

## Failover in Action

This Cisco Firewall Video Mentor lab demonstrates several different conditions that cause a failure in a firewall interface or unit. This, in turn, triggers the failover operation.

This lab also works through the “hitless” upgrade process, where you can upgrade the operating system image in each of the active-active failover units—without impacting the traffic passing through the firewall pair.

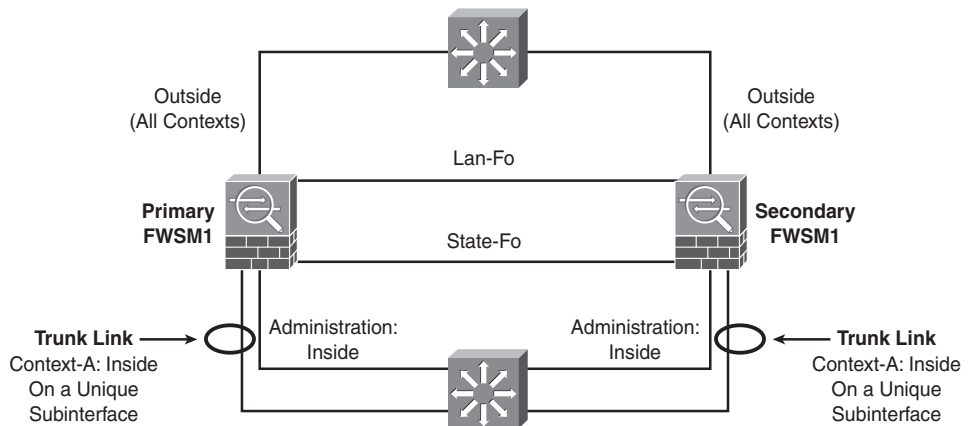
The objectives of this lab are as follows:

- Observe a physical interface failure
- Observe a logical interface failure
- Observe a failover unit failure
- Observe a hitless upgrade

## Scenario

This lab contains several failover demonstrations, using the two firewalls from Lab 6 configured as a failover pair. A network diagram of the failover pair is shown in Figure 7-1.

**Figure 7-1 Network Diagram for Lab 7 Scenarios**



- Scenario 1: Force the link state on the “admin” context inside interface to go down. This causes a failure on a physical firewall interface, which triggers a failover operation.
- Scenario 2: Remove the VLAN used on the “context-a” context inside interface while the interface stays up. This causes a failure on a logical interface, which indirectly triggers a failover operation.

- Scenario 3: Reload the primary firewall unit suddenly, as if it experiences a power cycle. This causes the failure of an entire firewall unit, which triggers a failover operation.
- Scenario 4: Manually control the failover operation so that the code image can be upgraded on each firewall unit. The upgrades occur while live connections are being handled by the failover pair, such that no traffic is impacted or lost.

## Initial Configurations

The failover pair of ASA devices configured in Lab 6 is used for the interface and unit failover demonstrations. No additional configuration commands are necessary to perform the first three scenarios.

The final scenario involves active-active failover and a hitless upgrade on two running firewalls. The FWSM platform is used. The initial configurations are listed in the Scenario 4 section.

## Video Presentation Reference

Refer to the following descriptions of each scenario presented in Lab 7.

### Scenario 1: Physical Interface Failure

In this scenario, the interface polltime remains configured at 500 ms, with a holdtime of 5 seconds. The switch interface connected to the primary unit's "admin" context inside interface (physical interface Ethernet0/0) is shut down, causing the link status to go down.

No additional configuration is necessary on the failover pair.

### Scenario 2: Logical Interface Failure

In this scenario, the interface polltime remains configured at 500 ms, with a holdtime of 5 seconds. The inside interface of the "context-a" context is mapped to VLAN 100, which is carried over a trunk link from an upstream switch to each firewall in the failover pair.

On the switch connected to the primary failover unit, VLAN 100 is removed from the trunk. This simulates a failure on a logical interface, where the two failover units can no longer communicate with each other on the context interface.

No additional configuration is necessary on the failover pair.

