Verifica delle violazioni di Control Plane Policing sulle piattaforme Nexus

Sommario

Introduzione

Questo documento descrive i dettagli relativi a Control Plane Policing (CoPP) sugli switch Cisco Nexus e il relativo impatto sulle violazioni delle classi non predefinite.

Prerequisiti

Cisco consiglia di comprendere le informazioni di base relative a Control Plane Policing (CoPP), le sue linee guida e limitazioni, la configurazione generale e la funzionalità di monitoraggio QoS (Quality-of-Service) (CIR). Per ulteriori informazioni su questa funzione, consultare i documenti applicabili:

- Guida alla configurazione della sicurezza di Cisco Nexus serie 9000 NX-OS, versione 10.2(x)
- CoPP su switch Nexus serie 7000
- Cisco Nexus serie 9000 NX-OS Quality of Service Configuration Guide, versione 10.2(x)

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutti i requisiti software e hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il traffico del control plane viene reindirizzato al modulo supervisor tramite il reindirizzamento degli access control list (ACL) programmati per puntare il traffico corrispondente che passa attraverso due livelli di protezione, i limitatori di velocità dell'hardware e il protocollo CoPP. Se non si verificano interruzioni o attacchi al modulo supervisor, si possono verificare gravi interruzioni della rete; in questo modo il CoPP può fungere da meccanismo di protezione. In caso di instabilità a livello di control plane, è importante controllare il CoPP, in quanto modelli di traffico anormali creati da loop o inondazioni o dispositivi non autorizzati possono applicare imposte e impedire al supervisore di elaborare il traffico legittimo. Tali attacchi, che possono essere perpetrati inavvertitamente da dispositivi malintenzionati o malintenzionati da utenti malintenzionati, in genere comportano alte velocità di traffico destinate al modulo supervisor o alla CPU.

Il Control Plan Policing (CoPP) è una funzione che classifica e regola tutti i pacchetti ricevuti sulle porte in banda (pannello anteriore) destinate all'indirizzo del router o che richiedono il coinvolgimento del supervisore. Questa funzionalità consente di applicare una mappa dei criteri al piano di controllo. Questa mappa dei criteri è simile a un normale criterio QoS (Quality of Service) e viene applicata a tutto il traffico che entra nello switch da una porta non di gestione. La protezione del modulo supervisor tramite la creazione di policy consente allo switch di mitigare le inondazioni del traffico che superano la velocità di input impegnata (CIR, Committed Input Rate) per ciascuna classe eliminando i pacchetti in modo da evitare che lo switch venga sovraccaricato e quindi influisca sulle prestazioni.

È importante monitorare continuamente i contatori CoPP e giustificarli, che è lo scopo del presente documento. Le violazioni CoPP, se non selezionate, possono impedire al control plane di elaborare il traffico autentico sulla classe interessata associata. La configurazione CoPP è un processo continuo e fluido che deve rispondere ai requisiti della rete e dell'infrastruttura. Sono disponibili tre criteri di sistema predefiniti per CoPP. Per impostazione predefinita, Cisco consiglia di utilizzare il criterio predefinito strict come punto di inizio iniziale e viene utilizzato come base per questo documento.

Il protocollo CoPP si applica solo al traffico in-band ricevuto tramite le porte del pannello anteriore. La porta di gestione fuori banda (mgmt0) non è soggetta al protocollo CoPP. L'hardware del dispositivo Cisco NX-OS esegue il protocollo CoPP per ciascun motore di inoltro. Pertanto, scegliere le tariffe in modo che il traffico aggregato non sovraccarichi il modulo supervisor. Ciò è particolarmente importante per gli switch a fine riga/modulari, poiché il CIR si applica al traffico aggregato di tutti i moduli in base alla CPU.

Dispositivi interessati

Il componente descritto in questo documento è applicabile a tutti gli switch per data center Cisco Nexus.

Interpretazione di Control Plane Policing

Questo documento ha lo scopo di risolvere le violazioni delle classi non predefinite più comuni e critiche rilevate sugli switch Nexus.

Profilo predefinito CoPP standard

Per capire come interpretare il protocollo CoPP, è necessario verificare prima di tutto che il profilo sia stato applicato e che sia stato applicato un profilo predefinito o personalizzato allo switch.

Nota: come buona norma, tutti gli switch Nexus devono avere il protocollo CoPP abilitato. Se questa funzione non è abilitata, potrebbe causare instabilità per tutto il traffico del control plane, in quanto piattaforme diverse potrebbero limitare il traffico in direzione del Supervisor (SUP). Ad esempio, se il protocollo CoPP non è abilitato su un Nexus 9000, la velocità del traffico destinato al protocollo SUP sarà limitata a 50 punti base, per cui lo switch sarà quasi inutilizzabile. Il CoPP è considerato un requisito per le piattaforme Nexus 3000 e Nexus 9000.

Se il protocollo CoPP non è abilitato, è possibile riabilitarlo o configurarlo sullo switch usando il **setup** comando o applicando una delle policy predefinite standard dell'opzione di configurazione: copp profile [dense|lenient|moderate|strict].

Un dispositivo non protetto non classifica e suddivide correttamente il traffico in classi, pertanto qualsiasi comportamento di negazione del servizio per una funzionalità o un protocollo specifico non è limitato a tale ambito e può influire sull'intero control plane.

Nota: le policy CoPP vengono implementate dai reindirizzamenti di classificazione TCAM (Ternary Content-Addressable Memory) e possono essere visualizzate direttamente sotto **show system internal access-list input statistics module X | b CoPP** o **show hardware access-list input entries detail**sotto.

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

Classi Control Plane Policing

Il protocollo CoPP classifica il traffico in base alle corrispondenze che corrispondono agli ACL IP o MAC. Pertanto, è importante capire quale traffico viene classificato in base a quale classe.

Le classi, dipendenti dalla piattaforma, possono variare. Quindi, è importante capire come verificare le classi.

Ad esempio, su Nexus 9000 top-of-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
...
```

Nell'esempio, la mappa delle classi copp-system-p-class-critical comprende il traffico relativo ai protocolli di routing, ad esempio Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Router Protocol (EIGRP), e include altri protocolli, ad esempio vPC.

La convenzione relativa al nome degli ACL IP o MAC è per lo più autoesplicativa per il protocollo o la funzionalità interessata, con il prefisso copp-system-p-acl-[protocol|feature].

Per visualizzare una classe specifica, è possibile specificarla direttamente durante l'esecuzione del comando **show**. Ad esempio:

```
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

Mentre i profili predefiniti CoPP sono in genere nascosti come parte della configurazione predefinita, è possibile visualizzare la configurazione con **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 mappa delle classi copp-system-p-class-critical, illustrata in precedenza, fa riferimento a più istruzioni match che utilizzano ACL di sistema, che per impostazione predefinita sono nascoste, e fanno riferimento alla classificazione a cui viene associata. Ad esempio, per 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)

Ciò significa che qualsiasi traffico BGP corrisponde a questa classe e viene classificato in copp-system-p-class-critical, insieme a tutti gli altri protocolli sulla stessa classe.

