Dépannez les erreurs de compteur de dépassement de capacité d'interface ASA

Contenu

Introduction

Ce document décrit le compteur d'erreurs de « dépassement de capacité » et comment étudier des problèmes de performance ou des problèmes de perte de paquets sur le réseau. Un administrateur pourrait noter des erreurs signalées dans la **commande d'interface d'exposition** sortie sur l'appliance de sécurité adaptable (ASA).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

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.

Problème

Le compteur d'erreurs d'interface ASA « débordent » dépiste le nombre de fois qu'un paquet a été reçues sur l'interface réseau, mais il n'y avait aucun espace disponible dans la file d'attente FIFO d'interface pour enregistrer le paquet. Ainsi, le paquet a été lâché. La valeur de ce compteur peut être vue avec la **commande d'interface d'exposition**.

Exemple de sortie qui affiche le problème :

```
ASA# show interface GigabitEthernet0/1
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
Full-Duplex(Full-duplex), 1000 Mbps(1000 Mbps)
Input flow control is unsupported, output flow control is off
MAC address 0026.0b31.0c59, MTU 1500
IP address 10.0.0.113, subnet mask 255.255.0.0
580757 packets input, 86470156 bytes, 0 no buffer
Received 3713 broadcasts, 0 runts, 0 giants
2881 input errors, 0 CRC, 0 frame, 2881 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
905828 packets output, 1131702216 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops, 0 tx hangs
input queue (blocks free curr/low): hardware (255/230)
output queue (blocks free curr/low): hardware (255/202)
```

Dans l'exemple ci-dessus, on a observé 2881 dépassements de capacité sur l'interface puisque l'ASA initialisée ou puisque le **clear interface de** commande a été écrit afin d'effacer les compteurs manuellement.

Causes des dépassements de capacité d'interface

Des erreurs de dépassement de capacité d'interface sont habituellement provoquées par une combinaison de ces facteurs :

- Logiciel de niveau - Le logiciel ASA ne retire pas les paquets de la file d'attente FIFO d'interface assez rapide. Ceci fait remplir la file d'attente FIFO et de nouveaux paquets à relâcher.
- Niveau matériel - La vitesse à laquelle les paquets entrent dans l'interface est trop rapide, qui fait remplir la file d'attente FIFO avant que le logiciel ASA puisse retirer les paquets. Habituellement, une rafale des paquets fait remplir la file d'attente FIFO jusqu'à la capacité maximale dans peu d'heure.

Les étapes pour dépanner la cause de l'interface déborde

Les étapes pour dépanner et aborder ce problème sont :

1. Déterminez si l'ASA éprouve des porcs CPU et s'ils contribuent au problème. Travaillez pour atténuer tous les longs ou fréquents porcs CPU.
2. Comprenez les débits de trafic d'interface et déterminez si l'ASA est due oversubscribed au profil du trafic.
3. Déterminez si les rafales intermittentes du trafic posent le problème. Si oui, implémentez le contrôle de flux sur l'interface ASA et les switchports adjacents.

Causes et solutions de potentiel

La CPU sur l'ASA est périodiquement trop occupée pour traiter des paquets entrant (les porcs CPU)

La plate-forme ASA traite tous les paquets en logiciel et utilise les cores du CPU principaux qui manipulent toutes les fonctions système (telles que des Syslog, la Connectivité d'Adaptive Security Device Manager, et l'inspection d'application) afin de traiter des paquets entrant. Si un processus de logiciel tient la CPU pour plus long qu'il devrait, l'ASA enregistre ceci comme événement de porc CPU puisque le processus « a accaparé » la CPU. Le seuil de porc CPU est placé en quelques millisecondes, et est différent pour chaque modèle d'appareils de matériel. Le seuil est basé sur combien de temps il pourrait prendre pour remplir file d'attente FIFO d'interface donnée la puissance CPU de la plate-forme matérielle et les débits de trafic potentiels le périphérique peuvent manipuler.

