



Overview

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

- [Data Encryption Overview, page 1-1](#)
- [VSA Overview, page 1-2](#)
- [Hardware Required, page 1-4](#)
- [Features, page 1-4](#)
- [Supported Standards, MIBs, and RFCs, page 1-5](#)
- [Enabling/Disabling the VSA, page 1-5](#)
- [LEDs, page 1-7](#)
- [Connectors, page 1-8](#)
- [Slot Locations, page 1-8](#)

Data Encryption Overview

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



Note

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

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

Cisco follows these data encryption standards:

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

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

The component technologies implemented for IPSec include:

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

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

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

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

VSA Overview

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

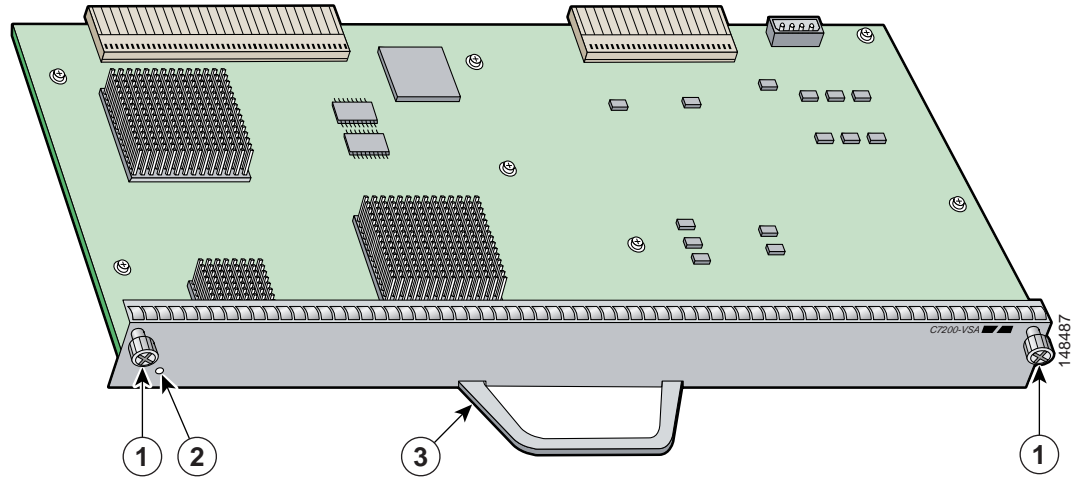


Note

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

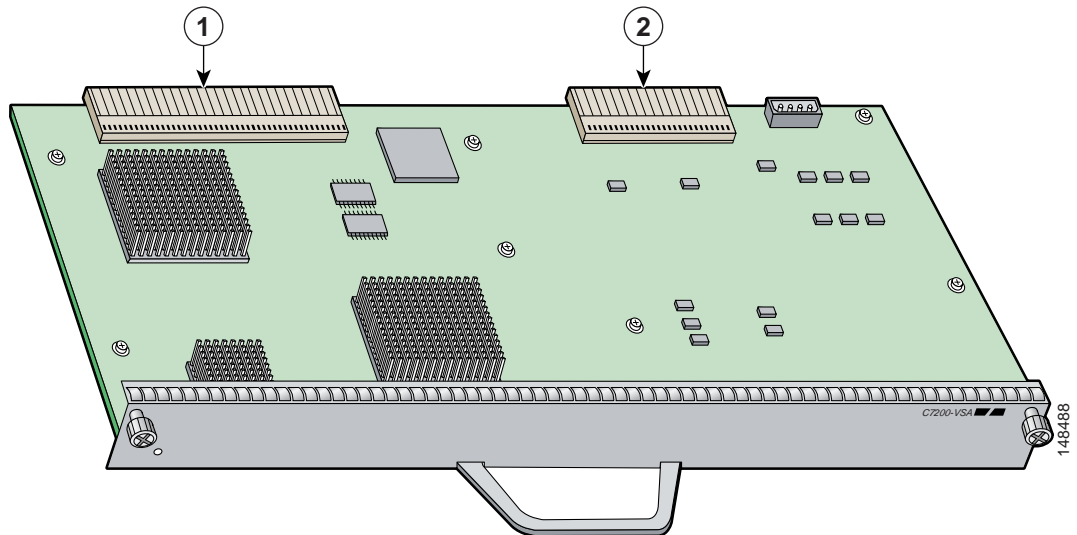
The VSA features hardware acceleration for Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES), providing increased performance for site-to-site and remote-access IPsec VPN services. The Cisco C7200 VSA solution provides quality of service (QoS), multicast and multiprotocol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

Figure 1-1 VSA Module - Front View



1	Screws	3	Handle
2	Status LED light		

Figure 1-2 VSA Module - Rear Connectors



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

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

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

Hardware Required

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

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

Features

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

Table 1-1 VSA Features

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

1. As measured with IPSec 3DES HMAC-SHA1 on 1400 byte packets.
2. Number of tunnels supported varies based on the total system memory installed.
3. On the NPE-G2, the minimum memory requirement is 1 GB of memory.

Performance

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

Table 1-2 Performance for VSA

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

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

Supported Standards, MIBs, and RFCs

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

Standards

- IPSec/IKE: RFCs 2401-2411, 2451

MIBs

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

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

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

RFCs

- IPSec/IKE: RFCs 2401-2411, 2451

Enabling/Disabling the VSA

This section includes the following topics:

- [Disabling the VSA during Operation, page 1-6](#)
- [Enabling/Disabling Scheme, page 1-6](#)

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

Disabling the VSA during Operation

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



Caution

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

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

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

Enabling/Disabling Scheme

This section describes how the VSA operates without OIR support.

