

ASA/PIX : Configuration du basculement actif/en veille en mode transparent

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Produits connexes](#)

[Conventions](#)

[Basculement actif/veille](#)

[Présentation du basculement actif/veille](#)

[État principal/secondaire et état actif/veille](#)

[Synchronisation d'initialisation et de configuration de périphérique](#)

[Réplication des commandes](#)

[Déclencheurs de basculement](#)

[Opérations de basculement](#)

[Basculement périodique et dynamique](#)

[Basculement périodique](#)

[Basculement dynamique](#)

[Configuration de basculement actif/veille basé sur le LAN](#)

[Diagramme du réseau](#)

[Configuration de l'unité principale](#)

[Configuration de l'unité secondaire](#)

[Configurations](#)

[Vérification](#)

[Utilisation de la commande show failover](#)

[Affichage des interfaces surveillées](#)

[Affichage des commandes de basculement dans la configuration en cours](#)

[Tests sur la fonctionnalité de basculement](#)

[Basculement forcé](#)

[Basculement désactivé](#)

[Restauration d'une unité défaillante](#)

[Dépannage](#)

[Surveillance du basculement](#)

[Défaillance d'une unité](#)

[Connexion allouée à LU défaillante](#)

[Messages système de basculement](#)

[Messages de débogage](#)

[SNMP](#)

[Délai d'interrogation du basculement](#)

[Exportation du certificat ou de la clé privée dans la configuration de basculement](#)

[AVERTISSEMENT : Échec du déchiffrement du message de basculement](#)

[Problème : Le basculement est toujours allumé après la configuration du basculement en mode multiple actif/veille transparent](#)

[Basculement des modules ASA](#)

[Échec de l'allocation du paquet de messages de basculement](#)

[Problème de basculement du module AIP](#)

[Problèmes identifiés](#)

[Informations connexes](#)

[Introduction](#)

La configuration de basculement requiert deux appliances de sécurité identiques connectées entre elles par un lien de basculement dédié et éventuellement un lien de basculement dynamique. La santé des interfaces et des unités actives est surveillée pour déterminer si les conditions spécifiques de basculement sont remplies. Si ces conditions sont remplies, le basculement se produit.

Le dispositif de sécurité supporte deux configurations de basculement :

- [Basculement actif/actif](#)
- [Basculement actif/veille](#)

Chaque configuration de basculement a sa propre méthode pour déterminer et exécuter le basculement. Avec le basculement actif/actif, les deux unités peuvent acheminer le trafic réseau. Cela vous permet de configurer l'équilibrage de charge sur votre réseau. Le basculement actif/actif est seulement disponible sur les unités qui fonctionnent en mode de contexte multiple. Avec le basculement actif/veille, seule une unité achemine le trafic tandis que l'autre unité attend en état de veille. Le basculement actif/veille est disponible sur les unités qui fonctionnent en mode de contexte unique ou multiple. Ces deux configurations de basculement supportent le basculement dynamique et le basculement statique (périodique).

Un pare-feu transparent est un pare-feu de couche 2 qui agit comme un *bossoir dans le câble*, ou un *pare-feu furtif*, et n'est pas vu comme un saut de routeur vers les périphériques connectés. L'appliance de sécurité connecte le même réseau sur ses ports intérieurs et extérieurs. Puisque le pare-feu n'est pas un saut de routeur, vous pouvez facilement introduire un pare-feu transparent dans le réseau existant ; il est inutile de réadresser IP. Vous pouvez configurer l'appliance de sécurité adaptable pour être exécutée dans le mode de pare-feu routé par défaut ou le mode pare-feu transparent . Quand vous changez les modes, l'appliance de sécurité adaptable efface la configuration parce que de nombreuses commandes ne sont pas prises en charge dans les deux modes. Si vous avez déjà une configuration chargée, assurez-vous de sauvegarder cette configuration avant de changer de mode ; vous pouvez utiliser cette configuration de secours pour référence quand vous créez une nouvelle configuration. Référez-vous à [Exemple de configuration de pare-feu transparent](#) pour plus d'informations sur la configuration de l'appliance de pare-feu en mode transparent.

Ce document se concentre sur la façon de configurer un basculement actif/veille en mode transparent sur le dispositif de sécurité ASA.

Remarque : le basculement VPN n'est pas pris en charge sur les unités qui s'exécutent en mode

de contexte multiple. Le basculement VPN est disponible pour les configurations **de basculement actif/veille** uniquement.

Cisco recommande de ne pas utiliser l'interface de gestion pour le basculement, notamment pour le basculement dynamique, où le dispositif de sécurité envoie constamment les informations de connexion d'un dispositif de sécurité à l'autre. L'interface utilisée pour le basculement doit être au moins de la même capacité que les interfaces qui acheminent le trafic habituel, et bien que les interfaces de l'ASA 5540 soient Gigabit, l'interface de gestion est FastEthernet seulement. L'interface de gestion est conçue pour le trafic de gestion seulement et est spécifiée comme management0/0. Mais vous pouvez utiliser la commande **management-only** afin de configurer n'importe quelle interface pour être une interface de gestion uniquement. En outre, pour Management 0/0, vous pouvez désactiver le mode gestion seule pour que l'interface puisse acheminer le trafic comme toute autre interface. Référez-vous à [Référence des commandes de Cisco Security Appliance, version 8.0](#) pour plus d'informations sur la commande **management-only**.

Ce guide de configuration fournit un exemple de configuration pour une brève introduction à la technologie actif/veille de PIX/ASA 7.x. Référez-vous au [Guide de référence des commandes ASA/PIX pour mieux comprendre la théorie à la base de cette technologie](#).

Conditions préalables

Conditions requises

Configuration matérielle

Les deux unités contenues dans une configuration de basculement doivent avoir la même configuration matérielle. Elles doivent avoir le même modèle, le même nombre et le même type d'interfaces, et la même quantité de RAM.

Remarque : Les deux unités n'ont pas besoin de la même taille de mémoire Flash. Si vous utilisez des unités avec différentes tailles de mémoire flash dans votre configuration de basculement, assurez-vous que l'unité avec la mémoire flash la plus petite a assez d'espace pour contenir les fichiers d'image logicielle et les fichiers de configuration. Sinon, la synchronisation de la configuration de l'unité avec la mémoire flash la plus grande et de l'unité avec la mémoire flash la plus petite échoue.

Configuration logicielle requise

Les deux unités présentes dans une configuration de basculement doivent être en mode opérationnel (routé ou transparent, contexte unique ou multiple). Elles doivent avoir la même version logicielle majeure (premier numéro) et mineure (second numéro), mais vous pouvez utiliser différentes versions du logiciel dans un processus de mise à niveau. Par exemple, vous pouvez mettre à niveau une unité de la version 7.0(1) vers la version 7.0(2) sans que le basculement ne se désactive. Cisco recommande de mettre à niveau les deux unités à la même version pour assurer la compatibilité à long terme.

Reportez-vous à la section [Exécution de mises à niveau sans interruption pour les paires de basculement](#) du *Guide de configuration de ligne de commande de l'appliance de sécurité Cisco, version 8.0* pour plus d'informations sur la mise à niveau du logiciel sur une paire de basculement.

Exigences de licence

Sur la plate-forme ASA Security Appliance, au moins une des unités doit avoir une **licence d'utilisation illimitée**.

