Éviter l'insuffisance TCAM ACL et QoS sur les commutateurs Catalyst 4500

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Informations générales
ACL du Catalyst 4500 et architecture de programmation de matériel de QoS
Types de TCAM
Dépannez l'épuisement TCAM
Algorithme de programmation suboptimal TCAM pour TCAM 2
Utilisation excessive de L4Ops dans un ACL
ACLs excessif pour le type d'engine ou de commutateur de superviseur
Résumé
Informations connexes

Introduction

Les commutateurs de la gamme Cisco Catalyst 4500 et Catalyst 4948 prennent en charge la liste de contrôle d'accès du débit câblé (ACL) et la fonction QoS avec l'utilisation de la mémoire associative ternaire (TCAM). L'activation des ACL et des politiques ne réduit pas la performance de commutation ou du routage du commutateur tant que les ACL sont complètement chargés dans la TCAM. Si la TCAM est entièrement utilisée, les paquets peuvent être expédiés par l'intermédiaire du CPU, ce qui peut réduire la performance de ces paquets. Ce document fournit des détails relatifs aux éléments suivants :

- Les différents types de TCAM qui l'utilisation du Catalyst 4500 et du Catalyst 4948
- Comment le Catalyst 4500 programme le TCAMs
- Comment configurer de façon optimale l'ACLs et le TCAM sur le commutateur afin d'éviter l'épuisement TCAM

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateurs de la gamme Catalyst 4500
- Commutateurs de la gamme Catalyst 4948

Remarque: Ce document applique seulement aux Commutateurs articulés autour d'un logiciel de Cisco IOS® et n'applique pas aux Commutateurs basés sur de SYSTÈME D'EXPLOITATION de Catalyst (CatOS).

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.

Conventions

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

Informations générales

Afin d'implémenter les divers types d'ACLs et des stratégies QoS dans le matériel, les tables de correspondance de matériel de programmes du Catalyst 4500 (TCAM) et de divers registres matériels dans l'engine de superviseur. Quand un paquet arrive, le commutateur exécute une consultation de table de matériel (consultation TCAM) et décide à l'autorisation ou refuse le paquet.

Types de supports du Catalyst 4500 les différents d'ACLs. Le tableau 1 trace les grandes lignes de ces types d'ACLs.

Tableau 1 – Tape d'ACLs qui sont pris en charge sur des Commutateurs du Catalyst 4500

Type d'ACL	Là où il est appliqué	Le trafic commandé	Direction
RACL[1]	Port L3[2], canal L3, ou SVI[3] (VLAN)	Le trafic IP conduit	D'arrivée ou sortant
VACL[4]	VLAN (par l'intermédiaire de la commande de **vlan filter**)	Tous les paquets lesquels sont conduits dans ou hors d'un VLAN ou lesquels pont dans un VLAN	Directionless
PACL[5]	Port L2[6] ou canal L2	Le tous les trafic IP et trafic non-IPv4[7] (par l'intermédiaire de l'ACL de MAC)	D'arrivée ou sortant

[1] ACL RACL = de routeur

[2] L3 = couche 3

[3] SVI = interface virtuelle commutée

[4] ACL VACL = VLAN

[5] ACL PACL = de port

[6] L2 = couche 2

[7] ipv4 = versions d'IP 4

ACL du Catalyst 4500 et architecture de programmation de matériel de QoS

Le Catalyst 4500 TCAM a le nombre suivant d'entrées :

- 32,000 entrées pour l'ACL de Sécurité, qui est également connu comme ACL de caractéristique
- 32,000 entrées pour l'ACL de QoS

Pour l'ACL et l'ACL de QoS de Sécurité, les entrées sont dédiées de la façon suivante :

- 16,000 entrées pour la direction d'entrée
- 16,000 entrées pour la direction de sortie

La figure 3 affiche le dévouement d'entrée TCAM. Voyez les types de section TCAM pour plus d'informations sur TCAMs.

Ajournez les 2show les ressources en ACL qui sont disponibles pour différents engines et Commutateurs de superviseur du Catalyst 4500.

