Cisco Firewall Services Module Release 4.0

PB530019

This product bulletin introduces the Cisco® Firewall Services Module (FWSM) Release 4.0 and includes the following sections:

- Introduction
- Migration Strategy
- Highlights
- Additional Information

Introduction

Release 4.0 is designed to be mainly focusing on Cisco Catalyst® 6500 switch integration. The main features of this release use the benefits of integrated aspects of a service module. This release follows the last major Release 3.2 on FWSM (April 2007).

The features of Release 4.0 can be divided into the following categories: improved performance, increased scalability, enhanced inspection, expanded routing protocol, and integration with network services such as the Virtual Switching System (VSS). Not all features of this release may be supported on both 6500 and 7600 platforms. Some features have a specific requirement about which Cisco IOS® Software release needs to be running on the supervisor. More detailed information regarding this can be found in the release notes and configuration guide for FWSM Release 4.0 at http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html.

Migration Strategy

FWSM Release 4.0 is the latest maintenance release train for the FWSM product. As with the previous release trains (3.1 and 3.2), Cisco will be offering periodic maintenance releases on 4.0 numbered as 4.0(x). Customers currently operating on Release 3.1(x) or 3.2(x) would be able to upgrade/migrate transparently to the latest 4.0 release.

Release 4.0(4) has been Safe Harbor certified. For more information, visit http://www-europe.cisco.com/en/US/docs/safe_harbor/enterprise/fwsm/4_0_4__12_2_33_SXI/FWSM_4.0.4.pdf.

Highlights

The following sections include FWSM Release 4.0 feature highlights. As mentioned earlier, this release spans multiple categories. Table 1 shows the features divided based on Cisco IOS Software release dependency.

Table 1. Features Requiring Cisco Catalyst 6500 Cisco IOS Software Release 12.2(33)SXI or 12.2(18)ZYA on the Supervisor

Feature	Release 4.0 Rebuild Number
Interoperability with VSS	FWSM Release 4.0(4)
Integration with Cisco Catalyst 6500 Supervisor Engine 32 PISA discovery/detection mechanism (requires Cisco IOS Software Release 12.2(18) ZYA or higher)	FWSM Release 4.0(4)
Route health injection (RHI)	FWSM Release 4.0(4)

Table 2. Features Requiring Cisco Catalyst 6500 Cisco IOS Software Release 12.2(18)SXF and Higher

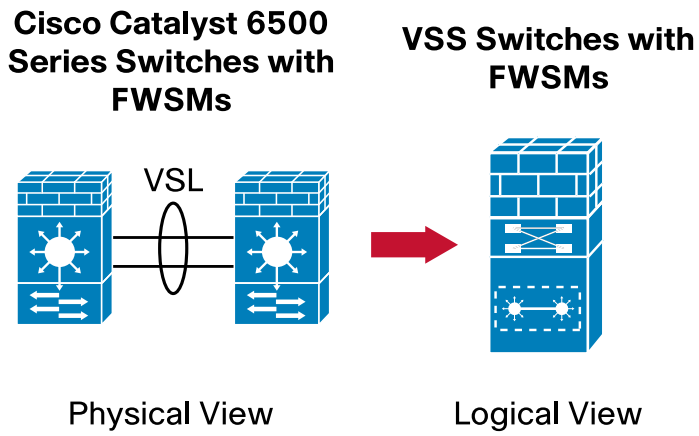
Feature
Increased access list capacity
Flexible and configurable access control list (ACL) rules
Distributed Computing Environment / Remote Procedure Calls (DCERPC)
Enhanced Session Initiation Protocol (SIP)
Enhanced HTTP
Enhanced Simple Mail Transfer Protocol (SMTP)
Enhanced Interior Gateway Routing Protocol (EIGRP)
Dynamic Host Configuration Protocol (DHCP) Option 82
Additional Simple Network Management Protocol (SNMP) MIBs

Interoperability with Virtual Switching System

The VSS is an innovative feature on Cisco Catalyst 6500 Series Switches that effectively allows clustering of two physical chassis together into a single logical entity. Such a technology allows new enhancements in all areas of enterprise campus and data center deployment, including high availability, scalability/performance, management, and maintenance. Service module support is a primary requirement for positioning of the VSS in the enterprise campus and enterprise data center market. FWSM Release 4.0(4) is the first release that will support FWSM integration in a VSS environment (Cisco Catalyst 6500 Series Virtual Switching Supervisor Engine 720 with 10GE uplinks needs to run Cisco IOS Software Release 12.2(33)SXI).

