Service Adapter VPN Acceleration Module 2 (SA-VAM2) Installation and Configuration Guide

Product Number: SA-VAM2(=)

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

Text Part Number: OL-4669-02

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This document is to be used in conjunction with the appropriate documentation that shipped with your router.

Preface

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

Audience

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

Warnings

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

Warning **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 Service Adapter VPN Acceleration Module 2 (SA-VAM2), a single-width acceleration module supported on the Cisco 7301 and the Cisco 7200 series routers with the network processing engine 225 (NPE-225), 400 (NPE-400), G1 (NPE-G1), and the Network Services Engine (NSE-1) services accelerator.

The part number for the SA-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 2-30 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 7200 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 installation and maintenance information for the Cisco 7200 series routers, refer to the following documents:
  - For a complete list of Cisco series router hardware documentation, refer to the *Cisco 7200, Cisco 7300, Cisco 7400, Cisco 7500 and Cisco 7200uBR Series Routers Documentation* flyer http://www.cisco.com/en/US/products/hw/routers/ps341/products_product_index09186a00800d9d8a.html
  - *Cisco 7200VXR Installation and Configuration Guide*—DOC-785469= http://www.cisco.com/en/US/products/hw/routers/ps341/products_installation_guide_book09186a008007daa6.html
  - *Cisco 7200VXR Quick Start Guide*—DOC-7812769= http://www.cisco.com/en/US/products/hw/routers/ps341/prod_quick_installation_guide09186a00800a93b6.html
  - *Cisco 7206 Installation and Configuration Guide*—DOC-783229= http://www.cisco.com/en/US/products/hw/routers/ps341/products_installation_guide_book09186a008007db27.html
  - *Cisco 7206 Quick Start Guide*—DOC-7812771= http://www.cisco.com/en/US/products/hw/routers/ps341/prod_quick_installation_guide09186a00800a85fe.html
  - *Quick Reference for the Cisco 7206 Installation*—DOC-783230= http://www.cisco.com/en/US/products/hw/routers/ps341/prod_quick_installation_guide09186a00800defba.html
  - *Cisco 7200 Regulatory Compliance and Safety Information*—DOC-783419= http://www.cisco.com/en/US/products/hw/routers/ps341/products_regulatory_approvals_and_compliance09186a00800a94d7.html
  - *Cisco 7200 Rack Density System (RDS) Installation Instructions*—DOC-7811310= http://www.cisco.com/en/US/products/hw/routers/ps341/products_installation_guide_chapter09186a008007cbe4.html
  - *Rack-Mount and Cable-Management Kit Installation Instructions*—DOC-783421= http://www.cisco.com/en/US/products/hw/routers/ps341/prod_installation_guide09186a00800f267a.html
  - For Cisco 7200 series router troubleshooting information: http://www.cisco.com/en/US/products/hw/routers/ps341/prod_troubleshooting_guides_list.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:
  - *Cisco IOS Security Configuration Guide, Release 12.2*
    http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080087df1.html
  - *Cisco IOS Security Command Reference, Release 12.2*
    http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_command_references_books_list.html
  - *Cisco IOS Security Configuration Guide, Release 12.1*
    http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1831/products_configuration_guide_book09186a0080088254.html
  - *Cisco IOS Security Command Reference, Release 12.1*
    http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1831/products_command_references_books_list.html
  - *Cisco IOS Software Release 12.0 Security Configuration Guide*
    http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1828/products_configuration_guides_books_list.html
  - *Cisco IOS Software Release 12.0 Security Command Reference*
    http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1828/products_command_references_books_list.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:
  - Tools, Maintenance, and Troubleshooting Tips for Cisco IOS Software for Cisco IOS Release 12.0
    http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/prod_troubleshooting_technique09186a008010929b.html
  - Tools, Maintenance, and Troubleshooting Tips for Cisco IOS Software for Cisco IOS Release 12.1
    http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/prod_troubleshooting_technique09186a0080107cc7.html

  - Tools, Maintenance, and Troubleshooting Tips for Cisco IOS Software for Cisco IOS Release 12.2
    http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_troubleshooting_technique09186a00800f9050.html
  - 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

Note We no longer ship the entire router documentation set automatically with each system. You must specifically order the documentation as part of the sales order. If you ordered documentation and did not receive it, we will ship the documents to you within 24 hours. To order documents, contact a customer service representative.

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail to bug-doc@cisco.com.

You can submit comments 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (http://www.cisco.com/tac) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

The online TAC Case Open Tool (http://www.cisco.com/tac/caseopen) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your 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.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation 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.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—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 Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- 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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

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

Overview

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

Data Encryption Overview

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

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

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

Cisco follows these data encryption standards:

- IPSec—IPSec is an IP layer open standards framework that provides data confidentiality, data integrity, and data authentication between participating peers. IKE handles negotiation of protocols and algorithms based on local policy, and generates the encryption and authentication keys to be used by IPSec. IPSec protects one or more data flows between a pair of hosts, between a pair of security routers, or between a security router and a host.
- IKE—Internet Key Exchange (IKE) is a hybrid security protocol that implements Oakley and Skeme key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. IKE can be used with IPSec and other protocols. IKE authenticates the IPSec peers, negotiates IPSec security associations, and establishes IPSec keys. IPSec can be configured with or without IKE.

