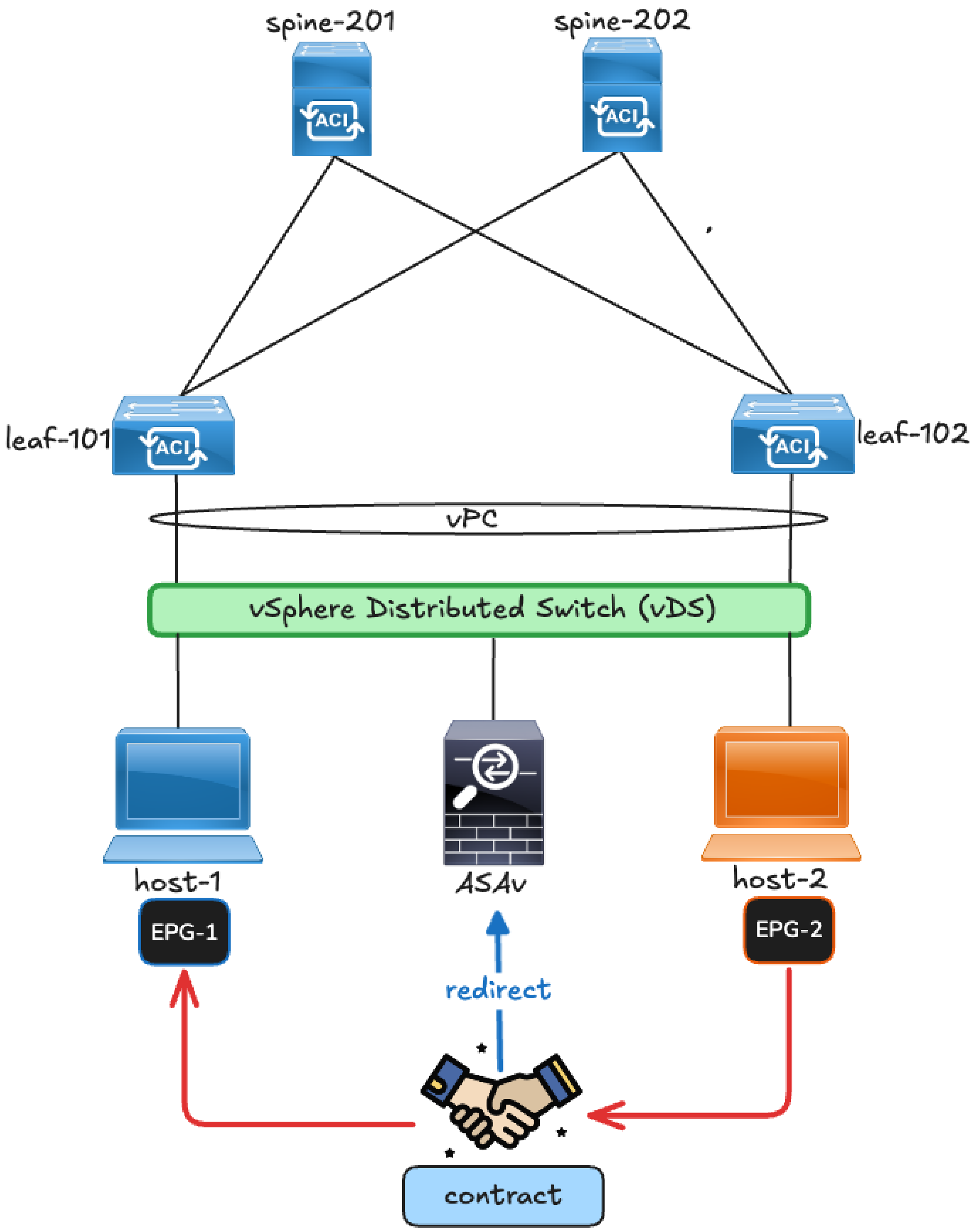
Lab by Titus Majeza

Cisco ACI L4-L7 Policy-Based Redirect (PBR)

(https://www.linkedin.com/in/titus-majeza/)



For more labs visit my GitHub repo: https://github.com/TitusM/Cisco-Data-Center

Note
This lab was conducted in a controlled environment. Any configurations in a production network should be implemented during a designated maintenance window. Additionally, always refer to official Cisco documentation relevant to your specific hardware and software.

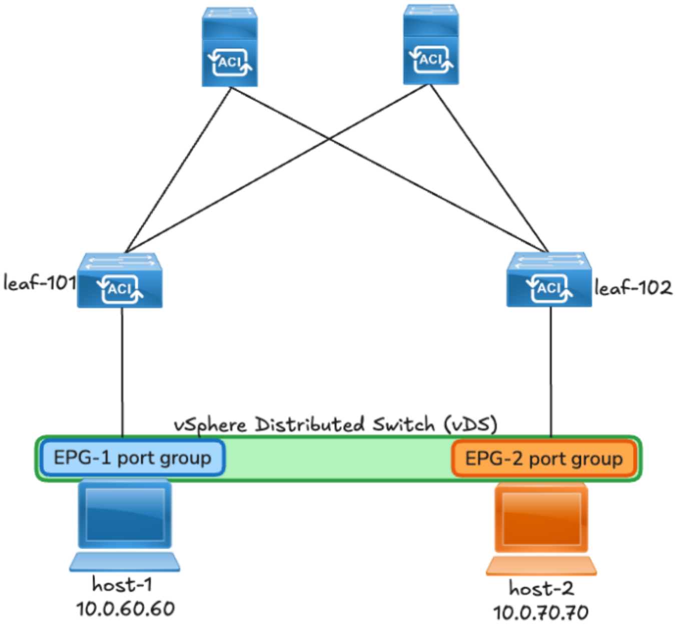
“Better to do something imperfectly than to do nothing flawlessly.” Robert H. Schuller

Introduction

Cisco ACI provides the capability to insert Layer 4 through Layer 7 devices (e.g. firewall, load balancer etc.) using a Service Graph. These devices are inserted between Endpoint Groups/Endpoint Security Groups. Cisco ACI Layer 4 – Layer 7 Policy-Based Redirect (PBR) is one of Cisco's most powerful features. ACI PBR allows traffic between two EPGs/ESGs to be bend towards an L4-L7 device. This lab showcases how to configure Cisco ACI L4-L7 PBR and how to validate the configuration. Furthermore, ELAM is used to showcase the packet walk from the source host **=>** firewall **=>** destination host.

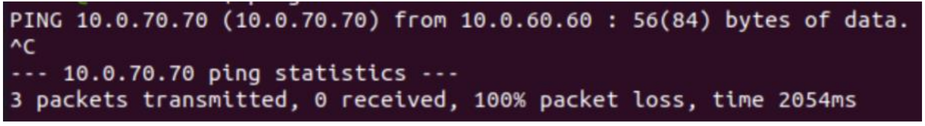
The Cisco Adaptive Security Virtual Appliance (ASAv) will be deployed as a firewall service in the Cisco ACI fabric. In this lab, ACI is already integrated with vCenter via VMM domain. The configurations in this lab are based on a one-arm deployment design whereby the same firewall interface is used for traffic entering and leaving the firewall.

Initial Configuration State



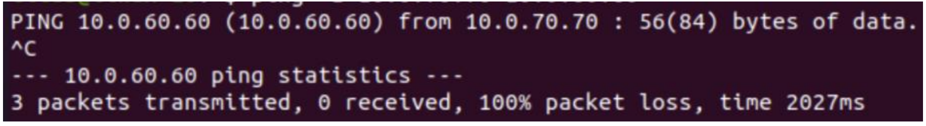
The initial communication state of the endpoints is shown by the output below.

host-1 (10.0.60.60) cannot ping host-2 (10.0.70.70).



```
PING 10.0.70.70 (10.0.70.70) from 10.0.60.60 : 56(84) bytes of data.
^C
--- 10.0.70.70 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2054ms
```

Vice-versa host-2 (10.0.70.70) cannot ping host-1 (10.0.60.60).



```
PING 10.0.60.60 (10.0.60.60) from 10.0.70.70 : 56(84) bytes of data.
^C
--- 10.0.60.60 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2027ms
```

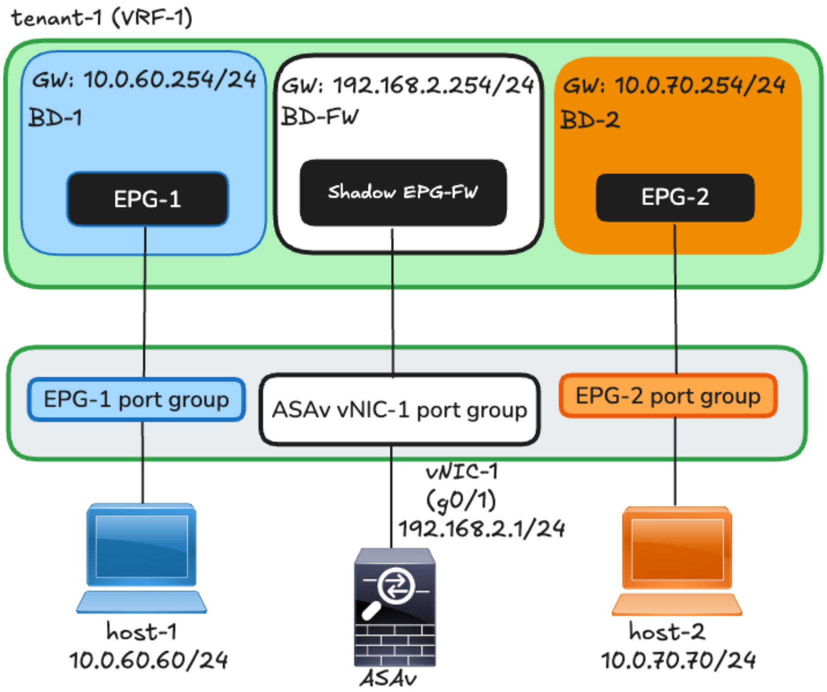
"Better to do something imperfectly than to do nothing flawlessly." Robert H. Schuller

Desired Configuration State

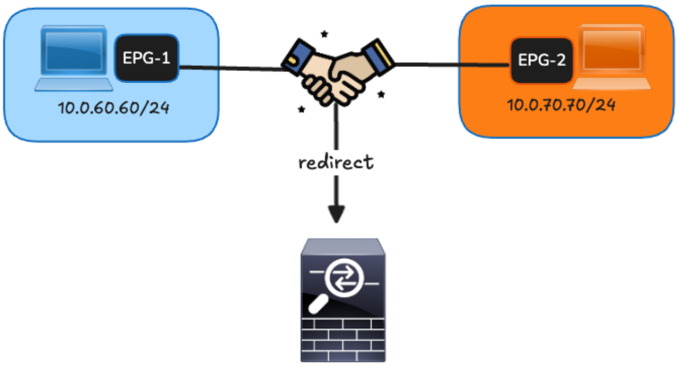
The desired configuration state for this lab is:

1. Configure the Service Device (firewall) Bridge Domain with a default gateway.
2. Configure the firewall with all the required configuration that will allow redirected traffic to traverse through.
3. Configure all the required elements for ACI Service Graph with PBR (Device, Redirect Policy, Service Graph Template, Device Selection Policy and the Contract that will be applied between the two EPGs).

   The image below shows the setup that will be in place to accomplish the required policy based redirect when host-1 in EPG-1 is communicating with host-2 in EPG-2.



A contract permitting all IP traffic will be applied between EPG-1 (consumer) and EPG-2 (provider). The contract's subject will be associated with the Service Graph Template to achieve the required Policy Based Redirect action.



