FWSM4.0(4): Virtual Switching System (VSS) Integration

One of the main objectives of FWSM 4.0 is to provide close integration and collaboration between FWSM and other Cisco® Catalyst® 6500 Series Switch services. This paper provides technical details for integration of FWSM4.0 with the Virtual Switching System (VSS).

Prerequisite

This feature relies on having an understanding of VSS concepts, and therefore it is highly recommended to review the relevant materials prior to reading this paper. There will be a brief description of VSS in this paper, but it is not meant to be a comprehensive explanation of it.

Background

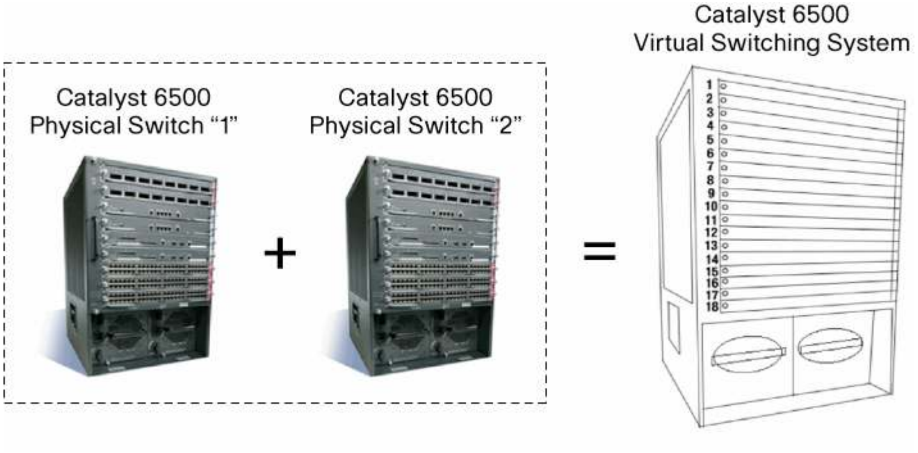
The Virtual Switching System (VSS) is a new and innovative feature on Cisco Catalyst 6500 Series Switches that effectively allows clustering of two physical chassis together into a single logical entity. Such a technology will allow for new enhancements in all areas of enterprise campus and data center deployment, including high availability, scalability/performance, management, and maintenance. Service module support is a primary requirement for positioning of the VSS in enterprise campus and enterprise data center market. The first release of the VSS included support for the Network Access Module (NAM) service module. As part of the second release of the VSS, we plan to extend support to the more popular service modules. The list of service modules that are going to be supported in the second release of the VSS are the Firewall Services Module (FWSM), the Intrusion Detection Service Module (IDSM), the Application Control Engine (ACE) service module, and the Wireless Service Module (WiSM). This document only focuses on the VSS and FWSM integration. The first release of VSS and FWSM integration is supported by FWSM4.0(4), which gets released at the time of Cisco IOS® Software Release 12.2(33)SXI image posting.

The integration and deployment of FWSM in a VSS environment are done transparently and do not require special configuration. There are only minor changes on the Cisco Catalyst 6500 Series side that need to be considered, and these are very much contained within the changes that are inherent to VSS model of Cisco IOS Software.

Overview of VSS and FWSM integration

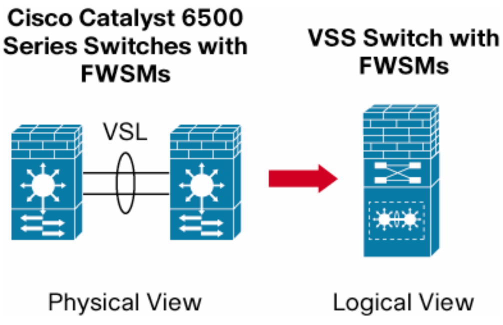
The current implementation of VSS allows for the merging of two physical Cisco Catalyst 6500 Series Switches together into a single logically managed entity. Figure 1 provides a graphical representation of this concept where two Cisco Catalyst 6509 Switch chassis can be managed as a single 18-slot chassis after VSS has been enabled.

