ACI에서 비인가/COOP 예외 목록 구성

목차

소개

이 문서에서는 ACI(Application Centric Infrastructure)의 Rogue/COOP Exception List 기능에 대해 설명하고 컨피그레이션 및 검증을 다룹니다.

예외 목록이 필요한 이유

ACI의 "비인가 EP 제어" 기능은 엔드포인트가 발생하는 특정 브리지 도메인 내에서 격리함으로써 임시 루프의 영향을 최소화합니다. 그러나 이 기능은 경우에 따라 불필요한 중단을 일으킬 수 있습니다. 예를 들어 방화벽 장애 조치 중에 두 방화벽이 동일한 MAC(Media Access Control) 주소를 사용하여 트래픽을 일시적으로 전송할 수 있으므로 네트워크가 통합될 때까지 결함이 발생합니다. 5.2(3) 이전 ACI에서 60초 내에 4개의 EP(엔드포인트) 이동을 탐지하면 정적으로 표시되며 이후 30분 동안 이동할 수 없습니다. 일부 구축에서는 60초 안에 4개의 이동이 현실적일 수 있습니다. EP 이동이 예상되는 시나리오의 경우 30분의 대기 시간이 매우 길어집니다.

솔루션

이 문제를 해결하기 위해 "Rogue/COOP 예외 목록"을 구성할 수 있습니다. 예외 목록의 MAC 주소는 더 높은 임계값 기준을 사용하여 Rogue를 탐지합니다. 예외 목록에 구성된 MAC은 10분 간격으로 3000번 이동한 후 비인가 상태가 됩니다. 예외 목록의 MAC 주소는 COOP에서 감소되지 않도록 더 높은 COOP(Council of Oracle Protocol) 댐프닝 임계값을 사용합니다. 예외 목록에 최대 100개의 MAC 주소를 추가할 수 있습니다.

사전 요구 사항

- 이 기능은 버전 5.2(3)부터 사용할 수 있습니다.
- 이 옵션은 BD(Bridge Domain)가 L2 BD인 경우에만 사용할 수 있습니다(BD가 IP 라우팅에 대해 구성되지 않은 경우).
- 비인가 예외 목록 동작이 작동하려면 비인가 기능을 활성화해야 합니다.

비인가/COOP 예외 목록의 구성

이 기능은 레이어 2 브리지 도메인(L2 BD)에서 사용할 수 있으며, 특정 MAC 주소가 합법적인 이동으로 인해 로그인으로 플래그되는 것을 방지할 수 있습니다.

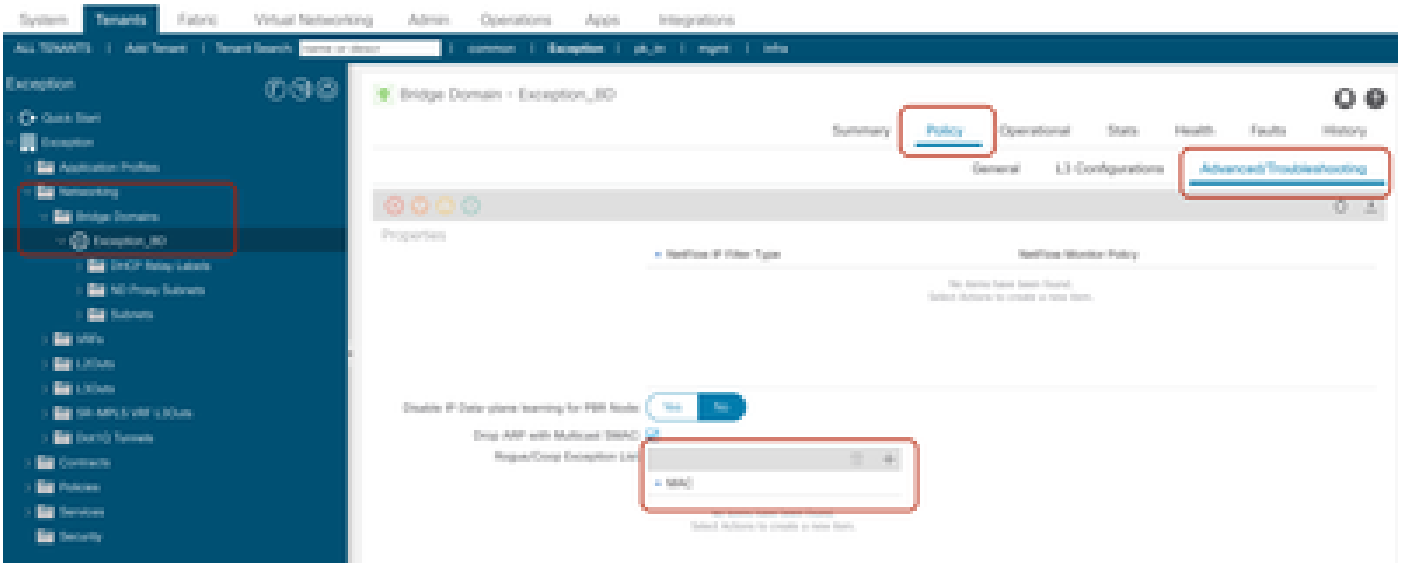
APIC(Application Policy Infrastructure Controller) GUI를 사용한 컨피그레이션

구성하려면

1단계. Cisco APIC GUI에 로그인합니다.

