

The background features a vibrant, abstract design with a color gradient from dark blue at the top to bright yellow and orange at the bottom. The design consists of overlapping, wavy horizontal bands and a series of radiating lines on the right side, creating a sense of motion and energy.

CISCO *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

ACI – “not just another network...”

Steve Sharman – Technical Solutions Architect
@sps2101
BRKDCN-2984

cisco *Live!*

#CiscoLiveAPJC

Cisco Webex App

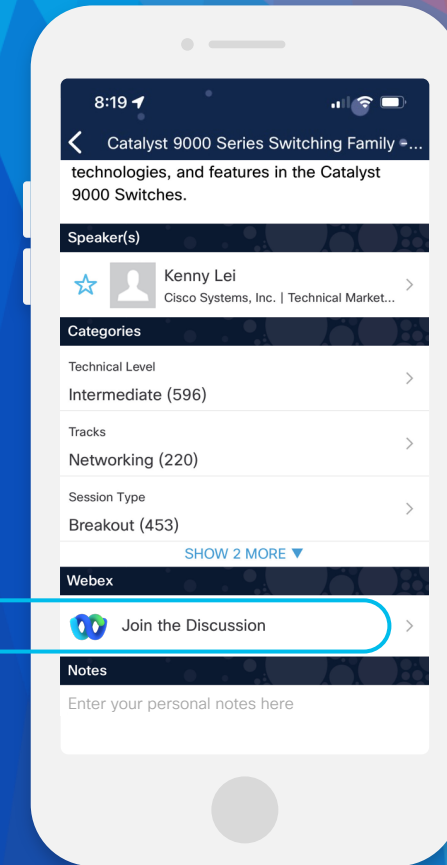
Questions?

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 by the speaker until December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKDCN-2984>

Agenda

- Setting the scene
- Network Centric vs Application Centric
- Greenfield vs Brownfield
- Converting from Network Centric to Application Centric
- Allowing open communication
- Security with ESGs
- Understanding Contracts
- External connectivity
- Firewall integration
- 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.

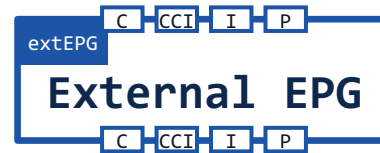
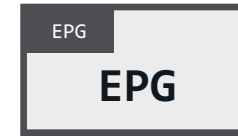
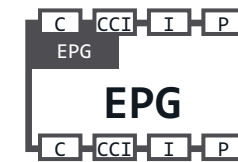
Before we get
started...

There are lots (and lots) of details in this presentation, please download through the [Cisco Live app](#).

Well unless you have binoculars with you...!



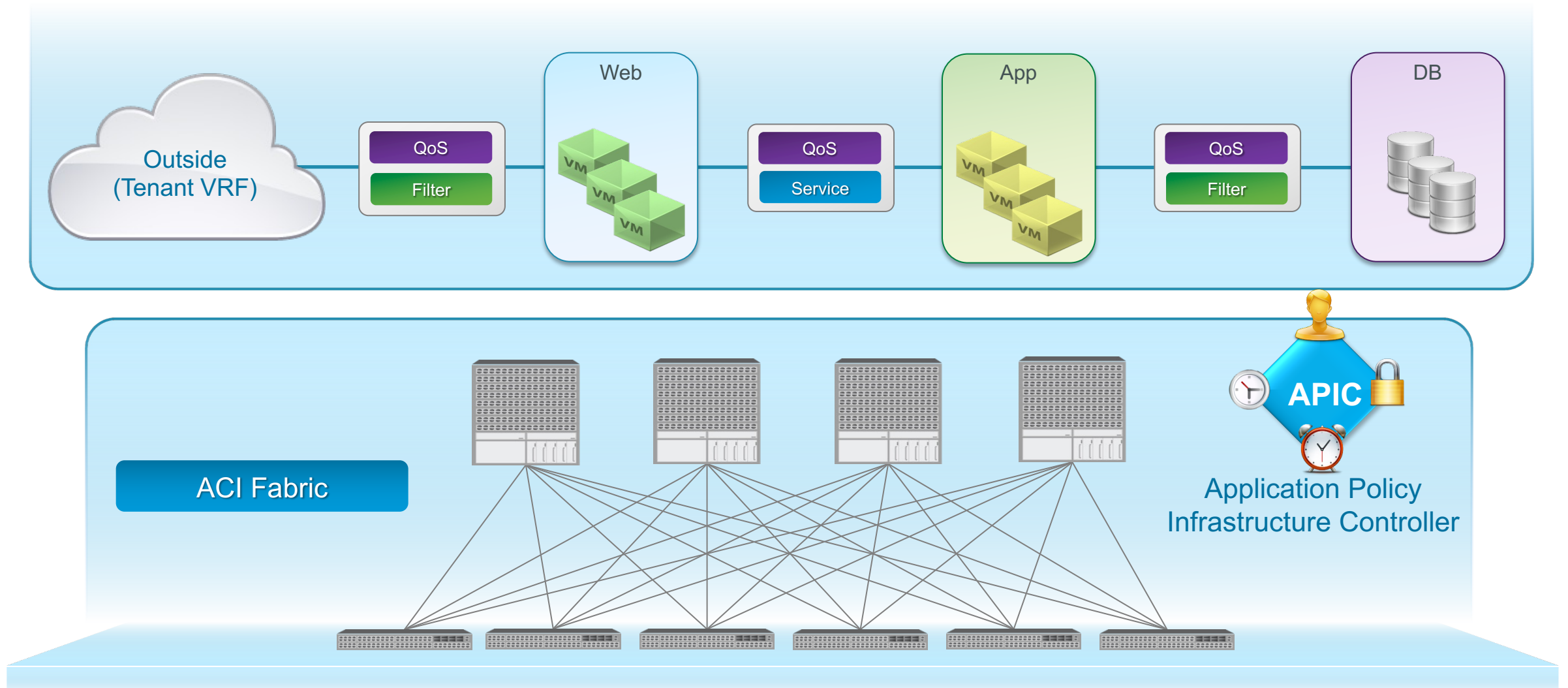
Icons



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

The ACI reference application from circa 2014...

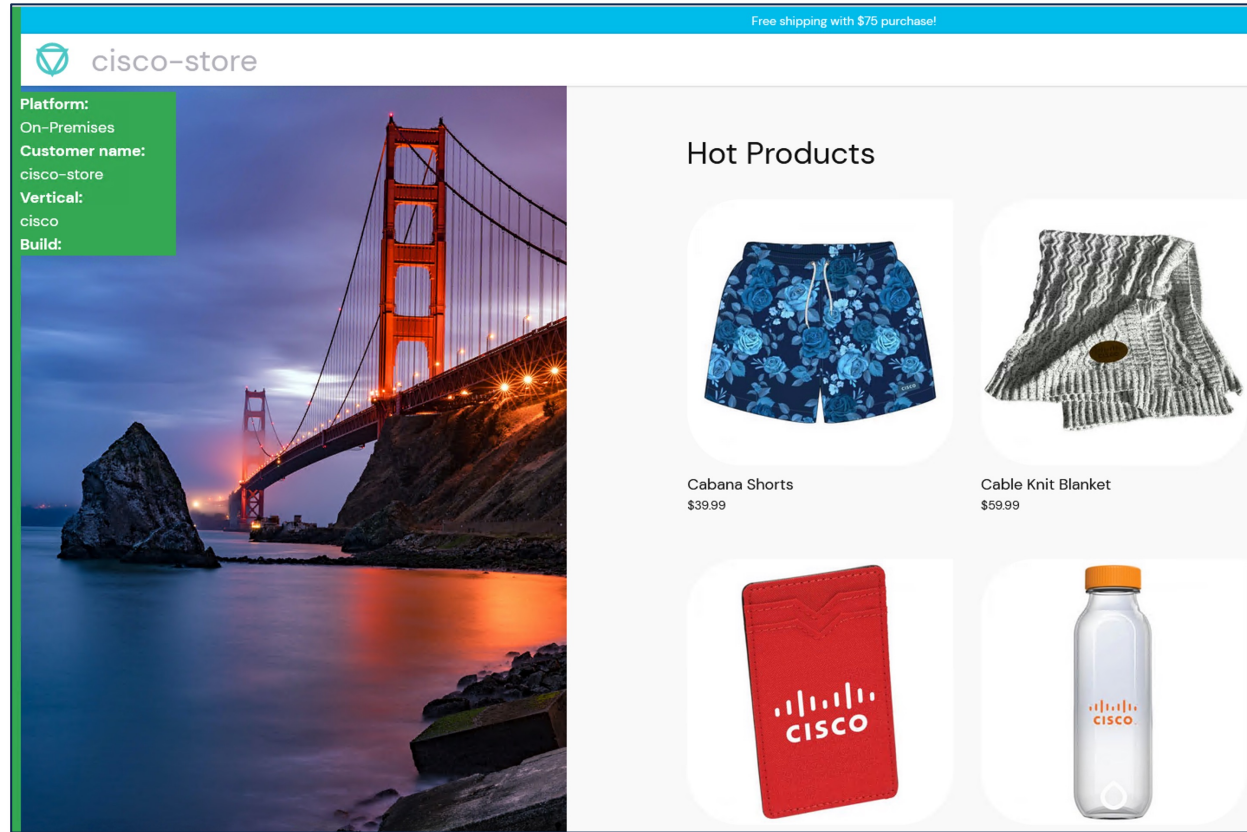
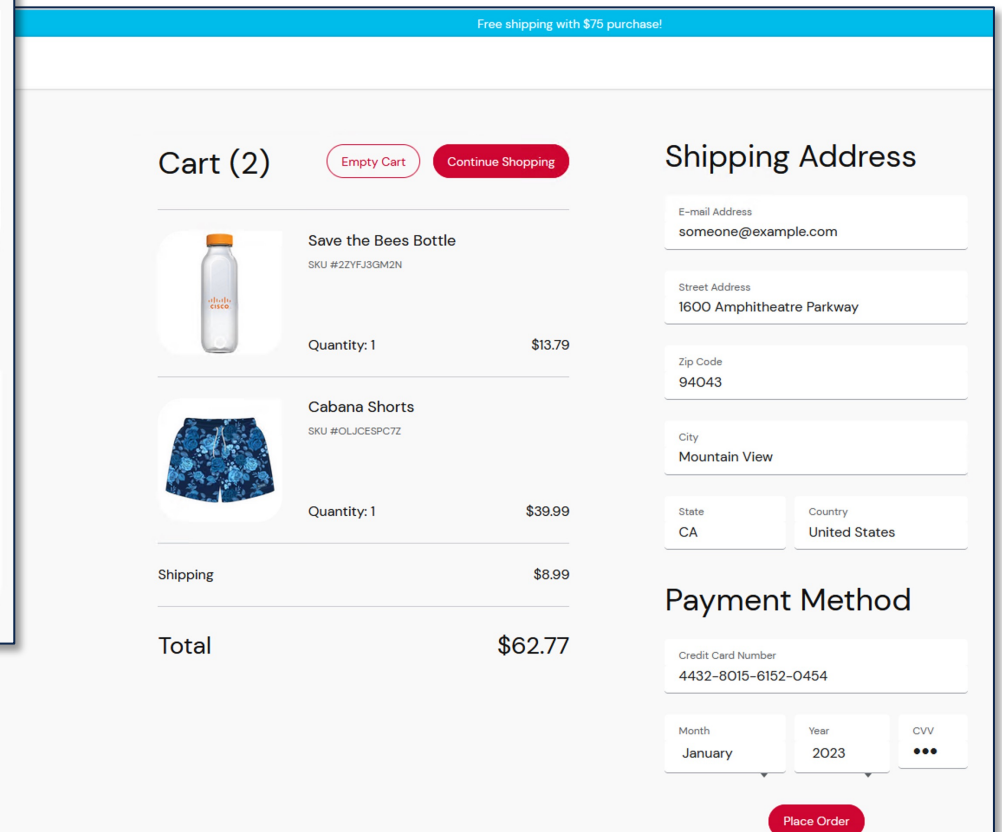
The mythical three tier application...!



Our reference application for this presentation...

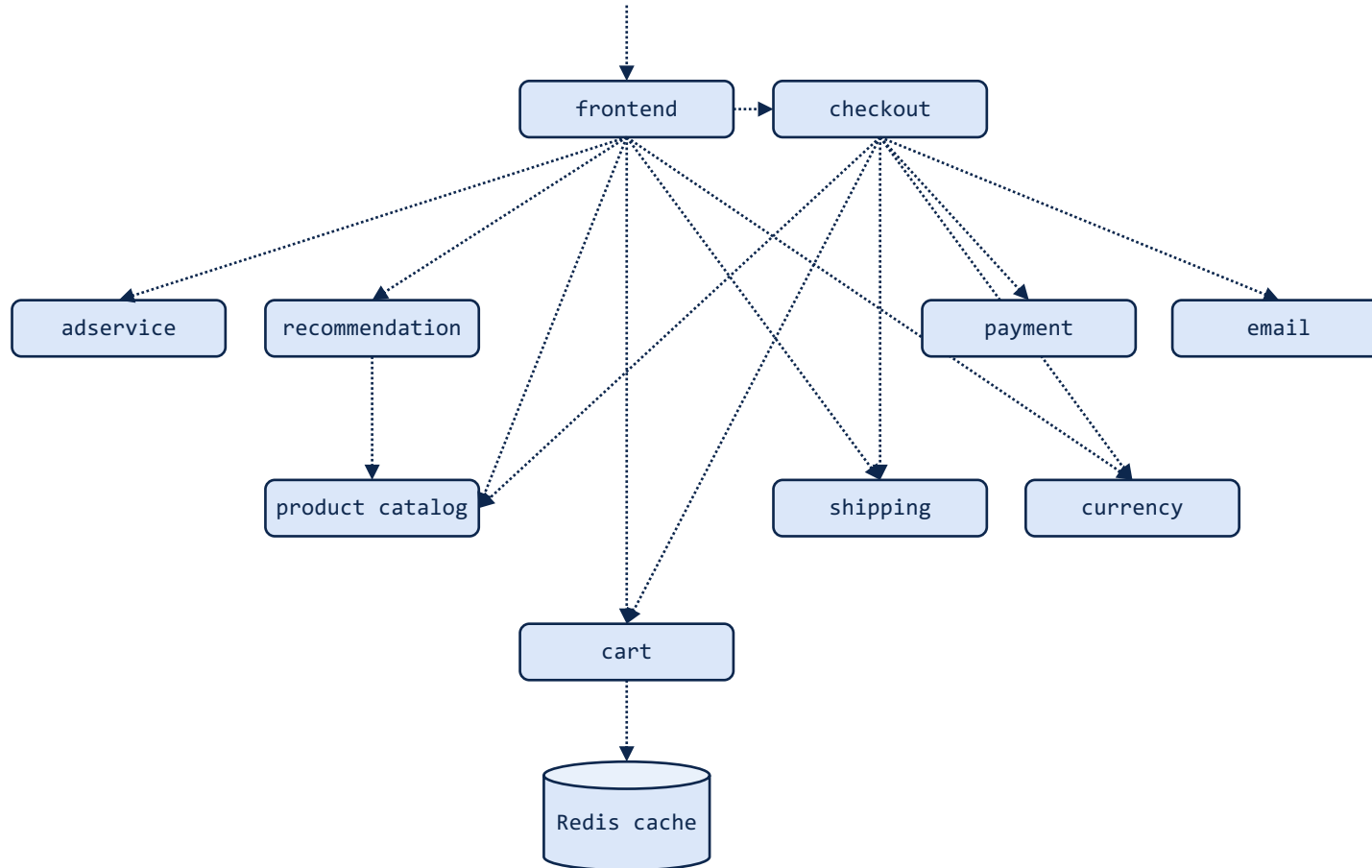
Online Boutique

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



Online Boutique

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

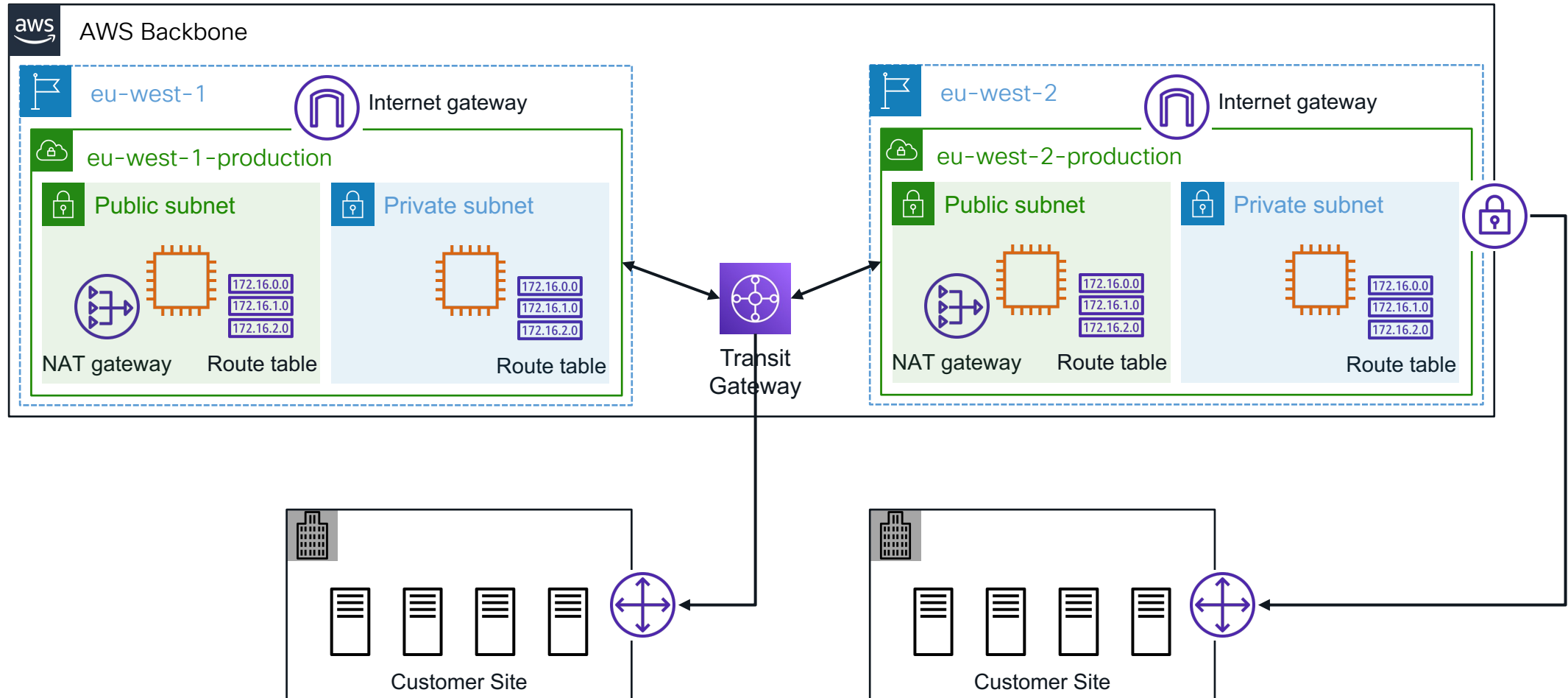


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 8080
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP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



Cross Functional
Teams



New Talent
Attraction



Scaling



New Culture



Think Agile



Evolution Instead
of Revolution



Partnerships 2.0

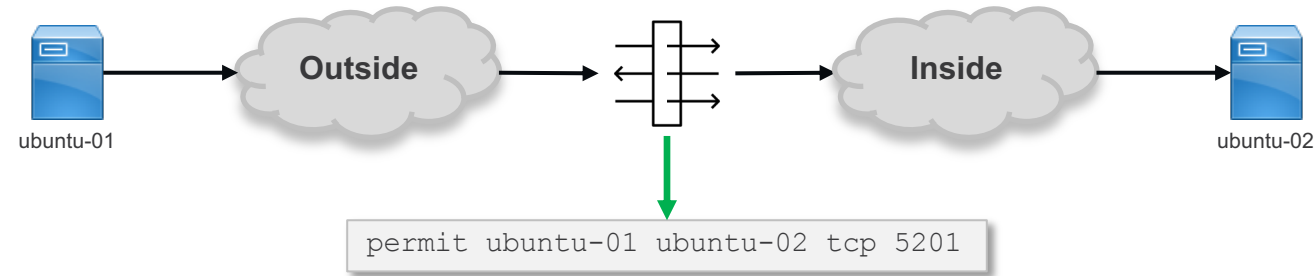
A cloud operating model succeeds best when there is a new organisational culture...

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

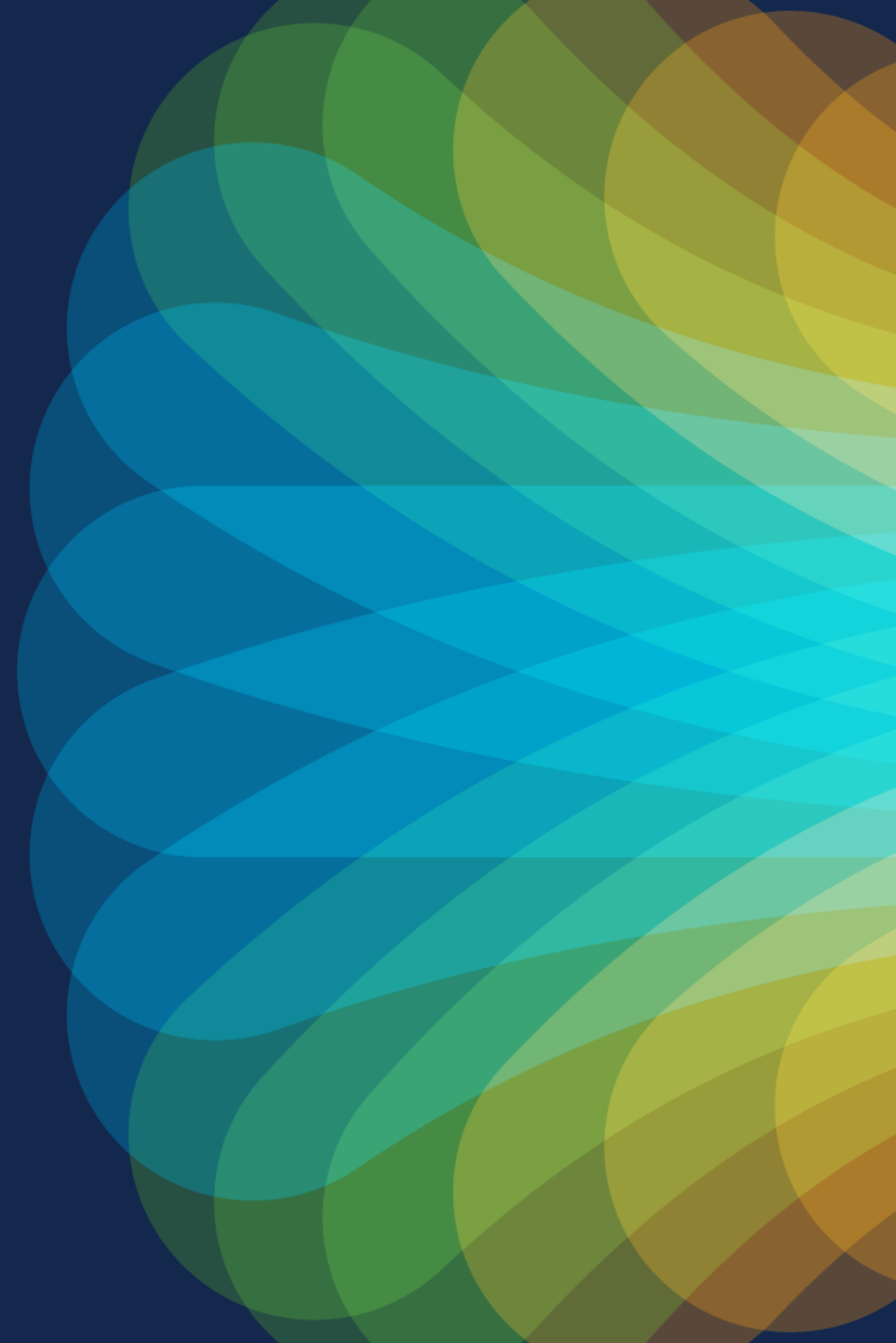


Single API Model for 100s of switches and 1000s of ports; cloud-like consumption model



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 icons for voice search, image search, and a magnifying glass. Below the search bar, there are tabs for "All", "Images", "Videos", "News", "Books", and "More". The results show "About 157,000 results (0.48 seconds)". The first result is from "https://ipwithease.com > Blog" 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 table snippet showing a comparison between Network Centric and Application Centric modes. Below this, 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?". The second 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 ...". The third result is 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 icons for voice search, image search, and a magnifying glass. Below the search bar, there are tabs for "All", "Images", "Videos", "News", "Books", and "More". The 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 ...". The second result is 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 ...". The third result is 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. ★★★★★ Rating: 5 · 86 reviews". The fourth result is 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. 5 pages". The fifth result is 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 ...". The sixth result is 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

What is my definition of Application Centric mode...?

An Application Centric deployment identifies where applications are running on the fabric – which switch, which interface, which VLAN...

An Application Centric deployment optionally controls security rules for inter and intra application traffic...

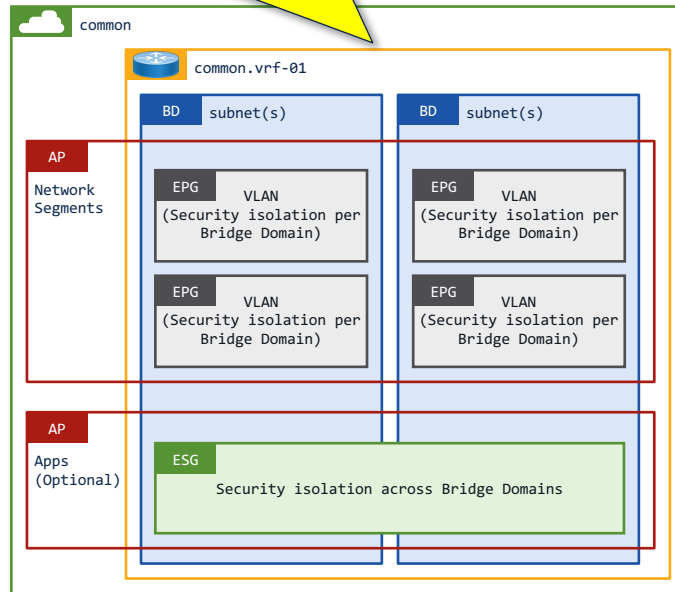
Where should
we start...?



Design Considerations...

