VPN Acceleration Module

Last Updated: December 3, 2012

VPN Acceleration Module (VAM) supports Data Encryption Standard (DES) or Triple DES (3DES) IPsec encryption at a rate greater than full-duplex DS-3 line rate (up to 145 Mbps) for site-to-site VPNs such as intranets and extranets. VAM also supports up to 5000 encrypted tunnels for mixed VPN environments that have both site-to-site and remote access VPN requirements. VAM integrates hardware-assisted Rivest, Shamir, and Adelman (RSA) and IP Payload Compression Protocol (IPPCP) layer 3 compression to accelerate RSA processing, thereby enhancing tunnel setup and improving overall VPN initialization. In environments where bandwidth is costly, VAM provides hardware-based IPPCP Lempel-Ziv-Stac (LZS) processing to compress network traffic before it is encrypted and sent over pay-per-byte WAN connections.

- Finding Feature Information, page 1
- Prerequisites for VPN Acceleration Module, page 1
- Information about VPN Acceleration Module (VAM), page 2
- How To Configure VPN Acceleration Module (VAM), page 5
- Configuration Examples for VPN Acceleration, page 17
- Additional References for VPN Acceleration Module, page 18
- Feature Information for VPN Acceleration Module, page 19
- Glossary, page 21

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 for VPN Acceleration Module

You must configure IPSec and IKE on the router and a crypto map to all interfaces that require encryption service from the VPN Acceleration Module.
Information about VPN Acceleration Module (VAM)

- VPN Acceleration Module (VAM) Overview, page 2
- Benefits, page 2

VPN Acceleration Module (VAM) Overview

The VPN Acceleration Module (VAM) is a single-width acceleration module. It provides high-performance, hardware-assisted tunneling and encryption services suitable for 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)
- Rivest, Shamir, Adelman (RSA) public-key algorithm
- Diffie-Hellman key exchange RC4-40

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.

