



## Touch Cisco

Remote Access wird zum  
Kinderspiel - mit SSL-VPN  
von Cisco



Sascha Ulfig  
Michael Goetze

# Webinar Zielsetzung: “Thema Security”

Remote Access wird zum Kinderspiel - mit SSL-VPN von Cisco

Nach dem Webinar sollte der Zuhörer in der Lage sein:

- Die Architektur und Vorteile von SSL-VPN zu kennen
- Die verfügbaren Techniken einer Cisco SSL-VPN-Lösung einzusetzen
- Die Vorteile und die Auswahl der Cisco Produktfamilie ASA 5500 für den Einsatz einer SSL-Lösung zu kennen

# AGENDA

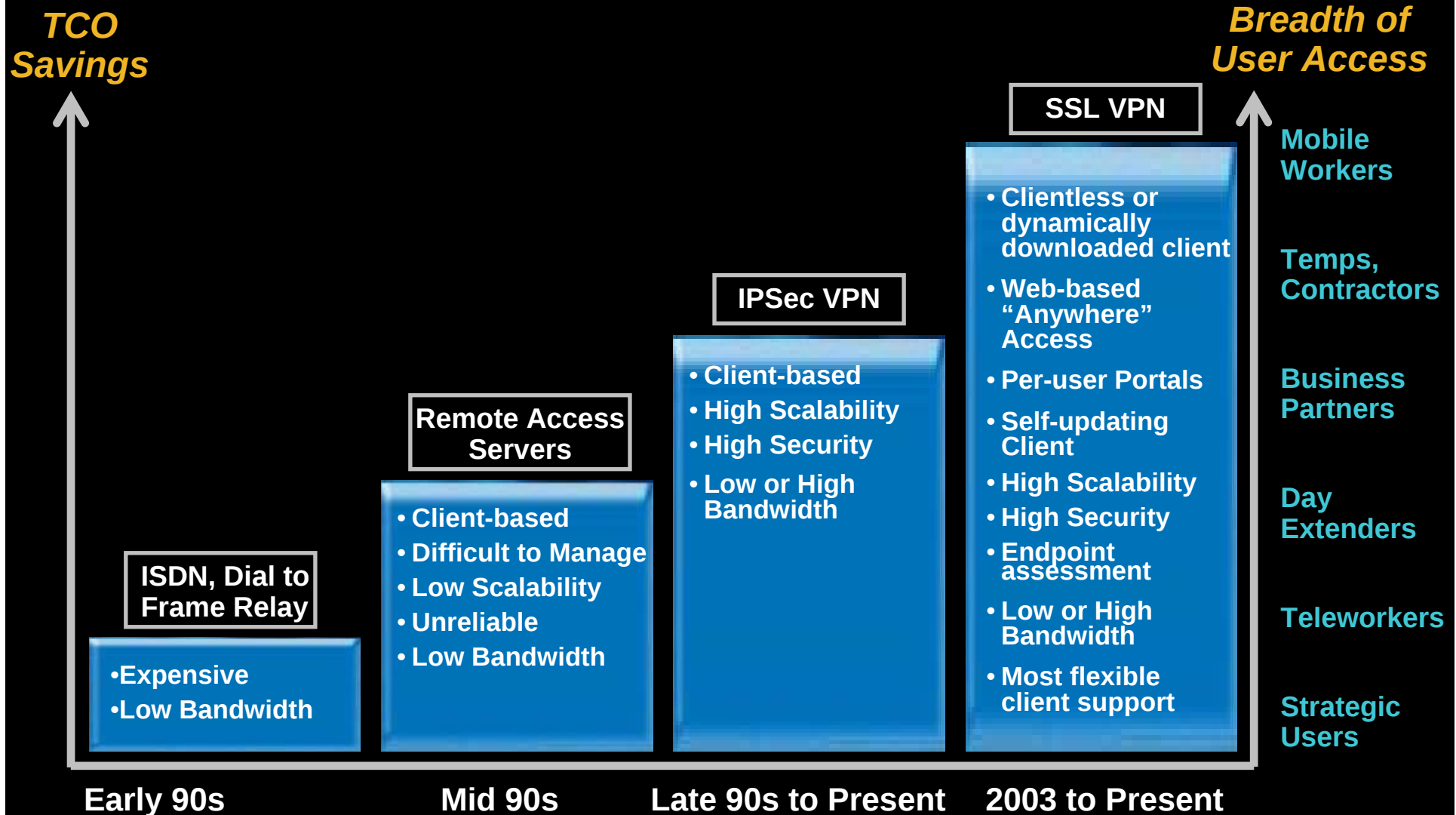
- Remote Access Lösungsansätze
- Client basiertes SSL VPN
- Clientless SSL VPN
- Schutz vor unsicheren Endsystemen mit “Cisco Secure Desktop”
- SSL VPN Konfiguration
- ASA 5500 Produktübersicht
- Zusammenfassung



