Cisco WebVPN for Routers

Industry's First Routing and Security Platform with SSL VPN Remote Access Connectivity

SSL VPN Enables SMB/Commercial Remote Access Needs

SMB/Commercial Customers' Security Drivers*

Customers need*:

Increased requirement for operational efficiency

- Proliferation of mobile workers

- Greater collaboration requirements—partners, vendors, customers

While still facing:

- Increased security threats
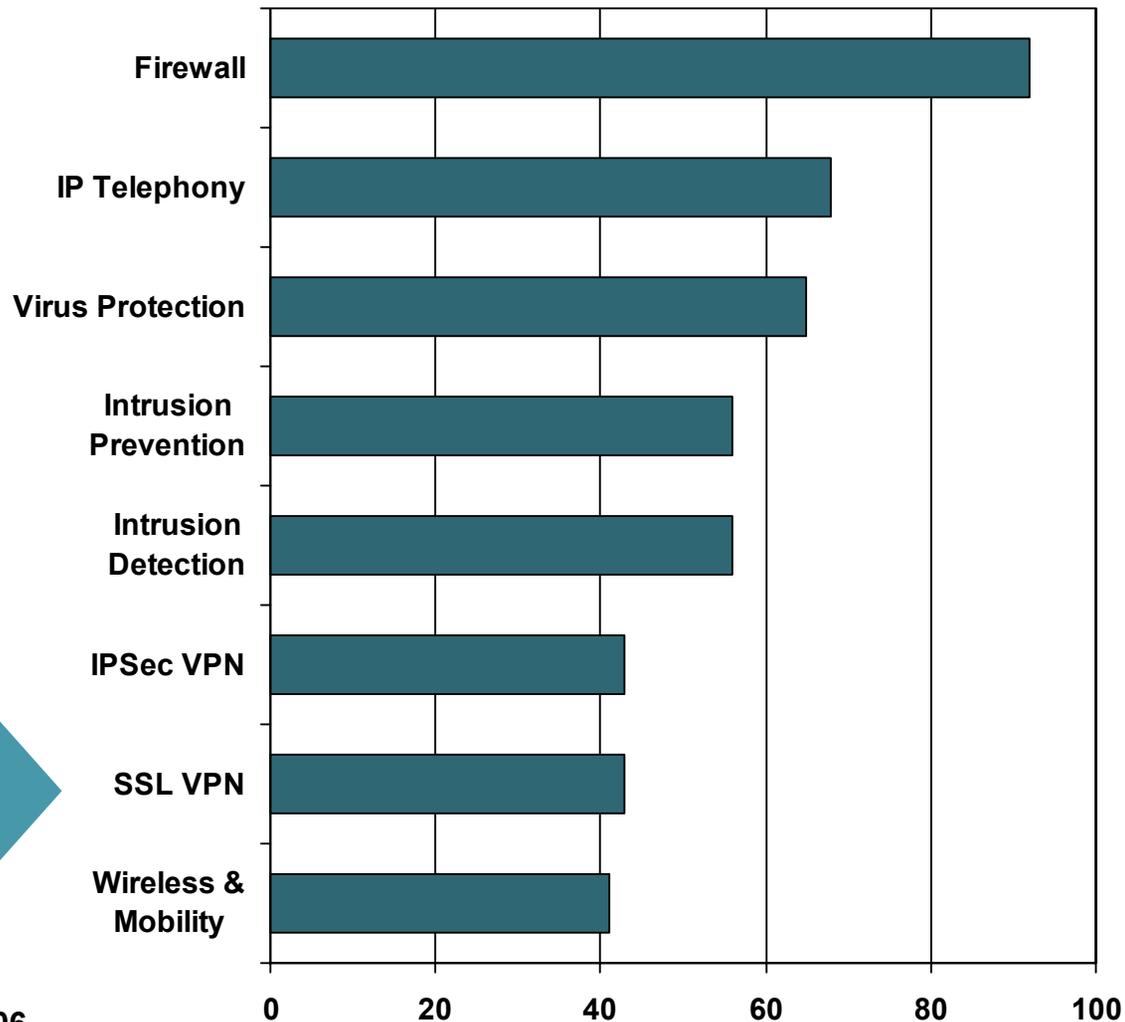
- Increased regulatory compliance burdens

SSL VPN technology offers mid-market customers

- Immediate and spur-of-the-moment employee access, whether on the road or as a teleworker

- Secure remote access without worry of operating system, device interoperability, or access to partner systems

- Threat defense and authentication capabilities reduce threat risk

- When combined with endpoint security, SSL VPN eases proof of regulatory compliance

