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

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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

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.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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: http://www.cisco.com/go/trademarks.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.(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

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 4

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 5

IPsec を使用した VPN のセキュリティの設定に関する情報 6

サポートされる規格 6

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 14

Suite-B の要件 15

Suite-B の設定情報の入手先 15

IPsec VPN の設定方法 16

クリプト アクセス リストの作成 16

次の作業 17

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 17

制約事項 17

IKEv1 のトランスフォーム セットの設定 18

次の作業 19

IKEv2 のトランスフォーム セットの設定 20

IKEv2 のトランスフォーム セットの例 22

次の作業 23

クリプト マップ セットの作成 23
スタティック クリプト マップの作成 23
トラブルシューティングのヒント 26
次の作業 26
ダイナミック クリプト マップの作成 26
トラブルシューティングのヒント 31
次の作業 31
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 31
トラブルシューティングのヒント 34
次の作業 34
インターフェイスへのクリプト マップ セットの適用 35
IPsec VPN の設定例 36
例：AES ベースのスタティック暗号マップの設定 36
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 37
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 40
用語集 41
IPSec 仮想トンネル インターフェイス 43
機能情報の確認 43
IPsec 仮想トンネル インターフェイスの制約事項 44
IPsec 仮想トンネル インターフェイスに関する情報 44
IPsec 仮想トンネル インターフェイスを使用するメリット 45
スタティック仮想トンネル インターフェイス 45
ダイナミック仮想トンネル インターフェイス 46
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 47
ダイナミック仮想インターフェイスに対するマルチ SA サポート 49
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 50
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 50
FlexVPN 混合モードのサポート 50
IKE プロファイル ベースのトンネル選択 50
IPsec での自動トンネル モードのサポート 51
VTI に対する IPSec 混合モードのサポート 52
IPsec 仮想トンネル インターフェイスの設定方法 52

スタティック IPsec 仮想トンネル インターフェイスの設定 52
ダイナミック IPsec 仮想トンネル インターフェイスの設定 54
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 56
SVTI に対する IPsec 混合モードのサポートの設定 61
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 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 67
例：VRF 認識スタティック仮想トンネル インターフェイス 68
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 69
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 72
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 73
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
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 77
IPsec 仮想トンネル インターフェイスに関する機能情報 79
失効したピア証明書の暗号セッションの削除 83
機能情報の確認 83

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 84
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 84
暗号セッションの削除方法 84
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 85
暗号セッションの削除の有効化 85
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 86
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 87
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 87
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 87
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 88
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 89
暗号条件付きデバッグ サポート 91
機能情報の確認 91
暗号条件付きデバッグ サポートの前提条件 92
暗号条件付きデバッグ サポートの制約事項 92
暗号条件付きデバッグ サポートに関する情報 92
サポートされる条件タイプ 92
暗号条件付きデバッグ サポートのイネーブル化方法 94
暗号条件付きデバッグ メッセージのイネーブル化 94
パフォーマンス上の考慮事項 94
暗号条件付きデバッグのディセーブル化 95
暗号エラー デバッグ メッセージのイネーブル化 96
デバッグ暗号エラー CLI 96
暗号条件付きデバッグ CLI の設定例 97
暗号条件付きデバッグのイネーブル化の例 97
暗号条件付きデバッグのディセーブル化の例 98
その他の参考資料 98
暗号条件付きデバッグ サポートに関する機能情報 99
IPv4 GRE トンネル保護経由の IPv6 101
機能情報の確認 101
IPv4 GRE トンネル保護経由の IPv6 の前提条件 102
IPv4 GRE トンネル保護経由の IPv6 の制約事項 102

IPv4 GRE トンネル保護経由の IPv6 に関する情報 102
IPsec を使用した GRE トンネル 102
IPv4 GRE トンネル保護経由の IPv6 の設定方法 105
クリプト マップを使用した IPv4 GRE 暗号化経由の IPv6 の設定 105
トンネル保護を使用した IPv4 GRE 暗号化経由の IPv6 の設定 110
IPv4 GRE トンネル保護経由の IPv6 の設定例 113
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 113
トンネル保護を使用した IPv4 GRE 暗号化経由の IPv6 の設定例 114
その他の参考資料 114
IPv4 GRE トンネル保護経由の IPv6 に関する機能情報 115
RFC 430x IPsec サポート 117
機能情報の確認 117
RFC 430x IPsec サポートに関する情報 118
RFC 430x IPsec サポート フェーズ 1 118
RFC 430x IPsec サポート フェーズ 2 118
RFC 430x IPsec サポートの設定方法 119
RFC 430x IPsec サポートのグローバル設定 119
クリプト マップ単位の RFC 430x IPsec サポートの設定 120
RFC 430x IPsec サポートの設定例 122
例：RFC 430x IPsec サポートのグローバル設定 122
例：クリプト マップ単位の RFC 430x IPsec サポートの設定 122
RFC 430x IPsec サポートに関する追加のリファレンス 123
RFC 430x IPsec サポートに関する機能情報 125

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

現行の Cisco IOS XE リリース 3.7.0E（Catalyst スイッチ用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、1 つのバージョンの統合されたリリース（Cisco IOS XE 16）へと発展しています。これにより、スイッチングおよびルーティング ポートフォリオの幅広い範囲のアクセスおよびエッジ製品に 1 つのリリースで対応できます。

（注） 技術設定ガイドの機能情報の表には、機能が導入された時期が示されています。他のプラットフォームでその機能がサポートされた時期については示されていない場合があります。特定の機能がご使用のプラットフォームでサポートされているかどうかを特定するには、製品のランディング ページに示されている技術設定ガイドを参照してください。技術設定ガイドが製品のランディング ページに表示されている場合は、その機能がプラットフォームでサポートされていることを示します。

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） セキュリティの脅威とそれに対抗するための暗号化技術は常に変化しています。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。

- 機能情報の確認，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，5 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，6 ページ
- IPsec VPN の設定方法，16 ページ
- IPsec VPN の設定例，36 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，37 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，40 ページ
- 用語集，41 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、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

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

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、スタティック 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。

ネストされた IPsec トンネル

IPsecは、同一ルータで終端するネストされたトンネルをサポートします。ローカルで生成されたIKEパケットおよびIPsecパケットの二重暗号化がサポートされるのは、Static Virtual Tunnel Interface（sVTI）が設定されている場合だけです。二重暗号化は、Cisco IOS リリース 12.4(15)T まではサポートされますが、それ以降のリリースではサポートされません。

CSCts46591 では、次のネストされた IPsec トンネルがサポートされます。

- VTI 内の仮想トンネル インターフェイス（VTI）
- Generic Routing Encapsulation（GRE）/IPsec 内の VTI
- VTI 内の GRE/IPsec
- GRE/IPSec 内の GRE/IPsec

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。

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。

IPsec を使用した VPN のセキュリティの設定に関する情報

サポートされる規格

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 サービスのプロトコル全体および IKE セキュリティ プロトコル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 プロトコルです。IKE は他のプロトコルで使用されますが、その初期実装は IPsec プロトコルで使用されます。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。