"Better to do something imperfectly than to do nothing flawlessly." Robert H. Schuller

Lab Configurations

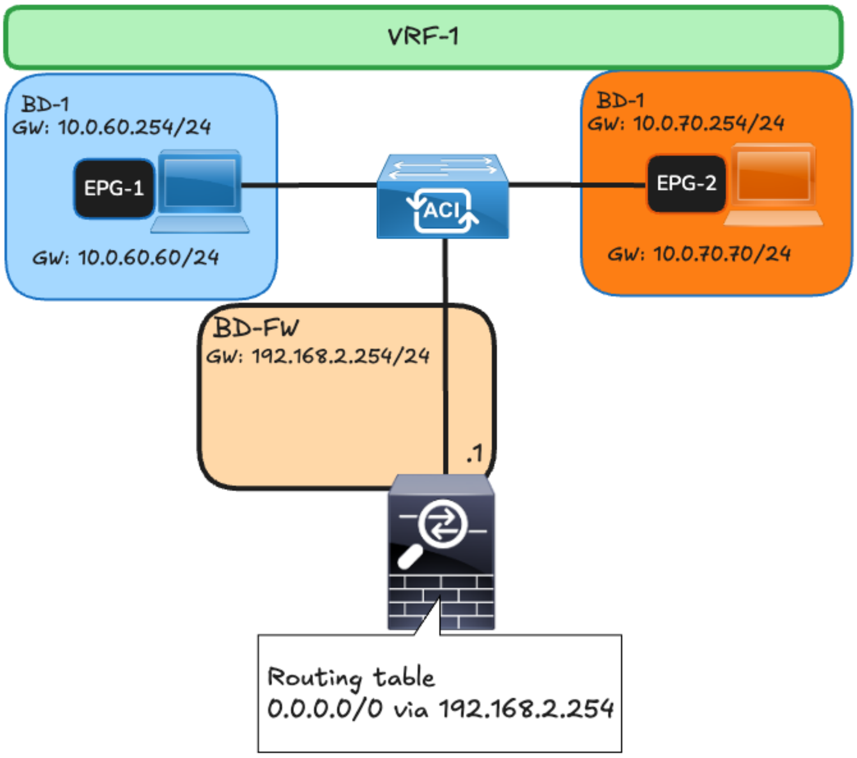
ASAv Basic Configuration

This lab does not showcase how to deploy an ASAv on VMWare vCenter, however it will showcase the basic configuration that is applied on the firewall instance.

```
ASAv#
!
interface GigabitEthernet0/0
  nameif inside
  security-level 50
  ip address 192.168.2.1 255.255.255.0
!
access-group permit_ACI in interface inside
access-list permit_ACI extended permit ip any any
!
same-security-traffic permit intra-interface
!
route inside 0.0.0.0 0.0.0.0 192.168.2.254
```

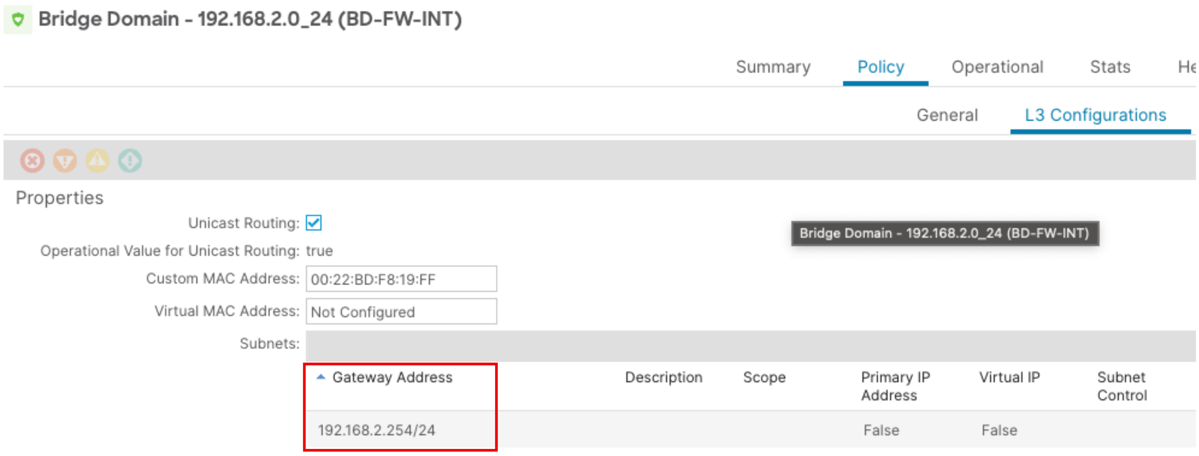
Firewall configuration considerations
The firewall may deny traffic coming into and going out through the same interface. You should configure the firewall to permit intra-interface traffic. For example, Cisco ASA denies intra-interface traffic by default.
To allow intra-interface traffic, configure **same-security-traffic permit intra-interface** on the ASA.

A simple static routing configuration is applied on the firewall pointing to the default address that is configured on ACI.



"Better to do something imperfectly than to do nothing flawlessly." Robert H. Schuller

The PBR node Bridge Domain is configured as follows:



Bridge Domain - 192.168.2.0_24 (BD-FW-INT)

Properties

Unicast Routing: ☑

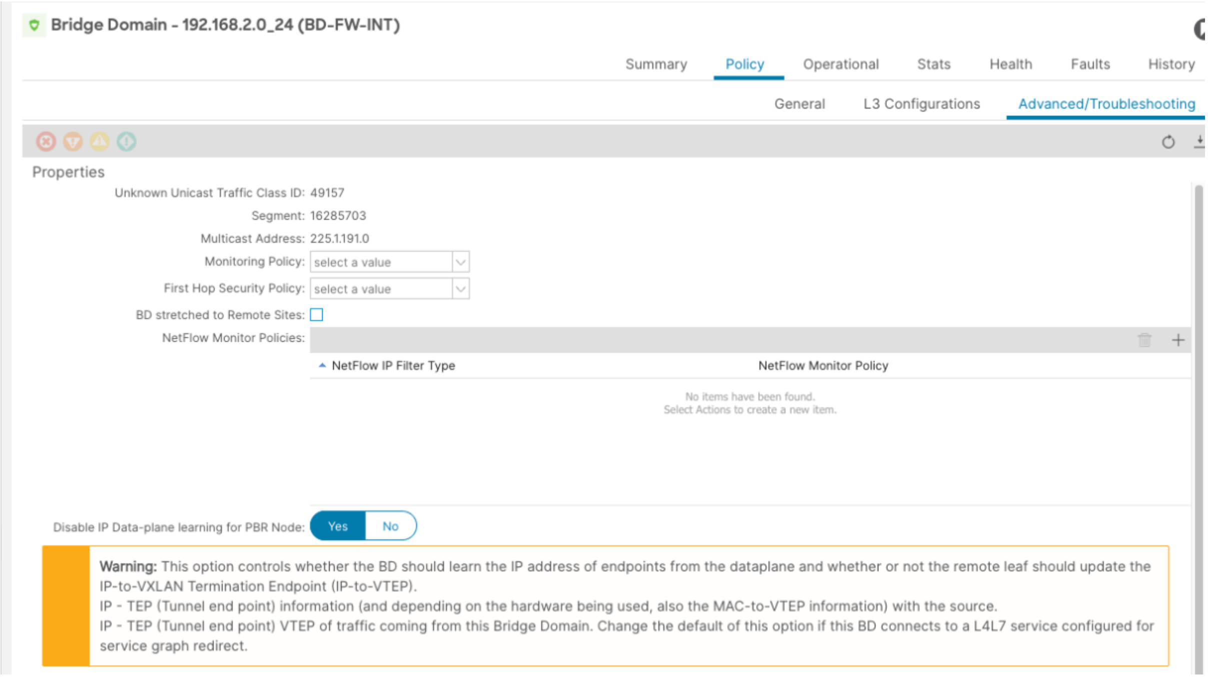
Operational Value for Unicast Routing: true

Custom MAC Address: 00:22:BD:F8:19:FF

Virtual MAC Address: Not Configured

Subnets:

Gateway Address	Description	Scope	Primary IP Address	Virtual IP	Subnet Control
192.168.2.254/24			False	False	



Bridge Domain - 192.168.2.0_24 (BD-FW-INT)

Properties

Unknown Unicast Traffic Class ID: 49157

Segment: 16285703

Multicast Address: 225.1.191.0

Monitoring Policy: select a value

First Hop Security Policy: select a value

BD stretched to Remote Sites: □

NetFlow Monitor Policies:

NetFlow IP Filter Type	NetFlow Monitor Policy

No items have been found.
Select Actions to create a new item.

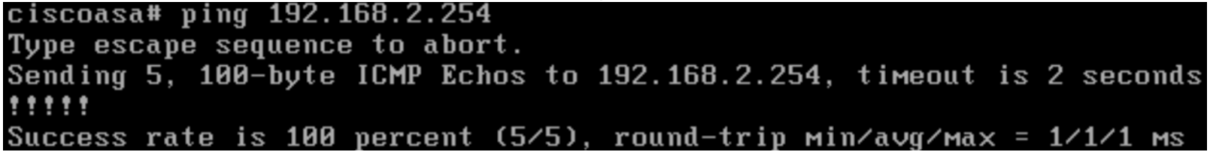
Disable IP Data-plane learning for PBR Node: [✓ Yes] No

Warning: This option controls whether the BD should learn the IP address of endpoints from the dataplane and whether or not the remote leaf should update the IP-to-VXLAN Termination Endpoint (IP-to-VTEP).
IP - TEP (Tunnel end point) information (and depending on the hardware being used, also the MAC-to-VTEP information) with the source.
IP - TEP (Tunnel end point) VTEP of traffic coming from this Bridge Domain. Change the default of this option if this BD connects to a L4L7 service configured for service graph redirect.

After the configuration has been applied on the firewall and ACI – verify that spine coop database has the firewall's MAC and IP address.

```
S1001# show coop internal info repo ep key 16285703 00:50:56:B3:0B:46 | egrep "EP|Real" | head -n 7
EP bd vnid : 16285703
EP mac :  00:50:56:B3:0B:46 (MAC address of the Firewall interface)
Current published TEP : 10.0.152.66
Real IPv4 EP : 192.168.2.1 (IP address of the firewall interface)
```

