Explicaciones de los incidentes del descenso del paquete en el ACI

Contenido

Introducción
Objetos administrados
Tipos del contador de caídas de la dotación física
Reenvío
SECURITY_GROUP_DENY
VLAN_XLATE_MISS
ACL_DROP
SUP_REDIRECT
Error
Almacenador intermediario
Ver el Stats del descenso en el CLI
Objetos administrados
Contadores de hardware
Hoja
Espina dorsal
Incidentes
F112425 - tarifa de los paquetes del descenso del ingreso (l2IngrPktsAg15min:dropRate)
Descripción:
Resolución:
F100264 - tarifa de los paquetes del descenso de memoria intermedia de ingreso (eqptIngrDropPkts5min:bufferRate)
Descripción:
Resolución:
F100696 - paquetes del descenso de la expedición del ingreso (eqptIngrDropPkts5min:forwardingRate)
Descensos de la espina dorsal de la descripción 1)
Resolución 1)
Descensos de la hoja de la descripción 2)
Resolución 2)
Umbral Stats
Tarifa delantera de los paquetes del descenso en los eqptIngrDropPkts
Tarifa de los paquetes del descenso del ingreso en l2IngrPktsAg

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 pulsan de los descensos del paquete.

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) relacionado para caer los incidentes del paquete**.

	Ejemplo:	Descripción	Muestra Paramters	Muestra ME contra se aumenta qué inciden
l2IngrPkts	l2IngrPkts5min l2IngrPkts15min l2IngrPkts1h etc….	Esto representa las estadísticas del paquete de ingreso por el VLA N durante cada período	dropRate floodRate multicastRate unicastRate	vlanCktEp (VLA N)
l2IngrPktsAg	l2IngrPktsAg15min l2IngrPktsAg1h l2IngrPktsAg1d etc….	Esto representa las estadísticas del paquete de ingreso por EPG, BD, VRF etc…. El ex.) stats EPG representa la agregación de los stats del VLA N que pertenecen al EPG	dropRate floodRate multicastRate unicastRate	fvAEPg (EP fvAp (perfil aplicación) fvBD (BD) l3extOut (L3OUT)
eqptIngrDropPkts	eqptIngrDropPkts15min eqptIngrDropPkts1h eqptIngrDropPkts1d etc….	Esto representa las estadísticas de paquete del descenso del ingreso por el interfaz durante cada período	forwardingRate *1 errorRate *1 bufferRate *1	l1PhysIf (puerto físic pcAggrIf (Canal de puerto)

*1: Estos contadores en los eqptIngrDropPkts pueden ser falso aumentado debido a una limitación ASIC en varios nexos 9000 Plataformas, porque los paquetes SUP_REDIRECT se están registrando como descensos delanteros. Vea también CSCvo68407 y CSCvn72699 para detalles y versiones corregidas más futuros.

Tipos del contador de caídas de la dotación física

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 conmutador 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 conmutador 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 conmutador mira el paquete para determinar si la configuración en el puerto permite este paquete. Por ejemplo, un marco ingresa la tela con una etiqueta del 802.1Q de 10. Si el conmutador tiene VLAN10 en el puerto, examinará el contenido y tomará una decisión de reenvío basada en el destino MAC. 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 de “XLATE” o “traduce” es porque en el ACI, el conmutador de la hoja tomará un marco con un encap del 802.1Q y lo traducirá a un nuevo VLA N que sea utilizado para el VXLAN y la otra normalización dentro de la tela. Si el marco viene adentro con un VLA N no desplegado, la “traducción” fallará.

ACL_DROP

Un descenso debido al sorbo-tcam.

el sorbo-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 sorbo-tcam son incorporadas y no usuario configurables. El objetivo de las reglas del sorbo-tcam es principalmente manejar algunas excepciones o algunas de tráfico del plano del control y no prepuestas para ser controlado o para ser vigilado por los usuarios. Cuando el paquete está golpeando las reglas del sorbo-tcam y la regla es caer el paquete, se cuenta el paquete eliminado 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 a la CPU.

Esto puede ocurrir solamente adentro - EX plataforma tal como N9K-C93180YC-EX. Éstos no se deben contar como “descenso” sin embargo que está debido a la EX plataforma de la limitación ASIC adentro -.

Error

Cuando el conmutador recibe un marco inválido en uno de los interfaces del panel frontal, se cae como error. Los ejemplos de esto incluyen los marcos con los errores FCS o CRC. Sin embargo, bajo funcionamientos normales, se espera que vea los paquetes de errores el incrementar en los puertos de link ascendente de hojas, o la espina dorsal vira hacia el lado de babor. Cuando mirar los puertos de la hoja Uplink, o la espina dorsal vira hacia el lado de babor, es el mejor controlar para saber si hay errores FCS/CRC usando el “interfaz de la demostración”.

Almacenador intermediario

Cuando el conmutador recibe un marco, y no hay créditos del búfer disponibles para el ingreso o la salida, el marco será caído con el “almacenador intermediario”. 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 del funcionamiento después de los comandos.

moquery apic1# **- c l2IngrPktsAg15min**

Esto proporcionará a 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 controlar los descensos del paquete en los switchports usando el CLI, la mejor manera de hacer esto está viendo los contadores de la plataforma en la dotación física. La mayoría, pero no todos los contadores se muestran usando el **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

F112425 - tarifa de los paquetes del descenso del ingreso

(l2IngrPktsAg15min:dropRate)

Descripción:

Uno de la razón popular de este incidente es que los paquetes de la capa 2 consiguen caídos con la razón del “descenso delantero”. Hay una variedad de razones, pero la más común es:

En algunas Plataformas (véase CSCvo68407), hay una limitación donde los paquetes L2 que necesitan conseguir reorientaron a la CPU (es decir CDP/LLDP/UDLD/BFD, etc), conseguirá registrado pues un “descenso delantero” así como consigue copiado a la CPU. Esto es debido a una limitación de ASIC usado en estos modelos.

