

Risoluzione dei problemi relativi ai criteri di sicurezza ACI - Contratti

Sommario

[Introduzione](#)

[Premesse](#)

[Panoramica](#)

[Metodi per programmare le regole di zoning](#)

[Confronto tra le metodologie delle regole di zoning](#)

[Lettura di una voce della regola di suddivisione in zone](#)

[CAM \(Policy Content-Addressable Memory\)](#)

[Perdita di VRF, pcTag globali e direzionalità di applicazione delle policy degli output L3 condivisi](#)

[Direzione applicazione controllo criteri VRF](#)

[Dove viene applicata la politica?](#)

[Applicazione in ingresso e in uscita](#)

[Strumenti](#)

[Convalida della regola di zoning](#)

['show zoning-rules'](#)

['show zoning-filter'](#)

['show system internal policy-mgr stats'](#)

['show logging ip access-list internal packet-log deny'](#)

[parser contratto](#)

[Convalida classificazione pacchetti](#)

[ELAM](#)

[Triage](#)

[App ELAM Assistant](#)

[Utilizzo CAM criteri](#)

[Vista 'Capacità foglia' del pannello di controllo Capacità](#)

['show platform internal hal health-stats'](#)

[da EPG a EPG](#)

[Considerazioni generiche sull'eliminazione dei criteri](#)

[Metodologia](#)

[Esempio di risoluzione dei problemi da EPG a EPG](#)

[Topologia](#)

[Identificare gli switch foglia di origine e destinazione coinvolti nel rilascio del pacchetto](#)

[Visibilità e risoluzione dei problemi](#)

[Configurazione di visibilità e risoluzione dei problemi](#)

[Identificazione rilascio](#)

[Elimina dettagli](#)

[Dettagli contratto](#)

[Visualizzazione contratto](#)

[ID risorsa tenant per trovare il tag e l'ambito del pcTag EPG](#)

[Verificare i criteri applicati al flusso di traffico in fase di risoluzione dei problemi](#)

[iBash](#)

[Acquisizione ELAM](#)

[ELAM Assistant:](#)

[Configurazione](#)

[Report Elam Assistant Express](#)

[Report Elam Assistant Express \(continua\)](#)

[Gruppo preferito](#)

[Informazioni sui gruppi di opzioni di contratto](#)

[Programmazione gruppo privilegiato contratto](#)

[Scenario di risoluzione dei problemi del gruppo preferito](#)

[Topologia](#)

[Flusso di lavoro](#)

[da vzAny a EPG](#)

[Informazioni su vzAny](#)

[Esempio di caso di utilizzo](#)

[Scenario di risoluzione dei problemi - Il traffico diminuisce se non è presente alcun contratto](#)

[Flusso di lavoro](#)

[Regole di zoning che consentono il traffico da/verso EPG NTP da altri EPG presenti nel VRF](#)

[L3Out condiviso in EPG](#)

[Informazioni su L3Out condiviso](#)

[Risoluzione dei problemi relativi a un'unità L3out condivisa](#)

[Flusso di lavoro](#)

Introduzione

In questo documento viene descritto come comprendere e risolvere i problemi relativi ai criteri di sicurezza ACI, noti come contratti.

Premesse

Il materiale di questo documento è stato estratto dal libro Troubleshooting Cisco Application Centric Infrastructure, Second Edition (Risoluzione dei problemi di Infrastruttura incentrata sulle applicazioni Cisco, Seconda edizione), in particolare i **capitoli** Security Policies - Overview, Security Policies - Tools, **Security Policies - EPG to EPG**, Security Policies - Preferred group e **Security Policies - vzAny to EPG** .

Panoramica

L'architettura di sicurezza fondamentale della soluzione ACI è basata su un modello di elenco di autorizzazioni. A meno che un VRF non sia configurato in modalità **non imposta**, tutti i flussi di traffico da EPG a EPG vengono eliminati in modo implicito. Come suggerisce il modello predefinito di elenco di autorizzazioni, l'impostazione predefinita di VRF è in modalità **imposizione**. I flussi di traffico possono essere autorizzati o negati esplicitamente implementando le regole di zoning sui nodi dello switch. Queste regole di zoning possono essere programmate in una varietà di configurazioni diverse a seconda del flusso di comunicazione desiderato tra gruppi di endpoint

(EPG) e il metodo utilizzato per definirli. Si noti che le voci delle regole di zoning non sono con conservazione dello stato e in genere consentono o negano l'accesso in base alla porta o al socket fornito da due EPG una volta che la regola è stata programmata.

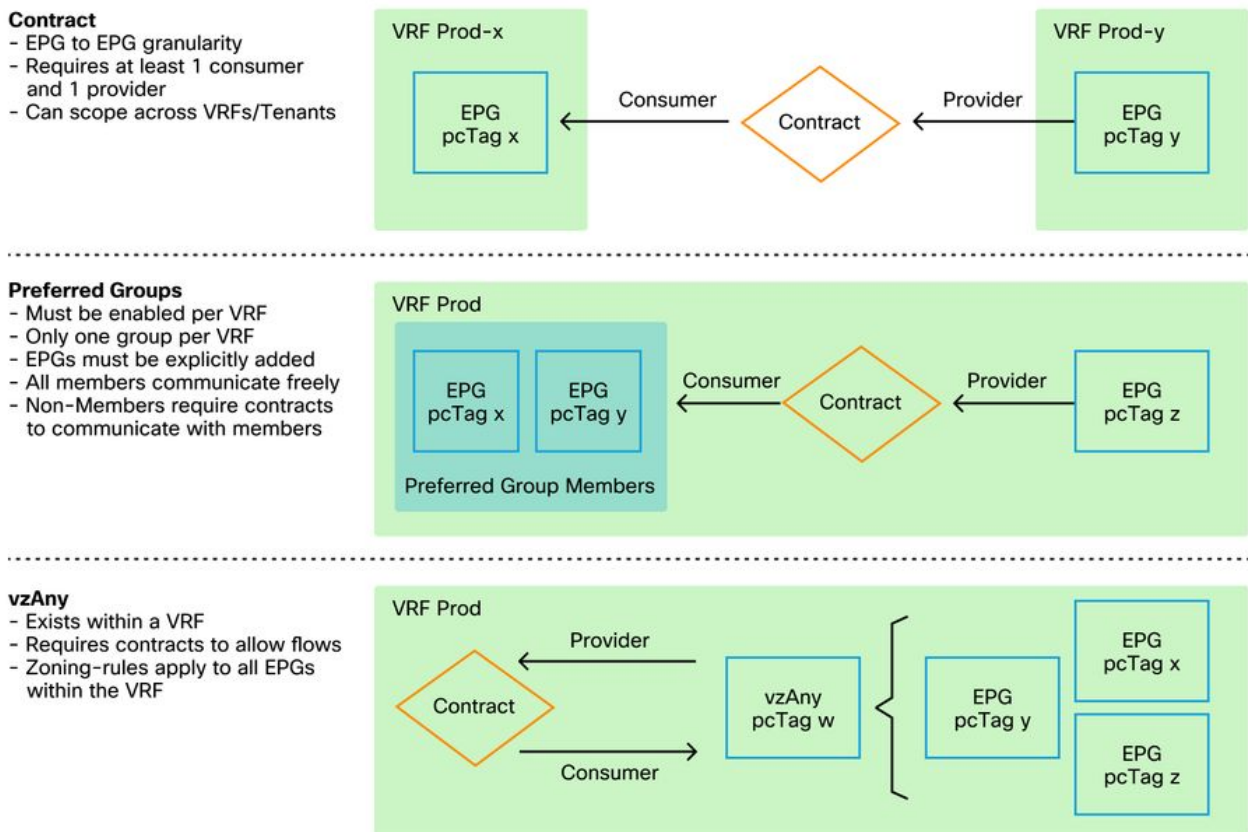
Metodi per programmare le regole di zoning

I metodi principali per programmare le regole di zoning all'interno di ACI sono i seguenti:

- **Contratti da EPG a EPG:** in genere sono necessari almeno un consumatore e un fornitore per programmare le regole di zoning in due o più gruppi di endpoint distinti.
- **Gruppi preferiti:** richiede l'abilitazione del raggruppamento a livello VRF; può esistere un solo gruppo per ogni VRF. Tutti i membri del gruppo possono comunicare liberamente. I non membri richiedono contratti per consentire i flussi al gruppo preferito.
- **vzAny:** una 'raccolta EPG' definita in un determinato VRF. vzAny rappresenta tutti gli EPG nel VRF. L'uso di vzAny consente i flussi tra un EPG e tutti gli EPG all'interno del VRF tramite una connessione contrattuale.

Il diagramma seguente può essere utilizzato per fare riferimento alla granularità della regola di zoning che ciascuno dei metodi sopra descritti consente di controllare:

Confronto tra le metodologie delle regole di zoning



Utilizzando il metodo del contratto di programmazione delle regole di zoning, c'è un'opzione per definire l'ambito del contratto. Questa opzione deve essere considerata con attenzione se è necessaria una perdita di percorso/progettazione del servizio condiviso. Se il desiderio è quello di passare da un VRF all'altro all'interno del fabric ACI, i contratti sono il metodo per farlo.

I valori di ambito possono essere i seguenti:

- **Applicazione:** una relazione tra consumatore/fornitore su contratto consente di programmare solo le regole tra EPG definite all'interno dello stesso profilo applicazione. Il riutilizzo dello stesso contratto in altri EPG di profili di applicazioni non consentirà di intercorrere tra di essi.
- **VRF (predefinito):** una relazione tra il consumatore e il fornitore del contratto programmerà le regole tra gli EPG definiti all'interno dello stesso VRF. Il riutilizzo dello stesso contratto in altri EPG di profili di applicazioni consentirà di interagire tra loro. Accertatevi che siano consentiti solo i flussi desiderati, altrimenti si dovrebbe definire un nuovo contratto per evitare l'incrocio involontario.
- **Tenant:** una relazione contrattuale tra consumatore/fornitore programmerà regole tra EPG definiti all'interno dello stesso tenant. Se esistono EPG legati a più VRF all'interno di un singolo tenant e utilizzano/forniscono lo stesso contratto, questo ambito può essere utilizzato per indurre la perdita di route per consentire la comunicazione tra VRF.
- **Globale:** un rapporto contrattuale tra cliente/fornitore programmerà regole tra EPG su qualsiasi tenant all'interno di un fabric ACI. Si tratta del campo di applicazione più ampio possibile della definizione e occorre prestare particolare attenzione quando ciò è consentito in contratti precedentemente definiti, in modo da evitare fuoriuscite involontarie di flusso.

Lettura di una voce della regola di suddivisione in zone

Una volta programmata, la regola di zoning verrà visualizzata come segue su una foglia:

```
+-----+-----+-----+-----+-----+-----+-----+-----+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name |
Action | Priority |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
```

- **ID regola:** l'ID della voce della regola. Nessun significato reale se non quello di agire come un identificatore unico.
- **EPG origine:** un ID univoco per VRF (pcTag) del gruppo di endpoint di origine.
- **EPG destinazione:** un ID univoco per VRF (pcTag) del gruppo di endpoint di destinazione.
- **FilterID:** l'ID del filtro a cui la regola sta tentando di trovare una corrispondenza. Il filtro contiene le informazioni sul protocollo a cui la regola corrisponderà.
- **Dir:** la direzionalità della regola di zoning.
- **OperSt:** lo stato operativo della regola.
- **Ambito:** ID univoco del VRF a cui la regola corrisponderà.
- **Nome:** il nome del contratto che ha determinato la programmazione di tale voce.
- **Azione:** operazione eseguita dalla foglia quando corrisponde alla voce. Include: [Elimina, Autorizza, Registra, Reindirizza].
- **Priorità:** l'ordine in cui le regole di zoning verranno convalidate per l'azione in base alle voci Scope, SrcEPG, DstEPG e Filter corrispondenti.

CAM (Policy Content-Addressable Memory)

Durante la programmazione di ciascuna regola di zoning, una matrice della voce della regola di zoning mappata rispetto alle voci di filtro inizierà a utilizzare **Policy CAM** sugli switch. Durante la progettazione dei flussi consentiti attraverso un fabric ACI, è necessario prestare particolare

attenzione quando si riutilizzano i contratti, anziché crearne di nuovi, a seconda della progettazione finale. Il riutilizzo casuale dello stesso contratto in più EPG senza comprendere le regole di zoning che ne derivano può rapidamente comportare l'autorizzazione inattesa di più flussi. Allo stesso tempo, questi flussi non intenzionali continueranno a consumare il CAM politico. Quando Policy CAM diventa pieno, la programmazione delle regole di zoning inizierà a fallire, il che può comportare una perdita imprevista e intermittente a seconda dei comportamenti di configurazione e degli endpoint.

