Vérifier les violations de réglementation du plan de contrôle sur les plates-formes Nexus

Table des matières

Introduction

Ce document décrit en détail la réglementation du plan de contrôle (CoPP) sur les commutateurs Cisco Nexus et son impact pertinent sur les violations de classe non par défaut.

Conditions préalables

Cisco vous recommande de comprendre les informations de base relatives à la fonction de contrôle du plan de contrôle (CoPP), à ses directives et à ses limites, à sa configuration générale et à sa fonctionnalité de contrôle de la qualité de service (QoS). Pour plus d'informations sur cette fonctionnalité, reportez-vous aux documents applicables :

- Guide de configuration de la sécurité NX-OS de la gamme Cisco Nexus 9000, version 10.2(x)
- CoPP sur les commutateurs Cisco Nexus de la série 7000
- Guide de configuration de la qualité de service NX-OS de la gamme Cisco Nexus 9000, version 10.2(x)

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à la configuration logicielle et matérielle requise.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Le trafic du plan de contrôle est redirigé vers le module de supervision par des listes de contrôle d'accès (ACL) de redirection programmées pour diriger le trafic correspondant qui passe par deux couches de protection, les limiteurs de débit matériels et CoPP. Toute interruption ou attaque du module de supervision, si elle n'est pas contrôlée, peut entraîner de graves pannes de réseau. La CoPP est donc là pour servir de mécanisme de protection. En cas d'instabilité au niveau du plan de contrôle, il est important de vérifier CoPP, car des modèles de trafic anormaux créés à partir de boucles ou d'inondations, ou des périphériques non autorisés peuvent taxer et empêcher le superviseur de traiter le trafic légitime. De telles attaques, qui peuvent être perpétrées par inadvertance par des périphériques non autorisés ou de manière malveillante par des pirates, impliquent généralement des taux élevés de trafic destiné au module de supervision ou au processeur.

La fonction Control Plan Policing (CoPP) classe et gère tous les paquets reçus sur les ports intrabande (façade) destinés à l’adresse du routeur ou nécessitant l’intervention d’un superviseur. Cette fonctionnalité permet d'appliquer une carte de stratégie au plan de contrôle. Cette carte de stratégie ressemble à une stratégie de qualité de service (QoS) normale et est appliquée à tout le trafic qui entre dans le commutateur à partir d'un port de non-gestion. La protection du module de supervision par la réglementation permet au commutateur d'atténuer les inondations de trafic qui vont au-delà du débit d'entrée garanti (CIR) pour chaque classe par l'abandon de paquets pour empêcher le commutateur d'être submergé et donc un impact sur les performances.

Il est important de surveiller les compteurs CoPP en permanence et de les justifier, ce qui est l'objectif de ce document. Les violations CoPP, si elles ne sont pas cochées, peuvent empêcher le plan de contrôle du processus de trafic réel sur la classe affectée associée. La configuration CoPP est un processus fluide et continu qui doit répondre aux exigences du réseau et de l'infrastructure. Il existe trois stratégies système par défaut pour CoPP. Par défaut, Cisco recommande l'utilisation de la stratégie par défaut strict comme point de départ initial et sert de base à ce document.

La CoPP s'applique uniquement au trafic intrabande reçu via les ports du panneau avant. Le port de gestion hors bande (mgmt0) n'est pas soumis au protocole CoPP. Le matériel du périphérique Cisco NX-OS exécute la CoPP par moteur de transfert. Par conséquent, choisissez des débits afin que le trafic agrégé ne submerge pas le module de supervision. Ceci est particulièrement important pour les commutateurs modulaires/de fin de ligne, car le CIR s'applique au trafic agrégé de tous les modules et au trafic lié au CPU.

Matériel applicable

Le composant traité dans ce document s'applique à tous les commutateurs de data center Cisco Nexus.

Interprétation de la réglementation du plan de contrôle

L'objectif de ce document est de traiter les violations de classe non par défaut les plus courantes et critiques observées sur les commutateurs Nexus.

Profil CoPP standard par défaut

Pour comprendre comment interpréter le protocole CoPP, la première vérification doit consister à s'assurer qu'un profil est appliqué et à déterminer si un profil par défaut ou personnalisé est appliqué sur le commutateur.

Remarque : la méthode CoPP doit être activée sur tous les commutateurs Nexus. Si cette fonctionnalité n'est pas activée, elle peut provoquer une instabilité pour tout le trafic du plan de contrôle, car différentes plates-formes peuvent restreindre le trafic lié au superviseur (SUP). Par exemple, si CoPP n'est pas activé sur un Nexus 9000, le trafic destiné au SUP est limité à 50 pps, ce qui rend le commutateur pratiquement inutilisable. Le protocole CoPP est considéré comme obligatoire sur les plates-formes Nexus 3000 et Nexus 9000.

Si CoPP n'est pas activé, il peut être réactivé ou configuré sur le commutateur à l'aide de la **setup** commande ou par l'application de l'une des politiques par défaut standard sous l'option de configuration : copp profile [dense|lenient|moderate|strict].

Un périphérique non protégé ne classifie pas et ne sépare pas correctement le trafic en classes. Par conséquent, tout comportement de déni de service pour une fonctionnalité ou un protocole spécifique n'est pas limité à cette portée et peut affecter l'ensemble du plan de contrôle.

Remarque : les politiques CoPP sont mises en oeuvre par des redirections de classification TCAM (Ternary Content-Addressable Memory) et peuvent être vues directement sous **show system internal access-list input statistics module X | b CoPP** ou **show hardware access-list input entries detail**.

N9K1# show copp status Last Config Operation: None Last Config Operation Timestamp: None Last Config Operation Status: None Policy-map attached t

Classes de réglementation du plan de contrôle

Le protocole CoPP classe le trafic en fonction des correspondances qui correspondent aux listes de contrôle d’accès IP ou MAC. Par conséquent, il est important de comprendre quel trafic est classé dans quelle classe.

Les classes, qui dépendent de la plate-forme, peuvent varier. Il est donc important de comprendre comment vérifier les classes.

Par exemple, sur Nexus 9000 haut de rack (TOR) :

```
N9K1# show policy-map interface control-plane
Control Plane

Service-policy input: copp-system-p-policy-strict
...
class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes
module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec
...
```

Dans cet exemple, la carte-classe copp-system-p-class-critical englobe le trafic lié aux protocoles de routage, tels que le protocole BGP (Border Gateway Protocol), OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Router Protocol), et inclut d'autres protocoles, tels que vPC.

La convention de nom des listes de contrôle d’accès IP ou MAC est généralement explicite pour le protocole ou la fonctionnalité concernés, avec le préfixe copp-system-p-acl-[protocol|feature].

Pour afficher une classe spécifique, vous pouvez la spécifier directement lors de l'exécution de la commande **show**. Exemple :

```
N9K-4# show policy-map interface control-plane class copp-system-p-class-management
Control Plane

Service-policy input: copp-system-p-policy-strict

class-map copp-system-p-class-management (match-any)
match access-group name copp-system-p-acl-ftp
match access-group name copp-system-p-acl-ntp
match access-group name copp-system-p-acl-ssh
match access-group name copp-system-p-acl-http
match access-group name copp-system-p-acl-ntp6
```

match access-group name copp-system-p-acl-sftp
match access-group name copp-system-p-acl-snmp
match access-group name copp-system-p-acl-ssh6
match access-group name copp-system-p-acl-tftp
match access-group name copp-system-p-acl-https
match access-group name copp-system-p-acl-snmp6
match access-group name copp-system-p-acl-tftp6
match access-group name copp-system-p-acl-radius
match access-group name copp-system-p-acl-tacacs
match access-group name copp-system-p-acl-telnet
match access-group name copp-system-p-acl-radius6
match access-group name copp-system-p-acl-tacacs6
match access-group name copp-system-p-acl-telnet6
set cos 2
police cir 36000 kbps , bc 512000 bytes
module 1 :
transmitted 0 bytes;
5-minute offered rate 0 bytes/sec
conformed 0 peak-rate bytes/sec

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec

Alors que les profils CoPP par défaut sont normalement masqués dans le cadre de la configuration par défaut, vous pouvez voir la configuration avec **show running-conf copp all**:

<#root>

N9K1# show running-config copp all

!Command: show running-config copp all
!Running configuration last done at: Tue Apr 26 16:34:10 2022
!Time: Sun May 1 16:41:55 2022

version 10.2(1) Bios:version 05.45
control-plane
scale-factor 1.00 module 1
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-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis

```
(snip)
...
```

La carte-classe copp-system-p-class-criticalci-dessus fait référence à plusieurs instructions de correspondance qui appellent des listes de contrôle d'accès système, qui par défaut sont masquées, et fait référence à la classification sur laquelle la correspondance est établie. Par exemple, pour BGP :

<#root>

N9K1# show running-config aclmgr all | b

copp-system-p-acl-bgp

```
ip access-list
```

copp-system-p-acl-bgp

```
10 permit tcp any gt 1023 any eq bgp
20 permit tcp any eq bgp any gt 1023
(snip)
```

Cela signifie que tout trafic BGP correspond à cette classe et est classé sous copp-system-p-class-critical, ainsi que tous les autres protocoles sur cette même classe.

