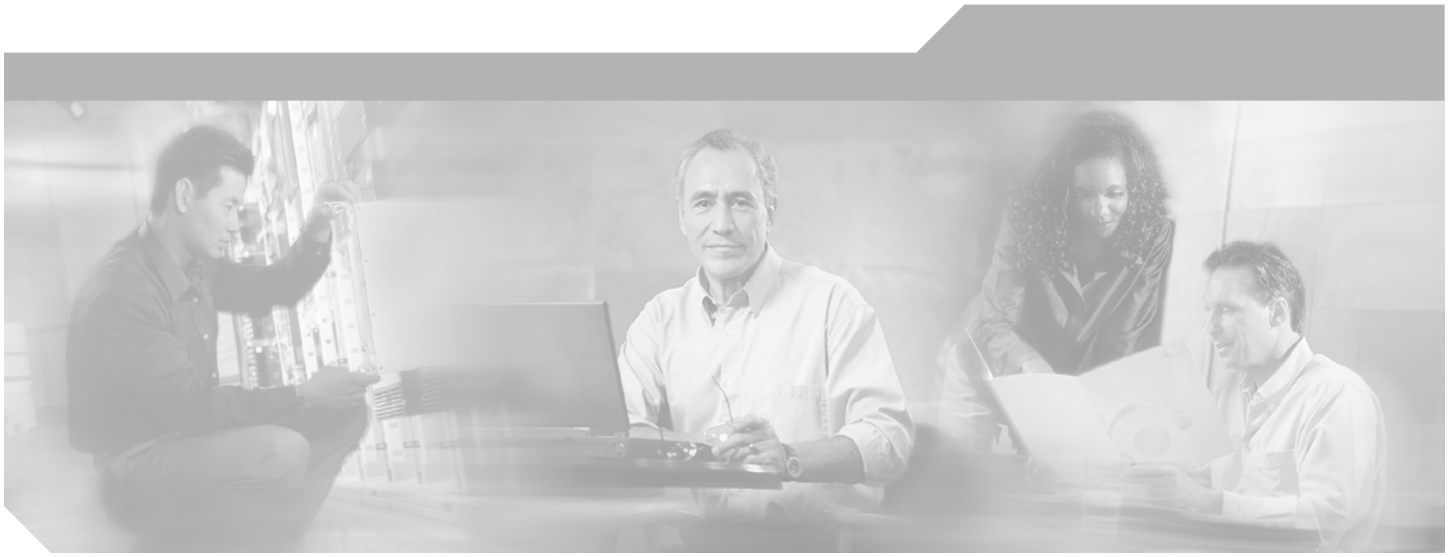


C7200 VSA (VPN Services Adapter) Installation and Configuration Guide

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-9129-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

C7200 VSA (VPN Services Adapter) Installation and Configuration Guide

CONTENTS

Preface

This preface describes the objectives and organization of this document and explains how to find additional information on related products and services. This preface contains the following sections:

Audience

The audience for this publication should be familiar with Cisco router hardware and cabling along with electronic circuitry and wiring practices. Experience as an electronic or electromechanical technician is recommended.

Warnings

Warning **To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 24°C (75°F).**

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the translated safety warnings that accompanied this device.

Note: SAVE THESE INSTRUCTIONS

Note: This documentation is to be used in conjunction with the specific product installation guide that shipped with the product. Please refer to the Installation Guide, Configuration Guide, or other enclosed additional documentation for further details.

Objectives

This document contains instructions and procedures for installing and configuring the C7200 VSA (VPN Services Adapter), a double-width acceleration module supported on the Cisco 7204VXR and Cisco 7206VXR routers with the NPE-G2 processor.

The part number for the VSA is C7200-VSA(=).

Note To ensure compliance with U.S. export laws and regulations, and to prevent future problems, see the "Compliance with U.S. Export Laws and Regulations Regarding Encryption" section on page 2-5 for specific, important information.

Organization

This document contains the following chapters:

Chapter	Title	Description
1	Overview	Describes the VSA and VSA LED displays.
2	Preparing for Installation	Describes safety considerations, tools required, and procedures you should perform before the actual installation.
3	Removing and Installing the VSA	Describes the procedures for installing and removing the VSA from the supported platform.
4	Configuring the VSA	Describes procedures needed to configure the VSA in the Cisco 7200VXR series routers.

Related Documentation

This section lists documentation related to your router and its functionality. Because we no longer ship the entire router documentation set automatically with each system, this documentation is available online, or on the Documentation CD-ROM.

Note Select translated documentation is available at http://www.cisco.com/ by selecting the topic 'Select a Location / Language' at the top of the page.

Some online documentation requires that you are a registered Cisco user. Complete the application at http://tools.cisco.com/RPF/register/register.do to become a registered Cisco user.

- For hardware installation and maintenance information for the Cisco 7200VXR series routers: http://www.cisco.com/en/US/products/hw/routers/ps341/tsd_products_support_series_home.html
- For port adapters and interface modules:
  - Port adapter installation and configuration guides, available online at: http://www.cisco.com/en/US/products/hw/modules/ps2033/tsd_products_support_series_home.html
  - Interfaces and services modules installation and configuration guides, available online at: http://www.cisco.com/en/US/products/hw/modules/tsd_products_support_category_home.html
- For Cisco IOS software configuration and support documentation, available online at: http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html
  - To find the right Cisco IOS software and the amount of memory you need to run the Cisco IOS features you want to run on your Cisco platform, use the Cisco IOS Software Selection Tool. Registered Cisco Direct users can access the Cisco IOS Software Selection Tool at: http://tools.cisco.com/ITDIT/ISTMAIN/servlet/index
  - To find the minimum Cisco IOS software requirements for your router, use the Software Advisor tool. Registered Cisco Direct users can access the Software Advisor at: http://www.cisco.com/cgi-bin/Support/CompNav/Index.pl
- For security and VPN documentation, available online at: http://www.cisco.com/en/US/tech/tk583/tsd_technology_support_category_home.html
- If you are a registered Cisco Direct Customer, you can access Technical Assistance Center tools and support at: http://www.cisco.com/kobayashi/support/tac/tools.shtml

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Overview

This chapter describes the C7200 VSA (VPN Services Adapter) and contains the following sections:

Data Encryption Overview

This section describes data encryption, including the IPSec, IKE, and certification authority (CA) interoperability features.

Note For additional information on these features, refer to the "IP Security and Encryption" chapter in the *Security Configuration Guide* and *Security Command Reference* publications.

IPSec is a network level open standards framework, developed by the Internet Engineering Task Force (IETF) that provides secure transmission of sensitive information over unprotected networks such as the Internet. IPSec includes data authentication, antireplay services and data confidentiality services.

Cisco follows these data encryption standards:

- IPSec—IPSec is an IP layer open standards framework that provides data confidentiality, data integrity, and data authentication between participating peers. IKE handles negotiation of protocols and algorithms based on local policy, and generates the encryption and authentication keys to be used by IPSec. IPSec protects one or more data flows between a pair of hosts, between a pair of security routers, or between a security router and a host.

- IKE—Internet Key Exchange (IKE) is a hybrid security protocol that implements Oakley and Skeme key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. IKE can be used with IPSec and other protocols. IKE authenticates the IPSec peers, negotiates IPSec security associations, and establishes IPSec keys. IPSec can be configured with or without IKE.
- CA—certification authority (CA) interoperability supports the IPSec standard, using Simple Certificate Enrollment Protocol (SCEP) and Certificate Enrollment Protocol (CEP). CEP permits Cisco IOS devices and CAs to communicate to permit your Cisco IOS device to obtain and use digital certificates from the CA. IPSec can be configured with or without CA. The CA must be properly configured to issue certificates. For more information, see the "Configuring Certification Authority Interoperability" chapter of the *Security Configuration Guide* at http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html

The component technologies implemented for IPSec include:

- DES and Triple DES—The Data Encryption Standard (DES) and Triple DES (3DES) encryption packet data. Cisco IOS implements the 3-key Triple DES and DES-CBC with Explicit IV. Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet.
- AES—The Advanced Encryption Standard, a next-generation symmetric encryption algorithm, used by the U.S. Government and organizations outside the U.S.
- MD5 (HMAC variant)—MD5 is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.
- SHA (HMAC variant)—SHA is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.
- RSA signatures and RSA encrypted nonces—RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA signatures provides non-repudiation while RSA encrypted nonces provide repudiation.

IPSec with the Cisco IOS software supports the following additional standards:

- AH—Authentication Header is a security protocol that provides data authentication and optional antireplay services.

  The AH protocol uses various authentication algorithms; Cisco IOS software has implemented the mandatory MD5 and SHA (HMAC variants) authentication algorithms. The AH protocol provides antireplay services.
- ESP—Encapsulating Security Payload, a security protocol, provides data privacy services, optional data authentication, and antireplay services. ESP encapsulates the data to be protected. The ESP protocol uses various cipher algorithms and (optionally) various authentication algorithms. Cisco IOS software implements the mandatory 56-bit DES-CBC with Explicit IV or Triple DES as the encryption algorithm, and MD5 or SHA (HMAC variants) as the authentication algorithms. The updated ESP protocol provides antireplay services.

