Uitleg van fouten van Packet Drop in ACI

Inhoud

Inleiding

Dit document beschrijft elk type fout en de procedure wanneer u deze fout ziet. Tijdens normaal gebruik van een Cisco Application Centric Infrastructure (ACI) Fabric kan de beheerder fouten zien voor bepaalde typen pakketdrops.

Beheerde objecten

In Cisco ACI, worden alle fouten verhoogd onder Beheerde Voorwerpen (MO). De fout " *F11245 - INGress druppelt Packets rate (l2IngrPacketsAg15min:dropRate)* is bijvoorbeeld wat betreft de parameter *dropRate* in MO *l2IngrPktsAg15min*.

Deze sectie introduceert een paar voorbeeld van **Managed Object (MO) met betrekking tot het sluiten van pakketfouten**.

Voorbeeld	Beschrijving	Steekproeven	Monster MO tegen welke gebreken zich voordoen
l2Ingr-producten	l2Ingr-pkts5min	Dit representeert	droging	VLANCktEp

	l2Ingr-poorten15min l2IngrPKTS1h enz.	inbraakpakketstatistieken per VLAN tijdens elke periode	overvloed multicast snelheid unicast	(VLAN)
l2IngrPktsAG	l2IngrPktsAg15min l2IngrPktsAg1h l2IngrPktsAg1d enz.	Dit staat voor inbraakpakketstatistieken per EPG, BD, VRF etc... Ex.) EPG-status staat voor aggregatie van VLAN-stats die tot de EPG behoren	droging overvloed multicast snelheid unicast	fvAEPg (EPG) APvAP (toepassingsprofiel) fvBD (BD) l3extOut (L3OUT)
qptIngrDrop	qptIngrDrop15min CWDM100 nm 2000 qptIngrDropPkts1d enz.	Dit staat voor inbraakpakketstatistieken per interface tijdens elke periode	*1 verzendingssnelheid *1 foutRate *1 buffersnelheid	l1PhysIf (fysieke poort) pcAggrAs (poortkanaal)

*1 : Deze tellers in qptIngrDropPkts kunnen vals verhoogd worden door een ASIC beperking in verscheidene Nexus 9000 Platforms, omdat de pakketten SUP_REDIRECT als voorwaartse druppels worden geregistreerd. Zie ook CSCvo68407 en CSCvn72699 voor meer details en vaste versies .

Hardware Drop Countertypes

Op Nexus 9000 switches die in ACI-modus draaien, zijn er 3 belangrijke hardwaretelers voor ingress interface-valreep op de ASIC.

Een dropRate in l2IngrPkts, l2IngrPktsAg bevat deze tellers. Drie parameters (forwardRate, errorRate, bufferRate) in de bovenstaande tabel voor qptIngrDropPkts vertegenwoordigen elke drie interfacetellers.

voorwaarts

Voorwaartse druppels, zijn pakketten die op de lookUp blok (LU) van de ASIC worden gedropt. In het blok LU wordt een pakketdoorvoerbeslissing genomen op basis van de informatie over de pakketheader. Als de beslissing is om het pakket te laten vallen, wordt Forward Drop geteld. Er zijn verschillende redenen waarom dit kan gebeuren, maar laten we het hebben over de belangrijkste:

SECURITY_GROUP_DENY

Een daling omdat er contracten ontbreken om de communicatie mogelijk te maken.

Wanneer een pakket in het weefsel komt, kijkt de switch naar de bron en de bestemming EPG om te zien of er een contract is dat deze communicatie toestaat. Als de bron en de bestemming in verschillende EPG's zijn, en er geen contract is dat dit pakkettype tussen hen toestaat, zal de switch het pakket laten vallen en het als SECURITY_GROUP_DENY labelen. Deze verhoging van de Voorwaartse teller.

VLAN_XLATE_MISS

Een daling vanwege ongepast VLAN.

Wanneer een pakje in het weefsel komt, kijkt de switch naar het pakje om te bepalen of de configuratie op de poort dit pakje toestaat. Bijvoorbeeld, ingaat een kader de stof met een tag 802.1Q van 10. Als de switch VLAN 10 op de haven heeft, zal zij de inhoud inspecteren en een expediteur besluit op basis van de MAC van de Bestemming maken. Maar als VLAN 10 niet op de haven is, zal het vallen en het als VLAN_XLATE_MISS etiketteren. Dit zal de Forward Drop teller verhogen.

De reden voor "XLATE" of "Vertaling" is dat de bladeswitch-switch in ACI een kader met een 802.1Q-netje neemt en deze vertaalt naar een nieuw VLAN dat wordt gebruikt voor VXLAN en andere normalisatie in het weefsel. Als het frame wordt ingestuurd met een VLAN dat niet wordt uitgevoerd, zal "vertaling" mislukken.

ACL_DROP

Een druppel vanwege sup-tcam.

sup-tcam in ACI-switches bevat bijzondere voorschriften die bovenop de normale L2/L3-verzendingsbeschikking moeten worden toegepast. De regels in sup-tcam zijn ingebouwd en kunnen niet door de gebruiker worden ingesteld. Het doel van de sup-tcam-regels is voornamelijk om bepaalde uitzonderingen of bepaalde vormen van controle-vliegtuigverkeer te verwerken en niet bedoeld om door gebruikers te worden gecontroleerd of gecontroleerd. Wanneer het pakje sup-tcam regels inslaat en de regel het pakket moet laten vallen, wordt het geworpen pakket geteld als ACL_DROP en het verhoogt de voorwaartse druppelteller. Wanneer dit gebeurde, betekent het meestal dat het pakje tegen de basisprincipes van het door-sturen van ACI doorgestuurd wordt.

Merk op dat, alhoewel de vervolgnaam ACL_DROP is, deze "ACL" niet hetzelfde is als normale Toegangscontrolelijst die kan worden ingesteld op standalone NX-OS apparaten of andere routing/switching apparaten.

SUP_REDIRECT

Dit is geen druppel.

Een vervolgbaar pakket (d.w.z. CDP/LLDP/UDLD/BFD enz.) kan worden geteld als voorwaartse Drop zelfs wanneer het pakket correct verwerkt en naar CPU wordt doorgestuurd.

Dit kan alleen voorkomen in -EX-platform zoals N9K-C93180YC-EX. Deze dienen niet als "val" te worden geteld, maar vanwege ASIC-beperking in het EX-platform.

Fout

Wanneer de switch een ongeldig kader op één van de voorpaneelinterfaces ontvangt, wordt het als een fout gedropt. Voorbeelden hiervan zijn frames met FCS- of CRC-fouten.
Bij normale activiteiten wordt echter verwacht dat de foutenpakketten in de Uplink-poorten van bladeren of ruggengraat toenemen. Wanneer u blaaspoorten of spinpoorten bekijkt, is het beter om op FCS/CRC-fouten te controleren met behulp van "Show interface".

buffer

Als de switch een frame ontvangt en er geen bufferkredieten beschikbaar zijn voor indringers of stress, zal het frame achteruit gaan met "Buffer". Dit wijst meestal op een congestie ergens in het netwerk. De link die de fout toont kan volledig zijn, of de link die de bestemming bevat kan verstopt zijn.

