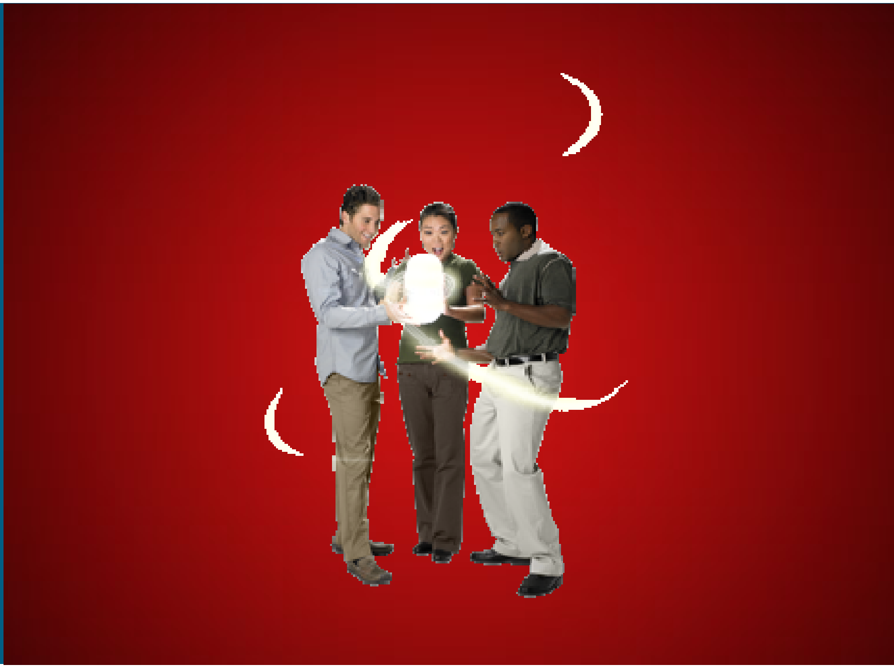
Deploying Remote-Access SSL & IPsec VPNs

BRKSEC-2010

Agenda

- Introduction to Remote Access VPNs
- Design Considerations
- Deployment Considerations
- Endpoint Security
- Q and 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)

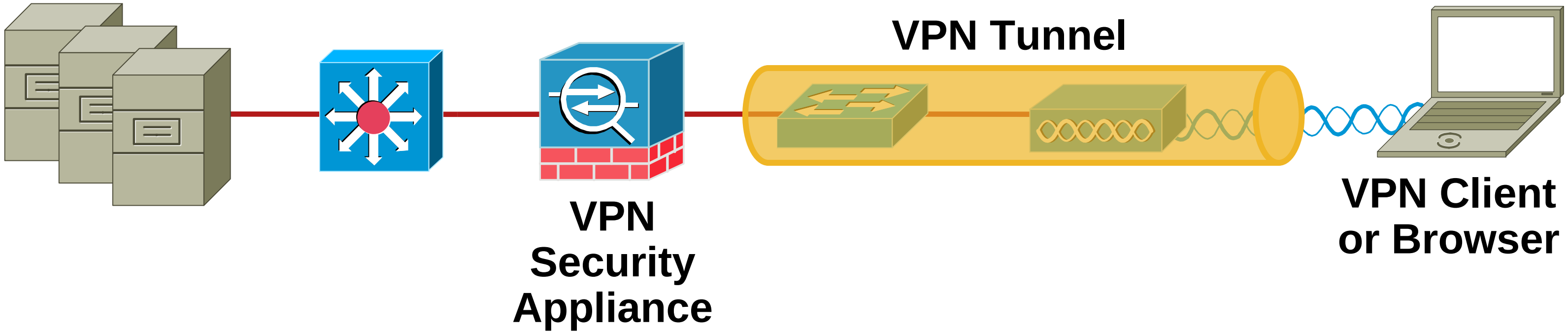
  Integrity (unaltered/tampered)

  Confidentiality (unread)

- Remote Access (RA) VPN components

  Client (mobile or fixed)

  Termination device (high number of endpoints)



Remote Access VPN over the Internet

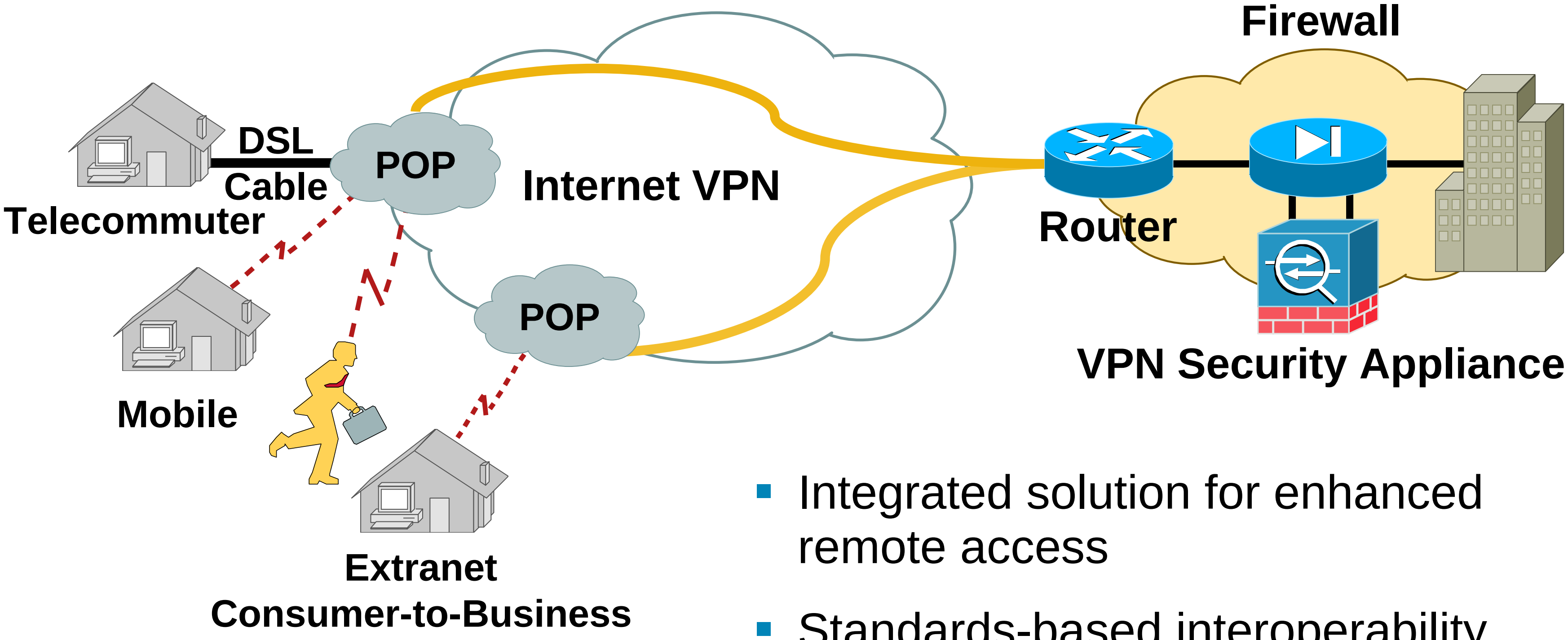
Remote Access Client

Cisco VPN Clients

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

Enterprise—Central Site

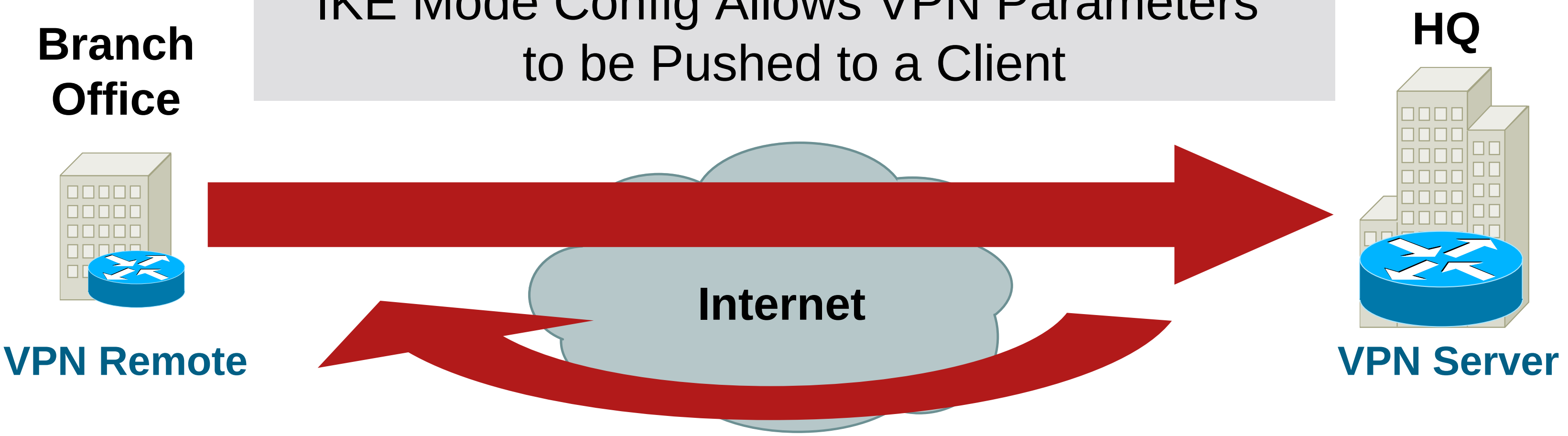
Router, Firewall, and
VPN Security Appliance: VPN Tunnel Termination



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

Easy VPN (IPsec) Implementation

IKE Mode Config Allows VPN Parameters
to be Pushed to a Client



Dynamically Updated:

- Central services and security policy
- Offload VPN function from local devices
- Client and network extension mode

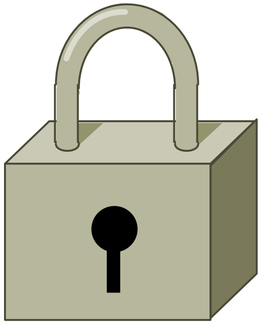
- **Internal IP Address**
- **Internal Network Mask**
- **Internal DNS Server**
- **Internal WINS Server**
- **Split Tunneling**
- **IPsec Transforms**

Centralized Control:

- Configuration and security policy pushed at the time of the VPN tunnel establishment

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

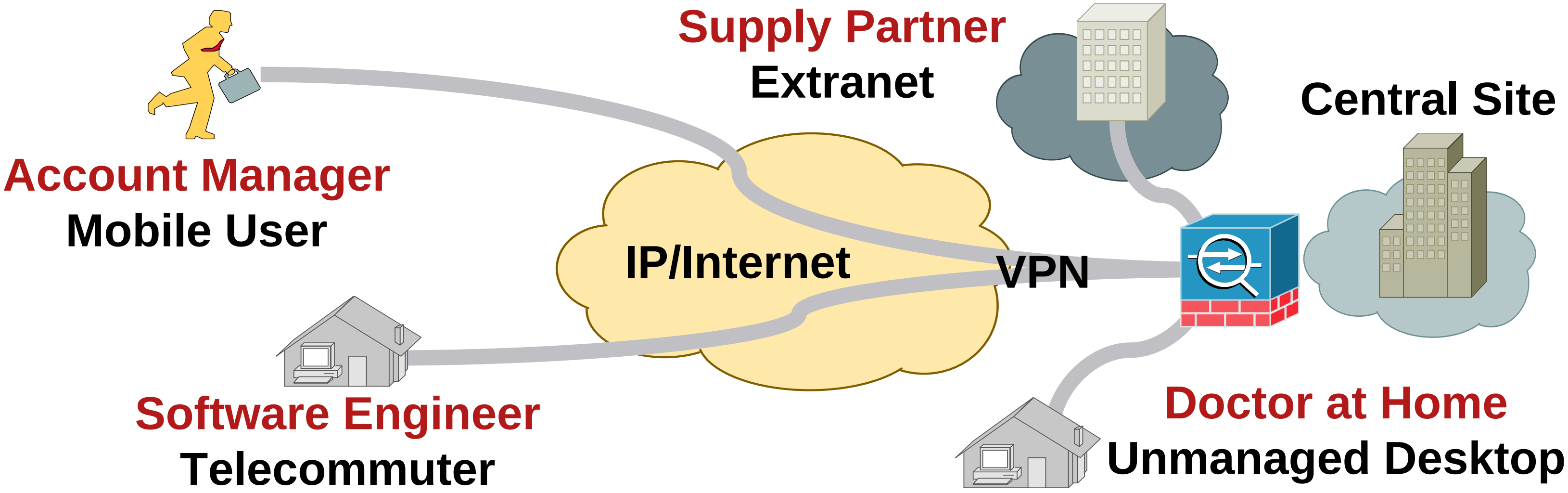


Understanding Your Remote Users

- 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

IPsec and SSL VPN Support Diverse User Populations



Clientless (L7) Clientless/AnyConnect VPN Client	Full Network Access (L3) Cisco 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

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/Mac OS X/iPhone VPN Client)

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

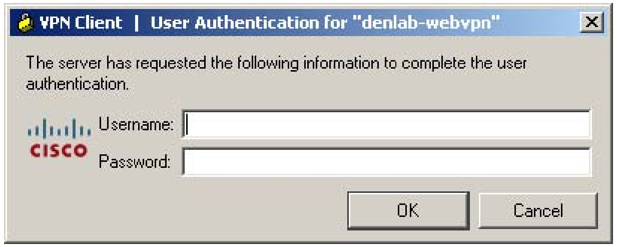
  IPsec/ESP is used to provide secure transport

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

Cisco VPN Client (IPsec Client)

Provisioning and Customization

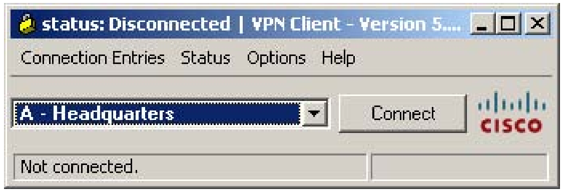
- Localized client
- Predefined profiles and policy configuration
- Admin defined graphics
- Simple mode
- Customizable MSI package



The server has requested the following information to complete the user authentication.

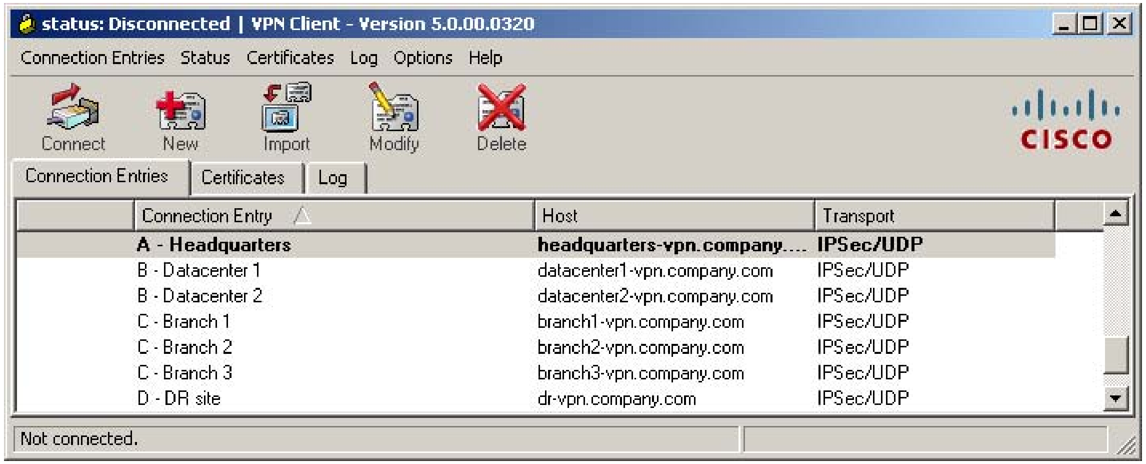
Username:

Password:



A - Headquarters

Not connected.

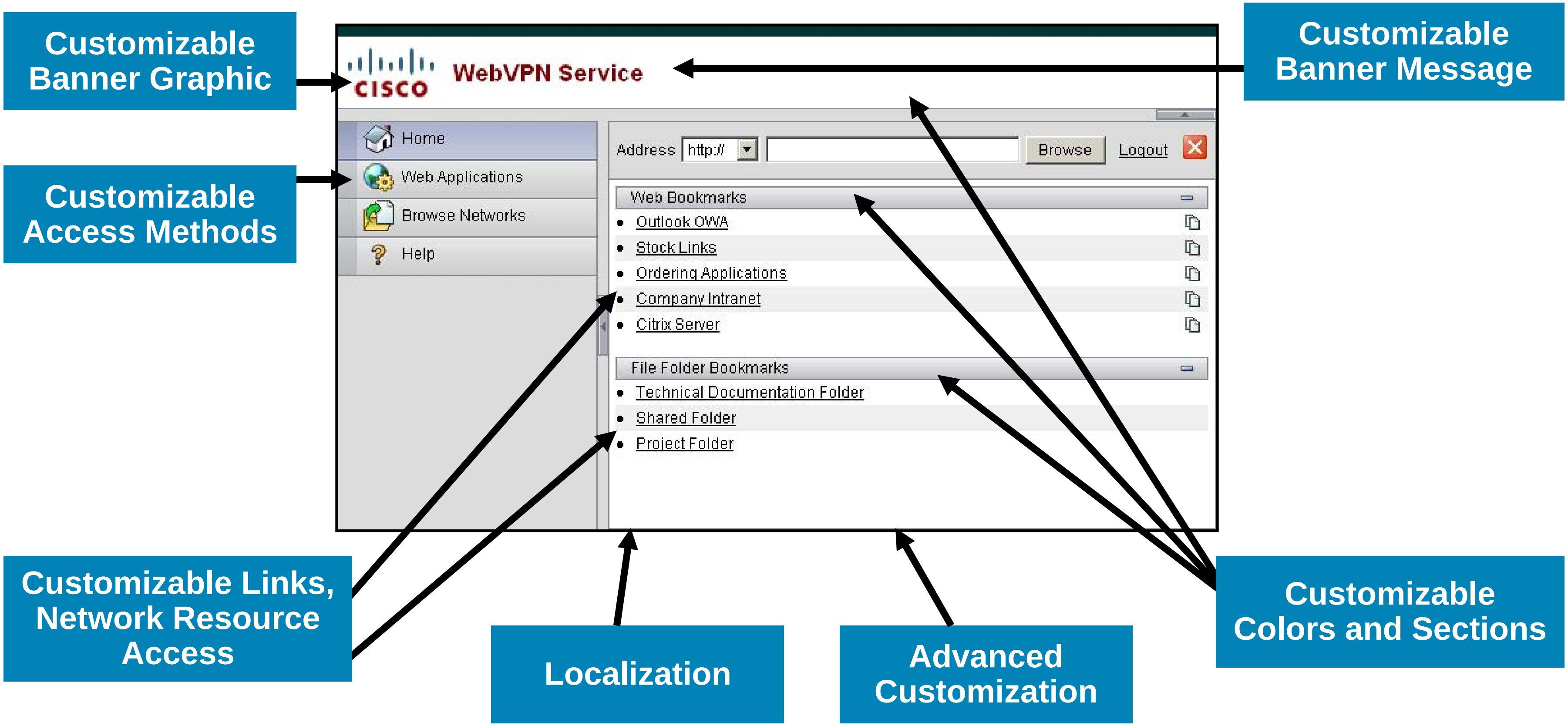


Connection Entry	Host	Transport
A - Headquarters	**headquarters-vpn.company....**	**IPSec/UDP**
B - Datacenter 1	datacenter1-vpn.company.com	IPSec/UDP
B - Datacenter 2	datacenter2-vpn.company.com	IPSec/UDP
C - Branch 1	branch1-vpn.company.com	IPSec/UDP
C - Branch 2	branch2-vpn.company.com	IPSec/UDP
C - Branch 3	branch3-vpn.company.com	IPSec/UDP
D - DR site	dr-vpn.company.com	IPSec/UDP

Not connected.

