CHAPTER 1

Overview of the VPN Services Port Adapter

This chapter provides an overview of the features of the VPN Services Port Adapter (VSPA).

This chapter includes the following sections:

Overview of the VSPA

The VPN Services Port Adapter (VSPA) is a Gigabit Ethernet IP Security (IPsec) cryptographic module that you can install in a Catalyst 6500 Series switch using the Services SPA Carrier-600 (SSC-600). The VSPA provides hardware acceleration for IPsec encryption and decryption, generic routing encapsulation (GRE), and Internet Key Exchange (IKE) key generation.

The VSPA acts as a bump-in-the-wire (BITW) in the data path to perform policy enforcement and bulk encryption and forwarding while the supervisor module performs session establishment, key management, and other features. BITW is an IPsec implementation that starts egress packet processing after the IP stack has finished with the packet and completes ingress packet processing before the IP stack receives the packet.

The VSPA can use multiple Fast Ethernet or Gigabit Ethernet ports on other Catalyst 6500 Series switch modules to connect to the Internet through WAN routers. Physical ports may be attached to the VSPA through a VLAN called the port VLAN. Packets received from the WAN routers pass through the VSPA for IPsec processing. The packets are output on a dedicated VLAN called the interface VLAN or inside VLAN. Depending on the configuration mode (VRF mode or crypto-connect mode), the interface VLAN or port VLAN may be configured explicitly or may be allocated implicitly by the system.

On the LAN side, traffic between the LAN ports can be routed or bridged on multiple Fast Ethernet or Gigabit Ethernet ports. Because the LAN traffic is not encrypted or decrypted, it does not pass through the VSPA.

The VSPA does not route, maintain routing information, or change the MAC header of a packet (except for the VLAN ID from one VLAN to another).

System Components

The cryptographic module consists of the following two components:

Description	Model Number
Services SPA Carrier-600 (SSC-600)	WS-SSC-600
VPN Services Port Adapter (VSPA)	WS-IPSEC-3

For details about the hardware installation and the physical characteristics of the VSPA and the SSC-600, see the *Cisco VPN Services Port Adapter Hardware Installation Guide*.

SSC-600

The SSC-600 inserts into a Catalyst 6500 Series switch chassis slot in the same manner as a line card and provides two subslots that are used to contain one or two VSPAs.

The SSC-600 supports online insertion and removal (OIR) with VSPAs present in the subslots. The VSPA also supports OIR and can be inserted or removed independently from the SSC-600.

VSPA

The VSPA inserts into a subslot of the SSC-600. The SSC-600 can hold one or two VSPAs.

The VSPA supports online insertion and removal (OIR). VSPAs can be inserted or removed independently from the SSC-600. The SSC-600 also supports online insertion and removal (OIR) with VSPAs inserted in its subslots.

Software Requirements

The Cisco IOS Release requirements for the VSPA are as follows:

Model	Cisco IOS Release
VSPA (WS-IPSEC-3)	12.2(33)SXI or later

In addition to the required Cisco IOS Release, you must be running one of the following crypto images on your switch:

- Supervisor Engine 720 (including 10G)

  - s72033-adventerprisek9_wan-mz
  - s72033-advipservicesk9_wan-mz
  - s72033-adventerprisek9_wan-vz
  - s72033-advipservicesk9_wan-vz
- Supervisor Engine 32 (including 10G)
  - s3223-adventerprisek9_wan-mz
  - s3223-advipservicesk9_wan-mz
  - s3223-adventerprisek9_wan-vz
  - s3223-advipservicesk9_wan-vz

Interoperability

This section lists the supervisor engines, service modules, and line cards that are compatible with the VSPA.

Table 1-1 lists the supervisor engine support for each release.

Table 1-1 Supervisor Engine Support for the VSPA by Release

		Cisco IOS Release 12.2
Supervisor	**Description**	SXI
WS-SUP720-3B	Supervisor Engine 720 Fabric MSFC3 PFC3B	Y
WS-SUP720-3BXL	Supervisor Engine 720 Fabric MSFC3 PFC3BXL	Y
VS-S720-10G-3C	Supervisor Engine 720 with 2 ports 10GbE MSFC3 PFC3C	Y
VS-S720-10G-3CXL	Supervisor Engine 720 with 2 ports 10GbE MSFC3 PFC3CXL	Y
WS-SUP32-GE-3B	Supervisor Engine 32 with 8 GbE uplinks and PFC3B	Y
WS-SUP32-10GE-3B	Supervisor Engine 32 with 2 ports 10GbE and PFC3B	Y

Table 1-2 lists the service module support for each release.

