Pre-Fragmentation for IPSec VPNs

Feature History

Release	Modification
12.1(11b)E	This feature was introduced.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.

This feature module describes the Pre-fragmentation for IPSec VPNs feature in Cisco IOS Release 12.2(13)T and 12.2(14)S. It includes the following sections:

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.

This feature allows 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 function avoids process level reassembly before decryption and helps improve decryption performance and overall IPSec traffic throughput.

Note The pre-fragmentation feature is turned off by default for tunnel interfaces. To receive pre-fragmentation performance benefits, turn pre-fragmentation on after insuring that the tunnel interfaces have the same MTU on both ends.

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 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 IPSec VPNs Dependencies

Pre-Fragmentation for IPSec 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.
Enabled	**crypto ipsec df-bit set**	0	Fragmentation occurs before encryption.

Table 1 Pre-Fragmentation for IPSec VPNs Dependencies (continued)

Pre-Fragmentation for IPSec VPNs Feature State (Enabled/Disabled)	Egress Interface "crypto ipsec df-bit" Configuration	Incoming Packet DF Bit State	Result
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

12.2(14)S and higher

The Pre-fragmentation for IPSec VPN feature is supported on the following platforms:

- Cisco 7200 series
- Cisco 7400 series

12.2(13)T

The Pre-fragmentation for IPSec VPN feature is supported on all platforms using Cisco IOS Release 12.2(13)T or higher, including:

- Cisco 1710
- Cisco 1720
- Cisco 1721
- Cisco 1751
- Cisco 1760
- Cisco 2600
- Cisco 2691
- Cisco 3620
- Cisco 3640
- Cisco 3660

- Cisco 3725
- Cisco 3745
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7400 series

12.1(11b)E

The Pre-fragmentation for IPSec VPN feature is supported on all platforms using Cisco IOS Release 12.1(11b)E or higher, including:

- Cisco 7100 series

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on 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 found at this URL:

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 standards are supported by this feature.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

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

To access Cisco MIB Locator, 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 found at this URL:

http://www.cisco.com/register

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 IPSec VPNs (required)
- Verifying Pre-Fragmentation For IPSec VPNs (optional)

Configuring Pre-Fragmentation For IPSec VPNs

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 **no** form of the commands to revert back to the default configuration, or use the commands themselves to enable configuration of the pre-fragmentation IPSec VPNs.

Note Manually enabling or disabling this feature 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 IPSec VPNs

To verify that this feature 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 IPSec VPNs Example

Enabling Pre-Fragmentation For IPSec VPNs Example

The following configuration example shows how to configure the Pre-Fragmentation for IPSec VPNs feature:

Note This 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 new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- **crypto ipsec fragmentation**
- **crypto ipsec fragmentation (interface configuration)**

crypto ipsec fragmentation

To enable pre-fragmentation for IP Security (IPSec) Virtual Private Networks (VPNs) on a global basis, use the **crypto ipsec fragmentation** command in global configuration mode. To disable a manually configured command, use the **no** form of this command.

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

If no other pre-fragmentation for IPSec VPNs commands are in the configuration, the router will revert to the default global configuration.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines

Use the **before-encryption** keyword to enable pre-fragmentation for IPSec VPNs; use the **after-encryption** keyword to disable pre-fragmentation for IPSec VPNs. This command allows 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.

Note This command does not appear in the a running configuration if the default global command is enabled. It shows in the running configuration only when you explicitly enable the command on an interface.

Examples

The following example shows how to globally enable pre-fragmentation for IPSec VPNs:

```
crypto ipsec fragmentation before-encryption
```

crypto ipsec fragmentation (interface configuration)

To enable pre-fragmentation for IP Security (IPSec) Virtual Private Networks (VPNs) on an interface, use the **crypto ipsec fragmentation** command in interface configuration mode. To disable a manually configured command, use the **no** form of this command.

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

If no other pre-fragmentation for IPSec VPNs commands are in the configuration, the router will revert to the default global configuration.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines

Use the **before-encryption** keyword to enable pre-fragmentation for IPSec VPNs per interface; use the **after-encryption** keyword to disable pre-fragmentation for IPSec VPNs. This command allows 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:

Note This command appears in the running configuration only when you explicitly enable it on the interface.

```
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
```