

## Securing Voice Traffic with Cisco IOS SSL VPN

This guide describes how to secure voice traffic with Cisco IOS SSL VPN and improve productivity for SOHO users and enterprise Teleworkers.

### Purpose and Scope

Data confidentiality has been an IP security challenge for years. When traditional telephony systems began evolving from PBXs to IP-based systems, organizations started to feel the threat of eavesdropping and the loss of confidentiality for voice communications.

A VoIP VPN combines voice over IP and virtual private network technologies to deliver secure voice. Because VoIP transmits digitized voice as a stream of data, the VoIP VPN solution accomplishes voice encryption simply, applying standard data-encryption mechanisms inherently available in the collection of protocols used to implement a VPN.

Using technology to improve operational efficiency and reduce costs is an ongoing effort for businesses of all sizes, especially for small and medium-sized businesses (SMBs). A 2006 Yankee Group survey shows that more than 50 percent of customers preferred to have these services and applications integrated as part of a complete routing system, with data security and voice ranking the highest.

### Solution

Cisco IOS<sup>®</sup> Software-based SSL VPN (Cisco IOS SSL VPN) provides a cost-saving solution to secure both voice and data traffic.

- You can use a Secure Sockets Layer (SSL)-enabled Web browser to securely establish an SSL tunnel back to the corporate office. This allows secure access to corporate servers from any PC, even if the PC is not a corporate asset.
- Cisco Unified CallManager or Cisco Unified CallManager Express can be easily deployed on voice-enabled routers, including Cisco 1700, 2600XM, 2800, 3700, and 3800 Series routers and Cisco 1861 routers, to provide call-processing capability while providing data connectivity, to a small or medium-sized office or branch.

Integrating voice with Cisco IOS SSL VPN has the following benefits:

- A convenient solution that offers secure voice and data to home offices and “road warriors.” The VPN will allow VoIP to pass through a firewall, which has been difficult without VPNs. User will have access to advanced applications, as though they were in the main office.
- Simplified user experience. Voice security is transparent to end users.
- Ideal for securing the increasing number of data applications within a unified communications infrastructure, such as presence, SMS, and integrated messaging.
- Centralized voice services with simplified billing (end users don’t have to submit expenses, and you can easily track the calls they make).
- Call savings (assuming the organization has a better call plan for each individual user).

- Cost-effective access to end-user services. Users can check voicemail or have calls routed to a home IP phone or soft phone.
- Controlled Internet access with centralized or remote URL filtering.
- Reduce total cost of ownership (TCO). Voice, SSL VPN, and routing can be deployed on the same device.
- Greater scalability with VPN architecture. One tunnel provides protection for multiple applications, including data and voice.

## Platforms and Images

Recommended platforms for Cisco IOS SSL VPN gateways are Cisco 3825 and 3845 Integrated Services Routers with AIM-VPN/SSL-3.

Supported platforms for Cisco IOS SSL VPN are Cisco 871 Integrated Services Routers; Cisco 1800, 2800, 3700, and 3800 Series Integrated Services Routers; Cisco 7200 Series Routers; and Cisco 7301 Routers.

Supported platforms for Cisco Unified CallManager Express are Cisco 1700 Series Modular Access Routers; Cisco 1800, 2800, 3700, and 3800 Series Integrated Services Routers; and Cisco 2600XM Multiservice Routers.

IP telephony is supported in Cisco IP SoftPhone deployments based on Cisco Unified Communicator.

Cisco IOS SSL VPN is available in Cisco IOS Software Release 12.4(6)T and later. An Advanced Enterprise or Advanced IP Services image is needed to have both SSL VPN and Cisco Unified CallManager Express capabilities. The image used in this guide is c3845-adventerprisek9-mz.124-15.T.bin.