Le Nexus 7000 utilise une structure de fonctionnalités CoPP très similaire au Nexus 9000 :

N77-A-Admin# show policy-map interface control-plane
Control Plane
service-policy input copp-system-p-policy-strict

class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-lisp
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-rise
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-lisp6
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-rise6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-otv-as
match access-group name copp-system-p-acl-mac-l2pt
match access-group name copp-system-p-acl-mpls-ldp
match access-group name copp-system-p-acl-mpls-rsvp

```
match access-group name copp-system-p-acl-mac-l3-isis
match access-group name copp-system-p-acl-mac-otv-isis
match access-group name copp-system-p-acl-mac-fabricpath-isis
match protocol mpls router-alert
set cos 7
police cir 36000 kbps bc 250 ms
conform action: transmit
violate action: drop
module 1:
conformed 300763871 bytes,
5-min offered rate 132 bytes/sec
peak rate 125 bytes/sec at Sun May 01 09:50:51 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 2:
conformed 4516900216 bytes,
5-min offered rate 1981 bytes/sec
peak rate 1421 bytes/sec at Fri Apr 29 15:40:40 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 6:
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
```

Il est important de noter que sur un Nexus 7000, comme il s'agit de commutateurs modulaires, vous voyez la classe divisée par module ; cependant, le CIR s'applique à l'ensemble de tous les modules et la CoPP s'applique à l'ensemble du châssis. La vérification CoPP et les résultats ne peuvent être vus que depuis le contexte de périphérique virtuel (VDC) par défaut ou d'administration.

Il est particulièrement important de vérifier CoPP sur un Nexus 7000 si des problèmes de plan de contrôle sont observés, car l'instabilité sur un VDC avec un trafic excessif lié au CPU qui provoque des violations CoPP peut affecter la stabilité d'autres VDC.

Sur un Nexus 5600, les classes varient. Ainsi, pour BGP, il s'agit de sa propre classe séparée :

```
N5K# show policy-map interface control-plane
Control Plane
(snip)
class-map copp-system-class-bgp (match-any)
match protocol bgp
police cir 9600 kbps , bc 4800000 bytes
conformed 1510660 bytes; action: transmit
violated 0 bytes;
(snip)
```

Sur un Nexus 3100, il y a 3 classes de protocole de routage, donc pour vérifier à quelle classe BGP appartient, recoupez la liste de contrôle d'accès CoPP 4 qui est référencée :

EIGRP est géré par sa propre classe sur le Nexus 3100.

<#root>

N3K-C3172# show policy-map interface control-plane
Control Plane

service-policy input: copp-system-policy

class-map copp-s-routingProto2 (match-any)
match access-group name copp-system-acl-routingproto2
police pps 1300
OutPackets 0
DropPackets 0
class-map copp-s-v6routingProto2 (match-any)
match access-group name copp-system-acl-v6routingProto2
police pps 1300
OutPackets 0
DropPackets 0
class-map copp-s-eigrp (match-any)
match access-group name copp-system-acl-eigrp
match access-group name copp-system-acl-eigrp6
police pps 200
OutPackets 0
DropPackets 0
class-map copp-s-routingProto1 (match-any)
match access-group name

copp-system-acl-routingproto1

match access-group name copp-system-acl-v6routingproto1
police pps 1000
OutPackets 0
DropPackets 0

N3K-C3172# show running-config aclmgr

!Command: show running-config aclmgr
!No configuration change since last restart
!Time: Sun May 1 18:14:16 2022

version 9.3(9) Bios:version 5.3.1
ip access-list copp-system-acl-eigrp
10 permit eigrp any 224.0.0.10/32
ipv6 access-list copp-system-acl-eigrp6
10 permit eigrp any ff02::a/128
ip access-list

copp-system-acl-routingproto1

10 permit tcp any gt 1024 any eq bgp

20 permit tcp any eq bgp any gt 1024

```
30 permit udp any 224.0.0.0/24 eq rip
40 permit tcp any gt 1024 any eq 639
50 permit tcp any eq 639 any gt 1024
70 permit ospf any any
80 permit ospf any 224.0.0.5/32
90 permit ospf any 224.0.0.6/32
ip access-list copp-system-acl-routingproto2
10 permit udp any 224.0.0.0/24 eq 1985
20 permit 112 any 224.0.0.0/24
ipv6 access-list copp-system-acl-v6routingProto2
10 permit udp any ff02::66/128 eq 2029
20 permit udp any ff02::fb/128 eq 5353
30 permit 112 any ff02::12/128
ipv6 access-list copp-system-acl-v6routingproto1
10 permit 89 any ff02::5/128
20 permit 89 any ff02::6/128
30 permit udp any ff02::9/128 eq 521
```

Dans ce cas, BGP est mis en correspondance par la liste de contrôle d'accès copp-system-acl-routingproto1, et donc la classe CoPP BGP tombe dans sa copp-s-routingProto1.

Statistiques et compteurs de réglementation du plan de contrôle

CoPP prend en charge les statistiques QoS pour suivre les compteurs agrégés de trafic qui confirment ou enfreignent le débit garanti (CIR) pour une classe particulière, pour chaque module.

Chaque class-map classe le trafic lié au CPU, en fonction de la classe à laquelle il correspond et joint un CIR pour tous les paquets qui relèvent de cette classification. Par exemple, la classe qui se rapporte au trafic BGP est utilisée comme référence :

Sur un commutateur Nexus 9000 haut de rack (TOR) pour copp-system-p-class-critical:

<#root>

class-map copp-system-p-class-critical (match-any)
match access-group name

copp-system-p-acl-bgp

```
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes
```

```
module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec
```

Dans la section de la carte-classe, après les instructions match, vous voyez les actions qui se rapportent à tout le trafic dans la classe. Tout le trafic classé dans copp-system-p-class-critical est défini avec une classe de service (CoS) de 7, qui est le trafic de priorité la plus élevée, et cette classe est régulée avec un débit de données garanti de 36000 kbits/s et un débit garanti en rafale de 1280000 octets.

Le trafic conforme à cette stratégie est transféré au SUP pour être traité et toutes les violations sont abandonnées.

<#root>

set cos 7

police cir 36000 kbps , bc 1280000 bytes

La section suivante contient les statistiques relatives au module, pour les commutateurs haut de rack (TOR), avec un seul module, le module 1 fait référence au commutateur.

module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec

Les statistiques affichées sur le résultat sont historiques, ce qui fournit un instantané des statistiques actuelles au moment de l'exécution de la commande.

Il y a deux sections à interpréter ici : les sections transmises et abandonnées :
Le point de données transmis assure le suivi de tous les paquets transmis qui sont conformes à la stratégie. Cette section est importante car elle fournit des informations sur le type de trafic traité par le superviseur.

La valeur du tarif offert de 5 minutes donne un aperçu du tarif actuel.
La fréquence et la date de pic conformes fournissent un instantané de la fréquence de pic la plus élevée par seconde qui est toujours conforme à la stratégie et de l'heure à laquelle elle s'est produite.
Si un nouveau pic est détecté, il remplace cette valeur et cette date.

La partie la plus importante des statistiques est le point de données abandonné. Tout comme les statistiques transmises, la section abandonnée suit les octets cumulés abandonnés en raison de violations du taux de police. Il indique également le taux de violation des 5 dernières minutes, le pic violé, et s'il y a un pic, l'horodatage de ce pic de violation. Et encore une fois, si un nouveau pic est vu, alors il remplace cette valeur et cette date. Sur d'autres plates-formes, les sorties varient, mais la logique est très similaire.

Nexus 7000 utilise une structure identique et la vérification est la même, bien que certaines classes varient légèrement sur les ACL référencées :

<#root>

class-map

copp-system-p-class-critical

(match-any)
match access-group name

copp-system-p-acl-bgp

match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-lisp
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-rise
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-lisp6
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-rise6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-otv-as
match access-group name copp-system-p-acl-mac-l2pt
match access-group name copp-system-p-acl-mpls-ldp
match access-group name copp-system-p-acl-mpls-rsvp
match access-group name copp-system-p-acl-mac-l3-isis
match access-group name copp-system-p-acl-mac-otv-isis
match access-group name copp-system-p-acl-mac-fabricpath-isis
match protocol mpls router-alert

set cos 7

police cir 36000 kbps bc 250 ms

conform action: transmit

violate action: drop
module 1:
conformed 300763871 bytes,
5-min offered rate 132 bytes/sec
peak rate 125 bytes/sec at Sun May 01 09:50:51 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 2:
conformed 4516900216 bytes,

```
5-min offered rate 1981 bytes/sec
peak rate 1421 bytes/sec at Fri Apr 29 15:40:40 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 6:
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
```

Sur un Nexus 5600 :

```
<#root>
```

```
class-map copp-system-class-bgp

 (match-any)

match protocol bgp


police cir 9600 kbps , bc 4800000 bytes
conformed 1510660 bytes; action: transmit
violated 0 bytes;
```

Bien qu'il ne fournisse pas d'informations sur le débit ou les pics, il fournit toujours les octets agrégés conformes et violés.

