Explicações de falhas da queda de pacote de informação na ACI

Índice

Introdução

Este documento descreve cada tipo da falha, e o procedimento quando você vê esta falha. Durante Operaton normal de uma tela céntrica da infraestrutura do aplicativo Cisco (ACI), o administrador pode ver que as falhas datilografam com certeza das quedas de pacote de informação.

Contribuído por Joseph Ristaino, Takuya Kishida, engenheiros de TAC da Cisco.

Objetos gerenciado

Em Cisco ACI, todas as falhas são levantadas sob os objetos gerenciado (MO). Por exemplo, uma falha "*F11245 - pacotes da gota do ingresso rate(l2IngrPktsAg15min:dropRate)*" está considerando o *dropRate do* parâmetro em MO *l2IngrPktsAg15min*.

Esta seção introduz algum do **objeto gerenciado do** exemplo **(MO) relacionou falhas do pacote da gota**.

	Exemplo	Descrição	Amostra Paramters
l2IngrPkts	l2IngrPkts5min l2IngrPkts15min l2IngrPkts1h etc….	Isto representa estatísticas do pacote de ingresso pelo VLAN durante cada período	dropRate floodRate multicastRat unicastRate
l2IngrPktsAg	l2IngrPktsAg15min l2IngrPktsAg1h l2IngrPktsAg1d etc….	Isto representa estatísticas do pacote de ingresso por EPG, BD, VRF etc…. .) O stats ex EPG representa a agregação dos stats VLAN que pertencem ao EPG	dropRate floodRate multicastRat unicastRate
eqptIngrDropPkts	eqptIngrDropPkts15min eqptIngrDropPkts1h eqptIngrDropPkts1d etc….	Isto representa estatísticas de pacote da gota do ingresso pela relação durante cada período	forwardingR *1 errorRate *1 bufferRate *

*1: Estes contadores nos eqptIngrDropPkts são usados já não 1.3(2) das liberações devido à - limitação da plataforma EX na gota dianteira com SUP_REDIRECT.

Seja notado por favor que esta aplicação poderia ser mudada outra vez no futuro.

Tipos do contador de queda do hardware

Nos 9000 Switch do nexo que são executado no modo ACI, há 3 contadores de hardware principais para a razão da gota da interface de ingresso no ASIC.

Um dropRate em l2IngrPkts, l2IngrPktsAg inclui aqueles contadores. Três parâmetros (forwardingRate, errorRate, bufferRate) na tabela acima para eqptIngrDropPkts representam cada três contadores de interface.

Encaminhar

As gotas dianteiras, são os pacotes que são deixados cair no bloco da consulta (LU) do ASIC. No bloco LU, uma decisão de encaminhamento de pacote de informação é feita baseado na informação de cabeçalho de pacote de informação. Se a decisão é deixar cair o pacote, a gota dianteira está contada. Há uma variedade de razões que este pode acontecer, mas para deixar-nos falar sobre principais:

SECURITY_GROUP_DENY

Uma gota devido aos contratos faltantes para permitir a comunicação.

Quando um pacote entra na tela, o interruptor olha a fonte e o destino EPG para considerar se há um contrato que permita esta comunicação. Se a fonte e o destino estão em EPG diferentes, e não há nenhum contrato que permite este tipo de pacote

entre eles, o interruptor deixará cair o pacote e etiquetá-lo-á como SECURITY_GROUP_DENY. Isto incrementa o contador de queda dianteiro.

VLAN_XLATE_MISS

Uma gota devido ao VLAN impróprio.

Quando um pacote entra na tela, o interruptor olha o pacote para determinar se a configuração na porta permite este pacote. Por exemplo, um quadro entra na tela com uma etiqueta do 802.1Q do 10. Se o interruptor tem o VLAN10 na porta, inspecionará os índices e fará uma decisão de encaminhamento baseada no MAC de destino. Contudo, se o VLAN10 não está na porta, deixá-la-á cair e etiquetá-la-á como um VLAN_XLATE_MISS. Isto incrementará o contador de queda dianteiro.

