Redes Privadas Virtuales (VPN) y Soluciones

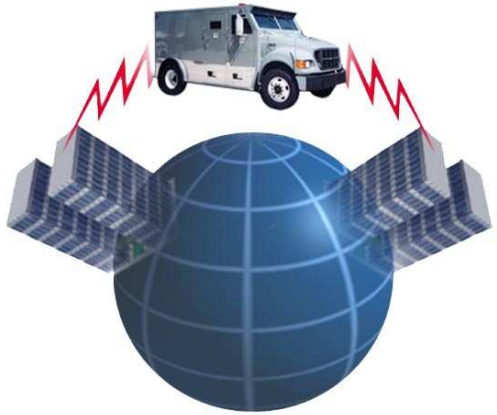
Pablo Mollinger

Systems Engineer

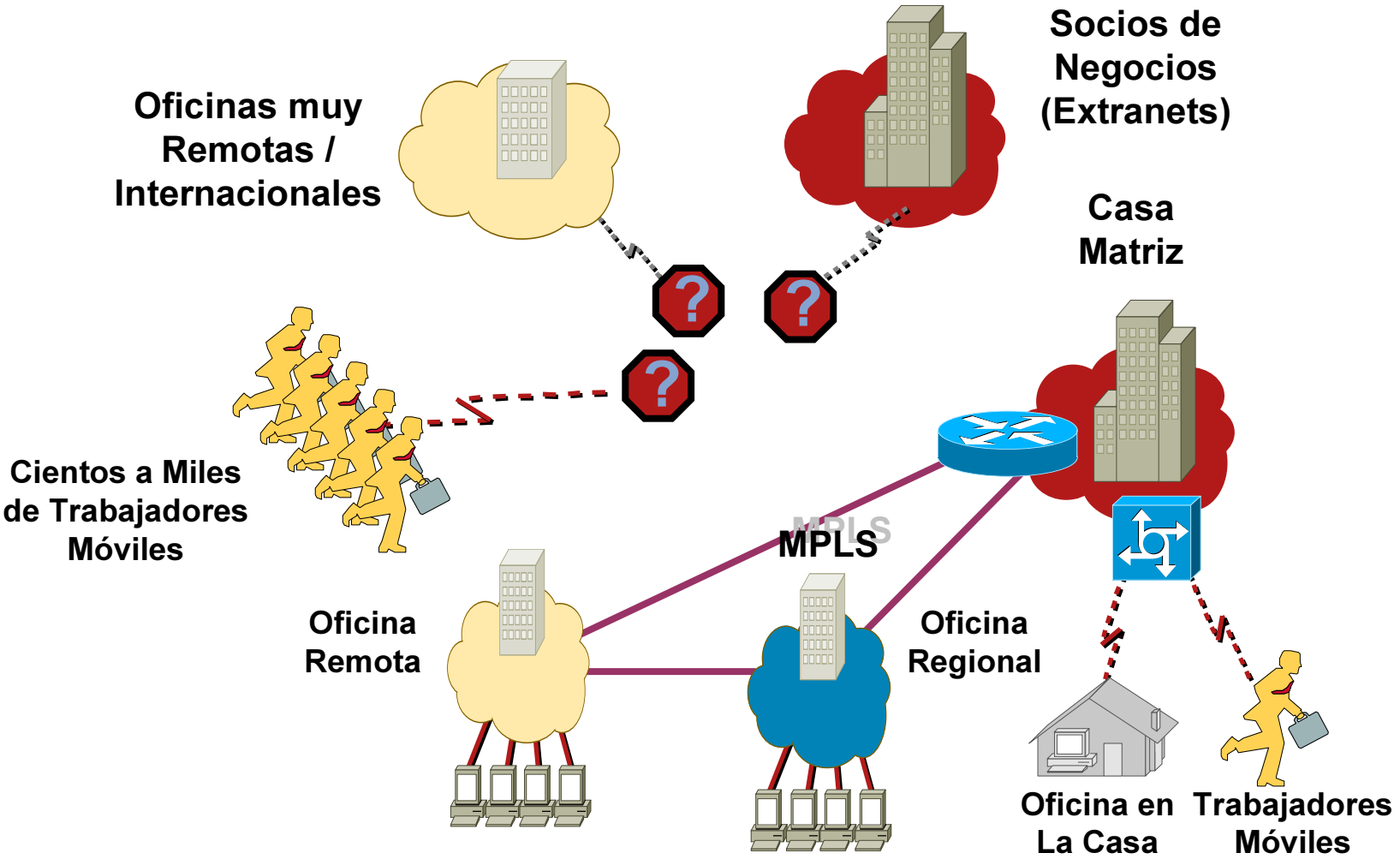
Cisco Chile

Agenda

- Introducción
- Site-to-Site VPNs
- VPNs Remotas



Desafios de Conectividad



Beneficios de las VPNs

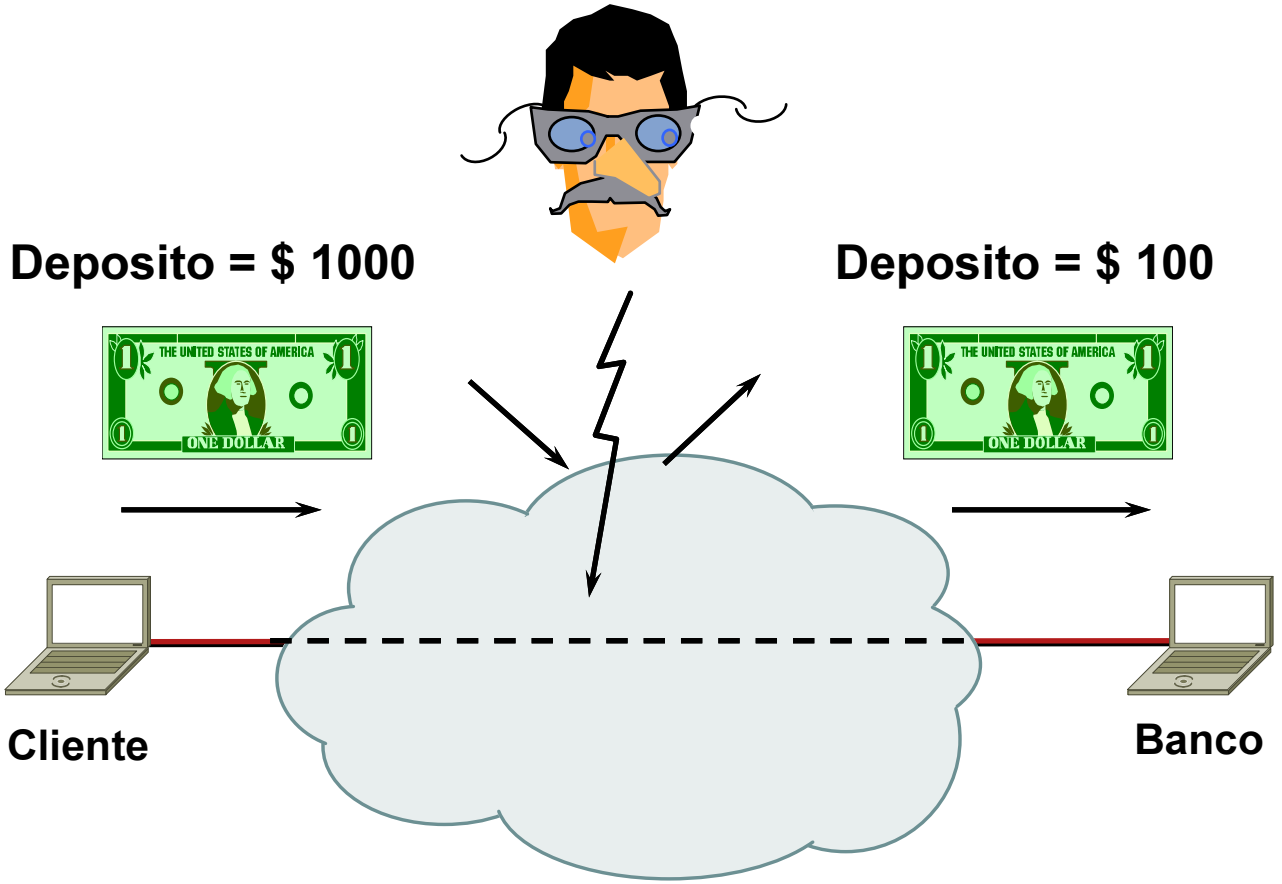
Flexibilidad	Menores Costos	Escalabilidad
Extender la red a usuarios remotos Habilitar el acceso a la red a Socios de Negocios Capacidad de configurar y reestructurar redes rapidamente	Ahorros en los costos de Ancho de Banda y conexiones conmutadas Delivers cost effective remote site bandwidth for new applications Reduced WAN and dial infrastructure expenditures	Potenciar y extender la WAN clásica a más usuarios remotos y externos Mejoras en la cobertura geográfica Operación simplificada de la WAN

Seguridad
Encriptación / Confidencialidad – Autenticación - Integridad

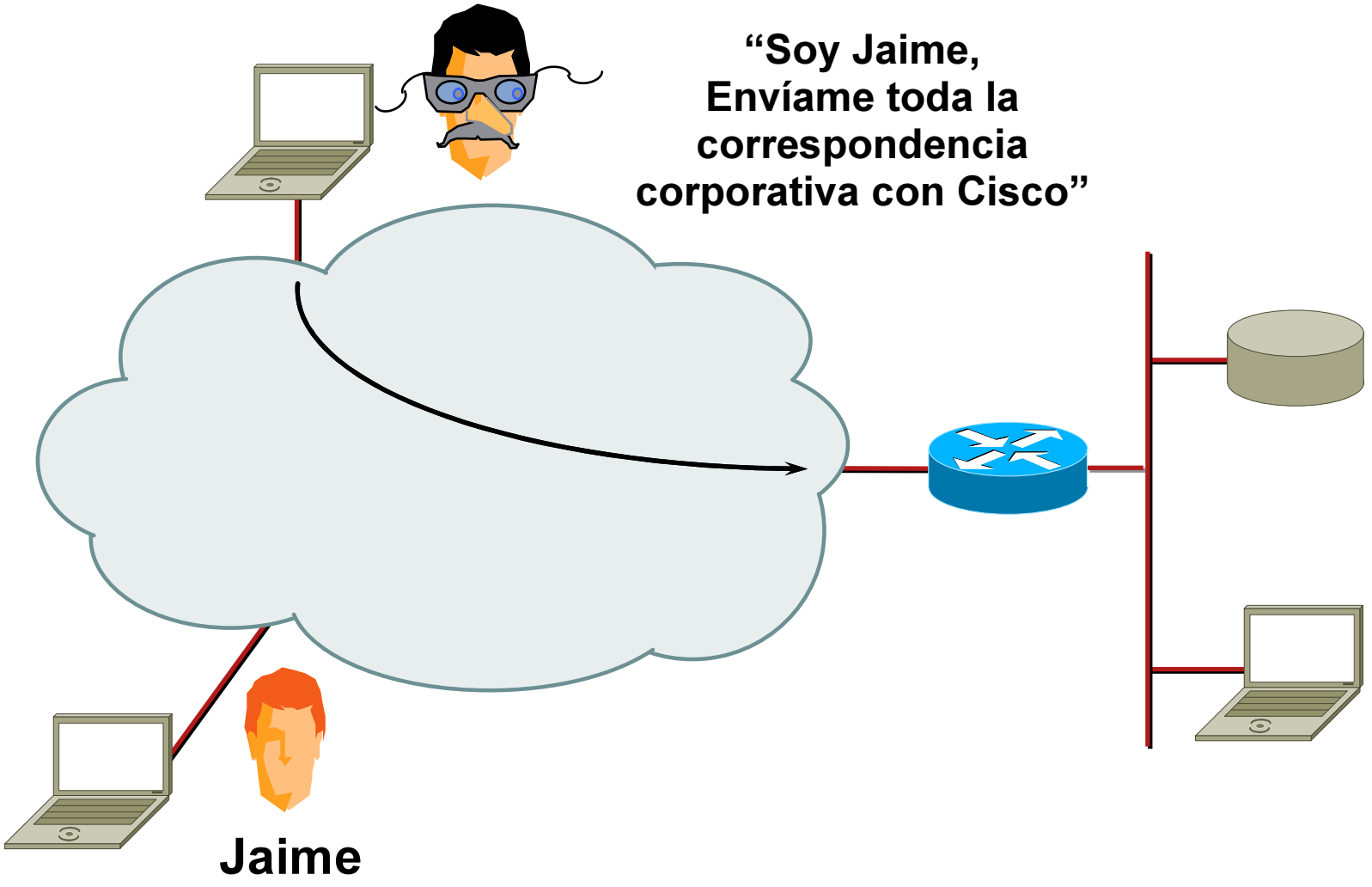
Tipos de VPNs y Aplicaciones

Tipo	Aplicación	Alternativa a	Beneficios
VPN de Acceso Remoto	**Conectividad Remota**	**Discado Análogo** **ISDN**	**Acceso Ubicuo** **Menor Costo**
Site-to-Site VPN	**Conectividad para Sucursales y Oficinas remotas**	**Líneas Dedicadas** **Frame Relay** **ATM**	**Extender la Conectividad** **Mayor Ancho de Banda** **Menor Costo**
Extranet VPN	**Conectividad Business to Business**	**Fax** **EDI** **Mail**	**Timing** **Menor Costo**