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

[Table 1-4](#) describes what occurs when the system is in run-time operation.

[Table 1-5](#) describes what occurs when the **crypto engine** command is entered.

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

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

Table 1-4 System is in Run-time Operation

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

Table 1-5 crypto engine Command

Command	Description of VSA Behavior
<code>Crypto engine slot 0</code> <code>Crypto engine accelerator 0</code>	This allows the VSA to come up and be registered as a crypto engine with the system.
Note The VSA can only be inserted in slot 0 (the I/O controller slot).	If you just performed this configuration and the VSA is currently disabled, reload or reset the system to bring the VSA up. Note The current crypto engine will be still running, and the VSA will take over after the next system reboot.
<code>No crypto engine slot 0</code> <code>No crypto engine accelerator 0</code>	These CLIs will disable the VSA. This is a configuration setting, so the VSA will remain disabled until you remove this configuration and system reloads or resets.

LEDs

The VSA has one LED, as shown in [Figure 1-3](#).

Figure 1-3 VSA LED



Table 1-6 VSA LED

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

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

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

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

Connectors

See [Figure 1-2](#) for the VSA connectors.

Slot Locations

This section includes the following topics:

- [Cisco 7204VXR Router, page 1-8](#)
- [Cisco 7206VXR Router, page 1-10](#)

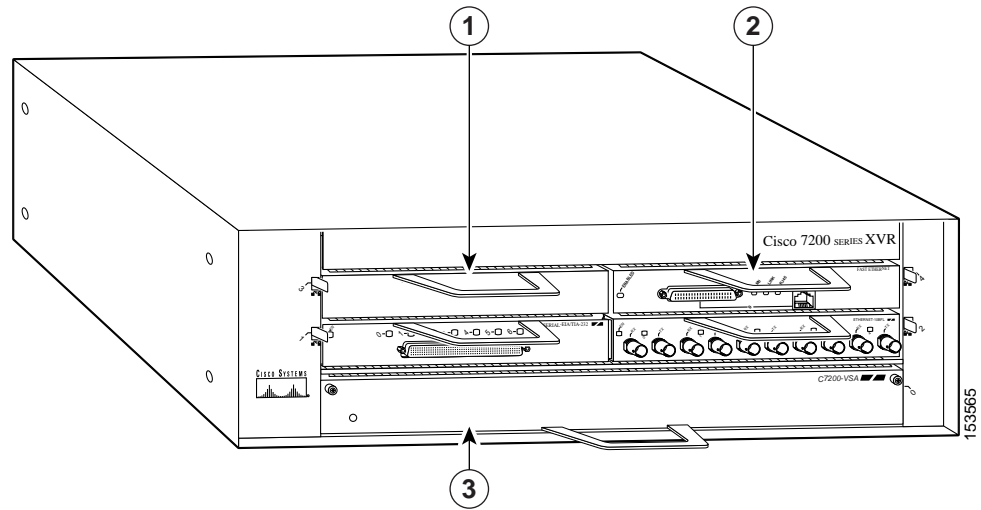
See [Figure 1-4](#) for the slot numbering for the Cisco 7204VXR router.

See [Figure 1-5](#) for the slot numbering for the Cisco 7206VXR router.

Cisco 7204VXR Router

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

Figure 1-4 Cisco 7204VXR Router - Front View

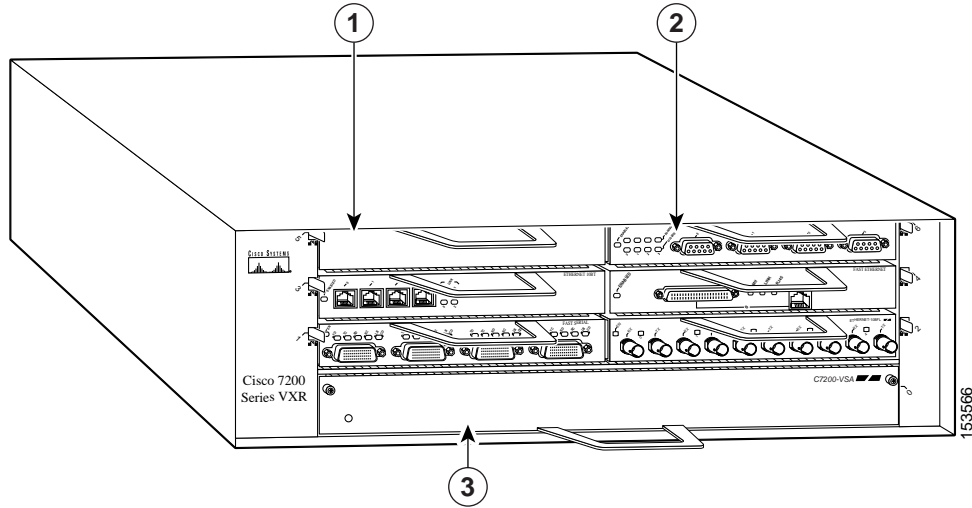


1	Port adapter	3	VSA in I/O controller slot
2	Port adapter lever		

Cisco 7206VXR Router

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

Figure 1-5 Cisco 7206VXR - Front View



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