Perdita di VRF, pcTag globali e direzionalità di applicazione delle policy degli output L3 condivisi

Callout speciale per lo Use Case dei servizi condivisi che richiede la configurazione dei contratti. I servizi condivisi implicano in genere traffico inter-VRF all'interno di una struttura ACI che si basa sull'utilizzo di un contratto con ambito "tenant" o "globale". Per comprendere a fondo questo concetto, è necessario innanzitutto ribadire che il valore pcTag tipico assegnato agli EPG non è globalmente univoco. I tag pc hanno un ambito VRF e lo stesso tag pc potrebbe essere riutilizzato all'interno di un altro VRF. Quando si parla di perdite di percorso, iniziare a far rispettare i requisiti sulla struttura ACI, inclusa la necessità di valori univoci a livello globale, tra cui subnet e pcTags.

Ciò che rende questa considerazione speciale è l'aspetto direzionale legato al fatto che un EPG è un consumatore contro un fornitore. In uno scenario con servizi condivisi, il provider in genere deve guidare un pcTag globale per ottenere un valore univoco dell'infrastruttura. Allo stesso tempo, il consumatore conserva il suo pcTag con ambito VRF che lo mette in una posizione speciale per essere in grado di programmare e comprendere l'uso del valore pcTag globale per applicare la policy.

Per riferimento, l'intervallo di allocazione pcTag è il seguente:

- Riservato al sistema: 1-15 .
- Ambito globale: 16-16384 per gli EPG dei provider di servizi condivisi.
- Ambito locale: 16385-65535 per EPG con ambito VRF.

Direzione applicazione controllo criteri VRF

In ogni VRF è possibile definire l'impostazione della direzione di imposizione.

- L'impostazione predefinita della direzione di imposizione è In entrata.
- L'altra opzione per la direzione dell'applicazione è Egregio.

La comprensione della posizione in cui viene applicato il criterio dipende da diverse variabili.

La tabella riportata di seguito consente di capire dove vengono applicati i criteri di sicurezza a livello foglia.

Dove viene applicata la politica?

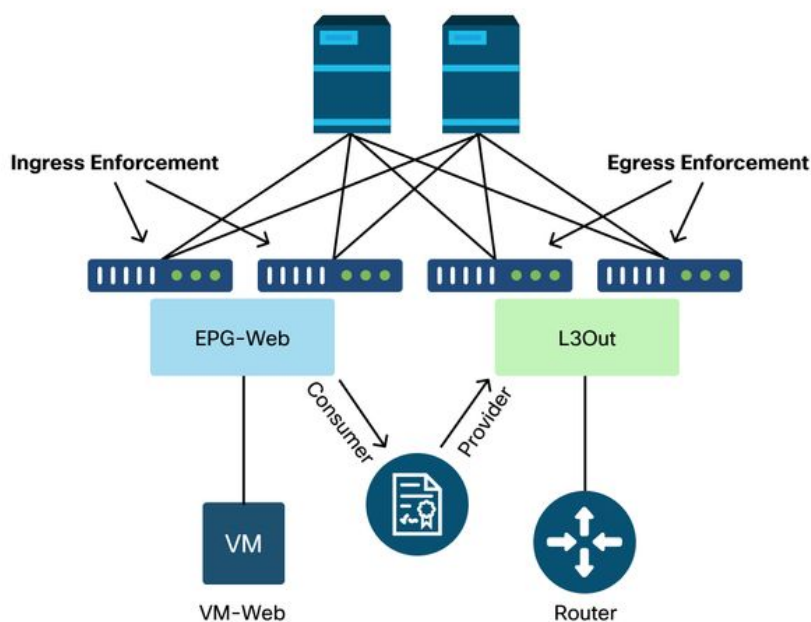
Scenario	Modalità di imposizione VRF	Consumer	Provider	Criterio applicato il
Intra-VRF	In entrata/in uscita	EPG	EPG	<ul style="list-style-type: none"> ·Se si apprende l'endpoint di destinazione: foglia in entrata* ·Se non si apprende l'endpoint di destinazione: foglia di uscita

In ingresso	EPG	EPG L3Out	Foglia di consumo (foglia non transfrontaliera)	
In ingresso	EPG L3Out	EPG	Foglia fornitore (foglia non transfrontaliera)	
In uscita	EPG	EPG L3Out	Foglia di confine -> traffico foglia non di confine ·Se si apprende l'endpoint di destinazione: foglia di bordo ·Se non si apprende l'endpoint di destinazione: foglia non frontiera	
In uscita	EPG L3Out	EPG	Traffico foglia -> frontiera ·Foglia	
In entrata/in uscita	EPG L3Out	EPG L3Out	Foglia in ingresso*	
In entrata/in uscita	EPG	EPG	Foglia	
In entrata/in uscita	EPG	EPG L3Out	Foglia di consumo (Foglia esterna)	
Inter-VRF	In entrata/in uscita	EPG L3Out	EPG	Foglia in ingresso*
In entrata/in uscita	EPG L3Out	EPG L3Out	Foglia in ingresso*	

*L'applicazione della policy viene applicata alla prima foglia colpita dal pacchetto.

La figura seguente mostra un esempio di applicazione del contratto in cui EPG-Web come consumatore e L3Out EPG come fornitore hanno un contratto intra-VRF. Se VRF è impostato sulla modalità di imposizione in ingresso, i criteri vengono applicati dai nodi foglia in cui risiede EPG-Web. Se VRF è impostato sulla modalità di imposizione uscita, i criteri vengono applicati dai nodi foglia del bordo in cui risiede L3Out se l'endpoint VM-Web viene appreso nell'elemento foglia del bordo.

Applicazione in ingresso e in uscita



Strumenti

Sono disponibili diversi strumenti e comandi che possono essere utilizzati per identificare una perdita di criteri. Una perdita di criteri può essere definita come perdita di pacchetti a causa di una configurazione del contratto o per mancanza di tale configurazione.

Convalida della regola di zoning

Gli strumenti e i comandi seguenti possono essere utilizzati per convalidare esplicitamente le regole di zoning programmate sugli switch foglia in seguito al completamento delle relazioni tra i fornitori e i consumatori.

'show zoning-rules'

Un comando a livello di switch che mostra tutte le regole di zoning in uso.

```
leaf# show zoning-rule
-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name |
| Action | Priority | | | | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
| 4156 | 25 | 16410 | 425 | uni-dir-ignore | enabled | 2818048 | external_to_ntp |
| permit | fully_qual(7) | | | | | | |
| 4131 | 16410 | 25 | 424 | bi-dir | enabled | 2818048 | external_to_ntp |
| permit | fully_qual(7) | | | | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
```

'show zoning-filter'

Filtro che contiene le informazioni sport/porta su cui agisce la regola di zoning. La programmazione del filtro può essere verificata con questo comando.

```
leaf# show zoning-filter
-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
| FilterId | Name | EtherT | Prot | ApplyToFrag | Stateful | SFromPort |
| SToPort | DFromPort | DToPort | Prio | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
| implarp | implarp | arp | unspecified | no | no | unspecified |
| unspecified | unspecified | unspecified | dport | | | |
| implicit | implicit | unspecified | unspecified | no | no | unspecified |
| unspecified | unspecified | unspecified | implicit | | | |
| 425 | 425_0 | ip | tcp | no | no | 123 |
| 123 | unspecified | unspecified | sport | | | |
| 424 | 424_0 | ip | tcp | no | no | unspecified |
| unspecified | 123 | 123 | dport | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
```

'show system internal policy-mgr stats'

Questo comando può essere eseguito per verificare il numero di accessi per regola di zoning. Questa opzione consente di determinare se una regola prevista viene trovata in contrapposizione a un'altra, ad esempio una regola di eliminazione implicita che potrebbe avere una priorità più alta.

```
leaf# show system internal policy-mgr stats
```

```
Requested Rule Statistics
```

```
Rule (4131) DN (sys/actrl/scope-2818048/rule-2818048-s-16410-d-25-f-424) Ingress: 0, Egress: 0, Pkts: 0 RevPkts: 0
```

```
Rule (4156) DN (sys/actrl/scope-2818048/rule-2818048-s-25-d-16410-f-425) Ingress: 0, Egress: 0, Pkts: 0 RevPkts: 0
```

'show logging ip access-list internal packet-log deny'

Comando a livello di switch che può essere eseguito a livello di iBash e che segnala le interruzioni relative agli ACL (contratto) e le informazioni relative al flusso, tra cui:

- VRF
- VLAN-ID
- MAC di origine/MAC di destinazione
- IP origine/IP destinazione
- Porta origine/Porta destinazione
- Interfaccia di origine

```
leaf# show logging ip access-list internal packet-log deny
```

```
[ Tue Oct 1 10:34:37 2019 377572 usecs]: CName: Prod1:VRF1(VXLAN: 2654209), VlanType: Unknown, Vlan-Id: 0, SMac: 0x000c0c0c0c0c, DMac:0x000c0c0c0c0c, SIP: 192.168.21.11, DIP: 192.168.22.11, SPort: 0, DPort: 0, Src Intf: Tunnel7, Proto: 1, PktLen: 98
```

```
[ Tue Oct 1 10:34:36 2019 377731 usecs]: CName: Prod1:VRF1(VXLAN: 2654209), VlanType: Unknown, Vlan-Id: 0, SMac: 0x000c0c0c0c0c, DMac:0x000c0c0c0c0c, SIP: 192.168.21.11, DIP: 192.168.22.11, SPort: 0, DPort: 0, Src Intf: Tunnel7, Proto: 1, PktLen: 98
```

parser_contratto

Script Python su dispositivo che produce un output che mette in correlazione le regole di zoning, i filtri e le statistiche di accesso durante l'esecuzione di ricerche di nomi da ID. Questo script è estremamente utile in quanto prende un processo a più fasi e lo trasforma in un singolo comando che può essere filtrato per EPG/VRF specifici o su altri valori correlati al contratto.

```
leaf# contract_parser.py
```

```
Key:
```

```
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]  
[flags][contract:{str}] [hit=count]
```

```
[7:4131] [vrf:common:default] permit ip tcp tn-Prod1/ap-Services/epg-NTP(16410) tn-Prod1/l3out-L3Out1/instP-extEpg(25) eq 123 [contract:uni/tn-Prod1/brc-external_to_ntp] [hit=0]
```

```
[7:4156] [vrf:common:default] permit ip tcp tn-Prod1/l3out-L3Out1/instP-extEpg(25) eq 123 tn-Prod1/ap-Services/epg-NTP(16410) [contract:uni/tn-Prod1/brc-external_to_ntp] [hit=0]
```

```
[12:4169] [vrf:common:default] deny,log any tn-Prod1/l3out-L3Out1/instP-extEpg(25) epg:any [contract:implicit] [hit=0]
```

```
[16:4167] [vrf:common:default] permit any epg:any tn-Prod1/bd-Services(32789) [contract:implicit] [hit=0]
```

Convalida classificazione pacchetti

ELAM

Report a livello ASIC utilizzato per controllare i dettagli di inoltro che indica, nel caso di un pacchetto scartato, il motivo del rilascio. In relazione a questa sezione, il motivo può essere un SECURITY_GROUP_DENY (perdita dei criteri di contratto).

Triage

Utility basata su Python sull'APIC in grado di tenere traccia del flusso di pacchetti end-to-end con ELAM.