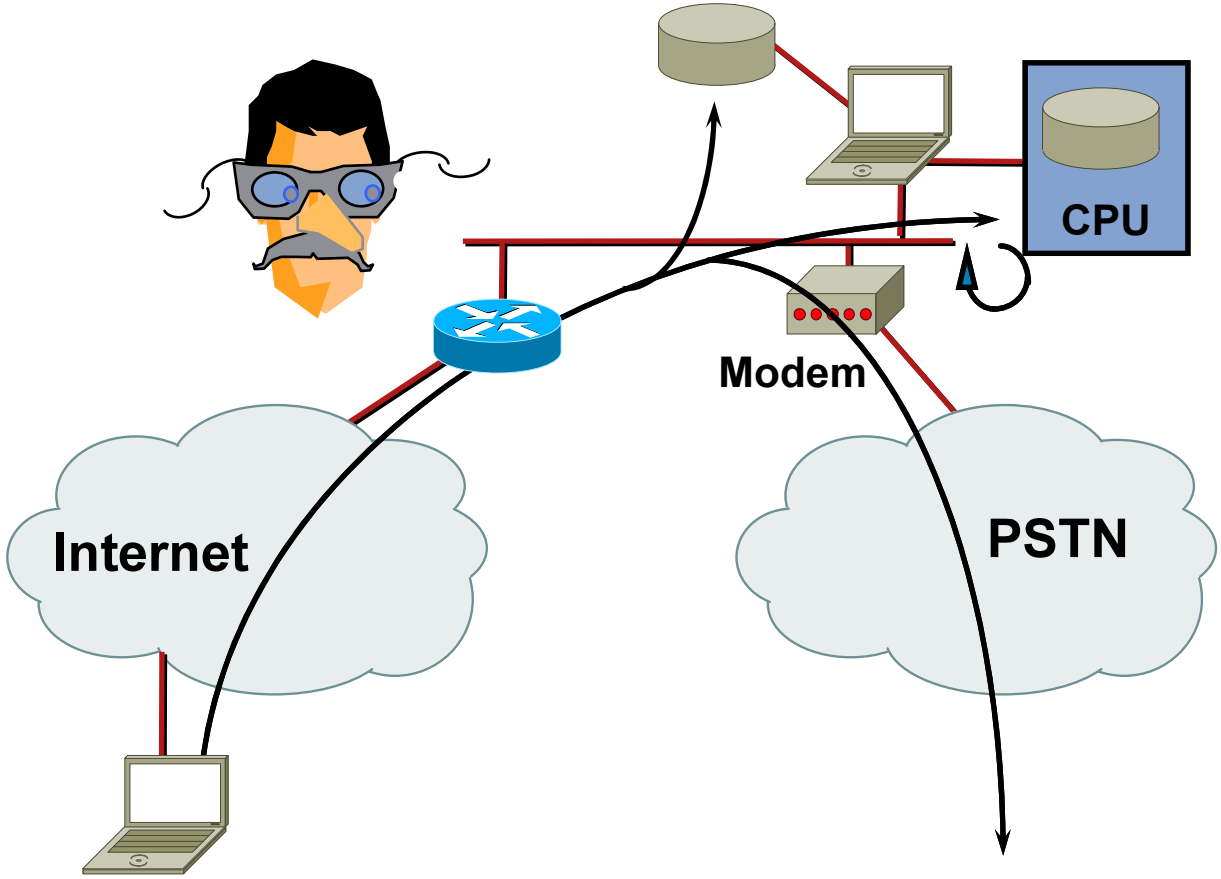
Integridad de Datos
Pérdida de la Integridad de Datos



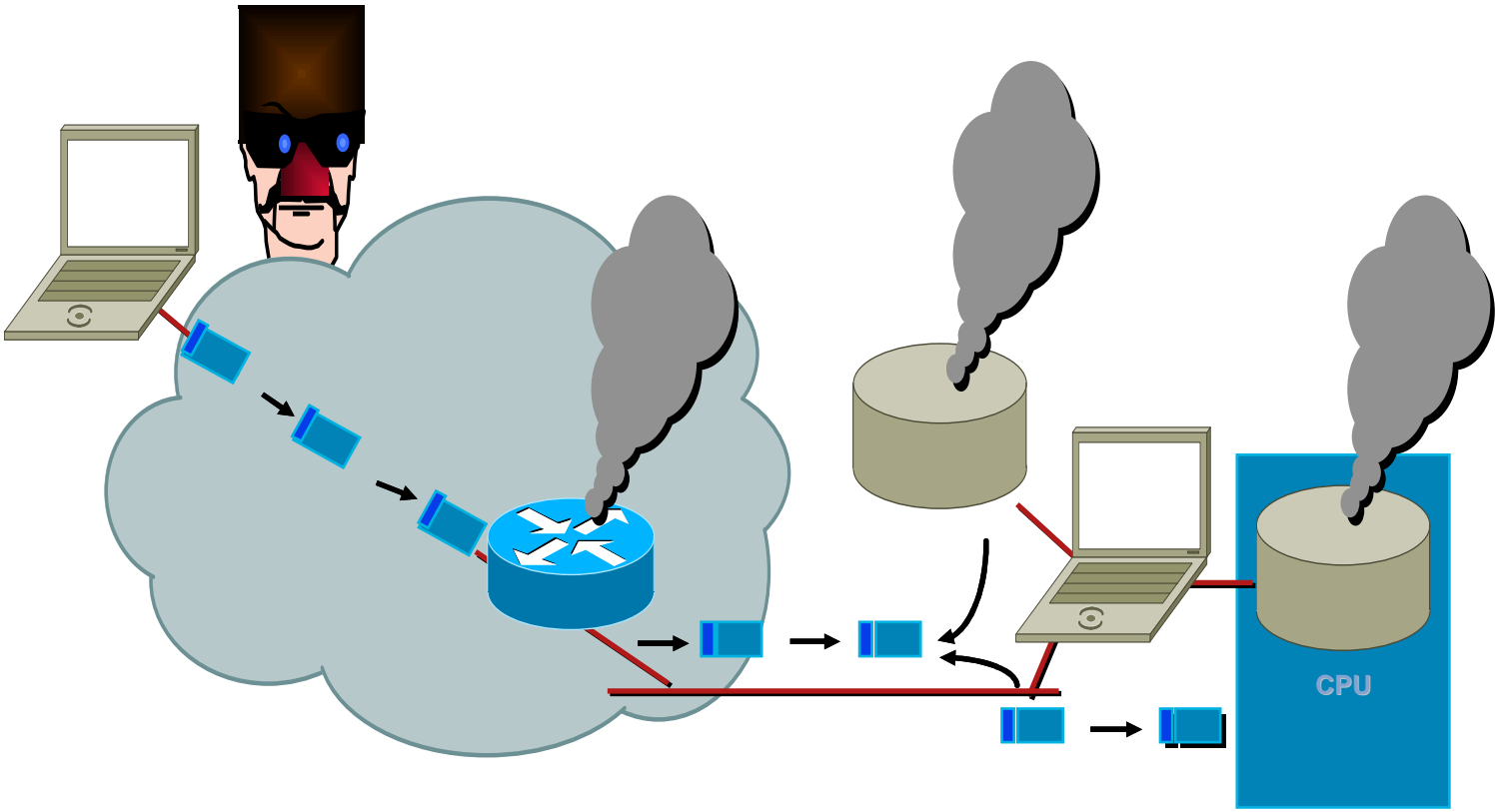
Impersonificación
Identity Spoofing



Confidencialidad
Pérdida de la Privacidad



Negación de Servicio



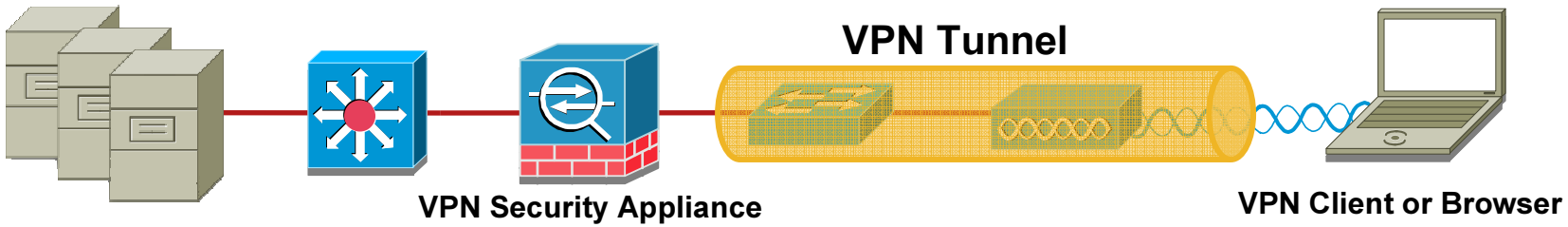
Cuáles son los desafíos que impone la protección de los datos ?

- Proteger la Confidencialidad de los datos en un Sistema de Comunicaciones “No confiable”
- Proteger la Integridad de los datos en un Sistema de Comunicaciones “No confiable”
- Asegurar la Identidad de usuarios y sistemas que intervienen en la comunicación
- Escalar desde redes pequeñas a redes muy grandes
- Desplegar un esquema público de Intercambio de Llaves de encriptación

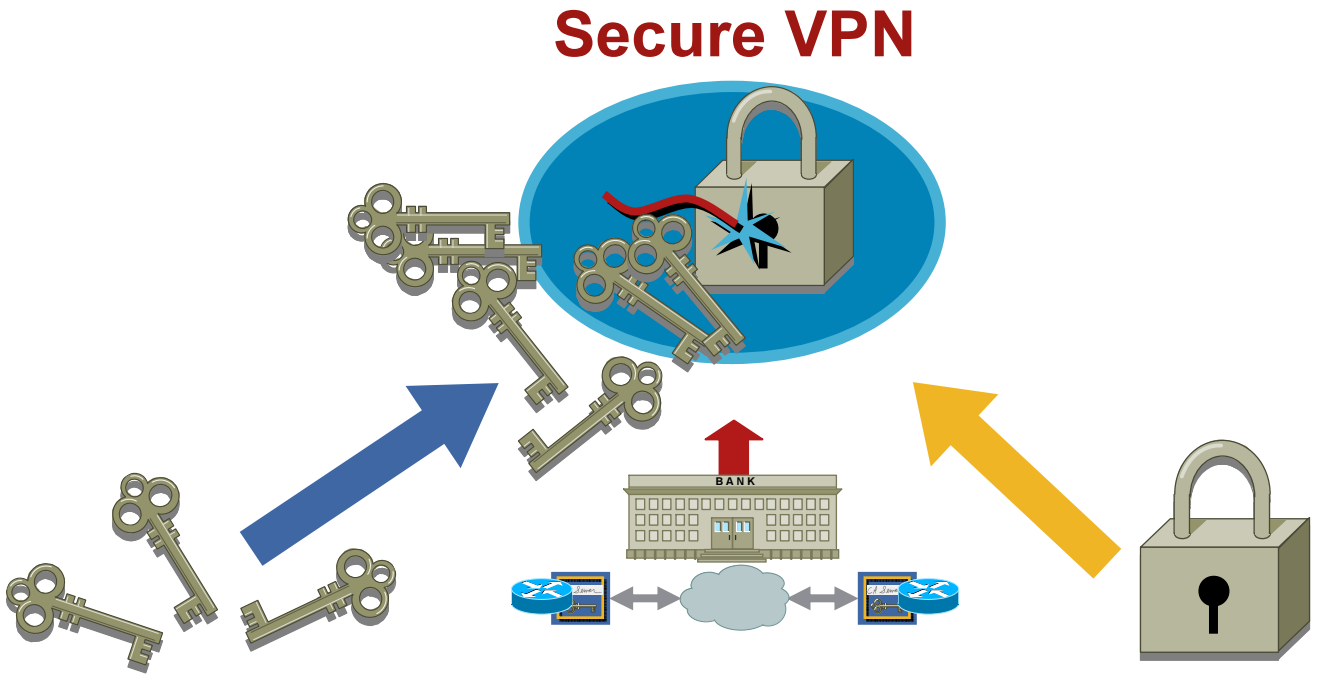
Virtual Private Network (VPN) Overview

IP security (IPsec) and Secure Socket Layer (SSL)

