CHAPTER 26

IPSec バーチャル プライベート ネットワーク（VPN）のフラグメンテーションと最大伝送ユニット（MTU）の設定

この章では、IPSec Virtual Private Network（VPN; バーチャル プライベート ネットワーク）のフラグメンテーションおよび Maximum Transmission Unit（MTU; 最大伝送ユニット）を設定する方法について説明します。具体的な内容は次のとおりです。

- 「IPSec VPN のフラグメンテーションと MTU の概要」（P.26-1）
- 「IPSec プリフラグメンテーションの設定」（P.26-10）
- 「MTU 値の設定」（P.26-13）

この章で使用するコマンドの詳細については、『*Cisco 7600 Series Cisco IOS Command* Reference, 12.2 SR』を参照してください。また、関連する Cisco IOS Release 12.2 ソフトウェア コマンド リファレンスおよびマスター インデックスも参照してください。これらのマニュアルの入手方法については、「関連資料」（P.li）を参照してください。

IPSec VPN のフラグメンテーションと MTU の概要

この項の内容は、次のとおりです。

- 「フラグメンテーションと MTU の概要」（P.26-1）
- 「IPSec プリフラグメンテーション」（P.26-3）
- 「モード別のフラグメンテーション」（P.26-3）

フラグメンテーションと MTU の概要

パケットのサイズが暗号化ルータの物理出力ポートの最大伝送ユニット（MTU）のサイズとほぼ同じで、そのパケットが IPSec ヘッダーでカプセル化される場合、パケットは出力ポートの MTU を超過する可能性があります。この状態では、パケットは暗号化後にフラグメント化されます（ポストフラグメンテーション）。これにより、IPSec ピアでは復号化の前に再アセンブリが必要になり、パフォーマンスが低下します。ポストフラグメンテーションを最小限にするには、フラグメンテーションが暗号化の前に発生するように（プリフラグメンテーション）、アップストリーム データ パスに MTU を設定します。IPSec VPN のプリフラグメンテーションは、再アセンブリ作業を受信側 IPSec ピアから受信側エンド ホストに移すことで、パフォーマンスが低下しないようにします。

（注）　このマニュアルでは、プリフラグメンテーションとは IPSec、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）など、あらゆるタイプのカプセル化の前に発生するフラグメンテーションをいいます。IPSec プリフラグメンテーションとは、IPSec 暗号化前のフラグメンテーションをいいます。

ほとんどの場合でプリフラグメンテーションが行われるように、次の MTU 設定を推奨します。

- IPSec VPN SPA に対応付けられている暗号インターフェイス Virtual LAN（VLAN; 仮想 LAN）MTU は、出力インターフェイス MTU 以下に設定する必要があります。
- GRE over IPSec の場合、GRE トンネル インターフェイスの IP MTU は、出力インターフェイス MTU より少なくとも IPSec 暗号化のオーバーヘッドおよび 24 バイトの GRE+IP ヘッダー（20 バイトの IP ヘッダー + 4 バイトの GRE ヘッダー）だけ下回るように設定する必要があります。トンネル キー（RFC 2890）などのオプションはサポートされていないため、GRE+IP ヘッダーは常に 24 バイトになります。

（注）　暗号インターフェイス VLAN MTU、出力インターフェイス MTU、および GRE トンネル インターフェイスの IP MTU はすべてレイヤ 3 パラメータです。

次に、暗号接続モードの IPSec プリフラグメンテーションおよび MTU に関するその他の注意事項を示します。

- パケットの Don't Fragment（DF）ビットが設定されており、パケットがデータ パス内のどこかで MTU を超過すると、このパケットはドロップされます。パケットがドロップされないように、Policy-Based Routing（PBR; ポリシーベース ルーティング）または **crypto df-bit clear** コマンドを使用して DF ビットをクリアします。
- Cisco IOS Release 12(33)SRA、SRB、および SRC 以前のリリースでは、IPSec VPN SPA は **tunnel path-mtu-discovery** コマンドを使用する、GRE トンネルの Path MTU Discovery（PMTUD）をサポートしません。Cisco IOS Release SXI 以降のリリースでは、PMTUD は GRE トンネルでサポートされます。
- GRE カプセル化が IPSec VPN SPA にテイクオーバーされていない場合、およびパケットが GRE トンネル インターフェイスの IP MTU を超過する場合、Route Processor（RP; ルート プロセッサ）はパケットをフラグメント化し、カプセル化します。

