Explicaciones de los incidentes de la caída de paquetes en el ACI

Contenido

Introducción

Este documento describe cada tipo del incidente, y el procedimiento cuando usted ve este incidente. Durante Operaton normal de una tela céntrica de la infraestructura de la aplicación de Cisco (ACI), el administrador puede ver que los incidentes con certeza teclean de las caídas de paquetes.

Contribuido por José Ristaino, Takuya Kishida, ingenieros de Cisco TAC.

Objetos administrados

En Cisco ACI, todos los incidentes se aumentan bajo objetos administrados (MES). Por ejemplo, un incidente "*F11245 - los paquetes del descenso del ingreso rate(l2IngrPktsAg15min:dropRate)*" está mirando el *dropRate del* parámetro en el MES *l2IngrPktsAg15min*.

Esta sección introduce algo del **objeto administrado del** ejemplo **(MES) relacionó los incidentes del paquete del descenso**.

	Ejemplo:	Descripción	Muestra Paramters
l2IngrPkts	l2IngrPkts5min l2IngrPkts15min l2IngrPkts1h etc….	Esto representa las estadísticas del paquete de ingreso por el VLA N durante cada período	dropRate floodRate multicastRa unicastRate
l2IngrPktsAg	l2IngrPktsAg15min l2IngrPktsAg1h l2IngrPktsAg1d etc….	Esto representa las estadísticas del paquete de ingreso por EPG, el BD, el VRF etc…. El ex.) stats EPG representa la agregación de los stats del VLA N que pertenecen al EPG	dropRate floodRate multicastRa unicastRate
eqptIngrDropPkts	eqptIngrDropPkts15min eqptIngrDropPkts1h eqptIngrDropPkts1d etc….	Esto representa las estadísticas de paquete del descenso del ingreso por la interfaz durante cada período	forwardingR *1 errorRate *1 bufferRate *

*1: Estos contadores en los eqptIngrDropPkts son no se utilizan más a partir 1.3(2) de las versiones debido a - limitación de la plataforma EX en el descenso delantero con SUP_REDIRECT.

Obsérvese por favor que esta implementación se podría cambiar otra vez en el futuro.

Tipos del contador de caídas del hardware

En los 9000 Switch del nexo que se ejecutan en el modo ACI, hay 3 Contadores de hardware importantes por la razón del descenso de la interfaz de ingreso en ASIC.

Un dropRate en l2IngrPkts, l2IngrPktsAg incluye esos contadores. Tres parámetros (forwardingRate, errorRate, bufferRate) en la tabla antedicha para los eqptIngrDropPkts representan a cada tres contadores de la interfaz.

Reenvío

Los descensos delanteros, son los paquetes que se caen en el bloque de las operaciones de búsqueda (LU) de ASIC. En el bloque LU, se toma una decisión de reenvío de paquetes basado en la información de encabezado de paquete. Si la decisión es caer el paquete, se cuenta el descenso delantero. Hay una variedad de razones que éste puede suceder, sino dejar hablamos los principales:

SECURITY_GROUP_DENY

Un descenso debido a los contratos que falta para permitir la comunicación.

Cuando un paquete ingresa la tela, el Switch mira la fuente y el destino EPG para considerar si hay un contrato que permite esta comunicación. Si la fuente y el destino están en diversos EPG, y no hay contrato que permite este tipo de paquete entre ellos, el Switch caerá el paquete y lo etiquetará como SECURITY_GROUP_DENY. Esto incrementa al contador de caídas delantero.

VLAN_XLATE_MISS

Un descenso debido al VLA N inadecuado.

Cuando un paquete ingresa la tela, el Switch mira el paquete para determinar si la configuración en el puerto permite este paquete. Por ejemplo, una trama ingresa la tela con una etiqueta del 802.1Q de 10. Si el Switch tiene VLAN10 en el puerto, examinará el contenido y tomará una decisión de reenvío basada en el MAC de destino. Sin embargo, si el VLAN10 no está en el puerto, lo caerá y lo etiquetará como VLAN_XLATE_MISS. Esto incrementará al contador de caídas delantero.

La razón del “XLATE” o “traduce” es porque en el ACI, el Switch de la hoja tomará una trama con un encap del 802.1Q y la traducirá a un nuevo VLA N que sea utilizado para el VXLAN y la otra normalización dentro de la tela. Si la trama viene adentro con un VLA N no desplegada, la “traducción” fallará.