Resolución:

Los descensos descritos arriba son puramente cosméticos, así que 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 “almacenador intermediario” como se mencionó anteriormente, esto sucede típicamente cuando hay congestión en un interfaz en el ingreso o la dirección de salida.

Resolución:

Este incidente representa los paquetes eliminados reales en el entorno debido a la congestión. Los paquetes eliminados 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 determinar 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: Una limitación ASIC como mencionado anteriormente para F11245 puede hacer estos incidentes ser aumentado también. Vea por favor CSCvo68407 para otros detalles.

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

Descensos de la espina dorsal de la descripción 1)

Si este incidente se considera en un interfaz de la espina dorsal, podría deber traficar hacia una punto final desconocida.

Cuando un paquete ARP o IP se remite a la espina dorsal para las operaciones de búsqueda del proxy y la punto final es desconocida en la tela, un special espiga el paquete será generado y enviado a todas las hojas en la dirección de grupo de multidifusión (interna) apropiada BD. Esto accionará una petición ARP de cada hoja en el dominio del puente (BD) de descubrir la punto final. Debido a una limitación, el paquete del espigueo recibido por la hoja también se refleja nuevamente dentro de la tela otra vez y acciona un descenso de la expedición en el link de la espina dorsal conectado con la hoja. El descenso delantero en este decorado se incrementa solamente en la dotación física de la espina dorsal de la generación 1.

Resolución 1)

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

De allí, usted puede funcionar con este comando de ver la dirección IP de la fuente (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 = 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
```

En esta salida de ejemplo, el paquete del espigueo es accionado por 192.168.21.150 y se recomienda para ver si esto puede ser atenuada.

Descensos de la hoja de la descripción 2)

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

Resolución 2)

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

Para conseguir los registros requeridos, si el interfaz el incidente se aumenta encendido es parte de al Canal de puerto, él se requiere para utilizar este comando y grep para el Canal de puerto. Si no, la interfaz física puede grepped.

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: 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
```

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 aumentar un incidente contra el contador de caídas.

Un umbral para las estadísticas de cada los objetos (es decir l2IngrPkts, los eqptIngrDropPkts) se configura con la directiva de la supervisión contra la variedad de objetos.

Como se menciona en la tabla al principio, los eqptIngrDropPkts se vigilan debajo, por ejemplo, los objetos l1PhysIf con la directiva de la supervisión.

Los paquetes delanteros del descenso valoran en los eqptIngrDropPkts

Hay dos porciones para esto.

+ políticas de acceso (puertos hacia los dispositivos externos. a.k.a puertos del panel frontal)

+ directivas de la tela (puertos entre la HOJA y la ESPINA DORSAL. a.k.a puertos de la tela)

Front Panel Ports (ports towards external devices)

Fabric Ports (ports between LEAF and SPINE)

Cada puerto se opone (l1PhysIf, pcAggrIf) se podría asignar su propia **directiva de la supervisión** vía el **grupo de políticas del interfaz** tal y como se muestra en de la imagen arriba.

Por abandono, hay una **directiva de la supervisión del valor por defecto** bajo la **tela > políticas de acceso** y la **tela > las directivas de la tela** en el GUI APIC. Estas directivas de la supervisión del valor por defecto se asignan a todos los puertos respectivamente. La directiva de la supervisión del valor por defecto bajo políticas de acceso está para los puertos del panel frontal y la directiva de la supervisión del valor por defecto bajo directivas de la tela está para los puertos de la tela.

A menos que se requiera para cambiar los umbrales por los puertos, la directiva de la supervisión del valor por defecto en cada sección se puede modificar directamente para aplicar el cambio para todos los puertos del panel frontal y/o los puertos de la tela.

El ejemplo siguiente está a los umbrales del chage para el descenso delantero en los eqptIngrDropPkts en los puertos de la tela (**directivas de la tela**). Realice por favor la misma **tela > las políticas de acceso del** udner de la cosa para los puertos del panel frontal.

1. Navegue a las **directivas >Fabric de la tela >Monitoring las directivas.**

2. El clic derecho y selecciona “crea la directiva de la supervisión”.

(Si el cambio del umbral se puede aplicar a todos los puertos de la tela, navegue **para omitir** en vez de crear un nuevo)