（注）　スーパーバイザ エンジンが GRE カプセル化を実行すると、カプセル化されたパケットには DF ビットが設定されます。

IPSec および GRE プリフラグメンテーション機能は Cisco IOS リリースによって異なります（表 26-1 を参照）。

表 26-1　Cisco IOS リリース別 IPSec および GRE プリフラグメンテーション

Cisco IOS リリース	プリフラグメンテーション機能
12.2(18)SXE	IP MTU と出力インターフェイス MTU の小さい方に基づいて、IPSec および GRE の両方に対してプリフラグメンテーション プロセスが行われます。フラグメンテーションまたはパケット損失を防ぐために、VLAN MTU を予測最大 GRE パケット サイズ（IP の長さ + GRE オーバーヘッド）で設定し、出力インターフェイス MTU を予測最大 GRE/IPSec パケット サイズ（IP の長さ + GRE オーバーヘッド + IPSec オーバーヘッド）で設定します。

表 26-1　Cisco IOS リリース別 IPSec および GRE プリフラグメンテーション （続き）

12.2(18)SXF	GRE フラグメンテーションと IPSec フラグメンテーションは異なるプロセスです。IPSec VPN SPA によって GRE カプセル化が実行される場合、アウトバウンド パケットのプリフラグメンテーションはトンネル インターフェイスの IP MTU に基づいて行われます。IPSec VPN SPA によって GRE カプセル化が実行された後、IPSec プリフラグメンテーション設定によってはさらにフラグメンテーションが行われることがあります。IPSec フラグメンテーション動作は Cisco IOS Release 12.2(18)SXE から変更されておらず、出力インターフェイスの IPSec MTU 設定に基づいて行われます。
12.2SRA	暗号接続モードで Path MTU Discovery（PMTUD）がサポートされます。

フラグメンテーションおよび MTU の問題に関する一般情報については、次の URL の『Resolve IP Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPSec』を参照してください。

http://www.cisco.com/en/US/tech/tk827/tk369/technologies_white_paper09186a00800d6979.shtml

IPSec プリフラグメンテーション

IPSec プリフラグメンテーション プロセス（別名 Look-Ahead Fragmentation（LAF））では、暗号化ルータは、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るトランスフォーム セットで使用可能な情報から、カプセル化パケットのサイズをあらかじめ規定できます。IPSec プリフラグメンテーションは、復号化前の受信側ルータによる再アセンブリを回避し、再アセンブリ作業をエンド ホストに移すことで IPSec トラフィックの全体的なスループットを向上させます。

暗号化されたパケットが出力インターフェイスの MTU を超過するように規定されている場合、パケットはフラグメント化されてから暗号化されます。

モード別のフラグメンテーション

フラグメンテーション プロセスは、IPSec VPN モードおよび GRE または Virtual Tunnel Interface（VTI）が使用されているかどうかによって異なります。次のセクションを参照してください。

- 「暗号接続モードでのフラグメンテーション」（P.26-3）
- 「VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）モードでの（暗号マップを使用する）IPSec パケットのフラグメンテーション」（P.26-5）
- 「VRF モードでのトンネル保護を使用した GRE パケットのフラグメンテーション」（P.26-7）
- 「VTI のフラグメンテーション」（P.26-8）

次のフラグメンテーションに関する説明では、フローチャートのパケットに DF（Don't Fragment）ビットが設定されていないことを前提としています。パケットにフラグメンテーションが必要で、DF ビットが設定されている場合は、パケットはドロップされます。

