FWSM Cluster Deployment Across Two VSS Domains

Executive Summary

Interconnected Virtual Switching Systems (VSSs) are commonly deployed in the distribution layer of many networks. Cisco supports the deployment of Firewall Services Modules (FWSMs) within the same Catalyst 6500 or within the same VSS, to maintain network security (for more information, refer to the white paper entitled "FWSM4.0(4): Virtual Switching System (VSS) Integration"). However, two alternate configurations were proposed, which required validation before being supported:

- Deployment of FWSM clusters across two different VSSs
- Deployment of FWSM clusters inside a Catalyst 6500 connected to each VSS

The Cisco Enhanced Customer Aligned Testing Services (ECATS) team conducted the verification/validation of these FWSM cluster deployment options, in a very specific VSS environment. The validation included some FWSM and VSS features, as well as a combination of these FWSM cluster modes: active/active, active/standby, routed and transparent mode, and multiple contexts.

This white paper describes these two FWSM cluster deployment options, and presents the ECATS recommendations. It provides high-level guidance on how to properly configure your network to deploy VSS with the FWSM. Links to additional information about these products are provided in appropriate sections.

To understand this document, you should have at least basic working knowledge of Cisco VSS and FWSM.

Introduction

VSS is a Cisco technology that binds together two Catalyst 6500 switches to form one virtual switch entity. Once the virtual entity is formed, only one of the two supervisors is active at a time. The other remains in standby mode. The virtual entity is perceived as one Catalyst 6500 switch by any device connected to it, or in communication with it.

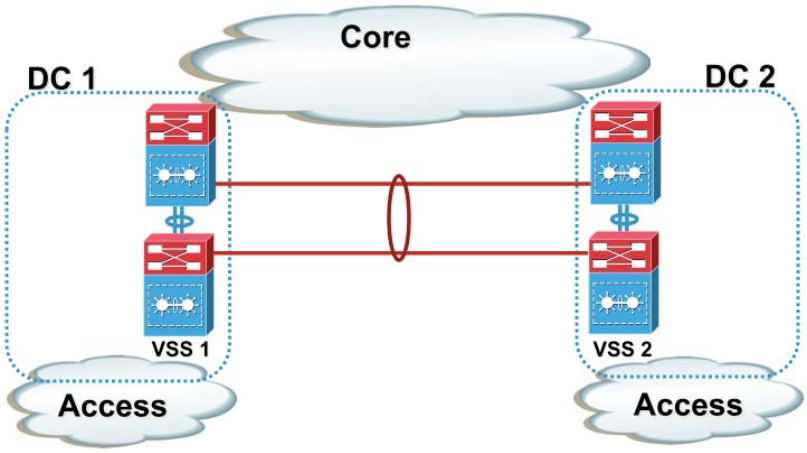
For more information on VSS, please refer to the "Configuring Virtual Switching Systems" chapter of the *Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide*:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html

The FWSM cluster refers to two peered FWSMs, with one being active and the other standby, for any given security context.

For more information on FWSM, please refer to the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide, 4.0*:
http://www.cisco.com/en/US/docs/security/fwsm/fwsm40/configuration/guide/fwsm_cfg.html

Figure 1 depicts a typical VSS environment where an FWSM cluster needs to be deployed. Each data center (DC) has one VSS, which is connected to the core, to the DC's related access, and to the other DC's VSS. The term "VSS domain" used in this document refers to the DC.

Figure 1 – Typical VSS Environment



There are two ways to add a level of security to this environment. Figure 2 depicts the first deployment option. The FWSM cluster is deployed across the two VSS domains inside the VSS chassis (switch 1 or switch 2).