App ELAM Assistant

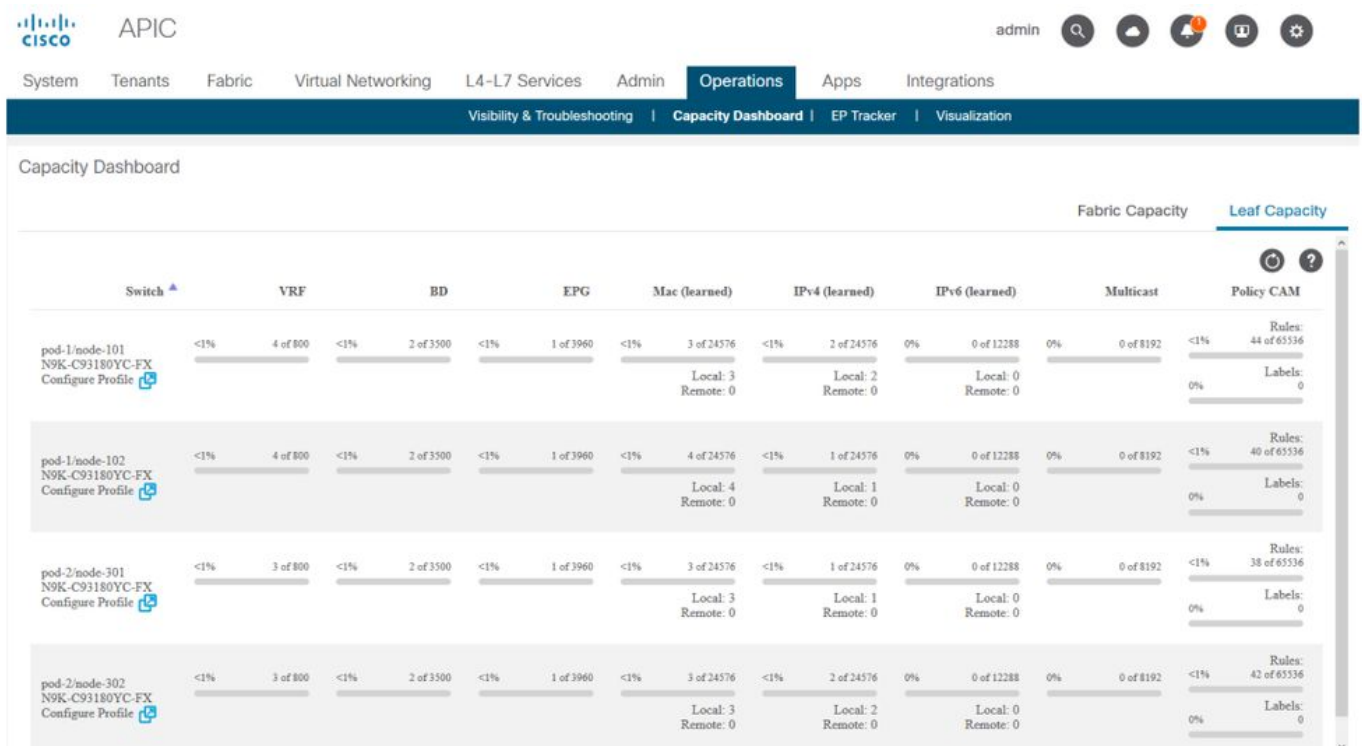
Un'app APIC che astrae la complessità dei vari ASIC per rendere l'ispezione delle decisioni di inoltro molto più comoda e facile da usare.

Fare riferimento alla sezione "Inoltro intra-fabric" per ulteriori dettagli sugli strumenti ELAM, fTriage e ELAM Assistant

Utilizzo CAM criteri

L'utilizzo della CAM delle policy per ogni foglia è un parametro importante da monitorare per garantire che il fabric sia in uno stato integro. Il modo più rapido per eseguire il monitoraggio consiste nell'utilizzare il 'Dashboard capacità' all'interno della GUI e controllare in modo esplicito la colonna 'Policy Cam'.

Vista 'Capacità foglia' del pannello di controllo Capacità



'show platform internal hal health-stats'

Questo comando è utile per convalidare diversi limiti di risorse e utilizzo, incluso il CAM criteri. Notare che questo comando può essere eseguito solo in vsh_lc, quindi passarlo utilizzando il flag

'-c' se eseguito da iBash.

```
leaf8# vsh_lc -c "show platform internal hal health-stats"
|Sandbox_ID: 0  Asic Bitmap: 0x0
|-----
...
Policy stats:
=====
policy_count           : 96
max_policy_count      : 65536
policy_otcam_count     : 175
max_policy_otcam_count : 8192
policy_label_count     : 0
max_policy_label_count : 0
=====
```

da EPG a EPG

Considerazioni generiche sull'eliminazione dei criteri

Esistono diversi modi per risolvere i problemi di connettività tra due endpoint. La seguente metodologia costituisce un buon punto di partenza per isolare in modo rapido ed efficace se il problema di connettività è il risultato di una **perdita di policy** (indotta dal contratto).

Ecco alcune domande di alto livello che vale la pena porre prima di immergersi:

- Gli endpoint sono nello stesso EPG o in un EPG diverso? Il traffico tra due endpoint che risiedono in EPG (inter-EPG) diversi viene negato implicitamente e richiede un contratto per consentire la comunicazione. Il traffico tra due endpoint all'interno dello stesso EPG (intra-EPG) è consentito implicitamente, a meno che non sia in uso l'isolamento intra-EPG.
- Il VRF viene applicato o non applicato? Quando un VRF è in modalità **forzata**, all'interno del VRF sono necessari contratti per la comunicazione tra gli endpoint di due diversi EPG. Quando un VRF è in modalità **non applicata**, all'interno del VRF tutto il traffico viene autorizzato dalla struttura ACI su più EPG appartenenti al VRF non applicato, indipendentemente dai contratti ACI applicati.

Metodologia

Con i vari strumenti disponibili, alcuni sono più adatti e comodi da iniziare rispetto ad altri, a seconda del livello di informazioni già noto sul flusso interessato.

Il percorso completo del pacchetto nel fabric ACI è noto (foglia in entrata, foglia in uscita...)?

- Se la risposta è sì, ELAM Assistant deve essere utilizzato per identificare il motivo della perdita sullo switch di origine o di destinazione.
- Se la risposta è no, i comandi Visibility & Troubleshooting, fTriage, contract_parser, Operational nella visualizzazione Tenant e iBash consentono di restringere il percorso del pacchetto o di dare maggiore visibilità ai motivi del rilascio.

Lo strumento fTriage non verrà descritto in dettaglio in questa sezione. Per ulteriori informazioni sull'uso di questo strumento, fare riferimento al capitolo "Inoltre intra-fabric".

Considerare che, mentre Visibility & Troubleshooting può aiutare a visualizzare rapidamente dove i pacchetti vengono scartati tra due endpoint, fTriage mostra informazioni più dettagliate per un'ulteriore risoluzione dei problemi. ovvero fTriage consente di identificare l'interfaccia, il motivo della perdita e altri dettagli di basso livello sul flusso interessato

In questo scenario di esempio viene illustrato come risolvere i problemi relativi a un rilascio di criteri tra due endpoint: 192.168.21.11 e 192.168.23.11

Supponendo che si verifichino perdite di pacchetti tra questi due endpoint, per identificare la causa principale del problema verrà utilizzato il flusso di lavoro di risoluzione dei problemi seguente:

Identificare le foglie src/dst coinvolte nel flusso del traffico:

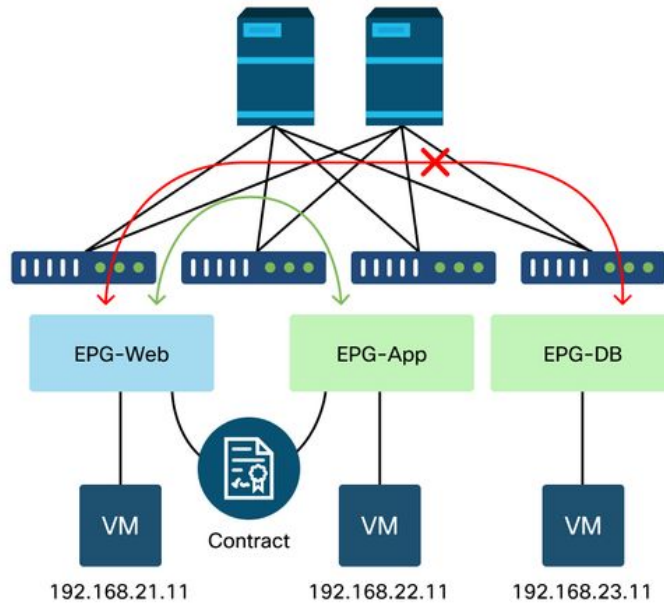
1. Usare **Visibility & Troubleshooting** per tracciare il flusso del pacchetto e identificare il dispositivo che lo sta scartando.
2. Eseguire il comando 'show logging ip access-list internal packet-log deny' sul dispositivo selezionato. Se un pacchetto con uno degli indirizzi IP di interesse viene rifiutato e registrato, il **log** dei **pacchetti** stamperà l'endpoint e il nome del contratto pertinenti in base alle singole risposte.
3. Utilizzare il comando 'contract_parser.py --vrf <tenant>:<VRF>' nella foglia di origine e di destinazione per osservare il numero di riscontri per il contratto configurato: Se un pacchetto supera il contratto sullo switch di origine o di destinazione, il contatore del contratto pertinente aumenterà. Questo metodo è meno granulare di quello del packet-log interno dell'elenco degli accessi IP in situazioni in cui molti flussi potrebbero raggiungere la stessa regola (molti endpoint/flussi tra i due EPG di interesse).

I passaggi di cui sopra sono descritti più avanti nel paragrafo successivo.

Esempio di risoluzione dei problemi da EPG a EPG

In questo scenario di esempio viene illustrato come risolvere i problemi relativi a un rilascio di criteri tra due endpoint: 192.168.21.11 in EPG-Web e 192.168.23.11 in EPG-DB.

Topologia



Identificare gli switch foglia di origine e destinazione coinvolti nel rilascio del pacchetto

Visibilità e risoluzione dei problemi

Lo strumento Visibility & Troubleshooting consente di visualizzare lo switch in cui si è verificata la perdita di pacchetti per un flusso da EP a EP specifico e di identificare la possibile perdita di pacchetti.

Configurazione di visibilità e risoluzione dei problemi

The screenshot shows the Cisco APIC Operations page. The 'Visibility & Troubleshooting' section is active. It includes a session configuration form and two tables for source and destination endpoints.

Session Configuration:

- Session Name: j12
- Session Type: Endpoint to Endpoint
- Description: (empty)

Targets:

Source:

Learned At	Tenant	Application	EPG
Pod:1, Leaf:105, Port:eth1/19	Prod1	AppProf	Web

Destination:

Learned At	Tenant	Application	EPG
Pod:1, Leaf:105, Port:eth1/19	Prod1	AppProf	DB

Configurare un nome di sessione, un'origine e un endpoint di destinazione. Quindi fare clic su 'Invia' o 'Genera report'.

Lo strumento troverà automaticamente gli endpoint nella struttura e fornirà informazioni sul tenant, il profilo dell'applicazione e l'EPG a cui appartengono gli EP.

In questo caso, si scoprirà che gli EP appartengono al tenant Prod1, appartengono allo stesso Profilo applicazione 'AppProf' e sono assegnati a diversi EPG: 'Web' e 'DB'.

Identificazione rilascio

The screenshot shows the Cisco APIC interface. At the top, there are navigation tabs: System, Tenants, Fabric, Virtual Networking, L4-L7 Services, Admin, Operations (selected), Apps, and Integrations. Below these are sub-tabs: Visibility & Troubleshooting (selected), Capacity Dashboard, EP Tracker, and Visualization. The main content area is titled 'Visibility & Troubleshooting' and shows a network diagram. On the left, there is a sidebar with various tools: Faults, Drop/Stats (selected), Contracts, Events and Audits, Traceroute, Atomic Counter, Time Window (set to 'latest 240 minutes' to 'now'), and Session Information (set to 'Endpoint -> Endpoint'). The network diagram shows a 'Leaf fab3-leaf5 (pod-1/node-105)' switch with interfaces 'eth1/49' and 'eth1/19'. A 'Source Endpoint' is shown with IP: 192.168.21.11 and MAC: F6:F2:6C:4E:C8:D0. A 'Spine fab3-p1-spine1 (pod-1/node-201)' switch is also visible with interface 'eth1/13'. A yellow warning icon is present on the leaf switch.

Lo strumento visualizzerà automaticamente la topologia dello scenario di risoluzione dei problemi. In questo caso, i due endpoint sono collegati allo stesso switch foglia.

Passando al sottomenu Rilascia/Statistiche, l'utente può visualizzare le gocce generali sulla foglia o sul dorso in questione. Fare riferimento alla sezione "Interface Drops" nel capitolo "Intra-Fabric Forwarding" di questo libro per ulteriori informazioni su come capire quali drop sono rilevanti.

Molte di queste gocce sono comportamenti attesi e possono essere ignorate.

Elimina dettagli

Statistics - fab3-leaf5

		Drop Stats	Contract Drops	Traffic Stats
<input type="checkbox"/> Show stats with zero values				
Time	Affected Object	Stats		Value
2019/10/02 03:49:58 - 2019/10/02 03:54:58	topology/pod-1/node-105/sys/ctx-[vxlan-2654209]/bd-[vxlan-16220082]/vlan-[vlan-701]	ingress drop packets periodic		3
2019/10/02 03:39:48 - 2019/10/02 03:44:58	topology/pod-1/node-105/sys/ctx-[vxlan-2654209]/bd-[vxlan-16121802]/vlan-[vlan-703]	ingress drop packets periodic		3
2019/10/02 03:29:58 - 2019/10/02 03:44:58	topology/pod-1/node-105/sys/ctx-[vxlan-2654209]/bd-[vxlan-16121802]/vlan-[vlan-703]	ingress drop packets periodic		3
2019/10/02 03:29:58 - 2019/10/02 03:44:58	topology/pod-1/node-105/sys/ctx-[vxlan-2654209]/bd-[vxlan-16220082]/vlan-[vlan-701]	ingress drop packets periodic		3
2019/10/02 03:14:58 - 2019/10/02 03:29:58	topology/pod-1/node-105/sys/ctx-[vxlan-2654209]/bd-[vxlan-16121802]/vlan-[vlan-703]	ingress drop packets periodic		3

Espandendo i dettagli utilizzando il pulsante giallo "Pacchetti scartati" sul diagramma dello switch, è possibile visualizzare i dettagli relativi al flusso scartato.

