Dépannage de l'utilisation du CPU élevée dans le processus d'entrée IP

Contenu

Introduction

Ce document explique comment dépanner la surutilisation de la CPU due au processus d'entrée IP.

Remarque: Ce document ne fournit pas des stratégies pour empêcher différents types d'attaques.

Conditions préalables

Conditions requises

Cisco recommande que vous lisiez la section Dépannage de surutilisation de la CPU sur des routeurs Cisco avant que vous poursuiviez ce document.

Composants utilisés

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

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

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

IP Input

Le processus de logiciel de Cisco IOS® a appelé l'*entrée IP* prend soin des paquets IP de processus-commutation. Si le processus d'entrée IP utilise des ressources CPU exceptionnellement élevées, le routeur effectue beaucoup de commutations de processus de trafic IP. Vérifiez ces problèmes :

- **La commutation d'interruption est désactivée sur une interface (ou des interfaces) qui a (ont) beaucoup de trafic de routage**La commutation d'interruption se rapporte à l'utilisation d'algorithmes de commutation autres que la commutation de processus. Les exemples incluent la commutation rapide, optimum, Cisco Express Forwarding, etc. (consultez les Bases du paramétrage dans un but de performances pour des détails). Examinez le résultat de la commande **show interfaces switching** pour voir quelle interface est chargée de trafic. Vous pouvez vérifier la commande **show ip interface** pour voir quelle méthode de commutation est utilisée sur chaque interface. Réactivez la commutation d'interruption sur cette interface. Souvenez-vous que la commutation rapide normale est configurée sur des interfaces de sortie : si la commutation rapide est configurée sur une interface, les paquets qui sortent de cette interface sont commutés rapidement. La commutation de Cisco Express Forwarding est configurée sur des interfaces d'entrée. Pour créer des entrées de la table de routage de base d'informations de transfert (BOBARD) et de juxtaposition sur une interface particulière, configurez la commutation de Cisco Express Forwarding sur toutes les interfaces qui conduisent à cette interface.
- **La commutation rapide sur la même interface est désactivée**Si une interface a beaucoup d'adresses secondaires ou de sous-interfaces et qu'il y a beaucoup de trafic de routage originaire de l'interface destiné à une adresse de la même interface, la commutation de processus est effectuée sur tous ces paquets. Dans cette situation, vous devez activer ip route-cache same-interface sur l'interface. Quand la commutation de Cisco Express Forwarding est utilisée, vous n'avez pas besoin d'activer la commutation de Cisco Express Forwarding sur la même interface séparément.
- **La commutation rapide sur une interface fournissant le routage de politique est désactivée**Si une carte de routage a été configurée sur une interface, et que beaucoup de trafic de routage est traité par la carte de routage, le routeur effectue la commutation de processus de ce trafic. Dans cette situation, vous devez activer la politique ip route-cache policy sur l'interface. Vérifiez les restrictions mentionnées dans la section « en activant routage basé sur la politique à commutation rapide » de configurer le routage basé sur la politique.
- **Le trafic qui ne peut pas être commuté par interruption arrive**Il peut s'agir de n'importe quel type de trafic énuméré. Cliquez sur les éléments liés pour plus d'informations.Paquets pour lesquels il n'y a encore aucune entrée dans le cache de commutationMême si la commutation rapide, optimum ou Cisco Express Forwarding (CEF) est configurée, tout paquet pour lequel il n'y a aucune correspondance dans le cache à commutation rapide ou le FIB et les tables de contiguïté est traité. Une entrée est alors créée dans le cache ou la table approprié(e), et tous les paquets suivants qui correspondent aux mêmes critères sont rapides, optimum ou commutés par CEF. Dans des circonstances normales, ces paquets traités n'entraînent pas l'utilisation élevée de la CPU. Cependant, si un des périphériques du réseau 1) génère des paquets à un débit extrêmement haut pour des périphériques accessibles par le routeur, et 2) utilise différentes adresses IP source ou de destination, il n'y a alors pas de correspondance pour ces paquets dans le cache de commutation ou la table de routage, de sorte qu'ils sont traités par le processus d'entrée IP (si la Commutation Netflow est configurée, les ports TCP

