VAM の設定

この章では、Cisco 7100 シリーズ ルータ、Cisco 7200 シリーズ ルータ、および Cisco 7401ASR ルータに搭載した VPN Acceleration Module（VAM）を設定するための情報および手順について説明します。具体的な内容は、次のとおりです。

概要

VAM は Cisco 7100 シリーズ ルータ、Cisco 7200 シリーズ ルータ、および Cisco 7401ASR ルータのあらゆるインターフェイスに暗号化サービスを提供します。IPSec が設定済みのルータに VAM を搭載すると、VAM は暗号化サービスを自動的に実行します。

（注） VAM に設定すべき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、IKE、および CA の設定に関する詳細は、『*Security Configuration Guide*』の「IP Security and Encryption」および『*Security Command Reference*』の適切な IOS Release バージョンを参照してください。

設定作業

起動時に ENABLED LED が点灯した場合、VAM は全面的に動作状態であり、コンフィギュレーション コマンドは不要です。ただし、VAM に暗号化サービスを提供させる場合は、ここで説明する手順が必要です。

- EXEC コマンド インタープリタの使用方法（p.4-2）（必須）
- IKE の設定（p.4-3）（必須）
- IPSec の設定（p.4-6）（必須）

（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　マニュアルの『*Configuring the VPN Acceleration Module*』を参照してください。

任意で、Certification Authority（CA; 認証局）相互運用性を設定できます（『*Security Configuration Guide*』の「Configuring Certification Authority Interoperability」の章を参照）。

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。

特権レベルのシステム 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、次の手順で特権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、特権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。パスワードは大文字 / 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、特権レベルのシステム プロンプト（#）が表示されます。

```
Router#
```

EXEC コマンド インタープリタの特権レベルを開始する手順は、これで完了です。

IKE の設定

IKE を設定するには、次の作業を実行します。

パラメータ値を指定しないと、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」の章を参照してください。

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 モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`crypto isakmp policy` *priority*	作成するポリシーを指定し、config-isakmp コマンド モードを開始します。
ステップ 2	`encryption {des | 3des}`	暗号化アルゴリズムを指定します。
ステップ 3	`group {1 | 2}`	Diffie-Hellman グループ アイデンティティを指定します。

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」の章を参照してください。

RSA 認証方式の指定

IKE ポリシーを設定する場合、次の RSA 認証方式のいずれかを指定します。

- *RSA シグニチャ方式* — ピアを設定して、認証局（CA）から証明書を取得できます（注：最初に、ご使用の Cisco IOS リリースの『*Cisco IOS Security Configuration Guide*』の「Configuring Certification Authority Interoperability」の章で説明されているように、証明書を発行するように CA を設定します）。

  ピアは証明書を使用して公開鍵を安全に交換します。各ピアにはリモート ピアの公開シグニチャ鍵があります。両方のピアに有効な証明書がある場合、2 つのピアは自動的に RSA シグニチャが使用される IKE ネゴシエーションの一部として公開鍵を交換します。

  手動で公開鍵を交換することもできます（「手動での RSA 鍵の設定」[p.4-4] を参照）。

- *RSA 暗号化ナンス方式* — 各ピアに、他のピアの公開鍵が付与されます。RSA シグニチャと違い、RSA 暗号化ナンス方式では公開鍵の交換に証明書を使用せず、次のいずれかの方式を使用します。
  - 手動で RSA 鍵を設定する（「手動での RSA 鍵の設定」[p.4-4] 参照）。
  - RSA シグニチャと証明書を使用して、すでにピア間で IKE を交換済みであることを確認する（証明書を使用すると、RSA シグニチャベースの IKE ネゴシエーション時にピア公開鍵は交換される）。

    2 つのポリシーを指定します。RSA 暗号化ナンスを使用した高プライオリティ ポリシーと、RSA シグニチャを使用した低プライオリティ ポリシーです。ピアが相互の公開鍵を取得していないため、RSA シグニチャが最初に使用されます。公開鍵が交換されるため、以降の IKE ネゴシエーションでは RSA 暗号化ナンスを使用します。

