

Dépannage de débit et de vitesse de connexion ASA et analyse des captures de paquet

Résumé

Introduction

Il décrit comment dépanner les problèmes de débit et de vitesse de connexion du Dispositif de sécurité adaptatif (ASA) dédié Cisco.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur l'appliance de sécurité adaptable Cisco (ASA).

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.

Informations générales

Quelques clients pourraient rencontrer un problème quand ils déploient d'abord une ASA ou quand ils testent la nouvelle Connectivité. Le problème est le débit de TCP pour les connexions qui traversent l'ASA sont beaucoup inférieure que quand l'ASA n'est pas dans le chemin de connexion (ou les connexions soyent beaucoup plus lent qu'avant que l'ASA ait été mise en application dans le réseau).

Par exemple, un client pourrait remplacer un routeur bas de gamme de D-lien (ou tout autre périphérique de routage) par une ASA 5505 ou une ASA 5510 ; cependant, une fois que le routeur est remplacé, la vitesse de connexion est considérablement réduite. Le client pourrait soulever un cas avec Cisco TAC parce qu'ils croient que l'ASA a entraîné la réduction de la vitesse de connexion.

Les informations de caractéristique

Dépannage de la méthodologie

Les écoulements de TCP ralentissent quand il y a retard de perte de paquets ou de paquet sur le réseau. Afin de comprendre la cause précise du problème, les données doivent afficher les paquets TCP réels sur le fil pour cette connexion et comment le réseau pourrait les affecter. Habituellement un administrateur réseau est alerté au problème quand ils exécutent une action spécifique, telle qu'un transfert de fichiers de FTP ou un test de vitesse en ligne. Le plus souvent le problème peut être reproduit. Par conséquent, l'administrateur peut recueillir les données priées afin de trouver la cause principale.

Afin de recueillir les données exigées, la commande de **tech d'exposition** devrait être exécutée de l'ASA avant et après le test. La configuration de cette commande montre et les statistiques de paquet (principalement du **show service-policy**) et affiche également si les erreurs d'interface incrémentent.

Des captures bidirectionnelles et simultanées de paquet (prises des deux interfaces ASA affectées que les traversées de connexion) sont requises de diagnostiquer entièrement la cause de la question.

Référez-vous à ces documents pour des exemples de la façon appliquer des captures de paquet à l'ASA :

- [Dépannage des connexions via PIX et ASA](#)
- [Épisode #1 de podcast de Sécurité TAC - Utilisant l'utilitaire de capture de paquet ASA pour le dépannage](#)

Analyse de données

Une fois que vous recueillez les données priées, vous pouvez utiliser les captures de paquet afin de déterminer lesquelles de ces questions pourraient s'être produites :

- Les paquets de l'hôte d'extérieur sont lâchés ou retardés avant qu'ils atteignent les ASA en dehors de l'interface.
- Les paquets sont retardés ou lâchés par l'ASA.
- Les paquets sont retardés ou lâchés quelque part sur le réseau intérieur.

Remarque: Cette analyse suppose que les données sont envoyées d'un hôte sur l'interface extérieure à un hôte sur l'interface interne.

Ce vidéo affiche un exemple de la façon exécuter l'analyse sur une capture de paquet :

Le flot de TCP fusionnant est une particularité technique de considération à ce problème parce que, quand vous engagez certaines caractéristiques sur l'ASA, le Pare-feu fusionne entièrement le flot de TCP qui le traverse.

