



IPsec を使用した VPN のセキュリティ コンフィギュレーション ガイド（Cisco IOS XE Gibraltar 16.10.x 向け）

最終更新：2026 年 10 月 6 日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

最初にお読みください 1

Short Description 2

第 2 章

IPsec を使用した VPN のセキュリティの設定 3

機能情報の確認 3

IPsec を使用した VPN のセキュリティの設定に関する前提条件 4

IPsec を使用した VPN のセキュリティの設定に関する制約事項 4

IPsec を使用した VPN のセキュリティの設定に関する情報 5

サポートされる標準 5

サポートされるカプセル化 8

IPsec 機能の概要 8

IKEv1 トランスフォーム セット 9

IKEv2 トランスフォーム セット 9

トランスフォーム セット：セキュリティ プロトコルとアルゴリズムの組み合わせ 10

トランスフォーム セットの概要 10

IKE および IPsec 暗号化アルゴリズムのための Cisco IOS Suite-B のサポート 12

Suite-B の要件 12

Suite-B の設定情報の入手先 13

IPsec VPN の設定方法 13

クリプト アクセス リストの作成 13

次の作業 14

IKEv1 および IKEv2 プロポーザルのトランスフォーム セットの設定 15

機能制限 15

IKEv1 のトランスフォーム セットの設定 15

IKEv2 のトランスフォーム セットの設定	17
クリプト マップ セット の作成	20
スタティック クリプト マップ の作成	20
ダイナミック クリプト マップ の作成	23
手動による SA を確立するためのクリプト マップ エントリの作成	28
インターフェイスへのクリプト マップ セット の適用	31
IPsec VPN の設定例	32
例 : AES ベースのスタティック暗号マップの設定	32
IPsec を使用した VPN のセキュリティの設定に関する追加のリファレンス	33
IPsec を使用した VPN のセキュリティの設定に関する機能情報	36
用語集	37

第 3 章

IPsec 仮想トンネル インターフェイス	39
機能情報の確認	39
IPsec 仮想トンネル インターフェイスの制約事項	40
IPsec 仮想トンネル インターフェイスに関する情報	41
IPsec 仮想トンネル インターフェイスを使用するメリット	41
スタティック仮想トンネル インターフェイス	41
SVTI のマルチ SA サポート	42
ダイナミック仮想トンネル インターフェイス	43
IPsec 仮想トンネル インターフェイスを使用したトラフィックの暗号化	44
ダイナミック仮想トンネル インターフェイスのライフ サイクル	46
IPsec 仮想トンネル インターフェイスを使用したルーティング	46
FlexVPN 混合モードのサポート	46
IPsec での自動トンネル モードのサポート	46
VTI に対する IPsec 混合モードのサポート	47
IPsec 仮想トンネル インターフェイスの設定方法	47
スタティック IPsec 仮想トンネル インターフェイスの設定	47
IPsec 仮想トンネル インターフェイスを介した BGP の設定	49
ダイナミック IPsec 仮想トンネル インターフェイスの設定	51

IKEv1 を使用したダイナミック仮想トンネルインターフェイスのマルチ SA サポートの設定	53
SVTI に対する IPsec 混合モードのサポートの設定	56
ダイナミック VTI に対する IPsec 混合モードのサポートの設定	58
スタティック IPsec 仮想トンネルインターフェイスのマルチ SA サポートの設定	60
デュアルオーバーレイとしてのトンネルモードの設定	63
IPsec 仮想トンネルインターフェイスの設定例	65
例：IPsec を使用したスタティック仮想トンネルインターフェイス	65
例：IPsec スタティック仮想トンネルインターフェイスの結果の確認	66
例：VRF 認識スタティック仮想トンネルインターフェイス	67
例：QoS を使用したスタティック仮想トンネルインターフェイス	68
例：仮想ファイアウォールを使用したスタティック仮想トンネルインターフェイス	68
例：ダイナミック仮想トンネルインターフェイス Easy VPN サーバ	70
例：ダイナミック仮想トンネルインターフェイス Easy VPN サーバの結果の確認	71
例：VRF が仮想テンプレートに基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPsec	71
例：VRF が仮想テンプレートと IPsec プロファイル内のゲートウェイ オプションに基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPsec	72
例：VRF が ISAKMP プロファイルに基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPsec	73
例：VRF が ISAKMP プロファイルと IPsec プロファイル内のゲートウェイ オプションに基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPsec	74
例：VRF が仮想テンプレートと ISAKMP プロファイルの両方に基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPsec	75
例：仮想ファイアウォールを使用したダイナミック仮想トンネルインターフェイス	76
例：QoS を使用したダイナミック仮想トンネルインターフェイス	77
例：複数の IPsec SA を使用したスタティック仮想トンネルインターフェイス	78
例：デュアルオーバーレイとしてのトンネルモードの設定	80
IPsec 仮想トンネルインターフェイスに関する追加のリファレンス	83
IPsec 仮想トンネルインターフェイスに関する機能情報	84

機能情報の確認	89
失効したピア証明書の暗号セッションの削除に関する制約事項	90
失効したピア証明書の暗号セッションの削除に関する情報	90
暗号セッションの削除方法	90
失効したピア証明書の暗号セッションの削除のイネーブル化方法	91
暗号セッションの削除の有効化	91
失効したピア証明書の暗号セッションの削除機能の確認	92
失効したピア証明書の暗号セッションを削除する設定例	93
例：IKE セッションの暗号セッションの削除のイネーブル化	93
例：IKEv2 セッションの暗号セッションの削除のイネーブル化	93
失効したピアの暗号セッションの削除に関する追加のリファレンス	94
失効したピア証明書の暗号セッションの削除に関する機能情報	95

第 5 章

暗号条件付きデバッグ サポート 97

機能情報の確認	97
暗号条件付きデバッグ サポートの前提条件	98
暗号条件付きデバッグ サポートの制約事項	98
暗号条件付きデバッグ サポートに関する情報	98
サポートされる条件タイプ	98
暗号条件付きデバッグ サポートのイネーブル化方法	100
暗号条件付きデバッグ メッセージのイネーブル化	100
パフォーマンス上の考慮事項	100
暗号条件付きデバッグのディセーブル化	100
暗号エラー デバッグ メッセージのイネーブル化	102
デバッグ暗号エラー CLI	102
暗号条件付きデバッグ CLI の設定例	103
暗号条件付きデバッグのイネーブル化の例	103
暗号条件付きデバッグのディセーブル化の例	103
その他の参考資料	104
暗号条件付きデバッグ サポートに関する機能情報	105

第 6 章

IPv4 GRE トンネル保護経由の IPv6 107

機能情報の確認 107

IPv4 GRE トンネル保護経由の IPv6 の前提条件 107

IPv4 GRE トンネル保護経由の IPv6 の制約事項 108

IPv4 GRE トンネル保護経由の IPv6 に関する情報 108

IPsec を使用した GRE トンネル 108

IPv4 GRE トンネル保護経由の IPv6 の設定方法 110

クリプト マップを使用した IPv4 GRE 暗号化経由の IPv6 の設定 110

トンネル保護を使用した IPv4 GRE 暗号化経由の IPv6 の設定 114

IPv4 GRE トンネル保護経由の IPv6 の設定例 117

クリプト マップを使用した IPv4 GRE 暗号化経由の IPv6 の設定例 117

トンネル保護を使用した IPv4 GRE 暗号化経由の IPv6 の設定例 118

その他の参考資料 118

IPv4 GRE トンネル保護経由の IPv6 に関する機能情報 119

第 7 章

RFC 430x IPsec サポート 121

機能情報の確認 121

RFC 430x IPsec サポートに関する情報 121

RFC 430x IPsec サポート フェーズ 1 121

RFC 430x IPsec サポート フェーズ 2 122

RFC 430x IPsec サポートの設定方法 123

RFC 430x IPsec サポートのグローバル設定 123

クリプト マップ単位の RFC 430x IPsec サポートの設定 124

RFC 430x IPsec サポートの設定例 126

例：RFC 430x IPsec サポートのグローバル設定 126

例：クリプト マップ単位の RFC 430x IPsec サポートの設定 126

RFC 430x IPsec サポートに関する追加のリファレンス 127

RFC 430x IPsec サポートに関する機能情報 128



第 1 章

最初にお読みください

重要事項



- (注) Cisco IOS XE Bengaluru 17.6.1a 以降のリリースでの CUBE 機能のサポート情報については、[Cisco Unified Border Element IOS-XE コンフィギュレーション ガイド](#)を参照してください。



- (注) この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザーインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

機能情報

機能のサポート、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.com のアカウントは必要ありません。

参考資料

- [Cisco IOS コマンド リファレンス、全リリース](#)

マニュアルの入手方法およびテクニカル サポート

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によって求めるビジネス成果を得るには、[Cisco Services](#) [英語] にアクセスしてください。

- サービスリクエストを送信するには、[Cisco Support](#) [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco Marketplace](#) [英語] にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。
- [Short Description](#) (2 ページ)

Short Description

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



第 2 章

IPsec を使用した VPN のセキュリティの設定

この部分では、基本的な IP VPN を設定する方法について説明します。IPsec は、IETF によって開発されたオープン規格のフレームワークです。インターネットなどの保護されていないネットワークを介して機密情報を伝達する場合にセキュリティを提供します。IPsec はネットワーク層で機能し、Cisco ルータなどの参加している IPsec 装置（「ピア」）間の IP パケットを保護および認証します。



(注) セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『[Next Generation Encryption](#)』（NGE）ホワイトペーパーを参照してください。

- [機能情報の確認](#) (3 ページ)
- [IPsec を使用した VPN のセキュリティの設定に関する前提条件](#) (4 ページ)
- [IPsec を使用した VPN のセキュリティの設定に関する制約事項](#) (4 ページ)
- [IPsec を使用した VPN のセキュリティの設定に関する情報](#) (5 ページ)
- [IPsec VPN の設定方法](#) (13 ページ)
- [IPsec VPN の設定例](#) (32 ページ)
- [IPsec を使用した VPN のセキュリティの設定に関する追加のリファレンス](#) (33 ページ)
- [IPsec を使用した VPN のセキュリティの設定に関する機能情報](#) (36 ページ)
- [用語集](#) (37 ページ)

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「[Bug Search Tool](#)」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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、<https://cfnng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

IPsec を使用した VPN のセキュリティの設定に関する前提条件

IKE の設定

インターネット キー エクスチェンジ (IKE) は、「*Configuring Internet Key Exchange for IPsec VPNs*」の手順に従って設定する必要があります。



(注) IKE を使用しない場合でも、「*Configuring Internet Key Exchange for IPsec VPNs*」の手順に従って、IKE をディセーブルにする必要があります。

アクセス リストが IPsec と互換性があるか確認する

IKE は UDP ポート 500 を使用します。IPsec Encapsulating Security Payload (ESP) プロトコルと認証ヘッダー (AH) プロトコルは、それぞれ、プロトコル番号 50 と 51 を使用します。プロトコル 50、51、および UDP ポート 500 からのトラフィックが IPsec によって使用されるインターフェイスでブロックされないように、アクセス リストが設定されていることを確認します。場合によっては、これらのトラフィックを明示的に許可する文をアクセス リストに追加する必要があります。

IPsec を使用した VPN のセキュリティの設定に関する制約事項

Cisco IPsec ポリシー マップ MIB

MIB OID オブジェクトは、IPsec セッションが起動中にしか表示されません。

不連続アクセス制御リスト

不連続マスクを持つアクセス制御リスト (ACL) を使用する暗号マップはサポートされません。

物理インターフェイスと暗号マップ

物理インターフェイスまたは送信元 IP がトンネル保護インターフェイスの送信元インターフェイスである場合、物理インターフェイスの暗号マップはサポートされません。

NAT の設定

ネットワークアドレス変換（NAT）を使用する場合は、IPsec が適切に動作するように、ステティック NAT を設定する必要があります。一般に、ルータが IPsec カプセル化を実行する前に、NAT が発生する必要があります。つまり、IPsec はグローバルアドレスと連動している必要があります。

ユニキャスト IP データグラム アプリケーションのみ

IPsec は、ユニキャスト IP データグラムにのみ適用できます。IPsec のワーキング グループがまだグループキー配布の問題に対処していないため、IPsec は現在マルチキャストまたはブロードキャスト IP データグラムを処理しません。

サポートされないインターフェイス タイプ

- 暗号 VPN は、ブリッジ ドメイン インターフェイス（BDI）上でサポートされません。
- 暗号マップは、トンネルインターフェイスとポートチャネルインターフェイス上でサポートされません。例外として、GDOI の暗号マップは、トンネルインターフェイス上でサポートされます。
- 暗号マップは、ループバック インターフェイス上ではサポートされません。
- トンネルでトランスポートプロファイルが有効になっている場合、トンネル送信元インターフェイス上では暗号マップはサポートされません。
- 暗号マップは、MFR のトンネルインターフェイス上ではサポートされません。
- 暗号マップは、VLAN インターフェイス上ではサポートされません。
- GetVPN 暗号マップは、ポートチャネルインターフェイス上でサポートされます。

IPsec を使用した VPN のセキュリティの設定に関する情報

サポートされる標準

シスコでは、この機能を使用して次の規格を実装しています。

- IPsec : IPsec は、参加しているピア間のデータ機密性、データ整合性、およびデータ認証を提供するオープンスタンダードのフレームワークです。IPsec は、これらのセキュリティ サービスを IP レイヤで提供します。IPsec は、IKE を使用して、ローカル ポリシーに基づいてプロトコルおよびアルゴリズムのネゴシエーションを処理し、IPsec で使用される暗号キーと認証キーを生成します。IPsec は、1 組のホスト間、1 組のセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間で 1 つ以上のデータ フローを保護するために使用できます。



(注) IPsec という用語は、IPsec データ サービスの protocols 全体および IKE セキュリティ protocols を表す場合に使用されることがあります。また、データ サービスだけを表す場合にも使用されることがあります。

- IKE (IKEv1 と IKEv2) : Oakley キー交換や SKEME キー交換を Internet Security Association and Key Management Protocol (ISAKMP) フレームワーク内部に実装したハイブリッド protocols です。IKE は他の protocols で使用されますが、その初期実装は IPsec protocols で使用されます。IKE は、IPsec ピアを認証し、IPsec セキュリティ アソシエーションをネゴシエーションし、IPsec キーを確立します。



(注) Cisco IOS XE Bengaluru 17.6.x 以降、脆弱な暗号化アルゴリズムを設定すると警告が生成されますが、警告は無視しても問題はなく、アルゴリズムの動作には影響しません。次の例では、脆弱な暗号アルゴリズムに関する警告メッセージを表示します。

```
Device(config-ikev2-proposal)# group 5
%Warning: weaker dh-group is deprecated
```

次の表に、すべての脆弱なアルゴリズムを示します。

IKEv1	IKEv2	IPsec
DH_GROUP_768_MODP/Group 1	DH_GROUP_768_MODP/Group 1	ah-md5-hmac
DH_GROUP_1024_MODP/Group 2	DH_GROUP_1024_MODP/Group 2	ah-sha-hmac
DH_GROUP_1536_MODP/Group 5	DH_GROUP_1536_MODP/Group 5	esp-des
DES	DES	esp-3des
3DES	3DES	esp-sha-hmac
MD5	MD5	esp-gmac
		esp-md5-hmac
		esp-null

IPsec のために実装されているコンポーネントテクノロジーには、次のものがあります。

- AES : Advanced Encryption Standard (AES)。暗号化アルゴリズムの 1 つで、重要ではあるが機密扱いではない情報を保護します。AES は、IPsec および IKE 用のプライバシー変換であり、DES に代わる規格として開発されました。AES は DES よりも安全度の高い設計となっています。AES ではキーのサイズが従来より大きく、侵入者がメッセージを解読するには、あらゆるキーを試してみるしか方法がありません。AES のキーは可変長であり、

アルゴリズムは128ビットキー（デフォルト）、192ビットキー、または256ビットキーを指定できます。

- **DES**：データ暗号規格（DES）。パケットデータの暗号化に使用されるアルゴリズムです。シスコ ソフトウェアは、必須の 56 ビット DES-CBC with Explicit IV を実装しています。Cipher Block Chaining（CBC）では、暗号化の開始に初期ベクター（IV）が必要です。IV は IPsec パケットに明示的に指定されます。下位互換性を確保するために、Cisco IOS IPsec は ESP DES-CBC の RFC 1829 バージョンも実装します。

また、Cisco IOS は、特定のプラットフォームで使用可能なソフトウェアバージョンに応じて、Triple DES（168 ビット）暗号化も実装します。Triple DES（3DES）は推奨されていません。



(注) 強力な暗号化を使用する Cisco IOS イメージ（56 ビットデータ暗号化フィーチャセットを含むがこれに限定されない）は、米国輸出規制の対象となり、配布が制限されます。米国以外の国でインストールされるイメージには、輸出許可が必要です。米国政府の規制により、お客様の注文が拒否されたり、納入が遅れたりすることがあります。詳細については、営業担当者または販売業者、あるいは export@cisco.com までお問い合わせください。

- **SHA-2 および SHA-1 ファミリ（HMAC バリエーション）**：セキュア ハッシュ アルゴリズム（SHA）の 1 および 2。SHA-1 および SHA-2 は、パケットデータの認証および IKE プロトコルの整合性確認メカニズムの検証に使用されるハッシュ アルゴリズムです。HMAC は、追加レベルのハッシュを提供するバリエーションです。SHA-2 ファミリには、SHA-256 ビットのハッシュ アルゴリズムと SHA-384 ビットのハッシュ アルゴリズムが加わっています。この機能は Suite-B の要件に含まれています。Suite-B は、IKE および IPsec で使用するための暗号化アルゴリズムの 4 つのユーザ インターフェイススイートで構成され、RFC 4869 に記述されています。各スイートは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー合意アルゴリズム、ハッシュまたはメッセージダイジェストアルゴリズムで構成されています。Cisco IOS での Suite-B サポートについての詳細は、「Configuring Security for VPNs with IPsec」機能モジュールを参照してください。
- **Diffie-Hellman**：公開キー暗号法プロトコルの 1 つで、2 者間に、安全でない通信チャネルでの共有秘密を確立できます。Diffie-Hellman は、IKE 内でセッション キーを確立するために使用されます。これは、768 ビット（デフォルト）、1024 ビット、1536 ビット、2048 ビット、3072 ビット、および 4096 ビット DH グループをサポートします。また、256 ビットサブグループを含む 2048 ビット DH グループと、256 ビットと 384 ビットの Elliptic Curve DH（ECDH）もサポートします。Cisco では、2048 ビット以上の DH キー交換または ECDH キー交換を使用することを推奨します。
- **MD5（ハッシュ ベースのメッセージ認証コード（HMAC）バリエーション）**：メッセージダイジェストアルゴリズム 5（MD5）はハッシュ アルゴリズムです。HMAC はデータの認証に使用されるキー付きハッシュ バリエーションです。



- (注) シスコは現在、DES、3DES、MD5（HMAC バリエーション含む）、および Diffie-Hellman（DH）グループ 1、2、および 5 の使用は推奨していません。代わりに、AES、SHA、および DH グループ 14 以降を使用する必要があります。最新のシスコの暗号化に関する推奨事項については、『[Next Generation Encryption](#)』（NGE）ホワイトペーパーを参照してください。



- (注) Cisco IOS XE Bengaluru 17.6.x 以降、ISAKMP ポリシーが有効になっている場合、設定に使用できるデフォルトのアルゴリズムは次のとおりです。

- 暗号化 : AES
- ハッシュ : SHA
- DH グループ : 14

シスコ ソフトウェアに実装された IPsec は、さらに次の規格をサポートします。

- AH : 認証ヘッダー。データ認証と、オプションとしてアンチリプレイ サービスを提供するセキュリティ プロトコルです。AH は、保護対象のデータ（完全 IP データグラム）に埋め込まれます。
- ESP : Encapsulating Security Payload。データ プライバシー サービスと、オプションとしてデータ認証およびアンチリプレイ サービスを提供するセキュリティ プロトコルです。ESP は保護対象のデータをカプセル化します。

サポートされるカプセル化

IPsec は、フレーム リレー、ハイレベル データ リンク制御（HDLC）、および PPP のシリアル カプセル化と連動します。

また、IPsec は、Generic Routing Encapsulation（GRE）、IPinIP レイヤ 3、データリンクスイッチング+（DLSw+）、および Source Route Bridging（SRB）トンネリングプロトコルとも連動します。ただし、マルチポイントトンネルはサポートされません。他のレイヤ 3 のトンネリングプロトコルと IPsec の併用はサポートされない場合があります。

IPsec 機能の概要

IPsec は、次のネットワークセキュリティ サービスを提供します。（一般に、ローカルセキュリティ ポリシーにより、これらのサービスを 1 つ以上使用するよう指示されます）。

- データ機密性 : ネットワークにパケットを伝送する前に IPsec 送信側がパケットを暗号化できます。

- データ整合性：IPsec 受信者は、IPsec 送信者から送信されたパケットを認証し、伝送中にデータが変更されていないかを確認できます。
- データ送信元認証：IPsec 受信者は、送信された IPsec パケットの送信元を認証できます。このサービスは、データ整合性サービスに依存します。
- アンチ リプレイ：IPsec 受信者は、再送されたパケットを検出し、拒否できます。

IPsec は、2 つのピア（2 台のルータなど）間にセキュア トンネルを確立します。機密性が高く、セキュア トンネルを介して送信する必要があるパケットを定義し、セキュア トンネルの特性を指定することによって、機密性の高いパケットを保護するために使用するパラメータを定義します。IPsec ピアが機密パケットを認識すると、ピアは適切なセキュア トンネルを設定し、このトンネルを介してリモートピアにパケットを送信します（この章で使用するトンネルという用語は、IPsec をトンネル モードで使用するものではありません）。

正確には、このトンネルは、2 つの IPsec ピア間に確立されるセキュリティ アソシエーション（SA）のセットです。SA は、機密パケットに適用するプロトコルおよびアルゴリズムを定義し、2 つのピアが使用するキー関連情報を指定します。SA は単方向で、セキュリティ プロトコル（AH または ESP）ごとに確立されます。

2 つのピア間に複数の IPsec トンネルを設定し、トンネルごとに個別の SA のセットを使用することにより、さまざまなデータ ストリームを保護できます。たとえば、一部のデータ ストリームは認証だけが必要で、他のデータ ストリームは暗号化と認証の両方が必要な場合があります。

IKEv1 トランスフォーム セット

インターネット キー エクスチェンジ バージョン 1（IKEv1） トランスフォーム セットは、セキュリティ プロトコルとアルゴリズムの特定の組み合わせを表します。IPsec SA のネゴシエーション中に、ピアは、特定のトランスフォーム セットを使用して特定のデータ フローを保護することに合意します。

IKEv2 トランスフォーム セット

インターネット キー エクスチェンジ バージョン 2（IKEv2） プロポーザルは、IKE_SA_INIT 交換の一部としての IKEv2 SA のネゴシエーションで使用されるトランスフォームのセットです。IKEv2 プロポーザルは、少なくとも 1 つの暗号化アルゴリズム、整合性アルゴリズム、および Diffie-Hellman（DH） グループが設定されている場合にのみ、完全であると見なされます。プロポーザルが設定されておらず、IKEv2 ポリシーに接続されていない場合、ネゴシエーションではデフォルトのプロポーザルが使用されます。デフォルトのプロポーザルは、次のような通常使用されるアルゴリズムのコレクションです。

```
encryption aes-cbc-128 3des
integrity sha1 md5
group 5 2
```

crypto ikev2 proposal コマンドは **crypto isakmp policy priority** コマンドに似ていますが、IKEv2 プロポーザルには次のような違いがあります。

- IKEv2 プロポーザルを使用すると、各トランスフォーム タイプに対して1つ以上のトランスフォームを設定できます。
- IKEv2 プロポーザルには関連付けられた優先順位はありません。



- (注) ネゴシエーションで IKEv2 プロポーザルを使用するには、それらを IKEv2 ポリシーにアタッチする必要があります。プロポーザルが設定されていない場合、デフォルトの IKEv2 プロポーザルとデフォルトの IKEv2 ポリシーが使用されます。

トランスフォーム セット：セキュリティ プロトコルとアルゴリズムの組み合わせ

トランスフォーム セットの概要



- (注) h-md5-hmac、esp-md5-hmac、esp-des、または esp-3des の使用は推奨されていません。代わりに、ah-sha-hmac、esp-sha-hmac、または esp-aes を使用する必要があります。最新のシスコの暗号化に関する推奨事項については、『[Next Generation Encryption](#)』（NGE）ホワイト ペーパーを参照してください。

トランスフォーム セットは、特定のセキュリティ プロトコルとアルゴリズムを組み合わせたものです。IPsec SA のネゴシエーション中に、ピアは、特定のトランスフォーム セットを使用して特定のデータ フローを保護することに合意します。

IKE との IPsec セキュリティ アソシエーション ネゴシエーションで、ピアは両方のピア用の同じトランスフォーム セットを探します。同一のトランスフォーム セットが検出された場合、そのトランスフォーム セットが選択され、両方のピアの IPsec SA の一部として、保護するトラフィックに適用されます。（手動で確立した SA は、ピアとネゴシエーションしないため、両方に同じトランスフォーム セットを指定する必要があります）。

