



poweredbycisco.
networkers
2005

DEPLOYING REMOTE ACCESS IPSEC AND SSL VPNS

SEC-2010

Carlos Pereira



Recuerde siempre:

Cisco.com



- Apagar su teléfono móvil/pager, o usar el modo “silencioso”.



- Completar la evaluación de esta sesión y entregarla a los asistentes de sala.



- Ser puntual para asistir a todas las actividades de entrenamiento, almuerzos y eventos sociales para un desarrollo óptimo de la agenda.



- Completar la evaluación general incluida en su mochila y entregarla el miércoles 8 de Junio en los mostradores de registración. Al entregarla recibirá un regalo recordatorio del evento.

Agenda

- **Introduction to Remote Access VPNs**
- **Design Considerations**
- **Deployment Considerations**
- **Unattended mode**
- **Wireless (WLAN) and VPN**
- **Case Study**
- **Q&A**

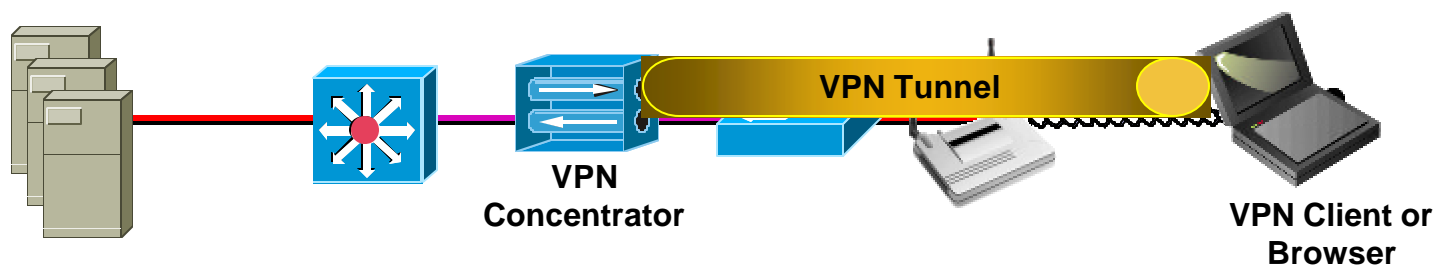
INTRODUCTION TO REMOTE ACCESS VPNS



Virtual Private Network (VPN) Overview

IP Security (IPSec) and 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)



Remote Access VPN Over the Internet

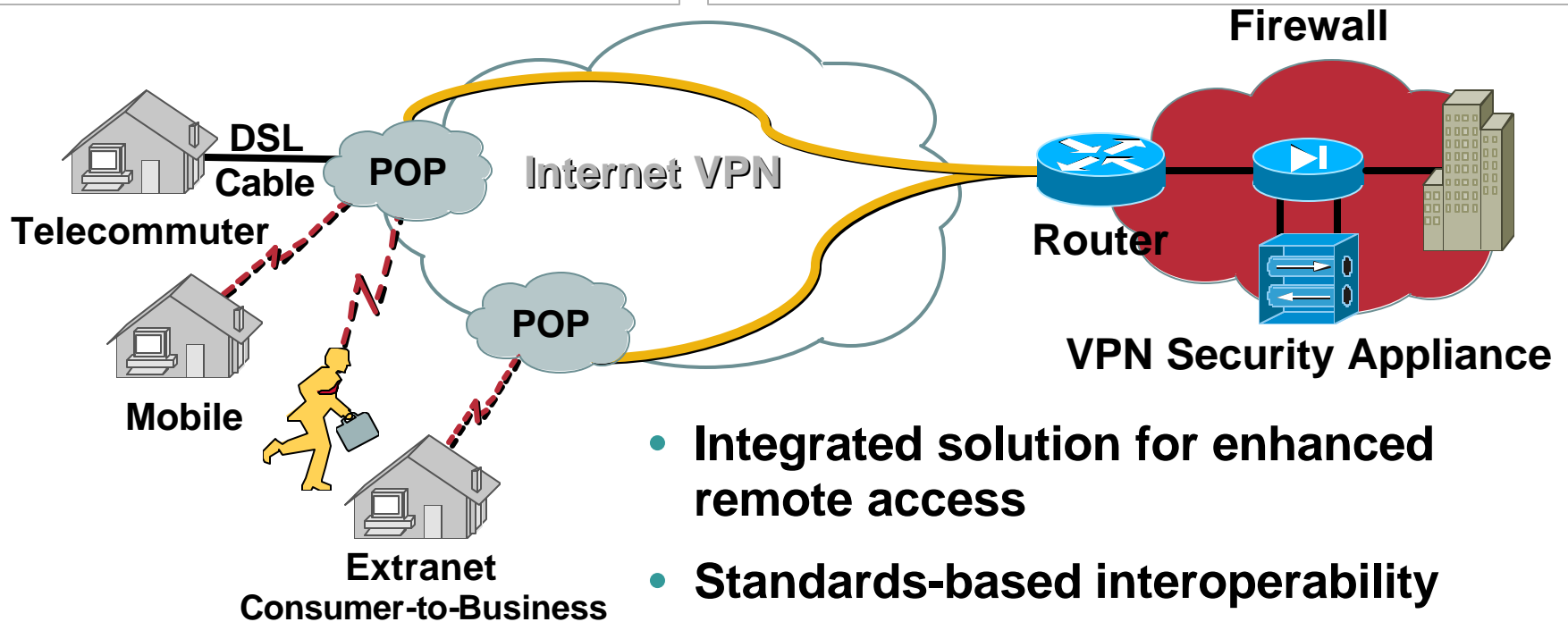
Remote Access Client

Cisco VPN Clients

Microsoft Win 2k/XP (L2TP+IPSec/PPTP)
Microsoft Win 9x/NT (L2TP+IPSec or PPTP)
SSL “clientless” or SSL VPN Client (SVC)

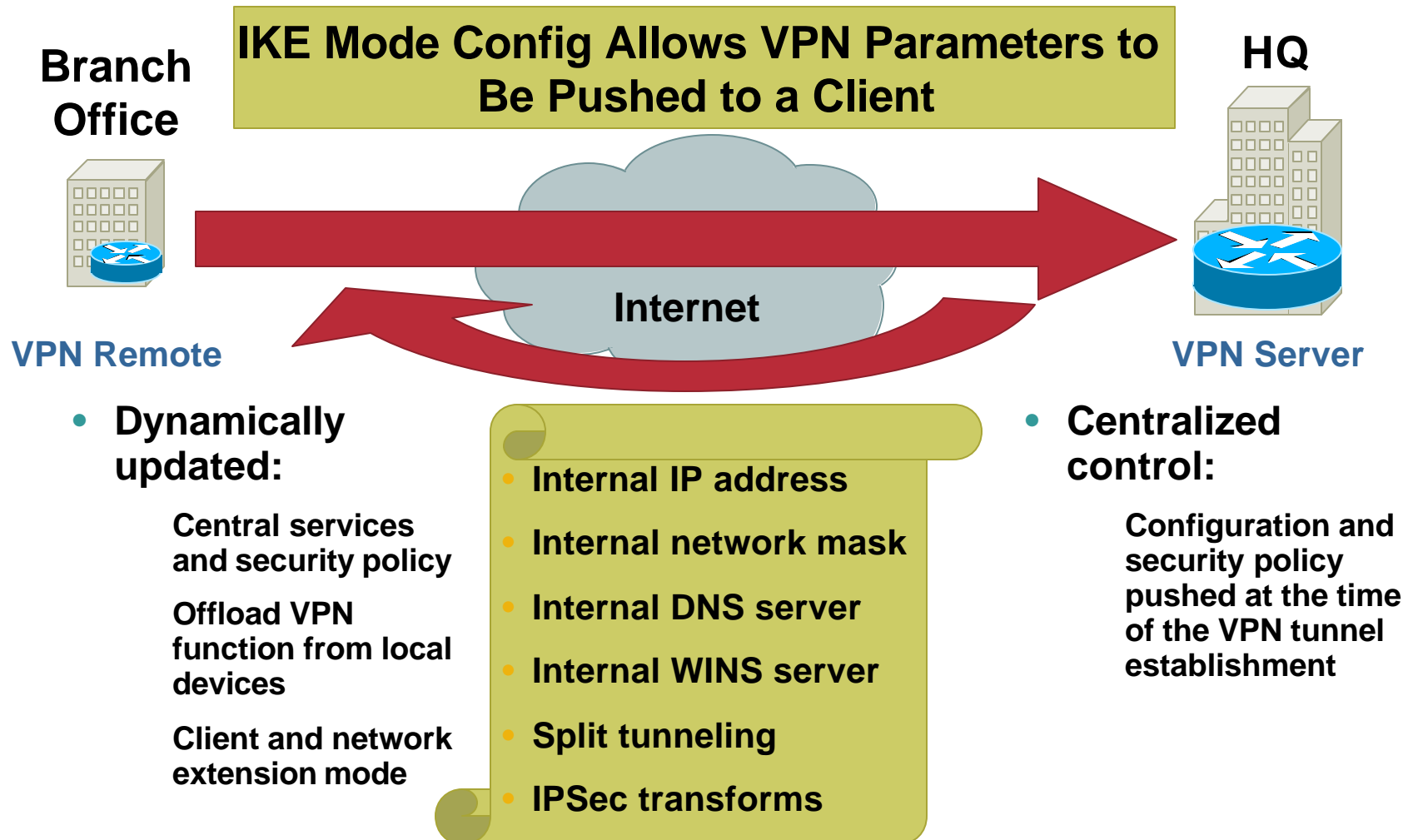
Enterprise—Central Site

Router, Firewall &
VPN Security Appliance: VPN Tunnel Termination



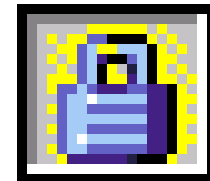
- Integrated solution for enhanced remote access
- Standards-based interoperability

Easy VPN Client (IPSec) Implementation



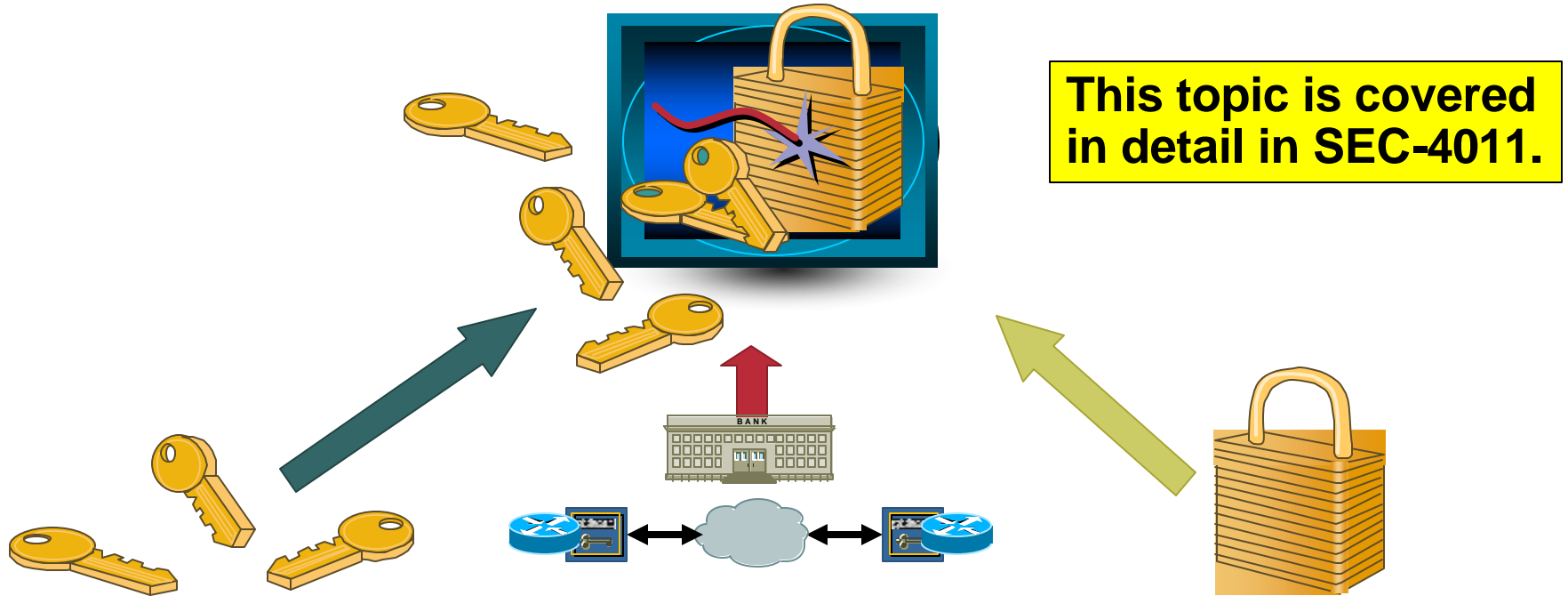
Secure Sockets Layer (SSL) Overview

- **Protocol developed by Netscape for secure e-commerce**
- **Creates a tunnel between web browser and web server**
 Authenticated and encrypted (RC4, 3DES, DES)
- **Capability shipped by default in leading browsers**
 Self-signed certificate
- **https://**
 Usually over port :443
 Closed lock indicates SSL enabled



What Are We Talking About?

Secure VPN



This topic is covered in detail in SEC-4011.

Tunneling	Encryption	Authentication*	Integrity
<ul style="list-style-type: none">• IPSec• L2TP/IPSec• PPTP• HTTPS/SSL	<ul style="list-style-type: none">• DES• 3DES• AES• RC4	<ul style="list-style-type: none">• RSA Digital Certificates• Pre-Shared Key <p>*IKE 1st phase, not user auth.</p>	<ul style="list-style-type: none">• HMAC-MD5• HMAC-SHA-1

Understanding Your Remote Users

Cisco.com

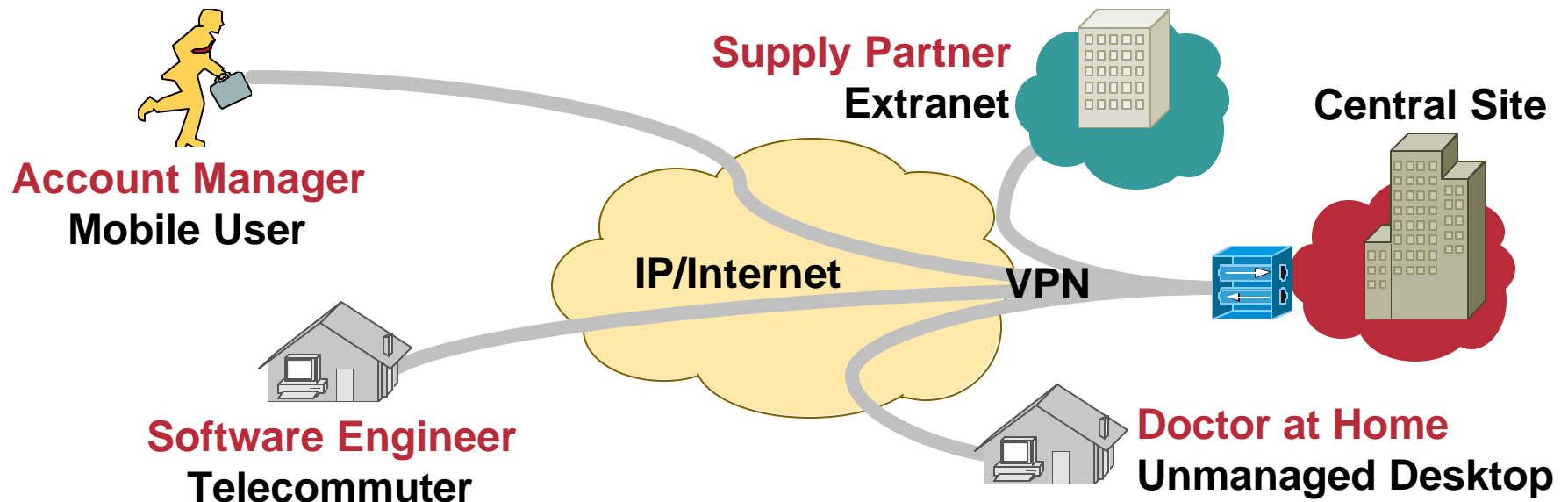
- **What applications do they need to access?**
 - Web browsing (including Web-based email)**
 - Thick client applications (TCP)**
 - Full network access**
- **Where will they be accessing from?**
 - Corporate managed computers**
 - Unmanaged computers**
 - Kiosks/Public systems**
- **How long will users stay connected?**
 - 24x7 or entire business day**
 - Limited period of time**



Deployment Example

Using IPsec and SSL VPN to Reach Diverse User Populations

Cisco.com



CLIENTLESS/THIN CLIENT SSL VPN

- **PARTNER**—Few apps/servers, tight access control, no control over desktop software environment, firewall traversal
- **DOCTOR**—Occasional access, few apps, no desktop software control

FULL CLIENT VPN

- **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

Two Common IPsec RA Methods

- **IKE/IPSec**

The IKE extension ModeCFG pushes IP address and other useful information (WINS, DNS, etc.) to client

The IKE extension Xauth authenticates users

IPSec/ESP provides secure transport

- **IKE + L2TP/IPSec (Microsoft VPN Client)**

L2TP is used to provide network transparency to the client (local virtual interface)

IPSec/ESP is used to provide secure transport

PPP handles assigning all necessary information (WINS, DNS, etc.)

