SA-VAM2 の設定

この章では、Service Adapter VPN Acceleration Module 2（SA-VAM2）を設定する際に必要な情報および手順を示します。この章で説明する内容は、次のとおりです。

概要

SA-VAM2 は、Network Processing Engine（NPE; ネットワーク処理エンジン）225（NPE-225）、400（NPE-400）、G1（NPE-G1）を搭載した Cisco 7200VXR ルータ、および Cisco 7301 ルータの任意のインターフェイスに暗号化サービスを提供します。IP Security Protocol（IPSec）が設定済みのルータに SA-VAM2 を搭載すると、SA-VAM2 は暗号化サービスを自動的に実行します。2 番めの SA-VAM2 を搭載すると、両方の SA-VAM2 が自動的にイネーブルになります。

（注）　Cisco 7301 ルータは、SA-VAM2 を 1 つだけサポートします。

（注）　Cisco 7200VXR ルータに 2 つの SA-VAM2 を搭載する場合、パケット単位でのロードバランスはサポートされません。2 つの SA-VAM2 を搭載した場合には、パケット単位でなく、IPSec トンネル単位でロードバランスが行われます。

SA-VAM2 上には設定するインターフェイスはありません。

ここでは、暗号化および IPSec トンネリング サービスを実施するための基本的な設定に限定して説明します。IPSec、Internet Key Exchange（IKE）、および CA（認証局）の設定の詳細については、『*Security Configuration Guide*』の「IP Security and Encryption」、および『*Security Command Reference*』を参照してください。

設定作業

（注）　Cisco 7200VXR Port Adapter Jacket Card は設定不要です。ここで説明するとおりに SA-VAM2 を設定します。

起動時に ENABLED LED が点灯した場合、SA-VAM2 は完全に動作しており、コンフィギュレーション コマンドは不要です。ただし、SA-VAM2 で暗号化サービスを提供する場合には、ここで説明する手順を行う必要があります。

- EXEC コマンド インタープリタの使用方法（p.4-4）（必須）
- OIR のディセーブル化（p.4-4）（必須）
- IKE ポリシーの設定（p.4-5）（必須）
- トランスフォーム セットの設定（p.4-6）（必須）
- IPSec の設定（p.4-10）（必須）
- 圧縮の設定（p.4-17）（任意）
- IPSec の設定例（p.4-20）（任意）
- IKE および IPSec の設定の確認（p.4-21）（任意）

（注）　スタティック クリプト マップの設定、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 マップのスタティック クリプト マップへの追加ができます。オンライン マニュアル『*Configuring the VPN Acceleration Module*』（http://www.cisco.com/univercd/cc/td/doc/product/core/7100/7100pacn/vam1/vamconf.htm）を参照してください。

任意で、CA インターオペラビリティを設定できます（『*Security Configuration Guide*』の「Configuring Certification Authority Interoperability」を参照）。

EXEC コマンド インタープリタの使用方法

EXEC（別名イネーブル モード）というソフトウェア コマンド インタープリタを使用して、ルータのコンフィギュレーションを変更します。**configure** コマンドを使用して新しいインターフェイスを設定する、またはインターフェイスの従来の設定を変更するには、その前に **enable** コマンドで EXEC コマンド インタープリタのイネーブル レベルを開始する必要があります。パスワードが設定されている場合は、パスワードを要求するプロンプトが表示されます。

イネーブル レベルのシステム プロンプトは、かぎカッコ（>）ではなくポンド記号（#）で終わります。コンソール端末から、次の手順でイネーブル レベルを開始します。

ステップ 1　ユーザ レベルの EXEC プロンプトから、**enable** コマンドを入力します。次のように、イネーブル パスワードが要求されます。

```
Router> enable

Password:
```

ステップ 2　パスワードを入力します。パスワードでは大文字と小文字が区別されます。機密保護のために、パスワードは表示されません。有効なパスワードを入力すると、イネーブル レベルのシステム プロンプト（#）が表示されます。

```
Router#
```

EXEC コマンド インタープリタのイネーブル レベルを開始する手順は、これで完了です。

OIR のディセーブル化

SA-VAM2 では、デフォルトで Online Insertion and Removal（OIR; ホットスワップ）がイネーブルです。

SA-VAM2 の OIR をディセーブルにするには、グローバル コンフィギュレーション モードを開始して次のコマンドを使用します。

	コマンド	目的
ステップ 1	**no crypto engine accelerator** *<slot number>*	SA-VAM2 の OIR をディセーブルにします。
ステップ 2	**crypto engine accelerator** *<slot number>*	SA-VAM2 の OIR をイネーブルにします。

OIR をディセーブルおよびイネーブルにする手順は、これで完了です。

IKE ポリシーの設定

パラメータ値を指定しない場合は、デフォルト値が使用されます。デフォルト値については、『*Security Command Reference*』の「IP Security and Encryption」を参照してください。

IKE ポリシーを設定するには、グローバル コンフィギュレーション モードを開始して、次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# crypto isakmp policy` *priority*	IKE ポリシーを定義し、Internet Security Association Key Management Protocol（ISAKMP）ポリシー コンフィギュレーション（config-isakmp）モードを開始します。
ステップ 2	`Router(config-isakmp)# encryption {des | 3des | aes | aes 192 | aes 256}`	IKE ポリシーの暗号化アルゴリズムを指定します。 • **des —** 56 ビット DES を暗号化アルゴリズムとして指定します。 • **3des —** 168 ビット DES を暗号化アルゴリズムとして指定します。 • **aes —** 128 ビット AES を暗号化アルゴリズムとして指定します。 • **aes 192 —** 192 ビット AES を暗号化アルゴリズムとして指定します。 • **aes 256 —** 256 ビット AES を暗号化アルゴリズムとして指定します。
ステップ 3	`Router(config-isakmp)# authentication {rsa-sig | rsa-encr | pre-share}`	（任意）IKE ポリシーの認証方式を指定します。 • **rsa-sig** — RSA シグニチャを認証方式として指定します。 • **rsa-encr —** RSA 暗号化 nonces を認証方式として指定します。 **（注）** Cisco IOS Release 12.3(10) 以降では、rsa-encr は SA-VAM2 暗号化カードでイネーブルです。 • **pre-share —** 事前共有鍵を認証方式として指定します。 **（注）** このコマンドをイネーブルにしない場合、デフォルト値（***rsa-sig***）が使用されます。
ステップ 4	`Router(config-isakmp)# lifetime` *seconds*	（任意）IKE Security Association（SA）のライフタイムを指定します。 *seconds* **—** 各 SA が期限切れになるまでの秒数。60 ～ 86,400 秒の範囲の整数を使用します。 **（注）** このコマンドをイネーブルにしない場合、デフォルト値（86,400 秒 [1 日]）が使用されます。