Tableau 2 – Ressources en ACL du Catalyst 4500 sur de divers engines et Commutateurs de superviseur

Produit	Version TCAM	Fonction TCAM (par direction)	QoS TCAM (par direction)
Engine II+ de superviseur	2	8000 entrées, 1000 masques	8000 entrées, 1000 masques
Engine II+TS/III/IV/V et WS-C4948 de superviseur	2	16,000 entrées, 2000 masques	16,000 entrées, 2000 masques
Engine V-10GE et WS-C4948-10GE de superviseur	3	16,000 entrées, 16,000	16,000 entrées, 16,000

		masques	masques

Les utilisations du Catalyst 4500 séparent, ont dédié TCAMs pour l'unicast sur IP et le routage de Multidiffusion. Le Catalyst 4500 peut avoir jusqu'à 128,000 entrées de route que l'unicast et les routes multicasts partagent. Cependant, ces détails sont hors de portée de ce document. Ce document discute seulement des titres et d'épuisement de QoS TCAM.

La figure 1 affiche que les étapes programmaient l'ACLs dans des tables de matériel sur le Catalyst 4500.

Figure 1 - Étapes pour programmer ACLs sur des Commutateurs du Catalyst 4500

Étape 1

Cette étape implique une de ces actions :

- Configuration et application d'un ACL ou d'une stratégie QoS à une interface ou à un VLANLa création d'ACL peut se produire dynamiquement. Un exemple est le cas de la caractéristique de la protection de source IP (IPSG). Avec cette configuration, le commutateur crée automatiquement un PACL pour les adresses IP qui sont associées avec le port.
- Modification d'un ACL qui existe déjà

Remarque: Seule la configuration d'un ACL n'a pas comme conséquence la programmation TCAM. L'ACL (stratégie QoS) doit appliqué à une interface afin de programmer l'ACL dans le TCAM.

Étape 2

L'ACL doit être fusionné avant qu'il puisse être programmé dans les tables de matériel (TCAM). Les programmes de fusion plusieurs ACLs (PACL, VACL, ou RACL) dans le matériel d'une mode combinée. De cette façon, seulement une consultation de matériel unique est nécessaire pour vérifier contre tout l'ACLs applicable dans le chemin de transfert logique de paquet.

Par exemple, dans la figure 2, un paquet qui est conduit du PC-Un au PCC potentiellement peut avoir ces ACLs :

- Une entrée PACL sur le port de PC-Un
- Un VACL sur le VLAN 1
- Un RACL en entrée sur l'interface VLAN 1 dans la direction d'entrée

Ces trois ACLs sont fusionnés de sorte qu'une consultation simple dans l'entrée TCAM soit assez pour prendre la décision d'expédition de laisser ou refuser. De même, seulement une consultation à sortie unique est nécessaire parce que le TCAM est programmé avec le résultat fusionné de ces trois ACLs :

- La sortie RACL sur l'interface VLAN 2
- Le VLAN 2 VACL
- La sortie PACL sur le port PCC

Avec une consultation simple pour l'entrée et une pour la sortie, il n'y a aucun expédition de matériel de pénalité des paquets quand tout ou une partie des ces ACLs sont dans le chemin de transfert de paquet.

Remarque: Les consultations de l'entrée et sortie TCAM se produisent en même temps dans le

matériel. Une fausse idée commune est que la consultation de la sortie TCAM se produit après la consultation de l'entrée TCAM, car l'écoulement logique de paquet suggère. Il est importante comprendre ces informations parce que la stratégie de sortie du Catalyst 4500 ne peut pas s'assortir sur des paramètres de QoS modifiés par politique d'entrée. Dans le cas de l'ACL de Sécurité, l'action la plus grave se produit. Le paquet est lâché dans l'un ou l'autre de ces situations :

- Si le résultat de recherche d'entrée est la baisse et le résultat de recherche de sortie est autorisation
- Si le résultat de recherche d'entrée est l'autorisation et le résultat de recherche de sortie est baisse

Remarque: On permet le paquet si les les deux les résultats de recherche d'entrée et sortie sont autorisation.

Figure 2 – Filtrage par l'intermédiaire de la Sécurité ACLs sur des Commutateurs du Catalyst 4500

La fusion d'ACL sur le Catalyst 4500 est commande-dépendante. Le processus est également connu comme fusion dépendante de commande (ODM). Avec l'ODM, des rubriques de liste ACL sont programmés dans la commande dans laquelle ils apparaissent dans l'ACL. Par exemple, si un ACL contient deux entrées de contrôle d'accès (as), le commutateur programme ACE 1 d'abord et programme ensuite ACE 2. Cependant, la dépendance de commande est seulement entre les as dans un ACL spécifique. Par exemple, les as dans l'ACL 120 peuvent commencer avant des as dans l'ACL 100 dans le TCAM.

