将ASA防火墙替换为主用/备用故障转移对

目录

简介

本文档介绍如何用主用/备用故障转移对替换自适应安全设备(ASA)防火墙。

背景信息

ASA防火墙支持两种故障切换配置：主用/主用故障切换和主用/备用故障切换。

有2个防火墙：

- firewall-a is primary/active
- 防火墙b为辅助/备用

故障切换配置中主设备和辅助设备之间的区别

此命令意味着此防火墙始终将活动配置推送到辅助防火墙。

```
# failover lan unit primary
```

此命令意味着此防火墙始终从主防火墙接收活动配置。

```
# failover lan unit secondary
```

故障切换配置中主用设备和备用设备之间的区别

此命令意味着此防火墙是故障转移对中的活动运行防火墙。

```
# failover active
```

此命令意味着此防火墙是运行故障切换对中防火墙的备用防火墙。

```
# failover standby
```

替换辅助防火墙故障

1. 验证主防火墙是否处于活动状态并处于联机状态。例如：

```
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. 关闭并实际移除辅助防火墙。

3. 以物理方式添加新的辅助防火墙并打开其电源。

4. 当新的辅助防火墙以默认出厂配置处于活动状态时，启用故障切换链路no shutdown(即故障切换物理链路)。

示例：

```
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. 配置故障切换命令。例如：

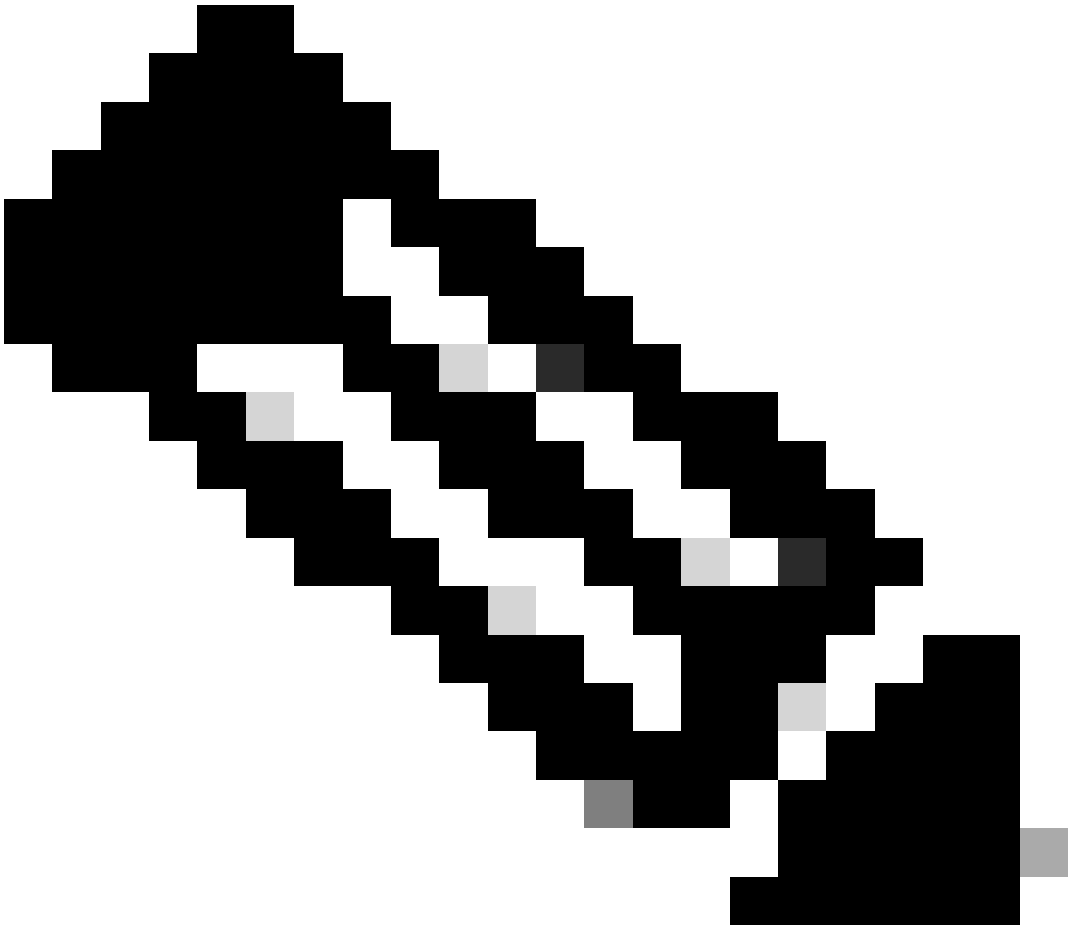
```
firewall-a/pri/act# sh run | inc fail
failover
failover lan unit primary
failover lan interface sync Port-channel1
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-a/pri/act#

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. 在新的辅助防火墙上启用故障切换。例如：