Drop Stats in CLI bekijken

Beheerde objecten

Secure Shell (SSH) aan een van de APIC en voer volgende opdrachten uit.

apic1# **moquery -c l2IngrPktsAg15min**

Dit biedt alle objectinstanties voor deze klasse l2IngrPacketAg15min.

Hier is een voorbeeld met een filter om een specifiek object te vragen. In dit voorbeeld moet het filter alleen een object met eigenschappen **dn** tonen dat "tn-TENANT1/ap-APP1/epg-EPG1" bevat.

In dit voorbeeld wordt gebruikgemaakt van rep om alleen de vereiste eigenschappen te tonen.

Voorbeeld uitvoer 1: EPG-tegenobject (l2IngrPktsAg15min) van huurder TENANT1, toepassingsprofiel APP1, zie EPG1.

```
apic1# moquery -c l2IngrPktsAg15min -f 'l2.IngrPktsAg15min.dn*"tn-TENANT1/ap-APP1/epg-EPG1"' |
egrep 'dn|drop[P,R]|rep'
dn : uni/tn-TENANT1/ap-APP1/epg-EPG1/CDl2IngrPktsAg15min dropPer : 30 <--- number of drop packet
in the current periodic interval (600sec) dropRate : 0.050000 <--- drop packet rate =
dropPer(30) / periodic interval(600s) repIntvEnd : 2017-03-03T15:39:59.181-08:00 <--- periodic
interval = repIntvEnd - repIntvStart repIntvStart : 2017-03-03T15:29:58.016-08:00 = 15:39 -
15:29
= 10 min = 600 sec
```

Of we kunnen een andere optie **D** gebruiken in plaats van **c** om een specifiek object te krijgen als je het object kent dn.

Voorbeeld uitvoer 2: EPG-tegenobject (l2IngrPktsAg15min) van huurder TENANT1, toepassingsprofiel APP1, EPG2.

```
apic1# moquery -d uni/tn-TENANT1/ap-APP1/epg-EPG2/CDl2IngrPktsAg15min | egrep 'dn|drop[P,R]|rep'
dn               : uni/tn-jw1/BD-jw1/CDl2IngrPktsAg15min
dropPer          : 30
dropRate         : 0.050000
repIntvEnd       : 2017-03-03T15:54:58.021-08:00
repIntvStart     : 2017-03-03T15:44:58.020-08:00
```

Hardware tellers

Als u fouten ziet, of pakketdruppels op wachtpoorten wilt controleren met behulp van de CLI, is de beste manier om dit te doen door de platformtellers in hardware te bekijken. De meeste,

maar niet alle tellers worden getoond die **tonen interface** gebruiken. De 3 belangrijkste uitvalredenen kunnen alleen met behulp van de perronettellers worden bekeken. Voer de volgende stappen uit om deze te bekijken:

Leaf

SSH naar het blad en voer deze opdrachten uit.

ACI-LEAF# **vsh_lc**
module-1# **Poorten platform interne tellers tonen <X>**
*** waar X het poortnummer vertegenwoordigt**

Voorbeeld uitvoer voor Ethernet 1/31:

```
ACI-LEAF# vsh_lc
vsh_lc
module-1#
module-1# show platform internal counters port 31
Stats for port 31
(note: forward drops includes sup redirected packets too)
IF          LPort                    Input                      Output
                                Packets       Bytes          Packets    Bytes
eth-1/31    31  Total           400719   286628225      2302918    463380330
                Unicast         306610   269471065       453831     40294786
                Multicast            0           0      1849091    423087288
                Flood            56783     8427482            0            0
               Total Drops       37327                       0
                Buffer               0                       0
                Error                0                       0
                Forward          37327
                LB                   0
                AFD RED                                      0
                    ----- snip -----
```

ruggegraat

Voor een bak-type wervelkolom (N9K-C9336PQ) is het precies hetzelfde als Leaf.

Voor modulaire stekkers (N9K-C9504 enz.) moet u eerst de specifieke lijnkaart toevoegen voordat u de platformtellers kunt bekijken. SSH aan de wervelkolom en voer deze opdrachten uit

ACI-SPINE# **v**

ACI-SPINE# **attach module <X>**

module-2# **tonen platform interne tellers poort <Y>**.

* waar X het modulenummer voor de lijnkaart weergeeft

Y vertegenwoordigt het poortnummer

Voorbeeld uitvoer voor Ethernet 2/1:

```
ACI-SPINE# vsh
Cisco iNX-OS Debug Shell
This shell should only be used for internal commands and exists
for legacy reasons. User should use ibash infrastructure as this
will be deprecated.
ACI-SPINE#
ACI-SPINE# attach module 2
Attaching to module 2 ...
To exit type 'exit', to abort type '$.'
Last login: Mon Feb 27 18:47:13 UTC 2017 from sup01-ins on pts/1
No directory, logging in with HOME=/
Bad terminal type: "xterm-256color". Will assume vt100.
module-2#
module-2# show platform internal counters port 1
Stats for port 1
(note: forward drops includes sup redirected packets too)
IF          LPort                    Input                        Output
                                Packets       Bytes          Packets    Bytes
eth-2/1      1  Total         85632884  32811563575     126611414   25868913406
                Unicast       81449096  32273734109     104024872   23037696345
                Multicast      3759719    487617769      22586542   2831217061
                Flood                0            0             0            0
              Total Drops            0                          0
                Buffer               0                          0
                Error                0                          0
                Forward              0
                LB                   0
                AFD RED                                         0
                     ----- snip -----
```

Fouten

F12425 - kosten voor druppelbeurten (12-poortsAg15min:dropRate)

Beschrijving:

Eén van de populaire redenen voor deze fout is dat Layer 2-pakketten vallen met de reden "Voorwaarts neerzetten". Er zijn verschillende redenen, maar de meest voorkomende is:

Op sommige platforms (zie CSCvo68407)), is er een beperking waar L2-pakketten die moeten worden omgeleid naar de CPU (d.w.z. CDP/LLDP/UDLD/BFD, enz.) moeten worden geregistreerd als een "voorwaartse drop" en naar de CPU worden gekopieerd. Dit is het gevolg van een beperking van de ASIC die in deze modellen wordt gebruikt.

Resolutie:

De hierboven beschreven druppels zijn puur cosmetisch, dus de aanbeveling voor beste praktijken is de drempel voor de fout te verhogen zoals in het gedeelte **Drempel** van de **staten** is aangegeven. Raadpleeg de instructies in de Drempel Stat om dit te doen.

F100-264 - snelheid voor inbraakbuffer-pakketjes (qptIngrDropPkts5min:buffersnelheid)

Beschrijving:

Deze fout kan groter worden wanneer pakketten op een poort worden gedropt met reden "Buffer" Zoals hierboven vermeld, gebeurt dit meestal wanneer er sprake is van stremmingen op een interface in de sleuf of in de bovenrichting.