Figure 1. Virtual Switching System



The primary enabler of the VSS technology is a special link that binds the two chassis together called a virtual switch link (VSL). The VSL carries special control information as well as encapsulates every frame with a header that passes across this link. The VSS concept allows for the combination of two switches into a single logical network entity from the network control plane and management perspective. To the neighboring devices, the VSS will appear as a single logical switch or router. Within the VSS, one chassis is designated as the virtual switch active, and the other is designated as the virtual switch standby. All control plane functions including management (SNMP, Telnet, SSH, and so on), Layer 2 protocols (BPDUs, PDUs, LACP, and so on), Layer 3 protocols (routing protocols and so on), and software data path are centrally managed by the active supervisor of the active virtual switch chassis. The supervisor on the virtual switch active is also responsible for programming the hardware forwarding information onto all the distributed forwarding cards (DFCs) across the entire VSS as well as the policy feature card (PFC) on the virtual switch standby supervisor. From a data plane and traffic forwarding perspective, both switches in the VSS are actively forwarding traffic. The PFC on the virtual switch active supervisor will perform central forwarding lookups for all traffic that ingresses the virtual switch active, whereas the PFC on the virtual switch standby supervisor will perform central forwarding lookups for all traffic that ingresses the virtual switch standby. The FWSM integration with VSS is aimed to behave similarly to availability of the service module as if both chassis were a single logical chassis. Therefore the user can access and activate the modules in either chassis in standalone mode as well as failover mode. (See Figure 2.)

Figure 2. FWSM Integration With VSS



VSS: FWSM Integration Configuration

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 impact is very well contained within the usual model change associated with VSS and non-VSS mode (standalone mode). Following is a summary of CLIs that are needed to have an FWSM function in VSS mode.

Cisco Catalyst 6500: VSS Configuration Implications	
pod2-vss#sh run Building configuration... firewall switch 1 module 5 vlan-group 5 firewall switch 2 module 5 vlan-group 5 ...	From the Cisco Catalyst 6500 point of view, the “firewall module <n> vlan-group” command needs to account for both switches once the VSS mode is turned on.
Cisco Catalyst 6500: VSS Show CLI Implications	
pod2-vss#sh mod switch 1 Switch Number: 1 Role: Virtual Switch Active ---------------------- ----------------------------- Mod Ports Card Type Model Serial No. --- ----- -------------------------------------- ------------------ ----------- 1 5 Supervisor Engine 720 10GE (Active) VS-S720-10G SAL11456FTW 2 4 CEF720 4 port 10-Gigabit Ethernet WS-X6704-10GE SAL1104EU3A 3 48 CEF720 48 port 10/100/1000mb Ethernet WS-X6748-GE-TX SAD105101ZW 4 6 Firewall Module ... pod2-vss#sh mod switch 2 Switch Number: 2 Role: Virtual Switch Standby ---------------------- ----------------------------- Mod Ports Card Type Model Serial No. --- ----- -------------------------------------- ------------------ ----------- 1 5 Supervisor Engine 720 10GE (Hot) VS-S720-10G SAL114560RJ 2 4 CEF720 4 port 10-Gigabit Ethernet WS-X6704-10GE SAL1104F1U6 3 48 CEF720 48 port 10/100/1000mb Ethernet WS-X6748-GE-TX SAL1108HAUX 4 6 Firewall Module WS-SVC-FWM-1 SAD070900BL ... pod2-vss#session switch 1 slot 4 pro 1 The default escape character is Ctrl-^, then x. ...	Relevant show commands will change accordingly to accommodate for accessing virtual switch 1 or 2.

As indicated above, the configuration changes to make VSS” FWSM integration are minimal and follow the basic Cisco Catalyst 6500: VSS model while in VSS mode.