```
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. 等待活动配置同步到新设备并验证正确的故障转移状态。例如：

```
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#
```



注意：请注意，主防火墙(firewall-a)将配置发送到辅助防火墙(firewall-b)。

---

8. 保存主/主上的配置并验证新的辅助/备用上的写入内存。例如：

```
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. 验证故障转移对在两个防火墙上均处于up/up活动状态。例如：

```
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)
```

替换主防火墙故障

1. 验证辅助防火墙是否处于活动状态并处于联机状态。例如：

```
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. 关闭并实际移除主防火墙。
3. 以物理方式添加新的主防火墙并打开其电源。
4. 现在，新的主防火墙使用默认出厂配置激活。
5. 启用故障切换链路，no shutdown故障切换物理链路。例如：

```
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. 保存配置.在辅助/活动防火墙上写入内存，并确保启动配置中有故障切换lan设备“secondary”。

示例：

```
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. 配置故障切换命令。
    1. 在辅助/活动防火墙上，必须首先设置failover lan unit primary命令，以确保活动配置从辅助/活动防火墙推送到新的默认配置主要/备用防火墙。例如：

```
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. 验证两台设备上的故障切换配置。例如：

```
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#
```

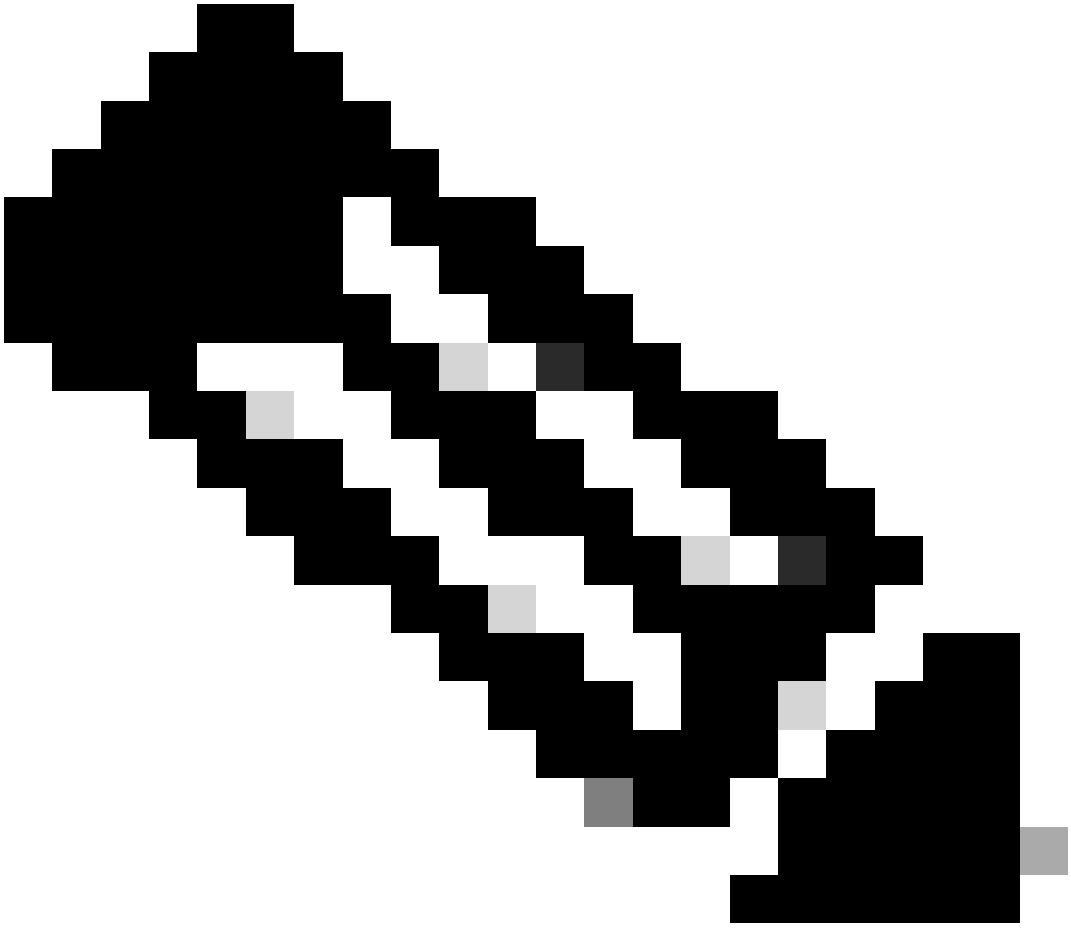
```
firewall-a/sec/stby# sh run | inc fail
no failover
failover lan unit secondary
failover lan interface sync Port-channel1
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-a/sec/stby#
```

8. 在新的主防火墙上启用故障切换。例如：