Remarque : Il peut être nécessaire de mettre à niveau les licences sur une paire de basculement afin d'obtenir des fonctionnalités et des avantages supplémentaires. Référez-vous à [Mise à niveau de clé de licence sur une paire de basculement](#) pour plus d'informations.

Remarque : Les fonctionnalités sous licence (telles que les homologues VPN SSL ou les contextes de sécurité) sur les deux appliances de sécurité qui participent au basculement doivent être identiques.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliance de sécurité ASA avec version 7.x et ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produits connexes

Cette configuration peut également être utilisée avec les versions de matériel et de logiciel suivantes :

- Appliance de sécurité PIX avec versions 7.x et postérieures

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Basculement actif/veille

Cette section décrit le basculement actif/veille et comprend les rubriques suivantes :

- [Présentation du basculement actif/veille](#)
- [État principal/secondaire et état actif/veille](#)
- [Synchronisation d'initialisation et de configuration de périphérique](#)
- [Réplication des commandes](#)
- [Déclencheurs de basculement](#)
- [Opérations de basculement](#)

Présentation du basculement actif/veille

Le basculement actif/veille permet d'utiliser un dispositif de sécurité en veille pour relayer la fonctionnalité d'une unité défaillante. Quand l'unité active est défaillante, elle passe à l'état de veille tandis que l'unité en veille passe à l'état actif. L'unité qui devient active suppose les

adresses IP ou, pour un pare-feu transparent, l'adresse IP de gestion et les adresses MAC de l'unité défaillante et commence à transmettre le trafic. L'unité qui est maintenant à l'état de veille se charge des adresses IP et MAC en veille. Étant donné que les périphériques réseau ne voient aucun changement dans le pairage des adresses MAC vers IP, aucune entrée ARP ne change ou ne dépasse le délai sur le réseau.

Remarque : Pour le mode de contexte multiple, l'appareil de sécurité peut basculer sur l'unité entière, qui inclut tous les contextes, mais ne peut pas basculer séparément sur des contextes individuels.

État principal/secondaire et état actif/veille

Les différences majeures entre les deux unités d'une paire de basculement concernent l'identité de l'unité active et celle de l'unité en veille, à savoir quelles sont les adresses à utiliser et quelle unité est l'unité principale et achemine le trafic activement.

Il existe quelques différences entre les unités en fonction de l'unité principale, comme spécifié dans la configuration, et de l'unité secondaire :

- L'unité principale devient toujours l'unité active si les deux unités démarrent en même temps (et ont la même santé opérationnelle).
- L'adresse MAC de l'unité principale est toujours couplée avec les adresses IP actives. Une exception à cette règle se produit quand l'unité secondaire est active et ne peut pas obtenir l'adresse MAC principale via le lien de basculement. Dans ce cas, l'adresse MAC secondaire est utilisée.

Synchronisation d'initialisation et de configuration de périphérique

La synchronisation de configuration a lieu quand un des périphériques ou les deux de la paire de basculement démarrent. Les configurations sont toujours synchronisées de l'unité active vers l'unité en veille. Lorsque l'unité de secours termine son démarrage initial, elle efface sa configuration en cours, à l'exception des commandes de basculement nécessaires pour communiquer avec l'unité active, et l'unité active envoie toute sa configuration à l'unité de secours.

L'unité active est déterminée par les éléments suivants :

- Si une unité démarre et détecte un homologue opérant déjà à l'état actif, elle devient l'unité en veille.
- Si une unité démarre et ne détecte aucun homologue, elle devient l'unité active.
- Si les deux unités démarrent simultanément, l'unité principale devient l'unité active, et l'unité secondaire devient l'unité en veille.

Remarque : Si l'unité secondaire démarre et ne détecte pas l'unité principale, elle devient l'unité active. Elle utilise ses propres adresses MAC pour les adresses IP actives. Quand l'unité principale devient disponible, l'unité secondaire remplace les adresses MAC par celles de l'unité principale, ce qui peut entraîner une interruption du trafic réseau. Pour éviter cela, configurez la paire de basculement avec des adresses MAC virtuelles. Consultez la section [Configuration du basculement actif/veille de ce document pour plus d'informations](#).

Lorsque la réplication démarre, la console de l'appareil de sécurité sur l'unité active affiche le message `Commencer la réplication de configuration : Envoi au partenaire` et, une fois terminé, le dispositif de sécurité affiche le message `Fin de la réplication de configuration à associer`. Lors

d'une réplication, les commandes entrées sur l'unité active ne peuvent pas être répliquées correctement sur l'unité en veille, et les commandes entrées sur l'unité en veille ne peuvent pas être remplacées par la configuration répliquée depuis l'unité active. N'entrez pas de commandes sur l'une ou l'autre unité de la paire de basculement durant le processus de réplication de la configuration. Selon la taille de la configuration, la réplication peut prendre quelques secondes à plusieurs minutes.

À partir de l'unité secondaire, vous pouvez observer le message de réplication lors de sa synchronisation à partir de l'unité principale :

```
ASA> .
```

```
          Detected an Active mate
Beginning configuration replication from mate.
End configuration replication from mate.
```

```
ASA>
```

Sur l'unité en veille, la configuration n'existe que dans la mémoire active. Pour enregistrer la configuration dans la mémoire flash après la synchronisation, entrez les commandes suivantes :

- Pour le mode de contexte unique, entrez la commande **copy running-config startup-config** sur l'unité active. La commande est répliquée sur l'unité en veille, laquelle enregistre alors sa configuration dans la mémoire flash.
- Pour le mode de contexte multiple, entrez la commande **copy running-config startup-config** sur l'unité active depuis l'espace d'exécution du système et à partir de chaque contexte figurant sur le disque. La commande est répliquée sur l'unité en veille, laquelle enregistre alors sa configuration dans la mémoire flash. Les contextes avec des configurations de démarrage sur des serveurs externes sont accessibles à partir de l'une ou l'autre unité via le réseau et il n'est pas nécessaire de les enregistrer séparément pour chaque unité. Vous pouvez aussi copier les contextes contenus sur le disque de l'unité d'active sur un serveur externe, puis les copier sur le disque de l'unité en veille, où ils deviennent disponibles lorsque l'unité se recharge.

Réplication des commandes

La réplication des commandes va de l'unité active à l'unité en veille. Lorsque les commandes sont entrées sur l'unité active, elles sont envoyées à l'unité en veille via le lien de basculement. Vous n'avez pas à enregistrer la configuration active dans la mémoire flash pour répliquer les commandes.

Remarque : les modifications apportées à l'unité de secours ne sont pas répliquées sur l'unité active. Si vous entrez une commande sur l'unité en veille, le dispositif de sécurité affiche le message ***** WARNING **** Configuration Replication is NOT performed from Standby unit to Active unit**. Les configurations ne sont plus synchronisées. Ce message s'affiche même si vous entrez des commandes qui n'affectent pas la configuration.

Si vous entrez la commande **write standby** sur l'unité active, l'unité en veille efface sa configuration en cours, à l'exception des commandes de basculement utilisées pour communiquer avec l'unité active, et l'unité active envoie sa configuration complète à l'unité en veille.

Pour le mode de contexte multiple, quand vous entrez la commande **write standby** dans l'espace

d'exécution du système, tous les contextes sont répliqués. Si vous entrez la commande `write standby` dans un contexte, la commande ne réplique que la configuration du contexte.