Il Nexus 7000 utilizza una struttura molto simile a quella del 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

È importante notare che su un Nexus 7000, poiché si tratta di switch modulari, la classe viene divisa per modulo; tuttavia, il CIR si applica all'aggregazione di tutti i moduli e il CoPP si applica all'intero chassis. La verifica e gli output CoPP possono essere visualizzati solo dal contesto di dispositivo virtuale predefinito o amministrativo (VDC).

È particolarmente importante verificare il CoPP su un Nexus 7000 se vengono rilevati problemi del control plane, in quanto l'instabilità su un VDC con un eccessivo traffico basato sulla CPU che provoca violazioni del CoPP può influire sulla stabilità di altri VDC.

Su un Nexus 5600 le classi variano. Pertanto, per BGP si tratta di una classe distinta:

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)

Su un Nexus 3100, sono disponibili 3 classi di protocolli di routing. Per verificare a quale classe appartiene BGP, fare riferimento incrociato

all'ACL CoPP a cui si fa riferimento:

L'EIGRP è gestito dalla propria classe sul 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
```

In questo caso, il BGP corrisponde all'ACL copp-system-acl-routingproto1, quindi la classe CoPP BGP rientra nella copp-s-routingProto1IOS.

Statistiche e contatori di Control Plane Policing

CoPP supporta le statistiche QoS per tenere traccia dei contatori aggregati del traffico che confermano o violano la velocità di input impegnata (CIR, Committed Input Rate) per una particolare classe, per ogni modulo.

Ogni mappa delle classi classifica il traffico associato alla CPU in base alla classe a cui corrisponde e collega un CIR per tutti i pacchetti che rientrano in tale classificazione. Ad esempio, la classe correlata al traffico BGP viene utilizzata come riferimento:

Su un Nexus 9000 top-of-rack (TOR) per 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
```

Nella sezione della mappa delle classi, dopo le istruzioni match, vengono visualizzate le azioni relative a tutto il traffico all'interno della classe. Tutto il traffico classificato all'interno di copp-system-p-class-critical è impostato con una Class of Service (CoS) di 7, che è il traffico con la massima priorità, e questa classe è controllata con un CIR di 36000 kbps e una velocità di burst commit di 1280000 byte.

Il traffico conforme a questo criterio viene inoltrato alla SUP per essere elaborato e le eventuali violazioni vengono eliminate.

<#root>

set cos 7

police cir 36000 kbps , bc 1280000 bytes

La sezione successiva contiene le statistiche relative al modulo. Per gli switch top-of-rack (TOR), con un unico modulo, il modulo 1 si riferisce allo switch.

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

Le statistiche visualizzate nell'output sono cronologiche, pertanto forniscono un'istantanea delle statistiche correnti al momento dell'esecuzione del comando.

A questo proposito, è necessario interpretare due sezioni: le sezioni trasmesse e quelle eliminate:
Il datapoint trasmesso tiene traccia di tutti i pacchetti trasmessi conformi al criterio. Questa sezione è importante in quanto fornisce informazioni sul tipo di traffico elaborato dal supervisore.

Il valore della tariffa offerta di 5 minuti fornisce informazioni dettagliate sulla tariffa corrente.
La data e la velocità di picco rese conformi forniscono uno snap della velocità di picco al secondo più elevata ancora conforme al criterio e l'ora in cui si è verificato.
Se viene rilevato un nuovo picco, questo valore e questa data vengono sostituiti.

La parte più importante delle statistiche è il punto dati eliminato. Proprio come le statistiche trasmesse, la sezione scartata traccia i byte cumulativi scartati a causa di violazioni alla frequenza della polizia. Fornisce anche la frequenza di violazione per gli ultimi 5 minuti, il picco

violato e, se esiste un picco, l'indicatore orario di tale picco di violazione. E ancora, se si nota un nuovo picco, questo valore e questa data vengono sostituiti. Su altre piattaforme, gli output variano, ma la logica è molto simile.

Nexus 7000 utilizza una struttura identica e la verifica è la stessa, anche se alcune classi variano leggermente negli ACL a cui si fa riferimento:

<#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
```

Su 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;
```

Anche se non fornisce informazioni sulla velocità o sui picchi, fornisce comunque i byte aggregati conformati e violati.

Su un Nexus 3100, l'output del control plane mostra OutPackets e 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 fa riferimento ai pacchetti resi conformi, mentre DropPackets fa riferimento alle violazioni al CIR. In questo scenario non viene visualizzata alcuna perdita sulla classe associata.

Su un Nexus 3500, l'output mostra i pacchetti HW e SW corrispondenti:

```
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
```

Per pacchetti corrispondenti all'hardware si intendono i pacchetti corrispondenti all'hardware dall'ACL. I pacchetti software corrispondenti sono quelli conformi al criterio. Qualsiasi differenza tra i pacchetti HW e SW corrispondenti implica una violazione.

In questo caso, non si verificano perdite di dati sui pacchetti di classe del protocollo di routing 1 (che include BGP), in quanto i valori corrispondono.

Controlla violazioni attive al rilascio

Dato che le statistiche di control plane policing sono storiche, è importante determinare se le violazioni attive sono in aumento. Il modo standard per eseguire questa operazione consiste nel confrontare due output completi e verificare le eventuali differenze.

Questa operazione può essere eseguita manualmente oppure gli switch Nexus forniscono lo strumento diff che consente di confrontare gli output.

Sebbene sia possibile confrontare l'intero output, non è necessario poiché lo stato attivo è solo sulle statistiche eliminate. Di conseguenza, l'output CoPP può essere filtrato in modo da concentrarsi solo sulle violazioni.

Il comando è: show policy-map interface control-plane | egrep class|module|violated|dropped | diff -y

---

Nota: per poter confrontare l'output corrente con quello precedente, il comando deve essere eseguito due volte.

```
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;
```

Il comando precedente consente di visualizzare il delta tra due classi e di individuare l'aumento delle violazioni.

Nota: poiché le statistiche CoPP sono cronologiche, è consigliabile cancellarle dopo l'esecuzione del comando per verificare se sono presenti aumenti attivi. Per cancellare le statistiche CoPP, eseguire il comando: **clear copp statistics**.

Tipi di rilasci CoPP

CoPP è una struttura di policy semplice, in quanto qualsiasi traffico legato alla CPU che viola il CIR viene scartato. Le implicazioni variano comunque in modo significativo a seconda del tipo di gocce.

Anche se la logica è la stessa, non è lo stesso per il traffico di destinazione 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
```

Confrontato con il traffico di rilascio destinato alla copp-system-p-class-monitoringmappa di classe.