- CA—certification authority (CA) interoperability supports the IPSec standard, using Simple Certificate Enrollment Protocol (SCEP) and Certificate Enrollment Protocol (CEP). CEP permits Cisco IOS devices and CAs to communicate to permit your Cisco IOS device to obtain and use digital certificates from the CA. IPSec can be configured with or without CA. The CA must be properly configured to issue certificates. For more information, see the "Configuring Certification Authority Interoperability" chapter of the *Security Configuration Guide* at http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html

The component technologies implemented for IPSec include:

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

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

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

  The AH protocol uses various authentication algorithms; Cisco IOS software has implemented the mandatory MD5 and SHA (HMAC variants) authentication algorithms. The AH protocol provides antireplay services.
- ESP—Encapsulating Security Payload, a security protocol, provides data privacy services, optional data authentication, and antireplay services. ESP encapsulates the data to be protected. The ESP protocol uses various cipher algorithms and (optionally) various authentication algorithms. Cisco IOS software implements the mandatory 56-bit DES-CBC with Explicit IV or Triple DES as the encryption algorithm, and MD5 or SHA (HMAC variants) as the authentication algorithms. The updated ESP protocol provides antireplay services.
- IPPCP—IP Payload Compression Protocol. When using Layer 3 encryption, lower layers (such as PPP at Layer 2) cannot provide compression. When compressing already encrypted packets, expansion usually results. IPPCP provides stateless compression for use with encryption services such as IPSec.

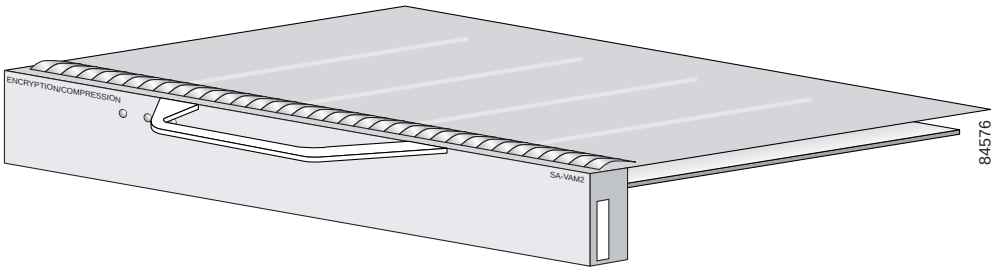
SA-VAM2 Overview

The Service Adapter VPN Acceleration Module 2 (SA-VAM2) is a single-width port adapter (see Figure 1-1) supported on the Cisco 7301 router and the Cisco 7200 series routers with the network processing engine 225 (NPE-225), 400 (NPE-400), G1 (NPE-G1), and the Network Services Engine (NSE-1) services accelerator.

Note The NPE-300 processor is no longer supported.

An SA-VAM2 provides hardware-assisted tunneling and encryption/compression services for Virtual Private Network (VPN) remote access, site-to-site intranets, and extranet applications, including security, quality of service (QoS), firewall and intrusion detection, and service-level validation and management. The SA-VAM2 offloads IPSec processing from the main processor to permit resources on the processor engines for other tasks.

Figure 1-1 SA-VAM2



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

- 128-bit Advanced Encryption Standard (AES) in hardware and 192/256 bits in HSP software
- 56-bit Data Encryption Standard (DES) standard mode: Cipher Block Chaining (CBC)
- Performance to OC3 full duplex with 300 byte packets
- 5000 tunnels for DES/3DES/AES
- Provides compression with IPSec at no extra overhead
- 3-Key Triple DES (168-bit)
- Secure Hash Algorithm (SHA)-1 and Message Digest 5 (MD5) hash algorithms
- Rivest, Shamir, Adelman (RSA) public-key algorithm
- Diffie-Hellman key exchange RC4-40
- IPSec tunnel mode

Features

This section describes the SA-VAM2 features (see Table 1-1), and the SA-VAM2 performance data (see Table 1-2).

Table 1-1 VAM2 Features

Feature	Description/Benefit
Physical	Service adapter; installs in a single port-adapter slot on any Cisco 7200 series[1] or Cisco 7301 router
Platform support	Cisco 7200 Series with NPE G1, NPE-400, NPE-225, or NSE-1 processors and Cisco 7301 Router
Number of IPSec protected tunnels[2]	Up to 5000 on the Cisco 7200 series routers Up to 5000 on the Cisco 7301 router
Hardware-based encryption	Data protection: IPSec DES, 3DES, and AES Authentication: RSA and Diffie-Hellman Data integrity: SHA-1 and Message Digest 5 (MD5)
VPN tunneling	IPsec tunnel mode; Generic Routing Encapsulation (GRE) and Layer 2 Tunneling Protocol (L2TP) protected by IPSec
Hardware-based compression	Layer 3 IPPCP LZS
LAN/WAN interface selection	Works with most Cisco 7200VXR-compatible port adapters
Standards supported	IPSec/IKE: RFCs 2401-2411, 2451 IPPCP: RFC 2393, 2395

1. The Cisco 7200 series supports up to two VAM2.
2. Number of tunnels supported varies based on the total system memory installed.

Performance

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

Table 1-2 Performance

Cisco Router	Throughput[1]	Description
Cisco 7301	Up to 386 Mbps	Cisco IOS: c7301-jk9o3s-mz.123-1.9 7301/single VAM2, 1GB system memory 3DES/SHA, pre-shared with no IKE-keepalive configured
Cisco 7200 with NPE-G1 or NPE-400	Up to 271 Mbps[2]	Cisco IOS: c7200-jk9o3s-mz.123-1 7200VXR/NP-G1(700Mhz) /single VAM2, 512MB system memory 3DES/SHA, pre-shared with no IKE-keepalive configured
	Up to 489 Mbps[2]	Same as above, but with dual VAM2s
Cisco 7200 with NPE-225	Up to 218 Mbps	Cisco IOS: c7200-jk9o3s-mz.123-1 7200VXR/NPE225/single VAM2, 256MB system memory 3DES/SHA, pre-shared with no IKE-keepalive configured
Cisco 7200 with NSE-1	Up to 250 Mbps	Cisco IOS: c7200-jk9o3s-mz.123-1 7200VXR/NSE-1/VAM2, 256MB system memory 3DES/SHA, pre-shared 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 12.3-1M image. Performance varies by Cisco IOS release.

