Resolución de problemas de políticas de seguridad de ACI - Contratos

Contenido

Introducción

Este documento describe los pasos para comprender y resolver problemas de las políticas de seguridad de ACI, conocidas como contratos.

Antecedentes

El material de este documento se ha extraído del libro Troubleshooting Cisco Application Centric Infrastructure, Second Edition, en concreto, los capítulos **Security Policies - Overview**, Security Policies - Tools, **Security Policies - EPG to EPG**, **Security Policies - Preferred group** y Security Policies - vzAny to EPG .

Overview

La arquitectura de seguridad fundamental de la solución ACI sigue un modelo de lista de permisos. A menos que se configure un VRF en el modo **no aplicado**, todos los flujos de tráfico de EPG a EPG se descartan implícitamente. Tal como implica el modelo de lista de permisos listo para usar, la configuración VRF predeterminada está en el modo **forzado**. Los flujos de tráfico se pueden permitir o denegar explícitamente mediante la implementación de reglas de zonificación en los nodos del switch. Estas reglas de zonificación se pueden programar en una variedad de configuraciones diferentes dependiendo del flujo de comunicación deseado entre los grupos de

terminales (EPG) y el método utilizado para definirlos. Tenga en cuenta que las entradas de regla de zonificación no son stateful y normalmente permitirán/denegarán basándose en el puerto/socket dado dos EPG una vez que la regla se haya programado.

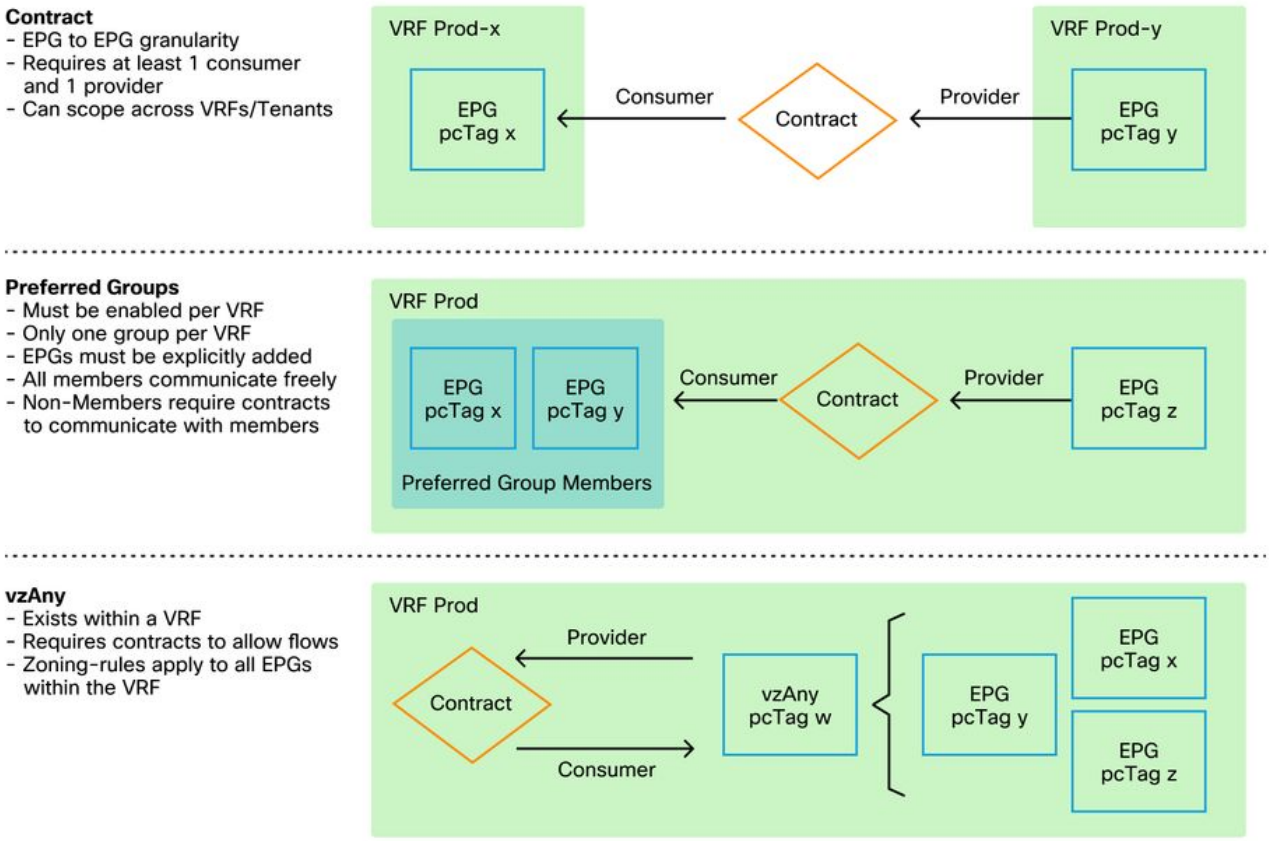
Métodos para programar reglas de zonificación

Los principales métodos para programar reglas de zonificación dentro de ACI son los siguientes:

- **Contratos de EPG a EPG:** normalmente se requiere al menos un consumidor y un proveedor para programar reglas de división en zonas en dos o más grupos de terminales distintos.
- **Grupos preferidos:** requiere habilitar la agrupación en el nivel VRF; solo puede existir un grupo por VRF. Todos los miembros del grupo pueden comunicarse libremente. Los no miembros requieren contratos para permitir flujos al grupo preferido.
- **vzAny:** Una 'colección EPG' definida en un VRF determinado. vzAny representa todos los EPG del VRF. El uso de vzAny permite flujos entre un EPG y todos los EPG dentro del VRF a través de una conexión de contrato.

El siguiente diagrama se puede utilizar para hacer referencia a la granularidad de la regla de zonificación que cada uno de los métodos anteriores permite para el control:

Comparación entre metodologías de reglas de zonificación



Si bien se utiliza el método contractual de programar reglas de zonificación, existe una opción para definir el alcance del contrato. Esta opción se debe considerar detenidamente si se requiere algún diseño de servicio compartido o con fuga de ruta. Si lo que se desea es pasar de un VRF a otro dentro del fabric de ACI, el método consiste en recurrir a contratos.

Los valores de ámbito pueden ser los siguientes:

- **Aplicación:** una relación de proveedor/consumidor de contrato sólo programará reglas entre los EPG definidos en el mismo perfil de aplicación. La reutilización del mismo contrato en otros EPG de perfiles de aplicación no permitirá interferencias entre ellos.
- **VRF (valor por defecto):** una relación de consumidor/proveedor de contrato programará reglas entre los EPG definidos en el mismo VRF. La reutilización del mismo contrato en otros EPG de perfiles de aplicación permitirá la interacción entre ellos. Asegúrese de que solo se permiten los flujos deseados; de lo contrario, debe definirse un nuevo contrato para evitar la interferencia involuntaria.
- **Arrendatario:** una relación de consumidor/proveedor contractual programará reglas entre los EPG que se definen dentro del mismo arrendatario. Si hay EPG vinculados a varios VRF dentro de un único arrendatario y consumen/proporcionan el mismo contrato, este alcance se puede utilizar para inducir la fuga de ruta para permitir la comunicación entre VRF.
- **Global:** una relación contractual entre un consumidor y un proveedor programará reglas entre los EPG en cualquier arrendatario dentro de un fabric de ACI. Este es el ámbito de aplicación más amplio posible de la definición, y se debe tener mucho cuidado cuando se habilita en contratos previamente definidos para evitar fugas de flujo no intencionales.

Lectura de una entrada de regla de zonificación

Una vez que la regla de zonificación está programada, aparecerá como la siguiente en una hoja:

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

- **ID de regla:** el ID de la entrada de regla. Ningún significado real más que actuar como identificador único.
- **Src EPG:** un ID único por VRF (pcTag) del grupo de terminales de origen.
- **EPG de destino:** un ID único por VRF (pcTag) del grupo de terminales de destino.
- **FilterID:** el ID del filtro con el que la regla está intentando coincidir. El filtro contiene la información de protocolo con la que coincidirá la regla.
- **Dir:** direccionalidad de la regla de zonificación.
- **OperSt:** el estado operativo de la regla.
- **Ámbito:** un identificador único del VRF con el que coincidirá la regla.
- **Nombre:** el nombre del contrato que dio lugar a la programación de esa entrada.
- **Acción:** qué hará la hoja cuando coincida con esa entrada. Incluye: [Drop, Permit, Log, Redirect].
- **Prioridad:** el orden en que se validarán las reglas de zonificación para la acción dada una coincidencia de Ámbito, SrcEPG, DstEPG y Entradas de filtro.

Memoria direccionable por contenido de políticas (CAM)

A medida que cada regla de zonificación se programa, una matriz de la entrada de regla de zonificación asignada contra las entradas de filtro comenzará a consumir **Policy CAM** en los switches. Al diseñar flujos permitidos a través de un fabric de ACI, se debe tener especial cuidado

al reutilizar los contratos, en lugar de crear otros nuevos, en función del diseño final. La reutilización accidental del mismo contrato en varios EPG sin comprender las reglas de zonificación resultantes puede derivar rápidamente en varios flujos permitidos de forma inesperada. Al mismo tiempo, estos flujos involuntarios seguirán consumiendo Policy CAM. Cuando el Policy CAM se llena, la programación de la regla de zonificación comenzará a fallar, lo que puede resultar en una pérdida inesperada e intermitente dependiendo de la configuración y los comportamientos de los terminales.

Filtración de VRF, pcTags globales y direccionalidad de aplicación de políticas de L3Outs compartidas

Se trata de un aviso especial para el caso práctico de los servicios compartidos, que requiere que se configuren los contratos. Los servicios compartidos normalmente implican tráfico entre VRF dentro de un fabric de ACI que se basa en el uso de un contrato de ámbito 'arrendatario' o 'global'. Para entender esto por completo, primero hay que reforzar la idea de que el valor de pcTag típico asignado a los EPG no es globalmente único. Las pcTags se asignan a un VRF y la misma pcTag podría reutilizarse dentro de otro VRF. Cuando surja el debate sobre la fuga de rutas, empiece a aplicar requisitos en el fabric de ACI, incluida la necesidad de valores globales únicos, como subredes y etiquetas de pc.

Lo que hace que esto sea una consideración especial es el aspecto de direccionalidad vinculado a que un EPG sea un consumidor frente a un proveedor. En un escenario de servicios compartidos, normalmente se espera que el proveedor dirija una pcTag global para obtener un valor único de fabric. Al mismo tiempo, el consumidor conservará su pcTag con alcance VRF, lo que lo coloca en una posición especial para poder programar y comprender el uso del valor global pcTag para aplicar políticas.

Como referencia, el intervalo de asignación de pcTag es el siguiente:

- Sistema reservado: 1-15.
- Ámbito global: 16-16384 para EPG de proveedores de servicios compartidos.
- Ámbito local: 16385-65535 para EPG de alcance VRF.

Dirección de aplicación de control de políticas VRF

En cada VRF es posible definir la configuración de dirección de aplicación.

- El valor predeterminado de la dirección de aplicación es Ingress.
- La otra opción para la dirección de aplicación es Egress.

La comprensión de dónde se aplica la política depende de varias variables diferentes.

La tabla siguiente ayuda a comprender dónde se aplica la política de seguridad en el nivel de hoja.

¿Dónde se aplica la política?

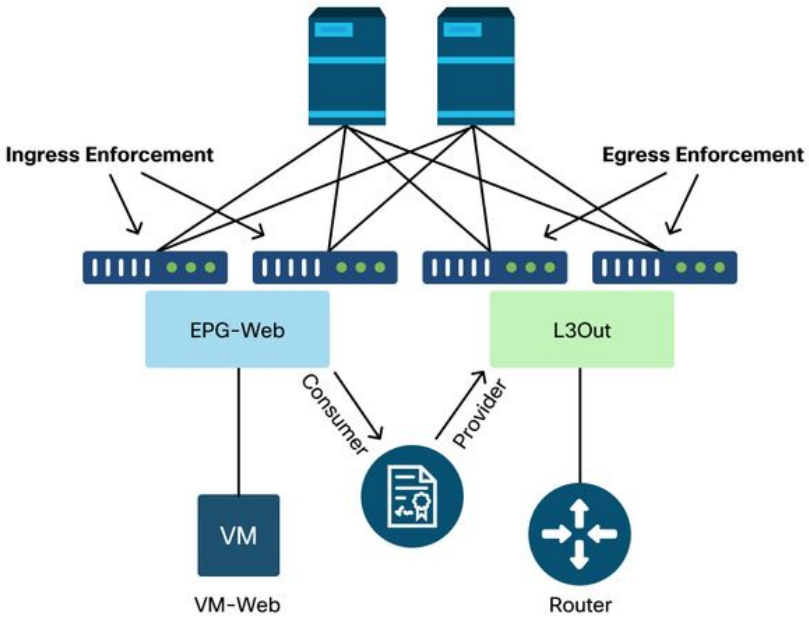
Situación	modo de aplicación VRF	Consumidor	Proveedor	Política aplicada el
Intra-VRF	Entrada/salida	EPG	EPG	·Si se descubre el terminal de destino: hoja de ingreso* ·Si no se aprende el punto final de

				destino: hoja de salida
	Acceso	EPG	L3Out EPG	Hoja de consumidor (hoja no fronteriza)
	Acceso	L3Out EPG	EPG	Hoja de proveedor (hoja no fronteriza)
	Egress	EPG	L3Out EPG	Tráfico de hoja fronterizo -> no fronterizo
	Egress	L3Out EPG	EPG	·Si se descubre el terminal de destino: hoja de borde ·Si no se aprende el punto final de destino: hoja no fronteriza Tráfico de hoja no fronterizo -> tráfico de hoja fronterizo ·Hoja fronteriza
	Entrada/salida	L3Out EPG	L3Out EPG	Hoja de ingreso*
	Entrada/salida	EPG	EPG	Hoja de consumidor
	Entrada/salida	EPG	L3Out EPG	Hoja de consumidor (hoja no fronteriza)
Inter-VRF	Entrada/salida	L3Out EPG	EPG	Hoja de ingreso*
	Entrada/salida	L3Out EPG	L3Out EPG	Hoja de ingreso*

*La aplicación de políticas se aplica en la primera hoja que recibe el paquete.

