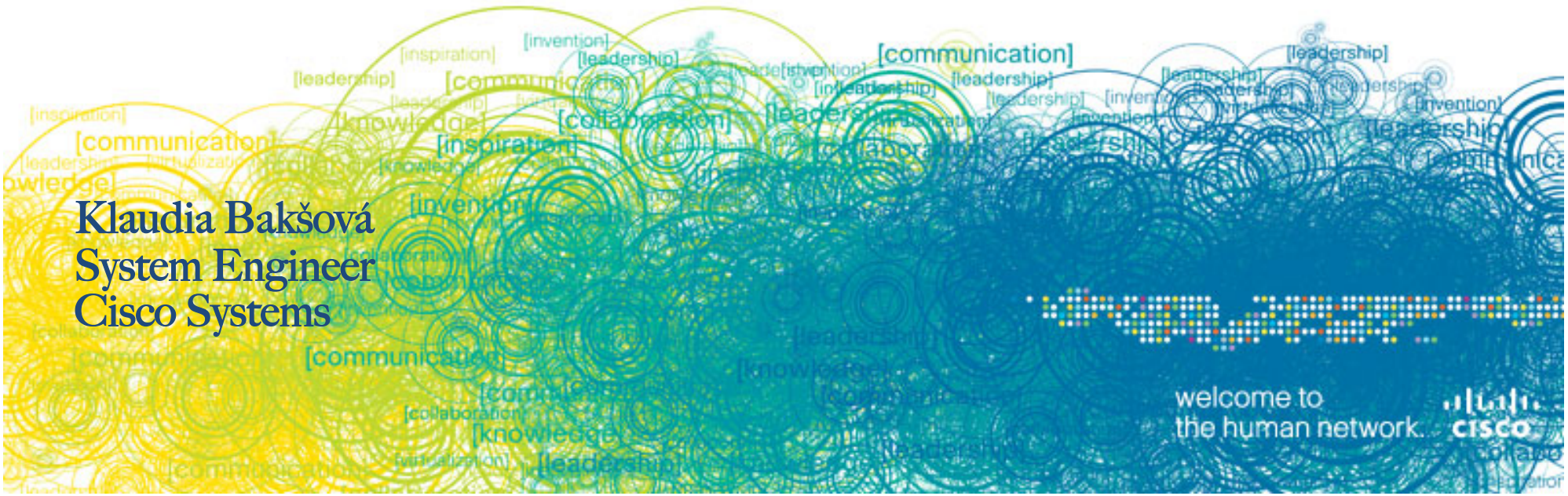
Cisco Expo
2009

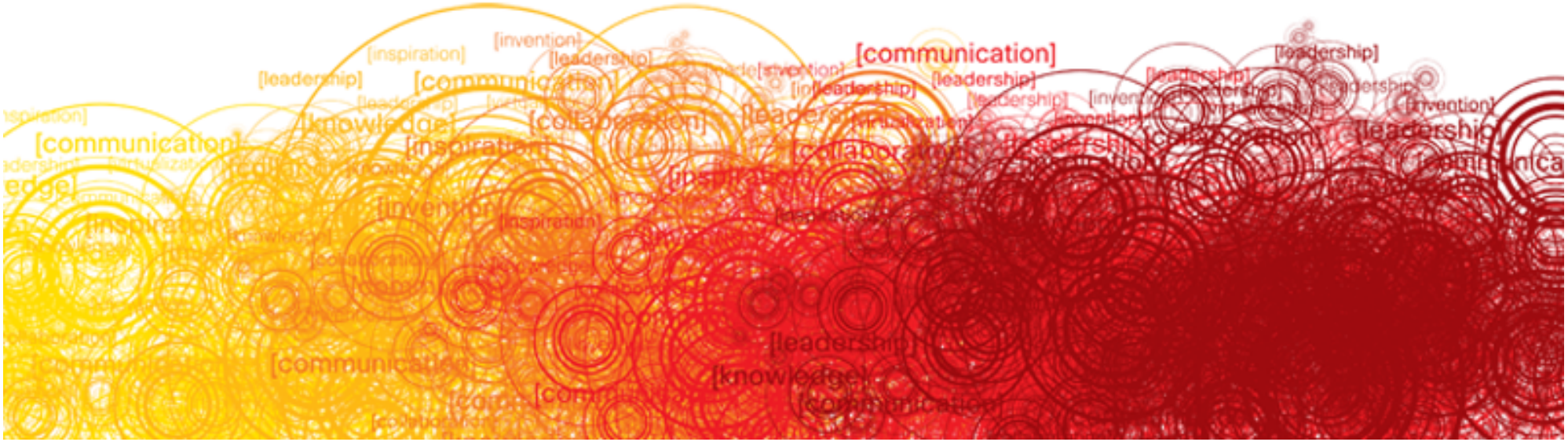
Cisco AnyConnect VPN



Klaudia Bakšová
System Engineer
Cisco Systems

Agenda

1. SSL Introduction
2. AnyConnect VPN
3. Technical Benefits



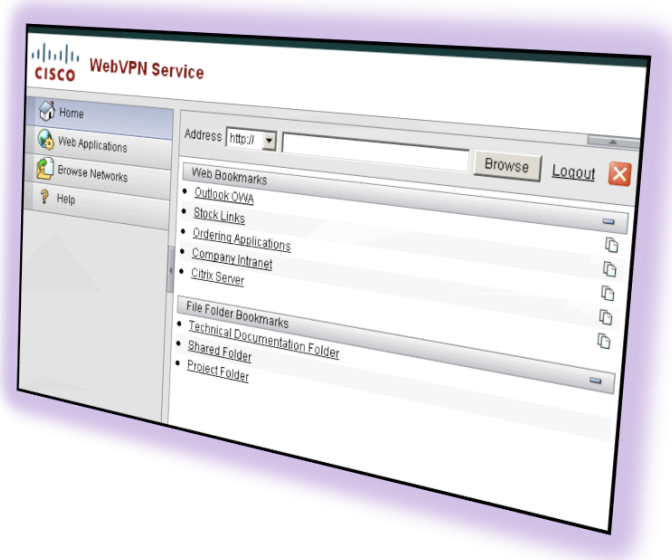
Secure Sockets Layer (SSL) Overview

- Protocol developed by Netscape for secure e-commerce – 1990s
- Application-transparent, platform-independent
- Requires reliable underlying packet delivery -> TCP
- 1999 – IETF RFC2246 – TLSv1.0
- Creates a tunnel between web browser and web server

