CoPP sur les commutateurs Cisco Nexus de la série 7000

Contenu

Introduction

Ce document décrit ce qui, comment et pourquoi la fonction CoPP (Control Plane Policing) est utilisée sur les commutateurs de la gamme Nexus 7000, qui incluent les modules F1, F2, M1 et M2 et les cartes de ligne (LC). Il comprend également des politiques de pratiques exemplaires, ainsi que la façon de personnaliser une politique CoPP.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître l'interface de ligne de commande du système d'exploitation Nexus.

Components Used

Les informations de ce document sont basées sur les commutateurs de la gamme Nexus 7000 avec module Supervisor 1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Présentation de CoPP sur les commutateurs de la gamme Nexus 7000

Le protocole CoPP est essentiel au fonctionnement du réseau. Une attaque par déni de service (DoS) sur le plan de contrôle/gestion, qui peut être perpétrée par inadvertance ou de manière malveillante, implique généralement des taux de trafic élevés qui entraînent une utilisation excessive du CPU. Le module Supervisor passe un temps excessif à traiter les paquets.

Voici quelques exemples de ces attaques :

- Requêtes d'écho ICMP (Internet Control Message Protocol).
- Paquets envoyés avec **ip-options** set.

Cela peut conduire à :

- Perte des messages de maintien de la vie et des mises à jour des protocoles de routage.
- Le remplissage des files d’attente de paquets entraîne des pertes indiscriminées.
- Sessions interactives lentes ou non réactives.

Les attaques peuvent submerger la stabilité et la disponibilité du réseau et entraîner des pannes de réseau ayant un impact sur l'entreprise.

CoPP est une fonctionnalité matérielle qui protège le superviseur des attaques DoS. Il contrôle le débit auquel les paquets sont autorisés à atteindre le superviseur. La fonctionnalité CoPP est modélisée comme une politique QoS d'entrée associée à l'interface spéciale appelée **plan de contrôle**. Cependant, CoPP est une fonctionnalité de sécurité et ne fait pas partie de la QoS. Afin de protéger le superviseur, la CoPP sépare les paquets du plan de données des paquets du plan de contrôle (Logique d'exception). Il identifie les paquets d'attaque DoS à partir de paquets valides (Classification). CoPP permet la classification de ces paquets :

- Recevoir des paquets
- Paquets de multidiffusion
- Paquets d'exception
- Rediriger les paquets
- Paquets MAC + non IP de diffusion
- Paquets MAC + IP de diffusion (voir ID de bogue Cisco CSCub47533 - Paquets du VLAN L2 (sans SVI) touchant CoPP)
- Paquets MAC + IP

- Paquets MAC + non IP du routeur
- Paquets ARP

Une fois qu'un paquet est classifié, il peut également être marqué et utilisé pour attribuer différentes priorités en fonction du type de paquet. Il est possible de configurer, de dépasser et de violer des actions (transmission, abandon, marquage). Si aucun régulateur n'est attaché à une classe, alors un régulateur par défaut est ajouté dont l'action de conformité est abandonnée. Les paquets glanés sont contrôlés avec la classe par défaut. Une fréquence, deux couleurs et deux fréquences, trois couleurs sont prises en charge.

Le trafic qui touche le processeur sur le module Supervisor peut passer par quatre chemins :

1. Interfaces intrabande (port du panneau avant) pour le trafic envoyé par les cartes de ligne.

2. Interface de gestion (mgmt0) utilisée pour le trafic de gestion.

3. Interface CMP (Control and Monitoring Processor) utilisée pour la console.

4. EOBC (Switched Ethernet Out Band Channel) pour contrôler les cartes de ligne à partir du module Supervisor et échanger des messages d'état.

Seul le trafic envoyé via l'interface Inband est soumis à CoPP, car il s'agit du seul trafic qui atteint le module Supervisor via les moteurs de transfert (FE) des cartes de ligne. L'implémentation du commutateur de la gamme Nexus 7000 de CoPP est uniquement basée sur le matériel, ce qui signifie que CoPP n'est pas exécuté dans le logiciel par le module Supervisor. La fonctionnalité CoPP (réglementation) est implémentée sur chaque FE indépendamment. Lorsque les différents taux sont configurés pour la carte de stratégie CoPP, il faut tenir compte du nombre de cartes de ligne dans le système.