Table 1-2 Service Module Support by Release

	Cisco IOS Release 12.2
Service Module	**SXI**
Firewall Services Module (WS-SVC-FWM-1-K9)	Y

Table 1-2 Service Module Support by Release (continued)

Service Module	Cisco IOS Release 12.2 SXI
Intrusion Detection System Module 2 (WS-SVC-IDS2BUNK9)	N
Network Analysis Module 2 (WS-SVC-NAM-2)	Y

Table 1-3 lists the SIP and SSC support for each release.

Table 1-3 SIP and SSC Support by Release

Line Card or Module	Cisco IOS Release 12.2 SXI
7600-SIP-200	Y
7600-SIP-400	Y
7600-SIP-600	Y
7600-SSC-400	Y
WS-SSC-600	Y

Table 1-4 lists the Ethernet line card and module support for each release.

Table 1-4 Ethernet Line Card and Module Support by Release

Line Card or Module	Cisco IOS Release 12.2 SXI
SPA-1X10GE	SIP-600
SPA-10X1GE[1]	SIP-600
SPA-2X1GE	SIP-400
SPA-2XT3/E3	N
SPA-4X1FE-TX-V2	N
SPA-5X1GE[1]	SIP-600
SPA-5X1GE-V2	N
SPA-8X1FE-TX-V2	N
WS-X6148-GE-TX	Y
WS-X6148-RJ-21	Y
WS-X6148-RJ-21V	Y
WS-X6148-RJ-45	Y
WS-X6148-RJ-45V	Y

Table 1-4 Ethernet Line Card and Module Support by Release (continued)

	Cisco IOS Release 12.2
Line Card or Module	**SXI**
WS-X6408A-GBIC	Y
WS-X6416-GBIC	Y
WS-X6502-10GE	Y
WS-X6516-GBIC	Y
WS-X6516-GE-TX	Y
WS-X6516A-GBIC	Y
WS-X6548-GE-TX	Y
WS-X6548-RJ-45	Y
WS-X6704-10GE	Y
WS-X6708-10GE	Y
WS-X6716-10GE	Y
WS-X6748-GE-TX	Y
WS-X6748-SFP	Y
WS-X6724-SFP	Y

1. Subinterfaces on SPA-5X1GE and SPA-10X1GE are not supported in any release.

Table 1-5 lists the ATM line card and module support for each release.

Table 1-5 ATM Line Card and Module Support by Release

	Cisco IOS Release 12.2
Line Card or Module	**SXI**
SPA-1XCHSTM1/OC3	N
SPA-1XOC48-ATM	SIP-400
SPA-2XOC3-ATM	SIP-200 SIP-400
SPA-4XOC3-ATM	N

Table 1-6 lists the POS line card and module support for each release.

Table 1-6 POS Line Card and Module Support by Release

	Cisco IOS Release 12.2
Line Card or Module	**SXI**
SPA-1XOC12-POS	SIP-400
SPA-1XOC48POS/RPR	N
SPA-2XOC3-POS	SIP-200 SIP-400
SPA-OC192POS-XFP	SIP-600

Table 1-7 lists the serial line card and module support for each release.

Table 1-7 Serial Line Card and Module Support by Release

	Cisco IOS Release 12.2
Line Card or Module	**SXI**
SPA-2XCT3/DS0	SIP-200 SIP-400
SPA-2XT3/E3	N
SPA-4XCT3/DS0	N
SPA-4XT3/E3	N
SPA-8XCHT1/E1	N
WS-6182-2PA	N
WS-6802-2PA	N
WS-X6582-2PA With the following PAs: PA-A3-OC3MM PA-POS-OC3MM PA-POS-2OC3 PA-MC-2T3+ PA-1FE-TX[1] PA-2FE-TX[1]	Y

1. Subinterfaces on PA-1FE-TX and PA-2FE-TX are not supported in any release.

Note The VSPA does not support OSM modules.

Restrictions

The VSPA is subject to the following restrictions:

- The SSC-600 and the VSPA require Cisco IOS Release 12.2(33)SXI or a later release.
- The VSPA is supported only on the SSC-600.
- The SSC-600 supports only the VSPA. It does not support any other modules.
- You can install the VSPA in all Catalyst 6500 Series switch models, including the E and non-E switch chassis, except the Catalyst 6503.

  For more information on the Catalyst 6500 Series switch, see the *Catalyst 6500 Series Switches Installation Guide* at this URL:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Chassis_Installation/Cat6500/6500_ins.html
- The MSFC DRAM requirements are as follows:

  – Up to 8,000 tunnels with 512-MB DRAM
  – Up to 16,000 tunnels with 1-GB DRAM

  These numbers allow for available memory for routing protocols and other applications. However, your particular use of the MSFC may demand more memory than the quantities that are listed above. In an extreme case, you could have one tunnel but still require 1-GB DRAM for other protocols and applications running on the MSFC.
- A maximum of 10 VSPAs per chassis are supported.
- VSPA state information is not maintained between the active and standby supervisor engine during normal operation. During a supervisor engine switchover in an SSO environment, the VSPA will reboot.
- GRE keepalives are not supported if **crypto engine gre vpnblade** is configured.

