Les connexions de mobilité sans fil échouent et ne se récupèrent pas lors du redémarrage de l'ASA

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Conventions](#)
[Problème](#)
[Exemple de topologie de réseau](#)
[Déclencheur de problème](#)
[Solution](#)
[Solution 1](#)
[Solution 2](#)
[Informations connexes](#)

Introduction

Ce document décrit un problème dans lequel une connexion de chemin de mobilité (utilisant le protocole UDP (User Datagram Protocol) et le protocole IP 93) qui traverse un dispositif de sécurité adaptatif (ASA) peut tomber en panne et continuer à échouer jusqu'à ce que les périphériques de mobilité soient rechargés, ou que le trafic de chemin de mobilité soit arrêté et laissé inactif pendant une courte période, puis redémarré.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appareil de sécurité adaptatif Cisco (ASA)
- Contrôleur LAN sans fil (WLC)

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

Conventions

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

Problème

Dans cette situation, un contrôleur de réseau local sans fil (WLC) à l'adresse 10.10.1.2 tente de communiquer avec le WLC à l'adresse 10.10.9.3, mais la communication échoue.

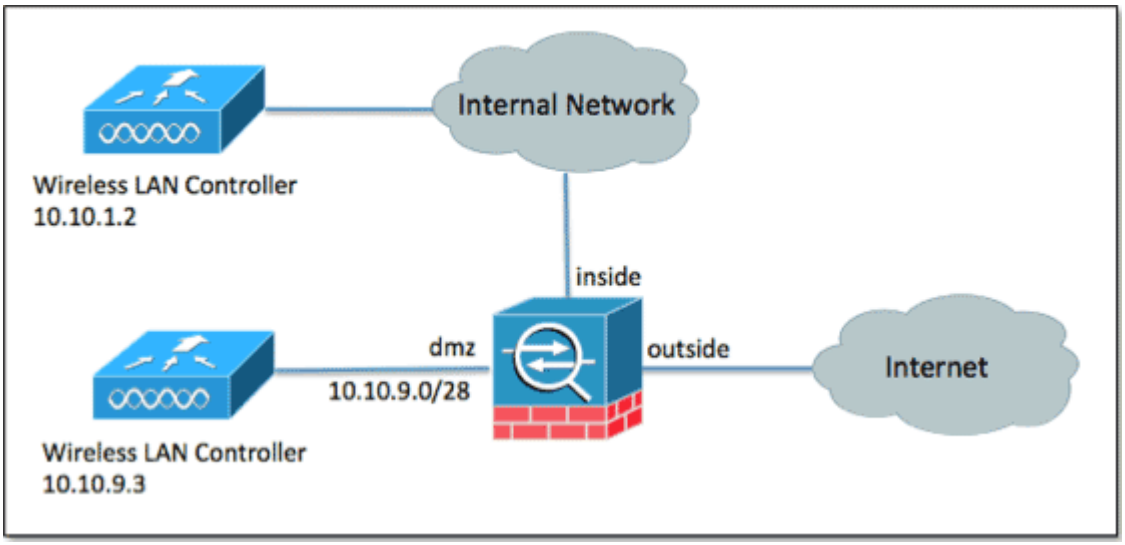
Ce problème peut être déclenché par l'un de ces événements :

- L'ASA est redémarré.
- La table de routage est modifiée par un administrateur ou un protocole de routage.
- Une interface est arrêtée, puis réactivée par l'administrateur.

Outre le trafic de mobilité, ce problème peut être rencontré pour tous les protocoles IP UDP ou non TCP.

Ce problème n'est pas un bogue, mais une conséquence de la topologie du réseau et de la configuration ASA. Reportez-vous à la section ci-dessous pour connaître la cause et la solution de ce problème.