Cisco AnyConnect VPN Client (SSL/DTLS Client) discussed later

SSL VPN Clientless (L7) Customization



Customizable Banner Graphic

Customizable Access Methods

Customizable Banner Message

Customizable Links, Network Resource Access

Localization

Advanced Customization

Customizable Colors and Sections

SSL for VPN Is Different Than E-Commerce

- 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 and application translation (clientless/L7)
  - Dynamic VPN client (full network access/L3)
  - SmartTunnel (thin client)
  - Port forwarding (thin client)

SSL VPN: Clientless (Content Rewriting and 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, increased focus on advanced transformation capabilities
- For application translation, VPN appliance “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)

Complex Content Handling

- Smart Tunnels

  Allows Winsock v2 TCP applications to use the VPN security appliance as a proxy gateway to the private side of a network

- Port Forwarding

  Local “thin” client acts as proxy

  Tunnels and forwards application traffic

- Application Profile Customization Framework
- Plug-ins

  Cirtix ICA, RDP, SSH/TELNET, VNC provided by Cisco

  Extensible framework for other popular protocols

Smart Tunnels

Applications Use VPN Appliance as Proxy Gateway

- Must create list of “authorized” processes
- Smart Tunnels loads a stub into each authorized process and intercepts socket calls and redirects them through the VPN appliance
- The parent of each authorized process passes on the information (cookie, etc.) to its children if a child is an authorized process
- Example

  Launch telnet via telnet.exe

  telnet.exe must be authorized process

Application Profile Customization Framework (APCF)

Application Helper

- Allows the security appliance to handle non-standard applications and web resources so they display correctly over a Clientless SSL VPN connection
- Profiles

  An APCF profile contains a script that specifies when (pre, post), where (header, body, request, response), and what data to transform for a particular application

  The script is in XML and uses sed (stream editor) syntax to transform strings/text

  Profile would come from Cisco TAC

Client/Server Plug-ins

Feature Overview

- ASA v8.0 supports a number of common client/server applications via Java plugins such as

  Windows Terminal Server (RDP)

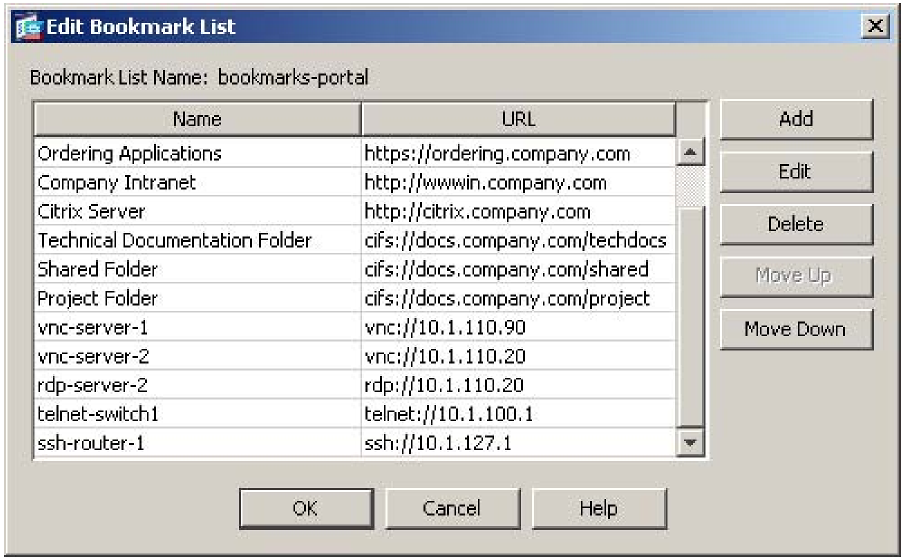
  Telnet/SSH

  Citrix ICA Client

  VNC

- Resource is defined as a URL with the appropriate protocol type

  rdp://server:port



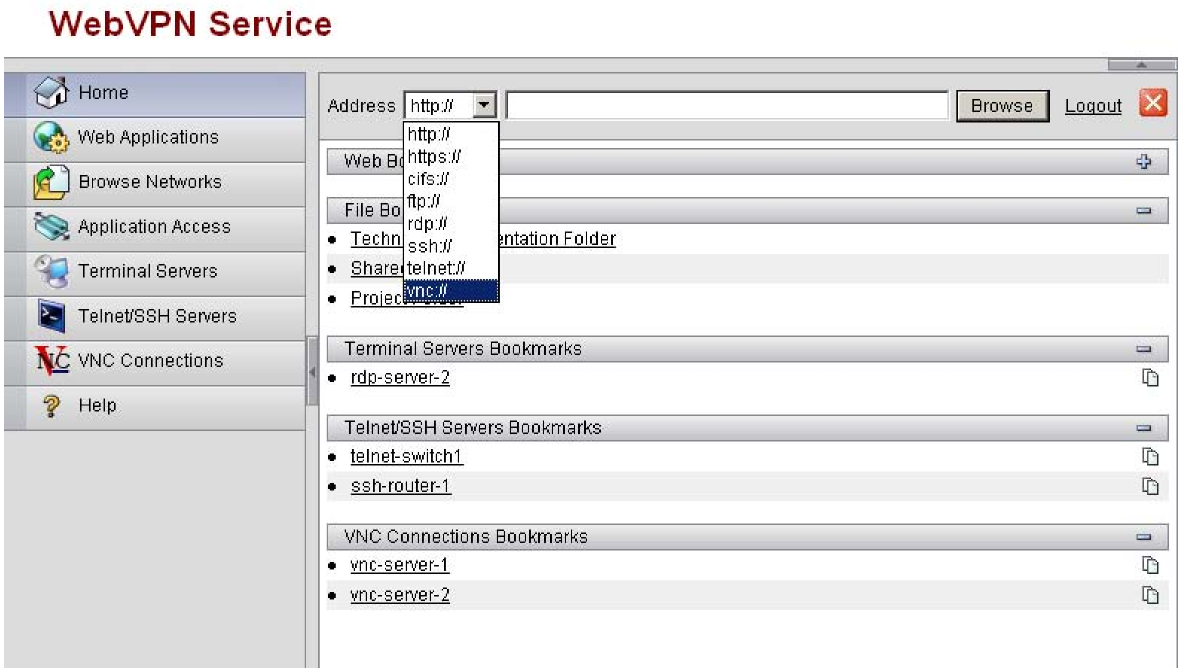
Bookmark List Name: bookmarks-portal

Name	URL
Ordering Applications	https://ordering.company.com
Company Intranet	http://wwwin.company.com
Citrix Server	http://citrix.company.com
Technical Documentation Folder	cifs://docs.company.com/techdocs
Shared Folder	cifs://docs.company.com/shared
Project Folder	cifs://docs.company.com/project
vnc-server-1	vnc://10.1.110.90
vnc-server-2	vnc://10.1.110.20
rdp-server-2	rdp://10.1.110.20
telnet-switch1	telnet://10.1.100.1
ssh-router-1	ssh://10.1.127.1

- Support for these third party applications exists in the form of packaged single archive files in the .jar file format

Client/Server Plug-ins

- When clicking on a resource link, a dynamic page is generated that hosts the ActiveX/Java applet
- The Java applet is rewritten and re-signed, ActiveX parameters are rewritten, and the helper port-forwarder ActiveX is injected if needed
- The Java applet is transparently cached in the gateway cache



Client/Server Plug-ins

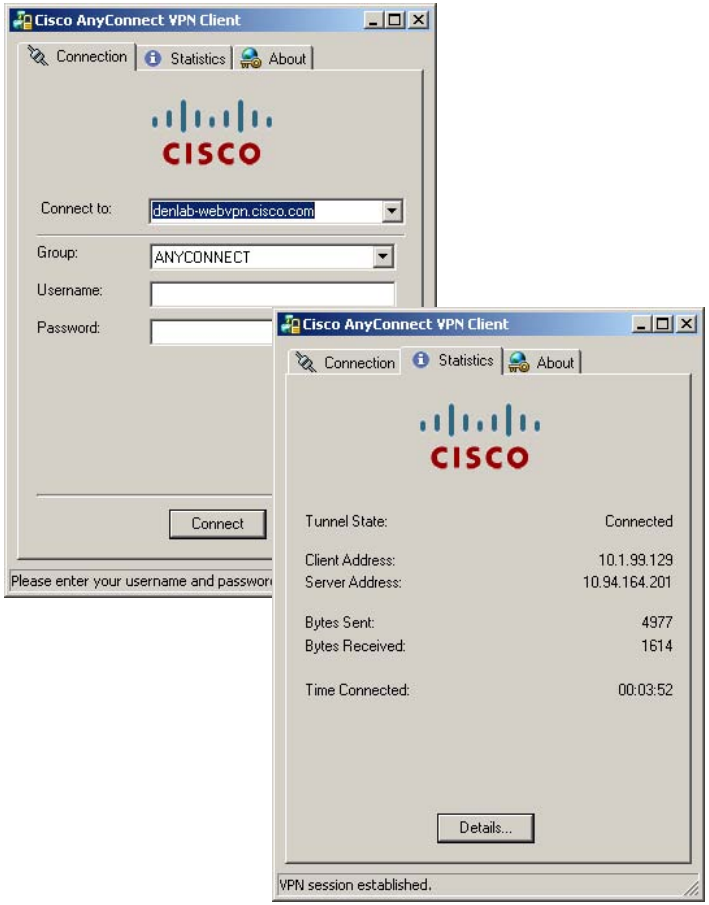
The Existing Capabilities of Java Rewriting and the Use of APCF Files with Its Own ActiveX Port Forwarder Lends Itself Well to the Techniques Used to Both Extend These Capabilities and Add Support for Additional Content Types

- SVG: (Scalable Vector Graphics) is an XML-based vector graphics format
- MHTML: RFC2557 MIME Encapsulation of Aggregate Documents
- XML/XSL: Extensible Stylesheet Language

SSL VPN Tunneling: AnyConnect Client

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

- Traditional-style client delivered via automatic download
- Requires administrative privileges for initial install only
- Stub installer has been replaced with an MSI out-of-band/pre-installation package
- Can use TLS or DTLS as transport
- Can be upgraded from a previous version upon connection



Connect to: denlab-webvpn.cisco.com

Group: ANYCONNECT

Username:

Password:

Please enter your username and passwor

Tunnel State: Connected

Client Address: 10.1.99.129

Server Address: 10.94.164.201

Bytes Sent: 4977

Bytes Received: 1614

Time Connected: 00:03:52

VPN session established.

Datagram TLS (DTLS)

Why DTLS?

- Limitations of TLS with SSL VPN tunnels

  TLS is used to tunnel TCP/IP over TCP/443

  TCP requires retransmission of lost packets

  Both application and TLS wind up retransmitting when packet loss is detected

- DTLS solves the TCP over TCP problem

  DTLS replaces underlying transport TCP/443 with UDP/443

  DTLS uses TLS to negotiate and establish DTLS connection (control messages and key exchange)

  Datagrams only are transmitted over DTLS

- Other benefits

  Low latency for real time applications

  DTLS is optional and can fallback to TLS if required

SSL VPN: AnyConnect Client

Installation Options

- WebLaunch

  Initiate via web browser

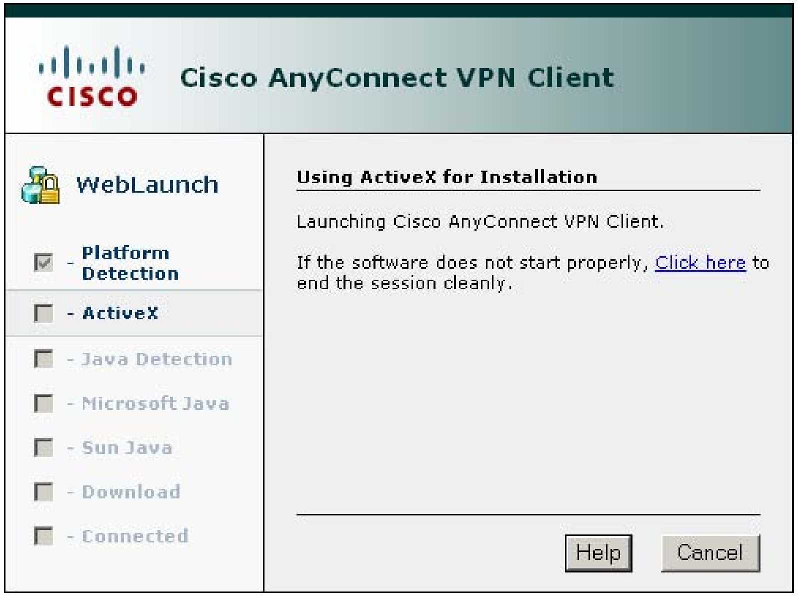
  Login via portal

  Auto-download (ActiveX/Java)

  Manual download

- Manual

  MSI installer

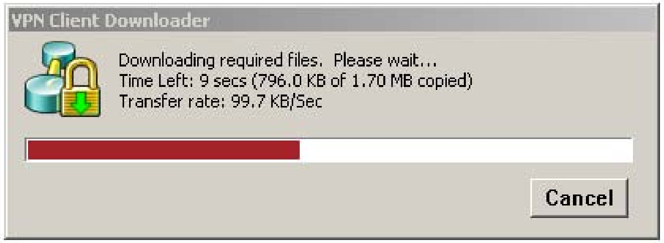


Cisco AnyConnect VPN Client

Using ActiveX for Installation

Launching Cisco AnyConnect VPN Client.

If the software does not start properly, Click here to end the session cleanly.



VPN Client Downloader

Downloading required files. Please wait...
Time Left: 9 secs (796.0 KB of 1.70 MB copied)
Transfer rate: 99.7 KB/Sec

SSL VPN: Cisco AnyConnect VPN Client

Connect Options

- Web-based Initiation

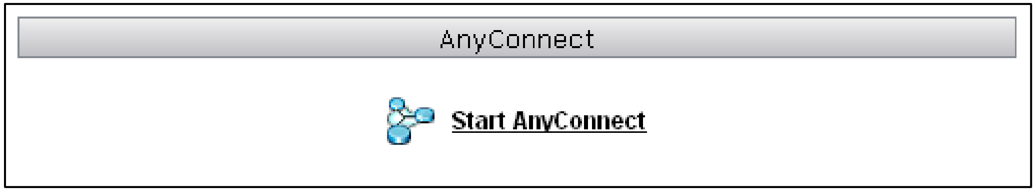
  Portal

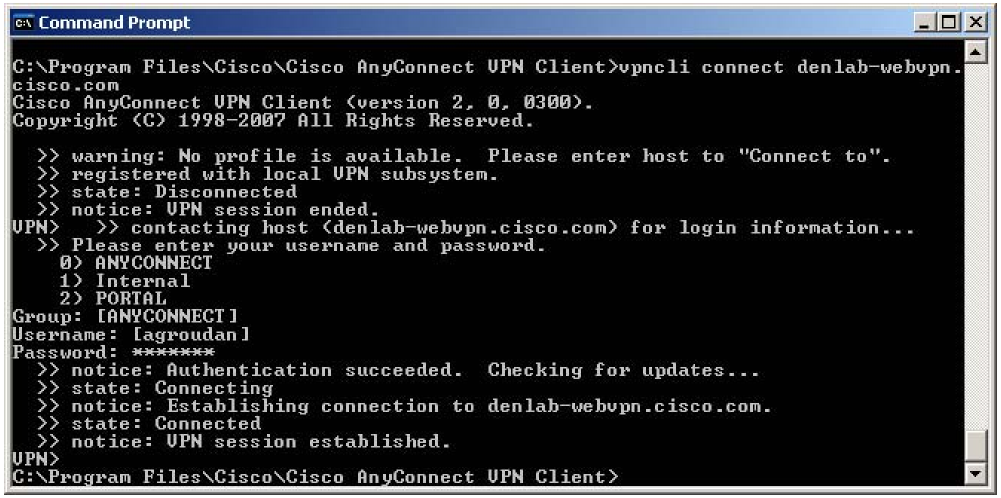
- Standalone Mode

  Shortcut

  Start Menu

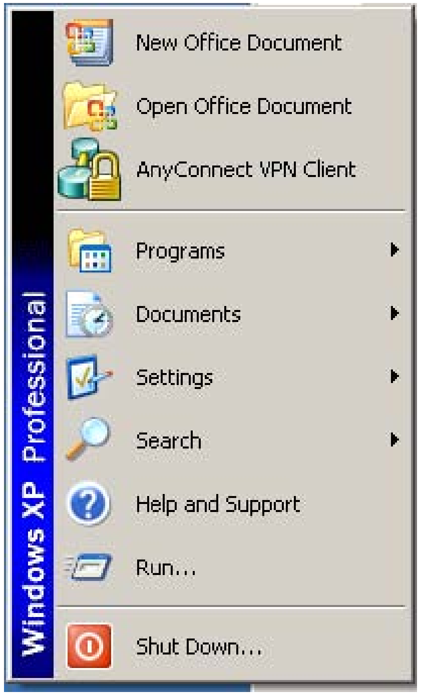
  Command Line





```
C:\Program Files\Cisco\Cisco AnyConnect VPN Client>vpncli connect denlab-webvpn.
cisco.com
Cisco AnyConnect VPN Client (version 2, 0, 0300).
Copyright (C) 1998-2007 All Rights Reserved.

  >> warning: No profile is available.  Please enter host to "Connect to".
  >> registered with local VPN subsystem.
  >> state: Disconnected
  >> notice: VPN session ended.
VPN>    >> contacting host (denlab-webvpn.cisco.com) for login information...
  >> Please enter your username and password.
    0) ANYCONNECT
    1) Internal
    2) PORTAL
Group: [ANYCONNECT]
Username: [agroudan]
Password: ********
  >> notice: Authentication succeeded.  Checking for updates...
  >> state: Connecting
  >> notice: Establishing connection to denlab-webvpn.cisco.com.
  >> state: Connected
  >> notice: VPN session established.
VPN>
C:\Program Files\Cisco\Cisco AnyConnect VPN Client>
```