Le trafic total reçu par le superviseur est N fois X, où N est le nombre de FE sur le système Nexus 7000, et X le taux autorisé pour la classe particulière. Les valeurs de régulateur configurées s'appliquent par FE, et le trafic agrégé susceptible d'atteindre le CPU est la somme du trafic conforme et transmis sur tous les FE. En d'autres termes, le trafic qui touche le processeur est égal au débit de conformité configuré multiplié par le nombre de FE.

- N7K-M148GT-11/L LC a 1 FE
- N7K-M148GS-11/L LC a 1 FE
- N7K-M132XP-12/L LC a 1 FE
- N7K-M108X2-12L LC a 2 FE
- N7K-F248XP-15 LC a 12 FE (SOC)
- N7K-M235XP-23L LC a 2 FE
- N7K-M206FQ-23L LC a 2 FE
- N7K-M202CF-23L LC a 2 FE

La configuration CoPP n'est implémentée que dans le contexte de périphérique virtuel par défaut (VDC); cependant, les politiques CoPP s'appliquent à tous les VDC. La même stratégie globale est appliquée à toutes les cartes de ligne. CoPP applique le partage de ressources entre les VDC si les ports des mêmes FE appartiennent à des VDC différents (LC de la gamme M1 ou M2). Par exemple, les ports d'un FE, même dans des VDC différents, comptent sur le même seuil pour CoPP.

Si le même FE est partagé entre différents VDC et qu'une classe donnée de trafic du plan de contrôle dépasse le seuil, cela affecte tous les VDC sur le même FE. Il est recommandé de

consacrer un FE par VDC afin d'isoler l'application CoPP, si possible.

Lorsque le commutateur est lancé pour la première fois, la stratégie par défaut doit être programmée pour protéger le **plan de contrôle**. CoPP fournit les stratégies par défaut, qui sont appliquées au **plan de contrôle** dans le cadre de la séquence de démarrage initiale.

Pourquoi CoPP sur le commutateur de la gamme Nexus 7000

Le commutateur Nexus 7000 est déployé en tant que commutateur d'agrégation ou commutateur principal. C'est donc l'oreille et le cerveau du réseau. Il gère la charge maximale dans le réseau. Il doit traiter les demandes fréquentes et en rafale. Voici quelques demandes :

- **Traitement BPDU (Spanning Tree Bridge Protocol Data Unit)** - La valeur par défaut est toutes les deux secondes.
- **Redondance du premier saut** - Ceci inclut le protocole HSRP (Hot Standby Router Protocol), le protocole VRRP (Virtual Router Redundancy Protocol) et le protocole GLBP (Gateway Load Balancing Protocol) - La valeur par défaut est toutes les trois secondes.
- **Résolution d'adresse** - Ceci inclut le protocole ARP/ND (Address Resolution Protocol/Neighbor-Discovery), le nettoyage FIB (Forwarding Information Base) - Jusqu'à une demande par seconde, par hôte, comme l'association du contrôleur d'interface réseau (NIC).
- **DHCP (Dynamic Host Control Protocol)** - Requête DHCP, relais - Jusqu'à une requête par seconde, par hôte.
- **Protocoles de routage** pour la couche 3 (L3).
- **Data Center Interconnect** - OTV (Overlay Transport Virtualization), MPLS (Multiprotocol Label Switching) et VPLS (Virtual Private LAN Service).

CoPP est essentiel afin de protéger le processeur contre les serveurs mal configurés ou les attaques DoS potentielles, ce qui permet au processeur d'avoir suffisamment de cycle pour traiter les messages du plan de contrôle critique.