Figure 2 –VSS Deployment Option 1

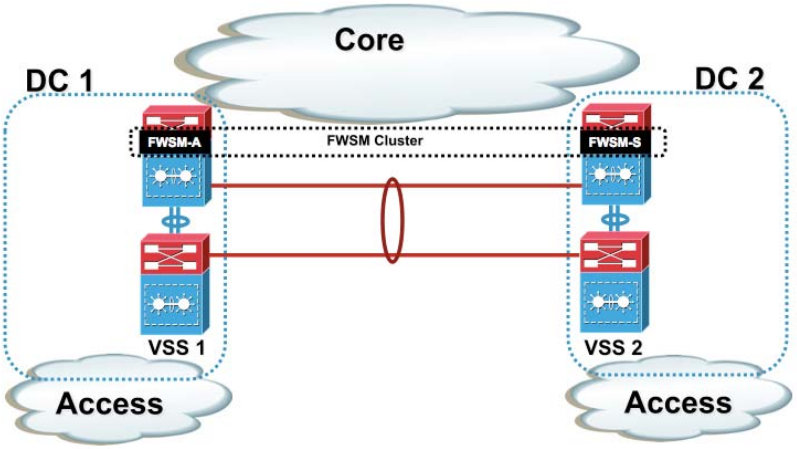
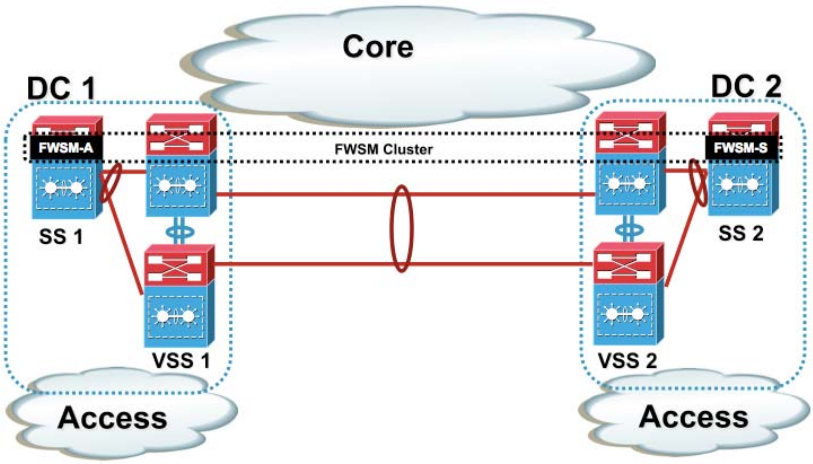


Figure 3 depicts the second deployment option. The FWSM cluster is deployed across two VSS domains inside two Catalyst 6500 service switches (SS), each connected to a VSS as shown. This method can be used if you don't want to place the FWSM inside the VSS chassis.

Figure 3 –VSS Deployment Option 2



Once deployed inside the chassis using either of the above options (VSS or SS), the FWSM cluster can then be configured for a single context, for multiple contexts, for active/standby or active/active mode, for transparent mode, or for routed mode.

The advantages or disadvantages of each the above deployment options are beyond the scope of this document.

Configuration Guidelines

The interaction of technologies and devices in any VSS/FWSM environment must be carefully planned and tuned. The location of the primary FWSM for any given security context or a group of security contexts is pivotal for this planning and the tuning. The following subsections describe the fundamental characteristics of these devices and technologies.

VSS Characteristics

The VSS is the essential part of this environment, and its configuration should be appropriately executed to guarantee a successful deployment. Apart from the standard VSS configuration guidelines (which can be found using the link provided in the "Introduction" section), there are two configuration guidelines that are strongly recommended:

- A **dual-active detection mechanism** must be configured. This mechanism prevents both VSS chassis from becoming active in the event of the VSL links' failure. Dual active can cause serious and severe network instabilities and disruptions. It mitigates network instabilities and disruptions by securely isolating one of the two chassis, and by ensuring an automatic recovery as soon as the VSL links recover. The dual-active detection mechanism implemented during the testing was the fast-hello, which is strongly recommended by Cisco. For more information on dual active documentation and configuration, refer to the "Dual-Active Detection" section of the *Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide*: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#wp1063718.
- It is recommended that **VSS preemption *not* be used** in this environment as its process causes outage and possible instabilities. (VSS preemption will be deprecated soon.)

FWSM Characteristics and Location

The FWSM is the key element of this deployment, as it supervises all the traffic going in and out through this environment. Its location and configuration are crucial, as the overall deployment configuration flows from it.

With no FWSM preemption enabled, it is difficult to locate and control the position of the active FWSM unit for any given security context, with obvious consequences to the overall environment's configuration. FWSM preemption makes that location and control more predictable. It is therefore imperative to configure FWSM preemption in order to deploy a FWSM cluster in this environment. This will then help to build a more accurate and stable configuration for the environment, especially in the areas of Spanning Tree Protocol (STP), Hot Standby Router Protocol (HSRP), and routing.

STP

RSTP (Rapid Spanning-Tree Protocol) was used during the testing. The VSS located in the VSS domain with the active FWSM for a security context should be the STP root primary for all the VLANS pertaining to that security context. The other VSS should be the STP root secondary.

Note: The above STP priority guidelines on the VSS should be the same whether the FWSM cluster is deployed in the VSS or in the SS. When the FWSM cluster is deployed in the SS, all the VLANs' STP priority should be left as default in the SS.