Supported MIBs

The following MIB is supported for the SSC-600 and the VSPA on a Catalyst 6500 Series switch:

- CISCO-IPSEC-FLOW-MONITOR-MIB

Note Gigabit Ethernet port SNMP statistics (for example, ifHCOutOctets and ifHCInOctets) are not provided for the internal VSPA trunk ports because these ports are not externally operational ports and are used only for configuration.

For more information about MIB support on a Catalyst 6500 Series switch, refer to the *Cisco 7600 Series Router MIB Specifications Guide*, at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/mibgde6.html

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

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

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

Using the Command-Line Interface

The software interface for the VSPA is the Cisco IOS command-line interface (CLI). To understand the Cisco IOS command-line interface and Cisco IOS command modes, see the *Cisco IOS Configuration Fundamentals Command Reference* at this URL:

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html

Commands specific to the Cisco IOS software release 12.2SX are described in the *Cisco IOS Master Command List, Release 12.2SX* at this URL:

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

For detailed information on configuring the security features of the VSPA, see the *Cisco IOS Security Configuration Guide, Release 12.2* at this URL:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html

For detailed information on configuring the Catalyst 6500 Series switch, see the *Catalyst 6500 Series Switch Software Configuration Guide, Release 12.2SXH* at this URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/book.html

Identifying Slots, Subslots, and Ports

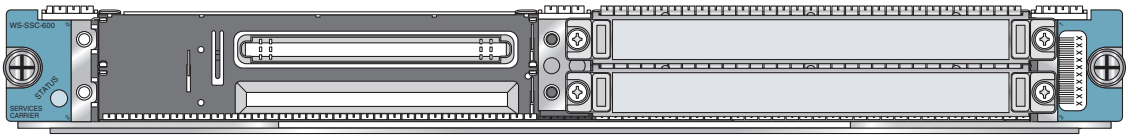
Some CLI commands, such as the **show idprom module** and **show hw-module subslot** commands, allow you to display information about the VSPA and the SSC-600. These commands require you to specify the physical location of the SSC-600 in the format *slot*, or the physical location of the VSPA in the format *slot/subslot*.

- *slot*—Specifies the chassis slot number in the Catalyst 6500 Series switch where the SSC-600 is installed.
- *subslot*—Specifies the secondary slot of the SSC-600 where the VSPA is installed.

The subslot numbering is indicated by a small numeric label beside the subslot on the faceplate of the SSC-600. In the horizontal card orientation shown in Figure 1-1, the SSC-600 subslot locations are as follows:

- Subslot 0—Left subslot (top subslot if vertical)
- Subslot 1—Right subslot (bottom subslot if vertical)

Figure 1-1 SSC-600 Faceplate



For example, to display the operational status of the VSPA installed in the first subslot of the SSC-600 in slot 6 of a Catalyst 6500 Series switch, enter the following command:

```
Router# show hw-module subslot 6/0 oir
```

Some CLI commands require you to specify the inside and outside ports of the VSPA in the format *slot/subslot/port*. Although the VSPA ports are not actual Gigabit Ethernet ports, and do not share all properties of external Gigabit Ethernet interfaces, they can be addressed for configuration as Gigabit Ethernet trunk ports, using port numbers as follows:

- Port 1—Inside port, attached to interface VLAN
- Port 2—Outside port, attached to port VLAN

For example, to configure the outside port of a VSPA in the first subslot (subslot 0) of an SSC-600 in slot 6 of a Catalyst 6500 Series switch, enter the following command:

```
Router(config)# interface GigabitEthernet6/0/2
```

VSPA Hardware Configuration Guidelines

The hardware configuration guidelines for the VSPA are as follows:

- A VSPA in a chassis is active only if power to the subslot is enabled. Use the [**no**] **hw-module subslot** *slot/subslot* **shutdown** [**powered** | **unpowered**] command in global configuration mode to enable or disable power to the VSPA. The **powered** option resets power to the specified subslot, and the **unpowered** option disables power to the specified subslot. Use the [**no**] **power enable module** *slot* command to enable or disable power to the SSC-600.

- When you remove a VSPA that has some ports participating in crypto connections, the crypto configuration remains intact. When you reinsert the same type of VSPA into the same slot, the crypto connections will be reestablished. To move the VSPA to a different slot, you must first manually remove the crypto connections before removing the VSPA. You can enter the **no crypto connect vlan** command from any interface when the associated physical port is removed.
- When you reboot a VSPA that has crypto connections, the existing crypto configuration remains intact. The crypto connections will be reestablished after the VSPA reboots. When a crypto connection exists but the associated interface VLAN is missing from the VSPA inside port, the crypto connection is removed after the VSPA reboots.
- When you remove a port VLAN or an interface VLAN with the **no interface vlan** command, the associated crypto connection is also removed.