Sur un Nexus 3100, la sortie du plan de contrôle affiche OutPackets et DropPackets.

```
class-map copp-s-routingProto1 (match-any)
match access-group name copp-system-acl-routingproto1
match access-group name copp-system-acl-v6routingproto1
police pps 1000
OutPackets 8732060
DropPackets 0
```

OutPackets fait référence aux paquets conformes, tandis que DropPackets fait référence aux violations du CIR. Dans ce scénario, vous ne voyez aucune suppression sur la classe associée.

Sur un Nexus 3500, la sortie affiche les paquets matériels et logiciels correspondants :

```
class-map copp-s-routingProto1 (match-any)
match access-group name copp-system-acl-routingproto1
```

police pps 900
HW Matched Packets 471425
SW Matched Packets 471425

Les paquets matériels mis en correspondance font référence aux paquets qui sont mis en correspondance dans le matériel par la liste de contrôle d’accès. Les paquets correspondant au logiciel sont ceux qui sont conformes à la politique. Toute différence entre les paquets correspondants matériels et logiciels implique une violation.

Dans ce cas, il n'y a pas d'abandon vu sur les paquets de classe du protocole de routage 1 (qui inclut le protocole BGP), car les valeurs correspondent.

Vérifier les violations de suppression actives

Étant donné que les statistiques de réglementation du plan de contrôle sont historiques, il est important de déterminer si les violations actives sont en augmentation. La méthode standard pour effectuer cette tâche consiste à comparer deux sorties complètes et à vérifier les différences éventuelles.

Cette tâche peut être effectuée manuellement ou les commutateurs Nexus fournissent l'outil diff qui peut vous aider à comparer les résultats.

Bien que l'ensemble du résultat puisse être comparé, il n'est pas nécessaire car l'accent est uniquement mis sur les statistiques abandonnées. Ainsi, la sortie CoPP peut être filtrée pour se concentrer uniquement sur les violations.

La commande est la suivante : show policy-map interface control-plane | egrep class|module|violated|dropped | diff -y

---

Remarque : la commande doit être exécutée deux fois pour que la différence puisse comparer le résultat actuel au résultat précédent.

```
N9K-3# show policy-map interface control-plane | egrep class|module|violated|dropped | diff -y
    class-map copp-system-p-class-l3uc-data (match-any)             class-map copp-system-p-class-l3uc-data (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-critical (match-any)              class-map copp-system-p-class-critical (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-important (match-any)             class-map copp-system-p-class-important (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-openflow (match-any)              class-map copp-system-p-class-openflow (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-multicast-router (match-any       class-map copp-system-p-class-multicast-router (match-any
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-multicast-host (match-any)        class-map copp-system-p-class-multicast-host (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-l3mc-data (match-any)             class-map copp-system-p-class-l3mc-data (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal (match-any)                class-map copp-system-p-class-normal (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-ndp (match-any)                   class-map copp-system-p-class-ndp (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-dhcp (match-any)           class-map copp-system-p-class-normal-dhcp (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-dhcp-relay-response        class-map copp-system-p-class-normal-dhcp-relay-response
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-igmp (match-any)           class-map copp-system-p-class-normal-igmp (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
```

La commande précédente vous permet d'afficher le delta entre deux classes et de rechercher les augmentations de violation.

Remarque : comme les statistiques CoPP sont historiques, une autre recommandation est d'effacer les statistiques après l'exécution de la commande, pour vérifier s'il y a des augmentations actives. Pour effacer les statistiques CoPP, exécutez la commande suivante : **clear copp statistics**.

Types de chutes CoPP

CoPP est une structure de réglementation simple, car tout trafic lié au CPU qui viole le CIR est abandonné. Les implications varient néanmoins considérablement en fonction du type de gouttes.

Bien que la logique soit la même, il n'est pas la même chose d'abandonner le trafic destiné à copp-system-p-class-critical.

class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7

police cir 36000 kbps , bc 1280000 bytes

Comparé à abandonner le trafic destiné à class-map copp-system-p-class-monitoring.

class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes

Le premier traite principalement des protocoles de routage, le second du protocole ICMP (Internet Control Message Protocol) qui a l'une des priorités les plus faibles et du CIR. La différence sur le débit de données garanti est de cent fois supérieure. Par conséquent, il est important de comprendre les classes, les impacts, les contrôles/vérifications communs et les recommandations.

Classes CoPP

Surveillance de classe - copp-system-p-class-monitoring

Cette classe englobe ICMP pour IPv4 et IPv6, et traceroute du trafic dirigé vers le commutateur en question.

class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes

Incidence

Une erreur courante lors du dépannage de la perte ou de la latence de paquets consiste à envoyer une requête ping au commutateur via ses ports intrabande, dont le débit est limité par le protocole CoPP. Étant donné que le protocole CoPP gère fortement le protocole ICMP, même en cas de trafic faible ou d’encombrement, la perte de paquets peut être observée par une requête ping envoyée directement aux interfaces intrabande si elles enfreignent le CIR.

Par exemple, en envoyant une requête ping aux interfaces directement connectées sur les ports routés, avec une charge utile de 500 paquets, des abandons peuvent être observés périodiquement.

<#root>

N9K-3# ping 192.168.1.1 count 1000 packet-size 500
...
--- 192.168.1.1 ping statistics ---

1000 packets transmitted, 995 packets received,

0.50% packet loss

round-trip min/avg/max = 0.597/0.693/2.056 ms

Sur le Nexus, où les paquets ICMP étaient destinés, vous voyez que CoPP les a abandonnés car la violation a été détectée et le CPU a été protégé :

<#root>

N9K-4# show policy-map interface control-plane class copp-system-p-class-monitoring
Control Plane

Service-policy input: copp-system-p-policy-strict

class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes
module 1 :
transmitted 750902 bytes;
5-minute offered rate 13606 bytes/sec
conformed 13606 peak-rate bytes/sec
at Sun May 01 22:49:24 2022

dropped 2950 bytes;

5-min violate rate 53 byte/sec

violated 53 peak-rate byte/sec at Sun May 01 22:49:24 2022

Pour résoudre les problèmes de latence ou de perte de paquets, il est recommandé d'utiliser les hôtes accessibles via le commutateur par le plan de données, qui n'est pas destiné au commutateur lui-même, qui serait le trafic du plan de contrôle. Le trafic du plan de données est transféré/routé au niveau matériel sans intervention du SUP et n'est donc pas réglementé par le CoPP, et ne subit généralement aucune perte.

Recommandations

- Envoyez une requête ping sur le commutateur via le plan de données, et non vers le commutateur, pour vérifier les résultats faussement positifs en cas de perte de paquets.
- Limitez le NMS (Network Monitoring System) ou les outils qui utilisent de manière agressive le protocole ICMP sur le commutateur pour éviter une rafale à travers le débit d'entrée validé pour la classe. Rappelez-vous que le protocole CoPP s'applique à tout le trafic agrégé appartenant à la classe.

Gestion des classes - copp-system-p-class-management

Comme on le voit ici, cette classe englobe différents protocoles de gestion qui peuvent être utilisés pour la communication (SSH, Telnet), les transferts (SCP, FTP, HTTP, SFTP, TFTP), l'horloge (NTP), AAA (Radius/TACACS) et la surveillance (SNMP), pour les communications IPv4 et IPv6.

class-map copp-system-p-class-management (match-any)
match access-group name copp-system-p-acl-ftp
match access-group name copp-system-p-acl-ntp
match access-group name copp-system-p-acl-ssh
match access-group name copp-system-p-acl-http
match access-group name copp-system-p-acl-ntp6
match access-group name copp-system-p-acl-sftp
match access-group name copp-system-p-acl-snmp
match access-group name copp-system-p-acl-ssh6
match access-group name copp-system-p-acl-tftp
match access-group name copp-system-p-acl-https
match access-group name copp-system-p-acl-snmp6
match access-group name copp-system-p-acl-tftp6
match access-group name copp-system-p-acl-radius
match access-group name copp-system-p-acl-tacacs
match access-group name copp-system-p-acl-telnet
match access-group name copp-system-p-acl-radius6
match access-group name copp-system-p-acl-tacacs6
match access-group name copp-system-p-acl-telnet6
set cos 2
police cir 36000 kbps , bc 512000 bytes

Incidence

Les comportements ou abandons les plus courants associés à cette classe sont les suivants :

- Lenteur de l'interface de ligne de commande perçue lors d'une connexion SSH/Telnet. S'il y a des abandons actifs dans la classe, les sessions de communication peuvent être lentes et subir des abandons.
- Transférez des fichiers avec les protocoles FTP, SCP, SFTP, TFTP sur le commutateur. Le comportement le plus courant est une tentative de transfert d'images de démarrage système/de démarrage par des ports de gestion intrabande. Cela peut entraîner des temps de transfert plus longs et des sessions de transmission fermées/terminées déterminées par la bande passante totale de la classe.
- Problèmes de synchronisation NTP, cette classe est également importante parce qu'elle atténue les agents ou les attaques NTP indésirables.
- Les services AAA Radius et TACACS entrent également dans cette catégorie. Si un impact est perçu sur cette classe, il peut affecter les services d'autorisation et d'authentification sur le commutateur pour les comptes d'utilisateurs, ce qui peut également contribuer à retarder les commandes CLI.
- SNMP est également réglementé dans cette classe. Les comportements les plus courants en raison des abandons dus à la classe SNMP sont sur les serveurs NMS, qui effectuent des promenades, des collectes en bloc ou des analyses de réseau. Lorsque l'instabilité périodique se produit, elle est généralement corrélée au programme de collecte NMS.

