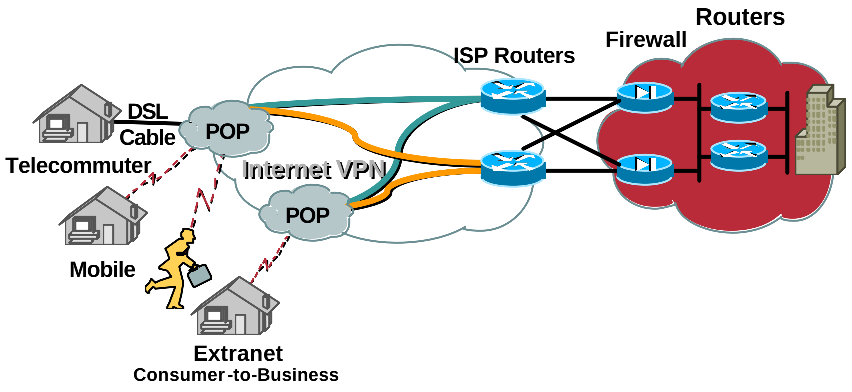
- Highly scalable solution
- Resiliency with VRRP

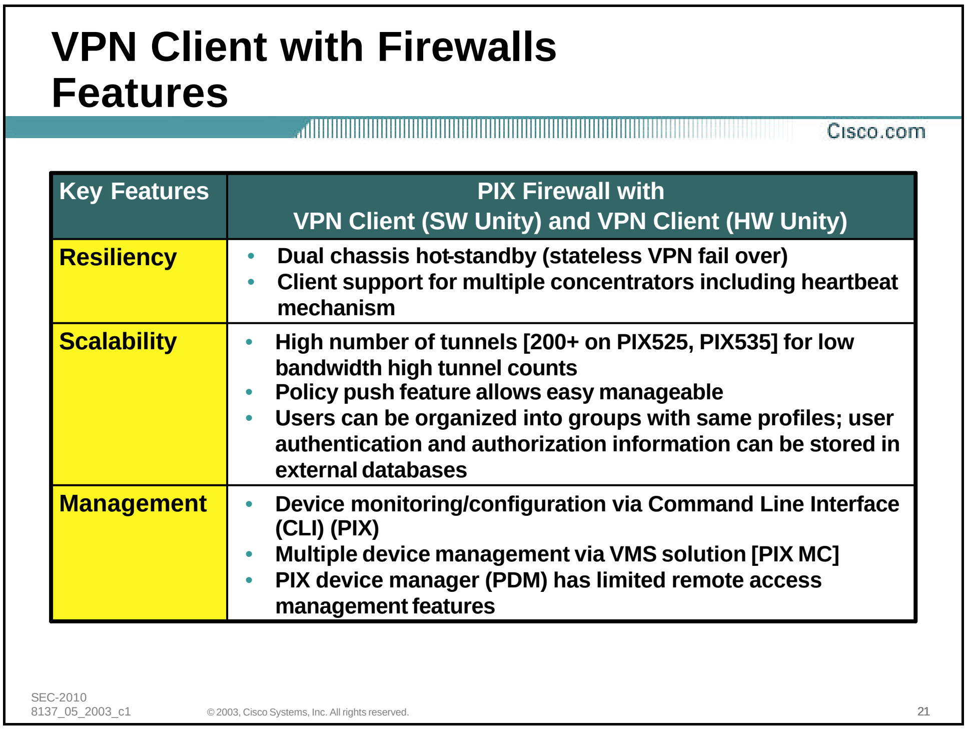
  or SEP
- Enforce security policy as stateful inspection of decrypted traffic
- Policy push for increased security at remote end

Disadvantages

- Migration to integrated solution is non trivial
- Configuration complexity is increased for firewall
- Firewall needs to route traffic to differentiate VPN verses non-VPN traffic

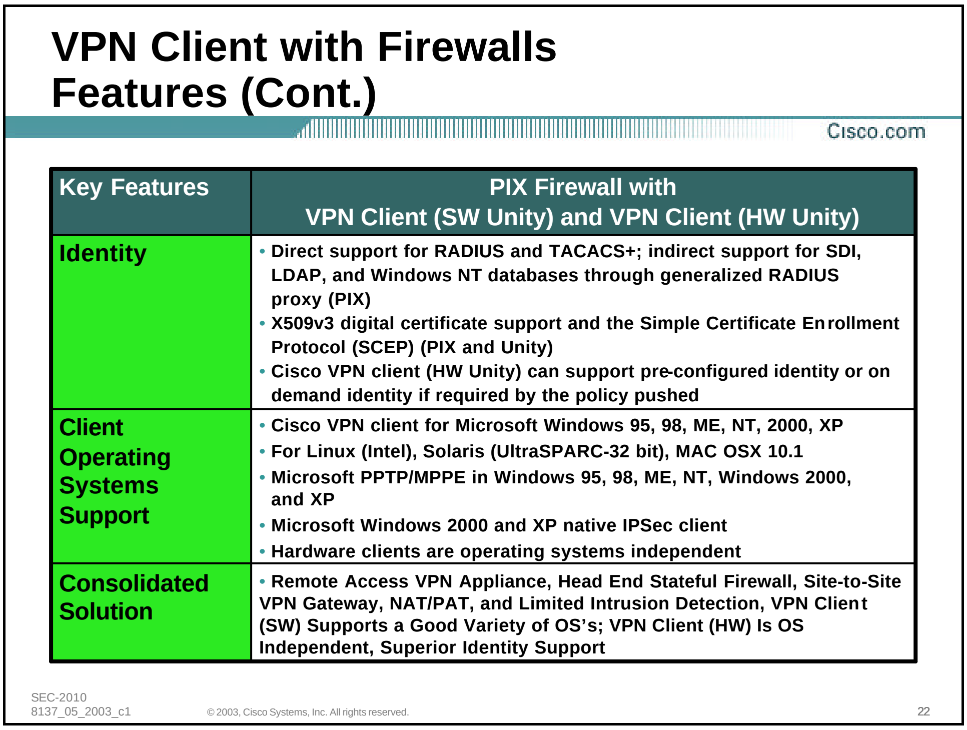
VPN Client with Firewall





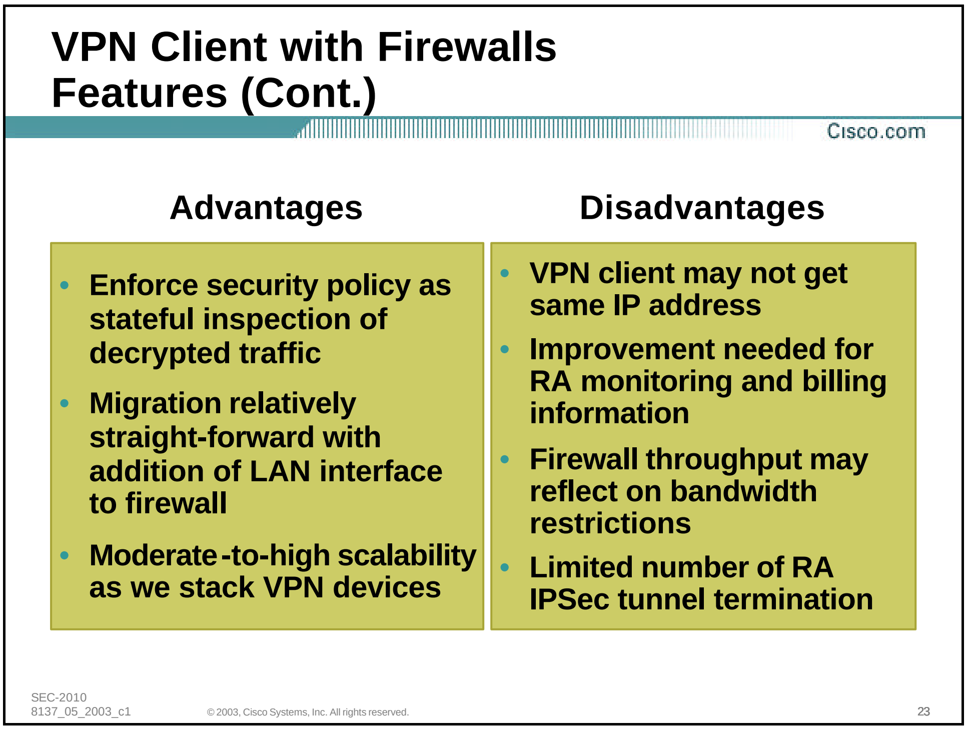
VPN Client with Firewalls Features

Key Features	PIX Firewall with VPN Client (SW Unity) and VPN Client (HW Unity)
Resiliency	• Dual chassis hot-standby (stateless VPN fail over) • Client support for multiple concentrators including heartbeat mechanism
Scalability	• High number of tunnels [200+ on PIX525, PIX535] for low bandwidth high tunnel counts • Policy push feature allows easy manageable • Users can be organized into groups with same profiles; user authentication and authorization information can be stored in external databases
Management	• Device monitoring/configuration via Command Line Interface (CLI) (PIX) • Multiple device management via VMS solution [PIX MC] • PIX device manager (PDM) has limited remote access management features



VPN Client with Firewalls Features (Cont.)

Key Features	PIX Firewall with VPN Client (SW Unity) and VPN Client (HW Unity)
Identity	• Direct support for RADIUS and TACACS+; indirect support for SDI, LDAP, and Windows NT databases through generalized RADIUS proxy (PIX) • X509v3 digital certificate support and the Simple Certificate Enrollment Protocol (SCEP) (PIX and Unity) • Cisco VPN client (HW Unity) can support pre-configured identity or on demand identity if required by the policy pushed
Client Operating Systems Support	• Cisco VPN client for Microsoft Windows 95, 98, ME, NT, 2000, XP • For Linux (Intel), Solaris (UltraSPARC-32 bit), MAC OSX 10.1 • Microsoft PPTP/MPPE in Windows 95, 98, ME, NT, Windows 2000, and XP • Microsoft Windows 2000 and XP native IPSec client • Hardware clients are operating systems independent
Consolidated Solution	• Remote Access VPN Appliance, Head End Stateful Firewall, Site-to-Site VPN Gateway, NAT/PAT, and Limited Intrusion Detection, VPN Client (SW) Supports a Good Variety of OS's; VPN Client (HW) Is OS Independent, Superior Identity Support



VPN Client with Firewalls Features (Cont.)

