IPsec VPN の Pre-fragmentation

機能の履歴

リリース	変更点
12.1(11b)E	この機能が追加されました。
12.2(13)T	この機能は、Cisco IOS Release 12.2(13)T に統合されました。
12.2(14)S	この機能は、Cisco IOS Release 12.2(14)S に統合されました。

このフィーチャ モジュールでは、Cisco IOS Release 12.2(13)T および 12.2(14)S の IPsec VPN の Pre-fragmentation 機能について説明します。次の項で構成されています。

機能の概要

パケットのサイズが暗号化ルータのアウトバウンド リンクの最大伝送ユニット（MTU）のサイズに近く、IPsec ヘッダーを含んでカプセル化されている場合は、アウトバウンド リンクの MTU を超えることがあります。この場合、暗号化の後にパケットのフラグメンテーションが行われます。これにより、復号化ルータがプロセス パスでパケットを再編成します。IPsec VPN の Pre-fragmentation により、プロセス パスではなく高パフォーマンスの CEF パスで復号化ルータが動作可能になるため、復号化ルータのパフォーマンスが向上します。

この機能により復号化ルータは、トランスフォーム セット（IPsec Security Association（SA; セキュリティ アソシエーション）の一部として設定されています）の利用可能な情報を基に、カプセル化されているパケットのサイズを事前に確認できます。パケットのサイズが出力インターフェイスの MTU を超えることが前もって確認されると、パケットは暗号化前にフラグメント化（分割）されます。この機能を使用すると、復号化前にプロセス レベルでパケットを再編成する必要がなくなるため、復号化のパフォーマンスと IPsec トラフィックの全体的なスループットが向上します。

（注） トンネル インターフェイスの Pre-fragmentation 機能はデフォルトでオフになっています。プレフラグメンテーションによってパフォーマンスを向上させるには、トンネル インターフェイスの両端に同じ MTU があることを確認してから、Pre-fragmentation 機能をオンにします。

利点

パフォーマンスの向上

暗号化ハードウェア アクセラレータの最大速度の暗号化スループットを実現します。パフォーマンスが向上するのは、パケットのサイズが MTU のサイズに近い場合です。

均一なフラグメンテーション

同じサイズの単位にパケットが分割され、以降の処理ではフラグメンテーションが不要になります。

相互運用性

この機能は、すべての Cisco IOS プラットフォームおよび多数の Cisco VPN クライアントと連携可能です。

制約事項

この機能の設定前に次の情報を考慮してください。

- IPsec VPN の Pre-fragmentation は IPsec トンネル モードおよび GRE を使用する IPsec トンネル モードで動作し、IPsec トランスポート モードでは動作しません。
- トラフィックが単一方向のネットワーク上で復号ルータに IPsec VPN の Pre-fragmentation を設定しても、パフォーマンスは向上せず、それぞれのピアの動作は変わりません。
- 発信パケットの圧縮がオンになっている場合は、IPsec VPN の Pre-fragmentation は変換前に実行されます。
- IPsec VPN の Pre-fragmentation は出力インターフェイス **crypto ipsec df-bit** の設定によって機能が異なります。着信パケットは（DF）ビットの状態を「分割しません」。表 1 を参照してください。

表 1　IPsec VPN の Pre-fragmentation の依存関係

IPsec VPN の Pre-fragmentation 機能の状態（イネーブル/ディセーブル）	出力インターフェイス「crypto ipsec df-bit」の設定	着信パケット DF ビットの状態	結果
イネーブル	crypto ipsec df-bit クリア	0	暗号化前にフラグメンテーションが実行されます。
イネーブル	crypto ipsec df-bit クリア	1	暗号化前にフラグメンテーションが実行されます。