Client Comparison

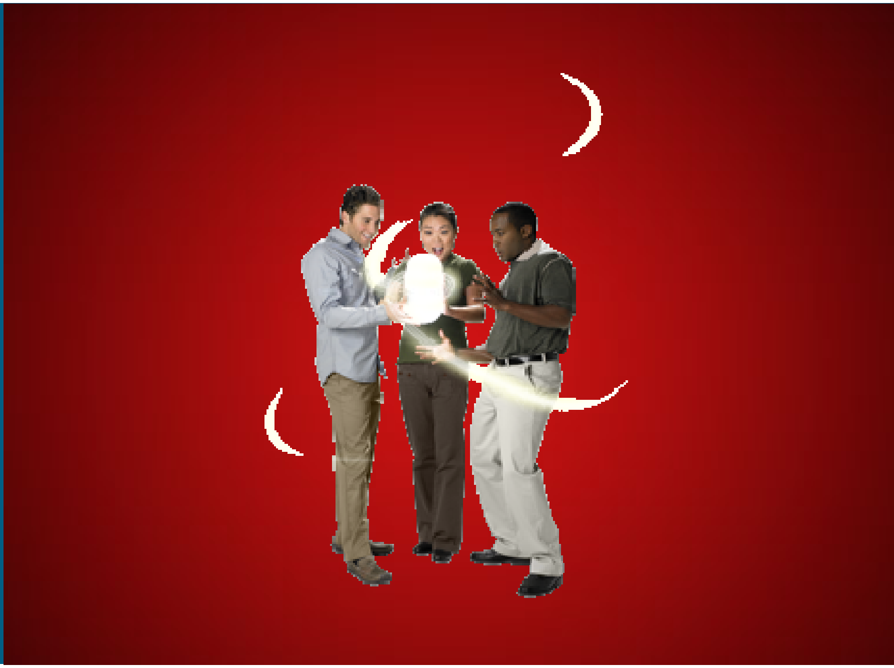
Key Differences

	Cisco VPN Client	Cisco AnyConnect VPN client
Approximate Size	~10 MB	~1.2 MB
Initial Install	Distribute	Auto Download Distribute
Admin Rights Required	Yes	Yes Initial Install Only
Protocol	IPsec	DTLS, TLS
OS Support	Multiple*	Multiple**
Head End	Cisco ASA®/Cisco PIX®/ Cisco IOS®	Cisco ASA/Cisco IOS
Client Reboot Required	Yes	No

* W2K/XP x32, Vista x32, Mac OS X 10.4/10.5, Linux Kernels 2.6, Solaris UltraSparc

** W2K x32, XP x32/x64, Vista x32/x64, Mac OS X 10.4/10.5, Linux Kernels 2.6

Design Considerations



Network Design Components

- VPN termination device (head-end)

  Security appliance/firewall

  VPN-enabled router

  Cisco Catalyst® Switch with VPN-SPA

- VPN client/SSL clientless

  Software

  Hardware

  Dynamic (AnyConnect or SSL VPN client)

  SSL VPN clientless access

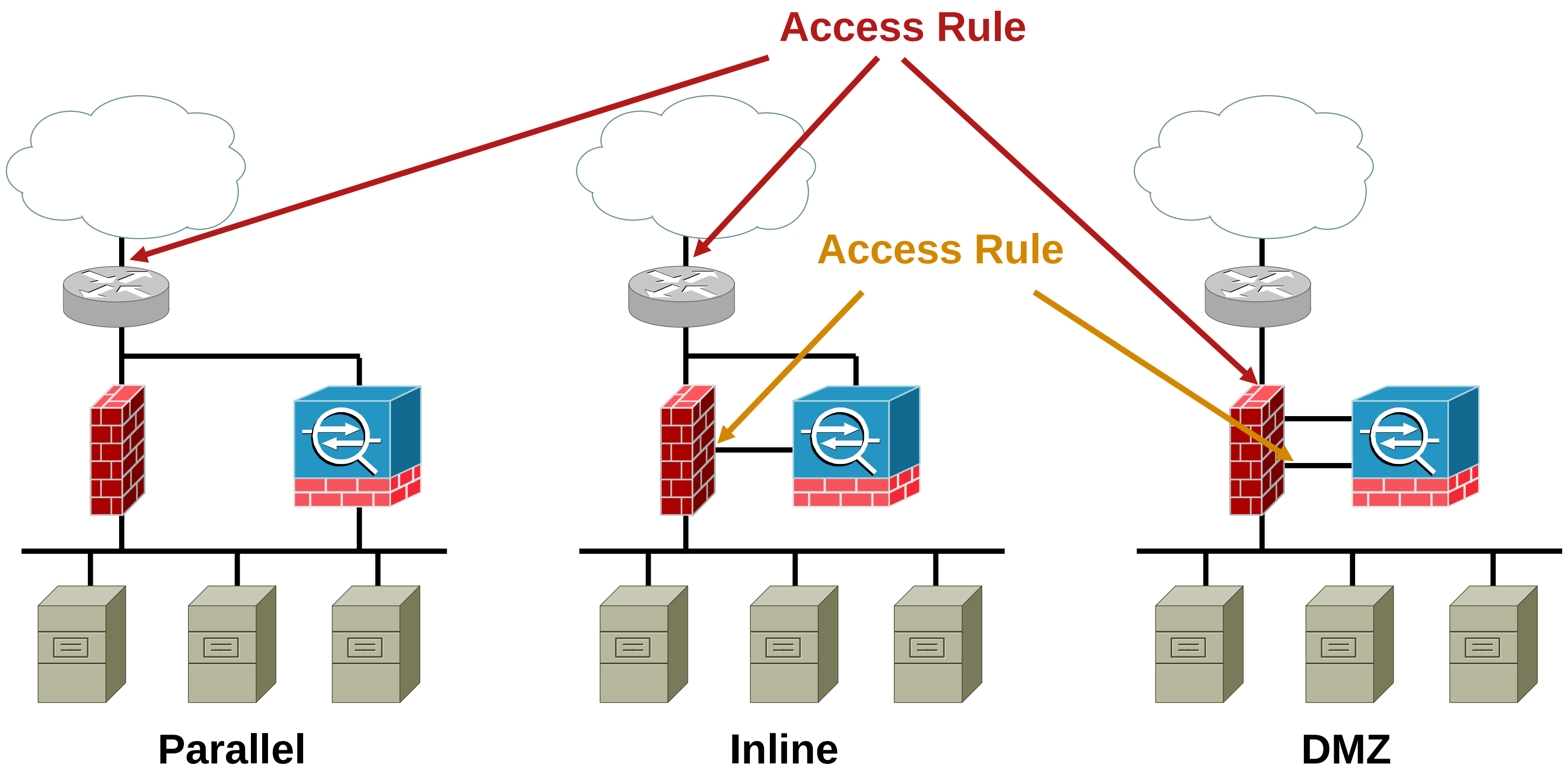
Design Considerations

- Firewall placement and configuration
- Routing
- Client authentication
- Address assignment
- Access control

Firewall Placement and Configuration

Controlling Access to/from Public/Private Interfaces

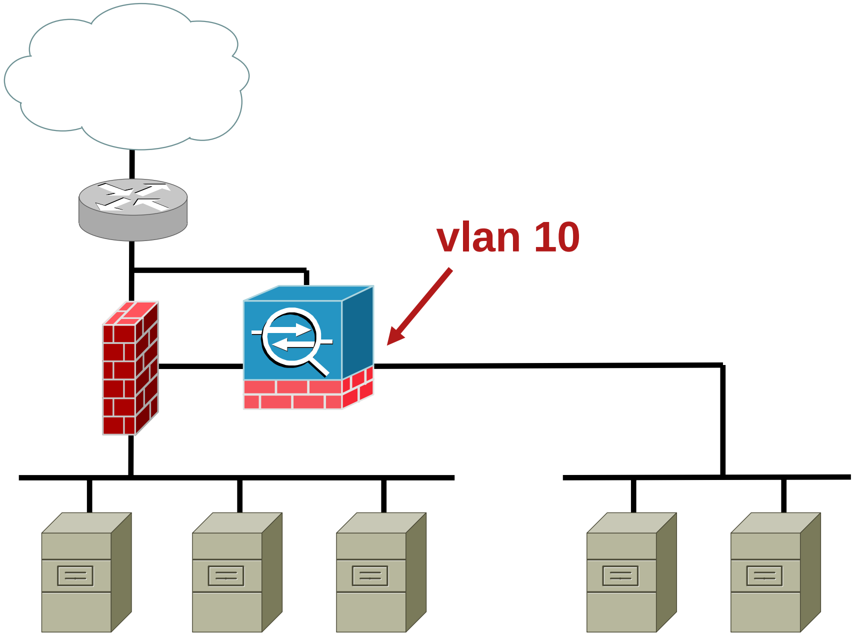
- Limit incoming traffic to IPsec and/or SSL for FW policy
- Use firewall to inspect IP traffic after decryption



Routing—Interfaces/VLANs

User/Group Based Policies

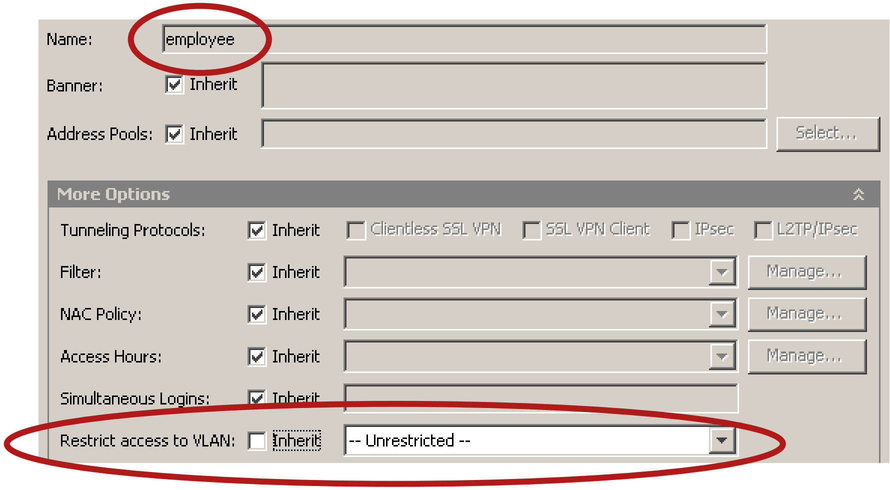
- Map users to group based on role
- Use group policy to restrict egress VLAN



vlan 10

Internal Resources

Shared Resources



Name: employee

Banner: ☑ Inherit

Address Pools: ☑ Inherit Select...

More Options

Tunneling Protocols: ☑ Inherit □ Clientless SSL VPN □ SSL VPN Client □ IPsec □ L2TP/IPsec

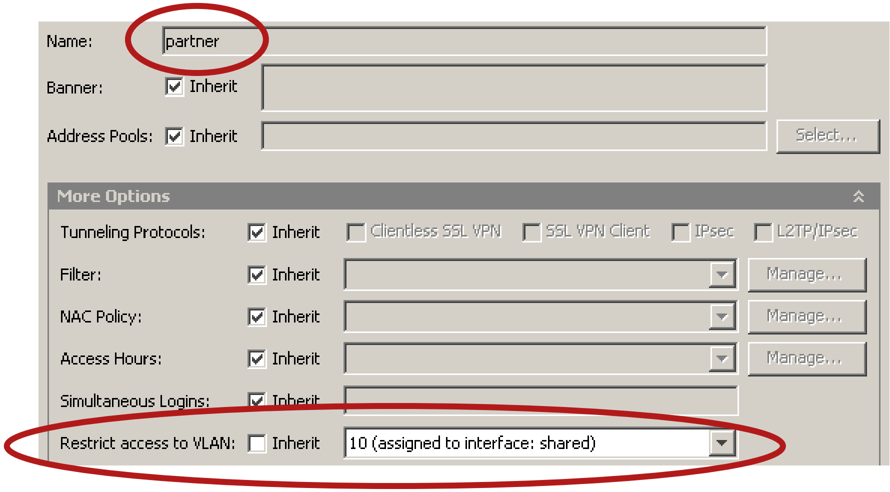
Filter: ☑ Inherit Manage...

NAC Policy: ☑ Inherit Manage...

Access Hours: ☑ Inherit Manage...

Simultaneous Logins: ☑ Inherit

Restrict access to VLAN: □ Inherit -- Unrestricted --



Name: partner

Banner: ☑ Inherit

Address Pools: ☑ Inherit Select...

More Options

Tunneling Protocols: ☑ Inherit □ Clientless SSL VPN □ SSL VPN Client □ IPsec □ L2TP/IPsec

Filter: ☑ Inherit Manage...

NAC Policy: ☑ Inherit Manage...

Access Hours: ☑ Inherit Manage...

Simultaneous Logins: ☑ Inherit

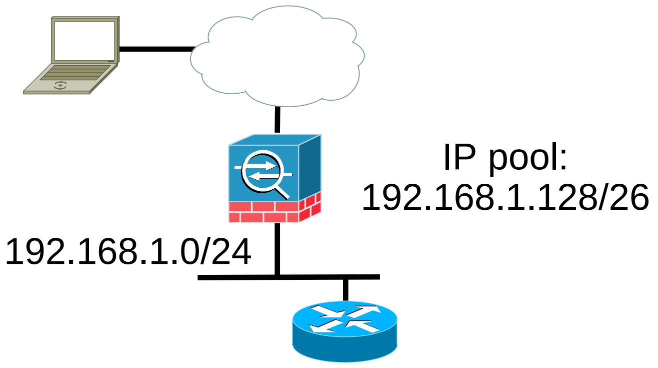
Restrict access to VLAN: □ Inherit 10 (assigned to interface: shared)

Address Assignment

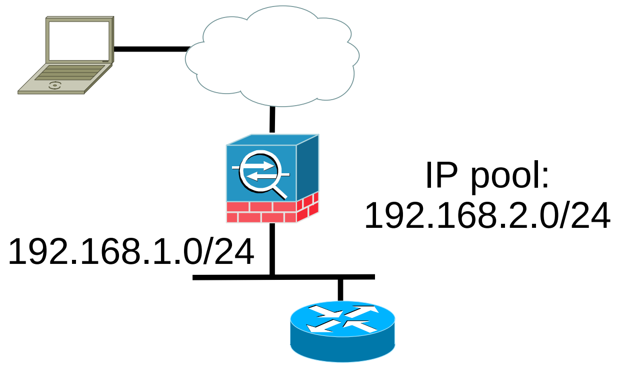
- Least complex and most commonly used are internal address pools
  - Global pool can be shared across multiple groups
  - Group-based and Interface-Specific address pools may be used for access control together with ACLs on a downstream device
- DHCP assignment allows for centralized IP management
- Static assignment requires RADIUS or LDAP to deploy
- Clientless users share the IP of the head-end device private interface
  - Downstream IP filtering capabilities are limited as all end users source the same IP address
  - Can use more granular filtering on VPN Security Appliance

Routing: Address Assignment

- Proxy-ARP
  - IP pool/DHCP scope/static included within range of private interface subnet
  - No changes required to router, no routing protocol required
  - Transit network must have enough available IP space
- Configured/Learned Routes
  - IP pools are unique
  - More scalable and can use unique per group IP pools
  - Use static route(s) on downstream router pointing to private interface
  - Use Reverse Route Injection (RRI), note IPsec only
  - Use static route and route redistribution

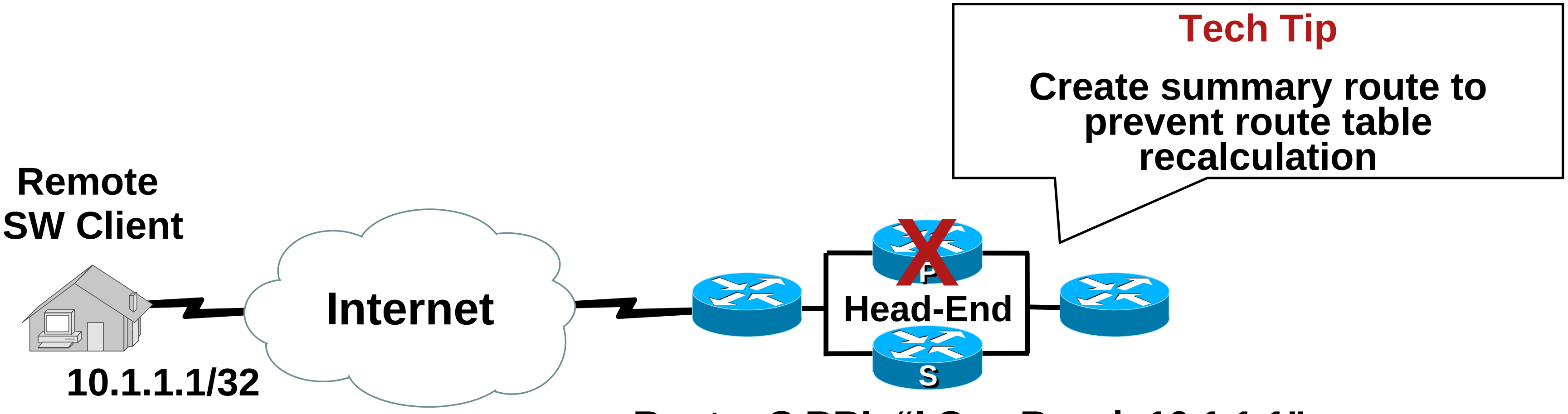


VPN Security Appliance Uses Proxy-ARP



Downstream Router Requires a Specific Route

Routing Design Consideration



Tech Tip

Create summary route to prevent route table recalculation

Router S RRI: “I Can Reach 10.1.1.1”

- Reverse Route Injection (RRI) is used to populate the routing table of internal routers via EIGRP, OSPF or RIPv2
- VPN software clients inject their assigned IP address as host routes
- A hardware client can connect using Network Extension Mode (NEM) and inject its protected network address (note that a hardware client in Port Address Translation [PAT] mode is treated just like a VPN client)

Client Authentication Design

- VPNs can utilize many types of databases for centralized authentication
    - Username and password
    - Tokens
    - Digital certificate/smartcards
- Authenticated against:
    - Authenticated against:
    - RADIUS
    - Active Directory (AD)/Kerberos
    - NT Domain
    - RSA SecurID
    - LDAP
    - Other One-Time Password server (OTP) via RADIUS

Commonly Deployed Authentication

- 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

This can get you going quickly for testing but for the long run look at PKI or OTP solutions