```
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. 等待活动配置同步到新设备并验证正确的故障转移状态。例如：

```
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#
```



注意：请注意，主防火墙(firewall-b)将配置发送到辅助防火墙(firewall-a)。请勿在现在的主用/主用防火墙(firewall-b)上写入内存。

10. 重新加载现在的主用/主用防火墙(firewall-b)，使其作为辅助/备用防火墙进行备份。

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

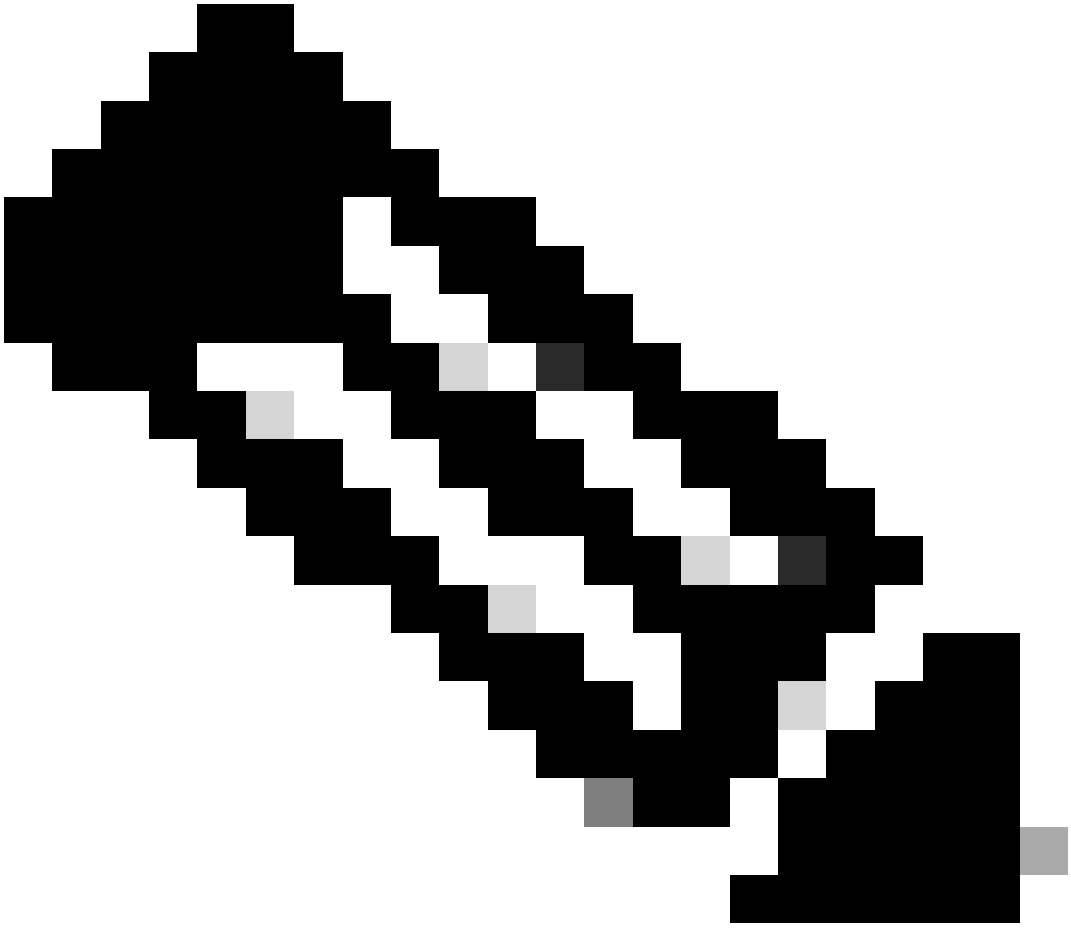
11. 在您执行“firewall-b reload”命令（等待15秒）之后，立即切换到新的主防火墙(firewall-a)，并输入failover lan unit primary命令，然后输入write memory。

```
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. 等待firewall-b完全启动，然后作为辅助/备用设备加入故障转移对。例如：

```
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#
```



注意：请注意，主防火墙(firewall-a)将配置发送到辅助防火墙(firewall-b)。

13. 保存配置，在主用/主用上写入内存，并验证新的辅助/备用上的写入内存。例如：

```
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. 验证故障转移对在两个防火墙上均处于up/up活动状态。例如：

```
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)
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。