Étape 3

L'ACL fusionné est programmé dans le TCAM. L'entrée ou la sortie TCAM pour l'ACL ou le QoS est davantage de fractionnement dans deux régions, PortAndVlan et PortOrVlan. L'ACL fusionné est programmé dans la région de PortAndVlan du TCAM si une configuration a *chacun des deux* ACLs dans le même chemin de paquet :

- UN PACL**Remarque:** Le PACL est un ACL de filtrage normal ou ACL dynamique IPSG-créé.
- Un VACL ou un RACL

Un ACL est programmé dans la région de PortOrVlan du TCAM si un chemin particulier du paquet a seulement un PACL ou un VACL ou un RACL. La figure 3 affiche l'ACL TCAM de Sécurité découpant pour différents types d'ACLs. QoS a un TCAM pareillement découpé, distinct, dédié.

Actuellement, vous ne pouvez pas modifier l'allocation de par défaut TCAM. Cependant, il y a des plans pour fournir la capacité de changer l'allocation TCAM qui est disponible pour les régions de PortAndVlan et de PortOrVlan dans de futures versions logicielles. Cette modification te permettra pour augmenter ou diminuer l'espace pour PortAndVlan et PortOrVlan dans l'entrée ou la sortie TCAMs.

Remarque: N'importe quelle augmentation d'allocation pour la région de PortAndVlan aura comme conséquence une diminution équivalente pour la région de PortOrVlan de l'entrée ou de la sortie TCAM.

Figure 3 – Structure de l'ACL TCAM de Sécurité sur les Commutateurs du Catalyst 4500

La commande brief d'utilisation de statistiques d'ACL de matériel de show platform affiche cette utilisation TCAM par région pour l'ACL et le QoS TCAMs. La sortie de commande affiche les masques et les entrées disponibles et les divise par région, comme dans la figure 3. Cette sortie témoin est d'une engine II+ de superviseur du Catalyst 4500 :

Remarque: Voyez les types de section TCAM de ce document pour plus d'informations sur les masques et les entrées.

```
Switch#show platform hardware acl statistics utilization brief Entries/Total(%) Masks/Total(%) -
--------------- --------------- Input Acl(PortAndVlan) 2016 / 4096 ( 49) 252 / 512 ( 49) Input
Acl(PortOrVlan) 6 / 4096 ( 0) 5 / 512 ( 0) Input Qos(PortAndVlan) 0 / 4096 ( 0) 0 / 512 ( 0)
Input Qos(PortOrVlan) 0 / 4096 ( 0) 0 / 512 ( 0) Output Acl(PortAndVlan) 0 / 4096 ( 0) 0 / 512 (
0) Output Acl(PortOrVlan) 0 / 4096 ( 0) 0 / 512 ( 0) Output Qos(PortAndVlan) 0 / 4096 ( 0) 0 /
512 ( 0) Output Qos(PortOrVlan) 0 / 4096 ( 0) 0 / 512 ( 0) L4Ops: used 2 out of 64
```

Types de TCAM

Le Catalyst 4500 utilise deux types de TCAM, comme 2show de Tableau. Cette section présente la différence entre les deux versions TCAM de sorte que vous puissiez sélectionner le produit approprié pour votre réseau et configuration.

TCAM 2 utilise une structure en laquelle masque du partage un de huit entrées. Un exemple est huit adresses IP dans les as. Les entrées doivent avoir le même masque que le masque qu'elles partagent. Si les as ont différents masques, les entrées doivent utiliser les masques distincts selon les besoins. Cette utilisation des masques distincts peut mener pour masquer l'épuisement. L'épuisement de masque dans le TCAM est l'une des raisons communes pour l'épuisement TCAM.

TCAM 3 n'a pas une telle restriction. Chaque entrée peut avoir son propre seul masque dans le TCAM. La pleine utilisation de toutes les entrées qui sont disponibles dans le matériel est possible, indépendamment du masque de ces entrées.

Afin d'expliquer cette architecture de matériel, l'exemple dans cette section affiche comment un TCAM 2 et un programme ACLs TCAM 3 dans le matériel.

```
access-list 101 permit ip host 8.1.1.1 any
access-list 101 deny ip 8.1.1.0 0.0.0.255 any
```

Cet ACL d'échantillon a deux entrées qui ont deux masques différents. ACE 1 est une entrée de hôte et ainsi elle a un masque de /32. ACE 2 est une entrée de sous-réseau avec un masque de /24. Puisque la deuxième entrée a un masque différent, des entrées vides dans le masque 1 ne peuvent pas être utilisées et un masque distinct est utilisé dans le cas de TCAM 2.