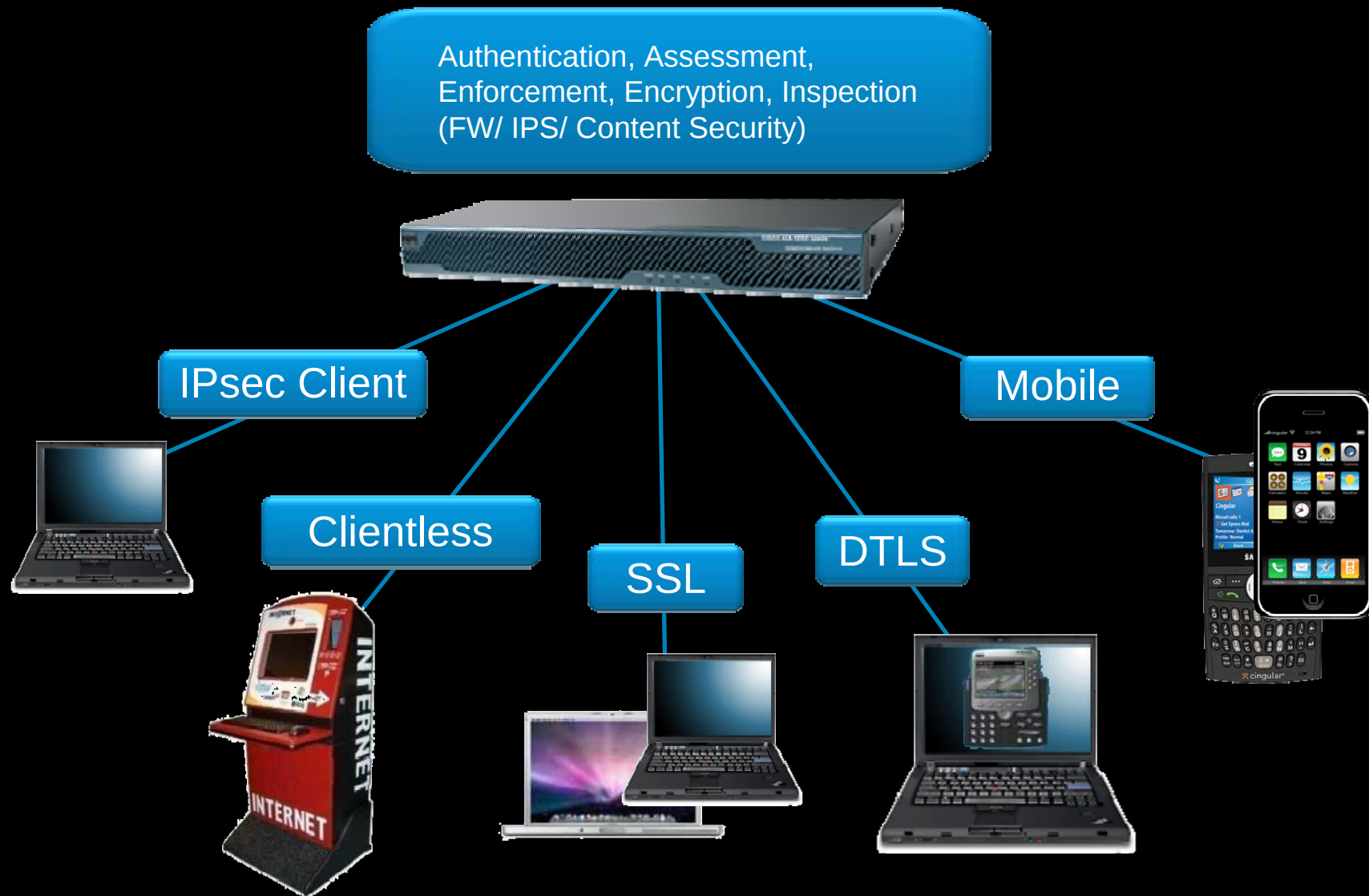
# Remote Access Lösungsansätze



# Evolution of Remote Access Technologies



# Cisco VPN – Unified Secure Access

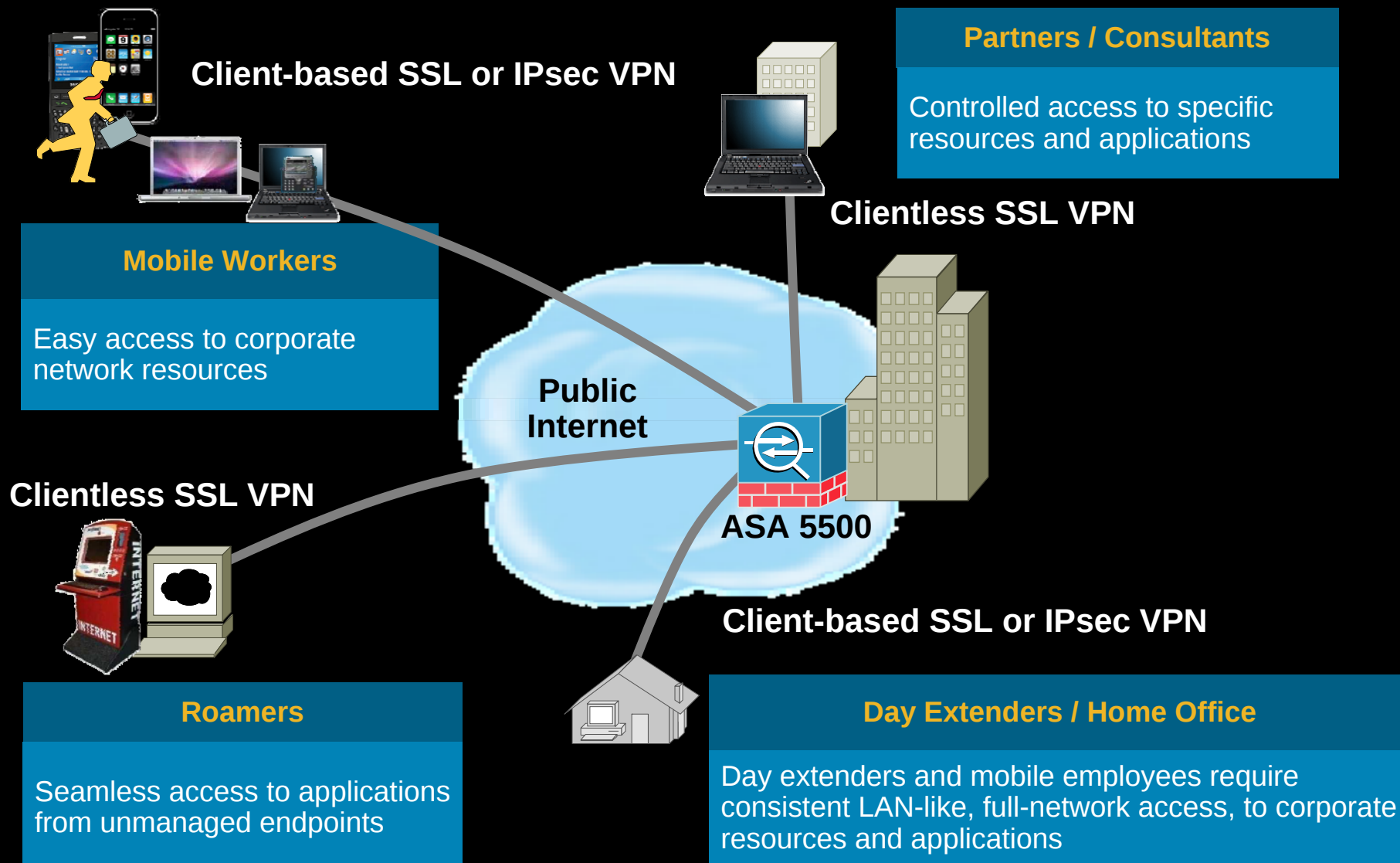


# Understanding Your Remote Users

- 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
  - SmartPhones
- How long will users stay connected?
  - 24x7 or entire business day
  - Limited period of time

# Secure Connectivity Everywhere

Extending the Self-Defending Network



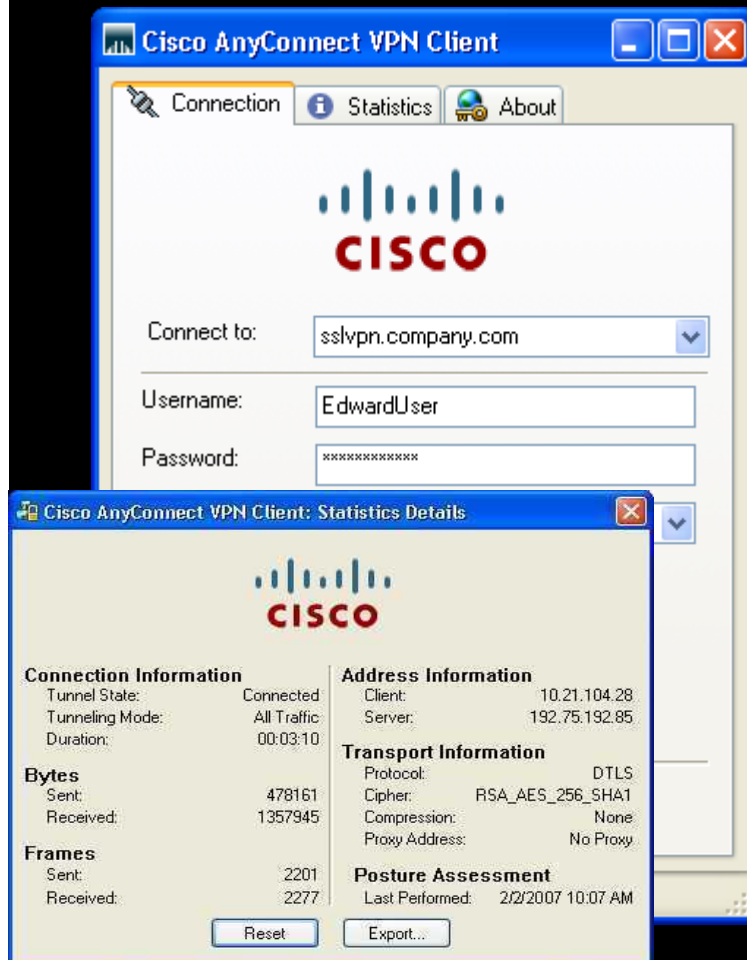


# Client-basierter SSL VPN



# SSL VPN Tunneling: AnyConnect Client

## Functionality



- **Extends the in-office experience**  
LAN-like full-network access, supports latency sensitive apps like voice (via DTLS transport)
- **Access across platforms**  
Windows 2K / XP (x86/x64) / Vista (x86/x64)  
Mac OS X 10.4 & 10.5, Linux Intel  
Windows Mobile 5 + 6 (March 09)
- **Always up to date**  
Remotely installable and configurable to minimize user demands
- **Simplified Connections**  
No reboots required  
MSI – Windows Pre-installation package  
Stays connected on IP address change