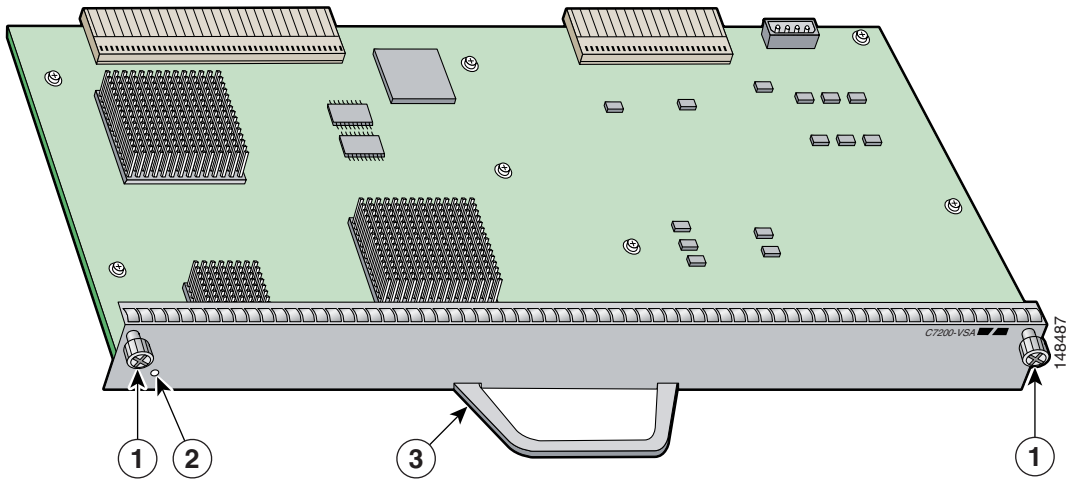
VSA Overview

The C7200 VSA (VPN Services Adapter) is a full-width service adapter (see Figure 1-1) supported in the I/O slot of the Cisco 7204VXR and Cisco 7206VXR routers with the NPE-G2 processor.

Note The C7200 VSA is only supported on the Cisco 7200VXR with the NPE-G2 processor.

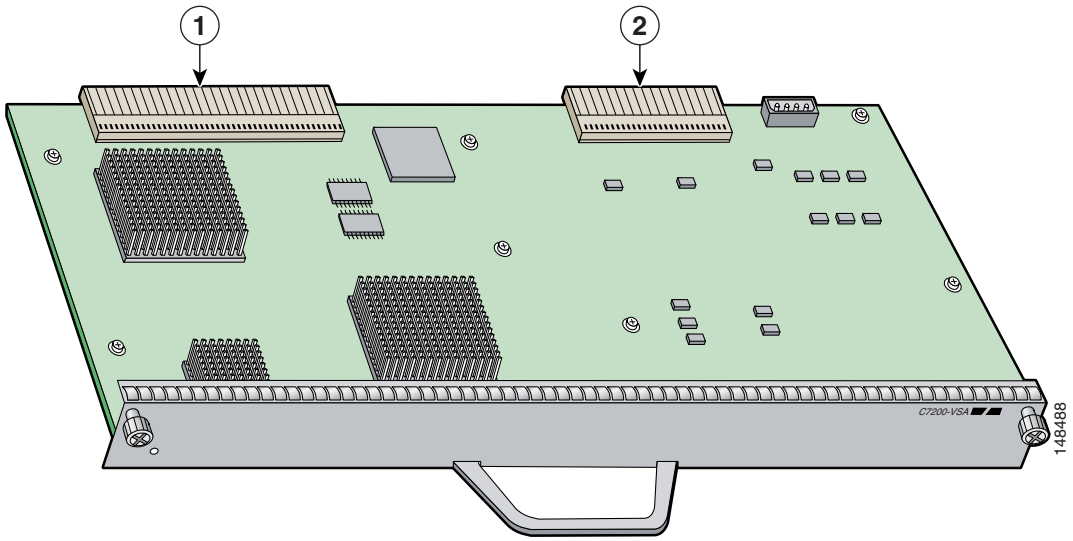
The VSA features hardware acceleration for Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES), providing increased performance for site-to-site and remote-access IPSec VPN services. The Cisco C7200 VSA solution provides quality of service (QoS), multicast and multiprotocol traffic, and broad support of integrated LAN/WAN media.

Figure 1-1 VSA Module - Front View



1	Screws	**3**	Handle
2	Status LED light		

Figure 1-2 VSA Module - Rear Connectors



1	Host IO Bus and PCI-X Bus	**2**	Power supply

The VSA provides hardware-accelerated support for multiple encryption functions:

- 128/192/256-bit Advanced Encryption Standard (AES) in hardware
- Data Encryption Standard (DES) standard mode with 56-bit key: Cipher Block Chaining (CBC)
- Performance to 900 Mbps encrypted throughput with 300 byte packets and 1000 tunnels
- 5000 tunnels for DES/3DES/AES
- Secure Hash Algorithm1 (SHA-1) and Message Digest 5 (MD5) hash algorithms
- Rivest, Shamir, Adelman (RSA) public-key algorithm
- Diffie-Hellman Groups 1, 2 and 5

Hardware Required

The hardware required to ensure proper operation of the C7200 VSA is as follows:

- The C7200 VSA is compatible with the Cisco NPE-G2 processor on the Cisco 7204VXR or Cisco 7206VXR routers.
- ROMmon requirement—12.4(4r)XD5
- I/O FPGA requirement—0x25 (decimal 0.37)
- VSA FPGA requirement—0x13 (decimal 0.19)

Features

This section describes the VSA features, as listed in Table 1-1.

Table 1-1 VSA Features

Feature	Description/Benefit
Throughput[1]	Performance to 900 Mbps encrypted throughput using 3DES or AES on the Cisco 7204VXR and Cisco 7206VXR routers
Number of IPSec protected tunnels[2]	Up to 5000 tunnels[3]
Number of tunnels per second	Note: will update after further testing
Hardware-based encryption	Data protection: IPSec DES, 3DES, and AES Authentication: RSA and Diffie-Hellman Data integrity: SHA-1 and Message Digest 5 (MD5)
VPN tunneling	IPsec tunnel mode; Generic Routing Encapsulation (GRE) and Layer 2 Tunneling Protocol (L2TP) protected by IPSec
Minimum Cisco IOS software release supported	12.4(4)XD3 fc2 or later release of 12.4XD 12.4(11)T or later release of 12.4T
Standards supported	IPSec/IKE: RFCs 2401-2411, 2451

1. As measured with IPSec 3DES HMAC-SHA1 on 1400 byte packets.

2. Number of tunnels supported varies based on the total system memory installed.
3. On the NPE-G2, the minimum memory requirement is 1 GB of memory.

Performance

Table 1-2 lists the performance information for the VSA.

Table 1-2 Performance for VSA

Cisco Router	Throughput[1] [2]	Description
Cisco 7200VXR series routers with the NPE-G2 processor	Performance to 900 Mbps encrypted throughput	Cisco IOS release: 12.4(4)XD3 fc2 7200VXR/NPE-G2/VSA, 1GB system memory 3DES/HMAC-SHA or AES/HMAC-SHA, preshared with no IKE-keepalive configured

1. As measured with IPSec 3DES or AES Hashed Message Authentication Code (HMAC)-SHA-1 on 1400-byte packets. Performance varies depending on the number of modules, bandwidth, traffic volume, Cisco IOS software release, and so forth.
2. Using Cisco 12.4(4)XD3 fc2 image. Performance varies by Cisco IOS software release.

Supported Standards, MIBs, and RFCs

This section describes the standards, Management Information Bases (MIBs), and Request for Comments (RFCs) supported on the VSA. Requests for Comments (RFCs) contain information about the supported Internet suite of protocols.

Standards

- IPSec/IKE: RFCs 2401-2411, 2451

MIBs

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

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

- IPSec/IKE: RFCs 2401-2411, 2451

Enabling/Disabling the VSA

This section includes the following topics:

The VSA crypto card does not support OIR. The VSA boots up only during system initialization. The VSA will not work if it is inserted after the system is up and running. The VSA can be shut down by a disabling CLI command. The VSA is ready for removal after the disabling CLI command is executed.

Disabling the VSA during Operation

Before removing the VSA, we recommend that you shut down the interface so that there is no traffic running through the VSA when it is removed. Removing an VSA while traffic is flowing through the ports can cause system disruption.

Caution You could damage the VSA, if you remove the VSA without entering the CLI command.

To disable the C7200 VSA, use the following commands, starting in global configuration mode:

	Command	Purpose
Step 1	`no crypto engine [slot | accelerator] 0`	Disables the C7200 VSA.
Step 2	`crypto engine [slot | accelerator] 0`	Enables the C7200 VSA after it has been disabled. **Note** See Table 1-5 for more details.

Enabling/Disabling Scheme

This section describes how the VSA operates without OIR support.

Table 1-3 describes what occurs when the system boots up after power-on or after the reload command is entered.

Table 1-4 describes what occurs when the system is in run-time operation.

Table 1-5 describes what occurs when the **crypto engine** command is entered.

Table 1-3 System Boots Up After Power-on or After the reload Command is Entered

Condition	System Initialization
VSA is present	The VSA subsystem comes up and initializes automatically. Other crypto engines will be disabled.
VSA is not present	The VSA subsystem will not be initialized and system will use other crypto engine if exist.

Table 1-4 System is in Run-time Operation

Condition	System is Configured
Inserting the VSA	The VSA runs in power-off, but you need to perform a system reload or a reset to bring the VSA up.
CLI Enabling VSA	Not supported.
CLI Disabling VSA	**Hw-module slot 0 shutdown**—Not supported. **[no] crypto engine [slot | accelerator] 0**—See Table 1-5
Removing VSA	You must enter a disabling CLI (see Table 1-5) before removing the card to avoid damaging the hardware.

Table 1-5 crypto engine Command

Command	Description of VSA Behavior

`Crypto engine slot 0`
`Crypto engine accelerator 0`
 	
Note The VSA can only be inserted in slot 0 (the I/O controller slot).
	This allows the VSA to come up and be registered as a crypto engine with the system.
	If you just performed this configuration and the VSA is currently disabled, reload or reset the system to bring the VSA up.
	Note The current crypto engine will be still running, and the VSA will take over after the next system reboot.

