DES/3DES/AES VPN Encryption Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3)

First Published: June 19, 2006
Last Updated: May 30, 2006

The DES/3DES/AES VPN Encryption Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3) feature describes how to configure virtual private network (VPN) encryption hardware advanced integration modules (AIM) in Cisco IOS Release 12.4(9)T.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for DES/3DES/AES VPN Encrytion Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3)" section on page 22.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- Prerequisites for the DES/3DES/AES VPN Encryption Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3), page 2
- Restrictions for the DES/3DES/AES VPN Encryption Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3), page 2
- Information About the DES/3DES/AES VPN Encryption Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3), page 2
- How to Configure the DES/3DES/AES VPN Encryption Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3), page 3

CISCO SYSTEMS

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

- Additional References, page 6
- Command Reference, page 7
- Feature Information for DES/3DES/AES VPN Encrytion Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3), page 22

Prerequisites for the DES/3DES/AES VPN Encryption Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3)

Installation Preconditions

- Cisco IOS software Release 12.4(9)T

Note See Table 1 for AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3 encryption module support by Cisco IOS release.

- A working IP network

  For more information about configuring IP, see the Cisco IOS IP configuration guides, Release 12.4, which may be accessed at *Cisco IOS Software Releases 12.4 Mainline Configuration Guides*.

Restrictions for the DES/3DES/AES VPN Encryption Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3)

- Rivest, Shamir, and Adelman (RSA) encryption supports only 512, 1024, 1536, and 2048 bit keys.
- To achieve maximum benefit from hardware-assisted IP Payload Compression Protocol (IPPCP), it is suggested that prefragmentation be disabled if IP compression with the Limpel Zif Stac (LZS) algorithm is enabled on IP Security (IPsec) sessions.
- Hardware acceleration is supported only for clients that are connecting to an SSL VPN gateway using SSL2.0 or SSL3.0 protocols when the rc4-md5 encryption transform is configured on the SSL VPN gateway. If aes-sha1 or 3des-sha1 encryption transforms are used, those protocols are processed on the router by the Cisco IOS software. SSL VPN clients should be configured for version 1.0 of the Transport Layer Security (TLS) protocol if you are using an encryption algorithm other than rc4-md5.

Information About the DES/3DES/AES VPN Encryption Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3)

Before using the DES/3DES/AES VPN Encryption Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3), you should be familiar with the following concept:

- Determining Which Encryption Module to Use, page 3

Determining Which Encryption Module to Use

Determine which VPN encryption module to use as described in Table 1.

Table 1 AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3 Encryption Module Support by Cisco IOS Release

Platform	Cisco IOS Release 12.4(9)T
Cisco 1841	AIM-VPN/SSL-1
Cisco 2691	AIM-VPN/SSL-2
Cisco 2801	AIM-VPN/SSL-2
Cisco 2811	AIM-VPN/SSL-2
Cisco 2821	AIM-VPN/SSL-2
Cisco 2851	AIM-VPN/SSL-2
Cisco 3725	AIM-VPN/SSL-3
Cisco 3745	AIM-VPN/SSL-3
Cisco 3825	AIM-VPN/SSL-3
Cisco 3845	AIM-VPN/SSL-3

How to Configure the DES/3DES/AES VPN Encryption Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3)

There are no configuration tasks that are specific to the encryption hardware. Both software-based and hardware-based encryption are configured in the same way. The system automatically detects the presence of the encryption hardware at bootup and uses it to encrypt data. If no encryption hardware is detected, software is used to encrypt data.

This section includes the following procedures:

- Disabling an AIM Encryption Module on a Specific Slot, page 3
- Reenabling an AIM Encryption Module on a Specific Slot, page 4
- Clearing the Statistical and Error Counters, page 5
- Verifying AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3 Encryption Information, page 5

Disabling an AIM Encryption Module on a Specific Slot

To disable an AIM encryption module on a specific slot, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no crypto engine aim** *aim-slot-number*

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no crypto engine aim** *aim-slot-number* **Example:** `Router (config)# no crypto engine aim 0`	Disables an AIM encryption module on a specific slot.

Reenabling an AIM Encryption Module on a Specific Slot

To reenable an AIM encryption module on a specific slot, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto engine aim** *aim-slot-number*

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto engine aim** *aim-slot-number* **Example:** `Router (config)# crypto engine aim 0`	Reenables an AIM encryption module on a specific slot.

