Overview

This chapter describes the VPN Acceleration Module 2+ (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.

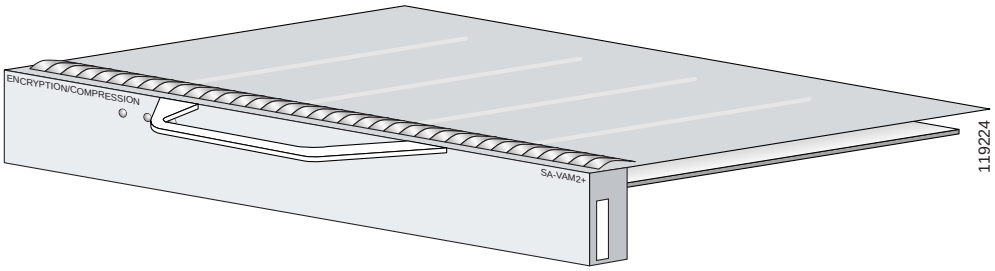
  The AH protocol uses various authentication algorithms; Cisco IOS software has implemented the mandatory MD5 and SHA (HMAC variants) authentication algorithms. The AH protocol provides antireplay services.
- ESP—Encapsulating Security Payload, a security protocol, provides data privacy services, optional 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. 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.

VAM2+ Overview

The VPN Acceleration Module 2+ (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, or the NPE-G1 processor, and the Cisco 7301 router.

VAM2+ features hardware acceleration for Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES), providing increased performance for site-to-site and remote-access IPSec VPN services. The Cisco 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.

Figure 1-1 VAM2+



The 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 260 Mbps
- 128/192/256-bit Advanced Encryption Standard (AES) in hardware
- Performance to OC3 full duplex with 300 byte packets
- 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

Features

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

Table 1-1 VAM2 Features

Feature	Description/Benefit
Throughput[1]	Up to 260 Mbps using 3DES on the Cisco 7200, and up to 370 Mbps using 3DES on the Cisco 7301 **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	14
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
Minimum Cisco IOS software release supported	Cisco IOS Release 12.3(12a)M Cisco IOS Release 12.3(11)T3
Standards supported	IPSec/IKE: RFCs 2401-2411, 2451 IPPCP: RFC 2393, 2395

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.

Performance

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

Table 1-2 Performance for VAM2+

Cisco Router	Throughput[1] [2]	Description
Cisco 7301	Up to 392 Mbps	Cisco IOS: c7301-jk9o3s-mz.123-10 7301/single VAM2+, 1GB system memory 3DES/SHA, preshared with no IKE-keepalive configured
	Up to 396 Mbps	Cisco IOS: c7301-jk9o3s-mz.123-10 7301/single VAM2+, 1GB system memory AES/SHA, preshared with no IKE-keepalive configured
Cisco 7200 with NPE-G1	Up to 292 Mbps	Cisco IOS: c7200-jk9o3s-mz.123-10 7200VXR/NP-G1(700Mhz) /single VAM2+, 512MB system memory 3DES/SHA, preshared with no IKE-keepalive configured
	Up to 295 Mbps	Cisco IOS: c7200-jk9o3s-mz.123-10 7200VXR/NP-G1(700Mhz) /single VAM2+, 512MB system memory AES/SHA, preshared with no IKE-keepalive configured
	Up to 527 Mbps	Cisco IOS: c7200-jk9o3s-mz.123-10 7200VXR/NP-G1(700Mhz) /dual VAM2+, 512MB system memory 3DES/SHA, preshared with no IKE-keepalive configured
	Up to 533 Mbps	Cisco IOS: c7200-jk9o3s-mz.123-10 7200VXR/NP-G1(700Mhz) /dual VAM2+, 512MB system memory AES/SHA/IPSec/Tunnel Mode, preshared
Cisco 7200 with NPE-400	Up to 349 Mbps	Cisco IOS: c7200-jk9o3s-mz.123-10 7200VXR/NPE400/VAM2+, 512MB system memory 3DES/SHA, preshared with no IKE-keepalive configured
	Up to 353 Mbps	Cisco IOS: c7200-jk9o3s-mz.123-10 7200VXR/NPE400/single VAM2+, 512MB system memory AES/SHA, preshared with no IKE-keepalive configured
Cisco 7200 with NPE-225	Up to 191 Mbps	Cisco IOS: c7200-jk9o3s-mz.123-10 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.

Supported Standards, MIBs, and RFCs

This section describes the standards, Management Information Bases (MIBs), and Request for Comments (RFCs) supported on the 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 VAM2+ has three LEDs, as shown in Figure 1-2. Table 1-3 lists the colors and functions of the LEDs.

Figure 1-2 VAM2+ LEDs

Table 1-3 VAM2+ LEDs

	LED Label	Color	State	Function
1	ENABLE	Green	On	Indicates the VAM2+ is powered up and enabled for operation.
2	BOOT	Amber	On	Indicates the 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 VAM2+ is correctly connected to the backplane and receiving power.
- The system bus recognizes the 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 VAM2+, so there are no cables, connectors, or pinouts.

