Protection de surcharge de mise en place pour des passerelles et des éléments de réseau voisins sur la gamme ASR5x00

Contenu

Introduction

Ce document décrit comment mettre en application les caractéristiques de protection qui sont disponibles pour des passerelles (GWs) et des éléments de réseau voisins sur la gamme 5x00 du routeur de services agrégée par Cisco (ASR) afin de protéger la performance du réseau globale.

Contrôle d'encombrement pour GWs

Le contrôle d'encombrement est une caractéristique générique d'autoprotection. Il est utilisé afin de protéger le système contre des surtensions d'utilisation de ces ressources :

- Utilisation du CPU sur traiter des cartes
- Utilisation de mémoire sur traiter des cartes

Quand l'utilisation dépasse les seuils prédéfinis, tous les nouveaux appels des lancements de Protocol de données de paquets ((PDP), des lancements de session de réseau informatique de données de paquets (PDN)) *sont abandonnés* ou *rejetés*, dépendant sur la configuration.

Voici un exemple qui affiche comment surveiller l'utilisation globale de la carte perforée (DPC) :

```
congestion-control threshold system-cpu-utilization 85
```

```
congestion-control threshold system-memory-utilization 85

congestion-control policy ggsn-service action drop

congestion-control policy sgw-service action drop

congestion-control policy pgw-service action drop
```

> Remarque: La limite de technicien système est 80% de l'utilisation du processeur, qui est définie comme limite de construction recommandée qui ne devrait pas être dépassée afin de garantir l'exécution régulière du système. Le chargement au delà de la valeur pourrait affecter des fonctionnements de la plate-forme, tels que sa stabilité et prévisibilité, et devrait être évité avec la planification de capacité appropriée.

> Remarque: Cisco recommande que vous utilisiez l'action de *baisse* plutôt que l'action d'*anomalie*, comme les tentatives répétées immédiates rejetées de reconnexion de cause d'appels de l'équipement de l'utilisateur (UE). Dans le cas d'une action de baisse, l'UE attend quelques secondes avant qu'il fasse des tentatives répétées de reconnexion, ainsi le débit d'appel est diminué.

Protection de surcharge de réseau pour l'étranglement de message du d'entrée GTP-C

Cette caractéristique protège le paquet le gw (P-GW) /Gateway GPRS prenant en charge des processus du noeud (GGSN) contre des surtensions de transmission et des pannes d'élément de réseau. Dans un P-GW/GPRS servant prenant en charge le noeud (SGSN), l'étranglement principal est lié au traitement de données d'utilisateur, tel que l'utilisation de gestionnaire de session et l'utilisation globale de CPU et mémoire DPC.

Une aucune valeur n'est configurée sur l'entité de Gestion SGSN/Mobility (MME.) afin d'étrangler les messages d'arrivée du Protocol-Control de perçage d'un tunnel GPRS (GTP-C) quand la protection de surcharge de réseau est lancée.

> Remarque: L'utilisation de GTP et de l'étranglement d'interface de diamètre exige qu'une clé de licence valide soit installée.

Cette caractéristique aide le contrôle le débit de messages d'arrivée/sortants sur le P-GW/GGSN, qui aide à s'assurer que le P-GW/GGSN n'est pas accablé par les messages de plan de contrôle GTP. En outre, il aide à s'assurer que le P-GW/GGSN n'accable pas le pair GTP-C avec les messages d'avion de contrôle GTP. Cette caractéristique exige que le GTP (version 1 (v1) et version 2 (v2)) contrôlez les messages soit formé/maintenu l'ordre au-dessus des interfaces Gn/Gp et S5/S8. Cette caractéristique couvre la protection de surcharge des Noeuds P-GW/GGSN et des autres Noeuds externes avec lesquels elle communique. L'étranglement est fait seulement pour les messages niveau de la session de contrôle, ainsi les messages de gestion de chemin ne sont pas débit limité du tout.