Les commandes répliquées sont enregistrées dans la configuration en cours. Pour enregistrer les commandes répliquées dans la mémoire flash de l'unité en veille, entrez les commandes suivantes :

- Pour le mode de contexte unique, entrez la commande **`copy running-config startup-config` sur l'unité active.** La commande est répliquée sur l'unité en veille, laquelle enregistre alors sa configuration dans la mémoire flash.
- Pour le mode de contexte multiple, entrez la commande **`copy running-config startup-config` sur l'unité active depuis l'espace d'exécution du système et dans chaque contexte contenu sur le disque.** La commande est répliquée sur l'unité en veille, laquelle enregistre alors sa configuration dans la mémoire flash. Les contextes avec des configurations de démarrage sur des serveurs externes sont accessibles à partir de l'une ou l'autre unité via le réseau et il n'est pas nécessaire de les enregistrer séparément pour chaque unité. Vous pouvez aussi copier les contextes contenus sur disque de l'unité active sur un serveur externe, puis les copier sur le disque de l'unité en veille.

Déclencheurs de basculement

L'unité peut avoir une défaillance si un des événements suivants se produit :

- L'unité a une défaillance matérielle ou une panne d'alimentation.
- L'unité a une défaillance logicielle.
- Trop d'interfaces surveillées ont une défaillance.
- La commande **`no failover active` est entrée sur l'unité active ou la commande `failover active` est entrée sur l'unité en veille.**

Opérations de basculement

Dans un basculement actif/veille, le basculement s'effectue unité par unité. Même sur des systèmes qui fonctionnent en mode de contexte multiple, vous ne pouvez pas relayer de contextes individuels ou de groupes de contextes.

Ce tableau montre l'opération de basculement pour chaque événement de défaillance. Pour chaque événement de défaillance, le tableau contient les règles de basculement (basculement ou aucun basculement), l'opération effectuée par l'unité active et des remarques particulières sur l'état de basculement et les opérations de basculement. Le tableau montre le comportement de basculement.

Événement de défaillance	Politique	Opération de l'unité active	Opération de l'unité en veille	Notes
L'unité active a eu une défaillance	Basculement	S/O	S'active Marque l'unité active	Aucun message hello n'est reçu sur une interface surveillée ou sur le

(matérielle ou d'alimentation)			comme défaillante	lien de basculement.
L'unité auparavant active reprend	Pas de basculement	Se met en veille	Aucune opération	Aucune
L'unité en veille a eu une défaillance (matérielle ou d'alimentation)	Pas de basculement	Marque l'unité en veille comme défaillante	S/O	Quand l'unité en veille est marquée comme défaillante, l'unité active ne tente aucun basculement, même si le seuil de défaillance de l'interface est dépassé.
Le lien de basculement a eu une défaillance en cours de fonctionnement	Pas de basculement	Marque l'interface de basculement comme défaillante	Marque l'interface de basculement comme défaillante	Vous devez restaurer le lien de basculement dès que possible car l'unité ne peut pas relayer l'unité en veille alors que le lien de basculement est défaillant.
Le lien de basculement a eu une défaillance au démarrage	Pas de basculement	Marque l'interface de basculement comme défaillante	S'active	Si le lien de basculement a une défaillance au démarrage, les deux unités deviennent actives.
Le lien de basculement dynamique a eu une défaillance	Pas de basculement	Aucune opération	Aucune opération	Les informations d'état sont périmées et les sessions se terminent si un basculement se produit.
Défaillance de l'interface sur l'unité active au-dessus du seuil	Basculement	Marque l'unité active comme défaillante	S'active	Aucune

Défaillance de l'interface sur l'unité en veille au-dessus du seuil	Pas de basculement	Aucune opération	Marque l'unité en veille comme défaillante	Quand l'unité en veille est marquée comme défaillante, l'unité active ne tente aucun basculement, même si le seuil de défaillance de l'interface est dépassé.
---	--------------------	------------------	--	---

Basculement périodique et dynamique

Le dispositif de sécurité supporte deux types de basculement : périodique et dynamique. Cette section comprend les rubriques suivantes :

- [Basculement périodique](#)
- [Basculement dynamique](#)

Basculement périodique

Quand un basculement se produit, toutes les connexions actives sont supprimées. Les clients doivent rétablir les connexions quand la nouvelle unité active prend le relais.

Basculement dynamique

Quand le basculement dynamique est activé, l'unité active transfère continuellement les informations d'état par connexion à l'unité en veille. Lorsqu'un basculement s'est produit, les mêmes informations de connexion sont disponibles sur la nouvelle unité active. Les applications utilisateur supportées ne doivent pas nécessairement se reconnecter pour garder la même session de transmission.

Les informations d'état transmises à l'unité en veille incluent les éléments suivants :

- La table de conversion NAT
- Les états des connexions TCP
- Les états des connexions UDP
- La table ARP
- Table de pont de couche 2 (uniquement lorsque le pare-feu fonctionne en mode **pare-feu transparent**)
- Les états des connexions HTTP (si la réplication HTTP est activée)
- La table SA ISAKMP et IPSec
- La base des connexions GTP PDP

Les informations transmises à l'unité en veille quand le basculement dynamique est activé incluent les éléments suivants :

- La table des connexions HTTP (sauf si la réplication HTTP est activée)
- La table des authentifications utilisateur (uauth)
- Les tables de routage

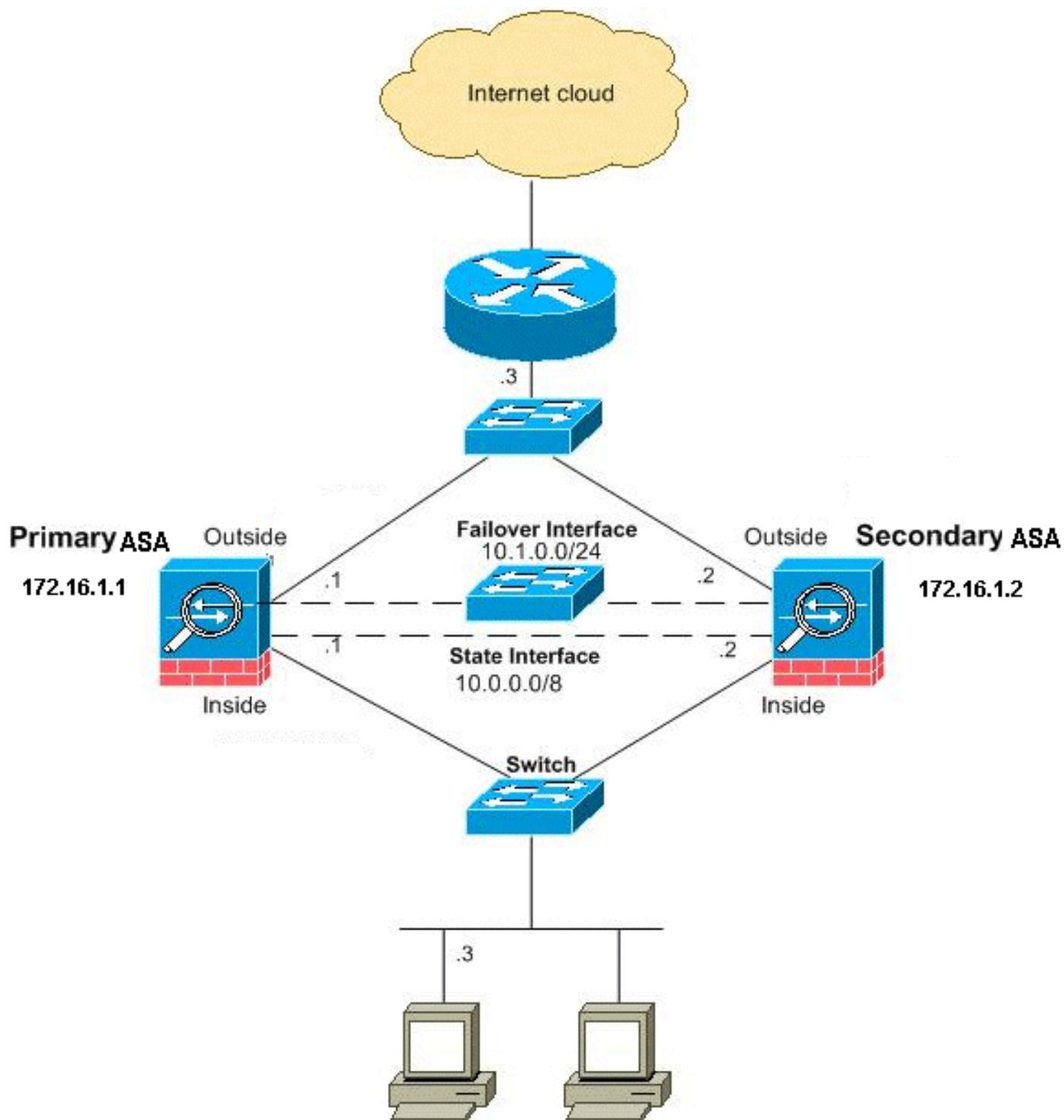
- Les informations d'état relatives aux modules des services de sécurité