Dettagli contratto

S Source Endpoint → Destination Endpoint

Filter ID: implicit							BD Allow (Prod1/DB)	
Info	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits	
					permit	node-105	0	
Filter ID: implicit							Context Implicit (Prod1/VRF1)	
Info	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits	
					deny,log	node-105	8636	

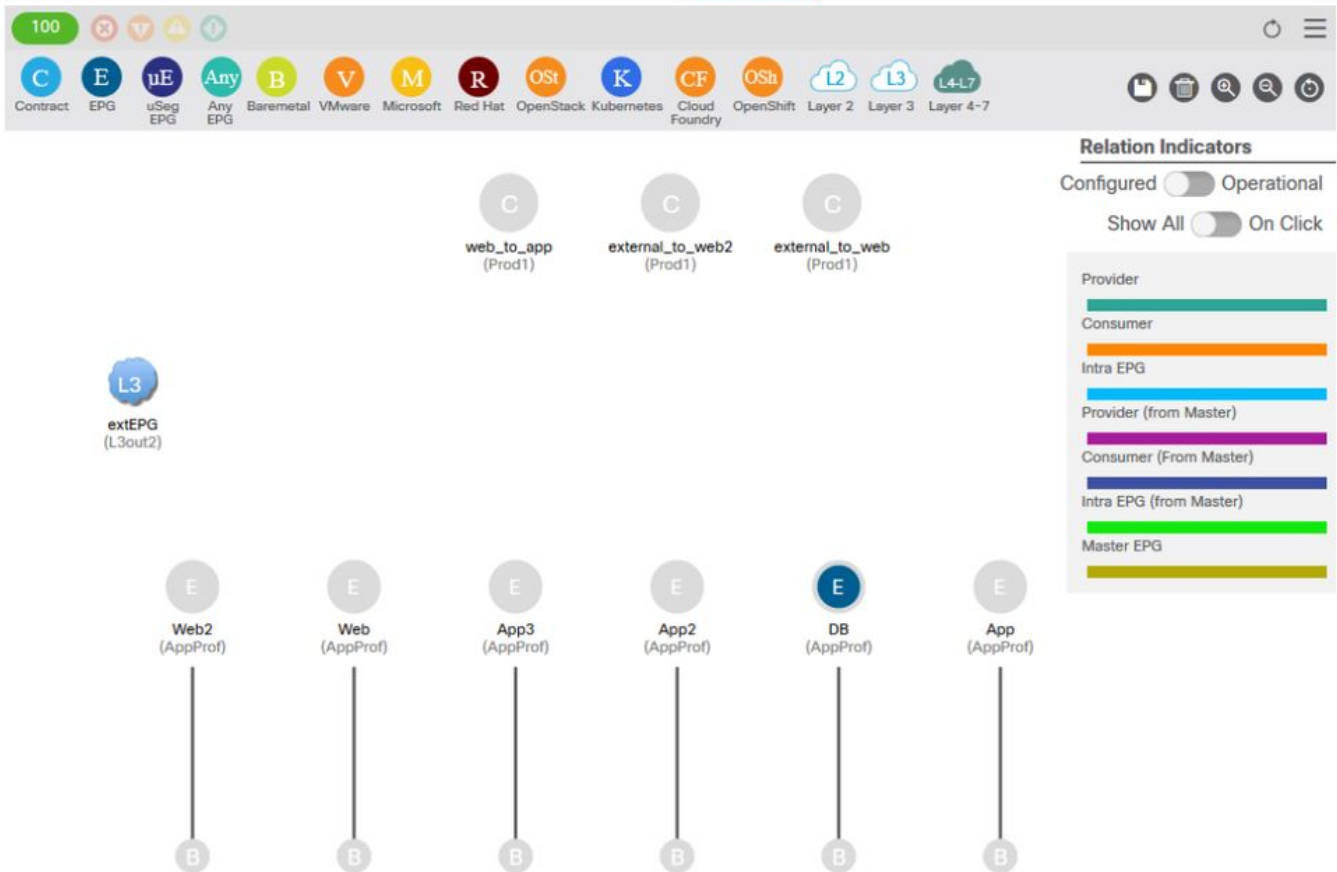
D Destination Endpoint → Source Endpoint

Filter ID: implicit							BD Allow (Prod1/Web)	
Info	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits	
					permit	node-105	0	
Filter ID: implicit							Context Implicit (Prod1/VRF1)	
Info	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits	
					deny,log	node-105	8636	

Passando al sottomenu Contratti, l'utente può identificare il contratto che causa l'eliminazione dei criteri tra gli EPG. Nell'esempio, è Implicit to Deny Prod1/VRF1 che mostra alcuni accessi. Ciò non significa necessariamente che il flusso specificato (192.168.21.11 e 192.168.23.11) stia raggiungendo questo rifiuto implicito. Se la regola di negazione implicita Hits of Context è in aumento, significa che esiste un traffico tra Prod1/DB e Prod1/Web che non ha effetto su nessuno dei contratti, quindi viene eliminato dalla regola di negazione implicita.

Nella vista Topologia profilo applicazione in Tenant > selezionare il nome del profilo applicazione a sinistra > Topologia , è possibile verificare quali contratti vengono applicati a DB EPG. In tal caso, all'EPG non viene assegnato alcun contratto:

Visualizzazione contratto



Ora che gli EPG di origine e di destinazione sono noti, è possibile identificare anche altre informazioni pertinenti, quali:

- Il **pcTag src/dst EPG** degli endpoint interessati. pcTag è l'ID di classe utilizzato per identificare un EPG con una regola di zoning.
- Il **VRFVNID src/dst**, definito anche **ambito**, degli endpoint interessati.

L'ID classe e l'ambito possono essere facilmente recuperati dalla GUI APIC aprendo il Tenant > selezionare il nome del tenant a sinistra > Operativo > ID risorse > EPG

ID risorsa tenant per trovare il tag e l'ambito del pcTag EPG

Tenant - Prod1

Summary Dashboard Policy **Operational** Stats Health Faults History

Flows Packets **Resource IDs**

Bridge Domains VRFs **EPGs** L3Outs External Networks (Bridged)

99

Application Profile Name	AP Alias	EPG Name	Class ID	Scope
AppProf		App	32774	2654209
AppProf		App2	32775	2654209
AppProf		App3	49160	2654209
AppProf		DB	49159	2654209
AppProf		Web	32778	2654209
AppProf		Web2	16388	2097160
Services		NTP	16410	2818048

In questo caso ID classe e ambiti sono:

- Web EPG pcTag 3278
- Web EPG ambito 2654209
- Tag DB EPG 49159
- Ambito EPG DB 2654209

Verificare i criteri applicati al flusso di traffico in fase di risoluzione dei problemi

iBash

Uno strumento interessante per verificare il pacchetto scartato su una foglia ACI è la riga di comando iBash: 'show logging ip access-list internal packet-log deny':

```
leaf5# show logging ip access-list internal packet-log deny | grep 192.168.21.11
[2019-10-01T14:25:44.746528000+09:00]: CName: Prod1:VRF1(VXLAN: 2654209), VlanType: FD_VLAN,
Vlan-Id: 114, SMac: 0xf6f26c4ec8d0, DMac:0x0022bdf819ff, SIP: 192.168.21.11, DIP: 192.168.23.11,
SPort: 0, DPort: 0, Src Intf: Ethernet1/19, Proto: 1, PktLen: 126
[2019-10-01T14:25:44.288653000+09:00]: CName: Prod1:VRF1(VXLAN: 2654209), VlanType: FD_VLAN,
Vlan-Id: 116, SMac: 0x3e2593f0eded, DMac:0x0022bdf819ff, SIP: 192.168.23.11, DIP: 192.168.21.11,
SPort: 0, DPort: 0, Src Intf: Ethernet1/19, Proto: 1, PktLen: 126
```

Come nell'output precedente, si può vedere che sullo switch foglia, sono stati scartati numerosi pacchetti ICMP originati da EP 192.168.23.11 verso 192.168.21.11.

Lo strumento contract_parser consente di verificare i criteri effettivi applicati al VRF a cui sono associati gli endpoint:

```
leaf5# contract_parser.py --vrf Prod1:VRF1
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]
[flags][contract:{str}] [hit=count]
```



```
[7:5159] [vrf:Prod1:VRF1] permit ip tcp tn-Prod1/ap-App1/epg-App(32771) eq 5000 tn-Prod1/ap-App1/epg-Web(32772) [contract:uni/tn-Prod1/brc-web_to_app] [hit=0]
[7:5156] [vrf:Prod1:VRF1] permit ip tcp tn-Prod1/ap-App1/epg-Web(32772) tn-Prod1/ap-App1/epg-App(32771) eq 5000 [contract:uni/tn-Prod1/brc-web_to_app] [hit=0]
[16:5152] [vrf:Prod1:VRF1] permit any epg:any tn-Prod1/bd-Web(49154) [contract:implicit] [hit=0]
[16:5154] [vrf:Prod1:VRF1] permit arp epg:any epg:any [contract:implicit] [hit=0]
[21:5155] [vrf:Prod1:VRF1] deny,log any epg:any epg:any [contract:implicit] [hit=38,+10]
[22:5153] [vrf:Prod1:VRF1] deny,log any epg:any pfx-0.0.0.0/0(15) [contract:implicit] [hit=0]
```

È possibile verificare questa condizione anche tramite la regola di zoning programmata nella pagina che segue, ossia i criteri applicati dallo switch.

```
leaf5# show zoning-rule scope 2654209
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
-----+-----+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name |
Action | Priority |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
-----+-----+
| 5155 | 0 | 0 | implicit | uni-dir | enabled | 2654209 |
deny,log | any_any_any(21) |
| 5159 | 32771 | 32772 | 411 | uni-dir-ignore | enabled | 2654209 | web_to_app |
permit | fully_qual(7) |
| 5156 | 32772 | 32771 | 410 | bi-dir | enabled | 2654209 | web_to_app |
permit | fully_qual(7) |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
-----+-----+
```

Come già rilevato dallo strumento Visibility & Troubleshooting, dallo strumento contract_parser e dalle regole di zoning, l'output conferma che non esiste alcun contratto tra gli EPG di origine e di destinazione nella risoluzione dei problemi. È facile supporre che i pacchetti ignorati corrispondano alla regola di negazione implicita 5155.

Acquisizione ELAM

L'acquisizione ELAM fornisce un report a livello ASIC utilizzato per controllare i dettagli di inoltro che indica, nel caso di un pacchetto scartato, il motivo del rilascio. Quando il motivo di un rilascio è un mancato rispetto delle regole, come in questo scenario, l'output dell'acquisizione ELAM sarà simile al seguente.

