



VPN Acceleration Module 2+ (VAM2+) Installation and Configuration Guide

Product Number: SA-VAM2+(=)

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.

Americas 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: 408 527-0883

Text Part Number: OL-5979-03

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 NON-INFRINGEMENT 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.

 Printed in the USA on recycled paper containing 10% postconsumer waste.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Copyright © 2006 Cisco Systems, Inc.
All rights reserved.



CONTENTS

Preface	vii
Revision History	vii
Audience	viii
Warnings	viii
Objectives	viii
Organization	viii
Related Documentation	ix
Obtaining Documentation	x
Cisco.com	x
Product Documentation DVD	xi
Ordering Documentation	xi
Documentation Feedback	xi
Cisco Product Security Overview	xi
Reporting Security Problems in Cisco Products	xii
Obtaining Technical Assistance	xii
Cisco Technical Support & Documentation Website	xiii
Submitting a Service Request	xiii
Definitions of Service Request Severity	xiii
Obtaining Additional Publications and Information	xiv

CHAPTER 1

Overview	1-1
Data Encryption Overview	1-1
SA-VAM2+ Overview	1-3
Features	1-4
Performance	1-5
Supported Standards, MIBs, and RFCs	1-6
Standards	1-6
MIBs	1-6
RFCs	1-6
Online Insertion and Removal (OIR)	1-7
SA-VAM2+	1-7
Port Adapter Jacket Card	1-7

LEDs	1 - 7
SA-VAM2+	1 - 7
Port Adapter Jacket Card	1 - 8
Cables, Connectors, and Pinouts	1 - 8
Slot Locations	1 - 9
Cisco 7200VXR Routers	1 - 9
Cisco 7301 Router	1 - 9

CHAPTER 2

Preparing for Installation 2 - 1

Required Tools and Equipment	2 - 1
Hardware and Software Requirements	2 - 1
Software Requirements	2 - 2
Hardware Requirements	2 - 2
Restrictions	2 - 3
Safety Guidelines	2 - 3
Safety Warnings and Guidelines	2 - 3
Electrical Equipment Guidelines	2 - 4
Preventing Electrostatic Discharge Damage	2 - 4
Compliance with U.S. Export Laws and Regulations Regarding Encryption	2 - 5

CHAPTER 3

Removing and Installing the SA-VAM2+ 3 - 1

Handling the SA-VAM2+	3 - 1
Online Insertion and Removal (OIR)	3 - 2
SA-VAM2+	3 - 2
Port Adapter Jacket Card	3 - 2
Warnings and Cautions	3 - 2
SA-VAM2+ Removal and Installation	3 - 2
Cisco 7200VXR Router Port Adapter Jacket Card	3 - 3
Cisco 7200VXR Series Routers	3 - 4
Cisco 7301 Router	3 - 6

CHAPTER 4

Configuring the SA-VAM2+ 4 - 1

Overview	4 - 1
Configuration Tasks	4 - 2
Using the EXEC Command Interpreter	4 - 2
Enabling SA-VAM2+	4 - 3
Configuring an IKE Policy	4 - 3
Configuring a Transform Set	4 - 4

Defining a Transform Set	4 - 5
IPSec Protocols: AH and ESP	4 - 6
Selecting Appropriate Transforms	4 - 7
The Crypto Transform Configuration Mode	4 - 7
Changing Existing Transforms	4 - 7
Transform Example	4 - 8
Configuring IPSec	4 - 8
Ensuring That Access Lists Are Compatible with IPSec	4 - 8
Setting Global Lifetimes for IPSec Security Associations	4 - 8
Creating Crypto Access Lists	4 - 9
Creating Crypto Map Entries	4 - 10
Creating Dynamic Crypto Maps	4 - 12
Applying Crypto Map Sets to Interfaces	4 - 14
Configuring Compression	4 - 14
Configure IKE Policy	4 - 14
Configure IKE Preshared Key	4 - 15
Configure ipsec transform set	4 - 15
Configure access-list	4 - 15
Configure crypto map	4 - 16
Apply crypto map to the Interface	4 - 16
Monitoring and Maintaining IPSec	4 - 17
IPSec Configuration Example	4 - 17
Verifying IKE and IPSec Configurations	4 - 18
Verifying the Configuration	4 - 19
Configuration Examples	4 - 21
Configuring IKE Policies Example	4 - 21
Configuring IPSec Configuration Example	4 - 21
Configuring Compression Example	4 - 22
Basic IPSec Configuration Illustration	4 - 22
Router A Configuration	4 - 23
Router B Configuration	4 - 24
Troubleshooting Tips	4 - 24
Monitoring and Maintaining the SA-VAM2+	4 - 26



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:

- [Revision History, page vii](#)
- [Audience, page viii](#)
- [Warnings, page viii](#)
- [Objectives, page viii](#)
- [Organization, page viii](#)
- [Related Documentation, page ix](#)
- [Obtaining Documentation, page x](#)
- [Documentation Feedback, page xi](#)
- [Cisco Product Security Overview, page xi](#)
- [Obtaining Technical Assistance, page xii](#)
- [Obtaining Additional Publications and Information, page xiv](#)

Revision History

Document Version	Date	Notes
OL-5979-01	December 2005	This version introduces the VPN Acceleration Module 2+ (VAM2+)
OL-5979-02	March, 2006	This version of the document adds Port Adapter Jacket Card information, and feature information for IPv6 IPSec and GDOI.
OL-5979-03	August 2006	This version of the document adds NPE-G2 support.

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 VPN Acceleration Module 2+ (SA-VAM2+), a single-width acceleration module that installs in the Cisco 7204VXR and Cisco 7206VXR routers with the NPE-225, NPE-400, NPE-G1 or NPE-G2 processors, and the Cisco 7301, and the Port Adapter Jacket Card in the I/O controller slot of a Cisco 7200VXR router with an NPE-G1 or NPE-G2 installed, and allows a port adapter to be installed in it.

The part number for the VAM2+ is SA-VAM2+(=).



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 SA-VAM2+ and SA-VAM2+ 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 SA-VAM2+	Describes the procedures for installing and removing the SA-VAM2+ from the supported platform.
4	Configuring the SA-VAM2+	Describes procedures needed to configure the SA-VAM2+ in the Cisco 7301 and Cisco 7200VXR series routers.

Related Documentation

This section lists documentation related to your router and its functionality. The documentation mentioned is available online, or on the Documentation CD-ROM.

- For hardware information on the Cisco 7200VXR Port Adapter Jacket Card, see the [Port Adapter Jacket Card Installation Guide](#).
- For hardware installation and maintenance information for the Cisco 7200VXR series routers, refer to the following URL:
http://www.cisco.com/en/US/products/hw/routers/ps341/tsd_products_support_series_home.html
- For Cisco 7301 router documentation, refer to the following URL:
http://www.cisco.com/en/US/products/hw/routers/ps352/prod_technical_documentation.html
- Port Adapter Installation and Configuration guides, available online at:
http://www.cisco.com/en/US/products/hw/modules/ps2033/prod_module_installation_guides_list.html
and
http://www.cisco.com/en/US/products/hw/modules/ps2033/products_module_installation_guides_books_list.html
- For configuration information and support, refer to the modular configuration and modular command reference publications in the Cisco IOS software configuration documentation set that corresponds to the software release installed on your Cisco hardware. Access these documents at:
<http://www.cisco.com/en/US/products/sw/iosswrel/index.html>



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.

- To determine the minimum Cisco IOS software requirements for your router, Cisco maintains the [Software Advisor](#) tool on Cisco.com. This tool does not verify whether modules within a system are compatible, but it does provide the minimum IOS requirements for individual hardware modules or components. Registered Cisco Direct users can access the [Software Advisor](#) at: <http://www.cisco.com/cgi-bin/Support/CompNav/Index.pl>
- For IP security and encryption, refer to the following URL:
http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html

- For FIPS 140 Security documents:
http://www.cisco.com/en/US/partner/products/hw/routers/ps341/products_regulatory_approvals_and_compliance09186a00800f009e.html
- For the VPN Device Manager documents:
http://www.cisco.com/en/US/partner/products/sw/cscowork/ps2322/products_release_and_installation_notes_list.html
- If you are a registered Cisco Direct Customer, you can access the following tools:
 - Bug Toolkit:
http://www.cisco.com/en/US/partner/products/hw/routers/ps341/prod_bug_toolkit.html
 - Bug Navigator:
http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl
 - Feature Navigator:
http://www.cisco.com/en/US/partner/products/prod_feature_navigator_for_cisco_IOS_tool_launch.html
 - Output Interpreter:
<https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>
 - Cisco IOS Error Message Decoder:
<http://www.cisco.com/cgi-bin/Support/Errordecoder/home.pl>
 - Cisco Dynamic Configuration Tool:
http://www.cisco.com/en/US/ordering/or13/or8/ordering_ordering_help_dynamic_configuration_tool_launch.html
 - MIB Locator:
<http://tools.cisco.com/ITDIT/MIBS/servlet/index>
- Additional tools include:
 - Tools Index:
http://www.cisco.com/en/US/partner/products/prod_tools_index.html
 - Cisco IOS Software Selector Tool:
<http://tools.cisco.com/ITDIT/ISTMAIN/servlet/index>

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

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 comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

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:

- 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 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 at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

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 (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI 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.