	コマンド	目的
ステップ 5	`Router(config-isakmp)# hash {sha | md5}`	（任意）IKE ポリシーのハッシュ アルゴリズムを指定します。 • **sha** — SHA-1（HMAC バリアント）をハッシュ アルゴリズムとして指定します。 • **md5** — MD5（HMAC バリアント）をハッシュ アルゴリズムとして指定します。 **（注）** このコマンドをイネーブルにしない場合、デフォルト値（**sha**）が使用されます。
ステップ 6	`Router(config-isakmp)# group {1 | 2 | 5}`	（任意）IKE ポリシーの Diffie-Hellman（DH）グループ識別子を指定します。 **1** — 768 ビット DH グループを指定します。 **2** — 1024 ビット DH グループを指定します。 ***5*** — 1536 ビット DH グループを指定します。 **（注）** このコマンドをイネーブルにしない場合、デフォルト値（768 ビット）が使用されます。

IKE ポリシー作成の詳細については、『*Security Configuration Guide*』の「Configuring Internet Key Exchange Security Protocol」を参照してください。

トランスフォーム セットの設定

トランスフォーム セット設定の詳細については、『*Advanced Encryption Standard (AES)*』フィーチャ モジュールを参照してください。

ここで説明する内容は次のとおりです。

- トランスフォーム セットの定義
- IPSec プロトコル：AH および ESP
- 適切なトランスフォームの選択
- 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
- 既存のトランスフォームの変更
- トランスフォームの例

トランスフォーム セットは、IPSec で保護するトラフィックに対して適用する設定（セキュリティ プロトコル、アルゴリズムなど）の適切な組み合わせです。IPSec SA のネゴシエーションを行うとき、特定のデータ フローを保護するために特定のトランスフォーム セットを使用することがピア間で合意されます。

トランスフォーム セットの定義

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組み合わせです。IPSec SA のネゴシエーションを行うとき、特定のデータ フローを保護するために特定のトランスフォーム セットを使用することがピア間で合意されます。

トランスフォーム セットを定義するには、グローバル コンフィギュレーション モードを開始して、次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# crypto ipsec transform-set` *transform-set-name transform1* [*transform2* [*transform3*]]	トランスフォーム セットを定義し、クリプト トランスフォーム コンフィギュレーション モードを開始します。 • *transform-set-name* — 作成（または変更）するトランスフォーム セットの名前を指定します。 • *transform1* [*transform2* [*transform3*] [*transform4*]] — IPSec セキュリティ プロトコルおよびアルゴリズムを定義します。指定できるトランスフォーム値については、表 4-1 を参照してください。
ステップ 2	`Router(cfg-crypto-tran)# mode [tunnel | transport]`	（任意）トランスフォーム セットに関連付けるモードを変更します。このモード設定は、送信元 / 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、その他のトラフィックについては無視されます（他のトラフィックはすべて、トンネル モードのみです）。
ステップ 3	**end**	クリプト トランスフォーム コンフィギュレーション モードを終了してイネーブル モードに戻ります。
ステップ 4	**clear crypto sa** または **clear crypto sa peer** {*ip-address* | *peer-name*} または **clear crypto sa map** *map-name* または **clear crypto sa spi** *destination-address protocol spi*	既存の IPSec SA を解消し、今後確立される SA でトランスフォーム セットの変更が有効になるようにします（手動で設定した SA は、ただちに再確立されます）。 パラメータを指定せずに **clear crypto sa** コマンドを実行すると、SA データベースの全内容が消去されるので、アクティブなセキュリティ セッションも消去されます。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** キーワードを指定します。

表 4-1 に、Authentication Header（AH）および Encapsulating Security Payload（ESP）プロトコルの有効なトランスフォームの組み合わせを示します。

表 4-1　使用でき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	内容
AH トランスフォーム（最大で 1 つを選択）	**ah-md5-hmac**	Message Digest 5（MD5）（HMAC バリアント）認証アルゴリズムを使用する AH
	ah-sha-hmac	Secure Hash Algorithm（SHA）（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（注 : **ESP 認証トランスフォーム**を使用する場合、いずれか 1 つを選択する必要があります。）	**esp-aes**	128 ビットの AES 暗号化アルゴリズムを使用する ESP
	esp-aes 192	192 ビットの AES 暗号化アルゴリズムを使用する ESP
	esp-aes 256	256 ビットの AES 暗号化アルゴリズムを使用する ESP
	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 ビットの DES 暗号化アルゴリズム（3DES つまり Triple DES）を使用する ESP
	esp-null	ヌル暗号化アルゴリズム
ESP 認証トランスフォーム（最大で 1 つを選択）	**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（最大で 1 つを選択）	**comp-lzs**	Lempel-Ziv-Stac（LZS）アルゴリズムを使用する IP 圧縮

指定できるトランスフォームの組み合わせを次に示します。

- ***ah-md5-hmac***
- ***esp-des***
- ***esp-3des*** および ***esp-md5-hmac***
- ***ah-sha-hmac*** および ***esp-des*** および ***esp-sha-hmac***
- ***comp-lzs***

無効な組み合わせを入力すると、解析プログラムによって拒否されます。たとえば、特定の AH トランスフォームを指定した場合、現在のトランスフォーム セットに別の AH トランスフォーム を指定することはできません。

IPSec プロトコル：AH および ESP

AH プロトコルおよび ESP プロトコルは、IPSec にセキュリティ サービスを実装します。

AH は、データ認証および抗リプレー サービスを提供します。

ESP は、パケット認証のほかに、任意選択でデータ認証および抗リプレー サービスを提供します。

ESP は保護対象のデータ（完全な IP データグラムまたはペイロードのみ）を、ESP ヘッダーおよび ESP トレーラーでカプセル化します。AH は保護対象のデータに埋め込まれる形になり、外側の IP ヘッダーの直後、および内側の IP データグラムまたはペイロードの直前に AH ヘッダーを挿入します。IPSec ピア間で送受信されるトラフィックは、トンネル モードまたはトランスポート モードのいずれかで送信できます。その他のトラフィックはすべてトンネル モードで送信されます。トンネル モードは IP データグラム全体をカプセル化して保護するのに対し、トランスポート モードは IP データグラムのペイロードをカプセル化して保護します。モードについての詳細は、**mode（IPSec）** コマンドの説明を参照してください。

適切なトランスフォームの選択

状況に適したトランスフォームを選択するには、次のヒントを参考にしてください。

- データの機密保護を提供するには、ESP 暗号化トランスフォームを使用します。
- データのほかに外側の IP ヘッダーについてもデータ認証が必要な場合は、AH トランスフォームを含めます（IP ヘッダー データの整合性には、あまり利点がないとする見方もあります）。
- ESP 暗号化トランスフォームを使用する場合は、トランスフォーム セットに認証サービスを提供するために、ESP 認証トランスフォームまたは AH トランスフォームを使用することも検討してください。
- （ESP または AH による）データ認証を希望する場合、MD5 または SHA（HMAC キー ハッシュ バリアント）認証アルゴリズムのいずれかを選択できます。SHA アルゴリズムは一般に MD5 よりも強力と考えられますが、やや低速になります。
- IPSec ピアによっては、一部のトランスフォームがサポートされない場合があるので注意してください。