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。

（注） DES、3DES、MD5（HMAC バリアントを含む）、および Diffie-Hellman（DH）グループ 1、2、および 5 の使用は推奨されていません。代わりに、AES、SHA、および DH グループ 14 以降を使用してください。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。

- AES：Advanced Encryption Standard（AES）。暗号アルゴリズムの 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 バリアント）：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アントです。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 サポートに関する詳細については、「Configuring Security for VPNs with IPsec」機能モジュールを参照してください。SHA-2 for ISAKMP は Cisco IOS XE 15.3(3)S 以降でサポートされます。
- Diffie-Hellman：公開キー暗号法プロトコルの 1 つで、2 者間に、セキュアでない通信チャネルによる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。2048 ビット以上の DH キー交換または ECDH キー交換の使用をお勧めします。
- MD5（ハッシュ ベースのメッセージ認証コード（HMAC）バリアント）：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 バリアントです。

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 モードで使用することではありません）。

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。

SA のセット（ピアへの発信）が確立されると、トリガーするパケットと後続の適用可能なパケットがルータを出るときにこの SA のセットが適用されます。「適用可能な」パケットとは、元のパケットが一致するのと同じアクセス リスト基準と一致するパケットです。たとえば、すべての適用可能なパケットを、リモート ピアに転送する前に暗号化できます。そのピアからの着信のトラフィックを処理するときには、対応する着信 SA が使用されます。

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、完全であるとみなされます。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 プロポーザルでは次のように異なります。

- 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）。

（注） Cisco IOS XE リリース内の同じトランスフォーム セットで AH アルゴリズムと ESP アルゴリズムを指定することはできません。

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 トランスフォーム（*1* つだけ選択）。	**ah-md5-hmac**	MD5（メッセージ ダイジェスト 5）（HMAC バリアント）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 バリアント）認証アルゴリズムを使用する AH。 AH と ESP のトランスフォーム セットの組み合わせは、Cisco IOS XE リリースではサポートされません。

トランスフォーム タイプ	トランスフォーム	説明
ESP暗号化トランスフォーム（*1* つだけ選択）。	**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-gcm **esp-gmac**	**esp-gcm** トランスフォームと **esp-gmac** トランスフォームは、128 ビットまたは 256 ビットの暗号化アルゴリズムを使用する ESP です。これらのトランスフォームのデフォルトは、いずれも 128 ビットです。 **esp-gcm** トランスフォームと **esp-gmac** トランスフォームは、いずれも **cryptoipsectransform-set** コマンドを使用して同じ暗号 IPsec トランスフォーム セット内の他の ESP トランスフォームと一緒に設定することはできません。 esp-gcm と esp-gmac の組み合わせは、次の ESP を使用した Cisco ASR 1001 ルータではサポートされません。 • ESP-5 • ESP-10 • ESP-20 • ESP-40
	esp-aes192	192 ビット AES 暗号化アルゴリズムを使用する ESP。
	esp-aes256	256 ビット AES 暗号化アルゴリズムを使用する ESP。

トランスフォーム タイプ	トランスフォーム	説明
	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）。 （注） ESP-100 または ESP-200 を使用した Cisco ASR 1001-X および Cisco ASR 1002-X ルータ上で DES、3DES、または GMAC トランスフォームを使用する場合は、AES や GCM に比べてパフォーマンスが 30% 低下する可能性があります。
	esp-3des	168 ビット DES 暗号化アルゴリズム（3DES、トリプル DES とも呼ばれる）を使用する ESP。（非推奨）。
	esp-null	ヌル暗号化アルゴリズム。
ESP認証トランスフォーム（*1* つだけ選択）。	**esp-md5-hmac**	MD5（HMAC バリアント）認証アルゴリズムを使用する ESP。（非推奨）。
	esp-sha-hmac	SHA（HMAC バリアント）認証アルゴリズムを使用する ESP。

（注） セキュリティの脅威とそれに対抗するための暗号化技術は常に変化しています。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、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。

Suite-B は次のハードウェア プラットフォームではサポートされません。

- Cisco ASR1001
- ESP-5
- ESP-10
- ESP-20
- ESP-40

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 バリアント）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. イネーブル化
2. **configure terminal**
3. 次のいずれかを実行します。
   - **access-list***access-list-number* {**deny** | **permit**} *protocolsourcesource-wildcarddestinationdestination-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

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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	次のいずれかを実行します。
	• **access-list***access-list-number* {**deny** | **permit**} *protocolsourcesource-wildcarddestinationdestination-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。

	コマンドまたはアクション	目的
		ヒント　IPsec で使用できるように "mirror image" クリプト アクセス リストを設定することを推奨します。また、**any** キーワードを使用することは推奨しません。
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

クリプト アクセス リストを 1 つ以上作成したら、トランスフォーム セットを「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」の手順に従って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」と「インターフェイスへのクリプトマップセットの適用」の手順に従ってください）。

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。

制約事項

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. イネーブル化
2. **configure terminal**
3. **crypto ipsec transform-set***transform-set-nametransform1* [*transform2* [*transform3*]]
4. **mode** [**tunnel** | **transport**]
5. **end**
6. **clear crypto sa** [**peer** {*ip-address* | *peer-name*} | **sa map***map-name* | **sa entry***destination-addressprotocolspi*]
7. **show crypto ipsec transform-set** [**tag***transform-set-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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	**crypto ipsec transform-set***transform-set-nametransform1* [*transform2* [*transform3*]] 例： `Device(config)# crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac`	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： `Device(cfg-crypto-tran)# mode transport`	（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）。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(cfg-crypto-tran)# end`	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-addressprotocolspi*] 例： `Device# clear crypto sa`	（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： `Device# show crypto ipsec transform-set`	（任意）設定済みのトランスフォーム セットを表示します。

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. イネーブル化
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

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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	**crypto ikev2 proposal***proposal-name* 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 • 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）。

	コマンドまたはアクション	目的
ステップ 5	**integrity***transform1* [*transform2*] ... 例： `Device(config-ikev2-proposal)# integrity sha1`	（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 バリアント）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 バリアント）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 バリアント）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 バリアント）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 バリアント）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： `Device(config-ikev2-proposal)# group 14`	（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。 • **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。

	コマンドまたはアクション	目的
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、「IPsec を使用した VPN のセキュリティの設定」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） セキュリティの脅威とそれに対抗するための暗号化技術は常に変化しています。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. イネーブル化
2. **configure terminal**
3. **crypto map** [**ipv6**] *map-nameseq-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* | **kilobytesdisable**}
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

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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	**crypto map** [**ipv6**] *map-nameseq-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 で保護する必要の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 aesset`	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。
ステップ 8	**set security-association lifetime** {**seconds***seconds* | **kilobytes***kilobytes* | **kilobytesdisable**}	（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。

	コマンドまたはアクション	目的
	例： `Device (config-crypto-m)# set security-association lifetime seconds 2700`	• 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： `Device(config-crypto-m)# set security-association level per-host`	（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ームによって急速にリソースが消費される可能性があるので、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： `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。 • 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。