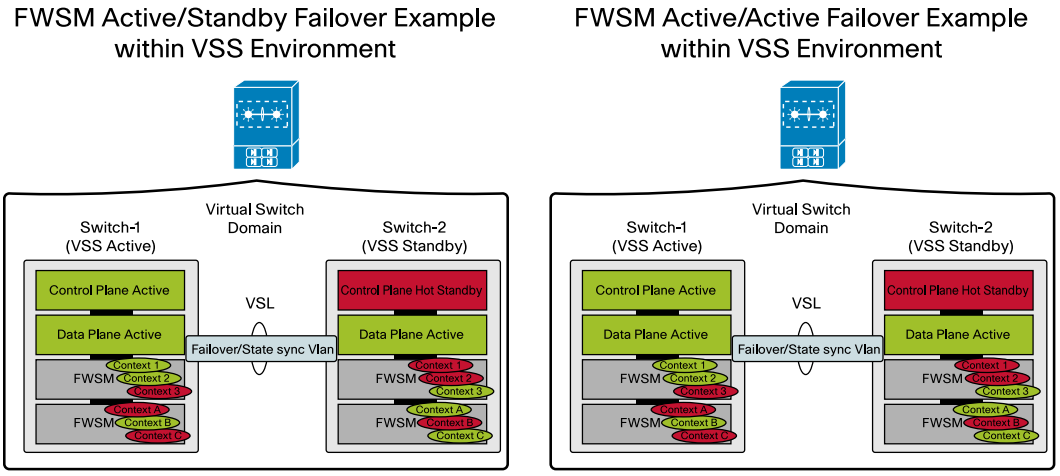
The configuration of FWSM in VSS environment is as transparent as other VSS components (such as Cisco Catalyst 6500 line cards). It is important to note that no special configuration is needed within the FWSM module, and the effect is very well contained within the usual model change associated with VSS and non-VSS mode (standalone mode). The physical and logical representation of FWSM with the Cisco Catalyst 6500 is shown in Figure 1.

Figure 1. VSS logical view



The FWSM modes of operations are left intact when switching from standalone mode to VSS mode. Namely, the FWSM can operate within VSS environment in single mode/multimode as well as routed or transparent mode. The standalone inter-/intrachassis failover units are supported in this model as well as both active/standby and active/active. (See Figure 2.)

Figure 2. VSS HA model



The highlights of FWSM VSS integration requirements and limitations are described here:

- Cisco Catalyst 6500 Series Virtual Switching Supervisor Engine 720 with 10GE uplinks is required.
- Cisco IOS Software Release 12.2(33)SXI is required.
- FWSM Release 4.0(4) is required.
- No interoperability between FWSM Release 4.0 RHI feature and VSS integration.
- No support across VSS domains; namely, service modules are only integrated in a single domain as VSS does not support hierarchy or chain of VSS domains today.

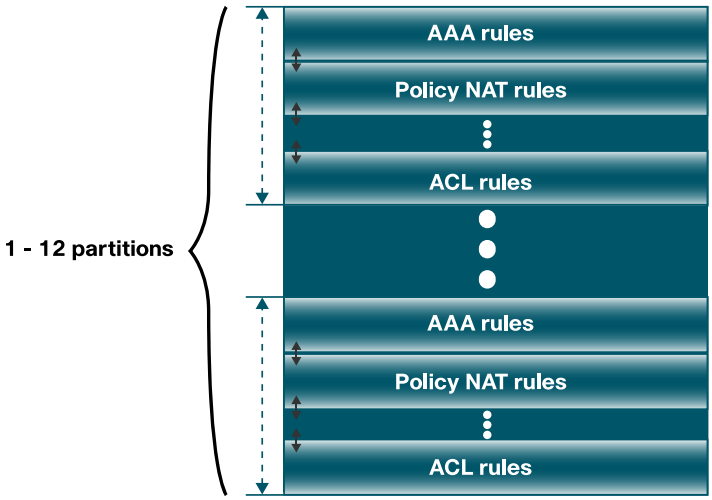
For more detailed information about VSS with FWSM, visit http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9336/white_paper_c11_513360.html.

Increased Access List Capacity

For Release 4.0 users will get to see increased ACL capacity from what was available in the prior releases. To achieve this feat, there was an overhaul of the ACLs stored in the memory and a lot of optimization to save on space. The number of total nodes is now close to 250,000. This represents a 74 percent increase over Release 2.3 and a 35 percent increase compared to Release 3.1. If we look at the maximum rule count, we notice the same 35 percent positive increase. The bottom line is that with Release 4.0, users would now have the capacity to store 130,000 ACL entries in single-context mode and 150,000 entries in multicontext mode.

In addition to increased capacity, users would have control over the size of each individual memory partition (in multicontext mode 12 partitions of equal size are created by default). A new CLI is introduced in Release 4.0 to let users resize each partition independently, allowing a very fine-tuned control over ACL resources available to specific virtual firewalls. If for instance a given virtual firewall requires three times as many ACL entries as another context, Release 4.0 makes it possible to carve out the memory in blocks that attempt to match the virtual firewall's requirements as closely as possible. The new CLI looks like this: acl-partition size <partition #> <partition size>. (See Figure 3.)