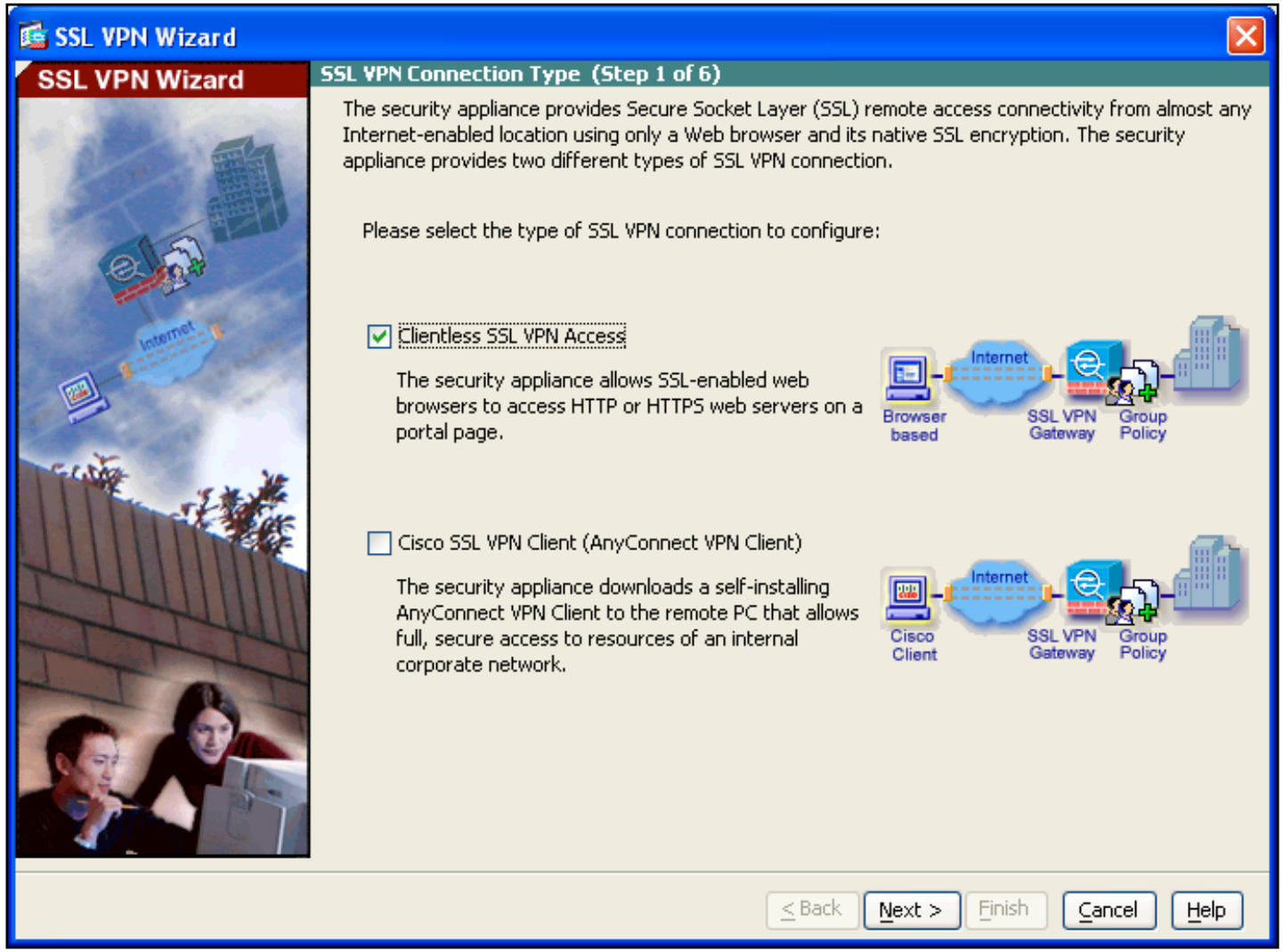
  authentication and confidentiality (RC4, 3DES, DES, AES)

  data integrity (MD5, SHA; key exchange RSA, DH)
- https://

  usually over port :443

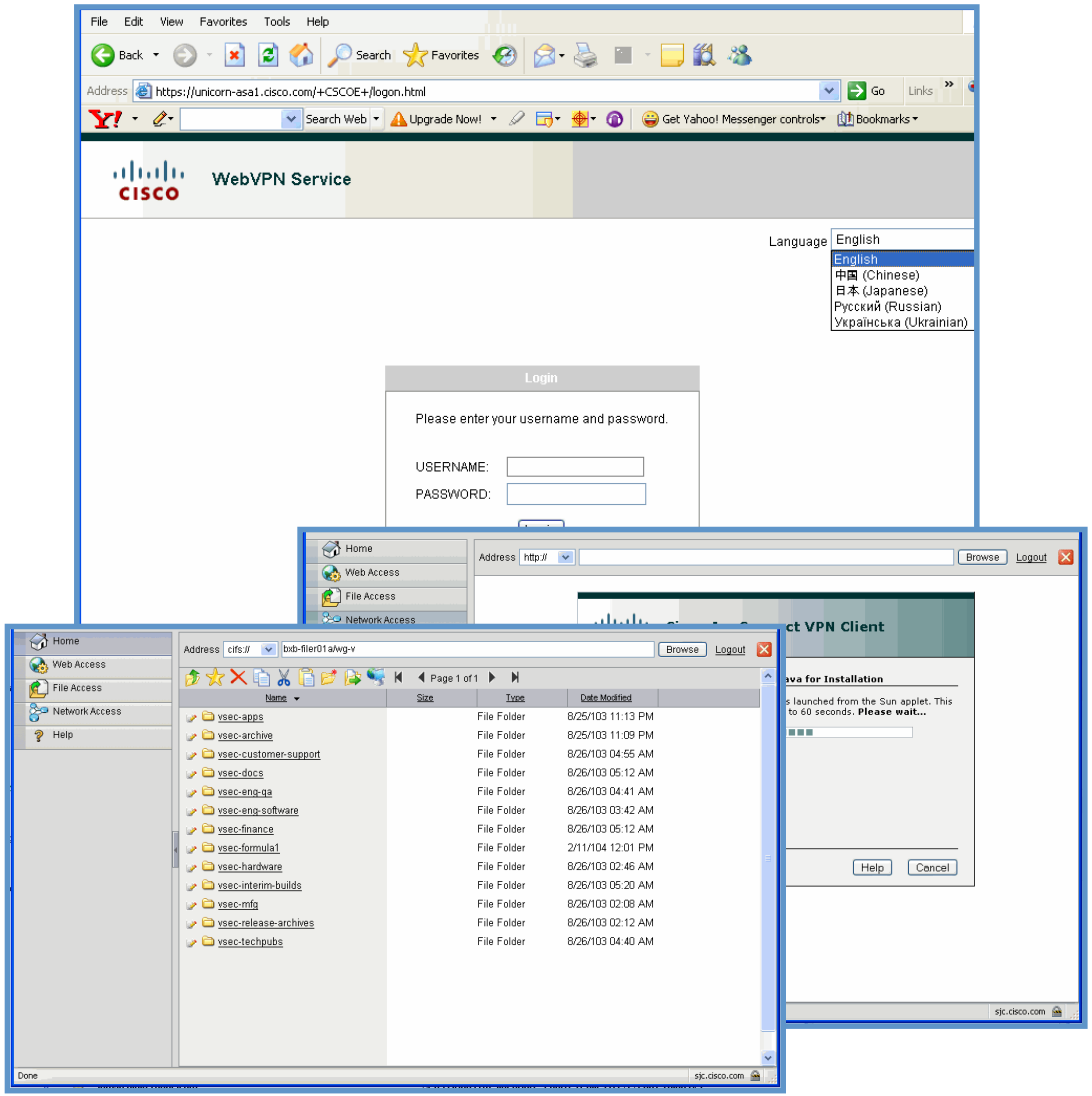


SSL or SSL VPN ???



Clientless SSL VPN
Seamless Access Anywhere

Personalized application and resource access



- **Personalized homepage**

  Localizable, RSS feeds, personal bookmarks, etc.