IPSec VPN Client Provisioning and Customization

- Localized client
- Predefined profiles and policy configuration
- Admin defined graphics
- Simple mode
- Customizable MSI package



SSL VPN Clientless Customization

Customizable Banner Graphic

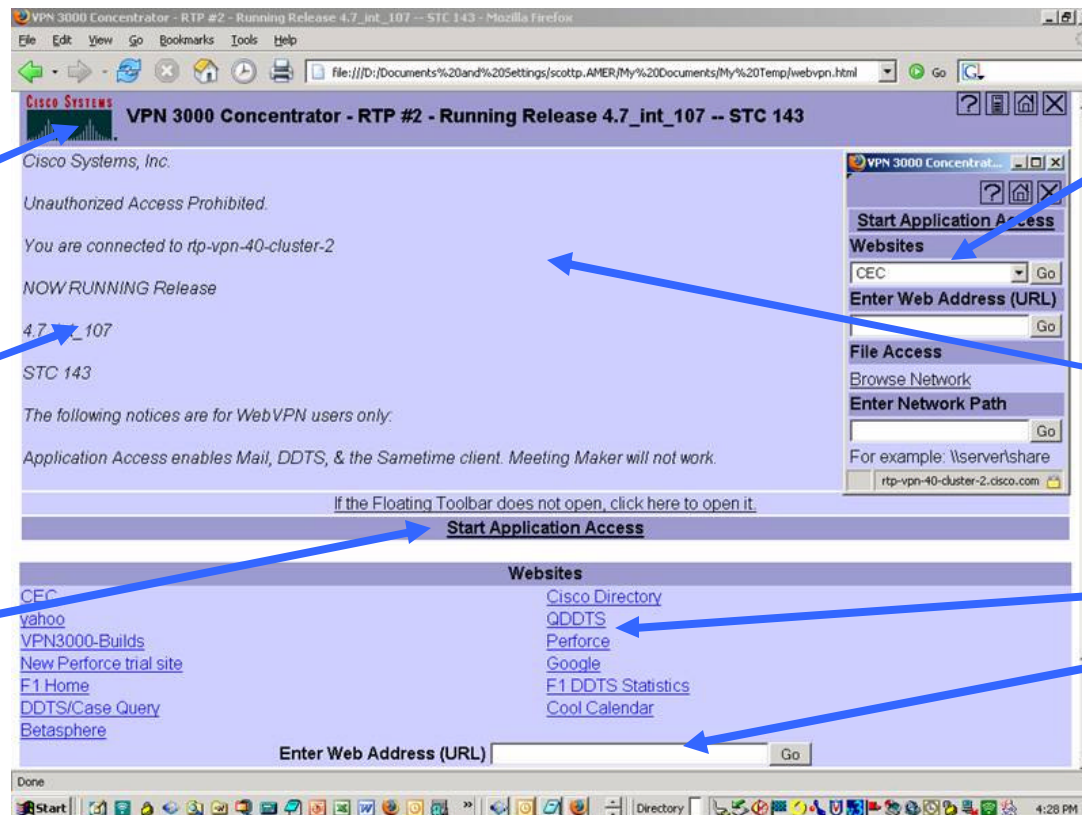
Customizable Banner Message

Customizable Access Methods

Customizable Floating Toolbar with Fast Links

Customizable Colors and Sections

Customizable Links, Network Resource Access



SSL for VPN is Different than eCommerce

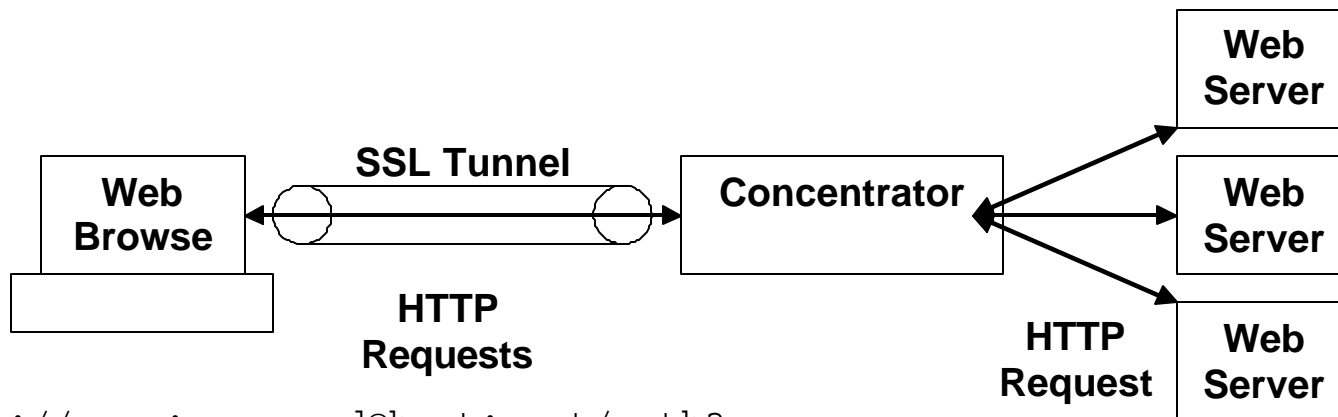
- **More complicated than just web pages**
- **Must fit into existing networks and application environments**
- **Must support all of the same authentication mechanisms and often extensive application list as available for IPsec**
- **SSL VPN has multiple access mechanisms**
 - Content rewriting & application translation (clientless)**
 - Port forwarding (thin client)**
 - VPN Client (full network access)**

SSL VPN: Clientless (Content Rewriting & Application Translation)

Standard Browser “Clientless”

- **Concentrator proxies HTTP(S) over SSL connection**
- **Limited to web pages**
 - HTML pages**
 - Web-based (webified) applications**
- **Imperfect science due to content rewriting, common issues with Java and Active X applets/applications**
- **For application translation, Concentrator “webifies” application**
 - Translates protocol to HTTP**
 - Requires detailed application knowledge**
 - Delivers HTML look-and-feel**
 - Expands use to some non-web applications**
 - CIFS (NT and Active Directory file sharing)**

SSL VPN: Data Flow Clientless



`protocol://user:password@host:port/path?query`

`https://user:password@chost:cport/protocol/flags/host/path?query`

`http://www.yahoo.com`

→ **`https://1.2.3.4/http/0/www.yahoo.com`**

`https://www.abc.com/d/index.html`

→ **`https://1.2.3.4/https/0/www.abc.com/d/index.html`**

`http://www.abc.com/x.cgi?a=b`

→ **`https://1.2.3.4/http/0/www.abc.com/x.cgi?a=b`**

`http://www.xyz.com:8080`

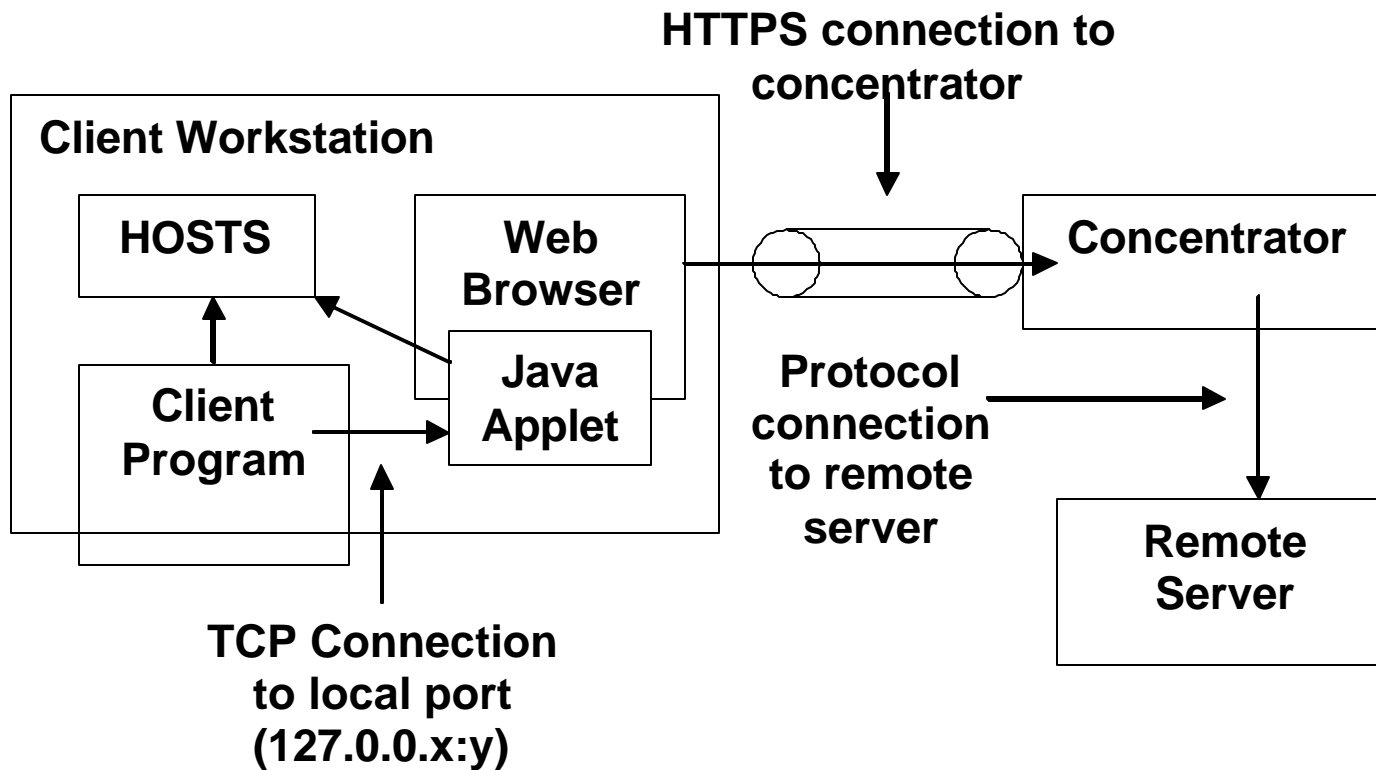
→ **`https://1.2.3.4/http/8080/www.xyz.com`**

SSL VPN: Port Forwarding (Thin Client)

“Thin” or “Enhanced” Client

- **Local “thin” client acts as proxy**
 - Tunnels and forwards application traffic
- **Delivered via Java from concentrator**
- **Some system permissions may be required, particularly for hostname mapping**
- **Maintains native application look-and-feel**
- **Works with predictable non-web applications**
 - Generally outbound, TCP-based, with static port(s)
 - Telnet, SMTP, POP3**

SSL VPN: Port Forwarding (Example)



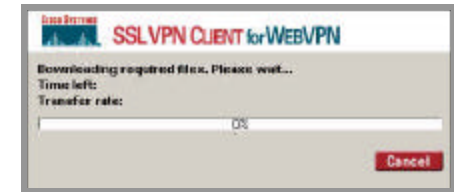
SSL VPN: Port Forwarding (Configuration)

Local Port	Destination	Protocol
1100	sun.test.com:22	SSH
1101	sun2.test.com:22	SSH
1102	mail.test.com:110	POP3
1103	mail.test.com:25	SMTP

127.0.0.1:1100; Host File Is Not Modified

If Host File Can be Modified: Applet Listens on Server.test.com:22; where server.test.com Is Mapped to 127.0.0.x (x Is Greater than 1, Determined at Run Time)

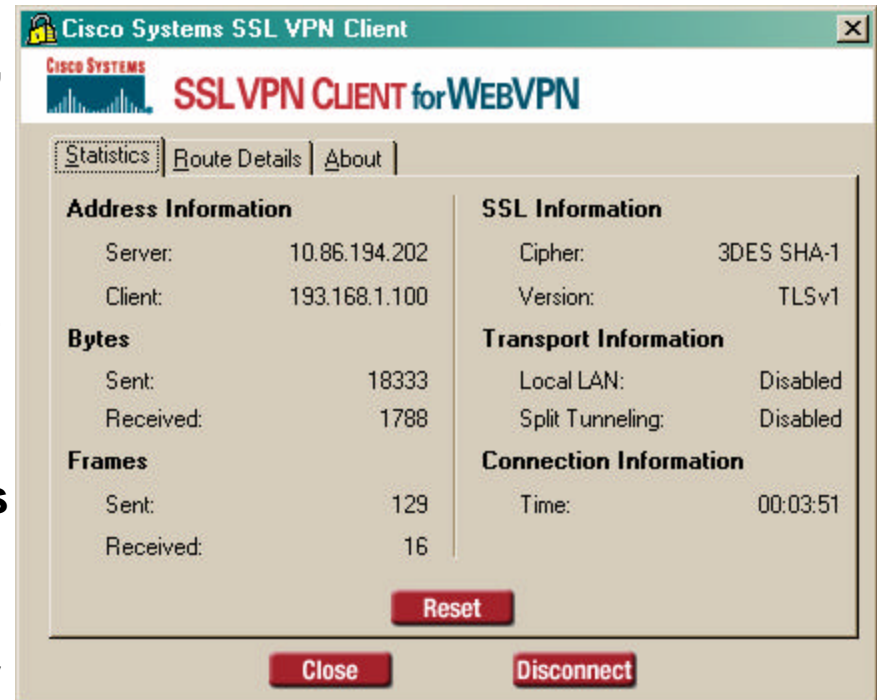
SSL VPN: VPN Client



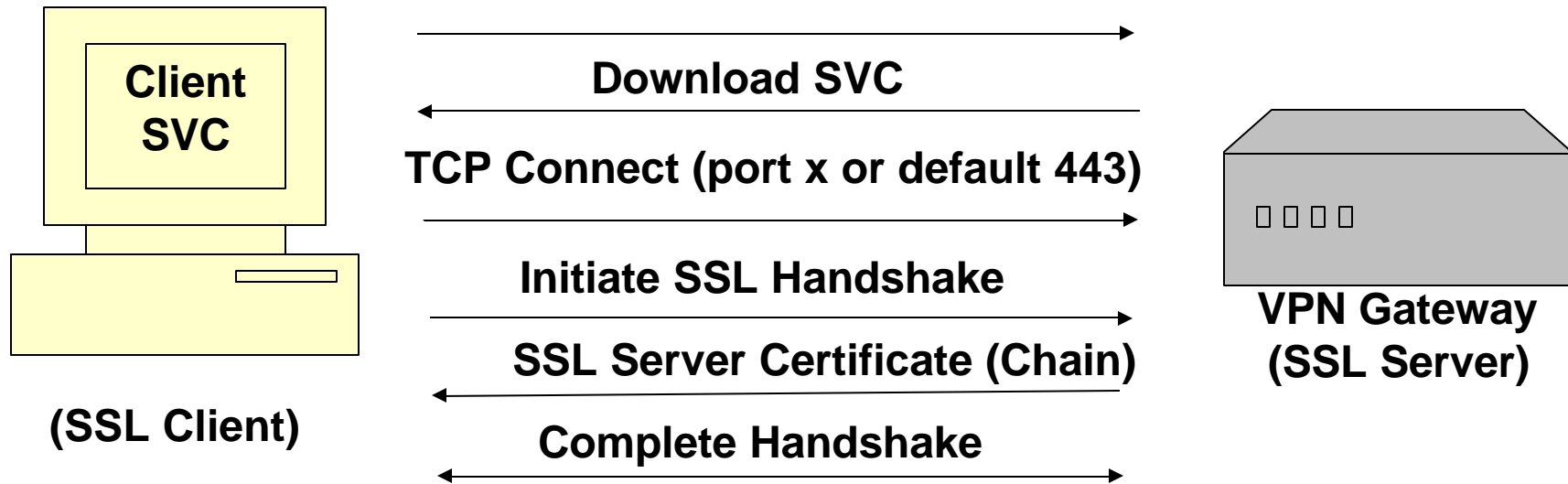
Cisco.com

Persistent “Thick”, “Full Tunneling” or “Tunnel” Client

- Traditional-style client delivered via automatic download (Active X, Java, and/or EXE)
- Requires administrative privileges for initial install
- Stub-installer used in cases where admin privileges are not available to the user
- Provides similar access to IPSec
 - Better accessibility over firewalls and NAT
 - Smaller installation package
- Lacks the access control granularity of other SSL mechanisms
- No reboots required