ACL_DROP

Un descenso debido al Sup-tcam.

el Sup-tcam en el Switches ACI contiene las reglas especiales que se aplicarán encima de la decisión de reenvío normal L2/L3. Las reglas en el Sup-tcam son incorporadas y no usuario configurables. El objetivo de las reglas del Sup-tcam es principalmente manejar algunas excepciones o algunas de tráfico del plano del control y no prepuestas para ser marcado o para ser monitoreado por los usuarios. Cuando el paquete está golpeando las reglas del Sup-tcam y la regla es caer el paquete, se cuenta el paquete perdidos pues ACL_DROP y él incrementarán al contador de caídas delantero. Cuando ocurrió esto, significa generalmente que el paquete está a punto de ser remitido contra los principales básicos de la expedición ACI.

Observe que, aunque el nombre del descenso es ACL_DROP, este “ACL” no es lo mismo que la lista de control de acceso normal que se puede configurar en los dispositivos independientes NX-OS o cualquier otra encaminamiento/dispositivo swtching.

SUP_REDIRECT

Esto no es un descenso.

Un paquete reorientado sorbo (es decir CDP/LLDP/UDLD/BFD etc…) se puede contar como descenso delantero incluso pensó que el paquete está procesado y que remitido correctamente al CPU.

Esto puede ocurrir solamente adentro - Plataforma EX tal como N9K-C93180YC-EX.

Éstos no se deben contar como “descenso” sin embargo que está debido a la plataforma de la limitación ASIC adentro - EX.

Error

Cuando el Switch recibe una trama inválida, se cae como error. Los ejemplos de esto incluyen las tramas con los errores FCS o CRC.

Buffer

Cuando el Switch recibe una trama, y no hay créditos del búfer disponibles para el ingreso o la salida, la trama será caída con el “buffer”. Esto hace alusión típicamente a la congestión en alguna parte en la red. El link que está mostrando que el incidente podría ser lleno, o, el link que contiene el destino puede ser congestionado.

Ver el Stats del descenso en el CLI

Objetos administrados

Secure Shell (SSH) a uno del APIC y de los siguientes comandos funcionados con.

moquery apic1# **- c l2IngrPktsAg15min**

Esto proporcionará todas las instancias de objeto para esta clase l2IngrPktsAg15min.

Aquí está un ejemplo con un filtro para preguntar un objeto específico. En este ejemplo, el filtro es mostrar solamente un objeto con los atributos **dn** cuál incluye el "tn-TENANT1/ap-APP1/epg-EPG1".

También este ejemplo utiliza el egrep para mostrar solamente los atributos requeridos.

Salida de ejemplo 1: EPG contradicen el objeto (l2IngrPktsAg15min) del arrendatario TENANT1, el perfil de aplicación APP1, el 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
```

O podríamos utilizar otra opción **- d** en vez de **- c** para conseguir un objeto específico si usted conoce el objeto dn.

Salida de ejemplo 2: EPG contradicen el objeto (l2IngrPktsAg15min) del arrendatario TENANT1, el perfil de aplicación APP1, el 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

Si usted ve los incidentes, o quiere marcar las caídas de paquetes en los switchports usando el CLI, la mejor manera de hacer esto está viendo los contadores de la plataforma en hardware. La mayoría, pero no todos los contadores se muestran usando la **interfaz de la demostración**. Las 3 razones principales del descenso se pueden ver solamente usando los contadores de la plataforma. Para ver éstos, realice estos pasos:

Hoja

SSH a la hoja y ejecutado estos comandos.

Vsh_lc ACI-LEAF#
<x> del puerto de los contadores internos de la plataforma de la demostración module-1#

* donde X representa el número del puerto

Salida de ejemplo 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 -----
```

Espina dorsal

Para una espina dorsal encajonada (N9K-C9336PQ), es exactamente lo mismo que la hoja.

Para las espinas dorsales modulares (N9K-C9504 etc…), usted debe primero asociar el linecard determinado antes de que usted pueda ver los contadores de la plataforma. SSH a la espina dorsal y ejecutado estos comandos

Vsh ACI-SPINE#

<x> del módulo de la fijación ACI-SPINE#

<y> del puerto de los contadores internos de la plataforma de la demostración module-2#.