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 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 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>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *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 for networking professionals to 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>
- 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>



CHAPTER 1

Overview

This chapter describes the VPN Acceleration Module 2+ (SA-VAM2+) and contains the following sections:

- [Data Encryption Overview, page 1-1](#)
- [SA-VAM2+ Overview, page 1-3](#)
- [Features, page 1-4](#)
- [Supported Standards, MIBs, and RFCs, page 1-6](#)
- [Online Insertion and Removal \(OIR\), page 1-7](#)
- [LEDs, page 1-7](#)
- [Cables, Connectors, and Pinouts, page 1-8](#)
- [Slot Locations, page 1-9](#)

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 software devices and CAs to communicate to permit your Cisco IOS software 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 software 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.
- IPComp—IP Payload Compression Protocol. IPComp provides stateless compression for use with encryption services such as IPSec. When using Layer 3 encryption, lower layers (such as PPP at Layer 2) cannot provide compression. When compressing already encrypted packets, expansion usually results.

SA-VAM2+ Overview

The VPN Acceleration Module 2+ (SA-VAM2+) is a single-width port adapter (see [Figure 1-1](#)) supported on the Cisco 7204VXR and Cisco 7206VXR routers with the NPE-225, NPE-400, the NPE-G1 or NPE-G2 processor, and the Cisco 7301 router.

SA-VAM2+ features 128/192/256-bit Advanced Encryption Standard (AES) in hardware, Data Encryption Standard (DES), Triple DES (3DES), and IPv6 IPSec, providing increased performance for site-to-site and remote-access IPSec VPN services. The Cisco SA-VAM2+ provides hardware-assisted Layer 3 compression services with its encryption services, conserving bandwidth and lowering network connection costs over secured links, as well as full Layer 3 routing, quality of service (QoS), multicast and multiprotocol traffic, and broad support of integrated LAN/WAN media.

The SA-VAM2+ can be installed directly in the port adapter slots (see [Figure 1-5](#)) of the Cisco 7000VXR series routers and the Cisco 7301 router. Alternatively, you can install the SA-VAM2+ into a Port Adapter Jacket Card (product ID:C7200-JC-PA) that is inserted in the I/O controller slot of a Cisco 7200VXR router with an NPE-G1 or NPE-G2 processor, for additional bandwidth (see [Figure 1-2](#)).

The SA-VAM2+ support in the Port Adapter Jacket Card allows you to take advantage of the increase in NPE-G1 or NPE-G2 performance, while maintaining VPN performance. You allow more bandwidth to the regular port adapter slots when you install the SA-VAM2+ in the Port Adapter Jacket Card. See the [Port Adapter Jacket Card Installation Guide](#) for more information.

Figure 1-1 SA-VAM2+

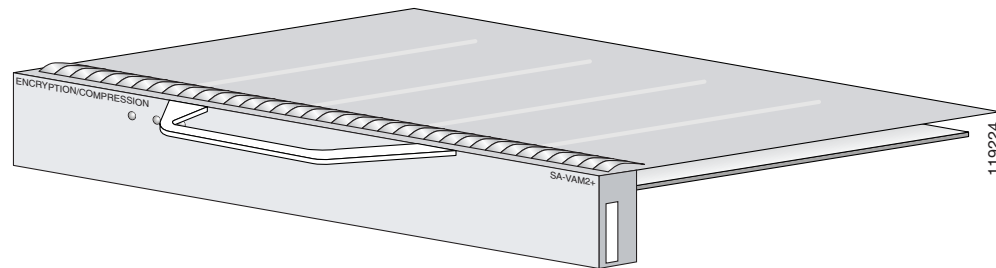
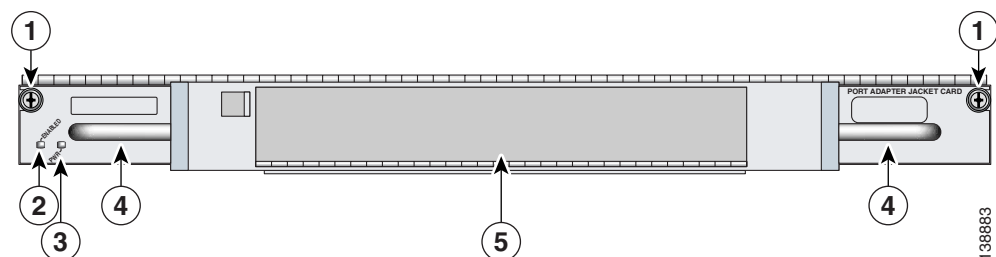


Figure 1-2 Port Adapter Jacket Card Faceplate



1	Captive installation screw	4	Handle
2	ENABLE LED	5	SA-VAM2+/port adapter slot
3	PWR (power) LED		

The SA-VAM2+ provides hardware-accelerated support for multiple encryption functions:

- Data Encryption Standard (DES) standard mode with 56-bit key: Cipher Block Chaining (CBC)
- 3-Key Triple DES (168-bit) algorithms at speeds up to 292 Mbps
- 128/192/256-bit Advanced Encryption Standard (AES) in hardware
- Performance to OC3 full duplex with 300 byte packets
- Up to 5000 tunnels for DES/3DES/AES
- Provides compression with IPSec at no extra overhead (LZS)
- Secure Hash Algorithm (SHA)-1 and Message Digest 5 (MD5) hash algorithms
- Rivest, Shamir, Adelman (RSA) public-key algorithm
- Diffie-Hellman Groups 1, 2 and 5
- Online Insertion and Removal (OIR)

Features

This section describes the SA-VAM2+ features, as listed in [Table 1-1](#).

Table 1-1 SA-VAM2+ Features

Feature	Description/Benefit
Throughput ¹	Up to 292 Mbps using 3DES on the Cisco 7200VXR routers, and up to 392 Mbps using 3DES on the Cisco 7301 router Note The number of IPSec tunnels depends on packet size
Number of IPSec protected tunnels ²	Up to 5000 tunnels ³
Number of tunnels per second	Up to 50
Hardware-based encryption	Data protection: IPSec DES, 3DES, AES, IPv6 IPSec 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
Hardware-based compression	Layer 3 IPCCP LZS
Standards supported	IPSec/IKE: RFCs 2401-2411, 2451 IPCCP: RFC 2393, 2395
(Optional) Port Adapter Jacket Card	The Port Adapter Jacket Card is available on the Cisco 7200VXR router with the NPE-G1 or NPE-G2 ⁴ processor. Note The Port Adapter Jacket Card supported on the Cisco 7200VXR router with the NPE-G2 is available on Cisco IOS Release 12.4(4)XD1 or later. The Port Adapter Jacket Card supported on the Cisco 7200VXR router with the NPE-G2 is available on Cisco IOS Release 12.4(4)XD or later.

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. To support 5000 tunnels, 512 MB of memory is required.
4. The Cisco 7200VXR with the NPE-G2 is only available with Cisco IOS software version 12.4(4)XD.

Performance

Table 1-2 lists the performance information for the SA-VAM2+.

Table 1-2 Performance for SA-VAM2+

Cisco Router	Throughput ^{1 2}	Description
Cisco 7301	Up to 392 Mbps	Cisco IOS release: c7301-jk9o3s-mz.123-10 ² 7301/single SA-VAM2+, 1GB system memory 3DES/SHA, preshared with no IKE-keepalive configured
	Up to 396 Mbps	Cisco IOS release: c7301-jk9o3s-mz.123-10 ² 7301/single SA-VAM2+, 1GB system memory AES/SHA, preshared with no IKE-keepalive configured
Cisco 7200VXR with NPE-G1 or NPE-G2	Up to 263 Mbps	Cisco IOS release: NPE-G1 c7200-jk9o3s-mz.124-4.T1 7200VXR (700Mhz) /single SA-VAM2+, 512MB system memory Cisco IOS release: NPE-G2 c7200p-adventerprisek9-mz.124-4.XD1 7200VXR (1.6 GHz)/single VAM2+, 1024 MB system memory 3DES/SHA, preshared with no IKE-keepalive configured
	Up to 222 Mbps	Cisco IOS release: NPE-G1 c7200-jk9o3s-mz.124-4.T1 7200VXR(700Mhz) /single SA-VAM2+, 512MB system memory Cisco IOS release: NPE-G2: c7200p-adventerprisek9-mz.124-4.XD1 7200VXR (1.6 GHz)/single VAM2+, 1024 MB system memory AES/SHA, preshared with no IKE-keepalive configured
	Up to 391 Mbps	Cisco IOS release: NPE-G1 c7200-jk9o3s-mz.124-4.T1 7200VXR (700Mhz) /dual SA-VAM2+, 512MB system memory Cisco IOS release: NPE-G2: c7200p-adventerprisek9-mz.124-4.XD1 7200VXR (1.6 GHz)/dual VAM2+, 1024 MB system memory 3DES/SHA, preshared with no IKE-keepalive configured
	Up to 391 Mbps	Cisco IOS release: NPE-G1 c7200-jk9o3s-mz.124-4.T1 7200VXR/NPE-G1(700Mhz) /dual SA-VAM2+, 512MB system memory Cisco IOS release: NPE-G2: c7200p-adventerprisek9-mz.124-4.XD1 7200VXR (1.6 GHz)/dual VAM2+, 1024 MB system memory AES/SHA/IPSec/Tunnel Mode, preshared

Table 1-2 Performance for SA-VAM2+ (continued)

Cisco Router	Throughput ^{1 2}	Description
Cisco 7200VXR with NPE-400	Up to 248 Mbps	Cisco IOS release: c7200-jk9o3s-mz.124-4.T1 7200VXR/NPE400/SA-VAM2+, 512MB system memory 3DES/SHA, preshared with no IKE-keepalive configured
	Up to 251 Mbps	Cisco IOS release: c7200-jk9o3s-mz. 124-4.T1 17200VXR/NPE400/single SA-VAM2+, 512MB system memory AES/SHA, preshared with no IKE-keepalive configured
Cisco 7200VXR with NPE-225	Up to 191 Mbps	Cisco IOS release: c7200-jk9o3s-mz.123-10 ² 7200VXR/NPE225/single VAM2+, 256MB system memory 3DES/SHA, preshared with no IKE-keepalive configured

1. As measured with IPSec 3DES Hashed Message Authentication Code (HMAC)-SHA-1 on 1400-byte packets. Performance varies depending on the number of modules, bandwidth, traffic volume, Cisco IOS release, etc.
2. Using Cisco 12.3-10 image. Performance varies by Cisco IOS release. It is recommended that you download the most recent image for your Cisco 7200VXR or Cisco 7301 router.

