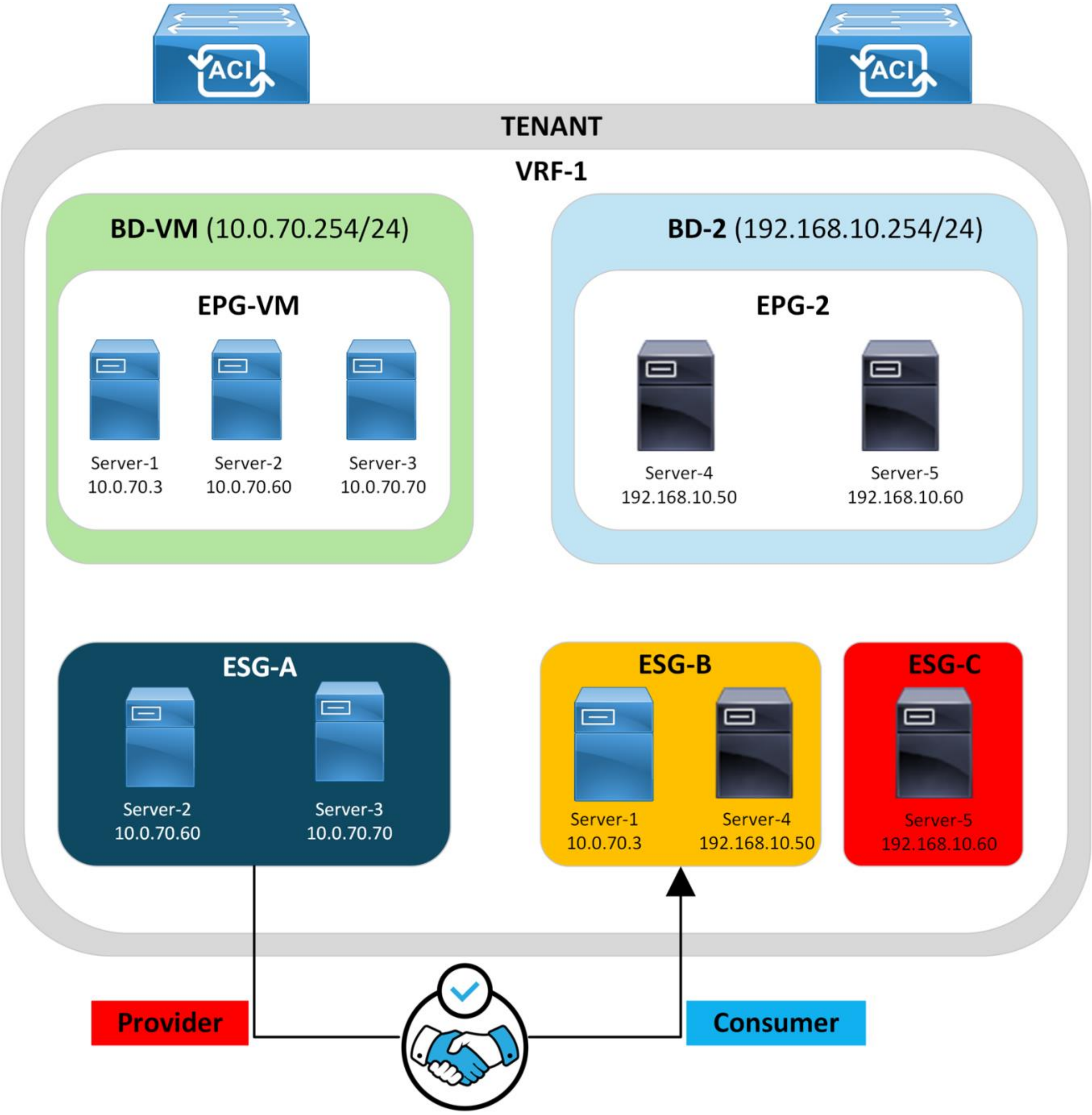
Cisco ACI Endpoint Security Groups (ESGs)



Lab By: Titus Majeza

Overview

An **Endpoint Security Group (ESG)** is a logical entity that contains network endpoints that are dynamically classified in them for segmentation purposes. Unlike an **Endpoint Group** (**EPG**), which defines a security zone under a **Bridge Domain (BD)**, an ESG defines a security zone within a **VRF** and is independent of the Bridge Domain. ESGs allows endpoints from any EPG within the same VRF to be classified inside them. It has no dependency with the Bridge domain. When ESGs are implemented in, the contracts are applied on the ESG level and not on the EPGs.

Endpoints are not automatically learned under the ESGs, instead there are match criteria that are defined and used to classify an endpoint into a specific ESG. This match criteria is known as ESG Selectors.
These selectors include:

- virtual machine name
- virtual machine tag
- Endpoint MAC address
- Endpoint IP address.

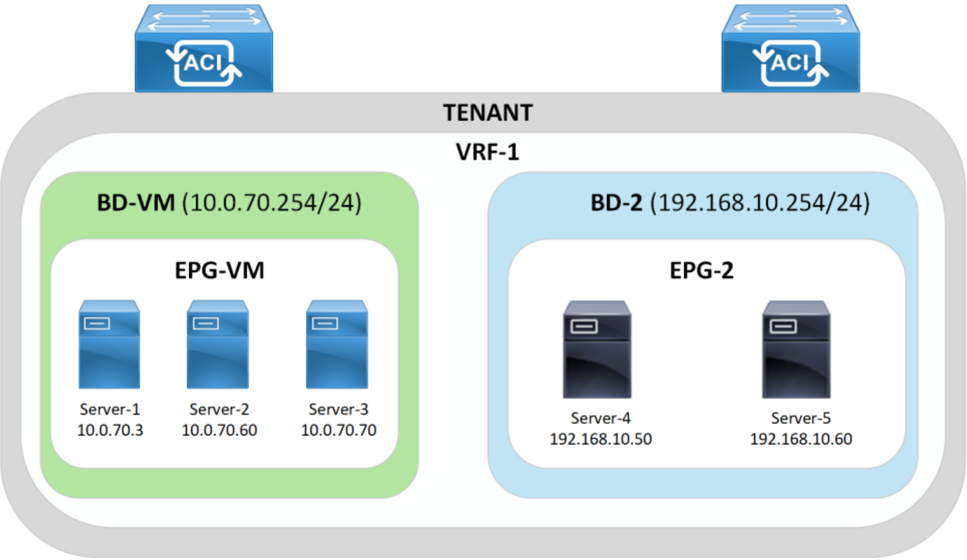
A selector is defined under the ESG object and any endpoint within its respective EPG that matches the defined attribute will be automatically classified into that ESG. If the ESG has a contract associated with it, the contract applies to all endpoints within that ESG.

For more details, refer to the official Cisco ACI Endpoint Security Group (ESG) Design Guide
https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-aci-esg-design-guide.html

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.

Lab-Setup

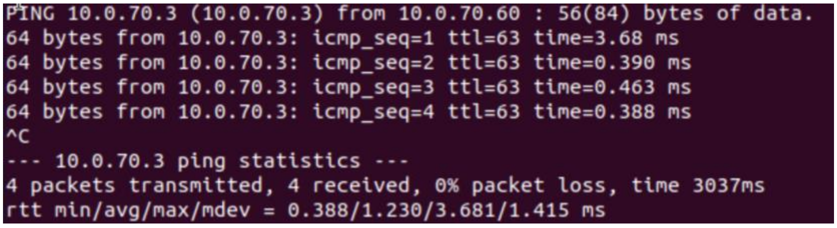
In this lab, there are two Endpoint Groups (EPGs), each within its respective Bridge Domain (BD), under the same Virtual Routing and Forwarding (VRF) instance. **EPG-VM** contains three endpoints and **EPG-2** contains two endpoints. These endpoints will be classified to different ESGs and contracts will be applied to the ESGs, instead of EPGs.



Verify endpoint learning:

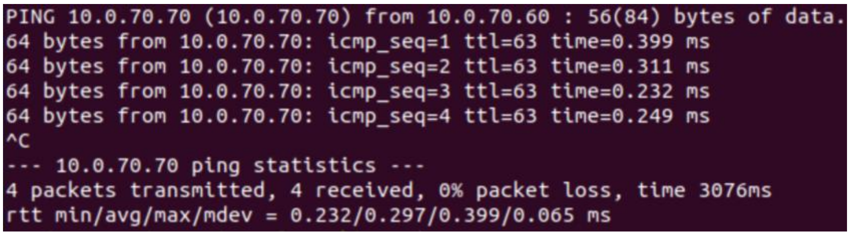
```
L101# show endpoint vrf tmajeza-tenant:VRF-1
Legend:
 S - static           s - arp              L - local            O - peer-attached
 V - vpc-attached     a - local-aged       p - peer-aged        M - span
 B - bounce           H - vtep             R - peer-attached-rl D - bounce-to-proxy
 E - shared-service   m - svc-mgr          C - control-ep
+-----------------------------------+---------------+-----------------+--------------+-------------+
      VLAN/                           Encap           MAC Address       MAC Info/       Interface
      Domain                          VLAN            IP Address        IP Info
+-----------------------------------+---------------+-----------------+--------------+-------------+
928                                       vlan-3129    0050.56b3.42c8 L                      eth1/5
tmajeza-tenant:VRF-1                      vlan-3129         10.0.70.3 L                      eth1/5
928                                       vlan-3129    0050.56b3.46ee O                    tunnel39
tmajeza-tenant:VRF-1                      vlan-3129        10.0.70.70 O                    tunnel39
928                                       vlan-3129    0050.56b3.5dd6 L                      eth1/5
tmajeza-tenant:VRF-1                      vlan-3129        10.0.70.60 L                      eth1/5
174                                       vlan-1929    cc16.7e82.a5f3 L                     eth1/50
tmajeza-tenant:VRF-1                      vlan-1929     192.168.10.50 L                     eth1/50
206                                       vlan-3014    0050.56b3.1ab7 L                      eth1/5
tmajeza-tenant:VRF-1                      vlan-3014     192.168.10.60 L                      eth1/5
```

ICMP reachability between Server-1 and Server-2 in the EPG-VM.



