# VPN Acceleration Module

**Last Updated: October 20, 2011**

This feature module describes the VPN Acceleration Module (VAM) feature

- Finding Feature Information, page 1
- Prerequisites, page 1
- Information about VPN Acceleration, page 1
- How To Configure VPN Acceleration, page 6
- Configuration Examples for VPN Acceleration, page 14
- Glossary, page 15

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Prerequisites

You must configure IPSec and IKE on the router and a crypto map to all interfaces that require encryption service from the VAM. See the Configuration Examples for VPN Acceleration, page 14 for configuration procedures.

## Information about VPN Acceleration

- Feature Information, page 2
- Feature Overview, page 2
- Benefits, page 3

**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Feature Information

### Feature History

| Release | Modification |
|---|---|
| 12.1(9)E | This feature was introduced on the Cisco 7200 series routers on NPE-225, NPE-400, and NSE-1 |
| 12.1(14)E | This feature was integrated into Cisco IOS Release 12.1(14)E and support for dual VAMs[1] on the Cisco 7200 series with NPE-G1 was added |
| 12.2(9)YE | Support for this feature was added to the Cisco 7401ASR router[2] |
| 12.2(13)T | This feature was integrated into Cisco IOS Release 12.2(13)T |
| 12.2(15)T | This feature was integrated into Cisco IOS Release 12.2(15)T |
| 12.3(1)Mainline | This feature was integrated into Cisco IOS Release 12.3(1) Mainline |
| 12.2(14)SU | This feature was integrated into Cisco IOS Release 12.2(14)SU |

# Feature Overview

The VPN Acceleration Module (VAM) is a single-width acceleration module. It provides high-performance, hardware-assisted tunneling and encryption services suitable for Virtual Private Network (VPN) remote access, site-to-site intranet, and extranet applications. It also provides platform scalability and security while working with all services necessary for successful VPN deployments -- security, quality of service (QoS), firewall and intrusion detection, service-level validation, and management. The VAM off-loads IPSec processing from the main processor, thus freeing resources on the processor engines for other tasks.

The VAM provides hardware-accelerated support for the following multiple encryption functions:

- 56-bit Data Encryption Standard (DES) standard mode: Cipher Block Chaining (CBC)
- 3-Key Triple DES (168-bit)
- Secure Hash Algorithm (SHA)-1 and Message Digest 5 (MD5)

[1] Support for dual VAMs is available on a Cisco 7200 series router with NPE-G1 on Cisco IOS Release 12.2(15)T, 12.1(14)E, and 12.3 Mainline only.

[2] The Cisco 7401ASR router is no longer sold.

- Rivest, Shamir, Adelman (RSA) public-key algorithm
- Diffie-Hellman key exchange RC4-40

The following commands are introduced or modified in the feature or features

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

# Benefits

The VAM provides the following benefits:

- 10 tunnels per second
- The following number of tunnels based on the corresponding memory of the NPE:
  - 800 tunnels for 64 MB
  - 1600 tunnels for 128 MB
  - 3200 tunnels for 256 MB
  - 5000 tunnels for 512 MB
- RSA encryption
- Accelerated Crypto performance
- Accelerated Internet Key Exchange (IKE)
- Certificate support for automatic authentication using digital certificates
- Dual VAM support

**Note** Support for dual VAMs is available on a Cisco 7200 series router with an NPE-G1, on Cisco IOS Release 12.2(15)T, 12.1(14)E, and 12.3 Mainline.

- Encryption services to any port adapter installed in the router. The interface on the port adapter must be configured with a crypto map to support IPSec.
- Full-duplex data transmission of over 100 Mbps with various encryption and compression schemes for 300 byte packages
- Hardware-based IPPCP LZS compression
- Network traffic compression that reduces bandwidth utilization
- Online Insertion and Removal (OIR)
- QoS, multiprotocol, and multicast feature interoperation
- Support for full Layer 3 routing, such as Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP) across the IPSec VPN
- Up to 145 Mbps throughput using 3DES
- VPN initialization improvements

### Performance Results for Single VAM

The following two tables provide performance results for a single VAM on a Cisco 7206VXR with an NPE-G1 processor, an onboard GE, and FE port adapters in slots 3 and 4.