*Source: Cisco®-sponsored research/Gartner June 2004

2

Customers See High Value in Intelligent Services Integration

- **64 percent of customers preferred integrated services**

- **Reasons:**

  Ease of support & management

  Lower operational costs

  Better performance, scalability

  Lower capital costs

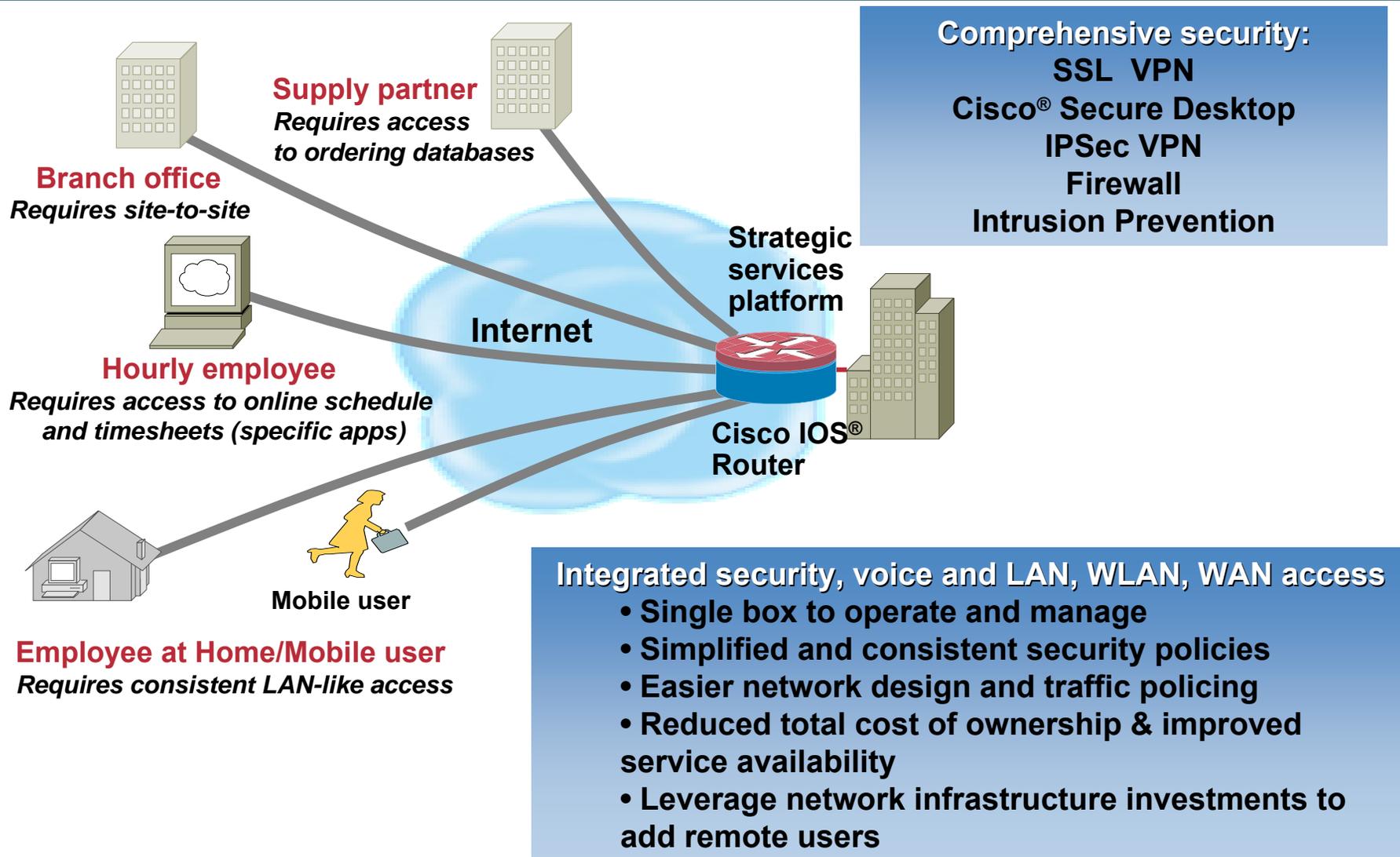 **Move intelligence to branch**

  Feature interoperability

Functions that SHOULD be router integrated

Source: Yankee Group Research Inc., Jan 2006

Bar chart (0–100 scale):
- Firewall: ~92
- IP Telephony: ~67
- Virus Protection: ~65
- Intrusion Prevention: ~55
- Intrusion Detection: ~55
- IPSec VPN: ~43
- SSL VPN: ~43
- Wireless & Mobility: ~41

3

Cisco Routers with WebVPN
Industry's First Routing and Security Platform with SSL VPN

Supply partner
Requires access to ordering databases

Branch office
Requires site-to-site

Hourly employee
Requires access to online schedule and timesheets (specific apps)

Internet

Strategic services platform

Cisco IOS® Router

Mobile user

Employee at Home/Mobile user
Requires consistent LAN-like access

Comprehensive security:
SSL VPN
Cisco® Secure Desktop
IPSec VPN
Firewall
Intrusion Prevention

Integrated security, voice and LAN, WLAN, WAN access
- Single box to operate and manage
- Simplified and consistent security policies
- Easier network design and traffic policing
- Reduced total cost of ownership & improved service availability
- Leverage network infrastructure investments to add remote users

Cisco WebVPN – Cisco IOS Software Release 12.4(6)T (Available March 2006)
Platforms: Cisco 1800, 2800, 3700, 3800 Series Routers