次の表に、許可されるトランスフォームの組み合わせを示します。

表 1: 許可されるトランスフォームの組み合わせ

トランス フォーム タイ プ	トランスフォー ム	説明
AH Transform (1 つ選択)	ah-md5-hmac	MD5 (メッセージ ダイジェスト 5) (HMAC バリエント) 認証アルゴリズムを使用する AH。 (非推奨)。
	ah-sha-hmac	SHA (セキュア ハッシュ アルゴリズム) (HMAC バリエント) 認証アルゴリズムを使用する AH。
ESP Encryption Transform (1 つ選択)	esp-aes	128 ビット Advanced Encryption Standard (AES) 暗号化アルゴリズムを使用する ESP。
	esp-aes 192	192 ビット AES 暗号化アルゴリズムを使用する ESP。
	esp-aes 256	256 ビット AES 暗号化アルゴリズムを使用する ESP。
		esp-des 56 ビットのデータ暗号規格 (DES) 暗号化アルゴリズムを使用する ESP。 (非推奨)。
esp-3des		168 ビット DES 暗号化アルゴリズム (3DES、トリプル DES と呼ばれる) を使用する ESP。 (非推奨)。
ESP Authentication Transform (1 つ選択)		esp-md5-hmac MD5 (HMAC バリエント) 認証アルゴリズムを使用する ESP。 (非推奨)。
	esp-sha-hmac	SHA (HMAC バリエント) 認証アルゴリズムを使用する ESP。



(注) セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『[Next Generation Encryption](#)』(NGE) ホワイト ペーパーを参照してください。

IKE および IPsec 暗号化アルゴリズムのための Cisco IOS Suite-B のサポート

Suite-B には次の暗号化アルゴリズムがあります。

- Suite-B-GCM-128 : ESP 整合性保護、機密性、および RFC 4106 で規定されている 128 ビット AES using Galois and Counter Mode (AES-GCM) を使用する IPsec 暗号化アルゴリズムを提供します。ESP の整合性の保護と暗号化の両方が必要な場合にはこのスイートを使用する必要があります。
- Suite-B-GCM-256 : RFC 4106 で規定されている 256 ビット AES-GCM を使用して、ESP 整合性保護と機密性を提供します。ESP の整合性の保護と暗号化の両方が必要な場合にはこのスイートを使用する必要があります。
- Suite-B-GMAC-128 : RFC 4543 で規定されている 128 ビット AES-Galois Message Authentication Code (GMAC) を使用して、ESP 整合性保護を提供しますが、機密性は提供しません。このスイートは、ESP の暗号化が不要である場合のみに使用する必要があります。
- Suite-B-GMAC-256 : RFC 4543 で規定されている 256 ビット AES-GMAC を使用して、ESP 整合性保護を提供しますが、機密性は提供しません。このスイートは、ESP の暗号化が不要である場合のみに使用する必要があります。

IPsec 暗号化アルゴリズムは、暗号化が必要な場合に AES-GCM を使用し、暗号化が不要な場合のメッセージの整合性には AES-GMAC を使用します。

IKE ネゴシエーションでは、AES 暗号ブロック連鎖 (CBC) モードを使用して暗号化を行い、RFC 4634 に定義されている SHA-256 および SHA-384 ハッシュアルゴリズムを含む Secure Hash Algorithm (SHA) -2 ファミリーを使用してハッシュ機能を実行します。キー交換には RFC 4753 に定義されている Elliptic Curves (ECP) を使用した Diffie-Hellman が使用され、認証を行うには RFC 4754 に定義されている楕円曲線デジタル署名アルゴリズム (ECDSA) が使用されます。

Suite-B の要件

IKE および IPsec を使用する場合、Suite-B によって次のソフトウェア暗号エンジンに要件が課せられます。

- HMAC-SHA256 と HMAC-SHA384 は疑似ランダム関数として使用されます。また、IKE プロトコル内の整合性チェックが使用されます。必要に応じて、HMAC-SHA512 を使用することもできます。
- 楕円曲線グループ 19 (256 ビットの ECP 曲線) および 20 (384 ビットの ECP 曲線) は、IKE で Diffie-Hellman グループとして使用されます。必要に応じて、グループ 21 (521 ビットの ECP 曲線) を使用できます。
- X.509 証明書内の署名操作で、楕円曲線デジタル署名アルゴリズム (ECDSA) (256 ビットおよび 384 ビットの曲線) が使用されます。

- ESP（128 ビットおよび 256 ビットのキー）には、GCM（16 バイトの ICV）および GMAC が使用されます。必要に応じて、192 ビットのキーを使用することもできます。
- ECDSA 署名を使用した X.509 証明書の確認に対する Public Key Infrastructure（PKI）サポートを使用する必要があります。
- ECDSA 署名を使用して証明書要求を生成する場合、および発行された証明書を IOS にインポートする場合に、PKI を使用する必要があります。
- 認証方式として ECDSA signature（ECDSA-sig）を使用できるようにする場合に、IKEv2 を使用する必要があります。

Suite-B の設定情報の入手先

Suite-B の設定のサポートについては、次のマニュアルで説明されています。

- SHA-2 ファミリ（HMAC バリエーション）および Elliptic Curve（EC）キー ペアの設定の詳細については、「*Configuring Internet Key Exchange for IPsec VPNs*」機能モジュールを参照してください。
- 整合性アルゴリズム タイプのトランスフォームの設定の詳細については、「*Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site*」機能モジュールの「*Configuring the IKEv2 Proposal*」を参照してください。
- ECDSA-sig を IKEv2 の認証方式として設定する場合の詳細については、「*Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site*」機能モジュールの「*Configuring IKEv2 Profile (Basic)*」を参照してください。
- IPsec SA ネゴシエーション用の Elliptic Curve Diffie-Hellman（ECDH）サポートの設定の詳細については、「*Configuring Internet Key Exchange for IPsec VPNs*」および「*Configuring Internet Key Exchange Version 2 and FlexVPN*」機能モジュールを参照してください。

PKI の証明書登録での Suite-B のサポートの詳細については、「*Configuring Certificate Enrollment for a PKI*」機能モジュールを参照してください。

IPsec VPN の設定方法

クリプト アクセス リストの作成

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかを実行します。
 - **access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**]

- **ip access-list extended name**

4. 作成するクリプト アクセス リストごとにステップ 3 を繰り返します。

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル構成モードを開始します。
ステップ 3	次のいずれかを実行します。 • access-list access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard [log] • ip access-list extended name 例 : Device(config)# access-list 100 permit ip 10.0.68.0 0.0.0.255 10.1.1.0 0.0.0.255 例 : Device(config)# ip access-list extended vpn-tunnel	保護する IP パケットを判別する条件を指定します。 • 番号または名前によって指定された IP アクセスリストを使用して、条件を指定します。 access-list コマンドでは、番号付き拡張アクセスリストを指定し、ip access-list extended コマンドでは、名前付きアクセスリストを指定します。 • これらの条件に一致するトラフィックに対して暗号化をイネーブルまたはディセーブルにします。  ヒント IPsec で使用できるように "mirror im す。また、any キーワードを使用す
ステップ 4	作成するクリプト アクセス リストごとにステップ 3 を繰り返します。	—

次の作業

少なくとも 1 つの暗号アクセスリストを作成したら、「[IKEv1 および IKEv2 プロポーザルのトランスフォームセットの設定](#)」セクションの説明に従って、トランスフォームセットを定義する必要があります。

次に、クリプトマップセットを設定してインターフェイスに適用するときに、クリプトアクセスリストを特定のインターフェイスに関連付ける必要があります。（「[クリプト マップ セッ](#)」

トの作成」および「インターフェイスへのクリプト マップ セットの適用」セクションの手順に従います)。

IKEv1 および IKEv2 プロポーザルのトランスフォーム セットの設定

この作業は、IKEv1 および IKEv2 プロポーザルとの IPsec SA のネゴシエーション時に IPsec ピアが使用するトランスフォーム セットを定義するために実行します。

機能制限

SEAL 暗号化を指定する場合は、次の制約事項に注意してください。

- ルータと他のピアがハードウェア IPsec 暗号化を備えていないこと。
- ルータおよび他のピアが IPsec をサポートすること。
- ルータおよび他のピアが k9 サブシステムをサポートすること。
- SEAL 暗号化はシスコ製の装置だけで使用可能。したがって、相互運用性はありません。
- IKEv1 と異なり、認証方式と SA ライフタイムは IKEv2 ではネゴシエーション可能ではありません。そのため、これらのパラメータを IKEv2 プロポーザルで設定することはできません。

IKEv1 のトランスフォーム セットの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]]**
4. **mode [tunnel | transport]**
5. **end**
6. **clear crypto sa [peer {ip-address | peer-name} | sa map map-name | sa entry destination-address protocol spi]**
7. **show crypto ipsec transform-set [tag transform-set-name]**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例 : <pre>Device# configure terminal</pre>	グローバル構成モードを開始します。
ステップ 3	crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]] 例 : <pre>Device(config)# crypto ipsec transform-set aasset esp-aes 256 esp-sha-hmac</pre>	トランスフォームセットを定義し、暗号化トランスフォーム コンフィギュレーション モードを開始します。 • transform 引数に使用できるエントリを定義する複合ルールがあります。これらルールについては、crypto ipsec transform-set コマンドのコマンド解説で説明します。また、「トランスフォームセットの概要」の表に、許可されるトランスフォームの組み合わせのリストを示します。
ステップ 4	mode [tunnel transport] 例 : <pre>Device(cfg-crypto-tran)# mode transport</pre>	(任意) トランスフォームセットに関連付けられたモードを変更します。 • このモード設定は、送信元アドレスと宛先アドレスが IPsec ピア アドレスであるトラフィックだけに適用され、その他すべてのトラフィックに対しては無視されます。(他のトラフィックはすべてトンネル モードです)。
ステップ 5	end 例 : <pre>Device(cfg-crypto-tran)# end</pre>	暗号トランスフォーム コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 6	clear crypto sa [peer {ip-address peer-name} sa map map-name sa entry destination-address protocol spi] 例 : <pre>Device# clear crypto sa</pre>	(任意) 既存の IPsec SA を消去して、その後確立された SA でトランスフォーム セットへの変更が有効になるようにします。 手動で確立した SA は、すぐに再確立されます。 • パラメータを指定せずに clear crypto sa コマンドを使用すると、SA データベースの内容が完全に消去されるので、アクティブなセキュリティセッションが消去されます。 • SA データベースのサブセットだけを消去するには、peer、map、または entry キーワードも指定します。
ステップ 7	show crypto ipsec transform-set [tag transform-set-name] 例 :	(任意) 設定済みのトランスフォームセットを表示します。

	コマンドまたはアクション	目的
	Device# show crypto ipsec transform-set	

次の作業

トランスフォーム セットを定義したら、「クリプト マップ セットの作成」の手順に従ってクリプト マップを作成する必要があります。

IKEv2 のトランスフォーム セットの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 proposal *proposal-name***
4. **encryption transform1 [transform2] ...**
5. **integrity transform1 [transform2] ...**
6. **group transform1 [transform2] ...**
7. **end**
8. **show crypto ikev2 proposal**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル構成モードを開始します。
ステップ 3	crypto ikev2 proposal <i>proposal-name</i> 例 : Device(config)# crypto ikev2 proposal proposal-1	プロポーザルの名前を指定し、暗号 IKEv2 プロポーザルコンフィギュレーションモードを開始します。 • IKEv2 ポリシーでは、プロポーザル名を使用してプロポーザルが参照されます。
ステップ 4	encryption transform1 [transform2] ... 例 : Device(config-ikev2-proposal)# encryption aes-cbc-128	(任意) 次の暗号化タイプのトランスフォームを 1 つ以上指定します。 • AES-CBC 128 : 128 ビット AES-CBC

	コマンドまたはアクション	目的
		• AES-CBC 192 : 192 ビット AES-CBC • AES-CBC 256 : 256 ビット AES-CBC • 3DES : 168 ビット DES (非推奨。AES が推奨されている暗号化アルゴリズムです)。
ステップ 5	integrity transform1 [transform2] ... 例 : <pre>Device(config-ikev2-proposal)# integrity sha1</pre>	(任意) 次の整合性タイプのトランスフォームを 1 つ以上指定します。 • sha256 キーワードは、ハッシュアルゴリズムとして SHA-2 ファミリ 256 ビット (HMAC バリエーション) を指定します。 • sha384 キーワードは、ハッシュアルゴリズムとして SHA-2 ファミリ 384 ビット (HMAC バリエーション) を指定します。 • sha512 キーワードは、ハッシュアルゴリズムとして SHA-2 ファミリ 512 ビット (HMAC バリエーション) を指定します。 • sha1 キーワードは、ハッシュアルゴリズムとして SHA-1 (HMAC バリエーション) を指定します。 • md5 キーワードは、ハッシュアルゴリズムとして MD5 (HMAC バリエーション) を指定します。 (非推奨。SHA-1 が推奨されている代替品です)。
ステップ 6	group transform1 [transform2] ... 例 : <pre>Device(config-ikev2-proposal)# group 14</pre>	(任意) 使用可能な DH グループタイプのトランスフォームを 1 つ以上指定します。 • 1 : 768 ビット DH (非推奨) • 2 : 1024 ビット DH (非推奨) • 5 : 1536 ビット DH (非推奨) • 14 : 2048 ビット DH グループを指定します。 • 15 : 3072 ビット DH グループを指定します。 • 16 : 4096 ビット DH グループを指定します。 • 19 : 256 ビット Elliptic Curve DH (ECDH) グループを指定します。 • 20 : 384 ビット ECDH グループを指定します。

	コマンドまたはアクション	目的
		• 24 : 2048 ビット DH/DSA グループを指定します。
ステップ 7	end 例 : Device(config-ikev2-proposal)# end	暗号 IKEv2 プロポーザル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 8	show crypto ikev2 proposal 例 : Device# show crypto ikev2 proposal	(任意) 各 IKEv2 プロポーザルのパラメータを表示します。

IKEv2 のトランスフォーム セットの例

次の例では、プロポーザルの設定方法を示しています。

各トランスフォーム タイプに対して 1 つのトランスフォームがある IKEv2 プロポーザル

```
Device(config)# crypto ikev2 proposal proposal-1
Device(config-ikev2-proposal)# encryption aes-cbc-128
Device(config-ikev2-proposal)# integrity sha1
Device(config-ikev2-proposal)# group 14
```

各トランスフォーム タイプに対して複数のトランスフォームがある IKEv2 プロポーザル

```
crypto ikev2 proposal proposal-2
encryption aes-cbc-128 aes-cbc-192
integrity sha1 sha256
group 14 15
```

トランスフォームの組み合わせのリストについては、「[Configuring Security for VPNs with IPsec](#)」を参照してください。

発信側と応答側の IKEv2 プロポーザル

発信側のプロポーザルは次のとおりです。

```
Device(config)# crypto ikev2 proposal proposal-1
Device(config-ikev2-proposal)# encryption aes-cbc-128 aes-cbc-196
Device(config-ikev2-proposal)# integrity sha1 sha256
Device(config-ikev2-proposal)# group 14 16
```

応答側のプロポーザルは次のとおりです。

```
Device(config)# crypto ikev2 proposal proposal-2
Device(config-ikev2-proposal)# encryption aes-cbc-196 aes-cbc-128
Device(config-ikev2-proposal)# integrity sha256 sha1
Device(config-ikev2-proposal)# group 16 14
```

このシナリオでは、発信側のアルゴリズムの選択が優先されます。選択されたアルゴリズムは次のとおりです。

```
encryption aes-cbc-128
integrity sha1
group 14
```

次の作業

トランスフォームセットを定義したら、「クリプトマップセットの作成」の手順に従ってクリプトマップを作成する必要があります。

クリプトマップセットの作成

スタティック クリプトマップの作成

IKE を使用して SA が確立されると、IPsec ピアは、新しいセキュリティ アソシエーションに使用する設定をネゴシエートできます。つまり、クリプトマップ エントリ内でリスト（許容されるトランスフォームのリストなど）を指定できます。

このタスクは、IKE を使用して SA を確立するクリプトマップ エントリを作成するために実行します。IPv6 クリプトマップ エントリを作成するには、**crypto map** コマンドで **ipv6** キーワードを使用する必要があります。IPv4 クリプトマップでは、**ipv6** キーワードなしで **crypto map** コマンドを使用します。



(注) セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『[Next Generation Encryption](#)』（NGE）ホワイト ペーパーを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map [ipv6] map-name seq-num [ipsec-isakmp]**
4. **match address access-list-id**
5. **set peer {hostname | ip-address}**
6. **crypto ipsec security-association dummy {pps rate | seconds seconds}**
7. **set transform-set transform-set-name1 [transform-set-name2...transform-set-name6]**
8. **set security-association lifetime {seconds seconds | kilobytes kilobytes | kilobytes disable}**
9. **set security-association level per-host**
10. **set pfs [group1 | group14 | group15 | group16 | group19 | group2 | group20 | group24 | group5]**
11. **end**
12. **show crypto map [interface interface | tag map-name]**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル構成モードを開始します。
ステップ 3	crypto map [ipv6] map-name seq-num [ipsec-isakmp] 例 : Device(config)# crypto map static-map 1 ipsec-isakmp	クリプト マップ エントリを作成または変更し、クリプト マップ コンフィギュレーション モードを開始します。 • IPv4 クリプトマップでは、ipv6 キーワードなしでコマンドを使用します。
ステップ 4	match address access-list-id 例 : Device(config-crypto-m)# match address vpn-tunnel	拡張アクセス リストに名前を付けます。 • このアクセス リストは、このクリプト マップ エントリに照らして、IPsec で保護する必要があるトラフィックと IPsec セキュリティで保護する必要のないトラフィックを判別します。
ステップ 5	set peer {hostname ip-address} 例 : Device(config-crypto-m)# set-peer 192.168.101.1	リモート IPsec ピアを指定します。これは、IPsec 保護されたトラフィックの転送先となるピアです。 • 複数のリモート ピアに対して、同じ作業を繰り返します。
ステップ 6	crypto ipsec security-association dummy {pps rate seconds seconds} 例 : Device(config-crypto-m)# set security-association dummy seconds 5	ダミー パケットの生成を有効にします。これらのダミー パケットは、クリプト マップ内で作成されたすべてのフローに対して生成されます。
ステップ 7	set transform-set transform-set-name1 [transform-set-name2...transform-set-name6] 例 : Device(config-crypto-m)# set transform-set aasset	このクリプト マップ エントリで許可するトランスフォーム セットを指定します。 • 複数のトランスフォーム セットをプライオリティ順（最高のプライオリティのものが最初）に列挙します。

	コマンドまたはアクション	目的
ステップ 8	set security-association lifetime {seconds seconds kilobytes kilobytes kilobytes disable} 例 : <pre>Device (config-crypto-m)# set security-association lifetime seconds 2700</pre>	(任意) クリプトマップ エントリの SA ライフタイムを指定します。 デフォルトでは、クリプトマップの SA はグローバルライフタイムに従ってネゴシエーションされ、これはディセーブルにできます。
ステップ 9	set security-association level per-host 例 : <pre>Device (config-crypto-m)# set security-association level per-host</pre>	(任意) 送信元と宛先ホストのペアごとに、個別の SA を確立するよう指定します。 デフォルトで、1 つの IPsec 「トンネル」を使用して、複数の送信元ホストと複数の宛先ホストのトラフィックを伝送できます。  注意 特定のサブネット間の複数のストリムをサポートするため、このコマンドは注意して使用してください。
ステップ 10	set pfs [group1 group14 group15 group16 group19 group2 group20 group24 group5] 例 : <pre>Device (config-crypto-m)# set pfs group14</pre>	(任意) IPsec がこのクリプトマップ エントリの新しい SA を要求するときに Password Forward Secrecy (PFS) を要求するか、IPsec ピアから受信する要求に PFS を含めるように要求するかを指定します。 - グループ 1 は、768 ビット Diffie-Hellman (DH) 識別子を指定します (デフォルト)。(非推奨)。 - グループ 2 は、1024 ビット DH 識別子を指定します。(非推奨)。 - グループ 5 は、1536 ビット DH 識別子を指定します。(非推奨)。 - グループ 14 は、2048 ビット DH 識別子を指定します。 - グループ 15 は、3072 ビット DH 識別子を指定します。 - グループ 16 は、4096 ビット DH 識別子を指定します。 - グループ 19 は、256 ビット Elliptic Curve DH (ECDH) 識別子を指定します。 - グループ 20 は、384 ビット ECDH 識別子を指定します。

	コマンドまたはアクション	目的
		- グループ 24 は、2048 ビット DH/DSA 識別子を指定します。 - デフォルトでは、PFS は要求されません。このコマンドでグループが指定されなかった場合は、グループ 1 がデフォルトとして使用されます。
ステップ 11	end 例： Device(config-crypto-m)# end	クリプト マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 12	show crypto map [interface interface tag map-name] 例： Device# show crypto map	クリプト マップ コンフィギュレーションを表示します。

トラブルシューティングのヒント

特定の設定変更は、それ以後の SA をネゴシエーションする場合にだけ有効になります。新しい設定をすぐに有効にする場合は、既存の SA が変更後の設定で再確立されるように、これらの SA を消去する必要があります。ルータが活発に IPsec トラフィックを処理する場合は、設定変更によって影響を受ける SA データベースの一部だけを消去します（つまり、所定のクリプト マップ セットで確立されている SA だけを消去します）。大規模な変更を行う場合や、ルータが他の IPsec トラフィックをほとんど処理しない場合を除いて、SA データベースを完全に消去しないでください。

IPsec SA をクリアするには、**clear crypto sa** コマンドと適切なパラメータを使用してください。（パラメータをすべて省略すると、SA データベースが完全に消去され、アクティブなセキュリティ セッションも消去されてしまいます）。

次の作業

スタティック クリプト マップ を正常に作成したら、IPsec トラフィック フローが通過する各インターフェイスにクリプト マップ セットを適用する必要があります。このタスクを完了するには、「[インターフェイスへのクリプト マップ セットの適用](#)」セクションを参照してください。

ダイナミック クリプト マップ の作成

ダイナミック クリプト マップ エントリにより、IPsec SA を確立できるトラフィックを制限するクリプト アクセス リストを指定します。トラフィックのフィルタリング中、アクセス リストを指定しないダイナミック クリプト マップ エントリは、無視されます。ダイナミック クリプト マップ エントリに空のアクセス リストが含まれていると、トラフィックが廃棄されます。クリプト マップ セットにダイナミック クリプト マップ エントリが 1 つしかない場合、クリプト マップ セットは許容範囲内のトランスフォーム セットを指定する必要があります。

このタスクは、SA の確立に IKE を使用するダイナミック クリプト マップ エントリを作成するために実行します。



(注) IPv6 アドレスは、ダイナミック クリプト マップではサポートされません。



(注) セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『[Next Generation Encryption](#)』（NGE）ホワイト ペーパーを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *dynamic-map-name* *dynamic-seq-num*
4. **set transform-set** *transform-set-name1* [*transform-set-name2*...*transform-set-name6*]
5. **match address** *access-list-id*
6. **set peer** {*hostname* | *ip-address*}
7. **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes* | **kilobytes disable**}
8. **set pfs** [**group1** | **group14** | **group15** | **group16** | **group19** | **group2** | **group20** | **group24** | **group5**]
9. **exit**
10. **exit**
11. **show crypto dynamic-map** [**tag** *map-name*]
12. **configure terminal**
13. **crypto map** *map-name* *seq-num* **ipsec-isakmp** **dynamic** *dynamic-map-name*
14. **exit**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル構成モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	crypto dynamic-map dynamic-map-name dynamic-seq-num 例 : Device(config)# crypto dynamic-map test-map 1	ダイナミック クリプト マップ エントリを作成し、クリプトマップ 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	set transform-set transform-set-name1 [transform-set-name2...transform-set-name6] 例 : Device(config-crypto-m)# set transform-set aasset	このクリプト マップ エントリで許可するトランスフォーム セットを指定します。 複数のトランスフォーム セットをプライオリティ順（最高のプライオリティのものが最初）に列挙します。これは、ダイナミック クリプト マップ エントリで必要とされる唯一の設定文です。
ステップ 5	match address access-list-id 例 : Device(config-crypto-m)# match address 101	（任意）拡張アクセス リストのリスト番号またはリスト名を指定します。 - このアクセス リストは、このクリプト マップ エントリに照らして、IPsec で保護する必要があるトラフィックと、IPsec セキュリティで保護しないトラフィックを決定します。  （注） ダイナミック クリプト マップで推奨します。 - アクセスリストが設定されている場合、IPsec ピアによって提示されるデータフロー ID は、このクリプトアクセスリストの permit ステートメントの範囲内である必要があります。 - アクセス リストが設定されていない場合、デバイスは、IPsec ピアが提示したデータフロー ID を受け入れます。ただし、アクセス リストが設定されていても指定されたアクセス リストが存在しない、あるいは空である場合、デバイスはすべてのパケットを廃棄します。これは、アクセス リストを指定する必要のあるスタティック クリプト マップと同様です。 - アクセスリストはネゴシエーションだけでなくパケットフィルタリングでも使用されるため、any キーワードをアクセスリストで使用する場合には注意が必要です。

