

Remplacer un pare-feu ASA par une paire de basculement actif/veille

Table des matières

[Introduction](#)

[Informations générales](#)

[Différence entre les unités principale et secondaire dans la configuration de basculement](#)

[Différence entre les unités actives et en veille dans la configuration de basculement](#)

[Remplacer l'échec du pare-feu secondaire](#)

[Remplacer l'échec du pare-feu principal](#)

Introduction

Ce document décrit comment remplacer un pare-feu ASA (Adaptive Security Appliance) par une paire de basculement actif/veille.

Informations générales

Les pare-feu ASA prennent en charge deux configurations de basculement, le basculement actif/actif et le basculement actif/en veille.

Il existe 2 pare-feu :

- firewall-a est principal/actif
- firewall-b est secondaire/en veille

Différence entre les unités principale et secondaire dans la configuration de basculement

Cette commande signifie que ce pare-feu transmet toujours la configuration active au pare-feu secondaire.

```
# failover lan unit primary
```

Cette commande signifie que ce pare-feu reçoit toujours la configuration active du pare-feu principal.

```
# failover lan unit secondary
```

Différence entre les unités actives et en veille dans la configuration de basculement

Cette commande signifie que ce pare-feu est le pare-feu actif dans la paire de basculement.

```
# failover active
```

Cette commande signifie que ce pare-feu est le pare-feu de secours exécutant un pare-feu dans la paire de basculement.

```
# failover standby
```

Remplacer l'échec du pare-feu secondaire

1. Vérifiez que le pare-feu principal est actif et en ligne. Exemple :

```
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. Arrêtez et retirez physiquement le pare-feu secondaire.
3. Ajoutez physiquement le nouveau pare-feu secondaire et mettez-le sous tension.
4. Une fois que le nouveau pare-feu secondaire est actif avec la configuration d'usine par défaut, activez le lien de basculement,`no shutdown`le lien physique de basculement.

Exemple :

```
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. Configurez les commandes de basculement. Exemple :

```
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#
```

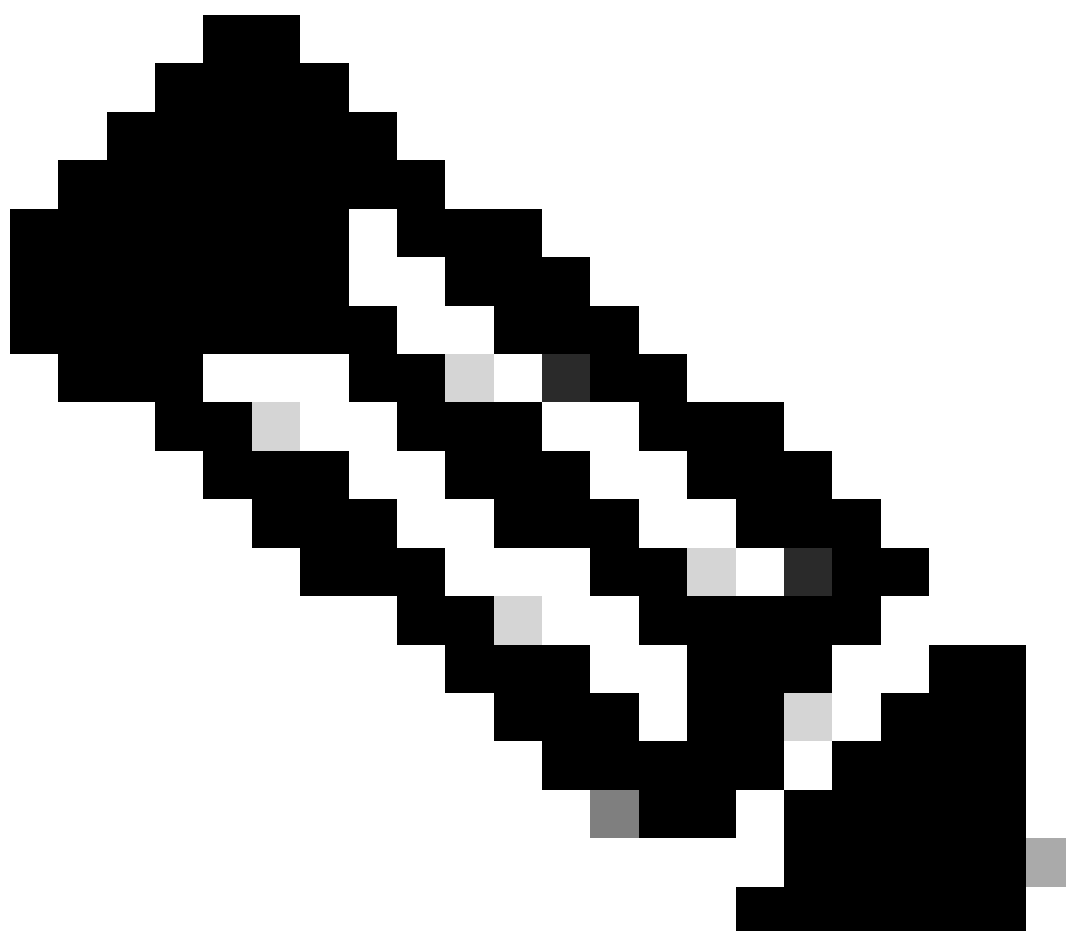
6. Activez le basculement sur le nouveau pare-feu secondaire. Exemple :

```
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. Attendez que la configuration active soit synchronisée avec la nouvelle unité et validez l'état de basculement correct. Exemple :