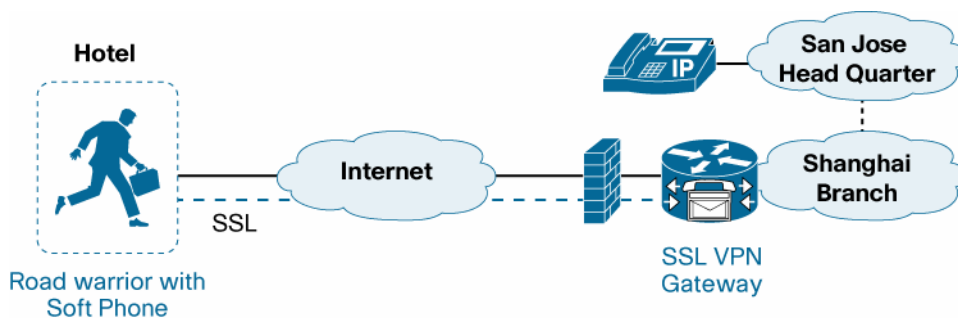
## Application Scenarios<sup>1</sup>

### Scenario A: Road Warrior at Hotel

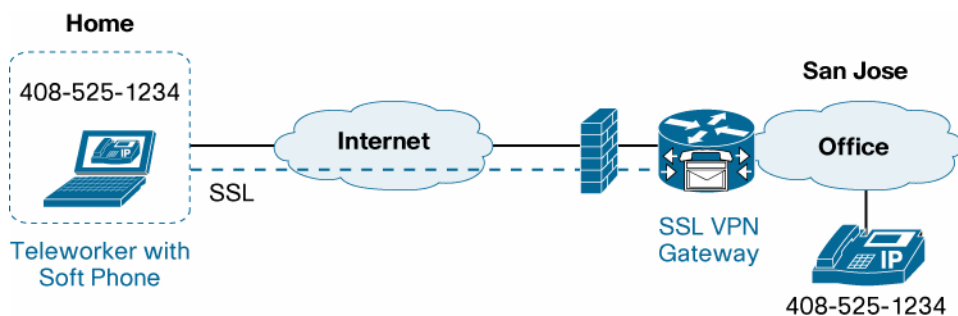
You are staying at a hotel while on a business trip in Shanghai, China. You need to talk to your colleagues and engineers in California, and have scheduled a conference call. International phone calls are expensive, and your manager has just announced a budget control policy. The hotel has Internet service, which is US\$5 per day. Using your laptop, you connect to the Internet, launch a Web browser, and connect to an SSL VPN gateway that is located in your company's Shanghai office. A VPN connection is established and you are able to use the soft phone on your laptop to dial into a conference call. The meeting lasts for two hours and your call costs nothing more than the \$5 Internet access fee.

---

<sup>1</sup> Those scenarios need to operate IOS SSL VPN in full tunnel mode with Cisco SSLVPN Client or Any Connect Client

**Figure 1.** Road Warrior at Hotel**Scenario B: Teleworker at Home**

You recently moved 40 miles away from your office. You decide to work from home every Friday to avoid the traffic. When you are at home, you open a Web browser and connect to the SSL VPN gateway at your corporate network. The gateway automatically pushes down a VPN client and a tunnel is established. You can access your e-mail, browse internal Websites, and make phone calls as though you are in the office. Your IP phone will maintain the same number you are using in the office. Your customers and colleagues call your office phone number can easily reach you. They can't even tell if you are picking up the phone at home or in the San Jose office!

**Figure 2.** Teleworker at Home**Scenario C: VPN Mobility**

You are at a coffee shop where Wi-Fi is available. You connect your laptop to the Internet and establish an SSL VPN tunnel to the corporate network. A colleague sends you an SMS message for a technical problem. As he invites you into a conference call, you open the soft phone on your laptop and dial into the meeting. Half an hour later, you hang up the phone and leave to catch a train. When you walk out of Wi-Fi range, the wireless adaptor on your laptop automatically falls back to your cellular phone or modem (such as 1xEVDO or HSDPA). During this period, your laptop has changed IP address, yet your SSL VPN client has not prompted for re-authentication. On the train, you open your laptop and your SSL VPN connection is still up and running; your SMS session is not interrupted. Because Cisco SSL VPN provides VPN mobility, you can roam different connection types without having to re-authenticate.

**Figure 3.** Roaming Without Re-authentication