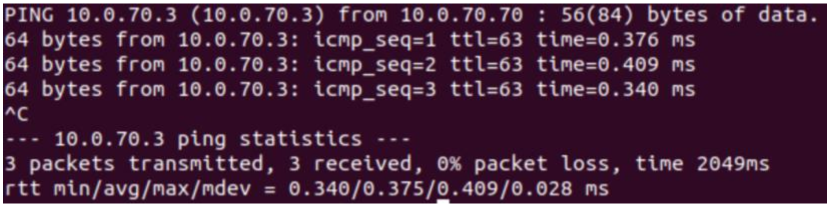
```
PING 10.0.70.3 (10.0.70.3) from 10.0.70.60 : 56(84) bytes of data.
64 bytes from 10.0.70.3: icmp_seq=1 ttl=63 time=3.68 ms
64 bytes from 10.0.70.3: icmp_seq=2 ttl=63 time=0.390 ms
64 bytes from 10.0.70.3: icmp_seq=3 ttl=63 time=0.463 ms
64 bytes from 10.0.70.3: icmp_seq=4 ttl=63 time=0.388 ms
^C
--- 10.0.70.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3037ms
rtt min/avg/max/mdev = 0.388/1.230/3.681/1.415 ms
```

ICMP reachability between Server-2 and Server-3 in the EPG-VM.



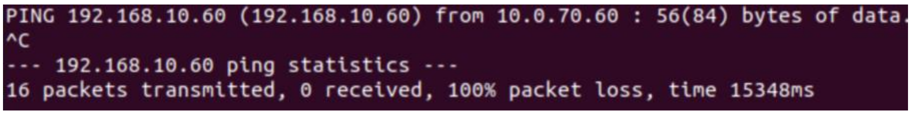
```
PING 10.0.70.70 (10.0.70.70) from 10.0.70.60 : 56(84) bytes of data.
64 bytes from 10.0.70.70: icmp_seq=1 ttl=63 time=0.399 ms
64 bytes from 10.0.70.70: icmp_seq=2 ttl=63 time=0.311 ms
64 bytes from 10.0.70.70: icmp_seq=3 ttl=63 time=0.232 ms
64 bytes from 10.0.70.70: icmp_seq=4 ttl=63 time=0.249 ms
^C
--- 10.0.70.70 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3076ms
rtt min/avg/max/mdev = 0.232/0.297/0.399/0.065 ms
```

ICMP reachability between Server-1 and Server-3 in the EPG-VM.



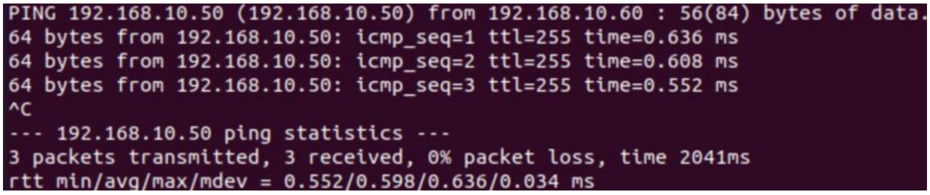
```
PING 10.0.70.3 (10.0.70.3) from 10.0.70.70 : 56(84) bytes of data.
64 bytes from 10.0.70.3: icmp_seq=1 ttl=63 time=0.376 ms
64 bytes from 10.0.70.3: icmp_seq=2 ttl=63 time=0.409 ms
64 bytes from 10.0.70.3: icmp_seq=3 ttl=63 time=0.340 ms
^C
--- 10.0.70.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2049ms
rtt min/avg/max/mdev = 0.340/0.375/0.409/0.028 ms
```

No communication is allowed between Servers in EPG-VM and Servers in EPG-2



```
PING 192.168.10.60 (192.168.10.60) from 10.0.70.60 : 56(84) bytes of data.
^C
--- 192.168.10.60 ping statistics ---
16 packets transmitted, 0 received, 100% packet loss, time 15348ms
```

ICMP reachability between Server-4 and Server-5 in the EPG-2.



```
PING 192.168.10.50 (192.168.10.50) from 192.168.10.60 : 56(84) bytes of data.
64 bytes from 192.168.10.50: icmp_seq=1 ttl=255 time=0.636 ms
64 bytes from 192.168.10.50: icmp_seq=2 ttl=255 time=0.608 ms
64 bytes from 192.168.10.50: icmp_seq=3 ttl=255 time=0.552 ms
^C
--- 192.168.10.50 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2041ms
rtt min/avg/max/mdev = 0.552/0.598/0.636/0.034 ms
```

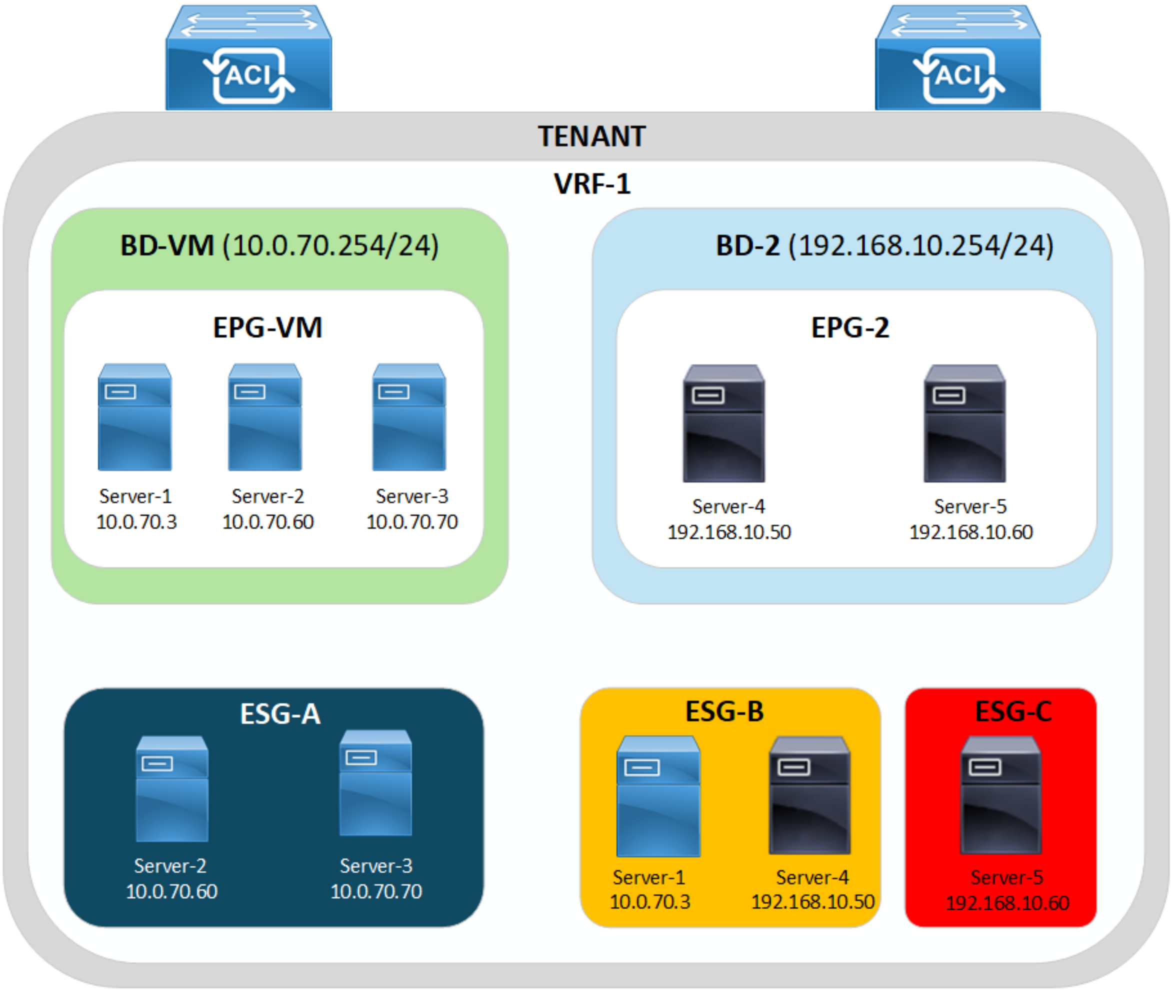
The communication matrix below provides an overview of server connectivity before any endpoint-to-ESG classification is applied. At this stage, endpoints can only communicate within their respective EPGs. No inter-ESG communication is permitted.