Displaying the Module Hardware Type

There are several commands on the Catalyst 6500 Series switch that provide VSPA hardware information.

- To verify the module hardware type that is installed in your switch, use the **show module** command.
- To display hardware information for the VSPA, use the **show crypto eli** command.
- To display platform and network interface controller statistics for the VSPA, use the **show crypto engine accelerator statistic** command.

For more information about these commands, see the *Cisco IOS Master Command List, Release 12.2SX* at this URL:

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

Table 1-8 shows the hardware description that appears in the **show module** command output for a VSPA on the Catalyst 6500 Series switch.

Table 1-8 Module Hardware Description in show module Command

Module	Description in show module Command
VSPA	WS-IPSEC-3

Example of the show module Command

The following example of the **show module** command reports an operational SSC-600 in slot 4 and an operational VSPA in slot 4, subslot 0:

```
Router# show module 4
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  4    0  2-subslot Services SPA Carrier-600     WS-SSC-600         JAB113100EN

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  4  001a.a2ff.1320 to 001a.a2ff.1327   0.302 12.2(SIERRA_ 12.2(SIERRA_ Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ----------- ------- -------
 4/0 IPSec Accelerator 3         WS-IPSEC-3         PRTA6104008  0.38   Ok
```

```
Mod  Online Diag Status
---- -------------------
  4  Pass
 4/0 Pass
```

Example of the show crypto eli Command

The following example shows output from the **show crypto eli** command on a Catalyst 6500 Series switch with a VSPAs installed in subslot 0 of an SSC-600 that is installed in slot 3. The output displays how many IKE-SAs and IPsec sessions are active and how many Diffie-Hellman keys are in use for each VSPA.

```
Router# show crypto eli

Hardware Encryption : ACTIVE
 Number of hardware crypto engines = 3

 CryptoEngine WS-IPSEC-3[3/0] details: state = Active
 Capability      :
     IPSEC: DES, 3DES, AES, RSA, IPv6

 IKE-Session   :     0 active, 16383 max, 0 failed
 DH            :     0 active,  9999 max, 0 failed
 IPSec-Session :     0 active, 65534 max, 0 failed
```

Example of the show crypto engine accelerator statistic Command

The following example shows output from the **show crypto engine accelerator statistic** command on a Catalyst 6500 Series switch with a VSPA in subslot 0 of a SSC-600 that is installed in slot 4. The output displays platform statistics for the VSPA and also displays the network interface controller statistics.

```
Router# show crypto engine accelerator statistic slot 4/0 detail

VPN module in slot 4/0:

Decryption Side Data Path Statistics
====================================
Packets RX..............: 7
Packets TX..............: 4
IPSec Transport Mode.....: 4
IPSec Tunnel Mode........: 0
AH Packets..............: 0
ESP Packets.............: 4
GRE Decapsulations.......: 0
NAT-T Decapsulations.....: 0
Clear...................: 0

Packets Drop............: 3
Authentication Errors....: 0
Decryption Errors........: 0
Replay Check Failed......: 0
Policy Check Failed......: 0
GRE Errors..............: 0
SPD Errors..............: 0
HA Standby Drop..........: 0
Hard Life Drop..........: 0
Invalid SA..............: 0
```

```
Reassembly Frag RX.......: 0

Decryption Side Controller Statistics
=====================================
Frames RX................: 24
Bytes RX.................: 5592
Mcast/Bcast Frames RX....: 0
RX Less 128Bytes.........: 12
RX Less 512Bytes.........: 12
RX Less 1KBytes..........: 0
RX Less 9KBytes..........: 0
RX Frames Drop...........: 0

Frames TX................: 4
Bytes TX.................: 552

Encryption Side Data Path Statistics
====================================
Packets RX...............: 24
Packets TX...............: 4
IPSec Transport Mode.....: 4
IPSec Tunnel Mode........: 0
GRE Encapsulations.......: 0
NAT-T Encapsulations.....: 0
LAF prefragmented........: 0
Fragmented...............: 0
Clear....................: 0

Packets Drop.............: 20
Encryption Errors........: 0
HA Standby Drop..........: 0
Hard life Drop...........: 0
Invalid SA...............: 0
ICMP Unreachable DF set..: 0

Reassembly Frag RX.......: 0

Encryption Side Controller Statistics
=====================================
Frames RX................: 24
Bytes RX.................: 5456
Mcast/Bcast Frames RX....: 0
RX Less 128Bytes.........: 16
RX Less 512Bytes.........: 8
RX Less 1KBytes..........: 0
RX Less 9KBytes..........: 0
RX Frames Drop...........: 0

Frames TX................: 4
Bytes TX.................: 416
```