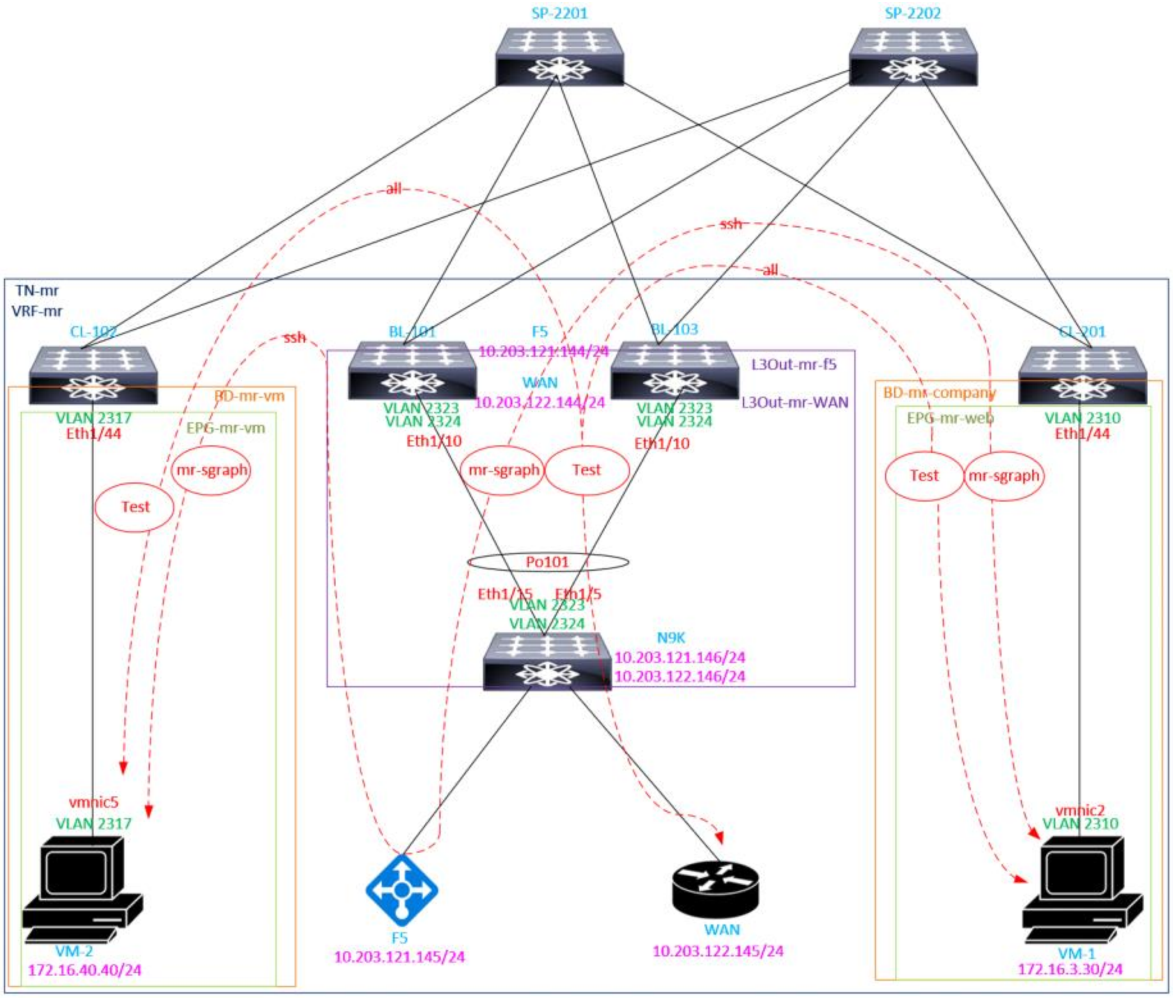
Cisco ACI PBR with L3Out (Service Device not Directly Connected to Fabric)

Monday, September 9, 2024 14:46

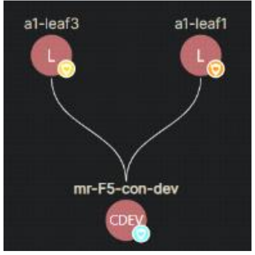
Since Cisco APIC release 5.2(1), an L4-L7 service device that's used as a PBR destination can have all its interfaces in an L3Out. This is particularly useful in a migration scenario where a service device has not yet been moved into ACI, yet still needs to be reachable from endpoints inside of the ACI fabric. In some cases, the service device may not be directly connected to the fabric. Fortunately, Cisco ACI still provides the ability to redirect traffic to a device like this. The purpose of this article is to demonstrate how this can be done. For guidelines and limitations, plus full configuration steps, please refer to the Policy -Based Redirect with an L3Out section in the deployment guide (https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/5x/layer-4-to-layer-7-services-configuration/cisco-apic-layer-4-to-layer-7-services-deployment-guide-53x/configuring-policy-based-redirect-53x.html#id_110094).



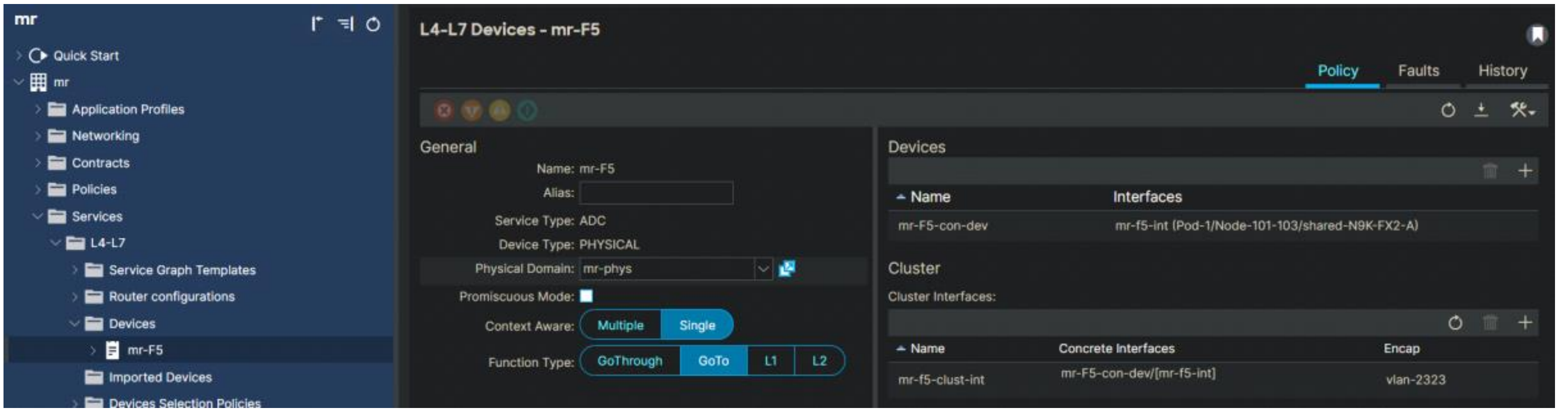
VM-1 needs to connect to VM-2 over SSH, but the SSH traffic must be redirected to the F5 load balancer first. Only SSH traffic should be allowed to reach the F5, all other traffic should be denied. However, all traffic should be allowed over the WAN. To make this work, you can use two separate L3Out EPGs, one for F5, and one for WAN (I used two separate L3Outs to accomplish this in my lab, but theoretically you could use a single L3Out with two separate L3Out EPGs in it).

Configuration
First, begin by creating the L4-L7 device. For exact steps, please refer to the Configuring a Layer 4 to Layer 7 Services Device Using the GUI section in the deployment guide.

L4-L7 device topology



L4-L7 device policy



L4-L7 Devices - mr-F5

General

Name: mr-F5

Alias:

Service Type: ADC

Device Type: PHYSICAL

Physical Domain: mr-phys

Promiscuous Mode: □

Context Aware: Multiple [✓ Single]

Function Type: GoThrough [✓ GoTo] L1 L2

Devices

Name	Interfaces
mr-F5-con-dev	mr-f5-int (Pod-1/Node-101-103/shared-N9K-FX2-A)

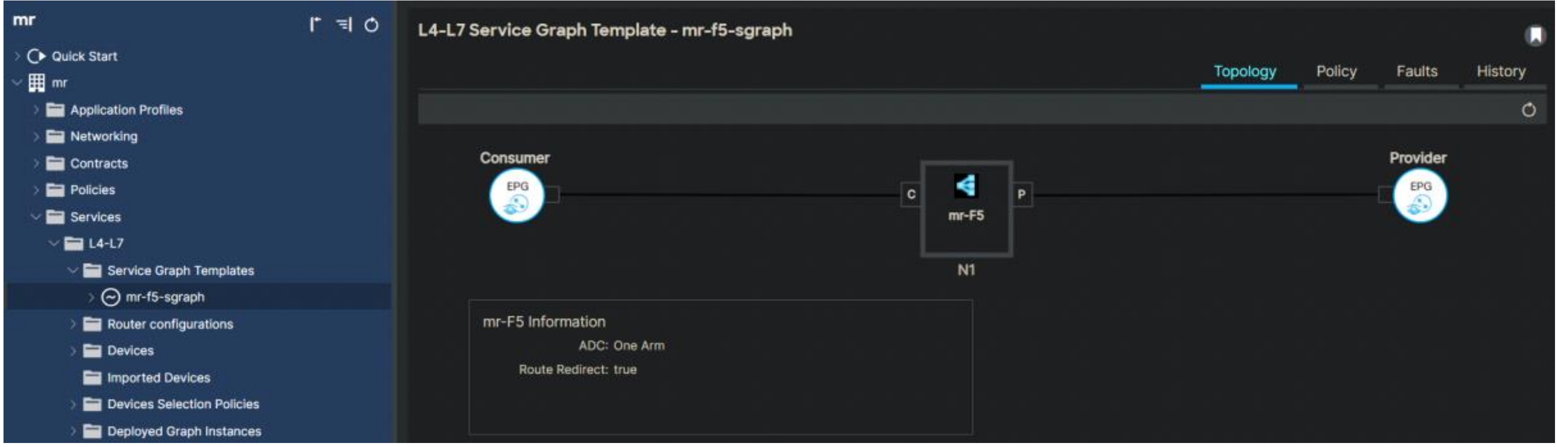
Cluster

Cluster Interfaces:

Name	Concrete Interfaces	Encap
mr-f5-clust-int	mr-F5-con-dev/[mr-f5-int]	vlan-2323

Next, create a service graph template. For exact steps, please refer to the Configuring a Service Graph Template Using the GUI section in the deployment guide (https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/5x/layer-4-to-layer-7-services-configuration/cisco-apic-layer-4-to-layer-7-services-deployment-guide-53x/configuring-a-service-graph-53x.html#task_85BC7D53988D4C1EA69626B5A1EE90DE).

Service graph template topology



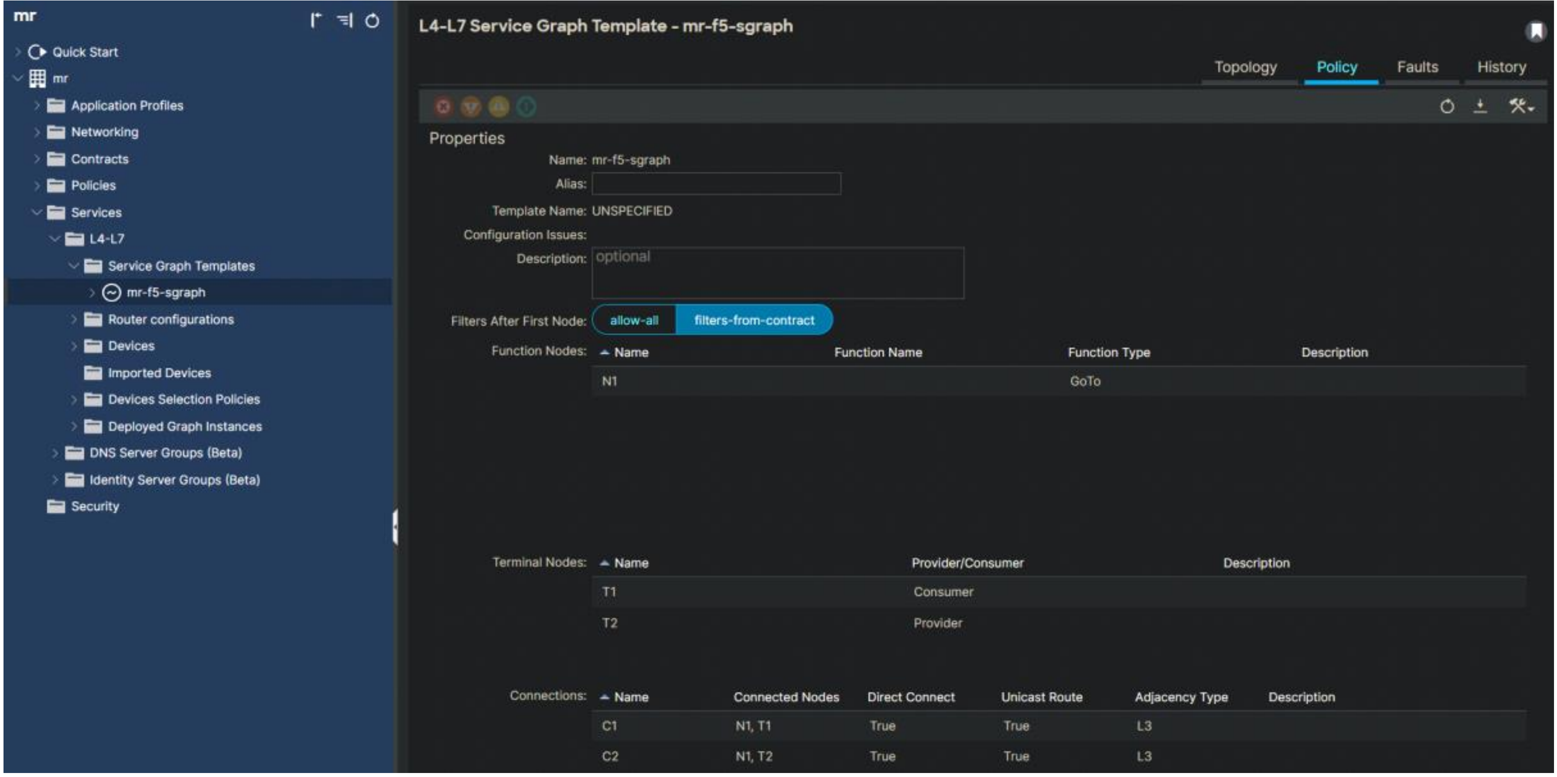
L4-L7 Service Graph Template - mr-f5-sgraph