Supported Standards, MIBs, and RFCs

This section describes the standards, Management Information Bases (MIBs), and Request for Comments (RFCs) supported on the SA-VAM2+. Requests for Comments (RFCs) contain information about the supported Internet suite of protocols.

Standards

- IPPCP: RFC 2393, 2395
- 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

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

Online Insertion and Removal (OIR)

SA-VAM2+

Online insertion and removal (OIR) is supported on the SA-VAM2+. Before removing the SA-VAM2+, we recommend that you shut down the interface so that there is no traffic running through the SA-VAM2+ when it is removed. Removing a SA-VAM2+ while traffic is flowing through the ports can cause system disruption.

Port Adapter Jacket Card

OIR on the Port Adapter Jacket Card is not supported; however, the SA-VAM2+ within the Port Adapter Jacket Card does support OIR. You must have the chassis powered off to install or remove the Port Adapter Jacket Card. See the [Port Adapter Jacket Card Installation Guide](#) for more information about the Port Adapter Jacket Card.

LEDs

This section includes information about the LEDs for the SA-VAM2+ and the Port Adapter Jacket Card. See the [Port Adapter Jacket Card Installation Guide](#) for more information about the Port Adapter Jacket Card.

SA-VAM2+

The SA-VAM2+ has three LEDs, as shown in [Figure 1-3](#). [Table 1-3](#) lists the colors and functions of the LEDs.

Figure 1-3 SA-VAM2+ LEDs



Table 1-3 SA-VAM2+ LEDs

	LED Label	Color	State	Function
1	ENABLE	Green	On	Indicates the SA-VAM2+ is powered up and enabled for operation.

Table 1-3 SA-VAM2+ LEDs

	LED Label	Color	State	Function
2	BOOT	Amber	On	Indicates the SA-VAM2+ is operating.
3	ERROR	Amber	On	Indicates an encryption error has occurred. This LED is normally off.

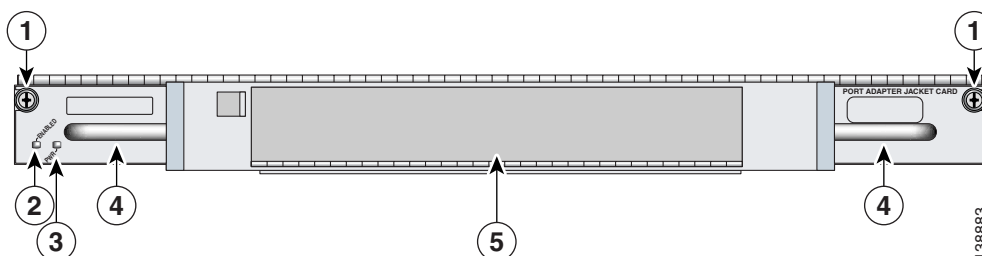
The following conditions must be met before the enabled LED goes on:

- The SA-VAM2+ is correctly connected to the backplane and receiving power.
- The system bus recognizes the SA-VAM2+.

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

Port Adapter Jacket Card

The Port Adapter Jacket Card has two LEDs, as shown in [Figure 1-4](#). [Table 1-3](#) lists the colors and functions of the LEDs.

Figure 1-4 Port Adapter Jacket Card Faceplate

1	Captive installation screw	4	Handle
2	ENABLE LED	5	Port adapter (SA-VAM2+) slot
3	PWR (power) LED		

Table 1-4 Port Adapter Jacket Card LEDs

LED	Color	Indicates
ENABLE	Green	Port Adapter Jacket Card is enabled for operation.
	Off	Port Adapter Jacket Card is not enabled for operation.
PWR (power)	Green	Port Adapter Card is receiving power.
	Off	Port Adapter Card is not receiving power.

Cables, Connectors, and Pinouts

There are no interfaces on the SA-VAM2+, so there are no cables, connectors, or pinouts.

Slot Locations

The topics in this section include:

- [Cisco 7200VXR Routers, page 1-9](#)
- [Cisco 7301 Router, page 1-9](#)

The SA-VAM2+ is supported in the port adapter slots on the Cisco 7200VXR series routers, and the Cisco 7301 routers. It is also supported in the Port Adapter Jacket Card that installs in the I/O controller port of the Cisco 7200VXR routers with the NPE-G1 or NPE-G2 processors.

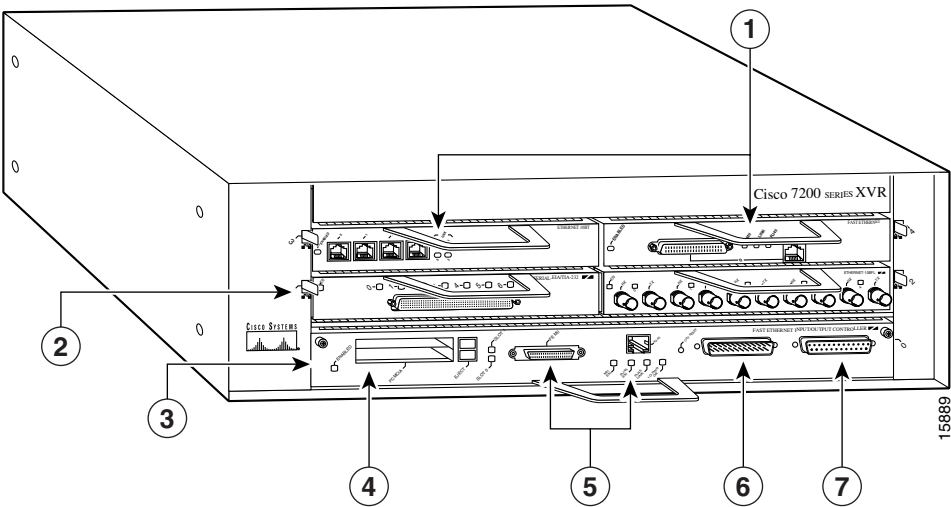


If a port adapter slot is not populated, insert a blank SM-PA filler in the slot (part number 800-00455-01).

Cisco 7200VXR Routers

See [Figure 1-5](#) for the input/output controller and ports for the Cisco 7200VXR routers.

Figure 1-5 Cisco 7200VXR Slot Numbering



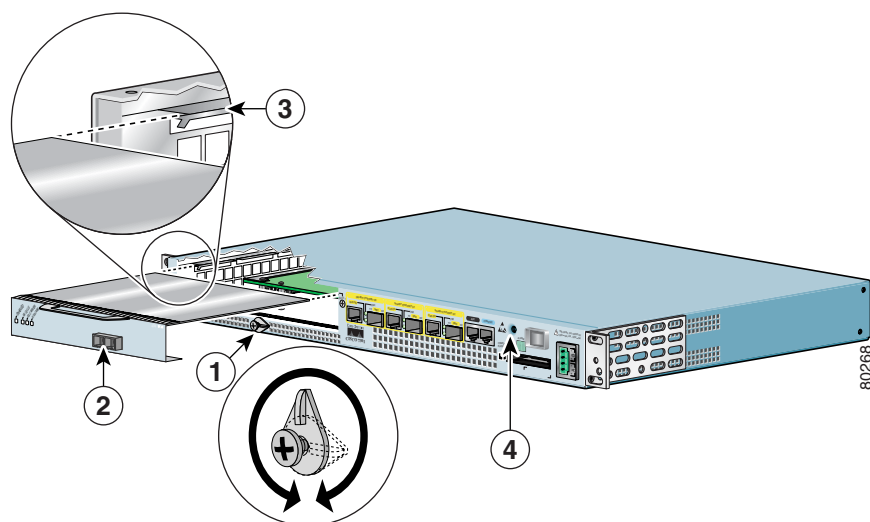
1	Port adapter	5	MII and RJ-45 Fast Ethernet ports
2	Port adapter latch	6	Auxiliary port
3	I/O controller	7	Console port
4	PC card slots		

Cisco 7301 Router

See [Figure 1-6](#) for the port numbering for the Cisco 7301 router.



The Cisco 7301 router supports a single SA-VAM2+, or port adapter.

Figure 1-6 Cisco 7301 Slot Numbering

1	Latch	3	Slot guides
2	Port adapter (SA-VAM2+)	4	Ground for ESD wrist strap banana jack



CHAPTER 2

Preparing for Installation

This chapter describes the general equipment, safety, and site preparation requirements for installing the VPN Acceleration Module 2+ (SA-VAM2+). This chapter includes the following sections:

- [Required Tools and Equipment, page 2-1](#)
- [Hardware and Software Requirements, page 2-1](#)
- [Restrictions, page 2-3](#)
- [Safety Guidelines, page 2-3](#)
- [Compliance with U.S. Export Laws and Regulations Regarding Encryption, page 2-5](#)

Required Tools and Equipment

You need the following tools and parts to install a SA-VAM2+. If you need additional equipment, contact a service representative for ordering information.