# SSL VPN: AnyConnect Client

## Installation Options

- WebLaunch

  - Initiate via web browser

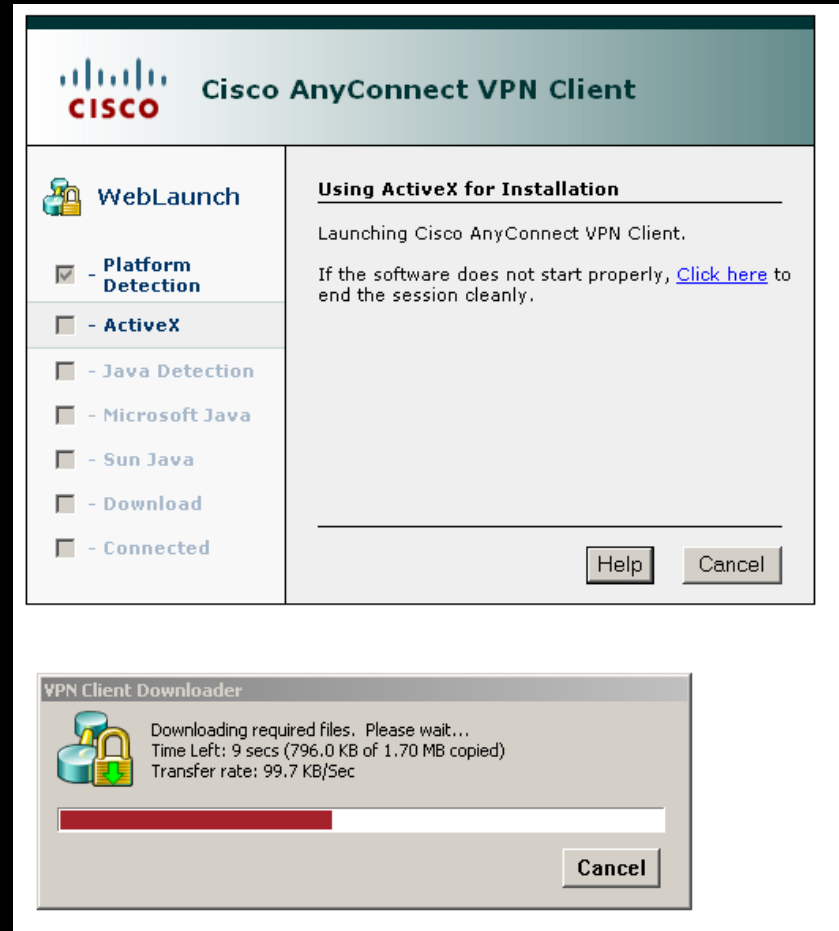
  - Login via portal

  - 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
  - Start Before Login

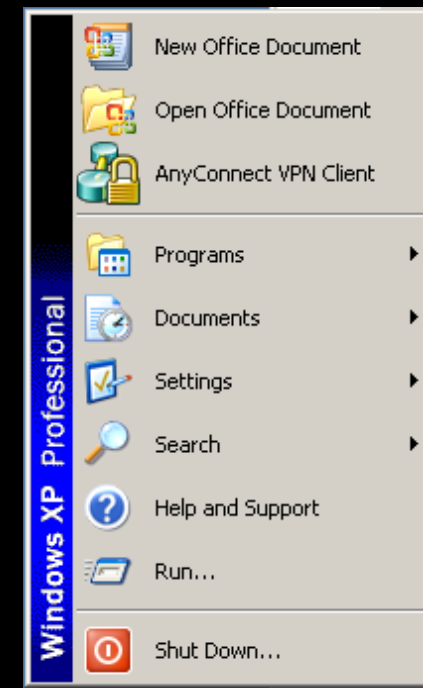


```

C:\Program Files\Cisco\Cisco AnyConnect VPN Client>vpnccli 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>

```



# AnyConnect: 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

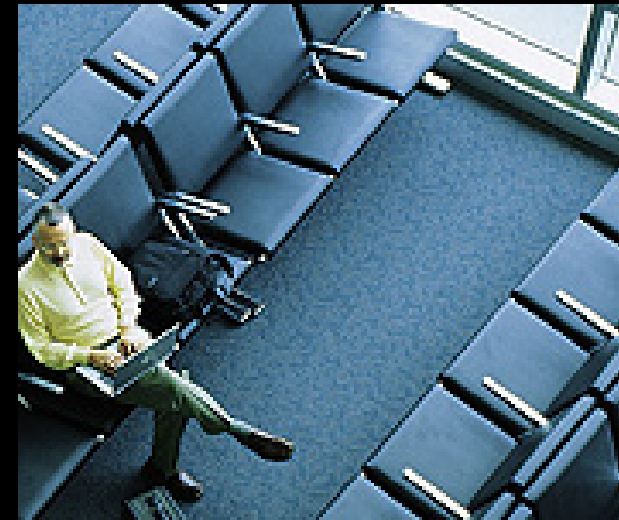


## Clientless SSL VPN



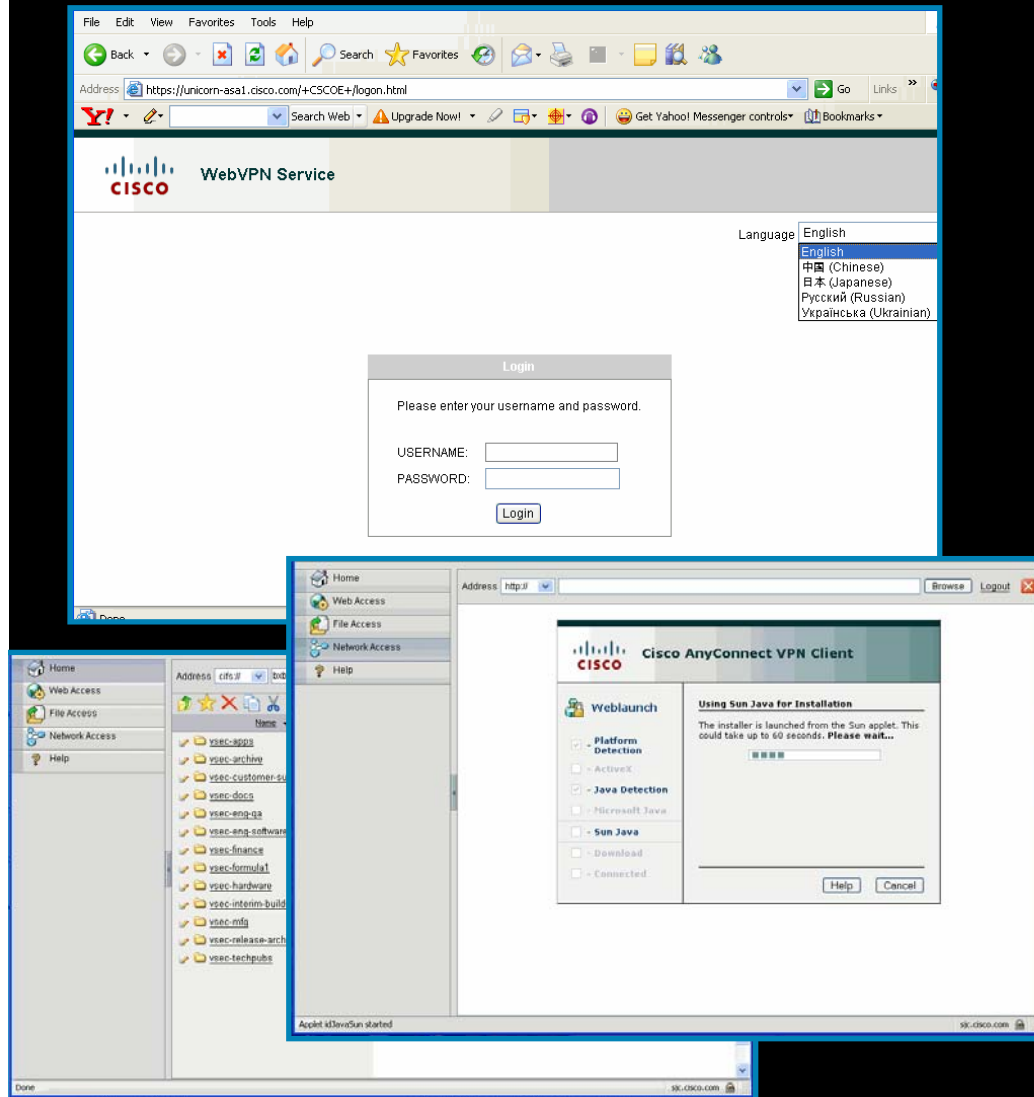
# Clientless access for mobile workers, partners and contractors

