IPsec を使用した VPN のセキュリティの設定

この章では、基本的な IP Security（IPsec）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を設定する方法について説明します。IPsec は、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）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。これにより、インターネットなどの保護されていないネットワーク上で機密性の高い情報を送信する際にセキュリティを確保します。IPsec はネットワーク レイヤで機能し、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。

機能情報の入手

ご使用のソフトウェア リリースでは、この章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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IPsec VPN のセキュリティの機能情報」（P.42）を参照してください。

プラットフォームのサポートと Cisco IOS および Catalyst OS 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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

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

Internet Key Exchange（IKE; インターネット キー エクスチェンジ）を「IPsec VPN のインターネット キー エクスチェンジ セキュリティの設定」の手順に従って設定する必要があります。

IKE を使用しない場合でも、「IPsec VPN のインターネット キー エクスチェンジの設定」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 User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート 500 を使用します。IPsec の Encapsulating Security Payload（ESP）および Authentication Header（AH; 認証ヘッダー）プロトコルは、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 のトラフィックが IPsec で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 リストの設定を確認してください。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

ユニキャスト IP データグラム アプリケーションのみ

現時点では、IPsec は、ユニキャスト IP データグラムだけに適用できます。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。

NAT の設定

Network Address Translation（NAT; ネットワークアドレス変換）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 変換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 変換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

Cisco IOS 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 Release 12.4(15)T までサポートされていますが、それ以降のリリースではサポートされていません。

IPsec を使用した VPN のセキュリティの設定に関する情報

基本的な IPsec VPN を設定するには、次の概念を理解しておく必要があります。

- 「サポートされる規格」（P.3）
- 「サポートされるハードウェア、スイッチング パスおよびカプセル化」（P.4）
- 「IPsec 機能の概要」（P.7）

- 「複数ピアにネストされた IPsec トラフィック」（P.10）

サポートされる規格

シスコシステムズでは、この機能を使用して次の規格を実装しています。

- IPsec：IP Security Protocol（IPsec; IP セキュリティ プロトコル）。IPsec はオープン規格のフレームワークであり、これにより、参加ピア間でデータ機密性、データ整合性、およびデータ認証が提供されます。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のネゴシエーションおよびアルゴリズムを処理し、IPsec で使用される暗号化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：ハイブリッド プロトコルで、Oakley キー交換と SKEME キー交換を ISAKMP フレームワーク内部に実装しています。IKE は他のプロトコルで使用できますが、その初期実装時は IPsec プロトコルで使用します。IKE は、IPsec ピアを認証し、IPsec Security Association（SA; 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。

- AES：Advanced Encryption Standard（AES; 高度暗号化規格）。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 よりセキュリティを向上させるために設計されています。具体的には、AES は、キーのサイズが従来より大きく、侵入者が既知の方式でメッセージを解読するには、キーを総当たりで試すしかありません。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：Data Encryption Standard（DES; データ暗号規格）。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。Cisco IOS は、必須の 56 ビット DES-CBC with Explicit IV を実装します。Cipher Block Chaining（CBC）では、暗号化の開始に Initialization Vector（IV; 初期ベクター）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、トリプル DES（168 ビット）暗号化も実装します。トリプル DES（3DES）は強力な暗号化方式であり、これにより、機密性の高い情報を非信頼ネットワーク上で送信できます。この方式では、ネットワーク レイヤ暗号化を使用できます。

  （注） 強力な暗号化を使用する Cisco IOS イメージ（56 ビット データ暗号化機能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 までお問い合せください。

- SEAL：Software Encryption Algorithm（SEAL; ソフトウェア暗号化アルゴリズム）。ソフトウェア ベースの DES、3DES、および AES に代わるアルゴリズムです。SEAL 暗号化では、160 ビットの暗号キーが使用され、他のソフトウェアベースのアルゴリズムに比べて、CPU に与える影響は小さくなります。
- MD5（Hash-based Message Authentication Code（HMAC; ハッシュ ベースのメッセージ認証コード）バリアント）：Message Digest Algorithm 5（MD5; メッセージ ダイジェスト アルゴリズム 5）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。
- SHA（HMAC バリアント）：SHA（Secure Hash Algorithm）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。

IPsec が Cisco IOS ソフトウェアに実装された場合、さらに次の規格をサポートします。

- AH：Authentication Header（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（カプセル化セキュリティ ペイロード）。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。

サポートされるハードウェア、スイッチング パスおよびカプセル化

IPsec には、ハードウェア、スイッチングパス、カプセル化方式に関して、次のような特定の要件があります。

- 「サポートされるハードウェア」（P.4）
- 「サポートされるスイッチング パス」（P.6）
- 「サポートされるカプセル化」（P.7）

サポートされるハードウェア

この項目は次のサブ項目から構成されます。

- 「VPN アクセラレータ モジュール（VAM）のサポート」（P.4）
- 「AIM および NM のサポート」（P.5）

VPN アクセラレータ モジュール（VAM）のサポート

VAM は、シングル幅のアクセラレーション モジュールです。VAM は、VPN リモート アクセス、サイト間イントラネットおよびエクストラネット アプリケーションに適した高性能のハードウェア支援トンネリングおよび暗号化サービスを提供します。また VAM は、セキュリティ、Quality of Service（QoS）、ファイアウォール、および侵入検知、サービスレベル検証や管理など、VPN 展開の成功に必要なすべてのサービスと連動しながら、プラットフォームのスケーラビリティとセキュリティも提供します。VAM は、IPsec 処理にかかる負荷をメイン プロセッサから除去して、プロセッサ エンジンのリソースを他のタスクに解放します。

VAM は、次の複数暗号化機能にハードウェア アクセラレーション サポートを提供します。

- 56 ビット DES 標準モード：CBC
- 3 キー トリプル DES（168 ビット）
- SHA-1 および MD5

- Rivest、Shamir、Adelman（RSA）公開キー アルゴリズム
- Diffie-Hellman キー交換 RC4 - 40

VAM の詳細については、マニュアル『VPN Acceleration Module (VAM)』を参照してください。

AIM および NM のサポート

データ暗号化 Advanced Integration Module（AIM）および Network Module（NM）により、ハードウェアベースの暗号化を実行します。

データ暗号化 AIM および NM は、ハードウェア レイヤ 3（IPsec）暗号化モジュールであり、複数の T1 または E1 帯域幅に DES およびトリプル DES IPsec 暗号化機能を提供します。これら製品は、Diffie-Hellman、RSA、および DSA キー生成のハードウェア サポートも提供します。

いずれのモジュールを使用する場合でも、RSA の手動キー入力がサポートされていないことに注意してください。

使用する VPN 暗号化モジュールを決定する場合は、表 1 を参照してください。

Cisco 2600 および Cisco 3600 シリーズ ルータで AIM および NM を使用するための IPPCP ソフトウェア

VPN モジュールが Cisco 2600 および Cisco 3600 シリーズ ルータに搭載されている場合、AIM および NM でソフトウェア IPPCP を使用すると、IPsec で Lempel-Ziv-Stac（LZS）ソフトウェア圧縮を使用できます。これにより、インターフェイスの帯域幅を効果的に増やすことができます。

IPPCP ソフトウェアを使用しない場合、VPN 暗号化ハードウェア AIM および NM で圧縮はサポートされません。つまり、ルータから VPN モジュールを取り外し、ソフトウェア圧縮を使用してソフトウェア暗号化を実行する必要があります。IPPCP により、すべての VPN モジュールは、ルータに搭載時にソフトウェアでの LZS 圧縮をサポートできます。これにより、ユーザはデータ圧縮を設定し、自身の帯域幅を増やすことできるので、IPPCP は低域のデータ リンクに有効です。

IPPCP を使用しない場合、圧縮はレイヤ 2 で、暗号化はレイヤ 3 でそれぞれ発生します。データ ストリームは、暗号化されると圧縮サービスに渡されます。圧縮エンジンが暗号化されたデータ ストリームを受け取ると、データは展開されますが、圧縮されません。この機能では、IPsec トランスフォーム セットと LZS を選択することによってデータの圧縮と暗号化の両方をレイヤ 3 で実行できます。つまり、LZS 圧縮が暗号化の前に発生するので、圧縮率を向上させることができます。