Recommandations

- Si la lenteur de l'interface de ligne de commande est perçue, ainsi que les abandons dans cette classe, utilisez l'accès console ou l'accès hors bande de gestion (mgmt0).
- Si des images système doivent être téléchargées sur le commutateur, utilisez le port de gestion hors bande (mgmt0) ou les ports USB pour un transfert plus rapide.
- Si des paquets NTP sont perdus, vérifiez show ntp peer-status, et vérifiez la colonne d'accessibilité, no drops do translate to 377.
- Si des problèmes sont constatés avec les services AAA, utilisez des utilisateurs locaux uniquement pour résoudre les problèmes, jusqu'à ce que le comportement soit atténué.
- La réduction des problèmes SNMP inclut un comportement moins agressif, une collecte ciblée ou la minimisation des analyseurs réseau. Examiner les intervalles périodiques entre les scanners et les événements observés au niveau du processeur.

Données de monodiffusion de classe L3 - copp-system-p-class-l3uc-data

Cette classe traite spécifiquement des paquets glanés. Ce type de paquet est également géré par le HWRL (Hardware Rate Limiter).

Si la requête ARP (Address Resolution Protocol) pour le tronçon suivant n'est pas résolue lorsque les paquets IP entrants sont transférés dans une carte de ligne, la carte de ligne transfère les paquets au module de supervision.

Le superviseur résout l'adresse MAC pour le saut suivant et programme le matériel.

```
class-map copp-system-p-class-l3uc-data (match-any)
match exception glean
set cos 1
```

Cela se produit normalement lorsque des routes statiques sont utilisées et que le tronçon suivant est inaccessible ou non résolu.

Lorsqu'une requête ARP est envoyée, le logiciel ajoute une contiguïté d'abandon /32 dans le matériel pour empêcher les paquets à la même adresse IP de tronçon suivant d'être transférés au superviseur. Une fois le protocole ARP résolu, l'entrée matérielle est mise à jour avec l'adresse MAC correcte. Si l'entrée ARP n'est pas résolue avant un délai d'attente, elle est supprimée du matériel.

Remarque : CoPP et HWRL fonctionnent en tandem pour garantir la protection du processeur. Alors qu'ils semblent exécuter des fonctions similaires, HWRL se produit en premier. La mise en oeuvre est basée sur l'emplacement où la fonctionnalité spécifique est mise en oeuvre sur les moteurs de transfert sur l'ASIC. Cette approche série permet une granularité et des protections multicouches qui évaluent tous les paquets liés au processeur.

Le HWRL est effectué par instance/moteur de transfert sur le module et peut être visualisé avec la commande **show hardware rate-limiter**. HWRL n'est pas couvert par ce document technique.

<#root>

show hardware rate-limiter

Units for Config: kilo bits per second
Allowed, Dropped & Total: aggregated bytes since last clear counters

Module: 1
R-L Class Config Allowed Dropped Total
+---------------+----------+--------------------+--------------------+--------------------+

L3 glean 100 0 0 0

L3 mcast loc-grp 3000 0 0 0
access-list-log 100 0 0 0
bfd 10000 0 0 0
fex 12000 0 0 0
span 50 0 0 0
sflow 40000 0 0 0
vxlan-oam 1000 0 0 0
100M-ethports 10000 0 0 0
span-egress disabled 0 0 0
dot1x 3000 0 0 0
mpls-oam 300 0 0 0
netflow 120000 0 0 0
ucs-mgmt 12000 0 0 0

Incidence

- Le trafic du plan de données est envoyé au superviseur comme une violation, car il ne peut pas être traité dans le matériel, et crée ainsi une pression sur le processeur.

Recommandations

- La résolution commune pour ce sujet de minimiser les pertes de glane est de s'assurer que le prochain saut est accessible, et d'activer la limitation de glane par la commande de configuration : **hardware ip glean throttle**.

Sur Nexus 7000 8.4(2), il a également introduit la prise en charge du filtre bloom pour les contiguïtés de glane pour les modules M3 et F4. Reportez-vous au Guide de configuration du routage de monodiffusion NX-OS de la gamme Cisco Nexus 7000

Passez en revue les configurations de routes statiques qui utilisent des adresses de tronçon suivant inaccessibles ou qui utilisent des protocoles de routage dynamique qui supprimeraient dynamiquement ces routes du RIB.

Classe critique - class-map copp-system-p-class-critical

Cette classe fait référence aux protocoles de plan de contrôle les plus critiques d'un point de vue L3, qui incluent les protocoles de routage pour IPv4 et IPv6 (RIP, OSPF, EIGRP, BGP), auto-RP, virtual port-channel (vPC) et l2pt et IS-IS.

class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l2pt
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes

Incidence

Abandon de l'instabilité de copp-system-p-class-critical transfert vers les protocoles de routage, ce qui peut inclure des contiguïtés abandonnées ou des échecs de convergence, ou une propagation de mise à jour/NLRI.
Les abandons de stratégie les plus courants sur cette classe peuvent concerner des périphériques indésirables sur le réseau qui agissent anormalement (en raison d'une mauvaise configuration ou d'une défaillance) ou d'une évolutivité.

Recommandations

- Si aucune anomalie n'est détectée, comme un périphérique non autorisé ou une instabilité de couche 2 qui entraîne une reconvergence continue des protocoles de couche supérieure, une configuration personnalisée de CoPP ou une classe plus souple peut être nécessaire pour s'adapter à l'échelle.

- Reportez-vous au guide de configuration CoPP pour savoir comment configurer un profil CoPP personnalisé à partir d'un profil par défaut existant.
Copie de la politique de meilleures pratiques CoPP

Classe importante - copp-system-p-class-important

Cette classe concerne les protocoles de redondance au premier saut (FHRP), qui incluent HSRP, VRRP et LLDP

class-map copp-system-p-class-important (match-any)
match access-group name copp-system-p-acl-hsrp
match access-group name copp-system-p-acl-vrrp
match access-group name copp-system-p-acl-hsrp6
match access-group name copp-system-p-acl-vrrp6
match access-group name copp-system-p-acl-mac-lldp
set cos 6
police cir 2500 kbps , bc 1280000 bytes

Incidence

Les comportements les plus courants qui entraînent des pertes sont les problèmes d'instabilité de couche 2, qui entraînent la transition des périphériques vers des scénarios d'état actif (split brain), des minuteurs agressifs, des erreurs de configuration ou l'évolutivité.

Recommandations:

- Assurez-vous pour FHRP que les groupes sont correctement configurés et que les rôles sont soit actifs/en veille, soit primaires/secondaires, et qu'ils sont correctement négociés, et qu'il n'y a pas d'instabilité sur l'état.
- Recherchez les problèmes de convergence au niveau de L2 ou de propagation multidiffusion pour le domaine L2.

Class L2 Unpoliced - copp-system-p-class-l2-unpoliced

La classe non réglementée de couche 2 fait référence à tous les protocoles critiques de couche 2 qui constituent la base de tous les protocoles de couche supérieure et sont donc considérés comme presque non réglementés avec le CIR et la priorité les plus élevés.

Cette classe gère efficacement les protocoles STP (Spanning Tree Protocol), LACP (Link Aggregation Control Protocol) et CFSoE (Cisco Fabric Service over Ethernet)

```
class-map copp-system-p-class-l2-unpoliced (match-any)
match access-group name copp-system-p-acl-mac-stp
match access-group name copp-system-p-acl-mac-lacp
match access-group name copp-system-p-acl-mac-cfsoe
match access-group name copp-system-p-acl-mac-sdp-srp
match access-group name copp-system-p-acl-mac-l2-tunnel
match access-group name copp-system-p-acl-mac-cdp-udld-vtp
set cos 7
police cir 50 mbps , bc 8192000 bytes
```

Cette classe a un débit de données garanti de 50 Mbits/s, le plus élevé de toutes les classes, ainsi que le taux d'absorption de rafales le plus élevé.

Incidence

Les abandons de cette classe peuvent entraîner une instabilité globale, car tous les protocoles de couche supérieure et toutes les communications sur les plans de données, de contrôle et de gestion reposent sur une stabilité de couche 2 sous-jacente.

Les problèmes de violations STP peuvent entraîner des problèmes de TCN et de convergence STP, notamment des conflits STP, des vidages MAC, des déplacements et des comportements d'apprentissage désactivés, ce qui entraîne des problèmes d'accessibilité et peut provoquer des boucles de trafic qui déstabilisent le réseau.