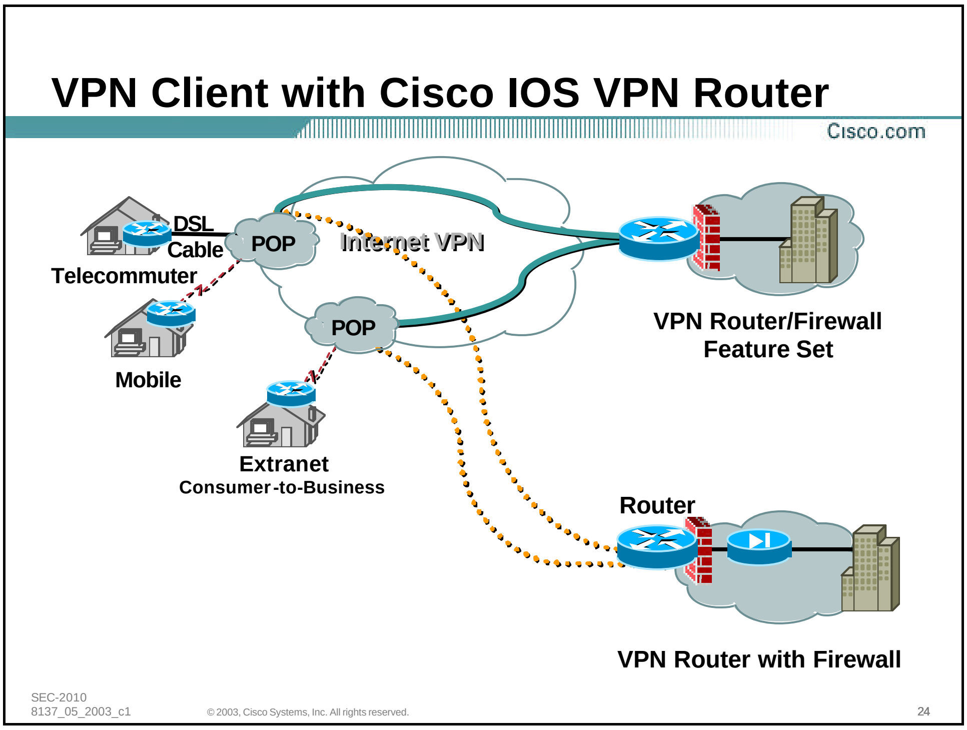
Cisco.com

Advantages

- Enforce security policy as stateful inspection of decrypted traffic
- Migration relatively straight-forward with addition of LAN interface to firewall
- Moderate-to-high scalability as we stack VPN devices

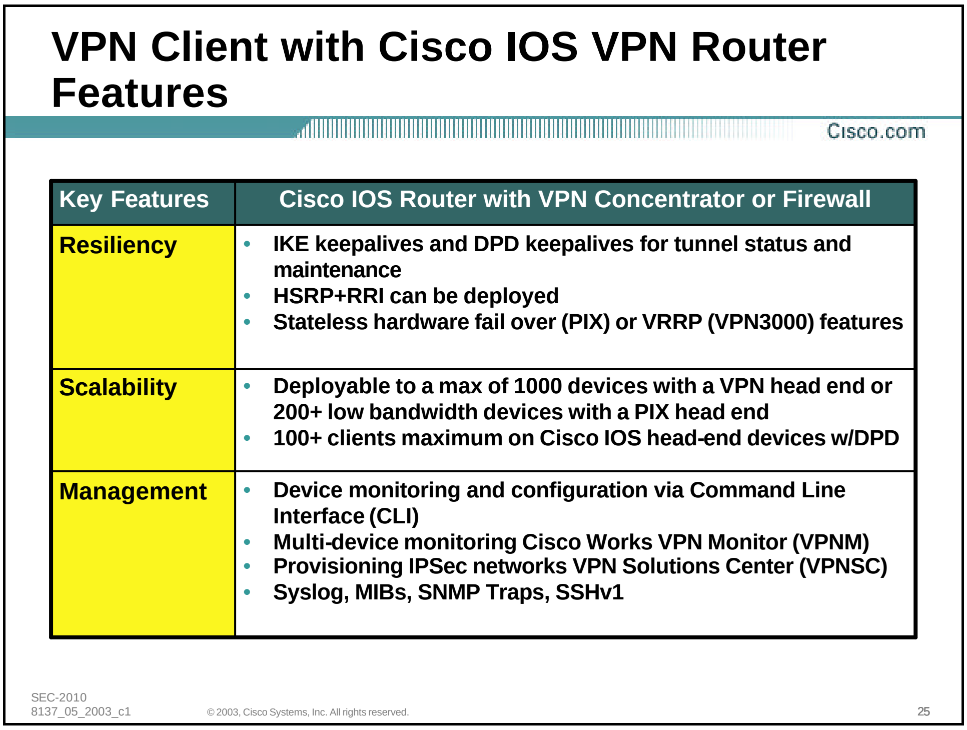
Disadvantages

- VPN client may not get same IP address
- Improvement needed for RA monitoring and billing information
- Firewall throughput may reflect on bandwidth restrictions
- Limited number of RA IPSec tunnel termination



VPN Client with Cisco IOS VPN Router

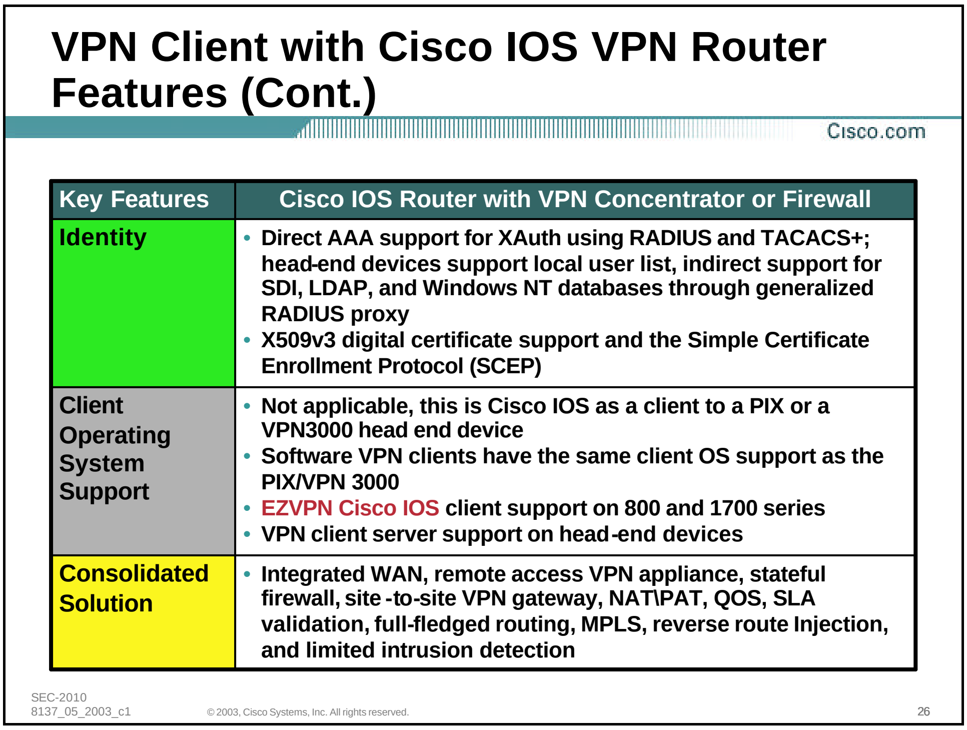
Cisco.com



VPN Client with Cisco IOS VPN Router Features

Cisco.com

Key Features	Cisco IOS Router with VPN Concentrator or Firewall
Resiliency	• IKE keepalives and DPD keepalives for tunnel status and maintenance • HSRP+RRI can be deployed • Stateless hardware fail over (PIX) or VRRP (VPN3000) features
Scalability	• Deployable to a max of 1000 devices with a VPN head end or 200+ low bandwidth devices with a PIX head end • 100+ clients maximum on Cisco IOS head-end devices w/DPD
Management	• Device monitoring and configuration via Command Line Interface (CLI) • Multi-device monitoring Cisco Works VPN Monitor (VPNM) • Provisioning IPSec networks VPN Solutions Center (VPNSC) • Syslog, MIBs, SNMP Traps, SSHv1



VPN Client with Cisco IOS VPN Router Features (Cont.)

Cisco.com

Key Features	Cisco IOS Router with VPN Concentrator or Firewall
Identity	• Direct AAA support for XAuth using RADIUS and TACACS+; head-end devices support local user list, indirect support for SDI, LDAP, and Windows NT databases through generalized RADIUS proxy • X509v3 digital certificate support and the Simple Certificate Enrollment Protocol (SCEP)
Client Operating System Support	• Not applicable, this is Cisco IOS as a client to a PIX or a VPN3000 head end device • Software VPN clients have the same client OS support as the PIX/VPN 3000 • EZVPN Cisco IOS client support on 800 and 1700 series • VPN client server support on head-end devices
Consolidated Solution	• Integrated WAN, remote access VPN appliance, stateful firewall, site-to-site VPN gateway, NAT\PAT, QOS, SLA validation, full-fledged routing, MPLS, reverse route Injection, and limited intrusion detection

VPN Client with Cisco IOS VPN Router Features (Cont.)

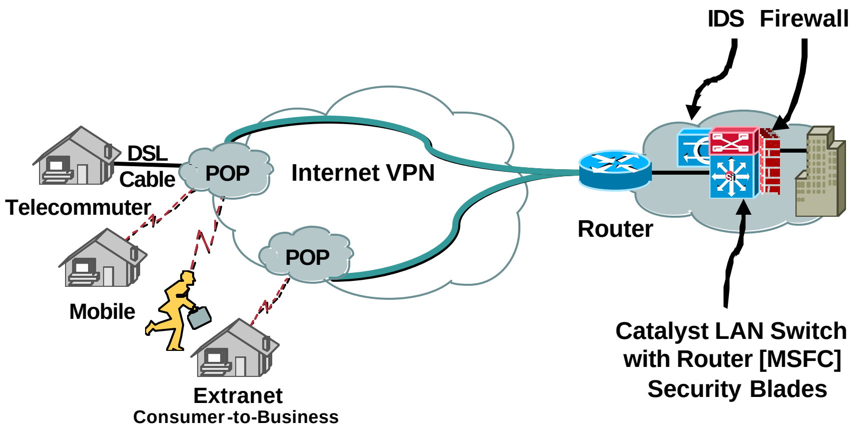
Advantages

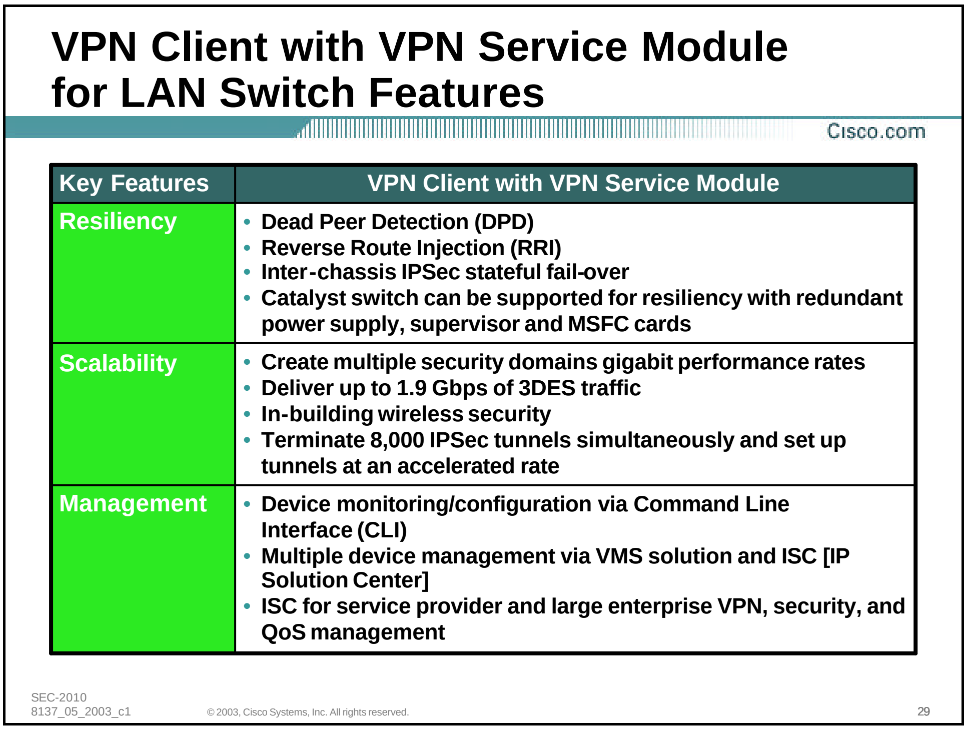
- Enforce security policy as stateful inspection of decrypted traffic
- Full-fledged routing protocol support
- Efficient to provide secure separation of clear traffic between private and public interfaces