Exemple de topologie de réseau



Configuration du routage ASA :

```
!
```

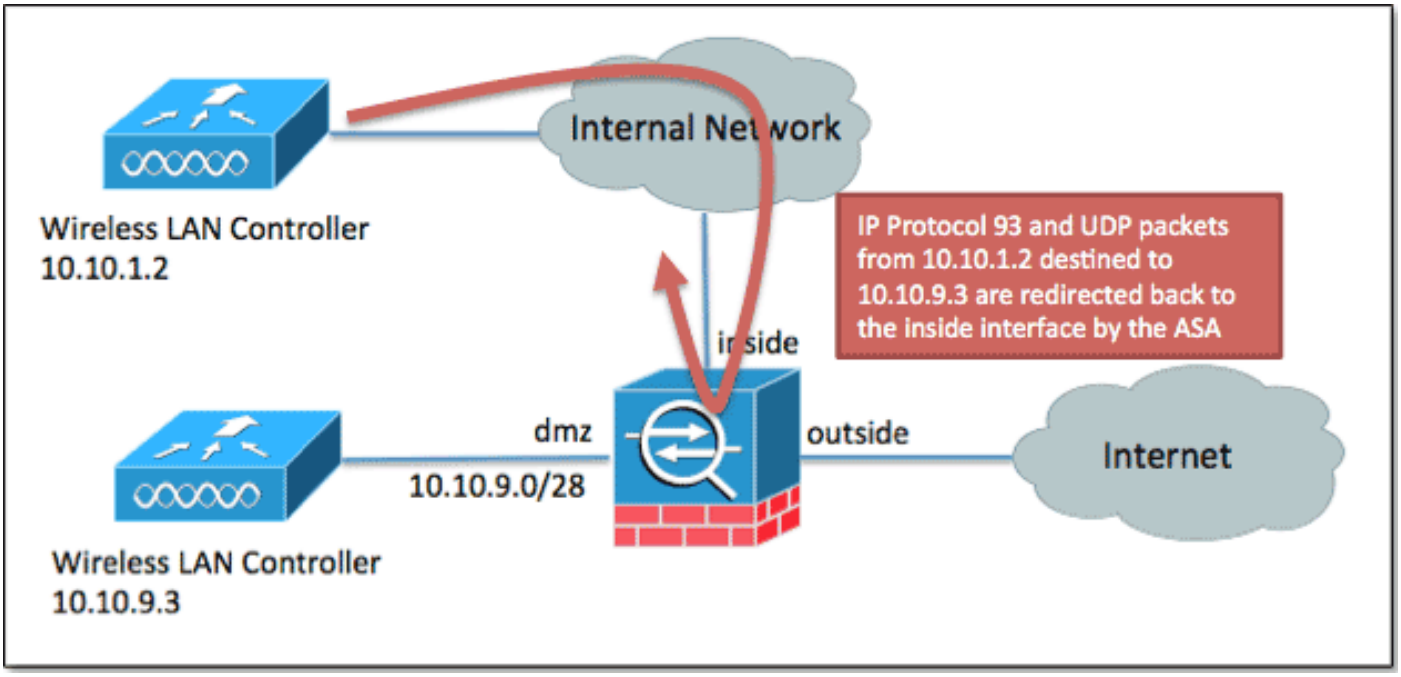
```
route outside 0.0.0.0 0.0.0.0 192.168.4.3 1
route inside 10.0.0.0 255.0.0.0 192.168.254.1 1
!
same-security-traffic permit intra-interface
!
```

Configuration de l'interface dmz ASA :

```
!
interface Gigabit-Ethernet0/1.10
vlan 10
nameif dmz
security-level 75
ip address 10.10.9.1 255.255.255.240 standby 10.10.9.2
!
```

Déclencheur de problème

Le problème est déclenché lorsque le WLC à 10.10.1.2 envoie le trafic destiné au WLC à 10.10.9.3. Ces paquets amènent l'ASA à créer une connexion dans sa table de connexion qui envoie le trafic de mobilité par la mauvaise interface ASA (interne).