| clear_packet _size | crypto_packet_size | out_packet_size |
|---|---|---|
| 64 | 96 | 114 |
| 300 | 336 | 354 |
| 1400 | 1432 | 1450 |
| Mixed packet size - 344 | 378 | 396 |

| pkt_size (bytes) | # of tunnels | 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 |
| Mixed packet size | 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 |

### Performance Results for Dual VAMs

The following two tables provide performance results for dual VAMs on a Cisco 7206VXR with an NPE-G1 processor, an onboard GE, and FE port adapters in slots 3 and 4.

| clear_packet _size | crypto_packet_size | out_packet_size |
|---|---|---|
| 64 | 96 | 114 |
| 300 | 336 | 354 |

| clear_packet _size | crypto_packet_size | out_packet_size |
|---|---|---|
| 1400 | 1432 | 1450 |
| Mixed packet size - 344 | 378 | 396 |

| pkt_size (bytes) | # of tunnels | 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 |
| Mixed packet size | 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 |

# Related Features and Technologies

The following features and technologies are related to the VAM:

- Internet Key Exchange (IKE)
- IP Security (IPSec)

# Related Documents

The following document describes the VAM hardware:

- VPN Acceleration Module Installation and Configuration

## Supported Platforms

The VAM feature is supported on the following platforms:

- Cisco 7200 series routers with NPE-225, NPE-400, NSE-1, and NPE-G1
- Dual VAM support is available on a Cisco 7200 series router with an NPE-G1, on Cisco IOS Release 12.2(15)T, 12.1(14)E, and 12.3M.
- Cisco 7401ASR router

## Supported Standards MIBs and RFCs

### Standards

- No new or modified standards are supported by this feature.

### MIBs

The following MIBs were introduced or modified in this feature:

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

http://www.cisco.com/register To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

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

### RFCs

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

# How To Configure VPN Acceleration

On power up if the enabled LED is on, the VAM is fully functional and does not require any configuration commands. However, for the VAM to provide encryption services, you must complete the following tasks:

- Configuring an IKE Policy, page 6 (required)
- Configuring IPSec, page 8 (required)

- Configuring an IKE Policy, page 6
- Configuring IPSec, page 8
- Troubleshooting Tips, page 12
- Monitoring and Maintaining the VPN Acceleration Module, page 13

## Configuring an IKE Policy

If you do not specify a value for a parameter, the default value is assigned. For information on default values, refer to the “IP Security and Encryption” chapter of the Security Command Reference publication.

To configure an IKE policy, use the following commands beginning in global configuration mode:

### SUMMARY STEPS

1. Router(config)# **crypto isakmp policy** *priority*
2. Router(config-isakmp)# **encryption** {**des**| **3des**| **aes**| **aes 192** | **aes 256**}
3. Router(config-isakmp)# **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
4. Router(config-isakmp)# **lifetime***seconds*
5. Router(config-isakmp)# **hash** {**sha** | **md5**}
6. Router(config-isakmp)# **group** {**1** | **2**| **5**}

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Router(config)# **crypto isakmp policy** *priority* | Defines an IKE policy and enters Internet Security Association Key Management Protocol (ISAKMP) policy configuration (config-isakmp) mode. |
| **Step 2** | Router(config-isakmp)# **encryption** {**des**\| **3des**\| **aes**\| **aes 192** \| **aes 256**} | Specifies the encryption algorithm within an IKE policy.<br>• des--Specifies 56-bit DES as the encryption algorithm.<br>• 3des--Specifies 168-bit DES as the encryption algorithm.<br>• **aes** --Specifies 128-bit AES as the encryption algorithm.<br>• **aes 192** --Specifies 192-bit AES as the encryption algorithm.<br>• **aes 256** --Specifies 256-bit AES as the encryption algorithm. |
| **Step 3** | Router(config-isakmp)# **authentication** {**rsa-sig** \| **rsa-encr** \| **pre-share**} | (Optional) Specifies the authentication method within an IKE policy.<br>• **rsa-sig** --Specifies Rivest, Shamir, and Adelman (RSA) signatures as the authentication method.<br>• **rsa-encr** --Specifies RSA encrypted nonces as the authentication method.<br>**Note** Beginning with Cisco IOS Release 12.3(10), rsa-encr is now enabled for VAM crypto cards.<br>• **pre-share** --Specifies preshared keys as the authentication method.<br>**Note** If this command is not enabled, the default value (**rsa-sig**) will be used. |
| **Step 4** | Router(config-isakmp)# **lifetime***seconds* | (Optional) Specifies the lifetime of an IKE security association (SA).<br>seconds--Number of seconds that each SA should exist before expiring. Use an integer from 60 to 86,400 seconds.<br>**Note** If this command is not enabled, the default value (86,400 seconds [one day]) will be used. |
| **Step 5** | Router(config-isakmp)# **hash** {**sha** \| **md5**} | (Optional) Specifies the hash algorithm within an IKE policy.<br>• **sha** --Specifies SHA-1 (HMAC variant) as the hash algorithm.<br>• **md5** --Specifies MD5 (HMAC variant) as the hash algorithm.<br>**Note** If this command is not enabled, the default value (**sha**) will be used. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | Router(config-isakmp)# **group** {**1** \| **2**\| **5**} | (Optional) Specifies the Diffie-Hellman (DH) group identifier within an IKE policy.<br>**1** --Specifies the 768-bit DH group.<br>**2** --Specifies the 1024-bit DH group.<br>**5** --Specifies the 1536-bit DH group.<br>**Note** If this command is not enabled, the default value (768-bit) will be used. |