Design Patterns

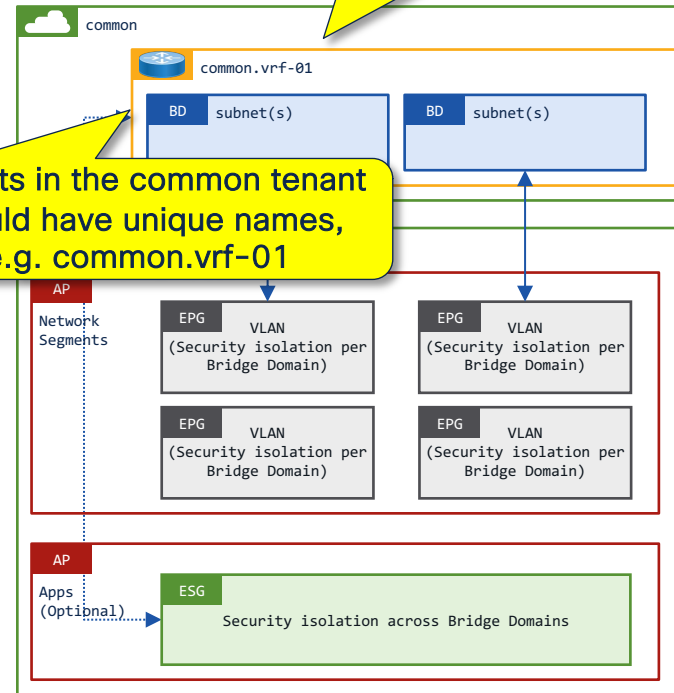
Everything in the “common” Tenant is not typically seen



Used for functions which are accessible from any Tenant

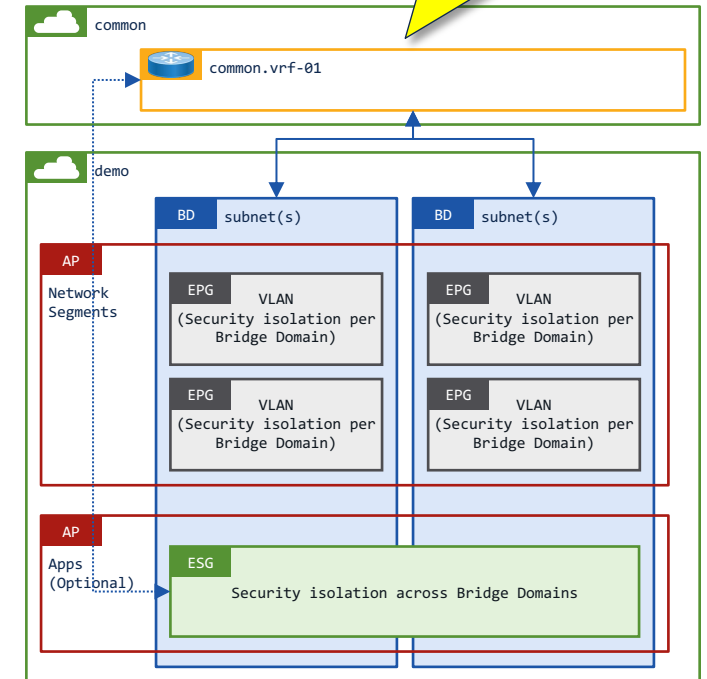
VRFs and BDs in “common” with EPGs and ESGs in the “user” tenant

Objects in the common tenant should have unique names, e.g. common.vrf-01



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

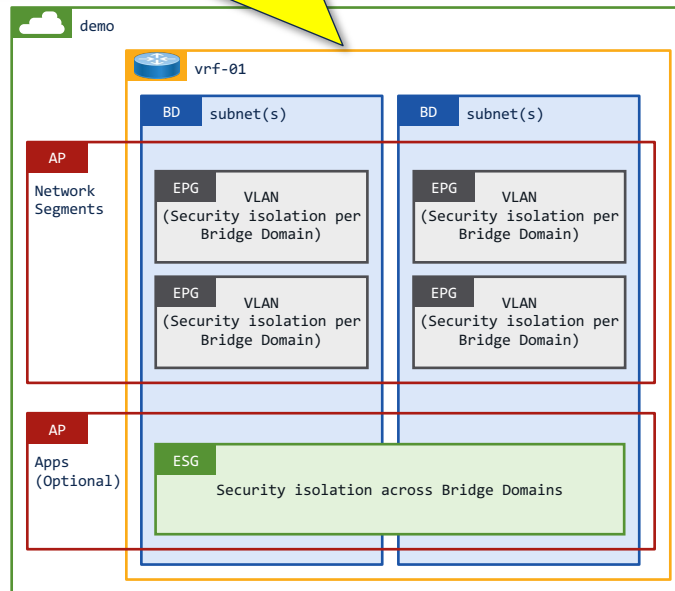
VRFs in “common” with BDs, EPGs and ESGs in the “user” tenant



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

Design Patterns

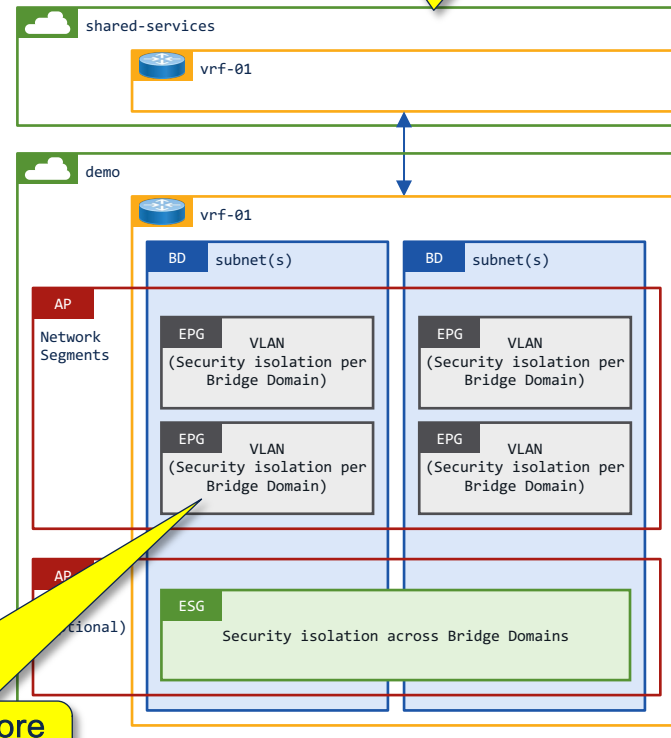
All networking constructs contained within a Tenant



Dedicated VRFs and subnets for each Tenant with Dedicated L3outs

Each Tenant has one or more network security groups

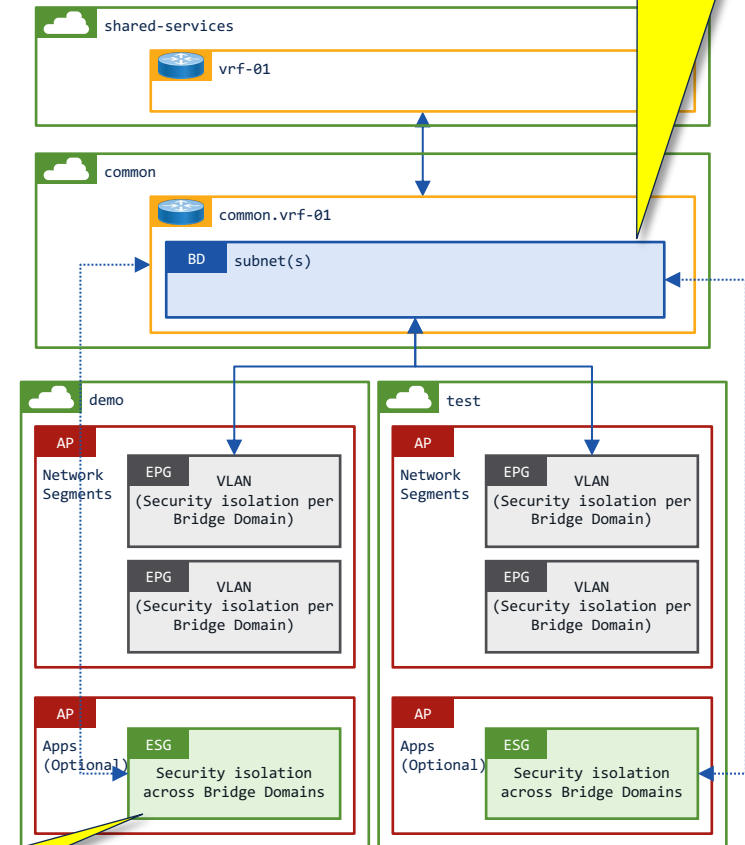
Network team controls inbound/outbound routing



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: <input type="text"/>	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: 2022-11-26T07:59 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

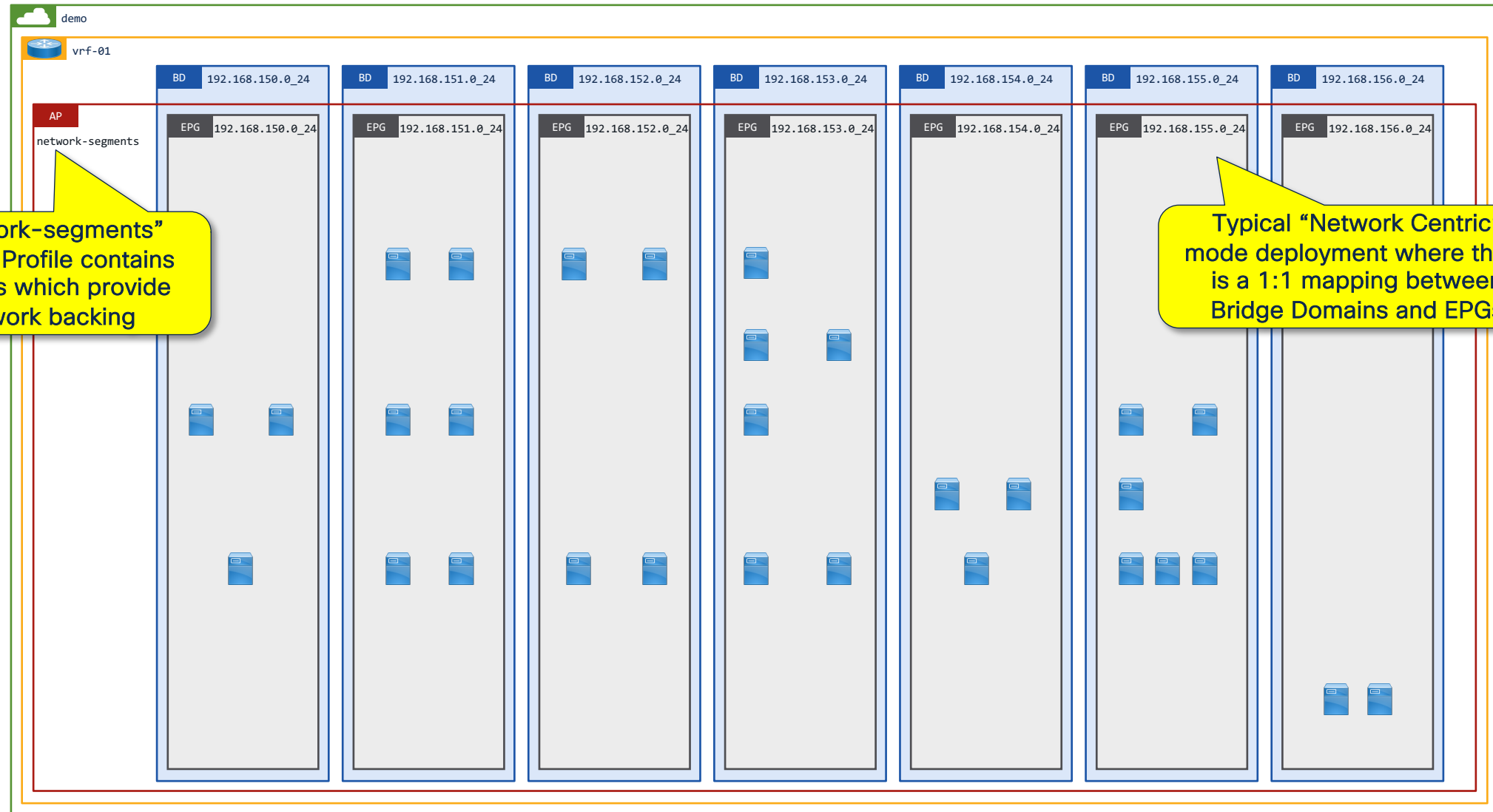
IP range per Tenant



Convert a Brownfield Network Centric environment to an Application Centric environment

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

Workloads identified by IP and Mac address

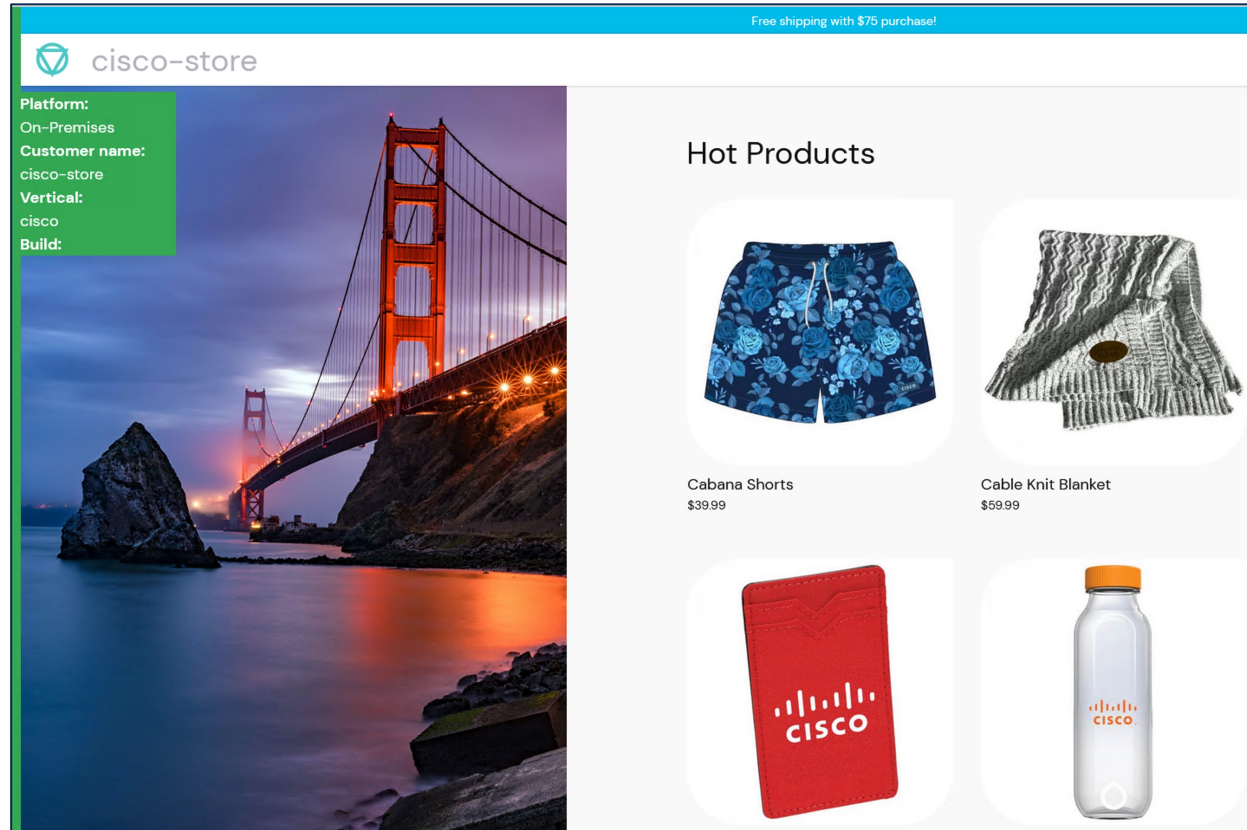
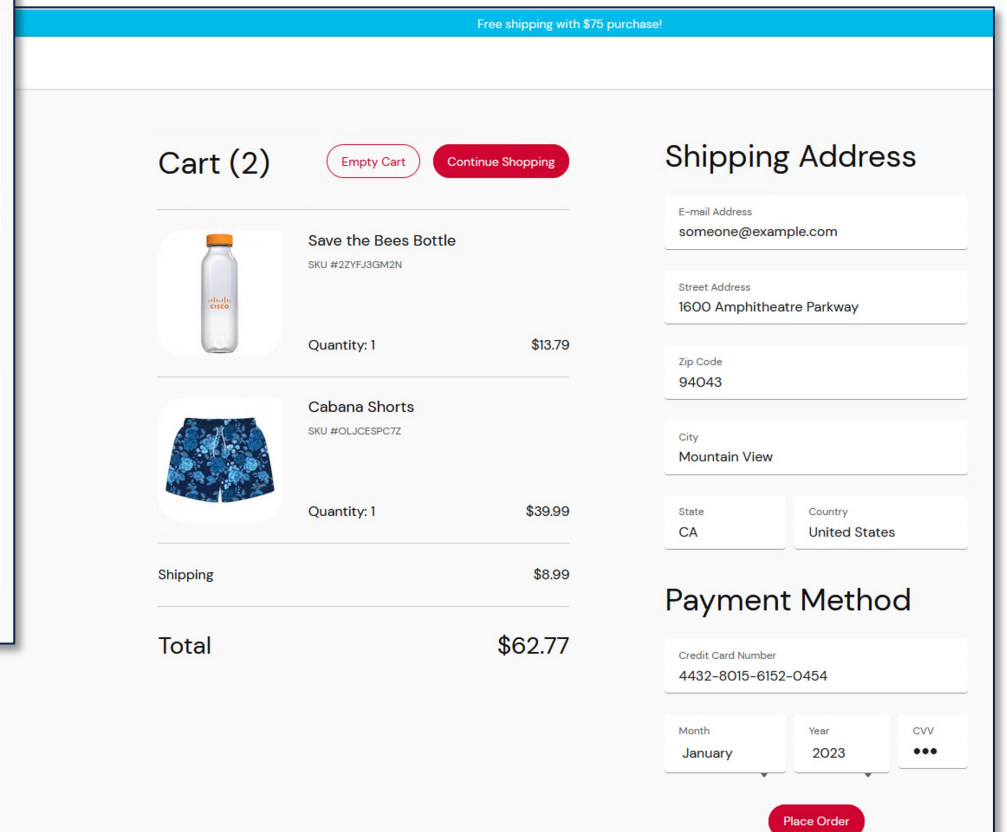


What does the application owner care about...?

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

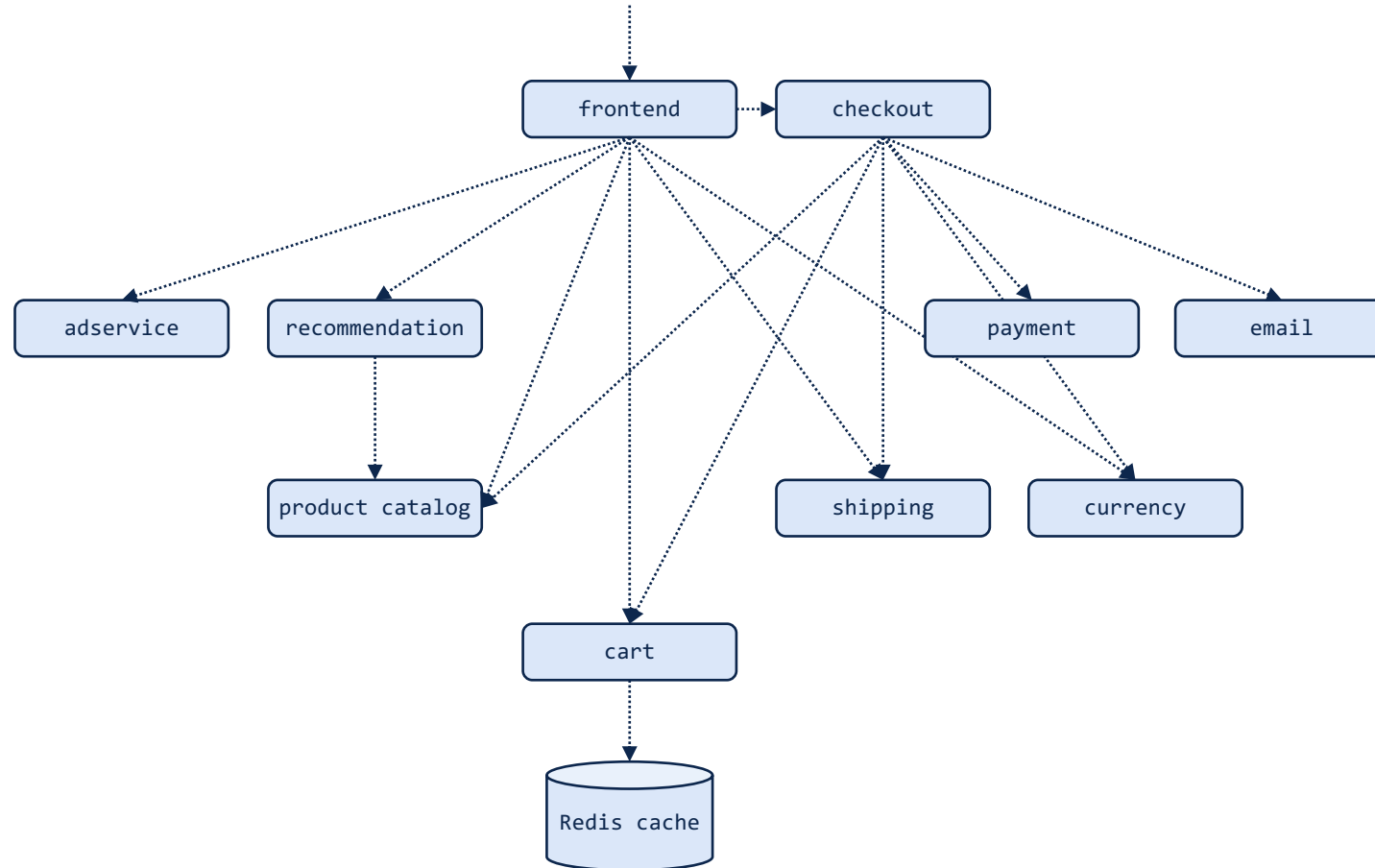
Online Boutique

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



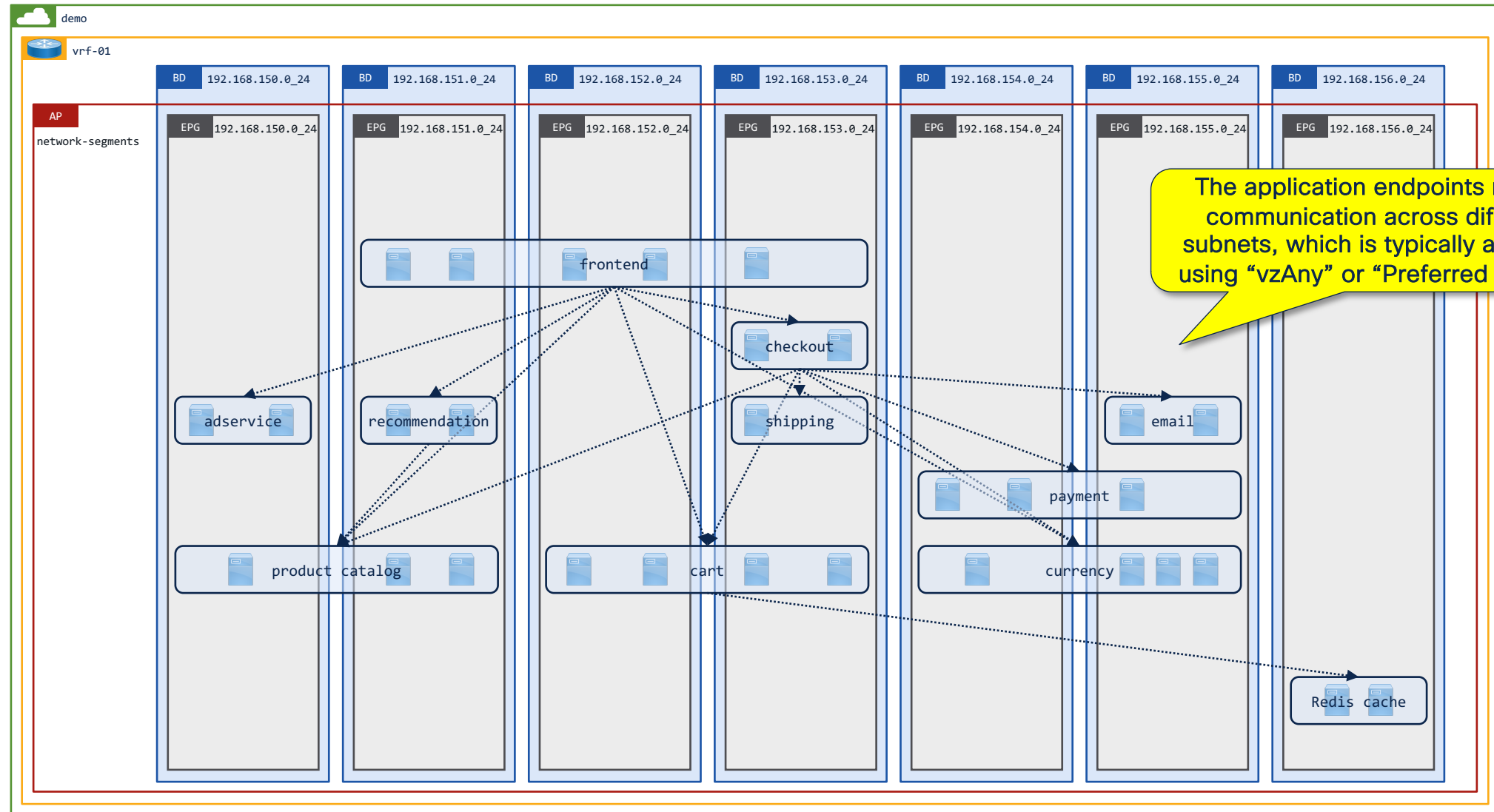
Online Boutique

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

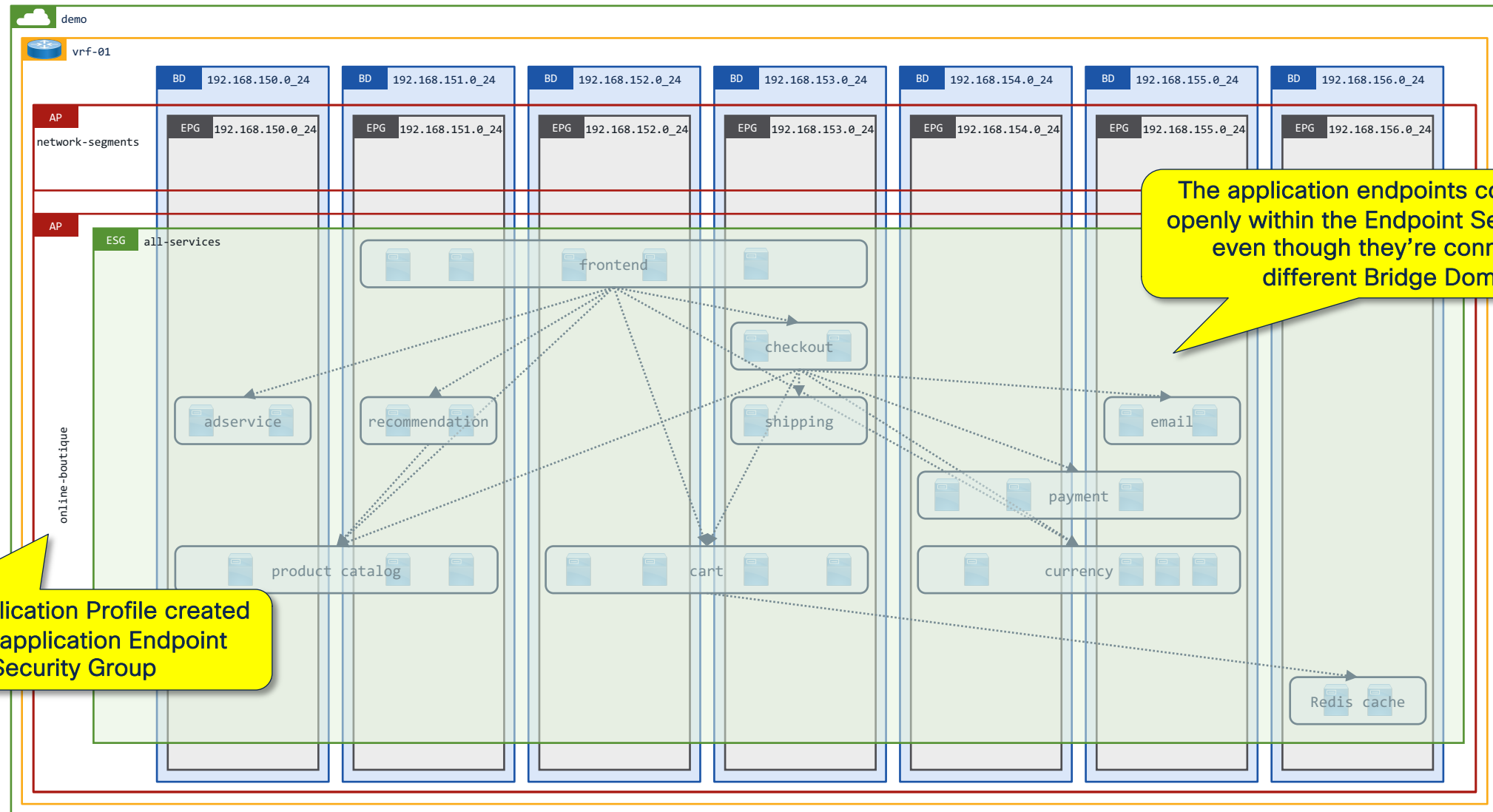


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 8080
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP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

Where is our application running...?



Let's convert to "Application Centric" mode



What does this mean to the network admin...?

Application Visibility...!

demo

ESG - all-services

Application Endpoint IP and MAC Information

Host Information

VLAN Information

Tag Information

MAC/IP	Endpoint Name	Hosting Server	Interface (learned)	Encap	Base EPG	Policy Tags
00:50:56:A1:1A:60 192.168.150.100	tn-demo-online-boutique-ad-service	10.237.98.165	Pod-1/Node-102/eth1/29 (learned,vm...	vlan-1146(P) vlan-1147(S)	demo:network-segments:192.168.150.0_24	_vmm:vmname tn-demo-online-boutique-ad-service Function tn-demo-online-boutique-ad-service
00:50:56:A1:3F:2C 192.168.151.101	tn-demo-online-boutique-frontend-service	10.237.98.168	Pod-1/Node-101/eth1/32 (learned,vmm)	vlan-1175(P) vlan-1176(S)	demo:network-segments:192.168.151.0_24	_vmm:vmname tn-demo-online-boutique-frontend-servic Function tn-demo-online-boutique-frontend-service
00:50:56:A1:7F:0B 192.168.153.155	tn-demo-online-boutique-checkout-service	10.237.98.168	Pod-1/Node-102/eth1/32 (learned,vm...	vlan-1177(P) vlan-1178(S)	demo:network-segments:192.168.153.0_24	_vmm:vmname tn-demo-online-boutique-checkout-servi Function tn-demo-online-boutique-checkout-service
00:50:56:A1:7F:A5 192.168.156.155	tn-demo-online-boutique-redis-cart	10.237.98.166	Pod-1/Node-101/eth1/30 (learned,vm...	vlan-1101(P) vlan-1102(S)	demo:network-segments:192.168.156.0_24	_vmm:vmname tn-demo-online-boutique-redis-cart Function tn-demo-online-boutique-redis-cart
00:50:56:A1:8F:09 192.168.153.156	tn-demo-online-boutique-payment-service	10.237.98.167	Pod-1/Node-101/eth1/31 (learned,vmm)	vlan-1150(P) vlan-1151(S)	demo:network-segments:192.168.154.0_24	_vmm:vmname tn-demo-online-boutique-payment-servic Function tn-demo-online-boutique-payment-service
00:50:56:A1:09:2F 192.168.150.101	tn-demo-online-boutique-shipping-service	10.237.98.166	Pod-1/Node-101/eth1/30 (learned,vm...	vlan-1177(P) vlan-1178(S)	demo:network-segments:192.168.153.0_24	_vmm:vmname tn-demo-online-boutique-shipping-servic Function tn-demo-online-boutique-shipping-service
00:50:56:A1:22:DE 192.168.152.100	tn-demo-online-boutique-product-catalog-service	10.237.98.166	Pod-1/Node-102/eth1/30 (learned,vm...	vlan-1146(P) vlan-1147(S)	demo:network-segments:192.168.150.0_24	_vmm:vmname tn-demo-online-boutique-product-catalog Function tn-demo-online-boutique-product-catalog-servic
00:50:56:A1:84:4D 192.168.155.155	tn-demo-online-boutique-cart-service	10.237.98.167	Pod-1/Node-102/eth1/31 (learned,vmm)	vlan-1148(P) vlan-1149(S)	demo:network-segments:192.168.152.0_24	_vmm:vmname tn-demo-online-boutique-cart-service Function tn-demo-online-boutique-cart-service
00:50:56:A1:B0:E2	tn-demo-online-boutique-email-service	10.237.98.167	Pod-1/Node-101/eth1/31 (learned,vmm)	vlan-1109(P) vlan-1110(S)	demo:network-segments:192.168.155.0_24	_vmm:vmname tn-demo-online-boutique-email-service Function tn-demo-online-boutique-email-service
00:50:56:A1:B0:E2	tn-demo-online-boutique-recommendation-service	10.237.98.168	Pod-1/Node-101/eth1/32 (learned,vmm)	vlan-1175(P) vlan-1176(S)	demo:network-segments:192.168.151.0_24	_vmm:vmname tn-demo-online-boutique-recommendatio Function tn-demo-online-boutique-recommendation-servic

Endpoint names

Switch and Interface Information

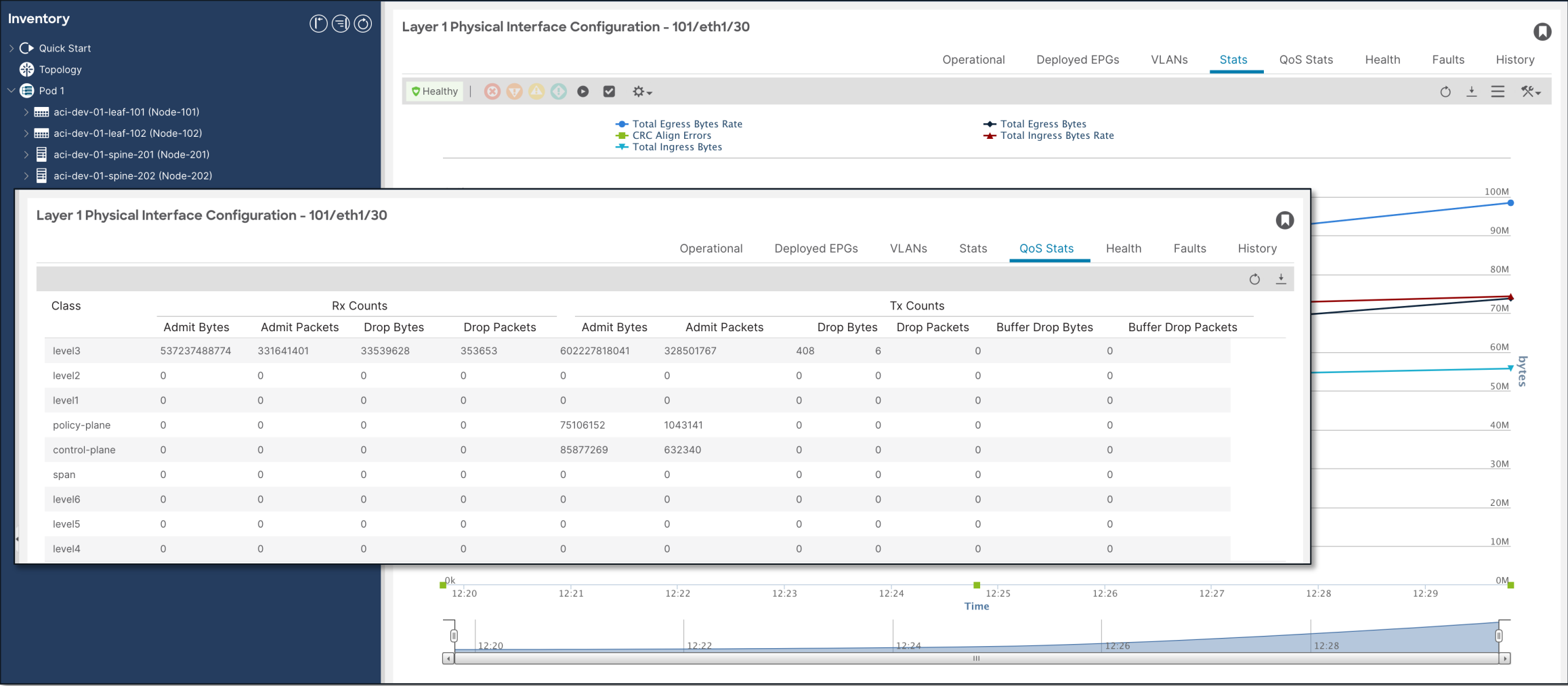
EPG/Subnet Information

Page 1 Of 1

Objects Per Page: 100

Displaying Objects 1 - 11 Of 11

Correlate Endpoints to Switch Interfaces...