source et de destination sont aussi vérifiés par rapport aux entrées de routage dans le cache de Netflow). Cet équipement d'origine peut être un périphérique non fonctionnel ou, plus probablement, un périphérique essayant une attaque.(*) Seulement avec juxtapositions glanées. Référez-vous à Cisco Express Forwarding pour plus d'informations sur des contiguïtés de Cisco Express Forwarding.Paquets destinés au routeurVoici des exemples de paquets destinés au routeur :Mises à jour de routage qui arrivent à un débit extrêmement haut. Si le routeur reçoit une énorme quantité de mises à jour du routage qui doivent être traitées, cette tâche pourrait surcharger la CPU. Normalement, ceci ne peut pas se produire dans un réseau stable. La façon dont vous pouvez recueillir plus d'informations dépend du protocole de routage vous avez configuré. **Cependant, vous pouvez commencer à vérifier le résultat de la commande de show ip route summary périodiquement.** Les valeurs qui changent rapidement sont un signe de réseau instable. Les changements fréquents dans la table de routage indiquent une augmentation du traitement de protocole de routage, qui a comme conséquence une utilisation accrue de la CPU. Pour plus d'informations sur la façon de dépanner ce problème, consultez la section Dépannage TCP/IP du Guide de dépannage d'interréseau.Tout autre type de trafic destiné au routeur. Contrôlez qui est connecté au routeur et aux actions de l'utilisateur. Si quelqu'un est connecté et émet des commandes qui produisent une longue sortie, l'utilisation élevée de la CPU par le processus d'« entrée d'IP » est suivie par une utilisation beaucoup plus élevée de la CPU par le processus EXEC virtuel.Attaque de détournement de trafic. **Pour identifier le problème, émettez la commande show ip traffic pour vérifier la quantité de trafic IP.** S'il y a un problème, le nombre de paquets reçus avec une destination locale est significatif. **Ensuite, examinez le résultat des commandes show interfaces et show interfaces switching pour vérifier sur quelle interface arrivent les paquets. Une fois que vous avez identifié l'interface réceptrice, activez l'ip accounting sur l'interface sortante et voyez s'il y a un motif.** S'il y a une attaque, l'adresse source est presque toujours différente, mais l'adresse de destination est identique. Une liste d'accès peut être configurée pour résoudre le problème temporairement (de préférence sur le périphérique le plus proche de la source des paquets), mais la véritable solution est de dépister l'équipement d'origine et d'arrêter l'attaque.Le trafic de diffusionVérifiez le nombre de paquets de diffusion dans le résultat de **show interfaces**. Si vous comparez la quantité de diffusions à la quantité totale de paquets qui ont été reçus sur l'interface, vous pouvez vous faire une idée de s'il y a une surcharge des diffusions. S'il y a un LAN avec plusieurs commutateurs connectés au routeur, ceci peut indiquer un problème de routage avec le spanning-tree.Paquets d'IP avec des optionsPaquets qui requièrent la conversion de protocoleProtocole Multilink Point-to-Point Protocol (pris en charge dans la commutation de Cisco Express Forwarding)Trafic compresséS'il n'y a aucun adaptateur de service de compression (CSA) dans le routeur, la commutation de processus doit être effectuée pour les paquets compressés.Le trafic chiffréS'il n'y a aucun adaptateur de service de chiffrement (ESA) dans le routeur, la commutation de processus doit être effectuée pour les paquets chiffrés.Paquets qui passent par des interfaces série avec l'encapsulation X.25Dans la suite de protocole X.25, le contrôle de flux est mis en application sur la deuxième couche d'Open System Interconnection (OSI).

- Beaucoup de paquets, arrivant à un débit extrêmement haut, pour une destination dans un sous-réseau directement attaché, pour lequel il n'y a aucune entrée dans la table de Protocole de résolution d'adresse (ARP). Ceci ne devrait pas se produire avec le trafic TCP en raison du mécanisme de fenêtrage, mais peut se produire avec le trafic de Protocole de datagramme utilisateur (UDP). Pour identifier le problème, répétez les actions suggérées afin de dépister une attaque de détournement de trafic.

- Beaucoup de trafic de multidiffusion passe par le routeur. Malheureusement, il n'y a aucune méthode simple d'examiner la quantité du trafic de multidiffusion. La commande show ip traffic montre seulement l'information résumée. Cependant, si vous avez configuré le routage de multicast sur le routeur, vous pouvez activer la commutation rapide des paquets de multidiffusion avec la commande de configuration d'interface ip mroute-cache (la commutation rapide des paquets de multidiffusion est désactivée par défaut).
- Le routeur est sursouscrit. Si le routeur est surutilisé et ne peut pas prendre en charge ce niveau de trafic, essayez de distribuer la charge entre d'autres routeurs ou achetez un routeur haut de gamme.
- Le routage de traduction d'adresse de réseau IP (NAT) est configuré sur le routeur, et bon nombre de paquets de Système de noms de domaine (DNS) passent par le routeur. Les paquets UDP ou TCP ayant comme port source ou de destination le port 53 (DNS) sont toujours dirigés vers le niveau de processus par NAT.
- Il y a d'autres types de paquets qui sont dirigés vers le traitement.
- Il y a de fragmentation de datagramme IP. Il y a une petite augmentation dans la CPU et mémoire au-dessus devant fragmenter d'un datagramme IP. Référez-vous à la fragmentation IP de résolution, aux questions de MTU, MSS, et PMTUD avec GRE et IPSEC pour plus d'informations sur la façon dépanner cette question.

