



IPsec トンネルを使用する DF ビット オーバーライド機能

IPsec トンネル機能による DF ビット オーバーライド機能では、トンネルモード IPsec トラフィックを、グローバルレベルまたは各インターフェイスレベルでカプセル化する際に、DF ビットを設定できます。したがって、ルータが DF ビットを消去するように設定されている場合、ルータは、元の DF のパケット設定に関係なく、パケットを断片化できます。

- [IPsec トンネルを使用する DF ビット オーバーライド機能の前提条件 \(1 ページ\)](#)
- [IPsec トンネルを使用する DF ビット オーバーライド機能の制約事項 \(1 ページ\)](#)
- [IPsec トンネルを使用する DF ビット オーバーライド機能に関する情報 \(2 ページ\)](#)
- [IPsec トンネルを使用する DF ビット オーバーライド機能の設定方法 \(3 ページ\)](#)
- [IPsec トンネルを使用する DF ビット オーバーライド機能の設定例 \(4 ページ\)](#)
- [その他の参考資料 \(5 ページ\)](#)
- [IPsec トンネルを使用する DF ビット オーバーライド機能の機能情報 \(6 ページ\)](#)

IPsec トンネルを使用する DF ビット オーバーライド機能の前提条件

ルータで IPsec がイネーブルに設定されている必要があります。

IPsec トンネルを使用する DF ビット オーバーライド機能の制約事項

パフォーマンス上の影響

各パケットがプロセスレベルで再アセンブルされるため、高いデータレートでパフォーマンスに大きな影響が生じます。主な警告事項には、次の2つがあります。

- 再アSEMBル キューが満杯になると、フラグメントが強制的に廃棄されることがあります。
- プロセス スイッチングにより、トラフィックの速度は低下します。

DF ビットの設定要件

複数のインターフェイスがローカルアドレス機能を使用して同じクリプト マップを共有する場合、これらのインターフェイスは同じ DF ビット設定を共有する必要があります。

機能の Availability

この機能は IPsec トンネル モードだけで使用できます (IPsec トランスポート モードは、カプセル化 IP ヘッダーを提供しないので、影響を受けません)。

IPsec トンネルを使用する DF ビット オーバーライド機能に関する情報

機能の概要

IPsec トンネル機能による DF ビット オーバーライド機能により、ルータがカプセル化ヘッダーの Don't Fragment (DF) ビットをクリア、設定、またはコピーするかどうかを指定できます。DF ビットは IP ヘッダー内のビットで、このビットは、ルータがパケットを断片化することを許可されているかどうか判別します。

一部のユーザ設定のホストでは、次の機能を実行します。

- 送信されたパケットに DF ビットを設定する。
- ファイアウォールを使用して、ファイアウォールの外部からくるインターネット制御メッセージプロトコル (ICMP) エラーをブロックし、ホストがファイアウォールの外部から最大伝送単位 (MTU) サイズを認識できないようにする。
- IP セキュリティ (IPsec) を使用してパケットをカプセル化し、MTU サイズを縮小する。

使用可能な MTU サイズを認識できないようにホストが設定されている場合、DF ビットをクリアし、パケットを断片化するよう、ルータを設定できます。



(注) この機能は、RFC 2401 に準拠して、グローバルに、またはインターフェイスごとに設定できます。両方のレベルを設定すると、インターフェイスコンフィギュレーションにより、グローバルコンフィギュレーションが上書きされます。

IPsec トンネルを使用する DF ビット オーバーライド機能の設定方法

トンネル モードでのカプセル化ヘッダーへの DF ビットの設定

トンネルモードでDF ビットをカプセル化ヘッダーに設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec df-bit [clear | set | copy]**

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： Router> enable	特権 EXEC モードを有効にします。 • 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： Router# configure terminal	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	crypto ipsec df-bit [clear set copy] 例： Router (config)# crypto ipsec df-bit set	すべてのインターフェイスのトンネルモードで DF ビットをカプセル化ヘッダーに設定します。 指定されたインターフェイスに DF ビットを設定するには、インターフェイスコンフィギュレーションモードで crypto ipsec df-bit コマンドを使用します。 (注) DF ビットインターフェイスコンフィギュレーション設定によって、すべての DF ビットグローバルコンフィギュレーション設定が上書きされます。

DF ビット設定の確認

ルータ上の現在の DF ビット設定を確認するには、**show running-config** コマンドを EXEC モードで使用します。

IPsec トンネルを使用する DF ビット オーバーライド機能 の設定例

DF ビットの設定例

次の例では、DF ビットの設定をグローバルに消去し、DF ビットを FastEthernet というインターフェイスにコピーするようにルータが設定されています。したがって、FastEthernet 以外のすべてのインターフェイスでは、ルータは使用可能な MTU サイズより大きいパケットを送信でき、FastEthernet では、ルータはパケットをフラグメント化できます。

```
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp key Delaware address 192.168.10.66
crypto isakmp key Key-What-Key address 192.168.11.19
!
!
crypto ipsec transform-set exampleset ah-md5-hmac esp-des
crypto ipsec df-bit clear
!
!
crypto map armadillo 1 ipsec-isakmp
set peer 192.168.10.66
set transform-set exampleset
match address 101
!
crypto map basilisk 1 ipsec-isakmp
set peer 192.168.11.19
set transform-set exampleset
match address 102
!
!
interface FastEthernet
  ip address 192.168.10.38 255.255.255.0
  ip broadcast-address 0.0.0.0
  media-type 10BaseT
  crypto map armadillo
  crypto ipsec df-bit copy
!
interface FastEthernet1
  ip address 192.168.11.75 255.255.255.0
  ip broadcast-address 0.0.0.0
  media-type 10BaseT
  crypto map basilisk
!
interface Serial0
  no ip address
  ip broadcast-address 0.0.0.0
  no ip route-cache
  no ip mroute-cache
```

その他の参考資料

次のセクションには、IPsec トンネル機能による DF ビット オーバーライド機能の関連資料が記載されています。

関連資料

関連項目	マニュアル タイトル
インターネット キー エクスチェンジ ネットワークと IPsec ネットワーク	「Configuring Internet Key Exchange for IPsec VPNs」
IPSec ネットワークのコマンド	『Cisco IOS Security Command Reference』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存規格のサポートはありません。	選択したプラットフォーム、Cisco IOS XE 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には、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能がサポートする新しい RFC または変更された RFC はありません。また、この機能は既存の規格に対するサポートに影響を及ぼしません。	--

シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	http://www.cisco.com/en/US/support/index.html

IPsec トンネルを使用する DF ビット オーバーライド機能の機能情報

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 1: IPsec トンネルを使用する DF ビット オーバーライド機能の機能情報

機能名	リリース	機能情報
IPsec トンネルを使用する DF ビット オーバーライド機能	Cisco IOS XE Release 2.1	<p>この機能により、ルータがカプセル化ヘッダーから Don't Fragment (DF) ビットを消去、設定、またはコピーするかどうかを指定できます。DF ビットは IP ヘッダー内のビットで、このビットは、ルータがパケットを断片化することを許可されているかどうか判別します。</p> <p>次のコマンドが導入または変更されました。 crypto ipsec df-bit。</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。