La surcharge externe de noeud peut se produire dans un scénario où le P-GW/GGSN génère des demandes de signalisation à un débit supérieur que les autres Noeuds peuvent manipuler. En outre, si le débit d'arrivée est élevé au noeud P-GW/GGSN, il pourrait inonder le noeud externe. Pour cette raison, l'étranglement des messages d'arrivée et sortants de contrôle est exigé. Pour la

protection des Noeuds externes contre une surcharge due au P-GW/GGSN contrôlez la signalisation, un cadre est utilisé afin de former et maintenir l'ordre les messages sortants de contrôle aux interfaces externes.

Configurez l'étranglement de message du d'entrée GTP-C

Sélectionnez cette commande afin de configurer l'étranglement de message du d'entrée GTP-C :

gtpc overload-protection Ingress

Ceci configure la protection de surcharge du GGSN/PGW en étranglant des messages du contrôle GTPv1 et GTPv2 d'arrivée au-dessus de l'interface Gn/Gp (GTPv1) ou S5/S8 (GTPv2) avec les autres paramètres pour les services qui sont configurés dans un contexte et appliqués au GGSN et au PGW.

Quand vous sélectionnez la commande précédente, cette demande est générée :

```
[context_name]host_name(config-ctx)# gtpc overload-protection ingress
{msg-rate msg_rate} [delay-tolerance dur] [queue-size size]
[no] gtpc overload-protection Ingress
```

Voici quelques notes au sujet de cette syntaxe :

- **non** : Ce paramètre désactive l'étranglement de message de contrôle d'arrivée GTP pour les services GGSN/PGW dans ce contexte.
- **msg_rate de msg-débit** : Ce paramètre définit le nombre de messages d'arrivée GTP qui peuvent être traités par seconde. *Le msg_rate* est un entier qui s'étend de cent à 12,000.
- **dur de retard-tolérance** : Ce paramètre définit le nombre maximal de secondes qu'un message d'arrivée GTP peut être aligné avant qu'il soit traité. Après que cette tolérance soit dépassée, le message est abandonné. *Le dur* est un entier qui s'étend d'un à dix.
- **taille de file d'attente-taille** : Ce paramètre définit la taille de file d'attente maximale pour les messages d'arrivée GTP-C. Si la file d'attente dépasse la taille définie, alors tous les nouveaux messages d'arrivée sont abandonnés. *La taille* est un entier qui s'étend de cent à 10,000.

Vous pouvez employer cette commande afin d'activer l'étranglement de message de contrôle d'arrivée GTP pour les services GGSN/PGW qui sont configurés dans le même contexte. Comme exemple, ce commandes enables les messages d'arrivée de contrôle GTP dans un contexte avec du débit de message de *1,000* par seconde, une taille de file d'attente de messages de *10,000*, et un retard d'une seconde :

gtpc overload-protection ingress msg-rate 1000 delay-tolerance 1 queue-size 10000

Protection voisine d'élément de réseau

Beaucoup d'éléments de réseau voisins emploient leurs propres mécanismes afin de se protéger, et la protection supplémentaire de surcharge de réseau du côté ASR5x00 ne pourrait pas être nécessaire. La protection des éléments de réseau voisins pourrait être exigée dans les cas où la stabilité du réseau globale peut être atteinte seulement quand l'étranglement de message est appliqué du côté de sortie.

Protection de surcharge de réseau avec le diamètre étranglant sur une interface S6a

Cette caractéristique protège les interfaces S6a et S13 dans la direction de sortie. Il protège le serveur à la maison d'abonné (HSS), l'agent de routage de diamètre (DR), et le registre d'identité de matériel (EIR). La caractéristique utilise la fonction de limitation de débit (RLF).

Considérez ces informations importantes quand vous appliquez la configuration de point final de diamètre :

- Un modèle RLF doit être associé avec le pair.
- Un RLF est relié seulement sur une base de par-pair (individuellement).