SSL VPN Client Tunnel Establishment



After handshake succeeds, client continues to

1. Obtain server certificate chain from system Library
2. Authenticate certificate chain and check revocation (except Root CA)
3. If revoked or severe error, tear down connection
4. If moderate error, ask user to view certificate and accept or deny
5. If user denies certificate chain, tear down connection

SSL VPN: Citrix Deployment

- **When using a full tunneling based option (IPSec or SSL VPN Client), Citrix connectivity would work similarly to use on the internal LAN.**

All modes of access are compatible including Program Neighborhood Client, Web Client and Java Client.

- **Citrix can also be supported using in conjunction with clientless SSL VPN.**

Java and Web client are compatible in this mode.

Typical Deployment for Hardware vs. Software Client

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

VPN Hardware Clients

PIX 501, Cisco IOS Routers, VPN 3002

Software Client

- Used by road warrior
- Client loaded on individual's PC or dynamic download (SVC)
- Supports individual's device only
- Tunnel launched by user or browser (SVC)

VPN Software Clients

Cisco VPN Client (SSL & IPsec), Microsoft Win2k/XP Native Client

DESIGN CONSIDERATIONS



Network Design Components

- **VPN termination device (headend)**
 - Dedicated firewall/VPN security appliance**
 - VPN-enabled router**
 - VPN Service Module (VSM) for LAN switch**
 - SSL Service Module (SSLSM) for LAN switch (NEW)**
- **VPN client / SSL clientless**
 - Software**
 - Hardware**
 - Dynamic (SSL VPN Client)**
 - SSL VPN clientless access**

Design Considerations

- **Firewall Placement & Configuration**
- **Routing**
- **Client Authentication**
- **Address Assignment**
- **Access Control**
- **Monitoring and User Accounting**
- **Management**

Firewall Placement and Configuration Design Consideration

- **Security**

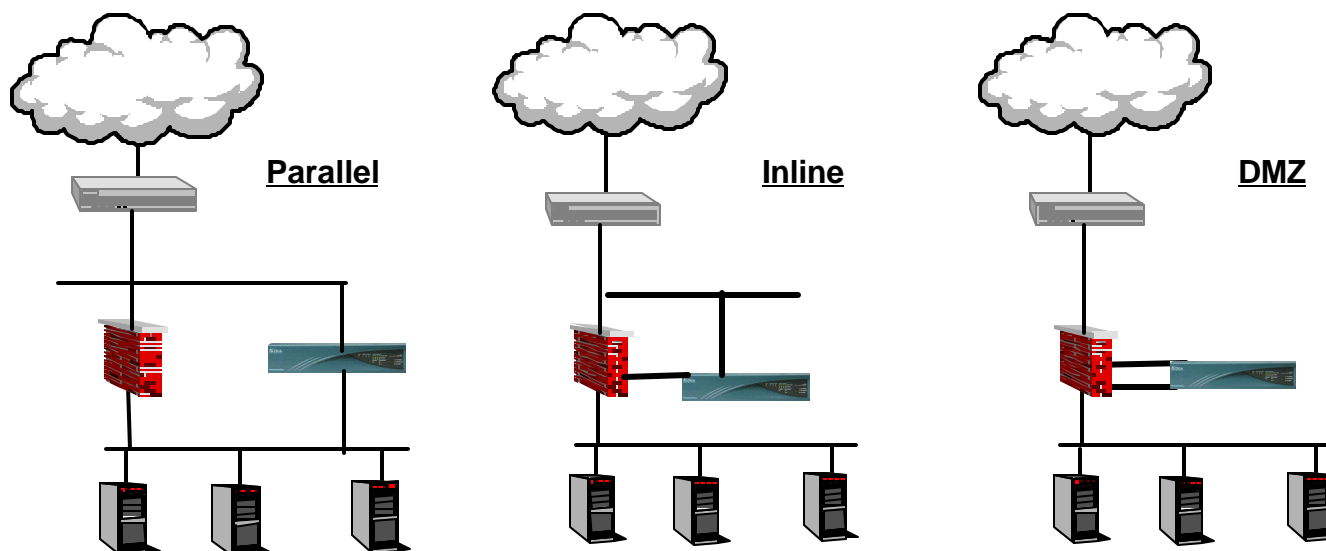
Encrypted traffic can **not** be statefully inspected so:

First limit incoming traffic to IPsec and SSL on firewall

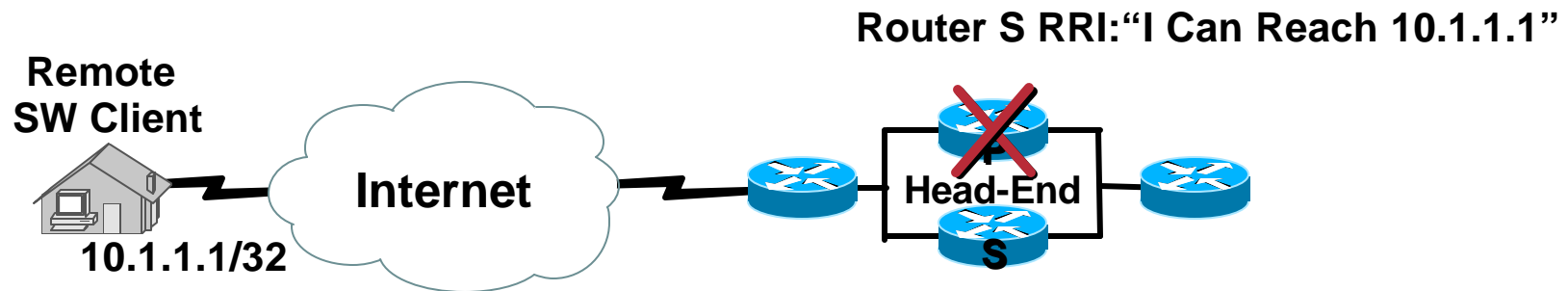
Secondly terminate IPsec tunnel on VPN

Finally send traffic back to firewall for stateful inspection

Enforce endpoint security compliance on remote system



Routing Design Consideration



- Reverse Route Injection (RRI) is used to populate the routing table of internal routers via OSPF or RIPv2
- VPN software clients inject their assigned IP address as hosts routes
- A VPN 3002 Hardware Client connects using Network Extension Mode (NEM) and injects its protected network address; (note that a VPN 3002 Hardware Client in Port Address Translation (PAT) mode is treated just like a VPN Client.
- RRI provides a hold-down route for VPN Client pools / other option is a static route for this pool to the appropriate device

Address Assignment Design Consideration

- **Least complex and most commonly used are internal address pools**
 - Group based address pools may be used to then provide ACLs on an internal firewall based on incoming user**
- **DHCP assignment is another popular choice**
- **Static assignment requires RADIUS or LDAP to deploy**
- **The head-end device will proxy ARP on behalf of all local subnet IP addresses**
- **For non-local subnet IP addresses, the most common configuration is that the internal router(s) have a static route for these address blocks pointing to the head-end device private interface**
 - Optionally, you must use Reverse Route Injection (RRI)**
 - All static IPs that may traverse multiple boxes must be announced as host routes**
- **Clientless users do not receive their own unique IP address, instead their traffic will originate from the head-end interface IP.**

Client Authentication Design Consideration

- **VPNs can utilize many types of databases for centralized authentication**

Username and password

Tokens

Digital Certificate / Smart cards

- **Authenticated against:**

RADIUS

Active Directory (AD)

NT Domain

RSA SecurID

Other One Time Password server (OTP) via RADIUS

Commonly Deployed Authentication Design Considerations

- **Most security conscious customers utilize One Time Passwords (OTPs)**
- **Government and financial customers are also some of the strongest adopters of Digital Certificates or Smartcards for greater security**
- **Customers mainly focused on convenience sometimes authenticate to an internal NT/AD domain controller or static RADIUS password database. Any type of static password configuration leaves the corporation vulnerable to brute force password attacks.**

Access Control Design Consideration

- **Unless your goal is to provide unrestricted network access, it is generally a good idea to provide access control rules for users.**
- **Tunnel based VPN (IPsec and SSL VPN client) provides control at the protocol/port and destination IP level.**
- **Clientless SSL VPN offers more granular access control including URL based access or file server directory level access control (in addition to controls set up via the servers authentication rules). This may be particularly useful for partners.**

Access Control Design Consideration

- **Some companies choose to maintain all access rules on an internal FW based on source IP of the client (addresses are assigned to a specific pool based on group assignment).**
- **Access control rules can generally be defined at a per-group basis on the head-end device (easy to deploy, but more difficult to main large numbers of policies or across multiple boxes) or they can be defined on the head-end RADIUS server. Unfortunately, RADIUS has a 4K packet size limit which makes using a generic RADIUS server for access control challenge. Cisco Secure ACS offers a downloadable ACL feature which can be used with Cisco head-end devices to support large sized policies.**

Monitoring and User Accounting Design Consideration

- **Most customers utilize RADIUS accounting for the purpose of logging user sessions. RADIUS accounting can log who logged in, when they logged in, when they logged out, originating IP, assigned IP and amount of data transmitted.**
- **For more advanced troubleshooting, device SYSLOG output may be logged to an internal server for historical reference and debugging.**

VPN Management Best Practices

Design Consideration

- **Manage out-of-band**

 - Use dedicated management interfaces if possible**

 - If not possible, use VPN for secure management and restrict access over the tunnel to management protocols only**

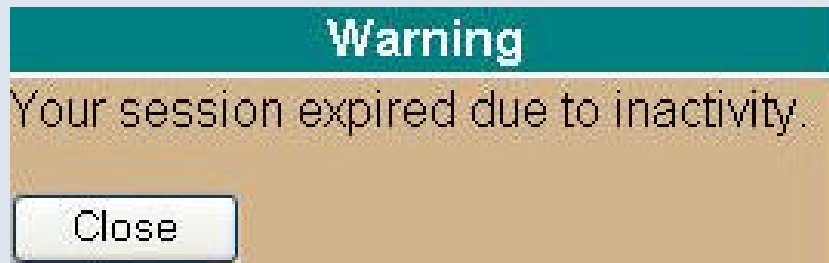
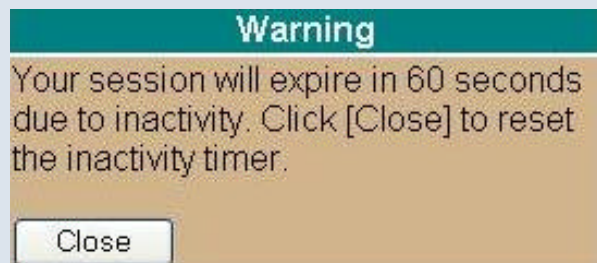
- **When managing a VPN device via a VPN:**

 - Use strong authentication, integrity, and encryption**

 - Use a different username for configuration management and troubleshooting**

 - If you cannot use IPSec, or at least use SSH/SSL encrypted management protocols**

Session Logoff / Idle Timeout Design Consideration



- **SSL VPN requires more stringent session control than IPsec since users are most likely to be accessing the network from public terminals**
- **Session control and termination is paramount to security**
 - **Ensure that users that leave their system or improperly disconnect (system failure or browser suddenly stopped) are properly logged out in order to free up resources for other users and prevent someone else visiting the system from gaining unauthorized network access**
 - **Session control can become challenging if you need to support users that require continuous access**
- **Client based (IPsec and SSL VPN Client) solutions often integrate the ability to determine if a peer has lost its connection; this makes continuous connectivity more practical (DPD—Dead Peer Detection)**
- **Clientless SSL/VPN relies on idle timeout and max connect timers to clean up sessions where the user does not properly disconnect**
- **Deploying a SSL solution without idle timeouts or max connect time may prevent sessions from being cleaned up and will cause unnecessary exposure to your network**

DEPLOYMENT CONSIDERATIONS

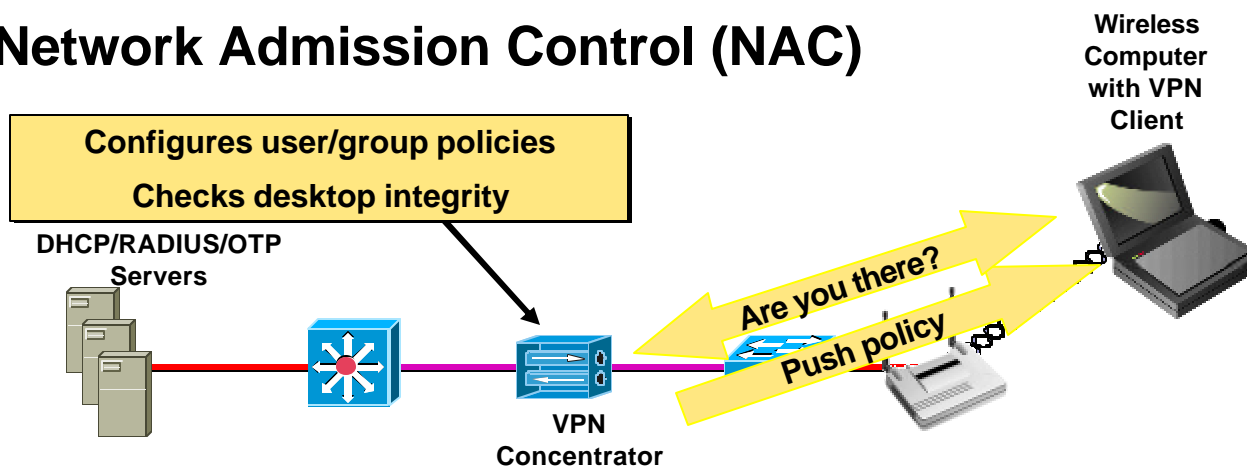


Deployment Objectives

- **Endpoint Security policy enforcement**
 - Network Admission Control (NAC)**
 - Cisco Secure Desktop (CSD)**
- **Security policies**
 - Split Tunneling**
 - Local (LAN) Access**
- **Firewall traversal**
- **Resiliency and availability**
 - Dead Peer Detection (DPD)**
 - HSRP/VRRP**
 - Backup peer list (VPN client)**
 - Remote Access load balancing**
 - Backup LAN to LAN**
- **Unattended mode**