`No crypto engine slot 0` `No crypto engine accelerator 0`	These CLIs will disable the VSA. This is a configuration setting, so the VSA will remain disabled until you remove this configuration and system reloads or resets.

LEDs

The VSA has one LED, as shown in Figure 1-3.

Figure 1-3 VSA LED

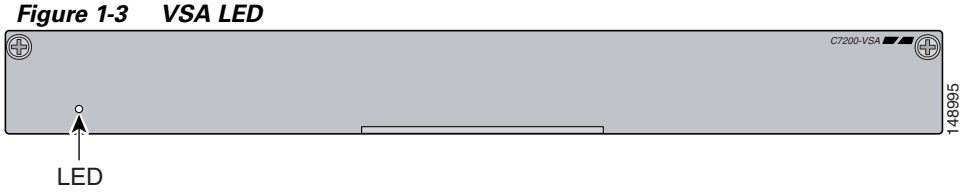


Table 1-6 VSA LED

Color	State	Function
No color	Off	Indicates that the VSA is disabled.
Green	On	Indicates the VSA is powered up and enabled for operation.
Amber	On	Indicates VSA is booting or has encountered errors.
Yellow	Powering Up	Indicates that the VSA is powering up, but software initialization has not started yet.

The following conditions must be met before the enabled LED goes on:

- The VSA is correctly connected to the backplane and receiving power.
- The system bus recognizes the VSA.

If either of these conditions is not met, or if the router initialization fails for other reasons, the enabled LED does not go on.

Connectors

See Figure 1-2 for the VSA connectors.

Slot Locations

This section includes the following topics:

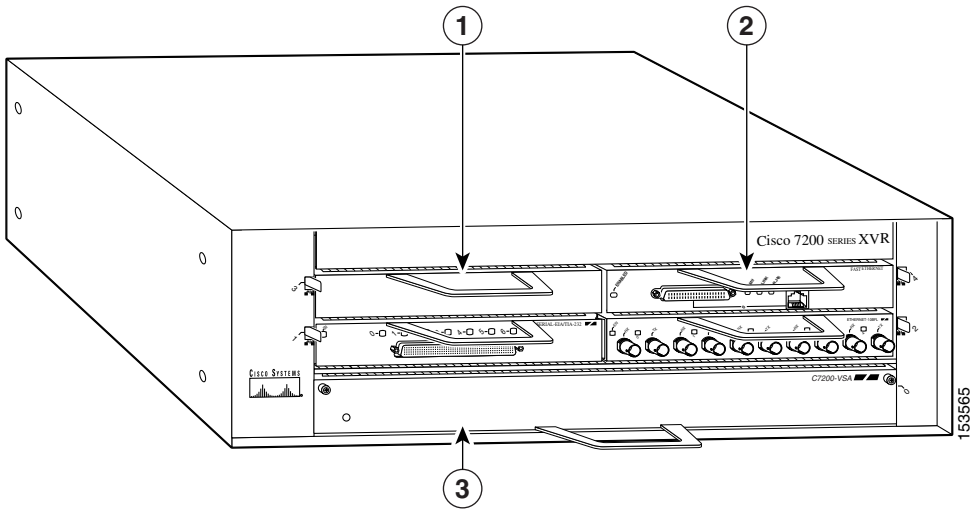
See Figure 1-4 for the slot numbering for the Cisco 7204VXR router.

See Figure 1-5 for the slot numbering for the Cisco 7206VXR router.

Cisco 7204VXR Router

The VSA is supported in the I/O controller port on the Cisco 7204VXR router (see 3 in Figure 1-4).

Figure 1-4 Cisco 7204VXR Router - Front View

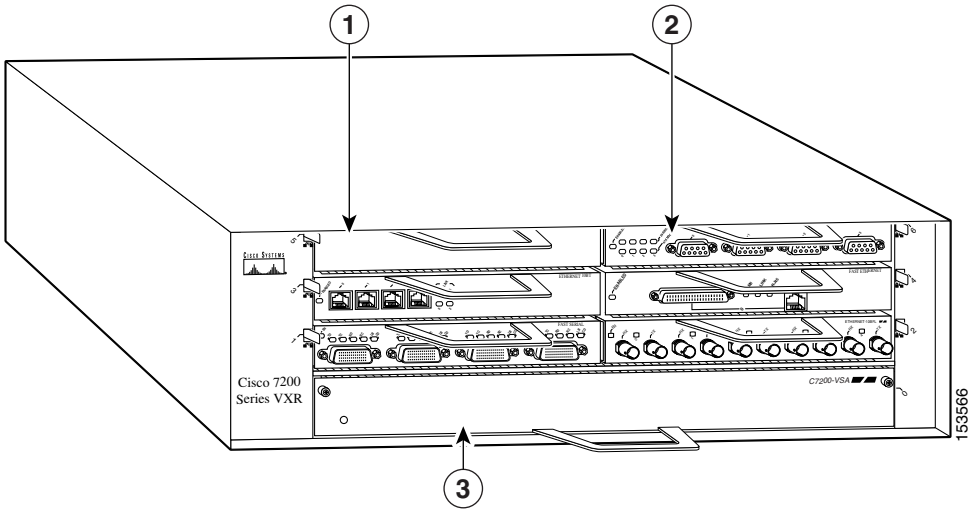


1	Port adapter	**3**	VSA in I/O controller slot
2	Port adapter lever		

Cisco 7206VXR Router

The VSA is supported in the I/O controller port on the Cisco 7206VXR router (see 4 in Figure 1-5).

Figure 1-5 Cisco 7206VXR - Front View



1	Blank port adapter	**3**	VSA in the I/O controller slot
2	Port adapter		

Preparing for Installation

This chapter describes the general equipment, safety, and site preparation requirements for installing the C7200 VSA (VPN Services Adapter). This chapter contains the following sections:

Required Tools and Equipment

You need the following tools and parts to install a VSA. If you need additional equipment, contact a service representative for ordering information.

- VSA
- Number 2 Phillips screwdriver
- Your own electrostatic discharge (ESD)-prevention equipment or the disposable grounding wrist strap included with all upgrade kits, field-replaceable units (FRUs), and spares
- Antistatic mat
- Antistatic container

Hardware and Software Requirements

This section describes the minimum software and hardware requirements for the VSA:

Software Requirements

Table 2-1 lists the recommended minimum Cisco IOS software release required to use the VSA in supported router or switch platforms. Use the **show version** command to display the system software version that is currently loaded and running.

Table 2-1 VSA Software Requirements

Platform	Recommended Minimum Cisco IOS Release
Cisco 7204VXR Cisco 7206VXR	12.4(4)XD3 fc2

To check the minimum software requirements of Cisco IOS software with the hardware installed on your router, Cisco maintains the Software Advisor tool on Cisco.com. Registered Cisco Direct users can access the Software Advisor at: http://www.cisco.com/cgi-bin/Support/CompNav/Index.pl. This tool does not verify whether modules within a system are compatible, but it does provide the minimum Cisco IOS software requirements for individual hardware modules or components.

Note Access to this tool is limited to users with Cisco.com login accounts.

Hardware Requirements

The hardware required to ensure proper operation of the VSA is as follows:

- The VSA is compatible with the Cisco NPE-G2 processor on the Cisco 7204VXR or Cisco 7206VXR routers.

  The Cisco NPE-G2 is the latest routing engine for the Cisco 7204VXR and 7206VXR, which provides the highest performance and scalability within the family of network processing engines (NPEs).
- ROMmon requirement—12.4(4r)XD5
- I/O FPGA requirement—0x25 (decimal 0.37)
- VSA FPGA requirement—0x13 (decimal 0.19)

Restrictions

The VSA has the following restrictions:

- VSA does not interoperate with other ISA or VAM/VAM2/VAM2+ crypto cards in the same router. The VAM/VAM2/VAM2+ crypto cards are disabled when the VSA is active in the Cisco 7200VXR series routers with the NPE-G2 processor.
- Only a single VSA card is supported on the Cisco 7200VXR series routers with the NPE-G2 processor.

Note Only Cisco 7200VXR series routers with the NPE-G2 processor are supported.

- The VSA module does not support Online Insertion and Removal (OIR). See "Enabling/Disabling the VSA" section on page 1-6 for details.
- Per packet count details for crypto map ACL are not displayed when the **show access-list** command is entered.

  Use other counters, such as the output from the **show crypto ipsec sa** and **show crypto engine accelerator statistics 0** commands, to determine if the VSA is processing the packets.
- An anti-replay window size of 1024 is not supported.

Online Insertion and Removal (OIR)

The VSA plugs into the I/O controller slot of the Cisco 7200VXR series chassis. The VSA crypto card does not support OIR. The VSA boots up only during system initialization. The VSA will not work if it is inserted after the system is up and running. The VSA can be shut down by a disabling CLI command (see "Enabling/Disabling the VSA" section on page 1-6). The VSA is ready for removal after the disabling CLI command is executed.

Caution You could damage the VSA, if you remove the VSA without entering the CLI command.

Before removing the VSA, we recommend that you shut down the interface so that there is no traffic running through the VSA when it is removed. Removing an VSA while traffic is flowing through the ports can cause system disruption.

For more information on OIR, go to "Enabling/Disabling the VSA" section on page 1-6.

Safety Guidelines

This section provides safety guidelines that you should follow when working with any equipment that connects to electrical power or telephone wiring. This section includes the following topics:

Safety Warnings

Safety warnings appear throughout this publication in procedures that, if performed incorrectly, might harm you. A warning symbol precedes each warning statement.

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.**

Hazardous voltage or energy is present on the backplane when the system is operating. Use caution when servicing.

