CHAPTER 16

Adaptive Security Appliance Services Module

This chapter provides information about the firewall solution, Cisco Adaptive Security Appliance Services Module (ASA SM).

This chapter contains the following topics:

Functional Overview of Firewalls

Firewalls protect inside networks from unauthorized access by users on outside networks. A firewall can also protect inside networks from each other, for example, keeping a human resources network separate from a user network. If you want network resources to be made available to an outside user, such as a Web or FTP server, you can place these resources on a separate network behind the firewall, called a demilitarized zone (DMZ). The firewall allows limited access to the DMZ. As the DMZ only includes the public servers, an attack there only affects the servers and does not affect other inside networks. You can also control when inside users access outside networks (for example, the Internet), by allowing only certain addresses out, requiring authentication or authorization, or coordinating with an external URL filtering server.

When discussing networks connected to a firewall, the outside network is in front of the firewall, the inside network is protected and behind the firewall, and a DMZ, while behind the firewall, allows limited access to outside users. Because ASA SM lets you configure many interfaces with varied security policies, including many inside interfaces, many DMZs, and even many outside interfaces if desired, these terms are used in a general sense only.

ASA SM Overview

Cisco Adaptive Security Appliance Services Module (ASA SM) is a high-speed, integrated network security module for Cisco 7600 series routers. ASA SM works with c7600 line cards, and delivers high throughput, low latency, and high availability. ASA SM has more advanced features than the service module, Firewall Services Module (FWSM). Although not all FWSM features are available in ASA SM, ASA SM has bridge groups and mixed context mode support.

ASA SM does not have any external interfaces.The module includes logical interfaces within the router itself. The console port is virtual and accessible directly through the router.

ASA SM Front Panel LEDs

Figure 16-1 shows the ASA SM front panel LEDs, and Table 0-1 describes them.

Figure 16-1 ASA Services Module (WSC-SVC-ASA-SM1-K9)

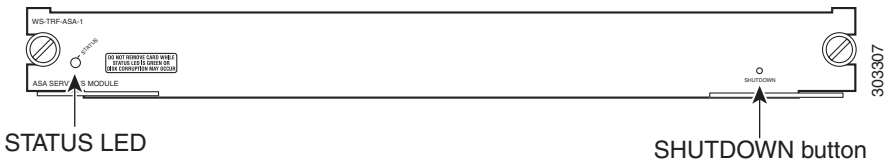

Table 16-1 ASA SM STATUS LED Description

Color/State	Description
Green	All diagnostic tests passed. The module is operational.
Red	A diagnostic test other than an individual port test failed.
Orange	Indicates one of the following 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 power for the firewall module is off.

ASA SM Support

This section lists the support available for ASA SM, the features that ASA SM supports and the extent of the support.

Support for ASA SM

ASA SM is supported on the following:

- 7606-S and 7609-S chassis
- Supervisor Engine 720 3B/ 3BXL, Route Switch Processor 720-1GE, and Route Switch Processor 720-10GE

Support on ASA SM

ASA SM supports the following:

- The 'Autostate' feature which allows the ASA SM blade to quickly detect that an interface connected to a real host has failed
- Over two million firewall rules and 12 GB addressable memory
- Multicast features that include multicast routing protocols like PIM-SM and IGMP stubmode.

  The span reflector that was needed on the Firewall Services Module to pass multicast is no longer required.
- 250 virtual contexts and 1000 VLANs
- Network address translation (NAT) system and global access control lists (ACLs)
- ASA failover mechanism

  The mechanism supports the following: high-speed failover between modules within a single Cisco 7600 chassis and high-speed failover between modules in separate chassis.
- Online diagnostic tests for bootup and periodic health monitoring. Health monitoring tests run at intervals configured by the user. The default interval for tests is 15 seconds.

  The tests include the following:
  - Processor Complex (PC) Loopback Test checks the health of the two backplane ports which form the data-path on ASA SM.
  - PC Device Status Test retrieves the status of the various hardware devices controlled by the processor complex.
  - DataPort Loopback Test initiates a hardware loopback at the datapath field-programmable gate array (FPGA) level with the capability to loop back diagnostic packets on the basis of a VLAN match. This test verifies if the Receive-Side Scaling (RSS) hash algorithm worked over data packets, and identifies the exact drop location of the packet within the FPGA.
  - Management Port Loopback Test initiates a software loopback of diagnostic packets from the inband port to test the health of the two management ports on the router service module. A special global VLAN reserved for the online diagnostic packets uniquely identifies the packet in the system. Run Software Loopback as a bootup, health monitoring, on-demand and scheduled diagnostic test.

Deployment of ASA SM

The ASA SM card can be deployed in 7606-S and 7609-S chassis. You can configure any physical port on the router to operate with firewall policy and protection. ASA SM is Network Equipment-Building System (NEBS) compliant. Slots adjacent to the ASA SM slot are either used or provided with ‘airdam’. Airdam is a blank panel that provides an air shield. Airdam cards in empty slots ensure correct air-flow around the cards.

You can deploy ASA SM in the following modes:

- In the homogeneous mode, only ASA SM resides in the 7600 chassis.
- In the coexistent mode, both ASA SM and FWSM reside in the same router chassis and network, or in the same network, but are managed by separate management tools.
- In the heterogeneous mode, both ASA SM and FWSM are deployed and in operation either in the same router chassis or in the same network, and are managed by the same management tool.