Resolutie:

Deze fout staat voor echte geworpen pakketten in de omgeving door congestie. De gedropte pakketten kunnen problemen opleveren met toepassingen in het ACI-weefsel. Netwerkbeheerders moeten de pakketstroom isoleren en bepalen of de congestie het gevolg is van onverwachte verkeersstromen, inefficiënte taakverdeling, enz.; of het verwachte gebruik in die havens.

F100-696 - druppels voor inbraaktransport (qptIngrDropPkts5min:expedentiëleRate)

Opmerking: Een ASIC-beperking zoals hierboven vermeld voor F11245 kan ertoe leiden dat deze gebreken ook worden verhoogd. Zie CSCvo68407 voor nadere bijzonderheden .

Deze fout wordt veroorzaakt door een paar scenario's. De meest voorkomende is:

Beschrijving 1) Spindruppels

Als deze fout op een ruggegraat wordt gezien, kan deze veroorzaakt worden door verkeer naar een onbekend eindpunt.

Wanneer een ARP- of IP-pakket naar de centrifuge wordt doorgestuurd voor een proxy-lookup en het endpointis in de stof niet bekend, wordt er een speciaal grilpakje gegenereerd en naar alle links op het juiste BD (interne) multicast groepsadres verzonden. Dit zal een ARP verzoek van elk blad in de Bridge Domain (BD) geactiveerd om het eindpunt te ontdekken. Vanwege een beperkingBovendien wordt het afgeslankte pakje dat door het blad wordt ontvangen, opnieuw in het weefsel gereflecteerd en wordt er een verzendende druppel geactiveerd op de wervelkolom die met het blad is verbonden. Bij dit scenario wordt de voorwaartse neerslag alleen verhoogd bij hardware van generatie 1.

Resolutie 1)

Aangezien bekend is dat het probleem wordt veroorzaakt door een apparaat dat onnodig veel onbekend Unicast-verkeer naar het ACI Fabric stuurt, moet u uitzoeken welk apparaat dit veroorzaakt en zien of dit kan worden voorkomen. Dit wordt meestal veroorzaakt door apparaten die voor IP adressen op subnetten scannen of testen voor controledoeleinden. Om te vinden wat IP dit verkeer verstuurt, SSH op het blad dat is aangesloten op de wervelkolom interface die de fout toont.

Vanaf daar kunt u deze opdracht uitvoeren om het Bron IP-adres (sip) te zien dat het slanke pakket start:

```
ACI-LEAF# show ip arp internal event-history event | grep glean | grep sip | more
    [116] TID 11304:arp_handle_inband_glean:3035: log_collect_arp_glean;sip = 192.168.21.150;dip
= 192.168.20.100;info = Received glean packet is an IP packet
    [116] TID 11304:arp_handle_inband_glean:3035: log_collect_arp_glean;sip = 192.168.21.150;dip
```

```
= 192.168.20.100;info = Received glean packet is an IP packet
```

In de uitvoer van dit voorbeeld wordt het greslische pakket geactiveerd door 192.168.21.150 en wordt aanbevolen om te zien of dit kan worden verzacht.

Beschrijving 2) Verpakkingsdruppels

Als deze fout gezien wordt op een bladinterface is de meest waarschijnlijke oorzaak te wijten aan de genoemde SECURITY_GROUP_DENY-druppels.

Resolutie 2)

ACI-blad houdt een logbestand bij van pakketten die worden ontkend als gevolg van contractschendingen.Dit logbestand slaat niet alle pakketten op om CPU-bronnen te beschermen, maar het biedt u nog steeds een enorme hoeveelheid logbestanden.

Om de vereiste logbestanden te krijgen, als de interface wordt opgeheven op onderdeel van een poortkanaal, is het vereist om deze opdracht en grijp voor het havenkanaal te gebruiken. Anders kan de fysieke interface worden grepped.

Dit logbestand kan snel worden gerold, afhankelijk van de hoeveelheid contracten die daalt.

```
ACI-LEAF# show logging ip access-list internal packet-log deny | grep port-channel2 | more
[ Sun Feb 19 14:16:12 2017 503637 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD_VLAN, Vlan-
Id: 59, SMac: 0x8c604f0288fc, DMac:0x0022bdf819ff, SIP: 192.168.21.150, DIP: 192.168.20.3,
SPort: 0, DPort: 0, Src Intf: port-channel2, Pr
oto: 1, PktLen: 98
[ Sun Feb 19 14:16:12 2017 502547 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD_VLAN, Vlan-
Id: 59, SMac: 0x8c604f0288fc, DMac:0x0022bdf819ff, SIP: 192.168.21.150, DIP: 192.168.20.3,
SPort: 0, DPort: 0, Src Intf: port-channel2, Pr
oto: 1, PktLen: 98
```

In dit geval probeert 192.168.21.150 ICMP-berichten (IP protocol nummer 1) naar 192.168.20.3 te verzenden. Er is echter geen contract tussen de 2 EPG's dat ICMP toestaat, dus wordt het pakje ingetrokken. Als ICMP zou moeten worden toegestaan, kan een contract worden toegevoegd tussen de twee EPG's.

Stats Drempel

In dit deel wordt beschreven hoe een drempel voor een statistiekobjecten kan worden gewijzigd die mogelijk een fout tegen valteller kunnen veroorzaken.

Een drempel voor statistieken van elke objecten (d.w.z. l2IngrPkts, equptIngrDropPkts) wordt ingesteld door Bewakingsbeleid tegen verschillende objecten.

Zoals in de tabel aan het begin vermeld, wordt qptIngrDropPkts onder, bijvoorbeeld, l1PhysIf objecten door monitoringbeleid gecontroleerd.

Forward Drop Packets Rate in QoIPDrop

Hier zijn twee delen voor.

+ Toegangsbeleid (havens voor externe apparatuur). a.k.a. poorten op het voorpaneel)

+ Fabricbeleid (poorten tussen LEAF en SPINE).

Front Panel Ports (ports towards external devices)

Fabric Ports (ports between LEAF and SPINE)

Elke poortobjecten (l1PhysIf, pcAggrAs) zouden zijn eigen **Toezichtbeleid** kunnen krijgen via **Interface Policy Group** zoals in het bovenstaande beeld wordt getoond.

Standaard is er een **beleid voor standaardbewaking** onder **Fabric > Toegangsbeleid** en **Fabric > Fabricbeleid** in APIC GUI. Dit beleid van standaardbewaking wordt respectievelijk aan alle havens toegewezen. Het standaard controlebeleid onder Toegangsbeleid is voor paneelpoorten en het standaard controlebeleid onder Fabric beleid is voor Fabric poorten.

Tenzij het vereist is om drempels per havens te veranderen, kan het standaard controlebeleid in elke sectie direct worden aangepast om de verandering voor alle havens van het voorpaneel en/of de havens van het weefsel toe te passen.

