Voice Integration with Cisco Enhanced EasyVPN

This guide describes how to integrate voice with Cisco Enhanced Easy VPN to provide voice quality control as well as data and voice security to the corporate network and improve productivity for enterprise teleworkers and small office/home office (SOHO) users.

Purpose and Scope

Maintaining data confidentiality is an ongoing IP security challenge that has become a key concern as organizations replace traditional telephony systems with IP-based systems. The threat of eavesdropping and loss of confidentiality in an IP based environment pose a range of risks including breaches of industry regulations and negative impacts on corporate image. As IP based voice systems evolve into unified communications, extending beyond the corporate network to include remote access services, the requirements for a flexible confidentiality solution grows.

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

Cisco Enhanced Easy VPN can be used to provide secure unified communications while greatly simplifying VPN deployment with centralized VPN management across all Cisco VPN devices. Using technology to improve operational efficiency and reduce costs is a common goal for businesses of all sizes. Cisco Enhanced Easy VPN supports integration of a variety of remote devices within a single deployment and with a consistent policy and key management method, which simplifies remote-side administration.

In addition, quality of service (QoS) policy can be applied on the Cisco Enhanced Easy VPN Server and Easy VPN Remote router for voice quality control. For example, residential broadband connectivity is a best-effort network that usually provides good downlink speed, but the uplink speed is not as good. Without QoS policy, regular data, voice, and other essential traffic are treated equally. When traffic becomes congested, packets are dropped randomly and you will suffer a cluttered voice call. QoS policies can be applied on the EasyVPN routers so that voice and other essential traffic get higher priority than regular data packets. QoS can also be applied to shape output traffic from a Server to prevent the over-saturation of the downstream Remote devices.

Benefits

Integrating voice with Cisco Enhanced Easy 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. Users will have access to advanced applications, as though they were in the main office.
- Simplified user experience. Unified communications security is transparent to end users.
- Voice quality is guaranteed, even upon traffic congestion.

- 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.
- Reduce total cost of ownership (TCO). Voice, IPsec 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

Supported platforms for Cisco Enhanced Easy VPN Server are:

- Cisco 1800 Series
- Cisco 2800 Series
- Cisco 3800 Series
- Cisco 7200 Series
- Cisco 7301

Supported platforms for Cisco Enhanced Easy VPN Remote are:

- Cisco 871
- Cisco 1800 Series
- Cisco 2800 Series

Supported software clients for Cisco Easy VPN Client are Cisco VPN Client Version 4.0 and later.
Supported platforms for Cisco Unified CallManager Express are:

- Cisco 1700 Series
- Cisco 2600XM Series
- Cisco 2800 Series
- Cisco 3700 Series
- Cisco 3800 Series

Supported unified communications deployments described in this guide are:

- VoIP physical phone deployment based on Cisco Unified IP Phone 7960G and Cisco Unified IP Phone 7970G
- VoIP Cisco IP SoftPhone deployment based on Cisco IP Communicator

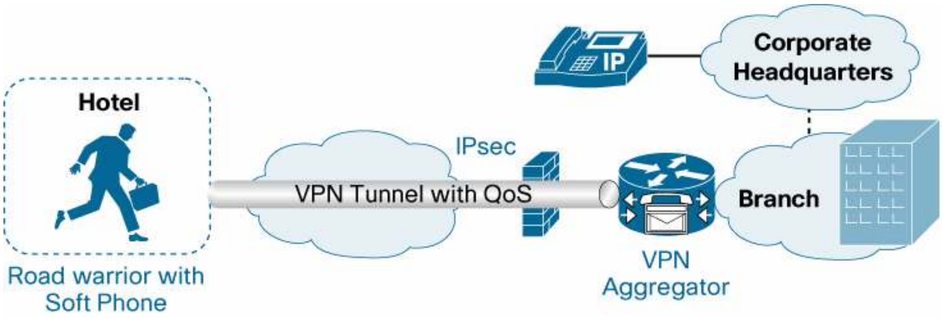
Cisco Enhanced Easy VPN is available in Cisco IOS Software Release 12.4(6)T and later. To have both Cisco Enhanced Easy VPN and Cisco Unified Communications Manager capabilities, an Advanced Enterprise or Advanced IP Services image is required. The images used in this guide are c3845-adventerprisek9-mz.124-15.T3.bin, c870-advsecurityk9-mz.124-15.T3.bin, and Cisco VPN Client Version 4.0.5(rel).

Application Scenarios

Scenario A: Road Warrior at Hotel

You are staying at a hotel while on an International business trip. You have scheduled a conference call to talk to your colleagues and engineers. International phone calls are expensive, and your manager has just announced a budget control policy. The hotel has Internet service, which costs US$10 per day. You open the laptop, connect to the Internet, double-click Cisco VPN Client, look through its connection profiles, and connect to the closest VPN server, which is located in your company's local branch. In a few seconds, the VPN tunnel is established and you are able to use the soft phone on your laptop to dial into the conference call. The meeting lasts for two hours and your call costs only $10 Internet access fee! How nice is that?!

