Dépannage des politiques de sécurité ACI - Contrats

Contenu

Introduction
Informations générales
Aperçu
Méthodes de programmation des règles de zonage
Comparaison entre les méthodologies de règles de zonage
Lecture d'une entrée de règle de zonage
Mémoire CAM (Content-Addressable Memory) de stratégie
Fuite VRF, pcTags globaux et directionnalité d'application des politiques des sorties L3 partagées
Direction d'application du contrôle de stratégie VRF
Où la stratégie est-elle appliquée ?
Application en entrée et en sortie
Outils
Validation des règles de zonage
'show zoning-rules'
'show zoning-filter'
'show system internal policy-mgr stats'
'show logging ip access-list internal packet-log deny'
contract_parser
Validation de la classification des paquets
ELAM
fTriage
Application Assistant ELAM
Utilisation du CAM de stratégie
La vue « Capacité leaf » du tableau de bord Capacité
'show platform internal hal health-stats'
EPG à EPG
Considérations relatives à la suppression de stratégie générique
Méthodologie
Exemple de scénario de dépannage EPG à EPG
Topologie
Identifier les commutateurs Leaf source et de destination impliqués dans la suppression de paquets
Visibilité et dépannage
Configuration de la visibilité et du dépannage
Identification du rejet
Supprimer les détails
Détails de contrat
Visualisation du contrat
ID de ressource du locataire pour rechercher le pcTag et l'étendue EPG

Vérifier la stratégie appliquée au flux de trafic en cours de dépannage
iBash
Capture ELAM
ELAM Assistant :
Configuration
Rapport Elam Assistant Express
Rapport Elam Assistant Express (suite)
Groupe préféré
À propos des groupes préférentiels de contrats
Programmation du groupe privilégié par contrat
Scénario de dépannage du groupe préféré
Topologie
Workflow
vzAny vers EPG
À propos de vzAny
Exemple d'utilisation
Scénario de dépannage - Le trafic est interrompu en l'absence de contrat
Workflow
Règles de zonage permettant le trafic vers/depuis EPG NTP à partir d'autres EPG dans le VRF présent
Partagé L3Out vers EPG
À propos de Shared L3Out
Dépannage d'une sortie L3 partagée
Workflow

Introduction

Ce document décrit les étapes à suivre pour comprendre et dépanner les politiques de sécurité de l'ACI, appelées contrats.

Informations générales

Le contenu de ce document a été extrait du livre Troubleshooting Cisco Application Centric Infrastructure, Second Edition (Dépannage de l'infrastructure axée sur les applications Cisco, deuxième édition), en particulier le livre Security Policies - Overview, Security Policies - Tools, **Security Policies - EPG to EPG**, **Security Policies - Preferred group** and **Security Policies - vzAny to EPG**.

Aperçu

L'architecture de sécurité de base de la solution ACI suit un modèle de liste d'autorisation. À moins qu'un VRF ne soit configuré en mode **non appliqué**, tous les flux de trafic EPG à EPG sont implicitement abandonnés. Comme l'indique le modèle de liste d'autorisation prêt à l'emploi, le paramètre VRF par défaut est en mode **imposé**. Les flux de trafic peuvent être autorisés ou explicitement refusés en implémentant des règles de zonage sur les noeuds de commutation. Ces règles de zonage peuvent être programmées dans différentes configurations en fonction du flux

de communication souhaité entre les groupes de terminaux (EPG) et de la méthode utilisée pour les définir. Notez que les entrées de la règle de zonage ne sont pas avec état et autorisent/refusent généralement en fonction du port/socket pour deux EPG une fois la règle programmée.

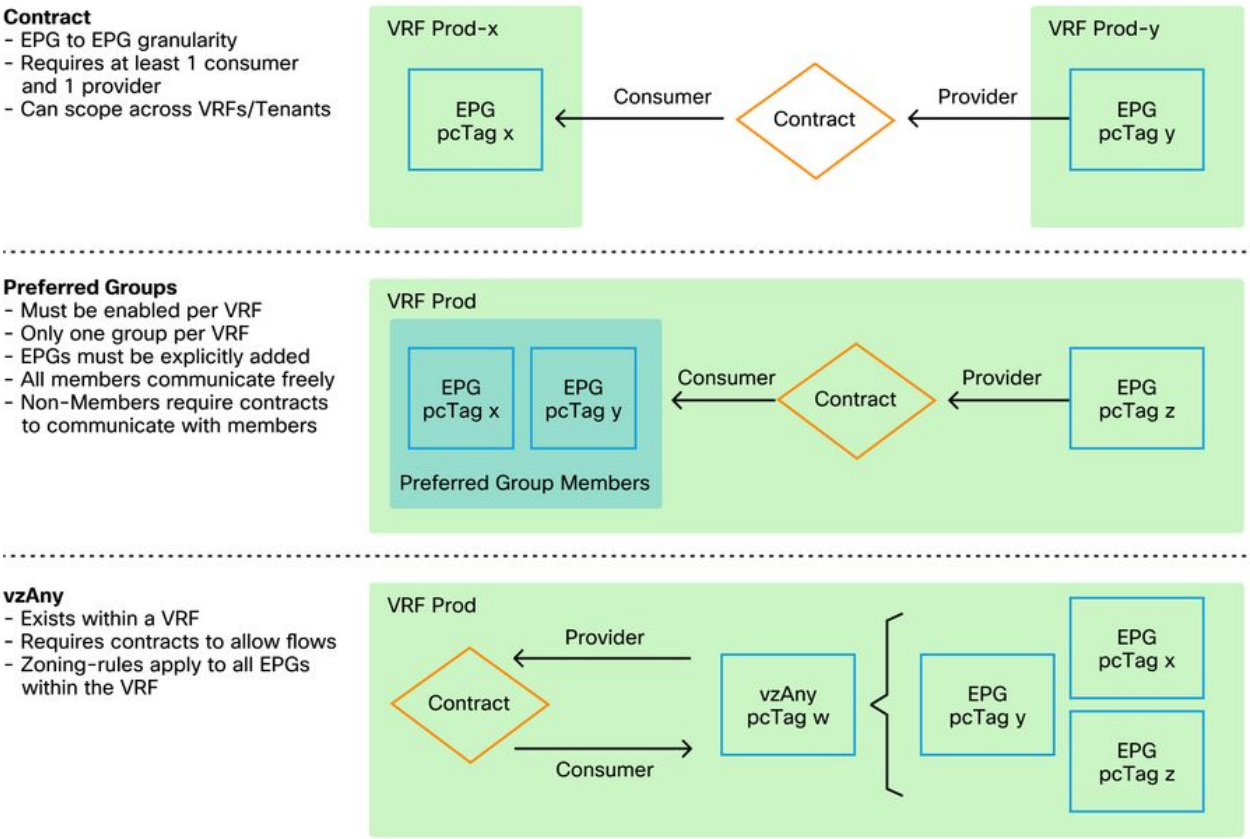
Méthodes de programmation des règles de zonage

Les principales méthodes de programmation des règles de zonage dans l'ACI sont les suivantes :

- **Contrats EPG à EPG :** nécessite généralement au moins un client et un fournisseur pour programmer des règles de zonage sur au moins deux groupes de terminaux distincts.
- **Groupes préférés :** nécessite l'activation du regroupement au niveau VRF ; un seul groupe peut exister par VRF. Tous les membres du groupe peuvent communiquer librement. Les non-membres ont besoin de contrats pour autoriser les flux vers le groupe préféré.
- **vzAny :** « collection EPG » définie sous un VRF donné. vzAny représente tous les EPG du VRF. L'utilisation de vzAny permet des flux entre un EPG et tous les EPG au sein du VRF via une connexion de contrat.

Le schéma suivant peut être utilisé pour référencer la granularité de la règle de zonage que chacune des méthodes ci-dessus permet de contrôler :

Comparaison entre les méthodologies de règles de zonage



Tout en utilisant la méthode contractuelle de programmation des règles de zonage, il existe une option pour définir la portée du contrat. Cette option doit être soigneusement étudiée si une conception de service partagé/fuite de route est requise. Si vous souhaitez passer d'un VRF à un autre au sein du fabric ACI, vous pouvez utiliser des contrats.

Les valeurs d'étendue peuvent être les suivantes :

- **Application :** une relation client/fournisseur contractuelle ne programmera que les règles entre les groupes de terminaux définis dans le même profil d'application. La réutilisation du même contrat sur d'autres EPG de profil d'application ne permettra pas la diaphonie entre eux.
- **VRF (par défaut) :** une relation client/fournisseur contractuelle permet de programmer des règles entre des groupes de terminaux définis dans le même VRF. La réutilisation du même contrat sur d'autres EPG de profil d'application permettra la diaphonie entre eux. Veillez à ce que seuls les flux souhaités soient autorisés. Dans le cas contraire, un nouveau contrat doit être défini afin d'éviter toute diaphonie involontaire.
- **Client :** une relation client/fournisseur contractuelle permet de programmer des règles entre des groupes de terminaux définis au sein du même client. S'il existe des EPG liés à plusieurs VRF dans un même locataire et qu'ils consomment/fournissent le même contrat, cette portée peut être utilisée pour induire une fuite de route afin de permettre la communication inter-VRF.
- **Global :** une relation client/fournisseur contractuelle permet de programmer des règles entre les groupes de terminaux sur tout locataire au sein d'un fabric ACI. Il s'agit de la portée la plus élevée possible de la définition, et il convient d'être très prudent lorsque cette option est activée sur des contrats précédemment définis afin d'éviter les fuites de flux non intentionnelles.

Lecture d'une entrée de règle de zonage

Une fois la règle de zonage programmée, elle apparaîtra comme suit sur un leaf :

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

- **ID de règle :** ID de l'entrée de règle. Aucune signification réelle autre que d'agir comme un identifiant unique.
- **Src EPG :** un ID unique par VRF (pcTag) du groupe de terminaux source.
- **Dst EPG :** identifiant unique par VRF (pcTag) du groupe de terminaux de destination.
- **FilterID :** l'ID du filtre auquel la règle tente de correspondre. Le filtre contient les informations de protocole par rapport auxquelles la règle doit correspondre.
- **Dir :** la direction de la règle de zonage.
- **OperSet :** état de fonctionnement de la règle.
- **Étendue :** ID unique du VRF avec lequel la règle sera mise en correspondance.
- **Nom :** nom du contrat qui a entraîné la programmation de cette entrée.
- **Action :** ce que le leaf fera quand il correspondra à cette entrée. Inclut : [Abandonner, Autoriser, Consigner, Rediriger].
- **Priority :** ordre dans lequel les règles de zonage seront validées pour l'action en fonction d'une portée, d'un SrcEPG, d'un DstEPG et d'entrées de filtre correspondants.

Mémoire CAM (Content-Addressable Memory) de stratégie

Au fur et à mesure que chaque règle de zonage est programmée, une matrice de l'entrée de règle de zonage mappée avec les entrées de filtre commence à consommer la **politique CAM** sur les

commutateurs. Lors de la conception des flux autorisés à travers un fabric ACI, une attention particulière doit être portée lors de la réutilisation des contrats, au lieu d'en créer de nouveaux, en fonction de la conception finale. La réutilisation du même contrat sur plusieurs groupes de terminaux sans comprendre les règles de zonage résultantes peut rapidement se répercuter sur plusieurs flux autorisés de manière inattendue. En même temps, ces flux non intentionnels continueront à consommer le CAM des politiques. Lorsque le CAM de la politique est plein, la programmation de la règle de zonage commence à échouer, ce qui peut entraîner une perte inattendue et intermittente selon la configuration et les comportements des points d'extrémité.

Fuite VRF, pcTags globaux et directionnalité d'application des politiques des sorties L3 partagées

Il s'agit d'une légende spéciale pour l'exemple d'utilisation des services partagés qui nécessite la configuration de contrats. Les services partagés impliquent généralement un trafic inter-VRF au sein d'un fabric ACI qui repose sur l'utilisation d'un contrat de portée « locataire » ou « global ». Pour bien comprendre ceci, il faut d'abord renforcer l'idée que la valeur pcTag typique assignée aux EPG ne sont pas uniques globalement. Les pcTags sont étendus à un VRF et le même pcTag peut potentiellement être réutilisé dans un autre VRF. Lorsque la question des fuites de route est abordée, commencez à appliquer les exigences sur le fabric ACI, notamment la nécessité de valeurs uniques au niveau mondial, y compris les sous-réseaux et les pcTags.

Ce qui en fait une considération spéciale est l'aspect directionnalité lié à un EPG étant un consommateur vs un fournisseur. Dans un scénario de services partagés, le fournisseur est généralement censé piloter un pcTag global pour obtenir une valeur unique de fabric. Dans le même temps, le consommateur conservera son pcTag avec étendue VRF, ce qui le place dans une position spéciale pour pouvoir désormais programmer et comprendre l'utilisation de la valeur pcTag globale pour appliquer la politique.

Pour référence, la plage d'allocation pcTag est la suivante :

- Système réservé : 1-15 .
- Étendue globale : 16-16384 pour les groupes de terminaux de fournisseurs de services partagés.
- Étendue locale : 16385-65535 pour les groupes de terminaux VRF.

Direction d'application du contrôle de stratégie VRF

Dans chaque VRF, il est possible de définir le paramètre de direction d'application.

- Le paramètre par défaut de la direction d'application est Ingress.
- L'autre option de direction d'application est Egress.

L'application de la stratégie dépend de plusieurs variables.

Le tableau ci-dessous permet de comprendre où la stratégie de sécurité est appliquée au niveau leaf.

Où la stratégie est-elle appliquée ?

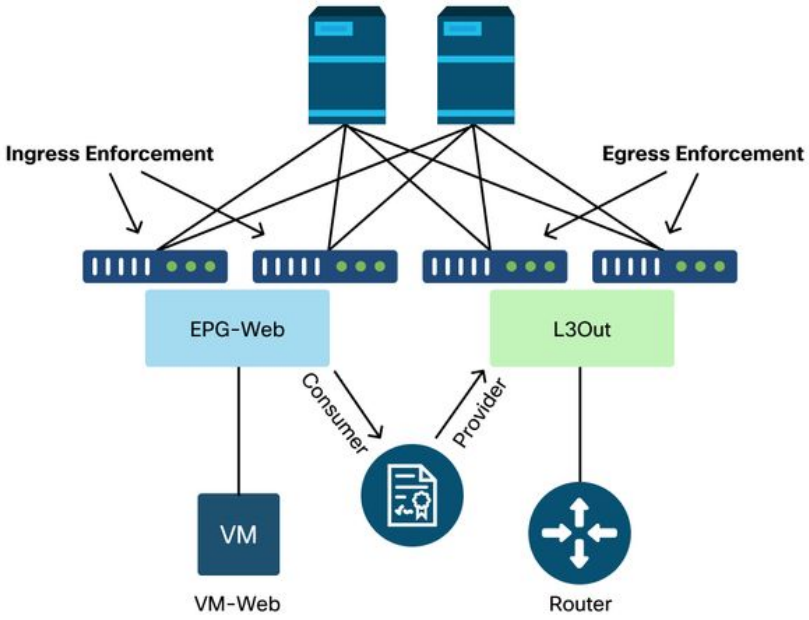
Scénario	Mode d'application VRF	Consommateur	Fournisseur	Stratégie appliquée sur
Intra-VRF	Entrée/sortie	EPG	EPG	·Si le terminal de destination est appris

				: feuille d'entrée* ·Si le terminal de destination n'est pas appris : feuille de sortie
	Entrée	EPG	EPG L3Out	Leaf consommateur (Leaf non-border)
	Entrée	EPG L3Out	EPG	Leaf du fournisseur (leaf non frontalier)
	Sortie	EPG	EPG L3Out	leaf frontière -> trafic leaf non-frontière ·Si le terminal de destination est appris : bordure
	Sortie	EPG L3Out	EPG	·Si le terminal de destination n'est pas appris : feuille non frontalière Trafic leaf non frontalier-> leaf frontalier ·Feuille de bordure
	Entrée/sortie	EPG L3Out	EPG L3Out	Feuille d'entrée*
	Entrée/sortie	EPG	EPG	Feuille de consommateur
	Entrée/sortie	EPG	EPG L3Out	Leaf consommateur (Leaf non-border)
Inter-VRF	Entrée/sortie	EPG L3Out	EPG	Feuille d'entrée*
	Entrée/sortie	EPG L3Out	EPG L3Out	Feuille d'entrée*

*L'application de la stratégie est appliquée au premier noeud leaf touché par le paquet.