Het volgende voorbeeld is om drempelwaarden voor Forward Drop in QptIngrDropPkts op fabric poorten (**Fabric Beleid**) te wijzigen. Voer hetzelfde uit onder **Fabric > Toegangsbeleid** voor voorpaneelpoorten.

1. Navigeer naar **fabricagebeleid > Fabricbeleid>Toezichtbeleid.**

2. Klik met de rechtermuisknop en selecteer "Toezichtbeleid maken".

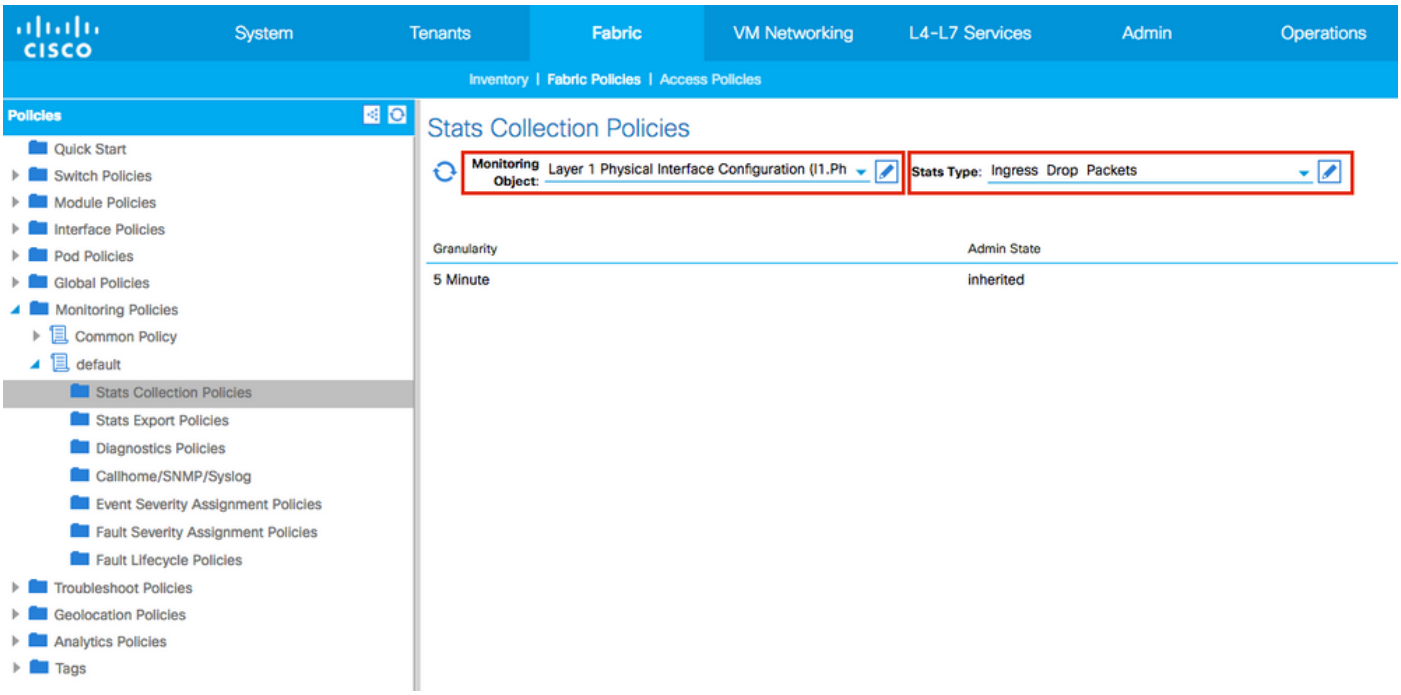
(Als de drempelverandering op alle kabelpoorten kan worden toegepast, navigeer dan naar **standaard** in plaats van een nieuwe poort te maken)

3. Het nieuwe monitoringbeleid of de huidige stand van zaken uitbreiden en **naar** een **nationaal beleid voor de verzameling van statistieken** navigeren**.**

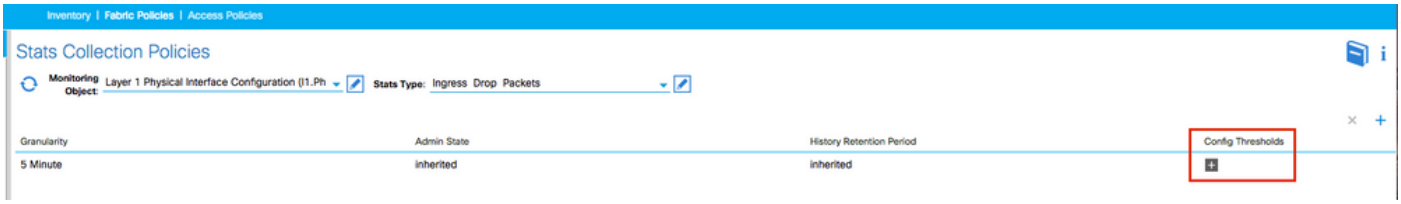
4. Klik op het pictogram van het **potlood** voor het **gedeelte Monitoring Object** in het juiste venster en selecteer **Layer 1 Physical Interface Configuration (l1.PhysIf)**.

(Deze stap 4 kan worden overgeslagen wanneer het standaardbeleid wordt gebruikt)