Figure 3. ACL Partitions



Built-in ACL optimization algorithm: FWSM Release 4.0 also incorporates an algorithm capable of optimizing ACLs by coalescing contiguous subnets referred to in different access-control entries into a single statement and detecting overlaps in port ranges. Note that after the optimization process, the ACL is likely to be different from the original one.

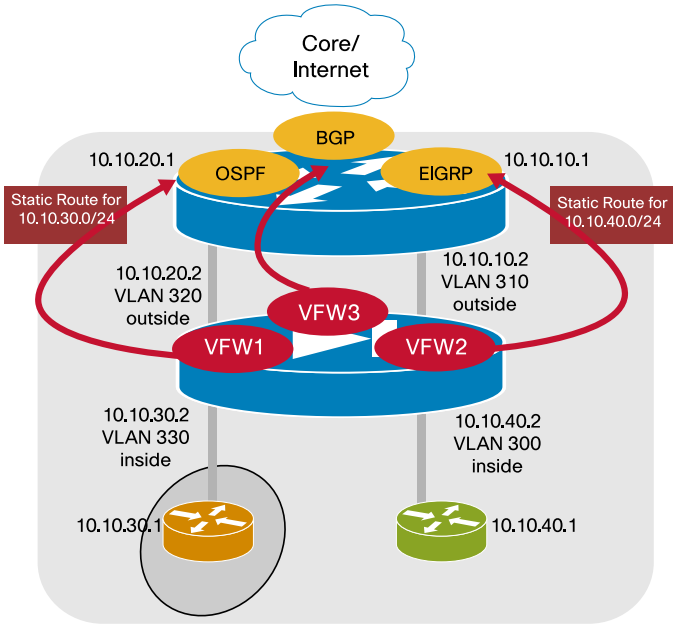
The FWSM keeps the original ACL in the configuration for user convenience. However, the version that is compiled into the hardware is the ACL displayed through the "show access-list optimization" command. Therefore, after entering the "access-list optimization enable" command, you will see two ACLs present in the configuration. Modifications are always made to the original ACL, and the optimization process runs its course using the new changes. Users cannot directly modify the optimized version of the ACL. There is, however, a command available to replace the existing ACL in the configuration with its new optimized version: "copy optimized-running-config running-config."

Route Health Injection

Route health injection, or RHI, is used for injecting the connected routes, static routes, and Network Address Translation (NAT) addresses configured on the FWSM into the Multilayer Switching Feature Card (MSFC) routing table. In multiple context mode, this feature is especially valuable because of the lack of dynamic routing protocol support. The MSFC can then redistribute the route to other routing tables. The injected routes specify the IP address of the FWSM interface as the next hop IP address for each of these FWSM networks. The FWSM injects routes into the MSFC using SCP messages.

When you configure NAT on the FWSM, the MSFC and other external routers do not know that those NAT addresses are connected to the FWSM unless you configure static routes on the MSFC to point to the FWSM interface. But by utilizing RHI, you can inject the NAT addresses to point to the FWSM interface so the MSFC can automatically forward that traffic to the FWSM. (See Figure 4.)

Figure 4. RHI logical view



- RHI is supported in routed firewall mode; it is not supported in transparent mode
- RHI is supported in both single and multiple context mode
- RHI is supported with failover (active/standby and active/active).
- The FWSM interface that you specify as the next hop interface must be an SVI between the FWSM and the MSFC

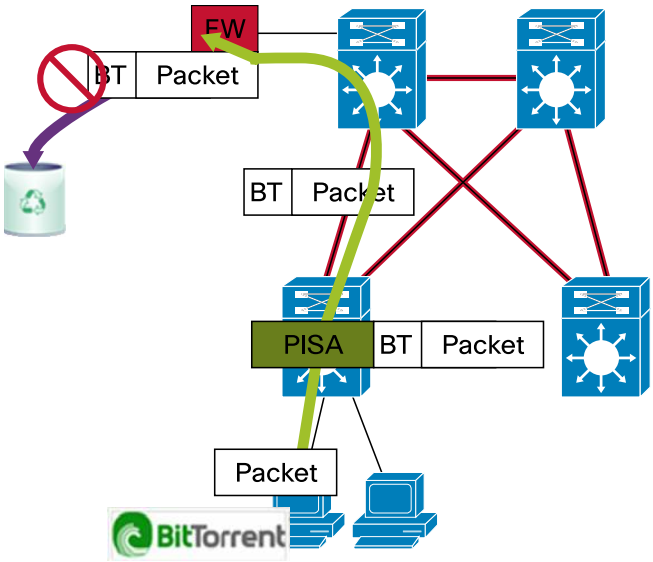
Integration with Cisco Catalyst 6500 Supervisor Engine 32 PISA