```
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
```

Il primo si occupa principalmente dei protocolli di routing, il secondo si occupa del protocollo ICMP (Internet Control Message Protocol), che ha una delle priorità più basse, e del CIR. La differenza con il CIR è centuplicata. È quindi importante comprendere le classi, gli impatti, i controlli/le verifiche comuni e le raccomandazioni.

Classi CoPP

Monitoraggio delle classi - copp-system-p-class-monitoring

Questa classe comprende ICMP per IPv4 e IPv6 e il traceroute del traffico diretto allo switch in questione.

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

Conseguenze

Quando il problema è la perdita o la latenza del pacchetto, si ha spesso l'impressione errata di eseguire il ping sullo switch tramite le porte in-band, la cui velocità è limitata dal protocollo CoPP. Mentre il protocollo CoPP applica una policy pesante sull'ICMP, anche in caso di traffico ridotto o congestione, la perdita dei pacchetti può essere rilevata dal ping sulle interfacce in-band direttamente se violano il CIR.

Ad esempio, eseguendo il ping sulle interfacce connesse direttamente sulle porte di routing, con un payload del pacchetto di 500, è possibile visualizzare periodicamente le cadute.

<#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

Sul Nexus, dove erano destinati i pacchetti ICMP, si vede che il CoPP li ha scartati perché la violazione è stata rilevata e la CPU protetta:

<#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

Per risolvere i problemi di latenza o perdita di pacchetti, si consiglia di utilizzare host raggiungibili tramite lo switch dal data plane, non destinati allo switch stesso, ossia al traffico del control plane. Il traffico del data plane viene inoltrato/instradato a livello hardware senza l'intervento del protocollo SUP e quindi non sottoposto a policy dal protocollo CoPP, senza che si verifichino perdite di dati.

Consigli

- Inviare un ping sullo switch tramite il piano dati, non allo switch, per verificare i risultati falsi positivi della perdita di pacchetti.
- Limitare il Network Monitoring System (NMS) o gli strumenti che utilizzano lo switch in modo aggressivo per evitare una frammentazione nella velocità di input vincolata per la classe. Tenere presente che il protocollo CoPP si applica a tutto il traffico aggregato che rientra nella classe.

Gestione classi - copp-system-p-class-management

Come mostrato di seguito, questa classe comprende diversi protocolli di gestione che possono essere utilizzati per la comunicazione (SSH, Telnet), i trasferimenti (SCP, FTP, HTTP, SFTP, TFTP), l'orologio (NTP), AAA (Radius/TACACS) e il monitoraggio (SNMP), per le comunicazioni IPv4 e 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

Conseguenze

I comportamenti o le eliminazioni più comuni associati a questa classe includono:

- Lentezza CLI percepita quando collegato da SSH/Telnet. Se ci sono cadute attive sulla classe, allora le sessioni di comunicazione possono essere lente e soffrire di cadute.
- Trasferire i file con i protocolli FTP, SCP, SFTP e TFTP sullo switch. Il comportamento più comune è rappresentato da un tentativo di trasferire le immagini di avvio del sistema/avvio tramite porte di gestione in-band. Ciò può portare a tempi di trasferimento più lunghi e a sessioni di trasmissione chiuse/terminate determinate dalla larghezza di banda aggregata per la classe.
- Problemi di sincronizzazione NTP, questa classe è importante anche perché mitigare gli agenti NTP non autorizzati o gli attacchi.
- In questa classe rientrano anche i servizi AAA Radius e TACACS. Se percepito come un impatto su questa classe, può influire sui servizi di autorizzazione e autenticazione sullo switch per gli account utente, il che può anche contribuire a ritardare i comandi della CLI.
- In questa classe è incluso anche il protocollo SNMP. Il comportamento più comune rilevato a causa di cali dovuti alla classe SNMP è nei server NMS, che eseguono spostamenti, raccolte in blocco o scansioni di rete. Quando si verifica un'instabilità periodica, in genere è correlata alla pianificazione della raccolta NMS.

Consigli

- Se si percepisce la lentezza CLI, oltre a cali in questa classe, utilizzare l'accesso da console o l'accesso fuori banda di gestione (mgmt0).
- Se è necessario caricare le immagini del sistema sullo switch, utilizzare la porta di gestione fuori banda (mgmt0) o le porte USB per il trasferimento più rapido.
- Se i pacchetti NTP vengono persi, selezionare show ntp peer-status (mostra stato peer ntp) e verificare la colonna reachability (raggiungibilità). In questo caso, nessuna perdita corrisponde a 377.
- Se si rilevano problemi con i servizi AAA, utilizzare gli utenti solo locali per la risoluzione dei problemi, fino a quando il comportamento non viene mitigato.
- Per ridurre i problemi relativi al protocollo SNMP, è possibile adottare un comportamento meno aggressivo, raccogliere dati in modo mirato o ridurre al minimo gli scanner di rete. Esaminare i tempi periodici dagli scanner agli eventi visualizzati a livello di CPU.

Dati Unicast di classe L3 - copp-system-p-class-l3uc-data

Questa classe tratta in modo specifico i pacchetti puliti. Questo tipo di pacchetto viene gestito anche dall'Hardware Rate Limiter (HWRL).

Se la richiesta Address Resolution Protocol (ARP) per l'hop successivo non viene risolta quando i pacchetti IP in arrivo vengono inoltrati in una scheda di linea, la scheda di linea inoltra i pacchetti al modulo supervisor.

Il supervisore risolve l'indirizzo MAC per l'hop successivo e programma l'hardware.

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

Questo si verifica in genere quando vengono utilizzate route statiche e l'hop successivo non è raggiungibile o non è risolto.

Quando si invia una richiesta ARP, il software aggiunge un'adiacenza di drop /32 nell'hardware per impedire che i pacchetti allo stesso indirizzo IP dell'hop successivo vengano inoltrati al supervisore. Una volta risolto l'ARP, la voce hardware viene aggiornata con l'indirizzo MAC corretto. Se la voce ARP non viene risolta prima di un periodo di timeout, viene rimossa dall'hardware.

Nota: CoPP e HWRL operano in tandem per garantire la protezione della CPU. Mentre sembrano eseguire funzioni simili, HWRL si verifica per primo. L'implementazione si basa sulla posizione in cui la funzionalità specifica viene implementata sui motori di inoltro dell'ASIC. Questo approccio seriale consente granularità e protezioni multilivello che classificano tutti i pacchetti vincolati alla CPU.

L'HWRL viene eseguito per istanza/motore di inoltro sul modulo e può essere visualizzato con il comando **show hardware rate-limiter**. HWRL non rientra nell'ambito di applicazione del presente documento tecnico.

<#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

Conseguenze

- Il traffico del piano dati viene punito al supervisore come una violazione, in quanto non può essere elaborato nell'hardware e quindi

crea pressione sulla CPU.

Consigli

- Per ridurre al minimo le glean drop, in genere la risoluzione di questo argomento è assicurare che l'hop successivo sia raggiungibile e abilitare la limitazione glean con il comando di configurazione: **hardware ip glean throttle**.

Su Nexus 7000 8.4(2), è stato introdotto anche il supporto del filtro bloom per le adiacenze glean per i moduli M3 e F4. Fare riferimento alla guida alla configurazione del routing unicast di Cisco Nexus serie 7000 NX-OS

Esaminare tutte le configurazioni di route statiche che utilizzano indirizzi dell'hop successivo non raggiungibili oppure utilizzare protocolli di routing dinamico che rimuovono tali route dal RIB in modo dinamico.

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

Questa classe fa riferimento ai protocolli del control plane più critici da una prospettiva L3, che includono i protocolli di routing per IPv4 e IPv6, (RIP, OSPF, EIGRP, BGP), auto-RP, virtual port-channel (vPC) e l2pt e 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
```

Conseguenze

Elimina l'instabilità del copp-system-p-class-critical trasferimento ai protocolli di routing, che possono includere adiacenze eliminate o errori di convergenza, o la propagazione update/NLRI.
Le perdite di criteri più comuni in questa classe possono essere correlate a dispositivi non autorizzati nella rete che agiscono in modo anomalo (a causa di una configurazione errata o di un errore) o in modo scalabile.