（注） ハードウェア（IPSec ピア）がサポートしていない IPSec トランスフォームを入力すると、**crypto ipsec transform-set** コマンドを入力した直後に警告メッセージが表示されます。

- 暗号化トランスフォームを指定する必要があっても、実際にはパケットを暗号化しない場合、***esp-null*** トランスフォームを使用できます。

考えられるトランスフォームの組み合わせを次に示します。

- ***esp-eas*** および ***esp-sha-hmac***
- ***ah-sha-hmac*** および ***esp-eas*** および ***esp-sha-hmac***

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

crypto ipsec transform-set コマンドを入力すると、クリプト トランスフォーム コンフィギュレーション モードが開始されます。このモードでは、モードをトンネルまたはトランスポートに変更できます（これらの変更は任意選択です）。これらの変更を行ったあと、グローバル コンフィギュレーション モードに戻るには **exit** を使用します。これらの任意選択の変更についての詳細は、**match address**（IPSec）および **mode**（IPSec）コマンドの説明を参照してください。

既存のトランスフォームの変更

既存のトランスフォーム セットに関して **crypto ipsec transform-set** コマンドで 1 つまたは複数のトランスフォームを指定すると、そのトランスフォーム セットの既存のトランスフォームが、指定したトランスフォームで置き換えられます。

トランスフォーム セットの定義を変更した場合、そのトランスフォーム セットを参照するクリプト マップ エントリに対してのみ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、新しい SA を確立する今後のネゴシエーションで使用されます。新しい設定をすぐに有効にするには、**clear crypto sa** コマンドを使用して SA データベースの全体または一部を消去します。

トランスフォームの例

次の例では、2 つのトランスフォーム セットを定義しています。最初のトランスフォーム セットは、新しい ESP プロトコルおよび AH プロトコルをサポートする IPSec ピアで使用されます。2 番めのトランスフォーム セットは、旧来のトランスフォームしかサポートしない IPSec ピアで使用されます。

```
crypto ipsec transform-set newer esp-3des esp-sha-hmac
crypto ipsec transform-set older ah-rfc-1828 esp-rfc1829
```

次に、入力した IPSec トランスフォームがハードウェアでサポートされていない場合に表示される警告メッセージの例を示します。

```
crypto ipsec transform transform-1 esp-aes 256 esp-md5
WARNING:encryption hardware does not support transform
esp-aes 256 within IPSec transform transform-1
```

IPSec の設定

ここで説明する内容は次のとおりです。

- アクセス リストと IPSec の互換性の確保（必須）
- IPSec SA のグローバル ライフタイムの設定（必須）
- クリプト アクセス リストの作成（必須）
- クリプト マップ エントリの作成（必須）
- ダイナミック クリプト マップの作成（必須）
- クリプト マップ セットのインターフェイスへの適用（必須）
- 設定の確認（任意）

IPSec の設定例は、「IPSec の設定例」を参照してください。

IPSec の設定についての詳細は、『*Cisco IOS Security Configuration Guide*』の「Configuring IPSec Network Security」を参照してください。

アクセス リストと IPSec の互換性の確保

IKE は、UDP ポート 500 を使用します。IPSec の ESP および AH プロトコルは、プロトコル番号 50 および 51 を使用します。プロトコル番号 50、51、および UDP ポート 500 のトラフィックが、IPSec を適用するインターフェイス上で阻止されないように、インターフェイスのアクセス リストを設定してください。状況によっては、これらのトラフィックを明示的に許可するステートメントを、アクセス リストに追加する必要があります。

IPSec SA のグローバル ライフタイムの設定

新しい IPSec SA をネゴシエートするときに使用されるグローバル ライフタイム値を変更できます（特定のクリプト マップ エントリについて、これらのグローバル ライフタイム値を上書きできます）。

これらのライフタイムが適用されるのは、IKE で確立する SA だけです。手動で確立する SA には、期限がありません。

IPSec SA のグローバル ライフタイムを変更するには、グローバル コンフィギュレーション モードで次のいずれかのコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# crypto ipsec security-association lifetime seconds seconds`	IPSec SA のグローバル ライフタイム（時間）を変更します。 このコマンドを使用した場合、SA は指定した秒数が経過すると期限切れになります。
ステップ 2	`Router(config)# crypto ipsec security-association lifetime kilobytes kilobytes`	IPSec SA のグローバル ライフタイム（トラフィック量）を変更します。 このコマンドを使用した場合、SA を使用する IPSec「トンネル」を指定した量（単位：キロバイト）のトラフィックが通過した時点で、SA が期限切れになります。

ステップ 3	`Router(config)# clear crypto sa`
	または
	`Router(config)# clear crypto sa peer {ip-address | peer-name}`
	または
	`Router(config)# clear crypto sa map map-name`
	または
	`Router (config)# clear crypto sa entry destination-address protocol spi`
		（任意）既存の SA を消去します。この場合、既存の SA はただちに期限切れになり、今後の SA は新しいライフタイムを使用するようになります。これらのコマンドを使用しない場合、既存の SA はあらかじめ設定されたライフタイムに応じて期限切れになります。
		（注） パラメータを指定せずに **clear crypto sa** コマンドを実行すると、SA データベースの全内容が消去されるので、アクティブなセキュリティ セッションも消去されます。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** キーワードを指定します。詳細については、**clear crypto sa** コマンドを参照してください。

クリプト アクセス リストの作成

クリプト アクセス リストでは、暗号化によって保護される IP トラフィックを定義します（これらのアクセス リストは、インターフェイスで転送またはブロックすべきトラフィックを指定する通常のアクセス リストとは*異なります*）。たとえば、サブネット A とサブネット Y の間の IP トラフィックをすべて保護するアクセス リストや、ホスト A とホスト B の間の Telnet トラフィックをすべて保護するアクセス リストを作成できます。

クリプト アクセス リストを作成するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# access-list` *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**] または `Router(config)# ip access-list extended` *name*	保護する IP パケットを判別するための条件を指定します[1]（これらの条件に適合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）。 IPSec には「ミラー イメージ」のクリプト アクセス リストを設定し、**any** キーワードは使用しないことを推奨します。
ステップ 2	必要に応じて、**permit** および **deny** ステートメントを追加します。	アクセス リストに許可または拒否のステートメントを追加します。
ステップ 3	**End**	コンフィギュレーション コマンド モードを終了します。

1. 条件を設定するには、対応する IP アクセス リストの番号または名前を指定します。**access-list** コマンドには、拡張アクセス リストの番号を指定します。**ip access-list extended** コマンドには、アクセス リストの名前を指定します。

アクセス リストの設定の詳細については、『*Security Configuration Guide*』の「Configuring IPSec Network Security」を参照してください。

