VPN Acceleration Module（VAM）

機能の履歴

リリース	変更点
12.1(9)E	この機能が NPE-225、NPE-400、および NSE-1 の Cisco 7200 シリーズ ルータに導入されました。
12.1(14)E	この機能は Cisco IOS Release 12.1(14)E に統合され、NPE-G1 を使用する Cisco 7200 シリーズの デュアル VAM[1] のサポートが追加されました。
12.2(9)YE	この機能のサポートが Cisco 7401ASR ルータが追加されました。[2]
12.2(13)T	この機能は、Cisco IOS Release 12.2(13)T に統合されました。
12.2(15)T	この機能は、Cisco IOS Release 12.2(15)T に統合されました。
12.3(1) 本体	この機能は、Cisco IOS Release 12.3(1) 本体に統合されました。
12.2(14)SU	この機能は、Cisco IOS Release 12.2(14)SU に統合されました。

1. デュアル VAM をサポートしているのは、Cisco IOS Release 12.2(15)T、12.1(14)E、および 12.3 本体の NPE-G1 を使用する Cisco 7200 シリーズ ルータだけです。
2. Cisco 7401ASR ルータは販売終了となっています。

この章では、VPN Acceleration Module（VAM）機能について説明します。次の項で構成されています。

機能の概要

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

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

- 56 ビット Data Encryption Standard（DES; データ暗号規格）標準モード：Cipher Block Chaining（CBC; 暗号ブロック連鎖）
- 3 キー トリプル DES（168 ビット）
- Secure Hash Algorithm（SHA）-1 および Message Digest 5（MD5; メッセージ ダイジェスト 5）
- Rivest、Shamir、Adelman（RSA）公開鍵アルゴリズム
- Diffie-Hellman 鍵交換 RC4 - 40

利点

VAM には次の利点があります。

- 毎秒 10 個のトンネル
- NPE の対応するメモリに基づいた次に示すトンネルの数
  - 64 MB の場合 800 個のトンネル
  - 128 MB の場合 1600 個のトンネル
  - 256 MB の場合 3200 個のトンネル
  - 512 MB の場合 5000 個のトンネル
- RSA 暗号化
- 暗号化のパフォーマンスの加速化
- Internet Key Exchange（IKE; インターネット キー エクスチェンジ）の加速化
- デジタル証明書を使用した自動認証のための証明書サポート
- デュアル VAM サポート

（注） デュアル VAM をサポートしているのは、Cisco IOS Release 12.2(15)T、12.1(14)E、および 12.3 本体の NPE-G1 を使用する Cisco 7200 シリーズ ルータです。

- ルータ内にインストールされたあらゆるポート アダプタに対する暗号化サービス。ポート アダプタ上のインターフェイスは、IPSec をサポートするクリプト マップを使用して設定する必要があります。
- 300 バイトのパッケージに対する各種暗号化および圧縮スキームによる 100 Mbps 超の全二重方式データ転送
- ハードウェアベースの IPPCP LZS 圧縮

- 帯域利用率を下げるネットワーク トラフィック圧縮
- Online Insertion and Removal（OIR; 活性挿抜）
- QoS、マルチプロトコル、およびマルチキャスト機能の相互運用
- IPSec VPN 上での Enhanced Interior Gateway Routing Protocol（EIGRP）、Open Shortest Path First（OSPF）、および Border Gateway Protocol（BGP; ボーダ ゲートウェイ プロトコル）など、フル レイヤ 3 ルーティングのサポート
- トリプル DES を使用した最大 145 Mbps のスループット
- VPN 初期化の改善

シングル VAM のパフォーマンス結果

次の 2 つの表に、NPE-G1 プロセッサ、オンボード GE、スロット 3 および 4 内の FE ポート アダプタが搭載された Cisco 7206VXR におけるシングル VAM のパフォーマンス結果を示します。

clear_packet _size	crypto_packet_size	out_packet_size
64	96	114
300	336	354
1400	1432	1450
混合パケット サイズ：344	378	396

pkt_size（バイト）	トンネル数	measured_pps（pps）	meas_clear_ndr（Mbps）	meas_crypto_ndr（Mbps）	meas_out_ndr（Mbps）
64	4	65,224	33.39	50.09	59.48
	500	41,888	21.44	32.17	38.20
	1,000	40,480	20.73	31.09	36.92
	5,000	39,408	20.18	30.27	35.94
300	4	38,032	91.28	102.23	107.71
	500	37,184	89.24	99.95	105.31
	1,000	36,064	86.55	96.94	102.13
	5,000	36,016	86.44	96.81	101.99
1400	4	9,984	111.82	114.38	115.81
	500	9,848	110.29	112.82	114.24
	1,000	9,648	108.06	110.53	111.92
	5,000	9,616	107.70	110.16	111.55
混合パケット サイズ	4	31,472	86.61	95.17	99.70
	500	31,056	85.47	93.91	98.39
	1,000	30,128	82.91	91.11	95.45
	5,000	29,264	80.53	88.49	92.71