```
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#
```



Remarque : notez que le pare-feu principal (firewall-a) envoie la configuration au pare-feu

secondaire (firewall-b).

8. Enregistrez la configuration sur le serveur principal/actif et validez la mémoire d'écriture sur le nouveau serveur secondaire/en veille. Exemple :

```
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. Vérifiez que la paire de basculement est active/active sur les deux pare-feu. Exemple :

```
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)

Remplacer l'échec du pare-feu principal

1. Vérifiez que le pare-feu secondaire est actif et en ligne. Exemple :

```
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. Arrêtez et retirez physiquement le pare-feu principal.
3. Ajouter physiquement le nouveau pare-feu principal et le mettre sous tension.
4. Maintenant, le nouveau pare-feu principal est actif avec la configuration par défaut.
5. Activez le lien de basculement, sans arrêter le lien physique de basculement. Exemple :

```
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. Enregistrez la configuration. Écrivez de la mémoire sur le pare-feu secondaire/actif et assurez-vous que l'unité LAN secondaire de basculement est dans la configuration de démarrage.

Exemple :

```
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. Configurer les commandes de basculement.

1. Sur le pare-feu secondaire/actif, vous devez d'abord définir la commande failover lan unit primary pour vous assurer que la configuration active est poussée du pare-feu secondaire/actif vers le nouveau pare-feu primaire/de secours de configuration par défaut. Exemple :

```
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. Validez la configuration du basculement sur les deux périphériques. Exemple :