- SA-VAM2+
- 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
- Grounding wrist strap
- (Optional) Port Adapter Jacket Card for installation of a port adapter in the I/O controller slot of Cisco 7200VXR routers with an NPE-G1 or NPE-G2 processor

Hardware and Software Requirements

This section describes the minimum software and hardware requirements for the SA-VAM2+:

- [Software Requirements, page 2-2](#)
- [Hardware Requirements, page 2-2](#)
- [Restrictions, page 2-3](#)

Software Requirements

Table 2-1 lists the recommended minimum Cisco IOS software release required to use the SA-VAM2+ 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 SA-VAM2+ Software Requirements

Platform	Recommended Minimum Cisco IOS Release ¹
Cisco 7200VXR router	Cisco IOS Release 12.3(12a)M or a later release of Cisco IOS Release 12.3M Cisco IOS Release 12.3(11)T3 or later release of 12.3T3
Cisco 7200VXR router with the NPE-G2 processor	Cisco IOS Release 12.4(4)XD1 or later release of 12.4(4)XD1 ²
Cisco 7301 router	Cisco IOS Release 12.3(12a)M or a later release of Cisco IOS Release 12.3M Cisco IOS Release 12.3(11)T3 or later release of 12.3T3
(Optional) Cisco 7200VXR Router with the Port Adapter Jacket Card	Cisco IOS Release 12.4(6)T or later release of Cisco IOS Release 12.4T Cisco IOS Release 12.4(7) or later release of Cisco IOS Release 12.4M Cisco IOS Release 12.4(4)XD1 or later release of Cisco IOS Release 12.4(4)XD1 Note The Port Adapter Jacket Card supported on the Cisco 7200VXR router with the NPE-G1 is available on Cisco IOS Release 12.4(6)T and 12.4(7) or later. The Port Adapter Jacket Card supported on the Cisco 7200VXR router with the NPE-G2 is available on Cisco IOS Release 12.4(4)XD or later.

1. The Cisco IOS Release 12.2(14)SU is no longer available for sale.

2. The Cisco 7200VXR router with the NPE-G2 processor is only available with Cisco IOS Release 12.4(4)XD.

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

Specific hardware prerequisites that ensure proper operation of the SA-VAM2+ follow:

- The SA-VAM2+ is compatible with the NPE-225, NPE-400, NPE-G1 or NPE-G2 processor on the Cisco 7200VXR routers. For more efficient performance, we recommend 512 MB of memory.
- For routers using SA-VAM2+, we recommend a minimum configuration of 256 MB of memory; for more efficient performance, we recommend 512 MB of memory.
- The SA-VAM2+ utilizes a specific number of bandwidth points in functioning, which affect performance. For more information on bandwidth requirements, see the [Cisco 7200 Series Port Adapter Hardware Configuration Guidelines](#).

Restrictions

The SA-VAM2+ has the following restrictions:

- SA-VAM2+ does not interoperate with other crypto cards, such as ISA, VAM, or VAM2, in a single Cisco 7204VXR or Cisco 7206VXR.
- The Cisco 7301 router only supports a single port adapter.
- Dual SA-VAM2+ cards are only supported on the Cisco 7200VXR routers with the NPE-G1 or NPE-G2 processor.
- (Optional) SA-VAM2+ is only supported in a Port Adapter Jacket Card on Cisco 7200VXR routers with an NPE-G1 or NPE-G2 processor. See the [Port Adapter Jacket Card Installation Guide](#) for more information about the Port Adapter Jacket Card.

The Port Adapter Jacket Card supported on the Cisco 7200VXR router with the NPE-G1 is available on Cisco IOS Release 12.4(6)T and 12.4(7) or later.

The Port Adapter Jacket Card supported on the Cisco 7200VXR router with the NPE-G2 is available on Cisco IOS Release 12.4 (XD) or later.

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 and Guidelines, page 2-3](#)
- [Electrical Equipment Guidelines, page 2-4](#)
- [Preventing Electrostatic Discharge Damage, page 2-4](#)

Safety Warnings and Guidelines

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



Warning

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

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.



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.

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/lawsurvey.htm> as one possible, unofficial source of international encryption laws.



CHAPTER 3

Removing and Installing the SA-VAM2+

This chapter describes how to remove the Service Adapter VPN Acceleration Module 2+ (SA-VAM2+) from the supported platforms and how to install a new or replacement SA-VAM2+.

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:

- [Handling the SA-VAM2+, page 3-1](#)
- [Online Insertion and Removal \(OIR\), page 3-2](#)
- [Warnings and Cautions, page 3-2](#)
- [SA-VAM2+ Removal and Installation, page 3-2](#)



Note

To ensure proper airflow in the router and compliance with EMI prevention standards, an empty port adapter slot must have a blank port adapter (part number 800-00455-01) installed in it.

The SA-VAM2+ circuit board is sensitive to ESD damage.

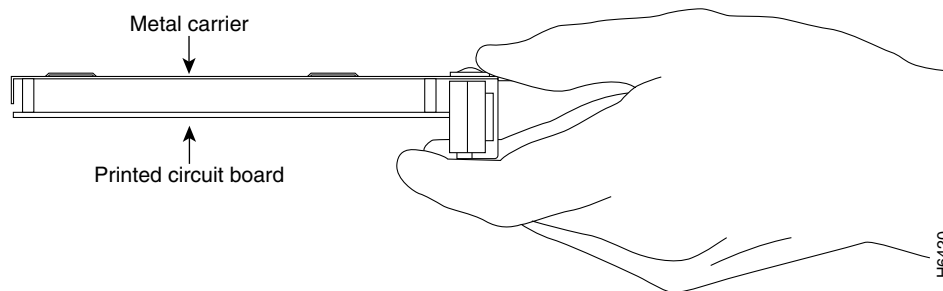
Handling the SA-VAM2+



Caution

Always handle the SA-VAM2+ by the carrier edges and handle; never touch the SA-VAM2+ components. (See [Figure 3-1](#).)

Figure 3-1 Handling the SA-VAM2+



Online Insertion and Removal (OIR)

The Online Insertion and Removal (OIR) feature is described in this section.

SA-VAM2+

Online insertion and removal (OIR) is supported on the SA-VAM2+. Before removing the SA-VAM2+, we recommend that you shut down the interface so that there is no traffic running through the SA-VAM2+ when it is removed. Removing a SA-VAM2+ while traffic is flowing through the ports can cause system disruption.

Port Adapter Jacket Card

OIR on the Port Adapter Jacket Card is not supported; however, the SA-VAM2+ within the Port Adapter Jacket Card does support OIR. You must have the chassis powered off to install or remove the Port Adapter Jacket Card. See the [Port Adapter Jacket Card Installation Guide](#) for more information about the Port Adapter Jacket Card.

Warnings and Cautions

Observe the following warnings and cautions when installing or removing VPN acceleration modules.



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.

SA-VAM2+ Removal and Installation

This section describes how to remove and install the SA-VAM2+, and covers the following topics:

- [Cisco 7200VXR Router Port Adapter Jacket Card, page 3-3](#)
- [Cisco 7200VXR Series Routers, page 3-4](#)

- [Cisco 7301 Router, page 3-6](#)

**Note**

Online insertion and removal (OIR) is not supported on the Port Adapter Jacket Card; however, OIR is supported on the SA-VAM2+. You must have the chassis powered off for the installation or removal process for the Port Adapter Jacket Card.

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

**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.

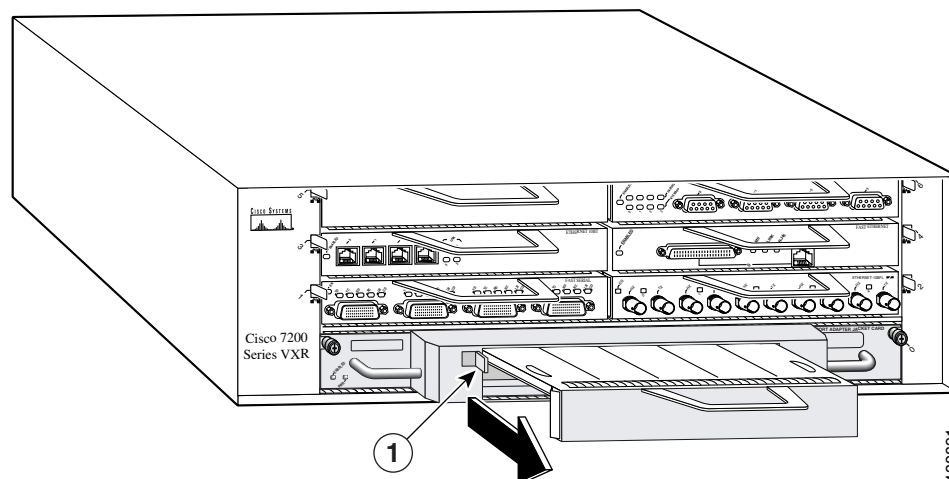
Cisco 7200VXR Router Port Adapter Jacket Card

The I/O controller slot of the Cisco 7200VXR router with an NPE-G1 or NPE-G2 processor supports the Port Adapter Jacket Card with a SA-VAM2+ installed in it. The NPE-G1 or NPE-G2, with a third dedicated peripheral component interconnect (PCI) bus, provides additional bandwidth to the chassis.

