Implémentation des listes d'accès sur les routeurs Internet des gammes Cisco 12000

Contenu

Introduction

Ce document décrit le soutien du Listes de contrôle d'accès (ACL) sur les Routeur Internet de la série Cisco 12000.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance des fondements de la façon dont un ACL travaille à un routeur de Cisco.

Référez-vous à ces documents pour des informations générales sur ACLs et leurs applications :

- Listes de contrôle d'accès : Aperçu et instructions
- Configurer des Services IP : Paquets IP de filtre

Composants utilisés

Les informations dans ce document sont basées sur des Routeur Internet de la série Cisco 12000.

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.

Aperçu de support d'ACL sur le Routeur Internet de la série Cisco 12000

Sur le Routeur Internet de la série Cisco 12000, ACLs peut être traité dans le matériel (circuit intégré spécifique à l'application - ASIC), le logiciel (la CPU d'un linecard), ou comme caractéristique hybride – traité dans le logiciel avec l'aide de matériel. Si un ACL est traité en matériel ou logiciel dépend de l'application d'ACL, du type de moteur de linecard, et de l'interaction d'ACLs dans d'autres linecards.

Les engines de linecard de gamme Cisco 12000 fournissent différentes capacités d'ACL. Pour les informations de support d'ACL pour une engine de carte de ligne particulière, allez à la section correspondante dans ce document.

Remarque: Le Protocole IP Multicast ACLs ne sont pas pris en charge dans la version de logiciel 12.0S de Cisco IOS®. La caractéristique d'ip multicast boundary peut être utilisée où le filtrage de Multidiffusion est exigé. Référez-vous à la Fonction Multicast Forwarding de Rapide-chemin sur le pour en savoir plus d'Engine 2 de gamme Cisco 12000 et de linecards ISE.

ACLs basé sur ASIC contre ACLs central de traitement CPU

Le Cisco 12000 prend en charge toutes les générations du traitement d'ACL. Une compréhension opérationnelle de la façon dont chacun de ces modes d'exploitation fonctionne, interagit, et se prend en charge est essentielle à l'utilisation efficace d'ACL sur le Cisco 12000.

Les premières générations du traitement d'ACL ont utilisé une CPU programmable pour traiter l'ACL. Au fil du temps, le paquet par seconde (PPS) traitant des conditions requises a dépassé la capacité de nouvelles CPU de continuer. Des ASIC ont été construits pour réaliser des débits plus supérieurs PPS pour l'expédition et les capacités de fonctionnalité de routeur. ACLs qui ont été chargés sur la CPU du linecard (LC) ont été alors chargés sur le LC ASIC. Des ASIC ont continué à être improvisés pour manipuler des débits plus supérieurs PPS. Ces la seconde génération ASIC ont été établies sur le travail pilote de la génération avant, et offrent plus de capacités ASIC.

Puisque le Cisco 12000 est une plate-forme de acheminement distribuée, l'interaction entre les diverses générations du traitement d'ACL peut créer une certaine confusion opérationnelle.

Des termes tels que l'ACL basé sur ASIC, l'ACL central de traitement CPU, le chemin rapide, le chemin lent, et les coups de volée ASIC sont utilisés dans tout ce document pour aider à expliquer ce qui se produit avec le traitement d'ACL. Voici les explications de ces termes :

- ACLs basé sur ASIC (chemin rapide) — ACLs sont chargés et traités dans le matériel ASIC. L'enveloppe de représentation de l'ASIC détermine la profondeur, la représentation, et les capacités d'ACL. Le chemin rapide a été utilisé dans le chemin pour illustrer la différence entre le traitement basé sur ASIC et le traitement fait dans la CPU LC-la prenant en charge. Plus le terme générique, basé sur ASIC, est utilisé dans ce document.
- ACLs central de traitement CPU (chemin lent) — ACLs sont traités en logiciel sur la CPU de linecard. Pour les cartes de première génération (l'engine 0 et dans certains cas l'engine 1), traitant tout est faite sur la CPU LC. les LCS basés sur ASIC exécutent l'ACL traitant sur les paquets qui sont donnés un coup de volée de l'ASIC. Le chemin lent a été utilisé dans le passé pour illustrer comment les coups de volée à la CPU LC étaient plus lents que l'ASIC. Plus le terme générique, central de traitement CPU, est utilisé dans ce document.
- Coups de volée ASIC — Les ASIC ont les enveloppes strictes de conception. Quand un paquet dépasse l'enveloppe conçue, il obtient donné un coup de volée de l'ASIC à traiter sur le LC prenant en charge la CPU ou envoyé jusqu'au processeur d'artère (RP). paquets basés sur ASIC de coup de volée d'ACLs qui tombent en dehors de la conception de l'ASIC. Un exemple est un ACL qui a ACE avec un log ou un mot clé log-input. Les informations requises pour se connecter le paquet doivent être traitées en dehors de l'ASIC, ainsi le paquet est automatiquement donné un coup de volée hors de l'ASIC, dans la CPU LC, et traité comme un ACL central de traitement CPU normal.

Remarque: Quand vous configurez la Gestion de réseau à base de règles avec des déclarations de correspondance pour apparier ACLs, l'ACLs ne devrait pas apparier le port de source. Le routeur de commutateur de gigabit (GSR) ne prend en charge pas la commutation de matériel pour les PBR avec ACLs qui apparient le port de source. Il déclenche la commutation de processus et la représentation GSR dégrade.

Filtrage plat de contrôle et de Gestion

Le processeur du routeur fournit des services plats de contrôle et de Gestion en architecture distribuée de la gamme Cisco 12000. Recevez le chemin ACLs (rACLs) fournissent une capacité de filtrage distribuée simple pour le contrôle et le trafic d'administration destiné pour le RP. Il peut être logiquement visualisé comme couche de sécurité supplémentaire qui tire profit des forces d'une architecture distribuée.