* donde X representa el número de módulo para el linecard que usted quisiera ver

Y representa el número del puerto

Salida de ejemplo para los Ethernetes 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 -----
```

Incidentes

F11245 - tarifa de los paquetes del descenso del ingreso (l2IngrPktsAg15min:dropRate)

Descripción:

Este incidente puede incrementar cuando los paquetes de la capa 2 consiguen caídos con la razón del “descenso delantero”. Puesto que hay una variedad de diversas razones,

el más común es:

En - Plataforma EX tal como N9K-C93180YC-EX, hay una limitación donde los paquetes L2 que necesitan conseguir reorientaron al CPU (es decir CDP/LLDP/UDLD/BFD, etc), conseguirá registrado pues un “descenso delantero” así como consigue copiado al CPU. Esto es debido a una limitación de ASIC usado en los modelos EX del nexo 9000.

Debido a esto, cuando las porciones de protocolos del avión del control se habilitan en una interfaz, estos incidentes pueden ser aumentados.

Resolución:

Puesto que no hay impacto del servicio, la recomendación de la mejor práctica es aumentar el umbral para el incidente tal y como se muestra en de la sección del **umbral Stats**. Para hacer esto, vea las instrucciones en el umbral Stats.

F100264 - los paquetes del descenso de memoria intermedia de ingreso valoran (eqptIngrDropPkts5min:bufferRate)

Descripción:

Este incidente puede incrementar cuando los paquetes se están cayendo en un puerto con la razón “buffer” como se mencionó anteriormente, esto sucede típicamente cuando hay congestión en una interfaz en el ingreso o la dirección de salida.

Resolución:

Este incidente representa los paquetes perdidos reales en el entorno debido a la congestión. Los paquetes perdidos pueden causar los problemas con las aplicaciones que se ejecutan en la tela ACI. Los administradores de la red deben aislar el flujo de paquetes y determinarlo si la congestión es debido a los flujos de tráfico inesperados, al Equilibrio de carga ineficaz, al etc; o utilización prevista en esos puertos.

F100696 - paquetes del descenso de la expedición del ingreso (eqptIngrDropPkts5min:forwardingRate)

Nota: Comenzando en la versión 1.3(2), los descensos delanteros se quitan del objeto eqptIngrDropPkts5min, así que este incidente no se debe considerar para este problema.

Este incidente es causado por algunos escenarios. El más común es:

Descensos de la espina dorsal de la descripción 1)

Cuando un ARP o un paquete del IP se remite a la espina dorsal para las operaciones de búsqueda del proxy y el punto final es desconocido en la tela, un special espiga el paquete será generado y enviado a todas las hojas en el BD apropiado
dirección de grupo de multidifusión. Esto accionará un pedido ARP de cada hoja en el dominio de Bridge (BD) de descubrir el punto final. Debido a una limitación, el paquete del espigueo recibido por la hoja también se refleja
nuevamente dentro de la tela y acciona un descenso de la expedición en el link de la espina dorsal. El descenso delantero se incrementa solamente en el hardware de la espina dorsal de la generación 1.

Resolución 1)

Puesto que usted sabe que el problema es causado por un dispositivo que envía el tráfico de la unidifusión desconocida en la tela ACI, usted necesita imaginar que el dispositivo está causando a esto, y ver si usted puede prevenirlo. Esto es causada generalmente por los dispositivos que analizan o sondan para los IP Addresses en las subredes para monitorear los propósitos. Para encontrar lo que está enviando el IP este tráfico, SSH sobre la hoja que está conectada con la interfaz de la espina dorsal que muestra el incidente.

De allí, usted puede funcionar con este comando de ver la dirección IP de origen (sorbo) que está accionando el paquete del espigueo:

```
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 allí, usted puede investigar porqué 192.168.21.150 está enviando este tráfico en la tela, y ver si usted puede atenuarla de allí.

Descensos de la hoja de la descripción 2)

Si este incidente se considera en una interfaz de la hoja, el casue más probable es debido a los descensos SECURITY_GROUP_DENY mencionados.

Resolución 2)

En una hoja, usted guarda un registro de los paquetes negados debido contratar las infracciones. Este registro no captura todos para proteger a los recursos de la CPU sin embargo que todavía le proporciona una gran cantidad de registros.