<table>
<thead>
<tr>
<th>clear_packet_size</th>
<th>crypto_packet_size</th>
<th>out_packet_size</th>
</tr>
</thead>
<tbody>
<tr>
<td>64</td>
<td>96</td>
<td>114</td>
</tr>
<tr>
<td>300</td>
<td>336</td>
<td>354</td>
</tr>
<tr>
<td>1400</td>
<td>1432</td>
<td>1450</td>
</tr>
<tr>
<td>Mixed packet size - 344</td>
<td>378</td>
<td>396</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>pkt_size (bytes)</th>
<th># of tunnels</th>
<th>measured_pps (pps)</th>
<th>meas_clear_ndr (Mbps)</th>
<th>meas_crypto_ndr (Mbps)</th>
<th>meas_out_ndr (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>64</td>
<td>4</td>
<td>65,224</td>
<td>33.39</td>
<td>50.09</td>
<td>59.48</td>
</tr>
<tr>
<td>500</td>
<td></td>
<td>41,888</td>
<td>21.44</td>
<td>32.17</td>
<td>38.20</td>
</tr>
<tr>
<td>1,000</td>
<td></td>
<td>40,480</td>
<td>20.73</td>
<td>31.09</td>
<td>36.92</td>
</tr>
<tr>
<td>5,000</td>
<td></td>
<td>39,408</td>
<td>20.18</td>
<td>30.27</td>
<td>35.94</td>
</tr>
<tr>
<td>300</td>
<td>4</td>
<td>38,032</td>
<td>91.28</td>
<td>102.23</td>
<td>107.71</td>
</tr>
<tr>
<td>500</td>
<td></td>
<td>37,184</td>
<td>89.24</td>
<td>99.95</td>
<td>105.31</td>
</tr>
<tr>
<td>1,000</td>
<td></td>
<td>36,064</td>
<td>86.55</td>
<td>96.94</td>
<td>102.13</td>
</tr>
<tr>
<td>5,000</td>
<td></td>
<td>36,016</td>
<td>86.44</td>
<td>96.81</td>
<td>101.99</td>
</tr>
<tr>
<td>1400</td>
<td>4</td>
<td>9,984</td>
<td>111.82</td>
<td>114.38</td>
<td>115.81</td>
</tr>
<tr>
<td>500</td>
<td></td>
<td>9,848</td>
<td>110.29</td>
<td>112.82</td>
<td>114.24</td>
</tr>
<tr>
<td>1,000</td>
<td></td>
<td>9,648</td>
<td>108.06</td>
<td>110.53</td>
<td>111.92</td>
</tr>
<tr>
<td>5,000</td>
<td></td>
<td>9,616</td>
<td>107.70</td>
<td>110.16</td>
<td>111.55</td>
</tr>
<tr>
<td>Mixed packet size</td>
<td>4</td>
<td>31,472</td>
<td>86.61</td>
<td>95.17</td>
<td>99.70</td>
</tr>
<tr>
<td>500</td>
<td></td>
<td>31,056</td>
<td>85.47</td>
<td>93.91</td>
<td>98.39</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>pkt_size (bytes)</th>
<th># of tunnels</th>
<th>measured_pps (pps)</th>
<th>meas_clear_ndr (Mbps)</th>
<th>meas_crypto_ndr (Mbps)</th>
<th>meas_out_ndr (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000</td>
<td>30,128</td>
<td>82.91</td>
<td>91.11</td>
<td>95.45</td>
<td></td>
</tr>
<tr>
<td>5,000</td>
<td>29,264</td>
<td>80.53</td>
<td>88.49</td>
<td>92.71</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear_packet_size</th>
<th>crypto_packet_size</th>
<th>out_packet_size</th>
</tr>
</thead>
<tbody>
<tr>
<td>64</td>
<td>96</td>
<td>114</td>
</tr>
<tr>
<td>300</td>
<td>336</td>
<td>354</td>
</tr>
<tr>
<td>1400</td>
<td>1432</td>
<td>1450</td>
</tr>
<tr>
<td>Mixed packet size</td>
<td>378</td>
<td>396</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>pkt_size (bytes)</th>
<th># of tunnels</th>
<th>measured_pps (pps)</th>
<th>meas_clear_ndr (Mbps)</th>
<th>meas_crypto_ndr (Mbps)</th>
<th>meas_out_ndr (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>64</td>
<td>4</td>
<td>135,544</td>
<td>69.40</td>
<td>104.10</td>
<td>123.61</td>
</tr>
<tr>
<td>500</td>
<td>61,520</td>
<td>31.50</td>
<td>47.25</td>
<td>56.11</td>
<td></td>
</tr>
<tr>
<td>1,000</td>
<td>56,928</td>
<td>29.15</td>
<td>43.72</td>
<td>51.92</td>
<td></td>
</tr>
<tr>
<td>5,000</td>
<td>43,744</td>
<td>22.40</td>
<td>33.60</td>
<td>39.89</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>4</td>
<td>71,336</td>
<td>171.21</td>
<td>191.75</td>
<td>202.02</td>
</tr>
<tr>
<td>500</td>
<td>60,416</td>
<td>145.00</td>
<td>162.40</td>
<td>171.10</td>
<td></td>
</tr>
<tr>
<td>1,000</td>
<td>56,016</td>
<td>134.44</td>
<td>150.57</td>
<td>158.64</td>
<td></td>
</tr>
<tr>
<td>5,000</td>
<td>42,496</td>
<td>101.99</td>
<td>114.23</td>
<td>120.35</td>
<td></td>
</tr>
<tr>
<td>1400</td>
<td>4</td>
<td>18,736</td>
<td>209.84</td>
<td>214.64</td>
<td>217.34</td>
</tr>
<tr>
<td>500</td>
<td>18,424</td>
<td>206.35</td>
<td>211.07</td>
<td>213.72</td>
<td></td>
</tr>
<tr>
<td>1,000</td>
<td>18,352</td>
<td>205.54</td>
<td>210.24</td>
<td>212.88</td>
<td></td>
</tr>
<tr>
<td>5,000</td>
<td>18,352</td>
<td>205.54</td>
<td>210.24</td>
<td>212.88</td>
<td></td>
</tr>
<tr>
<td>Mixed packet size</td>
<td>4</td>
<td>60,416</td>
<td>166.26</td>
<td>182.70</td>
<td>191.40</td>
</tr>
<tr>
<td>500</td>
<td>57,888</td>
<td>159.31</td>
<td>175.05</td>
<td>183.40</td>
<td></td>
</tr>
<tr>
<td>1,000</td>
<td>55,488</td>
<td>152.70</td>
<td>167.80</td>
<td>175.79</td>
<td></td>
</tr>
</tbody>
</table>
Creating IKE Policies

The following restrictions apply if you are configuring an AES IKE policy:

- Your device must support IPsec and long keys (the “k9” subsystem).
- AES cannot encrypt IPsec and IKE traffic if an acceleration card is present.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. crypto isakmp policy _priority_
4. encryption {des | 3des | aes | aes 192 | aes 256}
5. hash {sha | sha256 | sha384 | md5}
6. authentication {rsa-sig | rsa-encr | pre-share}
7. group {1 | 2 | 5 | 14 | 15 | 16 | 19 | 20 | 24}
8. lifetime _seconds_
9. exit
10. exit
11. show crypto isakmp policy
12. Repeat these steps for each policy you want to create.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>- Enter your password if prompted.</td>
</tr>
</tbody>
</table>

**How To Configure VPN Acceleration Module (VAM)**

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:

- Creating IKE Policies, page 5
- Configuring IPsec, page 8
- Troubleshooting Tips, page 15
- Monitoring and Maintaining the VPN Acceleration Module, page 16

<table>
<thead>
<tr>
<th>pkt_size (bytes)</th>
<th># of tunnels</th>
<th>measured_pps (pps)</th>
<th>meas_clear_ndr (Mbps)</th>
<th>meas_crypto_n dr (Mbps)</th>
<th>meas_out_ndr (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000</td>
<td>34,272</td>
<td>94.32</td>
<td>103.64</td>
<td>108.57</td>
<td></td>
</tr>
</tbody>
</table>
### Creating IKE Policies

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> crypto isakmp policy <em>priority</em></td>
<td>Defines an IKE policy and enters config-isakmp configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# crypto isakmp policy 10</td>
</tr>
<tr>
<td><strong>Step 4</strong> encryption {des</td>
<td>3des</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-isakmp)# encryption aes 256</td>
</tr>
<tr>
<td><strong>Step 5</strong> hash {sha</td>
<td>sha256</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-isakmp)# hash sha</td>
</tr>
<tr>
<td><strong>Step 6</strong> authentication {rsa-sig</td>
<td>rsa-encr</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-isakmp)# authentication pre-share</td>
</tr>
</tbody>
</table>

- **priority** —Uniquely identifies the IKE policy and assigns a priority to the policy. Valid values: 1 to 10,000; 1 is the highest priority.
- **des**—56-bit DES-CBC (No longer recommended. AES is the recommended encryption algorithm)
- **3des**—168-bit DES (No longer recommended. AES is the recommended encryption algorithm)
- **aes**—128-bit AES
- **aes 192**—192-bit AES
- **aes 256**—256-bit AES
- **sha256** keyword specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm.
- **sha384** keyword specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.
- **md5** keyword specifies MD5 (HMAC variant) as the hash algorithm. (No longer recommended. SHA-256 is the recommended replacement.)
- **rsa-sig**—RSA signatures require that you configure your peer routers to obtain certificates from a CA.
- **rsa-encr**—RSA encrypted nonces require that you ensure each peer has the other peer’s RSA public keys.
- **pre-share**—Preshared keys require that you separately configure these preshared keys.
## Creating IKE Policies

### How To Configure VPN Acceleration Module (VAM)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong> group {1</td>
<td>2</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-isakmp)# group 14</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> lifetime seconds</td>
<td>Specifies the lifetime of the IKE SA.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-isakmp)# lifetime 180</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> exit</td>
<td>Exits config-isakmp configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-isakmp)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> exit</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

The group chosen must be strong enough (have enough bits) to protect the IPsec keys during negotiation. A generally accepted guideline recommends the use of a 2048-bit group after 2013 (until 2030). Group 14 or higher (where possible) can be selected to meet this guideline. Even if a longer-lived security method is needed, the use of Elliptic Curve Cryptography is recommended, but group 15 and group 16 can also be considered.

The ISAKMP group and the IPsec perfect forward secrecy (PFS) group should be the same if PFS is used. If PFS is not used, a group is not configured in the IPsec crypto map.

The shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec SAs can be set up more quickly.
### Command or Action

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show crypto isakmp policy</td>
<td>(Optional) Displays all existing IKE policies.</td>
</tr>
</tbody>
</table>

**Example:**

```
Router# show crypto isakmp policy
```

### Step 12

Repeat these steps for each policy you want to create.

---

**Examples**

The following sample output from the `show crypto isakmp policy` command displays a warning message after a user tries to configure an IKE encryption method that the hardware does not support:

```
Router# show crypto isakmp policy
Protection suite of priority 1
WARNING: encryption hardware does not support the configured
 encryption method for ISAKMP policy 1
 hash algorithm: Secure Hash Standard 2 (256-bit)
 authentication method: Pre-Shared Key
 Diffie-Hellman group: #14 (2048 bit)
 lifetime: 3600 seconds, no volume limit
```

### Configuring IPsec

After you have completed IKE configuration, configure IPsec at each participating IPsec peer. This section contains basic steps to configure IPsec.

