在ACI中配置恶意/COOP例外列表

目录

简介

本文档介绍ACI(以应用为中心的基础设施)中的欺诈/COOP例外列表功能，并介绍配置和验证。

为什么选择例外列表？

ACI中的“恶意EP控制”功能通过将临时环路的影响隔离到发生环路的特定网桥域内，最大程度减少临时环路的影响。但是，此功能有时会导致不必要的中断。例如，在防火墙故障切换期间，两个防火墙都可以使用同一MAC（媒体访问控制）地址暂时传输流量，从而导致网络出现故障直至收敛。在5.2(3)之前，如果ACI在60秒内检测到4个EP（终端）移动，则会将其设置为静态，并且在接下来的30分钟内不允许移动。 在某些部署中，在60秒内执行4次移动可能比较现实。对于预期EP移动的情况，保持时间（30分钟）比较严格。

解决方案

为了解决此问题，可以配置“恶意/COOP例外列表”。 因此，“例外列表”中的MAC地址使用较高的阈值标准来检测“恶意”。在“例外清单”中配置的MAC在10分钟间隔内移动了3000次之后成为非法。例外清单中的MAC地址使用更高的COOP（Oracle协议委员会）阻尼阈值以避免在COOP中受到阻尼。您可以在例外列表中添加最多100个MAC地址。

前提条件

- 此功能从版本5.2(3)开始提供
- 此选项仅在BD（网桥域）是L2 BD时使用（好象没有为IP路由配置BD）
- 必须启用恶意程序功能才能使恶意程序例外列表行为生效。

