SECURITY

IKEv2 IPsec Virtual Private Networks

Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS

Graham Bartlett, CCIE No. 26709
Amjad Inamdar, CISSP No. 460898

ciscopress.com

Exclusive Offer – 40% OFF

Cisco Press Video Training

livelessons

ciscopress.com/video

Use coupon code CPVIDEO40 during checkout.

Video Instruction from Technology Experts

Advance Your Skills

Get started with fundamentals, become an expert, or get certified.

Train Anywhere

Train anywhere, at your own pace, on any device.

Learn

Learn from trusted author trainers published by Cisco Press.

Try Our Popular Video Training for FREE!

ciscopress.com/video

Explore hundreds of FREE video lessons from our growing library of Complete Video Courses, LiveLessons, networking talks, and workshops.

Cisco Press ciscopress.com/video

ALWAYS LEARNING PEARSON

IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS

Table of Contents

Cover
Title Page
Copyright Page
Contents
Foreword
Introduction
Part I: Understanding IPsec VPNs
Chapter 1 Introduction to IPsec VPNs
The Need and Purpose of IPsec VPNs
Building Blocks of IPsec
Security Protocols
Security Associations
Key Management Protocol
IPsec Security Services
Access Control
Anti-replay Services
Confidentiality
Connectionless Integrity
Data Origin Authentication
Traffic Flow Confidentiality
Components of IPsec
Security Parameter Index
Security Policy Database

Table of Contents

Security Association Database

Peer Authorization Database

Lifetime

Cryptography Used in IPsec VPNs

Symmetric Cryptography

Asymmetric Cryptography

The Diffie-Hellman Exchange

Public Key Infrastructure

Public Key Cryptography

Certificate Authorities

Digital Certificates

Digital Signatures Used in IKEv2

Pre-Shared-Keys, or Shared Secret

Encryption and Authentication

IP Authentication Header

Anti-Replay

IP Encapsulating Security Payload (ESP)

Authentication

Encryption

Anti-Replay

Encapsulation Security Payload Datagram Format

Encapsulating Security Payload Version 3

Extended Sequence Numbers

Traffic Flow Confidentiality

Dummy Packets

Modes of IPsec

Cover

IPsec Transport Mode

IPsec Tunnel Mode

Summary

References

Part II: Understanding IKEv2

Table of Contents

Chapter 2 IKEv2: The Protocol

- IKEv2 Overview
- The IKEv2 Exchange
- IKE_SA_INIT
  - Diffie-Hellman Key Exchange
  - Security Association Proposals
  - Security Parameter Index (SPI)
  - Nonce
  - Cookie Notification
  - Certificate Request
  - HTTP_CERT_LOOKUP_SUPPORTED
- Key Material Generation
- IKE_AUTH
  - Encrypted and Authenticated Payload
  - Encrypted Payload Structure
  - Identity
  - Authentication
  - Signature-Based Authentication
  - (Pre) Shared-Key-Based Authentication
  - EAP
  - Traffic Selectors
  - Initial Contact
- CREATE_CHILD_SA
  - IPsec Security Association Creation
  - IPsec Security Association Rekey
  - IKEv2 Security Association Rekey
- IKEv2 Packet Structure Overview
- The INFORMATIONAL Exchange
  - Notification
  - Deleting Security Associations
  - Configuration Payload Exchange
  - Dead Peer Detection/Keepalive/NAT Keepalive
  - IKEv2 Request Response

Table of Contents

IKEv2 and Network Address Translation

NAT Detection

Additions to RFC 7296

RFC 5998 An Extension for EAP-Only Authentication in IKEv2

RFC 5685 Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)

RFC 6989 Additional Diffie-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2)

RFC 6023 A Childless Initiation of the Internet Key Exchange Version 2 (IKEv2) Security Association (SA)