- Creating Crypto Access Lists, page 8
- Configuring Transform Sets for IKEv1, page 9
- Creating Static Crypto Maps, page 11
- Verifying the Configuration, page 13

### Creating Crypto Access Lists

**SUMMARY STEPS**

1. enable
2. configure terminal
3. Do one of the following:
   - `access-list access-list-number {deny | permit} protocol source source-wildcard destination destination-wildcard [log]`
   - `ip access-list extended name`
4. Repeat Step 3 for each crypto access list you want to create.
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> Do one of the following:</td>
<td>Specifies conditions to determine which IP packets are protected.</td>
</tr>
<tr>
<td>• access-list <strong>access-list-number</strong> {deny</td>
<td>permit} protocol <strong>source</strong> source-wildcard destination destination-wildcard [log]</td>
</tr>
<tr>
<td>• ip access-list extended <strong>name</strong></td>
<td>• You specify conditions using an IP access list designated by either a number or a name. The <strong>access-list</strong> command designates a numbered extended access list; the <strong>ip access-list extended</strong> command designates a named access list.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enable or disable crypto for traffic that matches these conditions.</td>
</tr>
<tr>
<td>Device(config)# access-list 100 permit ip 10.0.68.0 0.0.0.255 10.1.1.0 0.0.0.255</td>
<td><strong>Tip</strong> Cisco recommends that you configure “mirror image” crypto access lists for use by IPsec and that you avoid using the <strong>any</strong> keyword.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# ip access-list extended vpn-tunnel</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> Repeat Step 3 for each crypto access list you want to create.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Transform Sets for IKEv1

#### Summary Steps

1. enable
2. configure terminal
3. crypto ipsec transform-set **transform-set-name** transform1 [transform2 [transform3]]
4. mode [tunnel | transport]
5. end
6. clear crypto sa [peer \{ip-address | peer-name\} | sa map **map-name** | sa entry destination-address protocol spi]
7. show crypto ipsec transform-set [tag **transform-set-name**]
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |

**Example:**  
Device> enable

<table>
<thead>
<tr>
<th><strong>Step 2</strong> configure terminal</th>
<th>Enters global configuration mode.</th>
</tr>
</thead>
</table>

**Example:**  
Device# configure terminal

| **Step 3** crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]] | Defines a transform set and enters crypto transform configuration mode.  
- There are complex rules defining the entries that you can use for transform arguments. These rules are explained in the command description for the `crypto ipsec transform-set` command, and the table in “About Transform Sets” section provides a list of allowed transform combinations. |
|-----------------------------------------------|---------------------------------------------------------------------------------|

**Example:**  
Device(config)# crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac

| **Step 4** mode [tunnel | transport] | (Optional) 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.) |
|----------------------|-------------------------------------------------|

**Example:**  
Device(cfg-crypto-tran)# mode transport

<table>
<thead>
<tr>
<th><strong>Step 5</strong> end</th>
<th>Exits crypto transform configuration mode and enters privileged EXEC mode.</th>
</tr>
</thead>
</table>

**Example:**  
Device(cfg-crypto-tran)# end

| **Step 6** clear crypto sa [peer {ip-address | peer-name}] [sa map map-name | sa entry destination-address protocol spi] | (Optional) Clears existing IPsec security associations so that any changes to a transform set takes effect on subsequently established security associations.  
Manually established SAs are reestablished immediately.  
- Using the `clear crypto sa` command without parameters clears out the full SA database, which clears out active security sessions.  
- You may also specify the `peer`, `map`, or `entry` keywords to clear out only a subset of the SA database. |
|-------------------|--------------------------------------------------------------------------------|

**Example:**  
Device# clear crypto sa

<table>
<thead>
<tr>
<th><strong>Step 7</strong> show crypto ipsec transform-set [tag transform-set-name]</th>
<th>(Optional) Displays the configured transform sets.</th>
</tr>
</thead>
</table>

**Example:**  
Device# show crypto ipsec transform-set
Creating Static Crypto Maps

When IKE is used to establish SAs, the IPsec peers can negotiate the settings they use for the new security associations. This means that you can specify lists (such as lists of acceptable transforms) within the crypto map entry.

Perform this task to create crypto map entries that use IKE to establish SAs. To create IPv6 crypto map entries, you must use the ipv6 keyword with the crypto map command. For IPv4 crypto maps, use the crypto map command without the ipv6 keyword.

