



SECURITY

IPSec VPN Design

The definitive design and deployment guide
for secure virtual private networks



IPSec VPN Design

**Vijay Bollapragada
Mohamed Khalid
Scott Wainner**

Cisco Press

800 East 96th Street
Indianapolis, IN 46240 USA

IPSec VPN Design

Table of Contents

Contents

Introduction

Chapter 1 Introduction to VPNs

- Motivations for Deploying a VPN

- VPN Technologies

 - Layer 2 VPNs

 - Layer 3 VPNs

 - Remote Access VPNs

- Summary

Chapter 2 IPSec Overview

- Encryption Terminology

 - Symmetric Algorithms

 - Asymmetric Algorithms

 - Digital Signatures

- IPSec Security Protocols

 - IPSec Transport Mode

 - IPSec Tunnel Mode

 - Encapsulating Security Header (ESP)

 - Authentication Header (AH)

- Key Management and Security Associations

 - The Diffie-Hellman Key Exchange

 - Security Associations and IKE Operation

 - IKE Phase 1 Operation

 - IKE Phase 2 Operation

- IPSec Packet Processing

Table of Contents

Summary

Chapter 3 Enhanced IPsec Features

IKE Keepalives

Dead Peer Detection

Idle Timeout

Reverse Route Injection

RRI and HSRP

Stateful Failover

SADB Transfer

SADB Synchronization

IPsec and Fragmentation

IPsec and PMTUD

Look Ahead Fragmentation

GRE and IPsec

IPsec and NAT

Effect of NAT on AH

Effect of NAT on ESP

Effect of NAT on IKE

IPsec and NAT Solutions

Summary

Chapter 4 IPsec Authentication and Authorization Models

Extended Authentication (XAUTH) and Mode Configuration
(MODE-CFG)

Mode-Configuration (MODECFG)

Easy VPN (EzVPN)

EzVPN Client Mode

Network Extension Mode

Digital Certificates for IPsec VPNs

Digital Certificates

Table of Contents

Certificate Authority Enrollment

Certificate Revocation

Summary

Chapter 5 IPSec VPN Architectures

IPSec VPN Connection Models

IPSec Model

The GRE Model

The Remote Access Client Model

IPSec Connection Model Summary

Hub-and-Spoke Architecture

Using the IPSec Model

Transit Spoke-to-Spoke Connectivity Using IPSec

Internet Connectivity

Scalability Using the IPSec Connection Model

GRE Model

Remote Access Client Connection Model

Scalability of Client Connectivity Models

Full-Mesh Architectures

Native IPSec Connectivity Model

GRE Model

Summary

Chapter 6 Designing Fault-Tolerant IPSec VPNs

Link Fault Tolerance

Backbone Network Fault Tolerance

Access Link Fault Tolerance

Access Link Fault Tolerance Summary

IPSec Peer Redundancy

Simple Peer Redundancy Model

Virtual IPSec Peer Redundancy Using HSRP

Table of Contents

- IPSec Stateful Failover
- Peer Redundancy Using GRE
- Virtual IPSec Peer Redundancy Using SLB
- Server Load Balancing Concepts

IPSec Peer Redundancy Using SLB

- Cisco VPN 3000 Clustering for Peer Redundancy
- Peer Redundancy Summary

Intra-Chassis IPSec VPN Services Redundancy

- Stateless IPSec Redundancy
- Stateful IPSec Redundancy

Summary

Chapter 7 Auto-Configuration Architectures for Site-to-Site IPSec VPNs

IPSec Tunnel Endpoint Discovery

- Principles of TED
- Limitations with TED
- TED Configuration and State
- TED Fault Tolerance

Dynamic Multipoint VPN

- Multipoint GRE Interfaces
- Next Hop Resolution Protocol
- Dynamic IPSec Proxy Instantiation
- Establishing a Dynamic Multipoint VPN
- DMVPN Architectural Redundancy
- DMVPN Model Summary

Summary

Chapter 8 IPSec and Application Interoperability

QoS-Enabled IPSec VPNs

- Overview of IP QoS Mechanisms

Table of Contents

IPSec Implications for Classification

IPSec Implications on QoS Policies

VoIP Application Requirements for IPSec VPN Networks

Delay Implications

Jitter Implications

Loss Implications

IPSec VPN Architectural Considerations for VoIP

Decoupled VoIP and Data Architectures

VoIP over IPSec Remote Access

VoIP over IPSec-Protected GRE Architectures

VoIP Hub-and-Spoke Architecture

VoIP over DMVPN Architecture

VoIP Traffic Engineering Summary

Multicast over IPSec VPNs

Multicast over IPSec-protected GRE

Multicast on Full-Mesh Point-to-Point GRE/IPSec Tunnels

DMVPN and Multicast

Multicast Group Security

Multicast Encryption Summary

Summary

Chapter 9 Network-Based IPSec VPNs

Fundamentals of Network-Based VPNs

The Network-Based IPSec Solution: IOS Features

The Virtual Routing and Forwarding Table

Crypto Keyrings

ISAKMP Profiles

Operation of Network-Based IPSec VPNs

A Single IP Address on the PE

Front-Door and Inside VRF

Table of Contents

Configuration and Packet Flow

Termination of IPSec on a Unique IP Address Per VRF

Network-Based VPN Deployment Scenarios

IPSec to MPLS VPN over GRE

IPSec to L2 VPNs

PE-PE Encryption

Summary

Index