



Pre-fragmentation For Ipsec VPNs

Feature History

Release	Modification
12.1(11b)E	This feature was introduced.

This document describes the pre-fragmentation for ipsec VPNs feature in Cisco IOS Release 12.1(11b)E. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Configuration Tasks, page 4](#)
- [Configuration Examples, page 7](#)
- [Command Reference, page 7](#)

Feature Overview

When a packet is nearly the size of the maximum transmission unit (MTU) of the outbound link of the encrypting router, and it is encapsulated with IPSec headers, it is likely to exceed the MTU of the outbound link. This causes packet fragmentation after encryption, which makes the decrypting router reassemble in the process path. Pre-fragmentation for IPSec VPNs increases the decrypting router's performance by enabling it to operate in the high performance CEF path instead of the process path.

Pre-fragmentation for IPSec VPNs enables an encrypting router to predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPSec security association (SA). If it is predetermined that the packet will exceed the MTU of the output interface, the packet is fragmented before encryption. This avoids process level reassembly before decryption and helps improve decryption performance and overall IPSec traffic throughput.

Benefits

Increased Performance

Delivers encryption throughput at maximum encryption hardware accelerator speeds. This performance increase is for near MTU sized packets.

Uniform Fragmentation

Packets are fragmented into equally sized units to prevent further downstream fragmentation.

Interoperability

This feature is interoperable with all Cisco IOS platforms and a number of Cisco VPN clients.

Restrictions

Take the following information into consideration before this feature is configured:

- Pre-fragmentation for IPsec VPNs is on by default.
- Pre-fragmentation for IPsec VPNs operates in IPsec Tunnel mode and IPsec tunnel mode with GRE, but not with IPsec transport mode.
- Pre-fragmentation for IPsec VPNs configured on the decrypting router in a unidirectional traffic scenario does not improve the performance or change the behavior of either of the peers.
- Pre-fragmentation for IPsec VPNs occurs before the transform is applied if compression is turned on for outgoing packets.
- Pre-fragmentation for IPsec VPNs functionality depends on the egress interface **crypto ipsec df-bit** configuration and the incoming packet “do not fragment” (DF) bit state. See [Table 1](#).

Table 1 Pre-fragmentation For Ipv6 VPNs Dependencies

Pre-fragmentation For Ipv6 VPNs Feature State (Enabled/Disabled)	Egress Interface “crypto ipsec df-bit” Configuration	Incoming Packet DF Bit State	Result
Enabled	crypto ipsec df-bit clear	0	Fragmentation occurs before encryption.
Enabled	crypto ipsec df-bit clear	1	Fragmentation occurs before encryption.
Disabled	crypto ipsec df-bit clear	0	Fragmentation occurs after encryption and packets are reassembled before decryption.
Disabled	crypto ipsec df-bit clear	1	Fragmentation occurs after encryption and packets are reassembled before decryption.

Table 1 Pre-fragmentation For Ipv6 VPNs Dependencies (continued)

Pre-fragmentation For Ipv6 VPNs Feature State (Enabled/Disabled)	Egress Interface "crypto ipsec df-bit" Configuration	Incoming Packet DF Bit State	Result
Enabled	crypto ipsec df-bit set	0	Fragmentation occurs before encryption
Enabled	crypto ipsec df-bit set	1	Packets are dropped.
Disabled	crypto ipsec df-bit set	0	Fragmentation occurs after encryption and packets are reassembled before decryption.
Disabled	crypto ipsec df-bit set	1	Packets are dropped.
Enabled	crypto ipsec df-bit copy	0	Fragmentation occurs before encryption.
Enabled	crypto ipsec df-bit copy	1	Packets are dropped.
Disabled	crypto ipsec df-bit copy	0	Fragmentation occurs after encryption and packets are reassembled before decryption.
Disabled	crypto ipsec df-bit copy	1	Packets are dropped.

Supported Platforms

This feature runs on all platforms that support Cisco IOS Release 12.1(11b)E.

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature. To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

No new or modified RFCs are supported by this feature.

Configuration Tasks

See the following sections for configuration tasks for the pre-fragmentation for ipsec VPNs feature. Each task in the list is identified as either required or optional.

- [Configuring Pre-fragmentation For Ipv4 VPNs \(optional\)](#)
- [Verifying Pre-fragmentation For Ipv4 VPNs \(optional\)](#)

Configuring Pre-fragmentation For Ipv4 VPNs (optional)

Pre-fragmentation for IPSec VPNs is globally enabled by default. To enable or disable pre-fragmentation for ipsec VPNs while in interface configuration mode, enter the commands in the following table. Use the commands or the **no** form of the commands to revert the configuration.



Note

Manually enabling or disabling pre-fragmentation for ipsec VPNs will override the global configuration.