Quelle que soit le motif de l'utilisation élevée du CPU dans le processus d'entrée IP, la source du problème peut être dépistée si vous déboguez les paquets d'IP. Puisque l'utilisation du microprocesseur est déjà élevée, le processus de débogage doit être exécuté avec une attention extrême. Le processus de débogage produit beaucoup de messages, de sorte que seulement logging buffered doit être configuré.

Le fait de consigner à une console provoque des interruptions inutiles à la CPU et augmente l'utilisation de la CPU. Le fait de consigner à un hôte (ou la journalisation de surveillance) génère un trafic supplémentaire sur des interfaces.

Le processus de débogage peut être commencé par la commande exec debug ip packet detail. Cette session ne doit pas durer plus long que trois à cinq secondes. Les messages de débogage sont écrits dans le tampon de journalisation. Une capture d'une session d'élimination des imperfections IP témoin est fournie dans le paquet IP d'échantillon mettant au point la section de session de ce document. Une fois que l'équipement d'origine des paquets non désirés d'IP est recherché, ce périphérique peut être déconnecté du réseau, ou une liste d'accès peut être créée sur le routeur pour déposer des paquets provenant de cette destination.

Session exemple de débogage de paquet IP

Les destinations de journalisation configurées doivent d'abord être vérifiées avec la commande **show logging** :

```
router#show logging Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns) Console
logging: level debugging, 52 messages logged Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 148 messages logged Trap logging: level informational, 64
message lines logged Logging to 192.168.100.100, 3 message lines logged Logging to
192.168.200.200, 3 message lines logged --More--
```

Désactivez toutes les destinations de journalisation excepté le tampon de journalisation, et effacez le tampon de journalisation :

```
router#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
router(config)#no logging console router(config)#no logging monitor router(config)#no logging
```

```
192.168.100.100 router(config)#no logging 192.168.200.200 router(config)#^Z router#clear logging
Clear logging buffer [confirm] router#
```

Pour une meilleure lisibilité de résultat du débogage, la date-heure et les horodatages avec millisecondes doivent être activés :

```
router#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
router(config)#service timestamps log datetime msec router(config)#service timestamps debug
datetime msec router(config)#end router#
```

Une session de débogage peut maintenant être lancée :

```
router#debug ip packet detail IP packet debugging is on (detailed)
```

Le débogage ne devrait pas durer plus de trois à cinq secondes. La session peut être arrêtée avec la commande exec **undebug all** :

```
router#undebug all All possible debugging has been turned off
```

Les résultats peuvent être vérifiés avec la commande exec **show logging** :

```
router#show logging Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns) Console
logging: disabled Monitor logging: disabled Buffer logging: level debugging, 145 messages logged
Trap logging: level informational, 61 message lines logged Log Buffer (64000 bytes): *Mar 3
03:43:27.320: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.204 (Ethernet0/0), g=10.200.40.1,
len 100, forward *Mar 3 03:43:27.324: ICMP type=8, code=0 *Mar 3 03:43:27.324: IP:
s=192.168.40.53 (Ethernet0/1), d=144.254.2.205 (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar 3 03:43:27.324: ICMP type=8, code=0 *Mar 3 03:43:27.328: IP: s=192.168.40.53 (Ethernet0/1),
d=144.254.2.206 (Ethernet0/0), g=10.200.40.1, len 100, forward *Mar 3 03:43:27.328: ICMP type=8,
code=0 ...
```

Le journal montre cela :

- Un paquet a été reçu toutes les quatre millisecondes
- L'adresse IP source est 192.168.40.53
- Les paquets sont arrivés sur l'interface Ethernet0/1
- Les paquets ont des adresses IP de destination différentes
- Les paquets ont été envoyés sur l'interface Ethernet0/0
- L'adresse IP de prochain-saut est 10.200.40.1
- Les paquets étaient des requêtes de routage d'ICMP (type=8)Dans cet exemple, vous pouvez voir que l'utilisation élevée de la CPU dans le processus d'entrée IP a été entraînée par une inondation de ping de l'adresse IP 192.168.40.53.Les inondations SYN peuvent facilement être détectées de cette façon parce que la présence d'indicateur de synchronisation est indiquée dans le résultat du débogage :
```
*Mar 3 03:54:40.436: IP: s=192.168.40.53
(Ethernet0/1), d=144.254.2.204
   (Ethernet0/0), g=10.200.40.1, len 44, forward
*Mar 3 03:54:40.440: TCP src=11004, dst=53,
   seq=280872555, ack=0, win=4128 SYN
```

Informations connexes

- Dépannage de l'utilisation élevée du CPU sur les routeurs Cisco
- La commande show processes
- Utilisation élevée du processeur sur les commutateurs Catalyst 2900XL/3500XL
- Notions de base de l'optimisation des performances
- Support et documentation techniques - Cisco Systems