Para conseguir los registros qué usted quiere, si la interfaz el incidente se aumenta encendido es parte de al canal del puerto, usted necesita utilizar este comando y grep para el canal del puerto. Si no, usted puede utilizar la interfaz física:

Este registro se puede rodar rápidamente encima dependiendo de la cantidad de descensos del 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
```

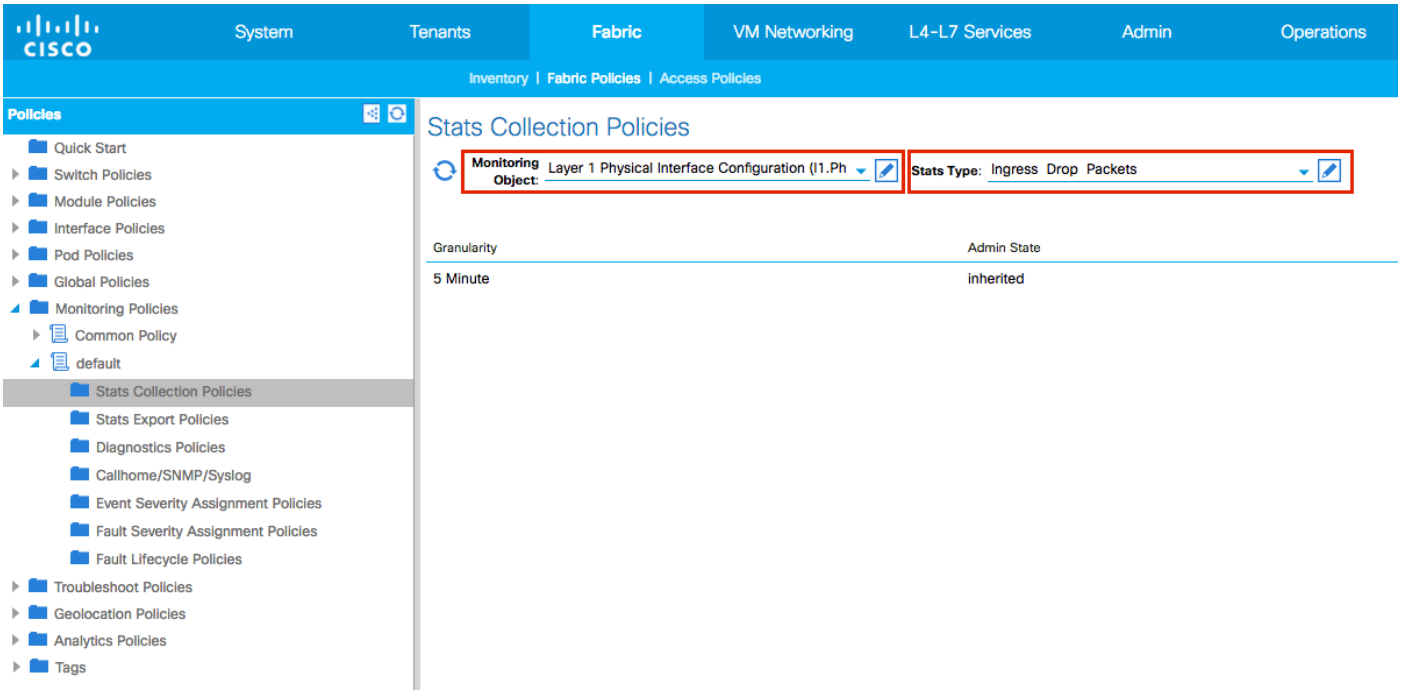
En este caso, 192.168.21.150 está intentando enviar los mensajes ICMP (protocolo IP número 1) a 192.168.20.3. Sin embargo, no hay contrato entre los 2 EPG que permite