The Cisco Catalyst 6500 Supervisor Engine 32 PISA can quickly determine the application type of a given flow by performing deep packet inspection. This determination can be made even if the traffic is not using standard ports. The FWSM can use the high-performance deep packet inspection of the PISA card so that it can permit or deny traffic based on the application type. Unlike the FWSM inspection feature, which passes through the control plane path, traffic that the PISA tags can pass through the FWSM accelerated path. Another benefit of FWSM and PISA integration is to consolidate your security configuration on a single FWSM instead of having to

configure multiple upstream switches with PISAs installed. Security policies might want to deny certain types of application traffic when you want to preserve bandwidth for critical application types. For example, a user might deny the use of peer-to-peer (P2P) applications if they are affecting your other critical applications.

After the PISA identifies the application used by a given traffic flow, it encapsulates all packets using generic routing encapsulation (GRE) and includes a tag informing the FWSM of the application type. In addition, an outer IP header almost identical (except for the Layer 4 protocol, which now indicates GRE) to the inner/original IP header is added. The original Layer 2 header is maintained. This preserves the original routing/switching paths for the modified packet. The GRE encapsulation adds 32 bytes (20 bytes for the outer IP header and 12 bytes for the GRE header). After the FWSM receives the packet and acts on the information, it strips the GRE encapsulation from the packet. (See Figure 5.)

Figure 5. FWSM with Pisa deployment



For more detailed information, visit http://www.cisco.com/en/US/docs/security/fwsm/fwsm40/configuration/guide/protct_f.html#wp1093163.

EIGRP Support in Single-Context Mode

In addition to having Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) routing protocol support in single context mode, this release introduces EIGRP. EIGRP is an enhanced version of IGRP developed by Cisco. Unlike IGRP and RIP, EIGRP does not send out periodic route updates. EIGRP updates are sent out only when the network topology changes. Neighbor discovery is the process that the FWSM uses to dynamically learn of other routers on directly attached networks. EIGRP routers send out multicast hello packets to announce their presence on the network. When the FWSM receives a hello packet from a new neighbor, it sends its topology table to the neighbor with an initialization bit set. When the neighbor receives the topology update with the initialization bit set, the neighbor sends its topology table back to the FWSM.

You can only enable one EIGRP routing process on the FWSM. Directly connected networks that fall within the defined network are advertised by the FWSM. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process.

For more detailed information, visit http://www.cisco.com/en/US/docs/security/fwsm/fwsm40/configuration/guide/ip_f.html#wp1120813.

Additional Features (Including Expanded Protocol Inspection)

Table 3 shows additional features.

Table 3. Additional Features

Feature	Description
DCERPC (MSRPC)	Provides support for applications running Microsoft Remote Procedure Call Protocol.
Enhanced SIP	Provides application security and protocol conformance, in addition to the basic firewall functionality (NAT and access-list pinholing), giving the user a more granular control on what policies and security checks to apply to SIP traffic and the capability to filter out unwanted messages and/or users.
Enhanced HTTP	Provides additional features to be added to the Application Firewall software (enhanced HTTP) in FWSM Release 3.2 to achieve a tighter protocol conformance and give the user a more granular control over the HTTP traffic that will flow through the firewall.
Enhanced ESMTP	Provides protocol conformance and application security by giving the user a more granular control over the ESMTP traffic that can traverse the firewall.
DHCP Option 82	Allows the FWSM to interoperate with the Cisco Catalyst 6500 switch acting as a relay agent preserving DHCP Option 82 information populated by the switch.
Additional SNMP MIBs	Additional MIBs give the ability to poll: • Access-list entries • ACL hit counters (with ACL name and line number so that direct correlation can be drawn between the hit counter and the ACE)

FWSM supports a wide variety of application protocols for inspection. In this release the existing protocols have been equipped with enhanced inspection capabilities such as ability to create regular expressions, regular expression class maps, and Inspection policy and class maps.

The following protocols support inspection policy and/or class maps:

- DCERPC
- ESMTP
- HTTP
- SIP

On the URL filtering side, FWSM Release 4.0 will now support HTTPS with Secure Computing Smartfilter (formerly known as N2H2). In addition, for Websense based URL filtering, FWSM will now add context name to Websense queries and lets Websense server use the context name for policy lookups.

For More Information

Release Notes:
http://www.cisco.com/en/US/docs/security/fwsm/fwsm40/release/notes/fwsmrn40.html

Configuration Guide:
http://www.cisco.com/en/US/docs/security/fwsm/fwsm40/configuration/guide/fwsm_cfg.html

Product Management contact: Amit Datar, datar@cisco.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C25-530019-00 04/09