Introduction to FlexVPN

Internet Key Exchange Version 2 (IKEv2), a next-generation key management protocol based on RFC 4306, is an enhancement of the IKE Protocol. IKEv2 is used for performing mutual authentication and establishing and maintaining security associations (SAs).

FlexVPN is Cisco's implementation of the IKEv2 standard featuring a unified paradigm and CLI that combines site to site, remote access, hub and spoke topologies and partial meshes (spoke to spoke direct). FlexVPN offers a simple but modular framework that extensively uses the tunnel interface paradigm while remaining compatible with legacy VPN implementations using crypto maps.

This guide contains the following modules:

Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Remote Access

This module describes IKEv2 CLI and is divided into basic and advanced sections.

The basic section introduces basic IKEv2 commands and describes IKEv2 smart defaults and the mandatory IKEv2 commands required for FlexVPN remote access. This module is a prerequisite for understanding subsequent chapters.

The advanced section describes global IKEv2 commands and how to override the default IKEv2 commands.

Configuring FlexVPN Server

This module describes FlexVPN server features, IKEv2 commands required to configure FlexVPN server, remote access clients and the supported RADIUS attributes.

Configuring FlexVPN Client

This module describes FlexVPN client features and the IKEv2 commands required for FlexVPN client.

Configuring IKEv2 Load Balancer

This module describes the IKEv2 Load Balancer Support feature and the IKEv2 commands required to configure the IKEv2 Load Balancer.

Configuring IKEv2 Fragmentation

The IKE Fragmentation adhering to RFC feature implements fragmentation of Internet Key Exchange Version 2 (IKEv2) packets as proposed in the IETF **draft-ietf-ipsecme-ikev2-fragmentation-10** document.

Configuring IKEv2 Reconnect

The IOS IKEv2 support for AutoReconnect feature of AnyConnect feature helps in reestablishing IKEv2 negotiation without user interaction with the Cisco AnyConnect client.

Configuring IKEv2 Packet of Disconnect

The IKEv2 Remote Access Change of Authorization (CoA)—Packet of Disconnect feature terminates an active crypto IKEv2 session on Cisco supported devices.

Configuring IKEv2 Change of Authorization Support

The FlexVPN - IKEv2 CoA for QoS and ACL feature supports RADIUS Change of Authorization (CoA) on an active IKEv2 crypto session.

Configuring Aggregate Authentication

The FlexVPN RA - Aggregate Auth Support for AnyConnect feature implements aggregate authentication method by extending support for Cisco AnyConnect client that uses the proprietary AnyConnect EAP

authentication method to establish a secure tunnel over the Internet between Cisco AnyConnect client and FlexVPN server.

Appendix: FlexVPN RADIUS Attributes

This module describes the RADIUS attributes supported by FlexVPN server.

Appendix: IKEv2 and Legacy VPNs

This module contains configuration examples on how to configure legacy VPNs such as crypto maps and DMVPN with Internet Key Exchange Version 2 (IKEv2).