暗号接続モードでのフラグメンテーション

次に、暗号接続モードでパケットのフラグメンテーションを行うための MTU 設定を示します。

- インターフェイス VLAN の MTU

  RP による非 GRE トラフィックのプリフラグメンテーションは、この MTU に基づいて行われます。

- GRE トンネルの IP MTU

  GRE トラフィックのプリフラグメンテーションはこの MTU に基づいて行われます。

- 物理出力インターフェイスの MTU

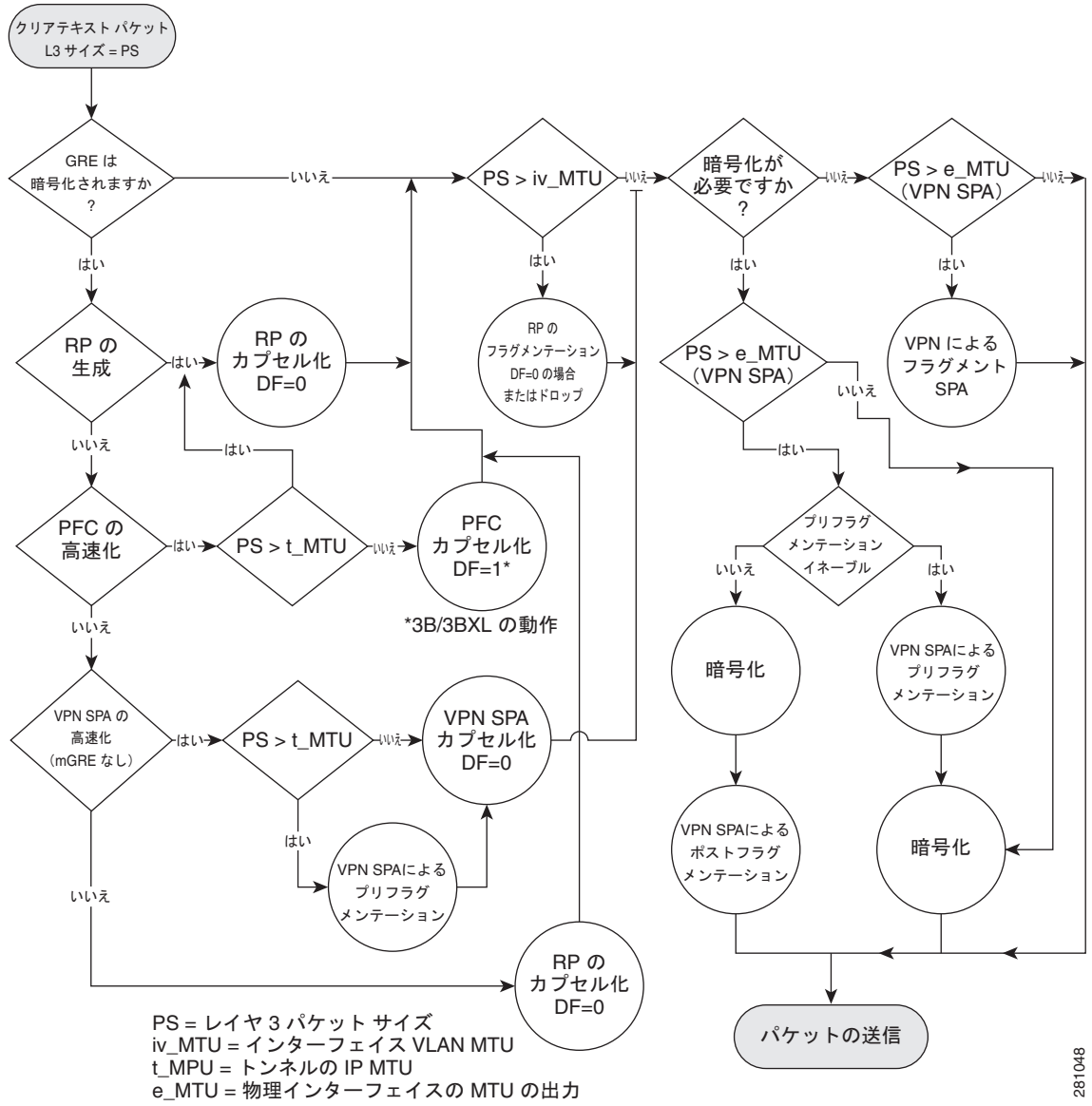
  IPSec VPN SPA によるプリフラグメンテーションおよびポストフラグメンテーションはこの MTU に基づいて行われます。

フラグメンテーションは次のように行われます。

- IPSec VPN SPA に送信されるパケットがインターフェイス VLAN の MTU を超過する場合、RP はプリフラグメンテーションを行ってからパケットを IPSec VPN SPA に送信します。
- GRE カプセル化されるパケットが GRE トンネルの IP MTU を超過する場合
  - トンネルが IPSec VPN SPA にテイクオーバーされていない場合は、RP がプリフラグメンテーションを実行します。
  - トンネルが IPSec VPN SPA にテイクオーバーされている場合は、IPSec VPN SPA がプリフラグメンテーションを実行します。
- 暗号化されるパケットが物理出力インターフェイスの MTU を超過する場合
  - IPSec プリフラグメンテーションがイネーブルの場合は、IPSec VPN SPA がパケットのプリフラグメンテーションを実行します。IPSec VPN SPA はポストフラグメンテーションを行いません。
  - IPSec プリフラグメンテーションがディセーブルの場合は、IPSec VPN SPA が暗号化されたパケットのポストフラグメンテーションを実行します。IPSec VPN SPA はプリフラグメンテーションを行いません。
- 暗号化されない出力パケットが物理出力インターフェイスの MTU を超過する場合は、IPSec VPN SPA がパケットのフラグメンテーションを実行します。