Configurez le diamètre étranglant sur une interface S6a

Voici la syntaxe de commande qui est utilisée afin de configurer le diamètre étranglant sur une interface S6a :

```
[context_na>me]host_name(config-ctx-diameter)#>peer [*] peer_name [*]
[ realm realm_name ] { address ipv4/ipv6_address [ [ port port_number ]
[connect-on-application-access] [ send-dpr-before-disconnect disconnect-cause
disconnect_cause ] [ sctp ] ] + | fqdn fqdn [ [ port port_number ]
[ send-dpr-before-disconnect disconnect-cause disconnect_cause ]
[ rlf-template rlf_template_name ] ] }

no peer peer_name [ realm realm_name ]
```

Voici quelques notes au sujet de cette syntaxe :

- **non** : Ce paramètre retire la configuration de homologue spécifiée.
- **[*] peer_name [*]** : Ce paramètre spécifie le nom de pair comme chaîne alphanumérique qui s'étend d'une à 63 caractères (des caractères de ponctuation sont permis).Remarque: Le point final de serveur de diamètre peut maintenant être un nom sauvage-cardé de pair (avec * le caractère comme caractre générique valide). Le client que des pairs qui satisfont le modèle sauvage-cardé sont traités comme pairs valides, et connexion est reçu. Le jeton sauvage-cardé indique que le nom de pair sauvage-est cardé, et * le caractère dans la chaîne qui précède est traité comme masque.
- **realm_name de royaume** : Ce paramètre spécifie le royaume de ce pair comme chaîne alphanumérique qui s'étend d'une à 127 caractères. Le nom de royaume peut être une société ou un nom de service.
- **adresse ipv4/ipv6_address** : Ce paramètre spécifie la notation deux points-séparer-hexadécimale d'adresse IP dans l'ipv4 notation-décimal, ou d'IPv6 de diameter peer. Cette adresse doit être l'adresse IP du périphérique avec lequel le châssis communique.
- **FQDN FQDN** : Ce paramètre spécifie le nom de domaine complet de diameter peer (FQDN) comme chaîne alphanumérique qui s'étend d'une à 127 caractères.

- **port_number de port** : Ce paramètre spécifie le numéro de port pour ce diameter peer. Le numéro de port doit être un entier qui s'étend d'un à 65,535.

- **connecter-sur-application-Access** : Ce paramètre lance le pair sur l'accès initial d'application.

- **envoyer-dpr-avant-débranchement** : Ce paramètre envoie la Débranchement-Pair-demande (DPR).

- **débranchement-cause** : Ce paramètre finit le DPR au pair spécifié, avec la raison spécifiée de débranchement. La cause de débranchement doit être un entier qui s'étend de zéro à deux, qui correspondent à ces causes :

  0 RÉINITIALISATIONS de du Â d'âÂ

  1 du Â d'âÂ OCCUPÉ

  2 DO_NOT_WANT_TO_TALK_TO_YOU du Â d'âÂ

- **rlf_template_name de rlf-modèle** : Ce paramètre spécifie le modèle RLF à associer avec ce diameter peer. *Le rlf_template_name* doit être une chaîne alphanumérique qui s'étend d'une à 127 caractères.

  Remarque: Un permis RLF est exigé afin de configurer un modèle RLF.

Protection de surcharge de réseau avec le diamètre étranglant sur une interface Gx/Gy

Cette caractéristique protège les interfaces de Gx et de la GY dans la direction de sortie. Il protège la stratégie et chargeant ordonne la fonction (PCRF) et le système de remplissage en ligne (OCS) et utilise RLF.

Considérez ces informations importantes quand vous appliquez la configuration de point final de diamètre :

- Un modèle RLF doit être associé avec le pair.

- Un RLF est relié seulement sur une base de par-pair (individuellement).