Traitement du plan de contrôle sur le commutateur Nexus 7000

Le commutateur Nexus 7000 adopte une approche basée sur un plan de contrôle distribué. Il comporte un multicoeur sur chaque module d'E/S, ainsi qu'un multicoeur pour le plan de contrôle du commutateur sur le module Supervisor. Il décharge des tâches intensives sur le processeur du module d'E/S pour les listes de contrôle d'accès (ACL) et la programmation FIB. Il fait évoluer la capacité du plan de contrôle avec le nombre de cartes de ligne. Cela évite le goulot d'étranglement du processeur du superviseur, qui est perçu dans une approche centralisée. Les limiteurs de débit matériel et la CoPP basée sur le matériel protègent le plan de contrôle contre les activités malveillantes ou mauvaises.

Stratégie des meilleures pratiques CoPP

La politique CoPP sur les meilleures pratiques (BPP) a été introduite dans Cisco NX-OS version 5.2. La sortie de la commande **show running-config** n'affiche pas le contenu du BPP CoPP. La commande **show run all** affiche le contenu de CoPP BPP.

```
-----------------------------------SNIP-----------------------------------------
SITE1-AGG1# show run copp

!! Command: show running-config copp
!! Time: Mon Nov 5 22:21:04 2012

version 5.2(7)
copp profile strict


SITE1-AGG1# show run copp all

!! Command: show running-config copp all
!! Time: Mon Nov 5 22:21:15 2012

version 5.2(7)
-----------------------------SNIP--------------------
control-plane
service-policy input copp-system-p-policy-strict
copp profile strict
```

CoPP fournit quatre options à l'utilisateur pour les stratégies par défaut :

- Strict
- Moderate (modéré)
- Lénite
- Dense (introduit dans la version 6.0(1))

Si aucune option n'est sélectionnée ou si la configuration est ignorée, une réglementation stricte est appliquée. Toutes ces options utilisent les mêmes class-maps et classes, mais différentes valeurs CIR (Committed Information Rate) et BC (Burst Count) pour la réglementation. Dans les versions de Cisco NX-OS antérieures à la version 5.2.1, la commande **setup** a été utilisée pour modifier l'option. La version 5.2.1 de Cisco NX-OS a introduit une amélioration du protocole BPP CoPP afin que l'option puisse être modifiée sans la commande **setup** ; utilisez la commande **copp profile**.

```
SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# copp profile ?
dense The Dense Profile
lenient The Lenient Profile
moderate The Moderate Profile
strict The Strict Profile
SITE1-AGG1(config)# copp profile strict
SITE1-AGG1(config)# exit
```

Utilisez la commande **show copp profile <profile-type>** pour afficher la configuration CoPP BPP par défaut. Utilisez la commande **show copp status** pour vérifier que la stratégie CoPP a été appliquée correctement.

```
SITE1-AGG1# show copp status
Last Config Operation: copp profile strict
Last Config Operation Timestamp: 20:40:27 PST Nov 5 2012
Last Config Operation Status: Success
```

```
Policy-map attached to the control-plane: copp-system-p-policy-strict
```

Pour afficher la différence entre deux BPP CoPP, utilisez la commande **show copp diff profile <profile-type 1> profile <profile-type 2>** :

```
SITE1-AGG1# show copp diff profile strict profile moderate
A '+' represents a line that has been added and
a '-' represents a line that has been removed.
-policy-map type control-plane copp-system-p-policy-strict
- class copp-system-p-class-critical
- set cos 7
- police cir 39600 kbps bc 250 ms conform transmit violate drop
- class copp-system-p-class-important
- set cos 6
- police cir 1060 kbps bc 1000 ms conform transmit violate drop
----------------------SNIP----------------------------------------
+policy-map type control-plane copp-system-p-policy-moderate
+ class copp-system-p-class-critical
+ set cos 7
+ police cir 39600 kbps bc 310 ms conform transmit violate drop
+ class copp-system-p-class-important
+ set cos 6
+ police cir 1060 kbps bc 1250 ms conform transmit violate drop
----------------------SNIP----------------------------------------
```

Personnalisation d'une stratégie CoPP

Les utilisateurs peuvent créer une stratégie CoPP personnalisée. Cloner le CoPP BPP par défaut et le fixer à l'interface **du plan de contrôle** car le CoPP BPP est en lecture seule.

```
SITE2-AGG1(config)# policy-map type control-plane copp-system-p-policy-strict
^
% String is invalid, 'copp-system-p-policy-strict' is not an allowed string at
'^' marker.
```