In questo capitolo non verranno trattati i dettagli relativi alla configurazione di un'acquisizione ELAM. Consultare il capitolo "Inoltro intra-fabric".

```
leaf5# vsh_lc
module-1# debug platform internal tah elam asic 0
module-1(DBG-elam)# trigger init in-select 6 out-select 0
module-1(DBG-elam)# trigger reset
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 192.168.21.11 dst_ip 192.168.23.11
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# status
```

```
ELAM STATUS
=====
Asic 0 Slice 0 Status Triggered
Asic 0 Slice 1 Status Armed
```

```
module-1(DBG-elam-insel6)# ereport | grep reason
RW drop reason : SECURITY_GROUP_DENY
LU drop reason : SECURITY_GROUP_DENY
```

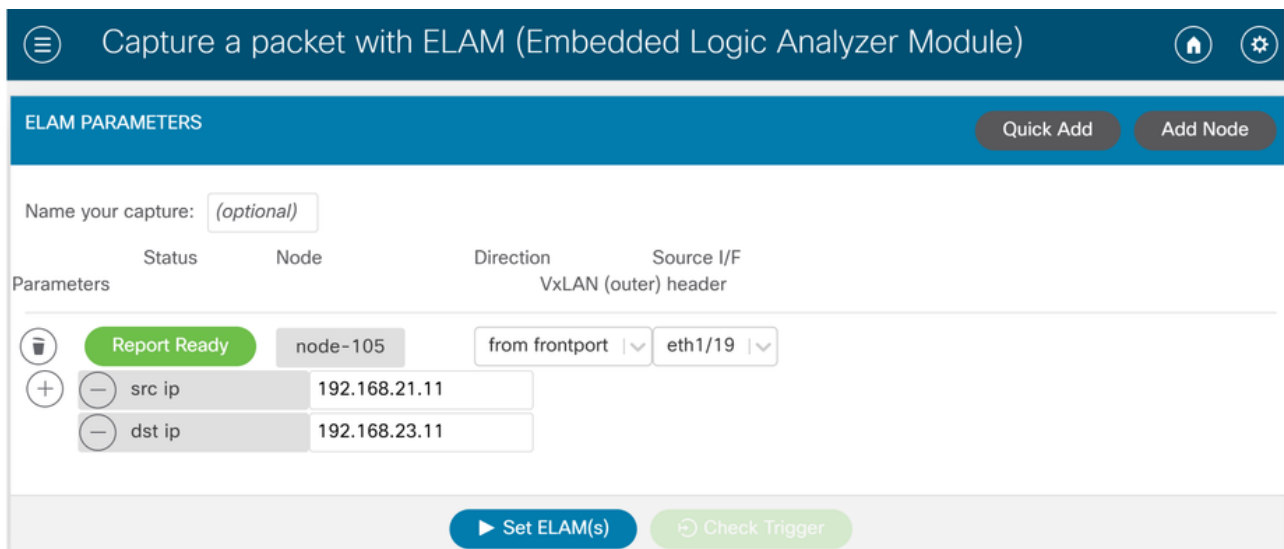
pkt.lu_drop_reason: 0x2D

Il report ELAM sopra riportato mostra chiaramente che il pacchetto è stato scartato a causa di una caduta di policy: 'SECURITY_GROUP_DENY'

ELAM Assistant:

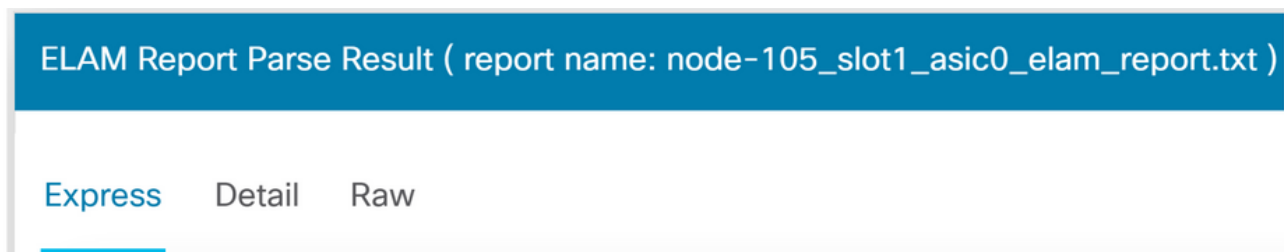
Lo stesso risultato dell'acquisizione ELAM può essere visualizzato tramite l'applicazione ELAM Assistant sull'interfaccia grafica APIC.

Configurazione



In genere, l'utente configura i dettagli di origine e di destinazione per il flusso di interesse. Nell'esempio, il protocollo IP di origine viene usato per acquisire il traffico verso l'endpoint nell'EPG di destinazione che non ha una relazione di contratto con l'EPG di origine.

Report Elam Assistant Express



Con ELAM Assistant è possibile visualizzare tre livelli di output. Si tratta di Express, Detail e Raw.

Report Elam Assistant Express (continua)

Packet Forwarding Information

Forward Result	
Destination Type	To a local port
Destination Logical Port	Eth1/19
Destination Physical Port	packet dropped
Sent to SUP/CPU instead	yes
SUP Redirect Reason (SUP code)	ISTACK_SUP_CODE_ACL_LOG

Contract	
Destination EPG pcTag (dclass)	16387 (Prod1:App1:DB)
Source EPG pcTag (sclass)	10935 (Prod1:App1:Web)
Contract was applied	0 (Contract was not applied on this node)

Drop	
Drop Code	SECURITY_GROUP_DENY

In Risultato rapido, il motivo per cui il codice viene eliminato SECURITY_GROUP_DENY indica che il rilascio è stato il risultato di una corrispondenza di contratto.

Gruppo preferito

Informazioni sui gruppi di opzioni di contratto

Esistono due tipi di applicazione delle policy disponibili per gli EPG in un VRF con un gruppo di preferenza del contratto configurato:

- EPG inclusi: Gli EPG possono comunicare liberamente tra loro senza contratto, se sono membri di un gruppo privilegiato su contratto. Questa regola è basata sulla regola predefinita source-any-destination-any-allow.
- EPG esclusi: Gli EPG che non sono membri di gruppi preferiti devono essere in possesso di contratti per comunicare tra loro. In caso contrario, si applicano le regole di rifiuto tra l'EPG escluso e qualsiasi EPG.

La funzione di gruppo con contratto preferito consente un maggiore controllo della comunicazione tra EPG in un VRF. Se la maggior parte degli EPG nel VRF dovrebbe avere una comunicazione aperta, ma alcuni dovrebbero avere solo una comunicazione limitata con gli altri EPG, configurare una combinazione di un gruppo di preferenza contrattuale e contratti con filtri per controllare più precisamente la comunicazione tra EPG.

Gli EPG esclusi dal gruppo preferito possono comunicare con altri EPG solo se è stato stipulato un contratto per sostituire la regola predefinita source-any-destination-any-deny.

Programmazione gruppo privilegiato contratto

Essenzialmente, i gruppi privilegiati del contratto sono l'inverso dei contratti regolari. Per i contratti regolari, le regole di zoning esplicite dei permessi sono programmate con una regola di zoning

implicita di negazione con l'ambito VRF. Per i Gruppi Preferiti, viene programmata una regola di zoning PERMIT implicita con il valore di priorità numerica più alto e vengono programmate regole di zoning DENY specifiche per impedire il traffico proveniente da EPG che non sono membri del Gruppo Preferito. Di conseguenza, le regole di negazione vengono valutate per prime e, se al flusso non corrispondono queste regole, il flusso è implicitamente consentito.

C'è sempre una coppia di regole di negazione della zonizzazione esplicite per ogni EPG al di fuori del gruppo preferito:

- Uno dal membro del gruppo non preferito a qualsiasi pcTag (valore 0).
- Altro da qualsiasi pcTag (valore 0) al membro del gruppo non preferito.

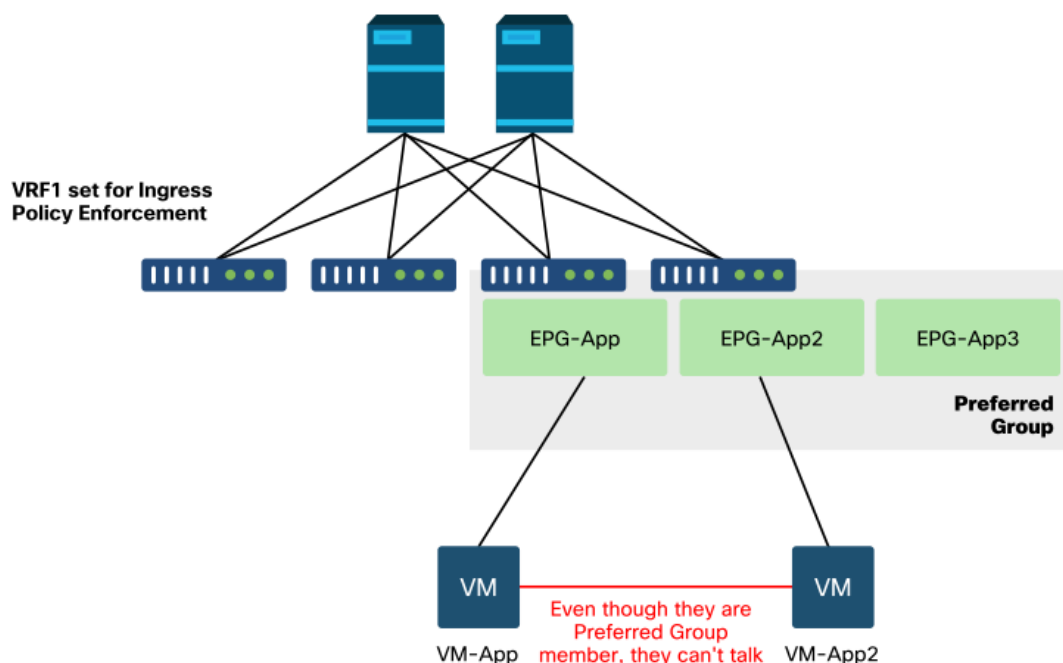
Scenario di risoluzione dei problemi del gruppo preferito

La figura seguente mostra una topologia logica in cui le applicazioni EPG App, App2 e App3 sono configurate come membri del gruppo preferito.

VM-App fa parte di EPG-App e VM-App2 fa parte di EPG-App2. Sia App che App2 EPG devono essere parte del preferito e quindi comunicare liberamente.

VM-App avvia un flusso di traffico sulla porta TCP 6000 verso VM-App2. Sia EPG-App che EPG-App2 sono membri del gruppo preferiti come parte di VRF1. VM-App2 non riceve mai pacchetti sulla porta TCP 6000.

Topologia



Flusso di lavoro

1. Cercare il pcTag di EPG APP e il relativo VRF VNID/Scope

EPG e VRF pcTags

The screenshot shows the Cisco APIC interface for the 'Prod1' tenant. The 'Operational' tab is selected, displaying a table of EPGs. The table has the following columns: Application Profile Name, AP Alias, EPG Name, Class ID, and Scope. The data rows are as follows:

Application Profile Name	AP Alias	EPG Name	Class ID	Scope
AppProf		App	32774	2654209
AppProf		App2	32775	2654209
AppProf		App3	49160	2654209
AppProf		DB	49159	2654209
AppProf		Web	16390	2654209
AppProf		Web2	16388	2097160

2. Verificare la programmazione del contratto utilizzando `contract_parser.py` sulla foglia in entrata

Utilizzare `contract_parser.py` e/o il comando `'show zoning-rule'` e specificare il VRF

```
fab3-leaf8# show zoning-rule scope 2654209
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action |
|         | Priority |         |         |    |        |       |      |        |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| 4165 | 0 | 0 | implicit | uni-dir | enabled | 2654209 | | permit |
grp_any_any_any_permit(20) |
| 4160 | 0 | 0 | implarp | uni-dir | enabled | 2654209 | | permit |
any_any_filter(17) |
| 4164 | 0 | 15 | implicit | uni-dir | enabled | 2654209 | | deny,log |
grp_any_dest_any_deny(19) |
| 4176 | 0 | 16386 | implicit | uni-dir | enabled | 2654209 | | permit |
any_dest_any(16) |
| 4130 | 32770 | 0 | implicit | uni-dir | enabled | 2654209 | | deny,log |
grp_src_any_any_deny(18) |
| 4175 | 49159 | 0 | implicit | uni-dir | enabled | 2654209 | | deny,log |
grp_src_any_any_deny(18) |
| 4129 | 0 | 49159 | implicit | uni-dir | enabled | 2654209 | | deny,log |
grp_any_dest_any_deny(19) |
| 4177 | 32778 | 0 | implicit | uni-dir | enabled | 2654209 | | deny,log |
grp_src_any_any_deny(18) |
| 4128 | 0 | 32778 | implicit | uni-dir | enabled | 2654209 | | deny,log |
grp_any_dest_any_deny(19) |
| 4178 | 32775 | 0 | implicit | uni-dir | enabled | 2654209 | | deny,log |
grp_src_any_any_deny(18) |
| 4179 | 0 | 32775 | implicit | uni-dir | enabled | 2654209 | | deny,log |
grp_any_dest_any_deny(19) |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

-----+

fab3-leaf8# **contract_parser.py --vrf Prod1:VRF1**