Disadvantages

- VPN client will have to reconnect
- Need hardware acceleration cards
- Limited number of RA IPSec tunnels
- In event of failure, IKE request handling by Cisco IOS router is slower than VPN appliance

VPN Client with VPN Service Module for LAN Switch

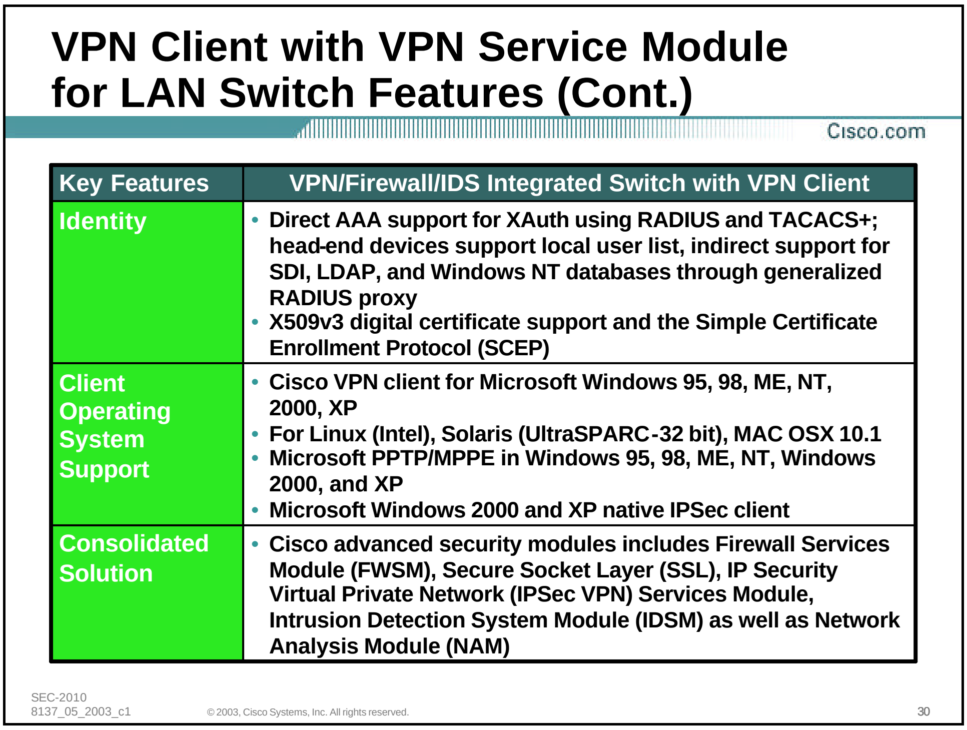




VPN Client with VPN Service Module for LAN Switch Features

Cisco.com

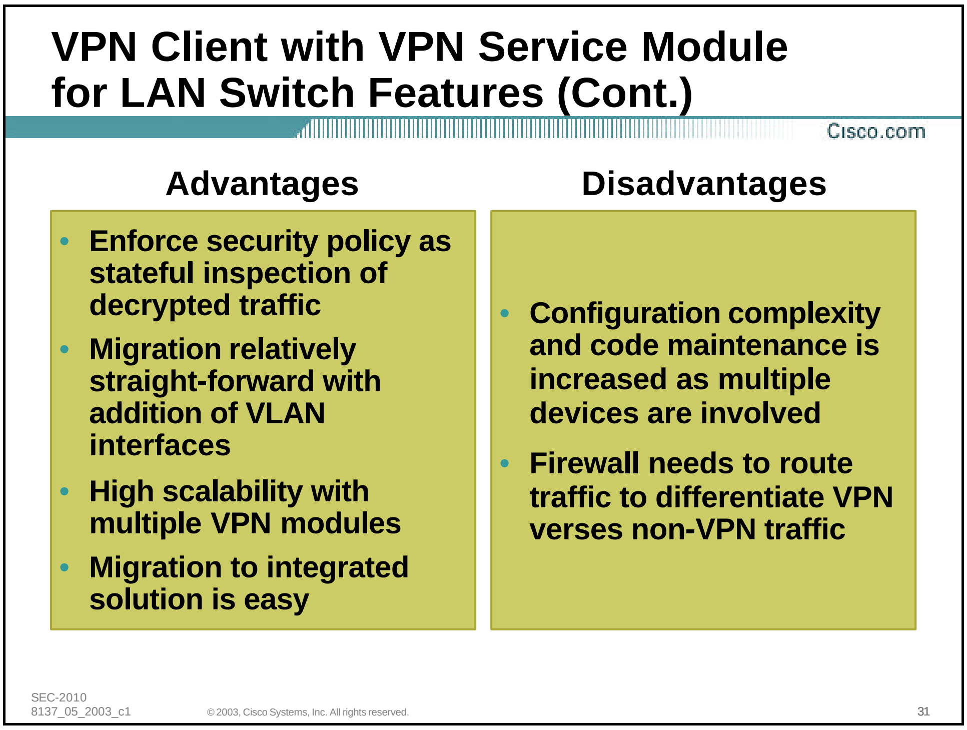
Key Features	VPN Client with VPN Service Module
Resiliency	• Dead Peer Detection (DPD) • Reverse Route Injection (RRI) • Inter-chassis IPSec stateful fail-over • Catalyst switch can be supported for resiliency with redundant power supply, supervisor and MSFC cards
Scalability	• Create multiple security domains gigabit performance rates • Deliver up to 1.9 Gbps of 3DES traffic • In-building wireless security • Terminate 8,000 IPSec tunnels simultaneously and set up tunnels at an accelerated rate
Management	• Device monitoring/configuration via Command Line Interface (CLI) • Multiple device management via VMS solution and ISC [IP Solution Center] • ISC for service provider and large enterprise VPN, security, and QoS management



VPN Client with VPN Service Module for LAN Switch Features (Cont.)

Cisco.com

Key Features	VPN/Firewall/IDS Integrated Switch with VPN Client
Identity	• Direct AAA support for XAuth using RADIUS and TACACS+; head-end devices support local user list, indirect support for SDI, LDAP, and Windows NT databases through generalized RADIUS proxy • X509v3 digital certificate support and the Simple Certificate Enrollment Protocol (SCEP)
Client Operating System Support	• Cisco VPN client for Microsoft Windows 95, 98, ME, NT, 2000, XP • For Linux (Intel), Solaris (UltraSPARC-32 bit), MAC OSX 10.1 • Microsoft PPTP/MPPE in Windows 95, 98, ME, NT, Windows 2000, and XP • Microsoft Windows 2000 and XP native IPSec client
Consolidated Solution	• Cisco advanced security modules includes Firewall Services Module (FWSM), Secure Socket Layer (SSL), IP Security Virtual Private Network (IPSec VPN) Services Module, Intrusion Detection System Module (IDSM) as well as Network Analysis Module (NAM)



VPN Client with VPN Service Module for LAN Switch Features (Cont.)

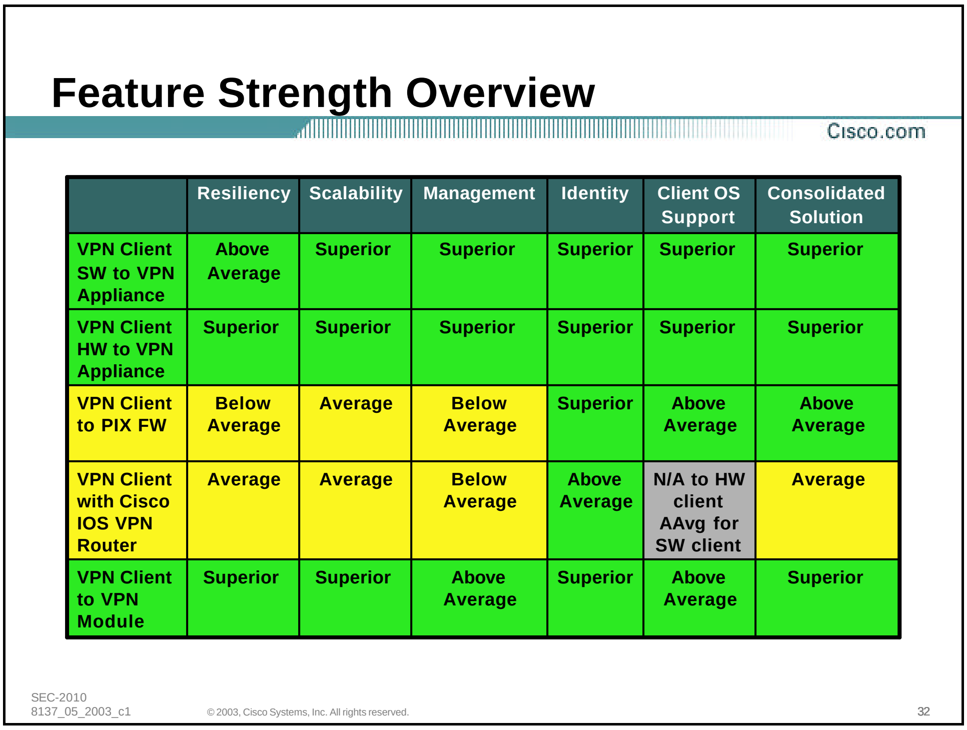
Cisco.com

Advantages

- Enforce security policy as stateful inspection of decrypted traffic
- Migration relatively straight-forward with addition of VLAN interfaces
- High scalability with multiple VPN modules
- Migration to integrated solution is easy

Disadvantages

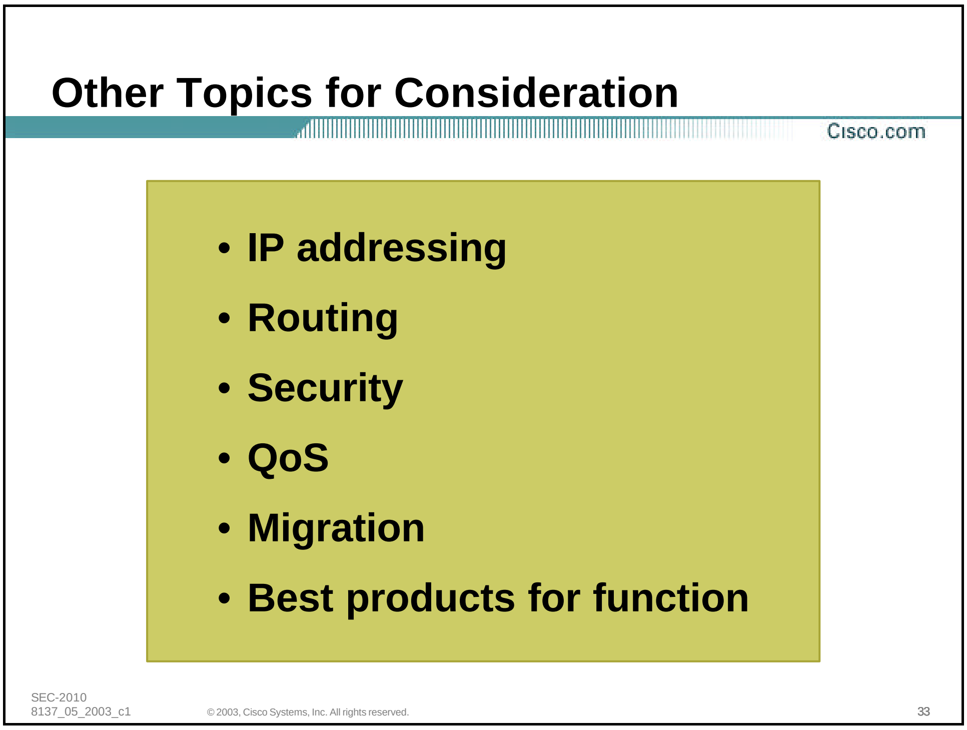
- Configuration complexity and code maintenance is increased as multiple devices are involved
- Firewall needs to route traffic to differentiate VPN verses non-VPN traffic