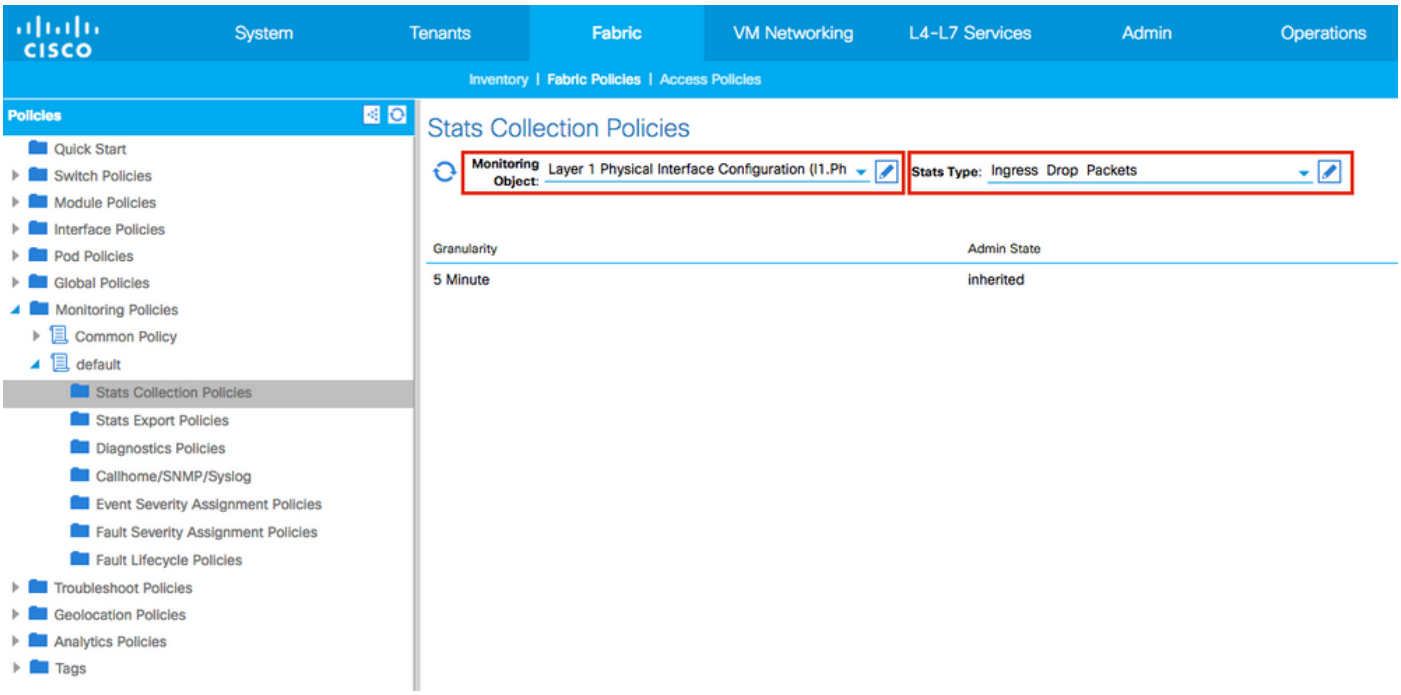
3. Amplíe la nueva directiva de la supervisión u omita y navegue a las **directivas de la recolección de estadísticas.**

4. Haga clic en el icono del lápiz para el objeto de la supervisión en el panel derecho, la configuración de interfaz física selecta del Layer 1 (l1.PhysIf).

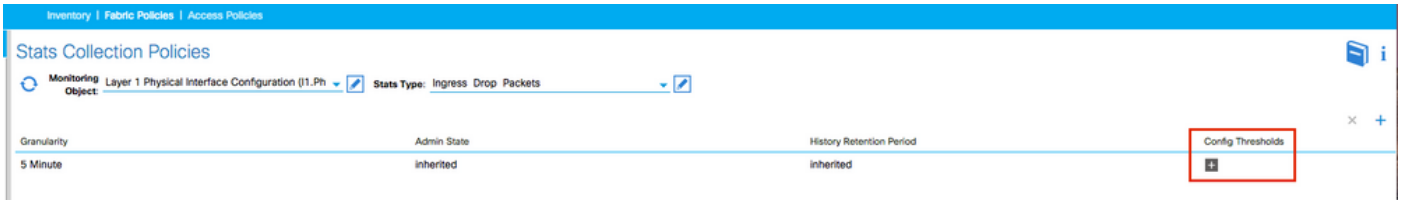
(Este paso 4 puede ser saltado cuando se utiliza la directiva predeterminada)

5. **Del objeto de la supervisión caiga abajo en el panel derecho, eligen la configuración de**