How do I change
“modes”...?

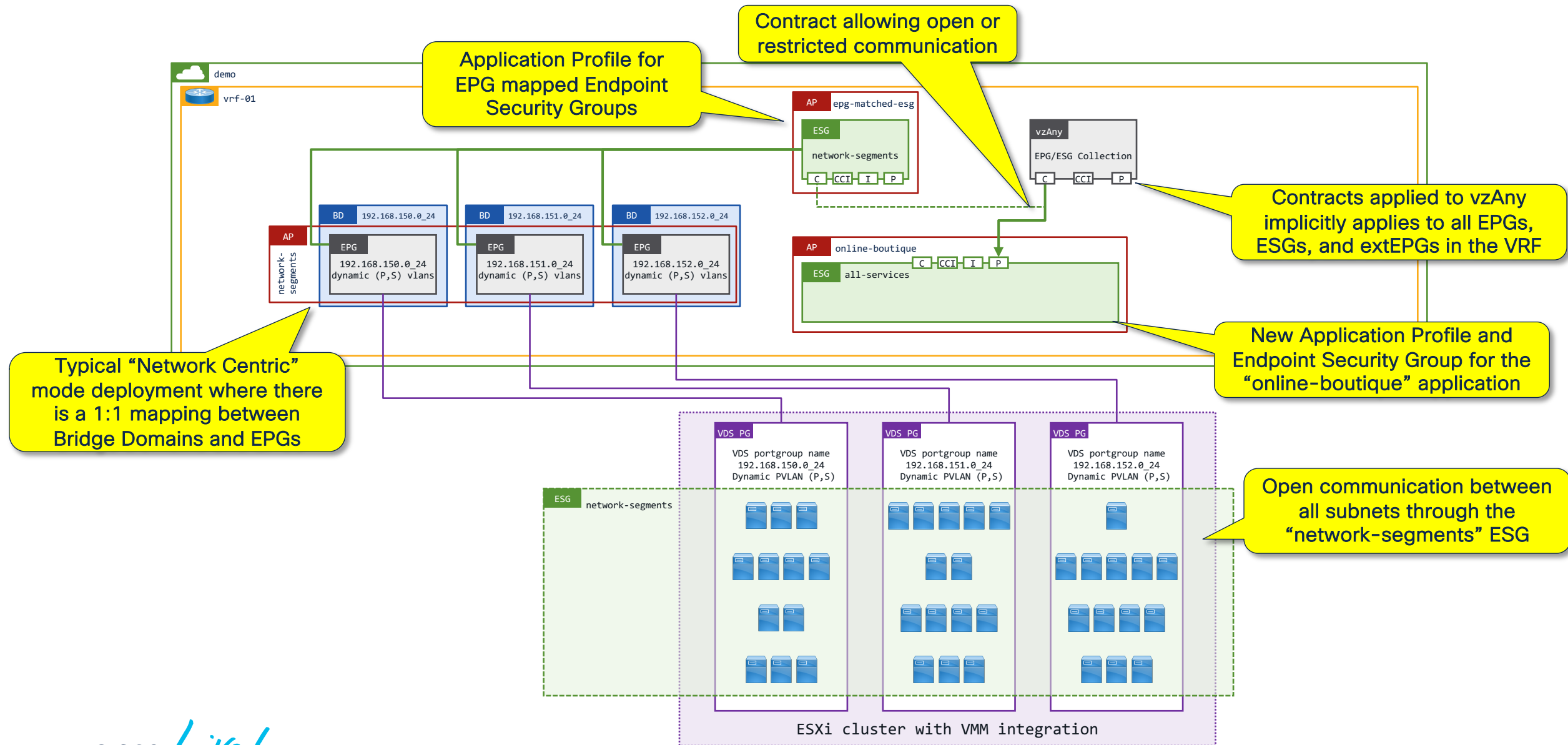


Application name + Application IP addresses...

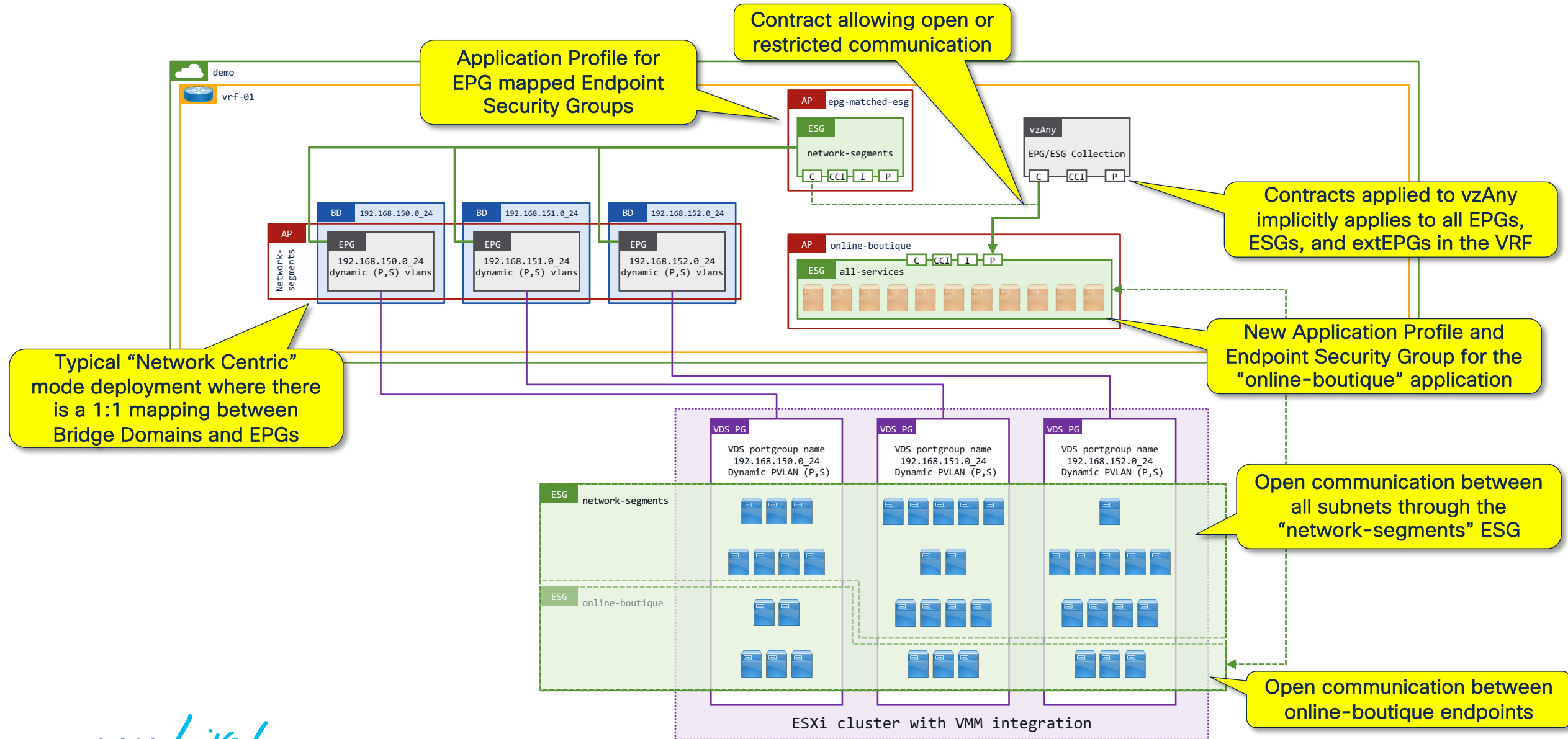
Physical or virtual workloads, with or without VMM Integration...!

You can convert from Network Centric mode to Application Centric mode in two simple steps...

Step 1: Create Application Profiles and Security Groups



Step 2: Tag Workloads to move into the new Security Group



Tagging Option 1: Static Tag Mapping

demo-non-vmm

- Quick Start
- demo-non-vmm
 - Application Profiles
 - epg-matched-esg
 - network-segments
 - online-boutique
 - Application EPGs
 - uSeg EPGs
 - Endpoint Security Groups
 - all-services
 - Contracts
 - Selectors
 - Tag Selectors
 - EPG Selectors
 - IP Subnet Selectors
 - Service EPG Selectors

- Policies
- Protocol
- Troubleshooting
- Host Protection
- Monitoring
- NetFlow
- VMM
- Endpoint Tags
- Endpoint MAC
- Endpoint IP
- Services
- Security

Tag Selectors

Tag Key	Value Operator	Tag Value
ApplicationName	Equals	online-boutique

Define ESG Tag Selector

ApplicationName = online-boutique

Map MAC or IP address to Tag Value

00:50:56:A1:0A:90 = ApplicationName online-boutique

Endpoint MAC

MAC Address	Bridge Domain	VRF	Tags	Matching Tag Selector
00:50:56:A1:0A:90	*	vrf-01	ApplicationName online-boutique	uni/tn-demo-non-vmm/ap-online-boutique/esg-all-services/tagselectorkey-[ApplicationName]-value-[online-boutique]
00:50:56:A1:11:B7	*	vrf-01	ApplicationName online-boutique	uni/tn-demo-non-vmm/ap-online-boutique/esg-all-services/tagselectorkey-[ApplicationName]-value-[online-boutique]
00:50:56:A1:15:9B	*	vrf-01	ApplicationName online-boutique	uni/tn-demo-non-vmm/ap-online-boutique/esg-all-services/tagselectorkey-[ApplicationName]-value-[online-boutique]
00:50:56:A1:41:B1	*	vrf-01	ApplicationName online-boutique	uni/tn-demo-non-vmm/ap-online-boutique/esg-all-services/tagselectorkey-[ApplicationName]-value-[online-boutique]
00:50:56:A1:4F:95	*	vrf-01	ApplicationName online-boutique	uni/tn-demo-non-vmm/ap-online-boutique/esg-all-services/tagselectorkey-[ApplicationName]-value-[online-boutique]
00:50:56:A1:6A:4F	*	vrf-01	ApplicationName online-boutique	uni/tn-demo-non-vmm/ap-online-boutique/esg-all-services/tagselectorkey-[ApplicationName]-value-[online-boutique]
00:50:56:A1:88:3B	*	vrf-01	ApplicationName online-boutique	uni/tn-demo-non-vmm/ap-online-boutique/esg-all-services/tagselectorkey-[ApplicationName]-value-[online-boutique]
00:50:56:A1:C7:4C	*	vrf-01	ApplicationName online-boutique	uni/tn-demo-non-vmm/ap-online-boutique/esg-all-services/tagselectorkey-[ApplicationName]-value-[online-boutique]
00:50:56:A1:E6:B8	*	vrf-01	ApplicationName online-boutique	uni/tn-demo-non-vmm/ap-online-boutique/esg-all-services/tagselectorkey-[ApplicationName]-value-[online-boutique]

Match Endpoints to Workload Tags

Automated conversion to “Application Centric”



Tagging Option 2: VMM Tag Mapping

The image shows a comparison between vCenter and Cisco ACI tagging interfaces. A yellow callout points to the 'Assign Tag...' button in vCenter, and another points to the 'Tag Selectors' table in ACI. A red box highlights the matching tag entries in both interfaces, with a third yellow callout stating they match.

vCenter Application Workload Tags

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

ADD TAG

☐	Tag Name	Category
☐	tn-demo-online-boutique-product-catalog-service	Function
☐	tn-demo-online-boutique-email-service	Function
☐	tn-demo-online-boutique-ad-service	Function
☐	tn-demo-online-boutique-recommendation-service	Function
☐	tn-demo-online-boutique-shipping-service	Function
☒	tn-demo-online-boutique-frontend-service	Function
☐	tn-demo-online-boutique-checkout-service	Function
☐	tn-demo-online-boutique-payment-service	Function
☐	tn-demo-online-boutique-currency-service	Function
☐	tn-demo-online-boutique-redis-cart	Function

ACI Application Workload Tags

Tag Selectors

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

ACI Application Workload Tags match vCenter Application Workload Tags

Automated conversion to “Application Centric”

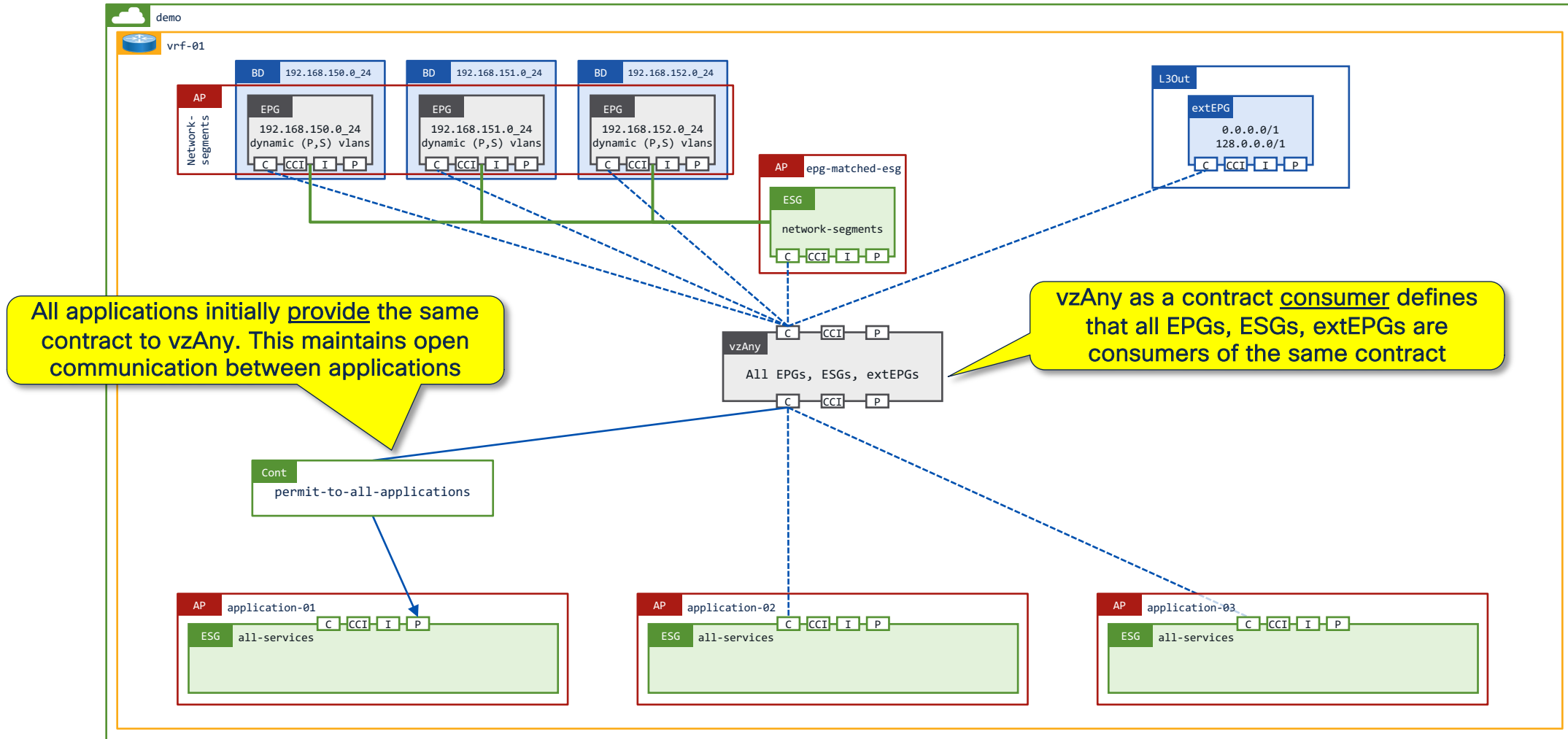
Endpoints mapped to the “network-segments” ESG through EPG → ESG mapping

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 192.168.152.101	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-
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-

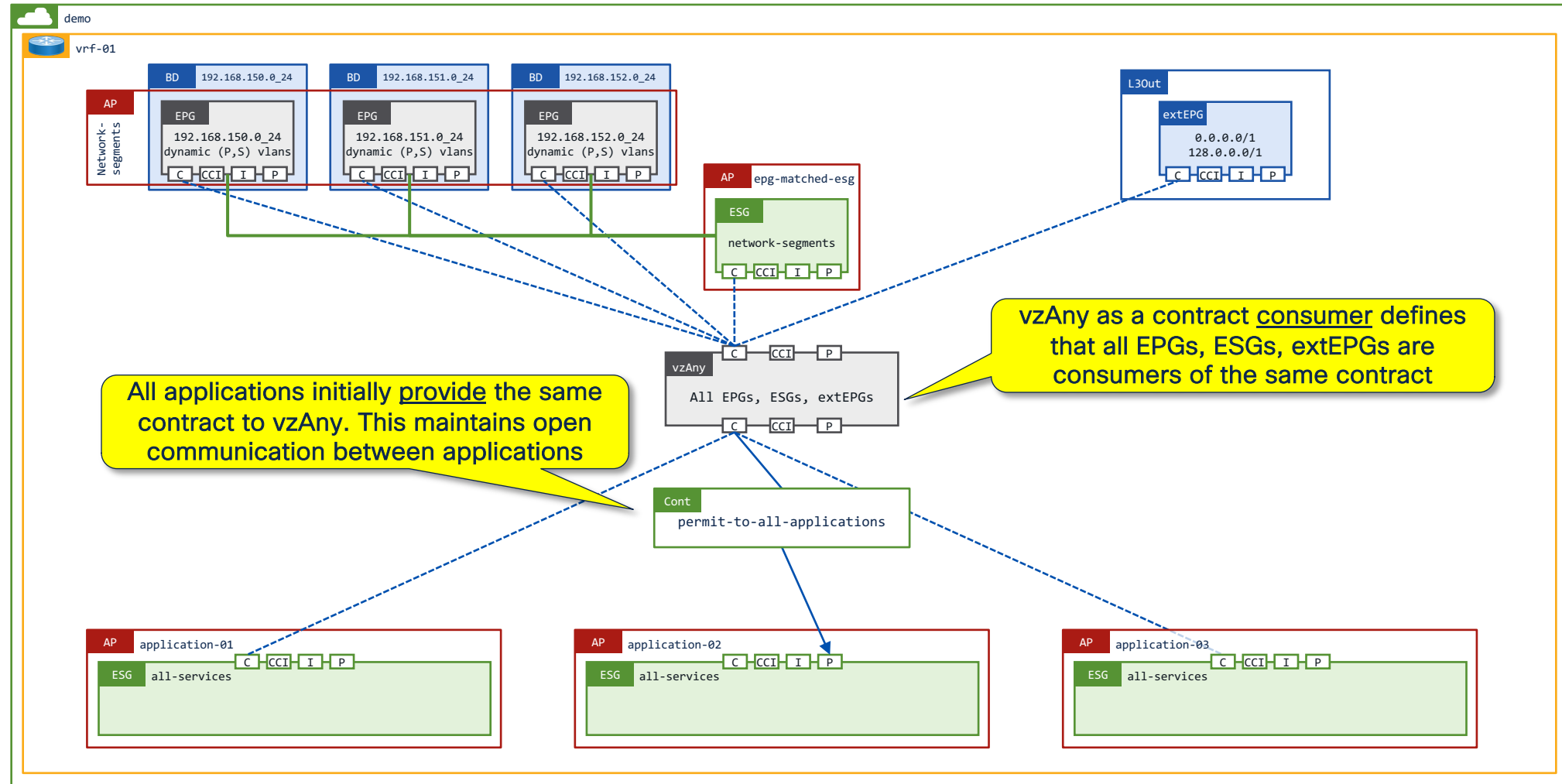
Page 1 Of 1 | Objects Per Page: 100 | Displaying Objects 1 - 11 Of 11

Scaling application connectivity with vzAny...

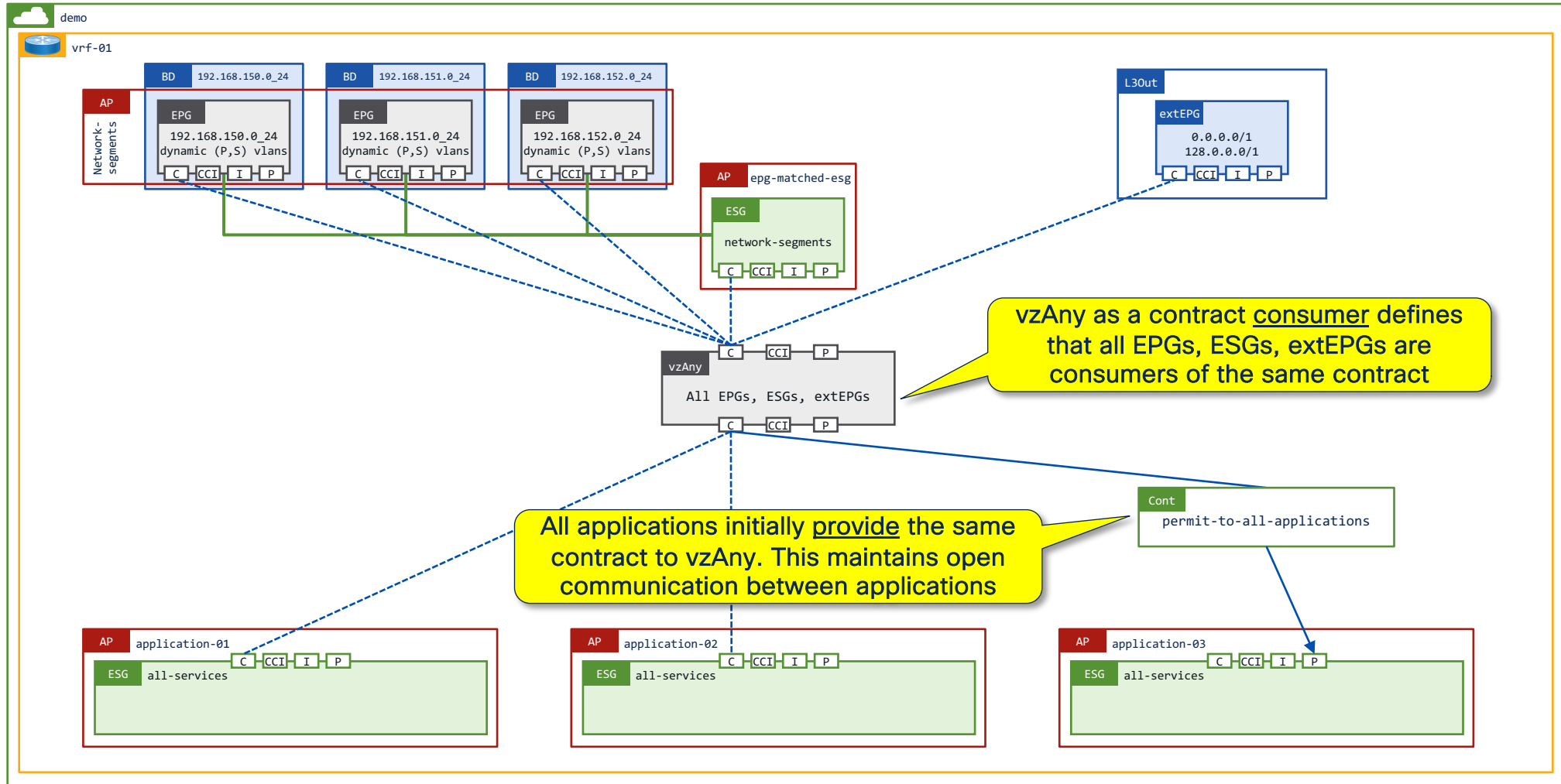
Scaling connectivity to “application-01”



Scaling connectivity to “application-02”



Scaling connectivity to “application-03”





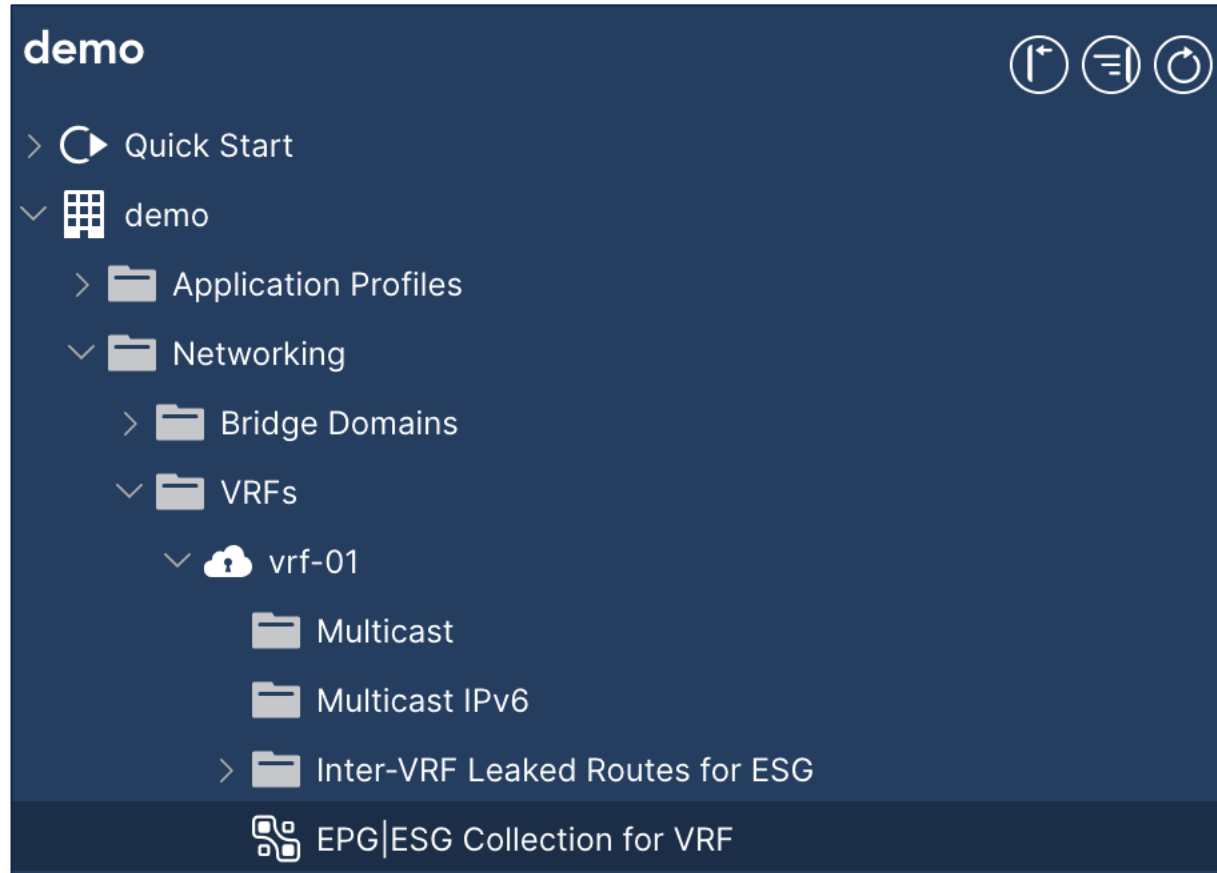
Allowing open communication in a
Brownfield environment...