Clearing the Statistical and Error Counters

To clear the statistical and error counters of the hardware accelerator of a router, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **clear crypto engine accelerator counter**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear crypto engine accelerator counter** **Example:** `Router# clear crypto engine accelerator counter`	Resets the statistical and error counters for the hardware accelerator of a router to zero.

Verifying AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3 Encryption Information

To verify AIM-VPN encryption information, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show crypto engine brief**
3. **show crypto engine accelerator statistic**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show crypto engine brief** **Example:** `Router# show crypto engine brief`	Displays a summary of the configuration information for the crypto engines.

	Command	Purpose

Step 3	`show crypto engine accelerator statistic`
	
	Example:
	`Router# show crypto engine accelerator statistic`
		Displays the statistics and error counters for the onboard hardware accelerator of the router for IPsec encryption.

Additional References

The following sections provide references related to DES/3DES/AES VPN Encryption Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3).

Related Documents

Related Topic	Document Title
Installation of VPN encryption modules	• *Installing and Upgrading Internal Modules in Cisco 1800 Series Routers (Modular)* • *Installing Advanced Integration Modules in Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers* • *Installing and Upgrading Internal Modules in Cisco 2800 Series Routers* • *Installing and Upgrading Internal Components in Cisco 3800 Series Routers*
Cisco 1800 series, Cisco 2600 series, Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series routers	• *Cisco 1800 Series Integrated Service Routers* • *Cisco 2600 Series Multiservice Platforms* • *Cisco 2800 Series Integrated Service Routers* • *Cisco 3700 Series Multiservice Access Routers* • *Cisco 3800 Series Integrated Service Routers*
Cisco IOS references	• *Cisco IOS Security Configuration Guide*, Release 12.4 • *Cisco IOS Security Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

Modified Commands

- **show crypto engine**
- **show crypto engine accelerator statistic**

New Commands

- **crypto engine aim**

Commands that may be used with this feature but are not modified in this release

For information about commands, see the *Cisco IOS Security Command Reference* (a link is provided in the "Related Documents" subsection of the Additional References section above).

- **crypto engine accelerator**

crypto engine aim

To reenable an advanced integration module (AIM) encryption module, use the **crypto engine aim** command in global configuration mode. To disable an AIM encryption module, use the **no** form of this command.

crypto engine aim *aim-slot-number*

no crypto engine aim *aim-slot-number*

Syntax Description

aim-slot-number	Slot number to which an AIM module is to be reenabled or disabled.

Defaults

An AIM module is not reenabled or disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Examples

The following example shows that the AIM module in slot 0 is to be reenabled:

```
crypto engine aim 0
```

The following example shows that the AIM module in slot 0 is to be disabled:

```
no crypto engine aim 0
```

show crypto engine

To display a summary of the configuration information for the crypto engines, use the **show crypto engine** command in privileged EXEC mode.

show crypto engine [**accelerator** | **brief** | **configuration** | **connections** | **qos**]

Syntax Description

accelerator	(Optional) Displays crypto accelerator information.
brief	(Optional) Displays a summary of the configuration information for the crypto engine.
configuration	(Optional) Displays the version and configuration information for the crypto engine.
connections	(Optional) Displays information about the crypto engine connections.
qos	(Optional) Displays quality of service (QoS) information. • This keyword has a null output if any advanced integration module (AIM) except AIM-VPN/SSL-1 is used. The command-line interface (CLI) will accept the command, but there will be no output.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced on the Cisco 7200, RSP7000, and 7500 series routers.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(4)T	IPv6 address information was added to command output.
12.4(9)T	AIM-VPN/SSL-3 encryption module information was added to command output.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command displays all crypto engines and displays the AIM-VPN product name.

