



The bridge to possible

ACI – “not just another network...”

Steve Sharman, Technical Solutions Architect
@sps2101

Agenda

- Setting the scene
- Network Centric vs Application Centric
- Greenfield vs Brownfield
- Converting from Network Centric to Application Centric
- Allowing open communication
- ESGs under the covers
- L4-L7 service integration
- External connectivity
- Increasing security
- Automated blueprints

Why are you here...?

ACI – "just another network", or the foundation of an internal private cloud?

There are thousands of customers globally who have successfully deployed ACI fabrics and operate them as "just another network", but what if you could operate your ACI fabric as programmable private cloud infrastructure?

In this session we will look at how you can operate your ACI fabric as the foundation of an internal private cloud. We will look at how to migrate services onto an ACI fabric (network centric) and then implement segmentation (application centric). We will look at how to use Endpoint Security Groups to wrap security around endpoints within a VRF. We will then see how we can block East / West traffic within a hypervisor, and finally we'll dynamically add in firewalls to provide targeted L7 control.

If you're thinking this might prove time consuming to implement from the UI, we will show how all the configuration can be fully automated using Terraform.

Consuming an ACI fabric as "just another cloud" allows organisations choice on where to place workloads. Whether workloads are hosted in a public cloud, or on an on-premise private cloud, the consumption model should, and can, be the same.

Before we get started...

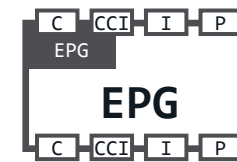
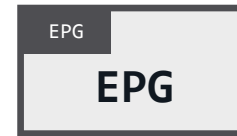
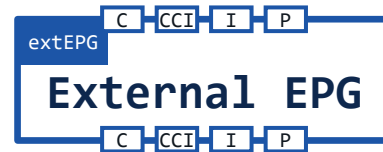


There are lots (and lots) of details in this presentation, please download through the Ciscolive app.

Well unless you have binoculars with you...!



Icons



*arrows indicate expected direction of traffic flow i.e. from consumer to provider

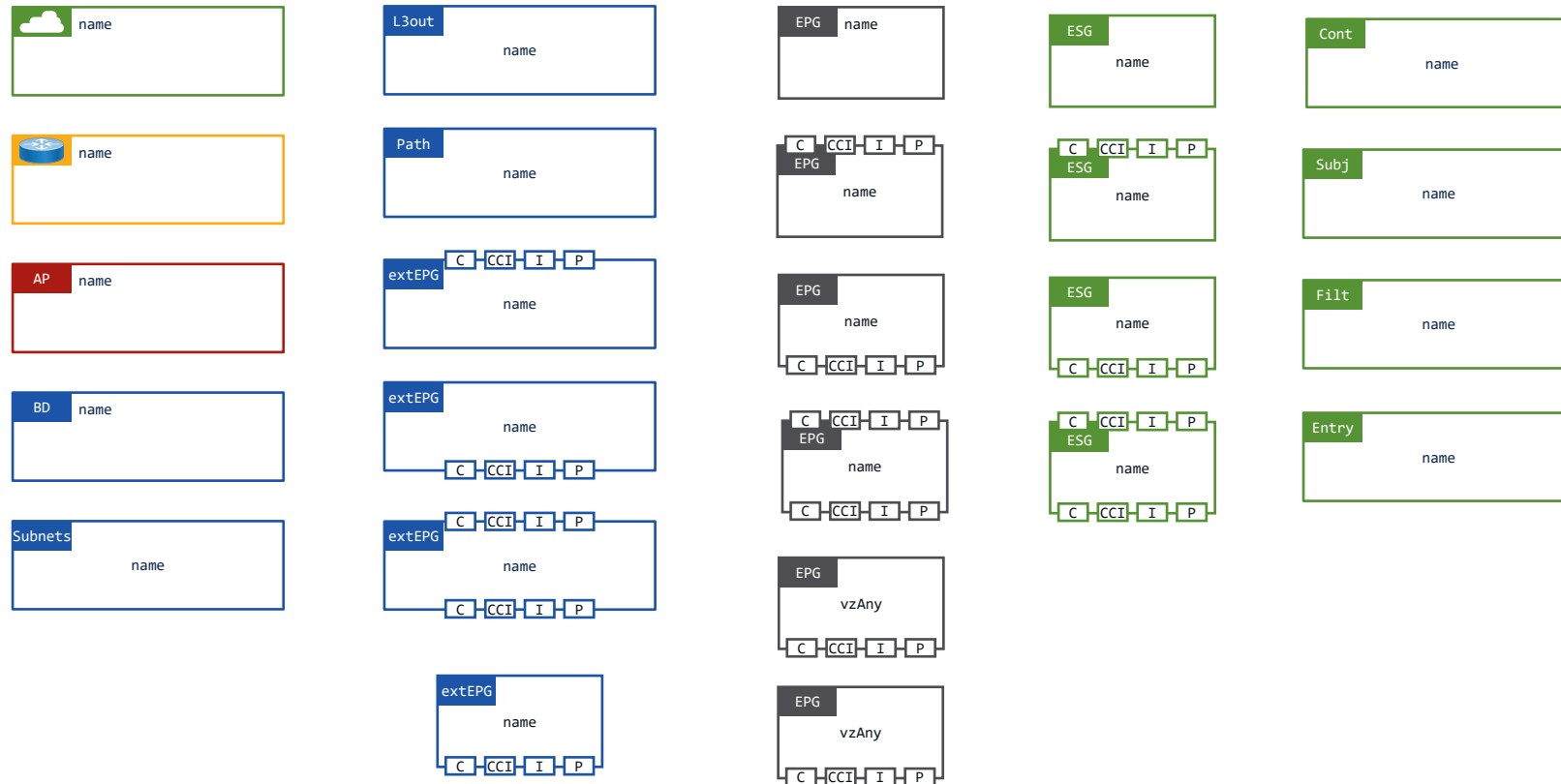
Icons



*arrows indicate expected direction of traffic flow i.e. from consumer to provider

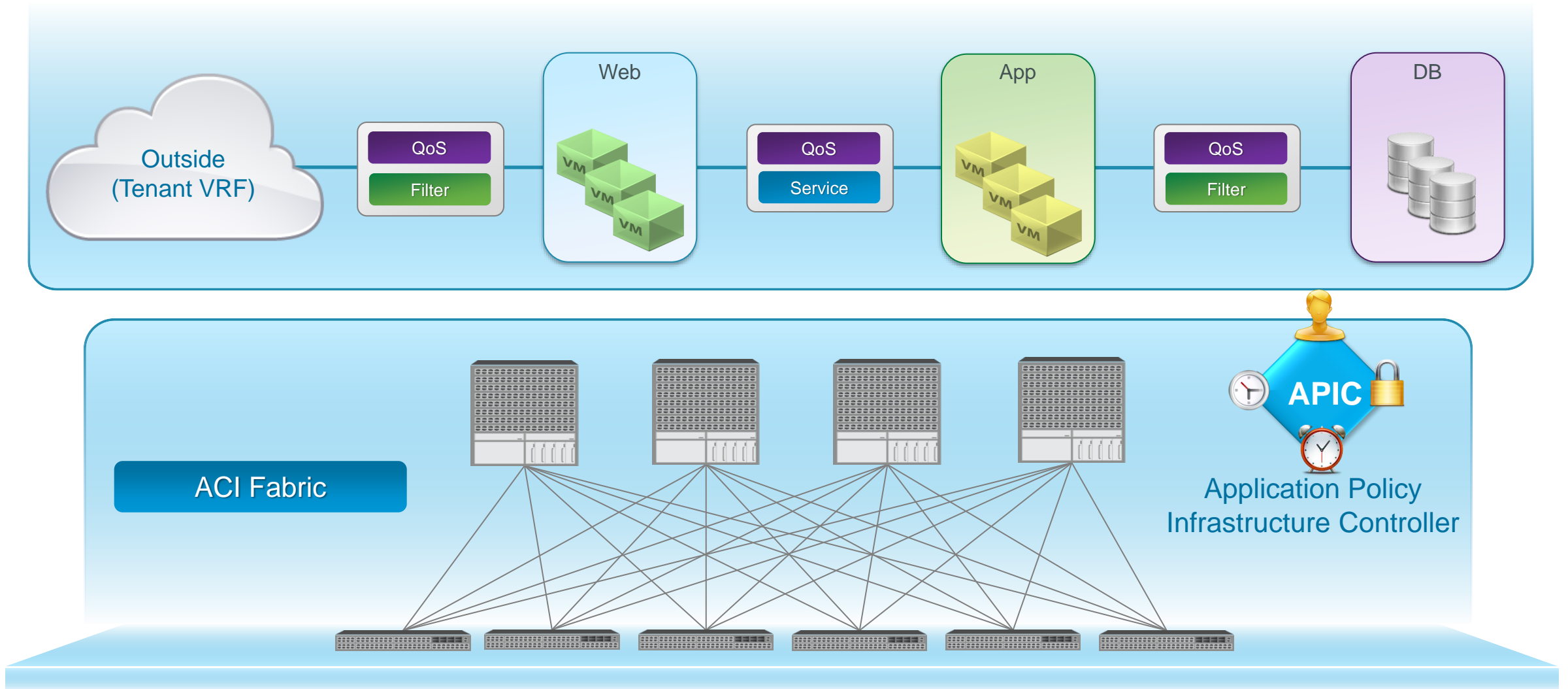
Resize by dragging the inner bottom right handle

Icons - small



The ACI reference application from circa 2014...

The mythical three tier application...!




Our reference application for this presentation...


Online Boutique

<https://github.com/GoogleCloudPlatform/microservices-demo>


Free shipping with \$75 purchase!

 cisco-store


Platform:
On-Premises
Customer name:
cisco-store
Vertical:
cisco
Build:




Hot Products




Cabana Shorts
\$39.99



Cable Knit Blanket
\$59.99






Free shipping with \$75 purchase!

Cart (2)

Empty Cart Continue Shopping




Save the Bees Bottle

SKU #2ZYFJ3GM2N

Quantity: 1

\$13.79



Cabana Shorts

SKU #OLJCESPC7Z

Quantity: 1

\$39.99

Shipping

\$8.99

Total

\$62.77

Shipping Address

E-mail Address
someone@example.com

Street Address
1600 Amphitheatre Parkway

Zip Code
94043

City
Mountain View

State
CA

Country
United States

Payment Method

Credit Card Number
4432-8015-6152-0454

Month
January

Year
2023

CVV
...

Place Order

CISCO Live!

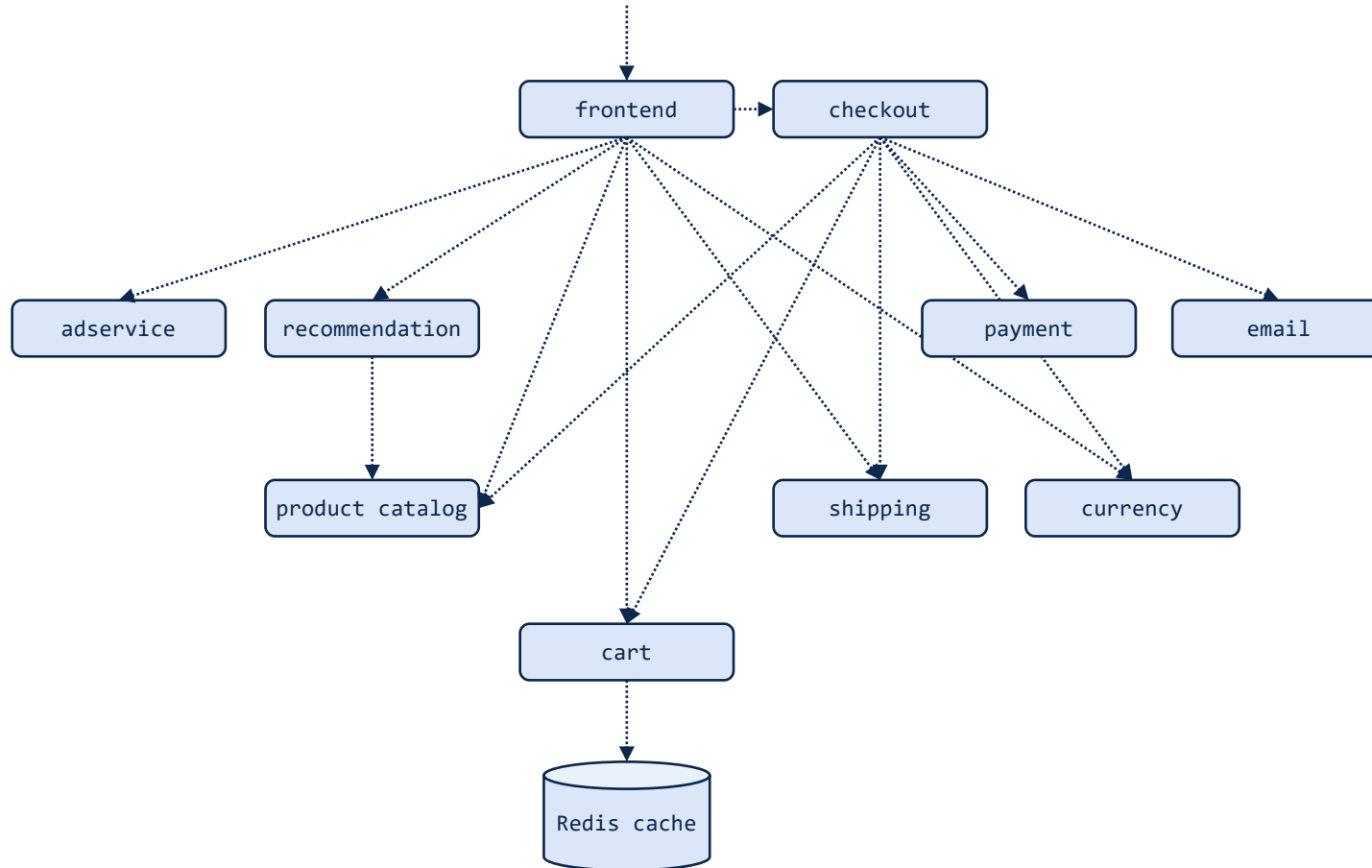
BRKDCN-2984

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

13

Online Boutique

<https://github.com/GoogleCloudPlatform/microservices-demo>



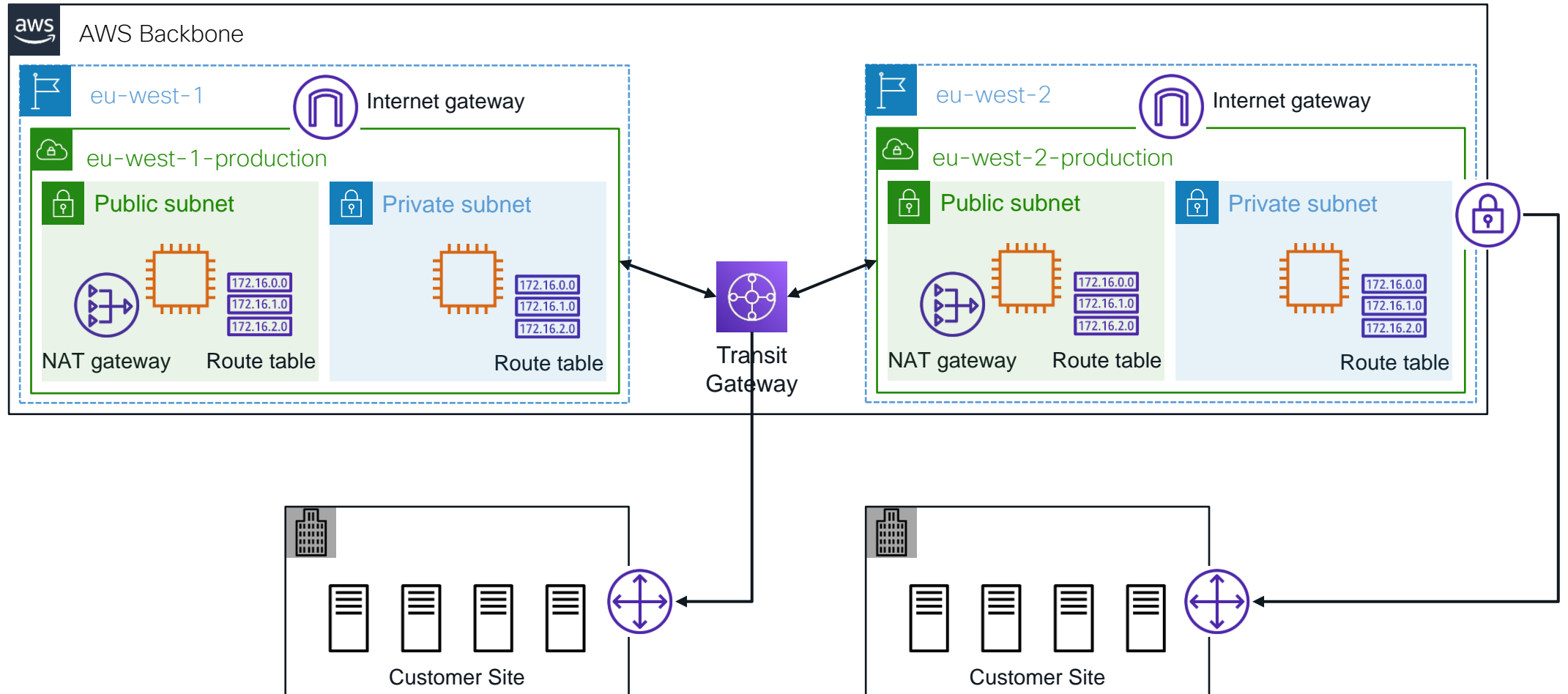
Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 8080
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP 3550
	recommendation	TCP 8080
	shipping	TCP 50051
outside	frontend	TCP 80/8080
recommendation	product catalog	TCP 3550

Who hasn't heard of "the journey to the cloud" ...?



AWS reference architecture

<https://docs.aws.amazon.com/vpc/latest/userguide/extend-intro.html>



Network Connectivity and Security are mandatory in the cloud...

Different clouds run different hypervisors

AWS Nitro System

A combination of dedicated hardware and lightweight hypervisor enabling faster innovation and enhanced security

[Get Started with a Nitro-based Instance Today](#)

The AWS Nitro System is the underlying platform for our next generation of EC2 instances that enables AWS to innovate faster, further reduce cost for our customers, and deliver added benefits like increased security and new instance types.

AWS has completely re-imagined our virtualization infrastructure. Traditionally, hypervisors protect the physical hardware and bios, virtualize the CPU, storage, networking, and provide a rich set of management capabilities. With the Nitro System, we are able to break apart those functions, offload them to dedicated hardware and software, and reduce costs by delivering practically all of the resources of a server to your instances.

Hypervisor security on the Azure fleet

Article • 11/11/2022 • 3 minutes to read • 4 contributors

[Feedback](#)

In this article

- [Strongly defined security boundaries enforced by the hypervisor](#)
- [Defense-in-depth exploit mitigations](#)
- [Strong security assurance processes](#)
- [Next steps](#)

The Azure hypervisor system is based on Windows Hyper-V. The hypervisor system enables the computer administrator to specify guest partitions that have separate address spaces. The separate address spaces allow you to load an operating system and applications operating in parallel of the (host) operating system that executes in the root partition of the computer. The host OS (also known as privileged root partition) has direct access to all the physical devices and peripherals on the system (storage controllers, networking adaptions). The host OS allows guest partitions to share the use of these physical devices by exposing "virtual devices" to each guest partition. Thus, an operating system executing in a guest partition has access to virtualized peripheral devices that are provided by virtualization services executing in the root partition.

The Azure hypervisor is built keeping the following security objectives in mind:

Objective	Source
Isolation	A security policy mandates no information transfer between VMs. This constraint requires capabilities in the Virtual Machine Manager (VMM) and hardware for isolation of memory, devices, the network, and managed resources such as persisted data.
VMM integrity	To achieve overall system integrity, the integrity of individual hypervisor components is established and maintained.

Google Cloud

7 ways we harden our KVM hypervisor at Google Cloud: security in plaintext

January 25, 2017

Andy Honig
Senior Product Manager

Nelly Porter
Group Product Manager, Google Cloud

Google Cloud uses the open-source KVM hypervisor that has been validated by scores of researchers as the foundation of [Google Compute Engine](#) and [Google Container Engine](#), and invests in additional security hardening and protection based on our research and testing experience. Then we contribute our changes to the KVM project, benefiting the overall open-source community.

Below is a list of the main ways we security harden KVM, to help improve the safety and security of our applications.

Proactive vulnerability search: There are multiple layers of security and isolation built into Google's KVM (Kernel-based Virtual Machine), and we're always working to strengthen them. Google's cloud security staff includes some of the world's foremost experts in the world of KVM security, and has uncovered multiple vulnerabilities in KVM, Xen and VMware hypervisors over the years. The Google



Executive
Sponsorship



New Talent
Attraction



New Culture



Evolution Instead
of Revolution



Cross Functional
Teams



Scaling



Think Agile



Partnerships 2.0

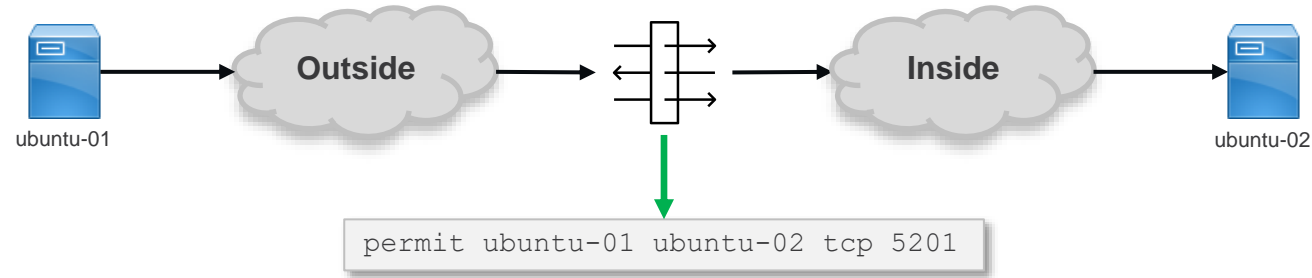
A cloud operating model succeeds best when there is a new organizational culture...

Cloud operating models have changed the way that security is implemented...

With a cloud operating model, security rules are typically declared with the application constructs...

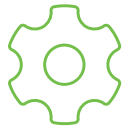
Conversely, within enterprise Data Centers security has been implemented by network and/or security administrators at a VRF boundary...

Traditional Enterprise Security Model



Traffic is routed to physical firewall which typically becomes a throughput pinch point with thousands of rules

ACI is the foundation for an internal private cloud...!



Day0 automation out-of-the-box; physical fabric and underlay



Per-application service-chaining



Pervasive Security Model



Hybrid cloud capability; public cloud-like networking constructs



Single API Model for 100s of switches and 1000s of ports; cloud-like consumption model



Infrastructure as Code with Ansible and Terraform

Network Centric vs Application Centric



What does Google say about the different modes...?

Google search results for "Cisco ACI what is the difference between network centric and applica". The search bar shows the query and the Google logo. Below the search bar, there are tabs for "All", "Images", "Videos", "News", "Books", and "More". The search results show "About 157,000 results (0.48 seconds)". The first result is from "https://ipwithease.com > Blog" and is titled "Cisco ACI Network Centric vs Application Centric approach". It includes a snippet: "Network Centric approach allows existing network architecture and flows to remain the same, henceforth allowing IT resources enough period to get acclimatized with the new terminologies of ACI fabric. Application Centric approach is comparatively a new approach model where application tiers are defined by EPGs." There is a small thumbnail image next to the snippet. Below the first result, there is a "People also ask" section with four questions: "What is application centric infrastructure ACI?", "What is network centric application?", "What are the 3 core components of ACI Architecture?", and "How Cisco application centric infrastructure ACI is related to SDN and how it differs?". Each question has a dropdown arrow. Below the "People also ask" section, there is another result from "https://community.cisco.com > application-centric > td-p" titled "Difference between ACI network centric mode and application ...". It includes a snippet: "Application centric is another way of thinking. Instead of having the network lead the application leads. This results into a network 'bubble' (for lack of ...". Below this, there is another result from "https://community.cisco.com > application-centric > td-p" titled "ACI network centric vs app centric - Cisco Community". It includes a snippet: "Application-centric mode: Application-centric mode gives ACI users the highest level of visibility and security. In this mode, we define groups and contracts ...".

Google search results for "site:cisco.com Cisco ACI what is the difference between network cent". The search bar shows the query and the Google logo. Below the search bar, there are tabs for "All", "Images", "Videos", "News", "Books", and "More". The search results show "About 21,100 results (0.45 seconds)". The first result is from "https://community.cisco.com > application-centric > td-p" titled "Difference between ACI network centric mode and application ...". It includes a snippet: "Application centric is another way of thinking. Instead of having the network lead the application leads. This results into a network 'bubble' (for lack of ...". Below this, there is another result from "https://community.cisco.com > application-centric > td-p" titled "ACI network centric vs app centric - Cisco Community". It includes a snippet: "Application-centric mode: Application-centric mode gives ACI users the highest level of visibility and security. In this mode, we define groups and contracts ...". Below this, there is a result from "https://www.cisco.com > networking > cloud-networking" titled "Cisco ACI - Application Centric Infrastructure". It includes a snippet: "Configure, operate, and analyze everything connected to your data center and cloud networks, all from one place. Connect to Cisco Nexus Dashboard." Below this, there is a result from "https://www.cisco.com > data-center-virtualization > pdf" titled "Network Centric to ACI Centric Migration - Cisco". It includes a snippet: "The Network-Centric model serves many customers well; it allows them to migrate their existing compute/applications/ network into ACI in a way that is familiar." Below this, there is a result from "https://community.cisco.com > application-centric > td-p" titled "Solved: ACI Network Centric to Application Centric Migration". It includes a snippet: "Nov 27, 2019 — Solved: We are planning to migrate our existing infrastructure to ACI in few steps. First to a Network Centric setup (EPG=VLAN=BD) with a L2 ...". Below this, there is a result from "https://www.cisco.com > Solutions > Data Center" titled "Application Centric Infrastructure (ACI) - Data Center - Cisco". It includes a snippet: "This solution provides automated network connectivity, consistent policy management, and simplified operations for multicloud environments. Unlock the full ...".

What does Google say about migration from one mode to another...?

Google

Cisco ACI migrate from network centric mode to application centric mode

https://unofficialaciguide.com › 2017/09/08 › network-...
Network Centric to ACI Centric Migration - - Unofficial ACI Guide
Sep 8, 2017 — Map existing Vlans into **ACI in Network-Centric Mode** (L2 only – no contracts) – Create legacy EPGs and BDs on the **ACI Fabric**. · Create L3out for ...

https://ipwithease.com › Blog
Cisco ACI Network Centric vs Application Centric approach
Network Centric approach is considered a soft transition for customers from traditional architecture to **ACI** architecture. · On the other hand, **Application** ...

https://www.youtube.com › watch
[HD] Cisco ACI Brownfield Network Centric to Application ...
In this video Ralph Carter discusses how to **migrate** into ACI from a legacy aka brownfield environment to a **Cisco ACI** fabric usin...
YouTube · Ralph Carter · Dec 2, 2019
29:36
10 key moments in this video

https://www.linkedin.com › pulse › cisco-aci-network-cen...
Cisco ACI – Network Centric vs. Application Centric Approach
Jun 30, 2019 — The **network-centric** approach is preferred when **migrating** the network from legacy/traditional networking to SDN based model. This is to ensure ...

https://www.wwt.com › ... › Data Center Networking
Demystifying ACI Application Centric "Mode" Through ... - WWT
Dec 15, 2020 — **Network Centric** is simple and straightforward -- VLAN, endpoint groups (EPG) and bridge domains (BDs) are mapped in a 1-to-1 relationship, hence ...

https://www.networkbachelor.com › network-vs-applica...
Network vs Application Centric
In short, the approach is called **application-centric** if the policies are created based on application details such as required port-for communication between ...

Google

site:cisco.com Cisco ACI migrate from network centric mode to applic

All Videos Books Images News More Tools

About 5,050 results (0.37 seconds)

https://www.cisco.com › data-center-virtualization › PDF
Network Centric to ACI Centric Migration - Cisco
The **Network-Centric** model serves many customers well; it allows them to **migrate** their existing compute/applications/ network into **ACI** in a way that is familiar.
5 pages

https://community.cisco.com › data-center-blogs › ba-p
All About Migration: Network Centric to ACI Centric Model
Apr 12, 2019 — All legacy vlans that will be a part **migrated** to the **ACI-Centric** application exist on the fabric (or will be operational prior to the **migration** ...

https://www.cisco.com › ... › Technical References
Migrating Existing Networks to Cisco ACI
Dec 23, 2015 — The recommended approach for a **network centric** migration consists of associating each VLAN originally defined in the brownfield infrastructure ...

https://community.cisco.com › application-centric › td-p
Difference between ACI network centric mode and application ...
hai guys, I have deploy **ACI** infrastructure on my customer, currently using **network centric mode**. Later, it will be converted to **application centric mode**.

https://www.cisco.com › networking › cloud-networking
Cisco ACI - Application Centric Infrastructure
Configure, operate, and analyze everything connected to your data center and cloud **networks**, all from one place. Connect to **Cisco Nexus** Dashboard.
★★★★★ Rating; 5 · 86 reviews
Read solution overview · White Papers · Cisco APIC · Simulator

https://community.cisco.com › application-centric › td-p
ACI network centric vs app centric - Cisco Community
Or, if the **network** is left in zero-trust **mode**, the contracts used will be very open, allowing all

Where should we start...?

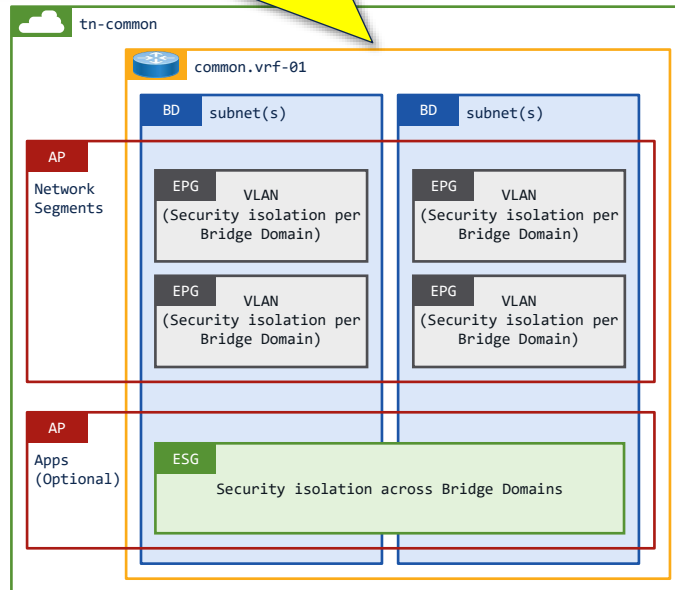




Design Considerations...

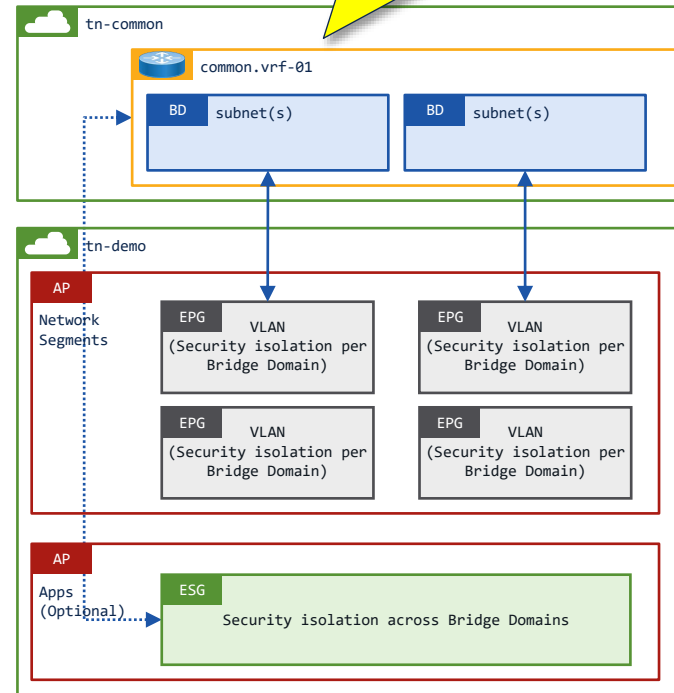
Design Patterns

Everything in the “common” Tenant is not typically seen



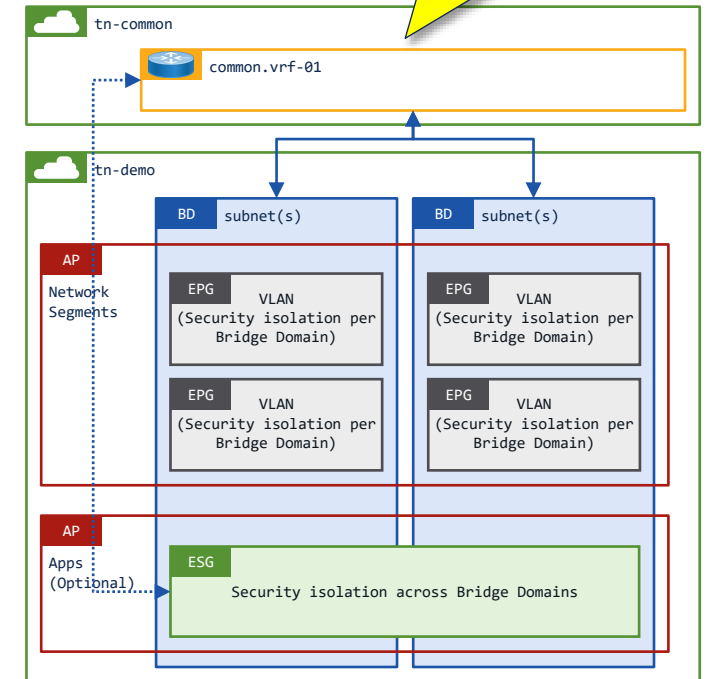
Used for functions which are accessible from any Tenant

VRFs and BDs in “common” with EPGs and ESGs in the “user” tenant



Typically, fewer larger subnets which can be (optionally) shared across Tenants

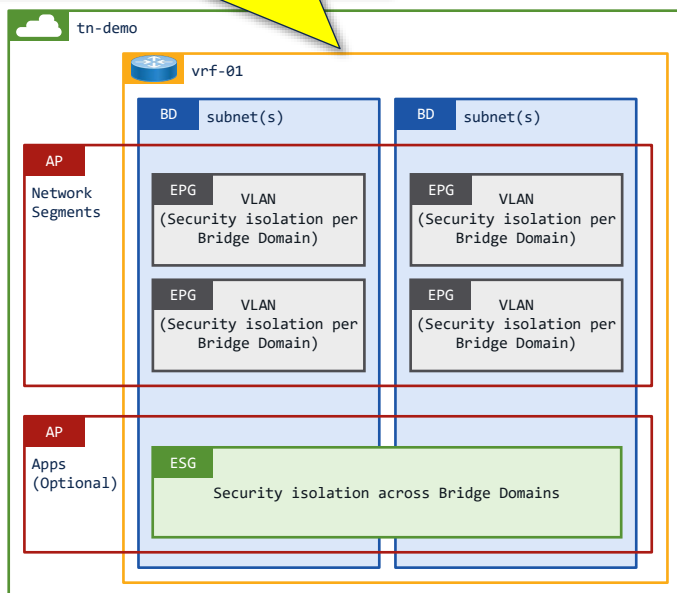
VRFs in “common” with BDs, EPGs and ESGs in the “user” tenant



Dedicated subnets for tenants with VRFs that can be (optionally) shared by different Tenants

Design Patterns

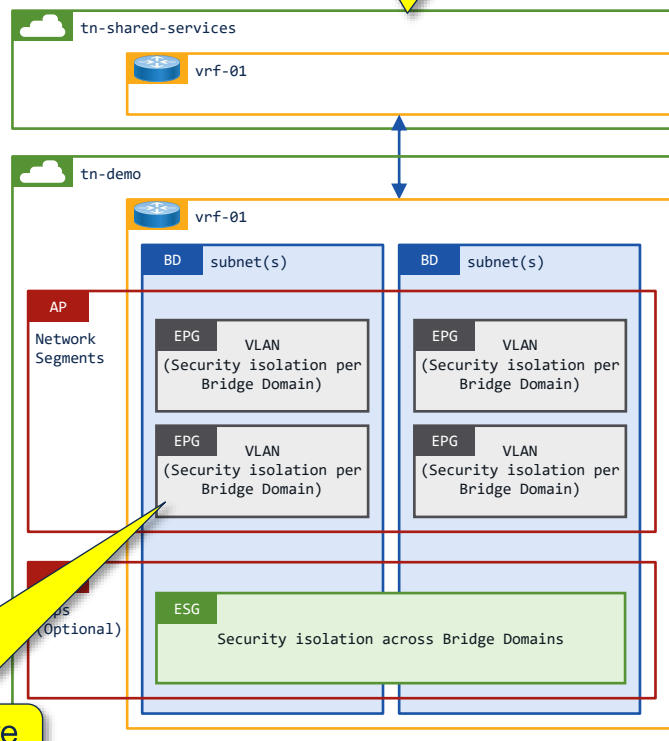
All networking constructs contained within a Tenant



Dedicated VRFs and subnets for each Tenant with Dedicated L3outs

Each Tenant has one or more network security groups

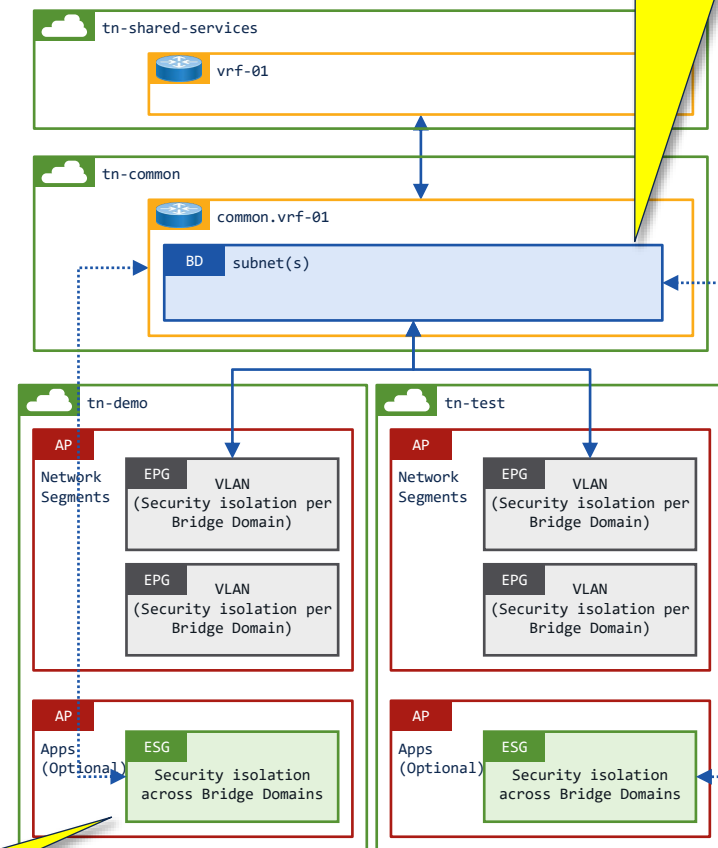
Network team controls inbound/outbound routing



Dedicated VRFs and subnets for each Tenant with Shared L3out

Each Tenant has one or more endpoint security groups

Large subnets can be shared across Tenants



EPG and ESG in the "user" Tenant with the VRF in the "common" Tenant, and a Shared L3out in shared-services

Each Tenant has their own IP Range

APIC (aci-dev-01)

System

Tenants

Fabric

Virtual Networking

Admin

Operations

Apps

Integrations

ALL TENANTS

Add Tenant

Tenant Search:

common

ciscolive-07

rwhitear

shared-services

ciscolive-08

All Tenants

Name	Alias	Description	Bridge Domains	VRFs
shared-services		L3out and shared devices	0	1
aci-infrastructure		Nexus Dashboard, MSO etc	1	0
ciscolive-01		Routable IP range 10.0.11-15.x	5	1
ciscolive-02		Routable IP range 10.0.21-25.x	0	1
ciscolive-03		Routable IP range 10.0.31-35.x	0	1
ciscolive-04		Routable IP range 10.0.41-45.x	0	1
ciscolive-05		Routable IP range 10.0.51-55.x	0	1
ciscolive-06		Routable IP range 10.0.61-65.x	0	1
ciscolive-07		Routable IP range 10.0.71-75.x	5	1
ciscolive-08		Routable IP range 10.0.81-85.x	5	1
ardica		Routable IP range 192.168.0-5.x	0	1
rwhitear		Routable IP range 192.168.10-15.x	6	1
ngorse		Routable IP range 192.168.120-125.x	1	1
demo		Routable IP range 192.168.150-155.x	3	1
fgandola		Routable IP range 192.168.151-158.x	11	2
roxadiaz		Routable IP range 192.168.20-25.x	6	1
ndsouzar		Routable IP range 192.168.30-35.x	6	1
esx-infrastructure		Routable IP range 192.168.4.x	1	0
adealdag		Routable IP range 192.168.40-45.x	6	1
ssharmar		Routable IP range 192.168.50-56.x	7	1
mgmt		Routable IP range 192.168.6.x	1	2
movaswan		Routable IP range 192.168.60-65.x	6	1
adossant		Routable IP range 192.168.70-75.x	0	1
fdagenha		Routable IP range 192.168.80-85.x	0	1
ylouis		Routable IP range 192.168.90-95.x	0	1

Page 1 Of 1

Objects Per Page: 100

Displaying Objects 1 - 32 Of 32

Last Login Time: 2022-11-26T07:06 UTC+00:00

Current System Time: 2022-11-26T07:58 UTC+00:00

All Tenants

Name	Alias	Description
shared-services		L3out and shared devices
aci-infrastructure		Nexus Dashboard, MSO etc
ciscolive-01		Routable IP range 10.0.11-15.x
ciscolive-02		Routable IP range 10.0.21-25.x
ciscolive-03		Routable IP range 10.0.31-35.x
ciscolive-04		Routable IP range 10.0.41-45.x
ciscolive-05		Routable IP range 10.0.51-55.x
ciscolive-06		Routable IP range 10.0.61-65.x
ciscolive-07		Routable IP range 10.0.71-75.x
ciscolive-08		Routable IP range 10.0.81-85.x
ardica		Routable IP range 192.168.0-5.x
rwhitear		Routable IP range 192.168.10-15.x
ngorse		Routable IP range 192.168.120-125.x

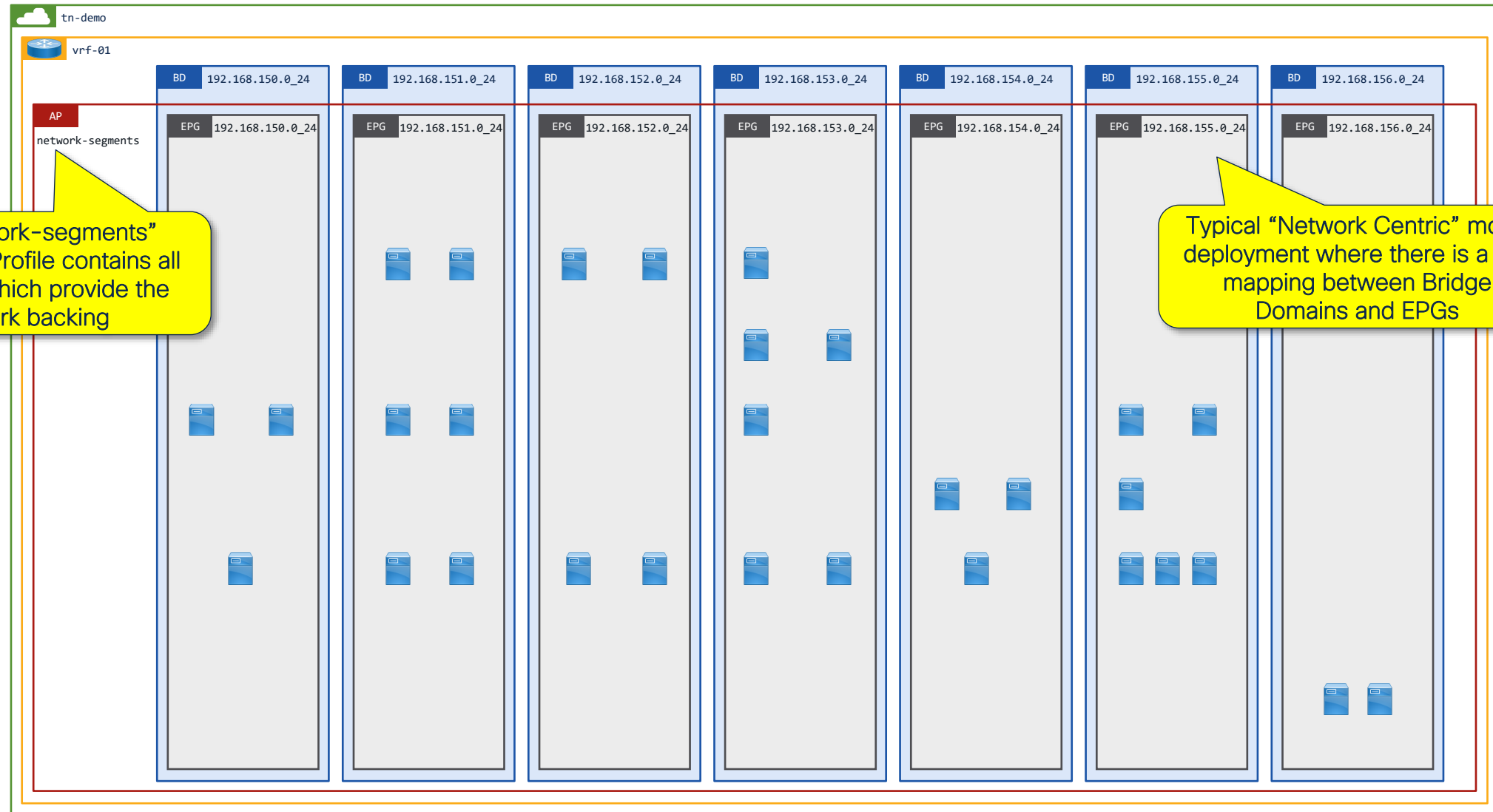
IP range per Tenant



Convert Brownfield Network Centric environment to Application Centric environment

Network engineers “view” of their ACI environment...

Workloads identified by IP and Mac address



The "network-segments" Application Profile contains all the EPGs which provide the network backing

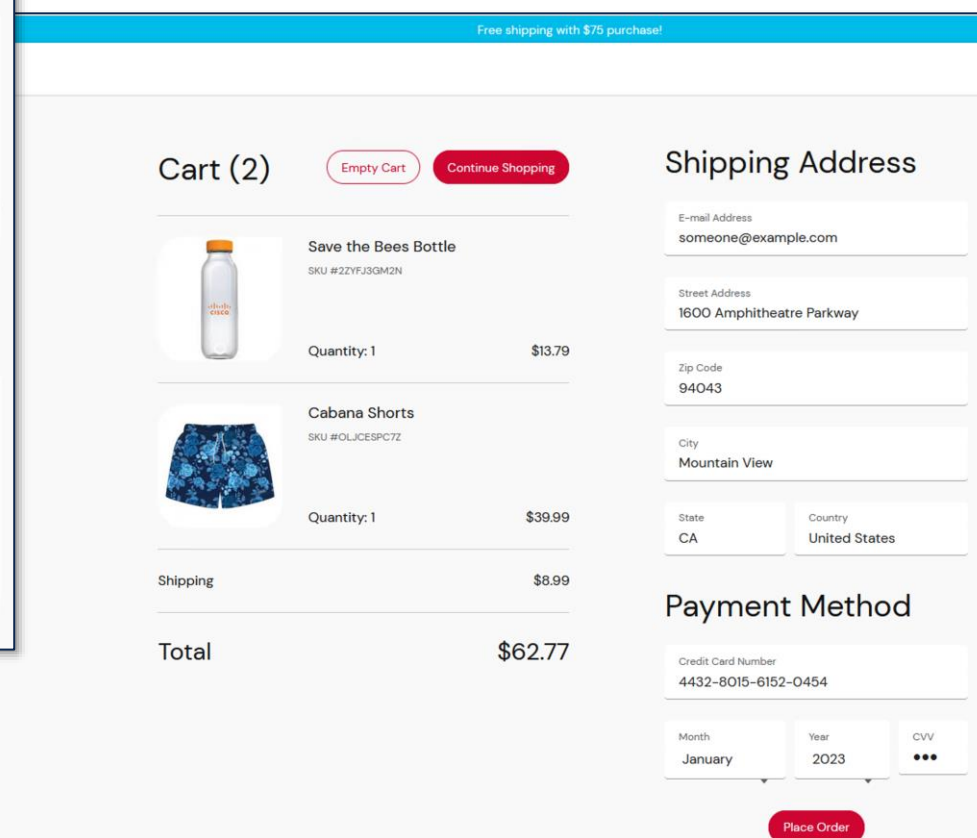
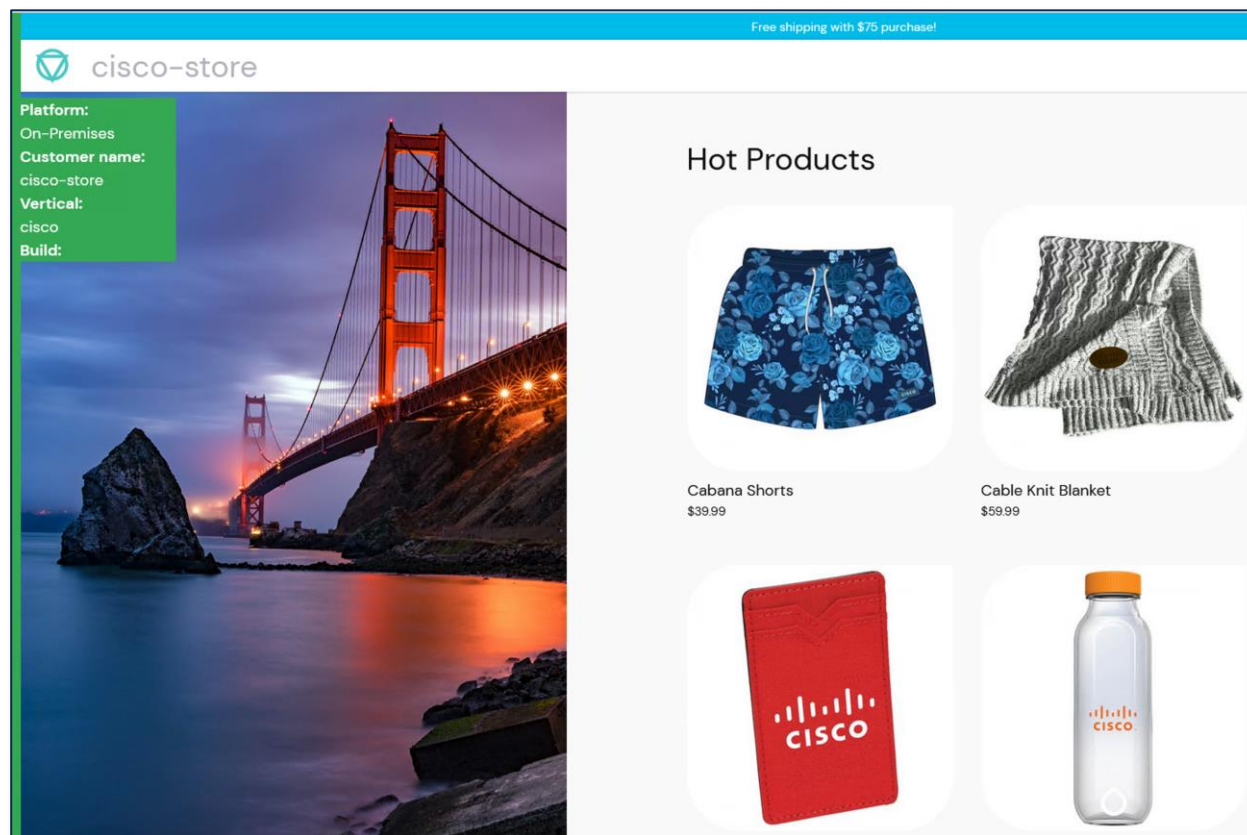
Typical "Network Centric" mode deployment where there is a 1:1 mapping between Bridge Domains and EPGs

What does the application owner care about...?

DNS names, IP addresses, Default Gateways, and
Security Rules...