el ICMP, así que se cae el paquete. Si el ICMP se supone para ser permitido, un contrato se puede agregar entre los dos EPG.

Umbral Stats

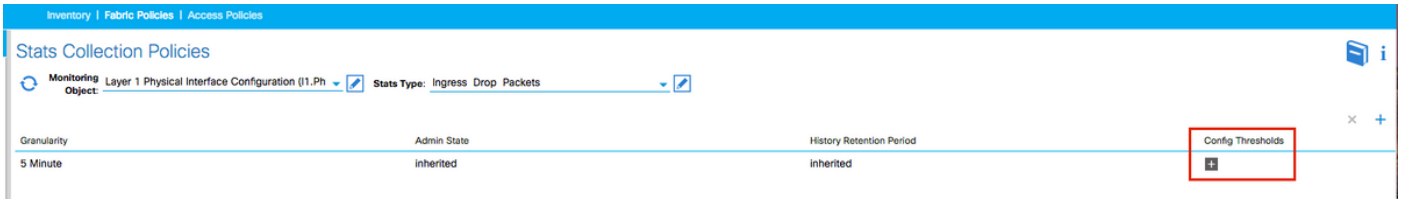
Esta sección describe cómo cambiar un umbral para los objetos de las estadísticas que podrían potencialmente criar a un contador de caídas del agaist del incidente.

El siguiente ejemplo es cambiar el umbral para el *descenso* delantero en los *eqptIngrDropPkts*.

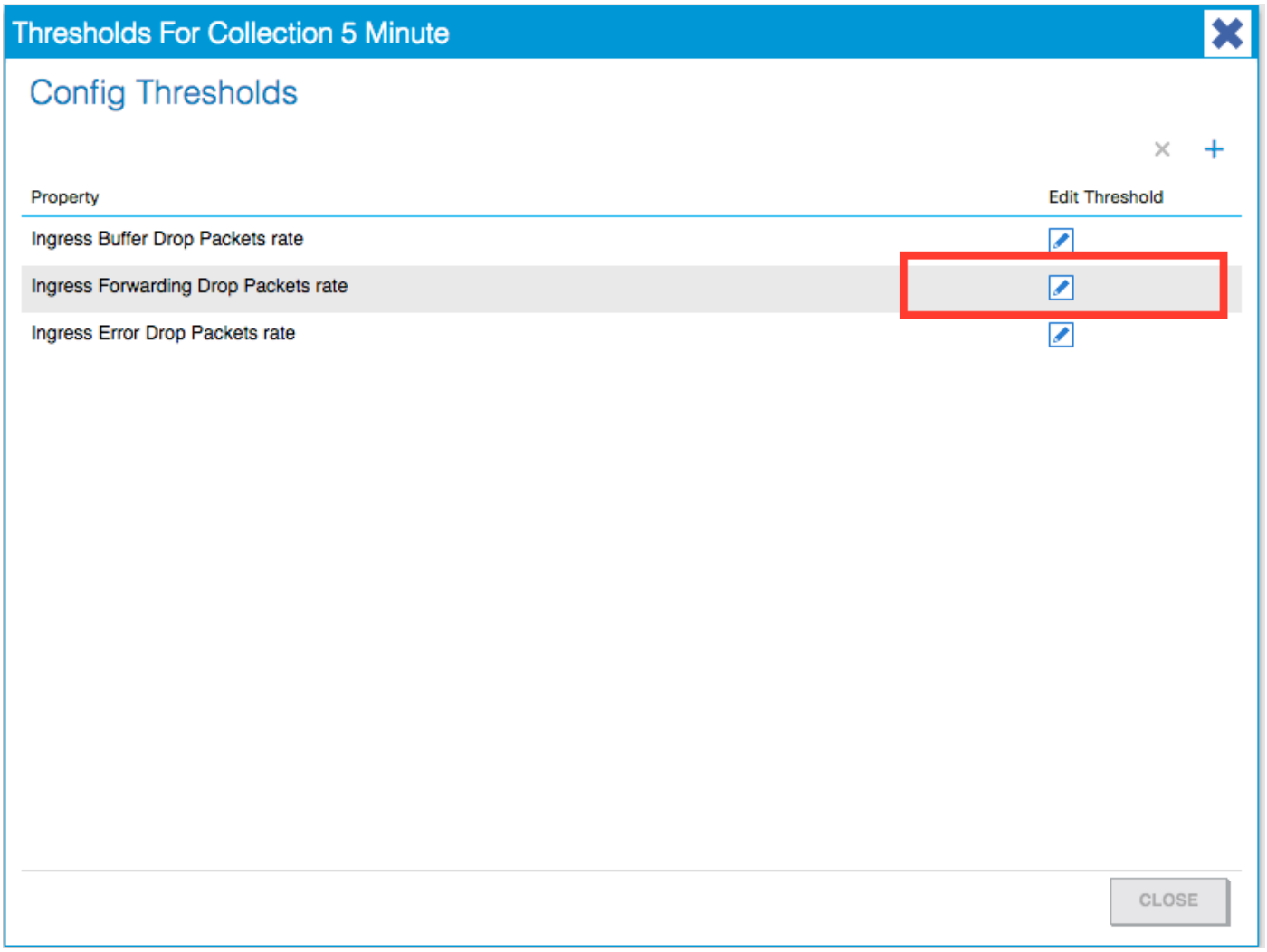
1. Navegue a las **directivas >Fabric de la tela >Monitoring las directivas de la colección de los >Stats de las directivas > del valor por defecto.**