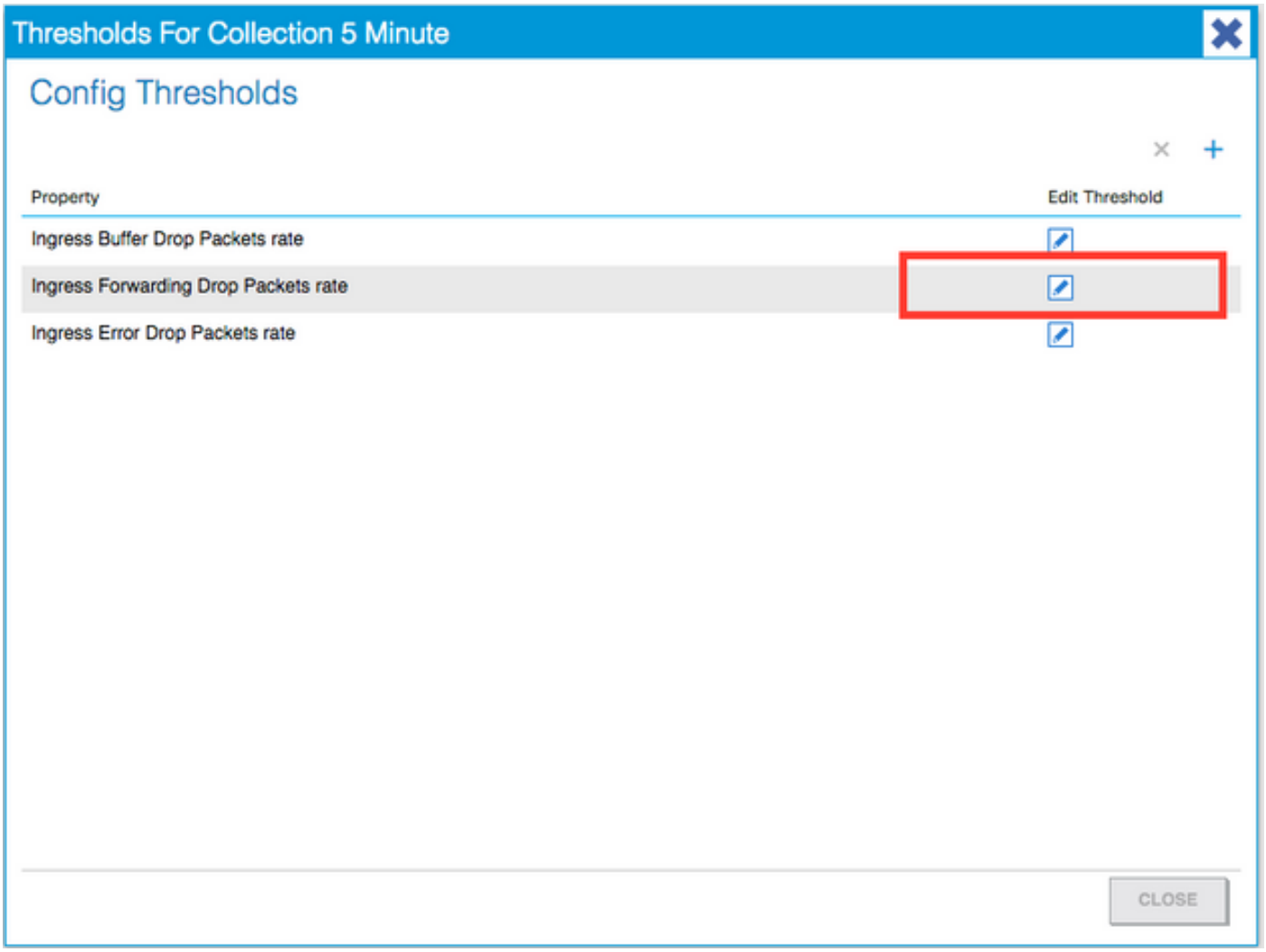
interfaz física del Layer 1 (l1.PhysIf) y el tipo Stats, elige los paquetes del descenso del ingreso



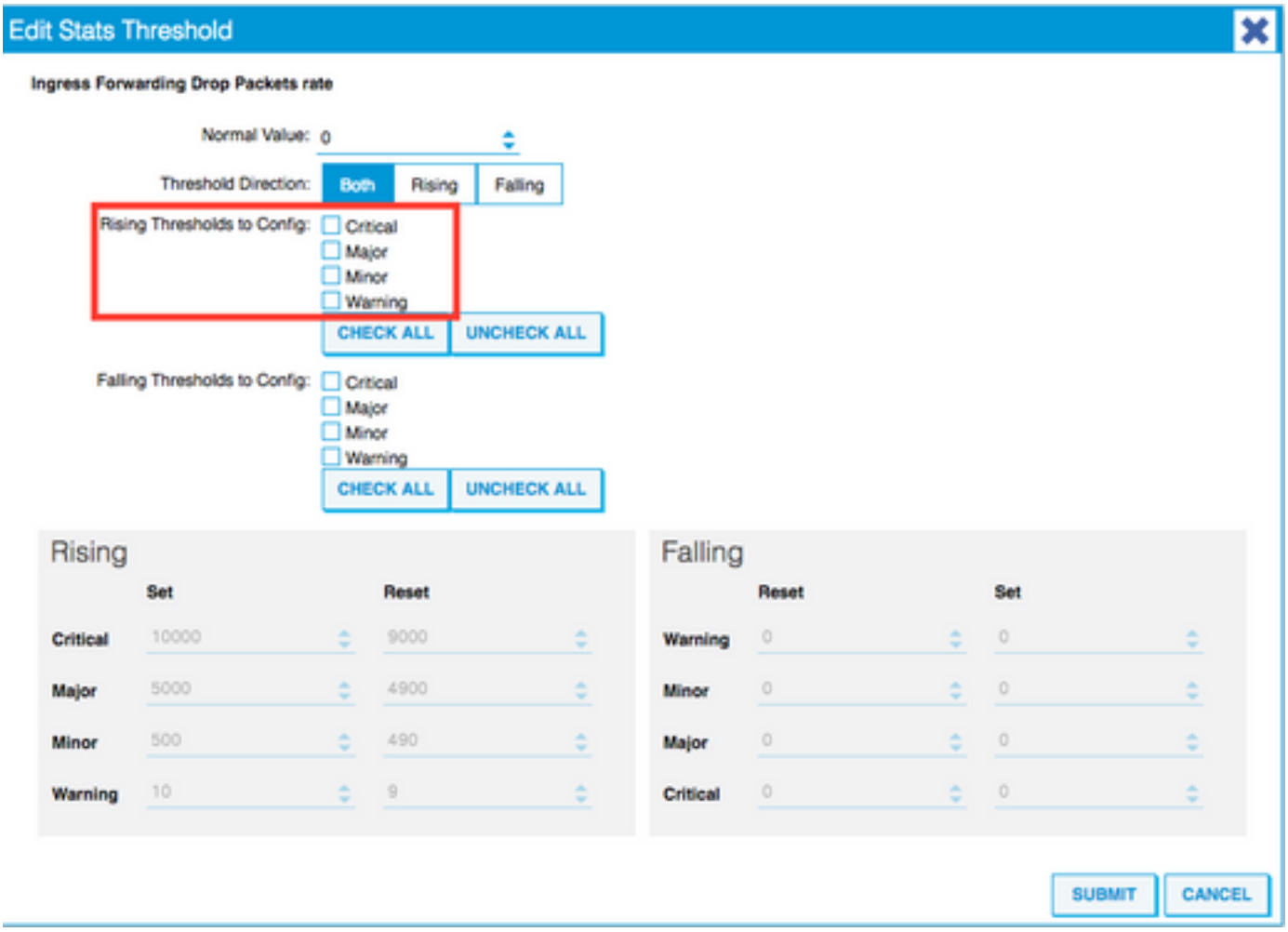
6. Haga clic en + al lado de los umbrales de los Config