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

LEDs

The SA-VAM2 has three LEDs, as shown in Figure 1-2. Table 1-3 lists the colors and functions of the LEDs.

Figure 1-2 SA-VAM2 LEDs

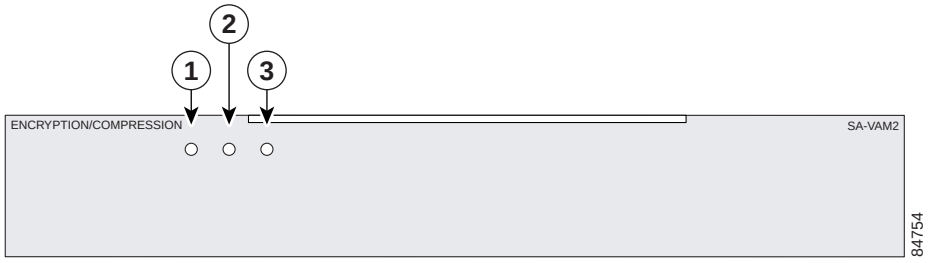


Table 1-3 SA-VAM2 LEDs

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

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:

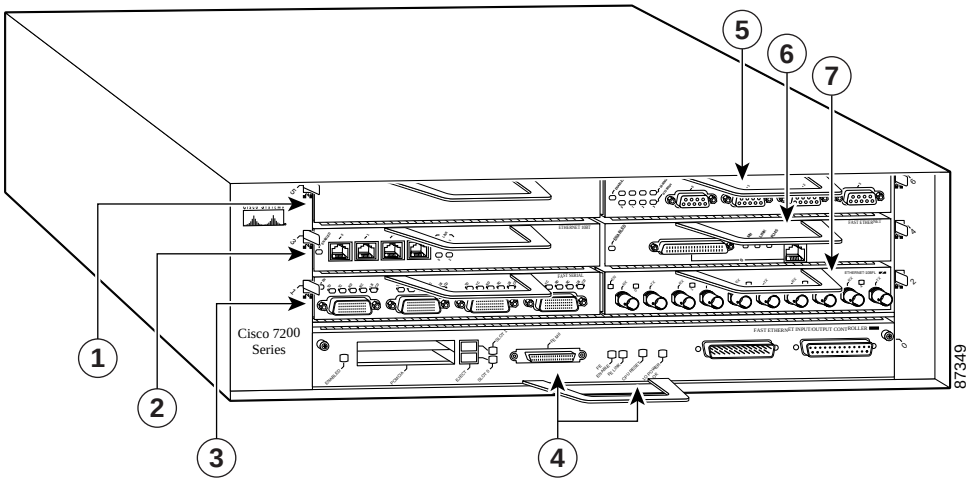
The SA-VAM2 is supported in the port adapter slots on the Cisco 7301 router and the Cisco 7200 series routers.

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

Cisco 7200 Series Routers

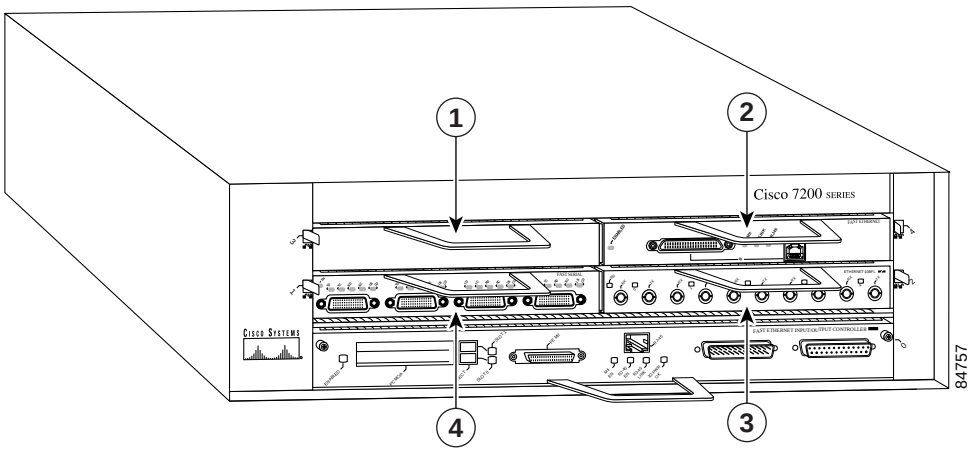
See Figure 1-3, Figure 1-4, and Figure 1-5 for the slot numbering for the Cisco 7200 series routers.

