Configuración de la lista de excepciones de no fiables/COOP en ACI

Contenido

Introducción

Este documento describe la función Lista de excepciones de no fiables/COOP en ACI (Application Centric Infrastructure) y abarca la configuración y la verificación.

¿Por qué lista de excepciones?

La función "Rogue EP Control" de ACI minimiza el impacto de los loops temporales poniendo en cuarentena los terminales dentro del dominio de bridge específico donde se producen. Sin embargo, esta función a veces puede causar interrupciones innecesarias. Por ejemplo, durante una recuperación ante fallos del firewall, ambos firewalls pueden transmitir tráfico momentáneamente mediante la misma dirección MAC (control de acceso a medios), lo que provoca fallos hasta que converge la red. Anterior a 5.2(3) Si ACI detecta 4 movimientos EP (terminal) en 60 segundos, se vuelve estático y no se le permite moverse durante los 30 minutos siguientes. 4 movimientos en 60 segundos pueden ser realistas en algunas implementaciones. El tiempo de espera de 30 minutos es agresivo para escenarios donde se esperan movimientos de EP.

Solución

Para solucionar este problema, es posible configurar una "Lista de excepciones de no fiables/COOP". MAC se dirige en la Lista de excepciones y, a continuación, utiliza criterios de umbral más altos para detectar el acceso no deseado. MAC configurado en la lista de excepciones se convierte en no fiable después de 3000 movimientos en un intervalo de 10 minutos.MAC la dirección de la lista de excepciones utiliza un umbral de atenuación COOP (Council of Oracle Protocol) más alto para evitar el dampening en COOP. Puede agregar hasta 100 direcciones MAC en la lista de excepciones.

Requisito previo

- Esta función está disponible desde la versión 5.2(3)
- Esta opción sólo se puede utilizar si el BD (dominio de puente) es un BD de nivel 2 (como si el BD no estuviera configurado para el routing IP)
- La función No fiable debe estar habilitada para que funcione el comportamiento Lista de excepciones no fiables.

Configuración de la lista de excepciones de no fiables/COOP

Esta función se puede utilizar en dominios de puente de capa 2 (L2 BD) para evitar que direcciones MAC específicas se marquen como no autorizadas debido a movimientos legítimos.

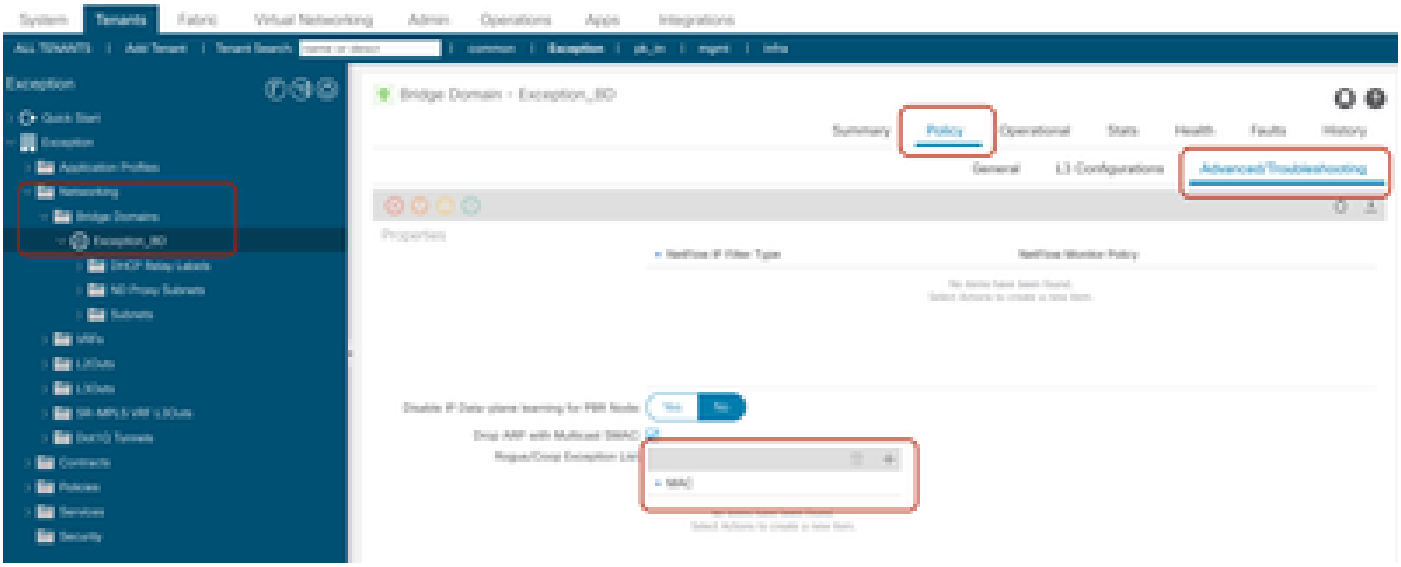
Configuración mediante la GUI de APIC (Application Policy Infrastructure Controller)

Para configurar:

Paso 1. Inicie sesión en la GUI de Cisco APIC.