- Mechanism for secure communication over IP
  - Authenticity (unforged/trusted party)
  - Integrity (unaltered/tampered)
  - Confidentiality (unread)
- Remote Access (RA) VPN components
  - Client (mobile or fixed)
  - Termination device (high number of endpoints)

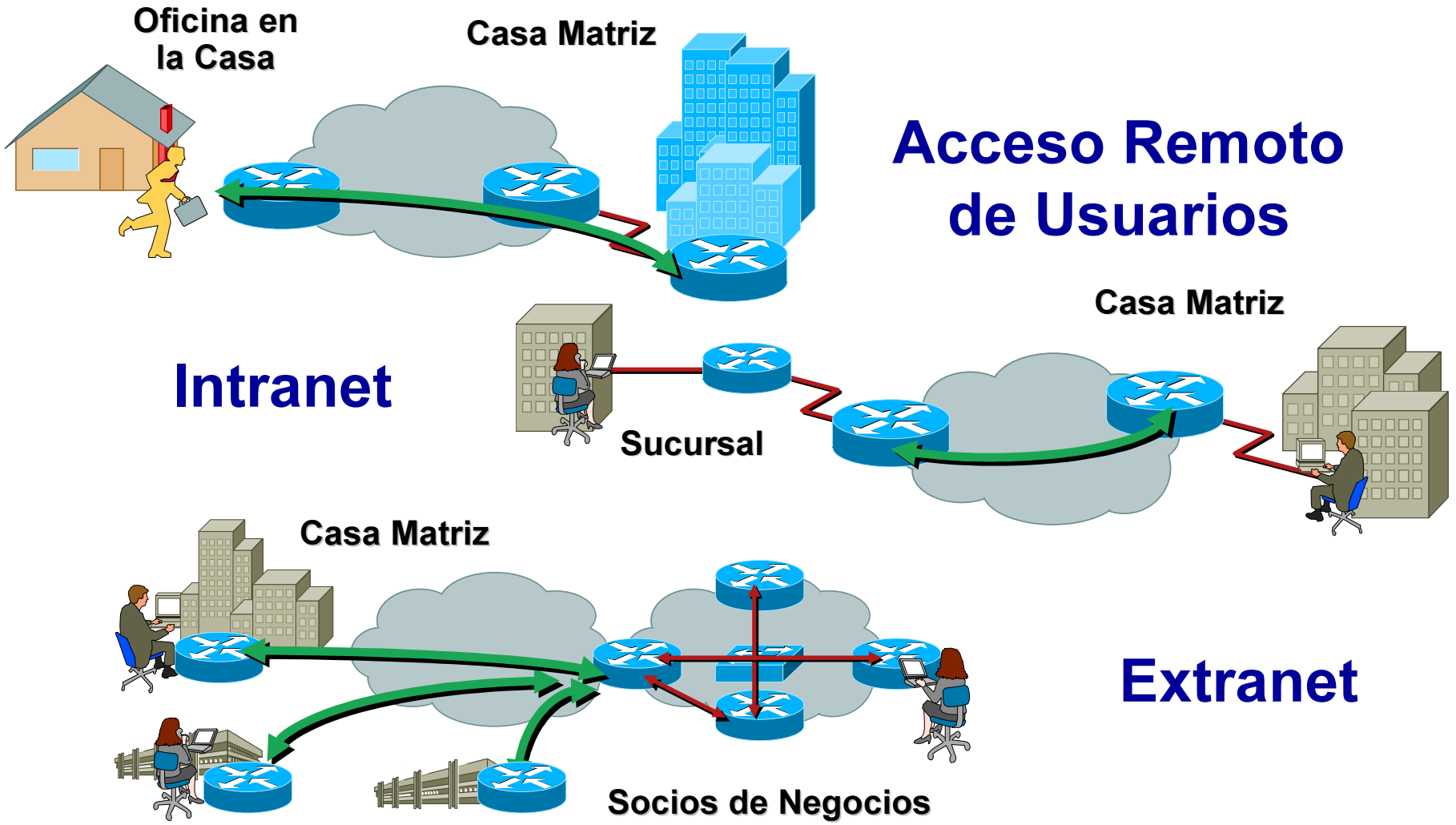


VPN – Seguras de Extemo a Extremo

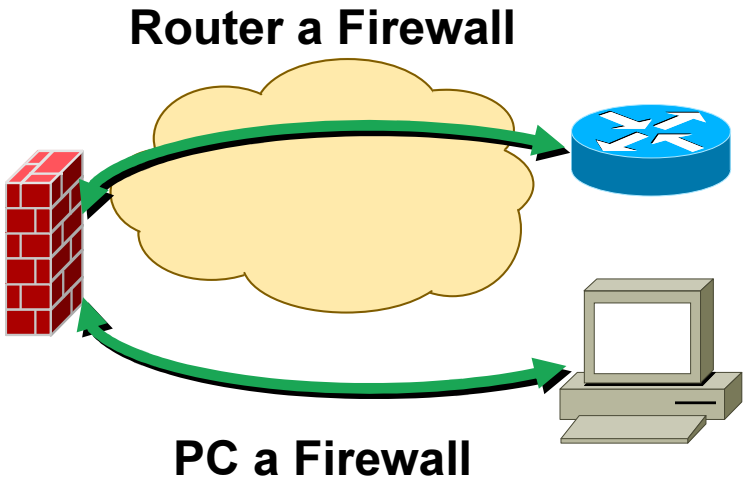


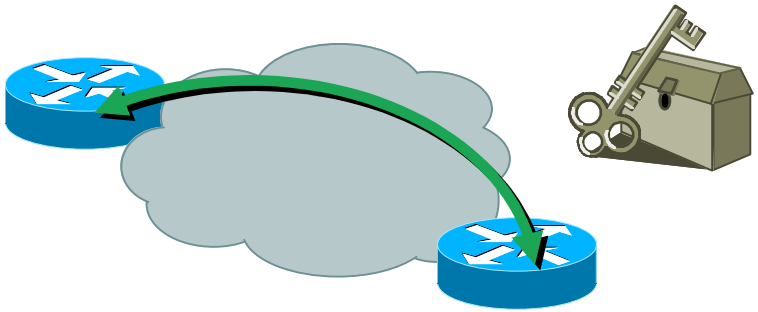
Tunneling	Encryption	Authentication*	Integrity
▪ IPsec ▪ L2TP/IPsec ▪ TLS (HTTPS/SSL) ▪ DTLS	▪ DES ▪ 3DES ▪ AES ▪ RC4	▪ RSA digital certificates ▪ Pre-Shared key **IKE 1st Phase, Not User Auth.*	▪ HMAC-MD5 ▪ HMAC-SHA-1

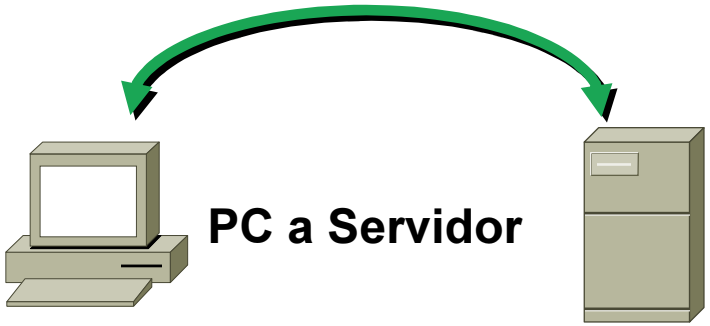
Aplicaciones

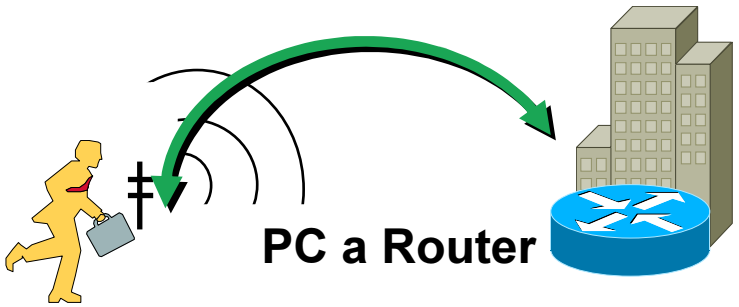


VPN’s en todas partes !





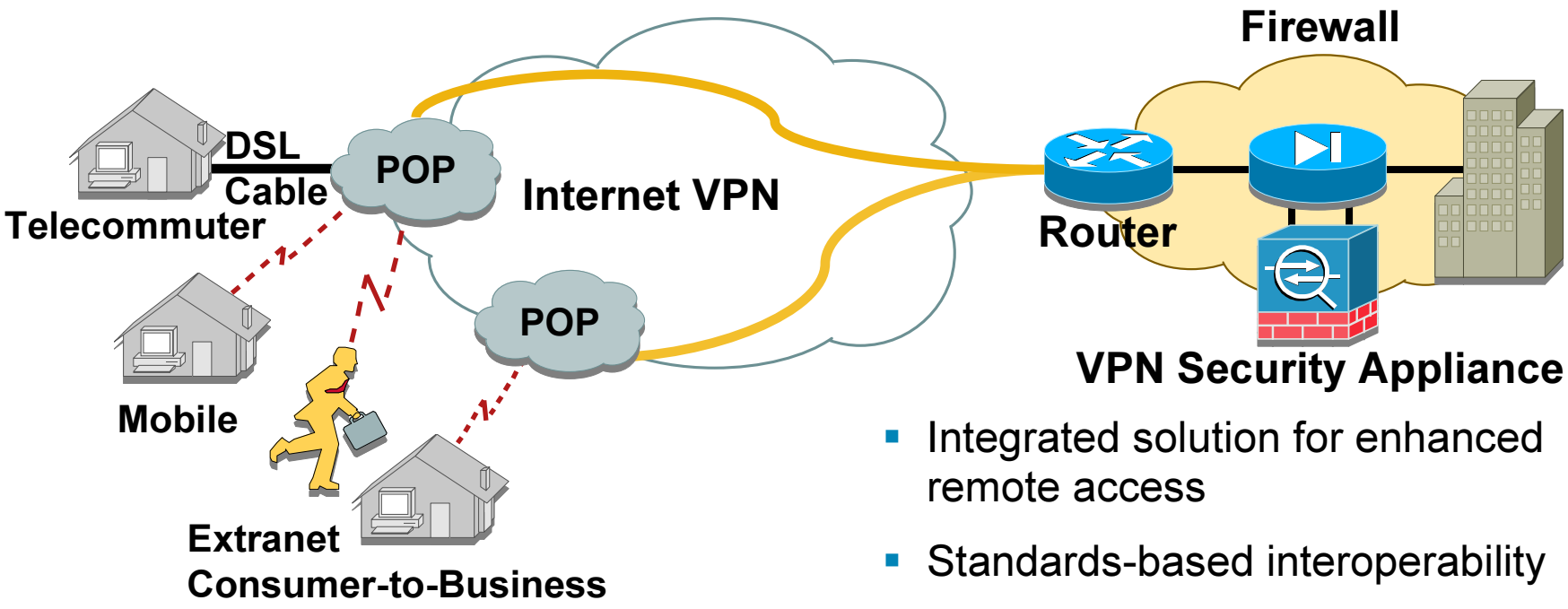




Remote Access VPN over the Internet

Remote Access Client
AnyConnect, IPsec VPN -Layer 3
Microsoft Windows, Mac OS X (L2TP/IPsec)
iPhone
SSL "Clientless"—Layer 7