図 26-1 に、暗号接続モードでのパケットのフラグメンテーション プロセスを示します。

図 26-1　暗号接続モードでのパケットのフラグメンテーション



VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）モードでの（暗号マップを使用する）IPSec パケットのフラグメンテーション

次に、VRF モードで IPSec トラフィックのフラグメンテーションを行うための MTU 設定を示します。

- インターフェイス VLAN の MTU

  RP によるプリフラグメンテーションはこの MTU に基づいて行われます。

- 物理出力インターフェイスの MTU

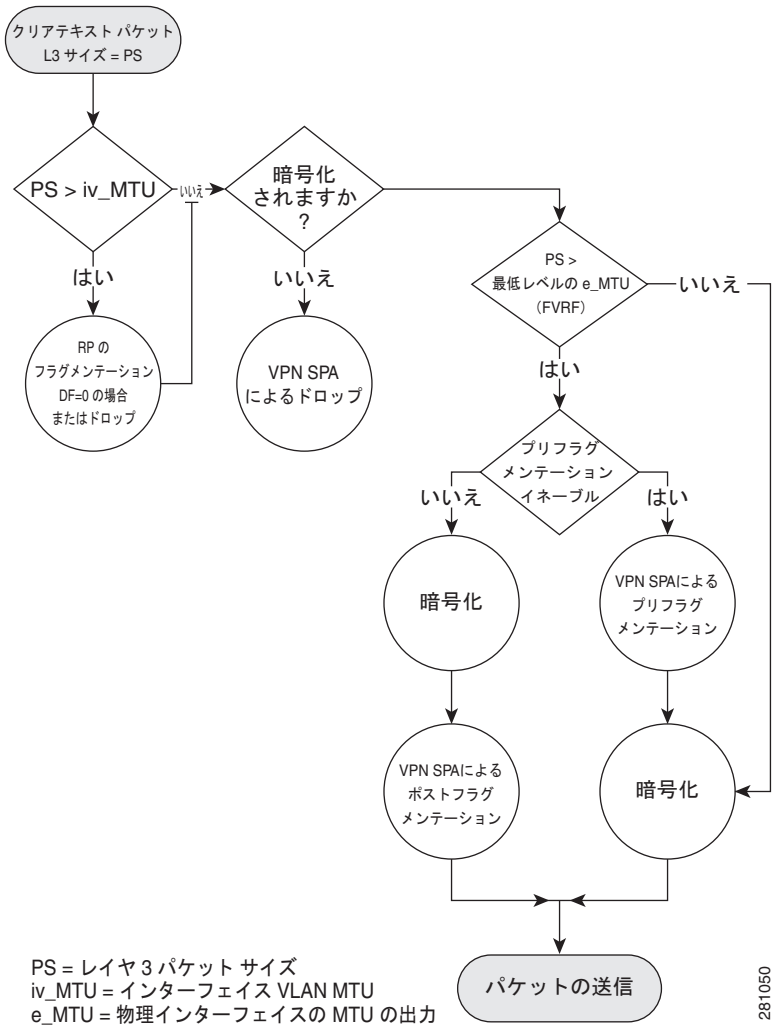
  IPSec VPN SPA によるプリフラグメンテーションおよびポストフラグメンテーションはこの MTU に基づいて行われます。

フラグメンテーションは次のように行われます。

- パケットがインターフェイス VLAN の MTU を超過する場合、RP がプリフラグメンテーションを実行します。
- 暗号化された出力パケットが Front Door VRF（FVRF; 前面扉 VRF）の物理出力インターフェイスの最低 MTU を超過する場合
  - IPSec プリフラグメンテーションがイネーブルの場合は、IPSec VPN SPA がパケットのプリフラグメンテーションを実行します。IPSec VPN SPA はポストフラグメンテーションを行いません。
  - IPSec プリフラグメンテーションがディセーブルの場合は、IPSec VPN SPA が暗号化されたパケットのポストフラグメンテーションを実行します。IPSec VPN SPA はプリフラグメンテーションを行いません。