Communication Matrix:

	Default Gateway	**Server-1**	**Server-2**	**Server-3**	**Server-4**	**Server-5**
Default Gateway	⊗	✓	✓	✓	✓	✓
Server-1	✓	⊗	✓	✓	✗	✗
Server-2	✓	✓	⊗	✓	✗	✗
Server-3	✓	✓	✓	⊗	✗	✗
Server-4	✓	✗	✗	✗	⊗	✓
Server-5	✓	✗	✗	✗	✓	⊗

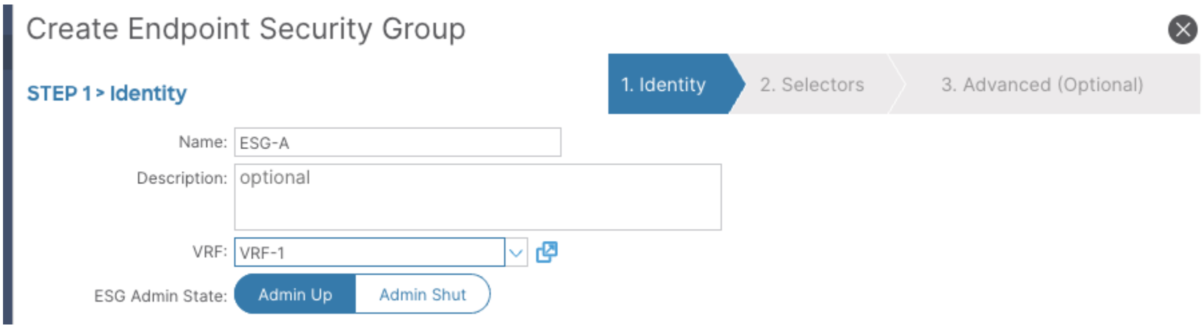
Target State

In this lab the design requirement is to place Server-2 & Server-3 in ESG-A, Server-1 & Server-4 in ESG-B and Server-5 in ESG-C. Classification of endpoints across the EPGs into the required ESGs will be achieved by the use of the following Selectors; Tag Selectors with VMM Integration (VM tags and VM names), IP Subnet selector, Endpoint IP Tag and Endpoint MAC Tag.



ESG Configuration

To configure an Endpoint Security Group navigate to Tenant >> Application Profile >> Endpoint Security Groups >> *Create Endpoint Security Group & Associate it with the VRF*



Create Endpoint Security Group

STEP 1 > Identity

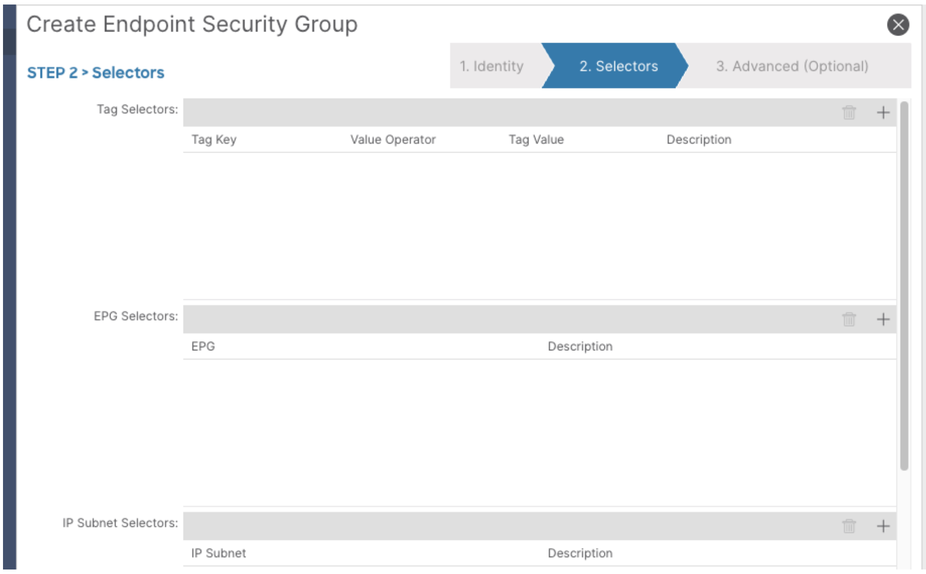
Name: ESG-A

Description: optional

VRF: VRF-1

ESG Admin State: [✓ Admin Up] Admin Shut

Leave the Selectors empty as these will be defined later after the creation of the required ESGs.



Create Endpoint Security Group

STEP 2 > Selectors

Tag Selectors:

Tag Key	Value Operator	Tag Value	Description

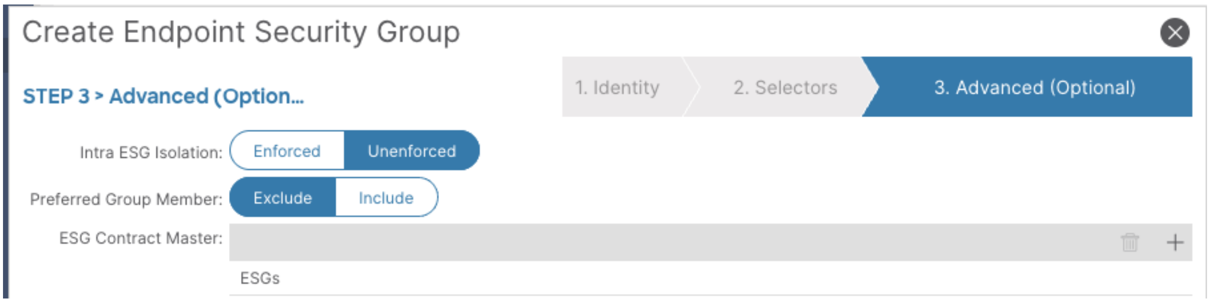
EPG Selectors:

EPG	Description

IP Subnet Selectors:

IP Subnet	Description

Leave the Advanced options in their default state.



Create Endpoint Security Group

STEP 3 > Advanced (Option...

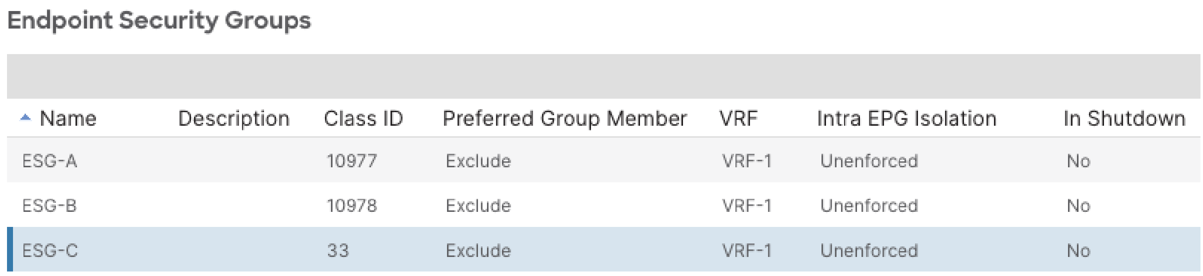
Intra ESG Isolation: Enforced [✓ Unenforced]

Preferred Group Member: [✓ Exclude] Include

ESG Contract Master:

ESGs

The required ESGs are successfully configured as follows:



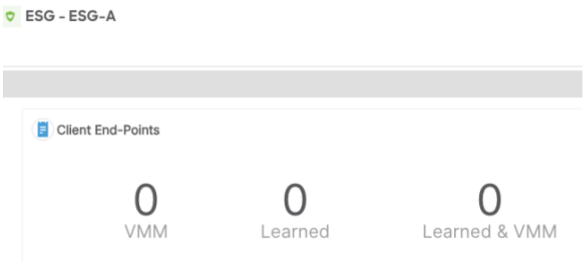
Endpoint Security Groups

Name	Description	Class ID	Preferred Group Member	VRF	Intra EPG Isolation	In Shutdown
ESG-A		10977	Exclude	VRF-1	Unenforced	No
ESG-B		10978	Exclude	VRF-1	Unenforced	No
ESG-C		33	Exclude	VRF-1	Unenforced	No

Note
Just like EPGs, ESGs are also assigned a unique “Class ID” or pcTag.

After the successful creation of ESGs, there are no endpoints classified in them until Selectors are defined in each ESG to classify the endpoints.

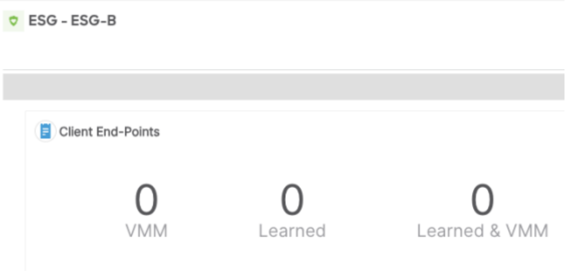
As shown below, there are no endpoints associated in any of the Endpoint Security Group.



ESG - ESG-A

Client End-Points

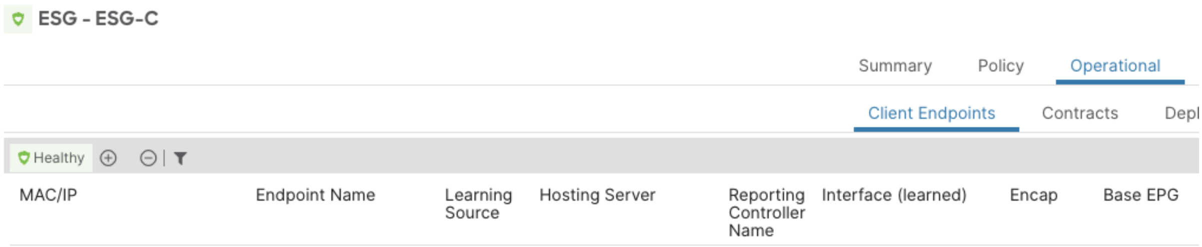
0 VMM
0 Learned
0 Learned & VMM



ESG - ESG-B

Client End-Points

0 VMM
0 Learned
0 Learned & VMM



ESG - ESG-C

MAC/IP | Endpoint Name | Learning Source | Hosting Server | Reporting Controller Name | Interface (learned) | Encap | Base EPG

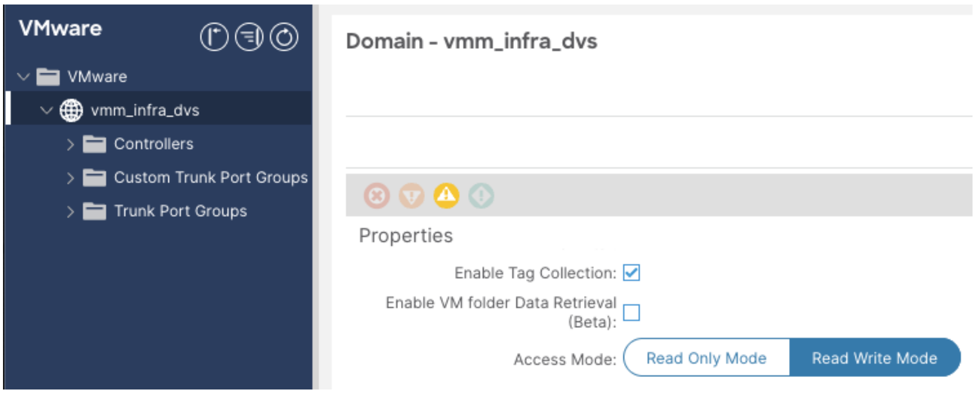
Selectors can be used to classify endpoints in the respective ESG according to the design requirements.

