VSA の設定

この章では、C7200-VSA（VPN Services Adapter）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

I/O コントローラ スロットの VSA は、NPE-G2 プロセッサを搭載した Cisco 7204VXR または Cisco 7206VXR ルータの I/O コントローラ ポート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 VSA を搭載すると、VSA は暗号化サービスを自動的に実行します。

（注）　Cisco 7204VXR および 7206VXR ルータは 1 つの VSA のみをサポートします。

VSA 上で設定するための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 Certification Authority（CA; 認証局）の設定の詳細については、『*Security Configuration Guide*』の「IP Security and Encryption」の章、および『*Security Command Reference*』を参照してください。

設定作業

VSA は起動した時点で動作可能な状態であり、コンフィギュレーション コマンドは不要です。ただし、VSA 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（p.4-3）（必須）
- IKE ポリシーの設定（p.4-3）（必須）
- トランスフォーム セットの設定（p.4-5）（必須）
- IPSec の設定（p.4-9）（必須）
- VSA のディセーブル化（任意）（p.4-5）（任意）
- IKE および IPSec の設定の確認（p.4-16）（任意）
- IPSec の設定例（p.4-20）（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。次の URL にあるオンライン マニュアルで設定例およびテクニカル ノートを参照してください。
http://www.cisco.com/en/US/products/sw/secursw/ps2308/prod_configuration_examples_list.html

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」の章を参照）。

EXEC コマンド インタープリタの使用

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。

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」の章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 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 128 | 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 Data Encryption Standard（DES; データ暗号化規格）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 Advanced Encryption Standard（AES; 高度暗号化規格）を暗号化アルゴリズムとして指定します。 • **aes 128 —** 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 —** Rivest, Shamir, and Adelman（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 nonce を認証方式として指定します。 • **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; セキュリティ アソシエーション）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。
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。

	コマンド	目的
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** — 1,024 ビット DH グループを指定します。 ***5*** — 1,536 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」の章を参照してください。

VSA のディセーブル化（任意）

VSA はデフォルトでイネーブルに設定されています。

VSA 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	`no crypto engine [slot | accelerator] 0` （注）　VSA はスロット 0 にのみ搭載可能です。	VSA をディセーブルにします。
ステップ 2	`crypto engine [slot | accelerator] 0`	次にシステムをリブートする時点で、VSA がイネーブルになります。

これで、VSA をディセーブルにして、次回のシステム リブートで VSA をイネーブルにするように準備する手順は完了です。

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 モードから始めて次のコマンドを使用します。

（注） 下記ステップ 4 の **clear** コマンドは、EXEC（イネーブル）モードで実行されます（詳細については「EXEC コマンド インタープリタの使用」[p.4-3] を参照してください）。

	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	`Router# clear crypto sa`
	または
	`Router# clear crypto sa peer {ip-address | peer-name}`
	または
	`Router# clear crypto sa map map-name`
	または
	`Router# 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 **spi** キーワードを指定します。

表 4-1 に、Authentication Header（AH; 認証ヘッダー）および Encapsulating Security Protocol（ESP）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（1 つを選択）	**ah-md5-hmac**	MD5（Message Digest 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（Secure Hash Algorithm）（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 128	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 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 [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（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

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***、***esp-des***、および ***esp-sha-hmac***

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、データ認証およびアンチ リプレイ サービスを提供します。

ESP は、パケットの暗号化のほかに、任意選択でデータ認証およびアンチ リプレイ 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 データの完全性には、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ります。

（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、**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-aes*** および ***esp-sha-hmac***
- ***ah-sha-hmac***、***esp-aes***、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に置き換えられます。