Blank faceplates and cover panels serve three important functions: they prevent exposure to

hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.

Electrical Equipment Guidelines

Follow these basic guidelines when working with any electrical equipment:

- Before beginning any procedures requiring access to the chassis interior, locate the emergency power-off switch for the room in which you are working.
- Disconnect all power and external cables before moving a chassis; do not work alone when potentially hazardous conditions exist.
- Never assume that power has been disconnected from a circuit; always check.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe; carefully examine your work area for possible hazards such as moist floors, ungrounded power extension cables, and missing safety grounds.

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) damage, which can occur when electronic cards or components are improperly handled, results in complete or intermittent failures. Port adapters and processor modules comprise printed circuit boards that are fixed in metal carriers. Electromagnetic interference (EMI) shielding and connectors are integral components of the carrier. Although the metal carrier helps to protect the board from ESD, use a preventive antistatic strap during handling.

Following are guidelines for preventing ESD damage:

- Always use an ESD wrist or ankle strap and ensure that it makes good skin contact.
- Connect the equipment end of the strap to an unfinished chassis surface.
- When installing a component, use any available ejector levers or captive installation screws to properly seat the bus connectors in the backplane or midplane. These devices prevent accidental removal, provide proper grounding for the system, and help to ensure that bus connectors are properly seated.
- When removing a component, use any available ejector levers or captive installation screws to release the bus connectors from the backplane or midplane.
- Handle carriers by available handles or edges only; avoid touching the printed circuit boards or connectors.
- Place a removed board component-side-up on an antistatic surface or in a static shielding container. If you plan to return the component to the factory, immediately place it in a static shielding container.
- Avoid contact between the printed circuit boards and clothing. The wrist strap only protects components from ESD voltages on the body; ESD voltages on clothing can still cause damage.
- Never attempt to remove the printed circuit board from the metal carrier.
- For safety, periodically check the resistance value of the antistatic strap. The measurement should be between 1 and 10 Mohm.

Compliance with U.S. Export Laws and Regulations Regarding Encryption

This product performs encryption and is regulated for export by the U.S. government. Persons exporting any item out of the United States by either physical or electronic means must comply with the Export Administration Regulations as administered by the U.S. Department of Commerce, Bureau of Export Administration. See http://www.bxa.doc.gov/ for more information.

Certain “strong” encryption items can be exported outside the United States depending upon the destination, end user, and end use. See http://www.cisco.com/wwl/export/encrypt.html for more information about Cisco-eligible products, destinations, end users, and end uses.

Check local country laws prior to export to determine import and usage requirements as necessary. See http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm as one possible, unofficial source of international encryption laws.

CHAPTER 3

Removing and Installing the VSA

This chapter describes how to remove the C7200 VSA (VPN Services Adapter) from the supported platforms and how to install a new or replacement VSA.

Before you begin installation, read Chapter 2, "Preparing for Installation" for a list of parts and tools required for installation.

This chapter contains the following sections:

Note A system without an I/O controller or VSA, should have an empty slot to maintain the air flow.

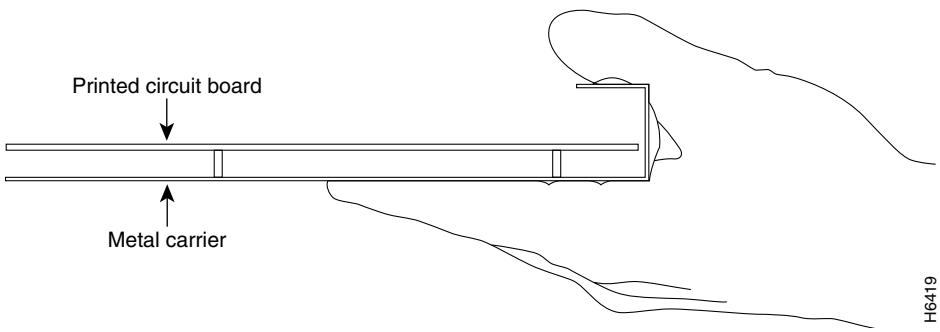
The VSA circuit board is sensitive to ESD damage.

Handling the VSA

The VSA is a double-width circuit board mounted on a metal carrier. (see Figure 3-1).

Caution Always handle the VSA by the carrier edges and handle; never touch the VSA components or connector pins. (See Figure 3-1.)

Figure 3-1 Handling the VSA



Online Insertion and Removal (OIR)

The VSA plugs into the I/O controller slot of the Cisco 7200VXR series chassis. The VSA crypto card does not support OIR. The VSA boots up only during system initialization. The VSA will not work if it is inserted after the system is up and running. The VSA can be shut down by a disabling CLI command (see "Enabling/Disabling the VSA" section on page 1-6). The VSA is ready for removal after the disabling CLI command is executed.

Caution You could damage the VSA, if you remove the VSA without entering the CLI command.

For more information on OIR, go to "Enabling/Disabling the VSA" section on page 1-6.

Warnings and Cautions

Observe the following warnings and cautions when installing or removing the VSA.

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.**

The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.

Warning **Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.**

Keep hands and fingers out of the power supply bays. High voltage is present on the power backplane when the system is running.

VSA Removal and Installation

This section describes how to remove and install the VSA.

Warning **When performing the following procedures, wear a grounding wrist strap to avoid ESD damage to the card. Some platforms have an ESD connector for attaching the wrist strap. Do not directly touch the midplane or backplane with your hand or any metal tool, or you could shock yourself.**

Note After powering off the router, wait at least 30 seconds before powering it on again.

Follow these steps to remove and insert the VSA in the Cisco 7200VXR series routers:

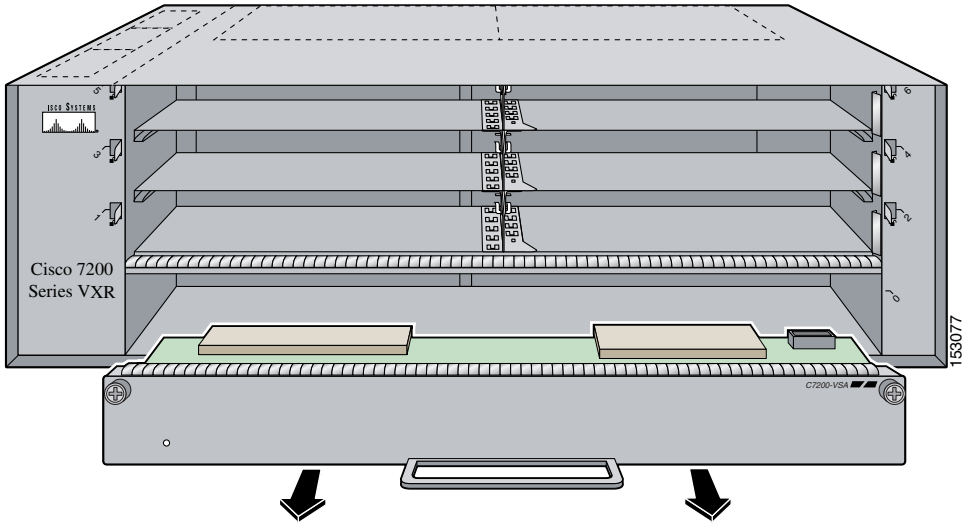
Step 1 Turn the power switch to the off position and then remove the power cable. (Optional on Cisco 7200VXR series routers; see Warnings and Cautions, page 3-2, above.)

Step 2 Attach an ESD wrist strap between you and an unpainted chassis surface.

Step 3 Unscrew the screws holding the VSA in the slot.

Step 4 Grasp the handle of the VSA and pull the VSA from the router (see Figure 3-2).

Figure 3-2 Cisco 7206VXR Chassis Shown - Removing VSA from I/O Controller Slot



Step 5 Carefully align the new VSA carrier between the upper and the lower edges of the I/O controller slot.

Caution To prevent jamming the carrier between the upper and the lower edges of the I/O controller slot, and to ensure that the edge connector at the rear of the VSA mates with the connection at the rear of the I/O controller slot, make certain that the carrier is positioned correctly, as shown in Figure 3-2.

Step 6 Slide the new VSA into the I/O controller slot until it is seated in the router midplane.

Caution Do not allow the VSA components to come in contact with the system board or the VSA could be damaged.

If you are removing, but not replacing a VSA, insert a blank service adapter filler in the unoccupied I/O controller slot, to ensure the proper flow of cooling air across the internal components.

Step 7 Reattach the power cable, and place the cable through any cable support brackets.

Step 8 Power on the router by turning the power switch to the on position.

This completes the removal and installation procedure of the VSA from the Cisco 7200VXR series routers.

Configuring the VSA

This chapter contains the information and procedures needed to configure the C7200-VSA (VPN Services Adapter). This chapter contains the following sections:

Overview

The VSA in the I/O controller slot provides encryption services for the I/O controller port in the Cisco 7204VXR or Cisco 7206VXR router with a NPE-G2 processor. If you have previously configured IPSec on the router and you install a VSA, the VSA automatically performs encryption services.

Note The Cisco 7204VXR and the 7206VXR routers support a single VSA.

There are no interfaces to configure on the VSA.

This section only contains basic configuration information for enabling encryption and IPSec tunneling services. Refer to the "IP Security and Encryption" part of the *Security Configuration Guide* and the *Security Command Reference* guide for detailed configuration information on IPSec, IKE, and CA.

