



Fragmentation of IKE Packets

First Published: September 12, 2008

Last Updated: September 19, 2008

Some third-party vendor devices, such as firewalls configured for stateful packet inspection, do not permit the passthrough of User Datagram Protocol (UDP) fragments in case they are part of a fragmentation attack. If all fragments are not passed through, Internet Key Exchange (IKE) negotiation fails because the intended responder for the virtual private network (VPN) tunnel cannot reconstruct the IKE packet and proceed with establishment of the tunnel.

This feature provides for the fragmentation of large IKE packets into a series of smaller IKE packets to avoid fragmentation at the UDP layer (for example, for large certificate payloads or certificate request payloads).

This feature provides support for Cisco IOS in terms of being a responder in an IKE main mode exchange.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Fragmentation of IKE Packets” section on page 6](#).

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Fragmentation of IKE Packets, page 2](#)
- [Restrictions for Fragmentation of IKE Packets, page 2](#)
- [Information About Fragmentation of IKE Packets, page 2](#)
- [How to Configure Fragmentation of IKE Packets, page 3](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- [Configuration Examples for Fragmentation of IKE Packets, page 3](#)
- [Additional References, page 4](#)
- [Feature Information for Fragmentation of IKE Packets, page 6](#)

Prerequisites for Fragmentation of IKE Packets

- You must be using Cisco IOS software Release 12.4(15)T7 or a later release.
- The Easy VPN software client must be configured to support Network Address Translation Transversal (NAT-T) or TCP transport for the client to send the fragmentation vendor-ID.

Restrictions for Fragmentation of IKE Packets

- IKE fragmentation must be proposed and supported by the initiator of the IKE exchange. You should consult documentation for Cisco Easy VPN clients to determine their capabilities for this feature.
- Do not use this feature with Cisco Easy VPN software client versions 5.01 through 5.03 because their use could lead to problems. Versions earlier than version 5.01 are not impacted, and the issue has been addressed in versions later than version 5.03.
- This feature does not support fragmentation during aggressive mode, configuration mode, or quick mode.

Information About Fragmentation of IKE Packets

The Fragmentation of IKE Packets feature provides for the fragmentation of large IKE packets into a series of smaller IKE packets to avoid fragmentation at the UDP layer (for example, for large certificate payloads or certificate request payloads).

The original IKE packet is checked for size against the minimum possible maximum transmission unit (MTU) size of 576 bytes and split into a series of smaller fragments. Each fragment is an individual IKE packet that has its own IKE header and is afforded the same protection as negotiated at the start of the IKE exchange.

A vendor_ID indicates the capability of the initiator to support IKE fragmentation. The Cisco IOS responder, if configured to support IKE fragmentation, responds with the same vendor_ID, thus acknowledging the capability to support IKE fragmentation if required.

The vendor_IDs are exchanged in the first two main-mode exchanges so that fragmentation of packets does not occur until at least the main mode 3 (MM3) exchange.

This feature provides support for Cisco IOS in terms of being a responder in an IKE main mode exchange.

After the capabilities have been agreed upon, fragmentation occurs automatically.

If all fragments in a series are not received within the normal course of the IKE exchanges, current IKE retransmission processes are used to request that information be resent.

**Note**

If an IKE packet is not greater than 576 bytes in size, the packet is not fragmented.

This feature is supported for IKE via port 500, IKE via port 4500 (NAT-T), and TCP wrappers.

After configuration, the feature is enabled on the router in global configuration mode so that all incoming IKE connection requests are possible candidates for fragmentation.

How to Configure Fragmentation of IKE Packets

To configure fragmentation of IKE packets, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp fragmentation**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp fragmentation Example: Router (config)# crypto isakmp fragmentation	Enables fragmentation of large IKE packets into a series of smaller IKE packets to avoid fragmentation at the UDP layer. Note The crypto isakmp fragmentation command is only applicable when the IOS Router is acting as an Easy VPN server and the remote peer is a Cisco IPsec VPN client.

Configuration Examples for Fragmentation of IKE Packets

The following output example shows that fragmentation of IKE packets has been enabled:

```
crypto isakmp fragmentation

crypto isakmp policy 1
 encryption 3des
crypto isakmp profile ezvpn-SW
 match group frag-clients
 vrf frags
```

Additional References

The following sections provide references related to the Fragmentation of IKE Packets feature.

Related Documents

Related Topic	Document Title
Security commands	Cisco IOS Security Command Reference

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

Feature Information for Fragmentation of IKE Packets

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS, software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Fragmentation of IKE Packets

Feature Name	Releases	Feature Information
Fragmentation of IKE Packets	12.4(15)T7	This feature provides for the fragmentation of large IKE packets into a series of small IKE packets to avoid fragmentation at the UDP layer. The following command was introduced or modified: crypto isakmp fragmentation.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.