For ESG-A, **Tag Selectors with VMM Integration** are going to be used to classify Server-2 and Server-3 in this ESG. VM tags and VM names from VMware vCenter will be used for endpoint classification in an ESG.

Note
For this use case, VMM domain integration with read-write permissions is required.

When VM tags or VM names are used for tag selectors, the following two configurations are required on top of the tag selectors themselves.

1. Enable "Tag Collection" under the VMM domain itself.



Domain - vmm_infra_dvs

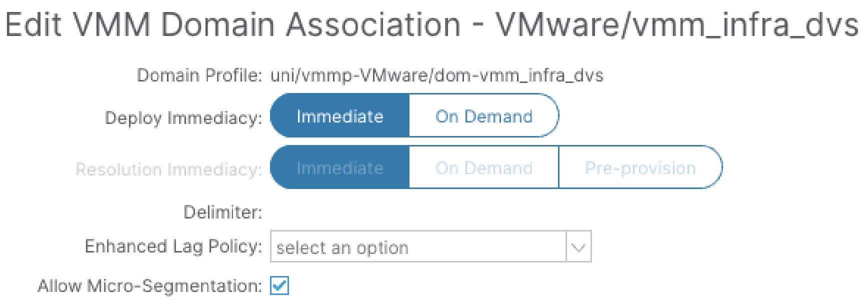
Properties

Enable Tag Collection: ☑

Enable VM folder Data Retrieval (Beta): □

Access Mode: Read Only Mode [✓ Read Write Mode]

2. Enable "Allow Micro-Segmentation" through the VMM domain association in the EPG.
   a. *This deploys PVLAN on Cisco ACI leaf switches and VMware vCenter port groups automatically. This is to prevent VMware virtual switches from bridging the traffic within the same port group without forwarding the traffic to Cisco ACI.*



Edit VMM Domain Association - VMware/vmm_infra_dvs

Domain Profile: uni/vmmp-VMware/dom-vmm_infra_dvs

Deploy Immediacy: [✓ Immediate] On Demand

Resolution Immediacy: [✓ Immediate] On Demand Pre-provision

Delimiter:

Enhanced Lag Policy: select an option

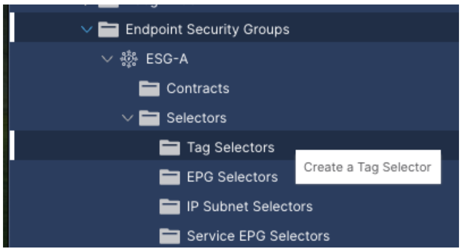
Allow Micro-Segmentation: ☑

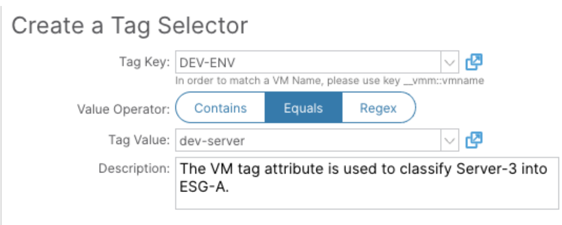
ESG-A Endpoint Classification

1. Server-2’s virtual name **(i.e. linux-10.0.70.60**) on VMware vCenter will be used as the attribute.

2. Server-3’s assigned tag on VMware vCenter **(tag: dev-server, Category: DEV-ENV)** will be used as the attribute.

Create the Tag selector under ESG-A and match the VM name and VM tag that are defined in VMWare vCenter for each VM.





Create a Tag Selector

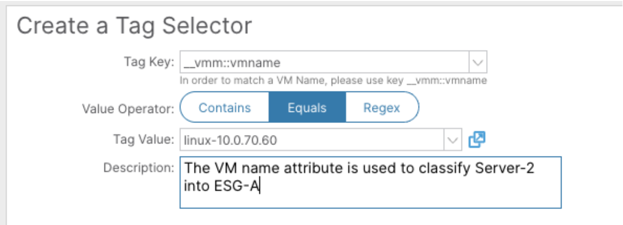
Tag Key: DEV-ENV

In order to match a VM Name, please use key __vmm::vmname

Value Operator: Contains [✓ Equals] Regex

Tag Value: dev-server

Description: The VM tag attribute is used to classify Server-3 into ESG-A.



Create a Tag Selector

Tag Key: __vmm::vmname

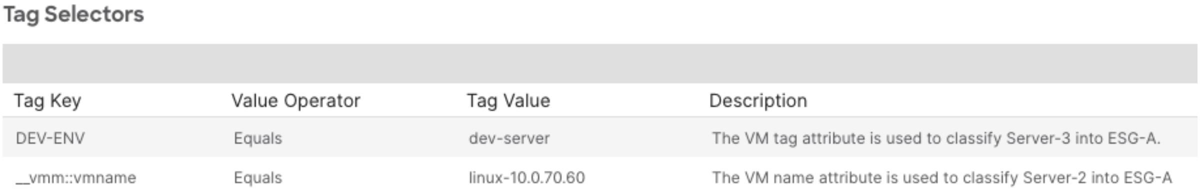
In order to match a VM Name, please use key __vmm::vmname

Value Operator: Contains [✓ Equals] Regex

Tag Value: linux-10.0.70.60

Description: The VM name attribute is used to classify Server-2 into ESG-A

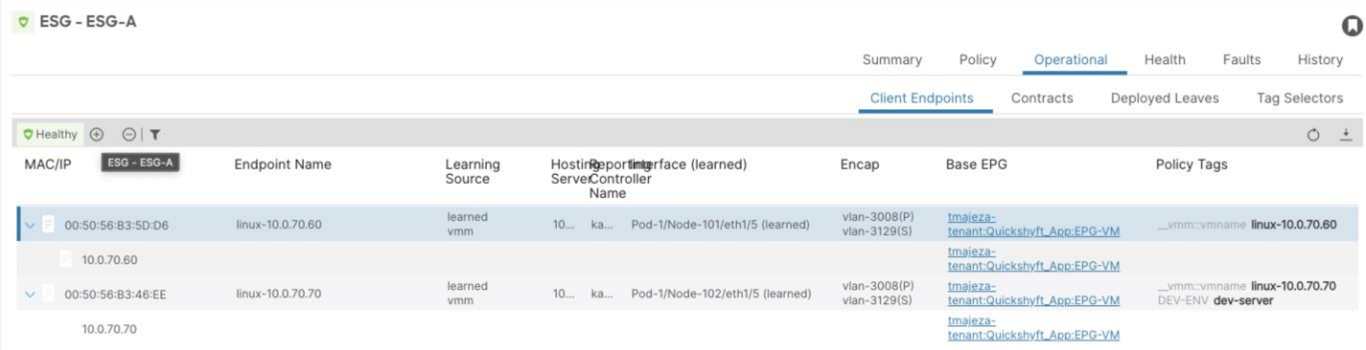
The resulting configuration is shown below (Tag selectors are successfully created under ESG-A):



Tag Selectors

Tag Key	Value Operator	Tag Value	Description
DEV-ENV	Equals	dev-server	The VM tag attribute is used to classify Server-3 into ESG-A.
__vmm::vmname	Equals	linux-10.0.70.60	The VM name attribute is used to classify Server-2 into ESG-A

The endpoints that match the defined criteria from the Tag Selectors are dynamically learned in ESG-A as shown below.