Use the following information to install a SA-VAM2+ into an installed Port Adapter Jacket Card. For information on installing the Port Adapter Jacket Card into a Cisco 7200VXR router, see the *Port Adapter Jacket Card Installation Guide*.

- Step 1** Remove any port adapter blank panel that may be in place (see [Figure 3-2](#)).
- Move the lock lever on the top left corner of the Port Adapter Jacket Card until the port adapter blank panel releases.
 - Pull the port adapter blank panel from the Port Adapter Jacket Card.

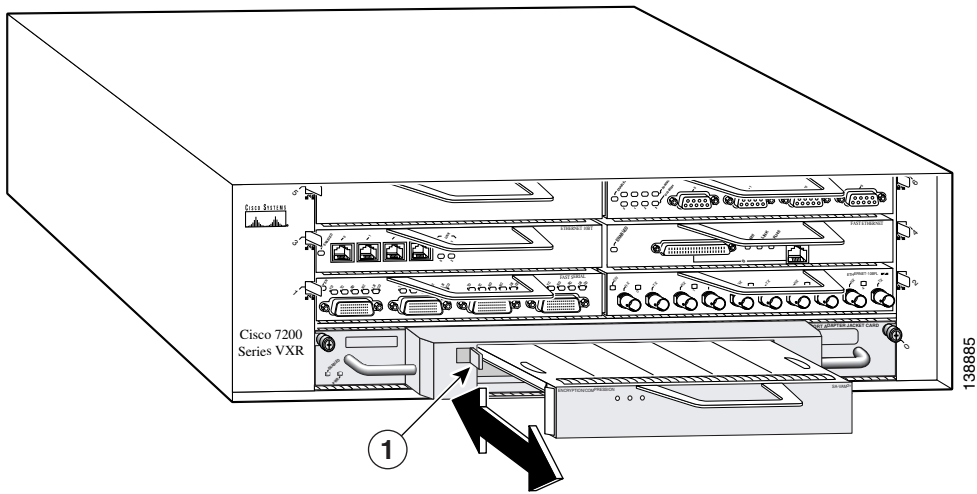
Figure 3-2 Removing the Port Adapter Blank Panel



1	Port adapter lock lever	
----------	-------------------------	--

Step 2 Insert the SA-VAM2+ into the Port Adapter Jacket Card until it is fully seated (see [Figure 3-3](#)).

Figure 3-3 *Installing a Port Adapter in the Port Adapter Jacket Card*



1	Port adapter lock lever		
---	-------------------------	--	--

Step 3 Move the port adapter lock lever to the locked position.

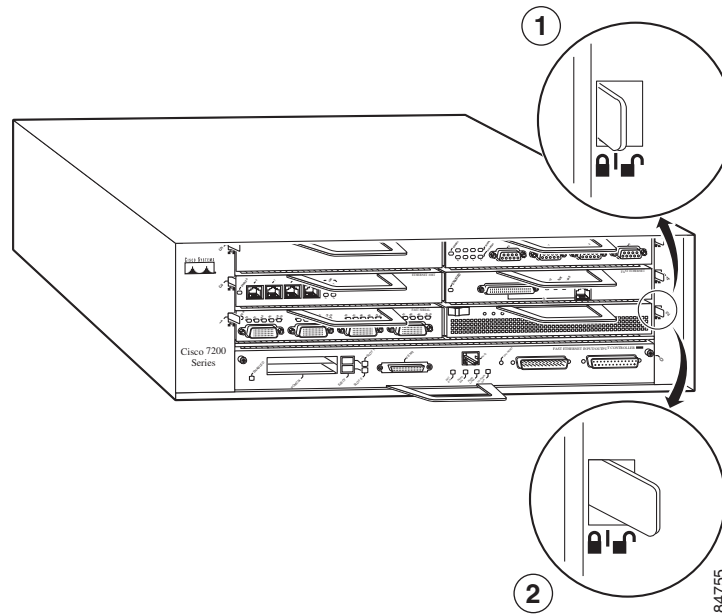
Step 4 If you removed the processing engine and port adapters, replace them in a bottom-to-top order.

Cisco 7200VXR Series Routers

Follow these steps to remove and insert the SA-VAM2+ 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 Caution, above)
- Step 2** Attach an ESD wrist strap between you and an unpainted chassis surface.
- Step 3** Place the SA-VAM2+ retaining lever in the unlocked position. (See [Figure 3-4](#).)

Figure 3-4 Placing the Port Adapter Lever in the Unlocked/Locked Position - Cisco 7206VXR Shown



1	Unlocked position	2	Locked position
---	-------------------	---	-----------------

Step 4 Grasp the handle of the SA-VAM2+ and pull the SA-VAM2+ from the router. If you are removing a blank port adapter, pull it completely out of the chassis slot.

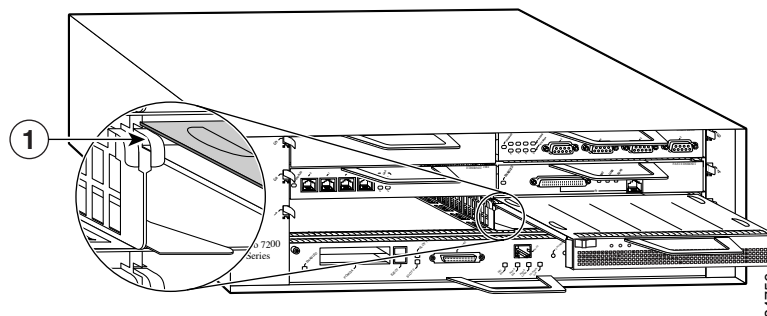
Step 5 Carefully align the new SA-VAM2+ carrier between the upper and the lower edges of the port adapter slot. (See [Figure 3-5](#).)



Caution

To prevent jamming the carrier between the upper and the lower edges of the port adapter slot, and to ensure that the edge connector at the rear of the SA-VAM2+ mates with the connection at the rear of the port adapter slot, make certain that the carrier is positioned correctly, as shown in the cutaway in [Figure 3-5](#).

Figure 3-5 Sliding the SA-VAM2+ into the Port Adapter Slot - Cisco 7206VXR Shown



1	Upper edge of the port adapter slot		
---	-------------------------------------	--	--

Step 6 Slide the new SA-VAM2+ into the port adapter slot until it is seated in the router midplane.



Caution

Do not allow the SA-VAM2+ components to come in contact with the system board or the SA-VAM2+ could be damaged.

Step 7 After the SA-VAM2+ is properly seated, lock the SA-VAM2+ in place, as shown in [Figure 3-4](#).



Note

If a retaining lever does not move to the locked position, the SA-VAM2+ is not completely seated in the midplane. Carefully pull the SA-VAM2+ out of the slot, reinsert it, and move the retaining lever or other mechanism to the locked position. See [Figure 3-4](#).



Caution

To ensure the proper flow of cooling air across the internal components, make sure a blank service adapter filler is installed in any unoccupied port adapter slots (part number 800-20675-01).

Step 8 If you powered off the router:

- a. Reattach the power cable, and place the cable through any cable support brackets.
- b. Power on the router by turning the power switch to the on position.

Cisco 7301 Router

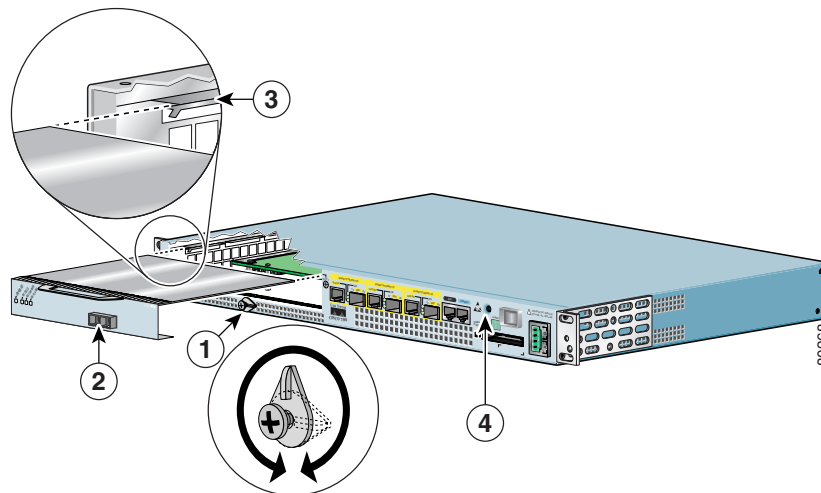
Use [Figure 3-6](#) and follow the steps below to remove and insert an SA-VAM2+ in the Cisco 7301 router:



Note

The Cisco 7301 supports a single SA-VAM2+ or port adapter.

Figure 3-6 Cisco 7301 Port Adapter/SA-VAM2+ Slot



1	Latch	3	Slot guides
2	SA-VAM2+ partially removed	4	Ground for ESD wrist strap banana jack

- Step 1** Use an ESD wrist strap to ground yourself to the router. A banana jack ground is to the left of the power switch.
- Step 2** To remove a SA-VAM2+, use a Phillips screwdriver to turn the screw holding the latch. The screw should be loose enough to allow the latch to rotate to an unlocked position (1). The latch can rotate 360°.
- Step 3** Grasp the handle and pull the SA-VAM2+ (2) from the router, about halfway out of its slot. If you are removing a blank port adapter, pull the blank port adapter completely out of the chassis slot.