Verify that the firewall has reachability to its default gateway.



```
ciscoasa# ping 192.168.2.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.254, timeout is 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

The table below shows the elements required to configure PBR:

Device	The device provides information on the interfaces and logical connectors of the firewall/service device.
Redirect Policy	The redirect policy defines the "next-hop" information.

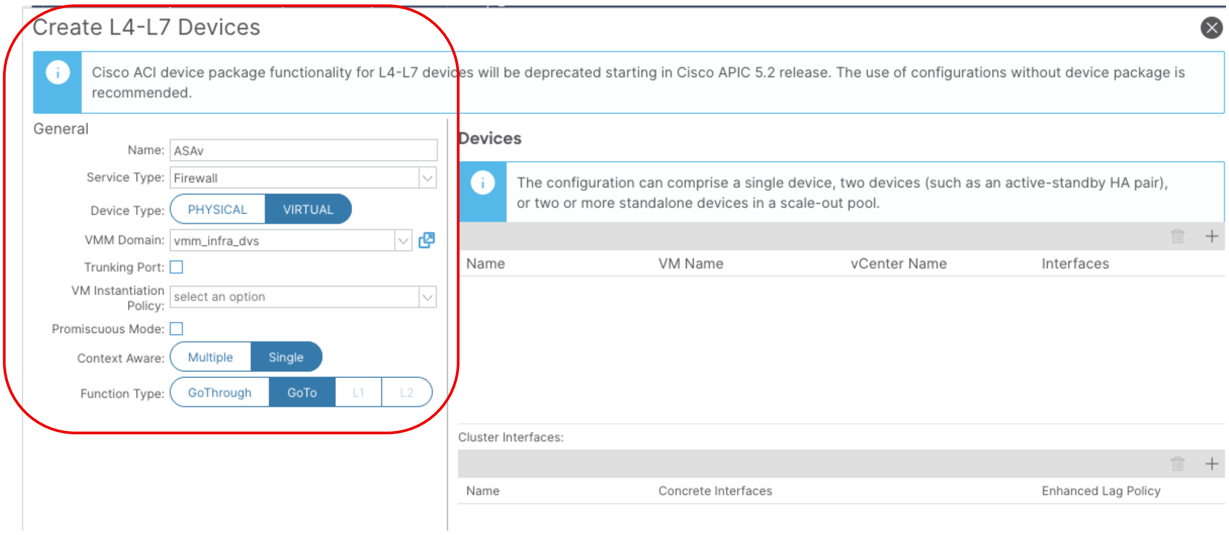
"Better to do something imperfectly than to do nothing flawlessly." Robert H. Schuller

Service Graph Template	The Service Graph Template defines “how” traffic should flow.
Device Selection Policy	The Device Selection Policy ties the logical device to a Service Graph template and contract. It defines how the Device will communicate with the fabric.
Contract	The Subject of the contract will be associated with the Service graph template so that the “redirect” policy will take effect when the contract is applied between two EPGs. The contract defines the type of traffic that will be redirected to the firewall.

Now let’s get into the configuration steps required for PBR.

1. **Create a L4-L7 Device (Cisco ASAv – firewall)**

Navigate to the **tenant >> Services >> L4-L7 >> Devices >> Create L4-L7 Devices**



Create L4-L7 Devices

Cisco ACI device package functionality for L4-L7 devices will be deprecated starting in Cisco APIC 5.2 release. The use of configurations without device package is recommended.

General

Name: ASAv
Service Type: Firewall
Device Type: PHYSICAL | VIRTUAL
VMM Domain: vmm_infra_dvs
Trunking Port: □
VM Instantiation Policy: select an option
Promiscuous Mode: □
Context Aware: Multiple | Single
Function Type: GoThrough | GoTo | L1 | L2

Devices

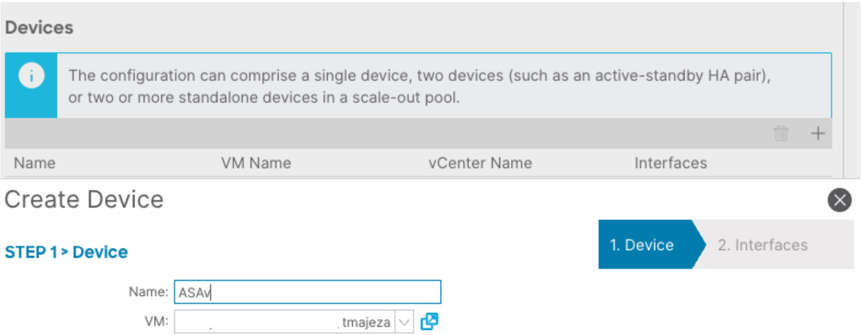
The configuration can comprise a single device, two devices (such as an active-standby HA pair), or two or more standalone devices in a scale-out pool.

Name	VM Name	vCenter Name	Interfaces

Cluster Interfaces:

Name	Concrete Interfaces	Enhanced Lag Policy

Click the (+) sign under **Devices** to add the concrete device details:



Devices

The configuration can comprise a single device, two devices (such as an active-standby HA pair), or two or more standalone devices in a scale-out pool.

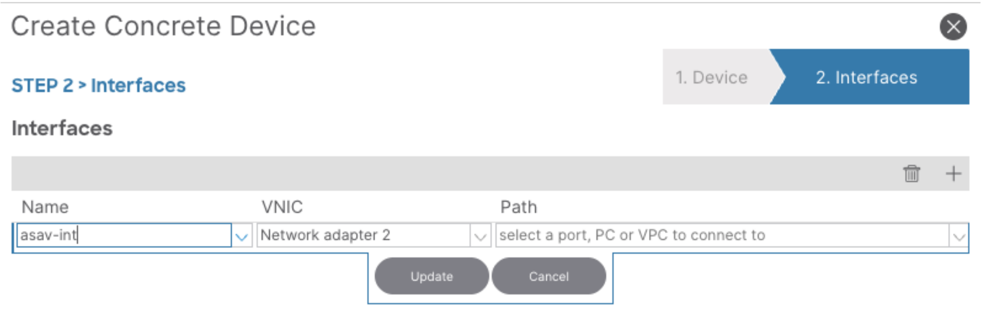
Name	VM Name	vCenter Name	Interfaces

Create Device

STEP 1 > Device

Name: ASAv
VM: tmajeza

Since ACI is already integrated with vCenter via VMM integration, the firewall VM will appear on the VM options.



Create Concrete Device

STEP 2 > Interfaces

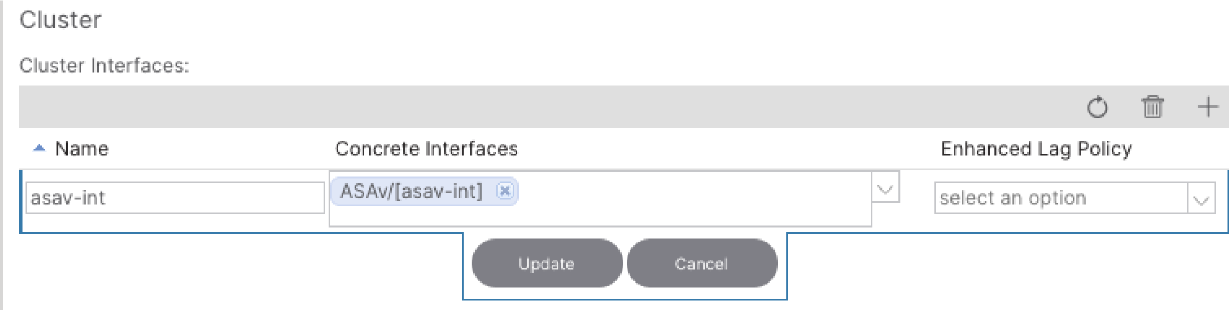
Interfaces

Name	VNIC	Path
asav-int	Network adapter 2	select a port, PC or VPC to connect to

“Better to do something imperfectly than to do nothing flawlessly.” Robert H. Schuller

Network Adapter 2 corresponds to the interface GigabitEthernet0/0 of the FW that was configured with an IP address.

Click the (+) sign under the **Cluster interfaces** to configure the logical interfaces and map them to the concrete interfaces. The interfaces of the device cluster (cluster interfaces) are the interfaces of the ASAv VM adapters. These interfaces specify how the ASAv VM connects to the ACI.

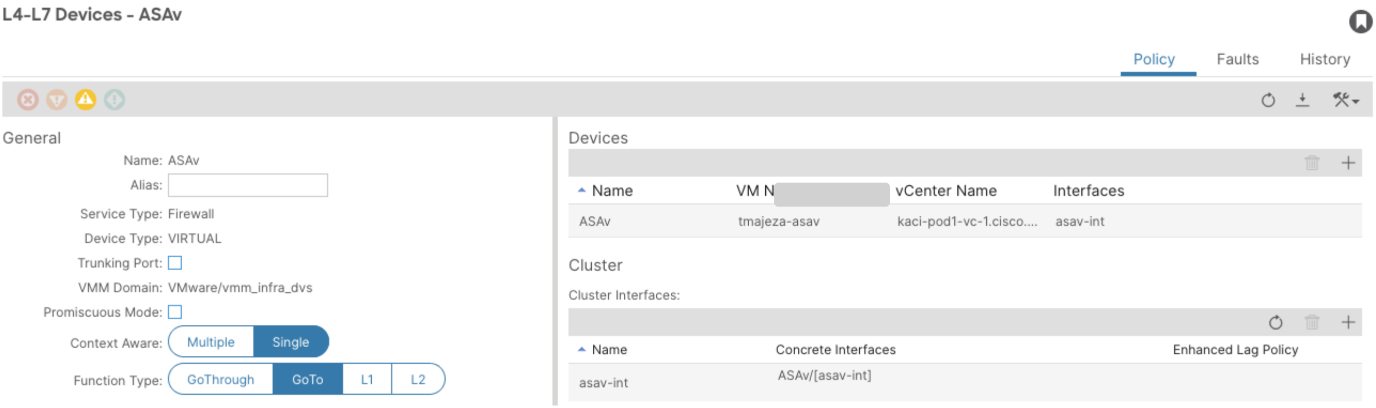


Cluster

Cluster Interfaces:

Name	Concrete Interfaces	Enhanced Lag Policy
asav-int	ASAv/[asav-int]	select an option

The resulting configuration is as follows:



L4-L7 Devices - ASAv

General

Name: ASAv
Alias:
Service Type: Firewall
Device Type: VIRTUAL
Trunking Port: □
VMM Domain: VMware/vmm_infra_dvs
Promiscuous Mode: □
Context Aware: Multiple [✓ Single]
Function Type: GoThrough [✓ GoTo] L1 L2

Devices

Name	VM N[redacted]	vCenter Name	Interfaces
ASAv	tmajeza-asav	kaci-pod1-vc-1.cisco....	asav-int

Cluster

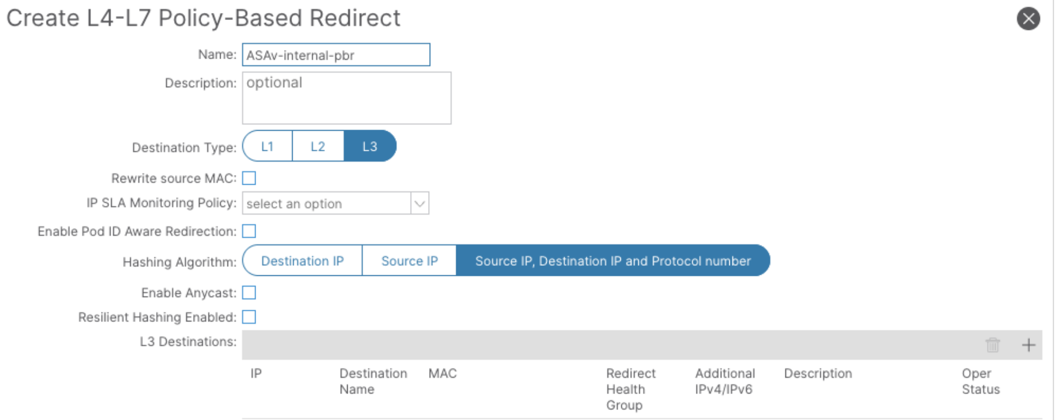
Cluster Interfaces:

Name	Concrete Interfaces	Enhanced Lag Policy
asav-int	ASAv/[asav-int]	

2. Configure the PBR Redirect Policy

The PBR policies define the next hop for the traffic that will be sent through the Layer 4 – layer 7 device.

To create the L4-L7 Policy-Based Policy navigate to the **tenant >> Policies >> L4-L4 Policy-Based Redirect >> Create L4-L7 Policy-Based Redirect**



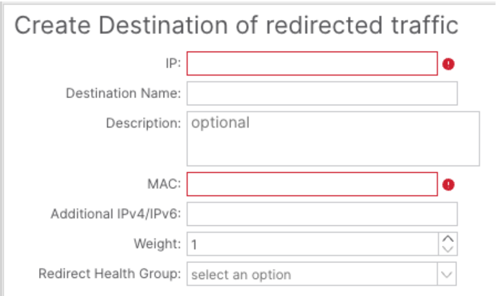
Create L4-L7 Policy-Based Redirect

Name: ASAv-internal-pbr
Description: optional
Destination Type: L1 L2 [✓ L3]
Rewrite source MAC: □
IP SLA Monitoring Policy: select an option
Enable Pod ID Aware Redirection: □
Hashing Algorithm: Destination IP Source IP [✓ Source IP, Destination IP and Protocol number]
Enable Anycast: □
Resilient Hashing Enabled: □
L3 Destinations:

IP	Destination Name	MAC	Redirect Health Group	Additional IPv4/IPv6	Description	Oper Status

Click the plus sign (**+**) in the **Layer 3 Destinations** table, enter the IP and MAC of ASAv Gi0/0. Click **OK** and **Submit**.

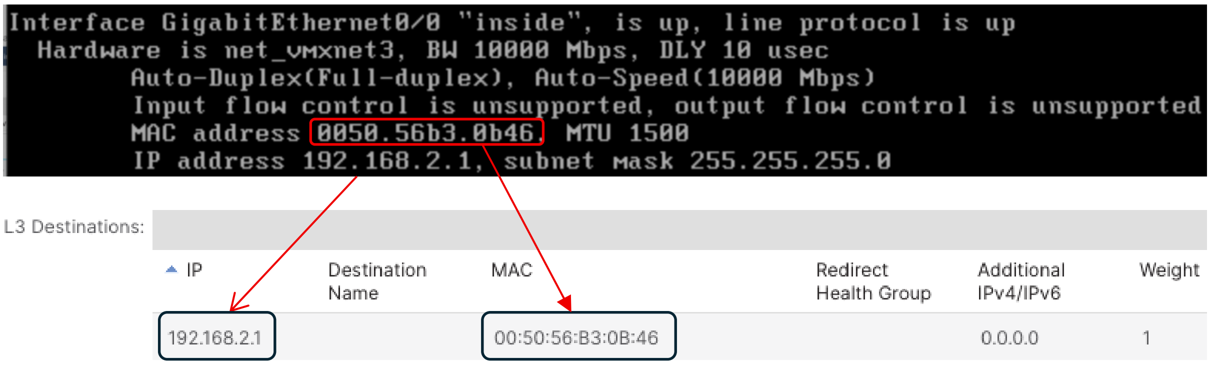
“Better to do something imperfectly than to do nothing flawlessly.” Robert H. Schuller



Create Destination of redirected traffic

IP:	
Destination Name:	
Description:	optional
MAC:	
Additional IPv4/IPv6:	
Weight:	1
Redirect Health Group:	select an option

It is important to configure the correct MAC and IP address of the firewall interface where traffic will be directed to:

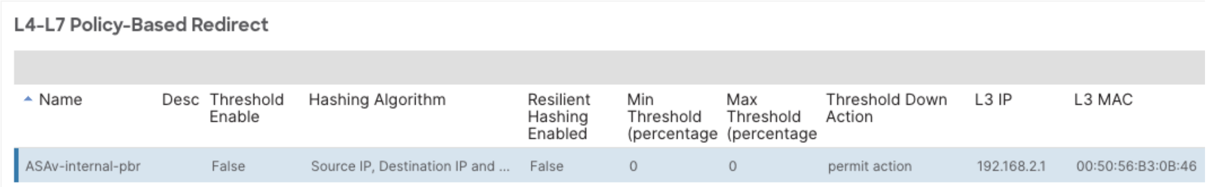


