Dépannage des erreurs de compteur de dépassement d'interface ASA

Contenu

Introduction

Ce document décrit le compteur d'erreurs « overrun » et comment étudier les problèmes de performances ou de perte de paquets sur le réseau. Un administrateur peut remarquer des erreurs signalées dans la sortie de la commande **show interface** sur l'appliance de sécurité adaptatif (ASA).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. 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.

Problème

Le compteur d'erreurs de l'interface ASA « overrun » suit le nombre de fois où un paquet a été

reçu sur l'interface réseau, mais il n'y avait pas d'espace disponible dans la file d'attente FIFO de l'interface pour stocker le paquet. Ainsi, le paquet a été abandonné. La valeur de ce compteur peut être vue à l'aide de la commande **show interface**.

Exemple de résultat 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, 2881 dépassements ont été observés sur l'interface depuis le démarrage de l'ASA ou depuis la commande **clear interface** a été entrée afin d'effacer les compteurs manuellement.

Causes des dépassements d'interface

Les erreurs de dépassement d'interface sont généralement causées par une combinaison de ces facteurs :

- Niveau logiciel : le logiciel ASA ne retire pas les paquets de la file d'attente FIFO de l'interface assez rapidement. Cela entraîne le remplissage de la file d'attente FIFO et l'abandon de nouveaux paquets.
- Niveau matériel : le débit auquel les paquets entrent dans l'interface est trop rapide, ce qui entraîne le remplissage de la file d'attente FIFO avant que le logiciel ASA puisse retirer les paquets. Généralement, une rafale de paquets entraîne le remplissage de la file d'attente FIFO jusqu'à la capacité maximale en peu de temps.

Étapes de dépannage de la cause des dépassements d'interface

Les étapes de dépannage et de résolution de ce problème sont les suivantes :

1. Déterminez si l'ASA rencontre des problèmes de CPU et s'ils contribuent au problème. Travaillez pour atténuer les problèmes de bogues longs ou fréquents du processeur.
2. Comprendre les débits de trafic de l'interface et déterminer si l'ASA est sursouscrit en raison du profil de trafic.
3. Déterminez si les rafales de trafic intermittentes sont à l'origine du problème. Si c'est le cas, mettez en oeuvre le contrôle de flux sur l'interface ASA et les ports de commutation

adjacents.

Causes et solutions potentielles

Le processeur de l'ASA est périodiquement trop occupé pour traiter les paquets entrants (bogues du processeur)

La plate-forme ASA traite tous les paquets dans le logiciel et utilise les principaux coeurs de CPU qui gèrent toutes les fonctions système (comme les Syslogs, la connectivité Adaptive Security Device Manager et l'inspection des applications) afin de traiter les paquets entrants. Si un processus logiciel conserve le processeur plus longtemps qu'il ne le devrait, l'ASA l'enregistre en tant qu'événement de blocage du processeur depuis que le processus a bloqué le processeur. Le seuil de pagination du processeur est défini en millisecondes et est différent pour chaque modèle d'appliance matérielle. Le seuil est basé sur le temps qu'il peut falloir pour remplir la file d'attente FIFO de l'interface, compte tenu de la puissance CPU de la plate-forme matérielle et des débits de trafic potentiels que le périphérique peut gérer.

Les bogues de CPU provoquent parfois des erreurs de dépassement d'interface sur les ASA monocoeurs, tels que les 5505, 5510, 5520, 5540 et 5550. Les longs porcs, qui durent 100 millisecondes ou plus, peuvent particulièrement provoquer des dépassements de trafic pour des niveaux de trafic relativement bas et des débits de trafic non-rafales. Le problème n'a pas autant d'impact sur les systèmes multicoeurs, car d'autres coeurs peuvent retirer des paquets d'un anneau Rx si l'un des coeurs du processeur est bloqué par un processus.

Un porc qui dure plus que le seuil du périphérique provoque la génération d'un syslog avec l'id 711004, comme illustré ici :

```
06 février 2013 14:40:42 : %ASA-4-711004 : Tâche exécutée pendant 60 ms, Processus = ssh, PC =
90b0155, Pile d'appels = Fév 06 2013 14:40:42 : %ASA-4-711004 : Tâche exécutée pendant 60 ms,
Processus = ssh, PC = 90b0155, Pile d'appels = 0x090b0155 0x090bf3b6 0x090b3b84 0x090b3f6e
0x090b 4459 0x090b44d6 0x08c46fcc 0x09860ca0 0x080fad6d 0x080efa5a 0x080f0a1c 0x080692 2c
```

Les événements de porc du processeur sont également enregistrés par le système. La sortie de la commande **show proc cpu-hog** affiche les champs suivants :