表 1　Cisco IOS リリースでサポートされる AIM/VPN 暗号化モジュール

<table>
<tr><th rowspan="2">プラットフォーム</th><th colspan="5">Cisco IOS リリースでサポートされる暗号化モジュール</th></tr>
<tr><th>12.2(13)T</th><th>12.3(4)T</th><th>12.3(5)</th><th>12.3(6)</th><th>12.3(7)T</th></tr>
<tr><td>Cisco 831</td><td colspan="5">ソフトウェアベースの AES</td></tr>
<tr><td>Cisco 1710
Cisco 1711
Cisco 1721
Cisco 1751
Cisco 1760</td><td colspan="5">ソフトウェアベースの AES</td></tr>
<tr><td>Cisco 2600 XM</td><td colspan="3">—</td><td>AIM-VPN/BPII-Plus ハードウェア暗号化モジュール</td><td></td></tr>
<tr><td>Cisco 2611 XM
Cisco 2621 XM
Cisco 2651 XM</td><td>—</td><td colspan="3">AIM-VPN/BPII ハードウェア暗号化モジュール</td><td>AIM-VPN/BPII-Plus ハードウェア暗号化モジュール</td></tr>
</table>

表 1　Cisco IOS リリースでサポートされる AIM/VPN 暗号化モジュール （続き）

プラットフォーム	Cisco IOS リリースでサポートされる暗号化モジュール				
	12.2(13)T	12.3(4)T	12.3(5)	12.3(6)	12.3(7)T
Cisco 2691 XM	AIM-VPN/EPII ハードウェア暗号化モジュール				AIM-VPN/EPII-Plus ハードウェア暗号化モジュール
Cisco 3735	AIM-VPN/EPII ハードウェア暗号化モジュール		AIM-VPN/EPII-Plus ハードウェア暗号化モジュール		
Cisco 3660 Cisco 3745	AIM-VPN/HPII ハードウェア暗号化モジュール		AIM-VPN/HPII-Plus ハードウェア暗号化モジュール		

AIM および NM の詳細については、『*Installing Advanced Integration Modules in Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers*』を参照してください。

サポートされるスイッチング パス

表 2 に、IPsec で動作する、サポートされるスイッチング パスを示します。

表 2　IPsec でサポートされるスイッチング パス

スイッチング パス	例
プロセス スイッチング	`interface ethernet0/0` ` no ip route-cache`
ファースト スイッチング	`interface ethernet0/0` ` ip route-cache` `! Ensure that you will not hit flow switching.` ` no ip route-cache flow` `! Disable CEF for the interface, which supercedes global CEF.` ` no ip route-cache cef`
シスコ エクスプレス フォワーディング	`ip cef` `interface ethernet0/0` ` ip route-cache` `! Ensure that you will not hit flow switching.` ` no ip route-cache flow`
ファースト フロー スイッチング	`interface ethernet0/0` ` ip route-cache` `! Enable flow switching` `p route-cache flow` `! Disable CEF for the interface.` `  no ip route-cache cef`
シスコ エクスプレス フォワーディング フロー スイッチング	`! Enable global CEF.` `ip cef` `interface ethernet0/0` ` ip route-cache` ` ip route-cache flow` `! Enable CEF for the interface` ` ip route-cache cef`

サポートされるカプセル化

IPsec は、High-Level Data-Links Control（HDLC; 高レベル データ リンク制御）、PPP、およびフレーム リレーのシリアル カプセル化と連動します。

また、IPsec は、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）、IPinIP レイヤ 3、Layer 2 Forwarding（L2F; レイヤ 2 転送）、Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）、データ リンク スイッチング+（DLSw+）、および 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 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 は現在グループ トラフィック（ブロードキャストまたはマルチキャスト トラフィックなど）の保護に使用できません。

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。これ以後、IPsec ピアがこのような機密性の高い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。

IPsec では、アクセス リストを設定し、これらのアクセス リストをクリプト マップ セットを使用してインターフェイスに適用することにより、2 つの IPsec ピア間で保護の必要があるトラフィックを定義します。したがって、トラフィックを送信元アドレスと宛先アドレス、レイヤ 4 プロトコル（必要に応じて）、およびポートに基づいて選択できます（IPsec に使用されるアクセス リストは、IPsec で保護する必要があるトラフィックを判別するためだけに使用され、インターフェイスを通じてブロックまたは許可されるトラフィックを判別するものではありません。インターフェイスでブロックするか許可するかは、別のアクセス リストで定義します）。

クリプト マップ セットには複数のエントリを含めることができ、それぞれが異なるアクセス リストに対応します。クリプト マップ エントリは、ルータがパケットをそのエントリで指定されたアクセス リストと照合しようとする順序で検索されます。

パケットが特定のアクセス リストの **permit** エントリに一致し、対応するクリプト マップ エントリが **cisco** とタグ付けされている場合、必要に応じて接続が確立されます。クリプト マップ エントリが **ipsec-isakmp** とタグ付けされている場合、IPsec がトリガーされます。ピアに対してこのトラフィックを保護するために IPsec を使用できる SA が存在しない場合、IPsec は IKE を使用してリモート ピアとネゴシエーションし、データ フローに必要な IPsec SA を設定します。ネゴシエーションでは、特定の

アクセス リスト エントリからのデータ フロー情報とともに、クリプト マップ エントリで指定された情報が使用されます（ダイナミック クリプト マップ エントリでは動作は異なります。この章の「ダイナミック クリプト マップの作成」を参照してください）。

クリプト マップ エントリが **ipsec-manual** とタグ付けされている場合、IPsec がトリガーされます。ピアへのこのトラフィックの保護に IPsec が使用できる SA が存在しない場合、トラフィックは廃棄されます。この場合、IKE が介入することなく、SA がコンフィギュレーションによってインストールされます。SA が存在しないと、IPsec には必要な情報がすべて設定されません。

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、あるデータス トリームで認証だけを実行する場合、他のデータ ストリームでは暗号化と認証を実行する必要があります。

IPsec クリプト マップ エントリに関連付けられたアクセス リストは、ルータが IPsec による保護を必要とするトラフィックも表します。着信トラフィックはクリプト マップ エントリに対して処理されます。保護されていないパケットが IPsec クリプト マップ エントリに関連付けられた特定のアクセス リスト内の **permit** エントリに一致すると、そのパケットは IPsec 保護されたパケットとして送信されていないので廃棄されます。

クリプト マップ エントリには、トランスフォーム セットも含まれます。トランスフォーム セットは、IPsec 保護されたトラフィックに適用されるセキュリティ プロトコル、アルゴリズムおよびその他の設定の適切な組み合せです。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。

IKEv1 トランスフォーム セット

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の組み合せを表します。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。

複数のトランスフォーム セットを指定し、これらのトランスフォーム セットの 1 つまたは複数をクリプト マップ エントリに指定できます。クリプト マップ エントリに定義されたトランスフォーム セットは、このクリプト マップ エントリのアクセス リストで指定されたデータ フローを保護するために、IPsec SA ネゴシエーションで使用されます。

IKE との IPsec SA のネゴシエーション中に、ピアは両方のピア上で同じトランスフォーム セットを検索します。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）。

トランスフォーム セットの定義を変更した場合には、トランスフォーム セットを参照するクリプト マップ エントリだけに変更が適用されます。変更は、既存の SA には適用されませんが、新規の SA を確立するために以降のネゴシエーションで使用されます。新しい設定をただちに有効にする場合は、**clear crypto sa** コマンドを使用して、SA データベースのすべてまたは一部を消去します。

IKEv2 トランスフォーム セット

IKEv2 プロポーザルは、IKE_SA_INIT 交換の一部として IKEv2 SA のネゴシエーションに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 sha md5
group 5 2
```

ここに示すトランスフォームは、次の優先順位で次のような組み合わせに変換されます。

```
aes-cbc-128, sha, 5
aes-cbc-128, sha, 2
aes-cbc-128, md5, 5
aes-cbc-128, md5, 2
3des, sha, 5
3des, sha, 2
3des, md5, 5
3des, md5, 2
```

このコマンドは **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プロポーザルを使用する場合、IKEv2 プロポーザルを IKEv2 ポリシーに接続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。

1 つのトランスフォーム タイプに対して複数のトランスフォームが設定された場合、優先順位は左から右の順になります。

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を持つプロポーザルは、トランスフォームの使用可能なすべての組み合わせに変換されます。これらの組み合わせのサブセットのみが必要な場合は、個別のプロポーザルとして設定する必要があります。

```
Router(config)# crypto ikev2 proposal proposal-1
Router(config-ikev2-proposal)# encryption 3des, aes-cbc-128
Router(config-ikev2-proposal)# integrity sha, md5
Router(config-ikev2-proposal)# group 2
```

たとえば、ここに示すコマンドは、次の組み合わせのトランスフォームに変換されます。