La **commande copp copy profile <profile-type> <prefix> [suffix]** crée un clone du BPP CoPP. Ceci est utilisé afin de modifier les configurations par défaut. La commande **copp copy profile** est une commande **en mode exec**. L'utilisateur peut choisir un préfixe ou un suffixe pour le nom de la liste d'accès, des mappages de classes et des mappages de politiques. Par exemple, **copp-system-p-policy-strict** est remplacé par **[prefix]copp-policy-strict[suffix]**. Les configurations clonées sont traitées comme des configurations utilisateur et sont incluses dans la sortie **show run**.

```
SITE1-AGG1# copp copy profile ?
dense The Dense Profile
lenient The Lenient Profile
moderate The Moderate Profile
strict The Strict Profile
SITE1-AGG1# copp copy profile strict ?
prefix Prefix for the copied policy
suffix Suffix for the copied policy
SITE1-AGG1# copp copy profile strict suffix ?
WORD Enter prefix/suffix for the copied policy (Max Size 20)
SITE1-AGG1# copp copy profile strict suffix CUSTOMIZED-COPP
SITE1-AGG1# show run copp | grep policy-map
policy-map type control-plane copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1#
```

Il est possible de marquer le trafic qui dépasse et viole un débit d'informations autorisé spécifié (PIR) à l'aide des commandes suivantes :

```
SITE1-AGG1(config)# policy-map type
control-plane copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap)# class copp-class-critical-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms ?
<CR>
conform Specify a conform action
pir Specify peak information rate

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir ?
<1-80000000000> Peak Information Rate in bps/kbps/mbps/gbps

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps ?
<CR>
<1-512000000> Peak Burst Size in bytes/kbytes/mbytes/packets/ms/us
be Specify extended burst
conform Specify a conform action

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps conform ?
drop Drop the packet
set-cos-transmit Set conform action cos val
set-dscp-transmit Set conform action dscp val
set-prec-transmit Set conform action precedence val
transmit Transmit the packet

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps conform
set-dscp-transmit ef exceed set dscp1 dscp2 table cir-markdown-map violate
set1 dscp3 dscp4 table1 pir-markdown-map
SITE1-AGG1(config-pmap-c)#
```

Appliquez la stratégie CoPP personnalisée au **plan de contrôle** de l'interface globale. Utilisez la commande **show copp status** afin de vérifier que la stratégie CoPP a été appliquée correctement.

```
SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# control-plane
SITE1-AGG1(config-cp)# service-policy input ?
copp-policy-strict-CUSTOMIZED-COPP

SITE1-AGG1(config-cp)# service-policy input copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-cp)# exit
SITE1-AGG1# sh copp status
Last Config Operation: service-policy input copp-policy-strict-CUSTOMIZED-COPP
Last Config Operation Timestamp: 18:04:03 UTC May 15 2012
Last Config Operation Status: Success
Policy-map attached to the control-plane: copp-policy-strict-CUSTOMIZED-COPP
```

Étude de cas personnalisée sur les politiques CoPP

Cette section décrit un exemple réel dans lequel le client a besoin de plusieurs périphériques de surveillance pour envoyer fréquemment des requêtes ping aux interfaces locales. Dans ce scénario, des difficultés se présentent lorsque le client souhaite modifier la stratégie CoPP afin de :

- Augmentez le débit de données garanti de sorte que ces adresses spécifiques puissent envoyer une requête ping au périphérique local et ne violent pas la stratégie.
- Autoriser les autres adresses IP à conserver la possibilité d’envoyer une requête ping au périphérique local, mais à un débit de données garanti inférieur à des fins de dépannage.

