CHAPTER 1

Overview

This chapter describes the 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 software devices and CAs to communicate to permit your Cisco IOS software device to obtain and use digital certificates from the CA. IPSec can be configured with or without CA. The CA must be properly configured to issue certificates. For more information, see the "Configuring Certification Authority Interoperability" chapter of the *Security Configuration Guide* at http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html

The component technologies implemented for IPSec include:

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

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

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

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

SA-VAM2+ Overview

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

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

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

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

Figure 1-1 SA-VAM2+

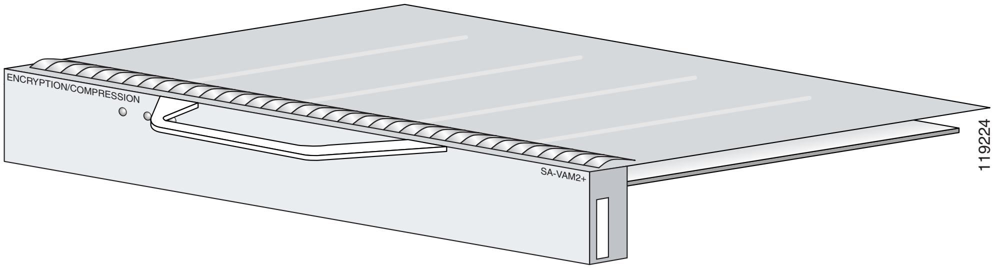
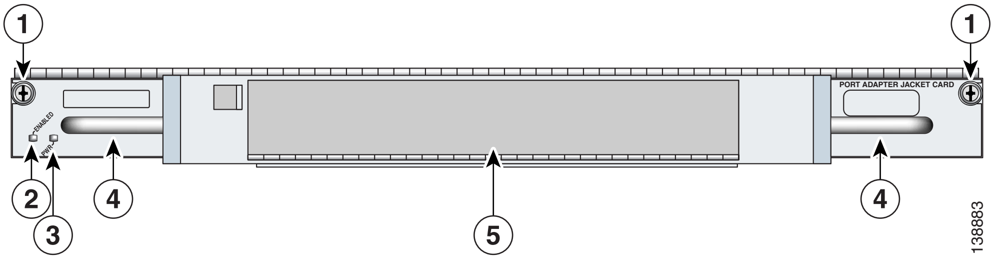


Figure 1-2 Port Adapter Jacket Card Faceplate



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

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

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

Features

This section describes the SA-VAM2+ features, as listed in Table 1-1.

Table 1-1 SA-VAM2+ Features

Feature	Description/Benefit
Throughput[1]	Up to 292 Mbps using 3DES on the Cisco 7200VXR routers, and up to 392 Mbps using 3DES on the Cisco 7301 router **Note** The number of IPSec tunnels depends on packet size
Number of IPSec protected tunnels[2]	Up to 5000 tunnels[3]
Number of tunnels per second	Up to 50
Hardware-based encryption	Data protection: IPSec DES, 3DES, AES, IPv6 IPSec Authentication: RSA and Diffie-Hellman Data integrity: SHA-1 and Message Digest 5 (MD5)
VPN tunneling	IPsec tunnel mode; Generic Routing Encapsulation (GRE) and Layer 2 Tunneling Protocol (L2TP) protected by IPSec
Hardware-based compression	Layer 3 IPPCP LZS
Standards supported	IPSec/IKE: RFCs 2401-2411, 2451 IPPCP: RFC 2393, 2395
(Optional) Port Adapter Jacket Card	The Port Adapter Jacket Card is available on the Cisco 7200VXR router with the NPE-G1 or NPE-G2[4] processor. **Note** The Port Adapter Jacket Card supported on the Cisco 7200VXR router with the NPE-G2 is available on Cisco IOS Release 12.4(4)XD1 or later. The Port Adapter Jacket Card supported on the Cisco 7200VXR router with the NPE-G2 is available on Cisco IOS Release 12.4(4)XD or later.

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

[2] Number of tunnels supported varies based on the total system memory installed.

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

Performance

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

Table 1-2 Performance for SA-VAM2+

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

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

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

[1] As measured with IPSec 3DES Hashed Message Authentication Code (HMAC)-SHA-1 on 1400-byte packets. Performance varies depending on the number of modules, bandwidth, traffic volume, Cisco IOS release, etc.

[2] Using Cisco 12.3-10 image. Performance varies by Cisco IOS release. It is recommended that you download the most recent image for your Cisco 7200VXR or Cisco 7301 router.

Supported Standards, MIBs, and RFCs

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

Standards

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

MIBs

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

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

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

RFCs

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

Online Insertion and Removal (OIR)