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

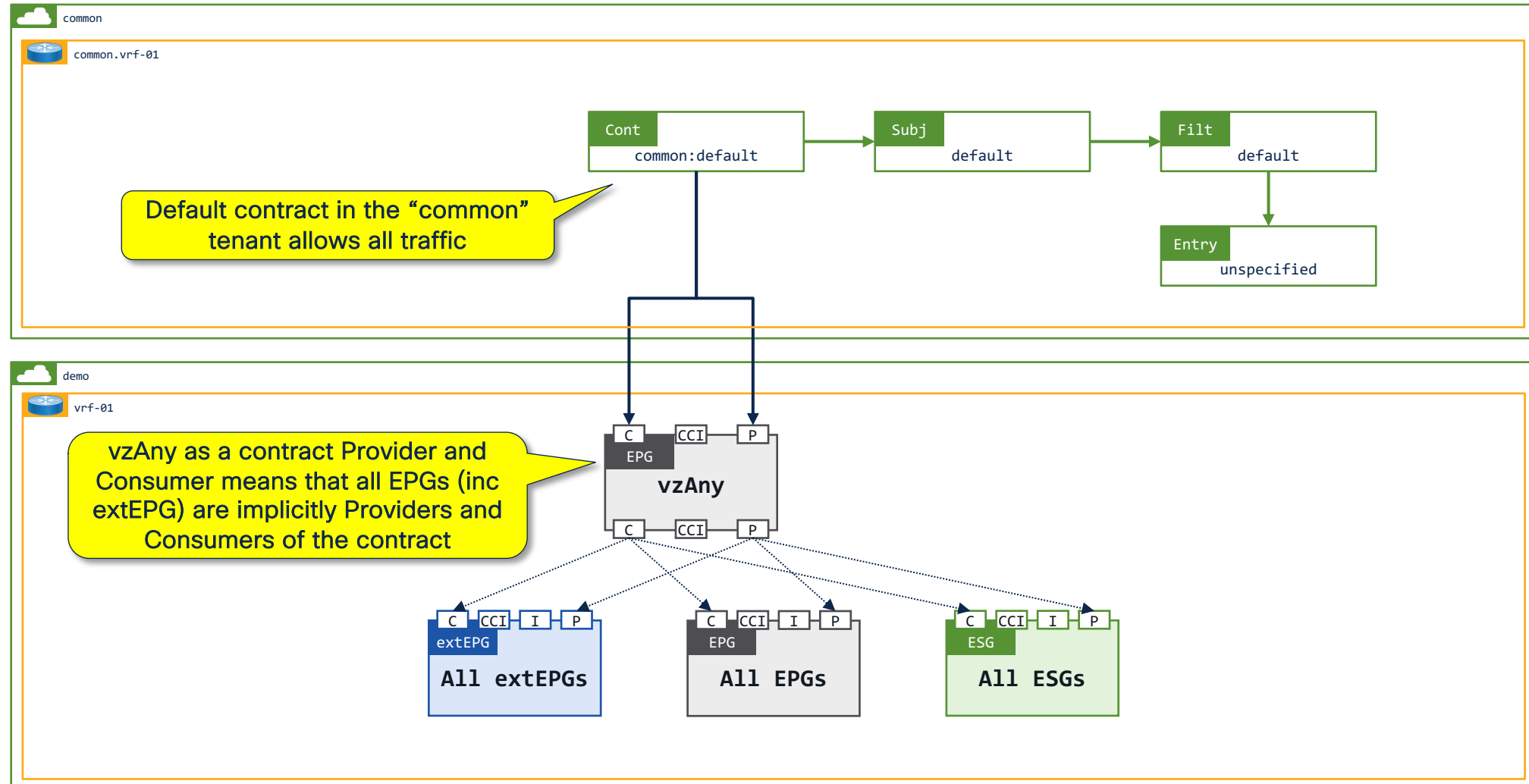


The great thing about vzAny provide/consume is that it allows open communication between all endpoints...

The “bad” thing about vzAny provide/consume is that it allows open communication between all endpoints...!

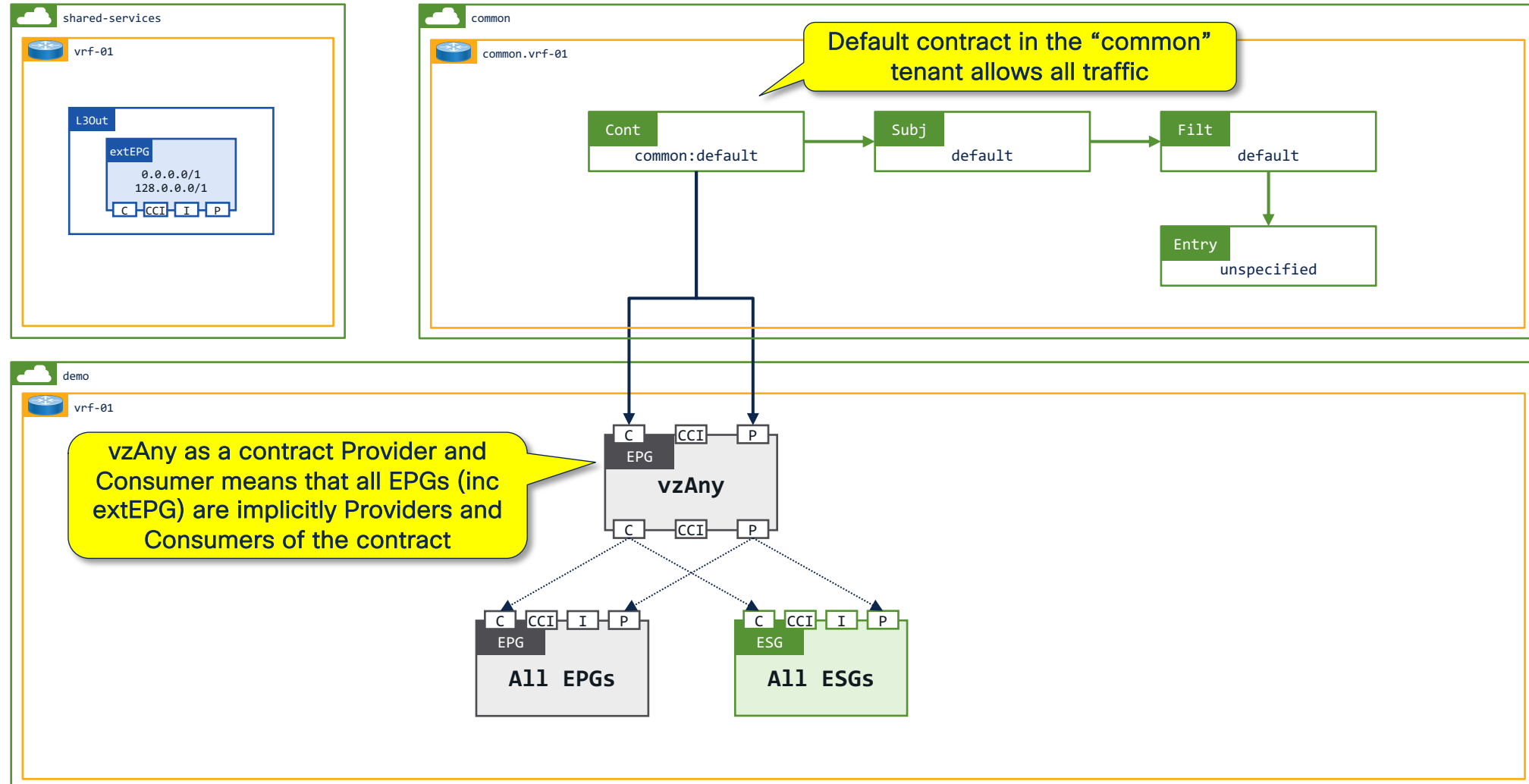
vzAny operation – consumer and provider

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

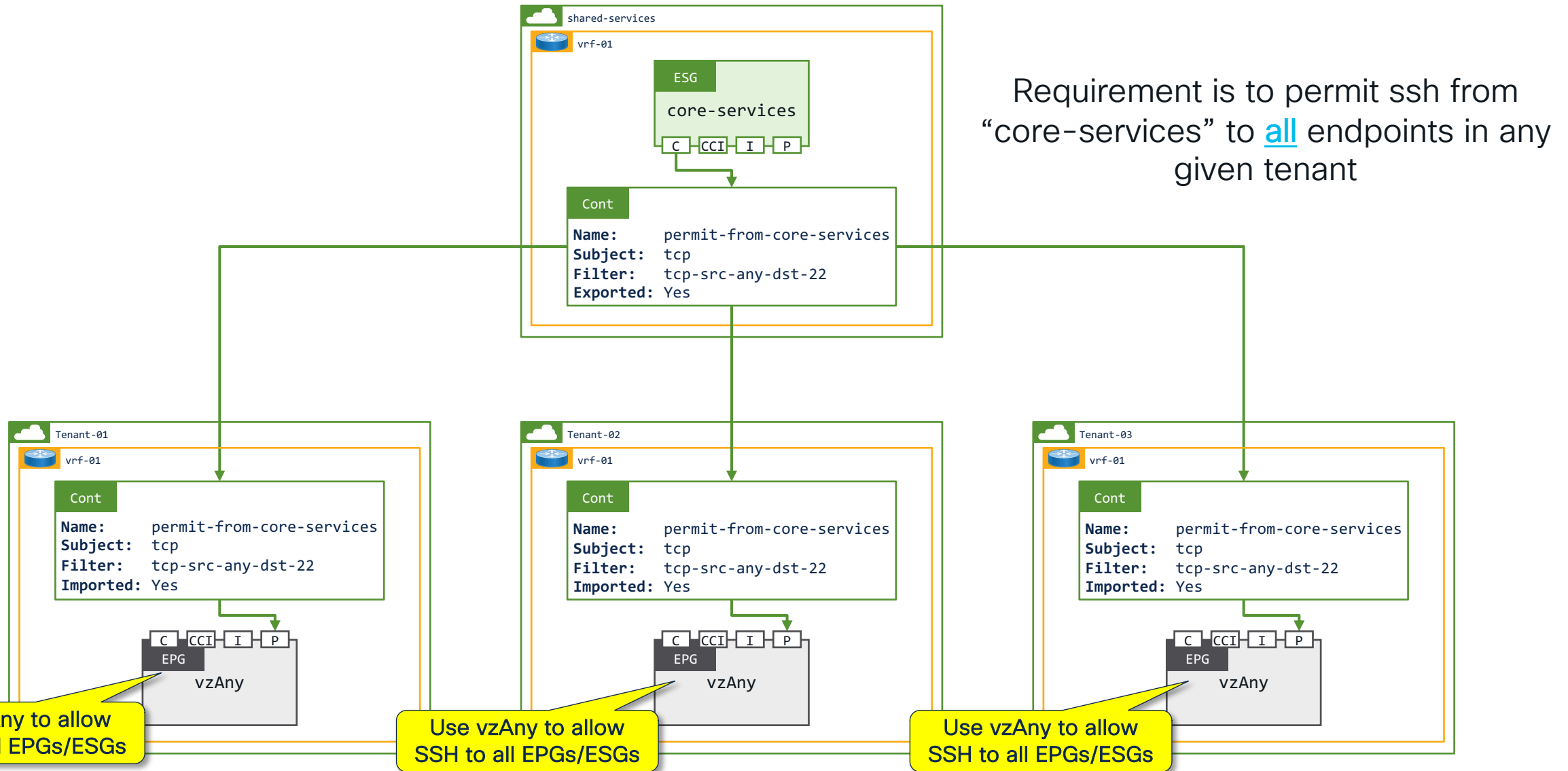


vzAny operation – consumer and provider

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

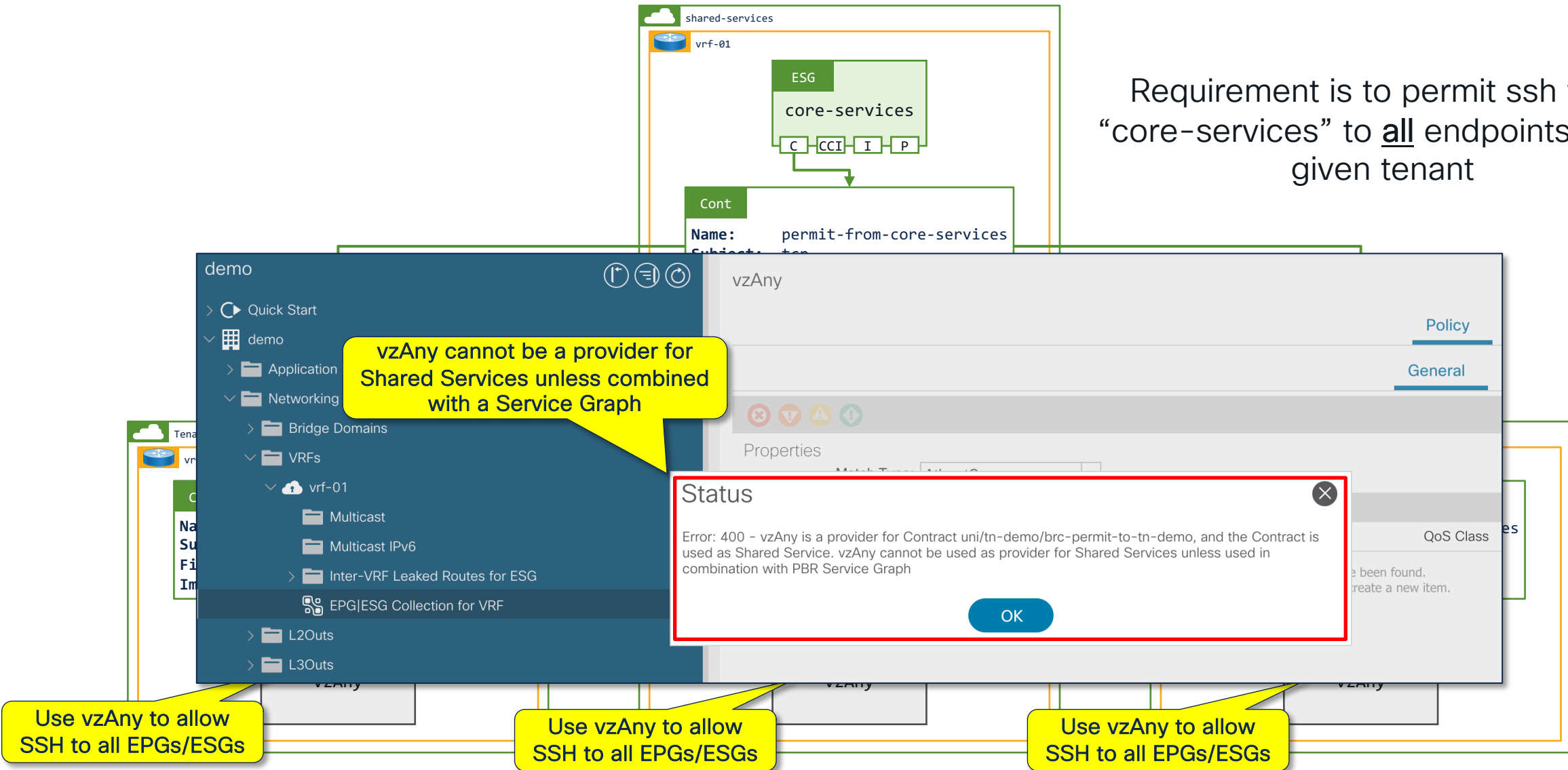


vzAny cannot be a Shared Service Provider



vzAny as a Shared Service Provider

Requirement is to permit ssh from “core-services” to all endpoints in any given tenant



vzAny can absolutely be your friend, but remember that vzAny contract relationships are applied to all EPGs, ESGs, extEPGs in the VRF...

Preferred Groups

Properties

Name: vrf-01

Alias:

Description: optional

Annotations:  Click to add a new annotation

Global Alias:

Routing Domain ID: 0

Segment: 2129922

Policy Control Enforcement Preference: Enforced Unenforced

Policy Control Enforcement Direction: Egress Ingress

BD Enforcement Status: ☐

Preferred Group: Disabled Enabled

BGP Timers: 

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

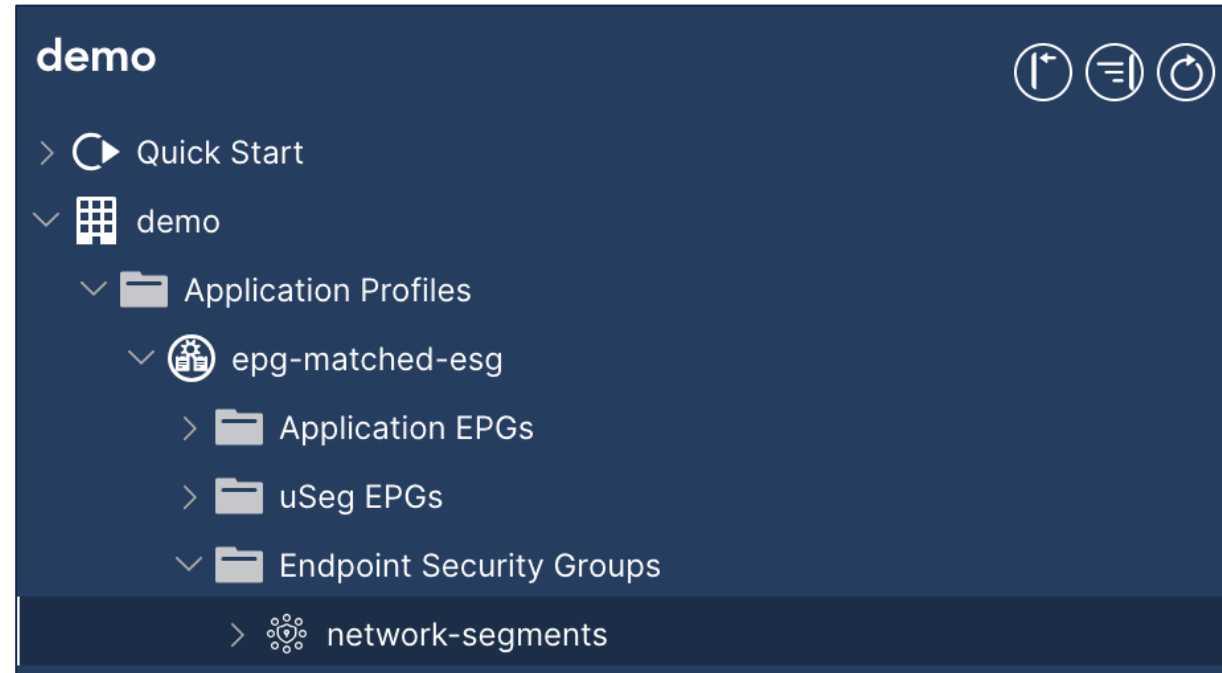
pcTag 16393

Include EPG in Preferred Group

There can only be one “Preferred Group” per VRF...

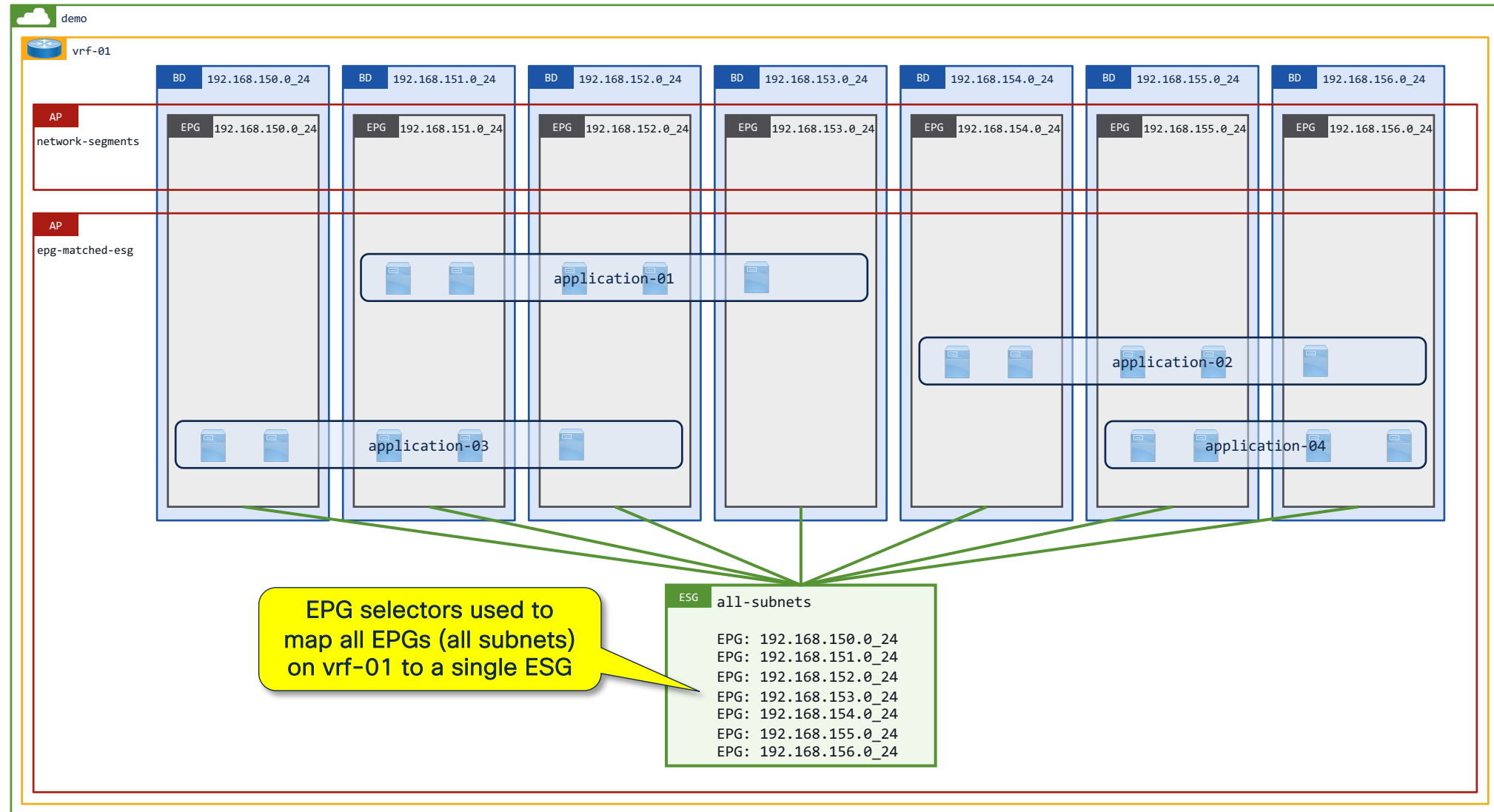
It is not possible to add Contract relationships to a
“Preferred Group”

EPG matched ESG



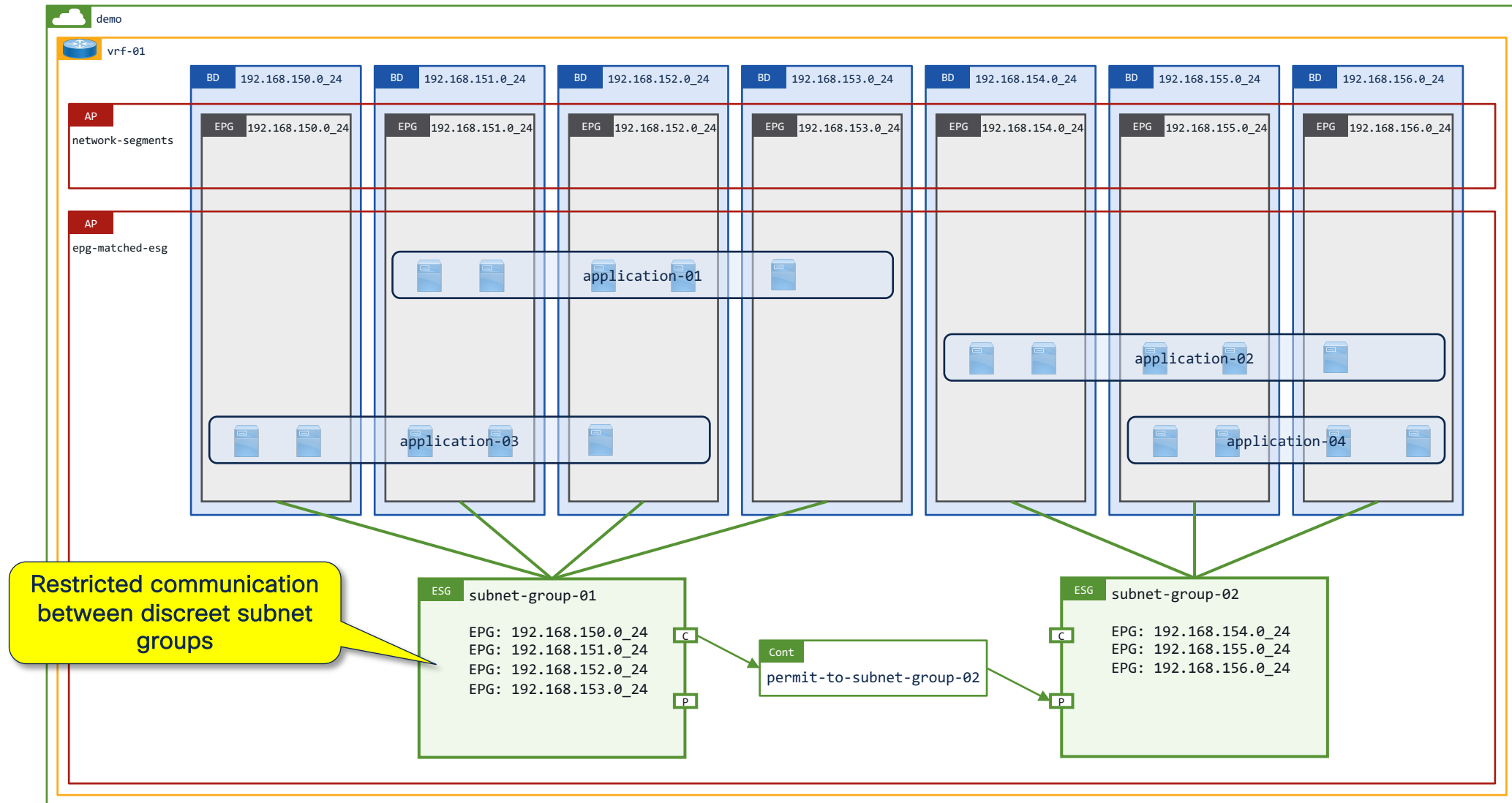
EPG to ESG Mapping

<https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-aci-esg-design-guide.html#FlexibleSecurityZoneswithESGs>



EPG to ESG Mapping

<https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-aci-esg-design-guide.html#FlexibleSecurityZoneswithESGs>



Benefits of EPG to ESG Mapping

- More flexible than using vzAny as it is applied to specific EPGs to create one or more security groups based on subnets/vlans*
- More secure than vzAny as EPG/ESG mapping **does not** include the extEPG – a contract is required for external communication
- More integrated than vzAny as supports provider function for Shared Services
- More flexible than Preferred Groups as you can multiple ESG groups vs a single preferred group
- More integrated than Preferred Groups as you can create a contract to the whole ESG

* Assumes 1:1 mapping between Bridge Domain and EPG. ESGs can mapping can also be performed on IP subnets

Let's step back and understand the impact of configuring EPG to ESG mapping...

Bridge Domain to EPG Mapping

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

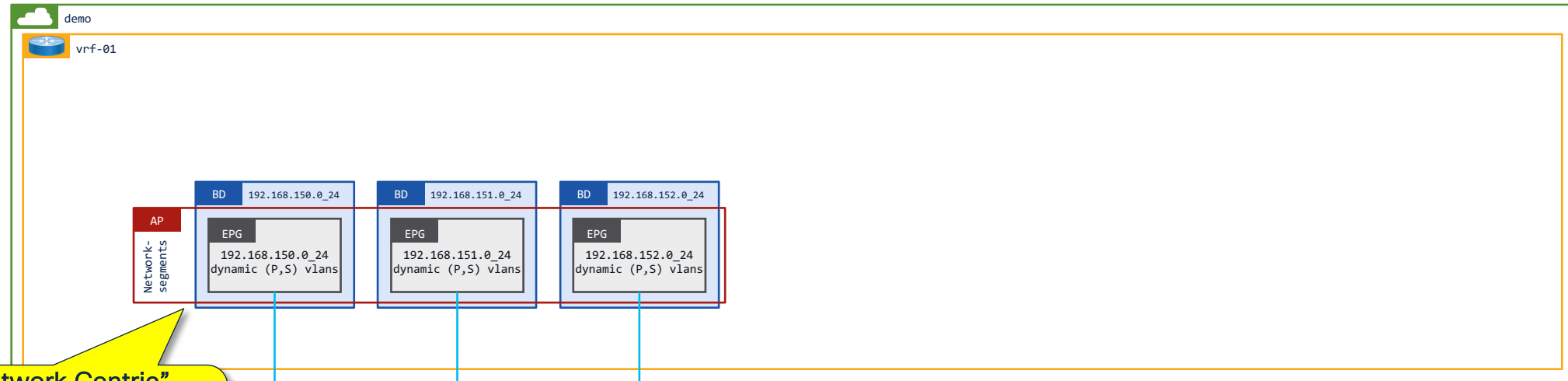
- demo
 - Application Profiles
 - network-segments
 - Application EPGs
 - 192.168.150.0_24
 - 192.168.151.0_24
 - 192.168.152.0_24
 - uSeg EPGs
 - Endpoint Security Groups
 - Networking
 - Bridge Domains
 - 192.168.150.0_24
 - 192.168.151.0_24
 - 192.168.152.0_24
 - VRFs
 - vrf-01
 - L2Outs
 - L3Outs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

The main content area shows the 'Application Profile - network-segments' configuration. The 'Topology' tab is selected, displaying a diagram with three EPGs (E) and three VMM domains (V). The EPGs are labeled '192.168.150.0_24 (network-segments)', '192.168.151.0_24 (network-segments)', and '192.168.152.0_24 (network-segments)'. The VMM domains are labeled 'V'. A yellow callout box points to the Bridge Domains in the left sidebar, stating 'Bridge Domain = EPG 1:1 mapping'. Another yellow callout box points to the VMM domains in the topology diagram, stating 'EPGs bound to VMM Domain'.

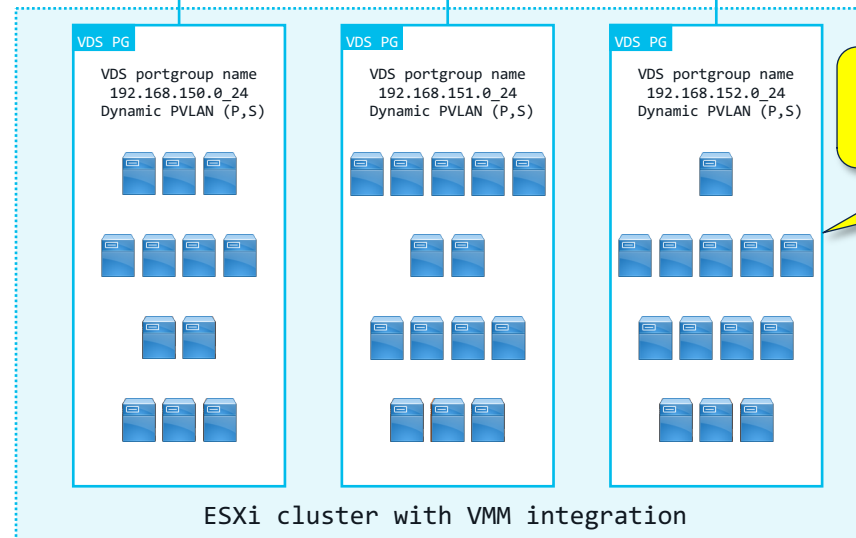
The right sidebar shows the 'Relation Indicators' section, which includes a legend for the following relations:

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

Initial state: Isolated groups of workloads



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



No communication between portgroup/subnets 192.168.150.0, 192.168.151.0 and 192.168.152.0

Each EPG has a unique security Tag (pcTag)

The screenshot shows the Cisco SD-WAN GUI for configuring an EPG. The left sidebar lists various configuration areas, with 'network-segments' selected. The main panel displays the 'Properties' for the EPG '192.168.150.0_24'. A yellow callout bubble points to the 'pcTag(sclass): 32771' field, which is highlighted with a red box. Other fields include 'Name: 192.168.150.0_24', 'Alias:', 'Description: optional', 'Annotations: + Click', 'Global Alias:', 'uSeg EPG: false', and 'Contract Exception Tag:'. The bottom section shows 'Preferred Group Member' with 'Exclude' and 'Include' buttons, 'Flood in Encapsulation' set to 'Disabled', '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', and 'EPG Contract Master: Application EPGs'.