- No administrator rights required
- Critical apps and data
- Web and non-Web content
- Multi-factor authentication
- Granular access control
- User, group, device posture



# SSL VPN: Clientless Access

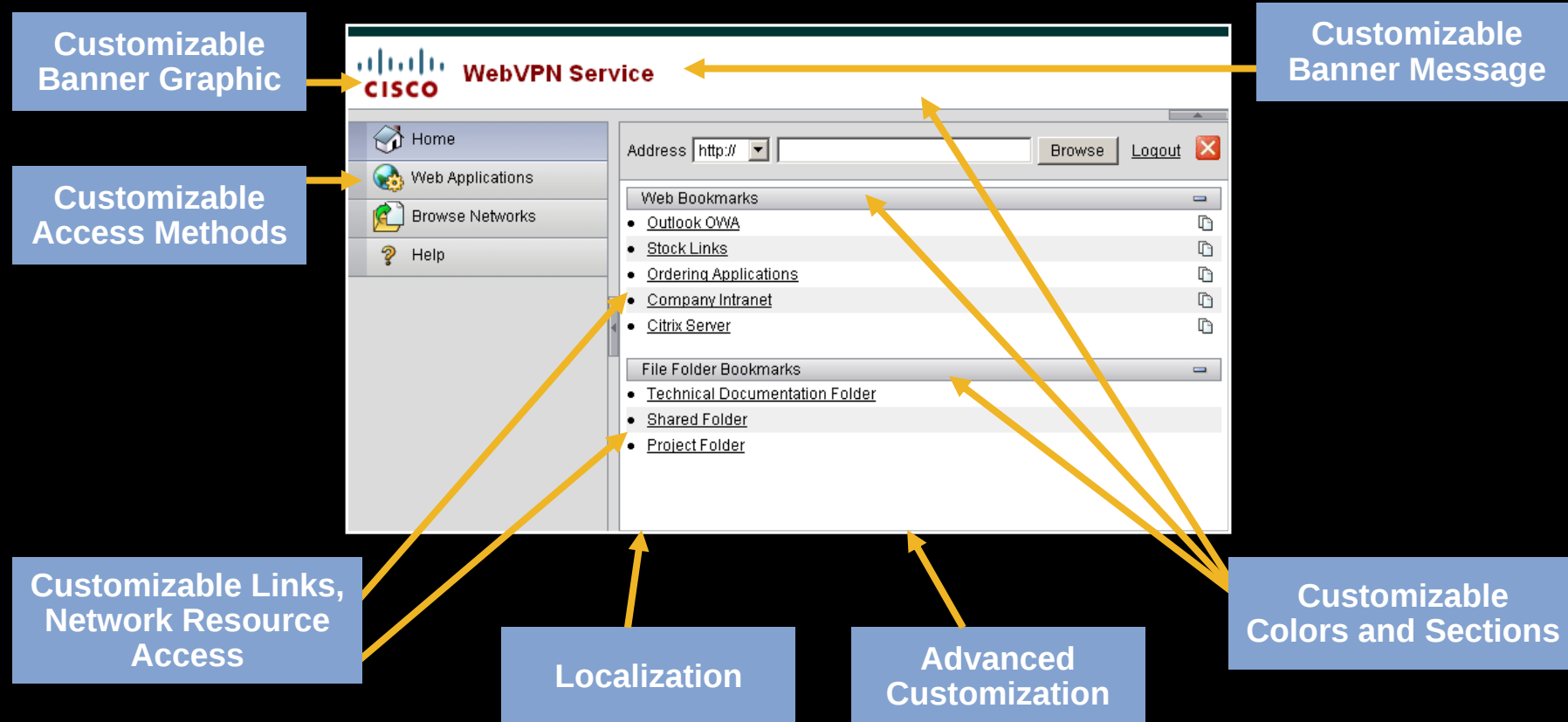
## ASA 5500 series



- Precise, granular access control to specific resources
- Flexible Portal Design
  - Localizable
  - RSS feeds
  - Personal bookmarks
  - AnyConnect Client access
- Drag and Drop file access and webified file transport
- Head-end deployed applets for Citrix, Telnet, SSH, RDP, VNC, TN5250, TN3270 and Sametime, framework supports add'l plug-ins
- Advanced port-forwarder for Windows (Smart Tunnel) accesses TCP applications without admin privileges on Client PC

# SSL VPN Clientless Customization

## Customizable per user group



# Complex Content Handling

- Port Forwarding

  - Local “thin” client acts as proxy

  - Tunnels and forwards application traffic

- Smart Tunnels

  - Allows Windows TCP applications to use the VPN security appliance as a proxy gateway to the private side of a network.

- Plug-ins

  - Citrix ICA, RDP, SSH/TELNET, VNC, TN3270, TN5250, HTTP Post, Sametime provided by Cisco

  - Extensible framework for other popular protocols

# Smart Tunnels

## Applications use VPN Appliance as Proxy Gateway

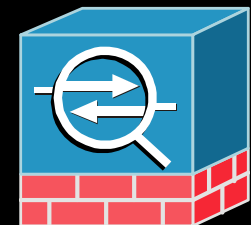
- Administrator creates list of “authorized” processes (e.g. Sametime etc.)
- Smart Tunnels loads a stub into each authorized process and redirects them through the SSL VPN tunnel

## Benefits

- Enables use of „non-webified“ applications
- Administrator decides which applications are allowed
- Does not require full SSL VPN client
- No administrative privileges required on client system