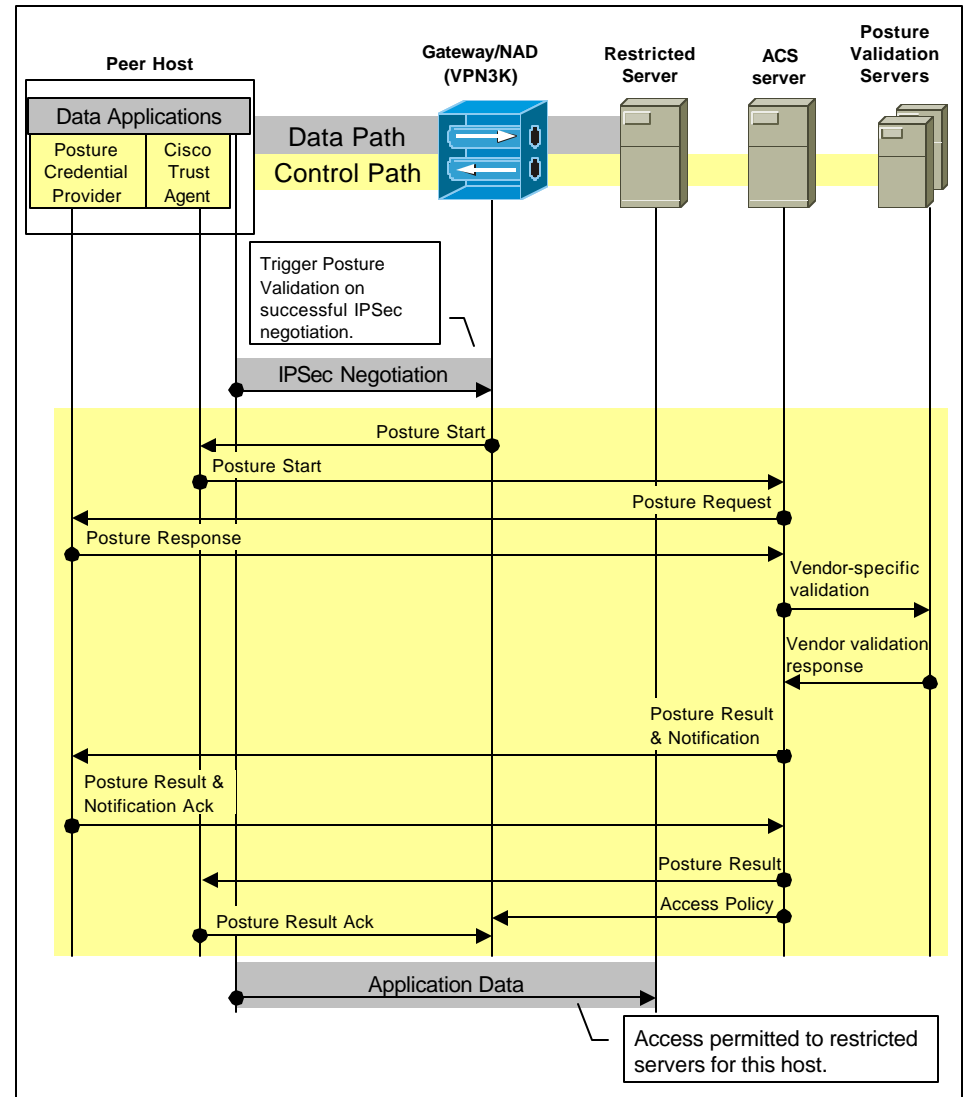
Security Policy Enforcement Deployment Consideration

- **Configure VPN policies for users and groups**
Access control / filters, IP pool, etc
Determine users posture before accessing network resources
Network Admission Control posture verification OR
Personal firewall/antivirus verification, “Are You There?”
- **Enforce desktop policy on end systems**
Integrated Personal Firewall—Policy Push
Network Admission Control (NAC)

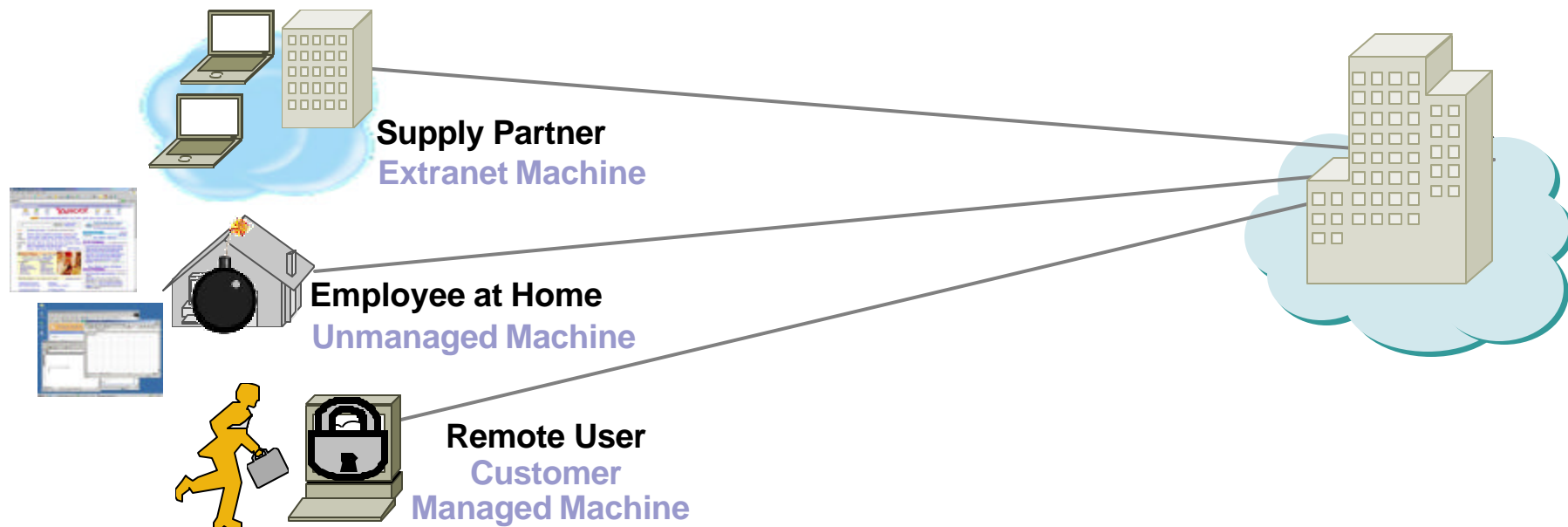


Network Admission Control for IPSec Overview Deployment Consideration

1. **New IPSec connection detected by VPN3K**
2. **VPN3K initiates Posture Validation process**
3. **ACS server receives Posture Credentials and sends access policy – *may* involve Vendor Server**
4. **VPN3K enforces access policy**



Endpoint Control for SSL VPN Deployment Consideration



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?

Protection of Confidential Information

What's Left Behind

Cisco.com

The Risk of VPN on Public Systems

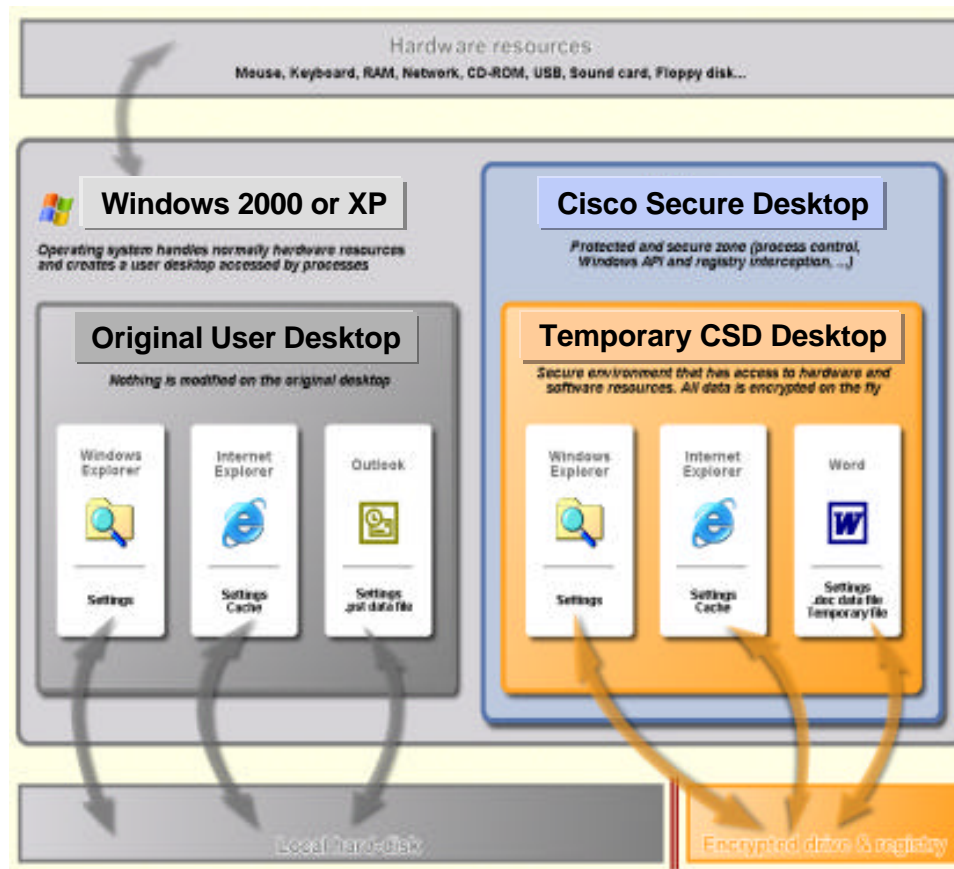
- **Cookies**
 - **Username and passwords**
- **URL history**
- **Page caches**
 - **Sensitive corporate data**
- **Downloaded files**

Cisco Secure Desktop

Comprehensive Endpoint Security for SSL VPN

Cisco.com

- Works with Desktop Guest Permissions
 - No admin privileges required
- Complete Pre-Connect Assessment:
 - Location assessment – managed or unmanaged desktop?
 - Security posture assessment – AV operational/up-to-date, personal firewall operational, malware present?
 - Specific applications running – defined by admin
- Comprehensive Session Protection:
 - Malware detection
 - Data sandbox and encryption protects every aspect of session
- Post-Session Clean-Up:
 - Encrypted partition overwrite (not just deletion) using DoD algorithm
 - Cache, history and cookie overwrite
 - File download and email attachment overwrite
 - Auto-complete password overwrite



Cisco Secure Desktop

How it works

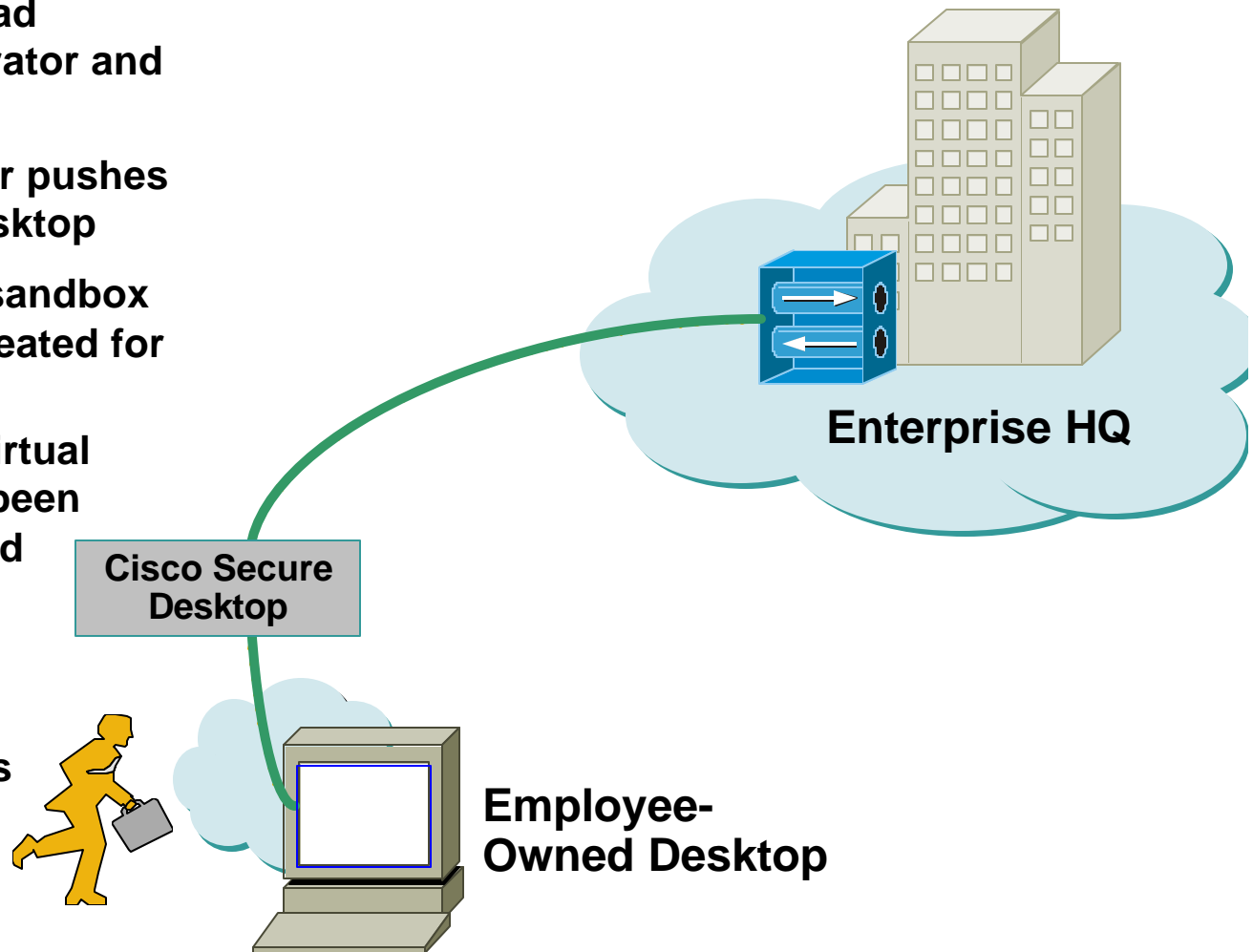
Step One: A user on the road connects with the concentrator and logs in

Step Two: The concentrator pushes down the Cisco Secure Desktop

Step Three: An encrypted sandbox or hard drive partition is created for the user to work in

Step Four: At Logout the Virtual Desktop that the user has been working in is eradicated and the user is notified

Note: CSD download and eradication is seamless to the user. If the user forgets to terminate the session auto-timeout will close the session and erase all session information



Secure Desktop – System Detection Capabilities

Cisco.com

Operating System Detected:

- Microsoft NT 4.0 SP6
- Microsoft Windows 98
- Microsoft Windows ME
- Microsoft Windows 2000 (Original – SP4)
- Microsoft Windows XP (Original – SP2)

Anti-Virus Detected:

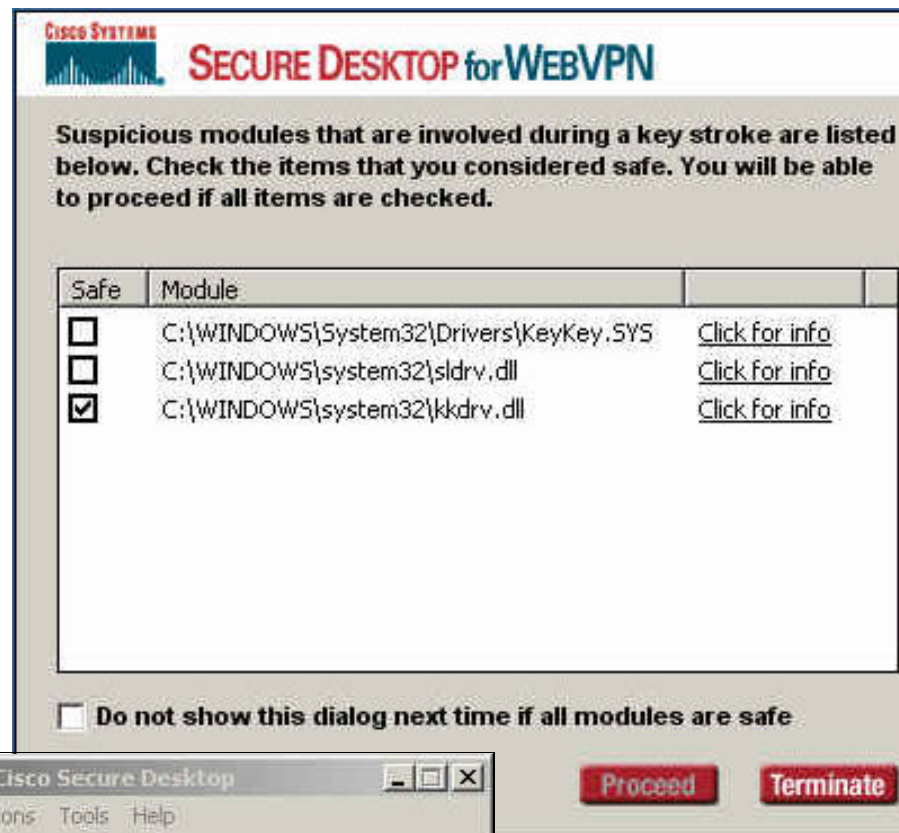
- Norton AntiVirus 2003-2005
- McAfee AntiVirus 7.0-9.0
- eTrust AntiVirus 7.0-2005
- Panda AntiVirus Platinum 7.0-8.0
- Panda AntiVirus Titanium 2004
- PC-Cillin 2003-2004
- F-Secure AntiVirus 2004-2005
- MS Anti Spyware

Personal Firewall Detected:

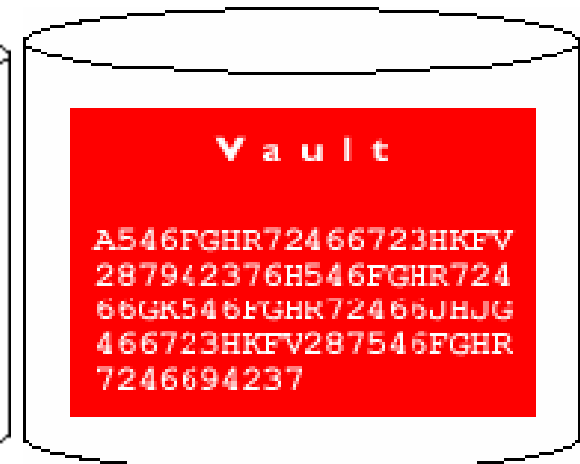
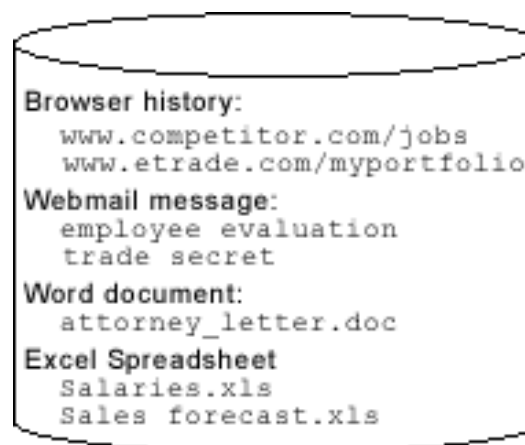
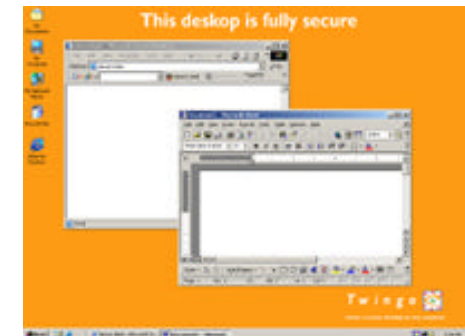
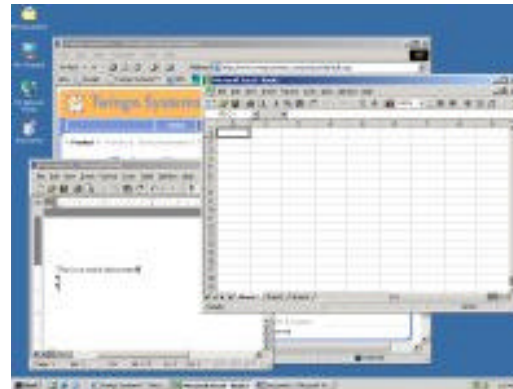
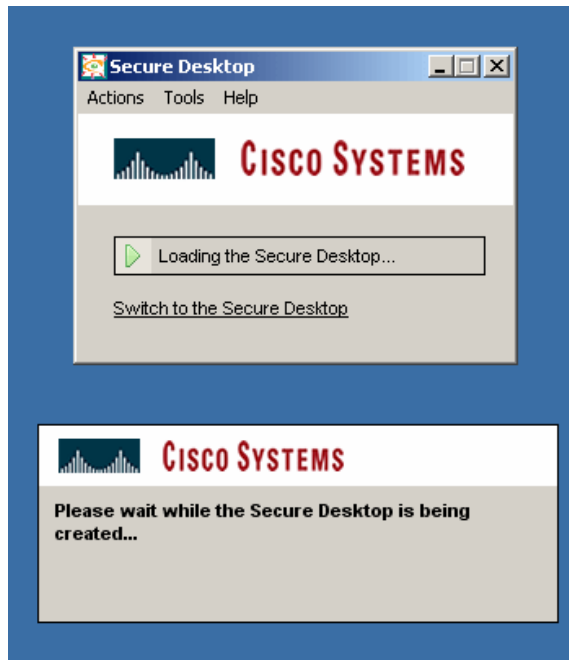
- Norton Personal Firewall 2004-2005
- McAfee Personal Firewall 5.0-6.0
- Sygate Personal Firewall 5.0-5.5
- ZoneAlarm Personal Firewall 4.0-5.0
- Microsoft Internet Connection Firewall SP1-SP2
- BlackICE PC Protector 3.6
- Cisco Security Agent 4.0

Cisco Secure Desktop Keystroke logger (KSL) detection

- At session initiation CSD checks the host system for abnormal drivers indicating the presence of keystroke logging programs
- CSD prompts the user to select and terminate the suspicious modules before loading the Secure Desktop
- If the user does not acknowledge that all unrecognized keystroke loggers are safe, the connection will not establish
- User is notified during the session if a keystroke logger is attempting install from within the secure desktop
- CSD can also be configured to check for the Microsoft AntiSpyware Software as part of its pre-connection host checking capability



Secure Desktop in action



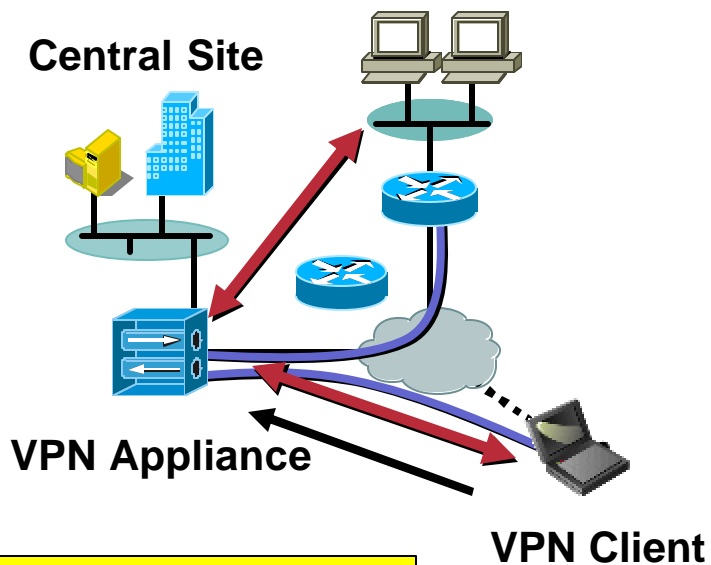
Only around 500kB, the Secure Desktop is set up in less than 15 seconds
And does not require neither administrative privileges nor reboot

Split Tunneling

Remote Access Client or Device

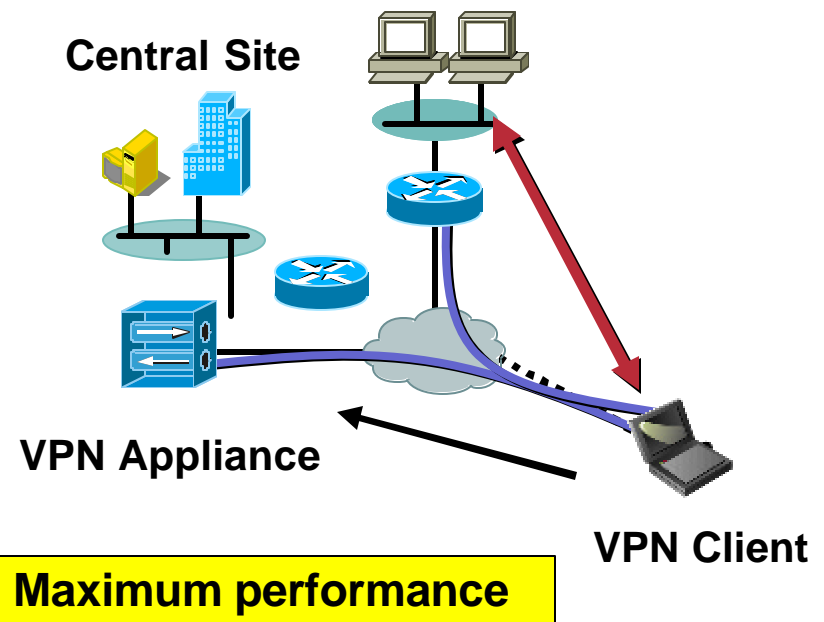
Without Split Tunneling

<http://www.cisco.com/>



With Split Tunneling

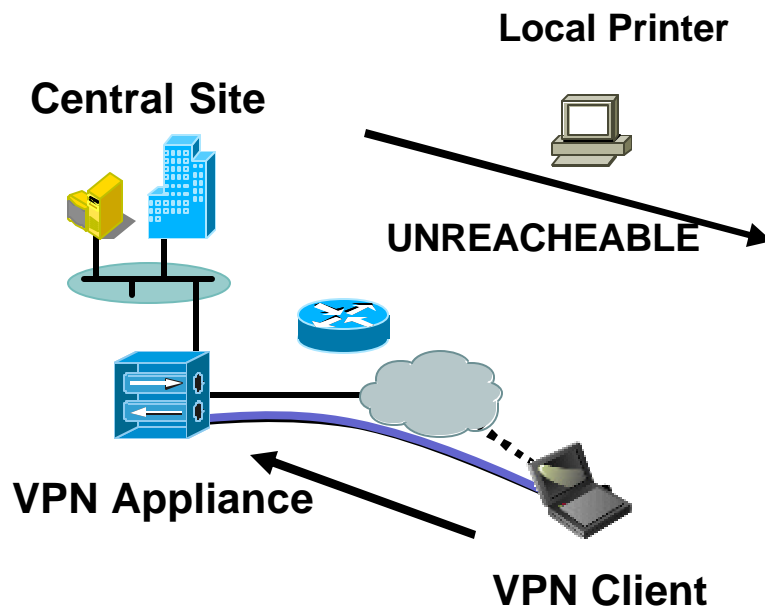
<http://www.cisco.com/>



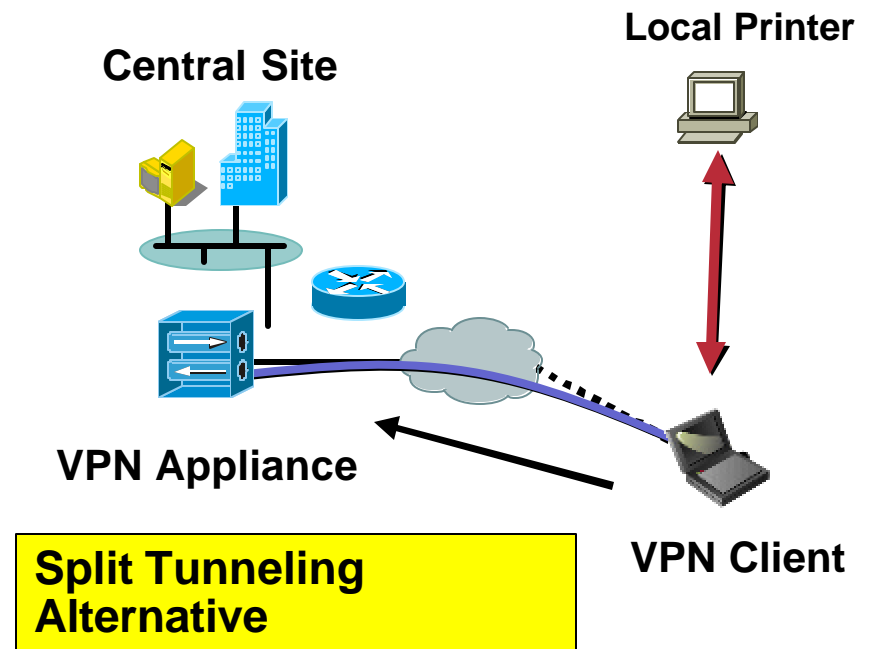
Local (LAN) Access

Remote Access Client or Device

Without Local LAN Access



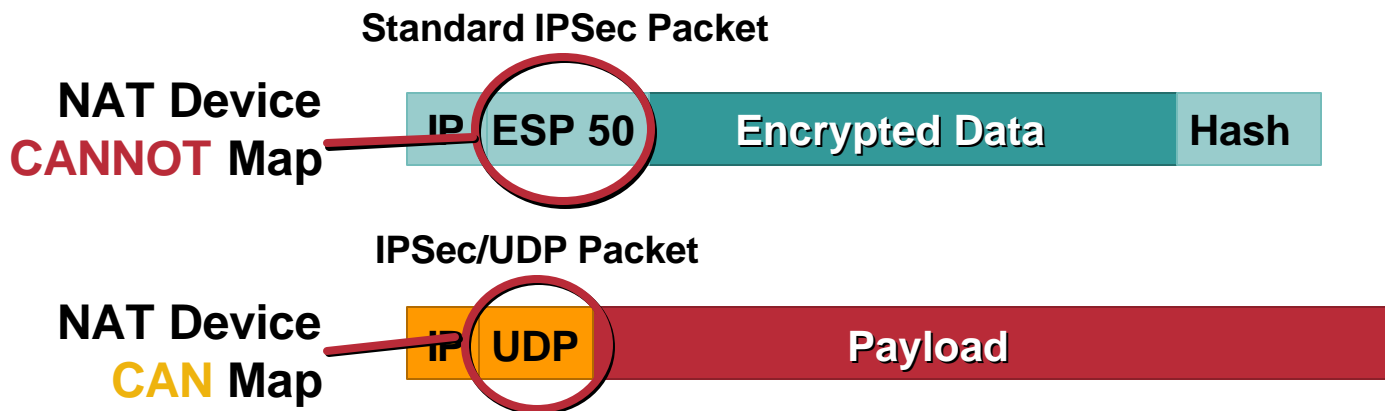
With Local LAN access



IPSec VPN and NAT/PAT Transparency

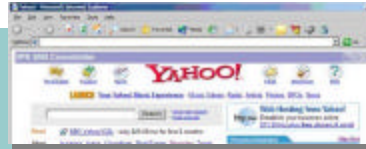
IPSec/UDP

- Allows clients to operate behind a NAT/PAT device
- It uses a UDP or TCP header with configurable port number to bypass PAT devices (default port 10,000)
- Provides the security of IPSec/ESP
- Requires no user intervention as administrator centrally controls IPSec/TCP or IPSec/UDP via group policies