The screenshot shows the Cisco SD-WAN GUI for configuring an EPG. The left sidebar lists various configuration areas, with 'network-segments' selected. The main panel displays the 'Properties' for the EPG '192.168.151.0_24'. A yellow callout bubble points to the 'pcTag(sclass): 49155' field, which is highlighted with a red box. Other fields include 'Name: 192.168.151.0_24', 'Alias:', 'Description: optional', 'Annotations: + Click', 'Global Alias:', 'uSeg EPG: false', and 'Contract Exception Tag:'. The bottom section shows 'Preferred Group Member' with 'Exclude' and 'Include' buttons, 'Flood in Encapsulation' set to 'Disabled', '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', and 'EPG Contract Master: Application EPGs'.

The screenshot shows the Cisco SD-WAN GUI for configuring an EPG. The left sidebar lists various configuration areas, with 'network-segments' selected. The main panel displays the 'Properties' for the EPG '192.168.152.0_24'. A yellow callout bubble points to the 'pcTag(sclass): 16390' field, which is highlighted with a red box. Other fields include 'Name: 192.168.152.0_24', 'Alias:', 'Description: optional', 'Annotations: + Click', 'Global Alias:', 'uSeg EPG: false', and 'Contract Exception Tag:'. The bottom section shows 'Preferred Group Member' with 'Exclude' and 'Include' buttons, 'Flood in Encapsulation' set to 'Disabled', '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', and '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 when there is an intermediary switching layer such as UCS FIs

Enabling ESG micro segmentation on a read/write VMM Domain implicitly enables PVLANS in the hypervisor to control East/West traffic...

Enabling ESG micro segmentation on a read/write VMM Domain also enables Proxy ARP and dynamic endpoint MAC Tagging...

PVLAN and MAC Tagging

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 1124

Details

Distributed switch ucsc-c220m5-vds-01

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 (1157, 1158)

Details

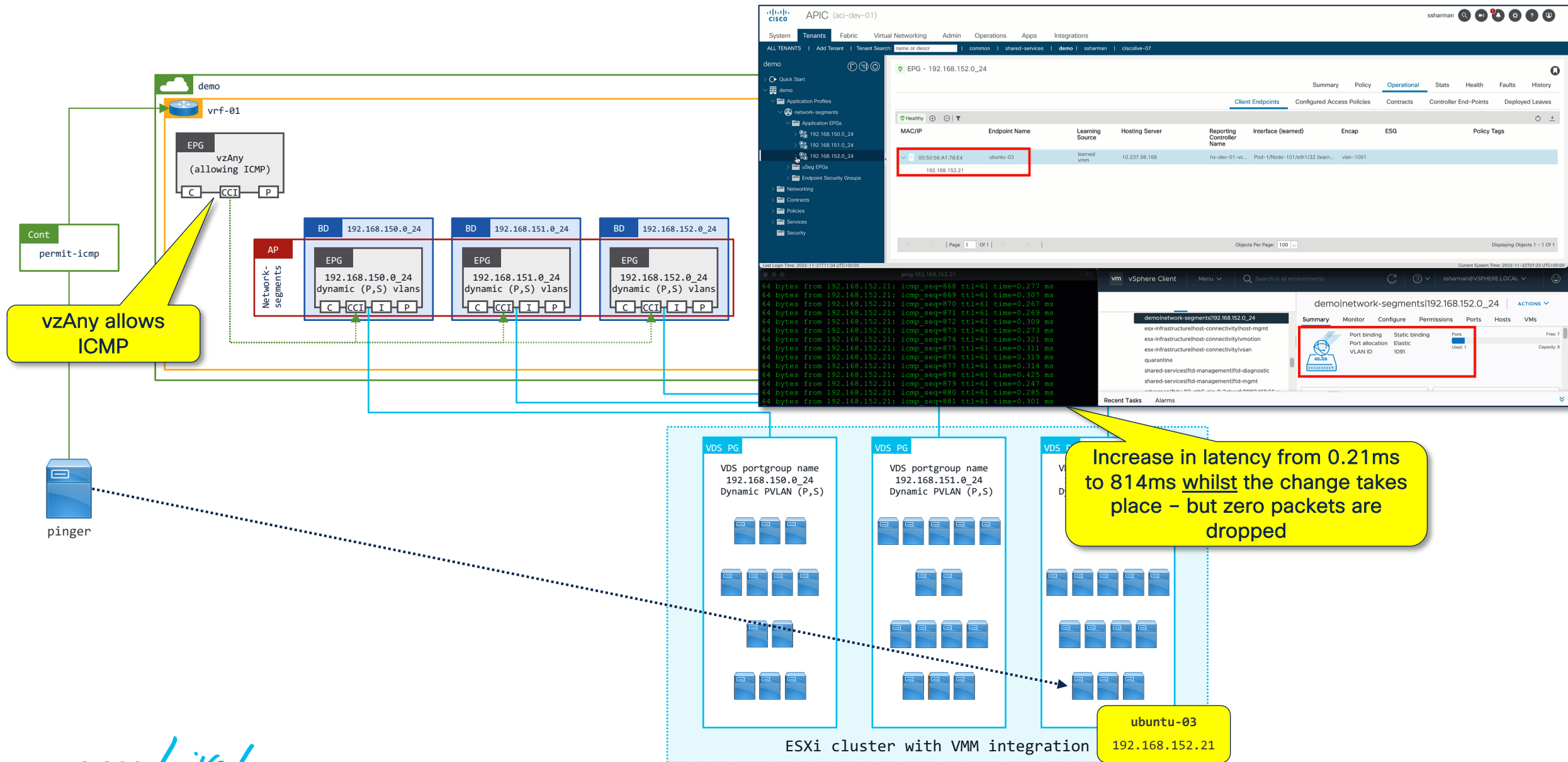
Distributed switch ucsc-c220m5-vds-01

Endpoint Tags

Endpoint MAC

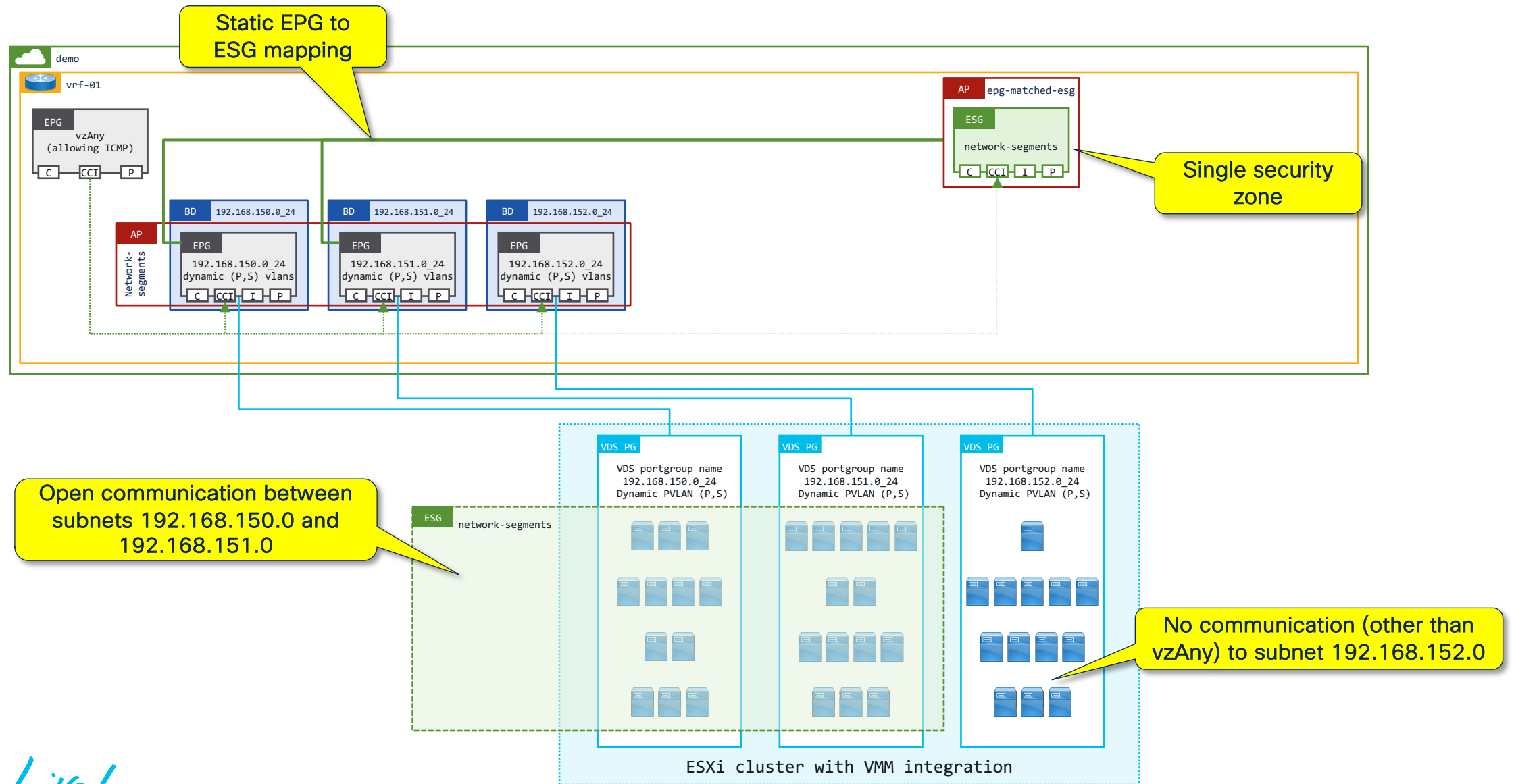
- 00:50:56:A1:1A:60 - 192.168.150.0_24 (VMM)
- 00:50:56:A1:3F:2C - 192.168.151.0_24 (VMM)
- 00:50:56:A1:7F:0B - 192.168.153.0_24 (VMM)
- 00:50:56:A1:7F:A5 - 192.168.156.0_24 (VMM)
- 00:50:56:A1:8E:DB - 192.168.154.0_24 (VMM)
- 00:50:56:A1:8F:09 - 192.168.153.0_24 (VMM)
- 00:50:56:A1:09:2F - 192.168.150.0_24 (VMM)
- 00:50:56:A1:22:DE - 192.168.152.0_24 (VMM)
- 00:50:56:A1:84:4D - 192.168.155.0_24 (VMM)
- 00:50:56:A1:B0:E2 - 192.168.151.0_24 (VMM)
- 00:50:56:A1:E9:20 - 192.168.154.0_24 (VMM)

What's the impact to traffic when we enable PVLANs...?



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

Create EPG matched Security Group



Create Application Profile for Security Groups

APIC (aci-dev-01)

System Tenants Fabric Virtual Networking Admin Operations Apps Integrations

ALL TENANTS | Add Tenant | Tenant Search: name or descr | common | demo | ssharman | ciscolive-07 | ciscolive-08

demo

Application Profiles

Create Application Profile

Create Application Profile

Name: epg-matched-security-groups

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

APIC (aci-dev-01)

System | **Tenants** | Fabric | Virtual Networking | Admin | Operations | Apps | Integrations

ALL TENANTS | Add Tenant | Tenant Search: name or descr | common | **demo** | cisco1ve-07 | cisco1ve-08 | ssharman

demo

Quick Start

demo

Application Profiles

network-segments

Contracts

Policies

Services

Security

Create Application EPG

Create uSeg EPG

Create Endpoint Security Group

Delete

Clone Application Profile

Save as ...

Post ...

Share

Open In Object Store Browser

domains

Application Profiles

Endpoint Security Groups

0 Total

0 Total

Create Endpoint Security Group

STEP 1 > Identity

1. Identity 2. Selectors 3. Advanced (Optional)

Name: network-segments

Description: optional

VRF: select a value

ESG Admin State: vrf-01 demo

common.vrf-01 common

copy common

default common

Create VRF

Create Endpoint Security Group

STEP 2 > Selectors

1. Identity 2. Selectors 3. Advanced (Optional)

Tag Selectors:

Tag Key	Value Operator	Tag Value	Description
---------	----------------	-----------	-------------

EPG Selectors:

EPG	Description
-----	-------------

IP Subnet Selectors:

IP Subnet	Description
-----------	-------------

Previous Cancel Next

Create an EPG Selector

EPGs In ESG VRF:

Name
☒ uni/tn-demo/ap-network-segments/epg-192.168.150.0_24
☒ uni/tn-demo/ap-network-segments/epg-192.168.151.0_24
☐ uni/tn-demo/ap-network-segments/epg-192.168.152.0_24

Description: optional

Cancel OK

Create Endpoint Security Group

STEP 3 > Advanced (Optional)

1. Identity 2. Selectors 3. Advanced (Optional)

Intra ESG Isolation: Enforced Unenforced

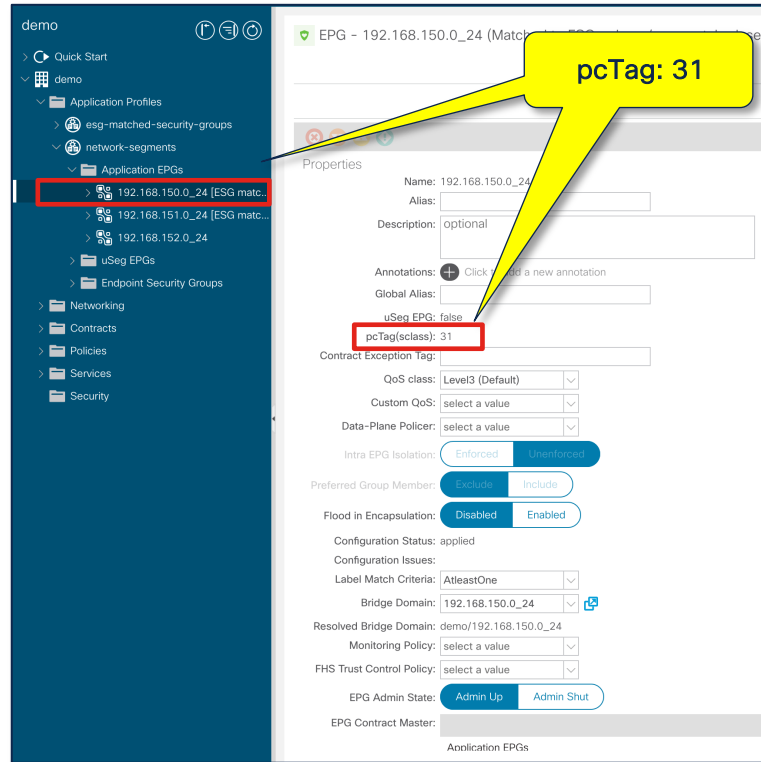
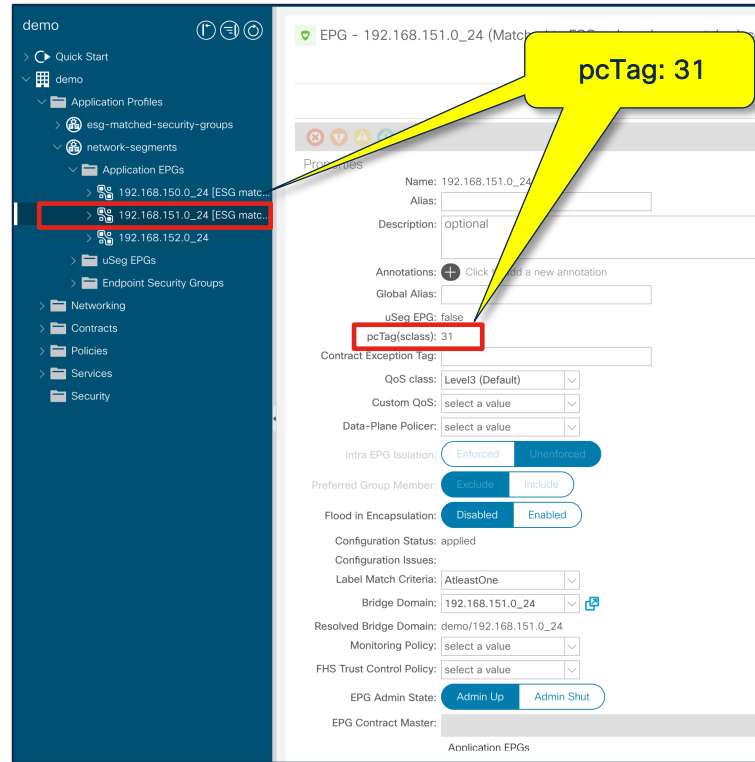
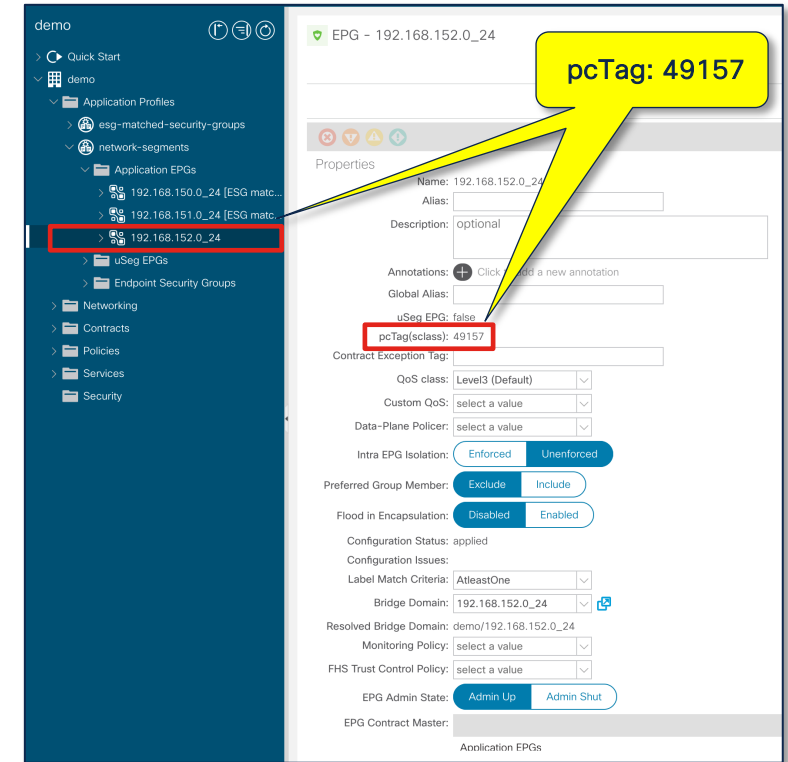
Preferred Group Member: Exclude Include

ESG Contract Master:

ESGs

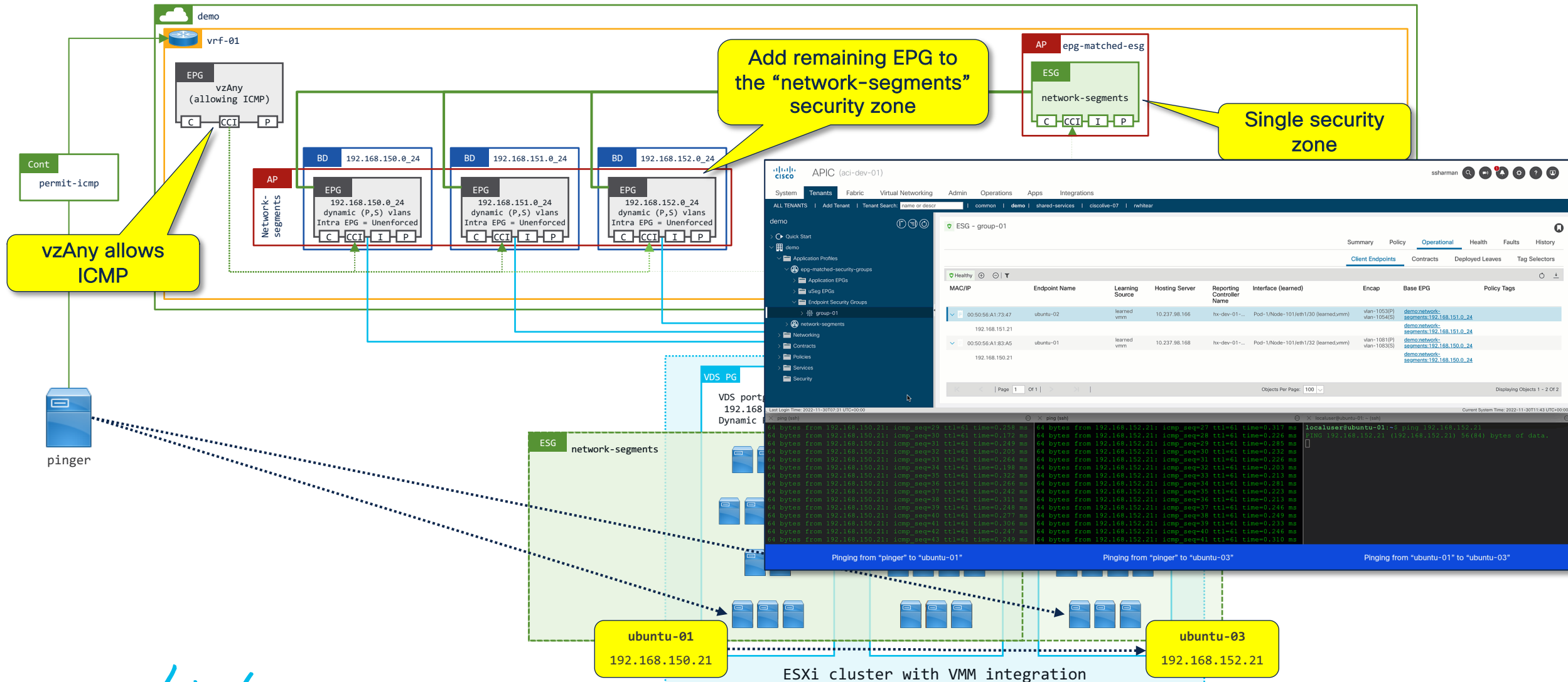
Previous Cancel Finish

Matched EPGs now classified with a common pcTag

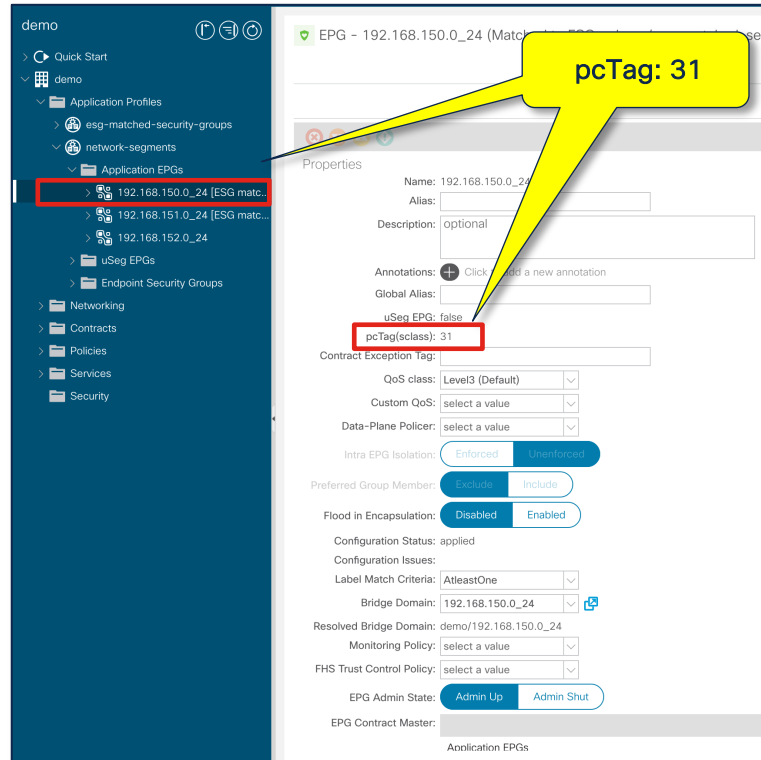
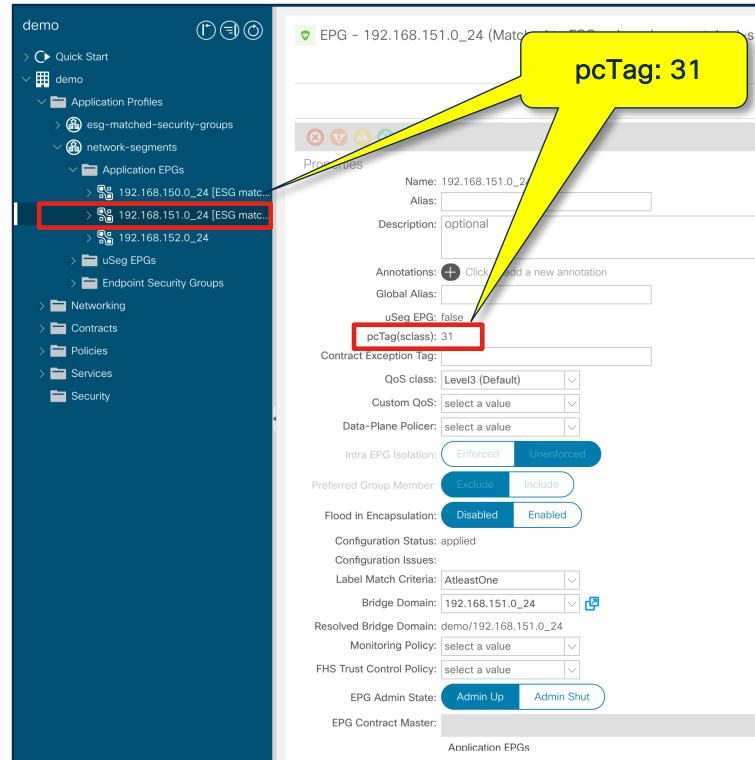
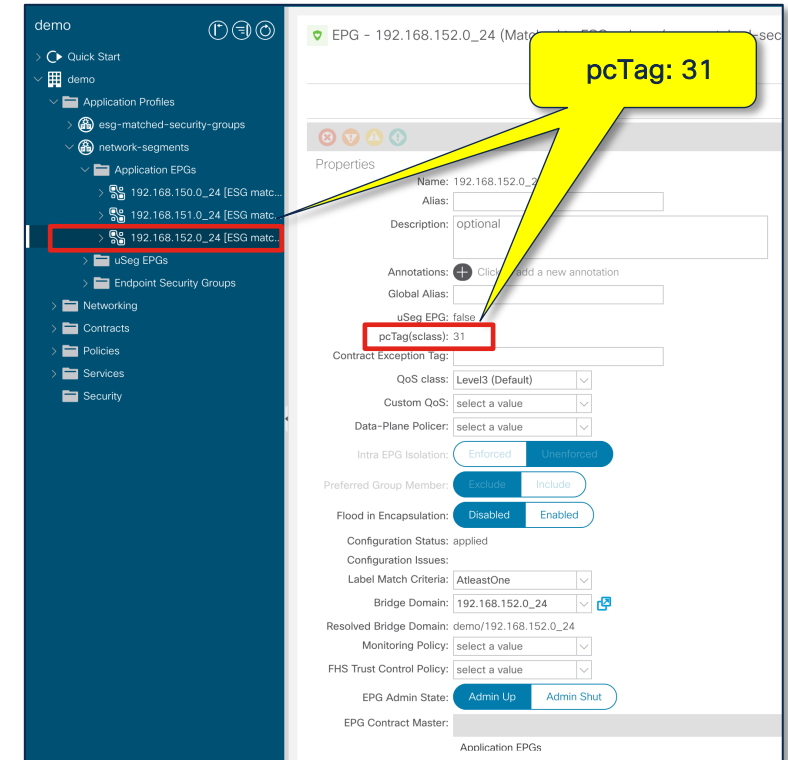


Let's consider any impact to traffic when adding the remaining EPG to the Security Group...