Summary

References

Chapter 3 Comparison of IKEv1 and IKEv2

Brief History of IKEv1

Exchange Modes

IKEv1

IKEv2

Anti-Denial of Service

Lifetime

Authentication

High Availability

Traffic Selectors

Use of Identities

Network Address Translation

Configuration Payload

Mobility & Multi-homing

Matching on Identity

Reliability

Cryptographic Exchange Bloat

Combined Mode Ciphers

Continuous Channel Mode

Summary

Table of Contents

References

Part III: IPsec VPNs on Cisco IOS

Chapter 4 IOS IPsec Implementation

Modes of Encapsulation

GRE Encapsulation

GRE over IPsec

IPsec Transport Mode with GRE over IPsec

IPsec Tunnel mode with GRE over IPsec

Traffic

Multicast Traffic

Non-IP Protocols

The Demise of Crypto Maps

Interface Types

Virtual Interfaces: VTI and GRE/IPsec

Traffic Selection by Routing

Static Tunnel Interfaces

Dynamic Tunnel Interfaces

sVTI and dVTI

Multipoint GRE

Tunnel Protection and Crypto Sockets

Implementation Modes

Dual Stack

Mixed Mode

Auto Tunnel Mode

VRF-Aware IPsec

VRF in Brief

VRF-Aware GRE and VRF-Aware IPsec

VRF-Aware GRE over IPsec

Summary

Reference

Part IV: IKEv2 Implementation

Table of Contents

Chapter 5 IKEv2 Configuration

IKEv2 Configuration Overview

The Guiding Principle

Scope of IKEv2 Configuration

IKEv2 Configuration Constructs

IKEv2 Proposal

Configuring the IKEv2 Proposal

Configuring IKEv2 Encryption

Configuring IKEv2 Integrity

Configuring IKEv2 Diffie-Hellman

Configuring IKEv2 Pseudorandom Function

Default IKEv2 Proposal

IKEv2 Policy

Configuring an IKEv2 Policy

Configuring IKEv2 Proposals under IKEv2 Policy

Configuring Match Statements under IKEv2 Policy

Default IKEv2 Policy

IKEv2 Policy Selection on the Initiator

IKEv2 Policy Selection on Responder

IKEv2 Policy Configuration Examples

Per-peer IKEv2 Policy

IKEv2 Policy with Multiple Proposals

IKEv2 Keyring

Configuring IKEv2 Keyring

Configuring a Peer Block in Keyring

Key Lookup on Initiator

Key Lookup on Responder

IKEv2 Keyring Configuration Example

IKEv2 Keyring Key Points

IKEv2 Profile

IKEv2 Profile as Peer Authorization Database

Configuring IKEv2 Profile

Configuring Match Statements in IKEv2 Profile

Table of Contents

Matching any Peer Identity

Defining the Scope of IKEv2 Profile

Defining the Local IKE Identity

Defining Local and Remote Authentication Methods

IKEv2 Dead Peer Detection

IKEv2 Initial Contact

IKEv2 SA Lifetime

NAT Keepalives

IVRF (inside VRF)

Virtual Template Interface

Disabling IKEv2 Profile

Displaying IKEv2 Profiles

IKEv2 Profile Selection on Initiator and Responder

IKEv2 Profile Key Points

IKEv2 Global Configuration

HTTP URL-based Certificate Lookup

IKEv2 Cookie Challenge

IKEv2 Call Admission Control

IKEv2 Window Size

Dead Peer Detection

NAT Keepalive

IKEv2 Diagnostics

PKI Configuration

Certificate Authority

Public-Private Key Pair

PKI Trustpoint

PKI Example

IPsec Configuration

IPsec Profile

IPsec Configuration Example

Smart Defaults

Summary

Chapter 6 Advanced IKEv2 Features

Table of Contents

Introduction to IKEv2 Fragmentation

IP Fragmentation Overview

IKEv2 and Fragmentation

IKEv2 SGT Capability Negotiation

IKEv2 Session Authentication

IKEv2 Session Deletion on Certificate Revocation

IKEv2 Session Deletion on Certificate Expiry

IKEv2 Session Lifetime

Summary

References

Chapter 7 IKEv2 Deployments

Pre-shared-key Authentication with Smart Defaults

Elliptic Curve Digital Signature Algorithm Authentication

RSA Authentication Using HTTP URL Lookup

IKEv2 Cookie Challenge and Call Admission Control

Summary

Part V: FlexVPN

Chapter 8 Introduction to FlexVPN

FlexVPN Overview

The Rationale

FlexVPN Value Proposition

FlexVPN Building Blocks

IKEv2

Cisco IOS Point-to-Point Tunnel Interfaces

Configuring Static P2P Tunnel Interfaces

Configuring Virtual-Template Interfaces

Auto-Detection of Tunnel Encapsulation and Transport

Benefits of Per-Peer P2P Tunnel Interfaces

Cisco IOS AAA Infrastructure

Configuring AAA for FlexVPN

IKEv2 Name Mangler

Table of Contents

Configuring IKEv2 Name Mangler
Extracting Name from FQDN Identity
Extracting Name from Email Identity
Extracting Name from DN Identity
Extracting Name from EAP Identity
IKEv2 Authorization Policy
Default IKEv2 Authorization Policy
FlexVPN Authorization
Configuring FlexVPN Authorization
FlexVPN User Authorization
FlexVPN User Authorization, Using an External AAA Server
FlexVPN Group Authorization
FlexVPN Group Authorization, Using a Local AAA Database
FlexVPN Group Authorization, Using an External AAA Server
FlexVPN Implicit Authorization
FlexVPN Implicit Authorization Example
FlexVPN Authorization Types: Co-existence and Precedence
User Authorization Taking Higher Precedence
Group Authorization Taking Higher Precedence
FlexVPN Configuration Exchange
Enabling Configuration Exchange
FlexVPN Usage of Configuration Payloads
Configuration Attributes and Authorization
Configuration Exchange Examples
FlexVPN Routing
Learning Remote Subnets Locally
Learning Remote Subnets from Peer
Summary
Chapter 9 FlexVPN Server
Sequence of Events
EAP Authentication
EAP Methods