	コマンドまたはアクション	目的
		一致アドレスを設定する必要があります。設定しない場合、パケットがクリアテキスト（暗号解除されて）で送信されるため、動作が不安定になり、TED をイネーブルにできません。
ステップ 6	set peer {hostname ip-address} 例 : Device(config-crypto-m)# set peer 192.168.101.1	（任意）リモート IPsec ピアを指定します。リモートピアが複数ある場合、このステップを繰り返します。  （注）ダイナミック クリプトマップ エントリは、多く
ステップ 7	set security-association lifetime {seconds seconds kilobytes kilobytes kilobytes disable} 例 : Device(config-crypto-m)# set security-association lifetime seconds 7200	（任意）IP セキュリティ SA をネゴシエーションするときに使用されるグローバル ライフタイム値を上書きします（特定のクリプトマップ エントリの場合）。  （注）高帯域幅環境でのキーの再生成時の量のライフタイム有効期限によつ
ステップ 8	set pfs [group1 group14 group15 group16 group19 group2 group20 group24 group5] 例 : Device(config-crypto-m)# set pfs group14	（任意）IPsec がこのクリプトマップ エントリの新しい SA を要求した場合、PFS を要求するように、または IPsec ピアから受信する要求に PFS が含まれることを要求するように指定します。 - グループ 1 は、768 ビット Diffie-Hellman (DH) 識別子を指定します（デフォルト）。（非推奨）。 - グループ 2 は、1024 ビット DH 識別子を指定します。（非推奨）。 - グループ 5 は、1536 ビット DH 識別子を指定します。（非推奨） - グループ 14 は、2048 ビット DH 識別子を指定します。 - グループ 15 は、3072 ビット DH 識別子を指定します。

	コマンドまたはアクション	目的
		- グループ 16 は、4096 ビット DH 識別子を指定します。 - グループ 19 は、256 ビット Elliptic Curve DH (ECDH) 識別子を指定します。 - グループ 20 は、384 ビット ECDH 識別子を指定します。 - グループ 24 は、2048 ビット DH/DSA 識別子を指定します。 - デフォルトでは、PFS は要求されません。このコマンドでグループが指定されなかった場合は、group1 がデフォルトとして使用されます。
ステップ 9	exit 例 : Device(config-crypto-m)# exit	クリプトマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	exit 例 : Device(config)# exit	グローバル コンフィギュレーション モードを終了します。
ステップ 11	show crypto dynamic-map [tag map-name] 例 : Device# show crypto dynamic-map	(任意) ダイナミック クリプト マップに関する情報を表示します。
ステップ 12	configure terminal 例 : Device# 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 13	crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-name 例 : Device(config)# crypto map static-map 1 ipsec-isakmp dynamic test-map	(任意) クリプトマップセットにダイナミック クリプトマップを追加します。 クリプトマップセット内のプライオリティの最も低いエントリに、ダイナミック マップを参照するクリプトマップ エントリを設定する必要があります。
ステップ 14	exit 例 : Device(config)# exit	グローバル構成モードを終了します。

トラブルシューティングのヒント

特定の設定変更は、それ以後の SA をネゴシエーションする場合にだけ有効になります。新しい設定をすぐに有効にする場合は、既存の SA が変更後の設定で再確立されるように、これらの SA を消去する必要があります。ルータが活発に IPsec トラフィックを処理する場合は、設定変更によって影響を受ける SA データベースの一部だけを消去します（つまり、所定のクリプトマップセットで確立されている SA だけを消去します）。大規模な変更を行う場合や、ルータが最小の IPsec トラフィックを処理している場合を除いて、SA データベース全体のクリアを予約しないでください。

IPsec SA をクリアするには、**clear crypto sa** コマンドと適切なパラメータを使用してください。（パラメータをすべて省略すると、SA データベースが完全に消去され、アクティブなセキュリティセッションも消去されてしまいます）。

次の作業

クリプトマップセットを正常に作成したら、IPsec トラフィックフローが通過する各インターフェイスにクリプトマップセットを適用する必要があります。このタスクを完了するには、「[インターフェイスへのクリプトマップセットの適用](#)」セクションを参照してください。

手動による SA を確立するためのクリプトマップエントリの作成

このタスクは、クリプトマップエントリを作成して手動 SA を確立するため（つまり、SA の確立に IKE が使用されない場合）に実行します。IPv6 クリプトマップエントリを作成するには、**crypto map** コマンドで **ipv6** キーワードを使用する必要があります。IPv4 クリプトマップでは、**ipv6** キーワードなしで **crypto map** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map [ipv6] map-name seq-num [ipsec-manual]**
4. **match address access-list-id**
5. **set peer {hostname | ip-address}**
6. **set transform-set transform-set-name**
7. 次のいずれかを実行します。
 - **set session-key inbound ah spi hex-key-string**
 - **set session-key outbound ah spi hex-key-string**
8. 次のいずれかを実行します。
 - **set session-key inbound esp spi cipher hex-key-string [authenticator hex-key-string]**
 - **set session-key outbound esp spi cipher hex-key-string [authenticator hex-key-string]**
9. **exit**
10. **exit**
11. **show crypto map [interface interface | tag map-name]**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル構成モードを開始します。
ステップ 3	crypto map [ipv6] map-name seq-num [ipsec-manual] 例 : Device(config)# crypto map mymap 10 ipsec-manual	作成または変更するクリプト マップ エントリを指定して、クリプト マップ コンフィギュレーションモードを開始します。 • IPv4 クリプトマップでは、ipv6 キーワードなしで crypto map コマンドを使用します。
ステップ 4	match address access-list-id 例 : Device(config-crypto-m)# match address 102	このクリプトマップエントリに照らして、IPsec で保護するトラフィックと、IPsec で保護しないトラフィックを決定する IPsec アクセスリストに名前を付けます • IKE を使用しない場合、アクセスリストは permit エントリを 1 つだけ指定できます。
ステップ 5	set peer {hostname ip-address} 例 : Device(config-crypto-m)# set peer 10.0.0.5	リモート IPsec ピアを指定します。これは、IPsec 保護されたトラフィックの転送先となるピアです • IKE を使用しない場合、ピアを 1 つだけ指定できます。
ステップ 6	set transform-set transform-set-name 例 : Device(config-crypto-m)# set transform-set someset	使用するトランスフォーム セットを指定します。 • これは、リモートピアの対応するクリプト マップ エントリで指定したトランスフォーム セットと同じである必要があります。  (注) IKE を使用しない場合、トラン

手動で確立された SA の場合、変更を有効にするために SA を消去し、再初期化する必要があります。IPsec SA をクリアするには、**clear crypto sa** コマンドと適切なパラメータを使用してください。（パラメータをすべて省略すると、SA データベース全体がクリアされ、アクティブなセキュリティ セッションもクリアされてしまいます）。

次の作業

クリプトマップセットを正常に作成したら、IPsec トラフィック フローが通過する各インターフェイスにクリプト マップ セットを適用する必要があります。このタスクを完了するには、「[インターフェイスへのクリプト マップ セットの適用](#)」セクションを参照してください。

インターフェイスへのクリプト マップ セットの適用

クリプトマップセットは、IPsec トラフィックが通過する各インターフェイスに適用する必要があります。インターフェイスにクリプト マップ セットを適用すると、デバイスに対して、トラフィックをクリプトマップで保護する代わりに、インターフェイスのトラフィックをクリプト マップ セットに対して評価し、接続中またはセキュリティ アソシエーション ネゴシエーション中に指定されたポリシーを使用するように指示されます。

インターフェイスにクリプト マップを適用するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type/number**
4. **crypto map map-name**
5. **exit**
6. **crypto map map-name local-address interface-id**
7. **exit**
8. **show crypto map [interface interface]**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル構成モードを開始します。
ステップ 3	interface type/number 例 : Device(config)# interface FastEthernet 0/0	インターフェイスを設定し、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。

	コマンドまたはアクション	目的
ステップ 4	crypto map map-name 例 : Device(config-if)# crypto map mymap	インターフェイスに対してクリプト マップ セットを適用します。
ステップ 5	exit 例 : Device(config-if)# exit	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 6	crypto map map-name local-address interface-id 例 : Device(config)# crypto map mymap local-address loopback0	(任意) 冗長インターフェイスが同じローカルアイデンティティを使用して、同じクリプトマップを共有できるようにします。
ステップ 7	exit 例 : Device(config)# exit	(任意) グローバル コンフィギュレーション モードを終了します。
ステップ 8	show crypto map [interface interface] 例 : Device# show crypto map	(任意) クリプト マップ コンフィギュレーションを表示します。

IPsec VPN の設定例

例 : AES ベースのスタティック暗号マップの設定

この例は、スタティック クリプト マップを設定し、暗号化方式として AES を定義する方法を示しています。

```
crypto isakmp policy 10
  encryption aes 256
  authentication pre-share
  group 14
  lifetime 180
crypto isakmp key cisco123 address 10.0.110.1
!
!
crypto ipsec transform-set aasset esp-aes 256 esp-sha-hmac
  mode transport
!
crypto map aesmap 10 ipsec-isakmp
  set peer 10.0.110.1
  set transform-set aasset
  match address 120
!
!
!
```

```
voice call carrier capacity active
!
!
mta receive maximum-recipients 0
!
!
interface FastEthernet0/0
 ip address 10.0.110.2 255.255.255.0
 ip nat outside
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
 crypto map aesmap
!
interface Serial0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 ip address 10.0.110.1 255.255.255.0
 ip nat inside
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
!
ip nat inside source list 110 interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.5.1.1
ip route 10.0.110.0 255.255.255.0 FastEthernet0/0
ip route 172.18.124.0 255.255.255.0 10.5.1.1
ip route 172.18.125.3 255.255.255.255 10.5.1.1
ip http server
!
!
access-list 110 deny ip 10.0.110.0 0.0.0.255 10.0.110.0 0.0.0.255
access-list 110 permit ip 10.0.110.0 0.0.0.255 any
access-list 120 permit ip 10.0.110.0 0.0.0.255 10.0.110.0 0.0.0.255
!
```

IPsec を使用した VPN のセキュリティの設定に関する追加のリファレンス

関連資料

関連項目	マニュアルタイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
IKE、IPsec、および PKI のコンフィギュレーション コマンド	『Cisco IOS Security Command Reference Commands A to C』 『Cisco IOS Security Command Reference Commands D to L』 『Cisco IOS Security Command Reference Commands M to R』 『Cisco IOS Security Command Reference Commands S to Z』
IKE 設定	「Configuring Internet Key Exchange for IPsec VPNs」
Suite-B SHA-2 ファミリ (HMAC バリエーション) および Elliptic Curve (EC) キーペアの設定	「Configuring Internet Key Exchange for IPsec VPNs」
Suite-B 整合性アルゴリズム タイプのトランスフォームの設定	「Configuring Internet Key Exchange Version 2 (IKEv2)」
IKEv2 用の Suite-B の Elliptic Curve Digital Signature Algorithm (ECDSA) signature (ECDSA-sig) 認証方式の設定	「Configuring Internet Key Exchange Version 2 (IKEv2)」
IPsec SA ネゴシエーションでの Suite-B の Elliptic Curve Diffie-Hellman (ECDH) のサポート	「Configuring Internet Key Exchange for IPsec VPNs」 「Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site」
PKI の証明書登録のための Suite-B サポート	「PKI の証明書登録の設定」
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準

標準	タイトル
なし	—

MIB

MIB	MIB のリンク
• CISCO-IPSEC-FLOW-MONITOR-MIB • CISCO-IPSEC-MIB • CISCO-IPSEC-POLICY-MAP-MIB	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、およびフィチャセットの 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。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2401	『Security Architecture for the Internet Protocol』
RFC 2402	『IP Authentication Header』
RFC 2403	『The Use of HMAC-MD5-96 within ESP and AH』
RFC 2404	『The Use of HMAC-SHA-1-96 within ESP and AH』
RFC 2405	『The ESP DES-CBC Cipher Algorithm With Explicit IV』
RFC 2406	『IP Encapsulating Security Payload (ESP)』
RFC 2407	『The Internet IP Security Domain of Interpretation for ISAKMP』
RFC 2408	『Internet Security Association and Key Management Protocol (ISAKMP)』

テクニカル サポート

説明	リンク
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。	http://www.cisco.com/cisco/web/support/index.html

IPsec を使用した VPN のセキュリティの設定に関する機能情報

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 トレー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、<https://cfmng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 2: IPsec VPN のセキュリティ設定に関する機能情報

機能名	ソフトウェア リリース	機能情報
Advanced Encryption Standard		この機能により、新しい暗号化規格 AES に対するサポートが追加されます。AES は、DES の後継として開発された IPsec および IKE のプライバシー トランスフォームです。 この機能により、次のコマンドが変更されました。 crypto ipsec transform-set 、 encryption (IKE policy) 、 show crypto ipsec transform-set 、 show crypto isakmp policy 。
IOS ソフトウェア暗号での Suite-B のサポート		Suite-B には、IKE と IPsec で使用するための暗号化アルゴリズムの 4 つのユーザ インターフェイス スイートのサポートが追加されています。これは RFC 4869 に記述されています。各スイートは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー合意アルゴリズム、ハッシュまたはメッセージダイジェスト アルゴリズムで構成されています。 この機能により、 crypto ipsec transform-set コマンドが変更されました。



(注) GetVPN 暗号マップは、IOS XE 16.9.1 以降のポートチャネルインターフェイスでサポートされています。

用語集

anti-replay : 受信者が再送攻撃から自身を保護するために、古いパケットまたは重複するパケットを拒否できるセキュリティサービス。IPSec は、データ認証とシーケンス番号を組み合わせることで使用することにより、このオプション サービスを提供します。Cisco IOS XE IPSec は、手動で確立された SA (IKE ではなく、設定によって確立された SA) を除いて、データ認証サービスを実行するときは必ずこのサービスを提供します。

data authentication : データの整合性および発信元の検証。データ認証は、整合性だけを意味する場合と、整合性と認証の両方の概念を意味する場合があります (ただし、データ発信元認証はデータの整合性に依存します)。

data confidentiality : 保護されたデータが第三者に読み取られないようにするセキュリティサービス。

data flow : 送信元アドレスまたはマスク、宛先アドレスまたはマスク、IP 次プロトコルフィールド、送信元および宛先ポートの組み合わせによって識別されるトラフィックの集まり。プロトコルフィールドおよびポートフィールドには **any** の値が含まれます。IPSec 保護はデータフローに適用されます。

IKE : Internet Key Exchange (インターネット キー エクスチェンジ) 。IKE は、共有セキュリティ ポリシーを確立し、キーを必要とするサービス (IPSec など) のキーを認証します。IPSec トラフィックが通過する前に、各ルータ、ファイアウォール、およびホストはそのピアの ID を検証する必要があります。それには、事前共有キーを両ホストに手動で入力するか、CA サービスを使用します。

IPsec : IP Security (IP セキュリティ) 。参加ピア間でのデータの機密性、整合性、および認証を提供するオープンスタンダードの枠組みです。IPSec は、このようなセキュリティ サービスを IP レイヤで提供します。IPSec は IKE を使用して、プロトコルやアルゴリズムのネゴシエーションをローカル ポリシーに基づいて処理し、IPSec で使用される暗号キーや認証キーを生成します。IPSec では、一対のホスト間、一対のセキュリティ ゲートウェイ間、または一対のセキュリティ ゲートウェイとホストの間で 1 つ以上のデータ フローを保護できます。

peer : ここで使用する「ピア」とは、IPsec に参加するルータまたはその他のデバイスです。

PFS : Perfect Forward Secrecy。これは、導き出される共有秘密値に関連する暗号特性です。PFS を使用すると、1 つのキーが損なわれても、これ以降のキーは前のキーの取得元から取得されないため、前および以降のキーには影響しません。

SA : Security Association (セキュリティ アソシエーション) 。2 つ以上のエンティティが、特定のデータフローにおいて安全に通信するために、特定のセキュリティ プロトコル (AH または ESP) と関連してセキュリティ サービスを使用する方法を記述します。トラフィックを保護するために、トランス フォームと共有秘密キーが使用されます。

SPI : Security Parameter Index (セキュリティ パラメータ インデックス) 。これは、宛先 IP アドレスおよびセキュリティ プロトコルを組み合わせ、特定の SA を一意に識別する番号です。IKE を使用しない場合、SPI は、手動で各セキュリティ アソシエーションに指定されます。

transform : データ認証、データ機密性、およびデータ圧縮を実現するためにデータフローで実行される処理のリスト。たとえば、トランスフォームには、HMAC MD5 認証アルゴリズムを使用する ESP プロトコル、56 ビット DES 暗号規格アルゴリズムを使用する AH プロトコルおよび HMAC-SHA 認証アルゴリズムを使用する ESP プロトコルなどがあります。

tunnel : ここで使用する「トンネル」とは、2つのピア間（2台のルータなど）の安全な通信パスです。トンネルモードで IPsec を使用することではありません。



第 3 章

IPSec 仮想トンネル インターフェイス

IPsec 仮想トンネル インターフェイス (VTI) では、IPsec トンネルを終了するためのルーティング可能なインターフェイス タイプと、オーバーレイ ネットワークを形成するためにサイト間の保護を定義する簡単な手段が提供されます。IPsec VTI によって、リモート リンクを保護するための IPsec の設定が簡素化され、マルチキャストがサポートされ、さらには、ネットワーク管理およびロード バランシングが簡単に実現できるようになります。



(注) セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『[Next Generation Encryption](#)』(NGE) ホワイトペーパーを参照してください。

- [機能情報の確認 \(39 ページ\)](#)
- [IPsec 仮想トンネル インターフェイスの制約事項 \(40 ページ\)](#)
- [IPsec 仮想トンネル インターフェイスに関する情報 \(41 ページ\)](#)
- [IPsec 仮想トンネル インターフェイスの設定方法 \(47 ページ\)](#)
- [IPsec 仮想トンネル インターフェイスの設定例 \(65 ページ\)](#)
- [IPsec 仮想トンネル インターフェイスに関する追加のリファレンス \(83 ページ\)](#)
- [IPsec 仮想トンネル インターフェイスに関する機能情報 \(84 ページ\)](#)

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「[Bug Search Tool](#)」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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、<https://cfnnng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

IPsec 仮想トンネル インターフェイスの制約事項

フラグメンテーション

フラグメンテーションは、IPsec トンネルではサポートされていません。ホストの MTU を小さく設定してパケットフラグメントを回避することや、任意のデバイスでパケットをフラグメント化することを選択できます。

IPsec トランスフォーム セット

IPsec トランスフォーム セットを設定できるのは、トンネル モードだけです。

IKE セキュリティ アソシエーション

インターネット キー交換 (IKE) セキュリティ アソシエーション (SA) は VTI にバインドされています。

IPsec SA トラフィック セレクタ

スタティック VTI では、VTI インターフェイスに接続している単一の IPsec SA だけがサポートされます。IPsec SA のトラフィック セレクタは常に "IP any any" です。

デフォルトでは、スタティック VTI (SVTI) は、仮想トンネルインターフェイスに接続された 1 つの IPsec SA のみをサポートします。IPsec SA のトラフィックセレクタは常に "IP any any" です。

IPv4 パケット

この機能は、IPv4 パケットをカプセル化するように設定された SVTI をサポートしますが、IPv4 パケットで IPv6 パケットを伝送したり、IPv6 パケットで IPv4 パケットを伝送したりすることはできません。

tunnel protection

IPsec IPv4 モードで **tunnel mode ipsec ipv4** コマンドを使用する場合は、**shared** キーワードを設定しないでください。

traceroute

VTI での暗号化オフロードを使用したトレースルート機能はサポートされていません。

VxLAN GPE トンネルインターフェイス

VxLAN GPE トンネルインターフェイスは、IPsec VTI と同じ送信元インターフェイスを使用できません。

IPsec 仮想トンネル インターフェイスに関する情報

IPsec VTI の使用により、リモートアクセスの保護を提供する必要がある場合の設定プロセスが簡素化され、カプセル化に Generic Routing Encapsulation (GRE) またはレイヤ 2 トンネリングプロトコル (L2TP) トンネルを使用する代替手段が提供されます。IPsec VTI を使用するメリットは、設定において物理インターフェイスに対する IPsec セッションのスタティックマッピングが必要ないことです。IPsec トンネルエンドポイントは実際 (仮想) のインターフェイスに関連付けられます。トンネルエンドポイントにはルーティング可能なインターフェイスがあるので、多くの共通インターフェイス機能を IPsec トンネルに適用できます。

IPsec VTI によって、複数パスの場合のように、物理インターフェイス上における IP ユニキャストおよびマルチキャストの両方の暗号化トラフィックの送受信の柔軟性が高まります。トラフィックは、トンネルインターフェイスから転送されるときに暗号化され、トンネルインターフェイスに転送されると復号化されます。また、IP ルーティング テーブルによって管理されます。IP ルーティングを使用してトラフィックをトンネルインターフェイスに転送すると、IPsec VPN 設定が簡単になります。DVTI は他のすべての実際のインターフェイスと同様に機能するため、トンネルがアクティブになるとすぐに Quality of Service (QoS)、ファイアウォール、およびその他のセキュリティ サービスを適用できます。

IPsec VTI に関する詳細については、次の各項を参照してください。

IPsec 仮想トンネル インターフェイスを使用するメリット

IPsec VTI によって、機能を適用できる仮想インターフェイスを設定できます。暗号化されていないテキスト パケットの機能は VTI 上で設定されます。暗号化されたパケットの機能は物理外部インターフェイス上で適用されます。IPsec VTI を使用すると、ネットワーク アドレス変換 (NAT)、ACL、QoS などの各種機能のアプリケーションを分離して、それらを暗号化されていないテキストまたは暗号化されたテキスト、あるいはその両方に適用できます。

スタティック VTI (SVTI) と DVTI という 2 つのタイプの VTI インターフェイスが存在します。

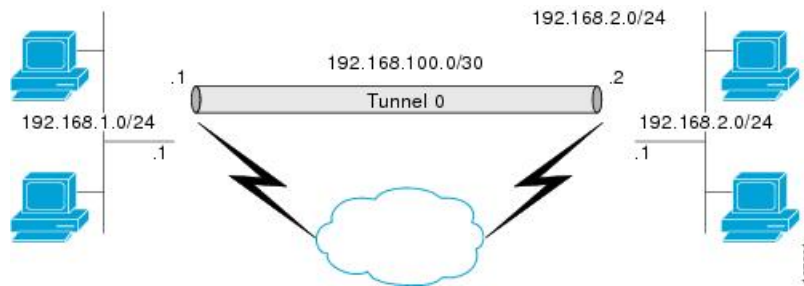
スタティック仮想トンネル インターフェイス

SVTI 設定は、トンネルによって 2 つのサイト間の常にオンであるアクセスが提供される、サイト間接続用に使用できます。

さらに、複数の Cisco IOS ソフトウェア機能を、トンネルインターフェイス上、およびトンネルインターフェイスの物理出力インターフェイス上で直接設定できます。この直接設定によって、ユーザは、暗号化前または暗号化後のパスにおける機能のアプリケーションを確実に管理できます。

次の図に、SVTI の使用方法を示します。

図 1: IPsec SVTI



IPsec VTI によって、ネイティブの IPsec トンネリングがサポートされ、物理インターフェイスのプロパティの大部分が示されます。

SVTI のマルチ SA サポート

デフォルトでは、SVTI のトラフィックセクタは「any any」に設定されます。その結果、「any any」トラフィックセクタに対応する SVTI に単一の IPsec SA が接続されます。

Cisco IOS XE Gibraltar 16.12.1 以降では、アクセス制御リスト（ACL）を定義して SVTI に関連付けることで、デフォルトで定義されている「any any」プロキシではなく特定の送信元プロキシと宛先プロキシの間のトラフィックを選択できます。非 any-any トラフィックセクタごとに IPsec SA が作成されるため、複数の SA が SVTI に接続されます。

この機能は、トンネルモードでの IPsec カプセル化による IPv4 および IPv6 トラフィック保護をサポートしています。この機能は IKEv1 と IKEv2 の両方をサポートしています。

機能制限

- この機能は、共有されたトンネル保護ではサポートされません。
- この機能は、IPsec 混合モードではサポートされません。
- トンネルの両端の SVTI に関連付けられたトラフィックセクタには、一致する送信元プロキシと宛先プロキシが必要です。トンネルを形成する SVTI のいずれかでトラフィックセクタを絞り込まないでください。

ACL の特性と SVTI IPsec SA への影響

- SVTI に関連付けられた ACL に「any any」プロキシを含めないでください。「any any」トラフィックセクタについては、SVTI のデフォルト動作を使用してください（ACL を SVTI に関連付けしないでください）。
- SVTI に関連付けられた ACL は **permit** ステートメントのみをサポートしているので、**deny** ステートメントを含めないでください。
- SVTI に関連付けられた ACL の実行時変更はサポートされていません。ACL の ACE を追加または変更する前にトンネルをシャットダウンしてください。

- SVTI への ACL の関連付けを解除すると、既存の IPSec SA が削除され、「IP any any」のデフォルト トラフィック セレクタに関する新しい IPSec SA が形成されます。
- SVTIに関連付けるアクセス制御エントリ（ACE）は100までにすることをお勧めします。また、さまざまなトンネルインターフェイスに関連付けられたすべての ACL で使用される ACE の合計が 2000 を超えないようにすることをお勧めします。

逆ルート注入

マルチ SA の SVTI の場合は、IPSec プロファイルで逆ルート注入（RRI）を設定できます。

拡張 ACL または ACE オプション（プロトコル、ポート番号、DHCP など）を使用する場合は、RRIを使用しないでください。ルーティングにはルートマップなどの他の手段を使用してください。