```
Interface GigabitEthernet0/0 "inside", is up, line protocol is up
  Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0050.56b3.0b46, MTU 1500
        IP address 192.168.2.1, subnet mask 255.255.255.0
```

L3 Destinations:

IP	Destination Name	MAC	Redirect Health Group	Additional IPv4/IPv6	Weight
192.168.2.1		00:50:56:B3:0B:46		0.0.0.0	1

The resulting configuration is showed below:



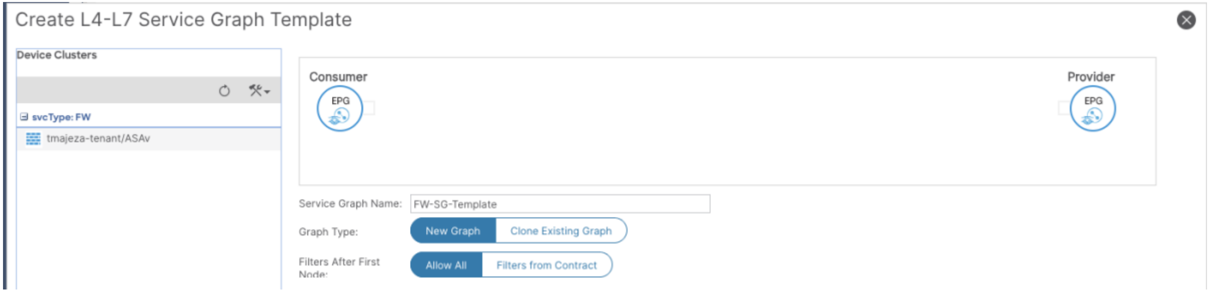
L4-L7 Policy-Based Redirect

Name	Desc	Threshold Enable	Hashing Algorithm	Resilient Hashing Enabled	Min Threshold (percentage	Max Threshold (percentage	Threshold Down Action	L3 IP	L3 MAC
ASAv-internal-pbr		False	Source IP, Destination IP and ...	False	0	0	permit action	192.168.2.1	00:50:56:B3:0B:46

3. Configure a Service Graph

A service graph allows for the insertion of a Layer 4–Layer 7 device in the traffic path between EPGs. To configure a Service Graph navigate to the **tenant >> Services >> L4-L7 >> Right Click Service Graph Templates and Create L4-L7 Service Graph Template.**

Enter the template name



Create L4-L7 Service Graph Template

Device Clusters

svcType: FW

tmajeza-tenant/ASAv

Service Graph Name: FW-SG-Template

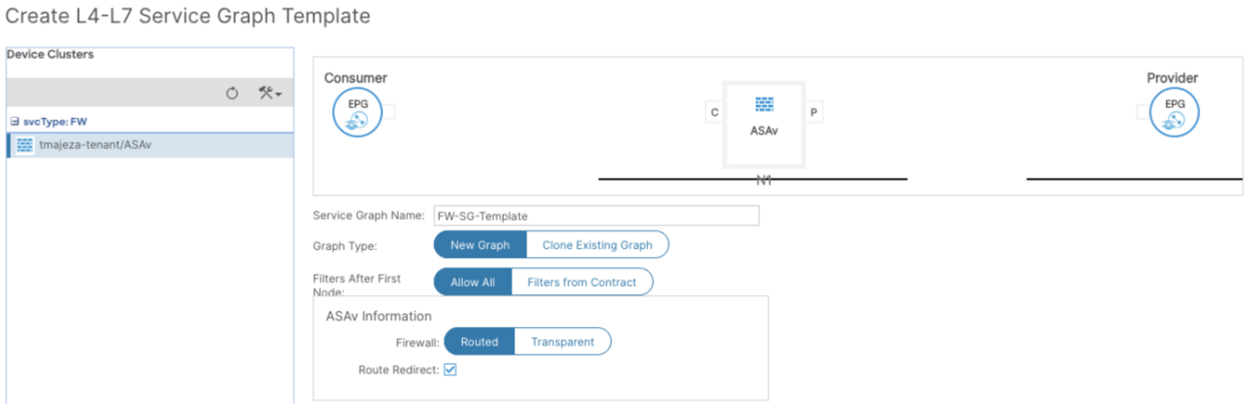
Graph Type: [✓ New Graph] Clone Existing Graph

Filters After First Node: [✓ Allow All] Filters from Contract

Drag and drop the device cluster ASAv in the work-pane (in-between the Consumer and Provider EPG).

Choose the configurations as reflected by the image below:

“Better to do something imperfectly than to do nothing flawlessly.” Robert H. Schuller



Create L4-L7 Service Graph Template

Device Clusters

⊟ svcType: FW

tmajeza-tenant/ASAv

Service Graph Name: FW-SG-Template

Graph Type: [✓ New Graph] Clone Existing Graph

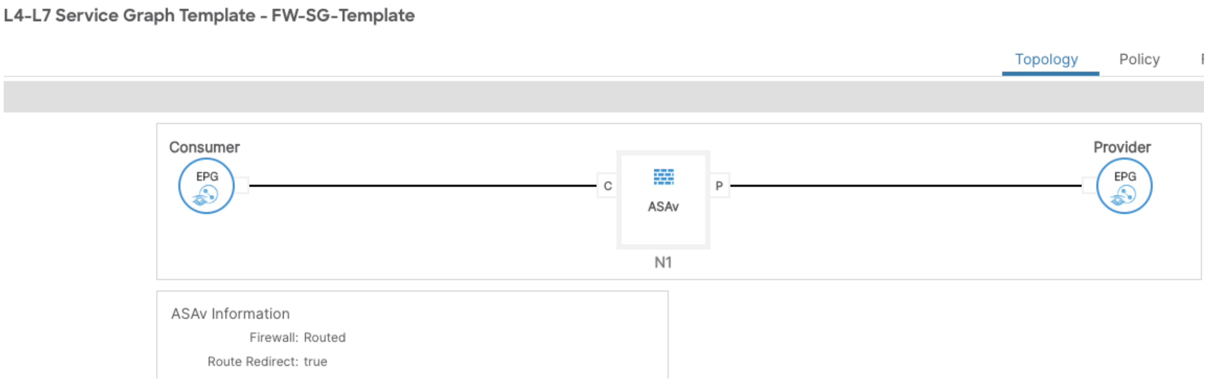
Filters After First Node: [✓ Allow All] Filters from Contract

ASAv Information

Firewall: [✓ Routed] Transparent

Route Redirect: ☑

At this point the Service Graph Template is configured successfully.



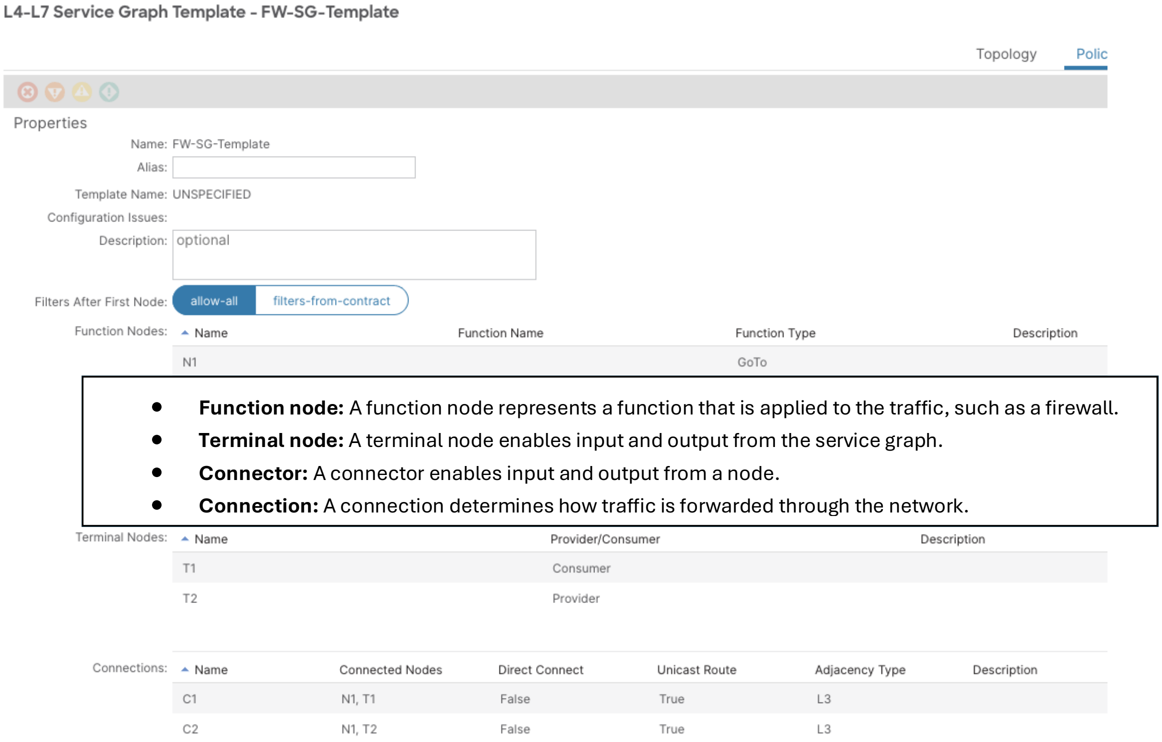
L4-L7 Service Graph Template - FW-SG-Template

ASAv Information

Firewall: Routed

Route Redirect: true

On the Service Graph Template, you can click on the Policy tab to review all the configuration associated with the Service Graph template.



L4-L7 Service Graph Template - FW-SG-Template

Properties

Name: FW-SG-Template

Alias:

Template Name: UNSPECIFIED

Configuration Issues:

Description: optional

Filters After First Node: [✓ allow-all] filters-from-contract

Function Nodes:

Name	Function Name	Function Type	Description
N1		GoTo	

- **Function node:** A function node represents a function that is applied to the traffic, such as a firewall.
- **Terminal node:** A terminal node enables input and output from the service graph.
- **Connector:** A connector enables input and output from a node.
- **Connection:** A connection determines how traffic is forwarded through the network.

Terminal Nodes:

Name	Provider/Consumer	Description
T1	Consumer	
T2	Provider	

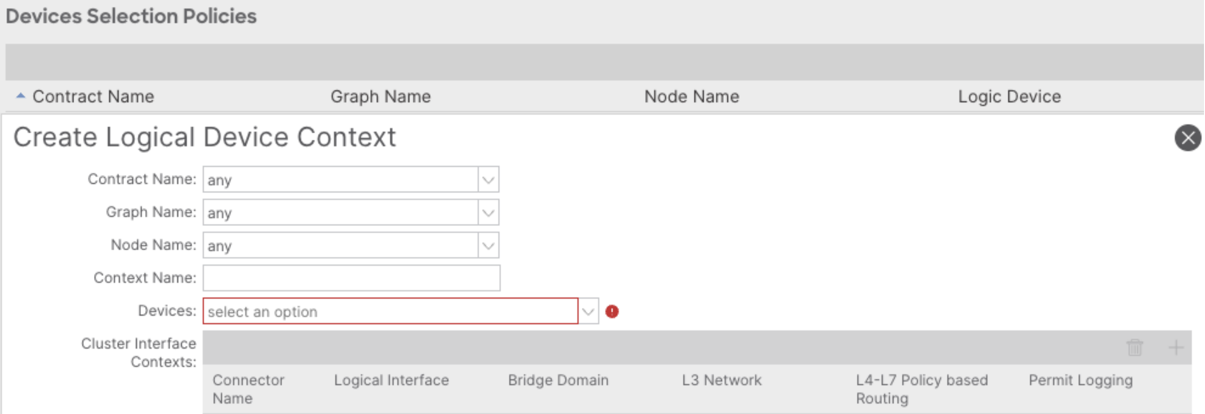
Connections:

Name	Connected Nodes	Direct Connect	Unicast Route	Adjacency Type	Description
C1	N1, T1	False	True	L3	
C2	N1, T2	False	True	L3	

“Better to do something imperfectly than to do nothing flawlessly.” Robert H. Schuller

4. **Configure Device Selection Policies:**

Navigate to **Services >> L4-L7 >> Device Selection Policies**



Devices Selection Policies

Contract Name	Graph Name	Node Name	Logic Device

Create Logical Device Context

Contract Name: any

Graph Name: any

Node Name: any

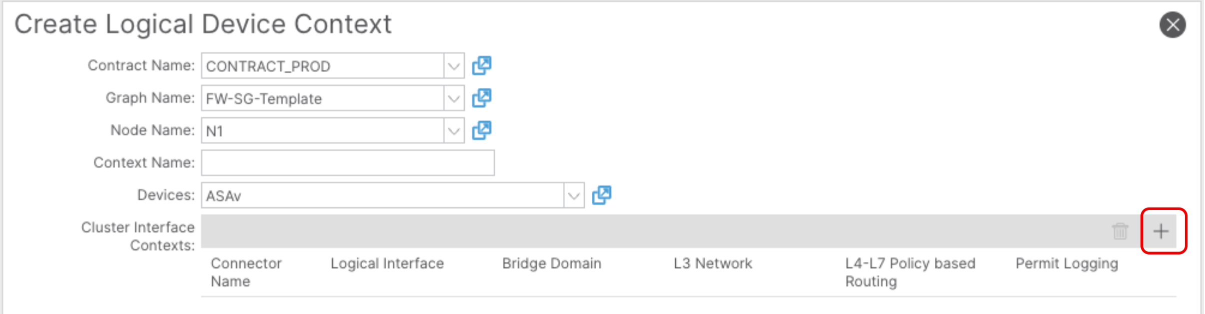
Context Name:

Devices: select an option

Cluster Interface Contexts:

Connector Name	Logical Interface	Bridge Domain	L3 Network	L4-L7 Policy based Routing	Permit Logging

- Select the Contract where the Service Graph will be applied.
- Select the configured Service Graph Template and the Function Node.
- Select the Device (ASAv) that was created earlier.



Create Logical Device Context

Contract Name: CONTRACT_PROD

Graph Name: FW-SG-Template

Node Name: N1

Context Name:

Devices: ASAv

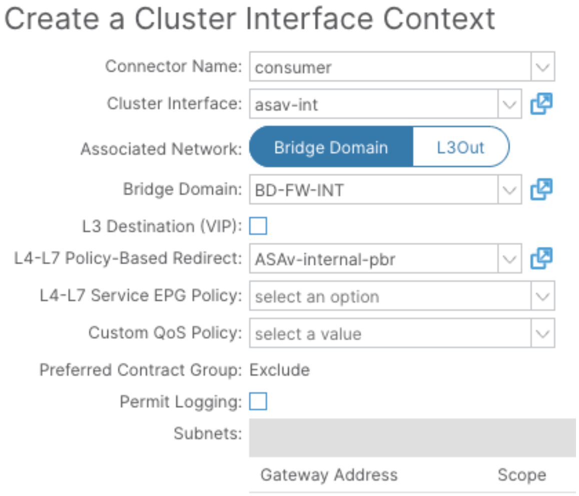
Cluster Interface Contexts:

Connector Name	Logical Interface	Bridge Domain	L3 Network	L4-L7 Policy based Routing	Permit Logging

Click on the (+) symbol to create the Cluster interface contexts:

> Although the PBR node has one interface, the device selection policy has both consumer and provider connector configuration settings. For a one-arm mode service graph, you just select the same options for both the consumer and provider connectors in the device selection policy, so that only one segment is deployed for the one interface during service graph instantiation.

Consumer connector



Create a Cluster Interface Context

Connector Name: consumer

Cluster Interface: asav-int

Associated Network: Bridge Domain | L3Out

Bridge Domain: BD-FW-INT

L3 Destination (VIP): □

L4-L7 Policy-Based Redirect: ASAv-internal-pbr

