Verify ACI Shared Services - Shared Service Consumer PcTag 14

Contents

Introduction

This document describes steps to configure and verify Shared Services configuration with Shared BD in ACI.

Background Information

A Shared Services configuration enables communication between EPGs across different VRFs within an ACI Fabric.

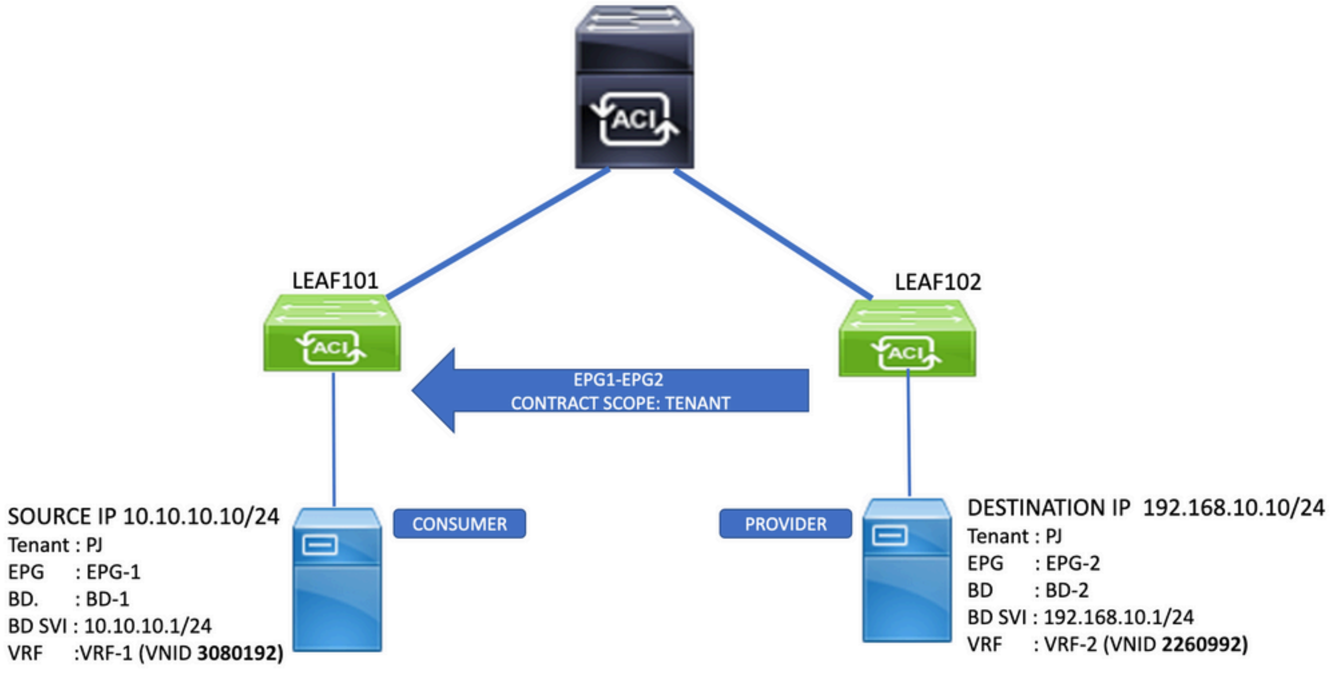
Shared Services takes full advantage of the 3 PcTag Categories:

Category Name	PcTag Range
System	1 - 15
Global	16 - 16385
Local	16386 - 65535

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Configuration Highlights

- The "Shared between VRFs" Subnet Scope is required on the subnet to be leaked, 192.168.10.1/24
- The Contract must have at least 'Tenant' Scope since the EPGs are in the same tenant. If the EPGs are in different tenants, the Contract must have 'Global' Scope
- If the Shared Subnet is defined under the Provider EPG, the Contract only needs to be Provided on the EPG to be shared and Consumed on the EPG to consume.

  OR

- If the Shared Subnet is defined under the Provider BD, the Contract must be Provided by both EPGs and Consumed by both EPGs and subnets on the BD only. This uses more TCAM space as more Zoning-Rules are programmed.

Note: VZany is not supported as a Provider of Shared services.

