Configura elenco eccezioni Rogue/COOP in ACI

Sommario

Introduzione

In questo documento viene descritta la funzione Rogue/COOP Exception List in ACI (Application Centric Infrastructure) e vengono illustrate la configurazione e la verifica.

Perché l'elenco delle eccezioni?

La funzione "Rogue EP Control" in ACI riduce al minimo l'impatto dei loop temporanei mettendo in quarantena gli endpoint all'interno del dominio bridge specifico in cui si verificano. Tuttavia, questa funzione può talvolta causare interruzioni non necessarie. Ad esempio, durante un failover del firewall, entrambi i firewall possono momentaneamente trasmettere il traffico utilizzando lo stesso indirizzo MAC (Media Access Control), creando problemi fino alla convergenza della rete. Prima della versione 5.2(3) Se l'ACI rileva 4 spostamenti EP (Endpoint) in 60 secondi, l'attività viene resa statica e non può essere spostata per i successivi 30 minuti. In alcune installazioni, 4 mosse in 60 secondi possono essere realistiche. Il tempo di attesa di 30 minuti è aggressivo per gli scenari in cui sono previsti spostamenti di EP.

Soluzione

Per risolvere questo problema, è possibile configurare un "elenco di eccezioni Rogue/COOP". MAC gli indirizzi nell'elenco eccezioni, quindi utilizza criteri di soglia superiori per rilevare i server non autorizzati. L'indirizzo MAC configurato nell'elenco eccezioni viene reso non autorizzato dopo 3000 spostamenti nell'intervallo di 10 minuti.MAC l'indirizzo nell'elenco eccezioni utilizza una soglia di smorzamento COOP (Council of Oracle Protocol) più alta per evitare di essere smorzato in COOP. È possibile aggiungere fino a 100 indirizzi MAC nell'elenco eccezioni.

Prerequisito

- Questa funzionalità è disponibile a partire dalla versione 5.2(3)
- Questa opzione può essere utilizzata solo se BD (Bridge Domain) è un BD L2 (come se BD non fosse configurato per il routing IP)
- Affinché il comportamento dell'elenco di eccezioni non valide funzioni correttamente, è

necessario che la funzionalità non valida sia attivata.

Configurazione dell'elenco di eccezioni Rogue/COOP

Questa funzione può essere utilizzata nei domini bridge di layer 2 (L2 BD) per impedire che determinati indirizzi MAC vengano contrassegnati come anomali a causa di movimenti legittimi.

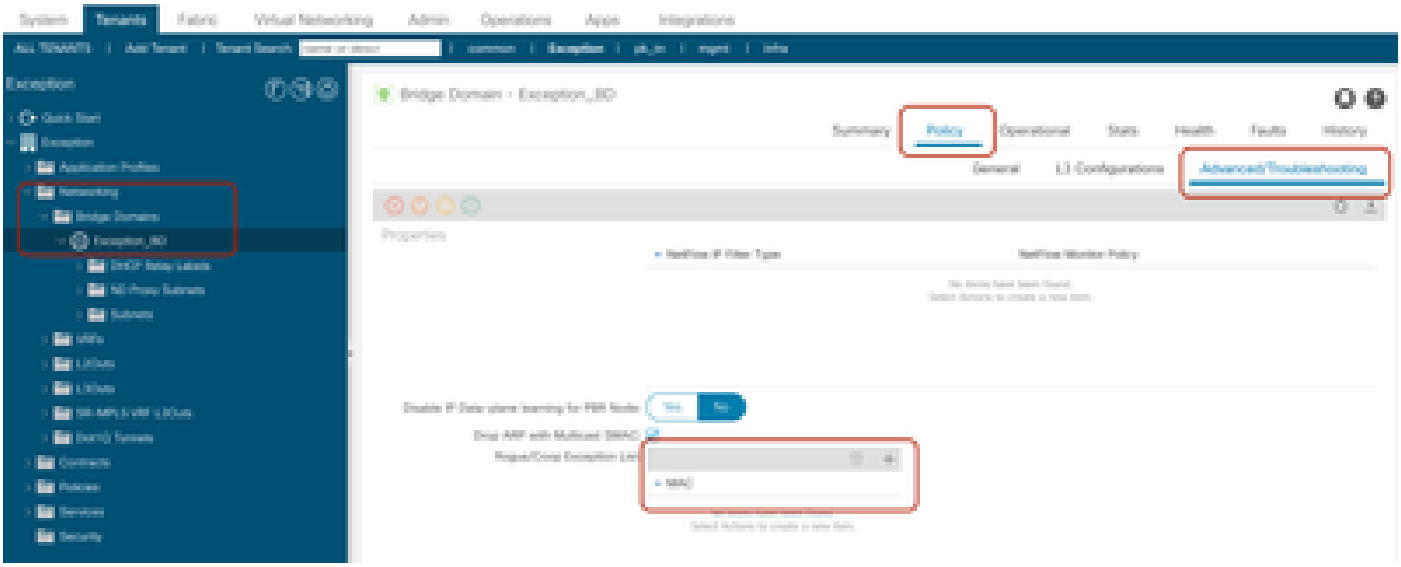
Configurazione utilizzando l'interfaccia grafica APIC (Application Policy Infrastructure Controller)

Per configurare:

Passaggio 1. Accedere alla GUI di Cisco APIC.