Ce problème est dû au fait que l'interface de destination « dmz » de l'ASA est en état down/down au moment de la création de la connexion, ce qui fait que la connexion est construite à partir d'une interface différente et non optimale. L'interface dmz peut être arrêtée en raison d'un problème de câble, d'un problème de négociation Ethernet ou Port-Channel, ou elle peut être désactivée par l'administrateur.

Au moment du problème, les connexions de chemin de mobilité peuvent être considérées comme étant créées comme étant « intra-interface » de l'ASA, qui achemine les paquets vers la même interface interne qu'ils sont arrivés :

```
ASA# show conn address 10.10.1.2
15579 in use, 133142 most used
97 inside 10.10.9.3 inside 10.10.1.2, idle 0:00:00, bytes 32210
UDP inside 10.10.9.3:16666 inside 10.10.1.2:16666, idle 0:00:00, bytes 4338, flags -
```

```
97 inside 10.10.9.3 inside 10.10.1.2, idle 0:00:00, bytes 157240
ASA#
```

Le point d'extrémité de mobilité 10.10.1.2 continue d'envoyer le trafic destiné à 10.10.9.3, qui correspond à ces connexions existantes. Même si l'interface dmz devait passer à l'état up/up, le trafic de mobilité provenant de 10.10.1.2 correspondrait aux connexions existantes dans la table (au lieu de créer une nouvelle connexion à l'interface dmz) qui réinitialise le délai d'expiration des connexions sur l'ASA, ce qui prolonge le problème.

En résumé, ces événements peuvent déclencher le problème :

1. Le périphérique 10.10.1.2 envoie un paquet UDP ou protocole 97 à 10.10.9.3.
2. L'ASA reçoit le paquet sur l'interface interne, mais l'interface dmz est désactivée, ce qui fait que la route plus spécifique vers le réseau de destination est absente de la table de routage. Étant donné que la commande **same-security permit intra-interface** est activée sur l'ASA, elle suit une route statique configurée pour le réseau 10.0.0.0/8 à travers l'interface interne, construit une connexion dans la table de connexion, puis renvoie le paquet de l'interface interne vers le réseau interne.
3. Àun moment donné, l'interface dmz peut revenir en mode up et la route est ajoutée à la table ; cependant, puisque la connexion pour le trafic du protocole 97 a déjà été créée à l'étape 2, les paquets suivants correspondent à la connexion et la table de routage est écrasée, et le trafic n'atteint pas le serveur sur la dmz.