Feature Strength Overview

Cisco.com

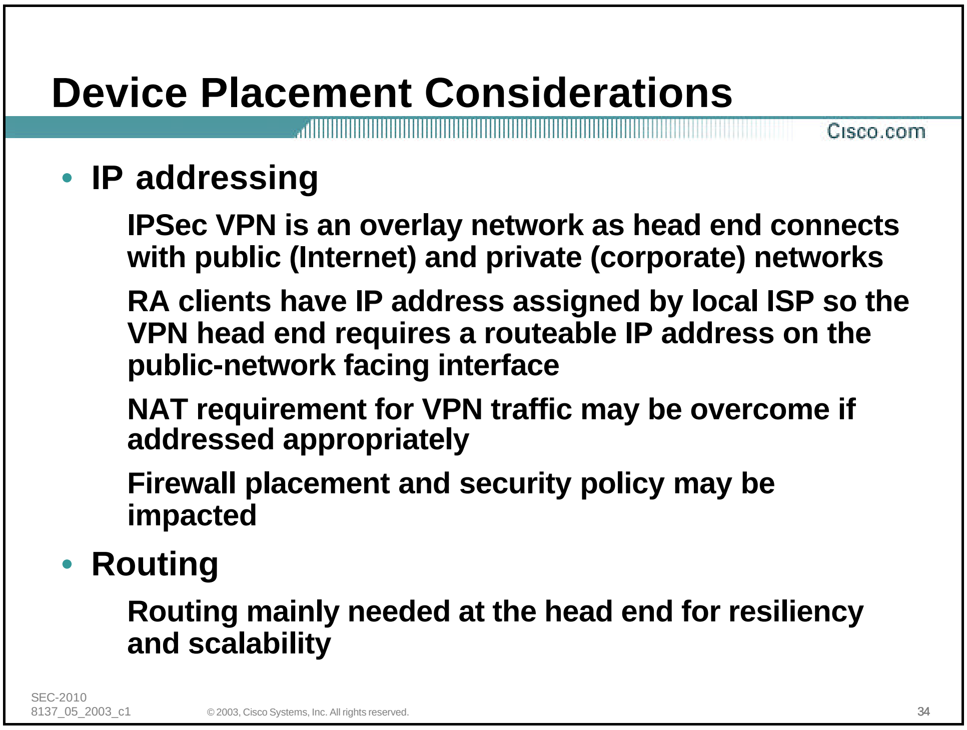
	Resiliency	Scalability	Management	Identity	Client OS Support	Consolidated Solution
VPN Client SW to VPN Appliance	Above Average	Superior	Superior	Superior	Superior	Superior
VPN Client HW to VPN Appliance	Superior	Superior	Superior	Superior	Superior	Superior
VPN Client to PIX FW	Below Average	Average	Below Average	Superior	Above Average	Above Average
VPN Client with Cisco IOS VPN Router	Average	Average	Below Average	Above Average	N/A to HW client AAvg for SW client	Average
VPN Client to VPN Module	Superior	Superior	Above Average	Superior	Above Average	Superior



Other Topics for Consideration

Cisco.com

- IP addressing
- Routing
- Security
- QoS
- Migration
- Best products for function



Device Placement Considerations

Cisco.com

- IP addressing

  IPSec VPN is an overlay network as head end connects with public (Internet) and private (corporate) networks

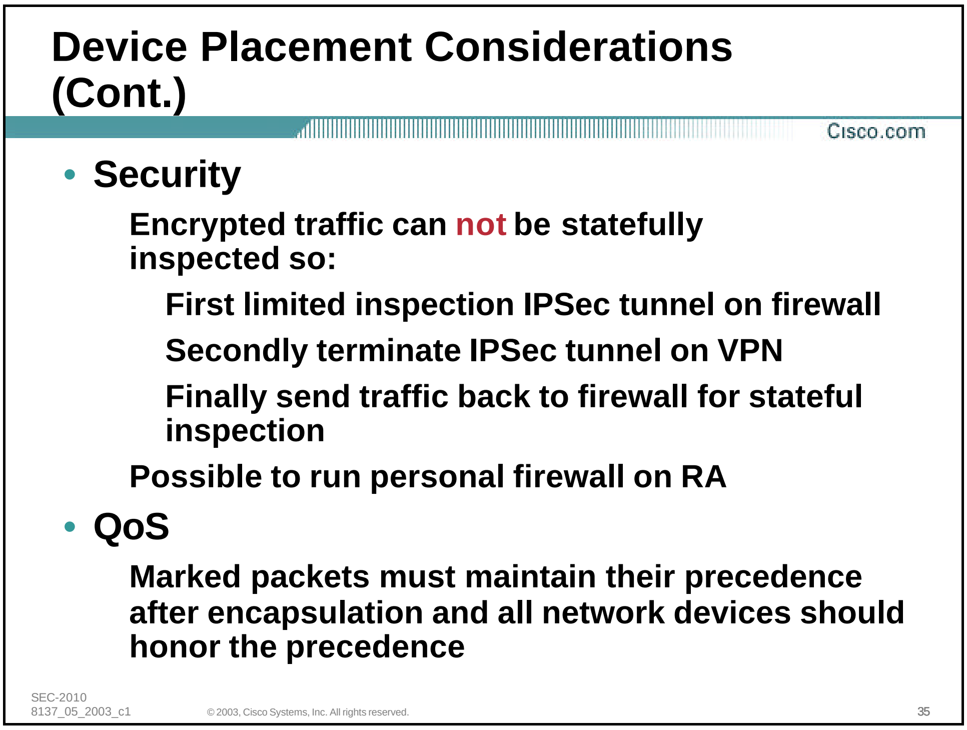
  RA clients have IP address assigned by local ISP so the VPN head end requires a routeable IP address on the public-network facing interface

  NAT requirement for VPN traffic may be overcome if addressed appropriately

  Firewall placement and security policy may be impacted

- Routing

  Routing mainly needed at the head end for resiliency and scalability



Device Placement Considerations (Cont.)

Cisco.com

- Security

  Encrypted traffic can not be statefully inspected so:

  First limited inspection IPSec tunnel on firewall

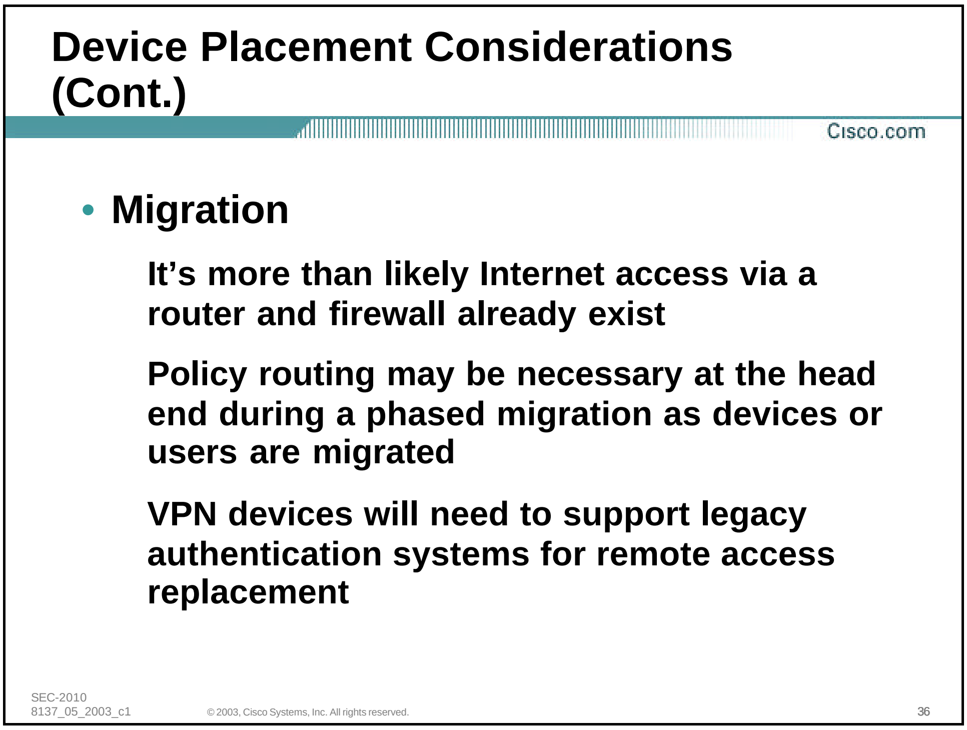
  Secondly terminate IPSec tunnel on VPN

  Finally send traffic back to firewall for stateful inspection

  Possible to run personal firewall on RA

- QoS

  Marked packets must maintain their precedence after encapsulation and all network devices should honor the precedence



Device Placement Considerations (Cont.)

Cisco.com

- Migration

  It’s more than likely Internet access via a router and firewall already exist

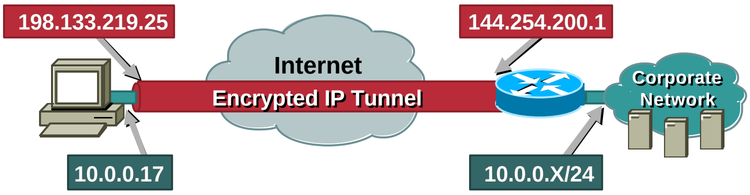
  Policy routing may be necessary at the head end during a phased migration as devices or users are migrated

  VPN devices will need to support legacy authentication systems for remote access replacement

Agenda

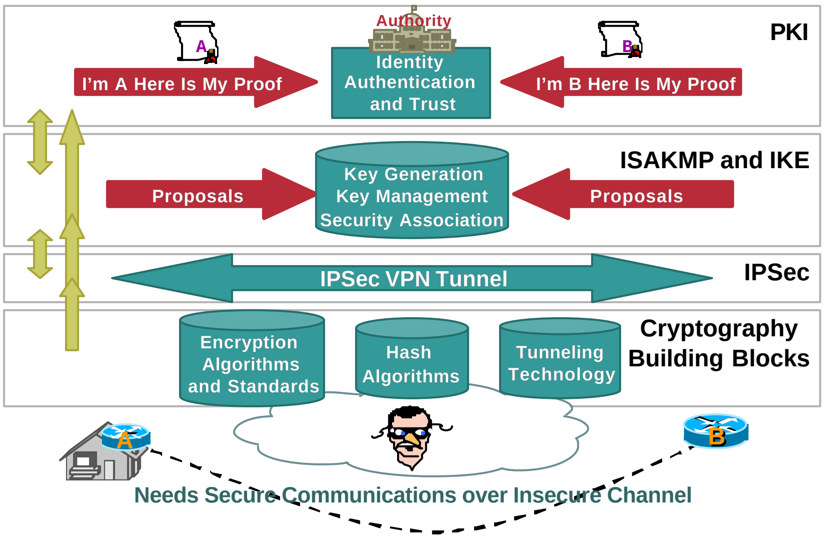
- What's and Why's of RA IPSec VPN
- Design Considerations
- Deployment Scenarios
- Case Study

Secure Communications—IPSec VPN



- Encapsulate original (green) packet in a new packet (red), traverse shared backbone and require:
  - Per packet encryption and authentication
  - Private address assignment
  - Private services assignment (DNS, WINS, domain,…)
  - End point authentication (user, device)
  - NAT traversal support

Secure Communications— IPSec VPN (Cont.)