mr-F5 Information

ADC: One Arm

Route Redirect: true

Service graph template policy



L4-L7 Service Graph Template - mr-f5-sgraph

Properties

Name: mr-f5-sgraph

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	

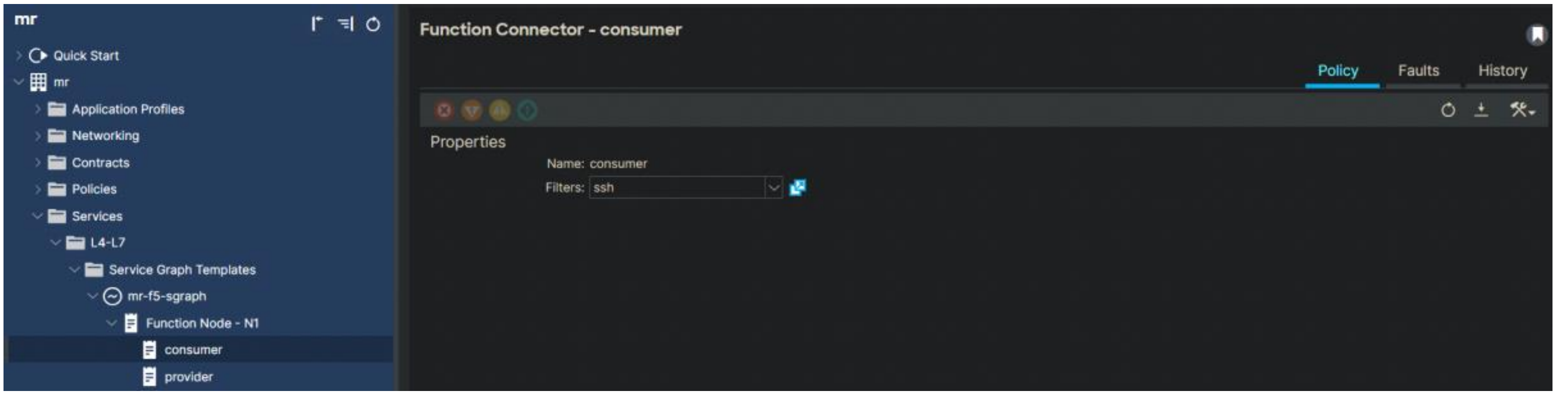
Terminal Nodes:

Name	Provider/Consumer	Description
T1	Consumer	
T2	Provider	

Connections:

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

Consumer filter



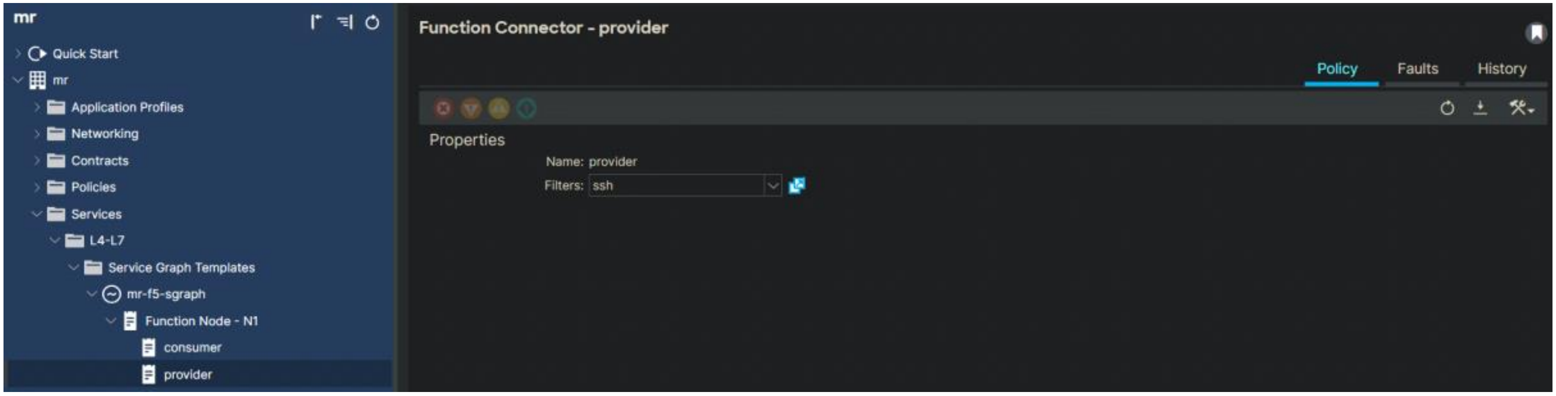
Function Connector - consumer

Properties

Name: consumer

Filters: ssh

Provider filter



Function Connector - provider

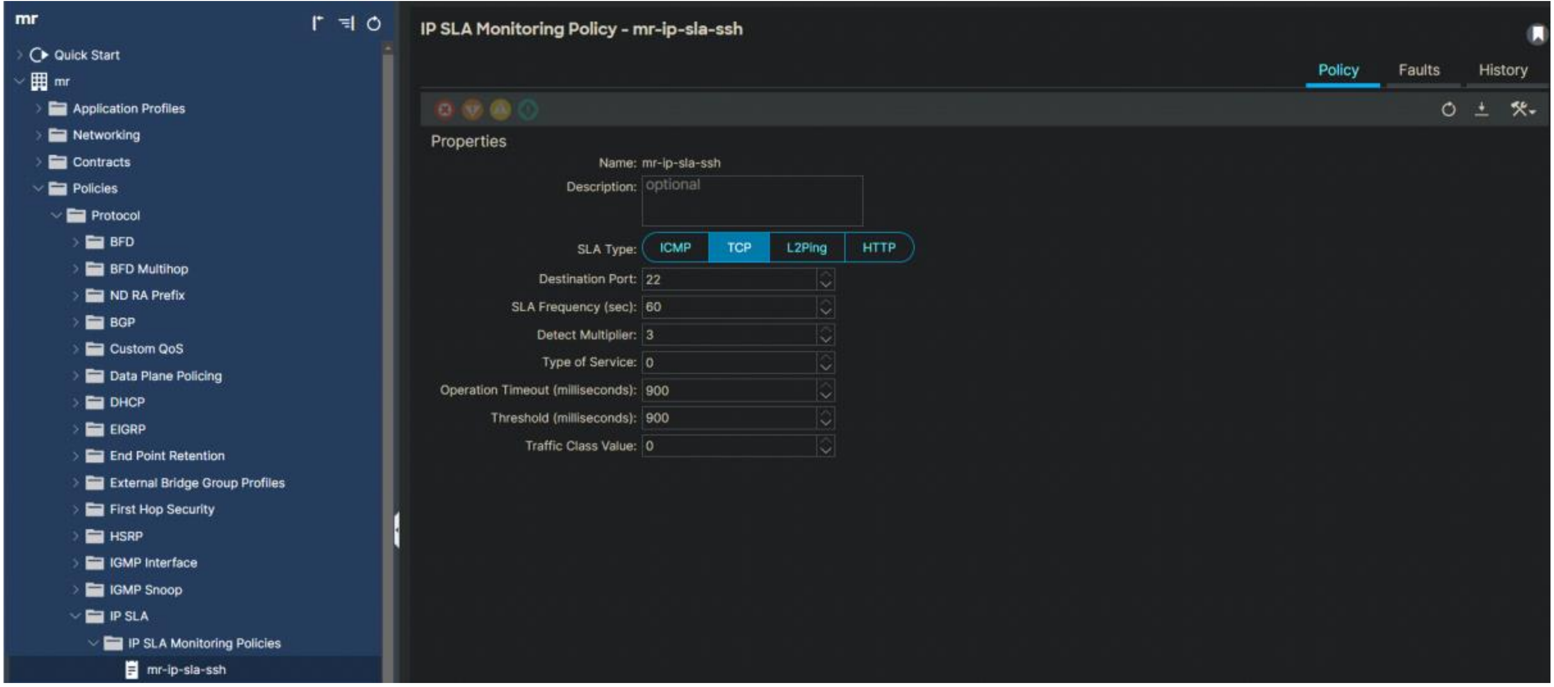
Properties

Name: provider

Filters: ssh

Next, create an IPA SLA monitoring policy. For exact steps, please refer to the Configuring an IP SLA Monitoring Policy Using the GUI section in the networking configuration guide (https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/6x/l3-configuration/cisco-apic-layer-3-networking-configuration-guide-60x/apic-ip-slas-layer3-config-60x.html#task_t41_ffd_q1b).

IP SLA monitoring policy



IP SLA Monitoring Policy - mr-ip-sla-ssh

Properties

Name: mr-ip-sla-ssh

Description: optional

SLA Type: ICMP [✓ TCP] L2Ping HTTP

Destination Port: 22

SLA Frequency (sec): 60

Detect Multiplier: 3

Type of Service: 0

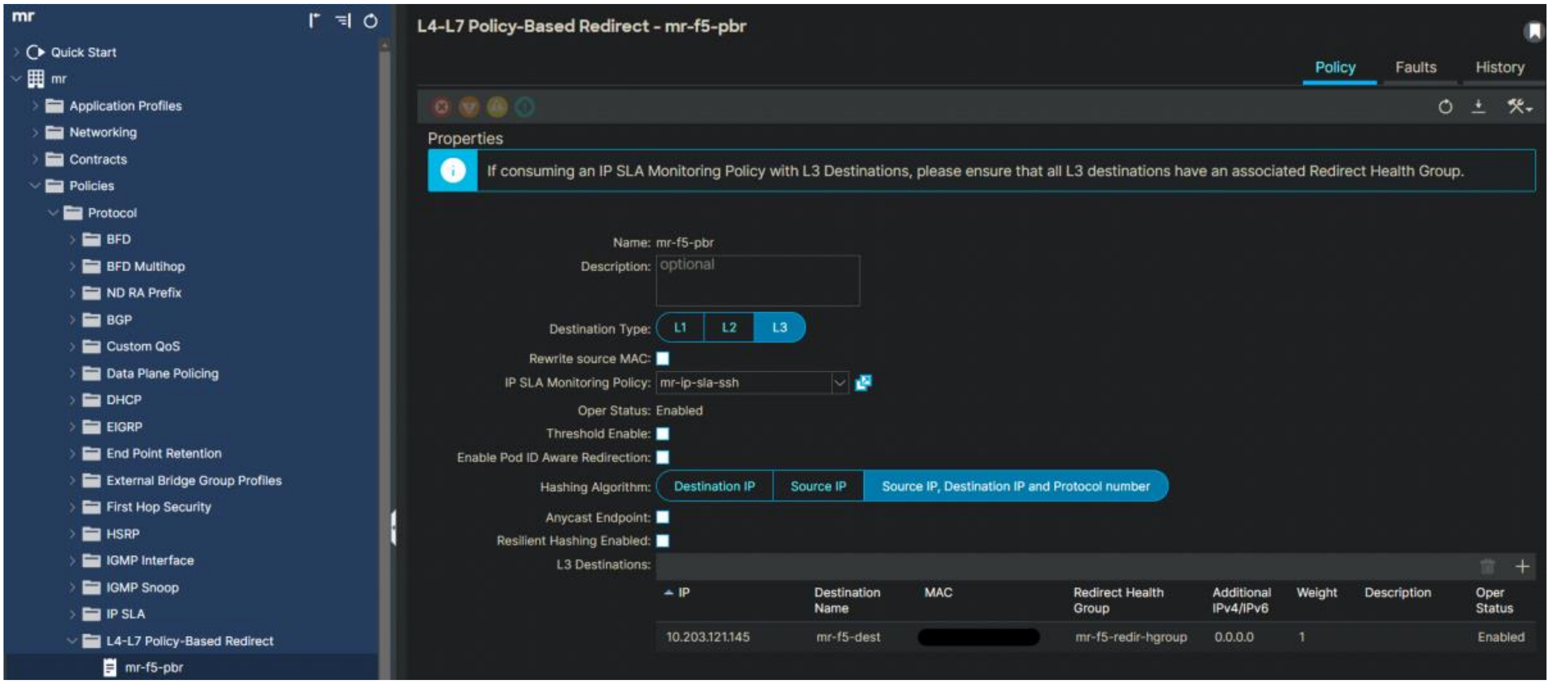
Operation Timeout (milliseconds): 900

Threshold (milliseconds): 900

Traffic Class Value: 0

Next, create a PBR policy. For exact steps, please refer to the Configuring Policy -Based Redirect Using the GUI section in the deployment guide (https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/5x/layer-4-to-layer-7-services-configuration/cisco-apic-layer-4-to-layer-7-services-deployment-guide-53x/configuring-policy-based-redirect-53x.html#id_27316). Associate the previously created IP SLA monitoring policy to the PBR policy. Also, create a redirect health group and associate it to the PBR policy. For exact steps, please refer to the Configuring a Redirect Health Group Using the GUI section in the deployment guide (https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/5x/layer-4-to-layer-7-services-configuration/cisco-apic-layer-4-to-layer-7-services-deployment-guide-53x/configuring-policy-based-redirect-53x.html#task_t41_ffd_q1b).