L4-L7 Service EPG Policy: select an option

Custom QoS Policy: select a value

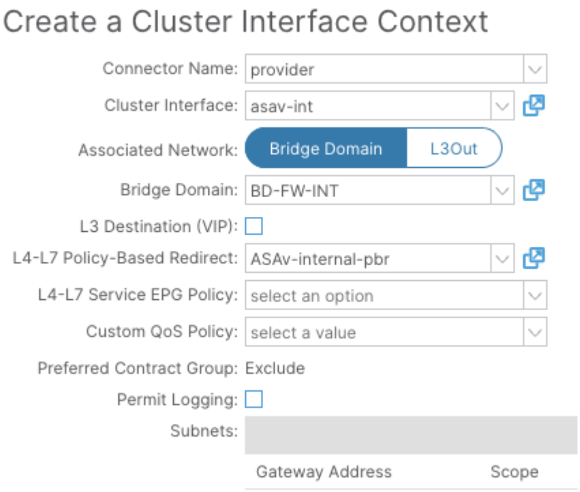
Preferred Contract Group: Exclude

Permit Logging: □

Subnets:

Gateway Address	Scope

Provider connector



Create a Cluster Interface Context

Connector Name: provider

Cluster Interface: asav-int

Associated Network: Bridge Domain | L3Out

Bridge Domain: BD-FW-INT

L3 Destination (VIP): □

L4-L7 Policy-Based Redirect: ASAv-internal-pbr

L4-L7 Service EPG Policy: select an option

Custom QoS Policy: select a value

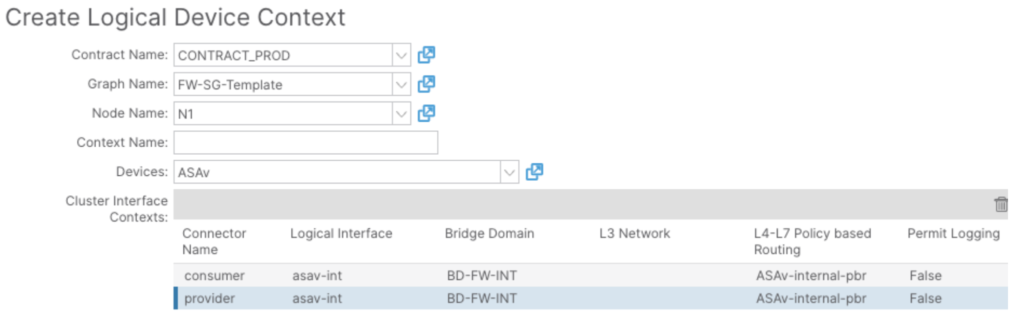
Preferred Contract Group: Exclude

Permit Logging: □

Subnets:

Gateway Address	Scope

Resulting configuration:

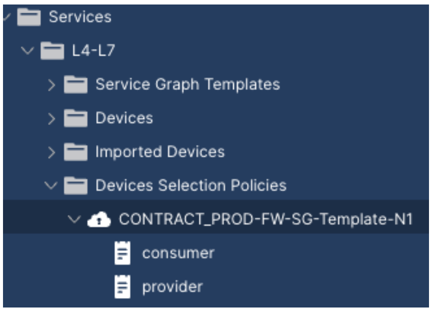


Create Logical Device Context

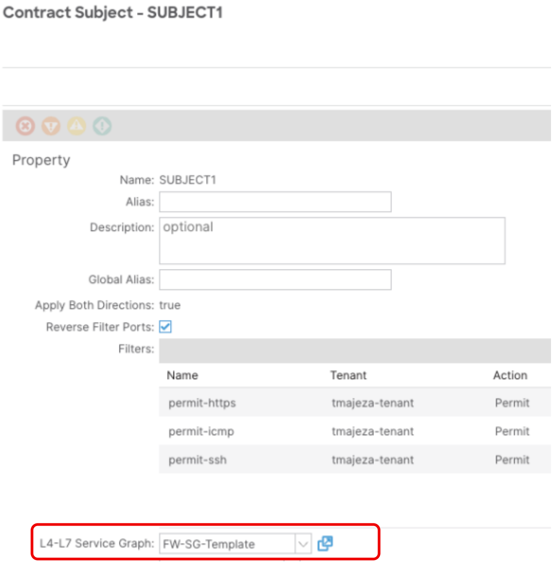
Contract Name:	CONTRACT_PROD
Graph Name:	FW-SG-Template
Node Name:	N1
Context Name:	
Devices:	ASAv

Cluster Interface Contexts:

Connector Name	Logical Interface	Bridge Domain	L3 Network	L4-L7 Policy based Routing	Permit Logging
consumer	asav-int	BD-FW-INT		ASAv-internal-pbr	False
provider	asav-int	BD-FW-INT		ASAv-internal-pbr	False



At this point all required configuration is in place however, the Graph Instance is not deployed as yet. The next step is to navigate to the **Contract's Subject >> L4-L7 Service Graph** and associate it with the Service Graph Template.



Contract Subject - SUBJECT1

Property

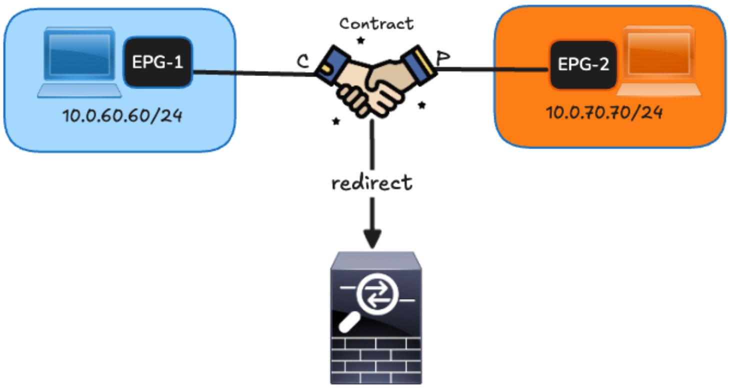
Name:	SUBJECT1
Alias:	
Description:	optional
Global Alias:	
Apply Both Directions:	true
Reverse Filter Ports:	☑

Filters:

Name	Tenant	Action
permit-https	tmajeza-tenant	Permit
permit-icmp	tmajeza-tenant	Permit
permit-ssh	tmajeza-tenant	Permit

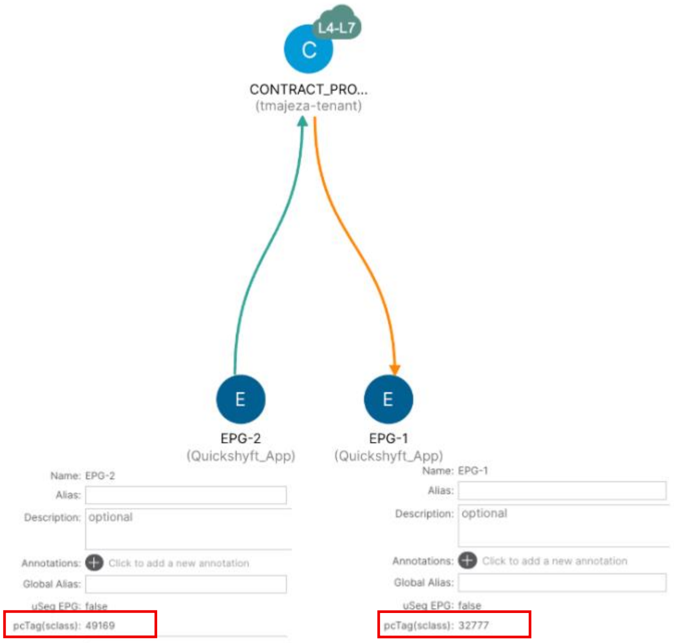
L4-L7 Service Graph: FW-SG-Template

Apply the contract between the two EPGs.



"Better to do something imperfectly than to do nothing flawlessly." Robert H. Schuller

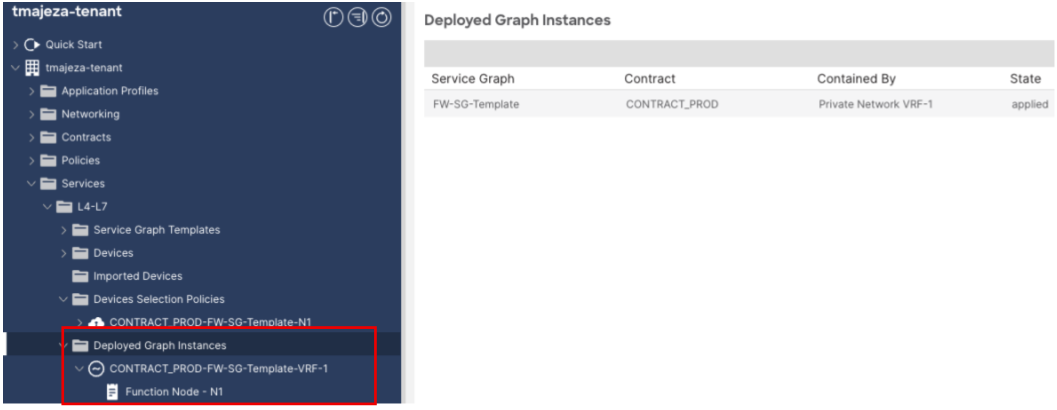
The image below (contract topology) shows that the contract with an L4-L7 Service Graph association is applied between the two EPGs.



Name: EPG-2
Alias:
Description: optional
Annotations: Click to add a new annotation
Global Alias:
uSeg EPG: false
pcTag(sclass): 49169

Name: EPG-1
Alias:
Description: optional
Annotations: Click to add a new annotation
Global Alias:
uSeg EPG: false
pcTag(sclass): 32777

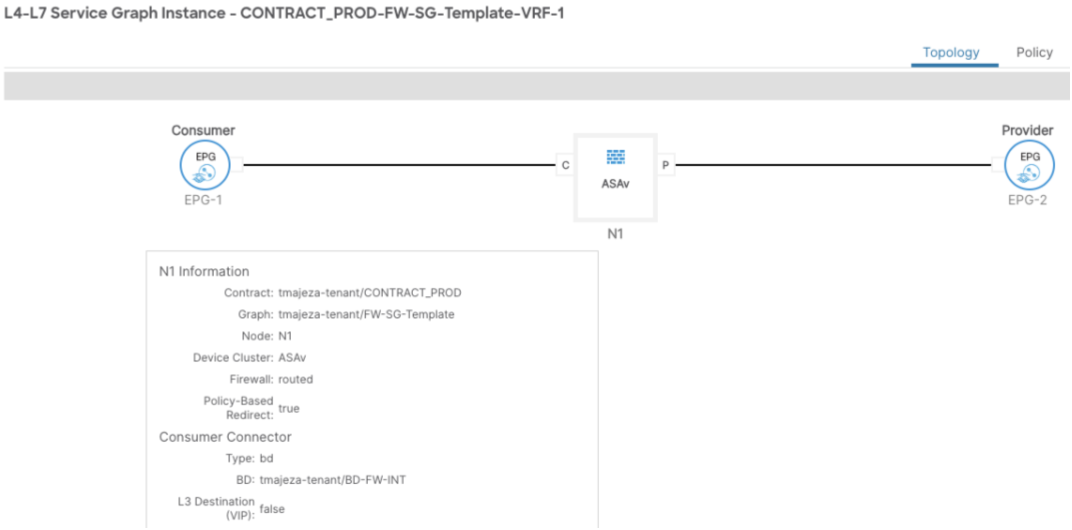
The moment the contract is successfully deployed between the two EPGs, a Graph instance is automatically deployed.



Deployed Graph Instances

Service Graph	Contract	Contained By	State
FW-SG-Template	CONTRACT_PROD	Private Network VRF-1	applied

Click on the Deployed Graph Instance to see the deployed configuration.


L4-L7 Service Graph Instance - CONTRACT_PROD-FW-SG-Template-VRF-1

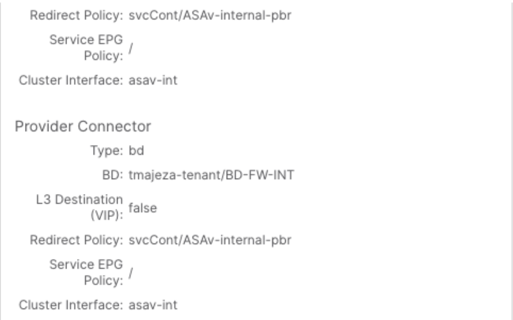
N1 Information

Contract: tmajeza-tenant/CONTRACT_PROD
Graph: tmajeza-tenant/FW-SG-Template
Node: N1
Device Cluster: ASAv
Firewall: routed
Policy-Based Redirect: true

Consumer Connector

Type: bd
BD: tmajeza-tenant/BD-FW-INT
L3 Destination (VIP): false

“Better to do something imperfectly than to do nothing flawlessly.” Robert H. Schuller



Redirect Policy: svcCont/ASAv-internal-pbr

Service EPG Policy: /

Cluster Interface: asav-int

Provider Connector

Type: bd

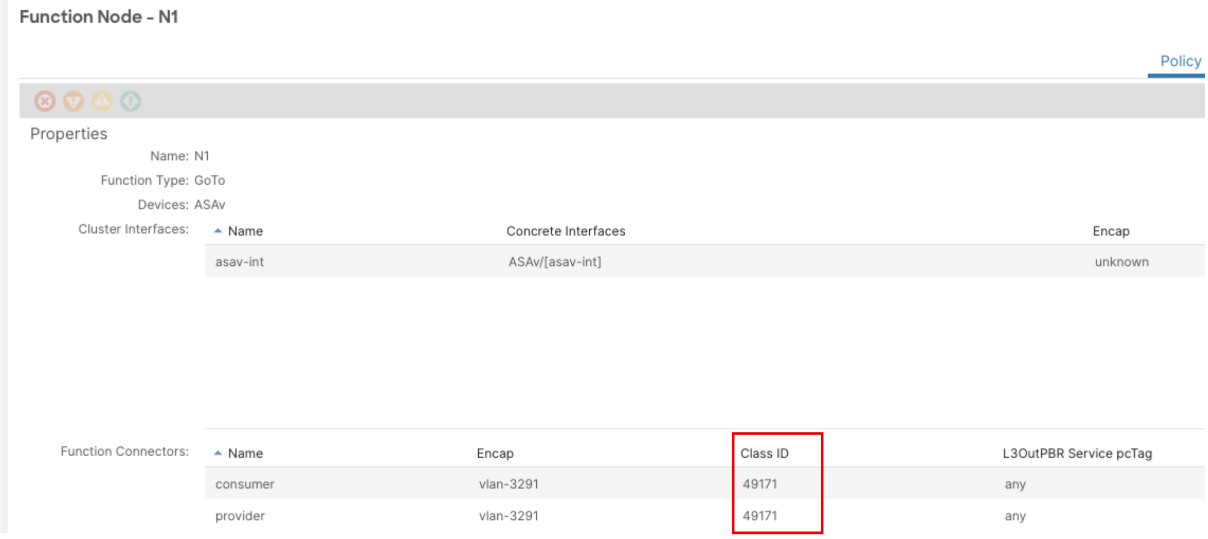
BD: tmajeza-tenant/BD-FW-INT

L3 Destination (VIP): false

Redirect Policy: svcCont/ASAv-internal-pbr

Service EPG Policy: /

Cluster Interface: asav-int



Function Node - N1

Properties

Name: N1

Function Type: GoTo

Devices: ASAv

Cluster Interfaces:

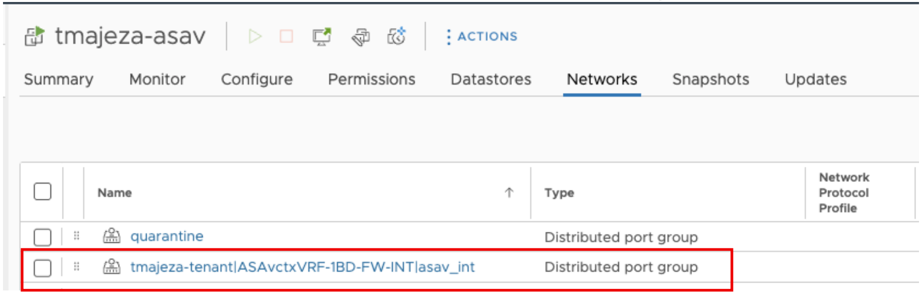
Name	Concrete Interfaces	Encap
asav-int	ASAv/[asav-int]	unknown

Function Connectors:

Name	Encap	Class ID	L3OutPBR Service pcTag
consumer	vlan-3291	49171	any
provider	vlan-3291	49171	any

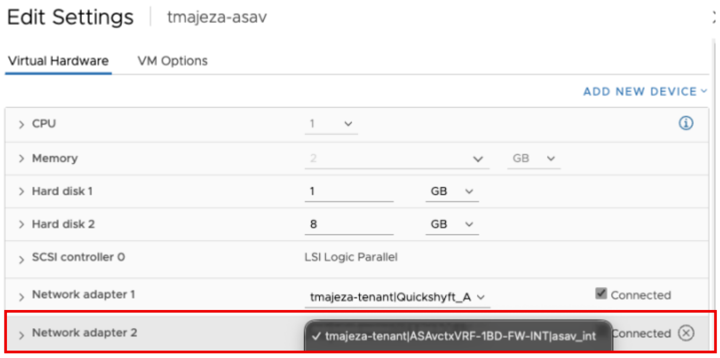
Note: The Class ID highlighted above is programmed by ACI for the provider and consumer connectors. This Class ID is the pcTag of the shadow EPG of the firewall. This Class ID will be observed in the zoning-rule table.

On the ASAv that is deployed on vCenter, a port group is dynamically created and the Network adapter for the relevant firewall interface is associated with the port-group.



tmajeza-asav

□	Name ↑	Type	Network Protocol Profile
□	quarantine	Distributed port group	
□	tmajeza-tenant|ASAvctxVRF-1BD-FW-INT|asav_int	Distributed port group	

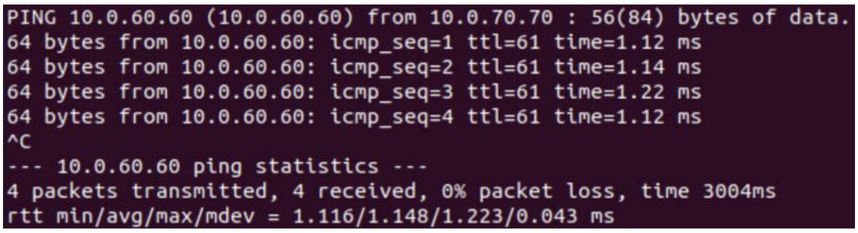


Edit Settings | tmajeza-asav

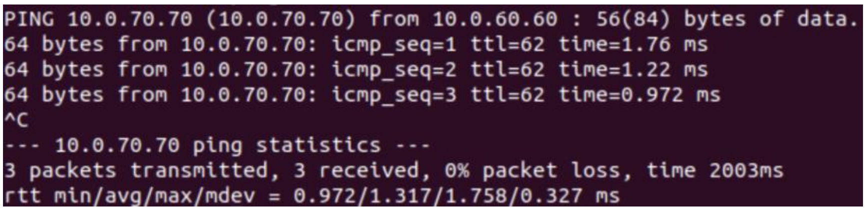
CPU	1	
Memory	2	GB
Hard disk 1	1	GB
Hard disk 2	8	GB
SCSI controller 0	LSI Logic Parallel	
Network adapter 1	tmajeza-tenant|Quickshyft_A	☑ Connected
Network adapter 2	✓ tmajeza-tenant|ASAvctxVRF-1BD-FW-INT|asav_int	Connected

Verifications

After the successful deployment of Service Graph instance, we can observe that host-1 and host-2 can communicate.

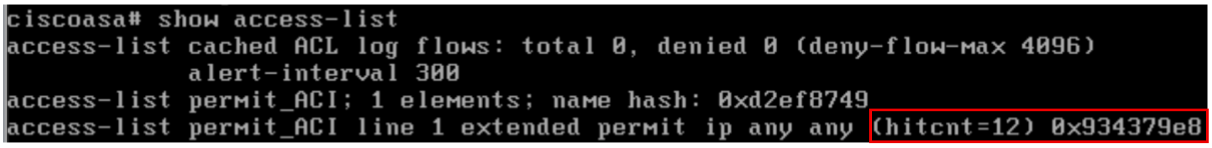