Cette table affiche comment cet ACL est programmé dans TCAM 2 :

Masques	Entrées
Correspondance du **masque 1** : chacun des 32 bits de l'adresse IP source « ne s'inquiète pas » : tous les bits restants	Source ip = 8.1.1.1
	Entrée vide 2
	Entrée vide 3
	Entrée vide

	4
	Entrée vide 5
	Entrée vide 6
	Entrée vide 7
	Entrée vide 8
Correspondance du **masque 2** : la plupart des 24 bits significatifs de l'adresse IP source « ne s'inquiètent pas » : tous les bits restants	Source ip = 8.1.1.0
	Entrée vide 2
	Entrée vide 3
	Entrée vide 4
	Entrée vide 5
	Entrée vide 6
	Entrée vide 7
	Entrée vide 8

Quoiqu'il y ait les entrées libres disponibles en tant qu'élément du masque 1, la structure TCAM 2 empêche la population d'ACE 2 dans l'entrée vide 2 pour le masque 1. L'utilisation de ce masque n'est pas permise parce que le masque d'ACE 2 n'apparie pas le masque de /32 d'ACE que 1. TCAM 2 doit programmer ACE 2 avec l'utilisation d'un masque distinct, un masque de /24.

Cette utilisation d'un masque distinct peut avoir comme conséquence un épuisement plus rapide des ressources disponibles, comme 2show de Tableau. L'autre ACLs peut encore utiliser les entrées restantes dans le masque 1. Cependant, dans la plupart des cas, l'efficacité de TCAM 2 est élevée mais n'est pas de 100 pour cent. L'efficacité varie avec chaque scénario de configuration.

Cette table affiche que le même ACL programmé dans le TCAM 3. TCAM 3 alloue un masque pour chaque entrée :

Masques	Entrées
Bits du masque 32 pour l'adresse IP 1	Source ip = 8.1.1.1
Bits du masque 24 pour l'adresse IP 2	Source ip = 8.1.1.0
Videz le masque 3	Entrée vide 3
Videz le masque 4	Entrée vide 4
Videz le masque 5	Entrée vide 5
Videz le masque 6	Entrée vide 6
Videz le masque 7	Entrée vide 7
Videz le masque 8	Entrée vide 8
Videz le masque 9	Entrée vide 9
Videz le masque 10	Entrée vide 10
Videz le masque 11	Entrée vide 11
Videz le masque 12	Entrée vide 12
Videz le masque 13	Entrée vide 13
Videz le masque 14	Entrée vide 14
Videz le masque 15	Entrée vide 15
Videz le masque 16	Entrée vide 16

Dans cet exemple, les 14 entrées restantes mettent en boîte chacune ont des entrées avec différents masques, sans des restrictions. Par conséquent, le TCAM 3 est beaucoup plus efficace que le TCAM 2. Cet exemple est excessivement simplifié afin de montrer la différence entre les versions TCAM. Le logiciel du Catalyst 4500 a de nombreuses optimisations pour augmenter l'efficacité de la programmation dans TCAM 2 pour un scénario pratique de configuration. L'algorithme de programmation suboptimal TCAM pour TCAM 2 sections de ce document discute ces optimisations.

Pour TCAM 2 et TCAM 3 sur le Catalyst 4500, les entrées TCAM sont partagées si le même ACL est appliqué sur différentes interfaces. Cette optimisation ménage de l'espace TCAM.

Dépannez l'épuisement TCAM

Quand l'épuisement TCAM se produit sur des Commutateurs du Catalyst 4500 pendant la programmation d'un ACL de Sécurité, une application partielle de l'ACL se produit par l'intermédiaire du chemin logiciel. Les paquets qui apparient les as qui ne sont pas appliqués dans le TCAM sont traités en logiciel. Ceci qui traite en logiciel entraîne l'utilisation du CPU élevé. Puisque la programmation d'ACL du Catalyst 4500 est commande-dépendante, l'ACL est toujours programmé de haut en bas. Si un ACL spécifique ne s'insère pas entièrement dans le TCAM, les as à la partie inférieure de l'ACL très probablement ne sont pas programmés dans le TCAM.