**Caution**

The SA-VAM2+ must slide into the slot guides (3) close to the chassis lid. Do not allow the SA-VAM2+ components to come in contact with the system board or the SA-VAM2+ could be damaged.

- Step 4** To insert the SA-VAM2+, carefully align the SA-VAM2+ carrier in the slot guides (3), then carefully slide the SA-VAM2+ all the way into the slot until the SA-VAM2+ is seated.
- Step 5** After the SA-VAM2+ is properly seated, turn and secure the latch in the upright, locked position (1). Tighten the screw to ensure the SA-VAM2+ remains firmly in place.
- Step 6** Reconnect the power cables.
- Step 7** Press the power switch to the ON position to power on the router.



CHAPTER 4

Configuring the SA-VAM2+

This chapter contains the information and procedures needed to configure the VPN Acceleration Module 2+ (SA-VAM2+). This chapter contains the following sections:

- [Overview, page 4-1](#)
- [Configuration Tasks, page 4-2](#)
- [Configuration Examples, page 4-21](#)
- [Basic IPSec Configuration Illustration, page 4-22](#)
- [Troubleshooting Tips, page 4-24](#)
- [Monitoring and Maintaining the SA-VAM2+, page 4-26](#)

Overview

The SA-VAM2+ provides encryption services for any interface in the Cisco 7301 router and the Cisco 7200VXR series routers with a NPE-225, NPE-400, NPE-G1 or NPE-G2 processor. If you have previously configured IPSec on the router and you install a SA-VAM2+, the SA-VAM2+ automatically performs encryption services. If you install a second SA-VAM2+, both SA-VAM2+s should be automatically enabled.



Note

The Cisco 7301 router supports a single SA-VAM2+.

When installing two SA-VAM2+s on the Cisco 7200VXR series routers, per packet load balancing is not supported. With dual SA-VAM2+s installed, load balancing is done on a per IPSec tunnel basis, rather than on a per packet basis.

There are no interfaces to configure on the SA-VAM2+.

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 if the enabled LED is on, the SA-VAM2+ is fully functional and does not require any configuration commands. However, for the SA-VAM2+ to provide encryption services, you must complete the steps in the following sections:

- [Using the EXEC Command Interpreter, page 4-2](#) (required)
- [Enabling SA-VAM2+, page 4-3](#) (required)
- [Configuring an IKE Policy, page 4-3](#) (required)
- [Configuring a Transform Set, page 4-4](#) (required)
- [Configuring IPSec, page 4-8](#) (required)
- [Configuring Compression, page 4-14](#) (optional)
- [IPSec Configuration Example, page 4-17](#) (optional)
- [Verifying IKE and IPSec Configurations, 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 online publication, [Configuring the VPN Acceleration Module](http://www.cisco.com/univercd/cc/td/doc/product/core/7100/7100pacn/vam1/vamconf.htm) at <http://www.cisco.com/univercd/cc/td/doc/product/core/7100/7100pacn/vam1/vamconf.htm>.

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.

Enabling SA-VAM2+

SA-VAM2+ is enabled by default.

To disable SA-VAM2+, use the following commands, starting in global configuration mode:

	Command	Purpose
Step 1	<code>no crypto engine accelerator <slot number></code>	Disables SA-VAM2+.
Step 2	<code>crypto engine accelerator <slot number></code>	Enables SA-VAM2+.

This completes the procedure for disabling and enabling OIR.

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	<code>Router(config)# crypto isakmp policy priority</code>	Defines an IKE policy and enters Internet Security Association Key Management Protocol (ISAKMP) policy configuration (config-isakmp) mode.
Step 2	<code>Router(config-isakmp)# encryption {des 3des aes aes 128 aes 192 aes 256}</code>	Specifies the encryption algorithm within an IKE policy. <ul style="list-style-type: none"> 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	<code>Router(config-isakmp)# authentication {rsa-sig rsa-encr pre-share}</code>	(Optional) Specifies the authentication method within an IKE policy. <ul style="list-style-type: none"> 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. <p>Note If this command is not enabled, the default value (rsa-sig) will be used.</p>

	Command	Purpose
Step 4	<code>Router(config-isakmp)# lifetime <i>seconds</i></code>	<p>(Optional) Specifies the lifetime of an IKE security association (SA).</p> <p><i>seconds</i>—Number of seconds that each SA should exist before expiring. Use an integer from 60 to 86,400 seconds.</p> <p>Note If this command is not enabled, the default value (86,400 seconds [one day]) will be used.</p>
Step 5	<code>Router(config-isakmp)# hash {sha md5}</code>	<p>(Optional) Specifies the hash algorithm within an IKE policy.</p> <ul style="list-style-type: none"> • sha—Specifies SHA-1 (HMAC variant) as the hash algorithm. • md5—Specifies MD5 (HMAC variant) as the hash algorithm. <p>Note If this command is not enabled, the default value (sha) will be used.</p>
Step 6	<code>Router(config-isakmp)# group {1 2 5}</code>	<p>(Optional) Specifies the Diffie-Hellman (DH) group identifier within an IKE policy.</p> <p>1—Specifies the 768-bit DH group.</p> <p>2—Specifies the 1024-bit DH group.</p> <p>5—Specifies the 1536-bit DH group.</p> <p>Note If this command is not enabled, the default value (768-bit) will be used.</p>

For detailed information on creating IKE policies, refer to the “Configuring Internet Key Exchange Security Protocol” chapter in the *Security Configuration Guide* publication.

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](#)
- [Selecting Appropriate Transforms](#)
- [The Crypto Transform Configuration Mode](#)
- [Changing Existing Transforms](#)
- [Transform Example](#)

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:

	Command	Purpose
Step 1	Router(config)# crypto ipsec transform-set <i>transform-set-name</i> <i>transform1</i> [<i>transform2</i> [<i>transform3</i>]]	Defines a transform set and enters crypto transform configuration mode. <ul style="list-style-type: none"> <i>transform-set-name</i>—Specifies the name of the transform set to create (or modify). <i>transform1</i> [<i>transform2</i> [<i>transform3</i>] [<i>transform4</i>]]—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 3	end	Exits the crypto transform configuration mode to enabled mode.
Step 4	clear crypto sa or clear crypto sa peer { <i>ip-address</i> <i>peer-name</i> } or clear crypto sa map <i>map-name</i> or clear crypto sa spi <i>destination-address</i> <i>protocol spi</i>	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 entry keywords to clear out only a subset of the SA database.

[Table 4-1](#) shows 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

Table 4-1 Allowed Transform Combinations (continued)

Transform type	Transform	Description
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
IP Compression Transform (Pick up to one.)	comp-lzs	IP compression with the Lempel-Ziv-Stac (LZS) 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**
- **comp-lzs**

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 “[IPSec Configuration Example](#)” section on page 4-17.

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 in global configuration mode:

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 <i>seconds</i>	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 <i>kilobytes</i>	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(config)# clear crypto sa or Router(config)# clear crypto sa peer { <i>ip-address</i> <i>peer-name</i> } or Router(config)# clear crypto sa map <i>map-name</i> or Router (config)# clear crypto sa entry <i>destination-address protocol spi</i>	(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 entry 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 <i>access-list-number</i> { deny permit } <i>protocol source source-wildcard destination destination-wildcard [log]</i> or Router(config)# ip access-list extended <i>name</i>	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 use IKE to establish the security associations, use the following commands, starting in global configuration mode:

	Command	Purpose
Step 1	Router(config)# crypto map <i>map-name seq-num ipsec-manual</i>	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 <i>access-list-id</i>	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 { <i>hostname</i> <i>ip-address</i> }	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.)
Step 4	Router(config-crypto-m)# set transform-set <i>transform-set-name</i>	Specifies which transform set should be used. This must be the same transform set that is specified in the remote peer’s corresponding crypto map entry. (Only one transform set can be specified when IKE is not used.)

	Command	Purpose
Step 5	<pre>Router(config-crypto-m)# set session-key inbound ah spi hex-key-string</pre> <p>and</p> <pre>Router(config-crypto-m)# set session-key outbound ah spi hex-key-string</pre>	<p>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.</p> <p>(This manually specifies the AH security association to be used with protected traffic.)</p>
Step 6	<pre>Router(config-crypto-m)# set session-key inbound esp spi cipher hex-key-string [authenticator hex-key-string]</pre> <p>and</p> <pre>Router(config-crypto-m)# set session-key outbound esp spi cipher hex-key-string [authenticator hex-key-string]</pre>	<p>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.</p> <p>(This manually specifies the ESP security association to be used with protected traffic.)</p>
Step 7	<pre>Router(config-crypto-m)# exit</pre>	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	<pre>Router(config)# crypto map map-name seq-num ipsec-isakmp</pre>	Names the crypto map entry to create (or modify). This command puts you into the crypto map configuration mode.
Step 2	<pre>Router(config-crypto-m)# match address access-list-id</pre>	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	<pre>Router(config-crypto-m)# set peer {hostname ip-address}</pre>	Specifies a remote IPsec peer. This is the peer to which IPsec protected traffic can be forwarded. Repeat for multiple remote peers.
Step 4	<pre>Router(config-crypto-m)# set transform-set transform-set-name1 [transform-set-name2...transform-set-name6]</pre>	Specifies which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first).
Step 5	<pre>Router(config-crypto-m)# set security-association lifetime seconds seconds</pre> <p>and</p> <pre>Router (config-crypto-m)# set security-association lifetime kilobytes kilobytes</pre>	<p>(Optional) Specifies a security association lifetime for the crypto map entry.</p> <p>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.</p>