(注) 距離とタグによる RRI 機能は、まだサポートされていません。

ダイナミック仮想トンネル インターフェイス

DVTIによって、リモートアクセスVPN用接続のセキュリティ保護とスケーラビリティが向上します。DVTIテクノロジーは、ダイナミッククリプトマップとトンネルを確立するためのダイナミック ハブアンドスポーク方式にとって代わるものです。



(注) IKEv1 または IKEv2 を使用して DVTI を設定できます。レガシー クリプト マップ ベースの設定は、IKEv1 を使用した DVTI しかサポートしません。IKEv2 を使用した DVTI 設定は FlexVPN でのみサポートされます。

DVTI は、サーバと、リモート設定の両方に対して使用可能です。トンネルにより、各 VPN セッションに対して、仮想アクセスインターフェイスがオンデマンドで個別に提供されます。仮想アクセスインターフェイス設定は、仮想テンプレート設定からコピーされます。このコピーには、IPsec 設定と、QoS、NetFlow、ACL といった、仮想テンプレートインターフェイス上で設定されたすべての Cisco IOS ソフトウェア機能が含まれています。

DVTI は、他の現実のインターフェイスと同様に機能するため、トンネルがアクティブになった直後に、QoS、ファイアウォール、またはその他のセキュリティサービスを適用できます。QoS機能を使用して、ネットワーク上の各種アプリケーションのパフォーマンスを向上させることが可能です。Cisco IOS ソフトウェア内で提供される各種 QoS 機能の組み合わせを使用して、音声、ビデオ、またはデータ アプリケーションをサポートできます。

DVTI によって、IP アドレスを効率的に使用できるようになり、また、セキュアな接続を実現できます。DVTI によって、動的にダウンロード可能な、グループごとおよびユーザーごとのポリシーを RADIUS サーバー上で設定できます。グループ単位またはユーザ単位の定義は、拡張認証（Xauth）User または Unity グループを使用して作成することも、証明書から抽出する

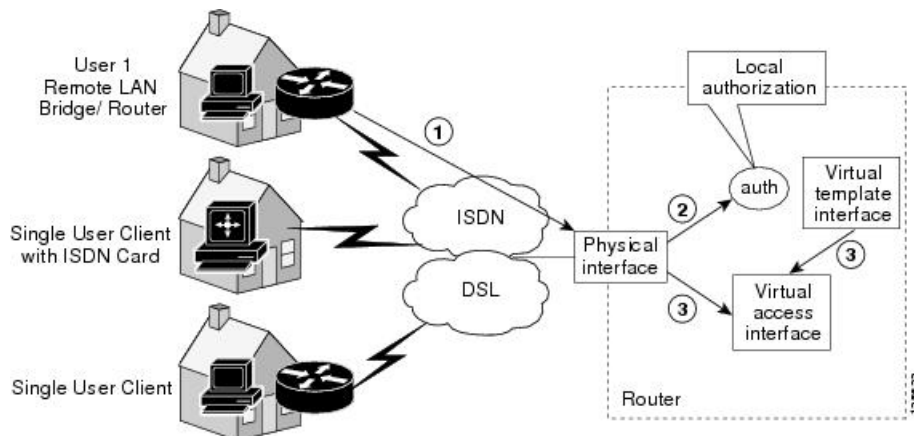
こともできます。DVTI は、標準ベースです。そのため、複数のベンダー環境における相互運用性がサポートされます。IPsec DVTI を使用すれば、リモート アクセス VPN 用のセキュリティ保護が強化された接続を作成できます。また、Cisco Architecture for Voice, Video, and Integrated Data (AVVID) と組み合わせて、IP ネットワーク経由で集約された音声、ビデオ、およびデータを転送できます。DVTI は VPN ルーティングおよび転送 (VRF) 対応 IPsec の導入を容易にします。VRF は、インターフェイス上で設定されます。

DVTI には、ルータ上での最小限の設定が必要です。単一の仮想テンプレートを設定およびコピーできます。

DVTI によって、IPsec セッション用のインターフェイスが作成され、ダイナミック IPsec VTI の動的なインスタンス化および管理のための仮想テンプレートインフラストラクチャが使用されます。仮想テンプレートインフラストラクチャは、ダイナミック仮想アクセス トンネル インターフェイスを作成するために拡張されます。DVTI は、ハブアンドスポーク設定で使用されます。単一の DVTI で複数のスタティック VTI をサポートできます。

次の図に、DVTI 認証パスを示します。

図 2: ダイナミック IPsec VTI



上の図の認証は、次のパスに従います。

1. ユーザ 1 がルータを呼び出します。
2. ルータ 1 によって ユーザ 1 が認証されます。
3. IPsec によって、仮想テンプレート インターフェイスから仮想アクセス インターフェイスがコピーされます。

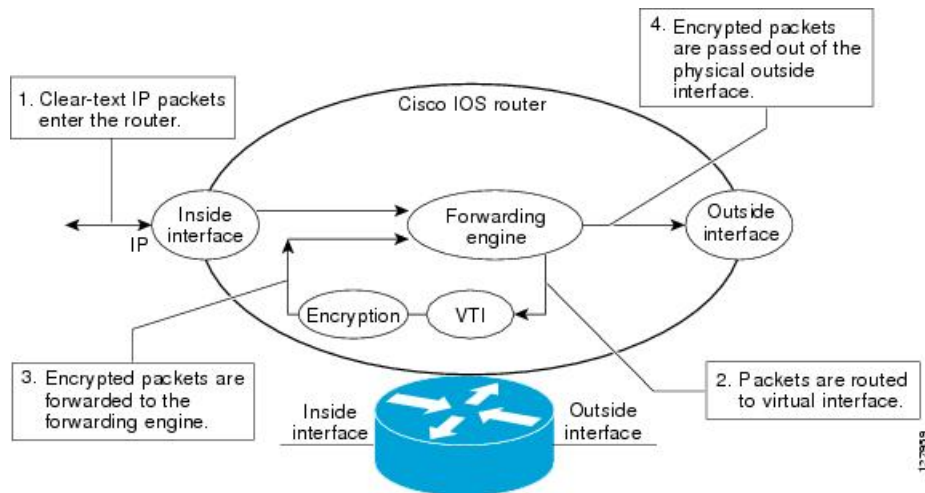
IPsec 仮想トンネル インターフェイスを使用したトラフィックの暗号化

IPsec VTI が設定されると、暗号化がトンネル内で実行されます。トラフィックがトンネル インターフェイスに転送されると、そのトラフィックが暗号化されます。トラフィックの転送は、IP ルーティングテーブルによって処理され、ダイナミックまたはスタティック ルーティ

ングを使用してトラフィックを SVTI にルーティングできます。DVTI では、逆ルート注入が使用されるので、ルーティングの設定がさらに簡単になっています。IP ルーティングを使用してトラフィックを暗号化に転送すると、IPsec VPN 設定が簡単になります。さらに、IPsec 仮想トンネルを使用すれば、IPsec によってマルチキャストトラフィックを暗号化できます。

次の図に、IPsec トンネルへの IPsec パケット フローを示します。

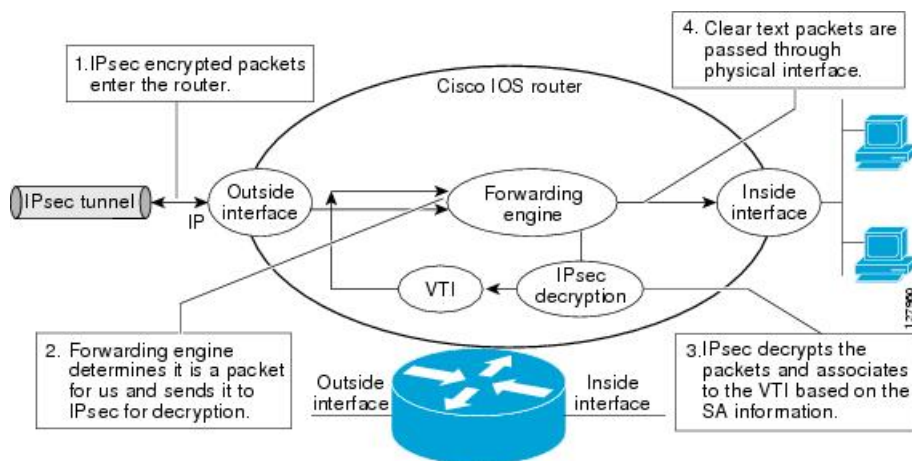
図 3: IPsec トンネルへのパケット フロー



パケットが内部インターフェイスに到着すると、転送エンジンによってパケットが VTI にスイッチングされ、そこで暗号化されます。暗号化されたパケットは転送エンジンに戻され、そこで外部インターフェイスを介してスイッチングされます。

次の図に、IPsec トンネルからのパケット フローを示します。

図 4: IPsec トンネルからのパケット フロー



ダイナミック仮想トンネル インターフェイスのライフサイクル

IPsec プロファイルによって、DVTI のポリシーが定義されます。ダイナミック インターフェイスが、IKE フェーズ 1 および IKE フェーズ 1.5 の終了時に作成されます。ピアに対する IPsec セッションが終了すると、インターフェイスが削除されます。ピアに対する IKE と IPsec SA の両方が削除されると、IPsec セッションが終了します。

IPsec 仮想トンネル インターフェイスを使用したルーティング

VTI はルーティング可能なインターフェイスなので、暗号化プロセスにおけるルーティングの役割は重要です。トラフィックは、VTI の外に転送される場合にだけ暗号化され、VTI に到着するトラフィックは、適宜、復号化およびルーティングされます。VTI を利用すれば、実際のインターフェイスをトンネルエンドポイントとして使用することによって、暗号化トンネルを確立できます。インターフェイスにルーティングしたり、QoS、ファイアウォール、ネットワーク アドレス変換 (NAT)、Netflow 統計情報などのサービスを必要に応じて他のインターフェイスに適用したりできます。インターフェイスをモニタして、それにルーティングできます。このインターフェイスは他の Cisco IOS インターフェイスと同様のメリットを提供します。

FlexVPN 混合モードのサポート

FlexVPN 混合モード機能は、IPsec IPv6 トランスポート経由の IPv4 トラフィックの伝送をサポートします。これは、IPsec スタック上でのデュアル スタックのサポートにつながる第 1 段階です。この実装は、IPv4 トラフィックと IPv6 トラフィックの両方に対する単一の IPsec セキュリティ アソシエーション (SA) ペアの使用をサポートしません。

この機能は、IKEv2 とダイナミック VTI を使用したリモート アクセス VPN に対してのみサポートされます。

FlexVPN 混合モード機能は、Cisco IOS XE Everest 16.4.1 からの IPsec IPv4 トランスポート経由の IPv6 トラフィック伝送をサポートします。

IPsec での自動トンネル モードのサポート

複数ベンダー シナリオで VPN ヘッドエンドを設定する場合は、ピアまたはレスポンドの技術的な詳細を認識しておく必要があります。たとえば、一部のデバイスは IPsec トンネルを使用しているが、他のデバイスは Generic Routing Encapsulation (GRE) または IPsec トンネルを使用している場合やトンネルが IPv4 または IPv6 の場合があります。最後のケースでは、インターネットキーエクスチェンジ (IKE) プロファイルと仮想テンプレートを設定する必要があります。

トンネルモード自動選択機能は、設定を容易にし、レスポンドの詳細の入手を支援します。この機能は、IKE プロファイルから仮想アクセスインターフェイスが作成されるとすぐに、トンネリング プロトコル (GRE または IPsec) とトランスポート プロトコル (IPv4 または IPv6) を自動的に仮想テンプレートに適用します。この機能は、Cisco AnyConnect VPN Client や Microsoft Windows 7 Client などのマルチベンダー リモート アクセスを集約しているデュアルスタック ハブ上で役に立ちます。



(注) トンネル モード自動選択機能は、レスポндаの設定のみを容易にします。トンネルはイニシエータに対して静的に設定する必要があります。

VTI に対する IPSec 混合モードのサポート

IPSec 混合モード機能は、IPsec IPv6 トランスポート経由の IPv4 トラフィックの伝送をサポートします。これは、IPsec スタック上でのデュアル スタックのサポートにつながる第 1 段階です。この実装は、IPv4 トラフィックと IPv6 トラフィックの両方に対する単一の IPSec セキュリティ アソシエーション (SA) ペアの使用をサポートしません。

この機能は、SVTI、DVTI、IKEv1、および IKEv2 でサポートされます。

IPsec 仮想トンネル インターフェイスの設定方法

スタティック IPsec 仮想トンネル インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto IPsec profile** *profile-name*
4. **set transform-set** *transform-set-name* [*transform-set-name2*...*transform-set-name6*]
5. **exit**
6. **interface** *type number*
7. **ip address** *address mask*
8. **tunnel mode ipsec ipv4**
9. **tunnel source** *interface-type interface-number*
10. **tunnel destination** *ip-address*
11. **tunnel protection IPsec profile** *profile-name*
12. **end**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル構成モードを開始します。
ステップ 3	crypto IPsec profile profile-name 例 : Device(config)# crypto IPsec profile PROF	2 つの IPsec デバイス間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec プロファイル コンフィギュレーション モードを開始します。
ステップ 4	set transform-set transform-set-name [transform-set-name2...transform-set-name6] 例 : Device(ipsec-profile)# set transform-set tset	使用可能なトランスフォームセットを指定します。
ステップ 5	exit 例 : Device(ipsec-profile)# exit	IPsec プロファイル コンフィギュレーション モードを終了して、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 6	interface type number 例 : Device(config)# interface tunnel 0	トンネル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 7	ip address address mask 例 : Device(config-if)# ip address 10.1.1.1 255.255.255.0	IP アドレスおよびマスクを指定します。
ステップ 8	tunnel mode ipsec ipv4 例 : Device(config-if)# tunnel mode ipsec ipv4	トンネルのモードを定義します。
ステップ 9	tunnel source interface-type interface-number 例 : Device(config-if)# tunnel source loopback 0	トンネルの送信元をループバック インターフェイスとして指定します。*  (注) * 仮想テンプレートを使用してトンネルを作成する場合は、<code>virtual-template number type tunnel</code> コマンドでトンネル送信元とトンネルモードを指定する必要があります。クライアントは接続に失敗します。

	コマンドまたはアクション	目的
ステップ 10	tunnel destination ip-address 例 : Device(config-if)# tunnel destination 172.16.1.1	トンネルの宛先の IP アドレスを指定します。
ステップ 11	tunnel protection IPsec profile profile-name 例 : Device(config-if)# tunnel protection IPsec profile PROF	トンネルインターフェイスを IPsec プロファイルに関連付けます。
ステップ 12	end 例 : Device(config-if)# end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPsec 仮想トンネルインターフェイスを介した BGP の設定

必要に応じて、2つのルータの仮想トンネルインターフェイスを介してBGPを設定するには、次の作業を実行します。

始める前に

[スタティック IPsec 仮想トンネルインターフェイスの設定 \(47 ページ\)](#) の手順を実行します。

手順の概要

1. **router bgp autonomous-system-number**
2. **neighbor ip-address remote-as autonomous-system-number**
3. **network network-ip-address mask subnet-mask**
4. **exit**
5. 2 番目のルータで次のコマンドを入力します。
6. **router bgp autonomous-system-number**
7. **neighbor ip-address remote-as autonomous-system-number**
8. **network network-ip-address mask subnet-mask**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	router bgp autonomous-system-number 例 :	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。

	コマンドまたはアクション	目的
	Device(config)# router bgp 65510	autonomous-system-number : 他の BGP ルータに対するルータを指定し、同時に渡されるルーティング情報のタギングをする自律システムの番号。番号の範囲は 1 ～ 65535 です。 この例では、この手順の最初のルータは「65510」として識別されます。
ステップ 2	neighbor ip-address remote-as autonomous-system-number 例 : <pre>Device(config-router)# neighbor 10.1.1.2 remote-as 65511</pre>	ip-address : 隣接ルータのトンネルインターフェイスの IP アドレス。 autonomous-system-number : 2 番目のルータのルータを識別する自律システムの番号。番号の範囲は 1 ～ 65535 です。
ステップ 3	network network-ip-address mask subnet-mask 例 : <pre>Device(config-router)# network 2.2.2.0 mask 255.255.255.0</pre>	network-ip-address : BGP でアドバタイズされるネットワークの IP アドレス。たとえば、ループバック インターフェイスの IP アドレスです。 subnet-mask : BGP でアドバタイズされるネットワークのサブネットマスク。  (注) BGP ネットワークコマンドの network アドバタイズされるように、ルーティングする必要がある。これは、network コマンドで指定するだけで、インターフェイスに OSPF とは異なります。
ステップ 4	exit 例 : <pre>Device(config-router)# exit</pre>	ルータ コンフィギュレーション モードを終了します。
ステップ 5	2 番目のルータで次のコマンドを入力します。	
ステップ 6	router bgp autonomous-system-number 例 : <pre>Device(config)# router bgp 65511</pre>	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。 autonomous-system-number : 他の BGP ルータに対するルータを指定し、同時に渡されるルーティング情報のタギングをする自律システムの番号。番号の範囲は 1 ～ 65535 です。 この例では、この手順の 2 番目のルータは「65511」として識別されます。

	コマンドまたはアクション	目的
ステップ 7	neighbor ip-address remote-as autonomous-system-number 例 : Device(config-router)# neighbor 10.1.1.1 remote-as 65510	ip-address : 隣接ルータのトンネルインターフェイスの IP アドレス。
ステップ 8	network network-ip-address mask subnet-mask 例 : Device(config-router)# network 1.1.1.0 mask 255.255.255.0	network-ip-address : BGP でアドバタイズされるネットワークの IP アドレス。たとえば、ループバック インターフェイスの IP アドレスです。 subnet-mask : BGP でアドバタイズされるネットワークのサブネットマスク。



(注) 正確なネットワーク IP アドレス

ダイナミック IPsec 仮想トンネル インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile profile-name**
4. **set transform-set transform-set-name [transform-set-name2...transform-set-name6]**
5. **exit**
6. **interface virtual-template number type tunnel**
7. **tunnel mode ipsec ipv4**
8. **tunnel protection IPsec profile profile-name**
9. **exit**
10. **crypto isakamp profile profile-name**
11. **match identity address ip-address mask**
12. **virtual template template-number**
13. **end**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 :	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	Device> enable	プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル構成モードを開始します。
ステップ 3	crypto ipsec profile profile-name 例 : Device(config)# crypto ipsec profile PROF	2 つの IPSec デバイス間の IPSec 暗号化に使用される IPSec パラメータを定義して、IPsec プロファイル コンフィギュレーション モードを開始します。
ステップ 4	set transform-set transform-set-name [transform-set-name2...transform-set-name6] 例 : Device(ipsec-profile)# set transform-set tset	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。
ステップ 5	exit 例 : Device(ipsec-profile)# exit	IPsec プロファイル コンフィギュレーション モードを終了して、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 6	interface virtual-template number type tunnel 例 : Device(config)# interface virtual-template 2 type tunnel	仮想テンプレート トンネル インターフェイスを定義し、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 7	tunnel mode ipsec ipv4 例 : Device(config-if)# tunnel mode ipsec ipv4	トンネルのモードを定義します。
ステップ 8	tunnel protection IPsec profile profile-name 例 : Device(config-if)# tunnel protection ipsec profile PROF	トンネルインターフェイスを IPsec プロファイルに関連付けます。
ステップ 9	exit 例 : Device(config-if)# exit	インターフェイス コンフィギュレーション モードを終了します。
ステップ 10	crypto isakamp profile profile-name 例 : Device(config)# crypto isakamp profile profile1	仮想テンプレートに使用される ISAKAMP プロファイルを定義します。

	コマンドまたはアクション	目的
ステップ 11	match identity address <i>ip-address mask</i> 例 : Device(conf-isa-prof)# match identity address 10.1.1.0 255.255.255.0	ISAKMP プロファイルからの ID を照合して、isakmp-profile コンフィギュレーション モードを開始します。
ステップ 12	virtual template <i>template-number</i> 例 : Device(config)# virtual-template 1	ISAKAMP プロファイルにアタッチされた仮想テンプレートを指定します。
ステップ 13	end 例 : Device(config)# end	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

IKEv1 を使用したダイナミック仮想トンネル インターフェイスのマルチ SA サポートの設定



- (注) セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『[Next Generation Encryption](#)』（NGE）ホワイト ペーパーを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **crypto keyring** *keyring-name*
7. **pre-shared-key** *address key key*
8. **exit**
9. **crypto isakmp profile** *profile-name*
10. **keyring** *keyring-name*
11. **match identity** *address mask*
12. **virtual-template** *template-number*
13. **exit**
14. **crypto ipsec transform-set** *transform-set-name transform1 [transform2] [transform3]*
15. **exit**
16. **crypto ipsec profile** *name*
17. **set security-policy limit** *maximum-limit*
18. **set transform-set** *transform-set-name [transform-set-name2 transform-set-name6]*

19. **exit**
20. **interface virtual-template** *number type tunnel*
21. **ip vrf forwarding** *vrf-name*
22. **ip unnumbered** *type number*
23. **tunnel mode ipsec ipv4**
24. **tunnel protection profile ipsec** *profile-name*
25. **end**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。
ステップ 2	configure terminal 例 : Device# 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	ip vrf <i>vrf-name</i> 例 : Device(config)# ip vrf VRF-100-1	VRF インスタンスを定義し、VRF 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	rd <i>route-distinguisher</i> 例 : Device(config-vrf)# rd 100:21	VRF のルーティング テーブルと転送テーブルを作成します。
ステップ 5	exit 例 : Device(config-vrf)# exit	VRF コンフィギュレーション モードを終了して、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 6	crypto keyring <i>keyring-name</i> 例 : Device(config)# crypto keyring cisco-100-1	暗号キーリングを定義し、キーリング コンフィギュレーション モードを開始します。
ステップ 7	pre-shared-key <i>address key key</i> 例 : Device(config-keyring)# pre-shared-key address 10.1.1.1 key cisco-100-1	インターネット キー エクスチェンジ (IKE) 認証に使用する事前共有キーを定義します。

	コマンドまたはアクション	目的
ステップ 8	exit 例 : Device(config-keyring)# exit	キーリング コンフィギュレーション モードを終了して、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 9	crypto isakmp profile profile-name 例 : Device(config)# crypto isakmp profile cisco-isakmp-profile-100-1	ISAKMP プロファイルを定義し、ISAKMP コンフィギュレーション モードを開始します。
ステップ 10	keyring keyring-name 例 : Device(conf-isa-prof)# keyring cisco-100-1	ISAKMP モードでキーリングを設定します。
ステップ 11	match identity address mask 例 : Device(conf-isa-prof)# match identity address 10.1.1.0 255.255.255.0	ISAKMP プロファイルからの ID を照合します。
ステップ 12	virtual-template template-number 例 : Device(conf-isa-prof)# virtual-template 101	仮想アクセス インターフェイスの複製に使用される仮想テンプレートを指定します。
ステップ 13	exit 例 : Device(conf-isa-prof)# exit	ISAKMP プロファイル コンフィギュレーション モードを終了して、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 14	crypto ipsec transform-set transform-set-name transform1 [transform2] [transform3] 例 : Device(config)# crypto ipsec transform-set cisco esp-aes esp-sha-hmac	トランスフォーム セットを定義し、暗号トランスフォーム コンフィギュレーション モードを開始します。
ステップ 15	exit 例 : Device(conf-crypto-trans)# exit	クリプト トランスフォーム コンフィギュレーション モードを終了して、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 16	crypto ipsec profile name 例 : Device(config)# crypto ipsec profile cisco-ipsec-profile-101	2 つの IPsec デバイス間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec プロファイル コンフィギュレーション モードを開始します。
ステップ 17	set security-policy limit maximum-limit 例 : Device(ipsec-profile)# set security-policy limit 3	仮想アクセス インターフェイスごとに作成可能なフロー数の上限を定義します。

	コマンドまたはアクション	目的
ステップ 18	set transform-set transform-set-name [transform-set-name2 transform-set-name6] 例 : Device(ipsec-profile)# set transform-set cisco	クリプト マップ エントリで使用されるトランスフォーム セットを指定します。
ステップ 19	exit 例 : Device(ipsec-profile)# exit	IPsec プロファイル コンフィギュレーション モードを終了して、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 20	interface virtual-template number type tunnel 例 : Device(config)# interface virtual-template 101 type tunnel	インターフェイスを設定可能な仮想テンプレート インターフェイスを作成し、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 21	ip vrf forwarding vrf-name 例 : Device(config-if)# ip vrf forwarding VRF-100-1	VRF インスタンスと仮想テンプレート インターフェイスを関連付けます。
ステップ 22	ip unnumbered type number 例 : Device(config-if)# ip unnumbered GigabitEthernet 0.0	明示的な IP アドレスをインターフェイスに割り当てずにインターフェイス上の IP 処理をイネーブルにします。
ステップ 23	tunnel mode ipsec ipv4 例 : Device(config-if)# tunnel mode ipsec ipv4	トンネルのモードを定義します。
ステップ 24	tunnel protection profile ipsec profile-name 例 : Device(config-if)# tunnel protection ipsec profile PROF	トンネル インターフェイスを IPsec プロファイルに関連付けます。
ステップ 25	end 例 : Device(config-if)# end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SVTI に対する IPsec 混合モードのサポートの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto IPsec profile profile-name**

4. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
5. **exit**
6. **interface** *type number*
7. **ip address** *address mask*
8. 次のいずれかを実行します。
 - **tunnel mode ipsec ipv4 v6-overlay**
 - **tunnel mode ipsec ipv6 v4-overlay**
9. **tunnel source** *interface-type interface-type*
10. **tunnel destination** *ip-address*
11. **tunnel protection IPsec profile** *profile-name*
12. **end**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル構成モードを開始します。
ステップ 3	crypto IPsec profile <i>profile-name</i> 例 : Device(config)# crypto IPsec profile PROF	2 つの IPsec デバイス間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec プロファイル コンフィギュレーション モードを開始します。
ステップ 4	set transform-set <i>transform-set-name</i> [<i>transform-set-name2...transform-set-name6</i>] 例 : Device(ipsec-profile)# set transform-set tset	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。
ステップ 5	exit 例 : Device(ipsec-profile)# exit	IPsec プロファイル コンフィギュレーション モードを終了して、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。

	コマンドまたはアクション	目的
ステップ 6	interface <i>type number</i> 例 : Device(config)# interface tunnel 0	トンネル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 7	ip address <i>address mask</i> 例 : Device(config-if)# ip address 10.1.1.1 255.255.255.0	IP アドレスおよびマスクを指定します。
ステップ 8	次のいずれかを実行します。 • tunnel mode ipsec ipv4 v6-overlay • tunnel mode ipsec ipv6 v4-overlay 例 : Device(config-if)# tunnel mode ipsec ipv4 v6-overlay	トンネルのモードを定義します。
ステップ 9	tunnel source <i>interface-type interface-type</i> 例 : Device(config-if)# tunnel source loopback 0	トンネルの送信元をループバック インターフェイスとして指定します。
ステップ 10	tunnel destination <i>ip-address</i> 例 : Device(config-if)# tunnel destination 172.16.1.1	トンネルの宛先の IP アドレスを指定します。
ステップ 11	tunnel protection IPsec profile <i>profile-name</i> 例 : Device(config-if)# tunnel protection IPsec profile PROF	トンネルインターフェイスを IPsec プロファイルに関連付けます。
ステップ 12	end 例 : Device(config-if)# end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ダイナミック VTI に対する IPSec 混合モードのサポートの設定

手順の概要

1. **enable**
2. **configure terminal**

3. **crypto ipsec profile** *profile-name*
4. **set mixed mode**
5. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
6. **exit**
7. **interface virtual-template** *number* **type tunnel**
8. **tunnel mode ipsec ipv4**
9. **tunnel protection IPsec profile** *profile-name*
10. **exit**
11. **crypto isakamp profile** *profile-name*
12. **match identity address** *ip-address mask*
13. **virtual template** *template-number*
14. **end**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル構成モードを開始します。
ステップ 3	crypto ipsec profile <i>profile-name</i> 例 : Device(config)# crypto ipsec profile PROF	2 つの IPsec デバイス間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec プロファイル コンフィギュレーションモードを開始します。
ステップ 4	set mixed mode 例 : Device(config)# set mixed mode	2 つの IPsec デバイス間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec プロファイル コンフィギュレーションモードを開始します。
ステップ 5	set transform-set <i>transform-set-name</i> [<i>transform-set-name2...transform-set-name6</i>] 例 : Device(ipsec-profile)# set transform-set tset	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。
ステップ 6	exit 例 : Device(ipsec-profile)# exit	IPsec プロファイル コンフィギュレーションモードを終了して、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。

	コマンドまたはアクション	目的
ステップ 7	interface virtual-template number type tunnel 例 : Device(config)# interface virtual-template 2 type tunnel	仮想テンプレート トンネル インターフェイスを定義し、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 8	tunnel mode ipsec ipv4 例 : Device(config-if)# tunnel mode ipsec ipv4	トンネルのモードを定義します。
ステップ 9	tunnel protection IPsec profile profile-name 例 : Device(config-if)# tunnel protection ipsec profile PROF	トンネルインターフェイスを IPsec プロファイルに関連付けます。
ステップ 10	exit 例 : Device(config-if)# exit	インターフェイス コンフィギュレーション モードを終了します。
ステップ 11	crypto isakamp profile profile-name 例 : Device(config)# crypto isakamp profile profile1	仮想テンプレートに使用される ISAKAMP プロファイルを定義します。
ステップ 12	match identity address ip-address mask 例 : Device(conf-isa-prof)# match identity address 10.1.1.0 255.255.255.0	ISAKMP プロファイルからの ID を照合して、isakmp-profile コンフィギュレーション モードを開始します。
ステップ 13	virtual template template-number 例 : Device(config)# virtual-template 1	ISAKAMP プロファイルにアタッチされた仮想テンプレートを指定します。
ステップ 14	end 例 : Device(config)# end	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

スタティック IPsec 仮想トンネルインターフェイスのマルチ SA サポートの設定

手順

ステップ 1 enable

例 :

```
Device> enable
```

特権 EXEC モードを有効にします。プロンプトが表示されたら、パスワードを入力します。

ステップ 2 **configure terminal**

例 :

```
Device# configure terminal
```

グローバル構成モードを開始します。

ステップ 3 **crypto IPsec profile profile-name**

例 :

```
Device(config)# crypto IPsec profile PROF
```

2 つの IPsec デバイス間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec プロファイル コンフィギュレーション モードを開始します。

ステップ 4 **set transform-set transform-set-name [transform-set-name2...transform-set-name6]**

例 :

```
Device(ipsec-profile)# set transform-set tset
```

使用可能なトランスフォームセットを指定します。

ステップ 5 **exit**

例 :

```
Device(ipsec-profile)# exit
```

IPsec プロファイル コンフィギュレーション モードを終了して、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 6 **interface type number**

例 :

```
Device(config)# interface tunnel 0
```

トンネル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 7 **ip address address mask**

例 :

```
Device(config-if)# ip address 10.1.1.1 255.255.255.0
```

IP アドレスおよびマスクを指定します。

ステップ 8 **tunnel mode ipsec {ipv4 | ipv6}**

例 :

```
Device(config-if)# tunnel mode ipsec ipv4
```

トンネルのモードを定義します。

ステップ 9 **tunnel source interface-type interface-number**

例 :

```
Device(config-if)# tunnel source loopback 0
```

トンネルの送信元をループバック インターフェイスとして指定します。

ステップ 10 **tunnel destination ip-address**

例 :

```
Device(config-if)# tunnel destination 172.16.1.1
```

トンネルの宛先の IP アドレスを指定します。

ステップ 11 **tunnel protection ipsec policy {ipv4 | ipv6} acl**

例 :

```
Device(config-if)# tunnel protection ipsec policy ipv4 ipsec-acl1
```

ACL を SVTI に関連付けて、非 any-any トラフィックセクタを定義します。

ステップ 12 **tunnel protection ipsec profile profile-name**

例 :

```
Device(config-if)# tunnel protection IPsec profile PROF
```

トンネル インターフェイスを IPsec プロファイルに関連付けます。

ステップ 13 **exit**

例 :

```
Device(config-if)# exit
```

インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。

ステップ 14 **ip access-list extended name** または **ipv6 access-list name**

例 :

IPv4 :

```
Device(config)# ip access-list extended ipsec-acl1
```

IPv6

```
Device(config)# ipv6 access-list ipsec-acl1
```

名前を使用して拡張 IP アクセス リストを定義し、拡張名前付きアクセス リストのコンフィギュレーション モードを開始します。

ステップ 15 **permit protocol source [source-wildcard] destination [destination-wildcard] [option option-name]**

例 :

```
Device(config-ext-nacl)# permit ip 30.0.1.0 0.0.0.255 10.0.1.0 0.0.0.255
```

ステートメントに指定されたすべての条件に一致するトラフィックを許可します。

送信元プロキシと宛先プロキシの両方にキーワード **any** をワイルドカードとして使用しないでください。
「any any」トラフィックセレクタの場合は、ACL が関連付けられていないデフォルトの SVTI を使用します。

deny ステートメントは使用しないでください。

ステップ 16 **end**

例 :

```
Device(config-ext-nacl)# end
```

標準の名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

デュアルオーバーレイとしてのトンネルモードの設定

トンネルモードをデュアルオーバーレイとして設定するには、次の手順を実行します。

手順

ステップ 1 **enable**

例 :

```
Device> enable
```

特権 EXEC モードを有効にします。プロンプトが表示されたら、パスワードを入力します。

ステップ 2 **configure terminal**

例 :

```
Device# configure terminal
```

グローバル構成モードを開始します。

ステップ 3 **interface tunnel type number**

例 :

```
Device(config)# interface tunnel 1
```

トンネルインターフェイスおよび番号を指定し、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 **ipv6 enable**

例 :

```
Device(config-if)# ipv6 enable
```

明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。

ステップ 5 **tunnel source { ipv4-address | interface-type | interface-number }**

例：

```
Device(config-if)# tunnel source Gigabitethernet 1
```

送信元 IPv6 アドレスまたは送信元インターフェイス タイプおよびトンネル インターフェイスの番号を指定します。インターフェイスのタイプと番号が指定されている場合、そのインターフェイスは IPv6 アドレスを使用して設定する必要があります。

ステップ 6 **tunnel mode ipsec dual-overlay**

例：

```
Device(config-if)# tunnel mode ipsec dual-overlay
```

デュアルオーバーレイ トンネルを指定します。**tunnel mode ipsec dual-overlay** コマンドは、トンネルのカプセル化プロトコルを指定します。

ステップ 7 **tunnel destination ip address address mask**

例：

```
Device(config-if)# tunnel destination 89.89.89.1 255.255.255.255.0
```

トンネル インターフェイスの宛先 IPv6 アドレスを指定します。

ステップ 8 **tunnel protection ipsec profile ipsec profile-name**

例：

```
Device(config-if)# tunnel protection IPsec profile ipsecprof
```

トンネル インターフェイスを IPsec プロファイルに関連付けます。*name* 引数には、IPsec プロファイルの名前を指定します。この値は、**crypto IPsec profile name** コマンドで指定した *name* と一致する必要があります。

ステップ 9 **exit**

例：

```
Device(config-if)# exit
```

インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。

ステップ 10 **end**

例：

```
Device(config-if)# end
```

インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPsec 仮想トンネル インターフェイスの設定例

例：IPsec を使用したスタティック仮想トンネル インターフェイス

次の設定例では、ピア間の認証用に事前共有キーが使用されています。VPN トラフィックは、暗号化のために IPsec VTI に転送されてから、物理インターフェイスに送信されます。サブネット 10 のトンネルでは、IPsec ポリシーに関してパケットがチェックされ、IPsec 暗号化のために暗号エンジン（CE）に渡されます。次の図に、IPsec VTI 設定を示しています。

図 5: IPsec を使用した VTI

ルータのコンフィギュレーション

```
version 12.3
service timestamps debug datetime
service timestamps log datetime
hostname 7200-3
no aaa new-model
ip subnet-zero
ip cef
controller ISA 6/1
!
crypto isakmp policy 1
encr aes
authentication pre-share
group 14
crypto isakmp key Cisco12345 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set T1 esp-aes esp-sha-hmac
crypto ipsec profile P1
set transform-set T1
!
interface Tunnel0
 ip address 10.0.51.203 255.255.255.0

 load-interval 30
 tunnel source 10.0.149.203
 tunnel destination 10.0.149.217
 tunnel mode IPsec ipv4
 tunnel protection IPsec profile P1
!

 ip address 10.0.149.203 255.255.255.0
 duplex full
!

 ip address 10.0.35.203 255.255.255.0
 duplex full
!
ip classless
ip route 10.0.36.0 255.255.255.0 Tunnel0
line con 0
line aux 0
line vty 0 4
end
```

ルータのコンフィギュレーション

```

version 12.3
hostname c1750-17
no aaa new-model
ip subnet-zero
ip cef
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 14
crypto isakmp key Cisco12345 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set T1 esp-aes esp-sha-hmac
crypto ipsec profile P1
  set transform-set T1
!
interface Tunnel0
  ip address 10.0.51.217 255.255.255.0

  tunnel source 10.0.149.217
  tunnel destination 10.0.149.203
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile P1
!
interface
  ip address 10.0.149.217 255.255.255.0
  speed 100
  full-duplex
!
interface
  ip address 10.0.36.217 255.255.255.0
  load-interval 30
  full-duplex
!
ip classless
ip route 10.0.35.0 255.255.255.0 Tunnel0
line con 0
line aux 0
line vty 0 4
end

```

例 : IPsec スタティック仮想トンネル インターフェイスの結果の確認

ここでは、設定が正しく動作しているか確認するうえで利用可能な情報を示します。次の出力では、Tunnel 0 およびラインプロトコルが「up」状態です。ラインプロトコルが「down」状態の場合、セッションは非アクティブです。

IPsec スタティック仮想トンネル インターフェイスの確認

```

Router# show interface tunnel 0

Tunnel0 is up, line protocol is up
Hardware is Tunnel
Internet address is 10.0.51.203/24
MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
reliability 255/255, txload 103/255, rxload 110/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.0.149.203, destination 10.0.149.217
Tunnel protocol/transport ipsec/ip, key disabled, sequencing disabled

```

```

Tunnel TTL 255
Checksumming of packets disabled, fast tunneling enabled
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Tunnel protection via IPsec (profile "P1")
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 1/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
30 second input rate 13000 bits/sec, 34 packets/sec
30 second output rate 36000 bits/sec, 34 packets/sec
191320 packets input, 30129126 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
59968 packets output, 15369696 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out

Router# show crypto session

Crypto session current status
Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.149.217 port 500
IKE SA: local 10.0.149.203/500 remote 10.0.149.217/500 Active
IPsec FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 4,
Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.0.35.0/24 is directly connected, Ethernet3/3
S 10.0.36.0/24 is directly connected, Tunnel0
C 10.0.51.0/24 is directly connected, Tunnel0
C 10.0.149.0/24 is directly connected, Ethernet3/0

```

例：VRF 認識スタティック仮想トンネル インターフェイス

VRF をスタティック VTI の例に追加するには、次の例で示すように、**ipvrf** コマンドおよび **ip vrf forwarding** コマンドを設定に含めます。

C8000 ルータ設定

```

hostname c8000
.
.
ip vrf sample-vti1
rd 1:1
route-target export 1:1
route-target import 1:1
!
.

```

例：QoS を使用したスタティック仮想トンネル インターフェイス

```
.
interface Tunnel0
 ip vrf forwarding sample-vti1
 ip address 10.0.51.217 255.255.255.0
 tunnel source 10.0.149.217
 tunnel destination 10.0.149.203
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile P1
.
.
!
```

```
end
```

例：QoS を使用したスタティック仮想トンネル インターフェイス

トンネルインターフェイスの下に **service-policy** ステートメントを指定することによって、QoS ポリシーをトンネルエンドポイントに適用できます。次に、トンネルインターフェイスからトラフィックをポリシングする例を示します。

C8000 ルータ設定

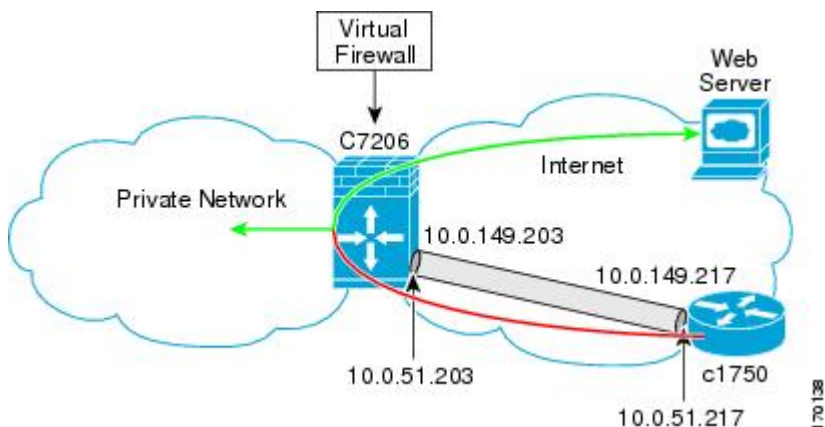
```
hostname c8000
.
.
class-map match-all VTI
 match any
!
policy-map VTI
 class VTI
  police cir 2000000
   conform-action transmit
   exceed-action drop
!
.
.
interface Tunnel0
 ip address 10.0.51.217 255.255.255.0
 tunnel source 10.0.149.217
 tunnel destination 10.0.149.203
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile P1
 service-policy output VTI
!
.
.
!
```

```
end
```

例：仮想ファイアウォールを使用したスタティック仮想トンネルインターフェイス

仮想ファイアウォールを SVTI トンネルに適用することによって、スポークからのトラフィックを、ハブを通過させてインターネットに送信できます。次の図に、企業ファイアウォールによって本質的に保護されているスポークを使用した SVTI を示します。

図 6: 仮想ファイアウォールを使用したスタティック VTI



SVTI の基本設定は、仮想ファイアウォール定義を含むように変更されています。

C8000 ルータ設定

```
hostname c8000
.
.
ip inspect max-incomplete high 1000000
ip inspect max-incomplete low 800000
ip inspect one-minute high 1000000
ip inspect one-minute low 800000
ip inspect tcp synwait-time 60
ip inspect tcp max-incomplete host 100000 block-time 2
ip inspect name IOSFW1 tcp timeout 300
ip inspect name IOSFW1 udp
!
.
.
interface GigabitEthernet0/1
description Internet Connection
ip address 172.18.143.246 255.255.255.0
ip access-group 100 in
ip nat outside
!
interface Tunnel0
ip address 10.0.51.217 255.255.255.0
ip nat inside
ip inspect IOSFW1 in
tunnel source 10.0.149.217
tunnel destination 10.0.149.203
tunnel mode ipsec ipv4
tunnel protection ipsec profile P1
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
ip nat translation timeout 120
ip nat translation finrst-timeout 2
ip nat translation max-entries 300000
ip nat pool test1 10.2.100.1 10.2.100.50 netmask 255.255.255.0
ip nat inside source list 110 pool test1 vrf test-vtil overload
!
access-list 100 permit esp any any
```

```

access-list 100 permit udp any eq isakmp any
access-list 100 permit udp any eq non500-isakmp any
access-list 100 permit icmp any any
access-list 110 deny    esp any any
access-list 110 deny    udp any eq isakmp any
access-list 110 permit ip any any
access-list 110 deny    udp any eq non500-isakmp any
!
end

```

例：ダイナミック仮想トンネル インターフェイス Easy VPN サーバ

次に、DVTI Easy VPN サーバを使用する例を示します。このサーバは、IPsec リモート アクセス アグリゲータになります。クライアントは、Cisco VPN Client を実行しているホームユーザにすることも、Easy VPN クライアントとして設定された Cisco IOS ルータにすることもできます。

C8000 ルータ設定

```

hostname c8000
!
aaa new-model
aaa authentication login local_list local
aaa authorization network local_list local
aaa session-id common
!
ip subnet-zero
ip cef
!
username cisco password 0 cisco123
!
controller ISA 1/1
!
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 14
!
crypto isakmp client configuration group group1
  key cisco123
  pool group1pool
  save-password
!
crypto isakmp profile vpn1-ra
  match identity group group1
  client authentication list local_list
  isakmp authorization list local_list
  client configuration address respond
  virtual-template 1
!
crypto ipsec transform-set VTI-TS esp-aes esp-sha-hmac
!
crypto ipsec profile test-vti1
  set transform-set VTI-TS
!
interface GigabitEthernet0/1
  description Internet Connection
  ip address 172.18.143.246 255.255.255.0
!

```

```

interface GigabitEthernet0/2
  description Internal Network
  ip address 10.2.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
  ip unnumbered GigabitEthernet0/1
  ip virtual-reassembly
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile test-vti1
!
ip local pool group1pool 192.168.1.1 192.168.1.4
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
end

```

例：ダイナミック仮想トンネル インターフェイス Easy VPN サーバの結果の確認

次に、DVTI が、Easy VPN サーバ用に設定されている例を示します。

```

Router# show running-config interface Virtual-Access2

Building configuration...
Current configuration : 250 bytes
!
interface Virtual-Access2
  ip unnumbered GigabitEthernet0/1
  ip virtual-reassembly
  tunnel source 172.18.143.246
  tunnel destination 172.18.143.208
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile test-vti1
  no tunnel protection ipsec initiate
end
Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.2.1.10 to network 0.0.0.0
 172.18.0.0/24 is subnetted, 1 subnets
C       172.18.143.0 is directly connected, GigabitEthernet0/1
 192.168.1.0/32 is subnetted, 1 subnets
S       192.168.1.1 [1/0] via 0.0.0.0, Virtual-Access2
 10.0.0.0/24 is subnetted, 1 subnets
C       10.2.1.0 is directly connected, GigabitEthernet0/2
S*    0.0.0.0/0 [1/0] via 172.18.143.1

```

例：VRF が仮想テンプレートに基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPsec

次に、仮想テンプレートに基づいて DVTI を利用するように VRF 認識 IPsec を設定する例を示します。

例：VRF が仮想テンプレートと IPsec プロファイル内のゲートウェイ オプションに基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPsec

```
hostname c8000
!
ip vrf VRF-100-1
  rd 1:1
!
ip vrf VRF-100-2
  rd 1:1
!
!
!
crypto keyring cisco-100-1
  pre-shared-key address 10.1.1.1 key cisco-100-1
crypto keyring cisco-100-2
  pre-shared-key address 10.1.2.1 key cisco-100-2
crypto isakmp profile cisco-isakmp-profile-100-1
  keyring cisco-100-1
  match identity address 10.1.1.0 255.255.255.0
  virtual-template 101
crypto isakmp profile cisco-isakmp-profile-100-2
  keyring cisco-100-2
  match identity address 10.1.2.0 255.255.255.0
  virtual-template 102
!
!
crypto ipsec transform-set cisco esp-aes esp-sha-hmac
!
crypto ipsec profile cisco-ipsec-profile-101
  set security-policy limit 3
  set transform-set cisco
!
crypto ipsec profile cisco-ipsec-profile-102
  set security-policy limit 5
  set transform-set Cisco
!
interface Virtual-Template101 type tunnel
  ip vrf forwarding VRF-100-1
  ip unnumbered Ethernet 0/0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile cisco-ipsec-profile-101
!
interface Virtual-Template102 type tunnel
  ip vrf forwarding VRF-100-2
  ip unnumbered Ethernet 0/0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile cisco-ipsec-profile-102
!
```

例：VRF が仮想テンプレートと IPsec プロファイル内のゲートウェイ オプションに基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPsec

次に、VRF が仮想テンプレートと IPsec プロファイル内のゲートウェイ オプションに基づいて設定されている場合に、DVTI を利用するように VRF 認識 IPsec を設定する例を示します。

```

hostname c8000
!
ip vrf VRF-100-1
  rd 1:1
!
ip vrf VRF-100-2
  rd 1:1
!
!
!
crypto keyring cisco-100-1
  pre-shared-key address 10.1.1.1 key cisco-100-1
crypto keyring cisco-100-2
  pre-shared-key address 10.1.2.1 key cisco-100-2
crypto isakmp profile cisco-isakmp-profile-100-1
  keyring cisco-100-1
  match identity address 10.1.1.0 255.255.255.0
  virtual-template 101
crypto isakmp profile cisco-isakmp-profile-100-2
  keyring cisco-100-2
  match identity address 10.1.2.0 255.255.255.0
  virtual-template 102
!
!
crypto ipsec transform-set cisco esp-3des esp-sha-hmac
!
crypto ipsec profile cisco-ipsec-profile-101
  set security-policy limit 3
  set transform-set cisco
  set reverse-route gateway 172.16.0.1
!
crypto ipsec profile cisco-ipsec-profile-102
  set security-policy limit 5
  set transform-set cisco
  set reverse-route gateway 172.16.0.1
!
interface Virtual-Template101 type tunnel
  ip vrf forwarding VRF-100-1
  ip unnumbered Ethernet 0/0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile cisco-ipsec-profile-101
!
interface Virtual-Template102 type tunnel
  ip vrf forwarding VRF-100-2
  ip unnumbered Ethernet 0/0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile cisco-ipsec-profile-102
!

```

例：VRF が ISAKMP プロファイルに基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPSec

```

hostname c8000
!
ip vrf VRF-100-1
  rd 1:1
!
ip vrf VRF-100-2
  rd 1:1

```

例：VRF が ISAKMP プロファイルと IPsec プロファイル内のゲートウェイ オプションに基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPsec

```

!
crypto keyring cisco-100-1
  pre-shared-key address 10.1.1.1 key cisco-100-1
crypto keyring cisco-100-2
  pre-shared-key address 10.1.2.1 key cisco-100-2
crypto isakmp profile cisco-isakmp-profile-100-1
  vrf VRF-100-1
  keyring cisco-100-1
  match identity address 10.1.1.0 255.255.255.0
  virtual-template 1
crypto isakmp profile cisco-isakmp-profile-100-2
  vrf VRF-100-2
  keyring cisco-100-2
  match identity address 10.1.2.0 255.255.255.0
  virtual-template 1
!
!
crypto ipsec transform-set cisco esp-aes esp-sha-hmac
crypto ipsec profile cisco-ipsec-profile
  set security-policy limit 3
  set transform-set cisco
!
!
!
interface Virtual-Template 1 type tunnel
  ip unnumbered ethernet 0/0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile cisco-ipsec-profile
!
!