PBR policy



L4-L7 Policy-Based Redirect - mr-f5-pbr

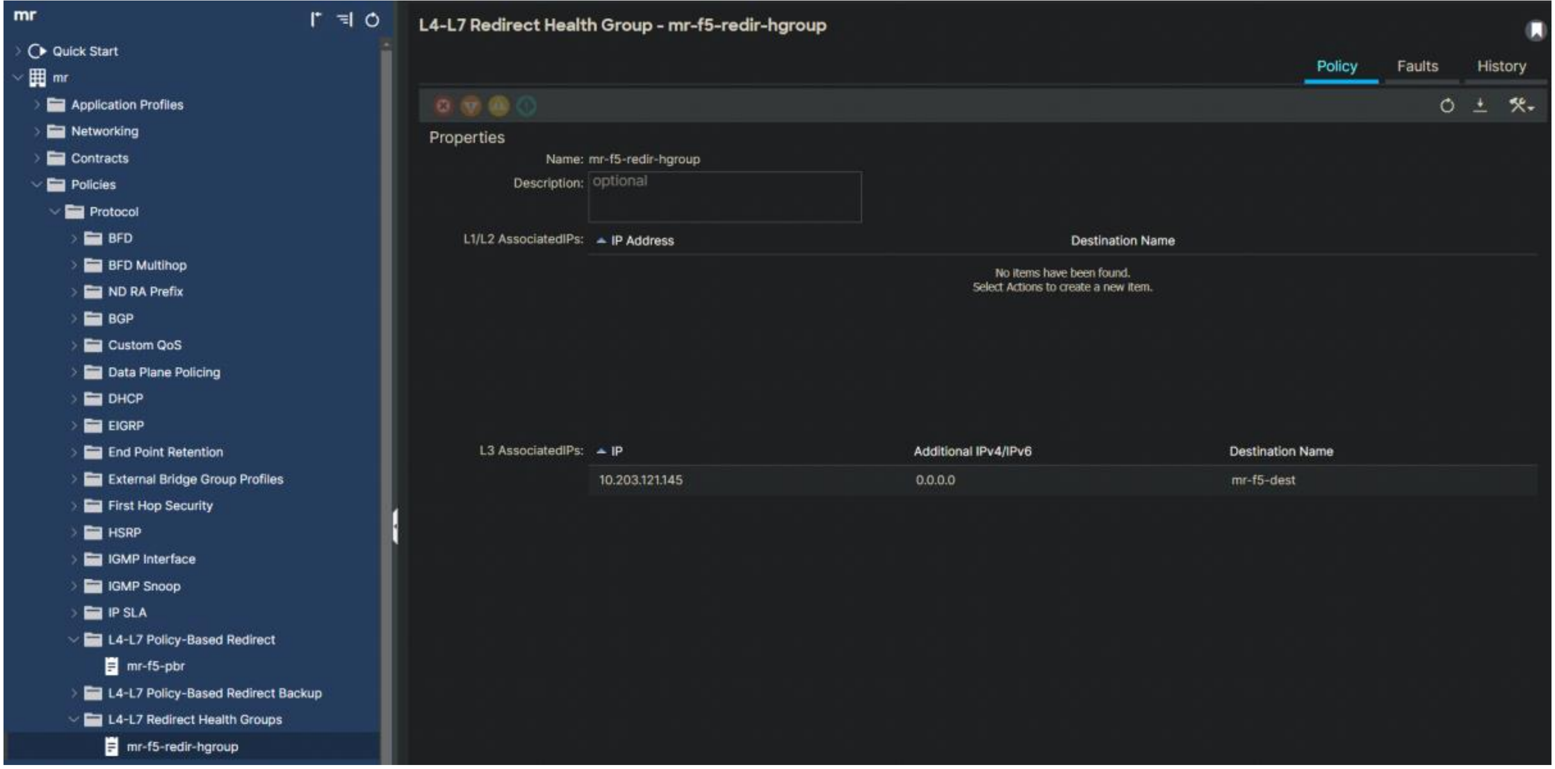
Properties

If consuming an IP SLA Monitoring Policy with L3 Destinations, please ensure that all L3 destinations have an associated Redirect Health Group.

Name: mr-f5-pbr
Description: optional
Destination Type: L1 L2 [✓ L3]
Rewrite source MAC: □
IP SLA Monitoring Policy: mr-ip-sla-ssh
Oper Status: Enabled
Threshold Enable: □
Enable Pod ID Aware Redirection: □
Hashing Algorithm: Destination IP Source IP [✓ Source IP, Destination IP and Protocol number]
Anycast Endpoint: □
Resilient Hashing Enabled: □
L3 Destinations:

IP	Destination Name	MAC	Redirect Health Group	Additional IPv4/IPv6	Weight	Description	Oper Status
10.203.121.145	mr-f5-dest	[redacted]	mr-f5-redir-hgroup	0.0.0.0	1		Enabled

Redirect health group policy



L4-L7 Redirect Health Group - mr-f5-redir-hgroup

Properties

Name: mr-f5-redir-hgroup
Description: optional

L1/L2 AssociatedIPs:

IP Address	Destination Name

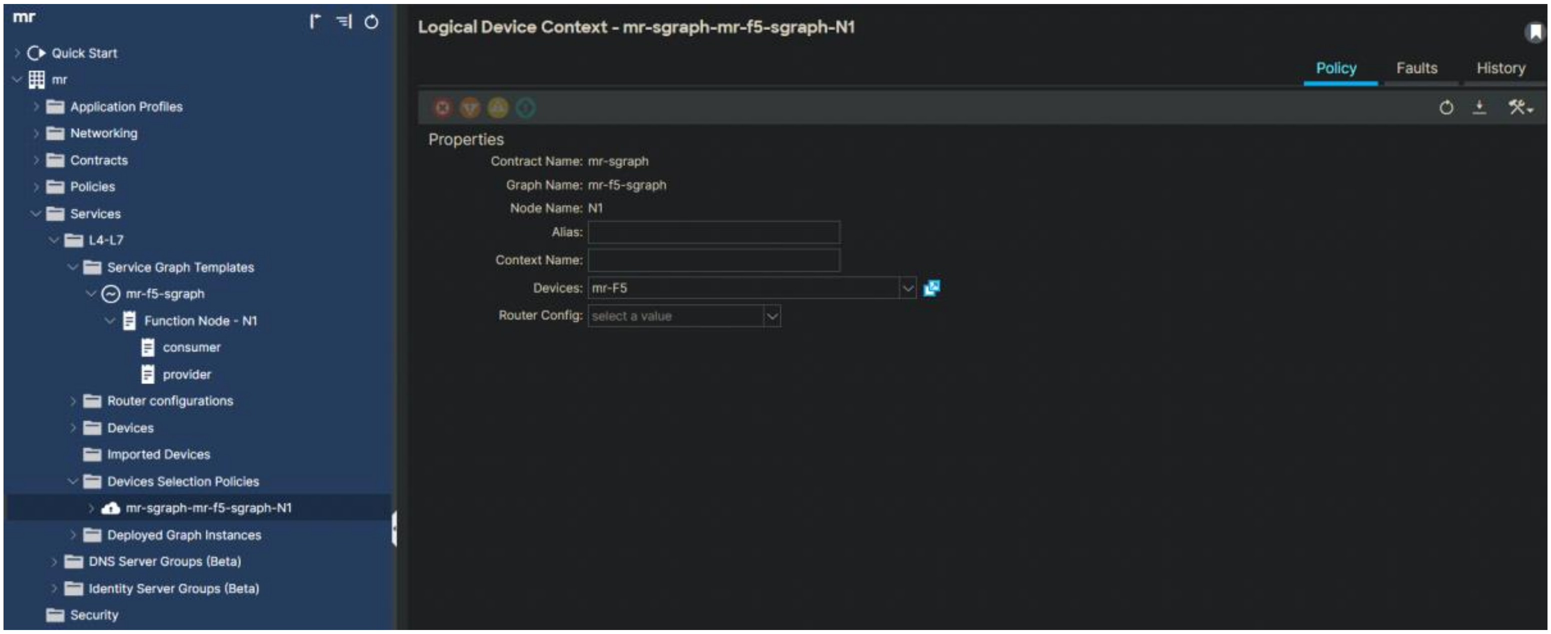
No items have been found.
Select Actions to create a new item.

L3 AssociatedIPs:

IP	Additional IPv4/IPv6	Destination Name
10.203.121.145	0.0.0.0	mr-f5-dest

Next, create a device selection policy. For exact steps, please refer to the Creating a Device Selection Policy Using the GUI section in the deployment guide (https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/5x/layer-4-to-layer-7-services-configuration/cisco-apic-layer-4-to-layer-7-services-deployment-guide-53x/selecting-a-layer-4-to-layer-7-device-to-render-a-graph-53x.html#task_F2BFF7545D9142EFB208C10F5DFBB1B4).

Device selection policy

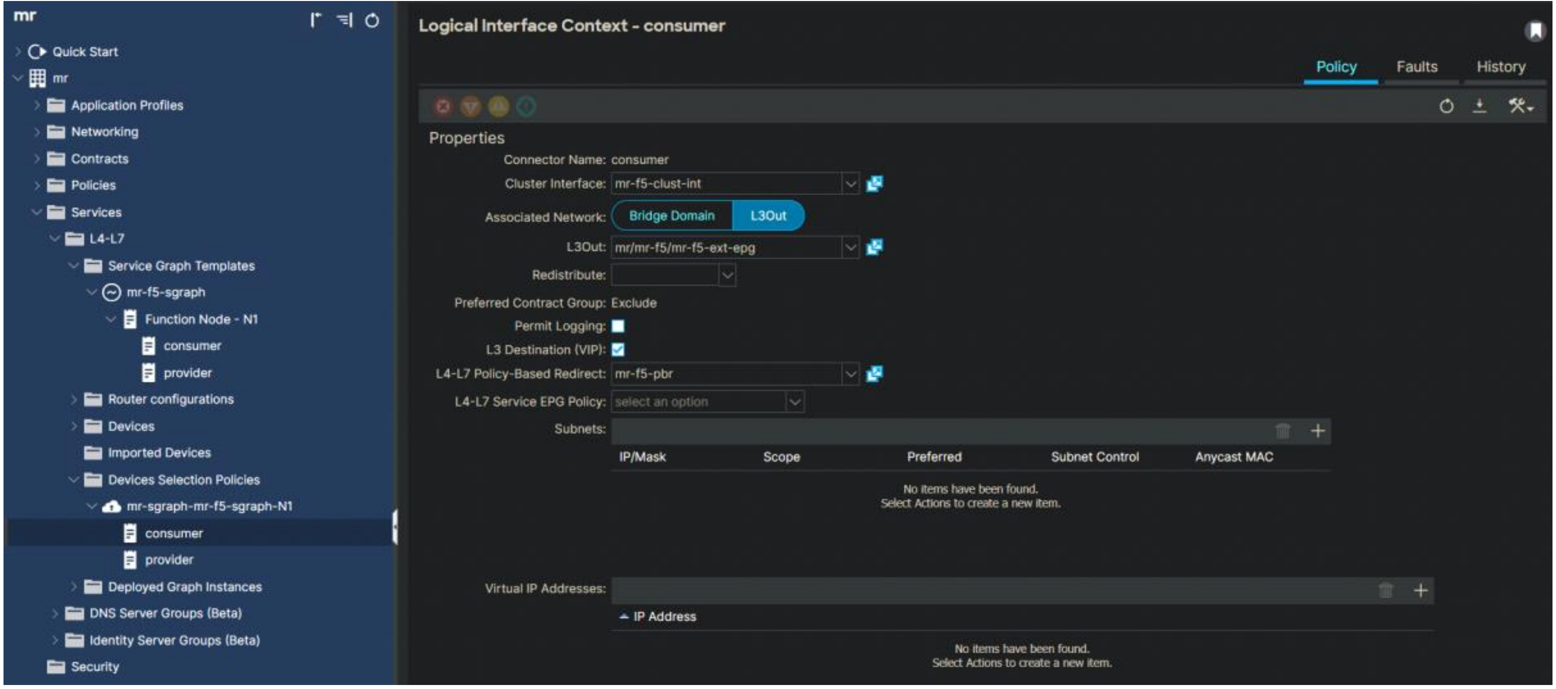


Logical Device Context - mr-sgraph-mr-f5-sgraph-N1

Properties

Contract Name: mr-sgraph
Graph Name: mr-f5-sgraph
Node Name: N1
Alias:
Context Name:
Devices: mr-F5
Router Config: select a value