La figure ci-dessous illustre un exemple d'application de contrat où EPG-Web en tant que consommateur et L3Out EPG en tant que fournisseur ont un contrat intra-VRF. Si VRF est défini sur le mode d'application en entrée, la stratégie est appliquée par les noeuds leaf où réside EPG-Web. Si VRF est défini sur le mode d'application de sortie, la politique est appliquée par les noeuds leaf en limite où L3Out réside si le point de terminaison VM-Web est appris sur le leaf en limite.

Application en entrée et en sortie



Outils

Il existe une variété d'outils et de commandes qui peuvent être utilisés pour aider à identifier un **abandon** de **stratégie**. Une suppression de politique peut être définie comme une suppression de paquet due à une configuration de contrat ou à un manque de configuration.

Validation des règles de zonage

Les outils et commandes suivants peuvent être utilisés pour valider explicitement les règles de zonage qui sont programmées sur les commutateurs Leaf à la suite de relations client/fournisseur terminées.

'show zoning-rules'

Une commande au niveau du commutateur montrant toutes les règles de zonage en place.

```
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'

Filtre qui contient les informations de sport/port sur lesquelles agit la règle de zonage. Cette

commande permet de vérifier la programmation du filtre.

```
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'

Cette commande peut être exécutée pour vérifier le nombre d'occurrences par règle de zonage. Cela est utile pour déterminer si une règle attendue est atteinte par opposition à une autre, telle qu'une règle de suppression implicite qui peut avoir une priorité plus élevée.

```
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'

Commande au niveau du commutateur qui peut être exécutée au niveau iBash et qui signale les pertes liées aux ACL (contrat) et les informations liées au flux, notamment :

- VRF
- VLAN-ID
- MAC source/MAC dest.
- IP source/IP destination
- Port source/Port de destination
- Interface source

```
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
```

contract_parser

Script Python sur le périphérique qui produit une sortie qui corrèle les règles de zonage, les filtres et les statistiques de succès tout en effectuant des recherches de noms à partir des ID. Ce script est extrêmement utile en ce qu'il prend un processus en plusieurs étapes et le transforme en une commande unique qui peut être filtrée sur des EPG/VRF spécifiques ou sur d'autres valeurs liées au contrat.

```
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]
```

Validation de la classification des paquets

ELAM

Rapport de niveau ASIC utilisé pour vérifier les détails de transmission qui indique, dans le cas d'un paquet abandonné, la raison de l'abandon. Dans cette section, la raison peut être un REFUS_GROUPE_SÉCURITÉ (abandon de stratégie de contrat).

fTriage

Utilitaire basé sur Python sur le contrôleur APIC qui peut suivre le flux de paquets de bout en bout avec ELAM.

Application Assistant ELAM

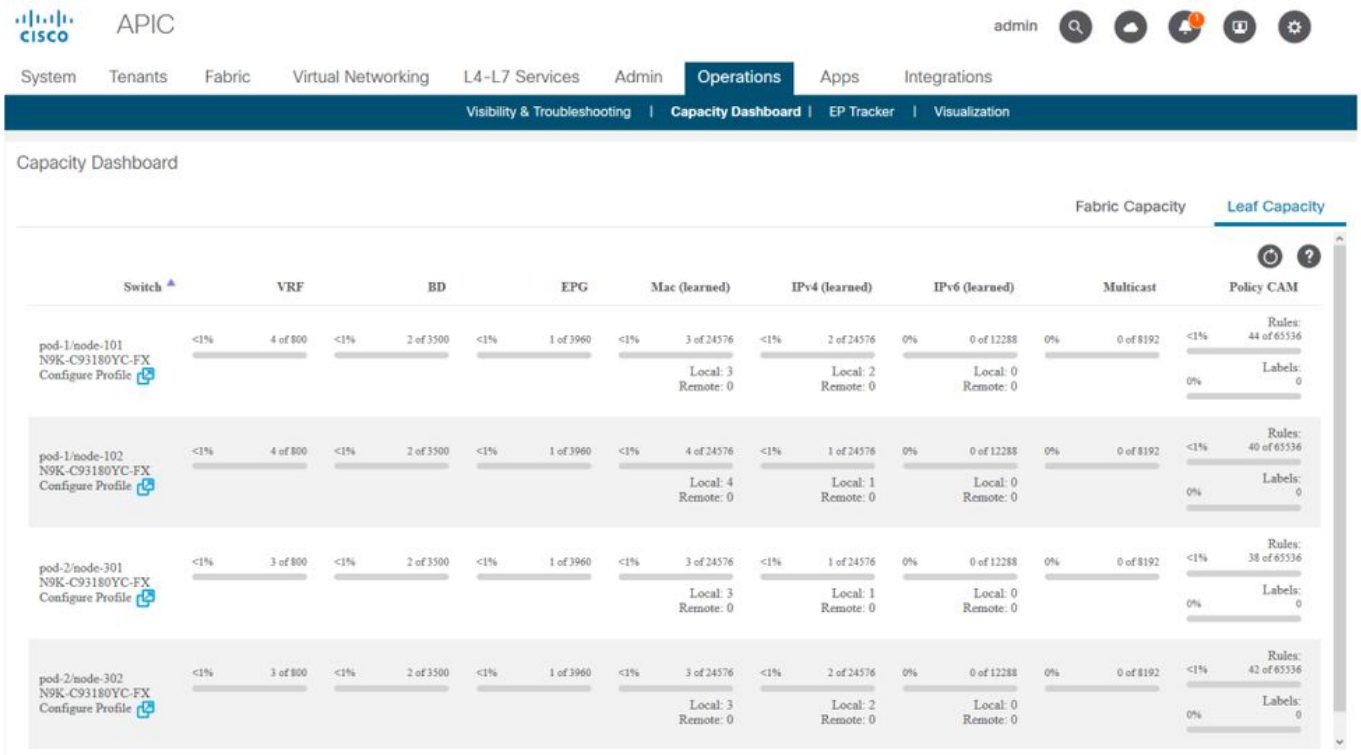
Une application APIC qui réduit la complexité de divers ASIC pour rendre l'inspection de la décision de transmission beaucoup plus pratique et conviviale.

Pour plus d'informations sur les outils ELAM, fTriage et ELAM Assistant, reportez-vous à la section « Transfert intra-fabric »

Utilisation du CAM de stratégie

L'utilisation de la politique CAM par feuille est un paramètre important à surveiller pour s'assurer que le fabric est en bon état. Le moyen le plus rapide de surveiller cela est d'utiliser le « Tableau de bord de capacité » dans l'interface graphique et de vérifier explicitement la colonne « Came de stratégie ».

La vue « Capacité leaf » du tableau de bord Capacité



'show platform internal hal health-stats'

Cette commande est utile pour valider une variété de limites de ressources et d'utilisation, y compris la CAM de stratégie. Notez que cette commande ne peut être exécutée que dans vsh_lc, donc passez-la en utilisant l'indicateur '-c'si elle est exécutée depuis 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
=============
```

EPG à EPG

Considérations relatives à la suppression de stratégie générique

Il existe de nombreuses façons de résoudre un problème de connectivité entre deux terminaux. La méthodologie suivante constitue un bon point de départ pour déterminer rapidement et efficacement si le problème de connectivité est le résultat d'une **perte de stratégie** (induite par un contrat).

Quelques questions de haut niveau à se poser avant de plonger :

- Les terminaux se trouvent-ils dans le même EPG ou dans des EPG différents ? Le trafic entre

deux terminaux résidant dans des EPG différents (inter-EPG) est implicitement refusé et nécessite un contact pour permettre la communication.Le trafic entre deux terminaux au sein du même EPG (intra-EPG) est implicitement autorisé, sauf si l'isolation intra-EPG est utilisée.
- Le VRF est-il appliqué ou non ? Lorsqu'un VRF est en mode **imposé**, — dans le VRF — des contrats sont requis pour que les terminaux de deux EPG différents communiquent.Lorsqu'un VRF est en mode **non appliqué**, — dans le VRF — tout le trafic serait autorisé par le fabric ACI sur plusieurs EPG appartenant au VRF non appliqué, indépendamment des contrats ACI appliqués.

Méthodologie

Avec les divers outils disponibles, certains sont plus appropriés et plus pratiques que d'autres, selon le niveau d'information déjà connu sur le flux affecté.

Le chemin complet du paquet dans le fabric ACI est-il connu (leaf d'entrée, leaf de sortie...) ?

- Si la réponse est oui, l’assistant ELAM doit être utilisé pour identifier la raison de l’abandon sur le commutateur source ou de destination.
- Si la réponse est non, les commandes Visibility & Troubleshooting, fTriage, contract_parser, Operational tab dans la vue Tenant et iBash permettent de réduire le chemin du paquet ou d'avoir plus de visibilité sur les raisons de l'abandon.

Veuillez noter que l'outil fTriage ne sera pas traité en détail dans cette section. Reportez-vous au chapitre « Intra-Fabric Forwarding » pour plus de détails sur l'utilisation de cet outil.

Considérez que si la fonction Visibilité et dépannage permet de visualiser rapidement l'emplacement où les paquets sont abandonnés entre deux points d'extrémité, fTriage affiche des informations plus détaillées pour un dépannage plus approfondi. Par exemple, fTriage permet d'identifier l'interface, la raison de l'abandon et d'autres détails de bas niveau sur le flux affecté

.

Cet exemple de scénario montre comment dépanner un abandon de stratégie entre deux points d'extrémité : 192.168.21.11 et 192.168.23.11

En supposant que les paquets sont abandonnés entre ces deux points d’extrémité, le workflow de dépannage suivant sera utilisé pour identifier la cause première du problème :

Identifiez le ou les leaf src/dst impliqués dans le flux de trafic :

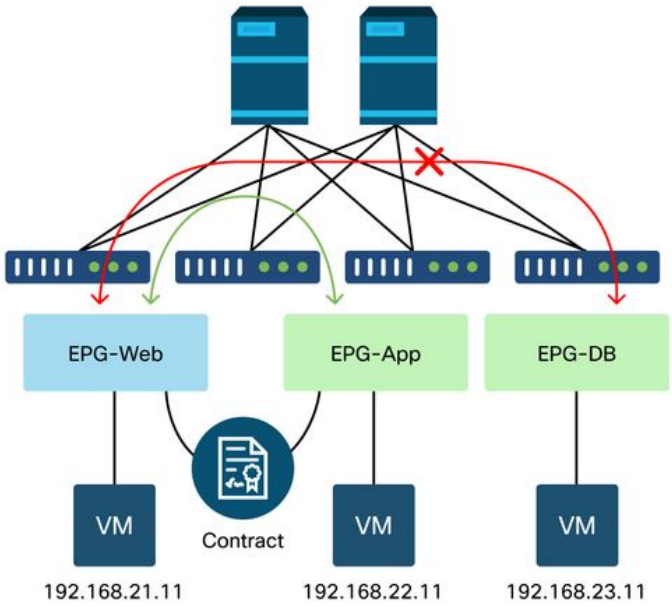
1. Utilisez **Visibility & Troubleshooting** pour suivre le flux de paquets et identifier le périphérique qui abandonne le paquet.
2. Exécutez la commande « show logging ip access-list internal packet-log deny » sur le périphérique sélectionné. Si un paquet avec l'une des adresses IP d'intérêt est refusé et consigné, le **packet-log** imprimera le point d'extrémité et le nom de contrat appropriés sur une base par accès.
3. Utilisez la commande « contract_parser.py —vrf <tenant>:<VRF> » sur le noeud leaf source et de destination pour observer le nombre d'occurrences pour le contrat configuré : Si un paquet atteint le contrat sur le commutateur source ou de destination, le compteur du contrat concerné est incrémentéCette méthode est moins granulaire que celle du journal de paquets interne de la liste d'accès IP dans les situations où de nombreux flux pourraient atteindre la

même règle (de nombreux terminaux/flux entre les deux groupes de terminaux concernés). Les étapes ci-dessus sont décrites plus en détail dans le paragraphe suivant.

Exemple de scénario de dépannage EPG à EPG

Cet exemple de scénario montre comment dépanner un abandon de stratégie entre deux points d'extrémité : 192.168.21.11 dans EPG-Web et 192.168.23.11 dans EPG-DB.

Topologie

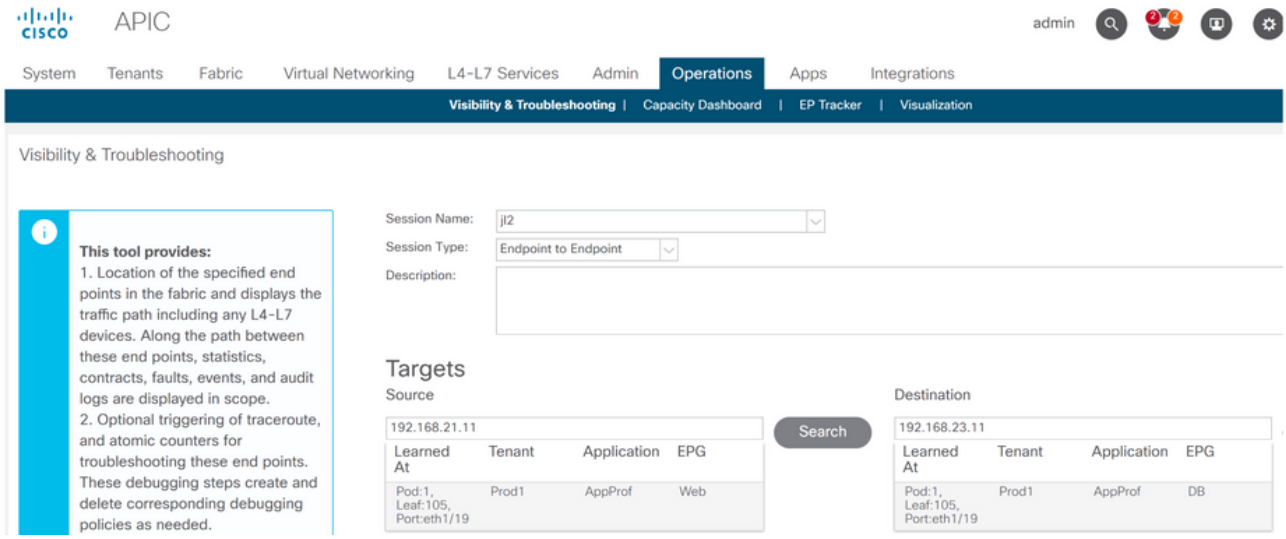


Identifier les commutateurs Leaf source et de destination impliqués dans la suppression de paquets

Visibilité et dépannage

L'outil Visibilité et dépannage permet de visualiser le commutateur où le paquet a été abandonné pour un flux EP-to-EP spécifique et d'identifier où les paquets ont été abandonnés.