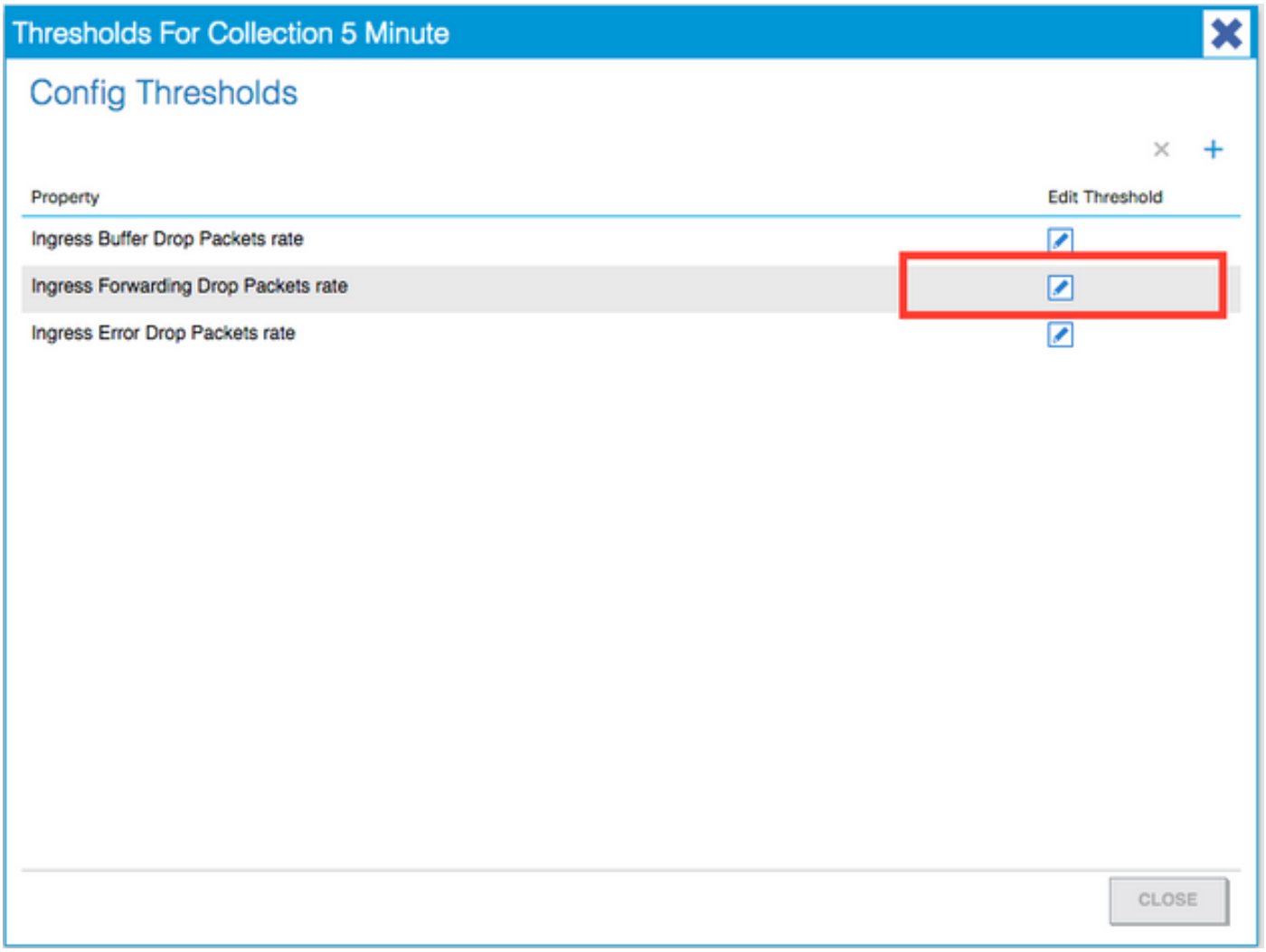
5. Kies in de vervolgkeuzelijst met het rechtervenster de optie **Layer 1 Physical Interface Configuration (l1.PhysIf)** en **Stats Type**, **Ingress Drop Packets**



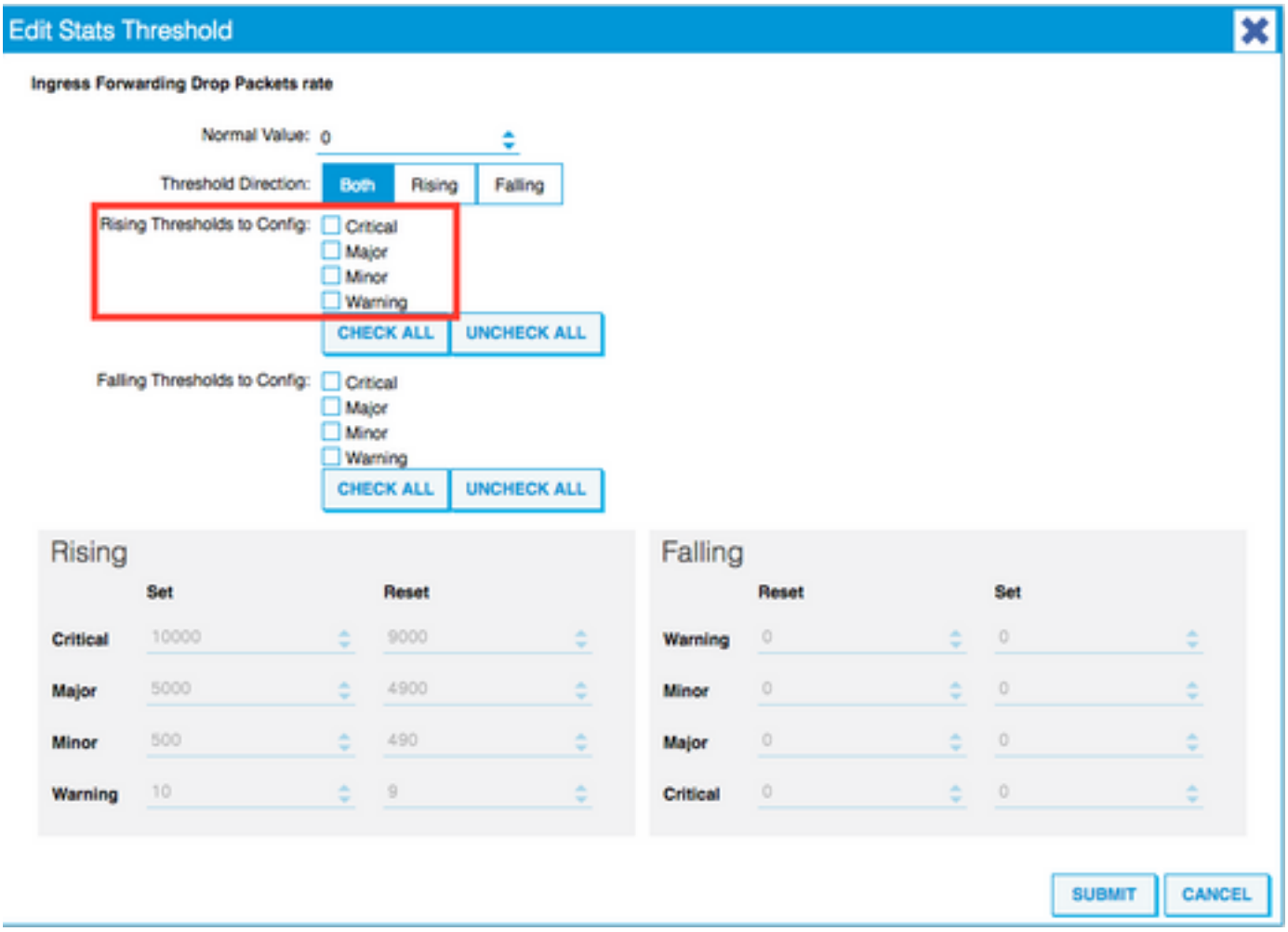
6. Klik op de **+** naast de drempels van configuratie