En configurant l'IP recevez le chemin ACLs

Le rACL a été introduit par une levée spéciale dans la commande de puissance de maintenance de la version de logiciel 12.0(21)S2 de Cisco IOS®. Il est officiellement pris en charge dans le Logiciel Cisco IOS version 12.0(22)S. Référez-vous à l'IP reçoivent le pour en savoir plus d'ACL.

Le processeur du routeur fournit des services plats de contrôle en architecture distribuée de la gamme Cisco 12000. La réception ACLs fournissent des capacités de filtrage pour le trafic de contrôle destiné pour le RP, tel que des mises à jour de routage et des requêtes de Protocole

SNMP (Simple Network Management Protocol).

Le rACL est considéré Phase 1 d'un effort multiphasé d'ajouter de nouvelles protections au contrôle et à la Gestion du trafic plat. De nouvelles améliorations de limitation de débit sont ajoutées par des mises à jour logicielles.

Support d'ACL d'ipv4 par le type de linecard

Les linecards de gamme 12000 fournissent différentes capacités d'ACL par type de moteur. Cette section décrit les capacités d'ACL des différentes engines de linecard. Pour les informations de support d'ACL pour une engine de carte de ligne particulière, voyez la section correspondante de ce document.

Il y a certaines caractéristiques générales pour tout l'ACLs (ASIC et CPU basés) :

- Seulement un ACL peut être appliqué à une interface pour chaque direction. Par exemple, l'interface pos 0/0 peut avoir seulement un ACL en entrée et un ACL de sortie.
- Le test du paquet contre un ACL arrête après qu'une correspondance soit trouvée. Si un ACL qui est 300 entrées longues apparie le paquet sur l'entrée de liste d'accès (ACE) #45, alors le paquet est traité et le traitement d'ACL est arrêté.
- Il y a un implicite **refusent toute l'**entrée à la fin de chaque ACL. En conséquence, s'il n'y a aucune correspondance sur l'ACL, le paquet obtient relâché. Cisco ACLs sont créés avec l'architecture *explicite d'*ACL d'*autorisation*. Ceci signifie qu'il doit y a ACE pour apparier le paquet pour qu'il soit traité et expédié.
- des as Nouveau-ajoutés sont toujours ajoutés à la fin de l'ACL. Toutes les fois que l'ACL exige des mises à jour, l'il est conseillé de retirent l'ACL (n'utilisez l'**aucune commande access-list**) et re-ajoutent le nouvel ACL.
- Puisque les fragments IP de non-initiale ne contiennent pas les informations de protocole de la couche 4 dans l'en-tête IP, seulement le critère de correspondance standard est pris en charge pour des fragments non initiaux. Des détails complets sur la façon dont Cisco ACLs sont conformes au filtrage de fragment IP peuvent être trouvés dans les listes de contrôle d'accès et les fragments IP.
- ACLs numéroté sont traités et appliqués dès qu'ils seront entrés par l'interface de ligne de commande (CLI). Avec grand ACLs, ceci a parfois comme conséquence un pic CPU sur le RP ou la CPU LC.

Engine 0 - Traitement d'ACL

L'engine 0 est le premier linecard livré pour le Cisco 12000. Il est tous les traitement et transmission centraux de traitement CPU. Par conséquent, les linecards de l'engine 0 traitent ACLs dans la CPU LC.

Ces linecards sont basés sur l'engine 0 :

Type de linecard	Type d'interface	Connectivité
DS3 12 x	Coaxial	PME
DS3 12 x	Coaxial	PME
12 E3 x	Coaxial	PME

1xCHOC12->DS3		L'IR
1xCHOC12/STM4 ->OC3/STM1	POS	L'IR
4xOC3c/STM1c	POS	SR
4xOC3c/STM1c	POS	LA LR
4xOC3c/STM1c	POS	Millimètre
1xOC12c/STM4c	POS	L'IR
1xOC12c/STM4c	POS	Millimètre
6xCT3->DS1		PME
2xCHOC3/STM1->DS1/E1		L'IR
4xOC3c/STM1c	Atmosphère	L'IR
4xOC3c/STM1c	Atmosphère	Millimètre
1xOC12c/STM4c	Atmosphère	L'IR
1xOC12c/STM4c	Atmosphère	Millimètre

Critère de correspondance pris en charge

Toute la version du logiciel Cisco IOS ACL standard et étendu 12.0S, et Turbo ACLs sont prises en charge sur l'engine 0.

Nombre d'as pris en charge

La taille d'ACL est limitée seulement par des exigences de marche et des ressources en mémoire disponible.

Traitement d'ACL de sortie

La sortie ACLs sont traitées dans le chemin de caractéristique d'entrée des autres linecards dans le système. Un pousser de l'ACL de sortie au côté d'entrée de l'autre LCS protège le fond de panier contre les transferts des paquets qui vont être lâchés. C'est une fonction héritée de l'architecture distribuée sur le Cisco 7500. Une explication détaillée, des raisons, et des instructions opérationnelles sont fournies dans l'ACL de sortie d'ipv4 - matrice d'interopérabilité de linecard.

Commandes de particularité de linecard

Aucun.

Instructions et interactions opérationnelles de linecard

- Si le NetFlow est configuré sur un linecard de l'engine 0 et un ACL de sortie est configuré sur un linecard 3 ou 4+ d'engine de sortie, l'ACL de sortie est traité par les linecards d'entrée et de sortie afin de permettre au NetFlow pour expliquer des paquets refusés par ACLs aussi bien que paquets expédiés.

Recommandations

Cisco recommande l'utilisation de Turbo ACLs sur l'engine 0 pour grand ACLs. Petit ACLs Linéaire sont plus efficace pour plus petit ACLs parce que Turbo ACLs exigent la mémoire supplémentaire.