	Command	Purpose
Step 6	Router(config-crypto-m)# set security-association level per-host	<p>(Optional) Specifies that separate security associations should be established for each source/destination host pair.</p> <p>Without this command, a single IPSec “tunnel” could carry traffic for multiple source hosts and multiple destination hosts.</p> <p>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.</p> <p>Use this command with care, as multiple streams between given subnets can rapidly consume resources.</p>
Step 7	Router(config-crypto-m)# set pfs [group1 group2]	(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 return 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 <i>dynamic-map-name</i> <i>dynamic-seq-num</i>	Creates a dynamic crypto map entry.
Step 2	Router(config-crypto-m)# set transform-set <i>transform-set-name1</i> [<i>transform-set-name2</i> ... <i>transform-set-name6</i>]	<p>Specifies which transform sets are allowed for the crypto map entry. List multiple transform sets in order of priority (highest priority first).</p> <p>This is the only configuration statement required in dynamic crypto map entries.</p>

	Command	Purpose
Step 3	Router(config-crypto-m)# match address <i>access-list-id</i>	<p>(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.</p> <p>Note Although access-lists are optional for dynamic crypto maps, they are highly recommended</p> <p>If this is configured, the data flow identity proposed by the IPSec peer must fall within a permit statement for this crypto access list.</p> <p>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.</p> <p>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.</p>
Step 4	Router(config-crypto-m)# set peer {hostname ip-address}	<p>(Optional) Specifies a remote IPSec peer. Repeat for multiple remote peers.</p> <p>This is rarely configured in dynamic crypto map entries. Dynamic crypto map entries are often used for unknown remote peers.</p>
Step 5	Router(config-crypto-m)# set security-association lifetime seconds <i>seconds</i> and Router (config-crypto-m)# set security-association lifetime kilobytes <i>kilobytes</i>	(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]	(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 return 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 <i>map-name</i> <i>seq-num</i> ipsec-isakmp dynamic <i>dynamic-map-name</i>	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 <i>map-name</i>	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 <i>map-name</i> local-address <i>interface-id</i>	Permits redundant interfaces to share the same crypto map, using the same local identity.

Configuring Compression

This section includes the following topics:

- [Configure IKE Policy](#) (required)
- [Configure IKE Preshared Key](#) (required)
- [Configure ipsec transform set](#) (required)
- [Configure access-list](#) (required)
- [Configure crypto map](#) (required)
- [Apply crypto map to the Interface](#) (required)

For IPSec configuration examples, refer to the “[Configuring Compression Example](#)”.

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

Configure IKE Policy

To configure IKE policy, follow the steps in “[Configuring an IKE Policy](#)” on page 3, using the commands in global configuration mode.

Configure IKE Preshared Key

To specify preshared keys at a peer, use the following commands in global configuration mode:

	Command	Purpose
Step 1	<pre>Router (config)# crypto isakmp key keystring address peer-address or Router (config)# crypto isakmp key keystring hostname peer-hostname</pre>	<p>At the local peer: Specify the shared key to be used with a particular remote peer.</p> <p>If the remote peer specified their ISAKMP identity with an address, use the address keyword in this step; otherwise use the hostname keyword in this step.</p>
Step 2	<pre>Router (config)# crypto isakmp key_keystring address peer-address or Router (config)# crypto isakmp key_keystring hostname peer-hostname</pre>	<p>At the remote peer: Specify the shared key to be used with the local peer. This is the same key you just specified at the local peer.</p> <p>If the local peer specified their ISAKMP identity with an address, use the address keyword in this step; otherwise use the hostname keyword in this step.</p>
Step 3	Repeat the previous two steps for each remote peer.	

Remember to repeat these tasks at each peer that uses preshared in an IKE policy.

Configure ipsec transform set

To define a transform set—an acceptable combination of security protocols and algorithms—use the `crypto ipsec transform-set` global configuration command. To delete a transform set, use the `no` form of the command.

Command	Purpose
<pre>Router (config)# crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]]</pre>	<p><i>transform-set-name</i> Specify the name of the transform set to create (or modify).</p> <p>transform1 transform2 transform3 Specify up to three transforms (one is required) that define the IPSec security protocol(s) and algorithm(s).</p>

Configure access-list

To establish MAC address access lists, use the `access-list` global configuration command. To remove a single access list entry, use the `no` form of this command.

Command	Purpose
<i>Router (config)#</i> access-list access-list-number { permit deny } address mask	<i>access-list-number</i> Specify an integer from 700 to 799 that you select for the list. permit Permits the frame. deny Denies the frame. <i>address mask</i> Specify 48-bit MAC addresses written in dotted triplet form. The ones bits in the mask argument are the bits to be ignored in the address value.

Configure crypto map

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

	Command	Purpose
Step 1	<i>Router (config)#</i> crypto map map-name seq-num ipsec-isakmp	Create the crypto map and enter crypto map configuration mode.
Step 2	<i>Router (config)#</i> set peer {hostname ip-address}	Specify a remote IPSec peer. This is the peer to which IPSec-protected traffic can be forwarded. Repeat for multiple remote peers.
Step 3	<i>Router (config)#</i> set transform-set transform-set-name1 [transform-set-name2...transform-set-name6]	Specify which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first).
Step 4	<i>Router (config)#</i> match address access-list-id	Specify an extended access list. This access list determines which traffic is protected by IPSec and which is not.

Apply crypto map to the Interface

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

	Command	Purpose
Step 1	<i>Router (config)#</i> interface type number	Specify an interface on which to apply the crypto map and enter interface configuration mode.
Step 2	<i>Router (config)#</i> crypto map map-name	Apply a crypto map set to an interface.
Step 3	<i>Router (config)#</i> end	Exit interface configuration mode.

This completes the process for configuring compression on the SA-VAM2+.

Monitoring and Maintaining IPSec

To clear (and reinitialize) IPSec security associations, use one of the following commands in global configuration mode:

Command	Purpose
Router(config)# clear crypto sa	<p>Clears IPSec security associations.</p> <p>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 entry keywords to clear out only a subset of the SA database. For more information, see the clear crypto sa command.</p>
or	
Router(config)# clear crypto sa counters	
or	
Router(config)# clear crypto sa peer {ip-address peer-name}	
or	
Router(config)# clear crypto sa map map-name	
or	
Router(config)# clear crypto sa entry destination-address protocol spi	

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.

IPSec Configuration Example

The following example shows a minimal IPSec configuration where the security associations will be established via IKE. For more information about IKE, see the “Configuring Internet Key Exchange Security Protocol” chapter.

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.

Verifying IKE and IPsec Configurations

To view information about your IPsec configurations, use **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** 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 global configuration mode:

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, page 4-21](#)
- [Configuring IPsec Configuration Example, page 4-21](#)
- [Configuring Compression Example, page 4-22](#)

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.

Configuring Compression Example

The following example shows a simple configuration example for configuring compression.

To configure an IKE policy:

```
crypto isakmp policy 1
 hash md5
 authentication pre-share
 group 2
```

To configure a IKE preshared key:

```
crypto isakmp key 12abcjhrweit345 address 16.0.0.2
```

To configure an ipsec transform set:

```
crypto ipsec transform-set proposal_01 esp-3des esp-md5-hmac comp-lzs
```

To configure an access-list:

```
access-list 101 permit ip host 16.0.0.1 host 16.0.0.2
```

To configure a crypto map:

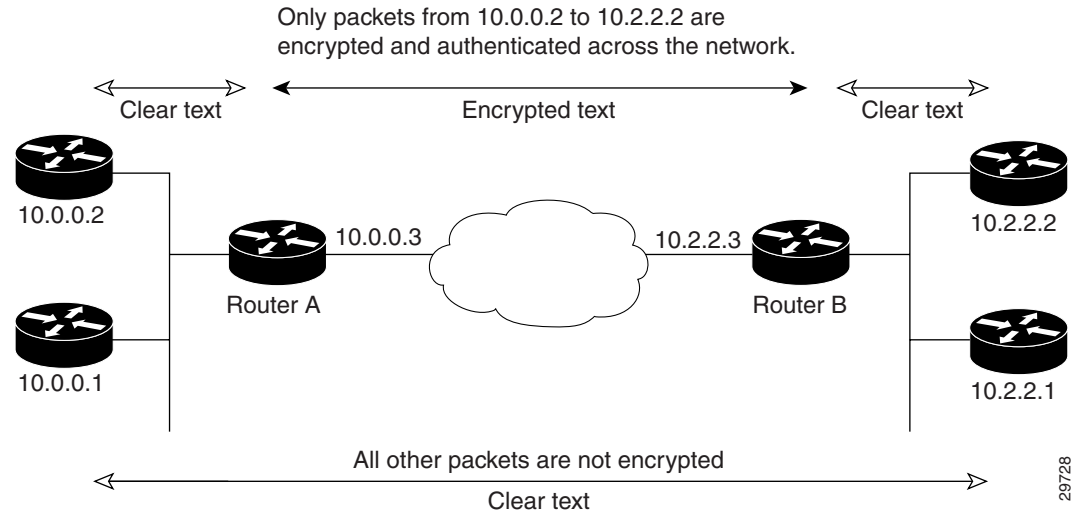
```
crypto map MAXCASE 10 ipsec-isakmp
 set peer 16.0.0.2
 set transform-set proposal_01
 match address 101
```