Configuration de la visibilité et du dépannage

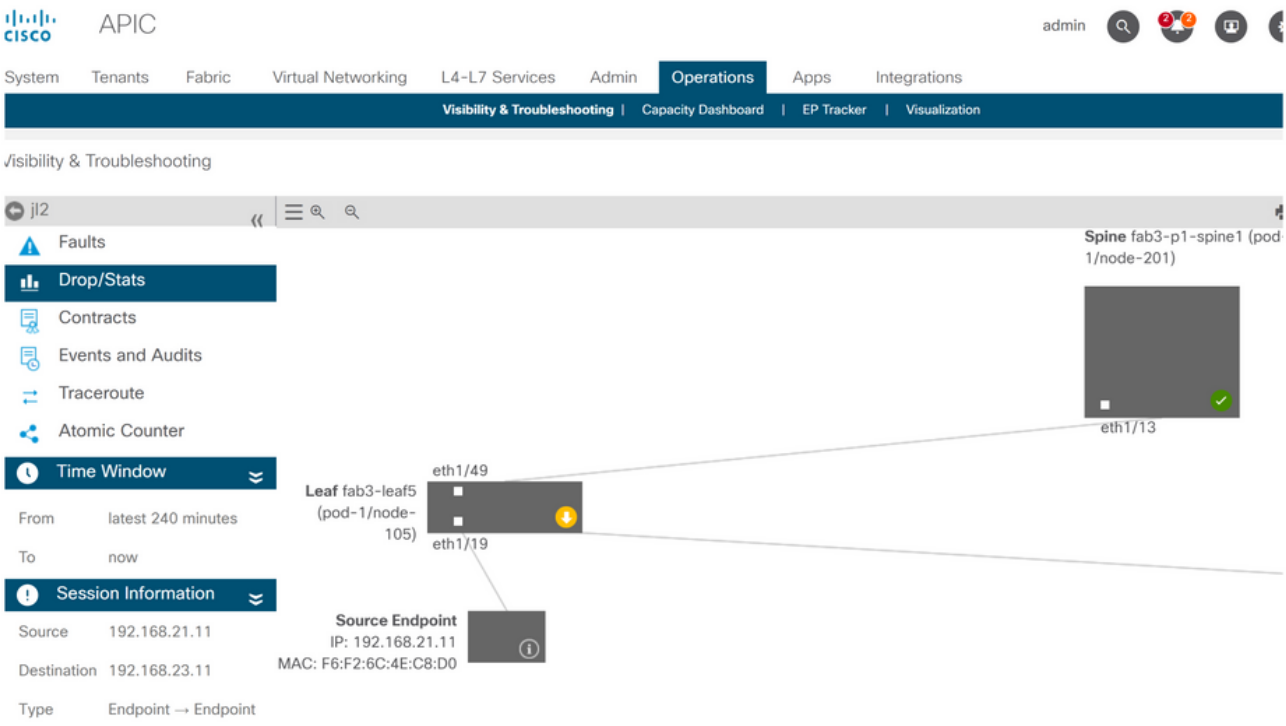


Configurez un nom de session, une source et un point de terminaison de destination. Cliquez ensuite sur Envoyer ou Générer un rapport.

L'outil recherche automatiquement les points d'extrémité dans le fabric et fournit des informations sur le locataire, le profil d'application et le groupe de terminaux auquel ces EP appartiennent.

Dans ce cas, il découvrira que les EP appartiennent au locataire Prod1, qu'ils appartiennent au même profil d'application « AppProf » et qu'ils sont affectés à des EPG différents : 'Web' et 'DB'.

Identification du rejet

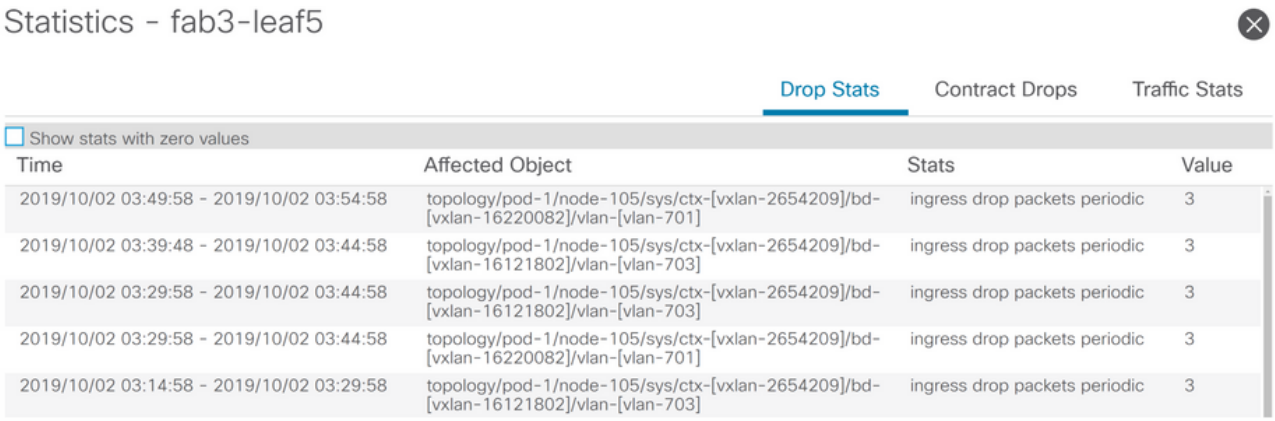


L'outil visualise automatiquement la topologie du scénario de dépannage. Dans ce cas, les deux points d'extrémité sont connectés au même commutateur leaf.

En naviguant jusqu'au sous-menu Drop/Stats, l'utilisateur peut afficher les drops généraux sur le noeud leaf ou spine en question. Reportez-vous à la section « Interface Drops » du chapitre « Intra-Fabric Forwarding » de ce manuel pour plus d'informations sur la compréhension des abandons pertinents.

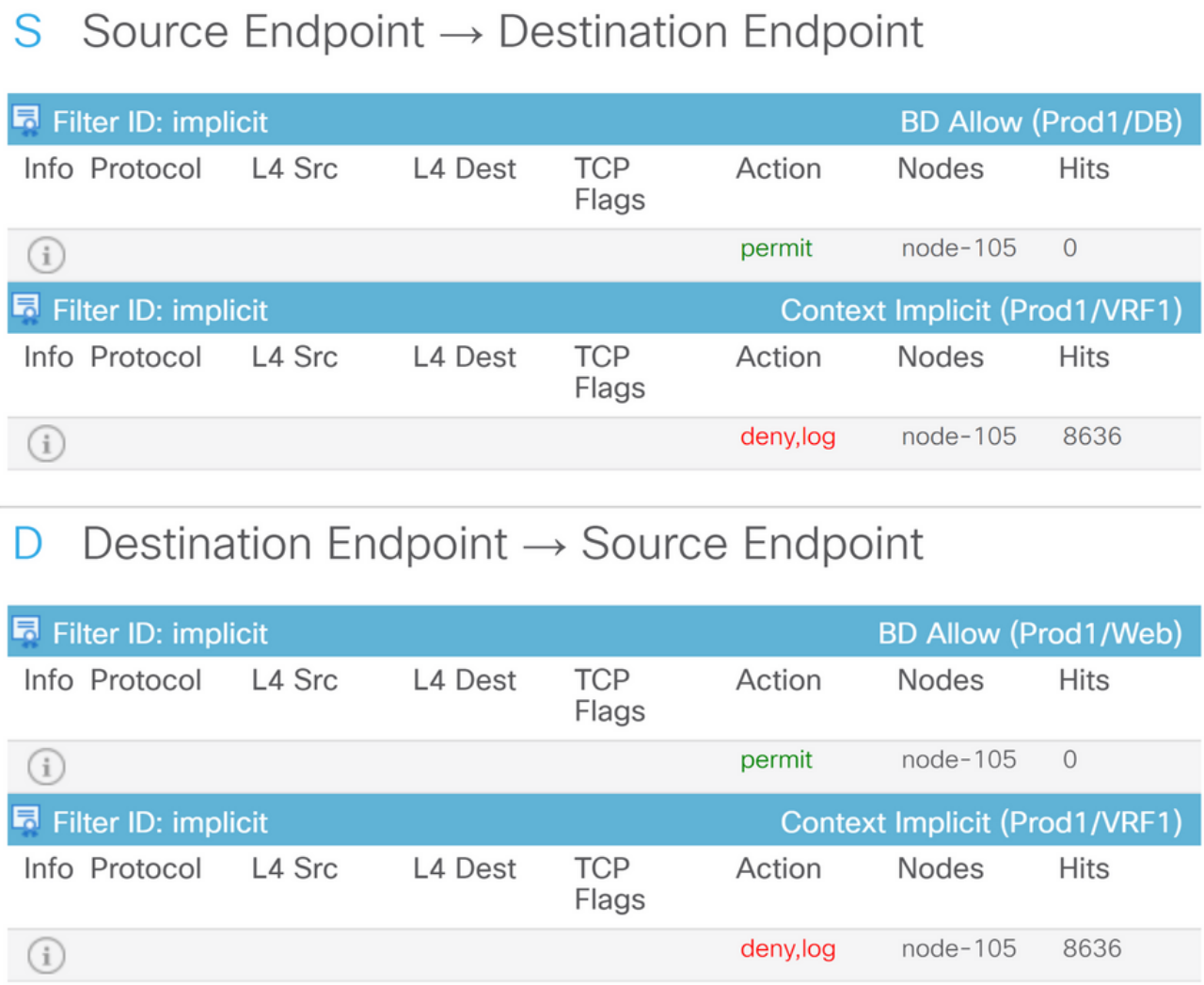
Beaucoup de ces abandons sont un comportement attendu et peuvent être ignorés.

Supprimer les détails



En effectuant une hiérarchisation vers le bas pour supprimer les détails à l'aide du bouton jaune « Packets drop » sur le schéma du commutateur, l'utilisateur peut afficher les détails du flux supprimé.

Détails de contrat



En accédant au sous-menu Contrats, l'utilisateur peut identifier le contrat à l'origine de l'abandon de la stratégie entre les groupes de terminaux. Dans l'exemple, il est implicite de refuser

Prod1/VRF1, ce qui indique certains résultats. Cela ne signifie pas nécessairement que le flux spécifié (192.168.21.11 et 192.168.23.11) rencontre ce refus implicite. Si la règle de refus implicite Hits of Context augmente, cela signifie qu'il y a du trafic entre Prod1/DB et Prod1/Web qui n'atteint aucun des contrats, donc qui sont abandonnés par le refus implicite.

Dans la vue Topologie du profil d'application sur le locataire > sélectionnez le nom du profil d'application sur la gauche > Topologie , il est possible de vérifier quels contrats sont appliqués à la DB EPG. Dans ce cas, aucun contrat n'est attribué à l'EPG :

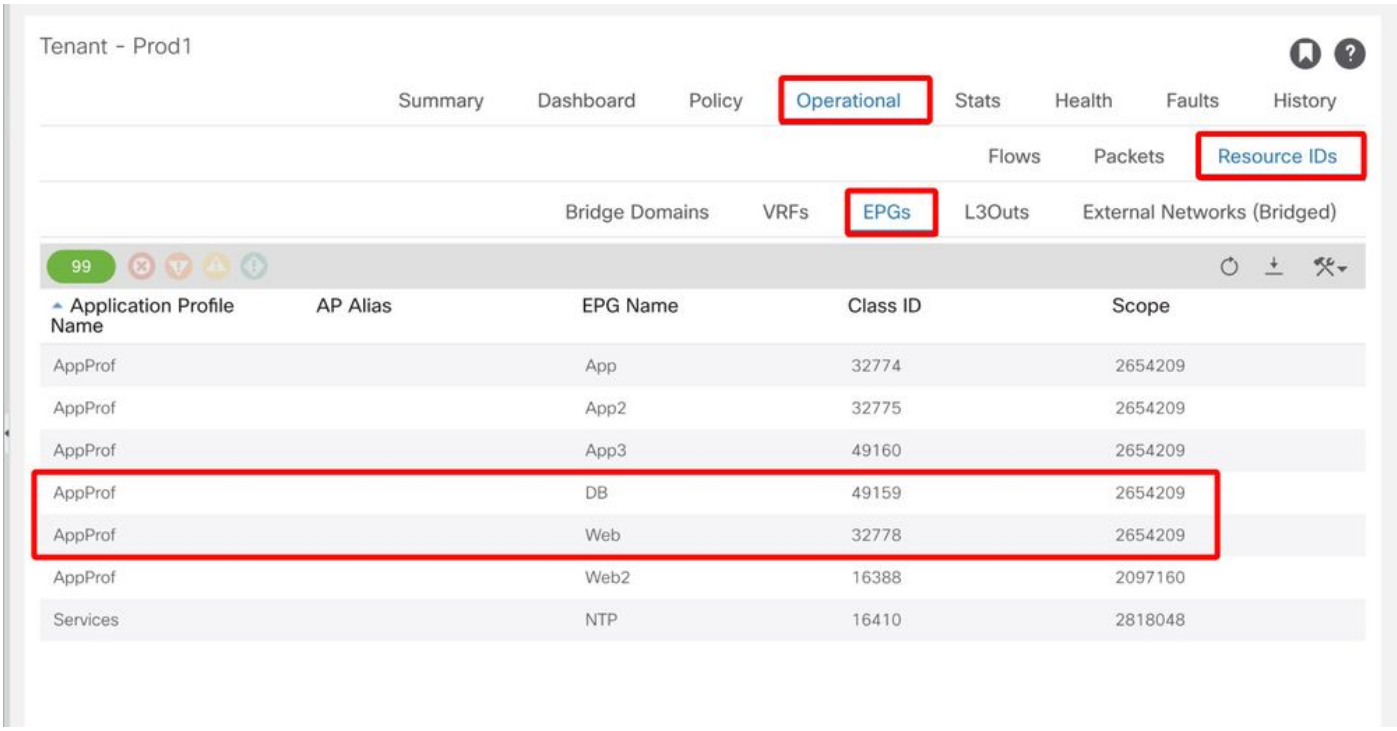
Visualisation du contrat

Maintenant que les EPG source et de destination sont connus, il est également possible d'identifier d'autres informations pertinentes, telles que :

- Le **pcTag** src/dst **EPG** des terminaux affectés. Le pcTag est l'ID de classe utilisé pour identifier un EPG avec une règle de zonage.
- Le **VRFVNID** src/dst**,** également appelé **portée**, des terminaux affectés.