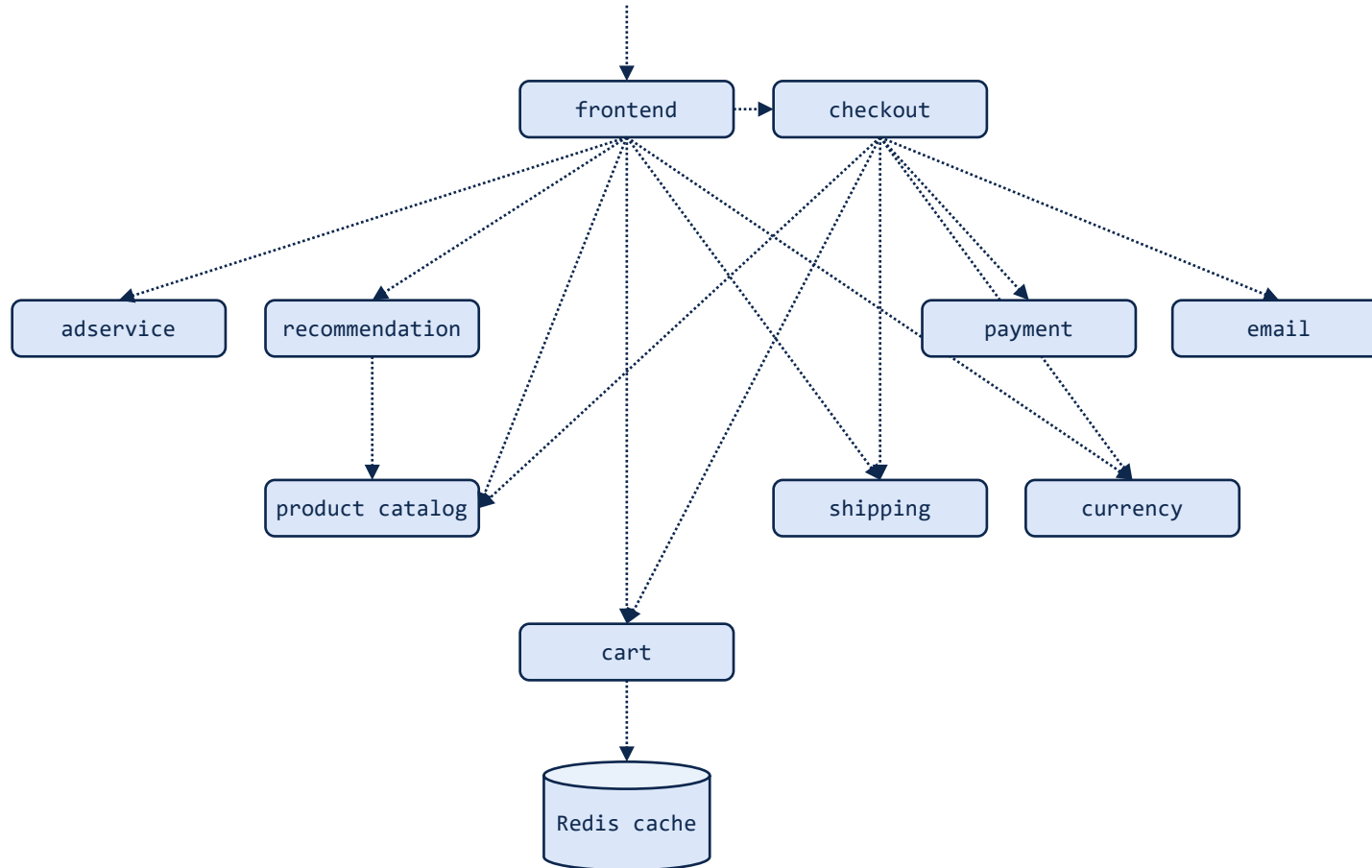
Online Boutique

<https://github.com/GoogleCloudPlatform/microservices-demo>



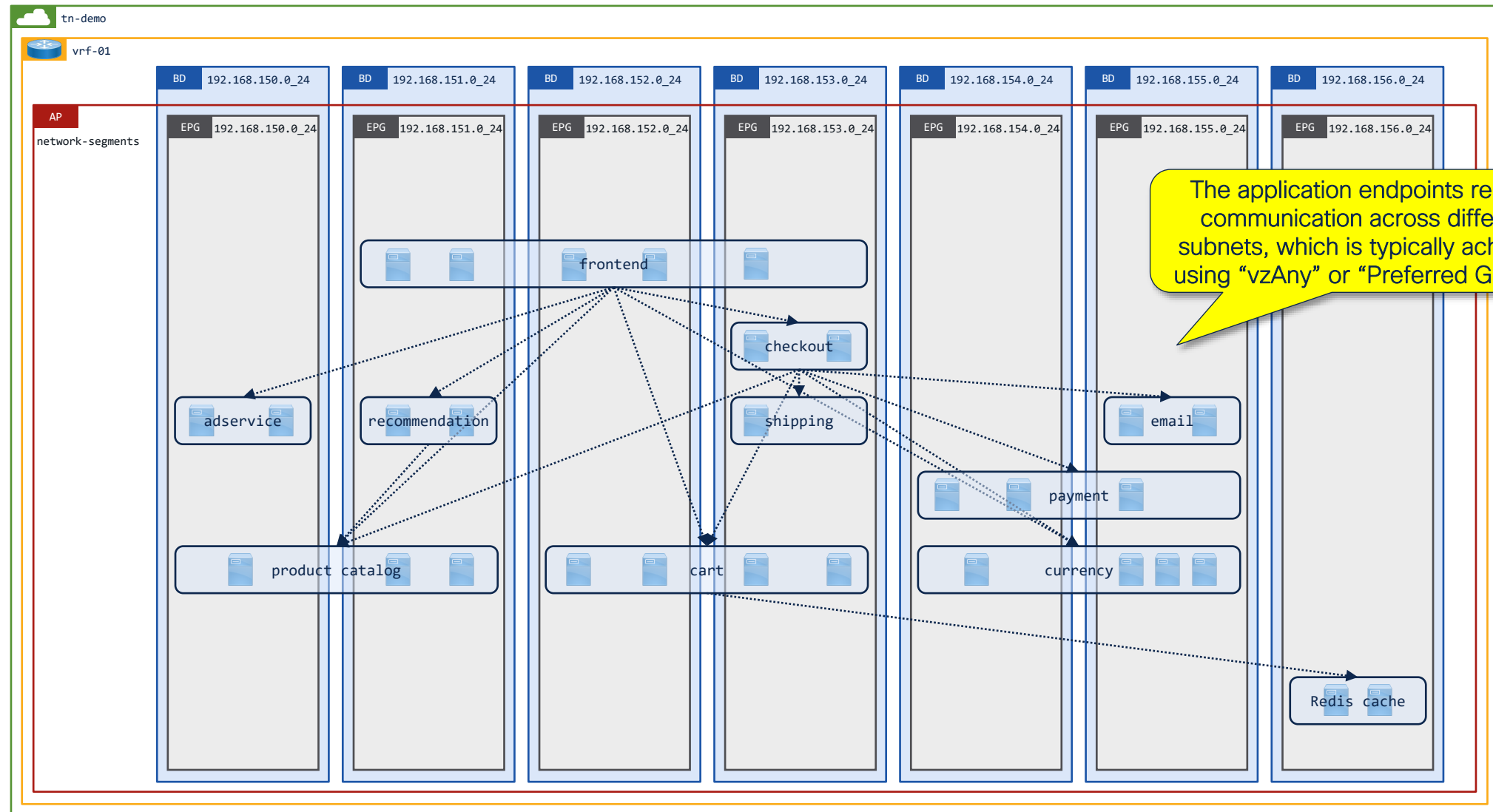
Online Boutique

<https://github.com/GoogleCloudPlatform/microservices-demo>

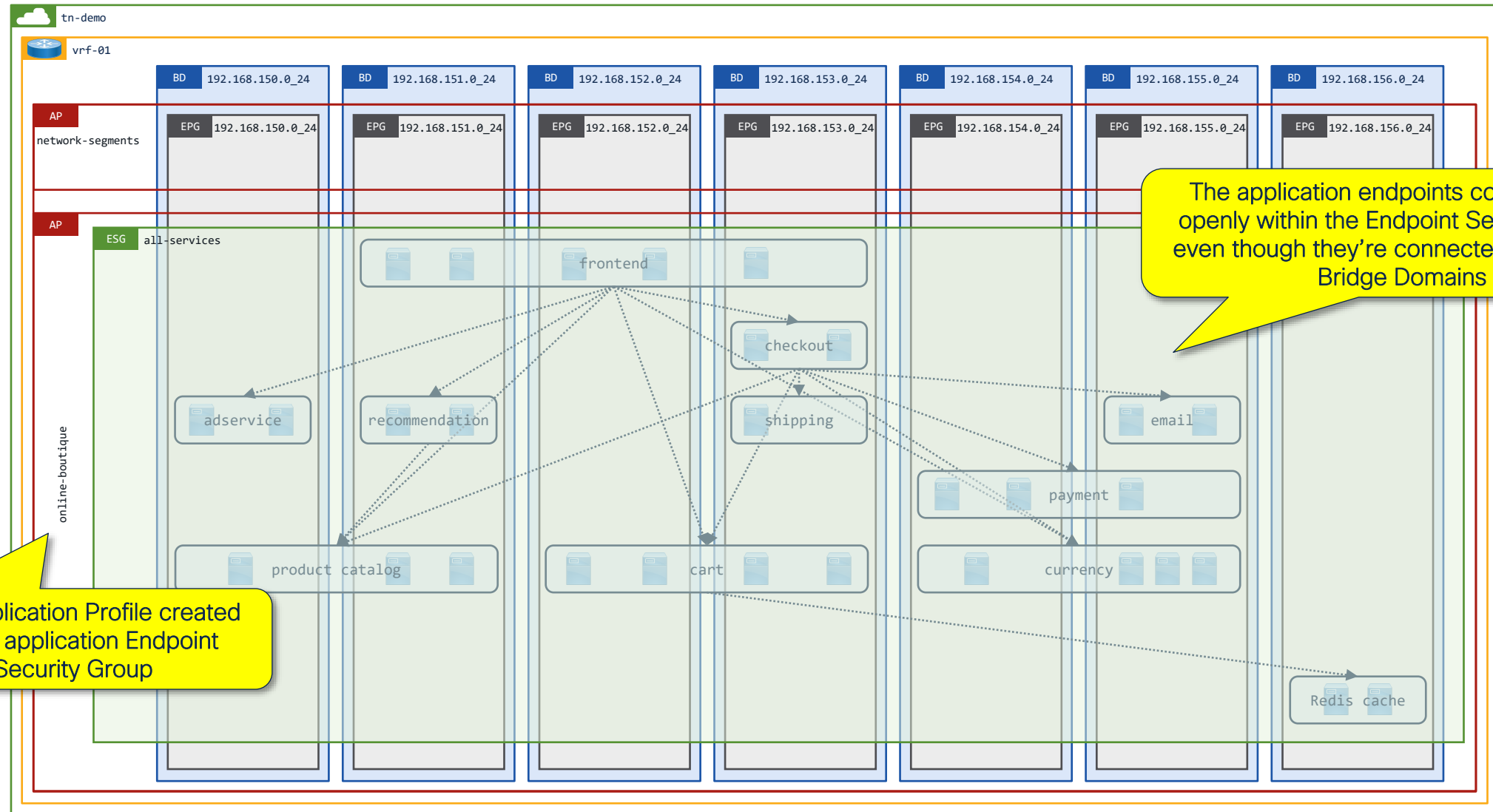


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart currency email payment product catalog shipping	TCP 7070 TCP 7000 TCP 8080 TCP 50051 TCP 3550 TCP 50051
frontend	adservice cart checkout currency product catalog recommendation shipping	TCP 9555 TCP 7070 TCP 5050 TCP 7000 TCP 3550 TCP 8080 TCP 50051
outside	frontend	TCP 80/8080
recommendation	product catalog	TCP 3550

Endpoints span subnets

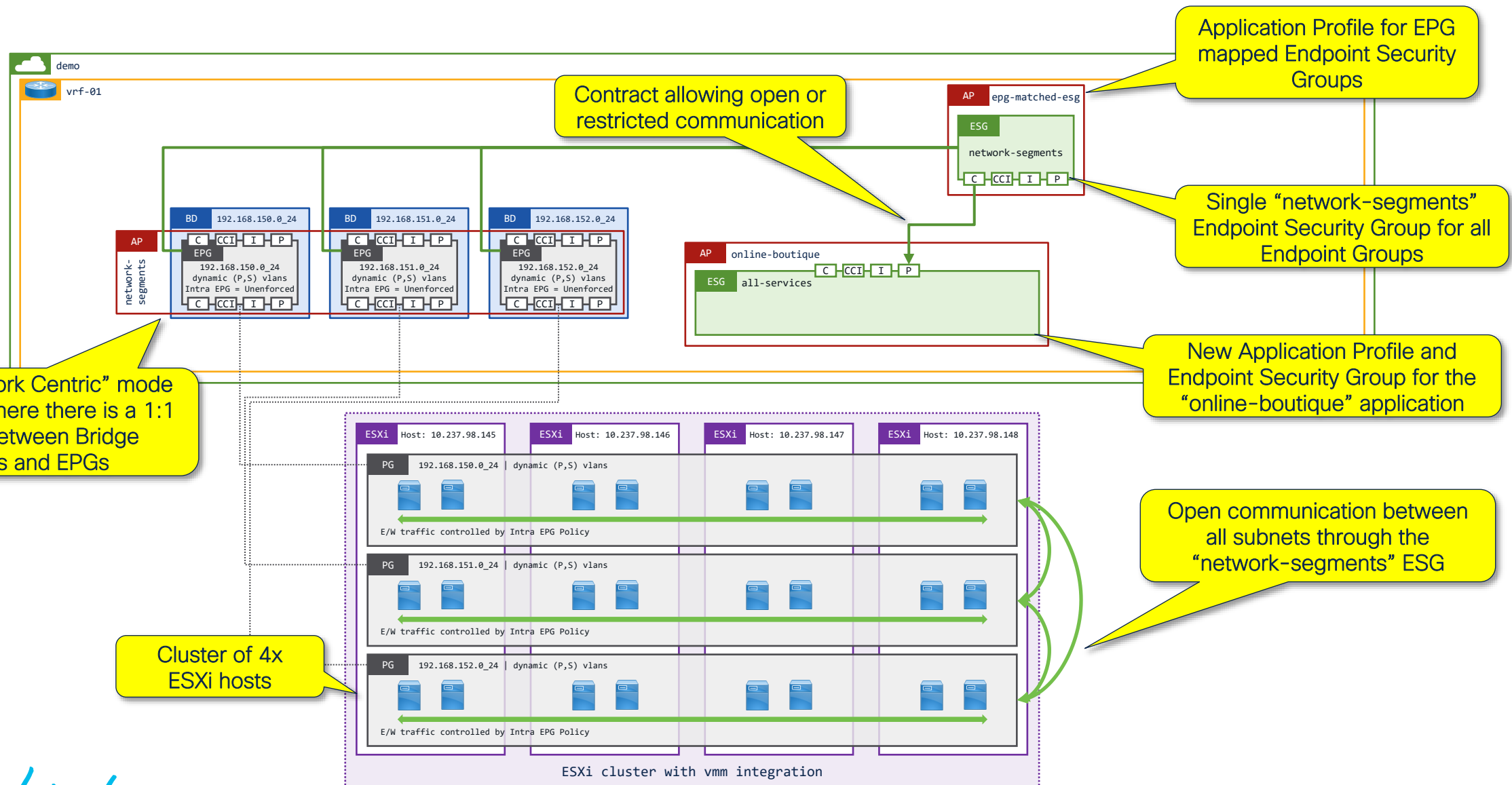


Let's convert to "Application Centric" mode



You can convert from Network Centric mode to Application Centric mode in Two Steps...

Step 1: Create Application Profiles and Security Groups



Step 2: Create ACI Tags to match vCenter Tags

The screenshot illustrates the configuration of ACI tags to match vCenter tags. The interface is divided into several sections:

- Left Sidebar:** Contains navigation options like 'Quick Start', 'demo', 'Application Profiles', 'Endpoint Security Groups', 'all-services', 'Contracts', 'Selectors', 'Tag Selectors', 'EPG Selectors', 'IP Subnet Selectors', and 'Service EPG Selectors'.
- Tree View:** Shows a hierarchy of services under 'tn-demo-online-boutique', including 'backend', 'frontend', and 'middleware'. The 'tn-demo-online-boutique-frontend-service' is selected.
- Tag Selectors Table:** A table with columns 'Tag Key', 'Value Operator', and 'Tag Value'. It lists various services and their corresponding tags.
- Assign Tag Dialog:** A dialog titled 'Assign Tag' for the selected service. It shows a list of available tags with checkboxes.

Tag Selectors Table:

Tag Key	Value Operator	Tag Value
Function	Equals	tn-demo-online-boutique-email-service
Function	Equals	tn-demo-online-boutique-frontend-service
Function	Equals	tn-demo-online-boutique-redis-cart
Function	Equals	tn-demo-online-boutique-currency-service
Function	Equals	tn-demo-online-boutique-payment-service
Function	Equals	tn-demo-online-boutique-cart-service
Function	Equals	tn-demo-online-boutique-ad-service
Function	Equals	tn-demo-online-boutique-product-catalog-service
Function	Equals	tn-demo-online-boutique-recommendation-service
Function	Equals	tn-demo-online-boutique-shipping-service
Function	Equals	tn-demo-online-boutique-checkout-service

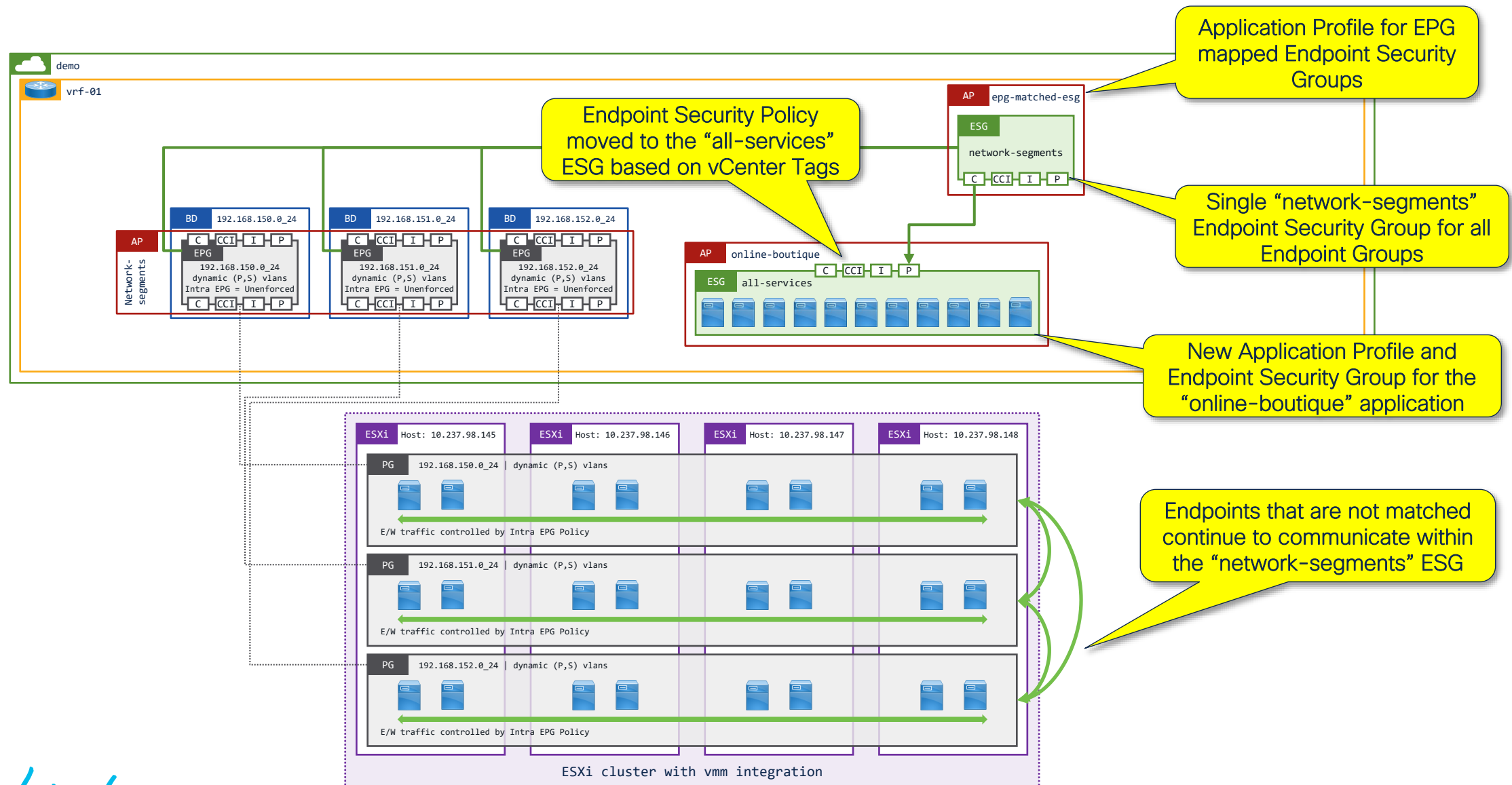
Assign Tag Dialog:

Assign Tag | tn-demo-online-boutique-frontend-service

ADD TAG

Tag Name	Category
<input type="checkbox"/> tn-demo-online-boutique-product-catalog-service	Function
<input type="checkbox"/> tn-demo-online-boutique-email-service	Function
<input type="checkbox"/> tn-demo-online-boutique-ad-service	Function
<input type="checkbox"/> tn-demo-online-boutique-recommendation-service	Function
<input type="checkbox"/> tn-demo-online-boutique-shipping-service	Function
<input checked="" type="checkbox"/> tn-demo-online-boutique-frontend-service	Function
<input type="checkbox"/> tn-demo-online-boutique-checkout-service	Function
<input type="checkbox"/> tn-demo-online-boutique-payment-service	Function
<input type="checkbox"/> tn-demo-online-boutique-currency-service	Function
<input type="checkbox"/> tn-demo-online-boutique-redis-cart	Function

Endpoints automatically move to new Security Group



Automated conversion to “Application Centric”

Endpoints mapped to the “network-segments” ESG through EPG → ESG mapping

MAC/IP	Endpoint Name	Learning Source	Hosting Server	Interface (learned)	Encap	Base EPG	Policy Tags
00:50:56:A1:1A:60	tn-demo-online-boutique-ad-service	learned vmm	10.237.98.165	Pod-1/Node-101/eth1/29 (learned...)	vlan-1038(P) vlan-1064(S)	demo:network-segments:192.168.150.0_24	__vmm:vmname tn-demo-ad-servic
00:50:56:A1:3F:2C	tn-demo-online-boutique-frontend-service	learned vmm	10.237.98.168	Pod-1/Node-101/eth1/32 (learned...)	vlan-1020(P) vlan-1021(S)	demo:network-segments:192.168.152.0_24	__vmm:vmname tn-demo-frontend-
192.168.152.101						demo:network-segments:192.168.152.0_24	
00:50:56:A1:7F:0B	tn-demo-online-boutique-checkout-service	learned vmm	10.237.98.168	Pod-1/Node-102/eth1/32 (learned...)	vlan-1017(P) vlan-1018(S)	demo:network-segments:192.168.151.0_24	__vmm:vmname tn-demo-checkout
00:50:56:A1:7F:A5	tn-demo-online-boutique-redis-cart	learned vmm	10.237.98.166	Pod-1/Node-102/eth1/30 (learned...)	vlan-1017(P) vlan-1018(S)	demo:network-segments:192.168.151.0_24	__vmm:vmname tn-demo-redis-car
00:50:56:A1:8E:DB	tn-demo-online-boutique-payment-service	learned vmm	10.237.98.167	Pod-1/Node-101/eth1/31 (learned...)	vlan-1038(P) vlan-1064(S)	demo:network-segments:192.168.150.0_24	__vmm:vmname tn-demo-payment-
00:50:56:A1:8F:09	tn-demo-online-boutique-shipping-service	learned vmm	10.237.98.166	Pod-1/Node-101/eth1/30 (learned...)	vlan-1020(P) vlan-1021(S)	demo:network-segments:192.168.152.0_24	__vmm:vmname tn-demo-shipping-

Page 1 Of 1 | Objects Per Page: 100 | Displaying Objects 1 - 11 Of 11



Allowing open communication in a
Brownfield environment...

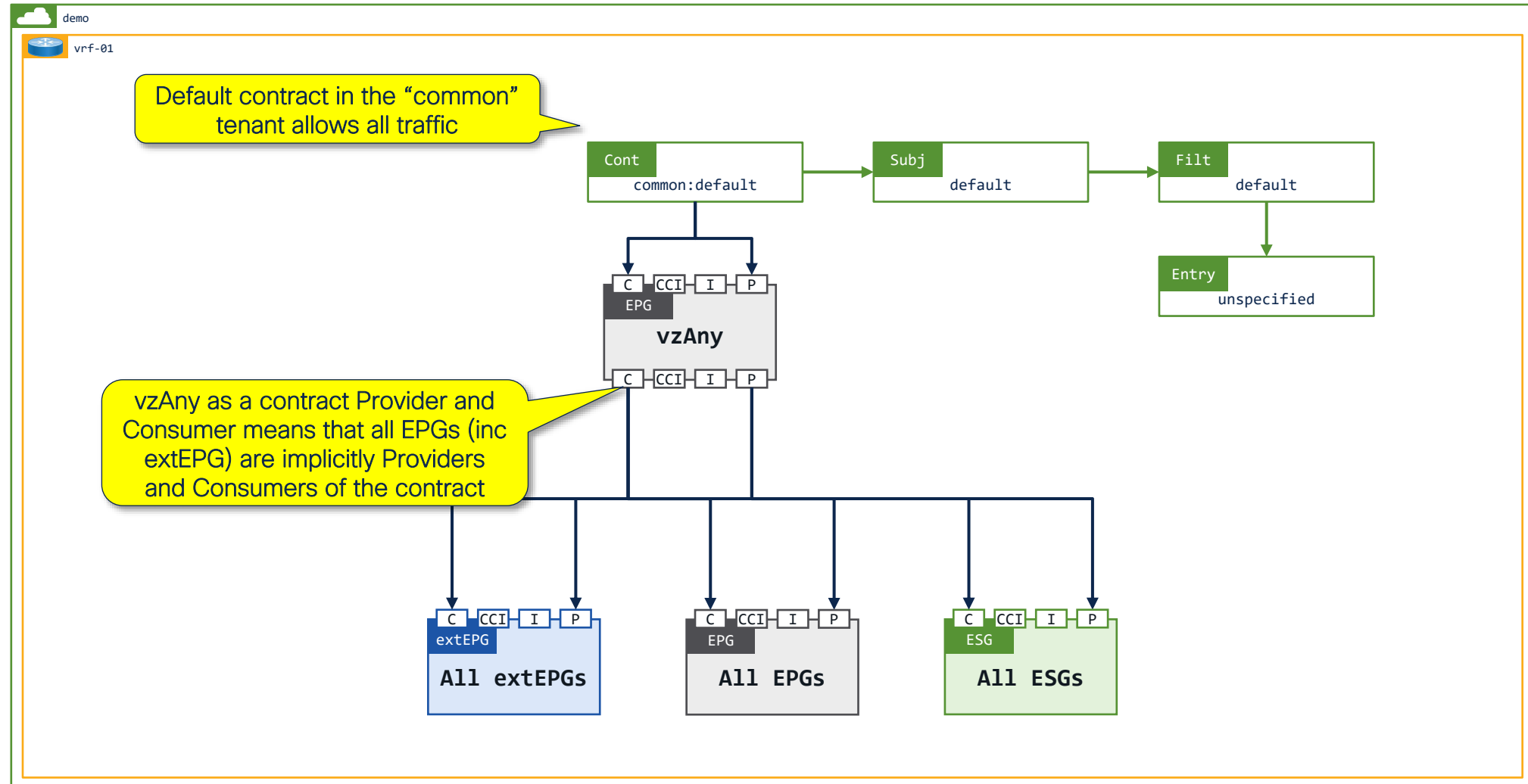
There are four options...

<https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-743951.html#Migrationexample>

- vzAny
- Preferred Groups
- EPGs mapped Endpoint Security Groups
- Disable security (not covered, because why would you...?)

vzAny operation – consumer and provider

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_KB_Use_vzAny_to_AutomaticallyApplyCommunicationRules_toEPGs.html



Preferred Groups

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_KB_Use_vzAny_to_AutomaticallyApplyCommunicationRules_toEPGs.html

There is only one preferred group per VRF

Enable Preferred Group on VRF

Typical "Network Centric" mode deployment where there is a 1:1 mapping between Bridge Domains and EPGs

pcTag 49160

Include EPG in Preferred Group

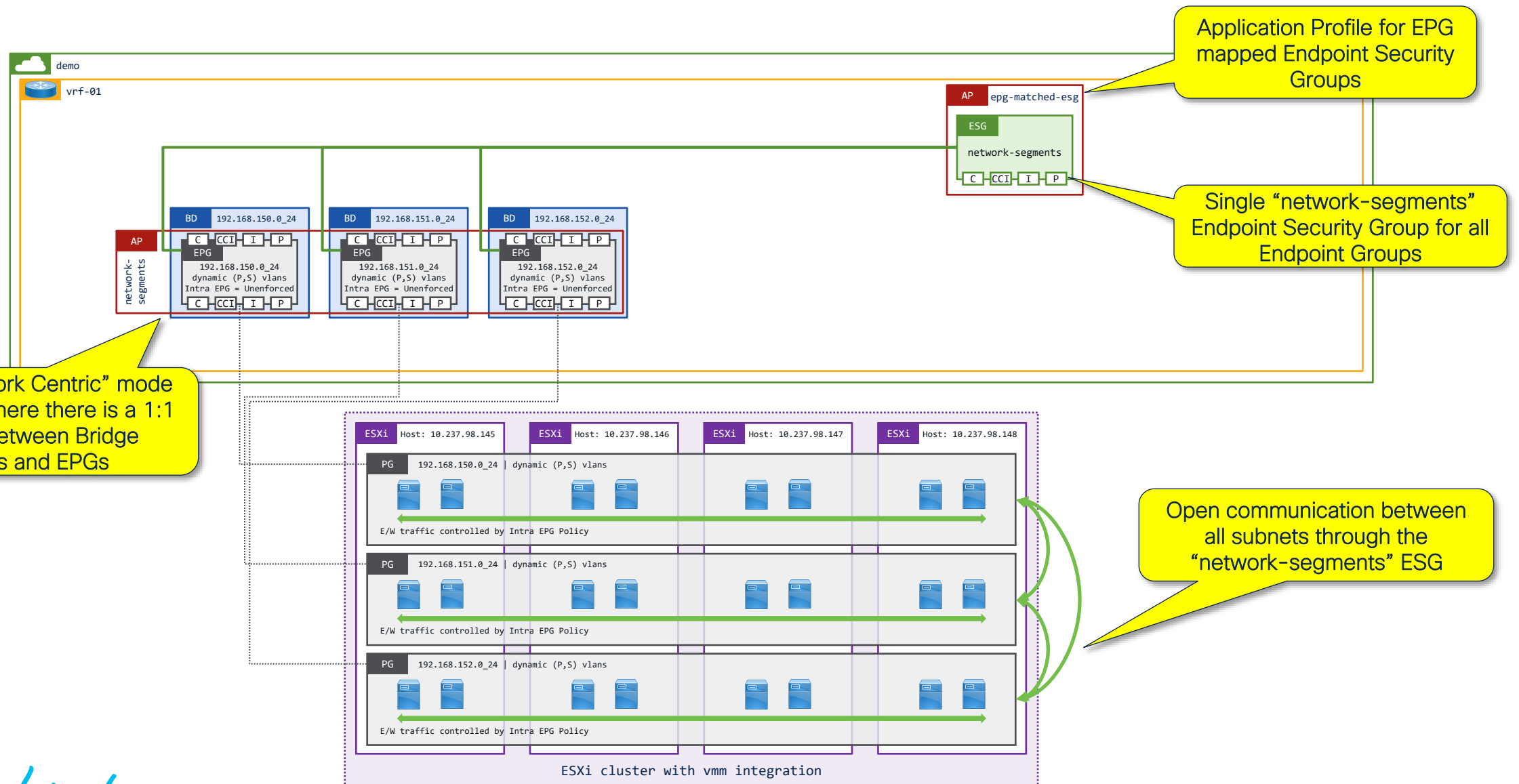
pcTag 49159

Include EPG in Preferred Group

pcTag 16393

Include EPG in Preferred Group

EPGs mapped to Endpoint Security Groups



Let's step back and look at the impact of the changes...

Bridge Domain to EPG Mapping

The screenshot shows the Cisco APIC (aci-dev-01) interface. The left sidebar contains the navigation tree with the following structure:

- demo
 - Application Profiles
 - network-segments
 - Application EPGs
 - 192.168.150.0_24
 - 192.168.151.0_24
 - 192.168.152.0_24
 - uSeg EPGs
 - Endpoint Security Groups
 - Networking
 - Bridge Domains
 - 192.168.150.0_24
 - 192.168.151.0_24
 - 192.168.152.0_24
 - VRFs
 - vrf-01
 - L2Outs
 - L3Outs
 - SR-MPLS VRF L3Outs
 - Dot1Q Tunnels
 - Contracts
 - Policies
 - Services
 - Security

The main area displays the 'Application Profile - network-segments' configuration page. The 'Topology' tab is selected, showing a diagram of the network segments. The diagram shows three EPGs (192.168.150.0_24, 192.168.151.0_24, 192.168.152.0_24) mapped to three VMM domains (V). A yellow callout box states 'Bridge Domain = EPG 1:1 mapping'. Another yellow callout box points to the VMM domains, stating 'EPGs bound to VMM Domain'.

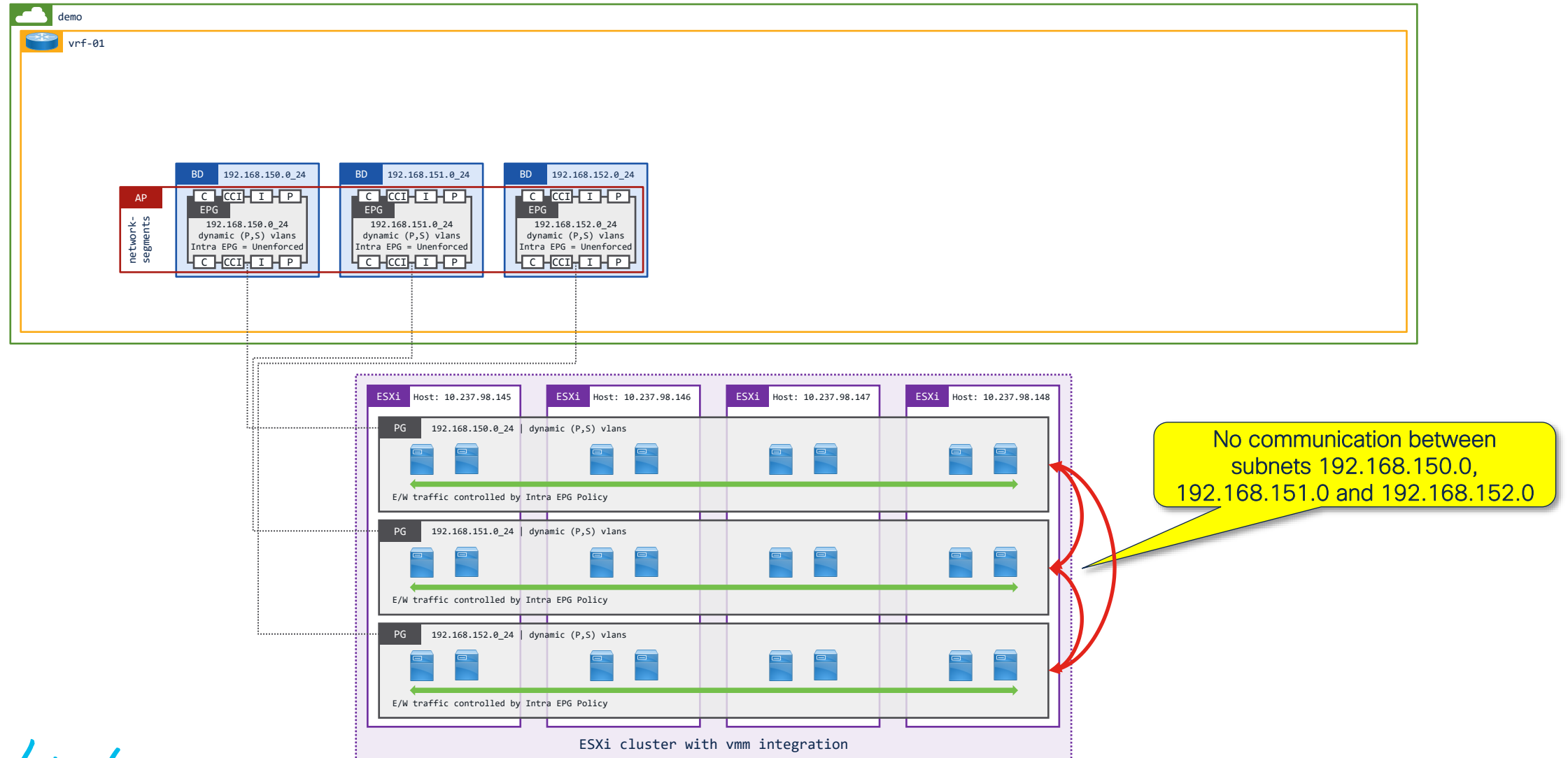
Relation Indicators

- Configured ☐ Operational ☐
- Show All ☐ On Click ☐
- Show VRF on EPG: ☐

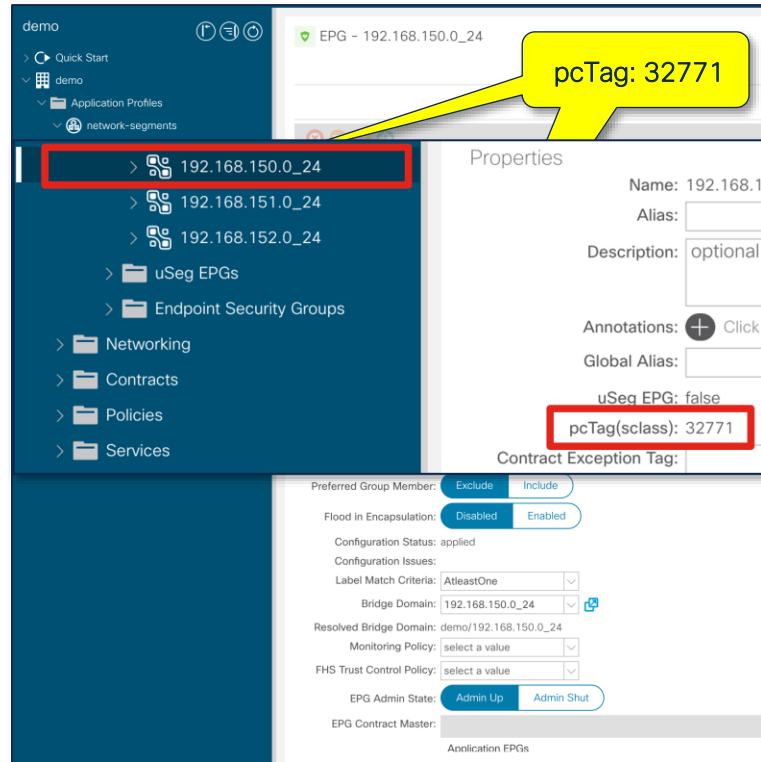
Provider

- Consumer
- Intra EPG/ESG
- Provider (from Master)
- Consumer (from Master)
- Intra EPG/ESG (from Master)
- Master EPG/ESG

Isolated groups of workloads



Each EPG has a unique security Tag (pcTag)



This screenshot shows the configuration page for EPG 192.168.150.0_24. A yellow callout bubble points to the EPG name in the left sidebar, stating "pcTag: 32771". In the "Properties" section, the "pcTag(sclass)" field is highlighted with a red box and contains the value "32771".

demo

EPG - 192.168.150.0_24

pcTag: 32771

Properties

Name: 192.168.150.0_24

Alias:

Description: optional

Annotations: + Click

Global Alias:

uSeg EPG: false

pcTag(sclass): 32771

Contract Exception Tag:

Preferred Group Member: Exclude Include

Flood in Encapsulation: Disabled Enabled

Configuration Status: applied

Configuration Issues:

Label Match Criteria: AtleastOne

Bridge Domain: 192.168.150.0_24

Resolved Bridge Domain: demo/192.168.150.0_24

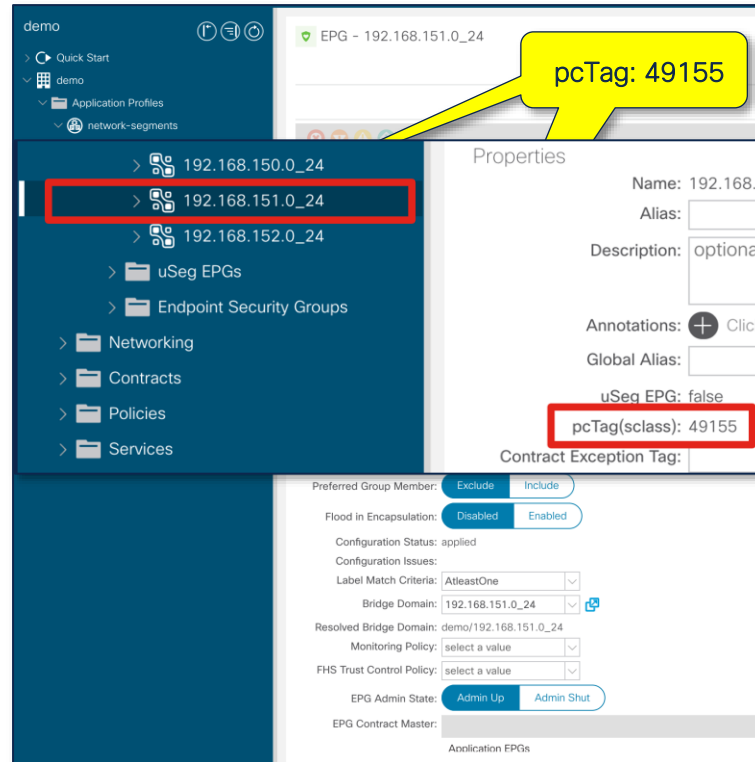
Monitoring Policy: select a value

FHS Trust Control Policy: select a value

EPG Admin State: Admin Up Admin Shut

EPG Contract Master:

Application EPGs



This screenshot shows the configuration page for EPG 192.168.151.0_24. A yellow callout bubble points to the EPG name in the left sidebar, stating "pcTag: 49155". In the "Properties" section, the "pcTag(sclass)" field is highlighted with a red box and contains the value "49155".

demo

EPG - 192.168.151.0_24

pcTag: 49155

Properties

Name: 192.168.151.0_24

Alias:

Description: optional

Annotations: + Click

Global Alias:

uSeg EPG: false

pcTag(sclass): 49155

Contract Exception Tag:

Preferred Group Member: Exclude Include

Flood in Encapsulation: Disabled Enabled

Configuration Status: applied

Configuration Issues:

Label Match Criteria: AtleastOne

Bridge Domain: 192.168.151.0_24

Resolved Bridge Domain: demo/192.168.151.0_24

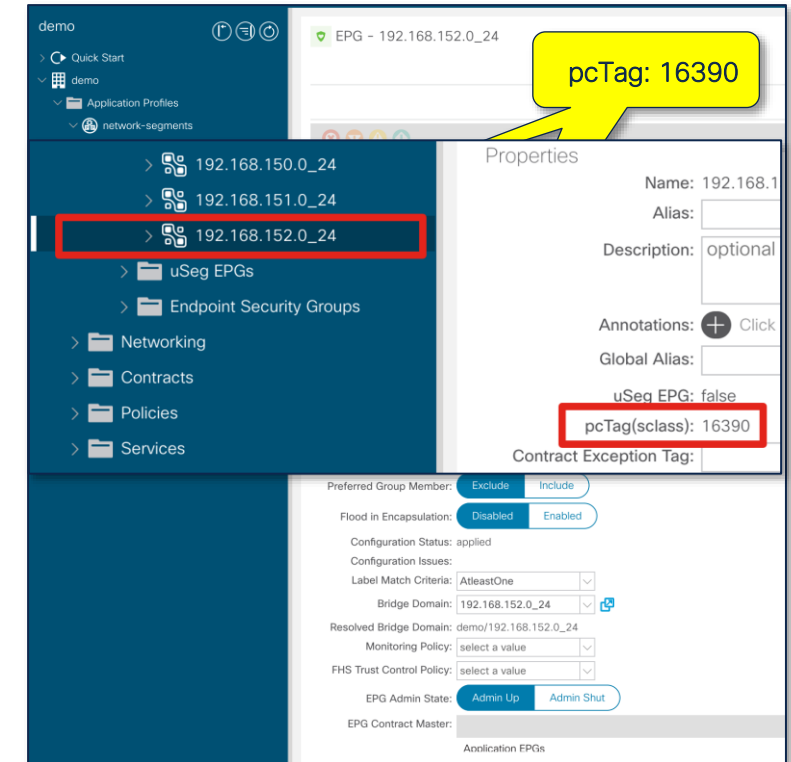
Monitoring Policy: select a value

FHS Trust Control Policy: select a value

EPG Admin State: Admin Up Admin Shut

EPG Contract Master:

Application EPGs



This screenshot shows the configuration page for EPG 192.168.152.0_24. A yellow callout bubble points to the EPG name in the left sidebar, stating "pcTag: 16390". In the "Properties" section, the "pcTag(sclass)" field is highlighted with a red box and contains the value "16390".

demo

EPG - 192.168.152.0_24

pcTag: 16390

Properties

Name: 192.168.152.0_24

Alias:

Description: optional

Annotations: + Click

Global Alias:

uSeg EPG: false

pcTag(sclass): 16390

Contract Exception Tag:

Preferred Group Member: Exclude Include

Flood in Encapsulation: Disabled Enabled

Configuration Status: applied

Configuration Issues:

Label Match Criteria: AtleastOne

Bridge Domain: 192.168.152.0_24

Resolved Bridge Domain: demo/192.168.152.0_24

Monitoring Policy: select a value

FHS Trust Control Policy: select a value

EPG Admin State: Admin Up Admin Shut

EPG Contract Master:

Application EPGs

Enable Endpoint Security Groups

demo

Domains (VMs and Bare-Metals)

Domain	Type	Deployment	Resolution	Allow Micro-Segmentation	Primary VLAN	Port Encap	Switching Mode	Encap Mode	Cos Value	Enhanced Lag Policy	Custom EPG Name
VMware/ucsc-c22...	VMM Domain	On Demand	Immediate	True			native	Auto	Cos0		

demo

Domains (VMs and Bare-Metals)

Domain	Type	Deployment	Resolution	Allow Micro-Segmentation	Primary VLAN	Port Encap	Switching Mode	Encap Mode	Cos Value	Enhanced Lag Policy	Custom EPG Name
VMware/ucsc-c22...	VMM Domain	On Demand	Immediate	True			native	Auto	Cos0		

demo

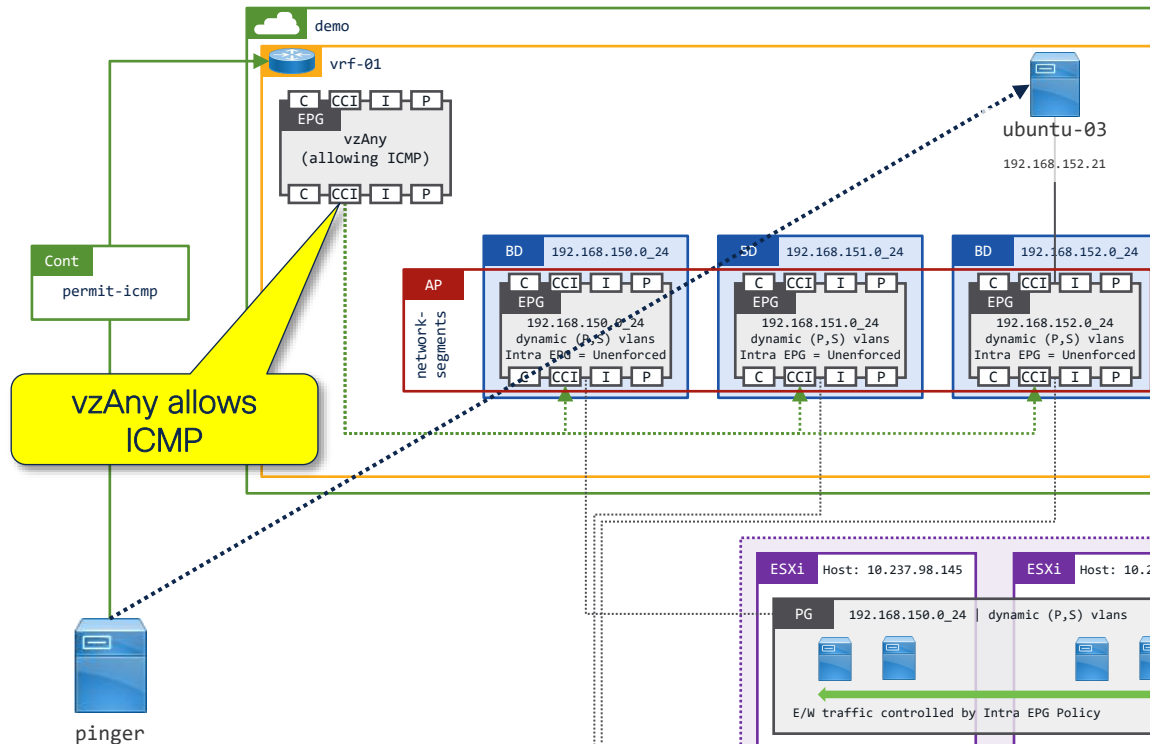
Domains (VMs and Bare-Metals)

Domain	Type	Deployment	Resolution	Allow Micro-Segmentation	Primary VLAN	Port Encap	Switching Mode	Encap Mode	Cos Value	Enhanced Lag Policy	Custom EPG Name
VMware/ucsc-c22...	VMM Domain	On Demand	Immediate	True			native	Auto	Cos0		

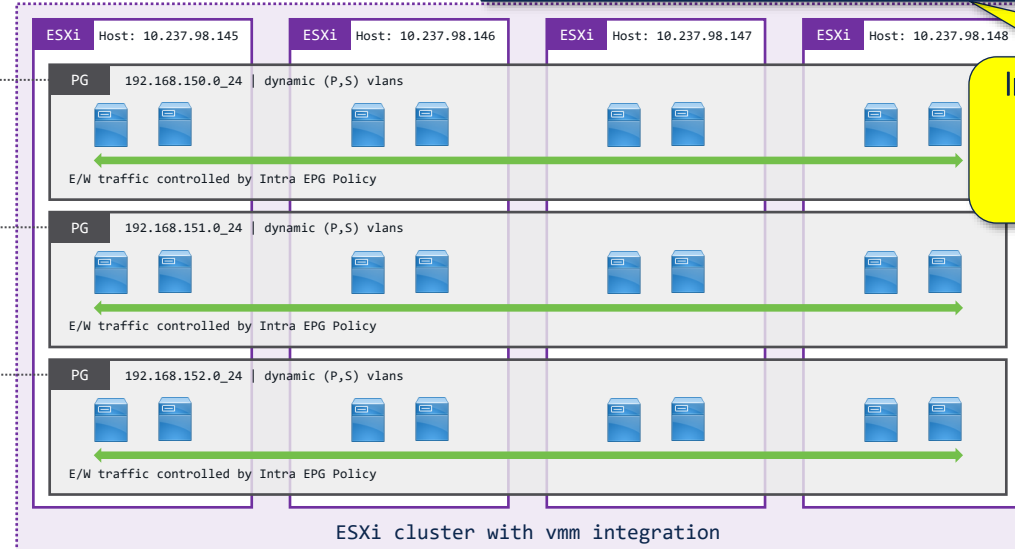
Primary/Port Encap VLANs not required for directly attached hosts

Static Primary / Encap VLANs are required with intermediary switching layer such as UCS FIs

ESGs allow control E/W traffic within the Hypervisor

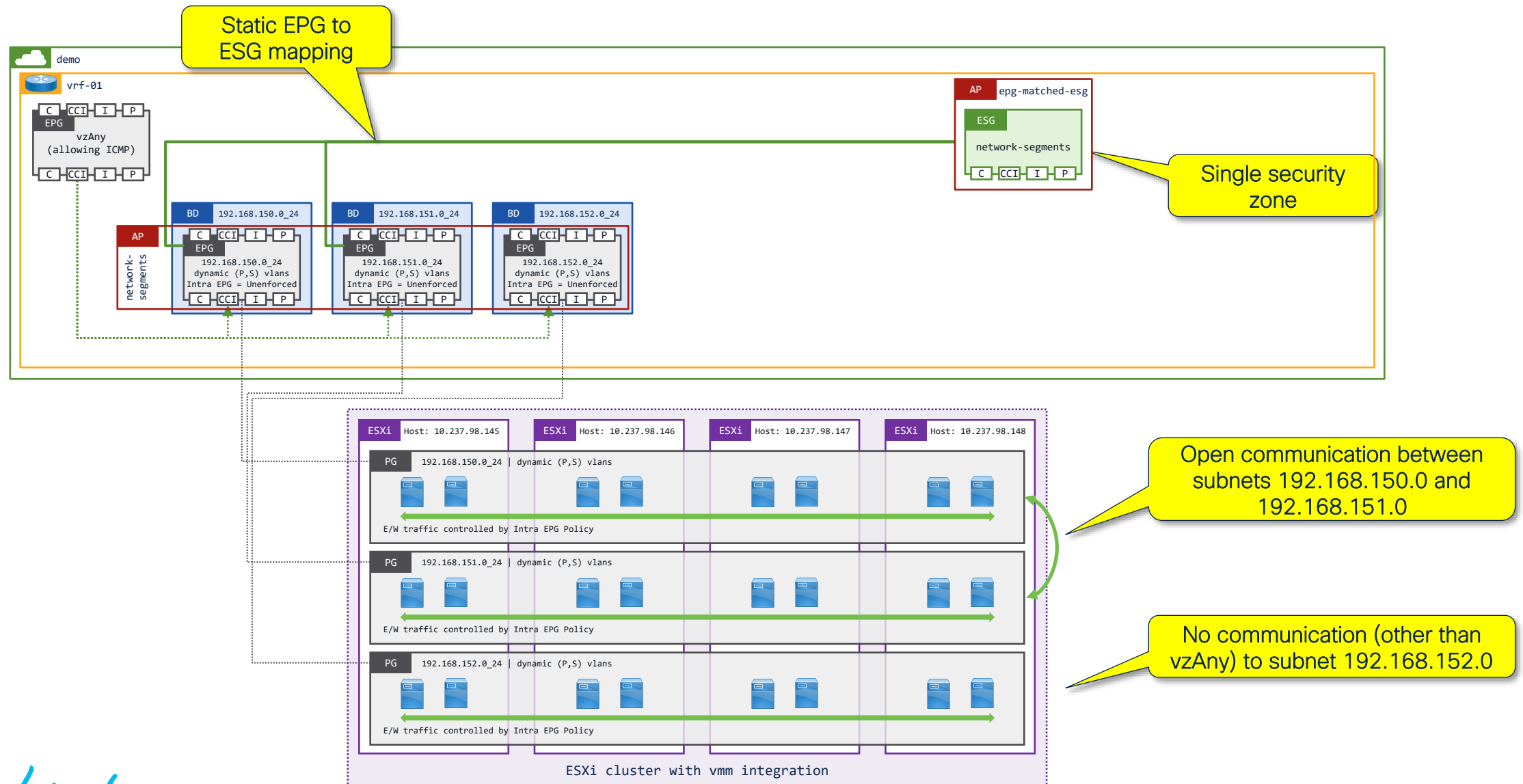


The top screenshot shows the APIC (aci-dev-01) interface. The 'demo' tab is selected, and the 'EPG - 192.168.152.0_24' is highlighted. The 'Client Endpoints' table shows a list of endpoints, with one entry highlighted in red: '192.168.152.21' with MAC '00:50:56:A1:78:64' and name 'ubuntu-03'. The bottom screenshot shows the vSphere Client interface. The 'demo' tab is selected, and the 'network-segments/192.168.152.0_24' is highlighted. The 'Ports' tab shows a list of ports, with one entry highlighted in red: '1091' with 'Static binding' and 'Elastic'.



Let's create an EPG matched Security Group...

Create EPG matched Security Group



Create Application Profile for Security Groups

New Application Profile for Security Groups

Create Application Profile

Create Application Profile

Name: epg-matched-security-group

Alias:

Description: optional

Annotations: Click to add a new annotation

Monitoring Policy: select a value

EPGs

Name	Alias	BD	Domain	Switching Mode	Static Path	Static Path VLAN	Provided Contract	Consumed Contract
------	-------	----	--------	----------------	-------------	------------------	-------------------	-------------------

Cancel Submit

epg-matched-security-groups

Do not create EPGs

Create new ESG for Network Segments

Create new ESG

Enter ESG name "group-01"

Select the VRF for the ESG to be applied against

Add EPGs

Select one or more EPGs

Allow Intra ESG traffic i.e. permit traffic between EPGs

Finish

The screenshots show the following steps in the APIC GUI:

- Navigation:** From the APIC dashboard, navigate to **Tenants** > **demo** > **network-segments** > **Create Endpoint Security Group**.
- STEP 1 > Identity:** Set **Name** to `network-segments` and **VRF** to `vrf-01`.
- STEP 2 > Selectors:** Click **+** to add EPGs. Select the desired EPGs from the list.
- STEP 3 > Advanced (Optional):** Set **Intra ESG Isolation** to **Unenforced** to allow traffic between EPGs.
- Finish:** Click the **Finish** button to complete the creation.