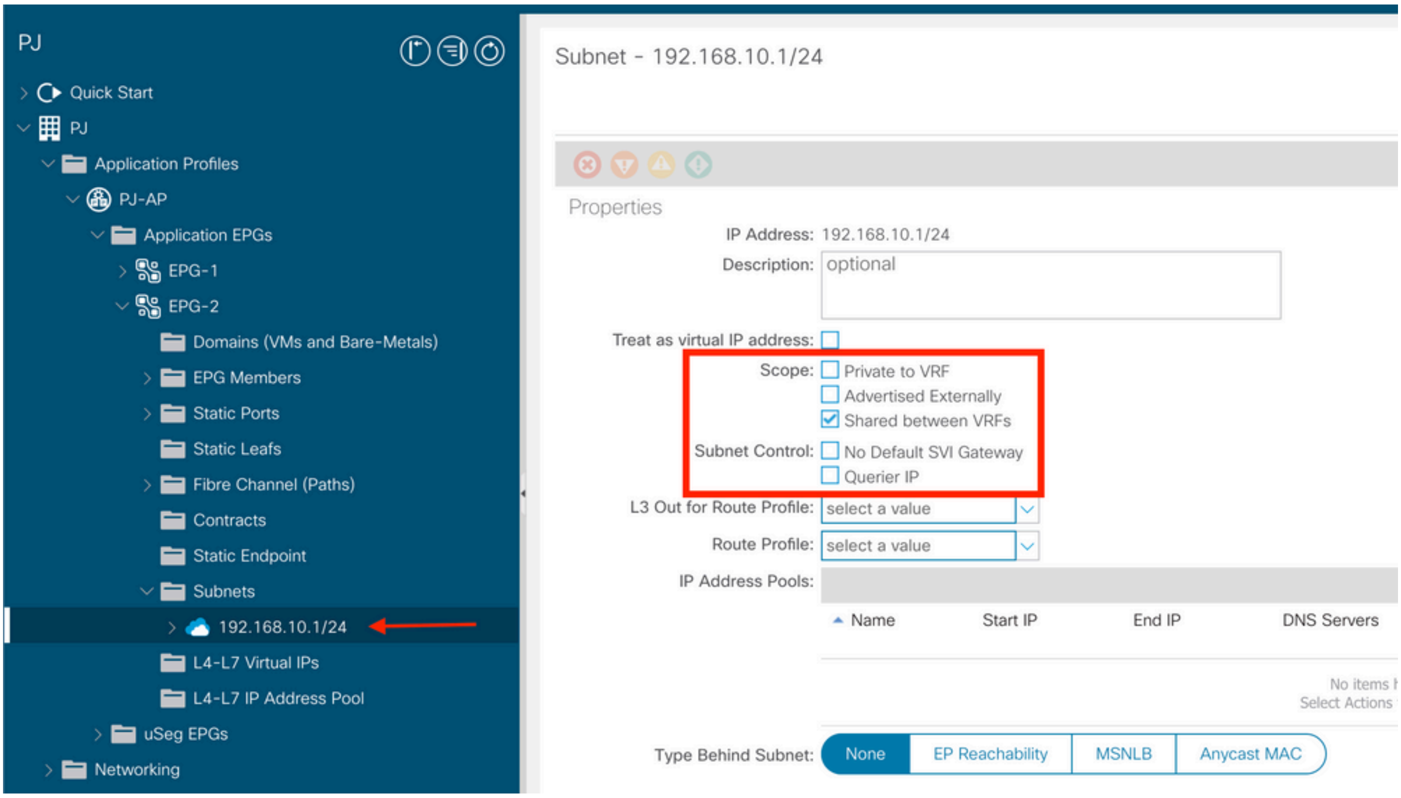
Verify

Scenario 1 - EPG-to-EPG: Shared Subnet defined in Provider EPG

In this example scenario, the Shared Subnet is configured under EPG-2.

Note: If the same subnet is defined under both an EPG and its associated BD, both definitions must have the same Scope values set.

This option optimizes TCAM utilzation and accomplishes the Shared Services configuration. TCAM is optimized as the Zoning-Rules only need to be programmed in the consumer VRF. In this scenario, the consumer VRF is only on Leaf 101.