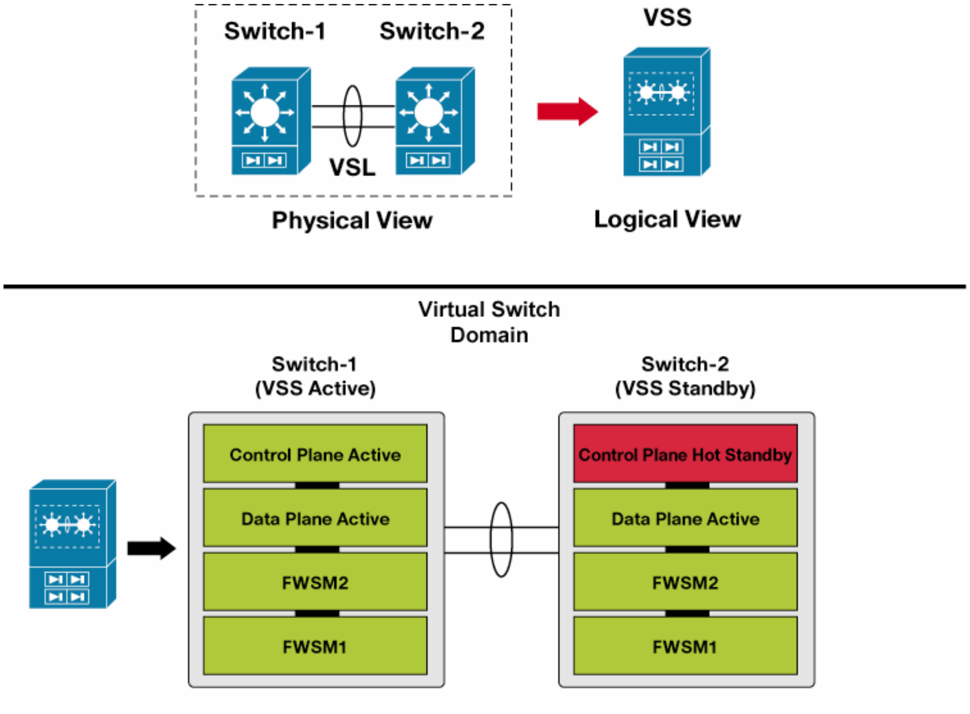
VSS and FWSM Modes of Operation

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. There are a few important points in this area that need attention, and they generally follow the normal VSS model. In the following sections these points are illustrated.

FWSM Standalone Mode

In this section we will cover the main points regarding FWSM standalone mode of operation and VSS integration. As illustrated in Figure 3, the FWSM units can operate in standalone mode within the logical chassis as they do today in non-VSS mode. One important point is that the number of FWSMs in a single physical chassis can scale up to 4 units. That number basically can grow to 8 (2 x 4) units for VSS mode of operation that includes two physical chassis (that is, 4 modules in each physical chassis).

Figure 3. Service Module (FWSM) Transition During Non-VSS to VSS Mode



Note that in the above VSS mode, the VSL (link) will be used in order to get packets to the right FWSM, and therefore proper capacity planning is required to accommodate for necessary rerouting of packets across VSL. There will be further discussions of packet flows during VSS mode in the following sections.

FWSM Failover Mode

This section provides detail on FWSM failover within VSS mode of operation. Note that both inter and intrachassis models of FWSM failover are supported in VSS mode; however, interchassis failover is used here for illustration purposes as it touches on important aspects of VSL capacity planning of FWSM failover. Fortunately, the impact from configuration point of view is minimal again. The user has to make sure that all VLANs (including failover/state VLANs) are pushed on both failover units (regardless of which physical chassis they reside in). For example, VLAN group N needs to be pushed on switch 1 as well as switch 2 if VLAN group N contains the necessary VLANs (including failover and state). Figures 4 and 5 illustrate an example of active/standby as well as active/active mode of operations within VSS.

Figure 4. FWSM Active/Standby Failover Example Within VSS Environment

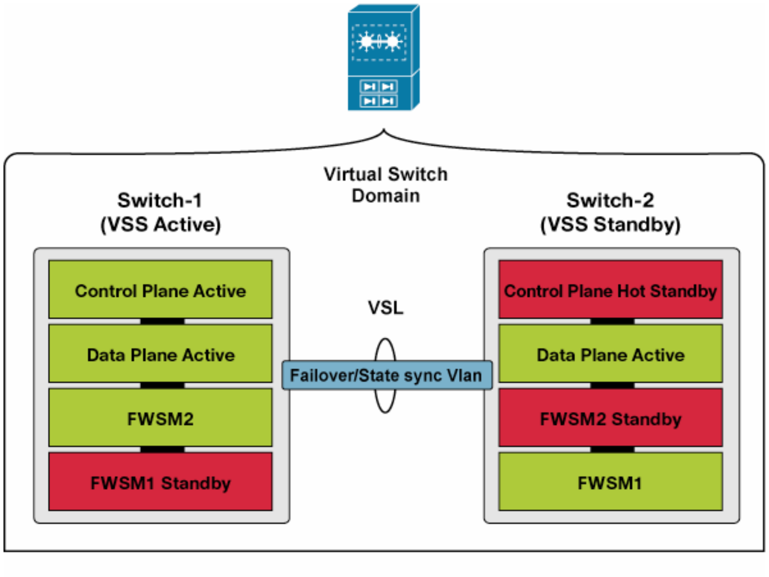
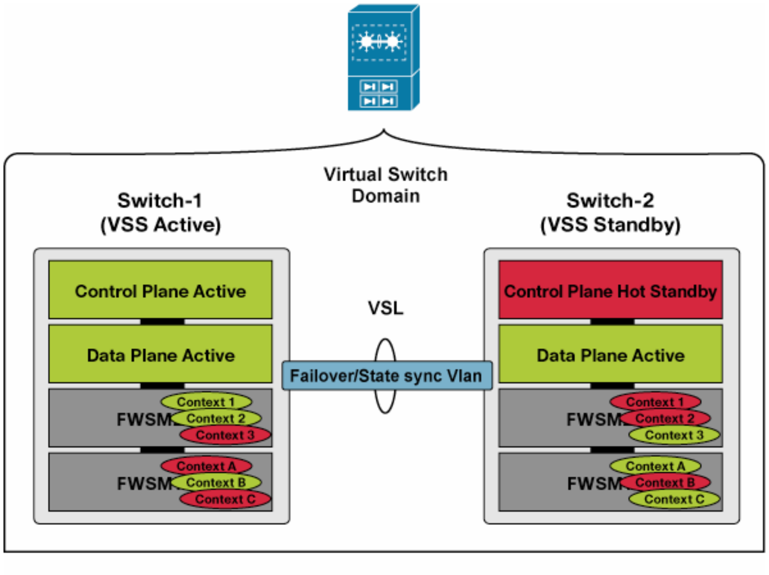