La figura siguiente ilustra un ejemplo de aplicación de contratos en el que EPG-Web como consumidor y L3Out EPG como proveedor tienen un contrato intra-VRF. Si VRF se establece en el modo de aplicación Ingress, los nodos de hoja en los que reside EPG-Web aplican la política. Si VRF se establece en el modo de aplicación Egress, la política se aplica en los nodos de hoja de borde en los que reside L3Out si se aprende el extremo web de VM en la hoja de borde.

Aplicación de entrada y aplicación de salida



Herramientas

Hay una variedad de herramientas y comandos que se pueden utilizar para ayudar en la identificación de una **caída** de **política**. Un descarte de política se puede definir como un descarte de paquete debido a una configuración de contrato o a la ausencia de esta.

Validación de regla de zonificación

Las siguientes herramientas y comandos se pueden utilizar para validar explícitamente las reglas de zonificación que se programan en los switches de hoja como resultado de las relaciones de consumidor/proveedor de contrato completadas.

'show zoning-rules'

Un comando switch level que muestra todas las reglas de zonificación en su lugar.

```
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 que contiene la información de deporte/deportación sobre la que actúa la regla de zonificación. La programación del filtro se puede verificar con este 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'

Este comando se puede ejecutar para verificar el número de aciertos por regla de zonificación. Esto es útil para determinar si una regla esperada está siendo alcanzada en lugar de otra, como una regla de descarte implícita que puede tener una prioridad más 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'

Un comando de nivel de switch que se puede ejecutar en el nivel iBash que informa caídas relacionadas con ACL (contrato) e información relacionada con el flujo que incluye:

- VRF
- VLAN-ID
- MAC de origen/MAC de destino
- IP de origen/IP de destino
- Puerto de origen/Puerto de destino
- Interfaz de origen

```
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

Una secuencia de comandos de Python en el dispositivo que produce una salida que correlaciona las reglas de zonificación, los filtros y las estadísticas de aciertos mientras se realizan búsquedas de nombres de ID. Esta secuencia de comandos es extremadamente útil, ya que toma un proceso de varios pasos y lo convierte en un solo comando que se puede filtrar a EPG/VRF específicos o a otros valores relacionados con el contrato.

```
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]
```

Validación de clasificación de paquetes

ELAM

Informe de nivel ASIC utilizado para comprobar los detalles de reenvío que indica, en el caso de un paquete descartado, el motivo del descarte. Relevante para esta sección, el motivo puede ser SECURITY_GROUP_DENY (caída de política de contrato).

fTriage

Utilidad basada en Python en el APIC que puede realizar un seguimiento del flujo de paquetes de extremo a extremo con ELAM.

Aplicación Asistente de ELAM

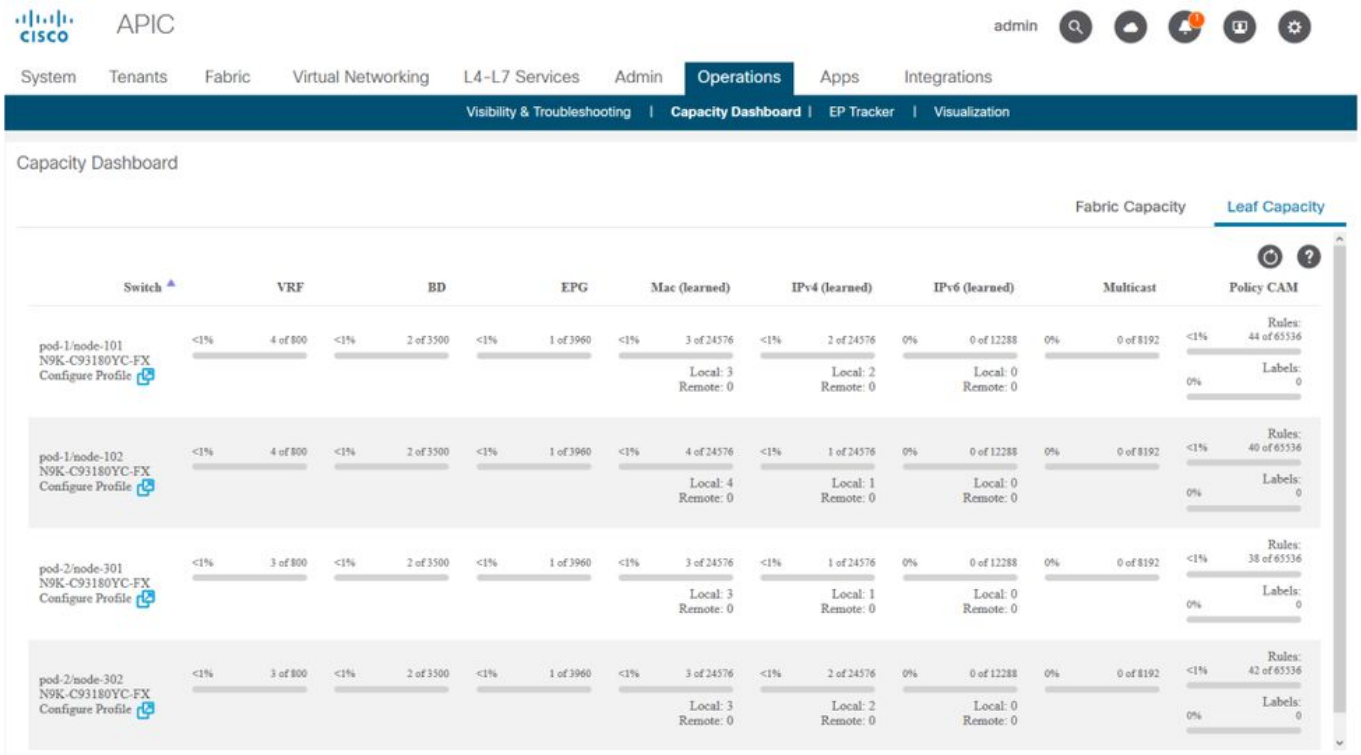
Una aplicación APIC que abstrae la complejidad de varios ASIC para que la inspección de decisiones de reenvío sea mucho más cómoda y fácil de usar.

Consulte la sección "Reenvío dentro del fabric" para obtener más información sobre las herramientas auxiliares de ELAM, fTriage y ELAM

Uso de CAM de políticas

El uso de políticas CAM por hoja es un parámetro importante que se debe supervisar para garantizar que el fabric se encuentre en un estado correcto. La forma más rápida de supervisar esto es utilizar el 'Panel de capacidad' en la GUI y comprobar explícitamente la columna 'Cámara de políticas'.

La vista "Capacidad de hoja" del panel de capacidad



'show platform internal hal health-stats'

Este comando es útil para validar una variedad de límites de recursos y uso, incluido Policy CAM. Tenga en cuenta que este comando sólo se puede ejecutar en vsh_lc, así que páselo usando el indicador '-c' si se ejecuta desde 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 a EPG

Consideraciones sobre el descarte de políticas genéricas

Existen numerosas formas de solucionar un problema de conectividad entre dos terminales. La siguiente metodología proporciona un buen punto de partida para aislar de forma rápida y eficaz si el problema de conectividad es el resultado de una **caída de políticas** (inducida por un contrato).

Algunas preguntas de alto nivel que vale la pena hacer antes de sumergirse:

- ¿Están los terminales en el mismo EPG o en otro diferente? El tráfico entre dos terminales que residen en diferentes EPG (entre EPG) se niega implícitamente y requiere un contacto para permitir la comunicación.El tráfico entre dos terminales dentro del mismo EPG (dentro de EPG) está permitido implícitamente, a menos que se utilice el aislamiento dentro de EPG.
- ¿Se aplica o no se aplica el VRF? Cuando un VRF está en el modo **forzado**, dentro del VRF, se requieren contratos para que los terminales de dos EPG diferentes se comuniquen.Cuando un VRF está en el modo **no aplicado**, — dentro del VRF — todo el tráfico sería permitido por el entramado de ACI a través de los EPG múltiples que pertenecen al VRF no aplicado, independientemente de los contratos de ACI aplicados.

Metodología

Con las diversas herramientas disponibles, hay algunas más apropiadas y convenientes para comenzar que otras, dependiendo del nivel de información ya conocido sobre el flujo afectado.

¿Se conoce la ruta completa del paquete en el fabric de ACI (hoja de entrada, hoja de salida...)?

- Si la respuesta es sí, se debe utilizar ELAM Assistant para identificar el motivo de la caída en el switch de origen o destino.
- Si la respuesta es no, los comandos Visibility & Troubleshooting, fTriage, contract_parser, Operational tab en la vista de arrendatario y iBash ayudarán a restringir la trayectoria del paquete o darán más visibilidad a las razones de la caída.

Tenga en cuenta que la herramienta de triaje no se tratará en detalle en esta sección. Consulte el

capítulo "Intra-Fabric Forwarding" para obtener más información sobre el uso de esta herramienta.

Tenga en cuenta que, si bien la visibilidad y la resolución de problemas pueden ayudar a visualizar rápidamente dónde se descartan los paquetes entre dos terminales, fTriage muestra información más detallada para la resolución de problemas. es decir, fTriage ayudará a identificar la interfaz, el motivo de la caída y otros detalles de bajo nivel sobre el flujo afectado

.

Este escenario de ejemplo mostrará cómo resolver problemas de caída de políticas entre dos extremos: 192.168.21.11 y 192.168.23.11

Suponiendo que se producen pérdidas de paquetes entre estos dos terminales, se utilizará el siguiente flujo de trabajo de solución de problemas para identificar la causa raíz del problema:

Identifique las hojas src/dst involucradas en el flujo de tráfico:

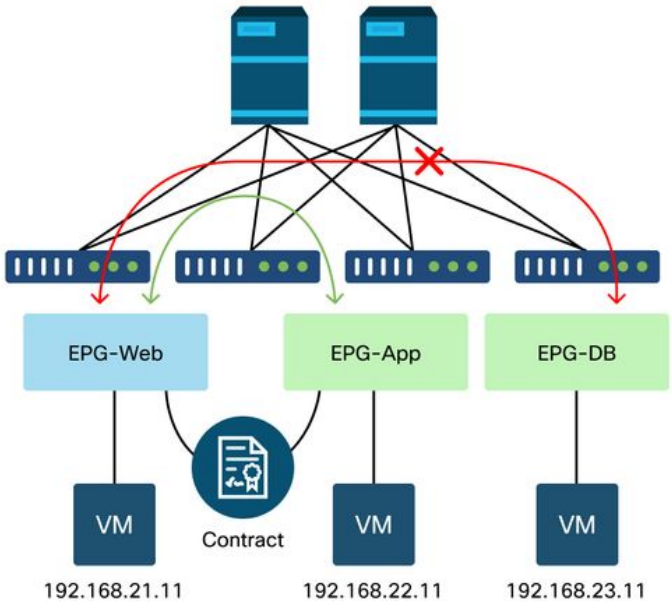
1. Utilice **Visibility & Troubleshooting** para rastrear el flujo de paquetes e identificar qué dispositivo está descartando el paquete.
2. Ejecute el comando 'show logging ip access-list internal packet-log deny' en el dispositivo seleccionado. Si se niega y registra un paquete con una de las direcciones IP de interés, el **registro de paquetes** imprimirá el terminal y el nombre de contrato relevantes en base a cada resultado.
3. Utilice el comando 'contract_parser.py —vrf <tenant>:<VRF>' en la hoja de origen y destino para observar el conteo de aciertos para el contrato configurado: Si un paquete llega al contrato en el switch de origen o de destino, el contador del contrato relevante se incrementaráEste método es menos granular que el de registro de paquetes interno de la lista de acceso IP en situaciones en las que muchos flujos podrían alcanzar la misma regla (muchos terminales/flujos entre los dos EPG de interés).

Los pasos anteriores se describen con más detalle en el siguiente párrafo.

Ejemplo de escenario de Troubleshooting de EPG a EPG

Este escenario de ejemplo mostrará cómo resolver problemas de caída de políticas entre dos extremos: 192.168.21.11 en EPG-Web y 192.168.23.11 en EPG-DB.

Topología

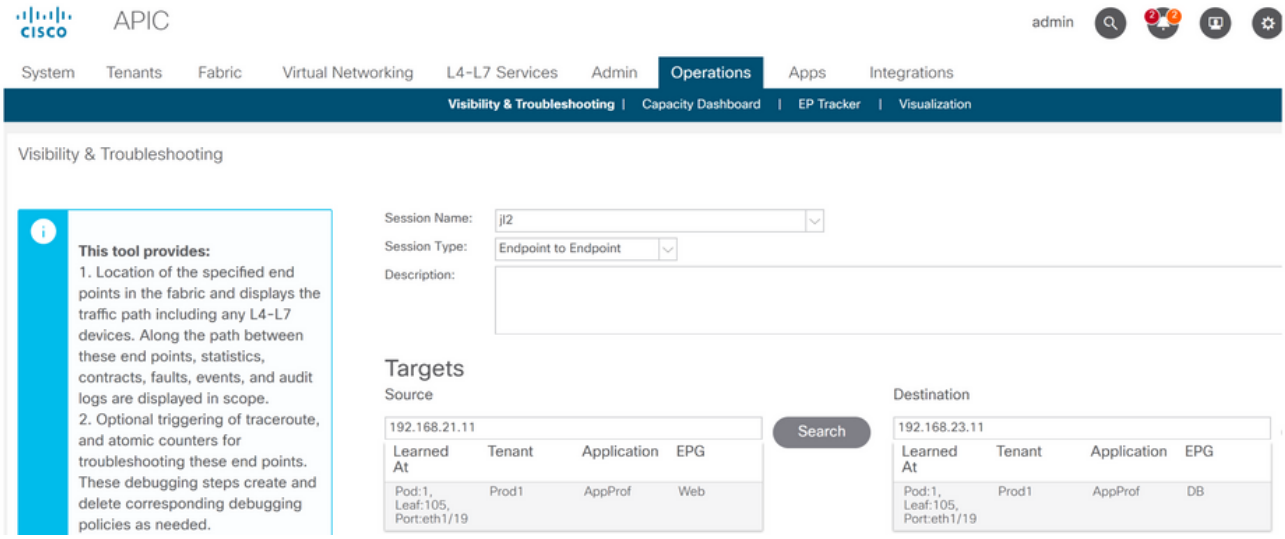


Identifique los switches de hoja de origen y destino involucrados en la caída de paquetes

Visibilidad y resolución de problemas

La herramienta Visibility & Troubleshooting (Visibilidad y resolución de problemas) le ayudará a visualizar el switch en el que se ha producido el descarte de paquetes para un flujo EP-to-EP específico e identificar dónde es posible que se descarten los paquetes.