- **Delivers web-based and traditional applications**

  Sophisticated web and other applications delivered seamlessly to the browser

- **Intuitive user experience**

  Drag and Drop file access and 'webified' file transport

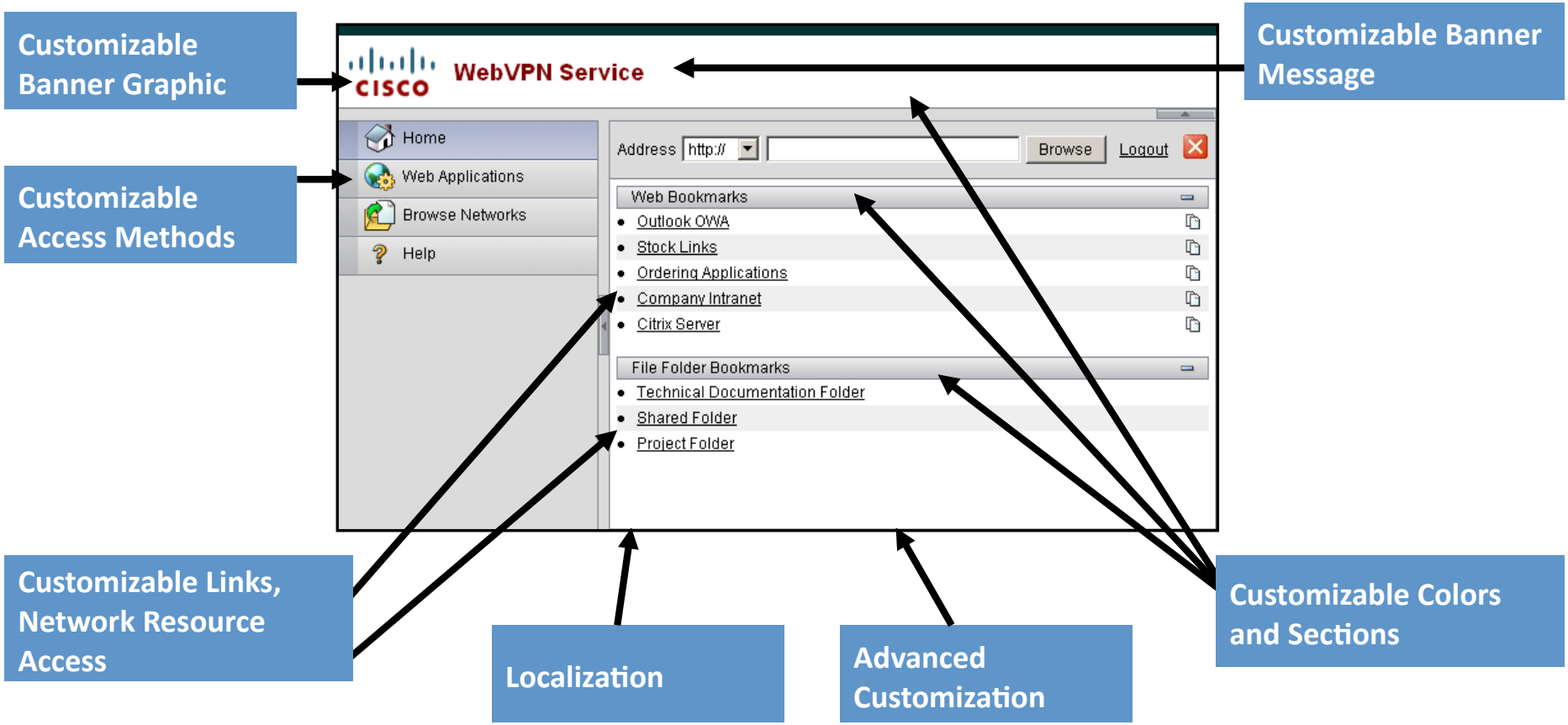
- **Delivers key applications beyond the browser**

  Smart Tunnels deliver more applications without admin privileges

- **URL Mangling/Content Rewriting**

Clientless SSL VPN
Seamless Access Anywhere

Enhanced clientless interface, highly customizable



Enhanced Clientless WebVPN

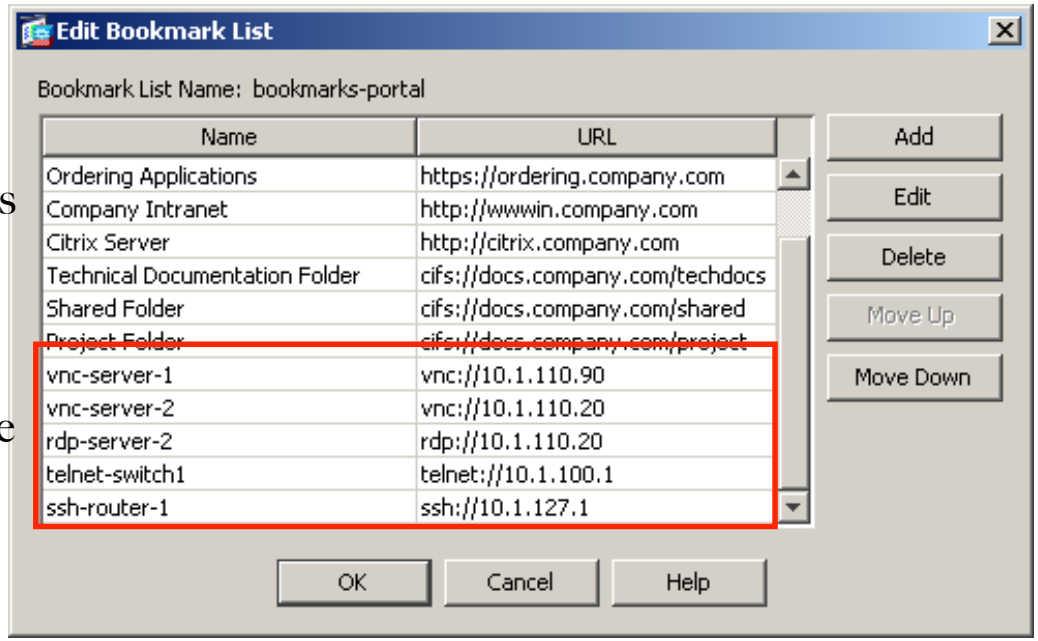
Java Client/Server Plugins

- Support for common TCP applications via Java plugins such as:
  - Windows Terminal Server (RDP)
  - TELNET & SSH
  - VNC
  - Citrix Java Presentation Server Client (plugin loaded by administrator)

- Resource is defined as a URL with the appropriate protocol type, i.e.

  rdp://server:port

- Support for these third party applications exists in the form of packaged single archive files in the .jar file format.
- Extensible plugin mechanism may provide support for additional applications in the future



Thin-Client SSL VPN

The Thin-Client SSL VPN Solution Comprises Two Major Features:
Port Forwarding and Smart Tunneling

Port Forwarding

- TCP applications only
- E-mail access
- CIFS access
- Customized user screen

Smart Tunneling

- Port-forwarding at the application layer (TCP only)
- SSL VPN loads a stub into each process spawned by an authorized application, and intercepts socket calls to redirect via ASA
- Used where other methods such as AnyConnect or port forwarding cannot be used
- Applications

Clientless WebVPN
Port Forwarding

- Port Forwarding Configuration Example:

  port-forward SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail

Application	Local Port	Server DNS Name	Remote Port	Description
IMAP4S e-mail	20143	IMAP4Sserver	143	Get Mail
SMTPS e-mail	20025	SMTPSserver	25	Send Mail
DDTS over SSH	20022	DDTSserver	22	DDTS over SSH
Telnet	20023	Telnetserver	23	Telnet

- To simplify access, temporary modifications are made to the local PC's hosts file to provide access to Port Forwarded services without requiring modification to application. Changes to hosts file requires Admin access.