Consigli

- Se non vengono rilevate anomalie, come un dispositivo anomalo o l'instabilità L2 che provoca una riconvergenza continua dei

protocolli di livello superiore, può essere necessaria una configurazione personalizzata di CoPP o una classe più indulgente per adattarsi alla scala.

- Per informazioni su come configurare un profilo CoPP personalizzato da un profilo predefinito esistente, consultare la guida alla configurazione di CoPP.

Copia della politica di best practice del CoPP

Importante classe - copp-system-p-class-important

Questa classe si riferisce ai protocolli di ridondanza del primo hop (FHRP), che includono HSRP, VRRP e anche 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
```

Conseguenze

Il comportamento più comune che si osserva qui e che porta a cali, sono i problemi di instabilità di livello 2, che portano a dispositivi che passano a scenari di stato attivo (separazione del cervello), timer aggressivi, configurazioni errate o scalabilità.

Consigli:

- Verificare che i gruppi siano configurati correttamente e che i ruoli siano attivi/standby o primari/secondari e siano negoziati correttamente e che non siano presenti flap nello stato.
- Verificare la presenza di problemi di convergenza su L2 o di problemi di propagazione multicast per il dominio L2.

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

La classe L2 unpoliced fa riferimento a tutti i protocolli critici di layer 2 che sono alla base di tutti i protocolli di layer superiore e che pertanto sono considerati quasi senza policy con il CIR e la priorità più elevati.

Questa classe gestisce efficacemente Spanning-Tree Protocol (STP), Link Aggregation Control Protocol (LACP), Cisco Fabric Service over Ethernet (CFSoE)

```
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

Questa classe ha un CIR di polizia di 50 Mbps, il più alto tra tutte le classi, insieme con il più alto assorbimento della velocità di scoppio.

Conseguenze

Le cadute su questa classe possono portare all'instabilità globale, in quanto tutti i protocolli di livello superiore e le comunicazioni su dati, controllo e piani di gestione si basano su una stabilità di livello 2 sottostante.

I problemi con le violazioni STP possono causare problemi di convergenza TCN e STP, che includono controversie STP, scaricamenti MAC, spostamenti e comportamenti disabilitati di apprendimento, che causano problemi di raggiungibilità e possono causare loop di traffico che destabilizzano la rete.

Questa classe fa riferimento anche a LACP e gestisce quindi tutti i pacchetti EtherType associati a 0x8809, che includono tutti i LACPDU utilizzati per mantenere lo stato dei collegamenti del canale porta. L'instabilità su questa classe può causare il timeout dei canali della porta se le LACPDU vengono eliminate.

Cisco Fabric Service over Ethernet (CSFoE) rientra in questa classe e viene utilizzato per comunicare gli stati di controllo delle applicazioni critiche tra gli switch Nexus; pertanto, è essenziale per la stabilità.

Lo stesso vale per altri protocolli all'interno di questa classe, che include CDP, UDLD e VTP.

Consigli

- Il comportamento più comune è correlato all'instabilità Ethernet L2. Verificare che l'STP sia progettato correttamente in modo deterministico, con i relativi miglioramenti alle funzionalità in gioco, per ridurre al minimo l'impatto di dispositivi di riconversione o anomali nella rete. Accertarsi che sia configurato il tipo di porta STP appropriato per tutti i dispositivi host finali che non partecipano all'estensione L2 e che siano configurate come porte trunk edge/edge per ridurre al minimo i TCN.

- Utilizzare i miglioramenti STP, ad esempio BPDUguard, Loopguard, BPDUfilter e RootGuard, quando appropriato, per limitare l'ambito di un guasto o i problemi relativi a configurazioni errate o dispositivi non autorizzati sulla rete.

- Fare riferimento alla guida alla configurazione dello switching di Cisco Nexus 9000 NX-OS Layer 2, versione 10.2(x)

- Verificare i comportamenti di spostamento MAC che possono comportare la disabilitazione dell'apprendimento e degli scaricamenti MAC. Fare riferimento a:Nexus 9000 Mac risoluzione dei problemi e metodi di prevenzione

Class Multicast Router - class-map copp-system-p-class-multicast-router

Questa classe fa riferimento ai pacchetti PIM (Control Plane Protocol Independent Multicast) utilizzati per la creazione e il controllo di alberi condivisi multicast instradati tramite tutti i dispositivi abilitati per PIM nel percorso del piano dati e include i router First-Hop (FHR), Last-Hop Router (LHR), i router Intermediate-Hop (IHR) e i punti di rendering (RP). I pacchetti classificati in questa classe includono la registrazione PIM per le origini, i join PIM per i ricevitori sia per IPv4 che per IPv6, in generale il traffico destinato a PIM (224.0.0.13) e il protocollo MSDP

(Multicast Source Discovery Protocol). Tenere presente che esistono diverse classi aggiuntive che si occupano di porzioni molto specifiche di funzionalità multicast o RP gestite da classi diverse.

```
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
```

Conseguenze

L'impatto principale sulle perdite relative a questa classe è associato a problemi di comunicazione con le origini multicast tramite la registrazione PIM verso le RP o i join PIM non elaborati correttamente, che destabilizzerebbero gli alberi dei percorsi condivisi o più brevi verso le origini del flusso multicast o le RP. Il comportamento può includere l'elenco di interfacce in uscita (OIL) non popolato correttamente a causa di join assenti, o (S, G), o (*, G) non visti in modo coerente nell'ambiente. Possono inoltre verificarsi problemi tra domini di routing multicast che utilizzano MSDP per l'interconnessione.