7. Corrija el umbral para remitir el descenso

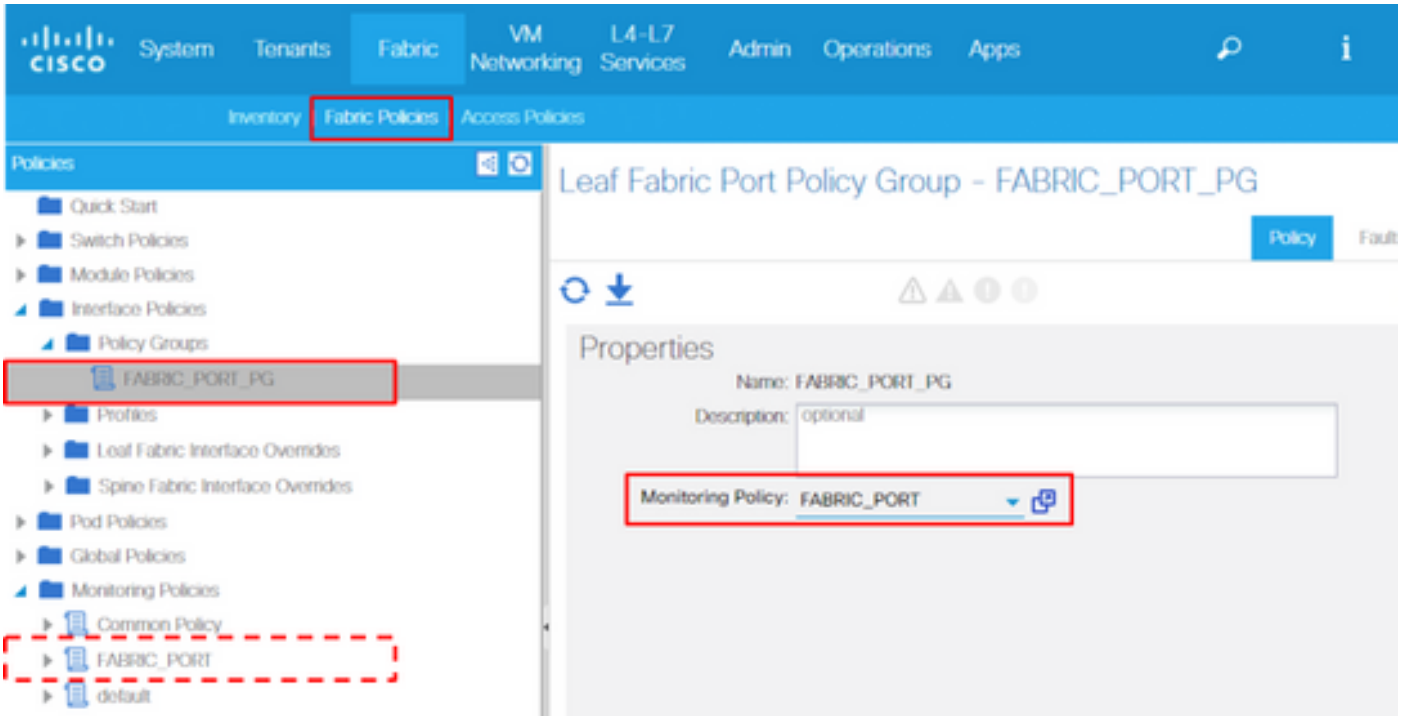


8. La recomendación es inhabilitar los umbrales de límite superior a los config para crítico, principal, de menor importancia, y advertir para remitir la tarifa del descenso.



9. Aplique esta nueva directiva de la supervisión al grupo de políticas del interfaz para los puertos requeridos. No olvide por favor configurar el perfil del interfaz, el perfil del conmutador, etc… en las directivas de la tela por consiguiente.