Configuración de visibilidad y resolución de problemas

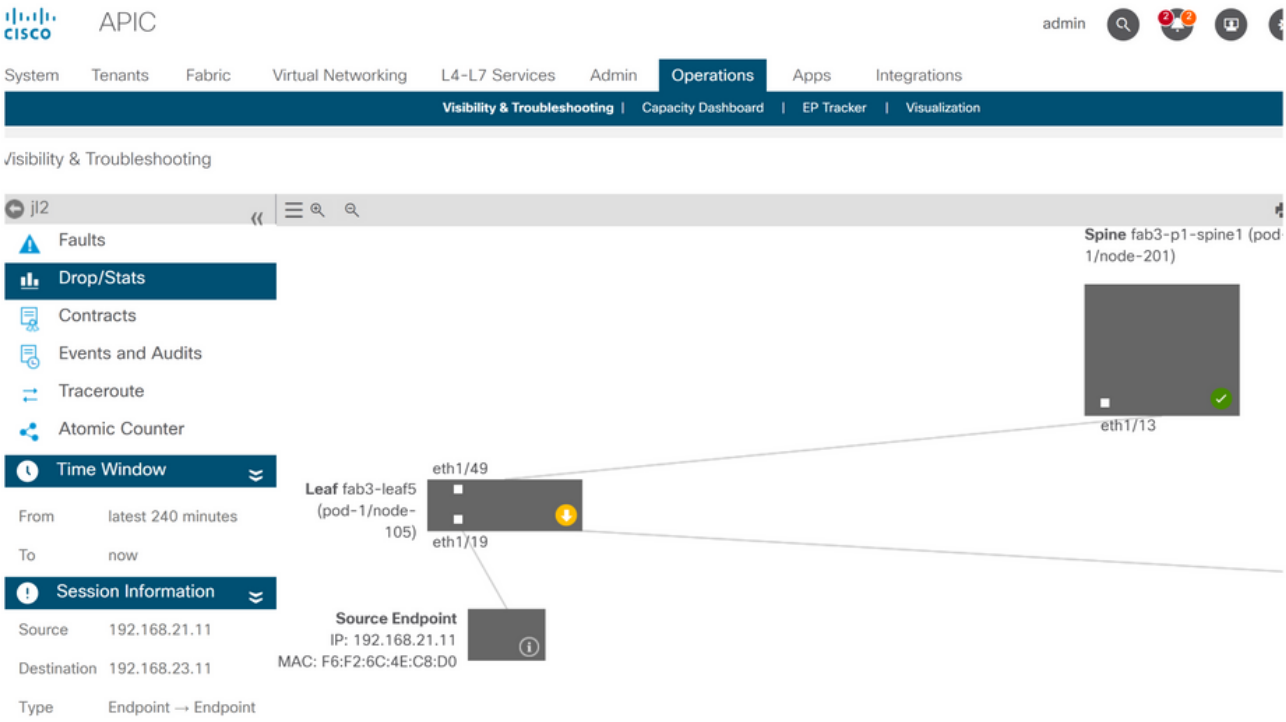


Configure un nombre de sesión, un origen y un extremo de destino. A continuación, haga clic en 'Enviar' o 'Generar informe'.

La herramienta buscará automáticamente los terminales en el fabric y proporcionará información sobre el arrendatario, el perfil de aplicación y el EPG al que pertenecen los EP.

En este caso, descubrirá que los EP pertenecen al arrendatario Prod1, pertenecen al mismo perfil de aplicación 'AppProf' y están asignados a diferentes EPG: 'Web' y 'DB'.

Identificación de descarte

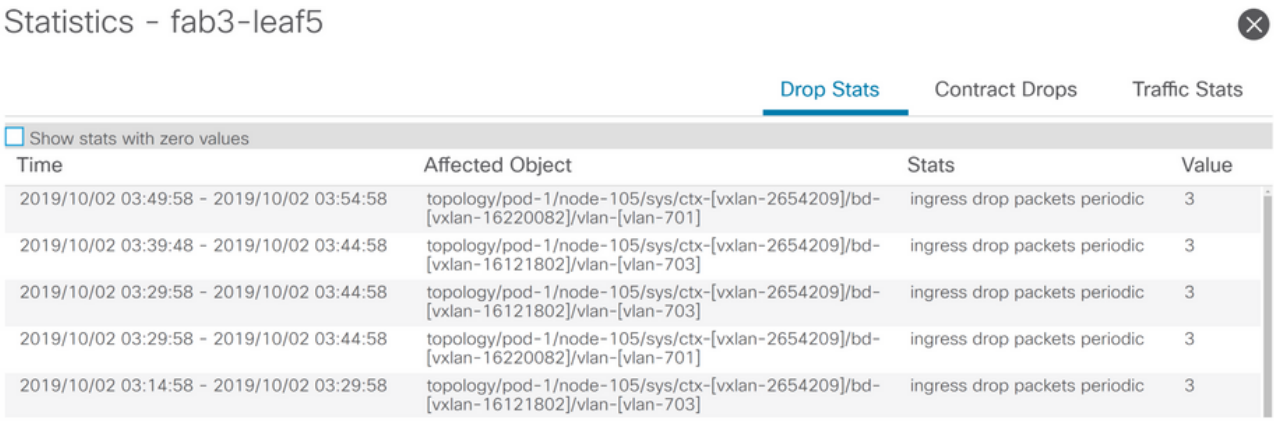


La herramienta visualizará automáticamente la topología del escenario de solución de problemas. En este caso, los dos terminales están conectados al mismo switch de hoja.

Si se desplaza al submenú Drop/Stats (Eliminar/estadísticas), el usuario puede ver las caídas generales en la hoja o columna en cuestión. Consulte la sección "Descartes de interfaz" en el capítulo "Reenvío dentro del fabric" de este manual para obtener más información sobre qué descartes son relevantes.

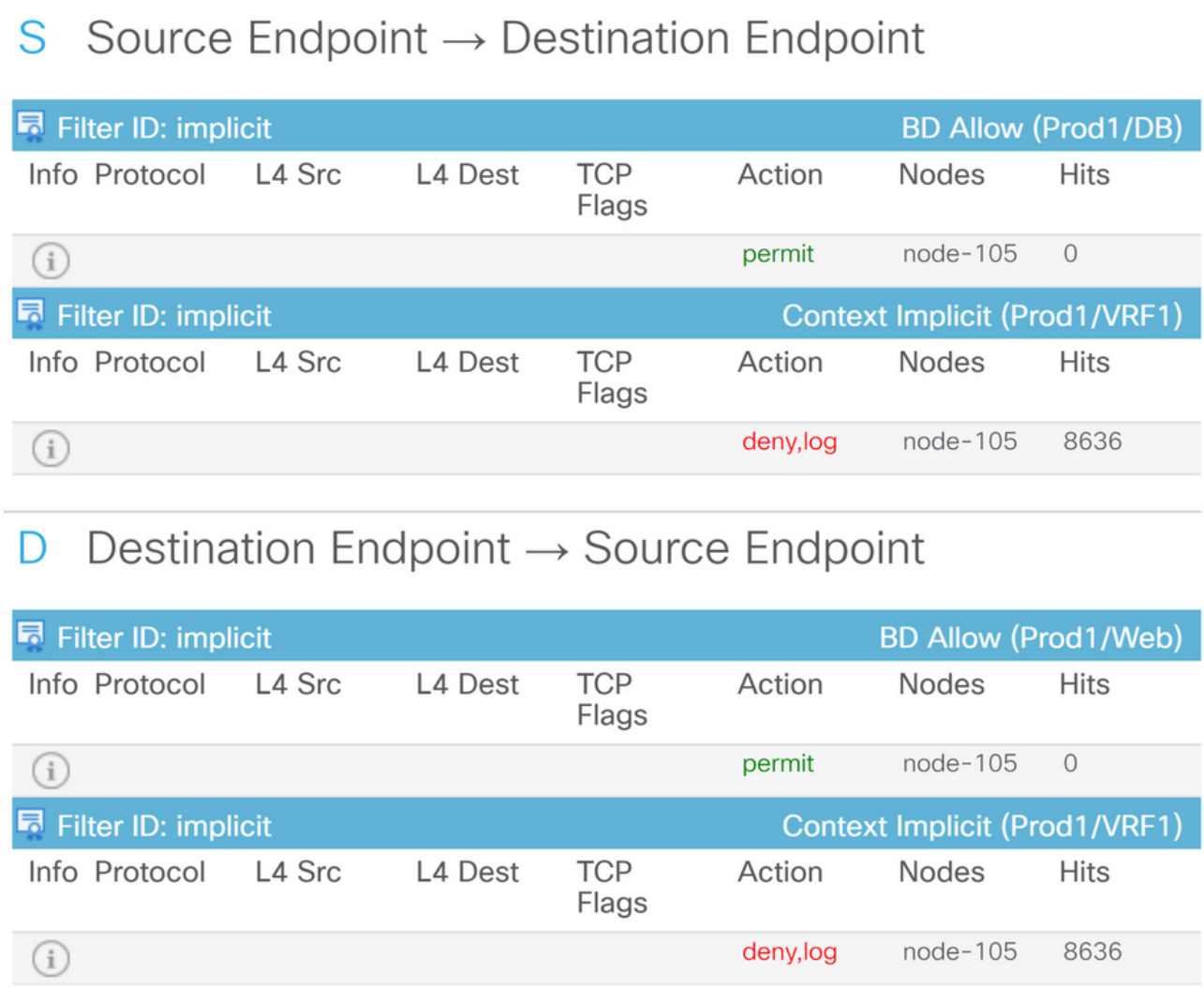
Muchas de estas caídas son un comportamiento esperado y se pueden ignorar.

Eliminar detalles



Si profundiza hasta los detalles de la lista desplegable utilizando el botón amarillo "Paquetes descartados" en el diagrama del switch, el usuario puede ver los detalles sobre el flujo descartado.

Detalles del contrato



Al acceder al submenú Contratos, el usuario puede identificar qué contrato está provocando el descarte de políticas entre los EPG. En el ejemplo, es Implicit to Deny Prod1/VRF1 que muestra algunos resultados. Esto no significa necesariamente que el flujo especificado (192.168.21.11 y 192.168.23.11) esté alcanzando esta negación implícita. Si la regla de denegación implícita de aciertos de contexto está aumentando, implica que hay tráfico entre Prod1/DB y Prod1/Web que no acierta en ninguno de los contratos y, por lo tanto, se descarta por la denegación implícita.

En la vista de topología de perfil de aplicación en Arrendatario > seleccione el nombre de perfil de aplicación a la izquierda > Topología , es posible verificar qué contratos se aplican al EPG de base de datos. En este caso, no se asigna ningún contrato al EPG:

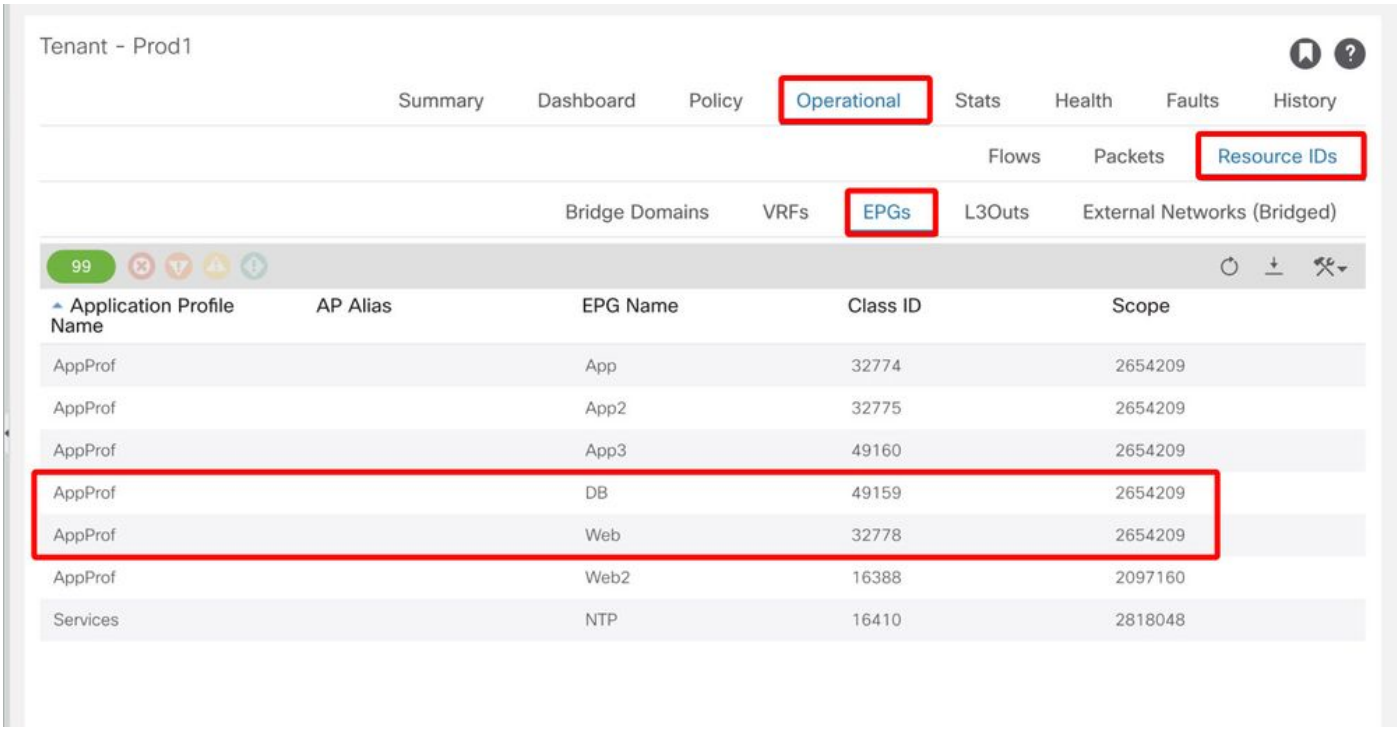
Visualización de contratos

Ahora que se conocen los EPG de origen y destino, también es posible identificar otra información relevante como la siguiente:

- El src/dst **EPG pcTag** de los terminales afectados. pcTag es el ID de clase utilizado para identificar un EPG con una regla de zonificación.
- El **VRFVNID** src/dst, también denominado **alcance**, de los terminales afectados.