Note

Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

SUMMARY STEPS

1. enable
2. configure terminal
3. crypto map [ipv6] map-name seq-num [ipsec-isakmp]
4. match address access-list-id
5. set peer {hostname | ip-address}
6. set transform-set transform-set-name1 [transform-set-name2...transform-set-name6]
7. set security-association lifetime {seconds seconds | kilobytes kilobytes | kilobytes disable}
8. set security-association level per-host
9. set pfs {group1 | group14 | group15 | group16 | group19 | group2 | group20 | group24 | group5}
10. end
11. show crypto map [interface interface | tag map-name]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>![Example](Device&gt; enable)</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>![Example](Device# configure terminal)</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Step 3** crypto map [ipv6] map-name seq-num [ipsec-isakmp] | Creates or modifies a crypto map entry, and enters crypto map configuration mode.  
- For IPv4 crypto maps, use the command without the `ipv6` keyword. |

*Example:*  
Device(config)# crypto map static-map 1 ipsec-isakmp

| **Step 4** match address access-list-id | Names an extended access list.  
- This access list determines the traffic that should be protected by IPsec and the traffic that should not be protected by IPsec security in the context of this crypto map entry. |

*Example:*  
Device(config-crypto-m)# match address vpn-tunnel

| **Step 5** set peer [hostname | ip-address] | Specifies a remote IPsec peer—the peer to which IPsec protected traffic can be forwarded.  
- Repeat for multiple remote peers. |

*Example:*  
Device(config-crypto-m)# set-peer 192.168.101.1

| **Step 6** set transform-set transform-set-name1  
[transform-set-name2...transform-set-name6] | Specifies the transform sets that are allowed for this crypto map entry.  
- List multiple transform sets in the order of priority (highest priority first). |

*Example:*  
Device(config-crypto-m)# set transform-set aeset

| **Step 7** set security-association lifetime {seconds seconds | kilobytes kilobytes | kilobytes disable} | (Optional) Specifies a SA lifetime for the crypto map entry.  
- By default, the SAs of the crypto map are negotiated according to the global lifetimes, which can be disabled. |

*Example:*  
Device {config-crypto-m)# set security-association lifetime seconds 2700

| **Step 8** set security-association level per-host | (Optional) Specifies that separate SAs should be established for each source and destination host pair.  
- By default, a single IPsec “tunnel” can carry traffic for multiple source hosts and multiple destination hosts.  
**Caution** Use this command with care because multiple streams between given subnets can rapidly consume resources. |

*Example:*  
Device(config-crypto-m)# set security-association level per-host
### Command or Action

| Step 9 | set pfs [group1 | group14 | group15 | group16 | group19 | group2 | group20 | group24 | group5] |
|--------|-----------------------------------------------|

**Purpose**

(Optional) Specifies that IPsec either should ask for password forward secrecy (PFS) when requesting new SAs for this crypto map entry or should demand PFS in requests received from the IPsec peer.

- Group 1 specifies the 768-bit Diffie-Hellman (DH) identifier (default). (No longer recommended).
- Group 2 specifies the 1024-bit DH identifier. (No longer recommended).
- Group 5 specifies the 1536-bit DH identifier. (No longer recommended)
- Group 14 specifies the 2048-bit DH identifier.
- Group 15 specifies the 3072-bit DH identifier.
- Group 16 specifies the 4096-bit DH identifier.
- Group 19 specifies the 256-bit elliptic curve DH (ECDH) identifier.
- Group 20 specifies the 384-bit ECDH identifier.
- Group 24 specifies the 2048-bit DH/DSA identifier.
- By default, PFS is not requested. If no group is specified with this command, group 1 is used as the default.

### Step 10

**end**

Exits crypto map configuration mode and returns to privileged EXEC mode.

**Example:**

```
Device(config-crypto-m)# end
```

### Step 11

**show crypto map [interface interface | tag map-name]**

Displays your crypto map configuration.

**Example:**

```
Device# show crypto map
```

---

### Verifying the Configuration

**SUMMARY STEPS**

1. show crypto ipsec transform-set
2. show crypto map [interface interface | tag map-name]
3. show crypto ipsec sa [map map-name | address | identity | detail | interface]

**DETAILED STEPS**

### Step 1

**show crypto ipsec transform-set**
Verifying the Configuration

Example:

Device# 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}
    {esp-des}
    will negotiate = {Tunnel,},
Displays the transform set configuration.

Step 2

show crypto map [interface interface | tag map-name]

Example:

Device# show crypto map

Crypto Map ºabcº 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,}
Displays the crypto map configuration.