A razão para o “XLATE” ou “traduz” é porque na ACI, o interruptor da folha tomará um quadro com um encap do 802.1Q e o traduzirá a um VLAN novo que seja usado para VXLAN e a outra normalização dentro da tela. Se o quadro entra com um VLAN não distribuído, a “tradução” falhará.

ACL_DROP

Uma gota devido ao sup-TCAM.

o sup-TCAM no Switches ACI contém as regras especiais a ser aplicadas sobre a decisão de encaminhamento L2/L3 normal. As regras no sup-TCAM são incorporados e não usuário configuráveis. O objetivo das regras sup-TCAM é principalmente segurar algumas exceções ou alguma do tráfego plano do controle e não pretendidas ser verificado ou monitorado por usuários. Quando o pacote está batendo as regras sup-TCAM e a regra é deixar cair o pacote, o pacote descartado está contado porque ACL_DROP e incrementarão o contador de queda dianteiro. Quando isto ocorreu, significa geralmente que o pacote está a ponto de ser enviada contra principais básicos da transmissão ACI.

Note que, mesmo que o nome da gota seja ACL_DROP, este “ACL” não é mesmo que o Access Control List normal que pode ser configurado em dispositivos autônomos NX-OS ou todo o outros roteamento/dispositivos swtching.

SUP_REDIRECT

Esta não é uma gota.

Um pacote reorientado sup (isto é CDP/LLDP/UDLD/BFD etc…) pode ser contado como a gota dianteira pensou mesmo que o pacote corretamente está processado e enviado ao CPU.

Isto pode ocorrer somente dentro - Plataforma EX tal como N9K-C93180YC-EX. Estes não devem ser contados como a “gota” contudo que está devido à plataforma da limitação de ASIC dentro - EX.

Erro

Quando o interruptor recebe um quadro inválido, está deixado cair como um erro. Os exemplos deste incluem quadros com FCS ou erros CRC.

Buffer

Quando o interruptor recebe um quadro, e há disponível dos créditos do sem buffer para o ingresso ou a saída, o quadro estará deixado cair com “buffer”. Isto sugere tipicamente na congestão em algum lugar na rede. O link que está mostrando que a falha poderia estar completa, ou, o link que contém o destino pode ser congestionado.

Vendo o Stats da gota no CLI

Objetos gerenciado

Shell Seguro (ssh) a um do APIC e dos comandos seguintes executados.

moquery apic1# **- c l2IngrPktsAg15min**

Isto fornecerá todos os exemplos do objeto para esta classe l2IngrPktsAg15min.

Está aqui um exemplo com um filtro para perguntar um objeto específico. Neste exemplo, o filtro é mostrar somente um objeto com atributos **dn** qual inclui "tn-TENANT1/ap-APP1/epg-EPG1".

Igualmente este exemplo usa o egrep para mostrar somente atributos requerido.

Saídas de exemplo 1: EPG opõem o objeto (l2IngrPktsAg15min) do inquilino TENANT1, o perfil do aplicativo APP1, o epg 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
```

Ou nós poderíamos usar uma outra opção **- d** em vez de **- c** para obter um objeto específico se você conhece o objeto dn.

Saídas de exemplo 2: EPG opõem o objeto (l2IngrPktsAg15min) do inquilino TENANT1, o perfil do aplicativo APP1, o epg 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
```

Contadores de hardware

Se você vê falhas, ou as quer verificar quedas de pacote de informação em switchports usando o CLI, a melhor maneira de fazer isto é vendo os contadores da plataforma no

hardware. A maioria, mas não todos os contadores são mostrados usando a **relação da mostra**. As 3 razões principais da gota podem somente ser vistas usando os contadores da plataforma. A fim ver estes, execute estas etapas:

Folha

SSH à folha e executado estes comandos.