Consigli

- Il comportamento più comune per i problemi relativi al controllo PIM si riferisce a problemi di scala o comportamenti anomali. Uno dei comportamenti più comuni è dovuto all'implementazione su UPnP, che può causare problemi di esaurimento della memoria. Questo problema può essere risolto tramite filtri e riduzione dell'ambito dei dispositivi non autorizzati. Per ulteriori informazioni su come mitigare e filtrare i pacchetti di controllo multicast che dipendono dal ruolo di rete del dispositivo, vedere: Configure Multicast Filtering on Nexus 7K/N9K - Cisco

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

Questa classe fa riferimento a MLD (Multicast Listener Discovery), in particolare ai tipi di pacchetti MLD query, report, reduction e MLDv2. MLD è un protocollo IPv6 utilizzato da un host per richiedere dati multicast per un gruppo specifico. Con le informazioni ottenute tramite MLD, il software mantiene un elenco di appartenenze a gruppi multicast o a canali per singola interfaccia. I dispositivi che ricevono i pacchetti MLD inviano i dati multicast che ricevono per i gruppi richiesti o per i canali al di fuori del segmento di rete dei ricevitori conosciuti. MLDv1 è derivato da IGMPv2, mentre MLDv2 è derivato da IGMPv3. IGMP utilizza i tipi di messaggi IP Protocol 2, mentre MLD utilizza i tipi di messaggi IP Protocol 58, che è un sottoinsieme dei messaggi 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
```

Conseguenze

I rilasci di questa classe si traducono in problemi relativi alle comunicazioni multicast IPv6 locali del collegamento, che possono causare l'eliminazione dei report del listener dai ricevitori o delle risposte alle query generali, impedendo l'individuazione dei gruppi multicast che gli host desiderano ricevere. Ciò può influire sul meccanismo di snooping e non inoltrare correttamente il traffico in uscita tramite le interfacce previste che hanno richiesto il traffico.

Consigli

- Poiché il traffico MLD è significativo a livello locale rispetto al collegamento per IPv6, se in questa classe vengono rilevate cadute, le cause di comportamento più comuni riguardano la scalabilità, l'instabilità L2 o i dispositivi non autorizzati.

Dati multicast Layer 3 classe - copp-system-p-class-l3mc-data e dati IPv6 multicast Layer 3 classe - copp-system-p-class-l3mcv6-data

Queste classi fanno riferimento al traffico che corrisponde al reindirizzamento di un'eccezione multicast verso la SUP. In questo caso, queste classi gestiscono due condizioni. Il primo è un errore di Inoltro percorso inverso (RPF), il secondo è un errore di destinazione (Destination Miss). Il mancato riscontro nella destinazione si riferisce a pacchetti multicast in cui la ricerca nell'hardware per la tabella di inoltro multicast di layer 3 ha esito negativo e quindi il pacchetto di dati viene indirizzato alla CPU. Questi pacchetti vengono talvolta utilizzati per attivare/installare il control plane multicast e aggiungere le voci delle tabelle di inoltro hardware, in base al traffico del data plane. Anche i pacchetti multicast del piano dati che violano l'RPF soddisferebbero questa eccezione e verrebbero classificati come violazioni.

```
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
```

Conseguenze

Gli errori RPF e gli errori della destinazione implicano un problema di progettazione o configurazione relativo al flusso del traffico attraverso il router multicast. Gli errori di destinazione sono comuni al momento della creazione dello stato, le cadute possono portare alla programmazione e alla creazione di errori (*, G), (S, G).

Consigli

- Apportare modifiche al progetto RIB unicast di base o aggiungere una route statica per indirizzare il traffico attraverso una particolare interfaccia, in caso di errori di RPF.

- Fare riferimento alla sezione Il router non inoltra i pacchetti multicast all'host a causa di un errore RPF

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

Questa classe fa riferimento a tutti i messaggi IGMP, per tutte le versioni utilizzate per richiedere dati multicast per un particolare gruppo, e utilizzate dalla funzionalità di snooping IGMP per mantenere i gruppi e il relativo elenco di interfacce in uscita (OIL) che inoltra il traffico ai ricevitori interessati al layer 2. I messaggi IGMP sono significativi a livello locale perché non attraversano un limite di layer 3, in quanto il valore TTL (Time to Live) deve essere 1, come documentato in RFC2236 (Internet Group Management Protocol, versione 2). I pacchetti IGMP gestiti da questa classe includono tutte le query di appartenenza (generali o specifiche dell'origine o del gruppo), insieme all'appartenenza e ai rapporti di uscita dei destinatari.

```
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
```

Conseguenze

Le interruzioni su questa classe si tradurrebbero in problemi a tutti i livelli di una comunicazione multicast tra origine e destinatario, a seconda del tipo di messaggio IGMP scartato a causa della violazione. Se i rapporti di appartenenza dai ricevitori vengono persi, il router non è a conoscenza dei dispositivi interessati al traffico e quindi non include l'interfaccia/VLAN nel relativo elenco di interfacce in uscita. Se questo dispositivo è anche il querier o il router designato, non attiva i messaggi di join PIM rilevanti verso l'RP se l'origine si trova oltre il dominio locale di layer 2, quindi non stabilisce mai il piano dati attraverso l'albero multicast fino al ricevitore o all'RP. Se il report di abbandono viene perso, il destinatario può continuare a ricevere traffico indesiderato. Ciò può inoltre influire su tutte le query IGMP rilevanti attivate dal querier e sulla comunicazione tra i router multicast di un dominio.

Consigli

- I comportamenti più comuni associati alle cadute IGMP riguardano l'instabilità L2, i problemi con i timer o la scala.

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

Questa classe si riferisce al traffico che corrisponde al traffico ARP standard e include anche il traffico associato a 802.1X, utilizzato per il controllo degli accessi alla rete basato sulle porte. Questa è una delle classi più comuni che incontrano violazioni quando le richieste ARP, i pacchetti ARP Gratuiti e ARP inverso vengono trasmessi e propagati attraverso l'intero dominio di layer 2. È importante ricordare che i pacchetti ARP non sono pacchetti IP, non contengono un'intestazione L3 e quindi la decisione viene presa esclusivamente sull'ambito delle intestazioni L2. Se un router è configurato con un'interfaccia IP associata a tale subnet, ad esempio una SVI (Switch Virtual Interface), il router invia i pacchetti ARP alla SUP per l'elaborazione, in quanto sono destinati all'indirizzo di broadcast hardware. Qualsiasi broadcast storm, loop di livello 2 (causato da STP o flap) o dispositivo di routing nella rete può portare a una tempesta ARP che provoca un aumento significativo delle violazioni.