```
3des, sha, 2
aes-cbc-128, sha, 2
3des, md5, 2
aes-cbc-128, md5, 2
```

1 番目と最後のトランスフォームの組み合わせを設定する場合、コマンドは次のようになります。

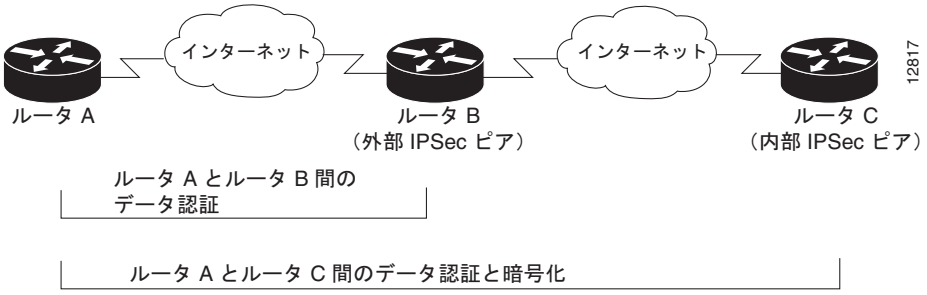
```
Router(config)# crypto ikev2 proposal proposal-1
Router(config-ikev2-proposal)# encryption 3des
Router(config-ikev2-proposal)# integrity sha
Router(config-ikev2-proposal)# group 2

Router(config)# crypto ikev2 proposal proposal-2
Router(config-ikev2-proposal)# encryption aes-cbc-128
Router(config-ikev2-proposal)# integrity md5
Router(config-ikev2-proposal)# group 2
```

複数ピアにネストされた IPsec トラフィック

IPsec トラフィックを一連の IPsec ピアにネストすることができます。たとえば、トラフィックが複数のファイアウォール（これらのファイアウォールには、認証されていないトラフィックを通過させないというポリシーが設定されています）を横断するには、ルータは、各ファイアウォールとの間に IPsec トンネルを順に設立する必要があります。近いファイアウォールほど、外側の IPsec ピアになります。

図 1 の例では、ルータ A が、IPsec のルータ C に転送されるトラフィックをカプセル化します（ルータ C が内側の IPsec ピアです）。ただし、ルータ A がこのトラフィックを送信する前に、ルータ A はこのトラフィックをルータ B（ルータ B が「外側の」IPsec ピア）に送信するには、まずこの IPsec でトラフィックを再カプセル化する必要があります。

図 1　　IPsec ピアのネスティング例



「外側の」ピア間のトラフィックに、ある種の保護（データ認証など）を設定し、「内側の」ピア間のトラフィックに別の保護（データ認証と暗号化など）を設定することが可能です。

IKE および IPsec 暗号化アルゴリズムでの 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 には次の暗号化アルゴリズムがあります。

- Suite-B-GCM-128：ESP の整合性の保護と機密性、および RFC 4106 に記述されている 128 ビットの Advanced Encryption Standard（AES; 高度暗号化規格）using Galois and Counter Mode（AES-GCM; Galois and Counter Mode を使用した AES）を使用する IPsec の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 に記述されている 256 ビットの AES-GCM を使用して、ESP の整合性の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 に記述されている 128 ビットの AES-Galois Message Authentication Code（GMAC）を使用して ESP の整合性を保護しますが、機密性は提供されません。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 に記述されている 256 ビットの AES-GMAC を使用して ESP の整合性を保護しますが、機密性は提供されません。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 Cipher Block Chaining（CBC; 暗号ブロック連鎖）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 Elliptic Curve Digital Signature Algorithm（ECDSA; 楕円曲線デジタル署名アルゴリズム）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 および HMAC-SHA384 は、疑似ランダム関数として使用され、IKE プロトコルが使用されている範囲内の整合性チェックを行います。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。
- ECDSA アルゴリズム（256 ビットおよび 384 ビットの曲線）は、X.509 証明書内の署名操作に使用されます。
- 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 署名を使用して X.509 証明書を確認する場合に、PKI 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。

- **esp-gcm** および **esp-gmac** トランスフォームの詳細については、「IKEv1 のトランスフォーム セットの設定」（P.18）を参照してください。
- 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』フィーチャ 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)』フィーチャ モジュールの「Configuring the IKEv2 Proposal」の項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)』フィーチャ モジュールの「Configuring the IKEv2 Proposal」の項を参照してください。
- IPsec SA のネゴシエーションでの 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 (IKEv2)』フィーチャ 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』フィーチャ 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

クリプト アクセス リストの概要

クリプト アクセス リストは、暗号化で保護する IP トラフィックと、暗号化で保護しないトラフィックを定義するために使用されます（このアクセス リストは、転送するトラフィックまたはインターフェイスでブロックするトラフィックを決定する、通常のアクセス リストと同じ*ものではありません*）。たとえば、アクセス リストを作成して、サブネット A とサブネット Y 間のすべての IP トラフィックまたはホスト A とホスト B 間の Telnet トラフィックを保護することができます。

アクセス リスト自体は IPsec に固有のものではありません。これは、アクセス リストの **permit** と一致するトラフィックに IPsec 処理を適用するかどうかを定義する固有のアクセス リストを参照するクリプト マップ エントリです。

IPsec クリプト マップ エントリに関連付けられたクリプト アクセス リストには、主に次の 4 つの機能があります。

- IPsec で保護される発信トラフィックを選択します（permit = protect）。
- IPsec SA のネゴシエーションを開始する場合に、新しい SA で保護されるデータ フローを指定します（単一の **permit** エントリで指定）。
- 着信トラフィックを処理して、IPsec で保護されていたトラフィック除外し、廃棄します。
- IPsec ピアからの IKE ネゴシエーションを処理するとき、要求されたデータ フローの代わりに IPsec SA の要求を受け入れるかどうかを決定します。
- ネゴシエーションは、**ipsec-isakmp** クリプト マップ エントリに対してだけ実行されます。要求を受け入れるには、ピアが IPsec ネゴシエーションを開始した場合に、**ipsec-isakmp** クリプト マップ エントリに関連付けられた暗号化アクセス リストで「許可する」データ フローを指定する必要があります。

一方のトラフィックに特定の組み合せの IPsec 保護（認証のみ）を適用し、もう一方のトラフィックに別の組み合せの IPsec 保護（認証と暗号化）を適用する場合は、2 つの異なるクリプト アクセス リストを作成して、2 つの異なるタイプのトラフィックを定義する必要があります。これらの異なるアクセス リストを異なるクリプト マップ エントリで使用して、異なる IPsec ポリシーを指定します。

クリプト アクセス リストで permit および deny キーワードを使用する場合

クリプト アクセス リストの特定の IP トラフィックに対して暗号保護を、次のように許可または拒否できます。

- 対応するクリプト マップ エントリで指定されたポリシー条件と一致する IP トラフィックを保護するには、アクセス リストで **permit** キーワードを使用します。
- 対応するクリプト マップ エントリで指定されたポリシー条件と一致する IP トラフィックの保護を拒否するには、アクセス リストで **deny** キーワードを使用します。

（注） IP トラフィックは、インターフェイスのすべてのクリプト マップ エントリで保護が拒否されると、暗号化によって保護されません。

対応するクリプト マップ エントリが定義され、クリプト マップ セットがインターフェイスに適用されると、定義されたクリプト アクセス リストがインターフェイスに適用されます。異なるアクセス リストを同じクリプト マップ セットの異なるエントリで使用する必要があります。ただし、着信トラフィックと発信トラフィックは、両方とも同じ「発信」IPsec アクセス リストに照らして評価されます。したがって、アクセス リストの基準は、ルータから出るトラフィックに対しては順方向に、ルータに入るトラフィックに対しては逆方向に適用されます。

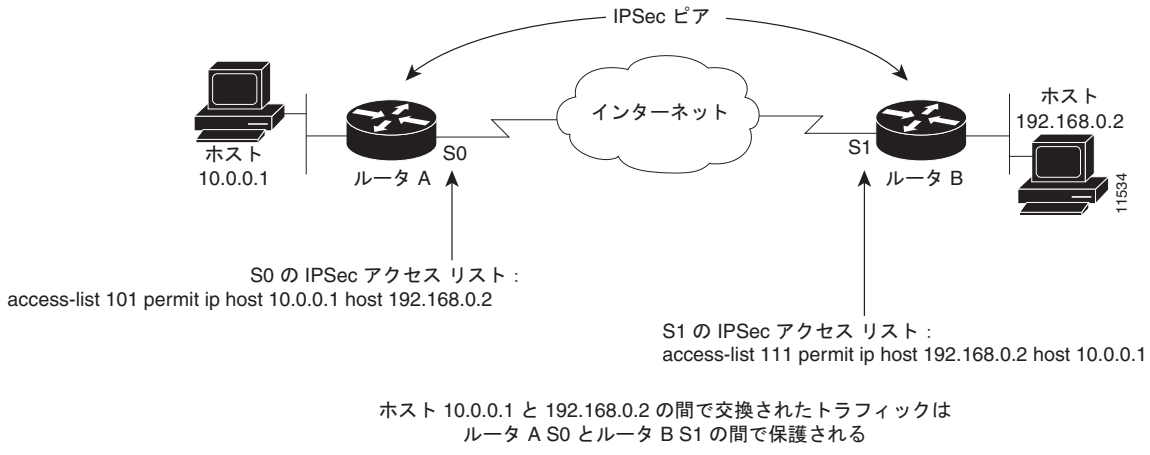
図 2 では、データがルータ A の S0 インターフェイスを出てホスト 192.168.0.2 に経路指定されている場合に、ホスト 10.0.0.1 とホスト 192.168.0.2 の間のトラフィックに IPsec 保護が適用されます。ホスト 10.0.0.1 からホスト 192.168.0.2 へのトラフィックについては、ルータ A でのアクセス リスト エントリは、次のように評価されます。