Un message d'avertissement apparaît quand un dépassement TCAM se produit. Voici un exemple :

```
%C4K_HWACLMAN-4-ACLHWPROGERRREASON: (Suppressed 1times) Input(null, 12/Normal)
```

```
Security: 140 - insufficient hardware TCAM masks.
%C4K_HWACLMAN-4-ACLHWPROGERR: (Suppressed 4 times) Input Security: 140 - hardware TCAM
limit, some packet processing will be software switched.
```

Vous pouvez également voir ce message d'erreur dans la sortie de commande de **show logging** si vous avez activé le Syslog. La présence de ce message indique d'une manière concluante que le traitement de logiciel aura lieu. En conséquence, il peut y avoir utilisation du CPU élevé. L'ACL qui a été déjà programmé dans les restes TCAM a programmé dans TCAM si l'épuisement de la capacité TCAM se produit pendant l'application du nouvel ACL. Les paquets qui apparient l'ACLs qui ont été déjà programmés continuent à être traités et expédiés dans le matériel.

Remarque: Si vous apportez des modifications à un grand ACL, le message TCAM-dépassé peut être affiché. Les essais de commutateur pour reprogrammer l'ACL dans TCAM. Dans la plupart des cas, l'ACL nouveau et modifié peut être reprogrammé entièrement dans le matériel. Si le commutateur peut avec succès reprogrammer l'ACL dans l'intégralité dans le TCAM, ce message apparaît :

```
*Apr 12 08:50:21: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All configured ACLs
now fully loaded in hardware TCAM - hardware switching / QoS restored
```

Employez la commande **récapitulative d'interface-***id d'***interface d'entrée d'acl de logiciel de show platform** afin de vérifier que l'ACL est entièrement programmé dans le matériel.

Cette sortie affiche la configuration de l'ACL 101 au VLAN 1 et à la vérification que l'ACL est entièrement programmé dans le matériel :

Remarque: Si l'ACL n'est pas entièrement programmé, un message d'erreur de TCAM-épuisement peut afficher.

```
Switch#configure terminal Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1 Switch(config-if)#ip access-group 101 in Switch(config-if)#end
Switch# Switch#show platform software acl input summary interface vlan 1 Interface
Name                 : Vl1   Path(dir:port, vlan)         : (in :null, 1)     Current
TagPair(port, vlan) : (null, 0/Normal)     Current Signature          : {FeatureCam:(Security:
101)}   Type                         : Current     Direction                 : In
TagPair(port, vlan)        : (null, 0/Normal)     FeatureFlatAclId(state)    :
0(FullyLoadedWithToCpuAces)     QosFlatAclId(state)        : (null)
Flags                      : L3DenyToCpu
```

Le champ d'`indicateurs` (`L3DenyToCpu`) indique que, si un paquet est refusé en raison de l'ACL, le paquet est donné un coup de volée à la CPU. Le commutateur envoie alors un Protocole ICMP (Internet Control Message Protocol) - message d'inaccessibilité. Ce comportement est le par défaut. Quand les paquets sont donnés un coup de volée à la CPU, l'utilisation du CPU élevé peut se produire sur le commutateur. Cependant, dans le Logiciel Cisco IOS version 12.1(13)EW et plus tard, ces paquets sont débit-limités à la CPU. Dans la plupart des cas, Cisco recommande que vous arrêtiez la caractéristique qui envoie des messages ICMP inaccessibles.

Cette sortie affiche que la configuration du commutateur n'envoyait pas des messages ICMP inaccessibles et la vérification du TCAM programmant après la modification. L'état de l'ACL 101 est maintenant `FullyLoaded`, car la sortie de commande affiche. Le trafic refusé ne va pas à la CPU.

```
Switch#configure terminal Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1 Switch(config-if)#no ip unreachables Switch(config-if)#end
Switch#show platform software acl input summary interface vlan 1 Interface Name
: Vl1   Path(dir:port, vlan)         : (in :null, 1)     Current TagPair(port, vlan) : (null,
1/Normal)     Current Signature          : {FeatureCam:(Security: 101)}
Type                         : Current     Direction                 : In     TagPair(port,
vlan)        : (null, 1/Normal)     FeatureFlatAclId(state)    : 0(FullyLoaded)
```

```
QosFlatAclId(state)        : (null)     Flags                       : None
```

Remarque: Si le QoS TCAM est dépassé pendant l'application d'une certaine stratégie QoS, cette stratégie spécifique n'est pas appliquée à l'interface ou au VLAN. Le Catalyst 4500 n'implémente pas la stratégie QoS dans le chemin logiciel. Par conséquent, l'utilisation du processeur ne cloue pas quand QoS TCAM est dépassé.

```
*May 13 08:01:28: %C4K_HWACLMAN-4-ACLHWPROGERR: Input Policy Map: 10Mbps - hardware TCAM
limit, qos being disabled on relevant interface.

*May 13 08:01:28: %C4K_HWACLMAN-4-ACLHWPROGERRREASON: Input Policy Map: 10Mbps - no
available hardware TCAM entries.
```