Subnet - 192.168.10.1/24

Properties

IP Address: 192.168.10.1/24

Description: optional

Treat as virtual IP address: □

Scope: □ Private to VRF
□ Advertised Externally
☑ Shared between VRFs

Subnet Control: □ No Default SVI Gateway
□ Querier IP

L3 Out for Route Profile: select a value

Route Profile: select a value

IP Address Pools:

Name	Start IP	End IP	DNS Servers

No items h
Select Actions

Type Behind Subnet: [✓ None] EP Reachability MSNLB Anycast MAC

EPG-1 to EPG-2 Flow Trace

Consumer Leaf 101

The route information on Leaf 101 Consumer VRF PJ:VRF-1 shows the route for 192.168.10.10 via VNID **2260992**, which is Provider VRF PJ:VRF-2:

```
leaf101# show ip route 192.168.10.10 vrf PJ:VRF-1
IP Route Table for VRF "PJ:VRF-1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

192.168.10.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.240.33%overlay-1, [1/0], 23:06:11, static, tag 4294967294, rwVnid: vxlan-2260992
         recursive next hop: 10.0.240.33/32%overlay-1
```

The traffic flow can be validated with an ELAM on Consumer Leaf 101 against the ICMP Request from source 10.10.10.10 to destination 192.168.10.1

```
leaf101# vsh_lc
module-1# trigger reset
module-1# trigger init in-select 6 out-select 1
module-1# set outer ipv4 src_ip 10.10.10.10 dst_ip 192.168.10.10
module-1# start


module-1# ereport
...
------------------------------------------------------------------------------------------------
-----------------------------------
Outer L3 Header
```

```
------------------------------------------------------------------------------------------------
-----------------------------------
...
IP Protocol Number            : ICMP
IP CheckSum                   : 37262( 0x918E )
Destination IP                : 192.168.10.10
Source IP                     : 10.10.10.10
------------------------------------------------------------------------------------------------
-----------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
-----------------------------------
IP Protocol                             : ICMP( 0x1 )
L4 Src Port                             : 2048( 0x800 )
L4 Dst Port                             : 16568( 0x40B8 )
sclass (src pcTag)                      : 16388( 0x4004 )
dclass (dst pcTag)                      : 10930( 0x2AB2 )
src pcTag is from local table           : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet          : no
If yes, Contract is not applied here because it is flooded

------------------------------------------------------------------------------------------------
-----------------------------------
Contract Result
------------------------------------------------------------------------------------------------
-----------------------------------
Contract Drop                           : no
Contract Logging                        : no
Contract Applied                        : yes
Contract Hit                            : yes
Contract Aclqos Stats Index             : 81874
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81874" )
```

The ereport shows that the Contract is applied on Consumer Leaf 101 and that Src pcTag 16388 (EPG-1) and Dst PcTAG 10930 (EPG-2) were assigned.

These values can be compared to the programmed Zoning-Rules in Consumer VRF PJ:VRF-1 (VNID 3080192) to identify which Rule IDs were hit:

```
leaf101# show zoning-rule scope 3080192
+---------+--------+--------+----------+----------------+---------+---------+--------------+----
------+-----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  |     Name     |
Action  |        Priority        |
+---------+--------+--------+----------+----------------+---------+---------+--------------+----
------+-----------------------+
|   4117  | 10930  |   0    | implicit |    uni-dir     | enabled | 3080192 |              |
deny,log | shsrc_any_any_deny(12) |
|   4108  | 10930  | 16388  |    8     | uni-dir-ignore | enabled | 3080192 | PJ:EPG1-EPG2 |
permit  |     fully_qual(7)      |
|   4118  | 16388  | 10930  |    8     |     bi-dir     | enabled | 3080192 | PJ:EPG1-EPG2 |
permit  |     fully_qual(7)      |
+---------+--------+--------+----------+----------------+---------+---------+--------------+----
------+-----------------------+
```

> **Note**: An implicit deny rule is automatically created from Provider EPG-2 (PcTag 10930) to any (PcTag 0). This is to prevent communication from the Provider VRF to the Consumer VRF without additional contracts across EPGs.