For detailed information on creating IKE policies, refer to the “ Configuring Internet Key Exchange for IPsec VPNsmodule in the *Cisco IOS Security Configuration Guide: Secure Connectivity* .

# Configuring IPSec

After you have completed IKE configuration, configure IPSec at each participating IPSec peer. This section contains basic steps to configure IPSec and includes the tasks discussed in the following sections:

- Creating Crypto Access Lists, page 8
- Defining Transform Sets, page 9
- Creating Crypto Map Entries using IKE, page 10
- Verifying the Configuration, page 10

## Creating Crypto Access Lists

To create crypto access lists, use the following commands in global configuration mode:

### SUMMARY STEPS

1. Do one of the following:
    - Router(config)# **access-list** *access-list-number* **deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**]
    - 
    - **ip access-list extended** *name*
2. Add **permit** and **deny** statements as appropriate.
3. Router(config-if)# **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Do one of the following:<br>• Router(config)# **access-list** *access-list-number* **deny** \| **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**]<br>•<br>• **ip access-list extended** *name* | Specifies conditions to determine which IP packets are protected. (Enable or disable encryption for traffic that matches these conditions.)<br>We recommend that you configure “mirror image” crypto access lists for use by IPSec and that you avoid using the **any** keyword.<br>**Note** You specify conditions using an IP access list designated by either a number or a name. The **access-list** command designates a numbered extended access list; the **ip access-list extended** command designates a named access list. |
| **Step 2** | Add **permit** and **deny** statements as appropriate. | Adds permit or deny statements to access lists. |
| **Step 3** | Router(config-if)# **end** | Exits the configuration command mode. |

## Defining Transform Sets

To define a transform set, use the following commands, starting in global configuration mode:

| Command | Purpose |
|---|---|
| `Router#` **crypto ipsec transform-set** `transform-set-name transform1 [transform2 [transform3]]` | Defines a transform set and enters crypto transform configuration mode. |
| `Router#` **mode** `[`**tunnel** `\|` **transport**`]` | Changes the mode associated with the transform set. The mode setting is applicable only to traffic whose source and destination addresses are the IPSec peer addresses; it is ignored for all other traffic. (All other traffic is in tunnel mode only.) |
| `Router#` **end** | Exits the crypto transform configuration mode to enabled mode. |

| Command | Purpose |
|---|---|
| `Router#` **clear crypto sa**<br>or<br>**clear crypto sa peer** `{ip-address \| peer-name}`<br>or<br>**clear crypto sa map** `map-name`<br>or<br>**clear crypto sa spi** `destination-address protocol spi` | Clears existing IPSec security associations so that any changes to a transform set take effect on subsequently established security associations (SAs). (Manually established SAs are reestablished immediately.)<br>Using the **clear crypto sa** command without parameters clears out the full SA database, which clears out active security sessions. You might also specify the **peer**, **map**, or **entry** keywords to clear out only a subset of the SA database. |

## Creating Crypto Map Entries using IKE

To create crypto map entries that use IKE to establish the security associations, use the following commands, starting in global configuration mode.

Repeat this task to create additional crypto map entries as required.

