Replace an ASA Firewall into an Active/Standby Failover Pair

Contents

Introduction

This document describes how to replace an Adaptive Security Appliance (ASA) firewall with an active/standby failover pair.

Background Information

The ASA firewalls support two failover configurations, active/active failover, and active/standby failover.

There are 2 firewalls:

- firewall-a is primary/active
- firewall-b is secondary/standby

Difference between Primary and Secondary Units in the Failover Configuration

This command means this firewall always pushes the active configuration to the secondary firewall.

```
# failover lan unit primary
```

This command means this firewall always receives the active configuration from the primary firewall.

```
# failover lan unit secondary
```

Difference between Active and Standby Units in the Failover Configuration

This command means this firewall is the active running firewall in the failover pair.

```
# failover active
```

This command means this firewall is the standby running a firewall in the failover pair.

```
# failover standby
```

Replace the Secondary Firewall Failure

1. Validate that the primary firewall is active and online. For example:

```
firewall-a/pri/act# show failover
Failover On
Failover unit Primary
Failover LAN Interface: sync Port-channel1 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL1, Mate JADSERIAL2
Last Failover at: 19:54:29 GMT May 23 2023
    This host: Primary - Active
        Active time: 2204 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.1): Normal (Not-Monitored)
          Interface outside (10.1.1.1): Normal (Not-Monitored)
          Interface management (10.2.2.1): Normal (Not-Monitored)
    Other host: Secondary - Failed
        Active time: 0 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.2): Normal (Not-Monitored)
          Interface outside (10.1.1.2): Normal (Not-Monitored)
          Interface management (10.2.2.2): Normal (Not-Monitored)
```

2. Shut down and physically remove the secondary firewall.

3. Physically add the new secondary firewall and power it on.

4. Once the new secondary firewall is active with the default factory configuration, enable the failover link, `no shutdown` the failover physical link.

Example:

```
firewall-a/pri/act#conf t
firewall-a/pri/act#(config)#interface Port-channel1
firewall-a/pri/act#(config-if)#no shutdown
firewall-a/pri/act#(config)#exit
firewall-a/pri/act#
firewall-b/sec/stby#conf t
firewall-b/sec/stby#(config)#interface Port-channel1
firewall-b/sec/stby#(config-if)#no shutdown
firewall-b/sec/stby#(config)#exit
firewall-b/sec/stby#
```

5. Configure failover commands. For example:

```
firewall-a/pri/act# sh run | inc fail
failover
failover lan unit primary
failover lan interface sync Port-channel1
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-a/pri/act#

firewall-b/sec/stby# sh run | inc fail
no failover
failover lan unit secondary
failover lan interface sync Port-channel1
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-b/sec/stby#
```

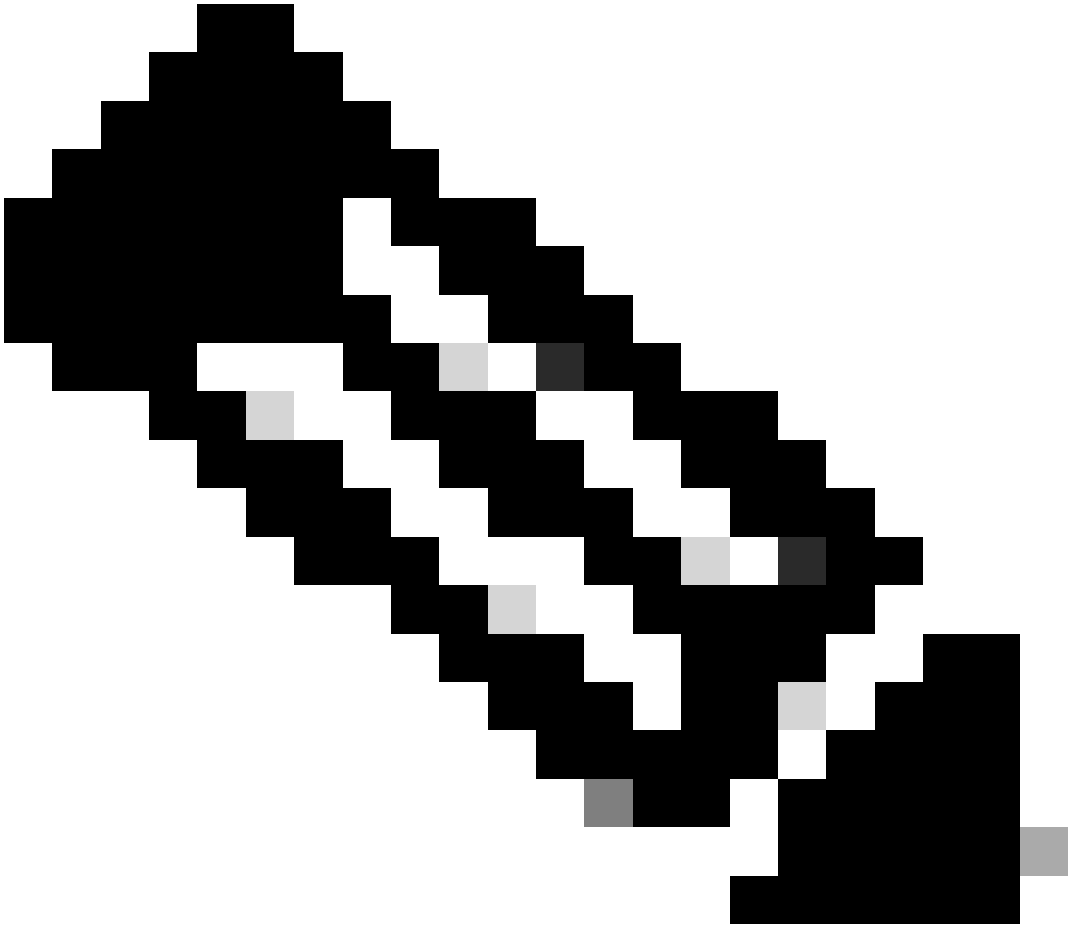
6. Enable failover on the new secondary firewall. For example:

```
firewall-b/sec/stby#conf t
firewall-b/sec/stby#(config)#failover
firewall-b/sec/stby#(config)#exit
firewall-b/sec/stby#
firewall-b/sec/stby# sh run | inc fail
failover
firewall-b/sec/stby#
```