```
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#
```

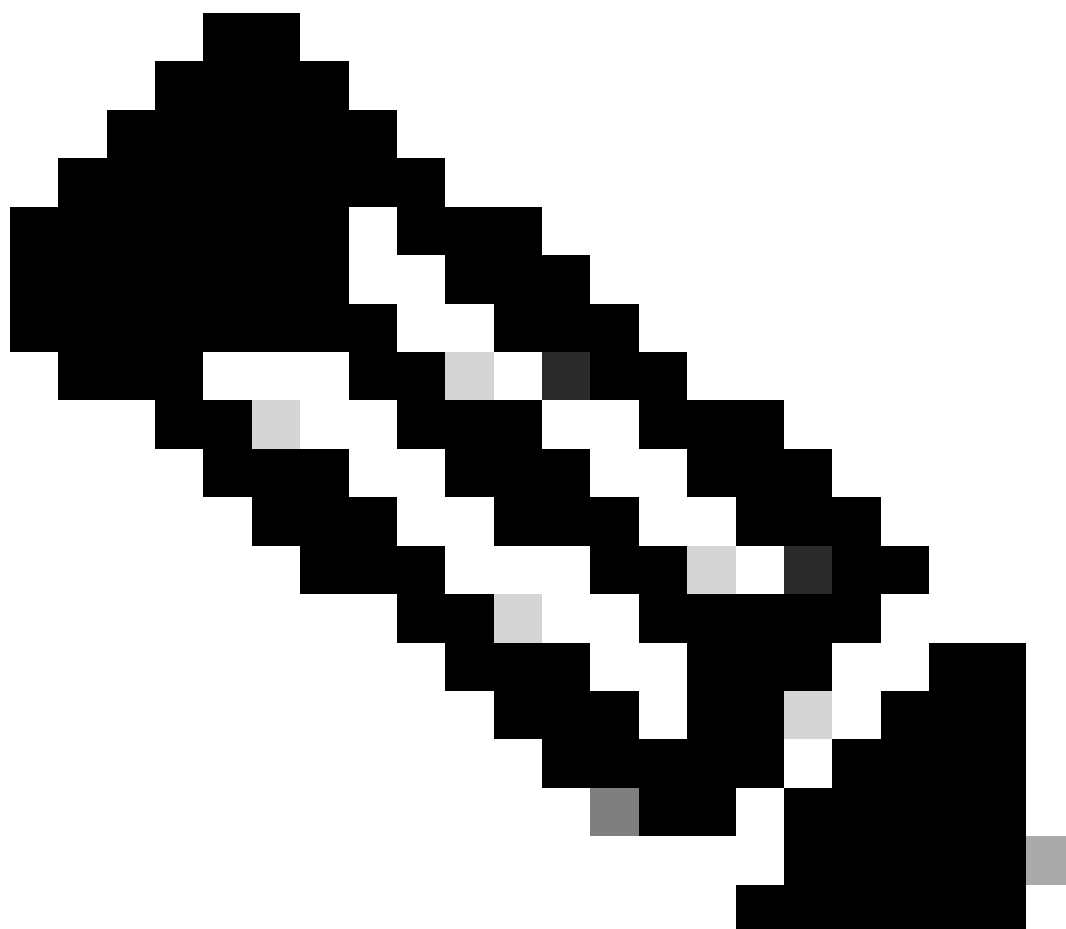
8. Activez le basculement sur le nouveau pare-feu principal. Exemple :

```
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. Attendez que la configuration active soit synchronisée avec la nouvelle unité et validez l'état de basculement correct. Exemple :

```
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#
```

Remarque : notez que le pare-feu principal (firewall-b) envoie la configuration au pare-feu secondaire (firewall-a). N'écrivez pas de mémoire sur le pare-feu maintenant principal/actif (firewall-b).

-
10. Rechargez le pare-feu maintenant principal/actif (firewall-b) afin qu'il redémarre en tant que pare-feu secondaire/de secours.

`firewall-b/pri/act#reload`

11. Juste après avoir exécuté la commande « `firewall-b reload` » (attendez 15 secondes), passez au nouveau pare-feu principal (firewall-a) et entrez la commande `failover lan unit primary`, suivie de la commande `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. Attendez que firewall-b démarre complètement et joigne la paire de basculement en tant que secondaire/veille. Exemple :

```
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#
```

Remarque : veuillez noter que le pare-feu principal (firewall-a) envoie la configuration au pare-feu secondaire (firewall-b).

13. Enregistrez la configuration, écrivez de la mémoire sur le serveur principal/actif et validez la mémoire d'écriture sur le nouveau serveur secondaire/en veille. Exemple :

```
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. Vérifiez que la paire de basculement est active/active sur les deux pare-feu. Exemple :

```
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)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.