L'ID de classe et l'étendue peuvent être facilement récupérés à partir de l'interface utilisateur graphique APIC en ouvrant le locataire > sélectionnez le nom du locataire sur la gauche > Opérationnel > ID de ressource > EPG

ID de ressource du locataire pour rechercher le pcTag et l'étendue EPG



Dans ce cas, l'ID de classe et les étendues sont :

- Web EPG pcTag 32778
- Portée Web EPG 2654209
- DB EPG pcTag 49159
- DB EPG portée 2654209

Vérifier la stratégie appliquée au flux de trafic en cours de dépannage

iBash

La ligne de commande iBash est un outil intéressant pour vérifier le paquet abandonné sur un leaf ACI : '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
```

Comme dans la sortie précédente, on peut voir que sur le commutateur leaf, de nombreux paquets ICMP provenant de l'EP 192.168.23.11 vers 192.168.21.11 ont été abandonnés.

L'outil contract_parser permet de vérifier les stratégies réelles appliquées au VRF auquel les terminaux sont associés :

```
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]
```

Cela peut également être vérifié par la règle de zonage programmée dans le leaf et les politiques appliquées par le commutateur.

```
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)       |
+---------+--------+--------+----------+----------------+---------+----------+------------+-----
-----+--------------------------+
```

Comme l'ont déjà constaté l'outil Visibilité et dépannage, l'outil contract_parser et les règles de zonage, le résultat confirme qu'il n'y a pas de contrat entre les groupes de terminaux source et de destination lors du dépannage. Il est facile de supposer que les paquets abandonnés correspondent à la règle de refus implicite 5155.

Capture ELAM

La capture ELAM fournit un rapport de niveau ASIC utilisé pour vérifier les détails de transmission qui indiquent, dans le cas d'un paquet abandonné, la raison de l'abandon. Lorsque la raison d'une perte est une perte de stratégie, comme dans ce scénario, le résultat de la capture ELAM ressemblera à ce qui suit.

Notez que les détails de la configuration d'une capture ELAM ne seront pas abordés dans ce chapitre. Reportez-vous au chapitre « Intra-Fabric Forwarding ».

```
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
```

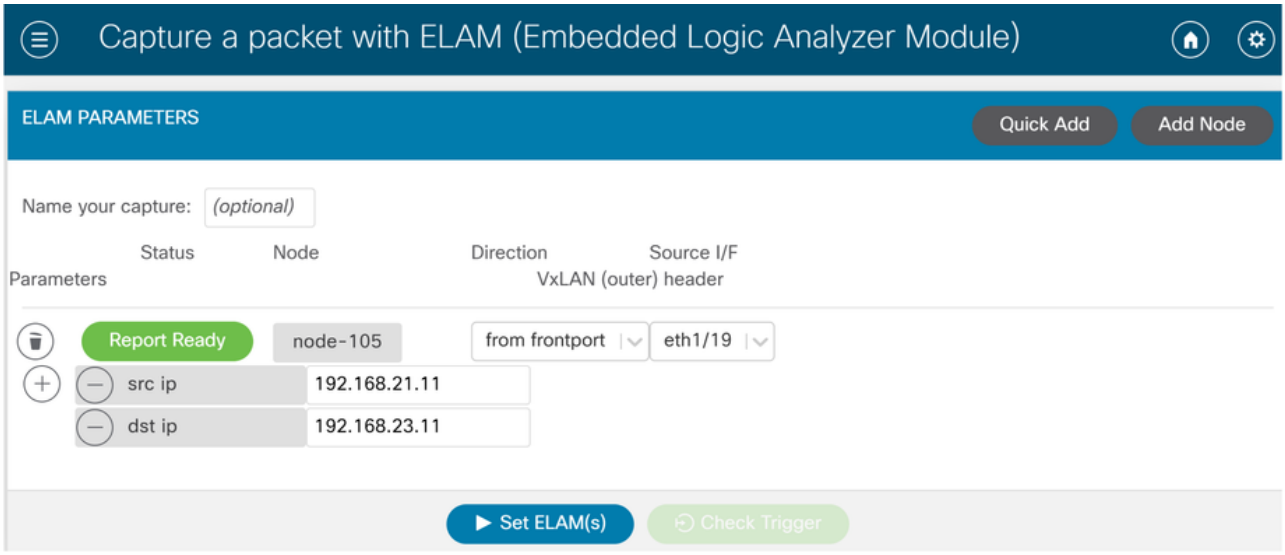
```
pkt.lu_drop_reason: 0x2D
```

Le rapport ELAM ci-dessus montre clairement que le paquet a été abandonné en raison d'une suppression de stratégie : 'GROUPE_SÉCURITÉ_REFUSER'

ELAM Assistant :

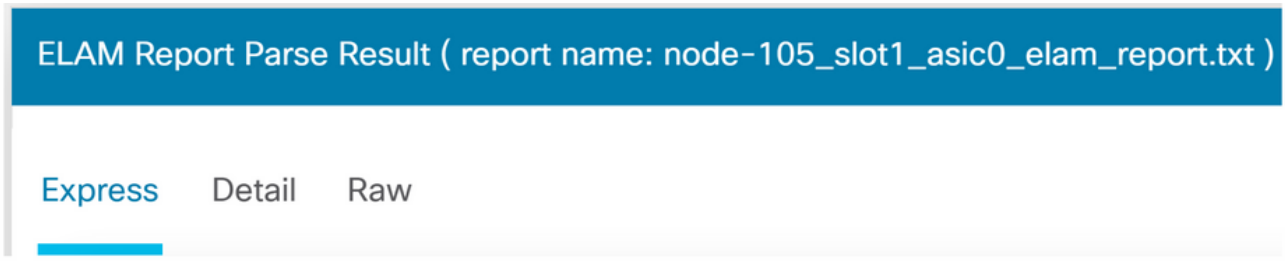
Le même résultat de la capture ELAM peut être affiché via l'application ELAM Assistant sur l'interface utilisateur graphique APIC.

Configuration



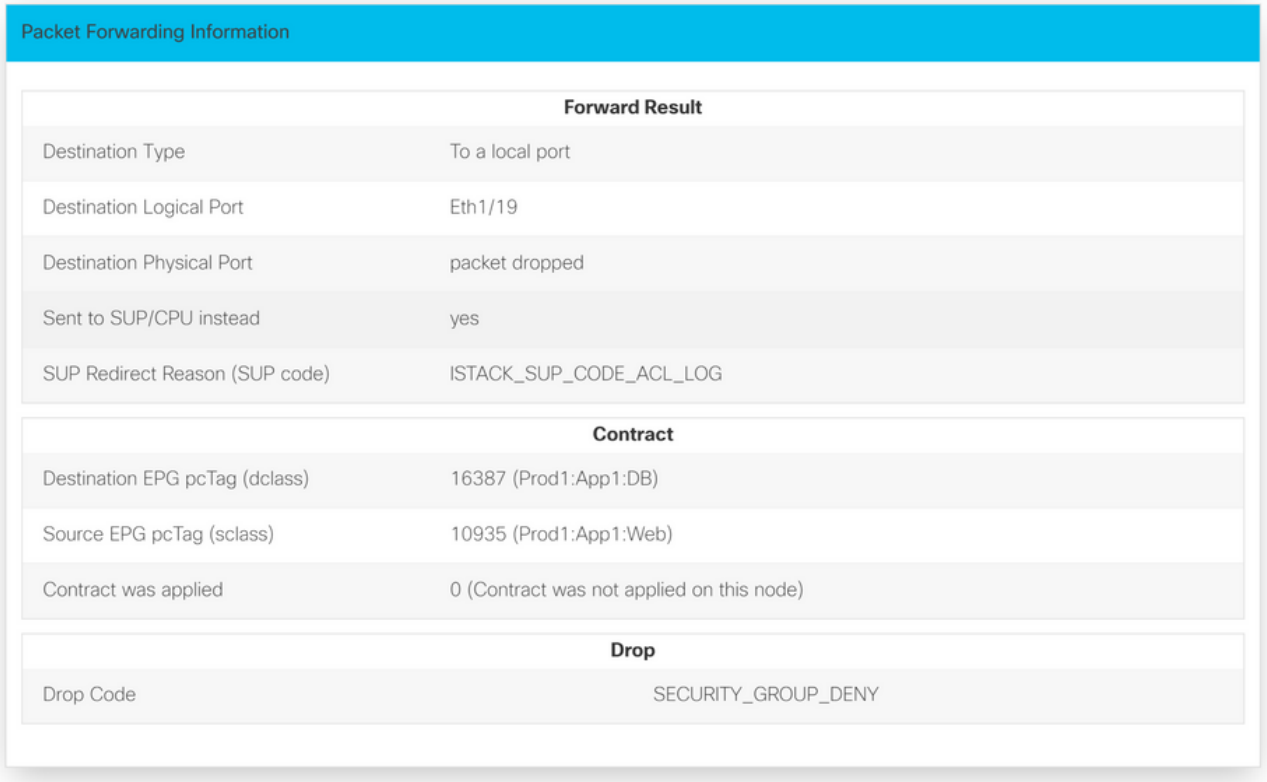
En général, l'utilisateur configure les détails de la source et de la destination pour le flux concerné. Dans cet exemple, src IP est utilisé pour capturer le trafic vers le point d'extrémité dans l'EPG de destination qui n'a pas de relation contractuelle avec l'EPG source.

Rapport Elam Assistant Express



Il existe trois niveaux de sortie qui peuvent être affichés avec ELAM Assistant. Express, Detail et Raw.

Rapport Elam Assistant Express (suite)



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

Sous le résultat express, le motif du code d'abandon SECURITY_GROUP_DENY indique que l'abandon est le résultat d'un résultat de contrat.

Groupe préféré

Àpropos des groupes préférentiels de contrats

Deux types d'application de stratégie sont disponibles pour les groupes de terminaux dans un VRF avec un groupe de préférences de contrat configuré :

- EPG inclus : Les groupes de terminaux peuvent communiquer librement entre eux sans contrat, s'ils appartiennent à un groupe privilégié par contrat. Elle est basée sur la règle par défaut source-any-destination-any-permit.
- EPG exclus : Les groupes de terminaux qui ne sont pas membres de groupes privilégiés nécessitent des contrats pour communiquer entre eux. Sinon, les règles de refus entre l'EPG exclu et tout EPG s'appliquent.

La fonction de groupe privilégié par contrat permet un meilleur contrôle de la communication entre les groupes de terminaux dans un VRF. Si la plupart des EPG du VRF doivent avoir une communication ouverte, mais que quelques-uns ne doivent avoir qu'une communication limitée avec les autres EPG, configurez une combinaison d'un groupe de préférence de contrat et de contrats avec des filtres pour contrôler plus précisément la communication inter-EPG.

Les groupes de terminaux exclus du groupe préféré ne peuvent communiquer avec d'autres groupes de terminaux que si un contrat est en place pour remplacer la règle par défaut source-any-destination-any-deny.

Programmation du groupe privilégié par contrat

Essentiellement, les groupes préférentiels de contrats sont l'inverse des contrats standard. Pour

les contrats standard, les règles de zonage d'autorisation explicites sont programmées avec une règle de zonage de refus implicite avec la portée VRF. Pour les groupes préférés, une règle de zonage PERMIT implicite est programmée avec la valeur de priorité numérique la plus élevée et des règles de zonage DENY spécifiques sont programmées pour interdire le trafic provenant de groupes de terminaux qui ne sont pas membres du groupe préféré. Par conséquent, les règles de refus sont évaluées en premier et si le flux ne correspond pas à ces règles, le flux est implicitement autorisé.

Il y a toujours une paire de règles de zonage de refus explicites pour chaque EPG en dehors du groupe préféré :

- Un élément du membre du groupe non préféré vers un pcTag (valeur 0).
- Un autre de pcTag (valeur 0) vers le membre du groupe non préféré.

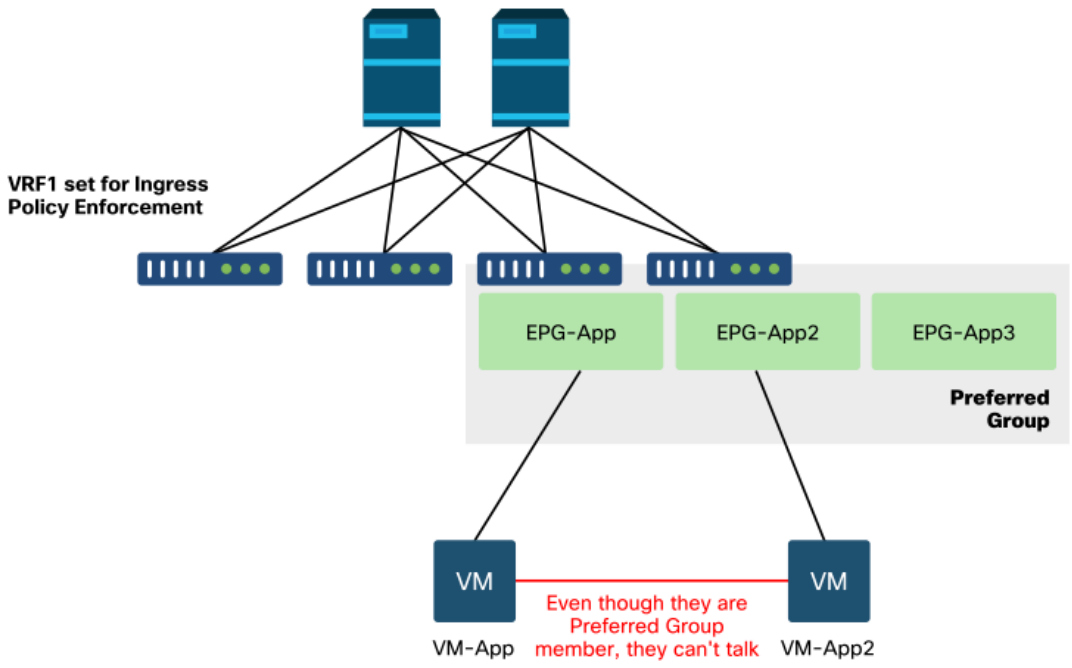
Scénario de dépannage du groupe préféré

La figure ci-dessous illustre une topologie logique dans laquelle les groupes de terminaux App, App2 et App3 sont tous configurés en tant que membres de groupe favoris.

VM-App fait partie d'EPG-App et VM-App2 fait partie d'EPG-App2. App et App2 EPG doivent faire partie de la préférence et donc communiquer librement.

VM-App initie un flux de trafic sur le port TCP 6000 vers VM-App2. EPG-App et EPG-App2 sont tous deux membres du groupe préféré dans le cadre de VRF1. VM-App2 ne reçoit jamais de paquets sur le port TCP 6000.

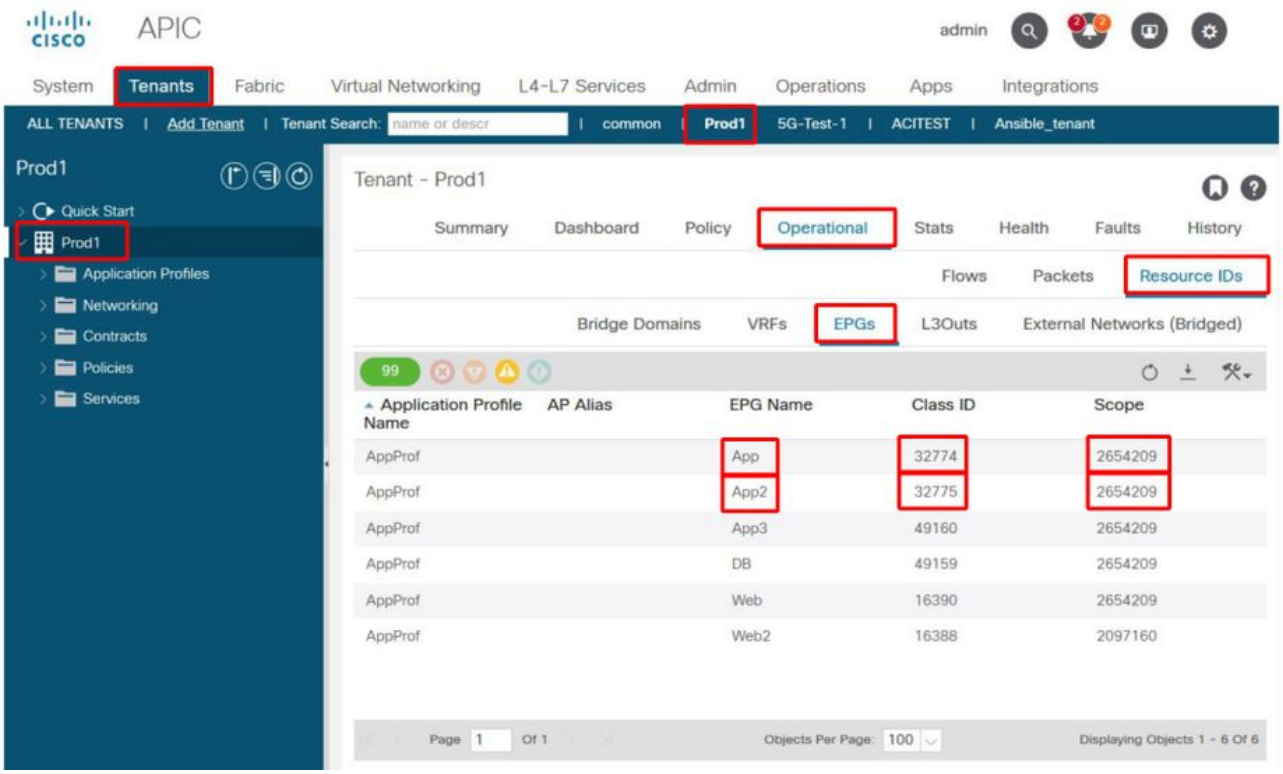
Topologie



Workflow

1. Recherchez le pcTag de l'application EPG et son VNID/étendue VRF

EPG et VRF pcTags



2. Vérifiez la programmation du contrat en utilisant contract_parser.py sur le leaf d'entrée

Utilisez contract_parser.py et/ou la commande « show zoning-rule » et spécifiez le 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-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]
[18:4130] [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]
```