Examples

The following example of the **show crypto engine** command and the **brief** keyword shows typical crypto engine summary information:

```
Router# show crypto engine brief

crypto engine name:  Virtual Private Network (VPN) Module
        crypto engine type:  hardware
                     State:  Enabled
                  Location:  aim 0
```

```
    VPN Module in slot:  0
          Product Name:  AIM-VPN/SSL-3
     Software Serial #:  55AA
             Device ID:  001F - revision 0000
             Vendor ID:  0000
           Revision No:  0x001F0000
          VSK revision:  0
          Boot version:  255
           DPU version:  0
           HSP version:  3.3(18) (PRODUCTION)
          Time running:  23:39:30
               Compression:  Yes
                       DES:  Yes
                     3 DES:  Yes
                   AES CBC:  Yes (128,192,256)
                  AES CNTR:  No
     Maximum buffer length:  4096
          Maximum DH index:  3500
          Maximum SA index:  3500
        Maximum Flow index:  7000
      Maximum RSA key size:  2048


        crypto engine name:  Cisco VPN Software Implementation
        crypto engine type:  software
             serial number:  CAD4FCE1
      crypto engine state:  installed
     crypto engine in slot:  N/A
```

The following example of the **show crypto engine** command shows IPv6 information:

```
Router# show crypto engine connections

    ID Interface  Type  Algorithm           Encrypt  Decrypt IP-Address
     1 Et2/0      IPsec MD5                       0       46 FE80::A8BB:CCFF:FE01:2C02
     2 Et2/0      IPsec MD5                      41        0 FE80::A8BB:CCFF:FE01:2C02
     5 Tu0        IPsec SHA+DES                   0        0
3FFE:2002::A8BB:CCFF:FE01:2C02
     6 Tu0        IPsec SHA+DES                   0        0
3FFE:2002::A8BB:CCFF:FE01:2C02
  1001 Tu0        IKE   SHA+DES                   0        0
3FFE:2002::A8BB:CCFF:FE01:2C02
```

Table 1 describes significant fields shown in the display.

Table 2 show crypto engine brief Field Descriptions

Field	Description
crypto engine name	Name of the crypto engine as assigned with the *key-name* argument in the **crypto key generate dss** command.
crypto engine type	If “software” is listed, the crypto engine resides in either the Route Switch Processor (RSP) (the Cisco IOS crypto engine) or in a second-generation Versatile Interface Processor (VIP2). If “crypto card” or “ESA” is listed, the crypto engine is associated with an Encryption Service Adapter (ESA).

Table 2 show crypto engine brief Field Descriptions (Continued)

Field	Description
crypto engine state	The state "installed" indicates that a crypto engine is located in the given slot, but it is not configured for encryption. The state "dss key generated" indicates the crypto engine found in that slot has DSS keys already generated.
crypto engine in slot	Chassis slot number of the crypto engine. For the Cisco IOS crypto engine, this is the chassis slot number of the RSP.

Related Commands

Command	Description
crypto engine accelerator	Enables the use of the onboard hardware accelerator for IPSec encryption.

show crypto engine accelerator statistic

To display IP Security (IPsec) encryption statistics and error counters for the onboard hardware accelerator of the router or the IPsec Virtual Private Network (VPN) Shared Port Adapter (SPA), use the **show crypto engine accelerator statistic** command in privileged EXEC mode.

show crypto engine accelerator statistic

IPsec VPN SPA

show crypto engine accelerator statistic [**slot** *slot*/*subslot* | **all**] [**detail**]

Syntax Description

slot *slot*/*subslot*	(IPsec VPN SPA only—Optional) Chassis slot number and secondary slot number on the SPA Interface Processor (SIP) where the SPA is installed. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. Displays platform statistics for the corresponding IPsec VPN SPA. This output will not include network interface controller statistics.
all	(IPsec VPN SPA only—Optional) Displays platform statistics for all IPsec VPN SPAs on the router. This output will not include network interface controller statistics.
detail	(IPsec VPN SPA only—Optional) Displays platform statistics for the IPsec VPN SPA and network interface controller statistics. Note that the controller statistics contain Layer 2 (L2) counters.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)XC	This command was introduced for the Cisco 1700 series router and other Cisco routers that support hardware accelerators for IPsec encryption.
12.1(3)XL	This command was implemented on the Cisco uBR905 cable access router.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII and AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745. In addition, the output for this **show** command was enhanced to display compression statistics.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	The AIM-VPN/BPII was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA to support the IPsec VPN SPA on Cisco 7600 series routers and Catalyst 6500 series switches.
12.4(9)T	Output was added for the AIM-VPN Secure Sockets Layer (SSL) encryption module.

Usage Guidelines

No specific usage guidelines apply to the hardware accelerators.