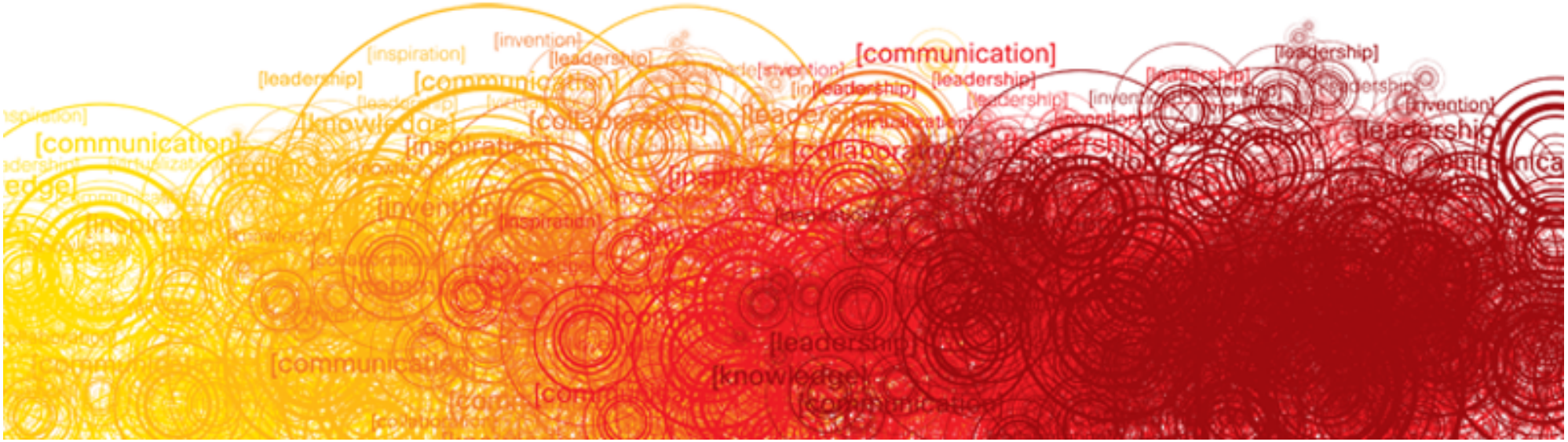
Clientless WebVPN

Smart Tunnels

- Smart Tunnels are application-level port forwarding
- It is a connection between a Winsock 2, TCP-based application and the private site, using a clientless (browser-based) SSL VPN session.
- You can specify client applications which you want to grant Smart Tunnel access including Telnet, SSH, RDP, VNC, Passive FTP, Outlook Express, Lotus Notes, Sametime, Citrix Program Neighborhood client, and Outlook via POP/SMTP/IMAP.
- SSL VPN loads a stub into each process spawned by an authorized application, and intercepts socket calls to redirect via ASA.
- This can be used where other methods such as AnyConnect or Port Forwarding cannot be used.
- A browser with Active-X, Java or JavaScript support is required on 32-bit OS's only, such as Windows XP & 2K

Agenda

1. SSL Introduction
2. AnyConnect VPN
3. Technical Benefits



Cisco AnyConnect VPN Client

- **Extends the in-office experience**

  LAN-like full-network access, supports latency sensitive apps like voice (via DTLS transport)

- **Access across platforms**

  Windows XP/Vista/7 (32/64-bit)

  Mac OS X 10.5/ 10.6 and 10.5,

  Linux: Red Hat 5 Desktop, Ubuntu 9.x

  Windows Mobile 5.0, 6.0 and 6.1 Pocket PC

- **Supported on ASA 8.0 and later**

- **Supported with Cisco IOS 12.4(15)T onwards**

  Initial installation requires admin rights; however, upgrading an existing install with a pushed package does not

Datagram TLS (DTLS)

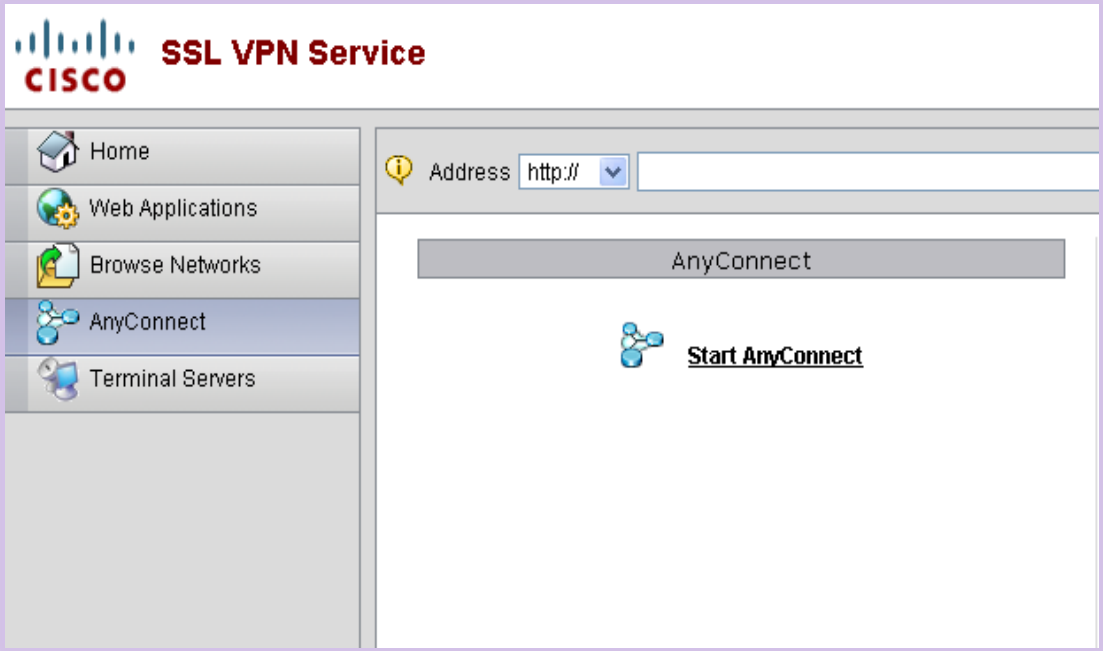
Why DTLS?