```
PING 10.0.60.60 (10.0.60.60) from 10.0.70.70 : 56(84) bytes of data.
64 bytes from 10.0.60.60: icmp_seq=1 ttl=61 time=1.12 ms
64 bytes from 10.0.60.60: icmp_seq=2 ttl=61 time=1.14 ms
64 bytes from 10.0.60.60: icmp_seq=3 ttl=61 time=1.22 ms
64 bytes from 10.0.60.60: icmp_seq=4 ttl=61 time=1.12 ms
^C
--- 10.0.60.60 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.116/1.148/1.223/0.043 ms
```



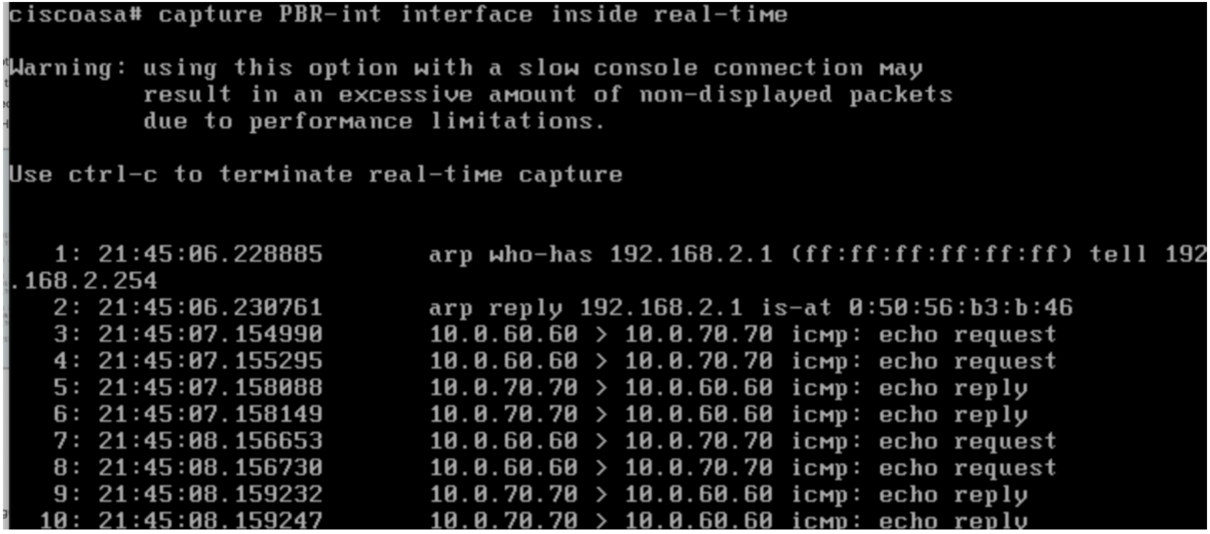
```
PING 10.0.70.70 (10.0.70.70) from 10.0.60.60 : 56(84) bytes of data.
64 bytes from 10.0.70.70: icmp_seq=1 ttl=62 time=1.76 ms
64 bytes from 10.0.70.70: icmp_seq=2 ttl=62 time=1.22 ms
64 bytes from 10.0.70.70: icmp_seq=3 ttl=62 time=0.972 ms
^C
--- 10.0.70.70 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.972/1.317/1.758/0.327 ms
```

To verify that the access-list configured on the firewall is indeed taking effect, we can check if the hit count is incrementing as traffic flows. The output below shows that the access-list has a non-zero hit count verifying that the access-list is indeed in full effect.