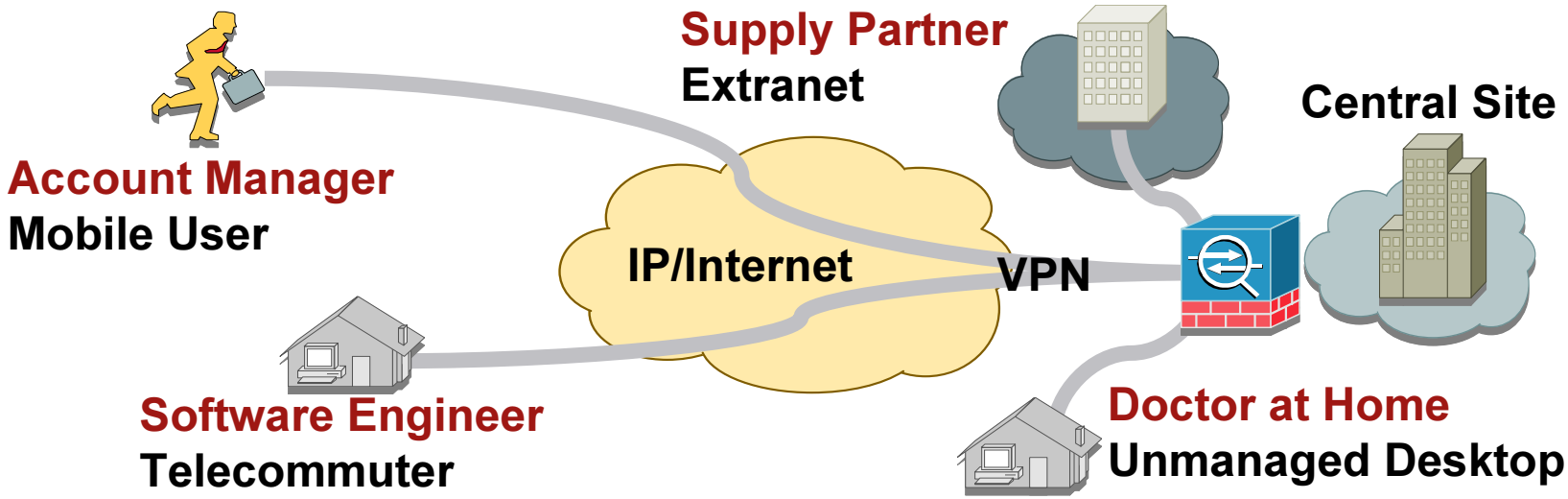
Enterprise—Central Site
Router, Firewall, and
VPN Security Appliance: VPN Tunnel Termination



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

Deployment Example

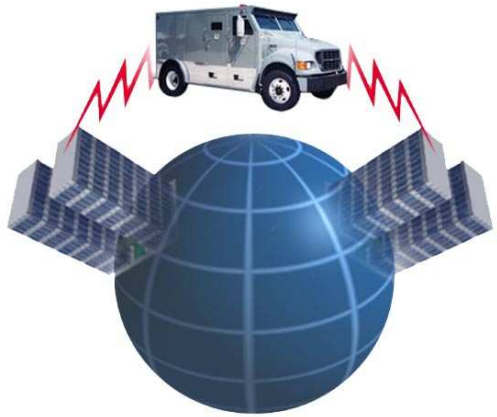
IPsec and SSL VPN Support Diverse User Populations



Clientless (L7) a browser	Full Network Access (L3) Cisco VPN Client//AnyConnect VPN Client
▪ Partner—Few apps/servers, tight access control, no control over desktop software environment, firewall traversal ▪ Doctor—Occasional access, few apps, no desktop software control	▪ Engineer—Many servers/apps, needs native app formats, VoIP, frequent access, long connect times ▪ Account Manager—Diverse apps, home-grown apps, always works from enterprise-managed desktop

Agenda

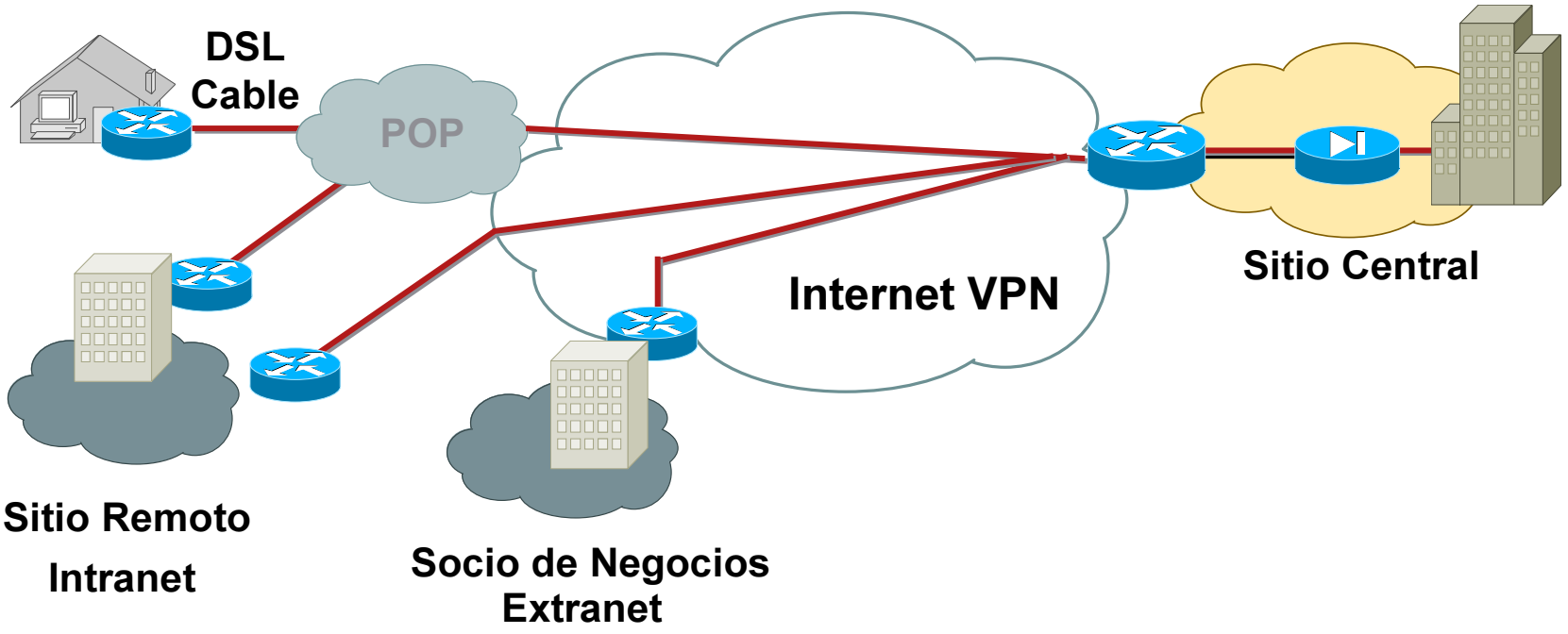
- Introducción
- Site-to-Site VPNs
- VPNs Remotas
- Selección de Plataformas