- **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

Cisco AnyConnect VPN Client
Deployment Models

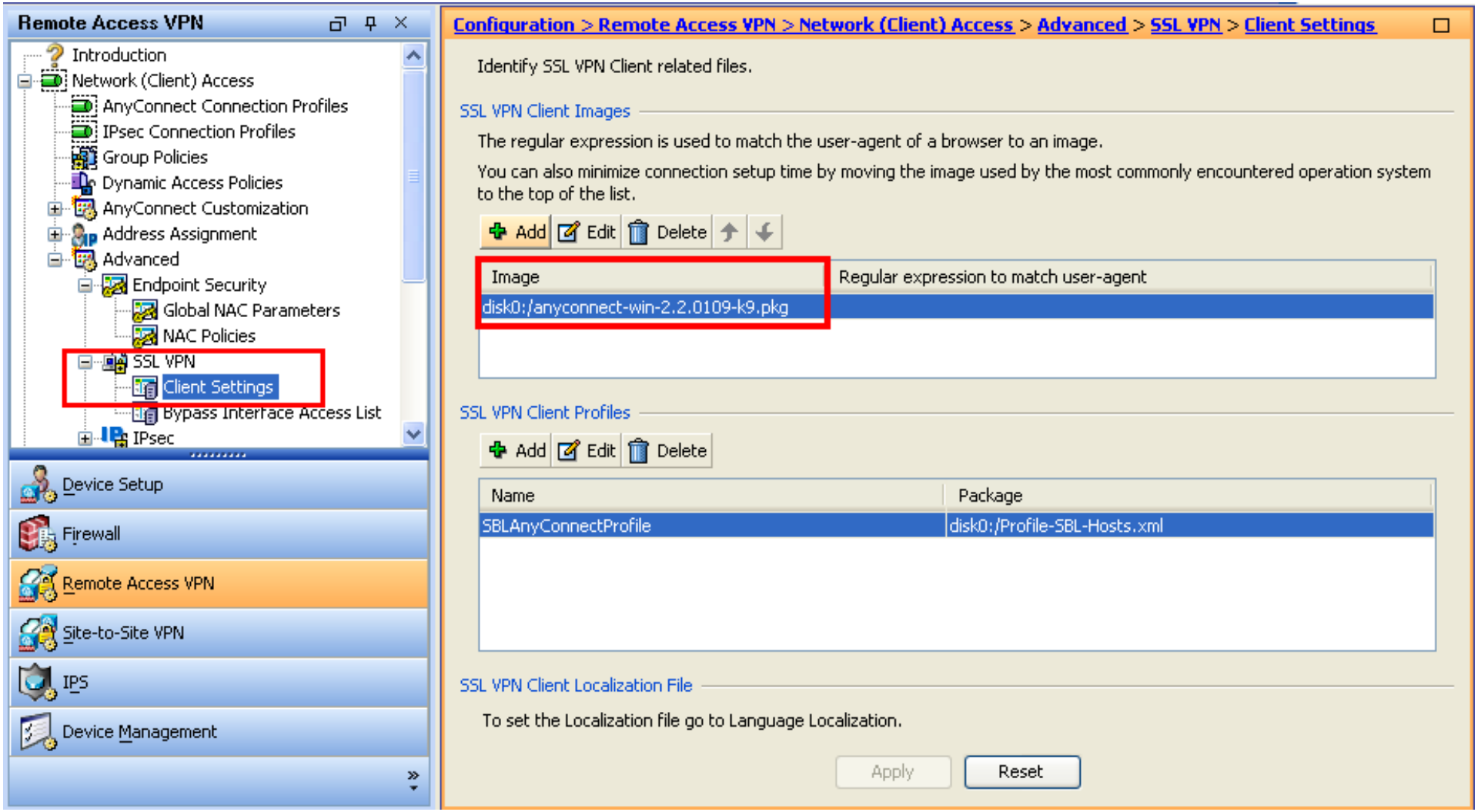
Methods of Deployment:

- Web-based initiation
- Standalone package



ASDM - AnyConnect Client Configuration

Load AnyConnect Client Images for each Supported OS



Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings

AnyConnect VPN Client Installation

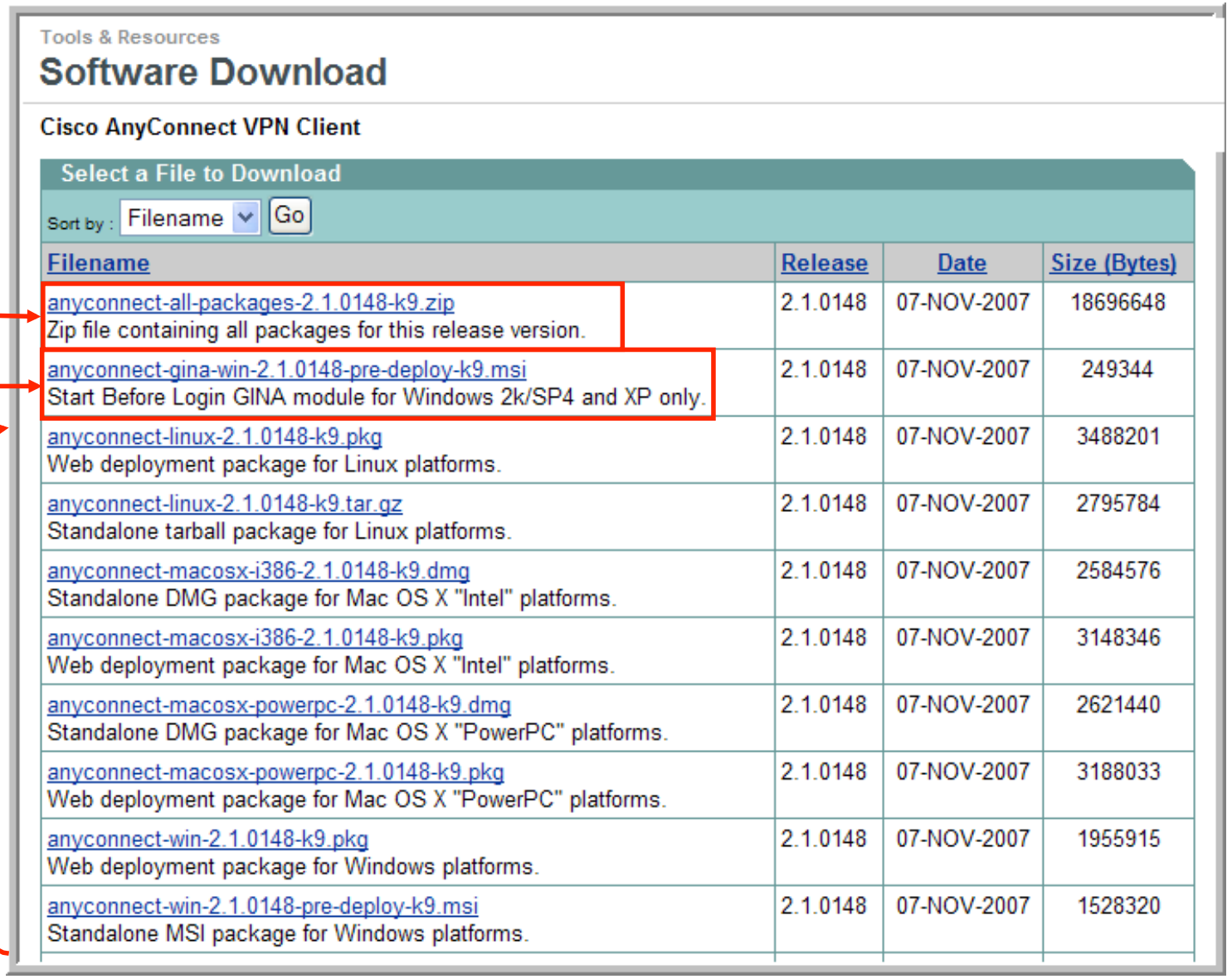
VPN Client Software on Software Center

Bundling of all Clients

SBL Login Module

Windows, Linux, MacOS clients:

- ***Web deployment packages*** are dynamically downloaded and installed from ASA
- ***Standalone packages*** support independent distribution



Tools & Resources

Software Download

Cisco AnyConnect VPN Client

Select a File to Download

Sort by : Filename Go

Filename	Release	Date	Size (Bytes)
anyconnect-all-packages-2.1.0148-k9.zip Zip file containing all packages for this release version.	2.1.0148	07-NOV-2007	18696648
anyconnect-gina-win-2.1.0148-pre-deploy-k9.msi Start Before Login GINA module for Windows 2k/SP4 and XP only.	2.1.0148	07-NOV-2007	249344
anyconnect-linux-2.1.0148-k9.pkg Web deployment package for Linux platforms.	2.1.0148	07-NOV-2007	3488201
anyconnect-linux-2.1.0148-k9.tar.gz Standalone tarball package for Linux platforms.	2.1.0148	07-NOV-2007	2795784
anyconnect-macosx-i386-2.1.0148-k9.dmg Standalone DMG package for Mac OS X "Intel" platforms.	2.1.0148	07-NOV-2007	2584576
anyconnect-macosx-i386-2.1.0148-k9.pkg Web deployment package for Mac OS X "Intel" platforms.	2.1.0148	07-NOV-2007	3148346
anyconnect-macosx-powerpc-2.1.0148-k9.dmg Standalone DMG package for Mac OS X "PowerPC" platforms.	2.1.0148	07-NOV-2007	2621440
anyconnect-macosx-powerpc-2.1.0148-k9.pkg Web deployment package for Mac OS X "PowerPC" platforms.	2.1.0148	07-NOV-2007	3188033
anyconnect-win-2.1.0148-k9.pkg Web deployment package for Windows platforms.	2.1.0148	07-NOV-2007	1955915
anyconnect-win-2.1.0148-pre-deploy-k9.msi Standalone MSI package for Windows platforms.	2.1.0148	07-NOV-2007	1528320

AnyConnect VPN Client Installation

Multiple deployment methods

- Example of client without ActiveX or any supported Java version.
- Client can be *automatically uninstalled* after user log-off or remain installed
- User can click on the link to manually launch installation of .exe file.