（注） この方法では、CA サポートを設定しておく必要があります。

（注） Cisco IOS Release 12.3(10) から、VAM カードの RSA 暗号化ナンス機能がイネーブルになりました。

- *事前共有鍵認証方式*— 「事前公開鍵の設定」（p.4-6）で説明されているように、事前共有鍵を設定できます。

  RSA 暗号化を設定して、シグニチャ モードがネゴシエーションされる（かつ、証明書がシグニチャ モードで使用される）と、ピアはシグニチャ鍵と暗号鍵を要求します。ルータは、設定のサポートと同数の鍵を要求します。RSA 暗号化が設定されていない場合、ルータはシグニチャ鍵のみを要求します。

手動での RSA 鍵の設定

RSA 暗号化ナンス認証方式を指定して、CA を使用しない場合は、手動で RSA 鍵を設定します。手動で設定するには、IKE ポリシーで RSA 暗号化ナンスを使用する IPSec ピアごとに、次の作業を実行します。

- RSA 鍵の生成（p.4-4）
- ISAKMP アイデンティティの設定（p.4-4）
- 他のピアの RSA 公開鍵の指定（p.4-5）

RSA 鍵の生成

RSA 鍵を生成するには、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)# crypto key generate rsa [usage-keys]`	RSA 鍵を生成します。
ステップ 2	`Router# show crypto key mypubkey rsa`	生成された RSA 公開鍵を表示します（EXEC モード）。

IKE ポリシーで RSA 暗号化ナンスを使用する、（CA によるサポートは受けない）ピアごとに上記の作業を繰り返します。

ISAKMP アイデンティティの設定

ここでは、IKE ポリシーで事前共有鍵を使用するピアごとに ISAKMP アイデンティティを設定する方法について説明します。

2 つのピアが IKE ポリシーを使用して IPSec Security Association（SA; セキュリティ アソシエーション）を確立すると、ピアはそれぞれリモート ピアに自身の アイデンティティを送信します。ルータの ISAKMP アイデンティティ セットの取得方法によって、各ピアはホスト名または IP アドレスを送信します。

デフォルトでは、ピアの ISAKMP アイデンティティはピアの IP アドレスです。適切な場合、アイデンティティをピアのホスト名に変更できます。一般的に、すべてのピアで IP アドレスを使用するか、すべてのピアでホスト名を使用するか、アイデンティティを同じものに揃えます。一部のピアではアイデンティティにホスト名を使い、別のピアでは IP アドレスを使うと、リモート ピアのアイデンティティが認識されず、DNS ルックアップでアイデンティティの解決ができない場合、IKE ネゴシエーションは失敗します。

ピアの ISAKMP アイデンティティを設定するには、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 identity {address | hostname}`	**ローカル ピア**：IP アドレスまたはホスト名で、ピアの ISAKMP アイデンティティを指定します。[1]
ステップ 2	`Router (config)# ip host hostname address1 [address2...address8]`	**リモート ピア**：ホスト名を使用してローカル ピアの ISAKMP アイデンティティを指定すると、ピアのホスト名がすべてのリモート ピアで IP アドレスにマッピングされます（ホスト名またはアドレスが DNS サーバにマッピング済みの場合、この手順は不要）。

1. IP アドレスまたはホスト名をいつ使用するかについては、**crypto isakmp identity** コマンドの説明を参照してください。

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。

他のピアの RSA 公開鍵の指定

グローバル コンフィギュレーション モードから始まる次のコマンドを使用して、各ピアで、他のピアの RSA 公開鍵を指定します。

	コマンド	目的
ステップ 1	`Router (config)# crypto key pubkey-chain rsa`	公開鍵チェーン 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-pubkey-c)# named-key key-name [encryption | signature]`
	または
	`Router (config-pubkey-c)# addressed-key key-address [encryption | signature]`
		指定するリモート ピアの RSA 公開鍵を示します。公開鍵コンフィギュレーション モードを開始します。
		リモート ピアが ISAKMP アイデンティティとしてホスト名を使用する場合、**named-key** コマンドを使用して、リモート ピアの完全修飾ドメイン名（例：somerouter.example.com）を key-name として指定します。
		リモート ピアが ISAKMP アイデンティティとして IP アドレスを使用する場合、**addressed-key** コマンドを使用して、リモート ピアの IP アドレスを key-address として指定します。

