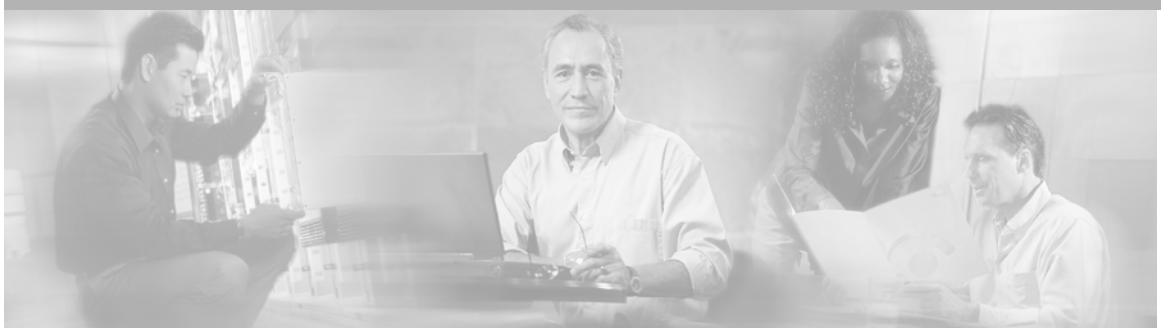


Data-only Site-to-Site IPSec VPN Design Guide

OL-7281-01
Version 1.0

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Data-only Site-to-Site IPSec VPN Design Guide

VPN Site-to-Site Solution Overview

This chapter includes the following sections:

Introduction

This design guide defines the comprehensive functional components required to build a site-to-site enterprise virtual private network (VPN) solution. The individual hardware requirements and their interconnections, software features, management needs, and partner dependencies are described, to provide for a customer-deployable, manageable, and maintainable site-to-site enterprise VPN solution.

This document focuses on Cisco IOS VPN router products and serves as a design guide for those intending to deploy a site-to-site VPN based on IP Security (IPSec).

The designs described in this guide are based on the SAFE VPN architecture. Additional information on how to deploy SAFE VPN is provided.

Note The reader should first be familiar with the *SAFE VPN White Paper*. Cisco SAFE documentation can be found at the following URL: http://www.cisco.com/go/safe.

This design guide provides an overview of three different VPN solutions, followed by design recommendations as well as product selection and performance information. Finally, configuration examples and a case study are presented.

The following three solutions are described:

- Solution One—IPSec in combination with Generic Routing Encapsulation (GRE)
- Solution Two—Dynamic Multipoint VPN (DMVPN)
- Solution Three—IPSec as the solitary tunneling method with Dead Peer Detection (DPD), Reverse Route Injection (RRI), and Hot Standby Router Protocol (HSRP) for failover

All three of these solutions share the following characteristics:

- Site-to-site VPN topologies
- Cisco VPN routers running Cisco Internetwork Operating System (IOS)

- Use of Enhanced Interior Gateway Routing Protocol (EIGRP) as a routing protocol across the VPN with GRE configurations
- Data as the primary traffic component
- No quality of service (QoS) features enabled
- Evaluation of Cisco VPN product performance in scalable and resilient designs

Note Information on related VPN topics can be found at the following URL: http://www.cisco.com/go/srnd

VPN Site-to-Site Design Overview

This section provides an overview of the VPN site-to-site design, and includes the following topics:

Starting Assumptions

The design approach presented in this design guide makes several starting assumptions:

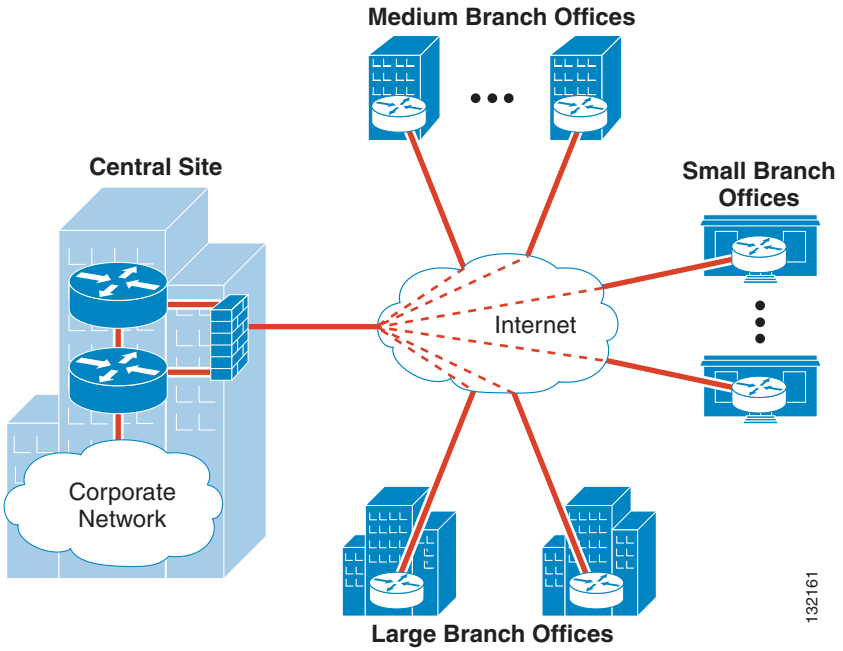
- The design supports a typical data traffic profile for customers (see Scalability Testing Methodology, page 3-1 for more detail on the traffic profile used during scalability testing). Later testing includes multi-service traffic in addition to the typical data traffic profile (see Subsequent Testing, page 3-2 for more information.)
- High availability and resiliency after failover are critically important; therefore, the recommendations in this design guide reflect the benefits of built-in redundancy and failover with fast convergence. This is discussed further in Chapter 3, "Selecting Solution Components."
- It is assumed that the customer has a need for diverse traffic requirements, such as IP multicast, multi-protocol, and support for routing. The use of GRE and a routing protocol are also discussed in more detail in Solution One (IPSec with GRE)—Design Recommendations, page 2-7 and Solution Two (DMVPN)—Design Recommendations, page 2-13.
- An additional design is presented in Solution Three (IPSec with DPD, RRI, and HSRP)—Design Recommendations, page 2-20. This design utilizes IPSec alone as the sole tunneling method. The "elimination" of GRE as an additional tunneling protocol reduces the encrypted packet size by an average of 24 bytes. This configuration proves useful for many enterprises that do not require support for a routing protocol passing through the tunnel, multi-cast traffic, or multi-protocol traffic.
- Cisco products should be maintained at reasonable CPU utilization levels. This is discussed in more detail in Chapter 3, "Selecting Solution Components," including recommendations for both head-end and branch-end devices, and software revisions.
- Although costs were certainly considered, the design recommendations assume that the customer will deploy current VPN technologies, including hardware-accelerated encryption.

- Voice over IP (VoIP), video, and other latency-sensitive traffic is not addressed in this design guide. Considerations for handling multi-service and other latency-sensitive applications may be found in the *Voice and Video Enabled IPSec VPN (V3PN) Design Guide* at the following URL: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79c.pdf
- Finally, this design is targeted for deployment by enterprise-owned VPNs; however, the concepts and conclusions are valid regardless of the ownership of the edge tunneling equipment, and are therefore valuable for service provider-managed VPNs as well.

Design Topology

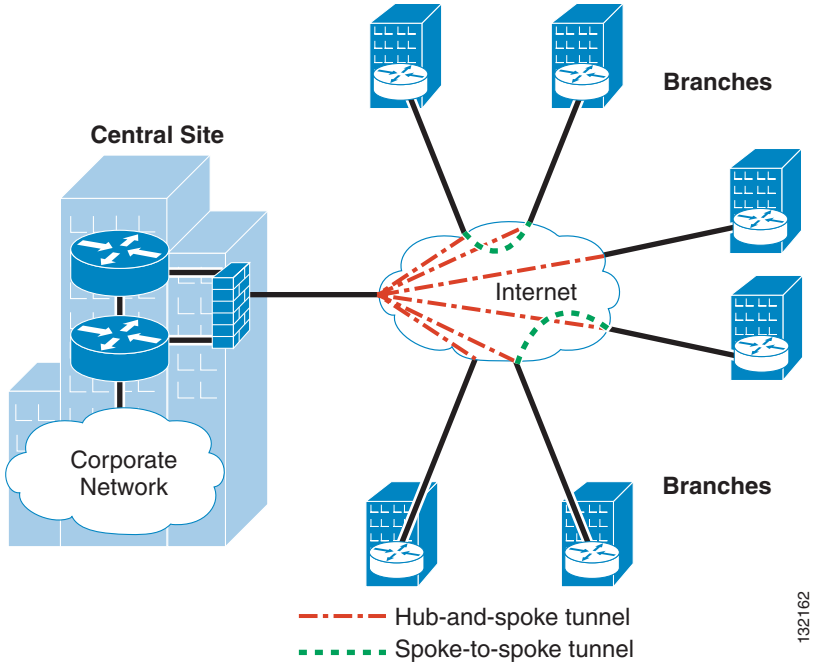
The primary topology discussed is a hub-and-spoke deployment model, where the primary enterprise resources are located in a large central site and multiple smaller sites or branch offices are connected directly to the central site over a VPN, as shown in Figure 1-1.

Figure 1-1 Hub-and-Spoke VPN



The introduction of DMVPN makes a design with hub-and-spoke connections possible, and provides the ability to create temporary connections between spoke sites using IPSec encryption. This topology is shown in Figure 1-2.

Figure 1-2 Spoke-to-Spoke VPN



Site-to-Site VPN Design Components

VPN applications include extending the reachability of an enterprise WAN and replacing classic WAN technologies such as leased lines, Frame Relay, and ATM. Site-to-site VPNs are primarily deployed to connect branch office locations to the central site (or sites) of an enterprise.

The requirements of enterprise customers for traditional private WAN services, such as multi-protocol support, high availability, scalability, and security, are also requirements for VPNs. VPNs can often meet these requirements more cost-effectively and with greater flexibility than private WAN services.

The key components of this site-to-site VPN design are the following:

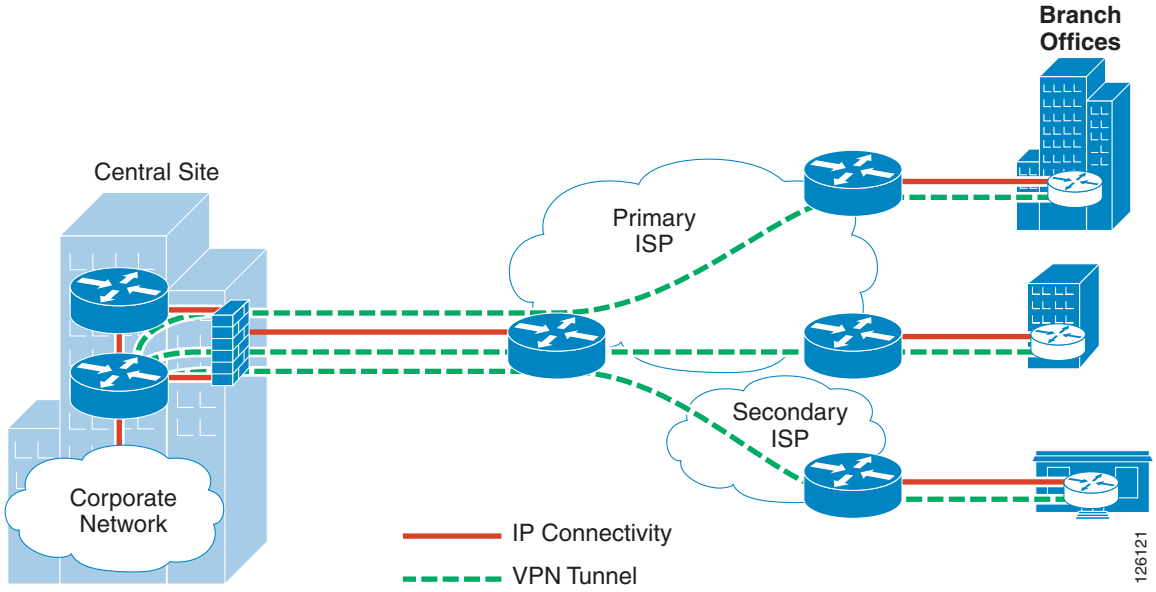
- Cisco high-end VPN routers serving as VPN head-end termination devices at a central campus (head-end devices)
- Cisco VPN access routers serving as VPN branch-end termination devices at branch office locations (branch-end devices)
- One of the following:
  - Solution One—IPSec/GRE tunnels that interconnect the head-end and branch-end devices in the VPN
  - Solution Two—IPSec/GRE tunnels created by DMVPN that interconnect the head-end and branch-end devices and allow dynamic spoke-to-spoke tunnels between branch-end devices in the VPN
  - Solution Three—IPSec tunnels with Dead Peer Detection (DPD), Reverse Route Injection (RRI), and Hot Standby Router Protocol (HSRP) to perform the head-end to branch-end interconnection
- Internet services procured from a third-party ISP (or ISPs) serving as the WAN interconnection medium

Cisco VPN routers are a good choice for site-to-site VPN deployments because they can accommodate any network requirement inherited from a Frame Relay or private line network, such as support for multicast and latency-sensitive traffic, routing for resiliency, and support for non-IP protocols such as Internetwork Packet Exchange (IPX) or Systems Network Architecture (SNA).

Note See Chapter 3, "Selecting Solution Components," for a discussion on selecting head-end and branch-end products.

The network topology of the hub-and-spoke design is shown in Figure 1-3.

Figure 1-3 VPN Hub-and-Spoke Solution Network Topology



This solution is a hub-and-spoke network with multiple head-end devices for redundancy. Head ends are high-end tunnel aggregation routers servicing multiple IPSec or IPSec/GRE tunnels for a prescribed number of branch office locations. In addition to terminating the VPN tunnels at the central site, head ends act as the distribution point for all routing information to and from branch-end devices if a routing protocol has been configured. In DMVPN deployments, head-end devices also act as Next Hop Resolution Protocol (NHRP) caching devices, and next hop servers for the branch-end devices.

Branch ends are typically access routers that provide IPSec or IPSec/GRE tunnels from the branch office locations to the central site. In addition to terminating the VPN tunnels, the branch end often provides WAN access and in some implementations may serve as a firewall.

To ensure authentication and encryption, IPSec tunnels are provisioned to interconnect branch offices to the central site.

Note See IPSec Overview, page 1-10 for a more detailed discussion of IPSec.

Network resiliency is provided differently depending on the initial network requirements. Solution One implements a routing protocol across the VPN. Because IPSec does not provide the ability to run protocols requiring IP multicast (such as EIGRP), IPSec must be used together with GRE. GRE also

provides the ability for the customer to support more diverse traffic across the VPN, including IP multicast and non-IP protocols. (See Solution One (IPSec with GRE)—Design Recommendations, page 2-7 for more information on the need for and benefits of GRE.)

For high availability in the case of a failure, each branch-end access router should have a primary and secondary IPSec/GRE tunnel provisioned to two different head-end tunnel aggregation routers. Solution Two uses a routing protocol with redundant head-end tunnel aggregation routers, but employs DMVPN (with the mGRE tunnel feature) to support tunnel creation and NHRP to discover the Non-Broadcast Multiple Access (NBMA) addresses of other devices for which an on-demand encrypted connection is required. DMVPN supports IP unicast and multicast but does not support non-IP protocols. (See Solution Two (DMVPN)—Design Recommendations, page 2-13 for a discussion of this design implementation.)

Solution Three uses IPSec as the sole tunneling method, with DPD for peer state detection, RRI for optimal packet routing from the head end to the remotes, and HSRP for resiliency. (See Solution Three (IPSec with DPD, RRI, and HSRP)—Design Recommendations, page 2-20 for a discussion on how to distribute and aggregate these tunnels.)

There are currently several service provider options available to enterprise customers for deploying a VPN, including the enterprise owning and managing the VPN, and needing only Internet service from ISPs. Optionally, an enterprise might consider outsourcing their VPN to the service provider. The architecture and recommendations provided in this design guide are generally valid for either VPN deployment option, differing only in the ownership of the edge VPN equipment.

This design guide supports a wide variety of alternatives for deploying a flexible VPN solution that will respond to changing customer requirements. However, the scale of deployment affects decisions on which products are used and the challenges of configuring them.

Cisco VPN Product Overview

The implementation presented in this guide is focused on using Cisco VPN router products in IPSec-based VPN applications. Table 1-1 provides a summary of the recommended deployment of Cisco VPN router product families to the different head end and branch office applications.

Table 1-1 Cisco VPN Product Applications Summary

Application	Cisco VPN Router Family	VPN Acceleration Options	VPN Performance (based on Cisco scalability tests) [1]
Central head end site	6500	VPNSM	Up to 1.1 Gbps
	7200	ISM (single or dual), VAM	Up to 66 Mbps
	7100	ISA (single or dual), VAM	Up to 30 Mbps
	3700	AIM (Base, Medium, High Perform)	Up to 16 Mbps
	PIX535	VAC+	Up to 167 Mbps
	3080	SEP-E	Up to 39.4 Mbps
Large branch office	3845	Hardware included	Up to 29 Mbps
	3845	AIM HPII	Up to 36 Mbps
	3825	Hardware included	Up to 22 Mbps
	3825	AIM HPII	Up to 27 Mbps
	3700	AIM HPII	Up to 35 Mbps
	3600	AIM (Base, Medium, High Perform)	Up to 15 Mbps
	2600	AIM (Base, Extended Perform)	Up to 10 Mbps
Medium branch office	2800	Hardware included	Up to 14 Mbps
	2800	AIM HPII	Up to 18 Mbps
	3600	AIM (Base, Medium, High Perform)	Up to 15 Mbps
	2600	AIM (Base, Extended Perform)	Up to 10 Mbps
	1800	Hardware included	Up to 3.5 Mbps
	1800	AIM HPII	Up to 5 Mbps
	1700	VPN Module	Up to 2.5 Mbps
Small office	1800	Hardware included	Up to 3.5 Mbps
	1800	AIM HPII	Up to 5 Mbps
	1700	VPN Module	Up to 2.5 Mbps
	800	Hardware included	Up to 900 kbps

1. The VPN performance typically listed is for large packets only and full CPU utilization. However, in the Cisco scalability test configuration with a packet mix and not exceeding 50 percent CPU utilization for head ends and 65 percent for branch offices, the performance is as listed here.

Note Results shown for the Cisco PIX and the Cisco VPN 3000 Concentrator are valid only in Solution Three designs (IPSec with DPD, RRI, and HSRP), because these devices are not capable of GRE-encapsulated tunnels.

Solution Benefits

Each solution design offers a number of advantages over competing approaches to deploying site-to-site VPNs. The primary benefits of deploying the solutions described in this guide include the following:

- Security
  - Traffic between branch offices or between the branch office and the central site is encrypted using Triple Data Encryption Standard (3DES).
  - Traffic between branch offices or between branch offices and the central site is authenticated with Secure Hash Algorithm (SHA)-1.
- High Availability
  - A dynamic routing protocol (EIGRP) can be used to manage network routing and provide fast convergence.
  - HSRP provides redundancy during a failure.
  - A level of redundancy is provided at the head end such that the design can tolerate a complete failure of a head end and recover quickly.
- Scalability
  - A building-block approach to scalability is used such that the design can support thousands of branch-offices, limited only by the number of head-end devices deployed.
  - Verified performance aggregating up to 500 branch offices (1000 tunnels) to each head end.
  - Although IPSec packet fragmentation can significantly reduce VPN throughput performance, there are features in Cisco IOS to somewhat mitigate this problem.
- Flexibility
  - Cisco VPN router product line allows customization of head end and branch office routers.
  - Either hardware-accelerated or software-supported encryption can be deployed. Use of hardware-accelerated encryption is highly recommended.
  - With GRE, it is possible to build a VPN network that can handle diverse network traffic requirements, such as multicast, multi-protocol, and support for routing.

Note Enabling QoS across the VPN for support of latency-sensitive traffic, such as Voice over IP and Video, is covered in a separate design guide available at the following URL: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79c.pdf

- Reducing Costs
  - Many VPN services offer the enterprise some level of cost reduction.

Three Solutions—Overview and Recommendations

This section presents a brief overview of the three solutions described in this guide, along with deployment recommendations. These solutions are described in more detail in the subsequent sections.

Solution One—IPSec with GRE

The following are high-level recommendations for Solution One (IPSec with GRE deployment supporting multi-protocol and/or multicast traffic including routing protocols):

- Use IPSec in tunnel mode with 3DES for encryption of transported data.
- Use GRE for transport of multi-protocol or multicast data across the VPN.
- Configure two tunnels between each remote to different redundant head-end routers for failover and resiliency.
- Configure a routing protocol with route summarization for dynamic routing.
- Implement path MTU discovery (PMTUD) to limit packet fragmentation.

Solution Two—DMVPN

The following are high-level recommendations for Solution Two (DMVPN deployment supporting IP unicast and/or multicast traffic including routing protocols):

- Use IPSec in transport mode with DMVPN, using 3DES for encryption of transported data.
- Use GRE, via DMVPN mGRE implementation, for transport of IP unicast or multicast data across the VPN.
- Configure two tunnels between each remote to different redundant head-end routers for failover and resiliency.
- Configure a routing protocol with route summarization for dynamic routing.
- Implement PMTUD to limit packet fragmentation.

Solution Three—IPSec with DPD, RRI, and HSRP

The following are high-level recommendations for Solution Three (IPSec deployment with DPD, RRI, and HSRP for unicast IP traffic only):

- Use IPSec in tunnel mode with 3DES for encryption of transported data.
- Use DPD for IPSec peer state feedback.
- Use RRI for optimal routing from the campus to the remote sites.
- Configure dynamic crypto maps to ensure optimal routing and simplify configurations on head-end routers.
- Use HSRP for redundancy and failover.

The following is a limitation with Solution Three:

- The IPSec tunnel must be initiated via the remote branch. When dynamic tunnels are configured, the head-end devices do not have the necessary information to initiate an IPSec connection.

Note See Solution Three Limitation—Tunnel Initiation Not Possible from Head Ends, page 2-22 for more information.

IPSec Overview

This section introduces IPSec and its application in VPNs, and includes the following topics:

Note For a more in-depth understanding of IPSec, see the *SAFE VPN White Paper*. Cisco SAFE documentation can be found at the following URL: http://www.cisco.com/go/safe.

Introduction to IPSec

The IPSec standard provides a method to manage authentication and data protection between multiple peers engaging in secure data transfer. IPSec includes the protocol ISAKMP/Oakley and two IPSec IP protocols, Encapsulating Security Protocol (ESP) and Authentication Header (AH).

IPSec uses symmetrical encryption algorithms for data protection. Symmetrical encryption transforms are more efficient and are easier to implement in hardware. These algorithms need a secure method of key exchange to ensure data protection. Internet Key Exchange (IKE) ISAKMP/Oakley protocols provide that capability.

This solution requires a standards-based way to secure data from eavesdropping and modification. IPSec provides such a method. IPSec has a choice of transform sets so that users may choose the strength of their data protection. IPSec also has several hash methods to choose from, each giving different levels of protection.

Tunneling Protocols

You can use several tunneling protocols, which vary in the features they support, the problems they are designed to solve, and the amount of security they provide to the data being transported. The designs presented in this paper focus on the use of IPSec as a tunneling protocol alone and IPSec used in conjunction with GRE tunnels.

When used alone, IPSec can provide a private, resilient network when support for multicast, routing protocols, or non-IP protocols is not required. When support for one or more of these features is required, IPSec should be used in conjunction with GRE. Neither of these two tunnel protocols by themselves have the necessary features to provide privacy and the ability to support multi-protocols, but the combination of IPSec and GRE achieves both functions.

Note Other tunneling protocols include Point-to-Point Tunneling Protocol (PPTP) and Layer Two Protocol (L2TP). Both of these are based in user- or client-to-concentrator networks, commonly called remote access solutions, and are not used in the solutions described in this design guide.

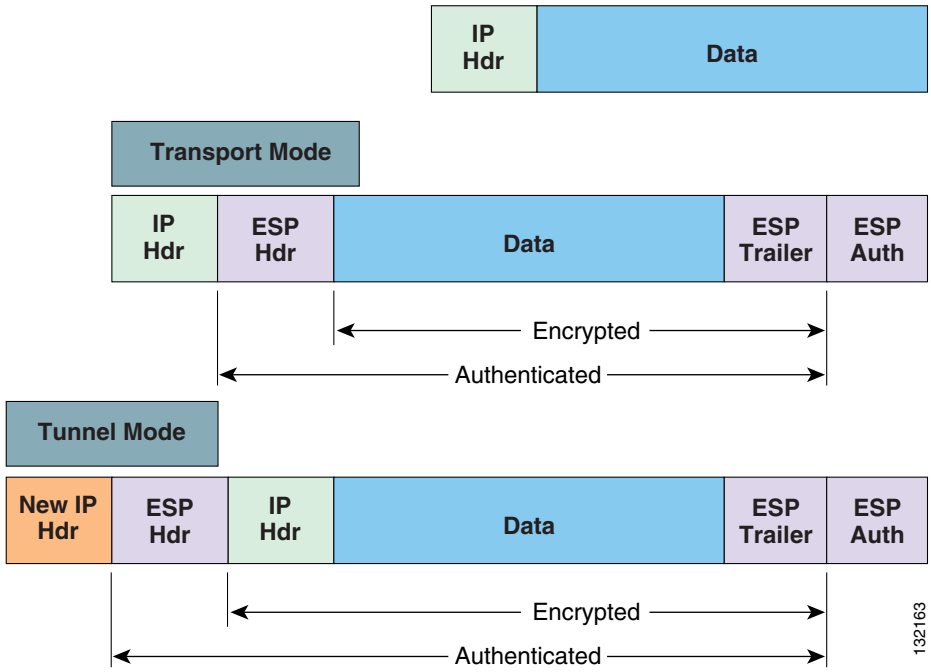
IPSec Protocols

The two IP protocols used in the IPSec standard are ESP and AH. These are discussed in more detail in the next two sections.