Clientless Access

SSL — Internet — Web browser

Full Network Access

IP over SSL — Internet — Web browser
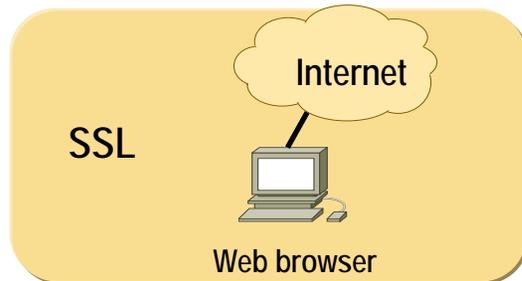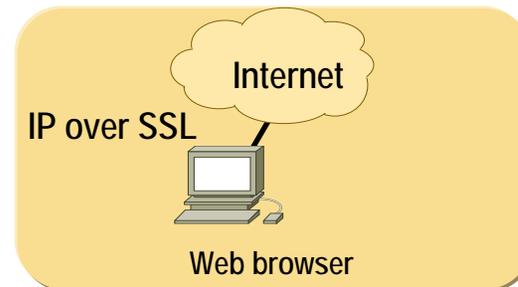
Web-based + application helper

- Browser-based (clientless)
- Intranet web pages, Outlook Web access, Citrix, Windows File Share (CIFS)
- Application helper for non-webified applications like POP/SMTP, IM, Telnet

IP-based applications

- SSL VPN client for virtually any application e.g. Cisco® Softphone
- Dynamically-loaded client may be permanently installed or removed automatically

Cisco Router and Security Device Manager – Simple GUI-based provisioning and management with step-by-step Wizards for turn-key deployment

Cisco Secure Desktop – Prevents digital leakage, protects user privacy, easy to implement & manage, works with desktop guest permissions

Virtualization and VRF awareness – Pool resources while masking the physical attributes and boundaries of the resources

Cisco Routers with WebVPN
SSL VPN Portfolio and Pricing

- **Simple and cost-effective pricing—all WebVPN functionality included in single license**
- **License packs available in 10, 25, and 100 increments**
- **Demo licenses: Two-user demo license available on Cisco® 870–3800 Series Integrated Services Routers and Cisco 7200 and 7301 Routers**

PRICE

Cisco 7200/7301
Up to 150 SSL VPN sessions

Cisco 3800
Up to 100 SSL VPN sessions

Cisco 2800
Up to 75 SSL VPN Sessions

Cisco 1800
Up to 25 SSL VPN sessions

Small Business / Branch

Medium Business / Branch

PERFORMANCE

Typical Scenario with Multiple Devices

Main office

App servers

FW VPN

SSL VPN

IPS

$ $ $

FW, VPN mgmt

IPS mgmt

SSL VPN mgmt

Internet

Secure SSL VPN tunnel

Secure IPSec tunnel

Remote user

Small office
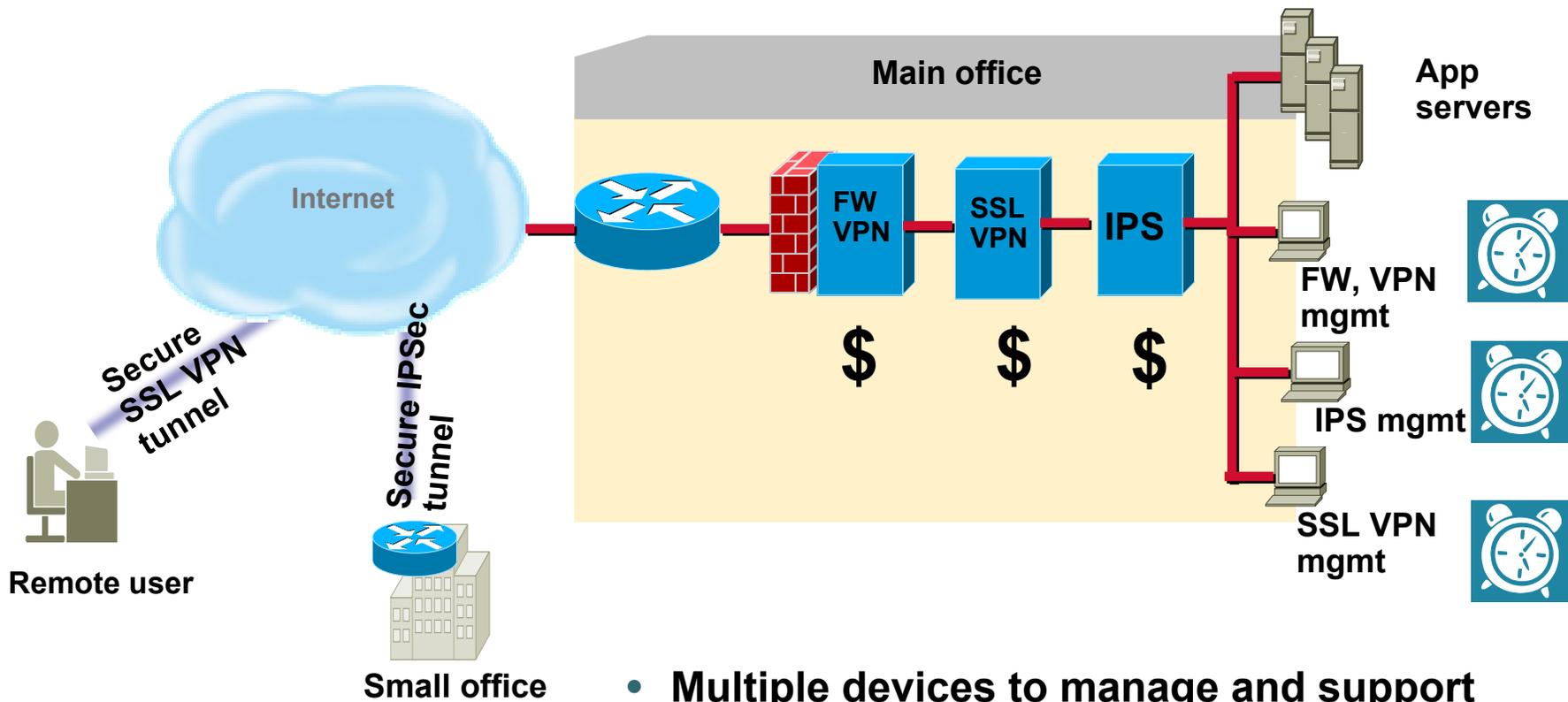
- **Multiple devices to manage and support**
- **Security policies may be inconsistent**
- **More complexity in network design**