クリプト マップ エントリの作成

クリプト マップ セットは、1 つのインターフェイスに対して 1 つのみ適用できます。クリプト マップ セットには、IPSec/IKE エントリおよび IPSec/ 手動エントリの組み合わせを含めることができます。複数のインターフェイスで同じクリプト マップ セットを共有させ、複数のインターフェイスに同じポリシーを適用できます。

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には、グローバル コンフィギュレーション モードから始めて次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# crypto map` *map-name seq-num* **ipsec-manual**	作成（または変更）するクリプト マップ エントリを指定します。 このコマンドを使用すると、クリプト マップ コンフィギュレーション モードが開始されます。
ステップ 2	`Router(config-crypto-m)# match address` *access-list-id*	IPSec アクセス リストの名前を指定します。このアクセス リストによって、このクリプト マップ エントリのコンテキストの中で、IPSec で保護するトラフィックと保護しないトラフィックが決定されます。（IKE を使用しない場合は、アクセス リストに指定できる **permit** エントリは 1 つだけです。）

	コマンド	目的
ステップ 3	`Router(config-crypto-m)# set peer {hostname | ip-address}`	リモート IPSec ピアを指定します。これは、IPSec で保護したトラフィックの転送先となるピアです。 （IKE を使用しない場合は、1 つのピアしか指定できません。）
ステップ 4	`Router(config-crypto-m)# set transform-set transform-set-name`	使用するトランスフォーム セットを指定します。 リモート ピアの対応するクリプト マップ エントリに指定されているものと同じトランスフォーム セットでなければなりません。 （IKE を使用しない場合は、1 つのトランスフォーム セットしか指定できません。）

ステップ 5	`Router(config-crypto-m)# set session-key inbound ah spi hex-key-string`
	
	および
	
	`Router(config-crypto-m)# set session-key outbound ah spi hex-key-string`
		指定し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に、保護対象の着信および発信トラフィックに対して適用する AH Security Parameter Index（SPI）および鍵を設定します。
		
		（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。）

ステップ 6	`Router(config-crypto-m)# set session-key inbound esp spi cipher hex-key-string [authenticator hex-key-string]`
	
	および
	
	`Router(config-crypto-m)# set session-key outbound esp spi cipher hex-key-string [authenticator hex-key-string]`
		指定し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に、保護対象の着信および発信トラフィックに対して適用する ESP SPI および鍵を設定します。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に、暗号鍵を指定します。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に、認証鍵を指定します。
		
		（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 7	`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。

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には、グローバル コンフィギュレーション モードから始めて次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# crypto map map-name seq-num ipsec-isakmp`	作成（または変更）するクリプト マップ エントリの名前を指定します。 このコマンドを使用すると、クリプト マップ コンフィギュレーション モードが開始されます。
ステップ 2	`Router(config-crypto-m)# match address access-list-id`	拡張アクセス リストの名前を指定します。このアクセス リストによって、このクリプト マップ エントリのコンテキストの中で、IPSec で保護するトラフィックと保護しないトラフィックが決定されます。
ステップ 3	`Router(config-crypto-m)# set peer {hostname | ip-address}`	リモート IPSec ピアを指定します。これは、IPSec で保護し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。

	コマンド	目的
ステップ 4	`Router(config-crypto-m)# set transform-set` *transform-set-name1* [*transform-set-name2...transform-set-name6*]	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。プライオリティの高い順から、複数のトランスフォーム セットを指定します（最優先するセットを最初に指定します）。
ステップ 5	`Router(config-crypto-m)# set security-association lifetime seconds` *seconds* および `Router (config-crypto-m)# set security-association lifetime kilobytes` *kilobytes*	（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。 グローバル ライフタイム以外の IPSec SA ライフタイムを使用してクリプト マップ エントリの SA をネゴシエートする場合に、このコマンドを使用します。
ステップ 6	`Router(config-crypto-m)# set security-association level per-host`	（任意）送信元 / 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。 このコマンドを使用しない場合、1 つの IPSec「トンネル」で複数の送信元ホストおよび宛先ホストのトラフィックが伝送されます。 このコマンドを使用すると、ルータは新しい SA を要求するとき、ホスト A とホスト B の間のトラフィック用と、ホスト A とホスト C の間のトラフィック用にそれぞれ 1 つずつの SA を確立します。 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、このコマンドは十分に注意して使用してください。
ステップ 7	`Router(config-crypto-m)# set pfs [group1 | group2]`	（任意）IPSec がこのクリプト マップ エントリの新しい SA を要求する場合に Perfect Forward Secrecy（PFS）を要求するか、または IPSec ピアから受信する要求に PFS が含まれていなければならないことを指定します。
ステップ 8	`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。

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 エントリは、一部のパラメータが設定されていないクリプト マップ エントリです。設定されていないパラメータは（IPSec ネゴシエーションの結果）動的に設定されます。ダイナミック クリプト マップは IKE でのみ使用可能です。

ダイナミック クリプト マップ エントリは、セットにまとめられます。セットとは、*dynamic-map-name* が同じで、*dynamic-seq-num* がそれぞれ異なるダイナミック クリプト マップ エントリのグループです。

ダイナミック クリプト マップ エントリを設定するには、グローバル コンフィギュレーション モードから始めて次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# crypto dynamic-map` *dynamic-map-name dynamic-seq-num*	ダイナミック クリプト マップ エントリを作成します。
ステップ 2	`Router(config-crypto-m)# set transform-set` *transform-set-name1* [*transform-set-name2...transform-set-name6*]	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。プライオリティの高い順から、複数のトランスフォーム セットを指定します（最優先するセットを最初に指定します）。 ダイナミック クリプト マップ エントリに必須の設定ステートメントは、これだけです。
ステップ 3	`Router(config-crypto-m)# match address` *access-list-id*	（任意）拡張アクセス リストのアクセス リスト番号または名前。このアクセス リストによって、このクリプト マップ エントリのコンテキストの中で、IPSec で保護するトラフィックと保護しないトラフィックが決定されます。 **（注）** ダイナミック クリプト マップではアクセス リストは任意指定ですが、アクセス リストを指定することを強く推奨します。 設定する場合、IPSec ピアによって提示されるデータ フローのアイデンティティは、このクリプト アクセス リストの **permit** ステートメントで許可されるものでなければなりません。 設定しない場合、ルータは IPSec ピアが提示する任意のデータ フロー アイデンティティを受け入れます。ただし、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場合、または空である場合には、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 マップの場合もアクセス リストを指定する必要があるので、同様の結果になります。 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 フィルタリングにも使用されるので、アクセス リストに **any** キーワードを使用する場合は注意が必要です。
ステップ 4	`Router(config-crypto-m)# set peer` {*hostname* | *ip-address*}	（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。 このコマンドは、ダイナミック クリプト マップ エントリではめったに設定しません。通常、ダイナミック クリプト マップ エントリは不明のリモート ピアを対象に使用します。

	コマンド	目的

ステップ 5	`Router(config-crypto-m)# set security-association lifetime seconds seconds`
	