```
source = host 10.0.0.1
dest = host 192.168.0.2
```

ホスト 192.168.0.2 からホスト 10.0.0.1 へのトラフィックについては、ルータ A での同じアクセス リスト エントリは、次のように評価されます。

```
source = host 192.168.0.2
dest = host 10.0.0.1
```

図 2　IPsec を処理するためにクリプト アクセス リストを適用する方法



IPsec に使用される指定のクリプト アクセス リストに複数の文を設定する場合、通常、一致する最初の **permit** 文によって、IPsec SA の範囲が決定されます。つまり、IPsec SA は、照合された文の基準を満たすトラフィックだけを保護するように設定されます。その後、クリプト アクセス リスト内の別の **permit** 文とトラフィックが一致すると、新しい、別個の IPsec SA がネゴシエーションされ、新たに照合されたアクセス リスト文と一致するトラフィックが保護されます。

IPsec としてマークが付けられたクリプト マップ エントリのクリプト アクセス リスト内の **permit** エントリと一致する、すべての保護されていない着信トラフィックは、IPsec によって保護されることが想定されていたため、廃棄されます。

（注） **show ip access-lists** などのコマンドを使用してルータのアクセス リストを表示すると、コマンド出力にすべての拡張 IP アクセス リストが表示されます。この表示出力には、トラフィックのフィルタリングおよび暗号化に使用される拡張 IP アクセス リストが含まれます。**show** コマンド出力では、拡張アクセス リストの各用途は区別されません。

次の例では、重複ネットワークが使用されている場合、最も具体的なネットワークが暗号シーケンス番号で定義されてから、それよりも具体的でないネットワークが定義されることを示します。この例では、より具体的なネットワークは、クリプト マップのシーケンス番号 10 によってカバーされ、その後に、クリプト マップ内のそれほど具体的でないネットワーク（シーケンス番号 20）が続きます。

```
crypto map mymap 10 ipsec-isakmp
 set peer 192.168.1.1
 set transform-set test
 match address 101
crypto map mymap 20 ipsec-isakmp
 set peer 192.168.1.2
 set transform-set test
 match address 102

access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255

access-list 102 permit ip 10.0.0.0 0.255.255.255 172.16.0.0 0.15.255.255
```

次の例では、あるクリプト マップ シーケンス番号に **deny** キーワードを指定し、別のクリプト マップ シーケンス番号の同じサブネットおよび IP 範囲に **permit** キーワードを指定する方法がサポートされないことを示します。

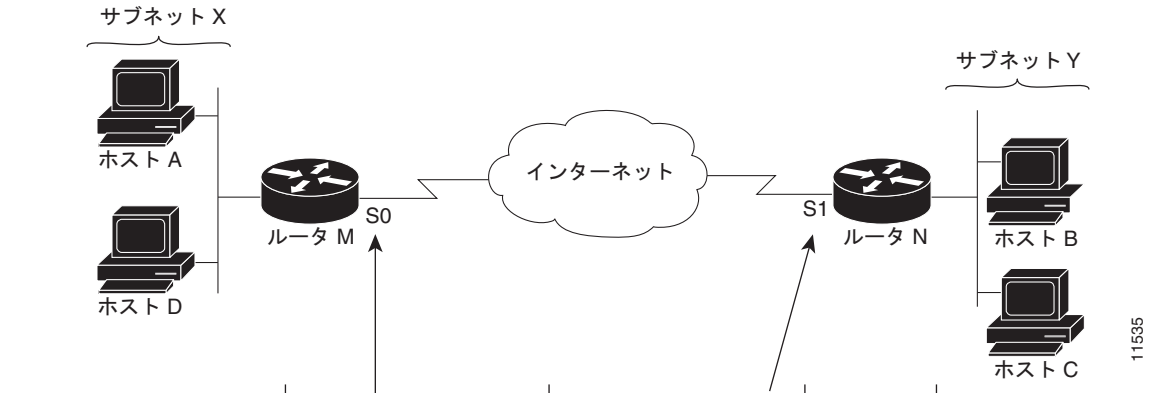
```
crypto map mymap 10 ipsec-isakmp
 set peer 192.168.1.1
 set transform-set test
 match address 101
crypto map mymap 20 ipsec-isakmp
 set peer 192.168.1.2
 set transform-set test
 match address 102

access-list 101 deny   ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 101 permit ip 10.0.0.0 0.255.255.255 172.16.0.0 0.15.255.255