En examinant le résultat ci-dessus, l'entrée d'autorisation implicite (ruleId 4165) avec la priorité la plus élevée de 20 est observée. Cette règle d'autorisation implicite autorise tous les flux de trafic, sauf s'il existe une règle de refus explicite avec une priorité inférieure interdisant le flux de trafic.

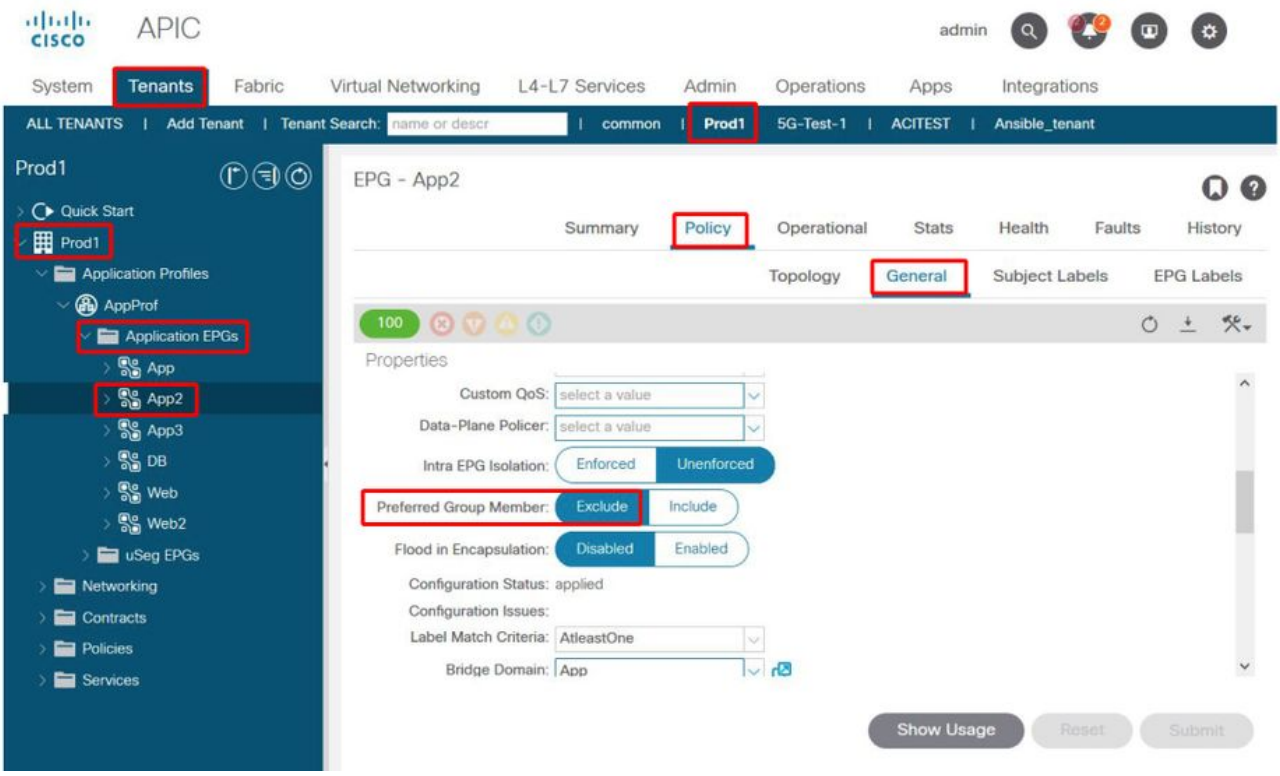
En outre, deux règles de refus explicites ont été observées pour pcTag 32775, qui est le pcTag d'EPG App2. Ces deux règles de zonage de refus explicites interdisent le trafic de tout EPG vers EPG App2, et vice versa. Ces règles ayant la priorité 18 et 19, elles seront prioritaires sur la règle d'autorisation par défaut.

La conclusion est que l'application EPG App2 n'est pas un membre du groupe préféré car les règles de refus explicites sont respectées.

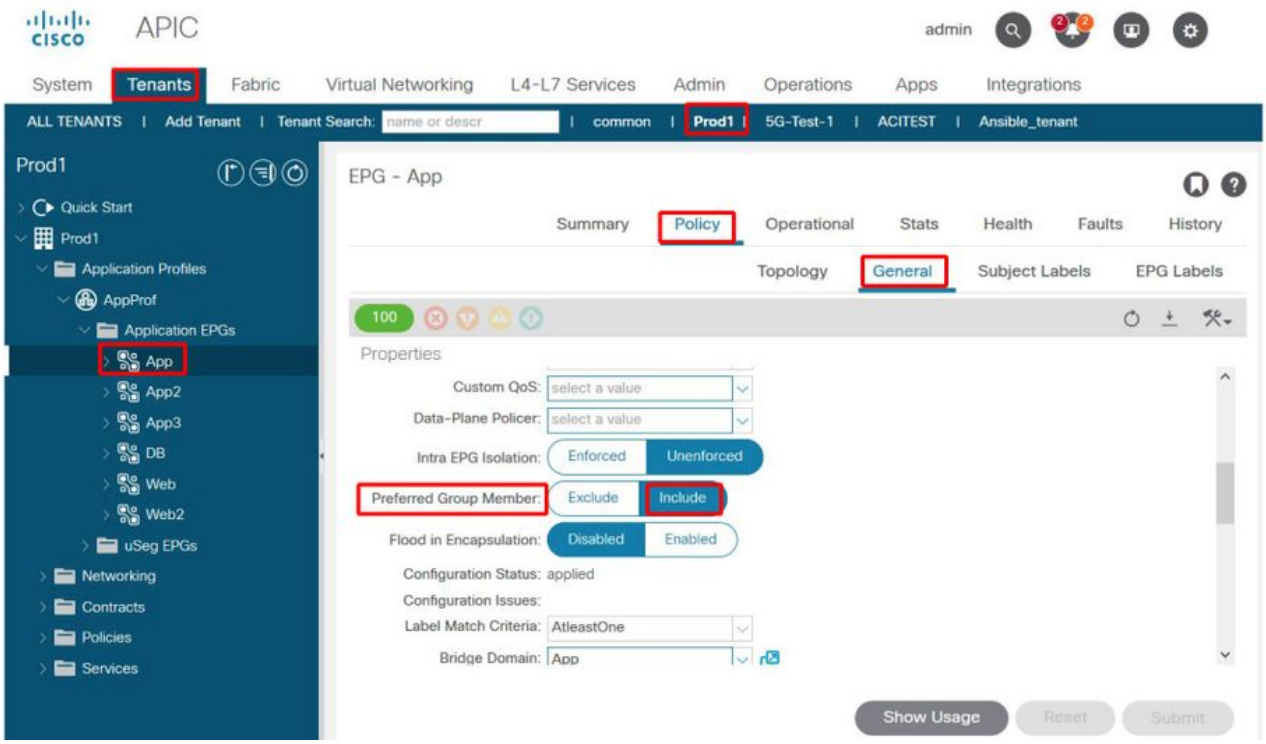
3. Vérifiez la configuration des membres du groupe EPG préféré

Naviguez dans l'interface graphique APIC et cochez EPG App2 et EPG App Preferred Group Member Configuration. Dans la figure suivante, voir EPG App2 n'est pas configuré en tant que membre du groupe préféré.

EPG App2 — Paramètre de membre du groupe préféré exclu



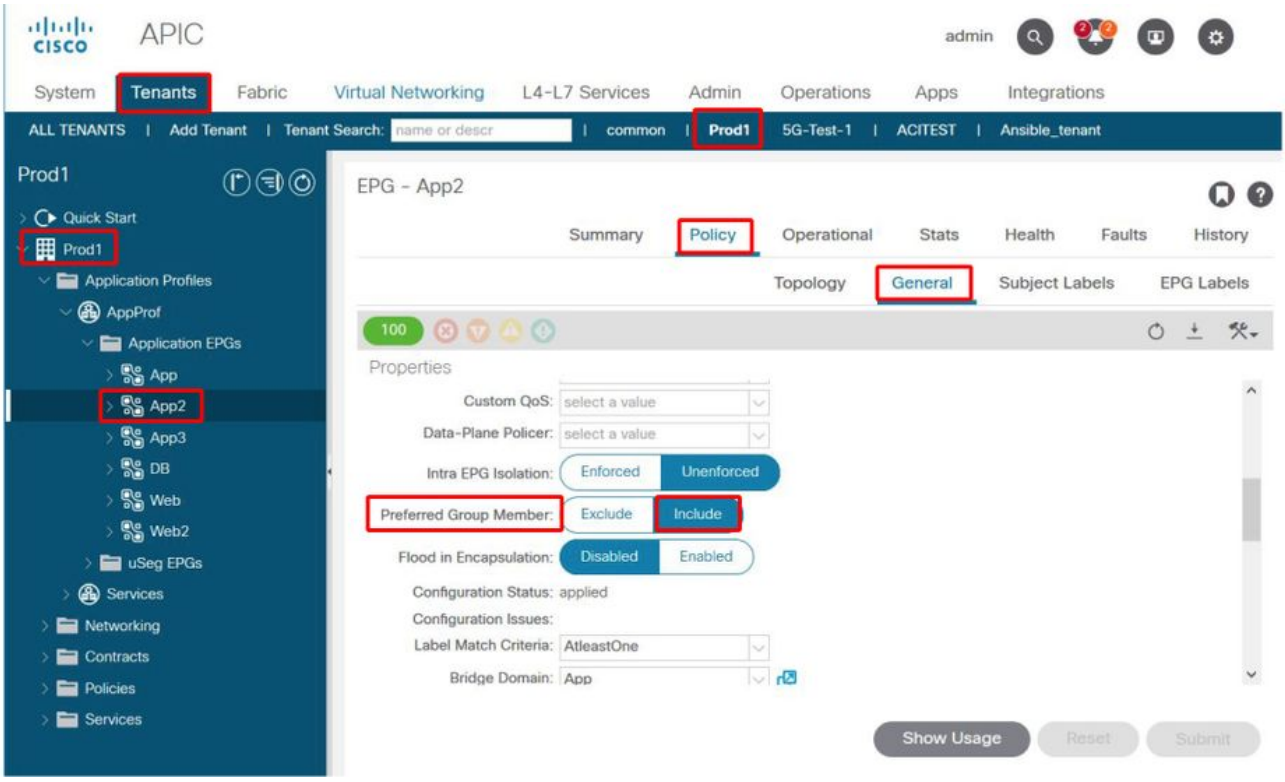
Application EPG — Paramètre de membre du groupe préféré inclus



4. Définissez l'application EPG App2 comme membre du groupe préféré

La modification de la configuration de l'EPG App2 permet au groupe préféré de communiquer librement dans le cadre du groupe préféré.