Configuration Tasks

On power up, the VSA is fully functional and does not require any configuration commands. However, for the VSA to provide encryption services, you must complete the steps in the following sections:

- Using the EXEC Command Interpreter, page 4-2 (required)
- Configuring an IKE Policy, page 4-2 (required)
- Configuring a Transform Set, page 4-4 (required)
- Configuring IPSec, page 4-8 (required)

- Disabling VSA (Optional), page 4-4 (optional)
- Verifying IKE and IPSec Configurations, page 4-15 (optional)
- Configuring IPSec Configuration Example, page 4-18 (optional)

Note You can configure a static crypto map, create a dynamic crypto map, or add a dynamic crypto map into a static crypto map. Refer to the configuration examples and tech notes located online at: http://www.cisco.com/en/US/products/sw/secursw/ps2308/prod_configuration_examples_list.html.

Optionally, you can configure certification authority (CA) interoperability (refer to the "Configuring Certification Authority Interoperability" chapter in the *Security Configuration Guide*).

Using the EXEC Command Interpreter

You modify the configuration of your router through the software command interpreter called the *EXEC* (also called enable mode). You must enter the privileged level of the EXEC command interpreter with the **enable** command before you can use the **configure** command to configure a new interface or change the existing configuration of an interface. The system prompts you for a password if one has been set.

The system prompt for the privileged level ends with a pound sign (#) instead of an angle bracket (>). At the console terminal, use the following procedure to enter the privileged level:

Step 1 At the user-level EXEC prompt, enter the **enable** command. The EXEC prompts you for a privileged-level password as follows:

```
Router> enable

Password:
```

Step 2 Enter the password (the password is case sensitive). For security purposes, the password is not displayed. When you enter the correct password, the system displays the privileged-level system prompt (#):

```
Router#
```

This completes the procedure for entering the privileged level of the EXEC command interpreter.

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:

	Command	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 128 | aes 192 | aes 256}`	Specifies the encryption algorithm within an IKE policy. • **des**—Specifies 56-bit DES as the encryption algorithm. • **3des**—Specifies 168-bit DES as the encryption algorithm. • **aes**—Specifies 128-bit AES as the encryption algorithm. • **aes 128**—Specifies 128-bit AES as the encryption algorithm. • **aes 192**—Specifies 192-bit AES as the encryption algorithm. • **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. • **rsa-sig**—Specifies Rivest, Shamir, and Adelman (RSA) signatures as the authentication method. • **rsa-encr**—Specifies RSA encrypted nonces as the authentication method. • **pre-share**—Specifies preshared keys as the authentication method. **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). *seconds*—Number of seconds that each SA should exist before expiring. Use an integer from 60 to 86,400 seconds. **Note** If this command is not enabled, the default value (86,400 seconds [one day]) will be used.

	Command	Purpose
Step 5	`Router(config-isakmp)# hash {sha | md5}`	(Optional) Specifies the hash algorithm within an IKE policy. • **sha**—Specifies SHA-1 (HMAC variant) as the hash algorithm. • **md5**—Specifies MD5 (HMAC variant) as the hash algorithm. **Note** If this command is not enabled, the default value (**sha**) will be used.
Step 6	`Router(config-isakmp)# group {1 | 2 | 5}`	(Optional) Specifies the Diffie-Hellman (DH) group identifier within an IKE policy. **1**—Specifies the 768-bit DH group. **2**—Specifies the 1024-bit DH group. **5**—Specifies the 1536-bit DH group. **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 Security Protocol" chapter in the *Security Configuration Guide* publication.

Disabling VSA (Optional)

The VSA is enabled by default.

To disable the VSA, use the following commands, starting in global configuration mode:

	Command	Purpose
Step 7	`no crypto engine [slot | accelerator] 0` **Note** The VSA can only be inserted in slot 0.	Disables VSA.
Step 8	`crypto engine [slot | accelerator] 0`	VSA will be enabled after the next system reboot.

This completes the procedure for disabling and preparing to enable VSA after the next system reboot.

Configuring a Transform Set

See the *Advanced Encryption Standard (AES)* feature module for more information on configuring a transform set.

This section includes the following topics:

- Defining a Transform Set
- IPSec Protocols: AH and ESP

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPSec protected traffic. During the IPSec security association (SA) negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

Defining a Transform Set

A transform set is a combination of security protocols and algorithms. During the IPSec security association negotiation, peers agree to use a specific transform set to protect a particular data flow.

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

Note The **clear** commands in Step 4 below are in EXEC or enable mode (see "Using the EXEC Command Interpreter" section on page 4-2 for more details).

	Command	Purpose
Step 1	`Router(config)# crypto ipsec transform-set` *transform-set-name transform1* `[`*transform2* `[`*transform3*`]]`	Defines a transform set and enters crypto transform configuration mode. • *transform-set-name*—Specifies the name of the transform set to create (or modify). • *transform1* [*transform2* [*transform3*] [*transform4*]]—Defines the IPSec security protocols and algorithms. Accepted transform values are described in Table 4-1.
Step 2	`Router(cfg-crypto-tran)# mode [tunnel | transport]`	(Optional) Changes the mode associated with the transform set. The mode setting is only applicable 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.)

Step 4	`Router# clear crypto sa`
	or
	`Router# clear crypto sa peer {`*ip-address* `|` *peer-name*`}`
	or
	`Router# clear crypto sa map` *map-name*
	or
	`Router# 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.)
		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 **spi** keywords to clear out only a subset of the SA database.

Table 4-1shows allowed transform combinations for the AH and ESP protocols.

Table 4-1 Allowed Transform Combinations

Transform type	Transform	Description
AH Transform (Pick up to one.)	**ah-md5-hmac**	AH with the MD5 (Message Digest 5) (HMAC variant) authentication algorithm
	ah-sha-hmac	AH with the SHA (Secure Hash Algorithm) (HMAC variant) authentication algorithm
ESP Encryption Transform (Note: If an **ESP Authentication Transform** is used, you must pick one.)	**esp-aes**	ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithm
	esp-aes 128	ESP with the 128-bit AES encryption algorithm
	esp-aes 192	ESP with the 192-bit AES encryption algorithm
	esp-aes 256	ESP with the 256-bit AES encryption algorithm
	esp-des	ESP with the 56-bit Data Encryption Standard (DES) encryption algorithm
	esp-3des	ESP with the 168-bit DES encryption algorithm (3DES or Triple DES)
	esp-null	Null encryption algorithm
ESP Authentication Transform (Pick up to one.)	**esp-md5-hmac**	ESP with the MD5 (HMAC variant) authentication algorithm
	esp-sha-hmac	ESP with the SHA (HMAC variant) authentication algorithm

Examples of acceptable transform combinations are as follows:

- **ah-md5-hmac**
- **esp-des**
- **esp-3des** and **esp-md5-hmac**
- **ah-sha-hmac** and **esp-des** and **esp-sha-hmac**

The parser will prevent you from entering invalid combinations; for example, once you specify an AH transform it will not allow you to specify another AH transform for the current transform set.

IPSec Protocols: AH and ESP

Both the AH and ESP protocols implement security services for IPSec.

AH provides data authentication and antireplay services.

ESP provides packet encryption and optional data authentication and antireplay services.

ESP encapsulates the protected data—either a full IP datagram (or only the payload)—with an ESP header and an ESP trailer. AH is embedded in the protected data; it inserts an AH header immediately after the outer IP header and before the inner IP datagram or payload. Traffic that originates and terminates at the IPSec peers can be sent in either tunnel or transport mode; all other traffic is sent in tunnel mode. Tunnel mode encapsulates and protects a full IP datagram, while transport mode encapsulates/protects the payload of an IP datagram. For more information about modes, refer to the **mode (IPSec)** command description.

Selecting Appropriate Transforms

The following tips may help you select transforms that are appropriate for your situation:

- If you want to provide data confidentiality, include an ESP encryption transform.
- If you want to ensure data authentication for the outer IP header as well as the data, include an AH transform. (Some consider the benefits of outer IP header data integrity to be debatable.)
- If you use an ESP encryption transform, also consider including an ESP authentication transform or an AH transform to provide authentication services for the transform set.
- If you want data authentication (either using ESP or AH) you can choose from the MD5 or SHA (HMAC keyed hash variants) authentication algorithms. The SHA algorithm is generally considered stronger than MD5 but is slightly slower.
- Note that some transforms might not be supported by the IPSec peer.

Note If a user enters an IPSec transform that the hardware (the IPSec peer) does not support, a warning message will be displayed immediately after the **crypto ipsec transform-set** command is entered.

- In cases where you need to specify an encryption transform but do not actually encrypt packets, you can use the **esp-null** transform.

Suggested transform combinations follow:

- **esp-aes** and **esp-sha-hmac**
- **ah-sha-hmac** and **esp-aes** and **esp-sha-hmac**

The Crypto Transform Configuration Mode

After you issue the **crypto ipsec transform-set** command, you are put into the crypto transform configuration mode. While in this mode, you can change the mode to tunnel or transport. (These are optional changes.) After you have made these changes, type **exit** to return to global configuration mode. For more information about these optional changes, refer to the **match address** (IPSec) and **mode** (IPSec) command descriptions.

Changing Existing Transforms

If one or more transforms are specified in the **crypto ipsec transform-set** command for an existing transform set, the specified transforms will replace the existing transforms for that transform set.

If you change a transform set definition, the change is only applied to crypto map entries that reference the transform set. The change will not be applied to existing SAs, but will be used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, you can clear all or part of the SA database by using the **clear crypto sa** command.

Transform Example

The following example defines two transform sets. The first transform set will be used with an IPSec peer that supports the newer ESP and AH protocols. The second transform set will be used with an IPSec peer that only supports the older transforms.

```
crypto ipsec transform-set newer esp-3des esp-sha-hmac
crypto ipsec transform-set older ah-rfc-1828 esp-rfc1829
```

Configuring IPSec

This section includes the following topics:

- Ensuring That Access Lists Are Compatible with IPSec (required)
- Setting Global Lifetimes for IPSec Security Associations (required)
- Creating Crypto Access Lists (required)
- Creating Crypto Map Entries (required)
- Creating Dynamic Crypto Maps (required)
- Applying Crypto Map Sets to Interfaces (required)
- Verifying the Configuration (optional)

For IPSec configuration examples, refer to the "Configuring IPSec Configuration Example" section on page 4-18.