Access Control Overview

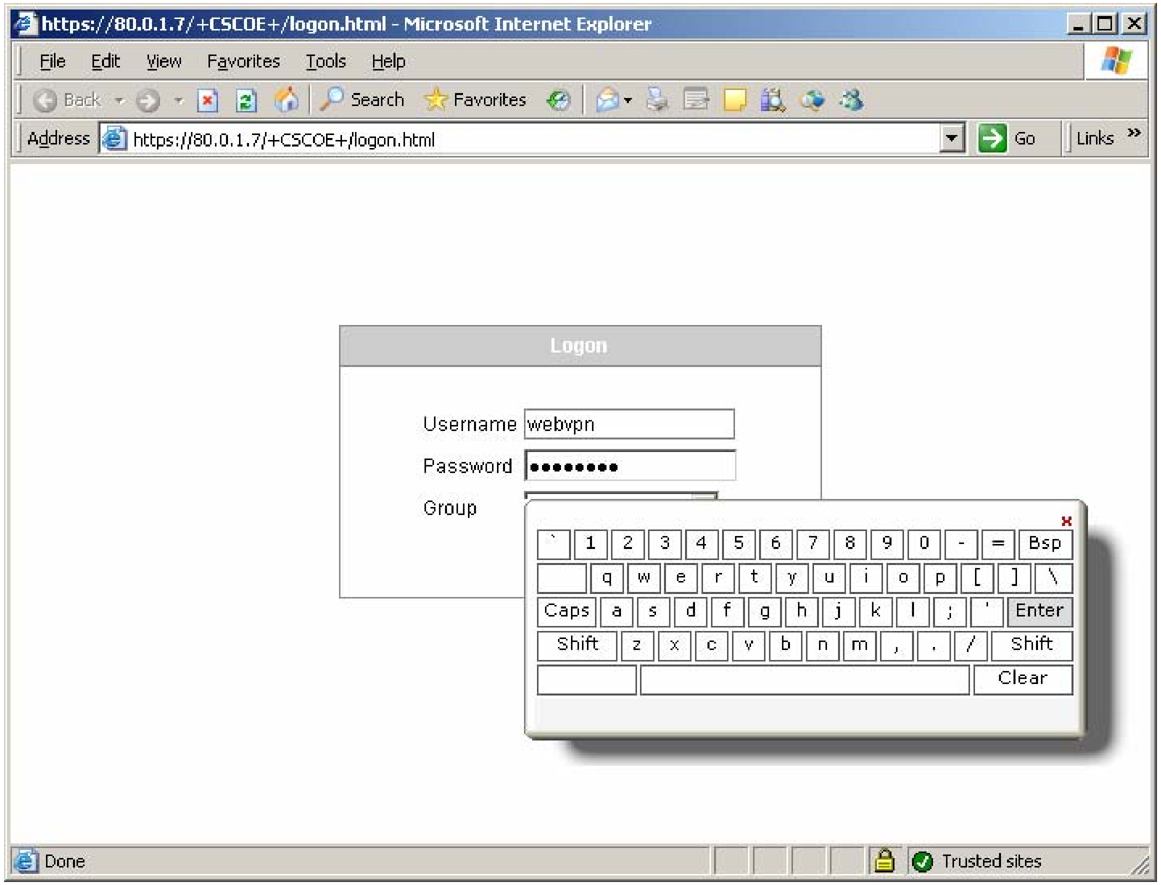
- Unless your goal is to provide unrestricted network access, it is generally a good idea to provide access control rules for users
- Some companies choose to maintain all access rules on an internal FW based on source IP of the client
- Access control rules can generally be defined at a per-group basis on the head-end device (easy to deploy, but more difficult to maintain large numbers of policies or across multiple boxes)
- Access control rules can be defined on the head-end RADIUS server; RADIUS has a 4K packet size limit which makes using a generic RADIUS server for access control challenging
- Cisco Secure ACS offers a downloadable ACL feature which can be used with Cisco head-end devices to support large-sized policies

Access Control: L3 and L7

- Tunnel-based (L3) VPN (IPsec and AnyConnect VPN client) provides control at the protocol/port and destination IP level
- Clientless (L7) 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

Virtual Keyboard

WebVPN Login Page



https://80.0.1.7/+CSCOE+/logon.html - Microsoft Internet Explorer

Logon

Username: webvpn

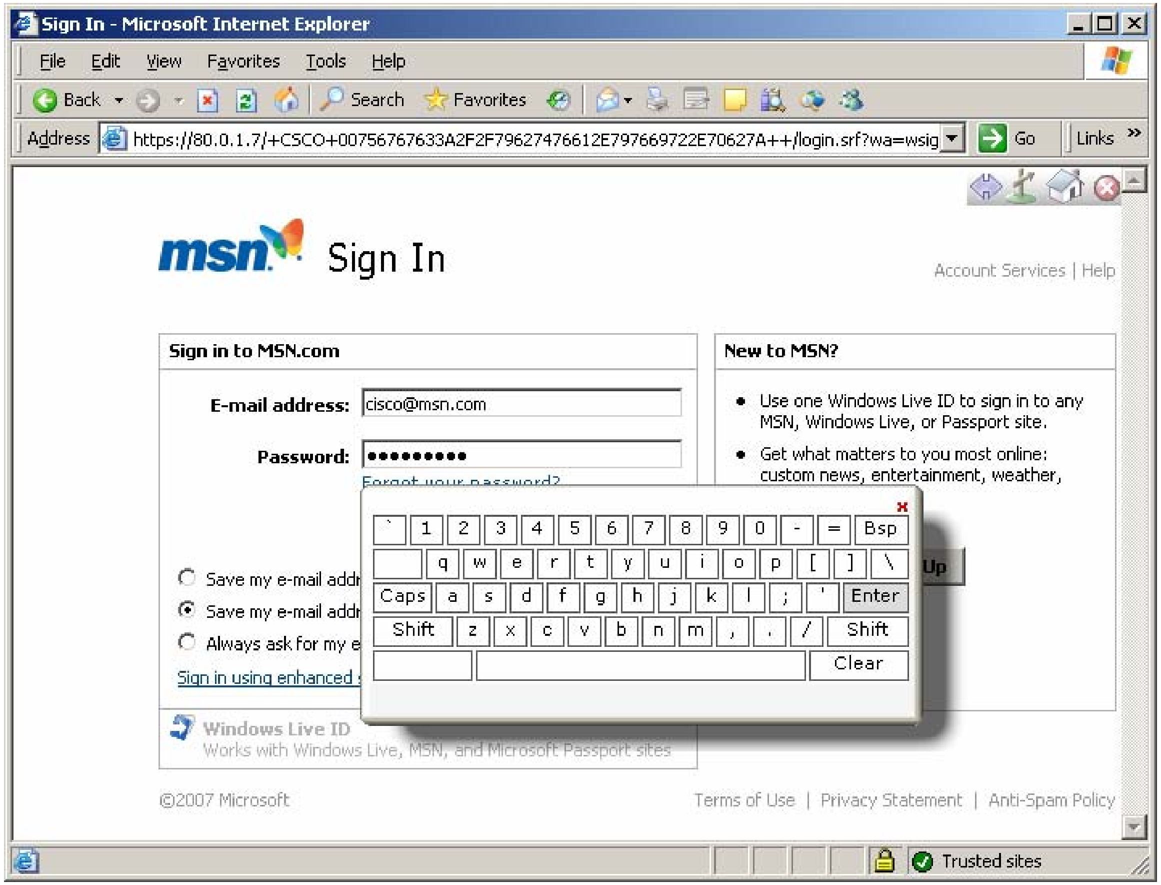
Password: ●●●●●●●●●

Group

File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address https://80.0.1.7/+CSCOE+/logon.html
Go
Links
` 1 2 3 4 5 6 7 8 9 0 - = Bsp
q w e r t y u i o p [ ] \
Caps a s d f g h j k l ; ' Enter
Shift z x c v b n m , . / Shift
Clear
Done
Trusted sites

Virtual Keyboard

All Clientless SSL VPN Pages Requiring Authentication



Sign In - Microsoft Internet Explorer

https://80.0.1.7/+CSCO+00756767633A2F2F79627476612E797669722E70627A++/login.srf?wa=wsig

Sign In

Account Services | Help

Sign in to MSN.com

E-mail address: cisco@msn.com

Password: ●●●●●●●●●

Forgot your password?

○ Save my e-mail addr

● Save my e-mail addr

○ Always ask for my e

Sign in using enhanced s

New to MSN?

- Use one Windows Live ID to sign in to any MSN, Windows Live, or Passport site.
- Get what matters to you most online: custom news, entertainment, weather,

` 1 2 3 4 5 6 7 8 9 0 - = Bsp
q w e r t y u i o p [ ] \
Caps a s d f g h j k l ; ' Enter
Shift z x c v b n m , . / Shift
Clear

Windows Live ID

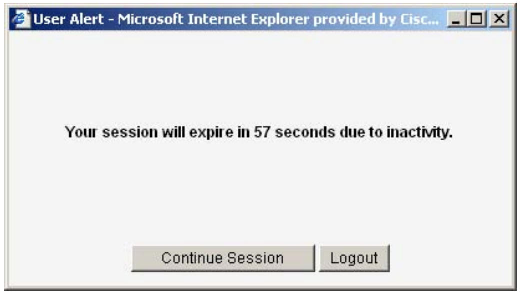
Works with Windows Live, MSN, and Microsoft Passport sites

©2007 Microsoft

Terms of Use | Privacy Statement | Anti-Spam Policy

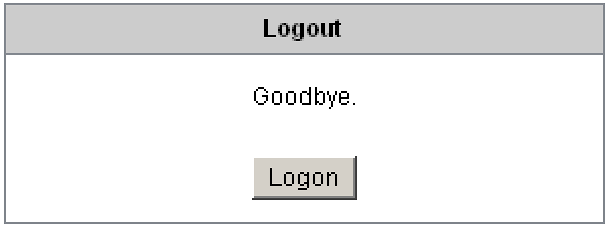
Trusted sites

Session Logoff/Idle Timeout



User Alert - Microsoft Internet Explorer provided by Cisc...

Your session will expire in 57 seconds due to inactivity.

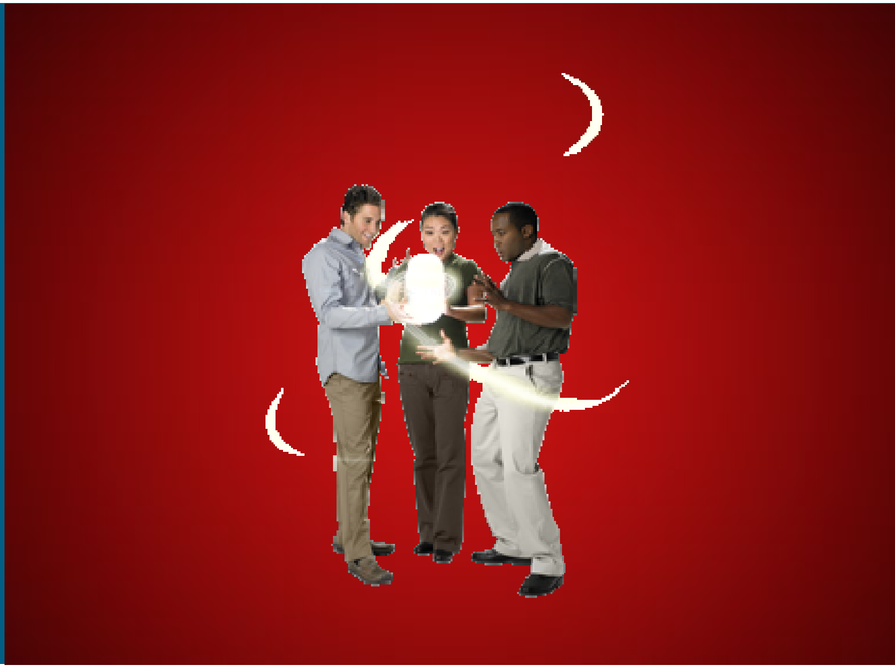


Logout

Goodbye.

- 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

- NAT/PAT Transparency
- Firewall traversal
- Security policies
  - Split tunneling
  - Local (LAN) access
- Resiliency and availability
  - Dead Peer Detection (DPD)
  - HSRP/VRRP
  - Backup peer list (VPN client)
  - Remote access load balancing

IPsec VPN and NAT/PAT Transparency

- Internet Security Association and Key Management Protocol (RFC 2408)

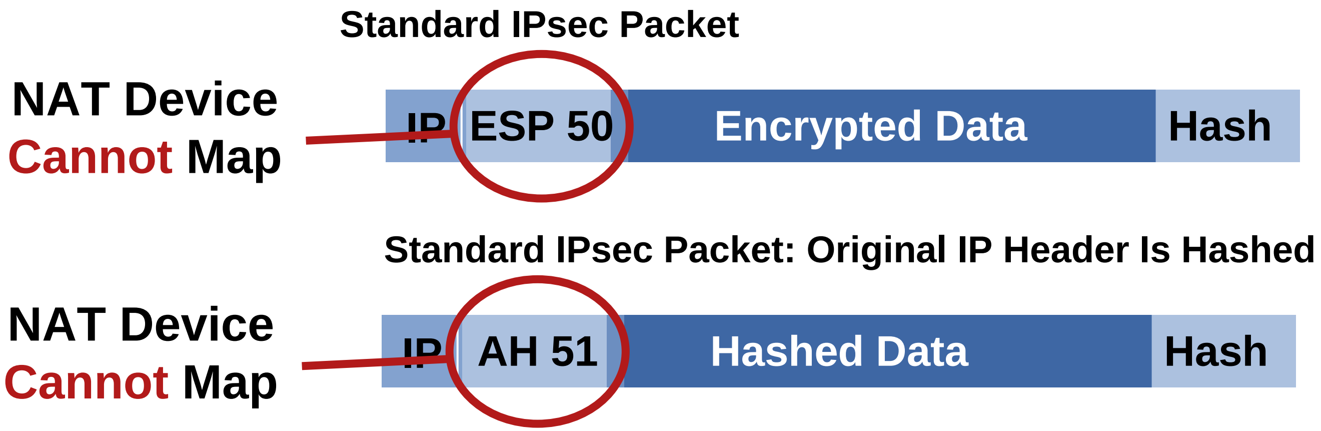
  ISAKMP: UDP 500

- IP Encapsulating Security Payload (RFC 2406)

  ESP: IP Protocol 50

- IP Authentication Header (RFC 2402)

  AH: IP Protocol 51 (typically not used for remote access VPN)

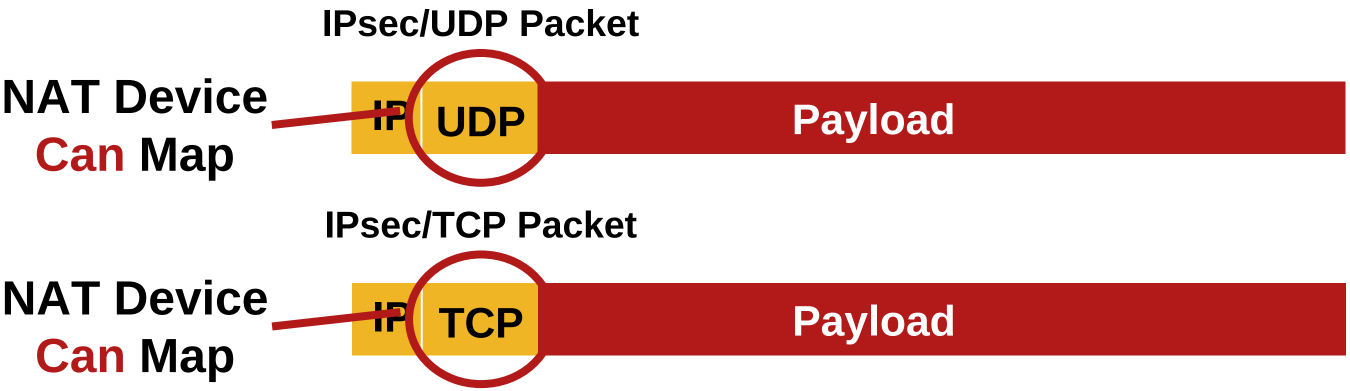


See RFC 3715 for more detail

IPsec VPN and NAT/PAT Transparency

IPsec/UDP and IPsec/TCP

- Allows clients to operate behind a NAT/PAT device
- It uses a UDP or TCP header with configurable (on server) port number to bypass PAT devices (default port 10,000)
- Provides the same security as IPsec/ESP
- Requires no user intervention as administrator centrally controls IPsec/UDP via group policies.
- IPsec/TCP is configured via global IKE parameters



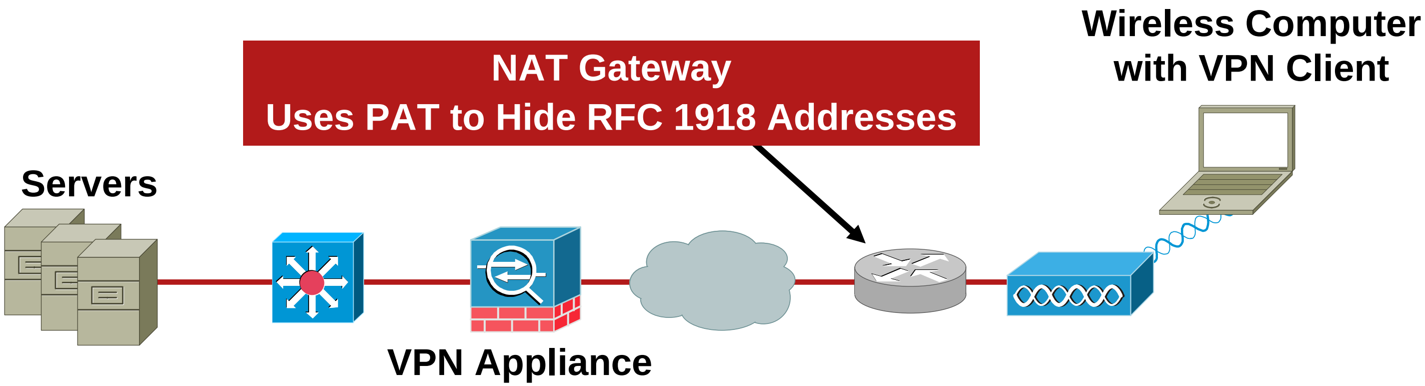
NAT Traversal (NAT-T)

- NAT discovery payload is used to discover the existence/ location of NAT device during IKE phase 1
- If there is NAT, encapsulate ESP packet as UDP payload (UDP/4500)
- IKE NAT keepalive is sent to keep translations from timeout

Tech Tip

If You Have Connectivity Problems the First Thing to Enable Is NAT-T.=

Typical Broadband Hotspot



Wireless Computer with VPN Client

NAT Gateway
Uses PAT to Hide RFC 1918 Addresses

Servers

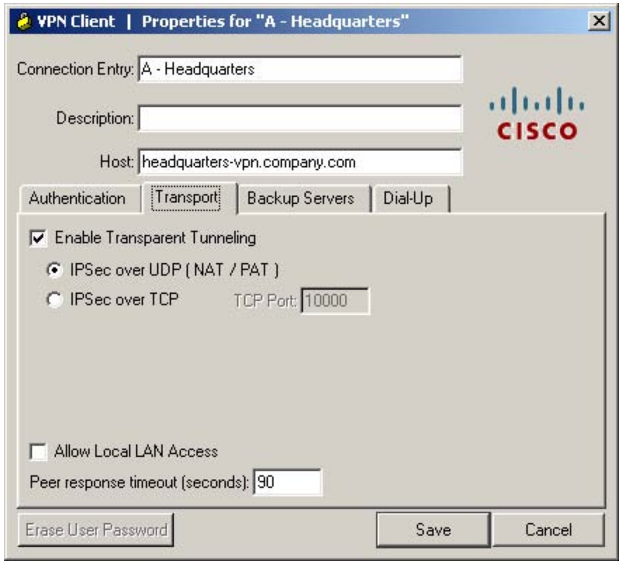
VPN Appliance

See RFCs 3947 and 3948 for more detail

NAT Transparency

UDP Encapsulation

Cisco VPN Client



VPN Client | Properties for "A - Headquarters"