Remarque : si le basculement se produit au sein d'une session Cisco IP SoftPhone active, l'appel reste actif car les informations d'état de la session d'appel sont répliquées sur l'unité de secours. Lorsque l'appel est interrompu, le client IP SoftPhone perd la connexion avec Cisco CallManager . Cela se produit car il n'ya aucune information de session pour le message de raccrochage CTIQBE sur l'unité en veille. Lorsque le client IP SoftPhone ne reçoit pas de réponse de Cisco CallManager dans un délai donné, il considère que Cisco CallManager est inaccessible et se désinscrit lui-même.

[Configuration de basculement actif/veille basé sur le LAN](#)

[Diagramme du réseau](#)

Ce document utilise la configuration réseau suivante :



Cette section décrit comment configurer le basculement actif/veille en mode transparent avec une liaison de basculement Ethernet. Quand vous configurez le basculement basé sur le LAN, vous devez amorcer le périphérique secondaire pour identifier le lien de basculement afin que le périphérique secondaire puisse obtenir la configuration en cours du périphérique principal.

Remarque : si vous passez du basculement basé sur le câble au basculement basé sur le LAN, vous pouvez ignorer de nombreuses étapes, telles que l'attribution des adresses IP actives et de secours pour chaque interface, que vous avez effectuées pour la configuration de basculement basé sur le câble.

[Configuration de l'unité principale](#)

Complétez ces étapes afin de configurer l'unité principale dans une configuration de basculement

actif/veille basée sur LAN. Les étapes ci-dessous permettent d'obtenir la configuration minimale requise pour activer le basculement sur l'unité principale. Pour le mode de contexte multiple, toutes les étapes sont exécutées dans l'espace d'exécution du système, sauf indication contraire.

Afin de configurer l'unité principale dans une paire de basculement actif/veille, procédez comme suit :

1. Si ce n'est déjà fait, configurez les adresses IP actives et de secours pour l'interface de gestion (mode transparent). L'adresse IP en standby est utilisée sur le dispositif de sécurité qui est l'unité en veille en cours. Elle doit se trouver sur le même sous-réseau que l'adresse IP active. **Remarque** : Ne configurez pas d'adresse IP pour le lien de basculement dynamique si vous utilisez une interface de basculement dynamique dédiée. La commande **failover interface ip** s'utilise pour configurer une interface de basculement dynamique dédiée dans une étape ultérieure.

```
hostname(config-if)#ip address active_addr netmask  
standby standby_addr
```

À la différence du mode routé, qui exige une adresse IP pour chaque interface, un pare-feu transparent a une adresse IP affectée au périphérique entier. L'appliance de sécurité utilise cette adresse IP comme adresse source pour les paquets créés sur l'appliance de sécurité, tels que les messages de système ou communications AAA. Dans l'exemple, l'adresse IP de l'ASA principal est configurée comme indiqué ci-dessous :

```
hostname(config)#ip address 172.16.1.1 255.255.0.0 standby 172.16.1.2
```

Ici, 172.16.1.1 est utilisé pour l'unité principale et 172.16.1.2 est affecté à l'unité secondaire (en veille). **Remarque** : En mode de contexte multiple, vous devez configurer les adresses d'interface à partir de chaque contexte. Utilisez la commande **changeto context** afin de basculer entre les contextes. L'invite de commande devient `hostname/context(config-if)#`, où `context` est le nom du contexte actif.

2. (Pour la plate-forme de dispositif de sécurité PIX uniquement) Activez le basculement basé sur le LAN.

```
hostname(config)#failover lan enable
```

3. Désignez l'unité comme l'unité principale.

```
hostname(config)#failover lan unit primary
```

4. Définissez l'interface de basculement. Spécifiez l'interface à utiliser comme interface de basculement.

```
hostname(config)#failover lan interface if_name phy_if
```

Dans cette documentation, le « failover » (nom d'interface pour Ethernet0) est utilisé pour une interface de basculement.

```
hostname(config)#failover lan interface failover Ethernet3
```

L'argument *if_name* affecte un nom à l'interface spécifiée par l'argument *phy_if*. L'argument *phy_if* peut être le nom du port physique, par exemple *Ethernet1*, ou une sous-interface créée précédemment, par exemple *Ethernet0/2.3*. Affectez l'adresse active et l'adresse en standby au lien de basculement.

```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

Dans cette documentation, pour configurer la liaison de basculement, 10.1.0.1 est utilisé pour active, 10.1.0.2 pour l'unité de secours, et « failover » est un nom d'interface Ethernet0.

```
hostname(config)#failover interface ip failover 10.1.0.1
                255.255.255.0 standby 10.1.0.2
```

L'adresse IP de secours doit être dans le même sous-réseau que l'adresse IP active. Vous n'avez pas besoin d'identifier le masque de sous-réseau de l'adresse en standby. L'adresse IP et l'adresse MAC du lien de basculement ne changent pas lors du basculement. L'adresse IP active du lien de basculement accompagne toujours l'unité principale, tandis que l'adresse IP en standby accompagne l'unité secondaire. Activez l'interface

```
hostname(config)#interface phy_if
```

```
hostname(config-if)#no shutdown
```

Dans l'exemple, Ethernet3 est utilisé pour le basculement :

```
hostname(config)#interface ethernet3
```

```
hostname(config-if)#no shutdown
```

5. (Facultatif) Pour activer le basculement dynamique, configurez le lien de basculement dynamique. Spécifiez l'interface à utiliser comme lien de basculement dynamique

```
hostname(config)#failover link if_name phy_if
```

Cet exemple a utilisé « state » comme nom d'interface pour Ethernet2 pour échanger les informations d'état du lien de basculement :

```
hostname(config)#failover link state Ethernet2
```

Remarque : si le lien de basculement dynamique utilise le lien de basculement ou une interface de données, vous devez uniquement fournir l'argument *if_name*. L'argument *if_name* affecte un nom logique à l'interface spécifiée par l'argument *phy_if*. L'argument *phy_if* peut être le nom du port physique, par exemple Ethernet1, ou une sous-interface créée précédemment, par exemple Ethernet0/2.3. Cette interface ne doit pas être utilisée dans un autre but, sauf éventuellement comme lien de basculement. Affectez une adresse IP active et une adresse IP en veille au lien de basculement dynamique. **Remarque** : si le lien de basculement dynamique utilise le lien de basculement ou l'interface de données, ignorez cette étape. Vous avez déjà défini l'adresse IP active et l'adresse IP en standby pour l'interface.

