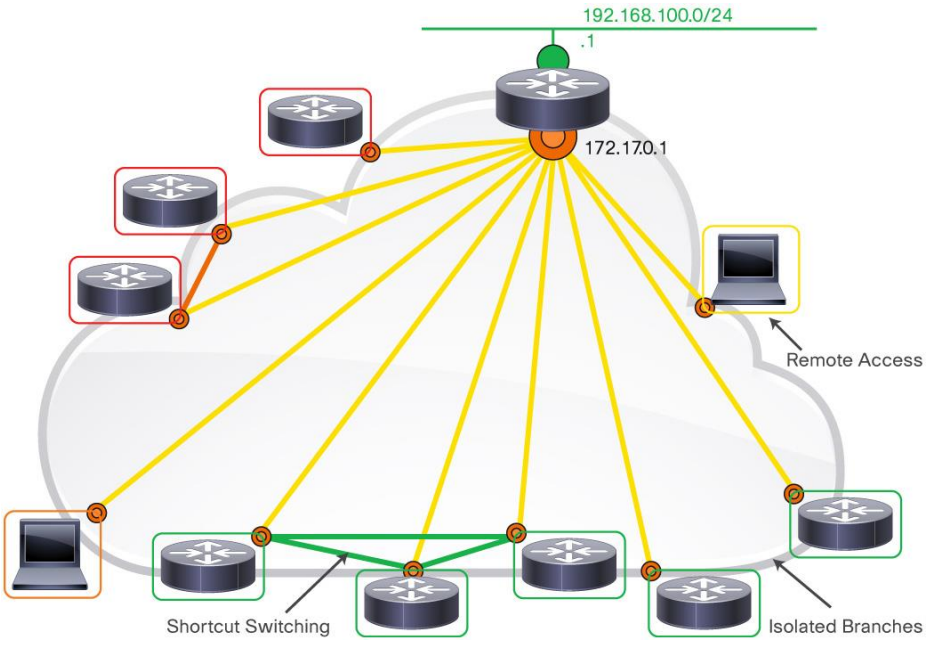
Cisco IOS FlexVPN

Large customers deploying IPSec VPN over IP networks are faced with high complexity and high cost of deploying multiple types of VPN to meet different types of connectivity requirements. Customers often have to learn different types of VPNs to manage and operate different types of network. And once a technology is selected for a deployment, migrating or adding functionality to enhance the VPN is often avoided. FlexVPN was created to simplify the deployment of VPNs, to address the complexity of multiple solutions, and as a unified ecosystem to cover all types of VPN: remote access, teleworker, site to site, mobility, managed security services, and others. See Figure 1.

As customer networks increase spans over private, public, and cloud systems, unifying the VPN technology becomes essential, and it became more important to address the need for simplification of design and configuration. Customers can dramatically increase the reach of their network without significantly expanding the complexity of the infrastructure by using Cisco IOS® FlexVPN. FlexVPN is a robust, standards-based encryption technology that helps enable large organizations to securely connect branch offices and remote users and provides significant cost savings compared to supporting multiple separate types of VPN solutions such as GRE, Crypto, and VTI-based solutions. FlexVPN relies on open-standards-based IKEv2 as a security technology and provides on top of it many Cisco® specific enhancements to provide high levels of security, added value, and competitive differentiations.

Figure 1. Typical Cisco IOS FlexVPN Deployment



Cisco IOS FlexVPN Features and Benefits

Cisco IOS FlexVPN is a unified VPN solution and provides the following benefits:

- **Transport network:** FlexVPN can be deployed either over a public internet or a private Multiprotocol Label Switching (MPLS) VPN network.
- **Deployment style:** Designed for the concentration of both site-to-site and remote access VPNs, one single FlexVPN deployment can accept both types of connection requests at the same time.
- **Failover redundancy:** Three different kinds of redundancy model can be implemented with FlexVPN:
  - Dynamic routing protocols (such as Open Shortest Path First [OSPF], Enhanced Interior Gateway Routing Protocol [EIGRP], Border Gateway Protocol [BGP]) over FlexVPN tunnels. Path/head-end selection is based on dynamic routing metrics.
  - IKEv2-based dynamic route distribution and server clustering.
  - IPsec/IKEv2 active/standby stateful failover between two chassis (available in the future).
- **Third-party compatibility:** As the IT world transitions to cloud- and mobile-based computing, more and more VPN routers and VPN endpoints from different vendors are required. The Cisco IOS FlexVPN solution provides compatibility with any IKEv2-based third-party VPN vendors, including native VPN clients from Apple iOS and Android devices.
- **IP Multicast support:** FlexVPN natively supports IP Multicast in two ways:
  - FlexVPN hub router replicates IP Multicast packets for each spoke.
  - If the transport network supports native IP Multicast, the FlexVPN hub router can choose to have the transport network do multicast packet replication after IPsec encryption (available in the future).
- **Superior quality of service (QoS):** The architecture of Cisco IOS FlexVPN easily allows hierarchical QoS to be integrated at the per tunnel or per SA basis:
  - Per tunnel QoS for each spoke at the FlexVPN hub router.
  - Per tunnel QoS dynamically applied to direct traffic between spokes (available in the future).
- **Centralized policy control:** VPN dynamic policies such as split-tunnel policy, encryption network policy, Virtual Route Forwarding (VRF) selection, Domain Name System (DNS) server (for remote access), and so on can be fully integrated with the authentication, authorization, and accounting (AAA)/RADIUS server and applied at a per peer basis.
- **VRF awareness:** The Cisco IOS FlexVPN solution can be fully integrated with MPLS VPN networks for service provider type of deployment. Both Inside VRF and front-door VRF are supported. Inside VRF assignment policy can be managed by the centralized AAA server.

Table 1 lists the platforms supported by Cisco IOS Flex VPN.

Table 1. Platform Support

Product	Platforms Supported
Cisco 800 Series Routers	Cisco 819, 86X (nonwireless), 881, 888, 88X, and 89X
Cisco 1900 Series Integrated Services Routers	Cisco 1921,1941 and 1941W
Cisco 2900 Series Integrated Services Routers	Cisco 2901, 2911, 2921, and 2951
Cisco 3900 Series Integrated Service Routers	Cisco 3925, 3945, 3925E, and 3945E
Cisco ASR 1000 Series Aggregation Services Routers	Cisco ASR 1001,1002, 1004, 1006, and 1013
Cisco 4400 Series Integrated Services Routers	Cisco 4451-X

Additional Resources

For more information about the Cisco IOS FlexVPN solution and other IPsec VPN technologies, visit the following web pages:

- Cisco IOS FlexVPN Configuration Guide: http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-flex-vpn-15-2mt-book.html
- Cisco IOS Software 15.2M/T Release Notes: http://www.cisco.com/en/US/partner/docs/ios/15_2m_and_t/release/notes/15_2m_and_t.html
- Cisco IOS FlexVPN Command References (look under **Security and VPN**): http://www.cisco.com/en/US/partner/products/ps11746/prod_command_reference_list.html
- IPsec VPN Design: http://www.ciscopress.com/bookstore/product.asp?isbn=1587051117

Please note the configuration examples; the documentation demonstrates how Cisco IOS FlexVPN can secure and protect your network. For specific Cisco ISR and ASR 1000 platform performance and scalability concerns, please contact a Cisco representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-704277-02 10/14