La solution est présentée dans l'exemple suivant, qui consiste à créer une stratégie personnalisée avec une carte de classe distincte. La class-map séparée contient les adresses IP spécifiées des périphériques de surveillance et la class-map a un CIR plus élevé. Ceci laisse également la *surveillance* de la carte de classe d'origine, qui capture le trafic ICMP pour toutes les autres adresses IP à un débit de données garanti inférieur.

```
F340.13.19-Nexus7000-1#
F340.13.19-Nexus7000-1#
F340.13.19-Nexus7000-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
F340.13.19-Nexus7000-1(config)# copp copy profile strict prefix TAC_CHANGE
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)# ip access-list TAC_CHANGE-copp-acl-specific-icmp
F340.13.19-Nexus7000-1(config-acl)#
F340.13.19-Nexus7000-1(config-acl)# permit icmp host 1.1.1.1 host 2.2.2.2 echo
F340.13.19-Nexus7000-1(config-acl)# permit icmp host 1.1.1.1 host 2.2.2.2 echo-reply
F340.13.19-Nexus7000-1(config-acl)#
F340.13.19-Nexus7000-1(config-acl)# exit
F340.13.19-Nexus7000-1(config)# sho ip access-lists TAC_CHANGE-copp-acl-specific-
icmp IP access list TAC_CHANGE-copp-acl-specific-icmp
10 permit icmp 1.1.1.1/32 2.2.2.2/32 echo
20 permit icmp 1.1.1.1/32 2.2.2.2/32 echo-reply
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)# class-map type control-plane match-any
TAC_CHANGE-copp-class-specific-icmp
F340.13.19-Nexus7000-1(config-cmap)# match access-group name TAC_CHANGE-copp
-acl-specific-icmp
F340.13.19-Nexus7000-1(config-cmap)#exit
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)#policy-map type control-plane TAC_CHANGE-copp-
policy-strict
F340.13.19-Nexus7000-1(config-pmap)# class TAC_CHANGE-copp-class-specific-icmp
insert-before
TAC_CHANGE-copp-class-monitoring
F340.13.19-Nexus7000-1(config-pmap-c)# set cos 7
F340.13.19-Nexus7000-1(config-pmap-c)# police cir 5000 kbps bc 250 ms conform transmit
violate drop
F340.13.19-Nexus7000-1(config-pmap-c)# exit
F340.13.19-Nexus7000-1(config-pmap)#
F340.13.19-Nexus7000-1(config-pmap)#
F340.13.19-Nexus7000-1(config-pmap)#
F340.13.19-Nexus7000-1(config-pmap)#
F340.13.19-Nexus7000-1(config-pmap)# exit
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)# control-plane
F340.13.19-Nexus7000-1(config-cp)# service-policy input TAC_CHANGE-copp-policy-strict
F340.13.19-Nexus7000-1(config-cp)# end
F340.13.19-Nexus7000-1#
F340.13.19-Nexus7000-1# sho policy-map interface control-plane
Control Plane
service-policy input TAC_CHANGE-copp-policy-strict
<abbreviated output>
class-map TAC_CHANGE-copp-class-specific-icmp (match-any)
match access-group name TAC_CHANGE-copp-acl-specific-icmp
set cos 7
police cir 5000 kbps bc 250 ms
conform action: transmit
violate action: drop
```

```
module 4:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 7:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/secclass-map TAC_CHANGE-copp-class-monitoring (match-any)
match access-group name TAC_CHANGE-copp-acl-icmp
match access-group name TAC_CHANGE-copp-acl-icmp6
match access-group name TAC_CHANGE-copp-acl-mpls-oam
match access-group name TAC_CHANGE-copp-acl-traceroute
match access-group name TAC_CHANGE-copp-acl-http-response
match access-group name TAC_CHANGE-copp-acl-smtp-response
match access-group name TAC_CHANGE-copp-acl-http6-response
match access-group name TAC_CHANGE-copp-acl-smtp6-response
set cos 1
police cir 130 kbps bc 1000 ms
conform action: transmit
violate action: drop
module 4:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 7:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
<abbreviated output>
```

Structure de données CoPP

La structure de données CoPP BPP est construite comme suit :