Command	Purpose
Router(config-if)# crypto ipsec fragmentation before-encryption	Enables pre-fragmentation for ipsec VPNs on the interface.
Router(config-if)# crypto ipsec fragmentation after-encryption	Disables pre-fragmentation for ipsec VPNs on the interface.
Router(config)# crypto ipsec fragmentation before-encryption	Enables pre-fragmentation for ipsec VPNs globally.
Router(config)# crypto ipsec fragmentation after-encryption	Disables pre-fragmentation for ipsec VPNs globally.

Verifying Pre-fragmentation For Ipv6 VPNs (optional)

To verify that pre-fragmentation for ipv6 VPNs is enabled, consult the interface statistics on the encrypting router and the decrypting router. If fragmentation occurs on the encrypting router, and no reassembly occurs on the decrypting router, fragmentation is happening before encryption, and thus the packets are not being reassembled before decryption. This means that the feature is enabled.



Note

This method of verification does not apply to packets destined for the decrypting router.

- Step 1** Enter the **show running-configuration** command on the encrypting router. If the feature is enabled, you will observe output similar to the following:

```
Router# show running-configuration
crypto isakmp policy 10
  authentication pre-share
crypto isakmp key abcd123 address 25.0.0.7
!
!
crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
!
crypto map bar 10 ipsec-isakmp
  set peer 25.0.0.7
  set transform-set fooprime
  match address 102
```

If the feature has been disabled, you will observe output similar to the following:

```
Router# show running-configuration
crypto isakmp policy 10
  authentication pre-share
crypto isakmp key abcd123 address 25.0.0.7
!
!
crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
crypto ipsec fragmentation after-encryption
!
crypto map bar 10 ipsec-isakmp
  set peer 25.0.0.7
  set transform-set fooprime
  match address 102
```

- Step 2** Enter the **show running-configuration interface type number** command to display statistics for the encrypting router egress interface. If the feature is enabled, you will observe output similar to the following:

```
Router# show running-configuration interface fastethernet 0/0
interface FastEthernet0/0
 ip address 25.0.0.6 255.0.0.0
 no ip mroute-cache
 load-interval 30
 duplex full
 speed 100
 crypto map bar
```

If the feature has been disabled, you will observe output similar to the following:

```
Router# show running-configuration interface fastethernet 0/0
interface FastEthernet0/0
 ip address 25.0.0.6 255.0.0.0
 no ip mroute-cache
 load-interval 30
 duplex full
 speed 100
 crypto map bar
 crypto ipsec fragmentation after-encryption
```

Configuration Examples

This section provides the following configuration example:

- [Enabling Pre-fragmentation For Ipv6 VPNs Example](#)

Enabling Pre-fragmentation For Ipv6 VPNs Example

The following is a configuration example of the pre-fragmentation for ipsec VPNs feature.



Note

The pre-fragmentation for ipsec VPNs feature does not show up in the running configuration in this example because the default global pre-fragmentation for ipsec VPNs feature is enabled. Pre-fragmentation for IPsec VPNs shows in the running configuration only when you explicitly enable the feature on the interface.

```
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key abcd123 address 25.0.0.7
!
!
crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
!
crypto map bar 10 ipsec-isakmp
 set peer 25.0.0.7
 set transform-set fooprime
 match address 102
```

Command Reference

This section documents the new **crypto ipsec fragmentation before-encryption** command that configures the pre-fragmentation for ipsec VPNs feature. All other commands used with this feature are documented in the [Cisco IOS Release 12.1 command reference](#) publications.

crypto ipsec fragmentation

To enable pre-fragmentation for ipsec VPNs, use the **crypto ipsec fragmentation before-encryption** command. To disable pre-fragmentation for ipsec VPNs, use the **crypto ipsec fragmentation after-encryption** command. Use the **no** form of these commands to disable a manually configured command. If no other pre-fragmentation for ipsec VPNs commands are in the configuration, the router will revert to the default global pre-fragmentation for ipsec VPNs configuration.

crypto ipsec fragmentation [before-encryption | after-encryption]

no crypto ipsec fragmentation [before-encryption | after-encryption]

Syntax Description

before-encryption	Enables pre-fragmentation for ipsec VPNs.
after-encryption	Disables pre-fragmentation for ipsec VPNs.

Defaults

Pre-fragmentation for IPSec VPNs is enabled by default.

Command Modes

Interface configuration mode or global configuration mode.

Command History

Release	Modification
Cisco IOS Release 12.1(11b)E	This command was introduced.

Usage Guidelines

Use the **crypto ipsec fragmentation** command to enable or disable pre-fragmentation for ipsec VPNs. Pre-fragmentation for IPSec VPNs enables an encrypting router to predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPSec security association (SA). If it is predetermined that the packet will exceed the MTU of output interface, the packet is fragmented before encryption.

Examples

The following example shows how to enable pre-fragmentation for ipsec VPNs on an interface and then how to display the output of the **show running configuration** command:

```
Router(config-if)# crypto ipsec fragmentation before-encryption
Router(config-if)# exit
Router# show running-config
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key abcd123 address 25.0.0.7
!
!
crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
!
crypto map bar 10 ipsec-isakmp
 set peer 25.0.0.7
 set transform-set fooprime
 match address 102
```