Device selection consumer policy



Logical Interface Context - consumer

Properties

Connector Name: consumer
Cluster Interface: mr-f5-clust-int
Associated Network: Bridge Domain [✓ L3Out]
L3Out: mr/mr-f5/mr-f5-ext-epg
Redistribute:
Preferred Contract Group: Exclude
Permit Logging: □
L3 Destination (VIP): ☑
L4-L7 Policy-Based Redirect: mr-f5-pbr
L4-L7 Service EPG Policy: select an option
Subnets:

IP/Mask	Scope	Preferred	Subnet Control	Anycast MAC

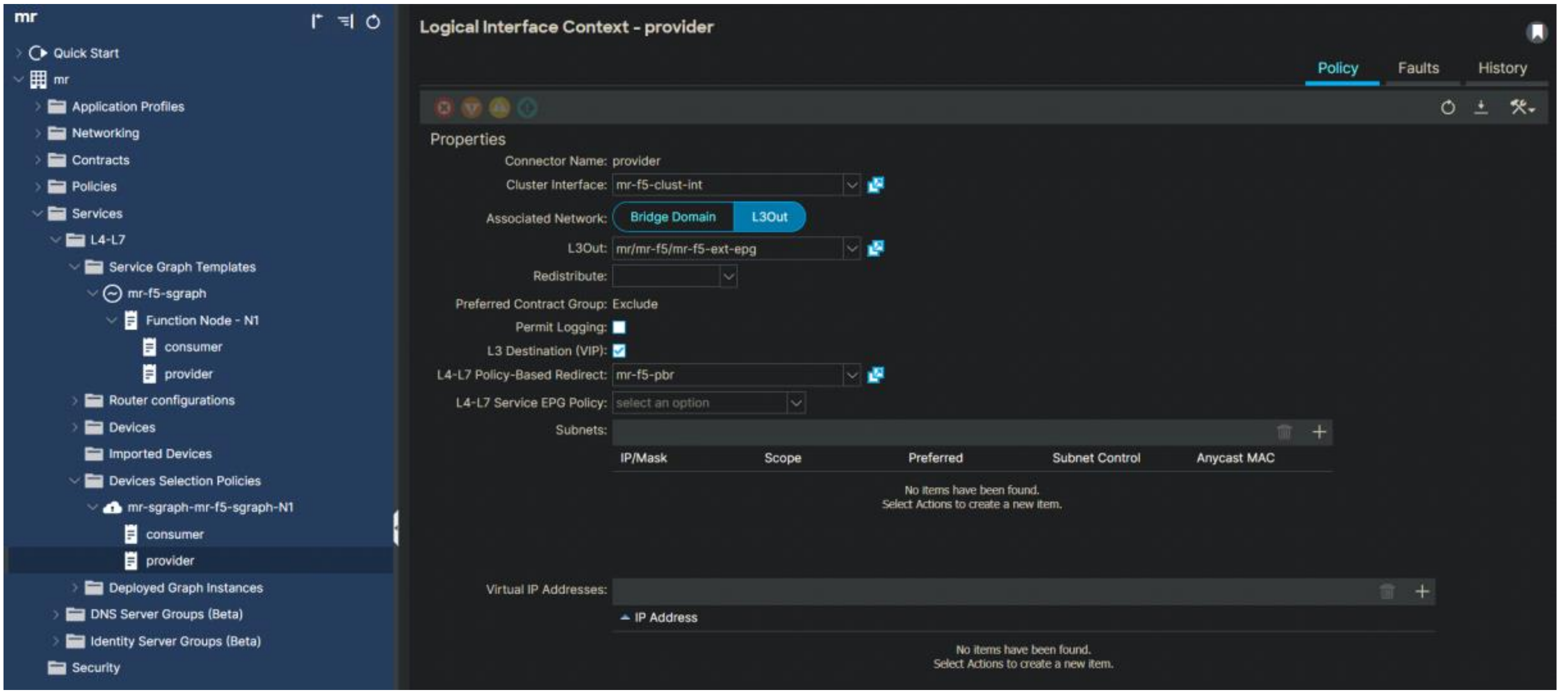
No items have been found.
Select Actions to create a new item.

Virtual IP Addresses:

IP Address

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

Device selection provider policy



Logical Interface Context - provider

Properties

Connector Name: provider
Cluster Interface: mr-f5-clust-int
Associated Network: Bridge Domain [✓ L3Out]
L3Out: mr/mr-f5/mr-f5-ext-epg
Redistribute:
Preferred Contract Group: Exclude
Permit Logging: □
L3 Destination (VIP): ☑
L4-L7 Policy-Based Redirect: mr-f5-pbr
L4-L7 Service EPG Policy: select an option
Subnets:

IP/Mask	Scope	Preferred	Subnet Control	Anycast MAC

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

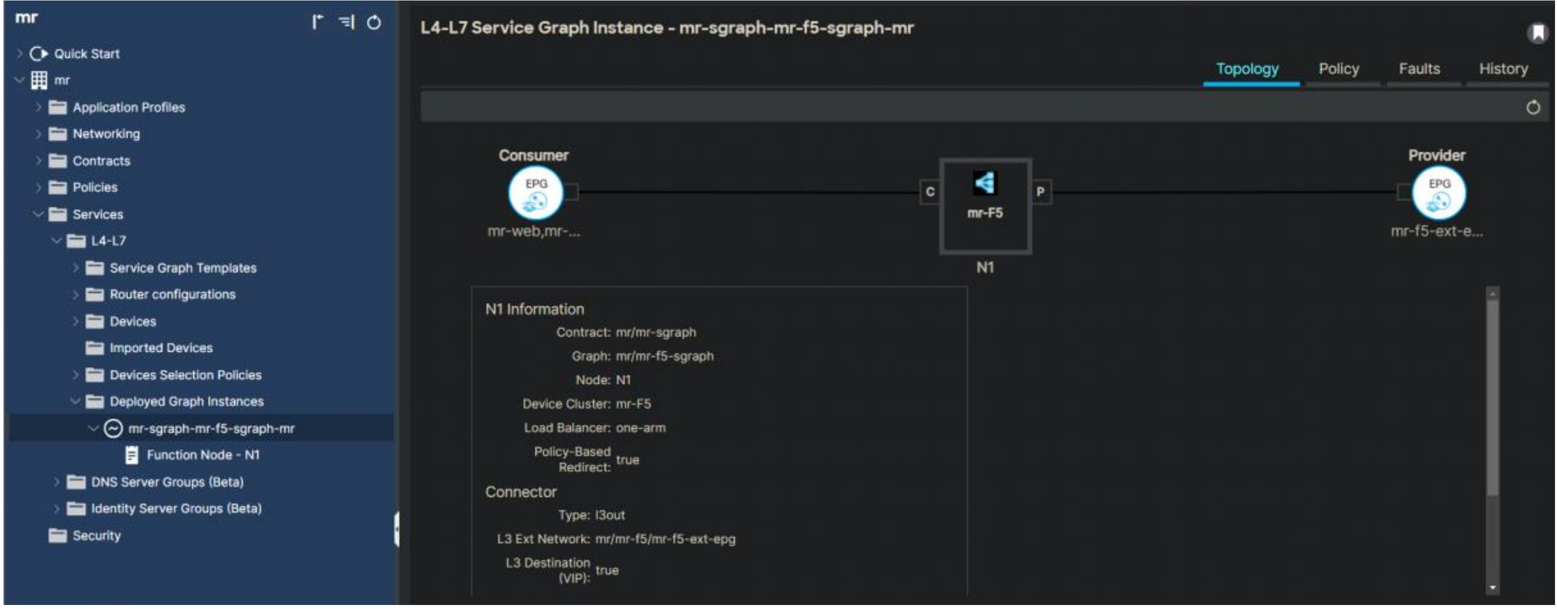
Virtual IP Addresses:

IP Address

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

Finally, apply the service graph. For exact steps, please refer to the Applying a Service Graph Template to Endpoint Groups Using the GUI section in the deployment guide (https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/5x/layer-4-to-layer-7-services-configuration/cisco-apic-layer-4-to-layer-7-services-deployment-guide-53x/configuring-a-service-graph-53x.html#task_1F0C0E9CEBF94D5982ECEEF8AB0CF796).

Deployed graph instance topology



L4-L7 Service Graph Instance - mr-sgraph-mr-f5-sgraph-mr

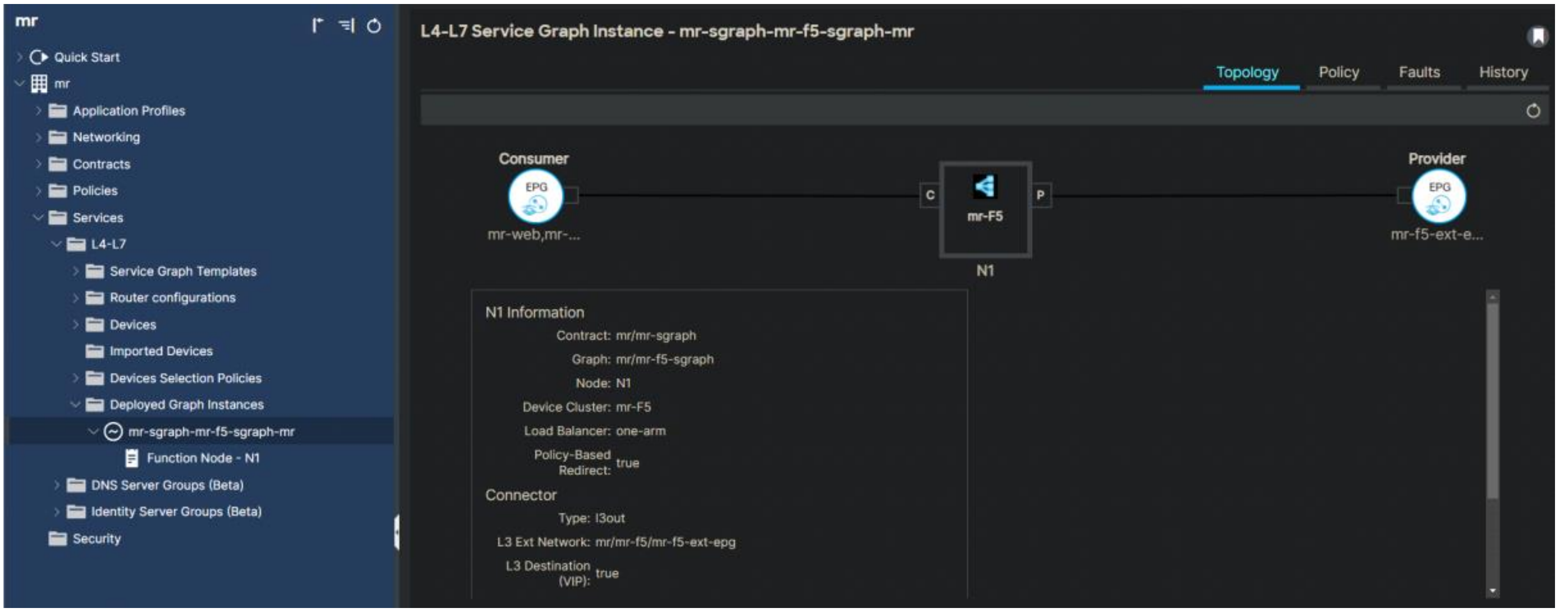
N1 Information

Contract: mr/mr-sgraph
Graph: mr/mr-f5-sgraph
Node: N1
Device Cluster: mr-F5
Load Balancer: one-arm
Policy-Based Redirect: true