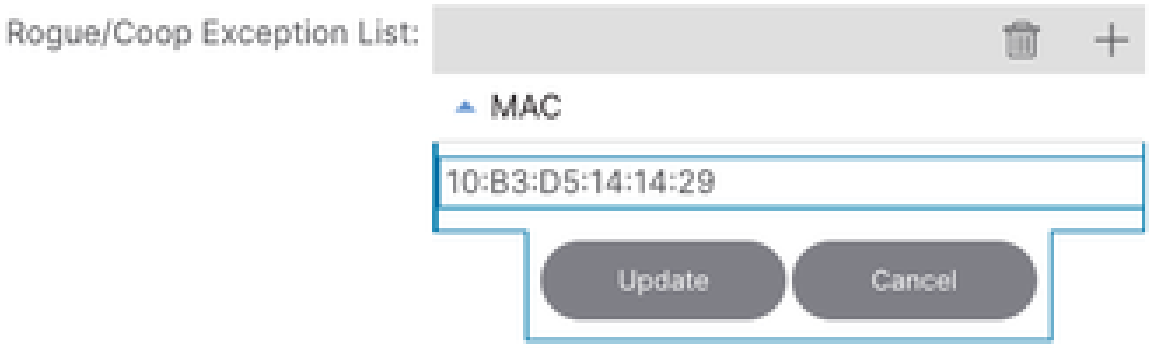
2단계. Tenant(테넌트) > Networking(네트워킹) > Bridge Domains(브리지 도메인) > BD > Policy(정책) > Advanced/Troubleshooting(고급/트러블슈팅) 탭으로 이동합니다.

이 페이지에서 예외 목록에 MAC 주소를 추가할 수 있습니다.



3단계. + 아이콘을 선택하여 비인가/COOP 예외 목록에 MAC 주소를 추가합니다.

4단계. MAC 주소를 추가하고 업데이트합니다.



확인

이 기능을 시연하기 위해 테넌트 예외 및 BD(Bridge Domain) BD-Exception 내의 ACI 패브릭에 연결된 MAC 주소 10:B3:D5:14:14:29의 엔드포인트가 있습니다.

이 문서의 "Configuration of Rogue/COOP Exception List" 섹션에 있는 예외 목록에 MAC 주소를 추가한 후 MO(Managed Object) 쿼리 moquery -c fvRogueExceptionMac을 사용하여 구성을 확인할 수 있습니다.

APIC CLI:

<#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#
```

리프 CLI:

이 moquery는 비인가 예외 목록에 적용된 타이머를 제공합니다.

<#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 :
```

moquery를 사용하면 예외 목록에 특정 mac이 추가되었는지 확인할 수 있습니다.

<#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#
```

Leaf CLI에서 예외 목록 매개변수를 확인하려면

<#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#
```

EPMC에서 학습한 엔드포인트를 확인하고 해당 엔드포인트의 이동 카운트도 확인합니다.

리프 CLI:

<#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#
```

예외 목록 구성을 확인하려면

리프 CLI:

<#root>

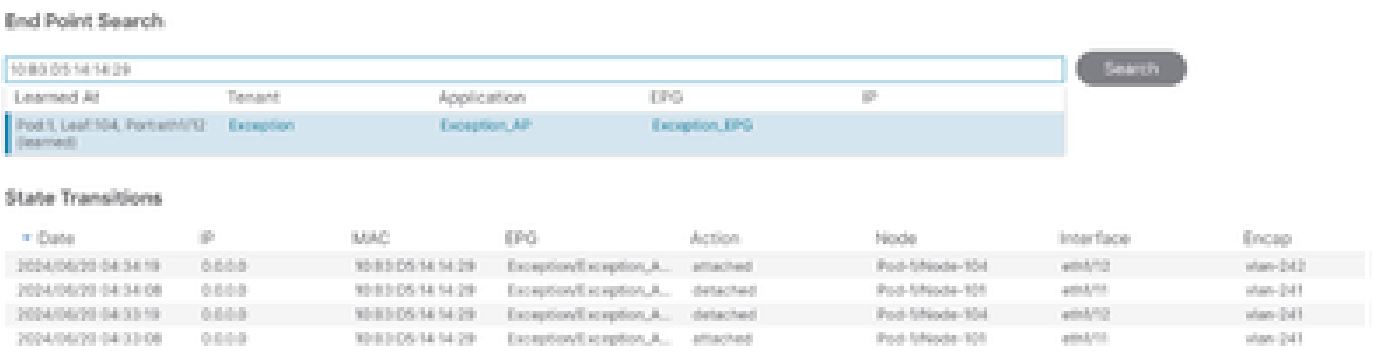
```
module-1#
```

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#
```

APIC GUI의 Operations(운영) > EP tracker(EP 추적기)에서 엔드포인트 이동을 확인할 수 있습니다. 여기서 MAC 주소를 검색합니다.



여전히 이 MAC 주소에 대한 이동이 있지만 현재 이 엔드포인트에 대한 비인가 플래그가 없습니다.

이는 명령으로 확인할 수 있습니다.

리프 CLI:

leaf epm(엔드포인트 관리자)에서 학습된 엔드포인트에 비인가 플래그가 추가되었는지 확인하려면 다음을 수행합니다.

<#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#
```

APIC CLI:

비인가 엔드포인트 엔드포인트에 대해 결함이 제기되었는지 확인합니다.

<#root>

```
bgl-aci04-apic1#

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


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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.