IPsec VPN SPA

Enter the **slot** keyword to display platform statistics for the corresponding IPSec VPN SPA. This output will not include network interface controller statistics.

Enter the **all** keyword to display platform statistics for all IPSec VPN SPAs on the router. This output will not include network interface controller statistics.

Enter the **detail** keyword to display platform statistics for the IPSec VPN SPA and network interface controller statistics. Note that the controller statistics contain L2 counters.

Examples

Hardware VPN Module

The following example displays compression statistics for a hardware VPN module:

```
Router# show crypto engine accelerator statistic

Device:   AIM-VPN/SSL-3
Location: AIM Slot: 0
Virtual Private Network (VPN) Module in slot : 0
    Statistics for Hardware VPN Module since the last clear
     of counters 85319 seconds ago
               560 packets in                        560 packets out
             95600 bytes in                       124720 bytes out
                 0 paks/sec in                         0 paks/sec out
                 0 Kbits/sec in                        0 Kbits/sec out
                 0 packets decrypted                 560 packets encrypted
                 0 bytes before decrypt            124720 bytes encrypted
                 0 bytes decrypted                  95600 bytes after encrypt
                 0 packets decompressed                0 packets compressed
                 0 bytes before decomp                 0 bytes before comp
                 0 bytes after decomp                  0 bytes after comp
                 0 packets bypass decompr              0 packets bypass compres
                 0 bytes bypass decompres              0 bytes bypass compressi
                 0 packets not decompress              0 packets not compressed
                 0 bytes not decompressed              0 bytes not compressed
                 1.0:1 compression ratio               1.0:1 overall
             10426 commands out                    10426 commands acknowledged
        Last 5 minutes:
                 0 packets in                          0 packets out
                 0 paks/sec in                         0 paks/sec out
                 0 bits/sec in                         0 bits/sec out
                 0 bytes decrypted                     0 bytes encrypted
                 0 Kbits/sec decrypted                 0 Kbits/sec encrypted
                 1.0:1 compression ratio               1.0:1 overall

    Errors:
       ppq full errors         :        0   ppq rx errors           :        0
       cmdq full errors        :        0   cmdq rx errors          :        0
```

```
    ppq down errors          :         0   cmdq down errors         :         0
    no buffer                :         0   replay errors            :         0
    dest overflow            :         0   authentication errors    :         0
    Other error              :         0   Raw Input Underrun       :         0
    IPSEC Unsupported Option:          0   IPV4 Header Length       :         0
    ESP Pad Length           :         0   IPSEC Decompression      :         0
    AH ESP seq mismatch      :         0   AH Header Length         :         0
    AH ICV Incorrect         :         0   IPCOMP CPI Mismatch      :         0
    IPSEC ESP Modulo         :         0   Unexpected IPV6 Extensio:         0
    Unexpected Protocol      :         0   Dest Buf overflow        :         0
    IPSEC Pkt is fragment    :         0   IPSEC Pkt src count      :         0
    Invalid IP Version       :         0   Unwrappable              :         0
    SSL Output overrun       :         0   SSL Decompress failure   :         0
    SSL BAD Decomp History   :         0   SSL Version Mismatch     :         0
    SSL Input overrun        :         0   SSL Conn Modulo          :         0
    SSL Input Underrun       :         0   SSL Connection closed    :         0
    SSL Unrecognised content:          0   SSL record header length:         0
    PPTP Duplicate packet    :         0   PPTP Exceed max missed p:         0
    RNG self test fail       :         0   DF Bit set               :         0
    Hash Miscompare          :         0   Unwrappable object       :         0
    Missing attribute        :         0   Invalid attrribute value:         0
    Bad Attribute            :         0   Verification Fail        :         0
    Decrypt Failure          :         0   Invalid Packet           :         0
    Invalid Key              :         0   Input Overrun            :         0
    Input Underrun           :         0   Output buffer overrun    :         0
    Bad handle value         :         0   Invalid parameter        :         0
    Bad function code        :         0   Out of handles           :         0
    Access denied            :         0   Out of memory            :         0
    NR overflow              :         0   pkts dropped             :         0

Warnings:
    sessions_expired         :         0   packets_fragmented       :         0
    general:                 :         0

HSP details:
    hsp_operations           :     10441   hsp_sessions             :         1
```

Tip In Cisco IOS Release 12.2(8)T and later releases, you can add a time stamp to show commands using the **exec prompt timestamp** command in line configuration mode.