	および
	
	`Router (config-crypto-m)# set security-association lifetime kilobytes kilobytes`
		（任意）グローバルに指定されたライフタイムではなく、短い IPSec SA ライフタイムを使用してこのクリプト マップの SA をネゴシエートするには、クリプト マップ エントリのライフタイムを指定します。

ステップ 6	`Router(config-crypto-m)# set pfs [group1 | group2]`	（任意）IPSec がこのクリプト マップ エントリの新しい SA を要求する場合に PFS を要求するか、または IPSec ピアから受信する要求に PFS が含まれていなければならないよう指定します。
ステップ 7	`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 8	この手順を繰り返して、必要な数だけクリプト マップ エントリを作成します。	

クリプト マップ セットにダイナミック クリプト マップ セットを追加するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-name`	ダイナミック クリプト マップ セットをスタティック クリプト マップ セットに追加します。

クリプト マップ セットのインターフェイスへの適用

IPSec トラフィックが流れるインターフェイスごとに、クリプト マップ セットを適用します。接続または SA ネゴシエーションが行われるとき、ルータはインターフェイス トラフィックをクリプト マップ セットに照らし合わせて評価し、保護対象のトラフィックに指定されたポリシーを使用します。

クリプト マップ セットをインターフェイスに適用するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)# crypto map map-name`	クリプト マップ セットをインターフェイスに適用します。

冗長インターフェイスを指定し、識別するインターフェイスに名前を付けるには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# crypto map map-name local-address interface-id`	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。

圧縮の設定

ここで説明する内容は次のとおりです。

- IKE ポリシーの設定（必須）
- IKE 事前共有鍵の設定（必須）
- IPSec トランスフォーム セットの設定（必須）
- アクセス リストの設定（必須）
- クリプト マップの設定（必須）
- クリプト マップのインターフェイスへの適用（必須）

IPSec の設定例は、「圧縮の設定例」を参照してください。

IPSec の設定についての詳細は、『*Cisco IOS Security Configuration Guide*』の「Configuring IPSec Network Security」を参照してください。

IKE ポリシーの設定

IKE ポリシーを設定するには、「IKE ポリシーの設定」（p.4-5）の手順に従い、グローバル コンフィギュレーション モードのコマンドを使用します。

IKE 事前共有鍵の設定

ピア側で事前共有鍵を指定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的

ステップ 1	`Router (config)# crypto isakmp key` *keystring* `address peer-address`
	
	または
	
	`Router (config)# crypto isakmp key` *keystring* `hostname peer-hostname`
		ローカル ピア：
		特定のリモート ピアと使用する共有鍵を指定します。
		
		リモート ピアがアドレスを使用して ISAKMP アイデンティティを指定している場合は、このステップで **address** キーワードを使用します。そうでない場合は、このステップで **hostname** キーワードを使用します。

ステップ 2	`Router (config)# crypto isakmp key_`*keystring* `address peer-address`
	
	または
	
	`Router (config)# crypto isakmp key_`*keystring* `hostname peer-hostname`
		リモート ピア：
		ローカル ピアと使用する共有鍵を指定します。これはローカル ピアで指定した鍵と同じです。
		
		ローカル ピアがアドレスを使用して ISAKMP アイデンティティを指定している場合は、このステップで **address** キーワードを使用します。そうでない場合は、このステップで **hostname** キーワードを使用します。

ステップ 3	各リモート ピアについて、上記の 2 ステップを繰り返します。	

IKE ポリシーで事前共有鍵を使用するピアごとに、これらの作業を繰り返します。

IPSec トランスフォーム セットの設定

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可能な組み合わせ）を定義するには、**crypto ipsec transform-set** グローバル コンフィギュレーション コマンドを使用します。トランスフォーム セットを削除するには、このコマンドの **no** 形式を使用します。

コマンド	目的
`Router (config)# crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]]`	*transform-set-name* 作成（または変更）するトランスフォーム セットの名前を指定します。 *transform1* *transform2* *transform3* IPSec セキュリティ プロトコルおよびアルゴリズムを定義するトランスフォームを最大 3 つ（最低でも 1 つ）指定します。

アクセス リストの設定

MAC（メディア アクセス制御）アドレス アクセス リストを設定するには、**access-list** グローバル コンフィギュレーション コマンドを使用します。特定のアクセス リスト エントリを削除するには、このコマンドの **no** 形式を使用します。

コマンド	目的
`Router (config)# access-list access-list-number {permit | deny} address mask`	*access-list-number* このリストの番号（700 ～ 799 の範囲の整数）を指定します。 **permit** フレームを許可します。 **deny** フレームを禁止します。 *address mask* 48 ビットの MAC アドレス（ドット付きの 3 つの数字列で表記）を指定します。この引数で 1 のビットが、アドレス値で無視されるビットになります。

クリプト マップの設定

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には、グローバル コンフィギュレーション モードから始めて次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router (config)# crypto map map-name seq-num ipsec-isakmp`	クリプト マップを作成し、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 2	`Router (config)# set peer {hostname | ip-address}`	リモート IPSec ピアを指定します。これは、IPSec で保護し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。

	コマンド	目的
ステップ 3	`Router (config)# set transform-set transform-set-name1 [transform-set-name2...transform-set-name6]`	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。プライオリティの高い順から、複数のトランスフォーム セットを指定します（最優先するセットを最初に指定します）。
ステップ 4	`Router (config)# match address access-list-id`	拡張アクセス リストを指定します。このアクセス リストでは、トラフィックを IPSec で保護するものと、保護しないものを特定します。

クリプト マップのインターフェイスへの適用

クリプト マップ セットをインターフェイスに適用するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router (config)# interface type number`	クリプト マップを適用す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 2	`Router (config)# crypto map map-name`	クリプト マップ セットをインターフェイスに適用します。
ステップ 3	`Router (config)# end`	インターフェイス コンフィギュレーション モードを終了します。

SA-VAM2 に圧縮を設定する手順は、これで完了です。

IPSec のモニタリングおよびメンテナンス

IPSec SA を消去（再初期化）するには、グローバル コンフィギュレーション モードで次のいずれかのコマンドを使用します。

コマンド	目的

`Router(config)# clear crypto sa`
 	
または
 	
`Router(config)# clear crypto sa peer {ip-address | peer-name}`
 	
または
 	
`Router(config)# clear crypto sa map map-name`
 	
または
 	
`Router(config)# clear crypto sa entry destination-address protocol spi`
	IPSec SA を消去します。
	
	（注） パラメータを指定せずに **clear crypto sa** コマンドを実行すると、SA データベースの全内容が消去されるので、アクティブなセキュリティ セッションも消去されます。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** キーワードを指定します。詳細については、**clear crypto sa** コマンドを参照してください。