図 26-2 に、VRF モードでの IPSec パケットのフラグメンテーション プロセスを示します。

図 26-2　VRF モードでの IPSec パケットのフラグメンテーション



VRF モードでのトンネル保護を使用した GRE パケットのフラグメンテーション

次に、VRF モードでトンネル保護を使用した GRE トラフィックのフラグメンテーションを行うための適切な MTU 設定を示します。

- GRE トンネルの IP MTU

  プリフラグメンテーションはこの MTU に基づいて行われます。

- FVRF の物理出力インターフェイスの最低 MTU

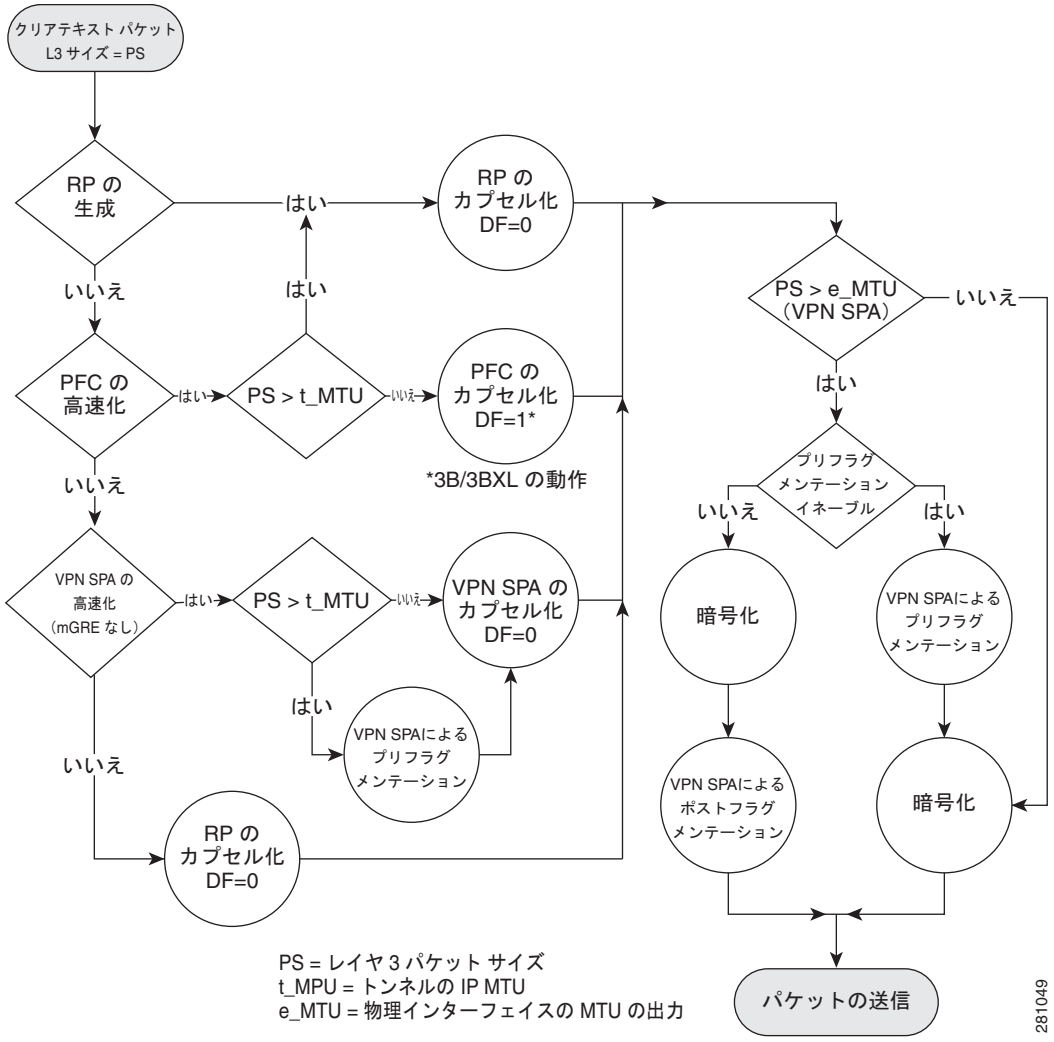
  IPSec VPN SPA によるプリフラグメンテーションおよびポストフラグメンテーションはこの MTU に基づいて行われます。

フラグメンテーションは次のように行われます。

- カプセル化されるパケットが GRE トンネルの IP MTU を超過する場合
  - トンネルが IPSec VPN SPA にテイクオーバーされていない場合は、RP がプリフラグメンテーションを実行します。
  - トンネルが IPSec VPN SPA にテイクオーバーされている場合は、IPSec VPN SPA がプリフラグメンテーションを実行します。
- 暗号化された GRE カプセル化パケットが FVRF の物理出力インターフェイスの最低 MTU を超過する場合
  - IPSec プリフラグメンテーションがイネーブルの場合は、IPSec VPN SPA が GRE カプセル化パケットのプリフラグメンテーションを実行します。IPSec VPN SPA はポストフラグメンテーションを行いません。
  - IPSec プリフラグメンテーションがディセーブルの場合は、IPSec VPN SPA が暗号化された GRE カプセル化パケットのポストフラグメンテーションを実行します。IPSec VPN SPA はプリフラグメンテーションを行いません。