Figure 5. FWSM Active/Active Failover Example Within VSS Environment



As shown above, FWSM failover mode of operations integrates transparently within a VSS environment. One very important aspect is that for both active/standby and active/active, the VSL link needs to have enough capacity to accommodate for “failover” as well as “state” link. It is recommended to plan around 1.5Gbps per pair of FWSM failover units as part of FWSM failover: VSL capacity requirements.

From a logical point of view it is important to note that the VSS chassis will behave as a single chassis, and therefore in this model “autostate + interface monitoring” feature of FWSM will not function even if the two units are spread across the two physical chassis. Remember that this behavior is similar to when both FWSM units reside in the same physical chassis in non-VSS mode (that is, autostate + interface monitoring is not supported).

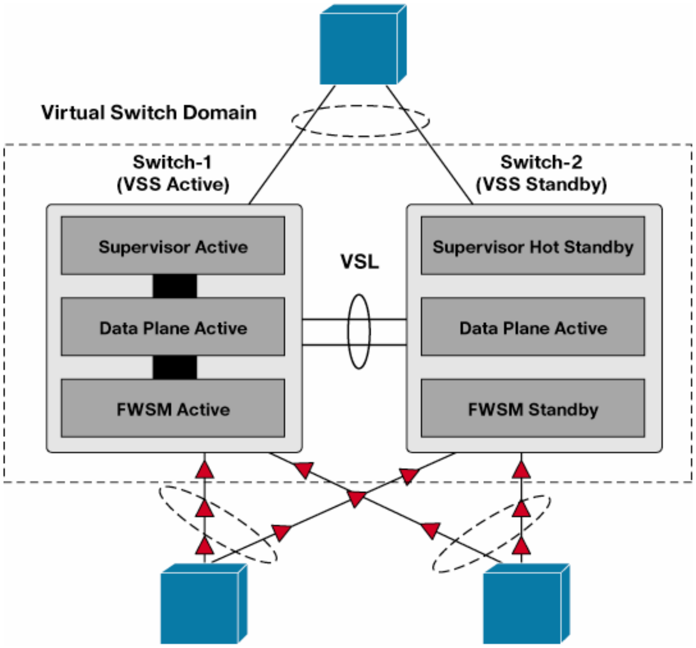
VSS: FWSM Packet Flows

In this section a few examples are considered to illustrate that packet flows for FWSM modules will follow the normal data path paradigm as expected within the VSS chassis.

Packet Flow: Ingress Traffic

Figure 6 illustrates the ingress traffic of VSS chassis. The traffic will arrive at the VSS chassis based upon the neighbor device’s load-balancing configuration; it is expected to have traffic transmitted across all interfaces that are part of MEC.