Connection Entry: A - Headquarters

Description:

Host: headquarters-vpn.company.com

☑ Enable Transparent Tunneling

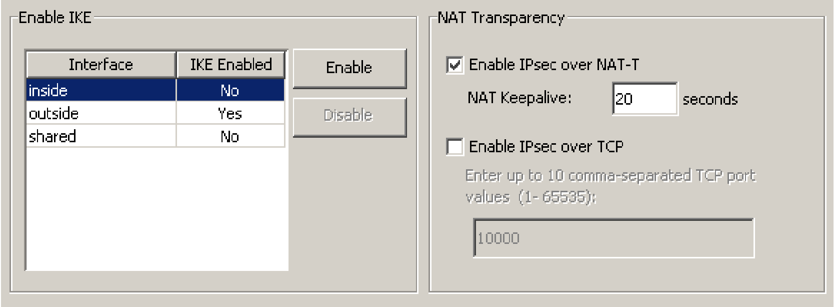
● IPSec over UDP (NAT / PAT)

○ IPSec over TCP TCP Port: 10000

□ Allow Local LAN Access

Peer response timeout (seconds): 90

VPN Security Appliance



Enable IKE

Interface	IKE Enabled
inside	No
outside	Yes
shared	No

NAT Transparency

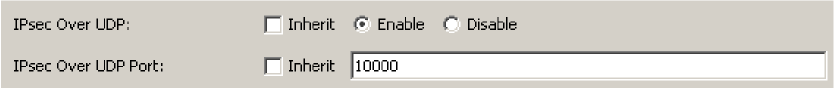
☑ Enable IPsec over NAT-T

NAT Keepalive: 20 seconds

□ Enable IPsec over TCP

Enter up to 10 comma-separated TCP port values (1- 65535):

10000



IPsec Over UDP: □ Inherit ● Enable ○ Disable

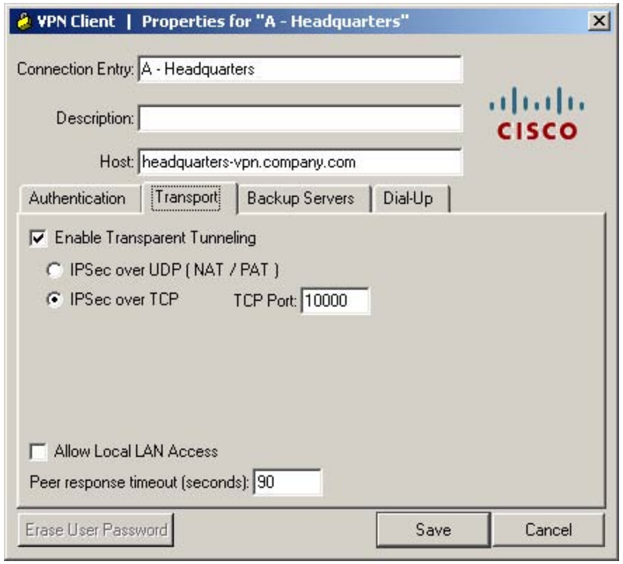
IPsec Over UDP Port: □ Inherit 10000

- NAT-T preferred over legacy IPsec over UDP
- NAT-T always uses UDP/4500
- IPsec over UDP uses administrator defined port
- IPsec over UDP configured at group policy

NAT Transparency

TCP Encapsulation

Cisco VPN Client



VPN Client | Properties for "A - Headquarters"

Connection Entry: A - Headquarters

Description:

Host: headquarters-vpn.company.com

☑ Enable Transparent Tunneling

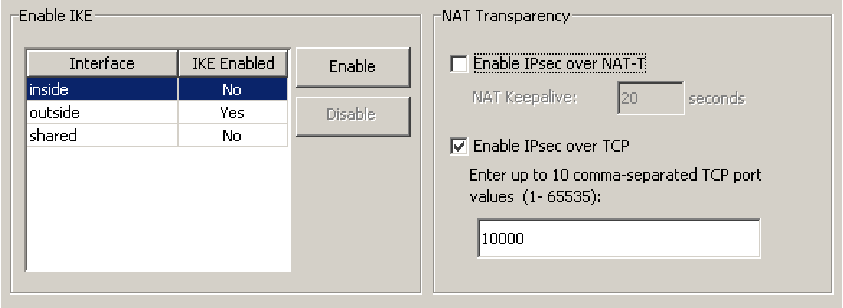
○ IPSec over UDP (NAT / PAT)

● IPSec over TCP   TCP Port: 10000

□ Allow Local LAN Access

Peer response timeout (seconds): 90

VPN Security Appliance



Enable IKE

Interface	IKE Enabled
inside	No
outside	Yes
shared	No

NAT Transparency

□ Enable IPsec over NAT-T

NAT Keepalive: 20 seconds

☑ Enable IPsec over TCP

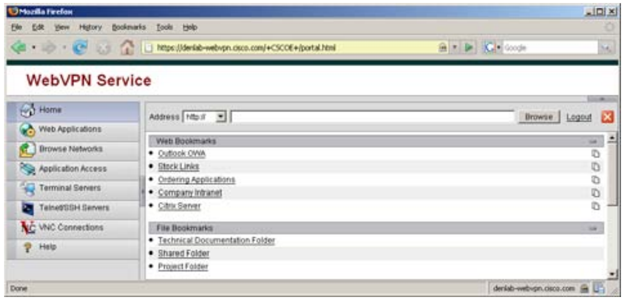
Enter up to 10 comma-separated TCP port values (1- 65535):

10000

- Select up to 10 administrator defined ports
- Select one port value from this set on client
- Do not use TCP 443 if you also want to use SSL VPN

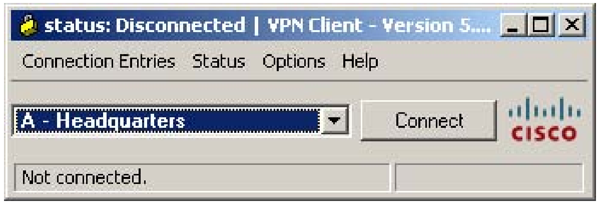
Firewall Traversal

SSL VPN



- HTTPS—TCP/443
- DTLS—UDP/443
  - Will fallback to TCP
- 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

IPsec VPN


status: Disconnected | VPN Client - Version 5....

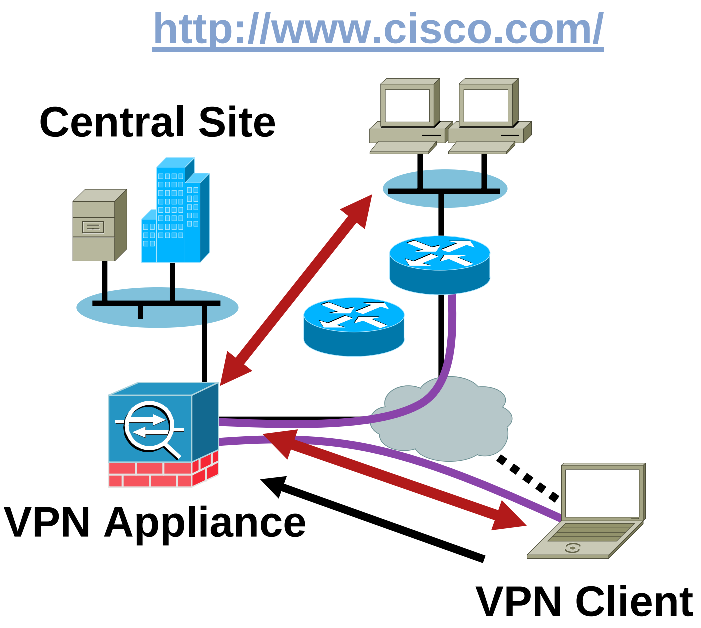
Not connected.

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

Split Tunneling

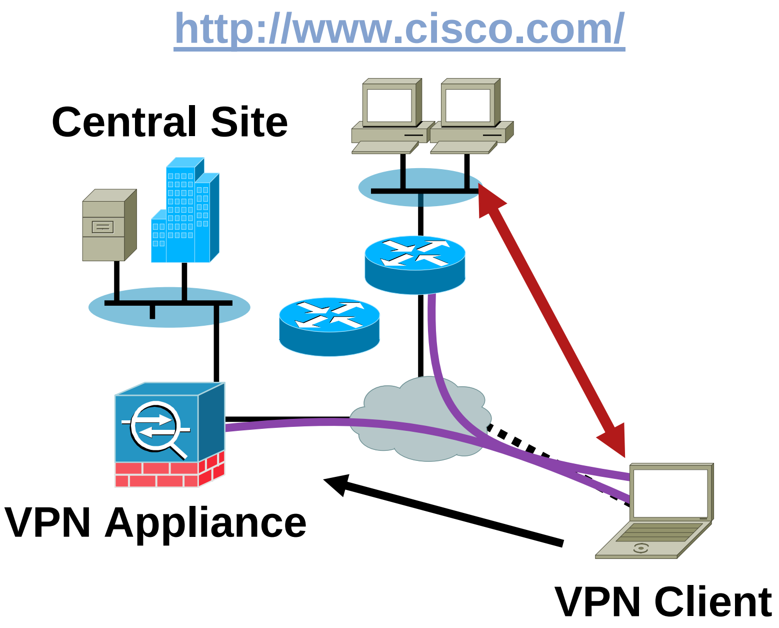
Remote Access Client or Device

Without Split Tunneling



Maximum Security

With Split Tunneling



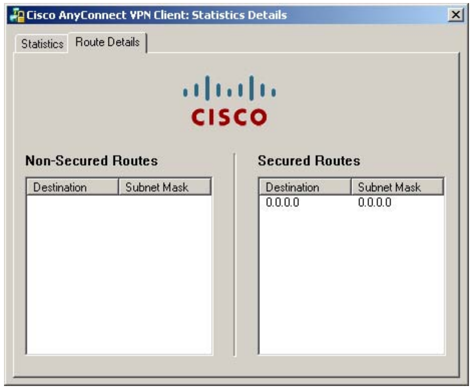
Maximum Performance

Split Tunneling

Enforced via Set of Routes on Client

No Split Tunneling (Default)

Tunnel All

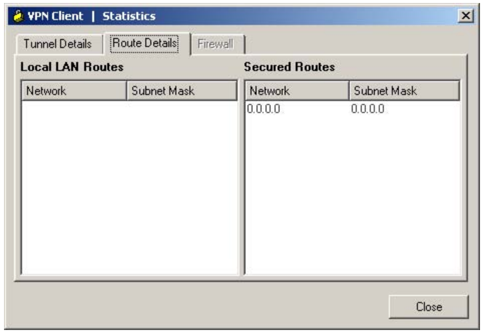


Non-Secured Routes

Destination	Subnet Mask

Secured Routes

Destination	Subnet Mask
0.0.0.0	0.0.0.0



Local LAN Routes

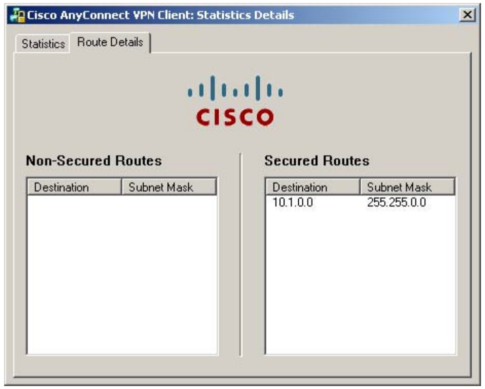
Network	Subnet Mask

Secured Routes

Network	Subnet Mask
0.0.0.0	0.0.0.0

With Split Tunneling

Tunnel List

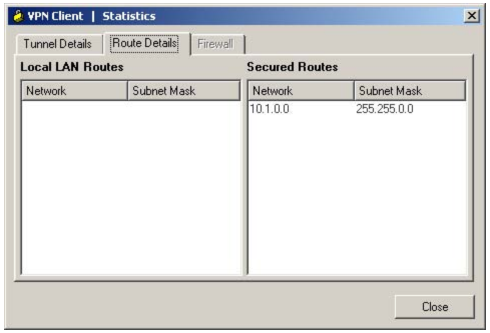


Non-Secured Routes

Destination	Subnet Mask

Secured Routes

Destination	Subnet Mask
10.1.0.0	255.255.0.0



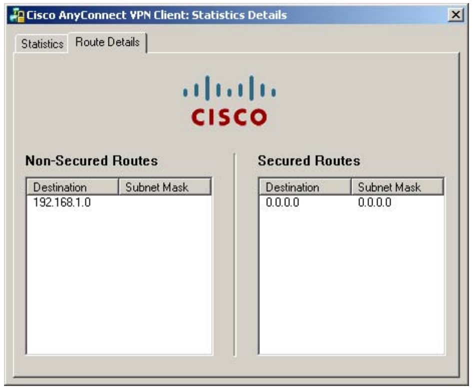
Local LAN Routes

Network	Subnet Mask

Secured Routes

Network	Subnet Mask
10.1.0.0	255.255.0.0

Exclude List

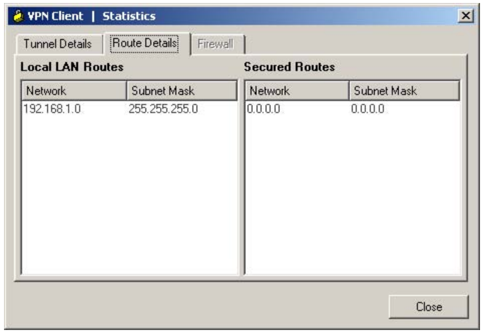


Non-Secured Routes

Destination	Subnet Mask
192.168.1.0	

Secured Routes

Destination	Subnet Mask
0.0.0.0	0.0.0.0



Local LAN Routes

Network	Subnet Mask
192.168.1.0	255.255.255.0

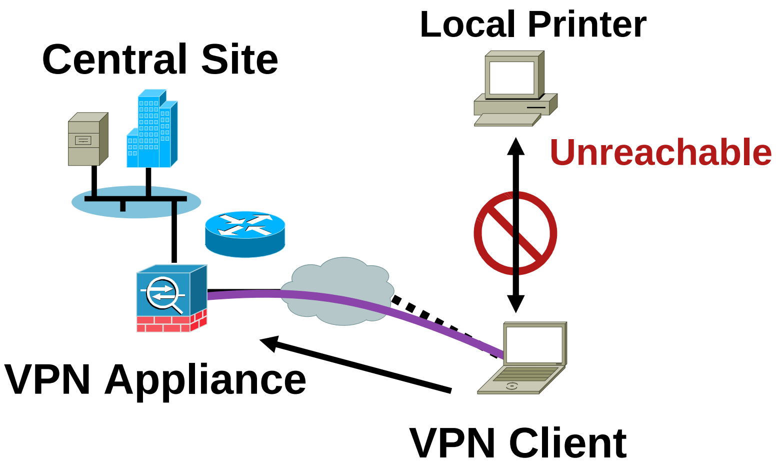
Secured Routes

Network	Subnet Mask
0.0.0.0	0.0.0.0

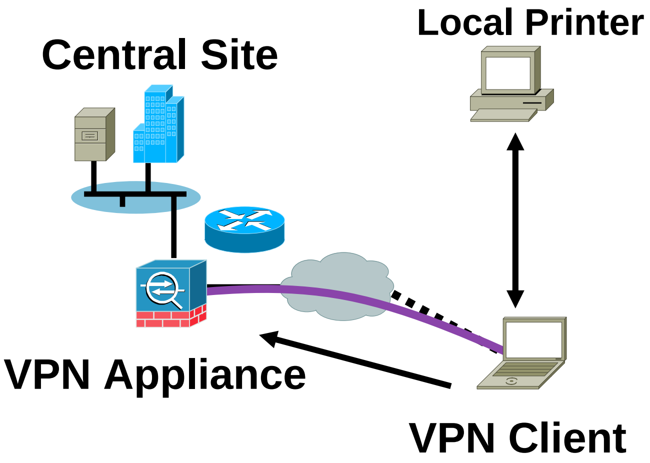
Local (LAN) Access

Remote Access Client or Device

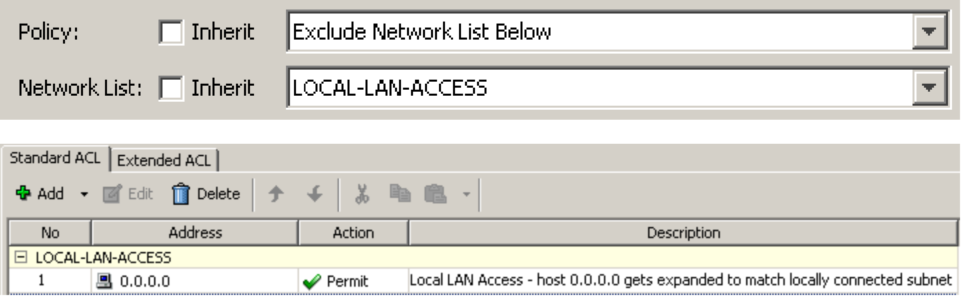
Without Local LAN Access



With Local LAN Access



Split Tunneling Special Case



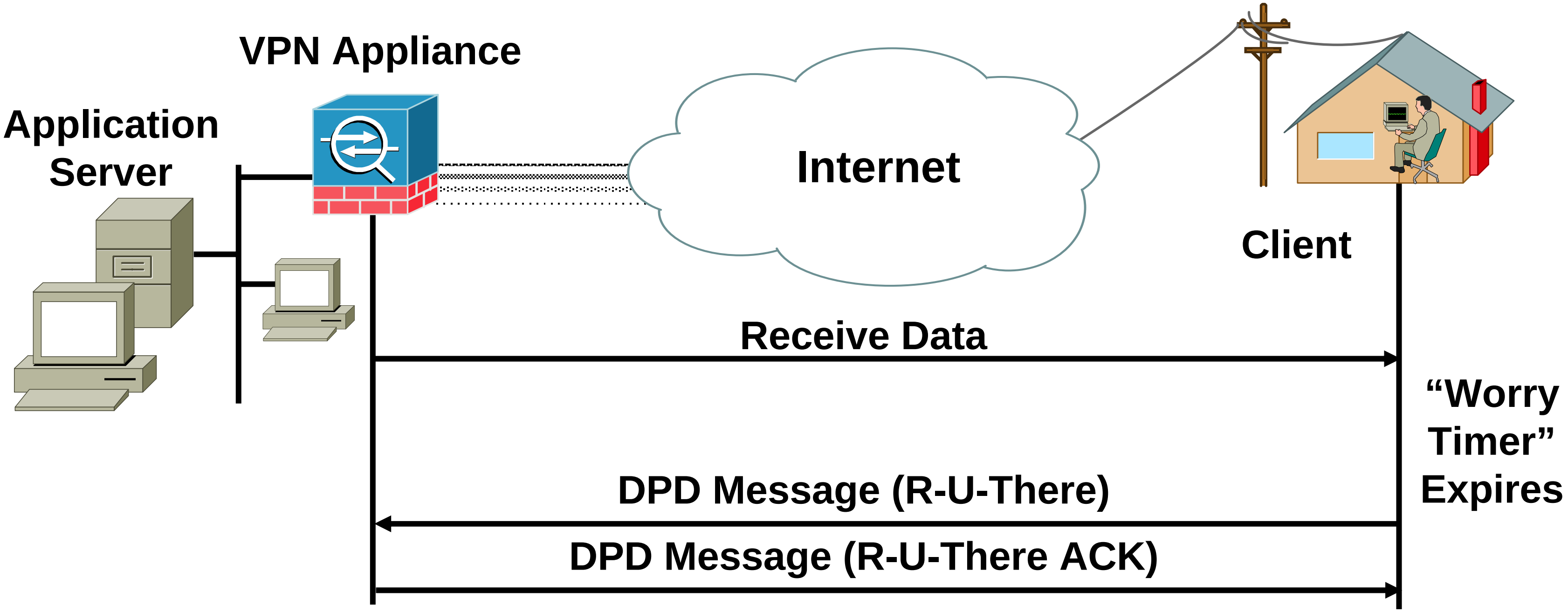
Policy: □ Inherit Exclude Network List Below