デュアル VAM のパフォーマンス結果

次の 2 つの表に、NPE-G1 プロセッサ、オンボード GE、スロット 3 および 4 内の FE ポート アダプタが搭載された Cisco 7206VXR におけるデュアル VAM のパフォーマンス結果を示します。

clear_packet _size	crypto_packet_size	out_packet_size
64	96	114
300	336	354
1400	1432	1450
混合パケット サイズ：344	378	396

pkt_size（バイト）	トンネル数	measured_pps（pps）	meas_clear_ndr（Mbps）	meas_crypto_ndr（Mbps）	meas_out_ndr（Mbps）
64	4	135,544	69.40	104.10	123.61
	500	61,520	31.50	47.25	56.11
	1,000	56,928	29.15	43.72	51.92
	5,000	43,744	22.40	33.60	39.89
300	4	71,336	171.21	191.75	202.02
	500	60,416	145.00	162.40	171.10
	1,000	56,016	134.44	150.57	158.64
	5,000	42,496	101.99	114.23	120.35
1400	4	18,736	209.84	214.64	217.34
	500	18,424	206.35	211.07	213.72
	1000	18,352	205.54	210.24	212.88
	5,000	18,352	205.54	210.24	212.88
混合パケット サイズ	4	60,416	166.26	182.70	191.40
	500	57,888	159.31	175.05	183.40
	1,000	55,488	152.70	167.80	175.79
	5,000	34,272	94.32	103.64	108.57

関連機能およびテクノロジー

次の機能およびテクノジーが VAM と関連しています。

- IKE
- IP Security（IPSec; IP セキュリティ）

関連資料

次のマニュアルで VAM ハードウェアの説明をしています。

- 『VPN Acceleration Module Installation and Configuration』

サポートされているプラットフォーム

次のプラットフォームで VAM 機能がサポートされています。

- NPE-225、NPE-400、NSE-1、および NPE-G1 搭載 Cisco 7200 シリーズ ルータ
- デュアル VAM をサポートしているのは、Cisco IOS Release 12.2(15)T、12.1(14)E、および 12.3 M の NPE-G1 を使用する Cisco 7200 シリーズ ルータです。
- Cisco 7401ASR ルータ

Cisco Feature Navigator を使用したプラットフォーム サポートの特定

Cisco IOS ソフトウェアは、特定のプラットフォームがサポートされている機能セットにパッケージングされています。この機能のプラットフォーム サポートに関連した更新情報を取得するには、Cisco Feature Navigator にアクセスします。新しいプラットフォーム サポートが機能に追加されると、Cisco Feature Navigator によって、サポートされているプラットフォームのリストが自動的に更新されます。

Cisco Feature Navigator は Web ベースのツールであり、特定の機能セットがサポートされている Cisco IOS ソフトウェア イメージ、および、特定の Cisco IOS イメージ内でサポートされている機能を特定できます。機能またはリリースごとに検索できます。リリース セクションでは、各リリースを横に並べて比較し、各ソフトウェア リリースに固有の機能と共通機能の両方を表示できます。

Cisco Feature Navigator にアクセスするには、Cisco.com のアカウントが必要です。アカウント情報を忘れたり、紛失したりした場合は、空の E メールを cco-locksmith@cisco.com に送信してください。自動チェックによって、E メール アドレスが Cisco.com に登録されているかどうかが確認されます。チェックが正常に終了したら、ランダムな新しいパスワードとともにアカウントの詳細が E メールで届きます。資格のあるユーザは、http://www.cisco.com/register にある指示に従って、Cisco.com にアカウントを作成できます。

Cisco Feature Navigator は定期的に更新されています（Cisco IOS ソフトウェアの主要なリリース時およびテクノロジー リリース時）。最新情報については、次の URL から Cisco Feature Navigator ホームページにアクセスしてください。

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

Cisco IOS ソフトウェア イメージの可用性

特定の Cisco IOS ソフトウェア リリースをサポートしているプラットフォームは、そのプラットフォーム用のソフトウェア イメージがあるかどうかによります。一部のプラットフォームのソフトウェア イメージは、事前の通知なしに延期、遅延、または変更される場合があります。各 Cisco IOS ソフトウェア リリースのプラットフォーム サポートおよび利用可能なソフトウェア イメージの更新情報は、オンライン リリース ノートまたは Cisco Feature Navigator（サポートされている場合）を参照してください。