See the "Configuring IPSec Network Security" of the *Cisco IOS Security Configuration Guide* for more information on configuring IPSec.

Ensuring That Access Lists Are Compatible with IPSec

IKE uses UDP port 500. The IPSec Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols use protocol numbers 50 and 51. Ensure that your interface access lists are configured so that protocol numbers 50, 51, and UDP port 500 traffic are not blocked at interfaces used by IPSec. In some cases you might need to add a statement to your access lists to explicitly permit this traffic.

Setting Global Lifetimes for IPSec Security Associations

You can change the global lifetime values which are used when negotiating new IPSec security associations. (These global lifetime values can be overridden for a particular crypto map entry).

These lifetimes only apply to security associations established via IKE. Manually established security associations do not expire.

To change a global lifetime for IPSec security associations, use one or more of the following commands:

Note The **clear** commands in Step 5 below are in EXEC or enable mode (see "Using the EXEC Command Interpreter" section on page 4-2 for more details).

Step	Command	Purpose
Step 1	`Router# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# crypto ipsec security-association lifetime seconds` *seconds*	Changes global lifetime values used when negotiating IPSec security associations (SAs). To reset a lifetime to the default value, use the no form of this command. Specifies the number of seconds a security association will live before expiring. The default is 3600 seconds (one hour).
Step 4	`Router(config)# crypto ipsec security-association lifetime kilobytes` *kilobytes*	Changes the global "traffic-volume" lifetime for IPSec SAs. Specifies the volume of traffic (in kilobytes) that can pass between IPSec peers using a given security association before that security association expires. The default is 4,608,000 kilobytes.

Step 5	`Router# clear crypto sa`
	or
	`Router# clear crypto sa peer {`*ip-address* `|` *peer-name*`}`
	or
	`Router# clear crypto sa map` *map-name*
	or
	`Router# clear crypto sa spi` *destination-address protocol spi*
		(Optional) Clears existing security associations. This causes any existing security associations to expire immediately; future security associations will use the new lifetimes. Otherwise, any existing security associations will expire according to the previously configured lifetimes.
		Note Using the **clear crypto sa** command without parameters will clear out the full SA database, which will clear out active security sessions. You may also specify the **peer**, **map**, or **spi** keywords to clear out only a subset of the SA database. For more information, see the **clear crypto sa** command.

Creating Crypto Access Lists

Crypto access lists define which IP traffic will be protected by encryption. (These access lists are *not* the same as regular access lists, which determine what traffic to forward or block at an interface.) For example, access lists can be created to protect all IP traffic between Subnet A and Subnet Y or Telnet traffic between Host A and Host B.

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

Step	Command	Purpose

Step 1	`Router(config)# access-list access-list-number {deny | permit} protocol source source-wildcard destination destination-wildcard [log]`
	or
	`Router(config)# ip access-list extended name`
		Specifies conditions to determine which IP packets will be protected.[1] (Enable or disable crypto for traffic that matches these conditions.)
		We recommend that you configure "mirror image" crypto access lists for use by IPSec and that you avoid using the **any** keyword.

Step 2	Add **permit** and **deny** statements as appropriate.	Adds permit or deny statements to access lists.
Step 3	`End`	Exits the configuration command mode.

1. 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.

For detailed information on configuring access lists, refer to the "Configuring IPSec Network Security" chapter in the *Security Configuration Guide* publication.

Creating Crypto Map Entries

You can apply only one crypto map set to a single interface. The crypto map set can include a combination of IPSec/IKE and IPSec/manual entries. Multiple interfaces can share the same crypto map set if you want to apply the same policy to multiple interfaces.

To create crypto map entries that do not use IKE to establish the security associations, use the following commands, starting in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# crypto map map-name seq-num ipsec-manual`	Specifies the crypto map entry to create (or modify). This command puts you into the crypto map configuration mode.
Step 2	`Router(config-crypto-m)# match address access-list-id`	Names an IPSec access list. This access list determines which traffic should be protected by IPSec and which traffic should not be protected by IPSec security in the context of this crypto map entry. (The access list can specify only one **permit** entry when IKE is not used.)
Step 3	`Router(config-crypto-m)# set peer {hostname | ip-address}`	Specifies the remote IPSec peer. This is the peer to which IPSec protected traffic should be forwarded. (Only one peer can be specified when IKE is not used.)

	Command	Purpose
Step 4	`Router(config-crypto-m)# set transform-set transform-set-name`	Specifies which transform set should be used. This must be the same transform set that is specified in the corresponding crypto map entry on the remote peer . (Only one transform set can be specified when IKE is not used.)

Step 5	`Router(config-crypto-m)# set session-key inbound ah spi hex-key-string`
	and
	`Router(config-crypto-m)# set session-key outbound ah spi hex-key-string`
		Sets the AH Security Parameter Indexes (SPIs) and keys to apply to inbound and outbound protected traffic if the specified transform set includes the AH protocol.
		(This manually specifies the AH security association to be used with protected traffic.)

Step 6	`Router(config-crypto-m)# set session-key inbound esp spi cipher hex-key-string [authenticator hex-key-string]`
	and
	`Router(config-crypto-m)# set session-key outbound esp spi cipher hex-key-string [authenticator hex-key-string]`
		Sets the ESP Security Parameter Indexes (SPIs) and keys to apply to inbound and outbound protected traffic if the specified transform set includes the ESP protocol. Specifies the cipher keys if the transform set includes an ESP cipher algorithm. Specifies the authenticator keys if the transform set includes an ESP authenticator algorithm.
		(This manually specifies the ESP security association to be used with protected traffic.)

Step 7	`Router(config-crypto-m)# exit`	Exits crypto-map configuration mode and return to global configuration mode.

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

	Command	Purpose
Step 1	`Router(config)# crypto map map-name seq-num ipsec-isakmp`	Names the crypto map entry to create (or modify). This command puts you into the crypto map configuration mode.
Step 2	`Router(config-crypto-m)# match address access-list-id`	Names an extended access list. This access list determines which traffic should be protected by IPSec and which traffic should not be protected by IPSec security in the context of this crypto map entry.
Step 3	`Router(config-crypto-m)# set peer {hostname | ip-address}`	Specifies a remote IPSec peer. This is the peer to which IPSec protected traffic can be forwarded. Repeat for multiple remote peers.
Step 4	`Router(config-crypto-m)# set transform-set transform-set-name1 [transform-set-name2...transform-set-name6]`	Specifies which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first).

	Command	Purpose

Step 5	`Router(config-crypto-m)# set security-association lifetime seconds seconds`
	and
	`Router (config-crypto-m)# set security-association lifetime kilobytes kilobytes`
		(Optional) Specifies a security association lifetime for the crypto map entry.
		Use this command if you want the security associations for this crypto map entry to be negotiated using different IPSec security association lifetimes than the global lifetimes.

Step 6	`Router(config-crypto-m)# set security-association level per-host`	(Optional) Specifies that separate security associations should be established for each source/destination host pair. Without this command, a single IPSec "tunnel" could carry traffic for multiple source hosts and multiple destination hosts. With this command, when the router requests new security associations it will establish one set for traffic between Host A and Host B, and a separate set for traffic between Host A and Host C. Use this command with care, as multiple streams between given subnets can rapidly consume resources.
Step 7	`Router(config-crypto-m)# set pfs [group1 | group2 | group5]`	(Optional) Specifies that IPSec should ask for perfect forward secrecy when requesting new security associations for this crypto map entry, or should demand perfect forward secrecy (PFS) in requests received from the IPSec peer.
Step 8	`Router(config-crypto-m)# exit`	Exits crypto-map configuration mode and returns to global configuration mode.

Creating Dynamic Crypto Maps

A dynamic crypto map entry is a crypto map entry with some parameters not configured.The missing parameters are later dynamically configured (as the result of an IPSec negotiation). Dynamic crypto maps are only available for use by IKE.

Dynamic crypto map entries are grouped into sets. A set is a group of dynamic crypto map entries all with the same *dynamic-map-name*, each with a different *dynamic-seq-num*.

To create a dynamic crypto map entry, use the following commands starting in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# crypto dynamic-map dynamic-map-name dynamic-seq-num`	Creates a dynamic crypto map entry.
Step 2	`Router(config-crypto-m)# set transform-set transform-set-name1 [transform-set-name2...transform-set-name6]`	Specifies which transform sets are allowed for the crypto map entry. List multiple transform sets in order of priority (highest priority first). This is the only configuration statement required in dynamic crypto map entries.

	Command	Purpose
Step 3	`Router(config-crypto-m)# match address` *access-list-id*	(Optional) Accesses list number or name of an extended access list. This access list determines which traffic should be protected by IPSec and which traffic should not be protected by IPSec security in the context of this crypto map entry. **Note** Although access-lists are optional for dynamic crypto maps, they are highly recommended. If this is configured, the data flow identity proposed by the IPSec peer must fall within a **permit** statement for this crypto access list. If this is not configured, the router will accept any data flow identity proposed by the IPSec peer. However, if this is configured but the specified access list does not exist or is empty, the router will drop all packets. This is similar to static crypto maps because they also require that an access list be specified. Care must be taken if the **any** keyword is used in the access list, because the access list is used for packet filtering as well as for negotiation.
Step 4	`Router(config-crypto-m)# set peer` {*hostname* | *ip-address*}	(Optional) Specifies a remote IPSec peer. Repeat for multiple remote peers. This is rarely configured in dynamic crypto map entries. Dynamic crypto map entries are often used for unknown remote peers.
Step 5	`Router(config-crypto-m)# set security-association lifetime seconds` *seconds* and `Router (config-crypto-m)# set security-association lifetime kilobytes` *kilobytes*	(Optional) If you want the security associations for this crypto map to be negotiated using shorter IPSec security association lifetimes than the globally specified lifetimes, specify a key lifetime for the crypto map entry.
Step 6	`Router(config-crypto-m)# set pfs` [**group1** | **group2** | **group5**]	(Optional) Specifies that IPSec should ask for perfect forward secrecy when requesting new security associations for this crypto map entry or should demand perfect forward secrecy in requests received from the IPSec peer.
Step 7	`Router(config-crypto-m)# exit`	Exits crypto-map configuration mode and returns to global configuration mode.
Step 8	Repeat these steps to create additional crypto map entries as required.	