To apply crypto map to the interface:

```
interface FastEthernet1/0
 crypto map MAXCASE
```

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:

```
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
```

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
  set peer 10.2.2.3
  set transform-set auth1
  match address 101
```

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
```

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
  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 SA-VAM2+, enter the **show diag** command and check the output. For example, when the router has the SA-VAM2+ in slot 4, the following output appears:

Router#**show diag 4**

Slot 4:

```
VAM2+ Encryption/Compression engine, Port adapter
Port adapter is analyzed
Port adapter insertion time 00:16:17 ago
EEPROM contents at hardware discovery:
Hardware Revision      :4.0
EEPROM format version 4
EEPROM contents (hex):
0x00:04 FF 40 04 B0 41 04 00 FF FF FF FF FF FF FF FF
0x10:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x20:FF FF FF FF FF FF FF FF FF FF FF FF FF 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
0x50: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
0x70:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

```

To see if the SA-VAM2+ is currently processing crypto packets, enter the **show pas vam interface** command. The following is sample output:

```

Router# show pas vam interface
VPN Acceleration Module Version II+ in slot : 3
Statistics for Hardware VPN Module since the last clear
of counters 314 seconds ago
      5290894 packets in          5290895 packets out
    1882478960 bytes in        1327439698 bytes out
      16850 paks/sec in          16850 paks/sec out
      47940 Kbits/sec in        33805 Kbits/sec out
    4222173 pkts compressed          0 pkts not compressed
    1190662374 bytes before compress  405331872 bytes after compress
      2.9:1 compression ratio      2.9:1 overall
      58 commands out            58 commands acknowledged
Last 5 minutes:
    4855704 packets in          4855705 packets out
      16185 paks/sec in          16185 paks/sec out
    46723079 bits/sec in        32921855 bits/sec out

Errors:
      ppq full errors           :          0    ppq rx errors           :          0
      cmdq full errors          :          0    cmdq rx errors           :          0
      no buffer                  :          0    replay errors           :          0
      dest overflow             :          0    authentication errors   :          0
      Other error               :          0    RNG self test fail      :          0
      DF Bit set                :          0    Hash Miscompare        :          0
Unwrappable object             :          0    Missing attribute       :          0
Invalid attribute value:       :          0    Bad Attribute           :          0
Verification Fail             :          0    Decrypt Failure         :          0
Invalid Packet                 :          0    Invalid Key             :          0
Input Overrun                  :          0    Input Underrun          :          0
Output buffer overrun          :          0    Bad handle value        :          0
Invalid parameter              :          0    Bad function code       :          0
Out of handles                 :          0    Access denied           :          0

Warnings:
      sessions_expired          :          0    packets_fragmented      :          0
      general                   :          0    compress_bypassed       :          4

HSP details:
      hsp_operations            :          75    hsp_sessions             :          6

```

When the SA-VAM2+ processes packets, the “packets in” and “packets out” counter changes. Counter “packets out” represents the number of packets directed to the SA-VAM2+. Counter “packets in” represents the number of packets received from the SA-VAM2+.



Note

The **show pas vam interface** command output includes ‘compression ratio’ (or the efficiency of the tunnel bandwidth) which represents the ratio of the original packet to the compressed packet plus the ipsec headers. It does not represent the ratio of the ipsec payload before compression to the ipsec payload after compression.

This ratio may fall below 1 when small packets are not compressible, resulting in the ratio representing unencrypted packet to the encrypted packet plus the ipsec header.

To see if the IKE/IPSec packets are being redirected to the SA-VAM2+ 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 SA-VAM2+:

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

CryptoEngine-0 (slot-5) details.
Capability-IPSec :IPPCP, 3DES, AES, RSA

IKE-Session      :    0 active,   5120 max, 0 failed
DH-Key           :    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.

During bootup or OIR, when the Cisco IOS software agrees to redirect crypto traffic to the SA-VAM2+, it prints a message similar to the following:

```
%ISA-6-INFO:Recognised crypto engine (0) at slot-1
...switching to hardware crypto engine
```

To disable the SA-VAM2+, use the configuration mode **no crypto engine accelerator <slot>** command, as follows:

```
Router(config)# no crypto engine accelerator <slot>
Router#
...switching to software crypto engine
*Oct  2 20:00:44 GMT:%VPN_HW-6-INFO:slot:4 Crypto Engine 0 in slot 4 going DOWN
*Oct  2 20:00:44 GMT: Changing crypto engine :Service Adapter:4 state change to:
DISABLED
*Oct  2 20:00:44 GMT:%ISA-1-ERROR:Slot-4:VAM2+ User initiated shutdown.
```

Monitoring and Maintaining the SA-VAM2+

Use the commands that follow to monitor and maintain the SA-VAM2+:

Command	Purpose
Router# show pas vam interface	Verifies the SA-VAM2+ is currently processing crypto packets.
Router# show pas vam controller	Displays the SA-VAM2+ controller configuration.
Router# Show version	Displays integrated service adapter as part of the interfaces.



INDEX

A

acceleration module, VPN (see VAM) [1 - 1](#)
access-list (encryption) command [4 - 10](#)

B

basic IPsec configuration [4 - 23](#)
 illustration [4 - 22](#)

C

cables, connectors, and pinouts [1 - 8](#)
clear crypto sa command [4 - 17, 4 - 19](#)
command
 clear crypto sa [4 - 19](#)
 crypto isakmp enable [4 - 3](#)
command interpreter, EXEC [4 - 2](#)
compliance
 FCC Class A [2 - 5](#)
 U.S. export laws and regulations regarding encryption [2 - 5](#)
configuring
 basic IPsec [4 - 23](#)
 examples [4 - 21](#)
 IKE example [4 - 21](#)
 IPsec example [4 - 21](#)
 router A example [4 - 23](#)
 router B example [4 - 24](#)
 tasks [4 - 2](#)
 verifying [4 - 24](#)
configuring IPsec
 example [4 - 21](#)

crypto dynamic-map command [4 - 12](#)
crypto ipsec security-association lifetime command [4 - 9](#)
crypto map command [4 - 10, 4 - 11](#)
crypto sa command, clear [4 - 19](#)
crypto transform configuration mode, enabling [4 - 7](#)

D

Data [1 - 1](#)
data encryption
 overview [1 - 4](#)
documentation
 other related [ix](#)

E

electrical equipment guidelines [2 - 4](#)
electrostatic discharge
 preventing damage [2 - 4](#)
electrostatic discharge damage
 See ESD prevention
equipment
 electrical guidelines [2 - 4](#)
 required tools and [2 - 1](#)
ESD prevention [2 - 4](#)
EXEC command interpreter [4 - 2](#)

G

guidelines, electrical equipment [2 - 4](#)
guidelines, safety [2 - 3](#)

H

hardware requirements [2 - 2](#)

I
IKE

configuring policies example [4 - 21](#)

interpreter, EXEC command [4 - 2](#)

IPSec

access lists [4 - 8](#)

monitoring [4 - 19](#)

transform sets

defining [4 - 5](#)

IPSec (IPSec network security protocol)

configuration

(example) [4 - 17](#)

configuring [4 - 17](#)

crypto access lists [4 - 9](#)

creating [4 - 9](#)

crypto maps

dynamic

creating [4 - 12](#)

definition [4 - 12](#)

entries, creating [?? to 4 - 13](#)

transforms

allowed combinations [4 - 6](#)

changing [4 - 7](#)

selecting [4 - 7](#)

IPSec, configuring [4 - 23](#)

L

LEDs [1 - 7](#)

SM-VAM [1 - 7](#)

M

maintenance, parts required for VIP installation and [2 - 1](#)

match address command [4 - 11, 4 - 13](#)

MIBs [1 - 6](#)

module, VPN acceleration (see VAM) [1 - 1](#)

P

prevention, ESD [2 - 4](#)

R

Required [2 - 1](#)

required tools and equipment [2 - 1](#)

requirements

hardware [2 - 2](#)

RFCs [1 - 6](#)

S

sa command, clear crypto [4 - 19](#)

safety guidelines [2 - 3](#)

safety warnings [2 - 3](#)

SAs (security associations)

clearing [4 - 9, 4 - 17](#)

lifetimes

global values, configuring [4 - 8](#)

set peer command [4 - 10, 4 - 11, 4 - 13](#)

set pfs command [4 - 12, 4 - 13](#)

set security-association level per-host command [4 - 12](#)

set security-association lifetime command [4 - 11, 4 - 13](#)

set session-key command [4 - 11](#)

set transform-set command [4 - 10, 4 - 11, 4 - 12](#)

show crypto dynamic-map command [4 - 17](#)

show crypto ipsec sa command [4 - 17](#)

show crypto ipsec security-association lifetime command [4 - 17](#)

show crypto ipsec transform-set command [4 - 17](#)

show crypto map command [4 - 17](#)

software

requirements [2 - 3](#)

software and hardware compatability [ix, 2 - 2](#)

standards

supported [1 - 6](#)

T

This [2 - 1](#)

tips, troubleshooting [4 - 24](#)

tools and equipment, required [2 - 1](#)

troubleshooting tips [4 - 24](#)

V

VAM

features [1 - 4](#)

handling [3 - 1](#)

monitoring and maintaining [4 - 26](#)

overview [viii, 4 - 1](#)

software requirements [2 - 2](#)

VPN Acceleration Module (see VAM) [1 - 1](#)

W

warnings, safety [2 - 3](#)