```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

Dans cet exemple, 10.0.0.1 est utilisé comme adresse IP active et 10.0.0.2 est utilisé comme adresse IP en standby pour le lien de basculement dynamique.

```
hostname(config)#failover interface ip state 10.0.0.1 255.0.0.0
                standby 10.0.0.2
```

L'adresse IP de secours doit être dans le même sous-réseau que l'adresse IP active. Vous n'avez pas besoin d'identifier le masque de sous-réseau de l'adresse en standby. L'adresse IP et l'adresse MAC du lien de basculement dynamique ne changent pas lors du basculement, sauf si elles utilisent une interface de données. L'adresse IP active reste toujours avec l'unité principale, tandis que l'adresse en standby reste avec l'unité secondaire. Activez l'interface. **Remarque** : si le lien de basculement dynamique utilise le lien de basculement ou l'interface de données, ignorez cette étape. Vous avez déjà activé

l'interface.

```
hostname(config)#interface phy_if
```

```
hostname(config-if)#no shutdown
```

Remarque : Par exemple, dans ce scénario, Ethernet2 est utilisé pour la liaison de basculement dynamique :

```
hostname(config)#interface ethernet2
```

```
hostname(config-if)#no shutdown
```

6. Activez le basculement.

```
hostname(config)#failover
```

Remarque : Émettez d'abord la commande **failover** sur le périphérique principal, puis émettez-la sur le périphérique secondaire. Une fois la commande **failover** exécutée sur le **périphérique secondaire**, le **périphérique secondaire extrait immédiatement la configuration du périphérique principal et se met en veille**. Le périphérique ASA principal demeure opérationnel, achemine le trafic normalement et se marque comme étant le périphérique *actif*. À partir de là, chaque fois qu'une défaillance se produit sur le périphérique actif, le périphérique en veille s'active.

7. Enregistrez la configuration système dans la mémoire flash.

```
hostname(config)#copy running-config startup-config
```

Configuration de l'unité secondaire

La seule configuration requise sur l'unité secondaire concerne l'interface de basculement. L'unité secondaire nécessite ces commandes pour communiquer au départ avec l'unité principale. Une fois que l'unité principale a envoyé sa configuration à l'unité secondaire, la seule différence permanente entre les deux configurations est la commande **failover lan unit**, qui identifie chaque **unité comme principale ou secondaire**.

Pour le mode de contexte multiple, toutes les étapes sont exécutées dans l'espace d'exécution du système, sauf indication contraire.

Pour configurer l'unité secondaire, procédez comme suit :

1. (Pour la plate-forme de dispositif de sécurité PIX uniquement) Activez le basculement basé sur le LAN.

```
hostname(config)#failover lan enable
```

2. Définissez l'interface de basculement. Utilisez les paramètres que vous avez utilisés pour l'unité principale. Spécifiez l'interface à utiliser comme interface de basculement.

```
hostname(config)#failover lan interface if_name phy_if
```

Dans cette documentation, Ethernet0 est utilisé pour une interface de basculement LAN.

```
hostname(config)#failover lan interface failover Ethernet3
```

L'argument *if_name* affecte un nom à l'interface spécifiée par l'argument *phy_if*. Affectez l'adresse active et l'adresse en standby au lien de basculement.

```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

Dans cette documentation, pour configurer la liaison de basculement, 10.1.0.1 est utilisé pour active, 10.1.0.2 pour l'unité de secours, et « failover » est un nom d'interface Ethernet0.

```
hostname(config)#failover interface ip failover 10.1.0.1  
255.255.255.0 standby 10.1.0.2
```

Remarque : Entrez cette commande exactement comme vous l'avez entrée sur l'unité principale lorsque vous avez configuré l'interface de basculement sur l'unité principale. Activez l'interface.

```
hostname(config)#interface phy_if
```

```
hostname(config-if)#no shutdown
```

Par exemple, dans ce scénario, Ethernet0 est utilisé pour le basculement.

```
hostname(config)#interface ethernet3
```

```
hostname(config-if)#no shutdown
```

3. (Facultatif) désignez cette unité comme l'unité secondaire.

```
hostname(config)#failover lan unit secondary
```

Remarque : Cette étape est facultative car, par défaut, les unités sont désignées comme secondaires, sauf si elles ont été préalablement configurées.

4. Activez le basculement.

```
hostname(config)#failover
```

Remarque : après avoir activé le basculement, l'unité active envoie la configuration en mémoire d'exécution à l'unité de secours. Lors de la synchronisation de la configuration, les messages *Beginning configuration replication: Sending to mate* et *End Configuration Replication to mate* apparaissent sur la console de l'unité active.

5. Un fois que la configuration en cours a terminé la réplication, enregistrez la configuration dans la mémoire flash.

```
hostname(config)#copy running-config startup-config
```

Configurations

Ce document utilise les configurations suivantes :

ASA principal
<pre>ASA#show running-config ASA Version 7.2(3) ! !--- To set the firewall mode to transparent mode, !--- use the firewall transparent command !--- in global configuration mode. firewall transparent hostname ASA domain-name default.domain.invalid enable password 2KFQnbNIdI.2KYOU encrypted</pre>

```
names
!
interface Ethernet0
  nameif failover

  description LAN Failover Interface
!
interface Ethernet1
  nameif inside
  security-level 100
!
interface Ethernet2
  nameif outside
  security-level 0

!--- Configure no shutdown in the stateful failover
interface !--- of both Primary and secondary ASA.

interface Ethernet3
  nameif state
  description STATE Failover Interface
!
interface Ethernet4
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Ethernet5
  shutdown
  no nameif
  no security-level
  no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
  domain-name default.domain.invalid
access-list 100 extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500

!--- Assign the IP address to the Primary and !---
Secondary ASA Security Appliance. ip address 172.16.1.1
255.255.255.0 standby 172.16.1.2

failover
failover lan unit primary
failover lan interface failover Ethernet0
failover lan enable
failover key *****
failover link state Ethernet3
failover interface ip failover 10.1.0.1 255.255.255.0
standby 10.1.0.2
failover interface ip state 10.0.0.1 255.0.0.0 standby
10.0.0.2

asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.3 1
timeout xlate 3:00:00
```

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

ASA secondaire