```
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
```

Conseguenze

L'impatto delle violazioni in questa classe dipende in larga misura dalla durata degli eventi e dal ruolo dello switch sull'ambiente. Le cadute in questa classe implicano che i pacchetti ARP sono al momento scartati e quindi non elaborati dal motore SUP, il che può portare a due comportamenti principali causati da risoluzioni ARP incomplete.

Dal punto di vista dell'host finale, i dispositivi nella rete non sono in grado di risolvere o completare la risoluzione degli indirizzi con lo switch. Se il dispositivo funge da gateway predefinito per il segmento, i dispositivi potrebbero non essere in grado di risolvere il gateway e quindi non essere in grado di eseguire il routing all'esterno del segmento Ethernet (VLAN) L2. I dispositivi possono ancora comunicare sul segmento locale se possono completare la risoluzione ARP per altri host terminali sul segmento locale.

Dal punto di vista dello switch, se la tempesta e le violazioni sono prevalenti, lo switch può anche non essere in grado di completare il processo per la richiesta ARP generata. Queste richieste vengono in genere generate per le risoluzioni di subnet con hop successivo o con connessione diretta. Anche se le risposte ARP sono di natura unicast, in quanto sono indirizzate al MAC di proprietà dello switch, sono classificate nella stessa classe, in quanto sono ancora pacchetti ARP. Questo si traduce in problemi di raggiungibilità perché lo switch non può elaborare correttamente il traffico se l'hop successivo non viene risolto. Inoltre, può causare problemi con la riscrittura dell'intestazione di layer 2, se il gestore delle adiacenze non dispone di una voce per l'host.

L'impatto dipende anche dalla portata della questione fondamentale che ha innescato la violazione ARP. Ad esempio, in una tempesta di trasmissione, gli host e lo switch continuano a raggiungere l'ARP per tentare di risolvere l'adiacenza, il che può portare a un ulteriore traffico di trasmissione sulla rete e, poiché i pacchetti ARP sono al layer 2, non esiste un TTL (Time to Live) di layer 3 per interrompere un loop L2 e quindi continuano a loop e a crescere esponenzialmente attraverso la rete fino a quando il loop non viene interrotto.

Consigli

- Risolvere qualsiasi instabilità L2 fondamentale che può causare tempeste ARP nell'ambiente, come STP, flap o dispositivi non autorizzati. Interrompere tali loop in base alle esigenze, con qualsiasi metodo desiderato per aprire il percorso del collegamento.

- Il controllo della tempesta può essere utilizzato anche per mitigare una tempesta ARP. Se il controllo temporale non è abilitato, verificare le statistiche dei contatori sulle interfacce per verificare la percentuale di traffico di broadcast rilevato sulle interfacce rispetto al traffico totale che passa attraverso l'interfaccia.

- Se non c'è nessuna tempesta, ma si osservano ancora cali costanti sull'ambiente, verificare il traffico SUP per identificare eventuali dispositivi anomali, che inviano costantemente pacchetti ARP sulla rete, che possono influire sul traffico legittimo.

- Gli incrementi che possono essere rilevati dipendono dal numero di host sulla rete e dal ruolo dello switch sull'ambiente. Il protocollo ARP è progettato per riprovare, risolvere e aggiornare le voci, in modo da visualizzare sempre il traffico ARP. Se vengono rilevate solo cadute sporadiche, possono essere transitorie a causa del carico della rete e non si percepisce alcun impatto. Ma è importante monitorare e conoscere la rete per identificare e differenziare in modo appropriato un'attesa da una situazione anomala.

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

Questa classe fa riferimento al traffico associato ai pacchetti di annunci e richieste router e ai pacchetti di annuncio dei router adiacenti IPv6 che utilizzano messaggi ICMP per determinare gli indirizzi del livello di collegamento locale dei router adiacenti e viene utilizzata per la raggiungibilità e il rilevamento dei dispositivi adiacenti.

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

Conseguenze

Le violazioni di questa classe possono impedire la comunicazione IPv6 tra dispositivi adiacenti, in quanto questi pacchetti vengono utilizzati per facilitare l'individuazione dinamica o le informazioni a livello di collegamento/locale tra host e router sul collegamento locale. Un'interruzione di questa comunicazione può inoltre causare problemi di raggiungibilità oltre o attraverso il collegamento locale associato. In caso di problemi di comunicazione tra i router adiacenti IPv6, assicurarsi che non vi siano cali in questa classe.

Consigli

- Esaminare tutti i comportamenti ICMP anomali rilevati dai dispositivi adiacenti, in particolare quelli relativi all'individuazione dei dispositivi adiacenti e/o del router.
- Verificare che tutti i valori di timer e intervallo previsti per i messaggi periodici siano coerenti nell'ambiente e rispettati. Ad esempio, per i messaggi di annuncio router (messaggi RA).

Class Normal DHCP - copp-system-p-class-normal-dhcp

Questa classe si riferisce al traffico associato al protocollo BOOTP (client/server BOOTP), comunemente noto come pacchetti DHCP (Dynamic Host Control Protocol) sullo stesso segmento Ethernet locale per IPv4 e IPv6. In particolare, questo riguarda solo le comunicazioni del traffico provenienti da qualsiasi client di avvio o destinate a qualsiasi server BOOTP, attraverso l'intero scambio di pacchetti DORA (Discovery, Offre, Request, and Recognition) e include anche le transazioni client/server DHCPv6 attraverso le porte 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

Conseguenze

Le violazioni di questa classe possono impedire agli host terminali di acquisire correttamente un indirizzo IP dal server DHCP e quindi di ripristinare l'intervallo di indirizzi IP privati automatici (APIPA), 169.254.0.0/16. Tali violazioni possono verificarsi in ambienti in cui i dispositivi tentano di avviarsi simultaneamente e quindi vanno oltre il CIR associato alla classe.

Consigli

- Verificare con le acquisizioni, sugli host e sul server DHCP che l'intera transazione DORA sia visibile. Se lo switch fa parte di questa comunicazione, è importante anche verificare i pacchetti elaborati o puntati alla CPU e verificare le statistiche sullo switch: **show ip dhcp global statistics** e i reindirizzamenti: **show system internal access-list sup-redirect-stats module 1 | grep -i dhcp**.

Risposta di inoltro DHCP normale alla classe - copp-system-p-class-normal-dhcp-relay-response

Questa classe fa riferimento al traffico associato alla funzionalità di inoltro DHCP per IPv4 e IPv6, indirizzato ai server DHCP configurati nell'inoltro. Questo riguarda specificamente solo le comunicazioni di traffico provenienti da qualsiasi server BOOTP o destinate a qualsiasi client BOOTP attraverso l'intero scambio di pacchetti DORA, e include anche le transazioni client/server DHCPv6 attraverso le porte 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
```

Conseguenze

Le violazioni per questa classe hanno lo stesso impatto delle violazioni per la classe copp-system-p-class-normal-dhcp, in quanto entrambe fanno parte della stessa transazione. Questa classe si concentra principalmente sulle comunicazioni di risposta dai server agente di inoltro. Nexus non funge da server DHCP, ma è progettato solo per funzionare come agente di inoltro.

Consigli

- Le stesse raccomandazioni della classe DHCP normale si applicano qui. Poiché la funzione di Nexus è quella di fungere solo da agente di inoltro, sulla SUP ci si aspetta di vedere l'intera transazione tra l'host e lo switch che funge da relay e lo switch e i server configurati.

- Verificare che non vi siano dispositivi non autorizzati, ad esempio server DHCP imprevisti nella rete che rispondono all'ambito o dispositivi bloccati in un loop che inviano pacchetti di individuazione DHCP alla rete. Controlli aggiuntivi possono essere eseguiti dai comandi: show ip dhcp relay e **show ip dhcp relay statistics**.