Les porcs CPU font parfois déborder l'interface des erreurs sur les ASA à un noyau, telles que les 5505, les 5510, les 5520, les 5540, et les 5550. Les longs porcs, cela durent pendant 100 millisecondes ou plus, peuvent particulièrement faire produire des dépassements de capacité pour les niveaux relativement à faible trafic et les débits de trafic non-bursty. Le problème n'affecte pas les systèmes multinucléaires autant, puisque d'autres noyaux peuvent retirer des paquets d'une sonnerie de Rx si un des cores du CPU est accaparé par un processus.

Un porc qui dure plus que le seuil de périphérique cause un Syslog d'être généré avec l'id 711004, comme affiché ici :

```
6 février 2013 14:40:42 : %ASA-4-711004 : La tâche a fonctionné pour 60 millisecondes, processus
= ssh, PC = 90b0155, pile des appels = le 6 février 2013 14:40:42 : %ASA-4-711004 : La tâche a
fonctionné pour 60 millisecondes, processus = ssh, PC = 90b0155, pile des appels = 0x090b0155
0x090bf3b6 0x090b3b84 0x090b3f6e 0x090b4459 0x090b44d6 0x08c46fcc 0x09860ca0 0x080fad6d
0x080efa5a 0x080f0a1c 0x0806922c
```

Des événements de porc CPU sont également enregistrés par le système. La sortie de la commande de CPU-**porc de show proc** affiche ces champs :

- Processus - le nom du processus qui a accaparé la CPU.
- PROC_PC_TOTAL - le nombre total de périodes que ce processus a accaparé la CPU.
- MAXHOG - le plus long temps de porc CPU observé pour ce processus, en quelques millisecondes.
- LASTHOG - la durée le dernier porc a tenu la CPU, en quelques millisecondes.
- LASTHOG lorsque le porc CPU s'est pour la dernière fois produit.
- PC - la valeur du compteur du programme du processus quand le porc CPU s'est produit. (Les informations pour le centre d'assistance technique Cisco (TAC))
- Pile des appels - la pile des appels du processus quand le porc CPU s'est produit. (Les informations pour Cisco TAC)

Cet exemple affiche la sortie de commande de CPU-**porc de show proc** :

```
ASA# show proc cpu-hog

Process:    ssh, PROC_PC_TOTAL: 1, MAXHOG: 119, LASTHOG: 119
LASTHOG At: 12:25:33 EST Jun 6 2012
PC:         0x08e7b225 (suspend)
```

```
Process:    ssh, NUMHOG: 1, MAXHOG: 119, LASTHOG: 119
LASTHOG At: 12:25:33 EST Jun 6 2012
PC:         0x08e7b225 (suspend)
Call stack: 0x08e7b225 0x08e8a106 0x08e7ebf4 0x08e7efde 0x08e7f4c9 0x08e7f546 0x08a7789c
            0x095a3f60 0x080e7e3d 0x080dcfa2 0x080ddf5c 0x0806897c

CPU hog threshold (msec): 10.240
Last cleared: 12:25:28 EST Jun 6 2012
ASA#
```

Le processus de SSH ASA a tenu la CPU pour 119ms sur le juin 2012 est de 12:25:33 6èmes.

Si les erreurs de dépassement de capacité augmentent continuellement sur une interface, vérifiez la sortie de la commande de CPU-**porc de show proc** afin de voir si corrélation d'événements de porc CPU avec une augmentation dans le compteur de dépassement de capacité d'interface. Si vous constatez que les porcs CPU contribuent à l'interface déborde des erreurs, il est le meilleur de rechercher des bogues avec le Bug Toolkit, ou soulevez un cas avec Cisco TAC. La sortie de la commande de **show tech-support** inclut également la sortie de commande de CPU-**porc de show proc**.

Le trafic Oversubscribes périodiquement traité par profil l'ASA

La personne à charge au moment sur le profil du trafic, le trafic qui traverse l'ASA pourrait être trop pour qu'il manipule et des dépassements de capacité pourrait se produire.

Le profil du trafic se compose (entre d'autres aspects) :

- Longueur de paquet
- Intervalle de paquet (débit de paquets)
- Protocol - quelques paquets sont soumis à l'inspection d'application sur l'ASA et exigent le traitement que d'autres paquets

Ces caractéristiques ASA peuvent être utilisées afin d'identifier le profil du trafic sur l'ASA :

- NetFlow - l'ASA peut être configurée pour exporter des enregistrements de version 9 de NetFlow vers un collecteur de NetFlow. Ces données peuvent alors être analysées pour comprendre plus au sujet du profil du trafic.