ステップ 3	`Router (config-pubkey-k)# address ip-address`	ステップ 2 で（**named-key** コマンドを使用して）、リモート ピア名を指定するのに完全修飾ドメイン名を使用した場合は、任意でリモート ピアの IP アドレスを指定できます。
ステップ 4	`Router (config-pubkey-k)# key-string key-string`	リモート ピアの RSA 公開鍵を指定します。これが、ルータの RSA 鍵を生成したときにリモート ピア管理者から見える鍵です。
ステップ 5	`Router (config-pubkey-k)# quit`	公開鍵チェーン コンフィギュレーション モードに戻ります。
ステップ 6	—	IKE ポリシーで RSA 暗号化ナンスを使用する他の IPSec ピアすべての RSA 公開鍵を指定するには、ステップ 2 ～ 4 を繰り返します。
ステップ 7	`Router (config-pubkey-c)# exit`	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 ポリシーで RSA 暗号化ナンスを使用するピアごとに、上記の作業を繰り返します。

設定中または設定後に RSA 公開鍵を表示するには、EXEC 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# show crypto key pubkey-chain rsa {name key-name | address key-address}`	ルータ内に保存された RSA 公開鍵の一覧または特定の RSA 公開鍵の詳細を表示します。

事前公開鍵の設定

事前共有鍵を設定するには、IKE ポリシーで事前共有鍵を使用するピアごとに次の作業を実行します。

- 最初に、各ピアの ISAKMP アイデンティティを設定します。各ピアのアイデンティティは、ホスト名または IP アドレスで設定される必要があります。デフォルトでは、ピアのアイデンティティは IP アドレスに設定されます。ISAKMP アイデンティティの設定については、「ISAKMP アイデンティティの設定」を参照してください。
- 次に、各ピアで事前共有鍵を指定します。特定の事前共有鍵は、ピア間で共有されることに注意してください。特定のピアでは同じ鍵を指定して複数のリモート ピアと共有できますが、異なるピアのペア間では異なる鍵を指定して共有する方がより安全です。

ピア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 ISAKMP アイデンティティにアドレスを指定した場合は、このステップでは **address** キーワードを使用し、ホスト名を指定した場合は **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。ローカル ピアで指定したのと同じ鍵を指定します。
		
		ローカル ピアが ISAKMP アイデンティティにアドレスを指定した場合は、このステップでは **address** キーワードを使用し、ホスト名を指定した場合は **hostname** キーワードを使用します。

ステップ 3	—	各リモート ピアでステップ 1 ～ 2 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、上記の手順を繰り返します。

IPSec の設定

IKE の設定を完了してから、関係する IPSec ピアごとに IPSec を設定します。ここでは、IPSec の基本的な設定手順について説明します。また、作業については次のとおりです。

- クリプト アクセス リストの作成（p.4-7）（必須）
- トランスフォーム セットの定義（p.4-7）（必須）
- 設定の確認（p.4-9）（任意）

IPSec の設定の詳細については、『*Security Configuration Guide*』の「Configuring IPSec Network Security」の章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。

（注）　IKE は、UDP ポート 500 を使用します。IPSec の Encapsulating Security Protocol（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 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、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。

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。

ステップ	コマンド	目的
ステップ 1	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**] または **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禁止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」の章を参照してください。

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コンビネーションです。IPSec セキュリティ アソシエーションのネゴシエーション時に、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で合意します。

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 モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	**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。 （注）　複合的なルールで、トランスフォームの引数として使用できるエントリを定義します。これらのルールについては **crypto ipsec transform-set** コマンドの解説を参照してください。表 4-1 に、使用できるトランスフォーム コンビネーションを示します。
ステップ 2	**mode** [**tunnel** | **transport**]	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 モード専用です）。
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 Security Association（SA; セキュリティ アソシエーション）を解消し、その後確立された 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、使用できるトランスフォーム コンビネーションを示します。