7. Wait for the active configuration to sync to the new unit and validate the correct failover state. For example:

```
firewall-a/pri/act#
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate
firewall-a/pri/act#
```

```
firewall-b/sec/stby#
Beginning configuration replication from mate.
End configuration replication from mate.
firewall-b/sec/stby#
```



Note: Notice the primary firewall (firewall-a) sends the configuration to the secondary firewall (firewall-b).

---

8. Save the configuration on the primary/active and validate the write memory on the new secondary/standby. For example:

```
firewall-a/pri/act#write memory
Building configuration...
Cryptochecksum: ad317407 935a773c 6c5fb66a c5edc342
64509 bytes copied in 9.290 secs (7167 bytes/sec)
[OK]
firewall-a/pri/act#
firewall-b/sec/stby#
```

May 24 2023 15:16:21 firewall-b : %ASA-5-111001: Begin configuration: console writing to memory
May 24 2023 15:16:22 firewall-b : %ASA-5-111004: console end configuration: OK
May 24 2023 15:16:22 firewall-b : %ASA-5-111008: User 'failover' executed the 'write memory' command.
May 24 2023 15:16:22 firewall-b : %ASA-5-111010: User 'failover', running 'N/A' from IP x.x.x.x , executed 'write memory'
firewall-b/sec/stby#

9. Validate the failover pair is up/up active on both firewalls. For example:

```
firewall-a/pri/act# show failover
Failover On
Failover unit Primary
Failover LAN Interface: sync Port-channel1 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL1, Mate JADSERIAL2
Last Failover at: 19:54:29 GMT May 23 2023
    This host: Primary - Active
        Active time: 71564 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.1): Normal (Not-Monitored)
          Interface outside (10.1.1.1): Normal (Not-Monitored)
          Interface management (10.2.2.1): Normal (Not-Monitored)
    Other host: Secondary - Standby Ready
        Active time: 0 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.2): Normal (Not-Monitored)
          Interface outside (10.1.1.2): Normal (Not-Monitored)
          Interface management (10.2.2.2): Normal (Not-Monitored)

firewall-b/sec/stby# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: sync Port-channel1 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL2, Mate JADSERIAL1
Last Failover at: 20:51:27 GMT May 23 2023
    This host: Secondary - Standby Ready
        Active time: 0 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.2): Normal (Not-Monitored)
          Interface outside (10.1.1.2): Normal (Not-Monitored)
          Interface management (10.2.2.2): Normal (Not-Monitored)
    Other host: Primary - Active
        Active time: 71635 (sec)
```

```
    slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
      Interface inside (10.0.0.1: Normal (Not-Monitored)
      Interface outide (10.1.1.1): Normal (Not-Monitored)
      Interface management (10.2.2.1): Normal (Not-Monitored)
```