MAC/IP	Endpoint Name	Learning Source	Hosting Server	Reporting Controller Name	Interface (learned)	Encap	Base EPG	Policy Tags

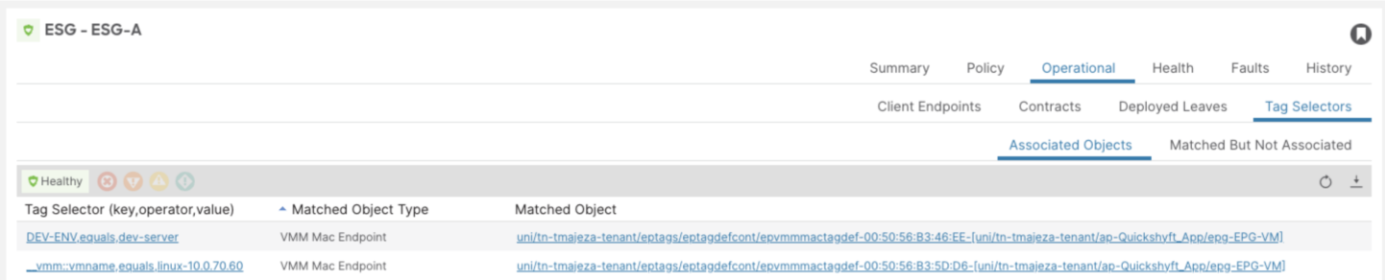
00:50:56:B3:5D:D6	linux-10.0.70.60	learned vmm	10...	ka...	Pod-1/Node-101/eth1/5 (learned)	vlan-3008(P)
						vlan-3129(S)
							tmajeza-tenant:Quickshyft_App:EPG-VM	__vmm::vmname **linux-10.0.70.60**

10.0.70.60							tmajeza-tenant:Quickshyft_App:EPG-VM	

00:50:56:B3:46:EE	linux-10.0.70.70	learned vmm	10...	ka...	Pod-1/Node-102/eth1/5 (learned)	vlan-3008(P)
						vlan-3129(S)
							tmajeza-tenant:Quickshyft_App:EPG-VM	__vmm::vmname **linux-10.0.70.70**
								DEV-ENV **dev-server**

10.0.70.70							tmajeza-tenant:Quickshyft_App:EPG-VM	

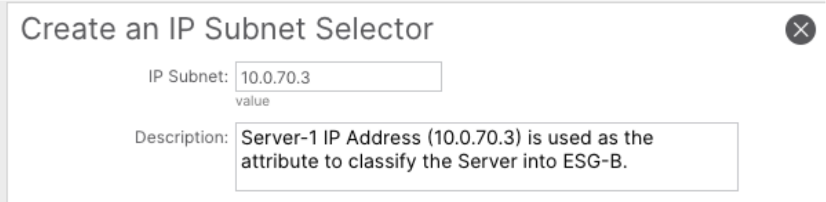
To view the endpoints that matched a specific classification criteria, navigate to ESG >> Operational >> Tag Selectors >> Associated Objects.



Tag Selector (key,operator,value)	Matched Object Type	Matched Object
DEV-ENV,equals,dev-server	VMM Mac Endpoint	uni/tn-tmajeza-tenant/eptags/eptagdefcont/epvmmmactagdef-00:50:56:B3:46:EE-[uni/tn-tmajeza-tenant/ap-Quickshyft_App/epg-EPG-VM]
__vmm::vmname,equals,linux-10.0.70.60	VMM Mac Endpoint	uni/tn-tmajeza-tenant/eptags/eptagdefcont/epvmmmactagdef-00:50:56:B3:5D:D6-[uni/tn-tmajeza-tenant/ap-Quickshyft_App/epg-EPG-VM]

ESG-B Endpoint Classification

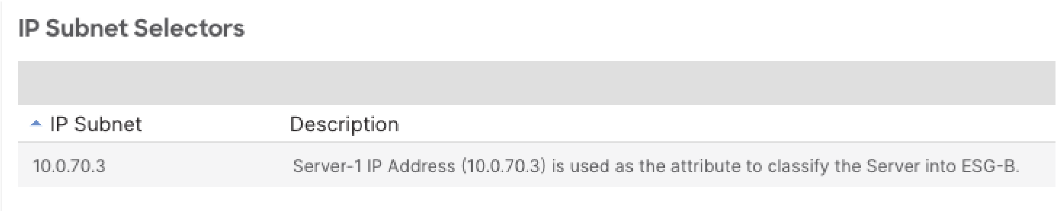
Server-1's IP Address is used to classify it into ESG-B. Under ESG-B, navigate to Selectors >> IP Subnet Selectors and Create an IP Subnet Selector. In this lab the specific IP address of Server-1 was defined.



Create an IP Subnet Selector

IP Subnet: 10.0.70.3
value

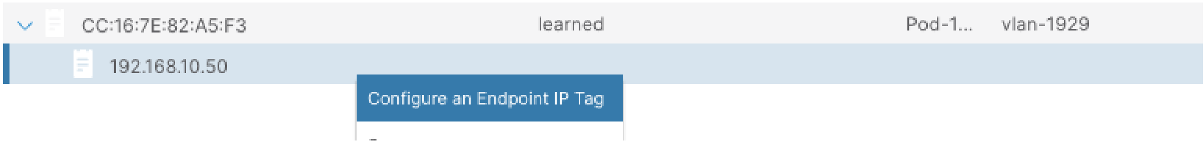
Description: Server-1 IP Address (10.0.70.3) is used as the attribute to classify the Server into ESG-B.



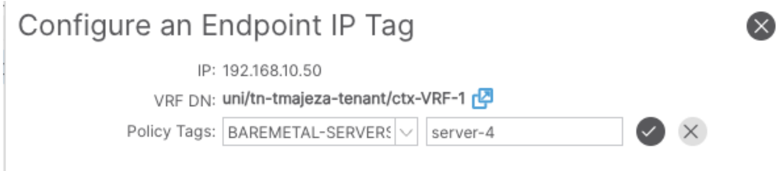
IP Subnet Selectors

IP Subnet	Description
10.0.70.3	Server-1 IP Address (10.0.70.3) is used as the attribute to classify the Server into ESG-B.

Server-4 in EPG-2 is assigned an ACI policy tag (server-4) and this tag will be used to classify the server in ESG-B.



CC:16:7E:82:A5:F3	learned	Pod-1...	vlan-1929
192.168.10.50			



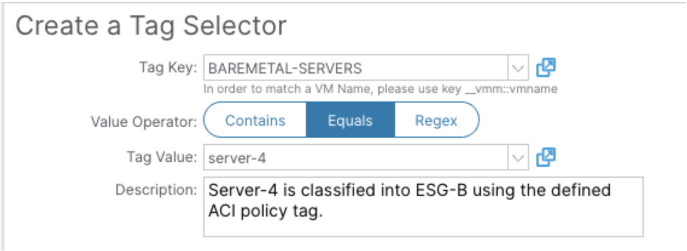
Configure an Endpoint IP Tag

IP: 192.168.10.50

VRF DN: uni/tn-tmajeza-tenant/ctx-VRF-1

Policy Tags: BAREMETAL-SERVERS server-4

Under the ESG, Create a Tag selector that matches the IP Endpoint tag that was defined for Server-4.



Create a Tag Selector

Tag Key: BAREMETAL-SERVERS

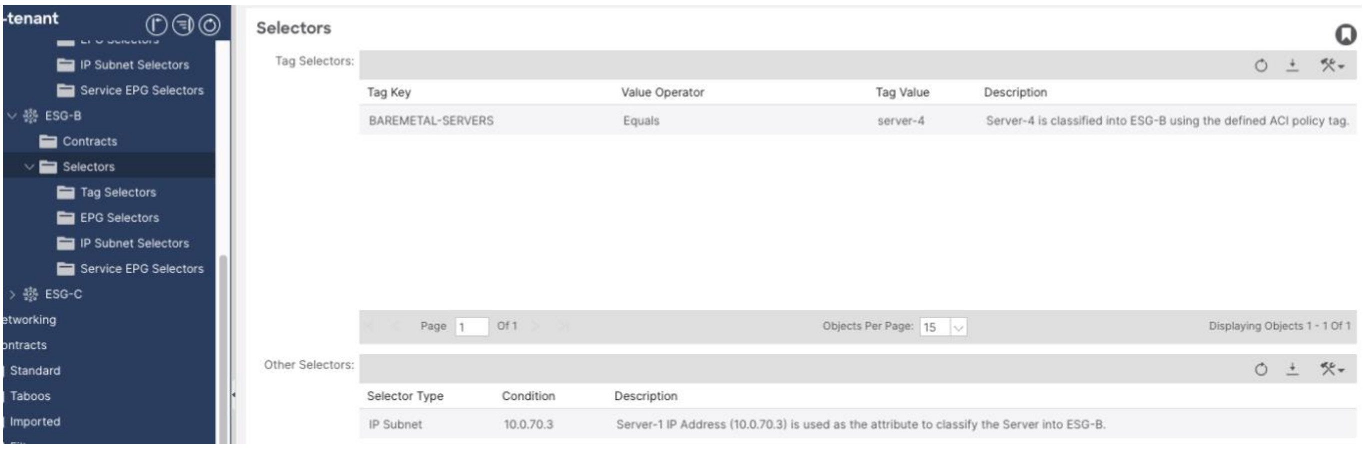
In order to match a VM Name, please use key __vmm::vmname

Value Operator: Contains [✓ Equals] Regex

Tag Value: server-4

Description: Server-4 is classified into ESG-B using the defined ACI policy tag.

To view the Selectors that were defined under ESG-B, Navigate and Click on “Selectors”:



Selectors

Tag Selectors:

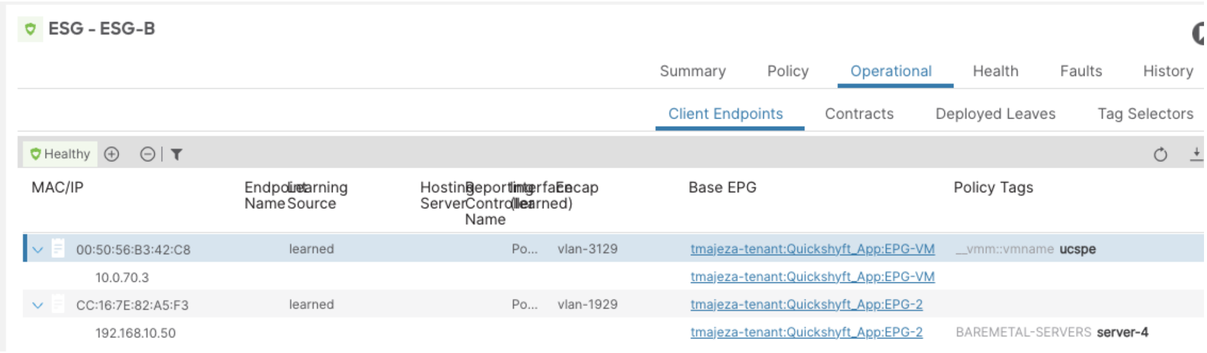
Tag Key	Value Operator	Tag Value	Description
BAREMETAL-SERVERS	Equals	server-4	Server-4 is classified into ESG-B using the defined ACI policy tag.