Connector

Type: l3out
L3 Ext Network: mr/mr-f5/mr-f5-ext-epg
L3 Destination (VIP): true

Deployed graph instance policy



L4-L7 Service Graph Instance - mr-sgraph-mr-f5-sgraph-mr

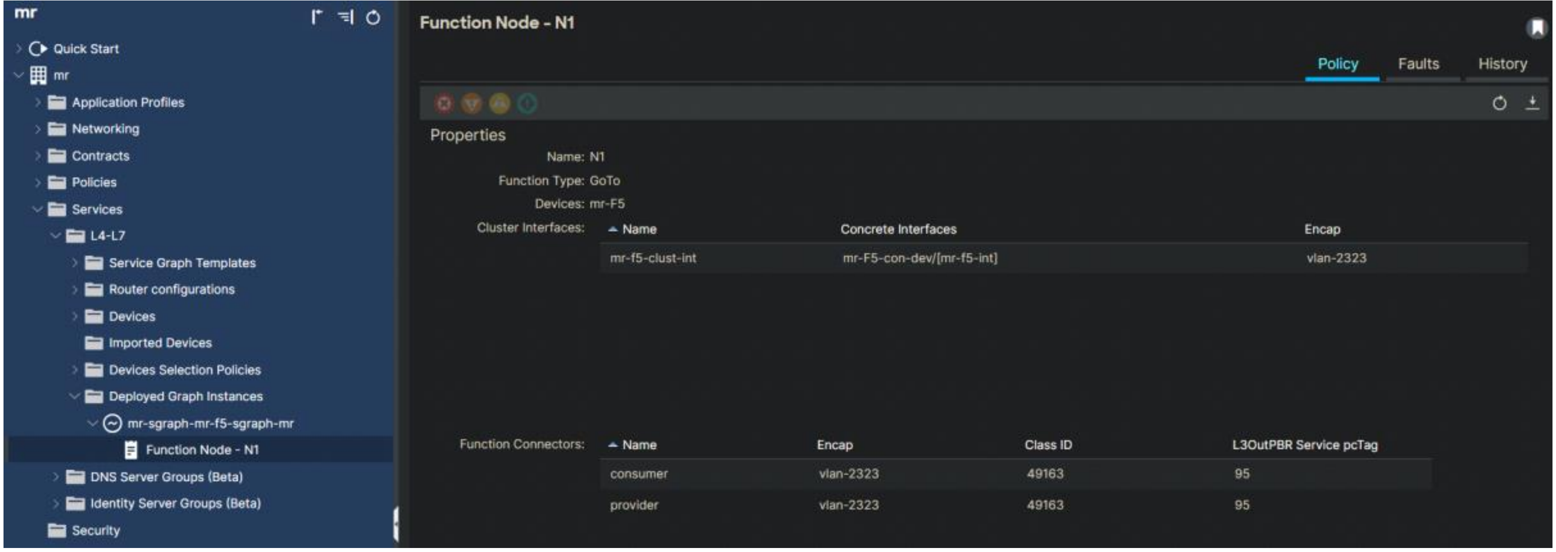
N1 Information

Contract: mr/mr-sgraph
Graph: mr/mr-f5-sgraph
Node: N1
Device Cluster: mr-F5
Load Balancer: one-arm
Policy-Based Redirect: true

Connector

Type: l3out
L3 Ext Network: mr/mr-f5/mr-f5-ext-epg
L3 Destination (VIP): true

Deployed function node



Function Node - N1

Properties

Name: N1
Function Type: GoTo
Devices: mr-F5
Cluster Interfaces:

Name	Concrete Interfaces	Encap
mr-f5-clust-int	mr-F5-con-dev/[mr-f5-int]	vlan-2323

Function Connectors:

Name	Encap	Class ID	L3OutPBR Service pcTag
consumer	vlan-2323	49163	95
provider	vlan-2323	49163	95

Testing

We will now test connectivity from VM-1 to VM-2 over port 22 (SSH). Using ELAMs we will verify that SSH traffic is being redirected to the F5 service device that resides outside of the fabric via an L3Out. We will also ensure that only SSH traffic is allowed between VM-1 and VM-2 (testing with both SSH and ICMP). Finally, we will ensure that all traffic is allowed from VM-1 and VM-2 to the WAN (again, testing with both SSH and ICMP).

Before we begin, I have provided JSON output of my internal EPGs and external (L3Out) EPGs, as well as the contracts that are associated to them.

EPG mr-web:

```
{
  "totalCount": "1",
  "imdata": [
    {
      "fvAEPg": {
        "attributes": {
          "annotation": "",
          "descr": "",
          "dn": "uni/tn-mr/ap-mr-ap/epg-mr-web",
          "exceptionTag": "",
          "floodOnEncap": "disabled",
          "fwdCtrl": "",
          "hasMcastSource": "no",
          "isAttrBasedEPg": "no",
          "matchT": "AtleastOne",
          "name": "mr-web",
          "nameAlias": "",
          "pcEnfPref": "unenforced",
          "prefGrMemb": "exclude",
          "prio": "level3",
          "shutdown": "no",
          "userdom": "all"
        },
        "children": [
          {
            "fvRsPathAtt": {
              "attributes": {
                "annotation": "",
                "descr": "",
                "encap": "vlan-2310",
                "instrImedcy": "lazy",
                "mode": "regular",
                "primaryEncap": "unknown",
                "tDn": "topology/pod-2/paths-201/pathep-[eth1/44]",
                "userdom": ":all:"
              }
            }
          },
                    {
                        "fvRsDomAtt": {
                            "attributes": {
                                "annotation": "",
                                "apiMode": "mgmt",
                                "bindingType": "none",
                                "classPref": "encap",
                                "customEpgName": "",
                                "delimiter": "",
                                "encap": "unknown",
                                "encapMode": "auto",
                                "epgCos": "Cos0",
                                "epgCosPref": "disabled",
                                "instrImedcy": "lazy",
                                "ipamDhcpOverride": "0.0.0.0",
                                "ipamEnabled": "no",
                                "ipamGateway": "0.0.0.0",
                                "lagPolicyName": "",
                                "netflowDir": "both",
                                "netflowPref": "disabled",
                                "numPorts": "0",
                                "portAllocation": "none",
                                "primaryEncap": "unknown",
                                "primaryEncapInner": "unknown",
                                "resImedcy": "immediate",
                                "secondaryEncapInner": "unknown",
                                "switchingMode": "native",
                                "tDn": "uni/phys-mr-phys",
                                "untagged": "no",
                                "userdom": "all",
                                "vnetOnly": "no"
                            }
                        }
                    },
                    {
                        "fvRsCons": {
                            "attributes": {
                                "annotation": "",
                                "intent": "install",
                                "prio": "unspecified",
                                "tnVzBrCPName": "mr-sgraph",
                                "userdom": ":all:"
                            }
                        }
                    },
                    {
                        "fvRsCons": {
                            "attributes": {
                                "annotation": "",
                                "intent": "install",
                                "prio": "unspecified",
                                "tnVzBrCPName": "Test",
                                "userdom": ":all:"
                            }
                        }
                    },
                    {
                        "fvRsCustQosPol": {
                            "attributes": {
                                "annotation": "",
                                "tnQosCustomPolName": "",
                                "userdom": "all"
                            }
                        }
                    },
                    {
                        "fvRsBd": {
                            "attributes": {
                                "annotation": "",
                                "tnFvBDName": "mr-company",
                                "userdom": "all"
                            }
                        }
                    }
                ]
            }
        }
    ]
}
```

EPG mr-vm:

```
{
    "totalCount": "1",
    "imdata": [
        {
            "fvAEPg": {
                "attributes": {
                    "annotation": "",
                    "descr": "",
                    "dn": "uni/tn-mr/ap-mr-ap/epg-mr-vm",
                    "exceptionTag": "",
                    "floodOnEncap": "disabled",
                    "fwdCtrl": "",
                    "hasMcastSource": "no",
                    "isAttrBasedEPg": "no",
                    "matchT": "AtleastOne",
                    "name": "mr-vm",
                    "nameAlias": "",
                    "pcEnfPref": "unenforced",
                    "prefGrMemb": "exclude",
                    "prio": "level3",
                    "shutdown": "no",
                    "userdom": "all"
                },
                "children": [
                    {
                        "fvRsProv": {
                            "attributes": {
                                "annotation": "",
                                "intent": "install",
                                "matchT": "AtleastOne",
                                "prio": "unspecified",
                                "tnVzBrCPName": "mr-sgraph",
                                "userdom": ":all:"
                            }
                        }
                    },
                    {
                        "fvRsDomAtt": {
                            "attributes": {
                                "annotation": "",
                                "apiMode": "mgmt",
                                "bindingType": "staticBinding",
                                "classPref": "encap",
                                "customEpgName": "",
                                "delimiter": "",
                                "encap": "vlan-2317",
                                "encapMode": "auto",
                                "epgCos": "Cos0",
                                "epgCosPref": "disabled",
                                "instrImedcy": "lazy",
                                "ipamDhcpOverride": "0.0.0.0",
                                "ipamEnabled": "no",
                                "ipamGateway": "0.0.0.0",
                                "lagPolicyName": "",
                                "netflowDir": "both",
                                "netflowPref": "disabled",
                                "numPorts": "0",
                                "portAllocation": "elastic",
                                "primaryEncap": "unknown",
                                "primaryEncapInner": "unknown",
                                "resImedcy": "pre-provision",
                                "secondaryEncapInner": "unknown",
                                "switchingMode": "native",
                                "tDn": "uni/vmmp-VMware/dom-mr-dvs",
                                "untagged": "no",
                                "userdom": ":all:",
                                "vnetOnly": "no"
                            },
                            "children": [
                                {
                                    "vmmSecP": {
                                        "attributes": {
                                            "allowPromiscuous": "reject",
                                            "annotation": "",
                                            "descr": "",
                                            "forgedTransmits": "reject",
                                            "macChanges": "reject",
                                            "name": "",
                                            "nameAlias": "",
                                            "ownerKey": "",
                                            "ownerTag": "",
                                            "userdom": ":all:"
                                        }
                                    }
                                }
                            ]
                        }
                    },
                    {
                        "fvRsCons": {
                            "attributes": {
                                "annotation": "",
                                "intent": "install",
                                "prio": "unspecified",
                                "tnVzBrCPName": "Test",
                                "userdom": ":all:"
                            }
                        }
                    },
                    {
                        "fvRsCustQosPol": {
                            "attributes": {
                                "annotation": "",
                                "tnQosCustomPolName": "",
                                "userdom": "all"
                            }
                        }
                    },
                    {
                        "fvRsBd": {
                            "attributes": {
                                "annotation": "",
                                "tnFvBDName": "mr-vm",
                                "userdom": "all"
                            }
                        }
                    }
                ]
            }
        }
    ]
}
```

L3Out EPG mr-f5-ext-epg:

```
{
    "totalCount": "1",
    "imdata": [
        {
            "l3extInstP": {
                "attributes": {
                    "annotation": "",
                    "descr": "",
                    "dn": "uni/tn-mr/out-mr-f5/instP-mr-f5-ext-epg",
                    "exceptionTag": "",
                    "floodOnEncap": "disabled",
                    "matchT": "AtleastOne",
                    "name": "mr-f5-ext-epg",
                    "nameAlias": "",
                    "pcEnfPref": "unenforced",
                    "prefGrMemb": "exclude",
                    "prio": "unspecified",
                    "targetDscp": "unspecified",
                    "userdom": ":all:"
                },
                "children": [
                    {
                        "fvRsProv": {
                            "attributes": {
                                "annotation": "",
                                "intent": "install",
                                "matchT": "AtleastOne",
                                "prio": "unspecified",
                                "tnVzBrCPName": "mr-sgraph",
                                "userdom": ":all:"
                            }
                        }
                    },
                    {
                        "l3extSubnet": {
                            "attributes": {
                                "aggregate": "",
                                "annotation": "",
                                "descr": "",
                                "ip": "10.203.121.0/24",
                                "name": "",
                                "nameAlias": "",
                                "scope": "import-security",
                                "userdom": ":all:"
                            }
                        }
                    },
                    {
                        "fvRsCustQosPol": {
                            "attributes": {
                                "annotation": "",
                                "tnQosCustomPolName": "",
                                "userdom": ":all:"
                            }
                        }
                    },
                    {
                        "fvRsCons": {
                            "attributes": {
                                "annotation": "",
                                "intent": "install",
                                "prio": "unspecified",
                                "tnVzBrCPName": "mr-sgraph",
                                "userdom": ":all:"
                            }
                        }
                    }
                ]
            }
        }
    ]
}
```

L3Out EPG mr-WAN-ext-epg:

```
{
    "totalCount": "1",
    "imdata": [
        {
            "l3extInstP": {
                "attributes": {
                    "annotation": "",
                    "descr": "",
                    "dn": "uni/tn-mr/out-mr-WAN/instP-mr-WAN-ext-epg",
                    "exceptionTag": "",
                    "floodOnEncap": "disabled",
                    "matchT": "AtleastOne",
                    "name": "mr-WAN-ext-epg",
                    "nameAlias": "",
                    "pcEnfPref": "unenforced",
                    "prefGrMemb": "exclude",
                    "prio": "unspecified",
                    "targetDscp": "unspecified",
                    "userdom": ":all:"
                },
                "children": [
                    {
                        "fvRsProv": {
                            "attributes": {
                                "annotation": "",
                                "intent": "install",
                                "matchT": "AtleastOne",
                                "prio": "unspecified",
                                "tnVzBrCPName": "Test",
                                "userdom": ":all:"
                            }
                        }
                    },
                    {
                        "l3extSubnet": {
                            "attributes": {
                                "aggregate": "",
                                "annotation": "",
                                "descr": "",
                                "ip": "0.0.0.0/0",
                                "name": "",
                                "nameAlias": "",
                                "scope": "import-security",
                                "userdom": ":all:"
                            }
                        }
                    },
                    {
                        "fvRsCustQosPol": {
                            "attributes": {
                                "annotation": "",
                                "tnQosCustomPolName": "",
                                "userdom": ":all:"
                            }
                        }
                    }
                ]
            }
        }
    ]
}
```

Contract mr-sgraph (this is the contract that has the service graph applied to it):