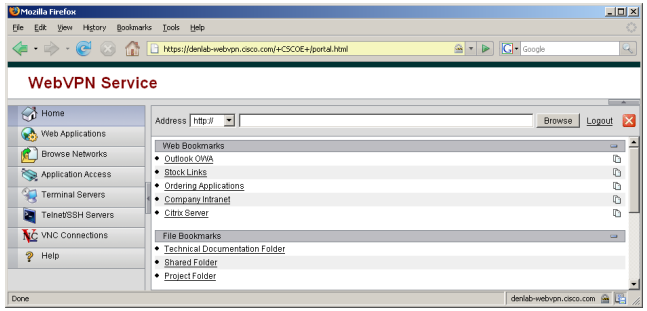
Cisco Remote Access VPN Clients

Comparison Between Full Tunnel Client Options

	Cisco VPN Client	Cisco AnyConnect VPN Client	Cisco SSL VPN Client
Approximate size	10 MB	1-3 MB	400KB
Initial install	distribute	auto download distribute	auto download distribute
Admin rights required	yes	Initial installation only (MSI available – Windows)	Initial installation only (Stub installer available)
Protocol	IPsec	DTLS, TLS (HTTPS) - Auto	TLS (HTTPS)
OS Support	multiple*	multiple**	2000/XP
Head End	ASA/PIX/3K/IOS	ASA/IOS	ASA/3K/IOS

Firewall Traversal

SSL VPN

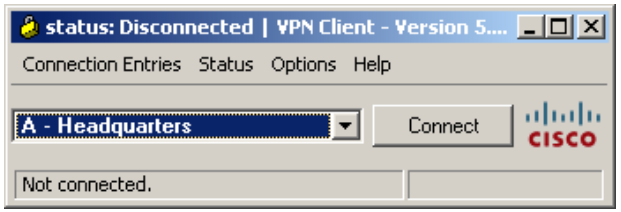


- HTTPS—TCP/443
- DTLS—UDP/443

  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



- Standard IPsec

  ESP (Protocol 50)

  IKE (UDP 500)
- Standard NAT/PAT Traversal

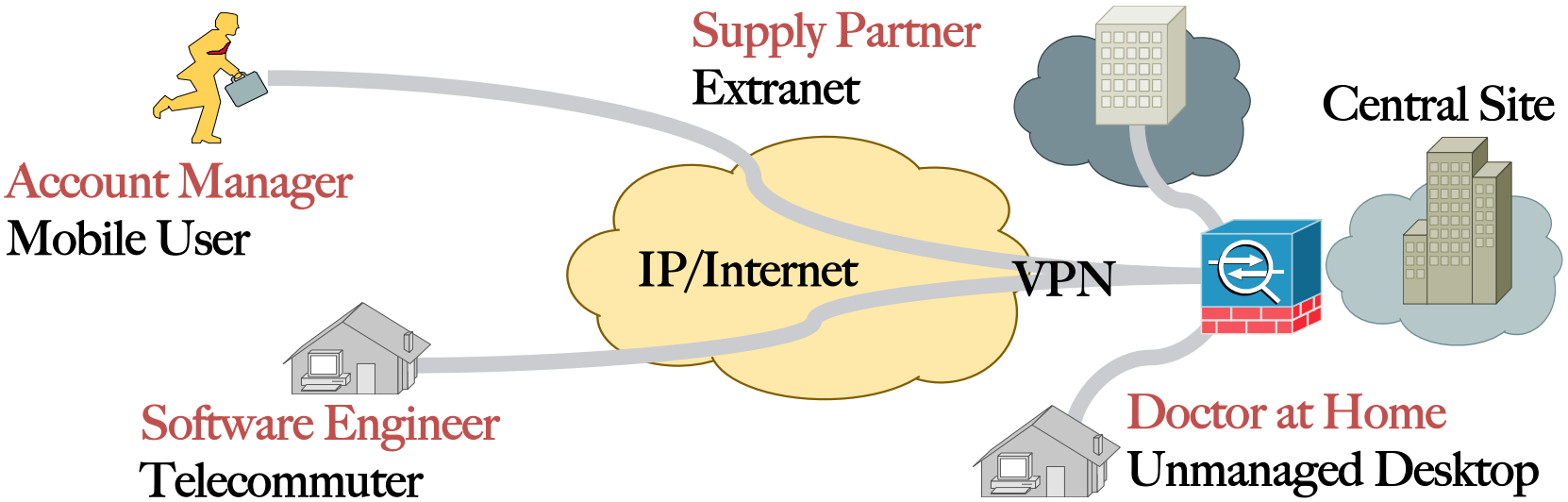
  IKE (UDP 500/UDP 4500)

  ESP over UDP (UDP 4500)
- Proprietary TCP Encapsulation

  Administrator defined TCP port(s)

Generic Deployment Example

IPsec and SSL VPN Support Diverse User Populations

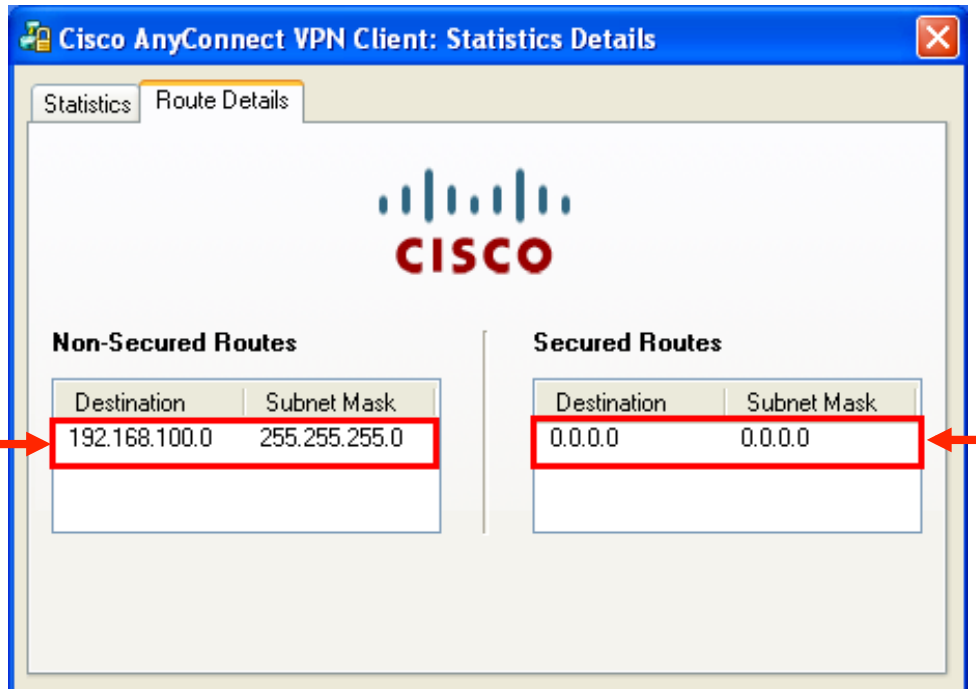


Clientless (L7) Clientless/AnyConnect VPN Client	Full Network Access (L3) Cisco VPN Client
▪ Partner—Few apps/servers, tight access control, no control over desktop software environment, firewall traversal ▪ Doctor—Occasional access, few apps, no desktop software control	▪ Engineer—Many servers/apps,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

AnyConnect VPN Client
Local LAN Access (Split Tunnel Variant)

To verify split tunnel configuration from remote PC, open AnyConnect VPN icon in task tray, then select: **Statistics > Details > Route Details**

In this example, only traffic to the Local PC LAN (192.168.100.0/24) is sent in clear (no VPN).