Page 1 Of 1 Objects Per Page: 15 Displaying Objects 1 - 1 Of 1

Other Selectors:

Selector Type	Condition	Description
IP Subnet	10.0.70.3	Server-1 IP Address (10.0.70.3) is used as the attribute to classify the Server into ESG-B.

Server-1 and Server-4 are successfully matched into ESG-B based on the IP Subnet selector and Tag selector that were defined as the match criteria. The Base EPG indicates the actual EPG where the matched endpoint belongs to. It is evident that endpoints from different EPGs can be classified in the same Endpoint Security Group.

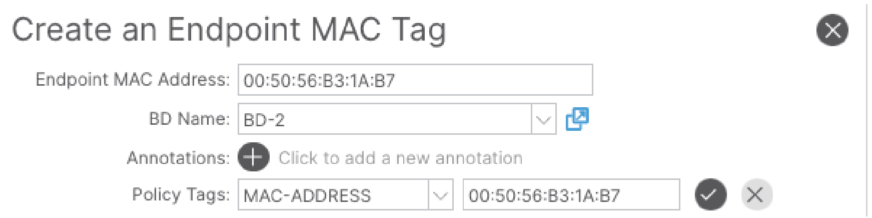


ESG - ESG-B

MAC/IP	Endpoint Name	Learning Source	Hosting Server	Reporting Controller Name	Interface	Encap (learned)	Base EPG	Policy Tags
00:50:56:B3:42:C8		learned			Po...	vlan-3129	tmajeza-tenant:Quickshyft_App:EPG-VM	__vmm::vmname ucspe
10.0.70.3							tmajeza-tenant:Quickshyft_App:EPG-VM	
CC:16:7E:82:A5:F3		learned			Po...	vlan-1929	tmajeza-tenant:Quickshyft_App:EPG-2	
192.168.10.50							tmajeza-tenant:Quickshyft_App:EPG-2	BAREMETAL-SERVERS server-4

ESG-C Endpoint Classification

An Endpoint MAC tag is created for Server-5.



Create an Endpoint MAC Tag

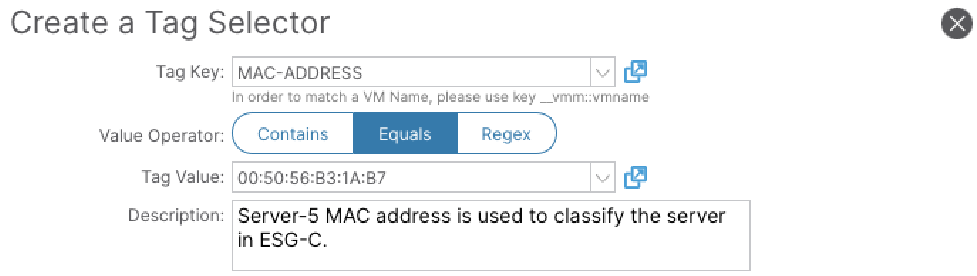
Endpoint MAC Address: 00:50:56:B3:1A:B7

BD Name: BD-2

Annotations: Click to add a new annotation

Policy Tags: MAC-ADDRESS 00:50:56:B3:1A:B7

Under ESG-C, a Tag Selector is created using the MAC-ADDRESS of Server-5.



Create a Tag Selector

Tag Key: MAC-ADDRESS

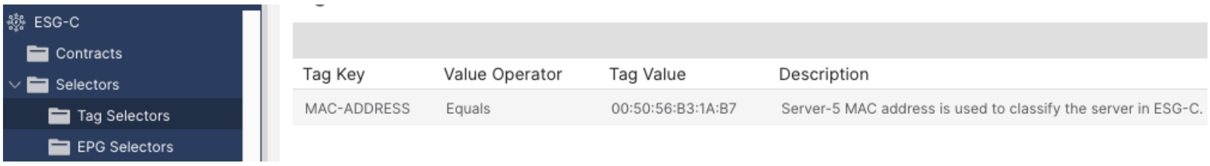
In order to match a VM Name, please use key __vmm::vmname

Value Operator: Contains Equals Regex

Tag Value: 00:50:56:B3:1A:B7

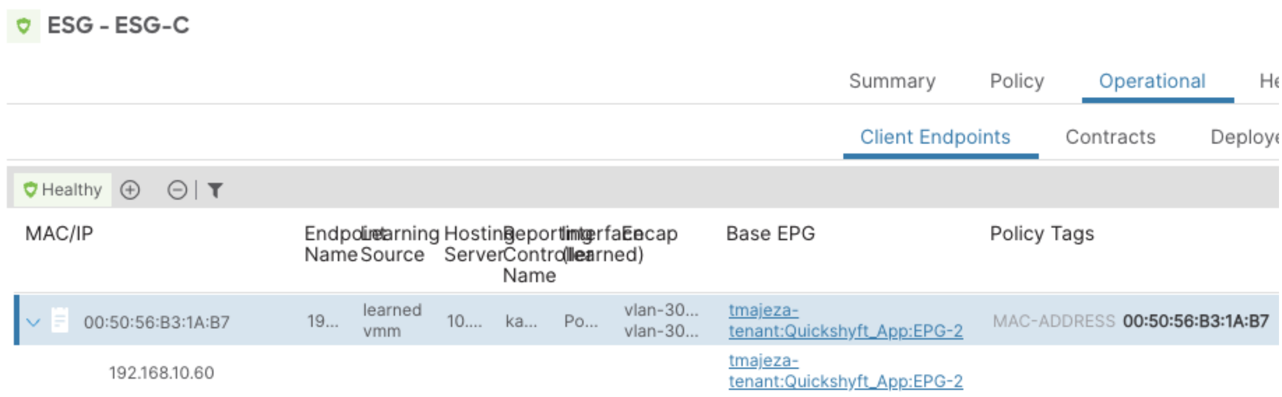
Description: Server-5 MAC address is used to classify the server in ESG-C.

The created Tag Selector can be seen under ESG-C>>Tag Selector



Tag Key	Value Operator	Tag Value	Description
MAC-ADDRESS	Equals	00:50:56:B3:1A:B7	Server-5 MAC address is used to classify the server in ESG-C.

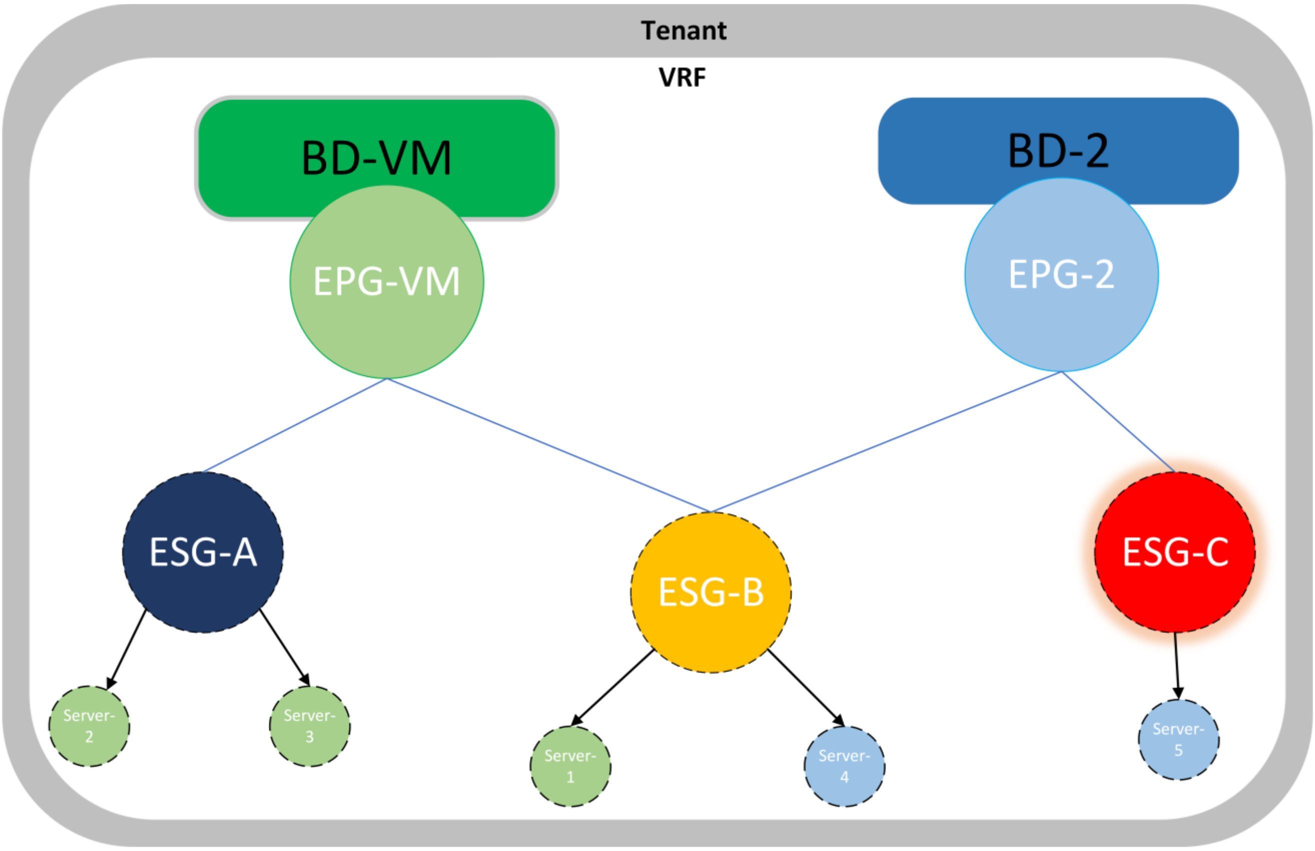
Server-5 from EPG-2 matches the defined criteria thus dynamically mapped to ESG-C.