EPG-2 to EPG-1 Flow Trace

Provider Leaf 102

The route information on Leaf 102 for Provider VRF PJ:VRF-2 shows the route for 10.10.10.10 via VNID **3080192**, which is Consumer VRF PJ:VRF-1:

```
leaf102# show ip route 10.10.10.10 vrf PJ:VRF-2
IP Route Table for VRF "PJ:VRF-2"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

10.10.10.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.240.33%overlay-1, [1/0], 1d22h, static, tag 4294967294, rwVnid: vxlan-3080192
         recursive next hop: 10.0.240.33/32%overlay-1
```

The traffic flow can be validated with an ELAM on Provider Leaf 101 against the ICMP Request from Source 192.168.10.10 to Destination 10.10.10.10:

```
leaf102# trigger reset
module-1# trigger init in-select 6 out-select 1
module-1# set outer ipv4 src_ip 192.168.10.10 dst_ip 10.10.10.10
module-1# start


module-1# ereport
... ---------------------------------------------------------------------------------------------
--------------------------------------- Outer L3 Header ----------------------------------------
------------------------------------------------------------------------------------------- ...
IP Protocol Number : ICMP IP CheckSum : 37262( 0x918E ) Destination IP                :
10.10.10.10
Source IP                   : 192.168.10.10

------------------------------------------------------------------------------------------------
-----------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
-----------------------------------
IP Protocol                             : ICMP( 0x1 )
L4 Src Port                             : 0( 0x0 )
L4 Dst Port                             : 18616( 0x48B8 )
sclass (src pcTag)                      : 10930( 0x2AB2 )
dclass (dst pcTag)                      : 14( 0xE )
src pcTag is from local table           : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet          : no
If yes, Contract is not applied here because it is flooded

------------------------------------------------------------------------------------------------
-----------------------------------
Contract Result
------------------------------------------------------------------------------------------------
-----------------------------------
Contract Drop                           : no
Contract Logging                        : no
Contract Applied                        : no
Contract Hit                            : yes
Contract Aclqos Stats Index             : 81873
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81873" )
```

In this ereport, observe that the sclass and dclass are both non-local values.

EPG-2, the Shared Service Provider, now drives a Global PcTag of10930.

The dclass assigned to this packet is **Shared Service Consumer PcTag 14**. PcTag 14 is the System PcTag reserved for Inter-VRF traffic.