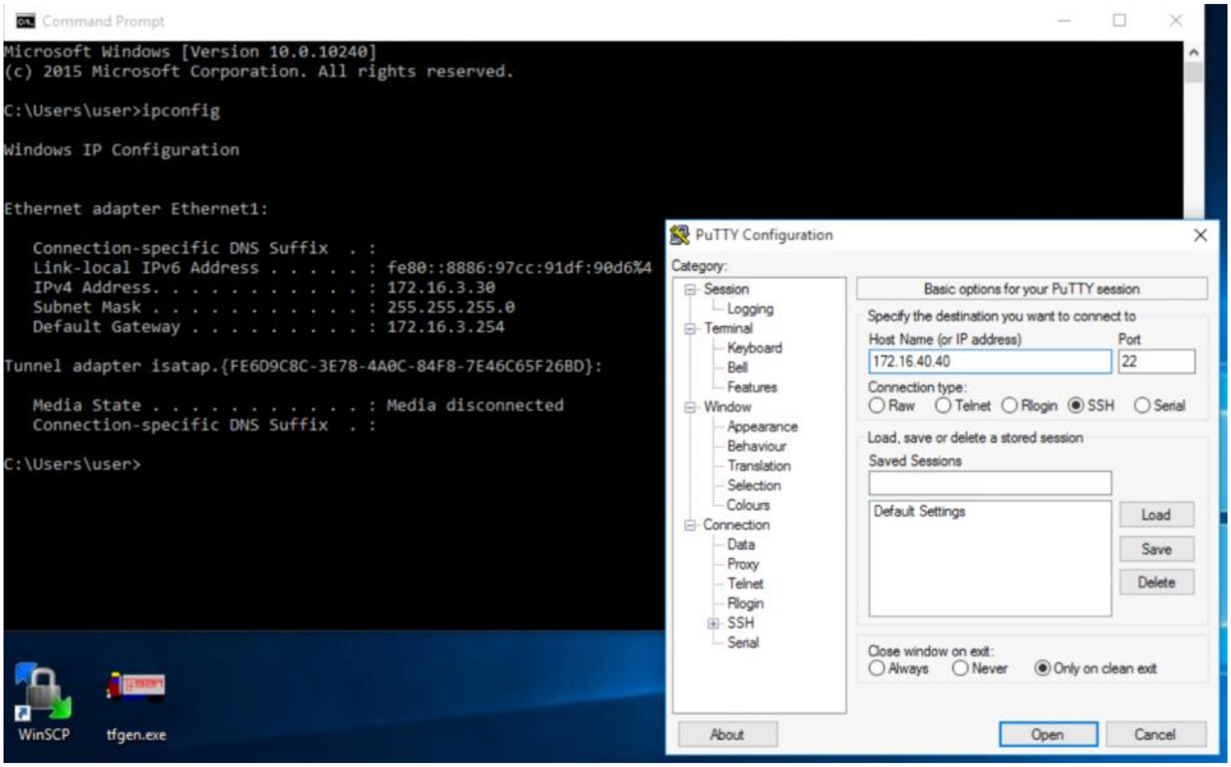
```
{
    "totalCount": "1",
    "imdata": [
        {
            "vzBrCP": {
                "attributes": {
                    "annotation": "",
                    "descr": "",
                    "dn": "uni/tn-mr/brc-mr-sgraph",
                    "intent": "install",
                    "name": "mr-sgraph",
                    "nameAlias": "",
                    "ownerKey": "",
                    "ownerTag": "",
                    "prio": "unspecified",
                    "scope": "context",
                    "targetDscp": "unspecified",
                    "userdom": ":all:"
                },
                "children": [
                    {
                        "vzSubj": {
                            "attributes": {
                                "annotation": "",
                                "consMatchT": "AtleastOne",
                                "descr": "",
                                "name": "mr-sgraph-subj",
                                "nameAlias": "",
                                "prio": "unspecified",
                                "provMatchT": "AtleastOne",
                                "revFltPorts": "yes",
                                "targetDscp": "unspecified",
                                "userdom": ":all:"
                            },
                            "children": [
                                {
                                    "vzRsSubjGraphAtt": {
                                        "attributes": {
                                            "annotation": "",
                                            "directives": "",
                                            "tnVnsAbsGraphName": "mr-f5-sgraph",
                                            "userdom": ":all:"
                                        }
                                    }
                                },
                                {
                                    "vzRsSubjFiltAtt": {
                                        "attributes": {
                                            "action": "permit",
                                            "annotation": "",
                                            "directives": "",
                                            "priorityOverride": "default",
                                            "tnVzFilterName": "ssh",
                                            "userdom": ":all:"
                                        }
                                    }
                                }
                            ]
                        }
                    }
                ]
            }
        }
    ]
}
```

Contract Test (this is the permit-all contract):

```
{
    "totalCount": "1",
    "imdata": [
        {
            "vzBrCP": {
                "attributes": {
                    "annotation": "",
                    "descr": "",
                    "dn": "uni/tn-mr/brc-Test",
                    "intent": "install",
                    "name": "Test",
                    "nameAlias": "",
                    "ownerKey": "",
                    "ownerTag": "",
                    "prio": "unspecified",
                    "scope": "context",
                    "targetDscp": "unspecified",
                    "userdom": ":all:"
                },
                "children": [
                    {
                        "vzSubj": {
                            "attributes": {
                                "annotation": "",
                                "consMatchT": "AtleastOne",
                                "descr": "",
                                "name": "Test",
                                "nameAlias": "",
                                "prio": "unspecified",
                                "provMatchT": "AtleastOne",
                                "revFltPorts": "yes",
                                "targetDscp": "unspecified",
                                "userdom": ":all:"
                            },
                            "children": [
                                {
                                    "vzRsSubjFiltAtt": {
                                        "attributes": {
                                            "action": "permit",
                                            "annotation": "",
                                            "directives": "",
                                            "priorityOverride": "default",
                                            "tnVzFilterName": "Permit-Any-Filter",
                                            "userdom": ":all:"
                                        }
                                    }
                                }
                            ]
                        }
                    }
                ]
            }
        }
    ]
}
```

Now, let's test SSH from VM-1 to VM-2.

SSH session from VM-1 to VM-2



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\user>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8886:97cc:91df:90d6%4
   IPv4 Address. . . . . . . . . . . : 172.16.3.30
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.3.254

Tunnel adapter isatap.{FE6D9C8C-3E78-4A0C-84F8-7E46C65F26BD}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\user>
```

PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 172.16.40.40

Port: 22

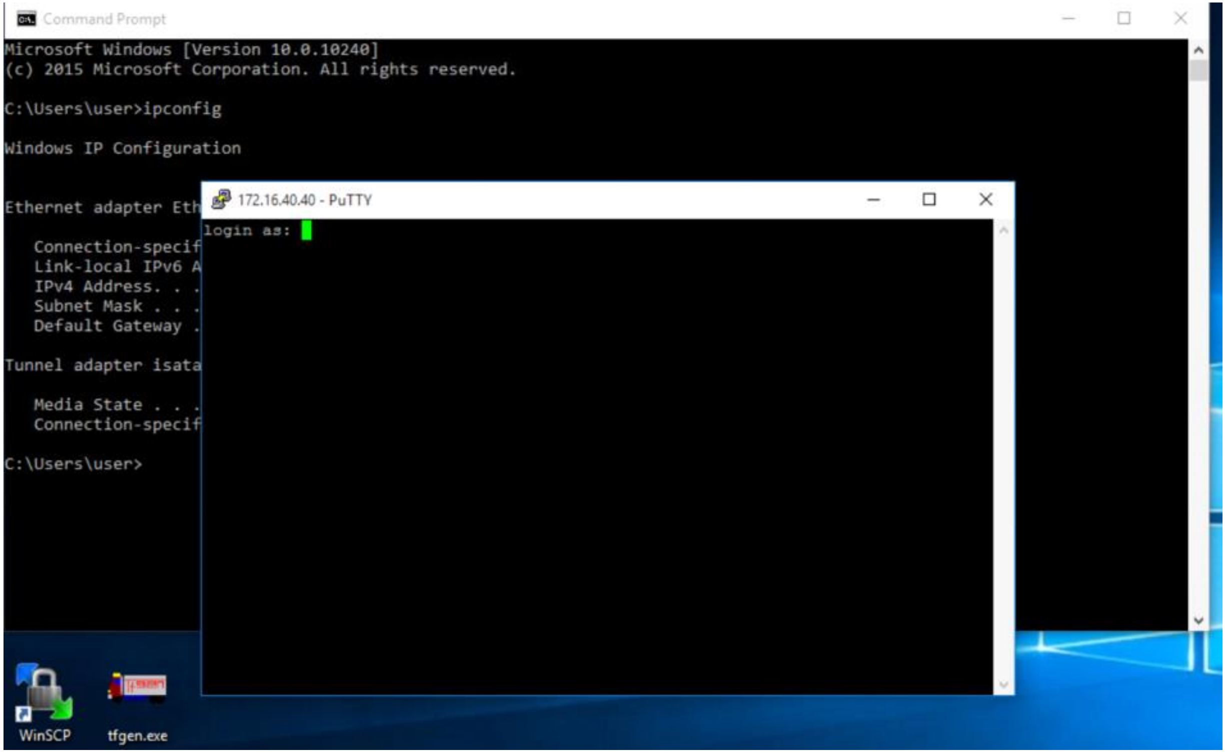
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

SSH successful



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\user>ipconfig

Windows IP Configuration


Ethernet adapter Eth

   Connection-specif
   Link-local IPv6 A
   IPv4 Address. . .
   Subnet Mask . . .
   Default Gateway .

Tunnel adapter isata

   Media State . . .
   Connection-specif

C:\Users\user>
```

172.16.40.40 - PuTTY

```
login as:
```

As shown above, the SSH traffic successfully made it from VM-1 to VM-2. But did it get redirected through the F5? Let's check with ELAMs in ACI.

CL-201:

a2-leaf1# **vsh_lc**
module-1# **debug platform internal roc elam asic 0**
module-1(DBG-elam)# **t r**
module-1(DBG-elam)# **t i i 6 o 0**
module-1(DBG-elam-insel6)# **set outer ipv4 src_ip 172.16.3.30 dst_ip 172.16.40.40**
module-1(DBG-elam-insel6)# **start**
module-1(DBG-elam-insel6)# **stat**
ELAM STATUS
===========
Asic 0 Slice 0 Status Triggered
Asic 0 Slice 1 Status Armed

module-1(DBG-elam-insel6)# **ereport**
<some output omitted below for brevity>

Outer L3 Header

```
L3 Type              : IPv4
IP Version           : 4
DSCP                 : 0
```

```
IP Packet Length            : 52 ( = IP header(28 bytes) + IP payload )
Don't Fragment Bit          : set
TTL                         : 128
IP Protocol Number          : TCP
IP CheckSum                 : 8940( 0x22EC )
Destination IP              : 172.16.40.40
Source IP                   : 172.16.3.30

------------------------------------------------------------------------------------------
Outer L4 Header
------------------------------------------------------------------------------------------
L4 Type                     : TCP
Source Port                 : 49479( 0xC147 )
Destination Port            : 22( 0x16 )
TCP/UDP CheckSum            : 0x9E3E( 0x9E3E )

------------------------------------------------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------
IP Protocol                             : TCP( 0x6 )
L4 Src Port                             : 49479( 0xC147 )
L4 Dst Port                             : 22( 0x16 )
sclass (src pcTag)                      : 16389( 0x4005 )
dclass (dst pcTag)                      : 1( 0x1 )
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             : 81903
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81903" )
```

BL-103:

```
a1-leaf3# vsh_lc
module-1# debug platform internal tah elam asic 0
module-1(DBG-elam)# t r
module-1(DBG-elam)# t i i 14 o 0
module-1(DBG-elam-insel14)# set inner ipv4 src_ip 172.16.3.30 dst_ip 172.16.40.40
module-1(DBG-elam-insel14)# start
module-1(DBG-elam-insel14)# stat
ELAM STATUS
===========
Asic 0 Slice 0 Status Armed
Asic 0 Slice 1 Status Triggered

module-1(DBG-elam-insel14)# ereport
<some output omitted below for brevity>
------------------------------------------------------------------------------------------
Outer L3 Header
------------------------------------------------------------------------------------------
L3 Type                     : IPv4
DSCP                        : 32
Don't Fragment Bit          : 0x0
TTL                         : 27
IP Protocol Number          : UDP
Destination IP              : 10.0.216.67
Source IP                   : 10.0.216.68

------------------------------------------------------------------------------------------
Inner L3 Header
------------------------------------------------------------------------------------------
L3 Type                     : IPv4
DSCP                        : 0
Don't Fragment Bit          : 0x1
TTL                         : 126
IP Protocol Number          : TCP
Destination IP              : 172.16.40.40
Source IP                   : 172.16.3.30

------------------------------------------------------------------------------------------
Outer L4 Header
------------------------------------------------------------------------------------------
L4 Type                     : iVxLAN
Don't Learn Bit             : 1
Src Policy Applied Bit      : 1
Dst Policy Applied Bit      : 1
sclass (src pcTag)          : 0x4005
VRF or BD VNID              : 2228239( 0x22000F )

------------------------------------------------------------------------------------------
Inner L4 Header
------------------------------------------------------------------------------------------
L4 Type                     : TCP
Source Port                 : 49479
Destination Port            : 22

------------------------------------------------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------
IP Protocol                             : TCP( 0x6 )
L4 Src Port                             : 49479( 0xC147 )
L4 Dst Port                             : 22( 0x16 )
sclass (src pcTag)                      : 16389( 0x4005 )
dclass (dst pcTag)                      : 0( 0x0 )
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                        : no
Contract Hit                            : no
Contract Aclqos Stats Index             : 0
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 0" )
```