Cette classe fait également référence à LACP, et gère donc tous les paquets EtherType associés à 0x8809, qui incluent tous les LACPDU utilisés pour maintenir l'état des liaisons port-channel. L'instabilité sur cette classe peut provoquer le dépassement du délai d'attente des ports-channels si les LACPDU sont abandonnées.

Cisco Fabric Service over Ethernet (CSFoE) appartient à cette classe et est utilisé pour communiquer les états de contrôle des applications critiques entre les commutateurs Nexus. Il est donc essentiel pour la stabilité.

Il en va de même pour les autres protocoles de cette classe, qui inclut CDP, UDLD et VTP.

Recommandations

- Le comportement le plus courant est lié à l'instabilité Ethernet de couche 2. Assurez-vous que le protocole STP est correctement conçu de manière déterministe avec les améliorations de fonctionnalités appropriées en jeu afin de minimiser l'impact de la reconvergence ou des périphériques non autorisés sur le réseau. Assurez-vous que le type de port STP approprié est configuré pour que tous les périphériques hôtes finaux qui ne participent pas à l'extension L2 soient configurés en tant que ports d'agrégation de périphérie/périphérie afin de minimiser les TCN.

- Utilisez les améliorations STP, telles que BPDUguard, Loopguard, BPDUfilter et RootGuard, le cas échéant, pour limiter l'étendue d'une panne ou les problèmes de configuration incorrecte ou de périphériques non autorisés sur le réseau.

- Reportez-vous au document Cisco Nexus 9000 NX-OS Layer 2 Switching Configuration Guide, Release 10.2(x)

- Recherchez les comportements de déplacement MAC pouvant entraîner la désactivation de l'apprentissage et des vidages MAC. Référez-vous à : Dépannage et méthodes préventives du déplacement de Mac Nexus 9000

Routeur multidiffusion de classe - class-map copp-system-p-class-multicast-router

Cette classe fait référence aux paquets PIM (Protocol Independent Multicast) du plan de contrôle utilisés pour l'établissement et le contrôle d'arborescences partagées de multidiffusion routées via tous les périphériques compatibles PIM dans le chemin du plan de données. Elle inclut les routeurs FHR (First-Hop Router), LHR (Last-Hop Router), IHR (Intermediate-Hop Routers) et RP (Rendezvous Points). Les paquets classés dans cette classe incluent l'enregistrement PIM pour les sources, les jonctions PIM pour les récepteurs pour IPv4 et IPv6, en général tout trafic destiné à PIM (224.0.0.13) et le protocole MSDP (Multicast Source Discovery Protocol). Sachez qu'il existe plusieurs classes supplémentaires, qui traitent de parties très spécifiques de la fonctionnalité multicast ou RP qui sont traitées par différentes classes.

```
class-map copp-system-p-class-multicast-router (match-any)
match access-group name copp-system-p-acl-pim
match access-group name copp-system-p-acl-msdp
match access-group name copp-system-p-acl-pim6
match access-group name copp-system-p-acl-pim-reg
match access-group name copp-system-p-acl-pim6-reg
match access-group name copp-system-p-acl-pim-mdt-join
match exception mvpn
set cos 6
police cir 2600 kbps , bc 128000 bytes
```

Incidence

L'impact principal sur les abandons qui se rapportent à cette classe sont associés à des problèmes qui communiquent aux sources de multidiffusion par l'enregistrement PIM vers les RP ou les jonctions PIM non correctement traitées, ce qui déstabiliserait les arbres de chemin partagé ou le plus court vers les sources du flux de multidiffusion ou vers les RP. Le comportement peut inclure une liste d'interfaces sortantes (OIL) incorrectement renseignée en raison de jointures absentes, ou (S, G), ou (*, G) incohérente dans l'environnement. Des problèmes peuvent également survenir entre les domaines de routage de multidiffusion qui dépendent du protocole MSDP pour l'interconnexion.

Recommandations

- Le comportement le plus courant pour les problèmes liés au contrôle PIM se rapporte aux problèmes d'échelle ou aux comportements indésirables. L'un des comportements les plus courants est dû à l'implémentation d'UPnP, qui peut également entraîner des problèmes d'épuisement de la mémoire. Cela peut être résolu par des filtres et une portée réduite des périphériques indésirables. Pour plus de détails sur la façon dont les paquets de contrôle d'atténuation et de filtrage de multidiffusion qui dépendent du rôle réseau du périphérique, référez-vous à : Configurer le filtrage de multidiffusion sur Nexus 7K/N9K - Cisco

Class Multicast Host - copp-system-p-class-multicast-host

Cette classe fait référence à la détection de l'écouteur de multidiffusion (MLD), en particulier aux types de paquets MLD requête, rapport, réduction et MLDv2. MLD est un protocole IPv6 qu'un hôte utilise pour demander des données de multidiffusion pour un groupe particulier. Avec les informations obtenues par le biais de MLD, le logiciel tient à jour une liste d'appartenances de groupes ou de canaux de multidiffusion par interface. Les périphériques qui reçoivent des paquets MLD envoient les données de multidiffusion qu'ils reçoivent pour les groupes ou les canaux demandés par le segment de réseau des récepteurs connus. MLDv1 provient d'IGMPv2 et MLDv2 provient d'IGMPv3. IGMP utilise les types de message IP Protocol 2, tandis que MLD utilise les types de message IP Protocol 58, qui est un sous-ensemble des messages ICMPv6.

```
class-map copp-system-p-class-multicast-host (match-any)
match access-group name copp-system-p-acl-mld
set cos 1
police cir 1000 kbps , bc 128000 bytes
```

Incidence

Les abandons de cette classe se traduisent par des problèmes sur les communications multidiffusion IPv6 link-local, ce qui peut entraîner la suppression des rapports d'écouteur des récepteurs ou des réponses aux requêtes générales, ce qui empêche la découverte des groupes multidiffusion que les hôtes souhaitent recevoir. Cela peut avoir un impact sur le mécanisme de surveillance et ne pas transférer correctement le trafic vers les interfaces attendues qui ont demandé le trafic.

Recommandations

- Comme le trafic MLD est important au niveau link-local pour IPv6, si des abandons sont observés sur cette classe, les causes de comportement les plus courantes sont l'évolutivité, l'instabilité L2 ou les périphériques non autorisés.

Données de multidiffusion de couche 3 de classe - copp-system-p-class-l3mc-data et données IPv6 de multidiffusion de couche 3 de classe - copp-system-p-class-l3mcv6-data

Ces classes font référence au trafic qui correspond à une redirection d'exception de multidiffusion vers le SUP. Dans ce cas, il y a deux conditions qui sont gérées par ces classes. La première est une défaillance du protocole RPF (Reverse-Path Forwarding) et la seconde est une absence de destination. L'absence de destination fait référence à des paquets de multidiffusion où la recherche dans le matériel pour la table de transfert de multidiffusion de couche 3 échoue, et donc le paquet de données est envoyé au CPU. Ces paquets sont parfois utilisés pour déclencher/installer le plan de contrôle de multidiffusion et ajouter les entrées des tables de transfert matérielles, en fonction du trafic du plan de données. Les paquets de multidiffusion de plan de données qui violent le RPF correspondraient également à cette exception et seraient classés comme une violation.

```
class-map copp-system-p-class-l3mc-data (match-any)
match exception multicast rpf-failure
match exception multicast dest-miss
set cos 1
police cir 2400 kbps , bc 32000 bytes

class-map copp-system-p-class-l3mcv6-data (match-any)
match exception multicast ipv6-rpf-failure
match exception multicast ipv6-dest-miss
set cos 1
police cir 2400 kbps , bc 32000 bytes
```

Incidence

Les échecs RPF et les échecs de destination impliquent un problème de conception ou de configuration lié à la façon dont le trafic circule dans le routeur de multidiffusion. Les échecs de destination sont fréquents lors de la création d'états, les abandons peuvent conduire à la programmation et à la création de défaillances (*, G), (S, G).

Recommandations

- Apporter des modifications à la conception de base du RIB monodiffusion ou ajouter une mroute statique pour diriger le trafic via une interface particulière, en cas de défaillance du protocole RPF.
- Référez-vous à Le routeur ne transfère pas les paquets multidiffusion à l'hôte en raison d'une défaillance RPF

Classe IGMP - copp-system-p-class-igmp

Cette classe fait référence à tous les messages IGMP, pour toutes les versions qui sont utilisées pour demander des données de multidiffusion pour un groupe particulier, et utilisées par la fonctionnalité de surveillance IGMP pour maintenir les groupes et la liste d'interfaces sortantes (OIL) appropriée qui transfère le trafic vers les récepteurs intéressés au niveau de la couche 2. Les messages IGMP ont une signification locale car ils ne traversent pas une limite de couche 3, car leur durée de vie (TTL) doit être de 1, comme indiqué dans le document RFC2236 (Internet Group Management Protocol, Version 2). Les paquets IGMP traités par cette classe incluent toutes les requêtes d'adhésion (générales ou spécifiques à la source/au groupe), ainsi que les rapports d'adhésion et de sortie des récepteurs.

```
class-map copp-system-p-class-normal-igmp (match-any)
match access-group name copp-system-p-acl-igmp
set cos 3
police cir 3000 kbps , bc 64000 bytes
```

Incidence

Les abandons sur cette classe se traduiraient par des problèmes à tous les niveaux d'une communication multidiffusion entre la source et le récepteur, selon le type de message IGMP abandonné en raison de la violation. Si les rapports d'appartenance des récepteurs sont perdus, le routeur ne connaît pas les périphériques intéressés par le trafic et n'inclut donc pas l'interface/le VLAN dans sa liste d'interfaces sortantes. Si ce périphérique est également le demandeur ou le routeur désigné, il ne déclenche pas les messages de jointure PIM pertinents vers le RP si la

source se trouve au-delà du domaine local de couche 2, de sorte qu'il n'établit jamais le plan de données à travers l'arborescence de multidiffusion jusqu'au récepteur ou au RP. Si le rapport de congé est perdu, le destinataire peut continuer à recevoir du trafic indésirable. Cela peut également affecter toutes les requêtes IGMP pertinentes déclenchées par le demandeur et la communication entre les routeurs de multidiffusion dans un domaine.