Cette commande est utilisée afin de configurer la protection de surcharge de réseau :

```
[context_name]host_name(config-ctx-diameter)# rlf-template rlf_template_name
```

Remarque: Un permis RLF est exigé afin de configurer un modèle RLF

Configurez le diamètre étranglant sur une interface Gx/Gy

Vous pourriez considérer l'utilisation du RLF pour des interfaces de diamètre. Voici un exemple de configuration :

```
rlf-template rlf1

msg-rate 1000 burst-size 100

threshold upper 80 lower 60

delay-tolerance 4

#exit


diameter endpoint Gy

use-proxy

origin host Gy address 10.55.22.3

rlf-template rlf1

peer peer1 realm foo.com address 10.55.22.1 port 3867 rlf-template rlf2

peer peer2 realm fo.com address 10.55.22.1 port 3870

#exit
```

Voici quelques notes au sujet de cette configuration :

- Le pair appelé le *peer1* est lié à *RFL2*, et le reste des pairs sous le point final sont liés à *RLF1*.
- Le modèle niveau du pair RLF a la priorité au-dessus du modèle niveau du point.
- Nombre de messages sont envoyés à un taux maximal de 1,000 par seconde. (msg-débit). Ces considérations s'appliquent également :

  Seulement cent messages (taille de rafale) sont envoyés chacun pendant cent millisecondes (afin d'atteindre les 1,000 messages par seconde).

  Si nombre de messages dans la file d'attente RLF dépasse 80% du débit de message (80% de 1,000 = de 800), les transitions RLF à l'état *OVER_THRESHOLD*.

  Si nombre de messages dans la file d'attente RLF dépasse le débit de message (1,000), les transitions RLF à l'état *OVER_LIMIT*.

  Si nombre de messages dans la file d'attente RLF diminue en-dessous de 60% du débit de message (60% de 1,000 = de 600), les transitions RLF de nouveau à l'état *PRÊT*.

  Le nombre maximal de messages qui peuvent être alignés égale le débit de message multiplié par la tolérance de retard (1,000 x 4 = 4,000).

  Si l'application envoie plus de 4,000 messages au RLF, les 4,000 premiers sont alignés et le repos sont abandonnés.

  Les messages qui sont abandonnés sont retried/re-sent par l'application au RLF dans une durée appropriée.

Le nombre de relances est la responsabilité de l'application.

- Le modèle peut être non lié du point final avec l'*aucun* paramètre de rlf-*modèle*. Par exemple, il déferait *RLF1 de peer2*.

- N'utilisez l'*aucun* paramètre du rlf-*modèle rlf1* dans le *mode de configuration de point final*, comme tentatives CLI de supprimer le modèle *RLF1* RLF. Cette commande CLI est une partie de la configuration globale, pas la configuration de point final.

- Le modèle peut être lié aux différents pairs par l'intermédiaire d'une de ces commandes :
  no peer peer2 realm foo.com

  peer peer2 realm foo.com address 10.55.22.1 port 3867
- Le RLF peut seulement être utilisé pour les points finaux de diamètre dans lesquels le diamproxy est utilisé.

- Le débit configuré de message est mis en application par-diamproxy. Par exemple, si le débit de message est 1,000, et 12 diamproxies sont en activité (châssis entièrement rempli de = carte active 12 services de paquets (PSC) + 1 Demux + 1 PSC de réserve), les transmissions efficaces par seconde (TPS) est 12,000. Vous pouvez sélectionner une de ces commandes afin de visualiser les statistiques de contexte RLF :
  show rlf-context-statistics diamproxy

  show rlf-context-statistics diamproxy verbose

Protection de surcharge de réseau par la page étranglant avec RLF

La caractéristique de étranglement de page limite le nombre de messages de pagination qui sont envoyés hors du SGSN. Il fournit la flexibilité et le contrôle à l'opérateur, qui peut maintenant réduire le nombre de messages de pagination qui sont envoyés du SGSN basé sur les conditions de réseau. Dans quelques emplacements, la quantité de messages de pagination qui sont initiés du SGSN est due très élevé à de mauvaises conditions par radio. Un nombre supérieur de messages de pagination a comme conséquence la consommation de la bande passante dans le réseau. Cette caractéristique fournit un raté limit configurable, dans lequel le message de pagination est étranglé à ces niveaux :

- Le niveau global pour accès 2G et 3G

- Le niveau de l'entité de service réseau (NSE) pour 2G accèdent à seulement

- Le niveau du contrôleur de réseau radio (RNC) pour 3G accèdent à seulement

Cette caractéristique améliore la consommation de bande passante sur l'interface par radio.