access-list 102 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
```

各 IPsec ピアでのミラー イメージ クリプト アクセス リスト

ローカル ピアで定義されたスタティッククリプト マップ エントリがある場合は、このエントリで指定された各クリプト アクセス リストに対して、リモート ピアで「ミラー イメージ」クリプト アクセス リストを定義することを推奨します。これにより、ローカルで IPsec 保護が適用されたトラフィックがリモート ピアで確実に処理されます（クリプト マップ エントリ自体も共通トランスフォームをサポートする必要があり、他のシステムをピアとして参照する必要があります）。

図 3 に、ミラー イメージ アクセス リストがある場合と、ミラー イメージ アクセス リストがない場合のサンプル シナリオをいくつか示します。

図 3　　ミラー イメージおよび 非ミラー イメージ クリプト アクセス リスト（IPsec の場合）



		S0 の IPSec アクセスリスト：	S1 の IPSec アクセスリスト：	最初のパケット	結果
ルータ M S0と ルータ N S1の ミラー イメージ アクセス リスト	ケース 1	許可 ホスト A → ホスト B	許可 ホスト B → ホスト A	A → B または B → A	トラフィック A ↔ B に SA が確立（good）
	ケース 2	許可 サブネット X → サブネット Y	許可 サブネット Y → サブネット X	A → B または B → A または A → C または C → D など	トラフィック X ↔ Y に SA が確立（good）
	ケース 3	許可 ホスト A → ホスト B	許可 サブネット Y → サブネット X	A → B	トラフィック A ↔ B に SA が確立（good）
	ケース 4			B → A	SA を確立できず、ホスト B からホスト A へのパケットが破棄される（bad）

図 3 のように、2 つのピアのクリプト アクセス リストが相互にミラー イメージになっていれば、必ず IPsec SA を想定どおりに確立できます。ただし、アクセス リストが互いのミラー イメージではない場合でも、IPsec SA を確立できることがあります。これは、図 3 のケース 3 および 4 に示すように、一方のピアのアクセス リスト内のエントリが、他方のピアのアクセス リスト内にあるエントリのサブセットである場合に確立できます。IPsec SA の確立は IPsec にとって重要です。SA が存在しないと、IPsec は機能せず、クリプト アクセス リスト基準に一致するパケットは、IPsec で転送されずに、すべて廃棄されてしまいます。

図 3 のケース 4 では、SA を確立できません。これは、開始元パケットが終了すると、クリプト アクセス リストに従って必ず SA が要求されるからです。ケース 4 では、ルータ N は、サブネット X とサブネット Y 間のすべてのトラフィックを保護するように要求しますが、このトラフィックはルータ M のクリプト アクセス リストによって許可される特定のフローのスーパーセットであるため、要求は許可されません。ルータ M の要求はルータ N のクリプト アクセス リストで許可される特定のフローのサブセットであるため、ケース 3 は機能します。

ピア IPsec 装置にクリプト アクセス リストをミラー イメージとして設定しないと、設定が複雑化するので、ミラー イメージ クリプト アクセス リストを使用することを強く推奨します。

クリプト アクセス リストに any キーワードを使用する場合

クリプト アクセス リストの作成時に、**any** キーワードを使用すると、問題が発生する場合があります。送信元アドレスまたは宛先アドレスの指定には、**any** キーワードを使用することは推奨しません。

IPsec インターフェイスを経由してマルチキャスト トラフィックを転送する場合、**permit** 文に **any** キーワードを 使用しないでください。**any** キーワードを使用すると、マルチキャスト トラフィックの転送が失敗する原因になります。

permit any any 文を使用しないことを強く推奨します。これは、すべての発信トラフィックが保護され（保護されたすべてのトラフィックが、対応するクリプト マップ エントリで指定されたピアに送信され）、すべての着信トラフィックの保護が必要になるからです。また、ルーティング プロトコル、Network Time Protocol（NTP; ネットワーク タイム プロトコル）、エコー、エコー応答用のパケットを含む、IPsec で保護されていないすべての着信パケットは、自動的に廃棄されます。

保護するパケットを確実に定義する必要があります。**permit** 文内で **any** キーワードを使用する必要がある場合は、保護しないすべてのトラフィックを除外する一連の **deny** 文を、**permit** 文の前に付加する*必要があります*（付加しない場合、これらのトラフィックが permit 文の対象になります）。

また、Reverse Route Injection（RRI; 逆ルート注入）を使用する Access Control List（ACL; アクセス制御リスト）では、**any** キーワードを使用できません（RRI の詳細については、「クリプト マップ セットの作成」（P.22）を参照してください）。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**]

   または

   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	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル 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	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**] **例：** `Router(config)# access-list 100 permit ip 10.0.68.0 0.0.0.255 10.1.1.0 0.0.0.255` または **ip access-list extended** *name* **例：** `Router(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。[1] • これらの条件に一致するトラフィックに対して暗号化をイネーブルまたはディセーブルにします。 **ヒント** IPsec で使用できるように「ミラー イメージ」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。	—

1. 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。

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」（P.17）の手順に従って定義する必要があります。

次に、設定対象および適用対象のインターフェイスに（「クリプト マップ セットの作成」（P.22）および「インターフェイスへのクリプト マップ セットの適用」（P.36）の手順に従って）クリプト マップ セットを設定し、適用したら、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。

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。

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

IKEv1 のトランスフォーム セットの設定

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル 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-name transform1* [*transform2* [*transform3*]] **例：** `Router(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。表 3 に、使用できるトランスフォームの組み合せを示します。
ステップ 4	**mode** [**tunnel**	**transport**] **例：** `Router(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）。
ステップ 5	**exit** **例：** `Router(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。

	コマンドまたはアクション	目的
ステップ 6	**clear crypto sa** [**peer** {*ip-address* | *peer-name*} | **sa map** *map-name* | **sa entry** *destination-address protocol spi*] **例：** `Router# 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：** `Router# 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。

表 3 に、使用できるトランスフォームの組み合せを示します。

表 3　使用できるトランスフォームの組み合せ

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。
	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。
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** および **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。 **（注）** **esp-gcm** と **esp-gmac** トランスフォームは、いずれも **crypto ipsec transform-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-aes 192	192 ビット AES 暗号化アルゴリズムを使用する ESP。
	esp-aes 256	256 ビット AES 暗号化アルゴリズムを使用する ESP。

表 3　使用できるトランスフォームの組み合せ （続き）

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 Data Encryption Standard（DES）暗号化アルゴリズムを使用する ESP。
	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。
	esp-null	ヌル暗号化アルゴリズム。
	esp-seal	160 ビット SEAL 暗号化アルゴリズムを使用する ESP
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。
	esp-sha-hmac	SHA（HMAC バリアント）認証アルゴリズムを使用する ESP。
IP 圧縮トランスフォーム	**comp-lzs**	Lempel-Ziv-Stac（LZS）アルゴリズムを使用した IP 圧縮

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」（P.22）で指定する手順でクリプト マップを作成する必要があります。

IKEv2 のトランスフォーム セットの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 proposal** *proposal-name*
4. **encryption** *transform1* [*transform2*] …
5. **integrity** *transform1* [*transform2*] …
6. **group** *transform1* [*transform2*] …
7. **exit**
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	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル 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：** `Router(config)# crypto ikev2 proposal proposal-1`	プロポーザルの名前を指定し、クリプト 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：** `Router(config-ikev2-proposal)# encryption 3des, 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 • AES-CBC 192 • AES-CBC 256 • 3DES • DES
ステップ 5	**integrity** *transform1* [*transform2*] … **例：** `Router(config-ikev2-proposal)# integrity sha, md5`	（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。 • SHA • MD5
ステップ 6	**group** *transform1* [*transform2*] … **例：** `Router(config-ikev2-proposal)# group 2`	（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。 • グループ 1 • グループ 2 • グループ 5
ステップ 7	**show crypto ikev2 proposal** **例：** `Router# 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：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

```
Router(config)# crypto ikev2 proposal proposal-1
Router(config-ikev2-proposal)# encryption 3des
Router(config-ikev2-proposal)# integrity sha
```

```
Router(config-ikev2-proposal)# group 2
```

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

```
Router(config)# crypto ikev2 proposal proposal-2
Router(config-ikev2-proposal)# encryption 3des aes-cbc-128
Router(config-ikev2-proposal)# integrity sha md5
Router(config-ikev2-proposal)# group 2 5
```

ここに示す IKEv2 プロポーザル **proposal-2** では、次の組み合わせのトランスフォームの優先順位リストに変換されます。

- 3des、sha、2
- 3des、sha、5
- 3des、md5、2
- 3des、md5、5
- aes-cbc-128、sha、2
- aes-cbc-128、sha、5
- aes-cbc-128、md5、2
- aes-cbc-128、md5、5

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。

```
Router(config)# crypto ikev2 proposal proposal-1
Router(config-ikev2-proposal)# encryption 3des aes-cbc-128
Router(config-ikev2-proposal)# integrity sha md5
Router(config-ikev2-proposal)# group 2 5
```

応答側のプロポーザルは次のとおりです。

```
Router(config)# crypto ikev2 proposal proposal-2
Router(config-ikev2-proposal)# encryption aes-cbc-128 3des
Router(config-ikev2-proposal)# integrity md5 sha
Router(config-ikev2-proposal)# group 5 2
```

ここに示すシナリオでは、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 3des
integrity sha
group 2
```

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」（P.22）で指定する手順でクリプト 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

クリプト マップ セットを作成するには、必要に応じて、次の項を参照してください。

- 「スタティック クリプト マップの作成」（P.25）
- 「ダイナミック クリプト マップの作成」（P.27）
- 「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」（P.34）

前提条件

クリプト マップ エントリを作成する前に、ネットワークのニーズに対処するための最適なクリプト マップのタイプ（スタティック、ダイナミック、または手動）を判別する必要があります。また、次の概念も理解しておく必要があります。

- 「クリプト マップの概要」（P.23）
- 「クリプト マップ間での負荷分散」（P.24）
- 「クリプト マップに関する注意事項」（P.24）

クリプト マップの概要

IPsec に対して作成されたクリプト マップ エントリにより、IPsec SA の設定に使用される各要素がまとめられます。この要素は次のとおりです。

- どのトラフィックを（クリプト アクセス リストごとに）IPsec で保護する必要があるか
- 一連の SA で保護されるフローの粒度
- IPsec で保護されるトラフィックの送信先（リモート IPsec ピア）
- IPsec トラフィックに使用されるローカル アドレス（詳細については、「インターフェイスへのクリプト マップ セットの適用」（P.36）を参照してください）
- どのような IPsec SA をこのトラフィック（1 つまたは複数のトランスフォーム セットのリストから選択）に適用する必要があるか
- SA を手動で確立するのか、IKE で確立するのか
- IPsec SA の定義に必要となる可能性があるその他のパラメータ

クリプト マップの動作原理

同じクリプト マップ名（マップ シーケンス番号が異なる）を持つクリプト マップ エントリは、クリプト マップ セットにグループ化されます。これらのクリプト マップ セットを後でインターフェイスに適用します。このとき、インターフェイスを通過するすべての IP トラフィックは、適用されたクリプト マップ セットに対して評価されます。クリプト マップ エントリは、保護の必要がある発信 IP トラフィックを確認し、クリプト マップによって IKE の使用が指定されている場合、SA が、クリプト マップ エントリに含まれているパラメータに従ってリモート ピアとネゴシエーションされます。また、クリプト マップ エントリによって手動による SA の使用が指定されている場合は、SA がすでに設定によって確立されている必要があります（保護の必要がある発信トラフィックがダイナミック クリプト マップ エントリによって確認され、SA が存在しない場合、パケットは廃棄されます）。