Engine 1 - Traitement d'ACL

Aperçu

Le linecard de l'engine 1 est une passerelle entre le traitement central de traitement CPU sur l'engine 0 et l'expédition de première génération/caractéristique ASIC sur les linecards de l'engine 1 de l'engine 2. ACLs de processus en logiciel par défaut. Avec le Logiciel Cisco IOS version 12.0(10)S et plus tard, l'engine 1 fournit le matériel ACLs pour des cartes équipées des versions 4 ou 5 du Salsa ASIC (voyez la référence de commandes de linecard ci-dessous pour déterminer avec quelle version de Salsa une carte particulière est équipé).

Ces linecards sont basés sur l'engine 1 :

Type de linecard	Type d'interface	Connectivité
8xFE	(RJ45)	100BaseT
8xFE	(Millimètre)	100BaseF
8xFE	(RJ45)	100BaseT
8xFE	(Millimètre)	100BaseF
1xGE	SX,	GBIC :
1xGE	SX,	GBIC :
2xOC12c/STM4c	DPT	L'IR
2xOC12c/STM4c	DPT	LA LR
2xOC12c/STM4 c	DPT	XLR
2xOC12c/STM4c	DPT	Millimètre
2xOC12c/STM4c	DPT	L'IR
2xOC12c/STM4c	DPT	LA LR
2cOC12c/STM4c	DPT	XLR
2xOC12c/STM4c	DPT	Millimètre

Critère de correspondance pris en charge

Tous les standard pris en charge par 12.0S de version du logiciel Cisco IOS, étendus, et Turbo ACLs sont pris en charge dans la CPU LC (chemin lent). En outre, l'engine 1 peut entrée de traitement ACLs dans le Salsa ASIC. Le Salsa ASIC manipule l'ACL en entrée traitant avec la recherche de route, ayant pour résultat des performances accrues une fois comparé à l'ACL Linéaire traditionnel traitant et traitement d'ACL de Turbo. Le Salsa ASIC ne peut pas traiter les ACLs de sortie ou la sous-interface ACLs.

Nombre d'as pris en charge

La taille d'ACL est limitée seulement par des exigences de marche et des ressources en mémoire

disponible.

Traitement d'ACL de sortie

La sortie ACLs sont traitées dans le chemin de caractéristique d'entrée des autres linecards dans le système. Voyez l'ipv4 sortir l'ACL - Pour en savoir plus de section Tableau d'interopérabilité de linecard.

Commandes de particularité de linecard

- **Salsa de matériel de liste d'accès**
- **show controller l3 | incluez l'ASIC**

Instructions et interactions opérationnelles de linecard

- Le Salsa ASIC et PSA ASIC ne peut pas être actionné en même temps. **La commande Hardware de liste d'accès** reçoit seulement PSA (engine 2) ou Salsa (engine 1) mais pas chacun des deux.
- Si le NetFlow est configuré sur un linecard de l'engine 1 et un ACL de sortie est configuré sur un linecard 3 ou 4+ d'engine de sortie, l'ACL de sortie est traité par les linecards d'entrée et de sortie afin de permettre au NetFlow pour expliquer des paquets refusés par ACLs aussi bien que paquets expédiés.

Recommandations

Pour des versions des linecards de l'engine 1 qui ne prennent en charge pas le matériel ACLs, Cisco recommande l'utilisation de Turbo ACLs pour grand ACLs. Petit ACLs (moins de 20 lignes) peut être mis en application en tant qu'ACLs Linéaire pour économiser la mémoire.

Engine 2 - Traitement d'ACL

Aperçu

L'Engine 2 était le premier linecard avec un expédition/configuration ASIC. Avec le Logiciel Cisco IOS version 12.0(10)S et plus tard, les linecards d'Engine 2 fournissent des capacités d'ACL de matériel dans la commutation par paquets à rendement élevé ASIC (PSA). Comme avec tous les expédition/configuration ASIC, les enveloppes strictes de performances placent des bornes sur la capacité de l'ASIC. L'enveloppe de performances de clé sur l'Engine 2 ACLs sont due aux limites de mémoire dans la PSA ASIC.

Le transfert de paquet dans l'Engine 2 est fait par la PSA ASIC. La PSA a trois mémoires externes principales :

- PLU (Chemin-consultation) — Utilisé pour enregistrer des Noeuds de mtrie
- TLU (consultation de Tableau) — Utilisé pour enregistrer des feuilles de FIB et probablement des structures de loadbalance. Également utilisé pour tenir plusieurs des structures de données d'ACL PSA
- SRAM — L'emplacement primaire pour des structures de loadshare

La fonctionnalité d'ACL PSA est une implémentation basée sur microcode de vérifier d'ACL. Un jeu d'instructions spécial est chargé dans la puce PSA qui tient compte de vérifier de base d'ACL. Il y a un certain nombre de limites à cette caractéristique qui devrait être soigneusement comprise avant de déployer. Un inconvénient majeur à PSA ACLs est un grand nombre de mémoire d'expédition de matériel exigée.

La fonctionnalité d'ACL PSA exige d'un grand bloc de mémoire PLU/TLU d'être préaffecté indépendamment du nombre de préfixes, etc. Puisque cette allocation est livré principalement de la zone TLU, elle a un impact important sur le nombre d'artères qui peuvent être mises à jour sur ces cartes quand PSA ACLs sont configurées.

En plus de la sortie initiale de la mémoire PLU/TLU, chaque préfixe enregistré dans la mémoire TLU exige sensiblement plus de mémoire. La quantité de mémoire exigée pour chaque préfixe varie, basé sur la direction de l'ACL appliqué (d'entrée contre le de sortie) et du type de linecard. Généralement le de sortie ACLs exigent plus de mémoire que le d'entrée, et les linecards avec plus de ports physiques exigent plus de mémoire cette ceux avec moins ports.