Firewall Traversal

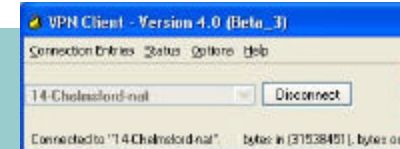
SSL VPN



- HTTPS (TCP 443)
- HTTP (TCP 80)
- (If HTTP redirection desired)

THE PORTS AND PROTOCOLS LISTED MUST BE OPEN FOR A REMOTE USER TO BE ABLE TO CONNECT SUCCESSFULLY; HTTPS (TCP 443) WILL BE OPEN THROUGH MOST NETWORKS WHILE THE PROTOCOLS REQUIRED FOR IPSEC MAY NOT BE OPEN BY DEFAULT ON A NETWORK THAT OUTBOUND PERFORMS FILTERING

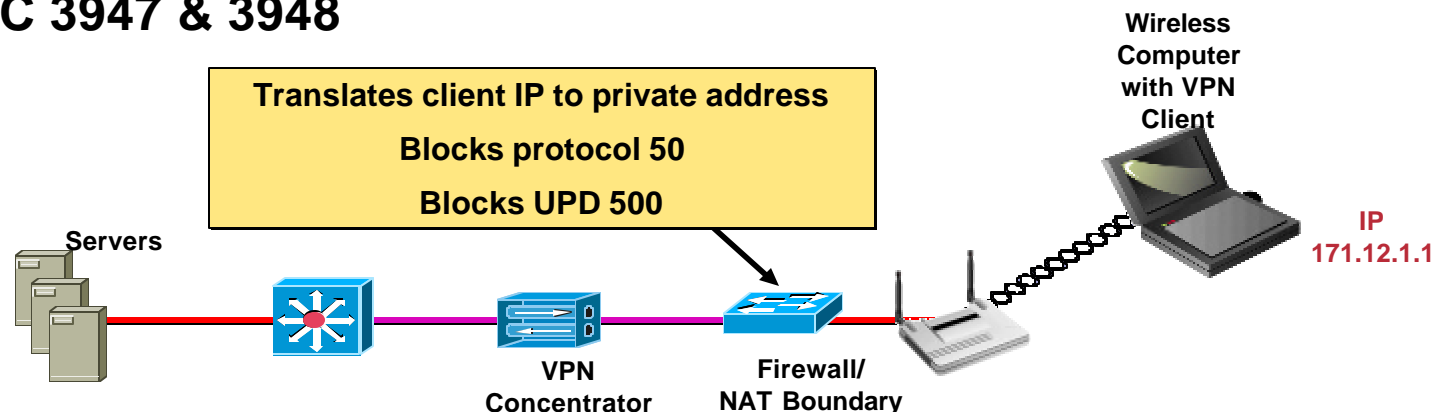
IPSec VPN



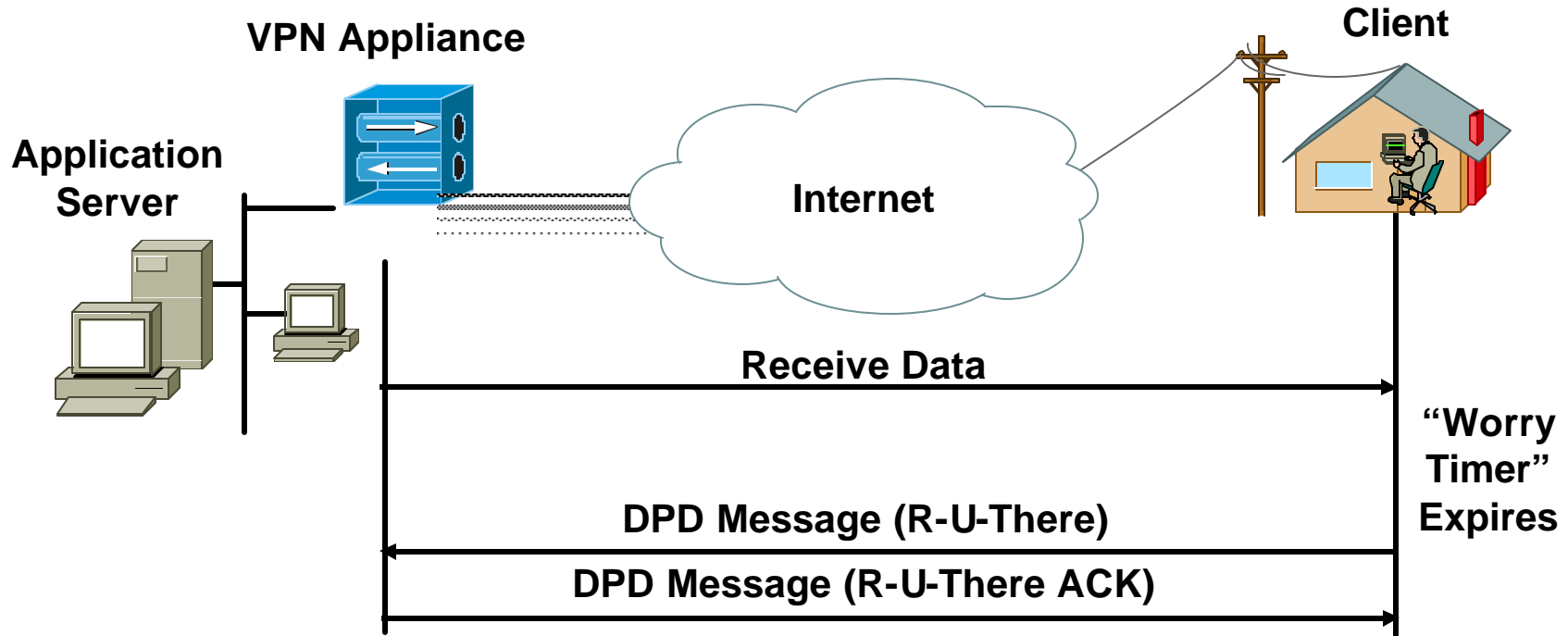
- **Standard IPSec**
 - ESP (Protocol 50)
 - IKE (UDP 500)
- **Standard NAT/PAT Traversal**
 - IKE (UDP 500)
 - ESP over UDP (UDP 4500)
- **Proprietary TCP Encapsulation**
 - Administrator defined TCP port(s)

NAT Traversal (NAT-T)

- During IKE phase I negotiation, special NAT discovery payload is used to discover the existence of NAT and location of NAT device
- If there is NAT, encapsulate ESP packet as UDP payload (UDP/4500)
- ISAKMP NAT keepalive is sent to keep NAT entry from timeout
- Order of Precedence—IPSec-over-TCP -> NAT-Traversal -> IPSec-over-UDP solution
- IETF RFC 3947 & 3948

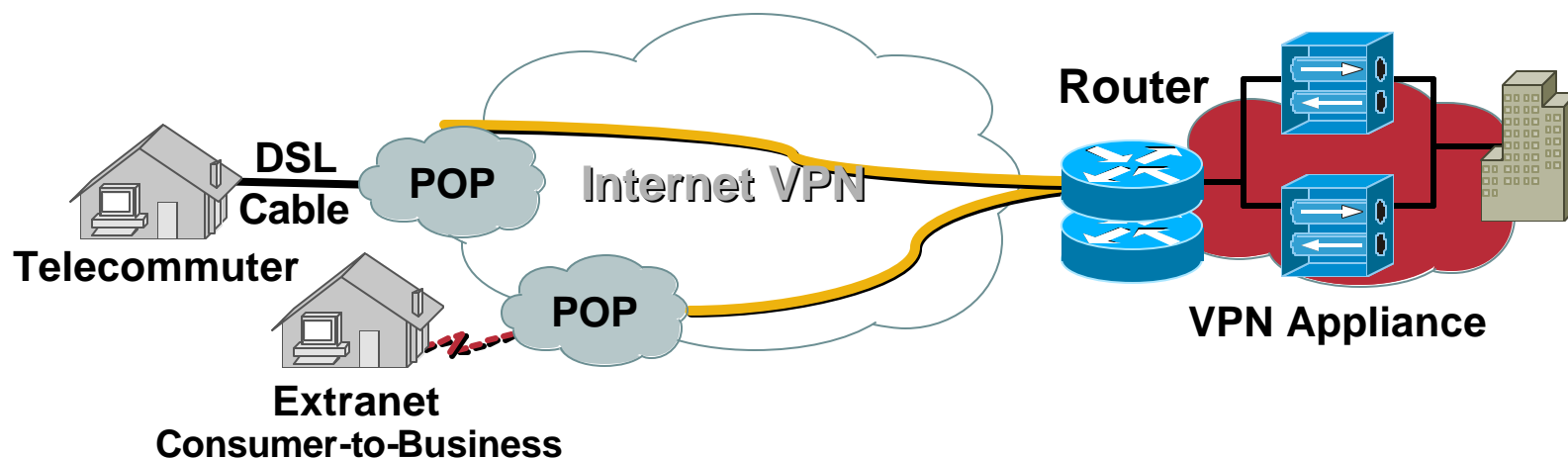


IKE Keepalives Dead Peer Detection (DPD)



DPD is the only reachability mechanism available for remote access clients
Make sure the headend devices support the same type of keepalives
RFC 3076

HSRP/VRRP Deployment Consideration



HSRP

- Available in Cisco IOS
- Active-active failover
- Reverse route injection (RRI) is required for the hosts behind HSRP routers to track tunnel states

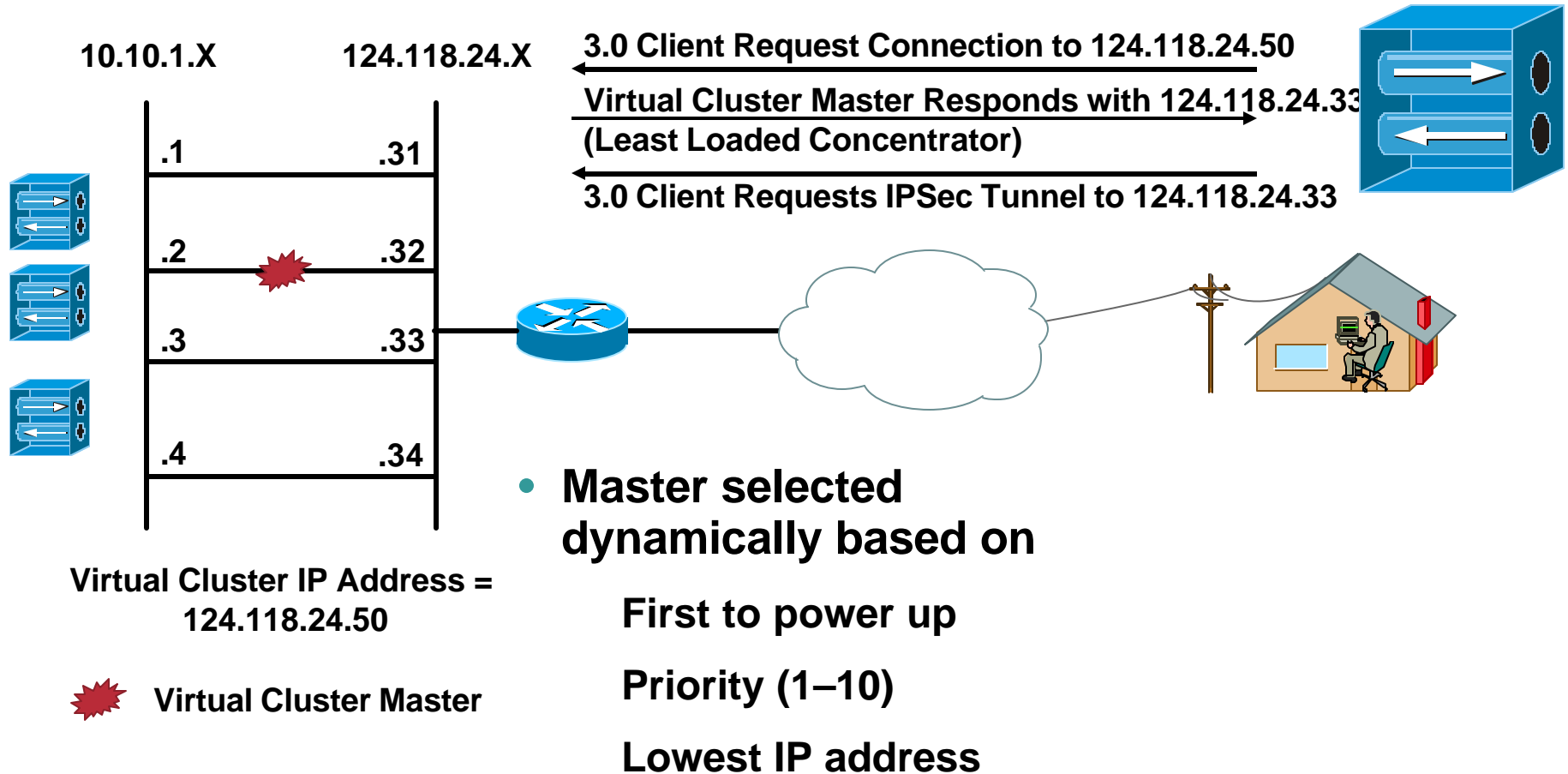
VRRP

- VRRP supported by VPN 3000 concentrator
- PIX failover is similar to VRRP mechanism
- Active-standby failover

Local/Geographical Failover/ Load-Balancing

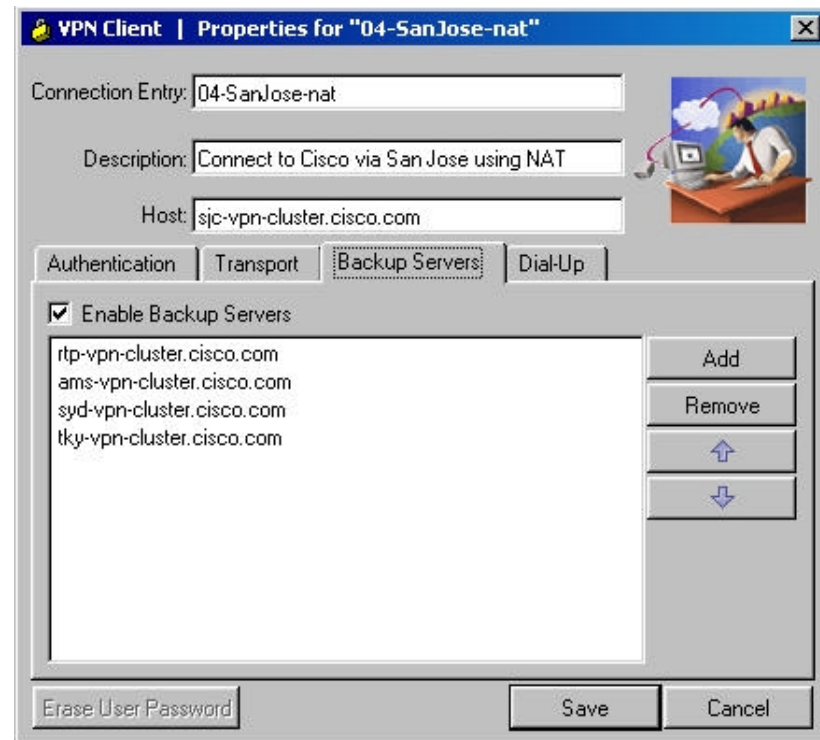
- **The Cisco VPN Client supports the notion of backup servers for high availability**
PIX, 3000, and Cisco IOS compatible
- **The VPN concentrator and PIX 7.0+ also support local clustering**
Supports local load sharing (not geographical)
DNS resolution-based load balancing could also be used as the client resolves the FQDN of the head-end device (geographical)