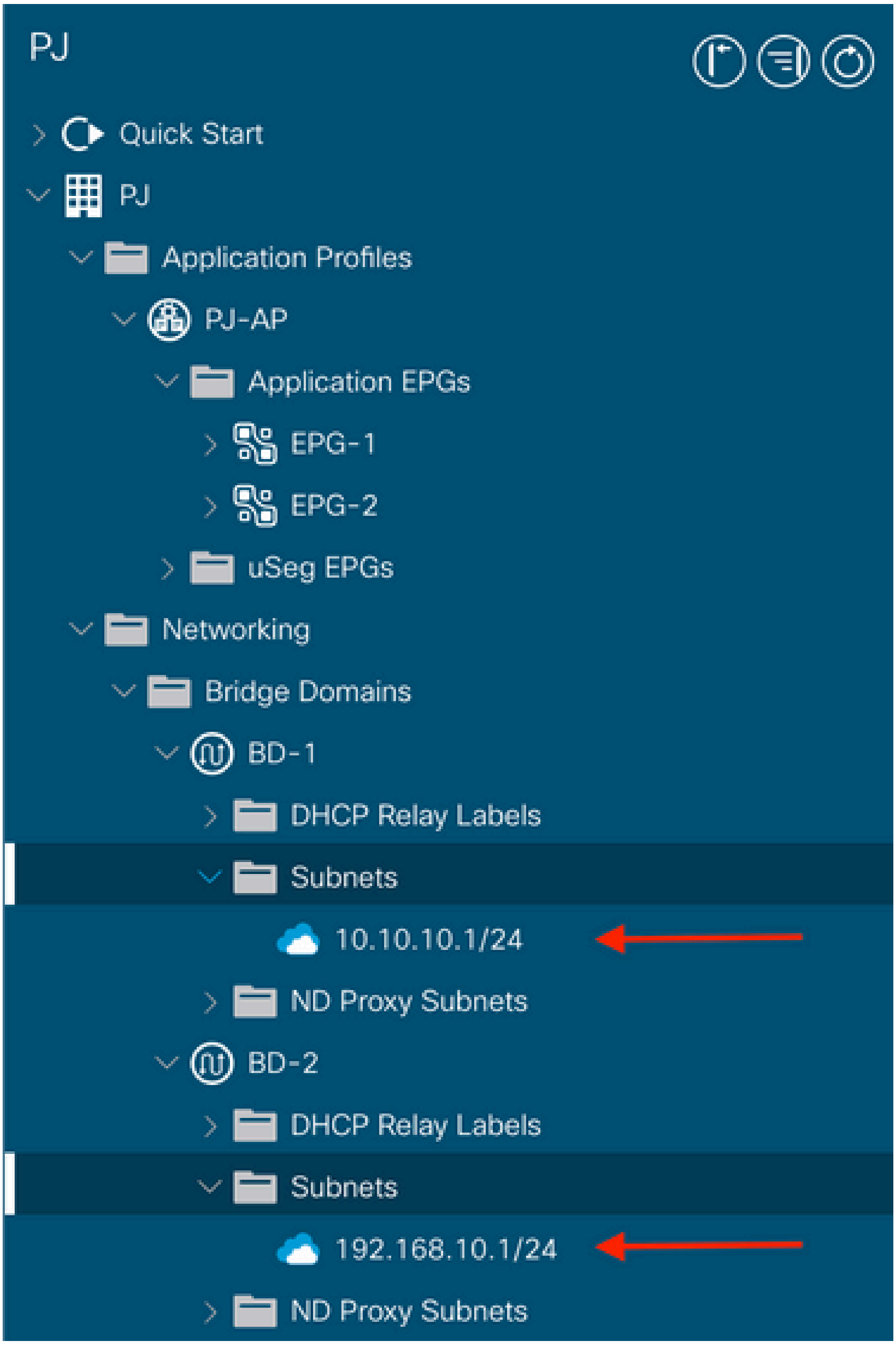
Observe there is a special Zoning-Rule programmed on Provider Leaf 102 between Provider EPG2 PcTag 10930 and Shared Service Consumer System PcTag 14 with the "Action" set to **"permit_override".** This rule allows matched flows to forward on to the Consumer Leaf for final policy lookup:

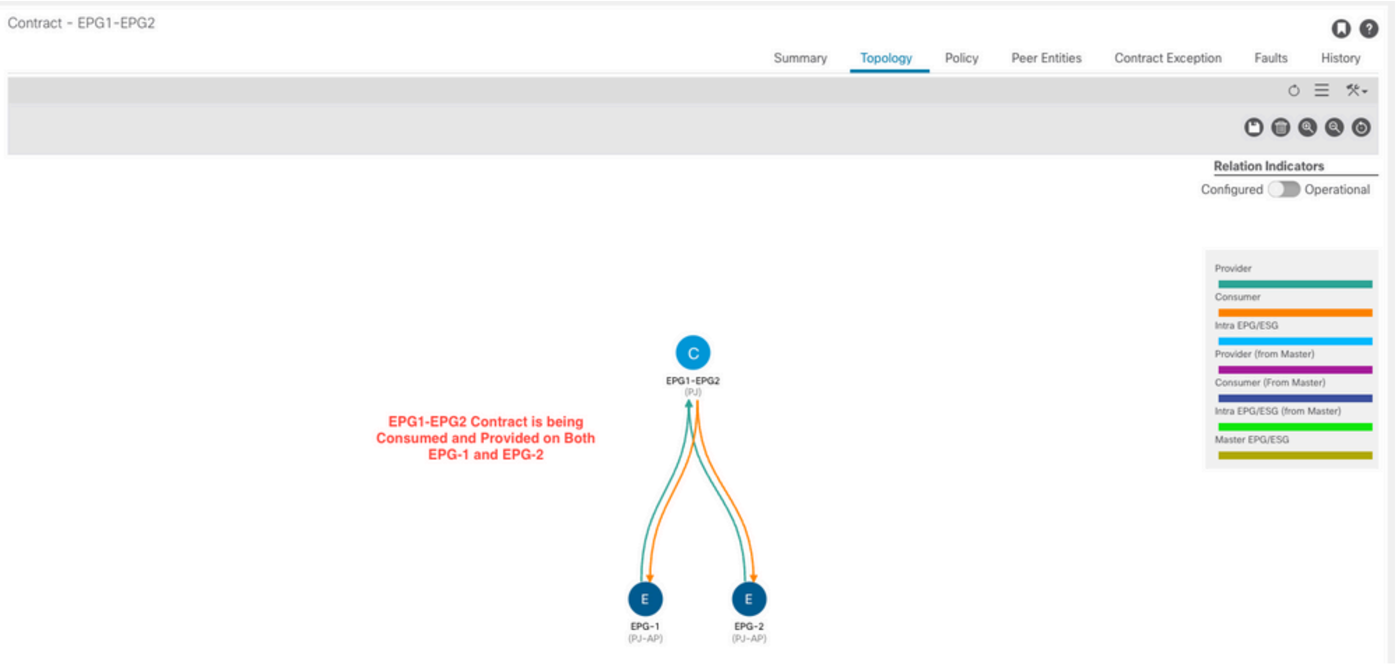
```
leaf102# show zoning-rule
+---------+--------+--------+----------+---------+---------+----------+------+-----------------
+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope   | Name |      Action     |
Priority       |
+---------+--------+--------+----------+---------+---------+----------+------+-----------------
+----------------------+
|   4113  | 10930  |   14   | implicit | uni-dir | enabled | 2260992  |      | permit_override |
src_dst_any(9)    |
+---------+--------+--------+----------+---------+---------+----------+------+-----------------
+----------------------+
```

Scenario 2 - BD-to-BD: Shared Subnet defined in Provider BD.

In this example scenario, the Shared Subnet is only configured in BD-2.

To complete the Shared Services configuration, Contracts must be both Consumed and Provided on both EPGs; EPG-1 and EPG-2.


PJ
Quick Start
PJ
Application Profiles
PJ-AP
Application EPGs
EPG-1
EPG-2
uSeg EPGs
Networking
Bridge Domains
BD-1
DHCP Relay Labels
Subnets
10.10.10.1/24
ND Proxy Subnets
BD-2
DHCP Relay Labels
Subnets
192.168.10.1/24
ND Proxy Subnets



EPG1-EPG2 Contract is being Consumed and Provided on Both EPG-1 and EPG-2

EPG-1 to EPG-2 Flow Trace

As a Shared Service Contract is Provided and Consumed on both EPGs, a packet flow between EPG-1 (Leaf 101) and EPG-2 (Leaf 102) observes these properties:

- EPG-1 is considered the Provider
- EPG-2 is considered the Consumer
- Leaf 102 is the Consumer leaf, and so final policy is applied here.

The route information is the same as Scenario 1.

"Provider" Leaf 101:

```
Leaf101# vsh_lc
module-1# trigger reset
module-1# trigger init in-select 6 out-select 1
module-1# set outer ipv4 src_ip 10.10.10.10 dst_ip 192.168.10.10
module-1# start
module-1# status


module-1# ereport
... ---------------------------------------------------------------------------------------------
--------------------------------------- Outer L3 Header ---------------------------------------
---------------------------------------------------------------------------------------------- ...
IP Protocol Number : ICMP IP CheckSum : 23304( 0x5B08 ) Destination IP               :
192.168.10.10
Source IP                     : 10.10.10.10

-----------------------------------------------------------------------------------------------
-----------------------------------
Contract Lookup Key
-----------------------------------------------------------------------------------------------
-----------------------------------
IP Protocol                               : ICMP( 0x1 )
L4 Src Port                               : 2048( 0x800 )
L4 Dst Port                               : 59074( 0xE6C2 )
sclass (src pcTag)                        : 18( 0x12 )
```

```
dclass (dst pcTag)                      : 14( 0xE )
src pcTag is from local table           : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet          : no
If yes, Contract is not applied here because it is flooded

------------------------------------------------------------------------------------------------
-----------------------------------
Contract Result
------------------------------------------------------------------------------------------------
-----------------------------------
Contract Drop                           : no
Contract Logging                        : no
Contract Applied                        : no
Contract Hit                            : yes
Contract Aclqos Stats Index             : 81873
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81873" )
```

Observe that dclass 14 is assigned. This means the traffic is allowed to continue via the "permit_override" rule so that the Consumer Leaf can drive the final policy lookup.