```
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-14] dst-epg [dst-14]
[flags][contract:{str}] [hit=count]
[16:4176] [vrf:Prod1:VRF1] permit any epg:any tn-Prod1/bd-App(16386) [contract:implicit] [hit=0]
[16:4160] [vrf:Prod1:VRF1] permit arp epg:any epg:any [contract:implicit] [hit=0]
[18:4130] [vrf:Prod1:VRF1] deny,log any tn-Prod1/vrf-VRF1(32770) epg:any [contract:implicit]
[hit=?]
[18:4178] [vrf:Prod1:VRF1] deny,log any epg:32775 epg:any [contract:implicit] [hit=?]
[18:4177] [vrf:Prod1:VRF1] deny,log any epg:32778 epg:any [contract:implicit] [hit=?]
[18:4175] [vrf:Prod1:VRF1] deny,log any epg:49159 epg:any [contract:implicit] [hit=?]
[19:4164] [vrf:Prod1:VRF1] deny,log any epg:any pfx-0.0.0.0/0(15) [contract:implicit] [hit=0]
[19:4179] [vrf:Prod1:VRF1] deny,log any epg:any epg:32775 [contract:implicit] [hit=?]
[19:4128] [vrf:Prod1:VRF1] deny,log any epg:any epg:32778 [contract:implicit] [hit=?]
[19:4129] [vrf:Prod1:VRF1] deny,log any epg:any epg:49159 [contract:implicit] [hit=?]
[20:4165] [vrf:Prod1:VRF1] permit any epg:any epg:any [contract:implicit] [hit=65]
```

Esaminando l'output precedente, viene osservata la voce di autorizzazione implicita (ruleId 4165) con la priorità più alta di 20. Questa regola di autorizzazione implicita consentirà di autorizzare tutti i flussi di traffico a meno che non esista una regola di negazione esplicita con una priorità inferiore che impedisce il flusso di traffico.

Inoltre, sono state osservate due regole di negazione esplicite per pcTag 32775, ovvero pcTag di EPG App2. Queste due regole di negazione esplicite impediscono il traffico da qualsiasi EPG a EPG App2 e viceversa. Tali regole hanno la priorità 18 e 19, quindi avranno la precedenza sulla regola di autorizzazione predefinita.

La conclusione è che EPG App2 non è un membro del gruppo preferito in quanto vengono rispettate le regole di negazione esplicite.

3. Verificare la configurazione dei membri del gruppo preferito EPG

Navigare nella GUI APIC e controllare la configurazione dei membri del gruppo preferito di EPG App2 ed EPG App. Nella figura seguente, vedere EPG App2 non è configurato come membro del gruppo preferito.

EPG App2 — Esclusa impostazione Membro gruppo preferito

The screenshot shows the Cisco APIC interface for configuring an EPG. The left sidebar shows the navigation tree with 'Prod1' selected, and 'Application EPGs' expanded to show 'App2'. The main panel displays the configuration for 'EPG - App2'. The 'Policy' tab is active, and the 'General' sub-tab is selected. The 'Preferred Group Member' is currently set to 'Exclude'.

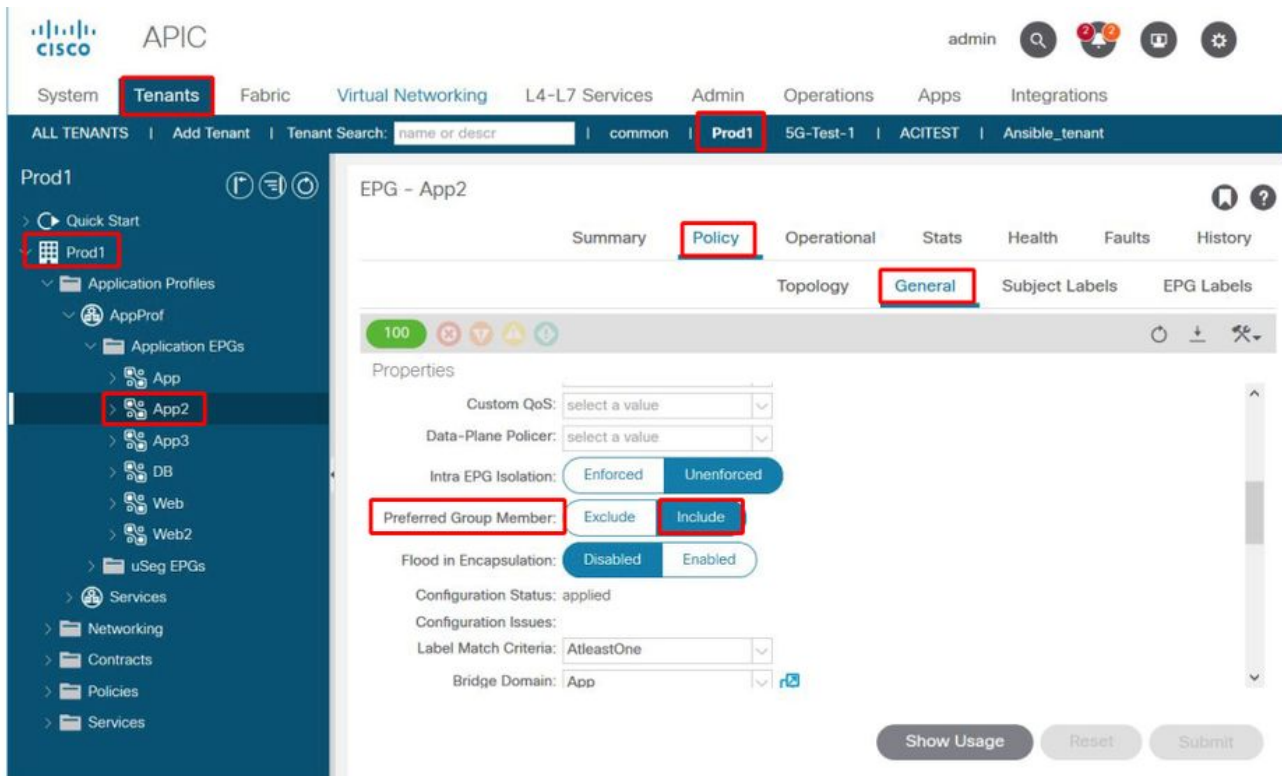
Applicazione EPG: impostazione Membro gruppo preferito inclusa

The screenshot shows the Cisco APIC interface for configuring an EPG. The left sidebar shows the navigation tree with 'Prod1' selected, and 'Application EPGs' expanded to show 'App'. The main panel displays the configuration for 'EPG - App'. The 'Policy' tab is active, and the 'General' sub-tab is selected. The 'Preferred Group Member' is currently set to 'Include'.

4. Impostare EPG App2 come membro del gruppo preferito

La modifica della configurazione di App2 EPG consente al gruppo preferito di comunicare liberamente come parte del gruppo preferito.

EPG App2 - Impostazione membri gruppo preferiti inclusa



5. Verificare nuovamente la programmazione del contratto utilizzando `contract_parser.py` nella foglia in cui risiede Src EP

Utilizzare di nuovo `contract_parser.py` e specificare il nome VRF per verificare se le regole di negazione esplicita per EPG App2 sono state eliminate.

```
fab3-leaf8# contract_parser.py --vrf Prod1:VRF1
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]
[flags][contract:{str}] [hit=count]
[16:4176] [vrf:Prod1:VRF1] permit any epg:any tn-Prod1/bd-App(16386) [contract:implicit] [hit=0]
[16:4160] [vrf:Prod1:VRF1] permit arp epg:any epg:any [contract:implicit] [hit=0]
[18:4175] [vrf:Prod1:VRF1] deny,log any epg:16390 epg:any [contract:implicit] [hit=0]
[18:4167] [vrf:Prod1:VRF1] deny,log any epg:23 epg:any [contract:implicit] [hit=0]
[18:4156] [vrf:Prod1:VRF1] deny,log any tn-Prod1/vrf-VRF1(32770) epg:any [contract:implicit]
[hit=0]
[18:4168] [vrf:Prod1:VRF1] deny,log any epg:49159 epg:any [contract:implicit] [hit=0]
[19:4164] [vrf:Prod1:VRF1] deny,log any epg:any pfx-0.0.0.0/0(15) [contract:implicit] [hit=0]
[19:4169] [vrf:Prod1:VRF1] deny,log any epg:any epg:16390 [contract:implicit] [hit=0]
[19:4159] [vrf:Prod1:VRF1] deny,log any epg:any epg:23 [contract:implicit] [hit=0]
[19:4174] [vrf:Prod1:VRF1] deny,log any epg:any epg:49159 [contract:implicit] [hit=0]
[20:4165] [vrf:Prod1:VRF1] permit any epg:any epg:any [contract:implicit] [hit=65]
```

Le regole di rifiuto esplicito per EPG App2 e il relativo pcTag 32775 non sono più osservate nell'output di cui sopra. Ciò significa che il traffico tra gli EP in EPG App e EPG App2 ora corrisponderà alla regola di autorizzazione implicita, ruleId 4165, con la priorità più alta di 20.

da vzAny a EPG

Informazioni su vzAny

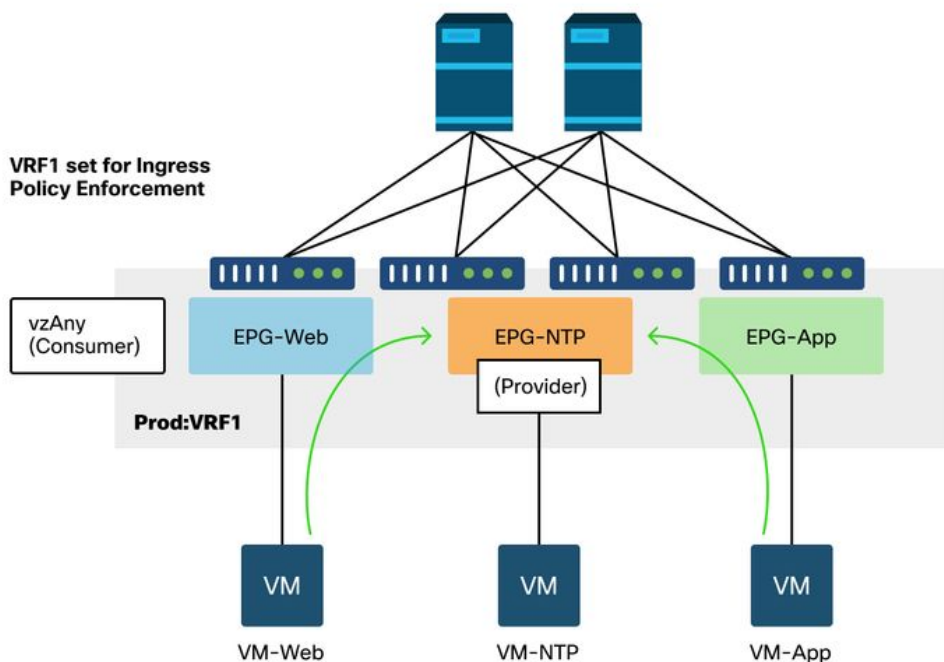
Quando si configurano contratti tra uno o più EPG, i contratti possono essere configurati come relazione consumata o fornita. Quando il numero di EPG aumenta, aumenta anche la quantità di

relazioni contrattuali tra di loro. Alcuni casi di utilizzo comuni richiedono che tutti gli EPG scambino flussi di traffico con un altro EPG specifico. Un tale caso di utilizzo potrebbe essere un EPG contenente EP che forniscono servizi che devono essere utilizzati da tutti gli altri EPG all'interno dello stesso VRF (ad esempio NTP o DNS). vzAny consente di ridurre il sovraccarico operativo nella configurazione delle relazioni contrattuali tra tutti gli EPG e gli EPG specifici che forniscono servizi che devono essere utilizzati da tutti gli altri EPG. Inoltre, vzAny consente un uso molto più efficiente della CAM dei criteri di sicurezza sugli switch foglia, in quanto vengono aggiunte solo 2 regole di zoning per ciascuna relazione contrattuale vzAny.

Esempio di caso di utilizzo

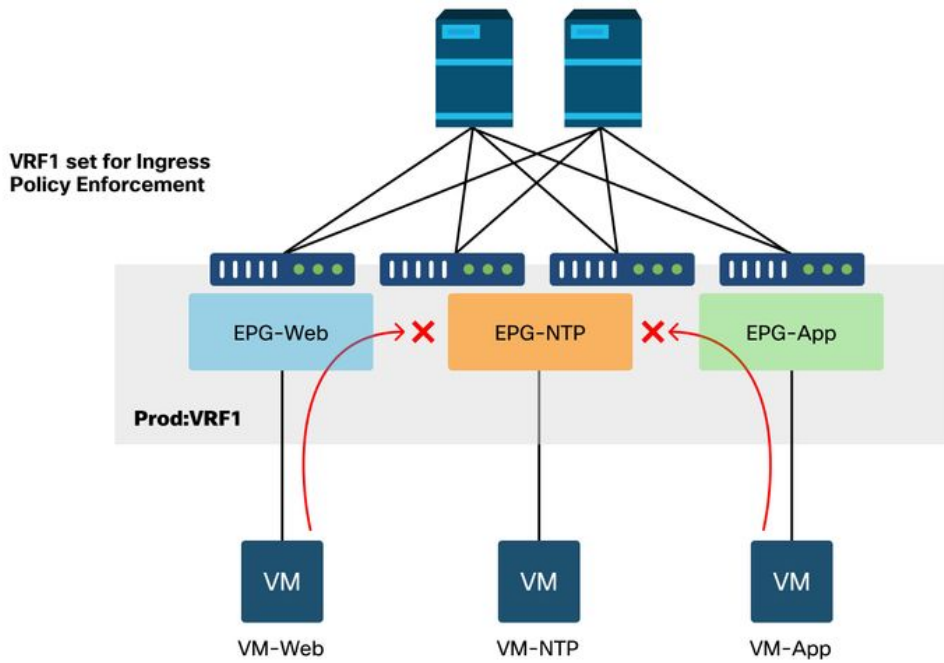
La figura seguente descrive un caso di utilizzo in cui VM-Web e VM-App rispettivamente in EPG Web e App devono utilizzare i servizi NTP da VM-NTP in EPG-NTP. Anziché configurare un contratto fornito su EPG NTP, e successivamente avere lo stesso contratto come contratto consumato su EPG Web e App, vzAny consente a ogni EPG in VRF Prod:VRF1 di utilizzare i servizi NTP da EPG NTP.

vzAny — Qualsiasi EPG in VRF Prod:VRF1 può utilizzare i servizi NTP da EPG NTP



Si consideri uno scenario in cui si osservano cali tra gli EPG che utilizzano i servizi NTP quando non vi è alcun contratto tra di essi.

Scenario di risoluzione dei problemi - Il traffico diminuisce se non è presente alcun contratto



Flusso di lavoro

1. Cercare il pcTag di EPG NTP e il relativo VRF VNID/Scope

'Tenant > Operativo > ID risorse > EPG' consente di trovare il tag pc e l'ambito

EPG NTP pcTag e relativo VRF VNID/ambito

Tenant - Prod1

Summary Dashboard Policy **Operational** Stats Health Faults History

Flows Packets **Resource IDs**

Bridge Domains VRFs **EPGs** L3Outs External Networks (Bridged)

Application Profile Name	AP Alias	EPG Name	Class ID	Scope
AppProf		App	32774	2654209
AppProf		App2	32775	2654209
AppProf		App3	49160	2654209
AppProf		DB	49159	2654209
AppProf		Web	32778	2654209
AppProf		Web2	16388	2097160
Services		NTP	16410	2818048

Page 1 Of 1 Objects Per Page: 100 Displaying Objects 1 - 7 Of 7

2. Verificare se un contratto è configurato come vzAny contratto consumato come parte del VRF

Passare al VRF e verificare se è presente un contratto utilizzato configurato come vzAny in 'EPG Collection for VRF'.

Contratto configurato come vzQualsiasi contratto sul VRF consumato

The screenshot shows the Cisco APIC interface. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'L4-L7 Services', 'Admin', 'Operations', 'Apps', and 'Integrations'. The 'Tenants' tab is active, and the 'Prod1' tenant is selected. The left sidebar shows a tree view with 'Networking' and 'VRFs' expanded, and 'EPG Collection for VRF' selected. The main content area shows the configuration for 'vzAny' with tabs for 'Policy', 'Operational', 'Faults', and 'History'. The 'General' tab is active, displaying a table of 'Consumed Contracts'.

Name	Tenant	Type	QoS Class	State
any_to_ntp	Prod1	Contract	Unspecified	formed

3. Verificare se lo stesso contratto è applicato come un contratto fornito su EPG NTP

Al fine di stabilire un rapporto contrattuale, lo stesso contratto deve essere applicato come un contratto fornito sull'EPG NTP che fornisce servizi NTP agli altri EPG nel suo VRF.

The screenshot shows the Cisco APIC interface. The 'Tenants' tab is selected, and the 'Prod1' tenant is active. In the left-hand navigation menu, the 'Contracts' folder is highlighted. The main content area displays a table of contracts. The table has columns for Tenant Name, Tena Alias, Contract Name, Contract Type, Provider / Consum, QoS Class, State, Label, and Subject Label. A single contract is listed with the name 'any_to_ntp' and state 'formed'.

Tenant Name	Tena Alias	Contract Name	Contract Type	Provider / Consum	QoS Class	State	Label	Subject Label
Prod1		any_to_ntp	Contract	Provid...	Unspecified	formed		

4. Verifica della regola di zoning sulla foglia in entrata utilizzando `contract_parser.py` o `'show zoning-rule'`

La foglia in entrata deve avere 2 regole di zoning per consentire flussi di traffico bidirezionali (se l'oggetto del contratto è impostato per consentire entrambe le direzioni) tra EPG e EPG NTP. 'Qualsiasi EPG' è indicato come pcTag 0 nella programmazione delle regole di zoning.

Se si utilizza `contract_parser.py` o il comando `"show zoning-rule"` sulla foglia in entrata mentre si specifica il VRF, è possibile assicurarsi che la regola di zoning sia programmata.

Regole di zoning che consentono il traffico da/verso EPG NTP da altri EPG presenti nel VRF

Usando `contract_parser.py` e `'show zoning-rule'` per controllare la presenza delle regole di zoning basate su `vzAny`.

Qui sono evidenti due tipi di regole:

1. Regole 4156 e 4168 che permettono a Any di NTP e viceversa. Hanno la priorità 13 e 14:
Regola di zoning che consente flussi di traffico da qualsiasi EPG (pcTag 0) a EPG NTP (pcTag 49161).
Regola di zoning che consente flussi di traffico da EPG NTP (pcTag 46161) a qualsiasi altro EPG (pcTag 0).
2. Regola 4165: regola di tipo "qualsiasi a qualsiasi regola di negazione" (predefinita) con priorità 21.

Dato che la priorità più bassa ha la precedenza, tutti gli EPG del VRF avranno accesso a NTP EPG.