La ID de clase y el alcance se pueden recuperar fácilmente desde la GUI de APIC abriendo el arrendatario > seleccione el nombre del arrendatario a la izquierda > Operativo > ID de recursos > EPG

ID de recurso de arrendatario para encontrar la etiqueta de equipo y el ámbito de EPG



En este caso, el ID de clase y los ámbitos son:

- Web EPG pcTag 32778
- Ámbito Web EPG 2654209
- DB EPG pcTag 49159
- Ámbito DB EPG 2654209

Verifique la política aplicada al flujo de tráfico que se está solucionando

iBash

Una herramienta interesante para verificar el paquete descartado en una hoja de ACI es la línea de comandos 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
```

Según la salida anterior, se puede ver que en el switch de hoja, numerosos paquetes ICMP originados por EP 192.168.23.11 hacia 192.168.21.11 se han descartado.

La herramienta contract_parser le ayudará a verificar las políticas reales aplicadas al VRF donde los terminales están asociados con:

```
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]
```

Esto también se puede verificar a través de la regla de zonificación programada en la hoja de las políticas aplicadas por el 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)       |
+---------+--------+--------+----------+----------------+---------+----------+------------+-----
-----+--------------------------+
```

Como ya han visto la herramienta Visibility & Troubleshooting, la herramienta contract_parser y las reglas de zonificación, la salida confirma que no hay ningún contrato entre los EPG de origen y de destino en la resolución de problemas. Es fácil suponer que los paquetes descartados coinciden con la regla de denegación implícita 5155.

Captura de ELAM

La captura de ELAM proporciona un informe de nivel ASIC utilizado para verificar los detalles de reenvío que indica, en el caso de un paquete descartado, el motivo del descarte. Cuando la razón de una caída es una caída de política, como en este escenario, la salida de la captura de ELAM será similar a la siguiente.

Tenga en cuenta que los detalles de la configuración de una captura de ELAM no se tratarán en este capítulo. Consulte el capítulo "Reenvío dentro del 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
```

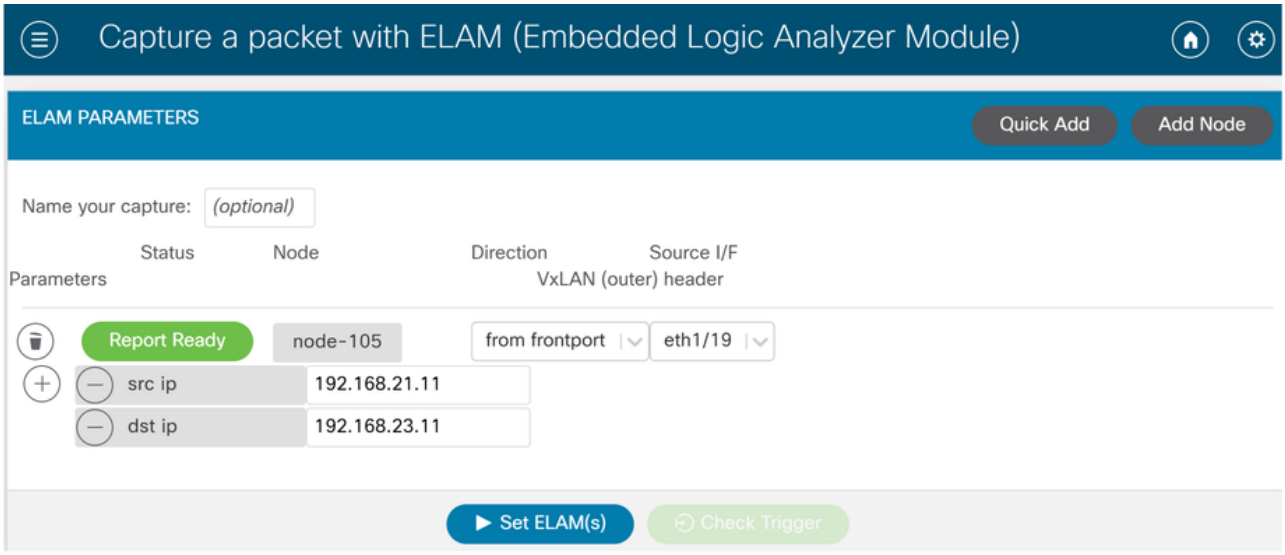
```
pkt.lu_drop_reason: 0x2D
```

El informe de ELAM anterior muestra claramente que el paquete se descartó debido a una caída de política: 'SECURITY_GROUP_DENY'

Asistente de ELAM:

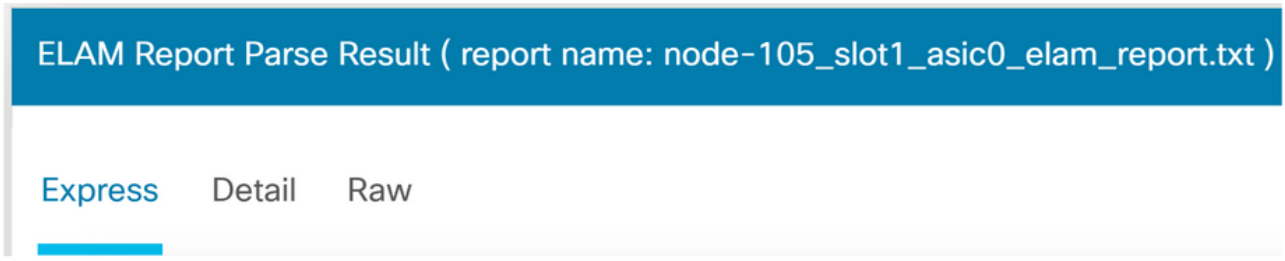
El mismo resultado de la captura de ELAM se puede mostrar a través de la aplicación ELAM Assistant en la GUI de APIC.

Configuración



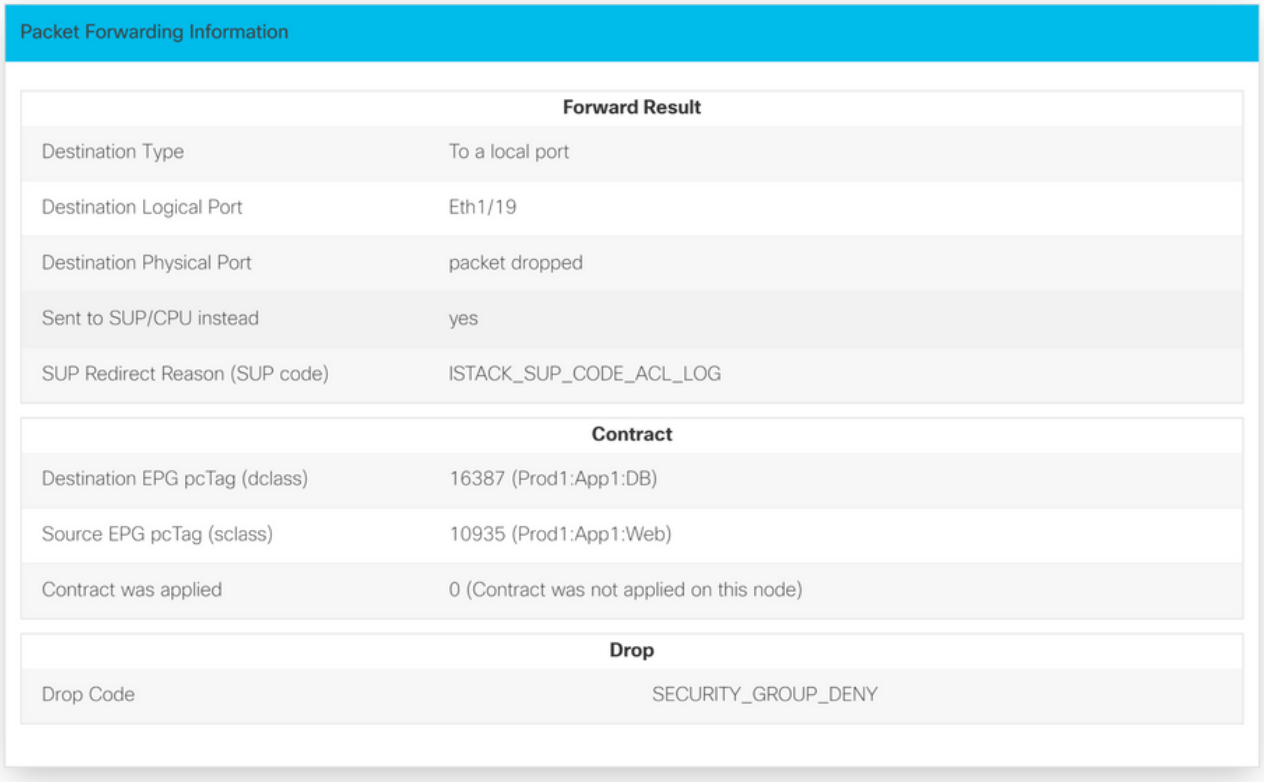
Normalmente, el usuario configurará los detalles de origen y destino para el flujo de interés. En este ejemplo, la IP de origen se utiliza para capturar el tráfico hacia el terminal en el EPG de destino que no tiene una relación de contrato con el EPG de origen.

Informe de Elam Assistant Express



Hay tres niveles de salida que se pueden ver con ELAM Assistant. Éstos son Express, Detail y Raw.

Informe de Elam Assistant Express (cont.)



En el resultado rápido, el motivo de código de descarte SECURITY_GROUP_DENY indica que el descarte fue resultado de un resultado de contrato.

Grupo preferido

Acerca de los grupos preferidos de contratos

Hay dos tipos de aplicación de políticas disponibles para los EPG en un VRF con un grupo de contratos preferidos configurado:

- EPG incluidos: Los EPG pueden comunicarse libremente entre sí sin contratos, si son miembros de un grupo preferente de contratos. Se basa en la regla predeterminada source-any-destination-any-permit.
- EPG excluidos: Los EPG que no son miembros de los grupos preferidos requieren contratos para comunicarse entre sí. De lo contrario, se aplicarán las reglas de denegación entre el EPG excluido y cualquier EPG.

La función de grupo preferida por contrato permite un mayor control de la comunicación entre los EPG en un VRF. Si la mayoría de los EPG del VRF deben tener una comunicación abierta, pero unos pocos deben tener una comunicación limitada con los otros EPG, configure una combinación de un grupo de contratos preferidos y contratos con filtros para controlar con mayor precisión la comunicación entre EPG.

Los EPG excluidos del grupo preferido solo pueden comunicarse con otros EPG si existe un contrato para invalidar la regla predeterminada source-any-destination-any-deny.

Programación de grupos preferidos por contrato

Básicamente, los grupos preferentes de contratos son una inversa de los contratos regulares. Para los contratos regulares, las reglas de zonificación de permisos explícitas se programan con

una regla de zonificación de negación implícita con el alcance VRF. Para los grupos preferidos, una regla de zonificación PERMIT implícita se programa con el valor de prioridad numérica más alto y las reglas de zonificación DENY específicas se programan para impedir el tráfico de los EPG que no son miembros del grupo preferido. Como resultado, las reglas de denegación se evalúan primero y, si el flujo no coincide con estas reglas, se permite implícitamente el flujo.

Siempre hay un par de reglas de zonificación de negación explícitas para cada EPG fuera del grupo preferido:

- Una del miembro del grupo no preferido a cualquier pcTag (valor 0).
- Otro de cualquier pcTag (valor 0) al miembro del grupo no preferido.

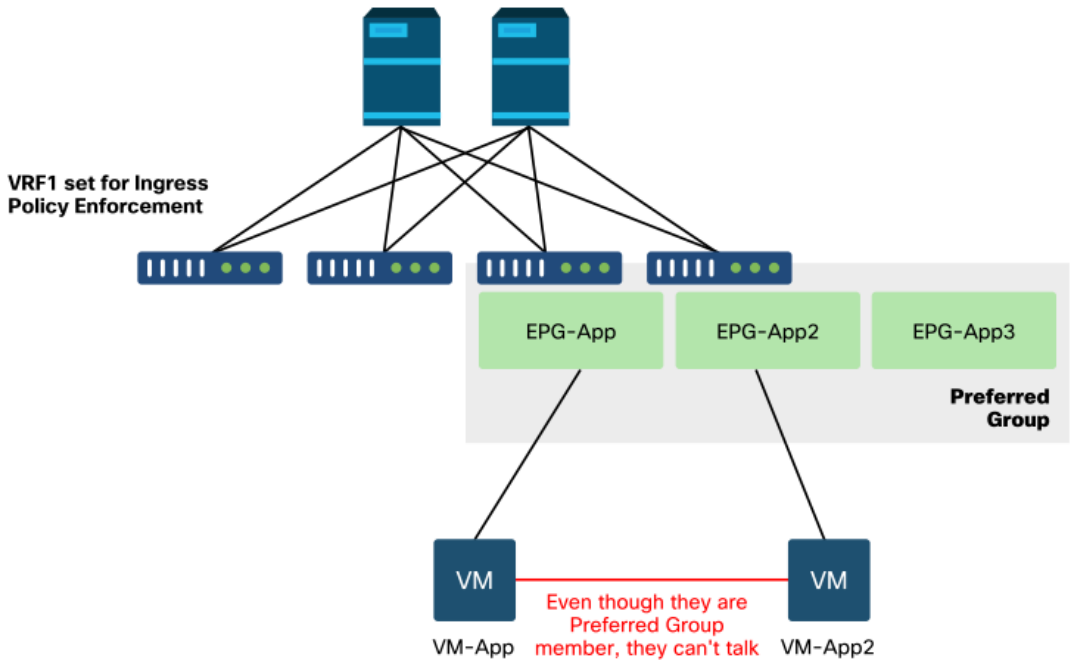
Escenario de Troubleshooting de Grupo Preferido

La siguiente figura muestra una topología lógica en la que las aplicaciones EPG App, App2 y App3 están configuradas como miembros de grupo preferidos.

VM-App forma parte de EPG-App y VM-App2 forma parte de EPG-App2. Tanto App como App2 EPG deben formar parte de las aplicaciones preferidas y, por tanto, comunicarse libremente.

VM-App inicia un flujo de tráfico en el puerto TCP 6000 a VM-App2. Tanto EPG-App como EPG-App2 son miembros de grupo preferidos como parte de VRF1. VM-App2 nunca recibe ningún paquete en el puerto TCP 6000.

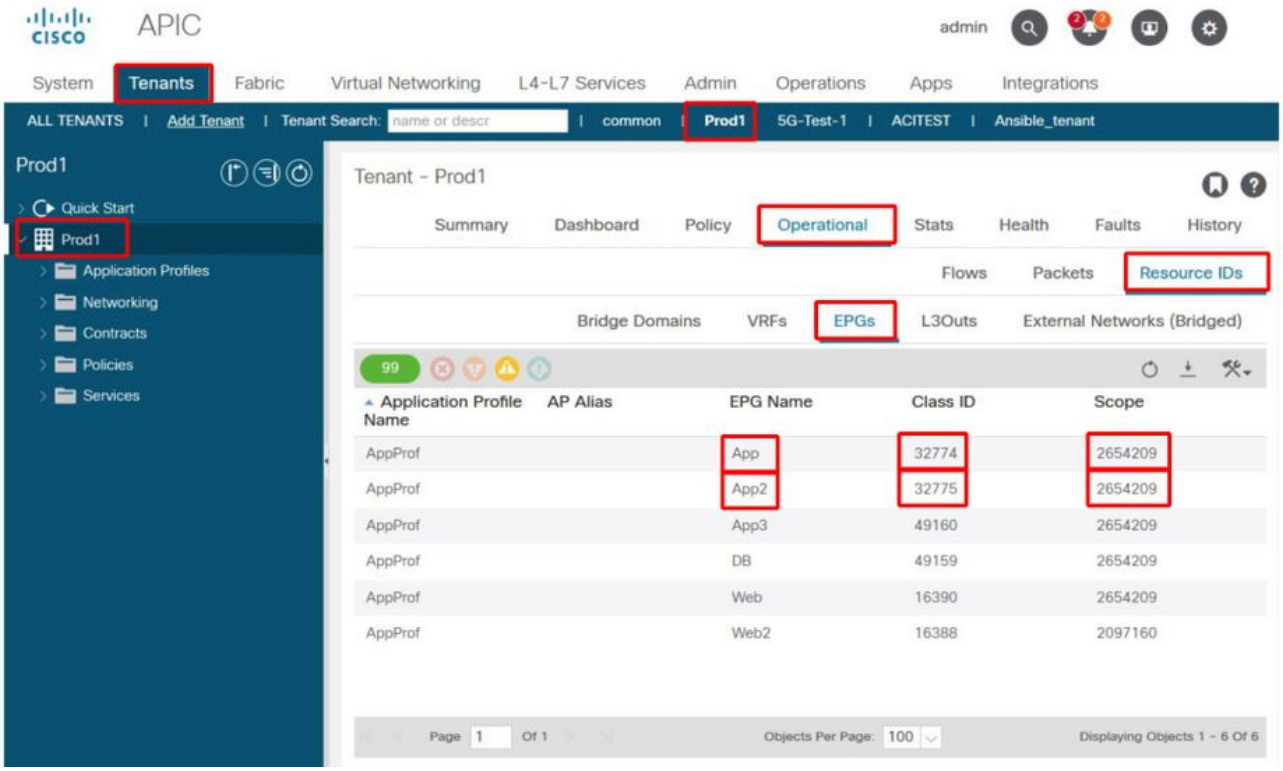
Topología



Flujo de trabajo

1. Busque la pcTag de la aplicación EPG y su VRF VNID/Scope

PcTags de EPG y VRF



2. Verifique la programación de contratos usando contract_parser.py en la hoja de ingreso

Utilice contract_parser.py o el comando 'show zoning-rule' y especifique el 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]
```