Matched EPGs now classified with a common pcTag

demo

- Quick Start
- demo
 - Application Profiles
 - esg-matched-security-groups
 - network-segments
 - Application EPGs
 - 192.168.150.0_24 [ESG matc.]
 - 192.168.151.0_24 [ESG matc.]
 - 192.168.152.0_24
 - uSeg EPGs
 - Endpoint Security Groups
 - Networking
 - Contracts
 - Policies
 - Services
 - Security

EPG - 192.168.150.0_24 (Matched)

Properties

Name: 192.168.150.0_24

Alias:

Description: optional

Annotations: Click to add a new annotation

Global Alias:

uSeg EPG: false

pcTag(class): 31

Contract Exception Tag:

QoS class: Level3 (Default)

Custom QoS: select a value

Data-Plane Policer: select a value

Intra EPG Isolation: Enforced Unenforced

Preferred Group Member: Exclude Include

Flood in Encapsulation: Disabled Enabled

Configuration Status: applied

Configuration Issues:

Label Match Criteria: AtleastOne

Bridge Domain: 192.168.150.0_24

Resolved Bridge Domain: demo/192.168.150.0_24

Monitoring Policy: select a value

FHS Trust Control Policy: select a value

EPG Admin State: Admin Up Admin Shut

EPG Contract Master:

Application EPGs

pcTag: 31

demo

- Quick Start
- demo
 - Application Profiles
 - esg-matched-security-groups
 - network-segments
 - Application EPGs
 - 192.168.150.0_24 [ESG matc.]
 - 192.168.151.0_24 [ESG matc.]
 - 192.168.152.0_24
 - uSeg EPGs
 - Endpoint Security Groups
 - Networking
 - Contracts
 - Policies
 - Services
 - Security

EPG - 192.168.151.0_24 (Matched)

Properties

Name: 192.168.151.0_24

Alias:

Description: optional

Annotations: Click to add a new annotation

Global Alias:

uSeg EPG: false

pcTag(class): 31

Contract Exception Tag:

QoS class: Level3 (Default)

Custom QoS: select a value

Data-Plane Policer: select a value

Intra EPG Isolation: Enforced Unenforced

Preferred Group Member: Exclude Include

Flood in Encapsulation: Disabled Enabled

Configuration Status: applied

Configuration Issues:

Label Match Criteria: AtleastOne

Bridge Domain: 192.168.151.0_24

Resolved Bridge Domain: demo/192.168.151.0_24

Monitoring Policy: select a value

FHS Trust Control Policy: select a value

EPG Admin State: Admin Up Admin Shut

EPG Contract Master:

Application EPGs

pcTag: 31

demo

- Quick Start
- demo
 - Application Profiles
 - esg-matched-security-groups
 - network-segments
 - Application EPGs
 - 192.168.150.0_24 [ESG matc.]
 - 192.168.151.0_24 [ESG matc.]
 - 192.168.152.0_24
 - uSeg EPGs
 - Endpoint Security Groups
 - Networking
 - Contracts
 - Policies
 - Services
 - Security

EPG - 192.168.152.0_24

Properties

Name: 192.168.152.0_24

Alias:

Description: optional

Annotations: Click to add a new annotation

Global Alias:

uSeg EPG: false

pcTag(class): 49157

Contract Exception Tag:

QoS class: Level3 (Default)

Custom QoS: select a value

Data-Plane Policer: select a value

Intra EPG Isolation: Enforced Unenforced

Preferred Group Member: Exclude Include

Flood in Encapsulation: Disabled Enabled

Configuration Status: applied

Configuration Issues:

Label Match Criteria: AtleastOne

Bridge Domain: 192.168.152.0_24

Resolved Bridge Domain: demo/192.168.152.0_24

Monitoring Policy: select a value

FHS Trust Control Policy: select a value

EPG Admin State: Admin Up Admin Shut

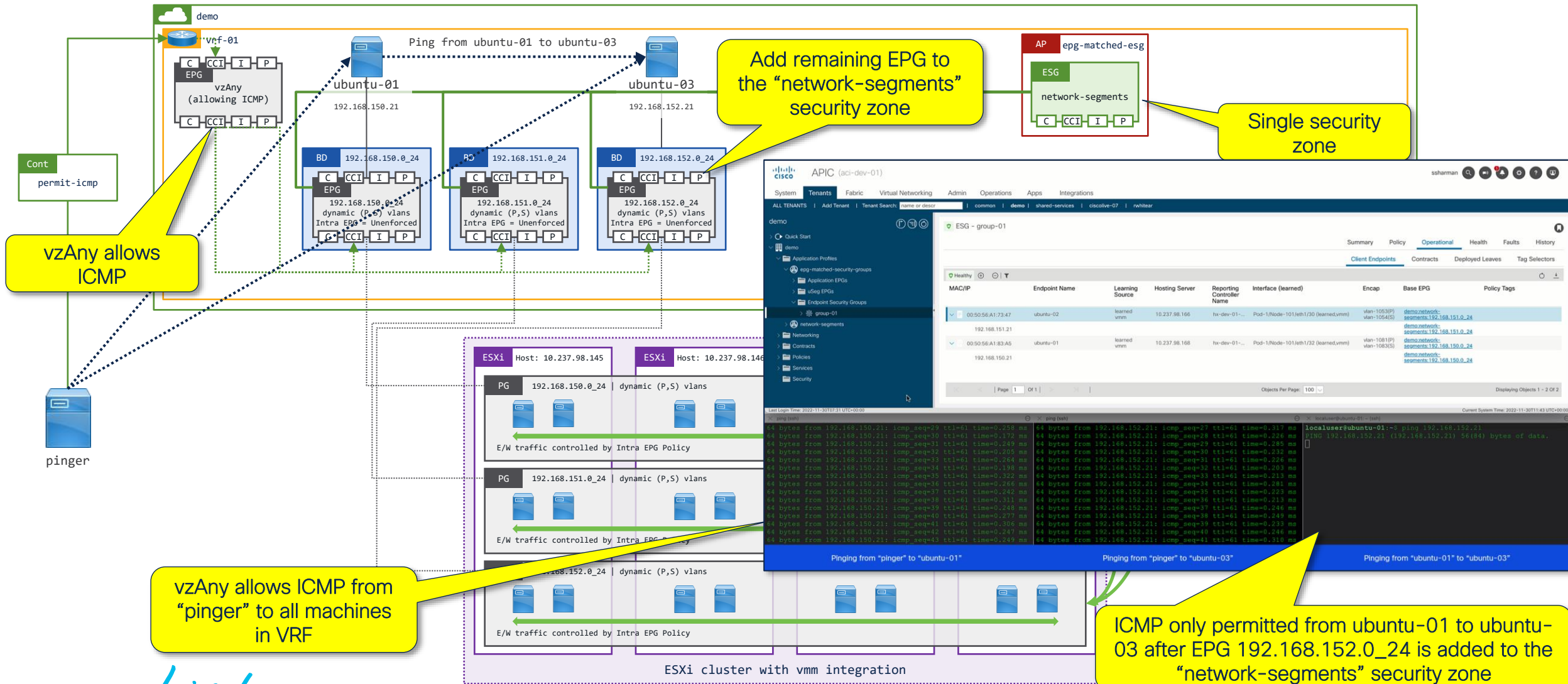
EPG Contract Master:

Application EPGs

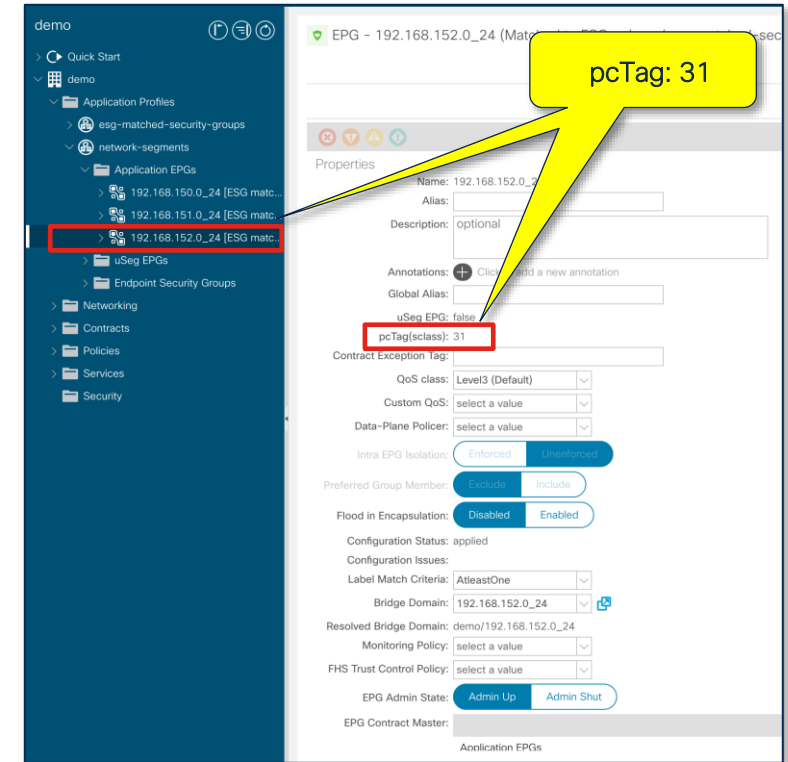
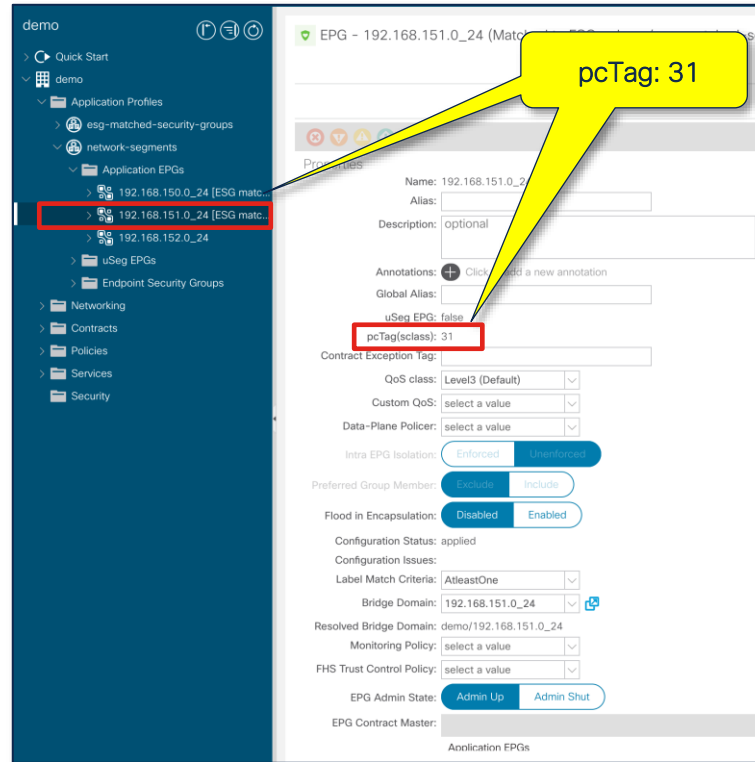
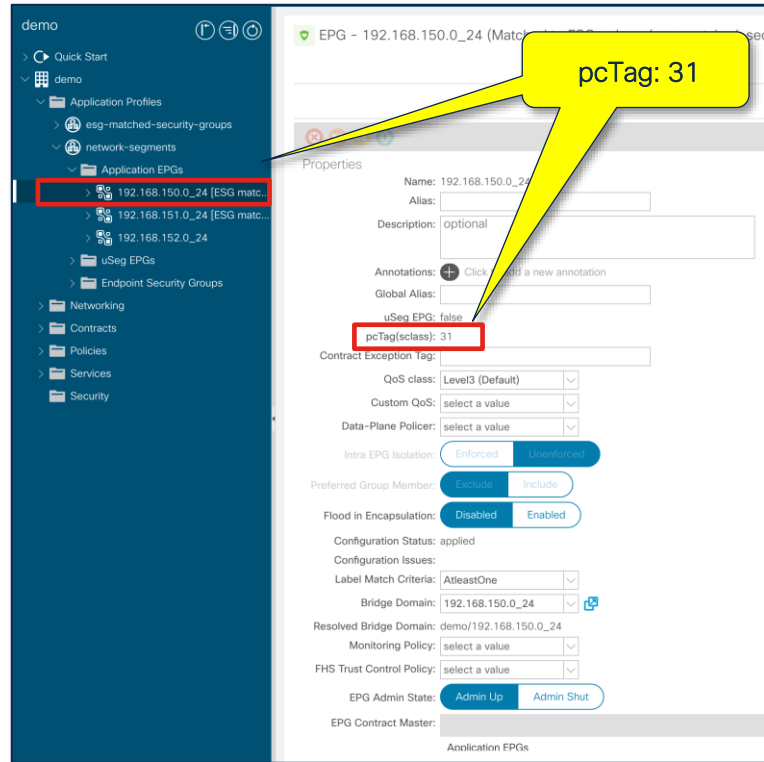
pcTag: 49157

Let's add the remaining EPG to the Security Group...

Add remaining EPG to Single Security Zone

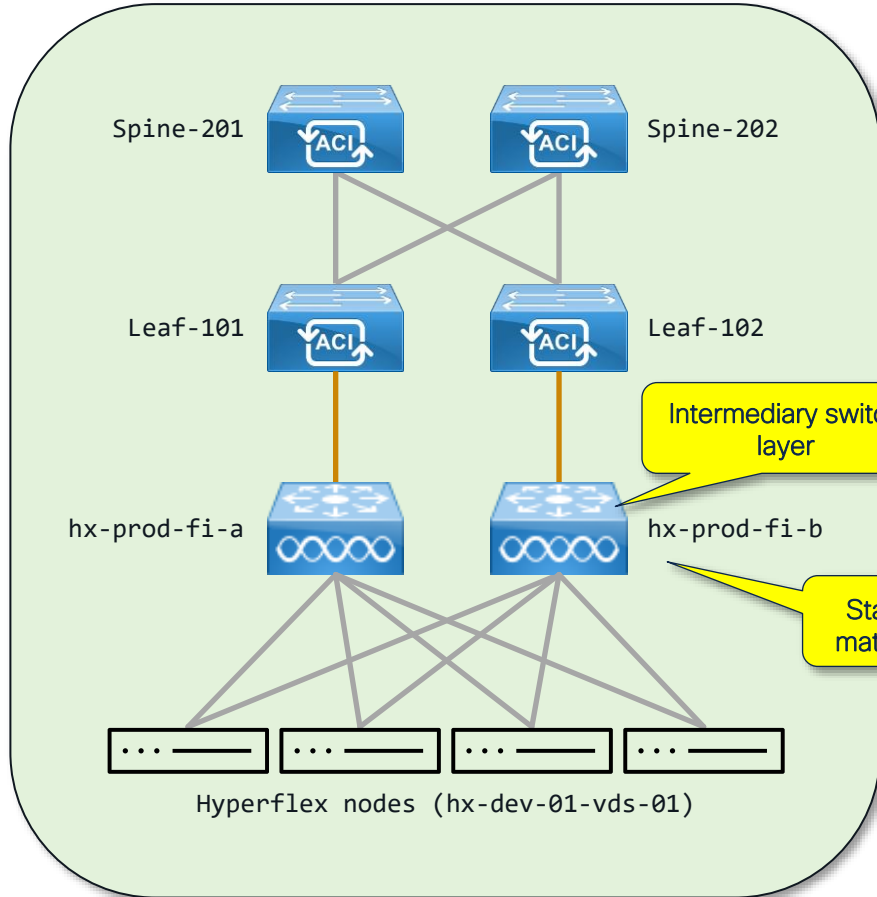


All EPGs now classified with a common pcTag



What if there is an intermediary switch layer...?

Define static PVLANS for VMM Domains



APIC

System Tenants Fabric

Inventory Fabric Policies

Policies

- Quick Start
- Interface Configuration
- Switches
- Modules
- Interfaces
- Policies
- Physical and External Domains
- VLAN
- all-vlans (Dynamic Allocation)
- Multicast Address

UCS Manager

LAN / LAN Cloud / VLANs

VLANs

Name	ID
VLAN aci-vds-pvlan-primary-1217 (1217)	1217
VLAN aci-vds-pvlan-isolated-1218 (1218)	1218

Add PVLANS to UCSM

Name: all-vlans

Description: optional

Allocation Mode: Dynamic Allocation

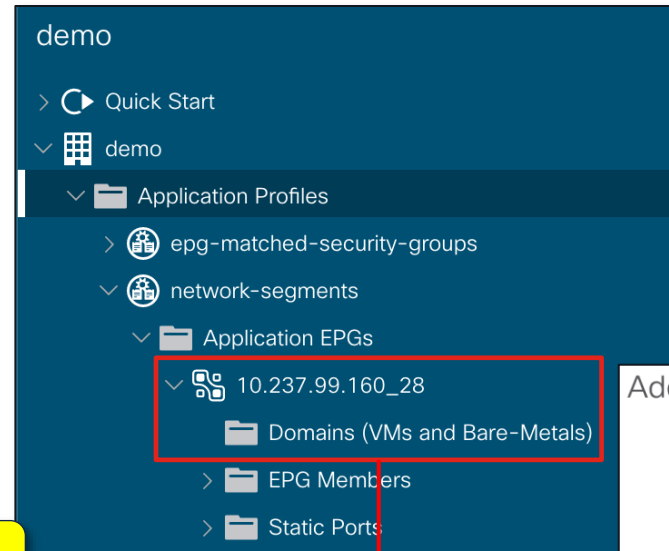
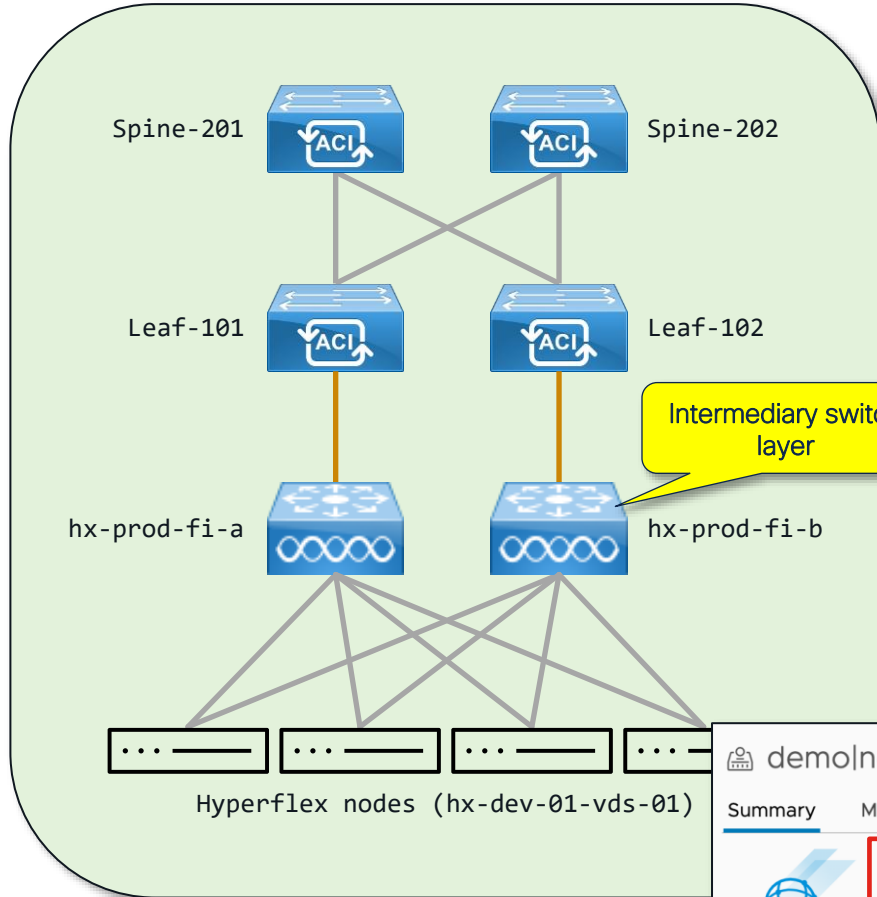
VLAN Range	Description	Allocation Mode	Role
[1217]	hx-dev-01-vds-01 primary vlan	Static Allocation	External or On the wire encapsulations
[1218]	hx-dev-01-vds-01 isolated vlan	Static Allocation	External or On the wire encapsulations
[1219]	hx-dev-01-vds-01 primary vlan	Static Allocation	External or On the wire encapsulations

Domains:

Name	Type
VMware/ucsc-c220m5-vds-01	VMM Domain
VMware/hx-dev-01-vds-01	VMM Domain

Map VLANs to VMM Domain(s)

Specify PVLANs for VMM domain



Add VMM Domain Association

VMM Domain Profile:

Deploy Immediacy: ☒ Immediate ☐ On Demand

Resolution Immediacy: ☒ Immediate ☐ On Demand ☐ Pre-provision

Delimiter:

Enhanced Lag Policy:

Allow Micro-Segmentation: ☒

Untagged VLAN Access: ☐

VLAN Mode: ☒ Dynamic ☐ Static

Primary VLAN for Micro-Seg:
For example, vlan-1

Secondary VLAN for Micro-Seg:
For example, vlan-1

Port Binding: ☒ Dynamic Binding ☐ Ephemeral ☐ Default ☐ Static Binding

Netflow: ☒ Disable ☐ Enable

Allow Promiscuous:

Forged Transmits:

MAC Changes:

Active Uplinks Order:

demo|network-segments|10.237.99.160_28

Summary	Monitor	Configure	Permissions	Ports	Hosts	VMs
	Port binding	Static binding				
	Port allocation	Elastic				
	Private VLAN	Isolated (1217, 1218)				

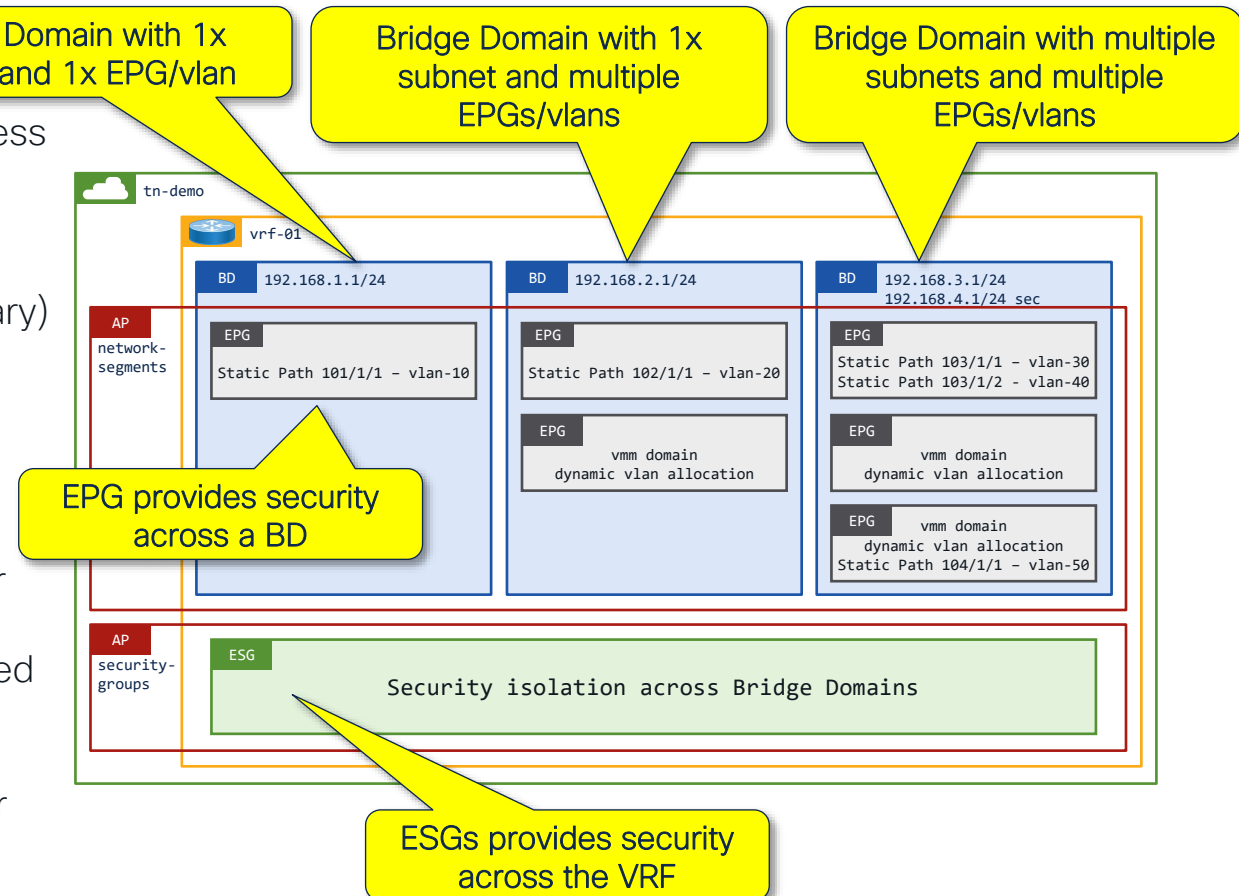
Security across Bridge Domains with ESGs



EPG Security vs ESG Security

ACI foundational building blocks:

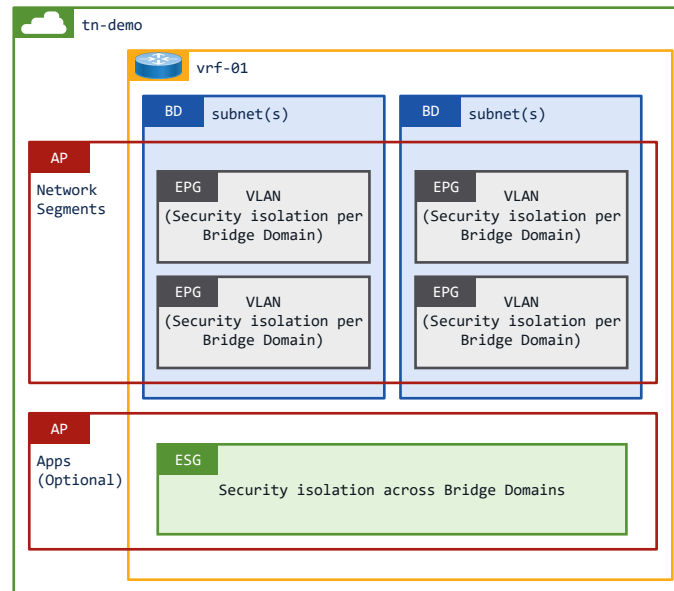
- A **Tenant** provides an RBAC boundary typically linked to a business function
- A **VRF** is mapped to a single Tenant
- A **Bridge Domain** is mapped to a single VRF
- A **Bridge Domain** provides one or more IP gateways (IP secondary)
- An EPG is mapped to a single Bridge Domain
- **An EPG provides network backing and maps to:**
 - VMM domains + static or dynamic VLAN(s)
 - Static path(s) + static VLAN(s)
- **An EPG defines a security boundary on a Bridge Domain**
- An EPG allows open communication for endpoints in the EPG, or (optionally) blocked communication for endpoints in the EPG
- Inter EPG communication requires contracts (typically not required when using ESGs)
- **An ESG forms a security boundary on a VRF**
- An **ESG** allows open communication for endpoints in the **ESG**, or (optionally) blocked communication for endpoints in the **ESG**
- Inter **ESG** communication requires contracts
- **ESG contracts supersede EPG contracts**



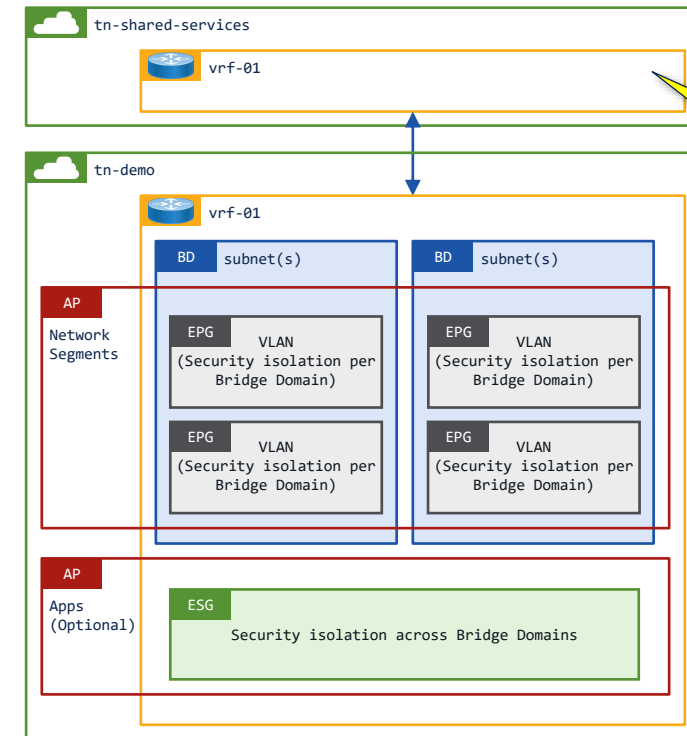
How do you map Endpoints into an ESG...?

Select a Design Pattern, then enable Proxy ARP and map your Endpoints to the ESG...

Design Patterns



EPG and ESG in the “user” Tenant with a dedicated L3out

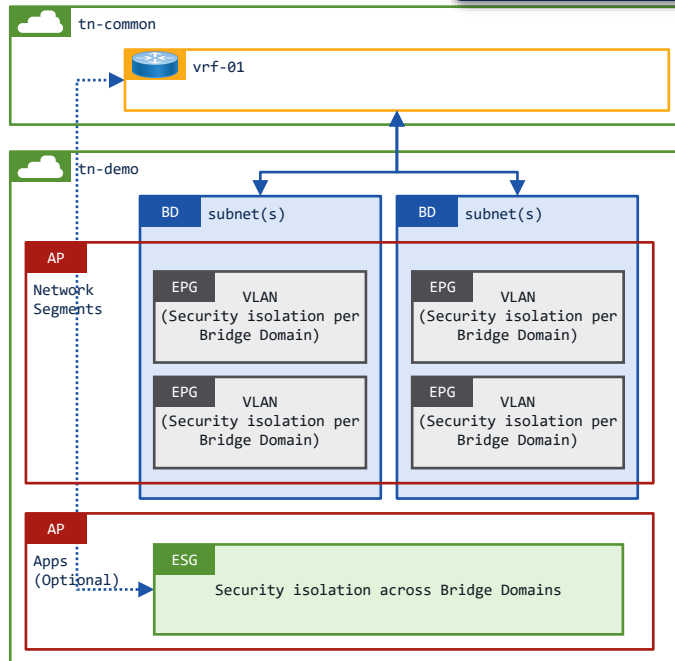


EPG and ESG in the “user” Tenant with a Shared L3out

Network team controls inbound/outbound routing

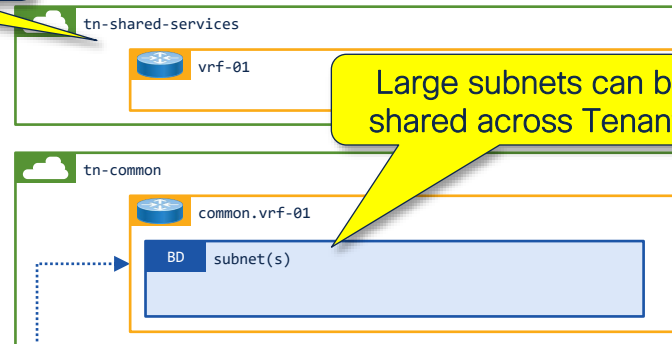
Design Patterns

Network team controls inbound/outbound routing

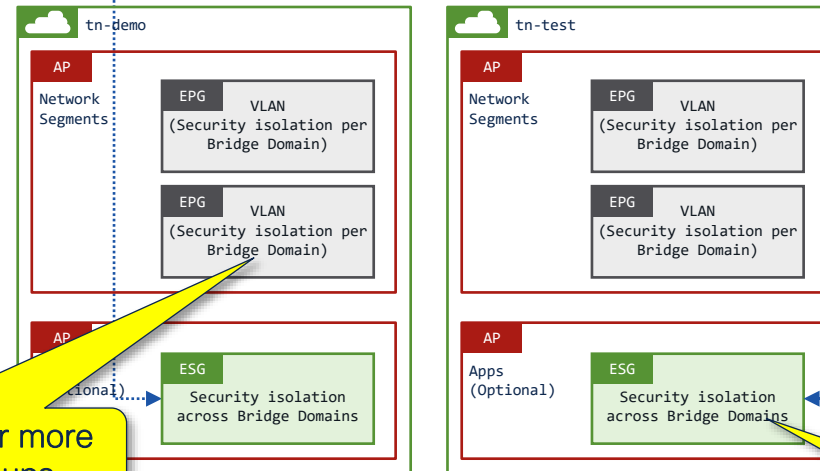


EPG and ESG in the “user” Tenant with the VRF in the “common” Tenant

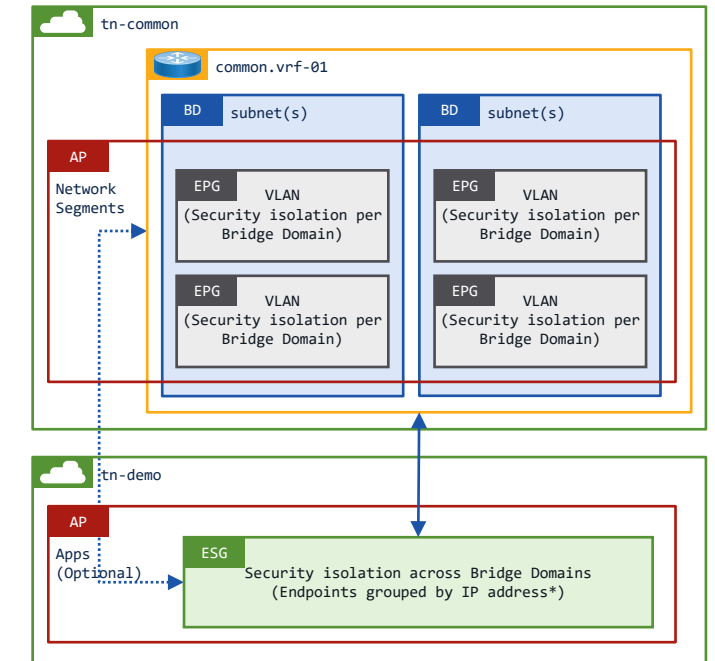
Each Tenant has one or more network security groups



Large subnets can be shared across Tenants



EPG and ESG in the “user” Tenant with the VRF in the “common” Tenant, and a Shared L3out in shared-services



EPG in the “common” Tenant with ESG in “user” Tenant

Each Tenant has one or more endpoint security groups

How do you enable Proxy ARP on the Leaf Switches...?

Enabling "Allow Micro-Segmentation" automatically enables Proxy ARP. Option in a 100% virtual deployment, use with or without Intra EPG isolation

Edit VMM Domain Association - VMware/ucsc-c220m5-vds-01

Deploy Immediacy: ☐ Immediate ☐ On Demand

Resolution Immediacy: ☐ Immediate ☐ On Demand ☐ Pre-provision

Delimiter:

Enhanced Lag Policy:

Allow Micro-Segmentation: ☒

Untagged VLAN Access: ☐

VLAN Mode: ☐ Dynamic ☐ Static

Port Binding: ☐ Dynamic Binding ☐ Ephemeral ☐ Default ☐ Static Binding

Netflow: ☐ Disable ☐ Enable

Allow Promiscuous:

Forged Transmits:

MAC Changes:

Active Uplinks Order:

Standby Uplinks:

Custom EPG Name:

demo|network-segments|192.168.150.0_24 ACTIONS

Summary Monitor Configure Permissions Ports Hosts VMs

Port binding Static binding

Port allocation Elastic

VLAN ID 1046

demo|network-segments|192.168.150.0_24 ACTIONS

Summary Monitor Configure Permissions Ports Hosts VMs

Port binding Static binding

Port allocation Elastic

Private VLAN Isolated (1094, 1095)

Enable Intra EPG isolation with Proxy ARP if you have a mixed virtual and physical environment

Enabling Intra EPG isolation / Allow Micro-Segmentation configures PVLANS on the port group

Proxy ARP is only available when Intra ESG isolation is enabled

Add an Intra EPG Contract

Properties

Name: 192.168.150.0_24

Alias:

Description: optional

Annotations: Click to add a new annotation

Global Alias:

uSeg EPG: false

pcTag(sclass): 16390

Exception Tag:

QoS class:

Custom QoS:

Data-Plane Policer:

Intra EPG Isolation: ☐ Enforced ☐ Unenforced

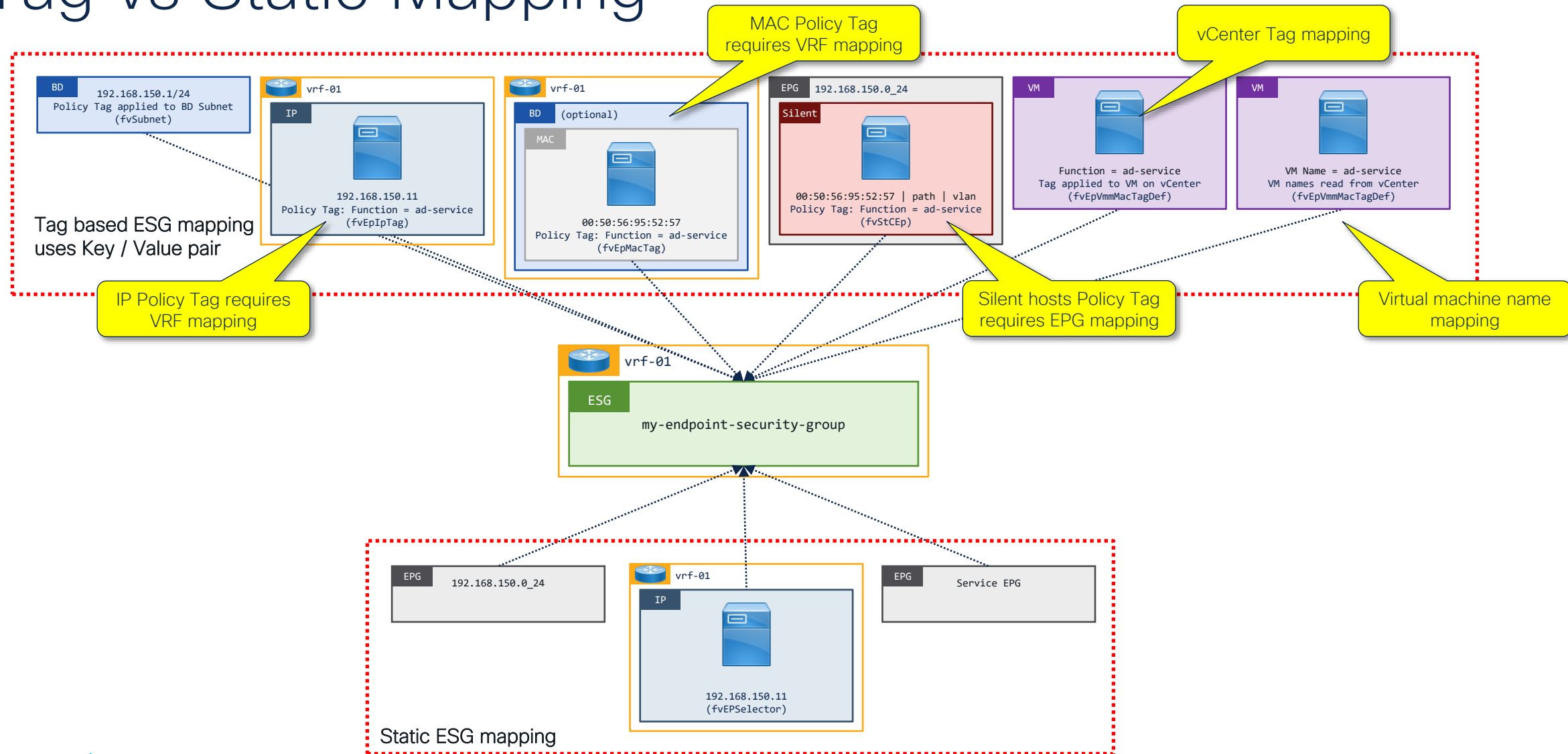
Forwarding Control: ☒ proxy-arp

Preferred Group Member: ☐ Exclude ☐ Include

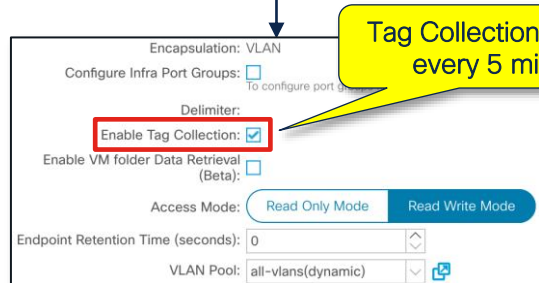
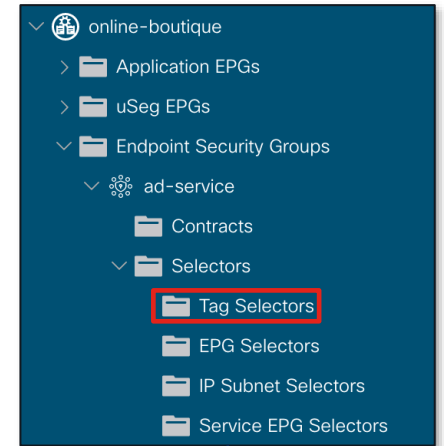
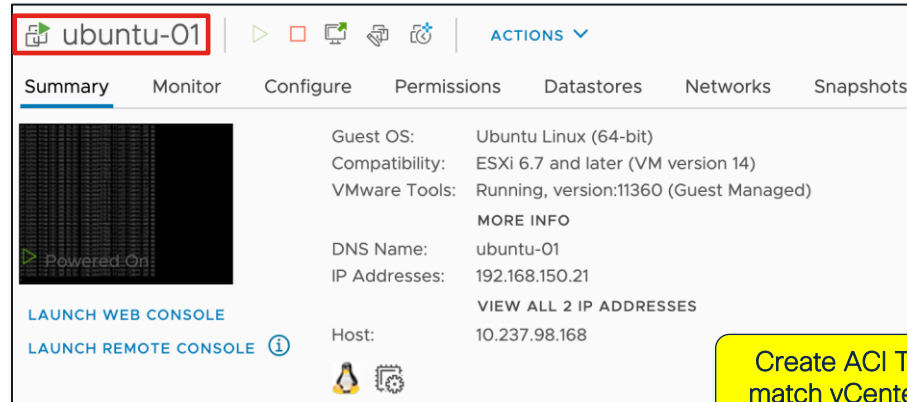
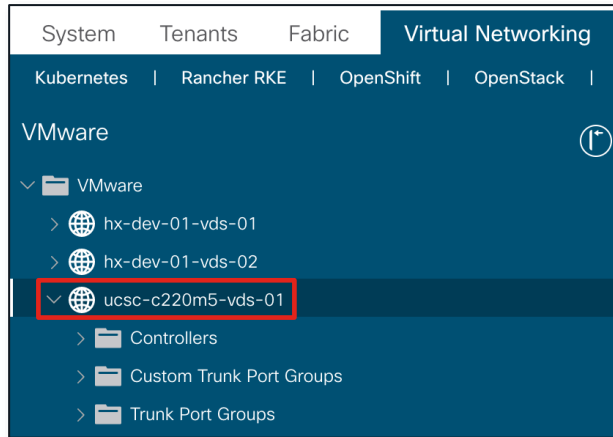
Flood In Encapsulation: ☐ Disabled ☐ Enabled

Name	Tenant	Contract Type
Contract Type: Intra EPG Contract		
permit-any	demo	Intra EPG Contract

Tag vs Static Mapping



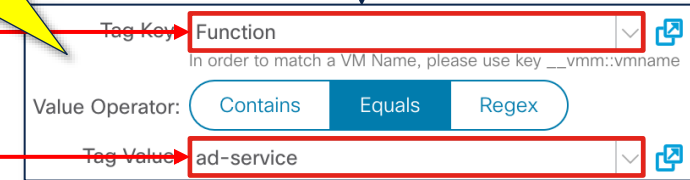
Dynamic Policy Tag matching from vCenter



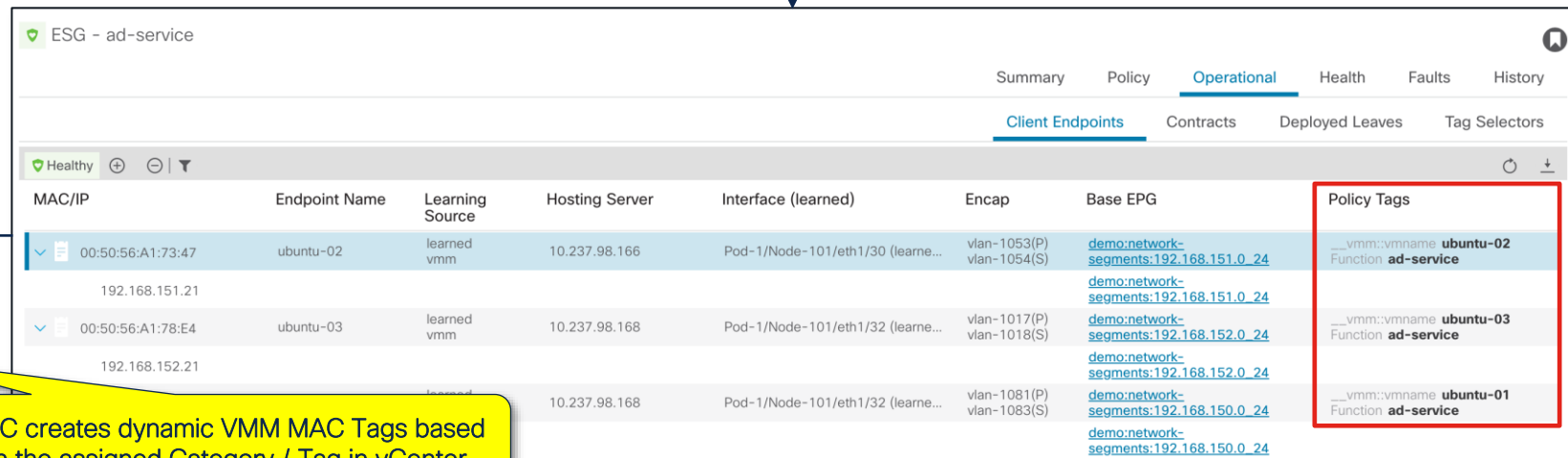
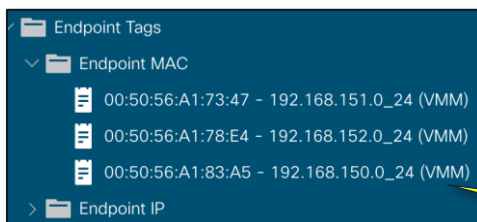
Tag Collection runs every 5 min



Create ACI Tags to match vCenter Tags



Tenant → Policies → Endpoint Tags



APIC creates dynamic VMM MAC Tags based on the assigned Category / Tag in vCenter

Static Mapping of EPGs to ESGs

ESG Selectors provide similar functionality to vzAny / Preferred Groups

ESG tied to either the “user” tenant VRF or a VRF in “common”

Create an EPG Selector

EPGs In ESG VRF:

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	uni/tn-demo/ap-network-segments/epg-192.168.150.0_24
<input checked="" type="checkbox"/>	uni/tn-demo/ap-network-segments/epg-192.168.151.0_24
<input checked="" type="checkbox"/>	uni/tn-demo/ap-network-segments/epg-192.168.152.0_24

Create an IP Subnet Selector

IP Subnet: 192.168.150.21

value

Description: optional

IP/subnet Selectors can select endpoints from either the “user” tenant VRF or a VRF in “common”

Create a Service EPG Selector

Service EPG: select an option

Description:

consumer
demo/c-any-g-redirect-to-ftdv-04-glg-0-4-n-N1

provider

demo/c-any-g-redirect-to-ftdv-04-glg-0-4-n-N1

Static Policy Tags on APIC

demo

- > Quick Start
- > demo
 - > Application Profiles
 - > epg-matched-security-groups
 - > **network-segments**
 - > online-boutique
 - > Networking
 - > **Bridge Domains**
 - > VRFs
 - > L2Outs
 - > L3Outs
 - > SR-MPLS VRF L3Outs
 - > Dot1Q Tunnels
 - > Contracts
 - > Policies
 - > Protocol
 - > Troubleshooting
 - > Host Protection
 - > Monitoring
 - > NetFlow
 - > VMM
 - > Endpoint Tags
 - > **Endpoint MAC**
 - > **Endpoint IP**
 - > Services
 - > Security

Static Endpoints

- > Application EPGs
 - > 192.168.150.0_24
 - > Domains (VMs and Bare-Metals)
 - > EPG Members
 - > Static Ports
 - > Static Leafs
 - > Fibre Channel (Paths)
 - > Contracts
 - > **Static Endpoint**
 - > Subnets
 - > L4-L7 Virtual IPs
 - > L4-L7 IP Address Pool

IP address ranges

- > 192.168.150.0_24
 - > DHCP Relay Labels
 - > ND Proxy Subnets
 - > Subnets
 - > **192.168.150.1/24**

MAC addresses

- > Endpoint MAC
 - > 00:50:56:A1:73:47 - *
 - > 00:50:56:A1:73:47 - 192.168.151.0_24 (VMM)
 - > 00:50:56:A1:78:E4 - *
 - > 00:50:56:A1:78:E4 - 192.168.152.0_24 (VMM)
 - > 00:50:56:A1:83:A5 - *
 - > 00:50:56:A1:83:A5 - 192.168.150.0_24 (VMM)

IP addresses

- > Endpoint IP
 - > 192.168.150.21
 - > 192.168.151.21
 - > 192.168.152.21

Policy Tags: + Click to add a new tag

Function **ad-service** X

online-boutique

- > Application EPGs
- > uSeg EPGs
- > Endpoint Security Groups
 - > **ad-service**
 - > Contracts
 - > Selectors
 - > **Tag Selectors**
 - > EPG Selectors
 - > IP Subnet Selectors
 - > Service EPG Selectors

Associated Object

Stats	Health	Faults	History
packets	Policy Tags	Resource IDs	
uni/tn-demo/BD-192.168.151.0_24/subnet-[192.168.151.1/24]			
uni/tn-demo/BD-192.168.150.0_24/subnet-[192.168.150.1/24]			
uni/tn-demo/BD-192.168.152.0_24/subnet-[192.168.152.1/24]			
uni/tn-demo/eptags/epiptag-[192.168.150.21]-vrf-01			
uni/tn-demo/eptags/epiptag-[192.168.151.21]-vrf-01			
uni/tn-demo/eptags/epmactag-00:50:56:A1:73:47-[*]			
uni/tn-demo/eptags/epmactag-00:50:56:A1:83:A5-[*]			
uni/tn-demo/eptags/epmactag-00:50:56:A1:78:E4-[*]			

Selector Precedence

For Switched Traffic:

Precedence Order	Selector
1	Tag Selector (Endpoint MAC Tag) Tag Selector (Static Endpoint)
2	Tag Selector (VMM Endpoint MAC Tag)
3	EPG Selector

For Routed Traffic:

Precedence Order	Selector
1	Tag Selector (Endpoint IP Tag) IP Subnet Selector (host IP)
2	Tag Selector (BD Subnet) IP Subnet Selector (subnet)
3	Tag Selector (Endpoint MAC Tag) Tag Selector (Static Endpoint)
4	Tag Selector (VMM Endpoint MAC Tag)
5	EPG Selector

ESG Contract Matrix

Source/Destination	Source/Destination*	Supported
ESG	ESG	Yes
ESG	EPG	No**
ESG	L3out extEPG	Yes
ESG	Shared L3out extEPG	Yes
ESG	Preferred Group	No
ESG	vzAny	Yes

*includes L4-L7 Service Graphs

**use EPG → ESG mapping

ESGs: The Hidden Details



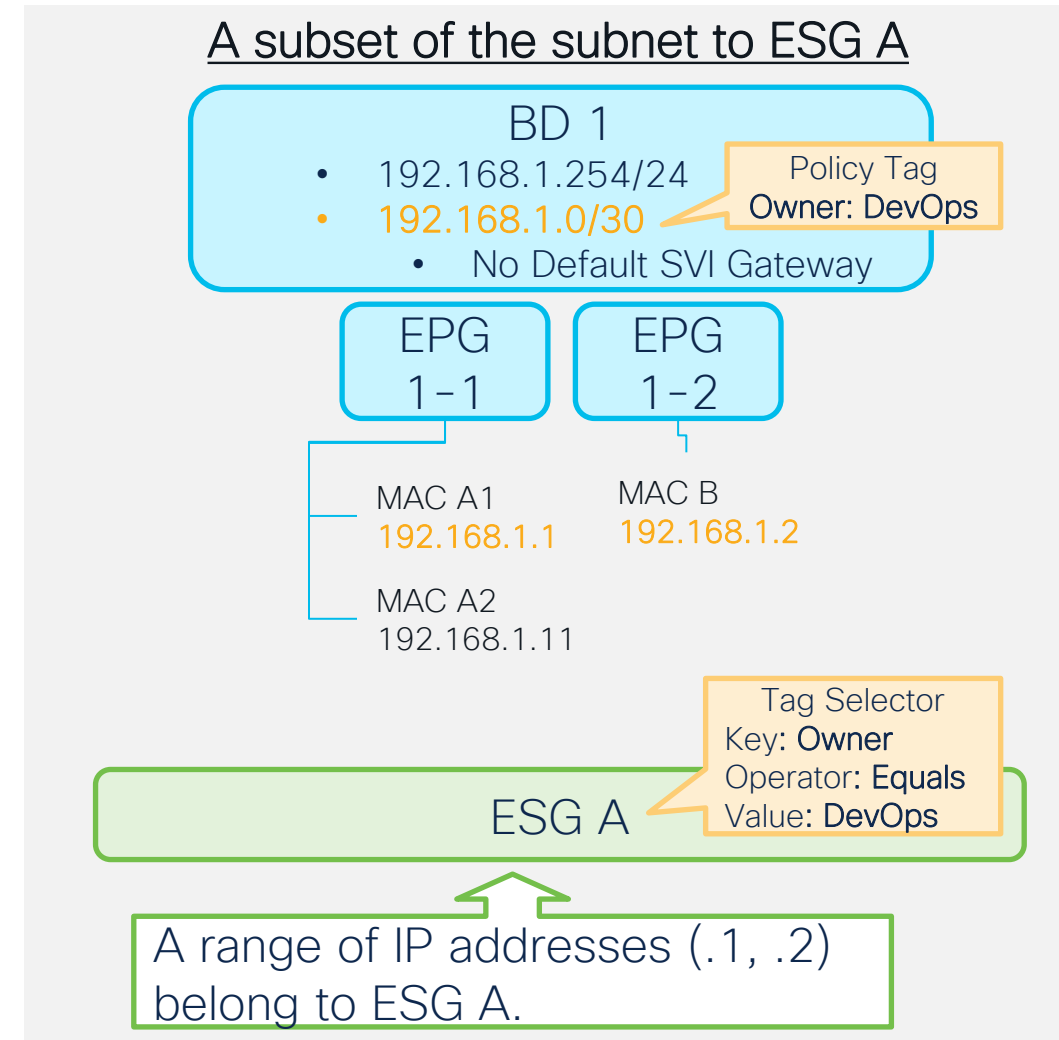
Policy Tags on BD Subnets (subset of a subnet)

- If only a subset of the BD subnet needs to be classified to an ESG, you can configure a smaller subnet in the same BD with “No Default SVI Gateway” option. Then attach a policy tag to the smaller subnet.
- “No Default SVI Gateway” prevents the additional subnet with this config from being deployed as an SVI on leaf nodes.