(Este paso 9 puede ser saltado cuando se utiliza la directiva predeterminada)

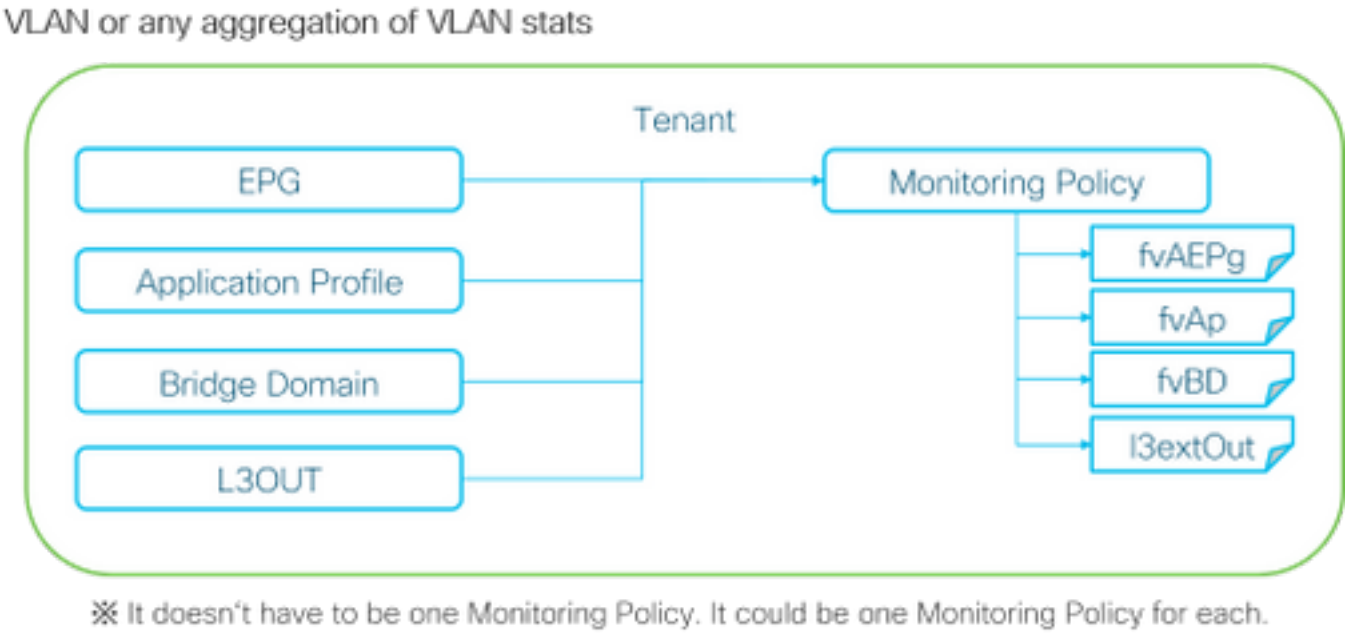


10. Si esto está para los puertos del panel frontal (políticas de acceso), realice por favor la misma cosa para el **interfaz Aggregated (pc.AggrIf)** en comparación con la **configuración de interfaz física del Layer 1 (l1.PhysIf)** para poder aplicarse esta nueva directiva de la supervisión al Canal de puerto así como al puerto físico.

(Este paso 10 puede ser saltado cuando se utiliza la directiva predeterminada)

Los paquetes del descenso del ingreso valoran en l2IngrPktsAg

Hay porciones múltiples para esto.



Mientras que la ilustración superior representa, l2IngrPktsAg se vigila bajo muchos objetos. La ilustración superior muestra solamente algunos ejemplos pero no todos los objetos para l2IngrPktsAg. Sin embargo, el umbral para las estadísticas se configura a través de la directiva así como de los eqptIngrDropPkts de la supervisión bajo l1PhysIf o pcAggrIf.

Cada uno se opone (EPG(fvAEPg), puente Domain(fvBD), etc…) se podría asignar su propia **directiva de la supervisión** tal y como se muestra en de la imagen arriba.

Por abandono, todos estos objetos bajo el arrendatario utilizan la **directiva de la supervisión del valor por defecto** bajo el **arrendatario > el campo común > supervisión limpian > valor por defecto** a menos que esté configurada de otra manera.

A menos que se requiera para cambiar los umbrales por cada componente, la directiva de la supervisión del valor por defecto bajo campo común del arrendatario se puede modificar directamente para aplicar el cambio para todos los componentes relacionados.

El ejemplo siguiente está a los umbrales del chage para los paquetes del descenso del ingreso valora en l2IngrPktsAg15min en el dominio del puente.

1. Navegue al **arrendatario > (nombre del arrendatario) > las directivas de la supervisión.**

(se utiliza el arrendatario necesita ser común si la directiva de la supervisión del valor por defecto o la nueva directiva de la supervisión necesita ser aplicada a través de los

arrendatarios)