Remarque: Un permis RLF est exigé afin de configurer un modèle RLF.

Voici un exemple du procédé de pagination avec l'accès 2G et la limitation de débit :

Voici un exemple du procédé de pagination avec l'accès 3G et la limitation de débit :

Configurez la page étranglant avec RLF

Les commandes qui sont décrites dans cette section sont utilisées afin de configurer la caractéristique de étranglement de page. Ces commandes CLI sont utilisées afin de s'associer/retirent le modèle RLF pour la page étranglant au niveau global, au niveau NSE, et au niveau RNC sur le SGSN.

Tracez le nom RNC à l'identifiant RNC

La commande d'interface est utilisée afin de configurer le mappage entre l'identifiant RNC (ID) et le nom RNC. Vous pouvez configurer le pagination-rlf-*modèle* l'un ou l'autre par le nom RNC ou l'ID RNC. Voici la syntaxe qui est utilisée :

```
config
sgsn-global
interface-management
[ no ] interface {gb
peer-nsei | iu peer-rnc} {name <value> | id <value>}
exit
```

> Remarque: *Le forme no de la* commande retire le mappage et toute autre configuration qui est associée avec la configuration de pagination-rlf-*modèle* RNC du SGSN et remet à l'état initial le comportement au par défaut pour cela RNC.

Voici un exemple de configuration :

```
[local]asr5000# configure
[local]asr5000(config)# sgsn-global
[local]asr5000(config-sgsn-global)# interface-management
[local]asr5000(config-sgsn-interface-mgmt)# interface
iu peer-rnc id 250 name bng_rnc1
[local]asr5000(config-sgsn-interface-mgmt)# end
[local]asr5000#
```

Associez un modèle de pagination RLF

Cette commande permet au SGSN pour associer un modèle RLF l'un ou l'autre au niveau global, qui limite les messages de pagination qui sont initiés à travers le 2G (niveau NSE) et accès 3G (niveau RNC), ou au niveau de par-entité, qui est au niveau RNC pour l'accès 3G ou au niveau NSE pour l'accès 2G. Voici la syntaxe qui est utilisée :

```
config
sgsn-global
interface-management
[no] paging-rlf-template {template-name <template-name>} {gb
peer-nsei | iu peer-rnc} {name <value> | id <value>}
exit
```

> Remarque: S'il n'y a aucun modèle RLF associé avec un NSE/RNC particulier, alors le chargement de pagination est limité basé sur le modèle global RLF qui est associé (si présent). Si aucun modèle global RLF n'est associé, alors aucune limitation de débit n'est appliquée sur le chargement de pagination.

Voici un exemple de configuration :

```
[local]asr5000(config)# sgsn-global
[local]asr5000(config-sgsn-global)# interface-management
```

```
[local]asr5000(config-sgsn-interface-mgmt)# paging-rlf-template
template-name rlf1
[local]asr5000(config-sgsn-interface-mgmt)# end
[local]asr5000#
[local]asr5000# configure
[local]asr5000(config)# sgsn-global
[local]asr5000(config-sgsn-global)# interface-management
[local]asr5000(config-sgsn-interface-mgmt)# paging-rlf-template
template-name rlf2 gb peer-nsei id 1
[local]asr5000(config-sgsn-interface-mgmt)# end
[local]asr5000#
[local]asr5000# configure
[local]asr5000(config)# sgsn-global
[local]asr5000(config-sgsn-global)# interface-management
[local]asr5000(config-sgsn-interface-mgmt)# paging-rlf-template
template-name rlf2 iu peer-rnc name bng_rnc1
[local]asr5000(config-sgsn-interface-mgmt)# end
[local]asr5000#
```