Examinando el resultado anterior, se observa la entrada de permiso implícita -ruleId 4165- con la prioridad más alta de 20. Esta regla de permiso implícita hará que se permitan todos los flujos de tráfico a menos que haya una regla de denegación explícita con una prioridad menor que no permita el flujo de tráfico.

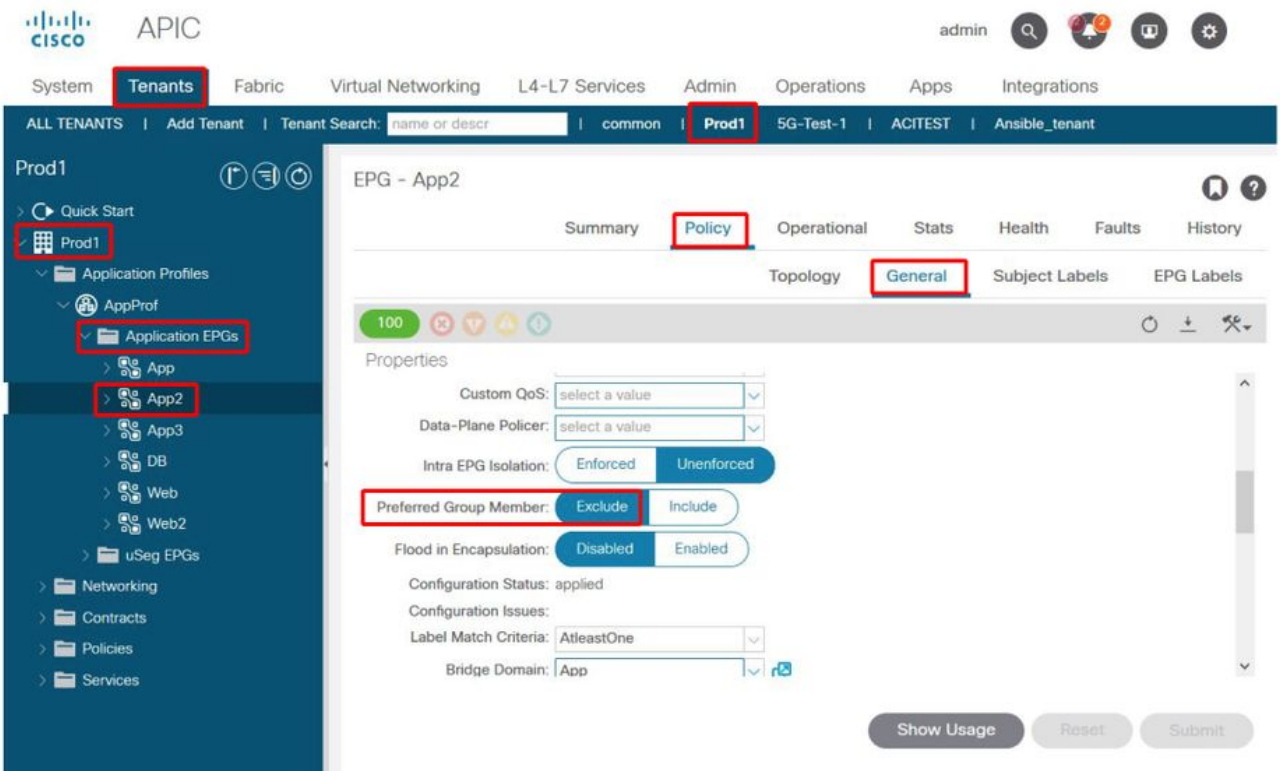
Además, se observan dos reglas de denegación explícitas para pcTag 32775, que es pcTag de EPG App2. Estas dos reglas de zonificación de denegación explícitas no permiten el tráfico de cualquier EPG a EPG App2 y viceversa. Esas reglas tienen prioridad 18 y 19, por lo que tendrán prioridad sobre la regla de permiso predeterminada.

La conclusión es que EPG App2 no es un miembro del grupo preferido, ya que se observan las reglas de denegación explícitas.

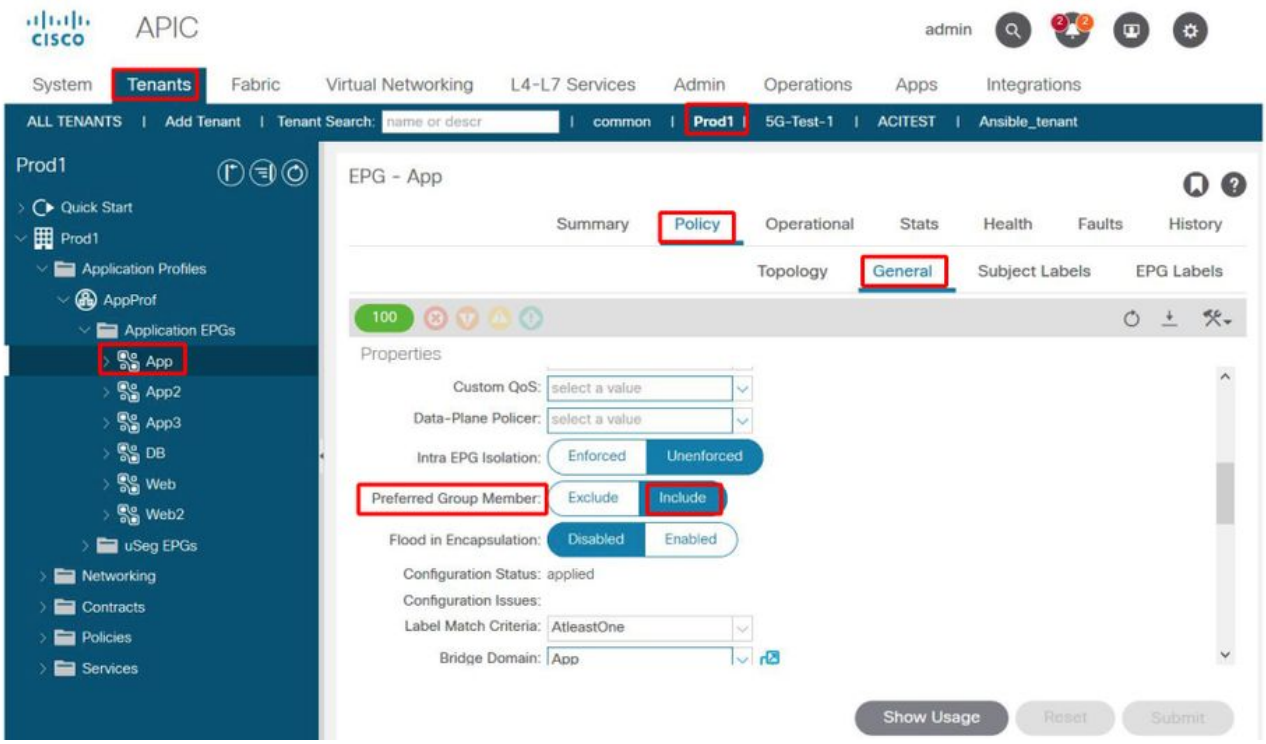
3. Verifique la configuración de miembro de grupo preferida por EPG

Navegue por la GUI de APIC y verifique EPG App2 y EPG App Preferred Group Member Configuration. En la siguiente figura, consulte EPG App2 no está configurado como miembro de grupo preferido.

EPG App2: se excluye la configuración de miembro de grupo preferido



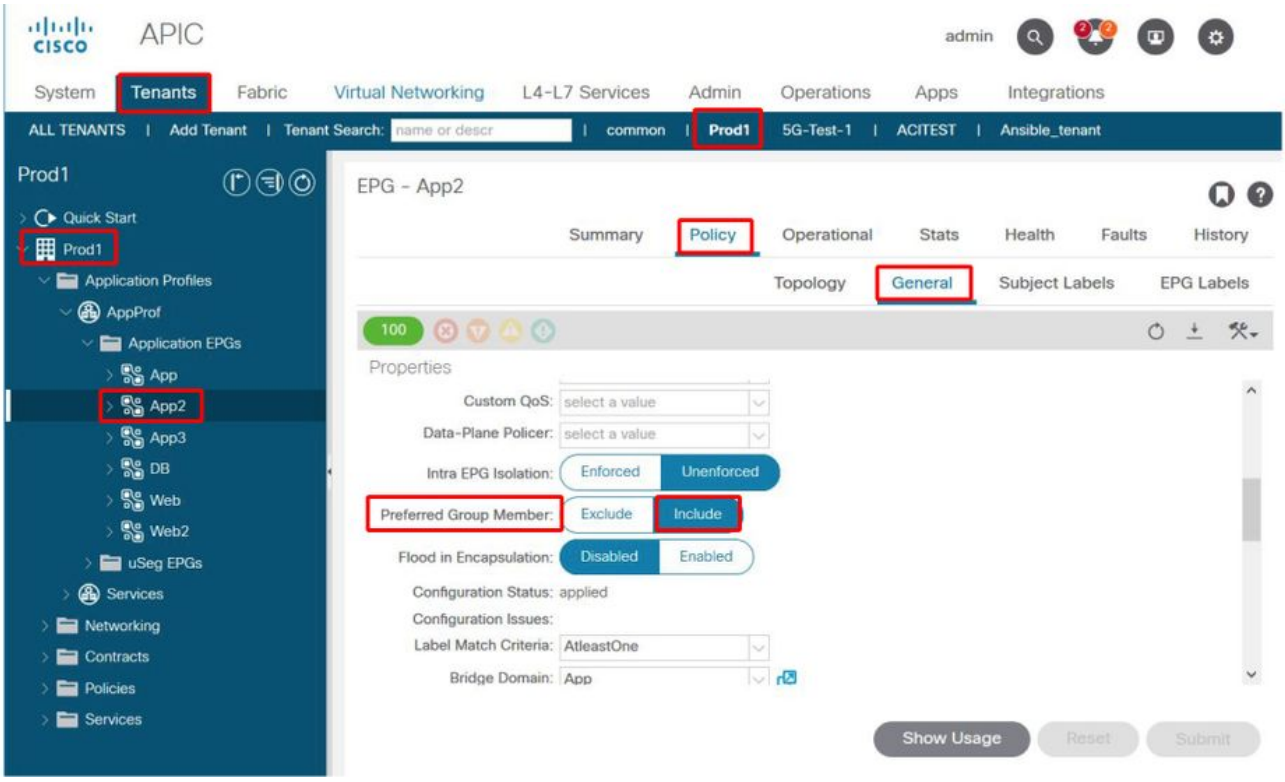
Aplicación EPG: se incluye la configuración de miembro de grupo preferido



4. Establezca EPG App2 como miembro preferido del grupo

El cambio de la configuración de App2 EPG permite al grupo preferido comunicarse libremente como parte del grupo preferido.