Cisco Routers with WebVPN
Industry's First Routing and Security Platform with SSL VPN Remote Access Connectivity

One box to learn, deploy, provision, manage, maintain

SSL VPN **Application firewall** **Intrusion prevention** **Network Admission Control** **URL filtering** **IPSec** **802.1x** **Firewall**

Security

IP Communications IP

Wireless

NetFlow NBAR
ACL WAN
BGP LAN
QoS OER **Networking** IP SLA GLBP
EIGRP GRE NHRP NAT IP Multicast OSPF DHCP

Cisco® Router and Security Device Manager (SDM)
Manage all security, routing and wireless
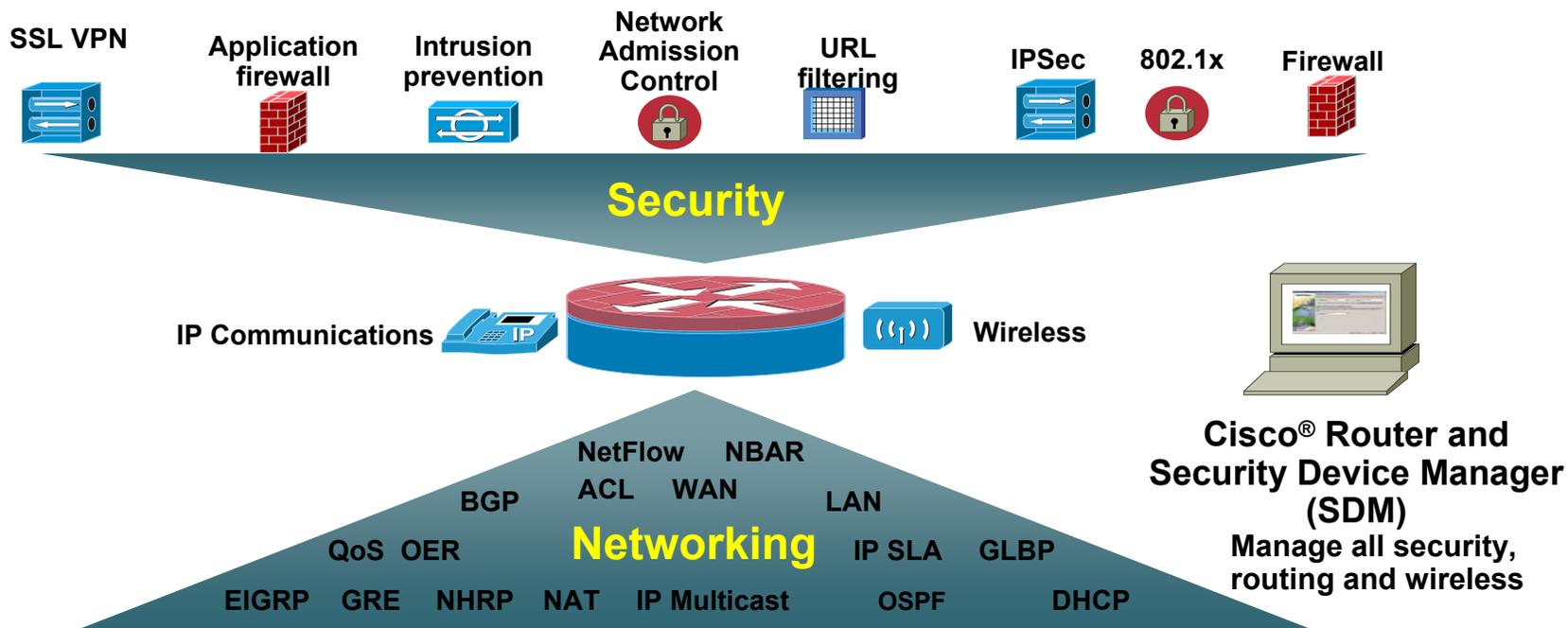
- **Reduced total cost of ownership & improved service availability**
- **Simplified and consistent security policies**
- **Easier network design and traffic policing**
- **Leverage network infrastructure investments**

