Preparing for Installation

This chapter describes the general equipment, safety, and site preparation requirements for installing the C7200 VSA (VPN Services Adapter). This chapter contains the following sections:

Required Tools and Equipment

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

- VSA
- 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

Hardware and Software Requirements

This section describes the minimum software and hardware requirements for the VSA:

Software Requirements

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

Platform	Recommended Minimum Cisco IOS Release
Cisco 7204VXR Cisco 7206VXR	12.4(4)XD3 fc2

To check the minimum software requirements of Cisco IOS software with the hardware installed on your router, Cisco maintains the Software Advisor tool on Cisco.com. Registered Cisco Direct users can access the Software Advisor at: http://www.cisco.com/cgi-bin/Support/CompNav/Index.pl. This tool does not verify whether modules within a system are compatible, but it does provide the minimum Cisco IOS software requirements for individual hardware modules or components.

Note Access to this tool is limited to users with Cisco.com login accounts.

Hardware Requirements

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

- The VSA is compatible with the Cisco NPE-G2 processor on the Cisco 7204VXR or Cisco 7206VXR routers.

  The Cisco NPE-G2 is the latest routing engine for the Cisco 7204VXR and 7206VXR, which provides the highest performance and scalability within the family of network processing engines (NPEs).
- ROMmon requirement—12.4(4r)XD5
- I/O FPGA requirement—0x25 (decimal 0.37)
- VSA FPGA requirement—0x13 (decimal 0.19)

Restrictions

The VSA has the following restrictions:

- VSA does not interoperate with other ISA or VAM/VAM2/VAM2+ crypto cards in the same router. The VAM/VAM2/VAM2+ crypto cards are disabled when the VSA is active in the Cisco 7200VXR series routers with the NPE-G2 processor.
- Only a single VSA card is supported on the Cisco 7200VXR series routers with the NPE-G2 processor.

Note Only Cisco 7200VXR series routers with the NPE-G2 processor are supported.

- The VSA module does not support Online Insertion and Removal (OIR). See "Enabling/Disabling the VSA" section on page 1-6 for details.
- Per packet count details for crypto map ACL are not displayed when the **show access-list** command is entered.

  Use other counters, such as the output from the **show crypto ipsec sa** and **show crypto engine accelerator statistics 0** commands, to determine if the VSA is processing the packets.
- An anti-replay window size of 1024 is not supported.

Online Insertion and Removal (OIR)

The VSA plugs into the I/O controller slot of the Cisco 7200VXR series chassis. 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 (see "Enabling/Disabling the VSA" section on page 1-6). The VSA is ready for removal after the disabling CLI command is executed.

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

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.

For more information on OIR, go to "Enabling/Disabling the VSA" section on page 1-6.

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.**

Hazardous voltage or energy is present on the backplane when the system is operating. Use caution when servicing.

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.