Vsh_lc ACI-LEAF#
<x> da porta dos contadores internos da plataforma da mostra module-1#
* onde X representa o número de porta

Saídas de exemplo para 1/31 etherent:

```
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 -----
```

Espinha

Para uma espinha em forma de caixa (N9K-C9336PQ), é exatamente mesma que a folha.

Para as espinhas modulares (N9K-C9504 etc…), você deve primeiramente anexar o a placa de linha particular antes que você possa ver os contadores da plataforma. SSH à espinha e executado estes comandos

Vsh ACI-SPINE#

<x> do módulo do anexo ACI-SPINE#

<y> da porta dos contadores internos da plataforma da mostra module-2#.

* onde X representa o número de módulo para a placa de linha que você gostaria de ver

Y representa o número de porta

Saídas de exemplo para os 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 -----
```

Falhas

F11245 - taxa dos pacotes da gota do ingresso (l2IngrPktsAg15min:dropRate)

Descrição:

Esta falha pode incrementar quando os pacotes da camada 2 obtêm deixados cair com “a razão da gota dianteira”. Desde que há uma variedade de razões diferentes,

o mais comum é:

Em - Plataforma EX tal como N9K-C93180YC-EX, há uma limitação onde os pacotes L2 que precisam de obter reorientem ao CPU (isto é CDP/LLDP/UDLD/BFD, etc.), obterá registrado porque “uma gota dianteira” assim como obtém copiado ao CPU. Isto é devido a uma limitação do ASIC usado nos modelos EX do nexo 9000.

Devido a isto, quando os lotes de protocolos do plano do controle são permitidos em uma relação, estas falhas podem ser levantadas.

Resolução:

Desde que não há nenhum impacto do serviço, a recomendação da melhor prática é aumentar o ponto inicial para a falha segundo as indicações da seção do **ponto inicial Stats**. A fim fazer isto, veja as instruções no ponto inicial Stats.

F100264 - pacotes da gota do buffer de ingresso avaliam (eqptIngrDropPkts5min:bufferRate)

Descrição:

Esta falha pode incrementar quando os pacotes estão sendo deixados cair em uma porta com razão “buffer” como mencionado acima, isto acontece tipicamente quando há uma congestão em uma relação no ingresso ou na direção de saída.

Resolução:

Esta falha representa pacotes descartado reais no ambiente devido à congestão. Os pacotes descartado podem causar edições com os aplicativos que são executado na tela ACI. Os administradores de rede devem isolar o fluxo de pacote de informação e determinar se a congestão é devido aos fluxos de tráfego inesperados, ao Balanceamento de carga incapaz, etc.; ou utilização prevista naquelas portas.

F100696 - pacotes da gota da transmissão do ingresso (eqptIngrDropPkts5min:forwardingRate)

Nota: Começando na versão 1.3(2), as gotas dianteiras são removidas do objeto eqptIngrDropPkts5min, assim que esta falha não deve ser considerada para esta edição.

Esta falha é causada por algumas encenações. O mais comum é:

Descrição 1) Gotas da espinha

Quando um ARP ou um pacote IP estão enviados à espinha para uma consulta do proxy e o valor-limite é desconhecido na tela, um special recolhe o pacote estará gerado e enviado a todas as folhas no BD apropriado
endereço de grupo de transmissão múltipla. Isto provocará uma requisição ARP de cada folha no domínio de Bridge (BD) descobrir o valor-limite. Devido a uma limitação, o pacote recolher recebido pela folha é refletido igualmente
de novo na tela e provoca uma gota da transmissão no link da espinha. A gota dianteira é incrementada somente no hardware da espinha da geração 1.

Definição 1)

Desde que você sabe que a edição está causada por um dispositivo que envia o tráfego do unicast desconhecido na tela ACI, você precisa de figurar para fora que o dispositivo está causando a isto, e de ver se você pode o impedir. Isto é causado geralmente pelos dispositivos que fazem a varredura ou sondam para endereços IP de Um ou Mais Servidores Cisco ICM NT em sub-redes para monitorar finalidades. A fim encontrar o que o IP está enviando a este tráfego, SSH na folha que é conectada à relação da espinha que mostra a falha.

De lá, você pode executar este comando ver o endereço IP de origem (sorvo) que está provocando o pacote recolher:

```
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 = Rece
ived 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 = Rece
ived 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 = Rece
ived 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 = Rece
ived glean packet is an IP packet
```

De lá, você pode investigar porque 192.168.21.150 está enviando este tráfego na tela, e ver se você pode a abrandar de lá.

Descrição 2) Gotas da folha

Se esta falha é considerada em uma relação da folha, o casue mais provável é devido às gotas SECURITY_GROUP_DENY mencionadas.

Definição 2)

Em uma folha, você mantém um log dos pacotes negados devido contratar violações. Este log não captura todo para proteger recursos do CPU contudo que ainda lhe fornece uma vasta quantidade de logs.

Para obter os logs o que você quer, se a relação a falha é levantada sobre é parte de um canal de porta, você precisa de usar estes comando e grep para o canal de porta. Se não, você pode usar a interface física:

Este log pode rapidamente ser rolado sobre segundo a quantidade de gotas do contrato.

```
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: 0x8c604
f0288fc, 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: 0x8c604
f0288fc, 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 500387 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD_VLAN, Vlan-
Id: 59, SMac: 0x8c604
f0288fc, 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 499779 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD_VLAN, Vlan-
Id: 59, SMac: 0x8c604
f0288fc, 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 499624 usecs]: CName: jr:sb(VXLAN: 2129921), VlanType: FD_VLAN, Vlan-
Id: 59, SMac: 0x8c604
f0288fc, 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