EPG App2 - Paramètre de membre du groupe préféré inclus



5. Vérifiez à nouveau la programmation des contrats à l'aide de contract_parser.py sur le leaf où se trouve l'EP src

Utilisez à nouveau contract_parser.py et spécifiez le nom VRF pour vérifier si les règles de refus explicites pour EPG App2 ont disparu.

```
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]
```

Les règles de refus explicites pour EPG App2 et son pcTag 32775 ne sont plus observées dans le résultat ci-dessus. Cela signifie que le trafic entre les EP dans l'application EPG et l'application EPG 2 correspondra désormais à la règle d'autorisation implicite (ruleId 4165) avec la priorité la plus élevée de 20.

vzAny vers EPG

Àpropos de vzAny

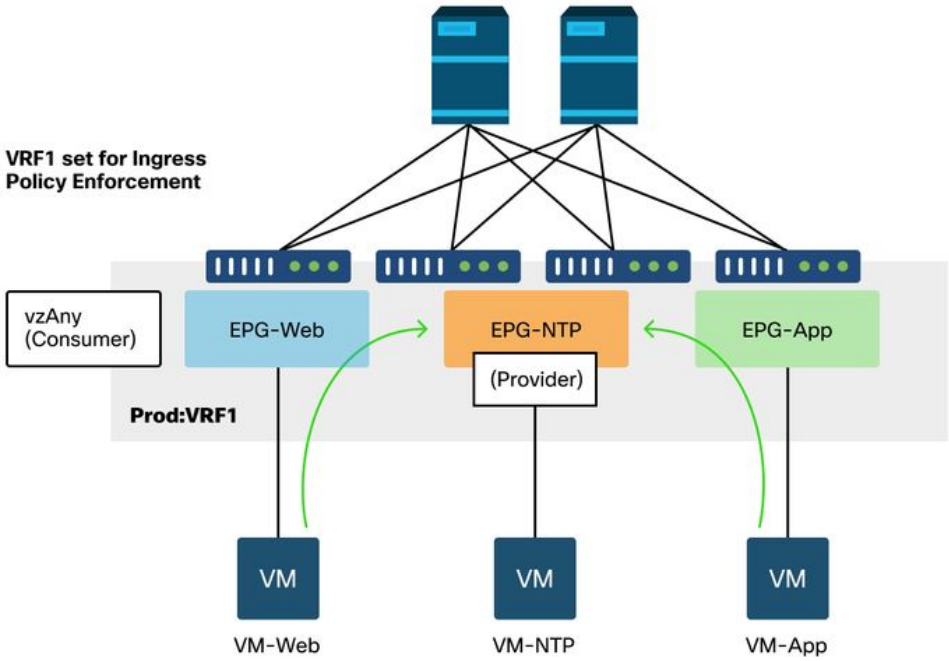
Lors de la configuration de contrats entre un ou plusieurs groupes de terminaux, les contrats

peuvent être configurés comme une relation consommée ou fournie. Lorsque le nombre de groupes de terminaux augmente, le nombre de relations contractuelles entre eux augmente également. Certains cas d'utilisation courants nécessitent que tous les EPG échangent des flux de trafic avec un autre EPG spécifique. Un tel cas d'utilisation pourrait être un EPG contenant des EP fournissant des services qui doivent être consommés par tous les autres EPG à l'intérieur du même VRF (NTP ou DNS par exemple). vzAny permet de réduire la charge opérationnelle lors de la configuration des relations contractuelles entre tous les EPG et les EPG spécifiques fournissant des services à utiliser par tous les autres EPG. En outre, vzAny permet une utilisation CAM de stratégie de sécurité beaucoup plus efficace sur les commutateurs Leaf, car seulement 2 règles de zonage sont ajoutées pour chaque relation de contrat vzAny.

Exemple d'utilisation

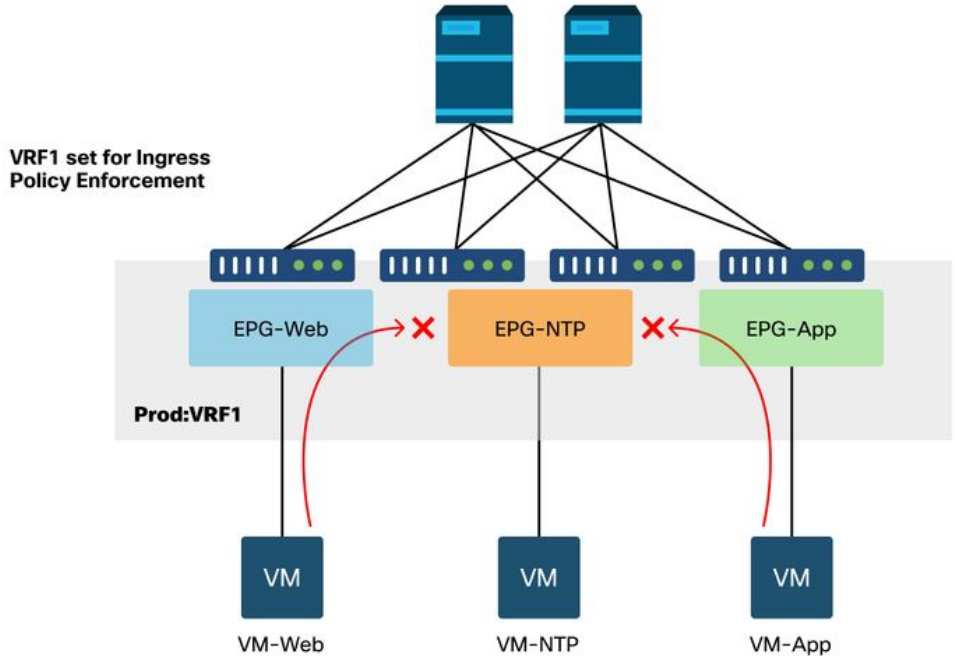
La figure ci-dessous décrit un tel cas d'utilisation dans lequel VM-Web et VM-App dans les EPG, Web et App doivent respectivement consommer les services NTP de VM-NTP dans EPG-NTP. Au lieu de configurer un contrat fourni sur EPG NTP, puis d'avoir le même contrat qu'un contrat consommé sur EPG Web et App, vzAny permet à chaque EPG dans VRF Prod : VRF1 de consommer les services NTP de EPG NTP.

vzAny — Tout EPG dans VRF Prod:VRF1 peut consommer des services NTP de EPG NTP



Imaginez un scénario dans lequel des abandons sont observés entre des EPG qui consomment les services NTP lorsqu'il n'y a pas de contrat entre eux.

Scénario de dépannage - Le trafic est interrompu en l'absence de contrat

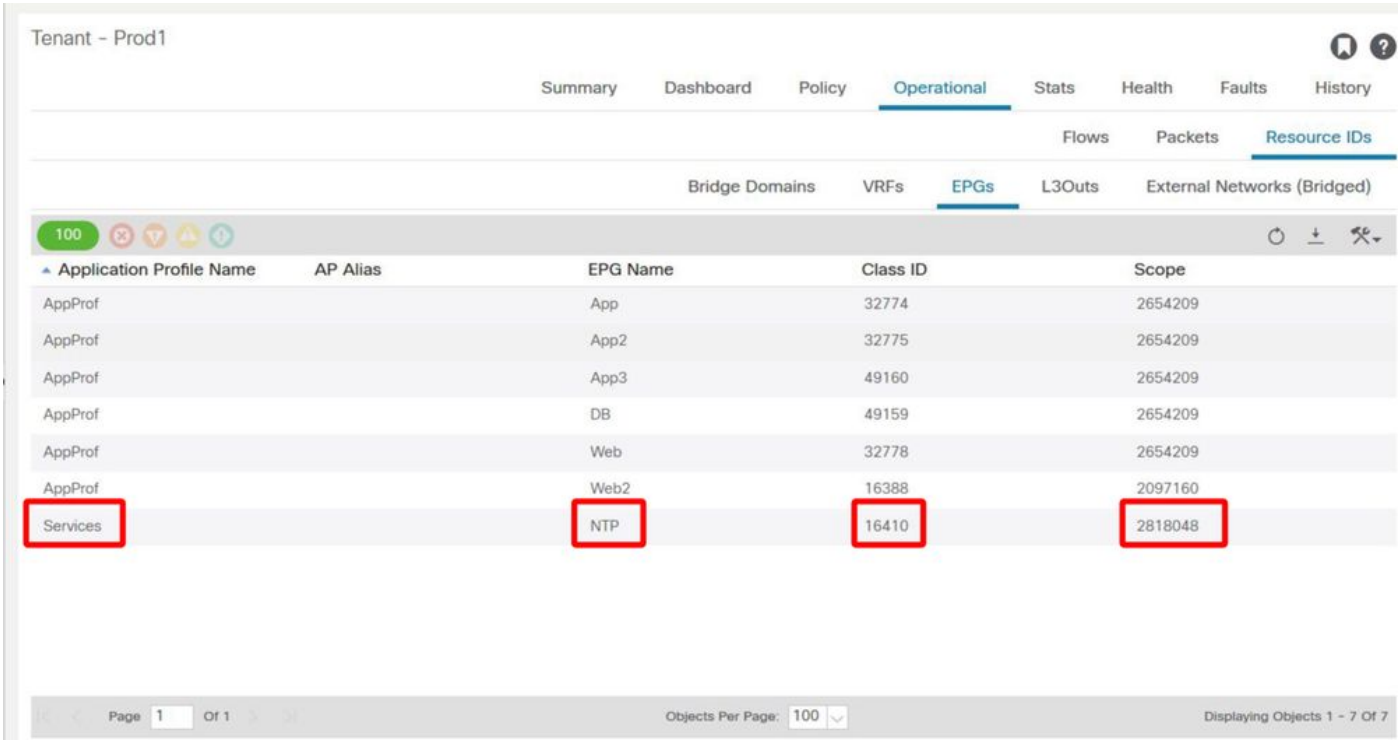


Workflow

1. Recherchez le pcTag de EPG NTP et son VNID/étendue VRF

'Tenant > Opérationnel > ID de ressource > EPG' permet de trouver le pcTag et la portée

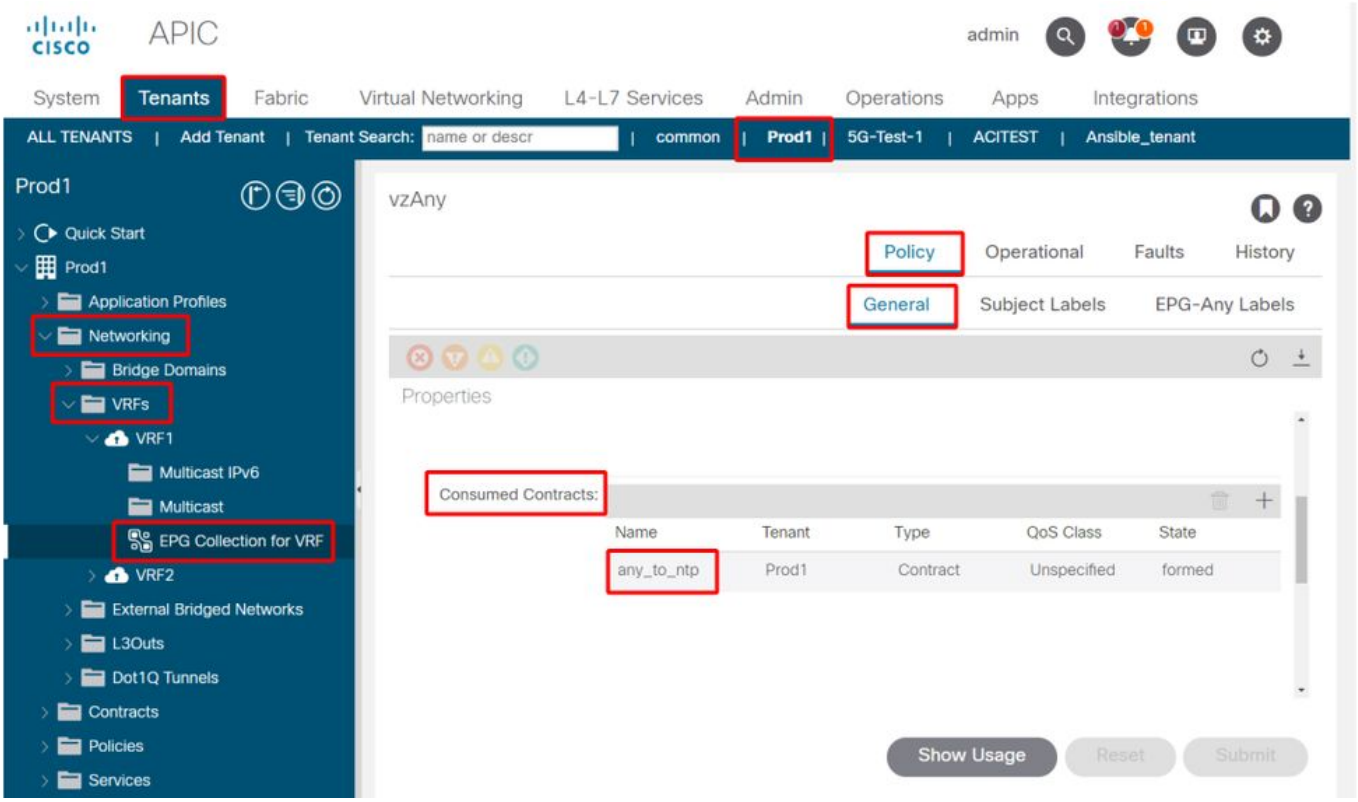
EPG NTP pcTag et son VNID/étendue VRF



2. Vérifiez si un contrat est configuré en tant que contrat vzAny consommé dans le cadre du VRF

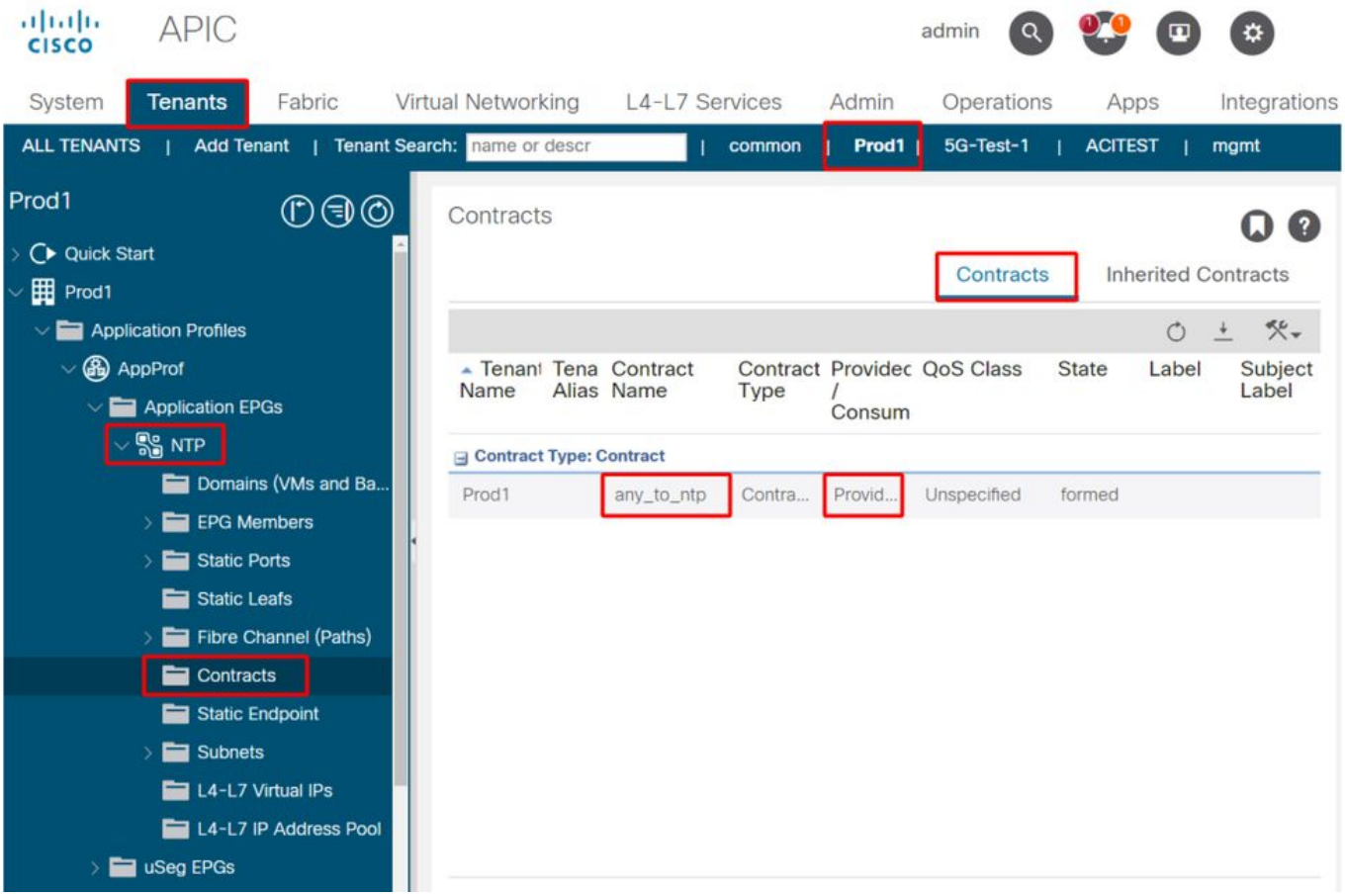
Accédez au VRF et vérifiez s'il existe un contrat consommé configuré en tant que vzAny dans la section « EPG Collection for VRF ».

