

Débit ASA et vitesse de connexion Dépannage et analyse des captures de paquets

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Méthodologie de dépannage](#)

[Analyse des données](#)

[Problèmes courants](#)

[Valeurs de vitesse et de duplex mal configurées sur l'interface qui connecte ASA à un périphérique adjacent](#)

[Envoyer le trafic au module IPS](#)

[La modification ASA de l'option TCP MSS entraîne une légère diminution des performances](#)

[Informations connexes](#)

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.

Components Used

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. 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.

Informations générales

Certains clients peuvent rencontrer un problème lorsqu'ils déploient un ASA pour la première fois ou lorsqu'ils testent une nouvelle connectivité. Le problème est que le débit TCP pour les connexions qui traversent l'ASA est beaucoup plus faible que lorsque l'ASA n'est pas dans le

chemin de connexion (ou que les connexions sont beaucoup plus lentes qu'avant l'implémentation de l'ASA dans le réseau).

Par exemple, un client peut remplacer un routeur D-Link bas de gamme (ou un autre périphérique de routage) par un ASA 5505 ou un ASA 5510 ; cependant, une fois le routeur remplacé, la vitesse de connexion est considérablement réduite. Le client peut soulever un cas auprès du centre d'assistance technique Cisco car il pense que l'ASA a entraîné une réduction de la vitesse de connexion.

Méthodologie de dépannage

Les flux TCP ralentissent en cas de perte de paquets ou de retard de paquets sur le réseau. Afin de comprendre la cause exacte du problème, les données doivent montrer les paquets TCP réels sur le câble pour cette connexion et comment le réseau peut les affecter. Généralement, un administrateur réseau est averti du problème lorsqu'il effectue une action spécifique, telle qu'un transfert de fichiers FTP ou un test de vitesse en ligne. Le plus souvent, le problème peut être reproduit. Par conséquent, l'administrateur peut collecter les données requises afin de trouver la cause racine.

Afin de collecter les données requises, la commande **show tech** doit être exécutée à partir de l'ASA avant et après le test. Cette commande affiche les statistiques de configuration et de paquets (principalement à partir de **show service-policy**) et indique également si les erreurs d'interface s'incrémentent.

Des captures de paquets simultanées bidirectionnelles (prises à partir des deux interfaces ASA affectées par la connexion) sont nécessaires pour diagnostiquer complètement la cause du problème.

Reportez-vous à ces documents pour obtenir des exemples d'application de captures de paquets à l'ASA :

- [Dépannage des connexions via PIX et ASA](#)
- [Épisode 1 du podcast de sécurité TAC - Utilisation de l'utilitaire de capture de paquets ASA pour le dépannage](#)

Analyse des données

Une fois que vous avez rassemblé les données requises, vous pouvez utiliser les captures de paquets afin de déterminer lequel de ces problèmes pourrait s'être produit :

- Les paquets de l'hôte externe sont abandonnés ou retardés avant d'atteindre l'interface externe de l'ASA.
- Les paquets sont retardés ou abandonnés par l'ASA.
- Les paquets sont retardés ou abandonnés quelque part sur le réseau interne.

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

Cette vidéo présente un exemple d'analyse sur une capture de paquets :

La fusion de flux TCP est une considération technique spécifique à ce problème car, lorsque vous engagez certaines fonctions sur l'ASA, le pare-feu fusionne entièrement le flux TCP qui le traverse.

Par exemple, si l'ASA découvre un paquet manquant sur le réseau (puisque'il n'est pas reçu à l'ASA), il envoie un ACK au nom de l'autre point de terminaison TCP pour les données manquantes. Ce scénario est le plus courant. Si l'ASA découvre des paquets qui arrivent dans le désordre, l'ASA réorganise les paquets et les transmet au récepteur dans le bon ordre. S'il n'y a pas de perte de réseau ou de réorganisation de paquets, il n'y a aucun effet secondaire à activer cette fonctionnalité. Si tous les paquets envoyés par l'un ou l'autre des points de terminaison TCP ont réussi à traverser le réseau et l'ASA, vous ne saurez pas que cette fonctionnalité est activée car elle n'agit pas sur les flux de paquets. Ce n'est que lorsqu'il y a des problèmes avec la connexion TCP sur le réseau que l'activation de cette fonctionnalité ralentira davantage le trafic réseau. L'association du flux TCP nécessite beaucoup de ressources pour l'ASA. Pour chaque paquet déposé sur le réseau, l'ASA doit non seulement envoyer une requête de paquet TCP pour la retransmission de ce paquet, mais il doit également mettre en mémoire tampon les paquets que l'expéditeur a continué d'envoyer après que le paquet a disparu.

Problèmes courants

Valeurs de vitesse et de duplex mal configurées sur l'interface qui connecte ASA à un périphérique adjacent

Ce problème se produit souvent lorsqu'un périphérique est remplacé par un ASA. Si les valeurs de vitesse et de duplex sur l'interface ASA ne sont pas identiques aux valeurs sur le périphérique adjacent, des pertes de paquets se produisent sur cette interface. Vérifiez les valeurs de vitesse et de duplex sur l'interface ASA ainsi que sur l'interface adjacente.

Vérifiez la sortie **show interface** de l'ASA pour les erreurs évidentes qui sont les 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

Envoyer le trafic au module IPS

Lorsque l'ASA est configuré pour envoyer le trafic au module IPS, la fonctionnalité de regroupement de flux TCP est activée sur l'ASA. Reportez-vous à la section *Analyse des données* de ce document pour plus d'informations sur la fonctionnalité de regroupement de flux TCP.

La modification ASA de l'option TCP MSS entraîne une légère diminution des performances

Par défaut, l'ASA définit l'option TCP MSS dans les paquets SYN sur 1380. Par conséquent, les terminaux TCP ne doivent pas transmettre un segment TCP de plus de 1 380 octets. Cette valeur est inférieure à la valeur souvent par défaut de 1 460 octets et représente une baisse des performances TCP d'environ 6 % (6 %). Les performances peuvent s'améliorer si vous augmentez le paramètre MSS maximum sur l'ASA ou désactivez le réglage MSS. Avant de modifier la commande par défaut sur l'ASA, comprenez les risques liés à la fragmentation potentielle si le paquet est encapsulé dans le chemin d'accès quelque part.

Pour plus d'informations, référez-vous à la section [sysopt connection tcpmss](#) du *Guide de référence des commandes de la gamme Cisco ASA 5500*.

Informations connexes

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