Le trafic UDP via ASA échoue après la remise en ligne de la liaison principale du FAI dans une configuration double du FAI

Contenu

Introduction

Si un dispositif de sécurité adaptatif (ASA) possède deux interfaces de sortie par sous-réseau de destination et que la route préférée vers une destination est supprimée de la table de routage pendant un certain temps, les connexions UDP (User Datagram Protocol) peuvent échouer lorsque la route préférée est réajoutée à la table de routage. Les connexions TCP peuvent également être affectées par le problème, mais puisque le protocole TCP détecte la perte de paquets, ces connexions sont automatiquement désactivées par les points d'extrémité et reconstruites à l'aide des routes les plus optimales après le changement de routes.

Ce problème peut également être observé si un protocole de routage est utilisé et qu'une modification de topologie déclenche une modification de la table de routage sur l'ASA.

Avant de commencer

Conditions requises

Pour résoudre ce problème, la table de routage de l'ASA doit changer. Cela est courant avec les liaisons ISP doubles de manière redondante ou lorsque l'ASA apprend des routes via un protocole IGP (OSPF, EIGRP, RIP).

Ce problème se produit lorsque la liaison principale du FAI revient en ligne ou que ledit IGP voit une reconvergence due à laquelle une route moins préférée utilisée par l'ASA est remplacée par la route moins métrique préférée. Vous verriez alors des connexions de longue durée, telles que les enregistrements SIP UDP, GRE, etc., échouer une fois que la route principale ou préférée est réinstallée dans la table de routage de l'ASA.

Components Used

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

- Tout dispositif de sécurité adaptatif de la gamme Cisco ASA 5500
- ASA versions 8.2(5), 8.3(2)12, 8.4(1)1, 8.5(1) et ultérieures

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Problème

Si une entrée de table de routage est supprimée de la table de routage de l'ASA et qu'il n'y a aucune route en dehors d'une interface pour atteindre une destination, les connexions construites par le pare-feu avec cette destination étrangère seront supprimées par l'ASA. Cela se produit afin que les connexions puissent être construites à nouveau à l'aide d'une interface différente avec des entrées de routage pour la destination présente.

Cependant, si des routes plus spécifiques sont ajoutées à nouveau à la table, les connexions ne seront pas mises à jour pour utiliser les nouvelles routes plus spécifiques et continueront à utiliser l'interface moins optimale.

Par exemple, considérez que le pare-feu a deux interfaces qui font face à Internet - « externe » et « de secours » - et que ces deux routes existent dans la configuration de l'ASA :

```
route outside 0.0.0.0 0.0.0.0 10.1.1.1 1 track 1
route backup 0.0.0.0 0.0.0.0 172.16.1.1 254
```

Si les interfaces externe et de sauvegarde sont actives, les connexions sortantes construites via le pare-feu utiliseront l'interface externe, car elle a la métrique préférée de 1. Si l'interface externe est arrêtée (ou si la fonction de surveillance SLA qui suit la route rencontre une perte de connectivité à l'adresse IP suivie), les connexions utilisant l'interface externe sont désactivées et reconstruites à l'aide de l'interface de sauvegarde, car l'interface de sauvegarde est la seule interface avec une route vers la destination.

Le problème se produit lorsque l'interface externe est réactivée ou que la route suivie redevient la route préférée. La table de routage est mise à jour pour préférer la route d'origine, mais les connexions existantes continuent d'exister sur l'ASA et traversent l'interface de sauvegarde et ne sont PAS supprimées et recréées sur l'interface externe avec la métrique la plus préférée. En effet, la route de secours par défaut existe toujours dans la table de routage spécifique à l'interface de l'ASA. La connexion continue à utiliser l'interface avec la route la moins préférée jusqu'à ce que la connexion soit supprimée ; dans le cas du protocole UDP, cela peut être illimité.

Cette situation peut entraîner des problèmes avec les connexions de longue durée, telles que les enregistrements SIP externes ou d'autres connexions UDP.

Solution

Afin de résoudre ce problème spécifique, une nouvelle fonctionnalité a été ajoutée à l'ASA qui provoquera le démontage et la reconstruction des connexions sur une nouvelle interface si une route plus préférée vers la destination est ajoutée à la table de routage. Afin d'activer la fonctionnalité (elle est désactivée par défaut), définissez un délai d'attente différent de zéro sur la commande **timeout flottante-conn**. Ce délai d'attente (spécifié dans le format HH:MM:SS) spécifie le délai d'attente de l'ASA avant de mettre fin à la connexion une fois qu'une route préférée est ajoutée à la table de routage :

Voici un exemple CLI d'activation de la fonctionnalité. Avec cette interface de ligne de commande, si un paquet est reçu sur une connexion existante pour laquelle il existe maintenant une route différente, plus préférée vers la destination, la connexion sera désactivée 1 minute plus tard (et reconstruite à l'aide de la nouvelle route préférée) :

```
ASA# config terminal
ASA(config)# timeout floating-conn 0:01:00
ASA(config)# end
ASA# show run timeout
timeout conn 1:00:00 half-closed 0:10:00 udp 0:50:00 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 sip-provisional-media 0:02:00 uauth 0:01:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout xlate 0:01:00
timeout pat-xlate 0:00:30
timeout floating-conn 0:01:00
ASA#
```

Cette fonctionnalité est ajoutée à la plate-forme ASA dans les versions 8.2(5), 8.3(2)12, 8.4(1)1 et 8.5(1), y compris les versions ultérieures du logiciel ASA.

Si vous exécutez une version du code ASA qui n'implémente pas cette fonctionnalité, une solution de contournement du problème consisterait à vider manuellement les connexions UDP qui continuent de prendre la route la moins préférée malgré une meilleure route rendue disponible via un **hôte local *<IP>*** ou **clear-conn *<IP>*** clair.

La référence de commande répertorie cette nouvelle fonctionnalité dans la section timeout.

Informations connexes

- Support et documentation techniques - Cisco Systems