Contrat configuré en tant que contrat vzAny consommé sur le VRF



3. Vérifier si le même contrat est appliqué en tant que contrat fourni sur EPG NTP

Pour établir une relation contractuelle, le même contrat doit être appliqué en tant que contrat fourni sur EPG NTP qui fournit des services NTP aux autres EPG dans son VRF.



4. Vérification de la règle de zonage sur le leaf d'entrée à l'aide de contract_parser.py ou de « show zoning-rule »

Le leaf d'entrée doit avoir 2 règles de zonage pour permettre des flux de trafic bidirectionnels (si l'objet du contrat est configuré pour autoriser les deux directions) entre n'importe quel EPG et NTP EPG. « N'importe quel EPG » est désigné par pcTag 0 dans la programmation de la règle de zonage.

L'utilisation de contract_parser.py ou des commandes « show zoning-rule » sur le leaf d'entrée tout en spécifiant le VRF permet de s'assurer que la règle de zonage est programmée.

Règles de zonage permettant le trafic vers/depuis EPG NTP à partir d'autres EPG dans le VRF présent

Utilisation de contract_parser.py et de « show zoning-rule » pour vérifier la présence des règles de zonage vzAny.

Ici, deux types de règles sont évidents :

1. Règle 4156 et règle 4168 qui autorisent Any à NTP et vice-versa. Ils ont la priorité 13 et 14 : Règle de zonage autorisant les flux de trafic de tout EPG (pcTag 0) vers EPG NTP (pcTag 49161).Règle de zonage autorisant les flux de trafic depuis EPG NTP (pcTag 46161) vers tout autre EPG (pcTag 0).
2. Règle 4165 qui est la règle « any to any deny » (par défaut) avec la priorité 21.

Étant donné que la priorité la plus basse a priorité, tous les EPG du VRF auront accès à l'EPG NTP.

```
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)  |
+---------+--------+--------+----------+---------+---------+---------+-----------+----------+--
--------------------+
```

Partagé L3Out vers EPG

Àpropos de Shared L3Out

Shared Layer 3 Out est une configuration qui permet d'avoir un L3Out dans un VRF fournissant certains services (accès externe) et un ou plusieurs autres VRF consomment ce L3Out. Vous trouverez plus de détails sur le routage L3Out partagé dans le chapitre « Routage externe ».

Lors de l'exécution de L3Out partagé, il est recommandé que le fournisseur du contrat soit L3Out partagé et que l'EPG soit le consommateur du contrat. Ce scénario sera illustré dans cette section.

Il n'est pas recommandé de faire l'inverse, c'est-à-dire L3Out utilisant un service fourni par un EPG. La raison en est l'évolutivité puisque pour les services partagés, les règles de zonage ne sont installées que sur le VRF consommateur. Les principes de consommation et de fourniture indiquent où les flux de trafic sont initiés. Avec l'application de la stratégie d'entrée par défaut, cela signifie que l'application de la stratégie sera appliquée du côté du consommateur et plus spécifiquement sur le leaf d'entrée (leaf non frontalier). Pour que le leaf d'entrée applique la

stratégie, il faut le pcTag de la destination. Dans ce scénario, la destination est le pcTag EPG externe. Le leaf d'entrée effectue ainsi l'application de la politique et transmet les paquets au leaf de bordure. Le leaf de bordure reçoit le paquet sur sa liaison de fabric qui effectue une recherche de route (LPM) et transfère le paquet sur la contiguïté pour le préfixe de destination.

Cependant, le leaf de bordure n'effectue AUCUNE application de stratégie lors de l'envoi du trafic sur l'EP de destination, ni sur le flux de trafic de retour vers l'EP source.

Par conséquent, seul le CAM de stratégie du leaf non BL entrant dispose d'entrées installées (dans le VRF client) et le CAM de stratégie du BL n'est pas affecté.

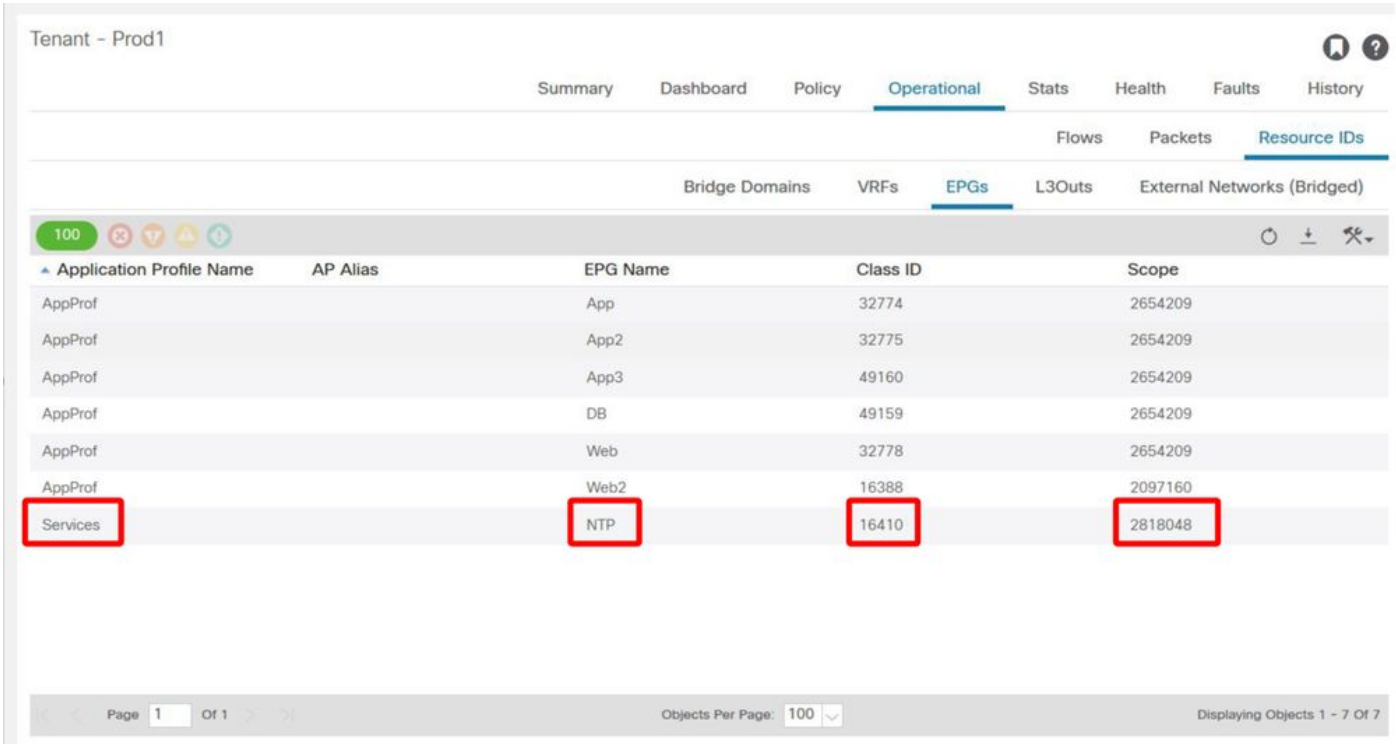
Dépannage d'une sortie L3 partagée

Workflow

1. Vérification de l'EPG pcTag et du VNID/étendue VRF pour l'EPG client

Avec l'option L3Out partagée, les règles de zonage sont uniquement installées dans le VRF consommateur. Le fournisseur doit avoir un pcTag global (inférieur à 16 Ko) qui permet à ce pcTag d'être utilisé dans tous les VRF grand public. Dans notre scénario, le fournisseur est l'EPG externe et aura un pcTag global. L'EPG consommateur aura un pcTag local comme d'habitude.

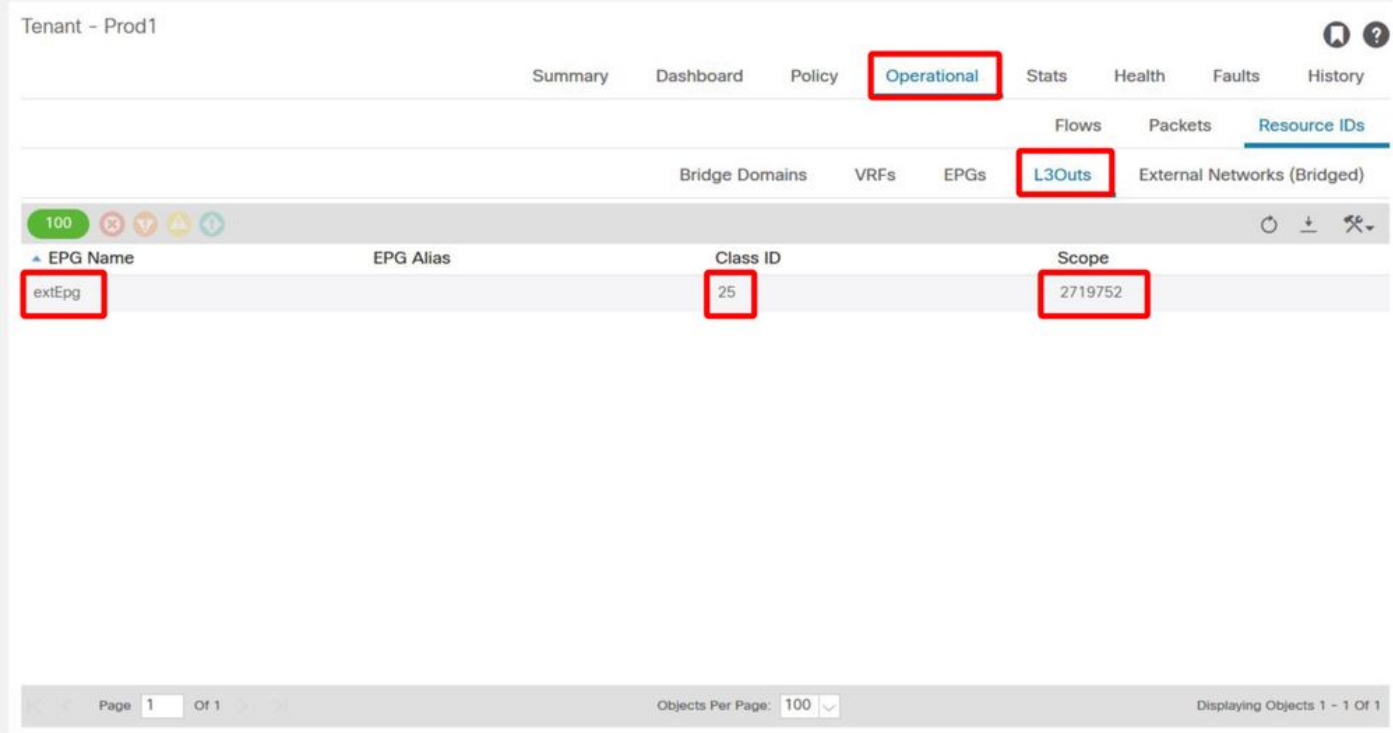
pcTag de l'EPG consommateur



2. Vérifiez le pcTag et le VNID/étendue VRF pour l'EPG L3Out du fournisseur

Comme indiqué à l'étape 1, le fournisseur L3Out EPG a une plage globale pcTag comme préfixes de L3Out qui sont divulgués dans le VRF consommateur. Par conséquent, l'EPG L3Out pcTag est nécessaire pour ne pas chevaucher pcTags dans le VRF consommateur, et il est donc dans la plage globale pcTag.