```
fab3-leaf8# contract_parser.py --vrf Prod1:VRF
```

```
Key:
```

```
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]  
[flags][contract:{str}] [hit=count]
```

```
[13:4156] [vrf:Prod1:VRF1] permit ip tcp tn-Prod1/ap-Services/epg-NTP(49161) eq 123 epg:any  
[contract:uni/tn-Prod1/brc-any_to_ntp] [hit=0]  
[14:4168] [vrf:Prod1:VRF1] permit ip tcp epg:any tn-Prod1/ap-Services/epg-NTP(49161) eq 123  
[contract:uni/tn-Prod1/brc-any_to_ntp] [hit=0]  
[16:4176] [vrf:Prod1:VRF1] permit any epg:any tn-Prod1/bd-App(16386) [contract:implicit] [hit=0]  
[16:4174] [vrf:Prod1:VRF1] permit any epg:any tn-Prod1/bd-Services(32776) [contract:implicit]  
[hit=0]  
[16:4160] [vrf:Prod1:VRF1] permit arp epg:any epg:any [contract:implicit] [hit=0]  
[21:4165] [vrf:Prod1:VRF1] deny,log any epg:any epg:any [contract:implicit] [hit=65]  
[22:4164] [vrf:Prod1:VRF1] deny,log any epg:any pfx-0.0.0.0/0(15) [contract:implicit] [hit=0]
```