Table 3 show crypto engine accelerator statistic Compression Statistics Descriptions

Counter	Description
packets decompressed	Number of packets that were decompressed by the interface.
packets compressed	Number of packets that were compressed by the interface.
bytes before decomp	Number of compressed bytes that were presented to the compression algorithm from the input interface on decrypt.
bytes before comp	Number of uncompressed bytes (payload) that were presented to the compression algorithm from Cisco IOS on encrypt.
bytes after decomp	Number of decompressed bytes that were sent to Cisco IOS by the compression algorithm on decrypt.
bytes after comp	Number of compressed bytes that were forwarded to Cisco IOS by the algorithm on encrypt.

Table 3 show crypto engine accelerator statistic Compression Statistics Descriptions

Counter	Description
packets bypass compres	Number of packets that were not compressed because they were too small (<128 bytes).
packets not compressed	Number of packets that were not compressed because the packets are expanded rather than compressed.
compression ratio	Ratio of compression and decompression of packets presented to the compression algorithm that were successfully compressed or decompressed. This statistic measures the efficiency of the algorithm for all packets that were compressed or decompressed.
overall	Ratio of compression and decompression of packets presented to the compression algorithm, including those that were not compressed due to expansion, too small. This ratio indicates whether the data traffic on this interface is suitable for compression. A ratio of 1:1 would imply that no successful compression is being performed on this data traffic.

IPsec VPN SPA

The following example shows the platform statistics for the IPSec VPN SPA in slot 1 subslot 0 and also displays the network interface controller statistics:

```
Router# show crypto engine accelerator statistic slot 1/0 detail

VPN module in slot 1/0


Decryption Side Data Path Statistics
====================================
Packets RX..............: 454260
Packets TX..............: 452480

IPSec Transport Mode.....: 0
IPSec Tunnel Mode........: 452470
AH Packets..............: 0
ESP Packets.............: 452470
GRE Decapsulations.......: 0
NAT-T Decapsulations.....: 0
Clear...................: 8
ICMP....................: 0

Packets Drop............: 193
Authentication Errors....: 0
Decryption Errors........: 0
Replay Check Failed......: 0
Policy Check Failed......: 0
Illegal CLear Packet.....: 0
GRE Errors..............: 0
SPD Errors..............: 0
HA Standby Drop..........: 0

Hard Life Drop..........: 0
Invalid SA..............: 191
SPI No Match............: 0
Destination No Match.....: 0
Protocol No Match........: 0
```

```
Reassembly Frag RX.......: 0
IPSec Fragments..........: 0
IPSec Reasm Done.........: 0
Clear Fragments..........: 0
Clear Reasm Done.........: 0
Datagrams Drop...........: 0
Fragments Drop...........: 0


Decryption Side Controller Statistics

====================================
Frames RX................: 756088
Bytes RX.................: 63535848
Mcast/Bcast Frames RX....: 2341
RX Less 128Bytes.........: 756025
RX Less 512Bytes.........: 58
RX Less 1KBytes..........: 2
RX Less 9KBytes..........: 3
RX Frames Drop...........: 0

Frames TX................: 452365
Bytes TX.................: 38001544
Mcast/Bcast Frames TX....: 9
TX Less 128Bytes.........: 452343
TX Less 512Bytes.........: 22
TX Less 1KBytes..........: 0
TX Less 9KBytes..........: 0


Encryption Side Data Path Statistics
====================================
Packets RX...............: 756344
Packets TX...............: 753880
IPSec Transport Mode.....: 0
IPSec Tunnel Mode........: 753869
GRE Encapsulations.......: 0
NAT-T Encapsulations.....: 0
LAF prefragmented........: 0

Fragmented...............: 0
Clear....................: 753904
ICMP.....................: 0

Packets Drop.............: 123
IKE/TED Drop.............: 27
Authentication Errors....: 0
Encryption Errors........: 0
HA Standby Drop..........: 0

Hard Life Drop...........: 0
Invalid SA...............: 191

Reassembly Frag RX.......: 0
Clear Fragments..........: 0
Clear Reasm Done.........: 0
Datagrams Drop...........: 0
Fragments Drop...........: 0


Encryption Side Controller Statistics
====================================
Frames RX................: 454065
Bytes RX.................: 6168274/
```

```
Mcast/Bcast Frames RX....: 1586
RX Less 128Bytes.........: 1562
RX Less 512Bytes.........: 452503
RX Less 1KBytes..........: 0
RX Less 9KBytes..........: 0
RX Frames Drop...........: 0

Frames TX................: 753558
Bytes TX.................: 100977246
Mcast/Bcast Frames TX....: 2
TX Less 128Bytes.........: 3
TX Less 512Bytes.........: 753555
TX Less 1KBytes..........: 0
TX Less 9KBytes..........: 0
```

Table 4 describes significant fields shown in the display.