Add remaining EPG to Single Security Zone

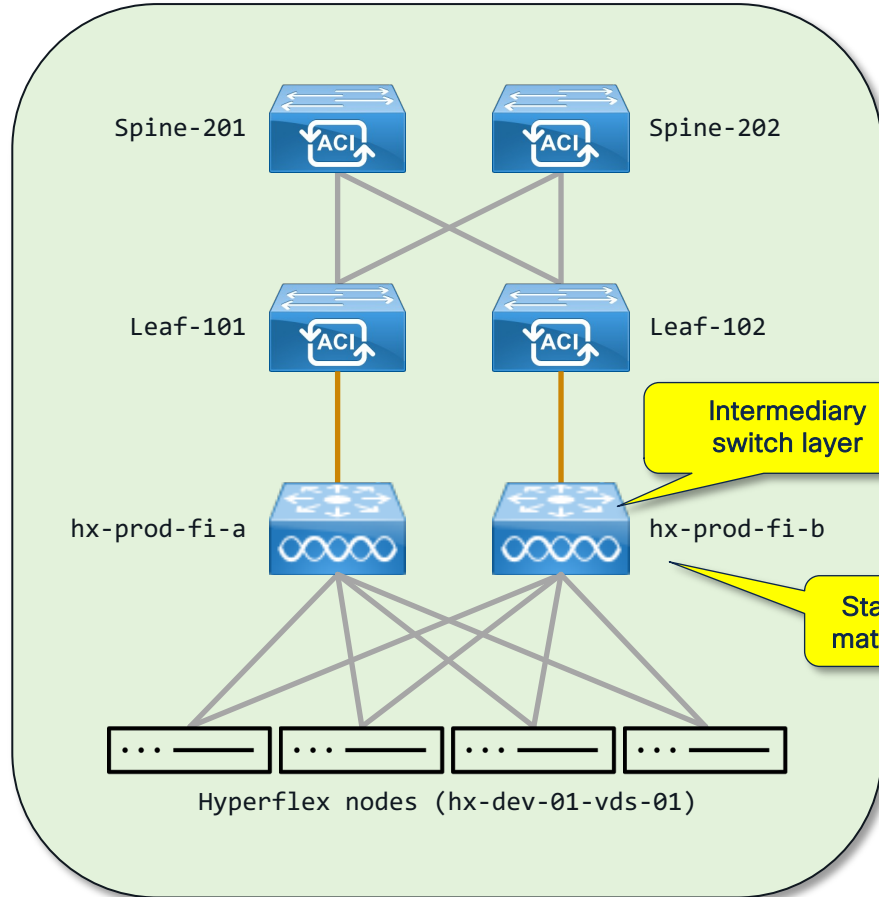


All EPGs now classified with a common pcTag



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

Define static PVLANS for VMM Domains



Inventory | Fabric Policies | Access Policies

Policies

- Quick Start
- Interface Configuration
- Switch Configuration
- Switches
- Modules
- Interfaces
- Policies
- Physical and External Domains
- Pools
- VLAN
 - external-switches (Static Allocation)
 - fabric-inband-mgmt (Static Allocation)
 - hx-dev-01-vds-01 (Dynamic Allocation)

UCS Manager

LAN / LAN Cloud / VLANs

Add PVLANS to UCSM

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

Name: hx-dev-01-vds-01
Description: optional

Mode: Dynamic Allocation

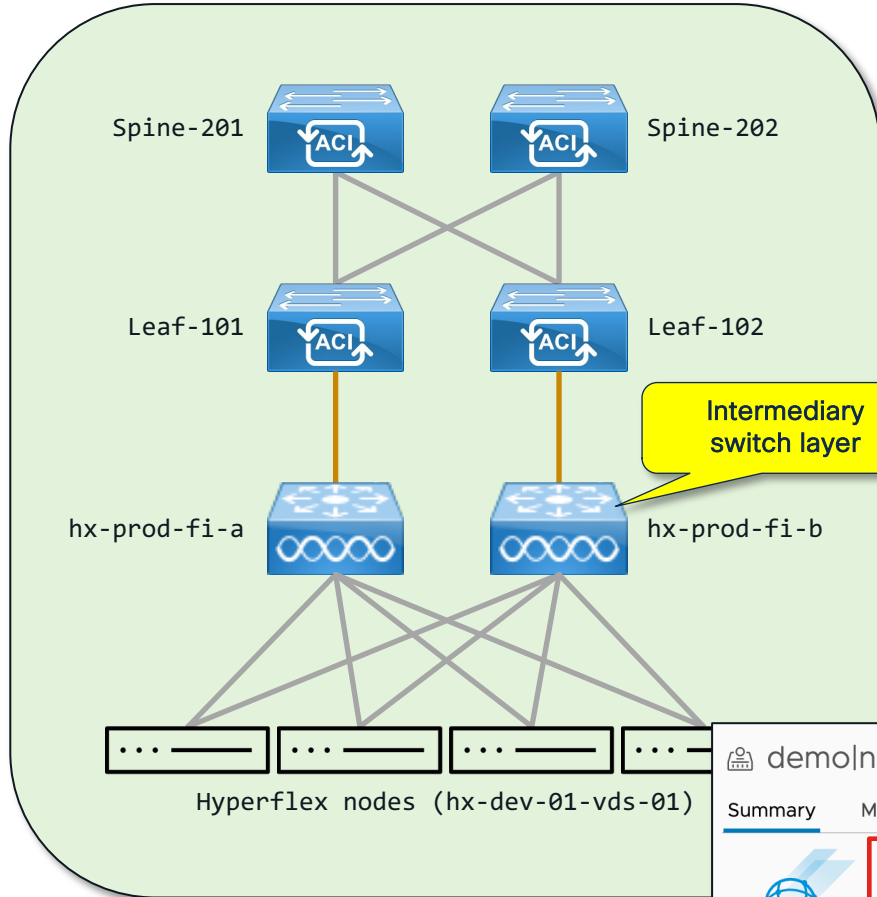
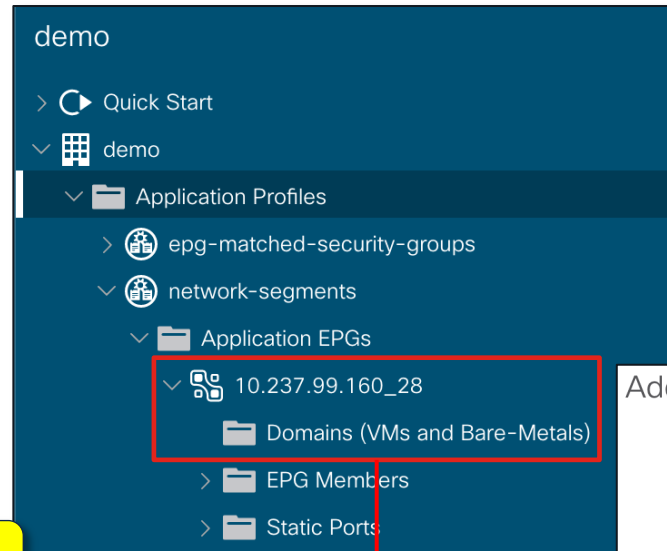
VLAN Range	Description	Allocation Mode	Role
[1217-1218]	primary/secondary PVLANS	Static Allocation	External or On the wire encapsulations
[1219-1220]	primary/secondary PVLANS	Static Allocation	External or On the wire encapsulations
[1221-1222]	primary/secondary PVLANS	Static Allocation	External or On the wire encapsulations

Domains:

Name	Type
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:

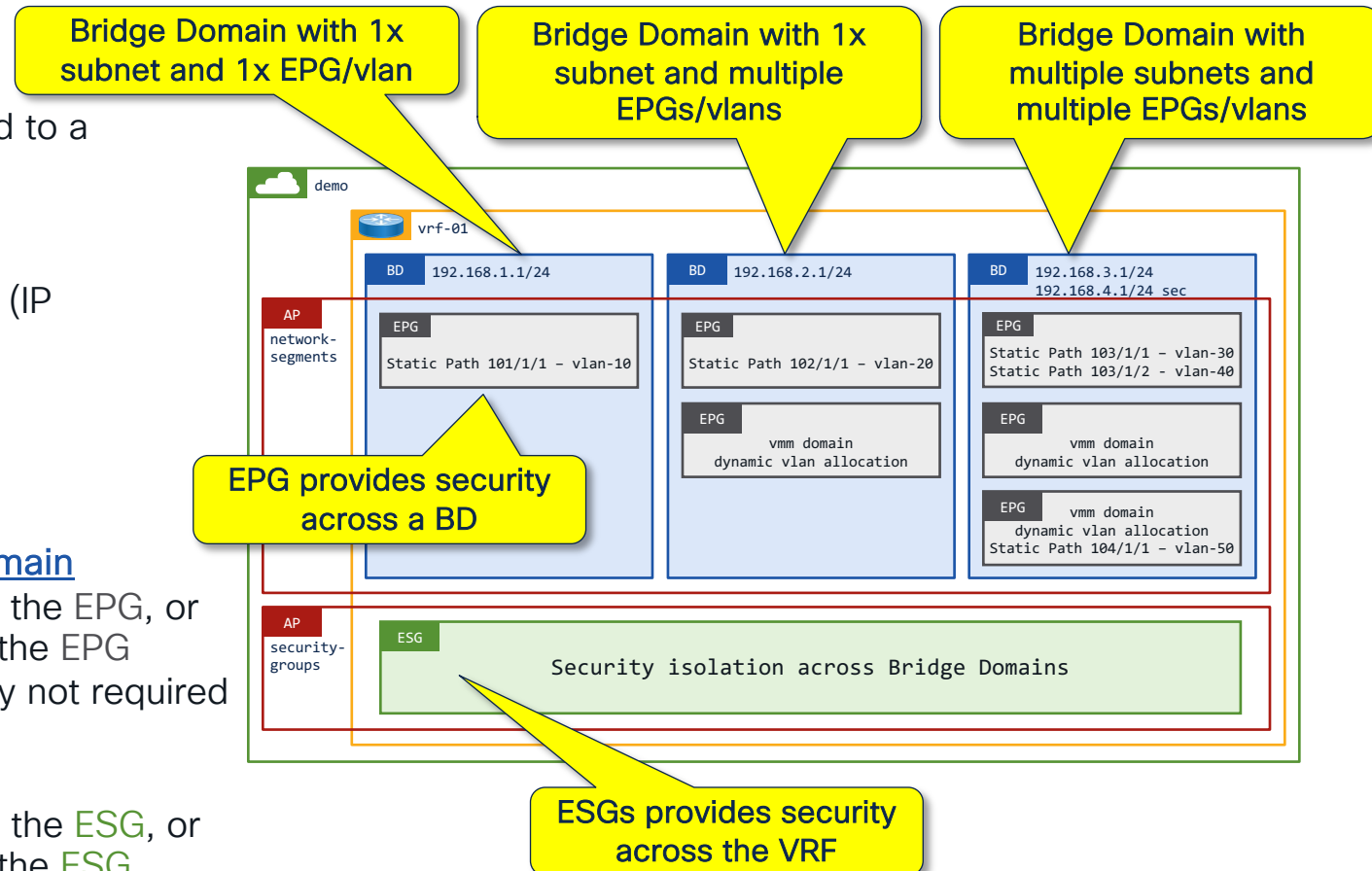
demo network-segments 10.237.99.160_28		ACTIONS	
Summary		Monitor	Configure
	Port binding	Static binding	
	Port allocation	Elastic	
	Private VLAN	Isolated (1217, 1218)	

Security within a VRF using ESGs

EPG Security vs ESG Security

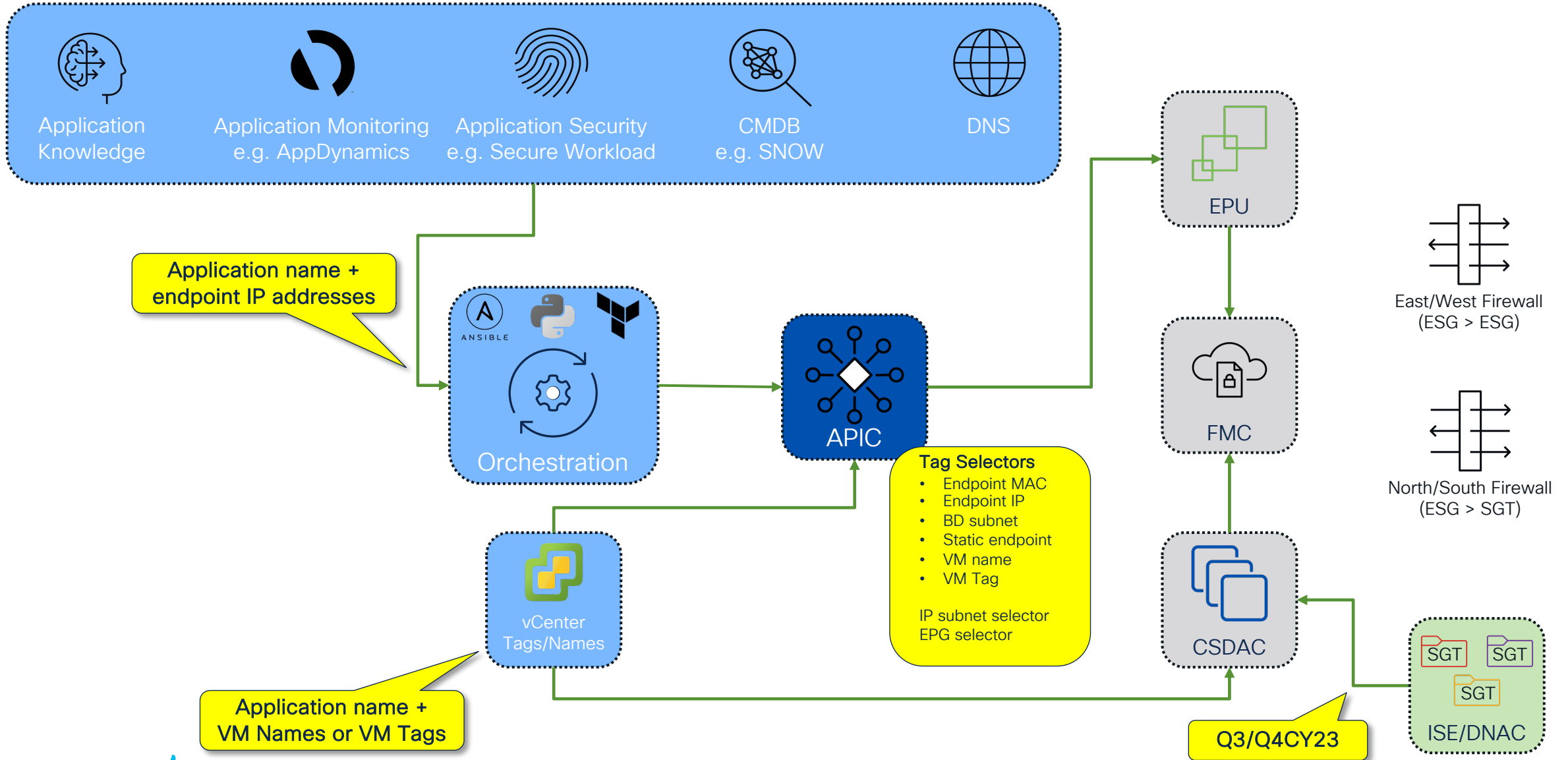
ACI foundational building blocks:

- 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



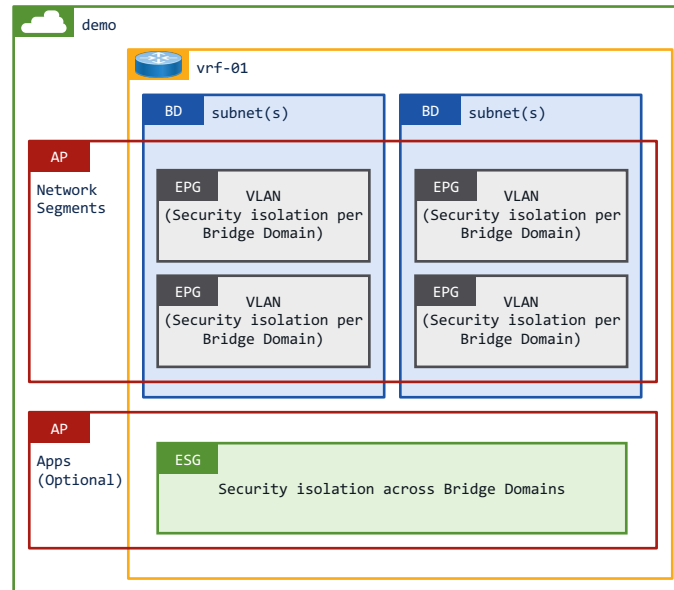
How do you map Endpoints into an ESG...?

Application Knowledge taken from any source

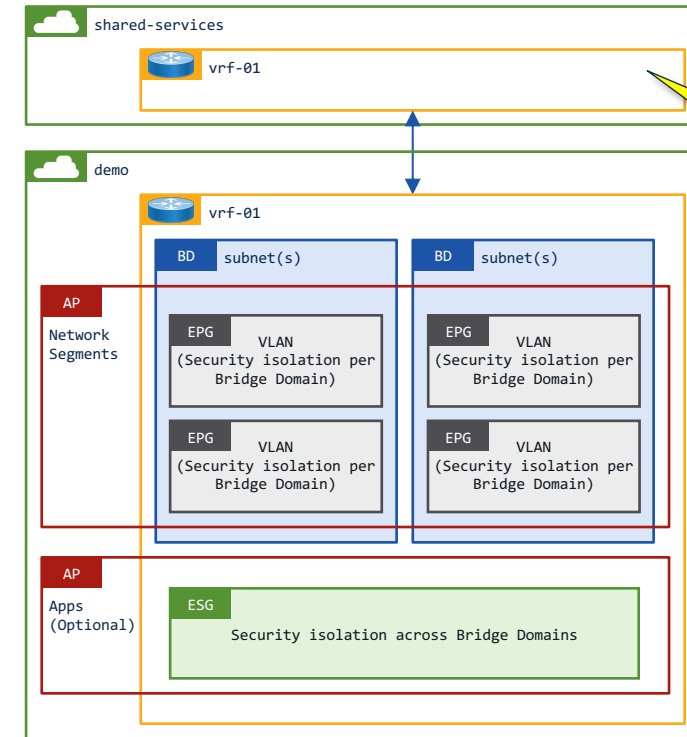


Select a Design Pattern and map your Endpoints to the ESG...

Design Patterns

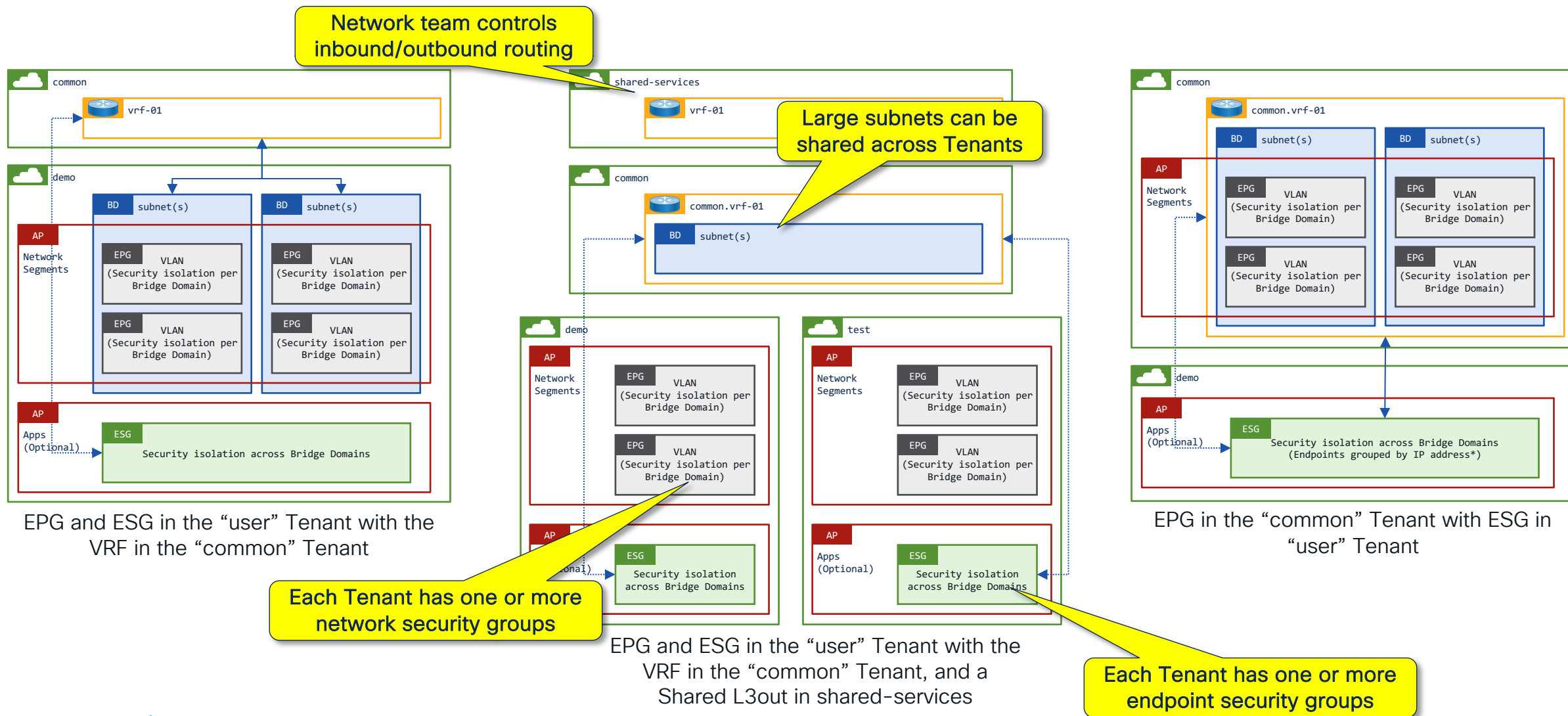


EPG and ESG in the "user" Tenant with a dedicated L3out



EPG and ESG in the "user" Tenant with a Shared L3out

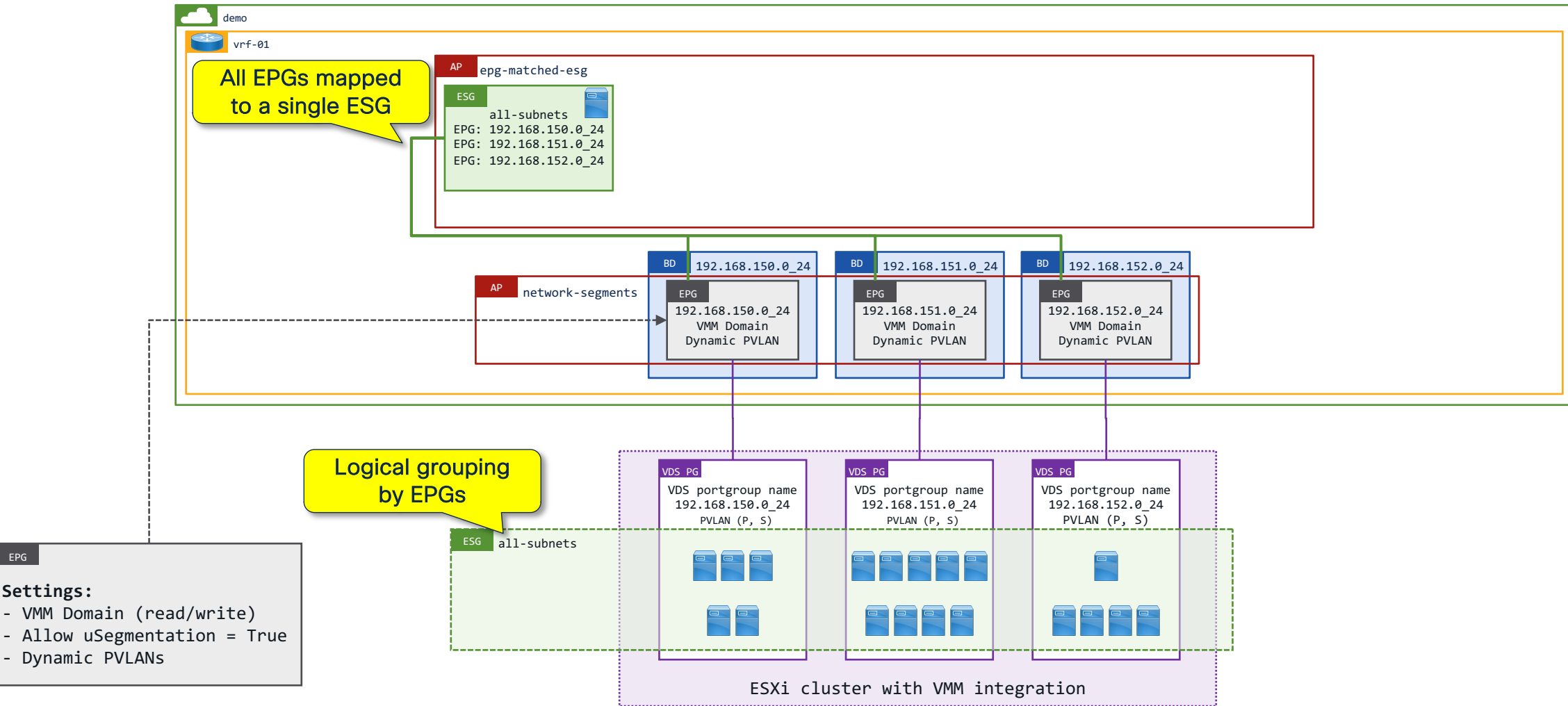
Design Patterns



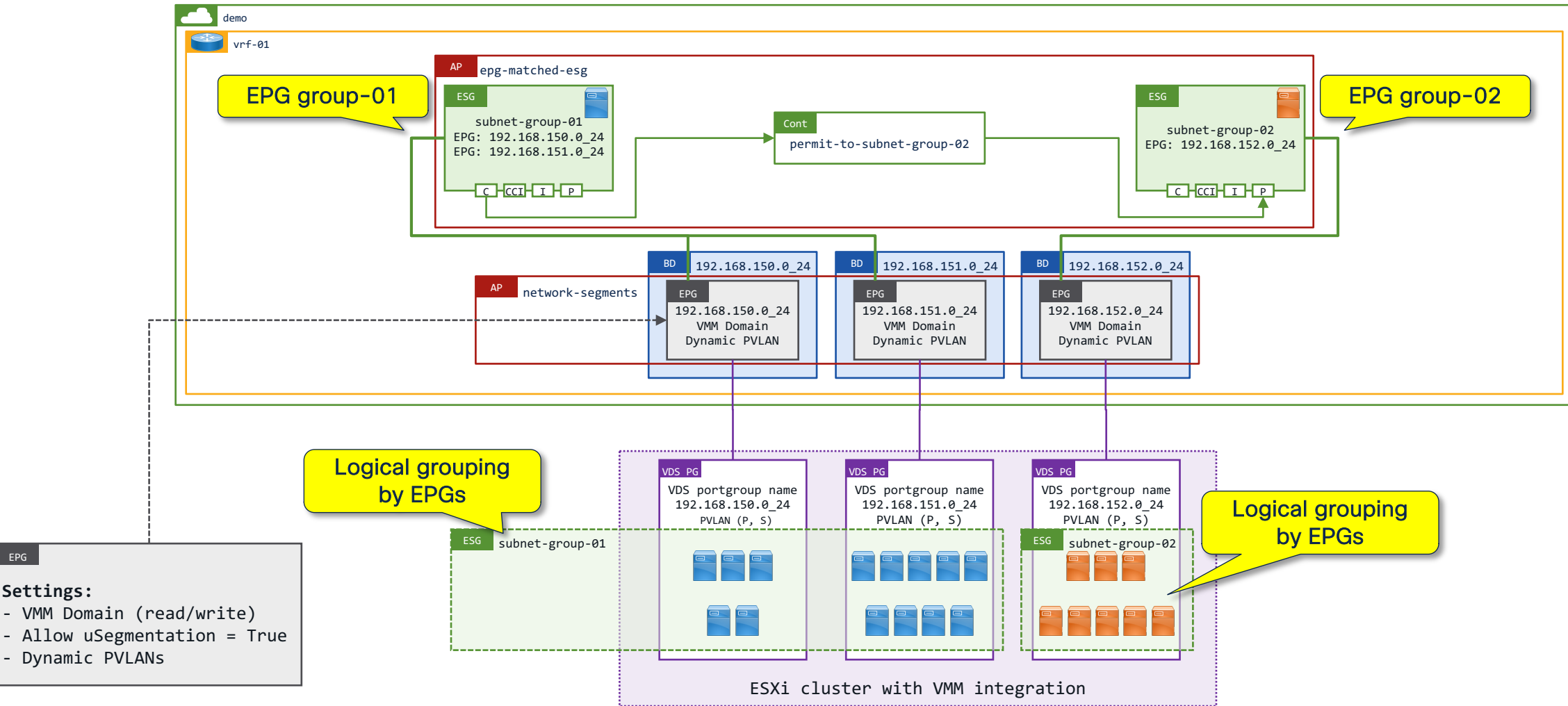
What are our mapping options...?

We can use EPGs, Tagged endpoints, Tagged subnets, or simply Static endpoint mapping...