HSRP

The SVI interface (in the same VLAN as the outside VLAN of the security context) in the VSS located in the VSS domain containing the active FWSM for a particular security context should be HSRP active. The corresponding SVI configured in the other VSS must be HSRP standby.

Note: It is important to mention that when the FWSM cluster is deployed in the SS, the above HSRP guidelines remain the same. No SVI (related to security contexts) should be configured on the SS, which is purely a Layer 2 device.

Routing

At the time of the validation/verification, OSPF was used as the routing protocol between the core and the two VSS domains, with no adjacency between the VSS domains.

Note: It is important to mention that the above result can be achieved using a routing protocol other than OSPF, as long as the implemented design guarantees a traffic flow similar to the one described here.

All the subnets related to the SVI interfaces (in the same VLAN as the outside VLAN of the security context) in both VSS domains should be advertised in OSPF to the core. Each SVI interface should be configured with an adapted OSPF cost, to ensure that the traffic from the core to a particular security context is sent to the correct VSS domain (where the active FWSM unit for that security context is located). The SVI on the VSS domain with the active FWSM for a particular security context should be configured with a lower OSPF cost than the SVI in the other VSS domain. The redistribution metric must also be lower on the VSS with the active FWSM for a particular security context, than that on the other VSS.

When static routing is used in routed mode, the default routes configured in the FWSM must point to the HSRP virtual IP addresses on the VSS. The static routes configured on the VSS to reach the inside subnet of each security context must also point to the FWSM outside IP address.

The above can be achieved with only one OSPF process for a FWSM cluster in active/standby mode. However, two OSPF processes are needed for a FWSM cluster in active/active mode, one per FWSM security context group.

When the FWSM cluster operates in transparent mode, there is no need to configure static routes either in the VSS or in the FWSM (unless for FWSM management). This is because both the inside and the outside VLANs share the same subnet, although they have different VLAN IDs.

Both access lists and route maps were used during the validation for redistributing the static routes into OSPF. These routes pointed to the inside subnet of each context.

The table below shows the STP priority, HSRP priority, OSPF cost, and OSPF redistribution metric used in the testing.

FWSM Cluster Mode	FWSM Location	STP Priority /HSRP Priority/ Interface OSPF Cost and Redistribution Metric in OSPF – OSPF process ID
A/S	Active in VSS1	Primary/120/9/ - 100
	Standby in VSS2	Secondary/90/19/ - 100
A/A	Group 1 active in VSS1	Primary/120/9/ - 100
	Group 1 standby in VSS2	Secondary/90/19/ - 100
	Group 2 standby in VSS1	Secondary/90/19/ - 200
	Group 2 active in VSS2	Primary/120/9/ - 200

Conclusion and Recommendations

Based on the results of the testing, the ECATS Team has made the following recommendations:

1. **Connection between the core and each VSS chassis.** It is recommended to have two links between the core and the VSS chassis, rather than a lone connection to the core. The second link provides redundancy in the event of a failover (which require the reload of one of the chassis), or in the event of the unavailability of the one of the chassis.

2. **OSPF configuration tuning.** It is more efficient to adapt the OSPF configuration to take into account the configured FWSM active default location, and to have the ingress and egress traffic routed accordingly.

3. **Dual active detection on the VSS.** It is highly recommended to have a dual active detection mechanism that appropriately and efficiently handles the VSS behavior in the event of the VSL link's failure and recovery. Cisco recommends the fast-hello dual active detection mechanism. (This was not implemented for the testing phase.)

4. **No VSS preemption.** This should reduce the outage of the VSS chassis. Preemption will not be supported in later versions of the code.

5. **FWSM preemption.** This guarantees that the primary FWSM unit for a particular security context will return to the active role in the event of an unexpected failover (preemption will not be triggered if failover is triggered manually with the following CLI:*"<no> failover active <group 1/2>"*).

Hardware and Software Requirements

Observe the following:

1. Cisco IOS Software Release 12.2(33)SXI(3) (minimum) is required.
2. FWSM4.0(7) (minimum) is required.

Acronyms

A/S	Active/Standby
A/A	Active/Active
DC	Data Center
ECATS	Enhanced Customer Aligned Testing Services
FWSM	Firewall Services Module
HSRP	Hot Standby Router Protocol
NAT	Network Address Translation
OSPF	Open Shortest Path First
SS	Standalone/Service Switch
RSTP	Rapid Spanning Tree Protocol
SVI	Switch Virtual Interface
VSS	Virtual Switching System
VLAN	Virtual Local Area Network
VSL	Virtual Switching Link

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.**