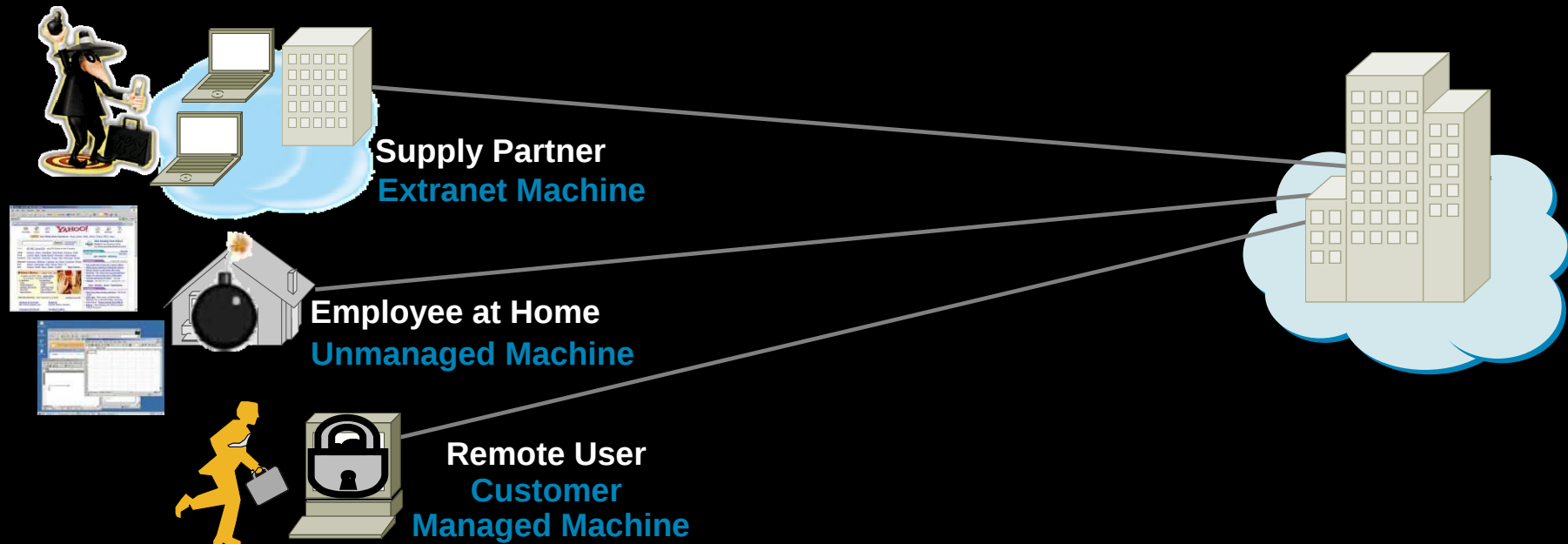


## Schutz vor unsicheren Endsystemen mit "Cisco Secure Desktop"



# 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?

# Cisco Secure Desktop (Secure Vault)

## *How it Works*

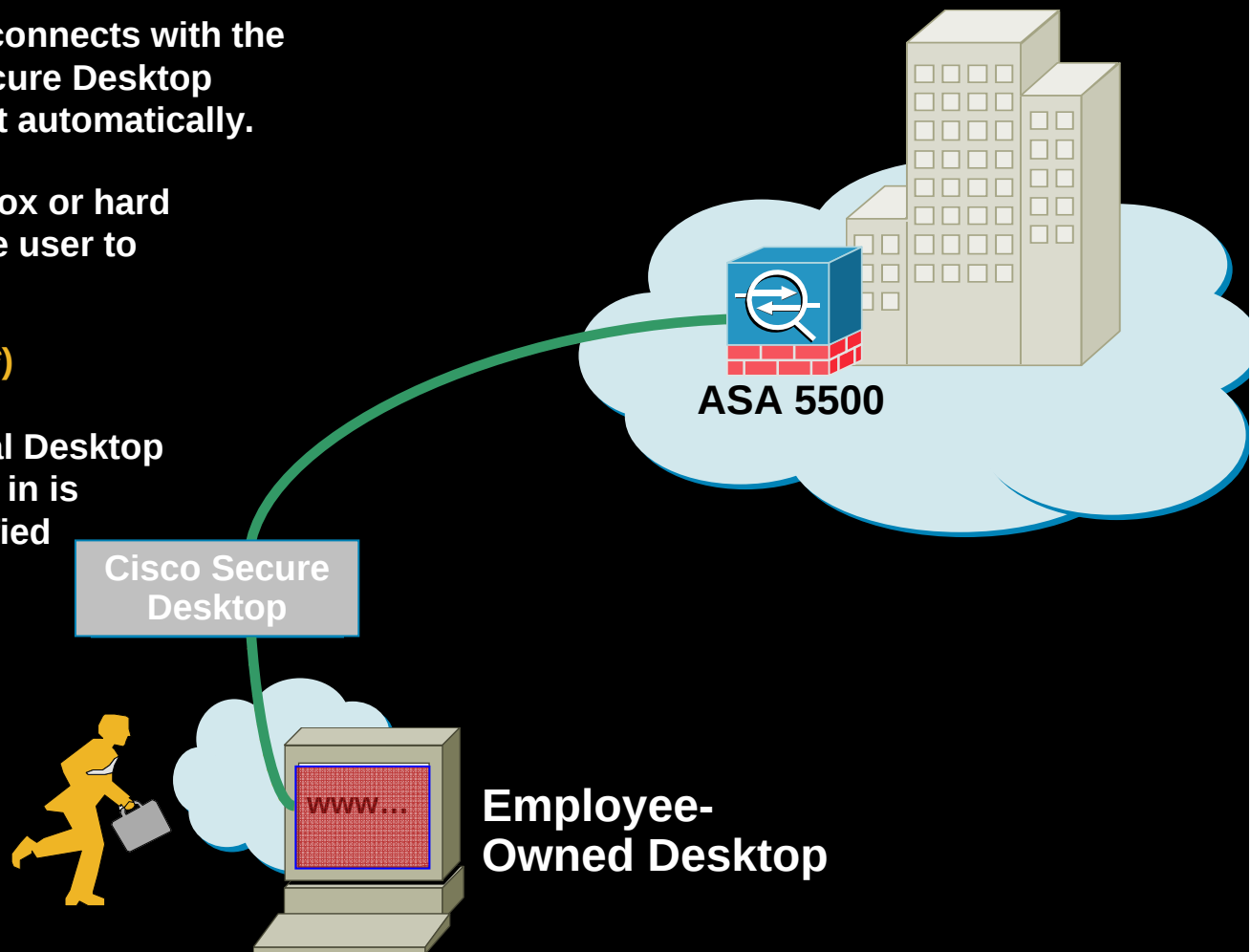
**Step One:** A user on the road connects with the concentrator and the Cisco Secure Desktop is pushed down to the endpoint automatically.

**Step Two:** An encrypted sandbox or hard drive partition is created for the user to work in (\*)

**Step Three:** The user logs in (\*\*)

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

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



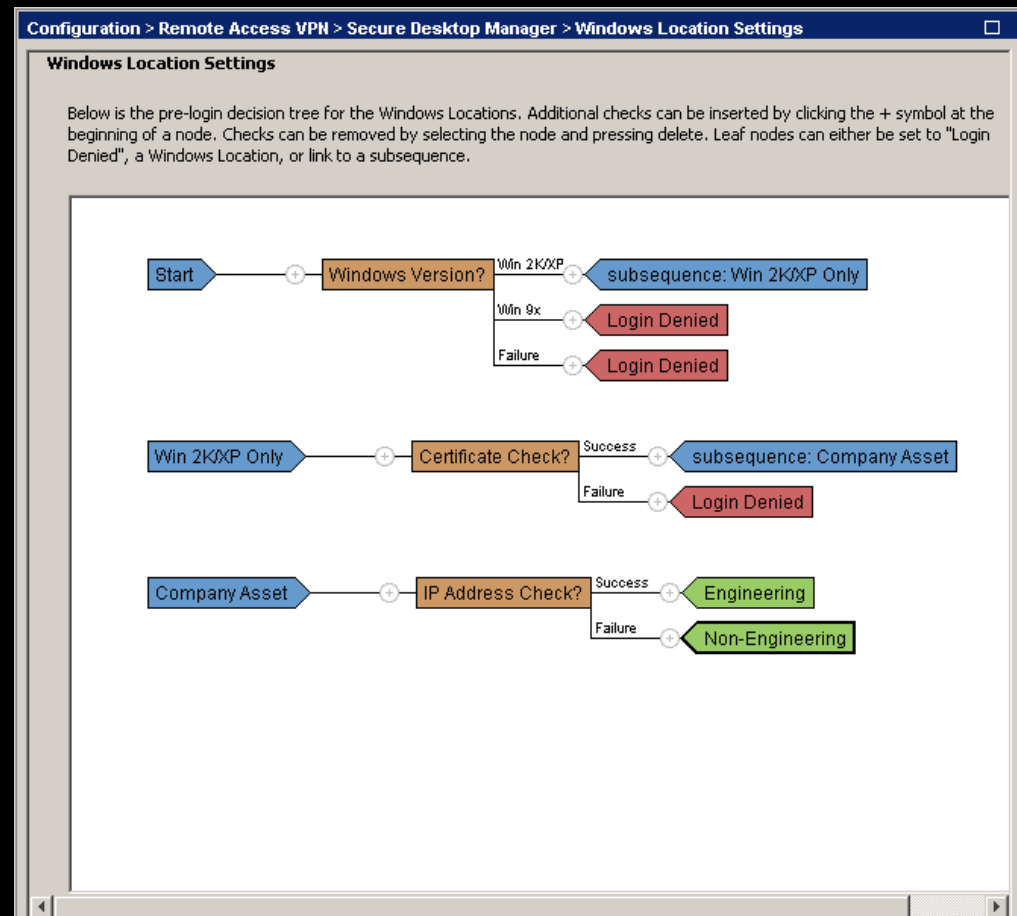
(\*) Pre-Login policy decides which Secure Desktop Features should be used