- Process : nom du processus qui a bloqué le processeur.
- PROC_PC_TOTAL : nombre total de fois où ce processus a bloqué le processeur.
- MAXHOG : la plus longue durée de connexion du processeur observée pour ce processus, en millisecondes.
- LASTHOG : durée, en millisecondes, pendant laquelle le dernier porc a conservé le processeur.
- LASTHOG At - l'heure à laquelle le hog CPU s'est produit pour la dernière fois.
- PC : valeur du compteur de programme du processus lorsque le bogue du processeur s'est produit. (Informations pour le centre d'assistance technique Cisco (TAC))
- Pile d'appels : pile d'appels du processus lorsque le bogue du processeur s'est produit. (Informations pour le TAC Cisco)

Cet exemple montre la sortie de commande **show proc cpu-hog** :

```
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 SSH ASA a retenu le processeur pour 119 ms le 6 juin 2012 à 12:25:33 EST.

Si les erreurs de dépassement augmentent continuellement sur une interface, vérifiez la sortie de la commande **show proc cpu-hog** afin de voir si les événements de blocage du CPU sont corrélés à une augmentation du compteur de dépassement de l'interface. Si vous constatez que les bogues du CPU contribuent aux erreurs de dépassement de l'interface, il est préférable de rechercher des bogues avec le Bug Toolkit, ou de soumettre un cas au TAC de Cisco. La sortie de la commande **show tech-support** inclut également la sortie de la commande **show proc cpu-hog**.

Profil de trafic traité Sursouscription périodique de l'ASA

En fonction du profil de trafic, le trafic qui traverse l'ASA peut être trop important pour qu'il puisse le gérer et des dépassements peuvent se produire.

Le profil de trafic comprend (entre autres aspects) :

- Taille du paquet
- Écart entre paquets (débit de paquets)
- Protocole : certains paquets sont soumis à une inspection d'application sur l'ASA et nécessitent plus de traitement que d'autres paquets.

Ces fonctionnalités ASA peuvent être utilisées afin d'identifier le profil de trafic sur l'ASA :

- Netflow - l'ASA peut être configuré pour exporter des enregistrements NetFlow version 9 vers un collecteur NetFlow. Ces données peuvent ensuite être analysées pour mieux comprendre le profil de trafic.

- SNMP - utiliser la surveillance SNMP afin de suivre les débits de trafic de l'interface ASA, le CPU, les débits de connexion et les débits de traduction. Les informations peuvent ensuite être analysées afin de comprendre le modèle de trafic et comment il change au fil du temps. Essayez de déterminer s'il y a une hausse des débits qui est corrélée à une augmentation des dépassements, et la cause de cette hausse du trafic. Il y a eu des cas dans le centre d'assistance technique où les périphériques du réseau se comportent mal (en raison d'une mauvaise configuration ou d'une infection virale) et génèrent périodiquement un flux de trafic.

Les rafales de paquets intermittentes surabonnent à la file d'attente FIFO de l'interface ASA

Une rafale de paquets arrivant sur la carte réseau peut entraîner le remplissage de la FIFO avant

