

# Catalyst 6500 FWSM – Replacement of Failover Unit after a Hardware Failure

Document ID: 65604

---

## Introduction

### Prerequisites

Requirements

Components Used

Conventions

### Overview

### Upgrade the FWSM Code

Enable a New Switch VLAN that is not Currently in Use

### Define Firewall VLANs on the Switch

### Basic FWSM for Failover Configuration

### Confirm Setup and Configuration

### NetPro Discussion Forums – Featured Conversations

### Related Information

---

## Introduction

This document describes how to configure and upgrade a replacement Firewall Services Module (FWSM) for one that has failed. This document also describes how to configure the Catalyst 6500 Series Switch in order to minimize downtime. This applies to a FWSM as part of a failover pair, and a FWSM that is already physically swapped (refer to the hardware installation guide for details).

## Prerequisites

### Requirements

Before you complete the procedures in this document:

- Ensure the basic properties of your switch are configured.

**Note:** This document does not describe the initial configuration of the FWSM and switch. Rather, it assumes the FWSM and switch successfully worked before a hardware failure.

### Components Used

The information in this document is based on the Cisco Catalyst 6500 Series Firewall Services Module.

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 the Cisco Technical Tips Conventions for more information on document conventions.

# Overview

These steps instruct you in the configuration, upgrade, and replacement of the FWSM. The steps are explained in further detail in the remaining sections of this document.

1. Define a separate VLAN as a firewall VLAN (remove the old firewall VLAN definitions) on the switch with the replacement FWSM.
2. Plug a PC into the Catalyst 6000 and assign the switch port to the same VLAN that you just defined.
3. Session to the FWSM and enable an interface.
4. Use the PC as a TFTP server to download the software. Ensure that you use the same version of code as the current Active device.
5. Configure basic failover settings on the FWSM and restore the old firewall VLANs and the failover interface (remove the interface configured for TFTP). At this time, configuration replication occurs and the FWSM becomes the backup.

## Upgrade the FWSM Code

In order to run failover, the two FWSMs must run the same version of code. In the case that the RMA'd FWSM does not come with the same version of code as the active firewall, complete these steps in order to upgrade.

Download FWSM software ( registered customers only) to your TFTP server.

## Enable a New Switch VLAN that is not Currently in Use

Complete these steps:

1. Add the VLAN to the switch.

The VLAN cannot be a reserved VLAN.

- ◆ Use the **vlan vlan\_number** command to add the VLAN if you run Cisco IOS® software on the switch.
  - ◆ Use the **set vlan vlan\_number** command to add the VLAN if you run Catalyst Operating System software on the switch.
2. Assign the VLAN to the switch port to which you plan to connect the PC.

- ◆ Enter these commands in order to assign a VLAN to a port, using Cisco IOS software:

```
router(config)#interface type slot/port
```

```
router(config-if)#switchport
```

```
router(config-if)#switchport mode access
```

```
router(config-if)#switchport access vlan vlan_id
```

- ◆ Enter this command in order to assign a VLAN to a port, using Catalyst Operating System software:

```
set vlan vlan_number mod/ports
```

3. Copy the old firewall commands to Notepad in order to back them up. Next, remove and then replace them by substituting the VLAN defined in steps 1 and 2.

- ◆ For Cisco IOS software:

```
Router(config)#firewall vlan-group firewall_group vlan_range
```

```
Router(config)#firewall module module_number vlan-group firewall_group
```

- ◆ For Catalyst Operating System software:

```
Console> (enable) set vlan vlan_list firewall-vlan mod_num
```

4. Enable an interface on the FWSM and IP address:

```
nameif interface interface_name security_lvl
```

```
ip address interface_name ip_address [mask]
```

```
interface interface_name
```

```
fwsn(config-interface) no shutdown
```

5. Test connectivity between the FWSM and the PC, using ping. Use this command to download the image from the TFTP server when connectivity is confirmed. Reload the FWSM when the download is complete.

```
FWSM#copy tftp://server[/path]/filename flash:
```

For example, enter this command:

```
FWSM#copy tftp://209.165.200.226/cisco/c6svc-fwm-k9.2-1-1.bin flash:
```

## Define Firewall VLANs on the Switch

Replace the commands that you removed in step 1 of the Upgrade the FWSM Code procedure.

- For Cisco IOS software:

```
Router(config)#firewall vlan-group firewall_group vlan_range
```

```
Router(config)#firewall module module_number vlan-group firewall_group
```

- For the Catalyst Operating System software:

```
Console> (enable)set vlan vlan_list firewall-vlan mod_num
```

## Basic FWSM for Failover Configuration

Setup some basic FWSM settings to prepare it for re-introduction into the pair. Then reconfigure the switch firewall groups/firewall VLANs to include it back into the failover pair.

1. Remove the old nameif and IP address defined in step 4 of the Enable a New Switch VLAN that is not Currently in Use procedure.

2. Define the device as the primary or secondary.

```
FWSM(config)#fail lan unit {primary|secondary}
```

3. Enter this command in the system execution space to configure the failover VLAN interface for multiple context mode:

```
primary(config)#failover lan interface interface_name vlan vlan
```

4. Enter this command to set the IP address of the failover interface:

```
primary(config)#failover interface ip failover_interface ip_address mask standby ip_address
```

5. Enable failover:

```
FWSM(config)#failover
```

This output shows an example:

```
FWSM(config)#failover lan unit secondary
FWSM(config)#failover interface ip fover 10.1.1.10 255.255.255.0 standby 10.1.1.11
FWSM(config)#failover LAN Interface fover vlan 50
FWSM(config)#failover
```

This output appears:

```
Detected an Active mate. Switching to Standby

Beginning configuration replication from mate.
This unit is in syncing state.
End configuration replication from mate.
```

## Confirm Setup and Configuration

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Issue this **show** command:

```
fws(config)#show failover
Failover On
Failover unit Primary
Failover LAN Interface fover Vlan 150
Unit Poll frequency 15 seconds
Interface Poll frequency 15 seconds
Interface Policy 50%
Monitored Interfaces 249 of 250 maximum
Config sync: active
Last Failover at: 10:58:08 Apr 15 2004
  This host: Primary - Standby
    Active time: 0(sec)
    admin Interface inside (10.6.8.91): Normal
    admin Interface outside (70.1.1.2): Normal
  Other host: Secondary - Active
    Active time: 2232 (sec)
    admin Interface inside (10.6.8.100): Normal
    admin Interface outside (70.1.1.3): Normal
```

Check to see that This host is in standby. Also check to see if you can ping devices off your interfaces from the FWSM. If you want the new device to become active, use the **no active failover** command to force

failover.

Enter this command on the active module to failover to the standby module:

```
primary(config)#no failover active
```

Enter this command on the standby module to force it to become active:

```
secondary(config)#failover active
```

Refer to Using Failover for more details on failover configuration options and troubleshooting.

## 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

- [Cisco Catalyst 6500 Series Firewall Services Module Product Support](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Jul 19, 2007

Document ID: 65604

---