2. El clic derecho y selecciona “crea la directiva de la supervisión”.

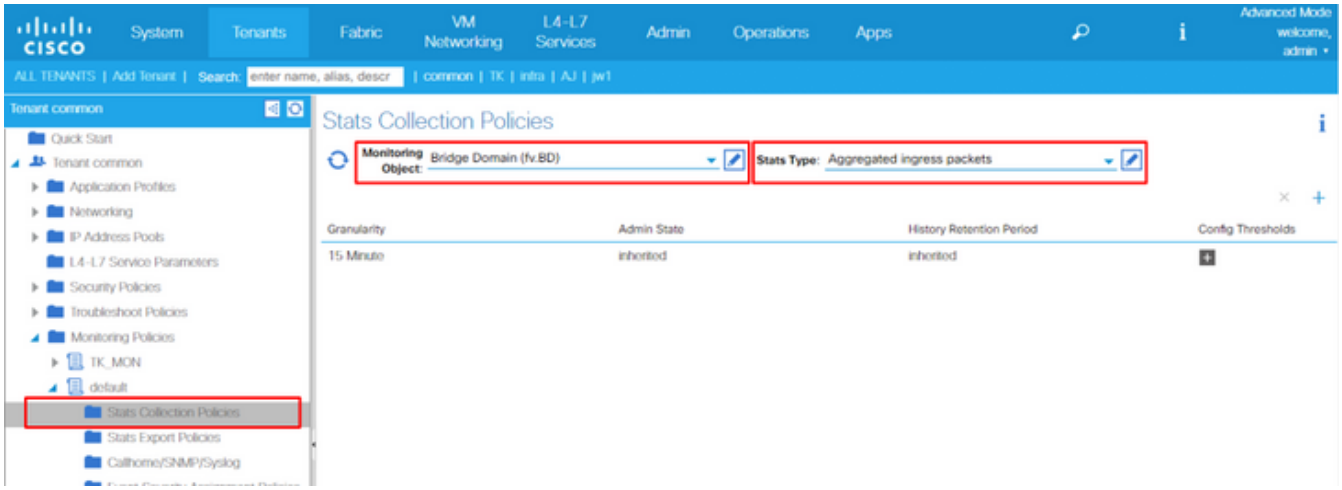
(Si el cambio del umbral se puede aplicar a todos los componentes, navegue **para omitir** en vez de crear un nuevo)

3. Amplíe la nueva directiva de la supervisión u omita y navegue a las **directivas de la recolección de estadísticas.**

4. Haga clic en el icono del lápiz para el objeto de la supervisión en el panel derecho, el dominio selecto del puente (fv.BD).

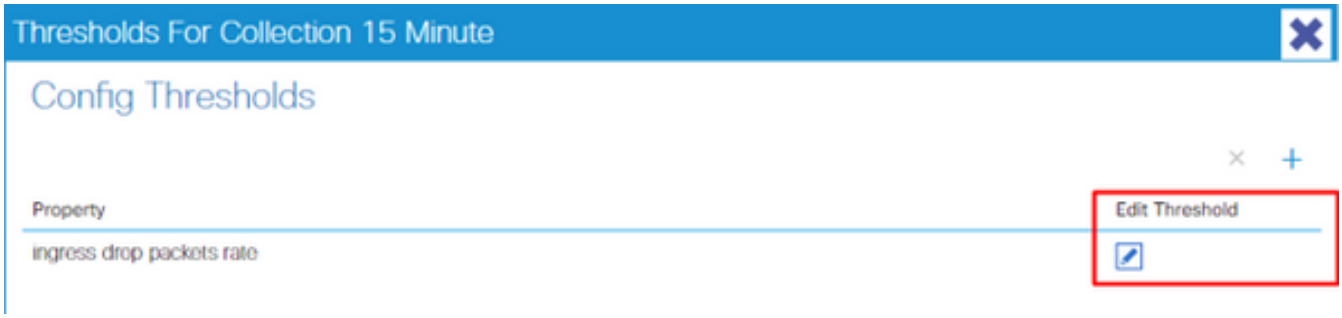
(Este paso 4 puede ser saltado cuando se utiliza la directiva predeterminada)

5. **Del objeto de la supervisión caiga abajo en el panel derecho, eligen el dominio del puente (fv.BD) y el tipo Stats, elige los paquetes de ingreso agregados.**