- **Configuration de la liste de contrôle d'accès** : ACL IP et ACL MAC.
- **Configuration du classifieur** : Liste de contrôle d’accès IP ou MAC correspondant à la carte de classe.
- **Configuration du régulateur** : Définissez CIR, BC, conformez l'action et violez l'action. Le policier a deux taux (CIR et BC) et deux couleurs (conformité et violation).

```
mac access-list copp-system-p-acl-mac-fabricpath-isis
permit any 0180.c200.0015 0000.0000.0000
permit any 0180.c200.0014 0000.0000.0000
```

```
ip access-list copp-system-p-acl-bgp
permit tcp any gt 1024 any eq bgp
permit tcp any eq bgp any gt 1024

class-map type control-plane match-any copp-system-p-class-critical
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-pim
<snip>
match access-group name copp-system-p-acl-mac-fabricpath-isis
policy-map type control-plane copp-system-p-policy-dense
class copp-system-p-class-critical
set cos 7
police cir 5000 kbps bc 250 ms conform transmit violate drop
```

Facteur d'échelle CoPP

La configuration du facteur d'échelle introduite dans Cisco NX-OS version 6.0 permet d'adapter le taux de régulateur de la stratégie CoPP appliquée à une carte de ligne particulière. Cela augmente ou réduit le taux de régulateur pour une carte de ligne particulière, mais ne modifie pas la stratégie CoPP actuelle. Les modifications entrent en vigueur immédiatement et il n'est pas nécessaire de réappliquer la politique CoPP.

```
scale factor option configured within control-plane interface:
Scale-factor <scale factor value> module <module number>
<scale factor value>: from 0.10 to 2.00
Scale factor is recommended when a chassis is loaded with both F2 and M
Series modules.
SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# control-plane
SITE1-AGG1(config-cp)# scale-factor ?
<whole>.<decimal> Specify scale factor value from 0.10 to 2.00

SITE1-AGG1(config-cp)# scale-factor 1.0 ?
module Module

SITE1-AGG1(config-cp)# scale-factor 1.0 module ?
<1-10> Specify module number

SITE1-AGG1(config-cp)# scale-factor 1.0 module 4
SITE1-AGG1# show system internal copp info
<snip>
Linecard Configuration:
-----------------------
Scale Factors
Module 1: 1.00
Module 2: 1.00
Module 3: 1.00
Module 4: 1.00
Module 5: 1.00
Module 6: 1.00
Module 7: 1.00
Module 8: 1.00
Module 9: 1.00
Module 10: 1.00
```

Surveillance et gestion CoPP

Avec Cisco NX-OS version 5.1, il est possible de configurer un seuil de perte par nom de classe CoPP qui déclenche un message Syslog en cas de dépassement du seuil. La commande est **logging drop threshold <nombre d'octets supprimés> level <niveau de journalisation>**.

```
SITE1-AGG1(config)# policy-map type control-plane
copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap)# class copp-class-critical-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap-c)# logging ?
drop Logging for dropped packets

SITE1-AGG1(config-pmap-c)# logging drop ?
threshold Threshold value for dropped packets

SITE1-AGG1(config-pmap-c)# logging drop threshold ?
<CR>
<1-80000000000> Dropped byte count

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 ?
<CR>
level Syslog level

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 level ?
<1-7> Specify the logging level between 1-7

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 level 7
```

Voici un exemple de message Syslog :

```
%COPP-5-COPP_DROPS5: CoPP drops exceed threshold in class:
copp-system-class-critical,
check show policy-map interface control-plane for more info.
```

Compteurs CoPP

CoPP prend en charge les mêmes statistiques QoS que toute autre interface. Il affiche les statistiques des classes qui constituent la stratégie de service pour chaque module d'E/S prenant en charge CoPP. Utilisez la commande **show policy-map interface control-plane** pour afficher les statistiques de CoPP.