"Consumer" Leaf 102

```
Leaf102# vsh_lc
module-1# trigger reset
module-1# trigger init in-select 14 out-select 1
module-1# set inner ipv4 src_ip 10.10.10.10  dst_ip 192.168.10.10
module-1# start

module-1# ereport
...
------------------------------------------------------------------------------------------------
----------------------------------- Inner L3 Header --------------------------------------------
------------------------------------------------------------------------------------------ ... IP
Protocol Number : ICMP Destination IP                : 192.168.10.10
Source IP                     : 10.10.10.10

------------------------------------------------------------------------------------------------
-----------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
-----------------------------------
IP Protocol                             : ICMP( 0x1 )
L4 Src Port                             : 2048( 0x800 )
L4 Dst Port                             : 26203( 0x665B )
sclass (src pcTag)                      : 18( 0x12 )
dclass (dst pcTag)                      : 10930( 0x2AB2 )
src pcTag is from local table           : no
derived from group-id in iVxLAN header of incoming packet
Unknown Unicast / Flood Packet          : no
If yes, Contract is not applied here because it is flooded

------------------------------------------------------------------------------------------------
-----------------------------------
Contract Result
------------------------------------------------------------------------------------------------
-----------------------------------
Contract Drop                           : no
Contract Logging                        : no
Contract Applied                        : yes
Contract Hit                           : yes
Contract Aclqos Stats Index            : 81874
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81874" )
```

Observe that both EPG-1 and EPG-2 now have Global PcTags; EPG-1 is PcTag 18 and EPG-2 is PcTag 10938.

EPG-2 to EPG-1 Flow Trace

As a Shared Service Contract is Provided and Consumed on both EPGs, a packet flow between EPG-2 (Leaf 102) and EPG-1 (Leaf 101) observes these properties:

- EPG-2 is considered the Provider
- EPG-1 is considered the Consumer
- Leaf 101 is the Consumer leaf, and so final policy is applied here.

The route information is the same as Scenario 1.

"Provider" Leaf 102

```
Leaf102# vsh_lc
module-1# trigger reset
module-1# trigger init in-select 6 out-select 1
module-1# set outer ipv4 src_ip 192.168.10.10 dst_ip 10.10.10.10
module-1# start


module-1# ereport
... -------------------------------------------------------------------------------------------
---------------------------------------- Outer L3 Header ---------------------------------------
--------------------------------------------------------------------------------------------- ...
IP Protocol Number : ICMP IP CheckSum : 23308( 0x5B0C ) Destination IP                :
10.10.10.10
Source IP                    : 192.168.10.10


------------------------------------------------------------------------------------------------
-----------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
-----------------------------------
IP Protocol                            : ICMP( 0x1 )
L4 Src Port                            : 0( 0x0 )
L4 Dst Port                            : 56682( 0xDD6A )
sclass (src pcTag)                     : 10930( 0x2AB2 )
dclass (dst pcTag)                     : 14( 0xE )
src pcTag is from local table          : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet         : no
If yes, Contract is not applied here because it is flooded

------------------------------------------------------------------------------------------------
-----------------------------------
Contract Result
------------------------------------------------------------------------------------------------
-----------------------------------
Contract Drop                          : no
Contract Logging                       : no
Contract Applied                       : no
Contract Hit                           : yes
Contract Aclqos Stats Index            : 81873
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81873" )
```

Observe that dclass 14 is assigned. This means the traffic is allowed to continue via the "permit_override" rule so that the Consumer Leaf can drive the final policy lookup.