表 4-1　使用できるトランスフォーム コンビネーション

AH トランスフォーム[1]		ESP 暗号化トランスフォーム[1]		ESP 認証トランスフォーム[2]	
トランスフォーム	説明	トランスフォーム	説明	トランスフォーム	説明
ah-md5-hmac	MD5（HMAC 系）認証アルゴリズムを使用する AH	**esp-3des**	168 ビットのトリプル DES 暗号化アルゴリズムを使用する ESP	**esp-md5-hmac**	MD5（HMAC 系）認証アルゴリズムを使用する ESP
ah-sha-hmac	SHA（HMAC 系）認証アルゴリズムを使用する AH	**esp-des**	56 ビットの DES 暗号化アルゴリズムを使用する ESP	**esp-sha-hmac**	SHA（HMAC 系）認証アルゴリズムを使用する ESP
		esp-null	暗号を使用しない ESP トランスフォーム		

1. トランスフォーム オプションを 1 つ選択します。
2. esp-null または ESP 暗号化トランスフォームを選択した場合に限り、トランスフォーム オプションを 1 つ選択します。

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、グローバル コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	**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	**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、どのトラフィックを IPSec で保護し、どれを保護しないのかを特定します。
ステップ 3	**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、同じ処理を繰り返します。
ステップ 4	**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	end	クリプトマップ コンフィギュレーション モードを終了します。
ステップ 6	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。	

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 のコマンドのいずれか 1 つを使用します。

表 4-2　IPSec セキュリティ アソシエーション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」の章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、3 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。また、IP アドレス 192.168.224.33 のリモート ピアで、ポリシー 20 で使用される事前共有鍵を生成し、ポリシー 30 で使用される RSA 暗号化鍵を生成します。

```
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
crypto isakmp policy 30
 encr 3des
 authentication rsa-encr
crypto key pubkey-chain rsa
 addressed-key 11.0.0.2
  address 11.0.0.2
  key-string
   305C300D 06092A86 4886F70D 01010105 00034B00 30480241 009E227B F7F489E2
   E980D39F 4A981644 C8A103F4 3CB1EFB1 CE8EDCC5 8E7BFDFC 6C4BCB3D 62BE76F3
   5E5F7F43 F0841163 D234138C 09725BA6 B30F50C5 63615E0B 45020301 0001
  quit
```

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、トリプル DES 暗号化および MD5（HMAC 系）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。

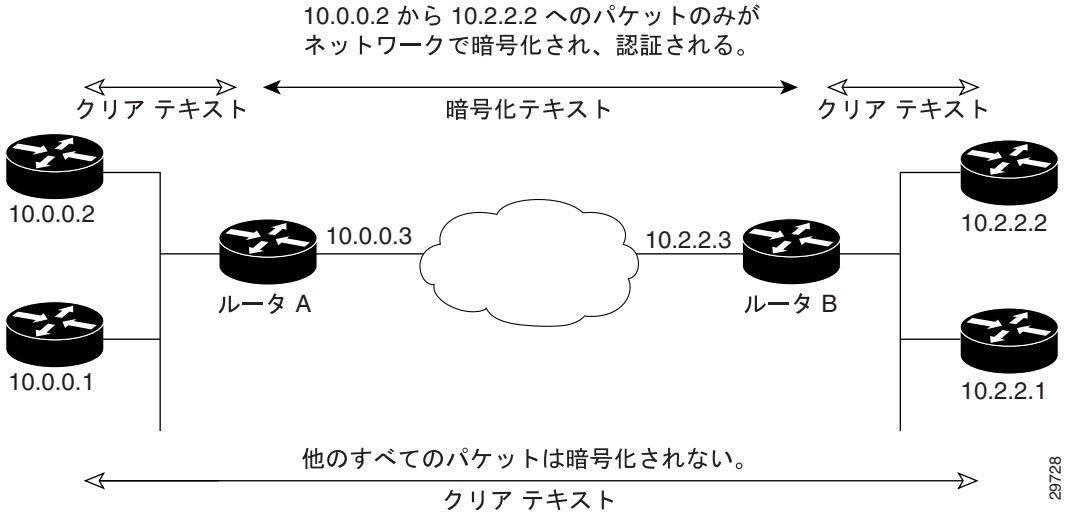
```
interface Serial0
 ip address 10.0.0.2
 crypto map toRemoteSite
```