For detailed information on configuring crypto maps, refer to the Configuring IPSec Network Security chapter in the Security Configuration Guide publication:

| Command | Purpose |
|---|---|
| `Router#` **crypto map** *map-name seq-num* **ipsec-isakmp** | Creates the crypto map and enters crypto map configuration mode. |
| `Router#` **match address** *access-list-id* | Specifies an extended access list. This access list determines which traffic is protected by IPSec and which is not. |
| `Router#` **set peer** {*hostname* \| *ip-address* | Specifies a remote IPSec peer. This is the peer to which IPSec-protected traffic can be forwarded.<br>Repeat for multiple remote peers. |
| `Router#` **set transform-set** *transform-set-name1* [*transform-set-name2. . .transform-set-name6* | Specifies which transform sets are allowed for this crypto map entry. Lists multiple transform sets in order of priority (highest priority first). |
| `Router#` **end** | Exits crypto map configuration mode. |

## Verifying the Configuration

The following steps provide information on verifying your configurations:

### SUMMARY STEPS

1. Enter the **show crypto ipsec transform-set** command to view your transform set configuration:
2. Enter the **show crypto map** [**interface** *interface* | **tag** *map-name*] command to view your crypto map configuration:
3. Enter the s**how crypto ipsec sa** [**map** *map-name* | **address** | **identity** | **detail** | **interface**] command to view information about IPSec security associations.

### DETAILED STEPS

**Step 1** Enter the **show crypto ipsec transform-set** command to view your transform set configuration:

**Example:**

```
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,},
```

**Step 2** Enter the **show crypto map** [**interface** *interface* | **tag** *map-name*] command to view your crypto map configuration:

**Example:**

```
outer# show crypto mapCrypto 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,}
```

**Step 3** Enter the s**how crypto ipsec sa** [**map** *map-name* | **address** | **identity** | **detail** | **interface**] command to view information about IPSec security associations.

**Example:**

```
Router# show crypto ipsec sainterface: 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:
```

# Troubleshooting Tips

To verify that Cisco IOS software has recognized VAM, enter the **show diag** command and check the output. For example, when the router has the VAM in slot 1, the following output appears:

```
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
```

To see if the VAM is currently processing crypto packets, enter the **show pas vam interface** command. The following is sample output:

```
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
```

When the VAM processes packets, the “packet in” and “packet out” counters change. Counter “packets out” represents the number of packets directed to the VAM. Counter “packets in” represents the number of packets received from the VAM.

**Note** In versions prior to Cisco IOS Release 12.2(5)T and Cisco IOS Release 12.1(10)E, upon reboot trap configurations are lost and need to be re-entered.

# Monitoring and Maintaining the VPN Acceleration Module

Use the commands below to monitor and maintain the VPN Acceleration Module:

| Command | Purpose |
|---|---|
| `Router#` **show pas isa interface** | Displays the ISA interface configuration. |
| `Router#` **show pas isa controller** | Displays the ISA controller configuration. |
| `Router#` **show pas vam interface** | Verifies the VAM is currently processing crypto packets. |
| `Router#` **show pas vam controller** | Displays the VAM controller configuration. |
| `Router#` **Show version** | Displays integrated service adapter as part of the interfaces. |

# Configuration Examples for VPN Acceleration

- Configuring IKE Policies Example, page 14
- Configuring IPSec Configuration Example, page 14

## Configuring IKE Policies Example

In the following example, two IKE policies are created, with policy 15 as the highest priority, policy 20 as the next priority, and the existing default priority as the lowest priority. It also creates a preshared key to be used with policy 20 with the remote peer whose IP address is 192.168.224.33.

```
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
```

## Configuring IPSec Configuration Example

The following example shows a minimal IPSec configuration where the security associations will be established via IKE:

An IPSec access list defines which traffic to protect:

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

A transform set defines how the traffic will be protected. In this example, transform set "myset1" uses DES encryption and SHA for data packet authentication:

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

Another transform set example is "myset2," which uses Triple DES encryption and MD5 (HMAC variant) for data packet authentication:

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

A crypto map joins together the IPSec access list and transform set and specifies where the protected traffic is sent (the remote IPSec peer):

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

The crypto map is applied to an interface:

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

**Note** In this example, IKE must be enabled.

# Glossary

**VAM** --VPN Acceleration Module.

**IKE** --Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each router/firewall/host must verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a CA service.

**IPSec** --IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.