IPSec の設定に関する情報を表示するには、EXEC モードで次のいずれかのコマンドを使用します。

コマンド	目的
Router# **show crypto ipsec transform-set**	トランスフォーム セットの設定を表示します。
Router# **show crypto map** [**interface** *interface* | **tag** *map-name*]	クリプト マップの設定を表示します。
Router# **show crypto ipsec sa** [**map** *map-name* | **address** | **identity**] [**detail**]	IPSec SA に関する情報を表示します。
Router# **show crypto dynamic-map** [**tag** *map-name*]	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。
Router# **show crypto ipsec security-association lifetime**	グローバルな SA ライフタイム値を表示します。

IPSec の設定例

次に、IKE によって SA が確立される、最小限の IPSec の設定例を示します。IKE の詳細については、「Configuring Internet Key Exchange Security Protocol」を参照してください。

IPSec アクセス リストで、保護するトラフィックを定義します。

```
access-list 101 permit ip 10.0.0.0 0.0.0.255 10.2.2.0 0.0.0.255
```

トランスフォーム セットで、トラフィックの保護方法を定義します。この例では、トランスフォーム セット [myset1] で DES 暗号化および SHA を使用して、データ パケットを認証します。

```
crypto ipsec transform-set myset1 esp-des esp-sha
```

次のトランスフォーム セットの例 [myset2] では、3DES 暗号化および MD5（HMAC バリアント）を使用して、データ パケットを認証します。

```
crypto ipsec transform-set myset2 esp-3des esp-md5-hmac
```

クリプト マップは IPSec アクセス リストとトランスフォーム セットを結合し、保護するトラフィックの送信先（リモート IPSec ピア）を指定します。

```
crypto map toRemoteSite 10 ipsec-isakmp
 match address 101
 set transform-set myset2
 set peer 10.2.2.5
```

クリプト マップをインターフェイスに適用します。

```
interface Serial0
 ip address 10.0.0.2
 crypto map toRemoteSite
```

（注）　この例では、IKE をイネーブルにする必要があります。

IKE および IPSec の設定の確認

IPSec の設定に関する情報を表示するには、**show crypto ipsec transform-set** EXEC コマンドを使用します。

（注）　ハードウェア（IPSec ピア）がサポートしていない IPSec トランスフォームを入力すると、**show crypto ipsec transform-set** の出力に警告メッセージが表示されます。

次に示す **show crypto ipsec transform-set** コマンドの出力例では、ハードウェアがサポートしていない IPSec トランスフォームを設定しようとしたので、警告メッセージが表示されています。

```
Router# show crypto ipsec transform-set
Transform set transform-1:{esp-256-aes esp-md5-hmac}
   will negotiate = {Tunnel, },

WARNING:encryption hardware does not support transform
esp-aes 256 within IPSec transform transform-1
```

IKE の設定に関する情報を表示するには、**show crypto isakmp policy** EXEC コマンドを使用します。

（注）　ハードウェアがサポートしていない IKE 暗号化方式を入力すると、**show crypto isakmp policy** の出力に警告メッセージが表示されます。

次に示す **show crypto isakmp policy** コマンドの出力例では、ハードウェアがサポートしていない IKE 暗号化方式を設定しようとしたので、警告メッセージが表示されています。

```
Router# show crypto isakmp policy

Protection suite of priority 1
        encryption algorithm:  AES - Advanced Encryption Standard (256 bit keys).
WARNING:encryption hardware does not support the configured
encryption method for ISAKMP policy 1
        hash algorithm:        Secure Hash Standard
        authentication method: Pre-Shared Key
        Diffie-Hellman group:  #1 (768 bit)
        lifetime:3600 seconds, no volume limit
```

設定の確認

設定変更によっては、その後、SA のネゴシエーションが行われて初めて有効になります。新しい設定値がただちに有効になるようにするには、既存の SA を消去します。

IPSec SA を消去（再初期化）するには、グローバル コンフィギュレーション モードで表 4-2 のいずれかのコマンドを使用します。

表 4-2　IPSec SA を消去するコマンド

コマンド	目的
clear crypto sa または **clear crypto sa peer** {*ip-address* | *peer-name*} または **clear crypto sa map** *map-name* または **clear crypto sa spi** *destination-address protocol spi*	IPSec SA を消去します。 パラメータを指定せずに **clear crypto sa** コマンドを実行すると、SA データベースの全内容が消去されるので、アクティブなセキュリティ セッションも消去されます。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 **spi** キーワードを指定します。

設定を確認する手順は、次のとおりです。

ステップ 1　**show crypto ipsec transform-set** コマンドを入力し、トランスフォーム セットの設定を表示します。

```
Router# show crypto ipsec transform-set
Transform set combined-des-md5: {esp-des esp-md5-hmac}
   will negotiate = {Tunnel,},
Transform set t1: {esp-des esp-md5-hmac}
   will negotiate = {Tunnel,},
Transform set t100: {ah-sha-hmac}
   will negotiate = {Transport,},
Transform set t2: {ah-sha-hmac}
   will negotiate = {Tunnel,},
   {esp-des}
   will negotiate = {Tunnel,},
```

ステップ 2　**show crypto map** [**interface** *interface* | **tag** *map-name*] コマンドを入力し、クリプト マップの設定を表示します。

```
Router# show crypto map
Crypto Map: "router-alice" idb: Ethernet0 local address: 172.21.114.123
Crypto Map "router-alice" 10 ipsec-isakmp
        Peer = 172.21.114.67
        Extended IP access list 141
            access-list 141 permit ip
                source: addr = 172.21.114.123/0.0.0.0
                dest:   addr = 172.21.114.67/0.0.0.0
        Current peer: 172.21.114.67
        Security-association lifetime: 4608000 kilobytes/120 seconds
        PFS (Y/N): N
        Transform sets={t1,}
```

ステップ 3　**show crypto ipsec sa** [**map** map-name | **address** | **identity** | **detail** | **interface**] コマンドを入力し、IPSec SA 情報を表示します。

```
Router# show crypto ipsec sa
interface: Ethernet0
    Crypto map tag: router-alice, local addr. 172.21.114.123
   local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
    current_peer: 172.21.114.67
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
    #send errors 10, #recv errors 0
     local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
     path mtu 1500, media mtu 1500
     current outbound spi: 20890A6F
     inbound esp sas:
      spi: 0x257A1039(628756537)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 26, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     outbound esp sas:
      spi: 0x20890A6F(545852015)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 27, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
interface: Tunnel0
   Crypto map tag: router-alice, local addr. 172.21.114.123
   local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
   current_peer: 172.21.114.67
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
    #send errors 10, #recv errors 0
     local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
     path mtu 1500, media mtu 1500
     current outbound spi: 20890A6F
     inbound esp sas:
      spi: 0x257A1039(628756537)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 26, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     outbound esp sas:
      spi: 0x20890A6F(545852015)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 27, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
```

show コマンドによって表示される情報の詳細については、『*Security Command Reference*』の「IP Security and Encryption」を参照してください。