クリプト マップ エントリに記述されたポリシーは、SA のネゴシエーション中に使用されます。ローカル ルータがネゴシエーションを開始する場合、このルータは、スタティック クリプト マップ エントリで指定されているポリシーを使用して、指定の IPsec ピアに送信されるオファーを作成します。IPsec ピアがネゴシエーションを開始すると、ローカル ルータはすべての参照先のスタティック クリプト マップ エントリおよびダイナミック クリプト マップ エントリからのポリシーを確認して、ピアの要求（オファー）を受け入れるか、拒否するかどうかを決定します。

2 つの IPsec ピア間で IPsec を正常に確立するには、両方のピアのクリプト マップ エントリに、互換性のある設定文が含まれている必要があります。

互換性があるクリプト マップ：SA の確立

2 つのピアが SA を確立しようとするとき、これらのピアは、他方のピアのクリプト マップ エントリのいずれかと互換性があるクリプト マップ エントリを 1 つ以上持っている必要があります。2 つのクリプト マップ エントリで互換性が成立するには、少なくとも次の基準を満たす必要があります。

- クリプト マップ エントリに、互換性があるクリプト アクセス リスト（ミラー イメージ アクセス リスト）が含まれている必要があります。応答側ピアがダイナミックなクリプト マップを使用している場合、ローカル クリプト アクセス リスト内のエントリは、ピアのクリプト アクセス リストで「許可される」必要があります。
- クリプト マップ エントリはそれぞれ他方のピアを識別する必要があります（応答側ピアがダイナミック クリプト マップを使用しない場合）。
- クリプト マップ エントリに、共通のトランスフォーム セットが少なくとも 1 つなくてはなりません。

クリプト マップ間での負荷分散

クリプト マップを使用して複数のリモート ピアを定義し、負荷分散を実行できます。1 つのピアに障害が発生しても保護されたパスが引き続き存在するため、負荷分散は便利です。パケットが実際に送信されるピアは、特定のデータ フローでルータが受信した最後のピア（トラフィックまたはネゴシエーション要求を受信した）によって決まります。最初のピアでの試行が失敗すると、IKE はクリプト マップ リストの次のピアを試行します。

各クリプト マップ パラメータを設定して他のピアとの互換性を確保する方法が不明な場合は、「ダイナミック クリプト マップの作成」（P.27）の説明に従って、ダイナミック クリプト マップの設定を検討することができます。ダイナミック クリプト マップは、IPsec トンネルの確立がリモート ピア（サーバ側の IPsec ルータなど）で開始される場合に便利です。ダイナミック クリプト マップは、ポリシー テンプレートであり、完全なポリシーの文ではないため、ローカルで IPsec トンネルの確立が開始される場合には有効ではありません（ただし、暗号パケット フィルタリングには、すべての参照先のダイナミック クリプト マップ エントリ内のアクセス リストが使用されます）。

クリプト マップに関する注意事項

単一のインターフェイスには、クリプト マップ セットを 1 つだけ適用できます。クリプト マップ セットには、IPsec/IKE と IPsec/ 手動のエントリの組み合せを含めることができます。複数のインターフェイスに同じポリシーを適用する場合、複数のインターフェイスが同じクリプト マップ セットを共有できます。

特定のインターフェイスに対して複数のクリプト マップ エントリを作成する場合は、各マップ エントリの *seq-num* 引数を使用して、マップ エントリにランク付けします。*seq-num* 引数が小さいほど、プライオリティは高くなります。クリプト マップ セットがあるインターフェイスでは、トラフィックは、最初にプライオリティの高いマップ エントリに対して評価されます。

次のいずれかの条件が存在する場合、特定のインターフェイスに複数のクリプト マップ エントリを作成する必要があります。

- データ フローが異なる場合は、別個の IPsec ピアで処理されます。
- 異なるタイプのトラフィックに異なる IPsec セキュリティを適用する場合（たとえば、一方のサブネットのセット間でトラフィックを（同一または別個の IPsec ピアに対して）認証し、もう一方のサブネットのセット間でトラフィックを認証および暗号化する場合）。この場合、異なるタイプのトラフィックが 2 つの個別のアクセス リストに定義されており、クリプト アクセス リストごとに個別のクリプト マップ エントリを作成する必要があります。
- 特定のセットの SA を確立するために IKE を使用しない場合に、複数のアクセス リスト エントリを指定する場合は、別個のアクセス リスト（**permit** エントリごとに 1 つ）を作成し、アクセス リストごとに個別のクリプト マップ エントリを指定する必要があります。

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 SA に使用する設定をネゴシエーションできます。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。

SA の確立に IKE を使用するクリプト マップ エントリを作成するには、次の作業を実行します。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル 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** *map-name seq-num* **ipsec-isakmp** **例：** `Router(config)# crypto map static-map 1 ipsec-isakmp`	作成（または変更）するクリプト マップ エントリに名前を付けて、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	**match address** *access-list-id* **例：** `Router(config-crypto-m)# match address vpn-tunnel`	拡張アクセス リストに名前を付けます。 このアクセス リストは、このクリプト マップ エントリに照らして、IPsec で保護する必要があるトラフィックと、IPsec セキュリティで保護しないトラフィックを決定します。

	コマンド	目的
ステップ 5	**set peer** {*hostname* | *ip-address*} **例：** `Router(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	**set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*] **例：** `Router(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の順に表示します（最もプライオリティの高いものを先頭に表示）。
ステップ 7	**set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes* | **kilobytes disable**} **例：** `Router (config-crypto-m)# set security-association lifetime seconds 2700`	（任意）クリプト マップ エントリの SA ライフタイムを指定します。 デフォルトでは、クリプト マップの SA はグローバル ライフタイムに従ってネゴシエーションされ、これはディセーブルにできます。
ステップ 8	**set security-association level per-host** **例：** `Router(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。 • デフォルトでは、単一の IPsec 「トンネル」で、複数の送信元ホストおよび複数宛先ホストのトラフィックが伝送されます。 **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 9	**set pfs** [**group1** | **group2** | **group 5**] **例：** `Router(config-crypto-map)# set pfs group2`	（任意）IPsec がこのクリプト マップ エントリの新しい SA を要求する場合、Perfect Forward Secrecy（PFS; 完全転送秘密）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。 • 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 10	**exit** **例：** `Router(config-crypto-m)# exit`	クリプト マップ コンフィギュレーション モードを終了します。
ステップ 11	**exit** **例：** `Router(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 12	**show crypto map** [**interface** *interface* | **tag** *map-name*] **例：** `Router# 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することを推奨します（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 を消去するには、**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。この作業を完了するには、「インターフェイスへのクリプト マップ セットの適用」（P.36）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 マップを使用すると、IPsec の設定が簡単になります。ダイナミック クリプト マップは、ピアが常に事前に決定されていないネットワークで使用することを推奨します。ダイナミック クリプト マップを作成するには、次の概念を理解しておく必要があります。

- 「ダイナミック クリプト マップの概要」（P.27）
- 「トンネル エンドポイント ディスカバリ（TED）」（P.28）

ダイナミック クリプト マップの概要

ダイナミック クリプト マップは、IKE だけで利用可能です。

ダイナミック クリプト マップ エントリは、本質的にパラメータがまったく設定されていないスタティック クリプト マップ エントリです。ダイナミック クリプト マップ エントリは、欠落しているパラメータが、リモート ピアの要件に合うように後で動的に設定される（IPsec ネゴシエーションの結果として）ポリシー テンプレートの役割を果たします。この設定により、ルータにリモート ピアの要件のすべてを満たすように特別に設定されたクリプト マップ エントリがなくても、リモート ピアは、IPsec トラフィックをルータと交換することができます。

ルータは、リモート ピアとの新しい IPsec SA を開始する場合にダイナミック クリプト マップを使用しません。ダイナミック クリプト マップは、リモート ピアがルータとの IPsec SA を開始しようとするときに使用されます。また、ダイナミック クリプト マップは、トラフィックの評価にも使用されます。

ダイナミック クリプト マップ セットは、クリプト マップセットの一部としてリファレンスに含まれます。ダイナミック クリプト マップ セットを参照するクリプト マップ エントリはすべて、クリプト マップ セット内でプライオリティが最低のマップ エントリ（シーケンス番号が最大）であって、他のクリプト マップ エントリが最初に評価されるようにする必要があります。つまり、他の（スタティック）マップ エントリが正常に一致しないときだけ、ダイナミック クリプト マップ セットが調べられます。

ルータが新しい IPsec SA をインストールした時点でピアの要求を受け入れると、一時クリプト マップ エントリもインストールされます。このエントリには、ネゴシエーションの結果が入れられます。この時点で、ルータは、この一時クリプト マップ エントリを通常のエントリとして使用して、通常の処理を実行します。さらに、現在の SA が失効する場合は（一時クリプト マップ エントリで指定されたポリシーに基づいて）、新しい SA を要求します。フローが失効する（つまり、対応する SA がすべて期限切れになる）と、一時クリプト マップ エントリは削除されます。