恶意/COOP例外列表的配置

此功能可在第2层网桥域(L2 BD)中使用，以防止特定MAC地址由于合法移动而被标记为非法。

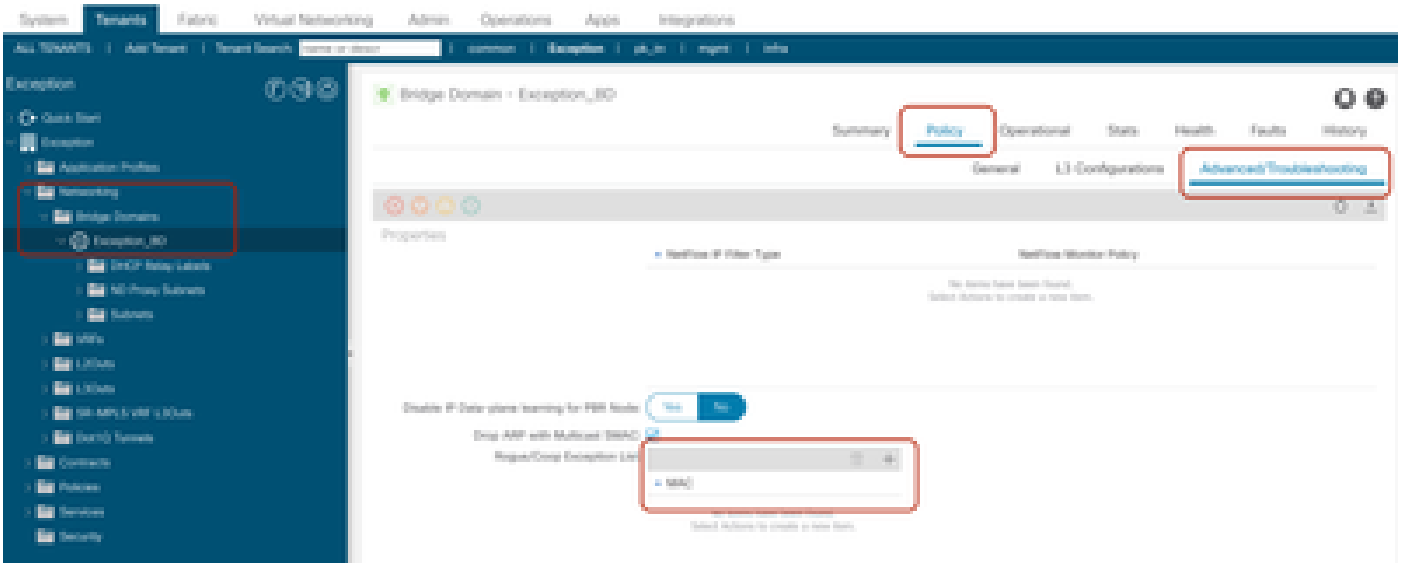
使用APIC（应用策略基础设施控制器）GUI进行配置

配置：

步骤1:登录到思科APIC GUI。

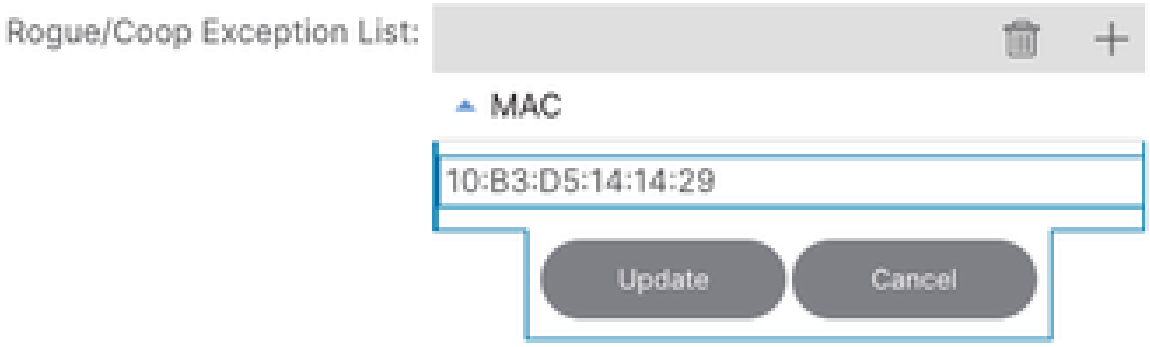
第二步：转至Tenant > Networking > Bridge Domains > BD > Policy > Advanced/Troubleshooting选项卡

在此页上，您可以在例外列表中添加MAC地址。



第三步：选择+图标可将MAC地址添加到恶意/COOP例外列表中。

第四步：添加MAC地址并更新。



确认

为了演示此功能，有一个终端的MAC地址10：B3：D5:14:14:29连接到租户例外和桥接域(BD) BD-例外内的ACI交换矩阵。

在将MAC地址添加到本文档“恶意/COOP异常清单的配置”部分的异常清单后，可以使用托管对象(MO)查询验证配置：moquery -c fvRogueExceptionMac

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#
```

枝叶CLI：

此模式提供应用于恶意例外列表的计时器。

<#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 :
```

使用moquery，您可以验证是否已将任何特定mac添加到“例外”列表中。

<#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#
```

要从枝叶CLI确认例外列表参数，请执行以下操作：

<#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#
```

在EPMC中验证已学习终结点，并检查该终结点的移动计数。

枝叶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#
```

要检查例外列表配置，请执行以下操作：

枝叶CLI：

<#root>

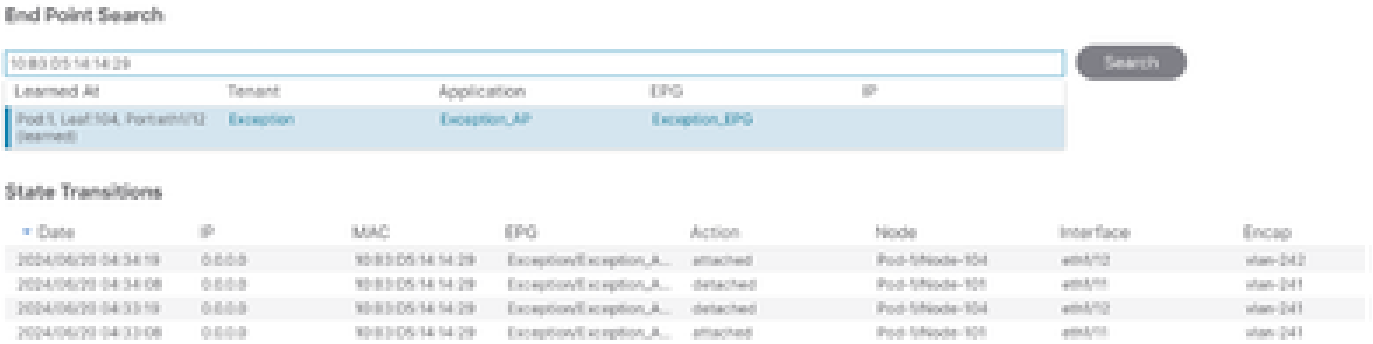
module-1#

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#
```

您可以在APIC GUI中的Operations > EP tracker处检查终端移动，并在此处搜索MAC地址。



由于此MAC地址仍有移动，但此终端现在没有恶意标志。

这可以通过命令来验证。

枝叶CLI：

检查是否向枝叶epm （终端管理器）中获悉的终端添加了恶意标记

<#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：

检查是否对恶意终端终端引发任何故障。

<#root>

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

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

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。