Figure 1-3 Cisco 7206 Slot Numbering



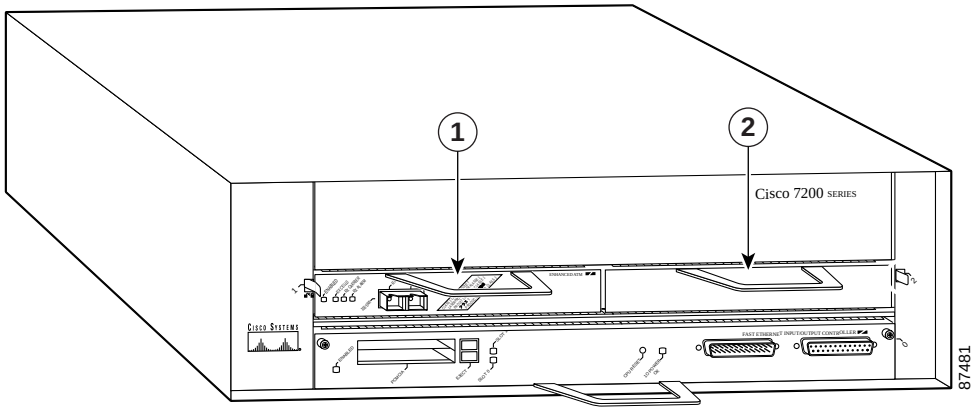
1	Port adapter slot 5 (left bus)	**5**	Port adapter slot 6 (right bus)
2	Port adapter slot 3 (left bus)	**6**	Port adapter slot 4 (right bus)
3	Port adapter slot 1(left bus)	**7**	Port adapter slot 2 (right bus)
4	Port adapter slot 0 (left bus)		

Figure 1-4 Cisco 7204 Slot Numbering



1	Port adapter slot 3	**3**	Port adapter slot 2
2	Port adapter slot 4	**4**	Port adapter slot 1

Figure 1-5 Cisco 7202 Slot Numbering



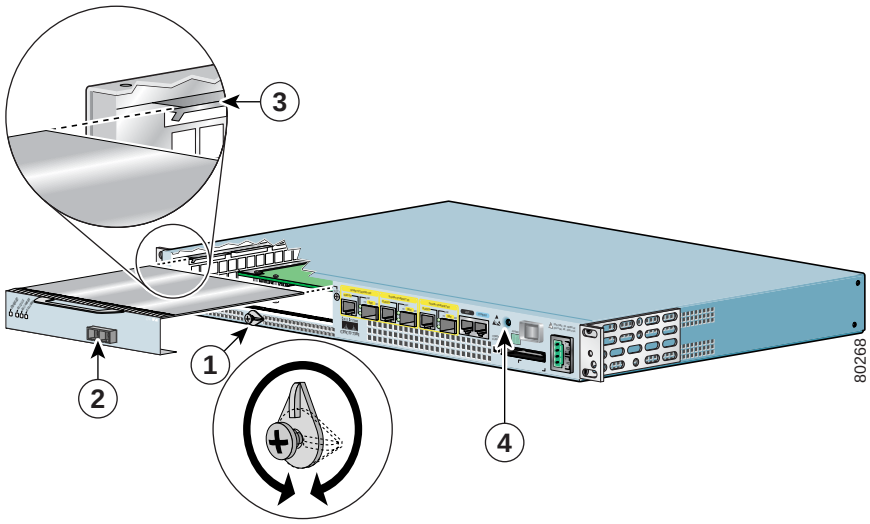
1	Port adapter slot 1	**2**	Port adapter slot 2

Cisco 7301 Router

See Figure 1-6 for the slot numbering for the Cisco 7301 router.

Note The Cisco 7301 router supports a single VAM2, or port adapter.

Figure 1-6 Cisco 7301 Slot Numbering



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

Preparing for Installation

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

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

Minimum Hardware and Software Requirements

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

Hardware Requirements

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

- The SA-VAM2 on the Cisco 7200 series routers requires a network processing engine 225 (NPE-225), 400 (NPE-400), G1 (NPE-G1), or the Network Services Engine (NSE-1) services accelerator.
- The Cisco 7200 series routers support up to two SA-VAM2s.
- The Cisco 7301 router supports a single SA-VAM2 in the port adapter slot.

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
Cisco 7200 series router	Cisco IOS Release 12.3(1)M or a later release of Cisco IOS Release 12.3M
	Cisco IOS Release 12.2(14)SU or a later release of Cisco IOS Release 12.2(14)SU
Cisco 7301 router	Cisco IOS Release 12.3(3) or a later release of Cisco IOS Release 12.3M
	Cisco IOS Release 12.3(2)T1 or a later release of Cisco IOS Release 12.3T1

Hardware and Software Compatibility

This section includes the following hardware and software compatibility requirements:

Hardware Compatibility

The Cisco 7301 router supports a single SA-VAM2 in the port adapter slot.

The Cisco 7200 series routers support up to two SA-VAM2 cards. SA-VAM2 cards can interoperate with port adapters supported on the Cisco 7200 chassis with the NPE-225, NPE-400, or NPE-G1 processor, or the NSE-1 services accelerator.

Note The SA-VAM2 is compatible with the NPE-225, NPE-400, or NPE-G1 processor, or the NSE-1 services accelerator on the Cisco 7200 series routers.

Software Compatibility

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.

Interoperability Between SA-VAM2, ISA, and SA-VAM

Note The integrated services adapter (ISA) is the predecessor of the SA-VAM. The Cisco 7200 series routers supports both the ISA and the SA-VAM with the SA-VAM2.

Table 2-1 describes the interoperability between ISA, SA-VAM, and SA-VAM2. You can use SA-VAM2 with ISA or with SA-VAM, provided you observe the following conditions:

- The Cisco 7200 series routers support two SA-VAM2s in the same chassis. If one SA-VAM2 is enabled at system bootup, and a second SA-VAM2 is added later, the second SA-VAM2 becomes active immediately, and depending on the configuration, the system attempts to load-balance between the two SA-VAM2s.
- If SA-VAM and SA-VAM2 are in the chassis at system bootup, the Cisco 7200 series router supports the newer version, in this case, SA-VAM2, provided the Cisco IOS Release supports SA-VAM2; and the SA-VAM remains inactive.
- If ISA and SA-VAM2 are in the chassis at system bootup, and the **encryption mppe** command is in the router's running configuration, then both ISA/ISM and SA-VAM2 are enabled at system bootup. The ISA/ISM card supports MPPE, and the SA-VAM2 supports ISAKMP/IPSec. You can enable **encryption mppe** by following the steps in "Configuring IPSec" section on page 4-46. To disable MPPE on an ISA card, use the **no encryption mppe** command. This disables the ISA.
- To disable a card, use the **no crypto engine accelerator** *type slot/port* (port-adapter-slot-number/interface-port-number) command.