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、従来のトランスフォームだけをサポートする 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
```

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」（p.4-20）を参照してください。

IPSec の設定の詳細については、『*Cisco IOS Security Configuration Guide*』の「Configuring IPSec Network Security」の章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、次のコマンドを 1 つまたは複数使用します。

（注）　下記ステップ 5 の **clear** コマンドは、EXEC（イネーブル）モードで実行されます（詳細については「EXEC コマンド インタープリタの使用」[p.4-3] を参照してください）。

	コマンド	目的
ステップ 1	`Router# enable`	イネーブル 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場合は、パスワードを入力してください。
ステップ 2	`Router# configure terminal`	グローバル コンフィギュレーション モードになります。
ステップ 3	`Router(config)# crypto ipsec security-association lifetime seconds seconds`	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します。ライフタイムをデフォルト値に戻すには、このコマンドの no 形式を使用します。 SA が期限切れになるまでの秒数を指定します。デフォルトは 3,600 秒（1 時間）です。
ステップ 4	`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。 SA が期限切れになるまでに SA を使って IPSec 間で送受信されるトラフィック量をキロバイト単位で指定します。デフォルトは 4,608,000 キロバイトです。

ステップ 5	`Router# clear crypto sa`
	
	または
	
	`Router# clear crypto sa peer {ip-address | peer-name}`
	
	または
	
	`Router# clear crypto sa map map-name`
	
	または
	
	`Router# clear crypto sa spi 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 **spi** 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する 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」の章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 を使用せずに 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、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）。
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。）

	コマンド	目的
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。
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）。

	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）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 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 | group5]`	（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。
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 エントリではアクセス 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。 このコマンドをダイナミック クリプト マップ エントリで設定することは、ほとんどありません。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。
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。

	コマンド	目的
ステップ 6	`Router(config-crypto-m)# set pfs [group1 | group2 | group5]`	（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。
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。

IPSec のモニタリングおよびメンテナンス

IPSec SA を消去（および再初期化）するには、EXEC（イネーブル）モードで次のいずれかのコマンドを使用します（詳細については「EXEC コマンド インタープリタの使用」[p.4-3] を参照）。

コマンド	目的

`Router# clear crypto sa`
 	
または
 	
`Router# clear crypto sa counters`
 	
または
 	
`Router# clear crypto sa peer {ip-address | peer-name}`
 	
または
 	
`Router# clear crypto sa map map-name`
 	
または
 	
`Router# clear crypto sa spi 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 **spi** 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。

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** コマンド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、SA のネゴシエーション後に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（および再初期化）するには、表 4-2 のいずれかのコマンドを EXEC（イネーブル）モードで使用します（詳細については「EXEC コマンド インタープリタの使用」[p.4-3] を参照）。

表 4-2　IPSec SA を消去するコマンド

コマンド	目的
clear crypto sa or **clear crypto sa peer** {*ip-address* | *peer-name*} or **clear crypto sa map** *map-name* or **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、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。

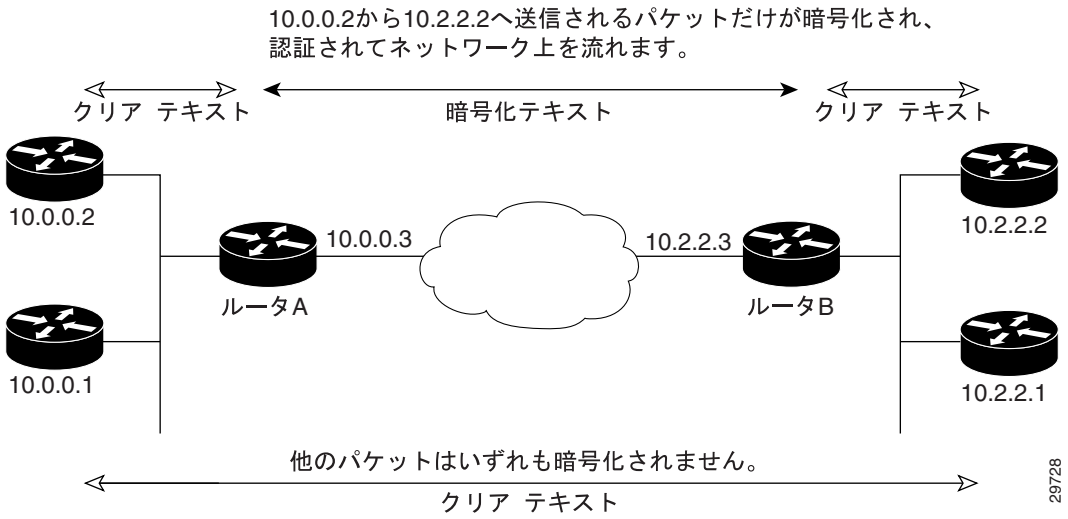
```
interface Serial0
 ip address 10.0.0.2
 crypto map toRemoteSite
```

（注）　この例では、IKE をイネーブルにする必要があります。

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
```

（注）　上記の例では、mode tunnel は書き込まれるコンフィギュレーションには含まれません。transform-set のデフォルト値だからです。

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
match address 101
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
```

（注）　上記の例では、パラメータ「mode tunnel」は書き込まれるコンフィギュレーションには含まれません。この設定のデフォルト値だからです。

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
  match address 101
  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 VSA 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。次の例では、IOS ソフトウェアはルータのスロット 0 に搭載されている C7200-VSA を認識しています。

```
Router# show diag 0
Slot 0:
        VSA IPsec Card Port adapter
        Port adapter is analyzed
        Port adapter insertion time 00:23:25 ago
        EEPROM contents at hardware discovery:
        PCB Serial Number         : PRTA4404055
        Product (FRU) Number      : C7200-VSA
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF C1 8B 50 52 54 41 34 34 30 34 30 35 35 40
          0x10: 05 0D CB 94 43 37 32 30 30 2D 56 53 41 20 20 20
          0x20: 20 20 20 20 20 20 20 20 D9 03 C1 40 CB FF FF FF
          0x30: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x40: FF FF FF FF FF FF FF FF FF FF FF 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
```

VSA 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 crypto engine accelerator statistic 0** コマンドを入力します。次に、出力例を示します。