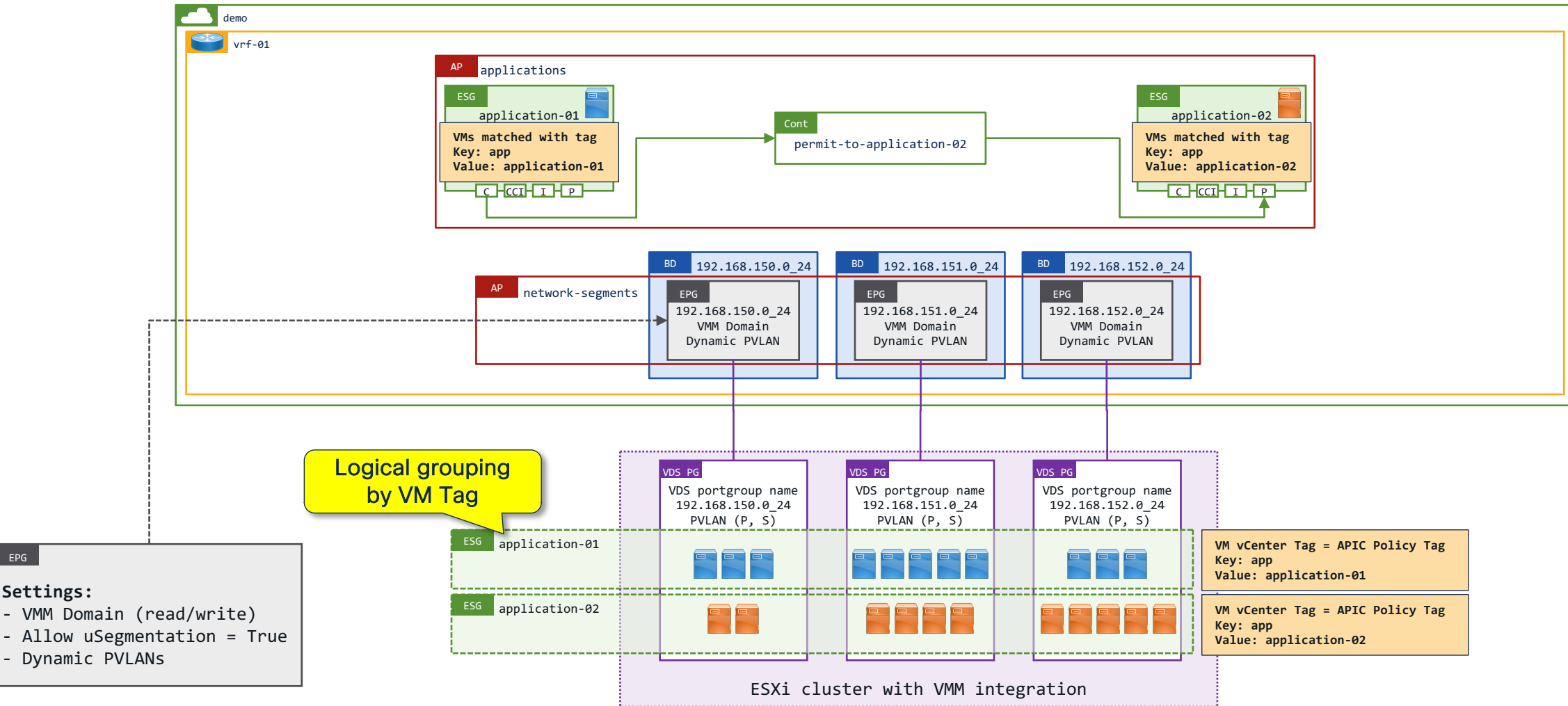
Option 1: EPG mapping to a single security zone



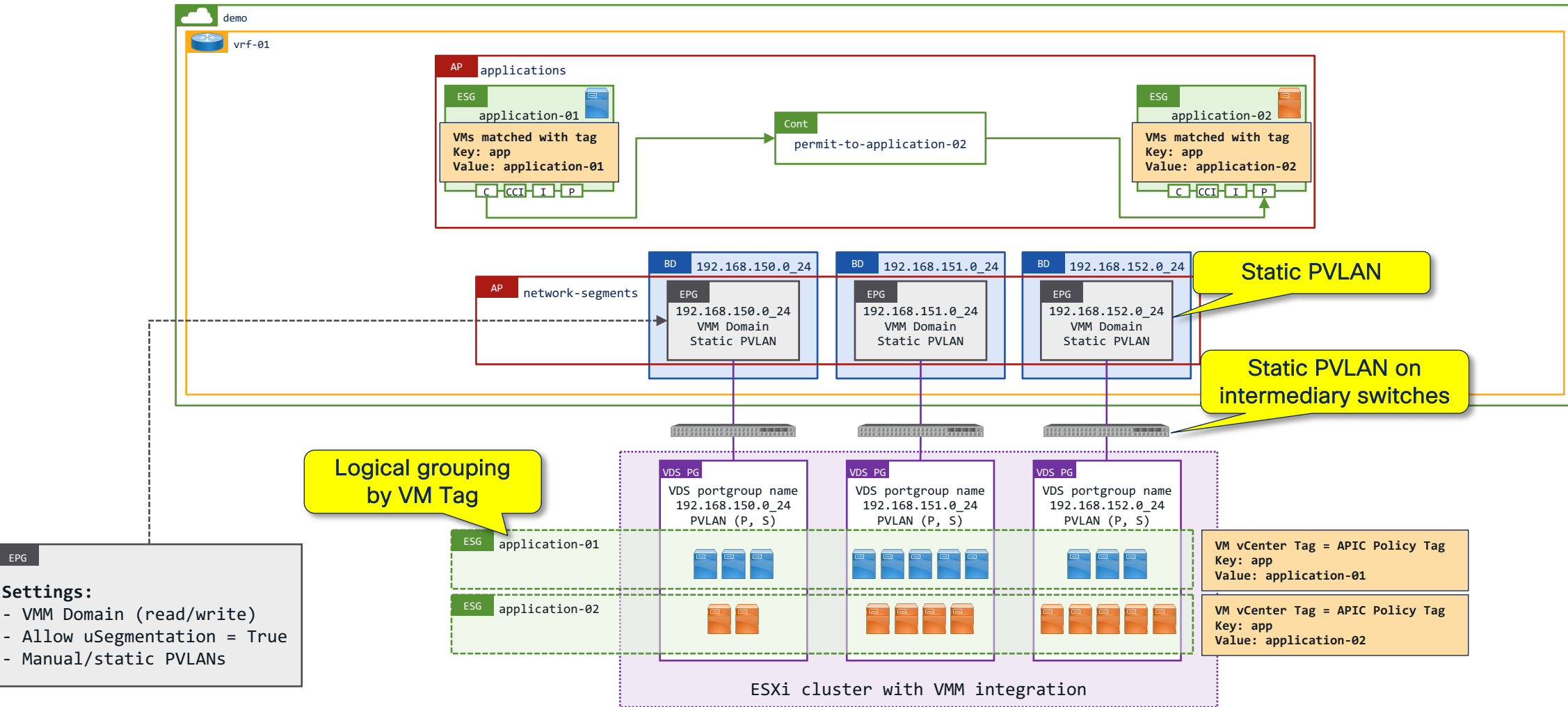
Option 2: EPG mapping for multiple security zones



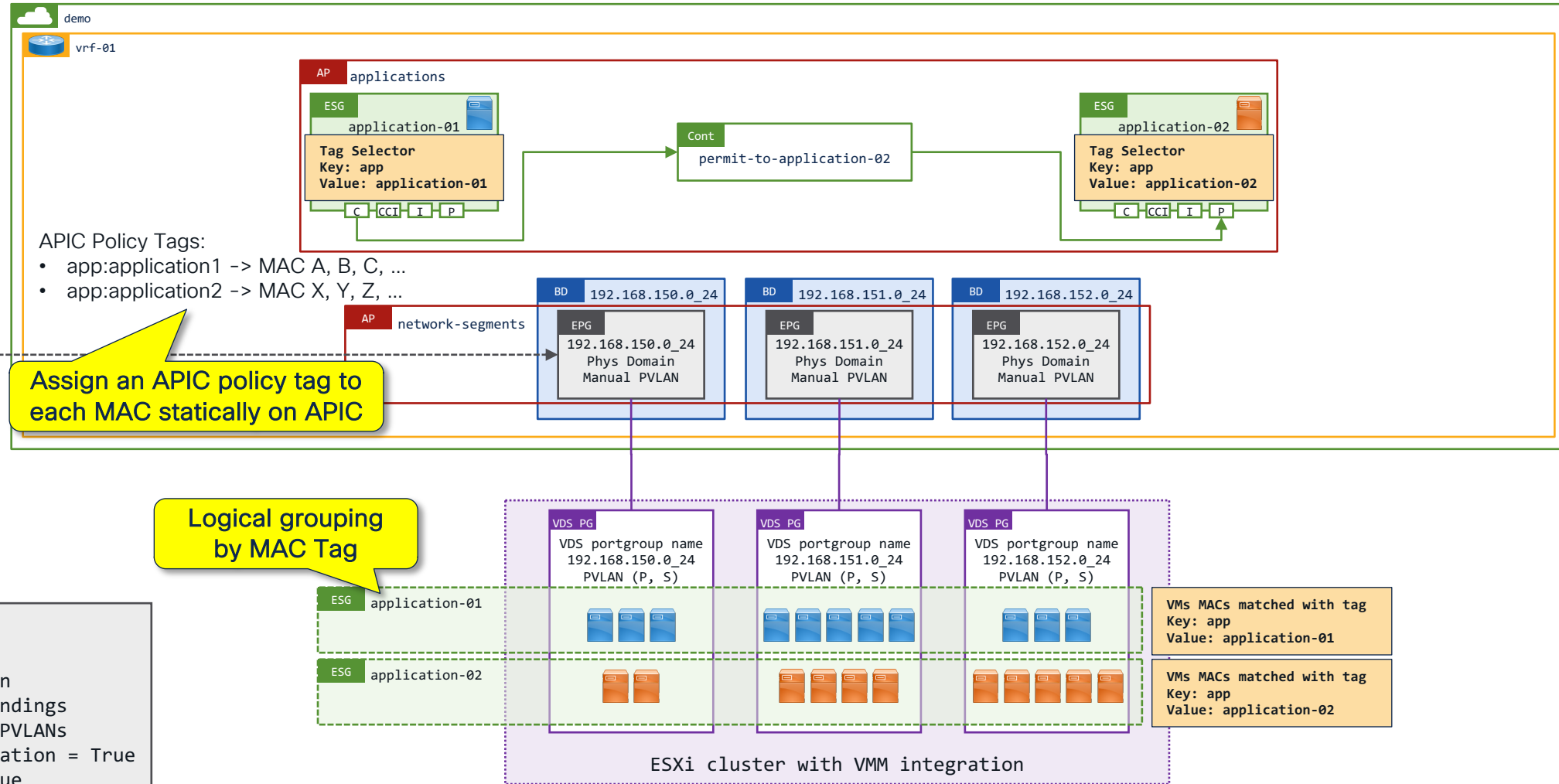
Option 3: Tag selectors with VMM integration



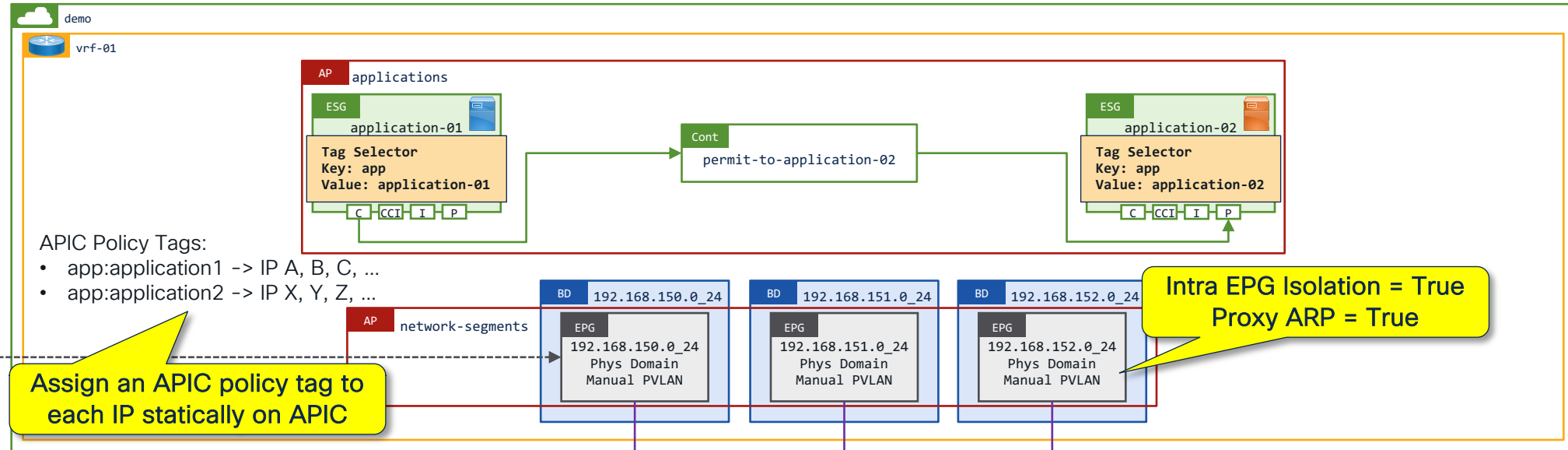
Option 4: Tag selectors with VMM integration and Intermediary switches



Option 5: MAC selectors, no VMM integration



Option 6: IP selectors, no VMM integration

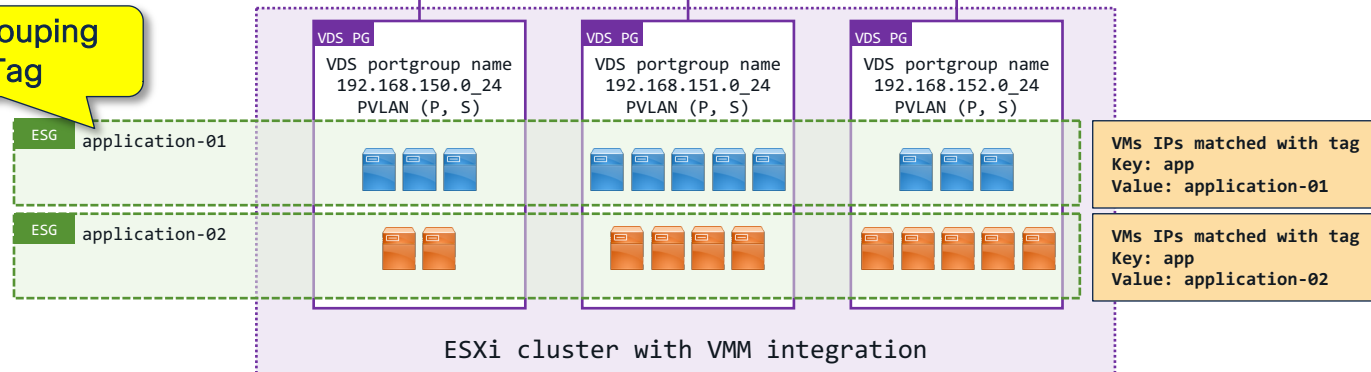


Logical grouping
by IP Tag

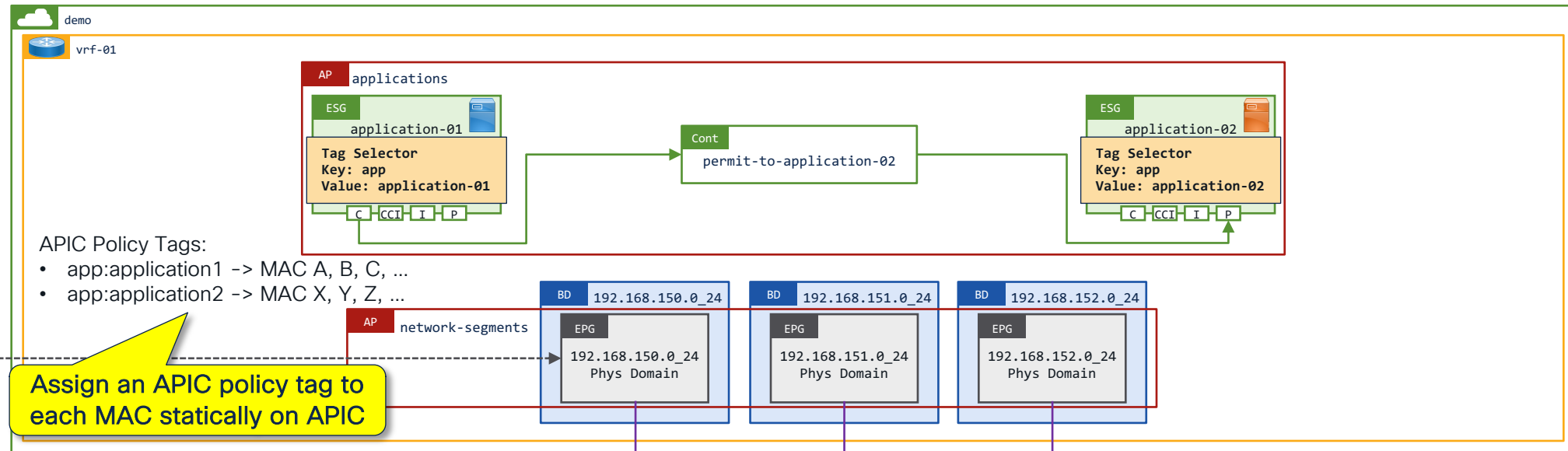
EPG

Settings:

- Physical Domain
- Static path bindings
- Manual/static PVLANS
- Intra EPG Isolation = True
- Proxy ARP = True



Option 7: MAC selectors for bare metal



Assign an APIC policy tag to each MAC statically on APIC

APIC Policy Tags:

- app:application1 -> MAC A, B, C, ...
- app:application2 -> MAC X, Y, Z, ...

Settings:

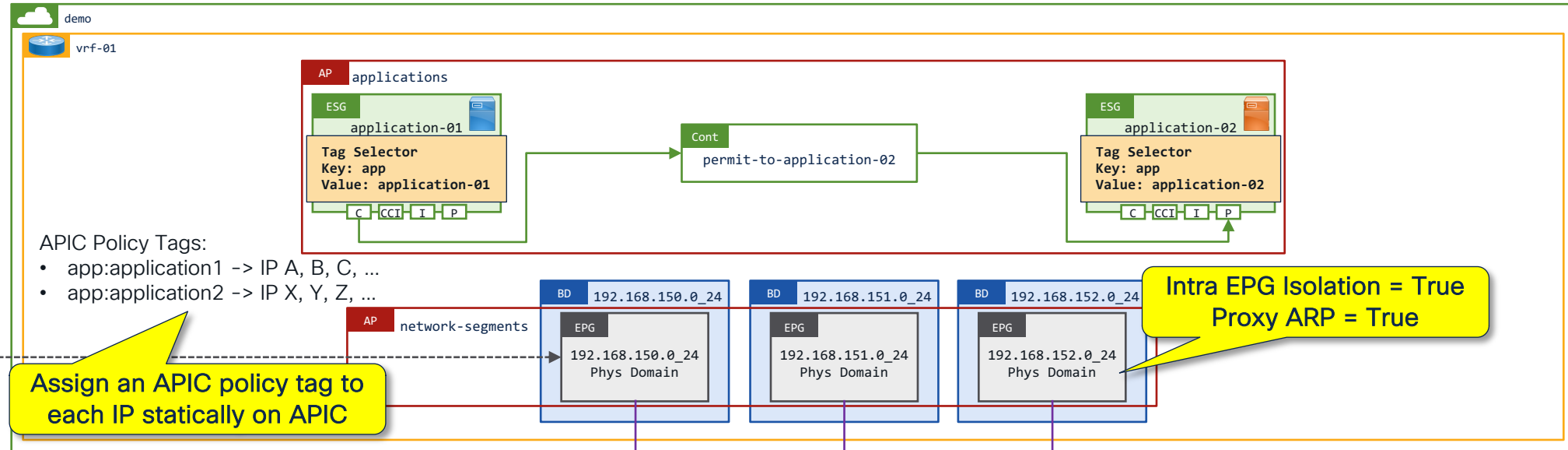
- Physical Domain
- Static path bindings

Logical grouping by MAC Tag

Bare metal MACs matched to the APIC tag
Key: app
Value: application-01

Bare metal MACs matched to the APIC tag
Key: app
Value: application-02

Option 8: IP selectors for bare metal



Assign an APIC policy tag to each IP statically on APIC

Intra EPG Isolation = True
Proxy ARP = True

EPG

Settings:

- Physical Domain
- Static path bindings
- Intra EPG Isolation = True
- Proxy ARP = True

Logical grouping
by IP Tag

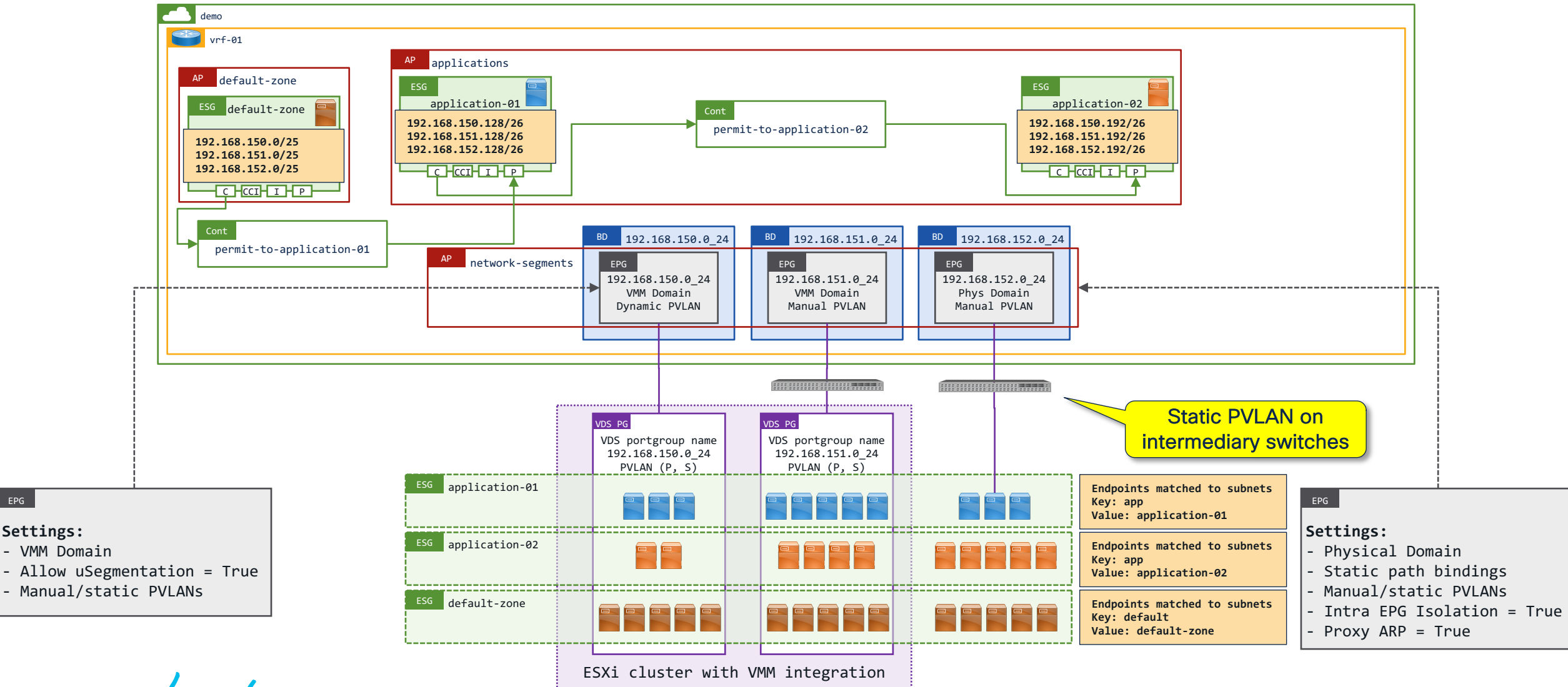
ESG application-01

ESG application-02

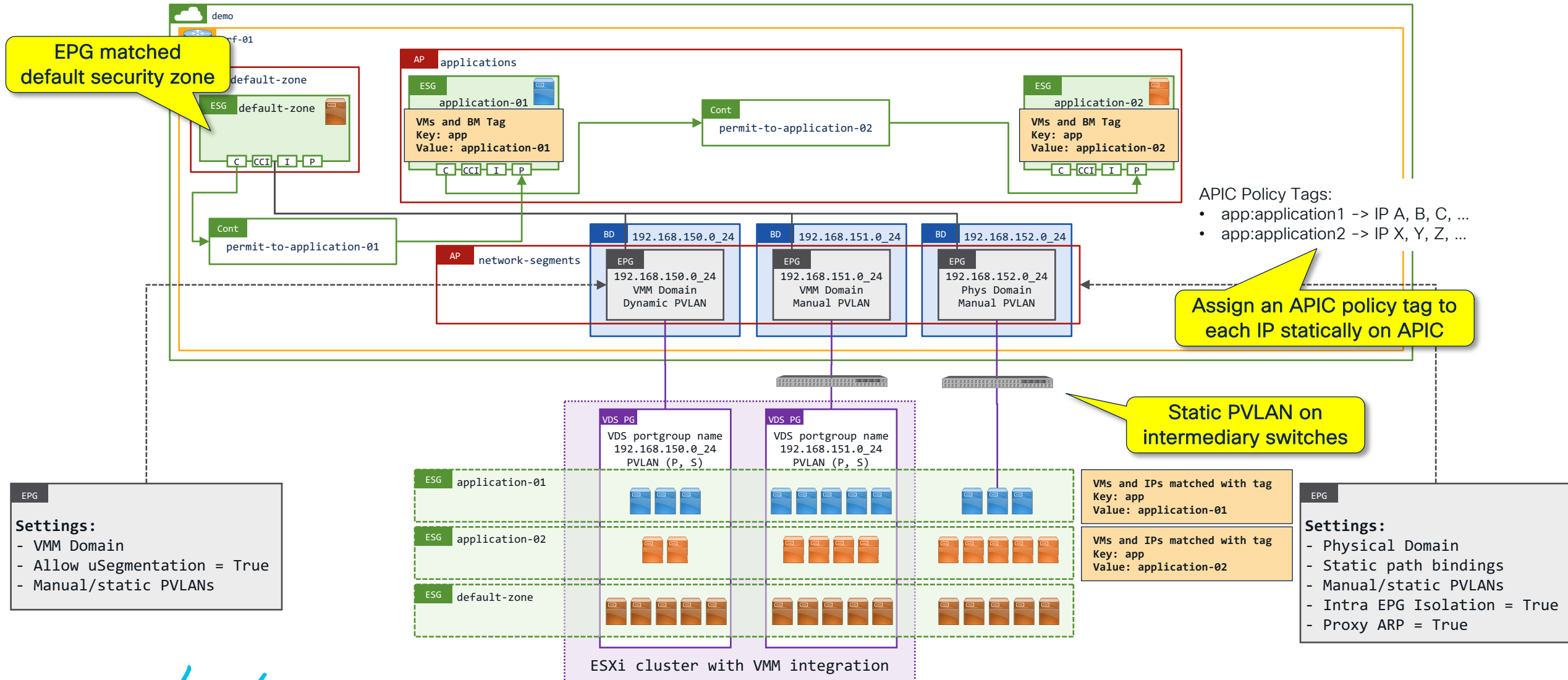
Bare metal IPs matched to the APIC tag
Key: app
Value: application-01

Bare Metal IPs matched to the APIC tag
Key: app
Value: application-02

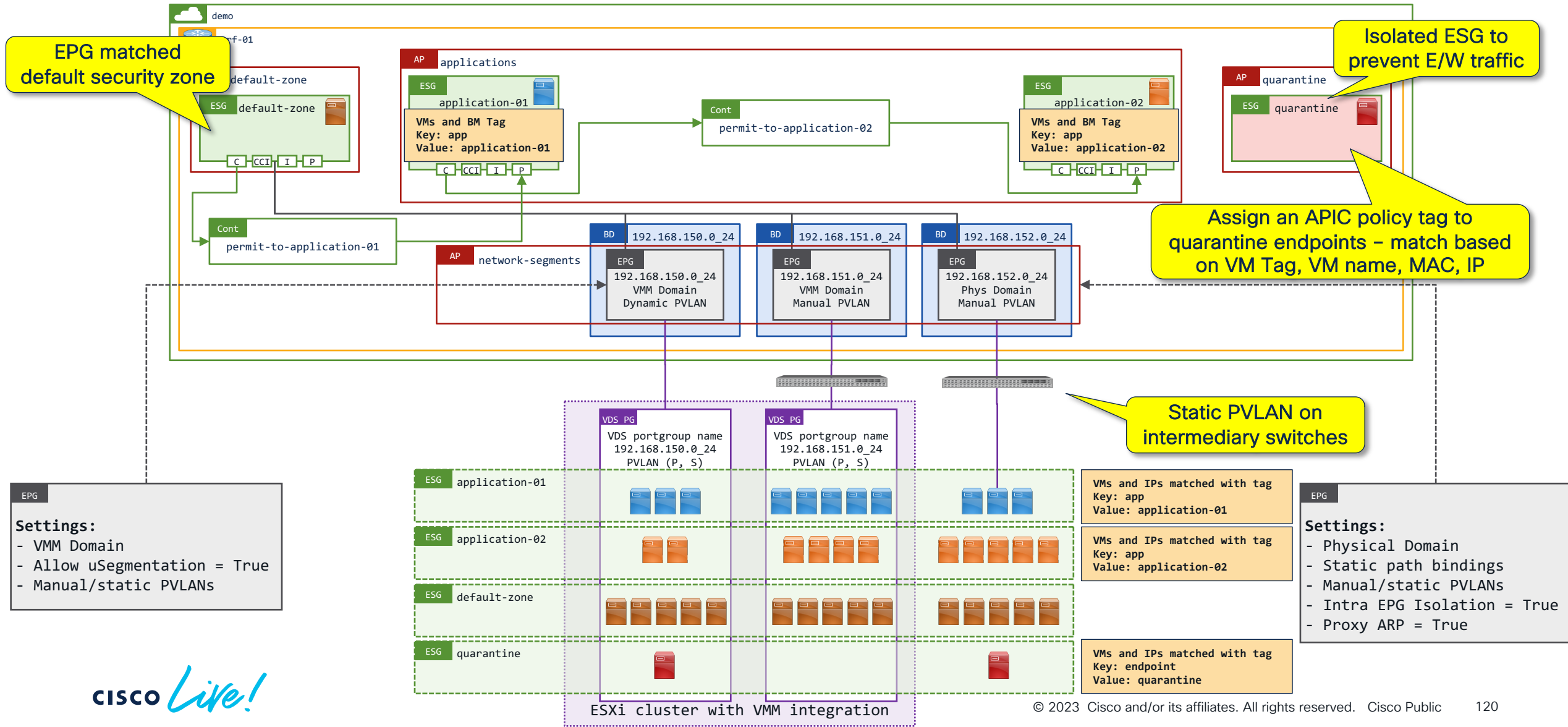
Option 9: Subnet selectors



Option 10: Combined solution



Option 11: Combined solution + Quarantine



Why do we need to enable Proxy ARP for IP mapping...

MAC addresses are not classified to ESGs when only IP-based selectors are used. 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 two IPs in the same subnet from the same EPG are classified into different ESGs, those two endpoints can still talk freely through the MAC and its original EPG...

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

demo

- Quick Start
- demo
 - Application Profiles
 - epg-matched-security-groups
 - network-segments
 - Application EPGs
 - 192.168.150.0_24**
 - 192.168.151.0_24
 - 192.168.152.0_24
 - uSeg EPGs
 - Endpoint Security Groups

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

Deploy Immediacy: **Immediate** On Demand

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

Delimiter: select an option

Enhanced Lag Policy: select an option

Allow Micro-Segmentation: ☒

Untagged VLAN Access: ☐

VLAN Mode: **Dynamic** Static

Port Binding: **Dynamic Binding** Ephemeral Default Static Binding

Netflow: **Disable** Enable

Allow Promiscuous: Reject

Forged Transmits: Reject

MAC Changes: Reject

Active Uplinks Order: Enter IDs of uplinks separated by comma

Standby Uplinks: Enter IDs of uplinks separated by comma

Custom EPG Name:

Properties

Name: 192.168.150.0_24

Alias:

Description: optional

Annotations: Click to add a new annotation

Global Alias:

uSeg EPG: false

Tag(class): 16390

Option Tag:

QoS class: Level3 (Default)

Custom QoS: select a value

Data-Plane Policer: select a value

Intra EPG Isolation: **Enforced Unenforced**

Forwarding Control: ☒ proxy-arp

Preferred Group Member: **Exclude** Include

Flood in Encapsulation: **Disabled** Enabled

Summary Monitor Configure Permissions Ports Hosts VMs

Port binding: **Static binding**

Port allocation: Elastic

VLAN ID: 1046

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

Proxy ARP is only available when Intra ESG isolation is enabled

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

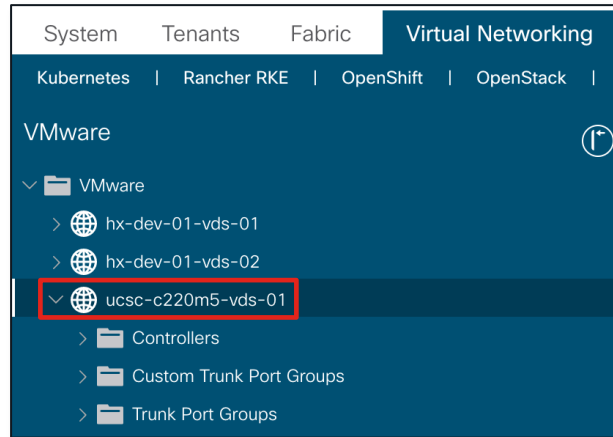
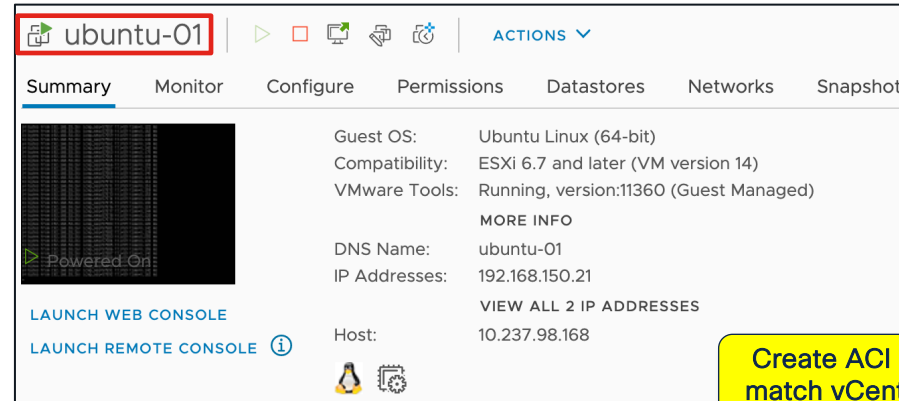
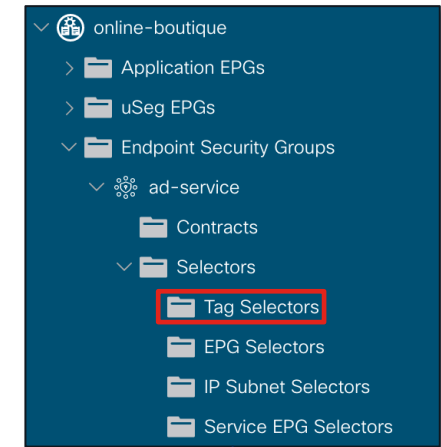
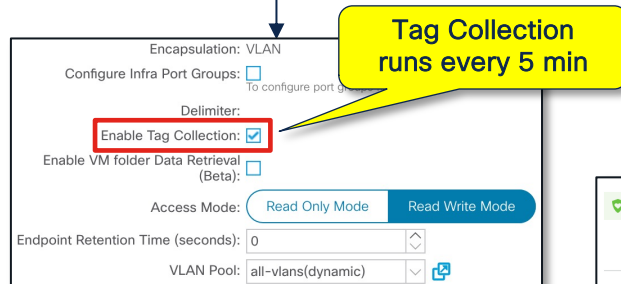
Add an Intra EPG Contract

Contract Type: Intra EPG Contract

Name	Tenant	Contract Type
permit-any	demo	Intra EPG Contract

vCenter tag/name matching requires read/write
vmm integration...