7. Bewerk de drempelwaarde voor doorsturen

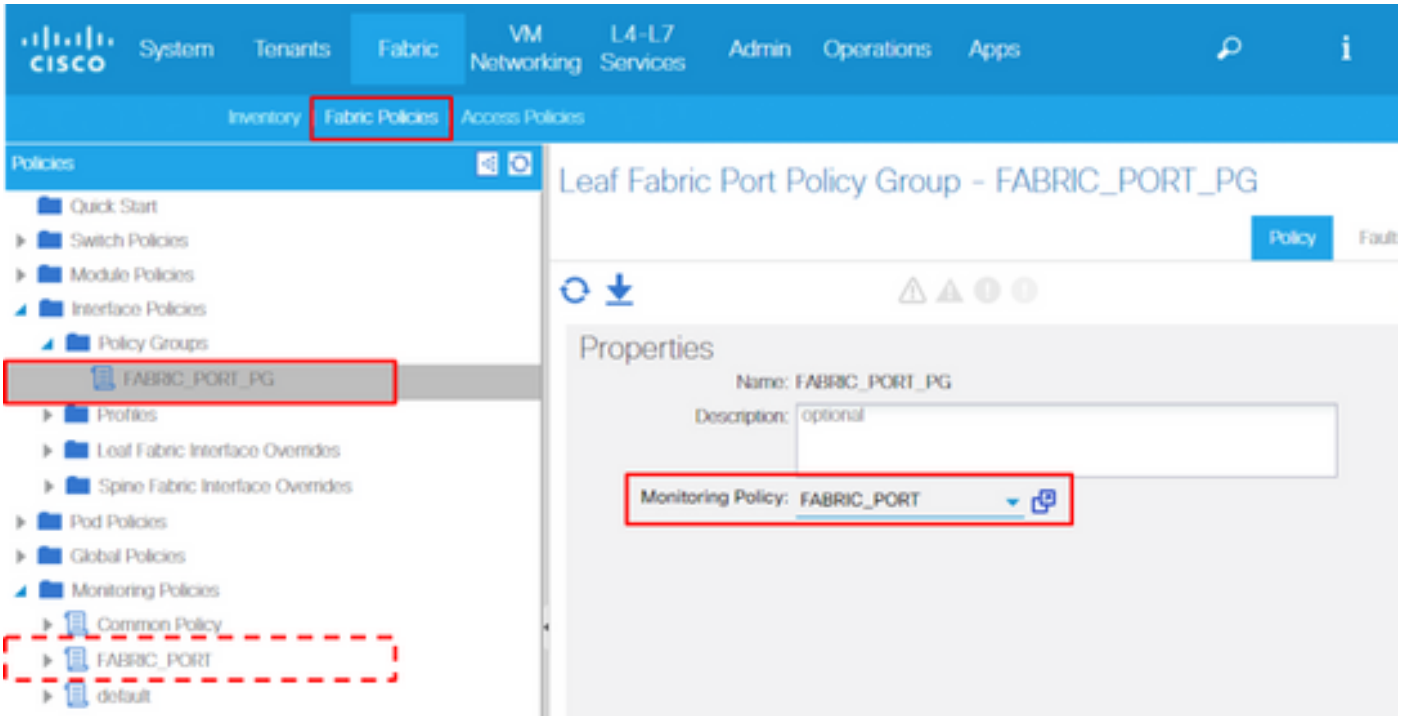


8. De aanbeveling is de stijgende drempelwaarden voor de configuratie van kritieke, belangrijke, kleine en waarschuwingssignalen voor de verzending uit te schakelen.



9. Pas dit nieuwe controlebeleid toe op de interfacebeleidsgroep voor de vereiste havens. Vergeet niet om in het fabric-beleid naar behoren interfaceprofiel, Switch profiel enzovoort te configureren.

(Deze stap 9 kan worden overgeslagen wanneer het standaardbeleid wordt gebruikt)

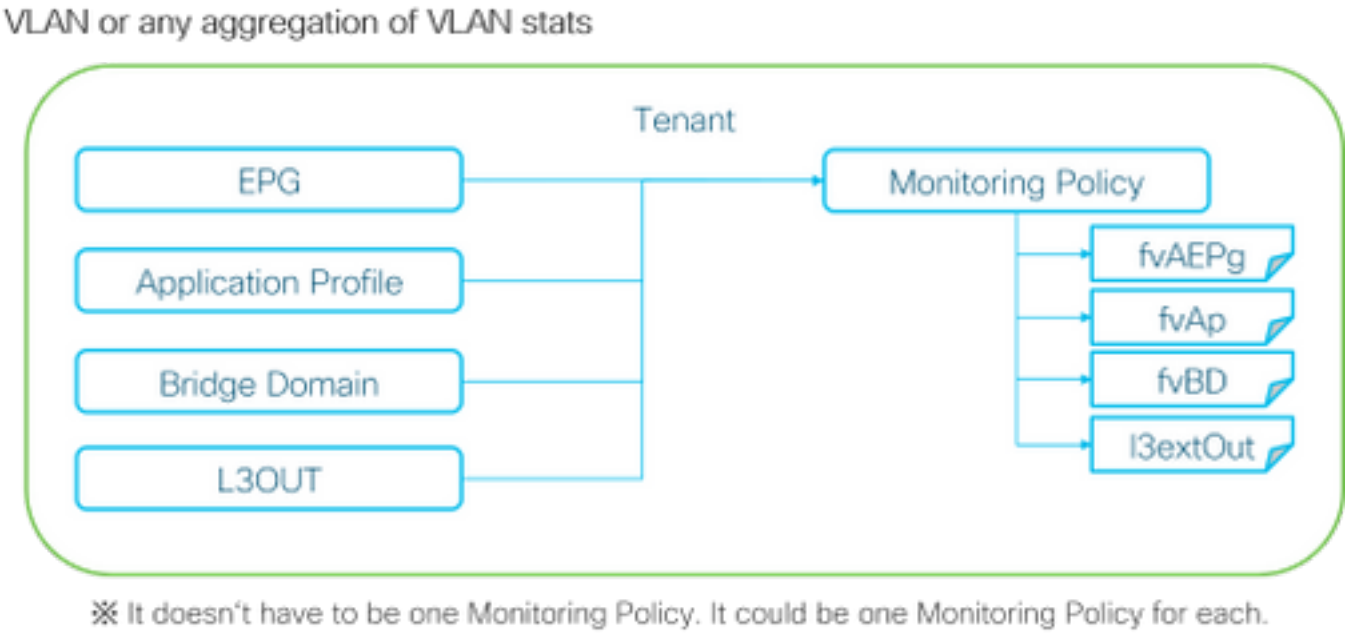


10. Als dit voor Frontpaneelpoorten is (Toegangsbeleid), voer dan hetzelfde voor **geaggregeerde interface (pc.AggrIf)** in plaats van **Layer 1 Physical Interface Configuration (l1.PhysIf)** zodat dit nieuwe monitoringbeleid zowel op poortkanaal als op fysieke poort kan worden toegepast.

(Deze stap 10 kan worden overgeslagen wanneer het standaardbeleid wordt gebruikt)

Ingress Drop Packets Rate in l2IngrPktsAg

Er zijn hier meerdere porties voor.



Zoals het bovenstaande beeld toont, wordt l2IngrPktsAg onder een hoop objecten gecontroleerd. Bovenstaande afbeelding geeft alleen een paar voorbeelden, maar niet alle objecten voor l2IngrPktsAg. De drempel voor statistieken wordt echter ingesteld door monitoringbeleid en door qptIngrDropPkts onder l1PhysIf of pcAggrIf.