Encapsulating Security Protocol

The ESP header (IP protocol 50) forms the core of the IPSec protocol. This protocol, in conjunction with an agreed-upon encryption method or transform set, protects data by rendering it undecipherable. This protocol protects only the data portion of the packet. It can optionally also provide for authentication of the protected data. Figure 1-4 shows how ESP encapsulates an IP packet.

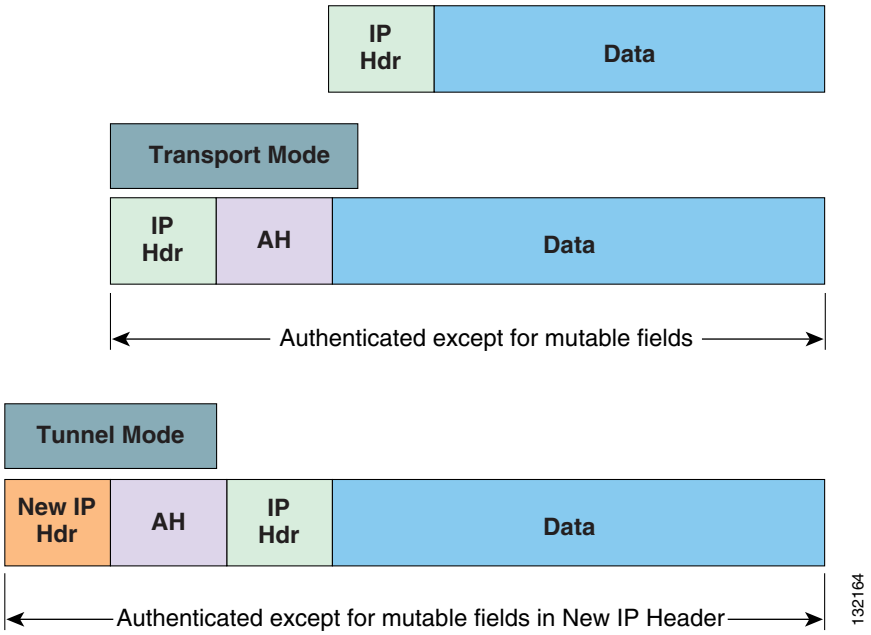
Figure 1-4 Encapsulating Security Protocol (ESP)



Authentication Header

The other part of IPSec is formed by the AH protocol (IP protocol 51). The AH does not protect data in the usual sense by hiding the data, but it adds a tamper-evident seal to the data. It also protects the non-mutable fields in the IP header carrying the data. This includes the address fields of the IP header. The AH protocol should not be used alone when there is a requirement for data confidentiality. Figure 1-5 shows how AH encapsulates an IP packet.

Figure 1-5 Authentication Header (AH)



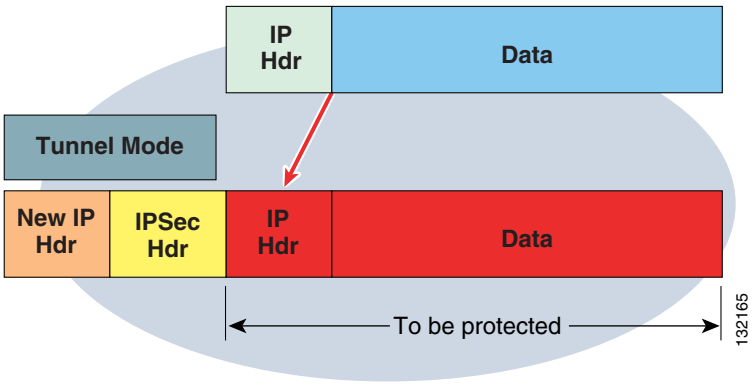
IPSec Modes

IPSec has two methods of forwarding data across a network: transport mode and tunnel mode, which differ in their application as well as in the amount of overhead added to the passenger packet. These modes are described in more detail in the next two sections.

Tunnel Mode

Tunnel mode works by encapsulating and protecting an entire IP packet. Because tunnel mode encapsulates or hides the IP header of the packet, a new IP header must be added for the packet to be successfully forwarded. The encrypting devices themselves own the IP addresses used in this new header. These addresses can be specified in the configuration in Cisco IOS routers. Tunnel mode may be employed with either or both ESP and AH. Tunnel mode results in an additional packet expansion of approximately 20 bytes because of the new IP header. Tunnel mode expansion of the IP packet is shown in Figure 1-6.

Figure 1-6 IPSec Tunnel Mode



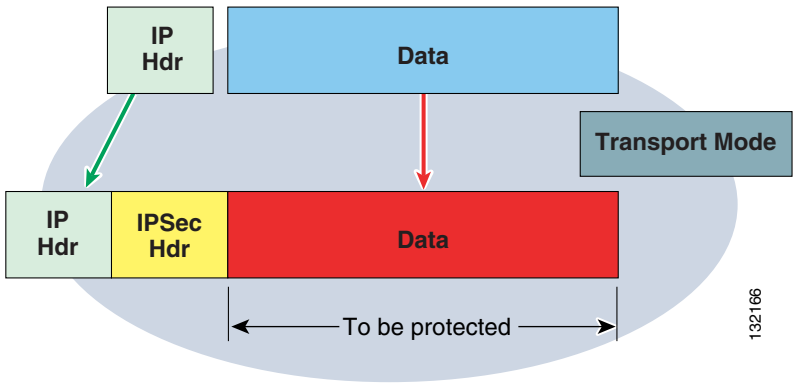
Transport Mode

Because packet expansion can be a concern during the forwarding of small packets, a second forwarding method is also possible. IPSec transport mode works by inserting the ESP header in between the IP header and the next protocol or the Transport layer of the packet.

Both IP addresses of the two network nodes whose traffic is being protected by IPSec are visible. This mode of IPSec can sometimes be susceptible to traffic analysis. However, because there is no additional IP header added, it results in less packet expansion. Transport mode can be deployed with either or both ESP and AH. This mode works well with GRE because GRE already hides the addresses of the end stations by adding its own IP header. Transport mode is the optimum choice for the tunnel protection method used by DMVPN.

Transport mode expansion of the IP packet is shown in Figure 1-7.

Figure 1-7 IPSec Transport Mode



Internet Key Exchange

To implement a VPN solution with encryption, the periodic changing of encryption keys is necessary. Failure to change these keys makes the network susceptible to brute force attacks. IPSec solves this problem with the IKE protocol, which uses two other protocols to authenticate a peer and generate keys.

This protocol uses a mathematical routine called a Diffie-Helman exchange to generate symmetrical keys to be used by two IPSec peers. IKE also manages the negotiation of other security parameters such as the data to be protected, the strength of the keys, the hash methods used, and whether the packets are protected from replay. IKE uses UDP port 500.

Security Association

A Security Association (SA) is an agreement between two peers engaging in an IPSec exchange. This agreement includes items such as the type and strength of the encryption used to protect the data, and it also includes the method and strength of the data authentication (if any) and the method of creating new keys for that data protection. SAs are performed in two phases, as described in the two sections that follow.

IKE Phase One

Phase one is the initial negotiation of SAs between two IPSec peers. Phase one can optionally also include an authentication in which each peer is able to verify the identity of the other. This conversation between two IPSec peers can be subject to eavesdropping with no significant vulnerability of the keys being recovered. Phase one SAs are bidirectional; data may be sent and received using the same key material generated.

Phase one has two possible authentication methods: pre-shared keys or RSA signatures/digital certificates. Configuration examples in this guide use pre-shared keys.

IKE Phase Two

Phase two SAs are negotiated by the IKE process (ISAKMP) on behalf of other services such as IPSec, which need key material for operation. Because the SAs used by IPSec are unidirectional, a separate key exchange is needed for data flowing in the forward direction from the reverse direction. This doubles the amount of work an eavesdropper needs to do to successfully recover both sides of a conversation. The two peers have already agreed upon the transform sets, hash methods, and other parameters during the phase one negotiation. Quick mode is the method used for the phase two SA negotiations.

IKE Authentication

There are two primary methods of configuring the VPN such that the VPN devices can authenticate with their peer: pre-shared keys and digital certificates. These are discussed in the following sections.

Pre-shared Keys

The pre-shared keys method involves advance configuration using a set of keys known to both of the peer VPN devices.

As the number of IPSec devices in the VPN grows, scalability becomes an issue because a separate key needs to be maintained for each IPSec peer. Replacement of a device in the network can also lead to compromise of the keys in use at the time.

The scalability testing performed for this guide uses the pre-shared keys method of authentication.

Digital Certificates

An alternative to the pre-shared keys method is to implement the use of digital signatures contained in digital certificates. Digital signatures make use of a trusted third party, known as a certificate authority (CA), to digitally sign the public key portion of the encrypted nonce.

Included with the signature are a name, serial number, validity period, and other information that an IPSec device can use to determine the validity of the certificate. Certificates can also be revoked, denying the IPSec device the ability to successfully authenticate.

For more information, see the Tech Tips on CCO:

- All URLs are listed on the TSP for IPSEC at the following URL: http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Technologies:IPSec&s=Implementation_and_Configuration
- Backup and restore options for your Cisco IOS CA Server— http://www.cisco.com/en/US/partner/tech/tk583/tk372/technologies_tech_note09186a008021ac26.shtml
- Ceritificate Expiration and Auto-Enroll (Automatic Re-Enrollment) Feature FAQ— http://www.cisco.com/en/US/partner/tech/tk583/tk372/technologies_q_and_a_item09186a00802149a8.shtml
- Certificate revocation list distribution over SCEP configuration example— http://www.cisco.com/en/US/partner/tech/tk583/tk372/technologies_configuration_example09186a008021bc55.shtml
- Certificate revocation list distribution over SCEP FAQ— http://www.cisco.com/en/US/partner/tech/tk583/tk372/technologies_q_and_a_item09186a008021bc50.shtml
- Cut-n-paste style certificate enrollment to a Cisco IOS CA configuration example— http://www.cisco.com/en/US/partner/tech/tk583/tk372/technologies_configuration_example09186a008021568b.shtml
- Enrollment over SCEP to a Cisco IOS CA (Headend Aggregrator VPN Router) configuration example— http://www.cisco.com/en/US/partner/tech/tk583/tk372/technologies_configuration_example09186a0080215686.shtml

Selecting a Site-to-Site VPN Solution

In designing a VPN deployment for a customer, it is essential to integrate broader design considerations such as high availability and resiliency, security, and potentially QoS.

This chapter starts with an overview of some general design considerations that must be factored into the design. This is followed by the requirements and prerequisites for each of the three solutions, as well as additional detailed sections on these solutions as required.

This chapter includes the following topics:

Types of Site-to-Site VPN Deployments

Several general factors must be considered before selecting a customer VPN solution. The following general factors should be considered when making a decision as to the type of site-to-site IPSec VPN to deploy:

- Network Profile
  - What applications does the customer expect to run over the VPN?

    The recommendations in this design guide focus on data applications. Multi-service applications such as voice or video over IP require additional design considerations, such as QoS. These requirements are covered in the *Voice and Video Enabled IPSec VPN (V3PN) Design Guide* at the following URL: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79c.pdf
  - Is multicast and/or multi-protocol support required?

    IPSec supports only tunneling of unicast IP traffic. Multicast IP is required to run a routing protocol across the VPN and to support applications such as video. GRE can be used in conjunction with IPSec to support multicast, multi-protocol traffic, and routing protocols.

  - How much packet fragmentation does the customer expect on their network?

    The VPN design needs to consider the amount of fragmentation that may occur, to minimize the performance impacts at the head end.

  - Are there requirements for dynamic spoke-to-spoke connections?

    Hub-and-spoke is a popular model inherited from traditional WANs. Some customers have legitimate needs for a design that includes spoke-to-spoke connectivity.

  - Are the NBMA (Non-Broadcast Multiple Access) addresses statically assigned at all locations, or do some branch sites receive these addresses via DHCP?

    When addresses are assigned via Dynamic Host Configuration Protocol (DHCP), certain aspects of router configuration at the host are simplified greatly by the DMVPN use of NHRP to cache NBMA addresses.

- Scalability
  - How many branches does the customer expect to aggregate to each central site?

    The number of branch offices, plus the amount of traffic expected from each branch, determines how many head-end aggregation devices are required. Improper aggregation can result in a VPN with unacceptable performance.

  - What is the expected traffic throughput between branch offices and the central site?

    The traffic throughput to and from branches has a direct impact on the number of branches that should be aggregated by a head-end device. If not properly considered, the resulting VPN design may have unacceptable performance.

- Resiliency
  - What are the customer expectations for resiliency?

    As in the case of a typical enterprise network, a VPN must be resilient to recover in the event of a failure. The designs discussed in this guide assume that a customer requires redundancy at the central site allowing for complete failure of a head-end device.

  - Is failover time or post-failure convergence time a concern?

    VoIP applications may have a much more stringent requirement for convergence times as compared to simple data applications. These solutions can be tuned somewhat to lower convergence times at a cost of router CPU utilization.

- Security
  - What type of IKE authentication method will be implemented?

    Different methods of IKE authentication necessitate different levels of implementation complexity. For example, configuring pre-shared keys is the least complex method; however, scalability may be an issue. Similarly, use of certificates is highly scalable, yet they are more complex to deploy.

- Services
  - What other services will run on the device?

    VPNs can be deployed with dedicated function devices or as multiple function devices, providing WAN access, firewall, and VPN services.

Note This design guide provides only general design considerations. Each customer network may require customization because of customer-specific requirements.

Solution Design Requirements

This section includes the following topics:

Network Requirements

Choosing which of the three solutions described in this guide to implement depends on network requirements such as the following:

- Is there a requirement for protocols other than unicast IP alone, or will this requirement exist at any time in the future? If so, the deployment should include an additional tunneling protocol; GRE should be used in this solution, even at the expense of creating additional CPU overhead and packet expansion.
- Is there a requirement for spoke-to-spoke tunnels, but no requirement for non-IP protocols? Do the majority of the branch sites receive their IP addresses via DHCP? If so, then the DMVPN version of GRE plus NHRP may be the best choice.

Consider this decision carefully because it may be difficult and time-consuming to change the deployment later. When no further requirements for either multicast or non-IP protocols require additional encapsulation methods such as GRE, the network implementer may opt to configure IPSec High Availability (HA). This solution utilizes IPSec as the sole tunneling method. This configuration utilizes DPD for peer state feedback, RRI for optimal routing from the campus network to the remotes, and HSRP for head end resilience. This solution is more conservative with router CPU resources than the IPSec with GRE solution.

The following recommendations are applicable to all three solutions. These good network design practices apply to these solutions as well as to networks in general.

- Designing the VPN
  - Minimize packet fragmentation. Keep IPSec packet fragmentation to a minimum on the customer network.
  - Deploy hardware encryption acceleration wherever possible, minimizing router CPU overhead.
  - Configure 3DES encryption where permitted (some exports of 3DES may be prohibited by law).
  - Configure IPSec authentication.
  - Consider the interactions of IPSec with other networking functions.

Note See IPSec Interactions with Other Networking Functions, page 2-27 for additional information.

- Selecting Cisco VPN products
  - Select Cisco VPN router products at the head end based on the following:
    - Number of tunnels aggregated up to 500 tunnels per head end

    - Throughput aggregated up to the maximum recommendations for each product
    - Maintaining CPU utilization below 50 percent
  - Calculate the number of head-end devices based on total tunnel and throughput aggregation requirements, as well as to handle failover. See Sizing the Head End, page 3-6 for additional information.
  - Select Cisco VPN router products at the branch offices based on the following:
    - Throughput aggregated up to the maximum recommendations for each product
    - Maintaining CPU utilization below 65 percent

Note See Sizing the Branch Site, page 3-11 for more information.

  - Use the recommended levels of Cisco IOS software as indicated.

Note See Software Releases Evaluated, page 3-18 for more information.

The following sections provide additional detailed information on some of these recommendations.

Using IPSec for Data Encryption

There are three elements to consider when securing the traffic flowing over the VPN:

- Authentication—Ensuring the senders/receivers of traffic are known, valid entities
- Confidentiality—Encrypting data to render it imperceptible without the proper key
- Message integrity—Identifying when data has been modified

IKE is used to ensure the authentication of the IPSec peers.

To ensure confidentiality of data transported over the VPN, encryption algorithms such as Data Encryption Standard (DES) or Triple Data Encryption Standard (3DES) are implemented. Because 3DES is more secure, it should be implemented if possible, except in cases where export restrictions may limit the implementation to DES.

To ensure message integrity, the IPSec protocol is used with a hash method, such as Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1).

It is possible to implement only a hash method or only an encryption standard to secure the VPN. However, it is highly recommended that both be implemented in combination. This design guide recommends the combination of 3DES and SHA-1.

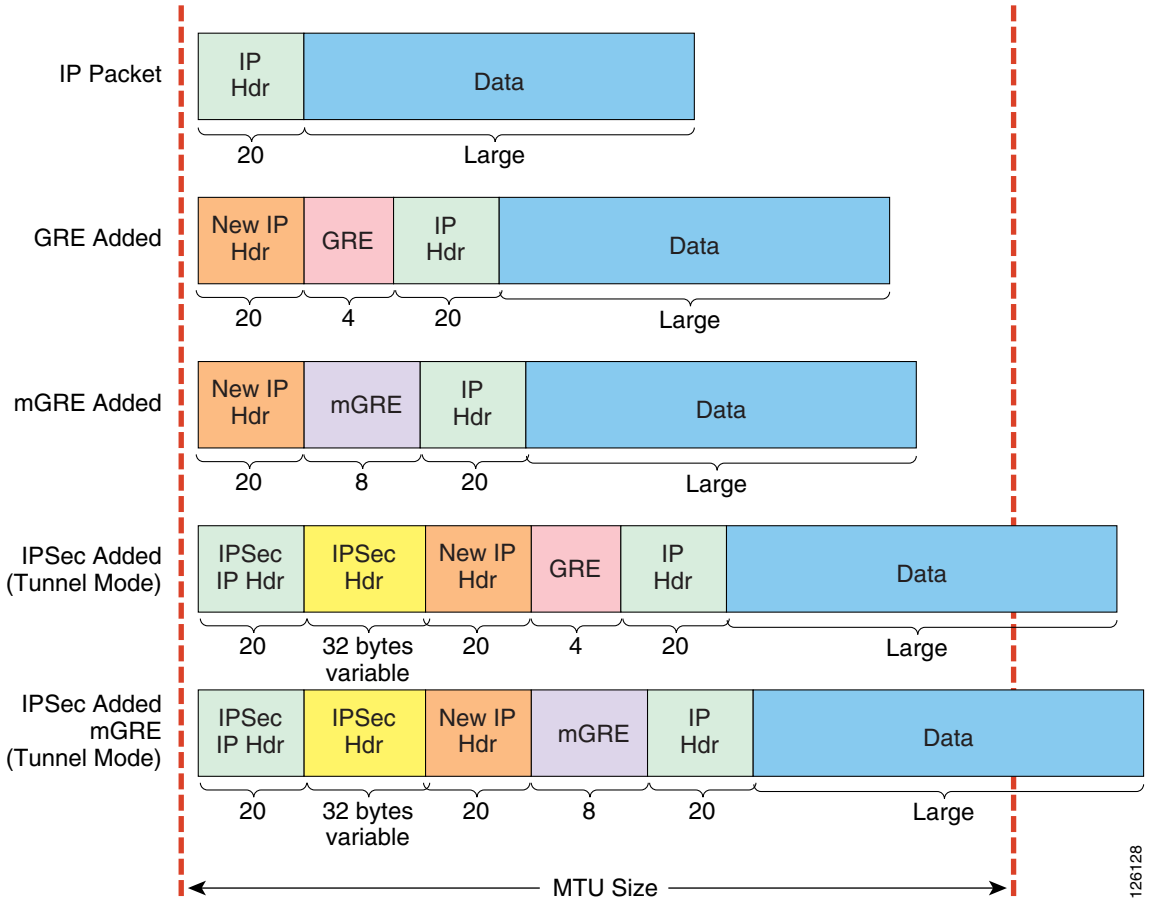
With hardware-accelerated encryption implemented, performance is not significantly affected by choice of encryption method.

Note Advanced Encryption Standard (AES) is another option for encryption of data. For more information about the Cisco implementation of AES, see the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110bb6.html

Minimizing Packet Fragmentation

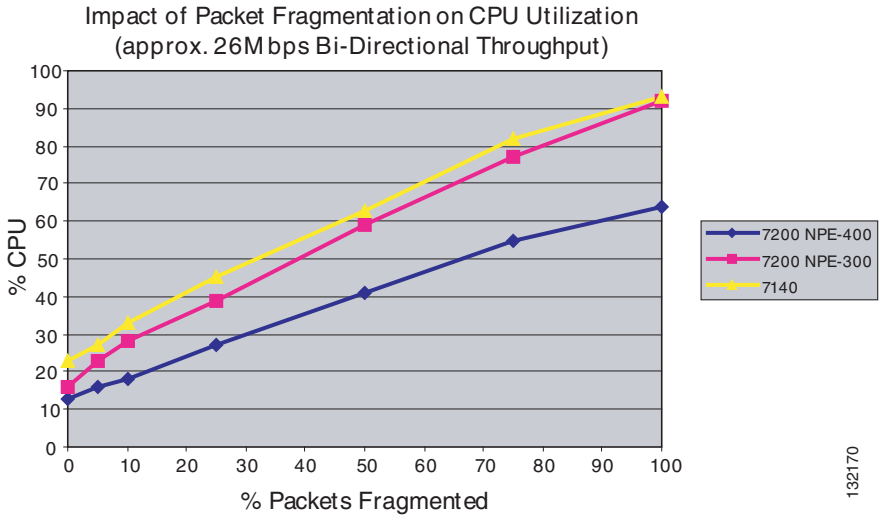
IPSec and GRE headers increase the size of packets, and packet fragmentation is a cause of decreased performance in IPSec networks. If the size of a packet before encryption is at or near the maximum transmission unit (MTU) of the transmission media, the encrypted packet with the additional IPSec and GRE headers becomes greater than the MTU of the transmitting interface. This results in Layer 3 fragmentations on the outbound interface, as shown in Figure 2-1:

Figure 2-1 IPSec/GRE Packet Expansion



This results in the packet being fragmented at Layer 3, and the need for these packets to be re-assembled before the decryption process. In the current Cisco IOS implementation, re-assembly is performed in process-switched mode, resulting in significantly lower throughput performance. Figure 2-2 shows an example of how CPU utilization increases with increasing Layer 3 packet fragmentation:

Figure 2-2 Increase in CPU from IPSec Packet Fragmentation



Cisco recommends avoiding fragmentation whenever possible by using one of the following methods. The methods below are listed in order of least to most effort, complexity, and cost to a customer:

- Employ path MTU discovery (PMTUD). See Path MTU Discovery, page 2-11 for more information on this method.
- Set the MTU of attached workstations to 1400 bytes.

There is a feature supported by current versions of Cisco IOS called Look Ahead Fragmentation (sometimes abbreviated LAF and sometimes called “pre-fragmentation”). With LAF enabled, the device looks at the MTU of the outbound crypto interface, evaluates the headers to be added to a packet, and performs fragmentation at the IP level before sending the fragments to the crypto engine. The receiving host decrypts the fragments and passes them to the receiving host, which then bears the burden of re-assembling the fragments into a packet.

In a Cisco IOS router running 12.1(11)E, 12.2(13)T or later, LAF is enabled by default on physical interfaces, but needs to be configured on tunnel interfaces. In the Catalyst 6500 switch or Cisco 7600 router with a Cisco VPN Services Module, LAF is enabled by default and does not need to be configured on the tunnel interfaces.

The throughput results presented in this design guide are shown with and without Layer 3 fragmentation whenever both measurements were recorded.

IP Addressing

Proper IP addressing is critical for a successful VPN. To maintain scalability, performance, and manageability, it is highly recommended that remote sites use a subnet of the major network to allow for summarization. Using this method, the crypto ACLs, where they are configured in the command-line interface (CLI), need only a single line for every local network; possibly a single entry if the local networks are summarized.

Proper address summarization is highly recommended. Address summarization conserves router resources, which makes routing table sizes smaller. Address summarization also saves memory in routers and eases troubleshooting tasks. In addition to conserving router resources, address summarization also simplifies the configuration of routers in IPSec networks.

Note Consult the "IP Addressing" section of the *Cisco SAFE VPN White Paper* for a more thorough discussion. Cisco SAFE documentation can be found at the following URL: http://www.cisco.com/go/safe.

Placing VPN Head Ends Relative to the Firewall

The placement of the VPN head-end devices in the network relative to the enterprise firewall can critically affect the security of any VPN deployment.

Recommended architectures are discussed in the SAFE VPN white papers available at the following URL: http://www.cisco.com/go/safe.

Solution One (IPSec with GRE)—Design Recommendations

This section details the recommendations specific to Solution One (IPSec with GRE). Solution One is recommended when multi-protocol, multicast support is needed, or when routing protocol support is necessary. For deployments without these specific requirements, Solution Three may be used instead.