Table 4 show crypto engine accelerator statistic IPsec VPN SPA Statistics Descriptions

Field	Description
Decryption Data Side Path Statistics	
Packets RX	Number of packets received on the decryption side of the IPSec VPN SPA.
Packets TX	Number of packets transmitted by IPSec VPN SPA in the decryption direction.
IPSec Transport Mode	Number of packets in IPSec Transport Mode.
IPSec Tunnel Mode	Number of packets in IPSec Tunnel Mode.
AH Packets	Number of packets with authentication headers (AHs).
ESP Packets	Number of packets with Encapsulating Security Payload (ESP) headers.
GRE Decapsulations	Number of packets that were generic routing encapsulating (GRE) decapsulated.
NAT-T Decapsulations	Number of packets that were Network Address Translation-Traversal (NAT-T) decapsulated.
Clear	Number of clear packets received.
ICMP	Number of Internet Control Message Protocol (ICMP) packets received.
Packets Drop	Number of packet drops.
Authentication Errors	Number of authentication errors.
Decryption Errors	Number of decryption errors.
Replay Check Failed	Number of replay check errors.
Policy Check Failed	Number of policy check errors.
Illegal Clear Packet	Number of illegal clear packets.
GRE Errors	Number of GRE errors due to invalid packets or invalid security associations (SAs).

Table 4 show crypto engine accelerator statistic IPsec VPN SPA Statistics Descriptions (Continued)

Field	Description
SPD Errors	Number of Security Policy Database (SPD) errors.
HA Standby Drop	Number of packet drops on a High Availability (HA) standby IPSec VPN SPA. **Note** The standby IPSec VPN SPA is not supposed to receive packets.
Hard Life Drop	Number of packet drops due to SA hard life expiration.
Invalid SA	Number of packet drops due to invalid SA.
SPI No Match	Number of packet drops due to SPI mismatch.
Destination No Match	Number of packet drops due to destination no match.
Protocol No Match	Number of packet drops due to protocol no match.
Reassembly Frag RX	Number of packets that required reassembly processing.
IPSec Fragments	Number of IPSec fragments.
IPSec Reasm Done	Number of IPSec fragments reassembled.
Clear Fragments	Number of clear fragments.
Clear Reasm Done	Number of clear fragments reassembled.
Datagrams Drop	Number of reassembled datagrams dropped.
Fragments Drop	Number of fragments dropped.
Decryption Side Controller Statistics	
Frames RX	Number of frames received.
Bytes RX	Number of bytes received.
Mcast/Bcast Frames RX	Number of multicast/broadcast frames received.
RX Less 128Bytes	Number of frames less than 128 bytes.
RX Less 512Bytes	Number of frames with size greater than or equal to 128 bytes and less than 512 bytes.
RX Less 1KBytes	Number of frames with size greater than or equal to 512 bytes and less than 1 kilobyte (KB).
RX Less 9KBytes	Number of frames with size greater than or equal to 1KB and less than 9 KBs.
RX Frames Drop	Number of frames dropped.
Frames TX	Number of frames transmitted.
Bytes TX	Number of bytes transmitted.
Mcast/Bcast Frames TX	Number of multicast/broadcast frames transmitted.
TX Less 128Bytes	Number of frames less than 128 bytes.