```
Router# show crypto engine accelerator statistic 0

Device:   VSA
Location: Service Adapter: 0
 VSA Traffic Statistics

  Inbound rate: 0pps 0kb/s  Outbound rate: 0pps 0kb/s
  TXR0 PKT: 0x00000000000028B2  Byte: 0x0000000000006ACF6  Full: 0x0000000000000000
  RXR0 PKT: 0x00000000000028B2  Byte: 0x00000000000A86398
  TXR1 PKT: 0x0000000000000000  Byte: 0x0000000000000000  Full: 0x0000000000000000
  RXR1 PKT: 0x0000000000000000  Byte: 0x0000000000000000
  TXR2 PKT: 0x0000000000000000  Byte: 0x0000000000000000  Full: 0x0000000000000000
  RXR2 PKT: 0x0000000000000000  Byte: 0x0000000000000000
  Inbound Traffic:
  Decrypted  PHY I/F:0x0000000000000000  TUNNEL I/F:    0x0000000000000000
  SPI Error  PHY I/F:0x0000000000000000  TUNNEL I/F:    0x0000000000000000
  Pass clear PHY I/F:0x0000000000000000  TUNNEL I/F:    0x0000000000000000
  SPD Drop:          0x0000000000000000  IKE Bypass:    0x0000000000000000
  Outbound Traffic:
  Encry CEF: 0x0000000000000000  FS: 0x0000000000000000  PROC: 0x0000000000000000
  Pass  CEF: 0x0000000000000000  FS: 0x0000000000000000  PROC: 0x0000000000000000
  ICMP Unreachable: 0x0000000000000000  ICMP Unreach Fail: 0x0000000000000000
  SPD Drop:  0x0000000000000000
  Special Traffic:
  VAM mode  PKT:     0x0000000000000000  Exception:     0x0000000000000000
  N2 Message:    :   0x00000000000028B2  Exception:     0x0000000000000000
  IP PKT Exception:  0x0000000000000000  DJ Overflow:   0x0000000000000000
  RAE Report PKT::   0x0000000000000000  PKT Consumed:  0x0000000000000000
  TCAM WR:           0x0000000000000001  TCAM RD:       0x0000000000000000
  SARAM WR:          0x0000000000008422  SARAM RD:      0x0000000000000000
  RAE WR:            0x0000000000080000  RAE RD:        0x0000000000000000
  Warnings:
  N2 interrupt:      0x0000000000000000  Invalid Op:    0x0000000000000000
  RX CTX error:      0x0000000000000000  TX CTX low:    0x0000000000000000
  PKT CTX Low:       0x0000000000000000  PKT Info Low:  0x0000000000000000
  PKT Header Low:    0x0000000000000000  Particle Low:  0x0000000000000000
  Missing SOP:       0x0000000000000000  Missing EOP:   0x0000000000000000
  TX Drop IB:        0x0000000000000000  TX Drop OB:    0x0000000000000000
  MSG Unknown:       0x0000000000000000  MSG too Big:   0x0000000000000000
```

```
  MSG Empty:          0x0000000000000000  MSG No Buffer: 0x0000000000000000
  PKT Info Missing:   0x0000000000000000  IB SB Error:   0x0000000000000000
  TX Drop Fastsend:   0x0000000000000000  IDMA Full:     0x0000000000000000
  Particle Fallback: 0x0000000000000000  STATISTIC:     0x0000000000000000

 Elrond statistic:
  TXDMA PKT Count:    0x00000000000028B2  Byte Count:    0x000000000006ACF6
  RXDMA PKT Count:    0x00000000000028B2  Byte Count:    0x0000000000A86398
  IPPE  PKT Count:    0x00000000000028B2  EPPE PKT Count:0x00000000000028B2
  PL3TX PKT Count:    0x00000000000028B2  Byte Count:    0x000000000009DADE
  PL3RX PKT Count:    0x00000000000028B2  Byte Count:    0x0000000000A86398
  CAM search IPPE:    0x0000000000000000  EPPE:          0x0000000000000000
  SARAM Req IPPE:     0x0000000000000000  EPPE:          0x0000000000000000
  RAE Frag Req IPPE: 0x0000000000000000  EPPE:          0x0000000000000000
  RAE ReAssembly:     0x0000000000000000  Re-Ordering:   0x0000000000000000
  REA Frag Finished: 0x0000000000000000
  Frag Drop Count:
   IPPE:              0x0000000000000000  EPPE:          0x0000000000000000
   FIFO:              0x0000000000000000  RAE:           0x0000000000000000