Flusso NAT classe - copp-system-p-class-nat-flow

Questa classe si riferisce al traffico di flusso NAT dello switch software. Quando viene creata una nuova traduzione dinamica, il flusso viene inoltrato tramite software fino a quando la traduzione non viene programmata nell'hardware, quindi viene controllato da CoPP per limitare il traffico indirizzato al supervisore durante l'installazione della voce nell'hardware.

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

Conseguenze

Le interruzioni in questa classe si verificano in genere quando nell'hardware viene installata una frequenza elevata di nuove conversioni e flussi dinamici. L'impatto si riferisce ai pacchetti con commutazione software che vengono scartati e non consegnati all'host finale, e che possono

causare perdite e ritrasmissioni. Una volta installata la voce nell'hardware, il supervisore non potrà ricevere altro traffico.

Consigli

- Verificare le linee guida e i limiti della NAT dinamica sulla piattaforma pertinente. Esistono limitazioni note documentate sulle piattaforme, ad esempio lo switch 3548, in cui la traduzione può richiedere alcuni secondi. Fare riferimento a: Restrizioni per NAT dinamico

Eccezione classe - copp-system-p-class-exception

Questa classe fa riferimento ai pacchetti di eccezione associati all'opzione IP e ai pacchetti IP ICMP "destinazione irraggiungibile". Se l'indirizzo di destinazione non è presente nella base di informazioni per l'inoltro (FIB) e si verifica un errore, la SUP invia un pacchetto ICMP "destinazione irraggiungibile" al mittente. Anche i pacchetti con opzioni IP abilitate rientrano in questa classe. Per i dettagli sulle opzioni IP, consultare il documento IANA: IP Option Numbers

```
 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
```

Conseguenze

Questa classe è sottoposta a un controllo rigoroso e le cadute su di essa non sono indicative di un errore, bensì di un meccanismo di protezione che limita l'ambito dei pacchetti ICMP "destinazione irraggiungibile" e IP Options.

Consigli

- Verificare se sono presenti flussi di traffico visti o puntati alla CPU per destinazioni non presenti sul FIB.

Reindirizzamento classe - copp-system-p-class-redirect

Questa classe si riferisce al traffico associato al protocollo PTP (Precision Time Protocol), utilizzato per la sincronizzazione dell'ora. Ciò include il traffico multicast per l'intervallo riservato 224.0.1.129/32, il traffico unicast sulla porta UDP 319/320 e l'etipo 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
```

Conseguenze

Le interruzioni in questa classe possono causare problemi nei dispositivi che non sono stati sincronizzati correttamente o che non hanno stabilito la gerarchia corretta.

Consigli

- Verificare la stabilità degli orologi e la loro corretta configurazione. Verificare che il dispositivo PTP sia configurato per la modalità PTP multicast o unicast, ma non per entrambe le modalità contemporaneamente. Anche questo è documentato dalle linee guida e dalle limitazioni e può spingere il traffico oltre la velocità di input impegnata.

- Esaminate la progettazione e la configurazione dell'orologio di contorno e di tutti i dispositivi PTP presenti nell'ambiente. Verificare che tutte le linee guida e le limitazioni siano rispettate per piattaforma in quanto sono diverse.

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

Questa classe fa riferimento al traffico associato alle operazioni dell'agente OpenFlow e alla connessione TCP corrispondente tra il controller e l'agente.