> **Note**: Toutes les classes doivent être surveillées en termes de paquets violés.

```
SITE1-AGG1# show policy-map interface control-plane
Control Plane

service-policy input: copp-policy-strict-CUSTOMIZED-COPP

class-map copp-class-critical-CUSTOMIZED-COPP (match-any)
match access-group name copp-acl-bgp-CUSTOMIZED-COPP
match access-group name copp-acl-bgp6-CUSTOMIZED-COPP
match access-group name copp-acl-eigrp-CUSTOMIZED-COPP
match access-group name copp-acl-igmp-CUSTOMIZED-COPP
match access-group name copp-acl-msdp-CUSTOMIZED-COPP
match access-group name copp-acl-ospf-CUSTOMIZED-COPP
match access-group name copp-acl-ospf6-CUSTOMIZED-COPP
match access-group name copp-acl-pim-CUSTOMIZED-COPP
match access-group name copp-acl-pim6-CUSTOMIZED-COPP
```

```
match access-group name copp-acl-rip-CUSTOMIZED-COPP
match access-group name copp-acl-rip6-CUSTOMIZED-COPP
match access-group name copp-acl-vpc-CUSTOMIZED-COPP
match access-group name copp-acl-eigrp6-CUSTOMIZED-COPP
match access-group name copp-acl-mac-l2pt-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-ldp-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-oam-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-rsvp-CUSTOMIZED-COPP
match access-group name copp-acl-otv-as-CUSTOMIZED-COPP
match access-group name copp-acl-mac-otv-isis-CUSTOMIZED-COPP
match access-group name copp-acl-mac-fabricpath-isis-CUSTOMIZED-COPP
match protocol mpls router-alert
match protocol mpls exp 6
set cos 7
threshold: 100, level: 7
police cir 39600 kbps , bc 250 ms
module 1 :
conformed 22454 bytes; action: transmit
violated 0 bytes; action: drop

module 2 :
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop

module 3 :
conformed 19319 bytes; action: transmit
violated 0 bytes; action: drop

module 4 :
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
```

Afin d'obtenir une vue globale des compteurs conformés et violés pour tous les modules de carte de classe et d'E/S, utilisez le **plan de contrôle d'interface show policy-map | i « class|conformement|Violé »**.

```
SITE1-AGG1# show policy-map interface control-plane | i "class|conform|violated"
class-map copp-class-critical-CUSTOMIZED-COPP (match-any)
conformed 123126534 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 107272597 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
class-map copp-class-important-CUSTOMIZED-COPP (match-any)
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
```

La **classe copp-class-l2-default et la classe-default** doivent être surveillées pour s'assurer qu'il n'y a pas d'augmentations élevées, même pour les compteurs conformes. Idéalement, ces deux classes doivent avoir des valeurs faibles pour le compteur conforme et au moins aucune augmentation de compteur non violée.

Compteurs ACL

La commande **statistics per-entry** n'est pas prise en charge pour les listes de contrôle d'accès IP ou MAC utilisées dans la carte de classe CoPP, et elle n'a aucun effet lorsqu'elle est appliquée à la liste de contrôle d'accès IP CoPP ou MAC. (Aucune vérification CLI n'est effectuée par l'analyseur CLI). Afin d'afficher les résultats de la liste de contrôle d'accès MAC ou IP CoPP sur un module d'E/S, utilisez la commande **show system internal access-list input detail**.

Voici un exemple :

```
!! 0180.c200.0041 is the destination MAC used for FabricPath IS-IS

SITE1-AGG1# show system internal access-list input entries det | grep 0180.c200.0041
[00fc:00f7:00f7] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [30042]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [29975]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [8965]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [8935]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [58233]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [27689]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[00fc:00f7:00f7] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
```

Meilleures pratiques de configuration CoPP

Voici les meilleures pratiques recommandées pour la configuration CoPP :

- Utilisez le mode CoPP strict par défaut.
- Le profil CoPP dense est recommandé lorsque le châssis est entièrement chargé avec des modules de la gamme F2 ou chargé avec plus de modules de la gamme F2 que tous les autres modules d'E/S.
- Il n'est pas recommandé de désactiver CoPP. Réglez le CoPP par défaut, si nécessaire.
- Surveillez les abandons involontaires et ajoutez ou modifiez la stratégie CoPP par défaut en fonction du trafic attendu.