Émettez la commande **show platform cpu packet statistics**. Déterminez si le `commutateur d'ACL traitant la` file d'attente reçoit un nombre élevé de paquets. Un nombre élevé de paquets indique l'épuisement de la Sécurité TCAM. Cet épuisement TCAM cause des paquets d'être envoyés à la CPU pour l'expédition de logiciel.

```
Switch#show platform cpu packet statistics !--- Output suppressed. Packets Received by Packet
Queue  Queue                  Total           5 sec avg 1 min avg 5 min avg 1 hour avg ---------
------------ -------------- --------- --------- --------- ----------
Control                      57902635        22        16        12          3 Host
Learning                       464678         0         0         0          0 L3 Fwd
Low                            623229         0         0         0          0 L2 Fwd
Low                          11267182         7         4         6          1 L3 Rx
High                             508         0         0         0          0 L3 Rx
Low                            1275695        10         1         0          0 ACL
fwd(snooping)                  2645752         0         0         0          0 ACL log,
unreach                     51443268         9         4         5          5 ACL sw
processing                  842889240      1453      1532      1267       1179  Packets Dropped by
Packet Queue  Queue                  Total           5 sec avg 1 min avg 5 min avg 1 hour avg --
-------------------- -------------- --------- --------- --------- ---------- L2 Fwd
Low                            3270         0         0         0          0 ACL sw
processing                    12636         0         0         0          0
```

Si vous constatez que le `commutateur d'ACL traitant la` file d'attente ne reçoit pas une quantité excessive du trafic, référez-vous à l'utilisation du CPU élevé sur les Commutateurs articulés autour d'un logiciel du Catalyst 4500 de Cisco IOS pour d'autres causes possibles. Le document fournit des informations sur la façon dont dépanner d'autres scénarios d'utilisation du CPU élevé.

Le Catalyst 4500 TCAM peut déborder pour ces raisons :

- Un algorithme de programmation suboptimal TCAM pour TCAM 2
- L'utilisation excessive des exécutions de la couche 4 (L4Ops) dans un ACL
- ACLs excessif pour le type d'engine ou de commutateur de superviseur

Algorithme de programmation suboptimal TCAM pour TCAM 2

Car les types de section de TCAM discute, l'efficacité TCAM 2 est due inférieur au fait que masque du partage un de huit entrées. Le logiciel du Catalyst 4500 tient compte de deux types d'algorithmes de programmation TCAM pour TCAM 2 qui améliorent l'efficacité de TCAM 2 :

- Emballé — Approprié à la plupart des scénarios d'ACL de Sécurité**Remarque:** Il s'agit de la configuration par défaut.
- Dispersé — Utilisé dans le scénario IPSG

Vous pouvez changer l'algorithme à un algorithme dispersé, mais ceci n'aide pas typiquement si vous avez configuré seulement la Sécurité ACLs, tel que RACLs. L'algorithme dispersé est seulement efficace dans les scénarios où le même ou un ACL semblable et petit est répété sur de

nombreux ports. Ce scénario est le cas avec un IPSG qui est activé sur des plusieurs interfaces. Dans le scénario IPSG, chaque ACL dynamique :

- A un nombre restreint d'entréesCeci inclut des autorisations pour les adresses IP permises et un refuser à l'extrémité afin d'empêcher l'accès du port par les adresses IP non autorisées.
- Est répété pour tous les ports d'accès configurésL'ACL est répété pour jusqu'à 240 ports sur un Catalyst 4507R.

Remarque: TCAM 3 utilise l'algorithme emballé par par défaut. Puisque la structure TCAM est un masque par entrée, l'algorithme emballé est le meilleur algorithme. Par conséquent, l'option dispersée d'algorithme n'est pas activée sur ces Commutateurs.