NOTE:

this config still deploys a BD route pointing to spine-proxy for 192.168.1.0/30. Although this itself doesn't impact any forwarding behavior, **it consumes an LPM table entry**.

If many of such configs are expected, consider using IP subnet selectors instead which doesn't deploy any routes, hence no impact to the LPM table.

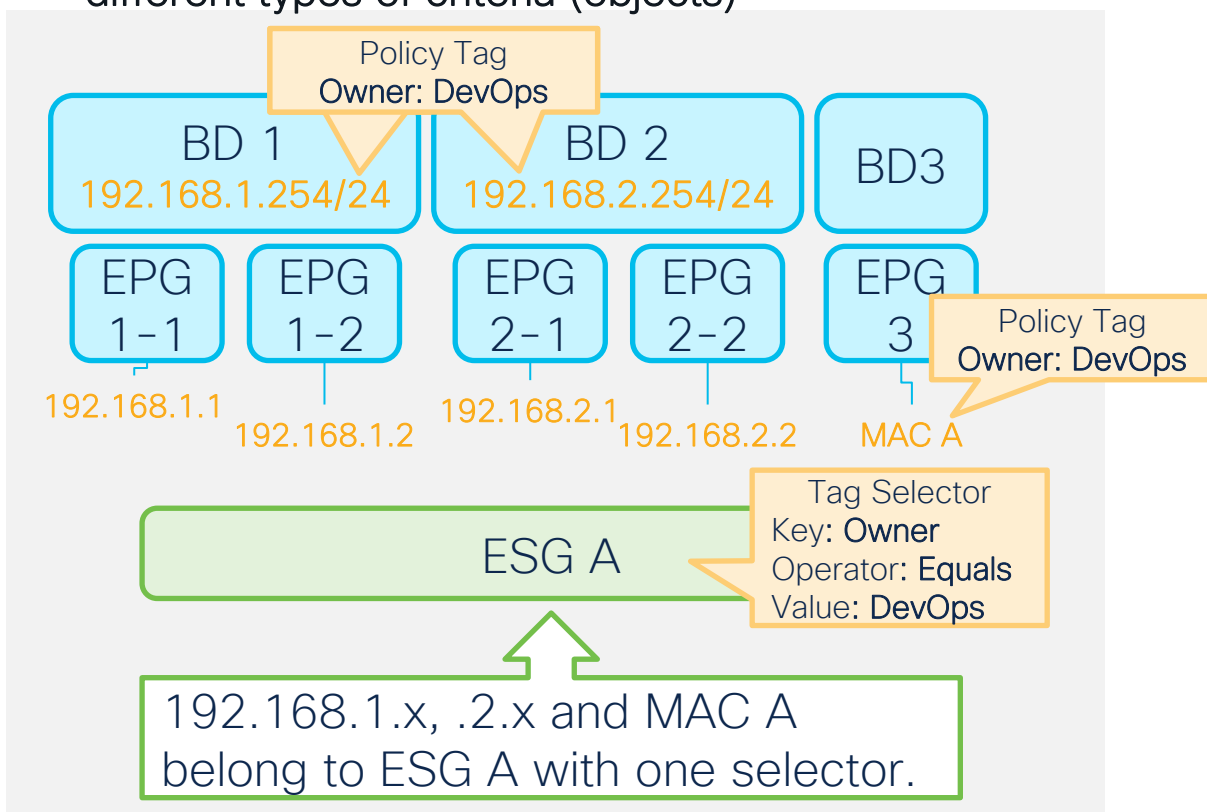


Tag selector (with BD subnets) or IP Subnet selector?

Tag selector (new)

When non-IP based classifications need to be used together.

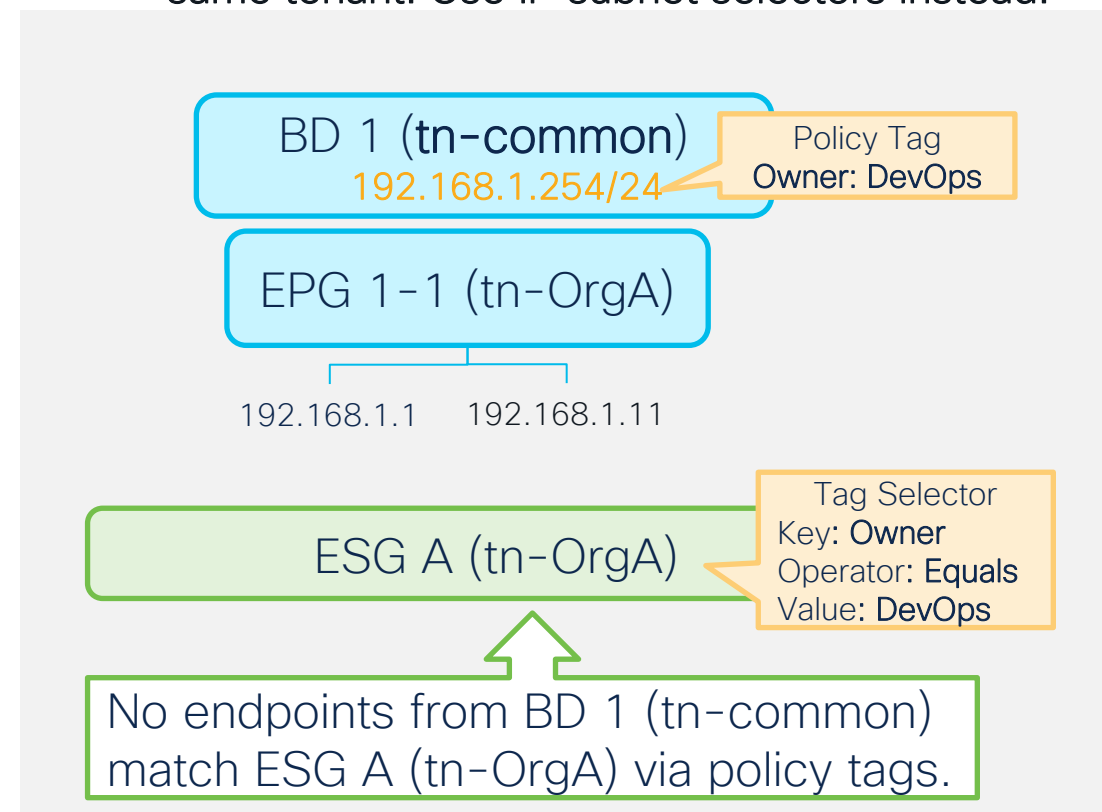
- One tag selector can manage endpoints through different types of criteria (objects)



IP Subnet selector (existing)

When the BD is under tenant common while the EPGs and ESGs are in a user tenant.

- Tag selectors match policy tags only within the same tenant. Use IP subnet selectors instead.



Policy Tags on endpoint IPs

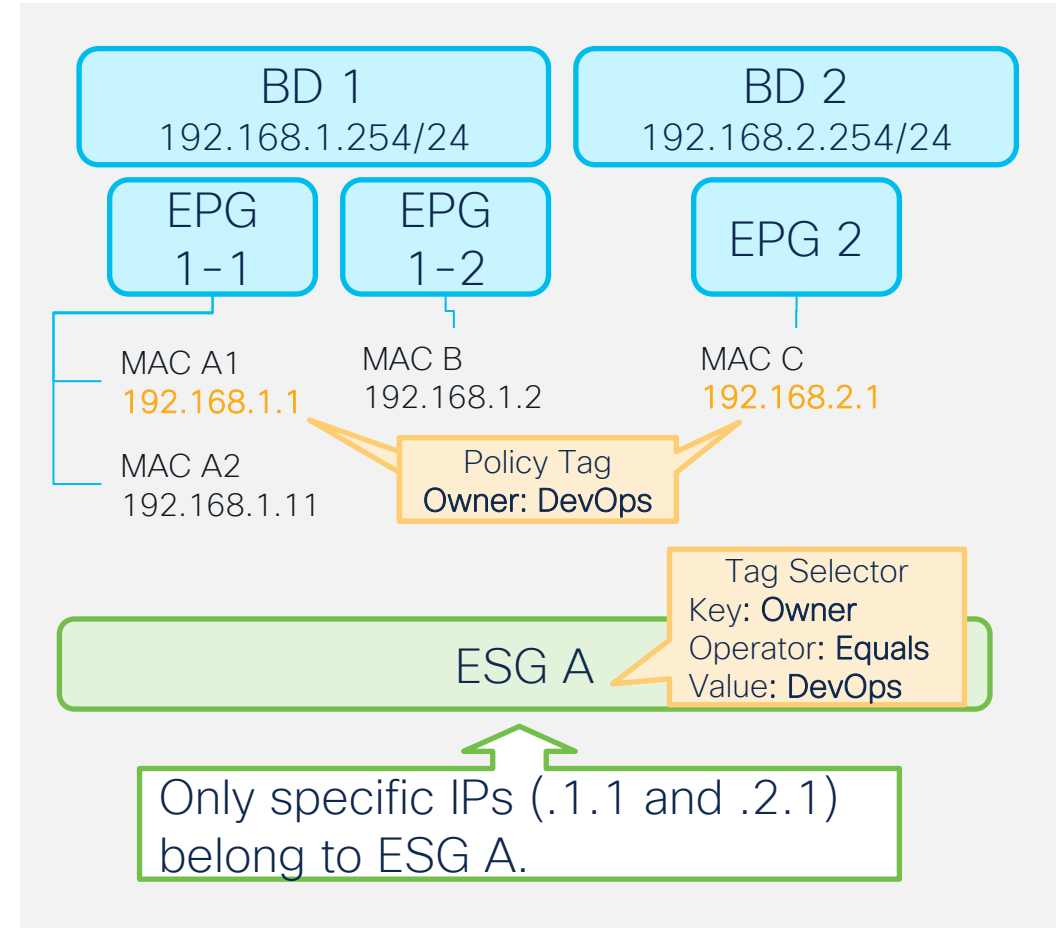
- It is difficult to assign a policy tag on each endpoint directly because endpoints are dynamically learned and aged out.
- APIC 5.2(1) introduced a new object (Endpoint IP Tag) to represent an endpoint IP address so that **policy tags can be assigned and maintained even when the endpoint is not learned yet, or even after the endpoint ages out.**
- By matching a policy tag assigned to an endpoint IP tag, **a tag selector can classify the specific endpoint IP address** to an ESG in the same VRF.

Guidelines:

- The Endpoint IP Tag must be in the same tenant and the same VRF as the ESG.

Limitations:

- This only classifies IP addresses, not MAC addresses. See the L2 Traffic Limitation with IP-based selector slide for its impact.

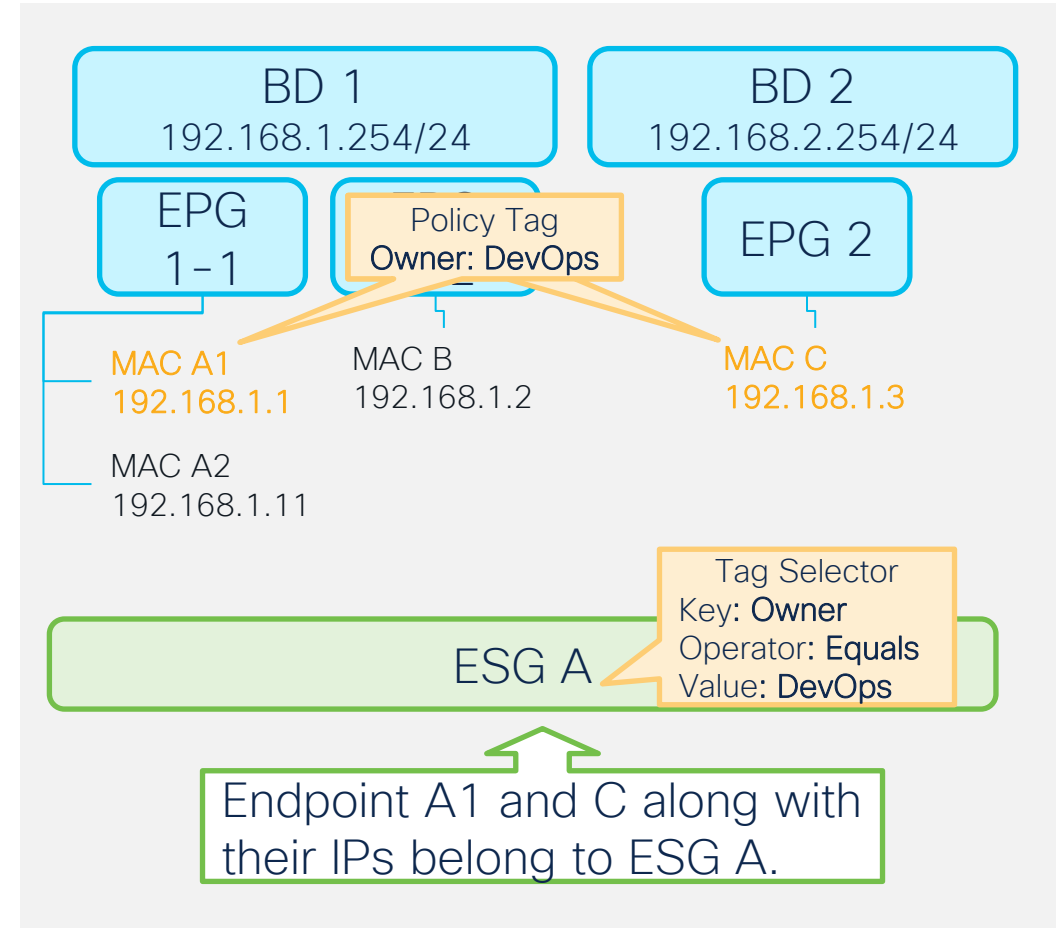


Policy Tags on endpoint MACs

- It is difficult to assign a policy tag on each endpoint directly because endpoints are dynamically learned and aged out.
- APIC 5.2(1) introduced a new object (Endpoint MAC Tag) to represent an endpoint MAC address so that **policy tags can be assigned and maintained even when the endpoint is not learned yet, or even after the endpoint ages out.**
- By matching a policy tag assigned to an endpoint MAC tag, **a tag selector can classify the entire endpoint (MAC and associated IPs)** to a given ESG in the same VRF.

Guidelines:

- The Endpoint MAC Tag must be in the same tenant and the same VRF as the ESG.

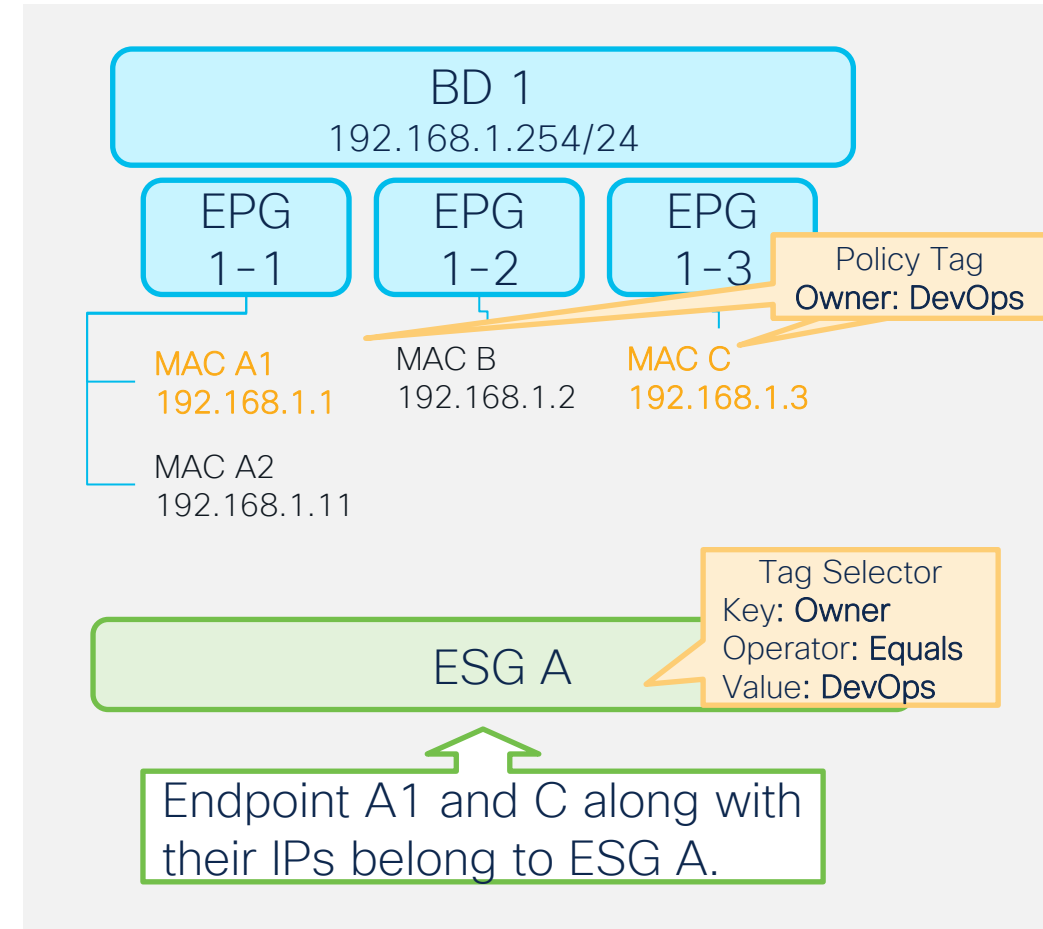


Policy Tags on VMM endpoint MACs

- APIC 5.2(1) introduced a new object (VMM Endpoint MAC Tag) to represent an endpoint MAC address discovered through VMM integration.
- APIC will translate some information of VMs through VMM integration into ACI policy tags.
Supported on 5.2(1):
 - **VMware VM name**
 - (key: __vmm::vmname, value: <VM name>)
 - **VMware Tag**
 - (key: <category>, value: <tag name>)
- By matching a policy tag assigned to a VMM endpoint MAC tag, a **tag selector** can classify the entire endpoint (MAC and associated IPs) to a given ESG in the same VRF.

Guidelines:

- The VMM Endpoint MAC Tag must be in the same tenant and the same VRF as the ESG.

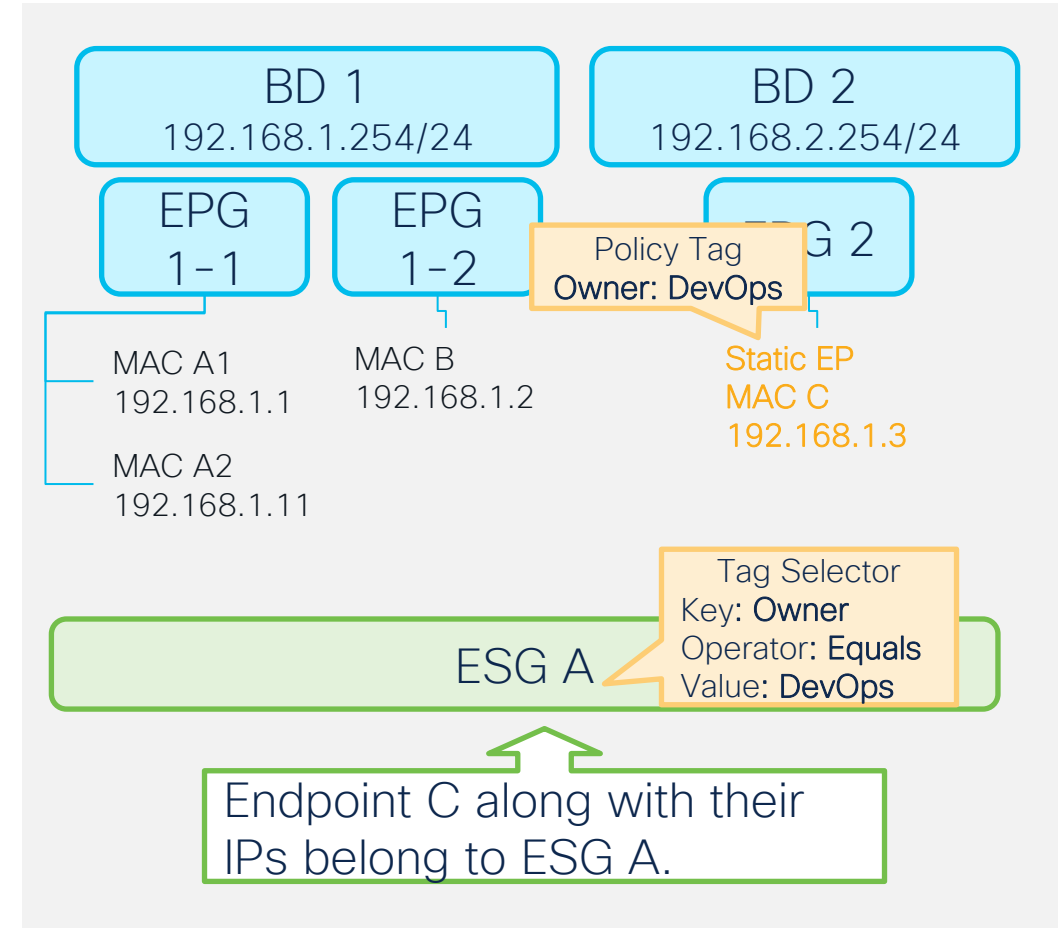


Policy Tags on Static Endpoint

- Essentially **the same as Endpoint MAC tags**.
- APIC allows users to configure policy tags directly on an existing static endpoint instead of configuring another object (Endpoint MAC tag) for the same MAC.
- If you prefer managing all policy tags for static and non-static endpoints in one location (Endpoint MAC tag), you can configure an Endpoint Mac tag for the static endpoint MAC instead of assigning policy tags on static endpoint config.

Guidelines:

- The static endpoint with policy tags must be in the same tenant and the same VRF as the ESG.
- Only type silent host is supported.
- Configuring policy tags on both static endpoint and Endpoint MAC tag for the same MAC is not allowed.



L2 Traffic Limitation with IP-based selectors



• Scenario 1:

- MAC_A is matched by a selector of **ESG 1**
- IP_A is **_not_** matched by **any ESG**
- Result:
 - Both MAC_A and IP_A are classified to **ESG 1**



• Scenario 2:

- MAC_A is matched by a selector of **ESG 1**
- IP_A is matched by a selector of **ESG 2**
- Result:
 - MAC_A is classified to **ESG 1**
 - IP_A is classified to **ESG 2**



• Scenario 3:

- MAC_A is **_not_** matched by **any ESG**
- IP_A is matched by a selector of **ESG 2**
- Result:
 - MAC_A is **_not_** classified to any ESG, and still belongs to the **original EPG**.
 - IP_A is classified to **ESG 2**

When only IP-based selectors are used, MAC addresses are not classified to ESGs.

- Switching traffic (i.e. within the same subnet) will not use ESG contracts even if its payload has the IP address classified to an ESG.
- If the two IPs in the same subnet from the same EPG are classified to different ESGs, those two endpoints can still talk freely through the MAC and its original EPG.

Workarounds for L2 Traffic Limitation

Proxy ARP (on all original EPGs)

- Proxy ARP makes sure that all traffic from the EPGs will be handled as a routing traffic. This means that all traffic uses the pcTag of IP. It does no longer matter whether the MAC still belongs to the original EPG.

How to enable Proxy ARP:

- Flood in Encapsulation
 - There is no functional difference if there is only one VLAN/EPG per BD.
Proxy ARP is enabled automatically when Flood in Encapsulation is enabled.
- Intra EPG Isolation
 - when all endpoints are classified to ESGs, or when any endpoints that are still in original EPGs should not talk with anyone even in the same EPG.
Proxy ARP needs to be explicitly enabled on top of Intra EPG Isolation.
- Intra EPG contract
 - If you want to set a default rule for communications between any endpoints that are still in original EPGs. If you want to allow such communications, use permit all contract.
Proxy ARP is enabled automatically when an intra EPG contract is configured for an EPG.
- Allow Microsegmentation for VMM integration
 - Proxy ARP is **enabled automatically** when Allow Microsegmentation is enabled on VMM domain association.

Prepare the fabric for L4-7 Service Insertion



ACI Endpoint Update App (optional)

<https://dcappcenter.cisco.com/aci-endpoint-update.html>

The image shows two overlapping screenshots from the Cisco APIC interface. The top screenshot is the 'Apps' page for 'aci-dev-01', listing three applications: ELAM Assistant, ACI Endpoint Update (highlighted with a red box), and Nexus Insights Cloud Connector. The bottom screenshot is the 'Firewall Management Center' interface, specifically the 'Objects / Object Management' section. A red line connects the 'ACI Endpoint Update' app to the 'External Attributes' menu item in the left sidebar. The 'Dynamic Objects' table is also highlighted with a red box, showing four entries with their names, descriptions, and the number of mapped IPs.

APIC (aci-dev-01) Apps

- ELAM Assistant** by Cisco
Help you perform ELAM(Embedded Logic Analyzer Module) on ACI nodes to capture a single packet at a time and analyze where the packet goes.
- ACI Endpoint Update** by Cisco
Pushes dynamic endpoint information from APIC to Secure Firewall ASA and Secure Firewall Management Center
- Nexus Insights Cloud Connector** by Cisco
Nexus Insights Cloud Connector (3.x or higher) implements Direct Streaming and Nexus Cloud capable telemetry functionality. These services perform backend functions only and do not have

Firewall Management Center
Objects / Object Management

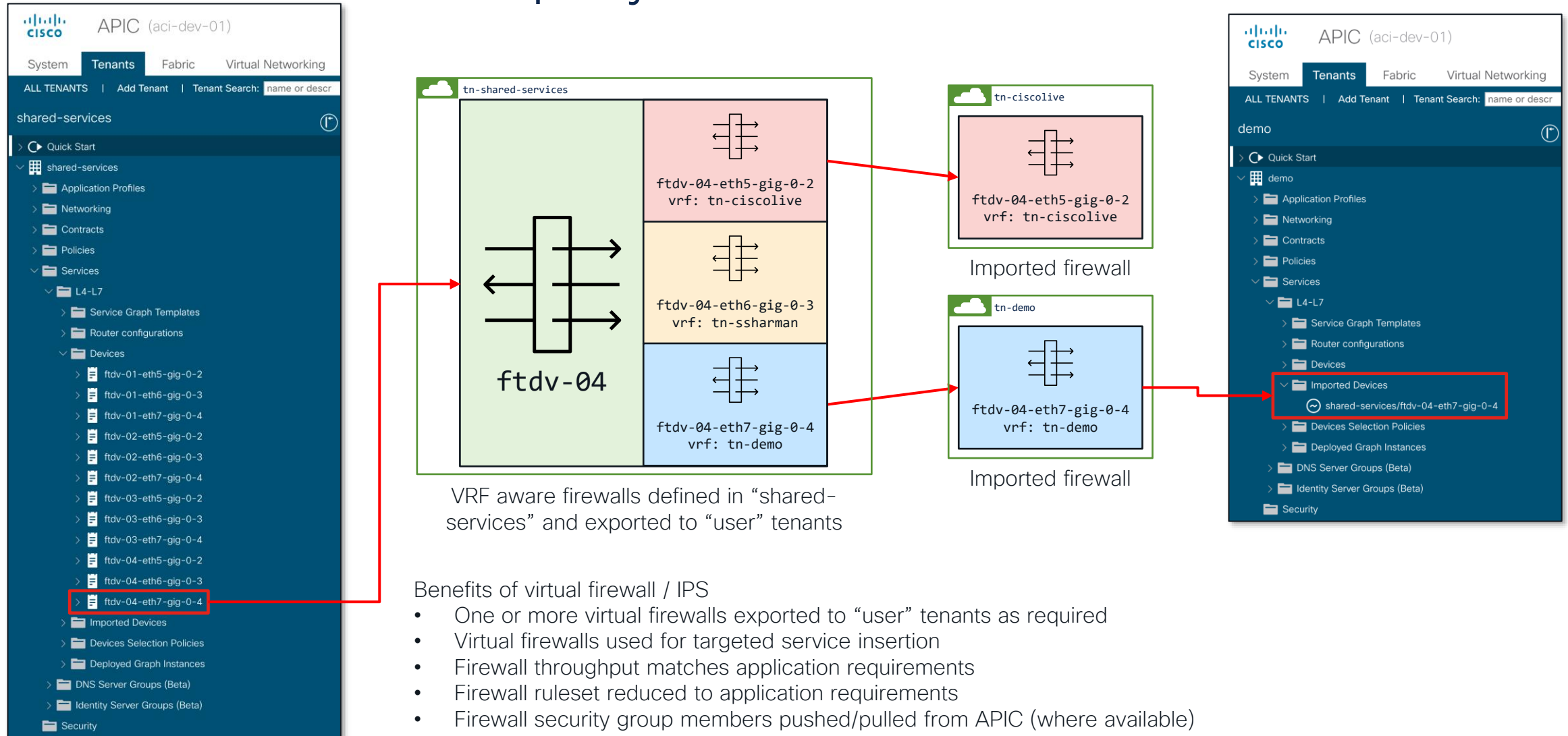
Dynamic Objects

Name	Description	Number of Mapped IPs
APIC_DEMO_EPG-MATCHED-SECURITY-GROUPS_ESG-...		3
APIC_DEMO_NETWORK-SEGMENTS_192.168.150.0_24		1
APIC_DEMO_NETWORK-SEGMENTS_192.168.151.0_24		1
APIC_DEMO_NETWORK-SEGMENTS_192.168.152.0_24		1

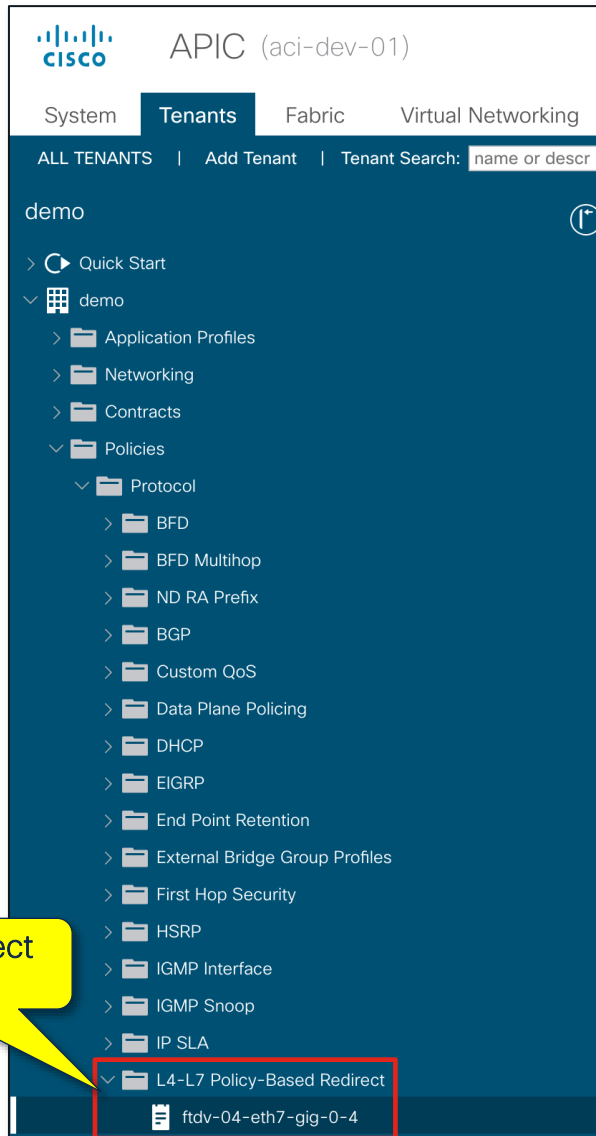
Where should you place your L4-7 devices...?

“common” tenant, “shared-services” tenant, or
“workload/user” tenant...

Virtual firewall deployment



Step 1: Define the Policy Based Redirect Target



Properties

Name: ftdv-04-eth7-gig-0-4

Description: optional

Destination Type: L1 L2 L3

Rewrite source MAC: ☐

IP SLA Monitoring Policy: select an option

Oper Status: Enabled

Enable Pod ID Aware Redirection: ☐

Hashing Algorithm: Destination IP Source IP Source IP, Destination IP and Protocol number

Anycast Endpoint: ☐

IP Address:

MAC Address:

IP	Destination Name	MAC	Redirect Health Group
192.168.156.10		00:50:56:A1:5C:36	

IP address of L4-7 device

MAC address of L4-7 device

Step 2: Define Service Graph Template and Device Selection Policy

The image displays the APIC (aci-dev-01) interface for configuring a Service Graph Template and a Device Selection Policy. The interface is divided into two main sections: Service Graph Templates and Devices Selection Policies.

Service Graph Template: The left pane shows the 'demo' tenant with a 'Service Graph Templates' folder. A template named 'redirect-to-ftdv-04-gig-0-4' is selected, showing a 'Function Node - N1' with 'consumer' and 'provider' endpoints. Below this, a diagram shows the 'Consumer' (EPG) connected to the 'Provider' (EPG) via a central node 'ftdv-04-eth7-gig-0-4' (N1). A box below the diagram provides information for 'ftdv-04-eth7-gig-0-4': Firewall: Routed, Route Redirect: true.

Devices Selection Policy: The right pane shows the 'demo' tenant with a 'Devices Selection Policies' folder. A policy named 'any-redirect-to-ftdv-04-gig-0-4-N1' is selected, showing 'consumer' and 'provider' endpoints. Below this, a diagram shows the 'Consumer' (EPG) connected to the 'Provider' (EPG) via a central node 'ftdv-04-eth7-gig-0-4' (N1). A box below the diagram provides information for 'ftdv-04-eth7-gig-0-4': Firewall: Routed, Route Redirect: true.

Configuration Details: The right pane shows the configuration for the 'consumer' and 'provider' endpoints. The 'consumer' configuration includes:

- Connector Name: consumer
- Cluster Interface: gig-0-4
- Associated Network: Bridge Domain (selected), L3Out
- Bridge Domain: 192.168.156.0_24
- Preferred Contract Group: Exclude
- Permit Logging: ☐
- L3 Destination (VIP): ☒
- L4-L7 Policy-Based Redirect: ftdv-04-eth7-gig-0-4
- L4-L7 Service EPG Policy: select an option
- Custom QoS Policy: select a value

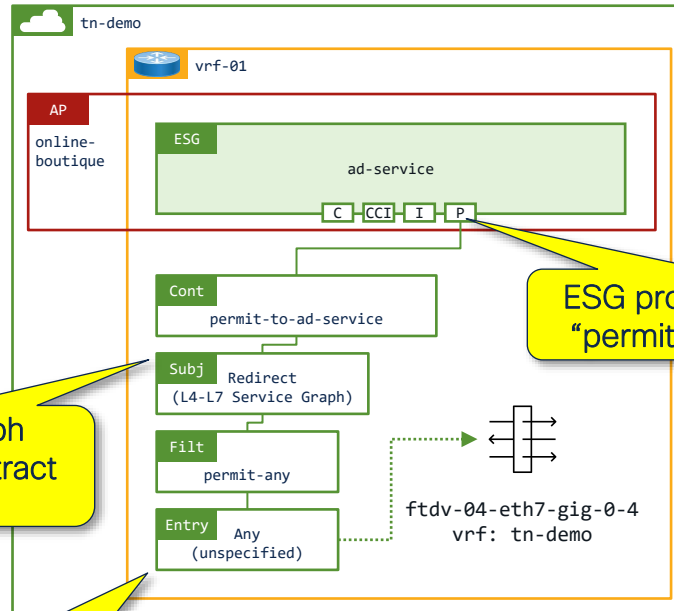
The 'provider' configuration includes:

- Connector Name: provider
- Cluster Interface: gig-0-4
- Associated Network: Bridge Domain (selected), L3Out
- Bridge Domain: 192.168.156.0_24
- Preferred Contract Group: Exclude
- Permit Logging: ☐
- L3 Destination (VIP): ☒
- L4-L7 Policy-Based Redirect: ftdv-04-eth7-gig-0-4
- L4-L7 Service EPG Policy: select an option
- Custom QoS Policy: select a value

Annotations: Yellow callouts highlight key configuration elements:

- Service Graph Template:** Points to the 'redirect-to-ftdv-04-gig-0-4' template.
- Device Selection Policy:** Points to the 'any-redirect-to-ftdv-04-gig-0-4-N1' policy.
- PBR target:** Points to the 'ftdv-04-eth7-gig-0-4' target in the L4-L7 Policy-Based Redirect field.
- Firewall interface and Bridge Domain for the Consumer interface:** Points to the 'gig-0-4' cluster interface and 'Bridge Domain' associated network.
- Firewall interface and Bridge Domain for the Provider interface:** Points to the 'gig-0-4' cluster interface and 'Bridge Domain' associated network.

Step 3: Apply Service Graph to Contract Subject



ESG provides a contract "permit-to-ad-service"

Service Graph applied to contract subject

All ports specified by the filter entries are redirected to the firewall

Contract Scope

Name: permit-to-ad-service
Alias:
Global Alias:

Scope: VRF

Service Graph is deployed once the contract is consumed

Contract Subject and Filter

Property

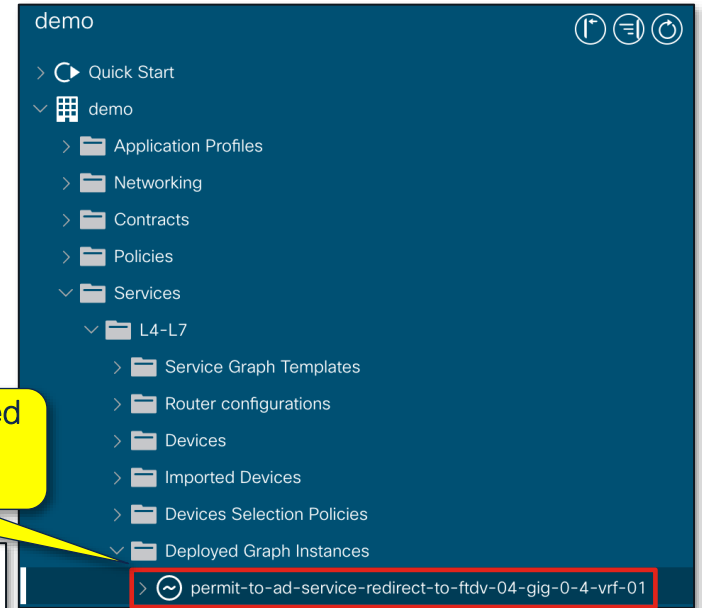
Name: redirect
Alias:
Description: optional
Global Alias:

Apply Both Directions: true
Reverse Filter Ports: ☒

Filters:

Name	Tenant	Action
permit-any	demo	Permit

L4-L7 Service Graph: redirect-to-ftdv-04-gig



Contract and Subject

External Connectivity...



Each Tenant has their own IP Range

APIC (aci-dev-01)

System

Tenants

Fabric

Virtual Networking

Admin

Operations

Apps

Integrations

ALL TENANTS

Add Tenant

Tenant Search:

common

ciscolive-07

rwhitear

shared-services

ciscolive-08

All Tenants

Name	Alias	Description	Bridge Domains	VRFs
shared-services		L3out and shared devices	0	1
aci-infrastructure		Nexus Dashboard, MSO etc	1	0
ciscolive-01		Routable IP range 10.0.11-15.x	5	1
ciscolive-02		Routable IP range 10.0.21-25.x	0	1
ciscolive-03		Routable IP range 10.0.31-35.x	0	1
ciscolive-04		Routable IP range 10.0.41-45.x	0	1
ciscolive-05		Routable IP range 10.0.51-55.x	0	1
ciscolive-06		Routable IP range 10.0.61-65.x	0	1
ciscolive-07		Routable IP range 10.0.71-75.x	5	1
ciscolive-08		Routable IP range 10.0.81-85.x	5	1
ardica		Routable IP range 192.168.0-5.x	0	1
rwhitear		Routable IP range 192.168.10-15.x	6	1
ngorse		Routable IP range 192.168.120-125.x	1	1
demo		Routable IP range 192.168.150-155.x	3	1
fgandola		Routable IP range 192.168.151-158.x	11	2
roxadiaz		Routable IP range 192.168.20-25.x	6	1
ndsouzar		Routable IP range 192.168.30-35.x	6	1
esx-infrastructure		Routable IP range 192.168.4.x	1	0
adealdag		Routable IP range 192.168.40-45.x	6	1
ssharmar		Routable IP range 192.168.50-56.x	7	1
mgmt		Routable IP range 192.168.6.x	1	2
movaswan		Routable IP range 192.168.60-65.x	6	1
adossant		Routable IP range 192.168.70-75.x	0	1
fdagenha		Routable IP range 192.168.80-85.x	0	1
ylouis		Routable IP range 192.168.90-95.x	0	1

Page 1 Of 1

Objects Per Page: 100

Displaying Objects 1 - 32 Of 32

Last Login Time: 2022-11-26T07:06 UTC+00:00

Current System Time: 2022-11-26T07:58 UTC+00:00

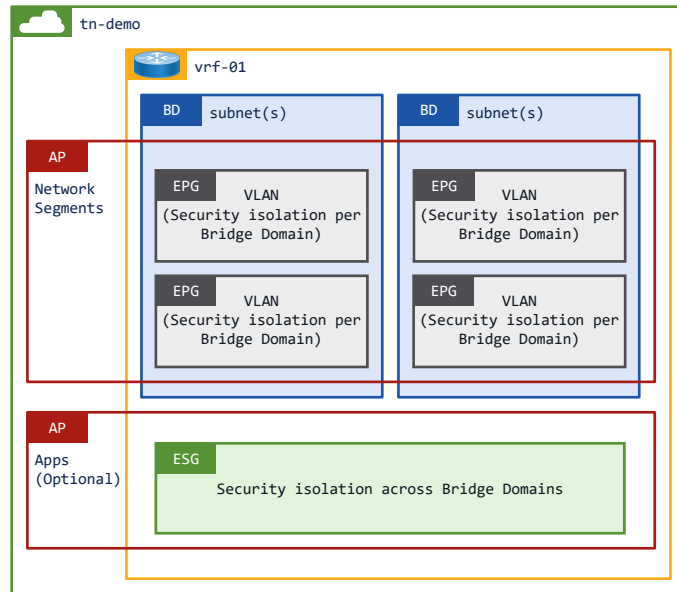
All Tenants

Name	Alias	Description
shared-services		L3out and shared devices
aci-infrastructure		Nexus Dashboard, MSO etc
ciscolive-01		Routable IP range 10.0.11-15.x
ciscolive-02		Routable IP range 10.0.21-25.x
ciscolive-03		Routable IP range 10.0.31-35.x
ciscolive-04		Routable IP range 10.0.41-45.x
ciscolive-05		Routable IP range 10.0.51-55.x
ciscolive-06		Routable IP range 10.0.61-65.x
ciscolive-07		Routable IP range 10.0.71-75.x
ciscolive-08		Routable IP range 10.0.81-85.x
ardica		Routable IP range 192.168.0-5.x
rwhitear		Routable IP range 192.168.10-15.x
ngorse		Routable IP range 192.168.120-125.x

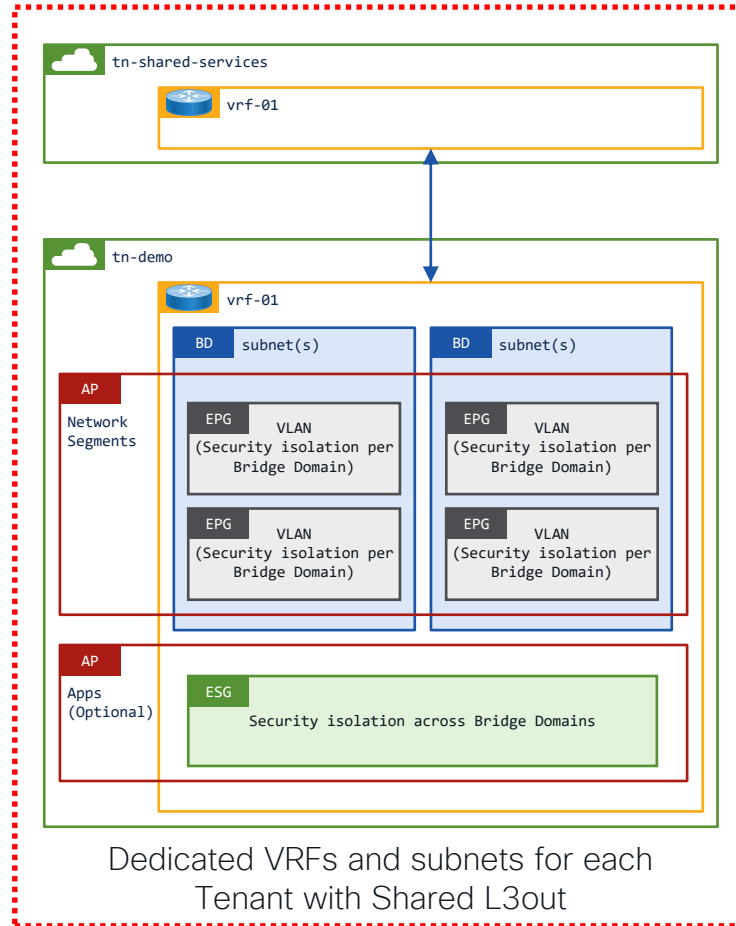
Where should you place your L3outs...?

“common” tenant, “shared-services” tenant, or
“workload/user” tenant...

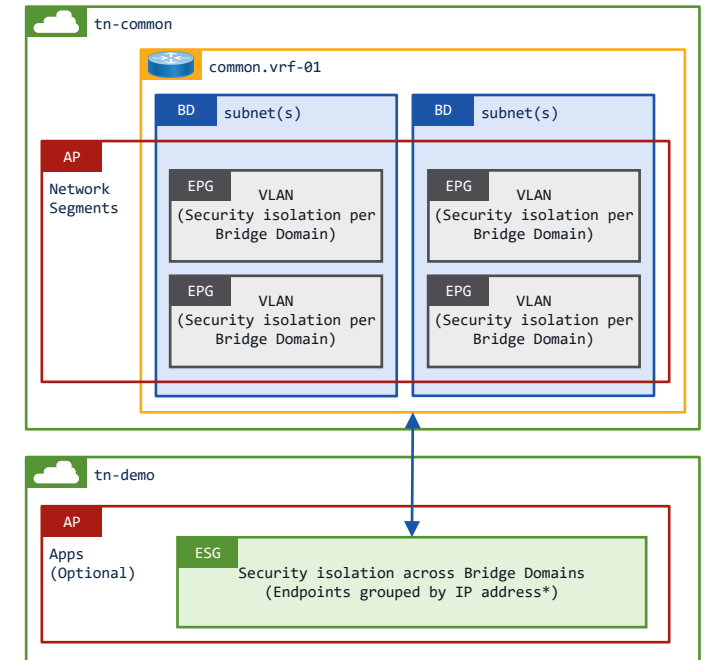
External Connectivity



Dedicated VRFs and subnets for each Tenant with Dedicated L3outs

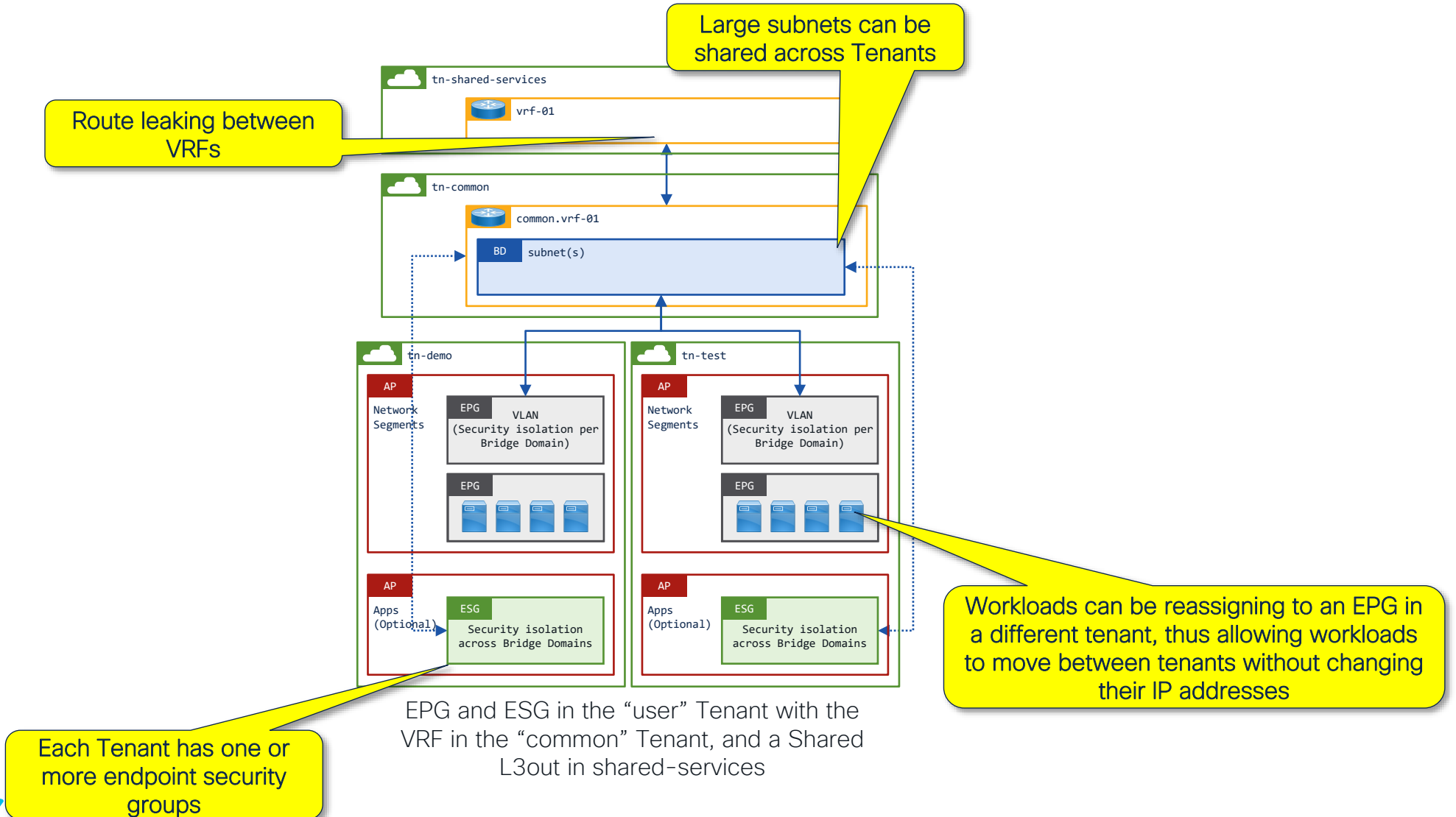


Dedicated VRFs and subnets for each Tenant with Shared L3out



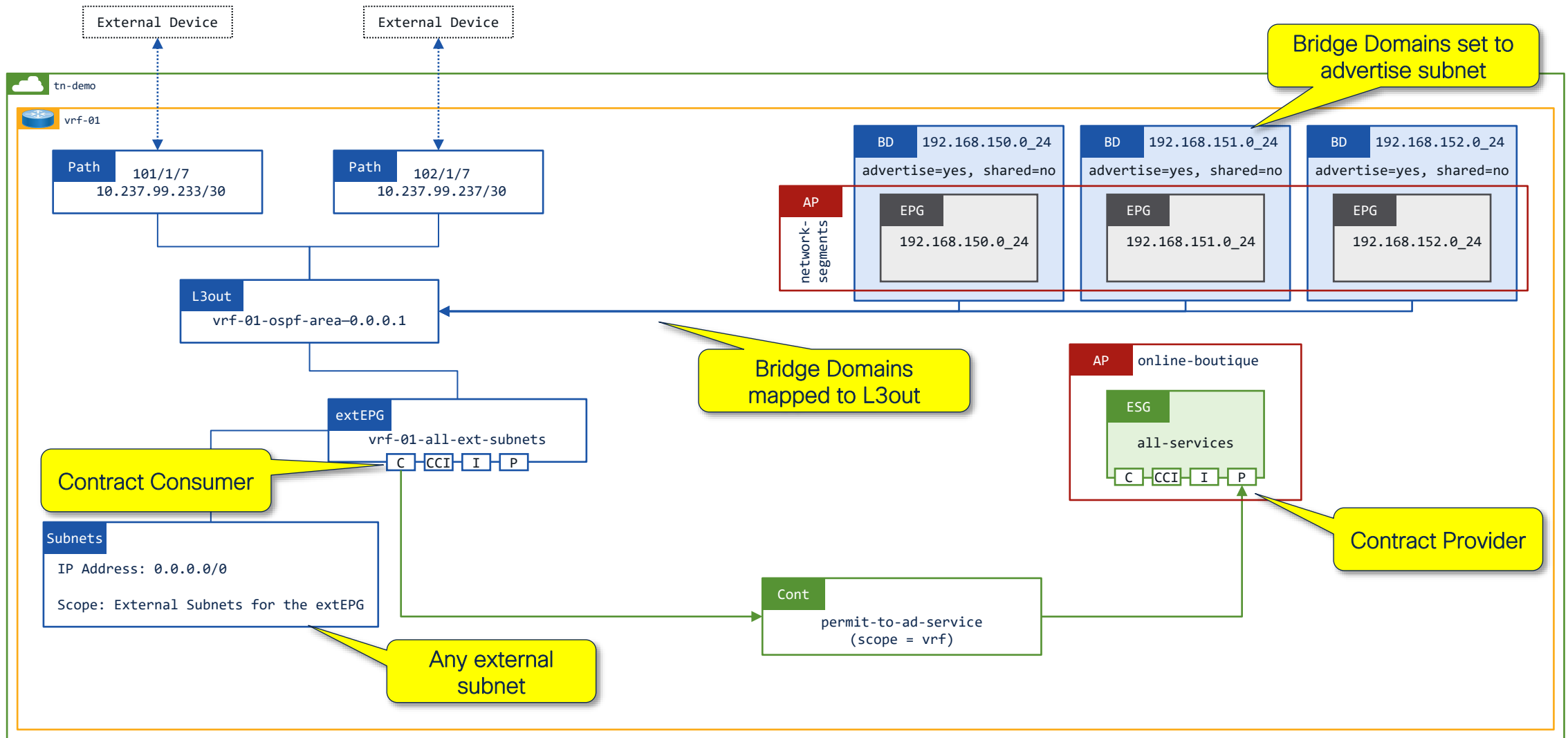
Shared networking with isolated security

Or even a combined solution...!