EPG App2: se incluye la configuración de miembro de grupo preferido



5. Vuelva a verificar la programación del contrato mediante contract_parser.py en la hoja en la que reside el PE de origen

Vuelva a utilizar contract_parser.py y especifique el nombre VRF para verificar si las reglas de denegación explícitas para EPG App2 han desaparecido.

```
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]
```

Las reglas de negación explícitas para EPG App2 y su pcTag 32775 ya no se observan en el resultado anterior. Esto significa que el tráfico entre los EP de la aplicación EPG y la aplicación EPG2 coincidirá ahora con la regla de permiso implícita (ruleId 4165) con la prioridad más alta de 20.

vzAny a EPG

Acerca de vzAny

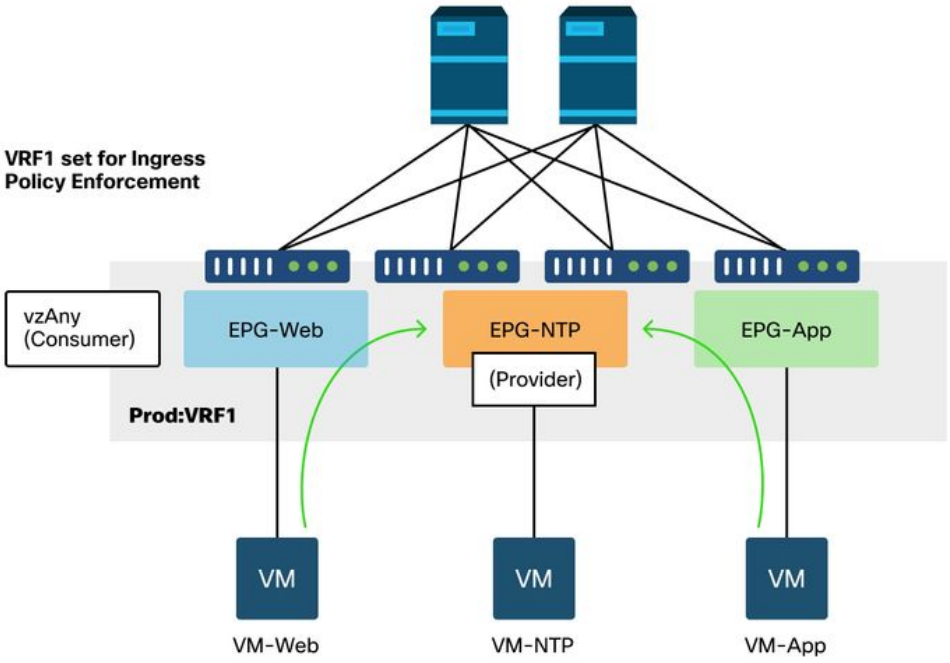
Al configurar contratos entre uno o varios EPG, los contratos se pueden configurar como una

relación consumida o proporcionada. Cuando el número de EPG aumenta, también lo hace la cantidad de relaciones contractuales entre ellos. Algunos casos prácticos comunes requieren que todos los EPG intercambien flujos de tráfico con otro EPG específico. Este caso de uso podría ser un EPG que contenga EP que proporcionen servicios que deban ser consumidos por todos los otros EPG dentro del mismo VRF (NTP o DNS, por ejemplo). vzAny permite una menor sobrecarga operativa al configurar las relaciones contractuales entre todos los EPG y los EPG específicos que proporcionan servicios que deben consumir todos los demás EPG. Además, vzAny permite un uso mucho más eficiente de la política de seguridad CAM en los switches de hoja, ya que solo se añaden 2 reglas de zonificación para cada relación de contrato vzAny.

Ejemplo de caso práctico

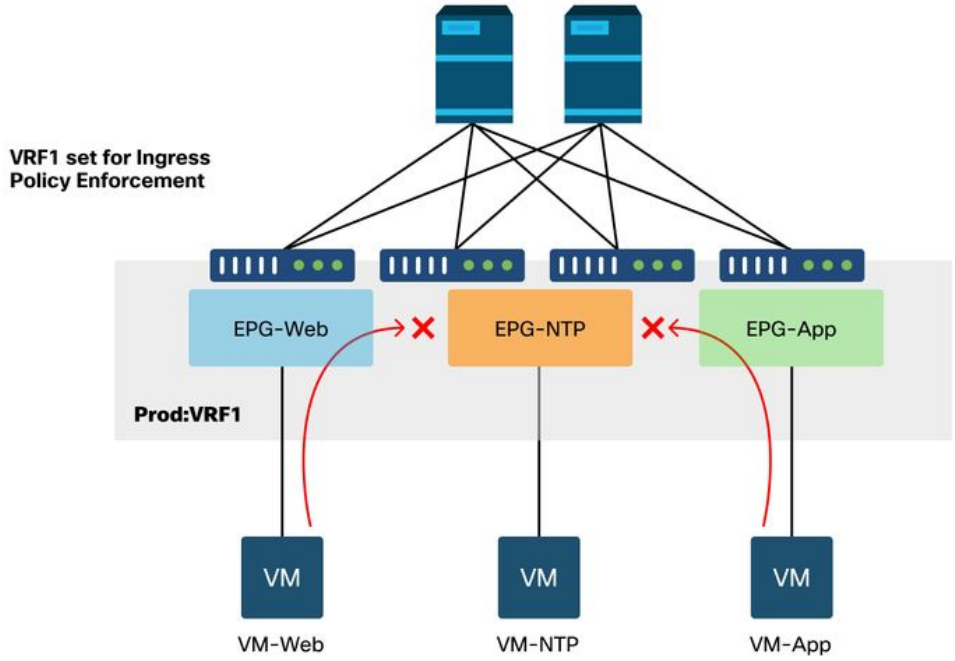
La siguiente figura describe un caso práctico en el que VM-Web y VM-App en EPG Web y App respectivamente necesitan consumir servicios NTP de VM-NTP en EPG-NTP. En lugar de configurar un contrato proporcionado en EPG NTP y, posteriormente, tener ese mismo contrato como un contrato consumido en EPG Web y App, vzAny permite que cada EPG en VRF Prod:VRF1 consuma servicios NTP de EPG NTP.

vzAny: cualquier EPG en el producto VRF:VRF1 puede consumir servicios NTP de EPG NTP



Considere un escenario en el que se observan caídas entre los EPG que consumen los servicios NTP cuando no hay ningún contrato entre ellos.

Situación de resolución de problemas: el tráfico se interrumpe si no hay ningún contrato

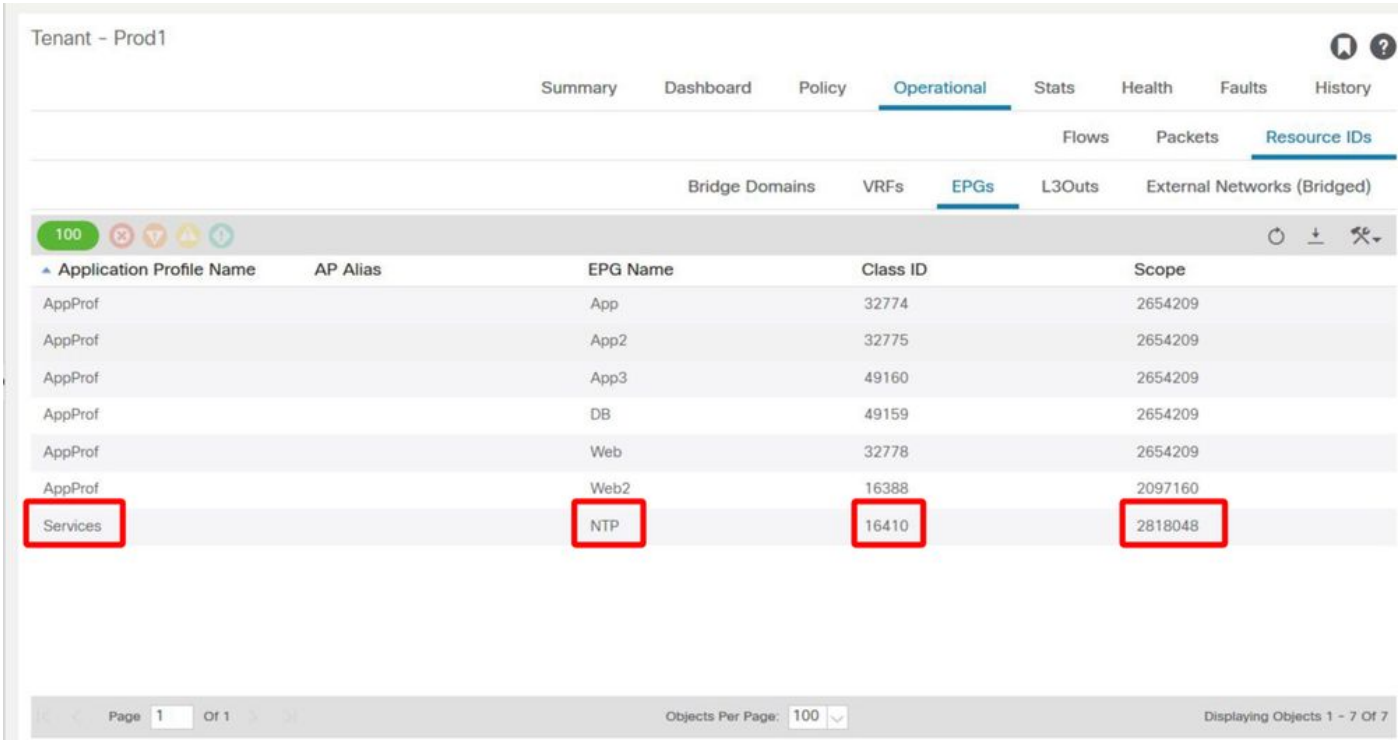


Flujo de trabajo

1. Busque la pcTag de EPG NTP y su VRF VNID/Scope

'Arrendatario > Operativo > ID de recursos > EPG' permite encontrar la pcTag y el alcance