（注）　この例では、IKE をイネーブルにする必要があります。

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 10.2.2.2 へのすべてのパケット、および IP アドレス 10.2.2.2 から 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 セットによって、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 セットによって、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 VAM 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 VAM 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 1

    Slot 1:
            VAM Encryption/Compression engine. Port adapter
            Port adapter is analyzed
            Port adapter insertion time 00:04:45 ago
            EEPROM contents at hardware discovery:
            Hardware Revision        :1.0
            PCB Serial Number        :15485660
            Part Number              :73-5953-04
            Board Revision           :
            RMA Test History         :00
            RMA Number               :0-0-0-0
            RMA History              :00
            Deviation Number         :0-0
            Product Number           :CLEO
            Top Assy. Part Number    :800-10496-04
            CLEI Code                :
            EEPROM format version 4
            EEPROM contents (hex):
              0x00:04 FF 40 02 8A 41 01 00 C1 8B 31 35 34 38 35 36
              0x10:36 30 00 00 00 82 49 17 41 04 42 FF FF 03 00 81
              0x20:00 00 00 00 04 00 80 00 00 00 00 CB 94 43 4C 45
              0x30:4F 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
              0x40:20 C0 46 03 20 00 29 00 04 C6 8A FF FF FF FF FF
              0x50:FF FF FF FF FF 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
```

VAM が現在、暗号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

    Interface VAM 1/1 :
            ds:0x632770C8        idb:0x62813728
            Statistics of packets and bytes that through this interface:
                    18 packets in                    18 packets out
                  2268 bytes in                    2268 bytes out
                     0 paks/sec in                    0 paks/sec out
                     0 Kbits/sec in                   0 Kbits/sec out
                    83 commands out                  83 commands acknowledged
            ppq_full_err   :0            ppq_rx_err       :0
            cmdq_full_err  :0            cmdq_rx_err      :0
            no_buffer      :0            fallback         :0
            dst_overflow   :0            nr_overflow      :0
            sess_expired   :0            pkt_fragmented   :0
            out_of_mem     :0            access_denied   :0
            invalid_fc     :0            invalid_param    :0
            invalid_handle :0            output_overrun   :0
            input_underrun :0            input_overrun    :0
            key_invalid    :0            packet_invalid   :0
            decrypt_failed :0            verify_failed    :0
            attr_invalid   :0            attr_val_invalid :0
            attr_missing   :0            obj_not_wrap     :0
            bad_imp_hash   :0            cant_fragment    :0
            out_of_handles :0            compr_cancelled  :0
            rng_st_fail    :0            other_errors     :0
            633 seconds since last clear of counters
```

VAM がパケットを処理すると、[packets in] および [packets out] カウントが変化します。[packets out] カウンタは、VAM に送られたパケット数を示します。[packets in] カウンタは、VAM から受信したパケット数を示します。

（注）　Cisco IOS Release 12.2(5)T および Cisco IOS Release 12.1(10)E より前のバージョンでは、再起動によってトラップの設定が失われるので、再入力が必要です。

IKE/IPSec パケットが VAM 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 VAM 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
Encryption Layer:  ACTIVE
 Number of crypto engines = 1.

 CryptoEngine-0 (slot-1) details.
 Capability-IPSec :IPPCP   , 3DES, 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。

起動時または活性挿抜（Online Insertion and Removal; OIR）時に、Cisco IOS ソフトウェアが VAM に暗号トラフィックをリダイレクトすることに合意した場合、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
```

VAM 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 **crypto card shut** コマンドを使用します。

```
Router(config)# crypto card shut 1
    Router#
    3w4d:%ISA-6-SHUTDOWN:VAM shutting down
    3w4d:%ISA-6-INFO:Crypto Engine 0 in slot 1 going DOWN
    3w4d:...switching to software crypto engine
```

VAM のモニタリングおよびメンテナンス

VAM 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**	VAM 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**	VAM 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。