Replace the Primary Firewall Failure

1. Validate that the secondary firewall is active and online. For example:

```
firewall-b/sec/act# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: sync Port-channel1 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL2, Mate JADSERIAL1
Last Failover at: 19:54:29 GMT May 23 2023
   This host: Secondary - Active
      Active time: 2204 (sec)
      slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
        Interface inside (10.0.0.1): Normal (Not-Monitored)
        Interface outside (10.1.1.1): Normal (Not-Monitored)
        Interface management (10.2.2.1): Normal (Not-Monitored)
   Other host: Primary - Failed
      Active time: 0 (sec)
      slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
        Interface inside (10.0.0.2): Normal (Not-Monitored)
        Interface outside (10.1.1.2): Normal (Not-Monitored)
        Interface management (10.2.2.2): Normal (Not-Monitored)
```

2. Shut down and physically remove the primary firewall.
3. Physically add the new primary firewall and power it on.
4. Now, the new primary firewall gets active with the default factory configuration.
5. Enable the failover link, **no shutdown** the failover physical link. For example:

```
firewall-a/pri/stby#conf t
firewall-a/pri/stby#(config)#interface Port-channel1
firewall-a/pri/stby#(config-if)#no shutdown
firewall-a/pri/stby#(config)#exit
firewall-a/pri/stby#

firewall-b/sec/act#conf t
firewall-b/sec/act#(config)#interface Port-channel1
firewall-b/sec/act#(config-if)#no shutdown
firewall-b/sec/act#(config)#exit
```

```
firewall-b/sec/act#
```

6. Save configuration. Write memory on the **secondary/active firewall** and ensure the **failover lan unit secondary** is in the startup configuration.

Example:

```
firewall-b/sec/act# write memory
Building configuration...
Cryptochecksum: ad317407 935a773c 6c5fb66a c5edc342

64509 bytes copied in 9.290 secs (7167 bytes/sec)
[OK]
firewall-b/sec/act# show start | inc unit
failover lan unit secondary
firewall-b/sec/act#
```

7. Configure failover commands.
    1. On the secondary/active firewall, you must first set the **failover lan unit primary** command to ensure the active configuration is pushed from the secondary/active firewall to the new default configuration primary/standby firewall. For example:

```
firewall-b/sec/act# sh run | inc unit
failover lan unit secondary
firewall-b/sec/act#

firewall-b/sec/act#conf t
firewall-b/sec/act#(config)#failover lan unit primary
firewall-b/sec/act#(config)#exit
firewall-b/sec/act# sh run | inc unit
failover lan unit primary
firewall-b/pri/act#
```

b. Validate failover configuration on both devices. For example:

```
firewall-b/pri/act# sh run | inc fail
failover
failover lan unit primary
failover lan interface sync Port-channel1
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-b/pri/act#

firewall-a/sec/stby# sh run | inc fail
no failover
failover lan unit secondary
failover lan interface sync Port-channel1
```

```
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-a/sec/stby#
```