Figure 6. Packet Flow: Ingress Traffic



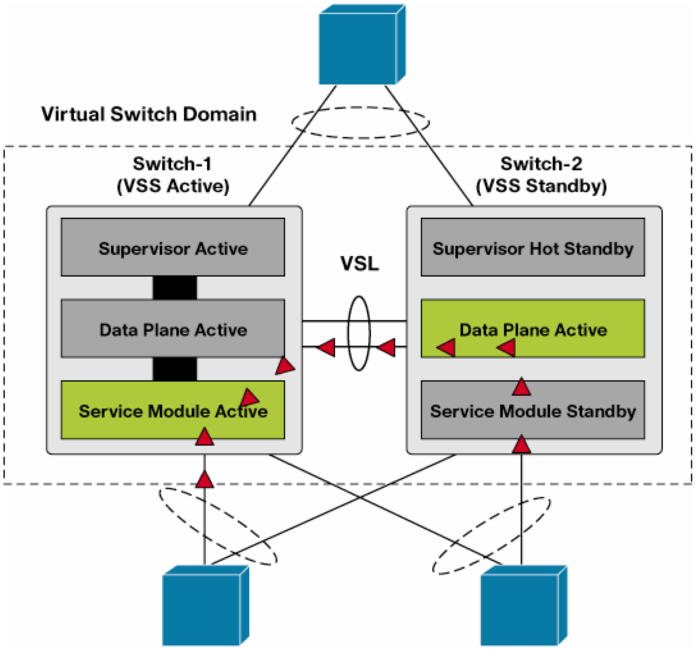
Packet Flow: Redirected Traffic

Figure 7 provides an example of packets destined to an active FWSM originating from either physical chassis of VSS. In this example, switch 2 ingress traffic will be redirected to the active service module in switch 1, as switch 1 ingress traffic will be sent to that active service module too. Therefore it is expected to have traffic destined to active service module traversing VSL.

Recommendations:

- Size the VSL link based on expected bandwidth requirement.
- Tune the load sharing algorithm for best traffic distribution.
- Plan 1–2Gbps per FWSM failover pair in VSL capacity for FWSM stateful failover traffic.

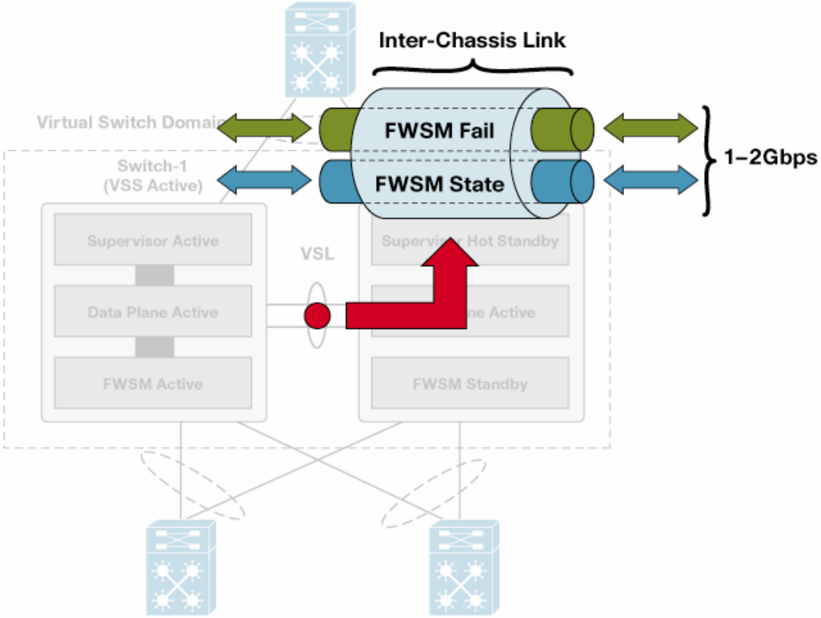
Figure 7. Packet Flow: Towards Active FWSM



Interchassis Link

Capacity planning for interchassis links is an important part of VSS deployment. Include capacity for FWSM failover pairs to account for failover/state VLAN links between the two chassis if FWSM interchassis failover is deployed. It is recommended to set aside 1–2Gbps for this purpose. (See Figure 8.)