Option 1 – Dedicated L3out per Tenant

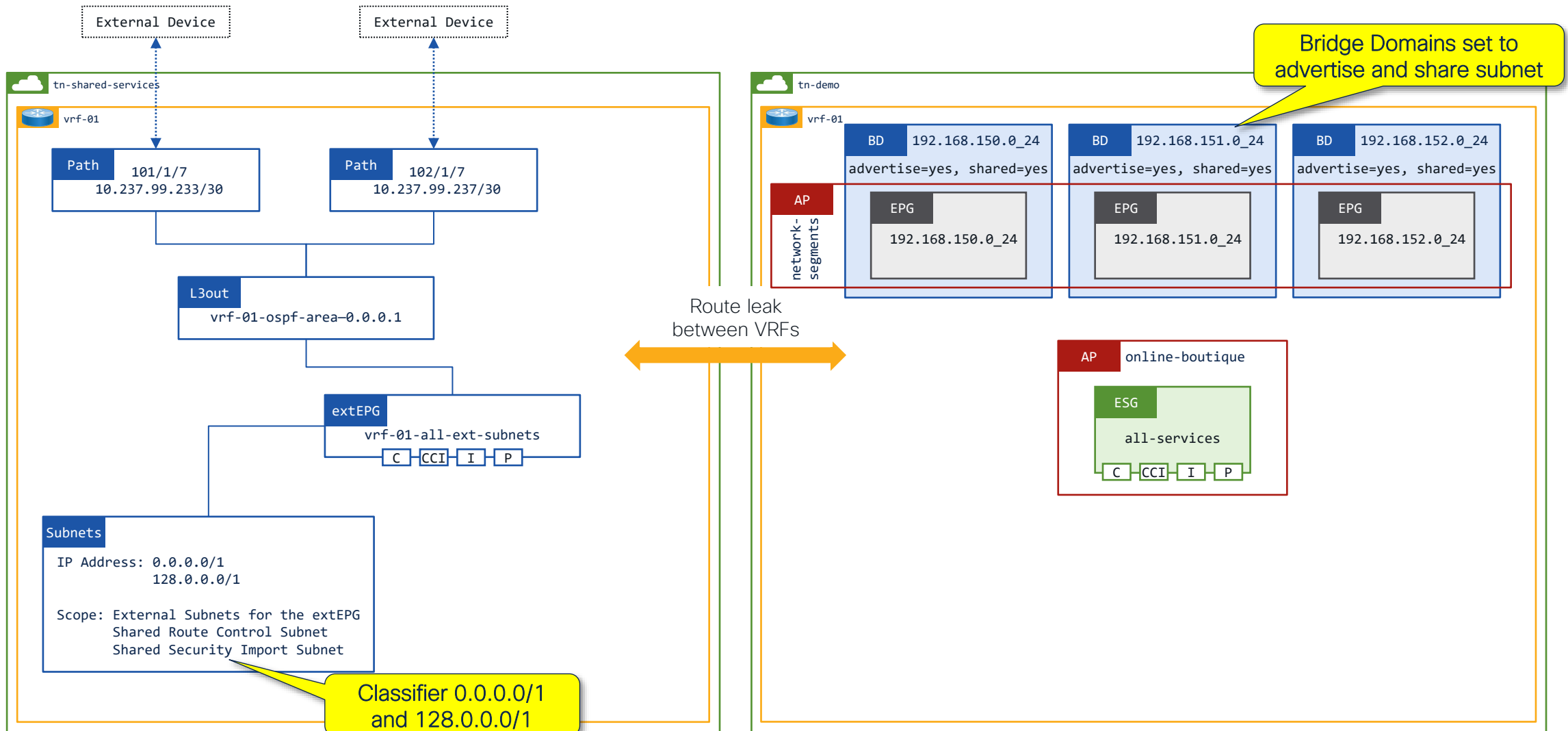
Dedicated L3out



*arrows indicates direction of traffic flow i.e. from consumer to provider

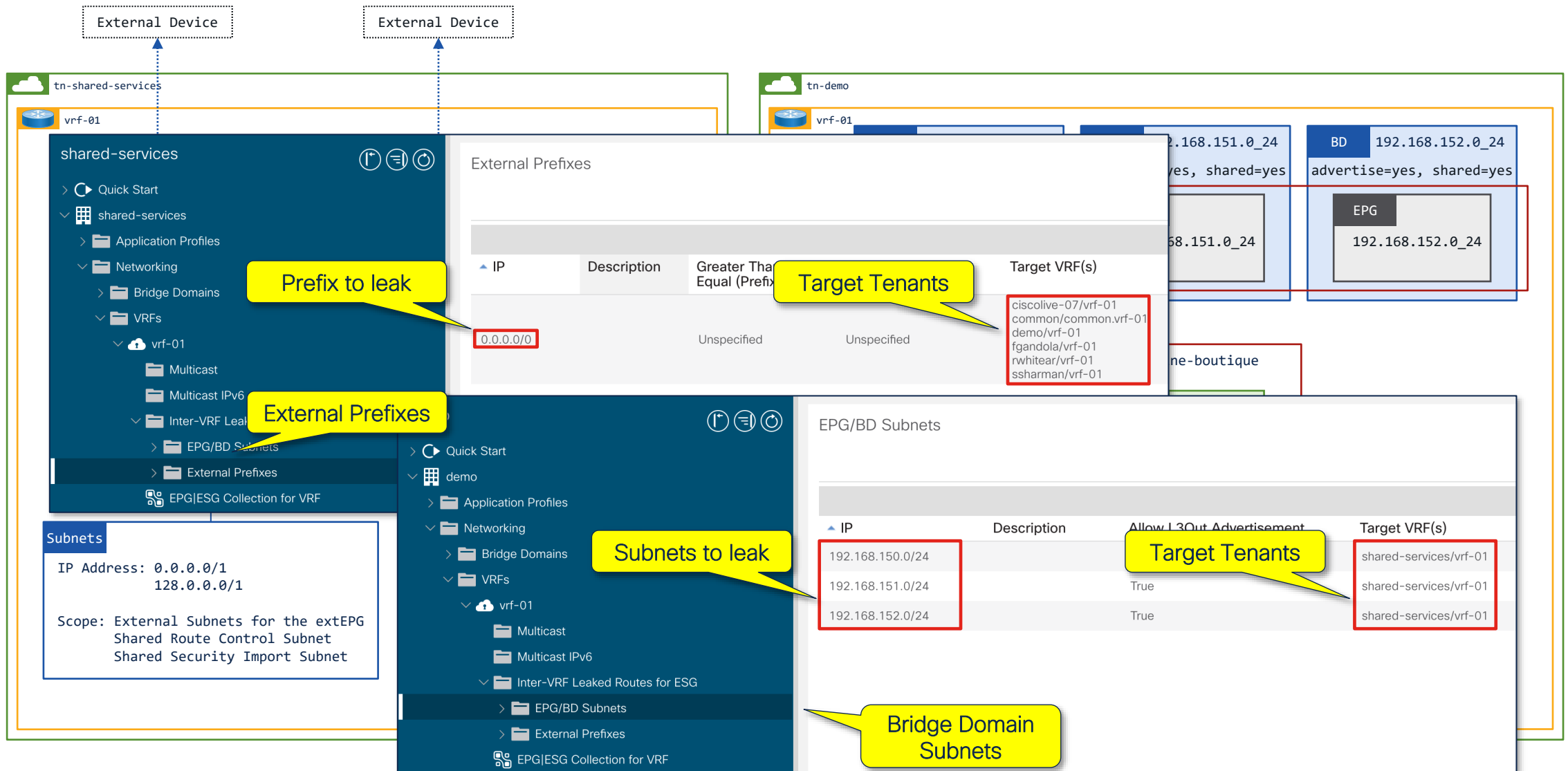
Option 2 – Shared L3out

Shared L3out Route Leaking



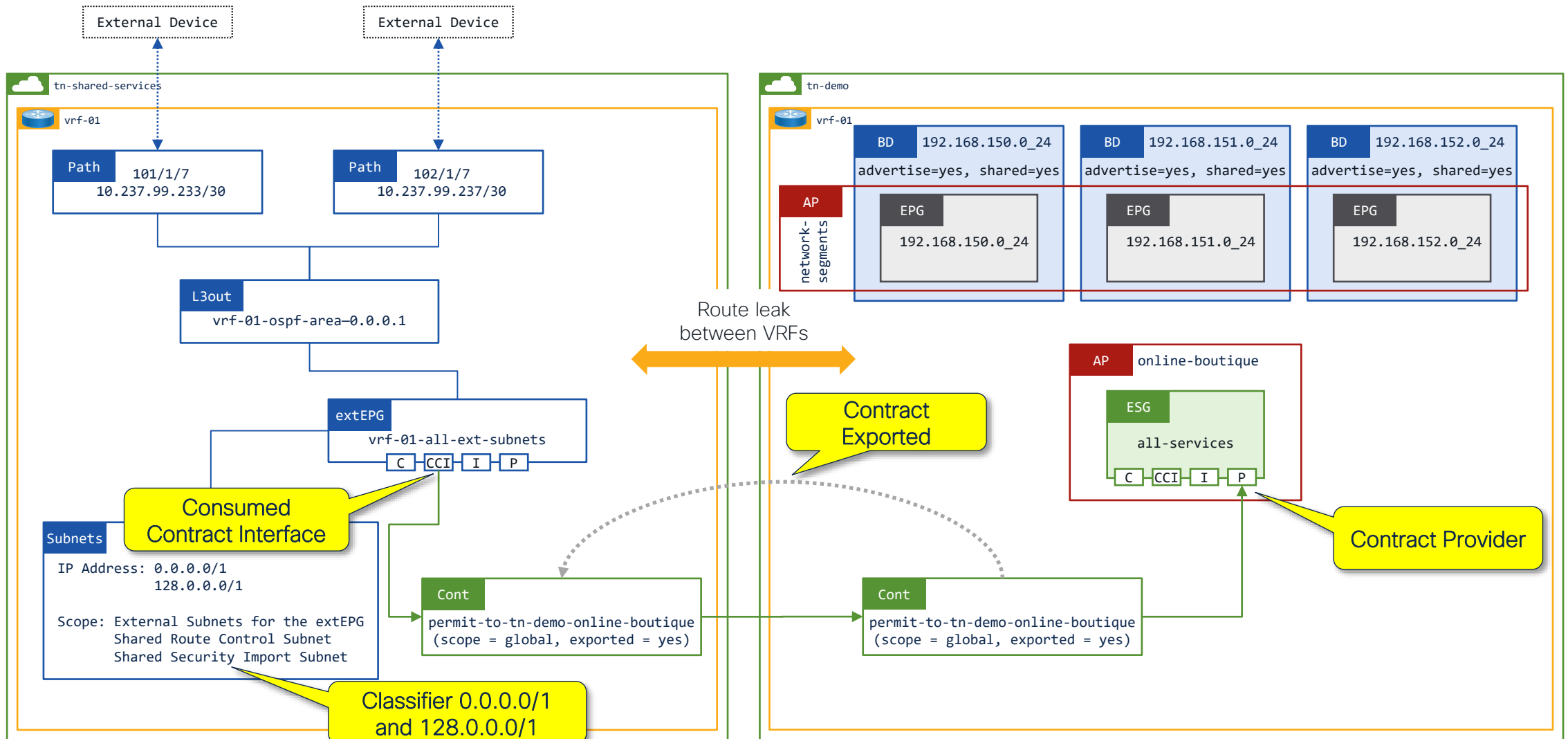
*arrows indicates direction of traffic flow i.e. from consumer to provider

Shared L3out Route Leaking



*arrows indicates direction of traffic flow i.e. from consumer to provider

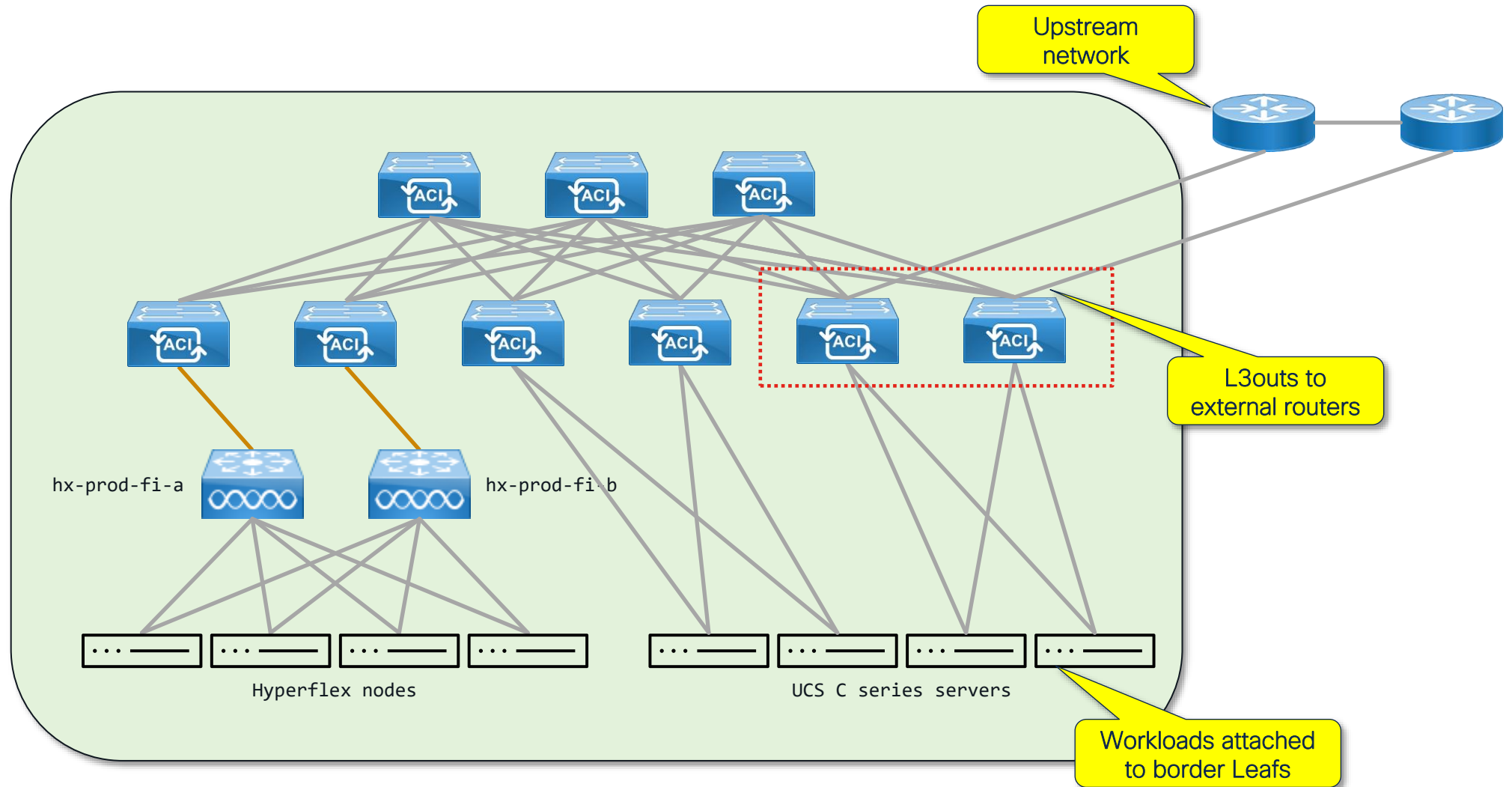
Shared L3out External Contracts



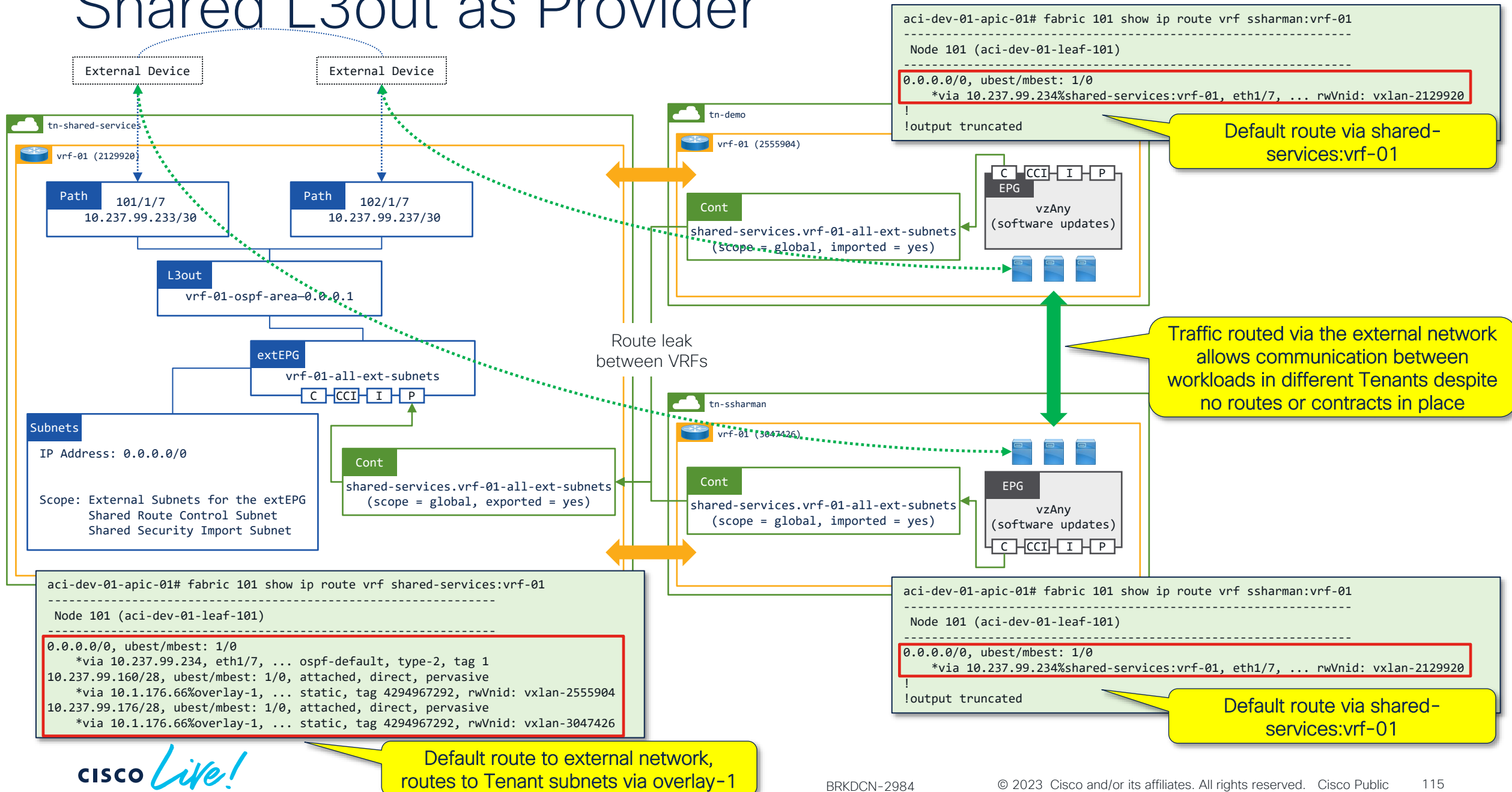
*arrows indicates direction of traffic flow i.e. from consumer to provider

Why are we classifying with 0.0.0.0/1 and
128.0.0.0/1...?

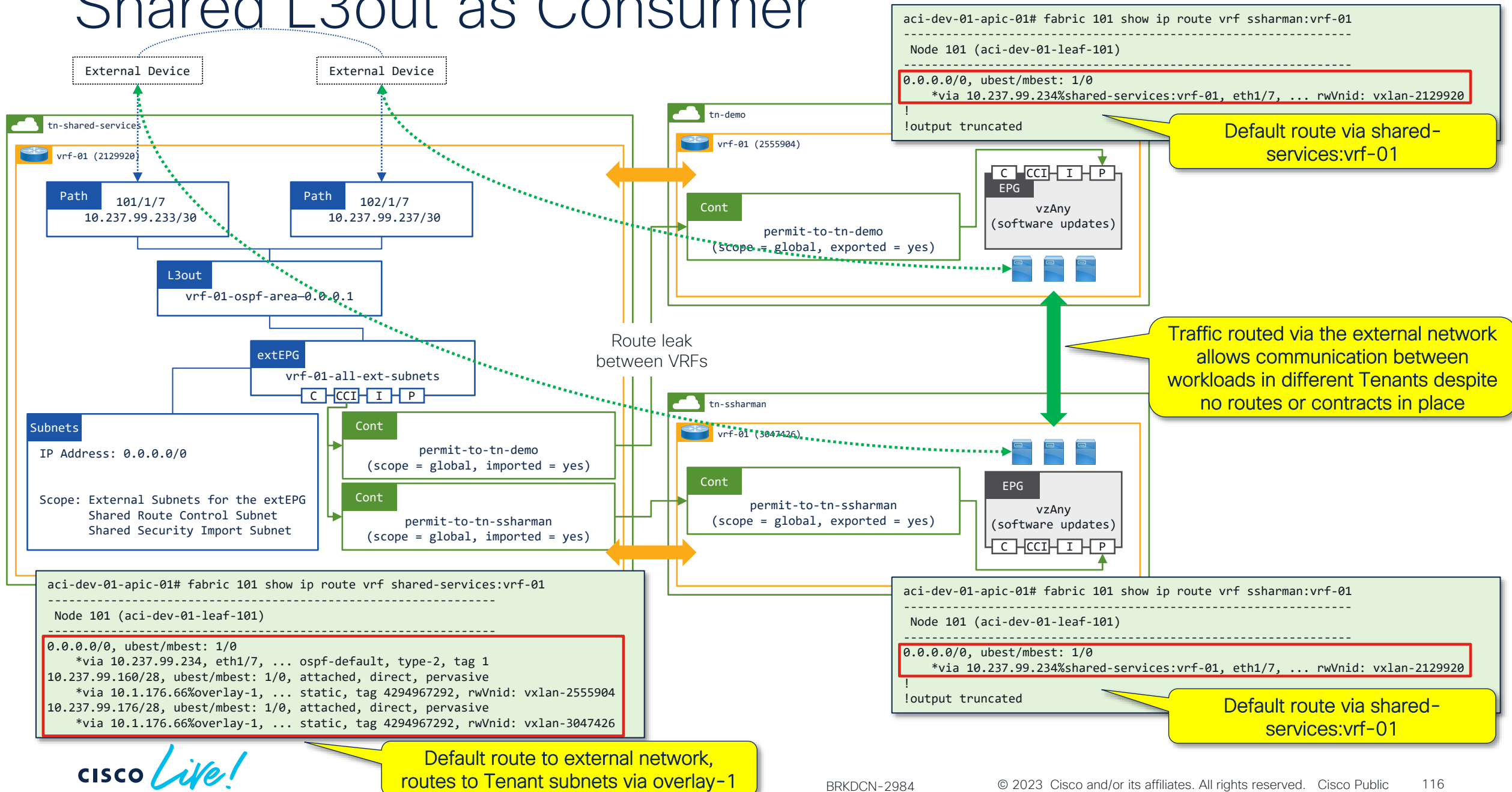
Non dedicated border Leafs



Shared L3out as Provider



Shared L3out as Consumer



Let's understand what's happening...

First, we need the ClassID or pcTag of the extEPG...

Get Class ID of the External EPG

```
aci-dev-01-apic-01# moquery -c l3extInstP -f 'l3ext.InstP.name=="all-external-subnets"' | egrep "^name|^pcTag|^dn|^scope"
name          : all-external-subnets
dn            : uni/tn-shared-services/out-shared-services.vrf-01-ospf-area-0.0.0.1/instP-all-external-subnets
nameAlias     :
pcTag         : 41
pcTagAllocSrc : idmanager
scope         : 2129920
```

shared-services:vrf-01
extEPG uses VXLAN Encap
2129920 and pcTag 41

PcTag Category Name	PcTag Range
System	1-15
Global	16-16385
Local (to VRF)	16386-65535

extEPG uses a pcTag from
the Global range

Summary

Dashboard

Policy

Operational

Stats

Health

Faults

History

Endpoints

Flows

Packets

Policy Tags

Resource IDs

Bridge Domains

VRFs

EPGs

ESGs

L3Outs

External Networks (Bridged)

Healthy

EPG Name

EPG Alias

Class ID

Scope

all-external-subnets

41

2129920

Resource IDs are visible in the GUI

Resource IDs are visible
in the GUI

Get VRF scopes and Class IDs

```
aci-dev-01-apic-01# show vrf vrf-01 detail | grep shared- -B 4 -A 1
```

VRF Information:					Consumed Contracts	Provided Contracts	Description
Tenant	VRF	VXLAN Encap	Policy Enforced	Policy Tag			
shared-services-	vrf-01	2129920	enforced	46	-		

shared-services:vrf-01 uses VXLAN Encap 2129920 and pcTag 46

```
aci-dev-01-apic-01# show vrf vrf-01 detail | grep demo -B 4 -A 1
```

VRF Information:					Consumed Contracts	Provided Contracts	Description
Tenant	VRF	VXLAN Encap	Policy Enforced	Policy Tag			
demo	vrf-01	2555904	enforced	49153	-		

demo:vrf-01 uses VXLAN Encap 2555904 and pcTag 49153

```
aci-dev-01-apic-01# show vrf vrf-01 detail | grep ssharman -B 4 A 1
```

VRF Information:					Consumed Contracts	Provided Contracts	Description
Tenant	VRF	VXLAN Encap	Policy Enforced	Policy Tag			
ssharman	vrf-01	3047426	enforced	49153	-		

demo:vrf-01 uses VXLAN Encap 3047426 and pcTag 49153

PcTag Category Name	PcTag Range
System	1-15
Global	16-16385
Local (to VRF)	16386-65535

shared-services:vrf-01 uses a pcTag from the Global range

Summary		Dashbo	Stats	Health	Faults	History
Endpoints		Flows	Packets	Policy Tags	Resource IDs	
Bridge Domains		VRFs	EPGs	ESGs	L3Outs	External Networks (Bridged)
Class ID	Segment ID	Scope				
46	2129920	2129920				

Resource IDs are visible in the GUI

Let's check the VRF zoning-rules...

Check the zoning rules for the shared VRF extEPG

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 src-epg 41
```

```
-----  
Node 101 (aci-dev-01-leaf-101)  
-----
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope

SrcEPG /DstEPG 41 = VRF extEPG ClassID

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 dst-epg 41
```

```
-----  
Node 101 (aci-dev-01-leaf-101)  
-----
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope

There are no zoning rules to the extEPG, so how is anything communicating...?

Check the zoning rules for the shared VRF

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 src-epg 46
```

```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope
4359	46	14	implicit	uni-dir	enabled	2129920
4293	46	0	default	uni-dir	enabled	2129920

SrcEPG /DstEPG 46 = VRF ClassID

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 dst-epg 46
```

```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Priority

There are zoning rules
to the VRF
(Output truncated)

Check the zoning rules for the shared VRF and extEPG

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 src-epg 46
```

```
Node 101 (aci-dev-01-leaf-101)
```

SrcEPG /DstEPG 46 = VRF ClassID

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Priority
4359	46	14	implicit	uni-dir	enabled	2129920		permit_override	src_dst_any(9)
4293	46	0	default	uni-dir	enabled	2129920	shared-services:shared-services.vrf-01-all-ext-subnets	permit	shsrc_any_any_perm(11)

DstEPG 14 = all EPGs/ESGs which are consumers of shared services

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 dst-epg 46
```

```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Priority

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 src-epg 41
```

```
Node 101 (aci-dev-01-leaf-101)
```

SrcEPG /DstEPG 41 = extEPG

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Priority

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 dst-epg 41
```

```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Priority

Why are there no zoning rules for the extEPG...?

Setting a scope of 0.0.0.0/0 triggers “system” pcTag 15

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 src-epg 15
```

```
-----  
Node 101 (aci-dev-01-leaf-101)  
-----
```

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

SrcEPG /DstEPG 15 = system classifier
for all remote subnets

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 dst-epg 15
```

```
-----  
Node 101 (aci-dev-01-leaf-101)  
-----
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+  
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope |  
+-----+-----+-----+-----+-----+-----+-----+-----+  
| 4370 | 0 | 15 | default | uni-dir | enabled | 2129920 |  
| 4498 | 0 | 15 | implicit | uni-dir | enabled | 2129920 |  
+-----+-----+-----+-----+-----+-----+-----+-----+
```

Output truncated

Setting a scope of 0.0.0.0/0 triggers “system” pcTag 15

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 src-epg 15
```

```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Priority
4370	0	15	default	uni-dir	enabled	2129920	shared-services:shared-services.vrf-01-all-ext-subnets	permit	any_dest_any(16)
4498	0	15	implicit	uni-dir	enabled	2129920		deny,log	any_vrf_any_deny(22)

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 dst-epg 15
```

```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Priority
4370	0	15	default	uni-dir	enabled	2129920	shared-services:shared-services.vrf-01-all-ext-subnets	permit	any_dest_any(16)
4498	0	15	implicit	uni-dir	enabled	2129920		deny,log	any_vrf_any_deny(22)

pcTag 15 is a “system” pcTag which is triggered when 0.0.0.0/0 is used for the external subnet classifier.

When 0.0.0.0/0 is configured, the source class is set to the VRF Class ID

Let's check the target tenants zoning rules...

Check the zoning rules for the demo VRF

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2555904 src-epg 46
```

```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Priority
4263	46	0	default	uni-dir	enabled	2555904	shared-services:shared-services.vrf-01-all-ext-subnets	permit	shsrc_any_any_perm(11)

SrcEPG = shared services VRF

DstEPG = all EPGs/ESGs which are consumers of shared services

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2555904 dst-epg 46
```

```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Priority
4263	46	0	default	uni-dir	enabled	2555904	shared-services:shared-services.vrf-01-all-ext-subnets	permit	shsrc_any_any_perm(11)

SrcEPG = shared services VRF

DstEPG = all EPGs/ESGs (vzAny)

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2555904 src-epg 15
```

```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Priority
4307	0	15	default	uni-dir	enabled	2555904	shared-services:shared-services.vrf-01-all-ext-subnets	permit	any_dest_any(16)
4465	0	15	implicit	uni-dir	enabled	2555904		deny,log	any_vrf_any_deny(22)

SrcEPG = vzAny

DstEPG = all extEPGs with 0.0.0.0/0

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2555904 dst-epg 15
```

```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Priority
4307	0	15	default	uni-dir	enabled	2555904	shared-services:shared-services.vrf-01-all-ext-subnets	permit	any_dest_any(16)
4465	0	15	implicit	uni-dir	enabled	2555904		deny,log	any_vrf_any_deny(22)

```
aci-dev-01-apic-01#
```

Check the zoning rules for the demo VRF

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2555904 dst-epg 14
```

```
Node 101 (aci-dev-01-leaf-101)
```

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

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2555904 src-epg 14
```

```
Node 101 (aci-dev-01-leaf-101)
```

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

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2555904 src-epg 46
```

```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Priority
4263	46	0	default	uni-dir	enabled	2555904	shared-services:shared-services.vrf-01-all-ext-subnets	permit	shsrc_any_any_perm(11)

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2555904 dst-epg 46
```

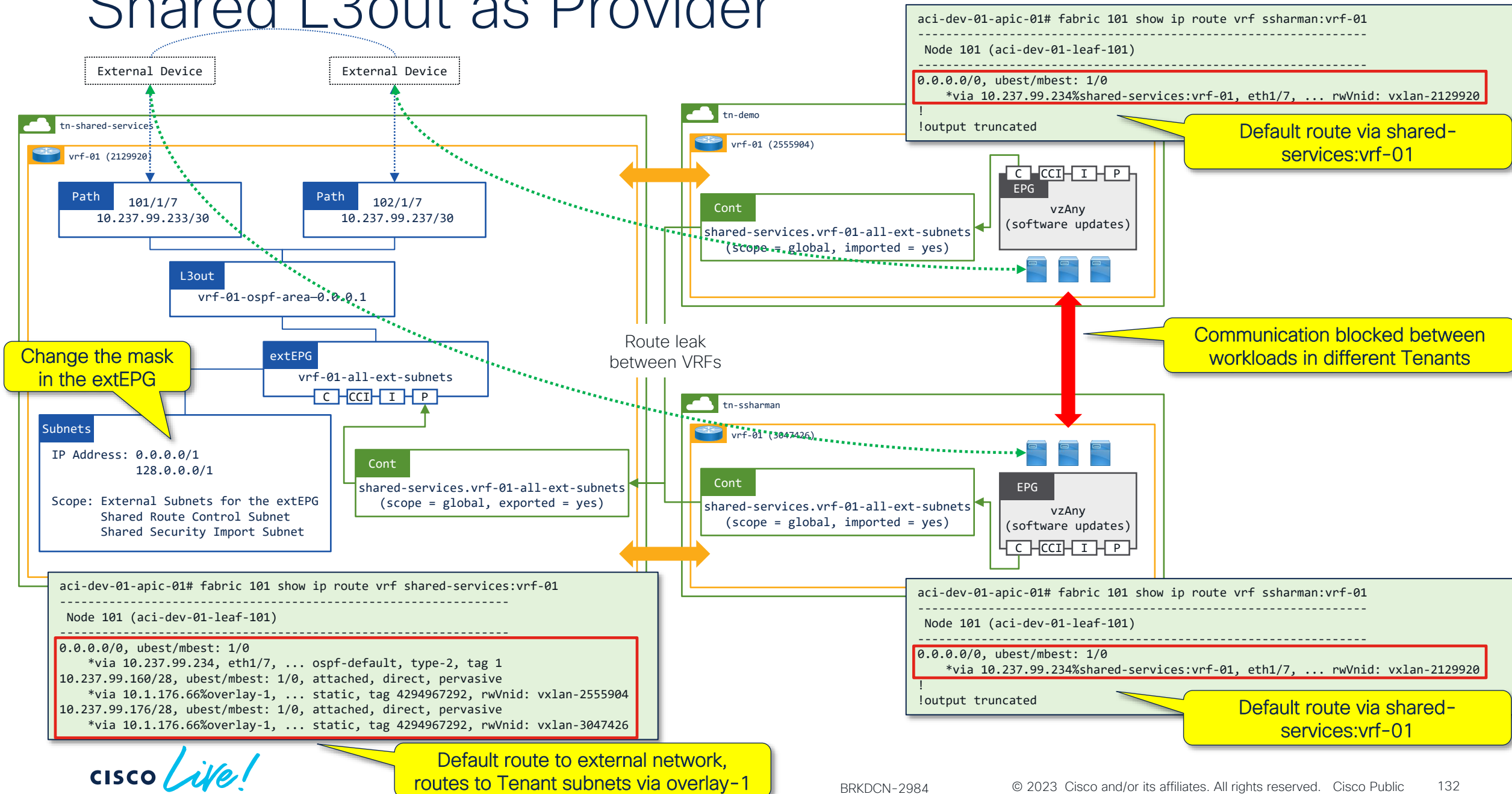
```
Node 101 (aci-dev-01-leaf-101)
```

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

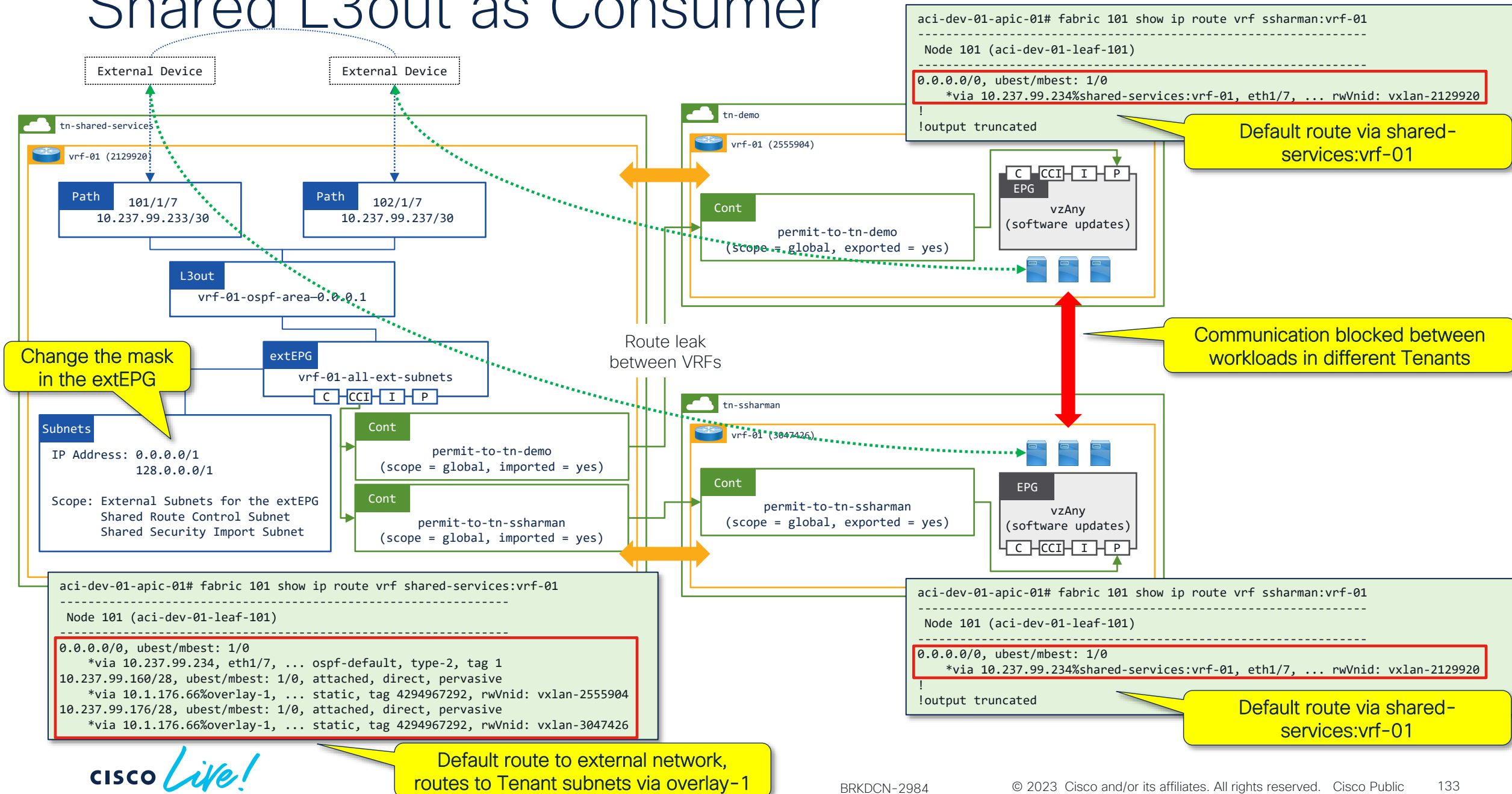
There is no zoning rule for DstEPG 14 in the consumer tenant, instead the zoning rules reflect the correct DstEPG

How should we resolve the unexpected communication...?

Shared L3out as Provider



Shared L3out as Consumer



So, what's changed...?

Get VRF scopes and Class IDs

```
aci-dev-01-apic-01# show vrf vrf-01 detail | grep shared- -B 4 -A 1
```

VRF Information:				
Tenant	VRF	VXLAN Encap	Policy Enforced	Policy Tag
shared-services-	vrf-01	2129920	enforced	16386

```
aci-dev-01-apic-01# show vrf vrf-01 detail | grep demo -B 4 -A 1
```

VRF Information:				
Tenant	VRF	VXLAN Encap	Policy Enforced	Policy Tag
demo	vrf-01	2555904	enforced	49153

```
aci-dev-01-apic-01# show vrf vrf-01 detail | grep ssharman -B 4 -A 1
```

VRF Information:				
Tenant	VRF	VXLAN Encap	Policy Enforced	Policy Tag
ssharman	vrf-01	3047426	enforced	49153

Removing 0.0.0.0/0 from the extEPG changes the pcTag to a local value

PcTag Category Name	PcTag Range
System	1-15
Global	16-16385
Local (to VRF)	16386-65535

Summary	Dashboard	Policy	Operational	Stats	Health	Faults	History
Endpoints		Flows	Packets	Policy Tags	Resource IDs		
Bridge Domains		VRFs	EPGs	ESGs	L3Outs	External Networks (Bridged)	
<div>↻ ⬇ ⚙</div>							
Class ID	Segment ID	Scope					
16386	2129920	2129920					

Get Class ID of the External EPG

```
aci-dev-01-apic-01# moquery -c l3extInstP -f 'l3ext.InstP.name=="all-external-subnets"' | egrep "^name|^pcTag|^dn|^scope"
name          : all-external-subnets
dn            : uni/tn-shared-services/out-shared-services.vrf-01-ospf-area-0.0.0.1/instP-all-external-subnets
nameAlias     :
pcTag         : 41
pcTagAllocSrc : idmanager
scope        : 2129920
```

shared-services:vrf-01
extEPG uses VXLAN Encap
2129920 and pcTag 41

PcTag Category Name	PcTag Range
System	1-15
Global	16-16385
Local (to VRF)	16386-65535

extEPG uses a pcTag from
the Global range

Summary

Dashboard

Policy

Operational

Stats

Health

Faults

History

Endpoints

Flows

Packets

Policy Tags

Resource IDs

Bridge Domains

VRFs

EPGs

ESGs

L3Outs

External Networks (Bridged)

Healthy

EPG Name

EPG Alias

Class ID

Scope

all-external-subnets

41

2129920

Resource IDs are visible in the GUI

Resource IDs are visible
in the GUI

Check the zoning rules for the shared VRF

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 src-epg 16386
```

```
-----  
Node 101 (aci-dev-01-leaf-101)  
-----
```

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

SrcEPG /DstEPG 16386 = VRF ClassID

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 dst-epg 16386
```

```
-----  
Node 101 (aci-dev-01-leaf-101)  
-----
```

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

Output truncated

There are now no
zoning rules to the VRF

Check the zoning rules for the shared VRF extEPG

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 src-epg 41
```

```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope
4301	41	14	implicit	uni-dir	enabled	2129920
4466	41	0	default	uni-dir-ignore	enabled	2129920

SrcEPG /DstEPG 41 = VRF extEPG ClassID

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 dst-epg 41
```

```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope
4487	0	41	default	bi-dir	enabled	2129920

Output truncated

There are now zoning rules to the extEPG

Do not use 0.0.0.0/0 in route leaking design...!

Check the zoning rules for the shared VRF and extEPG

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 src-epg 16386
```

```
Node 101 (aci-dev-01-leaf-101)
```

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

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 dst-epg 16386
```

```
Node 101 (aci-dev-01-leaf-101)
```

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

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 src-epg 41
```

```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Priority
4301	41	14	implicit	uni-dir	enabled	2129920		permit_override	src_dst_any(9)
4466	41	0	default	uni-dir-ignore	enabled	2129920	shared-services:shared-services.vrf-01-all-ext-subnets	permit	shsrc_any_any_perm(11)

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 dst-epg 41
```

```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Priority
4487	0	41	default	bi-dir	enabled	2129920	shared-services:shared-services.vrf-01-all-ext-subnets	permit	shsrc_any_any_perm(11)

SrcEPG = extEPG
DstEPG = all EPGs/ESGs which are consumers of shared services

pcTag 14 allows traffic from the provider to the consumer without the "policy applied bit" set

Let's check the target tenants zoning rules...

Check the zoning rules for the demo VRF

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2555904 src-epg 41
```

```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Priority
4305	41	0	default	uni-dir-ignore	enabled	2555904	shared-services:shared-services.vrf-01-all-ext-subnets	permit	shsrc_any_any_perm(11)
4228	41	0	implicit	uni-dir	enabled	2555904		deny,log	shsrc_any_any_deny(12)

SrcEPG = shared services extEPG
DstEPG = vsAny

```
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2555904 dst-epg 41
```

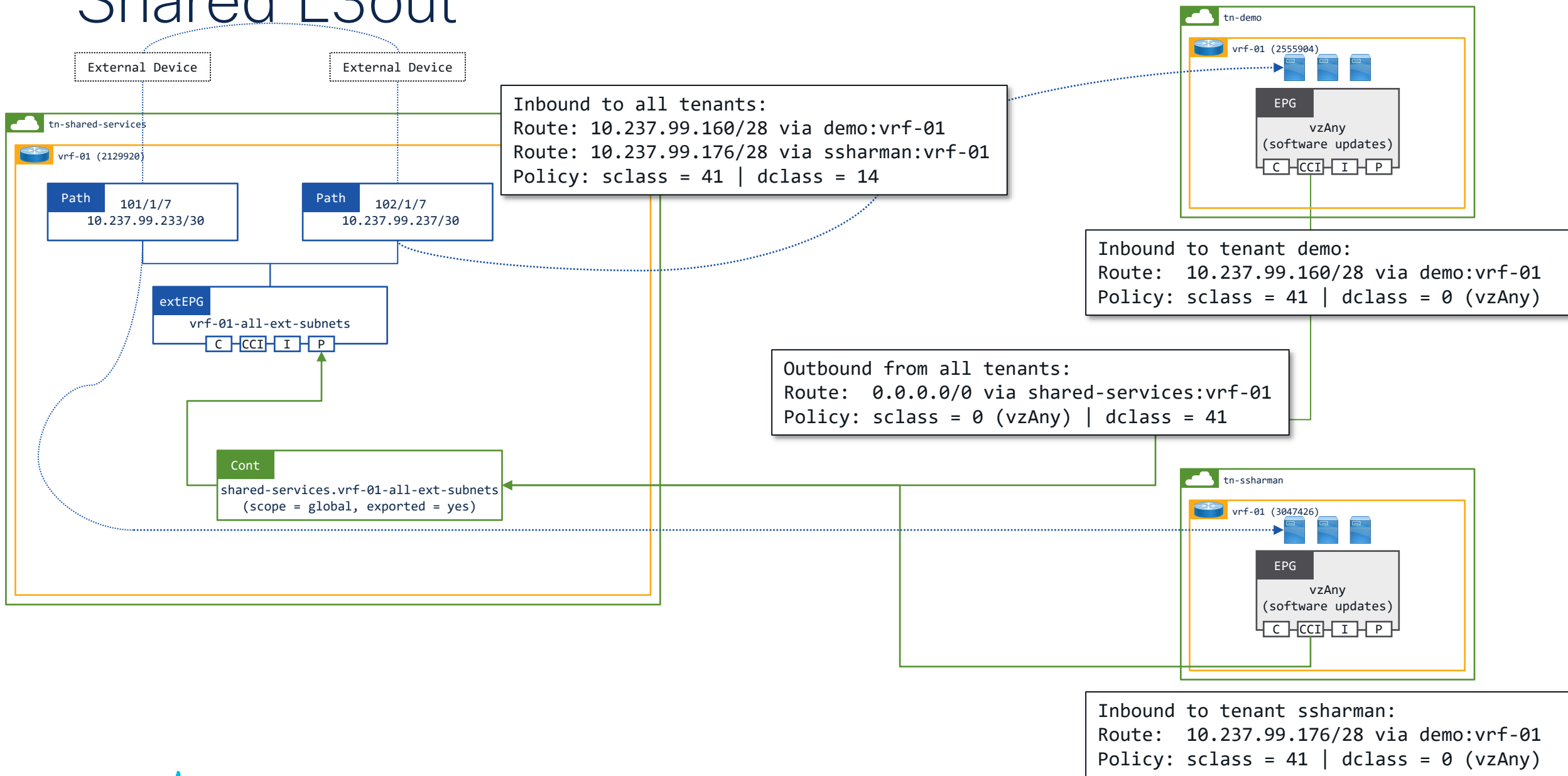
```
Node 101 (aci-dev-01-leaf-101)
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Priority
4339	0	41	default	bi-dir	enabled	2555904	shared-services:shared-services.vrf-01-all-ext-subnets	permit	shsrc_any_any_perm(11)

SrcEPG = shared services VRF
DstEPG = all EPGs/ESGs (vzAny)

```
aci-dev-01-apic-01#
```

Shared L3out



Scenario 1 – Provider and multiple Consumer VRFs are on the same Leaf with /0 mask

1. The packet from the source consumer VRF hits the contract for source EPG/ESG to pcTag 15 (extEPG with 0.0.0.0/0)
2. Since the leaf knows the egress port and destination VRF (shared), the packet will be sent out from that port without going through another lookup on the destination VRF (shared)
3. The packet comes back from the external router
4. The packet gets the sclass of VRF and dclass 14
5. The packet is allowed in the shared VRF because there are contracts between the VRF pcTag and 14 in the shared VRF
6. Just like step 2, the packet is sent out to the destination endpoint without going through another lookup in the destination consumer VRF because the leaf knows the egress port and its destination VRF

Scenario 2 – Provider and multiple Consumer VRFs are on different Leafs with /0 mask

1. The packet from the source consumer VRF hits the contract for vzAny to 15
2. The packet reaches the shared VRF leaf. Another lookup happens. The forwarding points another leaf
3. The packet gets dropped because of a internal TCAM ACL rule (not a contract) that prevents traffic bouncing back to spines without a bounce entry

Scenario 1 – Provider and multiple Consumer VRFs are on the same Leaf with /1 mask

1. The packet from the source consumer VRF hits the contract for source EPG/ESG to pcTag of extEPG with 0.0.0.0/1 and 128.0.0.0./1 mask
2. Since the leaf knows the egress port and destination VRF (shared), the packet will be sent out from that port without going through another lookup on the destination VRF (shared)
3. The packet comes back from the external router
4. The packet gets the sclass of the extEPG and dclass 14
5. The packet is allowed in the shared VRF because there are contracts between the VRF pcTag and 14 in the shared VRF
6. Just like step 2, the packet is sent out to the destination endpoint without going through another lookup in the destination consumer VRF because the leaf knows the egress port and its destination VRF

Scenario 2 – Provider and multiple Consumer VRFs are on different Leafs with /1 mask

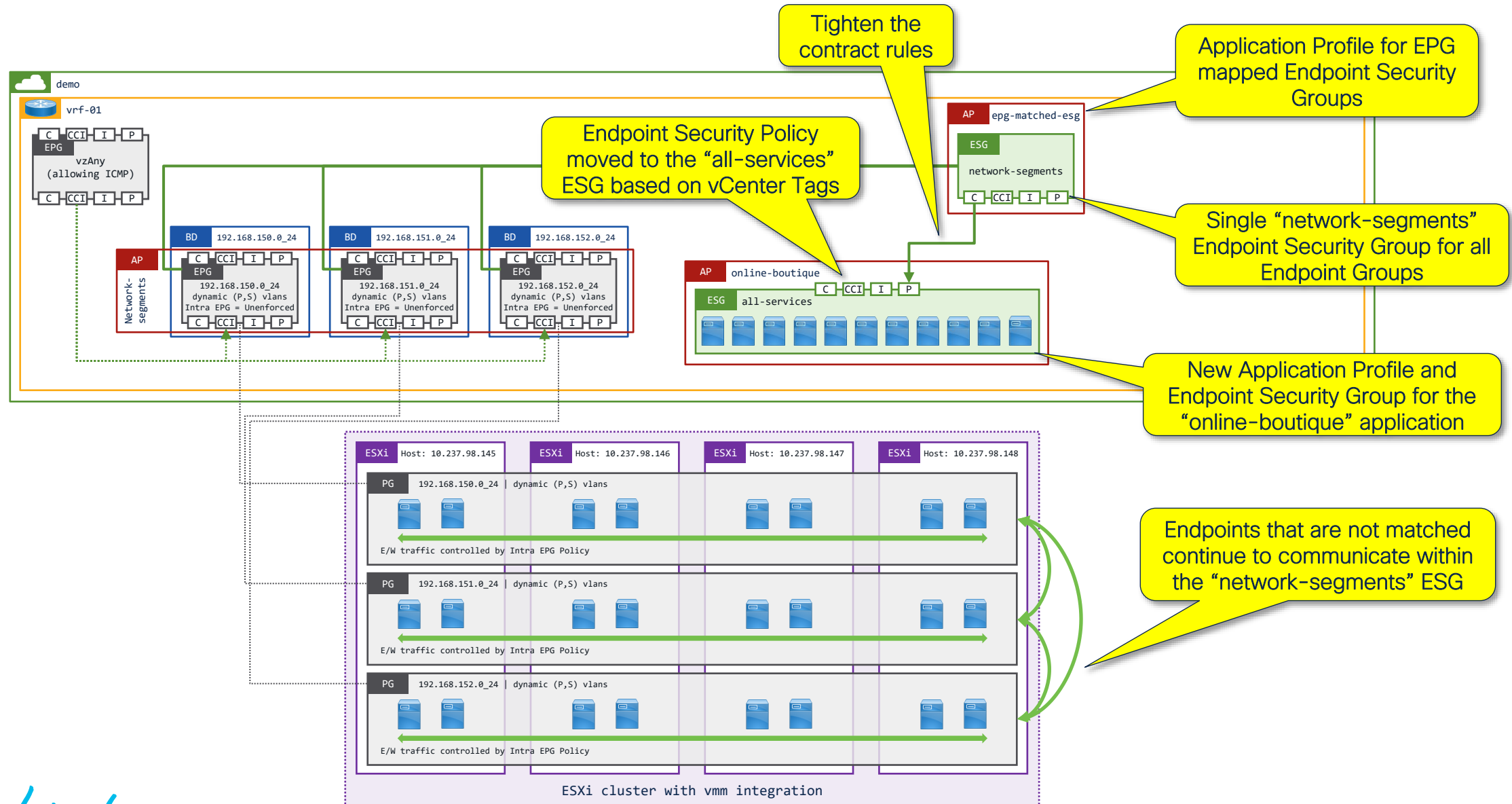
1. The packet from the source consumer VRF hits the contract for source EPG/ESG to pcTag of extEPG with 0.0.0.0/1 and 128.0.0.0./1 mask
2. The packet reaches the shared VRF leaf. Another lookup happens. The forwarding points another leaf
3. The packet gets dropped because of a internal TCAM ACL rule (not a contract) that prevents traffic bouncing back to spines without a bounce entry

Tightening Security...