Network List: □ Inherit LOCAL-LAN-ACCESS

No	Address	Action	Description
LOCAL-LAN-ACCESS			
1	0.0.0.0	✓ Permit	Local LAN Access - host 0.0.0.0 gets expanded to match locally connected subnet

Note: Requires checkbox on IPsec client

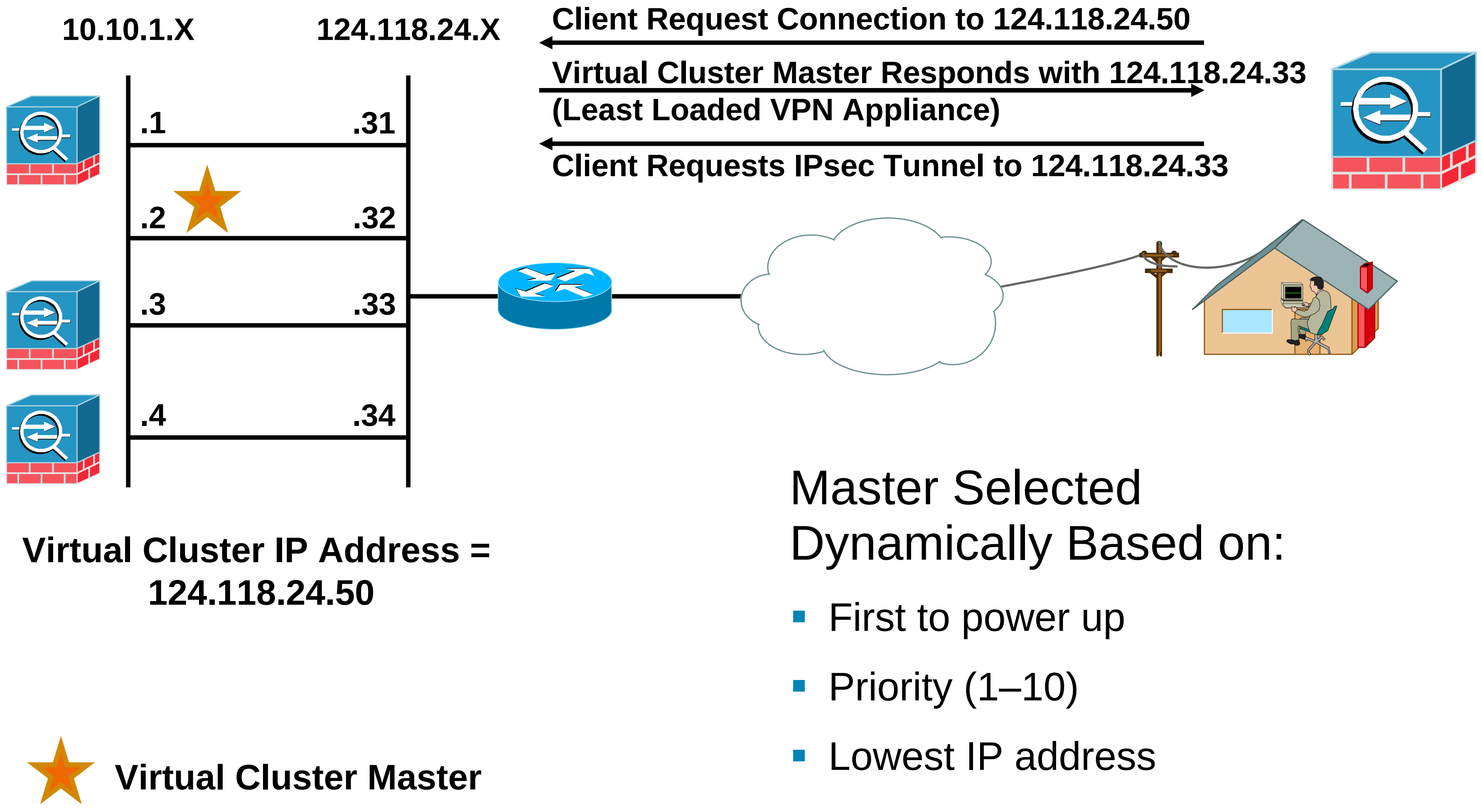
Dead Peer Detection (DPD)



- DPD is a special type of IKE keepalive for remote access IPsec clients
- Make sure the headend devices support the same type of keepalives
- Only when no traffic

See RFC 3706 for more detail

Local/Geographical Failover/ Load Balancing



Client Request Connection to 124.118.24.50

Virtual Cluster Master Responds with 124.118.24.33 (Least Loaded VPN Appliance)

Client Requests IPsec Tunnel to 124.118.24.33

Virtual Cluster IP Address = 124.118.24.50

★ Virtual Cluster Master

Master Selected Dynamically Based on:

- First to power up
- Priority (1–10)
- Lowest IP address

Backup Peers

- Configure locally or pushed from head-end
- Locally

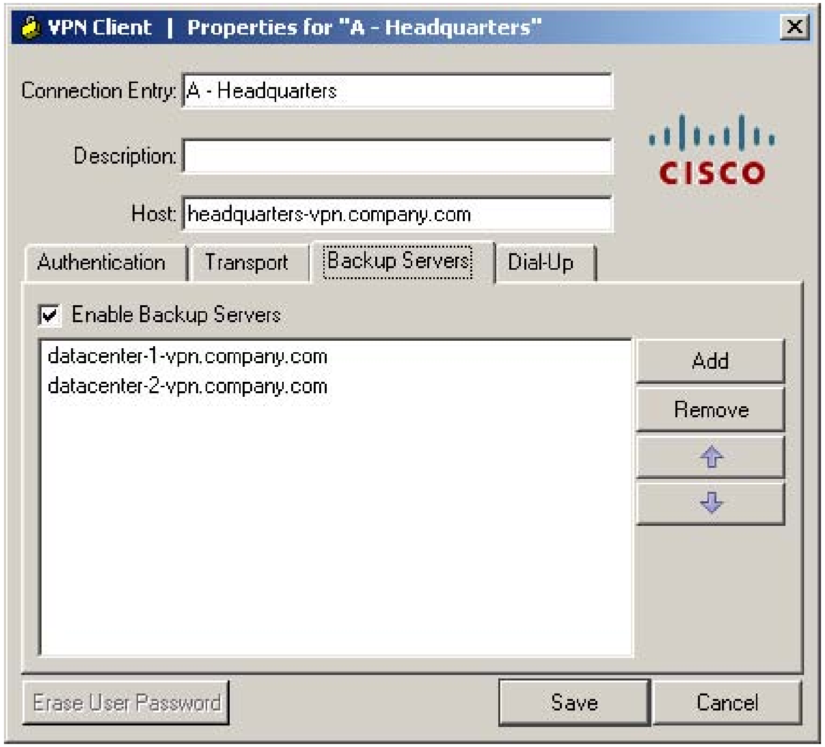
  Included in profile

  Can be part of client install script
- Head-end

  Keep client settings

  Clear client settings

  Force use of listed servers



VPN Client | Properties for "A - Headquarters"

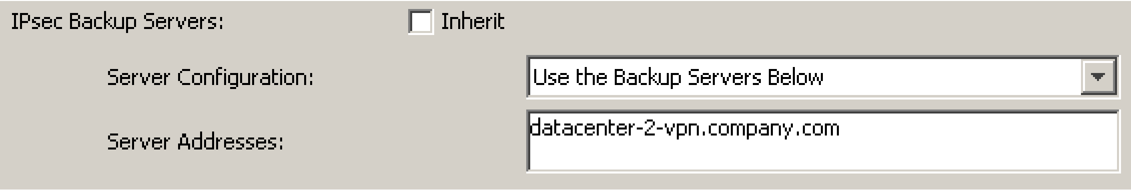
Connection Entry: A - Headquarters

Description:

Host: headquarters-vpn.company.com

☑ Enable Backup Servers

datacenter-1-vpn.company.com
datacenter-2-vpn.company.com



IPsec Backup Servers: □ Inherit

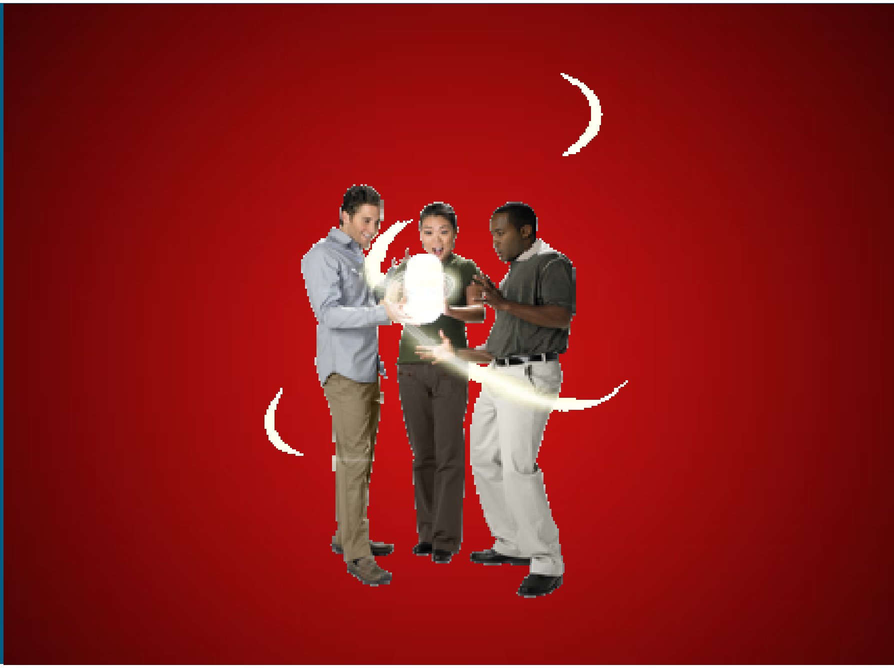
Server Configuration: Use the Backup Servers Below

Server Addresses: datacenter-2-vpn.company.com

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:
  - Cisco VPN Client auto-initiation—simple to deploy, limited flexibility
  - Cisco AnyConnect or Cisco VPN Client API—more complex to initially deploy, unlimited flexibility

Endpoint Security



Endpoint Security Capabilities

- Embedded capabilities on VPN Security Appliance
  - Time based access hours
  - Network ACL filters
  - Web ACL filters
  - Cisco Secure Desktop (CSD)
  - Host Scanning
  - Dynamic Access Policies (DAP)
- Extended capabilities with Network Admission Control
  - Network Admission Control (NAC) Appliance

Endpoint Security

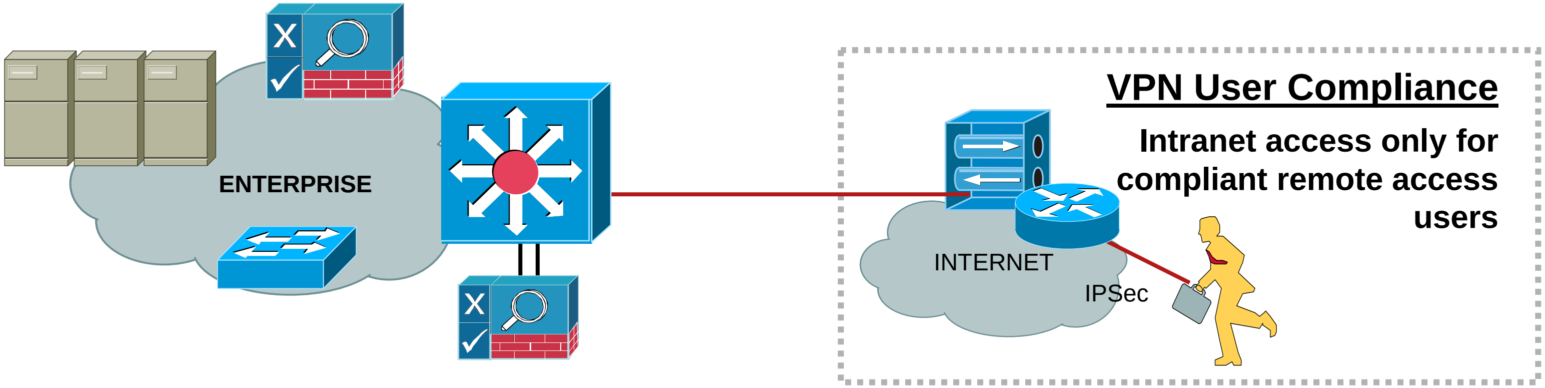
Best Practices by Access Method

- Full Tunneling (IPsec and SSL)
  - Consider as a remote node on network
  - Grant conditional access based on identity and security posture
  - Use Network ACLs filtering to limit access
- Clientless SSL VPN
  - Grant access for specific applications only
  - Grant conditional access based on identity and security posture
  - Use Web ACL filtering to limit access
  - Protect against leakage of confidential data

Endpoint Control for IPsec Full Tunnel

Cisco VPN Client

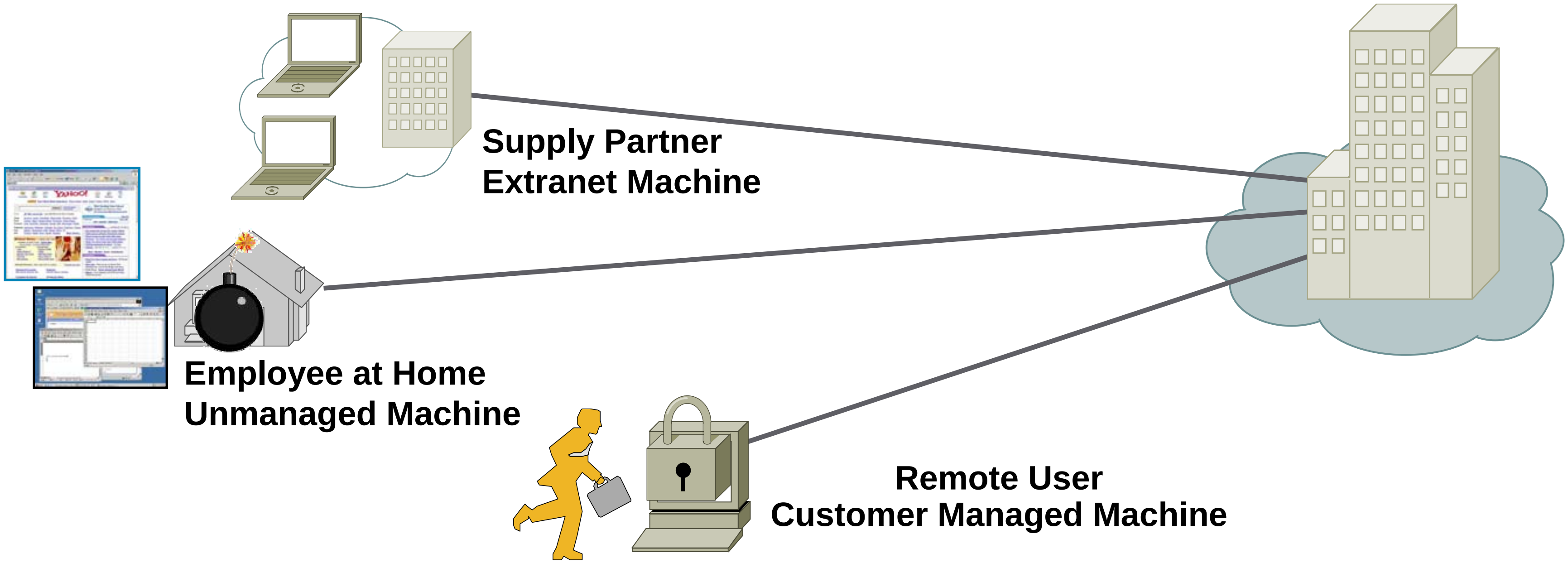
- Policies for users and groups
  - Assign IP address based on user/group identity
  - Apply network ACL filter
  - Restrict access to VLAN
- Policies applied via NAC Appliance



VPN User Compliance

Intranet access only for compliant remote access users

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?