Dans le point de droit où le linecard d'Engine 2 n'utilise pas ACLs, les structures de données pour l'ACL sont établies indépendamment d'ACLs réel ont configuré. Afin de changer en les structures plus petites de non-ACL, vous ne devez configurer **aucun matériel PSA de liste d'accès** sur le routeur. Cette commande désactive tout l'ACL traitant sur tous les linecards Engine2 dans toutes les directions. Recommeds de Cisco pour les utiliser avec l'extrême prudence.

Aperçu

Afin de fournir l'ACL traitant les performances qui sont indépendant de profondeur de correspondance, l'Engine 2 ACLs sont intégrés dans la table d'expédition de matériel. Voir ci-dessous pour des explications sur la façon dont ceci peut affecter l'évolutivité de préfixe.

Ces linecards sont basés sur l'Engine 2 :

Type de linecard	Type d'interface	Connectivité
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LA LR
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LA LR
1xOC192c/STM64c	Enabler	SR
16xOC3c/STM1c	POS	L'IR
16xOC3c/STM1c	POS	Millimètre
4xOC12c/STM4c	POS	L'IR
4xOC12c/STM4c	POS	Millimètre
4xOC12c/STM4c	POS	L'IR
4xOC12c/STM4c	POS	Millimètre
4xOC12c/STM4c	Atmosphère	L'IR

4xOC12c/STM4c	Atmosphère	Millimètre
8xOC3cSTM1c	ATM/TS	L'IR
8xOC3c/STM1c	ATM/TS	Millimètre
3xGE	SX	GBIC :
3xGE	CWDM	GBIC :
1xOC48c/STM16c	DPT	SR
1xOC48c/STM16c	DPT	LA LR
1xOC48c/STM16c	DPT	SR
1xOC48c/STM16c	DPT	LA LR

Critère de correspondance pris en charge

Toute la version du logiciel Cisco IOS 12.0S a pris en charge le critère de correspondance standard et étendu d'ACL, excepté des ports de source de la couche 4. Des ports des masques, les champs de Priorité IP, et de la source discontinus de la couche 4 sont donnés un coup de volée de la PSA ASIC et traités sur la CPU LC.

Nombre d'as pris en charge

Jusqu'à cinq ACLs en entrée 448-line dans la PSA. Un ACL peut être configuré par port. ACLs supplémentaire sont gérés par la CPU de linecard. Voyez la section de « restrictions » ci-dessous pour des restrictions sur des ACLs de sortie.

Traitement d'ACL de sortie

Un ACL de sortie configuré sur ce linecard sera exécuté dans le chemin de caractéristique d'entrée des autres linecards dans le système. Voyez l'ipv4 sortir l'ACL - Matrice d'interopérabilité de linecard pour des détails.

Commandes de particularité de linecard

- **limite 128 du matériel PSA de liste d'accès**
- **aucun matériel PSA de liste d'accès**
- **contournement PSA**
- **affichez le détail de la liste d'accès PSA**
- **affichez le résumé de la liste d'accès PSA**
- **caractéristique du show controller PSA**

Instructions et interactions opérationnelles de linecard

- Le traitement d'ACL de chemin rapide exige de ces conditions d'être remplies :L'ACL appliqué est dans le 128- ou le 448- ACE limitent.La longueur doit être moins de 128 as si la commande de la **limite 128 du matériel PSA de liste d'accès** est configurée.La longueur doit

être moins de 448 as quand le lot de microcode de l'ACL 448-line est exigé.L'entrée et sortie ACLs ne sont pas configurées ensemble par carte.Jusqu'à cinq ACLs de sortie peuvent être configurés sur le *routeur*.
- Seulement 128-line ACLs sont pris en charge sur des linecards de 8 et de POS 16-port OC-3/STM-1. 448 la ligne ACLs sont prises en charge sur le POS 4-port OC-12/STM-4, le POS 1-port OC-48/STM-16, et les linecards des Gigabit Ethernet 3-port.
- La priorité de prise d'ACLs d'entrée dans le chemin rapide au-dessus des ACLs de sortie quand chacun des deux sont configurés simultanément sur la même carte (l'ACL de sortie est traitée dans le chemin lent).
- Si un ACL de sortie est configuré sur une carte d'Engine 2, et la carte de ligne d'entrée est l'engine 0/1/2/4, un ACL de sortie sera traité dans la carte d'entrée. Pour d'autres types de moteur, l'ACL de sortie sera traité dans le chemin lent de sortie d'Engine 2.
- La sortie ACLs ne sont pas prises en charge pour le trafic IP-à-MPLS (premiers mpls label « étant poussés » sur un paquet IP).
- Les informations de traitement d'ACL sont intégrées dans le FIB de matériel et peuvent affecter l'évolutivité de préfixe. L'épuisement de mémoire de préfixe est signalé par des défaillances d'allocation de mémoire avec la signature « exmem=1 » dans le message de log de accompagnement.

Recommandations

- Les informations de traitement d'ACL sont intégrées dans la table d'expédition de CEF, qui réduit l'évolutivité de préfixe. Les applications qui n'utilisent pas ACLs peuvent désactiver le support d'ACL dans la table CEF et augmenter de ce fait la mémoire disponible de préfixe en n'émettant l'**aucune** commande du **matériel PSA de liste d'accès**.
- La configuration de l'**aucune** commande du **matériel PSA de liste d'accès** désactive tout l'ACL traitant par des cartes d'Engine 2 en plus de désactiver le soutien PSA d'ACLs. Il ne force pas l'exécution de logiciel d'ACLs. Cette condition s'applique également si le linecard de sortie a un ACL de sortie configuré.
- La configuration de la commande d'**access-list compiled** après la commande du **matériel PSA de liste d'accès** convertit les as qui dépassent la capacité de la PSA dans un ACL de Turbo. Ceci fournit la représentation optimale d'ACL pour ACLs plus de 448 as de longueur.Le microcode par défaut d'ACL est 128 (comme de version du logiciel Cisco IOS 12.0(14)S/ST). Si plus petit ACLs sont en service et la capacité 448-line n'est pas exigée, configurant le **matériel PSA de liste d'accès limitez 128 que la** commande économise la mémoire de l'expédition (TLU), qui améliore l'évolutivité de préfixe).Le traitement d'ACL de Turbo devrait être activé avec la commande d'**access-list compiled** pour de plus longues que 129 lignes d'ACLs avec la commande de la **limite 128 du matériel PSA de liste d'accès**. Cette combinaison traite les 128 premières lignes dans la PSA ASIC et les lignes restantes avec Turbo ACLs, qui optimise la représentation tout en économisant expédiant la mémoire.
- La carte de ligne ATM 4-port OC12 ne prend en charge pas des ACLs en entrée, mais fournit la détection d'ACL de sortie dans le microcode, qui permet le processus des ACLs de sortie dans le chemin lent.
- La carte de ligne ATM 8xOC3 prend en charge la ligne du par-circuit virtuel 128 ACLs avec le Logiciel Cisco IOS version 12.0(23)S et plus tard. Un maximum de 16 ACLs en entrée distincts peut être configuré dans le chemin rapide. l'ACL 448-input est pris en charge sur une base de par-circuit virtuel dans le chemin lent seulement. La sortie ACLs ne sont pas prises

