Deploying Remote-Access SSL & IPsec VPNs
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

Branch Office

VPN Remote

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

Internet

VPN Server

HQ

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

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

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

<table>
<thead>
<tr>
<th>Clientless (L7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clientless/AnyConnect VPN Client</td>
</tr>
<tr>
<td><strong>Partner</strong>—Few apps/servers, tight access control, no control over desktop software environment, firewall traversal</td>
</tr>
<tr>
<td><strong>Doctor</strong>—Occasional access, few apps, no desktop software control</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Full Network Access (L3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco VPN Client</td>
</tr>
<tr>
<td><strong>Engineer</strong>—Many servers/apps, needs native app formats, VoIP, frequent access, long connect times</td>
</tr>
<tr>
<td><strong>Account Manager</strong>—Diverse apps, home-grown apps, always works from enterprise-managed desktop</td>
</tr>
</tbody>
</table>
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

Cisco AnyConnect VPN Client (SSL/DTLS Client) discussed later
SSL VPN Clientless (L7) Customization

Customizable Banner Graphic

Customizable Access Methods

Customizable Links, Network Resource Access

Localized

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**
  Citrix 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

- 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
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
SSL VPN: Cisco AnyConnect VPN Client

Connect Options

- Web-based Initiation
  - Portal

- Standalone Mode
  - Shortcut
  - Start Menu
  - Command Line
## Client Comparison

### Key Differences

<table>
<thead>
<tr>
<th></th>
<th>Cisco VPN Client</th>
<th>Cisco AnyConnect VPN client</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Approximate Size</strong></td>
<td>~10 MB</td>
<td>~1.2 MB</td>
</tr>
<tr>
<td><strong>Initial Install</strong></td>
<td>Distribute</td>
<td>Auto Download Distribute</td>
</tr>
<tr>
<td><strong>Admin Rights Required</strong></td>
<td>Yes</td>
<td>Yes Initial Install Only</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>IPsec</td>
<td>DTLS, TLS</td>
</tr>
<tr>
<td><strong>OS Support</strong></td>
<td>Multiple*</td>
<td>Multiple**</td>
</tr>
<tr>
<td><strong>Head End</strong></td>
<td>Cisco ASA/Cisco PIX/Cisco IOS</td>
<td>Cisco ASA/Cisco IOS</td>
</tr>
<tr>
<td><strong>Client Reboot Required</strong></td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

* 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

![Diagram showing VLANs and policies for internal and shared resources]
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

![Routing Diagram](image)

**VPN Security Appliance Uses Proxy-ARP**

![Routing Diagram](image)

**Downstream Router Requires a Specific Route**
Routing Design Consideration

- 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).

Tech Tip
Create summary route to prevent route table recalculation.
Client Authentication Design

- VPNs can utilize many types of databases for centralized authentication
  - Username and password
  - Tokens
  - Digital certificate/smartcards

- 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
Virtual Keyboard
All Clientless SSL VPN Pages Requiring Authentication
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)

![Diagram showing standard IPsec packet and how NAT devices cannot map it](image)

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

NAT Gateway
Uses PAT to Hide RFC 1918 Addresses

See RFCs 3947 and 3948 for more detail
NAT Transparency
UDP Encapsulation

Cisco VPN Client

- 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

VPN Security Appliance
NAT Transparency
TCP Encapsulation

Cisco VPN Client

- 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

VPN Security Appliance

Enable IKE
- Inside: No
- outside: Yes
- shared: No
Firewall Traversal

**SSL VPN**

- HTTPS—TCP/443
  - Will fallback to TCP
- DTLS—UDP/443
  - Will fallback to TCP
- HTTP—TCP/80
  - If HTTP redirection desired

**IPsec VPN**

- 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)

The ports and protocols listed must be open for a remote user to be able to connect successfully.
Split Tunneling
Remote Access Client or Device

**Without** Split Tunneling

[Diagram showing without split tunneling]

**With** Split Tunneling

[Diagram showing with split tunneling]

**Maximum Security**

**Maximum Performance**
Split Tunneling
Enforced via Set of Routes on Client

**No Split Tunneling**
(Default)

Tunnel All

**With Split Tunneling**

Tunnel List

Exclude List
Local (LAN) Access
Remote Access Client or Device

**Without Local LAN Access**

Central Site

Local Printer

Unreachable

VPN Appliance

VPN Client

**With Local LAN Access**

Central Site

Local Printer

VPN Appliance

VPN Client

**Split Tunneling Special Case**

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

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
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
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?

Supply Partner
Extranet Machine

Employee at Home
Unmanaged Machine

Remote User
Customer Managed Machine
Endpoint Control for SSL Full Tunnel

AnyConnect Client

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

- Policies applied based on end station criteria
  - Cisco Secure Desktop (CSD)
  - Dynamic Access Policy (DAP)
  - Assign NAC policy
Endpoint Control for Clientless SSL VPN

- Policies for users and groups
  - Restrict access to VLAN
  - Apply Web ACL filter
  - Control URL entry
  - Control file server entry and browsing

- Policies applied based on end station criteria
  - Cisco Secure Desktop (CSD)
  - Dynamic Access Policy (DAP)
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
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

Below is the pre-login decision tree for the Windows Locations. Additional checks can be inserted by adding 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: [Select timeout (seconds)]
  - Enable Secure Desktop inactivity timeout audio alert
- Open following web page after Secure Desktop closes
  - URL: [Enter URL]
- Secure Delete: [Select delete option (e.g., 3 to pass(es))]
- Launch the following application after installation:
  - Program Files: [List of programs]

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
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 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
Cisco Secure Desktop
Host Scan

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

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
Dynamic Access Policies

- Rule sets 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

<table>
<thead>
<tr>
<th>Priority</th>
<th>Name</th>
<th>Network ACL</th>
<th>Web-Type ACL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>150</td>
<td>DAP-150</td>
<td></td>
<td></td>
<td>Disallow Vista</td>
</tr>
<tr>
<td>100</td>
<td>DAP-100</td>
<td></td>
<td></td>
<td>Most general policy - require A/V</td>
</tr>
<tr>
<td>50</td>
<td>DAP-50</td>
<td></td>
<td></td>
<td>More specific policy - require A/S for AnyConnect</td>
</tr>
<tr>
<td>-</td>
<td>DiffAccessPolicy</td>
<td></td>
<td></td>
<td>Default</td>
</tr>
</tbody>
</table>
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>`

#### NAC Appliance
- **VLAN ID**
  - `endpoint.vlan.id`
- **VLAN Type**
  - `endpoint.vlan.type`

#### NAC
- **NAC Posture**
  - `endpoint.nac.status`

#### Access Method
- **Application (client type)**
  - `endpoint.application.clientype`
## DAP Posture Assessment

### Capability by Connection Protocol

<table>
<thead>
<tr>
<th></th>
<th>Host Scan</th>
<th>Vault</th>
<th>NAC Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco VPN Client</td>
<td>No</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco AnyConnect</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Clientless SSL</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
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 issue 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 your 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

Available Onsite at the Cisco Company Store
Recommended Reading Flyer

- Troubleshooting Remote Access Networks

- CCSP™ Cisco Secure VPN Exam Certification Guide

- Cisco Secure Virtual Private Networks

- Network Security Architectures

- 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.