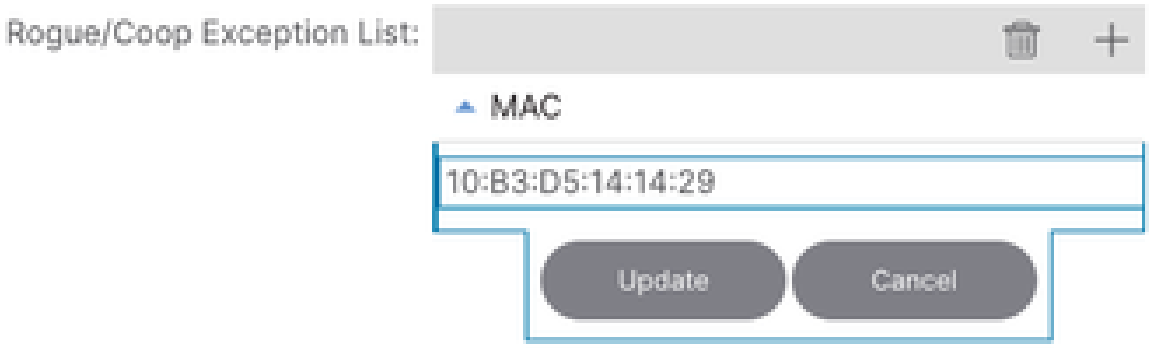
Passaggio 2. Selezionare Tenant > Networking > Bridge Domains > BD > Policy > Advanced/Troubleshooting

In questa pagina è possibile aggiungere indirizzi MAC nell'elenco Eccezioni.



Passaggio 3. Selezionare + icona per aggiungere l'indirizzo MAC nell'elenco delle eccezioni Rogue/COOP.

Passaggio 4. Aggiungere indirizzo MAC e aggiornamento.



Verifica

Per dimostrare questa funzionalità, c'è un endpoint con indirizzo MAC 10:B3:D5:14:14:29 connesso alla struttura ACI all'interno di BD-Exception Tenant Exception e Bridge Domain (BD).

Dopo aver aggiunto l'indirizzo MAC all'elenco eccezioni nella sezione "Configuration of Rogue/COOP Exception List" di questo documento, è possibile verificare la configurazione utilizzando la query MO (Managed Object): moquery -c fvRogueExceptionMac

CLI 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 foglia:

Questa moquery fornisce i timer applicati all'elenco di eccezioni non valide.

<#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 è possibile verificare che un determinato mac venga aggiunto nell'elenco delle eccezioni.

<#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#
```

Per confermare i parametri dell'elenco eccezioni dalla CLI foglia:

<#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#
```

Per verificare l'endpoint individuato in EPMC e controllare anche il conteggio degli spostamenti per l'endpoint.

CLI foglia:

<#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#
```

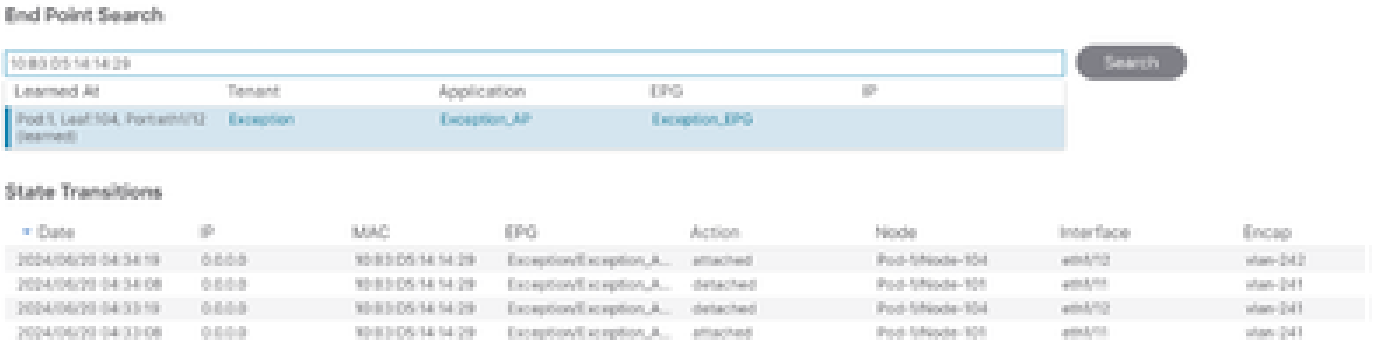
Per controllare la configurazione dell'elenco eccezioni:

CLI foglia:

<#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#
```

È possibile controllare gli spostamenti dell'endpoint nella GUI di APIC in Operations > EP tracker, Search MAC address here.



Poiché sono ancora presenti movimenti per questo indirizzo MAC, non è disponibile alcun flag Rogue per questo endpoint.

È possibile verificare questa condizione tramite i comandi.

CLI FOGLIA:

Per verificare se il flag rogue è stato aggiunto all'endpoint appreso nell'epm foglia (gestione endpoint)

<#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 APIC:

Per verificare se viene generato un errore per l'endpoint non autorizzato.

<#root>

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

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

```
No Mos found
```

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).