## Scenario 3: Failover Unit Failure

In this scenario, the unit polltime remains configured at 200 ms, with a holdtime of 800 ms. You reload the entire primary failover unit by entering the **reload** command from the system execution space.

This simulates a failover unit failure, where the secondary unit can no longer detect the primary unit.

No additional configuration is necessary on the failover pair.

## Scenario 4: Hitless Code Upgrade

In this scenario, the two failover units are configured for active-active failover operation. This scenario is unique because it uses two FWSMs as a failover pair.

The primary FWSM unit begins with the multiple context configuration that resulted from Lab 6. The initial Catalyst 6500 configuration commands related to FWSM operation are shown in Example 7-1. In this case, the primary FWSM is contained in module 3, and the secondary FWSM in slot 4.

### Example 7-1 Initial Catalyst 6500 Supervisor Configuration

```

vlan 2
  name lan-fo
!
vlan 3
  name stateful-fo
!
vlan 10
  name FWSM-outside
!
vlan 100
  name FWSM-inside
!
vlan 101
  name context-a-inside
!
vlan 102
  name context-b-inside
  firewall vlan-group 1 2,3,10,100-103
!
firewall module 3 vlan-group 1
firewall module 4 vlan-group 1

```

The initial configuration commands for the primary FWSM system execution space are shown in Example 7-2.

**Example 7-2 Initial FWSM System Execution Space Configuration**

```
hostname fwsm1
domain-name mycompany.com
enable password iE9e1CM0vCJAfUw3 encrypted
passwd 11L6nJyCpFrdy9oK encrypted
!
interface Vlan2
  description LAN Failover Interface
!
interface Vlan3
  description STATE Failover Interface
!
interface Vlan10
!
interface Vlan100
!
interface Vlan101
!
interface Vlan102
!
failover
failover lan unit primary
failover lan interface lan-fo Vlan2
failover polltime unit msec 500 holdtime 3
failover key *****
failover replication http
failover link state-fo Vlan3
failover interface ip lan-fo 192.168.254.1 255.255.255.0 standby 192.168.254.2
failover interface ip state-fo 192.168.253.1 255.255.255.0 standby 192.168.253.2
failover group 1
  preempt
  polltime interface 3
failover group 2
  secondary
  preempt
  polltime interface 3
!
admin-context admin
context admin
  description Admin context
  allocate-interface Vlan10
  allocate-interface Vlan100
  config-url disk:/admin.cfg
  join-failover-group 1
!
```

**Example 7-2 Initial FWSM System Execution Space Configuration**

```

context context-a
  description Example context A
  allocate-interface Vlan10 intf0
  allocate-interface Vlan101 intf1
  config-url disk:/context-a.cfg
  join-failover-group 1
!

context context-b
  description Example context B
  allocate-interface Vlan102 intf1
  allocate-interface Vlan103 intf0
  config-url disk:/context-b.cfg
  join-failover-group 2

```

The initial configuration commands for the primary FWSM “admin” context are shown in Example 7-3.

**Example 7-3 Initial FWSM “admin” Context Configuration**

```

hostname admin
passwd 1lL6nJyCpFrDy9oK encrypted
enable password iE9e1CM0vCJAfUw3 encrypted
!
interface Vlan10
  nameif outside
  security-level 0
  ip address 192.168.100.1 255.255.255.0 standby 192.168.100.2
!
interface Vlan100
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
monitor-interface outside
route outside 0.0.0.0 0.0.0.0 192.168.100.3 1
http 0.0.0.0 0.0.0.0 outside
http server enable
ssh 0.0.0.0 0.0.0.0 outside
ssh version 2
!
tftp-server outside 192.168.100.239 /

```

The initial configuration commands for the primary FWSM “context-a” context are shown in Example 7-4.