```
ciscoasa# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list permit_ACI; 1 elements; name hash: 0xd2ef8749
access-list permit_ACI line 1 extended permit ip any any (hitcnt=12) 0x934379e8
```

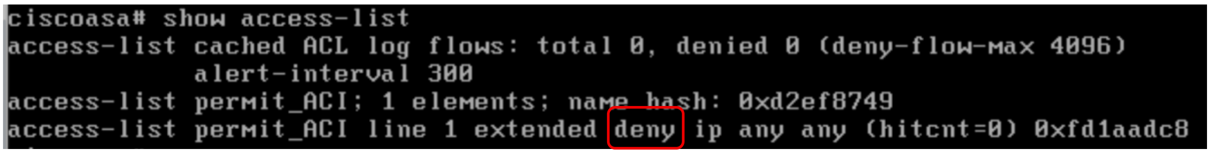
An additional check on the firewall is to capture real-time traffic on the firewall terminal. The output below reflects that ICMP traffic between host-1 (10.0.60.60) and host-2 (10.0.70.70) is being redirected to the firewall.



```
ciscoasa# capture PBR-int interface inside real-time

Warning: using this option with a slow console connection may
         result in an excessive amount of non-displayed packets
         due to performance limitations.

Use ctrl-c to terminate real-time capture


   1: 21:45:06.228885       arp who-has 192.168.2.1 (ff:ff:ff:ff:ff:ff) tell 192
.168.2.254
   2: 21:45:06.230761       arp reply 192.168.2.1 is-at 0:50:56:b3:b:46
   3: 21:45:07.154990       10.0.60.60 > 10.0.70.70 icmp: echo request
   4: 21:45:07.155295       10.0.60.60 > 10.0.70.70 icmp: echo request
   5: 21:45:07.158088       10.0.70.70 > 10.0.60.60 icmp: echo reply
   6: 21:45:07.158149       10.0.70.70 > 10.0.60.60 icmp: echo reply
   7: 21:45:08.156653       10.0.60.60 > 10.0.70.70 icmp: echo request
   8: 21:45:08.156730       10.0.60.60 > 10.0.70.70 icmp: echo request
   9: 21:45:08.159232       10.0.70.70 > 10.0.60.60 icmp: echo reply
  10: 21:45:08.159247       10.0.70.70 > 10.0.60.60 icmp: echo reply
```

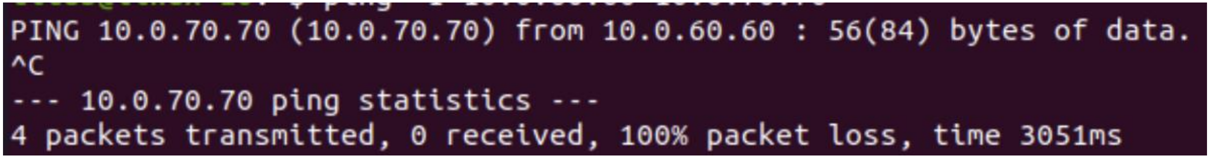
If the requirement was to block the traffic between these hosts, the access-list "permit" action can be changed to "deny".

"Better to do something imperfectly than to do nothing flawlessly." Robert H. Schuller

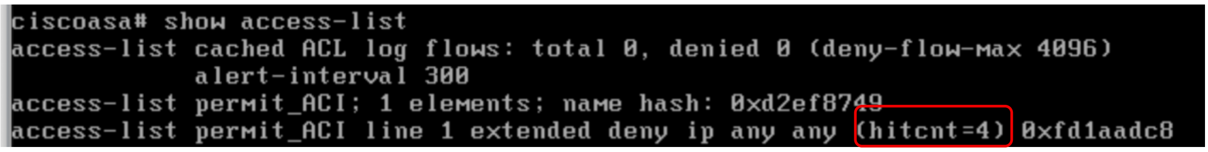


```
ciscoasa# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list permit_ACI; 1 elements; name hash: 0xd2ef8749
access-list permit_ACI line 1 extended deny ip any any (hitcnt=0) 0xfd1aadc8
```

Communication between the 2 hosts is now being denied.



```
PING 10.0.70.70 (10.0.70.70) from 10.0.60.60 : 56(84) bytes of data.
^C
--- 10.0.70.70 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3051ms
```



```
ciscoasa# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list permit_ACI; 1 elements; name hash: 0xd2ef8749
access-list permit_ACI line 1 extended deny ip any any (hitcnt=4) 0xfd1aadc8
```

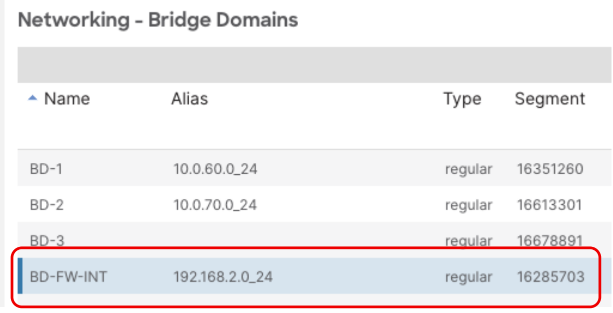
DEEP DIVE VERIFICATIONS

Now let’s perform some in-depth verifications on the command-line interface.

Verify the service redirect information. This output reflects the MAC and IP address of the firewall that was configured in the redirect policy.

```
L102# show service redir info
List of Dest Groups
GrpID Name          destination                             operSt
===== ====          ===========                             ==============
destgrp-5           dest-[192.168.2.1]-[vxlan-2129937]      enabled

List of destinations
Name                                                     bdVnid          vMac                vrf                      operSt
====                                                     ======          ====                ====                     =====
dest-[192.168.2.1]-[vxlan-2129937]                       vxlan-16285703  00:50:56:B3:0B:46   tmajeza-tenant:VRF-1     enabled
```

The bdVnid is the ID of the Bridge Domain that was configured for the firewall.



Networking - Bridge Domains

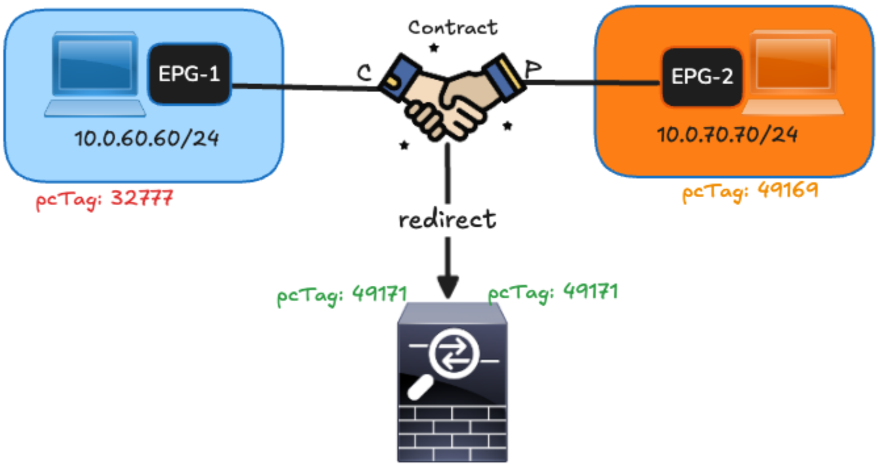
Name	Alias	Type	Segment
BD-1	10.0.60.0_24	regular	16351260
BD-2	10.0.70.0_24	regular	16613301
BD-3		regular	16678891
BD-FW-INT	192.168.2.0_24	regular	16285703

“Better to do something imperfectly than to do nothing flawlessly.” Robert H. Schuller

From a contract enforcement perspective, the zoning rule table highlights the rules that are applied between the hosts' EPGs and the shadow EPG of the firewall.

```
L102# show zoning-rule scope 2129937
+---------+--------+--------+----------+----------------+---------+---------+------+--------------------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action       |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+--------------------+----------------------+
|  15305  | 49169  | 32777  |    5     | uni-dir-ignore | enabled | 2129937 |      | redir(destgrp-5)   |    fully_qual(7)     |
|   4127  | 32777  | 49169  |    5     |     bi-dir     | enabled | 2129937 |      | redir(destgrp-5)   |    fully_qual(7)     |
|   4128  | 49171  | 32777  |    5     |    uni-dir     | enabled | 2129937 |      |       permit       |    fully_qual(7)     |
|  10582  | 49171  | 49169  | default  |    uni-dir     | enabled | 2129937 |      |       permit       |    src_dst_any(9)    |
+---------+--------+--------+----------+----------------+---------+---------+------+--------------------+----------------------+
```

Rule 15



Rule 4127: IP (ICMP) traffic from EPG-1 (32777) to EPG-2 (49169) is redirected to the firewall.
Rule 10582: any traffic from the firewall shadow EPG (49171) to EPG-2 (49169) is permitted.

Rule 15305: IP (ICMP) traffic from EPG-2 (49169) to EPG-1 (32777) is redirected to the firewall.
Rule 4128: Rule 10582: IP (ICMP) from the firewall shadow EPG (49171) to EPG-1 (32777) is permitted.

The ***contract_parser.py*** script is also used to get more details regarding each rule, what action is involved (redirect or permit), the redirect information (MAC and IP address of the firewall) and the hit count of each rule. This is important to verify that the contract is taking effect.

```
KACI-MS-S1-93180EX-L102# contract_parser.py --vrf tmajeza-tenant:VRF-1
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4] [flags][contract:{str}] [hit=count]
[7:4127] [vrf:tmajeza-tenant:VRF-1] redir ip icmp tn-tmajeza-tenant/ap-Quickshyft_App/epg-EPG-1(32777) tn-tmajeza-tenant/ap-Quickshyft_App/epg-EPG-2(49169)
[contract:uni/tn-tmajeza-tenant/brc-CONTRACT_PROD] [hit=96]
                                        destgrp-5 vrf:tmajeza-tenant:VRF-1 ip:192.168.2.1 mac:00:50:56:B3:0B:46 bd:uni/tn-tmajeza-tenant/BD-BD-FW-INT
[7:15305] [vrf:tmajeza-tenant:VRF-1] redir ip icmp tn-tmajeza-tenant/ap-Quickshyft_App/epg-EPG-2(49169) tn-tmajeza-tenant/ap-Quickshyft_App/epg-EPG-1(32777)
[contract:uni/tn-tmajeza-tenant/brc-CONTRACT_PROD] [hit=56453599]
                                         destgrp-5 vrf:tmajeza-tenant:VRF-1 ip:192.168.2.1 mac:00:50:56:B3:0B:46 bd:uni/tn-tmajeza-tenant/BD-BD-FW-INT
[7:4128] [vrf:tmajeza-tenant:VRF-1] permit ip icmp tn-tmajeza-tenant/G-ASAvctxVRF-1/C-asav-int(49171) tn-tmajeza-tenant/ap-Quickshyft_App/epg-EPG-1(32777)
[contract:uni/tn-tmajeza-tenant/brc-CONTRACT_PROD] [hit=49390149]
[9:10582] [vrf:tmajeza-tenant:VRF-1] permit any tn-tmajeza-tenant/G-ASAvctxVRF-1/C-asav-int(49171) tn-tmajeza-tenant/ap-Quickshyft_App/epg-EPG-2(49169)
[contract:uni/tn-tmajeza-tenant/brc-CONTRACT_PROD] [hit=256]
```

The policy manager can be used to verify the rules within the VRF and the "Pkts" count show whether the contract rule is being hit or not.