ESG - ESG-C

MAC/IP	Endpoint Name	Learning Source	Hosting Server	Reporting Controller Name	Interface	Encap (learned)	Base EPG	Policy Tags
00:50:56:B3:1A:B7	19...	learned vmm	10....	ka...	Po...	vlan-30... vlan-30...	tmajeza-tenant:Quickshyft_App:EPG-2	MAC-ADDRESS 00:50:56:B3:1A:B7
192.168.10.60							tmajeza-tenant:Quickshyft_App:EPG-2	

The diagram below shows the endpoints classification into ESGs that has been achieved. From this point, contracts can be applied to ESGs, and any endpoint within an ESG is subject to the security policies defined for that ESG.

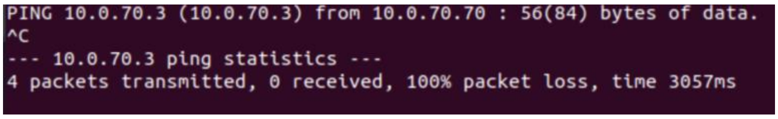


The communication matrix below shows which servers can communicate with each other before any contracts are applied between ESGs. It is evident that only endpoints within the same ESG can communicate, while inter-ESG communication is not permitted

Communication Matrix:

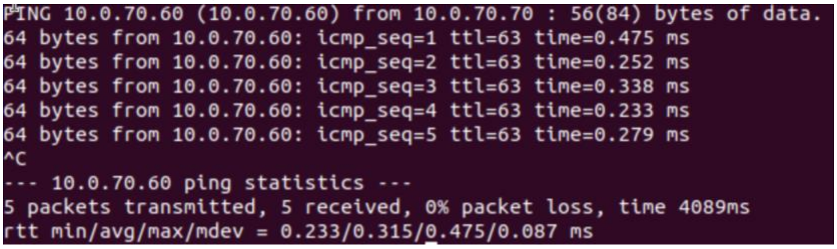
	Default Gateway	Server-1	Server-2	Server-3	Server-4	Server-5
Default Gateway	⊗	✅	✅	✅	✅	✅
Server-1	✅	⊗	✗	✗	✅	✗
Server-2	✅	✗	⊗	✅	✗	✗
Server-3	✅	✗	✅	⊗	✗	✗
Server-4	✅	✅	✗	✗	⊗	✗
Server-5	✅	✗	✗	✗	✗	⊗

No communication is allowed between Server-1 and (Server-2/Server3) as they are in different ESGs.



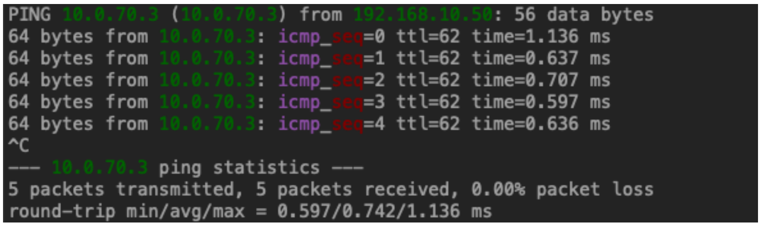
```
PING 10.0.70.3 (10.0.70.3) from 10.0.70.70 : 56(84) bytes of data.
^C
--- 10.0.70.3 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3057ms
```

ICMP reachability between Server-2 and Server-3 in ESG-A.



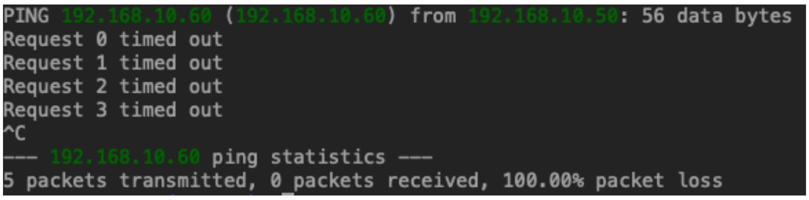
```
PING 10.0.70.60 (10.0.70.60) from 10.0.70.70 : 56(84) bytes of data.
64 bytes from 10.0.70.60: icmp_seq=1 ttl=63 time=0.475 ms
64 bytes from 10.0.70.60: icmp_seq=2 ttl=63 time=0.252 ms
64 bytes from 10.0.70.60: icmp_seq=3 ttl=63 time=0.338 ms
64 bytes from 10.0.70.60: icmp_seq=4 ttl=63 time=0.233 ms
64 bytes from 10.0.70.60: icmp_seq=5 ttl=63 time=0.279 ms
^C
--- 10.0.70.60 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4089ms
rtt min/avg/max/mdev = 0.233/0.315/0.475/0.087 ms
```

ICMP reachability between Server-1 and Server-4 in ESG-B.



```
PING 10.0.70.3 (10.0.70.3) from 192.168.10.50: 56 data bytes
64 bytes from 10.0.70.3: icmp_seq=0 ttl=62 time=1.136 ms
64 bytes from 10.0.70.3: icmp_seq=1 ttl=62 time=0.637 ms
64 bytes from 10.0.70.3: icmp_seq=2 ttl=62 time=0.707 ms
64 bytes from 10.0.70.3: icmp_seq=3 ttl=62 time=0.597 ms
64 bytes from 10.0.70.3: icmp_seq=4 ttl=62 time=0.636 ms
^C
--- 10.0.70.3 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.597/0.742/1.136 ms
```

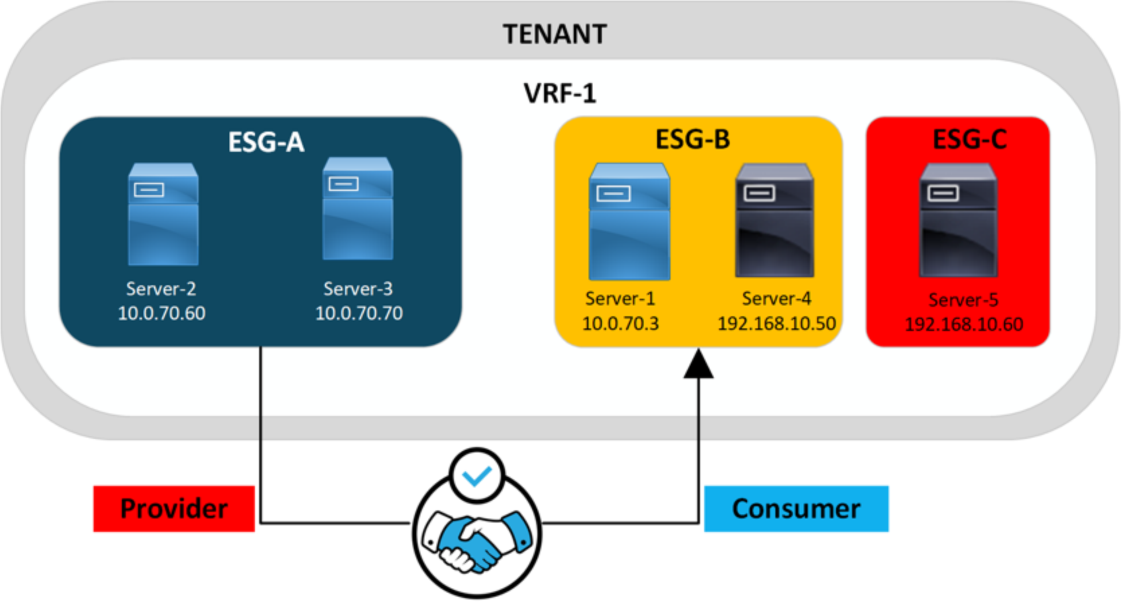
No communication is allowed between Server-4/Server-1 and Server-5 as they are in different ESGs.



```
PING 192.168.10.60 (192.168.10.60) from 192.168.10.50: 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
^C
--- 192.168.10.60 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
```