```

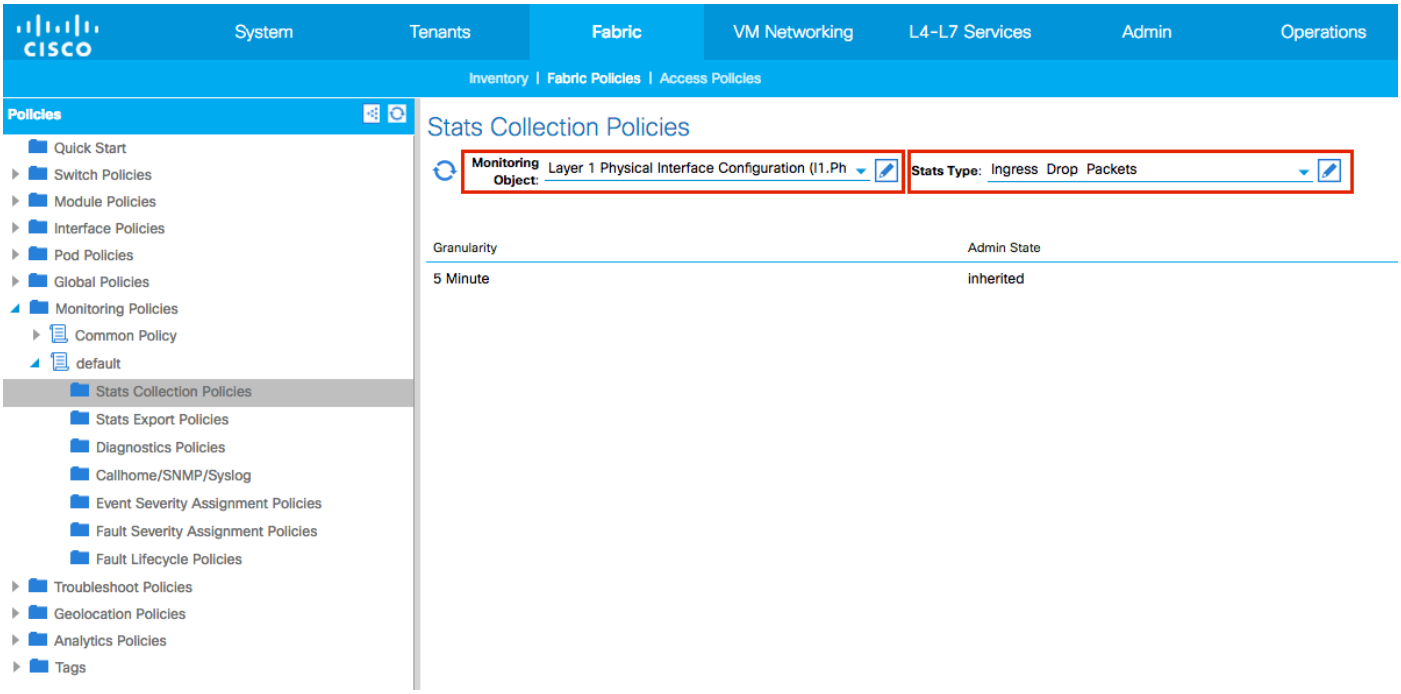
Neste caso, 192.168.21.150 está tentando enviar mensagens ICMP (protocolo IP número 1) a 192.168.20.3. Contudo, não há nenhum contrato entre os 2 EPG que permite o ICMP, assim que o pacote é deixado cair. Se o ICMP é suposto para ser permitido, um contrato pode ser adicionado entre os dois EPG.

Ponto inicial Stats

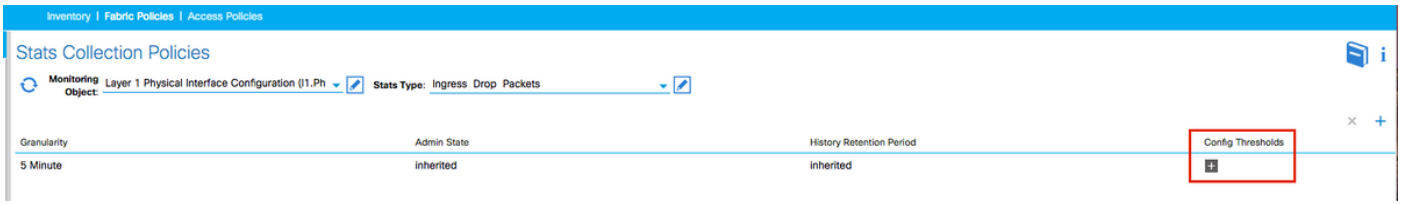
Esta seção descreve como mudar um ponto inicial para os objetos das estatísticas que poderiam potencialmente levantar um contador de queda do agaist da falha.

O exemplo seguinte é mudar o ponto inicial para a *gota* dianteira nos *eqptIngrDropPkts*.

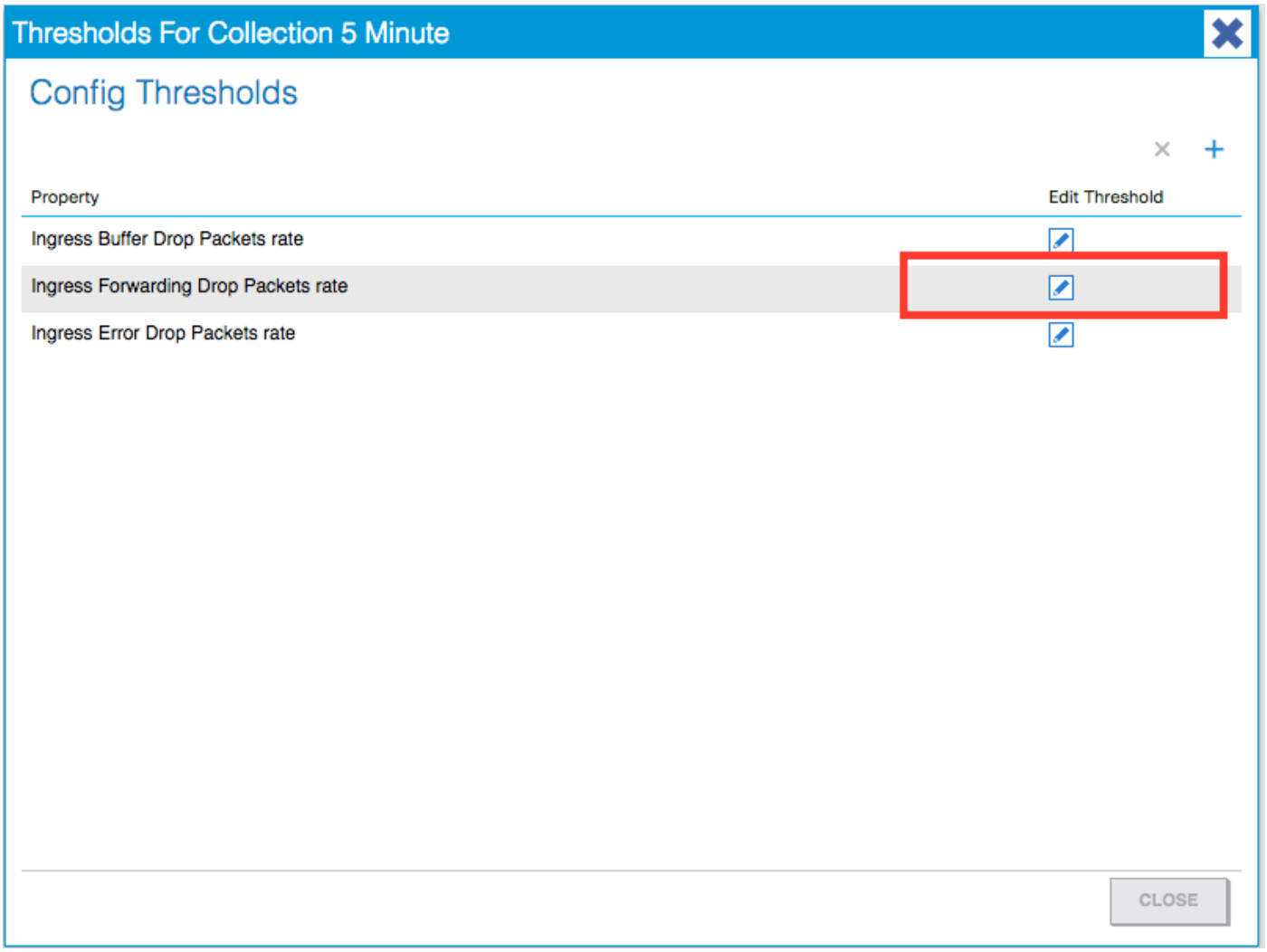
1. Navegue às **políticas >Fabric da tela que >Monitoring políticas da coleção dos >Stats das políticas > do padrão.**