```
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
```

Conseguenze

Le interruzioni in questa classe possono causare problemi agli agenti che non ricevono ed elaborano correttamente le istruzioni dal controller per gestire il piano di inoltro della rete

Consigli

- Assicurarsi che non venga rilevato traffico duplicato sulla rete o su qualsiasi dispositivo che impedisca la comunicazione tra il controller e gli agenti.

- Verificare che la rete L2 non presenti instabilità (STP o loop).

Risoluzione dei problemi relativi alle perdite CoPP

Per risolvere i problemi relativi alle violazioni del protocollo CoPP, è necessario innanzitutto determinare:

- Impatto e portata del problema.

- Comprendere il flusso del traffico attraverso l'ambiente e il ruolo dello switch nella comunicazione interessata.

- Determinare se sono presenti violazioni nella classe associata sospette e ripetere l'operazione se necessario.

Ad esempio, è stato rilevato il comportamento elencato:

- I dispositivi non possono comunicare con altri dispositivi esterni alla rete, ma possono comunicare localmente.
- L'impatto è stato isolato sulle comunicazioni indirizzate all'esterno della VLAN e lo switch funge da gateway predefinito.
- Un controllo degli host indica che non è possibile eseguire il ping del gateway. Dopo aver controllato la tabella ARP, la voce relativa al gateway rimane Incomplete.
- Tutti gli altri host in cui il gateway è stato risolto non hanno problemi di comunicazione. Un controllo del protocollo CoPP sullo switch che funge da gateway indica che sono presenti violazioni in 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;

- Inoltre, più controlli dei comandi mostrano che le cadute sono in aumento.
- Queste violazioni possono causare la perdita del traffico ARP legittimo e comportare un comportamento di rifiuto dei servizi.

È importante sottolineare che il CoPP isola l'impatto sul traffico associato alla classe specifica, che in questo esempio sono ARP e copp-system-p-class-normal. Il traffico correlato ad altre classi, ad esempio OSPF, BGP, non viene eliminato dal protocollo CoPP, in quanto rientrano interamente in una classe diversa. Se questa opzione non viene selezionata, i problemi ARP possono sovrapporsi ad altri problemi, che possono influire sui protocolli a partire dai quali si basano. Ad esempio, se una cache ARP scade e non viene aggiornata a causa di violazioni eccessive, una sessione TCP come BGP può terminare.

- Si consiglia di eseguire i controlli del piano di controllo, ad esempio l'etanalizzatore, lo stato in banda della CPU-mac e il processo della CPU per isolare ulteriormente la materia.

Etanalizzatore

Poiché il traffico controllato dal CoPP è associato solo al traffico basato sulla CPU, uno degli strumenti più importanti è l'Ethanalyzer. Questo strumento è un'implementazione Nexus di TShark e consente l'acquisizione e la decodifica del traffico inviato e ricevuto dal supervisore. Può

inoltre utilizzare filtri basati su criteri diversi, ad esempio protocolli o informazioni di intestazione, diventando così uno strumento prezioso per determinare il traffico inviato e ricevuto dalla CPU.

Si consiglia di esaminare in primo luogo il traffico ARP rilevato dal supervisore quando lo strumento Ethanalyzer viene eseguito direttamente nella sessione terminale o inviato a un file per l'analisi. È possibile definire filtri e limiti per focalizzare l'acquisizione su un modello o un comportamento specifico. A tale scopo, aggiungere filtri di visualizzazione flessibili.

Un'errata convinzione comune è che Ethanalyzer cattura tutto il traffico che attraversa lo switch. Il traffico del piano dati, tra gli host, viene commutato o instradato dagli ASIC hardware tra le porte dati senza il coinvolgimento della CPU e quindi di solito non viene rilevato dall'acquisizione di Ethanalyzer. Per catturare il traffico del piano dati, si consiglia di utilizzare altri strumenti, quali ELAM o SPAN. Ad esempio, per filtrare ARP, utilizzare il comando:

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

Campi configurabili importanti:

- interface inband - si riferisce al traffico diretto alla SUP
- display-filter arp - si riferisce al filtro applicato, la maggior parte dei filtri Wireshark sono accettati
- limit-captured-frames 0 - si riferisce al limite, 0 equivale a illimitato, fino a quando non viene arrestato da un altro parametro o viene arrestato manualmente da Ctrl+C
- autostop duration 60 - si riferisce all'arresto di Ethanalyzer dopo 60 secondi, creando così un'istantanea di 60 secondi di traffico ARP rilevato sulla CPU

L'output di Ethanalyzer viene reindirizzato a un file sul bootflash con > arpcpu, per essere elaborato manualmente. Dopo 60 secondi, l'acquisizione viene completata e l'etanalizzatore termina in modo dinamico. L'arpcpu dei file si trova sul bootflash dello switch, che può essere elaborato per estrarre i talker superiori. Ad esempio:

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

Questo filtro viene ordinato in base alle colonne di origine e di destinazione, quindi alle corrispondenze univoche trovate (ignorando la colonna della data), conta le istanze e aggiunge il numero visualizzato e infine ordina dall'alto in basso in base al conteggio e visualizza i primi 50 risultati.

In questo esempio di laboratorio, in 60 secondi, sono stati ricevuti più di 600 pacchetti ARP da tre dispositivi, identificati come dispositivi che potrebbero aver commesso il reato. Nella prima colonna del filtro viene indicato il numero di istanze dell'evento rilevate nel file di acquisizione nella durata specificata.

È importante capire che lo strumento Ethanalyzer agisce sul driver in banda, che è essenzialmente la comunicazione nell'ASIC. In teoria, il pacchetto deve passare attraverso il kernel e il gestore pacchetti per essere consegnato al processo associato stesso. Il CoPP e l'HWRL

intervengono prima che il traffico venga visto sull'Ethanalyzer. Anche se le violazioni sono in aumento, parte del traffico continua a passare ed è conforme alla frequenza della polizia, il che aiuta a fornire una visione dei flussi di traffico puniti alla CPU. Si tratta di una distinzione importante, in quanto il traffico visto sull'Ethanalyzer NON è il traffico che ha violato il CIR ed è stato scartato.

L'etanalyzer può anche essere usato in modo aperto, senza alcun filtro di visualizzazione o filtro di cattura specificato per catturare tutto il traffico SUP rilevante. Può essere utilizzato come misura di isolamento come parte dell'approccio per la risoluzione dei problemi.

Per ulteriori dettagli e per l'uso dell'etanalyzer, fare riferimento alla nota tecnica:

Guida alla risoluzione dei problemi di Ethanalyzer su Nexus 7000

Uso di Ethanalyzer su piattaforma Nexus per l'analisi del traffico del control plane e del data-plane

---

Nota: Nexus 7000, prima del rilascio del codice 8.X, può eseguire solo le acquisizioni di Ethanalyzer attraverso il VDC di amministrazione, che comprende il traffico associato a SUP da tutti i VDC. VDC-specifico Ethanalyzer è presente nei codici 8.X.

Statistiche in banda CPU-MAC

Le statistiche in banda associate al traffico basato sulla CPU mantengono le statistiche pertinenti del traffico in banda TX/RX della CPU. Queste statistiche possono essere controllate con il comando: show hardware internal cpu-mac inband stats, che fornisce informazioni dettagliate sulla velocità corrente e sulla velocità di picco.

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

È buona norma creare e tenere traccia di una baseline in quanto, a causa del ruolo dello switch e dell'infrastruttura, i risultati dell'output **show hardware internal cpu-mac inband stats** variano in modo significativo. In questo ambiente di laboratorio, i valori usuali e i picchi storici non sono in genere maggiori di qualche centinaio di punti percentuali, e quindi questo è anormale. Il comando **show hardware internal cpu-mac inband events** è utile anche come riferimento cronologico, in quanto contiene dati relativi al picco di utilizzo e all'ora in cui è stato rilevato.

CPU processo

Gli switch Nexus sono sistemi basati su Linux e il sistema operativo Nexus (NXOS) sfrutta i vantaggi della pianificazione preventiva della CPU, del multitasking e del multithreading della rispettiva architettura dei core per fornire un accesso equo a tutti i processi, pertanto i picchi non sono sempre indicativi di un problema. Tuttavia, se si rilevano violazioni del traffico prolungate, è probabile che anche il processo associato venga utilizzato in modo intensivo e venga visualizzato come una risorsa principale sotto gli output della CPU. Eseguire più istantanee dei processi della CPU per verificare l'elevato utilizzo di un determinato processo utilizzando: **show processes cpu sort | exclude 0.0 or show processes cpu sort | grep <process>**.

Le verifiche della CPU, dello stato in-band e di Ethanalyzer forniscono informazioni dettagliate sui processi e sul traffico attualmente elaborati dal supervisor e aiutano a isolare l'instabilità continua sul traffico del control plane che può verificarsi in caso di problemi del data plane. È importante capire che il CoPP è un meccanismo di protezione. È reazionario perché agisce solo sul traffico puntato alla SUP. L'obiettivo è salvaguardare l'integrità del supervisore eliminando i tassi di traffico che superano gli intervalli previsti. Non tutte le cadute indicano un problema o richiedono un intervento, in quanto la loro importanza riguarda la specifica classe CoPP e l'impatto verificato, in base alla progettazione dell'infrastruttura e della rete. Le cadute causate da eventi burst sporadici non si traducono in impatto, in quanto i protocolli dispongono di meccanismi incorporati, ad esempio keepalive e tentativi che possono gestire eventi transitori. Mantieni l'attenzione su eventi sostenuti o anormali oltre le previsioni stabilite. Tenere presente che il CoPP deve rispettare i protocolli e le funzionalità specifiche dell'ambiente e deve essere monitorato e ripetuto continuamente per ottimizzarlo in base alle esigenze di scalabilità man mano che si evolvono. In caso di caduta, stabilire se il CoPP ha interrotto il traffico in modo involontario o in risposta a un malfunzionamento o a un attacco. In entrambi i casi, analizzare la situazione e valutare la necessità di intervenire analizzando l'impatto e le misure correttive sull'ambiente, che possono esulare dall'ambito di applicazione dello switch stesso.

Ulteriori informazioni

Piattaforme/codici recenti, possono avere la capacità di eseguire un SPAN-to-CPU, dal mirror di una porta e punt del traffico del piano dati alla CPU. Questo è in genere fortemente limitato dalla velocità limite dell'hardware e dal CoPP. Si consiglia di usare con attenzione lo SPAN sulla CPU e ciò esula dall'ambito di questo documento.

Per ulteriori informazioni su questa funzione, consultare le note tecniche elencate:

Procedura SPAN-to-CPU Nexus 9000 Cloud Scale ASIC NX-OS

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).