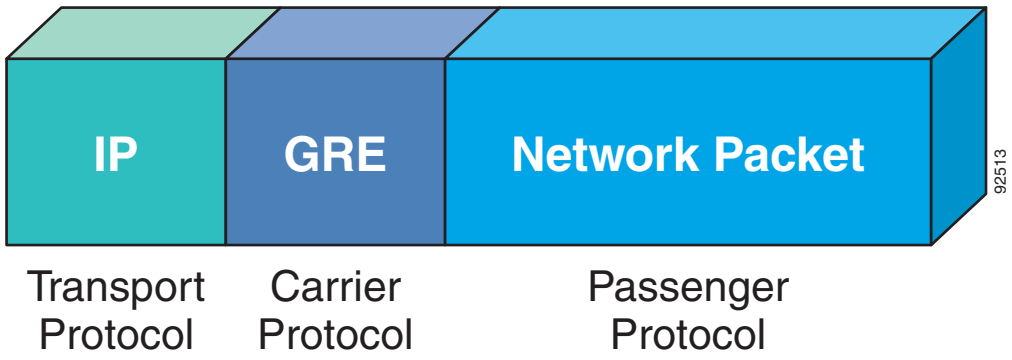
This section includes the following topics:

Implementing GRE

Although IPSec provides a secure method for tunneling data across an IP network, it has several limitations. First, IPSec does not support broadcast or multicast IP, preventing the use of protocols such as routing protocols that rely on these features. Second, IPSec does not support the use of multi-protocol traffic.

To overcome these limitations in networks that must support them, you should implement GRE tunnels. GRE is a protocol that can be used to "carry" other passenger protocols, such as broadcast or multicast IP, as well as non-IP protocols, as is shown in Figure 2-3.

Figure 2-3 GRE as a Carrier Protocol of IP



Using GRE tunnels in conjunction with IPSec extends the functionality of the VPN so that multicast IP and non-IP protocols are possible. This provides a critical element of this solution by providing the ability to run a routing protocol across the network between the central site and branch offices.

Even if requirements such as multicast IP, non-IP protocols, or supporting routing protocols do not exist in the current customer network, designing the VPN for maximum flexibility prevents a costly and potentially disruptive re-design in the future should these become requirements.

IPSec or IPSec/GRE also enable private addressing. Without a tunnel protocol running (either IPSec tunnel mode or GRE) all end stations are required to be addressed with registered IP addresses. By encapsulating the IP packet in a tunneling protocol, private address space can be used.

With the IPSec/GRE solution, all traffic between sites is encapsulated in a GRE packet before the encryption process. This simplifies the access list used in the crypto map statements because they need only one line permitting GRE (IP Protocol 47).

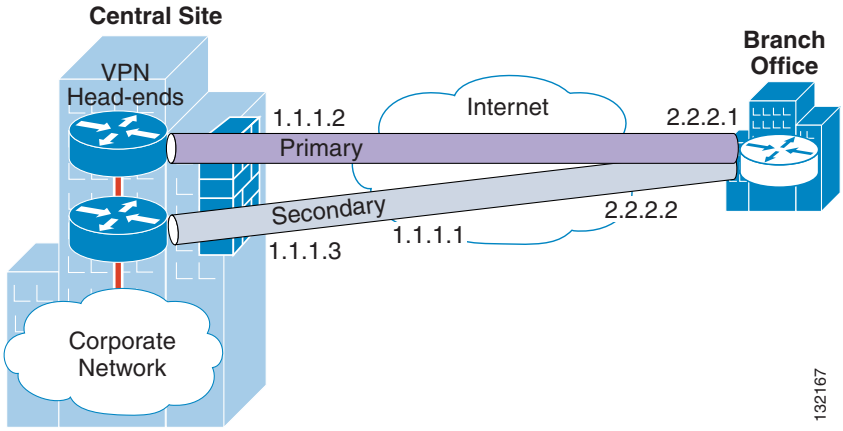
High Availability and Resiliency

Traditionally, data networks were deployed as best effort networks with no guarantee as to the actual performance of the network, and they were frequently deployed with many single points of failure. For the next level of applications to be successfully deployed, networks must behave in a much more predictable manner. This not only includes recovery from failures within specific timeframes but also includes the ability to transport the packets to their destination with specific and repeatable (minimized) delays.

In all cases, networks should be designed so that the individual network elements operate conservatively. These elements include network devices, routers, switches, and so on, and the LAN and WAN links that connect these devices together.

To provide a level of resiliency in the VPN design, Cisco recommends configuring a primary and a secondary tunnel between each branch-end device and the head ends. Under normal operating conditions, both the primary and secondary tunnels are established. The routing protocol, such as EIGRP, maintains both routes, with the secondary tunnel being configured as a less preferred route. Figure 2-4 shows this configuration.

Figure 2-4 High-Availability Tunnel Configuration



If a failure occurs at one of the head-end devices, the routing protocol detects that the route through the primary tunnel is no longer valid and, after convergence, the route through the secondary tunnel is used. When the primary is available again, traffic is routed back to the primary tunnel as the preferred route in the routing metrics.

The head end resiliency design presented here allows for failure of a single head-end device with proper failover to surviving head ends. This is normally adequate when the number of head ends is relatively low (for example, ten or less). If the number of head ends is relatively high (for example, twenty or more), the customer may want to consider designing for the possibility of multiple head-end device failures.

It may also be necessary in the customer strategy to have head-end devices geographically dispersed. Although not scalability tested, the architecture presented in this guide should readily support this configuration.

Note More information regarding this architecture is discussed in the SAFE VPN white papers available at the following URL: http://www.cisco.com/go/safe.

Configuration of primary and secondary tunnels to appropriate head ends is critical to maintain network resiliency. The next section discusses tunnel aggregation.

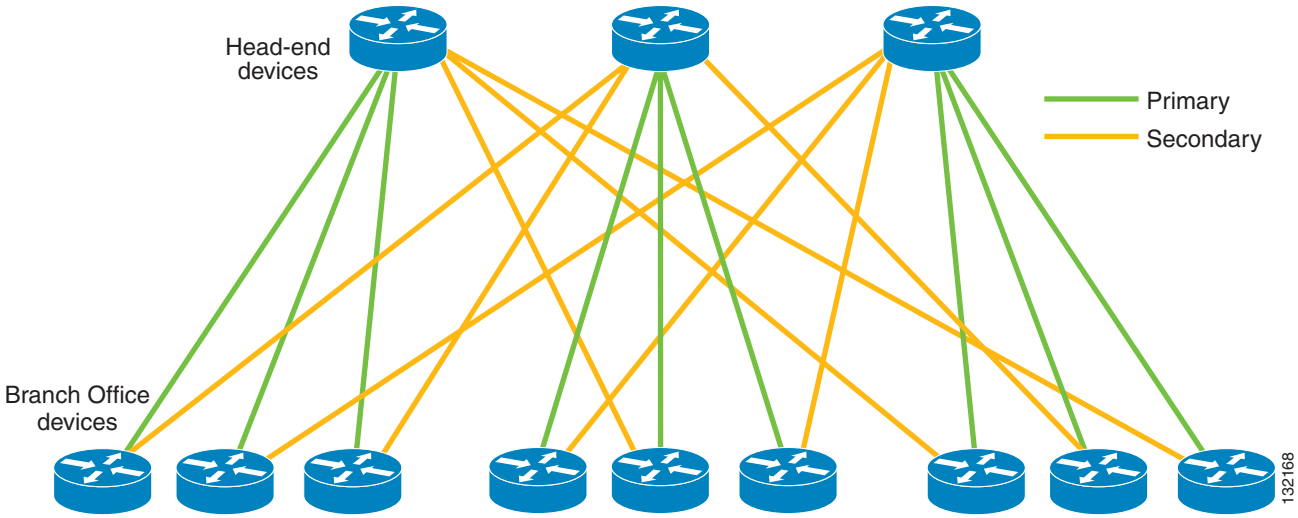
Head End Load Distribution

When laying out the network topology, it is important to consider load balancing across multiple head-end devices, especially in the case of a head-end device failure. This design recommends that there be at least two tunnels configured between a branch device and the head end.

The primary tunnel (the preferred route) should be configured (via a bandwidth statement) to carry traffic under normal circumstances. The preferred primary tunnels should be evenly divided among the head-end devices. The secondary tunnels for branches should be evenly spread among the remaining (surviving) head-end devices.

For example, it would be highly undesirable for all the tunnels from a failed head-end device to re-establish to a single secondary head-end device when there are more devices that could distribute the load from the failed device. Figure 2-5 shows a typical network topology with high resiliency.

Figure 2-5 Tunnel Aggregation for Resiliency



To plan for proper tunnel aggregation and load distribution in the case of a head-end device failure, the following algorithm should be used:

1. Start with the number of total branch devices to be aggregated at the head end.
2. Divide this number by the number of head-end devices.
3. Multiply the result by 2 for primary and secondary tunnels. This is the total tunnels per head-end device.
4. Allocate the primary tunnels to each head-end device in the arrangement shown in Figure 2-5 in green.
5. For each group, allocate the secondary tunnels in a round-robin fashion to all head-end devices except the one serving as a primary for that group. This arrangement is also shown in Figure 2-5 in yellow.
6. Check to see that each head-end device is now allocated the same number of total tunnels per head-end device.

Note Please note that this calculation should take into account any tunnel throughput variances.

Number of Tunnels per Device

The number of tunnels required for each head-end device should be scaled to the overall size of the network in which the VPN solution is being deployed. See Head End Devices, page 3-5 for more information.

Head end scalability testing did not include an exhaustive evaluation of the maximum number of tunnels that can be terminated to head-end devices. In addition, scalability testing of branch site devices in the Solution One design was performed with two tunnels per branch device. This did not include exhaustive testing of the number of tunnels these different platforms can support. Branch device testing, which focused specifically on the number of tunnels that can be safely terminated on specific products, was performed as part of design testing for Solution Two.

Path MTU Discovery

A feature of IP called path MTU discovery (PMTUD) can eliminate the possibility of fragmentation if it is supported by the end stations. This procedure is run between two end stations with the participation of the network devices between them.

During PMTUD, an MTU-sized packet is sent out by an end station with the "do not fragment" (DF) bit set. If this packet encounters a link with a lower MTU than the packet size, an ICMP error message is generated with a "3" in the type field (destination unreachable), a "4" in the code field (fragmentation needed and DF set), and the next-hop MTU size in the unused field of the ICMP header.

For this process to work over an IPSec network with GRE, the GRE tunnel MTU should be set to a value low enough to ensure that the packet makes it through the encryption process without exceeding the MTU on the outbound interface (usually 1400 bytes).

Alternative Network Topologies

The Solution One and Three designs recommend a hub-and-spoke topology. Partially meshed and fully meshed networks are supported with Solution Two (DMVPN).

Hub-and-spoke topologies are generally easier and safer to implement than partial or fully meshed designs. For example, in a meshed network, the larger number of active tunnels per peer places more of a performance burden on the devices running IPSec, possibly requiring more CPU and memory resources. Furthermore, path selection and network resiliency are not as predictable when spokes are able to create direct spoke-to-spoke tunnels, as is supported by DMVPN. However, there may be network designs in which partial or fully meshed networks meet the needs of the network implementers; in these instances, Solution Two is a good fit.

The configuration of the encrypting devices becomes more complex when attempting to create a partial or full mesh network with Solution One. At a minimum, an additional access list must be created for each peer connection, as well as additional crypto map entries. In addition, the routing protocol (as is recommended in this design guide) must deal with many more adjacencies, nullifying the advantages of routing protocol efficiencies such as summarization and stub.

For smaller deployments, a fully meshed or partially meshed topology may be possible, but the size of these deployments should be limited and carefully tested before roll out. Only limited testing of partial and full mesh topologies has been completed as part of scalability testing for this design guide.

Using a Routing Protocol across the VPN

This design recommends the use of a routing protocol to propagate routes from the head end to the branch offices. Using a routing protocol has several advantages over the current mechanisms in IPSec alone.

One key advantage of using a routing protocol is that the VPN receives the same level of benefit as doing so on a traditional network. This includes receiving information about the network connectivity available over a particular interface, topology information about a network, notification when that topology changes (such as when a link fails), and information about the status of remote peers.

Another advantage is that although there are alternatives to a routing protocol, most seek only to verify the "health" of the VPN device. With a routing protocol, it is additionally possible to verify that traffic is actually reaching its destination.

Several routing protocols are candidates for operation over an IPSec VPN, including EIGRP and OSPF. Solution One as presented in this design guide uses EIGRP as the routing protocol, because EIGRP was used during the scalability tests conducted. EIGRP is recommended as the routing protocol to use because of its conservative utilization of router CPU and network bandwidth as well as its quick convergence times. EIGRP also provides a range of options for address summarization and default route propagation.

Routing protocols do increase the CPU utilization on a network device, and this impact must be taken into consideration when sizing those devices.

Route Propagation Strategy

There are a number of approaches to propagating routes from the head end to the branch offices. For the Solution One design, the recommended approach is for each head-end router to advertise a default route to each of the tunnels it terminates with a preferred cost for the primary path. With this in mind, each of the branch office routers must add a static host route for each of the head-end peer (primary and secondary) IP addresses, with a next hop destined for their respective ISP IP addresses.

For example, in a scenario where one branch has a primary and secondary tunnel to two head-end routers, the configuration excerpts shown below are used (for EIGRP as the routing protocol):

Head-end router (primary):

```
interface e0
ip address 1.1.1.2 255.255.255.0
!
router eigrp 1
redistribute static
!
ip route 0.0.0.0 0.0.0.0 1.1.1.1
```

Head-end router (secondary):

```
interface e0
ip address 1.1.1.3 255.255.255.0
!
router eigrp 1
redistribute static
!
ip route 0.0.0.0 0.0.0.0 1.1.1.1
```

Branch-site router:

```
router eigrp 1
!
ip route 1.1.1.2 255.255.255.255 2.2.2.2
ip route 1.1.1.3 255.255.255.255 2.2.2.2
```

In this example, the IP address 2.2.2.2 refers to the ISP provider network of the branch office. IP addresses 1.1.1.2 and 1.1.1.3 represent the two head-end routers. Note that the branch-site router configuration contains static routes for the two head-end routers, with the ISP as the next-hop router. Also, note that the head-end routers advertise a default route to 1.1.1.1.

Solution Two (DMVPN)—Design Recommendations

This section details the recommendations specific to Solution Two (DMVPN). Solution Two is recommended when multicast traffic and routing protocol support is desirable, when dynamic spoke-to-spoke connectivity is needed, and when branch-site routers are dynamically addressed by the service provider. For deployments without these specific requirements, Solution Three may be used instead.

This section includes the following topics:

Generic Route Encapsulation with mGRE Tunnels and NHRP

A multipoint GRE (mGRE) tunnel serves as a template for the creation of multiple GRE tunnels, either between a hub router and multiple spoke routers, or between spoke routers. An advantage of mGRE tunnel implementation is that the tunnel destination does not need to be specified, which is a benefit when dealing with dynamically-addressed spoke devices. Used in combination with NHRP, an mGRE-encapsulated interface works much the same as a Point-to-Multipoint Frame Relay interface with inverse ARP enabled. When the spoke router (NHRP client) boots, or comes online to the network, it registers its real (NBMA) address with the hub (NHRP server), which enables the mGRE interface to build a dynamic tunnel back to it, without having to know the tunnel destination via CLI configuration.

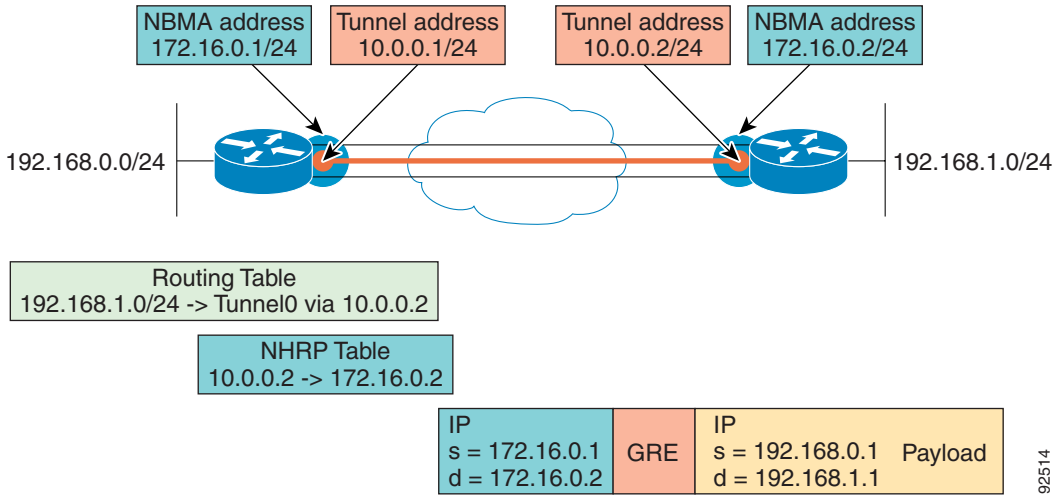
Like GRE, mGRE encapsulation adds to the size of the original data packet. The protocol header for an mGRE packet is four bytes larger than that of a GRE packet. The additional four bytes constitute a tunnel key value, which is used to differentiate between different mGRE interfaces in the same router. In early versions of DMVPN, if there is no tunnel key, a router can only support one mGRE interface, corresponding to one IP network. With tunnel keys, a router can aggregate multiple groupings of hub-to-spoke tunnels, or multiple IP networks. As of Cisco IOS version 12.3(9.13)T (because of a regression issue, Cisco recommends using 12.3(12.01)T or 12.3(11)T3), it is possible to configure mGRE tunnel interfaces without tunnel keys and have them serve separate DMVPN groupings. To do this, each mGRE interface must reference a unique IP address or interface as its tunnel source. A router can also aggregate multiple groupings of encrypted tunnels by using tunnel keys.

NHRP, as defined in RFC 2332, is a Layer 2 address resolution protocol and cache. When a tunnel interface is an mGRE tunnel, NHRP tells the mGRE process where to send a packet (the IP next hop) to reach a certain address. Consider the following example from the hub router:

```
interface FastEthernet0/0
 ip address 172.16.0.1 255.255.255.0
!
interface Tunnel0
 description mGRE Template Tunnel
 ip address 10.0.0.1 255.255.255.0
 tunnel source FastEthernet0/0
!
```

In this case, 10.0.0.1 is the router tunnel address, and 172.16.0.1 is the router NBMA address. NHRP tells the router querying it to map a tunnel IP address to an NBMA IP address. After the packet is encapsulated by the mGRE process, the IP destination address is the NBMA address, as shown in Figure 2-6.

Figure 2-6 NHRP and GRE



The NHRP cache can be populated with either static or dynamic entries. In DMVPN, all entries are added dynamically, via registration or resolution requests. The process begins by the spoke having an NHRP map configured pointing to the hub via the **ip nhrp map x.x.x.x y.y.y.y** command (x.x.x.x is the tunnel IP and y.y.y.y is the NBMA IP address of the hub/NHRP server). To participate in the NHRP registration process, all routers must belong to the same NHRP network, as configured by the **ip nhrp network-id <id>** command. The network-id defines an NHRP domain, and is unrelated to the tunnel key.

For the spoke routers to register with the hub, they are also configured with the hub NBMA address as their next-hop server, and they can authenticate with each other via a key string. After the hub has cached the tunnel and NBMA addresses of the spoke, it can now serve this information to other devices in the same NHRP network, for as long as the entry remains valid in its cache.

Tunnel Protection

The development of DMVPN has made router configurations simpler. In earlier versions of IPSec configurations, such as those shown in Solution One and Solution Three, dynamic or static crypto maps are configured via the router CLI. These crypto maps specify which IPSec transform set (encryption strength and Diffie-Hellman group) and perfect forward secrecy (PFS) group are used, and also specify a crypto access list, which defines interesting traffic for the crypto map. As of Cisco IOS Software Release 12.2(13)T, the concept of an IPSec profile exists.

The IPSec profile shares most of the same commands with the crypto map configuration, but only a subset of the commands is needed in an IPSec profile. Only commands that pertain to an IPSec policy can be issued under an IPSec profile; there is no need to specify the IPSec peer address or the access control list (ACL) to match the packets that are to be encrypted.

The IPSec profile is associated with a tunnel interface with the **tunnel protection ipsec profile <profile-name>** command. With tunnel protection mode, IPSec encryption is performed after the GRE encapsulation has been added to the tunnel packet. The **tunnel protection** command can be used with

mGRE and Point-to-Point GRE Tunnels. With Point-to-Point GRE tunnels, the tunnel destination address is used as the IPSec peer address. With mGRE tunnels, multiple IPSec peers are possible; the corresponding NHRP-mapped NBMA destination addresses are used as the IPSec peer addresses.

High Availability and Resiliency

As with Solution One, in a DMVPN design, Cisco recommends that two tunnels, a primary and secondary, be configured between each branch-end device and the head ends. Under normal operating conditions, both the primary and secondary tunnels are established. The routing protocol, such as EIGRP, maintains both routes, with the secondary tunnel being configured as a less preferred route. This allows branch-end devices to converge to a secondary head end without user intervention, in the event of a failure at one head-end device.

Head End Load Distribution

As with Solution One, it is important to consider load balancing across multiple head-end devices, especially in the case of a head-end device failure. This design recommends that there be at least two tunnels configured between a branch device and the head-ends. The primary tunnel (the preferred route) should be configured (via a bandwidth statement) to carry traffic under normal circumstances. The preferred primary tunnels should be evenly divided among the head-end devices. The secondary tunnels for branches should be evenly spread among the remaining (surviving) head-end devices.

The same principles of tunnel aggregation and load distribution as discussed in Solution One are applicable to Solution Two. Scalability testing with DMVPN in contrast to a design with Point-to-Point GRE tunnels (as described in Solution One) indicates that, in terms of resources at the head-end or hub device, DMVPN offers performance improvements over Solution One. See Head End Devices, page 3-5 for more information.

Path MTU Discovery

As with Solution One, the GRE tunnel MTU must be set to a value low enough to enable PMTUD to work as intended. The same recommendation (1400 bytes) as discussed in Solution One is applicable in Solution Two.

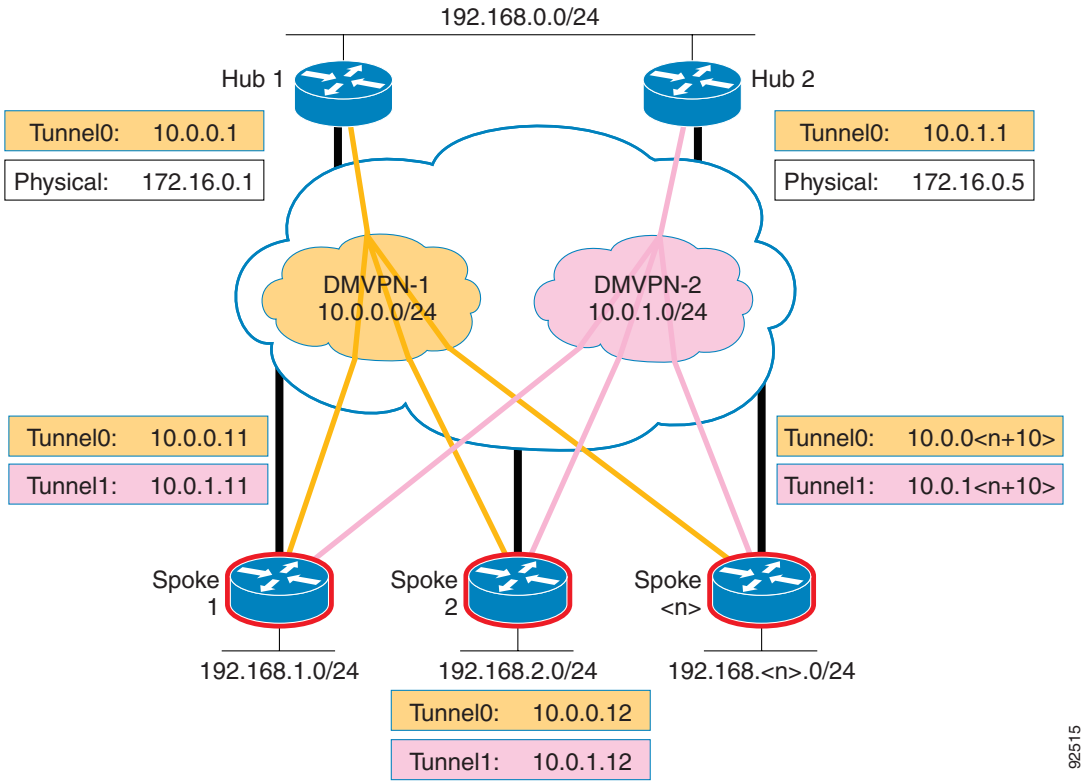
Supported Network Topologies

Using DMVPN, it is possible to create topologies that allow partially meshed and fully meshed networks, or to limit the topology to a pure hub-and-spoke design.

Hub-and-Spoke

If desirable to limit the topology to a hub-and-spoke model, then the hubs are configured with mGRE tunnel interfaces and the spokes (or branch-end devices) are configured with Point-to-Point GRE tunnels. With a Point-to-Point GRE tunnel, the tunnel destination is configured via the CLI. In this model, the branch-end has two tunnel interfaces, each pointing to a different head-end router, and each tunnel interface belongs to a unique IP network. This design is usually referred to as dual hub-dual DMVPN, and is shown in Figure 2-7.

