

# **IPSEC VPN DESIGN**

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

Summary

**BUY ONLINE AT:** <http://www.itgovernance.co.uk/products/730>

### **Chapter 3: Enhanced IPSec Features**

IKE Keep alives

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

**BUY ONLINE AT:** <http://www.itgovernance.co.uk/products/730>

Digital Certificates for IPSec VPNs

Digital Certificates

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

Transit Site-to-Site Connectivity

Transit Site-to-Site Connectivity with Internet Access

Scalability of GRE Hub-and-Spoke Models

Remote Access Client Connection Model

Easy VPN (EzVPN) Client Mode

EzVPN Network Extension Mode

Scalability of Client Connectivity Models

Full-Mesh Architectures

**BUY ONLINE AT:** <http://www.itgovernance.co.uk/products/730>

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

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

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

**BUY ONLINE AT: <http://www.itgovernance.co.uk/products/730>**

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

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

**BUY ONLINE AT:** <http://www.itgovernance.co.uk/products/730>

IPSec to L2 VPNs

PE-PE Encryption

Summary

Index

**BUY ONLINE AT:** <http://www.itgovernance.co.uk/products/730>