Clientless Access
Customizable Remote Application Access

Cisco® Router with WebVPN
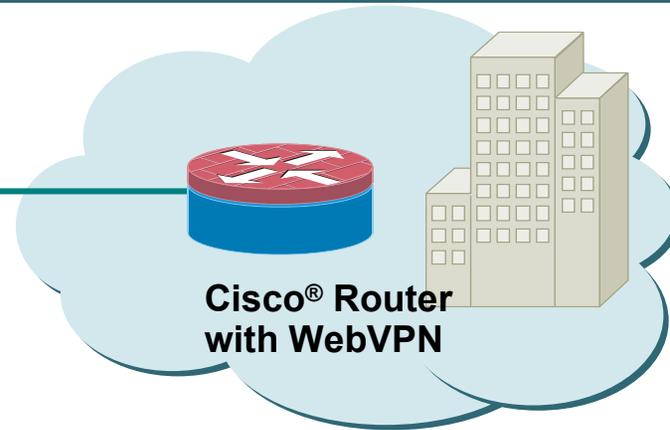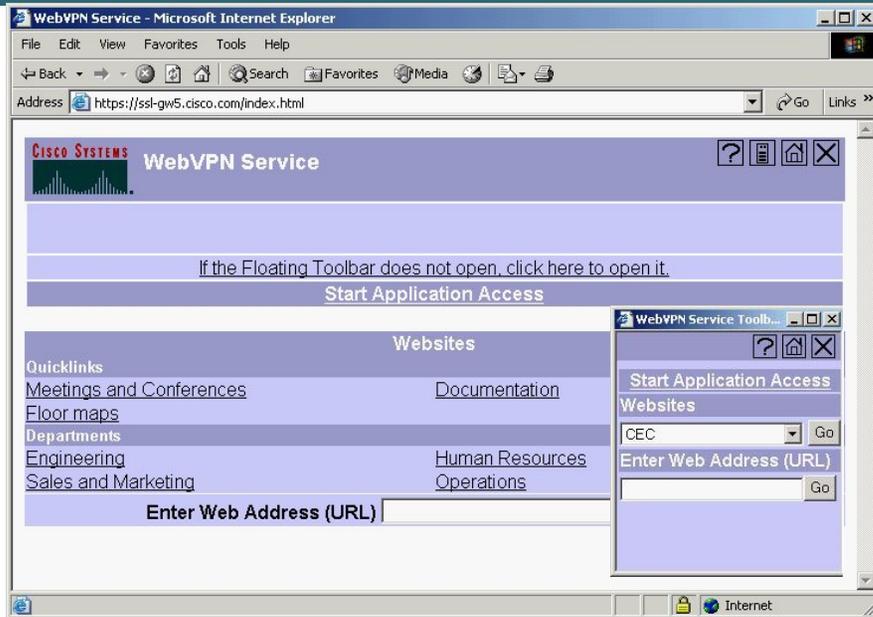
- **Clientless Web-based access allows anywhere access to network resources**
- **Web content transformation provides compatibility with Web pages containing HTML and JavaScript**
- **Uniform and efficient application delivery via fully clientless Citrix support**
- **Applications: Intranet (HTML and JavaScript), Citrix, Windows File Share (CIFS)**
- **Multiple browser support ensures broad connection compatibility**

Clientless Access
Port Forwarding Application Helper

Cisco® Router with WebVPN

Java-based application helper supplements clientless access by providing connectivity to non-webified applications like:

- POP, SMTP, or IMAP e-mail
- Instant messaging
- Calendar
- Client-initiated TCP-based applications like Telnet

Cisco SSL VPN Client
Full Network Access
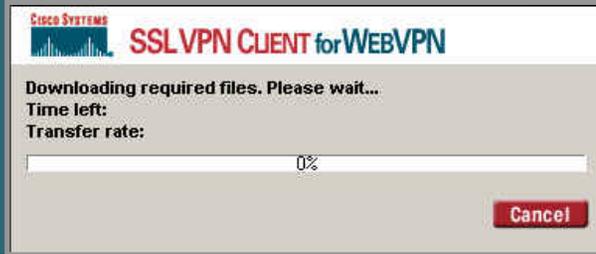
Leverages depth of Cisco® encryption client experience to deliver a **lightweight**, **stable,** and **easy-to-support** SSL VPN tunneling client

Features	Benefits
IPSec-like application access through "Web-pushed" client	Application-agnostic full network access
Touchless central site configuration	Low operating cost
Compatible with Cisco Softphone for VoIP support	Multimedia data, voice desktops for greatest user productivity
Client may be either removed at end of session or left permanently installed	No trace of client after session provides better security
Less than 250 KB download	Fast client download time
No reboot required after installation	Improved productivity, better user satisfaction

Cisco Secure Desktop
Security/Auditing Compliance

Issue: HIPAA, Sarbanes-Oxley, and numerous other regulations require privacy of sensitive information

Cisco® Secure Desktop eases regulatory compliance associated with remote access through:

- Easily demonstrated separation or "sandboxing" of all session data and downloaded content to compliance auditors

- Extensive logging for Cisco Secure Desktop activities

  Was it loaded on endpoint?

