CHAPTER 8

IPSec VPN Acceleration Services Module

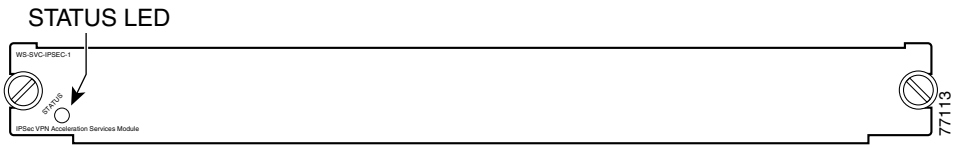
This chapter describes the IPSec VPN Acceleration Services Module (WS-SVC-IPSEC-1).

The IPSec VPN Acceleration Services module is a Gigabit Ethernet IPSec cryptographic module that you can install in the Cisco 7600 series routers. (See Figure 8-1.) The VPN module provides bump-in-the-wire (BITW) IPSec implementation using VLANs.

Note 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.

Note Specific combinations of supervisor engines and modules may not be supported in your chassis. Refer to the release notes of the software version running on your system for specific information on modules and supervisor engine combinations that are not supported.

Figure 8-1 IPSec VPN Acceleration Services Module (WS-SVC-IPSEC-1)



Configuring VPNs using the VPN module is similar to configuring VPNs on routers running Cisco IOS software. When you configure VPNs with the VPN module, you attach crypto maps to VLANs (using interface VLANs); when you configure VPNs on routers running Cisco IOS software, you configure individual interfaces.

Note With the VPN module, crypto maps are still attached to individual interfaces, but the set of interfaces allowed is restricted to “interface VLANs.”

When you configure a VPN on the Cisco routers, a packet is sent to a routed interface that is associated with an IP address. If the interface has an attached crypto map, the software checks that the packet is on an access control list (ACL) specified by the crypto map. If a match occurs, the packet is transformed (encrypted) before it is routed to the appropriate IPSec peer; otherwise, the packet is routed in the *clear* (unencrypted) state.

When you configure the VPN module, the same cryptographic operations are performed as on Cisco routers. The VPN module's implementation of VPN is generally the same as on Cisco routers other than the use of interface VLANs and some configuration guidelines specific to the VPN module.

Note For detailed information on Cisco IOS IPSec cryptographic operations and policies, refer to the "IP Security and Encryption" section of the *Cisco IOS Security Configuration Guide*, Release 12.2.

When you configure the VPN module on the Cisco 7600 series routers, you ensure that all packets coming from or going to the Internet pass through the VPN module. The VPN module has an extensive set of policies that validate a packet before the packet is sent onto the local (trusted) LAN. The VPN module can use multiple Fast Ethernet or Gigabit Ethernet ports on other Cisco 7600 series routers modules to connect to the Internet. Packets received from the WAN routers pass through the VPN module for IPSec processing.

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

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

The front panel LED on the IPSec VPN Acceleration Services Module is described in Table 8-1.

Table 8-1 IPSec VPN Acceleration Services Module STATUS LED

Color/State	Description
Green	All diagnostic tests pass. The module is operational.
Red	A diagnostic test other than an individual port test failed.
Orange	Indicates one of three conditions: • The module is running through its boot and self-test diagnostic sequence. • The module is disabled. • The module is in the shutdown state.
Off	The module power is off.