V^{3}PN SRND Introduction

This publication extends the Cisco Architecture for Voice, Video, and Integrated Data (AVVID) by enabling voice and video applications to be transported over a site-to-site IPSec VPN. Just as enterprise implementers expect to run these applications over a private WAN, such as Frame Relay or ATM, they also expect to run voice and video across their VPN implementation with the same quality and level of service. Further, the enterprise implementer should be able to do so and have the VPN be fairly transparent to these applications.

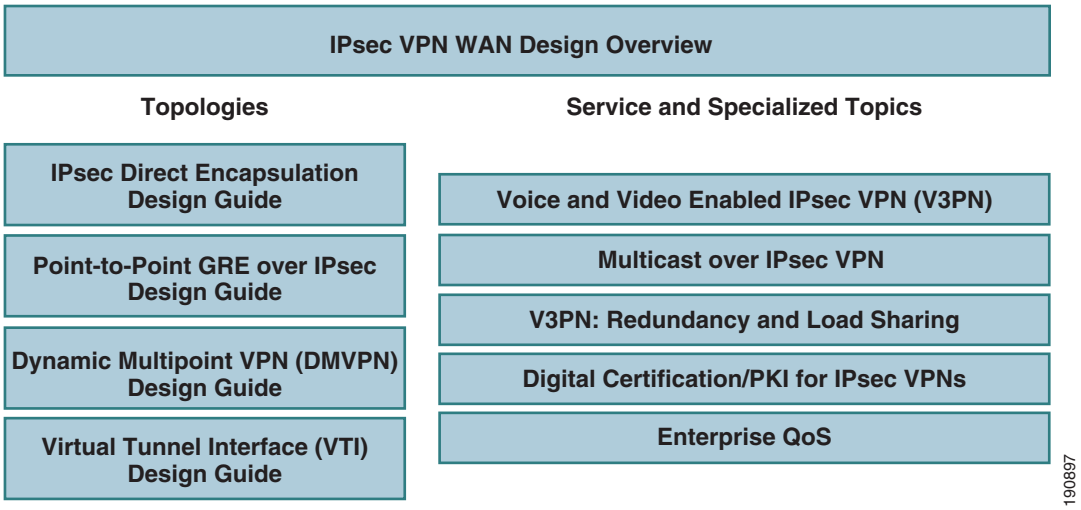
To provide these capabilities, Cisco designed Voice and Video Enabled IPSec VPN (V^{3}PN), which integrates three core Cisco technologies: IP Telephony, Quality of Service (QoS), and IP Security (IPSec) VPN. The result is an end-to-end VPN service that can guarantee the timely delivery of latency-sensitive applications such as voice and video.

This chapter presents the following topics:

Design Guide Structure

This design overview is part of a series of design guides, each based on different technologies for the IPsec VPN WAN architecture. (See Figure 1.) Each technology uses IPsec as the underlying transport mechanism for each VPN.

Figure 1 IPsec VPN WAN Design Guides



Supporting Designs

V^{3}PN is designed to overlay non-disruptively on other core Cisco AVVID designs, including:

- *Enterprise QoS Design Guidelines*— http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html

This SRND will not cover each of these three technologies in detail, but will instead focus on the intersection of, integration of, and interactions between these functions of the network. Familiarity with design and implementation guides for these underlying technologies will be extremely beneficial to the reader. Please review these guides before attempting to implement a V^{3}PN.