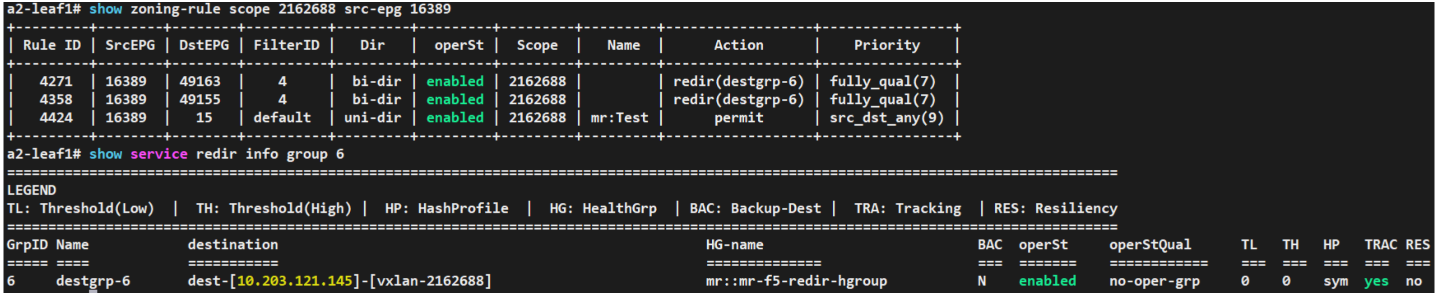
CL-102:

```
a1-leaf2# vsh_lc
module-1# debug platform internal roc elam asic 0
module-1(DBG-elam)# t r
module-1(DBG-elam)# t i i 14 o 0
module-1(DBG-elam-insel14)# set inner ipv4 src_ip 172.16.3.30 dst_ip 172.16.40.40
module-1(DBG-elam-insel14)# start
module-1(DBG-elam-insel14)# stat
ELAM STATUS
===========
Asic 0 Slice 0 Status Armed
Asic 0 Slice 1 Status Triggered
```

```
module-1(DBG-elam-insel14)# ereport
<some output omitted below for brevity>
------------------------------------------------------------------------------------------------------------
Outer L3 Header
------------------------------------------------------------------------------------------------------------
L3 Type                    : IPv4
DSCP                       : 32
Don't Fragment Bit         : 0x0
TTL                        : 29
IP Protocol Number         : UDP
Destination IP             : 10.0.216.68
Source IP                  : 10.2.168.65

------------------------------------------------------------------------------------------------------------
Inner L3 Header
------------------------------------------------------------------------------------------------------------
L3 Type                    : IPv4
DSCP                       : 0
Don't Fragment Bit         : 0x1
TTL                        : 127
IP Protocol Number         : TCP
Destination IP             : 172.16.40.40
Source IP                  : 172.16.3.30

------------------------------------------------------------------------------------------------------------
Outer L4 Header
------------------------------------------------------------------------------------------------------------
L4 Type                    : iVxLAN
Don't Learn Bit            : 0
Src Policy Applied Bit     : 0
Dst Policy Applied Bit     : 0
sclass (src pcTag)         : 0x4005
VRF or BD VNID             : 2162688( 0x210000 )

------------------------------------------------------------------------------------------------------------
Inner L4 Header
------------------------------------------------------------------------------------------------------------
L4 Type                    : TCP
Source Port                : 49479
Destination Port           : 22

------------------------------------------------------------------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------------------
IP Protocol                          : TCP( 0x6 )
L4 Src Port                          : 49479( 0xC147 )
L4 Dst Port                          : 22( 0x16 )
sclass (src pcTag)                   : 16389( 0x4005 )
dclass (dst pcTag)                   : 49155( 0xC003 )
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          : 78800
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 78800" )
```

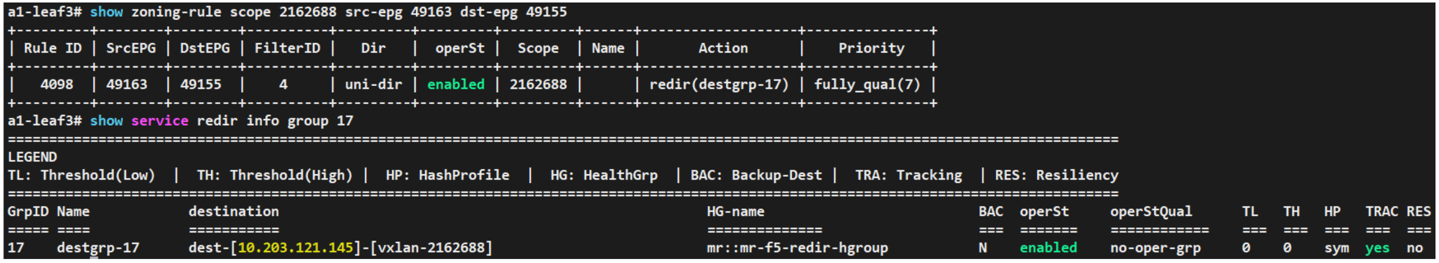
Based off the ELAM ereport output above, we can see that our SSH traffic is being redirected to the F5!
We can also quickly look for contract rules on the leaf switches by running the **show zoning-rule scope** *vrf-segment-id* **src-epg** *pctag(sclass)* **dst-epg** *pctag(dclass)* and **show service redir info group** *dst-grp* commands:

CL-201



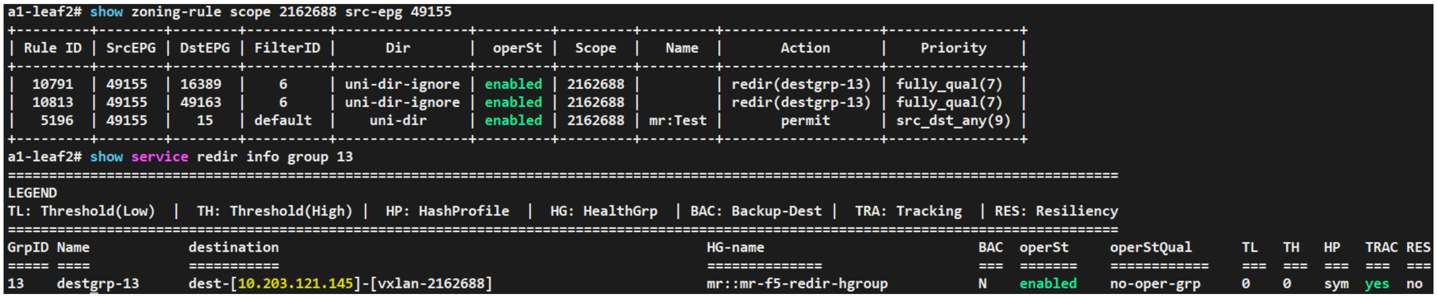
```
a2-leaf1# show zoning-rule scope 2162688 src-epg 16389
+---------+--------+--------+----------+---------+---------+---------+---------+------------------+----------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |   Name  |      Action      |    Priority    |
+---------+--------+--------+----------+---------+---------+---------+---------+------------------+----------------+
|   4271  | 16389  | 49163  |    4     |  bi-dir | enabled | 2162688 |         | redir(destgrp-6) | fully_qual(7)  |
|   4358  | 16389  | 49155  |    4     |  bi-dir | enabled | 2162688 |         | redir(destgrp-6) | fully_qual(7)  |
|   4424  | 16389  |   15   | default  | uni-dir | enabled | 2162688 | mr:Test |      permit      | src_dst_any(9) |
+---------+--------+--------+----------+---------+---------+---------+---------+------------------+----------------+
a2-leaf1# show service redir info group 6
=======================================================================================================================
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC: Backup-Dest |  TRA: Tracking  | RES: Resiliency
=======================================================================================================================
GrpID Name            destination                                       HG-name                     BAC  operSt     operStQual      TL   TH   HP   TRAC RES
===== ====            ===========                                       ==============              ===  =======    ============    ===  ===  ===  ===  ===
6     destgrp-6       dest-[10.203.121.145]-[vxlan-2162688]             mr::mr-f5-redir-hgroup      N    enabled    no-oper-grp     0    0    sym  yes  no
```

BL-103



```
a1-leaf3# show zoning-rule scope 2162688 src-epg 49163 dst-epg 49155
+---------+--------+--------+----------+---------+---------+---------+------+-------------------+---------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  | Name |       Action      |    Priority   |
+---------+--------+--------+----------+---------+---------+---------+------+-------------------+---------------+
|   4098  | 49163  | 49155  |    4     | uni-dir | enabled | 2162688 |      | redir(destgrp-17) | fully_qual(7) |
+---------+--------+--------+----------+---------+---------+---------+------+-------------------+---------------+
a1-leaf3# show service redir info group 17
=======================================================================================================================
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC: Backup-Dest |  TRA: Tracking  | RES: Resiliency
=======================================================================================================================
GrpID Name            destination                                       HG-name                     BAC  operSt     operStQual      TL   TH   HP   TRAC RES
===== ====            ===========                                       ==============              ===  =======    ============    ===  ===  ===  ===  ===
17    destgrp-17      dest-[10.203.121.145]-[vxlan-2162688]             mr::mr-f5-redir-hgroup      N    enabled    no-oper-grp     0    0    sym  yes  no
```

CL-102

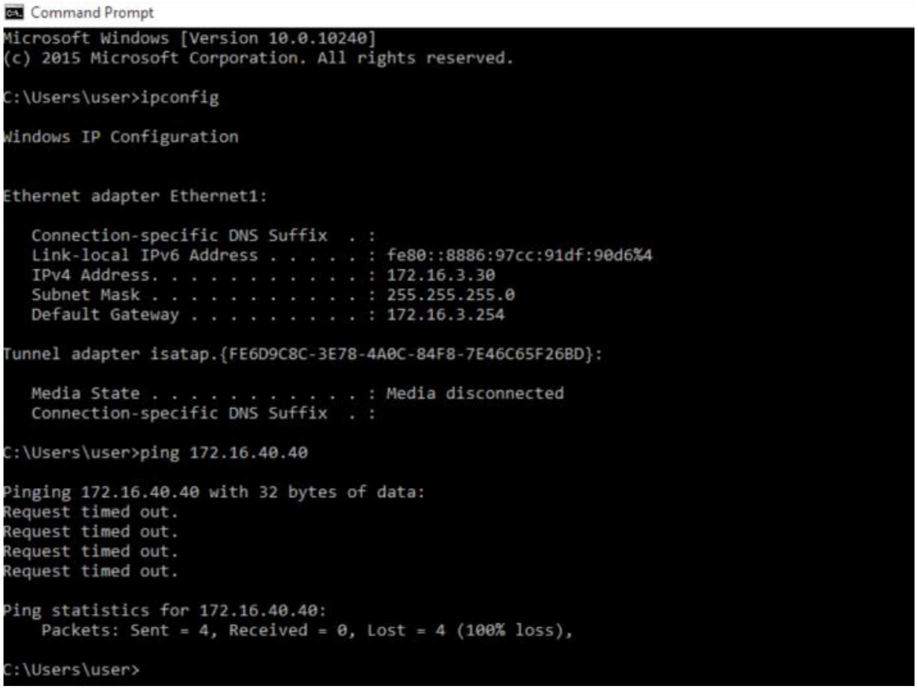


```
a1-leaf2# show zoning-rule scope 2162688 src-epg 49155
+---------+--------+--------+----------+----------------+---------+---------+---------+-------------------+----------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  |   Name  |       Action      |    Priority    |
+---------+--------+--------+----------+----------------+---------+---------+---------+-------------------+----------------+
|  10791  | 49155  | 16389  |    6     | uni-dir-ignore | enabled | 2162688 |         | redir(destgrp-13) | fully_qual(7)  |
|  10813  | 49155  | 49163  |    6     | uni-dir-ignore | enabled | 2162688 |         | redir(destgrp-13) | fully_qual(7)  |
|   5196  | 49155  |   15   | default  |    uni-dir     | enabled | 2162688 | mr:Test |       permit      | src_dst_any(9) |
+---------+--------+--------+----------+----------------+---------+---------+---------+-------------------+----------------+
a1-leaf2# show service redir info group 13
=======================================================================================================================================
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC: Backup-Dest |  TRA: Tracking  | RES: Resiliency
=======================================================================================================================================
GrpID Name            destination                                                HG-name                         BAC  operSt      operStQual      TL   TH   HP   TRAC RES
===== ====            ===========                                                ==============                  ===  =======     ============    ===  ===  ===  ===  ===
13    destgrp-13      dest-[10.203.121.145]-[vxlan-2162688]                      mr::mr-f5-redir-hgroup          N    enabled     no-oper-grp     0    0    sym  yes  no
```

***Note:** The VRF segment ID and the EPG pcTags can be found in the GUI at Tenants --> *your-tenant* --> Tenant --> Operational --> Resource IDs.

Next, let's test sending ICMP traffic from VM-1 to VM-2. It should *not* work.