```

例：VRF が ISAKMP プロファイルと IPsec プロファイル内のゲートウェイ オプションに基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPsec

次に、VRF が ISAKMP プロファイルと IPsec プロファイル内のゲートウェイ オプションに基づいて設定されている場合に、DVTI を利用するように VRF 認識 IPsec を設定する例を示します。

```

hostname C8000 server
!
ip vrf VRF-100-1
  rd 1:1
!
ip vrf VRF-100-2
  rd 1:1
!
crypto keyring cisco-100-1
  pre-shared-key address 10.1.1.1 key cisco-100-1
crypto keyring cisco-100-2
  pre-shared-key address 10.1.2.1 key cisco-100-2
crypto isakmp profile cisco-isakmp-profile-100-1
  vrf VRF-100-1
  keyring cisco-100-1
  match identity address 10.1.1.0 255.255.255.0

```

```

virtual-template 1
crypto isakmp profile cisco-isakmp-profile-100-2
vrf VRF-100-2
keyring cisco-100-2
match identity address 10.1.2.0 255.255.255.0
virtual-template 1
!
!
crypto ipsec transform-set cisco esp-3des esp-sha-hmac
crypto ipsec profile cisco-ipsec-profile
set security-policy limit 3
set transform-set cisco
set reverse-route gateway 172.16.0.1
!
!
!
interface Virtual-Template1 type tunnel
ip unnumbered Ethernet 0/0
tunnel mode ipsec ipv4
tunnel protection ipsec profile cisco-ipsec-profile
!
!

```

例：VRF が仮想テンプレートと ISAKMP プロファイルの両方に基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPSec



- (注) ISAKMP プロファイルと仮想テンプレートに基づいて別々の VRF が設定されている場合は、仮想テンプレートに基づいて設定された VRF が優先されます。この設定は推奨されません。

次に、VRF が仮想テンプレートと ISAKMP プロファイルの両方に基づいて設定されている場合に、DVTI を利用するように VRF 認識 IPSec を設定する例を示します。

```

hostname C8000 server
.
.
.
ip vrf test-vti2
rd 1:2
route-target export 1:1
route-target import 1:1
!
.
.
.
ip vrf test-vti1
rd 1:1
route-target export 1:1
route-target import 1:1
!
.
.
.

```

例：仮想ファイアウォールを使用したダイナミック仮想トンネル インターフェイス

```
crypto isakmp profile cisco-isakmp-profile
vrf test-vti2
keyring key
match identity address 10.1.1.0 255.255.255.0
!
.
.
.
interface Virtual-Template1 type tunnel
ip vrf forwarding test-vti1
ip unnumbered Loopback 0
ip virtual-reassembly
tunnel mode ipsec ipv4
tunnel protection ipsec profile test-vti1
!
.
.
.
end
```

例：仮想ファイアウォールを使用したダイナミック仮想トンネル インターフェイス

DVTIEasy VPN サーバは、仮想ファイアウォールの背後に設定できます。Behind-the-firewall 設定を使用すれば、ユーザはネットワークに入れますが、ネットワークファイアウォールは不正アクセスから保護されます。仮想ファイアウォールでは、コンテキストベースのアクセス コントロール (CBAC) と、インターネット インターフェイスおよび仮想テンプレートに対して適用される NAT が使用されます。

```
hostname c8000
.
.
ip inspect max-incomplete high 1000000
ip inspect max-incomplete low 800000
ip inspect one-minute high 1000000
ip inspect one-minute low 800000
ip inspect tcp synwait-time 60
ip inspect tcp max-incomplete host 100000 block-time 2
ip inspect name IOSFW1 tcp timeout 300
ip inspect name IOSFW1 udp
!
.
.
interface GigabitEthernet0/1
description Internet Connection
ip address 172.18.143.246 255.255.255.0
ip access-group 100 in
ip nat outside
!
interface GigabitEthernet0/2
description Internal Network
ip address 10.2.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
ip unnumbered Loopback0
ip nat inside
ip inspect IOSFW1 in
tunnel mode ipsec ipv4
```

```

    tunnel protection ipsec profile test-vti1
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
ip nat translation timeout 120
ip nat translation finrst-timeout 2
ip nat translation max-entries 300000
ip nat pool test1 10.2.100.1 10.2.100.50 netmask 255.255.255.0
ip nat inside source list 110 pool test1 vrf test-vti1 overload
!
access-list 100 permit esp any any
access-list 100 permit udp any eq isakmp any
access-list 100 permit udp any eq non500-isakmp any
access-list 100 permit icmp any any
access-list 110 deny esp any any
access-list 110 deny udp any eq isakmp any
access-list 110 permit ip any any
access-list 110 deny udp any eq non500-isakmp any
!
end

```

例：QoS を使用したダイナミック仮想トンネル インターフェイス

サービス ポリシーを仮想テンプレートに適用することによって、QoS を DVTI トンネルに追加できます。テンプレートを複製して仮想アクセス インターフェイスを作成した場合は、サービス ポリシーが仮想アクセス インターフェイスにも適用されます。次に、QoS が追加された DVTI 基本設定の例を示します。

```

hostname c8000
.
.
class-map match-all VTI
match any
!
policy-map VTI
class VTI
police cir 2000000
conform-action transmit
exceed-action drop
!
.
.
interface Virtual-Templat1 type tunnel
ip vrf forwarding test-vti1
ip unnumbered Loopback0
ip virtual-reassembly
tunnel mode ipsec ipv4
tunnel protection ipsec profile test-vti1
service-policy output VTI
!
.
.
!
end

```

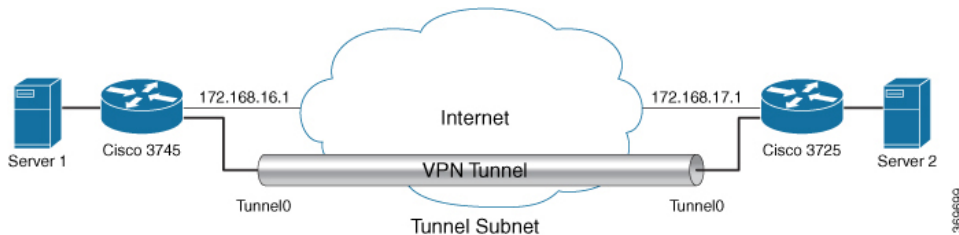
例：複数の IPsec SA を使用したスタティック仮想トンネルインターフェイス

例：複数の IPsec SA を使用したスタティック仮想トンネルインターフェイス

次の例では、SVTI を使用して Cisco 3745 と Cisco 3725 の 2 つのルータの間で IPSec トンネルを確立します。この設定では、非 any-any トラフィックセクタを使用し、複数の IPsec SA の形成を有効にします。

IPv4 トンネルモードのルータでの設定例：

次の図は、設定の参照トポロジを示しています。



Cisco 3745 ルータの設定例は、次のとおりです。

```
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp policy 5
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key example address 172.168.17.1
!
!
crypto ipsec transform-set svtil1 esp-3des esp-sha-hmac
 mode tunnel
!
!
crypto ipsec profile ipsec_prof
 set transform-set svtil1
!
!
interface Loopback0
 ip address 30.0.0.1 255.255.255.0
!
interface Loopback1
 ip address 50.0.0.1 255.255.255.0
!
interface Tunnel0
 ip address 11.1.1.2 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 172.168.17.1
 tunnel protection ipsec policy ipv4 ipsec_acl1
 tunnel protection ipsec profile ipsec_prof
!
interface Ethernet0/0
 ip address 172.168.16.1 255.255.255.0
!
```

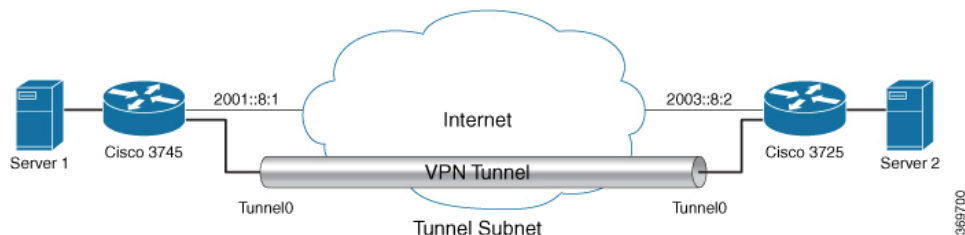
```

!
ip access-list extended ipsec_acl1
permit ip 30.0.0.0 0.0.0.255 40.0.0.0 0.0.0.255
permit ip 50.0.0.0 0.0.0.255 60.0.0.0 0.0.0.255

```

IPv6 トンネルモードのルータでの設定例：

次の図は、設定の参照トポロジを示しています。



Cisco 3745 ルータの設定例は、次のとおりです。

```

crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp policy 5
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key example address ipv6 2003::8:2/112
!
!
crypto ipsec transform-set svtil1 esp-3des esp-sha-hmac
 mode tunnel
!
!
crypto ipsec profile ipsec_prof
 set transform-set svtil1
!
!
!
interface Loopback0
 ipv6 address 2005::10:1/112
 ipv6 enable
!
interface Loopback1
 ipv6 address 2005::15:1/112
 ipv6 enable
!
interface Loopback2
 ipv6 address 2005::20:1/112
 ipv6 enable
!
interface Tunnel0
 ip address 11.1.1.2 255.255.255.0
 ipv6 address 400::10:1/112
 ipv6 enable
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv6
 tunnel destination 2003::8:2
 tunnel protection ipsec policy ipv6 ipsec_acl2
 tunnel protection ipsec profile ipsec_prof
!

```

例：デュアルオーバーレイとしてのトンネルモードの設定

```
interface Ethernet0/0
  ipv6 address 2001::8:1/112
  ipv6 enable
!
!
ipv6 access-list ipsec_acl2
sequence 10 permit ipv6 host 2005::10:1 host 2005::11:1
sequence 20 permit ipv6 host 2005::15:1 host 2005::16:1
sequence 30 permit ipv6 host 2005::20:1 host 2005::21:1
```

例：デュアルオーバーレイとしてのトンネルモードの設定

次に、トンネルモードをデュアルオーバーレイとして設定する例を示します。

```
Device# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ipv6 enable
Router(config-if)# tunnel source ethernet 0/0
Router(config-if)# tunnel mode ipsec dual-overlay
Router(config-if)# tunnel destination 89.89.89.1 255.255.255.255.0
Device(config-if)# tunnel protection IPsec profile ipsecprof
```

デュアルオーバーレイとしてのトンネルモードの設定の確認

次のコマンドを使用して、設定をトラブルシューティングします。

- **show crypto session [detail]**
- **show crypto ipsec sa**
- **show crypto map**
- **show crypto socket**
- **show crypto ikev2 session [detail]**

```
Device# show crypto map
Crypto Map: "Tunnel0-head-0" IKEv2 profile: prof

Crypto Map IPv4 "Tunnel0-head-0" 65536 ipsec-isakmp
  IKEv2 Profile: prof
  Profile name: prof
  Security association lifetime: 4608000 kilobytes/120 seconds
  Dualstack (Y/N): N

  Responder-Only (Y/N): N
  PFS (Y/N): N
  Mixed-mode : Disabled
  Transform sets={
    default: { esp-aes esp-sha-hmac } ,
  }

Crypto Map IPv4 "Tunnel0-head-0" 65537 ipsec-isakmp
  Map is a PROFILE INSTANCE.
  Peer = 10.10.10.2
  IKEv2 Profile: prof
  Extended IP access list
    access-list permit ip any any
  Current peer: 10.10.10.2
  Security association lifetime: 4608000 kilobytes/120 seconds
  Dualstack (Y/N): Y
```

```

TRUE ident (addr/mask/prot/port): {LOCAL -> REMOTE}
0.0.0.0/0.0.0.0/0/0 -> 0.0.0.0/0.0.0.0/0/0
::/0.0.0.0/0/0 -> ::/0/0/0
Responder-Only (Y/N): N
PFS (Y/N): N
Mixed-mode : Disabled
Transform sets={
  default: { esp-aes esp-sha-hmac } ,
}
Always create SAs
Interfaces using crypto map Tunnel0-head-0:
Tunnel0

Device# show crypto ipsec sa

interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 10.10.10.1

  protected vrf: (none)
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  TRUE ident (addr/mask/prot/port): {LOCAL -> REMOTE}
    0.0.0.0/0.0.0.0/0/0 -> 0.0.0.0/0.0.0.0/0/0
    ::/0.0.0.0/0/0 -> ::/0/0/0
  current_peer 10.10.10.2 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2
    plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
    current outbound spi: 0x4776A36B(1198957419)
    PFS (Y/N): N, DH group: none

  inbound esp sas:
    spi: 0xA97EDEE7(2843664103)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 4, flow_id: 4, sibling_flags FFFFFFFF80000040, crypto map: Tunnel0-head-0

      sa timing: remaining key lifetime (k/sec): (4377587/76)
      IV size: 16 bytes
      replay detection support: Y
      Status: ACTIVE(ACTIVE)

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
    spi: 0x4776A36B(1198957419)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 3, flow_id: 3, sibling_flags FFFFFFFF80000040, crypto map: Tunnel0-head-0

      sa timing: remaining key lifetime (k/sec): (4377587/76)
      IV size: 16 bytes
      replay detection support: Y
      Status: ACTIVE(ACTIVE)

```

例: デュアルオーバーレイとしてのトンネルモードの設定

```

outbound ah sas:

outbound pcp sas:

Device# show crypto socket

Number of Crypto Socket connections 1

Tu0 Peers (local/remote): 10.10.10.1/10.10.10.2
  Local Ident (addr/mask/port/prot): (0.0.0.0/0.0.0.0/0/0)
  Remote Ident (addr/mask/port/prot): (0.0.0.0/0.0.0.0/0/0)
  TRUE ident (addr/mask/port/port): {LOCAL -> REMOTE}
    0.0.0.0/0.0.0.0/0/0 -> 0.0.0.0/0.0.0.0/0/0
    ::/0.0.0.0/0/0 -> ::/0/0/0
  IPSec Profile: "prof"
  Socket State: Open
  Client: "TUNNEL SEC" (Client State: Active)
Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "prof" Map-name: "Tunnel0-head-0"

Device# show cry ikev2 session
IPv4 Crypto IKEv2 Session

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote fvrf/ivrf Status
1 10.10.10.1/500 10.10.10.2/500 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK,
Auth verify: PSK
Life/Active Time: 86400/145 sec
CE id: 1001, Session-id: 1
Local spi: 25A0B173944015D3 Remote spi: 9F0C7677425670E1
Child sa:
  local selector 0.0.0.0/0 - 255.255.255.255/65535
  local selector ::/0 - FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF/65535
  remote selector 0.0.0.0/0 - 255.255.255.255/65535
  remote selector ::/0 - FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF/65535
  ESP spi in/out: 0xA97EDEE7/0x4776A36B

IPv6 Crypto IKEv2 Session

Device# show crypto session
Crypto session current status

Interface: Tunnel0
Profile: prof
Session status: UP-ACTIVE
Peer: 10.10.10.2 port 500
Session ID: 1
IKEv2 SA: local 10.10.10.1/500 remote 10.10.10.2/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
TRUE IDENT (addr/mask/prot/port): {LOCAL -> REMOTE}
  0.0.0.0/0.0.0.0/0/0 -> 0.0.0.0/0.0.0.0/0/0
  ::/0.0.0.0/0/0 -> ::/0/0/0
Active SAs: 2, origin: crypto map

```

IPsec 仮想トンネル インターフェイスに関する追加のリファレンス

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	『Cisco IOS Security Command Reference Commands A to C』 『Cisco IOS Security Command Reference Commands D to L』 『Cisco IOS Security Command Reference Commands M to R』 『Cisco IOS Security Command Reference Commands S to Z』
IPsec の設定	『Configuring Security for VPNs with IPsec』
QoS の設定	『Cisco IOS Quality of Service Solutions Configuration Guide』
EasyVPN の設定	「Cisco Easy VPN Remote」 「Easy VPN Server」
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準および RFC

標準/RFC	タイトル
RFC 2401	『Security Architecture for the Internet Protocol』
RFC 2408	『Internet Security Association and Key Management Protocol』
RFC 2409	『The Internet Key Exchange (IKE)』

テクニカル サポート

説明	リンク
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。	http://www.cisco.com/cisco/web/support/index.html

IPsec 仮想トンネル インターフェイスに関する機能情報

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、<https://cfnnng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 3: IPsec 仮想トンネル インターフェイスに関する機能情報

機能名	リリース	機能の設定情報
ダイナミック IPsec VTI		ダイナミック VTI によって IP アドレスの使用が効率的になり、セキュアな接続が提供されます。ダイナミック VTI によって、動的にダウンロード可能な、グループごとおよびユーザごとのポリシーを RADIUS サーバ上で設定できます。IPsec ダイナミック VTI を使用すれば、リモート アクセス VPN 用の高度にセキュアな接続を構築することができます。ダイナミック VTI によって、VRF 認識 IPsec の導入が簡単になります。 次のコマンドが導入または変更されました。 crypto isakmp profile, interface virtual-template, show vtemplate, tunnel mode, virtual-template.
FlexVPN 混合モードのサポート		FlexVPN 混合モード機能は、IPsec IPv6 トランスポート経由の IPv4 トラフィックの伝送をサポートします。これは、IPsec スタック上でのデュアルスタックのサポートにつながる第 1 段階です。この実装は、IPv4 トラフィックと IPv6 トラフィックの両方に対する単一の IPsec セキュリティ アソシエーション (SA) ペアの使用をサポートしません。 この機能は、IKEv2 とダイナミック VTI を使用したリモートアクセス VPN に対してのみサポートされます。

機能名	リリース	機能の設定情報
ダイナミック VTI に対するマルチ SA		DVTIは、イニシエータから提案された複数の IPsec セレクタを受け入れることができます。 次のコマンドが導入または変更されました。 set security-policy limit, set reverse-route.
スタティック IPsec VTI		IPsec VTI では、IPsec トンネルを終端するためのルーティング可能なインターフェイス タイプと、オーバーレイ ネットワークを形成するためにサイト間の保護を定義する簡単な手段が提供されます。IPsec VTI によって、リモートリンクを保護するための IPsec の設定が簡素化され、マルチキャストがサポートされ、さらには、ネットワーク管理およびロード バランシングが簡単に実現できるようになります。
トンネル モード自動選択		トンネル モード自動選択機能は、設定を容易にし、レスポンドの詳細の入手を支援します。この機能は、IKE プロファイルから仮想アクセス インターフェイスが作成されるとすぐに、トンネリング プロトコル（GRE または IPsec）とトランスポート プロトコル（IPv4 または IPv6）を自動的に仮想テンプレートに適用します。 次のコマンドが導入または変更されました： virtual-template

機能名	リリース	機能の設定情報
FlexVPN 混合モード v4 経由 v6 トランスポート		FlexVPN 混合モード v4 経由 v6 トランスポート機能は、 IPsec IPv4 トランスポート経由 の IPv6 トラフィックの伝送を サポートします。この実装 は、IPv4 トラフィックと IPv6 トラフィックの両方に対する 単一の IPsec セキュリティ ア ソシエーション (SA) ペアの 使用をサポートしません。



CHAPTER 4

失効したピア証明書の暗号セッションの削除

CRL ダウンロード時の失効したピア証明書の暗号セッションの削除機能は、新しい CRL のダウンロード中に証明書が失効していることが判明した場合にピアとのアクティブな暗号セッションを削除します。

- 機能情報の確認 (89 ページ)
- 失効したピア証明書の暗号セッションの削除に関する制約事項, on page 90
- 失効したピア証明書の暗号セッションの削除に関する情報, on page 90
- 失効したピア証明書の暗号セッションの削除のイネーブル化方法, on page 91
- 失効したピア証明書の暗号セッションを削除する設定例, on page 93
- 失効したピアの暗号セッションの削除に関する追加のリファレンス, on page 94
- 失効したピア証明書の暗号セッションの削除に関する機能情報, on page 95

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「[Bug Search Tool](#)」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

失効したピア証明書の暗号セッションの削除に関する制約事項

- 失効チェックがオフで、この機能が有効になっている場合は、IKE データベースにセッション番号が入力されません。show 出力に、削除されたセッションに関する情報が表示されません。
- この機能を（デバイス上のアクティブセッションで）頻繁に有効化/無効化するのはお勧めできません。
- 同じ発行者名（CA サーバ）の CRL を頻繁にダウンロードする（30 分間隔）のはお勧めできません。
- CRL キャッシュを有効にする必要があります。CRL キャッシングをトラストポイントベースのプリフェッチに対して無効にすることはできません。ただし、CRL キャッシングを URL ベースのプリフェッチに対して無効にすることはできます。
- IKE 上の自動登録の場合は、セッションが次の IKE キー再生成まで削除されませんが、IKEv2 の場合は、トンネルを手動でクリアするか、証明書が失効するまで待つ必要があります。
- IKE が "issuer-name" と "SN" のデータベースを生成し、PKI から証明書の失効に関する通知を受け取ると、IKE がその PKI 通知を処理します。

失効したピア証明書の暗号セッションの削除に関する情報

暗号セッションの削除方法

- 証明書認証経由でネゴシエートする場合は、ピアが CERT ペイロードをデバイスに送信し、デバイスが各証明書を解析してシリアル番号と発行者名に関する情報を保存します。この情報は、対応する CA サーバによって発行されたシリアル番号のリストを形成し、PKI に渡され、失効がチェックされます。
- revocation-check crl コマンドがトラストポイント用に設定されている場合は、PKI が IKE に失効チェックの結果を伝達するため、IKE は不要なピア認定情報を保存せずに済みます。
- CRL のダウンロードが成功すると、PKI が IKE に "issuer-name" を含む通知を送信します。CRL の署名と内容が検証されます。CRL の内容に変更がなければ、PKI は IKE に通知しません。

4. PKI が IKE に発行者名を通知すると、IKE は発行者名に関するシリアル番号のリストを作成して、そのリストを PKI に渡し、リスト内のシリアル番号が失効しているかどうかを検証されます。
5. PKI は IKE から渡されたシリアル番号のリストに対して失効チェックを実行し、ダウンロードした CRL に照らしてそのリストをチェックします。失効したシリアル番号のリストが IKE に返されます。
6. 失効したシリアル番号のリストを含む通知を PKI から受信すると、IKE はそのようなシリアル番号に関連付けられたセッションを特定して削除します。

失効したピア証明書の暗号セッションの削除のイネーブル化方法

暗号セッションの削除の有効化

このタスクは、失効した証明書の暗号セッションの削除を有効にするために実行します。

SUMMARY STEPS

1. **enable**
2. **clear crypto session**
3. **configure terminal**
4. 次のいずれかを実行します。
 - **crypto isakmp disconnect-revoked-peers**
 - **crypto ikev2 disconnect-revoked-peers**
5. **end**

DETAILED STEPS

Procedure		
	Command or Action	Purpose
ステップ 1	enable Example: Device> enable	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	clear crypto session Example:	(任意) IPSec 暗号セッション、IKE、およびセキュリティ アソシエーションを削除します。

	Command or Action	Purpose
	Device# clear crypto session	 Note このコマンドは、以前確立したセッションの場合は、機能が新しいセッション
ステップ 3	configure terminal Example: Device# 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 4	次のいずれかを実行します。 • crypto isakmp disconnect-revoked-peers • crypto ikev2 disconnect-revoked-peers Example: Device(config)# crypto isakmp disconnect-revoked-peers Example: Device(config)# crypto ikev2 disconnect-revoked-peers	証明書が失効したピアとの IKE または IKEv2 暗号セッションを切断します。 このコマンドを有効にするには、既存のセッションを再接続します。
ステップ 5	end Example: Device(config)# exit	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

失効したピア証明書の暗号セッションの削除機能の確認

このタスクは、暗号セッションの削除機能が show 出力に表示されるかどうかを確認するために実行します。

SUMMARY STEPS

1. **enable**
2. **show crypto isakmp peers**
3. **show crypto ikev2 session detail**

DETAILED STEPS

Procedure

ステップ 1 enable

Example:

```
Device> enable
```

特権 EXEC モードを有効にします。

- プロンプトが表示されたら、パスワードを入力します。

ステップ 2 show crypto isakmp peers

Example:

```
Device# show crypto isakmp peers
```

Internet Security Association and Key Management Protocol (ISAKMP) ピアの説明を表示します。

ステップ 3 show crypto ikev2 session detail

Example:

```
Device# show crypto ikev2 session detail
```

アクティブなインターネット キー エクスチェンジバージョン 2 (IKEv2) セッションのステータスを表示します。

失効したピア証明書の暗号セッションを削除する設定例

例：IKE セッションの暗号セッションの削除のイネーブル化

```
Device> enable
Device# clear crypto session
Device# configure terminal
Device(config)# crypto isakmp disconnect-revoked-peers
Device# show crypto isakmp peers

Peer: 150.1.1.2 Port: 500 Local: 150.1.1.1
Phase1 id: 150.1.1.2
Disconnect Revoked Peer: Enabled
```