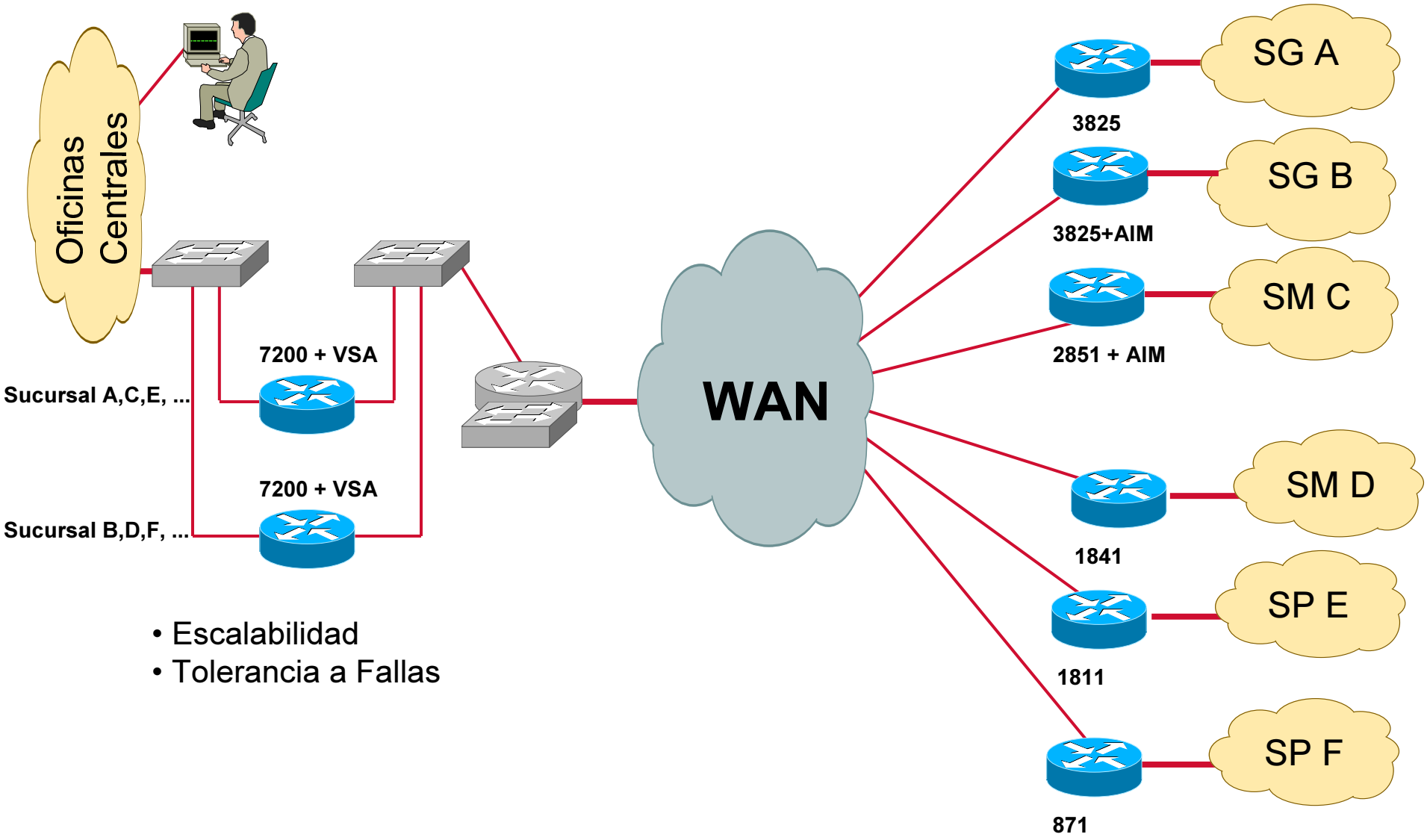
Site-to-Site VPNs

CPE – Sitio Remoto
VPN Router/Firewall
Firewall

Sitio Central
VPN Router/Firewall
Firewall



VPN LAN a LAN - Ejemplo



- Escalabilidad
- Tolerancia a Fallas

VPN Site to Site Advanced DMVPN GETVPN

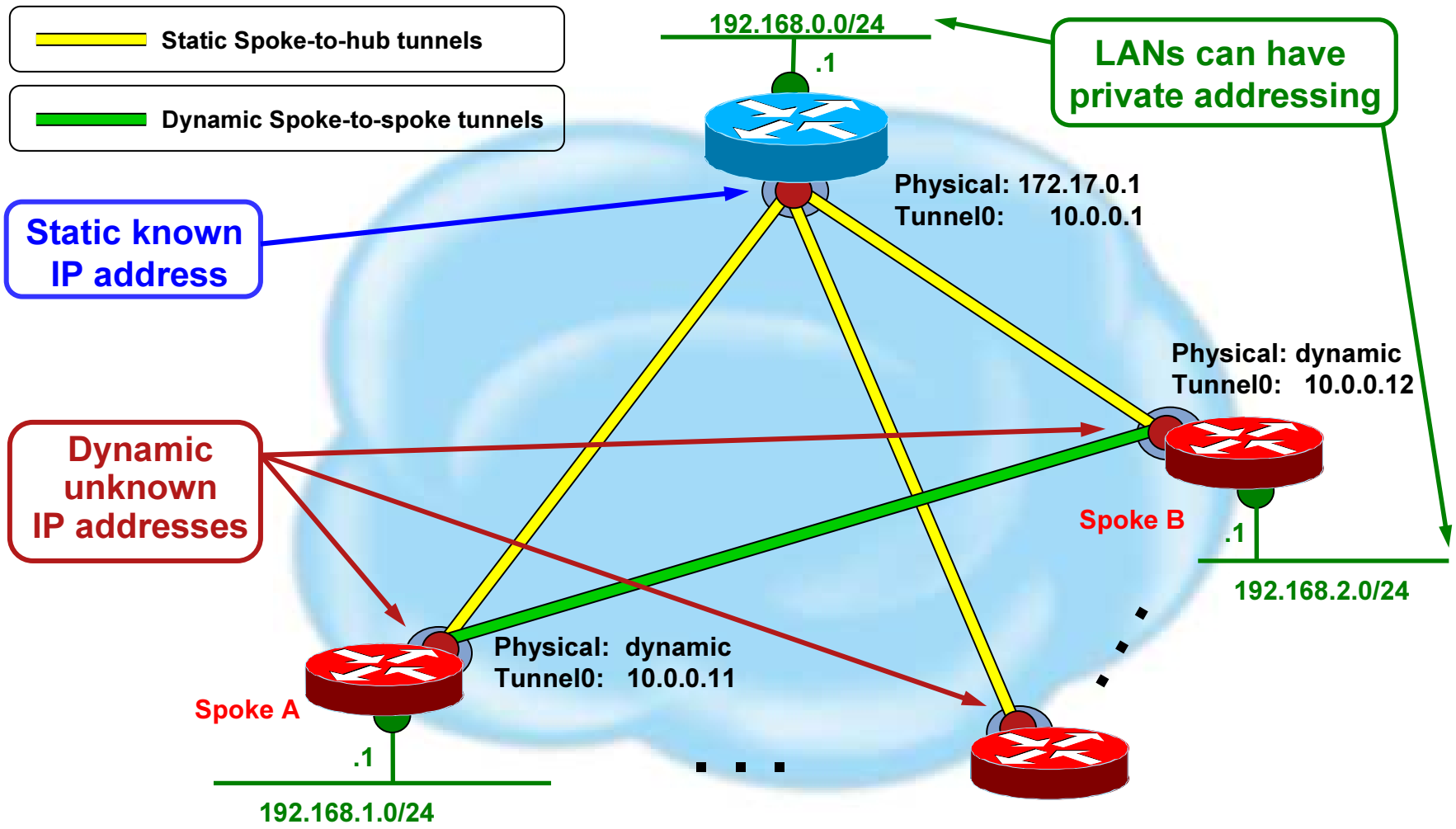
What is Dynamic Multipoint VPN ?

- DMVPN is a Cisco IOS Software solution for building IPsec+GRE VPNs in an easy, dynamic and scalable manner
- Relies on two proven technologies
  - Next Hop Resolution Protocol (NHRP)
    - Creates a distributed (NHRP) mapping database of all the spoke's tunnel to real (public interface) addresses
  - Multipoint GRE Tunnel Interface
    - Single GRE interface to support multiple GRE/IPsec tunnels
    - Simplifies size and complexity of configuration

DMVPN – How it works

- Spokes have a dynamic permanent GRE/IPsec tunnel to the hub, but not to other spokes. They register as clients of the NHRP server
- When a spoke needs to send a packet to a destination (private) subnet behind another spoke, it queries the NHRP server for the real (outside) address of the destination spoke
- Now the originating spoke can initiate a dynamic GRE/IPsec tunnel to the target spoke (because it knows the peer address).
- The spoke-to-spoke tunnel is built over the mGRE interface

Dynamic Multipoint VPN—Example



GET VPN:
Highly Scalable Encrypted Any-to-Any

What is it?

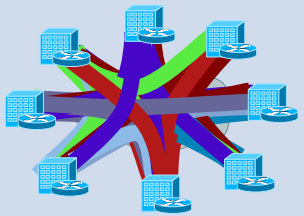
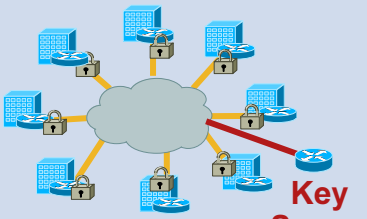
- New paradigm for encrypted WAN connectivity without IPsec tunnels

  "This is the way VPN should have been created all along"

Why is it innovative?

- Upsell security router bundles into MPLS / Frame Relay / Leased Lines
- Business drivers: compliance, outsourcing (managed security), mergers and acquisitions
- SPs can finally offer managed encryption without provisioning and management nightmare
- Unique selling proposition with 2+ years lead over competition

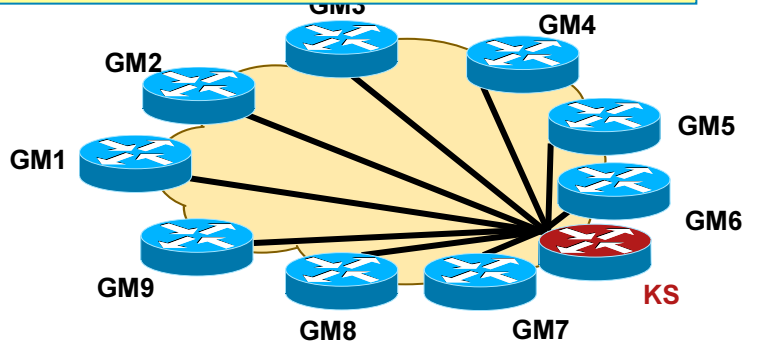
GET VPN: Advantage Cisco

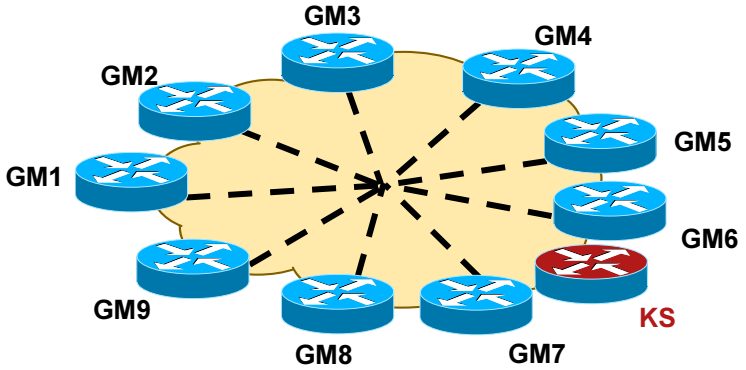
Point-to-Point IPsec VPN	Cisco GET VPN
	
IPsec overlay on top of IP routing	No overlays – native routing
Full mesh does not scale: ~N^2 tunnels for N sites	Scalable any-to-any
Two layers to manage and troubleshoot	Single IP layer
Limited QoS	Advanced QoS
Inefficient Multicast replication	Efficient Multicast replication

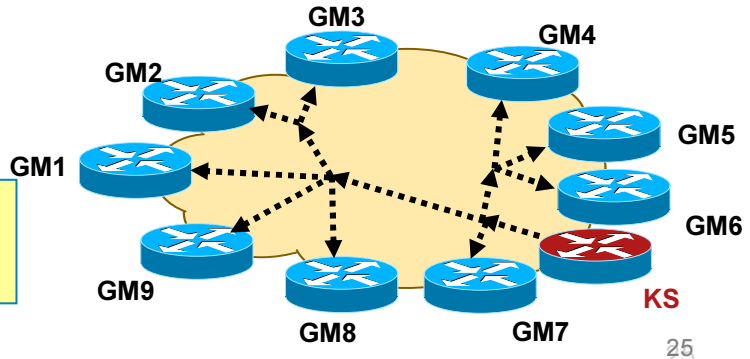
GETVPN: Innovation – Group Key Technology

Enables Simplified Key and Policy distribution to a large scale VPN network

- **Step 1**: Group Members (GM) "register" via GDOI (**IKE**) with the Key Server (KS)
  - KS authenticates & authorizes the GM
  - KS returns a set of IPsec SAs for the GM to use
- **Step 2**: Data Plane Encryption
  - GM exchange encrypted traffic using the group keys
  - The traffic uses **IPSec** Tunnel Mode with "address preservation"
- **Step 3**: Periodic Rekey of Keys
  - KS pushes out replacement IPsec keys before current IPsec keys expire. This is called a "rekey"



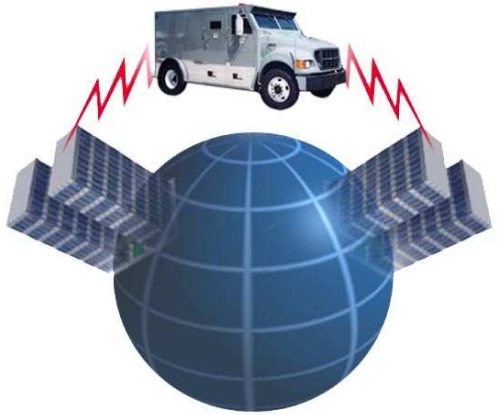




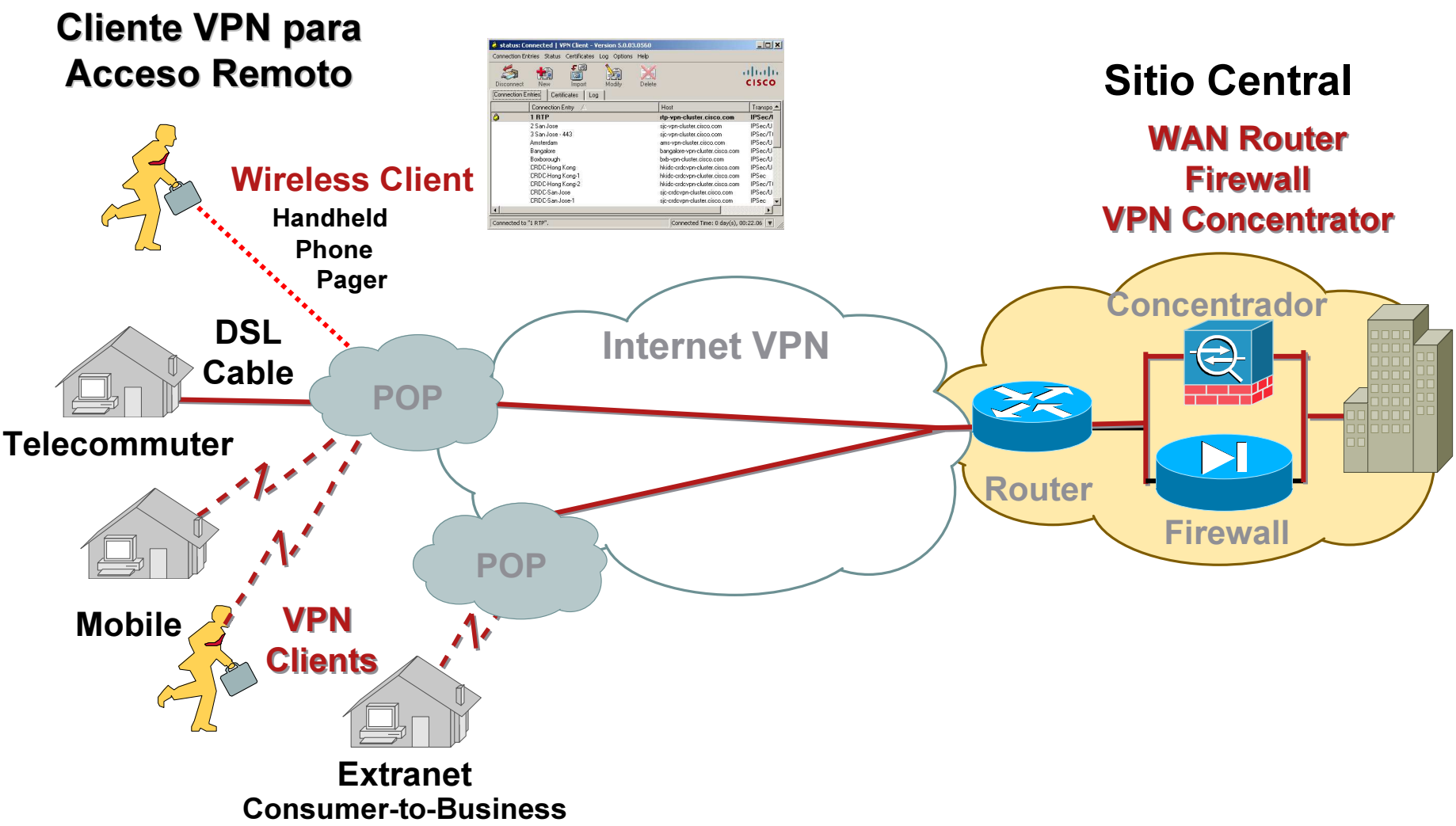
Once you have been admitted to the group, you can communicate freely with any/all group members.