Par exemple, si l'ASA découvre un paquet manquant sur le réseau (puisque'elle n'est pas reçue à l'ASA), il envoie un ACK au nom de l'autre point final de TCP pour les données manquantes. Ce scénario est le plus commun. Si l'ASA découvre les paquets qui arrivent en panne, l'ASA commande à nouveau les paquets et les passe au récepteur dans la commande appropriée. S'il n'y a aucune baisse ou paquet de réseau commandant à nouveau, il n'y a aucun effets

secondaires à activer cette caractéristique. Si tous les paquets envoyés par l'un ou l'autre de point final de TCP traversaient avec succès le réseau et l'ASA, vous ne sauriez pas que cette caractéristique est activée puisqu'elle n'agit pas sur les écoulements de paquet. Seulement quand il y a le problème avec la connexion TCP sur le réseau permettant à cette caractéristique plus loin de ralentir le trafic réseau. L'acte de la fusion le flot de TCP est très ressource intensive pour l'ASA. Pour chaque paquet relâché sur le réseau l'ASA doit non seulement envoyer à une demande de paquet TCP la retransmission de ce paquet, mais elle doit également mettre en mémoire tampon les paquets que l'expéditeur a continué à envoyer après que le paquet ait disparu des disparus.

Problèmes courants

Valeurs Misconfigured de la vitesse et le duplex sur l'interface qui connecte l'ASA au périphérique contigu

Cette question se produit souvent quand un périphérique est remplacé par une ASA. Si les valeurs de la vitesse et le duplex sur l'interface ASA ne sont pas identiques que les valeurs sur le périphérique contigu, les pertes de paquets se produisent sur cette interface. Vérifiez les valeurs de la vitesse et le duplex sur l'interface ASA aussi bien que l'interface adjacente.

Vérifiez la **sortie d'interface d'exposition de l'ASA** pour les erreurs évidentes qui sont des symptômes de ce problème :

```
Interface Ethernet0/0 "Outside", is up, line protocol is up
Hardware is i82546GB rev03, BW 100 Mbps
Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
MAC address 0019.2f58.c324, MTU 1500
IP address 192.168.222.122, subnet mask 255.255.255.252
124047996 packets input, 35340918453 bytes, 0 no buffer
Received 3 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
156918660 packets output, 40931551514 bytes, 0 underruns
1 output errors, 4286634 collisions, 0 interface resets
0 babbles, 123332 late collisions, 4752834 deferred
0 lost carrier, 0 no carrier
input queue (curr/max blocks): hardware (0/0) software (0/0)
output queue (curr/max blocks): hardware (0/245) software (0/0)
Traffic Statistics for "Outside":
124047995 packets input, 33107957301 bytes
157041993 packets output, 38195084709 bytes
103480 packets dropped
1 minute input rate 2140 pkts/sec, 477200 bytes/sec
1 minute output rate 2630 pkts/sec, 396763 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 2152 pkts/sec, 525496 bytes/sec
5 minute output rate 2701 pkts/sec, 421215 bytes/sec
5 minute drop rate, 0 pkts/sec
```

Envoyez le trafic au module IPS

Quand l'ASA est configurée pour envoyer le trafic au module IPS, la caractéristique de fusion de flot de TCP est engagée sur l'ASA. Référez-vous à la section d'*analyse de données de ce document* pour plus d'informations sur la caractéristique de fusion de flot de TCP.

La modification ASA des causes d'option de TCP MSS traitent à la légère la diminution de représentation

Par défaut l'ASA place l'option de TCP MSS dans les paquets de synchronisation à 1380. Par conséquent, les points finaux de TCP ne devraient pas transmettre des que 1380 octets plus grands d'un segment de TCP. Cette valeur est inférieure souvent à la valeur par défaut de 1460 octets et représente une chute de performances de TCP d'environ six pour cent (6%). La représentation pourrait s'améliorer est vous augmentation la configuration du maximum MSS sur l'ASA ou désactiver le réglage MSS. Avant que vous modifiez la commande par défaut sur l'ASA, comprenez les risques impliqués en ce qui concerne la fragmentation potentielle si le paquet est encore encapsulé dans le chemin quelque part.

Le pour en savoir plus, se rapportent à la section de [tcpmss de connexion de sysopt de la référence de commandes de gamme de Cisco ASA 5500](#).

FORUM AUX QUESTIONS

Informations connexes

- [Référence de commandes de gamme de Cisco ASA 5500, 8.2](#)
- [Support et documentation techniques - Cisco Systems](#)