

Ersetzen einer ASA-Firewall durch ein Aktiv/Standby-Failover-Paar

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Unterschied zwischen der primären und sekundären Einheit in der Failover-Konfiguration](#)

[Unterschied zwischen aktiven und Standby-Einheiten in der Failover-Konfiguration](#)

[Ersetzen Sie den sekundären Firewall-Fehler.](#)

[Ersetzen Sie den primären Firewall-Fehler.](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie eine Adaptive Security Appliance (ASA)-Firewall durch ein Aktiv/Standby-Failover-Paar ersetzen.

Hintergrundinformationen

Die ASA-Firewalls unterstützen zwei Failover-Konfigurationen: Active/Active-Failover und Active/Standby-Failover.

Es gibt 2 Firewalls:

- Firewall-a ist primär/aktiv
- Firewall-b ist sekundär/Standby

Unterschied zwischen der primären und sekundären Einheit in der Failover-Konfiguration

Dieser Befehl bedeutet, dass diese Firewall die aktive Konfiguration immer an die sekundäre Firewall weiterleitet.

```
# failover lan unit primary
```

Dieser Befehl bedeutet, dass diese Firewall immer die aktive Konfiguration von der primären Firewall erhält.

```
# failover lan unit secondary
```

Unterschied zwischen aktiven und Standby-Einheiten in der Failover-Konfiguration

Dieser Befehl bedeutet, dass diese Firewall die aktive aktive Firewall im Failover-Paar ist.

```
# failover active
```

Dieser Befehl bedeutet, dass diese Firewall als Standby-Firewall im Failover-Paar fungiert.

```
# failover standby
```

Ersetzen Sie den sekundären Firewall-Fehler.

1. Überprüfen Sie, ob die primäre Firewall aktiv und online ist. Beispiele:

```
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. Herunterfahren und physisches Entfernen der sekundären Firewall

3. Fügen Sie die neue sekundäre Firewall physisch hinzu, und schalten Sie sie ein.

4. Wenn die neue sekundäre Firewall mit der werkseitigen Standardkonfiguration aktiviert wurde, aktivieren Sie den Failover-Link, den physischen Failover-Link,no shutdown.

Beispiel:

```
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. Konfigurieren Sie Failover-Befehle. Beispiele:

```
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#
```

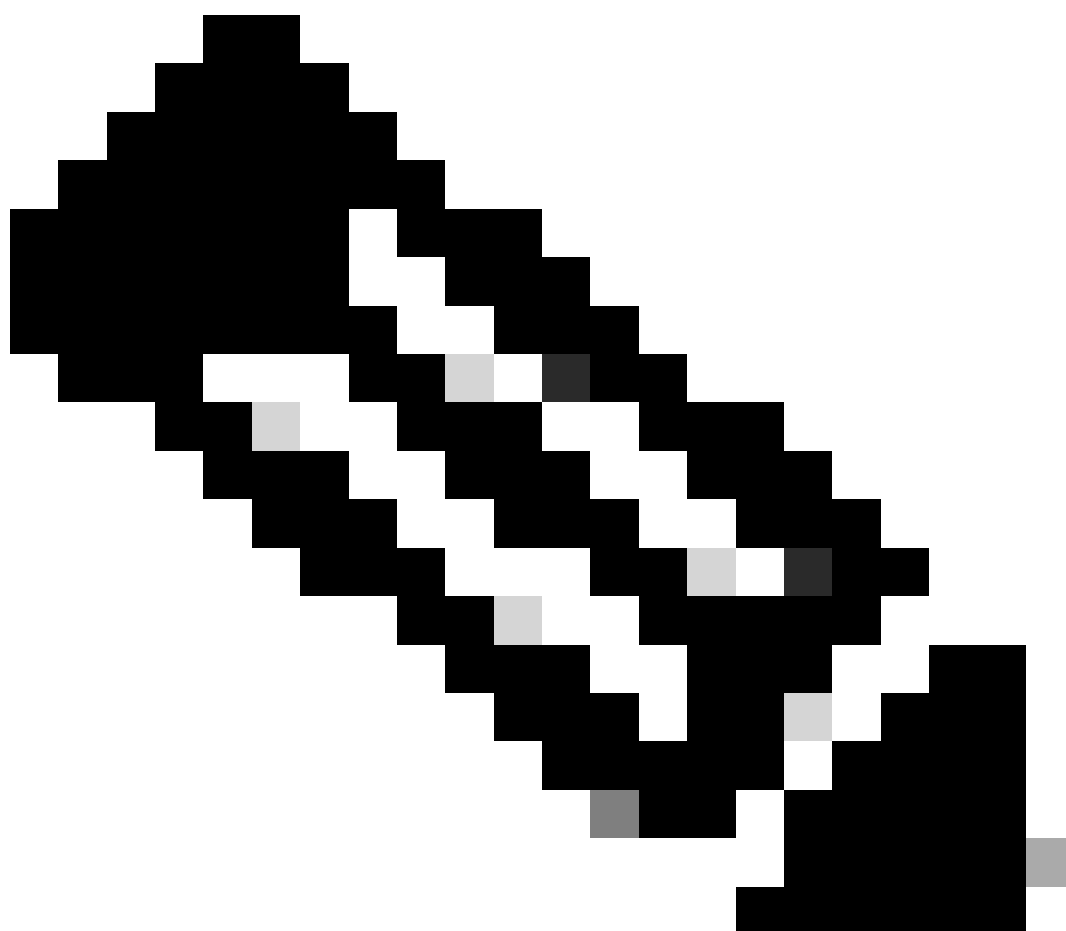
6. Aktivieren Sie Failover auf der neuen sekundären Firewall. Beispiele:

```
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. Warten Sie, bis die aktive Konfiguration mit der neuen Einheit synchronisiert wurde, und validieren Sie den korrekten Failover-Status. Beispiele:

```
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#
```



Hinweis: Beachten Sie, dass die primäre Firewall (Firewall-a) die Konfiguration an die

sekundäre Firewall (Firewall-b) sendet.

8. Speichern Sie die Konfiguration auf dem primären/aktiven Gerät, und validieren Sie den Schreibspeicher auf dem neuen sekundären/Standby-Gerät. Beispiele:

```
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. Überprüfen Sie, ob das Failover-Paar auf beiden Firewalls aktiv ist. Beispiele:

```
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 outside (10.1.1.1): Normal (Not-Monitored)
Interface management (10.2.2.1): Normal (Not-Monitored)

Ersetzen Sie den primären Firewall-Fehler.

1. Überprüfen Sie, ob die sekundäre Firewall aktiv und online ist. Beispiele:

```
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. Herunterfahren und physisches Entfernen der primären Firewall
3. Fügen Sie die neue primäre Firewall physisch hinzu, und schalten Sie sie ein.
4. Jetzt wird die neue primäre Firewall mit der werkseitigen Standardkonfiguration aktiviert.
5. Aktivieren Sie die Failover-Verbindung, und fahren Sie die physische Failover-Verbindung nicht herunter. Beispiele:

```
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. Speichern der Konfiguration Schreiben Sie Speicher auf die sekundäre/aktive Firewall, und stellen Sie sicher, dass sich die sekundäre Failover-LAN-Einheit in der Startkonfiguration befindet.

Beispiel:

```
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. Failover-Befehle konfigurieren.

1. Auf der sekundären/aktiven Firewall müssen Sie zuerst den Befehl failover lan unit primary festlegen, um sicherzustellen, dass die aktive Konfiguration von der sekundären/aktiven Firewall auf die neue Standardkonfiguration primary/standby Firewall verschoben wird. Beispiele:

```
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. Validierung der Failover-Konfiguration auf beiden Geräten Beispiele:

```
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. Aktivieren Sie Failover auf der neuen primären Firewall. Beispiele:

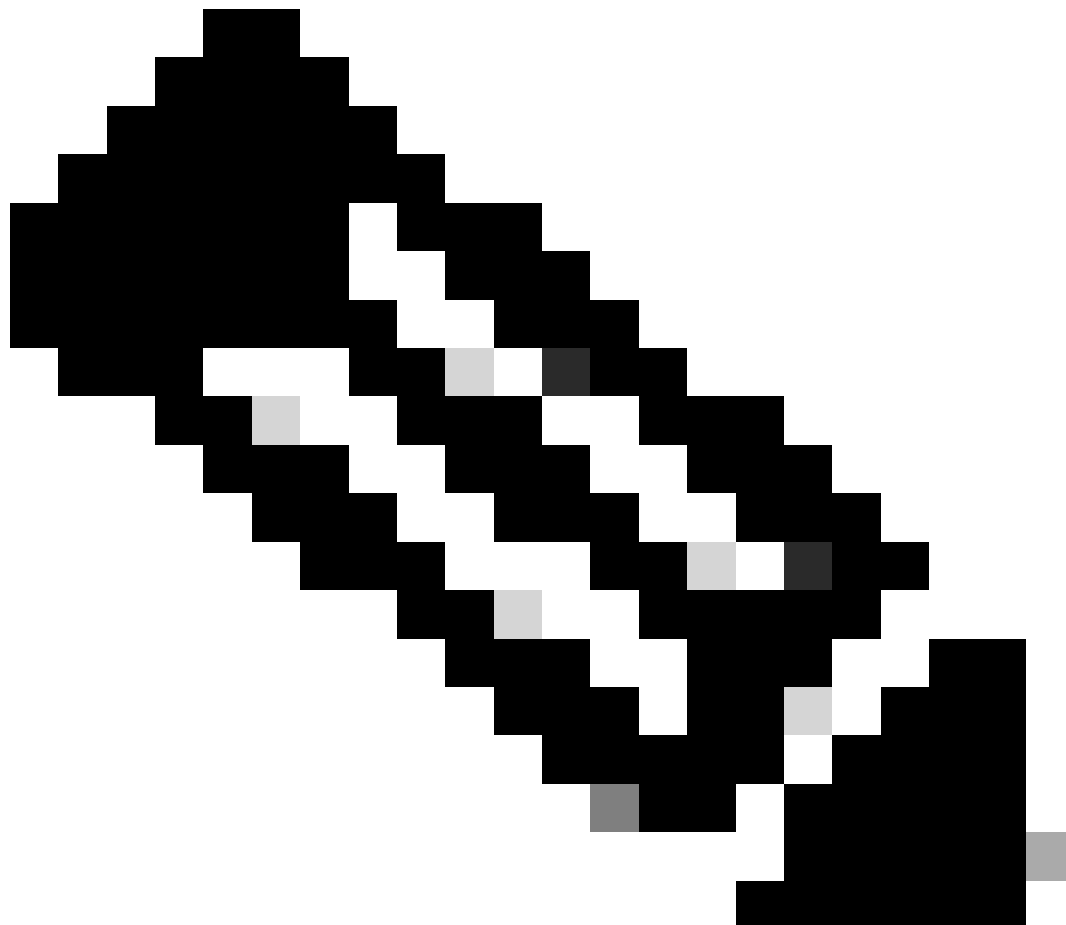
```
firewall-a/sec/stby#conf t
firewall-a/sec/stby#(config)#failover
firewall-a/sec/stby#(config)#exit
firewall-a/sec/stby#
```

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

9. Warten Sie, bis die aktive Konfiguration mit der neuen Einheit synchronisiert wurde, und validieren Sie den korrekten Failover-Status. Beispiele:

```
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#



Hinweis: Beachten Sie, dass die primäre Firewall (Firewall-b) die Konfiguration an die sekundäre Firewall (Firewall-a) sendet. Schreiben Sie keinen Speicher auf die nun primäre/aktive Firewall (Firewall-b).

10. Laden Sie die nun primäre/aktive Firewall (Firewall-b) neu, sodass sie wieder als sekundäre/Standby-Firewall gestartet wird.

firewall-b/pri/act#reload

11. Wechseln Sie direkt nach der Ausführung des Befehls "firewall-b reload" (warten Sie 15 Sekunden) zur neuen primären Firewall (firewall-a), und geben Sie den primären Befehl

failover lan unit gefolgt von Schreibspeicher ein.

```
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. Warten Sie, bis die Firewall-b vollständig gestartet ist, und verbinden Sie das Failover-Paar als sekundär/Standby. Beispiele:

```
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#
```



Hinweis: Beachten Sie, dass die primäre Firewall (Firewall-a) die Konfiguration an die sekundäre Firewall (Firewall-b) sendet.

13. Speichern Sie die Konfiguration, schreiben Sie Arbeitsspeicher auf das primäre/aktive Gerät, und validieren Sie den Schreibspeicher auf dem neuen sekundären/Standby-Gerät.

Beispiele:

```
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. Überprüfen Sie, ob das Failover-Paar auf beiden Firewalls aktiv ist. Beispiele:

```
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 outside (10.1.1.1): Normal (Not-Monitored)

Interface management (10.2.2.1): Normal (Not-Monitored)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.