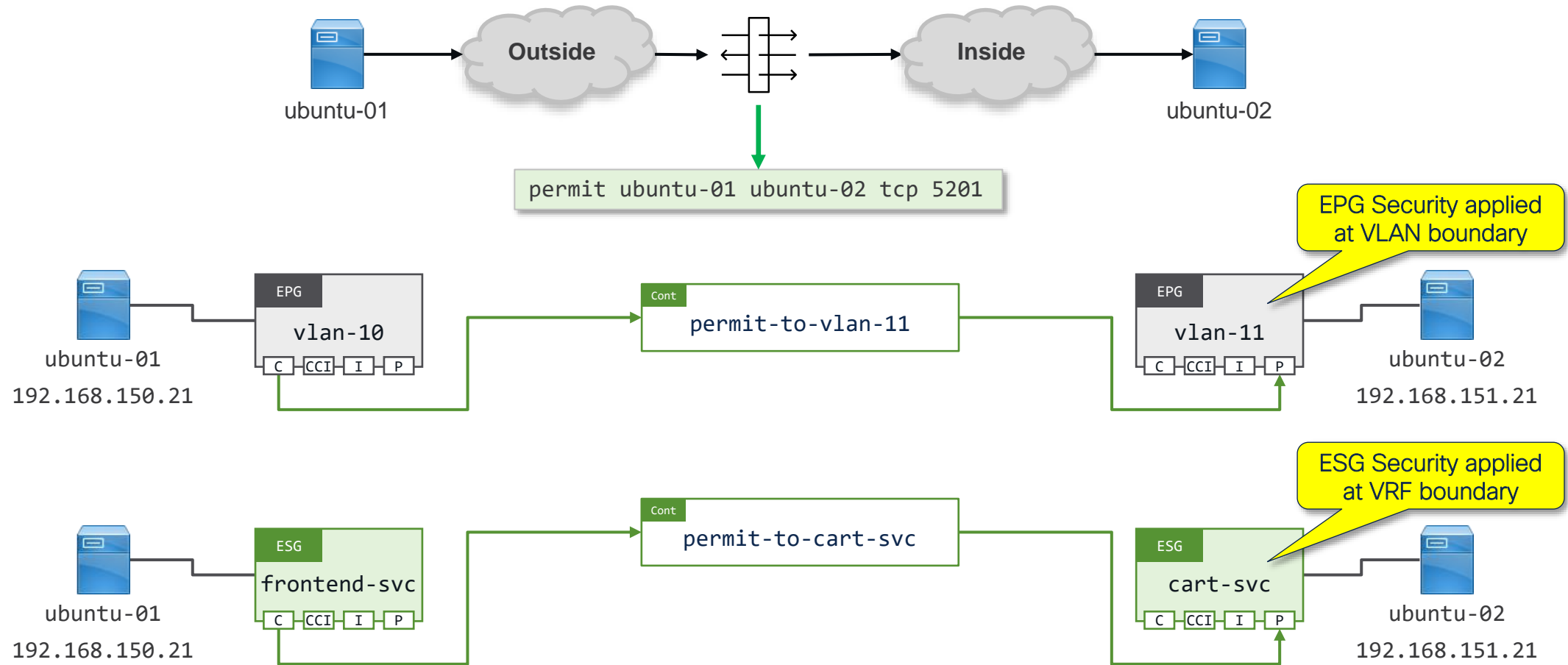
Let's tighten the contract to our online-boutique application...

Tighten the contract to our online-boutique application...



Before we do that, let's check our understanding on how contracts work...

How do contracts work...?

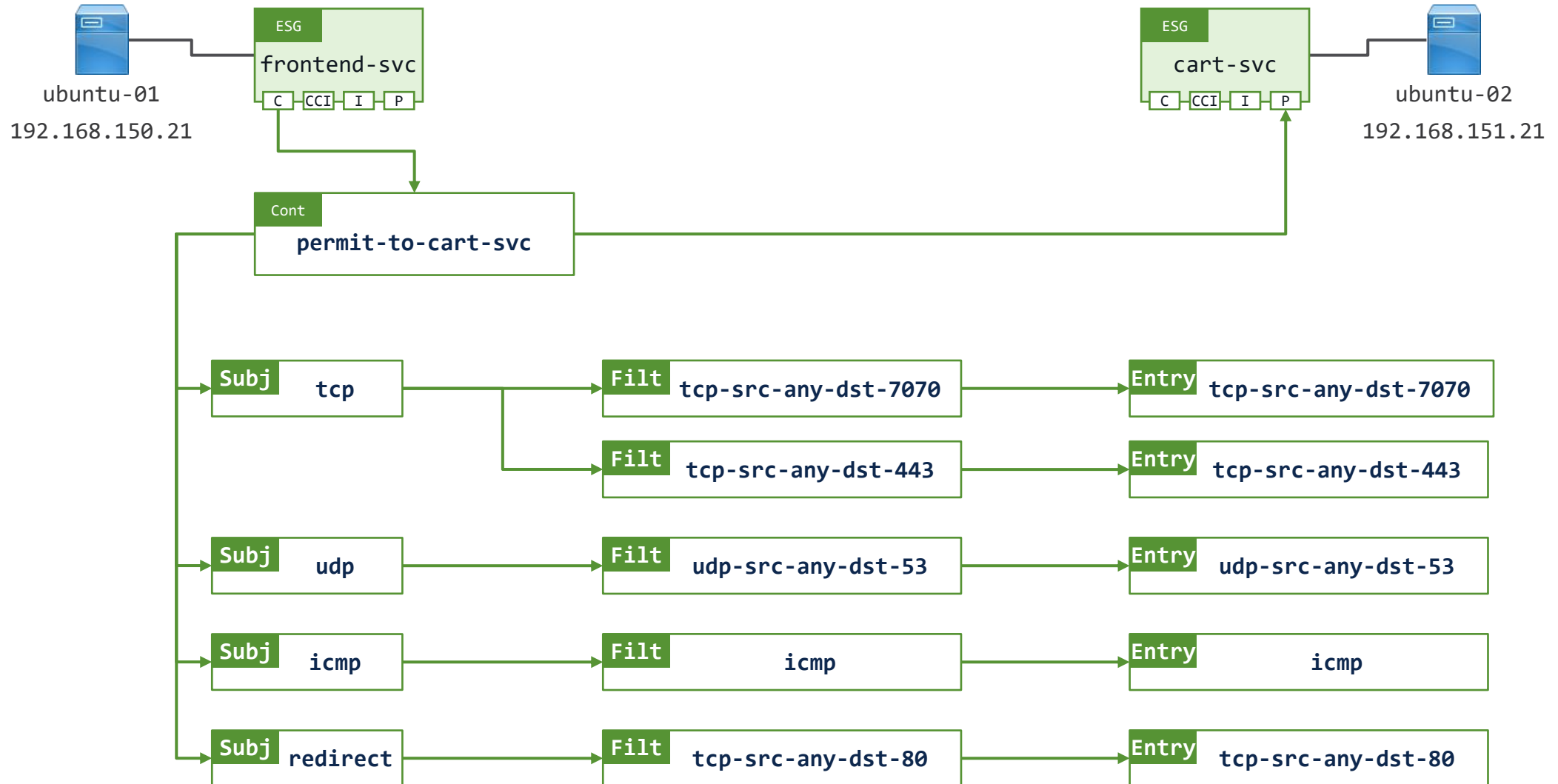


*arrows indicates direction of traffic flow i.e. from consumer to provider

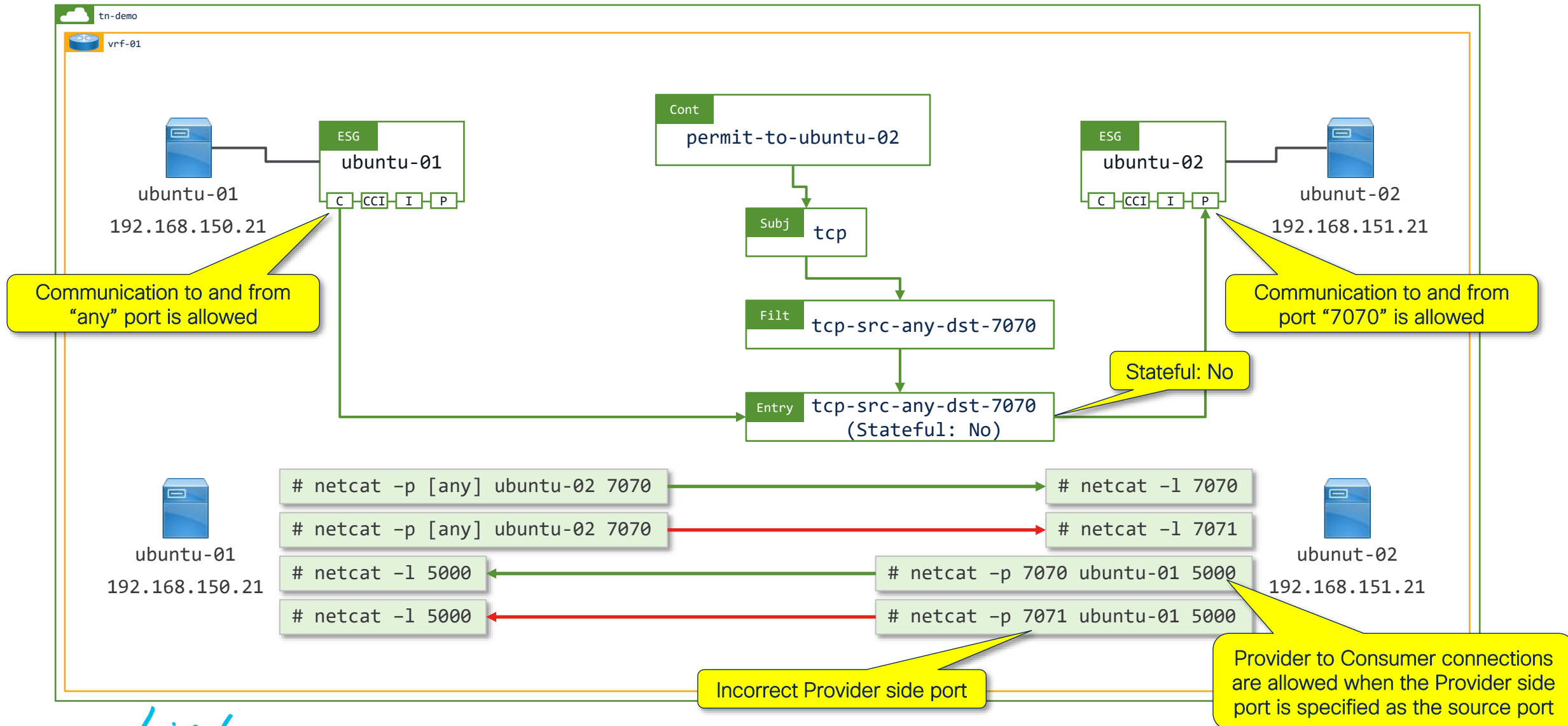
Consumer and Provider relationships are there to help you visualize the traffic
flow direction
i.e. (typically) from the consumer to the provider

Consumer and Provider relationships do not (by default) prevent TCP
connections being established from the Provider to the Consumer

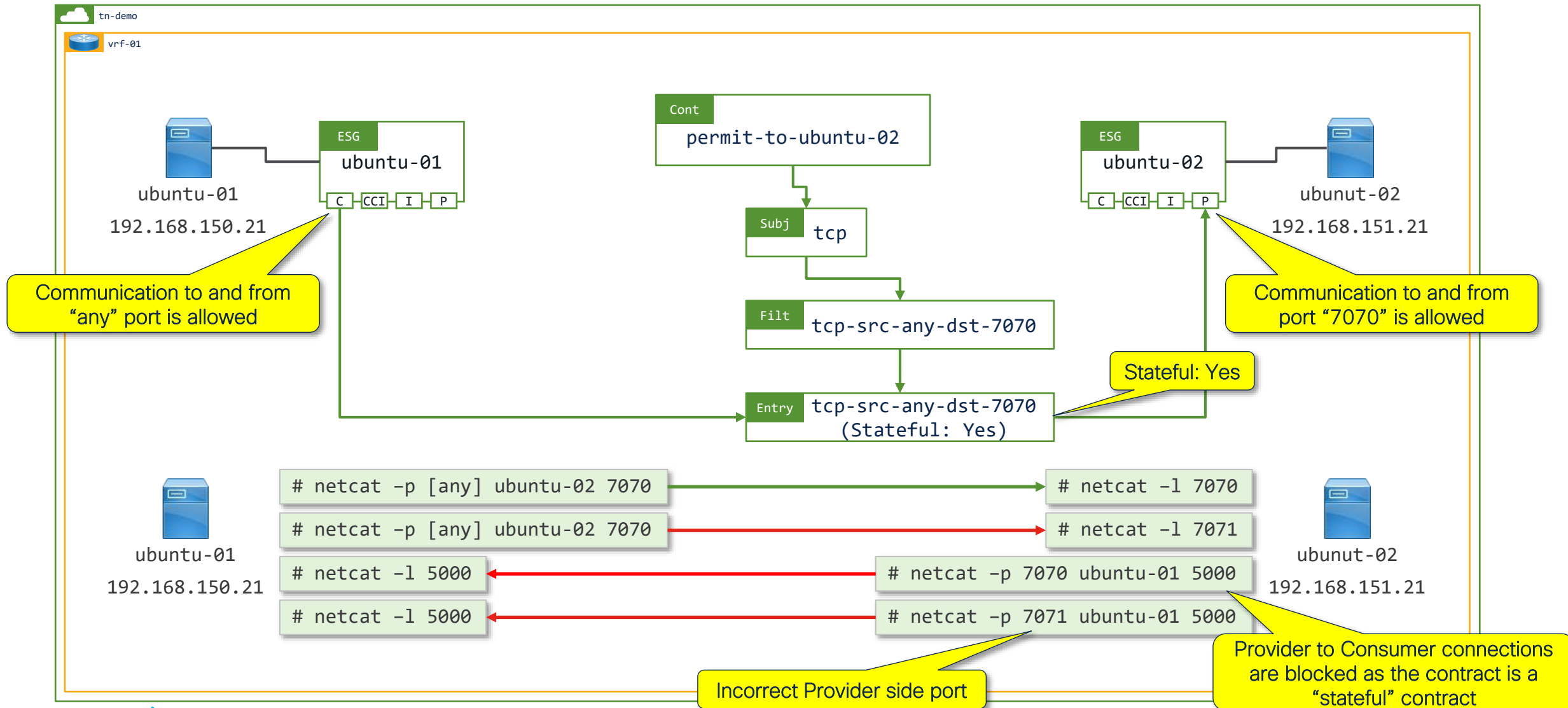
Contract structure...

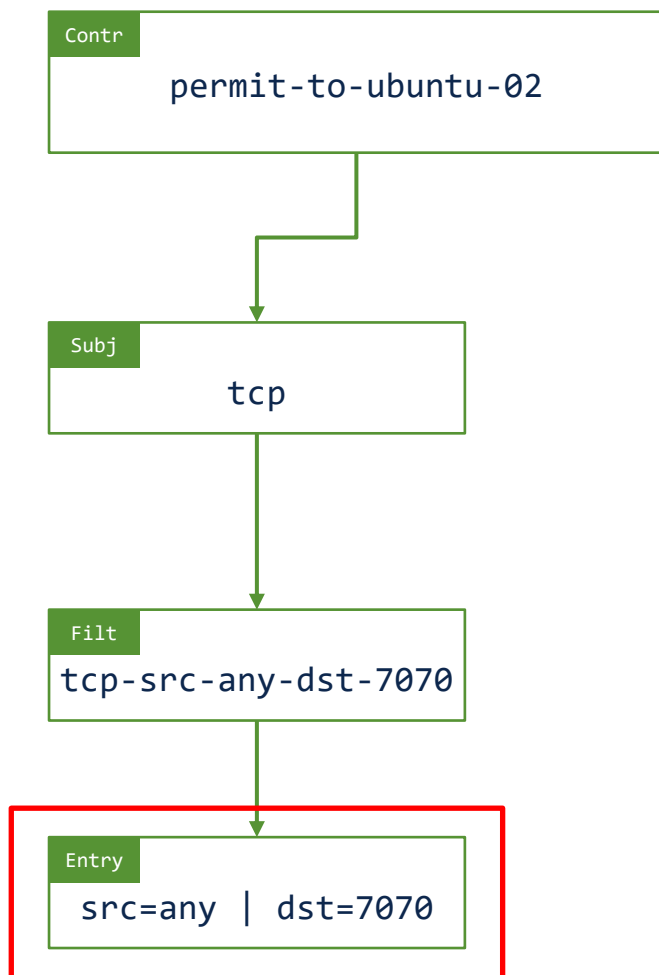


Verifying Contract operation with netcat – Stateful = No



Verifying Contract operation with netcat – Stateful = Yes

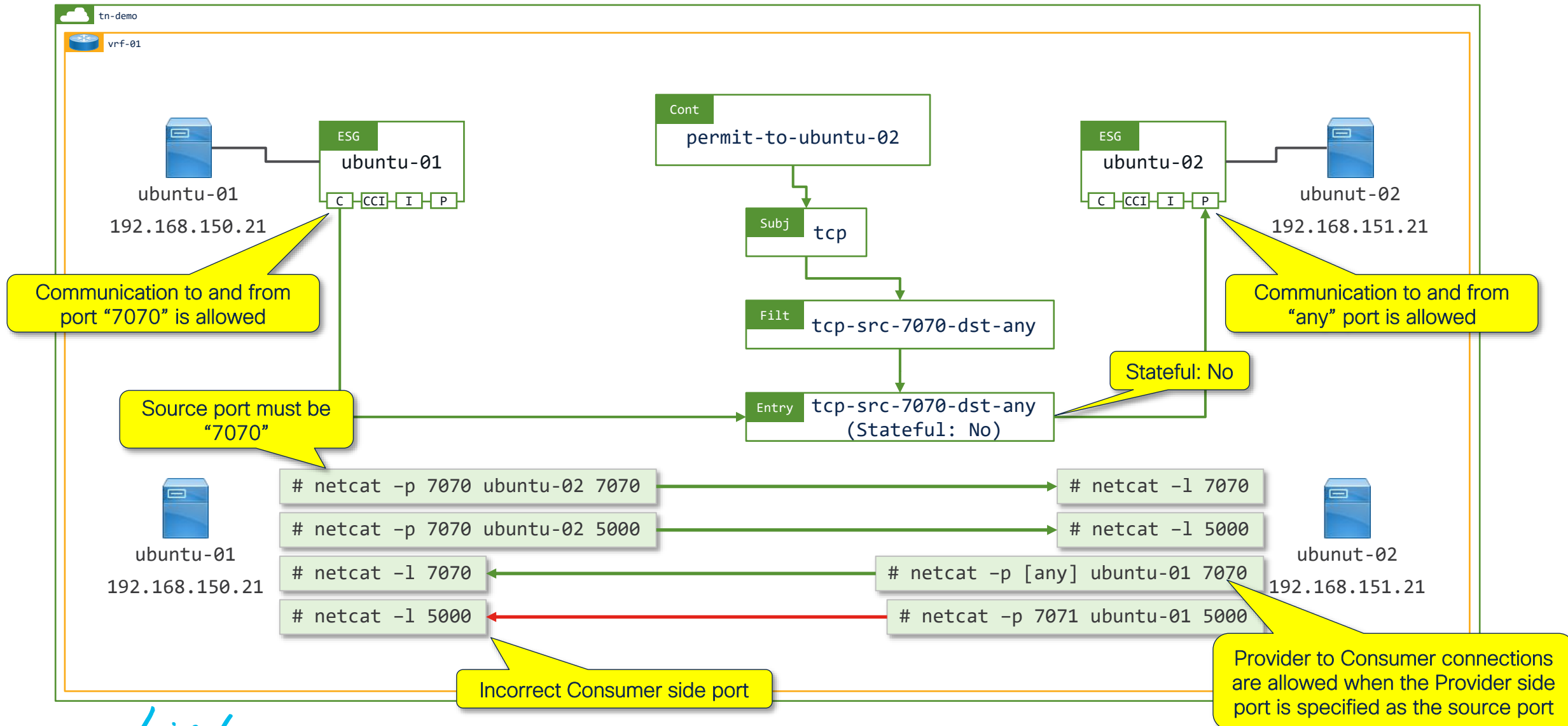




Filter Entry source port =
port opened on the consumer EPG/ESG

Filter Entry destination port =
port opened on the provider EPG/ESG

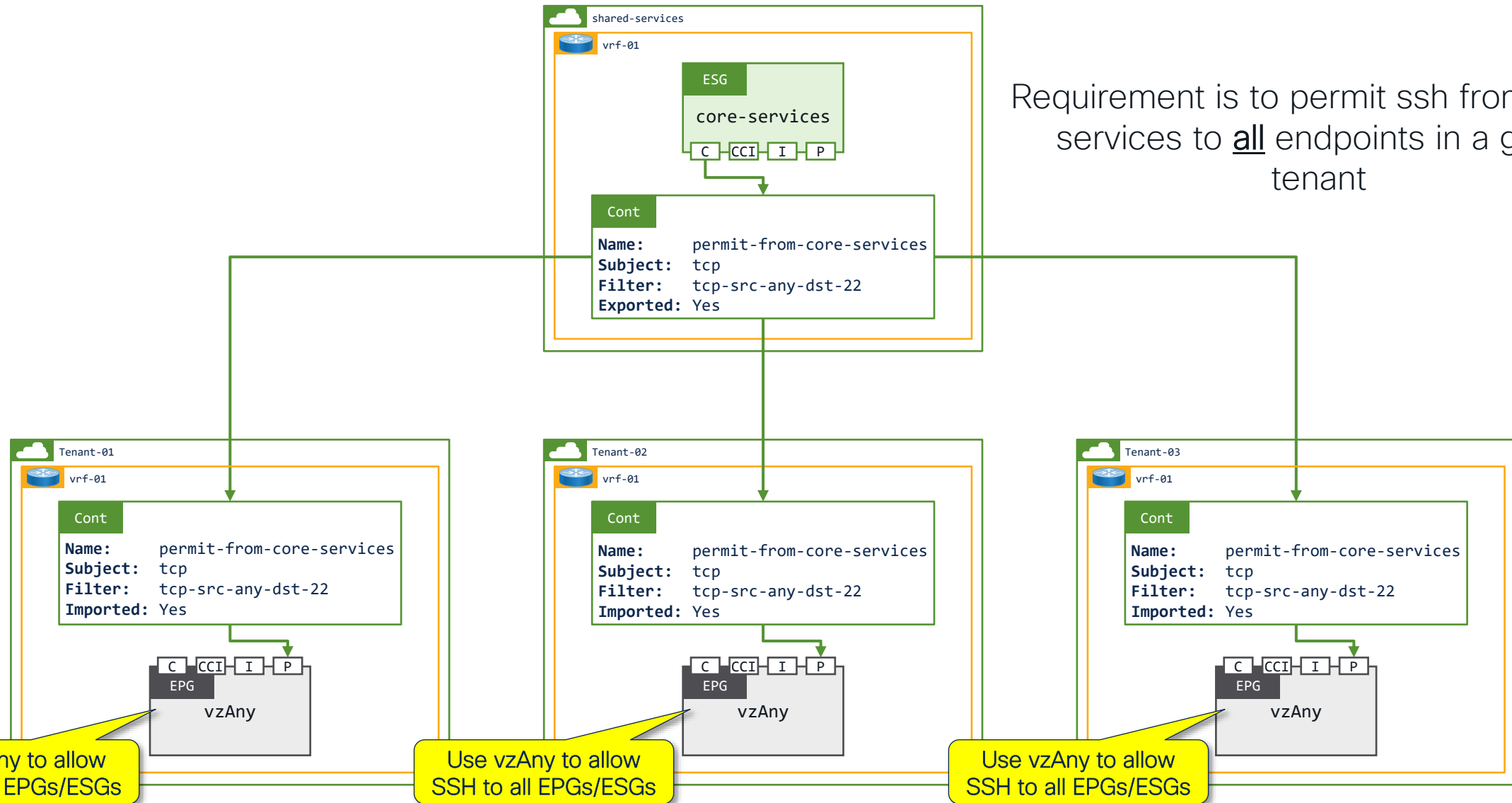
Reversing the Filter ports - Stateful = No



Why would you want to reverse the Consumer and Provider Filters...?

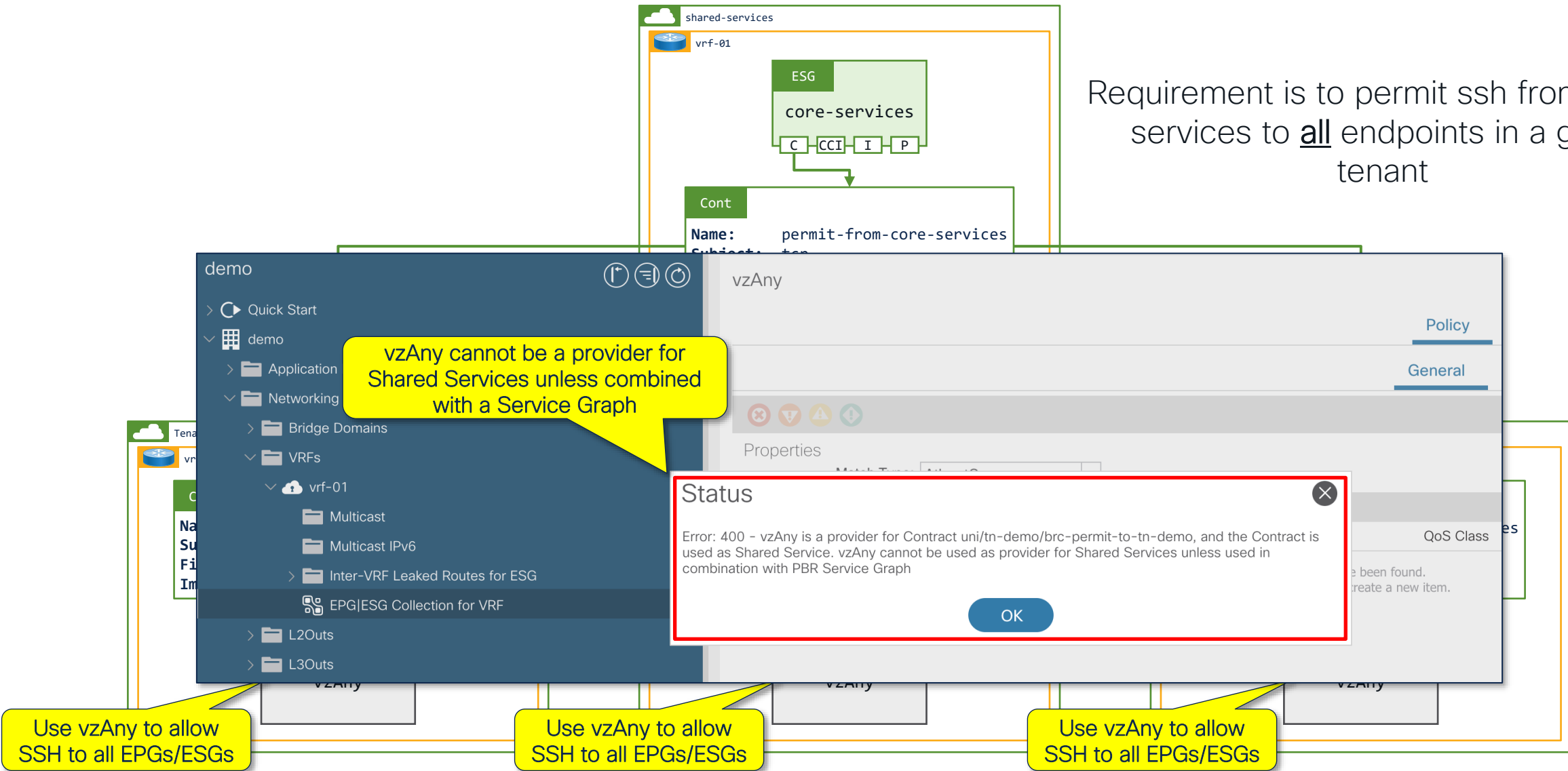
vzAny as a contract Provider

Requirement is to permit ssh from core-services to all endpoints in a given tenant

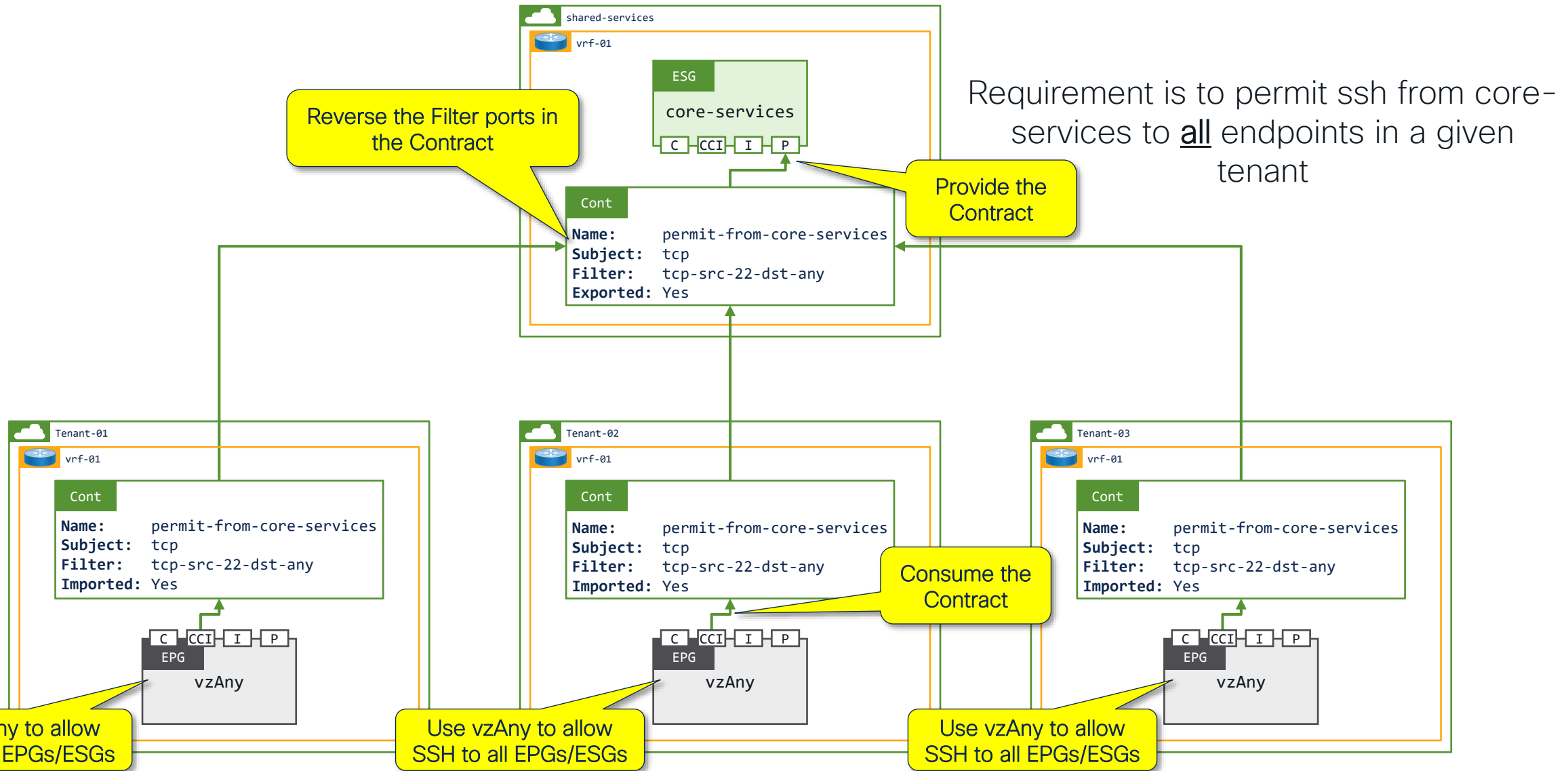


vzAny as a contract Provider

Requirement is to permit ssh from core-services to all endpoints in a given tenant



vzAny as a contract Consumer – Filters Reversed



vzAny as a contract Consumer – Filters Reversed

Requirement is to permit ssh from core- given

demo

- Quick Start
- demo
 - Application Profiles
 - Networking
 - Bridge Domains
 - VRFs
 - vrf-01
 - Multicast
 - Multicast IPv6
 - Inter-VRF Leaked Routes for E...
 - EPG|ESG Collection for VRF
 - L2Outs
 - L3Outs
 - SR-MPLS VRF L3Outs
 - Dot1Q Tunnels
 - Contracts
 - Policies
 - Services
 - Security

vzAny

Policy Operational

General Subject Labels

Properties

Match Type: AtleastOne

Provided Contracts:

Name	Tenant	Type	QoS Class	Match Type	State
No items have been found. Select Actions to create a new item.					

Consumed Contracts:

Name	Tenant	Type	QoS Class	State
No items have been found. Select Actions to create a new item.				

Contract Interfaces:

Name	Tenant	Type	QoS Class	State
permit-from-core-services	demo	Contract Interface	Unspecified	formed
permit-to-core-services	demo	Contract Interface	Unspecified	formed

Consume the exported contract(s)

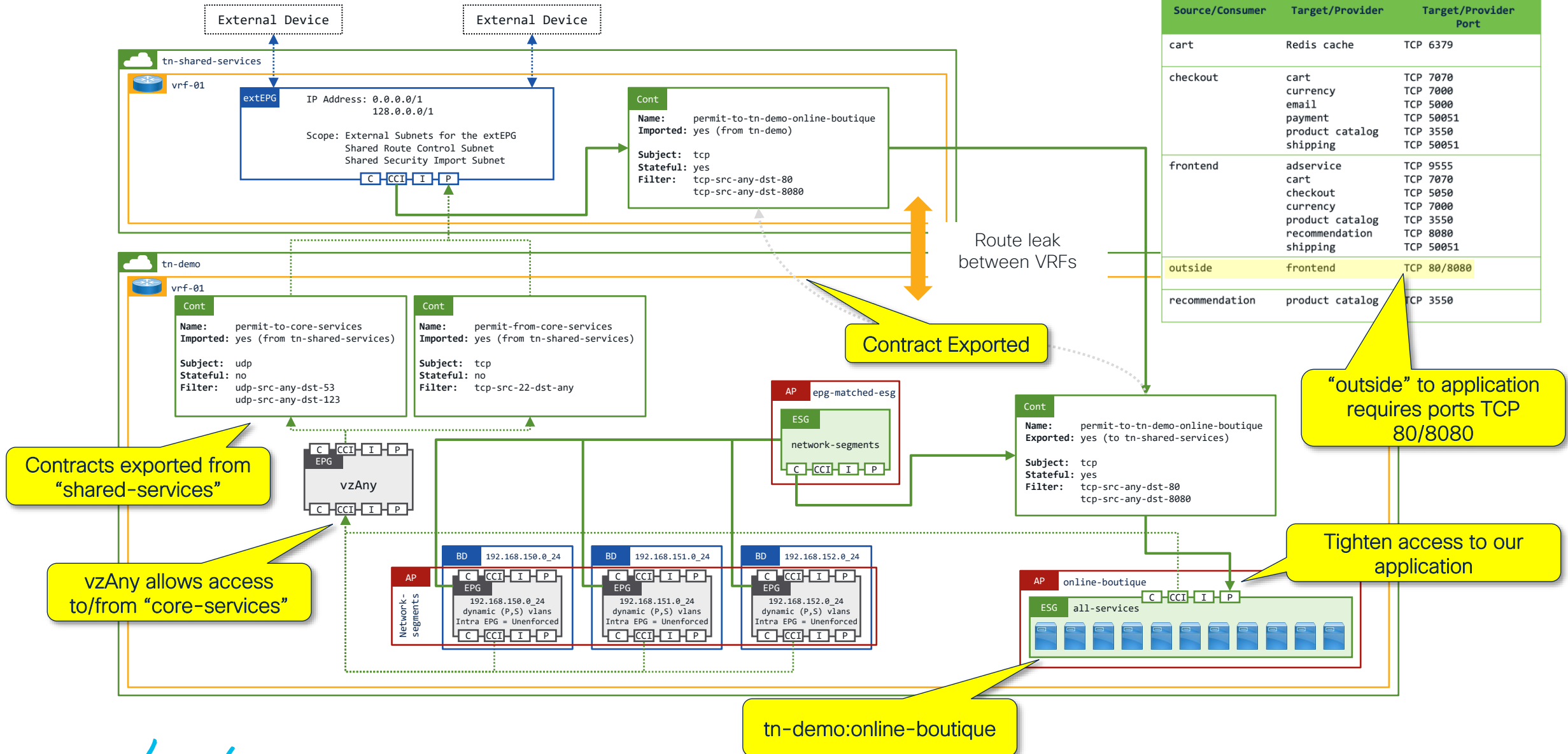
Use vzAny to allow SSH to all EPGs/ESGs

Use vzAny to allow SSH to all EPGs/ESGs

Use vzAny to allow SSH to all EPGs/ESGs

Let's tighten the contract to our online-boutique application...

Tighten access to our online-boutique application...



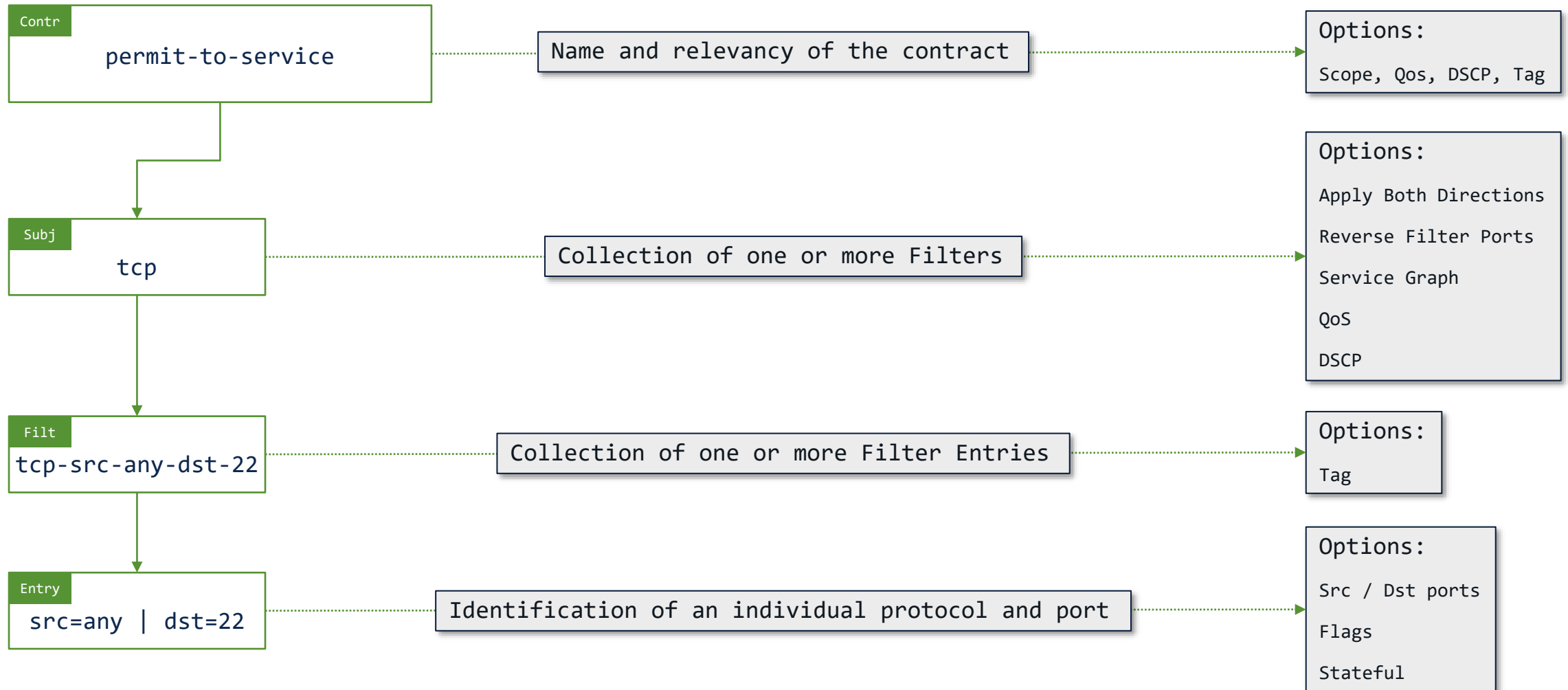
Contracts: The hidden details



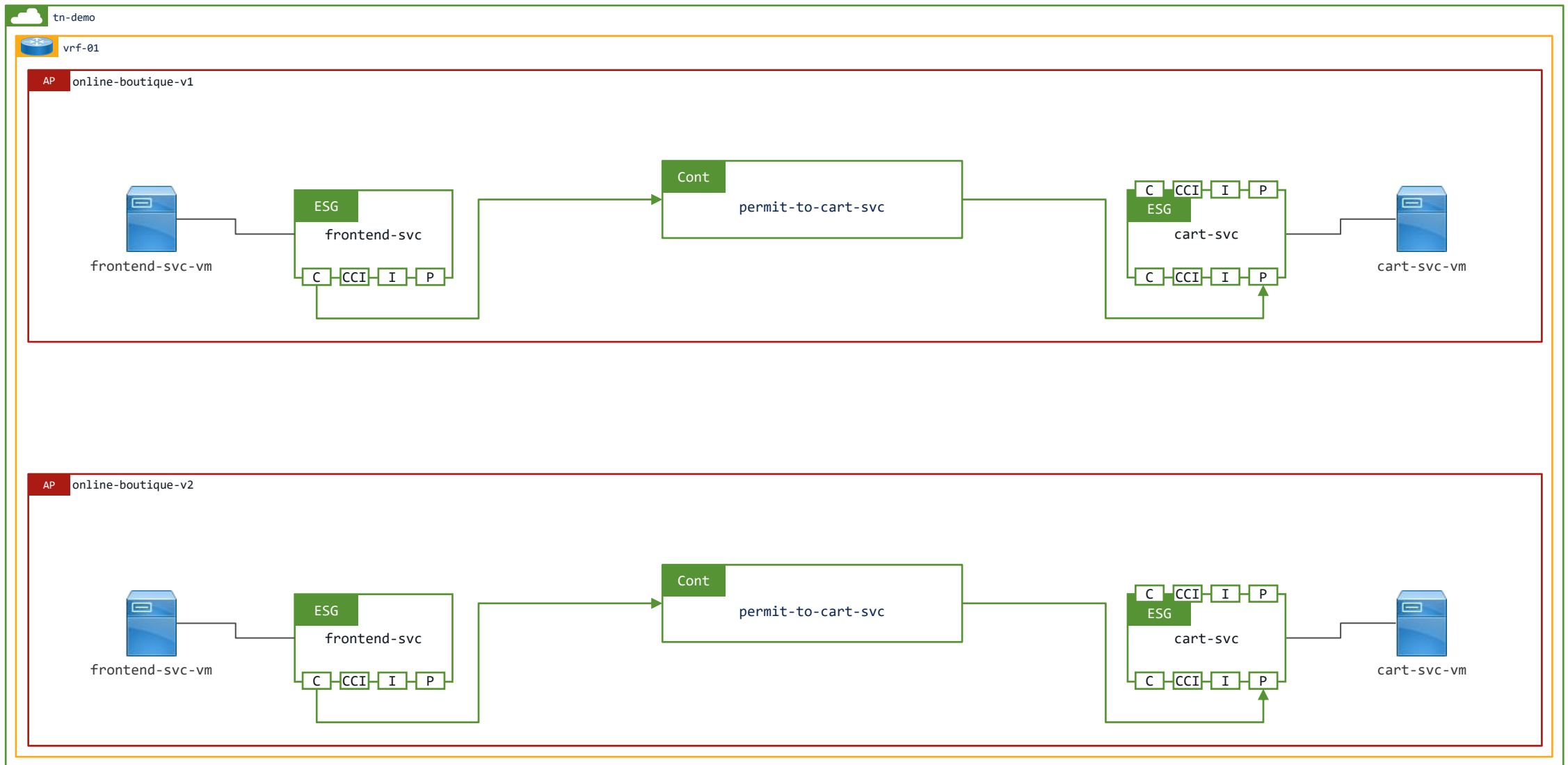
Contract Scope

- The scope of a contract defines where a contract is relevant, there are four options:
 - Application Profile– used to control traffic within an Application Profile
 - VRF – used to control traffic between EPG/ESG within a VRF
 - Tenant – used to control traffic between EPG/ESG across VRFs within a Tenant
 - Global – used to control traffic between EPG/ESG in different Tenants/VRFs
- Contract definitions can be reused allowing you define once and reference many times
 - Note: Exercise caution when reusing contract definitions at this can lead to unexpected communication
 - Recommendation: define explicit contracts rather than n:1 reference

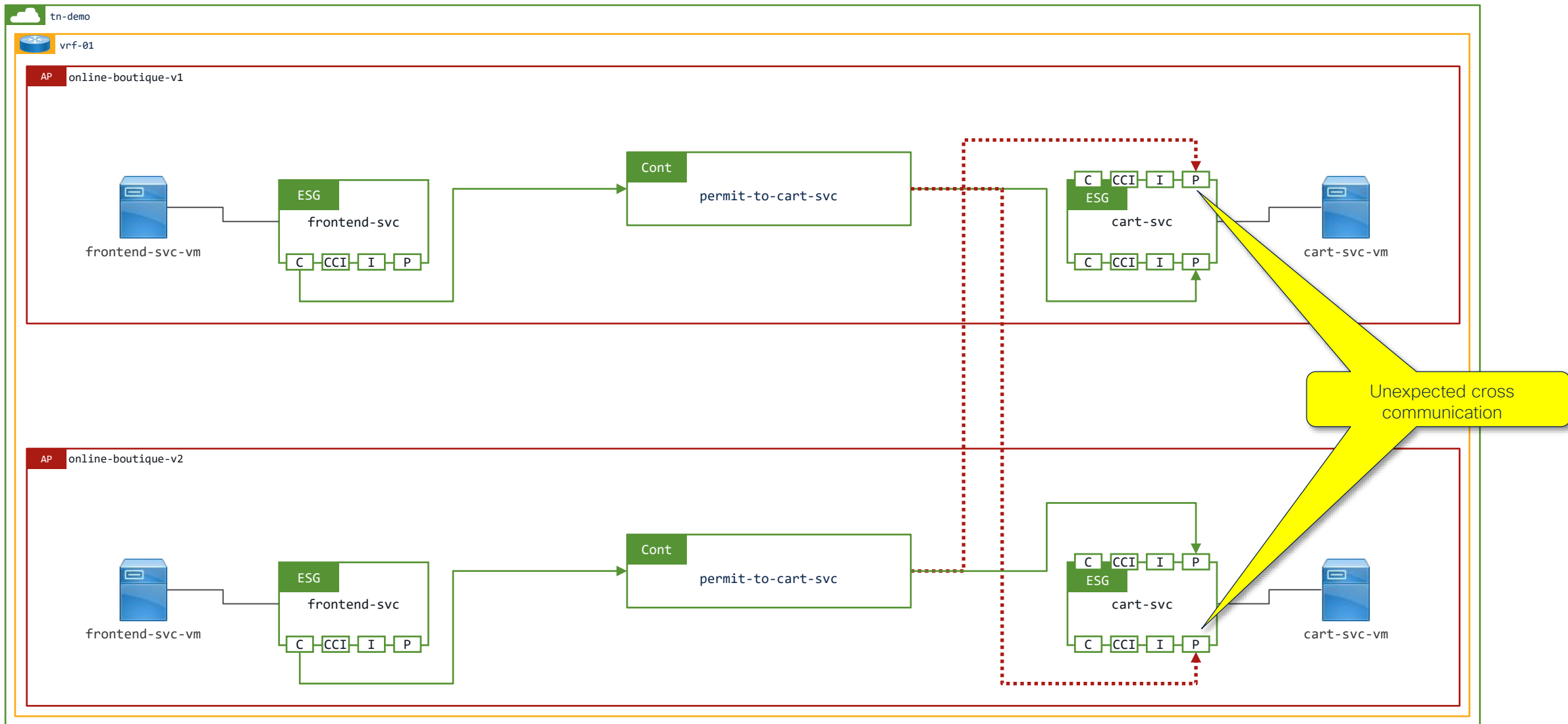
What are the components of a contract...



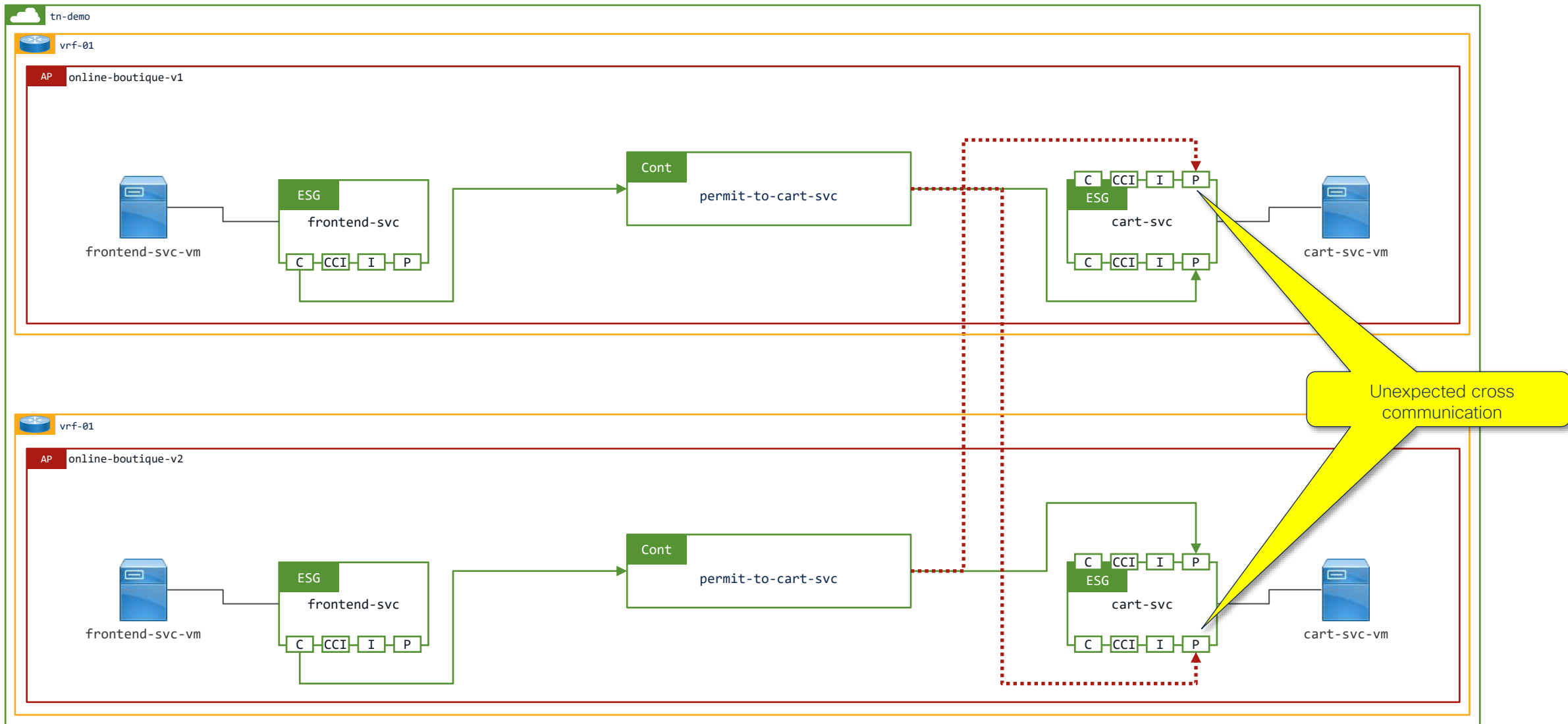
Contract Scope = Application, Contract re-use = yes



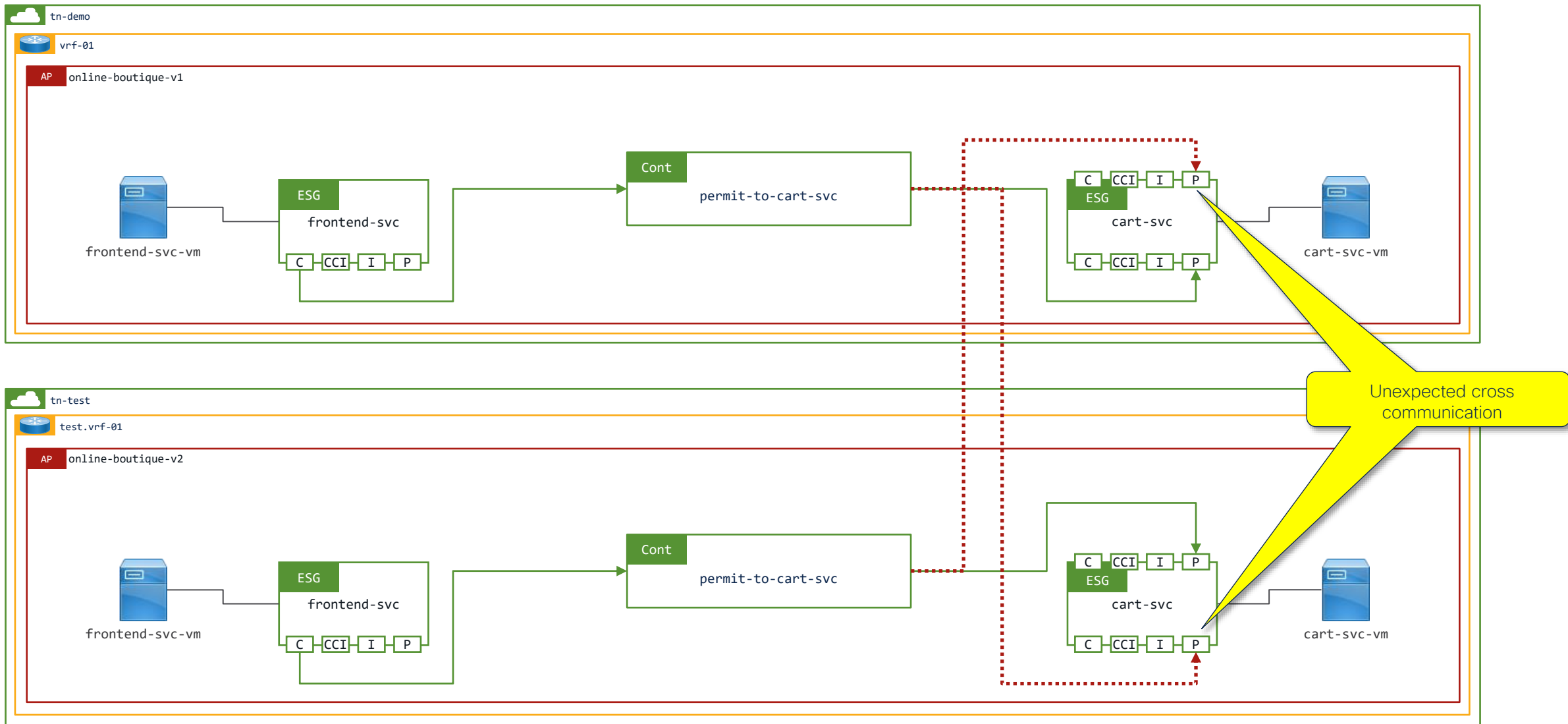
Contract Scope = VRF, Contract re-use = yes



Contract Scope = Tenant, Contract re-use = yes

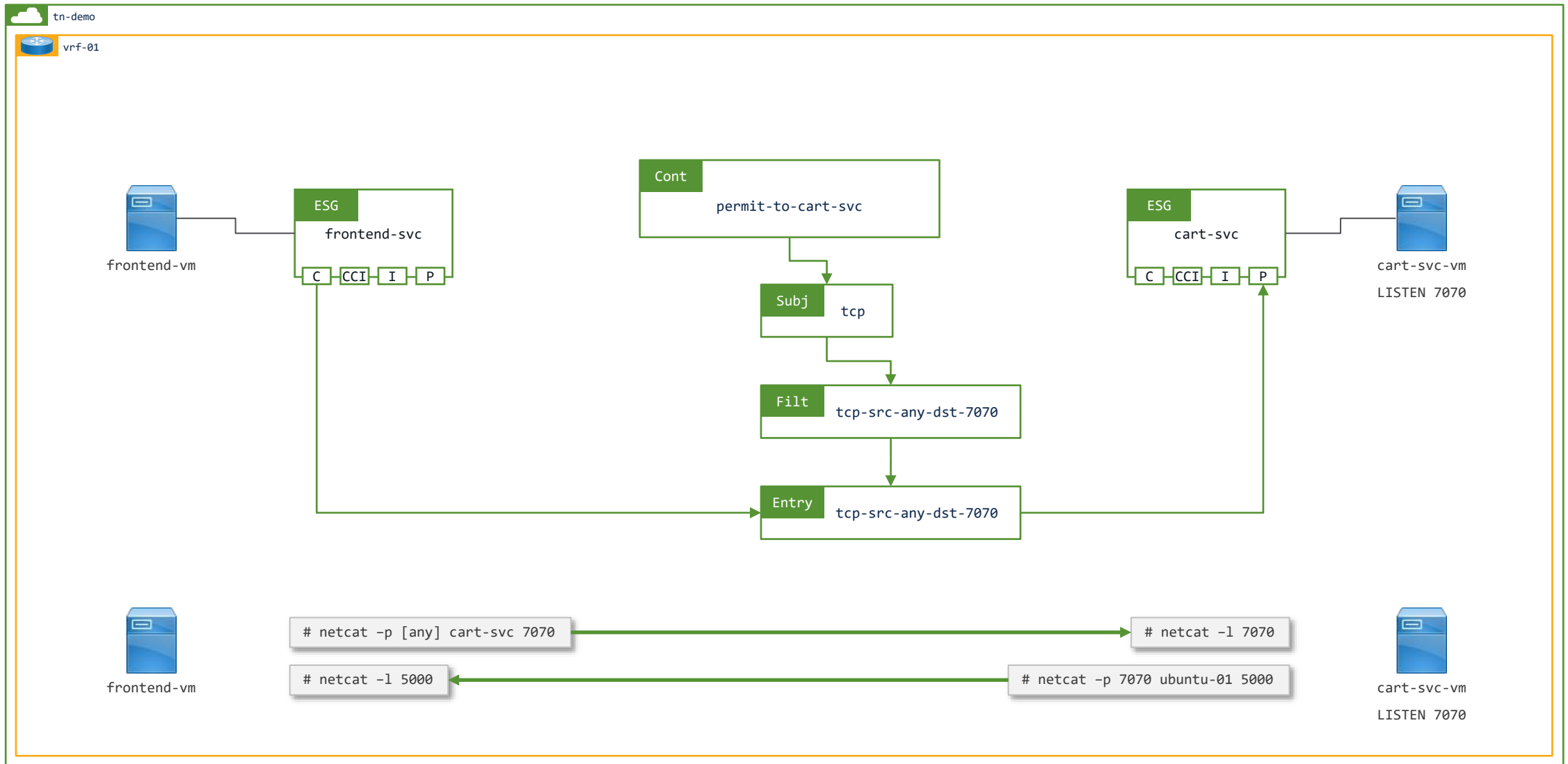


Contract Scope = Global, Contract re-use = yes



Option 1: Apply in both directions, reverse ports

Option 1: Apply in both directions, reverse ports (default)



Option 1: Apply in both directions, reverse ports (default)

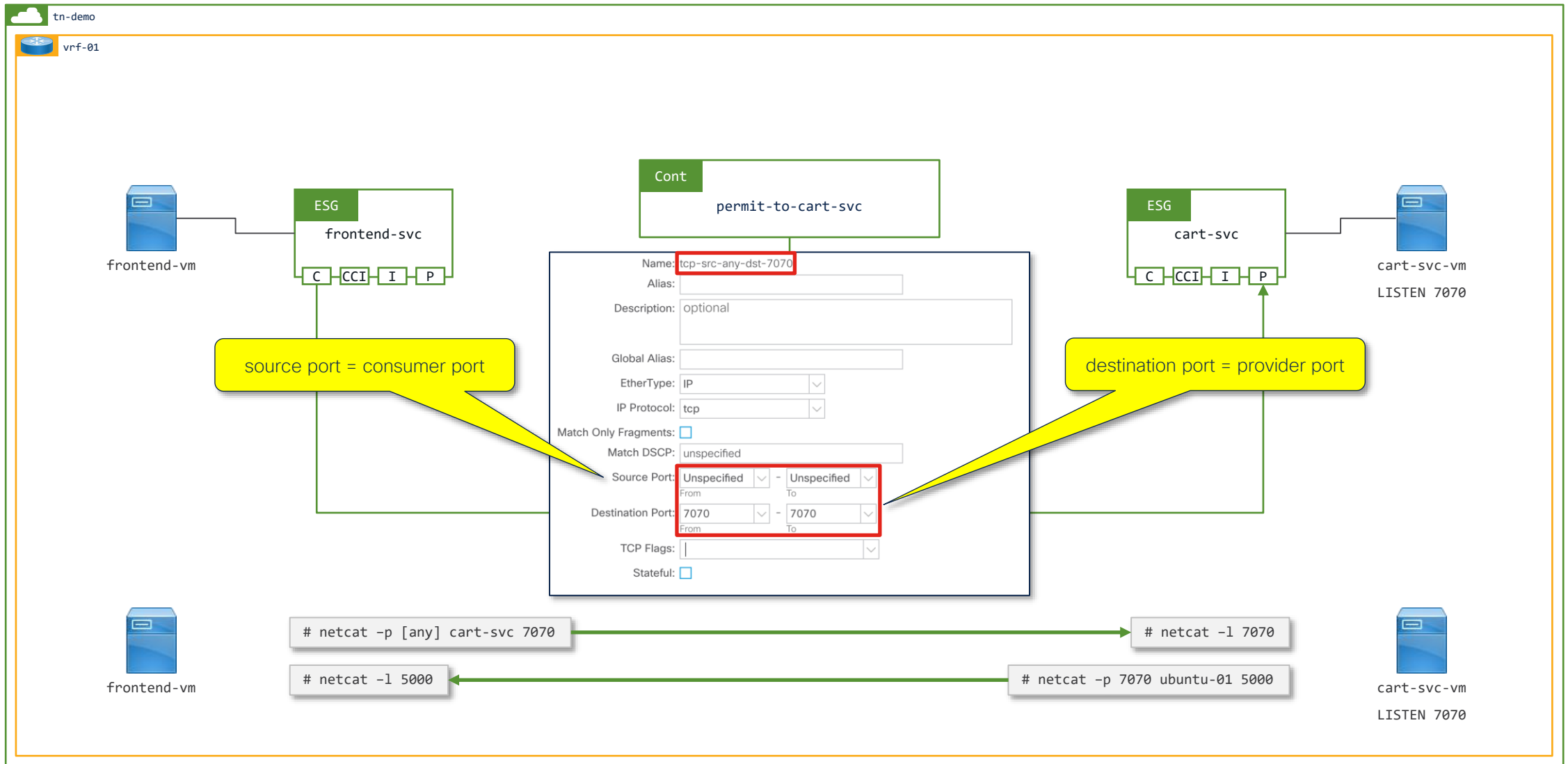
The screenshot displays the Cisco SD-WAN configuration interface for a contract named "permit-to-cart-svc". The contract is applied to the "frontend-svc" and "cart-svc" services. The configuration is shown in the "Policy" tab, with the "General" sub-tab selected. The "Contract Subject - tcp" is highlighted. The "Apply Both Directions" checkbox is checked, and the "Reverse Filter Ports" checkbox is also checked. The "Filters" table shows a single filter named "tcp-src-any-dst-7070" with a "Permit" action and "default level" priority.