```
ASA#show running-config
ASA Version 7.2(3)
!
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
failover
failover lan unit secondary
failover lan interface failover Ethernet0
failover lan enable
failover key *****
failover interface ip failover 10.1.0.1 255.255.255.0
standby 10.1.0.2
```

Vérification

Utilisation de la commande show failover

Cette section décrit la sortie de la commande **show failover** . Sur chaque unité, vous pouvez vérifier l'état de basculement avec la commande **show failover** .

ASA principal

```
ASA#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: failover Ethernet0 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Last Failover at: 00:08:03 UTC Jan 1 1993
  This host: Primary - Active
    Active time: 1820 (sec)
      Interface inside (172.16.1.1): Normal
      Interface outside (172.16.1.1): Normal
  Other host: Secondary - Standby Ready
    Active time: 0 (sec)
      Interface inside (172.16.1.2): Normal
      Interface outside (172.16.1.2): Normal
```

Stateful Failover Logical Update Statistics

```
Link : state Ethernet3 (up)
Stateful Obj      xmit      xerr      rcv      rerr
General          185        0        183       0
sys cmd          183        0        183       0
up time           0          0         0         0
RPC services      0          0         0         0
TCP conn          0          0         0         0
UDP conn          0          0         0         0
ARP tbl           0          0         0         0
L2BRIDGE Tbl     2          0         0         0
Xlate_Timeout    0          0         0         0
```

Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	1	7012
Xmit Q:	0	1	185

ASA secondaire

```
ASA(config)#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Secondary
Failover LAN Interface: failover Ethernet0 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
```

Last Failover at: 16:39:12 UTC Aug 9 2009

This host: Secondary - Standby Ready

Active time: 0 (sec)

Interface inside (172.16.1.2): Normal

Interface outside (172.16.1.2): Normal

Other host: Primary - Active

Active time: 1871 (sec)

Interface inside (172.16.1.1): Normal

Interface outside (172.16.1.1): Normal

Stateful Failover Logical Update Statistics

Link : state Ethernet3 (up)

Stateful Obj	xmit	xerr	rcv	rerr
General	183	0	183	0
sys cmd	183	0	183	0
up time	0	0	0	0
RPC services	0	0	0	0
TCP conn	0	0	0	0
UDP conn	0	0	0	0
ARP tbl	0	0	0	0
L2BRIDGE Tbl	0	0	0	0
Xlate_Timeout	0	0	0	0

Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	1	7043
Xmit Q:	0	1	183

Utilisez la commande **show failover state** pour vérifier l'état.

ASA principal

ASA#**show failover state**

	State	Last Failure Reason	Date/Time
This host -	Primary		
	Active	None	
Other host -	Secondary		
	Standby Ready	Comm Failure	00:02:36 UTC Jan 1 1993

====Configuration State====

Sync Done

====Communication State====

Mac set

Unité secondaire

ASA#**show failover state**

	State	Last Failure Reason	Date/Time
This host -	Secondary		
	Standby Ready	None	
Other host -	Primary		
	Active	None	

====Configuration State====

Sync Done - STANDBY

====Communication State====

Mac set

Afin de vérifier les adresses IP de l'unité de basculement, utilisez la commande **show failover interface**.

Unité principale

```
ASA#show failover interface
  interface failover Ethernet0
    System IP Address: 10.1.0.1 255.255.255.0
    My IP Address      : 10.1.0.1
    Other IP Address   : 10.1.0.2
  interface state Ethernet3
    System IP Address: 10.0.0.1 255.255.255.0
    My IP Address      : 10.0.0.1
    Other IP Address   : 10.0.0.2
```

Unité secondaire

```
ASA#show failover interface
  interface failover Ethernet0
    System IP Address: 10.1.0.1 255.255.255.0
    My IP Address      : 10.1.0.2
    Other IP Address   : 10.1.0.1
  interface state Ethernet3
    System IP Address: 10.0.0.1 255.255.255.0
    My IP Address      : 10.0.0.2
    Other IP Address   : 10.0.0.1
```

[Affichage des interfaces surveillées](#)

Pour afficher l'état des interfaces surveillées : En mode de contexte unique, entrez la commande **show monitor-interface en mode de configuration globale**. En mode de contexte multiple, entrez la commande **show monitor-interface dans un contexte**.

ASA principal

```
ASA(config)#show monitor-interface
  This host: Primary - Active
    Interface inside (172.16.1.1): Normal
    Interface outside (172.16.1.1): Normal
  Other host: Secondary - Standby Ready
    Interface inside (172.16.1.2): Normal
    Interface outside (172.16.1.2): Normal
```

ASA secondaire

```
ASA(config)#show monitor-interface
  This host: Secondary - Standby Ready
    Interface inside (172.16.1.2): Normal
    Interface outside (172.16.1.2): Normal
  Other host: Primary - Active
    Interface inside (172.16.1.1): Normal
    Interface outside (172.16.1.1): Normal
```

Remarque : si vous n'entrez pas d'adresse IP de basculement, la commande **show failover** affiche 0.0.0.0 pour l'adresse IP et la surveillance de l'interface reste dans un état *en attente*. Référez-vous à la section [show failover section](#) *Référence de commandes des dispositifs de sécurité Cisco, version 7.2 pour plus d'informations sur les différents états de basculement*.

[Affichage des commandes de basculement dans la configuration en cours](#)

Pour afficher les commandes de basculement dans la configuration en cours, entrez la commande suivante :

```
hostname(config)#show running-config failover
```

Toutes les commandes de basculement sont affichées. Sur les unités qui fonctionnent en mode de contexte multiple, entrez la commande **show running-config failover** dans l'espace d'exécution du système. Entrez la commande **show running-config all failover** afin d'afficher les commandes failover dans la configuration en cours et inclure les commandes pour lesquelles vous n'avez pas modifié la valeur par défaut.

Tests sur la fonctionnalité de basculement

Complétez ces étapes afin de tester la fonctionnalité de basculement :

1. Testez que votre unité active ou votre groupe de basculement achemine le trafic comme prévu avec FTP (par exemple) pour envoyer un fichier d'un hôte à l'autre sur différentes interfaces.
2. Forcez un basculement vers l'unité en veille avec la commande suivante : Pour le basculement actif/veille, entrez la commande suivante sur l'unité active :

```
hostname(config)#no failover active
```
3. Utilisez FTP pour transmettre un autre fichier entre les deux mêmes hôtes.
4. Si le test a échoué, entrez la **commande show failover** afin de vérifier l'état du basculement.
5. Lorsque vous avez fini, vous pouvez restaurer l'unité ou le groupe de basculement dans son état actif avec la commande : Pour le basculement actif/veille, entrez la commande suivante sur l'unité active :

```
hostname(config)#failover active
```

Basculement forcé

Pour forcer l'unité en veille à s'activer, entrez l'une des commandes suivantes :

Entrez la commande suivante sur l'unité en veille :

```
hostname#failover active
```

Entrez la commande suivante sur l'unité active :

```
hostname#no failover active
```

Basculement désactivé

Pour désactiver le basculement, entrez la commande suivante :

```
hostname(config)#no failover
```

Si vous désactivez le basculement sur une paire actif/veille, l'état actif et en veille de chaque unité

est conservé jusqu'à ce que vous redémarriez. Par exemple, l'unité en veille reste en mode de veille, et donc les deux unités ne commencent pas à acheminer le trafic. Pour activer l'unité en veille (même avec le basculement désactivé), référez-vous à la section [Basculement forcé](#).

Si vous désactivez le basculement sur une paire actif/actif, les groupes de basculement restent à l'état actif sur l'unité sur laquelle ils sont actuellement actifs, quelle que soit l'unité qu'ils doivent préférer selon leur configuration. La commande **No failover peut être entrée dans l'espace d'exécution du système**.

[Restauration d'une unité défaillante](#)

Pour remettre une unité défaillante dans un état non défaillant, entrez la commande suivante :