ASA SM Firewall Modes

ASA SM runs in the following firewall modes:

- Routed
- Transparent

Routed Mode

In the routed mode, ASA SM is considered to be a router hop in the network. It can use OSPF or RIP in the single context mode. Routed mode supports many interfaces. Each interface is on a different subnet. You can share interfaces between contexts. ASA SM acts as a router between the connected networks, and each interface requires an IP address on a different subnet. In the single context mode, the routed firewall supports Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP). Multiple context mode only supports static routes. We recommend using the advanced routing capabilities of the upstream and downstream routers instead of relying on ASA SM for extensive routing needs.

Transparent Mode

In the transparent mode, ASA SM is not considered a router hop, but acts like a “bump in the wire,” or a ‘stealth firewall’. ASA SM connects to the same network on its internal and external interfaces.

Use a transparent firewall for the following:

- Simplify your network configuration.
- Make the firewall invisible to attackers.
- Allow traffic that would be blocked in the routed mode. For example, a transparent firewall can allow multicast streams using an Ether Type access list.

Security Context Overview

You can partition a single ASA SM into multiple virtual devices, known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are equivalent to multiple standalone devices. Multiple context mode supports multiple features, routing tables, firewall features, IPS, and management. VPN and dynamic routing protocols are not supported.

In the multiple context mode, ASA SM includes a configuration for each context that identifies the security policy, interfaces, and most options you can configure on a standalone device. System administrators configure contexts to add and manage them in the system configuration.

The following are characteristics of the system configuration:

- Like a single mode configuration, the system configuration is the startup configuration.
- System configuration identifies the basic settings for ASA SM.
- System configuration does not include any network interfaces or network settings for itself. When the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the administrator context. The administrator context is just like any other context. However, it gives the user who logs into the admin context system administrator rights to access the system and all other contexts.

ASA SM Failover Mechanism

Failover supports redundancy in ASA SMs. The failover mechanism helps you configure two ASA SMs. If an ASA SM fails, the redundant ASA SM starts functioning.

ASA SM supports two failover configurations:

- Active-Active failover
- Active-Standby failover

Active-Active failover

Active-Active failover is only available on units that run in the multiple context mode. In this failover, both units can pass network traffic. This failover lets you configure load balancing on your network.

Active-Standby failover

Active-Standby failover is available on units that run in either the single or multiple context mode.

In this failover, one unit passes traffic while the other unit waits in a standby state.

Support on Chassis

ASA SM works with other modules in the router chassis to deliver robust security throughout the entire chassis, effectively making every port a security port. ASA SM and the Firewall Services Module can run simultaneously in the same chassis.

The number of ASA SMs supported on the chassis for centralized and distributed forwarding is as follows:

- Centralized Forwarding supports three ASA SM cards per chassis. Central forwarding has an ingress and an egress supervisor EARL lookup.
- Distributed Forwarding supports four ASA SM cards per chassis. In distributed forwarding, ingress lookup is done by the line-card, and egress lookup is done by the supervisor EARL.

Restrictions and Configuration

Restrictions

The following restrictions apply to ASA SM:

- ASA SM is only supported on the 7606-S and 7609-S chassis. Support for 7613-S and lead free version of 7606-S will become available later.
- ASA SM is not supported on Cisco 7603 and Cisco 7604 routers.

ASA Configuration

ASA SM uses one of the following multi-card configurations to scale bandwidth:

- VLAN-based approach: This approach uses multiple ASA SMs per chassis. Each ASA SM is assigned a distinct set of VLANs. Traffic is assigned to a specific ASA SM based on its incoming or outgoing VLAN tag.
- Policy-based routing approach: This approach is similar to the VLAN-based approach except that the supervisor uses a policy based routing (PBR) scheme based on the source of the traffic, application types, or destination to route packets across multiple ASA SM cards.

Note For information on all ASA SM configurations, see *Cisco ASA Services Module CLI Configuration Guide* available at: http://www.cisco.com/en/US/docs/security/asa/asa84/configuration85/guide/asa_cfg_cli_85.html

Troubleshooting

Command	Execution Location
Debug firewall	RP of Supervisor
Debug trifecta	SP of Supervisor

Debug commands

Requirement	Debug Command
To detect the following: • If SCP messages are dropped between the Supervisor SP or RP and the linecard • To check the SCP communication between the linecard and supervisor • To check whether the firewall slot is up, about the VLAN bitlist, and firewall configuration events • To check port channel IDB configurations for the firewall • To investigate errors of the following kind: errors in VLAN association, errors in port channel configurations of the firewall, SCP errors while initializing the packets, and invalid events	Use the **debug firewall** command.
To detect errors that pertain to major or severe events in the firewall module processes	Use the **debug trifecta** command.

ASA SM Documentation

Cisco ASA Series Documentation is available at:

http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html#wp39663

ASA hardware and software compatibility information is available at:

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

ASA SM compatibility documentation is available at:

http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html#wp45887

ASA SM hardware documentation is available at:

http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html#wp64793

ASA SM quick start documentation is available at:

http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html#wp57515

ASA SM New Features by Release is available at:

http://www.cisco.com/en/US/docs/security/asa/roadmap/asa_new_features.html