  Did it execute properly?

- Validation of remote system security posture prior to session initiation

- Full session data overwrite using government approved DoD sanitation algorithm

Cisco Confidential

Cisco Secure Desktop
Comprehensive Endpoint Security for SSL VPN

Complete preconnect assessment:

Location assessment—managed or unmanaged desktop?

Security posture assessment—AV operational/up-to-date, personal firewall operational, malware present?
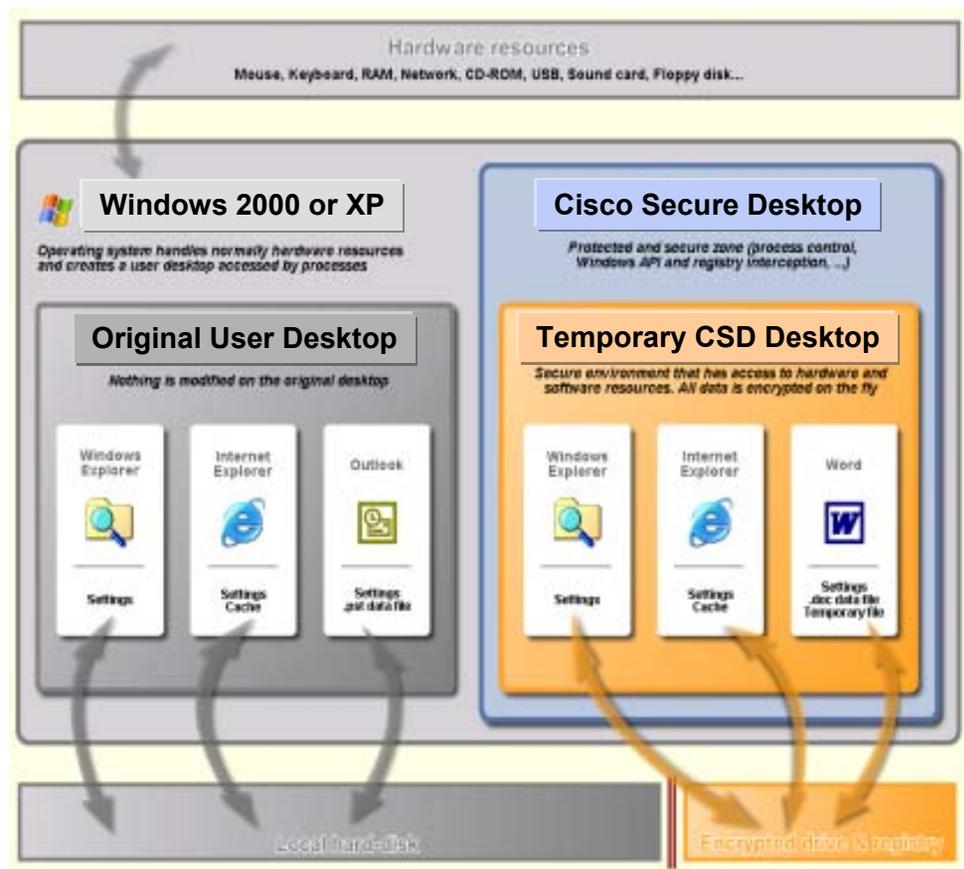
Comprehensive session protection:

- Data sandbox and encryption protects every aspect of session
- Malware detection with hooks to Microsoft free antispyware software
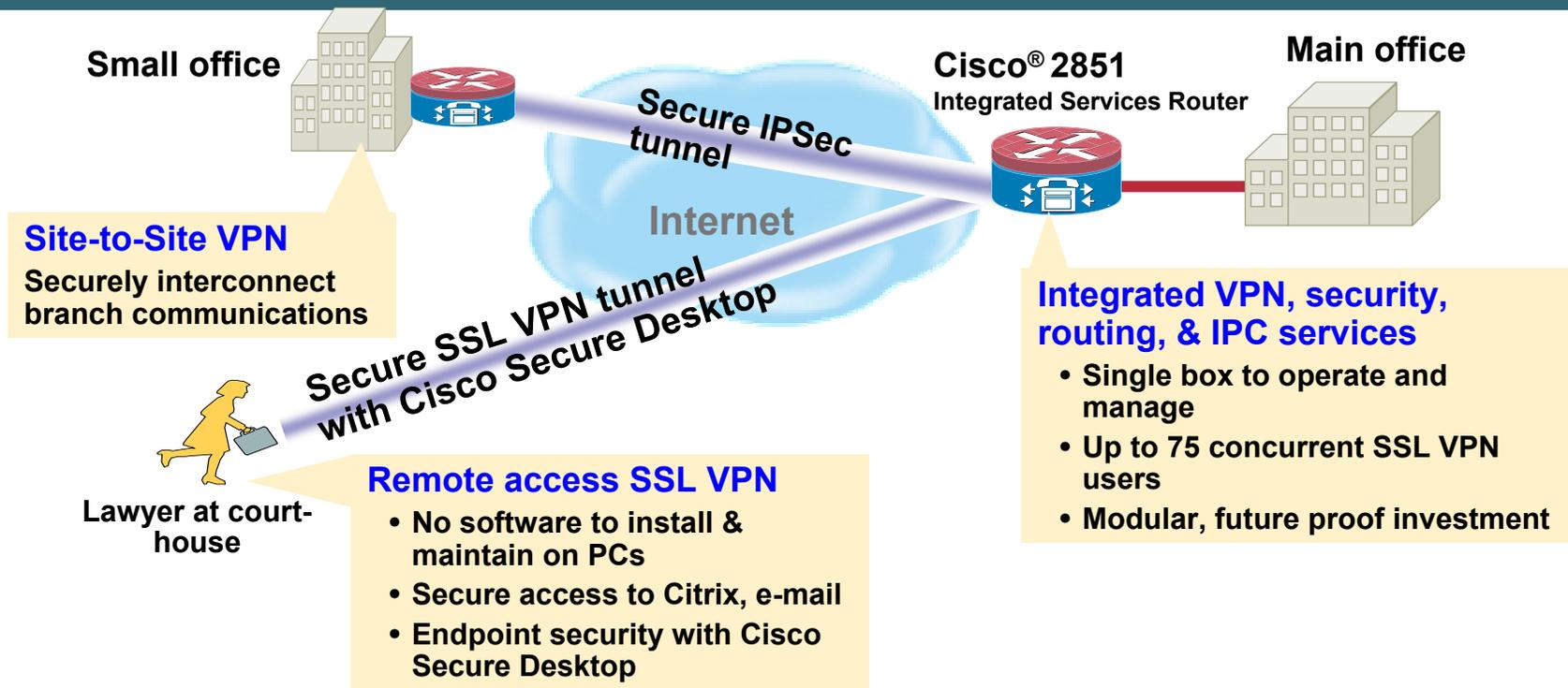
Post-session clean up:

- Encrypted partition overwrite (not just deletion) using DoD algorithm
- Cache, history, and cookie overwrite
- File download and e-mail attachment overwrite
- Auto-complete password overwrite

Works with desktop guest permissions No admin privileges required

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 Confidential

Use Case Scenario
Regional Law Firm with Multiple Offices

Small office

Main office

Cisco® 2851
Integrated Services Router

Secure IPSec tunnel

Internet

Secure SSL VPN tunnel with Cisco Secure Desktop

Site-to-Site VPN
Securely interconnect branch communications

Lawyer at court-house

Remote access SSL VPN
- **No software to install & maintain on PCs**
- **Secure access to Citrix, e-mail**
- **Endpoint security with Cisco Secure Desktop**

Integrated VPN, security, routing, & IPC services
- **Single box to operate and manage**
- **Up to 75 concurrent SSL VPN users**
- **Modular, future proof investment**

Improved staff productivity—On-road access to business applications

Compliance with regulations—All remote communications fully encrypted and logged

Proactive threat defense—Application firewall, inline intrusion prevention, touchless end-point security (Cisco Secure Desktop)

Cisco Router and Security Device Manager (SDM) v2.3 – Delivers Ease of Use

Available April 2006

- **Fast and easy deployment and management of integrated services on Cisco IOS® routers**

  Easy-to-use, Web-based GUI for single device management

  Loaded on router from factory at no additional cost

  Less than 30 minutes to deploy fixed configuration ISRs

  Featured on Cisco® 800—7301 routers

  Supported in seven international languages

- **What's new (v2.3):**

  Integrated Cisco IOS WebVPN Management

  > Simple GUI-based provisioning and monitoring, step-by-step wizards for easy turnkey deployments

  IPS security dashboard

  > Real-time updates on top threats with Cisco IPS Alert Center

  Real-time network and application monitoring

  > NetFlow-based top N statistics, application traffic monitoring, search operations on event tables

  On-box URL filtering management

  Enables zero-touch provisioning for high-volume deployments

  Simplified Cisco IOS Router image management
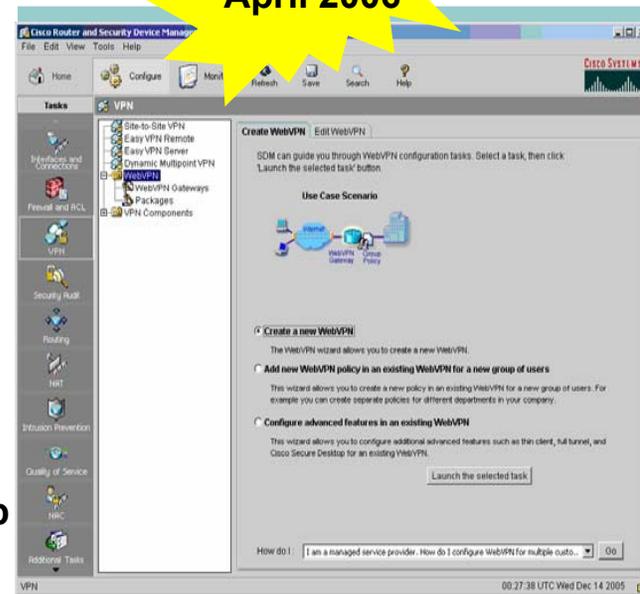
"Cisco Router and Security Device Manager significantly reduces technical expertise required to configure Cisco routers."