```
hostname(config)#failover reset
```

Si vous remettez une unité défaillante dans un état non défaillant, elle ne s'active pas automatiquement. Les unités ou groupes restaurés demeurent en état de veille jusqu'à ce que le basculement (forcé ou naturel) les active. Cela ne concerne pas un groupe de basculement configuré avec la commande preempt. Un groupe de basculement auparavant actif s'active s'il est configuré avec la commande preempt et si l'unité sur laquelle il a eu une défaillance est son unité préférée.

[Dépannage](#)

Quand un basculement se produit, les deux dispositifs de sécurité envoient des messages système. Cette section comprend les rubriques suivantes

- [Surveillance du basculement](#)
- [Défaillance d'une unité](#)
- [%ASA-3-210005 : Connexion allouée à LU défaillante](#)
- [Messages système de basculement](#)
- [Messages de débogage](#)
- [SNMP](#)
- [Problèmes identifiés](#)

[Surveillance du basculement](#)

Cet exemple montre ce qui se produit quand le basculement n'a pas commencé à surveiller les interfaces réseau. Le basculement ne commence pas à surveiller les interfaces réseau tant qu'il n'a pas entendu le deuxième paquet Hello de l'autre unité de cette interface. Cela prend environ 30 secondes. Si l'unité est connectée à un commutateur réseau qui exécute le protocole STP (Spanning Tree Protocol), cela prend deux fois le temps de retard de transfert configuré dans le commutateur, généralement configuré comme 15 secondes, plus ce délai de 30 secondes. En effet, au démarrage d'ASA et immédiatement après un événement de basculement, le commutateur réseau détecte une boucle de pont temporaire. Après détection de cette boucle, il s'arrête pour transférer des paquets sur ces interfaces pendant le temps de retard de transmission. Il entre ensuite en mode écoute pour un délai de transmission supplémentaire, au cours duquel le commutateur écoute les boucles de pont mais ne transmet pas le trafic ou ne transmet pas les paquets Hello de basculement. Après deux fois le délai de transmission

(30 secondes) le flux de trafic reprend. Chaque ASA reste en mode `d'attente` jusqu'à ce qu'il entende 30 secondes de paquets `Hello` de l'autre unité. Dans le temps où l'ASA passe le trafic, il ne tombe pas en panne sur l'autre unité en ne lisant pas les paquets `Hello`. Tous les autres contrôles de basculement se produisent toujours, c'est-à-dire, Power (Alimentation), Interface Loss of Link (Perte d'interface) et Failover Cable `Hello`.

Pour le basculement, Cisco recommande vivement aux clients d'activer portfast sur tous les ports de commutation qui se connectent aux interfaces ASA. En outre, le channeling et le trunking doivent être désactivés sur ces ports. Si l'interface de l'ASA tombe en panne pendant le basculement, le commutateur n'a pas à attendre 30 secondes pendant que le port passe d'un état d'écoute à l'apprentissage à la transmission.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Active
Active time: 6930 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
Other host: Secondary - Standby
Active time: 15 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Normal (Waiting)
```

En résumé, vérifiez ces étapes afin de réduire les problèmes de basculement :

- Contrôlez les câbles réseau connectés aux interfaces qui sont à l'état en attente/défaillant et remplacez-les si possible.
- Si un commutateur est connecté entre les deux unités, vérifiez que les réseaux connectés à l'interface qui sont à l'état en attente/défaillant fonctionnent correctement.
- Contrôlez le port de commutateur connecté à l'interface qui est à l'état en attente/défaillant et, si possible, utilisez l'autre port FE du commutateur.
- Vérifiez que vous avez activé portfast et désactivé le trunking et le channeling sur les ports de commutateur connectés à l'interface.

Défaillance d'une unité

Dans cet exemple, un basculement a détecté une défaillance. Notez que l'interface 1 de l'unité principale est à l'origine de la défaillance. Les unités sont de nouveau en mode `attente` en raison de la défaillance. L'unité défaillante s'est retirée du réseau (les interfaces sont en panne) et n'envoie plus de paquets `Hello` sur le réseau. L'unité active reste dans un état `en attente` jusqu'à ce que l'unité défaillante soit remplacée et que les communications de basculement redémarrent.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Standby (Failed)
Active time: 7140 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Failed (Waiting)
Other host: Secondary - Active
Active time: 30 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
```

Interface outside (172.16.1.1): Normal (Waiting)

Connexion allouée à LU défaillante

Un problème de mémoire peut exister si vous recevez le message d'erreur suivant :

Connexion allouée à LU défaillante

Ce problème est documenté dans l'ID de bogue Cisco [CSCte80027](#) (clients [enregistrés](#) uniquement). Afin de résoudre ce problème, mettez à niveau votre pare-feu vers une version logicielle dans laquelle ce bogue est corrigé. Certaines des versions du logiciel ASA sous lesquelles ce bogue a été corrigé sont 8.2(4), 8.3(2), 8.4(2).

Messages système de basculement

Le dispositif de sécurité émet un certain nombre de messages système relatifs au basculement au niveau de priorité 2, ce qui indique un état critique. Pour afficher ces messages, référez-vous à [Configuration de journalisation et messages du journal système des dispositifs de sécurité Cisco pour activer la journalisation et consulter les descriptions des messages système.](#)

Remarque : Au sein de la commutation, le basculement s'arrête logiquement, puis déclenche les interfaces, ce qui génère des messages syslog **411001** et **411002**. Cette activité est normale.

Messages de débogage

Pour consulter les messages de débogage, entrez la commande **debug fover**. Référez-vous à [Référence de commandes des dispositifs de sécurité Cisco version 7.2 pour plus d'informations.](#)

Remarque : Étant donné que la sortie de débogage se voit attribuer une priorité élevée dans le processus du processeur, elle peut affecter considérablement les performances du système. Par conséquent, n'utilisez les commandes **debug fover** que pour résoudre des problèmes spécifiques ou dans des sessions de dépannage avec le personnel d'assistance technique Cisco.

SNMP

Pour recevoir les interruptions SNMP syslog relatives au basculement, configurez les agents SNMP pour qu'ils envoient des interruptions SNMP aux stations de gestion SNMP, définissez un hôte syslog et compilez la MIB syslog Cisco sur votre station de gestion SNMP. Référez-vous aux commandes **snmp-server** et [logging dans le Guide de référence des commandes des dispositifs de sécurité Cisco pour plus d'informations.](#)

Délai d'interrogation du basculement

Pour spécifier les délais d'interrogation et de mise en suspens des unités de basculement, utilisez la commande **failover polltime** dans le mode de configuration globale.

L'unité de temps de basculement msec [time] interroge les messages Hello afin de représenter l'intervalle de temps afin de vérifier l'existence de l'unité de secours.

De même, **failover holdtime** unit msec [time] représente l'intervalle défini durant lequel une unité doit recevoir un message hello sur le lien de basculement et après lequel l'autre unité est déclarée défaillante.

Pour spécifier les délais d'interrogation et de mise en suspens de l'interface de données dans une configuration actif/veille, utilisez la commande **failover polltime interface en mode de configuration globale**. Pour restaurer les délais d'interrogation et de mise en suspens par défaut, utilisez la forme **no de cette commande**.