サポートされている規格、MIB、および RFC

規格

- この機能によってサポートされる新しい規格や変更された規格はありません。

MIB

この機能により、次の MIB が導入または変更されました。

- CISCO-IPSEC-FLOW-MONITOR-MIB
- CISCO-IPSEC-MIB
- CISCO-IPSEC-POLICY-MAP-MIB

選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。

http://www.cisco.com/go/mibs

RFC

- IPPCP：RFC 2393、2395
- IPSec/IKE：RFC 2401-2411、2451

前提条件

ルータ上で IPSec および IKE を設定し、VAM の暗号化サービスが必要なすべてのインターフェイスに対してクリプト マップを設定する必要があります。設定手順については、「設定例」（P.13）を参照してください。

設定作業

イネーブルド LED がオンになっている場合、電源を投入した時点で、VAM は完全に機能しており、いかなる設定コマンドも不要です。ただし、VAM によって暗号化サービスが提供されている場合は、次のタスクを完了させる必要があります。

- 「IKE ポリシーの設定」（必須）
- 「IPSec の設定」（必須）

IKE ポリシーの設定

パラメータの値を指定しない場合、デフォルト値が割り当てられます。デフォルト値については、マニュアル『*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 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。

	コマンド	目的
ステップ 2	`Router(config-isakmp)# encryption {des | 3des | aes | aes 192 | aes 256}`	IKE ポリシーの内で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 ポリシー内で認証方式を指定します。 • **rsa-sig**：Rivest、Shamir、Adelman（RSA）署名を認証方式として指定します。 • **rsa-encr**：RSA 暗号化ナンスを認証方式として指定します。 **（注）** Cisco IOS Release 12.3(10) から rsa-encr が VAM 暗号カードに使用できるようになっています。 • **pre-share**：事前共有キー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 が期限切れになる前に存在する必要がある秒数。60 ～ 86,400 秒の範囲で整数を使用して指定します。 **（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（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 ポリシー内でハッシュ 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 ポリシー内で Diffie-Hellman（DH; デフィーヘルマン）グループ ID 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 ポリシーの作成に関する詳細については『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Configuring Internet Key Exchange for IPsec VPNs」の章を参照してください。

IPSec の設定

IKE 設定が完了したら、各参加 IPSec ピアで IPSec を設定します。この項では、次の各項で説明される作業を含む、IPSec を設定するための基本手順について説明します。

- 「クリプト アクセス リストの作成」（P.8）
- 「トランスフォーム セットの定義」（P.9）

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**]	保護する IP パケットを判別する条件を指定します。[1] これらの条件に一致するトラフィックに対して暗号化をイネーブルまたはディセーブルにします。
	または **ip access-list extended** *name*	IPsec で使用できるように「ミラー イメージ」クリプト アクセス リストを設定することを推奨します。また、**any** キーワードを使用することは推奨しません。
ステップ 2	`Router(config-if)# Add permit and deny statements as appropriate.`	アクセス リストに permit または deny ステートメントを追加します。
ステップ 3	`Router(config-if)# 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. 番号または名前によって指定された IP アクセス リストを使用して、条件を指定します。**access-list** コマンドでは、番号付き拡張アクセス リストを指定し、**ip access-list extended** コマンドでは、名前付きアクセス リストを指定します。

アクセス リストの設定の詳細については、『*IP Access List Features Roadmap*』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
Router# **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、暗号化トランスフォーム コンフィギュレーション モードを開始します。
Router# **mode** [**tunnel** | **transport**]	トランスフォーム セットに関連付けられたモードを変更します。このモード設定は、送信元アドレスと宛先アドレスが IPsec ピア アドレスであるトラフィックだけに適用され、その他すべてのトラフィックに対しては無視されます（他のトラフィックはすべてトンネル モードです）。
Router# **end**	暗号化トランスフォーム モードを終了して、イネーブル モードを開始します。
Router# **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 を消去して、その後確立された SA でトランスフォーム セットへの変更が有効になるようにします。手動で確立した SA は、すぐに再確立されます。 パラメータを指定せずに **clear crypto sa** コマンドを使用すると、SA データベースの内容が完全に消去されるので、アクティブなセキュリティ セッションが消去されます。SA データベースのサブセットだけを消去するには、**peer**、**map**、または **entry** キーワードも指定します。

セキュリティ アソシエーションを確立するために IKE を使用するクリプト マップ エントリ作成するには、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
Router# **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。
Router# **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 リストによって IPSec によって保護されるトラフィックと保護されないトラフィックが決定されます。
Router# **set peer** {*hostname* | *ip-address*}	リモート IPSec ピアを指定します。このピアは、IPsec で保護されたトラフィックの転送先となるピアです。 複数のリモート ピアに対して、同じ作業を繰り返します。
Router# **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。複数のトランスフォーム セットをプライオリティの順に表示します（最もプライオリティの高いものを先頭に表示）。
Router# **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。