- SNMP - utilisez la surveillance SNMP afin de dépister les débits de trafic d'interface ASA, CPU, vitesses de connexion, et débits de traduction. Les informations peuvent alors être analysées afin de comprendre la structure de trafic et comment elles changent au fil du temps. Essayez de déterminer s'il y a un pic dans les débits de trafic qui le corrèle à une augmentation aux dépassements de capacité, et la cause de ce pic du trafic. Il y a eu des cas dans le TAC où les périphériques sur le réseau se conduisent mal (en raison de la mauvaise configuration ou de l'infection par un virus) et génèrent une pléthore du trafic périodiquement.

Packet Burst intermittents Oversubscribe la file d'attente FIFO d'interface ASA

Une rafale des paquets qui arrivent sur le NIC pourrait faire devenir le FIFO rempli avant que la CPU puisse retirer les paquets de elle. Il n'y a pas habituellement beaucoup qui peut être fait afin de résoudre ce problème, mais il peut être atténué en employant QoS dans le réseau pour lisser les rafales du trafic, ou contrôle de flux sur l'ASA et les switchports adjacents.

Le contrôle de flux est une caractéristique qui permet à l'interface de l'ASA pour envoyer un message au périphérique contigu (un switchport par exemple) afin de lui demander pour cesser d'envoyer le trafic pendant peu d'heure. Il fait ceci quand le FIFO atteint un certain seuil supérieur.

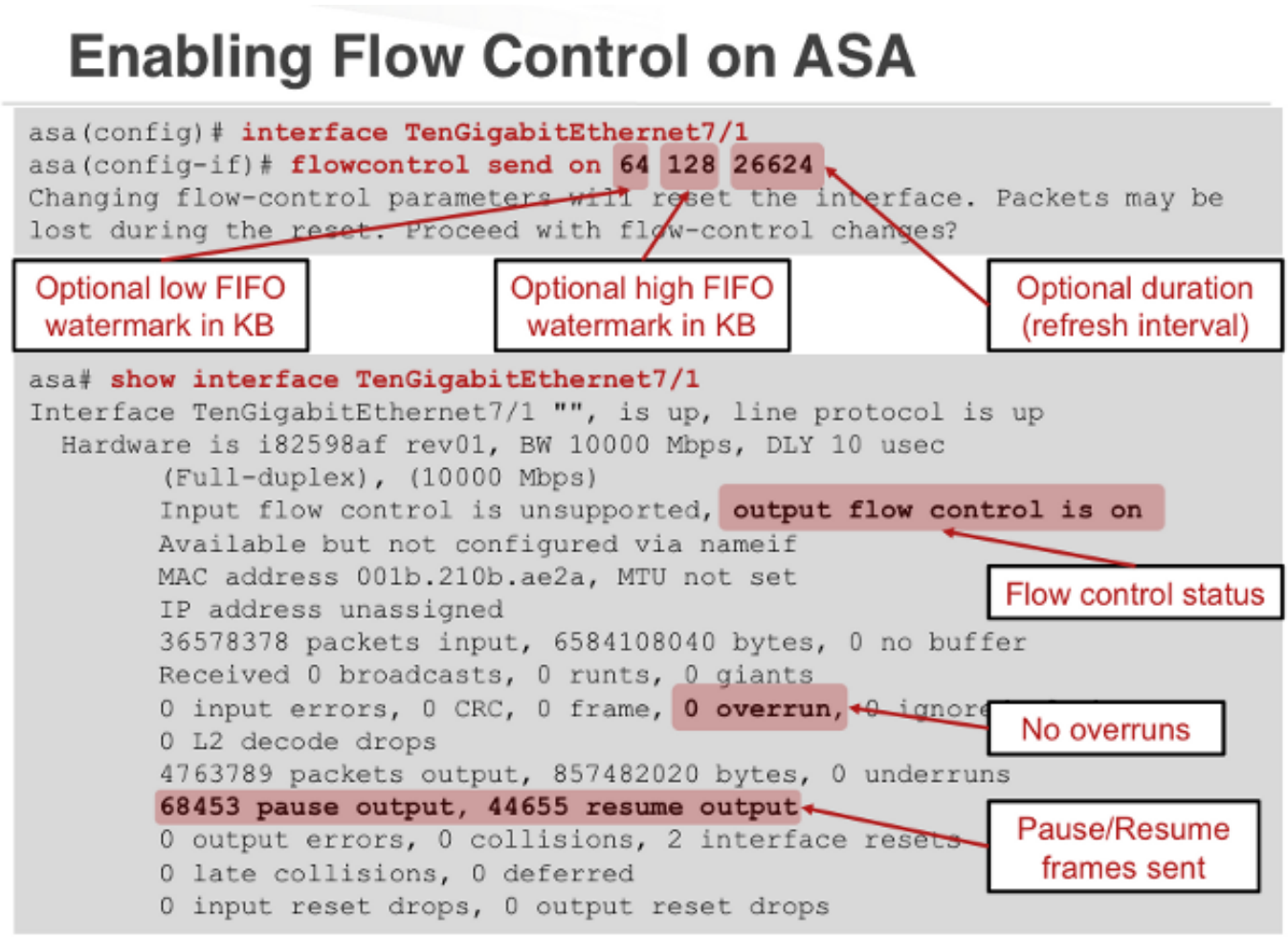
Une fois que le FIFO a été libéré vers le haut d'une certaine quantité, le NIC ASA envoie une trame de reprise, et le switchport continue à envoyer le trafic. Cette approche fonctionne bien parce que les switchports adjacents habituellement ont plus d'espace de mémoire tampon et peuvent faire de meilleurs paquets d'une mise en mémoire tampon du travail transmettent en fonction que l'ASA fait dans la direction de réception.

