Le trafic UDP par l'ASA échoue après que le lien primaire ISP revienne en ligne dans une double installation ISP

Contenu

Introduction

Si une appliance de sécurité adaptable (ASA) a deux interfaces de sortie par sous-réseau de destination et la route préférée à une destination est retirée de la table de routage pendant quelque temps, les connexions de Protocole UDP (User Datagram Protocol) peuvent échouer quand la route préférée obtient re-ajouté à la table de routage. Des connexions TCP pourraient également être affectées par le problème, mais puisque le TCP détecte la perte de paquets, ces connexions sont démolies automatiquement par les points finaux, et reconstruit utilisant plus de routes optimales après les artères changez.

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

Avant de commencer

Conditions requises

Afin de rencontrer ce problème, la table de routage de l'ASA doit changer. C'est commun avec de doubles liens ISP d'une mode redondante ou quand l'ASA apprend des artères par l'intermédiaire d'un IGP (OSPF, EIGRP, RIP).

Cette question se produit quand le lien primaire ISP revient en ligne ou ledit IGP voit une reconvergence due à ce que moins de route préférée qui était utilisée par l'ASA est remplacée par la bas-mesure-artère préférée. Vous verriez alors les connexions longévitales, telles que des enregistrements de SIP d'UDP, GRE, etc., manquant une fois que le primaire ou la route préférée est réinstallé dans la table de routage de l'ASA.

Composants utilisés

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

- Toute appliance de sécurité adaptatif de la gamme Cisco ASA 5500
- Versions 8.2(5) ASA, 8.3(2)12, 8.4(1)1, 8.5(1) et plus tard

Conventions

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

Problème

Si une entrée de table de routage est retirée de la table de routage de l'ASA et il n'y a aucune artère hors d'une interface pour atteindre une destination, des connexions établies par le Pare-feu avec cette destination étrangère seront supprimées par l'ASA. Ceci se produit de sorte que les connexions puissent être établies de nouveau utilisant une interface différente avec des entrées de routage pour le présent de destination.

Cependant, si plus d'artères spécifiques sont ajoutées de nouveau à la table, les connexions ne seront pas mises à jour pour utiliser le nouveau, plus d'artères de particularité, et continueront à utiliser l'interface moins-optimale.

Par exemple, considérez que le Pare-feu a deux interfaces qui font face à l'Internet - « extérieur » et « sauvegarde » - et ces deux artères 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 l'extérieur et les Interfaces de sauvegarde sont « vers le haut de », alors les connexions ont construit sortant par le Pare-feu utiliseront l'interface extérieure, car elle a la mesure préférée de 1. Si l'interface extérieure est arrêtée (ou la fonction de surveillance SLA qui dépiste l'artère rencontre une perte de connectivité à l'IP dépisté), des connexions utilisant l'interface extérieure seraient démolies et reconstruites utilisant l'Interface de sauvegarde, car l'Interface de sauvegarde est la seule interface avec une artère à la destination.

Le problème se pose quand l'interface extérieure est apportée sauvegardent ou l'artère dépistée devient l'artère favorisée de nouveau. La table de routage est mise à jour pour préférer l'artère d'origine, mais les connexions existantes continuent à exister sur l'ASA et à traverser l'Interface de sauvegarde et ne sont pas supprimées et sont recréées sur l'interface extérieure avec la mesure plus-préférée. C'est parce que le default route de sauvegarde existe toujours dans la table de routage de l'interface-particularité de l'ASA. La connexion continue à utiliser l'interface avec moins de route préférée jusqu'à ce que la connexion soit supprimée ; dans le cas de l'UDP, ceci pourrait être indéfini.

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

Solution

Afin d'aborder ce problème spécifique, une nouvelle caractéristique a été ajoutée à l'ASA qui causera des connexions d'être démolies et reconstruites sur une nouvelle interface si plus de route préférée à la destination est ajoutée à la table de routage. Afin de lancer la caractéristique (elle est désactivée par défaut), placez un délai d'attente différent de zéro à la commande flottement-**conn. de délai d'attente**. Ce délai d'attente (spécifié dans HH : Millimètre : Les solides solubles) spécifie le temps où l'ASA attend avant qu'elle démolisse la connexion une fois plus de route préférée est ajoutée de nouveau à la table de routage :

C'est un exemple CLI d'activer la caractéristique. Avec ce CLI, si un paquet est reçu sur une connexion existante pour laquelle il y a maintenant un différent, plus de route préférée à la destination, la connexion sera déchirée vers le bas 1 minute plus tard (et reconstruit utilisant le nouveau, plus de 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 caractéristique 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 des versions ultérieures de logiciel ASA.

Si vous exécutez une version du code ASA qui n'implémente pas cette caractéristique, un contournement à la question serait de vider manuellement les connexions d'UDP qui continuent à prendre moins de route préférée en dépit d'une meilleure artère étant rendue disponible par l'intermédiaire d'un **hôte local clair** *<IP>* ou du **clear conn** *<IP>*.

Les listes de référence de commandes cette nouvelle caractéristique sous la section de délai d'attente.

Informations connexes

- Support et documentation techniques - Cisco Systems