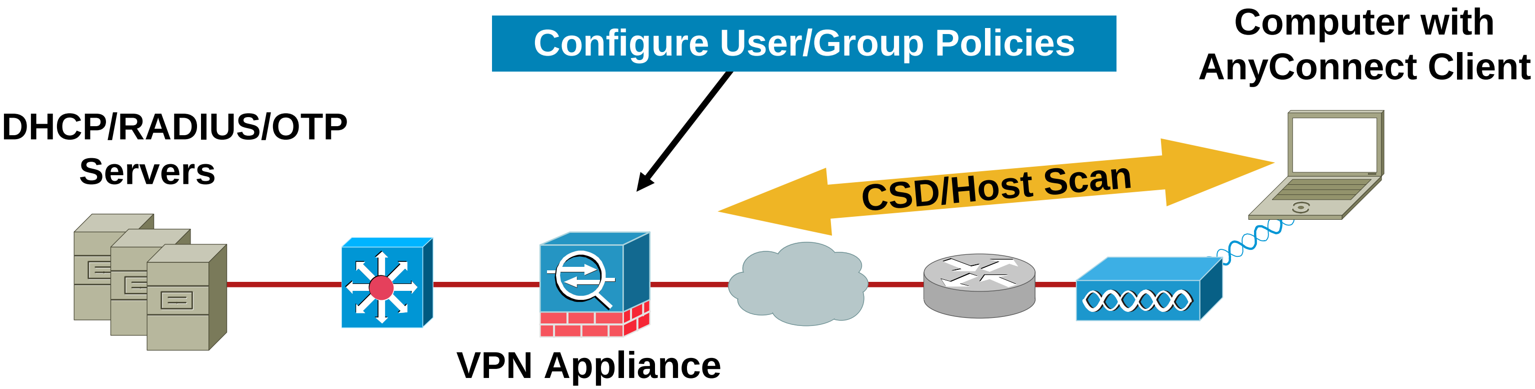
After SSL VPN Session

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

Endpoint Control for SSL Full Tunnel

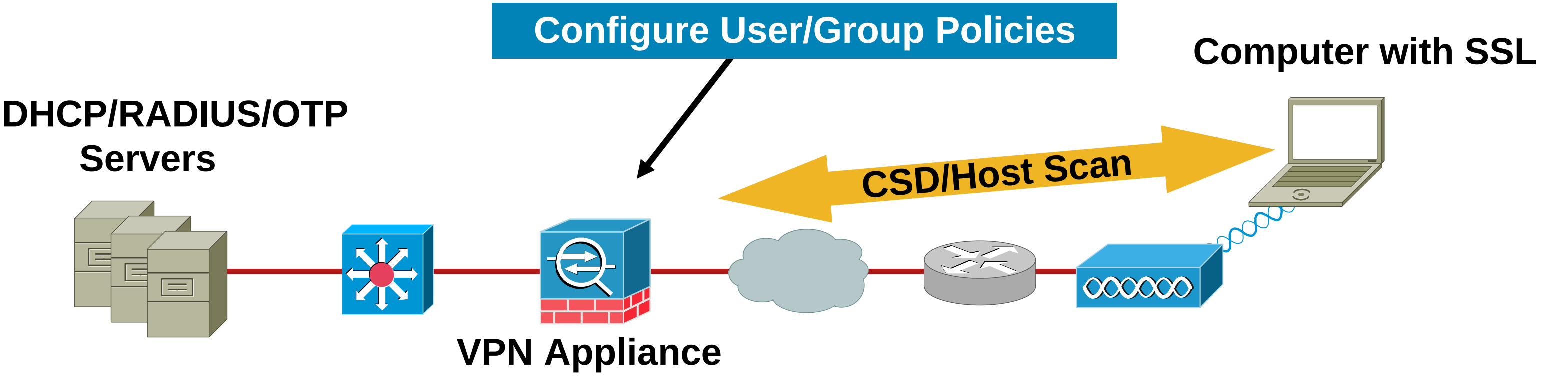
AnyConnect Client

- 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


Configure User/Group Policies
Computer with AnyConnect Client
DHCP/RADIUS/OTP Servers
CSD/Host Scan
VPN Appliance

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)



Protection of Confidential Information

The Risk of VPN on Public Systems

- Cookies

    Usernames and passwords

- URL history
- Page caches

    Sensitive corporate data

- Downloaded files

Cisco Secure Desktop

Comprehensive Endpoint Security for SSL VPN

- Works with desktop guest permissions

  No admin privileges required

- Complete pre-connect assessment:

  Location assessment—managed or unmanaged desktop?

  Gathers data for Dynamic Access Policy

  Specific applications running—defined by admin

- Comprehensive session protection:

  Malware detection

  Data sandbox and encryption protects every aspect of session

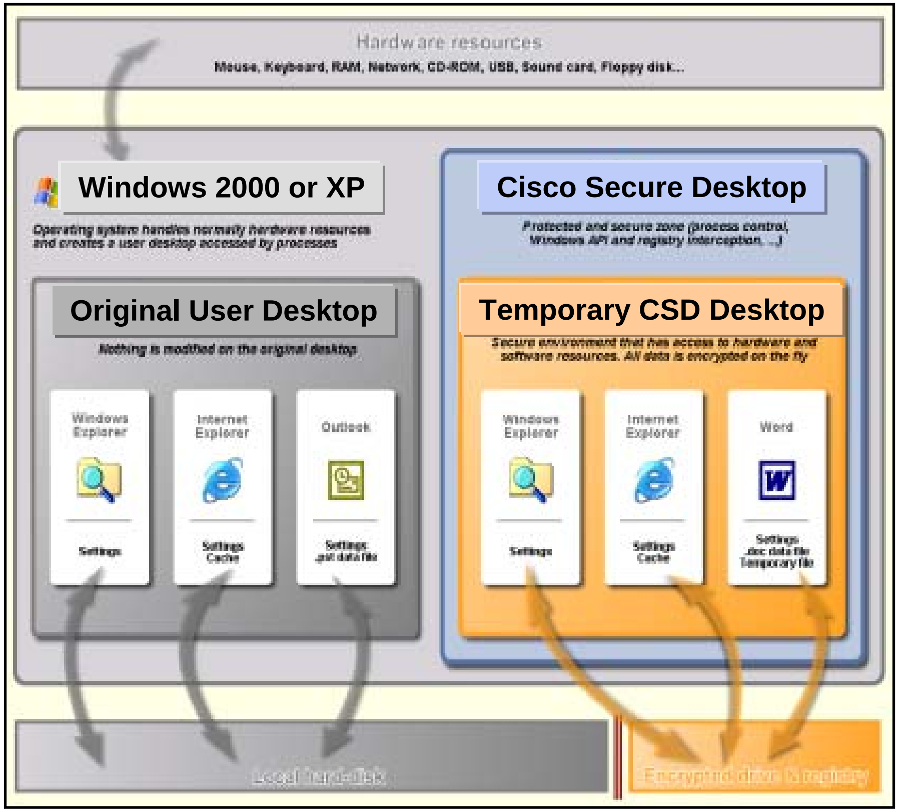
- Post-session clean-up:

  Encrypted partition overwrite (not just deletion) using DoD algorithm

  Cache, history and cookie overwrite

  File download and email attachment overwrite

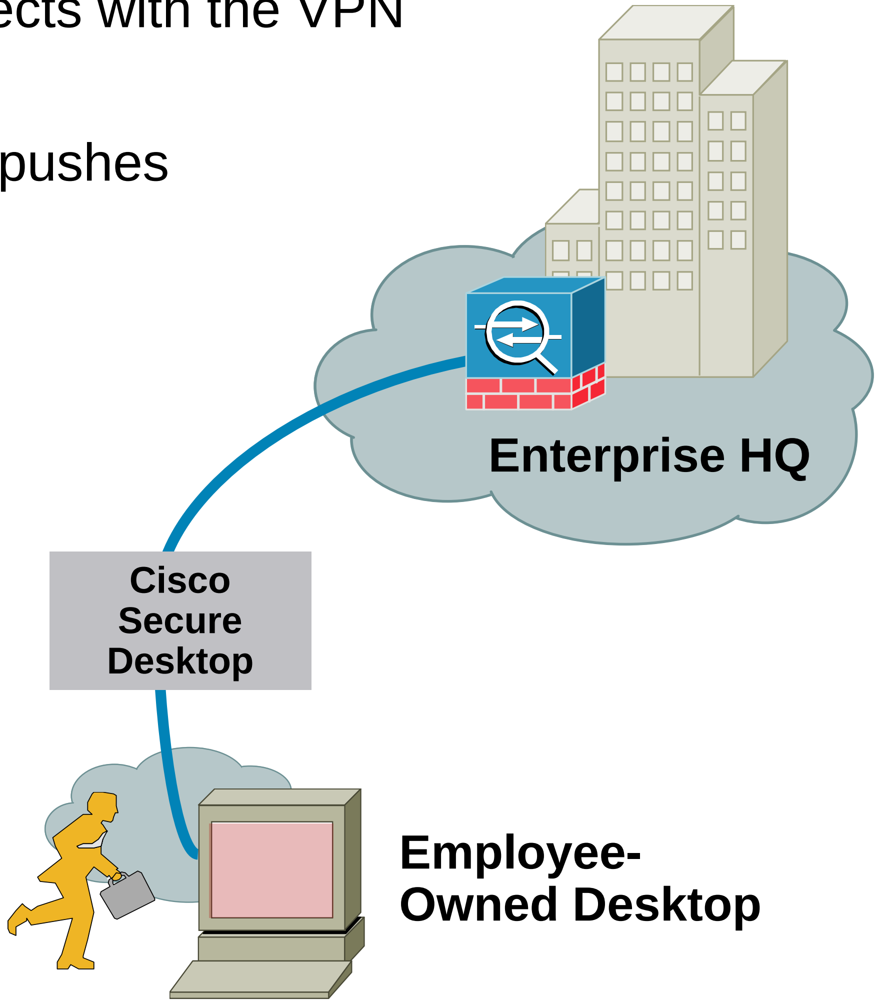
  Auto-complete password overwrite


Hardware resources
Mouse, Keyboard, RAM, Network, CD-ROM, USB, Sound card, Floppy disk...
Windows 2000 or XP
Operating system handles normally hardware resources and creates a user desktop accessed by processes
Cisco Secure Desktop
Protected and secure zone (process control, Windows API and registry interception, ...)
Original User Desktop
Nothing is modified on the original desktop
Temporary CSD Desktop
Secure environment that has access to hardware and software resources. All data is encrypted on the fly
Windows Explorer
Settings
Internet Explorer
Settings
Cache
Outlook
Settings
.pst data file
Windows Explorer
Settings
Internet Explorer
Settings
Cache
Word
Settings
.doc data file
Temporary file
Local hard-disk
Encrypted drive & registry

Cisco Secure Desktop

How it Works (Pre-Login)

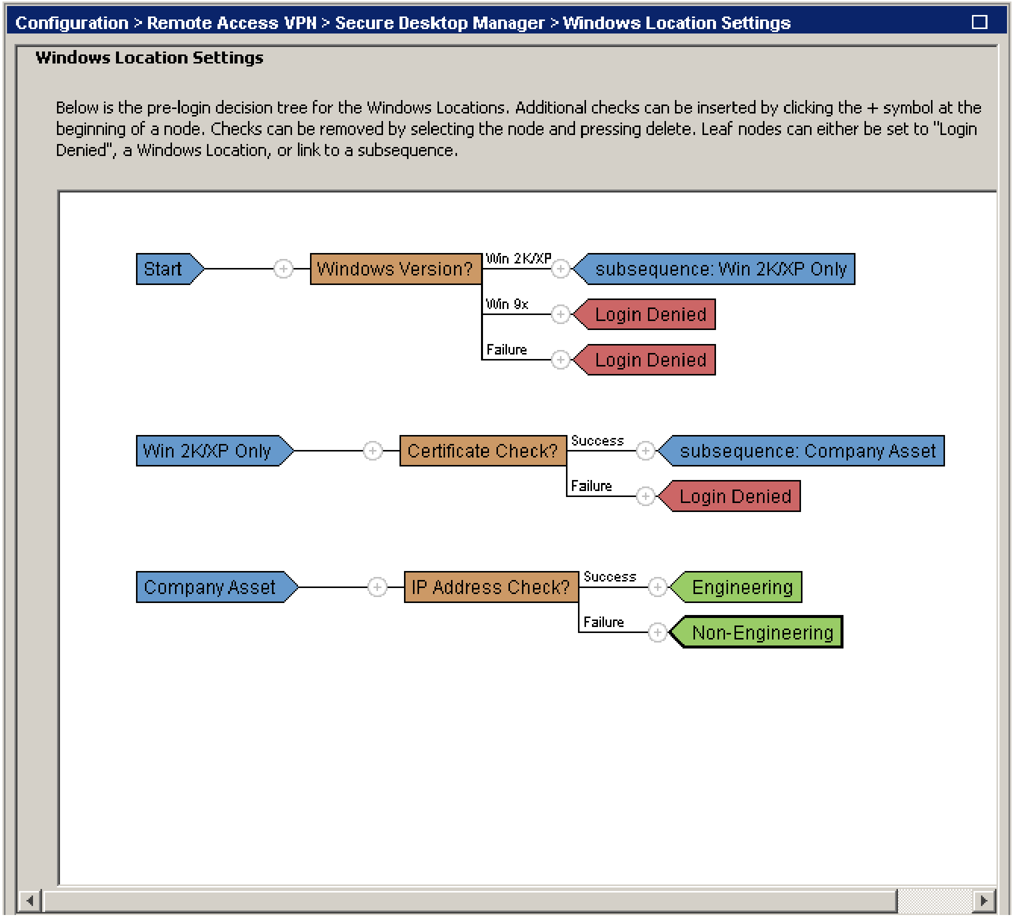
- **Step One:** A remote user connects with the VPN appliance via SSL
- **Step Two:** The VPN appliance pushes down the Secure Desktop
- **Step Three:** Based on checks, determine location (or fail login)
- **Step Four:** Based on location settings apply CSD policies



Cisco Secure Desktop

Pre-Login Decision Tree

- Supported Checks
  - Registry check
  - File check
  - Certificate check
  - Windows version check
  - IP address check
- Leaf Nodes
  - Login denied
  - Location
  - Subsequence



Configuration > Remote Access VPN > Secure Desktop Manager > Windows Location Settings

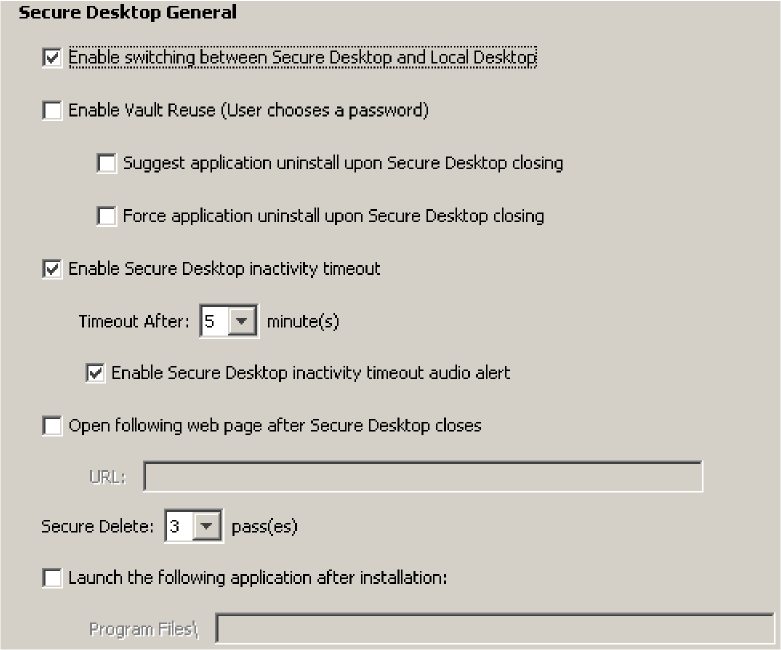
Windows Location Settings

Below is the pre-login decision tree for the Windows Locations. Additional checks can be inserted by clicking the + symbol at the beginning of a node. Checks can be removed by selecting the node and pressing delete. Leaf nodes can either be set to "Login Denied", a Windows Location, or link to a subsequence.

Cisco Secure Desktop

Location Settings

- Secure Desktop (Vault) or Cache Cleaner
- Keystroke logger and host emulation



Secure Desktop General

☑ Enable switching between Secure Desktop and Local Desktop

□ Enable Vault Reuse (User chooses a password)

  □ Suggest application uninstall upon Secure Desktop closing

  □ Force application uninstall upon Secure Desktop closing

☑ Enable Secure Desktop inactivity timeout

  Timeout After: 5 minute(s)

  ☑ Enable Secure Desktop inactivity timeout audio alert

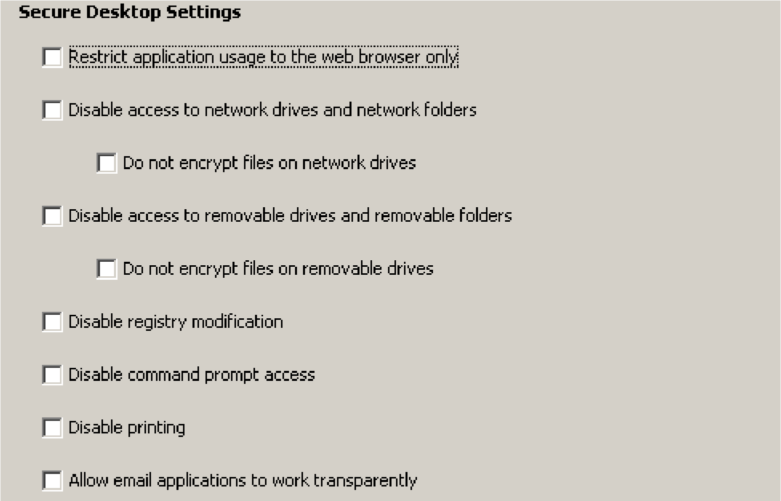
□ Open following web page after Secure Desktop closes

  URL:

Secure Delete: 3 pass(es)

□ Launch the following application after installation:

  Program Files\



Secure Desktop Settings

□ Restrict application usage to the web browser only

□ Disable access to network drives and network folders

  □ Do not encrypt files on network drives

□ Disable access to removable drives and removable folders

  □ Do not encrypt files on removable drives

□ Disable registry modification

□ Disable command prompt access

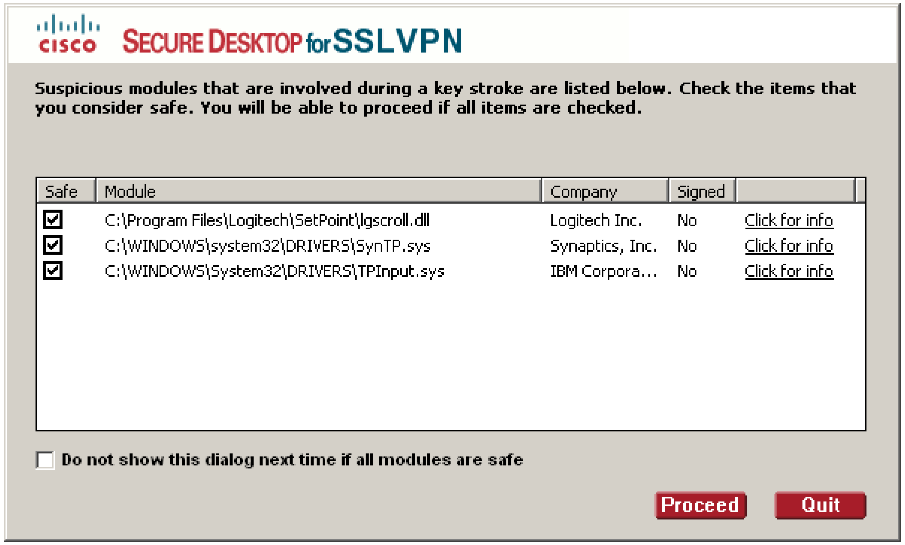
□ Disable printing

□ Allow email applications to work transparently

Cisco Secure Desktop

Keystroke Logger 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



Suspicious modules that are involved during a key stroke are listed below. Check the items that you consider safe. You will be able to proceed if all items are checked.