To add a dynamic crypto map set into a crypto map set, use the following command in global configuration mode:

Command	Purpose
`Router(config)# crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-name`	Adds a dynamic crypto map set to a static crypto map set.

Applying Crypto Map Sets to Interfaces

Apply a crypto map set to each interface through which IPSec traffic will flow. Crypto maps instruct the router to evaluate the interface traffic against the crypto map set and use the specified policy during connection or security association negotiation on behalf of traffic to be protected by crypto.

To apply a crypto map set to an interface, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# crypto map map-name`	Applies a crypto map set to an interface.

To specify redundant interfaces and name an identifying interface, use the following command in global configuration mode:

Command	Purpose
`Router(config)# crypto map map-name local-address interface-id`	Permits redundant interfaces to share the same crypto map, using the same local identity.

Monitoring and Maintaining IPSec

To clear (and reinitialize) IPSec security associations, use one of the following commands in EXEC or enable mode (see "Using the EXEC Command Interpreter" section on page 4-2 for more details):

Command	Purpose

`Router# clear crypto sa`
or
`Router# clear crypto sa counters`
or
`Router# clear crypto sa peer {ip-address | peer-name}`
or
`Router# clear crypto sa map map-name`
or
`Router# clear crypto sa spi destination-address protocol spi`
	Clears IPSec security associations.
	Note Using the **clear crypto sa** command without parameters will clear out the full SA database, which will clear out active security sessions. You may also specify the **peer**, **map**, or **spi** keywords to clear out only a subset of the SA database. For more information, see the **clear crypto sa** command.

To view information about your IPSec configuration, use one or more of the following commands in EXEC mode:

Command	Purpose
Router# **show crypto ipsec transform-set**	Displays your transform set configuration.
Router# **show crypto map** [**interface** *interface* | **tag** *map-name*]	Displays your crypto map configuration.
Router# **show crypto ipsec sa** [**map** *map-name* | **address** | **identity**] [**detail**]	Displays information about IPSec security associations.
Router# **show crypto dynamic-map** [**tag** *map-name*]	Displays information about dynamic crypto maps.
Router# **show crypto ipsec security-association lifetime**	Displays global security association lifetime values.

Verifying IKE and IPSec Configurations

To view information about your IPSec configurations, use the **show crypto ipsec transform-set** EXEC command.

Note If a user enters an IPSec transform that the hardware (the IPSec peer) does not support, a warning message will be displayed in the **show crypto ipsec transform-set** command output.

The following sample output from the **show crypto ipsec transform-set** command displays a warning message after a user tries to configure an IPSec transform that the hardware does not support:

```
Router# show crypto ipsec transform-set
Transform set transform-1:{esp-256-aes esp-md5-hmac}
   will negotiate = {Tunnel, },

WARNING:encryption hardware does not support transform
esp-aes 256 within IPSec transform transform-1
```

To view information about your IKE configurations, use **show crypto isakmp policy** EXEC command.

Note If a user enters an IKE encryption method that the hardware does not support, a warning message will be displayed in the **show crypto isakmp policy** output.

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
        encryption algorithm:  AES - Advanced Encryption Standard (256 bit keys).
WARNING:encryption hardware does not support the configured
encryption method for ISAKMP policy 1
        hash algorithm:        Secure Hash Standard
        authentication method: Pre-Shared Key
        Diffie-Hellman group:  #1 (768 bit)
        lifetime:              3600 seconds, no volume limit
```

Verifying the Configuration

Some configuration changes take effect only after subsequent security associations are negotiated. For the new settings to take effect immediately, clear the existing security associations.

To clear (and reinitialize) IPSec security associations, use one of the commands in Table 4-2 in EXEC or enable mode (see "Using the EXEC Command Interpreter" section on page 4-2 for more details):

Table 4-2 Commands to Clear IP Sec Security Associations

Command	Purpose
clear crypto sa or **clear crypto sa peer** {*ip-address* | *peer-name*} or **clear crypto sa map** *map-name* or **clear crypto sa spi** *destination-address protocol spi*	Clear IPSec security associations (SAs). 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 **spi** keywords to clear out only a subset of the SA database.

The following steps provide information on verifying your configurations:

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

```
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:

```
Router# show crypto map
Crypto Map: "router-alice" idb: Ethernet0 local address: 172.21.114.123
Crypto Map "router-alice" 10 ipsec-isakmp
        Peer = 172.21.114.67
        Extended IP access list 141
            access-list 141 permit ip
                source: addr = 172.21.114.123/0.0.0.0
                dest:   addr = 172.21.114.67/0.0.0.0
        Current peer: 172.21.114.67
        Security-association lifetime: 4608000 kilobytes/120 seconds
        PFS (Y/N): N
        Transform sets={t1,}
```

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

```
Router# show crypto ipsec sa
interface: Ethernet0
    Crypto map tag: router-alice, local addr. 172.21.114.123
   local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
```

```
   remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
    current_peer: 172.21.114.67
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
    #send errors 10, #recv errors 0
     local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
     path mtu 1500, media mtu 1500
     current outbound spi: 20890A6F
     inbound esp sas:
      spi: 0x257A1039(628756537)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 26, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     outbound esp sas:
      spi: 0x20890A6F(545852015)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 27, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
interface: Tunnel0
   Crypto map tag: router-alice, local addr. 172.21.114.123
   local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
   current_peer: 172.21.114.67
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
    #send errors 10, #recv errors 0
     local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
     path mtu 1500, media mtu 1500
     current outbound spi: 20890A6F
     inbound esp sas:
      spi: 0x257A1039(628756537)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 26, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     outbound esp sas:
      spi: 0x20890A6F(545852015)
        transform: esp-des esp-md5-hmac,
        in use settings ={Tunnel,}
        slot: 0, conn id: 27, crypto map: router-alice
        sa timing: remaining key lifetime (k/sec): (4607999/90)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
```

For a detailed description of the information displayed by the **show** commands, refer to the "IP Security and Encryption" chapter of the *Security Command Reference* publication.

Configuration Examples

This section provides the following configuration examples:

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 encryptions 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:

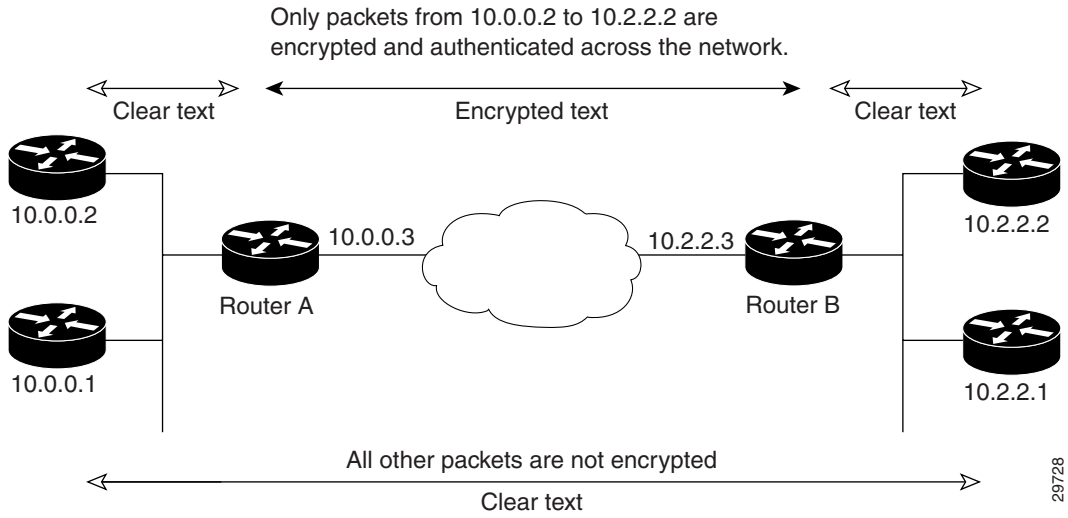
```
interface Serial0
 ip address 10.0.0.2
 crypto map toRemoteSite
```

Note In this example, IKE must be enabled.

Basic IPSec Configuration Illustration

The following is an example of an IPSec configuration in which the security associations are established through IKE. In this example, an access list is used to restrict the packets that are encrypted and decrypted. In this example, all packets going from IP address 10.0.0.2 to IP address 10.2.2.2 are encrypted and decrypted and all packets going from IP address 10.2.2.2 to IP address 10.0.0.2 are encrypted and decrypted. Also, one IKE policy is created.

Figure 4-1 Basic IPSec Configuration



Router A Configuration

Specify the parameters to be used during an IKE negotiation:

Update to 3DES/AES

```
crypto isakmp policy 15
  encryption des
  hash md5
  authentication pre-share
  group 2
  lifetime 5000

crypto isakmp key 1234567890 address 10.2.2.3
crypto isakmp identity address
```

Note In the preceding example, the encryption DES of policy 15 would not appear in the written configuration because this is the default value for the encryption algorithm parameter.