Elk object (EPG(fvAEPg), Bridge Domain (fvBD), enz.) kan een eigen **monitoringbeleid** krijgen, zoals in het bovenstaande beeld wordt getoond.

Standaard gebruikt al deze objecten onder huurder het **standaard bewakingsbeleid** onder **Tenant > common > Monitoring Policy > default**, tenzij anders ingesteld.

Tenzij het vereist is om de drempels per component te wijzigen, kan het standaard monitoringbeleid onder huurder gemeenschappelijk rechtstreeks worden gewijzigd om de wijziging voor alle gerelateerde componenten toe te passen.

Het volgende voorbeeld is om drempelwaarden voor Ingress Drop Packets Rate in l2IngrPacketsAg15min te wijzigen op Bridge Domain.

1. Navigeer naar **aanbesteding > (huurnaam) > Toezichtbeleid.**

(huurder moet gemeenschappelijk zijn indien het wanbetalingsbewakingsbeleid wordt gebruikt of het nieuwe toezichtsbeleid op huurders moet worden toegepast)

2. Klik met de rechtermuisknop en selecteer "Toezichtbeleid maken".

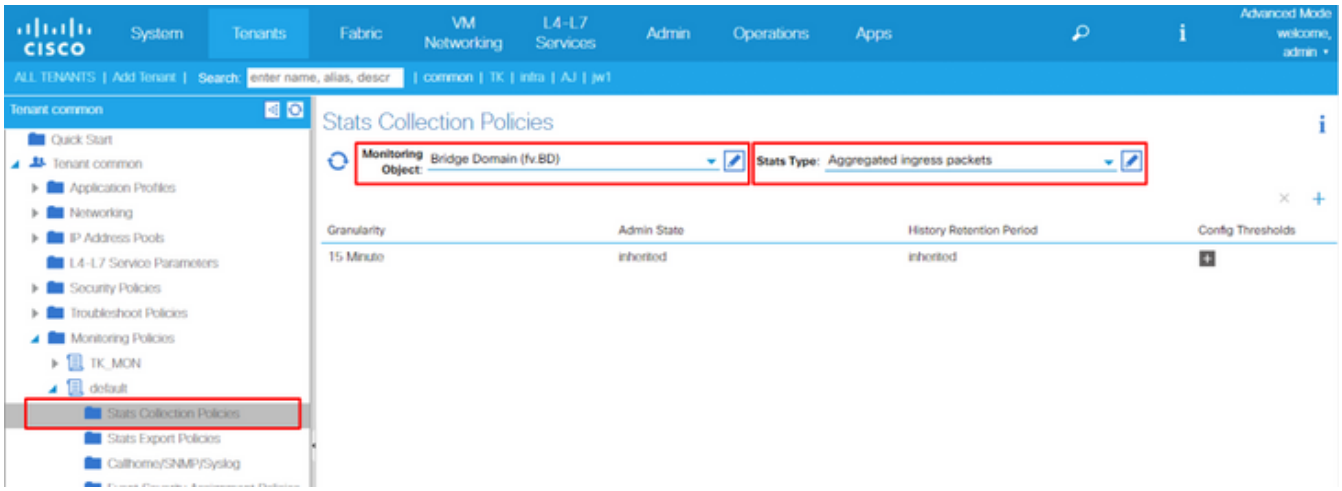
(Als de drempelverandering op alle componenten kan worden toegepast, navigeer dan naar **standaard** in plaats van een nieuwe te maken)

3. Het nieuwe monitoringbeleid of de huidige stand van zaken uitbreiden en **naar** een **nationaal beleid voor de verzameling van statistieken** navigeren.

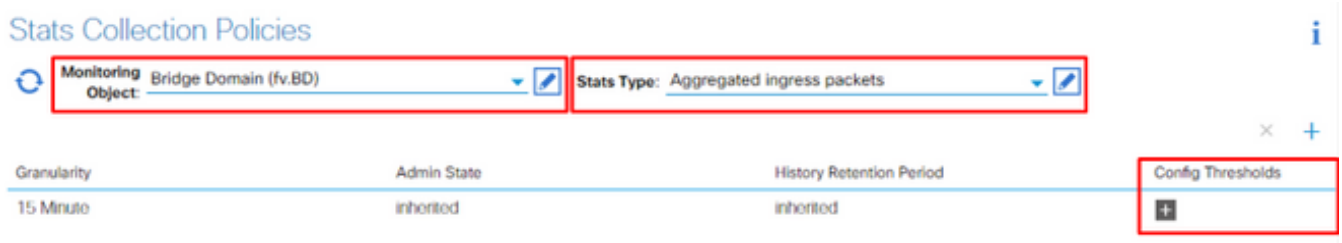
4. Klik op het pictogram van het potlood voor de **Voorwerp** van de **Controle** op het rechtervenster, selecteer **Bridge Domain (fv.BD).**

(Deze stap 4 kan worden overgeslagen wanneer het standaardbeleid wordt gebruikt)

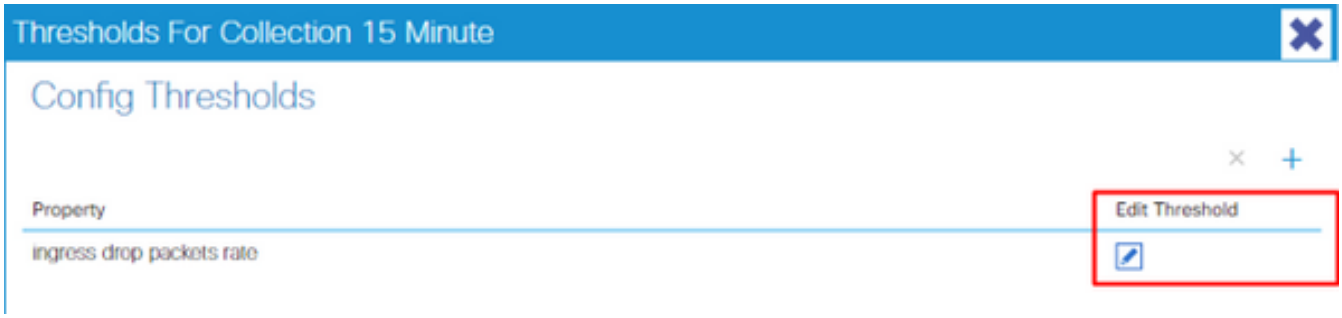
5. Kies in de vervolgkeuzelijst **Monitoring Object** in het rechter deelvenster de optie **Bridge Domain (fv.BD)** en **Stats Type**, **Aggregated Access-pakketten.**