図 26-3 に、VRF モードでのトンネル保護を使用した GRE パケットのフラグメンテーション プロセスを示します。

図 26-3　VRF モードでのトンネル保護を使用した GRE パケットのフラグメンテーション



VTI のフラグメンテーション

次に、VTI パケットのフラグメンテーションを行うための MTU 設定を示します。

- VTI トンネル インターフェイスの IP MTU

  プリフラグメンテーションはこの MTU に基づいて行われます。

（注）　VTI トンネル インターフェイスの IP MTU はデフォルト値のままにしておくことを推奨します。変更した場合は、物理出力インターフェイスの MTU から IPSec オーバーヘッドを差し引いた値を超えていないことを確認してください。

- 物理出力インターフェイスの MTU

IPSec VPN SPA によるポストフラグメンテーションはこの MTU に基づいて行われます。

フラグメンテーションは次のように行われます。

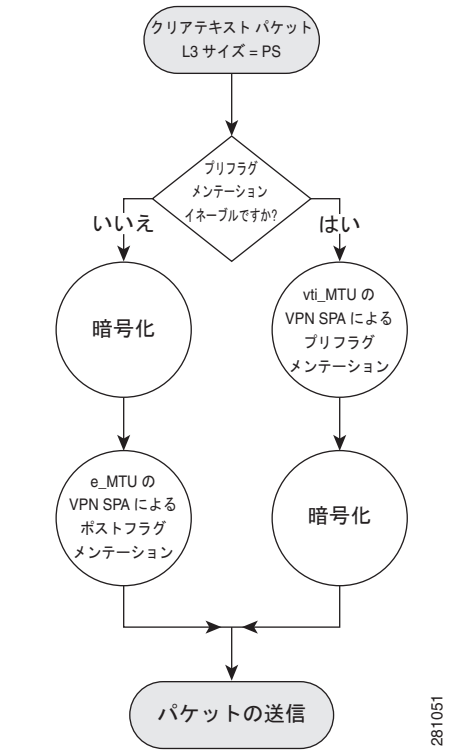
- IPSec プリフラグメンテーションがイネーブルの場合は、IPSec VPN SPA が VTI トンネル インターフェイスの IP MTU を超過するパケットのプリフラグメンテーションを実行します。IPSec VPN SPA はポストフラグメンテーションを行いません。

（注）　RP は、出力インターフェイスの MTU を超過するパケットのポストフラグメンテーションを実行します。これは設定ミスと見なされます。

- IPSec プリフラグメンテーションがディセーブルの場合は、IPSec VPN SPA が出力インターフェイスの MTU を超過するパケットのポストフラグメンテーションを実行します。IPSec VPN SPA はプリフラグメンテーションを行いません。

図 26-4 に、VTI パケットのフラグメンテーション プロセスを示します。

図 26-4　VTI パケットのフラグメンテーション



vti_MTU = VTI トンネル インターフェイスの IP MTU
e_MTU = 物理インターフェイスの MTU の出力

IPSec プリフラグメンテーションの設定

IPSec プリフラグメンテーションは、グローバルまたはインターフェイス レベルで設定できます。デフォルトでは、IPSec プリフラグメンテーションはグローバルにイネーブルです。インターフェイス レベルで IPSec プリフラグメンテーションをイネーブルまたはディセーブルにすると、グローバル設定が上書きされます。

IPSec プリフラグメンテーション設定時の注意事項

IPSec プリフラグメンテーションを設定する場合は、次の注意事項に従ってください。

- インターフェイス レベルで IPSec プリフラグメンテーションを設定するには、暗号マップの適用先となるインターフェイスに設定します。
- 大容量パケット フローによって IPSec ピアの CPU 利用率が高くなっている場合は、IPSec プリフラグメンテーションがイネーブルに設定されているかどうかを確認してください（ピアは大容量パケットを再アセンブルしている可能性があります）。
- IPSec VPN の IPSec プリフラグメンテーションは、IPSec トンネル モードで動作します。IPSec トランスポート モードでは適用されません。
- IPSec VPN の PSec プリフラグメンテーション機能は、インターフェイスの **crypto ipsec df-bit** 設定および着信パケットの「do not fragment」（DF）ビットの状態に依存します。プリフラグメンテーションに関する一般情報については、次の URL を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftprefrg.html