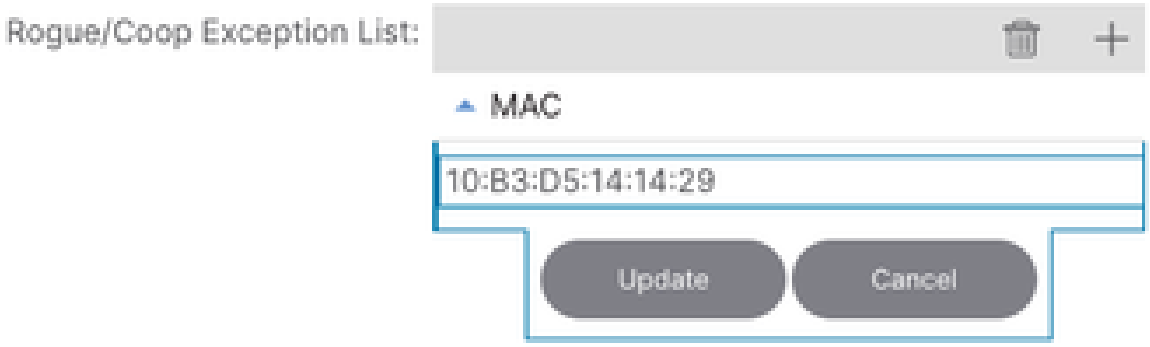
Paso 2. Vaya a Arrendatario > Redes > Dominios de puente > BD > Política > Ficha Avanzadas/Resolución de problemas

En esta página puede agregar direcciones MAC en la lista de excepciones.



Paso 3. Seleccione el icono + para agregar la dirección MAC en la lista de excepciones de no fiables/COOP.

Paso 4. Agregue la dirección MAC y actualícela.



Verificación

Para demostrar esta función, existe un terminal con la dirección MAC 10:B3:D5:14:14:29 conectado a nuestro fabric ACI dentro de la excepción de arrendatario y la excepción de BD de dominio de puente (BD).

Después de agregar la dirección MAC a la lista de excepciones de la sección "Configuración de la lista de excepciones de acceso no autorizado/COOP" de este documento, la configuración se puede verificar mediante la consulta de objetos administrados (MO): moquery -c fvRogueExceptionMac

CLI DE APIC:

<#root>

```
bgl-aci04-apic1#
moquery -c fvRogueExceptionMac

Total Objects shown: 1

# fv.RogueExceptionMac
mac : 10:B3:D5:14:14:29
annotation :
childAction :
descr :
dn : uni/tn-Exception/BD-Exception_BD/rgexpmac-10:B3:D5:14:14:29
extMngdBy :
lcOwn : local
modTs : 2024-07-17T04:57:04.923+00:00
name :
nameAlias :
rn : rgexpmac-10:B3:D5:14:14:29
status :
uid : 16222
userdom : :all:

bgl-aci04-apic1#
```

CLI de hoja:

Esta moconsulta proporciona los temporizadores aplicados en la lista de excepciones no autorizadas.

<#root>

```
bgl-aci04-leaf1#

moquery -c "topoctrlRogueExpP"


Total Objects shown: 1

# topoctrl.RogueExpP
childAction :
descr :
dn : sys/topoctrl/rogueexpp
lcOwn : local
modTs : 2024-07-13T15:51:57.921+00:00
name :
nameAlias :
rn : rogueexpp
rogueExpEpDetectIntvl : 600   <<< Detection Interval in second
rogueExpEpDetectMult : 3000   <<< Detection Multiple (No of moves)
rogueExpEpHoldIntvl : 30      <<< Hold Interval in second
status :
```

Con moquery puede verificar que cualquier mac en particular se agrega en la lista de excepciones.

<#root>

```
bgl-aci04-leaf1#

moquery -c "l2RogueExpMac" -f 'l2.RogueExpMac.mac=="10:B3:D5:14:14:29"'


Total Objects shown: 1
# l2.RogueExpMac
mac : 10:B3:D5:14:14:29
childAction :
dn : sys/ctx-[vxlan-2293760]/bd-[vxlan-15957970]/rogueexpmac-10:B3:D5:14:14:29
lcOwn : local
modTs : 2024-07-17T04:57:04.939+00:00
name :
operSt : up
rn : rogueexpmac-10:B3:D5:14:14:29
status :
bgl-aci04-leaf1#
```

Para confirmar los parámetros de la lista de excepciones desde la CLI de hoja:

<#root>

```
module-1#
```

show system internal epmc global-info | grep "Rogue Exception List"

```
Rogue Exception List Endpoint Detection Interval : 600
Rogue Exception List Endpoint Detection Multiple : 3000
Rogue Exception List Endpoint Hold Interval : 30
module-1#
module-1#
module-1#
```

Para verificar el terminal en el aprendizaje en EPMC y comprobar los recuentos de movimiento también para ese terminal.

