

De betekenis van ongebruikelijke TCAM-toepassingsniveaus op Nexus 7000

Inhoud

[Inleiding](#)

[Achtergrond](#)

[Voorwaarden](#)

[Gebruikte componenten](#)

[Waarneming](#)

[Egress RACL ingesteld op basis en subinterfaces terwijl NetFlow alleen is ingeschakeld voor hoofdinterfaces](#)

[Wanneer zowel RACL als NetFlow worden geconfigureerd op de hoofdinterface en de subinterface](#)

[Resolutie](#)

[Samenvatting](#)

[Verwante tekortkomingen](#)

[Verwante artikelen](#)

Inleiding

Dit document legt uit hoe TCAM onverwachts te veel wordt gebruikt, afhankelijk van de functiesets die zijn ingeschakeld op een Nexus 7000 Series-schakelaar.

Probleembeschrijving

Als atoomupdates beschikbaar zijn, in het geval van meer dan één functie zoals RACL, wordt NetFlow op verschillende interfaces toegepast, kan dit een overgebruikfoutmelding van de TCAM veroorzaken alhoewel de grens van 50% niet is bereikt.

Voorbeeld: Kan geen meerdere functies op de volgende subinterfaces toepassen, ondanks dat het gebruik 29,57 is, terwijl de bovenste limiet 50% is (omdat atoomupdates zijn ingeschakeld) en de onderstaande fout is weggegooid.

FOUT: Module 1 geeft de status terug: TCAM wordt overgebruikt, schakelt u bankketting in en/of schakelt u de atoomupdate uit. Indien de "bank-chaining" op andere modules is ingeschakeld en dit een nieuwe invoeging van lijnkaart is, schakelt u de "bank-chaining" in voordat u deze module opnieuw laadt.

Na het opnieuw laden verliezen alle interfaces hun configuratie en worden ze om deze reden toegewezen aan VDC 0.

Achtergrond

Door middel van atoomupdates die standaard op Nexus 7000 zijn ingeschakeld, kan slechts 50% van de gehele TCAM worden gebruikt. De andere 50% is voorbehouden om wijzigingen van ACL's aan te brengen zodat niet-ontwrichtende updates van ACL's beschikbaar zijn. Meer informatie hierover is te vinden via de links die in het hoofdstuk zijn opgenomen: Aanbevolen lezen

Voorwaarden

De volgende onderwerpen worden aangeraden:

Atoomupdates
TCAM op N7000

Gebruikte componenten

De informatie in dit document is gebaseerd op de laboratoriumtests die op N7718-chassis op de module zijn uitgevoerd: N77-F312CK-26 actief op versie 8.3(2)

Alle apparaten die in dit document worden gebruikt begonnen met een standaardconfiguratie en de tentoongestelde functies zijn RACL, NetFlow.

Waarneming

Egress RACL ingesteld op basis en subinterfaces terwijl NetFlow alleen is ingeschakeld voor hoofdinterfaces

Eerste configuratie:

```
Interface Ethernet 11/2: Layer-3; RACL
Interface Ethernet 11/2.300-302: Layer-3; RACL
```

TCAM-gebruik met alleen RACL toegepast is:

```
N7718(config-if)# show system internal access-list resource utilization module 11 | in "Tcam 1, Bank 0" across all instances:
```

```
Tcam 1, Bank 0 1211 2885 29.57
Tcam 1, Bank 0 1211 2885 29.57
Tcam 1, Bank 0 1211 2885 29.57
```

Opmerking: De TCAM-ruimtetoeëpassing voor uitgaande RACL in dit document wordt verondersteld 29,57% te zijn.

In één keer wordt NetFlow alleen op de hoofdinterface toegepast, verdubbelt de interfacebenutting, hoewel de NetFlow-configuratie in deze situatie nauwelijks 1% ruimte vergt.

```
Interface Ethernet 11/2: Layer-3; RACL; NetFlow
Interface Ethernet 11/2.300-302: Layer-3; RACL
```

Hier is de hoofdinterface NetFlow geconfigureerd terwijl de subinterface geen NetFlow(Atomic updates heeft om dit gedrag te observeren)

```
N7718(config-if)# show system internal access-list resource utilization module 11 | in "Tcam 1, Bank 0"
Tcam 1, Bank 0 2394 1702 58.45
Tcam 1, Bank 0 2394 1702 58.45
Tcam 1, Bank 0 2394 1702 58.45
```

Opmerking: Indien atoomupdates nog steeds waren ingeschakeld, zou dit verdubbelingsgedrag niet mogelijk zijn aangezien de limiet met atoomupdates slechts 50% is en de volgende fout is gezien:

FOOT: Module 1 geeft de status terug: TCAM wordt overgebruikt, schakelt u bankketting in en/of schakelt u de atoomupdate uit. Indien de "bank-chaining" op andere modules is ingeschakeld en dit een nieuwe invoeging van lijnkaart is, schakelt u de "bank-chaining" in voordat u deze module opnieuw laadt.