#### Example 7-4 Initial FWSM “context-a” Context Configuration

```
hostname context-a
domain-name mycompany.com
passwd 1lL6nJyCpFrDy9oK encrypted
enable password iE9e1CM0vCJAfUw3 encrypted
!
interface intf0
  nameif outside
  security-level 0
  ip address 192.168.100.10 255.255.255.0 standby 192.168.100.11
!
interface intf1
  nameif inside
  security-level 100
  ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2
!
access-list acl_outside extended permit ip 172.21.4.0 255.255.254.0 host
  192.168.100.100
access-list acl_inside extended permit ip 192.168.2.0 255.255.255.0 any
access-list acl_in extended permit ip 192.168.2.0 255.255.255.0 any
!
static (inside,outside) 192.168.100.100 192.168.2.100 netmask 255.255.255.255
!
access-group acl_outside in interface outside
access-group acl_in in interface inside
route outside 0.0.0.0 0.0.0.0 192.168.100.3 1
!
http server enable
http 0.0.0.0 0.0.0.0 outside
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 30
ssh version 2
```

The initial configuration commands for the primary FWSM “context-b” context are shown in Example 7-5.

**Example 7-5 Initial FWSM “context-b” Context Configuration**

```

hostname context-b
domain-name mycompany.com
passwd 1lL6nJyCpFrDy9oK encrypted
enable password iE9e1CM0vCJAfUw3 encrypted
!
interface intf1
  nameif inside
  security-level 100
  ip address 192.168.3.1 255.255.255.0 standby 192.168.3.2
!
interface intf0
  nameif outside
  security-level 0
  ip address 192.168.100.20 255.255.255.0 standby 192.168.100.21
!
http 0.0.0.0 0.0.0.0 outside
http server enable
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 30
ssh version 2

```

Finally, the initial configuration for the system execution space and all contexts are identical on the secondary FWSM unit—except for the failover configuration in the system execution space. The secondary unit’s failover configuration commands are shown in Example 7-6.

**Example 7-6 Initial Secondary FWSM Failover Configuration**

```

failover
failover lan unit secondary
failover lan interface lan-fo Vlan2
failover polltime unit msec 500 holdtime 3
failover key *****
failover replication http
failover link state-fo Vlan3
failover interface ip lan-fo 192.168.254.1 255.255.255.0 standby 192.168.254.2
failover interface ip state-fo 192.168.253.1 255.255.255.0 standby 192.168.253.2
failover group 1
  preempt
  polltime interface 3
failover group 2
  secondary
  preempt
  polltime interface 3

```

The primary unit is active for the “admin” and “context-a” contexts, and the secondary unit is active for the “context-b” context. The code image running on each failover unit is upgraded from 3.2(1) to 3.2(2) individually, as part of a hitless upgrade process.

The following steps demonstrate the hitless upgrade. All commands are entered in the system execution space on the primary unit.

**Step 1.** Download the new code image to each failover unit.

The code image is downloaded into FWSM flash with the following command:

```
Firewall# copy ftp: flash:image
```

Currently the FWSM platform supports only one code image in flash memory. Therefore, you don’t have to configure the specific image location and filename, as the ASA platform requires.

**Step 2.** Force the primary unit to be active in all contexts.

The following command causes the primary unit to immediately take the active role in all contexts:

```
Firewall# failover active
```

**Step 3.** Reload the secondary unit:

```
Firewall# failover reload-standby
```

When you force the secondary unit to reload, it automatically picks up the new code image.

**Step 4.** Swap failover roles.

As soon as the secondary unit finishes reloading and the failover operation has stabilized, the following command is used to push the active role to the secondary unit:

```
Firewall# no failover active
```

The primary unit immediately tells the secondary unit to take over the active role in all contexts, while the primary unit assumes the standby role.

**Step 5.** Reload the primary unit:

```
Firewall# reload
```

When you force the primary unit to reload, it automatically picks up the new code image. In the meantime, the secondary unit handles all firewall operations.

**Step 6.** Resume the original failover roles.

As soon as the primary unit has finished reloading and the failover operation has stabilized, the unit needs to take over the active role in the “admin” and “context-a” contexts—returning to the role it had before the hitless upgrade began. The following command can be used to accomplish this:

```
Firewall# failover active group 1
```

However, because the primary unit has been configured to preempt the active role for failover group 1, it automatically assumes the active role as soon as it reloads.