スタティック クリプト マップとダイナミック クリプト マップのどちらについても、保護されていない着信トラフィックがアクセス リストの **permit** 文と一致し、対応するクリプト マップ エントリが「IPsec」とタグ付けされた場合、トラフィックは IPsec 保護されていないため、廃棄されます（これは、クリプト マップ エントリによって指定されたセキュリティ ポリシーにより、このトラフィックを IPsec 保護する必要があると明記されているからです）。

スタティック クリプト マップ エントリの場合、発信トラフィックがアクセス リストの **permit** 文と一致し、対応する SA がまだ確立されていなければ、ルータは、リモート ピアとの新しい SA を開始します。ダイナミック クリプト マップ エントリの場合、SA が存在しなければ、トラフィックは単に廃棄されます（ダイナミック クリプト マップが新しい SA の開始に使用されないため）。

（注） ダイナミック クリプト マップの **permit** エントリに **any** キーワードを使用する場合には、注意が必要です。このような **permit** エントリによってカバーされるトラフィックが、マルチキャストまたはブロードキャスト トラフィックを含めることが可能な場合は、アクセス リストには該当するアドレス範囲に対する **deny** エントリも含める必要があります。アクセス リストには、ネットワークおよびサブネット ブロードキャスト トラフィック、および IPsec 保護しない他のトラフィックの **deny** エントリも含める必要があります。

ダイナミック クリプト マップに関する制約事項

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。

トンネル エンドポイント ディスカバリ（TED）

ダイナミック クリプト マップを定義すると、受信側ルータだけが動的に IPsec ピアを決定できるようになります。TED を使用すると、セキュアな IPsec 通信を行うために、発信側ルータが IPsec ピアを動的に決定できます。

ダイナミック TED は、大規模なネットワーク内の個々のルータでの IPsec 設定を簡素化する場合に役立ちます。各ノードには簡単な設定があり、この設定により、ルータが保護するローカル ネットワークおよび必要な IPsec トランスフォームが定義されます。

TED を*使用せずに*大規模な、フルメッシュ ネットワークを配置するには、各ピアがネットワーク内の他のピアすべてに対してスタティック クリプト マップを持っている必要があります。たとえば、大規模なフルメッシュ ネットワークに 100 のピアがある場合、各ルータは、そのルータの各ピアに対して 99 のスタティック クリプト マップを必要とします。TED を使用すると、ピアが動的に検出されるので、必要となるのは、TED がイネーブルのダイナミック クリプト マップ 1 つだけです。したがって、ピアごとにスタティック クリプト マップを設定する必要はありません。

（注） TED は、ピアを検出する場合だけに効果を発揮します。それ以外の場合、TED の機能は通常の IPsec と何ら変わりありません。TED は、IPsec のスケーラビリティ（性能あるいは、ピアまたはトンネルの数において）を向上させるものではありません。

図 4 および対応するステップでは、サンプルの TED ネットワーク トポロジについて説明します。

図 4　トンネル エンドポイント ディスカバリのサンプル ネットワーク トポロジ

ステップ 1　ホスト A は、ホスト B に転送されるパケットを送信します。

ステップ 2　ルータ 1 はパケットを捕捉し、解読します。IKE ポリシーに従って、ルータ 1 には、情報（パケットを暗号化する必要がある、パケットの SA がない、TED がイネーブルである）が含まれます。そのため、ルータ 1 はパケットを廃棄し、TED プローブをネットワークに送信します。TED プローブには、ペイロードに組み込まれているホスト A（送信元 IP アドレスとして）の IP アドレスとホスト B（宛先 IP アドレスとして）の IP アドレスが含まれています。

ステップ 3　ルータ 2 は TED プローブを捕捉し、プローブを保護対象の ACL と照合してチェックします。プローブが ACL と一致すると、そのプローブは、ルータによって保護されるプロキシの TED プローブとして認識されます。次に、ルータ 2 は、ホスト B の IP アドレス（送信元 IP アドレス）と、ホスト A の IP アドレス（宛先 IP アドレス）をペイロードに組み込んで、TED 応答を送信します。

ステップ 4　ルータ 1 は、TED 応答を捕捉し、ルータ 2 の IP アドレスおよびハーフ プロキシに対してペイロードをチェックします。ルータ 1 は、そのプロキシの送信元側を 2 番目のペイロードで検出されたプロキシと組み合せ、ルータ 2 との IKE セッションを開始します。その後、ルータ 1 は、ルータ 2 との IPsec セッションを開始します。

（注）　ピアが識別されるまで、IKE は発生しません。

TED のバージョン

次の表に、利用可能な TED バージョンを示します。

バージョン	利用可能になった最初のリリース	説明
TEDv1	12.0(5)T	非冗長ネットワークで基本的な TED 機能を実行します。
TEDv2	12.1M	送信元と宛先間の複数のセキュリティ ゲートウェイを通るパスを持つ冗長ネットワークと連動するように拡張されました。
TEDv3	12.2M	非 IP 関連エントリをアクセス リストで使用できるように拡張されました。

TED に関する制約事項

TED には、次の制約事項があります。

- これは、シスコ独自の機能です。
- ダイナミック クリプト マップだけで使用できます（ダイナミック クリプト マップ テンプレートは、ピア検出を実行するダイナミック クリプト マップに基づきます。ダイナミック クリプト マップ テンプレートには、アクセス リストの制約事項はありませんが、ダイナミック クリプト マップ テンプレートは、**any** キーワードを使用して、保護されたトラフィックから送信されたデータおよ

び受信側ルータをカバーする必要があります。**any** キーワードを使用する場合は、明示的に **deny** 文を指定してルーティング プロトコル トラフィックを除外したうえで、**permit any** コマンドを入力してください)。

- TED はトンネル モードだけで動作し、トランスポート モードでは動作しません。
- TED は、個々のプラットフォームでの IPsec のパフォーマンスおよびスケーラビリティに関する制限条件によって制限されます。

(注) TED をイネーブルにすると、ピア検出の設定オーバーヘッドにより、IKE メッセージの追加の「ラウンドトリップ」(TED プローブおよび応答) が発生するため、IPsec の全般的なスケーラビリティは若干低下します。ピア検出段階でデータ構造の保管に使用されるメモリ量は最小限に抑えられていますが、IPsec の全般的なスケーラビリティに悪影響を及ぼします。

- IP アドレスは、ネットワーク内でルーティング可能である必要があります。
- TED 用のクリプト マップで使用されたアクセス リストには、IP 関連エントリだけを含めることができます。このアクセス リストでは、TCP、UDP、またはその他のプロトコルを使用できません。

(注) この制限事項は、TEDv3 で適用されなくなりました。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル 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 dynamic-map** *dynamic-map-name dynamic-seq-num* **例：** `Router(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：** `Router(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の順に表示します（最もプライオリティの高いものを先頭に表示）。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。

	コマンド	目的
ステップ 5	**match address** *access-list-id* **例：** `Router(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にアクセスします。 • 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。 • ダイナミック クリプト マップ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** 文の範囲内である必要があります。 • ダイナミック クリプト マップが設定されていない場合、ルータは、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、ダイナミック クリプト マップ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、ルータはすべてのパケットを廃棄します。スタティック クリプト マップでもアクセス リストの指定が必要なので、これはスタティック クリプト マップに似ています。 • アクセス リストはネゴシエーションだけでなくパケット フィルタリングでも使用されるため、**any** キーワードをアクセス リストで使用する場合には注意が必要です。 • 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：** `Router(config-crypto-m)# set peer 192.168.101.1`	（任意）リモート IPsec ピアを指定します。複数のリモート ピアに対して、同じ作業を繰り返します。 **（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* | **kilobytes disable**} **例：** `Router(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。

	コマンド	目的
ステップ 8	**set pfs** [**group1** | **group2** | **group5**] **例：** `Router(config-crypto-m)# set pfs group2`	(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。 • 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：** `Router(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：** `Router(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：** `Router# 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：** `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 13	**crypto map** *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name* [**discover**] **例：** `Router(config)# crypto map static-map 1 ipsec-isakmp dynamic test-map 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 をイネーブルにするには、**discover** キーワードを発行する必要があります。

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することを推奨します（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 を消去するには、**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。この作業を完了するには、「インターフェイスへのクリプト マップ セットの適用」（P.36）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