Unsuccessful ping from VM-1 to VM-2

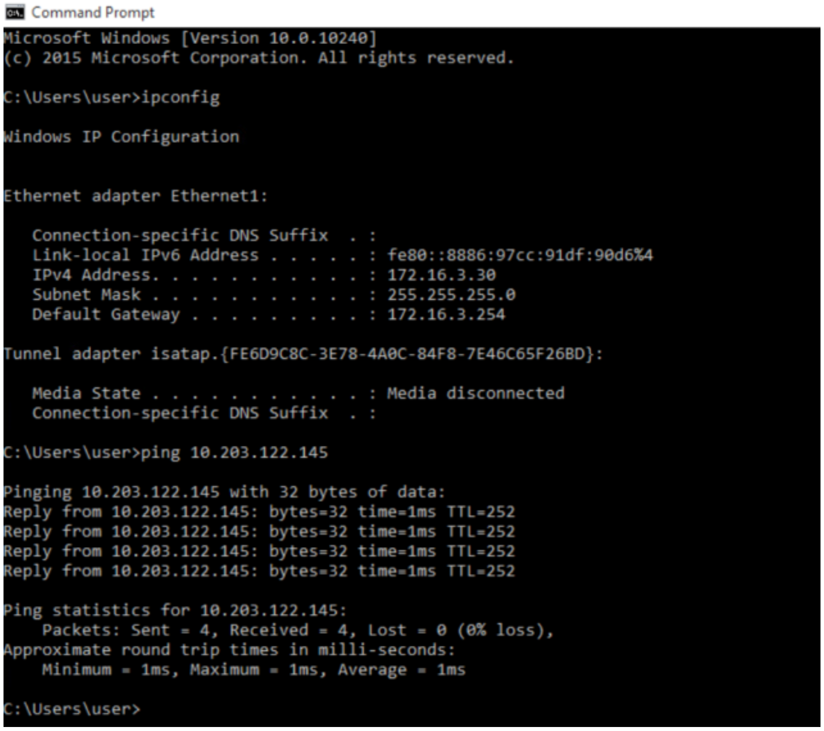


```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\user>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8886:97cc:91df:90d6%4
   IPv4 Address. . . . . . . . . . . : 172.16.3.30
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.3.254

Tunnel adapter isatap.{FE6D9C8C-3E78-4A0C-84F8-7E46C65F26BD}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\user>ping 172.16.40.40

Pinging 172.16.40.40 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.40.40:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\user>
```

The unsuccessful pings here are exactly what we want to see, since only SSH traffic should be allowed between VM-1 and VM-2.

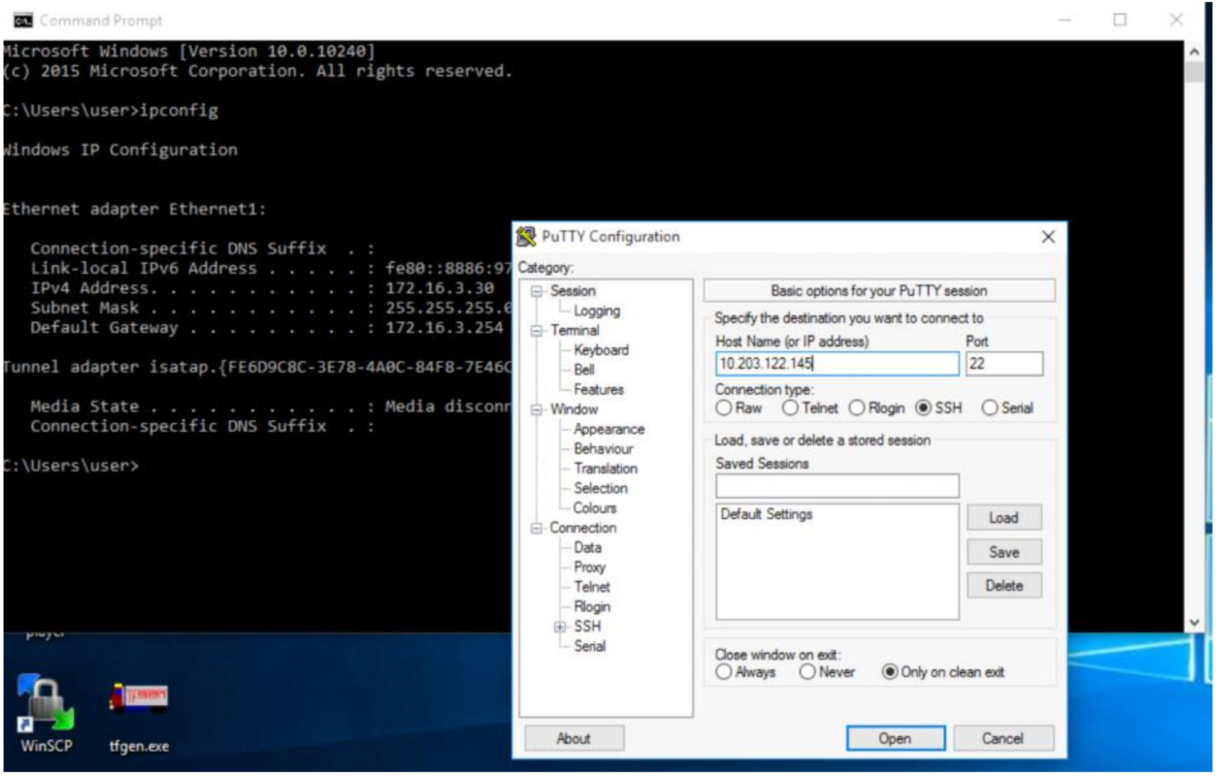
Finally, let's test sending ICMP and SSH traffic from VM-1 and VM-2 to the WAN. It *should* work.

Successful ping from VM-1 to WAN



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\user>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8886:97cc:91df:90d6%4
   IPv4 Address. . . . . . . . . . . : 172.16.3.30
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.3.254

Tunnel adapter isatap.{FE6D9C8C-3E78-4A0C-84F8-7E46C65F26BD}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\user>ping 10.203.122.145

Pinging 10.203.122.145 with 32 bytes of data:
Reply from 10.203.122.145: bytes=32 time=1ms TTL=252
Reply from 10.203.122.145: bytes=32 time=1ms TTL=252
Reply from 10.203.122.145: bytes=32 time=1ms TTL=252
Reply from 10.203.122.145: bytes=32 time=1ms TTL=252

Ping statistics for 10.203.122.145:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\user>
```

SSH session from VM-1 to WAN



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\user>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8886:97
   IPv4 Address. . . . . . . . . . . : 172.16.3.30
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.3.254

Tunnel adapter isatap.{FE6D9C8C-3E78-4A0C-84F8-7E46C

   Media State . . . . . . . . . . . : Media disconn
   Connection-specific DNS Suffix  . :

C:\Users\user>
```

Specify the destination you want to connect to

Host Name (or IP address): 10.203.122.145

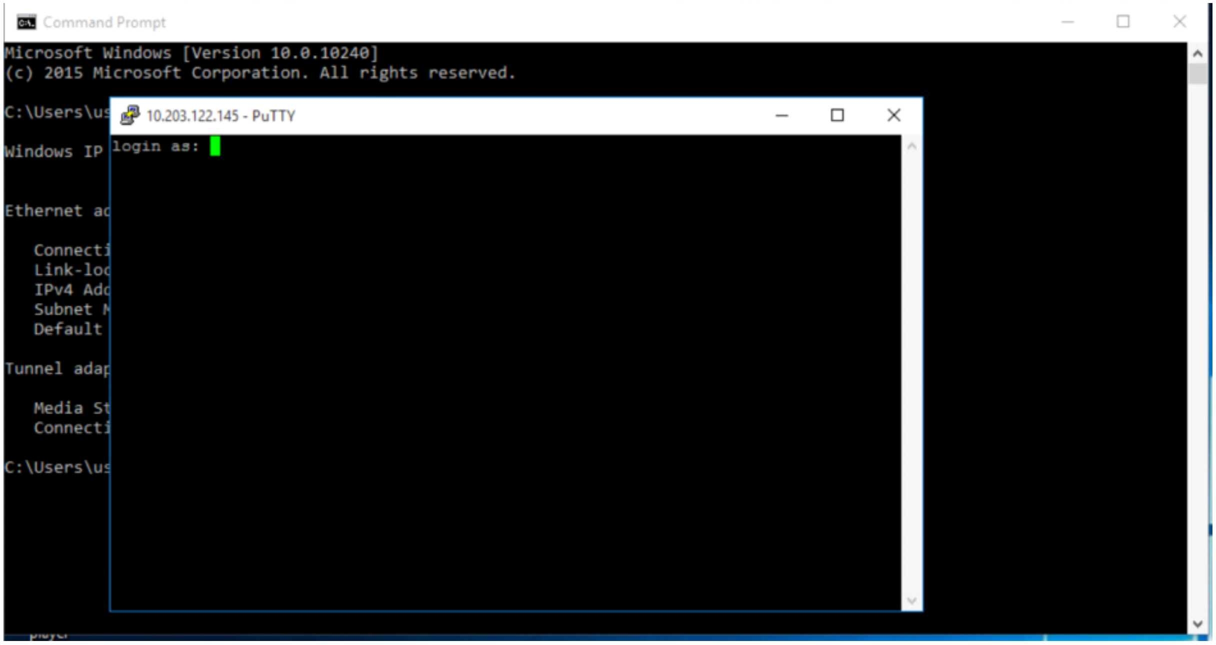
Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

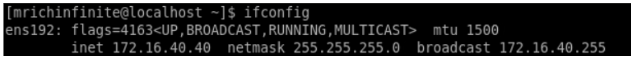
SSH successful



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.
```

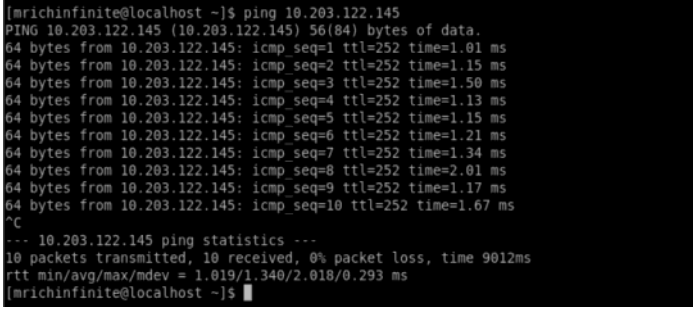
```
login as:
```

VM-2



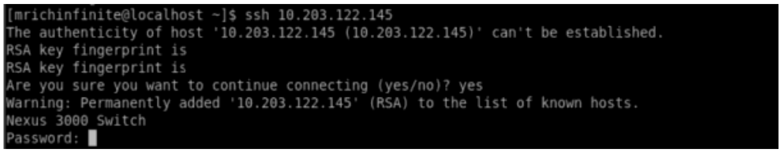
```
[mrichinfinite@localhost ~]$ ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.40.40  netmask 255.255.255.0  broadcast 172.16.40.255
```

Successful ping from VM-2 to WAN



```
[mrichinfinite@localhost ~]$ ping 10.203.122.145
PING 10.203.122.145 (10.203.122.145) 56(84) bytes of data.
64 bytes from 10.203.122.145: icmp_seq=1 ttl=252 time=1.01 ms
64 bytes from 10.203.122.145: icmp_seq=2 ttl=252 time=1.15 ms
64 bytes from 10.203.122.145: icmp_seq=3 ttl=252 time=1.50 ms
64 bytes from 10.203.122.145: icmp_seq=4 ttl=252 time=1.13 ms
64 bytes from 10.203.122.145: icmp_seq=5 ttl=252 time=1.15 ms
64 bytes from 10.203.122.145: icmp_seq=6 ttl=252 time=1.21 ms
64 bytes from 10.203.122.145: icmp_seq=7 ttl=252 time=1.34 ms
64 bytes from 10.203.122.145: icmp_seq=8 ttl=252 time=2.01 ms
64 bytes from 10.203.122.145: icmp_seq=9 ttl=252 time=1.17 ms
64 bytes from 10.203.122.145: icmp_seq=10 ttl=252 time=1.67 ms
^C
--- 10.203.122.145 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 1.019/1.340/2.018/0.293 ms
[mrichinfinite@localhost ~]$
```

Successful SSH session from VM-2 to WAN



```
[mrichinfinite@localhost ~]$ ssh 10.203.122.145
The authenticity of host '10.203.122.145 (10.203.122.145)' can't be established.
RSA key fingerprint is
RSA key fingerprint is
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.203.122.145' (RSA) to the list of known hosts.
Nexus 3000 Switch
Password: █
```

The successful pings and SSH sessions shown above are exactly what we want to see, since all traffic should be allowed from VM-1 and VM-2 to the WAN.

Conclusion

The purpose of this article was to demonstrate how to implement PBR in Cisco ACI when the service device is in an L3Out, and is not directly connected to the ACI fabric. With some practice, I think you will find that the configuration is fairly straightforward. However, there are some important things to consider when deploying this configuration, so please be sure to read the guidelines and limitations carefully (https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/5x/layer-4-to-layer-7-services-configuration/cisco-apic-layer-4-to-layer-7-services-deployment-guide-53x/configuring-policy-based-redirect-53x.html#id_110094). I hope you had as much fun reading about this as I did writing it. Happy networking!