(\*\*) Dynamic Access Policy can be applied at this step

# 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
- Visual policy simplifies administrative configuration



# Comprehensive Security Assessment

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

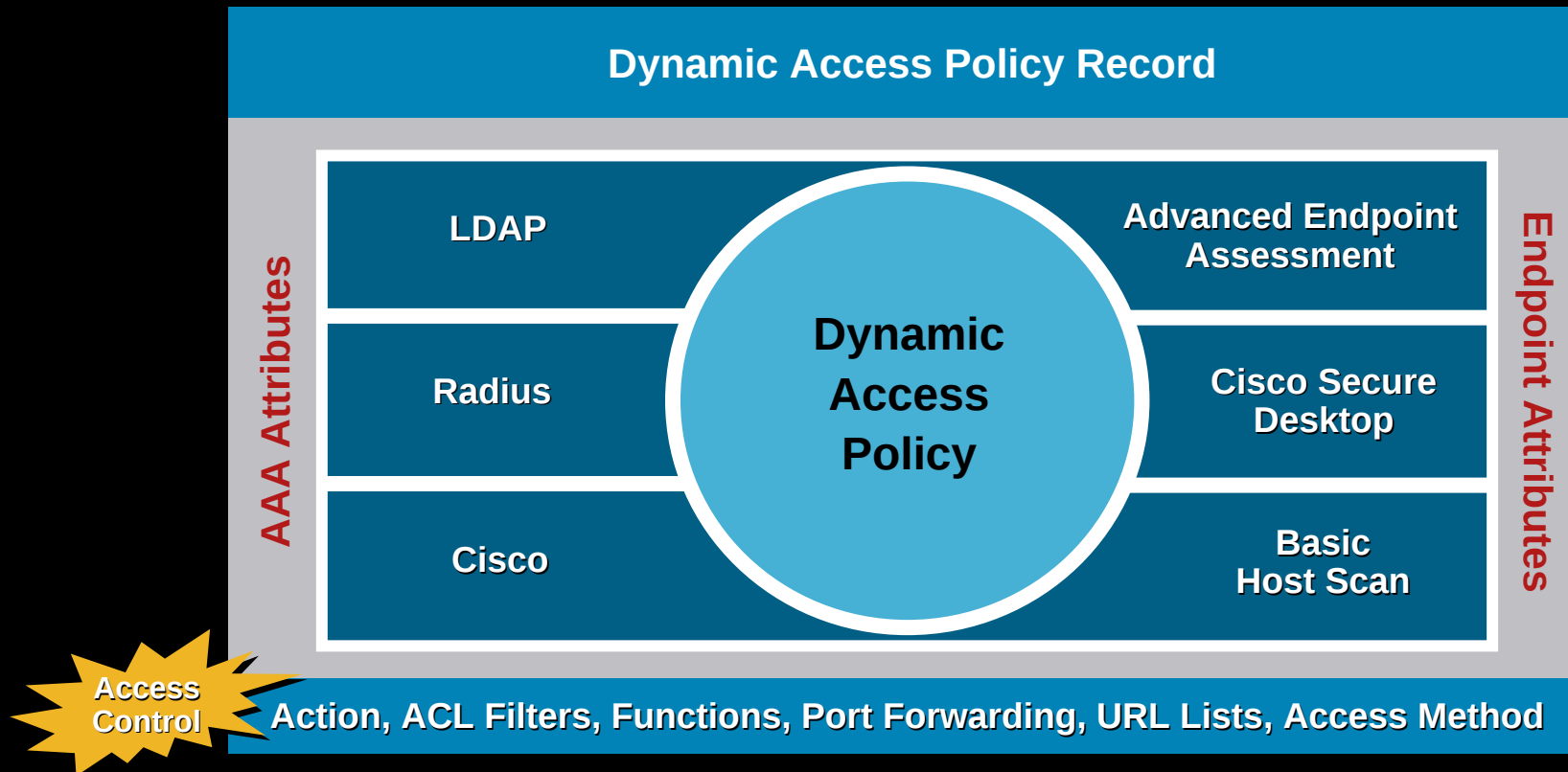
Anti-virus, anti-spyware, personal firewall, and more

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



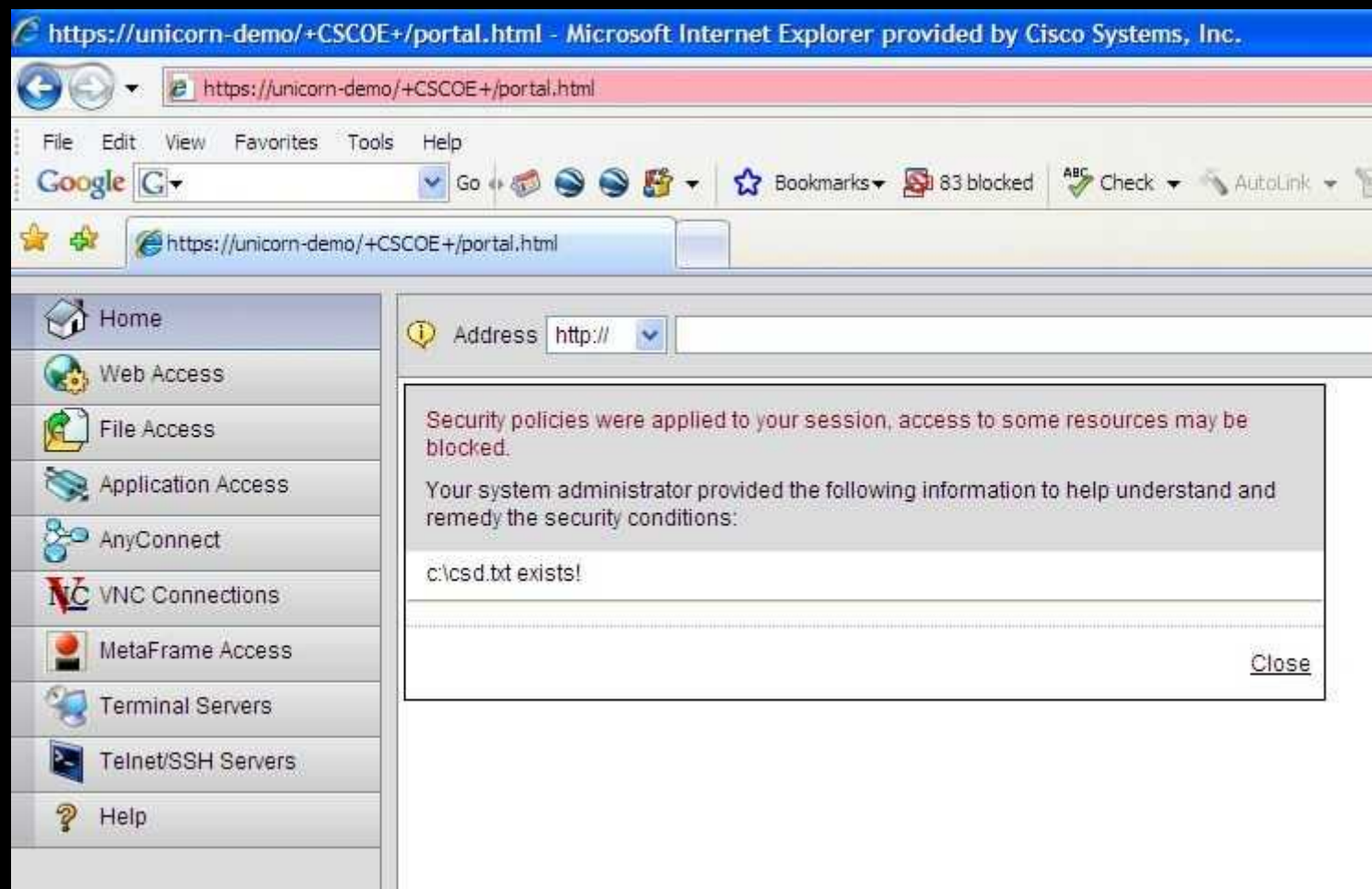
# Dynamic Access Policy (DAP)

