FlexVPN Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)

January 2014
OL-31239-01

This document provides an overview of how to configure FlexVPN on Cisco 1000 Series Connected Grid Routers (hereafter referred to as the CGR 1000). This document includes the following sections:

Information About FlexVPN

FlexVPN is a flexible and scalable Virtual Private Network (VPN) solution. The Static Virtual Tunnel Interface (SVTI) VPN model that the CGR 1000 used previously required explicit management of tunnel endpoints and associated routes, which is not scalable. FlexVPN simplifies the deployment of VPNs by providing a unified VPN framework that is compatible with legacy VPN technologies.

Benefits

FlexVPN provides the following benefits:

- Based on open standards-based IKEv2 security technology
- Integrates various topologies and VPN functions under one framework

Cisco Systems, Inc.
www.cisco.com

- Can coexist with previous VPN configurations
- Allows use of a single tunnel for both IPv4 and IPv6
- Uses virtual interfaces, which allow per-spoke features such as firewalls, ACLs, and QoS
- Supports static and dynamic routing
- Minimizes configuration by using IKEv2 Smart Defaults (see the "Default Settings" section on page 4)

Standards

FlexVPN implements the following standards:

- IP Security (IPsec)—A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses Internet Key Exchange (IKE) to handle negotiation of protocols and algorithms based on the local policy, and generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.
- Internet Key Exchange Version 2 (IKEv2)—A key exchange protocol that provides authentication of IPsec peers, negotiates IPsec security associations, and establishes IPsec keys.

  For more information about supported standards and component technologies, see the "Supported Standards for Use with IKE" section in the "Configuring Internet Key Exchange for IPsec VPNs" module in the Internet Key Exchange for IPsec VPNs Configuration Guide, Cisco IOS Release 15M&T.

Topologies

The CGR 1000 supports these topologies in FlexVPN configurations:

- Site-to-site—Basic IKEv2 configuration between two sites
- Hub-to-spoke—Multiple routers connected to a hub router using virtual access interfaces and P2P tunnels. In this configuration, the CGR 1000 functions as a client (spoke).

Note The CGR 1000 supports only the FlexVPN site-to-site and FlexVPN client features. Other FlexVPN capabilities are not supported and so are not described in this document.

Key Terms

- IKEv2 initiator—An IKE peer that initiates an IKE exchange.
- IKEv2 responder—An IKE peer that responds to a request for an IKE exchange.
- IKEv2 Name Mangler—Used to derive the username for IKEv2 authorization and obtain the AAA preshared key from the peer IKE identity.
- AAA-based pre-shared key—Shared secret stored on a RADIUS server.
- IKEv2 Authorization—Provides policy for authenticated session.
- Config-mode—Allows IKE peers to exchange configuration information such as IP addresses and subnets. The IKEv2 authorization is the source of the config-mode data.

Supported Features

The CGR 1000 supports the IKEv2 FlexVPN client feature. Functioning as the FlexVPN client (spoke) in a hub-and-spoke configuration, the CGR 1000 establishes a secure IPsec VPN tunnel to a FlexVPN server such as the Cisco ASR 1000 Series Router. Each FlexVPN client is associated with a unique tunnel interface, which implies that the IPsec security association (SA) retrieved by the specific FlexVPN client is bound to the tunnel interface.

Client capabilities include:

- GRE encapsulation support that allows IPv4/IPv6 over IPv4 /IPv6
- Dynamic routing protocol support
- Route exchange through config-mode
- Dynamic BGP peering through config-mode
- Backup Gateways
- Dial backup
- Split DNS
- NAT
- Learning Peer Networks

For more information about the FlexVPN client and related features, see the section Information About the FlexVPN Client in the FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS Release 15M&T.

Prerequisites

To configure FlexVPN, you should be familiar with the concepts and tasks in the documents listed in the "Related Documents" section on page 6.

Guidelines and Limitations

- You cannot configure an option that is not supported on a specific platform. For example, in a security protocol, the capability of the hardware-crypto engine is important, and you cannot specify the Triple Data Encryption Standard (3DES) or the Advanced Encryption Standard (AES) type of encryption transform in a nonexportable image, or specify an encryption algorithm that a crypto engine does not support.
- Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption white paper.
- If your network is live, make sure that you understand the potential impact of any command.
- CGR 1000 performance may degrade when the following encryption algorithms are used because they are supported only using the software-crypto engine: DES, 3DES, SEAL, MD5, and GMAC.
- Secure Sockets Layer VPN (SSLVPN) is not supported.

Default Settings

The IKEv2 Smart Defaults feature minimizes the FlexVPN configuration by covering most of the use cases. IKEv2 smart defaults can be customized for specific use cases, though this is not recommended.

For more information about smart defaults, see the “IKEv2 Smart Defaults” section in the “Information About Internet Key Exchange Version 2” module in the FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS Release 15M&T.

Configuring FlexVPN

This section lists the tasks in the FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS Release 15M&T required to configure FlexVPN site-to-site and FlexVPN client.

Configuring FlexVPN Site-to-Site

To configure FlexVPN site-to-site, perform these tasks in the section How to Configure Internet Key Exchange Version 2 in the FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS Release 15M&T:

- Configuring Basic Internet Key Exchange Version 2 CLI Constructs
  - Configuring the IKEv2 Key Ring
  - Configuring an IKEv2 Profile (Basic)
- Configuring Advanced Internet Key Exchange Version 2 CLI Constructs
  - Configuring Global IKEv2 Options
  - Configuring IKEv2 Fragmentation
  - Configuring IKEv2 Proposal
  - Configuring IKEv2 Policies

Configuring FlexVPN Client

To configure the FlexVPN client, perform these tasks in the How to Configure the FlexVPN Client section in the FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS Release 15M&T:

- Configuring the IKEv2 VPN Client Profile
  - Configuring the Tunnel Interface
  - Configuring the FlexVPN Client
  - Configuring EAP as the Local Authentication Method

Verifying Configuration

Note With the Smart Defaults feature, a default configuration is displayed in the corresponding **show** command with **default** as a keyword and with no argument. For example, the **show crypto ikev2 proposal default** command displays the default IKEv2 proposal, and the **show crypto ikev2 proposal** command displays the default IKEv2 proposal, along with any user-configured proposals.

Command	Purpose
show crypto ikev2 authorization policy [*policy-name* | **default**]	Displays the IKEv2 authorization policy.
show crypto ikev2 proposal [*proposal-name* | **default**]	Displays the IKEv2 proposal.
show crypto ikev2 policy [*policy-name* | **default**]	Displays the IKEv2 policy.
show crypto ikev2 profile [*profile-name* | **default**]	Displays the IKEv2 profile.
show crypto ikev2 sa	Displays the settings used by current security associations (SAs).
show crypto ikev2 session	Displays the status of active IKEv2 sessions.
show crypto ipsec profile	Displays the IPsec profile.
show crypto ipsec transform-set	Displays the configured transform sets or active default transform sets.

Configuration Example

See the following sections in the FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS Release 15M&T for configuration examples:

- Configuration Examples for Internet Key Exchange Version 2
- Configuration Examples for the FlexVPN Client

Related Documents

- FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS Release 15M&T
- Internet Key Exchange for IPsec VPNs Configuration Guide, Cisco IOS Release 15M&T
- Security for VPNs with IPsec Configuration Guide, Cisco IOS Release 15M&T
- Next Generation Encryption

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documents" section.