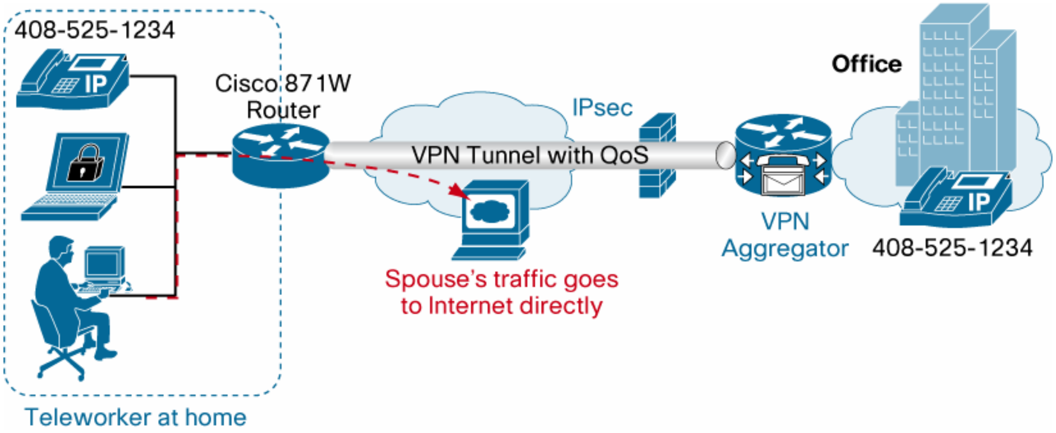
Figure 1. Road Warrior at Hotel



Scenario B: Teleworker at Home

You recently bought a house in suburb, which is 40 miles away from your company office. You decide to work from home every Friday to avoid the traffic. To connect to your office network, you subscribe to a cable-based broadband Internet service and use a Cisco 871 wireless router as an Easy VPN Remote router. Your router operates in client mode, to protect the IP phone and laptop behind the router from being reachable by the Internet attacks. You keep the tunnel always up so that you can access your e-mail, browse internal Websites, and make phone calls without the hassle of making VPN connections every time you access the office network. Your IP phone can even maintain the same number you use in the office. Your customers and colleagues can call your office phone number and easily reach you. Your spouse and kids' traffic goes directly to the Internet without being sent to the VPN tunnel.

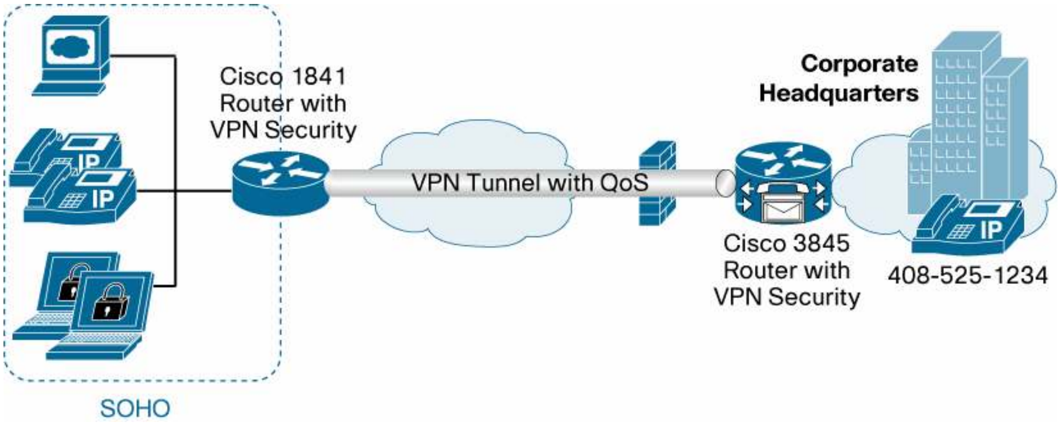
Figure 2. Teleworker at Home



Scenario C: SOHO Environment

You are working at a local sales office with three colleagues. The sales office connects to the headquarter using a Cisco 1841 Integrated Services Router as the Easy VPN Remote device. As in Scenario B, you have the VPN tunnel up all the time, only this time, the Easy VPN Remote is operating in network extension mode, so the network behind it is routable by the corporate network. You and your colleagues can access corporate e-mail, browse internal Websites, and make phone calls without the hassle of making VPN connections every time you access the corporate network. And your manager, who is located at headquarters, can easily access your wiki pages on a Web server at your local office.

Figure 3. SOHO Environment



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C27-458842-00 03/08