Local/Geographical Failover/ Load-Balancing



Backup Peers

- **Configure locally or pushed from head end**
- **Locally**
 - It can be part of client install script**
- **Headend**
 - Configuration -> User Management -> Group -> IPSec Backup Servers**



Backup LAN-to-LAN

- **On the VPN 3000 Concentrator, VRRP and Load Balancing may not be used on the same device**
- **For backup Lan-to-Lan configurations, you can define a server list that will be tried in case of a failure to connect**
- **For this feature to operate properly, Reverse Route Injection (RRI) must be used at the head-end. The head-ends must be configured as connection answerers only. The remote site must set up to be the connection originator.**

Unattended connectivity mode

- **Kiosk or back office application that typically connected over a leased line or dial-up**

Examples include: ATMs, Lottery machines, other various remote kiosk machines

- **Connections need to be able to be established without user intervention (saved credentials, certificates, or API authentication pass through)**
- **Connection migration to internet based VPN desired**

- **Options:**

IPSec VPN Client Auto-initiation – simple to deploy, limited flexibility

VPN Client API – more complex to initially deploy, unlimited flexibility

WIRELESS LAN (WLAN)



When to Consider Using VPNs with Wireless

- **Remote access users on a public networks**
- **Enterprise-class deployments**
- **High concerns for data**
 - Confidentiality (encryption)**
 - Integrity (packet authentication)**

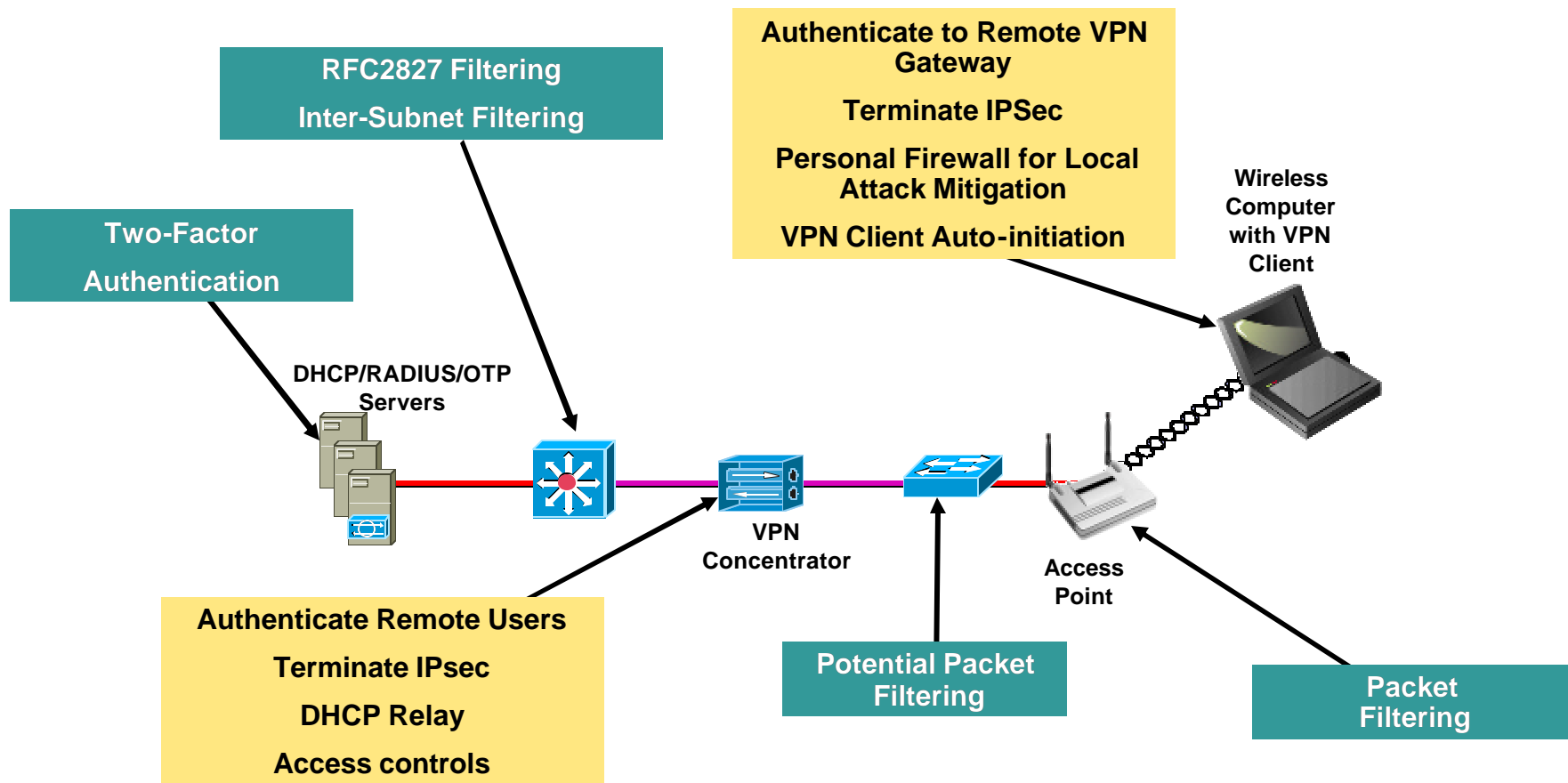
Wireless Encryption Technology Comparison

	Cisco LEAP with TKIP	EAP-TLS with TKIP	EAP-PEAP with TKIP	IPsec VPN	SSL VPN
Key length (in bits)	128	128	128	168/128, 192, 256	40/128, 56/168
Encryption algorithm	RC4	RC4	RC4	3DES or AES	RC4 or 3DES
Packet integrity	CRC-32/MIC	CRC-32/MIC	CRC-32/MIC	MD5-HMAC/SHA-HMAC	SHA-HMAC
Device authentication	No	Certificate	No	Pre-shared secret or certificates	Certificate
User authentication	Username/password	Certificate	Username/password or OTP	Username/Password, OTP, certificate	Username/Password, OTP, certificate
User differentiation	Group	Group	Group	User and Group	User and Group
Client OS support	Wide range	Wide range	Wide range	Wide range	"Clientless"
Open standard	No	Yes	IETF draft RFC	Yes	Yes

Benefits of Using IPSec VPN over WLAN

- **Secure transport throughout campus**
Data integrity ensured for all traffic
- **Able to utilize any existing VPN gateways**
- **Desktop security policy enforcement**
Personal firewall, etc.
- **Secure WLANs via “internal facing” VPNs**
- **Maximum available security**
Extensive Layer 3 and 4 filtering
- **Works with all NICS**

IPSec Security Overlay Services for WLAN



Source: Cisco SAFE Wireless LAN Security

Wireless Threats Mitigated by VPN

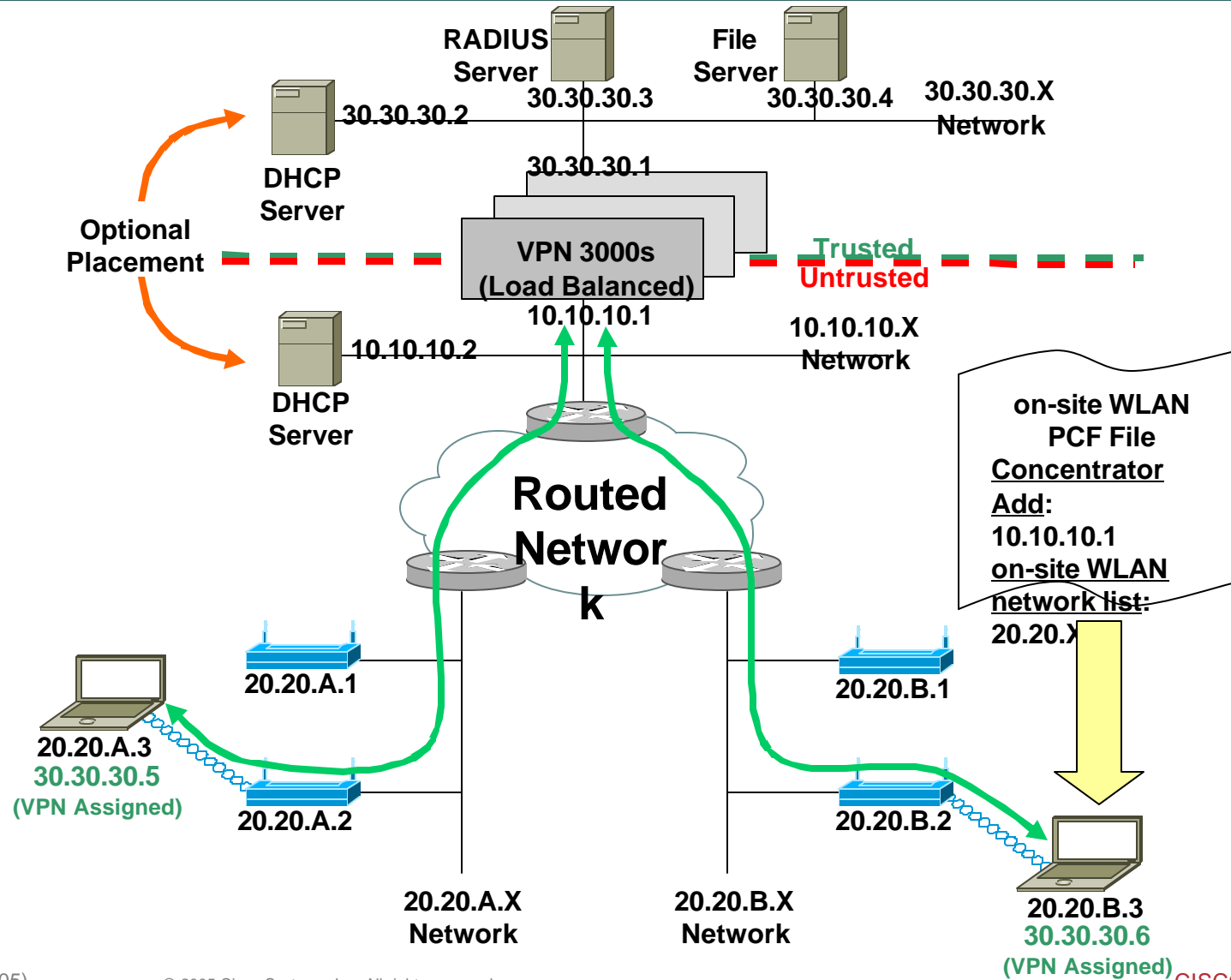
- **Wireless packet sniffers**
- **Man in the Middle (MITM)**
- **Unauthorized access**
- **IP spoofing**
- **ARP spoofing**
- **Password attacks**
- **Topology discovery**

Source: Cisco SAFE Wireless LAN Security

Auto-Initiation for WLAN

- **Automated security for WLAN**
 - Active when PC wakes from standby or hibernate
 - Detects it's on-site a wireless LAN
 - Establishes VPN tunnel for the network
- **Connectivity transparent to user**
 - Other than authentication
- **Vendor/technology agnostic**
 - Client NICs
 - Access points
 - WLAN technology: 802.11a/b/....

Client Auto-Initiation for "Onsite WLAN"



Benefits of Using SSL VPN over WLAN

- **No manual software deployment**
- **Easy firewall traversal from any location**
- **Anywhere access**
- **Seamless wireless roaming since session isn't locked to IP**
- **Access from non-corporate machines**
- **Customized user portals**
- **Granular access control**

CASE STUDY



Company Charter

- **VPN will be deployed for employees and partners that require access to Company network resources over an Internet connection. Employees may access the network from Corporate or non Corporate-managed assets.**

Company Infrastructure

Cisco.com

- **Existing infrastructure**

- 200+ partners require connectivity**

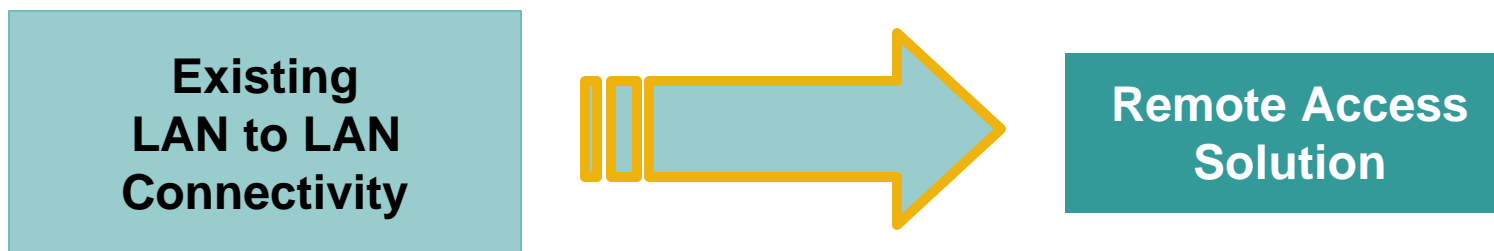
- 10,000 total worldwide employees**

- US, Americas, Europe and Asia regions**

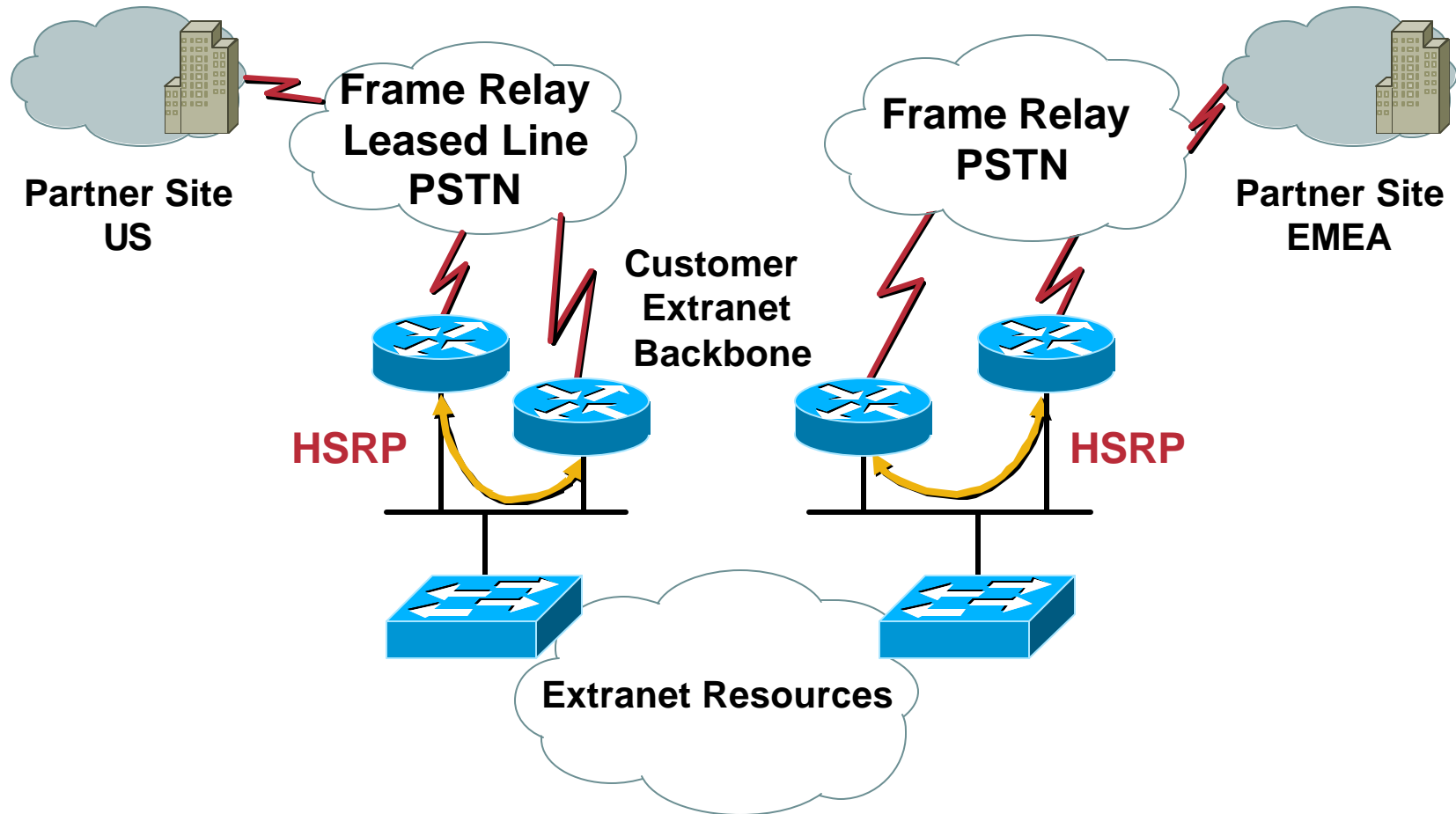
- Access to engineering and manufacturing resources from Extranet partners**