## Extensible Design Enables Flexible, Policy-Based VPN Access

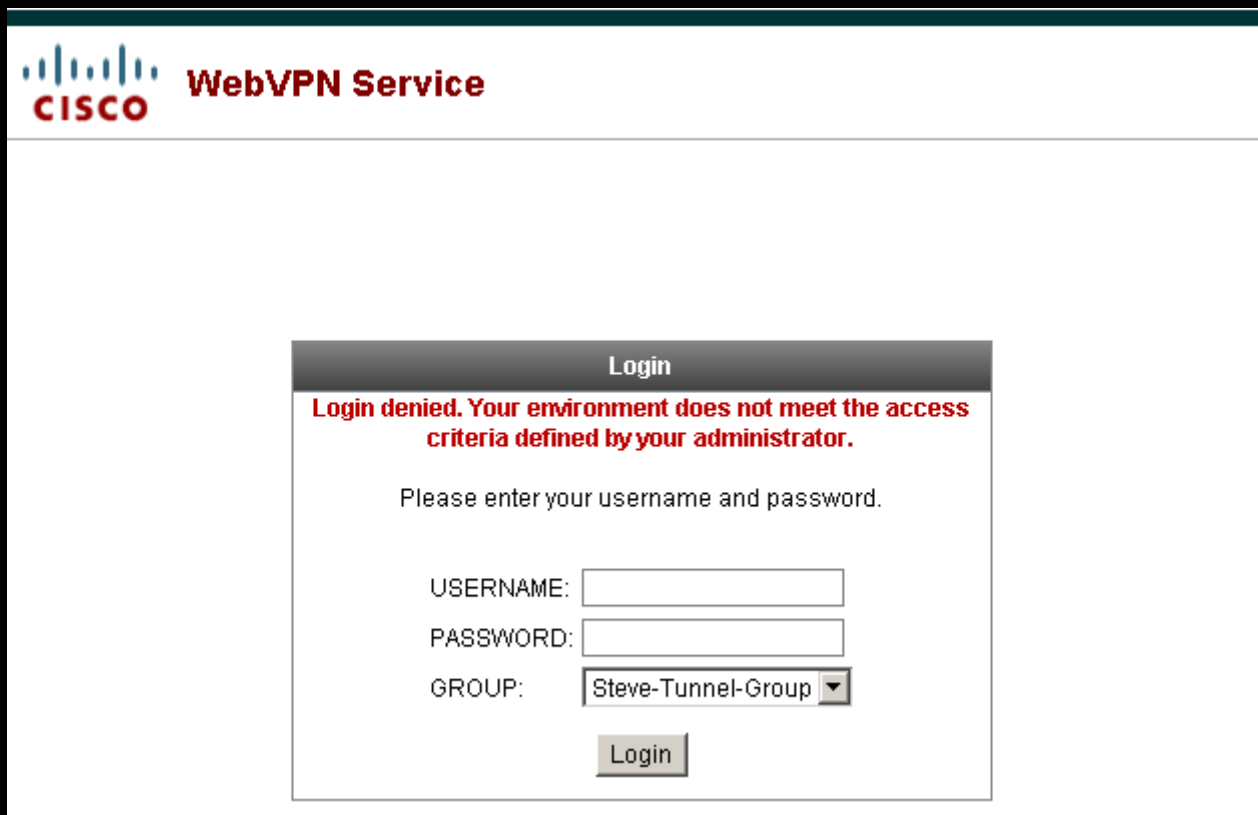


**DAP enables you to configure authorization that addresses the dynamics of VPN environments.**

# Example: Cisco Secure Desktop Access Restricted



# Example: Cisco Secure Desktop Access Denied



The screenshot shows the Cisco WebVPN Service login interface. At the top left is the Cisco logo and the text "WebVPN Service". In the center, there is a "Login" box. Inside this box, a red error message states: "Login denied. Your environment does not meet the access criteria defined by your administrator." Below this message, it says "Please enter your username and password." There are three input fields: "USERNAME:" with a text box, "PASSWORD:" with a text box, and "GROUP:" with a dropdown menu currently showing "Steve-Tunnel-Group". A "Login" button is located at the bottom of the input fields.

**CISCO WebVPN Service**

**Login**

**Login denied. Your environment does not meet the access criteria defined by your administrator.**

Please enter your username and password.

USERNAME:

PASSWORD:

GROUP:

Login



# SSL VPN Konfiguration



# Wide Range of Management Solutions

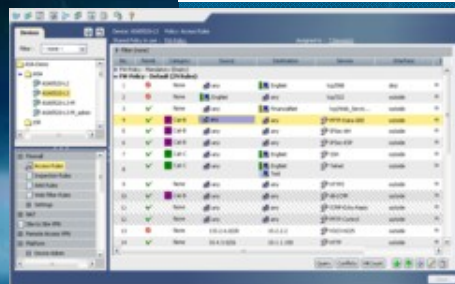
## Provide Scalable, Cost Optimized Options for Businesses

### Integrated Remote Management within ASA



- Configuration: Auto Update, SSH, Telnet, XML/HTTPS, and ASDM
- Real-time monitoring: Syslog, SNMP, HTTPS, and ASDM
- Software updates: Auto Update, SCP, HTTP, HTTPS, and TFTP

### Cisco Security Manager (CS-Manager)



- Scalable management solution for wide range of Cisco security solutions including routers, switches, blades, and appliances
- Delivers centralized management of firewall, VPN, IPS/IDS, networking, and other services via flexible user interface
- Provides role-based admin access and workflow capabilities

### Cisco Monitoring and Response Solution (CS-MARS)



- Family of high performance appliances designed to provide automated analysis of security event information to help identify, manage, and counter attacks
- Offers event correlation, visualization, rules engine, and reporting

# For Administrators, Visual Management

## ASDM – SSL & IPsec Wizards

Separate  
wizards for SSL  
and IPsec VPN  
configuration

The screenshot displays the Cisco ASDM 6.0 for ASA (Beta Release) interface. The title bar indicates the connection to 10.94.146.183. The menu bar includes File, View, Tools, Wizards, Window, and Help. The Wizards menu is open, showing options: Startup Wizard..., IPsec VPN Wizard..., SSL VPN Wizard..., High Availability and Scalability Wizard..., and Packet Capture Wizard....