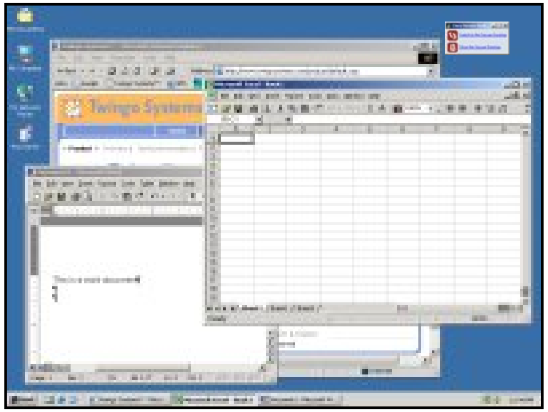
Safe	Module	Company	Signed	
☑	C:\Program Files\Logitech\SetPoint\lgscroll.dll	Logitech Inc.	No	Click for info
☑	C:\WINDOWS\system32\DRIVERS\SynTP.sys	Synaptics, Inc.	No	Click for info
☑	C:\WINDOWS\System32\DRIVERS\TPInput.sys	IBM Corpora...	No	Click for info

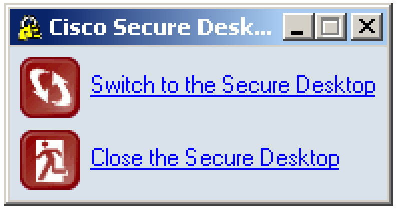
☐ Do not show this dialog next time if all modules are safe

Cisco Secure Desktop

How It Works (Login Phase)

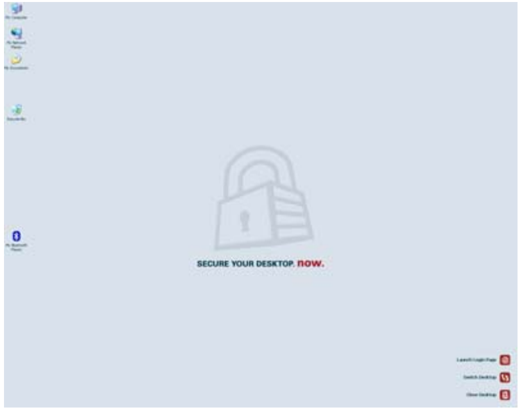
- Step Five: Check for keystroke logger and host emulation
- Step Six: Create the vault and switch to secure desktop
- Step Seven: Present login to user
- Step Eight: User logs in and initiates VPN session
- Step Nine: Host scan information gathered from endpoint for DAP




Cisco Secure Desk...

Switch to the Secure Desktop

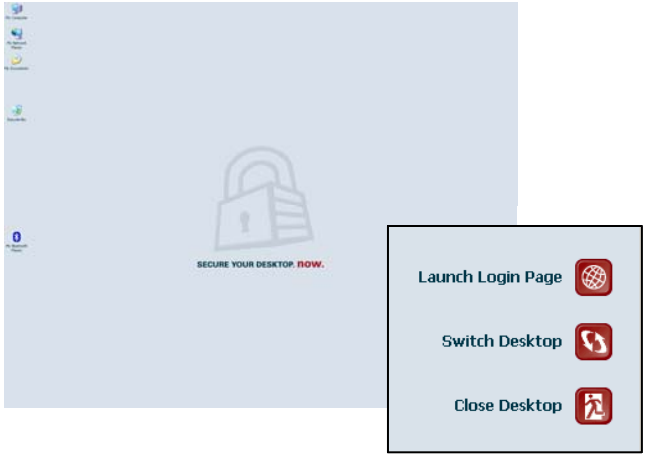
Close the Secure Desktop

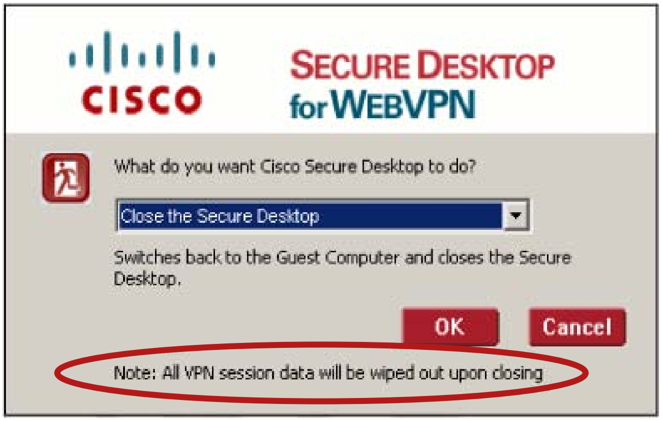


Cisco Secure Desktop

How It Works (Post Login)

- Step Ten: DAP checks applied
- Step Eleven: VPN connection active
- Step Twelve: User is able to access resources
- Step Thirteen: After session complete (or idle timeout expired) VPN is disconnected and Secure Desktop post session cleanup initiated





What do you want Cisco Secure Desktop to do?

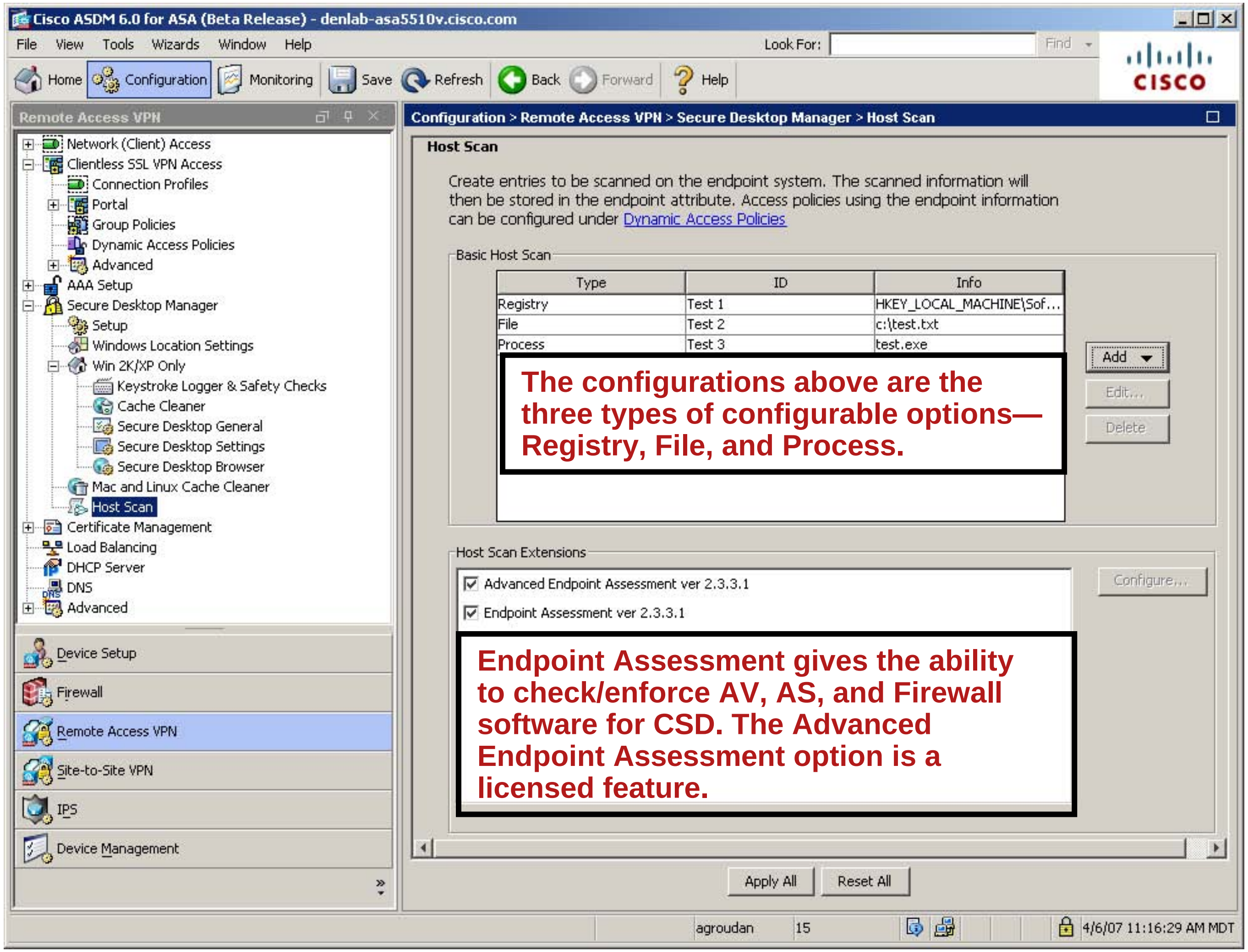
Close the Secure Desktop

Switches back to the Guest Computer and closes the Secure Desktop.

Note: All VPN session data will be wiped out upon closing

Cisco Secure Desktop

Host Scan



Host Scan

Create entries to be scanned on the endpoint system. The scanned information will then be stored in the endpoint attribute. Access policies using the endpoint information can be configured under Dynamic Access Policies

Basic Host Scan

Type	ID	Info
Registry	Test 1	HKEY_LOCAL_MACHINE\Sof...
File	Test 2	c:\test.txt
Process	Test 3	test.exe

The configurations above are the three types of configurable options—Registry, File, and Process.

Host Scan Extensions

☑ Advanced Endpoint Assessment ver 2.3.3.1

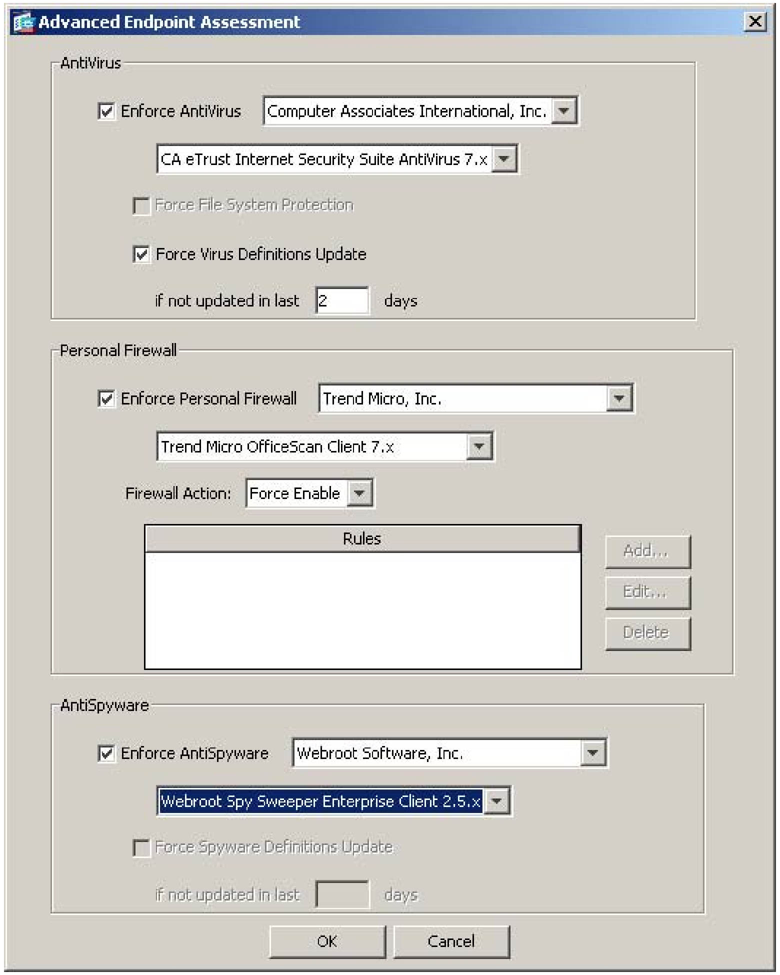
☑ Endpoint Assessment ver 2.3.3.1

Endpoint Assessment gives the ability to check/enforce AV, AS, and Firewall software for CSD. The Advanced Endpoint Assessment option is a licensed feature.

Advanced Endpoint Assessment

Built-in Enforcement Capability

- Supported endpoint components
  - Anti-Virus
  - Personal Firewall
  - Anti-Spyware
- Licensed feature
- Regular updates provided
- No Dynamic Access Policies required



Advanced Endpoint Assessment

AntiVirus

☑ Enforce AntiVirus: Computer Associates International, Inc.

CA eTrust Internet Security Suite AntiVirus 7.x

□ Force File System Protection

☑ Force Virus Definitions Update

if not updated in last 2 days

Personal Firewall

☑ Enforce Personal Firewall: Trend Micro, Inc.

Trend Micro OfficeScan Client 7.x

Firewall Action: Force Enable

Rules

AntiSpyware

☑ Enforce AntiSpyware: Webroot Software, Inc.

Webroot Spy Sweeper Enterprise Client 2.5.x

□ Force Spyware Definitions Update

if not updated in last days

Dynamic Access Policies

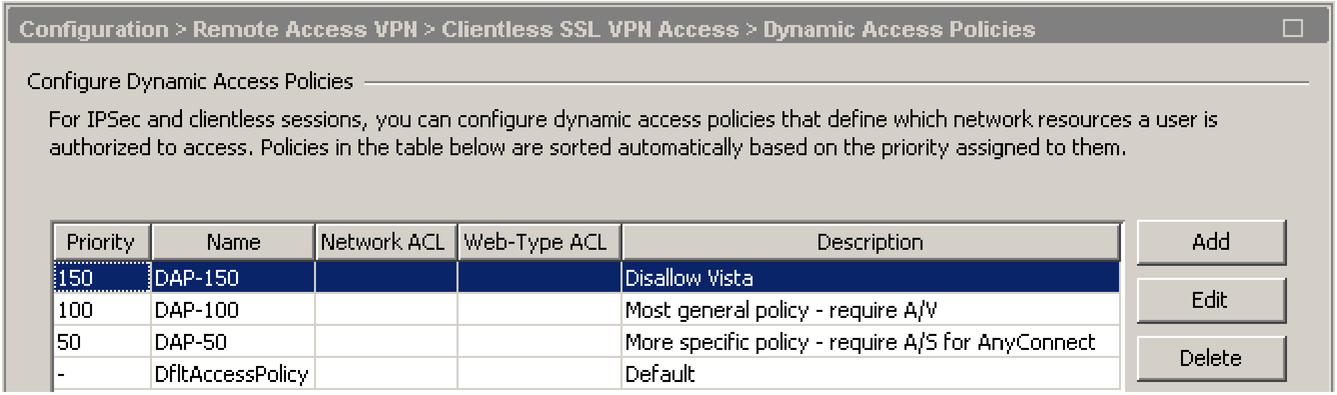
- Rulesets based on attributes
- Can terminate connection based on any match
- Can continue to evaluate against multiple rules
- Access Policy Attributes

  Network ACL and Web ACL Filters

  Portal Function Restrictions

  Port Forwarding and URL Lists

  Access Methods


Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies
Add
Edit
Delete

Configure Dynamic Access Policies

For IPSec and clientless sessions, you can configure dynamic access policies that define which network resources a user is authorized to access. Policies in the table below are sorted automatically based on the priority assigned to them.

Priority	Name	Network ACL	Web-Type ACL	Description
150	DAP-150			Disallow Vista
100	DAP-100			Most general policy - require A/V
50	DAP-50			More specific policy - require A/S for AnyConnect
-	DfltAccessPolicy			Default

Dynamic Access Policies

Endpoint Attributes

Host Scan

- Endpoint Assessment

  endpoint.fw {personal firewall}

  endpoint.as {anti-spyware}

  endpoint.av {anti-virus}

Secure Desktop

- OS Attributes

  endpoint.os.version

  endpoint.os.servicepack

  endpoint.policy.location

- Custom Scans

  endpoint.registry

  endpoint.file

  endpoint.process

Note: Cisco Secure Desktop must be enabled to return these attributes

Dynamic Access Policies

Additional Attributes

AAA

- Cisco
  - aaa.cisco.memberof
  - aaa.cisco.username
  - aaa.cisco.class
  - aaa.cisco.ipaddress
  - aaa.cisco.tunnelgroup
- LDAP
  - aaa.ldap.<label>
- RADIUS
  - aaa.ldap.<label>

Access Method

- Application (client type)
  - endpoint.application.clientype

NAC Appliance

- VLAN ID
  - endpoint.vlan.id
- VLAN Type
  - endpoint.vlan.type

NAC

- NAC Posture
  - endpoint.nac.status

DAP Posture Assessment

Capability by Connection Protocol

	Host Scan	Vault	NAC Appliance
Cisco VPN Client	No	N/A	Yes
Cisco AnyConnect VPN Client	Yes	Yes	Yes
Clientless SSL	Yes	Yes	No

Q and A

Key Takeaways

What Solution Fits Your Situation Best?

- If your customers carry their pc/laptop and installing a client is not an issues then focus on AnyConnect

  AnyConnect is the client for the future

- If your customers access corporate resources sporadically or you require access from non-employees then clientless SSL is best

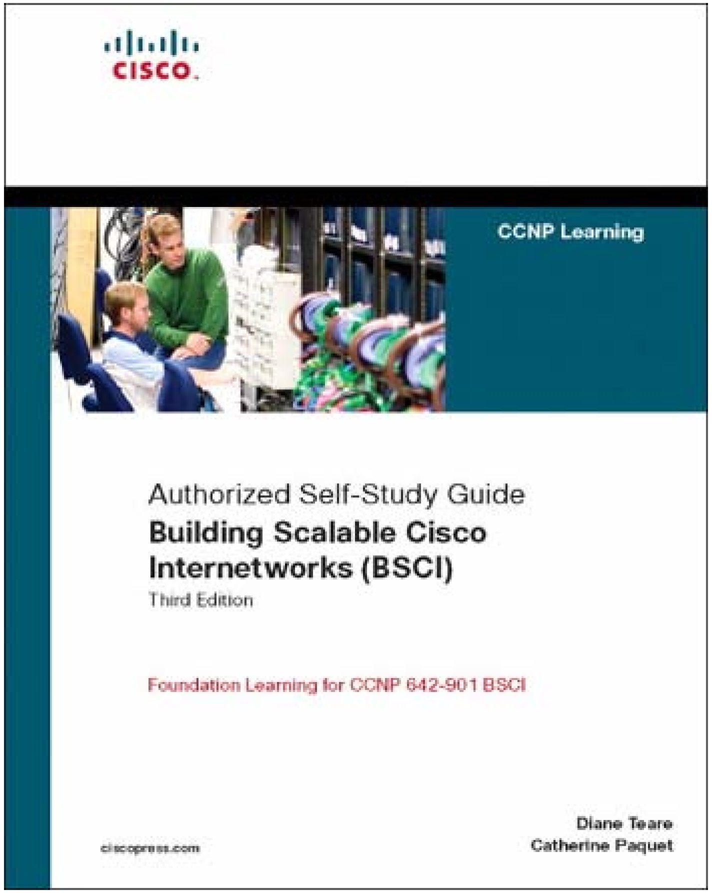
  Good for partner and occasional guest access

  Good for employees that need basic services

- If you workforce is dedicated telecommuters look into a hardware solution

Recommended Reading

- Continue your Cisco Live learning experience with further reading from Cisco Press®
- Check the Recommended Reading flyer for suggested books



cisco.

CCNP Learning

Authorized Self-Study Guide

Building Scalable Cisco Internetworks (BSCI)

Third Edition

Foundation Learning for CCNP 642-901 BSCI

ciscopress.com

Diane Teare
Catherine Paquet

Available Onsite at the Cisco Company Store

Recommended Reading Flyer

- 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

- Give us your feedback and you could win fabulous prizes; winners announced daily
- Receive 20 Passport points for each session evaluation you complete
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center

Don’t forget to activate your Cisco Live virtual account for access to all session material on-demand and return for our live virtual event in October 2008.

Go to the Collaboration Zone in World of Solutions or visit www.cisco-live.com.