	コマンドまたはアクション	目的
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」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） セキュリティの脅威とそれに対抗するための暗号化技術は常に変化しています。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. イネーブル化
2. **configure terminal**
3. **crypto dynamic-map***dynamic-map-namedynamic-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* | **kilobytesdisable**}
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-nameseq-num***ipsec-isakmpdynamic***dynamic-map-name* [**discover**]
14. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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。

	コマンドまたはアクション	目的
ステップ 3	**crypto dynamic-map***dynamic-map-namedynamic-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 aesset`	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 マップでは、アクセスリストの使用は任意ですが、使用することを強く推奨します。 • 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

	コマンドまたはアクション	目的
		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。 • 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 エントリでは、これを設定することはまれです。ダイナミック クリプト マップ エントリは、多くの場合、未知のリモート ピアで使用されます。
ステップ 7	**set security-association lifetime** {**seconds***seconds* | **kilobytes***kilobytes* | **kilobytesdisable**} 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にパケット損失が発生する可能性を最小限にするには、大量のライフタイム有効期限によってトリガーされるキーの再生成要求をディセーブルにできます。
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）

	コマンドまたはアクション	目的
		• 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。 • 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い場合は、**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-nameseq-num***ipsec-isakmpdynamic***dynamic-map-name* [**discover**]	（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

	コマンドまたはアクション	目的
	例： `Device(config)# crypto map static-map 1 ipsec-isakmp dynamic test-map discover`	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。 （注） TED を有効にするには、**discover** キーワードを入力する必要があります。
ステップ 14	**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。

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」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. イネーブル化
2. **configure terminal**
3. **crypto map** [**ipv6**] *map-nameseq-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***spihex-key-string*
   - **set session-key outbound ah***spihex-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

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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	**crypto map** [**ipv6**] *map-nameseq-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。

	コマンドまたはアクション	目的
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、トランスフォーム セットを 1 つだけ指定できます。

ステップ 7	次のいずれかを実行します。
	• **set session-key inbound ah***spihex-key-string*
	• **set session-key outbound ah***spihex-key-string*
	
	例：
	`Device(config-crypto-m)# set session-key inbound ah 256 98765432109876549876543210987654`
	
	例：
	`Device(config-crypto-m)# set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc`
		指定されたトランスフォーム セットに AH プロトコルが含まれている場合、保護対象の着信および発信トラフィックに適用する AH セキュリティ パラメータ インデックス（SPI）およびキーを設定します
		• 保護するトラフィックに使用する AH セキュリティ アソシエーションを手動で指定します。

ステップ 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*]	指定されたトランスフォーム セットに ESP プロトコルが含まれている場合、保護対象の着信および発信トラフィックに適用する Encapsulating Security Payload（ESP）セキュリティ パラメータ インデックス（SPI）およびキーを設定します。 または トランスフォーム セットに ESP 暗号化アルゴリズムが含まれている場合は、暗号キーを指定します。トランスフォーム

	コマンドまたはアクション	目的

	例：
	`Device(config-crypto-m)# set session-key inbound esp 256 cipher 0123456789012345`
	
	例：
	`Device(config-crypto-m)# set session-key outbound esp 256 cipher abcdefabcdefabcd`
		セットに ESP 認証アルゴリズムが含まれている場合は、認証キーを指定します。
		• 保護するトラフィックに使用する ESP セキュリティ アソシエーションを手動で指定します。

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 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

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」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. イネーブル化
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

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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	**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。
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。

	コマンドまたはアクション	目的
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 aesset esp-aes 256 esp-sha-hmac
 mode transport
!
crypto map aesmap 10 ipsec-isakmp
 set peer 10.0.110.1
 set transform-set aesset
 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 コンフィギュレーション コマンド：完全なコマンド構文、コマンドモード、デフォルト設定、使用に関する注意事項および例	• 『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』
IKE 設定	「*Configuring Internet Key Exchange for IPsec VPNs*」
Suite-B SHA-2 ファミリ（HMAC バリアント）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	「*Configuring Certificate Enrollment for a PKI*」
推奨される暗号化アルゴリズム	次世代暗号化

標準

標準	Title
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、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
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)*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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 トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *2*：***IPsec VPN*** の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	Cisco IOS XE Release 2.1	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**。

機能名	ソフトウェア リリース	機能情報
AAA サーバを使用する IKE 共有秘密	Cisco IOS XE Release 2.1	AAA サーバを使用した IKE 共有秘密機能は、AAA サーバからのキー ルックアップを可能にします。 Cisco IOS XE リリース 2.1 では、この機能が Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されていました。
IOS ソフトウェア暗号での Suite-B のサポート	Cisco IOS XE Release 3.7S	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、次のコマンドが変更されました。**crypto ipsec transform-set**。

用語集

アンチ リプレイ：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て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。

データ認証：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）。

データの機密性：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。

データ フロー：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**いずれか**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 キー交換）の略。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。

ピア：ここでのピアとは、IPsec に参加するルータまたはその他の装置です。

PFS：Perfect Forward Secrecy（完全転送秘密）。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：セキュリティ アソシエーション（SA）。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て、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。

トランスフォーム：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。

トンネル：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） セキュリティの脅威とそれに対抗するための暗号化技術は常に変化しています。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。

- 機能情報の確認，43 ページ
- IPsec 仮想トンネル インターフェイスの制約事項，44 ページ
- IPsec 仮想トンネル インターフェイスに関する情報，44 ページ
- IPsec 仮想トンネル インターフェイスの設定方法，52 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，77 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，79 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、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IPsec 仮想トンネル インターフェイスの制約事項

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 モードでだけです。

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。

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。

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大幅に簡易化され、カプセル化に Generic Routing Encapsulation（GRE）または Layer 2 Tunneling Protocol（L2TP）を使用するよりも簡単な代替手段を利用できます。IPsec VTI に関連した大きな利点は、設定に、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 マッピングが不要であることです。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。