Vous pouvez essayer de permettre à des captures sur l'ASA de détecter les micro-rafales du trafic, mais habituellement ce n'est pas utile puisque les paquets sont lâchés avant qu'ils puissent obtenir traité par l'ASA et ajouté à la capture dans la mémoire. Un renifleur externe peut être utilisé pour capturer et identifier la rafale du trafic, mais parfois le renifleur externe peut être aussi bien accablé par la rafale.

Contrôle de flux d'enable pour atténuer des dépassements de capacité d'interface

La caractéristique de contrôle de flux a été ajoutée à l'ASA dans la version 8.2(2) et ultérieures pour les interfaces 10GE, et à la version 8.2(5) et ultérieures pour les interfaces 1GE. La capacité d'activer le contrôle de flux sur les interfaces ASA que l'expérience déborde s'avère être une technique efficace pour empêcher des occurrences de perte de paquets.

Référez-vous à la [caractéristique de contrôle de flux dans la référence de commandes de gamme de Cisco ASA 5500, 8.2] pour en savoir plus.



(Diagramme de présentation vivante BRKSEC-3021 de Cisco d'Andrew Ossipov)

Notez que le « contrôle de flux de sortie est sur » signifie que l'ASA envoie à des trames de pause de contrôle de flux l'interface ASA vers le périphérique contigu (le commutateur). Le « contrôle de

flux d'entrée est sans support » signifie que l'ASA ne prend en charge pas la *réception des* trames de contrôle de flux du périphérique contigu.

Configuration d'échantillon de contrôle de flux :

```
interface GigabitEthernet0/2
 flowcontrol send on
 nameif DMZ interface
 security-level 50
 ip address 10.1.3.2 255.255.255.0
!
```

Informations connexes

- ASA 8.3 et plus tard : Surveiller et dépanner les problèmes de performance
- Présentation vivante de Cisco « maximisant la représentation de Pare-feu » - cette présentation trace les grandes lignes de l'architecture des diverses Plateformes ASA, et inclut des informations sur la représentation et l'accord. Pour l'accès à cette présentation, la procédure de connexion à Ciscolive!365 et recherchent le nombre BRKSEC-3021 de présentation.
- Épisode #7 « représentation de podcast de Sécurité de Cisco TAC de Pare-feu de surveillance » - cet épisode de podcast comporte un examen des techniques et des méthodes pour surveiller la représentation de Pare-feu et pour identifier des problèmes de performances.
- Support et documentation techniques - Cisco Systems