Les connexions de mobilité sans fil échouent et ne récupèrent pas quand l'ASA est redémarrée

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Conventions](#)
[Problème](#)
[Topologie du réseau d'échantillon](#)
[Déclencheur de problème](#)
[Solution](#)
[Solution 1](#)
[Solution 2](#)
[Informations connexes](#)

Introduction

Ce document décrit un problème où une connexion de chemin de mobilité (utilisant Protocole UDP (User Datagram Protocol) et protocole 93 IP) cette traverse une appliance de sécurité adaptable (ASA) pourrait descendre et continuer à échouer jusqu'à ce que les périphériques de mobilité soient rechargés, ou le trafic de chemin de mobilité est arrêté et pendant une courte période laissé inactif et alors redémarré.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appliance de sécurité adaptable Cisco (ASA)
- Contrôleur LAN Sans fil (WLC)

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

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 LAN Sans fil (WLC) chez 10.10.1.2 tente de communiquer avec le WLC chez 10.10.9.3, mais la transmission échoue.

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

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

Sans compter que le trafic de mobilité, ce problème pourrait être expérimenté pour tous les protocoles d'UDP ou IP de non-tcp.

Ce problème n'est pas une bogue mais une conséquence de la topologie du réseau et de configuration ASA. Voir ci-dessous pour la cause et la solution au problème.

Topologie du réseau d'échantillon

Configuration de 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 d'interface de 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 quand le WLC chez 10.10.1.2 envoie le trafic destiné au WLC chez

10.10.9.3. Ces paquets font établir l'ASA une connexion dans sa table de connexion qui envoie au trafic de mobilité l'interface fausse ASA (à l'intérieur).

Cette question est provoqué par par l'interface « dmz » de destination de l'ASA étant dans le bas/l'état d'indisponibilité lorsque la connexion a été établie, qui a comme conséquence la connexion étant construite une interface différente et non-optimale. L'interface de dmz pourrait être en baisse en raison d'un problème de câble, d'un Ethernet ou de la question de négociation de Port canalisé, ou elle pourrait être administrativement arrêtée.

Au moment du problème, les connexions de chemin de mobilité peuvent être vues comme étant créé en tant que « intra-interface » de l'ASA, qui conduit les paquets soutiennent la même interface interne qu'ils sont arrivée en fonction :

```
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 final de mobilité chez 10.10.1.2 continue à envoyer le trafic destiné à 10.10.9.3, qui apparie ces connexions existantes. Même si l'interface de dmz étaient de progresser à l'état up/up, le trafic de mobilité originaire de 10.10.1.2 apparierait les connexions existantes dans la table (au lieu d'établir une nouvelle connexion à l'interface de dmz) qui remet à l'état initial le délai d'attente des connexions sur l'ASA, qui prolonge le problème.

En résumé, ces événements peuvent déclencher la question :

1. Le périphérique chez 10.10.1.2 envoie un protocole 97 ou le paquet UDP à 10.10.9.3.
2. L'ASA reçoit le paquet sur l'interface interne, mais l'interface de dmz est en baisse, qui résulte dans plus d'artère spécifique aux disparus de réseau de destination de la table de routage. Puisque la commande **intra-interface d'autorisation de même-Sécurité** est activée sur l'ASA, elle suit une route statique configurée pour le dos de 10.0.0.0/8 réseaux par l'interface interne, établit une connexion dans la table de connexion, et puis envoie le paquet soutiennent l'interface interne vers le réseau interne.
3. Àun certain point l'interface de dmz pourrait se réactiver et l'artère est ajoutée de nouveau à la table ; cependant, puisque la connexion pour le trafic du protocole 97 a été déjà établie dans l'étape #2, les paquets suivants apparieront la connexion et la table de routage est remplacée, et le trafic n'atteint pas le serveur sur le dmz.

Solution

Solution 1

Une solution possible pour cette question est de retirer la commande **intra-interface d'autorisation de même-Sécurité de l'**ASA. Cette solution empêche la connexion de demi-tour d'être construite soutiennent la même interface sur laquelle le paquet d'origine a été reçu, qui permet la connexion correcte à construire quand l'interface est soulevée. Cependant, selon la table de routage de l'ASA, cette solution ne pourrait pas fonctionner (le trafic pourrait être conduit à une autre interface autre que la destination destinée basée sur la table de routage), et la commande **intra-interface d'autorisation de même-Sécurité** pourrait être nécessaire pour d'autres

connexions sur l'ASA.

Solution 2

Pour cet exemple spécifique, le problème a été avec succès atténué en activant la caractéristique flottement-**conn. de délai d'attente**. Cette caractéristique, qui n'est pas activée par défaut, a fait démolir l'ASA ces connexions une minute après que plus de route préférée à un des points finaux est ajoutée à la table de routage une nouvelle interface de l'ASA, qui se produit quand l'interface de dmz est soulevée. Les connexions alors sont immédiatement reconstruites quand le paquet suivant arrive à l'ASA, utilisant l'interface plus préférée (dmz, au lieu de l'intérieur pour l'hôte de 10.10.9.3).

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

Quand le problème est atténué, les connexions correctes sont établies 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 de commandes ASA 9.1 - commande flottement-conn. de délai d'attente
- Support et documentation techniques - Cisco Systems