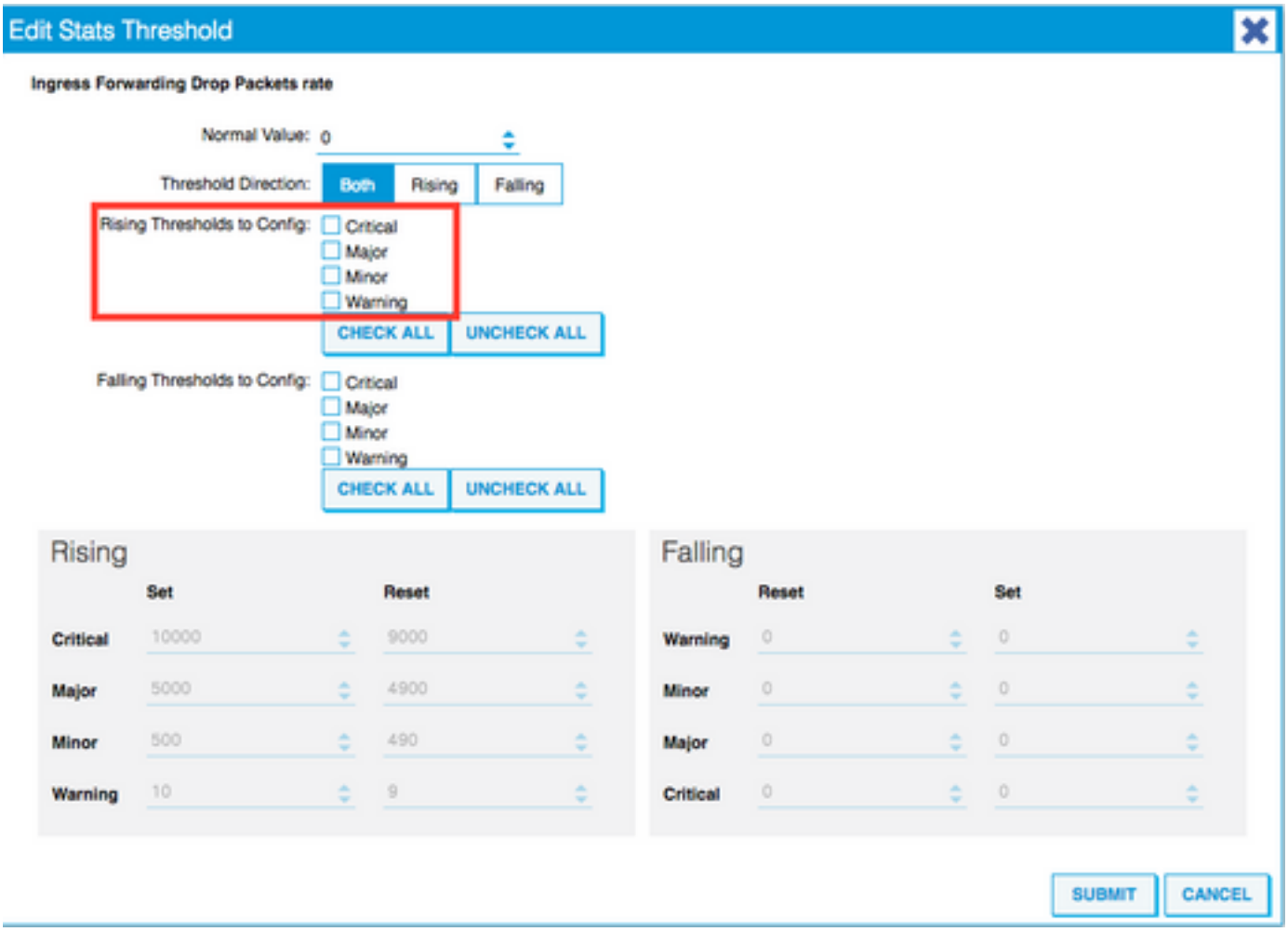
6. Klik op de **+** naast de drempels van configuratie



7. Bewerk de drempelwaarde voor doorsturen

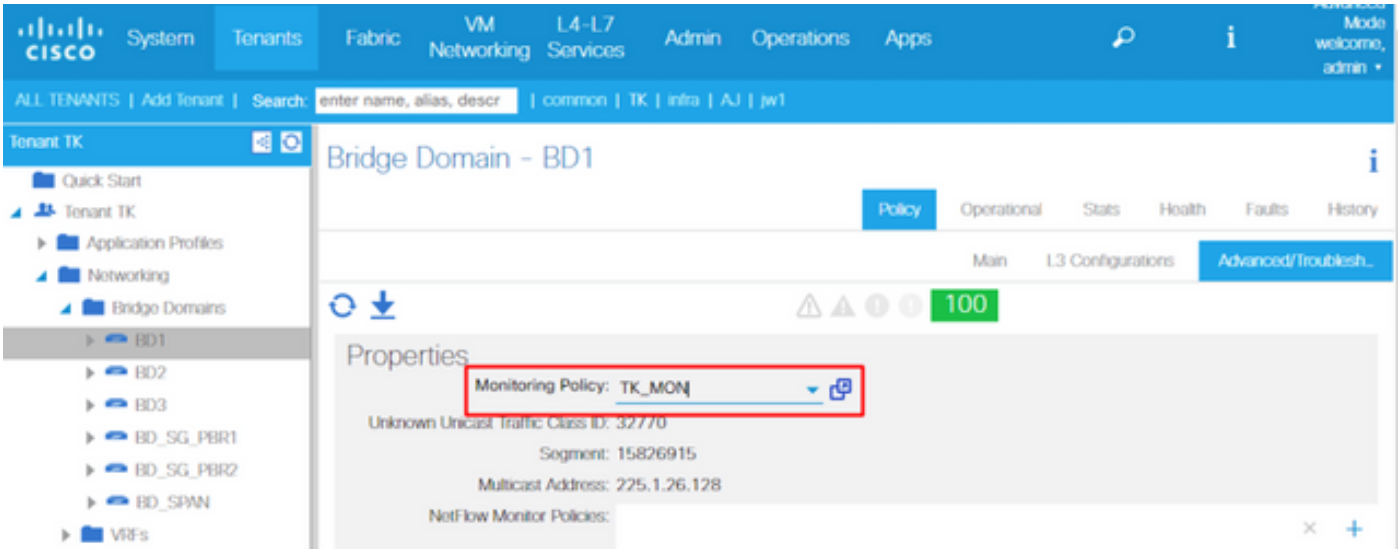


8. De aanbeveling is de stijgende drempelwaarden voor de configuratie van kritieke, belangrijke, kleine en waarschuwingssignalen voor de verzending uit te schakelen.



9. Pas dit nieuwe monitoringbeleid toe op het Bridge Domain, dat een drempelwijziging vereist.

(Deze stap 9 kan worden overgeslagen wanneer het standaardbeleid wordt gebruikt)



OPMERKING

Het kan zijn dat het niet-standaard controlebeleid geen configuraties heeft die aanwezig zijn in het standaard controlebeleid. Als het wordt vereist om die configuratie gelijk te houden aan het standaard Bewakingsbeleid, moeten de gebruikers de standaard Controle van het Beleid van de Controle controleren en handmatig het zelfde beleid op het beleid van de niet-standaard Controle van het Beleid vormen.