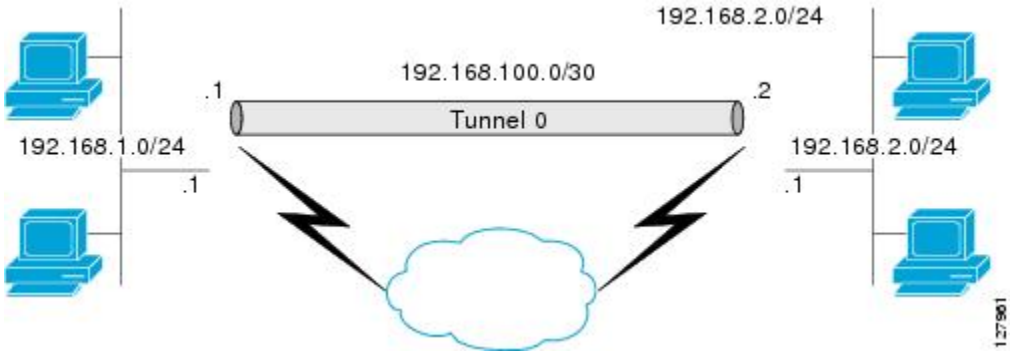
スタティック仮想トンネル インターフェイス

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。

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。

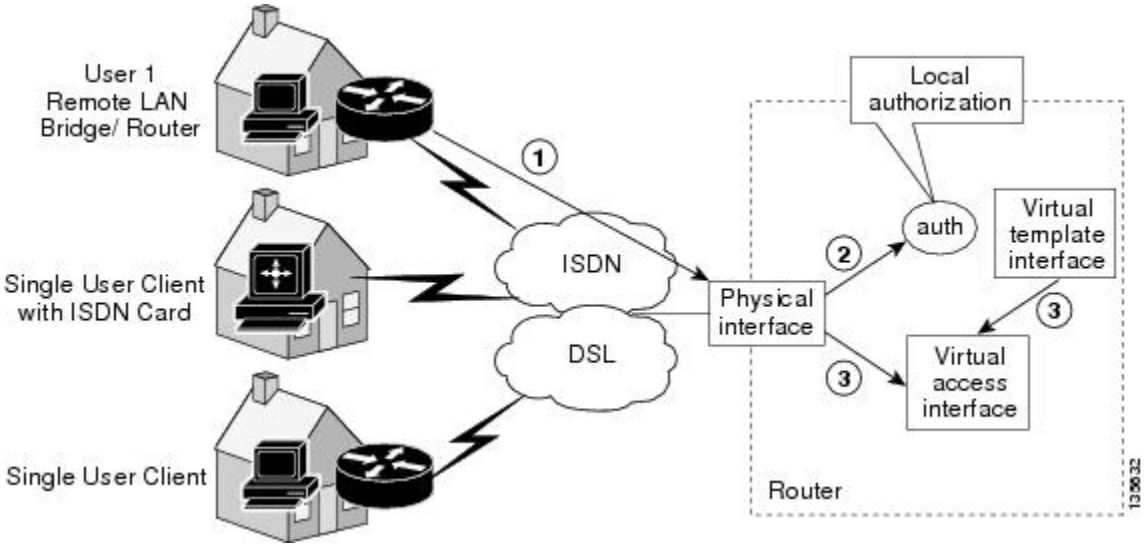
DVTI によって、IP アドレスを効率的に使用できるようになり、また、セキュアな接続を実現できます。DVTI によって、動的にダウンロード可能な、グループごとおよびユーザごとのポリシーを RADIUS サーバ上で設定できます。グループ単位またはユーザ単位の定義は、拡張認証（Xauth）User または Unity グループを使用して作成することも、証明書から抽出することもできます。DVTI は、標準ベースです。そのため、複数のベンダー環境における相互運用性がサポートされます。IPsec DVTI を使用すれば、リモート アクセス VPN 用のセキュリティ保護が強化された接続を作成できます。また、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。

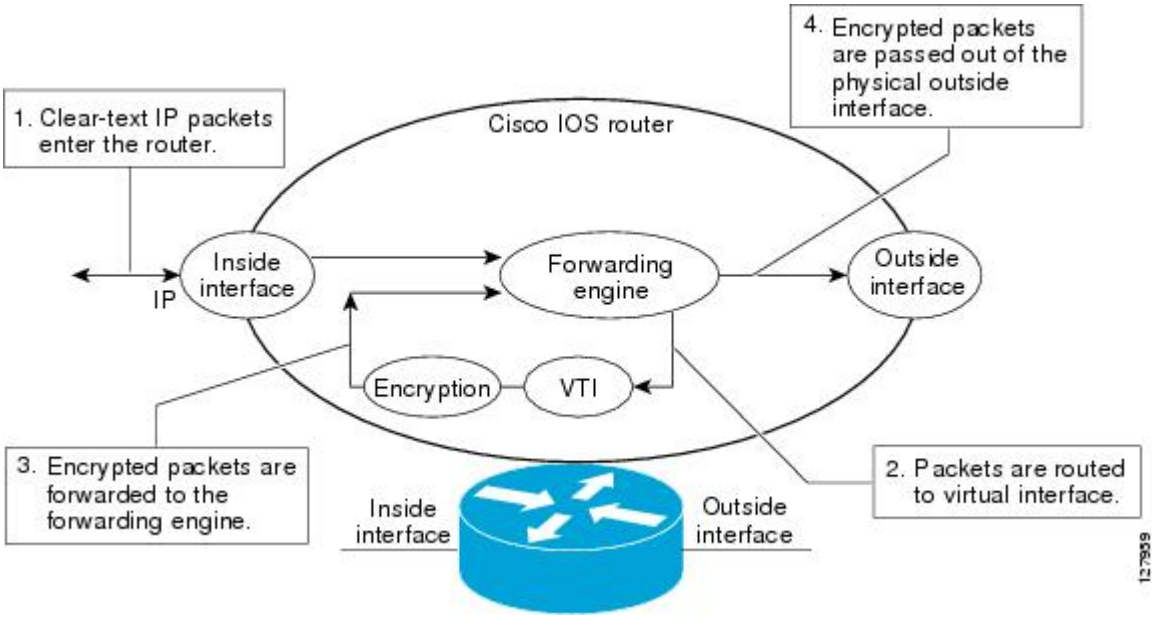
1. ユーザ 1 がルータを呼び出します。
2. ルータ 1 によって ユーザ 1 が認証されます。
3. IPsec によって、仮想テンプレート インターフェイスから仮想アクセス インターフェイスがコピーされます。

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。

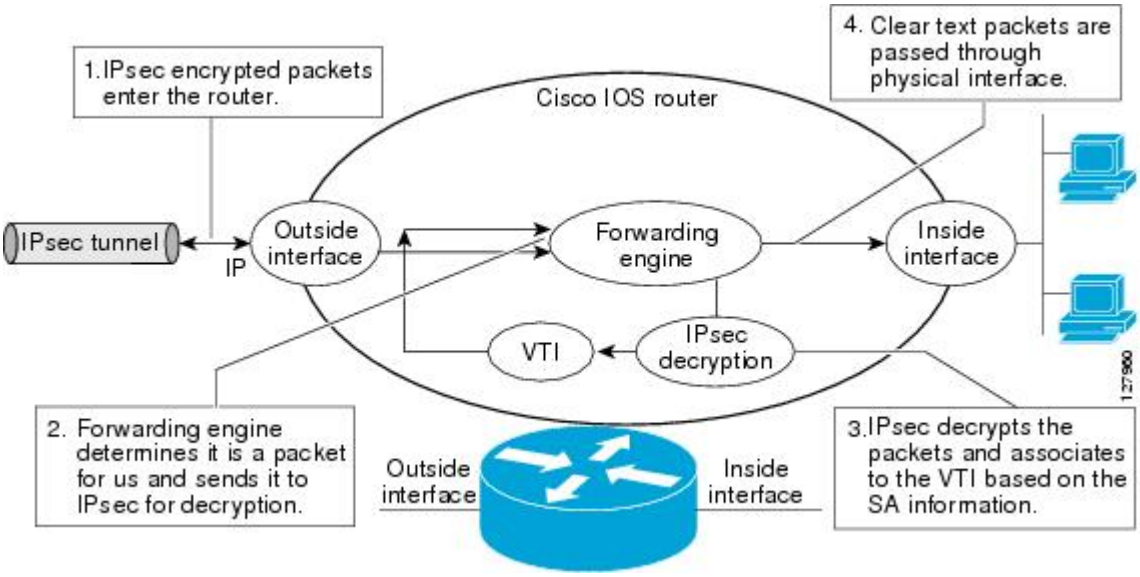
図 3 : *IPsec* トンネルへのパケット フロー



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



ダイナミック仮想インターフェイスに対するマルチ SA サポート

DVTI は、複数の IPsec SA をサポートします。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。