que le processeur puisse retirer les paquets. Il n'y a généralement pas grand-chose à faire pour résoudre ce problème, mais il peut être atténué par l'utilisation de la QoS dans le réseau pour lisser les rafales de trafic ou le contrôle de flux sur l'ASA et les ports de commutation adjacents.

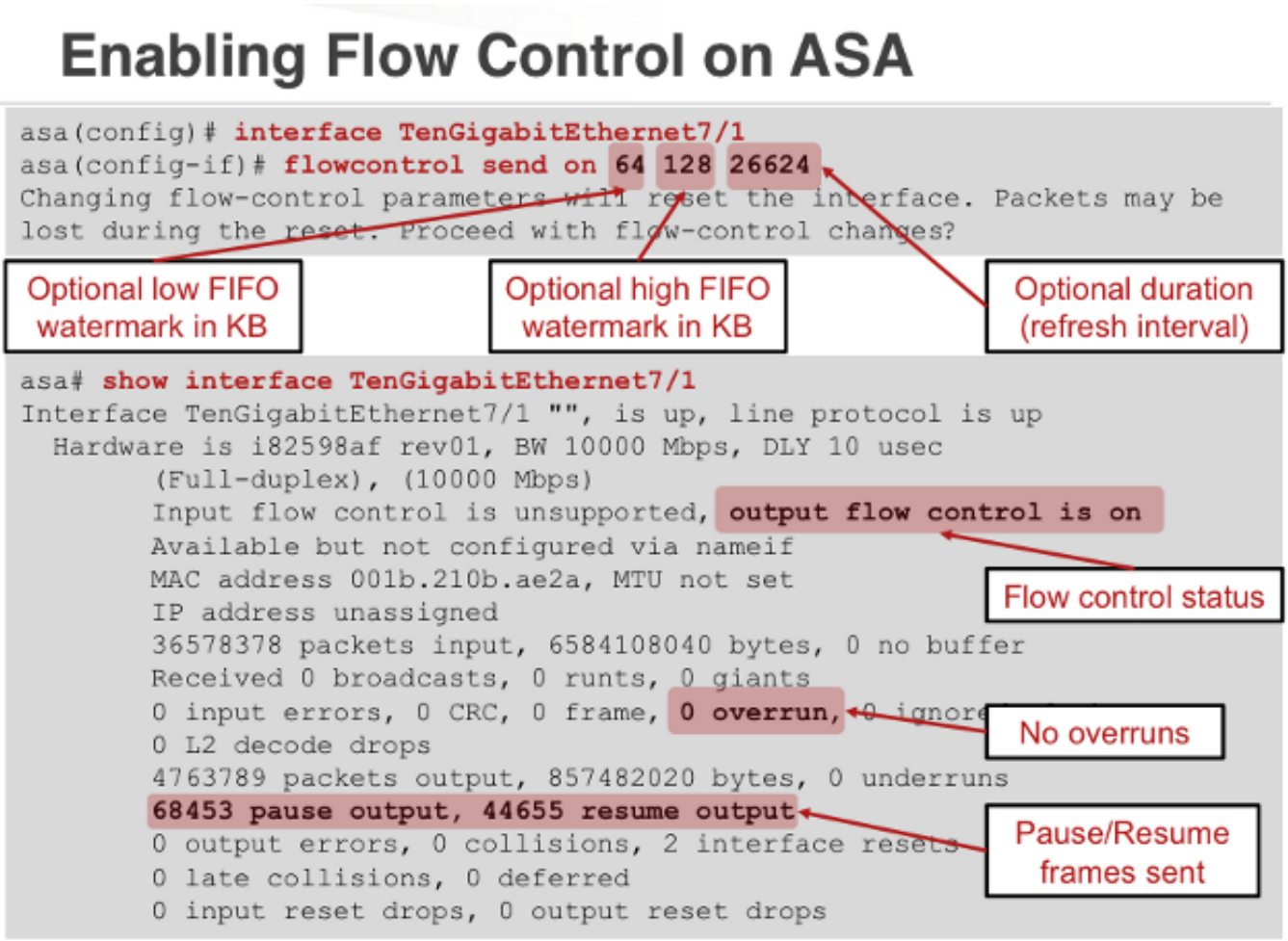
Le contrôle de flux est une fonctionnalité qui permet à l'interface de l'ASA d'envoyer un message au périphérique adjacent (un port de commutation par exemple) afin de lui demander d'arrêter d'envoyer du trafic pendant une courte durée. Il le fait quand la FIFO atteint une certaine limite d'eau. Une fois que la FIFO a été libérée, la carte réseau ASA envoie une trame de reprise et le port de commutateur continue à envoyer du trafic. Cette approche fonctionne bien parce que les ports de commutation adjacents ont généralement plus d'espace tampon et peuvent faire un meilleur travail de mise en mémoire tampon des paquets lors de la transmission que l'ASA dans la direction de réception.

Vous pouvez essayer d'activer les captures sur l'ASA pour détecter les micro-rafales de trafic, mais généralement cela n'est pas utile car les paquets sont abandonnés avant qu'ils puissent être traités par l'ASA et ajoutés à la capture dans la mémoire. Un analyseur externe peut être utilisé pour capturer et identifier le trafic en rafale, mais parfois, le renifleur externe peut également être submergé par la rafale.

Activer le contrôle de flux pour réduire les dépassements d'interface

La fonctionnalité de contrôle de flux a été ajoutée à l'ASA dans les versions 8.2(2) et ultérieures pour les interfaces 10GE, et dans les versions 8.2(5) et ultérieures pour les interfaces 1GE. La possibilité d'activer le contrôle de flux sur les interfaces ASA qui subissent des dépassements de capacité s'avère être une technique efficace pour empêcher les abandons de paquets.

Référez-vous à la fonctionnalité de contrôle de flux dans le Guide de référence des commandes de la gamme Cisco ASA 5500, 8.2 pour plus d'informations.



(Schéma de la présentation Cisco Live d'Andrew Ossipov BRKSEC-3021)

Notez que « output flow control is on » signifie que l'ASA envoie des trames de pause de contrôle de flux de l'interface ASA vers le périphérique adjacent (le commutateur). « Le contrôle de flux d'entrée n'est pas pris en charge » signifie que l'ASA ne prend pas en charge la *réception* des trames de contrôle de flux à partir du périphérique adjacent.

Exemple de configuration 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 versions ultérieures : Surveiller et dépanner les problèmes de performance]
- [Présentation Cisco Live « Optimiser les performances du pare-feu »] - Cette présentation décrit l'architecture des différentes plates-formes ASA et contient des informations sur les performances et le réglage. Pour accéder à cette présentation, connectez-vous à [CiscoLive]

!365 et recherchez le numéro de présentation BRKSEC-3021.
- Épisode 7 du podcast Cisco TAC Security intitulé Monitoring Firewall Performance - Cet épisode de podcast présente les techniques et les méthodes de surveillance des performances des pare-feu et d'identification des problèmes de performances.
- Support et documentation techniques - Cisco Systems