2. **Del objeto de la supervisión** caiga abajo, eligen la **configuración de interfaz física del Layer 1 (l2.PhysIf)** y el **tipo Stats**, elige los **paquetes del descenso del ingreso**



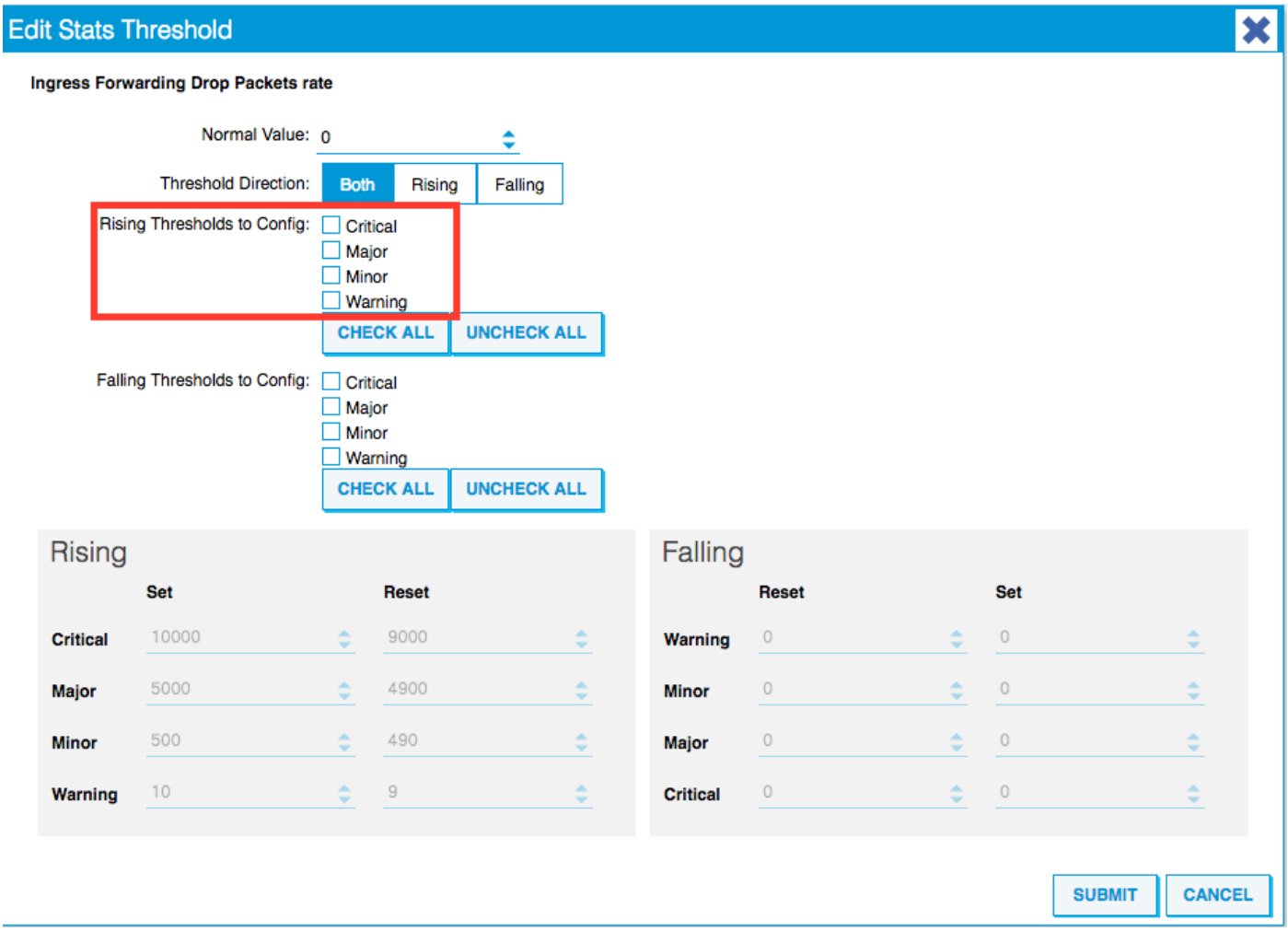
3. Haga clic en **+** al lado de los umbrales de los Config



4. Edite el umbral para las caídas del búfer



5. La recomendación es inhabilitar los umbrales de límite superior a los config para crítico, principal, de menor importancia, y advertir para remitir la tarifa del descenso.


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