Table 2-2 Interoperability Between ISA, SA-VAM, and SA-VAM2

SA-VAM2 with ISA	SA-VAM2 with SA-VAM	SA-VAM2 with SA-VAM2
• Supports MPPE	• Does not support MPPE	• Does not support MPPE
• Supports ISAKMP/IPSec	• Supports ISAKMP/IPSec	• Supports ISAKMP/IPSec
• If ISA and SA-VAM2 are enabled in the chassis at power up, ISA is used for MPPE, and SA-VAM2 is used for ISAKMP/IPSec, provided the router's running configuration includes the **encryption mppe** command	• If SA-VAM2 and SA-VAM are in the chassis at power up, the router supports SA-VAM2, and SA-VAM remains inactive	• If SA-VAM2 and SA-VAM2 are enabled in the chassis at power up, the router supports both
• If ISA is enabled in the chassis at bootup, and SA-VAM2 is added later, the SA-VAM2 remains inactive until the next reboot, or until the configuration is changed to enable the SA-VAM2	• If SA-VAM is enabled in the chassis at bootup, and SA-VAM2 is added later, the SA-VAM2 remains inactive until the next reboot, or until the configuration is changed to enable the SA-VAM2	• If SA-VAM2 is enabled in the chassis at bootup, and another SA-VAM2 is added later, the second SA-VAM2 immediately becomes active and depending on the configuration, the system attempts to load-balance between the two SA-VAM2s

Safety Guidelines

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

Safety Warnings

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

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

Warning **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/lawsurvy.htm as one possible, unofficial source of international encryption laws.

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:

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.

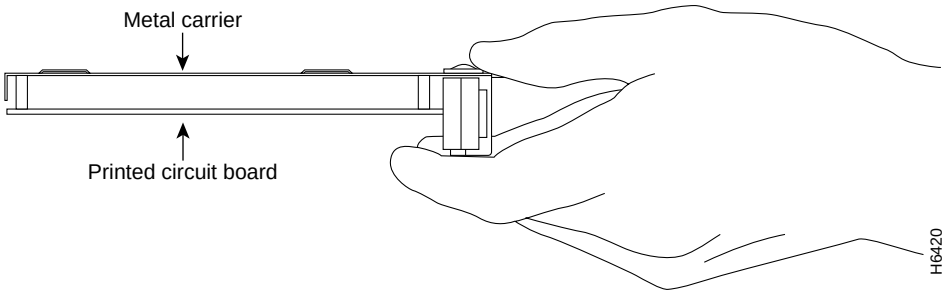
The SA-VAM2 circuit board is sensitive to ESD damage.

Handling the SA-VAM2

The SA-VAM2 is a single-width circuit board mounted on a metal carrier. (see Figure 3-1).

Caution Always handle the SA-VAM2 by the carrier edges and handle; never touch the SA-VAM2 components or connector pins. (See Figure 3-1.)

Figure 3-1 Handling the SA-VAM2



Online Insertion and Removal (OIR)

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 an SA-VAM2 while traffic is flowing through the ports can cause system disruption.

Caution The SA-VAM2 supports online insertion and removal (OIR) of the SA-VAM2 in the Cisco 7200 series routers. You do not need to power down the router when removing and replacing the SA-VAM2. However, online removal will disrupt existing tunnels. You will need to reestablish your tunnels. See Site-to-Site and Extranet VPN Business Scenarios at http://www.cisco.com/univercd/cc/td/doc/product/core/7100/swcg/6342gre.htm#xtocid247834 for additional information on configuring tunnels.

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.**

Warning **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.**

Warning **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:

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

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

Cisco 7200 Series Routers

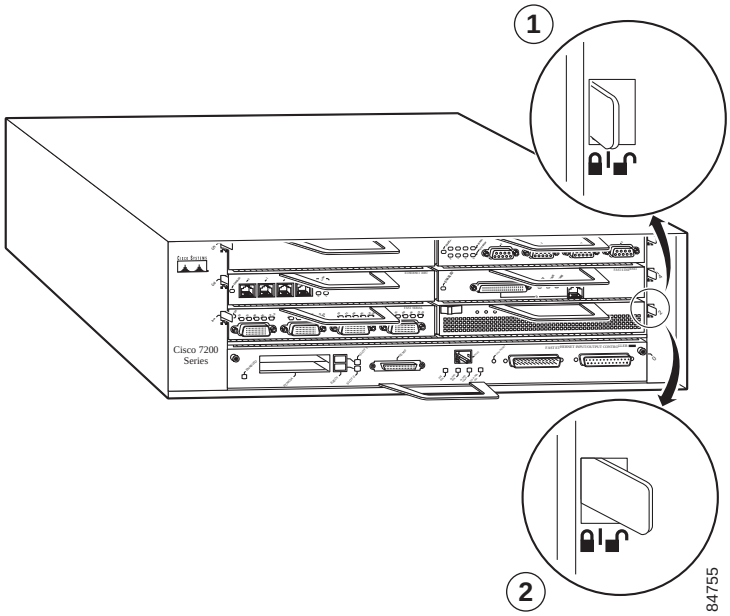
Follow these steps to remove and insert the SA-VAM2 in the Cisco 7200 series routers:

Step 1 Turn the power switch to the off position and then remove the power cable. (Optional on Cisco 7200 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 1 in Figure 3-2.)