Recommandations

- Les comportements les plus courants associés aux abandons IGMP sont liés à l'instabilité de couche 2, aux problèmes avec les compteurs ou à l'échelle.

Classe Normal - copp-system-p-class-normalcopp-system-p-class-normal

Cette classe fait référence au trafic qui correspond au trafic ARP standard, et inclut également le trafic associé à 802.1X, utilisé pour le contrôle d'accès réseau basé sur les ports. Il s'agit de l'une des classes les plus courantes qui rencontre des violations lorsque des requêtes ARP, des paquets ARP gratuits ou des paquets ARP inverses sont diffusés et se propagent dans l'ensemble du domaine de couche 2. Il est important de se rappeler que les paquets ARP ne sont pas des paquets IP, qu'ils ne contiennent pas d'en-tête L3 et que la décision est donc prise uniquement sur la portée des en-têtes L2. Si un routeur est configuré avec une interface IP associée à ce sous-réseau, telle qu'une interface virtuelle de commutateur (SVI), le routeur envoie les paquets ARP au SUP à traiter, car ils sont destinés à l'adresse de diffusion matérielle. Toute tempête de diffusion, boucle de couche 2 (en raison du protocole STP ou des volets) ou tout périphérique non autorisé sur le réseau peut entraîner une tempête ARP qui entraîne une augmentation significative des violations.

```
class-map copp-system-p-class-normal (match-any)
match access-group name copp-system-p-acl-mac-dot1x
match protocol arp
set cos 1
police cir 1400 kbps , bc 32000 bytes
```

Incidence

L'impact des violations dans cette classe dépend fortement de la durée des événements et du rôle du commutateur sur l'environnement. Les abandons dans cette classe impliquent que les paquets ARP sont actuellement rejetés et donc non traités par le moteur SUP, ce qui peut conduire à deux comportements principaux provoqués par des résolutions ARP incomplètes.

Du point de vue de l’hôte final, les périphériques du réseau ne sont pas en mesure de résoudre ou de terminer la résolution d’adresse avec le commutateur. Si ce périphérique agit comme passerelle par défaut pour le segment, il peut empêcher les périphériques de résoudre leur passerelle et donc de router en dehors de leur segment Ethernet de couche 2 (VLAN). Les périphériques peuvent toujours communiquer sur le segment local s'ils peuvent effectuer la résolution ARP pour d'autres hôtes finaux sur le segment local.

Du point de vue du commutateur, si l'orage et les violations sont répandus, cela peut également empêcher le commutateur de terminer le processus de requête ARP qu'il a généré. Ces requêtes sont normalement générées pour les résolutions de sous-réseau de tronçon suivant ou connecté directement. Bien que les réponses ARP soient de type monodiffusion, puisqu'elles sont adressées à l'adresse MAC appartenant au commutateur, elles sont classées dans cette même classe, car elles sont toujours des paquets ARP. Cela se traduit par des problèmes d'accessibilité, car le commutateur ne peut pas traiter correctement le trafic si le saut suivant n'est pas résolu, et peut entraîner des problèmes de réécriture d'en-tête de couche 2, si le gestionnaire de contiguïté n'a pas d'entrée pour l'hôte.

L'impact dépend également de l'étendue du problème fondamental qui a déclenché la violation ARP. Par exemple, dans une tempête de diffusion, les hôtes et le commutateur continuent à utiliser le protocole ARP pour tenter de résoudre la contiguïté, ce qui peut entraîner un trafic de diffusion supplémentaire sur le réseau, et comme les paquets ARP sont de couche 2, il n'y a pas de durée de vie de couche 3 (TTL) pour rompre une boucle de couche 2 et donc ils continuent à boucler et à croître de façon exponentielle à travers le réseau jusqu'à ce que la boucle soit rompue.

Recommandations

- Résolvez toute instabilité de couche 2 fondamentale qui peut provoquer des tempêtes ARP sur l'environnement, telles que STP, des volets ou des périphériques non autorisés. Cassez ces boucles selon les besoins, selon la méthode souhaitée pour ouvrir le chemin de liaison.

- Le contrôle des tempêtes peut également être utilisé pour atténuer une tempête ARP. Si le contrôle des tempêtes n'est pas activé, vérifiez les statistiques de compteur sur les interfaces pour vérifier le pourcentage de trafic de diffusion vu sur les interfaces par rapport au trafic total qui passe par l'interface.

- S'il n'y a pas de tempête, mais que des pertes constantes sont toujours observées dans l'environnement, vérifiez le trafic SUP pour identifier les périphériques indésirables, qui envoient constamment des paquets ARP sur le réseau, qui peuvent affecter le trafic légitime.

- Les augmentations visibles dépendent du nombre d'hôtes sur le réseau et du rôle du commutateur dans l'environnement. Le protocole ARP est conçu pour réessayer, résoudre et actualiser les entrées et, par conséquent, il est prévu que le trafic ARP soit visible à tout moment. Si seules des pertes sporadiques sont observées, elles peuvent être transitoires en raison de la charge du réseau et aucun impact n'est perçu. Mais il est important de surveiller et de connaître le réseau pour identifier et différencier correctement une situation attendue d'une situation anormale.

Class NDP - copp-system-p-acl-ndp

Cette classe fait référence au trafic associé à la découverte/annonce de voisinage IPv6 et aux paquets de sollicitation et d'annonce de routeur qui utilisent des messages ICMP pour déterminer les adresses de couche liaison locales des voisins. Elle est également utilisée pour l'accessibilité et le suivi des périphériques voisins.

```
class-map copp-system-p-class-ndp (match-any)
match access-group name copp-system-p-acl-ndp
set cos 6
police cir 1400 kbps , bc 32000 bytes
```

Incidence

Les violations sur cette classe peuvent entraver la communication IPv6 entre les périphériques voisins, car ces paquets sont utilisés pour faciliter la découverte dynamique ou les informations de couche liaison/locales entre les hôtes et les routeurs sur la liaison locale. Une interruption de cette communication peut également entraîner des problèmes d'accessibilité au-delà ou via la liaison locale associée. Si des problèmes de communication surviennent entre des voisins IPv6, assurez-vous qu'il n'y a pas d'abandon sur cette classe.

Recommandations

- Examinez les comportements ICMP anormaux des périphériques voisins, en particulier ceux liés à la découverte de voisins et/ou de routeurs.

- Assurez-vous que toutes les valeurs de temporisation et d'intervalle attendues pour les messages périodiques sont cohérentes dans l'ensemble de l'environnement et respectées. Par exemple, pour les messages d'annonce de routeur (messages RA).

Classe DHCP normal - copp-system-p-class-normal-dhcp

Cette classe fait référence au trafic associé au protocole Bootstrap (client/serveur BOOTP), communément appelé paquets DHCP (Dynamic Host Control Protocol) sur le même segment Ethernet local pour IPv4 et IPv6. Cela concerne spécifiquement uniquement la communication de trafic qui provient d'un client d'amorçage ou destinée à un serveur BOOTP, par l'intermédiaire de l'échange de paquets DORA (détection, offre, requête et accusé de réception) complet, et inclut également la transaction client/serveur DHCPv6 par l'intermédiaire des ports UDP 546/547.

class-map copp-system-p-class-normal-dhcp (match-any)
match access-group name copp-system-p-acl-dhcp
match access-group name copp-system-p-acl-dhcp6
set cos 1
police cir 1300 kbps , bc 32000 bytes

Incidence

Les violations de cette classe peuvent empêcher les hôtes finaux d'acquérir correctement une adresse IP auprès du serveur DHCP et de revenir ainsi à leur plage d'adresses IP privées automatiques (APIPA), 169.254.0.0/16. De telles violations peuvent se produire dans des environnements où les périphériques essaient de démarrer simultanément et dépassent ainsi le CIR associé à la classe.

Recommandations

- Vérifiez avec les captures que la transaction DORA est vue dans son intégralité sur les hôtes et le serveur DHCP. Si le commutateur fait partie de cette communication, alors il est également important de vérifier les paquets traités ou envoyés au CPU, et de vérifier les statistiques sur switch: **show ip dhcp global statistics** et redirections: **show system internal access-list sup-redirect-stats module 1 | grep -i dhcp**.