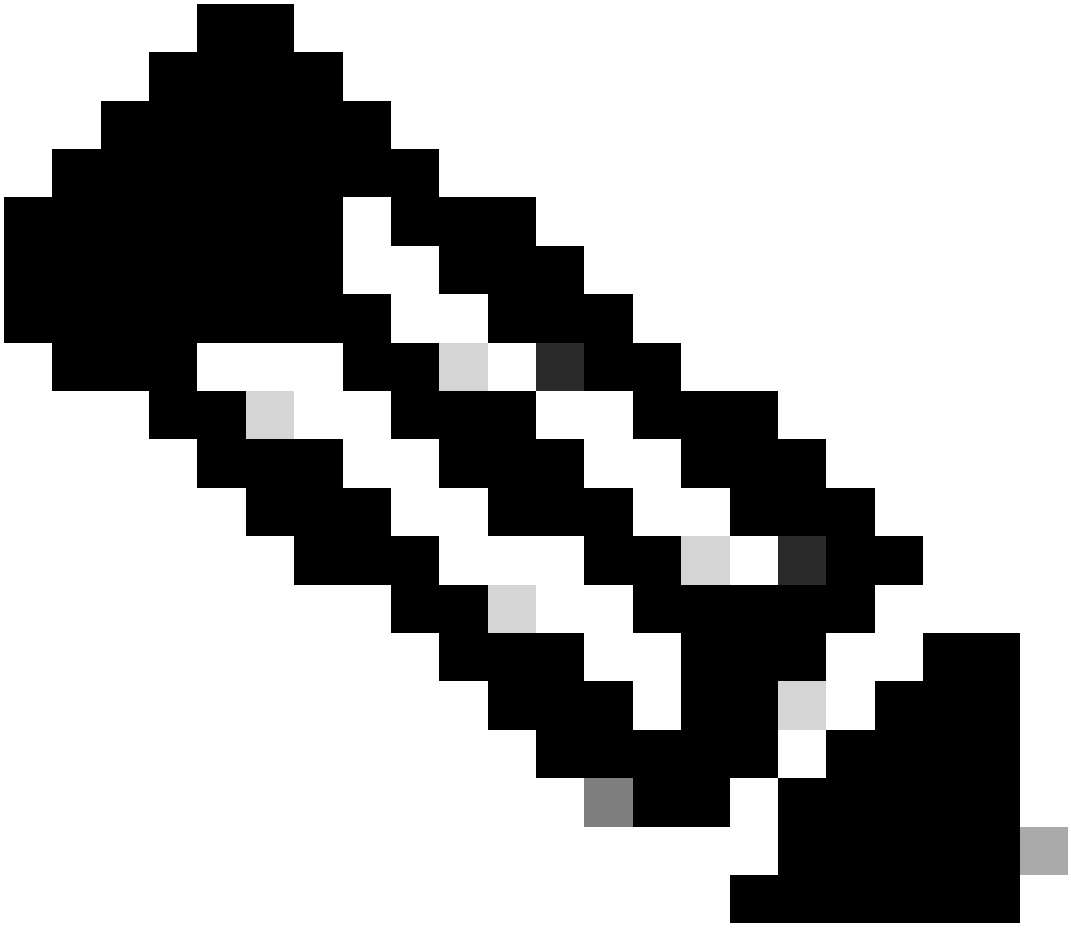
8. Enable failover on the new primary firewall. For example:

```
firewall-a/sec/stby#conf t
firewall-a/sec/stby#(config)#failover
firewall-a/sec/stby#(config)#exit
firewall-a/sec/stby#

firewall-a/sec/stby# sh run | inc fail
failover
firewall-a/sec/stby#
```

9. Wait for the active configuration to sync to the new unit and validate the correct failover state. For example:

```
firewall-b/pri/act#
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate
firewall-b/pri/act#
firewall-a/sec/stby#
Beginning configuration replication from mate.
End configuration replication from mate.
firewall-a/sec/stby#
```



Note: Notice the primary firewall (firewall-b) sends the configuration to the secondary firewall (firewall-a). Do not write memory on the now primary/active firewall (firewall-b).

10. Reload the now primary/active firewall (firewall-b) so that it boots back up as the secondary/standby firewall.

```
firewall-b/pri/act#reload
```

11. Right after you execute the "firewall-b reload" command (wait for 15 seconds), switch to the new Primary Firewall (firewall-a) and enter the **failover lan unit primary** command, followed by **write memory**.

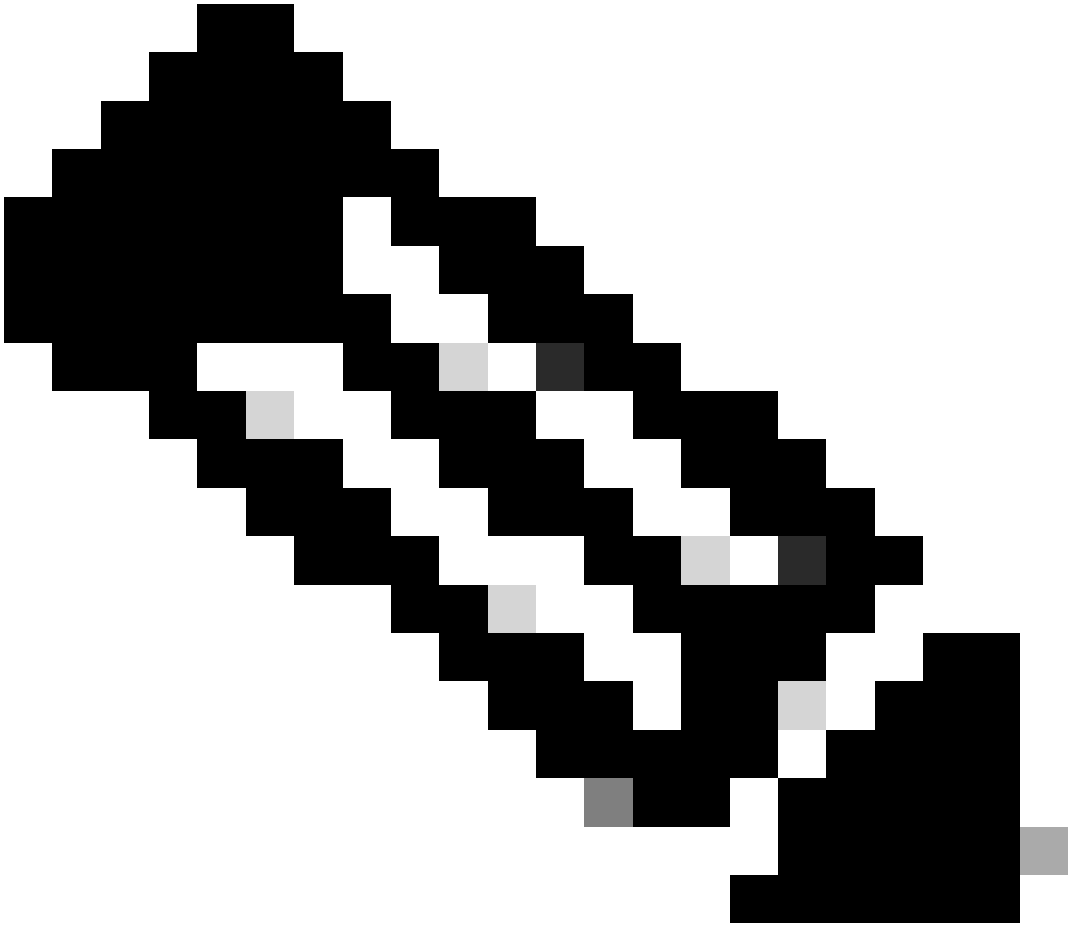
```
firewall-a/sec/act#conf t
firewall-a/sec/act#(config)#failover lan unit primary
firewall-a/sec/act#(config)#exit
firewall-a/sec/act# sh run | inc unit
```

```
failover lan unit primary
firewall-a/pri/act# write memory
Building configuration...
Cryptochecksum: ad317407 935a773c 6c5fb66a c5edc342

64509 bytes copied in 9.290 secs (7167 bytes/sec)
[OK]
firewall-a/pri/act# show start | inc unit
failover lan unit primary
firewall-a/pri/act#
```