Annotations:

- Apply the rules in both directions
- Automatically reverse the filter ports
- Reference the required Filters

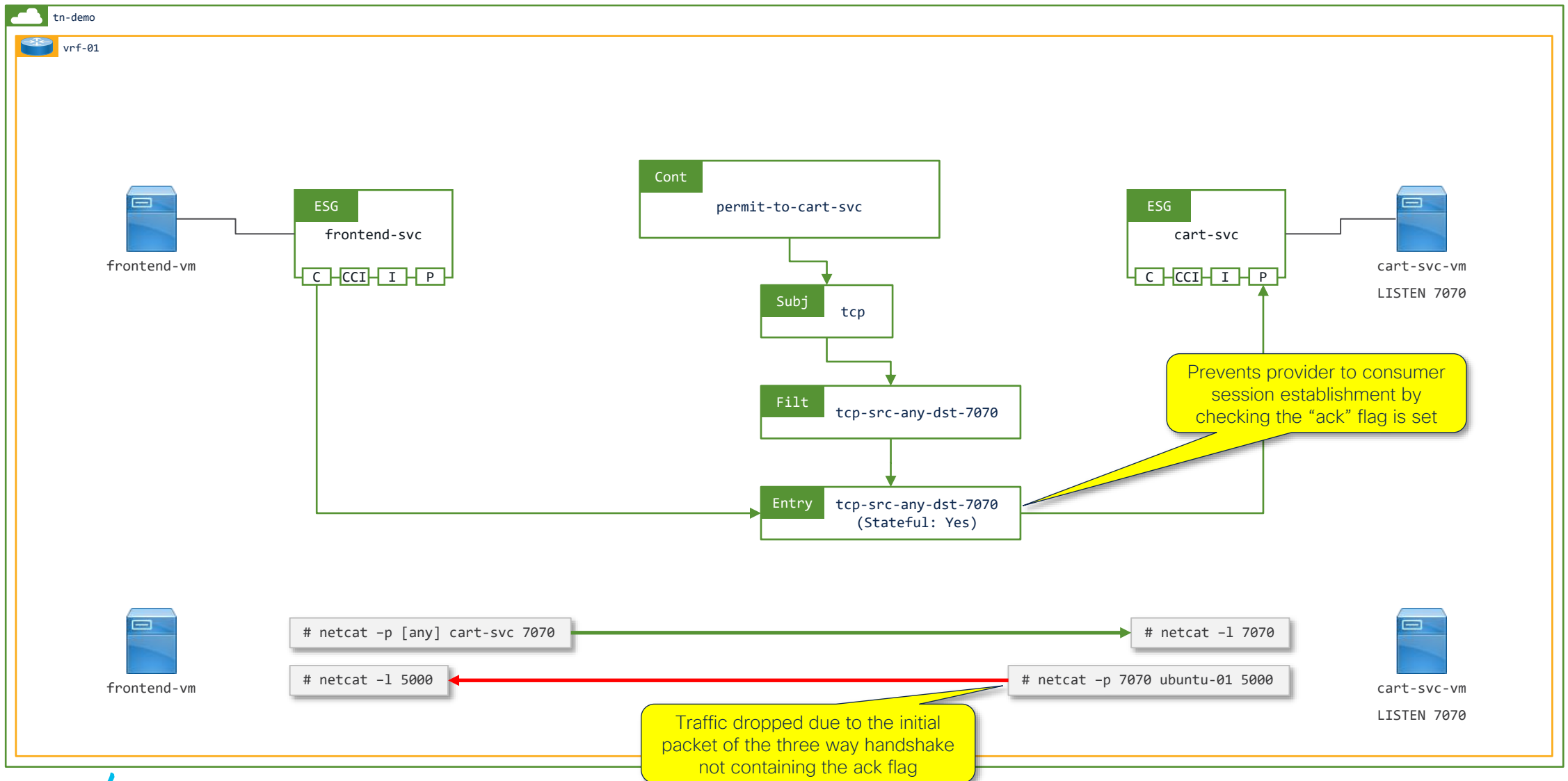
Name	Tenant	Action	Priority	Directives	State
tcp-src-any-dst-7070	demo	Permit	default level		formed

Option 1: Apply in both directions, reverse ports (default)



Option 2: Apply in both directions, reverse ports,
stateful

Option 2: Apply in both directions, reverse ports, stateful/ack check



Option 2: Apply in both directions, reverse ports, stateful/ack check

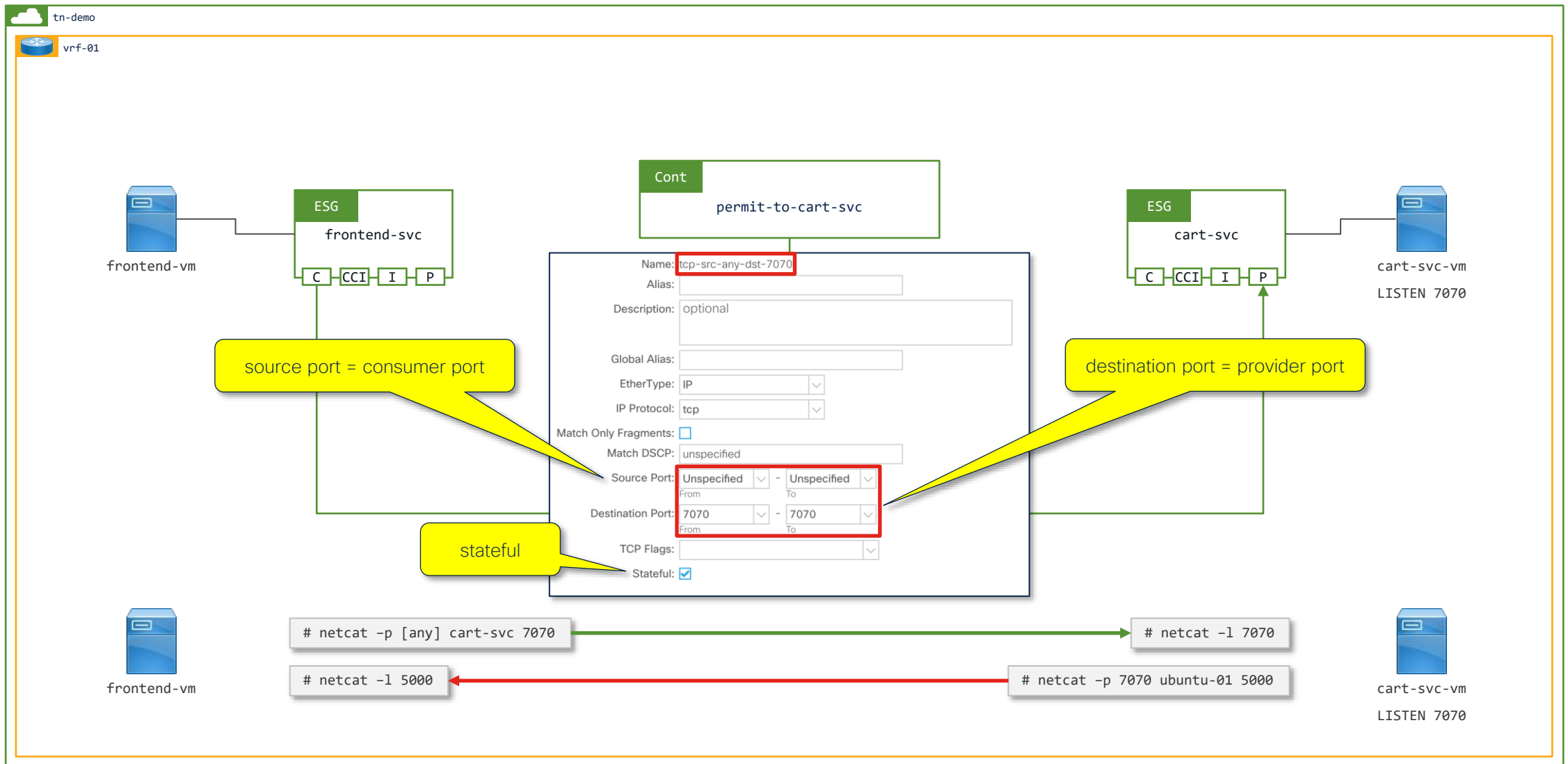
The screenshot displays the Cisco SD-WAN configuration interface for a contract named "permit-to-cart-svc". The contract is applied to the "frontend-svc" and "cart-svc" services. The configuration is shown in the "Policy" tab, with the "General" sub-tab selected. The "Contract Subject - tcp" is highlighted. The "Apply Both Directions" checkbox is checked, and the "Reverse Filter Ports" checkbox is also checked. The "Filters" table shows a filter named "tcp-src-any-dst-7070" with the action "Permit".

Annotations:

- Apply the rules in both directions
- Automatically reverse the filter ports
- Reference the required Filters

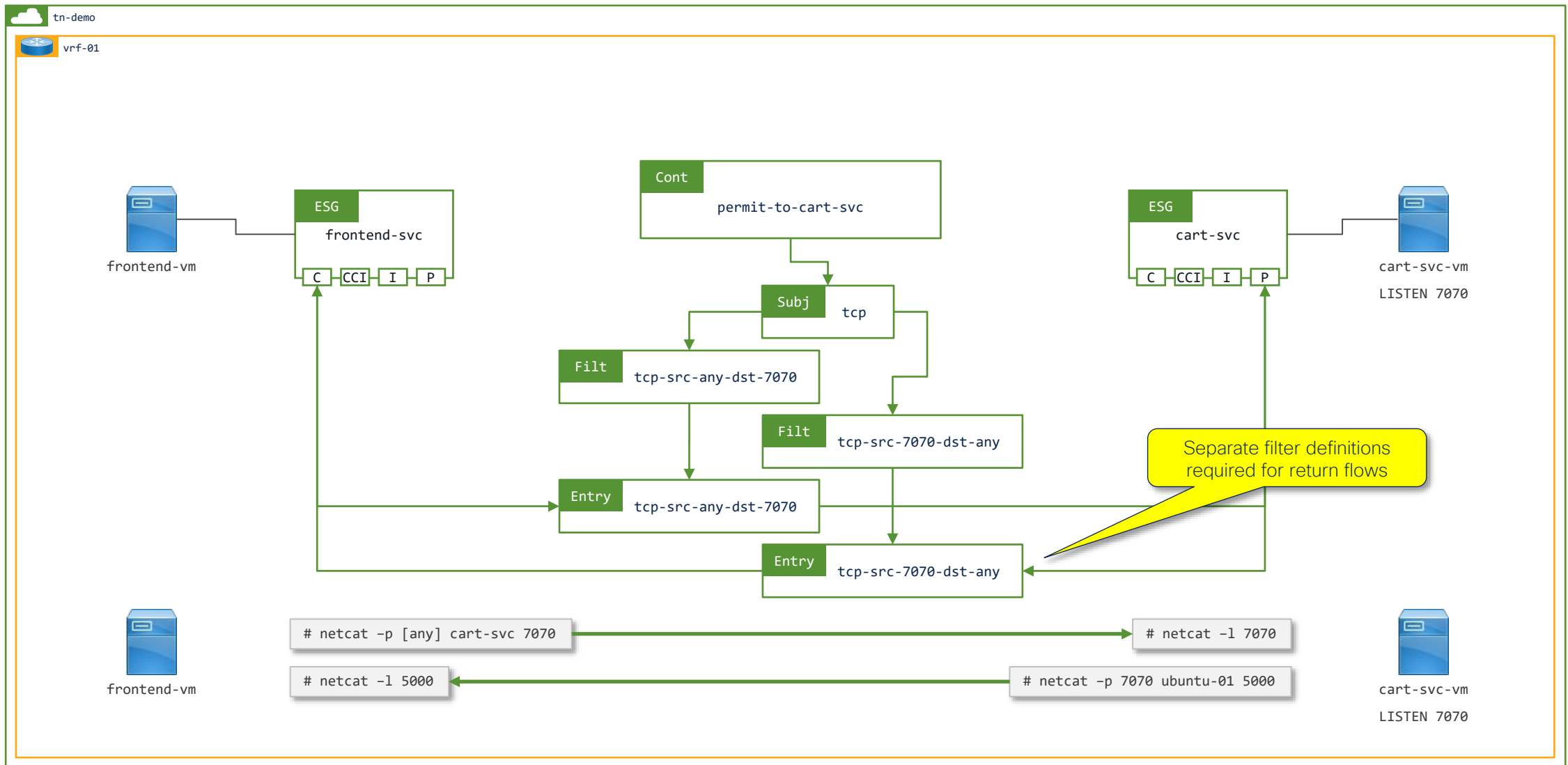
Name	Tenant	Action	Priority	Directives	State
tcp-src-any-dst-7070	demo	Permit	default level		formed

Option 2: Apply in both directions, reverse ports, stateful/ack check

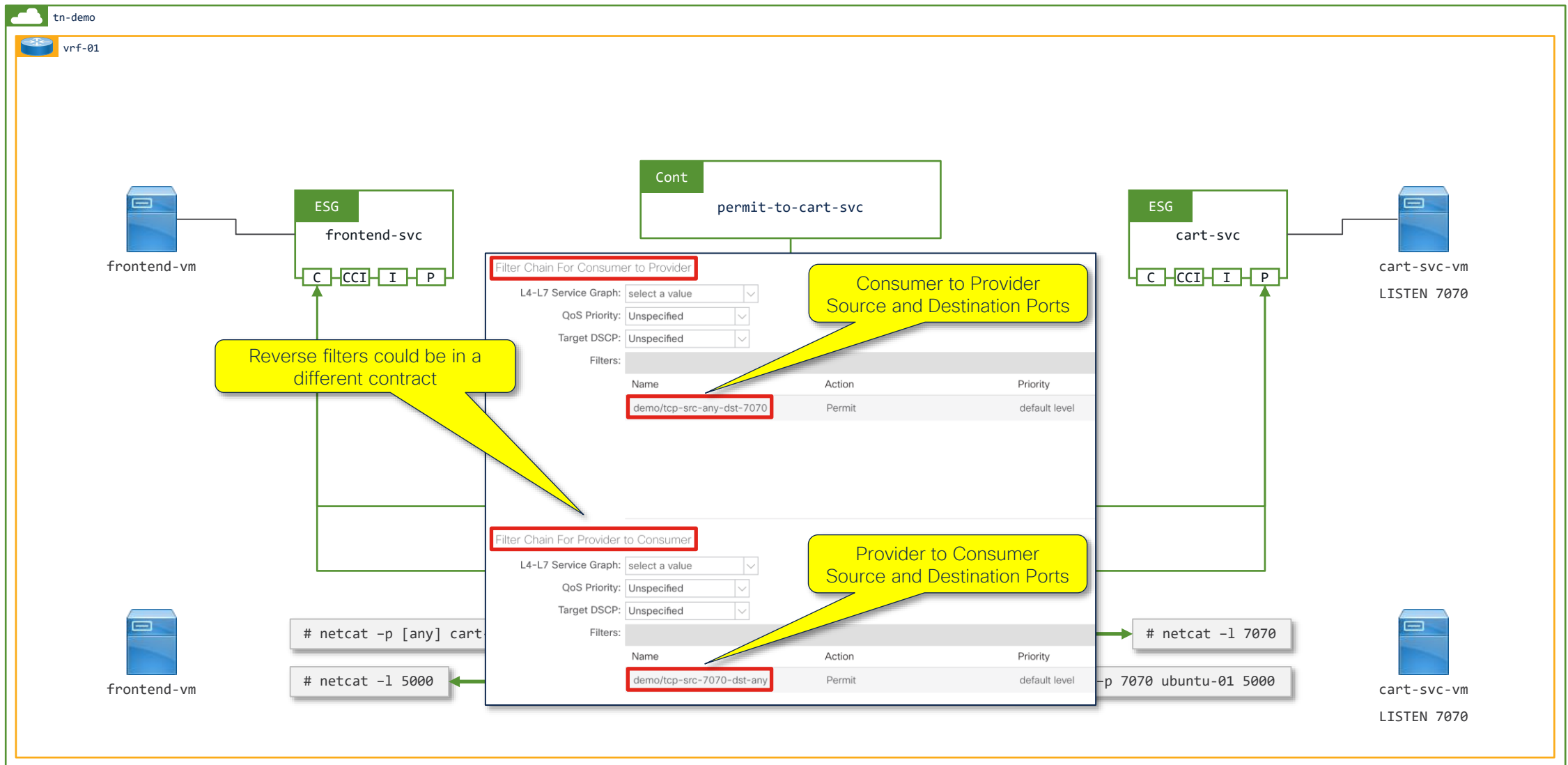


Option 3: Apply in single direction

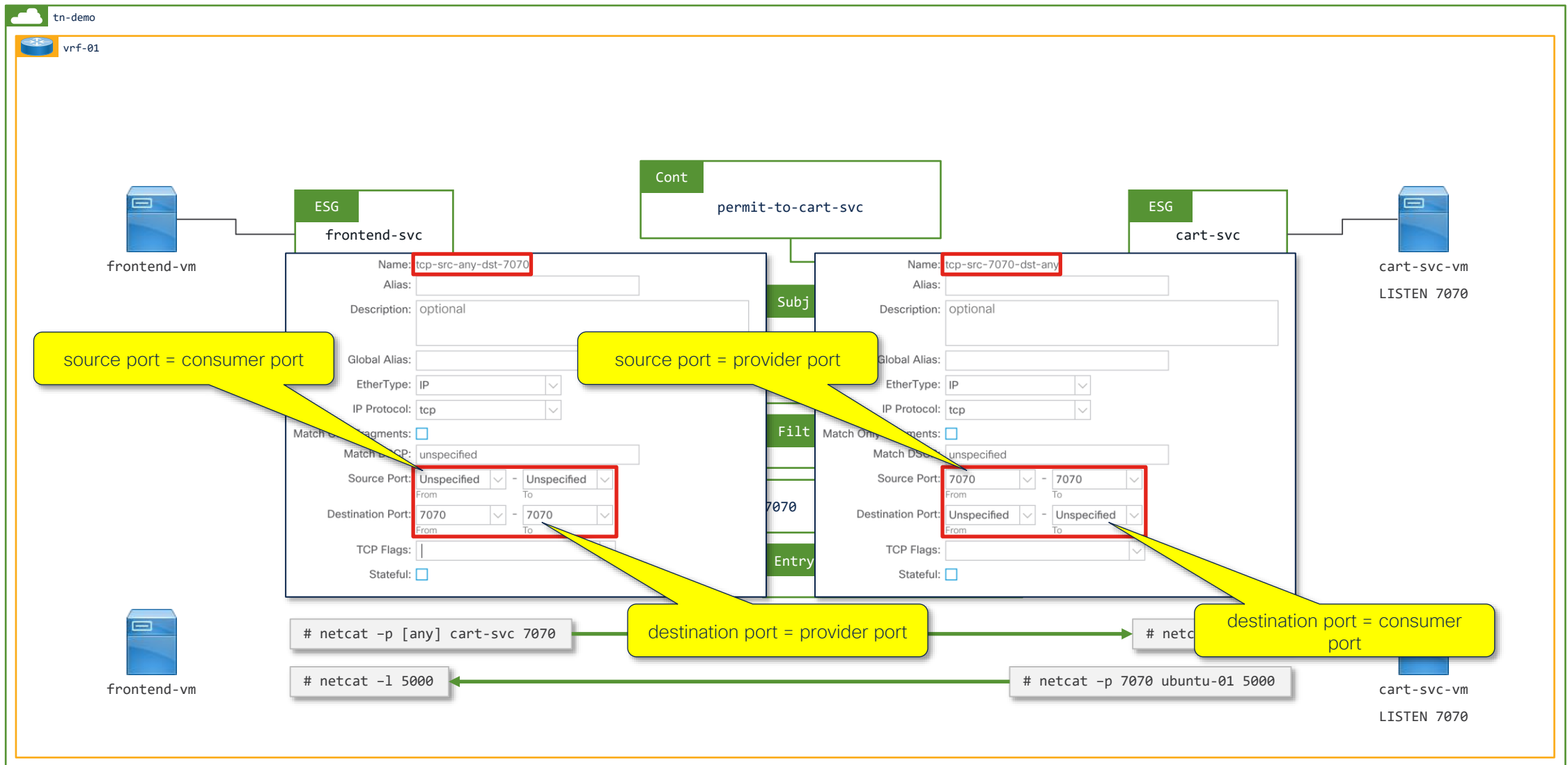
Option 3: Apply in single direction – requires you to specify the return ports in the same or different contract



Option 3: Apply in single direction – requires you to specify the return ports in the same or different contract

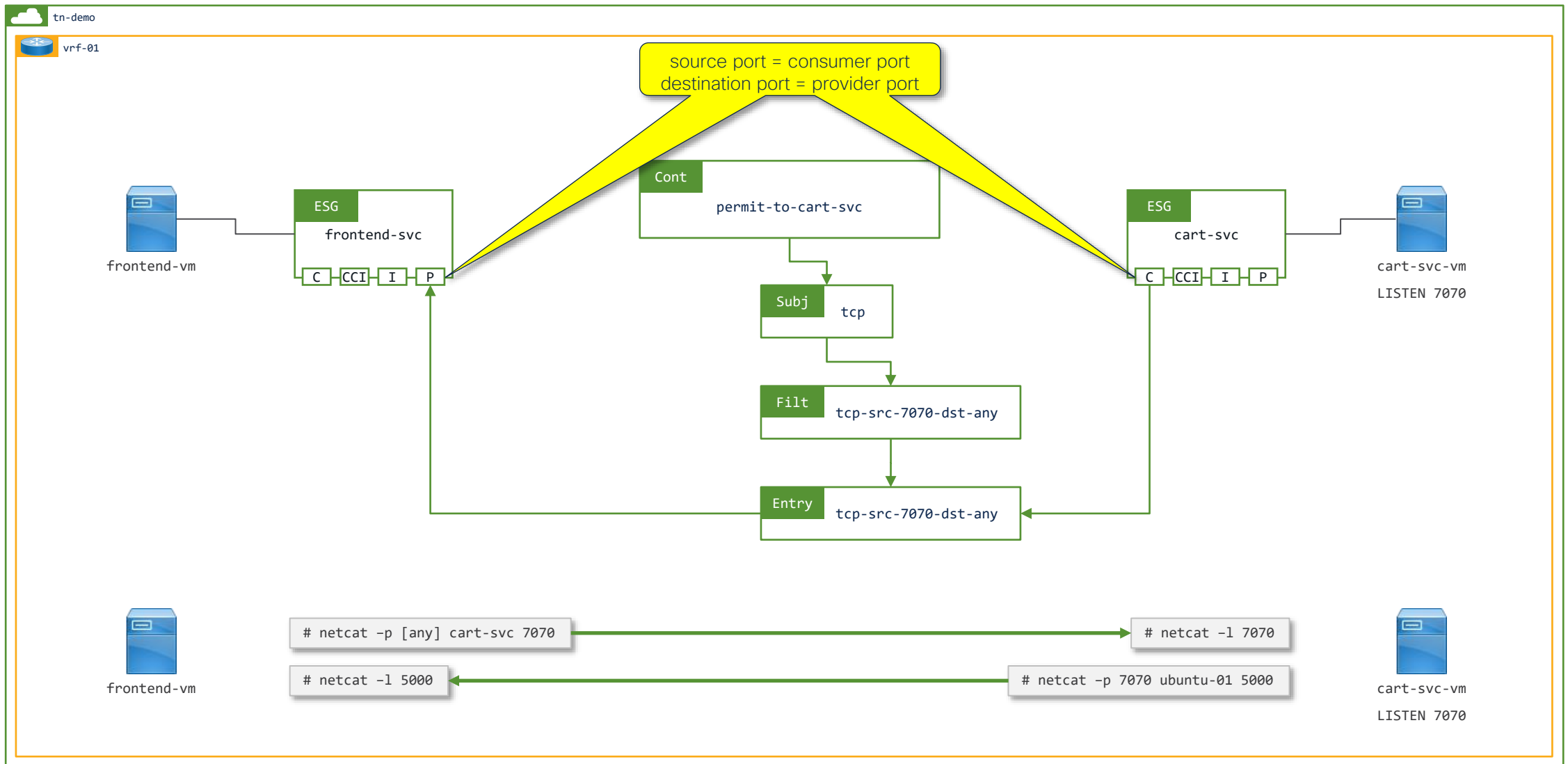


Option 3: Apply in single direction – requires you to specify the return ports in the same or different contract

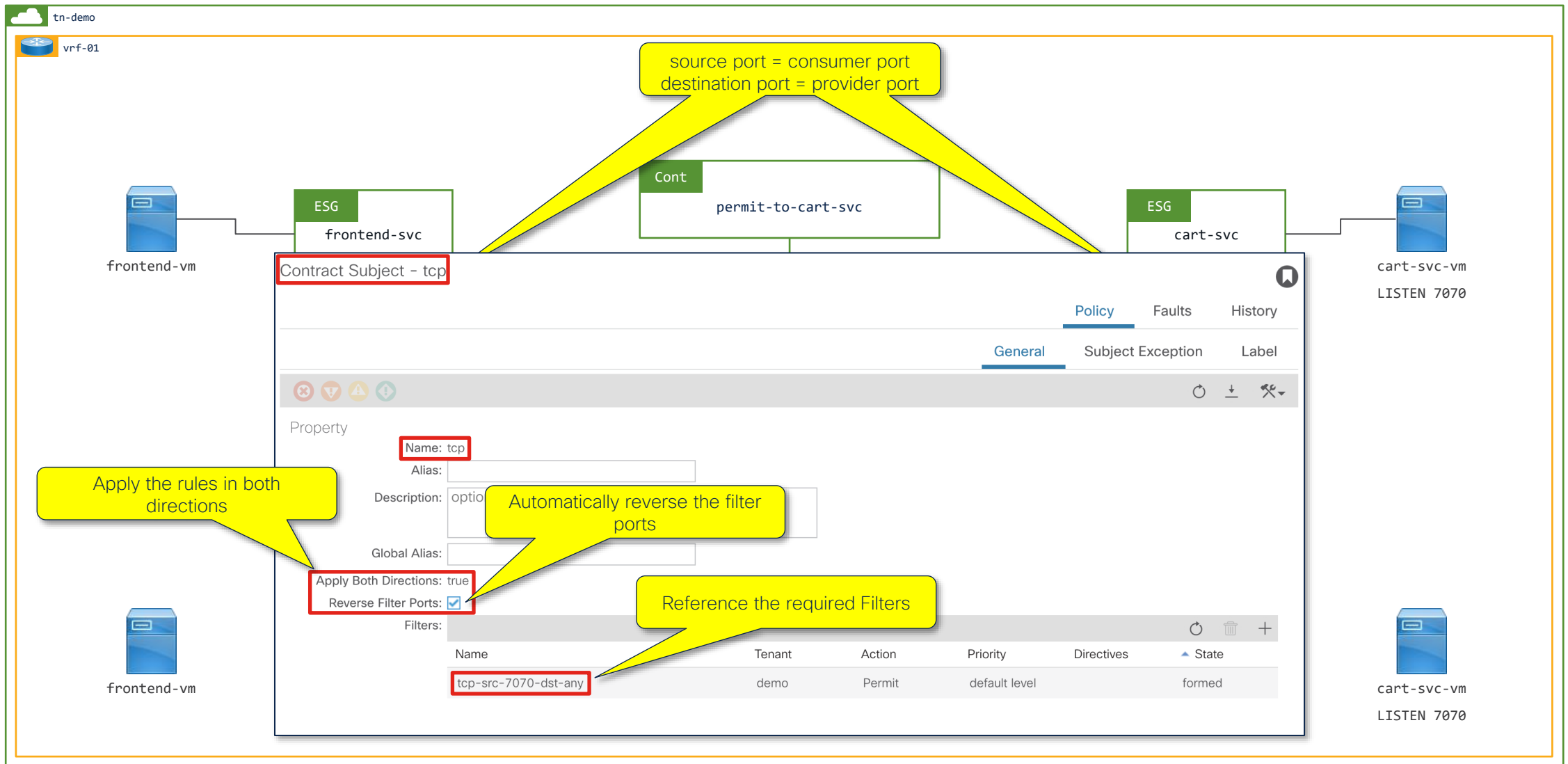


Option 4: Apply in both directions, reverse ports,
“flipped” – (this might hurt a little bit)

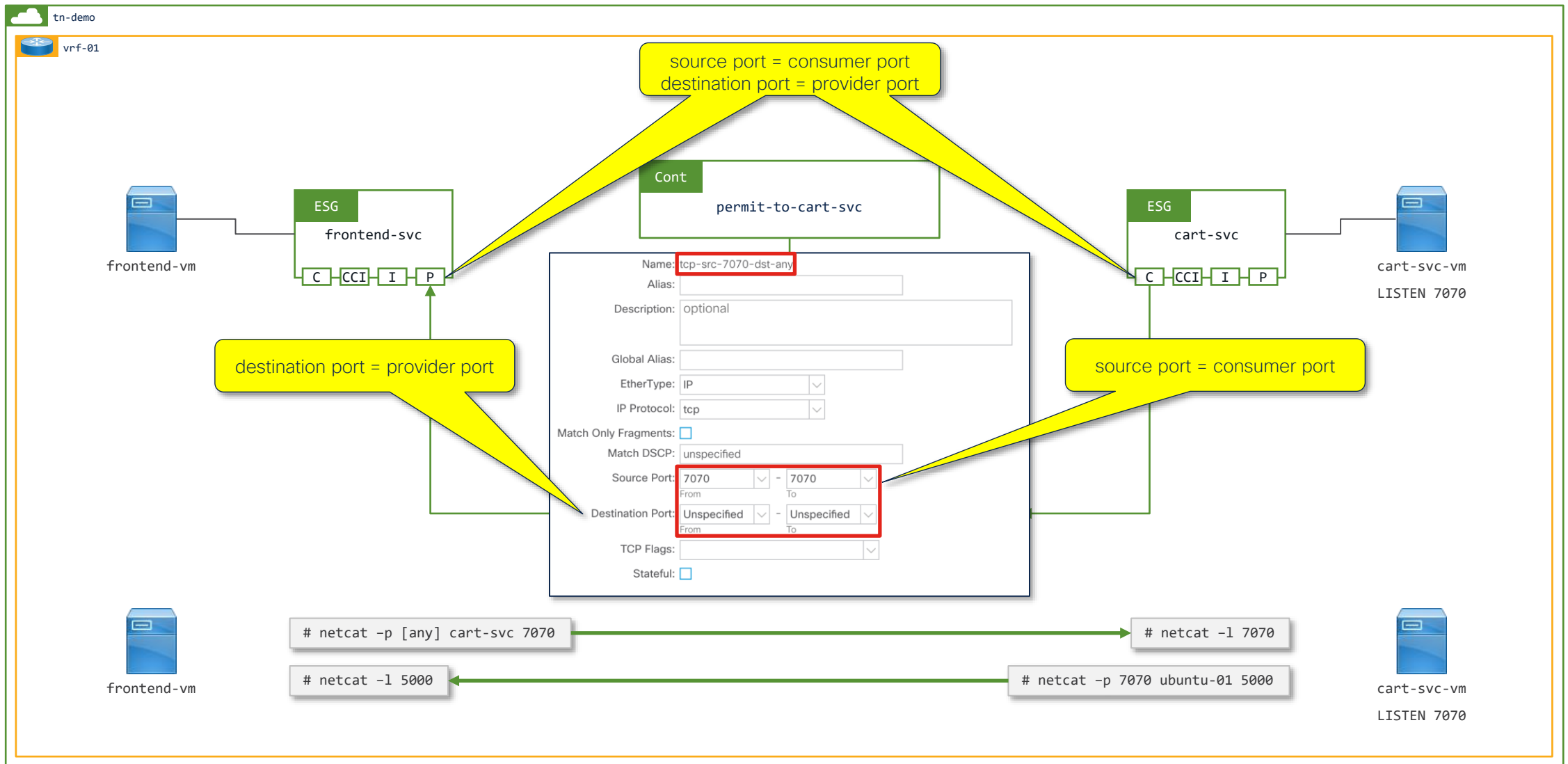
Option 4: Consumer and Provider Flipped



Option 4: Consumer and Provider Flipped

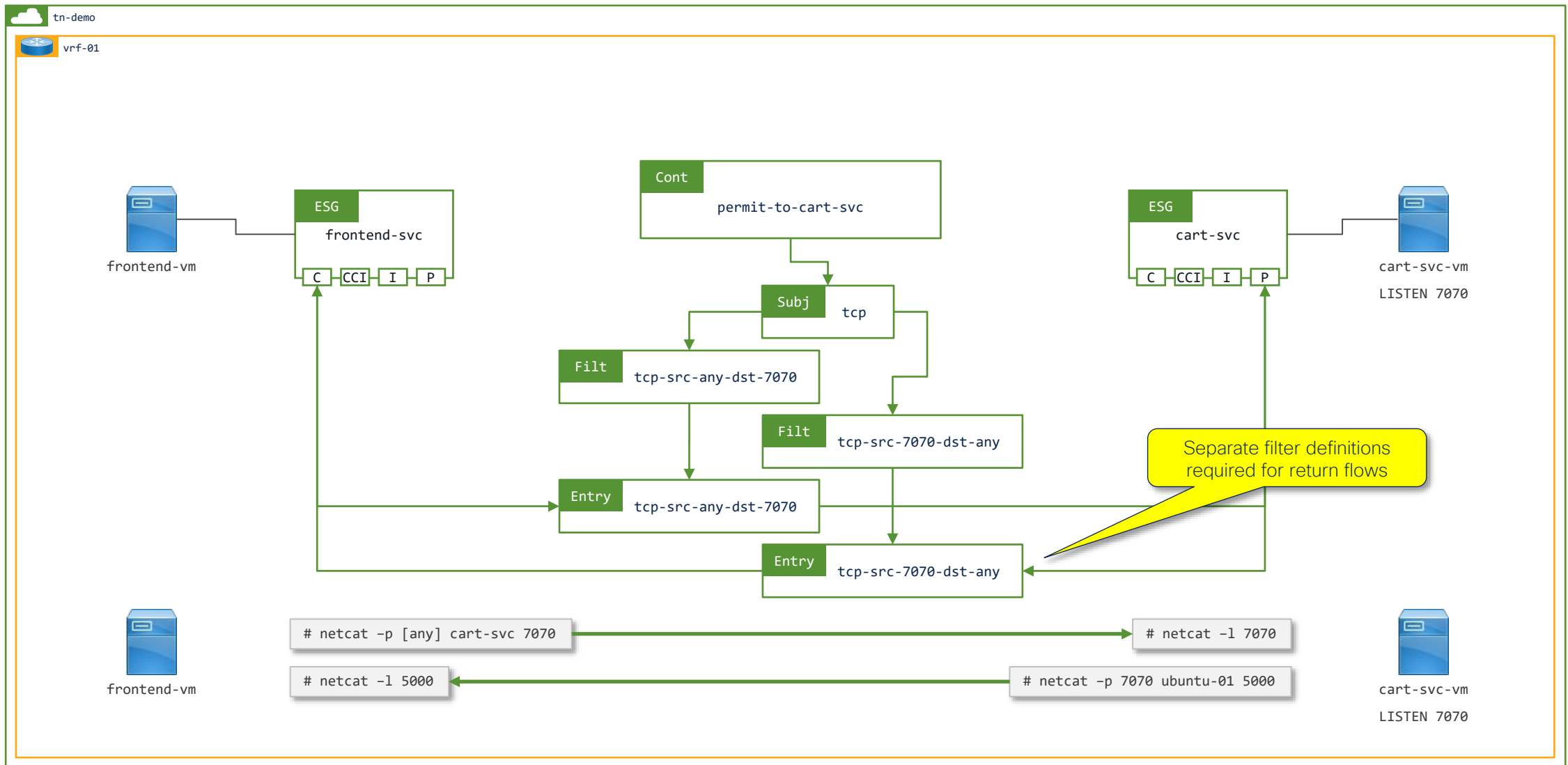


Option 4: Consumer and Provider Flipped

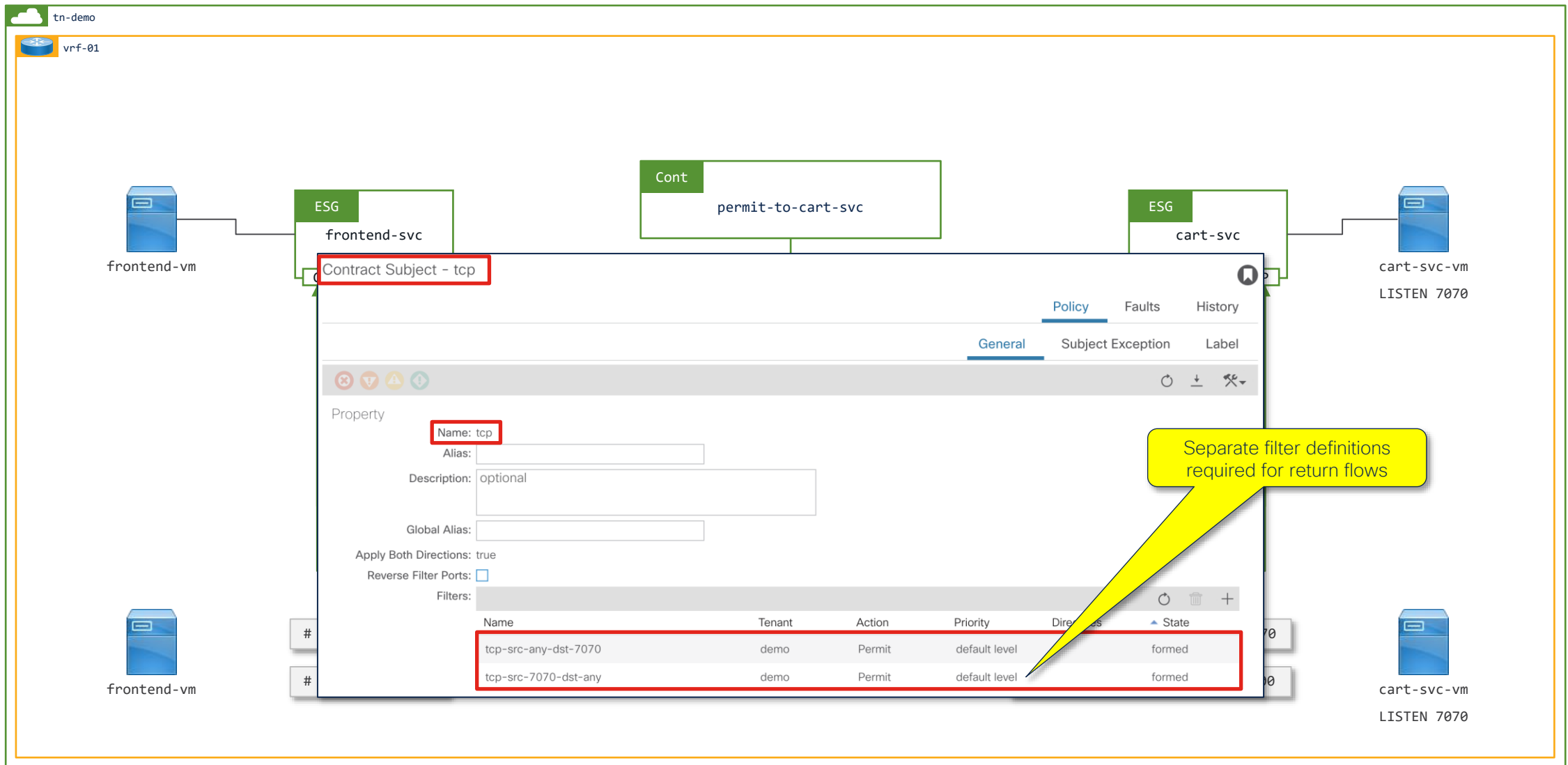


Option 5: Apply in both directions
(not recommended)

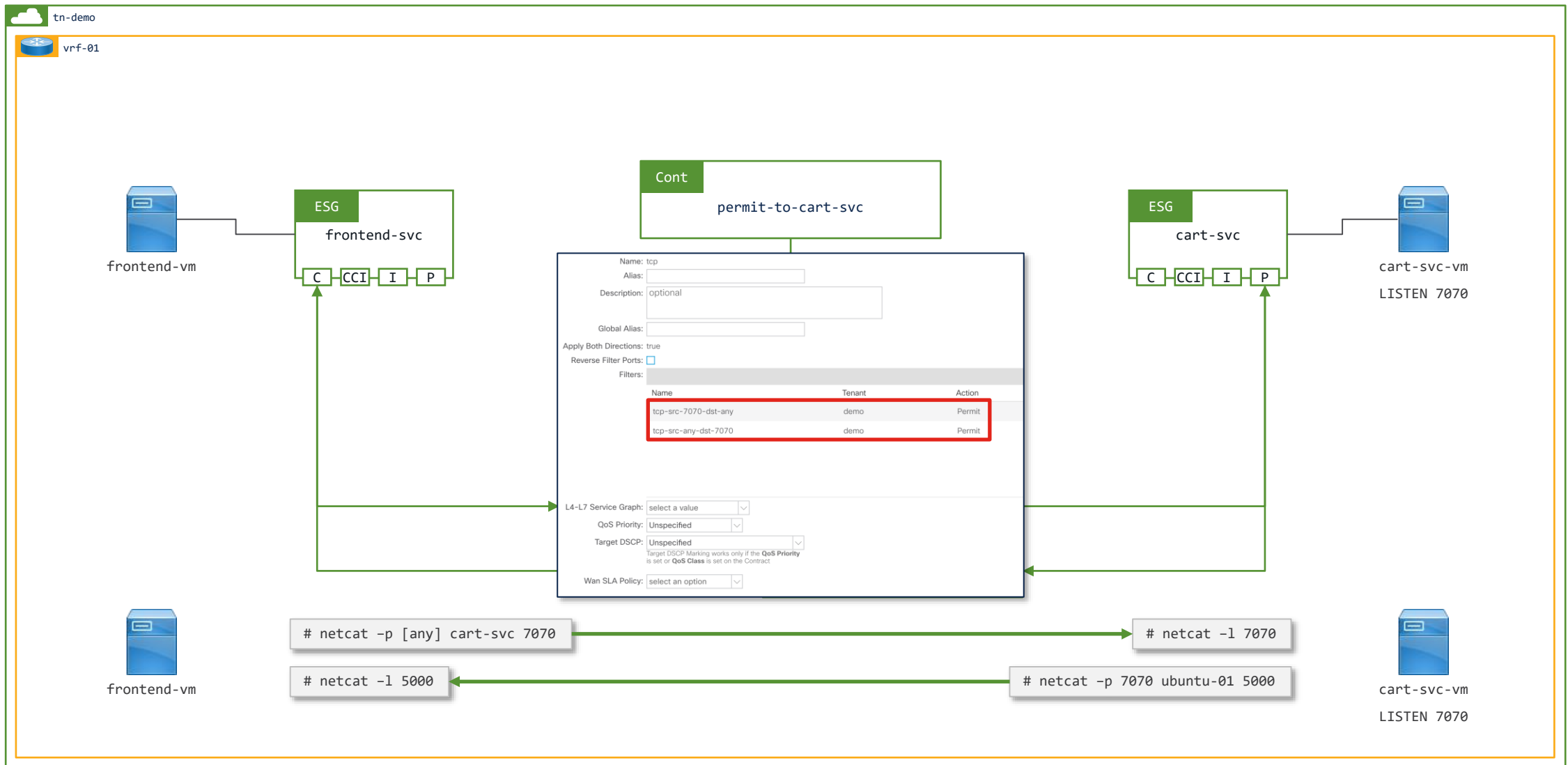
Option 5: Apply in both directions (no reverse ports) – requires you to specify the return ports



Option 5: Apply in both directions (no reverse ports) – requires you to specify the return ports

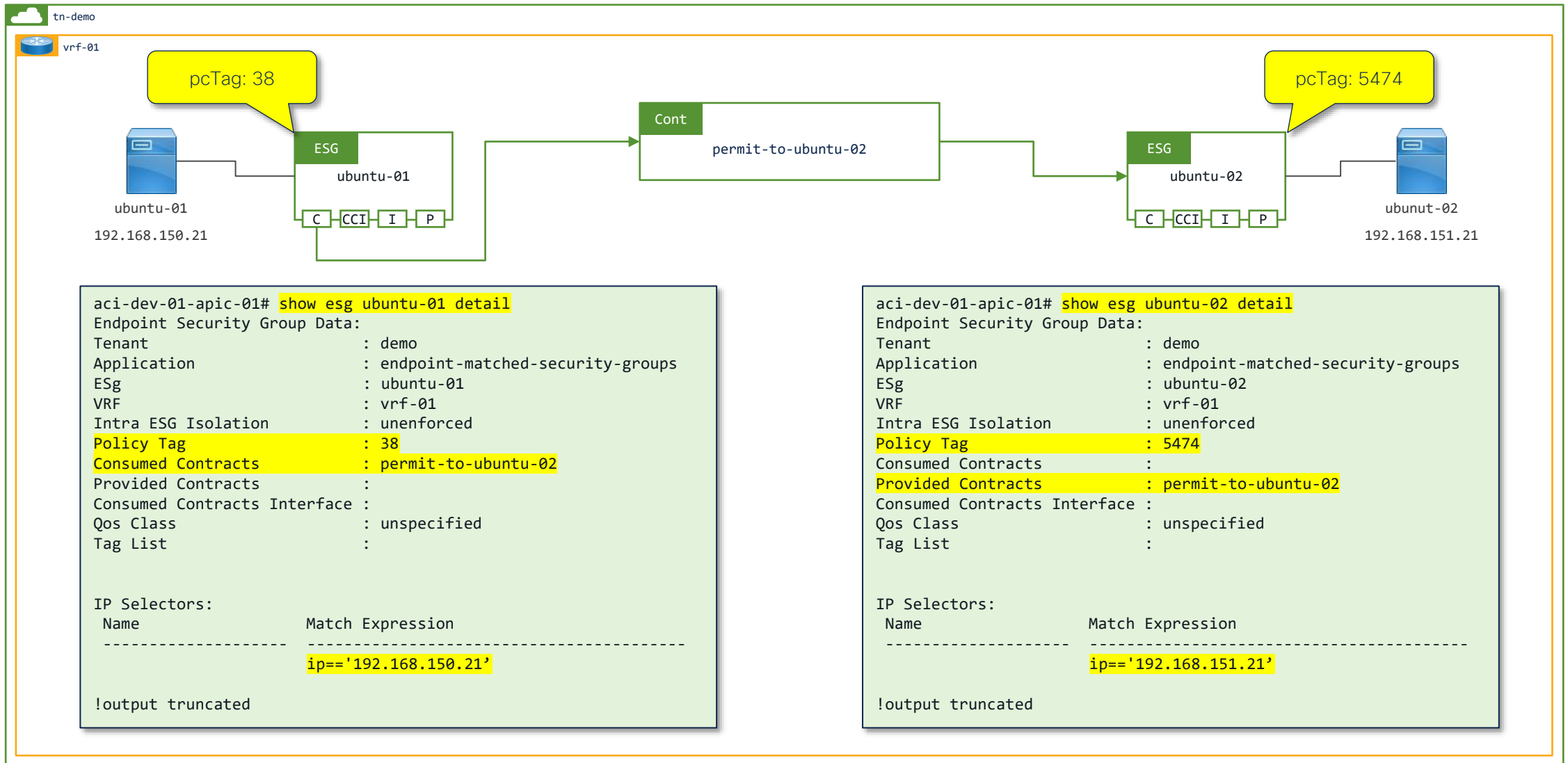


Option 5: Apply in both directions (no reverse ports) – requires you to specify the return ports

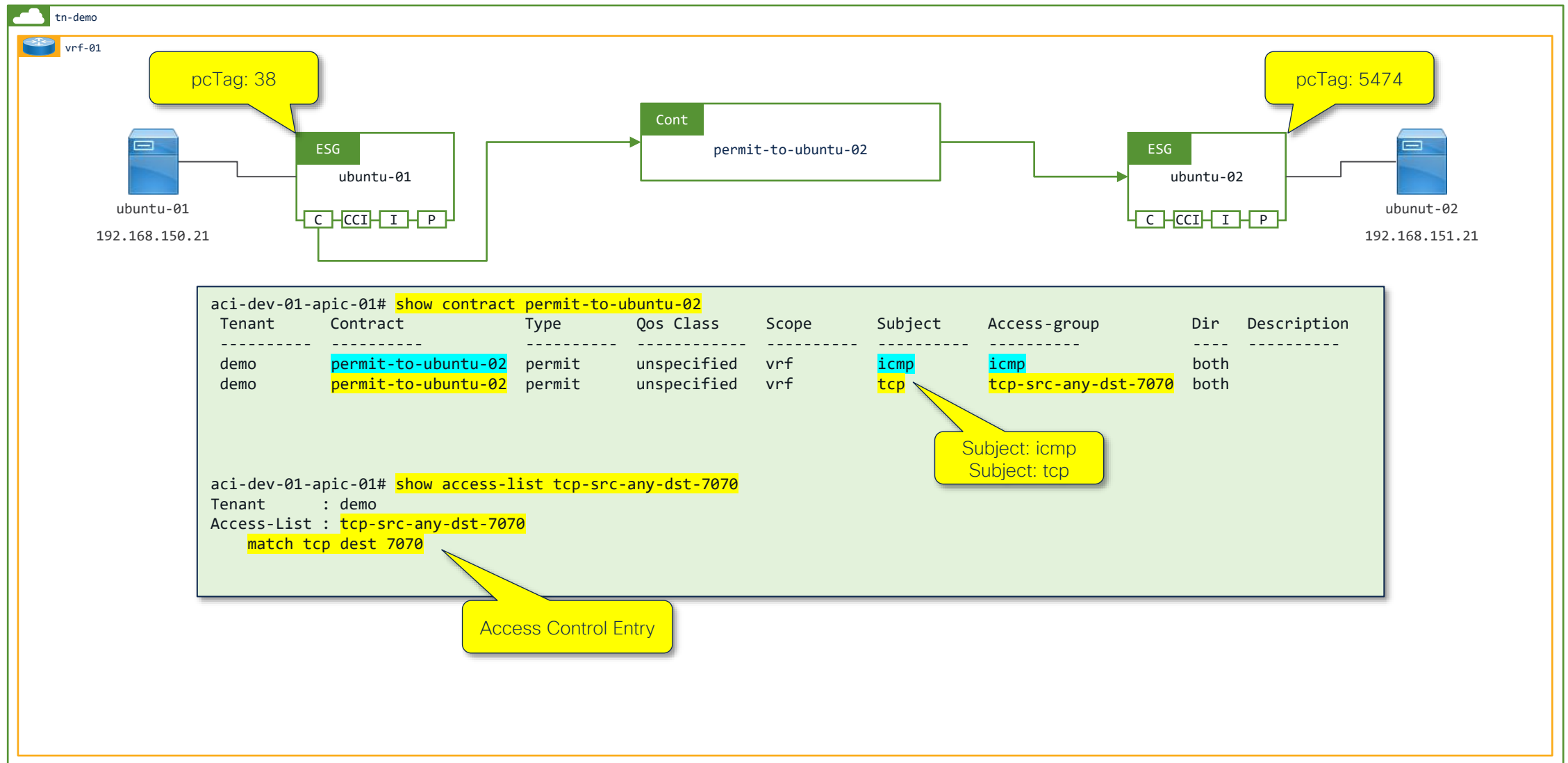


Verifying contracts...