Table 4 show crypto engine accelerator statistic IPsec VPN SPA Statistics Descriptions (Continued)

Field	Description
TX Less 512Bytes	Number of frames with size greater than or equal to 128 bytes and less than 512 bytes.
TX Less 1KBytes	Number of frames with size greater than or equal to 512 bytes and less than 1 KB.
TX Less 9KBytes	Number of frames with size greater than or equal to 1 KB and less than 9 KBs.
Encryption Side Data Path Statistics	
Packets RX	Number of packets received on the encryption side of the IPSec VPN SPA.
Packets TX	Number of packets transmitted by the IPSec VPN SPA in the encryption direction.
IPSec Transport Mode	Number of packets in IPSec Transport Mode.
IPSec Tunnel Mode	Number of packets in IPSec Tunnel Mode.
GRE Encapsulations	Number of packets that were GRE encapsulated.
NAT-T Encapsulations	Number of packets that were NAT-T encapsulated.
LAF prefragmented	Number of packets with Look Ahead Fragmentation set and that were prefragmented.
Fragmented	Number of packets fragmented.
Clear	Number of clear packets.
ICMP	Number of ICMP packets.
Packets Drop	Number of packet drops.
IKE/TED Drop	Number of packet drops because SA has not been set up.
Authentication Errors	Number of authentication errors.
Encryption Errors	Number of Encryption errors.
HA Standby Drop	Number of packet drops on a HA standby IPSec VPN SPA. **Note** The standby IPSec VPN SPA is not supposed to receive packets.
Hard Life Drop	Number of packet drops due to SA hard-life expiration.
Invalid SA	Number of packet drops due to invalid SA.
Reassembly Frag RX	Number of packets that required reassembly processing.
Clear Fragments	Number of clear fragments.
Clear Reasm Done	Number of clear fragments reassembled.
Datagrams Drop	Number of reassembled datagrams dropped.
Fragments Drop	Number of fragments dropped.

Table 4 show crypto engine accelerator statistic IPsec VPN SPA Statistics Descriptions (Continued)

Field	Description
Encryption Side Controller Statistics	
Frames RX	Number of frames received.
Bytes RX	Number of bytes received.
Mcast/Bcast Frames RX	Number of multicast/broadcast frames received.
RX Less 128Bytes	Number of frames less than 128 bytes.
RX Less 512Bytes	Number of frames with size greater than or equal to 128 bytes and less than 512 bytes.
RX Less 1KBytes	Number of frames with size greater than or equal to 512 bytes and less than 1 KB.
RX Less 9KBytes	Number of frames with size greater than or equal to 1 KB and less than 9 KBs.
RX Frames Drop	Number of frames dropped.
Frames TX	Number of frames transmitted.
Bytes TX	Number of bytes transmitted.
Mcast/Bcast Frames TX	Number of multicast/broadcast frames transmitted.
TX Less 128Bytes	Number of frames less than 128 bytes.
TX Less 512Bytes	Number of frames with size greater than or equal to 128 bytes and less than 512 bytes.
TX Less 1KBytes	Number of frames with size greater than or equal to 512 bytes and less than 1 KB.
TX Less 9KBytes	Number of frames with size greater than or equal to 1 KB and less than 9 KBs.

Related Commands

Command	Description
clear crypto engine accelerator counter	Resets the statistical and error counters for the hardware accelerator to zero.
crypto ca	Defines the parameters for the certification authority used for a session.
crypto cisco	Defines the encryption algorithms and other parameters for a session.
crypto dynamic-map	Creates a dynamic map crypto configuration for a session.
crypto engine accelerator	Enables the use of the onboard hardware accelerator of the Cisco uBR905 and Cisco uBR925 routers for IPSec encryption.
crypto ipsec	Defines the IPsec SAs and transformation sets.
crypto isakmp	Enables and defines the IKE protocol and its parameters.
crypto key	Generates and exchanges keys for a cryptographic session.
crypto map	Creates and modifies a crypto map for a session.

Command	Description
debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator ring	Displays the contents of command and transmit rings for the crypto engine.
show crypto engine accelerator sa-database	Displays the active (in-use) entries in the crypto engine security association (SA) database.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

Feature Information for DES/3DES/AES VPN Encrytion Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3)

Table 5 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 5 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 5 Feature Information for DES/3DES/AES VPN Encryption Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3)

Feature Name	Releases	Feature Information
DES/3DES/AES VPN Encryption Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3)	12.4(9)T	The DES/3DES/AES VPN Encryption Module (AIM-VPN/SSL-1, AIM-VPN/SSL-2, and AIM-VPN/SSL-3) feature describes how to configure virtual private network (VPN) encryption hardware advanced integration modules (AIM).