- GRE フラグメンテーション動作は、ソフトウェア リリースによって次のように異なります。
  - Cisco IOS Release 12.2(18)SXE では、IPSec VPN SPA の GRE フラグメンテーション動作は GRE インターフェイスの IP MTU と出力インターフェイスのレイヤ 2 MTU の小さい方によって決定されます。フラグメンテーションまたはパケット損失を防ぐために、VLAN MTU を予測最大 GRE パケット サイズ（IP の長さ + GRE オーバーヘッド）で設定し、出力インターフェイス MTU を予測最大 GRE/IPSec パケット サイズ（IP の長さ + GRE オーバーヘッド + IPSec オーバーヘッド）で設定する必要があります。
  - Cisco IOS Releases 12.2(18)SXF および 12(33)SRA 以降のリリースでは、GRE フラグメンテーションと IPSec フラグメンテーションは異なるプロセスです。IPSec VPN SPA によって GRE カプセル化が実行される場合、アウトバウンド パケットのプリフラグメンテーションはトンネル インターフェイスの IP MTU に基づいて行われます。IPSec VPN SPA によって GRE カプセル化が実行された後、IPSec LAF（Look Ahead Fragmentation）設定によってはさらにフラグメンテーションが行われることがあります。IPSec フラグメンテーション動作は Cisco IOS Release 12.2(18)SXE から変更されておらず、出力インターフェイスの IPSec MTU 設定に基づいて行われます。
- GRE+IP カプセル化によってパケット サイズが 24 バイト増加します。予想される GRE オーバーヘッドに基づいてプリフラグメンテーションを設定する場合は、この値を使用します。
- IPSec 暗号化により、設定されている IPSec トランスフォーム セットに応じてパケット サイズにさまざまなバイト数が加算されます。予想される IPSec オーバーヘッドに基づいてプリフラグメンテーションを設定する場合は、さまざまな IPSec トランスフォーム セットに対する最悪の場合の IPSec オーバーヘッドを示す次の表を参照してください。

IPSec トランスフォーム セット	IPSec オーバーヘッド（最大バイト数）
esp-aes-（256 または 192 または 128）esp-sha-hmac または md5	73
esp-aes （256 または 192 または 128）	61
esp-3des、esp-des	45
esp-（des または 3des）esp-sha-hmac または md5	57
esp-null esp-sha-hmac または md5	45
ah-sha-hmac または md5	44

IPSec プリフラグメンテーションのグローバル設定

IPSec プリフラグメンテーションは、デフォルトではグローバル レベルでイネーブルに設定されています。グローバル レベルで IPSec VPN のプリフラグメンテーションをイネーブルまたはディセーブルにするには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto ipsec fragmentation before-encryption`	IPSec VPN のプリフラグメンテーションをグローバルでイネーブルにします。
ステップ 2	`Router(config)# crypto ipsec fragmentation after-encryption`	IPSec VPN のプリフラグメンテーションをグローバルでディセーブルにします。

インターフェイスでの IPSec プリフラグメンテーションの設定

IPSec プリフラグメンテーションは、デフォルトではグローバル レベルでイネーブルに設定されています。インターフェイス レベルで IPSec VPN のプリフラグメンテーションをイネーブルまたはディセーブルにするには、暗号マップの適用先であるインターフェイスのインターフェイス コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config-if)# crypto ipsec fragmentation before-encryption`	インターフェイスで IPSec VPN のプリフラグメンテーションをイネーブルにします。
ステップ 2	`Router(config-if)# crypto ipsec fragmentation after-encryption`	インターフェイスで IPSec VPN のプリフラグメンテーションをディセーブルにします。

（注）　インターフェイス レベルで IPSec プリフラグメンテーションをイネーブルまたはディセーブルにすると、グローバル設定が上書きされます。

IPSec プリフラグメンテーション設定の確認

IPSec プリフラグメンテーションがイネーブルに設定されているかどうかを確認するには、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調べます。暗号化ルータでフラグメンテーションが発生していて、かつ復号化ルータで再アセンブリが発生していない場合、暗号化の前にフラグメンテーションが実行されており、パケットは再アセンブリされずに復号化されていることになります。つまり、この機能はイネーブルです。

IPSec プリフラグメンテーション機能がイネーブルに設定されていることを確認するには、暗号化ルータで show running-configuration コマンドを入力します。この機能がイネーブルの場合は、次のようにコマンド出力にフラグメンテーション機能は表示されません。

```
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
!!! the postfragmentation feature appears here if IPSec prefragmentation is disabled
crypto map bar 10 ipsec-isakmp
 set peer 25.0.0.7
 set transform-set fooprime
 match address 102
```

IPSec プリフラグメンテーションがディセーブルに設定されている場合は、次のようにコマンド出力にポストフラグメンテーション機能が表示されます。

```
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
```