SA-VAM2+

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

Port Adapter Jacket Card

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

LEDs

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

SA-VAM2+

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

Figure 1-3 SA-VAM2+ LEDs

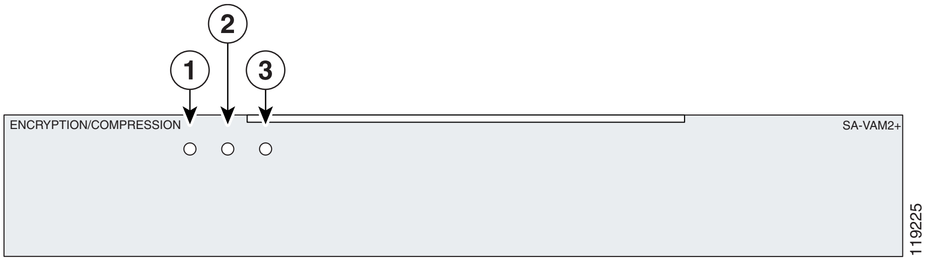


Table 1-3 SA-VAM2+ LEDs

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

Table 1-3 SA-VAM2+ LEDs

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

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

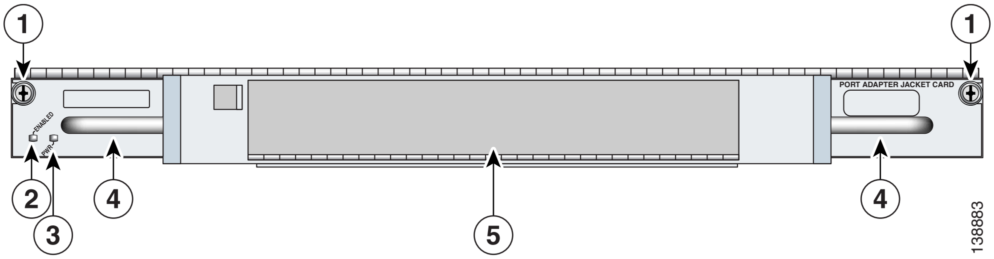
- The SA-VAM2+ is correctly connected to the backplane and receiving power.
- The system bus recognizes the SA-VAM2+.

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

Port Adapter Jacket Card

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

Figure 1-4 Port Adapter Jacket Card Faceplate



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

Table 1-4 Port Adapter Jacket Card LEDs

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

Cables, Connectors, and Pinouts

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

Slot Locations

The topics in this section include:

- Cisco 7200VXR Routers, page 1-9
- Cisco 7301 Router, page 1-9

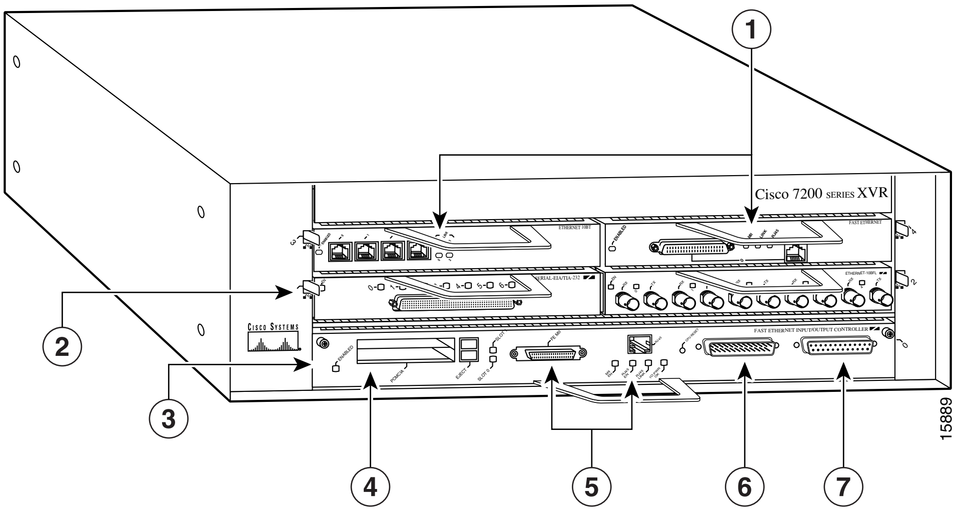
The SA-VAM2+ is supported in the port adapter slots on the Cisco 7200VXR series routers, and the Cisco 7301 routers. It is also supported in the Port Adapter Jacket Card that installs in the I/O controller port of the Cisco 7200VXR routers with the NPE-G1 or NPE-G2 processors.

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

Cisco 7200VXR Routers

See Figure 1-5 for the input/output controller and ports for the Cisco 7200VXR routers.

Figure 1-5 Cisco 7200VXR Slot Numbering



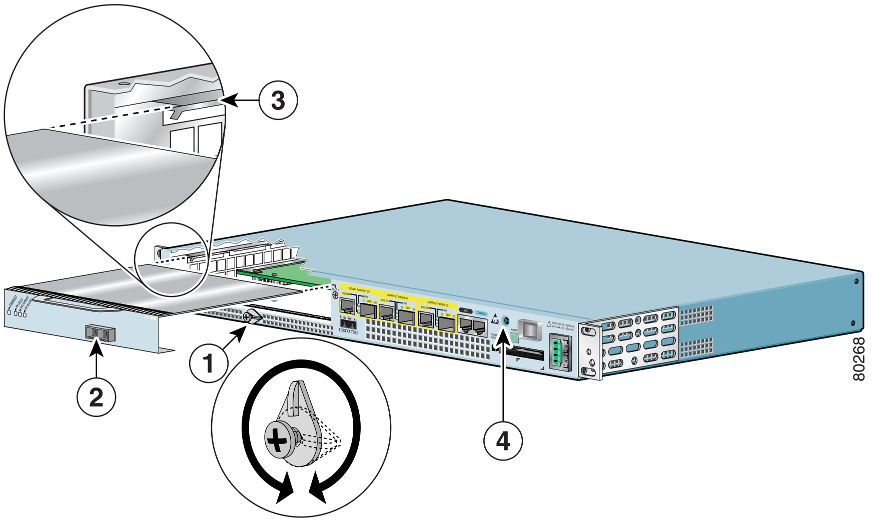
1	Port adapter	**5**	MII and RJ-45 Fast Ethernet ports
2	Port adapter latch	**6**	Auxiliary port
3	I/O controller	**7**	Console port
4	PC card slots		

Cisco 7301 Router

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

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

Figure 1-6 Cisco 7301 Slot Numbering



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