ED MIER, MIERCOM

Cisco IOS WebVPN Wizard – WebVPN Gateway Creation

Cisco Confidential   16

Cisco IOS WebVPN Wizard – WebVPN Full Tunnel Configuration Wizard

Summary

Industry's first router to integrate SSL VPN as a form of secure remote access connectivity

- Richest remote access and site-to-site secure access capabilities in the industry

- Cost-effective SSL VPN solution

- Integrating security in a routers saves money and time

- Cisco® Secure Desktop and encryption supports burden-of-proof for regulatory compliance

- **Cisco Router and Security Device Manager adds support for SSL VPN, IPS Security dashboard, and real-time network and application monitoring**
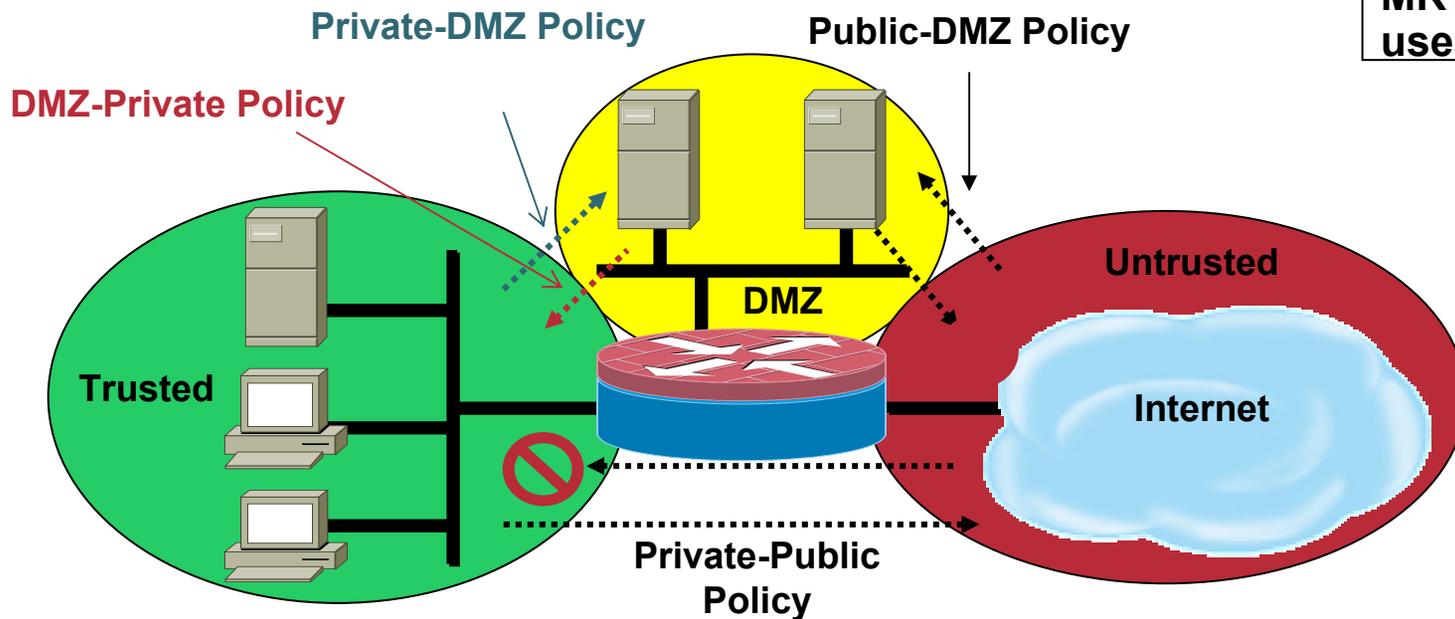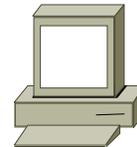
Cisco Confidential

ICSA-Certified Cisco IOS Firewall
What's New in 12.4(6)T ?

HP Open View
OpenNMS
MRTG,etc
uses MIB

Private-DMZ Policy

Public-DMZ Policy

DMZ-Private Policy

Untrusted

DMZ

Trusted

Internet

Private-Public Policy

- Zone-based policy and SNMP MIB for easier administration
- Improved performance for faster session set up and bandwidth
- Improved resiliency through stateful failover
- Efficient shared state with inline intrusion prevention for improved performance

* Cisco® 3800/7200/7301 routers only