Figure 3-2 Placing the Port Adapter Lever in the Unlocked/Locked Position - Cisco 7206VXR Shown



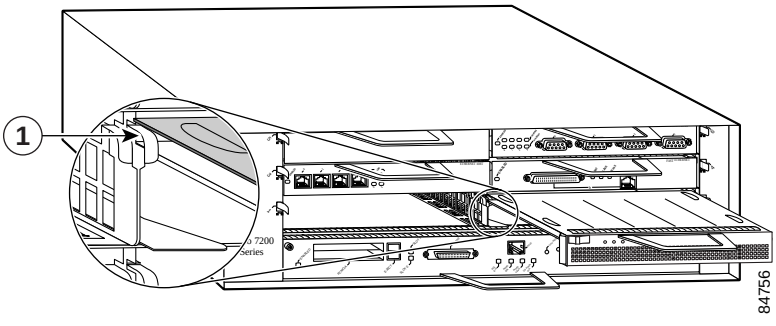
1	Unlocked position	**2**	Locked position

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 3-3.)

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 3-3.

Figure 3-3 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 2 of Figure 3-2.

Note If a retaining lever does not move to the locked position, the module is not completely seated in the midplane. Carefully pull the module out of the slot, reinsert it, and move the retaining lever or other mechanism to the locked position. See Figure 3-2.

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.

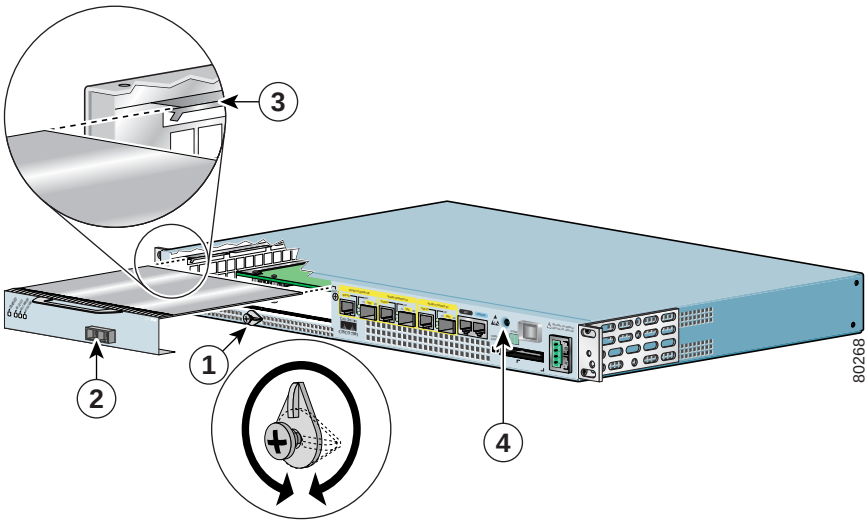
This completes the removal and installation procedure of the SA-VAM2 from the Cisco 7200 series routers.

Cisco 7301 Router

Use Figure 3-4 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 3-4 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.

This completes the removal and installation procedure of the SA-VAM2 from the Cisco 7301 router.

Configuring the SA-VAM2

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

Overview

The SA-VAM2 provides encryption services for any interface in the Cisco 7301 router and the Cisco 7200 series routers with a network processing engine 225 (NPE-225), 400 (NPE-400), G1 (NPE-G1), and the Network Services Engine (NSE-1) services accelerator. 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-VAM2s should be automatically enabled.

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

Note When installing two SA-VAM2s on the Cisco 7200 series routers, per packet load balancing is not supported. With dual SA-VAM2s 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 4-40 (required)
- Disabling OIR, page 4-41 (required)
- Configuring an IKE Policy, page 4-41 (required)
- Configuring a Transform Set, page 4-43 (required)
- Configuring IPSec, page 4-46 (required)
- Configuring Compression, page 4-52 (optional)
- IPSec Configuration Example, page 4-56 (optional)
- Verifying IKE and IPSec Configurations, page 4-56 (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* 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.

Disabling OIR

Online insertion and removal (OIR) on the SA-VAM2 is enabled by default.

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

	Command	Purpose
Step 1	**no crypto engine accelerator** *<slot number>*	Disables OIR of the SA-VAM2.
Step 2	**crypto engine accelerator** *<slot number>*	Enables OIR of the 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	Router(config)# **crypto isakmp policy** *priority*	Defines an IKE policy and enters Internet Security Association Key Management Protocol (ISAKMP) policy configuration (config-isakmp) mode.
Step 2	Router(config-isakmp)# **encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}	Specifies the encryption algorithm within an IKE policy. • **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 192**—Specifies 192-bit AES as the encryption algorithm. • **aes 256**—Specifies 256-bit AES as the encryption algorithm.
Step 3	Router(config-isakmp)# **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}	(Optional) Specifies the authentication method within an IKE policy. • **rsa-sig**—Specifies Rivest, Shamir, and Adelman (RSA) signatures as the authentication method. • **rsa-encr**—Specifies RSA encrypted nonces as the authentication method. **Note** Beginning with Cisco IOS Release 12.3(10), rsa-encr is now enabled for VAM2 crypto cards. • **pre-share**—Specifies preshared keys as the authentication method. **Note** If this command is not enabled, the default value (**rsa-sig**) will be used.