The main content area is divided into several sections:

- Device Information:**
  - General: Host Name: pod5-asa.cisco.com, ASA Version: 8.0(0)205, ASDM Version: 6.0(0)107, Firewall Mode: Routed.
  - License: Device Uptime: 1d 3h 10m 50s, Device Type: ASA 5520, Context Mode: Single, Total Memory: 512 MB.
- VPN Tunnels:** IKE: 0, IPsec: 0, Clientless SSL VPN: 0, SSL VPN Client: 0.
- System Resources Status:**
  - CPU: CPU Usage (percent) graph showing 0% usage.
  - Memory: Memory Usage (MB) graph showing 256 MB usage.
- Interface Status:**

| Interface | IP Address/Mask  | Line | Link | Kbps |
|-----------|------------------|------|------|------|
| inside    | 172.16.10.1/24   | up   | up   | 0    |
| mgmt      | 172.16.254.10/24 | up   | up   | 3    |
| outside   | 172.16.50.10/24  | up   | up   | 0    |

inside Input Kbps: 0 Output Kbps: 0
- Traffic Status:**
  - Connections Per Second Usage graph showing 0 connections.
  - 'outside' Interface Traffic Usage (Kbps) graph showing 0 input and output Kbps.
- Latest ASDM Syslog Messages:**

| Severity | Date        | Time     | Syslog ID | Source IP      | Destination IP | Description                                                                  |
|----------|-------------|----------|-----------|----------------|----------------|------------------------------------------------------------------------------|
| 6        | Feb 11 2007 | 16:23:42 | 302016    | 172.16.254.50  | 172.16.254.10  | Teardown UDP connection 23092416 for mgmt:172.16.254.50/514 to NP Identity   |
| 6        | Feb 11 2007 | 16:22:04 | 106015    | 172.16.254.254 | 172.16.254.10  | Deny TCP (no connection) from 172.16.254.254/1024 to 172.16.254.10/443 flags |
| 6        | Feb 11 2007 | 16:21:45 | 725007    |                |                | SSL session with client mgmt:172.16.254.254/1043 terminated.                 |

Device configuration loaded successfully. Status bar shows <admin> 15 and timestamp 2/11/07 4:47:50 PM UTC.

# Example: Customized Portal Page

The screenshot displays a web browser window showing the "ASA VPN Marketing" portal. The browser's address bar shows "http://". The page features a left-hand navigation menu with links: "Marketing Home", "Internet Applications", "Explore Networks", "Terminal Servers", "MetaFrame Access", and "Telnet/SSH Servers". The main content area is titled "ASA VPN Marketing" and includes a "Web Bookmarks" section with links to "Cisco Security Marketing" and "ASA Marketing". Below this is a "Custom Intranet web page" section featuring the Cisco logo, a search bar, and navigation tabs for "Solutions", "Products & Services", "Ordering", "Support", "Training & Events", and "Partner Central". The "Solutions" tab is active, displaying a large banner with the text "The network can do much more than move data." and a "Learn More" link. To the right of the banner is a "Related Tools" section with links to "Cisco Powered - Find Recommended Service Providers", "Partner Locator", and "Discussion Forums". Below the banner is a "Technology Solutions for Business" section with sub-sections for "Data Center", "Security", "Mobility", and "TelePresence". To the right of this is an "Industry Solutions" section with links for "Education", "Financial Services", "Government", "Healthcare", "Legal", and "Manufacturing". A small video player is visible in the bottom right corner of the main content area.

Marketing

## ASA VPN Marketing

Marketing Home  
Internet Applications  
Explore Networks  
Terminal Servers  
MetaFrame Access  
Telnet/SSH Servers

Address:

Web Bookmarks

-  [Cisco Security Marketing](#)
-  [ASA Marketing](#)

Custom Intranet web page

 Worldwide   [Log In](#) | [Register](#) | [About Cisco](#)

[Solutions](#) | [Products & Services](#) | [Ordering](#) | [Support](#) | [Training & Events](#) | [Partner Central](#)

### Solutions

  
The network can do much more than move data.

Deliver the best user experience, increase operational excellence, and innovate with a comprehensive set of Cisco network solutions that address the present and future needs of your business, whether it is large or small.

[Learn More](#)

#### Related Tools

- [Cisco Powered - Find Recommended Service Providers](#)
- [Partner Locator](#)
- [Discussion Forums](#)

#### Technology Solutions for Business

-  **Data Center**  
Transform business effectiveness with network-based data center infrastructure services.
-  **Security**  
Protect critical business processes against attack and disruption.
-  **Mobility**  
Intelligent mobility solutions deliver
-  **TelePresence**  
Create a live, face-to-face meeting

#### Industry Solutions

- [Education](#)
- [Financial Services](#)
- [Government](#)
- [Healthcare](#)
- [Legal](#)
- [Manufacturing](#)

See how Cisco technology is redefining collaboration. welcome to the human network. 

# Cisco ASA 5500 Produkt Übersicht



# Cisco ASA 5500 Series: Breadth and Depth

## Industry First Scalable, Multi-Function, Feature Rich Appliance

### Firewall with Application Layer Security



- Multi-layer packet and traffic analysis
- Advanced application and protocol inspection services
- Network application controls
- Advanced VoIP/multimedia security

### IPS and Anti-X Defenses



- Real-time protection from application and OS level attacks
- Network-based worm and virus mitigation
- Spyware, adware, malware detection and control
- On-box event correlation and proactive response

### Access Control and Authentication



- Flexible user and network based access control services
- Stateful packet inspection
- Integration with popular authentication sources including Microsoft Active Directory, LDAP, Kerberos, and RSA SecurID

### SSL and IPSec Connectivity



- Threat protected SSL and IPSec VPN services
- Zero-touch, automatically updateable IPSec remote access
- Flexible clientless and full tunneling client SSL VPN services
- QoS/routing-enabled site-to-site VPN

### Cisco Intelligent Networking Services



- Low latency
- Diverse topologies
- Multicast support
- Services virtualization
- Network segmentation & partitioning
- Routing, resiliency, load-balancing

# Wide-Range of Cisco ASA 5500 Series Security Service Modules (SSMs)

## IPS Security Services Module (AIP-SSM)



- Provides **full-featured IPS and IDS services** for protection of critical network assets
- Available in 3 models: SSM-10, SSM-20, SSM-40
- Delivers up to 650 Mbps of IPS throughput
- Has thumbscrews for easy insertion/removal
- 10/100/1000 out-of-band management port
- Supported on ASA 5510, 5520, and 5540

## Content Security Services Module (CSC-SSM)



- Provides **full-featured Anti-X services** (anti-virus, anti-spyware, anti-spam, anti-phishing, URL filtering, and more)
- Available in two models SSM-10 and SSM-20
- Anti-virus and anti-spyware services licensed by number of users, others optional add-on
- Supported on ASA 5510, 5520, and 5540

## 4-Port GE Services Module (4GE-SSM)



- I/O module offers **four copper 10/100/1000 ports** in addition to **four SFP ports** for improved flexibility and network segmentation
- Customers can use up-to four ports total out of these eight ports, with the ability to mix and match copper and optical GE ports
- Supported on ASA 5510, 5520, and 5540

# Cisco ASA 5500 Series Adaptive Security Appliances

## Solutions Ranging from Desktop to Data Center

### Cisco ASA 5500 Platforms

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



ASA 5505



ASA 5510



ASA 5520



ASA 5540



ASA 5550



ASA 5580-20



ASA 5580-40

Common Criteria & FIPS certified



Teleworker

Branch  
Office

Internet  
Edge

Campus

Data Center

# Zusammenfassung



# Cisco SSL VPN Summary

## Simple and Secure Access from Anywhere



- Broad access from anywhere
- User-friendly interfaces
- World-class security
- Flexible, controlled access options
- Intuitive management
- Fully integrated with the Cisco Self-Defending Network

[www.cisco.com/go/sslvpn](http://www.cisco.com/go/sslvpn)

# Q&A