必要に応じてこれらの手順を繰り返し、追加のクリプト マップ エントリを作成します。

クリプト マップの設定の詳細については、マニュアル『*Security Configuration Guide*』の「Configuring IPSec Network Security」の章を参照してください。

設定の確認

次の手順では、設定の確認に関する情報を説明します。

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

```
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*] コマンドを入力して、クリプト マップ設定を表示します。

```
outer# 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**] コマンドを入力して、IPSec Enter セキュリティ アソシエーションに関する情報を表示します。

```
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:
```

トラブルシューティングのヒント

Cisco IOS ソフトウェアによって VAM が認識されていることを確認するには、**show diag** コマンドを入力して、出力をチェックします。たとえば、ルータのスロット 1 に VAM がある場合、次の出力が表示されます。

```
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 によって暗号パケットが処理中であることを確認するには、**show pas vam interface** コマンドを入力します。次にサンプル出力を示します。

```
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 によってパケットが処理されると、「packet in」および「packet out」カウンタが変化します。「packet out」カウンタは、VAM に転送されたパケットの数を表します。「packet in」カウンタは、VAM から受信したパケットの数を表します。

（注） Cisco IOS Release 12.2(5)T および Cisco IOS Release 12.1(10)E よりも前のバージョンでは、リブートトラップ設定がないので、再入力が必要です。

VPN Acceleration Module のモニタおよびメンテナンス

次のコマンドを使用して、VPN Acceleration Module をモニタおよびメンテナンスします。

コマンド	目的
Router# **show pas isa interface**	ISA インターフェイス コンフィギュレーションを表示します。
Router# **show pas isa controller**	ISA コントローラ コンフィギュレーションを表示します。
Router# **show pas vam interface**	VAM によって暗号パケットが処理中であることを確認します。
Router# **show pas vam controller**	VMA コントローラ コンフィギュレーションを表示します。
Router# **Show version**	統合サービス アダプタをインターフェイスの一部として表示します。

設定例

ここでは、次の設定例について説明します。

- 「IKE ポリシー例の設定」（P.13）
- 「IPSec 設定例の設定」（P.13）

IKE ポリシー例の設定

次の例では、2 つの IKE ポリシーが作成されます。最大のプライオリティとして policy 15、次のプライオリティとして policy 20、最小のプライオリティとして既存のデフォルト プライオリティを使用します。また、IP アドレスが 192.168.224.33 のリモート ピアに、policy 20 で使用する事前共有鍵も作成します。

```
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 設定例の設定

次に、セキュリティ アソシエーションが IKE を介して確立される最低限の IPSec 設定の例を示します。

IPSec アクセス リストによって保護対象のトラフィックが定義されます。

```
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 セットによってどのようにトラフィックを保護するかが定義されます。この例では、トランスフォーム セット「myset1」によって、データ パケット認証に DES 暗号化および SHA が使用されています。

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

もう 1 つのトランスフォーム セットである「myset2」では、データ パケットの認証にトリプル DES 暗号化および MD5（HMAC バリアント）が使用されています。

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

クリプト マップによって、IPSec アクセス リストとトランスフォーム セットが結合され、保護対象トラフィックの送信先（リモート IPSec ピア）が指定されます。

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

クリプト マップがインターフェイスに適用されます。

```
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。

コマンド リファレンス

次のコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。

- **show pas vam interface**
- **show pas vam controller**
- **crypto engine sw ipsec**

これらのコマンドの詳細については、『Cisco IOS Security Command Reference』（http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html）を参照してください。

Cisco IOS の全コマンドを参照する場合は、Command Lookup Tool（http://tools.cisco.com/Support/CLILookup）にアクセスするか、または『*Master Command List*』を参照してください。

用語集

VAM：VPN Acceleration Module。

IKE：Internet Key Exchange（IKE; インターネット キー エクスチェンジ）。IKE によって、キーが必要なサービス（IPsec など）のための共有セキュリティ ポリシーおよび認証キーが確立されます。IPsec トラフィックを通過させる前に、ルータ、ファイアウォール、ホストそれぞれでピアの ID を検証する必要があります。それには、事前共有鍵を両ホストに手動で入力するか、CA サービスを使用します。

IPsec：IP Security（IP セキュリティ）。オープン規格のフレームワークであり、関与するピア間におけるデータの機密保持、データ整合性、データ認証を実現します。IPsec では、これらのセキュリティ サービスが IP レイヤで実現されます。IPsec では、ローカル ポリシーに基づいたプロトコルやアルゴリズムのネゴシエーションの処理や、IPsec に使用される暗号鍵や認証鍵の生成が、IKE を通じて行われます。IPsec は、1 組のホスト間、1 組のセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間で 1 つ以上のデータ フローを保護するために使用できます。