VSA RX Exception statistics:
   IRH Not valid           :        0   Invalid SA              :        0
   SA configuration error  :        0   Enc Dec mismatch        :        0
   Insufficient Push       :        0   Next Header mismatch    :        0
   Pad mismatch            :        0   MAC mismatch            :        0
   Atomic OP failed        :        0   L2 UDD GE 256           :        0
   Max BMI Read too small  :        0   Max BMI Read No payload :        0
   Anti replay failed      :        0   Enc Seq num overflow    :        0
   Dec IPver mismatch      :        0   Enc IPver mismatch      :        0
   TTL Decr                :        0   Selector checks         :        0
   UDP mismatch            :        0   Reserved                :        0
   Soft byte lifetime      :        0   hardbyte lifetime       :        0
   IP Parse error          :        0   Fragmentation Error     :        0
   Unknown Exception       :        0
```

VSA 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、VSA に送られたパケット数を示します。「packets in」カウンタは、VSA から受信したパケット数を示します。

IKE/IPSec パケットが VSA 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 VSA 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 : ACTIVE
 Number of hardware crypto engines = 1

 CryptoEngine VSA details: state = Active
 Capability      : DES, 3DES, AES, RSA

 IKE-Session   :     0 active,  5120 max, 0 failed
 DH            :     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。

Cisco IOS ソフトウェアが VSA に暗号トラフィックを転送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-0
    ...switching to hardware crypto engine
```

VSA 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 0
...switching to SW crypto engine
Router(config)#
*Feb  6 11:57:26.763: %VPN_HW-6-INFO_LOC: Crypto engine: slot 0  State changed to:
Disabled
*Feb  6 11:57:26.779: %PA-3-DEACTIVATED: port adapter in bay [0] powered off.
*Feb  6 11:57:26.779: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
Router(config)#end
```

VSA のモニタリングおよびメンテナンス

ここで説明する内容は次のとおりです。

アクセス リストでの拒否ポリシーの使用

アクセス リストに拒否アドレスの範囲を指定すると、「ジャンプ」動作が発生します。拒否されているアドレス範囲にヒットした時点で、クリプト マップの次のシーケンスに対応付けられたアクセス リストの先頭に「ジャンプ」し、そこから検索が続けられます。これらのアドレスにクリア トラフィックを送信するには、クリプト マップのシーケンスごとに拒否アドレスの範囲を挿入しなければなりません。アドレスの許可リストはそれぞれ、アクセス リストで指定されたすべての拒否アドレスの範囲を継承します。拒否アドレスの範囲を指定することで、ソフトウェアは許可リストから拒否アドレスの範囲を差し引き、ハードウェアにプログラムする必要のある複数の許可アドレスの範囲を作成します。この動作によって、拒否アドレスの範囲 1 つのために、ハードウェアへのアドレス範囲のプログラミングが繰り返される場合があるため、1 つのアクセス リストに複数の許可アドレスの範囲が存在する結果になります。

この問題を回避するには、**crypto ipsec ipv4 deny-policy** {jump | clear | drop} コマンドが役立ちます。clear キーワードを使用すると、拒否アドレスの範囲がハードウェアにプログラムされたあと、その拒否アドレスは暗号化 / 復号化の対象外になります。拒否アドレスにヒットすると、検索が停止し、トラフィックがクリアな（暗号化されていない）状態で通過できるようになります。drop キーワードを使用すると、拒否アドレスにヒットした時点でトラフィックが廃棄されます。これら 2 つの新しいキーワードを使用して、アドレス範囲がハードウェアに繰り返しプログラムされるのを防ぎ、スペース利用を効率化することができます。

設定時の注意事項と制約事項

- **crypto ipsec ipv4 deny-policy** {jump | clear | drop} コマンドは、VSA モジュールに適用できるグローバル コマンドです。指定したキーワード（jump、clear、または drop）は VSA モジュールの ACE ソフトウェアに伝播されます。デフォルトの動作は jump です。
- VSA モジュールにクリプト マップがすでに設定されている場合に特定のキーワード（jump、clear、または drop）を適用すると、既存の IPSec セッションがすべて一時的に削除されてから再開され、ネットワークのトラフィックに影響します。
- アクセス リストに指定できる拒否エントリの数は、指定するキーワードによって異なります。
  - jump — アクセス リストごとに最大 8 つの拒否エントリを使用できます。
  - clear — アクセス リストごとに最大 1000 個の拒否エントリを使用できます。
  - drop — アクセス リストごとに最大 1000 個の拒否エントリを使用できます。

モニタリングおよびメンテナンス用のコマンド

VSA 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 crypto engine accelerator statistic 0`	VSA 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 version`	インターフェイスの一部として組み込まれているサービス アダプタを表示します。