

FWSM Failover Troubleshooting

Document ID: 100871

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Failover Checklist

- Verify the Interfaces
- Licenses
- Context Mode
- Software Requirements
- Minimal FWSM Configuration for Stateful Failover
- Minimal Switch Configuration

Troubleshooting

- Version Mismatch
- Incompatible Licenses
- Different Modes (single vs. multiple context)
- Two FWSMs Become Active
- VLAN Mismatch
- Failover is Disabled in the Configuration

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document explains the procedures you can use in order to resolve problems with the Firewall Service Module (FWSM) failover configuration.

This document also provides a checklist of common procedures to try before you begin to troubleshoot the failover connection.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the FWSM 2.3 and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

The failover feature allows a standby FWSM to take over the functionality of a failed FWSM. The two FWSMs involved must have the same major (first number) and minor (second number) software version, license, and operating modes (routed or transparent, single or multiple context). When the active unit fails, the state changes to standby, while the standby unit moves into the active state. After a failover occurs, the same connection information is available at the new active unit.

For additional information, refer to the Configuring Failover section of Using Failover.

Failover Checklist

This checklist helps you to successfully configure the failover in FWSM:

- Verify the Interfaces
- Licenses
- Context Mode
- Software Requirements
- Minimal FWSM Configuration for Stateful Failover
- Minimal Switch Configuration

Verify the Interfaces

Verify that all interfaces on the FWSM have a configured standby IP address. If you have not done so already, configure the active and standby IP addresses for each interface (routed mode), or for the management address (transparent mode). The standby IP address is used on the FWSM that is currently the standby unit. It must be in the same subnet as the active IP address.

This is an example configuration:

```
ip address <active-ip> <netmask> standby <standby-ip>
```

Note: Do not configure an IP address for the failover link or for the state link (if you are going to use Stateful Failover).

Note: You do not need to identify the standby address subnet mask. The failover link IP address and MAC address do not change at failover. The active IP address for the failover link always stays with the primary unit, while the standby IP address stays with the secondary unit.

Licenses

Both active and standby units must have the same license.

Context Mode

If the primary unit is in single context mode, the secondary unit must also be in single context mode and in the same firewall mode as the primary unit.

If the primary unit is in multiple context mode, the secondary unit must also be in multiple context mode. You do not need to configure the firewall mode of the security contexts on the secondary unit because the failover and state links reside in the system context. The secondary unit obtains the security context configuration from the primary unit.

Note: The **mode** command does not get replicated to the secondary unit.

Note: Multicast is not supported in the multiple context mode of the security appliance. Refer to the Unsupported Features section for more information.

Software Requirements

The two units in a failover configuration must have the same major (first number) and minor (second number) software version. However, you can use different versions of the software during an upgrade process. For example, you can upgrade one unit from Version 3.1(1) to Version 3.1(2) and have failover remain active. Cisco recommends to upgrade both units to the same version to ensure long-term compatibility.

Minimal FWSM Configuration for Stateful Failover

Primary FWSM

```
failover lan unit primary
failover lan interface if_name vlan vlan
failover interface ip if_name ip_addr mask standby ip_addr
failover link if_name vlan vlan
failover interface ip if_name ip_addr mask standby ip_addr
```

Secondary FWSM

```
failover lan unit secondary
failover lan interface if_name vlan vlan
failover interface ip if_name ip_addr mask standby ip_addr
failover link if_name vlan vlan
failover interface ip if_name ip_addr mask standby ip_addr
```

For more information on how to configure Active and Standby failover, refer to Configuring Active/Standby Failover.

Minimal Switch Configuration

- The VLANs sent to the primary FWSM by the Catalyst that contains the primary must match the VLANs sent to the secondary FWSM by the Catalyst that contains the secondary. (Output of the **show run | i firewall** command must be identical.)

Primary Chassis

```
cat6k-7(config)#do sh run | i fire
firewall multiple-vlan-interfaces
firewall module 9 vlan-group 1
firewall vlan-group 1 3,4,100-106
```

Secondary Chassis

```
cat6k-7(config)#do sh run | i fire
firewall multiple-vlan-interfaces
firewall module 9 vlan-group 1
firewall vlan-group 1 3,4,100-106
```

- All the VLANs that are sent must be present in the VLAN database and be active.

In order to perform this, issue these commands on the switch in configuration mode:

```
vlan 10
no shut
```

In order to verify if the VLANs are in the database and active, the output of the **show vlan** command on both chassis must contain the VLANs sent to the FWSM and show as active.

This is a sample output:

Primary Chassis

```
cat6k-7(config)#do sh vlan
```

VLAN	Name	Status	Ports
1	default	active	
3	VLAN0003	active	Fa4/47
4	VLAN0004	active	Fa4/48

Secondary Chassis

```
cat6k-7(config)#do sh vlan
```

VLAN	Name	Status	Ports
1	default	active	
3	VLAN0003	active	Fa4/47
4	VLAN0004	active	Fa4/48

- Make sure that the two FWSMs have Layer2 connectivity in each VLAN (they must be in the same subnet).

Transparent Firewall Requirements:

In order to avoid loops when you use failover in transparent mode, you must use switch software that supports Bridge Protocol Data Unit (BPDU) forwarding. Also, you must configure the FWSM to allow BPDUs. In order to allow BPDUs through the FWSM, configure an EtherType? ACL and apply it to both interfaces.

Note: As opposed to the PIX and ASA platform, the hardware of two FWSM blades is always the same, there are no different models or memory configurations.

Troubleshooting

When the FWSM reloads, the scenarios explained in this section will cause failover to be disabled.

The FWSM can reload for reasons such as crash, reset from chassis, reload issued from FWSM CLI, or it can just be a new module that is inserted or reseated into a different slot or powered back up from the chassis.