Table of Contents

- EAP Message Flow
- EAP Identity
- EAP Timeout
- EAP Authentication Steps
- Configuring EAP
- EAP Configuration Example

AAA-based Pre-shared Keys

- Configuring AAA-based Pre-Shared Keys
- RADIUS Attributes for AAA-Based Pre-Shared Keys
- AAA-Based Pre-Shared Keys Example

Accounting

Per-Session Interface

- Deriving Virtual-Access Configuration from a Virtual Template
- Deriving Virtual-Access Configuration from AAA Authorization
- The interface-config AAA Attribute
- Deriving Virtual-Access Configuration from an Incoming Session
- Virtual-Access Cloning Example

Auto Detection of Tunnel Transport and Encapsulation

RADIUS Packet of Disconnect

- Configuring RADIUS Packet of Disconnect
- RADIUS Packet of Disconnect Example

RADIUS Change of Authorization (CoA)

- Configuring RADIUS CoA
- RADIUS CoA Examples
- Updating Session QoS Policy, Using CoA
- Updating the Session ACL, Using CoA

IKEv2 Auto-Reconnect

- Auto-Reconnect Configuration Attributes
- Smart DPD
- Configuring IKEv2 Auto-Reconnect

User Authentication, Using AnyConnect-EAP

- AnyConnect-EAP

Table of Contents

AnyConnect-EAP XML Messages for User Authentication

Configuring User Authentication, Using AnyConnect-EAP

AnyConnect Configuration for Aggregate Authentication

Dual-factor Authentication, Using AnyConnect-EAP

AnyConnect-EAP XML Messages for dual-factor authentication

Configuring Dual-factor Authentication, Using AnyConnect-EAP

RADIUS Attributes Supported by the FlexVPN Server

Remote Access Clients Supported by FlexVPN Server

FlexVPN Remote Access Client

Microsoft Windows7 IKEv2 Client

Cisco IKEv2 AnyConnect Client

Summary

Reference

Chapter 10 FlexVPN Client

Introduction

FlexVPN Client Overview

FlexVPN Client Building Blocks

IKEv2 Configuration Exchange

Static Point-to-Point Tunnel Interface

FlexVPN Client Profile

Object Tracking

NAT

FlexVPN Client Features

Dual Stack Support

EAP Authentication

Dynamic Routing

Support for EzVPN Client and Network Extension Modes

Advanced Features

Setting up the FlexVPN Server

EAP Authentication

Split-DNS

Components of Split-DNS

Table of Contents

Windows Internet Naming Service (WINS)