Cet exemple est sur une engine II+ de superviseur qui est configurée pour la caractéristique IPSG. La sortie prouve que, bien que seulement 49 pour cent des entrées soient utilisés, 89 pour cent des masques sont consommés :

```
Switch#show platform hardware acl statistics utilization brief
                                     Entries/Total(%)  Masks/Total(%)
                                    ----------------  --------------
                                                                  Input
Acl(PortAndVlan)  2016 / 4096 ( 49)   460 /  512 ( 89)             Input  Acl(PortOrVlan)      6
/ 4096 (  0)     4 /  512 (  0)             Input  Qos(PortAndVlan)     0 / 4096 (  0)     0 /
512 (  0)             Input  Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
Output Acl(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)             Output
Acl(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)             Output Qos(PortAndVlan)     0
/ 4096 (  0)     0 /  512 (  0)             Output Qos(PortOrVlan)      0 / 4096 (  0)     0 /
512 (  0)             L4Ops: used 2 out of 64
```

Dans ce cas, un changement de l'algorithme de programmation du par défaut a emballé l'algorithme aux aides dispersées d'algorithme. L'algorithme dispersé ramène toute l'utilisation de masque de 89 pour cent à 49 pour cent.

```
Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#access-list hardware entries scattered Switch(config)#end Switch#show platform
hardware acl statistics utilization brief Entries/Total(%) Masks/Total(%) ----------------- ----
----------- Input Acl(PortAndVlan) 2016 / 4096 ( 49) 252 / 512 ( 49) Input Acl(PortOrVlan) 6 /
4096 ( 0) 5 / 512 ( 0) Input Qos(PortAndVlan) 0 / 4096 ( 0) 0 / 512 ( 0) Input Qos(PortOrVlan) 0
/ 4096 ( 0) 0 / 512 ( 0) Output Acl(PortAndVlan) 0 / 4096 ( 0) 0 / 512 ( 0) Output
Acl(PortOrVlan) 0 / 4096 ( 0) 0 / 512 ( 0) Output Qos(PortAndVlan) 0 / 4096 ( 0) 0 / 512 ( 0)
Output Qos(PortOrVlan) 0 / 4096 ( 0) 0 / 512 ( 0) L4Ops: used 2 out of 64
```

Pour des informations sur des pratiques recommandées pour des fonctionnalités de sécurité sur des Commutateurs du Catalyst 4500, référez-vous aux pratiques recommandées de fonctionnalités de sécurité du Catalyst 4500 pour des superviseurs.

Utilisation excessive de L4Ops dans un ACL

Le terme L4Ops se rapporte à l'utilisation du **gt**, du **lt**, du **neq**, et des mots clé de **plage** dans la configuration d'ACL. Le Catalyst 4500 a des limites sur le nombre de ces mots clé que vous pouvez utiliser dans un ACL simple. La limite, qui varie par l'engine et le commutateur de superviseur, est six ou huit L4Ops par ACL. Le tableau 3 affiche la limite par engine de superviseur et par ACL.

Tableau 3 – Limite L4Op par ACL sur différents engines et Commutateurs de superviseur du Catalyst 4500

Produit	L4Op
Supervisor Engine II+/II+TS	32 (6 par ACL)

Engine III/IV/V et WS-C4948 de superviseur	32 (6 par ACL)
Engine V-10GE et WS-C4948-10GE de superviseur	64 (8 par ACL)

Si la limite L4Op par ACL est dépassée, un message d'avertissement est affiché sur la console. Le message est semblable à ceci :

```
%C4K_HWACLMAN-4-ACLHWPROGERR: Input Security: severn - hardware TCAM limit, some
packet processing will be software switched.
19:55:55: %C4K_HWACLMAN-4-ACLHWPROGERRREASON: Input Security: severn - hardware TCAM L4
operators/TCP flags usage capability exceeded.
```

En outre, si la limite L4Op est dépassée, la particularité ACE est développée dans le TCAM. Résultats supplémentaires d'utilisation TCAM. Cet ACE sert comme exemple :

```
access-list 101 permit tcp host 8.1.1.1 range 10 20 any
```

Avec cet ACE dans un ACL, le commutateur utilise seulement une entrée et un L4Op. Cependant, si six L4Ops sont déjà utilisés dans cet ACL, cet ACE est développé à 10 entrées dans le matériel. Une telle extension peut potentiellement épuiser beaucoup d'entrées dans le TCAM. L'utilisation soigneuse de ces L4Ops empêche le dépassement TCAM.

Remarque: Si ce cas implique l'engine V-10GE et WS-C4948-10GE de superviseur, huit L4Ops précédemment utilisés dans l'ACL ont comme conséquence l'extension d'ACE.