- En fonction du nombre de FE dans le châssis, les paramètres CIR et BC pour CoPP peuvent être augmentés ou réduits. Cela dépend également du rôle des périphériques sur le réseau, des protocoles en cours d'exécution, etc.

- Comme les modèles de trafic changent constamment dans un **data center**, la personnalisation d'une CoPP est un processus constant.

- CoPP et VDC : Tous les ports du même FE doivent appartenir au même VDC, ce qui est facile pour un LC de la gamme F2, mais pas aussi facile pour un LC de la gamme M2 ou M108. En effet, le partage de ressources CoPP entre les VDC si les ports du même FE appartiennent à des VDC différents (série M1 ou LC série M2). Les ports d'un FE, même dans des VDC différents, comptent sur le même seuil pour CoPP.

- La configuration du facteur d'évolutivité est recommandée lorsqu'un châssis est chargé à la fois avec des modules de la gamme F2 et M.

Meilleures pratiques de surveillance CoPP

Voici les meilleures pratiques recommandées pour la surveillance CoPP :

- Configurez un seuil de message syslog pour CoPP (Cisco NX-OS version 5.1) afin de surveiller les abandons appliqués par CoPP.

- Les messages Syslog sont générés si les pertes dans une classe de trafic dépassent le seuil configuré par l'utilisateur.

- Le seuil et le niveau de journalisation peuvent être personnalisés dans chaque classe de trafic à l'aide de la commande **logging drop threshold <packet-count> level <level>**.

- Comme l'option « statistics per entry » pour la liste de contrôle d'accès MAC CoPP ou IP n'est pas prise en charge, utilisez la commande **show system internal access-list input det** pour surveiller les entrées de contrôle d'accès (ACE).

- La commande **class copp-class-l2-default et class-default** doit être surveillée pour s'assurer qu'il n'y a pas d'augmentation élevée, même pour les compteurs conformes.

- Toutes les classes doivent être surveillées en termes de paquets violés.

- Étant donné que **copp-class-Critical** est hautement vital mais a une politique de **violation**, il est recommandé de surveiller le taux de paquets conformes afin de recevoir une indication précoce lorsque la classe devient proche du moment où elle commence la violation. Si le compteur violé augmente pour cette classe, cela ne signifie pas nécessairement une alerte rouge. Cela signifie plutôt que cette situation doit faire l'objet d'une enquête à court terme.

- Utilisez la commande **copp profile strict** après chaque mise à niveau du code Cisco NX-OS, ou au moins après chaque mise à niveau majeure du code Cisco NX-OS ; si une modification

CoPP a déjà été effectuée, elle doit être réappliquée.

Conclusions

- CoPP est une fonctionnalité matérielle qui protège le superviseur des attaques DoS.
- Les LC des gammes M1, F2 et M2 prennent en charge CoPP. Les LC de la gamme F1 ne prennent pas en charge CoPP.
- La configuration CoPP est similaire à MQC (Modular QoS CLI).
- La configuration et la surveillance CoPP sont effectuées uniquement dans un VDC par défaut.
- Le protocole BPP CoPP par défaut peut être utilisé avec des options strictes, modérées, indulgentes et denses.
- Cloner CoPP BPP vers des règles CoPP personnalisées afin de répondre à des exigences réseau spécifiques.
- Les compteurs CoPP (conformes et violés en octets par class-map) sont affichés avec la commande **show policy-map interface control-plane**.
- Le trafic reçu par le processeur du module Supervisor est égal au nombre total de FE multiplié par le débit autorisé.
- Essayez d'éviter les ports partagés d'un FE sur différents VDC.
- Suivez les meilleures pratiques de CoPP afin de mettre en oeuvre et de contrôler les fonctionnalités.

Fonctions non prises en charge

Ces fonctionnalités ne sont pas prises en charge :

- Stratégie d'agrégation distribuée.
- Contrôle des microflux.
- Réglementation des exceptions de sortie.
- Prise en charge CoPP pour les BPDU provenant d'un port de tunnel dot1q (QinQ) : CDP (Cisco Discovery Protocol), DOT1x, STP (Spanning Tree Protocol) et VTP (VLAN Trunk Protocol).