Uitleg:

In dit geval zijn hier twee verschillende beleidsvormen aanwezig. De ene bestemming heeft alleen RACL en een andere bestemming heeft RACL +NF. Daarom worden twee reeksen TCAM-items toegewezen voor dezelfde functies, wat het verdubbelende gedrag veroorzaakt dat we zien als de werkelijke consumptie zou slechts 29,57 gedrag moeten zijn.

Het apparaat bereikt dit door twee aparte labels voor beide interfaces te genereren, zoals hieronder wordt aangegeven:

```
module-11# show system internal access-list interface e11/2 out statistics

INSTANCE 0x0
```

Tcam 1 resource usage:

Label_b = 0x801 >>> LABEL is 0x801

module-11# show system internal access-list interface e11/2.300 out statistics

INSTANCE 0x0

Tcam 1 resource usage:

Label_b = 0x802 >>> NEW LABEL 0x802 IS GENERATED

Wanneer zowel RACL als NetFlow worden geconfigureerd op de hoofdinterface en de subinterface

reeds bestaande configuratie uit zaak 1:

Interface Ethernet 11/2: Layer-3; RACL; NetFlow

Interface Ethernet 11/2.300-302: Layer-3; RACL

Pas nu ook NetFlow op de rest van de subinterfaces toe:

Interface Ethernet 11/2: Layer-3; RACL; NetFlow

Interface Ethernet 11/2.300-302: Layer-3; RACL; NetFlow

Aangezien alle bestemmingen nu RACL + NetFlow zijn geconfigureerd, wordt hetzelfde label gedeeld met b/w bestemming (één set TCAM-items die door alle interfaces worden gerefereerd).

N7718(config-if)# show system internal access-list resource utilization module 11 | in "Tcam 1, Bank 0"

Tcam 1, Bank 0 1211 2885 29.57

Tcam 1, Bank 0 1211 2885 29.57

Tcam 1, Bank 0 1211 2885 29.57

module-11# show system internal access-list interface ethernet11/2 out statistics |in Label_b p 5 n 4

INSTANCE 0x0

Tcam 1 resource usage:

Label_b = 0x802 >>> LABEL is 0x802

module-11# show system internal access-list interface ethernet11/2.300 out statistics |in Label_b p 5 n 4

INSTANCE 0x0

Tcam 1 resource usage:

Label_b = 0x802 >>> SAME LABEL IS MAINTAINED

Opmerking: Dit gedrag wordt ook uitgebreid naar fysieke interfaces, subinterfaces. Alleen wanneer alle betrokken bestemmingen dezelfde configuratie hebben, zal de TCAM-benutting niet worden verdubbeld.

Merk op dat de TCAM alleen nadat NetFlow is toegepast op alle interfaces die al RACL hebben, zal teruglopen naar origineel 29,57%

1. Pas RACL toe op interface "1": 29.57%

2. Pas RACL op volgende interfaces toe: 29.57%

3. Pas NF toe na de RACL-toepassing op interface "1": 58.45%

4. NF op volgende interfaces toepassen: 58.45%

5. NF op laatste interface toepassen: 29.57%

Resolutie

1. Schakel atoomupdates uit.

<OF>

2. Verlaag de ACL-grootte om de limiet op <25% te houden.

Samenvatting

Met atoomupdates:

Zodra, wordt NetFlow op de eerste interface toegepast, wordt de creatie van een afzonderlijk exemplaar van TCAM geprobeerd aangezien de eerste interface nu zowel ACL, NF gevormd heeft maar de tweede interface slechts RACL gevormd heeft.

Als er echter atoomupdates worden ingeschakeld, zal een afzonderlijke instantie-creatie er niet in slagen dit te doen, het gebruik tot > 50 verhogen. Bijgevolg wordt de te veel gebruikte TCAM-fout geworpen.

Zonder atoomupdates:

1. Bij toepassing van ACL op alle interfaces: Het blijft op 29 jaar, omdat er geen andere kenmerken zijn.
2. Pas NetFlow op de eerste interface toe: Switch veronderstelt dit om een afzonderlijke configuratie van functies/combinatie van functies (handhaaft een afzonderlijk intern label) en creëert daarom een afzonderlijk exemplaar op dezelfde bank.
3. Zodra NetFlow is toegepast op alle andere interfaces die ACL zijn ingesteld, is de configuratie/combinatie van functies hetzelfde (Label is nu hetzelfde voor beide interfaces) en vindt er dus een herschikking plaats
4. TCAM is nu gedeeld voor beide interfaces en het gebruik is gedaald naar 29,57%.

Dit is een methode van optimalisatie wanneer combinaties van functies op verschillende interfaces worden gebruikt.

Verwante tekortkomingen

[CSCvs50014](#) ACL en NetFlow op subinterface beslaan dubbele TCAM-items

Verwante artikelen

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/security/config/cisco_nexus7000_security_config_guide_8x/configuring_ip_acls.html

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/security/configuration/guide/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide_Release_6-x/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide_Release_6-x_chapter_01110.html#con_1458580