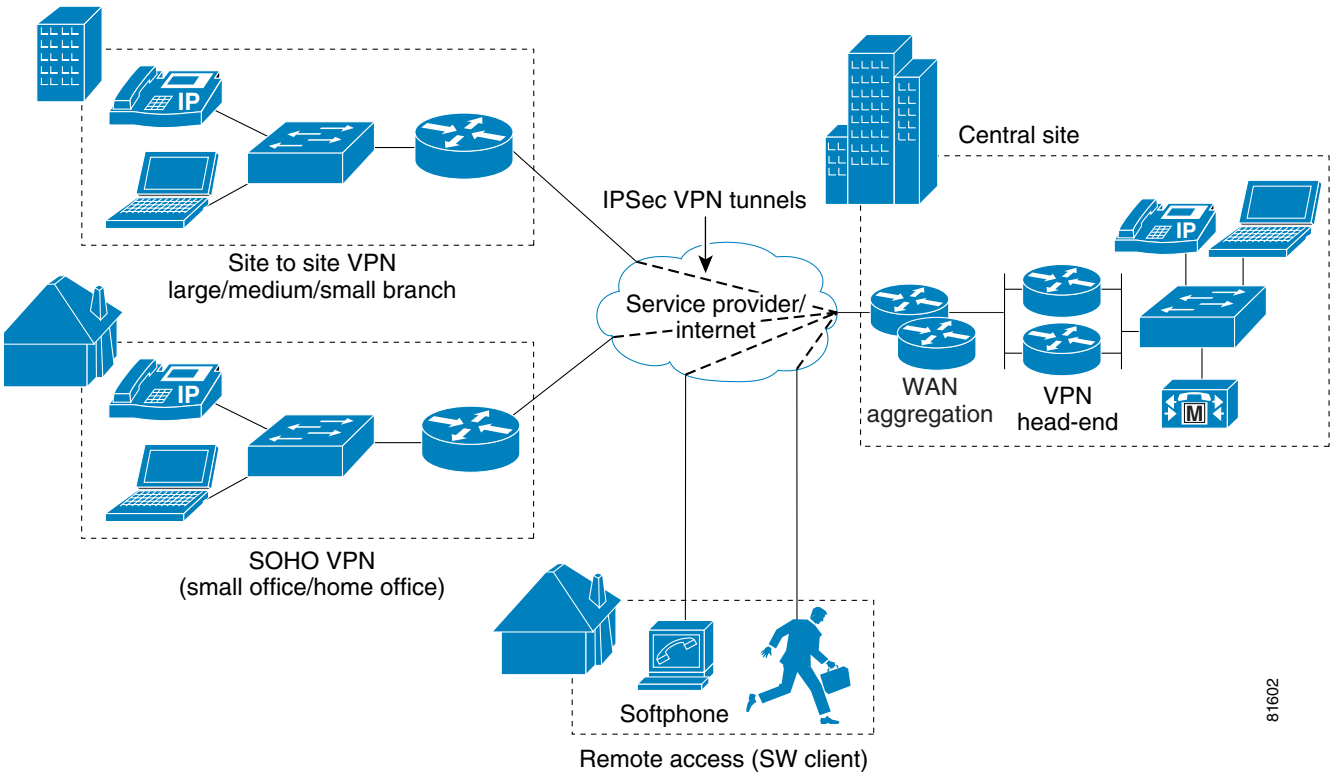
The underlying VPN design principles are based on the SAFE VPN Architecture, therefore the reader should also first be familiar with that architecture and recommendations.

Technical Assistance Center (TAC) Technical Tips are a valuable source of configuration examples for the technologies deployed in this design guide. Please refer to the Technical Tip section after logging on the Cisco TAC Cisco.Com page at: http://www.cisco.com/tac.

Composite Solution Description

IPSec VPNs have been deployed as private WAN alternatives for enterprise networks whether managed by the enterprise themselves or as part of a service provider managed service. Figure 1-2 illustrates the composite IPSec VPN deployment models that are deployed today:

Figure 1-2 Composite IPSec VPN Deployment Models



Site-to-site IPSec VPN's are used to connect small, medium, and large branch offices to a central location or locations. This model is referred to in Cisco Enterprise Solutions Engineering Design Guides as *Site-to-Site Branch VPN*.

IPSec VPN's can also be used to connect small office/home office (SOHO) locations to corporate locations. When the VPN connections are *static* (fixed) in nature this model is referred to as *site-to-site SOHO VPN*.

Finally, when the VPN connections are *dynamic* (session-by-session) this model is referred to as *Remote Access VPN*.

The site-to-site branch VPN model is capable of enabling voice and video transport across the VPN in a high quality manner—including transport over service provider networks that support QoS. The site-to-site SOHO VPN model is also capable of transporting high quality voice and video over the VPN; however, broadband service providers are in the early stages of providing QoS support.

This version of this Design Guide focuses primarily on the site-to-site branch VPN model of deployments, as this model currently has the highest level of proven deployability both in terms of Cisco IOS VPN Router functionality as well as service providers being capable of offering a multi-service VPN service to enterprise implementers.

The primary objectives for this Design Guide will be to:

- Define the safe boundaries in which this solution may be deployed including design and implementation considerations as well as highlighting appropriate caveats.
- Provide hardware platform and software code recommendations based on the requirements of a given deployment, including performance and configuration information where applicable.

Since an IPSec VPN deployment involves a service provider this document will delineate requirements of the enterprise as well as what the service provider must provide in order to ensure a successful V^{3}PN deployment.