en charge.

Engine 3 ISE (engine de Services IP) - traitement d'ACL

Aperçu

L'engine 3 est le premier double linecard d'expédition d'étape. L'engine 3 a l'expédition/caractéristique ASIC sur le chemin d'entrée et de sortie. Ceci permet ACLs à placer dans l'ASIC sur les chemins d'entrée et de sortie. En outre, la structure de l'engine 3 ASIC est un pipeline/baie hybrides de parallèle. La structure ASIC implémente l'ACL traitant dans la mémoire associative ternaire ultra-rapide parallèle (TCAM), qui fournit le traitement de ligne-débit de jusqu'aux as 20K par d'entrée, et 20K ACEs par de sortie.

Ces linecards sont basés sur l'engine 3 :

Type de linecard	Type d'interface	Connectivité
4xOC12c/STM4c	POS	L'IR
4xOC12c/STM4c	POS	Millimètre
4xCHOC12/STM4->OC3/STM1->DS3/E3	POS	L'IR
16xOC3c/STM1c	POS	L'IR
16xOC3c/STM1c	POS	Millimètre
8xOC3/STM1c	POS	L'IR
8xOC3c/STM1c	POS	Millimètre
4xOC3c/STM1c	POS	L'IR
4xOC3c/STM1c	POS	Millimètre
4xOC3c/STM1c	POS	LA LR
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LA LR
1xCHOC48/STM16->STM4->OC3/STM1->DS3/E3	POS	SR
4xOC12c/STM4c	ATM/IP	L'IR
4xOC12c/STM4c	ATM/IP	Millimètre
4xGE	GE	
4xOC12c/STM4c	DPT	L'IR
4xOC12c/STM4c	DPT	XLR

Critère de correspondance pris en charge

Toute la version du logiciel Cisco IOS critère de correspondance standard et étendu 12.0S sont prises en charge dans le chemin rapide excepté les as de log qui sont traités par la CPU de linecard.

Nombre d'as pris en charge

- Rayez le débit traitant dans le d'entrée et la direction de sortie par port, par VLAN, par sous-interface de relais de trame, et par sous-interface atmosphère. Jusqu'à 20,000 as étendus par direction et par carte sont pris en charge.
- Le critère de correspondance pour la source/destination port TCP/UDP « plage », « lt », et « gt » est tout manipulé dans le matériel utilisant « des ressources en opérateur L4 ».
- Le nombre d'opérandes L4 distincts est limité à 32 pour le linecard entier. Des opérateurs de port de source sont limités à un maximum de six.

Traitement d'ACL de sortie

Soutien indigène de rapide-chemin de l'ACL de sortie de ligne-débit traitant dans le traitement de paquets ASIC de transmettre-chemin. Voyez l'ipv4 sortir l'ACL - Matrice d'interopérabilité de linecard pour des détails.

Commandes de particularité de linecard

- **le tcam de** *#>* ***de*** **<slot de hw-module compilent la NO--fusion***! ---12.0(21)S3*
- *nom de* **<interface d'interface de matériel d'exposition-Access-liste >**
- **POS du show cef international [***x/y***] | if_number inc.**

Instructions et interactions opérationnelles de linecard

- Des paquets s'assortissant se connectant des as sont traités dans le chemin lent.
- Des paquets qu'apparier refusent des as (étranglés pour s'assurer contre l'interruption de système) sont traités dans le chemin lent.
- Quand un ACL inclut une plage d'adresses, les as spéciaux d'utilisations de matériel appelés la « plage ACEs » qui exigent jusqu'à trois as.
- Le fusionnement d'ACL peut économiser des ressources TCAM en partageant les as communs à travers ACLs individuel. Pour déterminer si un ACL est fusionné, utilisez la **commande d'interface de matériel d'exposition-Access-liste**.
- Des compteurs d'ACL ne sont pas pris en charge pour ACLs fusionné. Avec le Logiciel Cisco IOS version 12.0(21)S3 et plus tard, le fusionnement d'ACL peut être désactivé avec le **tcam de #> de <slot de hw-module compilent la** commande de NO--**fusion**. Afin de déterminer si un ACL est fusionné, utilisez la **commande d'interface de matériel d'exposition-Access-liste**.
- Si le NetFlow est configuré sur un linecard de l'engine 0/1 et un ACL de sortie est configuré sur un linecard 3 ou 4+ d'engine de sortie, l'ACL de sortie sera traité par les linecards d'entrée et de sortie afin de permettre au NetFlow pour expliquer des paquets refusés par ACLs aussi bien que paquets expédiés.