手動による SA は、ローカル ルータのユーザと IPsec ピアのユーザとで事前に合意したうえで使用します。両者は、手動による SA を開始してから、IKE によって確立された SA を使用できるようになります。この操作を行わないと、リモート側のシステムが IKE をサポートしないことがあります。SA の確立に IKE を使用しない場合、SA のネゴシエーションは行われません。IPsec がトラフィックを正常に処理するには、両システムの設定情報が同一である必要があります。

ローカル ルータは、単一のクリプト マップ セット内であっても、手動および IKE によって確立された SA を同時にサポートできます。

ローカル ルータで IKE をディセーブルにする理由はほぼありません（ルータが手動による SA だけサポートしている場合を除きますが、このようなことはまずありません）。

（注） **ipsec-manual** とタグ付けされたクリプト マップ エントリのアクセス リストでは、**permit** エントリは 1 つに制限され、それ以降のエントリは無視されます。つまり、特定のクリプト マップ エントリによって確立された SA は、その単一のデータ フロー専用です。異なる種類のトラフィックごとに、手動で確立された複数の SA をサポートできるようにするには、複数のクリプト アクセス リストを定義し、これらのリストを 1 つずつ **ipsec-manual** クリプト マップ エントリに適用します。各アクセス リストには、保護するトラフィックを定義する **permit** 文が 1 つ含まれている必要があります。

クリプト マップ エントリを作成して手動による SA を確立するには（つまり、SA の確立に IKE を使用しない場合）、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* **ipsec-manual**
4. **match address** *access-list-id*
5. **set peer** {*hostname* | *ip-address*}
6. **set transform-set** *transform-set-name*
7. **set session-key inbound ah** *spi hex-key-string*

   または

   set session-key outbound ah *spi hex-key-string*
8. **set session-key inbound esp** *spi* **cipher** *hex-key-string* [**authenticator** *hex-key-string*]

   または

   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	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル 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** *map-name seq-num* **ipsec-manual** **例：** `Router(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。
ステップ 4	**match address** *access-list-id* **例：** `Router(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：** `Router(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：** `Router(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	**set session-key inbound ah** *spi hex-key-string* **例：** `Router(config-crypto-m)# set session-key inbound ah 256 98765432109876549876543210987654` または **set session-key outbound ah** *spi hex-key-string* **例：** `Router(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 Security Parameter Index（SPI; セキュリティ パラメータ インデックス）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 SA を手動で指定します)

	コマンド	目的
ステップ 8	**set session-key inbound esp** *spi* **cipher** *hex-key-string* [**authenticator** *hex-key-string*] **例：** `Router(config-crypto-m)# set session-key inbound esp 256 cipher 0123456789012345` または **set session-key outbound esp** *spi* **cipher** *hex-key-string* [**authenticator** *hex-key-string*] **例：** `Router(config-crypto-m)# set session-key outbound esp 256 cipher abcdefabcdefabcd`	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 ESP SPI およびキーを設定します。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 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 SA を手動で指定します）。
ステップ 9	**exit** **例：** `Router(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：** `Router(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：** `Router# 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 を消去するには、**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。この作業を完了するには、「インターフェイスへのクリプト マップ セットの適用」（P.36）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

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。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、ルータには、接続中にクリプト マップ セットに対してすべてのインターフェイスのトラフィックを評価し、暗号で保護するトラフィックのために、指定されたポリシーまたは SA のネゴシエーション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。

同じクリプト マップを共有する冗長インターフェイス

冗長性を確保するために、同じクリプト マップ セットを複数のインターフェイスに適用できます。デフォルトの動作は次のとおりです。

- 各インターフェイスには、専用の SA データベースがあります。
- ローカル インターフェイスの IP アドレスは、このインターフェイスから発信された IPsec トラフィックまたは、そのインターフェイスに送信される IPsec トラフィックのローカル アドレスとして使用されます。

冗長性を確保するために、同じクリプト マップ セットを複数のインターフェイスに適用する場合は、識別インターフェイスを指定する必要があります。識別インターフェイスとしてループバック インターフェイスを使用することを推奨します。これには、次のような効果があります。

- IPsec SA データベースの per-interface 部分は一度確立されると、同じクリプト マップを共有するすべてのインターフェイスを通過するトラフィックで共有されます。
- 識別インターフェイスの IP アドレスは、同じクリプト マップ セットを共有する、IPsec トラフィックの発信元または送信先インターフェイスのローカル アドレスとして使用されます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル 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：** `Router(config)# Interface FastEthernet 0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**crypto map** *map-name* **例：** `Router(config-if)# crypto map mymap`	インターフェイスに対してクリプト マップ セットを適用します。
ステップ 5	**exit** **例：** `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 6	**crypto map** *map-name* **local-address** *interface-id* **例：** `Router(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：** `Router(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：** `Router# 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

AES を使用するスタティック クリプト マップの例

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
 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
!
```

その他の参考資料

関連資料

内容	参照先
IKE の設定	『Configuring IKE for IPsec VPNs』フィーチャ モジュール
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*』
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』フィーチャ モジュール
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)』フィーチャ モジュール
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)』フィーチャ モジュール
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』および『Configuring Internet Key Exchange Version 2 (IKEv2)』フィーチャ モジュール
PKI の証明書登録のための Suite-B サポート	『Configuring Certificate Enrollment for a PKI』フィーチャ モジュール

規格

規格	タイトル
なし	—

MIB

MIB	MIB 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	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 2402	『*IP Authentication Header*』
RFC 2403	『*The Use of HMAC-MD5-96 within ESP and AH*』

RFC	タイトル
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	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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 VPN のセキュリティの機能情報

表 4 に、この機能のリリース履歴を示します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 4 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。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。

表 4　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
高度暗号化規格	12.2(8)T	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。 この機能に関する詳細については、次の各項を参照してください。 • 「サポートされる規格」（P.3） • 「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」（P.17） この機能により、**crypto ipsec transform-set**、**encryption（IKE ポリシー）**、**show crypto ipsec transform-set**、**show crypto isakmp policy** の各コマンドが変更されました。
DES/3DES/AES VPN 暗号化モジュール（AIM-VPN/EPII、AIM-VPN/HPII、AIM-VPN/BPII ファミリ）	12.3(7)T	この機能により、特定の Cisco IOS ソフトウェア リリースでサポートされる VPN 暗号化ハードウェア AI および NM が示されます。 この機能に関する詳細については、次の項を参照してください。 • 「AIM および NM のサポート」（P.5）
SEAL 暗号化	12.3(7)T	この機能により、IPsec での SEAL 暗号化に対するサポートが追加されました。 この機能に関する詳細については、次の項を参照してください。 • 「サポートされる規格」（P.3） • 「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」（P.17） この機能により、**crypto ipsec transform-set** コマンドが変更されました。

表 4　IPsec VPN のセキュリティ設定に関する機能情報 （続き）

機能名	ソフトウェア リリース	機能情報
ソフトウェア IPPCP（LZS）とハードウェア暗号化の併用	12.2(13)T	VPN モジュールが Cisco 2600 および Cisco 3600 シリーズ ルータに搭載されている場合、この機能により、IPsec で LZS ソフトウェア圧縮を使用できます。 この機能に関する詳細については、次の項を参照してください。 • 「AIM および NM のサポート」（P.5）
ボリューム ベースの IPsec ライフタイム キーの再作成をディセーブルにするオプション	15.0(1)M	この機能により、大量のデータ処理時の IPsec セキュリティ アソシエーション キーの再作成をディセーブルにできます。 この機能に関する詳細については、次の項を参照してください。 • 「クリプト マップ セットの作成」（P.22） この機能により、**crypto ipsec security association lifetime** コマンドと **set security-association lifetime** コマンドが変更されました。

表 4　IPsec VPN のセキュリティ設定に関する機能情報 （続き）

機能名	ソフトウェア リリース	機能情報
IKEv2 プロポーザルのサポート	15.1(1)T	IKEv2 プロポーザルは、IKE_SA_INIT 交換の一部として IKEv2 SA のネゴシエーションに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。 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。 • 「IKEv2 トランスフォーム セット」（P.8） • 「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」（P.17） この機能により、次のコマンドが変更されました。**crypto ikev2 proposal**、**encryption (ikev2 proposal)**、**group (ikev2 proposal)**、**integrity (ikev2 proposal)**、**show crypto ikev2 proposal**
IOS SW の暗号化での Suite-B のサポート	15.1(2)T	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、および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。 この機能に関する詳細については、次の各項を参照してください。 • 「IKEv2 トランスフォーム セット」（P.8） • 「IKE および IPsec 暗号化アルゴリズムでの Cisco IOS Suite-B のサポート」（P.10） • 「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」（P.17） この機能により、**crypto ipsec transform-set** コマンドが変更されました。