例：IKEv2 セッションの暗号セッションの削除のイネーブル化

```
Device> enable
Device# clear crypto session
Device# configure terminal
Device(config)# crypto ikev2 disconnect-revoked-peers
Device# show crypto ikev2 session detail

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id  Local          Remote          fvrf/ivrf       Status
1          10.0.0.1/500      10.0.0.2/500    (none)/(none)   READY
    Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
    Life/Remaining/Active Time: 86400/86157/248 sec
    CE id: 0, Session-id: 1, MIB-id: 1
    Status Description: Negotiation done
    Local spi: 750CBE827434A245      Remote spi: 4353FEDBABEBF24C
    Local id:      10.0.0.1          Remote id:      10.0.0.2
    Local req mess id: 0              Remote req mess id: 0
```

```

Local next mess id:      0          Remote next mess id: 2
Local req queued:       0          Remote req queued: 0
Local window:          5          Remote window: 5
DPD configured for 0 seconds
NAT-T is not detected
Disconnect Revoked Peer: Enabled
Child sa: local selector 10.0.0.1/0 - 10.0.0.1/65535
          remote selector 10.0.0.2/0 - 10.0.0.2/65535
          ESP spi in/out: 0x9360A95/0x6C340600
          CPI in/out: 0x9FE5/0xC776
          AH spi in/out: 0x0/0x0
          Encr: AES CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: Unknown - 0, comp: IPCOMP_LZS, mode tunnel

```

失効したピアの暗号セッションの削除に関する追加のリファレンス

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『 Cisco IOS Master Commands List, All Releases 』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
IKE の設定	「 Configuring Internet Key Exchange for IPsec VPNs 」
IKEv2 の設定	『 Configuring Internet Key Exchange Version 2 and FlexVPN Site-to-Site 』
推奨される暗号化アルゴリズム	『 Next Generation Encryption 』

テクニカル サポート

説明	リンク
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。	http://www.cisco.com/cisco/web/support/index.html

失効したピア証明書の暗号セッションの削除に関する機能情報

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、<https://cfnnng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

Table 4: 失効したピア証明書の暗号セッションの削除に関する機能情報

機能名	リリース	機能情報
CRL ダウンロード時の失効したピア証明書の暗号セッションの削除		CRL ダウンロード時の失効したピア証明書の暗号セッションの削除機能は、新しい CRL のダウンロード中に証明書が失効していることが判明した場合にピアとのアクティブな暗号セッションを削除します。 次のコマンドが導入または変更されました。 crypto ikev2 disconnect-revoked-peers、crypto isakmp disconnect-revoked-peers、show crypto isakmp peers、show crypto ikev2 session detail



第 5 章

暗号条件付きデバッグ サポート

暗号条件付きデバッグサポート機能では、新しいdebug コマンドが導入され、これらのコマンドにより、ユーザは、ピア IP アドレス、暗号エンジンの接続 ID、セキュリティパラメータインデックス (SPI) などの事前に定義された暗号条件に基づいて IP セキュリティ (IPSec) トンネルをデバッグできます。特定の IPSec 処理に限定してデバッグ メッセージを表示し、デバッグ出力の量を減らすことにより、多数のトンネルを使用するルータを効率的にトラブルシューティングできます。

- 機能情報の確認 (97 ページ)
- 暗号条件付きデバッグ サポートの前提条件 (98 ページ)
- 暗号条件付きデバッグ サポートの制約事項 (98 ページ)
- 暗号条件付きデバッグ サポートに関する情報 (98 ページ)
- 暗号条件付きデバッグ サポートのイネーブル化方法 (100 ページ)
- 暗号条件付きデバッグ CLI の設定例 (103 ページ)
- その他の参考資料 (104 ページ)
- 暗号条件付きデバッグ サポートに関する機能情報 (105 ページ)

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「[Bug Search Tool](#)」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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、<https://cfnng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

暗号条件付きデバッグ サポートの前提条件

暗号条件付きデバッグ サポートの制約事項

- 条件付きデバッグは、特定のピアまたは機能に関連するインターネットキー交換（IKE）および IPSec の問題をトラブルシューティングする際に役立ちますが、デバッグ条件が多すぎると、そのデバッグ条件を定義およびチェックできない場合があります。デバッグ条件値を保管するために空き領域が余分に必要となるため、CPU の処理オーバーヘッドが増加し、メモリ使用量も増加します。したがって、大量のトラフィックを処理するルータで暗号条件付きデバッグをイネーブルにする場合は、注意が必要です。

暗号条件付きデバッグ サポートに関する情報

サポートされる条件タイプ

新しい暗号条件付きデバッグ CLI（**debug crypto condition**、**debug crypto condition unmatched**、**and show crypto debug-condition**）を使用すれば、条件（フィルタ値）を指定して、指定した条件に関連するデバッグメッセージだけを生成して表示することができます。次の表に、サポートされる条件タイプを示します。



- (注) **ipv4** または **ipv6** キーワードを指定した **debug crypto condition peer** コマンドは、ハードウェアプラットフォーム固有のデバッグ出力を提供できます。残りの条件フィルタは、プラットフォーム固有のデバッグ出力を提供しません。

表 5: 暗号デバッグ CLI でサポートされる条件タイプ

条件タイプ（キーワード）	説明
connid ¹	1 ～ 32766 の整数。現在の IPSec 処理で、この値が暗号エンジンのあるインターフェイスへの接続 ID として使用されている場合、関連するデバッグメッセージが表示されます。
FVRF	バーチャルプライベート ネットワーク（VPN）ルーティング/転送（VRF）インスタンスの名前を表す文字列。この VRF インスタンスが、現在の IPSec 処理で、前面扉 VRF（FVRF）として使用されている場合、関連するデバッグメッセージが表示されます。

条件タイプ（キーワード）	説明
ikev2	IKEv2 プロファイルの名前文字列。IKEv2 プロファイル名が指定された場合は、関連するデバッグメッセージが表示されます。
isakmp	ISAKMP プロファイルの名前文字列。ISAKMP プロファイル名が指定された場合は、関連するデバッグメッセージが表示されます。
IVRF	VRF インスタンスの名前を表す文字列。この VRF インスタンスが、現在の IPSec 処理で、内部 VRF（IVRF）として使用されている場合、関連するデバッグメッセージが表示されます。
local	IPv4 または IPv6 ローカルアドレスの名前文字列。
peer group	Unity グループ名を表す文字列。このグループ名をピアがアイデンティティとして使用している場合、関連するデバッグメッセージが表示されます。
peer hostname	完全修飾ドメイン名（FQDN）を表す文字列。この文字列をピアがアイデンティティとして使用している場合、関連するデバッグメッセージが表示されます（たとえば、ピアがこの FQDN 文字列を使用して IKE Xauth をイネーブルにする場合）。
peer ipv4 または peer ipv6	単一の IP アドレス。現在の IPSec 処理が、このピアの IP アドレスに関係している場合、関連するデバッグメッセージが表示されます。
peer subnet	ピアの IP アドレスの範囲を指定するサブネットおよびサブネットマスク。現在の IPSec ピアの IP アドレスが、指定したサブネット範囲に属する場合、関連するデバッグメッセージが表示されます。
peer username	ユーザ名を表す文字列。このユーザ名をピアがアイデンティティとして使用している場合、関連するデバッグメッセージが表示されます（たとえば、ピアがこのユーザ名を使用して IKE 拡張認証（Xauth）をイネーブルにする場合）。
session	暗号セッションに関する情報を提供します。
SPI	32 ビットの符号なし整数。現在の IPSec 処理がこの値を SPI として使用する場合、関連するデバッグメッセージが表示されます。
unmatched	コンテキスト情報が使用できない場合にデバッグメッセージを提供します。

¹ IPSec connid、flowid、または SPI をデバッグ条件として使用する場合、関連する IPSec フローに関するデバッグメッセージが生成されます。IPSec フローには、connid、flowid、および SPI が 2 つ（インバウンドとアウトバウンド）ずつ含まれています。各 2 つの connid、flowid、および SPI は、IPSec フローのデバッグメッセージをトリガーするデバッグ条件として使用できます。

暗号条件付きデバッグ サポートのイネーブル化方法

暗号条件付きデバッグ メッセージのイネーブル化

パフォーマンス上の考慮事項

- 暗号条件付きデバッグをイネーブルにする前に、使用するデバッグ条件タイプ（デバッグフィルタとしても知られる）および値を決める必要があります。デバッグメッセージの量は、定義する条件数によって異なります。



(注) 多数のデバッグ条件を指定すると、CPU サイクルが消費され、ルータのパフォーマンスに悪影響を及ぼすことがあります。

- ルータによって条件付きデバッグが実行されるのは、最低 1 つのグローバル `crypto debug` コマンド（`debug crypto isakmp`、`debug crypto ipsec`、および `debug crypto engine`）がイネーブルに設定されている場合に限られます。この要件により、条件付きデバッグを使用していないときは、ルータのパフォーマンスに影響が出ないようにになっています。

暗号条件付きデバッグのディセーブル化

暗号条件付きデバッグをディセーブルにするには、発行済みのグローバルな暗号デバッグ CLI を事前にディセーブルにする必要があります。その後で、条件付デバッグをディセーブルにできます。



(注) **reset** キーワードを使用すると、設定されたすべての条件を同時にディセーブルにできます。

手順の概要

- enable**
- debug crypto condition** [*connid integer engine-id integer*] [*flowid integer engine-id integer*] [*fvr string*] [*ivrf string*] [*peer [group string] [hostname string] [ipv4 ipaddress] [subnet subnet mask] [username string]] [spi integer] [reset]*
- show crypto debug-condition** {[*peer*] [*connid*] [*spi*] [*fvr*] [*ivrf*] [*unmatched*]}
- debug crypto isakmp**
- debug crypto ipsec**
- debug crypto engine**
- debug crypto condition unmatched** [*isakmp | ipsec | engine*]

手順の詳細

手順

	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。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	debug crypto condition <i>[connid integer engine-id integer] [flowid integer engine-id integer] [fvrf string] [ivrf string] [peer [group string] [hostname string] [ipv4 ipaddress] [subnet subnet mask] [username string]] [spi integer] [reset]</i> 例 : <pre>Router# debug crypto condition connid 2000 engine-id 1</pre>	条件付きデバッグ フィルタを定義します。
ステップ 3	show crypto debug-condition <i>{[peer] [connid] [spi] [fvrf] [ivrf] [unmatched]}</i> 例 : <pre>Router# show crypto debug-condition spi</pre>	ルータ上ですでにイネーブルに設定されている暗号デバッグ条件を表示します。
ステップ 4	debug crypto isakmp 例 : <pre>Router# debug crypto isakmp</pre>	グローバル IKE デバッグをイネーブルにします。
ステップ 5	debug crypto ipsec 例 : <pre>Router# debug crypto ipsec</pre>	グローバル IPSec デバッグをイネーブルにします。
ステップ 6	debug crypto engine 例 : <pre>Router# debug crypto engine</pre>	グローバル暗号エンジンデバッグをイネーブルにします。
ステップ 7	debug crypto condition unmatched <i>[isakmp ipsec engine]</i> 例 :	(任意) デバッグ条件をチェックするためのコンテキスト情報がない場合、デバッグ条件付き暗号メッセージを表示します。

	コマンドまたはアクション	目的
	Router# debug crypto condition unmatched ipsec	オプションのキーワードを指定しない場合は、暗号関連のすべての情報が表示されます。

暗号エラー デバッグ メッセージのイネーブル化

暗号エラー デバッグ フィルタリングをイネーブルにするには、次の作業を実行する必要があります。

デバッグ暗号エラー CLI

debug crypto error コマンドを有効にすると、エラーに関連するデバッグメッセージだけが表示されます。これにより、IKE ネゴシエーションなどの暗号処理がシステム内で失敗した理由を簡単に判別できます。



- (注) このコマンドをイネーブルにする場合は、グローバル暗号 **debug** コマンドがイネーブルに設定されていないことを確認してください。設定されていると、グローバル コマンドによってエラー関連のデバッグ メッセージが上書きされます。

手順の概要

1. **enable**
2. **debug crypto isakmp | ipsec | engine} error**

手順の詳細

手順

	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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	debug crypto isakmp ipsec engine} error 例 : Router# debug crypto ipsec error	暗号エリアに関するエラー デバッグ メッセージだけをイネーブルにします。

暗号条件付きデバッグ CLI の設定例

暗号条件付きデバッグのイネーブル化の例

次の例では、ピアの IP アドレスが 10.1.1.1、10.1.1.2、または 10.1.1.3 で、暗号エンジン 0 の接続 ID に 2000 が使用されている場合のデバッグ メッセージの表示例を示します。また、この例では、グローバルデバッグ暗号 CLI をイネーブルする方法と、**show crypto debug-condition** コマンドをイネーブルにして条件付きの設定を確認する方法も示します。

```
Router#
debug crypto condition connid 2000 engine-id 1
Router#
debug crypto condition peer ipv4 10.1.1.1
Router#
debug crypto condition peer ipv4 10.1.1.2
Router#
debug crypto condition peer ipv4 10.1.1.3
Router#
debug crypto condition unmatched
! Verify crypto conditional settings.
Router#
show crypto debug-condition
Crypto conditional debug currently is turned ON
IKE debug context unmatched flag:ON
IPsec debug context unmatched flag:ON
Crypto Engine debug context unmatched flag:ON
IKE peer IP address filters:
10.1.1.1 10.1.1.2 10.1.1.3
Connection-id filters:[connid:engine_id]2000:1,
! Enable global crypto CLIs to start conditional debugging.
Router#
debug crypto isakmp
Router#
debug crypto ipsec
Router#
debug crypto engine
```

暗号条件付きデバッグのディセーブル化の例

次の例では、すべての暗号条件付き設定をディセーブルにし、またこれらの設定がディセーブルになったことを確認する方法を示します。

```
Router#
debug crypto condition reset
! Verify that all crypto conditional settings have been disabled.
Router#
show crypto debug-condition
Crypto conditional debug currently is turned OFF
IKE debug context unmatched flag:OFF
IPsec debug context unmatched flag:OFF
Crypto Engine debug context unmatched flag:OFF
```

その他の参考資料

ここでは、暗号条件付きデバッグ サポート機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
IPSec および IKE 設定作業	『Cisco IOS XE Security Configuration Guide: Secure Connectivity』の「Internet Key Exchange for IPsec VPNs」の章
IPSec および IKE コマンド	『Cisco IOS Security Command Reference』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	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
なし	--

テクニカル サポート

説明	リンク
Cisco のサポート Web サイトでは、Cisco 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。 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。 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。	http://www.cisco.com/en/US/support/index.html

暗号条件付きデバッグ サポートに関する機能情報

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、<https://cfng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。



第 6 章

IPv4 GRE トンネル保護経由の IPv6

IPv4 GRE トンネル保護経由の IPv6 機能は、IPv6 ユニキャストトラフィックと IPv6 マルチキャストトラフィックの両方が保護された Generic Routing Encapsulation (GRE) を通過できるようにします。

- 機能情報の確認 (107 ページ)
- IPv4 GRE トンネル保護経由の IPv6 の前提条件 (107 ページ)
- IPv4 GRE トンネル保護経由の IPv6 の制約事項 (108 ページ)
- IPv4 GRE トンネル保護経由の IPv6 に関する情報 (108 ページ)
- IPv4 GRE トンネル保護経由の IPv6 の設定方法 (110 ページ)
- IPv4 GRE トンネル保護経由の IPv6 の設定例 (117 ページ)
- その他の参考資料 (118 ページ)
- IPv4 GRE トンネル保護経由の IPv6 に関する機能情報 (119 ページ)

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「[Bug Search Tool](#)」およびご使用のプラットフォームおよびソフトウェアリリースのリリースノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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、<https://cfnng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

IPv4 GRE トンネル保護経由の IPv6 の前提条件

- この機能を有効にするには、IPv4 GRE トンネル上で IPsec トンネル保護を設定する必要があります。

- IPv6 マルチキャストを有効にするには、IPv6 マルチキャスト ルーティングを設定する必要があります。

IPv4 GRE トンネル保護経由の IPv6 の制約事項

IPv4 GRE トンネル保護経由の IPv6 機能は、IPv4 ポイントツーポイント GRE トンネル保護経由の IPv6 をサポートしますが、IPv4 mGRE トンネル保護経由の IPv6 はサポートしません。

IPv4 GRE トンネル保護経由の IPv6 に関する情報

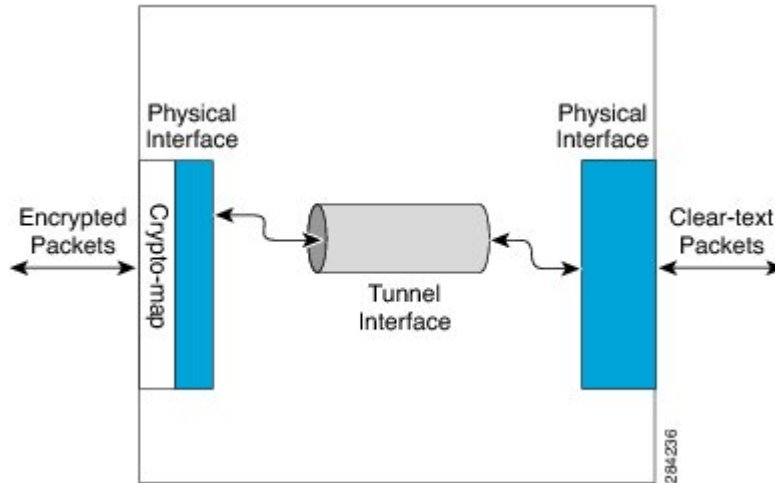
IPsec を使用した GRE トンネル

Generic Routing Encapsulation (GRE) トンネルは、ときどき、IPsec と組み合わせて使用されます。これは、IPsec が IPv6 マルチキャスト パケットをサポートしていないためです。これにより、ダイナミック ルーティング プロトコルが IPsec VPN ネットワーク経由で正しく機能しません。GRE トンネルは IPv6 マルチキャスト をサポートしているため、ダイナミック ルーティング プロトコルを GRE トンネル経由で実行できます。ダイナミック ルーティング プロトコルが GRE トンネル経由で設定されている場合は、IPsec を使用して GRE IPv6 マルチキャスト パケットを暗号化できます。

IPsec は、クリプト マップまたはトンネル保護を使用して GRE パケットを暗号化できます。いずれの方法でも、GRE カプセル化の設定後に、IPsec 暗号化を実行するように指定されます。クリプト マップを使用している場合は、暗号化が GRE トンネル パケット用のアウトバウンド物理インターフェイスに適用されます。トンネル保護を使用している場合は、暗号化が GRE トンネル インターフェイス上で設定されます。

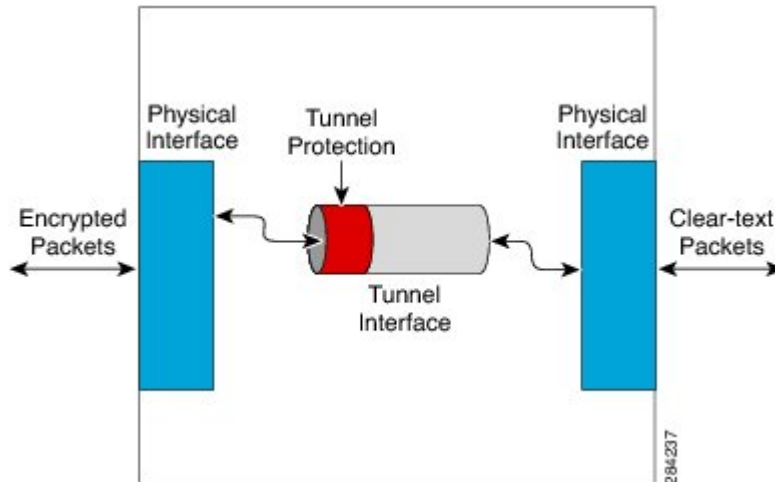
次の図に、物理インターフェイス上でクリプト マップを使用して、GRE トンネル インターフェイス経由でルータに入る暗号化されたパケットを示します。パケットは、復号化およびカプセル化解除されてから、クリア テキストとして IP 宛先に送られます。

図 7: クリプトマップを使用した IPv4 GRE トンネル暗号化経路の IPv6 の設定



次の図に、GRE トンネル インターフェイス上で `tunnel protection` コマンドを使用した暗号化を示します。暗号化されたパケットは、トンネルインターフェイス経由でルータに入り、復号化およびカプセル化解除されてから、クリア テキストとして宛先に送られます。

図 8: トンネル保護を使用した IPv4 GRE トンネル暗号化経路の IPv6 の設定



クリプトマップ方式を使用した場合とトンネル保護方式を使用した場合の重要な違いを以下に示します。

- IPsec クリプトマップは、物理インターフェイスに関連付けられ、パケットが物理インターフェイスを通して転送されるときにチェックされます。この時点で、パケットはすでに GRE トンネル内でカプセル化されています。
- トンネル保護は、暗号化機能を GRE トンネルに関連付け、パケットが GRE カプセル化されてから物理インターフェイスに転送されるまでの間にチェックされます。

IPv4 GRE トンネル保護経由の IPv6 の設定方法

クリプト マップを使用した IPv4 GRE 暗号化経由の IPv6 の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 multicast-routing**
4. **ipv6 unicast-routing**
5. **interface** *type number*
6. **ipv6 address** {*ipv6-address/prefix-length* | **prefix-name** *sub-bits/prefix-length*}
7. **tunnel mode** {*aurp* | *cayman* | *dvmrp* | *eon* | **gre** | **gre multipoint** | **gre ip** | **gre ipv6** | **ipip** | *decapsulate-any*} | **ipsec ipv4** | *iptalk* | **ipv6** | **ipsec ipv6** | *mpls* | *nos* | *rbscp*}
8. **tunnel source** {*ip-address* | *ipv6-address* | *interface-type**interface-number*}
9. **tunnel destination** {*hostname* | *ip-address* | *ipv6-address*}
10. **exit**
11. **crypto isakmp policy** *priority*
12. **authentication** {*rsa-sig* | *rsa-encr* | **pre-share**}
13. **hash** {*sha* | *md5*}
14. **group** {**1** | **2** | **5**}
15. **encryption** {*des* | *3des* | *aes 192* | *aes 256*}
16. **exit**
17. **crypto isakmp key** *enc-type-digit* *keystring* {*address* *peer-address* [*mask*] | **ipv6** {*ipv6-address/ipv6-prefix*} | *hostname* *hostname*} [**no-xauth**]
18. **crypto ipsec transform-set** *transform-set-name* *transform1* [*transform2*] [*transform3*] [*transform4*]
19. **access-list** *access-list-number* [**dynamic** *dynamic-name* [*timeout minutes*]] {**deny** | **permit**} *protocol* *source* *source-wildcard* *destination* *destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-range-name*] [**fragments**] [**log** [*word*]] | **log-input** [*word*]]
20. **crypto map** [**ipv6**] *map-name* *seq-num* [**ipsec-isakmp** | **dynamic** *dynamic-map-name* | **discover** | *profile* *profile-name*]]
21. **set peer** {*hostname* [**dynamic**] [**default**] | *ip-address* [**default**]}
22. **set transform-set** *transform-set-name* [*transform-set-name2*...*transform-set-name6*]
23. **match address** [*access-list-id* | *name*]
24. **exit**
25. **interface** *type number*
26. **crypto map** *map-name* [**redundancy** *standby-group-name* [**stateful**]]
27. **end**

手順の詳細

手順

	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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例 : Router# configure terminal	グローバル構成モードを開始します。
ステップ 3	ipv6 multicast-routing 例 : Router(config)# ipv6 multicast-routing	ルータのすべての IPv6 対応インターフェイス上で Protocol Independent Multicast (PIM) とマルチキャストリスナー検出 (MLD) を使用したマルチキャストルーティングを有効にして、マルチキャスト転送を有効にします。 • このコマンドは、IPv6 マルチキャストを使用している場合にのみ有効にします。IPv6 ユニキャストを使用している場合は、このコマンドを有効にしないようにする必要があります。
ステップ 4	ipv6 unicast-routing 例 : Router(config)# ipv6 unicast-routing	IPv6 ユニキャスト データグラムの転送を有効にします。
ステップ 5	interface type number 例 : Router(config)# interface tunnel 10	トンネル インターフェイスおよび番号を指定し、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 6	ipv6 address {ipv6-address/prefix-length prefix-name sub-bits/prefix-length} 例 : Router(config-if)# ipv6 address 0:0:0:7272::72/64	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 7	tunnel mode {aurp cayman dvmrp eon gre gre multipoint gre ip gre ipv6 ipip [decapsulate-any] ipsec ipv4 iptalk ipv6 ipsec ipv6 mpls nos rbscp} 例 : Router(config-if)# tunnel mode gre ip	トンネル インターフェイスのカプセル化モードを設定します。