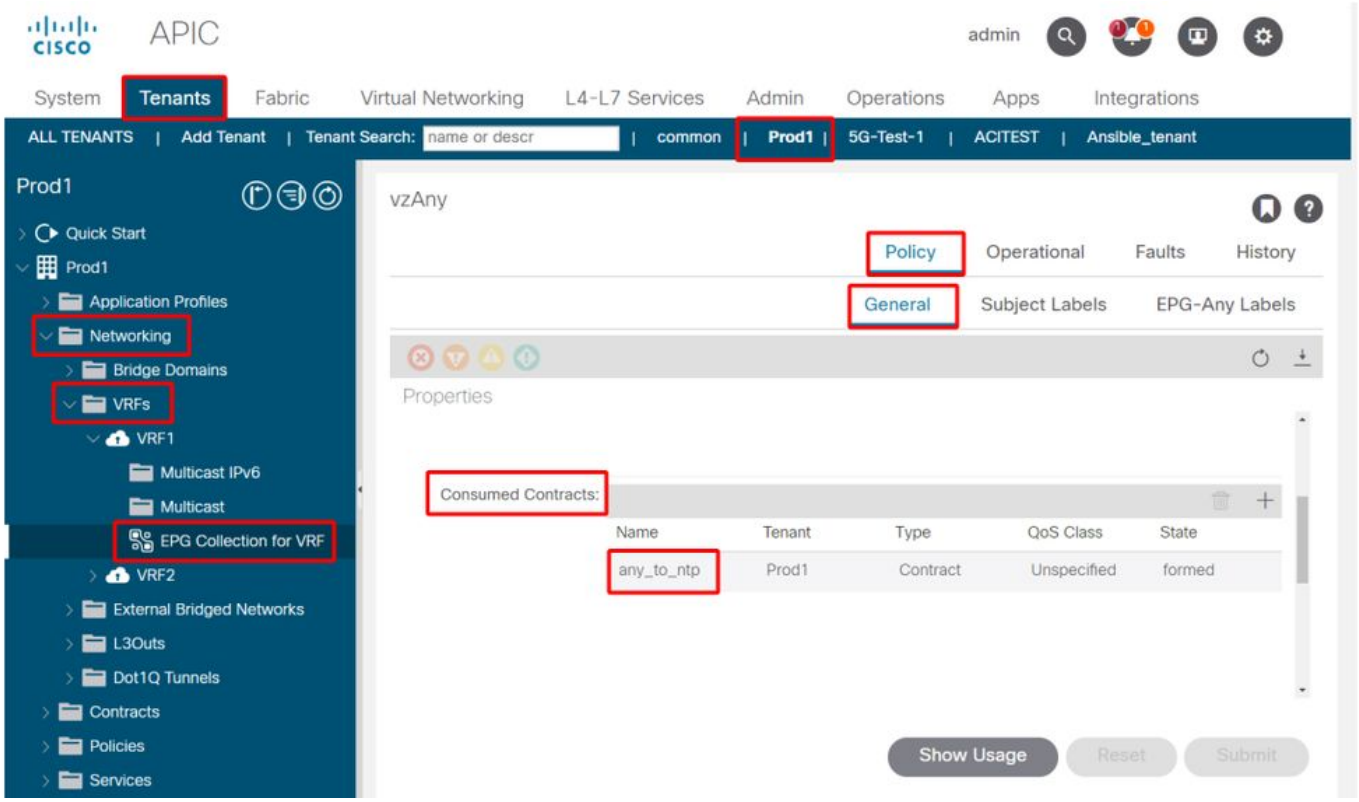
EPG NTP pcTag y su VRF VNID/Scope



2. Compruebe si un contrato está configurado como un contrato vzAny consumido como parte del VRF

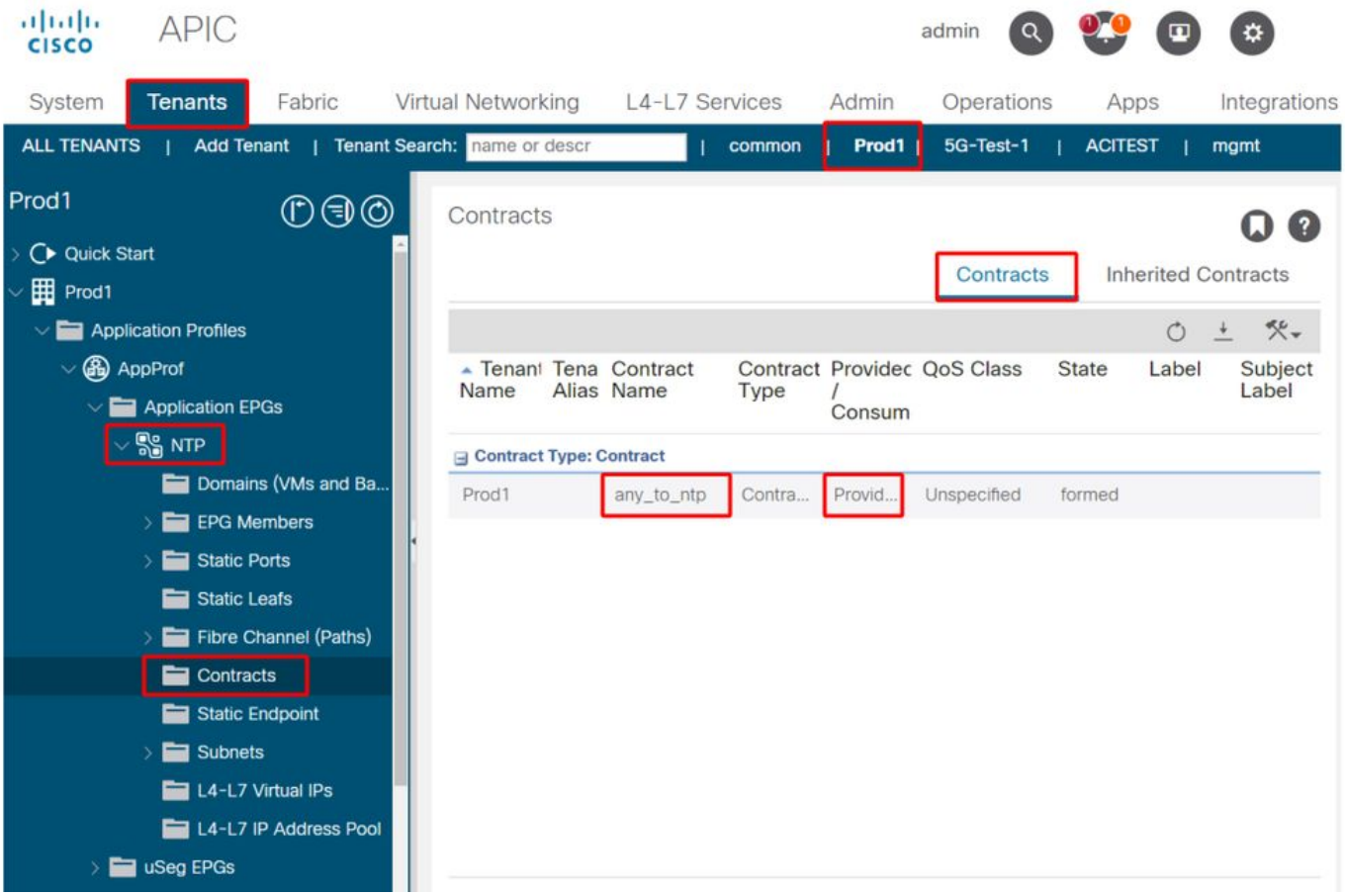
Desplácese hasta el VRF y compruebe si hay un contrato consumido configurado como vzAny en la recopilación de EPG para VRF.

Contrato configurado como vzAny consumido en el VRF



3. Verifique si se aplica el mismo contrato que un contrato proporcionado en EPG NTP

A fin de establecer una relación contractual, debe aplicarse el mismo contrato que un contrato facilitado sobre EPG NTP que presta servicios NTP a los otros EPG en su VRF.



4. Verificación de regla de zonificación en hoja de ingreso mediante contract_parser.py o 'show zoning-rule'

La hoja de ingreso debe tener 2 reglas de zonificación para permitir los flujos de tráfico bidireccionales (si el sujeto del contrato está configurado para permitir ambas direcciones) entre cualquier EPG y EPG NTP. 'Cualquier EPG' se denota como pcTag 0 en la programación de reglas de zonificación.

El uso de contract_parser.py o los comandos 'show zoning-rule' en la hoja de ingreso mientras se especifica el VRF permite garantizar que la regla de zonificación esté programada.

Reglas de zonificación que permiten el tráfico hacia/desde EPG NTP desde otros EPG en el VRF presente

Uso de contract_parser.py y 'show zoning-rule' para verificar la presencia de las reglas de zonificación basadas en vzAny.

Aquí se pueden observar dos tipos de reglas:

1. Regla 4156 y Regla 4168 que permiten el uso de Any en NTP y viceversa. Tienen prioridad 13 y 14: Regla de división en zonas que permite el flujo de tráfico desde cualquier EPG (pcTag 0) a EPG NTP (pcTag 49161).Regla de zonificación que permite el flujo de tráfico desde EPG NTP (pcTag 46161) a cualquier otro EPG (pcTag 0).
2. Regla 4165, que es la regla de denegación cualquiera a cualquiera (predeterminada) con prioridad 21.

