Securing Internet Telephony: Encrypting Voice with VoIP-over-VPN

Voice-encrypted VoIP-over-VPN protects the privacy of corporate voice communications over the Internet while delivering the cost-saving benefits of Voice-over-IP.

PATTON Electronics Co.

Network Access & Connectivity

Introduction

Voice over Internet Protocol (VoIP) offers tremendous cost-savings for the enterprise by means of reduced or eliminated telephony charges, consolidated network architectures, and reduced network operations and maintenance overhead. As with any new technology, however, there can be a down-side.

Most VoIP gateways compromise communication security by transporting VoIP and data traffic over public networks without encryption, making the information susceptible to interception by snoopers, hackers, and so forth. Because of such security concerns, enterprises that handle highly-sensitive information (such as financial, government, and military institutions) have been reluctant to cash in on the benefits of deploying a VoIP system.

Standards for voice encryption, such as SRTP and SIP TLS, are emerging. These techniques encrypt the voice as the analog signal is converted to digital form in the coder-decoder (CODEC). But the standards are still under development and are not yet ready for the commercial market. VoIP-over-VPN, in contrast, offers a secure solution for converged digital voice and data communications today.

VoIP gateways with VoIP-over-VPN offer companies that handle sensitive information–and the carriers that serve them—a way to move forward and implement secure, converged VoIP and Data networks.

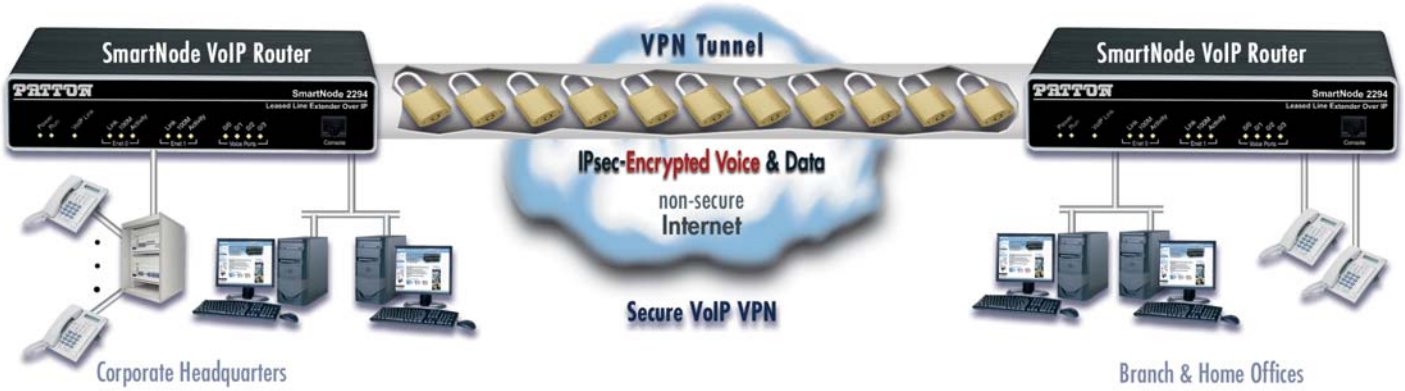
VoIP-over-VPN Technology for Commercial Implementations

Patton Electronics Co. pioneered an early commercial implementation of encrypted VoIP-over-VPN technology in 2006 by adding voice encryption to their SmartNode™ brand of VoIP gateway routers.

Secure Encrypted Voice

A VoIP VPN combines Voice-over-IP and Virtual-Private-Network technologies to offer a method for delivering secure voice. Because VoIP transmits digitized voice as a stream of data packets, the VoIP VPN solution accomplishes voice encryption simply and elegantly. The technique applies existing standard data-encryption mechanisms inherently available in the collection of protocols used to implement a VPN.

The VoIP gateway-router first converts the analog voice signal to digital form, encapsulates the digitized voice within IP packets, then encrypts the digitized voice using IPsec, and finally routes the encrypted voice packets securely through a VPN tunnel. At the remote site, another VoIP router decodes the voice and converts the digital voice to an analog signal for delivery to the phone.



Even the most security-conscious enterprises can cash in on the cost-savings of VoIP.

Other advantages

Security is not the only reason to pass Voice-over- IP through a Virtual Private Network, however. Session Initiation Protocol, the preferred VoIP protocol is notoriously difficult to pass through a firewall because it uses random port numbers to establish connections. A VPN solution avoids this firewall issue when configuring remote VoIP clients. The VPN virtually moves users inside the same local network as the VoIP server.

Voice-over-VPN creates a virtual private network (VPN)—a private network that traverses the Internet—while maintaining privacy via IPsec and DES/AES 256-bit encryption. IPsec is the standard for securing data communications over the Internet, while DES and AES provide strong encryption. The SmartNode IPsec creates private VPN tunnels ensuring secure VoIP, voice and data traffic while protecting all inter-office voice and data communications over the Internet. The tunnels allow users, located in separate offices, to communicate as if they were connected by a single private network. VPN tunnels protect all communications (both VoIP and Data) from prying eyes and ears while ensuring that all communications came from the trusted source.

SmartNode IKE is a dynamic and automatic security exchange function that further enhances the security and ease-of-use for Voice-over-VPNs and data VPNs. By constantly changing the encryption key on a user-configurable interval (e.g. once per hour), IKE dramatically reduces any chance of the traffic may be intercepted. IKE also simplifies VoIP gateway deployment. Eliminating manual key configuration makes the encryption software much easier to configure and administer. With dynamic key exchange, the network administrator can maintain the highest levels of security without having to perpetually reconfigure the encryption key.

SmartNode Voice-over-VPN and IKE are available starting with SmartWare release 3.20 for all SmartNodes as part of the VPN software license key option. Registered customers with the VPN license key installed can download and use the software from upgrades.patton.com.

SmartNode™ VoIP-VPN Feature Highlights

- IPsec 256-bit encryption for voice and data
- DES/3DES & AES strong encryption keys
- Internet Key Exchange (IKE) for automatic, dynamic keying
- Configurable automatic key exchange interval
- Standard upstream and Patton's DownStreamQoS for toll-quality voice
- Prioritized traffic scheduling and shaping

Conclusion

By encrypting both voice and data, VoIP-over-VPN technology unlocks the cost-savings of Voice-over-IP for security-conscious enterprises. By building voice encryption with IPsec and Internet Key Exchange (IKE) into SmartNode™ VoIP gateway-routers, Patton makes cost-saving voice-and-data convergence a viable option for enterprises that handle even the most highly-sensitive information.

Strong encryption. SmartNode™ VoIP routers use VPN tunnels to create secure inter-office connections that carry encrypted voice and data through non-secure networks (such as the Internet). Patton's VoIP-VPN technology employs 256-bit AES/DES strong encryption to lock out prying eyes and eavesdropping ears. IKE protects against hackers by continuously changing the encryption key at configurable intervals.

Secure voice-encryption and VoIP-VPN technology lets users communicate with utmost confidence, so, even the most security-conscious network administrators can save money with converged infrastructures for VoIP, voice, and data communication.

7622 Rickenbacker Drive Gaithersburg, MD 20879 USA
Phone **+1-301-975-1007** • Fax +1-301-869-9293
URL **www.patton.com** • E-mail **marketing@patton.com**
Document 07MVOIPVPN-WP