Authority

Identity Authentication and Trust

I'm A Here Is My Proof

I'm B Here Is My Proof

PKI

Key Generation Key Management Security Association

Proposals

Proposals

ISAKMP and IKE

IPSec VPN Tunnel

IPSec

Encryption Algorithms and Standards

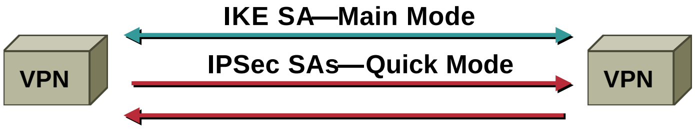
Hash Algorithms

Tunneling Technology

Cryptography Building Blocks

Needs Secure Communications over Insecure Channel

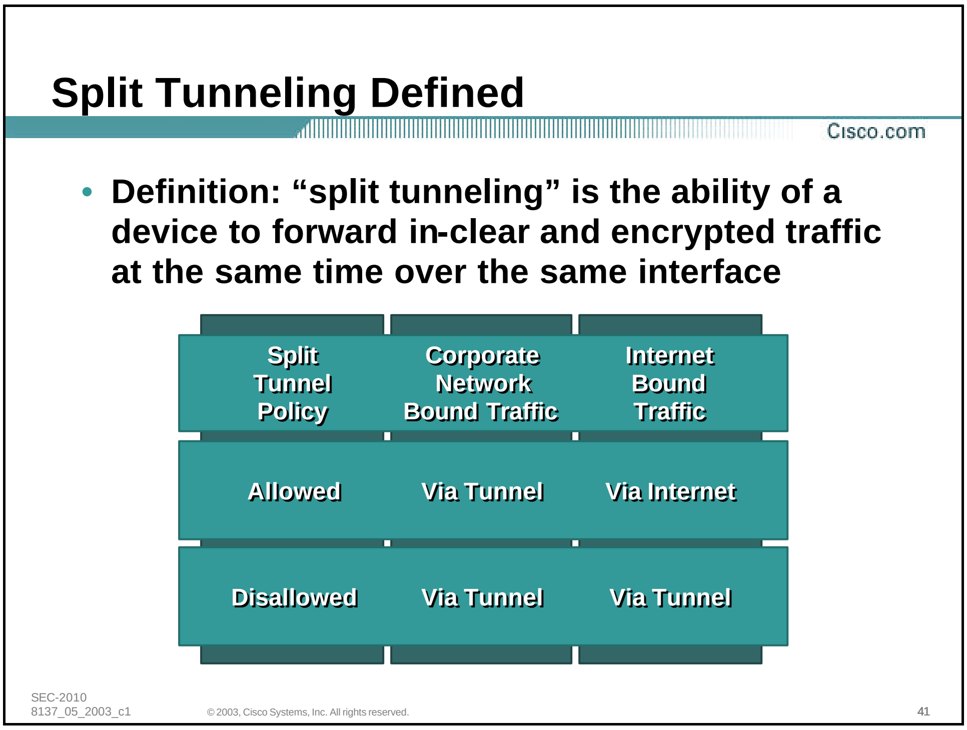
Review: Security Associations



IKE SA—Main Mode

IPSec SAs—Quick Mode

- Agreement between two entities on a security policy, including:
  - Encryption algorithm
  - Authentication algorithm
  - Shared session keys
  - SA lifetime
  - Data flows to protect (IPSec SAs only)
- Types of security associations
  - Bi-directional for management (IKE SA)
  - Unidirectional for data (IPSec SA)
  - 1 "Tunnel" = 1 IKE SA + 2 IPSec SAs

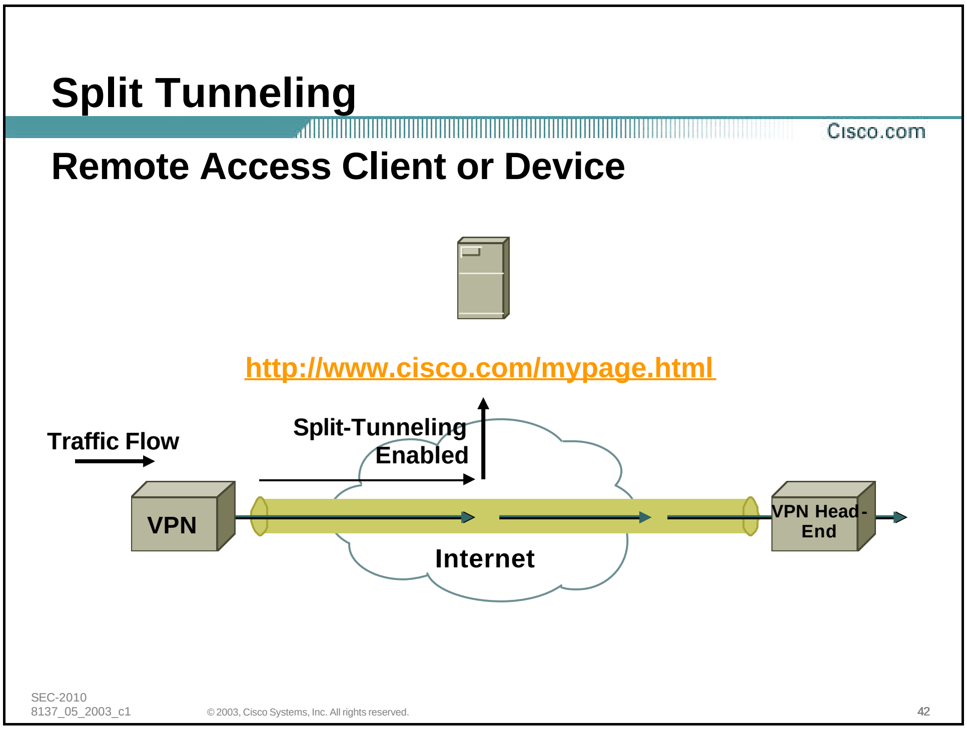


Split Tunneling Defined

Cisco.com

- Definition: “split tunneling” is the ability of a device to forward in-clear and encrypted traffic at the same time over the same interface

Split Tunnel Policy	Corporate Network Bound Traffic	Internet Bound Traffic
Allowed	Via Tunnel	Via Internet
Disallowed	Via Tunnel	Via Tunnel



Split Tunneling

Cisco.com

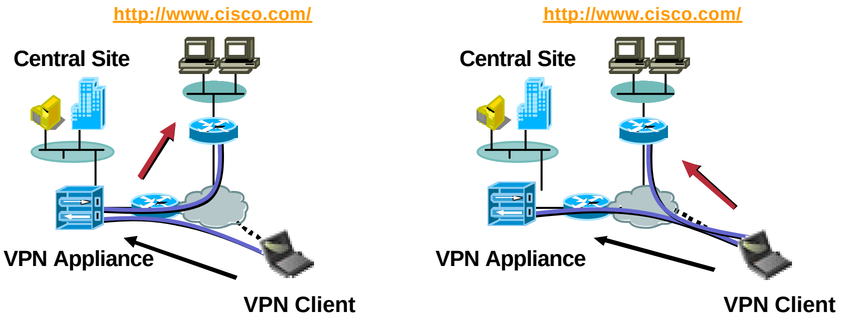
Remote Access Client or Device

Split Tunneling

Cisco.com

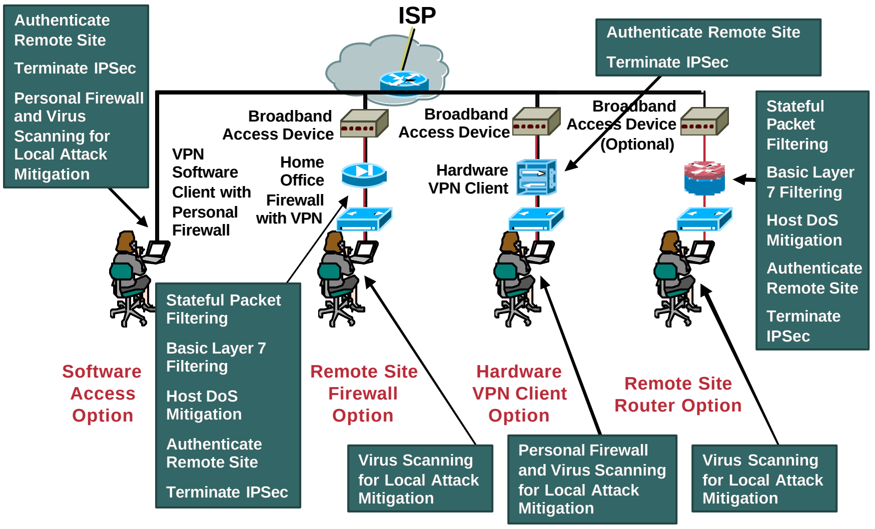
Remote Access Client or Device

Without Split Tunneling | **With Split Tunneling**



SAFE Remote User Network Options

Cisco.com


ISP
Broadband Access Device
Broadband Access Device
Broadband Access Device (Optional)
VPN Software Client with Personal Firewall
Home Office Firewall with VPN
Hardware VPN Client
Software Access Option
Remote Site Firewall Option
Hardware VPN Client Option
Remote Site Router Option