設定例

ここでは、次の設定例を紹介します。

IKE ポリシーの設定例

次の例では、2 つの IKE ポリシーを作成し、ポリシー 15 に最高のプライオリティ、ポリシー 20 にその次に高いプライオリティを与え、既存のデフォルト プライオリティを最下位のプライオリティにします。さらに、IP アドレス 192.168.224.33 のリモート ピアに対して、ポリシー 20 で使用する事前共有鍵を作成します。

```
crypto isakmp policy 15
 encryption 3des
 hash md5
 authentication rsa-sig
 group 2
 lifetime 5000
crypto isakmp policy 20
 authentication pre-share
 lifetime 10000
crypto isakmp key 1234567890 address 192.168.224.33
```

IPSec の設定例

次に、IKE によって SA が確立される、最小限の IPSec の設定例を示します。

IPSec アクセス リストで、保護するトラフィックを定義します。

```
access-list 101 permit ip 10.0.0.0 0.0.0.255 10.2.2.0 0.0.0.255
```

トランスフォーム セットで、トラフィックの保護方法を定義します。この例では、トランスフォーム セット [myset1] で DES 暗号化および SHA を使用して、データ パケットを認証します。

```
crypto ipsec transform-set myset1 esp-des esp-sha
```

次のトランスフォーム セットの例 [myset2] では、3DES 暗号化および MD5（HMAC バリアント）を使用して、データ パケットを認証します。

```
crypto ipsec transform-set myset2 esp-3des esp-md5-hmac
```

クリプト マップは IPSec アクセス リストとトランスフォーム セットを結合し、保護するトラフィックの送信先（リモート IPSec ピア）を指定します。

```
crypto map toRemoteSite 10 ipsec-isakmp
 match address 101
 set transform-set myset2
 set peer 10.2.2.5
```

クリプト マップをインターフェイスに適用します。

```
interface Serial0
 ip address 10.0.0.2
 crypto map toRemoteSite
```

（注）　この例では、IKE をイネーブルにする必要があります。

圧縮の設定例

次に、圧縮を設定する簡単な例を示します。

IKE ポリシーの設定：

```
crypto isakmp policy 1
hash md5
authentication pre-share
group 2
```

IKE 事前共有鍵の設定：

```
crypto isakmp key 12abcjhrweit345 address 16.0.0.2
```

IPSec トランスフォーム セットの設定：

```
crypto ipsec transform-set proposal_01 esp-3des esp-md5-hmac comp-lzs
```

アクセス リストの設定：

```
access-list 101 permit ip host 16.0.0.1 host 16.0.0.2
```

クリプト マップの設定：

```
crypto map MAXCASE 10 ipsec-isakmp
set peer 16.0.0.2
set transform-set proposal_01
match address 101
```

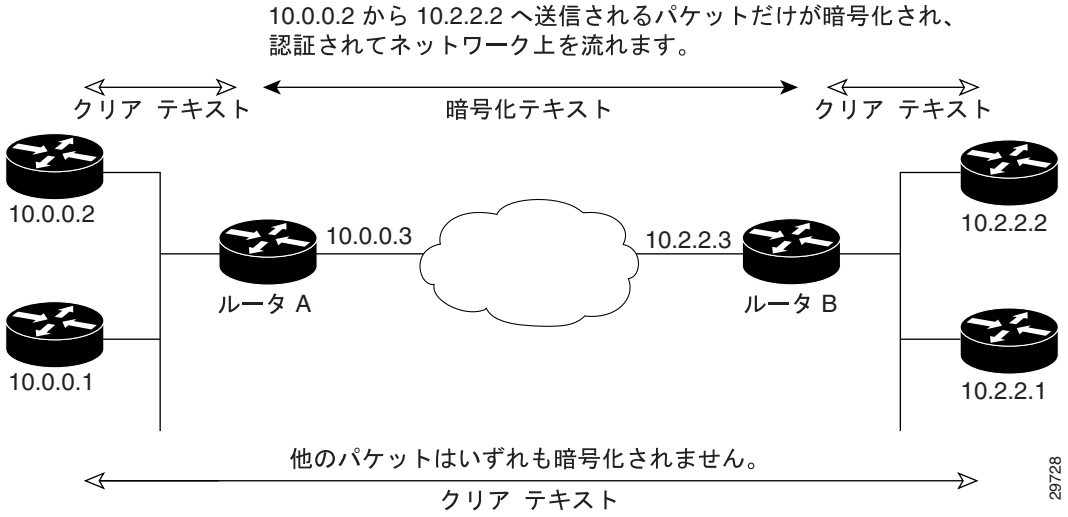
クリプト マップのインターフェイスへの適用：

```
interface FastEthernet1/0
crypto map MAXCASE
```

IPSec の基本的な設定例

次に、IKE によって SA が確立される、IPSec の設定例を示します。この例では、アクセス リストを使用して、暗号化 / 復号化するパケットを制限します。この例では、IP アドレス 10.0.0.2 から IP アドレス 10.2.2.2 へのすべてのパケットが暗号化 / 復号化され、さらに IP アドレス 10.2.2.2 から IP アドレス 10.0.0.2 へのすべてのパケットが暗号化/復号化されます。IKE ポリシーも 1 つ作成します。

図 4-1　IPSec の基本設定



ルータ A の設定

IKE ネゴシエーションで使用するパラメータを指定します。

```
crypto isakmp policy 15
  encryption des
  hash md5
  authentication pre-share
  group 2
  lifetime 5000

crypto isakmp key 1234567890 address 10.2.2.3
crypto isakmp identity address
```

（注）　上記の例では、ポリシー 15 の暗号化 DES は、書き込まれるコンフィギュレーションに含まれません。暗号化アルゴリズム パラメータのデフォルト値だからです。

トランスフォーム セットで、トラフィックの保護方法を定義します。

```
crypto ipsec transform-set auth1 ah-md5-hmac esp-des esp-md5-hmac
  mode tunnel
```

クリプト マップはトランスフォーム セットと結合し、保護するトラフィックの送信先（リモート IPSec ピア）を指定します。

```
crypto map toRemoteSite 10 ipsec-isakmp
set peer 10.2.2.3
set transform-set auth1
```

クリプト マップをインターフェイスに適用します。

```
  interface Serial0
  ip address 10.0.0.3
crypto map toRemoteSite
```

IPSec アクセス リストで、保護するトラフィックを定義します。

```
access-list 101 permit ip host 10.0.0.2 host 10.2.2.2
access-list 101 permit ip host 10.0.0.3 host 10.2.2.3
```

ルータ B の設定

IKE ネゴシエーションで使用するパラメータを指定します。

```
crypto isakmp policy 15
  encryption des
  hash md5
  authentication pre-share
  group 2
  lifetime 5000

crypto isakmp key 1234567890 address 10.0.0.3
crypto isakmp identity address
```

トランスフォーム セットで、トラフィックの保護方法を定義します。

```
crypto ipsec transform-set auth1 ah-md5-hmac esp-des ah-md5-hmac
  mode tunnel
```

クリプト マップはトランスフォーム セットと結合し、保護するトラフィックの送信先（リモート IPSec ピア）を指定します。

```
crypto map toRemoteSite 10 ipsec-isakmp
  set peer 10.0.0.3
  set transform-set auth1
```

