Preface

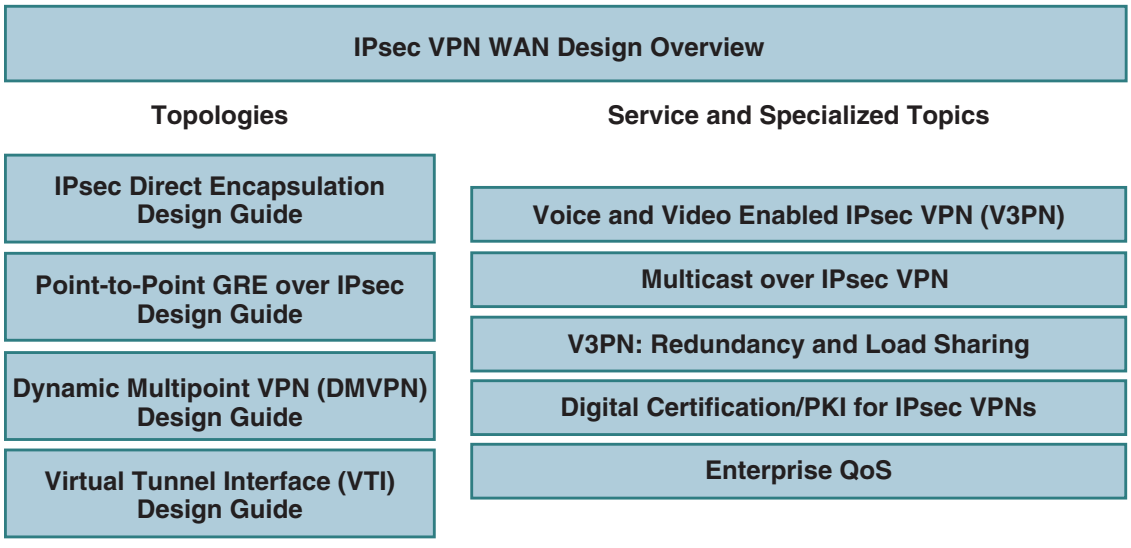
This design guide defines the comprehensive functional components required to build a site-to-site virtual private network (VPN) system in the context of enterprise wide area network (WAN) connectivity. This design guide covers the design topology of point-to-point (p2p) Generic Route Encapsulation (GRE) over IP Security (IPsec).

This design 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 IPsec VPN WAN architecture documentation.

Figure 1 IPsec VPN WAN Architecture Documentation



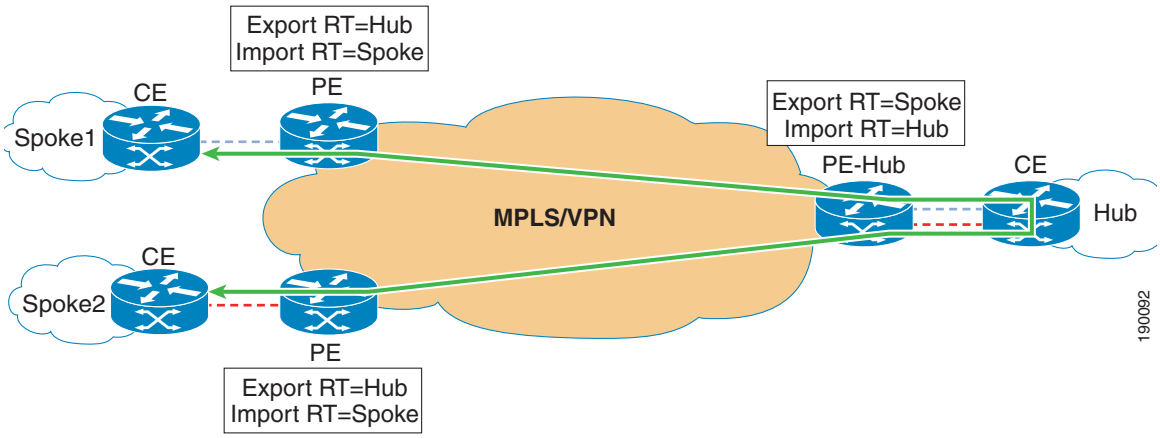
The IPsec VPN WAN architecture is divided into multiple design guides based on technologies. These guides are available at the following URL: http://www.cisco.com/en/US/netsol/ns742/networking_solutions_program_category_home.html.

Each technology uses IPsec as the underlying transport mechanism for each VPN. The operation of IPsec is outlined in the *IPsec VPN WAN Design Overview*. The reader must have a basic understanding of IPsec before reading further. The *IPsec VPN WAN Design Overview* also 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 a site-to-site VPN based on IPsec and GRE. This version of the design guide focuses on Cisco IOS VPN router products.

The primary topology discussed is a hub-and-spoke design, where the primary enterprise resources are located in a large central site, with a number of smaller sites or branch offices connected directly to the central site over a VPN. A high-level diagram of this topology is shown in Figure 2.

Figure 2 Hub-and-Spoke VPN



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

Target Audience

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

Scope of Work

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

- Cisco VPN routers running IOS
- p2p GRE tunneling over IPsec is the tunneling method
- Site-to-site VPN topologies

- Use of Enhanced Interior Gateway Routing Protocol (EIGRP) as a routing protocol across the VPN with GRE configurations
- Dynamic crypto peer address with static GRE endpoints
- Dead Peer Detection (DPD)
- Converged data and voice over IP (VoIP) traffic requirements
- Quality of service (QoS) features are enabled
- Evaluation of Cisco VPN product performance in scalable and resilient designs

Document Organization

This guide contains the chapters in the following table.

Section	Description
Chapter 1, "Point-to-Point GRE over IPsec Design Overview."	Provides an overview of the VPN site-to-site design topology and characteristics.
Chapter 2, "Point-to-Point GRE over IPsec Design and Implementation."	Provides an overview of some general design considerations that need to be factored into the design, followed by sections on implementation, high availability, QoS, and IP 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 test results from the Cisco test lab to provide design guidance on the scalability of various platforms in p2p GRE over IPsec VPN configurations.
Chapter 5, "Case Studies."	Provides two case studies as reference material for implementing p2p GRE over IPsec designs.
Appendix A "Scalability Test Bed Configuration Files."	Provides the configurations for the central and branch sites.
Appendix B "Legacy Platform Test Results."	Provides scalability test results for legacy products.
Appendix C "References and Reading."	Provides references to further documentation.
Appendix D "Acronyms."	Provides definitions for acronyms.