Authenticate Remote Site

Terminate IPSec

Personal Firewall and Virus Scanning for Local Attack Mitigation

Stateful Packet Filtering

Basic Layer 7 Filtering

Host DoS Mitigation

Authenticate Remote Site

Terminate IPSec

Virus Scanning for Local Attack Mitigation

Personal Firewall and Virus Scanning for Local Attack Mitigation

Authenticate Remote Site

Terminate IPSec

Stateful Packet Filtering

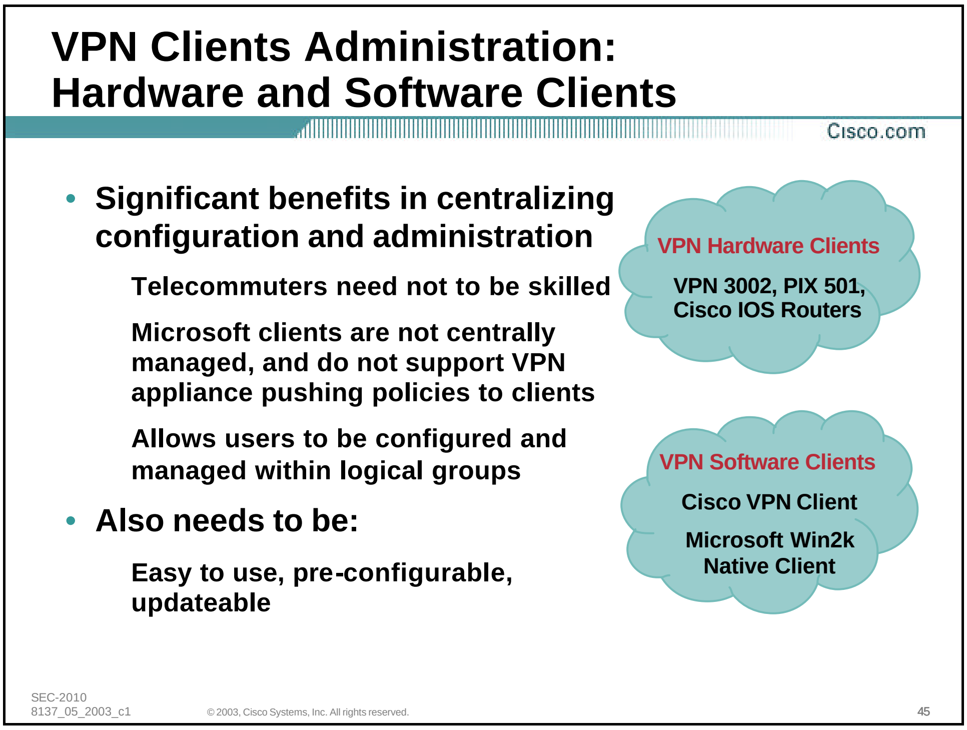
Basic Layer 7 Filtering

Host DoS Mitigation

Authenticate Remote Site

Terminate IPSec

Virus Scanning for Local Attack Mitigation



VPN Clients Administration: Hardware and Software Clients

Cisco.com

- Significant benefits in centralizing configuration and administration

  Telecommuters need not to be skilled

  Microsoft clients are not centrally managed, and do not support VPN appliance pushing policies to clients

  Allows users to be configured and managed within logical groups

- Also needs to be:

  Easy to use, pre-configurable, updateable

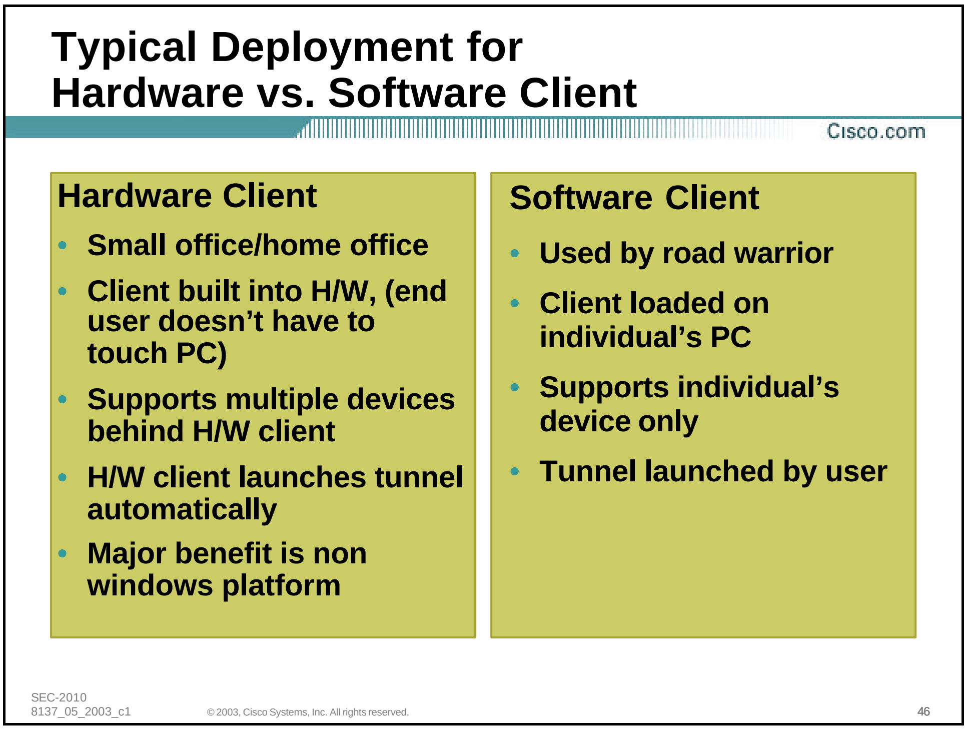
VPN Hardware Clients

VPN 3002, PIX 501, Cisco IOS Routers

VPN Software Clients

Cisco VPN Client

Microsoft Win2k Native Client



Typical Deployment for Hardware vs. Software Client

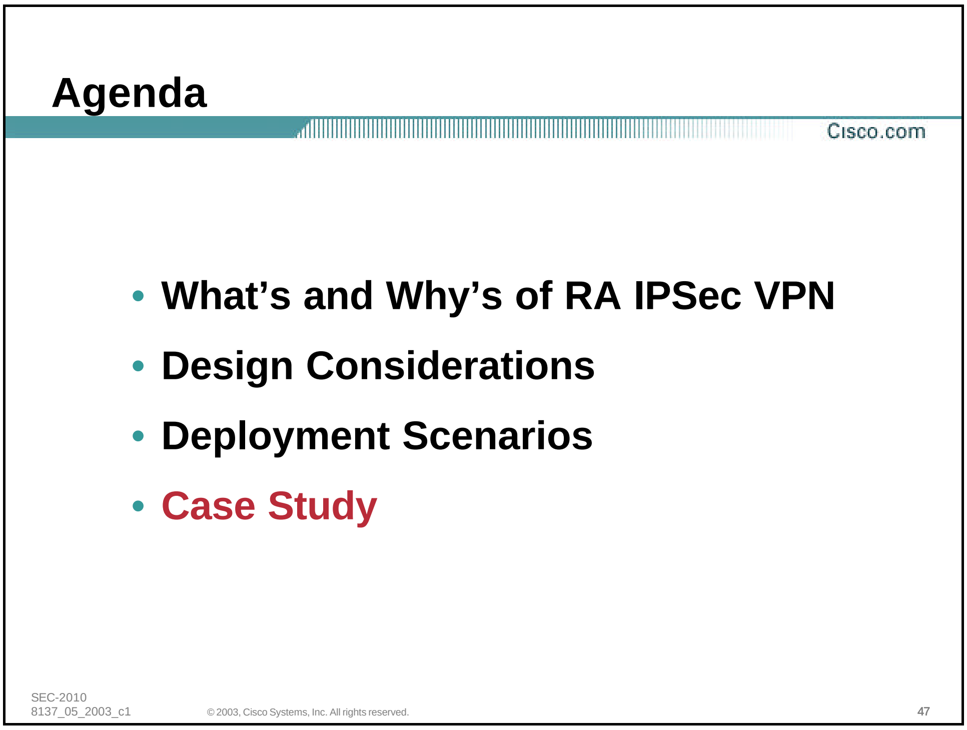
Cisco.com

Hardware Client

- Small office/home office
- Client built into H/W, (end user doesn't have to touch PC)
- Supports multiple devices behind H/W client
- H/W client launches tunnel automatically
- Major benefit is non windows platform

Software Client

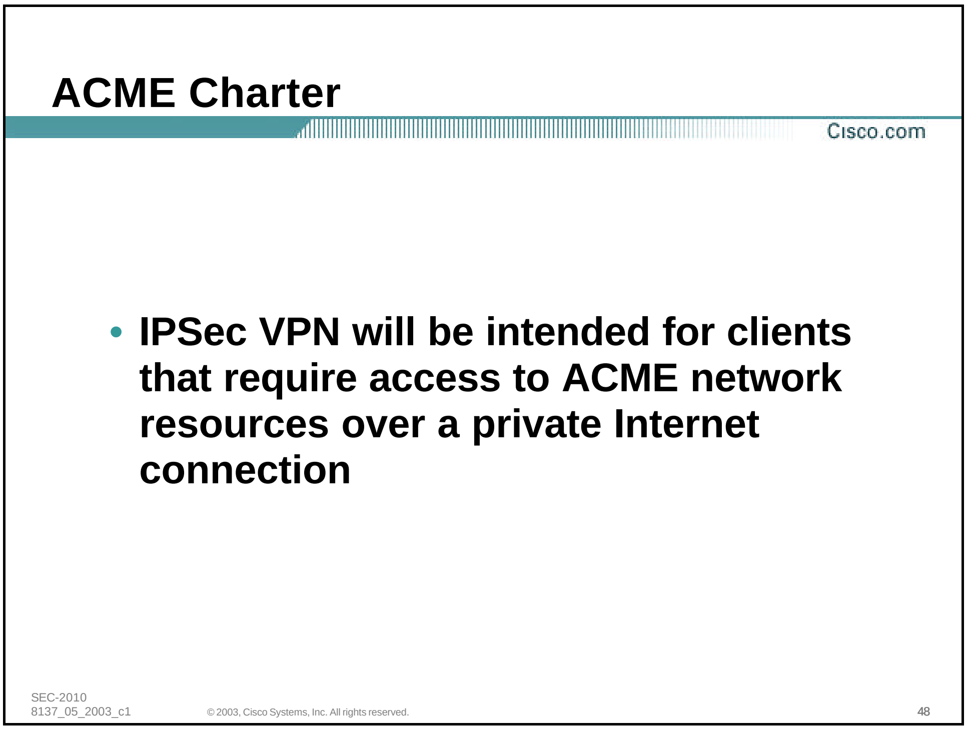
- Used by road warrior
- Client loaded on individual's PC
- Supports individual's device only
- Tunnel launched by user



Agenda

Cisco.com

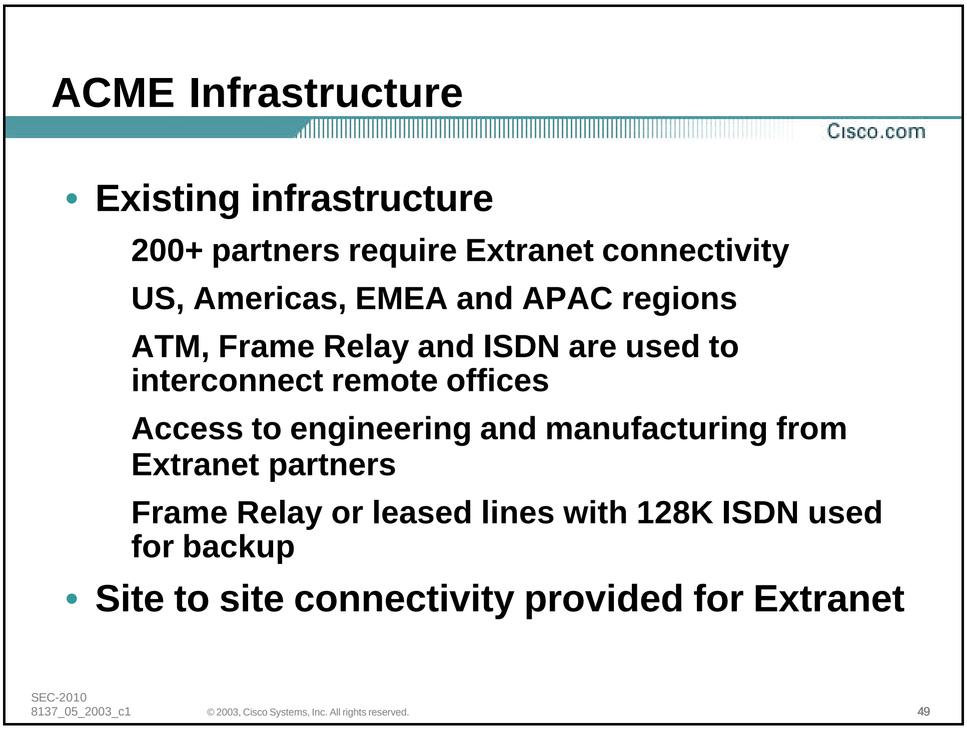
- What’s and Why’s of RA IPSec VPN
- Design Considerations
- Deployment Scenarios
- Case Study