Figure 2-7 Dual Hub-Dual DMVPN

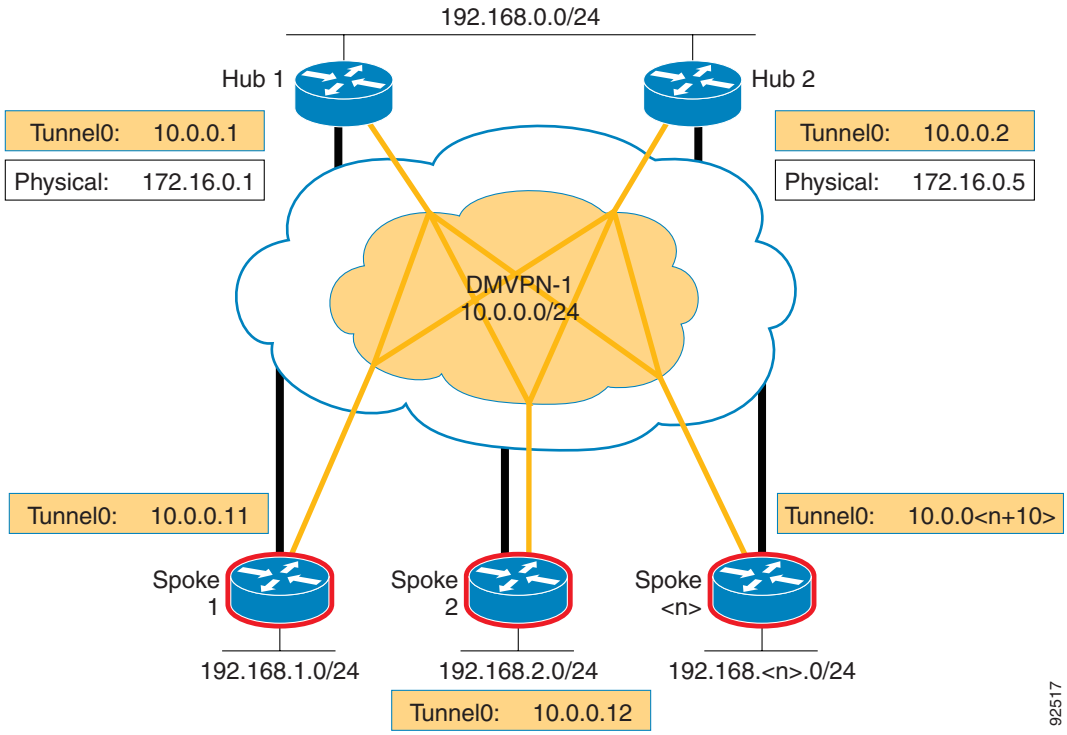


In this design, the two head ends have IP connectivity to each other, but there is no requirement for any DMVPN connectivity between head ends.

Spoke-to-Spoke

If dynamic spoke-to-spoke tunnels are a design requirement, then the branch-end devices, as well as those at the head end, are configured with mGRE tunnel interfaces. All devices to which a spoke may initiate a spoke-to-spoke tunnel must be part of the same DMVPN; therefore, Cisco recommends maximizing the number of reachable devices using a dual hub-single DMVPN design, as shown in Figure 2-8.

Figure 2-8 Dual Hub-Single DMVPN



In this design, the branch-end devices have a single mGRE tunnel interface, but have NHRP mapping statements and next-hop server definitions for each of the two head ends. When spoke-to-spoke tunnels are created, the two spokes do not become routing peers of each, but they do need to perform IKE authentication with each other before traffic can flow over the spoke-to-spoke tunnel.

To avoid asymmetrical routing of the traffic between the hubs and the spokes (and the undesirable consequences of per-packet load balancing), the **bandwidth** (for EIGRP) and **ip ospf cost** (for OSPF) configurations can be tweaked on the hub routers, to determine which path (via Hub1 or Hub2) routers behind the hubs select to reach the networks at a spoke. A drawback to this approach, however, is that it is not possible to balance multiple spokes across two or more hubs; only one hub is used at a time. Also, there is a potential for asymmetrical routing to occur from the perspective of the spoke router, because it has only a single tunnel interface. A workaround is to use the **distance** command under **router ospf 1** on the spokes, as in the following example:

```
router ospf 1
 ...
 distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```

Given unequal administrative distances, the spoke routers prefer the path with the lower administrative distance, and choose the path with the higher administrative distance only if the preferred router becomes unavailable. A side-effect of this approach is that only the preferred hub (the one with the lower administrative distance) is used, even if the other hub is advertising the same route with a lower metric.

With EIGRP as a routing protocol, there is more flexibility in a dual hub-single DMVPN to provide resiliency, avoid asymmetrical routing, and allow load balancing of multiple spokes across two or more hubs. One approach uses the **offset list** command. To implement this, begin by dividing the spokes into as many groups as there are hub routers. Identify the networks behind the spokes in group 1 in an ACL on Hub2, the spokes in group 2 by an ACL on Hub1, and so on. For the purpose of the following example, the ACLs are called “ACL-net-gr1” and “ACL-net-gr2”:

Hub1:

```
router eigrp 1
 ...
 offset-list ACL-net-gr2 in 256000 tunnel0
 offset-list ACL-net-gr2 out 256000 tunnel0
```

Hub2:

```
router eigrp 1
 ...
 offset-list ACL-net-gr1 in 256000 tunnel0
 offset-list ACL-net-gr1 out 256000 tunnel0
```

The **offset-list** command applies an offset value of 256000 to the delay component of networks in the given ACL. The net effect is that spokes in group 1 prefer Hub 1, and spokes in group 2 prefer Hub 2, which permits load balancing of the spokes across the two hubs while avoiding asymmetrical routing.

In the dual hub-single DMVPN configuration, intra-hub communications must flow over mGRE tunnels built between the hubs. This means that the hubs are NHRP clients of each other, and are defined as next-hop servers of each other. The NHRP relationship is required so that the hubs can be routing neighbors of each other.

If the network design grows beyond two hubs, NHRP maps between hubs are bi-directional; for instance, in a design with three hubs, the NHRP maps are as follows:

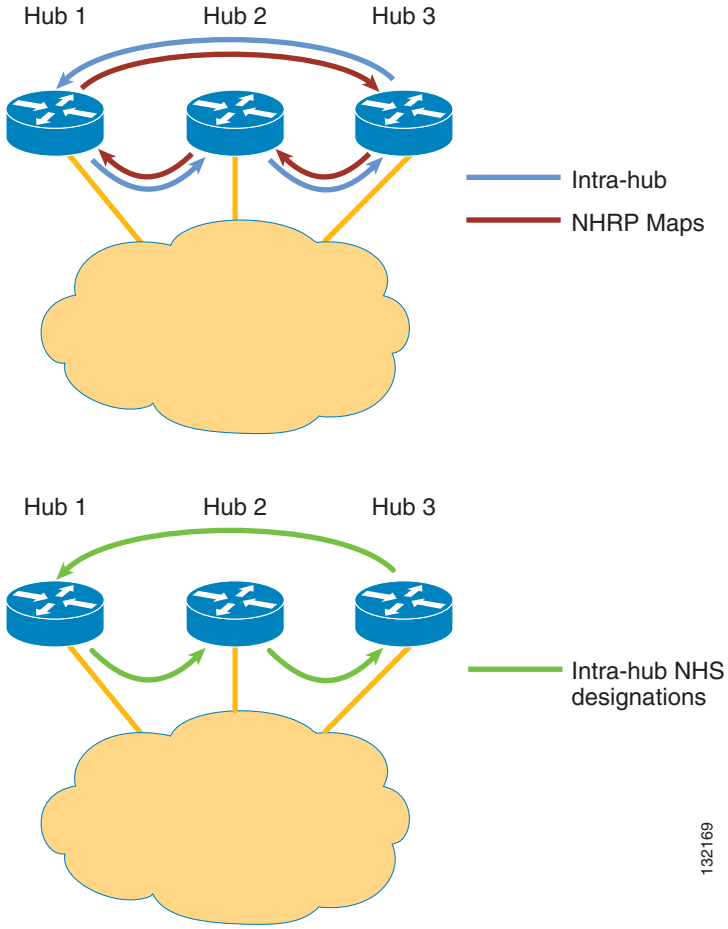
1->2, 2->1, 2->3, 3->2, 3->1, 1->3

The next-hop server definitions are done in a daisy-chain, as follows:

1->2, 2->3, 3->1

This is shown in Figure 2-9**.**

Figure 2-9 Intra-hub NHRP and NHS in Multi-hub—Single DMVPN



Spoke-to-Spoke Design Considerations

In general, the partially or fully meshed topology is a less predictable, less conservative design. It is possible that the bandwidth of the spoke device, or the spoke device itself, may be overrun by a large number of other devices attempting to setup tunnels to it. Also, path selection and network resiliency are not as predictable as in a hub-and-spoke topology, especially if the medium of connection is the public Internet. When designing a DMVPN that supports spoke-to-spoke tunnels, keep in mind the following good design principles:

- Design the network with adequate bandwidth for the anticipated application load.
- Select platforms with sufficient resources for the anticipated network load.
- Balance the percentage of hub-to-spoke and spoke-to-spoke flows to a reasonable level; the design recommendation is 80 percent hub-to-spoke and 20 percent spoke-to-spoke.
- Set user expectations of the response time, and even availability, of the link appropriately.

Solution Three (IPSec with DPD, RRI, and HSRP)—Design Recommendations

This section includes the following topics:

Often a VPN does not require multi-protocol or multicast data. In this case, an IPSec VPN can achieve a higher throughput without the use of GRE because the routers configured for the VPN do not need to perform the GRE encapsulation, and the packets themselves do not contain the usual 24-byte GRE overhead. As a rule of thumb, the CPU utilization on head-end routers is about ten percent less when GRE is not configured.

Alternatives to Using a Routing Protocol

A routing protocol provides several vital features when deployed over a network. These include peer state detection, optimal routing, and the ability to facilitate alternate routes in the event of a failure.

Dead Peer Detection

Dead Peer Detection (DPD) is a relatively new Cisco IOS feature that is actually an enhancement of the IKE keepalives feature. When DPD has not received traffic from an IPSec peer during a specified configurable period, DPD sends a hello message to the IPSec peer. If normal IPSec traffic is received from a peer and decrypted correctly, then that peer is assumed to be alive, no hello message is sent, and the DPD counter for that peer is reset. This results in lower CPU utilization than that which would have occurred with IKE keepalives.

Reverse Route Injection

Another recent IPSec feature addition to Cisco IOS is Reverse Route Injection (RRI). RRI functions by taking the information derived from the negotiated IPSec SAs and creating a static route to the networks contained in those SAs. Route redistribution can then take place between these “static” routes and any routing protocol configured on the head-end router.

Dynamic Crypto Maps

Rather than pre-defining all the IPSec peers, another option is to create dynamic crypto maps. Dynamic crypto maps allow an IPSec connection between two peers when one of the peers, usually the central site peer, does not have the complete configuration necessary to complete an IPSec negotiation with a remote

peer. This situation can occur when the remote peer has its IP address dynamically assigned, as in the case of a residential class service connection such as a cable or xDSL connection. Because the remote peer IP address is unknown, it cannot be preconfigured into the central site device.

IKE is required for authentication with dynamic crypto maps. The IKE authentication completes based on an identity other than the remote IP address, such as the fully qualified domain name (FQDN) of the peer, and information from the IKE session is used to complete the missing information in the dynamic crypto map configuration.

Hot Standby Router Protocol

IPSec has also been enhanced with Hot Standby Router Protocol (HSRP). This feature enables IPSec to use the standby group address as its IPSec peer address. If the current owner of the HSRP group fails, that address transfers over to the secondary standby router. HSRP works between the active and standby routers in either stateless or stateful modes.

Stateless Failover

In stateless failover mode, no IPSec or IKE SA state information is transferred during failure. A remote peer router configured with an HSRP group address as an IPSec peer must renegotiate its IKE SAs and IPSec SAs before any subsequent traffic transmission. Stateless operation is supported with all platforms and ISAKMP authentication types.

Stateful Failover

IPSec stateful failover (VPN High Availability) allows the head-end routers to share information in the SA database with each other. In the event of a head-end device failure, as detected by HSRP, the spoke router continues the same IPSec SA with the backup head end without the need to create a new SA. This greatly reduces failover time and the amount of re-keying required in the event of a head end failure.

Cisco has developed different versions of stateful failover in conjunction with different platforms. The feature was initially released to work with State Synchronization Protocol on the Cisco 7200 VXR Series Routers with NPE-400 and the Catalyst 6500/7600 Series Routers with the VPN Services Module (VPNSM). Cisco IOS Software Release 12.2(11)YX or later is required for use with the Cisco 7200 VXR, and Catalyst IOS Software Release 12.2(14)SY or later is required for use with the Catalyst 6500/7600 and VPNSM.

Note Further information about this implementation is available at the following URL: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5012/products_feature_guide09186a0080116d4c.html

A newer version of this feature using Stateful Switchover (SSO) with HSRP was developed for the Cisco 7200 VXR with NPE-G1, and platforms using the Advanced Integration Module (AIM)-VPN/HPII encryption module. Cisco IOS Software Release 12.3(11)T or later is required for this version of VPN High Availability.

Note Further information on this implementation is available at the following URL: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_feature_guide09186a00802d03f2.html

These two versions of this feature cannot be used together. In both cases, the only form of ISAKMP authentication supported is pre-shared keys.

Solution Three Limitation—Tunnel Initiation Not Possible from Head Ends

A limitation exists with Solution Three with regard to tunnel initiation. Because of the use of dynamic tunnels, the IPSec connection can only be initiated by the branch router. Because the head-end devices use dynamic crypto maps, they do not have all the information necessary to create an IPSec SA by themselves. This is of concern when traffic forwarding is required from a central site to a remote site without the remote site initiating the connection. If the IPSec tunnel initiation from the head end is required, static crypto maps should be used.

Number of Tunnels per Device and Load Distribution

The number of tunnels required for each head-end device should be scaled to the overall size of the network in which the VPN solution is being deployed. See Head End Devices, page 3-5 for more information.

In addition, the normal load from a number of branch sites may be distributed across two or more head-end devices, if stateless failover is employed. This is accomplished by configuring multiple standby groups; one group for each group of branch devices. By using HSRP in this manner, a number of remotes may be evenly divided among a number of head-end devices for load sharing during normal operation. During a failure event, only the branch devices connected as primary to the failed HSRP group owner are subject to re-negotiation of the IPSec SAs, resulting in enhanced failover performance.

If stateful failover is configured, it is not possible to distribute groups of branch sites by HSRP groups across different head-end devices. In stateful failover, one head-end router is “active” (terminates all ISAKMP and IPSec SAs) and the other is completely dedicated to “standby” operations.

Head end scalability testing did not include an exhaustive evaluation of the maximum number of tunnels that can be terminated to head-end devices. In addition, scalability testing of branch site devices was performed with two tunnels per branch device. This did not include exhaustive testing of the number of tunnels these different platforms can support.

Comparing Failover and Convergence Performance

Network performance in the event of a failure is a primary concern during an IPSec VPN deployment.

This section includes the following topics:

Solution One—Failover and Convergence Performance

Each customer may have different convergence time requirements. The design principles in this guide were used to perform a scalability test with up to 480 branch offices aggregated to two head-end devices.

The test was performed by powering off one of the head-end devices to simulate a complete failure. In this test, the network fully converged after a maximum of approximately 32 seconds. The starting and failover traffic/tunnel aggregation conditions are shown in Table 2-1.

Table 2-1 Three Head End Failover Scenarios IPSec/GRE

	Head End 1	Head End 2	Head End 3
Cisco 7140			
Starting condition	23 Mbps 80 branches 33% CPU	23 Mbps 80 branches 33% CPU	37 Mbps 80 branches 40% CPU
During failover	Failure	33 Mbps 120 branches 48% CPU	48 Mbps 120 branches 58% CPU
Cisco 7200 VXR NPE-300			
Starting condition	22 Mbps 80 branches 33% CPU	22 Mbps 80 branches 37% CPU	37 Mbps 80 branches 38% CPU
During failover	Failure	33 Mbps 120 branches 49% CPU	49 Mbps 120 branches 58% CPU
Cisco 7200 VXR NPE-400			
Starting condition	27 Mbps 80 branches 32% CPU	28 Mbps 80 branches 32% CPU	44 Mbps 80 branches 37% CPU
During failover	Failure	41 Mbps 120 branches 46% CPU	56 Mbps 120 branches 50% CPU

The same test was then performed with 240 branch offices aggregated to two head-end devices. All 120 branches from the failed head end successfully failed over to the single surviving head end. In this test, the network fully converged after approximately 22 seconds for the 7200 NPE-400 and 24–26 seconds for the 7140 and 7200 NPE-300.

The starting and failover traffic/tunnel aggregation conditions are shown in Table 2-2:

Table 2-2 Two head end Failover Scenario IPSec/GRE

	Head End 1	Head End 2
Cisco 7140		
Starting condition	17 Mbps 120 branches 28% CPU	16 Mbps 120 branches 30% CPU

Table 2-2 Two head end Failover Scenario IPSec/GRE

	Head End 1	Head End 2
During failover	Failure	33 Mbps 240 branches 58% CPU
Cisco 7200 VXR NPE-300		
Starting condition	18 Mbps 120 branches 28% CPU	17 Mbps 120 branches 28% CPU
During failover	Failure	35 Mbps 240 branches 52% CPU
Cisco 7200 VXR NPE-400		
Starting condition	21 Mbps 120 branches 28% CPU	21 Mbps 120 branches 25% CPU
During failover	Failure	42 Mbps 240 branches 44% CPU

In both scenarios, the failed head-end device was then powered back on, resulting in the network re-converging in less than two seconds. The IPSec tunnels re-established a few at a time as their corresponding SAs were renegotiated. The last IPSec tunnels re-established connectivity after 1.5 to 2 minutes.

Subsequent failover testing has been performed with the Cisco 3745 router and AIM II as head-end devices and with the 7200 VXR with the NPE-G1 processor engine and the VPN Accelerator Module (VAM) as the encryption accelerator, and up to 500 tunnels. The complete failover event lasted 32 seconds after the head-end device was failed. During the re-convergence, when the failed head end was restored, the convergence of each branch device took approximately two seconds each, with the total time for re-convergence at about 5.5 minutes. These results are presented in Table 2-3 along with the resulting CPU utilization percentages:

Table 2-3 Two Head End Failover Scenario Subsequent Testing

	Head End 1	Head End 2
Cisco 3745	IOS ver. 12.2(13)T	IOS ver. 12.2(13)T
Starting condition	4.2 Mbps 30 branches 33% CPU	4.4 Mbps 30 branches 34% CPU

Table 2-3 Two Head End Failover Scenario Subsequent Testing (continued)

	Head End 1	Head End 2
During failover	Failure	8.8 Mbps 60 branches 73% CPU
Cisco 3745	IOS ver. 12.2(13)T	IOS ver. 12.2(13)T
Starting condition	3.6 Mbps 60 branches 37% CPU	3.8 Mbps 60 branches 45% CPU
During failover	Failure	7.7 Mbps 120 branches 80% CPU
Cisco 7200 VXR NPE-G1	IOS ver. 12.2(13)S	IOS ver. 12.2(13)S
Starting condition	45.9 Mbps 125 branches 39% CPU	45.7 Mbps 125 branches 38% CPU
During failover	Failure	79.8 Mbps 250 branches 77% CPU
Cisco 7200 VXR NPE-G1	IOS ver. 12.2(13)S	IOS ver. 12.2(13)S
Starting condition	37.5 Mbps 250 branches 43% CPU	35.6 Mbps 250 branches 43% CPU
During failover	Failure	45.7 Mbps 500 branches 84% CPU

After a failure, the total traffic levels through the surviving router may be somewhat lower that the total traffic through the head ends with all of them up. This is because of the normal TCP back off process.

Solution Two—Failover and Convergence Performance

Failover and convergence testing has not been performed with Solution Two. However, because DMVPN is GRE-based and uses a routing protocol for convergence, there is no reason to believe that results with DMVPN configurations would be dramatically different from the results shown for Solution One. In fact, because testing comparing DMVPN with Point-to-Point GRE on the various head-end platforms shows that DMVPN offers performance improvements over Solution One, it is safe to assume that the results shown for failover and convergence in Solution One are conservative for Solution Two.

Solution Three—Failover and Convergence Performance

Exhaustive failover and convergence testing has not been performed with Solution Three. While this testing is planned, several considerations must be taken into account with this solution. In addition to the time needed for the HSRP process to discover that its primary router has failed, because there is only a single IPSec tunnel established, IPSec must re-negotiate IKE and IPSec SAs with the standby router, which now "owns" the standby group address. For a network with a large number of peers, this process can take several minutes. This requirement is not necessary when IPSec stateful SA failover can be used.

Testing results are shown in Table 2-4.

Table 2-4 Two Head End Failover, IPSec/DPD/RRI

	Head End 1	Head End 2
Cisco 7200 VXR NPE-G1	IOS ver. 12.2(13)S	IOS ver. 12.2(13)S
Starting condition	81 Mbps 250 branches 64% CPU	0 Mbps 0 branches 0% CPU
During failover	Failure	81 Mbps 250 branches 64% CPU
Cisco 7200 VXR NPE-G1	IOS ver. 12.2(13)S	IOS ver. 12.2(13)S
Starting condition	79 Mbps 500 branches 68% CPU	0 Mbps 0 branches 0% CPU
During failover	Failure	79 Mbps 500 branches 68% CPU

After completion of the test, the peers renegotiated SAs with their primary head end via the **HSRP preempt** command. Both the failover and renegotiation processes took approximately 3.5 minutes to complete with the 250 tunnel scenario and 5.5 minutes to complete with the 500 tunnel test.

Additional Design Considerations

This section describes additional design considerations when deploying a site-to-site VPN solution.

It includes the following topics:

- Management, page 2-29

Security

In planning for deployment of a site-to-site VPN topology, it is necessary to consider the integration of enterprise network security functions. Various enterprise security components complement and enhance the VPN solution.

For more information on how to integrate these essential security components, see the Cisco SAFE security blueprint and seminar series. Cisco SAFE documentation can be found at the following URL: http://www.cisco.com/go/safe.

Split Tunneling

Split tunneling is the process by which packets being transmitted from a site can be either protected by IPSec or unprotected, depending upon their destination. When split tunneling is configured for a branch site, that site must be protected by a stateful firewall.

At this time, split tunneling has not been addressed within this design.

Multicast

The popularity of multimedia applications such as video has led many network administrators to support multicast traffic on their networks. VPNs can also support these applications.

IPSec supports only tunneling of unicast IP traffic, so it is necessary to implement GRE in conjunction with IPSec to support multicast. See section Solution One (IPSec with GRE)—Design Recommendations, page 2-7 or Solution Two (DMVPN)—Design Recommendations, page 2-13 for options for supporting multicast traffic over a VPN. Solution One is recommended when multi-protocol and/or multicast support is needed; Solution Two is recommended when multicast support is needed. Both solutions also support routing protocols. For deployments without these specific requirements, Solution Three may be used instead.

Multicast traffic is not currently supported by most firewalls. This would require the termination of the IPSec tunnels on the inside interface of the firewall.

IPSec Interactions with Other Networking Functions

Because IPSec hides the packet and increases the packet size, interactions with other networking functions must also be taken into consideration. The following sections discuss various aspects to consider when deploying site-to-site IPSec-based VPNs.

Routing Protocols

All IP routing protocols use either broadcast or multicast as a method of transmitting routing table information. Because IPSec does not support either broadcast or multicast, this design guide recommends using GRE as a tunneling method to overcome this limitation. See section Solution One (IPSec with GRE)—Design Recommendations, page 2-7 and section Solution Two (DMVPN)—Design Recommendations, page 2-13. These sections detail the recommendations specific to the use of IPSec in combination with GRE.

Solution One is the recommendation when multi-protocol or multicast support is needed, or when routing protocol support is necessary. Solution Two is recommended when multicast and routing protocol support is needed. For deployments without these specific requirements, Solution Three may be used instead. See section Using a Routing Protocol across the VPN, page 2-11 for more information on running a routing protocol across a VPN.

Network Address Translation and Port Address Translation

Although Network Address Translation (NAT) and Port Address Translation (PAT) can result in an added layer of security and address conservation, they both present challenges to the implementation of an IPSec VPN. ISAKMP relies on an individual IP address per peer for proper operation. PAT works by masquerading multiple peers behind a single IP address.

IPSec NAT Traversal (NAT-T) introduces support for IPSec traffic to travel through NAT or PAT points in the network by encapsulating IPSec packets in a UDP wrapper, which allows the packets to travel through NAT devices. NAT-T was first introduced in Cisco IOS Software Release 12.2(13)T, and is auto-detected by VPN devices. There are no configuration steps for a Cisco IOS router running this release or later. If both VPN devices are NAT-T capable and a NAT device lies in the crypto path, NAT-T is auto-detected and auto-negotiated.

Dynamic Host Configuration Protocol

For a host at a remote site to be able to use a Dynamic Host Configuration Protocol (DHCP) server over an IPSec tunnel at a central site, an IP helper address must be configured on the router interface associated with the host.

One drawback of this approach is that if connectivity to the central site is lost, a host at a remote site may not receive an IP address. This can cause the host to be unable to communicate with other hosts on its local network.

A Cisco IOS router may also be configured to act as a standalone DHCP server.

Service Provider Dependencies

VPNs inherently rely on one or more service providers to provide Internet service to the head end and branch offices to deploy the network. Choosing a service provider is thus a critical element of deploying a VPN. Many factors have to be considered including cost, services available, reliability, and the expected geographical coverage of the customer VPN.

At a minimum, the enterprise should have a service level agreement (SLA) with the service provider that outlines the critical service elements of their VPN. These factors include availability, bandwidth, and latency.

When an enterprise must use multiple service providers to cover their branch locations, obtaining the desired level of end-to-end VPN service can be more complex and problematic. This can be especially critical in the case where the customer has mission-critical applications that are delay-sensitive. Whether the customer wants to run latency-sensitive applications such as voice and video over IP across the VPN in the future must also be considered. For this reason, Cisco recommends seeking an SLA with a single service provider that can guarantee a level of end-to-end service for the enterprise locations.

Another issue is that some Internet service providers for DSL and cable services implement policing of traffic for residential class service. This means that protocols such as IPSec may be blocked unless there is a subscription to business class service. For more information about residential class services and

other specifics of teleworker designs, see the *Business Ready Teleworker SRND* at the following URL: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79d.pdf

Management

Cisco coordinates all of its VPN products through management systems that provide such status information as device availability and throughput with products such as VPN/Security Management Solution (VMS) and IP Solution Center (ISC).

For more information on how to implement network management over IPSec tunnels, see the Cisco SAFE security blueprint and seminar series. Cisco SAFE documentation can be found at the following URL: http://www.cisco.com/go/safe.

Selecting Solution Components

This chapter presents the steps to selecting Cisco products for a deployable VPN solution, starting with sizing the head end, and then choosing Cisco products that can be deployed for head-end devices. It concludes with product sizing and selection information for branch-end devices.

This chapter includes the following topics:

Scalability Testing Methodology

This section describes how the performance data presented in the subsequent section was derived for each product.

As shown in the diagram in Scalability Test Bed Network Diagram, page A-1, the scalability test bed initially included 240 branch offices aggregated to three head-end devices (aggregation to two head ends was also tested). The head ends consisted of the Cisco 7100 and 7200 series VPN router products (see Head End Devices, page 3-5 for exact models tested). Later testing scaled the branch offices to 1040 devices. The branch offices routers consisted of Cisco VPN router products from the 800, 1700, 2600, and 3600 series (see Branch Site Devices, page 3-11 for exact models tested). Later testing incorporated the Cisco Integrated Services Router (ISR) models: 1800, 2800, and 3800 series.

Head-end products were evaluated with hardware-accelerated encryption installed, while, initially, branch products were evaluated with both software-based encryption and hardware-accelerated encryption. 3DES was selected as the encryption standard and SHA-1 as the hash method. In later testing, for example with the ISR models, tests compared router performance with the integrated crypto accelerator with that derived with the AIM encryption modules.

For head end testing, each branch router was provisioned with two IPSec/GRE tunnels (primary and secondary) back to two different head ends. EIGRP was configured as the routing protocol to distribute routes from the head ends to the branches. The testing was conducted with a fully summarized network configuration.

Traffic flows were then established using the NetIQ Chariot™ testing tool. The mix of traffic was approximately 35 percent UDP and 65 percent TCP, with packet sizes of 64 bytes (RTP), 100 bytes (DNS), and 1400 bytes (FTP). Traffic rates were increased to find the throughput points on each product type where the CPU utilization reached 50 percent for head ends, and 65 percent for branch products, without packet loss.

An initial finding was the effect of IPSec packet fragmentation on the throughput of the head-end devices (see Minimizing Packet Fragmentation, page 2-5 for more information on the performance impact and mitigation strategies). Therefore, the testing was conducted both with fragmentation occurring in the network as well as with no fragmentation (MTU was set to 1400 on the test endpoints). In later tests, testing with fragmentation occurring in the network was discontinued, because it became a design recommendation to avoid such fragmentation.

Individual product throughput performance data is presented in Cisco VPN Routers for Head Ends, page 3-8 for head-end products, and Cisco VPN Routers for Branch Sites, page 3-12 for branch products.

In addition to throughput testing, failover testing was also conducted. See Comparing Failover and Convergence Performance, page 2-22 for more information on the failover test scenarios.

All scalability testing for this design guide revision was obtained using IPSec tunnel mode in Solutions One and Three; therefore, the throughput results may differ in transport mode. Solution Two, DMVPN, is optimized by the use of transport mode, so all test results for DMVPN uses IPSec transport mode.

Subsequent Testing

This section includes the following topics:

To speed solution testing and to provide accurate information in a more timely fashion, the site-to-site VPN testing was combined with Voice and Video Enabled IPSec VPN (V3PN) solution testing. This entailed changing the traffic mix to more closely emulate VoIP traffic. Because of the VoIP traffic in the V3PN solution, this solution uses a slightly different traffic profile than what would normally be encountered in a data-only enterprise network. These tests also yielded results that are more conservative than what would ordinarily be obtained with the previous testing methods. Therefore, a network carrying data-only traffic has a larger average packet size than what was used in the testing, and routers in this network achieve better performance.

New Traffic Mix

Enterprise traffic was simulated by using a variety of traffic mixes and packet sizes. IMIX is available in many different forms. For V3PN testing, samples were taken from several enterprise verticals; these include health care and the insurance industry. Profiles were created to simulate these packet mixes with the Chariot test tool used by Cisco labs. The flows generated match very closely the traffic patterns found in the sampled enterprise networks.

The single change to these flows in the current and future rounds of testing are the inclusion of simulated VoIP flows. Although these are not actual VoIP flows, periodic checks were made with real VoIP flows to ensure that the results obtained are accurate. The VoIP flows are characterized by smaller packet sizes, which lower the overall average packet size handled by each router. The greater proportion of smaller packets causes a higher CPU utilization on the routers performing encryption.

The most noticeable impact of this new traffic profile is that results shown here are conservative for a data-only network. An increase in the number of small packets in the traffic mix drives the overall packets per second (pps) rate up, which in turn drives the router CPU higher. Cisco attempted to test to three different CPU utilization levels: 50 percent, 65 percent, and 80 percent. With the new traffic mix, these CPU utilization levels are reached earlier than they normally would be because of the higher pps rate.

Tunnel Quantity Affects Throughput

As tunnel quantities are increased, the overall throughput tends to decrease. When a router receives a packet from a different peer than the one whose packet was just decrypted, a lookup based on the security parameters index of the new packet must be performed. The new transform set information and negotiated key of the packet is then loaded into the hardware decryption engine for processing. Having traffic flowing on a larger numbers of SAs tends to negatively affect throughput performance. In the test results shown, head-end devices have multiple tunnels established, with traffic distributed as evenly as possible across each active tunnel. When it was not possible to distribute the traffic evenly, it is noted. In test results for Solutions One and Three, branch-end devices are shown with either one or two tunnels configured.

GRE Encapsulation Affects Throughput

The configuration of GRE negatively affected router encryption throughput. In addition to the headers that are added to the beginning of each packet, these headers also must be encrypted. The GRE encapsulation process itself affects total CPU utilization, which is approximately ten percent higher if GRE encapsulation has been configured than with IPSec alone.

Routing Protocols Affect Throughput

Throughput is also affected by running a routing protocol. Router processing of keepalives and the maintenance of a routing table uses a certain amount of CPU time, which varies with the number of routing peers and the size of the routing table. This guide attempts to conclude the number of permissible routing peers based on a safe number for the total network size.

How the Test Results are Presented

The targeted CPU utilization for a router deployment is always the subject of debate. This guide attempts to provide a representative range of CPU utilizations on the higher side of a normal network deployment. These utilizations are 50 percent, 65 percent, and 80 percent. While the high number (80 percent) is not recommended during normal operation, this number is provided to enable an engineer to see what traffic levels can be handled by a router in a failover scenario.

Deploying Hardware-Accelerated Encryption

This section includes the following topics:

The scalability testing performed as part of the VPN solution development indicates a strong need for hardware-accelerated encryption to achieve predictable performance results. For head-end devices, all throughput results presented in this design guide, and the recommended architecture, assume that hardware-acceleration is implemented.

For branch-end devices, both software-based encryption and hardware-accelerated encryption were evaluated. In the case of software-based encryption, throughput results were much lower than with hardware-accelerated encryption (up to an 80 percent decrease in performance).

For these reasons, Cisco strongly recommends hardware acceleration in all devices performing encryption. This is especially true in the case of the following:

- 3DES encryption is being implemented
- Significant data throughput requirements exist
- Multi-service applications, such as VoIP, are to be run over the VPN

Head End Encryption Acceleration Options

Cisco has different names for the acceleration modules of the 7200 and 7100 families. The Integrated Services Adapter (ISA) may be used on the 7100 or 7200. The Integrated Services Modules (ISM) may be used on the 7100. These offer comparable performance. Multiple cards (dual ISA on a 7200, ISM+ISA on 7100) can be used to increase encryption throughput.

The Cisco VPN Acceleration Module (VAM), and its successor the VAM2, are additional high-performance VPN encryption options. These modules, in the form of a port adapter (PA), are available for the 7200 series. They can also be used in tandem (two VAMs per chassis) to increase performance. When dual VAMs are used, performance increases when they are installed in the same chassis bus (for instance, in Slots 1 and 3, or in Slots 3 and 5). In the Cisco switching family, the VPNSM is available for the Catalyst 6500 and Cisco 7600 family.

Hardware Encryption Acceleration Options for 2600, 3600, and 3700 Routers

The hardware acceleration options for the 2600, 3600, and 3700 series can be somewhat confusing. Table 3-1 shows the options available for some of these platforms:

Table 3-1 AIM Options

	AIM-BP	AIM-MP	AIM-EP	AIM-HP	AIM-EPII	AIM-HPII
Cisco 26xx	X		X			
Cisco 26xx-XM	X		X			
Cisco 3620/40		X				
Cisco 2691			X		X	
Cisco 3660				X		

Table 3-1 AIM Options (continued)

	AIM-BP	AIM-MP	AIM-EP	AIM-HP	AIM-EPII	AIM-HPII
Cisco 3725			X		X	
Cisco 3745				X		X

The recommended deployment for the 1700 series with these solutions also includes hardware acceleration. The 1700s are configurable with the VPN module for encryption acceleration.

The Cisco 800 series of routers that are recommended have built-in hardware acceleration. These models are the 831 dual Ethernet, the 836 ADSL over ISDN, and the 837 ADSL router. Other models of the 800 series without hardware encryption are no longer recommended for these applications.

The ISR models are configurable to use either an integrated encryption module or a separately-purchased AIM. The AIM option for the 1800 series is an AIM-VPN/BPII-PLUS, and the AIM option for the 2800 series is an AIM-VPN/EPII-PLUS. The 3800 series can be configured with either the AIM-VPN/EPII-PLUS or the AIM-VPN/HPII-PLUS.

See Head End Devices, page 3-5 and Branch Site Devices, page 3-11 for more detailed performance data that supports these recommendations.

Head End Devices

This section includes the following topics:

In Solutions One and Two, the head-end devices are responsible for the following:

- Originating/terminating IPSec encapsulated GRE tunnels from the branch sites
- Running a routing protocol inside GRE tunnels to advertise internal routes to branches
- Providing redundancy to eliminate the possibility of a single point of failure

In Solution Two, the head-end devices are responsible for the following:

- Serving as an NHRP cache and server to the branch sites
- Serving as a next-hop server, both to the branch sites and to other head ends

In Solution Three, the head-end devices are responsible for the following:

- Originating/terminating ISAKMP and IPSec SAs from the branch sites
- Sending/receiving IKE keepalives to verify the state of the SAs to the branches
- Installing routes to the branch networks via RRI, replacing the need for a dynamic routing protocol

The next sections identify factors to take into account in sizing the head-end devices or sites.

Sizing the Head End

It is important to size the head end correctly before choosing the devices to deploy. This ensures that the overall network can support the intended (and possibly future) traffic profiles that the enterprise desires to run over the VPN.

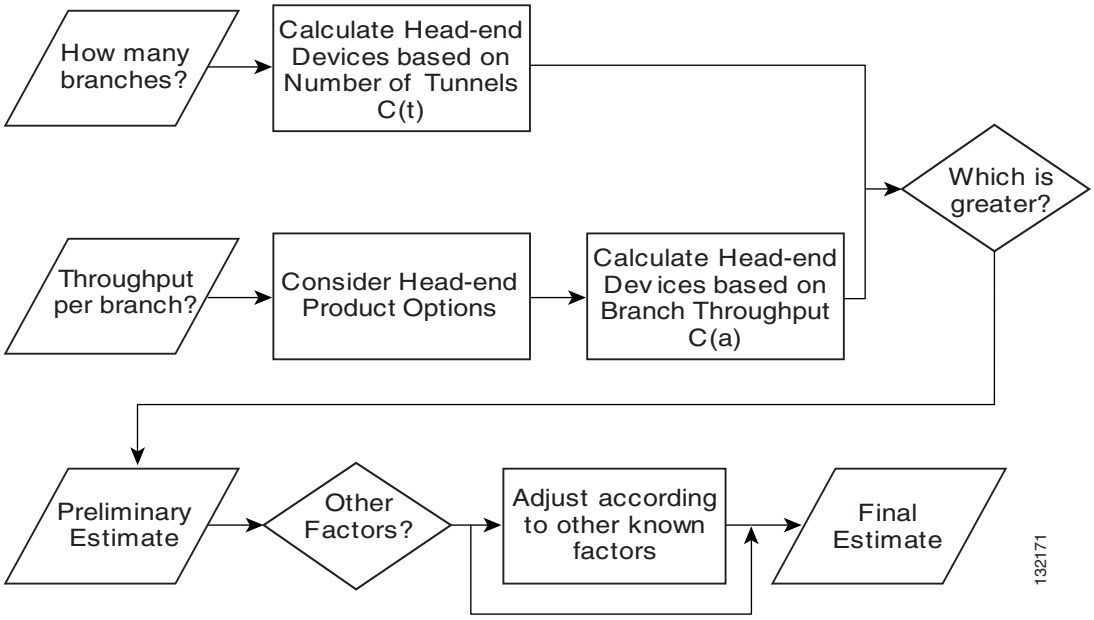
The following two critical factors must be considered when sizing the head end:

- How many branch offices need to be connected to the head end? This information provides the number of primary tunnels requiring aggregation.
- What is the expected traffic profile, including the average pps and bits per second (bps) throughput rates for each branch office? This information provides the aggregated data throughput required across the VPN.

Either or both of these factors can be the limiting factor in sizing the head end; therefore, both must be considered together.

The decision flow shown in Figure 3-1 can be applied to size the head end.

Figure 3-1 Head End Sizing Decision Flow



This design assumes a level of redundancy at the head end to handle a failover scenario.

In Solution One (IPSec with GRE), the total number of tunnels per head-end device (assuming a Cisco 7200 VXR with NPE-G1 and VAM or VAM2) should be kept below 500. In Solution Two (DMVPN), the total number of branch ends aggregated on a head-end device should be limited to 700, with 350 aggregated on each of two mGRE interfaces; this, again, assumes a Cisco 7200 VXR with NPE-G1 and VAM or VAM2. In Solution Three, scalability testing was conducted for up to 1040 tunnels, with the same head-end device and dual VAM2s. All testing assumes an IP unicast, fully summarized network configuration.

Based on the number of branch offices, the required number of head-end devices, C(t), can be sized with the following algorithm:

N = total number of branch offices

T = total number of tunnels = N x 2 (for primary and secondary tunnels)

Y = total number of tunnels recommended per solution (500, 750, 1040)

C(t) = (T /Y) rounded up to next full integer + 1 (for resiliency)

For example, an enterprise with 950 branch offices planning a Solution One design would require five head-end devices, as follows:

N = 950

T = 1900

C(t) = 1900/500 rounded up + 1 = 5

The next step is to obtain traffic profile data from the customer that indicates expected average throughput (pps and bps) for each branch office and head-end device.

The aggregate throughput is calculated by adding up all of the throughput estimates for all branch offices.

At this point, it is necessary to consider the available head-end devices and the maximum throughput supported by each. The Cisco 7140 and 7200 VXR routers or the Catalyst 6500/Cisco 7600 are the preferred platforms for use as IPSec VPN head-end devices. Each of these routers has a range of options for interfaces as well as the ability to configure hardware-accelerated encryption.

Next, divide the aggregate throughput requirements by the throughput value for each respective platform value in Table 3-2, Table 3-3**,** and Table 3-4 below. This provides the number of head-end devices required, based on aggregate throughput:

A = sum of throughput estimates for each branch office (that is, the aggregate)

H = single head-end device throughput

C(a) = A/H, rounded up to nearest full integer, + 1 for resiliency

For example, an enterprise with 300 branch offices, each having throughput requirements of 500 kbps, and planning a Solution One design, would require four head-end devices, as follows:

A = 300 branches @ 500 kbps = 300 x 0.5 Mbps = 150 Mbps

H = 66 Mbps (for Cisco 7200VXR router)

C(a) = 150/66 (rounded to next nearest integer) + 1 = 4

Compare the number of head-end devices calculated based on number of tunnels, C(t), to the number based on aggregate throughput, C(a). The greater of the two numbers is required to support the design.

As the number of tunnels increases, there is a corresponding decrease in encrypted throughput. This means that a design that has a uniformly distributed traffic load from branch offices across many tunnels requires more CPU than a design where the majority of traffic load is generated from a subset of the total tunnels being aggregated.

In addition to the two critical factors identified above, the following factors must also be considered at this point:

- Given the current network topology and traffic profile of the customer, what is the current CPU utilization on each distribution router, and how many branch offices are connected to each distribution router? This information provides a baseline of expected CPU utilization levels.
- What are the aggregate WAN sizes for each respective branch? How the aggregate WAN speed is subdivided into a number of tunnels affects the overall number of tunnels that can be supported in this design. As discussed previously, as the number of tunnels increases, there is a corresponding decrease in throughput (or an increase in CPU utilization).

- What other applications/protocols does the customer intend to run across the VPN? Multi-protocols perform differently in Cisco IOS compared to unicast IP. In the scalability testing performed to date, multi-protocols have not been comprehensively evaluated.

The result is that the number of head-end devices may need to be adjusted upward after these additional factors are considered.

Cisco recommends that head-end devices be chosen so that CPU utilization does not exceed 50 percent. This ensures that the device has enough performance left over to deal with various events that take place during the course of normal network operations, including network re-convergence in the event of a failure, re-keying IPSec SAs, and bursts of traffic seen in a normal operating network.

After initial deployment and testing, it may be possible to run head-end devices at CPU utilization levels higher than 50 percent (60–65 percent, for example). However, this design guide conservatively recommends staying at or below 50 percent, and therefore the throughput results presented are generally chosen at the 50 percent level.

Cisco VPN Routers for Head Ends

Cisco VPN routers suitable for head end deployments include the 7100 series, the 7200 series, the 3700 series, the 3600 series, and the Catalyst 6500/Cisco 7600 platform (using the VPNSM). Specific platforms were selected from within each product family for evaluation.

All products were configured with hardware-accelerated encryption enabled. Each product supports several hardware-accelerated encryption options. For example, both the 7100 and 7200 can be configured with one or two ISA/ISM cards; the 7200 can be configured with the newer VAM or VAM2. The 3600 series can be configured with different AIM performance levels, including Base (AIM-BP), Medium (AIM-MP), or High (AIM-HP), depending on the platform.

The configurations selected for scalability testing, along with the throughput thresholds attained (at 50–55 percent CPU utilization and 500, 700, or 1040 tunnels configured) are shown in Table 3-2, Table 3-3, and Table 3-4. As mentioned earlier in Subsequent Testing, page 3-2, the site-to-site VPN testing was combined with the VoIP testing to save time. The results produced by these tests are more conservative than those that would ordinarily have been obtained because of the smaller average packet size of the VoIP flows. As a rule of thumb, these results may always be increased to get results consistent with the larger average packet sizes.

Table 3-2 Head End Products Throughput—Solution One (IPSec with GRE)

Router Platform	Hardware Acceleration	# of Tunnels Active	Throughput	CPU % Utilization
Cisco 7200 w/NPE-G1	SA-VAM	148	44.8 Mbps	46%
Cisco 7200 w/NPE-G1	SA-VAM	196	66.3 Mbps	65%
Cisco 7200 w/NPE-G1	SA-VAM	240	80 Mbps	80%
Cisco 7200 w/NPE-G1	SA-VAM	500	78.1 Mbps	80%
Cisco 6500 w/MSFC2	VPNSM	500	924 Mbps	NA
Cisco 3745	AIM-HPII	43	11.4 Mbps	50%
Cisco 3745	AIM-HPII	53	14 Mbps	62%
Cisco 3745	AIM-HPII	60	17.6 Mbps	72%

The effect described in Tunnel Quantity Affects Throughput, page 3-3 is visible in the results with the 7200 w/NPE-G1. At the 80 percent CPU mark, there is actually reduced throughput when 500 tunnels are active, as compared to 240 tunnels. It is also important to note that these limits were established during testing without IPSec fragmentation occurring in the network. See Minimizing Packet Fragmentation, page 2-5 for more information on the impact of fragmentation on VPN device performance and mitigation strategies. In addition, these results were obtained with the VoIP and enterprise traffic mix. The results produced are more conservative than what would ordinarily be obtained; for additional information on the testing, see Subsequent Testing, page 3-2.

Head End Products for Solution Two

Table 3-3 shows results for testing with a configuration for Solution Two (DMVPN) using a dual hub-dual DMVPN design. In the results shown for the 7200 VXR, the head end is aggregating and maintaining EIGRP neighbor relationships with 400 branch-end routers on each of two mGRE interfaces (a total of 800 EIGRP neighbors, which is beyond the design recommendation of 700). It is exchanging voice and data with the number of spokes shown in the "# of Tunnels Active" column and maintaining its routing protocol relationship with the others. In the case of the 3745, the head-end router maintains routing neighbor relationships with 200 EIGRP neighbors on a single mGRE interface, and exchanges encrypted voice and data with the number of spokes shown in the "# of Tunnels Active" column.

Table 3-3 Head End Products Throughput—Solution Two (DMVPN)

Router Platform	Hardware Acceleration	# of Tunnels Active	Throughput	CPU % Utilization
Cisco 7200 w/NPE-G1	SA-VAM	150	67.04 Mbps	53%
Cisco 7200 w/NPE-G1	SA-VAM	200	84.9 Mbps	68%
Cisco 7200 w/NPE-G1	SA-VAM	250	104.3 Mbps	82%
Cisco 3745	AIM-HPII	77	28.92 Mbps	50%
Cisco 3745	AIM-HPII	108	40.56 Mbps	62%
Cisco 3745	AIM-HPII	139	52.03 Mbps	72%

As with other test results shown in this chapter, these limits were established during testing without IPSec fragmentation occurring in the network. Furthermore, the traffic mix used includes VoIP streams, making the average packet size smaller than what would be seen in a data-only enterprise network. For additional information regarding the traffic mix, see Subsequent Testing, page 3-2.

Head End Products for Solution Three

Table 3-4 shows results for testing with a configuration for Solution Three: IPSec with DPD, RRI, and HSRP in place of IPSec with GRE and a routing protocol. The traffic mix used was that of the VoIP test. This traffic mix consists of packets with an average packet size smaller than what would normally be seen in an enterprise network, because of the inclusion of VoIP packets. Consequently, the results presented in Table 3-4 are more conservative than what could ordinarily be obtained. For additional information regarding the subsequent testing, see Subsequent Testing, page 3-2.

Table 3-4 Head End Products Throughput—Solution Three (IPSec with DPD, RRI and HSRP)

Head End Router Platform	Hardware Acceleration Option	# of Tunnels Active	Throughput	CPU % Utilization
Cisco 6500	VPNSM	1040	1.03 Gbps	N/A
Cisco 7200 w/NPE-G1	Dual SA-VAM	1040	106.7 Mbps	81%
Cisco 7200 w/NPE-G1	Dual SA-VAM2	1040	108.7 Mbps	77%
Cisco 7200 w/NPE-G1	Dual SA-VAM	250	83.9 Mbps	68%
Cisco 3745	AIM-HPII	53	15.1 Mbps	41%
Cisco 3745	AIM-HPII	60	17 Mbps	47%
Cisco 3745	AIM-HPII	95	28.69 Mbps	80%

As with results shown for Solutions One and Two, these results were determined during testing without IPSec fragmentation occurring in the network. The use of dual VAMs allows further scalability in Solution Three that would not be realized in Solutions One or Two. The VAM or VAM2 handles encryption processing, but does not accelerate GRE processing. In testing for Solutions One and Two, the router runs out of main CPU cycles in dealing with GRE overhead before the VAM runs out of processing power for encryption.

Other Cisco Products for the Head End

Several other Cisco products support IPSec VPN tunnel termination in a head end environment; for example, the VPN 3000 Concentrator series, and the Cisco PIX Firewall Series. The results for the Cisco PIX model 535 with the VAC Plus and 3080 with SEP and SEP/E are shown in Table 3-5.

Table 3-5 Other Head End Product Performance

Head End Router Platform	Hardware Acceleration Option	# of Tunnels Active	Throughput	CPU % Utilization
Cisco PIX 535	VAC Plus	240	67.9 Mbps	50%
Cisco PIX 535	VAC Plus	330	93.6 Mbps	66%
Cisco PIX 535	VAC Plus	435	122.9 Mbps	80%
Cisco PIX 535	VAC Plus	500	166 Mbps	89%
Cisco 3080	SEP	138	38.8 Mbps	80%
Cisco 3080	SEP-E	138	39.4 Mbps	52%

These products are only capable of supporting Solution Three (IPSec with DPD, RRI and HSRP). They are not capable of performing GRE encapsulation or running routing protocols. Remember that these are conservative results. For additional information regarding the subsequent testing, see Subsequent Testing, page 3-2.

Cisco PIX VPN Limitations

Firewall rules require traffic entering an interface on a firewall to exit that firewall through a different interface, in effect passing all the way through the device. As a firewall, the Cisco PIX products share this characteristic. A result of this feature is that firewall devices do not support branch site to branch site communications over site-to-site VPNs with a hub-and-spoke model. The traffic from a branch site must be passed completely through the PIX, and is subject to the rules specified in the firewall. This prevents communication between two branch sites using the PIX as an intermediary.

See the following links for more product information on the Cisco VPN 3000 and PIX series:

- http://www.cisco.com/warp/public/cc/pd/hb/vp3000/
- http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/

Branch Site Devices

This section includes the following topics:

In Solutions One and Two, the branch site devices are responsible for the following:

- Originating/terminating IPSec-encapsulated GRE tunnels from the head end
- Running a routing protocol inside of the GRE tunnels to advertise internal routes

In Solution Two, the branch site devices are also responsible for the following:

- Initiating NHRP entries with the head-end devices, so that they can build encrypted GRE tunnels back to the branch site
- Querying the head-end device for IP next-hop information, when spoke-to-spoke tunnel setup is required

In Solution Three, the branch site devices are responsible for the following:

- Originating/terminating ISAKMP and IPSec SAs from the head end
- Sending/receiving IKE keepalives to verify the state of the SAs to the head ends

The branch site device may also be responsible for forwarding DHCP requests to the central site, or even functioning as the DHCP server.

The next sections identify factors to consider when sizing the branch sites.

Sizing the Branch Site

The most important factor to consider when choosing a product for the branch office is the expected traffic throughput to the head end.

Other factors that should be considered include the following:

- What other features/functionality is the branch router providing (for example, WAN access, VoIP, Cisco IOS Firewall, and so on)?

- Different branch devices offer a range of features that accommodate various levels of growth. For example, the Cisco 3660 supports six modular slots and various WAN adapters, whereas the Cisco 2600 series supports only two slots.

Although the number of IPSec tunnels does not play as large a role in the branch device sizing, each branch site router must be able to terminate at least two IPSec-encapsulated GRE tunnels (primary and secondary) in Solutions One and Two, or two IPSec SAs, not encapsulated in GRE, in designs based on Solution Three.

The primary concern is the amount of traffic throughput along with the corresponding CPU utilization. Cisco recommends that branch devices be chosen so that CPU utilization does not exceed 65 percent. This ensures that the device has enough performance left over to deal with various events that take place during the course of normal network operations. The CPU on a branch-site router may run slightly higher than a head-end router because of the minimal routing convergence duties.

After initial deployment and testing, it may be possible to run branch-site devices at CPU utilization levels higher than 65 percent. However, this design guide conservatively recommends staying at or below 65 percent, and therefore the throughput results presented were chosen at the 65 percent level.

Cisco VPN Routers for Branch Sites

Cisco VPN routers suitable for branch site deployments include the 3700 series, the 3600 series, the 2600 series, the 1700 series, and the 800 series. More recently, the 3800, 2800, and 1800 ISR have been released. All recommended branch devices support hardware-accelerated encryption. The ISRs are configurable to work with either an integrated encryption module or with a separately purchased AIM.

Phase One Tests

Specific platforms were selected from within each product family for throughput comparison with hardware versus software encryption, and with fragmentation versus no fragmentation. Throughput results (taken at approximately 60–65 percent CPU utilization) are summarized in Table 3-6.

Table 3-6 Branch Site Device Throughput

Branch Router Platform	Hardware Acceleration Option	HW Encryption No Fragmentation	HW Encryption With Fragmentation[1]	SW Encryption No Fragmentation
Cisco 3660	AIM-HP	16.0 Mbps	14.0 Mbps	2.4 Mbps
Cisco 3640	AIM-MP	3.5 Mbps	2.6 Mbps	900 kbps
Cisco 3620	AIM-MP	1.8 Mbps	1.6 Mbps	480 kbps
Cisco 2651[2]	AIM-BP	2.8 Mbps	3.0 Mbps	960 kbps
Cisco 2621	AIM-BP	2.4 Mbps	2.5 Mbps	520 kbps
Cisco 2611	AIM-BP	2.0 Mbps	1.9 Mbps	380 kbps
Cisco 1750	VPN Module	2.6 Mbps	2.5 Mbps	560 kbps
Cisco 805	N/A	N/A	N/A	100 kbps

1. Fragmentation tests were performed with approximately 60 percent of packets fragmented, with the exception of the 2621 at approximately 30 percent fragmentation.
2. Because of limitations in the scalability test, the 2651 was not tested beyond 2.2 Mbps. At this throughput rate, the 2651 experienced 43 percent CPU utilization. It is believed that the 2651 can handle additional throughput at higher line rates.

Subsequent testing of branch-site devices has been completed with the enterprise VoIP traffic mix, with hardware-accelerated encryption, and with no fragmentation. This traffic mix has a smaller average packet size than would normally be seen in a data-only enterprise network. The results of using this traffic mix are the more conservative numbers produced. For additional information on this testing, see Subsequent Testing, page 3-2.

Solution One Test Results

In subsequent testing, all testing was performed with hardware-accelerated encryption, and a range of results, corresponding to different CPU levels, were collected for each platform. These results for the branch sites devices in Solution One are shown in Table 3-7.

Table 3-7 Branch Site Device Throughput—Solution One (IPSec with GRE)

Branch Router Platform	Hardware Acceleration Option	Throughput (bps)	Throughput (pps)	CPU % Utilization
Cisco 3745	AIM-HPII	16.5 Mbps	7,597 pps	32%
Cisco 3745	AIM-HPII	33.1 Mbps	15,184 pps	61%
Cisco 3745	AIM-HPII	41.9 Mbps	19,055 pps	75%
Cisco 3725	AIM-EPII	6.3 Mbps	2,997 pps	27%
Cisco 3725	AIM-EPII	16.7 Mbps	7,626 pps	60%
Cisco 3725	AIM-EPII	25.2 Mbps	11,459 pps	86%
Cisco 3660	AIM-HPII	6.3 Mbps	2,994 pps	35%
Cisco 3660	AIM-HPII	16.4 Mbps	7,582 pps	74%
Cisco 3660	AIM-HPII	20.2 Mbps	9,197 pps	88%
Cisco 2691	AIM-EPII	4.9 Mbps	2,282 pps	26%
Cisco 2691	AIM-EPII	6.4 Mbps	3,014 pps	33%
Cisco 2691	AIM-EPII	16.8 Mbps	7,634 pps	79%
Cisco 831	Included	410 kbps	250 pps	31%
Cisco 831	Included	812 kbps	392 pps	59%
Cisco 831	Included	1.2 Mbps	505 pps	85%

Solution Three Testing

Applying the same test strategy as explained in Solution One, results were collected for the branch site devices using Solution Three. These results are shown in Table 3-8.

Table 3-8 Branch Site Device Throughput—Solution Three (IPSec with DPD, RRI and HSRP)

Branch Router Platform	Hardware Acceleration Option	Throughput (bps)	Throughput (pps)	CPU % Utilization
Cisco 3745	AIM-HPII	27.51 Mbps	13,205 pps	50%
Cisco 3745	AIM-HPII	38.6 Mbps	18,058 pps	65%
Cisco 3745	AIM-HPII	46.67 Mbps	23,105 pps	80%
Cisco 3725	AIM-EPII	16.89 Mbps	7,874 pps	52%

Table 3-8 Branch Site Device Throughput—Solution Three (IPSec with DPD, RRI and HSRP) (continued)

Branch Router Platform	Hardware Acceleration Option	Throughput (bps)	Throughput (pps)	CPU % Utilization
Cisco 3725	AIM-EPII	20.96 Mbps	9,916 pps	67%
Cisco 3725	AIM-EPII	26.11 Mbps	12,890 pps	82%
Cisco 2691	AIM-EPII	10.25 Mbps	4,759 pps	48%
Cisco 2691	AIM-EPII	15.27 Mbps	7,108 pps	65%
Cisco 2691	AIM-EPII	18.32 Mbps	8,560 pps	80%
Cisco 2651XM	AIM-BPII	2.46 Mbps	1,178 pps	49%
Cisco 2651XM	AIM-BPII	2.96 Mbps	1,523 pps	63%
Cisco 2651XM	AIM-BPII	4.02 Mbps	1,923 pps	76%
Cisco 1760	1700VPN	2.04 Mbps	942 pps	55%
Cisco 1760	1700VPN	2.54 Mbps	1,192 pps	65%
Cisco 1760	1700VPN	2.68 Mbps	1,465 pps	78%
Cisco 831	Included	867 kbps	413 pps	50%
Cisco 831	Included	1.16 Mbps	541 pps	65%
Cisco 831	Included	1.41 Mbps	665 pps	80%

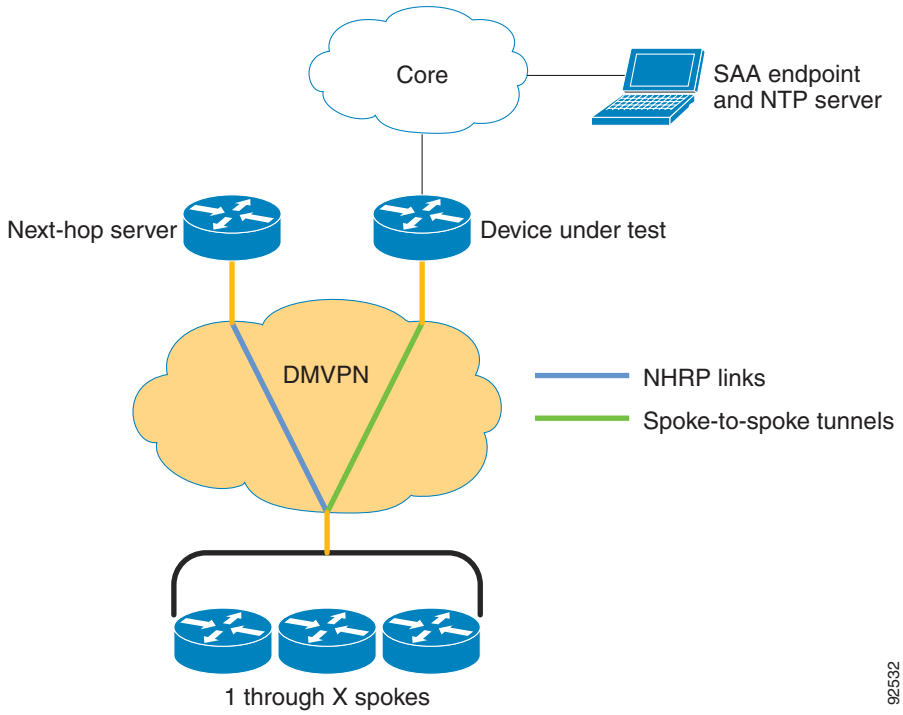
Solution Two Testing

As Solution Two (DMVPN) was developed, two changes to test strategy occurred in the test labs.

- Customer usage of branch site routers indicated that most of these devices are required to perform various security or packet scrutiny functions, in addition to simple WAN termination, routing protocol, GRE tunnel maintenance, and encryption/decryption functions. To make test scenarios more realistic, Solution Two tests included the use of the following features:
  - Outbound firewall inspection
  - Inbound and outbound ACLs
  - NAT
- Because branch site routers may have multiple tunnels active at a time (if spoke-to-spoke tunnels are permitted in the design), part of the test strategy was to establish what would be considered a “safe” maximum number of tunnels, as well as determining GRE and encryption performance on some number of those tunnels.

The Solution Two scalability test bed is shown in Figure 3-2.

Figure 3-2 Solution Two Scalability Test Bed



The routers tested are inserted in turn into the "Device Under Test" location. Different numbers of "1 through X" spokes are brought into the test bed. These routers each open one IPSec SA (or tunnel) to the next-hop server, which supplies them the NBMA address of the device under test (DUT). Each spoke opens a spoke-to-spoke tunnel to the DUT. Tunnels are kept alive via Service Assurance Agent (SAA) and Network Time Protocol (NTP).

Traffic is then generated through a certain number of these tunnels to assess the DUT router performance in terms of pps and bps, as it maintains what is considered its "safe maximum" number of tunnels. Each spoke router outside interface (other than the DUT) is shaped to 192 kbps; it is then known that the DUT is aggregating (192 kbps x the number of tunnels shown).

Performance results for the branch-site devices in Solution Three are shown below. Table 3-9 shows results for the ISR platforms, allowing comparison of the integrated hardware encryption card with the add-on AIM.

Table 3-9 Branch Site Device Throughput, DMVPN, ISR Platforms

Branch Router Platform/HW Acceleration Option	# Tunnels Passing Data/Active	Throughput (bps)	Throughput (pps)	CPU % Utilization
Cisco 3845 Integrated	66/400	21.73 Mbps	10,879 pps	49%
Cisco 3845 Integrated	90/400	29.2 Mbps	14,508 pps	62%
Cisco 3845 Integrated	114/400	37.15 Mbps	18,147 pps	81%
Cisco 3845 AIM-HPII+	76/400	25.91 Mbps	12,419 pps	51%
Cisco 3845 AIM-HPII+	107/400	36.0 Mbps	17,140 pps	62%
Cisco 3845 AIM-HPII+	135/400	45.23 Mbps	21,411 pps	78%

Table 3-9 Branch Site Device Throughput, DMVPN, ISR Platforms (continued)

Branch Router Platform/HW Acceleration Option	# Tunnels Passing Data/Active	Throughput (bps)	Throughput (pps)	CPU % Utilization
Cisco 3825 Integrated	49/300	16.13 Mbps	8,081 pps	49%
Cisco 3825 Integrated	68/300	22.18 Mbps	11,003 pps	64%
Cisco 3825 Integrated	89/300	28.81 Mbps	14,196 pps	80%
Cisco 3825 AIM-HPII+	57/300	19.77 Mbps	9,466 pps	51%
Cisco 3825 AIM-HPII+	81/300	27.21 Mbps	12,792 pps	64%
Cisco 3825 AIM-HPII+	104/300	34.78 Mbps	16,484 pps	78%
Cisco 2851 Integrated	33/100	11.38 Mbps	5,249 pps	53%
Cisco 2851 Integrated	43/100	14.67 Mbps	6,763 pps	67%
Cisco 2851 Integrated	54/100	18.48 Mbps	8,459 pps	80%
Cisco 2851 AIM-EPII+	40/200	13.89 Mbps	6,500 pps	54%
Cisco 2851 AIM-EPII+	54/200	18.64 Mbps	8,648 pps	68%
Cisco 2851 AIM-EPII+	67/200	22.98 Mbps	10,616 pps	79%
Cisco 2821 Integrated	30/100	10.26 Mbps	4,769 pps	49%
Cisco 2821 Integrated	40/100	13.68 Mbps	6,301 pps	63%
Cisco 2821 Integrated	50/100	17.1 Mbps	7,841 pps	80%
Cisco 2821 AIM-EPII+	33/200	11.59 Mbps	5,437 pps	49%
Cisco 2821 AIM-EPII+	43/200	15.01 Mbps	6,980 pps	63%
Cisco 2821 AIM-EPII+	55/200	18.92 Mbps	8,783 pps	78%
Cisco 2811 Integrated	7/50	2.46 Mbps	1,167 pps	46%
Cisco 2811 Integrated	10/50	3.48 Mbps	1,628 pps	64%
Cisco 2811 Integrated	13/50	4.94 Mbps	2,085 pps	77%
Cisco 2811 AIM-EPII+	9/50	3.15 Mbps	1,472 pps	48%
Cisco 2811 AIM-EPII+	13/50	4.51 Mbps	2,090 pps	63%
Cisco 2811 AIM-EPII+	17/50	5.86 Mbps	2,700 pps	77%
Cisco 2801 Integrated	7/50	2.48 Mbps	1,169 pps	50%
Cisco 2801 Integrated	10/50	3.49 Mbps	1,630 pps	69%
Cisco 2801 Integrated	13/50	4.53 Mbps	2,094 pps	80%
Cisco 2801 AIM-EPII+	11/50	3.84 Mbps	1,788 pps	50%
Cisco 2801 AIM-EPII+	15/50	5.17 Mbps	2,394 pps	64%
Cisco 2801 AIM-EPII+	20/50	6.81 Mbps	3,152 pps	80%
Cisco 1841 Integrated	7/50	2.48 Mbps	1,174 pps	49%
Cisco 1841 Integrated	10/50	3.47 Mbps	1,624 pps	63%
Cisco 1841 Integrated	13/50	4.47 Mbps	2,079 pps	78%
Cisco 1841 AIM-EPII+	11/50	3.81 Mbps	1,777 pps	48%

Table 3-9 Branch Site Device Throughput, DMVPN, ISR Platforms (continued)

Branch Router Platform/HW Acceleration Option	# Tunnels Passing Data/Active	Throughput (bps)	Throughput (pps)	CPU % Utilization
Cisco 1841 AIM-EPII+	15/50	5.19 Mbps	2,395 pps	62%
Cisco 1841 AIM-EPII+	20/50	6.81 Mbps	3,146 pps	79%

Table 3-10 shows results for the legacy platforms in Solution Two designs. The Cisco 7200 VXR with NPE-G1 and VAM2 is included here as well. Considering the ability of DMVPN to set up spoke-to-spoke tunnels, designs with high-bandwidth access at the branch sites, and/or designs in which a large portion of the tunnels created may be encrypting spoke-to-spoke application flows, should consider using the most powerful platforms available at the branch location.

Table 3-10 Branch Site Device Throughput—Solution Two (DMVPN, Legacy Platforms)

Branch Router Platform/HW Acceleration Option	# Tunnels Passing Data/Active	Throughput (bps)	Throughput (pps)	CPU % Utilization
Cisco 7200VXR 2 x SA-VAM2	33.65 Mbps	100/400	16,060 pps	58%
Cisco 7200VXR 2 x SA-VAM2	125/400	42.05 Mbps	19,921 pps	70%
Cisco 7200VXR 2 x SA-VAM2	160/400	53.29 Mbps	25,206 pps	89%
Cisco 3745 AIM-HPII	40/200	13.82 Mbps	6,479 pps	48%
Cisco 3745 AIM-HPII	54/200	18.48 Mbps	8,612 pps	63%
Cisco 3745 AIM-HPII	71/200	24.08 Mbps	11,183 pps	81%
Cisco 3725 AIM-HPII	22/125	7.67 Mbps	3,599 pps	48%
Cisco 3725 AIM-HPII	30/125	10.39 Mbps	4,834 pps	65%
Cisco 3725 AIM-HPII	37/125	12.8 Mbps	5,913 pps	79%
Cisco 2691 AIM-EPII	16/100	5.59 Mbps	2,640 pps	47%
Cisco 2691 AIM-EPII	22/100	7.62 Mbps	3,553 pps	65%
Cisco 2691 AIM-EPII	28/100	9.65 Mbps	4,473 pps	79%
Cisco 3660 AIM-HPII	14/100	4.95 Mbps	2,338 pps	48%
Cisco 3660 AIM-HPII	20/100	6.98 Mbps	3,256 pps	64%
Cisco 3660 AIM-HPII	26/100	8.99 Mbps	4,172 pps	82%
Cisco 2651XM AIM-BPII	4/25	1.4 Mbps	661 pps	47%
Cisco 2651XM AIM-BPII	5/25	1.7 Mbps	811 pps	57%
Cisco 2651XM AIM-BPII	7/25	2.4 Mbps	1116 pps	77%
Cisco 1760 1700VPN	4/25	1.4 Mbps	660 pps	58%
Cisco 1760 1700VPN	5/25	1.7 Mbps	816 pps	70%
Cisco 1760 1700VPN	6/25	2.08 Mbps	966 pps	82%
Cisco 1711 1700VPN	3/25	1.07 Mbps	509 pps	54%

Table 3-10 Branch Site Device Throughput—Solution Two (DMVPN, Legacy Platforms) (continued)

Branch Router Platform/HW Acceleration Option	# Tunnels Passing Data/Active	Throughput (bps)	Throughput (pps)	CPU % Utilization
Cisco 1711 1700VPN	4/25	1.4 Mbps	663 pps	70%
Cisco 1711 1700VPN	5/25	1.74 Mbps	815 pps	82%
Cisco 831 Integrated	1/10	355,400 kbps	171 pps	27%
Cisco 831 Integrated	2/10	688,400 kbps	323 pps	49%
Cisco 831 Integrated	3/10	1.02 Mbps	474 pps	70%

Other Cisco Products for the Branch

Several other Cisco products support IPSec VPN tunnel termination in a branch site environment; for example, the Cisco VPN 3002 Concentrator Series and the Cisco PIX 501 and 506 Firewalls. These platforms were not part of the scalability testing and therefore are not fully discussed in this version of the design guide.

See the following links for more product information on the Cisco VPN3000 and PIX series:

- http://www.cisco.com/warp/public/cc/pd/hb/vp3000/
- http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/

Software Releases Evaluated

The following software releases were used in the initial scalability testing:

- Cisco head-end routers (7140, 7200)—Cisco IOS Software Release 12.1(9)E (with 3DES IPSec support)
- Cisco branch office routers (1750, 26xx, 36xx)—Cisco IOS Software Release 12.2(3.5)T (with 3DES IPSec support)

Note Note that several Cisco IOS images exist, configured with various levels of encryption technology. There are certain restrictions and laws governing the use and export of encryption technology.

With the Cisco IOS images referenced above, all VPN features may be enabled, including 3DES.

Subsequent testing has been completed with the following Cisco IOS versions:

- Cisco 6500 VPNSM—Cisco IOS Software Release 12.2(9)YO
- Cisco head-end routers (7140, 7200) —Cisco IOS Software Release 12.2(13)S, IOS 12.3(5)
- Cisco branch office routers (1750, 26xx, 36xx, 37xx)— Cisco IOS Software Release 12.2(13)T, IOS 12.3(8)T5
- Cisco branch office ISRs (1841, 28xx, 38xx)—Cisco IOS Software Release 12.3(8)T5, IOS 12.3(11)T2
- Cisco remote office routers (831)—Cisco IOS Software Release 12.2(4)YB, IOS 12.3(13)ZH
- Cisco PIX 535—Cisco PIX 6.3.1

As always, before selecting Cisco IOS software, perform the appropriate research on the Cisco website and consult with Cisco Associates. It is also important to have an understanding of issues in those levels of code that may affect other features configured on the customer routers.

Configuring the Three Solutions

This chapter provides configuration examples for the three solutions, and includes the following sections:

Configuring Solution One

The configuration issues defined in this section are specific to VPN implementation for Solution One. It is presumed that the reader is reasonably familiar with standard Cisco CLI configuration practices.

All example configurations shown are for IPSec in tunnel mode.

An IPSec configuration is implemented by completing the steps described in the following sections:

The sections that follow cover each of these steps in more detail. For more information, see the following URL: http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Internetworking:IPSec

IKE Policy Configuration

There must be at least one matching IKE policy between two potential IPSec peers. The sample configuration below shows a policy using pre-shared keys with 3DES as the encryption transform. There is a default IKE policy that contains the default values for the transform, hash method, Diffie-Helman group, authentication, and lifetime parameters. This is the lowest priority IKE policy.

When using pre-shared keys, Cisco recommends that wildcard keys not be used. Instead, the example shows two keys configured for two separate IPSec peers. The keys should be carefully chosen; “bigsecret” is used only as an example. The use of alphanumeric and punctuation characters as keys is recommended.

Head-end router:

```
interface FastEthernet1/0
ip address 192.168.251.1 255.255.255.0
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key bigsecret address 192.168.161.2
```

Branch-site router:

```
interface s0/0
ip address 192.168.161.2 255.255.255.0
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key bigsecret address 192.168.251.1
```

The default values and more information can be found at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/fipsencr/srfike.htm#xocid17729

IPSec Transform and Protocol Configuration

The transform set must match between the two IPSec peers. The transform set names are locally significant only. However, the encryption transform, hash method, and the particular protocols used (ESP or AH) must match. You may also configure data compression here but it is not recommended on peers with high speed links. There can be multiple transform sets for use between different peers.

Head-end router:

```
interface FastEthernet1/0
ip address 192.168.251.1 255.255.255.0
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
```

Branch-site router:

```
interface s0/0
ip address 192.168.161.2 255.255.255.0
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
```

More information can be found at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/fipsencr/srfipsec.htm#xtocid105784

Access List Configuration for Encryption

The access list entries defining the traffic to be encrypted should be mirror images of each other on the IPSec peers. If access list entries include ranges of ports, then a mirror image of those same ranges must be included on the remote peer access lists. The addresses specified in these access lists are independent of the addresses used by the IPSec peers. In this example, the IP protocol GRE is specified on both the source and destination parts of the access list. All traffic encapsulated in the GRE packets is protected.

Head-end router:

```
interface FastEthernet1/0
ip address 192.168.251.1 255.255.255.0
!
ip access-list extended vpn-static1
permit gre host 192.168.251.1 host 192.168.1.2
```

Branch-site router:

```
interface s0/0
ip address 192.168.161.2 255.255.255.0
!
ip access-list extended vpn-static2
permit gre host 192.168.1.2 host 192.168.251.1
```

An example such as that shown above is logical for Solution One, where all packets to be encrypted are identified as "GRE" and are carried between two peers designated as crypto peers to each other. In newer releases of Cisco IOS Software, the requirement for "strict mirroring" on crypto ACLs is discontinued.

Crypto Map Configuration

The crypto map entry ties together the IPSec peers, the transform set used, and the access list used to define the traffic to be encrypted. The crypto map entries are evaluated sequentially.

In the example below, the crypto map name "static-map" and crypto map numbers (for example. "1" and "20") are locally significant only. The first statement sets the IP address used by this peer to identify itself to other IPSec peers in this crypto map. This address must match the set peer statement in the remote IPSec peers crypto map entries. This address also needs to match the address used with any pre-shared keys the remote peers might have configured. The IPSec mode defaults to tunnel mode.

Head-end router:

```
interface FastEthernet1/0
ip address 192.168.251.1 255.255.255.0
!
crypto map static-map local-address FastEthernet1/0
crypto map static-map 1 ipsec-isakmp
 set peer 192.168.161.2
 set transform-set vpn-test
 match address vpn-static1
```

Branch-site router:

```
interface s0/0
ip address 192.168.161.2 255.255.255.0
!
crypto map static-map local-address Serial0/0
crypto map static-map 20 ipsec-isakmp
 set peer 192.168.251.1
 set transform-set vpn-test
 match address vpn-static2
```

A more complete description can be found at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/fipsencr/srfipsec.htm - xtocid105785

Applying Crypto Maps

Before Cisco IOS Software Release 12.2(13)T, the crypto maps must be applied to both the physical interface and the logical interfaces, such as the GRE tunnel interfaces. As of Cisco IOS Software Release 12.2(13)T (assumed in the example below), the crypto map is applied only to the physical interface, not to the logical interface.

Head-end router:

```
interface Tunnel1
 bandwidth 1536
 ip address 10.62.1.193 255.255.255.252
 tunnel source 192.168.251.1
 tunnel destination 192.168.161.2
!
interface FastEthernet1/0
ip address 192.168.251.1 255.255.255.0
crypto map static-map
!
```

Branch-site router:

```
interface Tunnel1
 bandwidth 1536
 ip address 10.62.1.194 255.255.255.252
 tunnel source 192.168.161.2
 tunnel destination 192.168.251.1
!
interface Serial0/0
 bandwidth 1536
 ip address 192.168.161.2 255.255.255.0
 crypto map static-map
```

Common Configuration Mistakes

The following sections outline some common mistakes and problems encountered when configuring IPSec with GRE.

ACL Mirroring

In older versions of Cisco IOS Software, the access lists that define the traffic to be encrypted must be mirror images of each other. This is no longer true per Cisco IOS Software conventions however, as explained in Access List Configuration for Encryption, page 4-2. In this solution, all packets are sourced from and destined to the GRE tunnel addresses and can be identified as type GRE, which is the best way to create the crypto ACL. The source port and source address in the access list on one peer must also match the destination port and destination address on the other peer. The elimination of the source and destination ports is permissible; however, the use of the keyword “any” for the addresses is strongly discouraged. This ensures proper processing of encrypted traffic on the remote peer.

Peer Address Matching

The IP address used as the IPSec source address must match the address configured as the destination address on the IPSec peer and vice-versa. Unless the address is configured specifically, the address of the outgoing interface will be used as the IPSec peer address.

Transform Set Matches

At least one matching transform set must be configured between two IPSec peers. When specifying a particular strength of encryption algorithm, a similar strength IKE algorithm should also be configured. Failure to do so can weaken the encryption strength of the entire solution.

IKE Policy Matching

There is a default IKE policy present in all Cisco IOS Software devices. This policy uses lower security hash methods and encryption transform sets. If a stronger IKE policy is desired, at least one matching IKE policy must be configured between each IPSec peer.

Cisco recommends using the same transform set and hash methods in IKE and IPSec policies.

Configuring Solution Two

This section describes the configuration issues specific to VPN implementation for Solution Two (DMVPN). A DMVPN IPSec configuration is implemented by completing the steps described in the following sections:

- IKE Policy Configuration, page 4-5
- IPSec Profile Configuration, page 4-6
- mGRE or GRE Tunnel Configuration, page 4-7
- NHRP Configuration, page 4-8
- Applying Tunnel Protection, page 4-9
- Tunnels Sharing a Tunnel Source Interface, page 4-9

The sections that follow cover each of these steps in more detail. For more information, see the following URL: http://www.cisco.com/warp/customer/471/dcmvpn.html

IKE Policy Configuration

As with Solution One, there must be at least one matching IKE policy between two potential IPSec peers. For DMVPN, this means that head-end and branch-end routers must be able to authenticate with each other and, if spoke-to-spoke IPSec SAs are permitted, the branch-end devices must also be able to authenticate with each other to create a matching IKE policy between them. The sample configuration below shows a policy using pre-shared keys with 3DES as the encryption transform. The key “bigsecret” is shared by all devices, with the branch device configured to the match on the address of each head-end router; the head-end routers are configured with a wildcard.

Note that this only an example. In general, wildcard keys are not recommended, and key strings should include alphanumeric and punctuation characters. Digital certificates, AAA authentication via a RADIUS server, or RSA encrypted nonces are also options for IKE authentication.

Head-end router #1:

```
interface FastEthernet1/0
ip address 192.168.251.1 255.255.255.0
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
```

```
crypto isakmp key bigsecret address 0.0.0.0 0.0.0.0
```

Head-end router #2:

```
interface FastEthernet1/0
ip address 192.168.252.1 255.255.255.0
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key bigsecret address 0.0.0.0 0.0.0.0
```

Branch-site router:

```
interface Serial0/0
ip address 192.168.161.2 255.255.255.0
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 192.168.251.1
crypto isakmp key bigsecret address 192.168.252.1
!
```

The default values and more information can be found at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/fipsencr/srfike.htm - xtocid17729

IPSec Profile Configuration

An IPSec profile must be configured that matches between two IPSec peers. An IPSec profile includes the transform set, perfect forward secrecy (PFS) group settings, SA parameters such as lifetime and idletime, and identity restrictions. The transform set is configured independently of the IPSec profile, but referenced by name in the profile definition; names are locally significant only. However, the encryption transform, hash method, and the particular protocols used (ESP or AH) must match between peers. Multiple transform sets and multiple profile definitions for use between different peers can be defined in one router.

Head-end router:

```
crypto ipsec transform-set ENTERPRISE esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-HEAD
 set transform-set ENTERPRISE
!
```

Branch-site router:

```
crypto ipsec transform-set ENTERPRISE esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-BRANCH
 set transform-set ENTERPRISE
!
```

mGRE or GRE Tunnel Configuration

The head-end devices must be configured with mGRE tunnels, allowing a single GRE interface to support multiple IPSec tunnels. The branch-end devices can be configured with either mGRE tunnels, if spoke-to-spoke tunnel setup is to be supported in the network, or with point-to-point GRE tunnels, if the design is to be restricted to hub-and-spoke. An mGRE tunnel requires the configuration of an IP address to serve as tunnel source, but no tunnel destination address. A point-to-point GRE tunnel requires both a source and destination address in its configuration.

When mGRE is in use, a tunnel key value is usually configured, which allows a router with more than one mGRE interface to differentiate between them. As of Cisco IOS Software Release 12.3(9.13)T, it is possible to configure mGRE tunnel interfaces without tunnel keys and have them serve separate DMVPN groupings; to do so, each mGRE interface must reference a unique IP address or interface as its tunnel source.

Note Because of a regression issue, Cisco recommends using Cisco IOS Software Release 12.3(12.01)T or 12.3(11)T3 if configuring an mGRE interface without a tunnel key.

The example below shows two head-end devices and one branch-end device with a point-to-point tunnel to each head-end router, using tunnel keys.

Head-end router #1:

```
interface Tunnel0
 description mGRE Template Tunnel
 ip address 10.0.0.1 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 10000
!
```

Head-end router #2:

```
interface Tunnel0
 description mGRE Template Tunnel
 ip address 10.0.1.1 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 10001
!
```

Branch-site router:

```
interface Tunnel0
 description GRE Tunnel
 ip address 10.0.0.2 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.1
 tunnel key 10000
!
interface Tunnel1
 description GRE Tunnel
 ip address 10.0.1.2 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.2
 tunnel key 10001
!
```

NHRP Configuration

NHRP is a Layer 2 address resolution protocol and cache, similar to ARP and Frame Relay inverse ARP. The head-end routers function as NHRP servers to the branch-end routers. Branch-end routers send registration requests with both their tunnel and NBMA addresses; the head ends cache this information and can then serve it to other devices inquiring for it.

Branch-end routers require **ip nhrp map** statements to the hub addresses. All routers must belong to the same NHRP network, as configured by the **ip nhrp network-id <id>** command. The network-id defines an NHRP domain and is unrelated to the tunnel key. Also, the routers in an NHRP domain must agree on an NHRP holdtime (the recommendation is 10 minutes, or roughly three times the NHRP registration request interval), and they can be configured to authenticate with each other via a key string.

To support routing protocols that use multicast for their updates (for instance, EIGRP and OSPF), or any other form of multicast across DMVPN, the hub router is configured to send multicast to all spokes that register with it dynamically. On the branch router, a configuration line pointing to the hub router is needed for mGRE tunnel interfaces, but not for point-to-point GRE. Configuration examples for two hub routers and one branch router in a single DMVPN (all interfaces using mGRE) are as follows:

Head-end router #1:

```
interface Tunnel0
 description mGRE Template Tunnel
 ip address 10.0.0.1 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 10000
 ip nhrp network-id 100
 ip nhrp holdtime 600
!
interface FastEthernet0/0
 description Outside interface
 ip address 172.16.0.1 255.255.255.0
!
```

Head-end router #2:

```
interface Tunnel0
 description mGRE Template Tunnel
 ip address 10.0.0.2 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 10000
 ip nhrp network-id 100
 ip nhrp holdtime 600
!
interface FastEthernet0/0
 description Outside interface
 ip address 172.16.0.2 255.255.255.0
!
```

Branch-site router:

```
interface Tunnel0
 description mGRE Template Tunnel
 ip address 10.0.0.3 255.255.255.0
 ip nhrp authentication cisco123
 tunnel source Ethernet0/0
```

```
 tunnel mode gre multipoint
 tunnel key 10000
 ip nhrp map 10.0.0.1 172.16.0.1
 ip nhrp map multicast 172.16.0.1
 ip nhrp map 10.0.0.1 172.16.0.2
 ip nhrp map multicast 172.16.0.2
 ip nhrp network-id 100
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.0.1
 ip nhrp nhs 10.0.0.2
!
```

Applying Tunnel Protection

The final step in DMVPN configuration is the application of the **tunnel protection** command to the tunnel interface. The **tunnel protection** command is not applied to the router outside interface, or to any other interface in the router. For brevity, in the example below, only a few lines of the tunnel interface configurations are shown.

Head-end router:

```
crypto ipsec transform-set ENTERPRISE esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-HEAD
 set transform-set ENTERPRISE
!
interface Tunnel0
 description mGRE Template Tunnel
 ip address 10.0.0.1 255.255.255.0
 …
 tunnel protection ipsec profile DMVPN-HEAD
!
```

Branch-site router:

```
crypto ipsec transform-set ENTERPRISE esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-BRANCH
 set transform-set ENTERPRISE
!
interface Tunnel0
 description mGRE Template Tunnel
 ip address 10.0.0.2 255.255.255.0
 …
 tunnel protection ipsec profile DMVPN-BRANCH
!
```

Tunnels Sharing a Tunnel Source Interface

If more than one mGRE tunnel is configured on a router (for instance, on a hub router), it is possible to reference the same tunnel source address on each tunnel interface. In this case, the keyword “shared” is used in the **tunnel protection** command on both interfaces. This does not tie the two mGRE tunnels into the same DMVPN “cloud”; each tunnel interface requires a unique tunnel key, NHRP network-id, and IP subnet. An example is as follows:

Head-end router:

```
interface Tunnel0
 description mGRE Template Tunnel
 ip address 10.0.0.1 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 10000
 ip nhrp network-id 100
 ip nhrp holdtime 600
 tunnel protection ipsec profile DMVPN-HEAD shared
!
interface Tunnel1
 description mGRE Template Tunnel
 ip address 10.0.11.1 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 10011
 ip nhrp network-id 110
 ip nhrp holdtime 600
 tunnel protection ipsec profile DMVPN-HEAD shared
!
```

Configuring Solution Three

This section describes the details of the configuration for Solution Three, and includes the following sections:

IKE Configuration

The IKE configuration for Solution Three currently uses pre-shared keys. The preferred method for IKE authentication is the use of digital certificates. The use of digital certificates is more scalable and more secure than the use of pre-shared keys.

Within the context of Solution Three, one pre-shared key must be assigned per remote peer. Each pre-shared key is configured on a line by itself. An alternative to configuring the pre-shared keys in the head end configuration is the use of a RADIUS server. That configuration is not presented here. In the following example, only a single pre-shared key for one peer is shown, for clarity.

Dead Peer Detection

An enhancement to the **isakmp keepalive** command has changed the way that IKE keepalives work, creating the feature known as Dead Peer Detection (DPD). DPD no longer automatically sends hello messages to the IKE peer if live traffic has been received from that peer within a specified period. The first variable in the **crypto isakmp keepalive** command is the number of seconds that the peer waits for

valid traffic from its IPSec neighbor. If no traffic has been received, the second variable is the number of seconds between retries. This scheme helps conserve router CPU by not sending the keepalive messages if a router has just received valid traffic.

Head-end router #1:

```
interface GigabitEthernet0/1
ip address 192.168.251.5 255.255.255.0
standby ip 192.168.251.1
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 192.168.161.2
crypto isakmp keepalive 60 5
!
```

Head-end router #2:

```
interface GigabitEthernet0/1
ip address 192.168.252.6 255.255.255.0
standby ip 192.168.251.1
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 192.168.161.2
crypto isakmp keepalive 60 5
!
```

Branch-site router #1:

```
interface Serial0/0
ip address 192.168.161.2 255.255.255.0
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 192.168.251.1
crypto isakmp keepalive 60 5
!
```

IPSec Configuration

Two features in Cisco IOS Software each provide part of the IPSec High Availability (HA) feature. Reverse Route Injection (RRI) places static routes into a router forwarding table for networks it has learned about from IPSec SAs. These static routes can then be redistributed into any routing protocol running on the router.

Dynamic IPSec Tunnels

Dynamic tunnels are necessary when using IPSec HA features because of the way that RRI operates. When a static crypto map exists on a router, the network information from that crypto map is used to create a static route. However, in the case of this solution, only one head end has a live connection to a branch router. If static crypto maps are used, both head-end routers create static routes corresponding to the same branch locations. Each of these static routes is then redistributed into the routing protocol

running on the particular head-end device. This can cause asymmetrical routing and more than the necessary number of IKE and IPSec SAs to be negotiated. The use of dynamic tunnels also greatly simplifies the configuration on head-end routers. There is no access list associated with a crypto map entry configured on routers with dynamic crypto maps. In this configuration, access lists are not required.

Reverse Route Injection

RRI is implemented by the single **reverse-route** command under the crypto map of an IPSec configuration. If RRI has been configured on a router with static crypto maps, the network information from the access lists used in the crypto maps is used to create the static route entries, whether or not the SA for the particular line in the access list has been negotiated and is active. If dynamic crypto maps are configured, the network information is not placed in the routing table as a static route until the SA negotiation has been completed.

Head-end router #1:

```
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto dynamic-map dmap 10
 set transform-set vpn-test
 reverse-route
!
!
crypto map dynamic-map local-address GigabitEthernet0/1
crypto map dynamic-map 10 ipsec-isakmp dynamic dmap
!
```

Head-end router #2:

```
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto dynamic-map dmap 10
 set transform-set vpn-test
 reverse-route
!
!
crypto map dynamic-map local-address GigabitEthernet0/1
crypto map dynamic-map 10 ipsec-isakmp dynamic dmap
!
```

Branch router #1:

```
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto map static-map local-address Serial0/0
crypto map static-map 10 ipsec-isakmp
 set peer 192.168.251.1
 set transform-set vpn-test
 match address b000
!
ip access-list extended b000
 permit ip 10.60.0.0 0.0.0.255 10.0.0.0 0.255.255.255
!
```

Head End HSRP and Interface Configuration

Hot Standby Router Protocol (HSRP) is used as part of HA IPSec to ensure that the head end IPSec peer address is always available for remote devices.

HSRP and IPSec

The HSRP configuration used on an interface with a crypto map is identical to the normal use of HSRP. All the standby commands operate as they normally would without an IPSec configuration. The one difference between an IPSec configuration without HSRP and the configuration that includes HSRP is the elimination of the local peer address command. When a crypto map is applied to an interface with the redundancy keyword, the IP address that has been assigned to the standby group is now automatically used as the local IPSec peer address without any requirement for a local peer statement.

Head-end router #1:

```
interface GigabitEthernet0/1
 description GigabitEthernet0/1
 ip address 192.168.251.5 255.255.255.248
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
 standby ip 192.168.251.1
 standby timers msec 50 1
 standby priority 101
 standby preempt
 standby name outside
 standby track GigabitEthernet0/2
 crypto map dynamic-map redundancy outside
!
```

Head-end router #2:

```
interface GigabitEthernet0/1
 description GigabitEthernet0/1
 ip address 192.168.251.6 255.255.255.248
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
 standby ip 192.168.251.1
 standby timers msec 50 1
 standby preempt
 standby name outside
 standby track GigabitEthernet0/2
 crypto map dynamic-map redundancy outside
!
```

Note that one router, Head-end router #1 in this case, has a standby priority configured. This causes it to be the preferred router for this standby group. If the number of IPSec peers is large, multiple standby groups may be configured, with a separate set of peers configured to each standby group. In this manner, the failure of the active router for one group causes a failover for only that group. The operational router does not have to complete IKE negotiations for both standby groups.

At the branch site, no special configurations are required to make this router aware that HSRP is in use at the head end. The crypto map is applied to the physical interface as usual.

Branch router #1:

```
interface Serial0/0
```

```
 description Serial0/0
 ip address 192.168.0.2 255.255.255.252
 crypto map static-map
!
```

Head End Redistribution for RRI Configuration

RRI operates by creating a static route that is placed into the routing table for any network information derived from SAs associated with the crypto map that has the **reverse route** command statement applied. This is half of the procedure necessary to inject this network information into the routing information provided to upstream networks. A routing protocol should be running on the head-end routers to use RRI.

Static Route Redistribution

The redistribution of the static routes inserted by RRI takes place via the normal route redistribution mechanisms already present in Cisco IOS Software. In the example, the default metric applied is the typical default used for an Ethernet interface.

Head-end router #1:

```
router eigrp 1
 redistribute static metric 1000 100 255 1 1500
 network 10.0.0.0
 default-metric 10000 100 255 1 1500
 no auto-summary
!
```

Head-end router #2:

```
router eigrp 1
 redistribute static metric 1000 100 255 1 1500
 network 10.0.0.0
 default-metric 10000 100 255 1 1500
 no auto-summary
!
```

RRI is not configured on the branch devices. The branch routers use a static default pointing to the upstream next hop.

CHAPTER 5

Site-to-Site VPN Case Study

This case study provides a reference example for a site-to-site VPN design, describing how these design principles can be applied in a real-world scenario.

This case study assumes that all of the design considerations in Chapter 2, "Selecting a Site-to-Site VPN Solution," and Chapter 3, "Selecting Solution Components," have been addressed, and that best practice design recommendations are adopted by the customer.

The case study also assumes that the Cisco IOS Software levels listed in Software Releases Evaluated, page 3-18 are acceptable to the customer.

The details of the service provider backbone and WAN connectivity are not addressed in this case study, because the focus is on VPN deployment on the enterprise customer side.

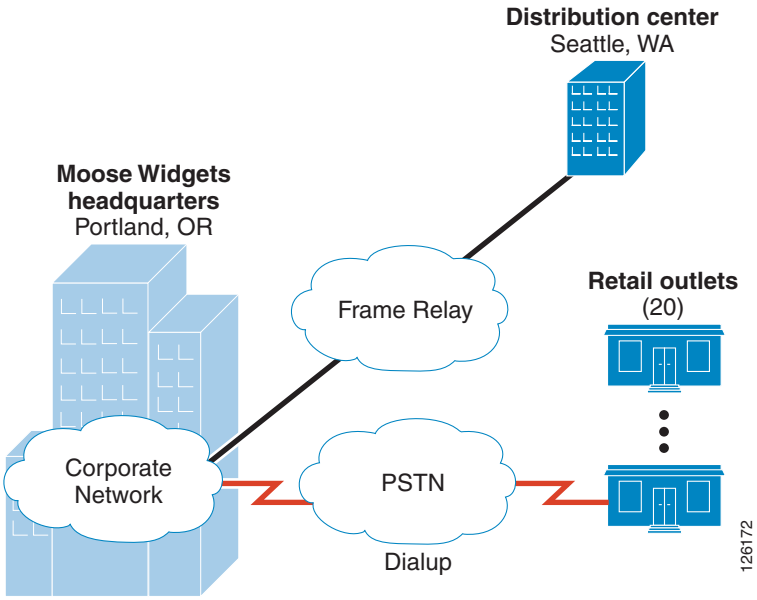
This chapter includes the following topics:

Customer Overview

Moose Widgets has been developing products at its Portland, Oregon headquarters (HQ) for several years. In addition, Moose has a single distribution center and 20 retail outlets across the United States (US).

Currently, Moose Widgets uses a traditional Frame Relay (FR) WAN service to connect its HQ to its distribution center. There is currently no connectivity to retail outlets, with the exception of a few outlets that use a personal computer (PC) to dial up to the corporate HQ. The current network topology is shown in Figure 5-1.

Figure 5-1 Moose Widgets Case Study—Current Topology



Moose has recently acquired two companies; one in San Jose, California and the other in Great Falls, Montana. Moose wants to connect its newly acquired companies and its retail outlets to its corporate network as an intranet. In addition, Moose plans to expand its retail outlets to 40–50 outlets over the next year, and sees already that it will most likely need additional distribution centers on the east and west coasts of the US.

As part of a corporate initiative, Moose is implementing a centralized inventory tracking system to significantly lower costs and to better manage inventory in its growing distribution centers and retail outlets. The existing dial-in access does not provide adequate bandwidth to support the new applications. Also, Moose is concerned about escalating dial-in charges as each retail outlet relies more on corporate resources. As a result, Moose is looking to transition to a dedicated connection for each of its retail outlets using the Internet and VPN technology.

Moose is concerned about the costs of adding the connections, and about the ability to quickly get retail outlets up and running. Moose indicates that it is primarily concerned about data traffic today, but there is some degree of interest in adding voice services in the future.

Moose estimates its traffic requirements for its different site locations as shown in Table 5-1.

Table 5-1 Moose Widgets Case Study—Traffic Profile

Location	Estimated Traffic
Distribution Center (1 today, potentially 3 in the future)	1 Mbps
San Jose	4 Mbps
Great Falls	4 Mbps
Retail Outlets (up to 50)	50 kbps—typical (40); 200 kbps—larger (10)
TOTAL	15 Mbps

Moose has approached Cisco to see how a VPN might solve its problems.

Design Considerations

A site-to-site IPSec VPN will be deployed, with the Moose corporate HQ serving as the head end and all other locations treated as branch sites. This will allow a branch office to subscribe to a local ISP, get authenticated, and be inside the corporate intranet.

At the same time, end-to-end encryption is attained using IPSec tunneling. Switching to VPN offers Moose significant cost savings over dial-up solutions and the ability to outsource to a service provider who has VPN service as a core competency, providing more efficiency with cost and scalability.

Following the design practice outlined in Chapter 2, "Selecting a Site-to-Site VPN Solution" and Chapter 3, "Selecting Solution Components," there are four main design steps to perform, as described in the following sections:

Preliminary Design Considerations

The design is straightforward and offers flexibility. As new retail locations are put into service, Moose can purchase Internet connectivity from the local ISP, deploy a Cisco VPN router at the branch site, configure the IPSec tunnels to the head-end devices at the corporate headquarters, and be up and running in a short amount of time.

Using the questions from Types of Site-to-Site VPN Deployments, page 2-1, Table 5-2 summarizes the preliminary design considerations.

Table 5-2 Preliminary Design Considerations

Question	Answer	Comments
What applications does the customer expect to run over the VPN?	Data	Interested in future voice services
Is multi-protocol support required?	Yes, IP and multicast	GRE tunnels will enable multi-protocol traffic transport.
How much packet fragmentation does the customer expect on its network?	Minimal	Path MTU discovery enabled
How many branches does the customer expect to aggregate to the head end?	55 sites	
What is the customer expected traffic throughput to/from branch offices?	See Table 5-1	
What are the customer expectations for resiliency?	Resiliency is required	1 primary, 1 backup tunnel
What encryption level is required?	3DES	

Table 5-2 Preliminary Design Considerations (continued)

Question	Answer	Comments
What type of IKE authentication method will be used?	The use of pre-shared keys is selected because of relatively small number of sites to manage.	Migration to digital certificates should be considered if number of branches increases beyond 50 in the future.
What other services will be run on the branch VPN routers?	None	

EIGRP is recommended as the routing protocol, with route summarization.

Sizing the Head End

Although the traffic loads involved do not exceed the recommended capacity of a single head-end device, Moose would like built-in redundancy at the central location. The tunnels from the remote ends will be allocated to each of the head-end devices to balance the traffic load. Secondary tunnels will also be configured and allocated so that, in the event of a head end failure, traffic is transitioned to the partner head-end device.

Applying the sizing algorithm defined in Head End Devices, page 3-5, the calculation of head end sizing based on number of GRE tunnels is as follows:

N = 55

T = N x 2 = 110

C(t) = (T / 500) rounded up + 1 = 110/500 rounded +1 = 1 + 1 = 2 head ends

Next, applying the sizing algorithm defined in Head End Devices, page 3-5 and using the throughput estimates from Table 5-1, the calculation of head end sizing based on branch traffic throughput is as follows:

A = (3*(1 Mbps)+4 Mbps+4 Mbps+40*(50kbps)+10*(200kbps)) = 15 Mbps

H = 66 Mbps (for Cisco 7206VXR NPE-G1 in Solution One design)

C(a) = A/H, rounded up + 1 = 15/66 rounded up + 1 = 1+1 = 2 head ends

Comparing the number of head-end devices calculated based on number of tunnels, C(t), to the number based on aggregate throughput, C(a), the outcomes match. Therefore, it is appropriate to deploy two head-end devices.

Presented with the head end product options, the customer selects to deploy two Cisco 7206 VXR NPE-G1s, each equipped with an SA-VAM2 hardware encryption adapter.

Sizing the Branch Sites

The primary consideration for sizing of branch office sites is expected traffic throughput. Accordingly, starting with Table 5-1, and applying the concepts presented in Branch Site Devices, page 3-11, the branch products selected are summarized in Table 5-3.

Table 5-3 Moose Widgets Case Study—Branch Site Devices

Location	Estimated Throughput	Branch Office Platform Selected
Distribution centers	1 Mbps	Cisco 2691
San Jose	4 Mbps	Cisco 3745
Great Falls	4 Mbps	Cisco 3745
Retail outlets (typical)	50 kbps	Cisco 1760
Retail outlets (larger)	200 kbps	Cisco 2651XM

At each of the acquired company locations, a Cisco 3745 VPN Router is deployed with high performance hardware-accelerated encryption (AIM-HP). The choice of the 3745 platform is based on the assumption that the acquired companies are large offices with a substantial number of employees.

At each of the distribution centers, a Cisco 2691 Series VPN Router is deployed with enhanced performance hardware-accelerated encryption (AIM-EPII).

Finally, at each of the retail locations, the Cisco 2651 XM is recommended for the larger retail outlets, and the Cisco 1760 for the smaller retail outlets.

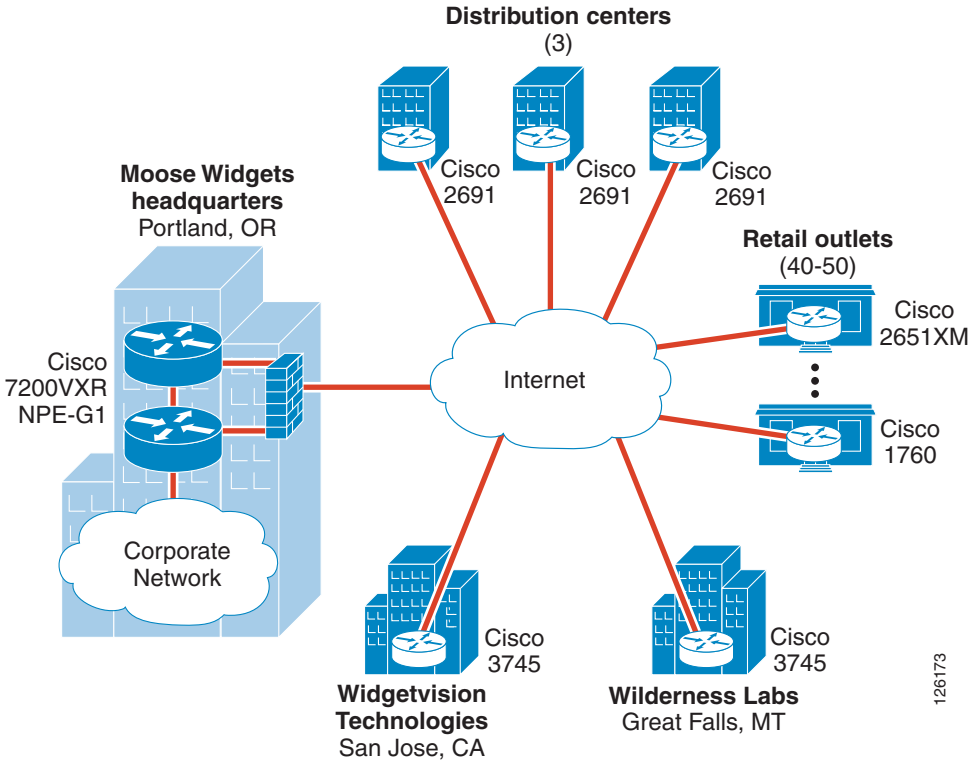
Tunnel Aggregation and Load Distribution

Given 55 branch sites, the total number of tunnels that need to be aggregated is 110 (primary and secondary). Therefore, the first head-end device is allocated 27 primary and 28 backup tunnels, and the second head-end device is allocated 28 primary and 27 backup tunnels.

Network Layout

The new network topology is shown in Figure 5-2.

Figure 5-2 Moose Widgets Case Study—VPN Topology



Future Migration for Teleworkers

At some point in the future, Moose Widgets may also start offering telecommuting options for its employees at the two acquisition locations (necessary in San Jose because of the extremely congested traffic conditions, and necessary in Montana because of excessive snowfalls).

For more information on VPN expansion, see the *Business Ready Teleworker SRND* at the following URL:
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79d.pdf

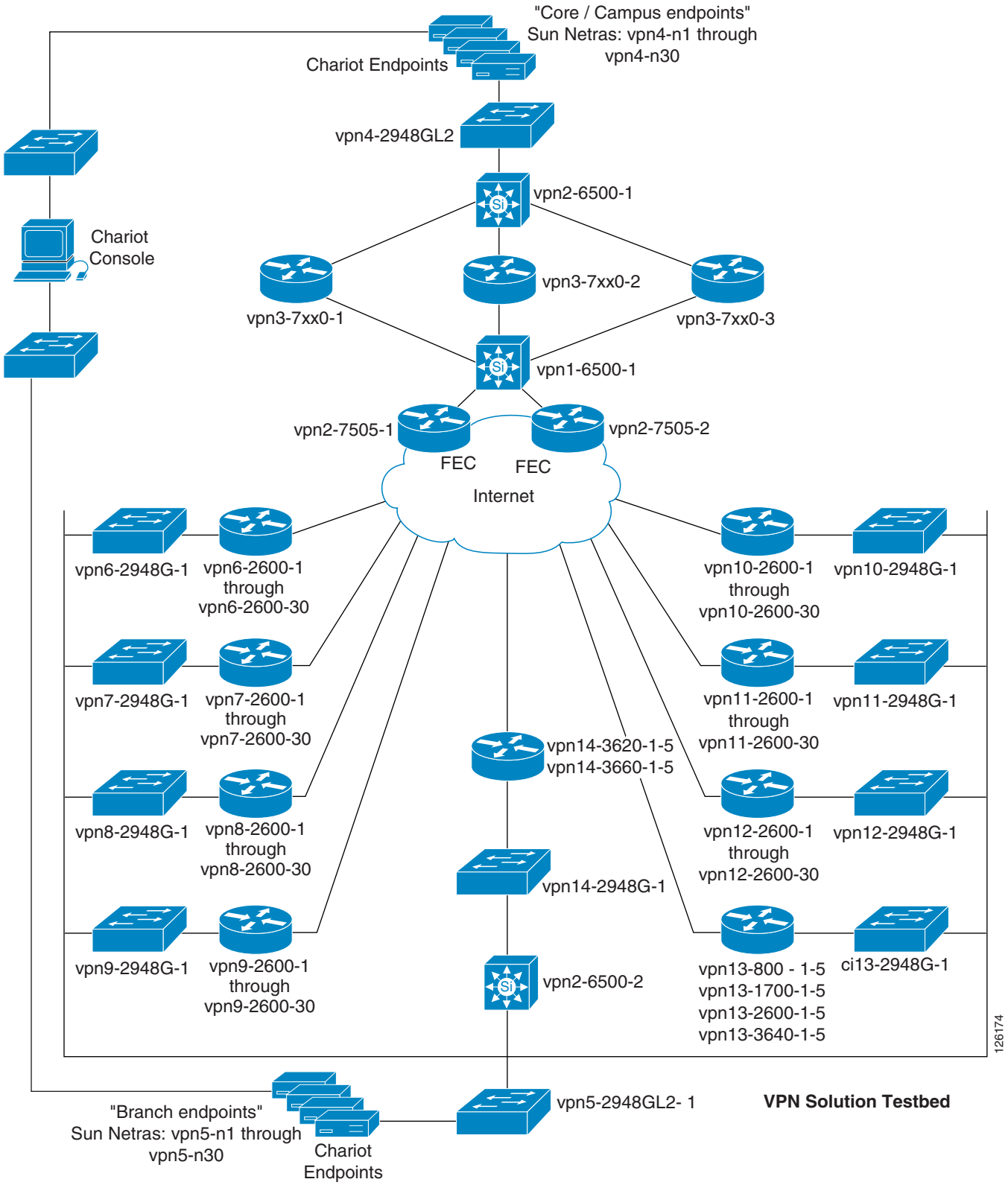
Test Bed Configuration

This section includes the following topics:

Scalability Test Bed Network Diagram

Figure A-1 shows the test bed topology used in the scalability testing.

Figure A-1 Test Bed Topology



Scalability Test Bed Configuration Files

The configurations for the central and branch sites are listed below in the following sections. It should be noted that these configurations have been extracted from real configurations used in scalability testing. They are provided as a reference only.

This section includes the following topics:

Solution One—IPSec with GRE

The following configurations are excerpts of the devices under test in the Solution One testing. The use of GRE as a tunneling method requires static tunnel endpoint configuration.

Head End Configuration

There are two head-end devices in the test bed, each terminating a GRE tunnel from all branch site routers. The configuration shown below is an excerpt of the first head end and does not contain configuration commands for all branches. The ISAKMP pre-shared key, the IPSec peer, the tunnel interface, and the crypto access list are shown for one device.

Head-end router #1:

```
ip cef
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 192.168.0.2
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto map static-map local-address GigabitEthernet0/1
crypto map static-map 100 ipsec-isakmp
 set peer 192.168.0.2
 set transform-set vpn-test
 match address b000
!
interface Loopback0
 description Loopback0
 ip address 10.57.1.255 255.255.255.255
!
interface Tunnel0
 description vpn5-2600-1-000
 ip address 10.60.0.193 255.255.255.252
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0 5
 tunnel source 192.168.251.1
 tunnel destination 192.168.0.2
 crypto map static-map
!
interface GigabitEthernet0/1
 description GigabitEthernet0/1
 ip address 192.168.251.1 255.255.255.248
```

```
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
 crypto map static-map
!
interface GigabitEthernet0/2
 description GigabitEthernet0/2
 ip address 10.57.1.1 255.255.255.248
 duplex auto
 speed auto
media-type gbic
 negotiation auto
!
router eigrp 1
 network 10.0.0.0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 192.168.251.2
!
ip access-list extended b000
 permit gre host 192.168.251.1 host 192.168.0.2
!
```

Branch Site Configuration

The following shows relevant configurations for one branch-site router. For resiliency, two tunnels are configured (primary and secondary), one to each head end. The EIGRP delay metric is used to make Tunnel0 the preferred path. This configuration shows QoS for VoIP flows (shaping and queuing) applied to the physical (outside) interface, the recommended use of summary routes, and an EIGRP stub configuration.

Branch-site router #1:

```
ip cef
!
class-map match-all call-setup
  match ip precedence 3
class-map match-all mission-critical
  match ip precedence 2
class-map match-all voice
  match ip precedence 5
class-map match-any internetworkcontrol
  match ip precedence 6
  match access-group 101
!
policy-map 192kb
  class call-setup
   bandwidth percent 5
  class internetworkcontrol
   bandwidth percent 5
  class mission-critical
   bandwidth percent 22
   queue-limit 16
  class voice
    priority 56
  class class-default
   fair-queue
   queue-limit 6
policy-map 192kb-shaper
  class class-default
```

```
   shape average 182400 1824 0
   service-policy 192kb
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 192.168.251.1
crypto isakmp key bigsecret address 192.168.252.1
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto map static-map local-address Serial0/0
crypto map static-map 10 ipsec-isakmp
 set peer 192.168.251.1
set transform-set vpn-test
 match address b000
 qos pre-classify
crypto map static-map 20 ipsec-isakmp  set peer 192.168.252.1 set transform-set vpn-test
 match address b001
 qos pre-classify
!
interface Loopback0
 description Loopback0
 ip address 10.61.138.254 255.255.255.255
!
interface Tunnel0
 description Tunnel0
 ip address 10.61.138.194 255.255.255.252
 ip summary-address eigrp 1 10.61.138.0 255.255.255.0 5
 qos pre-classify
 tunnel source 192.168.0.2
 tunnel destination 192.168.251.1
!
interface Tunnel1
 description Tunnel1
 ip address 10.61.138.198 255.255.255.252
 ip summary-address eigrp 1 10.61.138.0 255.255.255.0 5
 delay 60000
 qos pre-classify
 tunnel source 192.168.0.2
 tunnel destination 192.168.252.1
!
interface Serial0/0
 description Serial0/0
 bandwidth 192
 ip address 192.168.0.2 255.255.255.252
 service-policy output 192kb-shaper
 crypto map static-map
!
interface FastEthernet0/1
 description FastEthernet0/1
 ip address 10.61.138.129 255.255.255.192 secondary
 ip address 10.61.138.1 255.255.255.128
 speed 100
 full-duplex
!
router eigrp 1
 network 10.0.0.0
 no auto-summary
 eigrp stub connected summary
!
ip route 0.0.0.0 0.0.0.0 192.168.90.5!
ip access-list extended b000
```

```
 permit gre host 192.168.0.2 host 192.168.251.1
ip access-list extended b001
 permit gre host 192.168.0.2 host 192.168.252.1
!
access-list 101 permit udp any eq isakmp any eq isakmp
!
```

Solution Two—DMVPN

The following configurations are excerpts of the devices under test in the Solution Two testing.

Head End Configuration

There are two head-end devices in the test bed, each configured with one mGRE tunnel. A dual hub-dual DMVPN design is assumed. The configuration shown below is an excerpt of the first head end and does not show the entire configuration. Pre-shared keys with a wildcard address are used at the head end for simplicity of the ISAKMP authentication, although this is not recommended for customer use.

Head-end router #1:

```
ip cef
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
 mode transport
no crypto ipsec nat-transparency udp-encaps
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
!
interface Loopback0
 description Loopback0
 ip address 10.57.1.255 255.255.255.255
!
interface Tunnel0
 description Tunnel0
 bandwidth 1000000
 ip address 10.56.0.1 255.255.252.0
 no ip redirects
 ip hold-time eigrp 1 35
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105600
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0 5
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel key 105600
 tunnel protection ipsec profile vpn-dmvpn
!
interface GigabitEthernet0/1
 description GigabitEthernet0/1
 ip address 192.168.251.1 255.255.255.248
 duplex auto
 speed auto
```

```
 media-type gbic
 negotiation auto
!
interface GigabitEthernet0/2
 description GigabitEthernet0/2
 ip address 10.57.1.1 255.255.255.248
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
router eigrp 1
 network 10.0.0.0
 no auto-summary
!
ip route 192.168.0.0 255.255.0.0 192.168.251.2
!
```

Branch Site Configuration

The following shows relevant configurations for one branch-site router. A dual hub-dual DMVPN design is employed by using two tunnels, one to each head end. The EIGRP delay metric is used to make Tunnel0 the preferred path. This configuration shows QoS for VoIP flows (shaping and queuing) applied to the physical (outside) interface, the recommended use of summary routes, and an EIGRP stub configuration.

Branch-site router #1:

```
ip cef
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 192.168.251.1
crypto isakmp key bigsecret address 192.168.252.1
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
  mode transport
no crypto ipsec nat-transparency udp-encaps
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
!
class-map match-all VOICE
  match ip dscp ef
 class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
 class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match access-group name IKE
 class-map match-all TRANSACTIONAL-DATA
  match ip dscp af21
!
 policy-map 192kb
  class CALL-SETUP
   bandwidth percent 2
  class INTERNETWORK-CONTROL
   bandwidth percent 5
  class TRANSACTIONAL-DATA
```

```
   bandwidth percent 22
   queue-limit 16
  class VOICE
   priority 64
  class class-default
   fair-queue
   queue-limit 6
 policy-map 192kb-shaper
  class class-default
   shape average 182400 1824 0
service-policy 192kb
!
interface Loopback0
 description Loopback0
 ip address 10.61.138.254 255.255.255.255
!
interface Tunnel0
 description Tunnel0
 bandwidth 192
 ip address 10.56.3.10 255.255.252.0
 ip hold-time eigrp 1 35
 ip nhrp authentication test
 ip nhrp map 10.56.0.1 192.168.251.1
 ip nhrp map multicast 192.168.251.1
 ip nhrp network-id 105600
 ip nhrp holdtime 300
 ip nhrp nhs 10.56.0.1
 ip summary-address eigrp 1 10.61.148.0 255.255.255.0 5
 qos pre-classify
 tunnel source 192.168.100.6
 tunnel destination 192.168.251.1
 tunnel key 105600
 tunnel protection ipsec profile vpn-dmvpn
!
interface Tunnel1
 description Tunnel1
 bandwidth 192
 ip address 10.56.7.10 255.255.252.0
 ip hold-time eigrp 1 35
 ip nhrp authentication test
 ip nhrp map 10.56.4.1 192.168.252.1
 ip nhrp map multicast 192.168.252.1
 ip nhrp network-id 105640
 ip nhrp holdtime 300
 ip nhrp nhs 10.56.4.1
 ip summary-address eigrp 1 10.61.148.0 255.255.255.0 5
 delay 60000
 qos pre-classify
 tunnel source 192.168.100.6
 tunnel destination 192.168.252.1
 tunnel key 105640
 tunnel protection ipsec profile vpn-dmvpn
!
interface Serial0/0
 description Serial0/0
 bandwidth 192
 ip address 192.168.100.6 255.255.255.252
 service-policy output 192kb-shaper
!
interface FastEthernet0/1
 description FastEthernet0/1
 ip address 10.61.148.129 255.255.255.192 secondary
 ip address 10.61.148.1 255.255.255.128
 speed 100
```

```
 full-duplex
!
router eigrp 1
 network 10.0.0.0
 no auto-summary
 eigrp stub connected summary
!
ip route 0.0.0.0 0.0.0.0 192.168.100.5!
ip access-list extended IKE
 permit udp any any eq isakmp
!
```

Solution Three—IPSec with DPD, RRI and HSRP

The following configurations are excerpts of the devices under test in the Solution Three testing.

Head End Configuration

There are two head-end devices in the test bed, configured for dynamic crypto maps, DPD, RRI, and HSRP. The first head-end device is shown. No crypto peer statement or crypto access list is required. The ISAKMP pre-shared key is shown for one branch router.

Head-end router #1:

```
ip cef
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 192.168.0.2
!
crypto isakmp keepalive 10
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto dynamic-map dmap 10
 set transform-set vpn-test
 reverse-route
!
crypto map dynamic-map local-address GigabitEthernet0/1
crypto map dynamic-map 10 ipsec-isakmp dynamic dmap
!
interface GigabitEthernet0/1
 description GigabitEthernet0/1
 ip address 192.168.251.5 255.255.255.248
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
 standby ip 192.168.251.1
 standby timers msec 50 1
 standby priority 101
 standby preempt
 standby name outside
 standby track GigabitEthernet0/2
 crypto map dynamic-map redundancy outside
!
interface GigabitEthernet0/2
 description GigabitEthernet0/2
```

```
 ip address 10.57.1.1 255.255.255.248
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
router eigrp 1
 redistribute static metric 1000 100 255 1 1500
 network 10.0.0.0
 default-metric 10000 100 255 1 1500
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 192.168.251.2
!
```

Branch Site Configuration

The following shows relevant configurations for one branch-site router. The crypto peer is the HSRP address at the head end. This configuration shows QoS for VoIP flows (shaping and queuing) applied to the physical (outside) interface.

Branch-site router #1:

```
ip cef
!
class-map match-all VOICE
  match ip dscp ef
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match access-group name IKE
class-map match-all TRANSACTIONAL-DATA
  match ip dscp af21
!
policy-map 192kb
  class CALL-SETUP
   bandwidth percent 2
  class INTERNETWORK-CONTROL
   bandwidth percent 5
  class TRANSACTIONAL-DATA
   bandwidth percent 22
   queue-limit 16
  class VOICE
    priority 56
  class class-default
   fair-queue
   queue-limit 6
policy-map 192kb-shaper
  class class-default
   shape average 182400 1824 0
   service-policy 192kb
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 192.168.251.1
crypto isakmp keepalive 10
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
```

```
crypto map static-map local-address Serial0/0
crypto map static-map 10 ipsec-isakmp
set peer 192.168.251.1
 set transform-set vpn-test
 match address b000
!
interface Loopback0
 description Loopback0
 ip address 10.61.138.254 255.255.255.255
!
interface Serial0/0
 description Serial0/0
 bandwidth 192
 ip address 192.168.90.6 255.255.255.252
 service-policy output 192kb-shaper
 crypto map static-map
!
interface FastEthernet0/1
 description FastEthernet0/1
 ip address 10.61.138.129 255.255.255.192 secondary
 ip address 10.61.138.1 255.255.255.128
 speed 100
 full-duplex
!
ip route 0.0.0.0 0.0.0.0 192.168.90.5
!
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
ip access-list extended b000
 permit ip 10.61.138.0 0.0.0.255 10.0.0.0 0.255.255.255
```

References and Reading

This section includes the following topics:

Documents

- SAFE: VPN IPSec Virtual Private Networks in Depth—http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801dca2d.shtml
- Business Ready Teleworker SRND—http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79d.pdf

Request For Comment (RFC) Papers

- RFC 2401—Security Architecture for the Internet Protocol
- RFC 2402—IP Authentication Header
- RFC 2403—The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404—The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405—The ESP DES-CBC Cipher Algorithm With Explicit IV
- RFC 2406—IP Encapsulating Security Payload (ESP)
- RFC 2407—The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408—Internet and Key Management Protocol (ISAKMP)
- RFC 2409—The Internet Key Exchange (IKE)
- RFC 2410—The NULL Encryption Algorithm and Its Use With IPsec
- RFC 2411—IP Security Document Roadmap
- RFC 2412—The OAKLEY Key Determination Protocol

Websites

- Enterprise VPNs—http://www.cisco.com/go/evpn
- Cisco SAFE Blueprint—http://www.cisco.com/go/safe
- Cisco Network Security—http://www.cisco.com/go/security
- Cisco AVVID Partner Program—http://www.cisco.com/go/securityassociates
- 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/warp/public/707/21.html
- Essential IOS Features Every ISP Should Consider—http://www.cisco.com/warp/public/707/EssentialIOSfeatures_pdf.zip
- Increasing Security on IP Networks—http://www.cisco.com/en/US/partner/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml
- Cisco TAC Security Technical Tips—http://www.cisco.com/cgi-bin/Support/browse/index.pl?i=Technologies&f=774
- IPSec Support Page—http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Internetworking:IPSec
- Networking Professionals Connection—http://forums.cisco.com

Acronyms and Definitions

This section contains acronyms and their definitions.

- 3DES—Triple Data Encryption Standard
- ACL—Access control list
- AES—Advanced Encryption Standard
- AH—Authentication Header
- AIM—Advanced Integration Module
- ATM—Asynchronous Transfer Mode
- AVVID—Architecture for Voice, Video, and Integrated Data
- CA—Certificate Authority
- CAC—Call Admission Control
- CANI—Cisco AVVID Network Infrastructure
- CAR—Committed Access Rate
- CBWFQ—Class Based Weighted Fair Queuing
- CEF—Cisco Express Forwarding
- CPE—Customer Premises Equipment
- cRTP—Compressed Real-Time Protocol
- DES—Data Encryption Standard
- DHCP—Dynamic Host Configuration Protocol
- DLSw—Data Link Switching
- DMVPN—Dynamic Multipoint Virtual Private Network
- DMZ—De-Militarized Zone
- DNS—Domain Name Service
- DPD—Dead Peer Detection
- DSL—Digital Subscriber Line
- EIGRP—Enhanced Interior Gateway Routing Protocol
- ESP—Encapsulating Security Protocol
- FIFO—First In First Out
- FQDN—Fully Qualified Domain Name

- FR—Frame Relay
- FRTS—Frame Relay Traffic Shaping
- FTP—File Transfer Protocol
- GRE—Generic Route Encapsulation
- HSRP—Hot Standby Router Protocol
- ICMP—Internet Control Message Protocol
- IKE—Internet Key Exchange
- IOS—Internetwork Operating System
- IP—Internet Protocol
- IPMc—IP Multicast
- IPSec—IP Security
- IP GRE—See GRE
- ISA—Integrated Service Adapter
- ISM—Integrated Service Module
- ISP—Internet Service Provider
- Layer 2—OSI reference model Link Layer
- Layer 3—OSI reference model Network Layer
- Layer 4—OSI reference model Transport Layer
- LFI—Link Fragmentation and Interleaving
- LLQ—Low Latency Queuing
- L2TP—Layer 2 Tunneling Protocol
- MDRR—Modified Deficit Round Robin
- mGRE—Multipoint Generic Route Encapsulation
- MLPPP—Multi-link Point-to-point Protocol
- MPLS—Multi-Protocol Label Switching
- MTU—Maximum Transmission Unit
- NAT—Network Address Translation
- NetFlow—Cisco IOS component, collects and exports traffic statistics
- NHRP—Next Hop Resolution Protocol
- NHS—Next-Hop Server
- NTP—Network Time Protocol
- ODR—On-Demand Routing
- OSPF—Open Shortest Path First
- PAT—Port Address Translation
- PBR—Policy Based Routing
- PE—Premises Equipment
- PPTP—Point-to-Point Tunneling Protocol
- PVC—Permanent Virtual Circuit

- QoS—Quality of service
- RADIUS—Remote Authentication Dial In User System
- RTP—Real-Time Protocol
- SA—Security Association
- SAA—Service Assurance Agent
- SHA-1—Secure Hash Algorithm One
- SLA—Service Level Agreement
- SNMP—Simple Network Management Protocol
- SOHO—Small Office / Home Office
- SRST—Survivable Remote Site Telephony
- TCP—Transmission Control Protocol
- TED—Tunnel Endpoint Discovery
- ToS—Type of service
- UDP—User Datagram Protocol
- VAD—Voice Activity Detection
- VoIP—Voice over IP
- V3PN—Voice and Video Enabled IPSec VPN
- VAM—VPN Acceleration Module
- VPN—Virtual Private Network
- WAN—Wide Area Network
- WRED—Weighted Random Early Detection