Support de compteur d'ACL

	Per-ACE	Per-ACE (hardware counters)	Aggregate
21S3/ST3		X	
22S		X	X
23S	X	X	X

Définitions :

- PAR-ACE — Le support logiciel normal de Cisco IOS, le **<number de liste d'accès d'exposition >** commande sur le RP/LC affiche l'ACL et le compteur associés avec chaque ACE. Il est disponible seulement quand la **fusion** est désactivée avant que vous configuriez n'importe quel ACLs. Ceci peut être fait à l'aide de cette commande de configuration :`Router(config)#hw-module slot <number> tcam compile acl no-merge` Cette option une fois activée arrête des optimisations de fusion certain TCAM et affecte l'évolutivité. L'effet précis dépend d'ACLs individuel.Notez également que les compteurs ne seront pas corrects si le routage basé sur la politique est appliqué sur cette interface. Dans ce cas, l'agrégat contre- devrait être utilisé.
- Par-ACE (TCAM) — Compteurs matériels associés avec chaque entrée TCAM. Aucune configuration n'est nécessaire et il n'y a aucune incidence sur la représentation/évolutivité. Disponible seulement sur le linecard utilisant ce CLI. Ces compteurs ne peuvent pas être effacés par le logiciel.`LC-Slot4#show contr tofab alpha acl <if-number> vmr2ace` Un nouveau CLI générique pour cette commande sera disponible dans la version du logiciel Cisco IOS 22S :`LC-Slot4#show access-list hardware interface p0:1 in` Comme avec par-ACE contre-, les compteurs TCAM sont valides seulement quand PBR n'est pas utilisé sur cette interface avec l'ACL.
- Agrégat — Chaque ACL affiche qu'une autorisation récapitulative/refusent le compteur. C'est la somme de tous les différents compteurs d'ACE. Aucune configuration n'est nécessaire et il n'y a aucune incidence sur la représentation ou l'évolutivité.

Recommandations

Aucun à ce moment.

Engine 4 (POS) - Traitement d'ACL

Aperçu

L'engine 4 fournit à ce support d'ACL le Logiciel Cisco IOS version 12.0(18)S et plus tard :

- La sortie ACLs sont prises en charge sur les linecards E0/1/2 si un linecard de l'engine 4 est la carte d'entrée. Dans cette configuration, l'ACL de sortie est traité par la CPU de linecard de sortie.

Ces linecards sont basés sur l'engine 4 :

Type de linecard	Type d'interface	Type de moteur	Connectivité
4xOC48c/STM16c	POS	E4	
4xOC48c/STM16c	POS	E4	LA LR
1xOC192c/STM64c	POS	E4	L'IR
1xOC192c/STM64c	POS	E4	SR

1xOC192c/STM64c	POS	E4	VSR-1
10xGE	SFP	E4	

Engine 4+ (POS et DPT) - traitement d'ACL

Aperçu

L'engine 4+ introduit la fonctionnalité d'ACL au dossier de la gamme Cisco 12000 10-Gigabit.

Jusqu'à 1024 as sont pris en charge dans chacun des chemins d'entrée et de sortie. Les deux l'entrée et sortie ACLs sont traitées à la ligne débit pour jusqu'à 96 as. La représentation pour de plus longues correspondances varie avec la profondeur de correspondance.

Ces linecards de POS sont basés sur l'engine 4+ :

Type de linecard	Type d'interface	Connectivité
4xOC48c/STM16c	POS	SR
4xOC48c/STM16c	POS	LA LR
1xOC192c/STM64c	POS	L'IR
1xOC192c/STM64c	POS	SR
1xOC192c/STM64c	POS	VSR-1
1xOC192/STM64c	POS	LA LR
4xOC48c/STM16c	DPT	SFP :
1xOC192c/STM64c	DPT	L'IR
1xOC192c/STM64c	DPT	SR
1xOC192c/STM64c	DPT	VSR-1
1xOC192c/STM64c	DPT	LA LR

Critère de correspondance pris en charge

Toute la version du logiciel Cisco IOS 12.0S a pris en charge standard et des critères étendus d'ACL sont pris en charge dans le chemin rapide excepté le log ou fragmentent des as.

Nombre d'as pris en charge

Jusqu'à 1024 as sont par-direction prise en charge dans le chemin rapide.

Remarque: 1021 des as sont configurables. Trois entrées en sont réservées pour l'**IP** implicite **tout d'autorisation d'**as, **refusent l'IP tout**, et **l'envoient aux** commandes **CPU**.

Il n'y a aucune limite supérieure au nombre d'as pris en charge. Tous les as au delà de la limite 1021 sont exécutés dans le chemin lent de linecard.

Traitement d'ACL de sortie

La sortie ACLs sont traitées dans le chemin rapide de transmettre-side. Voyez l'ipv4 sortir l'ACL - Matrice d'interopérabilité de linecard pour des détails.

Commandes de particularité de linecard

- **show tcam APPL [acl-***dans* **/ tcam d'***acl***-] <label-aucun >**
- **show tcam APPL [acl-***dans* **/ <port de mémoire d'***acl***-] > <number des** *entrées* **>**

Instructions et interactions opérationnelles de linecard

- La sous-interface ACLs ne sont pas prises en charge.
- La représentation varie avec la profondeur de correspondance.
- Règles d'ACL de l'utilisation deux d'entrées de plage (trois si les deux entrées croisent une borne).
- Un ACL est pris en charge par interface physique.
- Jusqu'à 1024 as (par direction) sont pris en charge dans le chemin rapide.
- Des 1024 as l'uns des de chemin rapide peuvent être partagés à travers des ports.
- Des as qui utilisent le mot clé de fragment sont filtrés dans le chemin lent.
- Des paquets refusés ne sont pas comptés pour des as étant traités dans le chemin lent.
- Si le NetFlow est configuré sur un linecard de l'engine 0 et un ACL de sortie est configuré sur un linecard 3 ou 4+ d'engine de sortie, l'ACL de sortie sera traité par les linecards d'entrée et de sortie pour permettre au NetFlow pour expliquer des paquets refusés par ACLs aussi bien que paquets expédiés.