Dado que la prioridad más baja tiene precedencia, todos los EPG del VRF tendrán acceso al 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)  |
+---------+--------+--------+----------+---------+---------+---------+-----------+----------+--
--------------------+
```

Salida L3 compartida a EPG

Acerca de L3Out compartida

Shared Layer 3 Out es una configuración que permite tener una salida L3 en un VRF que proporciona algunos servicios (acceso externo) y uno o más VRF consumen esta salida L3. Puede encontrar más detalles sobre L3Out compartida en el capítulo "Routing externo".

Al realizar L3Out compartido, se recomienda que el proveedor del contrato sea el L3Out compartido y que el EPG sea el consumidor del contrato. Este escenario se ilustrará en esta sección.

No se recomienda hacer lo contrario, que es L3Out consumiendo un servicio proporcionado por un EPG. La razón de esto tiene que ver con la escalabilidad, ya que para los servicios compartidos, las reglas de zonificación sólo se instalan en el VRF de consumidor. Los principios de consumo y suministro indican dónde se inician los flujos de tráfico. Con la aplicación de políticas de entrada predeterminada, esto significa que la aplicación de políticas se aplicará en el lado del consumidor y más específicamente en la hoja de entrada (hoja no fronteriza). Para que la

hoja de ingreso aplique la política, se requiere la pcTag del destino. En esta situación, el destino es la pcTag EPG externa. De este modo, la hoja de ingreso realiza la aplicación de políticas y reenvía los paquetes a la hoja de borde. La hoja de borde recibe el paquete en su link de fabric que realiza una búsqueda de ruta (LPM) y reenvía el paquete a la adyacencia para el prefijo de destino.

Sin embargo, la hoja de frontera NO realiza ninguna aplicación de políticas al enviar tráfico al EP de destino ni tampoco lo hace en el flujo de tráfico de retorno al EP de origen.

Como resultado, sólo la política CAM de la hoja no BL de ingreso tiene entradas instaladas (en el VRF de consumidor) y la política CAM de BL no se ve afectada.

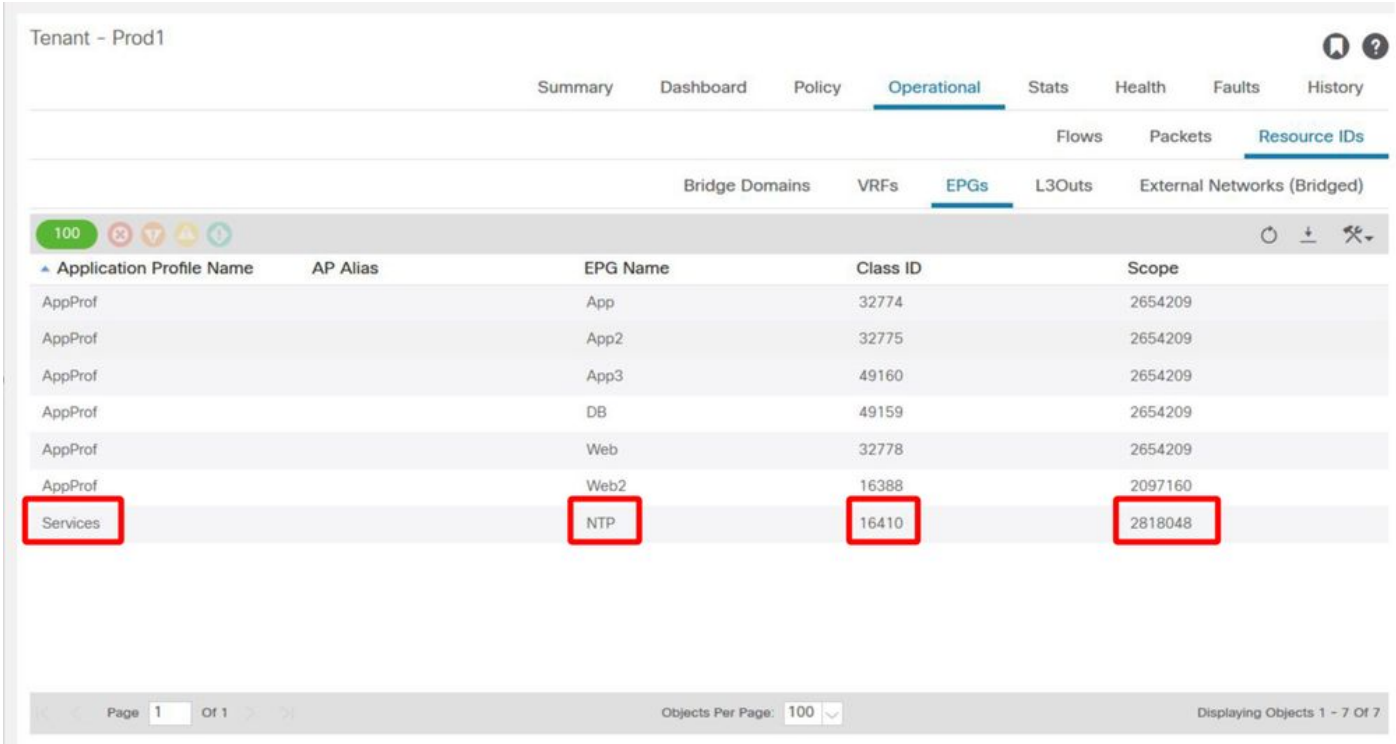
Solución de problemas de una salida L3 compartida

Flujo de trabajo

1. Verifique EPG pcTag y VRF VNID/Scope para el EPG del consumidor

Con L3Out compartido, las reglas de zonificación sólo se instalan en el VRF de consumidor. El proveedor debe tener una pcTag global (por debajo de 16k) que permita utilizar esta pcTag en todos los VRF de consumidor. En nuestra situación, el proveedor es el EPG externo y tendrá una pcTag global. El EPG del consumidor tendrá una pcTag local como de costumbre.

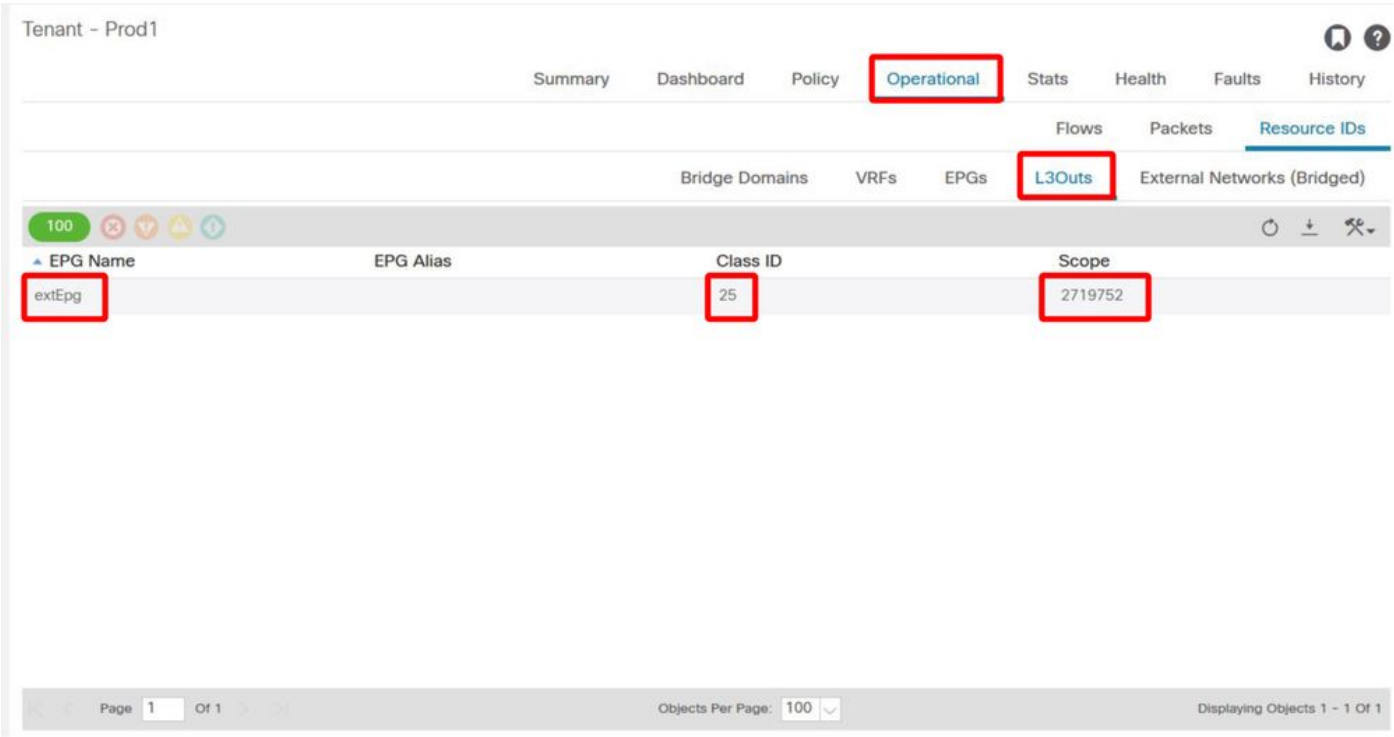
pcTag de EPG de consumidor



2. Verifique pcTag y VRF VNID/Scope para el proveedor L3Out EPG

Como se indicó en el paso 1, el proveedor L3Out EPG tiene un rango global pcTag como prefijos de L3Out que se filtran en el VRF del consumidor. Como resultado, se requiere que la pcTag L3Out EPG no se superponga con pcTags en el VRF de consumidor, por lo que se encuentra dentro del rango global pcTag.

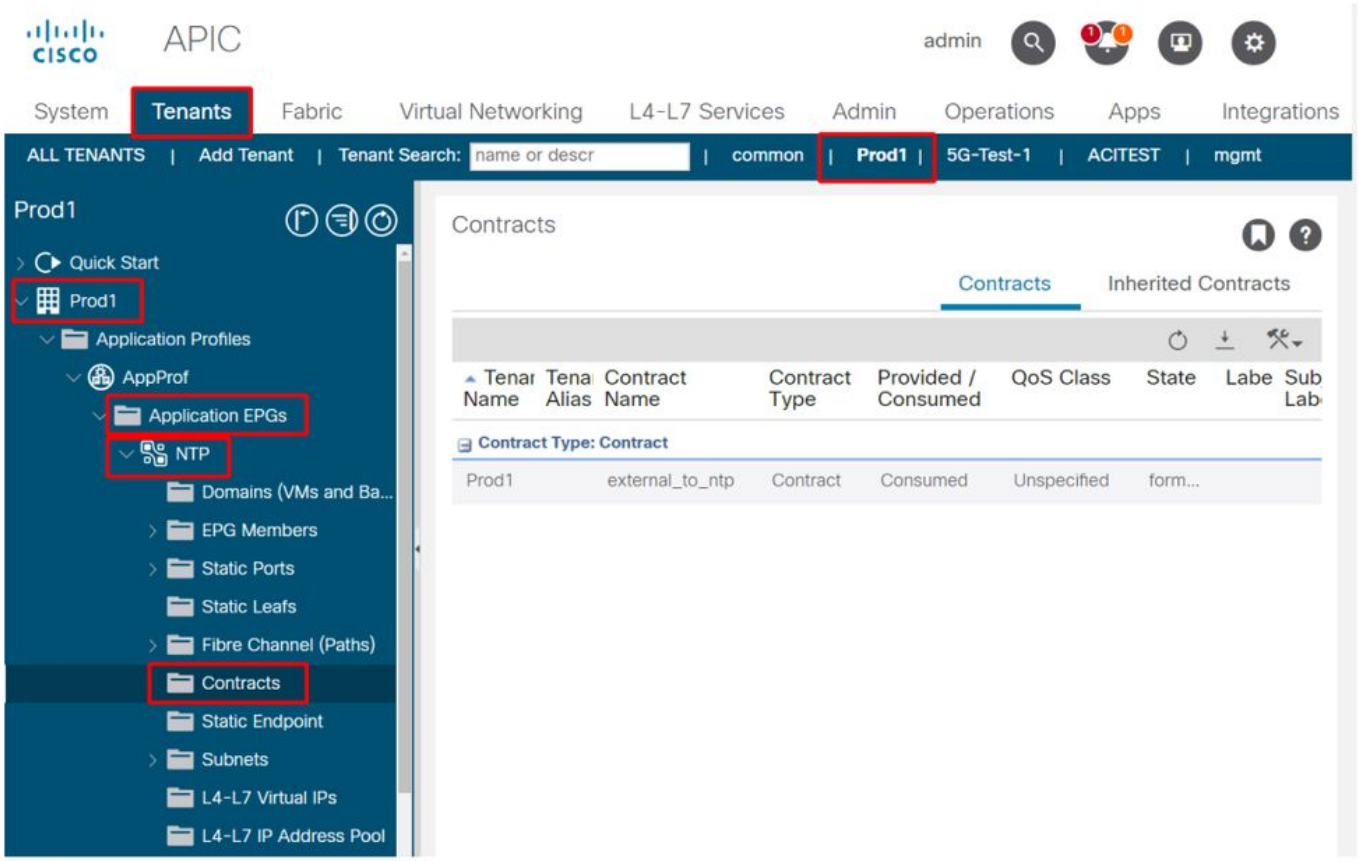
pcTag de EPG externo del proveedor



3. Compruebe que el EPG del consumidor tiene configurado un contrato de ámbito de arrendatario importado o un contrato global

El NTP de EPG de consumidor con subred definida en EPG/BD consume el contrato de ámbito 'arrendatario' o 'global'

Contrato consumido por EPG



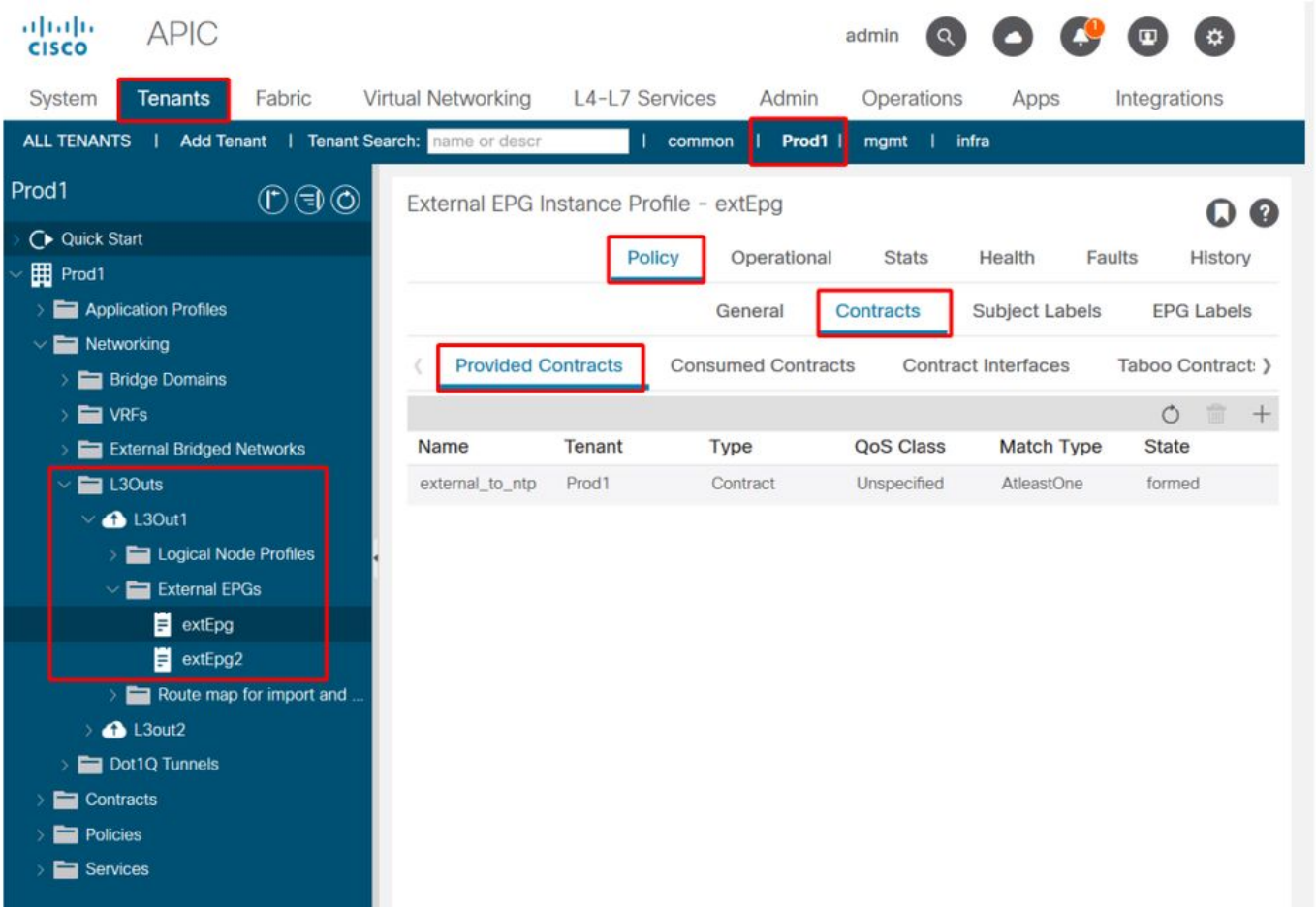
4. Verifique si el BD del EPG del consumidor tiene una subred configurada con su alcance configurado como 'Compartido entre VRF'

La subred del EPG se configura en el dominio de bridge pero debe tener el indicador 'shared between VRF' (para permitir la fuga de ruteo) y el indicador 'advertised externally' (para permitir anunciar a L3Out)

5. Compruebe que el EPG L3Out del proveedor tiene configurado un contrato de ámbito de arrendatario importado o un contrato global

El EPG L3Out debe tener un contrato de ámbito de arrendatario o un contrato global configurado como contrato proporcionado.

Contrato del proveedor L3Out



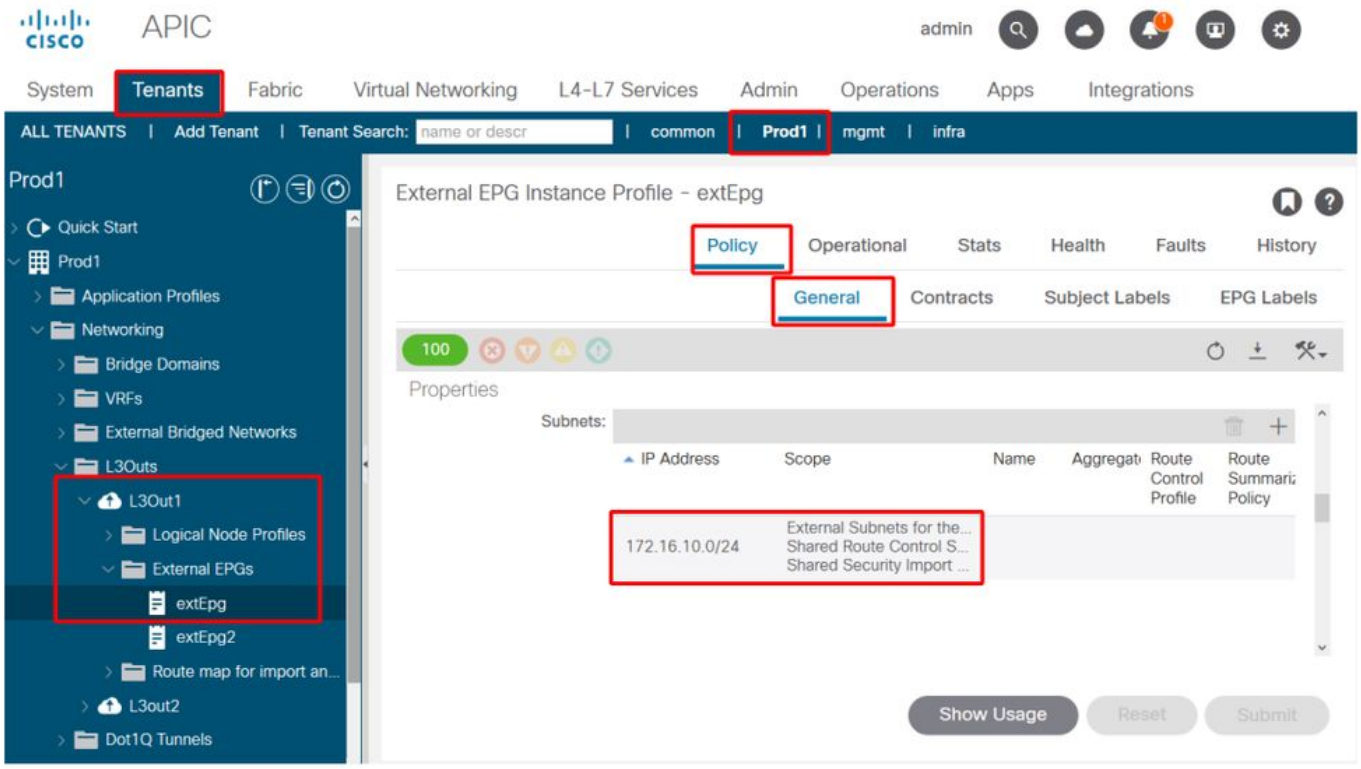
6. Compruebe si el EPG L3Out del proveedor tiene una subred configurada con los ámbitos necesarios marcados

El proveedor L3Out EPG debe tener el prefijo que se va a filtrar configurado con los siguientes ámbitos:

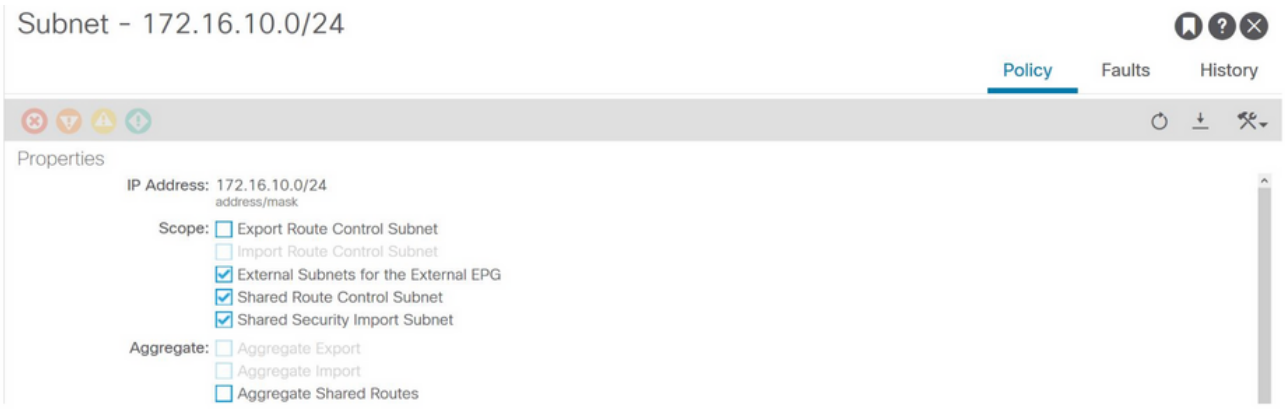
- Subredes externas para el EPG externo.
- Subred de control de rutas compartidas.
- Subred de importación de seguridad compartida.

Para obtener más información sobre el indicador de subred en el EPG L3Out, consulte el capítulo "Reenvío externo".

Configuración de subred EPG externa



Configuración de subred EPG externa expandida



7. Verifique la pcTag de la subred EPG L3Out en el VRF no BL para el consumidor

Cuando el tráfico destinado a la subred EPG externa ingresa en la no BL, se realiza una búsqueda en el prefijo de destino para determinar la pcTag. Esto se puede verificar usando el siguiente comando en el no BL.

Tenga en cuenta que esta salida se toma en el ámbito de VNI 2818048, que es el VRF VNID de consumidor. Al observar la tabla, el consumidor puede encontrar la pcTag del destino, aunque no esté en el mismo 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
```

El resultado anterior muestra la combinación de la subred EPG L3Out y su pcTag global 25.

8. Verifique las reglas de zonificación programadas en el VRF no BL para el consumidor

Utilice 'contract_parser.py' o el comando 'show zoning-rule' y especifique el VRF.

A continuación, los resultados del comando muestran que se instalan dos reglas de división en zonas para permitir el tráfico desde la pcTag 16410 local de EPG de consumidor a la pcTag global 25 de EPG L3Out. Esto se encuentra en el ámbito 2818048, que es el ámbito del VRF de consumidor.

```
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. Verifique las reglas de zonificación programadas en la BL para el VRF del proveedor

Utilice 'contract_parser.py' o el comando 'show zoning-rule' y especifique el VRF. Los siguientes resultados del comando muestran que **NO** hay reglas de zonificación específicas en el VRF del proveedor como se describió varias veces antes.

Está en el alcance 2719752 que es el alcance del VRF del proveedor.

```
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]
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).