CLI de hoja:

<#root>

```
module-1#
```

show system internal epmc endpoint mac 10:B3:D5:14:14:29

```
MAC : 10b3.d514.1429 ::: Num IPs : 0
Vlan id : 9 ::: Vlan vnid : 8193 ::: BD vnid : 15957970
Encap vlan : 802.1Q/101
VRF name : Exception:Exception_vrf ::: VRF vnid : 2293760
phy if : 0x1a015000 ::: tunnel if : 0 ::: Interface : Ethernet1/22
Ref count : 5 ::: sclass : 16386
Timestamp : 07/17/2024 05:20:20.523019
::: last mv ts: 07/17/2024 05:19:17.424213 ::: ep move cnt: 9   <<<< Shows how many times endpoint move
::: Learns Src: Hal
EP Flags : local|MAC|sclass|timer|
Aging: Timer-type : HT ::: Timeout-left : 784 ::: Hit-bit : Yes ::: Timer-reset count : 0

PD handles:
[L2]: Hdl : 0x18c1e ::: Hit: Yes
::::


module-1#
```

Para comprobar la configuración de la lista de excepciones:

CLI de hoja:

<#root>

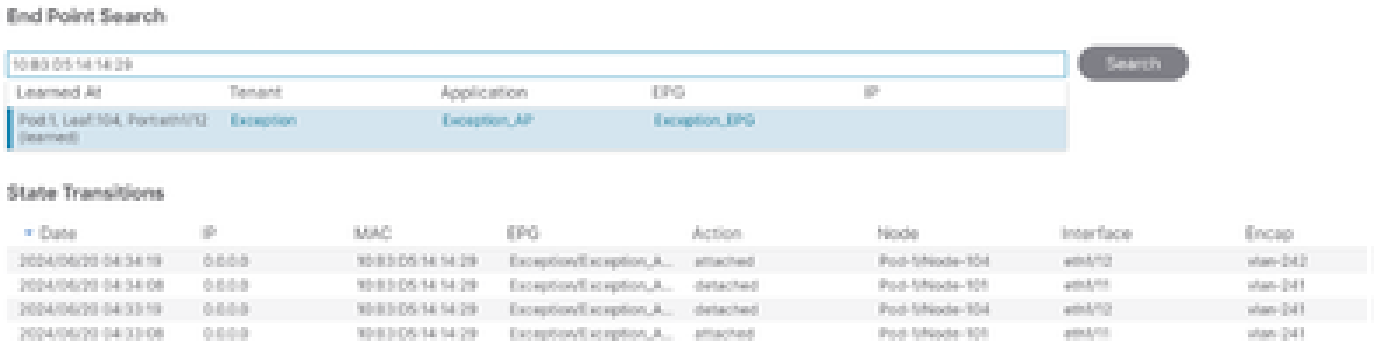
```
module-1#
```

show system internal epmc rogue-exp-ep

```
BD: 15957970 MAC:10b3.d514.1429
[01/01/1970 00:00:00.000000] : 0 Moves in 60 sec

module-1#
```

Puede comprobar los movimientos del terminal en la GUI de APIC en Operations > EP tracker, Search MAC address here.



Como todavía hay movimientos para esta dirección MAC, pero ahora no hay Rogue Flag para este punto final.

Esto se puede verificar con comandos.

CLI DE HOJA:

Para comprobar si el indicador de no fiable se agrega al terminal aprendido en el epm de hoja (administrador de terminales)

<#root>

```
bgl-aci04-leaf1#
```

show system internal epm endpoint mac 10:B3:D5:14:14:29

```
MAC : 10b3.d514.1429 ::: Num IPs : 0
Vlan id : 9 ::: Vlan vnid : 8193 ::: VRF name : Exception:Exception_vrf
BD vnid : 15957970 ::: VRF vnid : 2293760
Phy If : 0x1a015000 ::: Tunnel If : 0
Interface : Ethernet1/22
Flags : 0x80004804 ::: sclass : 16386 ::: Ref count : 4
EP Create Timestamp : 07/17/2024 05:19:10.424033
EP Update Timestamp : 07/17/2024 05:22:03.674624
EP Flags : local|MAC|sclass|timer|                <<<< Once if endpoint is rogue a Rogue flag is added

::::

bgl-aci04-leaf1#
```

CLI DE APIC:

Para comprobar si se ha producido algún error en el extremo de terminales no fiables.

<#root>

```
bgl-aci04-apic1#
```

```
moquery -c faultInst -f 'fault.Inst.code=="F3014"'
```

```
No Mos found
bgl-aci04-apic1#
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).