Agenda

- Introducción
- Site-to-Site VPNs
- VPNs Remotas
- Selección de Plataformas

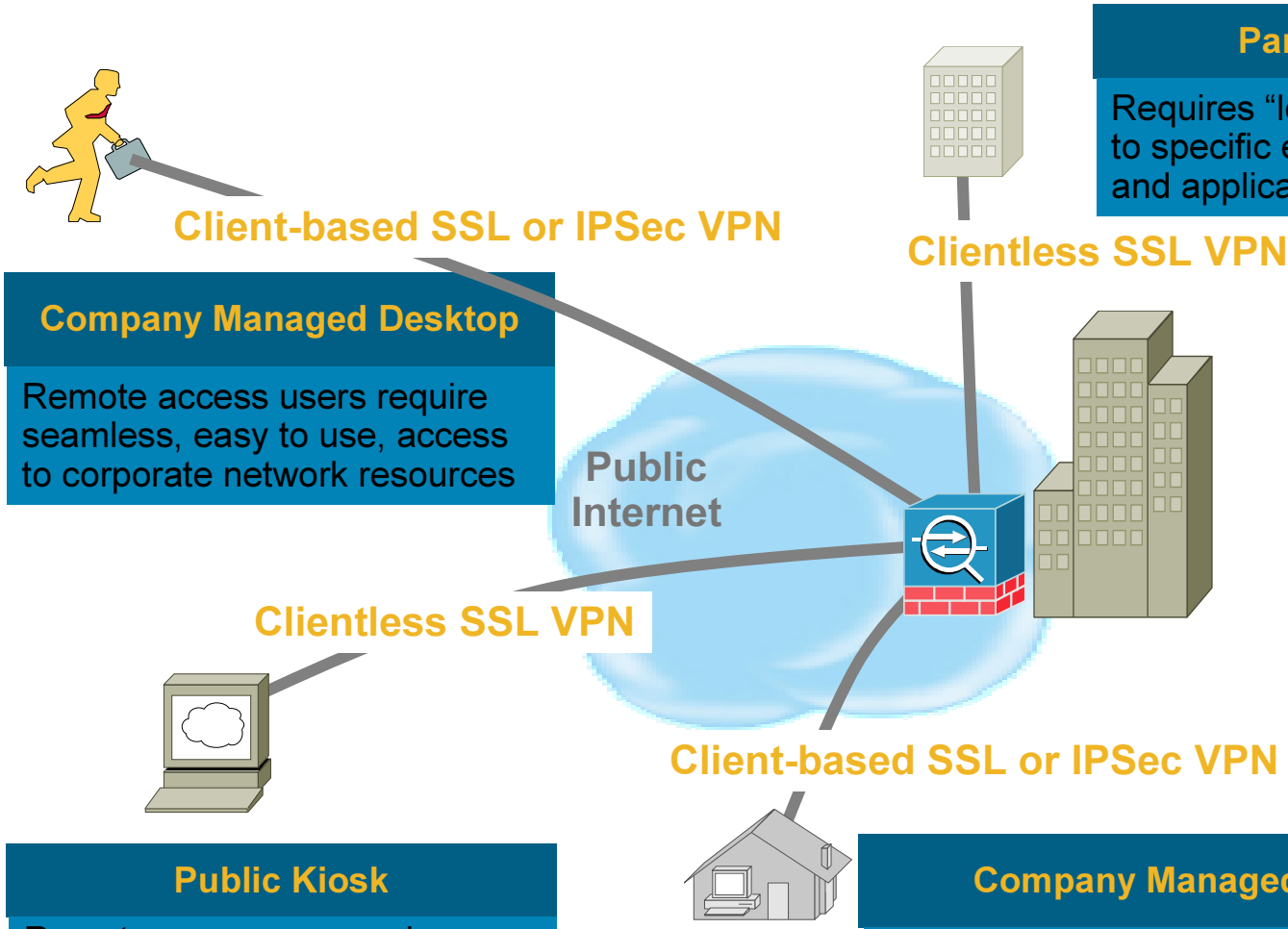


VPNs de Acceso Remoto



Comprehensive Secure Connectivity

VPN Services for Any Access Scenario



Company Managed Desktop

Remote access users require seamless, easy to use, access to corporate network resources

Partner Access

Requires “locked-down” access to specific extranet resources and applications

Public Kiosk

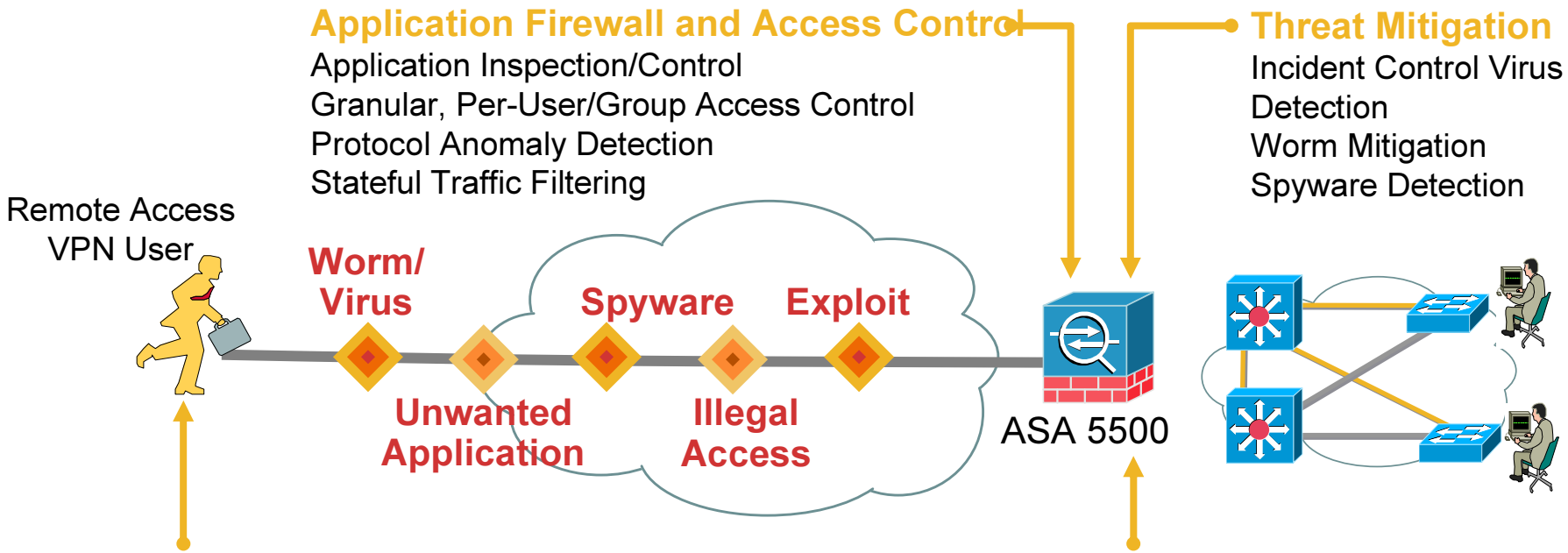
Remote users may require lightweight access to e-mail and web-based applications from a public machine

Company Managed Desktops at Home

Day extenders and mobile employees require consistent LAN-like, full-network access, to corporate resources and applications

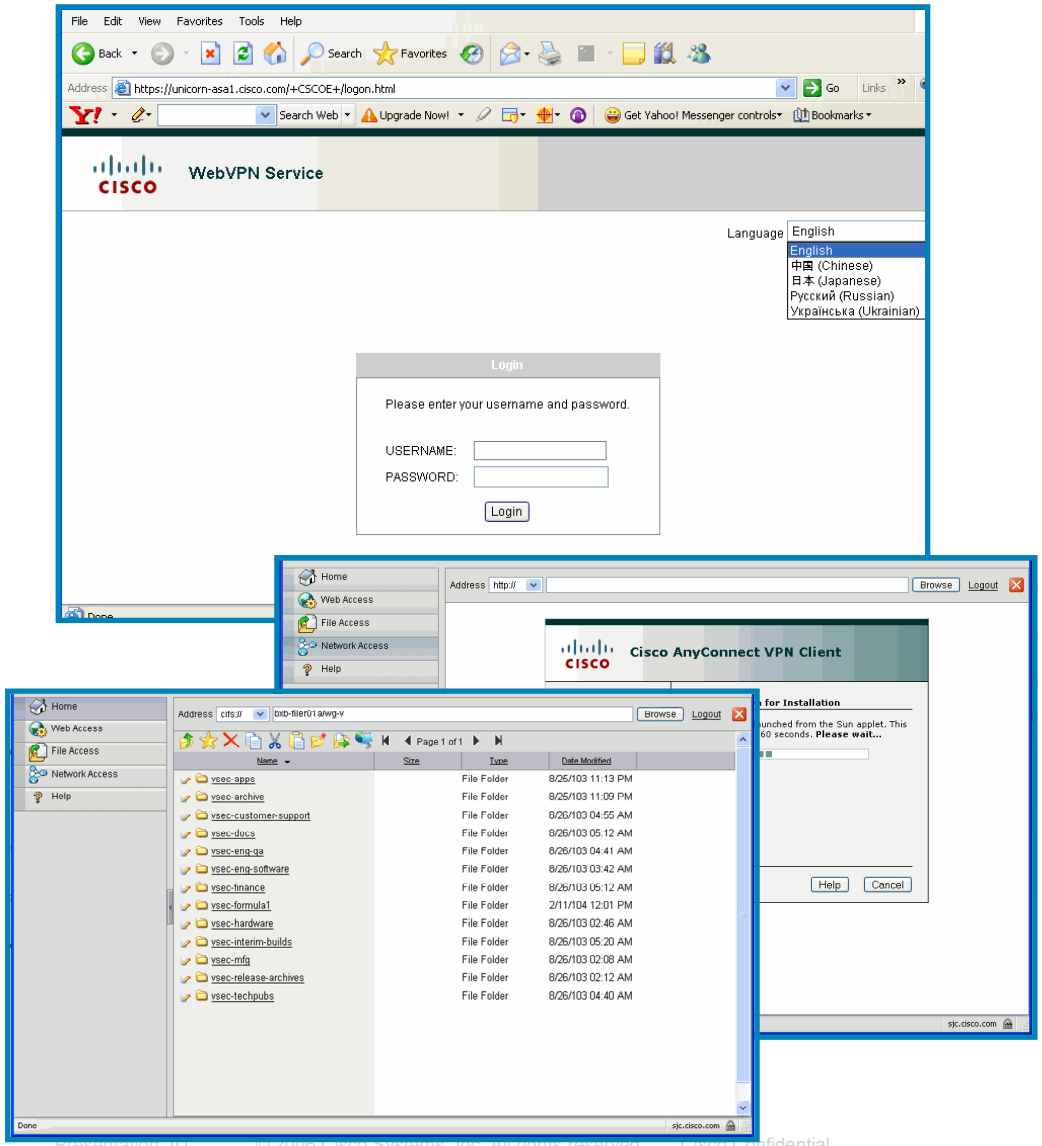
Threat Protected VPN Services

Leveraging On-Board Security to Protect the VPN Threat Vector



Leverages Depth of Threat Defense Features to Stop Malicious Worms, Viruses, and More…and Without External Devices or Performance Loss!