表 1　IPsec VPN の Pre-fragmentation の依存関係 （続き）

IPsec VPN の Pre-fragmentation 機能の状態（イネーブル/ディセーブル）	出力インターフェイス「crypto ipsec df-bit」の設定	着信パケット DF ビットの状態	結果
ディセーブル	crypto ipsec df-bit クリア	0	暗号化後にフラグメンテーションが実行され、復号前にパケットが再編成されます。
ディセーブル	crypto ipsec df-bit クリア	1	暗号化後にフラグメンテーションが実行され、復号前にパケットが再編成されます。
イネーブル	crypto ipsec df-bit セット	0	暗号化前にフラグメンテーションが実行されます。
イネーブル	crypto ipsec df-bit セット	1	パケットは廃棄されます。
ディセーブル	crypto ipsec df-bit セット	0	暗号化後にフラグメンテーションが実行され、復号前にパケットが再編成されます。
ディセーブル	crypto ipsec df-bit セット	1	パケットは廃棄されます。
イネーブル	crypto ipsec df-bit コピー	0	暗号化前にフラグメンテーションが実行されます。
イネーブル	crypto ipsec df-bit コピー	1	パケットは廃棄されます。
ディセーブル	crypto ipsec df-bit コピー	0	暗号化後にフラグメンテーションが実行され、復号前にパケットが再編成されます。
ディセーブル	crypto ipsec df-bit コピー	1	パケットは廃棄されます。

サポートされているプラットフォーム

12.2(14)S 以降

IPsec VPN の Pre-fragmentation 機能は次のプラットフォームでサポートされています。

- Cisco 7200 シリーズ
- Cisco 7400 シリーズ

12.2(13)T

IPsec VPN の Pre-fragmentation 機能は、Cisco IOS Release 12.2(13)T 以降を使用する、次のすべてのプラットフォームでサポートされています。

- 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 シリーズ
- Cisco 7200 シリーズ
- Cisco 7400 シリーズ

12.1(11b)E

IPsec VPN の Pre-fragmentation 機能は、Cisco IOS Release 12.1(11b)E 以降を使用する、次のすべてのプラットフォームでサポートされています。

- Cisco 7100 シリーズ

Cisco Feature Navigator を使用したプラットフォーム サポートの特定

Cisco IOS ソフトウェアは、特定のプラットフォームがサポートされている機能セットにパッケージングされています。この機能のプラットフォーム サポートに関連した更新情報を取得するには、Cisco Feature Navigator にアクセスします。新しいプラットフォーム サポートが機能に追加されると、Cisco Feature Navigator によって、サポートされているプラットフォームのリストが自動的に更新されます。

Cisco Feature Navigator は Web ベースのツールであり、特定の機能セットがサポートされている Cisco IOS ソフトウェア イメージ、および、特定の Cisco IOS イメージ内でサポートされている機能を特定できます。機能またはリリースごとに検索できます。リリース セクションでは、各リリースを横に並べて比較し、各ソフトウェア リリースに固有の機能と共通機能の両方を表示できます。

Cisco Feature Navigator にアクセスするには、Cisco.com のアカウントが必要です。アカウント情報を忘れたり、紛失したりした場合は、空の E メールを cco-locksmith@cisco.com に送信してください。自動チェックによって、E メール アドレスが Cisco.com に登録されているかどうかが確認されます。チェックが正常に終了したら、ランダムな新しいパスワードとともにアカウントの詳細が E メールで届きます。資格のあるユーザは、Cisco.com のアカウントを作成できます。次の URL にある指示に従ってください。

http://www.cisco.com/register

Cisco Feature Navigator は定期的に更新されています（Cisco IOS ソフトウェアの主要なリリース時およびテクノロジー リリース時）。最新情報については、次の URL から Cisco Feature Navigator ホームページにアクセスしてください。

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

Cisco IOS ソフトウェア イメージの可用性

プラットフォームが特定の Cisco IOS ソフトウェア リリースをサポートするかどうかは、そのプラットフォーム用のソフトウェア イメージの有無により異なります。一部のプラットフォームのソフトウェア イメージは、事前の通知なしに延期、遅延、または変更される場合があります。各 Cisco IOS ソフトウェア リリースのプラットフォーム サポートおよび利用可能なソフトウェア イメージの更新情報は、オンライン リリース ノートまたは Cisco Feature Navigator（サポートされている場合）を参照してください。