Step 3

show crypto ipsec sa [map map-name | address | identity | detail | interface]

Example:

Device# show crypto map ipsec sa interface

Crypto map tag: abc, 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
    #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

14
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: abc, local addr. 172.21.114.123
remote ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
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
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:
Displays information about IPsec security associations.

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 85 36
0x10:36 30 00 00 00 82 49 17 41 04 42 FF 03 00 81
0x20:00 00 00 00 04 00 80 00 00 00 00 CB 94 43 4C 45
0x30:FF 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
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
   pppq_full_err :0     pppq_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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show pas isa interface</td>
<td>Displays the ISA interface configuration.</td>
</tr>
<tr>
<td>Router# show pas isa controller</td>
<td>Displays the ISA controller configuration.</td>
</tr>
<tr>
<td>Router# show pas vam interface</td>
<td>Verifies the VAM is currently processing crypto packets.</td>
</tr>
<tr>
<td>Router# show pas vam controller</td>
<td>Displays the VAM controller configuration.</td>
</tr>
</tbody>
</table>
### Configuration Examples for VPN Acceleration

- Example: Configuring IKE Policies, page 17
- Example: Configuring IPsec Configuration, page 17

### Example: Configuring IKE Policies

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
```

### Example: Configuring IPsec Configuration

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.

### Additional References for VPN Acceleration Module

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>Security commands</td>
<td>• Cisco IOS Security Command Reference Commands A to C</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference Commands D to L</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference Commands M to R</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference Commands S to Z</td>
</tr>
<tr>
<td>IPsec configuration</td>
<td>Configuring IPsec</td>
</tr>
<tr>
<td>IKE configuration</td>
<td>Configuring IKE</td>
</tr>
<tr>
<td>VAM installation and configuration tasks</td>
<td>VAM Installation and Configuration Guide</td>
</tr>
</tbody>
</table>

#### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2393</td>
<td>IP Payload Compression Protocol (IPComp)</td>
</tr>
<tr>
<td>RFC 2395</td>
<td>IP Payload Compression Using LZS</td>
</tr>
<tr>
<td>RFCs 2401 to 2411</td>
<td>IPsec—IKE</td>
</tr>
<tr>
<td>RFC 2451</td>
<td>The ESP CBC-Mode Cipher Algorithms</td>
</tr>
</tbody>
</table>
### Feature Information for VPN Acceleration Module

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-IPSEC-FLOW-MONITOR-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
<tr>
<td>CISCO-IPSEC-MIB</td>
<td></td>
</tr>
<tr>
<td>CISCO-IPSEC-POLICY-MAP-MIB</td>
<td></td>
</tr>
</tbody>
</table>

---

### Standard/RFC

**Title**

IPSec/IKE: RFCs 2401-2411, 2451

---

### Technical Assistance

**Description**

The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.

**Link**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Acceleration Module (VAM)</td>
<td>12.1(9)E</td>
<td>VPN Acceleration Module (VAM) supports Data Encryption Standard (DES) or Triple DES (3DES) IPsec encryption at a rate greater than full-duplex DS-3 line rate (up to 145 Mbps) for site-to-site VPNs such as intranets and extranets. VAM also supports up to 5000 encrypted tunnels for mixed VPN environments that have both site-to-site and remote access VPN requirements. VAM integrates hardware-assisted Rivest, Shamir, and Adelman (RSA) and IP Payload Compression Protocol (IPPCP) layer 3 compression to accelerate RSA processing, thereby enhancing tunnel setup and improving overall VPN initialization. In environments where bandwidth is costly, VAM provides hardware-based IPPCP Lempel-Ziv-Stac (LZS) processing to compress network traffic before it is encrypted and sent over pay-per-byte WAN connections. In 12.1(9)E, this feature was introduced on the Cisco 7200 series routers on NPE-225, NPE-400, and NSE-1. In 12.1(14)E, this feature was integrated into Cisco IOS Release 12.1(14)E and support for dual VAMs on the Cisco 7200 series with NPE-G1 was added. In 12.2(9)YE, support for this feature was added to the Cisco 7401ASR router. The following commands were introduced or modified: <code>crypto engine sw ipsec, show pas vam</code></td>
</tr>
<tr>
<td></td>
<td>12.1(14)E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2(9)YE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2(13)T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2(15)T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.3(1)Mainline</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2(14)SU</td>
<td></td>
</tr>
</tbody>
</table>

---

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.
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.