



IPsec VPN の Pre-fragmentation

IPsec VPN の Pre-fragmentation 機能で、最大伝送ユニット (MTU) サイズに近いパケットに対し、暗号化スループットが暗号化ハードウェア アクセラレータの速度で提供されることにより、Cisco IOS XE ルータと VPN クライアントとの間のパフォーマンスが向上します。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。

- [IPsec VPN の Pre-fragmentation の制約事項 \(1 ページ\)](#)
- [IPsec VPN の Pre-fragmentation に関する情報 \(3 ページ\)](#)
- [IPsec VPN の Pre-fragmentation の設定方法 \(4 ページ\)](#)
- [その他の参考資料 \(5 ページ\)](#)
- [IPsec VPN の Pre-fragmentation の機能情報 \(5 ページ\)](#)

IPsec VPN の Pre-fragmentation の制約事項

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** の設定と着信パケットの「do not fragment」 (DF) ビットの状態によって機能が異なります。次の表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。 |
| 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 | パケットがドロップされます。 |
| 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 | パケットがドロップされます。 |
| 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 | パケットがドロップされます。 |
| ディセーブル | crypto ipsec df-bit コピー | 0 | 暗号化の後にフラグメンテーションが発生し、復号化の前にパケットがリアセンブルされます。 |
| ディセーブル | crypto ipsec df-bit コピー | 1 | パケットがドロップされます。 |

IPsec VPN の Pre-fragmentation に関する情報

IPsec VPN の Pre-fragmentation

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MTUのサイズに近く、IPsec ヘッダー付き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。これにより、暗号化後にパケットフラグメンテーションが発生します。よって復号化ルータでは、その復号化ルータのパフォーマンスを低下させているプロセスパスの当該パケットがリアセンブルされる必要があります。

IPsec VPN の Pre-fragmentation 機能により、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、その復号化ルータのパフォーマンスが向上します。復号化ルータでは、トランスフォームセット (IPsec セキュリティアソシエーション (SA) の一部として設定) 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リアセンブルすることがなくなるため、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。Pre-fragmentation 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 があるようにしてから、Pre-fragmentation をオンにします。
-

暗号マップは、暗号化の前後に発生するフラグメンテーションの動作を定義するためには使用されなくなっています。現在、IPsec 仮想トンネルインターフェイス (仮想テンプレートインターフェイスともいう) (VTI) のフラグメンテーションの動作は、VTI で設定されている IP MTU の設定によって決定されます。

VTI の詳細については、IPsec 仮想トンネルインターフェイス機能のドキュメントを参照してください。



-
- (注) フラグメンテーションを暗号化後に動作させる場合、VTI の IP MTU は、出力ルータインターフェイスの IP MTU よりも大きい値に設定します。IP MTU の値を表示するには、**show ip interface tunnel** コマンドを使用します。
-

IPsec VPN の Pre-fragmentation の設定方法

IPsec VPN の Pre-fragmentation の設定

このタスクを実行して、IPsec VPN の Pre-Fragmentation を設定します。

手順の概要

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `ip mtu bytes`

手順の詳細

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 1 | enable 例 : <pre>Router> enable</pre> | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例 : <pre>Router# configure terminal</pre> | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | interface type number 例 : <pre>Router(config-if)# interface tunnel0</pre> | VTI が設定されるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | ip mtu bytes 例 : <pre>Router(config-if)# ip mtu 1500</pre> 例 : | IPsec VPN の出力インターフェイスにおける IP パケットの VTI MTU サイズをバイト単位で設定します。 (注) フラグメンテーションを暗号化後に動作させる場合、VTI の IP MTU は、出力ルータインターフェイスの IP MTU よりも大きい値に設定します。IP MTU の値を表示するには、 show ip interface tunnel コマンドを使用します。 |

その他の参考資料

関連資料

| 関連項目 | マニュアル タイトル |
|------------|--|
| セキュリティコマンド | 『Cisco IOS Security Command Reference』 |
| IPsec | IPsec 仮想トンネルインターフェイス機能のドキュメント |

MIB

| MIB | MIB のリンク |
|-----|--|
| なし | <p>選択したプラットフォーム、Cisco ソフトウェアリリース、およびフィーチャセットの 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。</p> <p>http://www.cisco.com/go/mibs</p> |

シスコのテクニカル サポート

| 説明 | リンク |
|--|--|
| <p>右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。</p> | <p>http://www.cisco.com/cisco/web/support/index.html</p> |

IPsec VPN の Pre-fragmentation の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 2: IPsec VPN の Pre-fragmentation の機能情報

| 機能名 | リリース | 機能情報 |
|-------------------------------|------------------|---|
| IPsec VPN の Pre-fragmentation | Cisco IOS XE 2.1 | <p>この機能で、最大伝送ユニット (MTU) サイズに近いパケットに対し、暗号化スループットが暗号化ハードウェアアクセラレータの速度で提供されることにより、Cisco IOS XE ルータと VPN クライアントとの間のパフォーマンスが向上します。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。</p> <p>次のコマンドが導入または変更されました。ip mtu (interface configuration) .</p> |

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。