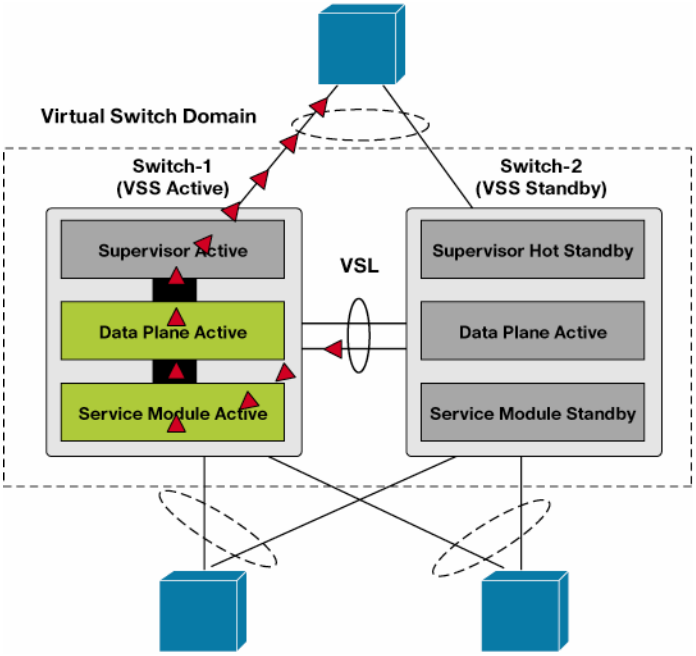
Figure 8. Failover Links Across Interchassis Link



Packet Flow: Egress Traffic

Once the flows that arrive on switch 1 and flows that get redirected from switch 2 are processed by the active service module, then they will get forwarded to the next hop device. For egress traffic, locally connected interfaces are favored in MEC and L3 ECMP interfaces. This is illustrated in Figure 9.

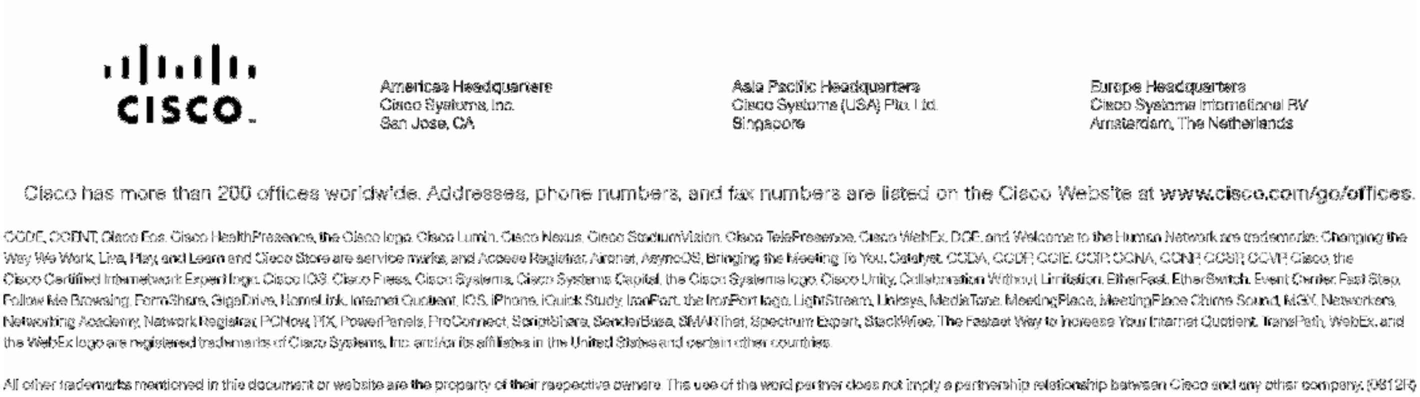
Figure 9. Packet Flow: Egress Traffic



FWSM4.0 Hardware/Software Feature Considerations

FWSM4.0 is a phased release that is based on FWSM Cisco IOS Software independent features (FWSM4.0(1)), cyclical maintenance releases with bug fixes, and Cisco IOS Software dependent features. VSS support is part of Cisco IOS Software dependent features, and therefore it is targeted to be released in the timeframe that Cisco IOS Software Release 12.2(33)SXI is planned to be posted. Note that FWSM4.0 will have interim images until Cisco IOS Software Release 12.2(33)SXI is posted: that is, FWSM4.0(2) and FWSM4.0(3) are current maintenance releases with bug fixes. There are a number of other FWSM4.0 IOS dependent features as well that may or may not interoperate with FWSM VSS integration, and also keep in mind that VSS has its own set of hardware/software requirements. The highlights of FWSM VSS integration requirements and limitations are described here:

1. SUP720-10G is required.
2. Cisco IOS Software Release 12.2(33)SXI is required.
3. FWSM4.0(4) is required.
4. No interoperability between FWSM4.0 RHI feature and VSS integration.



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