12. Wait for firewall-b to fully boot up and join the failover pair as secondary/standby. For example:

```
firewall-a/pri/act#
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate
firewall-a/pri/act#
firewall-b/sec/stby#
Beginning configuration replication from mate.
End configuration replication from mate.
firewall-b/sec/stby#
```



Note: Please take note that the primary firewall (firewall-a) sends the configuration to the secondary firewall (firewall-b).

13. Save configuration, write memory on the primary/active, and validate the write memory on the new secondary/standby. For example:

```
firewall-a/pri/act#write memory
Building configuration...
Cryptochecksum: ad317407 935a773c 6c5fb66a c5edc342

64509 bytes copied in 9.290 secs (7167 bytes/sec)
[OK]
firewall-a/pri/act#

firewall-b/sec/stby#
May 24 2023 15:16:21 firewall-b : %ASA-5-111001: Begin configuration: console writing to memory
May 24 2023 15:16:22 firewall-b : %ASA-5-111004: console end configuration: OK
May 24 2023 15:16:22 firewall-b : %ASA-5-111008: User 'failover' executed the 'write memory' command.
May 24 2023 15:16:22 firewall-b : %ASA-5-111010: User 'failover', running 'N/A' from IP x.x.x.x , executed 'write memory'
```

```
firewall-b/sec/stby#
```

14. Validate the failover pair is up/up active on both firewalls. For example:

```
firewall-a/pri/act# show failover
Failover On
Failover unit Primary
Failover LAN Interface: sync Port-channel1 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL1, Mate JADSERIAL2
Last Failover at: 19:54:29 GMT May 23 2023
    This host: Primary - Active
        Active time: 71564 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.1): Normal (Not-Monitored)
          Interface outside (10.1.1.1): Normal (Not-Monitored)
          Interface management (10.2.2.1): Normal (Not-Monitored)
    Other host: Secondary - Standby Ready
        Active time: 0 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.2): Normal (Not-Monitored)
          Interface outside (10.1.1.2): Normal (Not-Monitored)
          Interface management (10.2.2.2): Normal (Not-Monitored)

firewall-b/sec/stby# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: sync Port-channel1 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL2, Mate JADSERIAL1
Last Failover at: 20:51:27 GMT May 23 2023
    This host: Secondary - Standby Ready
        Active time: 0 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.2): Normal (Not-Monitored)
          Interface outside (10.1.1.2): Normal (Not-Monitored)
          Interface management (10.2.2.2): Normal (Not-Monitored)
    Other host: Primary - Active
        Active time: 71635 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.1: Normal (Not-Monitored)
          Interface outide (10.1.1.1): Normal (Not-Monitored)
          Interface management (10.2.2.1): Normal (Not-Monitored)
```