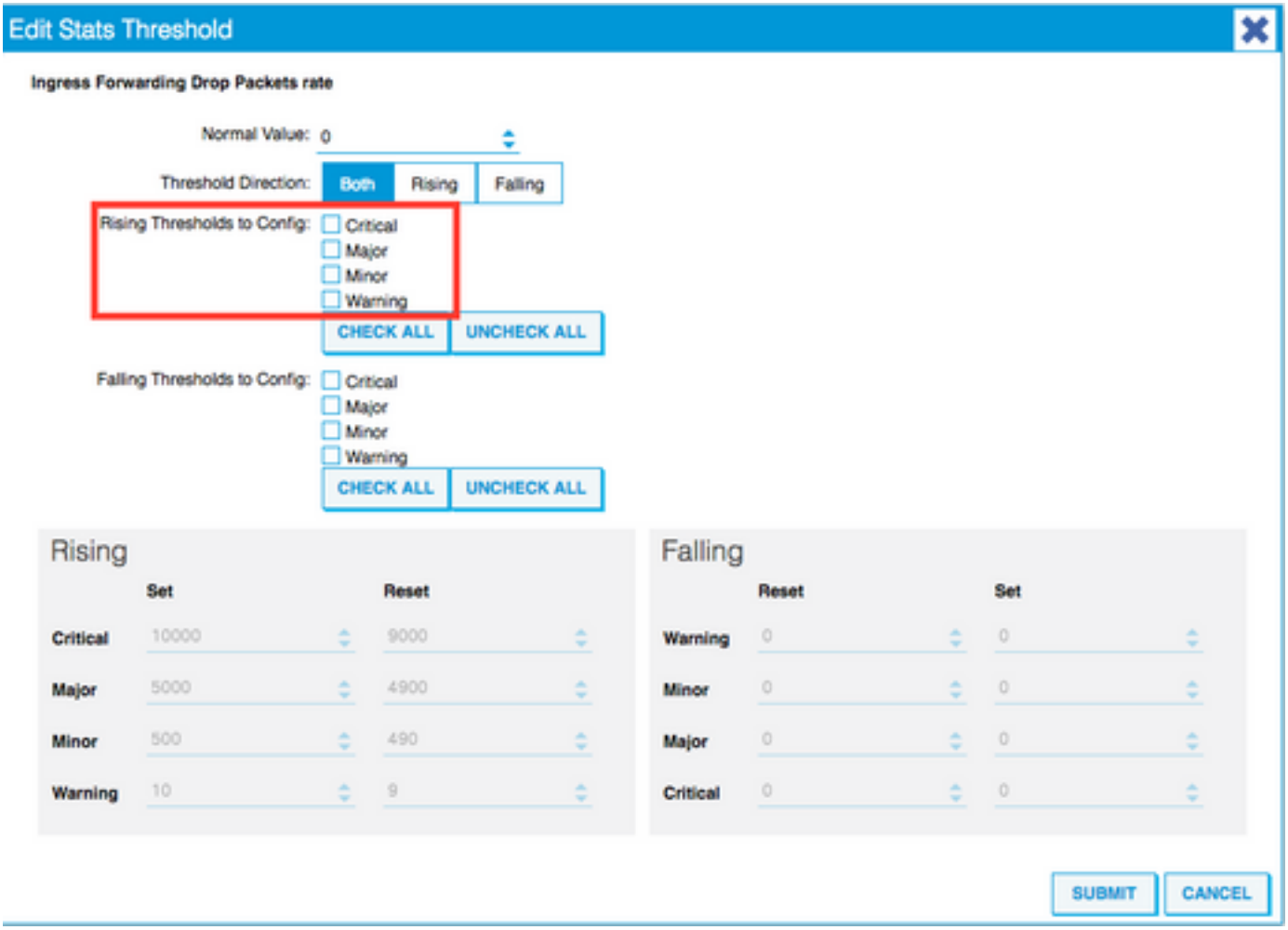
6. Haga clic en **+** al lado de los umbrales de los Config

7. Corrija el umbral para remitir el descenso



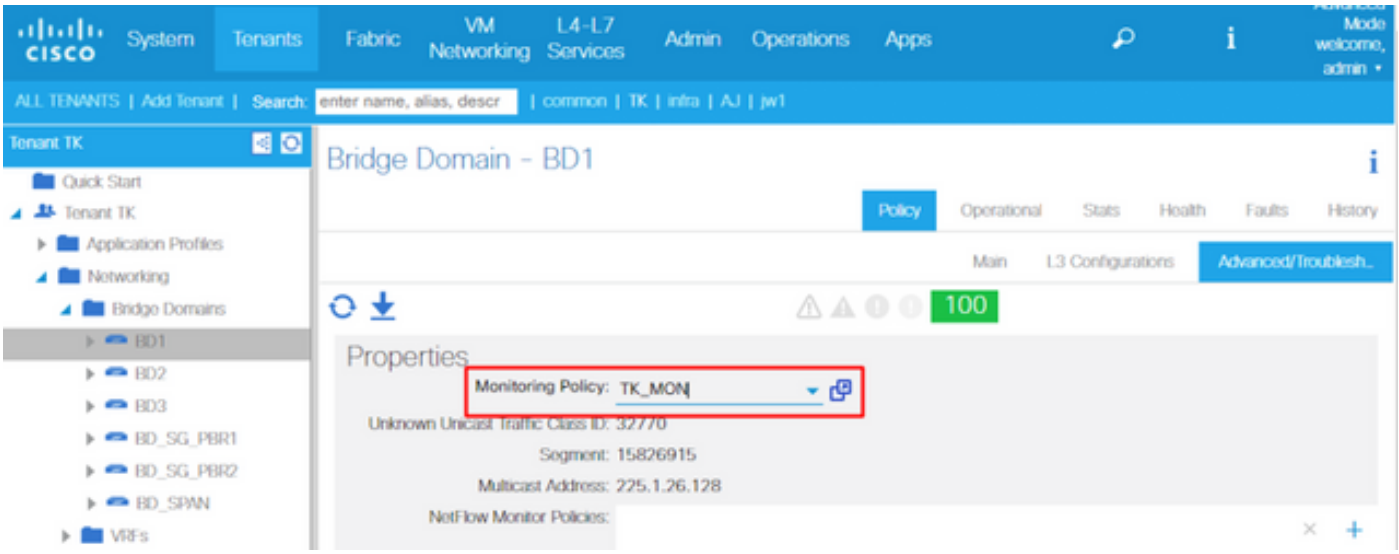
8. La recomendación es inhabilitar los umbrales de límite superior a los config para crítico,

principal, de menor importancia, y advertir para remitir la tarifa del descenso.



9. Aplique esta nueva directiva de la supervisión al dominio del puente que requiere el cambio del umbral.

(Este paso 9 puede ser saltado cuando se utiliza la directiva predeterminada)



NOTA
no la directiva de la supervisión del valor por defecto puede no tener configuraciones que está presente en la directiva de la supervisión del valor por defecto. Si se requiere para guardar eso la configuración lo mismo que la directiva de la supervisión del valor por

defecto, necesidad de usuarios de controlar los config de la directiva de la supervisión del valor por defecto y de configurar manualmente las mismas directivas en la directiva de la supervisión del no-valor por defecto.