```
KACI-MS-S1-93180EX-L102# show system internal policy-mgr stats | grep 2129937
Rule (4127) DN (sys/actrl/scope-2129937/rule-2129937-s-32777-d-49169-f-5) Ingress: 0, Egress: 0, Pkts: 84  RevPkts: 0
Rule (4128) DN (sys/actrl/scope-2129937/rule-2129937-s-49171-d-32777-f-5) Ingress: 0, Egress: 0, Pkts: 24695111  RevPkts: 0
Rule (10582) DN (sys/actrl/scope-2129937/rule-2129937-s-49171-d-49169-f-default) Ingress: 0, Egress: 0, Pkts: 162  RevPkts: 0
Rule (15305) DN (sys/actrl/scope-2129937/rule-2129937-s-49169-d-32777-f-5) Ingress: 0, Egress: 0, Pkts: 24695038  RevPkts: 0
```

"Better to do something imperfectly than to do nothing flawlessly." Robert H. Schuller

The section below uses the Embedded Logic Analyzer Module (ELAM) to showcase the PBR packet walk from the source to the destination.

What is ELAM ?

ELAM is an engineering tool that gives you the ability to look inside Cisco ASICs and understand how a packet is forwarded. It is embedded within the forwarding pipeline. ELAM can capture a packet in real time without disruptions to performance or control-plane resources. It helps to answer questions such as: Did the packet reach the forwarding engine? How does the packet appear (Layer 2-Layer 4 data)? How is the packet altered and where is it sent?

To run the ELAM on the nodes in this lab, I used ELAM CLI Tool for Cisco ACI obtained from (https://developer.cisco.com/codeexchange/github/repo/tskanai1/elam-tool2/ or https://github.com/tskanai1/elam-tool2)

The first ELAM capture is performed on the LEAF102 access port where the source endpoint is sending traffic from.

Let’s look into the generated report (only important output is shown)

```
==========================================================================================
Captured Packet
==========================================================================================
------------------------------------------------------------------------------------------
Outer Packet Attributes
------------------------------------------------------------------------------------------
Outer Packet Attributes        : l2uc ipv4 ip ipuc ipv4uc
Opcode                         : OPCODE_UC
--------------------------------------------------------------------------------------------------------
---------------------------------------------
Outer L2 Header
--------------------------------------------------------------------------------------------------------
---------------------------------------------
Destination MAC                : 0022.BDF8.19FF    MAC address of the destination host (10.0.70.70)
Source MAC                     : 0050.56B3.1AB7    MAC address of the source host (10.0.60.60)
802.1Q tag is valid            : yes( 0x1 )
CoS                            : 0( 0x0 )
Access Encap VLAN              : 3461( 0xD85 )
--------------------------------------------------------------------------------------------------------
Outer L3 Header
--------------------------------------------------------------------------------------------------------
L3 Type                        : IPv4
IP Version                     : 4
DSCP                           : 0
IP Packet Length               : 84 ( = IP header(28 bytes) + IP payload )
Don't Fragment Bit             : set
TTL                            : 64
IP Protocol Number             : ICMP
IP CheckSum                    : 5849( 0x16D9 )
Destination IP                 : 10.0.70.70
Source IP                      : 10.0.60.60
========================================================================================================
Contract Lookup ( FPC )
========================================================================================================
--------------------------------------------------------------------------------------------------------
Contract Lookup Key
--------------------------------------------------------------------------------------------------------
IP Protocol                              : ICMP( 0x1 )
L4 Src Port                              : 2048( 0x800 )
L4 Dst Port                              : 6668( 0x1A0C )
sclass (src pcTag)                       : 32777( 0x8009 )
dclass (dst pcTag)                       : 49169( 0xC011 )
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               : 81658
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81658" )
```

The output reflects that policy enforcement (contract rule) was applied on the leaf where the source host is connected.

Check which zoning-rule is being enforced when the packet hits the leaf from the source.

```
module-1(DBG-elam-insel6)# show sys int aclqos zoning-rules | grep -B 9 "Idx: 81658"
Rule ID: 4127 Scope 23 Src EPG: 32777 Dst EPG: 49169 Filter 5
  Redir group: 5
```

Sclass for source endpoint

Sclass for destination endpoint

LEAF-102

```
show system internal epm endpoint ip 10.0.60.60 |
egrep "VRF vnid|sclass"
BD vnid : 16351260 ::: VRF vnid : 2129937
Flags : 0x80004c04 ::: sclass : 32777 ::: Ref
count : 5
EP Flags : local|IP|MAC|sclass|timer|
```

LEAF-102

```
show system internal epm endpoint ip 10.0.70.70 |
egrep "VRF vnid|sclass"
BD vnid : 16613301 ::: VRF vnid : 2129937
Flags : 0x80000c80 ::: sclass : 49169 ::: Ref
count : 5
EP Flags : on-peer|IP|MAC|sclass|
```

On Leaf 102, it is evident that Rule ID:4127 is enforced. This rule's action is a "redirect" to the firewall.

```
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |      Action       |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
|   4127  | 32777  | 49169  |    5     |     bi-dir     | enabled | 2129937 |      | redir(destgrp-5)  |    fully_qual(7)     |
```

The ELAM report furthermore verifies that indeed the packet has been redirected.

```
cat elam_report_ L102_LC1_ASIC0.txt | grep service_redir
  sug_luc_latch_results_vec.luc3_0.service_redir: 0x1 (0x1 means that the packet is being redirected)
```

The next capture is on the fabric port of the of the spine connected to the leaf where the packet is coming from.

The packet on this port will now be encapsulated with a VXLAN header as it will be traversing in the ACI fabric.

```
------------------------------------------------------------------------------------------------------------------
Inner L2 Header
------------------------------------------------------------------------------------------------------------------
----------------------
Inner Destination MAC         : 0050.56B3.0B46    The inner destination MAC was changed by the leaf to the FW vMAC address
Source MAC                    : 0050.56B3.1AB7    Source MAC of host-1 remains unchanged.
802.1Q tag is valid           : no
CoS                           : 0
Access Encap VLAN             : 0
------------------------------------------------------------------------------------------------------------------
Outer L3 Header
------------------------------------------------------------------------------------------------------------------
L3 Type                       : IPv4
DSCP                          : 0
Don't Fragment Bit            : 0x0
TTL                           : 32
```

"Better to do something imperfectly than to do nothing flawlessly." Robert H. Schuller

```
IP Protocol Number              : UDP
Destination IP                  : 10.0.80.65       This is the PHYSICAL,PROXY-ACAST-MAC IP address on the spine.
Source IP                       : 10.0.152.66      This is the TEP IP of LEAF102 where the packet is coming from.
------------------------------------------------------------------------------------------------------------------------------
Inner L3 Header
------------------------------------------------------------------------------------------------------------------------------
L3 Type                         : IPv4
DSCP                            : 0
Don't Fragment Bit              : 0x1
TTL                             : 63
IP Protocol Number              : ICMP
Destination IP                  : 10.0.70.70
Source IP                       : 10.0.60.60
Outer L4 Header
------------------------------------------------------------------------------------------------------------------------------
L4 Type                         : iVxLAN
Don't Learn Bit                 : 1
Src Policy Applied Bit          : 1
Dst Policy Applied Bit          : 1
sclass (src pcTag)              : 0x8009
VRF or BD VNID                  : 16285703( 0xF88007 )    Outer L4 header contains the BD_VNID of the firewall
```

The next capture is performed on the fabric port of LEAF102. The packet comes from the spine towards LEAF102 where the service device (firewall) is connected. The packet is destined to the Firewall (seen from the Inner destination MAC address).

```
---------------------------------------------------------------------------------------------------
Inner L2 Header
---------------------------------------------------------------------------------------------------
Inner Destination MAC           : 0050.56B3.0B46
Source MAC                      : 0050.56B3.1AB7
802.1Q tag is valid             : no
CoS                             : 0
Access Encap VLAN               : 0
---------------------------------------------------------------------------------------------------
Outer L3 Header
---------------------------------------------------------------------------------------------------
L3 Type                         : IPv4
DSCP                            : 0
Don't Fragment Bit              : 0x0
TTL                             : 32
IP Protocol Number              : UDP
Destination IP                  : 10.0.152.66
Source IP                       : 10.0.152.66
---------------------------------------------------------------------------------------------------
Inner L3 Header
---------------------------------------------------------------------------------------------------
L3 Type                         : IPv4
DSCP                            : 0
Don't Fragment Bit              : 0x1
TTL                             : 63
IP Protocol Number              : ICMP
Destination IP                  : 10.0.70.70
Source IP                       : 10.0.60.60
---------------------------------------------------------------------------------------------------
Outer L4 Header
---------------------------------------------------------------------------------------------------
L4 Type                         : iVxLAN
Don't Learn Bit                 : 1
Src Policy Applied Bit          : 1
Dst Policy Applied Bit          : 1
sclass (src pcTag)              : 0x8009
VRF or BD VNID                  : 16285703( 0xF88007 )
```

The output below captures the packet on Leaf 102 as it comes back from the firewall and is destined for the destination endpoint.

```
------------------------------------------------------------------------------------------------
Outer L2 Header
------------------------------------------------------------------------------------------------
Destination MAC                : 0022.BDF8.19FF
Source MAC                     : 0050.56B3.0B46           MAC address of the firewall
802.1Q tag is valid            : yes( 0x1 )
CoS                            : 0( 0x0 )
Access Encap VLAN              : 3291( )
------------------------------------------------------------------------------------------------
Outer L3 Header
------------------------------------------------------------------------------------------------
L3 Type                        : IPv4
IP Version                     : 4
DSCP                           : 0
IP Packet Length               : 84 ( = IP header(28 bytes) + IP payload )
Don't Fragment Bit             : set
TTL                            : 63
IP Protocol Number             : ICMP
IP CheckSum                    : 36245( 0x8D95 )
Destination IP                 : 10.0.70.70
Source IP                      : 10.0.60.60
```

```
Contract Lookup ( FPC )
------------------------------------------------------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
IP Protocol                              : ICMP( 0x1 )
L4 Src Port                              : 2048( 0x800 )
L4 Dst Port                              : 23362( 0x5B42 )
sclass (src pcTag)                       : 49171( 0xC013 )
dclass (dst pcTag)                       : 49169( 0xC011 )
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              : 71256
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 71256" )
================================================================================================
```

```
module-1(DBG-elam-insel6)# show sys int aclqos zoning-rules | grep -B 9 "Idx: 71256"
===========================================
Rule ID: 10582 Scope 23 Src EPG: 49171 Dst EPG: 49169 Filter 65535
    unit_id: 0
    === Region priority: 2462 (rule prio: 9 entry: 158)===
```

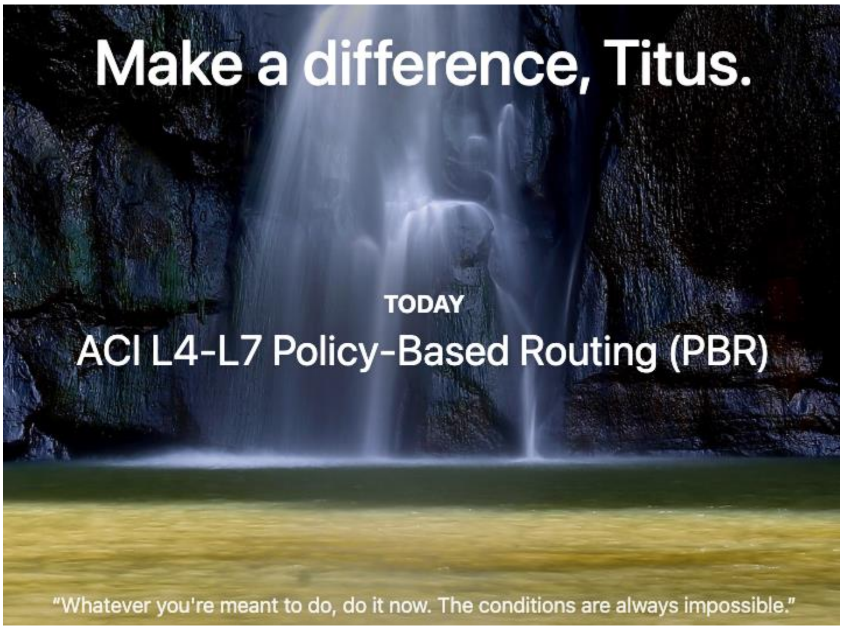
On Leaf 102, it is evident that Rule ID:10582 is enforced. This rule's action is a "permit any".

```
L102# show zoning-rule scope 2129937
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action      |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
|  10582  | 49171  | 49169  | default  |    uni-dir     | enabled | 2129937 |      |       permit      |   src_dst_any(9)     |
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
```

```
L102# show zoning-filter filter default
+----------+------+-------------+-------------+-------------+-------------+----------+-------------+-------------+-------------+-------------+------+-------------+-------------+----------+
| FilterId | Name |    EtherT   |    ArpOpc   |     Prot    | ApplyToFrag | Stateful |  SFromPort  |   SToPort   |  DFromPort  |   DToPort   | Prio |   Icmpv4T   |   Icmpv6T   | TcpRules |
+----------+------+-------------+-------------+-------------+-------------+----------+-------------+-------------+-------------+-------------+------+-------------+-------------+----------+
| default  | any  | unspecified | unspecified | unspecified |      no     |    no    | unspecified | unspecified | unspecified | unspecified | def  | unspecified | unspecified |          |
+----------+------+-------------+-------------+-------------+-------------+----------+-------------+-------------+-------------+-------------+------+-------------+-------------+----------+
```

"Better to do something imperfectly than to do nothing flawlessly." Robert H. Schuller

From this point the packet will be sent to the destination leaf where the destination host resides. The reverse traffic from 10.0.70.70 to 10.0.60.60 will follow a similar pattern as shown above.


Make a difference, Titus.
TODAY
ACI L4-L7 Policy-Based Routing (PBR)
"Whatever you're meant to do, do it now. The conditions are always impossible."

For more labs visit my GitHub repo: https://github.com/TitusM/Cisco-Data-Center

References

https://www.ciscolive.com/on-demand/on-demand-library.html?search=PBR&search=PBR#/video/1751036943771001hQGc

https://www.ciscolive.com/on-demand/on-demand-library.html?search=PBR&search=PBR%2C+PBR#/video/1751295632557002SSZc

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739971.html