Slot Locations

The topics in this section include:

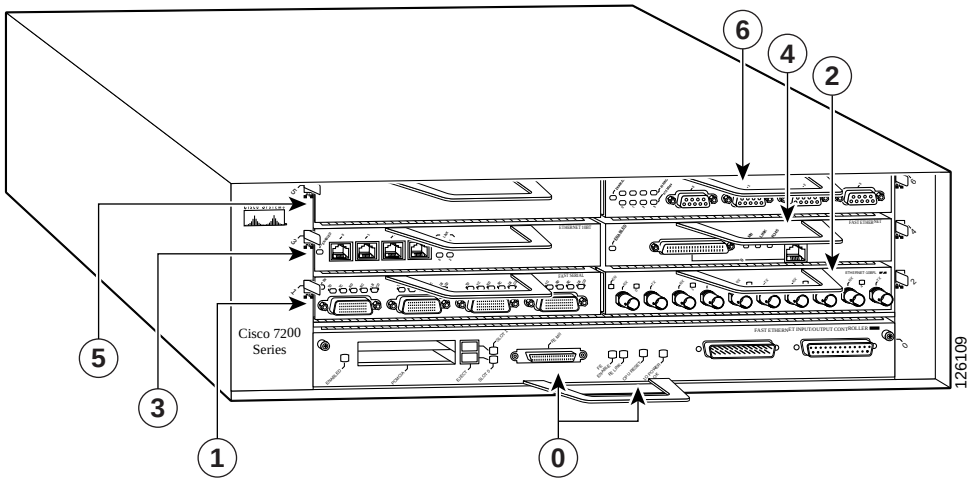
The VAM2+ is supported in the port adapter slots on the Cisco 7204VXR, the Cisco 7206VXR, and the Cisco 7301 routers.

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

Cisco 7200VXR Series Routers

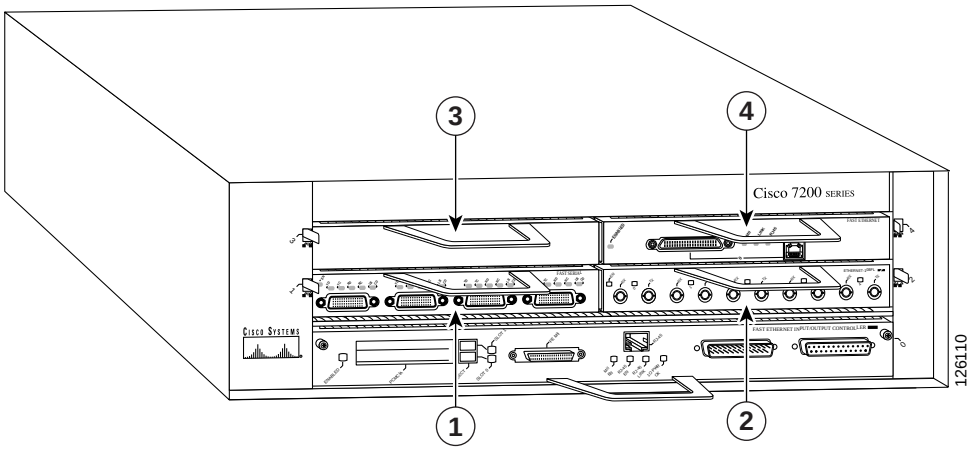
See Figure 1-3, and Figure 1-4 for the slot numbering for the Cisco 7200VXR series routers.

Figure 1-3 Cisco 7206VXR Slot Numbering



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

Figure 1-4 Cisco 7204VXR Slot Numbering



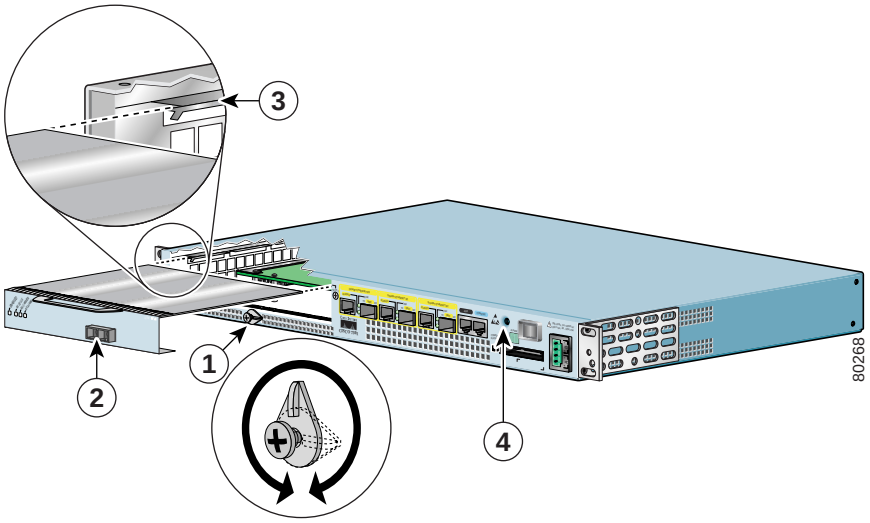
1	Port adapter slot 1	**3**	Port adapter slot 3
2	Port adapter slot 2	**4**	Port adapter slot 4

Cisco 7301 Router

See Figure 1-5 for the slot numbering for the Cisco 7301 router.

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

Figure 1-5 Cisco 7301 Slot Numbering



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