クリプト マップをインターフェイスに適用します。

```
interface Serial0
  ip address 10.2.2.3
  crypto map toRemoteSite
```

IPSec アクセス リストで、保護するトラフィックを定義します。

```
access-list 101 permit ip host 10.2.2.2 host 10.0.0.2
access-list 101 permit ip host 10.2.2.3 host 10.0.0.3
```

トラブルシューティングのヒント

Cisco IOS ソフトウェアが SA-VAM2 を認識しているかどうかを確認するには、**show diag** コマンドを入力し、出力を調べます。たとえば、ルータのスロット 1 に SA-VAM2 が搭載されている場合、次のような出力が得られます。

```
Router# show diag
Slot 6:
        VAM2 Encryption/Compression engine, Port adapter
        Port adapter is analyzed
        Port adapter insertion time 00:01:32 ago
        EEPROM contents at hardware discovery:
        Hardware Revision        :1.0
        PCB Serial Number        :
        Part Number              :73-8491-00
        Board Revision           :
        RMA Test History         :00
        RMA Number               :0-0-0-0
        RMA History              :00
        Deviation Number         :0-0
        Product Number           :SA-VAM2
        Top Assy. Part Number    :800-22836-00
        CLEI Code                :
        EEPROM format version 4
        EEPROM contents (hex):
          0x00:04 FF 40 03 E4 41 01 00 C1 8B 00 00 00 00 00 00
          0x10:00 00 00 00 00 82 49 21 2B 00 42 00 00 03 00 81
          0x20:00 00 00 00 04 00 80 00 00 00 00 CB 94 53 41 2D
          0x30:56 41 4D 32 20 20 20 20 20 20 20 20 20 20 20 20
          0x40:20 C0 46 03 20 00 59 34 00 C6 8A 00 00 00 00 00
          0x50:00 00 00 00 00 FF FF FF FF FF FF FF FF FF FF FF
          0x60:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

SA-VAM2 が現在、暗号化パケットを処理しているかどうかを確認するには、**show pas vam interface** コマンドを入力します。次に、出力例を示します。

```
Router# show pas vam interface
VPN Acceleration Module Version II in slot : 3
        Statistics for Hardware VPN Module since the last clear
         of counters 314 seconds ago
               5290894 packets in                    5290895 packets out
            1882478960 bytes in                   1327439698 bytes out
                 16850 paks/sec in                     16850 paks/sec out
                 47940 Kbits/sec in                    33805 Kbits/sec out
               4222173 pkts compressed                     0 pkts not compressed
            1190662374 bytes before compress        405331872 bytes after compress
                 2.9:1 compression ratio               2.9:1 overall
                    58 commands out                       58 commands acknowledged
               Last 5 minutes:
               4855704 packets in                    4855705 packets out
                 16185 paks/sec in                     16185 paks/sec out
              46723079 bits/sec in                  32921855 bits/sec out

Errors:
           ppq full errors         :        0   ppq rx errors           :        0
           cmdq full errors        :        0   cmdq rx errors          :        0
           no buffer               :        0   replay errors           :        0
           dest overflow           :        0   authentication errors   :        0
           Other error             :        0   RNG self test fail      :        0
           DF Bit set              :        0   Hash Miscompare         :        0
    Unwrappable object      :        0   Missing attribute       :        0
           Invalid attrribute value:        0   Bad Attribute           :        0
           Verification Fail       :        0   Decrypt Failure         :        0
           Invalid Packet          :        0   Invalid Key             :        0
           Input Overrun           :        0   Input Underrun          :        0
           Output buffer overrun   :        0   Bad handle value        :        0
           Invalid parameter       :        0   Bad function code       :        0
           Out of handles          :        0   Access denied           :        0

        Warnings:
           sessions_expired        :        0   packets_fragmented      :        0
           general                 :        0   compress_bypassed       :        4

        HSP details:
           hsp_operations          :       75   hsp_sessions            :        6
```

SA-VAM2 がパケットを処理すると、[packets in] および [packets out] カウンタが変化します。[packets out] カウンタは、SA-VAM2 に送信されたパケット数を示します。[packets in] カウンタは、SA-VAM2 から受信したパケット数を示します。

（注）　**show pas vam interface** コマンドの出力には [compression ratio] が含まれますが、これは圧縮されたパケットと IPSec ヘッダーに対する元のパケットの比率（すなわちトンネル帯域幅の効率性）を示しています。これは圧縮された IPSec ペイロードと圧縮前の IPSec ペイロードとの比率を示しているわけではありません。

この比率は、パケットが小さく圧縮できない場合には 1 まで低下し、暗号化されたパケットと IPSec ヘッダーを加えたものに対する、暗号化されていないパケットの比率になります。

IKE/IPSec パケットが SA-VAM2 に転送されて IKE ネゴシエーションおよび IPSec 暗号化 / 復号化が行われているかどうかを調べるには、**show crypto eli** コマンドを入力します。次に、Cisco IOS ソフトウェアが SA-VAM2 にパケットを転送している場合の出力例を示します。

```
Router# show crypto eli
Hardware Encryption Layer :  ACTIVE
 Number of crypto engines = 1 .

 CryptoEngine-0 (slot-5) details.
 Capability-IPSec :IPPCP, 3DES, AES, RSA

 IKE-Session   :    0 active,  5120 max, 0 failed
 DH-Key        :    0 active,  5120 max, 0 failed
 IPSec-Session :    0 active, 10230 max, 0 failed
```

ソフトウェア暗号化エンジンがアクティブな場合、**show crypto eli** コマンドを入力しても出力は得られません。

起動時または OIR 時に、Cisco IOS ソフトウェアが SA-VAM2 に暗号トラフィックを転送することで合意した場合、次のようなメッセージが出力されます。

```
%ISA-6-INFO:Recognised crypto engine (0) at slot-1
    ...switching to hardware crypto engine
```

SA-VAM2 をディセーブルにするには、次のように、コンフィギュレーション モードで **no crypto engine accelerator** <*slot*> コマンドを使用します。

```
Router(config)# no crypto engine accelerator <slot>
    Router#
    3w4d:%ISA-6-SHUTDOWN:VAM2 shutting down
    3w4d:%ISA-6-INFO:Crypto Engine 0 in slot 1 going DOWN
    3w4d:...switching to software crypto engine
```

SA-VAM2 のモニタおよびメンテナンス

SA-VAM2 のモニタおよびメンテナンスには、次のコマンドを使用します。

コマンド	目的
Router# **show pas isa interface**	ISA インターフェイスの設定を表示します。
Router# **show pas isa controller**	ISA コントローラの設定を表示します。
Router# **show pas vam interface**	SA-VAM2 が現在暗号パケットを処理しているかどうかを確認します。
Router# **show pas vam controller**	SA-VAM2 コントローラの設定を表示します。
Router# **Show version**	インターフェイスの一部として統合サービス アダプタを表示します。