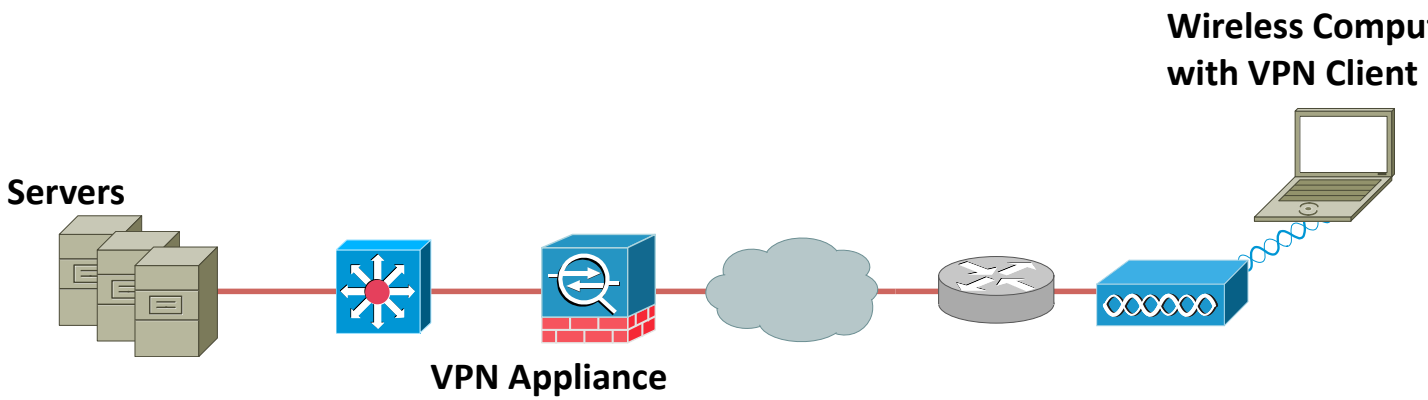


All other traffic is sent encrypted over VPN to ASA.

AnyConnect VPN Client

Auto-Reconnect feature

- Attempt to reestablish the VPN connection after loss of physical connectivity
- Requires ASA to have a still valid VPN session
- Agnostic to psychical NIC of end user's computer– AnyConnect Virtual Adapter
- System suspend situation – hibernation/sleep mode – system resume supported, but disabled by default (explicit configuration required)



AnyConnect VPN Client

Trusted Network Detection (v2.4)

- **Automatic managing of VPN connections without user intervention**
- Ability to tear down a VPN connection when the user is inside the corporate network (the *trusted* network) and start the connection when the user is outside the corporate network (the *untrusted* network)
- *First Phase* - based on DNSsuffix and DNServer of active physical interface(s)
- *Later Phases* – based on further criteria, e.g. of *ipconfig /all*
- Supported on Windows XP and later (not including Windows Mobile) and all Mac OSes supported by AnyConnect 2.4

Interface configuration:

DNS suffix: cisco.com, DNS servers: 161.44.124.122, 64.102.6.247, 171.68.226.120 → User in Untrusted Network

DNS suffix: cisco.com, DNS servers: 161.44.124.122 → User in Trusted Network

AnyConnect VPN Client
Start Before Logon

- User forced to connect to corporate network before logging on to the computer
- Administrator control over use of login scripts, passwords caching, drives mapping
- *Requires additional modules – VPNgina/PLAP*
- Supported on Windows XP, Vista and Windows 7

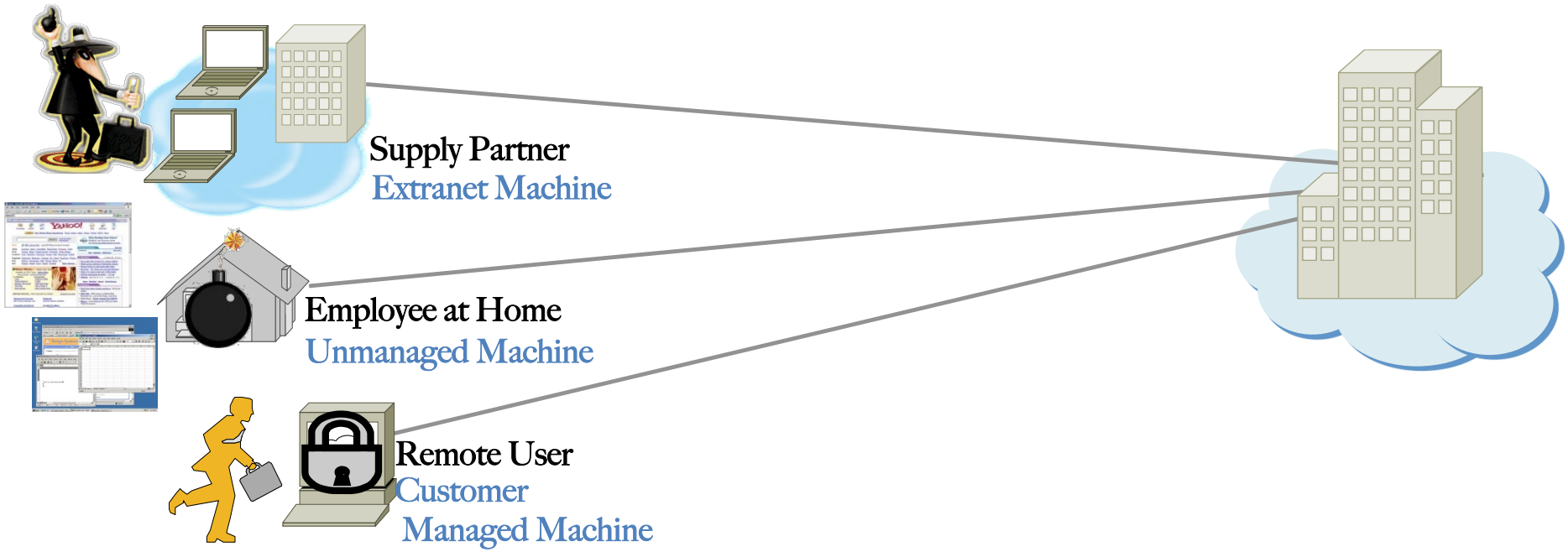
```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://
    www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://
    schemas.xmlsoap.org/encoding/
   AnyConnectProfile.xsd">

<ClientInitialization>
    <UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>
```

UserControllable option with AnyConnect v2.3

Unique Security Challenges on the Endpoint

SSL VPN Brings New Points of Attack



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?

Post SSL VPN Session

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

ASA 5500 Series – Threat-Protected VPN

Cisco Secure Desktop: Comprehensive Endpoint Security for SSL VPN

Complete Pre-Connect Assessment:

- Location assessment – managed or unmanaged desktop?
- Security posture assessment – AV operational/ up-to-date, personal firewall operational, malware present?