Recommandations

Aucun à ce moment.

Engine 4+ (Ethernets) - Traitement d'ACL

Aperçu

Les cartes de ligne Ethernet de l'engine 4+ introduisent la fonctionnalité d'ACL en entrée de par-VLAN dans le matériel au dossier d'Ethernet 10 gigabits de Cisco 12000. Ce sont certaines des caractéristiques :

- L'entrée et sortie ACLs peut être appliquée simultanément sur un port unique sans incidence des performances.

- ACLs peut être appliqué par VLAN ou par port.
- La représentation d'ACL d'entrée jusqu'aux as 15K ne dégrade pas avec la profondeur de correspondance.
- La sortie ACLs sont traitées à la ligne débit pour jusqu'à 96 as. La représentation pour de plus longues correspondances varie avec la profondeur de correspondance.

Ces cartes de ligne Ethernet sont basées sur l'engine 4+ :

Type de linecard	Type d'interface	Type de moteur
10xGE Rév B (« X-B »)	SFP :	E4+
Modulaire	SFP :	E4+
1x10GE	10G	E4+
1x10GE	10G	E4+

Critère de correspondance pris en charge

Toute la version du logiciel Cisco IOS 12.0S a pris en charge standard et des critères étendus d'ACL sont pris en charge dans le chemin rapide excepté le log ou fragmentent des as.

Nombre d'as pris en charge

- Jusqu'à 15,000 ACLs en entrée qui peuvent être configurés par port ou par VLAN.
- 1024 sortent des as par carte qui peut être appliquée sur a par base de port.**Remarque:** 1021 des as sont configurables. Trois entrées en sont réservées pour l'**IP** implicite **tout d'autorisation d'**as, **refusent l'IP tout**, et **l'envoient aux** commandes **CPU**.

Traitement d'ACL de sortie

La sortie ACLs sont traitées à la façon des indigènes dans le chemin rapide de transmettre-side. Voyez l'ipv4 sortir l'ACL - Pour en savoir plus de matrice d'interopérabilité de linecard.

Commandes de particularité de linecard

- **<number de hw-module slot > fusion d'acl d'IP**

Instructions et interactions opérationnelles de linecard

- Des as qui contiennent le mot clé de fragment sont traités dans le chemin lent.
- Des compteurs d'ACL ne sont pas pris en charge pour ACLs ont combiné avec d'autres configurations.
- Des compteurs d'ACL ne sont pas pris en charge pour ACLs fusionné. ACLs fusionné sont configurable avec la commande de *nombre de* **<slot de hw-module slot > de fusion d'acl d'IP**.
- Des exécutions hautes to168 L4 sont prises en charge par linecard. Une fois que ceci est dépassé, l'ACL est exécuté dans le chemin lent.
- Si un linecard de l'engine 1 a échantillonné le NetFlow activé et un ACL de sortie est activé sur un linecard 3 ou 4+ d'engine de sortie, l'ACL de sortie est traité par les linecards d'entrée

et de sortie afin de permettre au NetFlow pour expliquer des paquets refusés par ACLs aussi bien que paquets expédiés.

Recommandations

Aucun à ce moment.

Se connecter d'ACL

Avant Logiciel Cisco IOS version 12.0(21)S, les informations de journalisation d'ACL ont été envoyées au RP exclusivement au-dessus du bus de maintenance (MBUS). Pendant les hauts niveaux de l'ACL se connectant l'activité, il était possible de dépasser la capacité du MBUS. Le Logiciel Cisco IOS version 12.0(21)S introduit plusieurs optimisations qui empêchent ce scénario.

Des situations de surcharge MBUS sont signalées par le logiciel de Cisco IOS avec ces messages d'erreur :

```
LCLOG-3-INVSTATE
```

```
MBUS_SYS-3-SEQUENCE
```

Avec le Logiciel Cisco IOS version 12.0(21)S et plus tard, des messages de journalisation de à sévérité élevée (sévérité 0-4) sont fournis au RP par le MBUS tandis que des messages de log inférieurs de sévérité (sévérité 5-7) sont fournis au RP par la matrice de plus grande capacité de commutation. Les messages de log d'ACL sont à sévérité élevée, ainsi sont maintenant livrés au RP par la matrice de commutation.

C'ajouté se connectant la fonctionnalité est configurable utilisant ces commandes :

- **se connectant le mbus de méthode [***sévérité***]** — Détermine quels messages, par sévérité, seront envoyés au RP utilisant le MBUS. Des messages plus élevés de sévérité seront envoyés par la matrice de commutateur.
- **méthode de show logging** — Affiche la méthode se connectante en cours pour tous les niveaux de gravité du message.
- **se connectant l'ordre-nums** — Ce commandes enables le linecard de envoi aux messages de log de numéro de séquence de sorte que des messages puissent être correctement commandés à nouveau par le RP. Sans cette commande, des messages de log peuvent être fournis au RP dans la commande non séquentielle.

ACL de sortie d'ipv4 - Matrice d'interopérabilité de linecard

Avant que l'introduction de l'ACL de sortie traitant avec la release de l'engine 3 et de l'engine 4+, des ACLs de sortie aient été traitées par la carte de ligne d'entrée. La sortie ACLs ont été mises à jour des capacités de traitement pour tirer profit de hautes performances de l'engine 3 et de l'engine 4+ d'ACL de sortie.

Ce tableau fournit un résumé d'où des ACLs de sortie sont traités pour différentes combinaisons de linecard :

	Linecard de sortie

Carte de ligne d'entrée (ACL de sortie appliqué à l'interface de membre)	E0	E1	E2	E3	E4	E4+
E0	D'entrée	D'entrée	D'entrée	De sortie	S/O	De sortie
E1	D'entrée	D'entrée	D'entrée	De sortie	S/O	De sortie
E2	D'entrée	D'entrée	D'entrée	De sortie	S/O	De sortie
E3	De sortie	De sortie	De sortie	De sortie	S/O	De sortie
E4	De sortie	De sortie	De sortie	De sortie	S/O	De sortie
E4+	De sortie	De sortie	De sortie	De sortie	S/O	De sortie

Support d'ACL d'IPv6

ACLs étendu par IPv6 sont pris en charge dans le chemin lent (d'entrée et de sortie) sur E0, E1, E2, E3, et E4+ dans le Logiciel Cisco IOS version 12.0(23)S.