Maintenez ces éléments dans l'esprit quand vous utilisez L4Op sur des Commutateurs du Catalyst 4500 :

- Les exécutions L4 sont considérées différentes si l'opérateur ou l'opérande diffèrent.Par exemple, cet ACL contient trois exécutions L4 différentes parce que le **gt 10** et le **gt 11** sont considérés deux exécutions L4 différentes :`access-list 101 permit tcp host 8.1.1.1 any gt 10 access-list 101 deny tcp host 8.1.1.2 any lt 9 access-list 101 deny tcp host 8.1.1.3 any gt 11`
- Les exécutions L4 sont considérées différentes si le même couple d'opérateur/opérande s'applique une fois à un port de source et une fois à une destination port.Voici un exemple :`access-list 101 permit tcp host 8.1.1.1 gt 10 any access-list 101 permit tcp host 8.1.1.2 any gt 10`
- Les Commutateurs du Catalyst 4500 partagent L4Ops si possibles.Dans cet exemple, les lignes en ***italique en caractères gras*** expliquent ce scénario :Utilisation L4Op pour l'ACL 101 = 5Utilisation L4Op pour l'ACL 102 = 4 **Remarque:** Le mot clé d'**eq** ne consomme pas la ressource en matériel l'une des L4Op.Utilisation totale L4Op = **8Remarque:** Partage un L4Op de l'ACL 101 et 102.**Remarque:** L4Op est partagé même si le protocole, tel que le TCP ou le Protocole UDP (User Datagram Protocol), ne s'assortit pas ou l'autorisation/refusent l'action n'apparie pas.

ACLs excessif pour le type d'engine ou de commutateur de superviseur

Comme 2show de Tableau, TCAM est une ressource limitée. Vous pouvez dépasser la ressource TCAM en n'importe quelle engine de superviseur si vous configurez ACLs excessif ou caractéristiques comme IPSG avec un nombre élevé d'entrées IPSG.

Si vous dépassez l'espace TCAM pour votre engine de superviseur, prenez ces mesures :

- Si vous avez une engine II+ de superviseur et vous exécutez une version logicielle de Cisco IOS qui est *plus tôt* que la version du logiciel Cisco IOS 12.2(18)EW, améliorez à la dernière version de maintenance de la version du logiciel Cisco IOS 12.2(25)EWA.La capacité TCAM a été augmentée dans les versions ultérieures.
- Si vous utilisez la surveillance DHCP et l'IPSG et vous commencez à manquer de TCAM, à utiliser la dernière version de maintenance de la version du logiciel Cisco IOS 12.2(25)EWA et à utiliser l'algorithme dispersé dans le cas des Produits TCAM 2.**Remarque:** L'algorithme dispersé est disponible dans la version du logiciel Cisco IOS 12.2(20)EW et plus tard.La dernière release a également des améliorations pour une meilleure utilisation TCAM avec piller DCHP et les configurations dynamiques d'inspection de Protocole ARP (Address Resolution Protocol) (DAI).
- Si vous commencez à manquer de TCAM parce que la limite L4Op est dépassée, essai pour réduire l'utilisation L4Op dans l'ACL afin d'empêcher le dépassement TCAM.
- Si vous utilisez beaucoup ACLs semblable ou stratégies sur de divers ports dans le même VLAN, agrégez-les dans un ACL ou une stratégie simple sur l'interface VLAN.Cette agrégation ménage de l'espace certain TCAM. Par exemple, quand vous appliquez des stratégies basées sur Voix, le QoS basé sur port par défaut est utilisé pour la classification. Ce par défaut QoS peut entraîner la capacité TCAM d'être dépassé. Si vous commutez le QoS à basé sur VLAN, vous réduisez l'utilisation TCAM.
- Si vous avez toujours les problèmes avec TCAM espacent, considèrent une engine à extrémité élevé de superviseur, telle que l'engine V-10GE de superviseur ou le Catalyst 4948-10GE.Ces Produits utilisent le matériel TCAM le plus efficace 3.

Résumé

Le Catalyst 4500 programme l'ACLs configuré avec l'utilisation du TCAM. TCAM tient compte de l'application de l'ACLs dans le chemin de matériel-expédition sans l'incidence sur la représentation du commutateur. La performance est constante quelle que soit la taille de l'ACL car la performance des recherches ACL est à plein débit. Cependant, TCAM n'est pas une ressource inépuisable. Par conséquent, si vous configurez un nombre excessif d'entrées ACL, vous dépasserez la capacité TCAM. Le Catalyst 4500 a mis en application de nombreuses optimisations et si des commandes de varier l'algorithme de programmation de TCAM afin de réaliser l'efficacité maximum. Les Produits TCAM 3 tels que l'engine V-10GE de superviseur et le Catalyst 4948-10GE offrent les la plupart des ressources TCAM pour l'ACL et les stratégies QoS de Sécurité.

Informations connexes

- Pages de support pour les produits LAN
- Page de support sur la commutation LAN
- Support et documentation techniques - Cisco Systems