ACME Charter

Cisco.com

- IPSec VPN will be intended for clients that require access to ACME network resources over a private Internet connection



ACME Infrastructure

Cisco.com

- Existing infrastructure

  200+ partners require Extranet connectivity

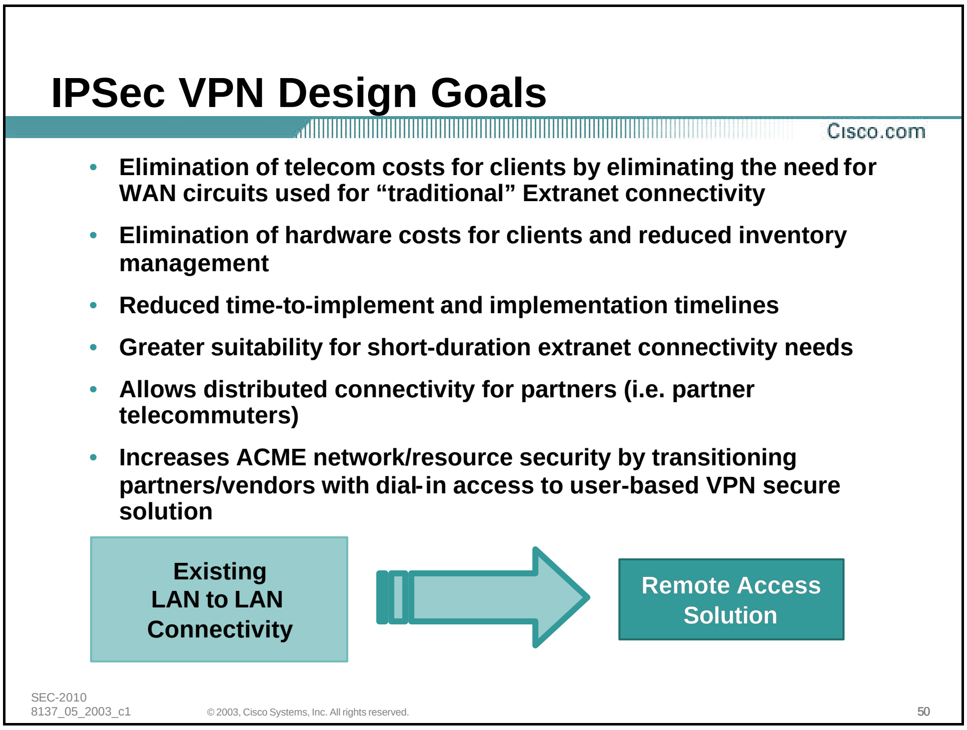
  US, Americas, EMEA and APAC regions

  ATM, Frame Relay and ISDN are used to interconnect remote offices

  Access to engineering and manufacturing from Extranet partners

  Frame Relay or leased lines with 128K ISDN used for backup

- Site to site connectivity provided for Extranet



IPSec VPN Design Goals

Cisco.com

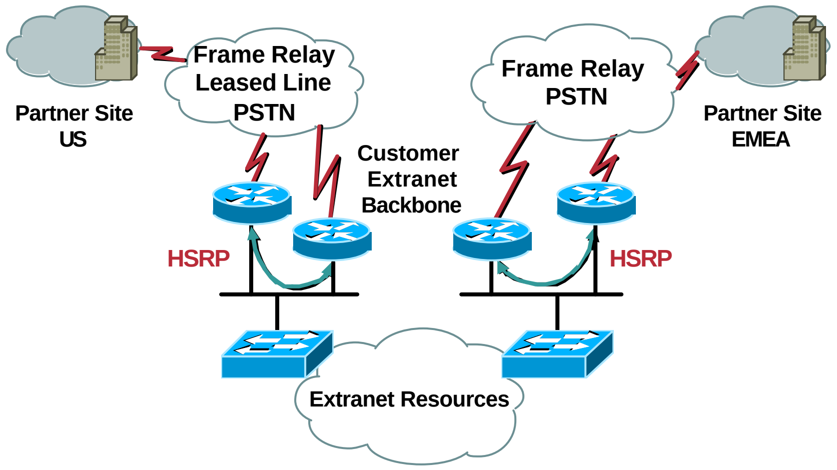
- Elimination of telecom costs for clients by eliminating the need for WAN circuits used for "traditional" Extranet connectivity
- Elimination of hardware costs for clients and reduced inventory management
- Reduced time-to-implement and implementation timelines
- Greater suitability for short-duration extranet connectivity needs
- Allows distributed connectivity for partners (i.e. partner telecommuters)
- Increases ACME network/resource security by transitioning partners/vendors with dial-in access to user-based VPN secure solution

Existing LAN to LAN Connectivity

Remote Access Solution

ACME Topology

Cisco.com



ACME Profile: Application and Traffic

Cisco.com

- Frame Relay network

  Head-end: ~45 Mbps throughput

  Remote sites: 56/64K–T1, ~1 Mbps throughput

  Intranet services: database, HTTP, FTP, mail, etc.