VPN Design Goals

- **Elimination of telecom costs for clients by eliminating the need for long distance and 800# access charges**
- **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 employees and partners (i.e. telecommuters)**
- **Increases Company network/resource security by transitioning users with dial-in or leased-line access to user-based VPN solution**



Existing Topology



Company 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

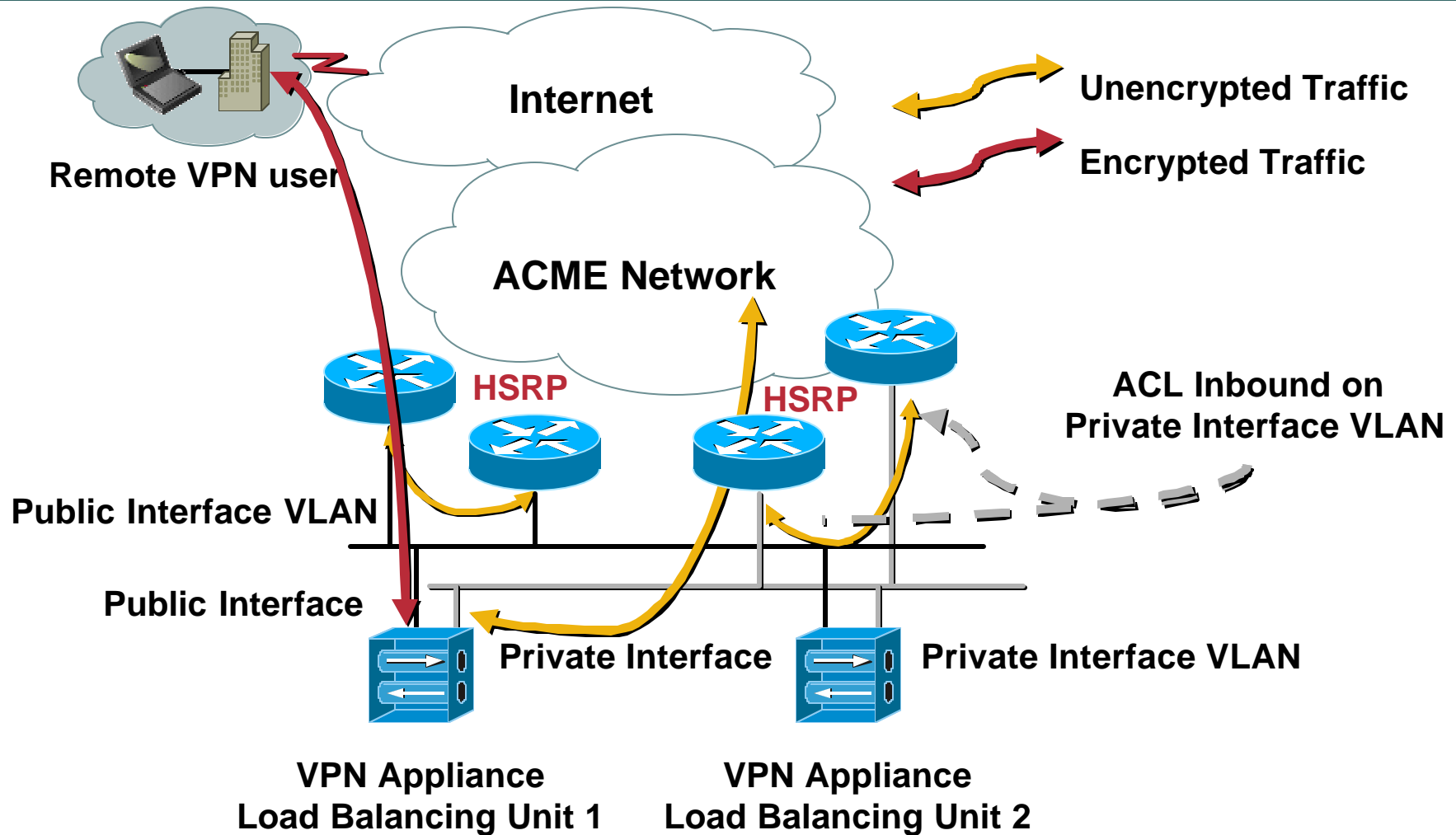
 - HTTP, FTP and other traffic

- **PSTN network**

 - Head-end: access server—PRI lines

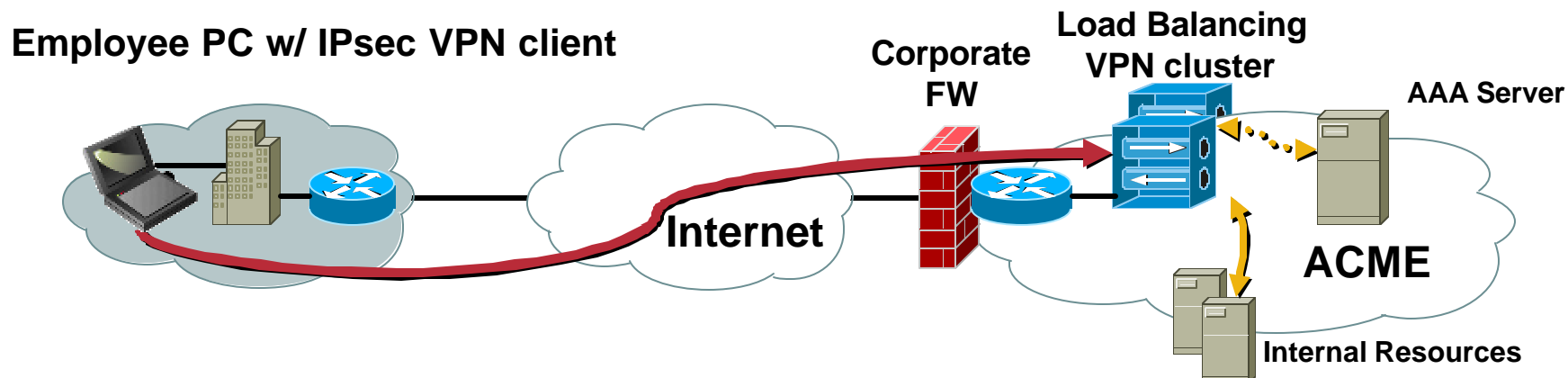
 - Remote sites: 128K ISDN & analog dial-up

VPN Design: Architecture



VPN Design: Employee Connection Flow (Corporate Asset)

Cisco.com

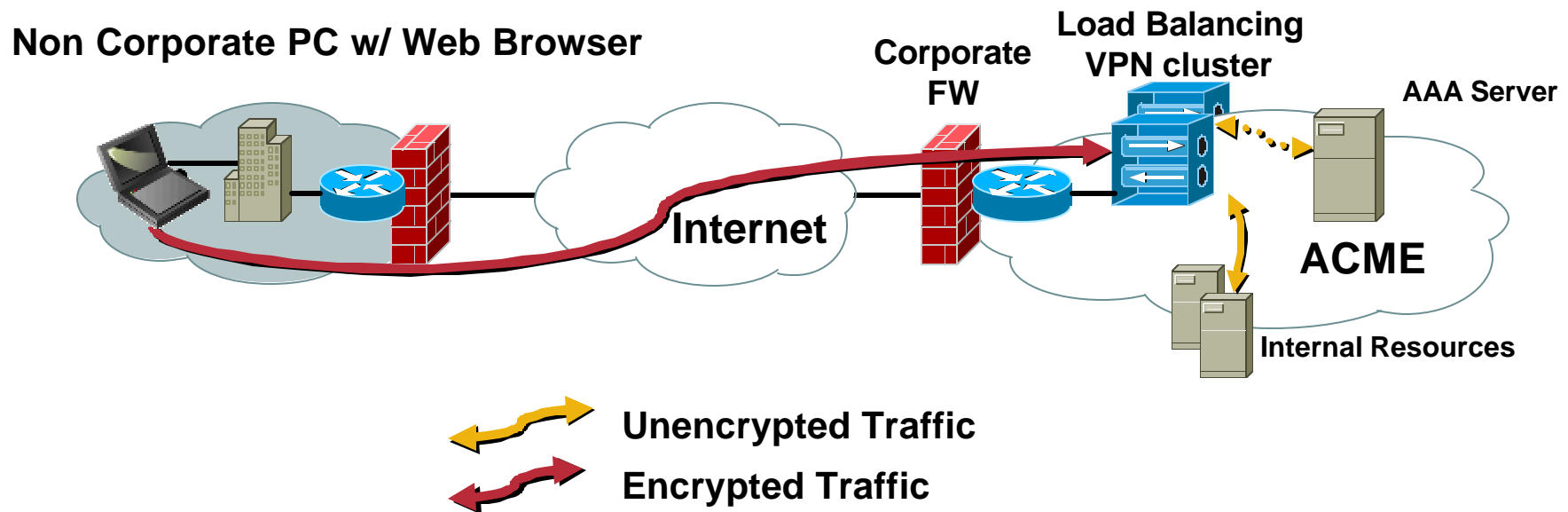


1. Two factor authentication with SoftToken
2. Group authentication and user authentication to token server (AAA)
3. IPsec VPN client authenticated by AAA server
4. Policy push for the VPN SW client
5. Network Admission Control (NAC) compliance checked
6. IPSec tunnel terminates on central site VPN cluster
7. Traffic from client, between VPN cluster and internal resources is unencrypted
8. Authentication data is unencrypted, but generally protected via AAA specific protocol






VPN Design: Partner or Non-Corporate Owned Asset Connection Flow

Cisco.com






1. Two factor authentication with SoftToken
2. Corporate asset check and AV/PFW compliance via Cisco Secure Desktop (CSD)
3. Remote user's web browser authenticated by AAA server
4. Automatic push of SSL VPN Client if desired for full network access
5. VPN tunnel terminates on central site VPN cluster
6. Traffic from client, between VPN cluster and internal resources is unencrypted
7. Authentication data is unencrypted, but generally protected via AAA specific protocol
8. All data wiped out if desired at termination of connection

Design Key Features

Key Features	VPN Client with VPN Concentrator
Resiliency 	<ul style="list-style-type: none">• Load balancing Provides for stateless failover and capacity growth• IPsec VPN Client Backup server list for each geography including Dead Peer Detection (DPD)
Scalability 	<ul style="list-style-type: none">• Scalable user support available with hardware acceleration• Load balancing clusters• Policy push for each remote user• Users organized into various groups with appropriate security policy profiles and user authentication and authorization information• Resiliency with multiple concentrators located on the same network
Management 	<ul style="list-style-type: none">• Device Monitoring, Wizard Setup, and Advanced Configuration via Web-Based GUI and/or Command Line Interface (CLI); Multiple Device Monitoring

Design Key Features (Cont.)

Key Features	VPN Client with VPN Concentrator
Identity 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Cisco VPN client for Microsoft Windows 95, 98, ME, NT, 2000, XP • For Linux (Intel), Solaris (UltraSPARC-32 bit), MAC OS X 10.X • Microsoft PPTP/MPPE in Windows 95, 98, ME, NT, Windows 2000, and XP • Microsoft Windows 2000 and XP Native IPsec Client • Clientless SSL VPN with optional Port Forwarding feature • SSL VPN Client (Windows 2000 and XP) • Hardware Clients Are Operating Systems Independent
Consolidated Solutions 	<ul style="list-style-type: none"> • Remote Access VPN Concentrator, Stateless Packet Filter, Site-to-Site VPN Gateway, Outbound NAT Device (Non-Static), Integrated Local Logging and Accounting

Conclusions

- **Cost saving**
 - Monthly cost to subscribe to Internet
 - Initial equipment cost is re-captured by monthly savings
 - Deploy VPN software, clientless, dynamic client or hardware clients
- **Security**
 - Run personal firewall on all clients
 - Push policy in effortless manner
 - Endpoint integrity compliance via Network Admission Control (IPSec) or Cisco Secure Desktop (CSD)
- **Scalability**
 - VPN appliances can be added to load balancing cluster at head-end
 - VPN software client is downloaded from Cisco.com
 - VPN hardware client
- **Flexible design**
 - Future growth and resiliency with multiple geographic sites

Q AND A

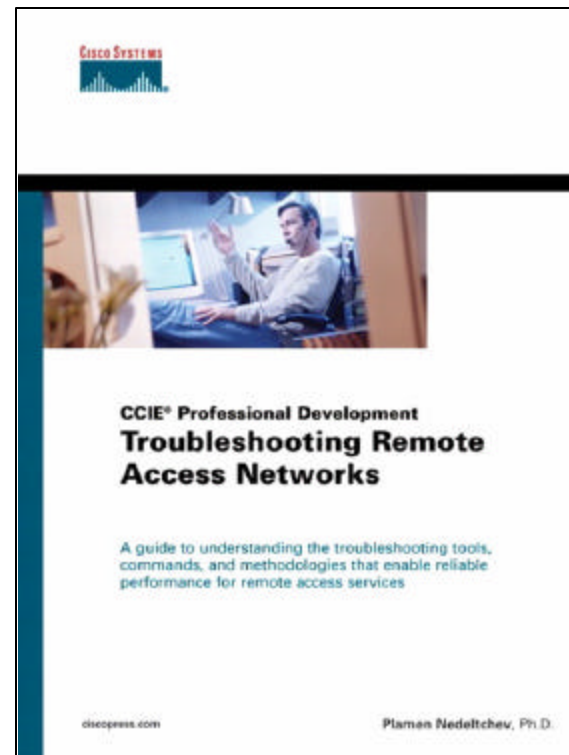


Reference Material

- **Cisco SAFE: Blueprints for VPN and Remote-User Networks**
www.cisco.com/go/safe
- **Cisco IT @ Work: Remote Access VPN Case Study**
<http://www.cisco.com/go/ciscoitatwork>
- **Cisco Remote Access VPN Solutions**
www.cisco.com/go/evpn
- **Cisco WebVPN Solutions**
www.cisco.com/go/sslvpn
- **Cisco VPN Client**
www.cisco.com/go/vpnclient
- **Cisco VPN 3000 Product Line**
www.cisco.com/go/vpn3k
- **Network Admission Control (NAC)**
www.cisco.com/go/nac
- **Configuring Cisco Automatic VPN Initiation**
http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/4_6/admin/vcach4.htm

Recommended Reading

- **Troubleshooting Remote Access Networks**
ISBN: 1-58705-076-5
- **CCSP Cisco Secure VPN Exam Certification Guide**
ISBN: 1-58720-070-8
- **Cisco Secure Virtual Private Networks**
ISBN: 1-58705-145-1
- **Network Security Architectures**
ISBN: 1-58705-115-X
- **Troubleshooting Virtual Private Networks**
ISBN: 1-58705-104-4



Complete Your Online Session Evaluation!

Cisco.com

Por favor, complete el formulario de evaluación.

Muchas gracias.

Session ID: SEC-2010

**DEPLOYING REMOTE ACCESS
IPSEC AND SSL VPNS**

CISCO SYSTEMS