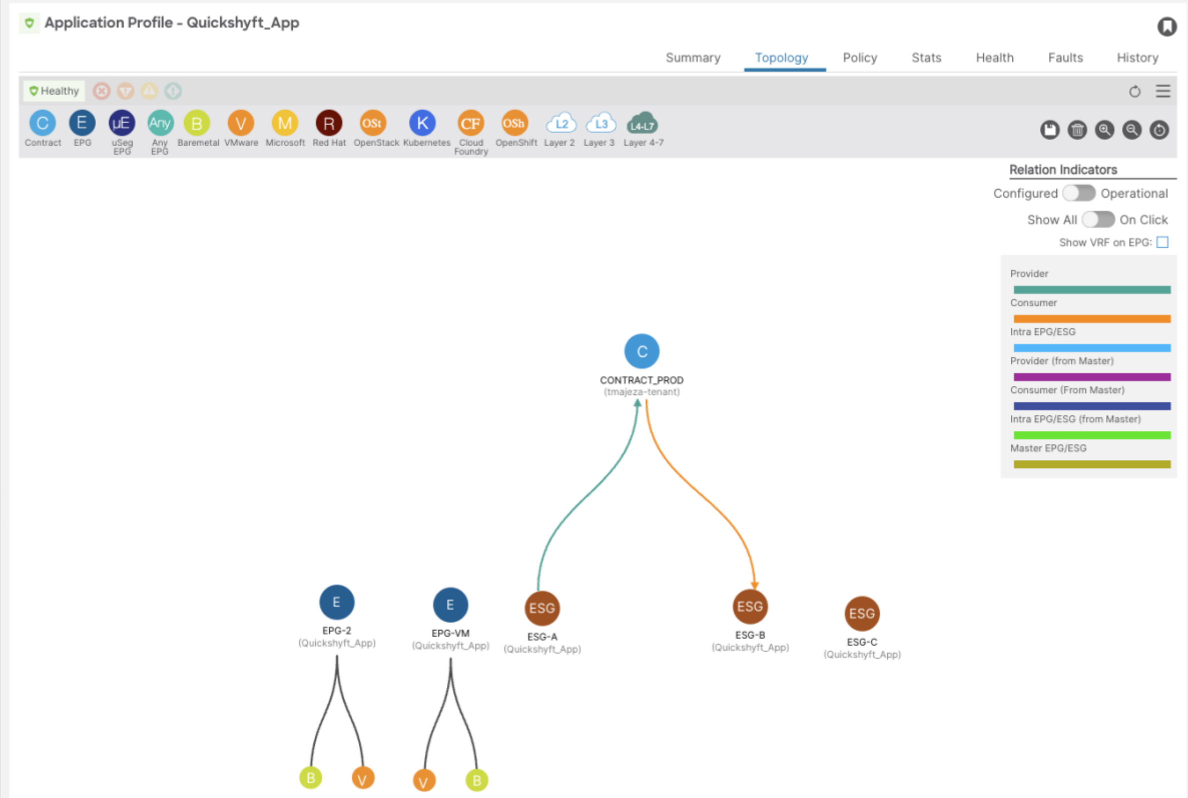
Contracts Applied to ESGs

A contract that permits ICMP and https traffic is now applied on the ESG level to enable communication between endpoints in ESG-A and ESG-B.

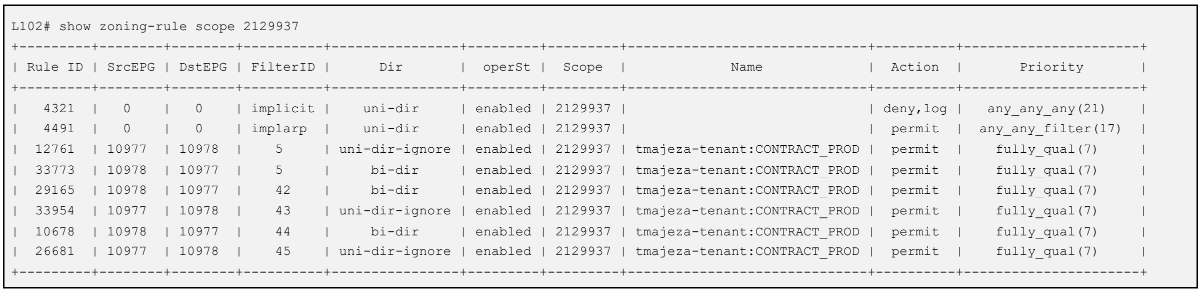


To apply contracts to the ESGs, navigate to an **ESG >> Contracts >>** *Add Provided/Consumed Contract.*

After the contract has been applied on ESG-A and ESG-B, the Provider – Consumer relationship can be observed from the Application Profile Topology.



Applying the Contracts configurations result in zoning-rules programmed to the hardware in order to enforce the required policy.



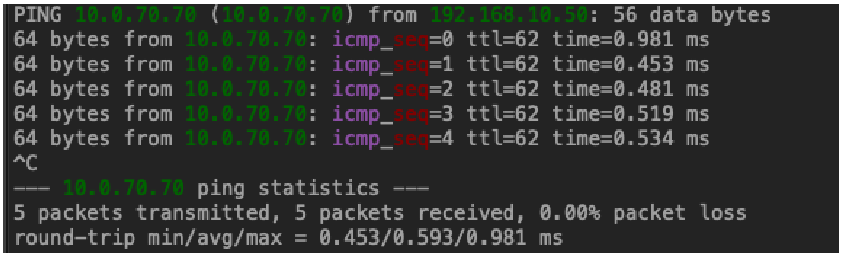
```
L102# show zoning-rule scope 2129937
+---------+--------+--------+----------+---------------+---------+---------+------------------------------+----------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir      |  operSt |  Scope  |             Name             |  Action  |       Priority       |
+---------+--------+--------+----------+---------------+---------+---------+------------------------------+----------+----------------------+
|   4321  |   0    |   0    | implicit |    uni-dir    | enabled | 2129937 |                              | deny,log |   any_any_any(21)    |
|   4491  |   0    |   0    | implarp  |    uni-dir    | enabled | 2129937 |                              |  permit  |  any_any_filter(17)  |
|  12761  | 10977  | 10978  |    5     | uni-dir-ignore | enabled | 2129937 | tmajeza-tenant:CONTRACT_PROD |  permit  |    fully_qual(7)     |
|  33773  | 10978  | 10977  |    5     |     bi-dir    | enabled | 2129937 | tmajeza-tenant:CONTRACT_PROD |  permit  |    fully_qual(7)     |
|  29165  | 10978  | 10977  |    42    |     bi-dir    | enabled | 2129937 | tmajeza-tenant:CONTRACT_PROD |  permit  |    fully_qual(7)     |
|  33954  | 10977  | 10978  |    43    | uni-dir-ignore | enabled | 2129937 | tmajeza-tenant:CONTRACT_PROD |  permit  |    fully_qual(7)     |
|  10678  | 10978  | 10977  |    44    |     bi-dir    | enabled | 2129937 | tmajeza-tenant:CONTRACT_PROD |  permit  |    fully_qual(7)     |
|  26681  | 10977  | 10978  |    45    | uni-dir-ignore | enabled | 2129937 | tmajeza-tenant:CONTRACT_PROD |  permit  |    fully_qual(7)     |
+---------+--------+--------+----------+---------------+---------+---------+------------------------------+----------+----------------------+
```

Note
The ESGs pcTags are used in the zoning-rule table, not EPG pcTags.

After the contract has been applied:

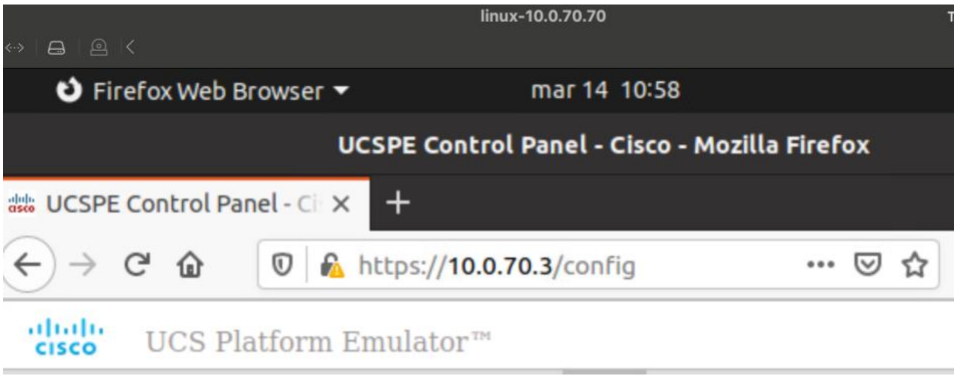
Endpoints in ESG-A can communicate with endpoints in ESG-B and vice-versa.

ICMP:



```
PING 10.0.70.70 (10.0.70.70) from 192.168.10.50: 56 data bytes
64 bytes from 10.0.70.70: icmp_seq=0 ttl=62 time=0.981 ms
64 bytes from 10.0.70.70: icmp_seq=1 ttl=62 time=0.453 ms
64 bytes from 10.0.70.70: icmp_seq=2 ttl=62 time=0.481 ms
64 bytes from 10.0.70.70: icmp_seq=3 ttl=62 time=0.519 ms
64 bytes from 10.0.70.70: icmp_seq=4 ttl=62 time=0.534 ms
^C
--- 10.0.70.70 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.453/0.593/0.981 ms
```

https:



The communication matrix below indicates that inter-ESG communication is now permitted between endpoints in ESG-A and ESG-B, based on the contract security policies defined.

Communication Matrix:

	Default Gateway	Server-1	Server-2	Server-3	Server-4	Server-5
Default Gateway	⊗	✓	✓	✓	✓	✓
Server-1	✓	⊗	✓	✓	✓	✗
Server-2	✓	✓	⊗	✓	✓	✗
Server-3	✓	✓	✓	⊗	✓	✗
Server-4	✓	✓	✓	✓	⊗	✗
Server-5	✓	✗	✗	✗	✗	⊗

This lab successfully demonstrated the fundamental configurations needed to define ESGs and to classify endpoints into the different ESGs based on defined match criteria. Each endpoint is identified by a specific attribute (e.g., VM name, VM tag, IP address, or MAC address). ESGs use match criteria aligned with these attributes to classify endpoints into their respective groups. Additionally, a contract was applied to the ESGs to showcase how ACI enforces security policies at the ESG level.

References:

https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-aci-esg-design-guide.html
https://blogs.cisco.com/datacenter/aci-segmentation-and-migrations-made-easier-with-endpoint-security-groups-esg
https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/6x/security-configuration/cisco-apic-security-configuration-guide-60x/endpoint-security-groups-60x.html