Réponse de relais DHCP normal de classe - copp-system-p-class-normal-dhcp-relay-response

Cette classe fait référence au trafic associé à la fonctionnalité de relais DHCP pour IPv4 et IPv6, dirigé vers les serveurs DHCP configurés sous le relais. Cela concerne spécifiquement uniquement la communication de trafic qui provient de n'importe quel serveur BOOTP ou destinée à n'importe quel client BOOTP via l'échange de paquets DORA entier, et inclut également la transaction client/serveur DHCPv6 via les ports UDP 546/547.

class-map copp-system-p-class-normal-dhcp-relay-response (match-any)
match access-group name copp-system-p-acl-dhcp-relay-response
match access-group name copp-system-p-acl-dhcp6-relay-response
set cos 1
police cir 1500 kbps , bc 64000 bytes

Incidence

Les violations de cette classe ont le même impact que celles de la classe copp-system-p-class-normal-dhcp, car elles font toutes deux partie de la même transaction. Cette classe se concentre principalement sur les communications de réponse des serveurs d'agent de relais. Le Nexus n'agit pas en tant que serveur DHCP, il est conçu uniquement pour agir en tant qu'agent de relais.

Recommandations

- Les mêmes recommandations que pour le DHCP normal de classe s'appliquent ici. Comme la fonction du Nexus est seulement d'agir en tant qu'agent de relais, sur le SUP vous vous attendez à voir la transaction entière entre l'hôte et le commutateur agissant en tant que relais, et le commutateur et les serveurs configurent.

- Assurez-vous qu'il n'y a aucun périphérique indésirable, tel que des serveurs DHCP inattendus sur le réseau qui répondent à l'étendue, ou des périphériques bloqués dans une boucle qui inondent le réseau avec des paquets de détection DHCP. Des vérifications supplémentaires peuvent être effectuées par les commandes : show ip dhcp relay et **show ip dhcp relay statistics**.

Flux NAT de classe - copp-system-p-class-nat-flow

Cette classe fait référence au trafic de flux NAT du commutateur logiciel. Lorsqu'une nouvelle traduction dynamique est créée, le flux est transféré par logiciel jusqu'à ce que la traduction soit programmée dans le matériel, puis il est réglementé par le CoPP pour limiter le trafic envoyé au superviseur pendant que l'entrée est installée dans le matériel.

```
class-map copp-system-p-class-nat-flow (match-any)
match exception nat-flow
set cos 7
police cir 800 kbps , bc 64000 bytes
```

Incidence

Les abandons de cette classe se produisent généralement lorsqu'un taux élevé de nouvelles traductions et de nouveaux flux dynamiques sont installés dans le matériel. L'impact concerne les paquets commutés par logiciel qui sont rejetés et non remis à l'hôte final, ce qui peut entraîner des pertes et des retransmissions. Une fois l'entrée installée dans le matériel, aucun autre trafic n'est envoyé au superviseur.

Recommandations

- Vérifier les directives et les limites de la NAT dynamique sur la plate-forme appropriée. Il existe des limitations connues qui sont documentées sur les plates-formes, telles que le 3548 dans lequel la traduction peut prendre quelques secondes. Reportez-vous à : Restrictions for Dynamic NAT

Exception de classe - copp-system-p-class-exception

Cette classe fait référence aux paquets d'exception associés à l'option IP et aux paquets IP ICMP inaccessibles. Si une adresse de destination n'est pas présente sur la base d'informations de transfert (FIB) et entraîne un échec, le SUP renvoie un paquet ICMP inaccessible à l'expéditeur. Les paquets dont les options IP sont activées font également partie de cette classe., Reportez-vous au document IANA pour plus de détails sur les options IP : Numéros d'option IP

class-map copp-system-p-class-exception (match-any)
match exception ip option
match exception ip icmp unreachable
match exception ipv6 option
match exception ipv6 icmp unreachable
set cos 1
police cir 150 kbps , bc 32000 bytes

Incidence

Cette classe est fortement réglementée, et les abandons sur cette classe ne sont pas indicatifs d'une défaillance, mais plutôt d'un mécanisme de protection pour limiter la portée des paquets d'options IP et d'ICMP inaccessibles.

Recommandations

- Vérifiez s'il existe des flux de trafic vus ou dirigés vers le processeur pour des destinations qui ne se trouvent pas sur la FIB.

Redirection de classe - copp-system-p-class-redirect

Cette classe fait référence au trafic associé au protocole PTP (Precision Time Protocol), utilisé pour la synchronisation temporelle. Cela inclut le trafic de multidiffusion pour la plage réservée 224.0.1.129/32, le trafic de monodiffusion sur le port UDP 319/320 et l'Ethetype 0X88F7.

class-map copp-system-p-class-redirect (match-any)
match access-group name copp-system-p-acl-ptp
match access-group name copp-system-p-acl-ptp-l2
match access-group name copp-system-p-acl-ptp-uc
set cos 1
police cir 280 kbps , bc 32000 bytes

Incidence

Les abandons de cette classe peuvent entraîner des problèmes sur les périphériques qui ne sont pas correctement synchronisés ou qui n'ont pas établi la hiérarchie appropriée.

Recommandations

- Assurez-vous que les horloges sont stables et qu'elles sont configurées correctement. Assurez-vous que le périphérique PTP est configuré pour le mode PTP multidiffusion ou monodiffusion, mais pas les deux en même temps. Ceci est également documenté dans les directives et les limites, et peut pousser le trafic au-delà du débit d'entrée validé.

- Examiner la conception et la configuration de l'horloge de périphérie et de tous les périphériques PTP dans l'environnement. Assurez-vous que toutes les consignes et restrictions sont respectées par plate-forme, car elles varient.

Classe OpenFlow - copp-system-p-class-openflow

Cette classe fait référence au trafic associé aux opérations de l'agent OpenFlow et à la connexion TCP correspondante entre le contrôleur et l'agent.

class-map copp-system-p-class-openflow (match-any)
match access-group name copp-system-p-acl-openflow
set cos 5
police cir 1000 kbps , bc 32000 bytes

Incidence

Les abandons de cette classe peuvent entraîner des problèmes sur les agents qui ne reçoivent pas et ne traitent pas correctement les instructions du contrôleur pour gérer le plan de transfert du réseau

Recommandations

- Assurez-vous qu'aucun trafic en double n'est détecté sur le réseau ou sur tout périphérique qui empêche la communication entre le contrôleur et les agents.
- Vérifiez que le réseau L2 n'a aucune instabilité (STP ou boucles).

Dépannage des pertes CoPP

Les premières étapes du dépannage des violations CoPP consistent à déterminer :

- Impact et portée du problème.
- Comprendre le flux de trafic dans l'environnement et le rôle du commutateur dans la communication affectée.
- Déterminez s'il existe des violations sur la classe associée suspectée et répétez l'opération si nécessaire.

Par exemple, le comportement répertorié a été détecté :

- Les périphériques ne peuvent pas communiquer avec d'autres périphériques en dehors de leur réseau, mais peuvent communiquer localement.
- L’impact a été isolé sur les communications routées en dehors du VLAN et le commutateur agit comme passerelle par défaut.
- Une vérification des hôtes indique qu'ils ne peuvent pas envoyer de requête ping à la passerelle. Après vérification de leur table ARP, l'entrée de la passerelle reste Incomplète.
- Tous les autres hôtes que la passerelle a résolus n'ont aucun problème de communication. Une vérification de CoPP sur le commutateur qui agit comme passerelle indique qu'il y a des violations sur copp-system-p-class-normal.

<#root>

class-map copp-system-p-class-normal (match-any)
match access-group name copp-system-p-acl-mac-dot1x
match protocol arp
set cos 1
police cir 1400 kbps , bc 32000 bytes
module 1 :
transmitted 3292445628 bytes;

dropped 522023852 bytes;

- En outre, plusieurs contrôles de commandes montrent que les abandons sont activement en augmentation.
- Ces violations peuvent entraîner l'abandon du trafic ARP légitime, ce qui entraîne un comportement de déni de service.

Il est important de souligner que CoPP isole l'impact sur le trafic associé à la classe spécifique, qui dans cet exemple sont ARP et copp-system-p-class-normal. Le trafic lié à d'autres classes, telles que OSPF, BGP n'est pas abandonné par CoPP, car ils appartiennent entièrement à une classe différente. Si cette case n’est pas cochée, les problèmes ARP peuvent se répercuter sur d’autres problèmes, ce qui peut affecter les protocoles qui s’y fient au départ. Par exemple, si un cache ARP expire et n'est pas actualisé en raison de violations excessives, une session TCP telle que BGP peut se terminer.

- Il est conseillé d'effectuer des vérifications du plan de contrôle, telles que l'analyse Ethnographique, les statistiques intrabande CPU-mac et le processus CPU, afin d'isoler davantage le sujet.