- Leased access

  T1/E1 or J1 leased lines and edge/ISP router

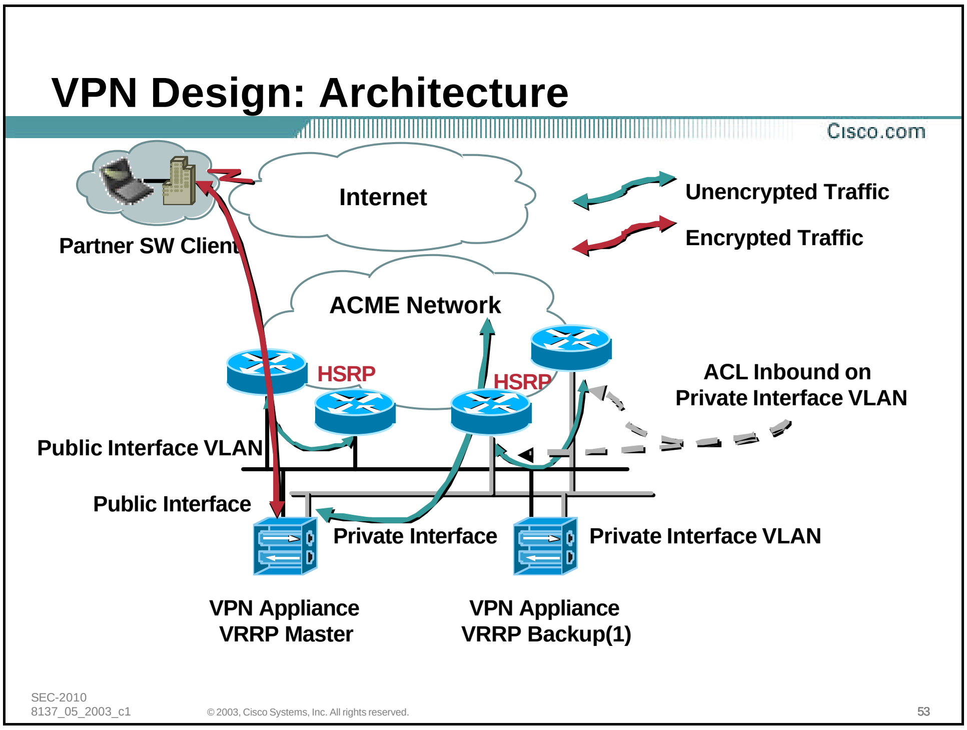
  Head-end: ~15 Mbps throughput

  HTTP, FTP and other traffic

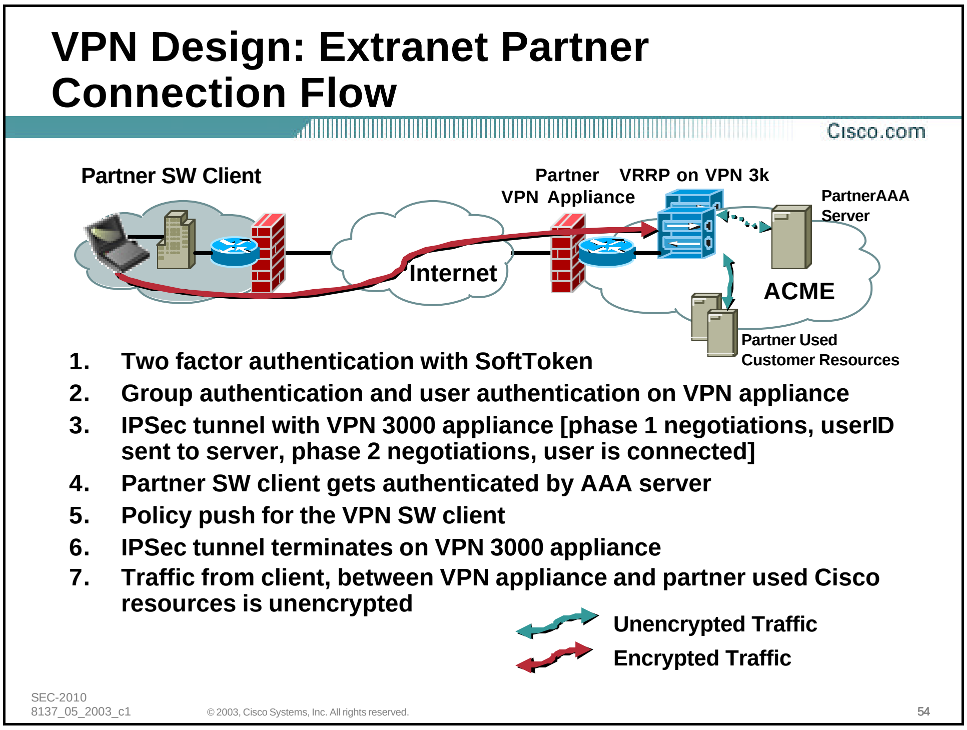
- PSTN network

  Head-end: access server—PRI lines

  Remote sites: 128K ISDN

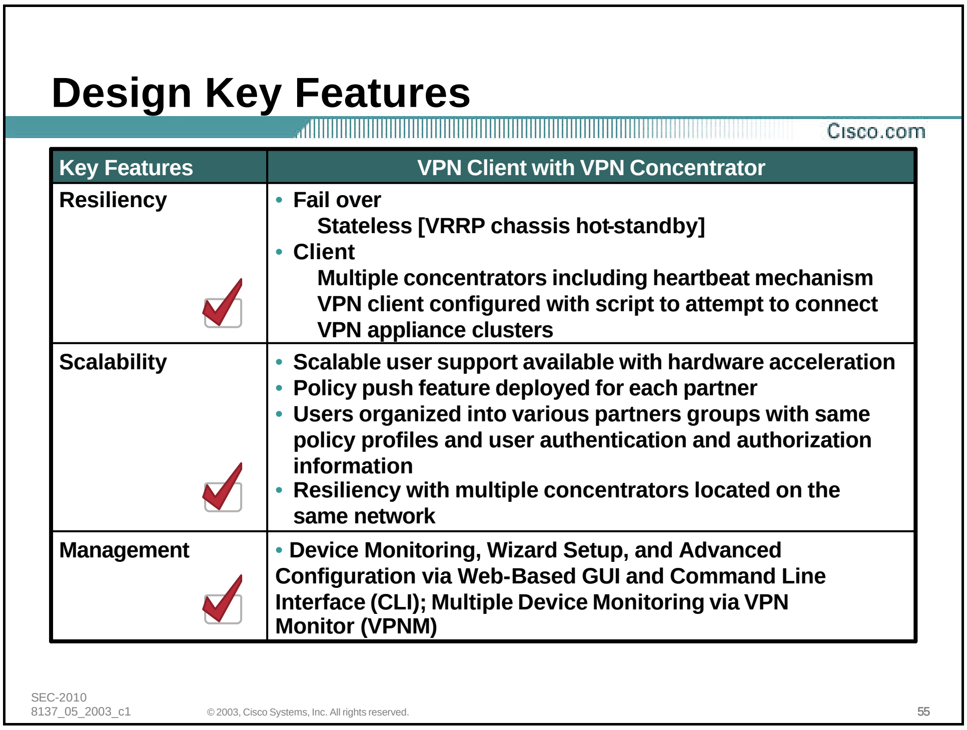


VPN Design: Architecture



VPN Design: Extranet Partner Connection Flow

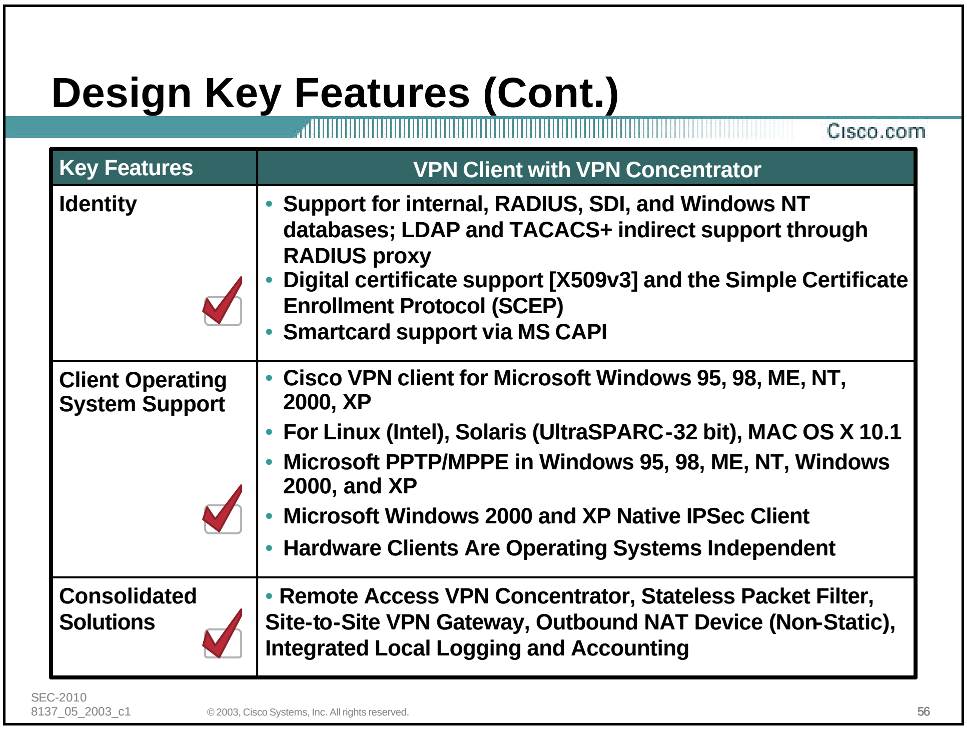
1. Two factor authentication with SoftToken
2. Group authentication and user authentication on VPN appliance
3. IPSec tunnel with VPN 3000 appliance [phase 1 negotiations, userID sent to server, phase 2 negotiations, user is connected]
4. Partner SW client gets authenticated by AAA server
5. Policy push for the VPN SW client
6. IPSec tunnel terminates on VPN 3000 appliance
7. Traffic from client, between VPN appliance and partner used Cisco resources is unencrypted



Design Key Features

Cisco.com

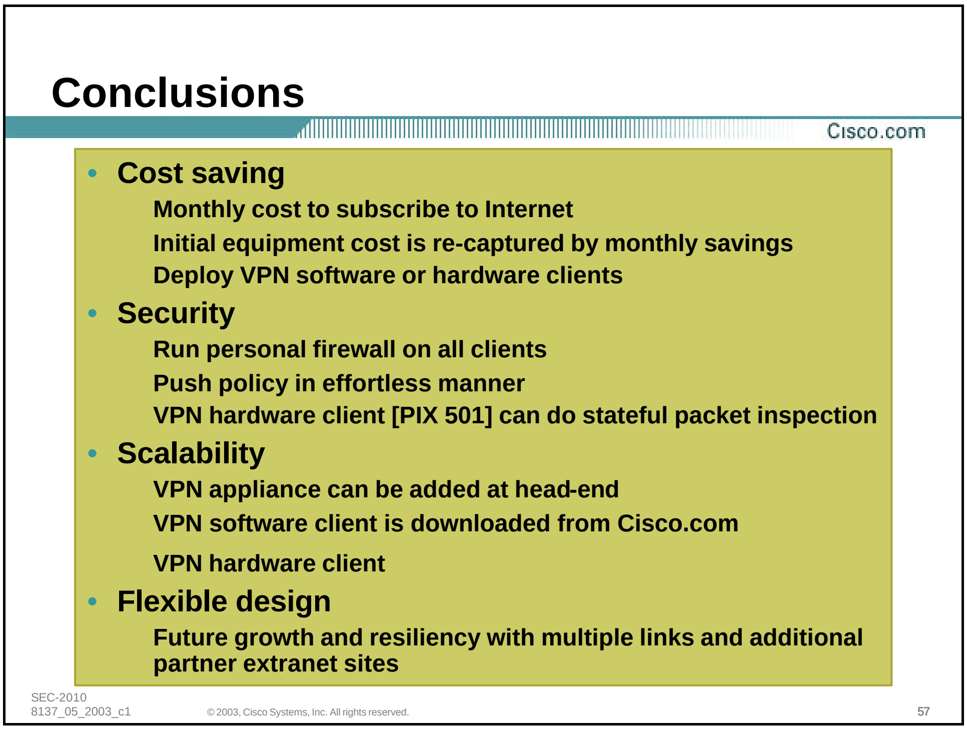
Key Features	VPN Client with VPN Concentrator
Resiliency ✓	• Fail over Stateless [VRRP chassis hot-standby] • Client Multiple concentrators including heartbeat mechanism VPN client configured with script to attempt to connect VPN appliance clusters
Scalability ✓	• Scalable user support available with hardware acceleration • Policy push feature deployed for each partner • Users organized into various partners groups with same policy profiles and user authentication and authorization information • Resiliency with multiple concentrators located on the same network
Management ✓	• Device Monitoring, Wizard Setup, and Advanced Configuration via Web-Based GUI and Command Line Interface (CLI); Multiple Device Monitoring via VPN Monitor (VPNM)



Design Key Features (Cont.)

Cisco.com

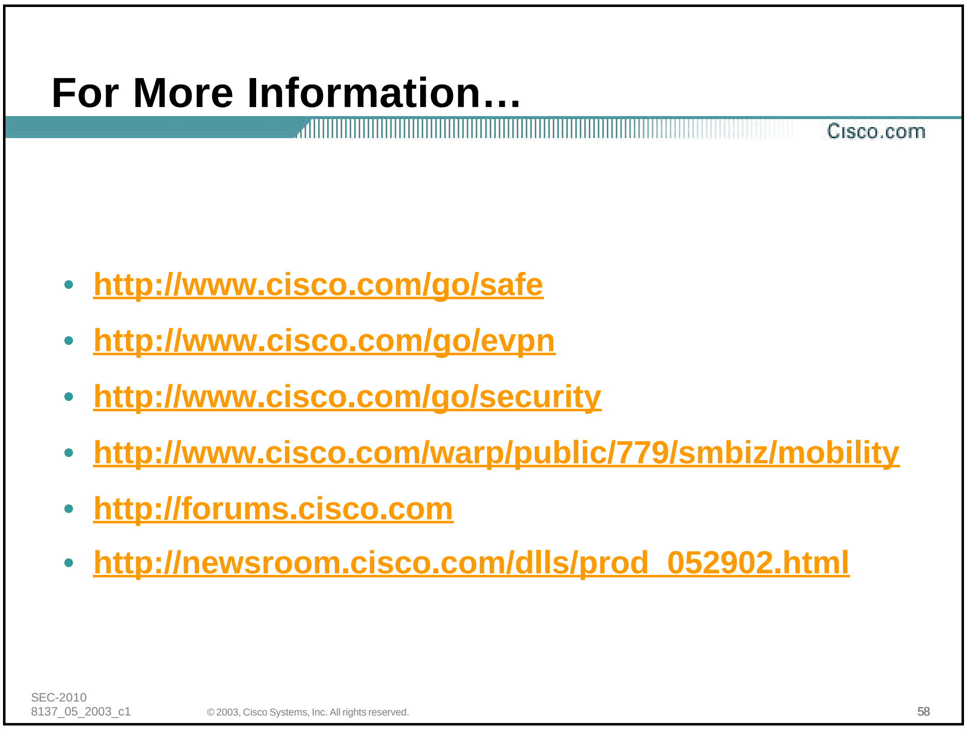
Key Features	VPN Client with VPN Concentrator
Identity ✓	• Support for internal, RADIUS, SDI, and Windows NT databases; LDAP and TACACS+ indirect support through RADIUS proxy • Digital certificate support [X509v3] and the Simple Certificate Enrollment Protocol (SCEP) • Smartcard support via MS CAPI
Client Operating System Support ✓	• Cisco VPN client for Microsoft Windows 95, 98, ME, NT, 2000, XP • For Linux (Intel), Solaris (UltraSPARC-32 bit), MAC OS X 10.1 • Microsoft PPTP/MPPE in Windows 95, 98, ME, NT, Windows 2000, and XP • Microsoft Windows 2000 and XP Native IPSec Client • Hardware Clients Are Operating Systems Independent
Consolidated Solutions ✓	• Remote Access VPN Concentrator, Stateless Packet Filter, Site-to-Site VPN Gateway, Outbound NAT Device (Non-Static), Integrated Local Logging and Accounting



Conclusions

Cisco.com

- Cost saving
  - Monthly cost to subscribe to Internet
  - Initial equipment cost is re-captured by monthly savings
  - Deploy VPN software or hardware clients
- Security
  - Run personal firewall on all clients
  - Push policy in effortless manner
  - VPN hardware client [PIX 501] can do stateful packet inspection
- Scalability
  - VPN appliance can be added at head-end
  - VPN software client is downloaded from Cisco.com
  - VPN hardware client
- Flexible design
  - Future growth and resiliency with multiple links and additional partner extranet sites



For More Information…

Cisco.com

- http://www.cisco.com/go/safe
- http://www.cisco.com/go/evpn
- http://www.cisco.com/go/security
- http://www.cisco.com/warp/public/779/smbiz/mobility
- http://forums.cisco.com
- http://newsroom.cisco.com/dlls/prod_052902.html

Cisco Systems