Dans l'engine 3, la fonctionnalité d'ACL d'IPv6 est prise en charge dans le matériel dans le Logiciel Cisco IOS version 12.0(25)S. ACLs sont appliqués à une interface spécifique, avec une instruction de refus implicite à la fin de chaque liste d'accès. L'IPv6 ACLs sont configurés utilisant la commande d'**ipv6 access-list** avec le refuser et permettent des mots clé en mode de configuration globale. Les cartes de l'engine 3-based prennent en charge le filtrage des en-têtes basées sur trafic d'option d'IPv6, des étiquettes d'écoulement, et sur option, les informations de type de protocole de couche supérieure.

Référence de commandes d'ACL de Cisco 12000

Commandes de l'engine 1

- Salsa de matériel de liste d'accès
- show controller l3 | incluez l'ASIC

Commandes d'Engine 2

- limite 128 du matériel PSA de liste d'accès
- aucun matériel PSA de liste d'accès
- contournement PSA
- affichez le détail de la liste d'accès PSA
- affichez le résumé de la liste d'accès PSA
- caractéristique du show controller PSA

Commandes de l'engine 3

- le tcam de *#> de* <slot de hw-module compilent la NO--fusion*! ------ en date du Logiciel Cisco IOS version 12.0(21)S3*
- *nom de* <interface d'interface de matériel d'exposition-Access-liste >
- affichez le contr [*tofab*/alpha <int d'acl de *frfab*] > vmr2ace

Commandes de l'engine 4+

- affichez l'étiquette de la liste d'accès gen7
- show tcam APPL [acl-*dans* / tcam d'*acl*-] <label-aucun >
- show tcam APPL [acl-*dans* / ><number de <port de mémoire d'*acl*-] des *entrées* >

Commandes d'Ethernets de l'engine 4+

- <number de hw-module slot > fusion d'acl d'IP

Glossaire

Cette section fournit des définitions standard des termes appropriés :

- **Plans du traitement** — Un périphérique de réseau peut être logiquement divisé en trois plans de traitement :Plan de données — Traitement sur les paquets traversant le périphérique de réseau.Avion de contrôle — Traitement sur les paquets utilisés pour coller des périphériques de réseau ensemble. Ceci inclut la ligne protocoles (tels que le protocole point-à-point - PPP et contrôle de liaison de données de haut niveau - HDLC), les protocoles de routage (Border Gateway Protocol - BGP, version 2 de Routing Information Protocol - RIPv2, Shortest Path First ouvert - OSPF, etc), et les protocoles de synchronisation (tels que le Network Time Protocol - NTP).Avion de Gestion — Traitement sur les paquets qui sont utilisés pour gérer les périphériques de réseau. Ceci inclut le telnet, le Protocole Secure Shell (SSH), le Protocole FTP (File Transfer Protocol), le Protocole TFTP (Trivial File Transfer Protocol), le SNMP, et d'autres protocoles de gestion.
- **ACLs standard** — Filtre standard d'ACLs exclusivement à la couche 3.
- **ACLs étendu** — Les Listes d'accès étendues IP utilisent la source et les adresses de destination pour des exécutions assorties aussi bien que des informations facultatives de type de protocole pour la granularité plus fine du contrôle.
- **ACLs traité Linéaire** — Traité linéairement en logiciel. La représentation varie avec la profondeur de correspondance (le nombre d'entrées qui doivent être vérifiées avant qu'une correspondance soit déterminée).
- **Turbo ACLs (compilé)** — Turbo ACLs optimisent l'ACL de logiciel transformant en compilant un ACL en gamme de tables de correspondance haut-optimisée qui expédient le traitement de logiciel. La représentation de Turbo ACLs ne varie pas avec la profondeur de correspondance.
- **Entrée ACLs** — Un ACL a appliqué au trafic entrant le port auquel il est appliqué.
- **Sortie ACLs** — Un ACL s'est appliqué pour trafiquer quittant le port sur lequel il est appliqué. À quelques exceptions, des ACLs de sortie sont traités par le linecard d'entrée.
- **Recevez le chemin ACLs** — Recevez le chemin ACLs fournissent le filtrage pour le trafic de contrôle destiné pour le routeur lui-même, tel que des mises à jour de routage et des requêtes SNMP.

- **Double linecard d'expédition d'étape** — Linecards qui ont l'expédition/caractéristique ASIC sur le d'entrée et le chemin de sortie. Ceci permet au linecard pour exécuter des caractéristiques sur chacun des deux l'écoulement de paquet d'entrée et écoulement de paquet de sortie sans donner un coup de volée des paquets à la CPU LC. Il tient compte également de nouvelles ondes de doubles algorithmes de transfert d'étape à utiliser dans le Cisco 12000. Le linecard de l'engine 3 est un exemple d'un double linecard d'expédition d'étape.
- **Linecard d'expédition d'étape unique** — Linecards qui ont l'expédition/caractéristique ASIC sur juste le chemin d'entrée. Ces linecards exécutent seulement le traitement basé sur ASIC sur les paquets qui circulent sur le chemin d'entrée. Le trafic en sortie n'est pas traité (juste expédié), est traité par le d'entrée ASIC de l'autre LCS, ou géré par la CPU LC. L'Engine 2, l'engine 4, et l'engine 4+ sont des exemples des linecards d'expédition d'étape unique.

Informations connexes

- Routeur Internet de la série Cisco 12000
- Support et documentation techniques - Cisco Systems