DVTI を使用すれば、専用のインターフェイス上でピア単位の機能を適用することができます。仮想アクセス インターフェイス上で適用されるすべての機能が、暗号の適用前に適用されるように機能を順序付けることができます。加えて、物理インターフェイス上で適用されるすべての機能が、暗号の適用後に適用されます。暗号化の前に VRF 間のトラフィックが漏洩しないように、すべての VRF でクリーン ルーティングを使用できます。

マルチ SA VTI は、サードパーティ製デバイスとの相互運用を保証し、柔軟で、クリーンで、モジュール式の機能セットを提供します。

Cisco IOS XE ソフトウェアがクリプト マップのみを実装したサードパーティ製デバイスと相互運用している場合でも、マルチ SA VTI はクリーンな Cisco IOS XE インフラストラクチャを可能にします。

ベースライン設定の VRF と拡張性：

仮想アクセスインスタンスは、テンプレート設定から Inside-VRF（IVRF）を継承します。ユーザは、顧客ごとに異なる IVRF を適用するためにテンプレートを複数設定する必要があります。テンプレートの数は、ヘッドエンドに接続されている顧客の数と一致する必要があります。このような設定は、テンプレートを宣言するたびにインターフェイス記述子ブロック（IDB）が 1 つずつ消費されるため、複雑になり、望ましいものではないうえ、パフォーマンスにも影響を与えます。

この複雑さは、IKE プロファイルに設定された VRF を使用して仮想アクセス VRF をオーバーライドすることによって回避できます。より良い解決策は、IKE プロファイルで AAA を使用して仮想アクセス VRF をオーバーライドする方法ですが、この方法は IKEv2 でしかサポートされません。

ISAKMP プロファイル内で設定された VRF は、最初に、仮想アクセスに適用されます。その後で、仮想テンプレートからの設定が仮想アクセスに適用されます。仮想テンプレートに **ip vrf forwarding** コマンド設定が含まれている場合は、このテンプレートからの VRF によって ISAKMP プロファイルからの VRF がオーバーライドされます。

VRF の初期設定に関するルール：

次のルールを VRF の初期設定中に適用する必要があります。

- IVRF を IKE プロファイル内で設定して、仮想テンプレート内では設定しなかった場合は、この IKE プロファイルから抽出された仮想アクセスごとに IKE プロファイルからの VRF を適用する必要があります。
- VRF を IKE プロファイル内と仮想テンプレート内で設定した場合は、仮想テンプレート IVRF が優先されます。

VRF の変更に関するルール：

IKE プロファイル内で設定された VRF を変更すると、このプロファイルから抽出されたすべての IKE SA、IPSec SA、および仮想アクセス識別子が削除されます。同じルールが、VRF を初めて IKE プロファイル上で設定するときも適用されます。

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。

IKE プロファイル ベースのトンネル選択

IKE プロファイル ベースのトンネル選択機能は、インターネット キー エクスチェンジ（IKE）プロファイル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）プロファイルを使用して IPsec セッション用のトンネル インターフェイスを選択します。**tunnel protection** コマンドで **isakmp-profile** キーワードまたは **ikev2-profile** キーワードを使用して、それぞれ、IKE プロファイルまたは IKEv2 プロファイルを指定します。

IKE プロファイル ベースのトンネル選択機能を使用すれば、トンネル インターフェイスで、IPSec セキュリティ アソシエーション データベース（SADB）を共有しなくても、トンネル送信元 IP アドレスと IPSec トランスフォーム セットを共有できるため、次のようなメリットがあります。

- トンネルはセキュアで、トラフィック漏洩がない。
- すべてのトンネル タイプがサポートされる。
- レガシー VPN テクノロジーからの設定を新しい VPN テクノロジーを使用したローカル アドレスと共存および共有するように調整することによる IKEv1 から IKEv2 へのシームレスな移行。
- 同じローカル アドレスまたはリモート アドレスを共有しているピア間で複数の IKE トンネルと IPSec トンネルをセットアップできる。

IKEv2 プロファイルは、ikev2 セッションを開始するために IPsec プロファイル内で手動で適用する必要があります。レスポンダでは、IPsec が着信接続を受け入れるように、ダイナミック仮想トンネル インターフェイス（DVTI）IKEv2 プロファイルを IPsec プロファイルに基づいて手動で適用する必要があります。DVTI レスポンダでは、IPsec がプロポーザル要求を検証するために仮想テンプレートに基づいて設定された親 IKE プロファイルを使用します。IKE プロファイルが IPsec プロファイル上で設定されていない場合は、デフォルトで、IPsec が IKE セッションを開始して受け入れます。IPsec プロファイル上で IKE プロファイルと IKEv2 プロファイルを同時に設定することはできません。IPsec プロファイル上で IKE プロファイルと IKEv2 プロファイルを設定すると、IKE プロファイルが IKEv2 プロファイルによってオーバーライドされます。

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ダの技術的詳細がわかっている必要があります。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、レスポンダ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 Windows7 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、レスポンダ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。

トンネル モード自動選択機能は、仮想トンネル インターフェイス設定で **tunnel mode** コマンドの **auto** キーワードを使用してアクティブにすることができます。

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. イネーブル化
2. **configureterminal**
3. **cryptoIPsecprofile***profile-name*
4. **settransform-set***transform-set-name* [*transform-set-name2...transform-set-name6*]
5. **exit**
6. **interface***typenumber*
7. **ipaddress***addressmask*
8. **tunnel mode ipsec ipv4**
9. **tunnelsource***interface-typeinterface-type*
10. **tunneldestination***ip-address*
11. **tunnelprotectionIPsecprofile***profile-name* [**shared**]
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**cryptoIPsecprofile***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	**settransform-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***typenumber* 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	**ipaddress***addressmask* 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	**tunnelsource***interface-typeinterface-type* 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。

	コマンドまたはアクション	目的
ステップ 10	**tunneldestination***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	**tunnelprotectionIPsecprofile***profile-name* [**shared**] 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 IPsec 仮想トンネル インターフェイスの設定

手順の概要

1. イネーブル化
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*
7. 次のいずれかを実行します。
   - **tunnel mode ipsec ipv4**
   - **tunnel mode auto**
8. **tunnel protection IPsec profile***profile-name* [**shared**]
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

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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	**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* 例： `Device(config)# interface virtual-template 2`	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	次のいずれかを実行します。 • **tunnel mode ipsec ipv4** • **tunnel mode auto** 例： `Device(config-if)# tunnel mode ipsec ipv4`	トンネルのモードを定義します。

	コマンドまたはアクション	目的
ステップ 8	**tunnel protection IPsec profile***profile-name* [**shared**] 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。
ステップ 11	**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 12	**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 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） セキュリティの脅威とそれに対抗するための暗号化技術は常に変化しています。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. イネーブル化
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. **tunnelmodeipsecipv4**
24. **tunnel protection profile ipsec***profile-name* [*shared*]
25. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。
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。