	Command	Purpose
Step 4	`Router(config-isakmp)# lifetime` *seconds*	(Optional) Specifies the lifetime of an IKE security association (SA). *seconds*—Number of seconds that each SA should exist before expiring. Use an integer from 60 to 86,400 seconds. **Note** If this command is not enabled, the default value (86,400 seconds [one day]) will be used.
Step 5	`Router(config-isakmp)# hash {sha | md5}`	(Optional) Specifies the hash algorithm within an IKE policy. • **sha**—Specifies SHA-1 (HMAC variant) as the hash algorithm. • **md5**—Specifies MD5 (HMAC variant) as the hash algorithm. **Note** If this command is not enabled, the default value (**sha**) will be used.
Step 6	`Router(config-isakmp)# group {1 | 2 | 5}`	(Optional) Specifies the Diffie-Hellman (DH) group identifier within an IKE policy. **1**—Specifies the 768-bit DH group. **2**—Specifies the 1024-bit DH group. **5**—Specifies the 1536-bit DH group. **Note** If this command is not enabled, the default value (768-bit) will be used.

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

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:

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` *transform-set-name transform1* `[`*transform2* `[`*transform3*`]]`	Defines a transform set and enters crypto transform configuration mode. • *transform-set-name*—Specifies the name of the transform set to create (or modify). • *transform1* [*transform2* [*transform3*] [*transform4*]]—Defines the IPSec security protocols and algorithms. Accepted transform values are described in Table 4-1.
Step 2	`Router(cfg-crypto-tran)# mode [tunnel | transport]`	(Optional) Changes the mode associated with the transform set. The mode setting is only applicable to traffic whose source and destination addresses are the IPSec peer addresses; it is ignored for all other traffic. (All other traffic is in tunnel mode only.)
Step 4	**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*	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.
Step 3	**end**	Exits the crypto transform configuration mode to enabled mode.

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

Table 4-1 Allowed Transform Combinations

Transform type	Transform	Description
AH Transform (Pick up to one.)	**ah-md5-hmac**	AH with the MD5 (Message Digest 5) (HMAC variant) authentication algorithm
	ah-sha-hmac	AH with the SHA (Secure Hash Algorithm) (HMAC variant) authentication algorithm
ESP Encryption Transform (Note: If an **ESP Authentication Transform** is used, you must pick one.)	**esp-aes**	ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithm
	esp-aes 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-eas** and **esp-sha-hmac**
- **ah-sha-hmac** and **esp-eas** 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
```

The following example is a sample warning message that is displayed when a user enters an IPSec transform that the hardware does not support:

```
crypto ipsec transform transform-1 esp-aes 256 esp-md5
WARNING:encryption hardware does not support transform
esp-aes 256 within IPSec transform transform-1
```

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".

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(config)# crypto ipsec security-association lifetime seconds` *seconds*	Changes the global "timed" lifetime for IPSec SAs. This command causes the security association to time out after the specified number of seconds have passed.
Step 2	`Router(config)# crypto ipsec security-association lifetime kilobytes` *kilobytes*	Changes the global "traffic-volume" lifetime for IPSec SAs. This command causes the security association to time out after the specified amount of traffic (in kilobytes) have passed through the IPSec "tunnel" using the security association.
Step 3	`Router(config)# clear crypto sa` 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*	(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 access-list-number {deny | permit} protocol source source-wildcard destination destination-wildcard [log]`
	or
	`Router(config)# ip access-list extended name`
		Specifies conditions to determine which IP packets will be protected.[1] (Enable or disable crypto for traffic that matches these conditions.)
		We recommend that you configure "mirror image" crypto access lists for use by IPSec and that you avoid using the **any** keyword.

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

1. You specify conditions using an IP access list designated by either a number or a name. The **access-list** command designates a numbered extended access list; the **ip access-list extended** command designates a named access list.

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

Creating Crypto Map Entries

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

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

	Command	Purpose
Step 1	`Router(config)# crypto map map-name seq-num ipsec-manual`	Specifies the crypto map entry to create (or modify). This command puts you into the crypto map configuration mode.
Step 2	`Router(config-crypto-m)# match address access-list-id`	Names an IPSec access list. This access list determines which traffic should be protected by IPSec and which traffic should not be protected by IPSec security in the context of this crypto map entry. (The access list can specify only one **permit** entry when IKE is not used.)
Step 3	`Router(config-crypto-m)# set peer {hostname | ip-address}`	Specifies the remote IPSec peer. This is the peer to which IPSec protected traffic should be forwarded. (Only one peer can be specified when IKE is not used.)
Step 4	`Router(config-crypto-m)# set transform-set transform-set-name`	Specifies which transform set should be used. This must be the same transform set that is specified in the remote peer's corresponding crypto map entry. (Only one transform set can be specified when IKE is not used.)

	Command	Purpose

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

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

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

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

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

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

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

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

Applying Crypto Map Sets to Interfaces

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

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

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

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

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

Configuring Compression

This section includes the following topics:

- Configure IKE Policy (required)
- Configure IKE Pre-Shared 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 41, using the commands in global configuration mode.

Configure IKE Pre-Shared Key

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

	Command	Purpose

Step 1	`Router (config)# crypto isakmp key keystring address peer-address`
	
	or
	
	`Router (config)# crypto isakmp key keystring hostname peer-hostname`
		At the local peer:
		Specify the shared key to be used with a particular remote peer.
		
		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.

Step 2	`Router (config)# crypto isakmp key_keystring address peer-address`
	
	or
	
	`Router (config)# crypto isakmp key_keystring hostname peer-hostname`
		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.
		
		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.

Step 3	Repeat the previous two steps for each remote peer.	

Remember to repeat these tasks at each peer that uses pre-shared 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
`Router (config)# crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]]`	*transform-set-name* Specify the name of the transform set to create (or modify). *transform1* *transform2* *transform3* Specify up to three transforms (one is required) that define the IPSec security protocol(s) and algorithm(s).

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
`Router (config)# access-list access-list-number {permit | deny} address mask`	*access-list-number* Specify an integer from 700 to 799 that you select for the list. **permit** Permits the frame. **deny** Denies the frame. *address mask* 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	`Router (config)# crypto map map-name seq-num ipsec-isakmp`	Create the crypto map and enter crypto map configuration mode.
Step 2	`Router (config)# 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	`Router (config)# 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	`Router (config)# 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	`Router (config)# interface type number`	Specify an interface on which to apply the crypto map and enter interface configuration mode.
Step 2	`Router (config)# crypto map map-name`	Apply a crypto map set to an interface.
Step 3	`Router (config)# end`	Exit interface configuration mode.

This completes the process for configuring compression on the 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`
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`
	Clears IPSec security associations.
	Note Using the **clear crypto sa** command without parameters will clear out the full SA database, which will clear out active security sessions. You may also specify the **peer**, **map**, or **entry** keywords to clear out only a subset of the SA database. For more information, see the **clear crypto sa** command.

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

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

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 4-59
- Configuring IPSec Configuration Example, page 4-59
- Configuring Compression Example, page 4-60

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 pre-shared 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
```