Ethanalyseur

Comme le trafic contrôlé par CoPP n'est associé qu'au trafic lié au CPU, l'un des outils les plus importants est l'Ethanalyzer. Cet outil est une implémentation Nexus de TShark et permet au trafic envoyé et reçu par le superviseur d'être capturé et décodé. Il peut également utiliser des filtres basés sur différents critères, tels que des protocoles ou des informations d'en-tête, et devient ainsi un outil précieux pour déterminer le trafic envoyé et reçu par le processeur.

Il est recommandé d'examiner d'abord le trafic ARP vu par le superviseur lorsque l'outil Ethanalyzer est exécuté directement sur la session du terminal ou envoyé à un fichier pour analyse. Des filtres et des limites peuvent être définis pour focaliser la capture sur un modèle ou un comportement spécifique. Pour ce faire, ajoutez des filtres d'affichage flexibles.

Une idée fausse courante est que l'analyseur Ethanalyzer capture tout le trafic qui traverse le commutateur. Le trafic du plan de données, entre les hôtes, est commuté ou routé par les circuits ASIC matériels entre les ports de données, ne nécessite pas l'intervention du processeur et n'est donc normalement pas vu par la capture d'analyseur de données. Pour capturer le trafic du plan de données, il est conseillé d'utiliser d'autres outils, tels qu'ELAM ou SPAN. Par exemple, pour filtrer ARP, utilisez la commande suivante :

ethanalyzer local interface inband display-filter arp limit-captured-frames 0 autostop duration 60 > arpcpu

Champs configurables importants :

- interface inband - fait référence au trafic dirigé vers le SUP

- display-filter arp - fait référence au filtre tshark appliqué, la plupart des filtres Wireshark sont acceptés

- limit-captured-frames 0 - fait référence à la limite, 0 équivaut à illimité, jusqu'à ce qu'il soit arrêté par un autre paramètre ou arrêté manuellement par Ctrl+C

- autostop duration 60 - fait référence à l'arrêt de l'Ethanalyzer après 60 secondes, ce qui crée un instantané de 60 secondes de trafic ARP vu sur le CPU

La sortie d'Ethanalyzer est redirigée vers un fichier sur le bootflash avec > arpcpu, pour être traitée manuellement. Au bout de 60 secondes, la capture est terminée et l'analyseur Ethanalyzer se termine dynamiquement, et le fichier arpcpu se trouve sur le bootflash du commutateur, qui peut ensuite être traité pour extraire les principaux émetteurs. Exemple :

show file bootflash:arpcpu | sort -k 3,5 | uniq -f 2 -c | sort -r -n | head lines 50

669 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:47 -> ff:ff:ff:ff:ff:ff ARP Who has 10.1.1.1? Tell 10.1.1.2
668 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:43 -> ff:ff:ff:ff:ff:ff ARP Who has 10.2.1.1? Tell 10.2.1.2
668 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:41 -> ff:ff:ff:ff:ff:ff ARP Who has 10.3.1.1? Tell 10.3.1.2

Ce filtre est trié en fonction des colonnes source et de destination, puis des correspondances uniques trouvées (mais ignore la colonne de date), compte les instances et ajoute le nombre vu, et enfin trie de haut en bas, en fonction du nombre, et affiche les 50 premiers résultats.

Dans cet exemple de travaux pratiques, en 60 secondes, plus de 600 paquets ARP ont été reçus de trois périphériques, identifiés comme des périphériques suspects. La première colonne du filtre détaille le nombre d'instances de cet événement qui ont été vues sur le fichier de capture pendant la durée spécifiée.

Il est important de comprendre que l'outil Ethanalyzer agit sur le pilote intrabande, qui est essentiellement la communication dans l'ASIC. En théorie, le paquet doit passer par le noyau et le gestionnaire de paquets pour être transféré au processus associé lui-même. CoPP et HWRL agissent avant que le trafic ne soit détecté sur l'analyseur Ethanalyzer. Même si les violations sont activement en augmentation, une partie du trafic passe toujours par et est conforme au taux de police, ce qui permet de fournir un aperçu des flux de trafic acheminés vers le processeur. Il s'agit d'une distinction importante, car le trafic vu sur l'analyseur Ethnologique n'est PAS le trafic qui a violé le CIR et a été abandonné.

L'analyseur Ethanalyzer peut également être utilisé de manière ouverte, sans aucun filtre d'affichage ou de capture spécifié pour intercepter tout le trafic SUP pertinent. Cela peut être utilisé comme mesure d'isolation dans le cadre de l'approche de dépannage.

Pour plus de détails et sur l'utilisation d'Ethanalyzer, reportez-vous à la TechNote :

Guide de dépannage d'Ethanalyzer sur Nexus 7000

Utilisation d'Ethanalyzer sur la plate-forme Nexus pour l'analyse du trafic des plans de contrôle et de données

---

Remarque : Nexus 7000, antérieur à la version du code 8.X, ne peut effectuer des captures Ethanalyzer que via le VDC d'administration, qui englobe le trafic lié au SUP de tous les VDC. Ethanalyzer spécifique à VDC est présent dans les codes 8.X.

Statistiques intrabande CPU-MAC

Les statistiques intrabande associées au trafic lié au CPU conservent des statistiques pertinentes du trafic intrabande du CPU TX/RX. Ces statistiques peuvent être vérifiées à l'aide de la commande suivante : show hardware internal cpu-mac inband stats, qui donne un aperçu des statistiques de taux en cours et de taux de pointe.

show hardware internal cpu-mac inband stats`
================ Packet Statistics ======================
Packets received: 363598837
Bytes received: 74156192058
Packets sent: 389466025
Bytes sent: 42501379591
Rx packet rate (current/peak): 35095 / 47577 pps
Peak rx rate time: 2022-05-10 12:56:18
Tx packet rate (current/peak): 949 / 2106 pps
Peak tx rate time: 2022-05-10 12:57:00

Il est recommandé de créer et de suivre une ligne de base car, en raison du rôle du commutateur et de l'infrastructure, le résultat du **show hardware internal cpu-mac inband stats** varie considérablement. Dans cet environnement de travaux pratiques, les valeurs habituelles et les pics historiques ne dépassent généralement pas quelques centaines de pps, ce qui est anormal. La commande **show hardware internal cpu-mac inband events** est également utile en tant que référence historique, car elle contient des données relatives à l'utilisation maximale et à l'heure de détection.

Procéder au CPU

Les commutateurs Nexus sont des systèmes basés sur Linux, et le système d'exploitation Nexus (NXOS) tire parti du planificateur préemptif de CPU, du multitâche et du multithreading de son architecture de coeur respective, pour fournir un accès équitable à tous les processus, et ainsi les pics ne sont pas toujours indicatifs d'un problème. Cependant, si des violations continues du trafic sont observées, il est probable que le processus associé est également fortement utilisé et apparaît comme une ressource principale sous les sorties du CPU. Prenez plusieurs instantanés des processus du processeur pour vérifier l'utilisation élevée d'un processus particulier à l'aide de : **show processes cpu sort | exclude 0.0 or show processes cpu sort | grep <process>**.

Les vérifications de l'UC des processus, des états intrabande et de l'Ethanalyzer fournissent des informations sur les processus et le trafic actuellement traités par le superviseur et permettent d'isoler l'instabilité continue sur le trafic du plan de contrôle qui peut se répercuter sur les problèmes du plan de données. Il est important de comprendre que la CoPP est un mécanisme de protection. Il est réactionnaire car il n'agit que sur le trafic envoyé au SUP. Il est conçu pour préserver l'intégrité du superviseur en éliminant les débits de trafic qui dépassent les plages prévues. Les abandons ne signalent pas tous un problème ou nécessitent une intervention, car leur importance est liée à la classe CoPP spécifique et à l'impact vérifié, sur la base de la conception de l'infrastructure et du réseau. Les abandons dus à des rafales sporadiques ne se traduisent pas par un impact, car les protocoles disposent de mécanismes intégrés, tels que le keepalive et les nouvelles tentatives qui peuvent traiter des événements transitoires. Maintenir l'accent sur les événements durables ou anormaux au-delà des valeurs de référence établies. Rappelez-vous que le protocole CoPP doit respecter les protocoles et les fonctionnalités spécifiques à l'environnement et doit être surveillé et continuellement itéré pour l'ajuster avec précision, en fonction des besoins d'évolutivité à mesure qu'ils évoluent. Si des abandons se produisent, déterminez si CoPP a abandonné le trafic de manière non intentionnelle ou en réponse à un dysfonctionnement ou une attaque. Dans un cas comme dans l'autre, analysez la situation et évaluez la nécessité d'intervenir en analysant l'impact et la mesure corrective sur l'environnement, ce qui peut sortir du cadre du commutateur lui-même.

Additional Information

Les plates-formes/codes récents peuvent avoir la capacité d'effectuer une SPAN vers CPU, par le miroir d'un port et le point du trafic du plan de données vers le CPU. Ce débit est normalement fortement limité par la limite de débit du matériel et la CoPP. L'utilisation prudente de la fonctionnalité SPAN vers CPU est conseillée et n'entre pas dans le cadre de ce document.

Reportez-vous à la note technique répertoriée pour plus d'informations sur cette fonctionnalité :

Procédure SPAN-to-CPU du Nexus 9000 Cloud Scale ASIC NX-OS

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.