Solution Benefits

V^{3}PN provides the following benefits for enterprise networks:

- Higher Productivity—Enables extension of central site voice, video, and data resources and applications at all corporate sites, thereby enabling employees to work as productively and efficiently as if they were located at the central site.
- Ease of Provisioning—V^{3}PN provides enterprises with a flexible means of deploying additional sites that are voice enabled by simply connecting to a service provider instead of procuring private WAN connectivity.
- Lower Cost—Pricing for connection via a local Internet service provider is distance insensitive, analogous to Frame Relay. Further, an enterprise can attain converged inter-site connectivity, lowering both the costs of bandwidth and toll cost.
- Flexibility—V^{3}PN provides support for extensions to the enterprise applications, such as IP Call Centers (IPCC), Video Conferencing, e-Learning, and Teleworking, irrespective of the physical location of resources and users of these resources.
- Increased Security—V^{3}PN is implemented using IPSec encryption and device authentication, thereby providing a higher level of security compared to typical unencrypted and unauthenticated time-division multiplexing (TDM) and voice/video transport.
- Return on Investment—Because V^{3}PN is implemented across the Cisco IOS VPN Router product portfolio, existing investments are preserved and can be extended.

For service providers, V^{3}PN provides the following benefits:

- New Revenue – Enabling voice and video transport across IPSec VPN's provide a potential source of incremental revenue for the service provider if deploying a Managed Service. The service provider also benefits even if the enterprise manages the IPSec VPN carrying VoIP where as the service provider can achieve incremental revenue by providing value add QoS enabled services.
- Service Differentiation—V^{3}PN provides the ability to encrypt voice and video, which is a new security feature that can be offered relative to traditional TDM networks.
- New Customers—By qualifying for the *IP Multi-service* VPN Cisco Powered Network designation, service providers are better positioned to receive new enterprise customers being referred by Cisco account teams for V^{3}PN services.
- Customer Retention—By adding additional value to the enterprise customer, the retention likelihood is greater for service providers, particularly as the enterprise customer becomes more reliant upon the V^{3}PN service for mission critical applications beyond data transport, in other words voice and video.

Solution Scope

This publication will be extended and updated over time as capabilities expand the addressable market. This version of this Design Guide focuses on the following:

- Site-to-site IPSec branch VPN deployment model, where the interface to the service provider is typically a media such as Point-to-Point (PPP), High-Level Data Link Control (HDLC), Frame Relay (FR), Asynchronous Transfer Mode (ATM) or Ethernet (in the case of Metropolitan Area Networks). This Design Guide will be extended in a future revision to include information on the site-to-site SOHO VPN deployment model, typically utilizing DSL or Cable media.
- Cisco IOS VPN Routers to terminate the IPSec VPN tunnels. The PIX platforms will be addressed in a later Design Guide.
- Video and IP Multicast are not fully addressed in this design guide version however where appropriate known design recommendations will be made for both. Tested design recommendations for Video and IP Multicast will be the focus of a subsequent revision of this design guide.
- V^3PN was evaluated in a design utilizing IPSec with GRE to support dynamic routing protocols and IP Multicast. However, the performance and scalability results for IPSec/GRE should also be applicable to an IPSec only configuration. An IPSec-only configuration is used as the design for an internal Cisco deployment of V^3PN.

Other features that were not evaluated for this revision of the Design Guide include:

- IPSec Stateful Failover
- LZS Compression
- GRE Tunnel Keepalives
- Voice Activity Detection (VAD)

References and Reading

Table 1-1 IETF Requests for Comment

IETF Request for Comment (RFC)	Topic
RFC2401	Security Architecture for the Internet Protocol
RFC2402	IP Authentication Header
RFC2403	The Use of HMAC-MD5-96 within ESP and AH
RFC2404	The Use of HMAC-SHA-1-96 within ESP and AH
RFC2405	The ESP DES-CBC Cipher Algorithm With Explicit IV
RFC2406	IP Encapsulating Security Payload (ESP)
RFC2407	The Internet IP Security Domain of Interpretation for ISAKMP
RFC2408	Internet and Key Management Protocol (ISAKMP)
RFC2409	The Internet Key Exchange (IKE)
RFC2410	The NULL Encryption Algorithm and Its Use With IPsec
RFC2411	IP Security Document Roadmap
RFC2412	The OAKLEY Key Determination Protocol

Table 1-2 Reference Websites

Topic	Link
Enterprise VPNs	http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking_solutions_packages_list.html
Cisco SAFE Blueprint	http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solution_relevant_networking_solutions_listing_intro_sc.html
Cisco Network Security	http://www.cisco.com/en/US/products/hw/vpndevc/
Cisco VPN Product Documentation	http://www.cisco.com/univercd/cc/td/doc/product/vpn/
Download VPN Software from CCO	http://www.cisco.com/kobayashi/sw-center/sw-vpn.shtml
Improving Security on Cisco Routers	http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml
Essential Cisco IOS Features Every ISP Should Consider	http://www.cisco.com/warp/public/707/EssentialIOSfeatures_pdf.zip
IPSec Support Page	http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Internetworking:IPSec
Networking Professionals Connection	http://forums.cisco.com/eforum/servlet/NetProf?page=main
NetFlow	http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html