"Consumer" Leaf 101

```
Leaf101# vsh_lc
module-1# trigger reset
module-1# trigger init in-select 6 out-select 1
module-1# set outer ipv4 src_ip 192.168.10.10 dst_ip 10.10.10.10
module-1# start


module-1# ereport
------------------------------------------------------------------------------------------------
----------------------------------- Inner L3 Header --------------------------------------------
--------------------------------------------------------------------------------------- L3 Type
: IPv4 DSCP : 0 Don't Fragment Bit : 0x0 TTL : 254 IP Protocol Number : ICMP Destination IP
: 10.10.10.10
Source IP                   : 192.168.10.10

------------------------------------------------------------------------------------------------
-----------------------------------
------------------------------------------------------------------------------------------------
-----------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
-----------------------------------
IP Protocol                            : ICMP( 0x1 )
L4 Src Port                            : 0( 0x0 )
L4 Dst Port                            : 22874( 0x595A )
sclass (src pcTag)                     : 10930( 0x2AB2 )
dclass (dst pcTag)                     : 18( 0x12 )
src pcTag is from local table          : no
derived from group-id in iVxLAN header of incoming packet
Unknown Unicast / Flood Packet         : no
If yes, Contract is not applied here because it is flooded

------------------------------------------------------------------------------------------------
-----------------------------------
Contract Result
------------------------------------------------------------------------------------------------
-----------------------------------
Contract Drop                          : no
Contract Logging                       : no
Contract Applied                       : yes
Contract Hit                           : yes
Contract Aclqos Stats Index            : 81874
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81874" )
```

TCAM Usage Highlight

In the BD-to-BD scenario, observe that Zoning-Rules have doubled since both EPG-1 and EPG-2 are Shared Services Contract Consumers:

```
Leaf101# show zoning-rule scope 3080192
+---------+--------+--------+----------+----------------+---------+---------+--------------+----
-------------+-----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  |     Name     |
Action      |        Priority        |
+---------+--------+--------+----------+----------------+---------+---------+--------------+----
-------------+-----------------------+
|   4117  | 10930  |    0   | implicit |    uni-dir     | enabled | 3080192 |              |
deny,log    | shsrc_any_any_deny(12) |
|   4129  |   18   |   14   | implicit |    uni-dir     | enabled | 3080192 |              |
permit_override |     src_dst_any(9)      |
|   4128  | 10930  |   18   |    8     |     bi-dir     | enabled | 3080192 | PJ:EPG1-EPG2 |
permit      |      fully_qual(7)       |
|   4127  |   18   | 10930  |    8     | uni-dir-ignore | enabled | 3080192 | PJ:EPG1-EPG2 |
permit      |      fully_qual(7)       |
+---------+--------+--------+----------+----------------+---------+---------+--------------+----
-------------+-----------------------+
```

```
Leaf102# show zoning-rule scope 2260992
+---------+--------+--------+----------+----------------+---------+---------+--------------+----
-------------+-----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  |     Name     |
Action      |        Priority        |
+---------+--------+--------+----------+----------------+---------+---------+--------------+----
-------------+-----------------------+
|   4113  | 10930  |   14   | implicit |    uni-dir     | enabled | 2260992 |              |
permit_override |     src_dst_any(9)      |
|   4123  |   18   | 10930  |    8     |     bi-dir     | enabled | 2260992 | PJ:EPG1-EPG2 |
permit      |      fully_qual(7)       |
|   4124  |   18   |    0   | implicit |    uni-dir     | enabled | 2260992 |              |
deny,log    | shsrc_any_any_deny(12) |
|   4122  | 10930  |   18   |    8     | uni-dir-ignore | enabled | 2260992 | PJ:EPG1-EPG2 |
permit      |      fully_qual(7)       |
+---------+--------+--------+----------+----------------+---------+---------+--------------+----
-------------+-----------------------+
```

> **Note**: Observe that the number of implicit "**shsrc_any_any_deny**" and "**permit_override**" Zoning-Rules has also doubled due to this configuration.

Conclusion

Both configuration scenarios accomplish the Shared Services functionality, however the BD-to-BD method comes at the cost of extra TCAM consumption.

References & Useful links

Cisco ACI Contract Guide

Understand and Troubleshoot ACI Shared Services - DGTL-TSCDCN-305