```
fab3-leaf8# show zoning-rule scope 2654209
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+  
-----+  
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action |  
| Priority | | | | | | | | |  
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+  
-----+  
| 4165 | 0 | 0 | implicit | uni-dir | enabled | 2654209 | | deny,log |  
any_any_any(21) |  
| 4160 | 0 | 0 | implarp | uni-dir | enabled | 2654209 | | permit |  
any_any_filter(17) |  
| 4164 | 0 | 15 | implicit | uni-dir | enabled | 2654209 | | deny,log |  
any_vrf_any_deny(22) |  
| 4176 | 0 | 16386 | implicit | uni-dir | enabled | 2654209 | | permit |  
any_dest_any(16) |  
| 4174 | 0 | 32776 | implicit | uni-dir | enabled | 2654209 | | permit |  
any_dest_any(16) |  
| 4168 | 0 | 49161 | 424 | uni-dir | enabled | 2654209 | any_to_ntp | permit |  
any_dest_filter(14) |  
| 4156 | 49161 | 0 | 425 | uni-dir | enabled | 2654209 | any_to_ntp | permit |  
src_any_filter(13) |  
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+  
-----+
```

L3Out condiviso in EPG

Informazioni su L3Out condiviso

Shared Layer 3 Out è una configurazione che consente di avere un L3Out in un VRF che fornisce alcuni servizi (accesso esterno) e uno o più VRF utilizzano questo L3Out. Per ulteriori informazioni sul file L3Out condiviso, vedere il capitolo "External routing".

Quando si esegue la condivisione di L3Out, si consiglia di fare in modo che il fornitore del contratto sia la condivisione L3Out e che l'EPG sia il consumatore del contratto. Questo scenario verrà illustrato in questa sezione.

Si sconsiglia di fare l'opposto, ovvero L3Out che utilizza un servizio fornito da EPG. Il motivo è legato alla scalabilità, in quanto per i servizi condivisi le regole di zoning vengono installate solo sui VRF consumer. I principi di consumo e fornitura indicano dove i flussi di traffico sono iniziati. Con l'applicazione predefinita della politica in entrata, ciò significa che l'applicazione della politica verrà applicata sul lato del consumatore e più specificamente sul lato in entrata (foglia non frontaliera). Per applicare i criteri alla foglia in entrata, è necessario il pcTag di destinazione. In questo scenario, la destinazione è il pcTag EPG esterno. In questo modo, la foglia in entrata

applica la policy e inoltra i pacchetti alla foglia di confine. La foglia di bordo riceve il pacchetto sul relativo collegamento fabric che esegue una ricerca del percorso (LPM) e inoltra il pacchetto all'adiacenza del prefisso di destinazione.

La foglia di confine, tuttavia, NON esegue alcuna applicazione delle policy durante l'invio del traffico all'EP di destinazione né esegue questa operazione sul flusso del traffico di ritorno all'EP di origine.

Di conseguenza, solo la Policy CAM della foglia non BL in entrata ha voci installate (nel VRF consumer) e la Policy CAM della BL non è interessata.

Risoluzione dei problemi relativi a un'unità L3out condivisa

Flusso di lavoro

1. Verificare EPG pcTag e VRF VNID/Scope per il consumer EPG

Con L3Out condiviso, le regole di zoning vengono installate solo nel VRF consumer. Il provider deve disporre di un pcTag globale (inferiore a 16k) che consenta di utilizzare questo pcTag in tutte le VRF consumer. Nel nostro scenario, il provider è l'EPG esterno e avrà un pcTag globale. L'EPG consumer disporrà di un pcTag locale come al solito.

pcTag di EPG consumer

Application Profile Name	AP Alias	EPG Name	Class ID	Scope
AppProf		App	32774	2654209
AppProf		App2	32775	2654209
AppProf		App3	49160	2654209
AppProf		DB	49159	2654209
AppProf		Web	32778	2654209
AppProf		Web2	16388	2097160
Services		NTP	16410	2818048

2. Verificare il VNID/ambito pcTag e VRF per il provider L3Out EPG

Come indicato nel passo 1, il provider L3Out EPG dispone di un intervallo globale pcTag come prefissi da L3Out che vengono trapelati nel VRF consumer. Di conseguenza, il pcTag EPG L3Out non deve sovrapporsi a pcTags nel VRF consumer e quindi è compreso nell'intervallo globale di pcTag.

pcTag del provider EPG esterno

Tenant - Prod1

Summary Dashboard Policy **Operational** Stats Health Faults History

Flows Packets **Resource IDs**

Bridge Domains VRFs EPGs **L3Outs** External Networks (Bridged)

EPG Name	EPG Alias	Class ID	Scope
extEpg		25	2719752

Page 1 Of 1 Objects Per Page: 100 Displaying Objects 1 - 1 Of 1

3. Verificare che l'EPG consumer disponga di un contratto con ambito tenant importato o di un contratto globale configurato

L'NTP EPG consumer con subnet definita in EPG/BD utilizza il contratto con ambito "tenant" o "globale"

Contratto utilizzato da EPG

CISCO APIC admin

System **Tenants** Fabric Virtual Networking L4-L7 Services Admin Operations Apps Integrations

ALL TENANTS | Add Tenant | Tenant Search: name or descr | common | **Prod1** | 5G-Test-1 | ACITEST | mgmt

Prod1

- Quick Start
- Prod1**
- Application Profiles
 - AppProf
 - Application EPGs**
 - NTP**
 - Domains (VMs and Ba...
 - EPG Members
 - Static Ports
 - Static Leafs
 - Fibre Channel (Paths)
 - Contracts**
 - Static Endpoint
 - Subnets
 - L4-L7 Virtual IPs
 - L4-L7 IP Address Pool

Contracts

Contracts Inherited Contracts

Tenar Name	Tena Alias	Contract Name	Contract Type	Provided / Consumed	QoS Class	State	Label	Sub Lab
Contract Type: Contract								
Prod1		external_to_ntp	Contract	Consumed	Unspecified	form...		

4. Verificare se il BD dell'EPG consumer ha una subnet configurata con il relativo ambito impostato su 'Condiviso tra VRF'

La subnet dell'EPG è configurata nel dominio bridge, ma deve avere il flag 'shared between VRF' (per consentire le perdite instradate) e il flag 'advertising externally' (per consentire l'annuncio a L3Out)

5. Verificare che il provider L3Out EPG disponga di un contratto con ambito tenant importato o di un contratto globale configurato

L'EPG L3Out deve avere un contratto con ambito tenant o un contratto globale configurato come contratto fornito.

Contratto su L3Out provider

The screenshot shows the Cisco APIC interface. The 'Tenants' tab is selected, and the 'Prod1' tenant is chosen. In the left-hand navigation pane, the 'L3Outs' folder is expanded, showing 'L3Out1' and its sub-items: 'Logical Node Profiles', 'External EPGs', 'extEpg', and 'extEpg2'. The 'External EPG Instance Profile - extEpg' page is displayed, with the 'Policy' tab selected. Under the 'Contracts' sub-tab, the 'Provided Contracts' section is active, showing a table with one entry:

Name	Tenant	Type	QoS Class	Match Type	State
external_to_ntp	Prod1	Contract	Unspecified	AtleastOne	formed

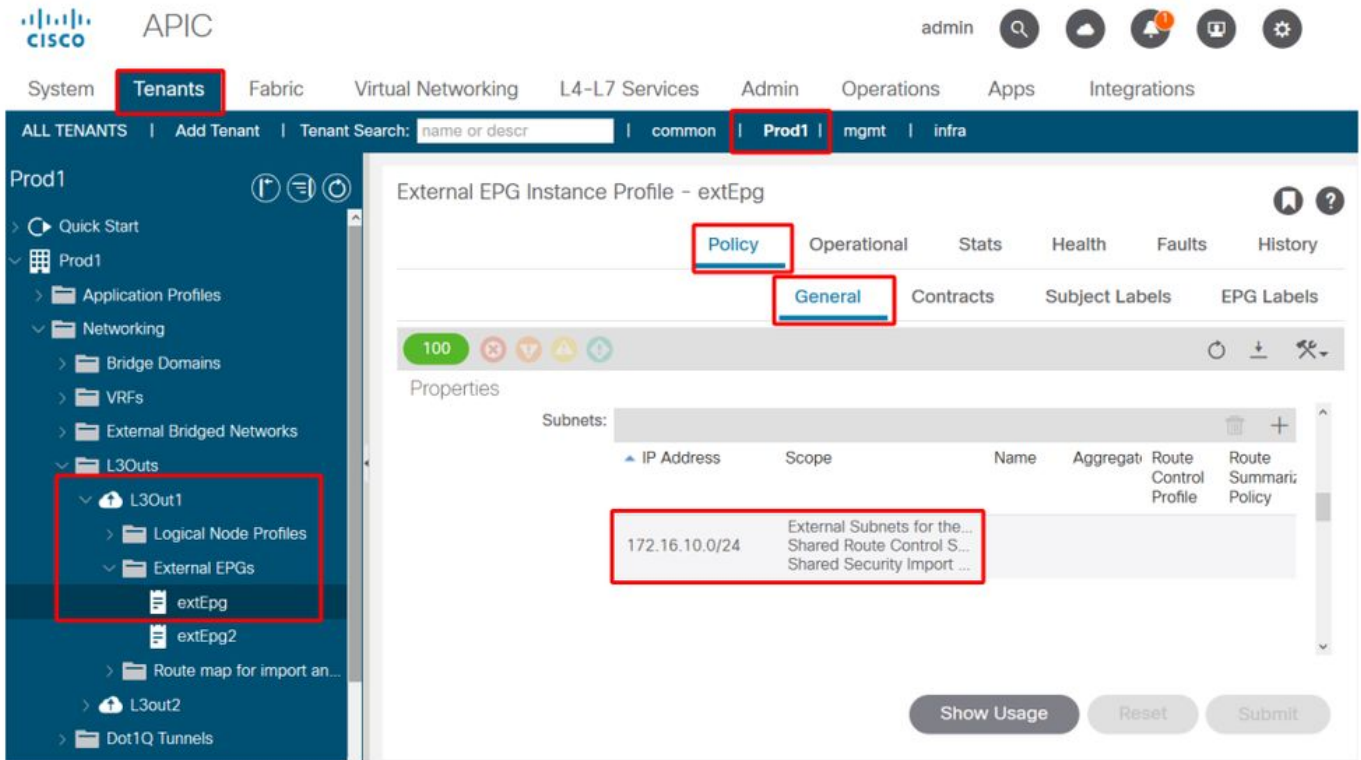
6. Verificare se il provider L3Out EPG dispone di una subnet configurata con gli ambiti necessari selezionati

Per il provider L3Out EPG è necessario configurare il prefisso da trafugare con gli ambiti seguenti:

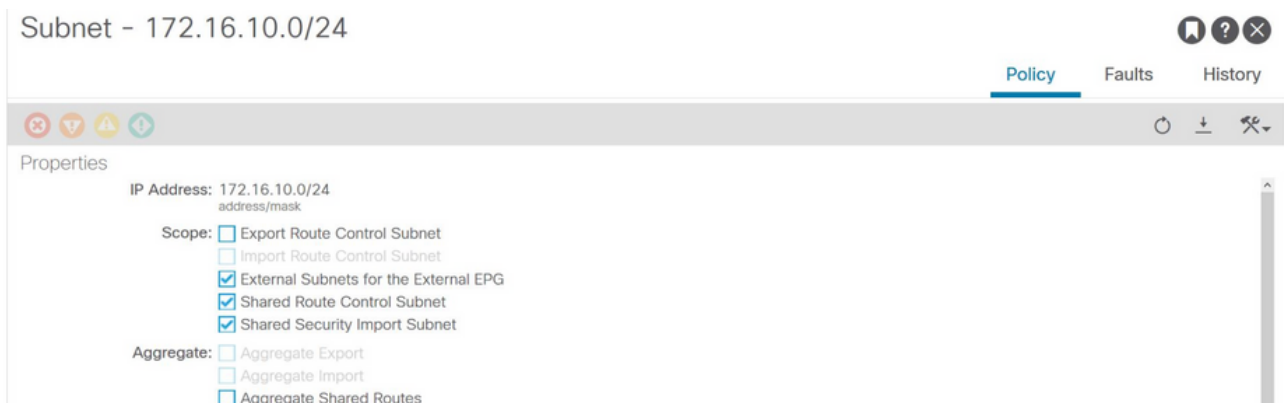
- Subnet esterne per l'EPG esterno.
- Subnet di controllo route condivisa.
- Subnet di importazione della protezione condivisa.

Per ulteriori informazioni sul flag subnet in L3Out EPG, fare riferimento al capitolo "External forwarding".

Impostazioni subnet EPG esterne



Impostazioni subnet EPG esterne espanse



7. Verificare il pcTag della subnet EPG L3Out su una rete non BL per il VRF consumer

Quando il traffico destinato alla subnet EPG esterna entra nella non-BL, viene eseguita una ricerca sul prefisso di destinazione per determinare il pcTag. È possibile verificare questa condizione utilizzando il seguente comando nella non-BL.

Notare che questo output viene preso nell'ambito del VNI 2818048 che è il VRF VNID consumer. Guardando la tabella, il consumatore può trovare il pcTag di destinazione, anche se non si trova nello stesso VRF.

```
fab3-leaf8# vsh -c 'show system internal policy-mgr prefix' | egrep 'Vrf-Vni|==|common:default'
Vrf-Vni Vrf-Id Table-Id Table-State VRF-Name
Addr Class Shared Remote Complete
=====
=====
2818048 19 0x13 Up common:default
0.0.0.0/0 15 False False False
2818048 19 0x80000013 Up common:default
```

```

::/0 15 False False False
2818048 19 0x13 Up common:default
172.16.10.0/24 25 True True False

```

L'output precedente mostra la combinazione della subnet L3Out EPG e del relativo pcTag 25 globale.

8. Verificare le regole di zoning programmate sulla non-BL per il VRF consumer

Utilizzare il comando 'contract_parser.py' o 'show zoning-rule' e specificare il VRF.

Sotto gli output del comando vengono visualizzate due regole di zoning installate per consentire il traffico dal pcTag 16410 locale EPG del consumer al pcTag 25 globale L3Out EPG. Questo è nell'ambito 2818048, che è l'ambito del VRF del consumer.

```
fab3-leaf8# show zoning-rule scope 2818048
```

```

+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name |
Action | Priority |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| 4174 | 0 | 0 | implarp | uni-dir | enabled | 2818048 |
permit | any_any_filter(17) |
| 4168 | 0 | 15 | implicit | uni-dir | enabled | 2818048 |
deny,log | any_vrf_any_deny(22) |
| 4167 | 0 | 32789 | implicit | uni-dir | enabled | 2818048 |
permit | any_dest_any(16) |
| 4159 | 0 | 0 | implicit | uni-dir | enabled | 2818048 |
deny,log | any_any_any(21) |
| 4169 | 25 | 0 | implicit | uni-dir | enabled | 2818048 |
deny,log | shsrc_any_any_deny(12) |
| 4156 | 25 | 16410 | 425 | uni-dir-ignore | enabled | 2818048 | external_to_ntp |
permit | fully_qual(7) |
| 4131 | 16410 | 25 | 424 | bi-dir | enabled | 2818048 | external_to_ntp |
permit | fully_qual(7) |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+

```

```
fab3-leaf8# contract_parser.py --vrf common:default
```

```

Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]
[flags][contract:{str}] [hit=count]

[7:4131] [vrf:common:default] permit ip tcp tn-Prod1/ap-Services/epg-NTP(16410) tn-Prod1/l3out-L3Out1/instP-extEpg(25) eq 123 [contract:uni/tn-Prod1/brc-external_to_ntp] [hit=0]
[7:4156] [vrf:common:default] permit ip tcp tn-Prod1/l3out-L3Out1/instP-extEpg(25) eq 123 tn-Prod1/ap-Services/epg-NTP(16410) [contract:uni/tn-Prod1/brc-external_to_ntp] [hit=0]
[12:4169] [vrf:common:default] deny,log any tn-Prod1/l3out-L3Out1/instP-extEpg(25) epg:any [contract:implicit] [hit=0]
[16:4167] [vrf:common:default] permit any epg:any tn-Prod1/bd-Services(32789) [contract:implicit] [hit=0]
[16:4174] [vrf:common:default] permit arp epg:any epg:any [contract:implicit] [hit=0]
[21:4159] [vrf:common:default] deny,log any epg:any epg:any [contract:implicit] [hit=0]
[22:4168] [vrf:common:default] deny,log any epg:any pfx-0.0.0.0/0(15) [contract:implicit] [hit=0]

```

9. Verificare le regole di zoning programmate sul BL per il provider VRF

Utilizzare il comando 'contract_parser.py' o 'show zoning-rule' e specificare il VRF. I seguenti output del comando mostrano che **NON** esistono regole di zoning specifiche nel VRF del provider

come descritto più volte in precedenza.

È nell'ambito 2719752 che è l'ambito del provider VRF.

```
border-leaf# show zoning-rule scope 2719752
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name
4134	10937	24	default	uni-dir-ignore	enabled	2719752	vrf1_to_vrf2
4135	24	10937	default	bi-dir	enabled	2719752	vrf1_to_vrf2
4131	0	0	implicit	uni-dir	enabled	2719752	
4130	0	0	implarp	uni-dir	enabled	2719752	
4132	0	15	implicit	uni-dir	enabled	2719752	

```
border-leaf# contract_parser.py --vrf Prod1:VRF3
```

Key:

```
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]  
[flags][contract:{str}] [hit=count]
```

```
[9:4134] [vrf:Prod1:VRF3] permit any tn-Prod1/l3out-L3Out1/instP-extEpg2(10937) tn-Prod1/l3out-L3Out2/instP-extEpg2(24) [contract:uni/tn-Prod1/brc-vrf1_to_vrf2] [hit=0]  
[9:4135] [vrf:Prod1:VRF3] permit any tn-Prod1/l3out-L3Out2/instP-extEpg2(24) tn-Prod1/l3out-L3Out1/instP-extEpg2(10937) [contract:uni/tn-Prod1/brc-vrf1_to_vrf2] [hit=0]  
[16:4130] [vrf:Prod1:VRF3] permit arp epg:any epg:any [contract:implicit] [hit=0]  
[21:4131] [vrf:Prod1:VRF3] deny,log any epg:any epg:any [contract:implicit] [hit=0]  
[22:4132] [vrf:Prod1:VRF3] deny,log any epg:any pfx-0.0.0.0/0(15) [contract:implicit] [hit=0]
```

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).