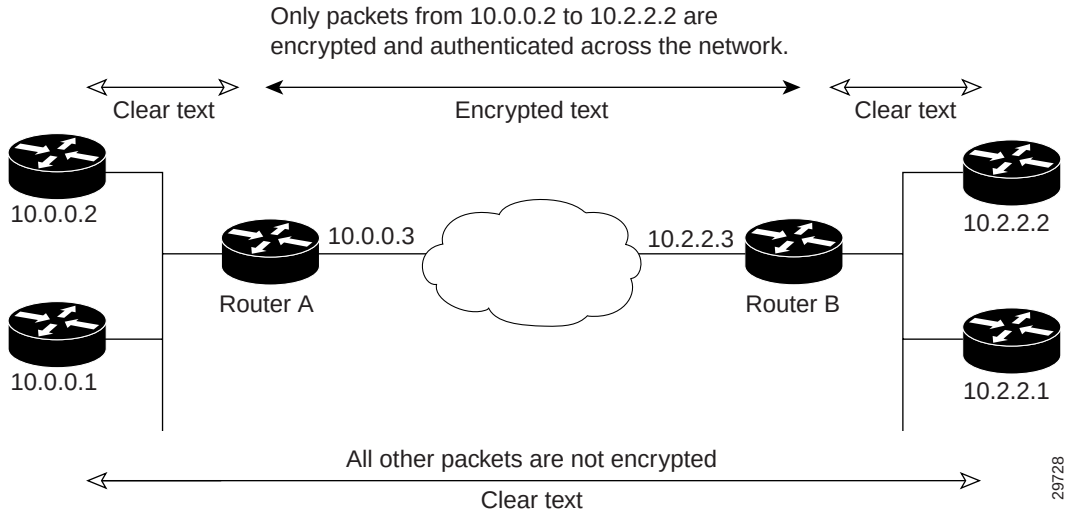
To apply crypto map to the interface:

```
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
```

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 1, the following output appears:

```
Router# show diag
Slot 6:
        VAM2 Encryption/Compression engine, Port adapter
        Port adapter is analyzed
        Port adapter insertion time 00:01:32 ago
        EEPROM contents at hardware discovery:
        Hardware Revision        :1.0
        PCB Serial Number        :
        Part Number              :73-8491-00
        Board Revision           :
        RMA Test History         :00
        RMA Number               :0-0-0-0
        RMA History              :00
        Deviation Number         :0-0
        Product Number           :SA-VAM2
        Top Assy. Part Number    :800-22836-00
        CLEI Code                :
        EEPROM format version 4
        EEPROM contents (hex):
          0x00:04 FF 40 03 E4 41 01 00 C1 8B 00 00 00 00 00 00
          0x10:00 00 00 00 00 82 49 21 2B 00 42 00 00 03 00 81
          0x20:00 00 00 00 04 00 80 00 00 00 00 CB 94 53 41 2D
          0x30:56 41 4D 32 20 20 20 20 20 20 20 20 20 20 20 20
          0x40:20 C0 46 03 20 00 59 34 00 C6 8A 00 00 00 00 00
          0x50:00 00 00 00 00 FF FF FF FF FF FF FF FF FF FF FF
          0x60:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

To see if the 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 attrribute value:        0   Bad Attribute           :        0
```

```
   Verification Fail       :         0   Decrypt Failure         :         0
   Invalid Packet          :         0   Invalid Key             :         0
   Input Overrun           :         0   Input Underrun          :         0
   Output buffer overrun   :         0   Bad handle value        :         0
   Invalid parameter       :         0   Bad function code       :         0
   Out of handles          :         0   Access denied           :         0

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#
    3w4d:%ISA-6-SHUTDOWN:VAM2 shutting down
    3w4d:%ISA-6-INFO:Crypto Engine 0 in slot 1 going DOWN
    3w4d:...switching to software crypto engine
```

Monitoring and Maintaining the SA-VAM2

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

Command	Purpose
Router# **show pas isa interface**	Displays the ISA interface configuration.
Router# **show pas isa controller**	Displays the ISA controller configuration.
Router# **show pas vam interface**	Verifies the 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.

H

I

L

M

O

P

R

S

T

V

W