	コマンドまたはアクション	目的
ステップ 3	**ip vrf***vrf-name* 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***route-distinguisher* 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***keyring-name* 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***address***key***key* 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。
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。

	コマンドまたはアクション	目的
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。
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。

	コマンドまたはアクション	目的
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	**tunnelmodeipsecipv4** 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* [*shared*] 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. イネーブル化
2. **configureterminal**
3. **cryptoIPsecprofile***profile-name*
4. **settransform-set***transform-set-name* [*transform-set-name2...transform-set-name6*]
5. **exit**
6. **interface***typenumber*
7. **ipaddress***addressmask*
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. **tunnelsource***interface-typeinterface-type*
10. **tunneldestination***ip-address*
11. **tunnelprotectionIPsecprofile***profile-name*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**cryptoIPsecprofile***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。

	コマンドまたはアクション	目的
ステップ 4	**settransform-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***typenumber* 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	**ipaddress***addressmask* 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	**tunnelsource***interface-typeinterface-type* 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	**tunneldestination***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。

	コマンドまたはアクション	目的
ステップ 11	**tunnelprotectionIPsecprofile***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。

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. イネーブル化
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*
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

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	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 コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec 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 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***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 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。
ステップ 7	**interface virtual-template***number* 例： `Device(config)# interface virtual-template 2`	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。

	コマンドまたはアクション	目的
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。

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 **ipvrfforwarding** コマンドを設定に含めます。

Cisco 7206 ルータのコンフィギュレーション

```
hostname cisco 7206
.
.
ip vrf sample-vti1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
.
.
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** 文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。

Cisco 7206 ルータのコンフィギュレーション

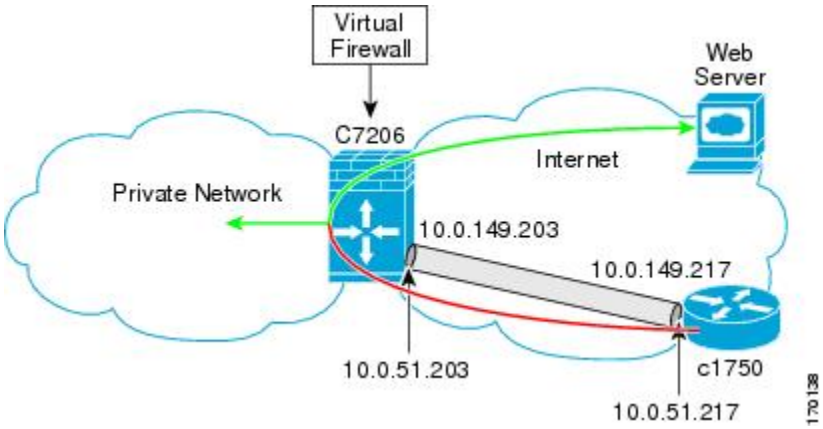
```
hostname cisco 7206
.
.
class-map match-all VTI
 match any
!
policy-map VTI
  class VTI
  police cir 2000000
    conform-action transmit
    exceed-action drop
!
.
.
interface Tunnel0
 ip address 10.0.51.217 255.255.255.0
 tunnel source 10.0.149.217
 tunnel destination 10.0.149.203
 tunnel mode ipsec 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。

Cisco 7206 ルータのコンフィギュレーション

```
hostname cisco 7206
.
.
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-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：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。

Cisco 7206 ルータのコンフィギュレーション

```
hostname cisco 7206
!
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。

```
hostname cisco 7206
!
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 ASR 1000
!
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 cisco 7206
```

```
!
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-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 ASR 1000
!
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 ASR 1000
.
.
.
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
!
.
.
.
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

DVTI Easy 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 cisco 7206
.
.
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 基本設定をの例を示します。

```
hostname cisco 7206
.
.
class-map match-all VTI
 match any
!
policy-map VTI
  class VTI
  police cir 2000000
    conform-action transmit
    exceed-action drop
!
.
.
interface Virtual-Template1 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
```

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』

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』
IPsec の設定	*IPsec を使用した VPN のセキュリティの設定*
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	次世代暗号化

標準および RFC

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

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *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	Cisco IOS XE Release 2.1	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	Cisco IOS XE Release 3.10S	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
IKEプロファイルベースのトンネル選択	Cisco IOS XE Release 3.10S	プロファイル ベースのトンネル選択機能は、インターネット キー エクスチェンジ（IKE）プロファイル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）プロファイルを使用して IPsec セッション用のトンネル インターフェイスを選択します。そのため、トンネル インターフェイスで、IPsec セキュリティ アソシエーションデータベース（SADB）を共有しなくても、トンネル送信元 IP アドレスと IPsec トランスフォーム セットを共有できます。 次のコマンドが導入または変更されました。**tunnel protection ipsec profile**。
ダイナミック VTI に対するマルチ SA	Cisco IOS XE Release 3.2S	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	Cisco IOS XE Release 2.1	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。

機能名	リリース	機能の設定情報
トンネル モード自動選択	Cisco IOS XE リリース 3.12S	トンネル モード自動選択機能は、設定を容易にし、レスポンダ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。**tunnel mode**。
IPsec VTI に対する混合モード		混合モード機能は、トンネリング対象のトラフィックが IPv4 と IPv6 の両方ではなくどちらかの場合のサポートを提供します。この実装は、IKEv1 と IKEv2 の両方に対して VTI の混合モードのみをサポートします。 次のコマンドが導入または変更されました。**tunnel mode**、**crypto ipsec profile**。

第 4 章

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，83 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，84 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情報，84 ページ
- 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，85 ページ
- 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，87 ページ
- 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，88 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機能情報，89 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、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

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

1. 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。
2. 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。
3. 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が検証されます。

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。

手順の概要

1. イネーブル化
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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear crypto session** 例： `Device# clear crypto session`	（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。 （注） このコマンドは、以前確立したセッションの機能を有効にするために使用します。そうでない場合は、機能が新しいセッションでのみ有効になります。

	コマンドまたはアクション	目的
ステップ 3	**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 4	次のいずれかを実行します。
	• **crypto isakmp disconnect-revoked-peers**
	• **crypto ikev2 disconnect-revoked-peers**
	
	例：
	`Device(config)# crypto isakmp disconnect-revoked-peers`
	
	例：
	`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** 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、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。

手順の概要

1. イネーブル化
2. **show crypto isakmp peers**
3. **show crypto ikev2 session detail**

手順の詳細

ステップ 1　イネーブル化

例：
`Device> enable`

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

ステップ 2 **show crypto isakmp peers**

例：
```
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**