Solution

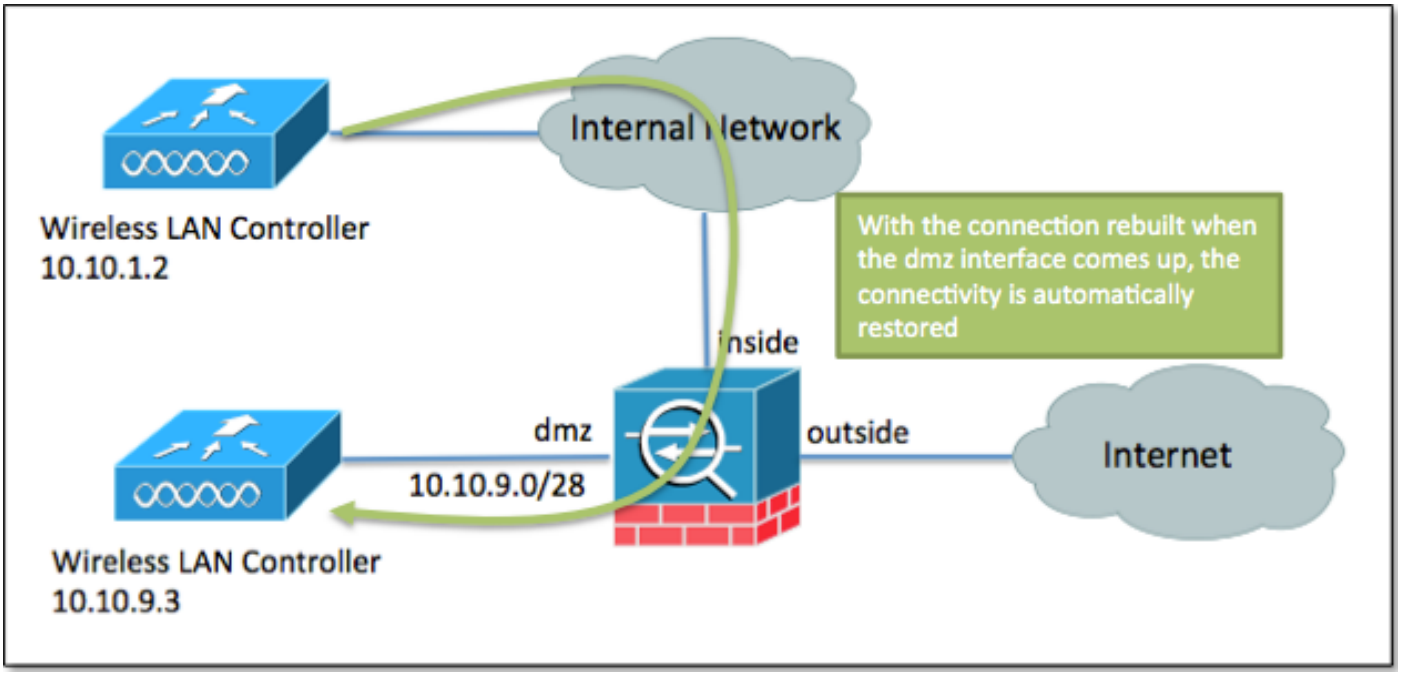
Solution 1

Une solution possible à ce problème est de supprimer la commande **same-security permit intra-interface** de l'ASA. Cette solution empêche la connexion de retour en arrière d'être construite à partir de la même interface sur laquelle le paquet d'origine a été reçu, ce qui permet de créer la connexion correcte lorsque l'interface s'active. Cependant, selon la table de routage de l'ASA, cette solution peut ne pas fonctionner (le trafic peut être acheminé vers une autre interface autre que la destination prévue en fonction de la table de routage), et la commande **same-security permit intra-interface** peut être nécessaire pour d'autres connexions sur l'ASA.

Solution 2

Pour cette instance spécifique, le problème a été atténué avec succès en activant la fonction **temporisation conn flottante**. Cette fonctionnalité, qui n'est pas activée par défaut, a provoqué la désactivation de ces connexions une minute après l'ajout d'une route préférée vers l'un des points d'extrémité à la table de routage via une nouvelle interface de l'ASA, qui se produit lorsque l'interface dmz s'active. Les connexions sont ensuite immédiatement reconstruites lorsque le paquet suivant arrive à l'ASA, en utilisant l'interface préférée (dmz, au lieu de l'intérieur de l'hôte 10.10.9.3).

```
ASA(config)# timeout floating-conn 0:01:00
```



Lorsque le problème est atténué, les connexions correctes sont construites dans la table de connexion ASA et la connectivité est automatiquement restaurée :

```
ASA# show conn address 10.10.1.2
15329 in use, 133142 most used
97 dmz 10.10.9.3 inside10.10.1.2, idle 0:00:00, bytes 3175742510
UDP dmz 10.10.9.3:16666 inside 10.10.1.2:16666, idle 0:00:00, bytes 40651338, flags -
97 dmz 10.10.9.3 inside10.10.1.2, idle 0:00:00, bytes 1593457240
ASA#
```

Informations connexes

- Référence des commandes ASA 9.1 - timeout, commande de conn flottante
- Support et documentation techniques - Cisco Systems