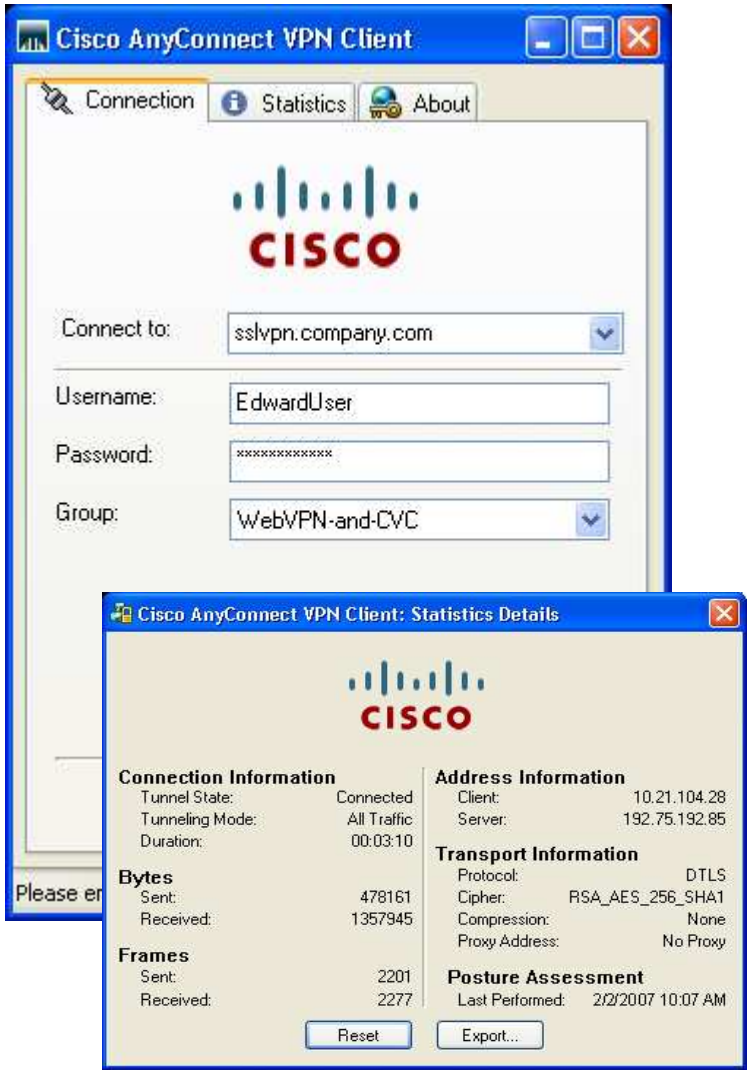
Cisco ASA 5500 Software v8.0 Introduces Significant Enhancements in Clientless Access



- Precise, granular access control to specific resources
- Enhanced Portal Design
  - Localizable
  - RSS feeds
  - Personal bookmarks
  - AnyConnect Client access
- Drag and Drop file access and webified file transport
- Transformation enhancements including Flash support
- Head-end deployed applets for telnet, SSH, RDP, and VNC, framework supports add'l plug-ins
- Advanced port-forwarder for Windows (Smart Tunnel) accesses TCP applications without admin privileges on Client PC

Cisco AnyConnect Client

- **Next generation VPN client, available on many platforms including:**
  - Windows Vista 32- and 64-bit, Windows XP 32- and 64-bit, and Windows 2000
  - Mac OS X 10.4 (Intel and PPC)
  - Intel-based Linux
  - Windows Mobile 5 Pocket PC Edition
- **Stand-alone, Web Launch, and Portal Connection Modes**
- **Start before Login (SBL) and DTLS support**
  - **Windows 2000 and XP only**



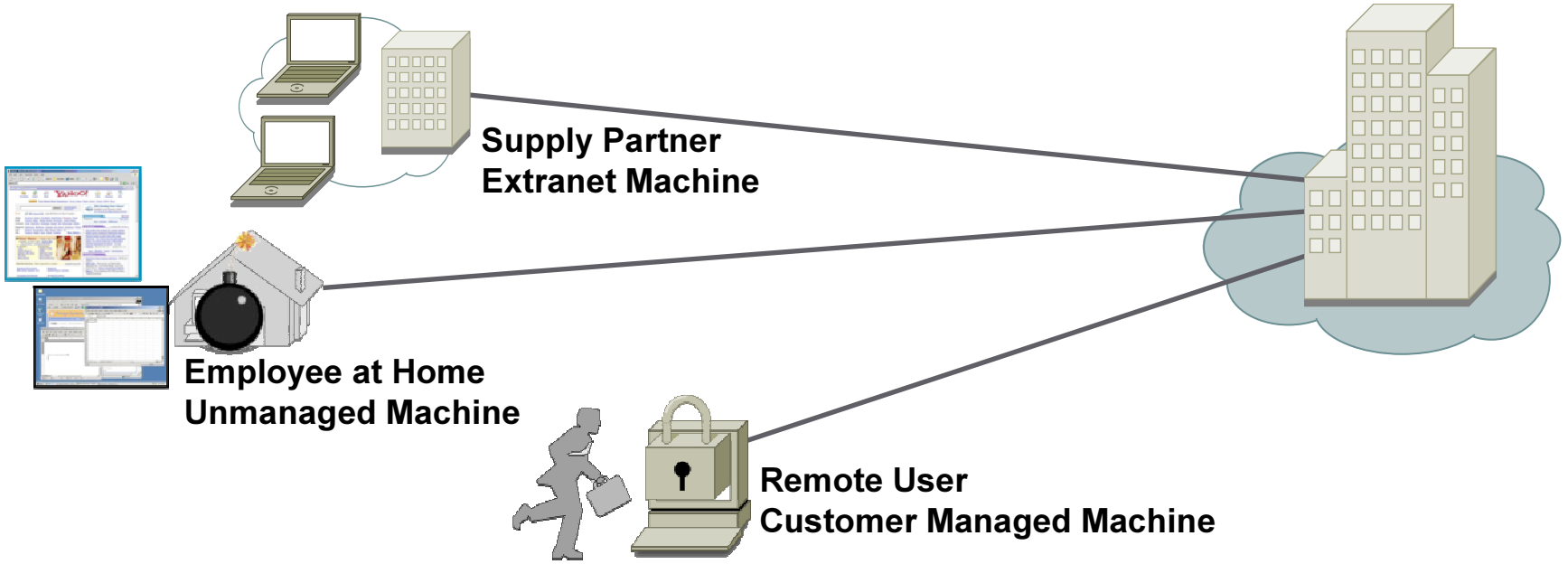
Comprehensive EndPoint Security

- Cisco Secure Desktop (CSD) now supports hundreds of pre-defined products, updated frequently

  Anti-virus, anti-spyware, personal firewall, and more

- Administrators can define custom checks including running processes
- CSD posture policy presented visually to simplify configuration and troubleshooting

Security Concerns for SSL VPN



Before SSL VPN Session

Who owns the endpoint?

Endpoint security posture: AV, personal firewall?

Is malware running?

During SSL VPN Session

- Is session data protected?
- Are typed passwords protected?
- Has malware launched?

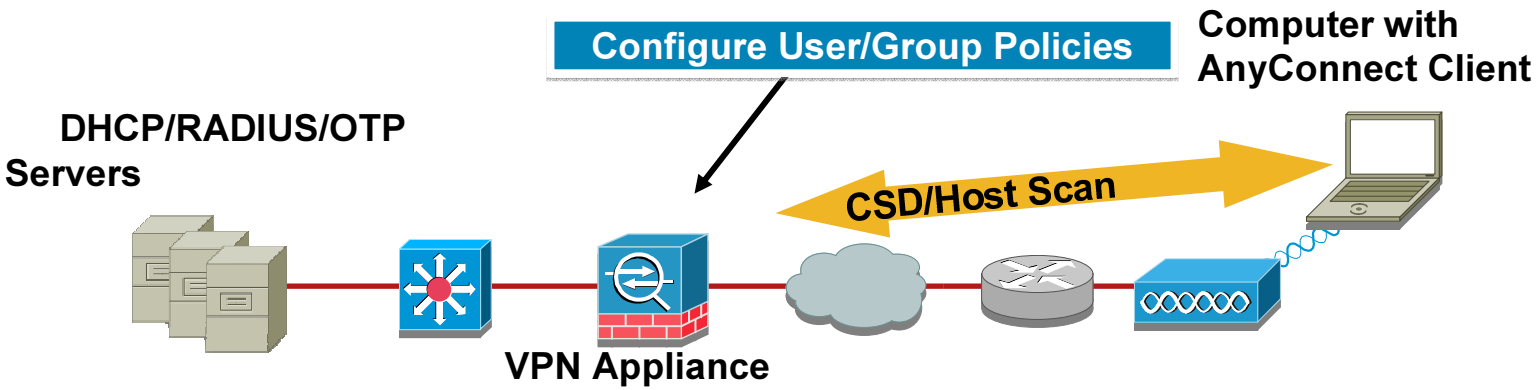
After SSL VPN Session

- Browser cached intranet Web pages?
- Browser stored passwords?
- Downloaded files left behind?

Endpoint Control for SSL Full Tunnel

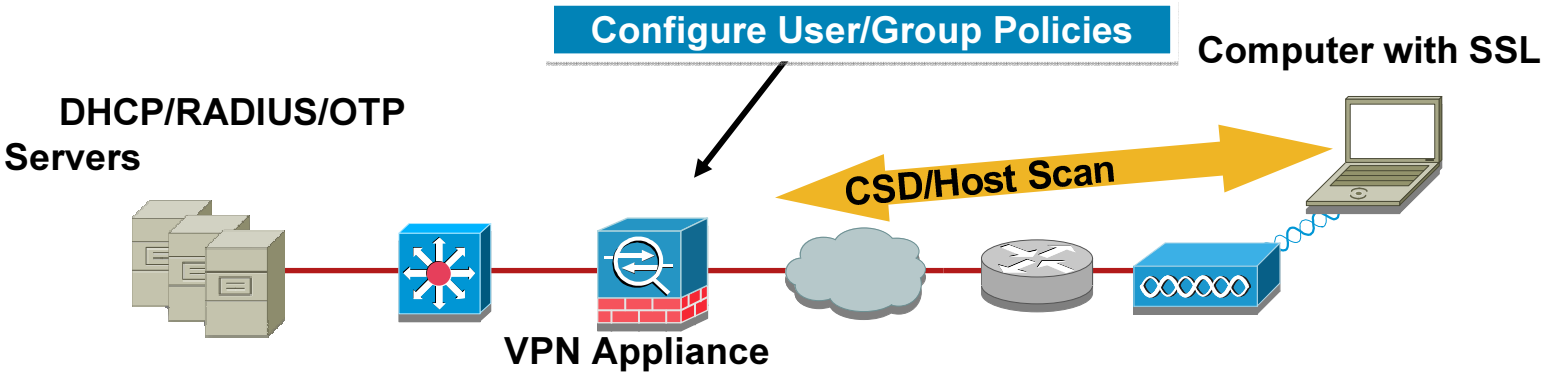
AnyConnect Client

- Policies for users and groups
  - Assign IP address based on user/group identity
  - Apply network ACL filter
  - Restrict access to VLAN
- Policies applied based on end station criteria
  - Cisco Secure Desktop (CSD)
  - Dynamic Access Policy (DAP)
  - Assign NAC policy