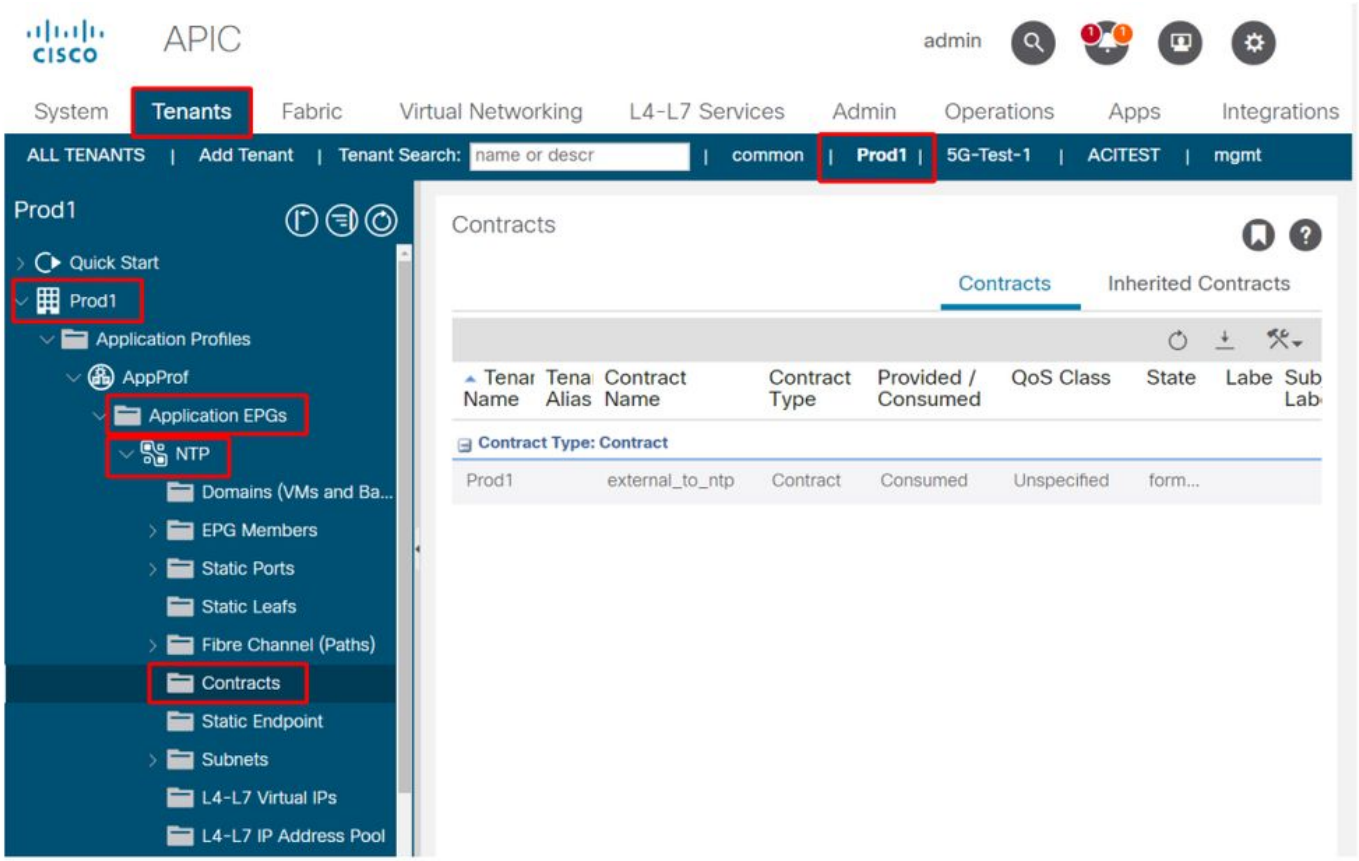
pcTag de l'EPG externe du fournisseur



3. Vérifiez que l'EPG client a un contrat étendu au locataire importé ou un contrat global configuré

Le NTP EPG client avec sous-réseau défini dans l'EPG/BD utilise le contrat étendu « locataire » ou « global »

Contrat consommé par EPG



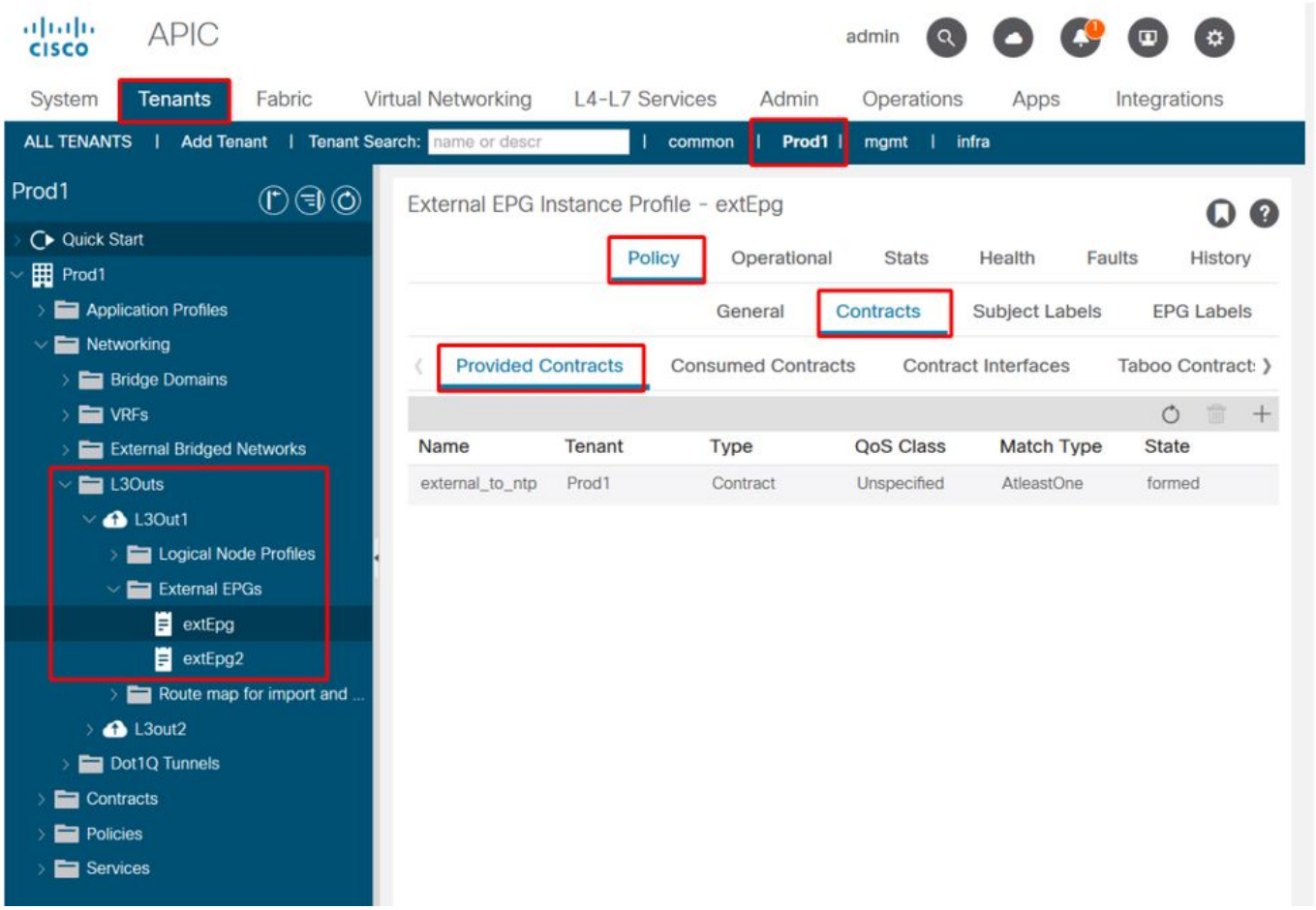
4. Vérifiez si le BD de l'EPG consommateur a un sous-réseau configuré avec son étendue définie sur « Partagé entre VRF »

Le sous-réseau de l'EPG est configuré sous le domaine de pont, mais doit avoir l'indicateur « shared between VRF » (pour autoriser les fuites routées) et l'indicateur « adverited external » (pour autoriser l'annonce à L3Out)

5. Vérifiez que l'EPG L3Out du fournisseur a un contrat étendu au locataire importé ou un contrat global configuré

L'EPG L3Out doit disposer d'un contrat de portée locataire ou d'un contrat global configuré en tant que contrat fourni.

Contrat sur le fournisseur L3Out



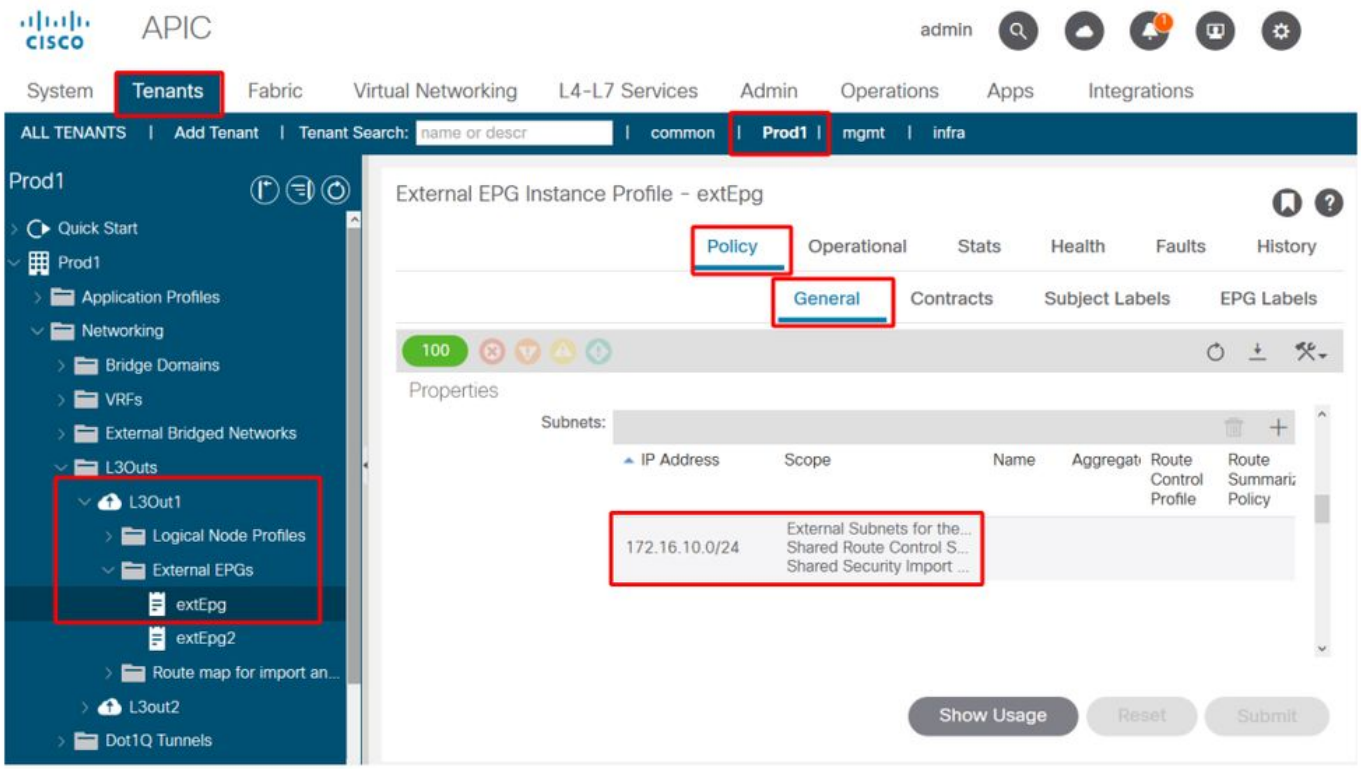
6. Vérifiez si le fournisseur L3Out EPG dispose d'un sous-réseau configuré avec les étendues nécessaires vérifiées

Le préfixe à fuiter doit être configuré pour l'EPG L3Out du fournisseur avec les étendues suivantes :

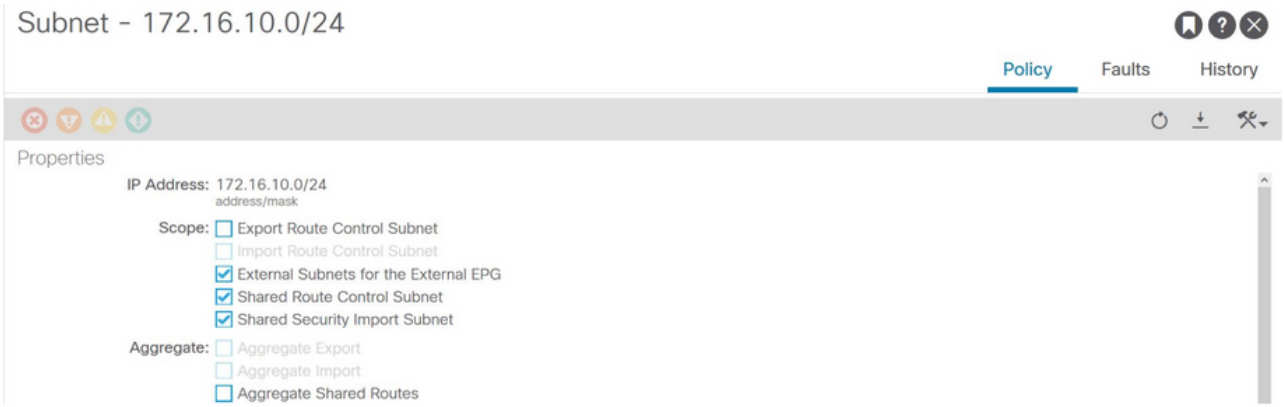
- Sous-réseaux externes pour l'EPG externe.
- Sous-réseau de contrôle de route partagé.
- Sous-réseau d'importation de sécurité partagée.

Pour plus de détails sur l'indicateur de sous-réseau dans L3Out EPG, reportez-vous au chapitre « External forwarding ».

Paramètres de sous-réseau EPG externe



Paramètres de sous-réseau EPG externe développés



7. Vérifiez le pcTag du sous-réseau L3Out EPG sur le non-BL pour le VRF consommateur

Lorsque le trafic destiné au sous-réseau EPG externe entre dans la non-BL, une recherche est effectuée sur le préfixe de destination pour déterminer le pcTag. Vous pouvez le vérifier à l'aide de la commande suivante sur la non-BL.

Notez que ce résultat est pris dans le cadre du VNI 2818048 qui est le VNID VRF du consommateur. En consultant la table, le consommateur peut trouver le pcTag de la destination, même s'il ne se trouve pas dans le même 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
```

La sortie ci-dessus montre la combinaison du sous-réseau EPG L3Out et de son pcTag global 25.

8. Vérifiez les règles de zonage programmées sur la non-BL pour le VRF consommateur

Utilisez la commande « contract_parser.py » ou « show zoning-rule » et spécifiez le VRF.

Sous les sorties de commande, deux règles de zonage sont installées pour autoriser le trafic de l'EPG client pcTag 16410 vers l'EPG L3Out global pcTag 25. Ceci est dans la portée 2818048, qui est la portée du VRF consommateur.

```
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. Vérifiez les règles de zonage programmées sur le BL pour le VRF fournisseur

Utilisez la commande « contract_parser.py » ou « show zoning-rule » et spécifiez le VRF. Les sorties de commande suivantes montrent qu'il n'y a **AUCUNE règle de zonage** spécifique dans le VRF fournisseur comme indiqué plusieurs fois auparavant.

Il est dans le domaine 2719752 qui est le domaine du fournisseur VRF.

```
border-leaf# show zoning-rule scope 2719752
+---------+--------+--------+----------+----------------+---------+---------+-------------+----
------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  |     Name    |
Action  |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+-------------+----
------+----------------------+
|   4134  | 10937  |   24   | default  | uni-dir-ignore | enabled | 2719752 | vrf1_to_vrf2 |
permit  |    src_dst_any(9)    |
|   4135  |   24   | 10937  | default  |     bi-dir     | enabled | 2719752 | vrf1_to_vrf2 |
permit  |    src_dst_any(9)    |
|   4131  |   0    |   0    | implicit |    uni-dir     | enabled | 2719752 |              |
deny,log |   any_any_any(21)    |
|   4130  |   0    |   0    | implarp  |    uni-dir     | enabled | 2719752 |              |
permit  |  any_any_filter(17)  |
|   4132  |   0    |   15   | implicit |    uni-dir     | enabled | 2719752 |              |
deny,log | any_vrf_any_deny(22) |
+---------+--------+--------+----------+----------------+---------+---------+-------------+----
------+----------------------+

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]
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.