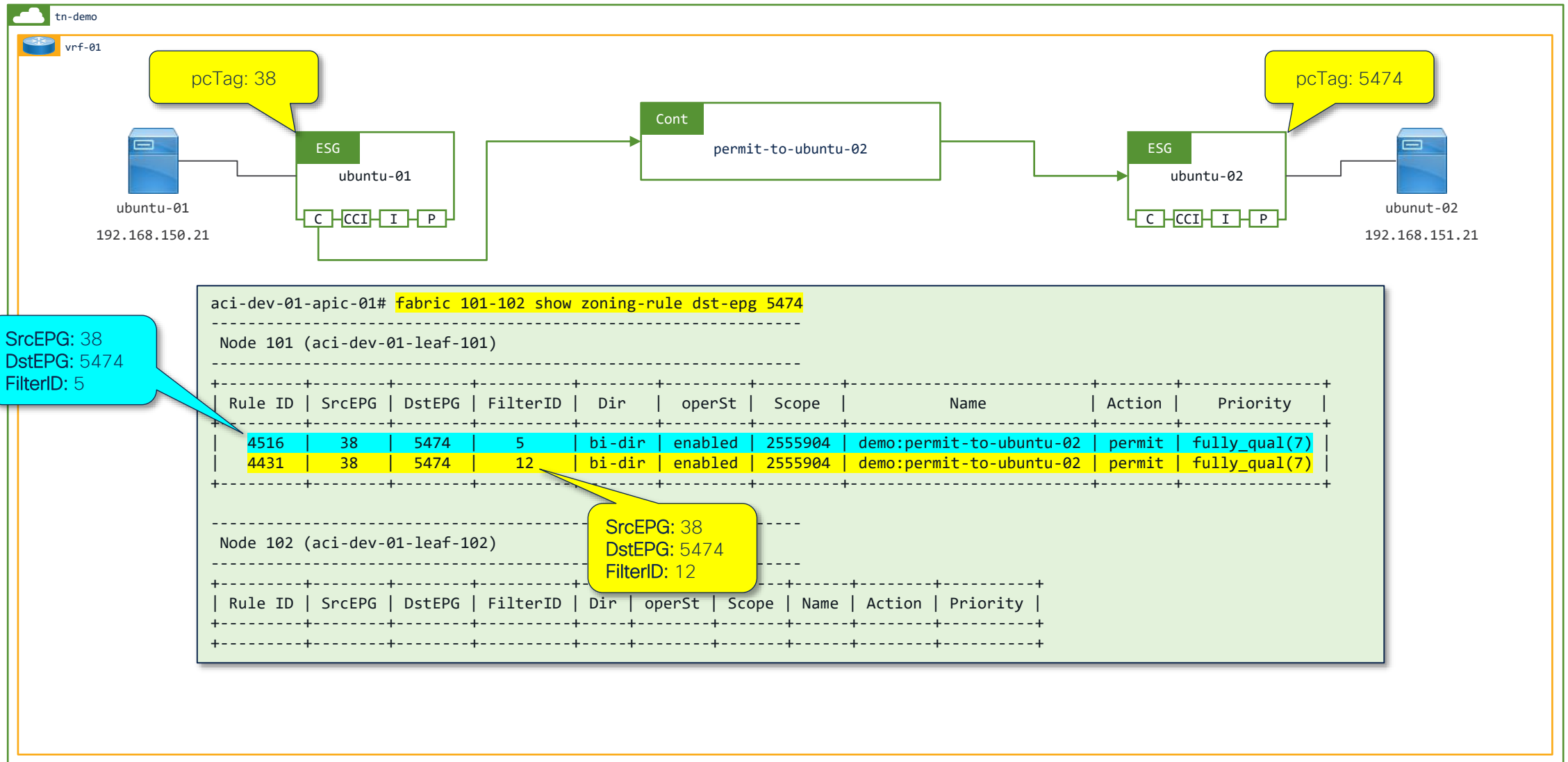
Verifying Contract Operation



Verifying Contract Operation



Verifying Contract Operation



Verifying Contract Operation



```
aci-dev-01-apic-01# fabric 101-102 show zoning-filter filter 12
```

```
Node 101 (aci-dev-01-leaf-101)
```

FilterId	Name	EtherT	ArpOpc	Prot	ApplyToFrag	Stateful	SFromPort	SToPort	DFromPort	DToPort	Prio	Icmpv4T	Icmpv6T	TcpRules
12	12_0	ip	unspecified	tcp	no	no	unspecified	unspecified	7070	7070	dport	unspecified	unspecified	

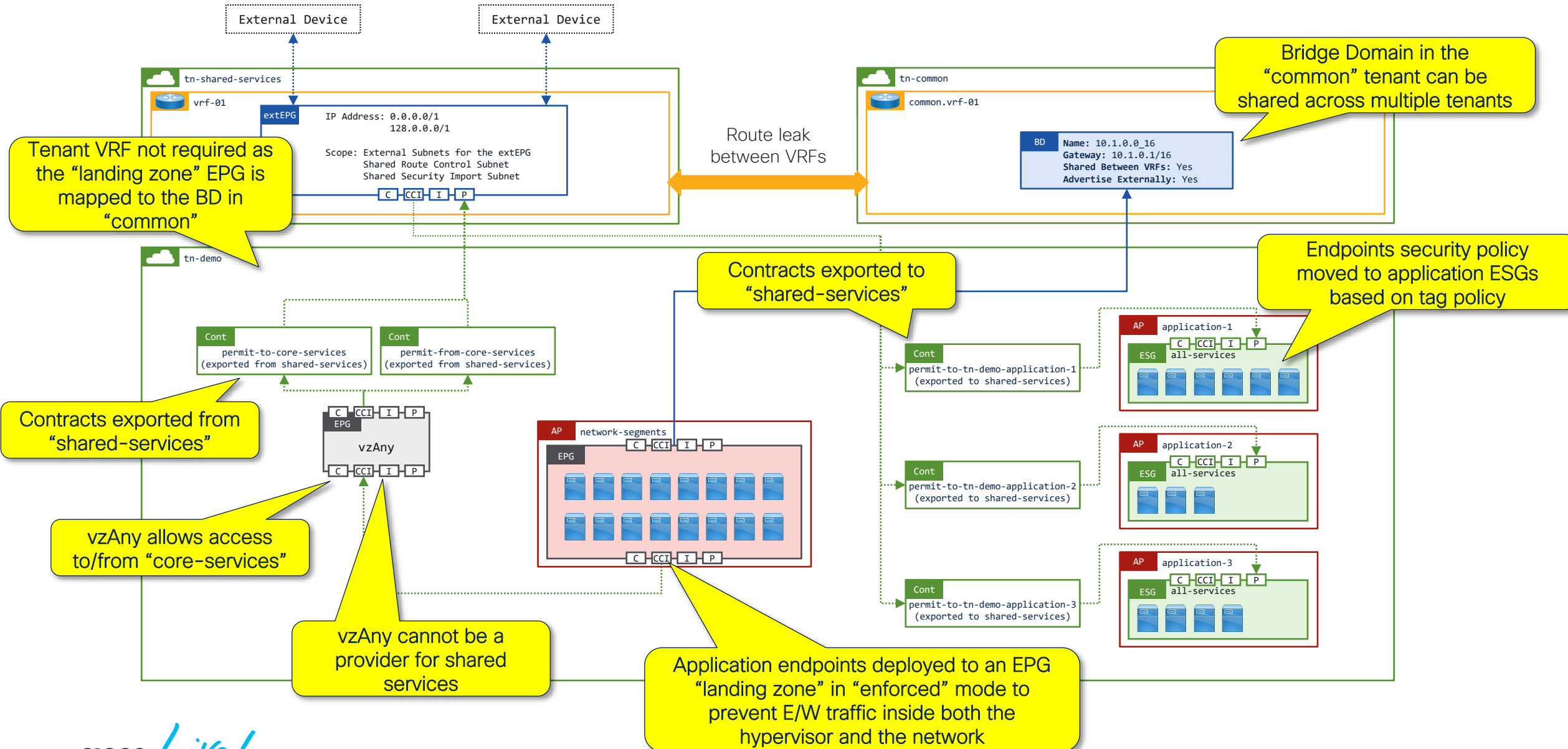
```
Node 102 (aci-dev-01-leaf-102)
```

FilterId	Name	EtherT	ArpOpc	Prot	ApplyToFrag	Stateful	SFromPort	SToPort	DFromPort	DToPort	Prio	Icmpv4T	Icmpv6T	TcpRules
12	12_0	ip	unspecified	tcp	no	no	unspecified	unspecified	7070	7070	dport	unspecified	unspecified	

Blueprints

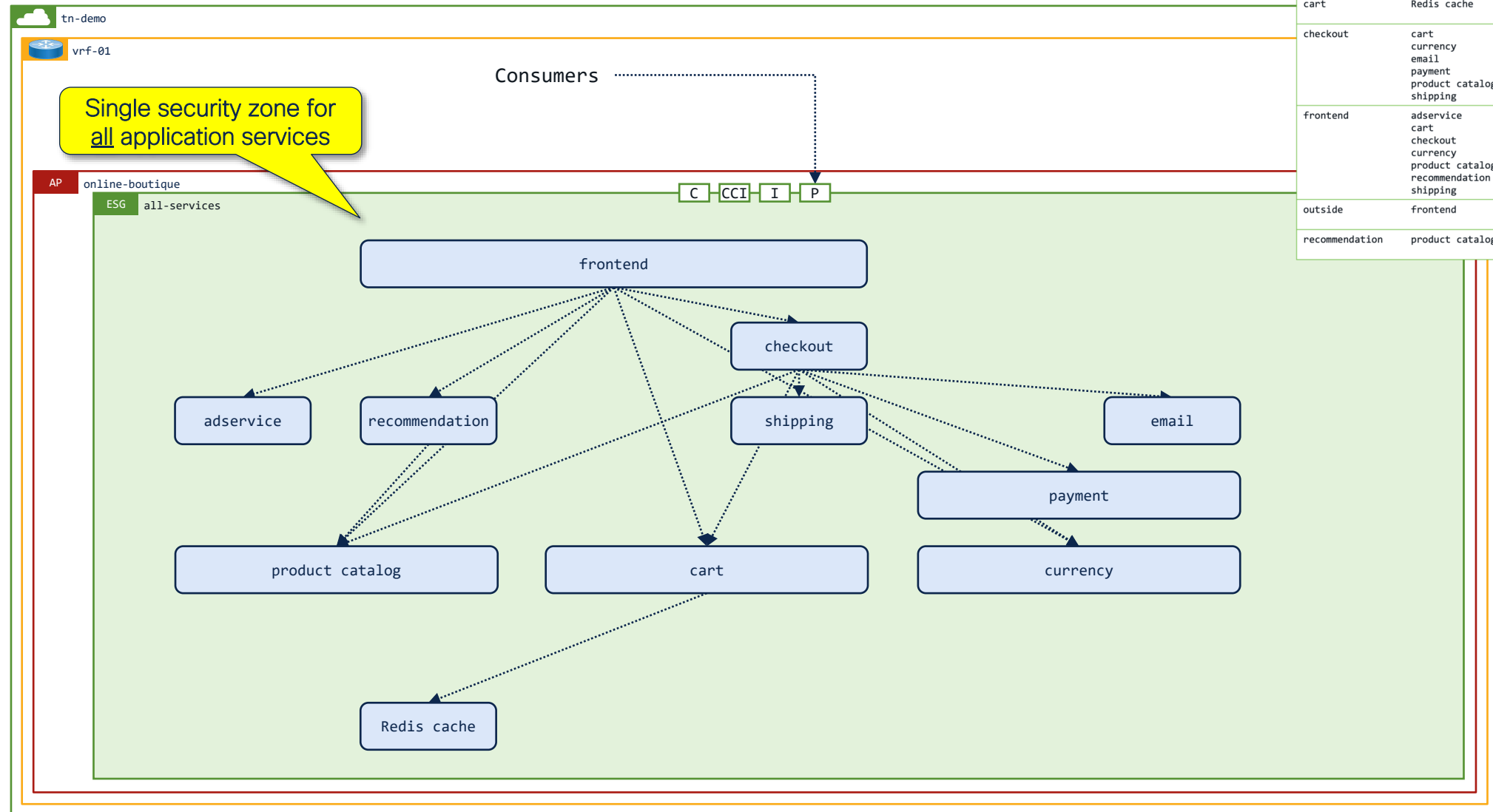


Example Internal Private Cloud Design – shared subnet(s)



Application tiers across subnets

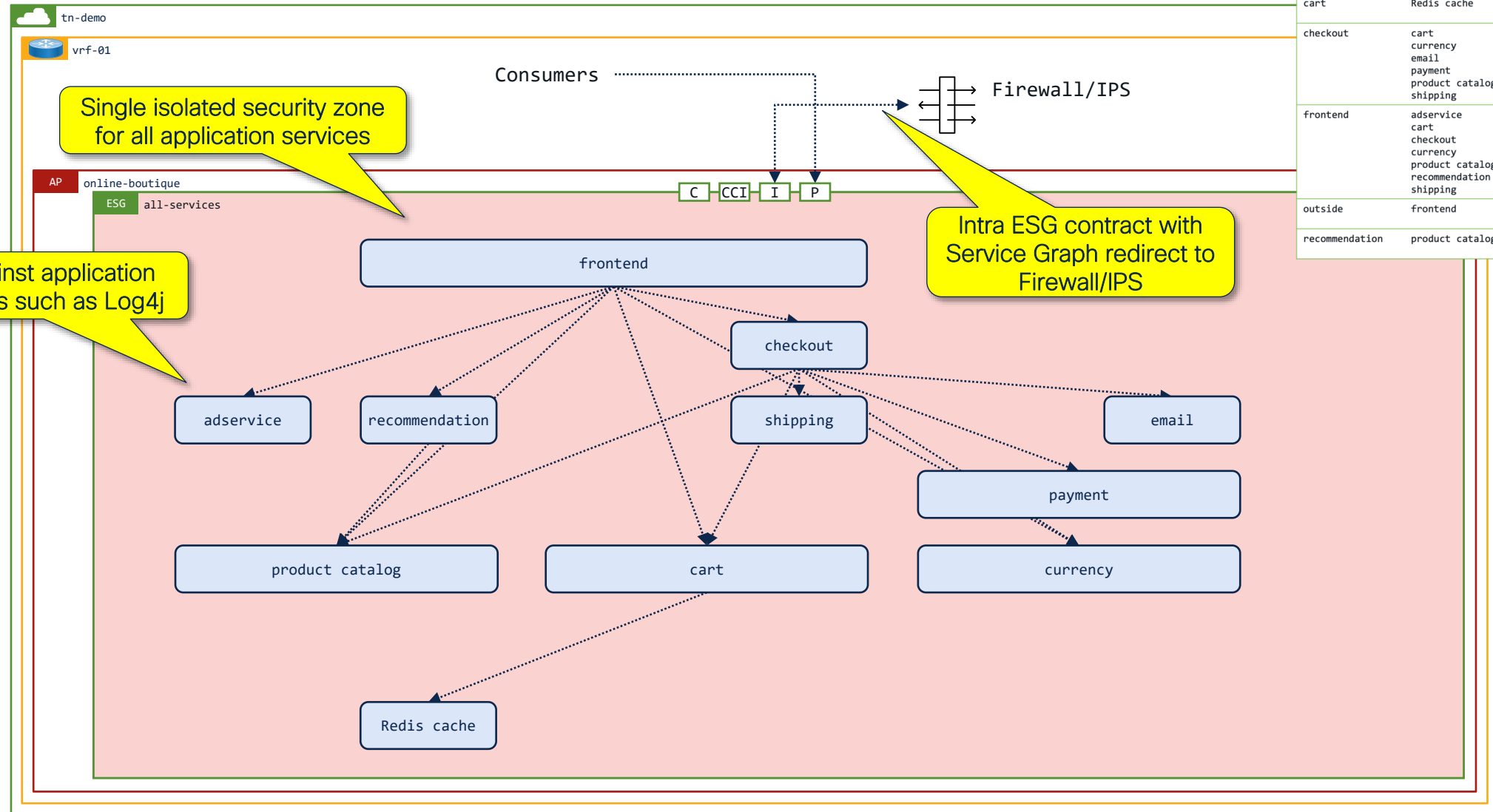
Application Centric Blueprint #1 – ESG “wrapper” for all services



Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP 3550
	recommendation	TCP 8080
	shipping	TCP 50051
outside	frontend	TCP 80/8080
recommendation	product catalog	TCP 3550

Application tiers across subnets

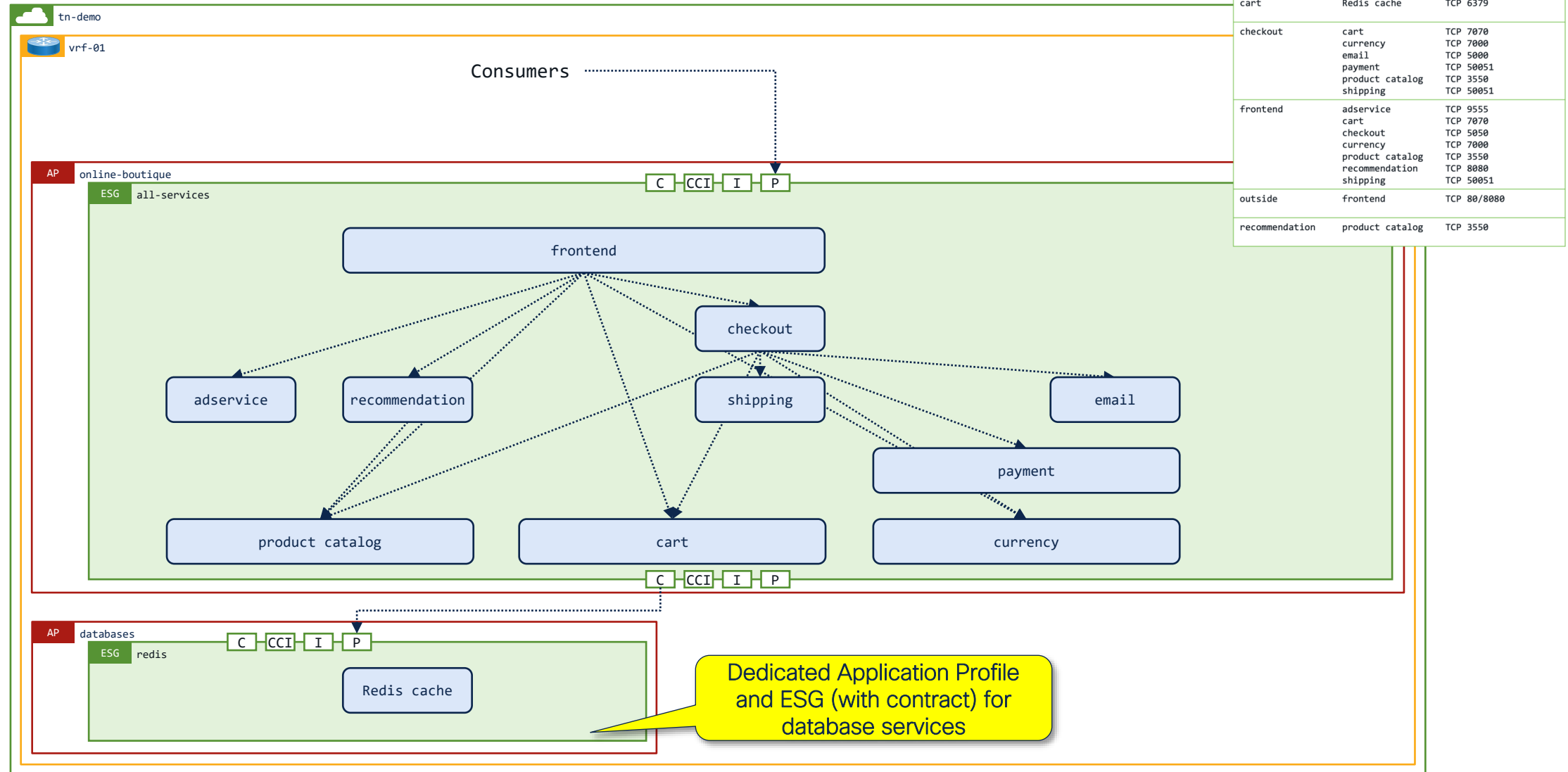
Application Centric Blueprint #2 – Intra ESG Isolation



Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP 3550
	recommendation	TCP 8080
	shipping	TCP 50051
outside	frontend	TCP 80/8080
recommendation	product catalog	TCP 3550

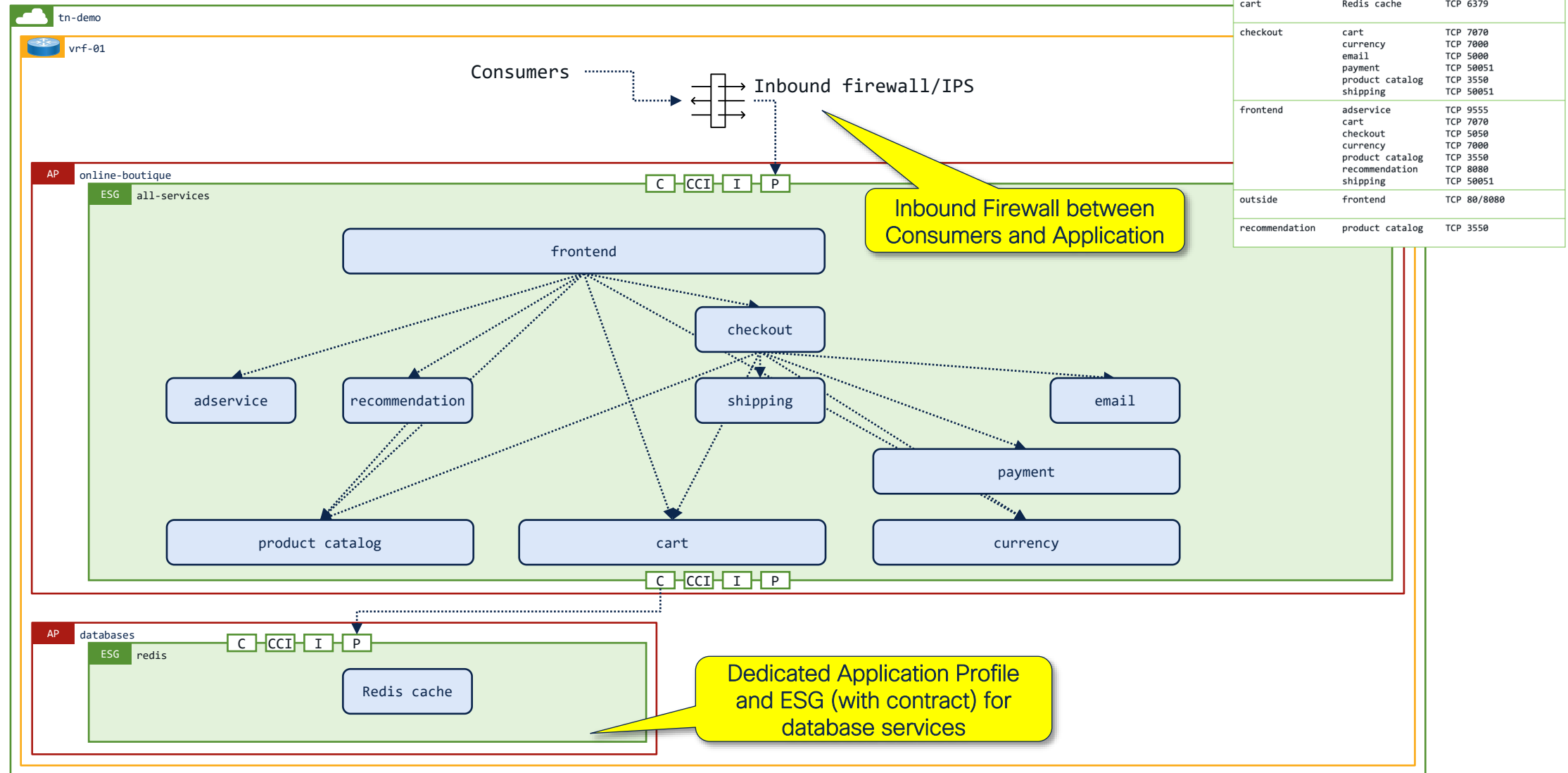
Application tiers across subnets

Application Centric Blueprint #3 – Dedicated AP/ESG for backend database



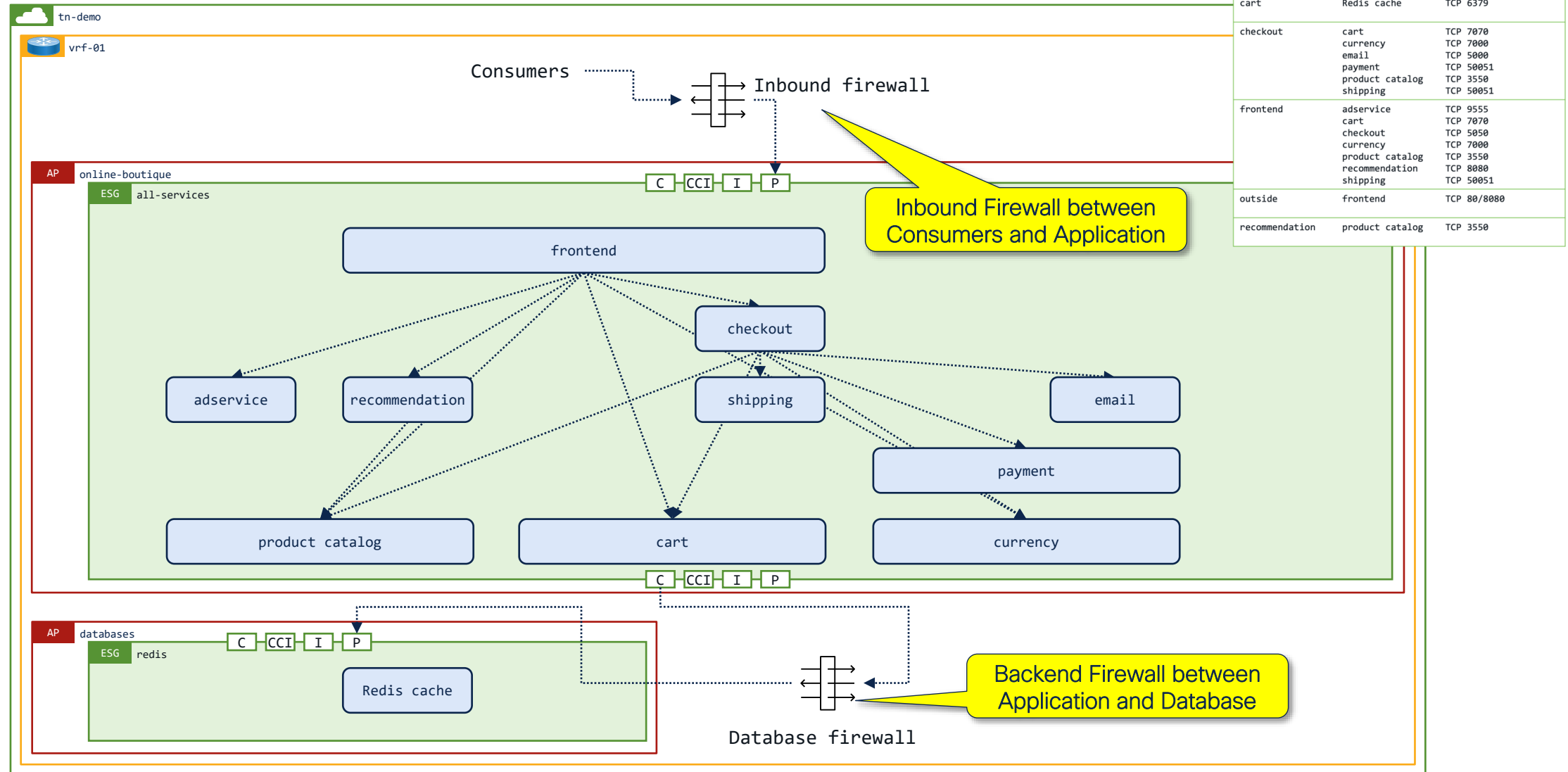
Application tiers across subnets

Application Centric Blueprint #4 – Inbound firewall/IPS + backend contract



Application tiers across subnets

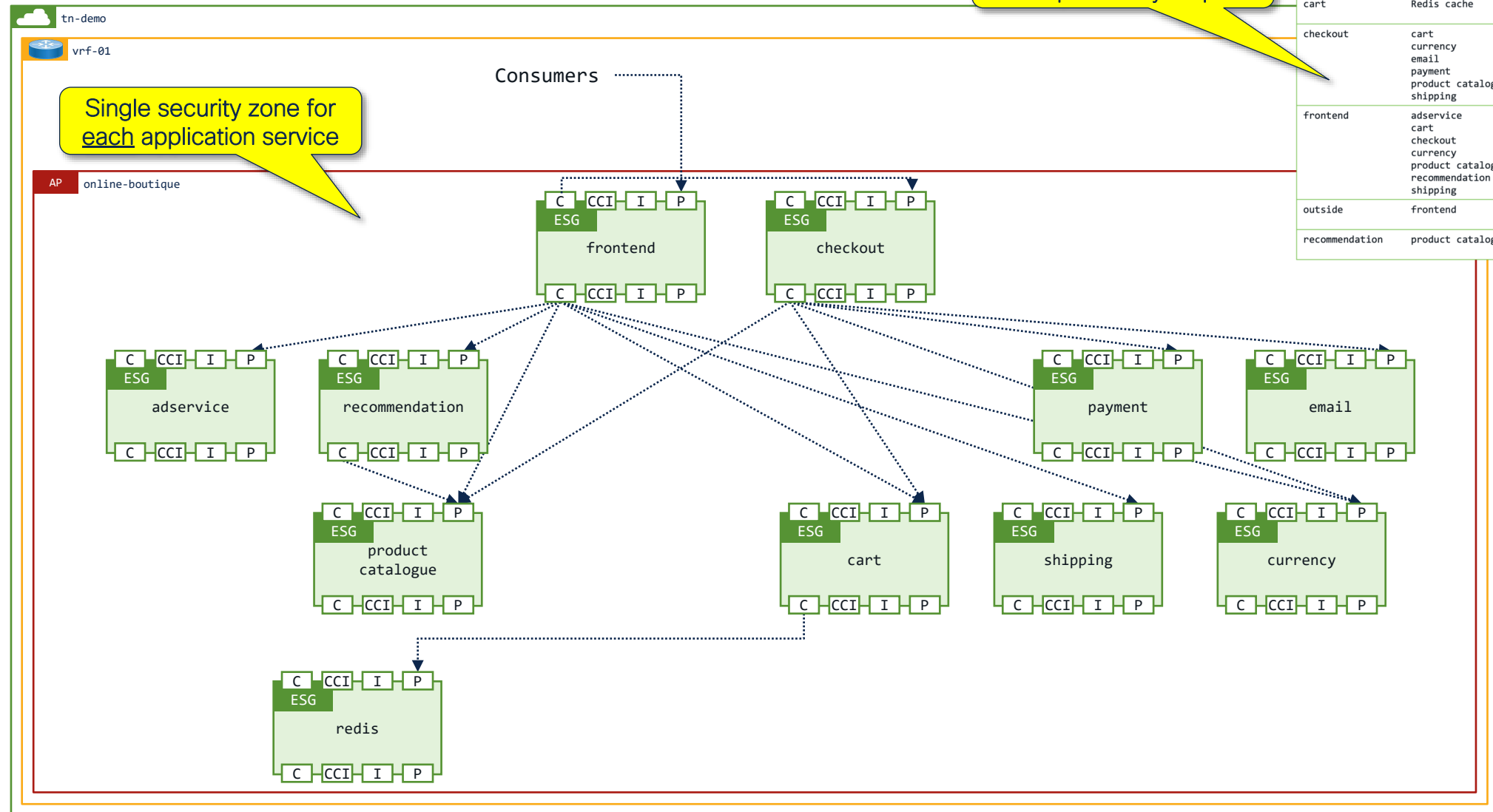
Application Centric Blueprint #5 – Inbound firewall/IPS + backend firewall/IPS



Application tiers across subnets

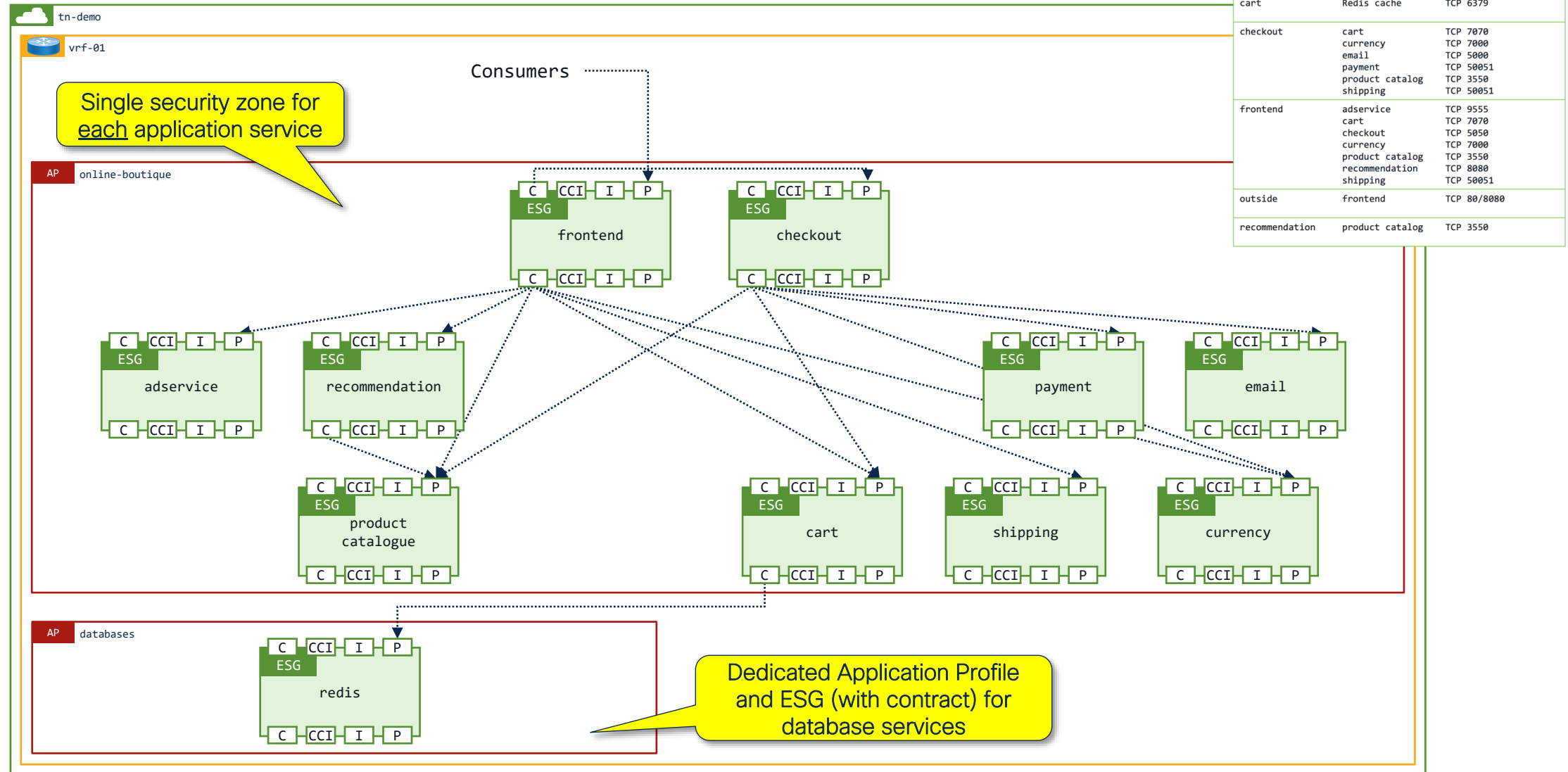
Application Centric Blueprint #6 – ESG per application tier

Requires application dependency map



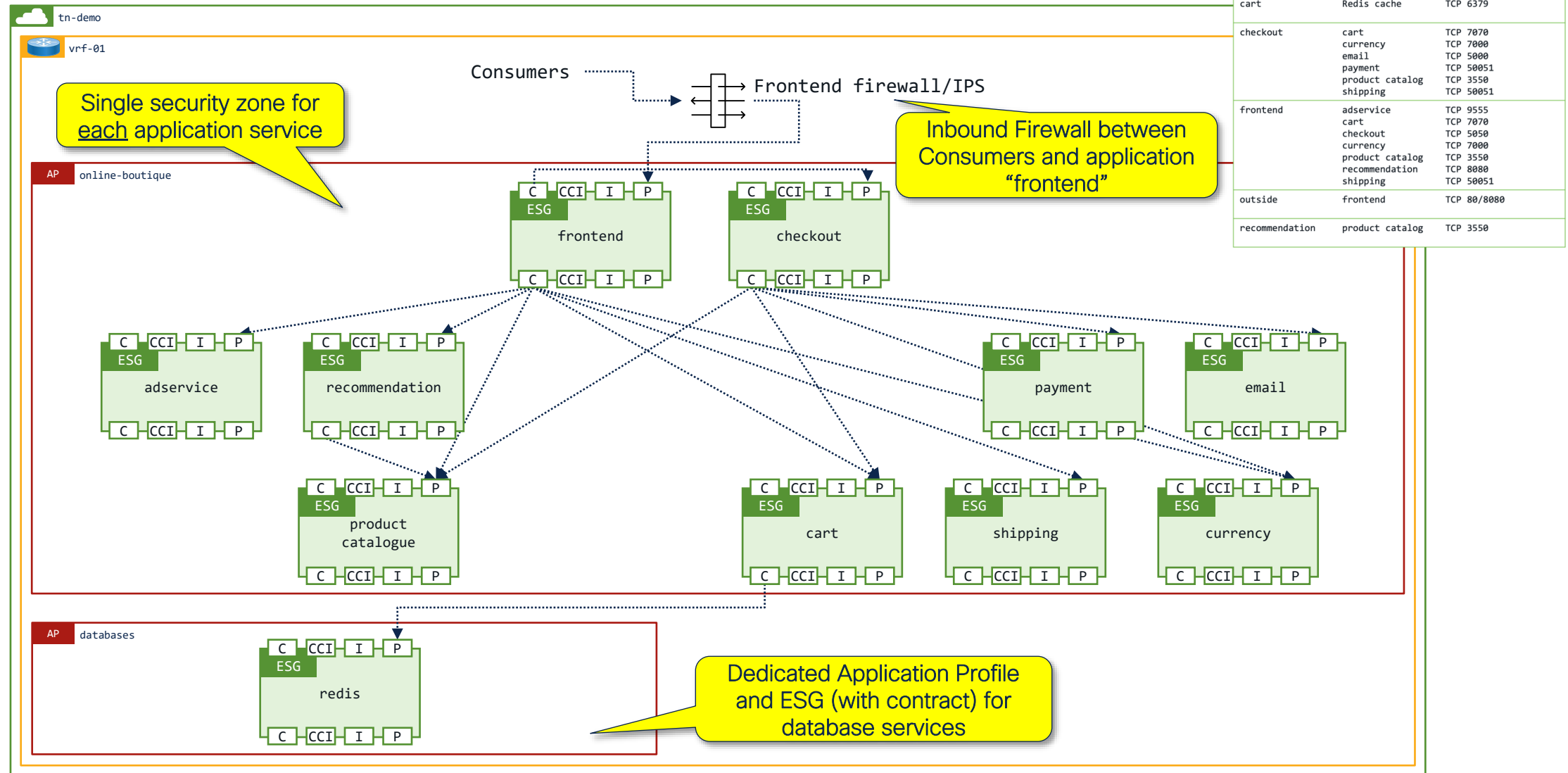
Application tiers across subnets

Application Centric Blueprint #7 – Dedicated AP/ESG for backend database



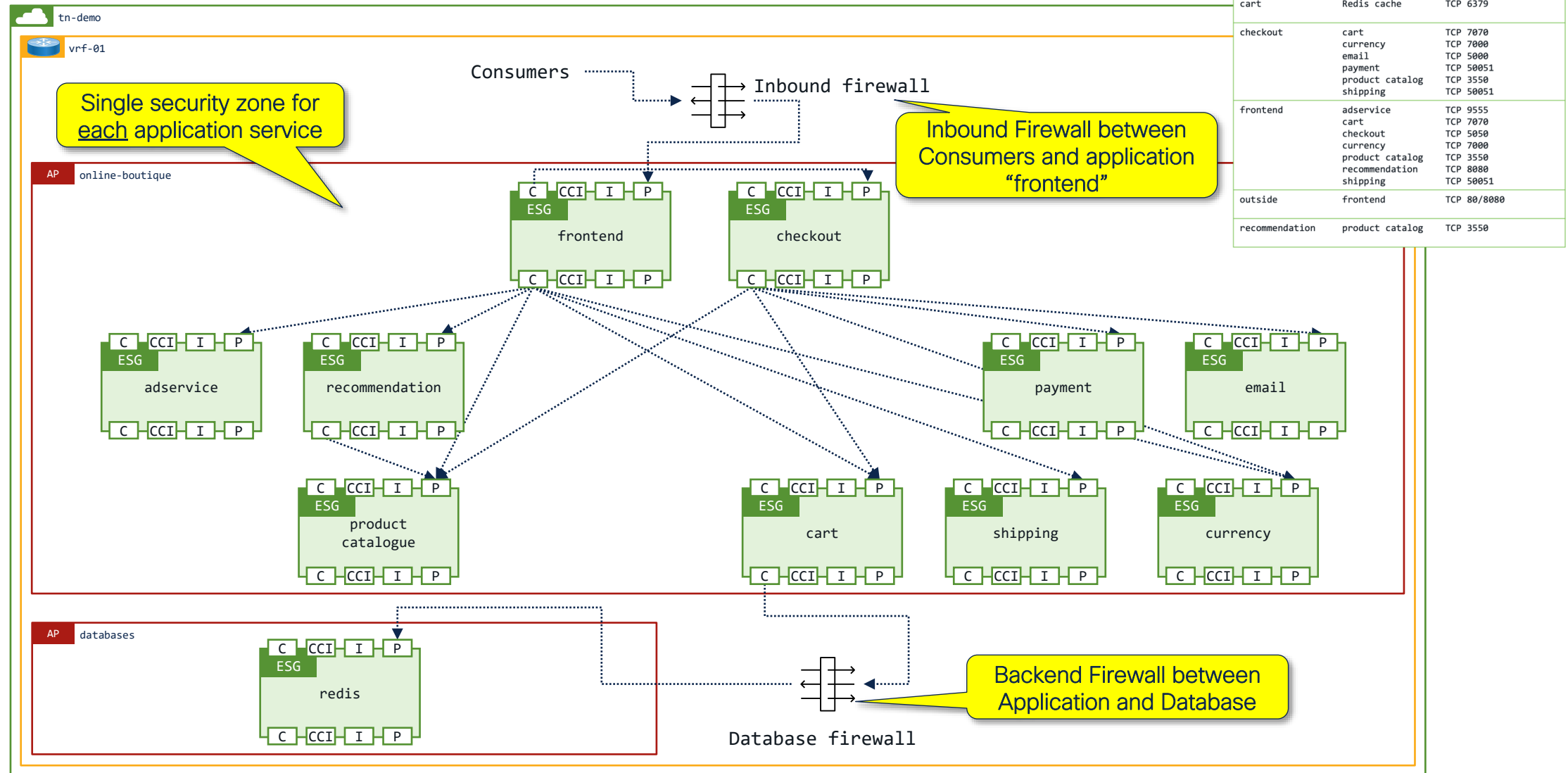
Application tiers across subnets

Application Centric Blueprint #8 – ESG per application tier + frontend firewall/IPS



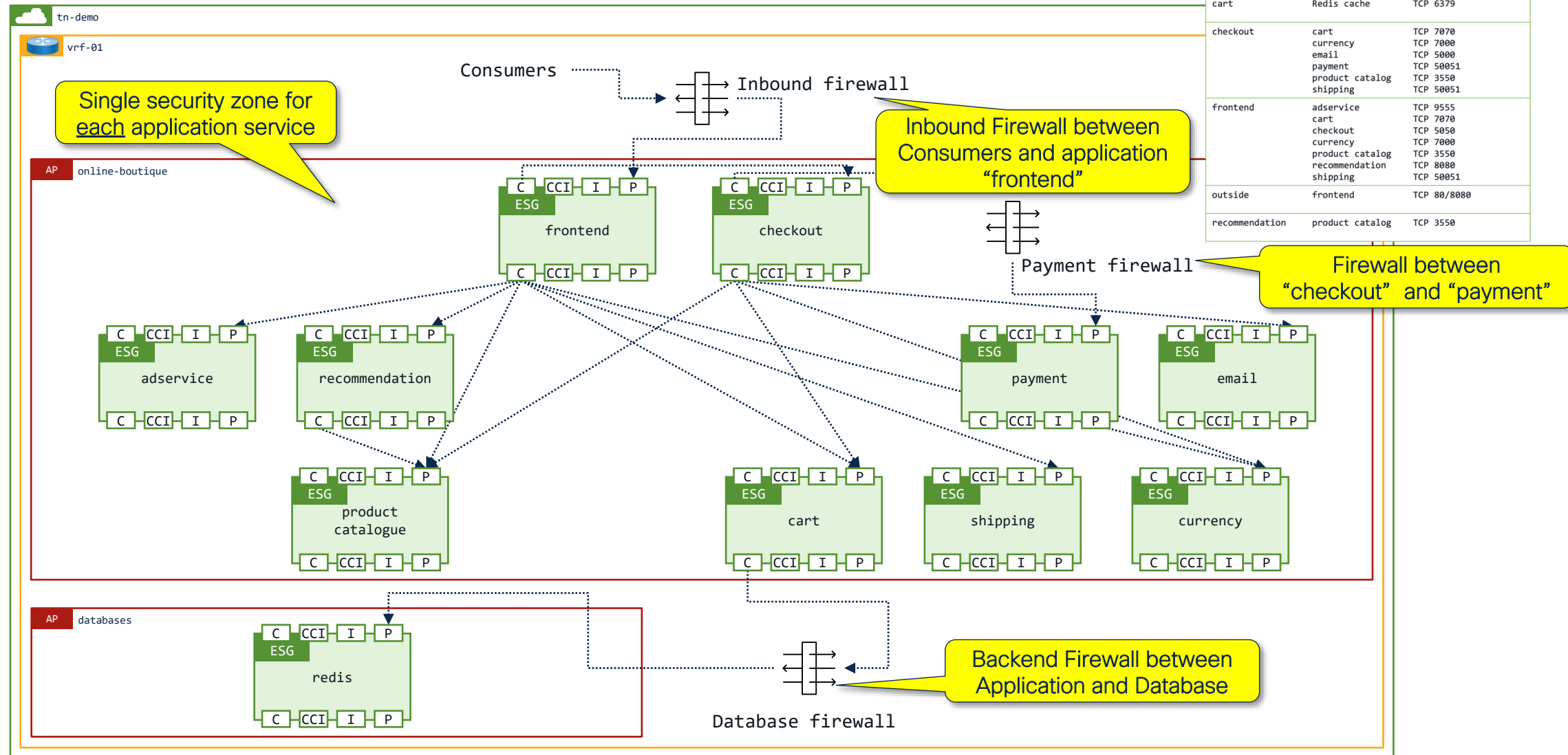
Application tiers across subnets

Application Centric Blueprint #9 – ESG per application tier + frontend firewall/IPS + backend firewall/IPS



Application tiers across subnets

Application Centric Blueprint #10 – ESG per application tier + frontend, backend, and payment firewall/IPS



Wrapping up...



Select one or more Design Patterns...

Carefully consider the use of:

- The “common” tenant
- Using a “shared services” tenant
- vzAny
- Dedicated border Leafs (recommended)
- External EPG with the classifier 0.0.0.0/0

Implement ESG “wrappers” ...

Wrapping applications into ESGs provides the following benefits for both virtual and physical workloads:

- Improved application visibility
- Improved auditing capabilities
- Improved troubleshooting
- Intelligent service insertion
- Security tied applications rather than network segments
- Reduce the reliance on monolithic physical security devices

Benefits of Shared Service model...

- Looks and feels like a Public Cloud model of working
- Network team maintains control of North / South route peering
- Network team maintains control of Inter VRF route leaking
- Each Tenant can control their own CIDR range
- Each Tenant can control their own security rules
- Each Tenant can have private (non routable subnets)
- Security services can be easily inserted in the Tenants
- Do not use 0.0.0.0/0 as the extEPG classifier

Automation Considerations...

- A simple consumption model is everything
- Single API for all networking functions
- Application security requirements should be declared to the infrastructure
- Add virtual application firewalls to deployments if required
- Large physical monolithic firewalls are useful at network boundaries, however they should only provide broad security rules
- Remove unnecessary overlay networks that add layers of complexity

Now available on dCloud

Getting Started with Cisco ACI 6.0 v1

[Schedule](#)[Information](#)[Resources](#)

Overview

Cisco Application Centric Infrastructure (ACI) is a software-defined networking (SDN) solution designed for data centers, the cloud and hybrid-cloud. Cisco ACI allows network infrastructure to be defined based upon network policies - simplifying, optimizing, and accelerating the application deployment lifecycle.

The Cisco Application Policy Infrastructure Controller (Cisco APIC) is the unifying point of automation and management for the Cisco Application Centric Infrastructure (Cisco ACI) fabric. The Cisco APIC provides centralized access to all fabric information, optimizes the application lifecycle for scale and performance, supporting flexible application provisioning across physical and virtual resources.

Cisco ACI virtual machine networking provides hypervisors from multiple vendors programmable and automated access to high-performance, scalable, virtualized data center infrastructure. Programmability and automation are critical features of scalable data center virtualization infrastructure. The ACI open REST API enables virtual machine (VM) integration with and orchestration of the policy-model-based ACI fabric. ACI VM networking enables consistent enforcement of policies across both virtual and physical workloads that are managed by hypervisors from multiple vendors.

This lab provides an introduction to Cisco ACI, taking the user through the initial setup process and configuring integration with a VMware vSphere. Then the user reviews the the ACI security model, and how to implement it, learning about Tenants, Application Profiles, Endpoint Groups, Endpoint Security Groups, and Contracts and Filters.

For additional information, visit www.cisco.com/go/apic.

Cisco Webex App

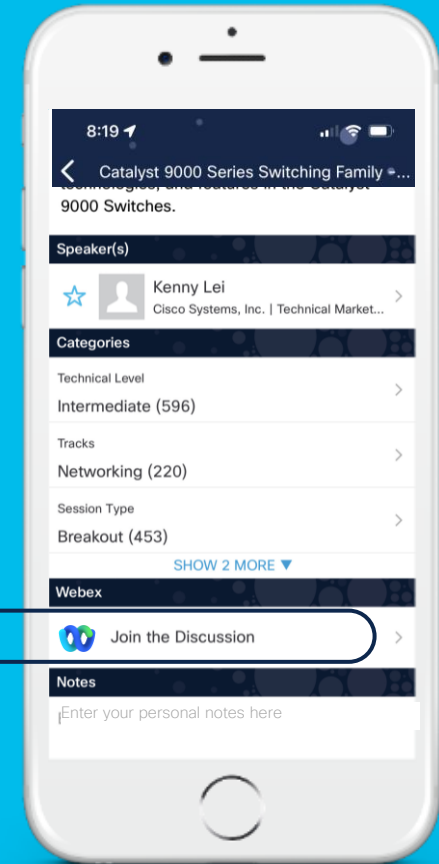
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated until February 24, 2023.



Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at <https://www.ciscolive.com/emea/learn/sessions/session-catalog.html>



Continue Your Education



Visit the Cisco Showcase for related demos.



Book your one-on-one Meet the Engineer meeting.



Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.



Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.



The bridge to possible

Thank you

CISCO *Live!*

ALL

IN