```
failover polltime interface [msec] time [holdtime time]
```

Utilisez la commande **failover polltime interface** pour changer la fréquence d'envoi des paquets **hello aux interfaces de données**. Cette commande est disponible uniquement pour le basculement actif/veille. Pour le basculement actif/actif, utilisez la commande **polltime interface dans le mode de configuration du groupe de basculement au lieu de la commande failover polltime interface**.

Vous ne pouvez pas entrer de **valeur de mise en suspens inférieure à 5 fois le délai d'interrogation de l'interface**. Avec un délai d'interrogation inférieur, le dispositif de sécurité peut détecter une défaillance et déclencher un basculement plus rapidement. Cependant, une détection plus rapide peut entraîner des commutations inutiles lorsque le réseau est temporairement encombré. Le test de l'interface commence quand un paquet hello n'est pas entendu sur l'interface pendant plus de la moitié du temps de mise en suspens.

Vous pouvez inclure à la fois la commande **failover polltime unit** et la commande **failover polltime interface** dans la configuration.

Dans cet exemple, la fréquence d'interrogation de l'interface est définie à 500 millisecondes et délai de mise en suspens à 5 secondes :

```
hostname(config)#failover polltime interface msec 500 holdtime 5
```

Référez-vous à la section [failover polltime de Référence de commandes des dispositifs de sécurité Cisco, version 7.2 pour plus d'informations](#).

[Exportation du certificat ou de la clé privée dans la configuration de basculement](#)

Le périphérique principal réplique automatiquement la clé privée/le certificat sur l'unité secondaire. Émettez la commande **write memory** dans l'unité active afin de répliquer la configuration, qui inclut le certificat/la clé privée, à l'unité de secours. Tous les certificats/clés sur l'unité en veille sont effacés et réintroduits par la configuration de l'unité active.

Remarque : Vous ne devez pas importer manuellement les certificats, les clés et les points d'approbation à partir du périphérique actif, puis exporter vers le périphérique de secours.

[AVERTISSEMENT : Échec du déchiffrement du message de basculement](#)

Message d'erreur :

```
Failover message decryption failure. Please make sure both units have the same failover shared key and crypto license or system is not out of memory
```

Ce problème provient de la configuration de la clé de basculement. Pour résoudre ce problème, supprimez la clé de basculement et configurez la nouvelle clé partagée.

Problème : Le basculement est toujours allumé après la configuration du basculement en mode multiple actif/veille transparent

Le basculement est constant lorsque les interfaces internes des deux ASA sont directement connectées et que les interfaces externes des deux ASA sont directement connectées. Mais le basculement clignote lorsqu'un commutateur est utilisé entre les deux.

Solution : Désactivez la BPDU sur les interfaces ASA afin de résoudre ce problème.

Basculement des modules ASA

Si Advanced Inspection and Prevention Security Services Module (AIP-SSM) ou Content Security and Control Security Services Module (CSC-SSM) sont utilisés sur les unités actives et en veille, elles fonctionnent indépendamment du ASA en matière de basculement. **Les modules doivent être configurés manuellement dans les unités actives et en veille, le basculement ne répliquera pas la configuration du module.**

En matière de basculement, les unités ASA qui ont des modules AIP-SSM ou CSC-SSM doivent avoir le même type de matériel. Par exemple, si l'unité principale comporte le module ASA-SSM-10, l'unité secondaire doit contenir aussi le module ASA-SSM-10.

Échec de l'allocation du paquet de messages de basculement

Message d'erreur %PIX|ASA-3-105010 : (Primary) Failover message block alloc failed

Explication : Le bloc de mémoire est épuisé. Il s'agit d'un message provisoire. Le dispositif de sécurité doit reprendre. *Principal peut aussi être répertorié comme Secondaire pour l'unité secondaire.*

Action recommandée : Utilisez la commande **show blocks** pour surveiller le bloc de mémoire actuel.

Problème de basculement du module AIP

Si vous avez deux ASA dans une configuration de basculement et que chacun contient un module AIP-SSM, vous devez répliquer manuellement la configuration des AIP-SSM. Seule la configuration du ASA est répliquée par le mécanisme de basculement. Le module AIP-SSM n'est pas inclus dans le basculement.

L'AIP-SSM commence par fonctionner indépendamment du ASA pour le basculement. Pour le basculement, tout ce qui est nécessaire concernant l'ASA est que les modules AIP aient le même type de matériel. En outre, comme avec toute autre opération de basculement, la configuration du ASA doit être synchronisée entre l'unité active et l'unité en veille.

Quant à la configuration des AIP, ce sont effectivement des détecteurs indépendants. Il n'y a aucun basculement entre les deux, et ils n'ont aucune connaissance l'un de l'autre. Ils peuvent exécuter des versions de code indépendantes. En effet, ils ne doivent pas se correspondre et l'ASA ne s'occupe pas de la version de code exécutée sur l'AIP pour le basculement.

ASDM initie une connexion avec l'AIP via l'interface de gestion IP que vous avez configurée sur l'AIP. En d'autres termes, il se connecte au capteur généralement via HTTPS, ce qui dépend de la

manière dont vous configurez le capteur.

Vous pouvez avoir un basculement de l'ASA indépendamment des modules IPS (AIP). Vous êtes toujours connecté au même car vous vous connectez à son adresse IP de gestion. Pour vous connecter à l'autre AIP, vous devez vous reconnecter à son IP de gestion pour le configurer et y accéder.

Consultez [ASA : Envoyer le trafic réseau de l'ASA vers l'exemple de configuration AIP SSM](#) pour plus d'informations et d'exemples de configuration sur la façon d'envoyer le trafic réseau qui passe par l'appliance de sécurité adaptable (ASA) de la gamme Cisco ASA 5500 au module AIP-SSM (Advanced Inspection and Prevention Security Services Module) (IPS)

Problèmes identifiés

Lorsque vous essayez d'accéder à l'ASDM sur l'ASA secondaire avec le logiciel version 8.x et l'ASDM version 6.x pour la configuration de basculement, cette erreur est reçue :

Erreur : `The name on the security certificate is invalid or does not match the name of the site`

Dans le certificat, l'émetteur et le nom du sujet sont l'adresse IP de l'unité *active*, et non l'adresse IP de l'unité *en veille*.

Dans ASA version 8.x, le certificat interne (ASDM) est répliqué de l'unité active à l'unité en veille, ce qui provoque le message d'erreur. Mais, si le même pare-feu s'exécute sur le code version 7.x avec l'ASDM 5.x et que vous essayez d'accéder à l'ASDM, vous recevez cet avertissement de sécurité régulier :

`The security certificate has a valid name matching the name of the page you are trying to view`

Lorsque vous vérifiez le certificat, l'émetteur et le nom du sujet est l'adresse IP de l'unité en veille.

Informations connexes

- [Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500](#)
- [Logiciels pare-feu Cisco PIX](#)
- [Configuration de basculement de Firewall Services Module \(FWSM\)](#)
- [Dépannage du basculement FWSM](#)
- [Fonctionnement du basculement sur le pare-feu Cisco Secure PIX](#)
- [Support et documentation techniques - Cisco Systems](#)