例：
```
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	次世代暗号化

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *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	Cisco IOS XE リリース 3.13S	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。 この機能は、Cisco IOS XE リリース 3.13S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 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，91 ページ
- 暗号条件付きデバッグ サポートの前提条件，92 ページ
- 暗号条件付きデバッグ サポートの制約事項，92 ページ
- 暗号条件付きデバッグ サポートに関する情報，92 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，94 ページ
- 暗号条件付きデバッグ CLI の設定例，97 ページ
- その他の参考資料，98 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，99 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、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

暗号条件付きデバッグ サポートの前提条件

新しい暗号 CLI を使用するには、Cisco IOS XE リリースで k9 サブシステム暗号イメージを使用する必要があります。

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（**debugcryptocondition**、**debugcryptoconditionunmatched**、および **showcryptodebug-condition**）を使用すれば、条件（フィルタ値）を指定して、その条件を満たすデバッグ 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。

条件タイプ（キーワード）	説明
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。
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。

条件タイプ（キーワード）	説明
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ギン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

1. イネーブル化
2. **debugcryptocondition** [**connid***integer***engine-id***integer*] [**flowid***integer***engine-id***integer*] [**fvrf***string*] [**ivrf***string*] [**peer** [**group***string*] [**hostname***string*] [**ipv4***ipaddress*] [**subnet***subnetmask*] [**username***string*]] [**spi***integer*] [**reset**]
3. **showcryptodebug-condition**{[**peer**] [**connid**] [**spi**] [**fvrf**] [**ivrf**] [**unmatched**]}
4. **debugcryptoisakmp**
5. **debugcryptoipsec**
6. **debugcryptoengine**
7. **debugcryptoconditionunmatched** [**isakmp** | **ipsec** | **engine**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debugcryptocondition** [**connid***integer***engine-id***integer*] [**flowid***integer***engine-id***integer*] [**fvrf***string*] [**ivrf***string*] [**peer** [**group***string*] [**hostname***string*] [**ipv4***ipaddress*] [**subnet***subnetmask*] [**username***string*]] [**spi***integer*] [**reset**] 例： `Router# debug crypto condition connid 2000 engine-id 1`	条件付きデバッグ フィルタを定義します。

	コマンドまたはアクション	目的
ステップ 3	**showcryptodebug-condition**{[**peer**] [**connid**] [**spi**] [**fvrf**] [**ivrf**] [**unmatched**]} 例： `Router# show crypto debug-condition spi`	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	**debugcryptoisakmp**
	
	例：
	
	`Router#`
	`debug crypto isakmp`
		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	**debugcryptoipsec**
	
	例：
	
	`Router#`
	`debug crypto ipsec`
		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	**debugcryptoengine**
	
	例：
	
	`Router#`
	`debug crypto engine`
		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	**debugcryptoconditionunmatched** [**isakmp** | **ipsec** | **engine**] 例： `Router# debug crypto condition unmatched ipsec`	（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。 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. イネーブル化
2. **debugcryptoisakmp** | **ipsec** | **engine**} **error**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debugcryptoisakmp** | **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	**Title**
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 Release、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	Title
なし	--

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、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、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *6*：暗号条件付きデバッグ サポートに関する機能情報

機能名	リリース	機能情報
暗号条件付きデバッグ サポート	Cisco IOS XE Release 2.1	暗号条件付きデバッグ サポート機能では、3 つの新規のコマンドライン インターフェイス（CLI）が導入され、これらのインターフェイスにより、ユーザは、ピア IP アドレス、暗号エンジンの接続 ID、およびセキュリティ パラメータ インデックス（SPI）などの事前に定義し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。

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，101 ページ
- IPv4 GRE トンネル保護経由の IPv6 の前提条件，102 ページ
- IPv4 GRE トンネル保護経由の IPv6 の制約事項，102 ページ
- IPv4 GRE トンネル保護経由の IPv6 に関する情報，102 ページ
- IPv4 GRE トンネル保護経由の IPv6 の設定方法，105 ページ
- IPv4 GRE トンネル保護経由の IPv6 の設定例，113 ページ
- その他の参考資料，114 ページ
- IPv4 GRE トンネル保護経由の IPv6 に関する機能情報，115 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、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

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

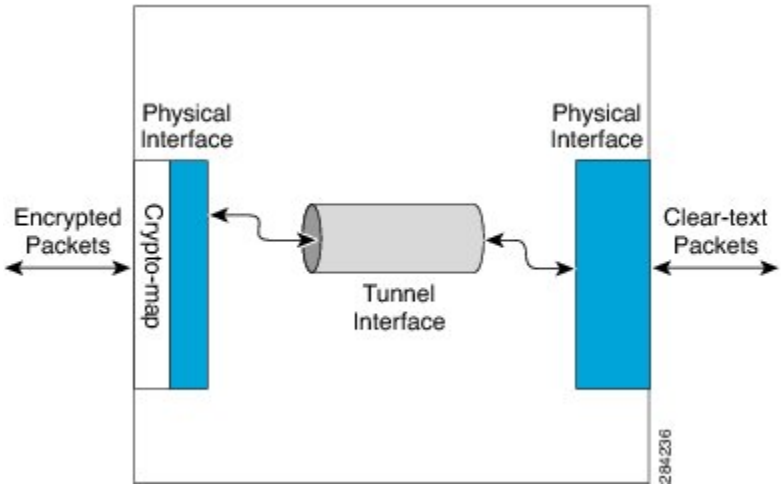
IPsec を使用した GRE トンネル

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。

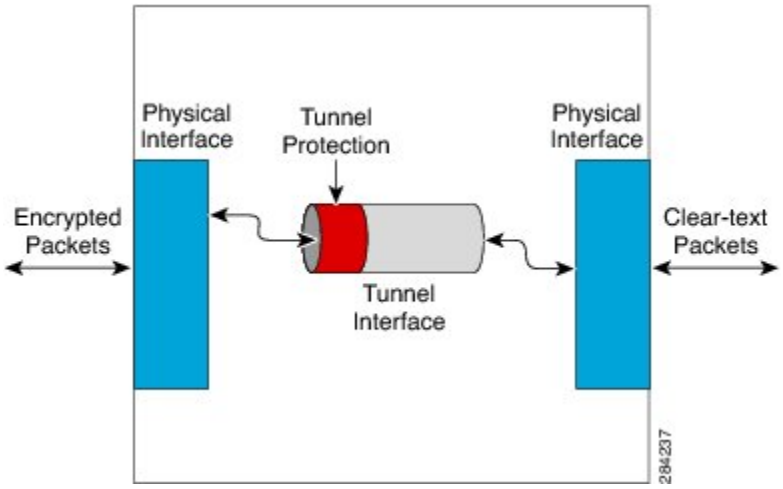
次の図に、物理インターフェイス上でクリプト マップを使用して、GRE トンネル インターフェイス経由でルータに入る暗号化されたパケットを示します。パケットは、復号化およびカプセル化解除されてから、クリア テキストとして IP 宛先に送られます。

図 *7*：クリプト マップを使用した *IPv4 GRE* トンネル暗号化経由の *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* トンネル暗号化経由の *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. イネーブル化
2. **configureterminal**
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-typeinterface-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. **cryptoisakmpkey***enc-type-digitkeystring* {**address***peer-address* [*mask*] | **ipv6** {*ipv6-address*/*ipv6-prefix*} | **hostname***hostname*} [**no-xauth**]
18. **cryptoipsectransform-set***transform-set-nametransform1* [*transform2*] [*transform3*] [*transform4*]
19. **access-list***access-list-number* [**dynamic***dynamic-name* [**timeout***minutes*]] {**deny** | **permit**} *protocolsource source-wildcarddestinationdestination-wildcard* [**precedence***precedence*] [**tos***tos*] [**time-range***time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]]
20. **crypto map** [**ipv6**] *map-nameseq-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

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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イネーブルにします。
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。*priority* 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。

	コマンドまたはアクション	目的
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	**cryptoisakmpkey***enc-type-digitkeystring* {**address***peer-address* [*mask*] | **ipv6** {*ipv6-address*/*ipv6-prefix*} | **hostname***hostname*} [**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 18	**cryptoipsectransform-set***transform-set-nametransform1* [*transform2*] [*transform3*] [*transform4*] 例： `Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des`	トランスフォーム セットを定義します。
ステップ 19	**access-list***access-list-number* [**dynamic***dynamic-name* [**timeout***minutes*]] {**deny** | **permit**} *protocolsource source-wildcarddestinationdestination-wildcard* [**precedence***precedence*] [**tos***tos*] [**time-range***time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]] 例： `Router(config)# access-list 110 permit gre host 192.168.0.16 host 172.16.0.12`	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-nameseq-num* [**ipsec-isakmp** [**dynamic***dynamic-map-name* | **discover** | **profile***profile-name*]] 例： `Router(config)# crypto map mymap 10 ipsec-isakmp`	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： `Router(config-crypto-map)# set peer 10.0.0.1`	クリプト マップ エントリ内の IP Security（IPsec）ピアを指定します。

	コマンドまたはアクション	目的