	コマンドまたはアクション	目的
ステップ 8	tunnel source {ip-address ipv6-address interface-typeinterface-number} 例 : Router(config-if)# tunnel source ethernet0	トンネル インターフェイスの送信元アドレスを設定します。
ステップ 9	tunnel destination {hostname ip-address ipv6-address} 例 : Router(config-if)# tunnel destination 172.16.0.12	トンネル インターフェイスの宛先を指定します。
ステップ 10	exit 例 : Router(config-if)# exit	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 11	crypto isakmp policy priority 例 : Router(config)# crypto isakmp policy 15	インターネット キー エクスチェンジ (IKE) ポリシーを定義して、ISAKMP ポリシー コンフィギュレーション モードを開始します。 ポリシー番号1は、最もプライオリティが高いポリシーを示します。<i>priority</i> 引数値が低いほど、優先順位が高くなります。
ステップ 12	authentication {rsa-sig rsa-encr pre-share} 例 : Router(config-isakmp-policy)# authentication pre-share	IKE ポリシー内の認証方式を指定します。 rsa-sig キーワードと rsa-encr キーワードは IPv6 でサポートされません。
ステップ 13	hash {sha md5} 例 : Router(config-isakmp-policy)# hash md5	IKE ポリシー内のハッシュ アルゴリズムを指定します。
ステップ 14	group {1 2 5} 例 : Router(config-isakmp-policy)# group 2	IKE ポリシー内部での D-H グループの識別番号を指定します。
ステップ 15	encryption {des 3des aes 192 aes 256} 例 : Router(config-isakmp-policy)# encryption 3des	IKE ポリシー内の暗号化アルゴリズムを指定します。
ステップ 16	exit 例 : Router(config-isakmp-policy)# exit	ISAKMP ポリシー コンフィギュレーション モードを終了して、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 17	crypto isakmp key enc-type-digit keystring {address peer-address [mask] ipv6 {ipv6-address/ipv6-prefix} hostname hostname} [no-xauth]	事前共有認証キーを設定します。

	コマンドまたはアクション	目的
	例 : <pre>Router(config)# crypto isakmp key cisco-10 address 172.16.0.12 255.240.0.0</pre>	
ステップ 18	crypto ipsec transform-set transform-set-name transform1 [transform2] [transform3] [transform4] 例 : <pre>Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des</pre>	トランスフォーム セットを定義します。
ステップ 19	access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [time-range time-range-name] [fragments] [log [word] log-input [word]] 例 : <pre>Router(config)# access-list 110 permit gre host 192.168.0.16 host 172.16.0.12</pre>	拡張 IP アクセス リストを定義します。
ステップ 20	crypto map [ipv6] map-name seq-num [ipsec-isakmp [dynamic dynamic-map-name discover profile profile-name]] 例 : <pre>Router(config)# crypto map mymap 10 ipsec-isakmp</pre>	新しいクリプト マップ エントリまたはプロファイルを作成し、クリプトマップコンフィギュレーション モードを開始します。
ステップ 21	set peer {hostname [dynamic] [default] ip-address [default]} 例 : <pre>Router(config-crypto-map)# set peer 10.0.0.1</pre>	クリプト マップ エントリ内の IP Security (IPsec) ピアを指定します。
ステップ 22	set transform-set transform-set-name [transform-set-name2...transform-set-name6] 例 : <pre>Router(config-crypto-map)# set transform-set myset0</pre>	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。
ステップ 23	match address [access-list-id name] 例 : <pre>Router(config-crypto-map)# match address 102</pre>	クリプト マップ エントリの拡張アクセス リストを指定します。
ステップ 24	exit 例 : <pre>Router(config-crypto-map)# exit</pre>	クリプト マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 25	interface <i>type number</i> 例 : Router(config)# interface ethernet 1	インターフェイスと番号を指定し、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 26	crypto map <i>map-name</i> [redundancy <i>standby-group-name</i> [stateful]] 例 : Router(config-if)# crypto map mymap	定義済みのクリプト マップ セットをアウトバウンド インターフェイスに適用します。
ステップ 27	end 例 : Router(config-if)# end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トンネル保護を使用した IPv4 GRE 暗号化経由の IPv6 の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 multicast-routing**
4. **ipv6 unicast-routing**
5. **crypto isakmp policy** *priority*
6. **authentication** {*rsa-sig* | *rsa-encr* | *pre-share*}
7. **hash** {*sha* | *md5*}
8. **group** {*1* | *2* | *5*}
9. **encryption** {*des* | *3des* | *aes* | *aes 192* | *aes 256*}
10. **exit**
11. **crypto isakmp key** *enc-type-digit keystring* {*address peer-address* [*mask*] | **ipv6** {*ipv6-address/ipv6-prefix*} | *hostname hostname*} [**no-xauth**]
12. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
13. **crypto ipsec profile** *profile-name*
14. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
15. **exit**
16. **interface** *type number*
17. **ipv6 address** {*ipv6-address / prefix-length* | *prefix-name sub-bits/prefix-length*}
18. **tunnel mode** {*aurp* | *cayman* | *dvmrp* | *eon* | **gre** | **gre multipoint** | **gre ip** | **gre ipv6** | *ipip*[*decapsulate-any*] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}
19. **tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*}
20. **tunnel destination** {*hostname* | *ip-address* | *ipv6-address*}
21. **tunnel protection ipsec profile** *name* [**shared**]
22. **end**

手順の詳細

手順

	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。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例 : <pre>Router# configure terminal</pre>	グローバル構成モードを開始します。
ステップ 3	ipv6 multicast-routing 例 : <pre>Router(config)# ipv6 multicast-routing</pre>	ルータのすべての IPv6 対応インターフェイス上で Protocol Independent Multicast (PIM) とマルチキャストリスナー検出 (MLD) を使用したマルチキャストルーティングを有効にして、マルチキャスト転送を有効にします。 このコマンドは、IPv6 マルチキャストを使用している場合にのみ有効にします。IPv6 ユニキャストを使用している場合は、このコマンドを有効にする必要はありません。
ステップ 4	ipv6 unicast-routing 例 : <pre>Router(config)# ipv6 unicast-routing</pre>	IPv6 ユニキャスト データグラムの転送を有効にします。
ステップ 5	crypto isakmp policy <i>priority</i> 例 : <pre>Router(config)# crypto isakmp policy 15</pre>	IKE ポリシーを定義し、ISAKMP ポリシー コンフィギュレーション モードを開始します。 ポリシー番号 1 は、最もプライオリティが高いポリシーを示します。 <i>priority</i> 引数値が低いほど、優先順位が高くなります。
ステップ 6	authentication {rsa-sig rsa-encr pre-share} 例 : <pre>Router(config-isakmp-policy)# authentication pre-share</pre>	インターネット キー エクスチェンジ (IKE) ポリシー内の認証方式を指定します。 rsa-sig キーワードと rsa-encr キーワードは IPv6 でサポートされません。
ステップ 7	hash {sha md5} 例 : <pre>Router(config-isakmp-policy)# hash md5</pre>	IKE ポリシー内のハッシュ アルゴリズムを指定します。

	コマンドまたはアクション	目的
ステップ 8	group {1 2 5} 例 : Router(config-isakmp-policy)# group 2	IKE ポリシー内部での D-H グループの識別番号を指定します。
ステップ 9	encryption {des 3des aes aes 192 aes 256} 例 : Router(config-isakmp-policy)# encryption 3des	IKE ポリシー内の暗号化アルゴリズムを指定します。
ステップ 10	exit 例 : Router(config-isakmp-policy)# exit	ISAKMP ポリシー コンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	crypto isakmp key <i>enc-type-digit</i> <i>keystring</i> { address <i>peer-address</i> [<i>mask</i>] ipv6 { <i>ipv6-address/ipv6-prefix</i> } hostname <i>hostname</i> } [no-xauth] 例 : Router(config)# crypto isakmp key cisco-10 address 172.16.0.12 255.240.0.0	事前共有認証キーを設定します。
ステップ 12	crypto ipsec transform-set <i>transform-set-name</i> <i>transform1</i> [<i>transform2</i>] [<i>transform3</i>] [<i>transform4</i>] 例 : Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des	トランスフォーム セットを定義し、ルータを暗号化トランスフォーム コンフィギュレーション モードにします。
ステップ 13	crypto ipsec profile <i>profile-name</i> 例 : Router(config)# crypto ipsec profile ipsecprof	2 つの IPsec ルータ間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec プロファイル コンフィギュレーション モードを開始します。
ステップ 14	set transform-set <i>transform-set-name</i> [<i>transform-set-name2</i> ... <i>transform-set-name6</i>] 例 : Router(ipsec-profile)# set transform-set myset0	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。
ステップ 15	exit 例 : Router(ipsec-profile)# exit	IPsec プロファイル コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 16	interface <i>type number</i> 例 : Router(config)# interface tunnel 1	トンネル インターフェイスおよび番号を指定し、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。

	コマンドまたはアクション	目的
ステップ 17	ipv6 address { <i>ipv6-address / prefix-length</i> <i>prefix-name sub-bits/prefix-length</i> } 例 : <pre>Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127</pre>	インターフェイスに割り当てられている IPv6 ネットワークを指定し、インターフェイスで IPv6 処理をイネーブルにします。
ステップ 18	tunnel mode { <i>aurp</i> <i>cayman</i> <i>dvmrp</i> <i>eon</i> gre gre multipoint gre ip gre ipv6 ipip [<i>decapsulate-any</i>] ipsec ipv4 iptalk ipv6 ipsec ipv6 mpls nos rbscp } 例 : <pre>Router(config-if)# tunnel mode gre ip</pre>	GRE IPv6 トンネルを指定します。
ステップ 19	tunnel source { <i>ip-address</i> <i>ipv6-address</i> <i>interface-type interface-number</i> } 例 : <pre>Router(config-if)# tunnel source 10.0.0.1</pre>	トンネル インターフェイスの送信元アドレスまたは送信元インターフェイス タイプと番号を指定します。
ステップ 20	tunnel destination { <i>hostname</i> <i>ip-address</i> <i>ipv6-address</i> } 例 : <pre>Router(config-if)# tunnel destination 172.16.0.12</pre>	トンネル インターフェイスの宛先アドレスまたはホスト名を指定します。
ステップ 21	tunnel protection ipsec profile name [<i>shared</i>] 例 : <pre>Router(config-if)# tunnel protection ipsec profile ipsecprof</pre>	トンネルインターフェイスを IPsec プロファイルに関連付けます。
ステップ 22	end 例 : <pre>Router(config-if)# end</pre>	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPv4 GRE トンネル保護経由の IPv6 の設定例

クリプト マップを使用した IPv4 GRE 暗号化経由の IPv6 の設定例

```
Router> enable
Router# configure terminal
Router(config)# ipv6 multicast-routing
Router(config)# ipv6 unicast-routing
Router(config)# interface tunnel 10
Router(config-if)# ipv6 address my-prefix 0:0:0:7272::72/64
Router(config-if)# tunnel mode gre ip
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 172.16.0.12
Router(config-if)# exit
Router(config)# crypto isakmp policy 15
```

```

Router(config-isakmp-policy)# authentication pre-share
Router(config-isakmp-policy)# hash md5
Router(config-isakmp-policy)# group 2
Router(config-isakmp-policy)# encryption 3des
Router(config-isakmp-policy)# exit
Router(config)# crypto isakmp key cisco-10 address 172.16.0.12 255.240.0.0
Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des
Router(config)# access-list 110 permit gre host 192.168.0.16 host 172.16.0.12
Router(config)# crypto map mymap 10 ipsec-isakmp
Router(config-crypto-map)# set peer 10.0.0.1
Router(config-crypto-map)# set transform-set myset0
Router(config-crypto-map)# match address 102
Router(config-crypto-map)# exit
Router(config)# interface ethernet1
Router(config-if)# crypto map mymap
Router(config-if)# end

```

トンネル保護を使用した IPv4 GRE 暗号化経由の IPv6 の設定例

次に、IPv4 GRE トンネル上で IPsec トンネル保護を設定する例を示します。IPv6 マルチキャストルーティングは、`ipv6 multicast-routing` コマンドを使用して有効にします。

```

Router> enable
Router# configure terminal
Router(config)# ipv6 multicast-routing
Router(config)# ipv6 unicast-routing
Router(config)# crypto isakmp policy 15
Router(config-isakmp-policy)# authentication pre-share
Router(config-isakmp-policy)# hash md5
Router(config-isakmp-policy)# group 2
Router(config-isakmp-policy)# encryption 3des
Router(config-isakmp-policy)# exit
Router(config)# crypto isakmp key cisco-10 address 172.16.0.12 255.240.0.0
Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des
Router(config)# crypto ipsec profile ipsecprof
Router(ipsec-profile)# set transform-set myset0
Router(ipsec-profile)# exit
Router(config)# interface tunnel 1
Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127
Router(config-if)# tunnel mode gre ip
Router(config-if)# tunnel source 10.0.0.1
Router(config-if)# tunnel destination 172.16.0.12
Router(config-if)# tunnel protection ipsec profile ipsecprof
Router(config-if)# end

```

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
IPv6 マルチキャスト ルーティング	『IPv6 Implementation Guide』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Security Command Reference Commands A to C』 『Cisco IOS Security Command Reference Commands D to L』 『Cisco IOS Security Command Reference Commands M to R』 『Cisco IOS Security Command Reference Commands S to Z』

テクニカル サポート

説明	リンク
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。	http://www.cisco.com/cisco/web/support/index.html

IPv4 GRE トンネル保護経由の IPv6 に関する機能情報

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、<https://cfnnng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。



第 7 章

RFC 430x IPsec サポート

RFC 430x IPsec サポートには、RFC 4301 で規定されているインターネット キー エクスチェンジ (IKE) と IPsec の動作を実装する機能 (RFC 430x IPsec サポート フェーズ 1 およびフェーズ 2) が含まれます。

- [機能情報の確認 \(121 ページ\)](#)
- [RFC 430x IPsec サポートに関する情報 \(121 ページ\)](#)
- [RFC 430x IPsec サポートの設定方法 \(123 ページ\)](#)
- [RFC 430x IPsec サポートの設定例 \(126 ページ\)](#)
- [RFC 430x IPsec サポートに関する追加のリファレンス \(127 ページ\)](#)
- [RFC 430x IPsec サポートに関する機能情報 \(128 ページ\)](#)

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「[Bug Search Tool](#)」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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、<http://www.cisco.com/go/cfn>に進みます。Cisco.com のアカウントは必要ありません。

RFC 430x IPsec サポートに関する情報

RFC 430x IPsec サポート フェーズ 1

RFC 430x IPsec サポートフェーズ 1 機能は、RFC 4301 で規定されているインターネット キー エクスチェンジ (IKE) と IPsec の動作を実装します。

RFC 4301 は IPsec に準拠したシステムの基本アーキテクチャを規定しています。RFC 4301 には、IPv4 と IPv6 の両方の環境で、IP レイヤのトラフィックに一連のセキュリティ サービスを提供する方法が記載されています。RFC 430x IPsec サポート フェーズ 1 機能は、Cisco IOS ソフトウェア上の次の RFC 4301 実装をサポートします。

- **Security association (SA) lifetime** : IPsec とインターネット キー エクスチェンジ (IKE) またはインターネット キー エクスチェンジ バージョン 2 (IKEv2) 間のセキュリティ アソシエーションのライフタイムは認証証明書のライフタイムを超えないようにする必要があります。
- **OPAQUE selectors** : OPAQUE は、対応するセクタフィールドが検証に使用できないことを示します。IKEv2 が OPAQUE セクタに遭遇すると、IKEv2 はスキップして、OPAQUE セクタを処理せず、ポリシー検証のために次のセクタに移動します。
- **Explicit Congestion Notification (ECN) support** : ECN は、IPsec パケットの復号時に伝播されるため、パケットの送信元と宛先がネットワーク内で発生した輻輳を認識することが保証されます。
- **Fragment processing** : ピアは、同じトンネル内で初期フラグメントと非初期フラグメントを送信しないようにする必要があります。初期フラグメントと非初期フラグメントを伝送するためのトンネルモード SA と非初期フラグメント用のトンネルモード SA を分ける必要があります。IPsec ピアは、バイパス トラフィックに適合するために、パケットの破棄とステートフルフラグメントチェックをサポートする必要があります。
- **Do not fragment-(DF) bit processing** : DF ビット処理は、SA 単位で設定する必要があります。
- **Dummy packet generation support** : トラフィックが IPsec SA トンネル経由で流れている場合に IPsec SA 経由でダミーパケットを送信してパケットをカプセル化できる必要があります。

RFC 430x IPsec サポート フェーズ 2

RFC 430x IPsec サポート フェーズ 2 機能は、Cisco IOS ソフトウェア上の Internet Control Message Protocol (ICMP) パケットの暗号化と復号化の RFC 4301 実装をサポートします。

ICMP エラーが発生すると、ICMP エラー メッセージが送信されます。たとえば、ホストが到達不能の場合は、中間デバイスが ICMP 要求の発信元にホストが到達不能であることを示すメッセージを送信します。ICMP エラー メッセージが IPsec 暗号化ポリシーに届いた場合は、既存の SA と一致するように分類されない可能性があります。そのため、パケットは ICMP エラーメッセージ内のデータに基づいて分類されます。このデータには、元の ICMP メッセージの送信元アドレスと宛先アドレスが含まれています。SA が ICMP エラーメッセージ内のアドレスに基づいて検出された場合は、その SA が使用されます。SA が存在しない場合は、ポリシーで許可されていれば、SA が作成されます。復号化では、有効な SA が見つからない場合に、ICMP エラーメッセージ内のデータに基づいて復号化後チェックが実行されます。

ICMP エラーメッセージの暗号化と復号は、**show crypto ipsec sa** コマンドの出力に表示される暗号化カウンタと復号カウンタを通して確認できます。

RFC 430x IPsec サポートの設定方法

RFC 430x IPsec サポートのグローバル設定

このタスクは、RFC 4301 実装をグローバルに設定するために実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec security-association dummy {pps rate | seconds seconds}**
4. **crypto ipsec security-association ecn {discard | propogate}**
5. **exit**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル構成モードを開始します。
ステップ 3	crypto ipsec security-association dummy {pps rate seconds seconds} 例： Device(config)# crypto ipsec security-association dummy seconds 5	IPSec トラフィック フロー内のダミー パケットの生成と送信を可能にします。
ステップ 4	crypto ipsec security-association ecn {discard propogate} 例： Device(config)# crypto ipsec security-association ecn discard	IPSec トラフィック フロー内の明示的輻輳通知 (ECN) 設定を可能にします。
ステップ 5	exit 例： Device(config-crypto-map)# exit	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

クリプト マップ単位の RFC 430x IPsec サポートの設定

このタスクは、RFC 4301 実装をクリプト マップ単位で設定するために実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map map-name seq-num ipsec-isakmp**
4. **set ipsec security-association dfbit {clear | copy | set}**
5. **set ipsec security-association dummy {pps rate | seconds seconds}**
6. **set ipsec security-association ecn {discard | propogate}**
7. **end**
8. **show crypto map ipsec sa**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル構成モードを開始します。
ステップ 3	crypto map map-name seq-num ipsec-isakmp 例 : Device(config)# crypto map cmap 1 ipsec-isakmp	作成または変更するクリプト マップ エントリを指定して、クリプト マップ 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	set ipsec security-association dfbit {clear copy set} 例 : Device(config-crypto-map)# set ipsec security-association dfbit set	クリプトマップ内の IPSec トラフィックフローのセキュリティ アソシエーション (SA) 単位の Do not Fragment (DF) ビット処理を有効にします。
ステップ 5	set ipsec security-association dummy {pps rate seconds seconds} 例 : Device(config-crypto-map)# set ipsec security-association dummy seconds 5	クリプトマップ内の IPSec トラフィックフロー用のダミー パケットの生成と送信を有効にします。

	コマンドまたはアクション	目的
ステップ 6	set ipsec security-association ecn {discard propagate} 例 : Device(config-crypto-map)# set ipsec security-association ecn propagate	クリプトマップ内の IPsec トラフィック フロー用の SA 単位の明示的輻輳通知 (ECN) 設定を有効にします。
ステップ 7	end 例 : Device(config-crypto-map)# end	クリプト マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 8	show crypto map ipsec sa 例 : Device# show crypto map ipsec sa	IPsec SA によって使用される設定を表示します。

例

次に、**show crypto map ipsec sa** コマンドの出力例を示します。

Device# **show crypto map ipsec sa**

```
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 3FFE:2002::32F7:DFF:FE54:7FD1
  protected vrf: (none)
  local ident (addr/mask/prot/port): (3FFE:2002::32F7:DFF:FE54:7FD1/128/47/0)
  remote ident (addr/mask/prot/port): (3FFE:2002::C671:FEFF:FE88:EB82/128/47/0)
  current_peer 3FFE:2002::C671:FEFF:FE88:EB82 port 500
    PERMIT, flags={origin_is_acl,}
  #pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
  #pkts decaps: 28, #pkts decrypt: 28, #pkts verify: 28
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0
  #send dummy packets 852600, #recv dummy packets 424905

  local crypto endpt.: 3FFE:2002::32F7:DFF:FE54:7FD1,
  remote crypto endpt.: 3FFE:2002::C671:FEFF:FE88:EB82
  plaintext mtu 1430, path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb GigabitEthernet0/0/1
  current outbound spi: 0xE963D1EC(3915633132)
  PFS (Y/N): N, DH group: none
  Dummy packet: Initializing

inbound esp sas:
  spi: 0xF4E01B9A(4108327834)
    transform: esp-3des esp-md5-hmac,
    in use settings = {Tunnel, }
    conn id: 2053, flow_id: ESG:53, sibling_flags FFFFFFFF80000049, crypto map: Tunnel0-head-0

  sa timing: remaining key lifetime (k/sec): (4608000/2343)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE(ACTIVE)

inbound ah sas:
```

```

inbound pcip sas:

outbound esp sas:
spi: 0xE963D1EC(3915633132)
transform: esp-3des esp-md5-hmac,
in use settings ={Tunnel, }
conn id: 2054, flow_id: ESG:54, sibling_flags FFFFFFFF80000049, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4608000/2343)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcip sas:

```

RFC 430x IPsec サポートの設定例

例：RFC 430x IPsec サポートのグローバル設定

次に、RFC 430x IPsec サポートをグローバルに設定する例を示します。

```

Device> enable
Device# configure terminal
Device(config)# crypto ipsec security-association dummy seconds 15
Device(config)# crypto ipsec security-association ecn propagate
Device(config-crypto-map)# exit

```

例：クリプト マップ単位の RFC 430x IPsec サポートの設定

次に、RFC 430x IPsec サポートをクリプト マップ単位で設定する例を示します。

```

Device> enable
Device# configure terminal
Device(config)# crypto map cmap 1 ipsec-isakmp
Device(config-crypto-map)# set security-association copy
Device(config-crypto-map)# set security-association dummy seconds 15
Device(config-crypto-map)# set security-association ecn propagate
Device(config-crypto-map)# end
Device# show crypto map ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 3FFE:2002::32F7:DFF:FE54:7FD1
protected vrf: (none)
local ident (addr/mask/prot/port): (3FFE:2002::32F7:DFF:FE54:7FD1/128/47/0)
remote ident (addr/mask/prot/port): (3FFE:2002::C671:FEFF:FE88:EB82/128/47/0)
current_peer 3FFE:2002::C671:FEFF:FE88:EB82 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
#pkts decaps: 28, #pkts decrypt: 28, #pkts verify: 28
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0

```

```
#send errors 0, #recv errors 0
#send dummy packets 852600, #recv dummy packets 424905

local crypto endpt.: 3FFE:2002::32F7:DFF:FE54:7FD1,
remote crypto endpt.: 3FFE:2002::C671:FEFF:FE88:EB82
plaintext mtu 1430, path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb GigabitEthernet0/0/1
current outbound spi: 0xE963D1EC(3915633132)
PFS (Y/N): N, DH group: none
Dummy packet: Initializing

inbound esp sas:
spi: 0xF4E01B9A(4108327834)
transform: esp-3des esp-md5-hmac,
in use settings ={Tunnel, }
conn id: 2053, flow_id: ESG:53, sibling_flags FFFFFFFF80000049, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4608000/2343)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcg sas:

outbound esp sas:
spi: 0xE963D1EC(3915633132)
transform: esp-3des esp-md5-hmac,
in use settings ={Tunnel, }
conn id: 2054, flow_id: ESG:54, sibling_flags FFFFFFFF80000049, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4608000/2343)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcg sas:
```

RFC 430x IPsec サポートに関する追加のリファレンス

関連資料

関連項目	マニュアルタイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

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 Commands A to C』 『Cisco IOS Security Command Reference Commands D to L』 『Cisco IOS Security Command Reference Commands M to R』 『Cisco IOS Security Command Reference Commands S to Z』
IKEv2 の設定	
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準および RFC

標準/RFC	タイトル
RFC 4301	『Security Architecture for the Internet Protocol』

テクニカル サポート

説明	リンク
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。	http://www.cisco.com/cisco/web/support/index.html

RFC 430x IPsec サポートに関する機能情報

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 トレー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、<https://cfnnng.cisco.com/>に進みます。Cisco.com のアカウントは必要ありません。

表 6: RFC430x IPsec サポートに関する機能情報

機能名	リリース	機能情報
RFC430x IPsec サポート フェーズ 1		RFC 430x IPsec サポート フェーズ 1 機能は、RFC 4301 で規定されているインターネット キー エクスチェンジ (IKE) と IPsec の動作を実装します。 次のコマンドが導入または変更されました。 crypto ipsec security-association dummy, crypto ipsec security-association ecn, set ipsec security-association dfbit, set ipsec security-association dummy, set ipsec security-association ecn, show crypto map ipsec sa.
RFC430x IPsec サポート フェーズ 2		RFC 430x IPsec サポート フェーズ 2 機能は、Cisco IOS ソフトウェア上の Internet Control Message Protocol (ICMP) パケットの暗号化と復号化の RFC 4301 実装をサポートします。 この機能に関して変更または更新されたコマンドはありません。

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。