サポートされている規格、MIB、および RFC

規格

- この機能によってサポートされる新しい規格や変更された規格はありません。

MIB

- この機能によってサポートされる新しい規格や変更された規格はありません。

選択したプラットフォーム、Cisco IOS ソフトウェア リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。

http://www.cisco.com/go/mibs

RFC

- この機能によってサポートされる新しい RFC や変更された RFC はありません。

設定作業

IPsec VPN の Pre-fragmentation 機能の設定作業については、次の項を参照してください。一覧内の各作業は、必須と任意に分けています。

- 「IPsec VPN の Pre-fragmentation の設定」（必須）
- 「IPsec VPN の Pre-fragmentation の確認」（任意）

IPsec VPN の Pre-fragmentation の設定

デフォルトでは、IPsec VPN の Pre-fragmentation はグローバルでイネーブルになっています。インターフェイス コンフィギュレーション モードで IPsec VPN の Pre-fragmentation をイネーブルまたはディセーブルにするには、次の表のコマンドを入力します。デフォルト設定に戻すには、コマンドを **no** 形式で実行します。IPsec VPN の Pre-fragmentation の設定をイネーブルにするには、表のコマンドを実行します。

（注） この機能を手動でイネーブルまたはディセーブルにすると、グローバル コンフィギュレーションが上書きされます。

コマンド	目的
Router(config-if)# **crypto ipsec fragmentation before-encryption**	インターフェイスで IPsec VPN の Pre-fragmentation をイネーブルにします。
Router(config-if)# **crypto ipsec fragmentation after-encryption**	インターフェイスで IPsec VPN の Pre-fragmentation をディセーブルにします。
Router(config)# **crypto ipsec fragmentation before-encryption**	IPsec VPN の Pre-fragmentation をグローバルにイネーブルにします。
Router(config)# **crypto ipsec fragmentation after-encryption**	IPsec VPN の Pre-fragmentation をグローバルにディセーブルにします。

IPsec VPN の Pre-fragmentation の確認

この機能がイネーブルになっているか確認するには、暗号化ルータおよび復号化ルータのインターフェイス統計情報を参照します。パケットに対して暗号化ルータでフラグメンテーションが実行され、復号化ルータで再編成しない場合、フラグメンテーションは暗号化前に実行され、復号化前には再編成されないということになります。これはこの機能がイネーブルであることを意味しています。

（注） この確認方法は、復号化ルータ宛てのパケットには使用できません。

ステップ 1 暗号化ルータで **show running-configuration** コマンドを入力します。機能がイネーブルの場合は、次のような出力が表示されます。

```
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
```

機能がディセーブルの場合は、次のような出力が表示されます。

```
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
```

ステップ 2 **show running-configuration interface** *type number* コマンドを入力し、暗号化ルータ出力インターフェイスの統計情報を表示します。機能がイネーブルの場合は、次のような出力が表示されます。

```
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
```

機能がディセーブルの場合は、次のような出力が表示されます。

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
```

設定例

ここでは、次の設定例について説明します。

- 「IPsec VPN の Pre-fragmentation のイネーブル例」

IPsec VPN の Pre-fragmentation のイネーブル例

次の設定例は、IPsec VPN の Pre-fragmentation 機能の設定方法を示しています。

（注） この例では、デフォルトのグローバル IPsec VPN の Pre-fragmentation 機能がイネーブルになっているため、実行コンフィギュレーションにはこの機能は表示されません。実行コンフィギュレーションに IPsec VPN の Pre-fragmentation が表示されるのは、インターフェイスで明示的にこの機能をイネーブルにしている場合だけです。

```
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
```

コマンド リファレンス

次のコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。

- **crypto ipsec fragmentation**
- **crypto ipsec fragmentation**（インターフェイス コンフィギュレーション）

これらのコマンドの詳細については、『Cisco IOS Security Command Reference』（http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html）を参照してください。

Cisco IOS の全コマンドを参照する場合は、Command Lookup Tool（http://tools.cisco.com/Support/CLILookup）にアクセスするか、または『*Master Command List*』を参照してください。