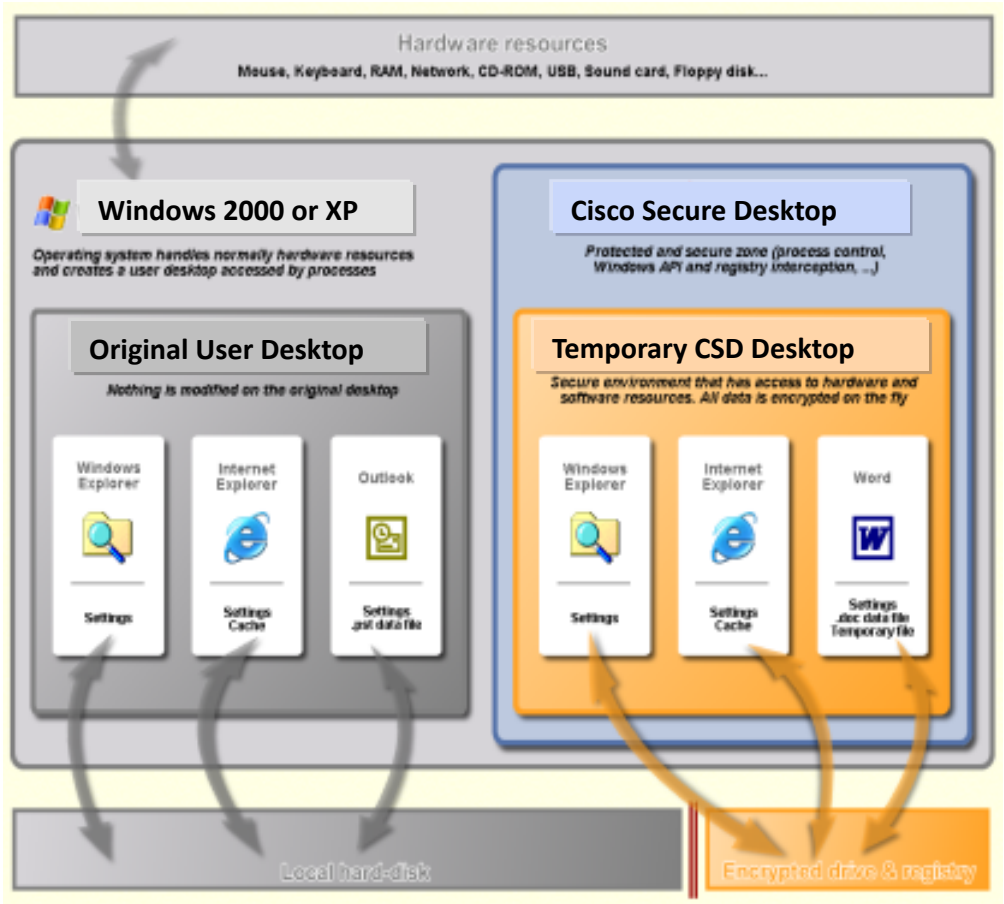
Comprehensive Session Protection:

- Data sandbox and encryption helps protect the session
- Malware detection with hooks to Microsoft free anti-spyware software

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

Works with Desktop Guest Permissions
No Admin Privileges Required



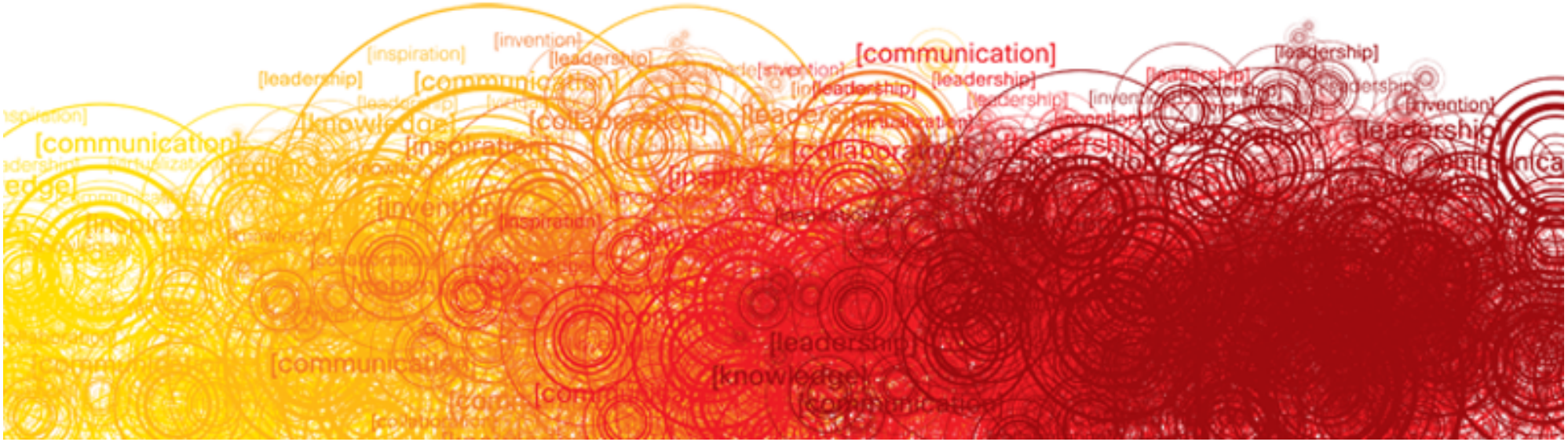
ASA 5500 Series

VPN Licensing Overview

AnyConnect Premium SSL VPN Edition (single device) 	SSL VPN, Clientless SSL VPN, Cisco Secure Desktop (Host scan & Vault) - simultaneous users – 10 -> 10k
FLEX Licenses (single device) 	60-day temporary license for emergency scenarios -Additional users – 250 -> 10k
AnyConnect Premium SSL VPN Edition Shared License (main device and participant device) 	Same capabilities as single-device license, but SSL user count may be shared among any number of internally connected devices that have an installed participant license.
AnyConnect Essentials 	AnyConnect tunneling without clientless SSL VPN and Cisco Secure Desktop capabilities.
AnyConnect Mobile 	Required per-device in addition to Essentials or Premium licenses

Agenda

1. SSL Introduction
2. AnyConnect VPN
3. Technical Benefits



Market Evolution…

Today

IPSec?

SSL?

Mobile Security?

Client?

Clientless?

Fixed Platforms?

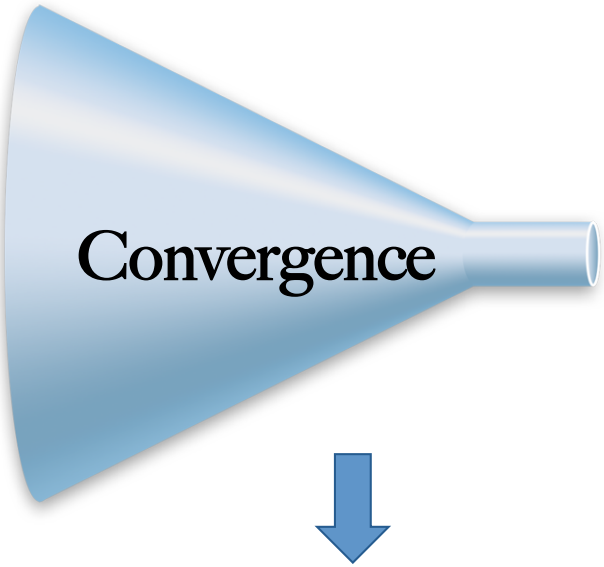
Mobile Platforms?

Voice Apps?

Video Apps?

Data Apps?

Tomorrow



Cisco Secure Remote Access