ステップ 22	**set transform-set***transform-set-name* [*transform-set-name2...transform-set-name6*] 例： `Router(config-crypto-map)# 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 23	**match address** [*access-list-id* | *name*] 例： `Router(config-crypto-map)# match address 102`	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： `Router(config-crypto-map)# 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 25	**interface***type number* 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***map-name* [**redundancy***standby-group-name* [**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. イネーブル化
2. **configureterminal**
3. **ipv6 multicast-routing**
4. **ipv6 unicast-routing**
5. **cryptoisakmppolicy***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. **cryptoisakmpkey***enc-type-digitkeystring* {**address***peer-address* [*mask*] | **ipv6** {*ipv6-address*/*ipv6-prefix*} | **hostname***hostname*} [**no-xauth**]
12. **cryptoipsectransform-set***transform-set-nametransform1* [*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. **ipv6address** {*ipv6-address*/*prefix-length* | *prefix-namesub-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. **tunnelsource**{*ip-address* | *ipv6-address* | *interface-typeinterface-number*}
20. **tunnel destination** {*hostname* | *ip-address* | *ipv6-address*}
21. **tunnel protectionipsec profile***name* [**shared**]
22. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
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する必要はありません。
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イネーブルにします。
ステップ 5	**cryptoisakmppolicy***priority* 例： `Router(config)# crypto isakmp policy 15`	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。*priority* 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： `Router(config-isakmp-policy)# authentication pre-share`	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： `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 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。

	コマンドまたはアクション	目的
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	**cryptoisakmpkey***enc-type-digitkeystring* {**address***peer-address* [*mask*] | **ipv6** {*ipv6-address*|*ipv6-prefix*} | **hostname***hostname*} [**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	**cryptoipsectransform-set***transform-set-nametransform1* [*transform2*] [*transform3*] [*transform4*] 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***profile-name* 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***transform-set-name* [*transform-set-name2...transform-set-name6*] 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***type number* 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。
ステップ 17	**ipv6address** {*ipv6-address*|*prefix-length* | *prefix-namesub-bits*|*prefix-length*} 例： `Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127`	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。

	コマンドまたはアクション	目的
ステップ 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**} 例： `Router(config-if)# tunnel mode gre ip`	GRE IPv6 トンネルを指定します。
ステップ 19	**tunnelsource**{*ip-address* | *ipv6-address* | *interface-typeinterface-number*} 例： `Router(config-if)# tunnel source 10.0.0.1`	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** {*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アドレスまたはホスト名を指定します。
ステップ 21	**tunnel protectionipsec profile***name* [**shared**] 例： `Router(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。
ステップ 22	**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。

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』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *7*：***IPv4 GRE*** トンネル保護経由の ***IPv6*** に関する機能情報

機能名	リリース	機能情報
IPv4 GRE トンネル保護経由の IPv6	Cisco IOS XE Release 3.5S	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 GRE を通過できるようにします。 この機能に関する詳細については、次の各項を参照してください。 • IPv4 GRE トンネル保護経由の IPv6 に関する情報 • IPv4 GRE トンネル保護経由の IPv6 の設定方法

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，117 ページ
- RFC 430x IPsec サポートに関する情報，118 ページ
- RFC 430x IPsec サポートの設定方法，119 ページ
- RFC 430x IPsec サポートの設定例，122 ページ
- RFC 430x IPsec サポートに関する追加のリファレンス，123 ページ
- RFC 430x IPsec サポートに関する機能情報，125 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、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

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。

- **セキュリティ アソシエーション（SA）ライフタイム**：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 セレクタ**：OPAQUE は、対応するセレクタ 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 セレクタに遭遇すると、IKEv2 はスキップして、OPAQUE セレクタを処理せず、ポリシー検証のために次のセレクタに移動します。
- **明示的輻輳通知（ECN）サポート**：ECN は、IPsec パケットの復号化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。
- **フラグメント処理**：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）ビット処理**：DF ビット処理は、SA 単位で設定する必要があります。
- **ダミー パケット生成サポート**：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化は、**show crypto ipsec sa** コマンドの出力に表示される暗号カウンタと復号カウンタを通して確認できます。

ICMP エラー メッセージの分類を表示するには、条件付き debug コマンドの **debug platform condition feature ipsec dataplane submode feature level info**、**debug platform condition both**、および **debug platform condition start** を使用します。

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. イネーブル化
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

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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	**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。

	コマンドまたはアクション	目的
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. イネーブル化
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

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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。

	コマンドまたはアクション	目的
ステップ 3	**crypto map***map-nameseq-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。
ステップ 6	**set ipsec security-association ecn** {**discard** | **propogate**} 例： `Device(config-crypto-map)# set ipsec security-association ecn propogate`	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。

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 pcp 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 pcp 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 propogate
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 propogate
```

```
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 pcp 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 pcp 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	「Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site」
推奨される暗号化アルゴリズム	次世代暗号化

標準および RFC

標準/RFC	Title
RFC 4301	『*Security Architecture for the Internet Protocol*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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 トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *8*：***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	Cisco IOS XE リリース 3.12S	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**。

機能名	リリース	機能情報
RFC430x IPsec サポート フェーズ 2	Cisco IOS XE リリース 3.14S	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。 この機能は、Cisco IOS XE リリース 3.14S で、Cisco 4431 サービス統合型ルータと Cisco 4451-X サービス統合型ルータに導入されました。 この機能は、Cisco IOS XE リリース 3.15S で、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータと Cisco CSR 1000V シリーズ クラウド サービスルータに実装されました。 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。