2. **Do objeto da monitoração** deixe cair para baixo, escolhem a **configuração de interface física do Layer 1 (l2.PhysIf)** e o **tipo Stats**, escolhe **pacotes da gota do ingresso**



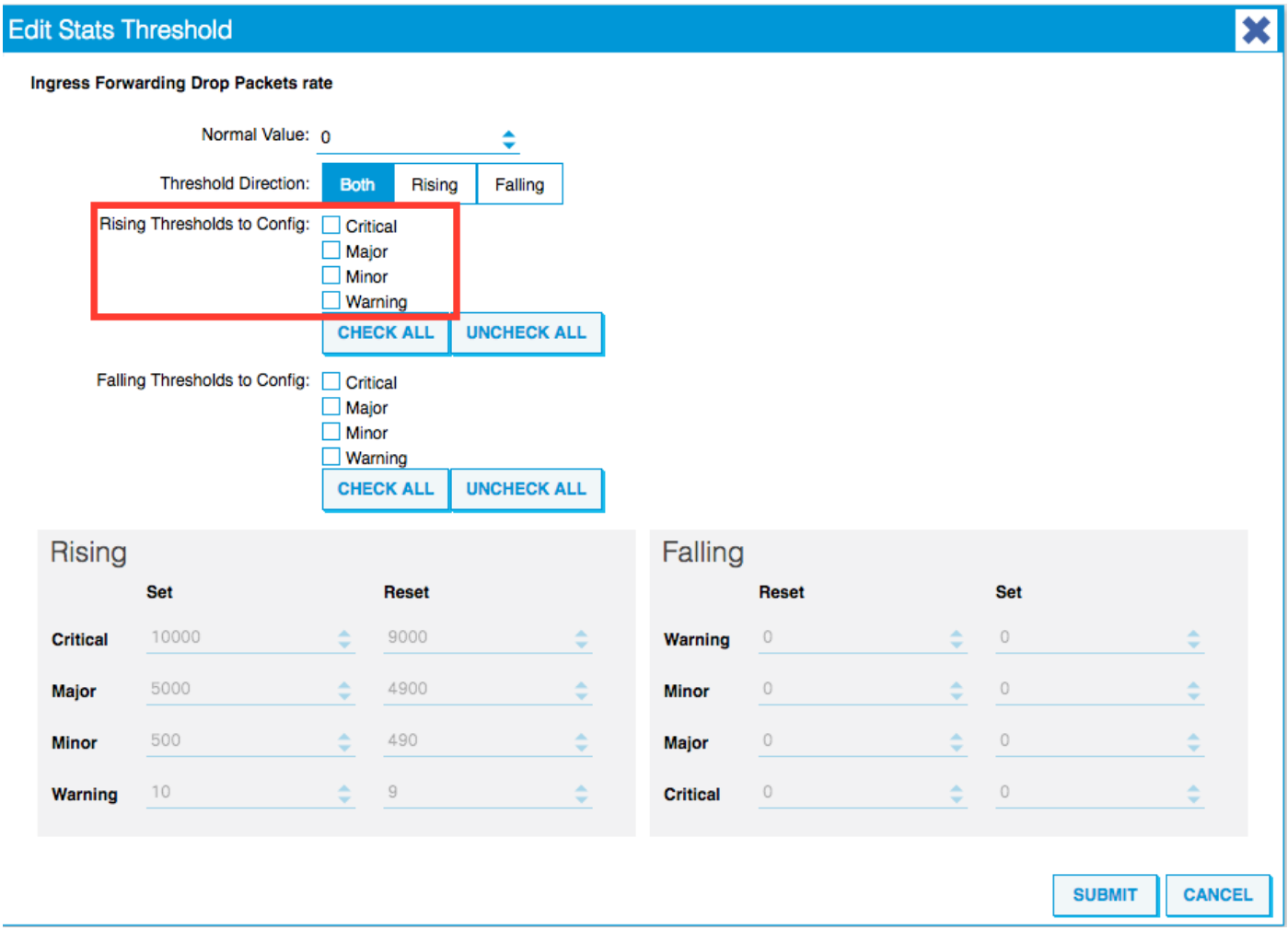
3. Clique sobre **+** ao lado dos pontos iniciais da configuração



4. Edite o ponto inicial para quedas de buffer



5. A recomendação é desabilitar as elevações de limiar à configuração para crítico, principal, menor, e advertir para enviar a taxa da gota.


Edit Stats Threshold
Ingress Forwarding Drop Packets rate
Normal Value: 0
Threshold Direction: Both Rising Falling
Rising Thresholds to Config: Critical Major Minor Warning
CHECK ALL UNCHECK ALL
Falling Thresholds to Config: Critical Major Minor Warning
CHECK ALL UNCHECK ALL
Rising
Set Reset
Critical 10000 9000
Major 5000 4900
Minor 500 490
Warning 10 9
Falling
Reset Set
Warning 0 0
Minor 0 0
Major 0 0
Critical 0 0
SUBMIT CANCEL