Preface

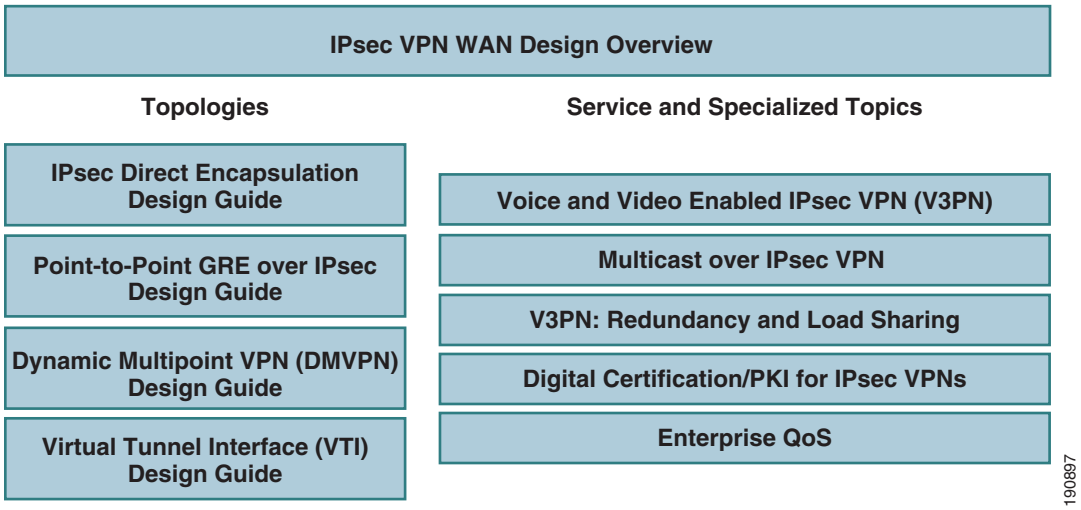
This design guide defines the comprehensive functional components required to build a site-to-site virtual private network (VPN) system in the context of enterprise wide area network (WAN) connectivity. This design guide covers the design topology of dynamic multipoint VPN (DMVPN).

This guide is part of an ongoing series that addresses VPN solutions, using the latest VPN technologies from Cisco, and based on practical design principles that have been tested to scale.

Introduction

Figure 1 lists the documents for the IP Security (IPsec) VPN WAN architecture, which are available at the following URL: http://www.cisco.com/en/US/netsol/ns817/networking_solutions_program_home.html.

Figure 1 IPsec VPN WAN Architecture Documents



The IPsec VPN WAN architecture is divided into multiple design guides based on technologies, each of which uses IPsec. The reader must have a basic understanding of IPsec before reading further. The *IPsec VPN WAN Design Overview* outlines the criteria for selecting a specific IPsec VPN WAN technology. This document should be used to select the correct technology for the proposed network design.

This document serves as a design guide for those intending to deploy the Cisco DMVPN technology. This version of the design guide focuses on Cisco IOS VPN router products.

This design guide begins with an overview, followed by design recommendations, as well as product selection and performance information. Finally, configuration examples are presented.

Audience

This design guide provides guidelines and best practices to systems engineers for customer deployments.

Updates to Version 1.1

Version 1.1 of this document provides hub-and-spoke scalability test results for Cisco ASR 1000.

Scope of Work

This version of the design guide addresses the following applications of the solution:

- Cisco VPN routers running Internetwork Operating System (IOS)
- Multipoint GRE (mGRE) and point-to-point (p2p) GRE tunneling over IPsec are the tunneling methods
- Site-to-site VPN topologies
- Use of Enhanced Interior Gateway Routing Protocol (EIGRP) as a routing protocol across the VPN with mGRE configurations
- Dynamic crypto peer address with static GRE endpoints
- Next Hop Routing Protocol (NHRP)
- Tunnel Protection mode
- Converged data and VoIP traffic requirements
- Quality of service (QoS) features are enabled
- Evaluation of Cisco VPN product performance in scalable and resilient designs

Document Objectives

This design guide addresses the following applications of the technology:

- DMVPN used in hub-and-spoke designs
- DMVPN used in spoke-to-spoke designs

Scalability test results of these designs with devices under load, taken from Cisco testing, are presented for design guidance.

Document Organization

This guide contains the chapters in the following table.

Section	Description
Chapter 1, “DMVPN Design Overview.”	Provides an overview of the DMVPN design topology and characteristics.
Chapter 2, “DMVPN Design and Implementation.”	Provides an overview of some general design considerations, followed by sections on implementation, high availability, QoS, and multicast.
Chapter 3, “Scalability Considerations.”	Provides guidance in selecting Cisco products for a VPN solution, including sizing the headend, choosing Cisco products that can be deployed for headend devices, and product sizing and selection information for branch devices.
Chapter 4, “Scalability Test Results (Unicast Only).”	Provides Cisco test results to provide design guidance on the scalability of various platforms in DMVPN configurations.
Appendix A “Scalability Test Bed Configuration Files.”	Provides the configurations for the central and branch sites.
Appendix B “Legacy Product Test Results.”	Provides scalability test results for legacy products.
Appendix C “Acronyms.”	Provides definitions for acronyms.