Version Mismatch

The two units in a failover configuration must have the same major (first number) and minor (second number) software version.

Related syslog message – 105040

Incompatible Licenses

You might receive this syslog because of an incompatible license:

```
FWSM-1-105045: (Primary) Mate license (number contexts) is not compatible
with my license (number contexts).
FWSM-1-105001: (Primary) Disabling failover.
```

Related syslog messages – 105045, 105001

Different Modes (single vs. multiple context)

Both the primary and secondary FWSM must be in the same mode (single or multiple). For example, if the primary is configured as single mode and the secondary as multiple mode and the secondary is reloaded, then both the modules will turn off failover.

Primary in single mode:

```
%FWSM-1-103001: (Primary) No response from other firewall (reason code = 1).
%FWSM-1-105044: (Primary) Mate operational mode (Multi) is not compatible
with my mode (Single).
%FWSM-1-105001: (Primary) Disabling failover.
```

Secondary in multiple mode (this blade is reloaded):

```
%FWSM-5-111008: User 'Config' executed the 'no snmp-server location' command.
%FWSM-5-111008: User 'Config' executed the 'inspect tftp' command.
%FWSM-5-111008: User 'Config' executed the 'service-policy global_policy global'
command.
%FWSM-5-111008: User 'Config' executed the 'config-url disk:/admin.cfg' command.
%FWSM-5-111008: User 'Config' executed the 'prompt hostname context' command.
%FWSM-4-411001: Line protocol on Interface LAN, changed state to up
%FWSM-4-411001: Line protocol on Interface LAN, changed state to up
%FWSM-1-105044: (Secondary) Mate operational mode (Single) is not compatible
with my mode (Multi).
%FWSM-1-105001: (Secondary) Disabling failover.
%FWSM-6-199002: Startup completed. Beginning operation.
%FWSM-6-605005: Login permitted from 127.0.0.51/15518 to eobc:127.0.0.91/telnet
for user ""
%FWSM-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15
%FWSM-5-111008: User 'enable_15' executed the 'changeto context admin' command.
```

Primary in multiple mode:

```
%FWSM-1-105044: (Primary) Mate operational mode (Single) is not compatible
with my mode (Multi).
%FWSM-1-105001: (Primary) Disabling failover.
```

Related syslog messages – 105044, 103001, 105001

Two FWSMs Become Active

When you see this error message in the log:

```
fw_create_pc_sw: fw_create_portchannel failed
```

The reason for this error is because the recommended number of port-channels in the switch exceeded the maximum (128 is maximum in Cisco IOS software release 12.2(33)SXH4 on Cat6000/6500). Therefore, Interface Descriptor Block (IDB) limit is being exhausted.

Because to this, you might end up with these two issues:

- When you have two switches with FWSM modules each to act as active and standby, two FWSM modules become active at the same time.
- You cannot create an additional port-channel.

As part of resolving the issue, delete port-channels which are not needed and reload the FWSMs.

VLAN Mismatch

Problem

The FWSM receives this error message: **'Detected an Active Mate' 'Vlan configuration mismatch' 'failover will be disabled'**.

OR

The configuration of the firewall service modules and the corresponding switch configuration appear to be complete. However, the FWSMs are unable to sync each other. This message is received on the secondary host:

```
State check detected an Active mate

Unable to verify vlan configuration with mate.
Check that mate's failover is enabled

No Response from Mate
```

OR

The output of the **show failover** command shows the failover status on secondary module is OFF, FWSM failover state in Failover Off (pseudo-Standby).

```
FWSM-secondary(config)#show failover
Failover Off (pseudo-Standby)
```

Solution

The problem might be the mismatch VLAN assignment across the firewall (FWSMs and supervisors). For example, in the Firewall vlan-group 1 statement, the same number of VLANs assigned on each switch to the firewall can vary. This might cause the issue. If you assign the same number of VLANs in the firewall, then failover will work.

In order to avoid getting a VLAN configuration mismatch error, the **show vlan** command output must be identical on both FWSMs. This error message only occurs when you modify or load the failover configuration on the FWSM. For example, when a FWSM boots it loads the startup-config from the flash and attempts to initialize failover. At this time, it checks to make sure both modules are receiving the correct VLANs. If the VLANs do not match, the error message is displayed and failover remains disabled.

Note: For failover to work, the FWSM requires identical configurations and port assignments. It is possible to do inter-chassis failover, but each VLAN assigned to the firewall must be in the trunk between the two

chassis.

FWSM does not include any external physical interfaces. Instead, it uses VLAN interfaces. Assigning VLANs to the FWSM is similar to assigning a VLAN to a switch port. The FWSM includes an internal interface to the Switch Fabric Module (if present) or the shared bus. For more information, refer to Assigning VLANs to the Firewall Services Module.

Be aware that the VLAN mapping can get modified during a working FWSM setup and will fail during next boot.

Problem

When stateful failover between two FWSMs is enabled, the FWSMs stop working.

Solution

The problem might be the **spanning-tree vlan priority** is configured while stateful failover is enabled. Sometimes, enabling stateful failover when VLAN with spanning tree priority is configured might cause the problem and stop working the FWSMs.

You might have to remove the **spanning-tree vlan priority** command when stateful failover is enabled in the switch in order to avoid the issues with FWSM.

In order to remove the **spanning-tree vlan priority** command:

```
no spanning-tree vlan 333 priority 8000
```

Failover is Disabled in the Configuration

If failover is disabled in the configuration in the flash, then it will be disabled when it reloads.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- **FWSM: Configuring Failover**
- **FWSM: System Log Messages**
- **Technical Support & Documentation – Cisco Systems**