Domain Name

FlexVPN Client Profile

Backup Gateways

Resolution of Fully Qualified Domain Names

Reactivating Peers

Backup Gateway List

Tunnel Interface

Tunnel Source

Tunnel Destination

Tunnel Initiation

Automatic Mode

Manual Mode

Track Mode

Tracking a List of Objects, Using a Boolean Expression

Dial Backup

Backup Group

Network Address Translation

Design Considerations

Use of Public Key Infrastructure and Pre-Shared Keys

The Power of Tracking

Tracked Object Based on Embedded Event Manager

Troubleshooting FlexVPN Client

Useful Show Commands

Debugging FlexVPN Client

Clearing IKEv2 FlexVPN Client Sessions

Summary

Chapter 11 FlexVPN Load Balancer

Introduction

Components of the FlexVPN Load Balancer

IKEv2 Redirect

Table of Contents

Hot Standby Routing Protocol

FlexVPN IKEv2 Load Balancer

Cluster Load

IKEv2 Redirect

Redirect Loops

FlexVPN Client

Troubleshooting IKEv2 Load Balancing

IKEv2 Load Balancer Example

Summary

Chapter 12 FlexVPN Deployments

Introduction

FlexVPN AAA-Based Pre-Shared Keys

Configuration on the Branch-1 Router

Configuration on the Branch-2 Router

Configuration on the Hub Router

Configuration on the RADIUS Server

FlexVPN User and Group Authorization

FlexVPN Client Configuration at Branch 1

FlexVPN Client Configuration at Branch 2

Configuration on the FlexVPN Server

Configuration on the RADIUS Server

Logs Specific to FlexVPN Client-1

Logs Specific to FlexVPN Client-2

FlexVPN Routing, Dual Stack, and Tunnel Mode Auto

FlexVPN Spoke Configuration at Branch-1

FlexVPN Spoke Configuration at Branch-2

FlexVPN Hub Configuration at the HQ

Verification on FlexVPN Spoke at Branch-1

Verification on FlexVPN Spoke at Branch-2

Verification on the FlexVPN Hub at HQ

FlexVPN Client NAT to the Server-Assigned IP Address

Configuration on the FlexVPN Client

Table of Contents

Verification on the FlexVPN Client

FlexVPN WAN Resiliency, Using Dynamic Tunnel Source

FlexVPN Client Configuration on the Dual-Homed Branch Router

Verification on the FlexVPN Client

FlexVPN Hub Resiliency, Using Backup Peers

FlexVPN Client Configuration on the Branch Router

Verification on the FlexVPN Client

FlexVPN Backup Tunnel, Using Track-Based Tunnel Activation

Verification on the FlexVPN Client

Summary

Part VI: IPsec VPN Maintenance

Chapter 13 Monitoring IPsec VPNs

Introduction to Monitoring

Authentication, Authorization, and Accounting (AAA)

NetFlow

Simple Network Management Protocol

VRF-Aware SNMP

Syslog

Monitoring Methodology

IP Connectivity

VPN Tunnel Establishment

Cisco IPsec Flow Monitor MIB

SNMP with IKEv2

Syslog

Pre-Shared Key Authentication

PKI Authentication

EAP Authentication

Authorization Using RADIUS-Based AAA

Data Encryption: SNMP with IPsec

Overlay Routing

Data Usage

Summary

Table of Contents

References

Chapter 14 Troubleshooting IPsec VPNs

Introduction

Tools of Troubleshooting

Show Commands

Syslog Messages

Event-Trace Monitoring

Debugging

IKEv2 Debugging

IPsec Debugging

Key Management Interface Debugging

PKI Debugging

Conditional Debugging

IP Connectivity

VPN Tunnel Establishment

IKEv2 Diagnose Error

Troubleshooting the IKE_SA_INIT Exchange

Troubleshooting the IKE_AUTH Exchange

Authentication

Troubleshooting RSA or ECDSA Authentication

Certificate Attributes

Debugging Authentication Using PKI

Certificate Expiry

Matching Peer Using Certificate Maps

Certificate Revocation

Trustpoint Configuration

Trustpoint Selection

Pre-Shared Key

Extensible Authentication Protocol (EAP)

Authorization

Data Encryption

Debugging IPsec

Pearson

Table of Contents

IPsec Anti-Replay

Data Encapsulation

Mismatching GRE Tunnel Keys

Overlay Routing

Static Routing

IKEv2 Routing

Dynamic Routing Protocols

Summary

References

Part VII: IPsec Overhead

Chapter 15 IPsec Overhead and Fragmentation

Introduction

Computing the IPsec Overhead

General Considerations

IPsec Mode Overhead (without GRE)

GRE Overhead

Encapsulating Security Payload Overhead

Authentication Header Overhead

Encryption Overhead

Integrity Overhead

Combined-mode Algorithm Overhead

Plaintext MTU

Maximum Overhead

Maximum Encapsulation Security Payload Overhead

Maximum Authentication Header Overhead

Extra Overhead

IPsec and Fragmentation

Maximum Transmission Unit

Fragmentation in IPv4

Fragmentation in IPv6

Path MTU Discovery

TCP MSS Clamping

Table of Contents

MSS Refresher

MSS Adjustment

IPsec Fragmentation and PMTUD

Fragmentation on Tunnels

IPsec Only (VTI)

GRE Only

GRE over IPsec

Tunnel PMTUD

The Impact of Fragmentation

Summary

References

Part VIII: Migration to IKEv2

Chapter 16 Migration Strategies

Introduction to Migrating to IKEv2 and FlexVPN

Consideration when Migrating to IKEv2

Hardware Limitations

Current VPN Technology

Routing Protocol Selection

Restrictions When Running IKEv1 and IKEv2 Simultaneously

Current Capacity

IP Addresses

Software

Amending the VPN Gateway

Global IKE and IPsec Commands

FlexVPN Features

Familiarization

Client Awareness

Public Key Infrastructure

Internet Protocol Version 6

Authentication

High Availability

Asymmetric Routing

Table of Contents

Migration Strategies

Hard Migration

Soft Migration

Soft Migration Example

Migration Verification

Consideration for Topologies

Site-to-Site

Hub and Spoke

Remote Access

Summary

Index