A transform set defines how the traffic will be protected:

```
crypto ipsec transform-set auth1 ah-md5-hmac esp-des esp-md5-hmac
  mode tunnel
```

Note In the preceding example, the mode tunnel would not appear in the written configuration because this is the default value for the transform-set.

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

```
crypto map toRemoteSite 10 ipsec-isakmp
match address 101
set peer 10.2.2.3
set transform-set auth1
```

The crypto map is applied to an interface:

```
  interface Serial0
  ip address 10.0.0.3
crypto map toRemoteSite
```

An IPSec access list defines which traffic to protect:

```
access-list 101 permit ip host 10.0.0.2 host 10.2.2.2
access-list 101 permit ip host 10.0.0.3 host 10.2.2.3
```

Router B Configuration

Specify the parameters to be used during an IKE negotiation:

```
crypto isakmp policy 15
  encryption des
  hash md5
  authentication pre-share
  group 2
  lifetime 5000

crypto isakmp key 1234567890 address 10.0.0.3
crypto isakmp identity address
```

A transform set defines how the traffic will be protected:

```
crypto ipsec transform-set auth1 ah-md5-hmac esp-des ah-md5-hmac
  mode tunnel
```

Note In the preceding example, the parameter “mode tunnel” would not appear in the written configuration because this is the default value for this configuration.

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

```
crypto map toRemoteSite 10 ipsec-isakmp
  match address 101
  set peer 10.0.0.3
  set transform-set auth1
```

The crypto map is applied to an interface:

```
interface Serial0
  ip address 10.2.2.3
  crypto map toRemoteSite
```

An IPSec access list defines which traffic to protect:

```
access-list 101 permit ip host 10.2.2.2 host 10.0.0.2
access-list 101 permit ip host 10.2.2.3 host 10.0.0.3
```

Troubleshooting Tips

To verify that Cisco IOS software has recognized the VSA, enter the **show diag** command and check the output. In the following example, the IOS software recognizes the C7200-VSA, which is found in slot 0 in the router.

```
Router# show diag 0
Slot 0:
        VSA IPsec Card Port adapter
        Port adapter is analyzed
        Port adapter insertion time 00:23:25 ago
        EEPROM contents at hardware discovery:
        PCB Serial Number        : PRTA4404055
        Product (FRU) Number     : C7200-VSA
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF C1 8B 50 52 54 41 34 34 30 34 30 35 35 40
          0x10: 05 0D CB 94 43 37 32 30 30 2D 56 53 41 20 20 20
          0x20: 20 20 20 20 20 20 20 20 D9 03 C1 40 CB FF FF FF
          0x30: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

To see if the VSA is currently processing crypto packets, enter the **show crypto engine accelerator statistic 0** command. The following is sample output:

```
Router# show crypto engine accelerator statistic 0

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

  Inbound rate: 0pps 0kb/s  Outbound rate: 0pps 0kb/s
  TXR0 PKT: 0x00000000000028B2  Byte: 0x000000000006ACF6  Full: 0x0000000000000000
  RXR0 PKT: 0x00000000000028B2  Byte: 0x0000000000A86398
  TXR1 PKT: 0x0000000000000000  Byte: 0x0000000000000000  Full: 0x0000000000000000
  RXR1 PKT: 0x0000000000000000  Byte: 0x0000000000000000
  TXR2 PKT: 0x0000000000000000  Byte: 0x0000000000000000  Full: 0x0000000000000000
  RXR2 PKT: 0x0000000000000000  Byte: 0x0000000000000000
  Inbound Traffic:
```

```
  Decrypted  PHY I/F:0x0000000000000000  TUNNEL I/F:    0x0000000000000000
  SPI Error  PHY I/F:0x0000000000000000  TUNNEL I/F:    0x0000000000000000
  Pass clear PHY I/F:0x0000000000000000  TUNNEL I/F:    0x0000000000000000
  SPD Drop:          0x0000000000000000  IKE Bypass:    0x0000000000000000
  Outbound Traffic:
  Encry CEF: 0x0000000000000000  FS: 0x0000000000000000  PROC: 0x0000000000000000
  Pass  CEF: 0x0000000000000000  FS: 0x0000000000000000  PROC: 0x0000000000000000
  ICMP Unreachable: 0x0000000000000000  ICMP Unreach Fail: 0x0000000000000000
  SPD Drop:  0x0000000000000000
  Special Traffic:
  VAM mode  PKT:     0x0000000000000000  Exception:     0x0000000000000000
  N2 Message:    :   0x00000000000028B2  Exception:     0x0000000000000000
  IP PKT Exception:  0x0000000000000000  DJ Overflow:   0x0000000000000000
  RAE Report PKT::   0x0000000000000000  PKT Consumed:  0x0000000000000000
  TCAM WR:           0x0000000000000001  TCAM RD:       0x0000000000000000
  SARAM WR:          0x0000000000008422  SARAM RD:      0x0000000000000000
  RAE WR:            0x0000000000080000  RAE RD:        0x0000000000000000
  Warnings:
  N2 interrupt:      0x0000000000000000  Invalid Op:    0x0000000000000000
  RX CTX error:      0x0000000000000000  TX CTX low:    0x0000000000000000
  PKT CTX Low:       0x0000000000000000  PKT Info Low:  0x0000000000000000
  PKT Header Low:    0x0000000000000000  Particle Low:  0x0000000000000000
  Missing SOP:       0x0000000000000000  Missing EOP:   0x0000000000000000
  TX Drop IB:        0x0000000000000000  TX Drop OB:    0x0000000000000000
  MSG Unknown:       0x0000000000000000  MSG too Big:   0x0000000000000000
  MSG Empty:         0x0000000000000000  MSG No Buffer: 0x0000000000000000
  PKT Info Missing:  0x0000000000000000  IB SB Error:   0x0000000000000000
  TX Drop Fastsend:  0x0000000000000000  IDMA Full:     0x0000000000000000
  Particle Fallback: 0x0000000000000000  STATISTIC:     0x0000000000000000

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

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

When the VSA processes packets, the “packets in” and “packets out” counter changes. Counter “packets out” represents the number of packets directed to the VSA. Counter “packets in” represents the number of packets received from the VSA.

To see if the IKE/IPSec packets are being redirected to the VSA for IKE negotiation and IPSec encryption and decryption, enter the **show crypto eli** command. The following is sample output when Cisco IOS software redirects packets to the VSA:

```
Router# show crypto eli
Hardware Encryption : ACTIVE
 Number of hardware crypto engines = 1

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

 IKE-Session   :     0 active,  5120 max, 0 failed
 DH            :     0 active,  5120 max, 0 failed
 IPSec-Session :     0 active, 10230 max, 0 failed
```

When the software crypto engine is active, the **show crypto eli** command yields no output.

When the Cisco IOS software agrees to redirect crypto traffic to the VSA, it prints a message similar to the following:

```
%ISA-6-INFO:Recognised crypto engine (0) at slot-0
    ...switching to hardware crypto engine
```

To disable the VSA, use the configuration mode **no crypto engine accelerator** <*slot*> command, as follows:

```
Router(config)# no crypto engine accelerator 0
...switching to SW crypto engine
Router(config)#
*Feb  6 11:57:26.763: %VPN_HW-6-INFO_LOC: Crypto engine: slot 0  State changed to:
Disabled
*Feb  6 11:57:26.779: %PA-3-DEACTIVATED: port adapter in bay [0] powered off.
*Feb  6 11:57:26.779: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
Router(config)#end
```

Monitoring and Maintaining the VSA

This section includes the following topics:

Using Deny Policies in Access Lists

Specifying a deny address range in an access list results in “jump” behavior. When a denied address range is hit, it forces the search to “jump” to the beginning of the access list associated with the next sequence on a crypto map and continue the search. If you want to pass clear traffic on these addresses, you must insert a deny address range for each sequence on a crypto map. In turn, each permit list of addresses inherits all the deny address ranges specified in the access list. A deny address range causes the software to do a subtraction of the deny address range from a permit list, and creates multiple permit address ranges that need to be programmed in hardware. This behavior can cause repeated address ranges to be programmed in the hardware for a single deny address range, resulting in multiple permit address ranges in a single access list.

The **crypto ipsec ipv4 deny-policy** {jump | clear | drop} command helps you avoid this problem. The clear keyword allows a deny address range to be programmed in hardware, the deny addresses are then filtered out for encryption and decryption. When a deny address is hit, the search is stopped and traffic is allowed to pass in the clear (unencrypted) state. The drop keyword causes traffic to be dropped when a deny address is hit. These two new keywords are used to prevent repeated address ranges from being programmed in the hardware, resulting in more efficient space utilization.

Configuration Guidelines and Restrictions

- The **crypto ipsec ipv4 deny-policy** {jump | clear | drop} command is a global command that can be applied to a VSA module. The specified keyword (jump, clear, or drop) is propagated to the ACE software of the VSA module. The default behavior is jump.
- If you apply the specified keyword (jump, clear, or drop) when crypto maps are already configured on the VSA module, all existing IPSec sessions are temporarily removed and restarted which impacts traffic on your network.
- The number of deny entries that can be specified in an access list are dependent on the keyword specified:
  - jump—Supports up to 8 deny entries in an access list
  - clear—Supports up to 1000 deny entries in an access list
  - drop—Supports up to 1000 deny entries in an access list

Monitor and Maintenance Commands

Use the commands that follow to monitor and maintain the VSA:

Command	Purpose
`Router# show crypto engine accelerator statistic 0`	Verifies the VSA is currently processing crypto packets.
`Router# Show version`	Displays integrated service adapter as part of the interfaces.

I

L

M

O

P

R

S

T

V

W