暗号化ルータ インターフェイス VLAN の設定を表示するには、**show running-configuration interface** コマンドを入力します。IPSec プリフラグメンテーション機能がイネーブルの場合は、次のようにコマンド出力にプリフラグメンテーション文が表示されます。

```
Router# show running-configuration interface vlan2

interface Vlan2
 ip address 15.0.0.2 255.255.255.0
 crypto map testtag
 crypto engine slot 1/0
 crypto ipsec fragmentation before-encryption
```

インターフェイス VLAN で IPSec プリフラグメンテーション機能がディセーブルの場合は、次のようにコマンド出力にポストフラグメンテーション文が表示されます。

```
Router# show running-configuration interface vlan2

interface Vlan2
 ip address 15.0.0.2 255.255.255.0
 crypto map testtag
 crypto engine slot 1/0
 crypto ipsec fragmentation after-encryption end
```

MTU 値の設定

Cisco IOS ソフトウェアでは、インターフェイスおよび VLAN のレイヤ 3 最大伝送ユニット（MTU）を設定できます。パケットの不要なフラグメンテーションを回避するために、すべての MTU 値に一貫性を持たせる必要があります。

（注）　MTU を設定する場合、**ip mtu** コマンドが適用されるのは IP プロトコル トラフィックだけです。その他のレイヤ 3 プロトコル トラフィックは、**mtu** コマンドによって設定された MTU を確認します。

MTU 値の設定時の注意事項および制約事項

IPSec VPN SPA の MTU 値を設定する場合は、次の注意事項および制約事項に従ってください。

- IPSec VPN SPA がフラグメンテーションの決定に使用する MTU 値は、次のセキュア ポートの MTU 値に基づいています。
  - ルーテッド ポート：自身に対応付けられているセキュア ポートの MTU 値を使用します。
  - アクセス ポート：自身のインターフェイス VLAN に対応付けられているセキュア ポートの MTU 値を使用します。
  - トランク ポート：自身のインターフェイス VLAN に対応付けられているセキュア ポートの MTU 値を使用します。
- GRE トンネリングが設定されている場合は、「IPSec プリフラグメンテーション」（P.26-3）で推奨される MTU 値に関する情報を参照してください。

（注）　パケット フラグメンテーションの詳細については、「IPSec プリフラグメンテーションの設定」（P.26-10）を参照してください。

物理出力インターフェイス MTU の変更

物理出力インターフェイスのレイヤ 3 MTU または IP MTU を設定できます。物理出力インターフェイスの MTU 値を変更するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-if)# mtu` *bytes*	インターフェイスの最大伝送ユニット（MTU）サイズを設定します。 • *bytes*：範囲は 1500 ～ 9216 です。デフォルトは 1500 です。

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

トンネル インターフェイス MTU の変更

トンネル インターフェイスの IP MTU は設定できますが、レイヤ 3 MTU は設定できません。トンネルの IP MTU 値を変更するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# interface tunnel_name`	トンネルのインターフェイス コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-if)# ip mtu bytes`	トンネルの IP MTU サイズを設定します。 • *bytes*：最小値は 68 です。最大値およびデフォルト値はインターフェイス メディアによって異なります。

インターフェイス VLAN MTU の変更

インターフェイス VLAN のレイヤ 3 MTU を設定できます。インターフェイス VLAN の MTU 値を変更するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# interface vlan_ID`	VLAN のインターフェイス コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-if)# mtu bytes`	インターフェイス VLAN の MTU サイズを設定します。 • *bytes*：範囲は 64 ～ 9216 です。デフォルトは 1500 です。

MTU サイズの確認

インターフェイスの MTU サイズを確認するには、次の例のように **show interface** コマンドまたは **show ip interface** コマンドを入力します。

セキュア ポートの MTU 値を表示するには、**show interface** コマンドを入力します。

```
Router# show interface g1/1

GigabitEthernet1/1 is up, line protocol is up (connected)
Hardware is C6k 1000Mb 802.3, address is 000a.8ad8.1c4a (bia 000a.8ad8.1c4a)
MTU 9216 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
...
```

インターフェイス VLAN の MTU サイズを表示するには、**show interface** コマンドを入力します。

```
Router# show interface vlan2
Vlan2 is up, line protocol is up
  Hardware is EtherSVI, address is 000e.39ad.e700 (bia 000e.39ad.e700)
  Internet address is 192.168.1.1/16
  MTU 1000 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
...
```

GRE トンネルの IP MTU 値を表示するには、**show ip interface** コマンドを入力します。

```
Router# show ip interface tunnel 2

Tunnel2 is up, line protocol is up
Internet address is 11.1.0.2/16
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1450 bytes
...
```