Endpoint Control for Clientless SSL VPN

- Policies for users and groups
  - Restrict access to VLAN
  - Apply Web ACL filter
  - Control URL entry
  - Control file server entry and browsing
- Policies applied based on end station criteria
  - Cisco Secure Desktop (CSD)
  - Dynamic Access Policy (DAP)



Cisco Secure Desktop

Comprehensive Endpoint Security for SSL VPN

- **Pre-connect assessment:**

  Location assessment—managed or unmanaged desktop?
  Gathers data about the end machine

- **Session protection:**

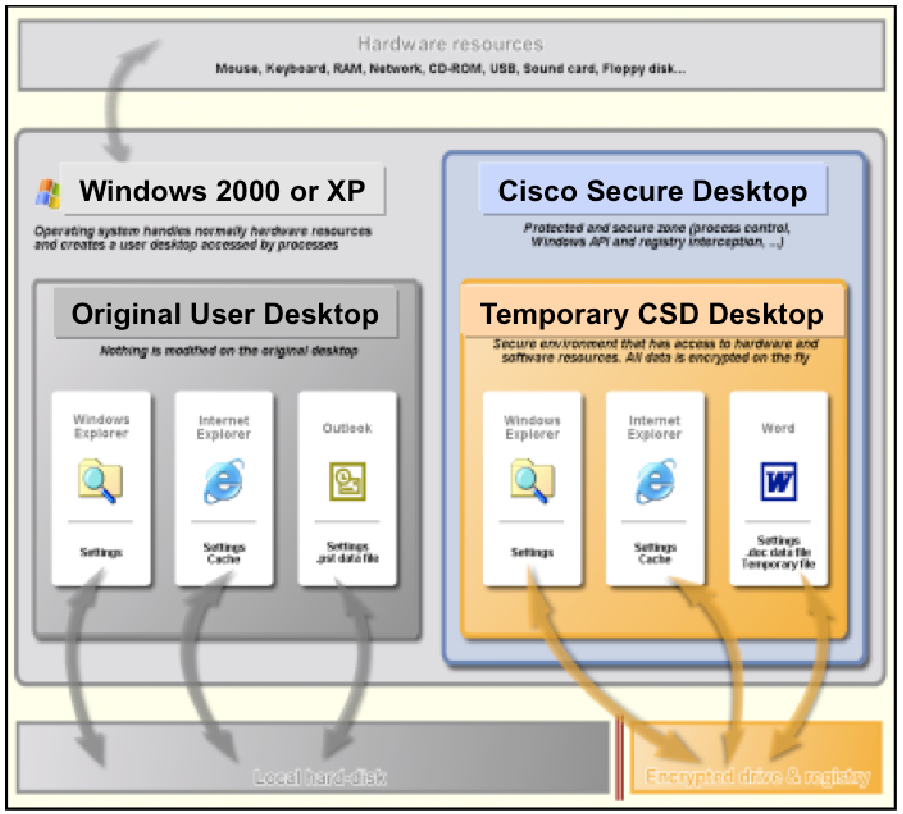
  Data sandbox and encryption protects every aspect of session

- **Post-session clean-up:**

  Encrypted partition overwrite (not just deletion)
  Cache, history and cookie overwrite

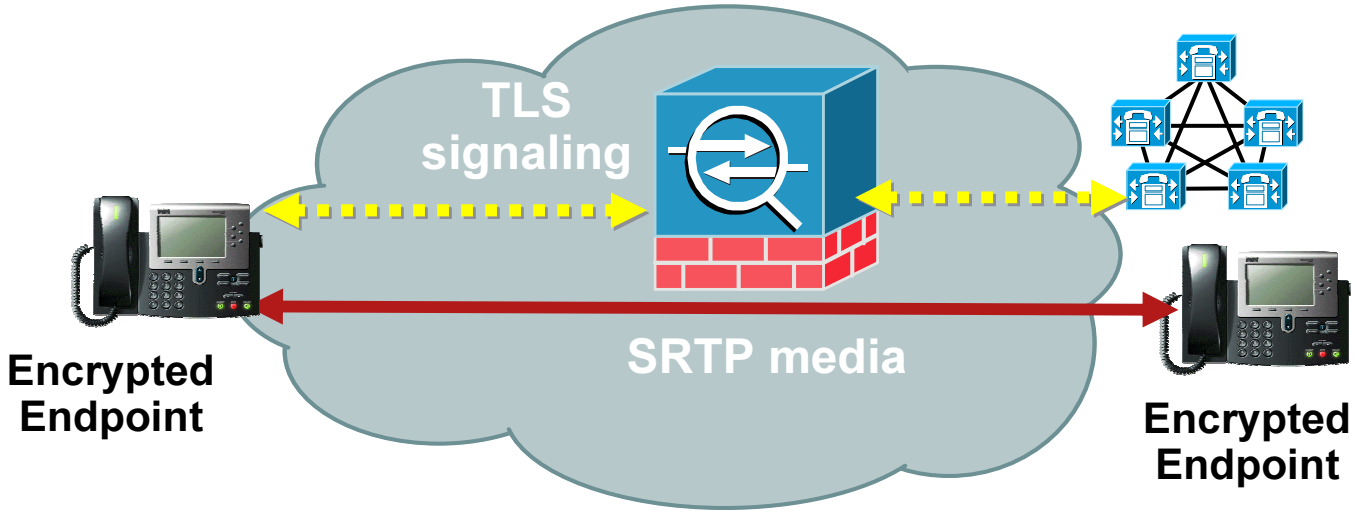
  File download and email attachment overwrite

  Auto-complete password overwrite



Industry-First Encrypted Voice Security Solution

Now Available with Cisco ASA 5500 Software v8.0



Any Cisco voice/video communications encrypted with SRTP/TLS can now be inspected by Cisco ASA 5500 Adaptive Security Appliances:

- **Maintains integrity and confidentiality of call while enforcing security policy through advanced SIP/SCCP firewall services**
- **TLS signaling is terminated and inspected, then re-encrypted for connection to destination (leveraging integrated hardware encryption services for scalable performance)**
- **Dynamic port is opened for SRTP encrypted media stream, and automatically closed when call ends**

Cisco ASA 5500 Series Adaptive Security Appliances

Solutions Ranging from Desktop to Data Center

Cisco ASA 5500 Platforms

- Integrates, market-proven firewall, SSL/IPsec, IPS, and content security technologies
- Extensible multi-processor architecture delivers high concurrent services performance and significant investment protection
- Flexible management lowers cost of ownership
- Easy-to-use Web-based user interface
- Numerous certifications and awards
- And much more…

New

ASA 5580-40

New

ASA 5580-20

ASA 5550

ASA 5540

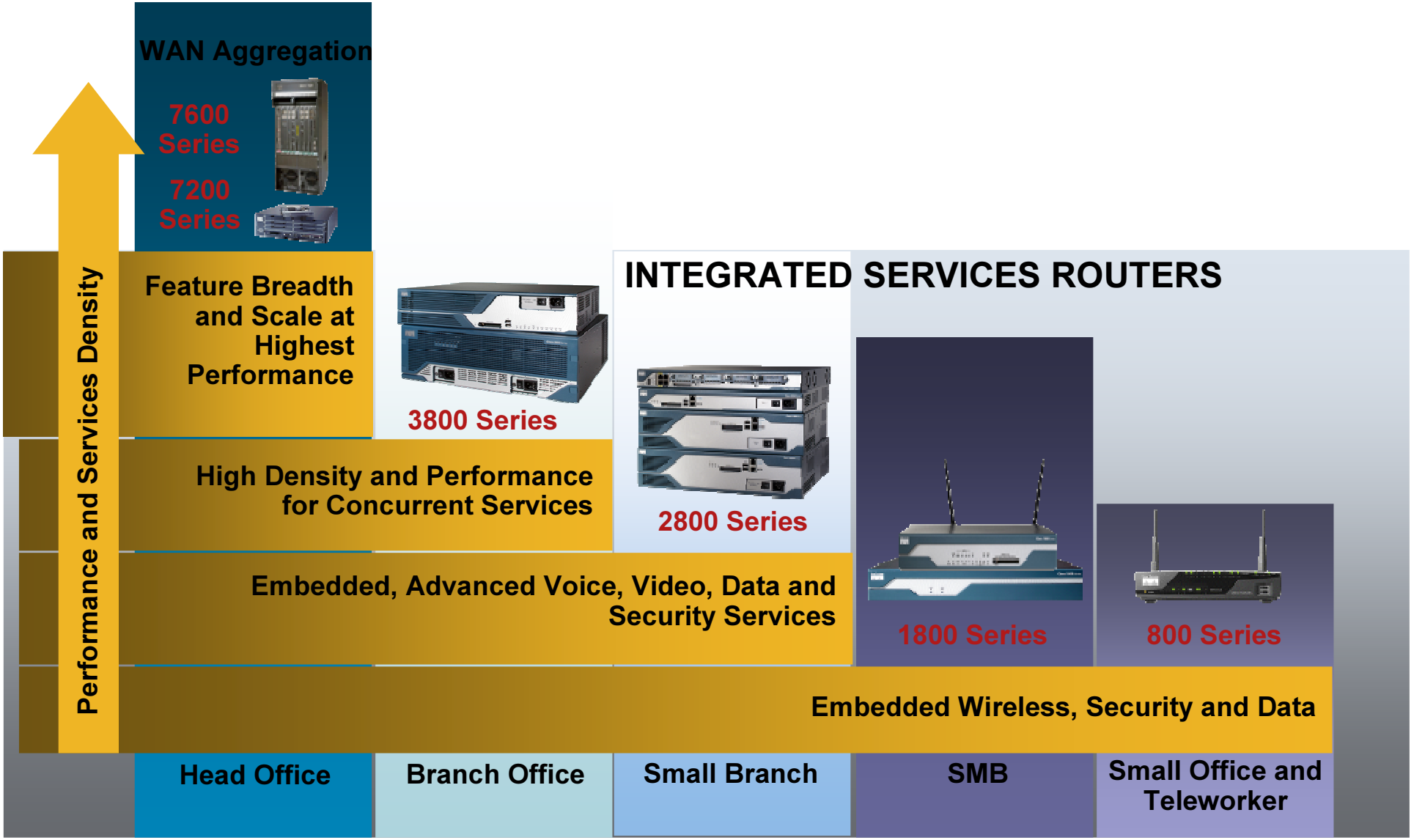
ASA 5520

ASA 5510

ASA 5505

Teleworker | Branch Office | Internet Edge | Campus | Data Center

Integrated Services Router Portfolio



Additional Resources

HOME
SOLUTIONS
SECURITY
SECURITY SOLUTIONS
Cisco Network Identity and Access Policy Solution
Data Loss Prevention
SAFE

SAFE
Introduction

Cisco SAFE

Take advantage of this validated next-generation security architecture and its design and implementation guidelines for building highly secure networks. (4:16 min)

Attend the SAFE technical sessions at Cisco Live! June 27-July 2

Register Now

Overview | **Branch** | **Campus** | **Data Center** | **Internet Edge** | **WAN Edge**

Cisco SAFE provides detailed design and implementation guidelines for organizations looking to build highly secure and reliable networks.

SAFE takes advantage of the collaboration between Cisco's security and network platforms. The results are:

- Greater visibility into devices and security events on the network
- Enhanced control of users, devices, and traffic for coordinated threat responses

High-Level View

Display Other Views

Cisco SAFE Poster

The Cisco SAFE Security Reference Architecture

The Foundation for Secure E-Business

Cisco® SAFE is a security reference architecture that provides detailed design and implementation guidelines to assist organizations looking to build highly secure and reliable networks. SAFE's modular designs take advantage of cross-platform network intelligence and collaboration between Cisco security and network devices, to better address the unique security and business needs of different places within the network, and interoperability between network segments, including campus, data center, branches, partners, and remote workers. The result is greater visibility into device and network security events, and enhanced control of users, devices, and traffic for coordinated threat response. SAFE's comprehensive security strategy improves an organization's ability to identify, prevent, and respond to threats, and securely deploy critical business applications and services.

High-Level View

Icon Key

For More Information

› cisco.com/go/safe › cisco.com/go/security