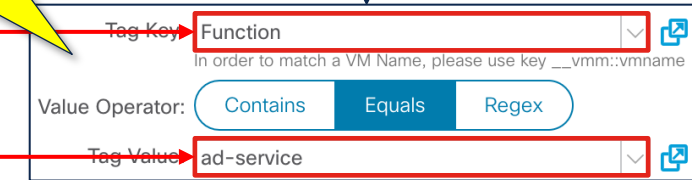
Dynamic Policy Tag matching from vCenter



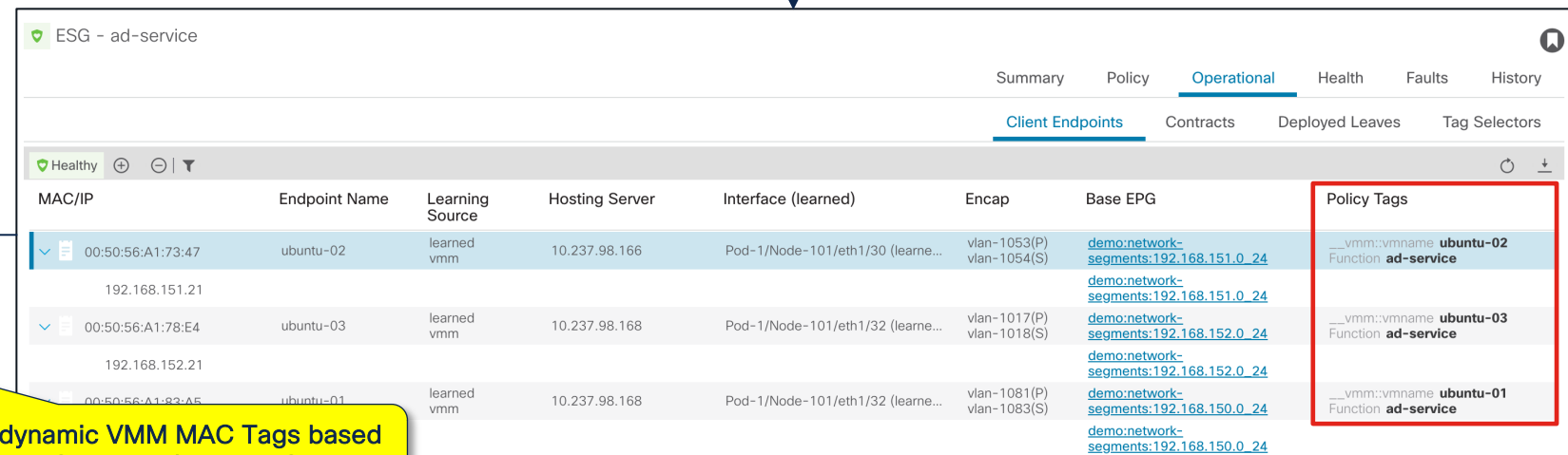
Tag Collection runs every 5 min



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 endpoint mapping...

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

Stats Health Faults History

Packets **Policy Tags** Resource IDs

Associated Object

- [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-\[*\]](#)

ESG Selector Precedence and Contract Matrix...

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

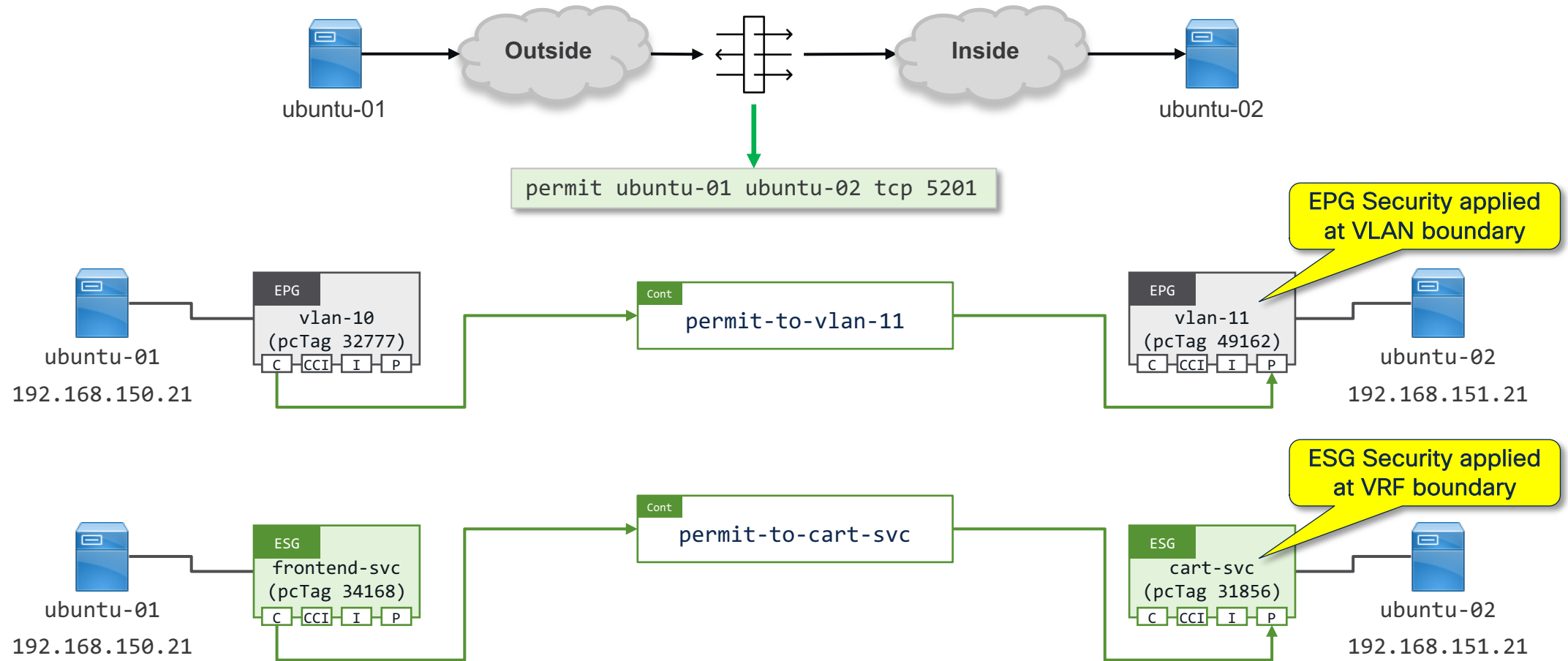
**use EPG → ESG mapping

My preferred option is to automate static MAC tagging from the endpoint IP address...

Understanding contracts

Let's check our understanding on how contracts work...

How do contracts work...?

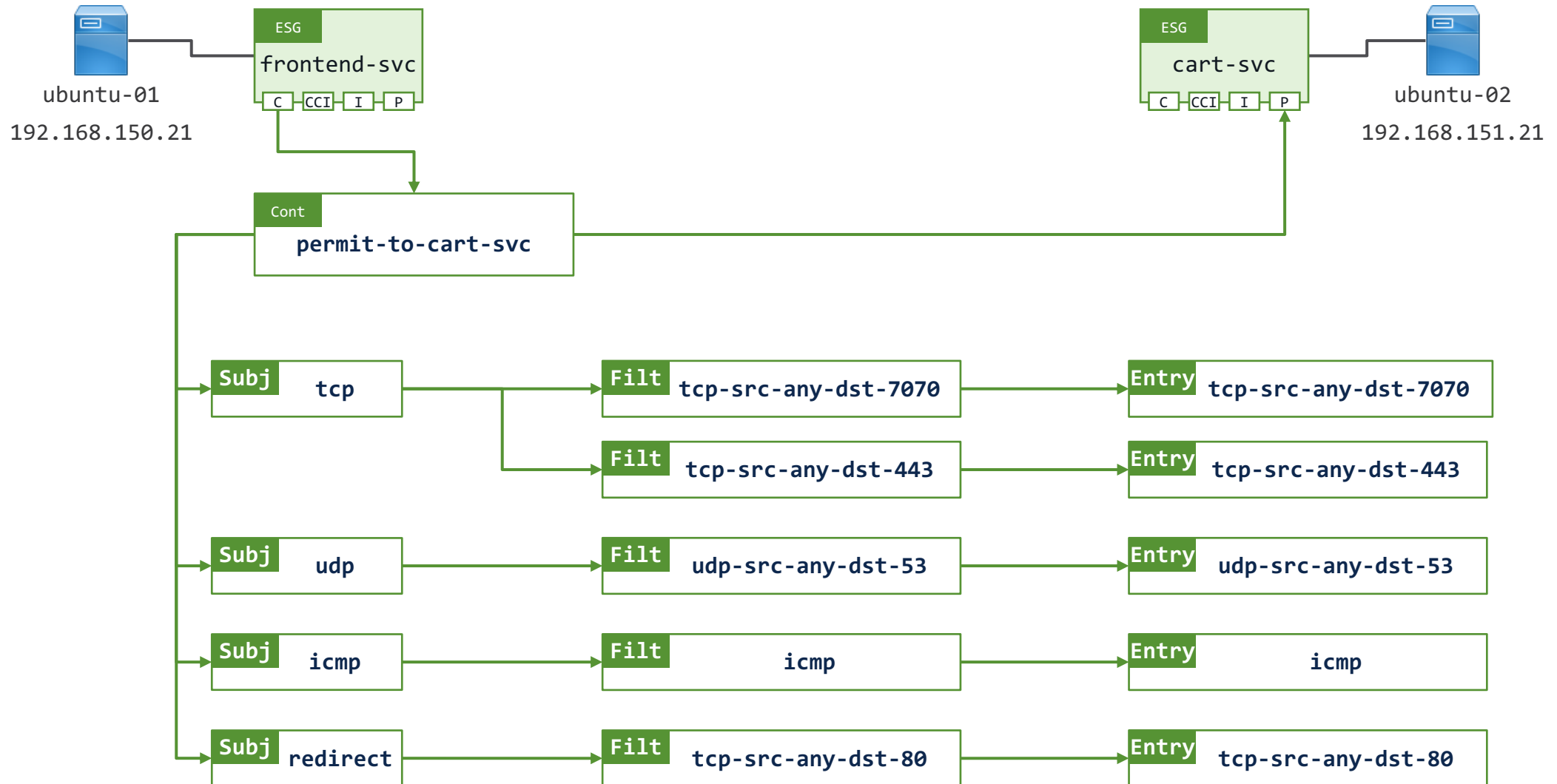


*arrows indicates direction of traffic flow i.e. from consumer to provider

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

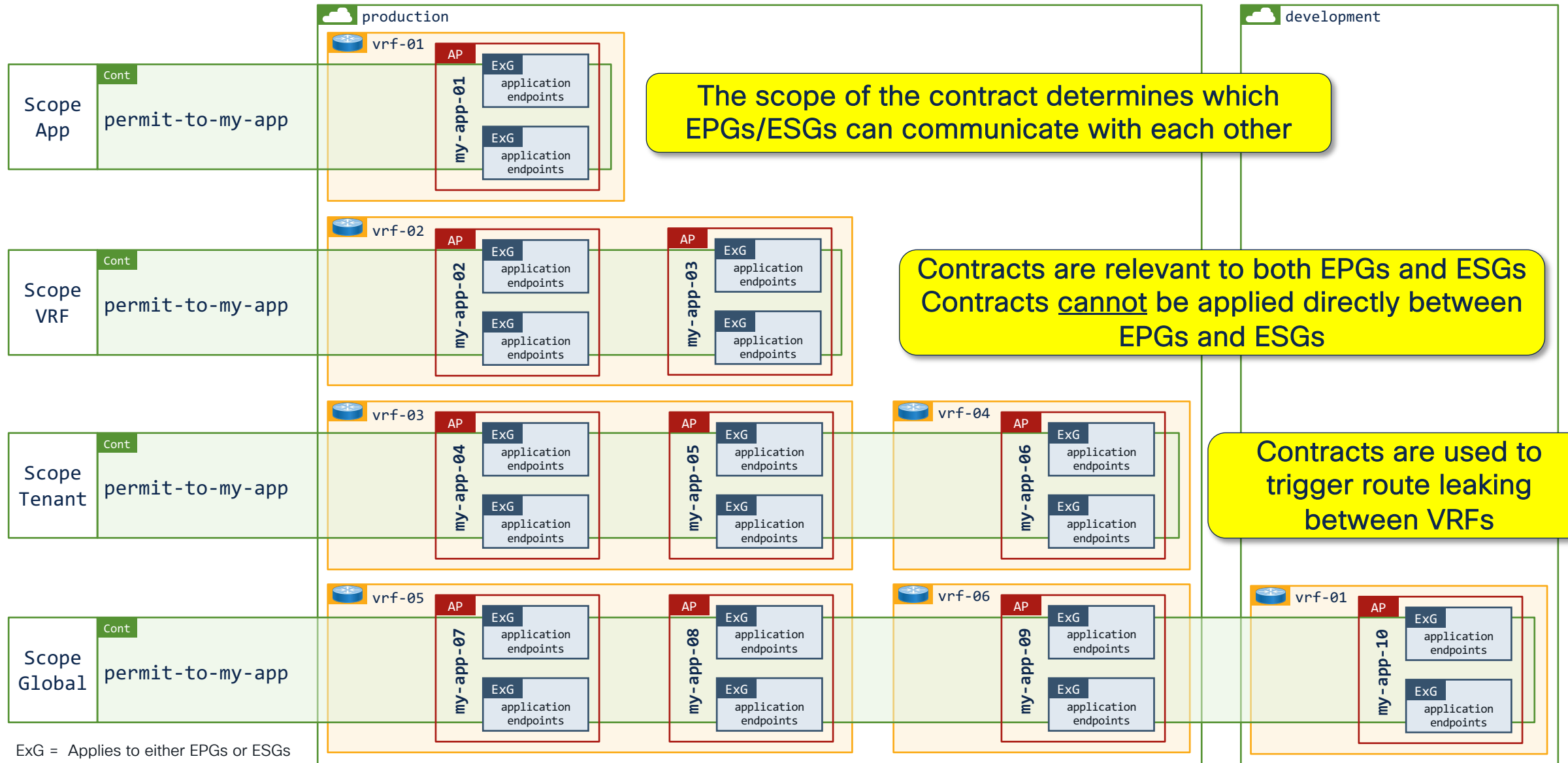
Contract Structure...



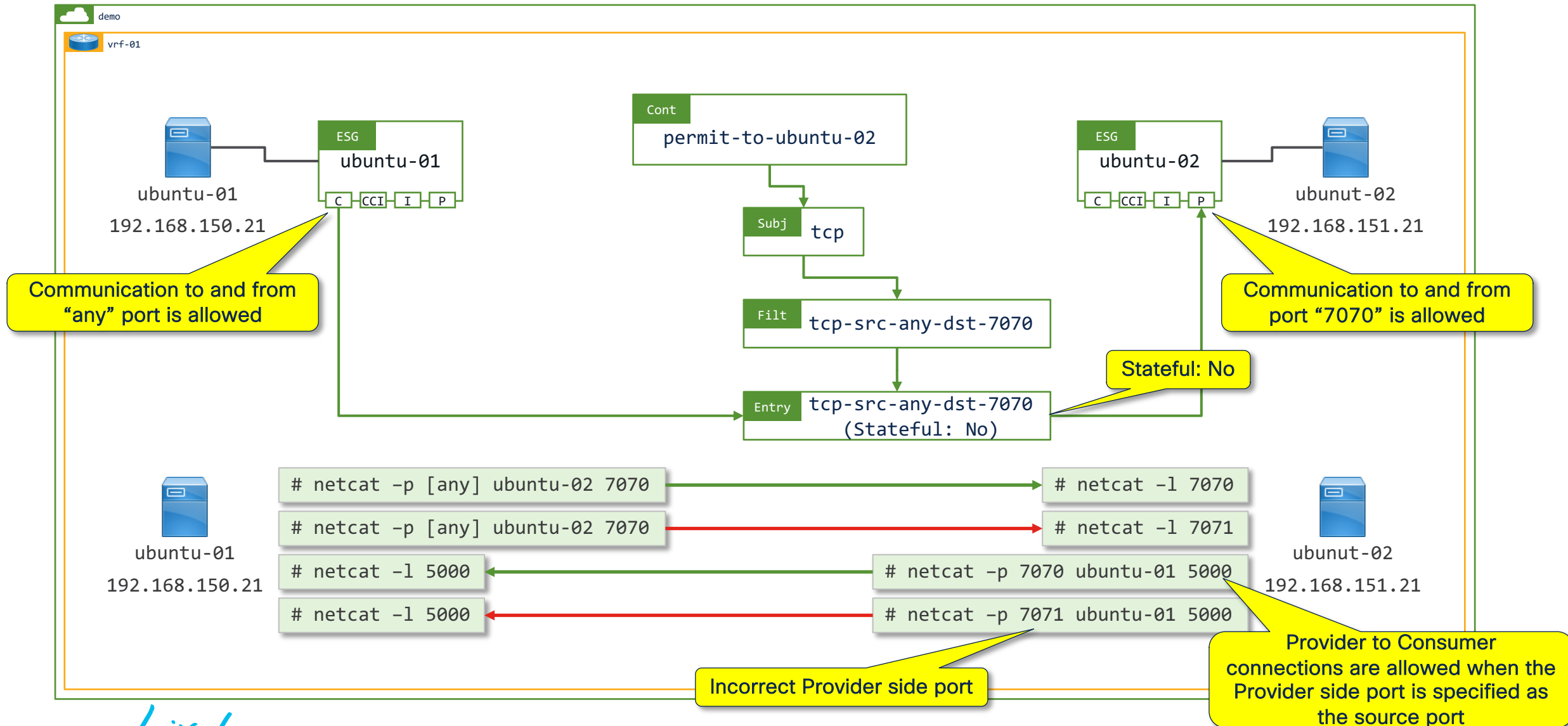
Contract Scope (Relevancy)

- The scope of a contract defines where a contract is relevant, there are four options:
 - Global – used to control traffic between EPG/ESG in different Tenants/VRFs
 - Tenant – used to control traffic between EPG/ESG across VRFs within a Tenant
 - VRF – used to control traffic between EPG/ESG within a VRF
 - Application Profile– used to control traffic within an Application Profile
- 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 if the scope is not fully considered
 - Note: Contract trigger route leaking between VRFs
 - Recommendation: define explicit contracts rather than n:1 reference

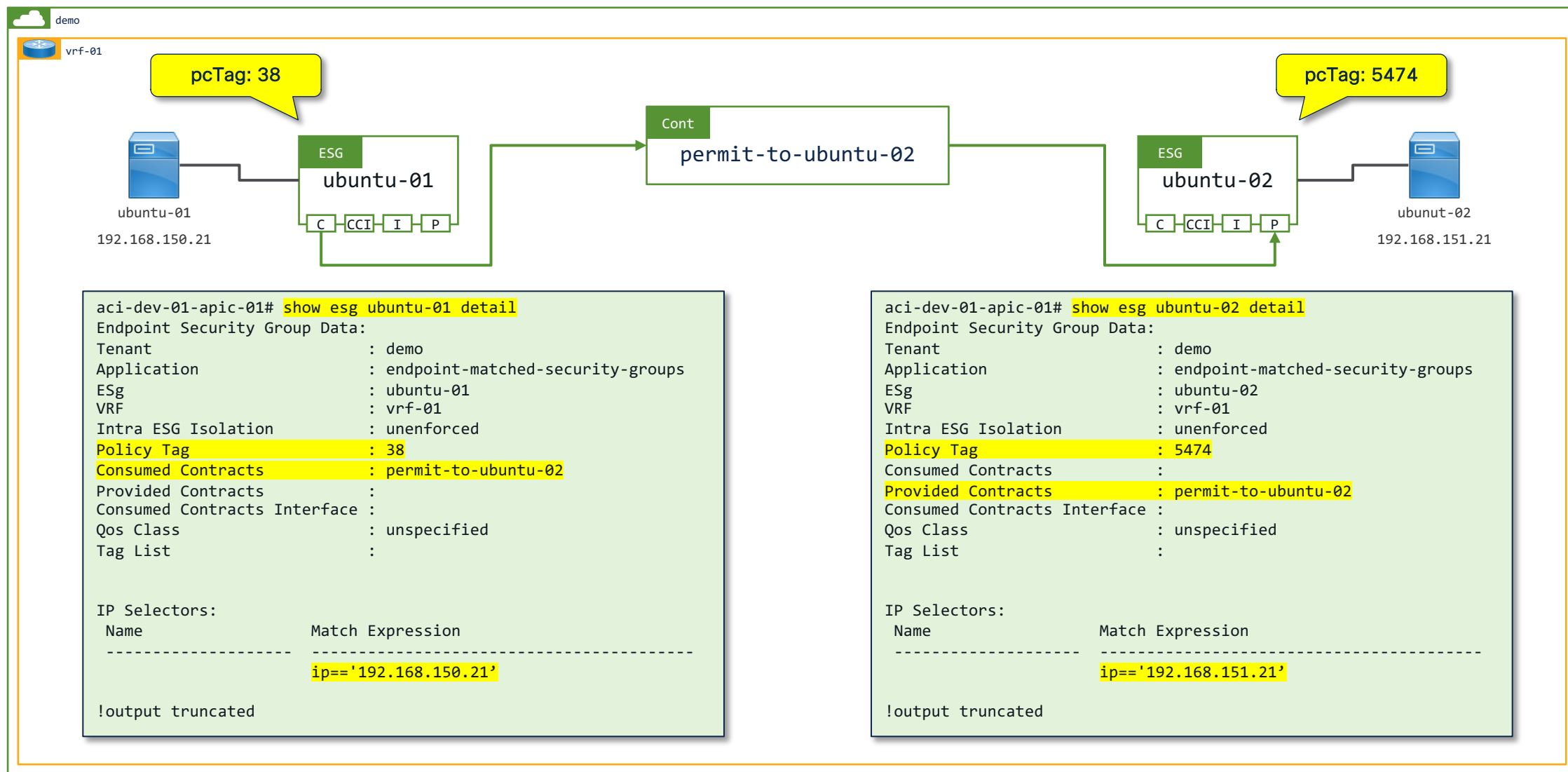
Contract Scope



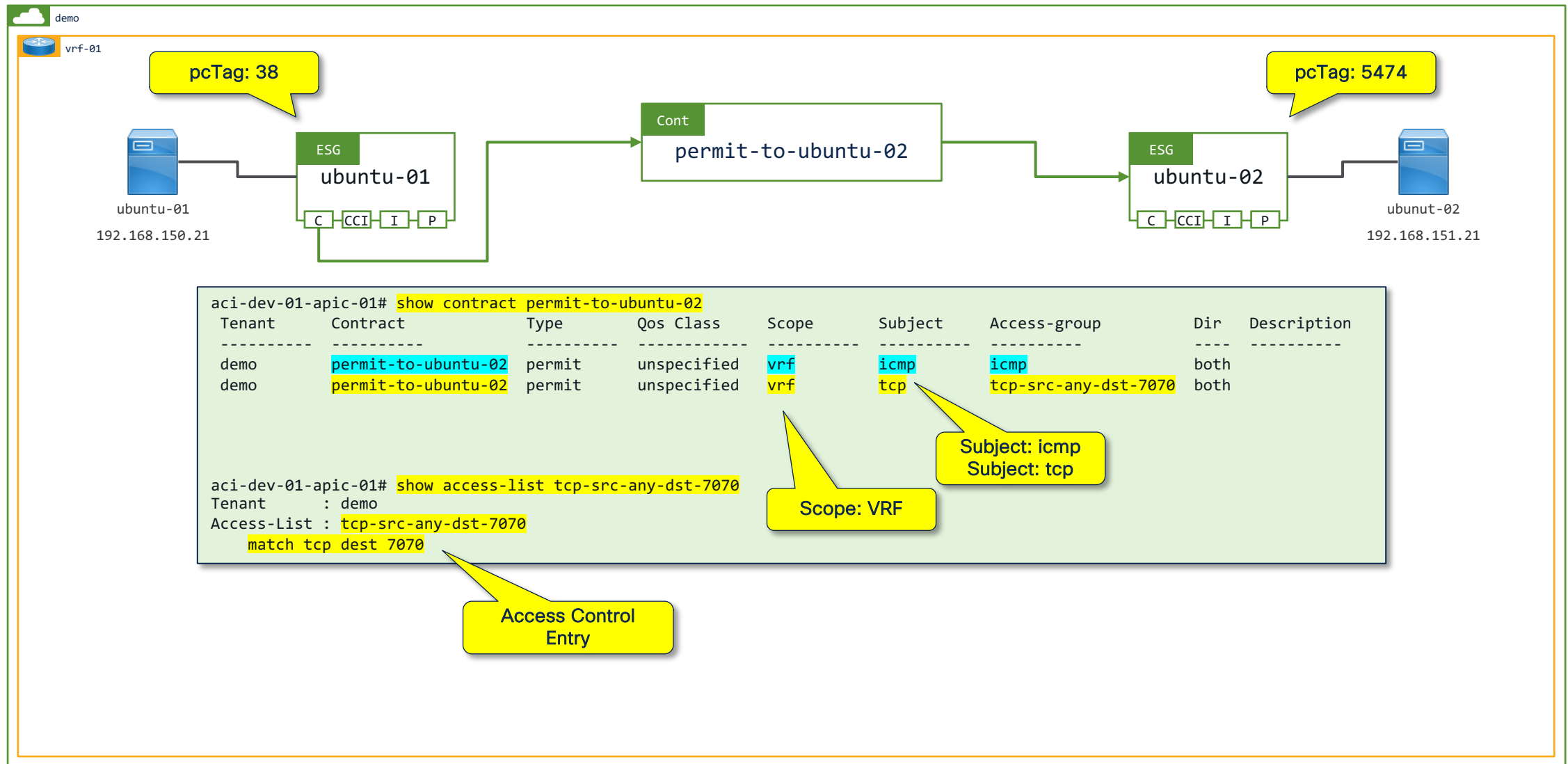
Verifying Contract operation with netcat – Stateful = No



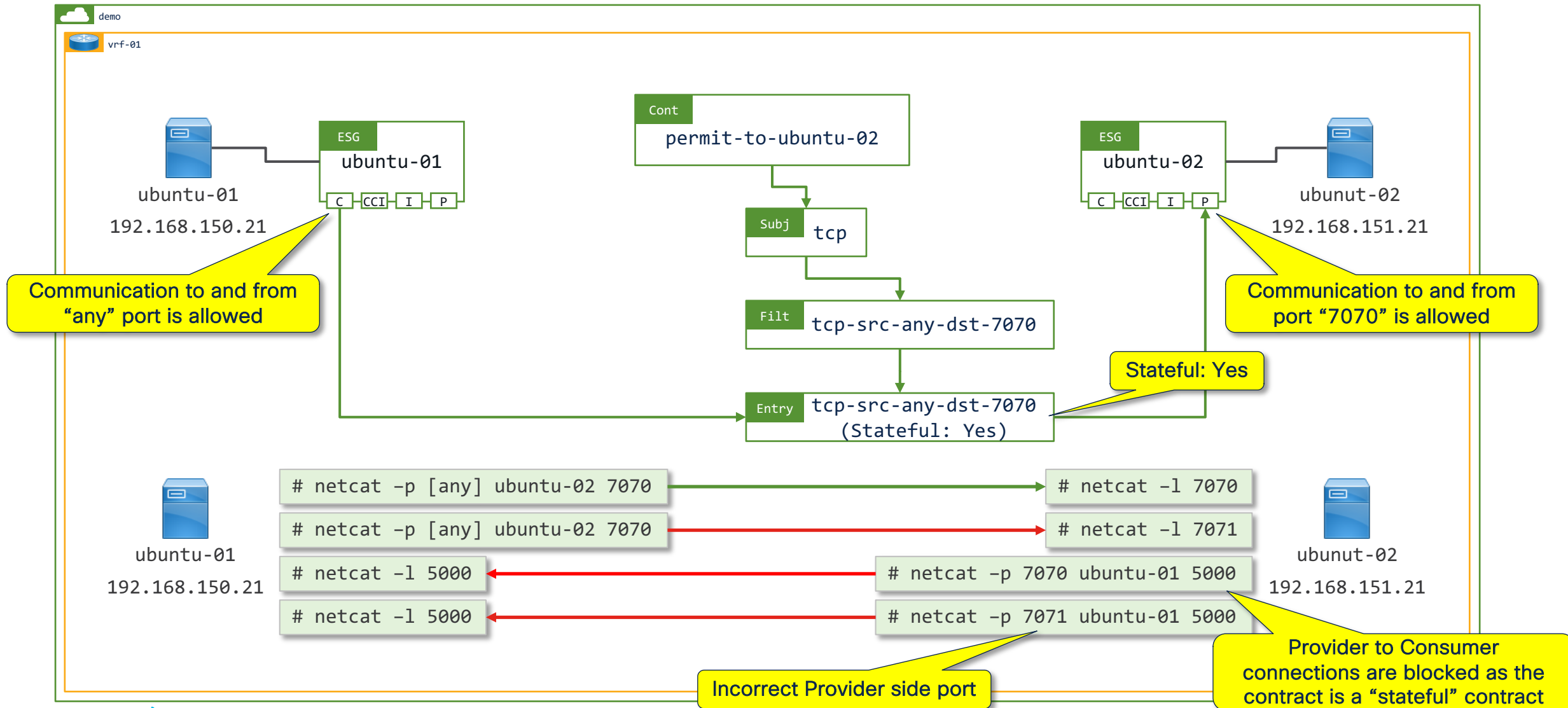
Verifying Contract Operation: EPG/ESG details



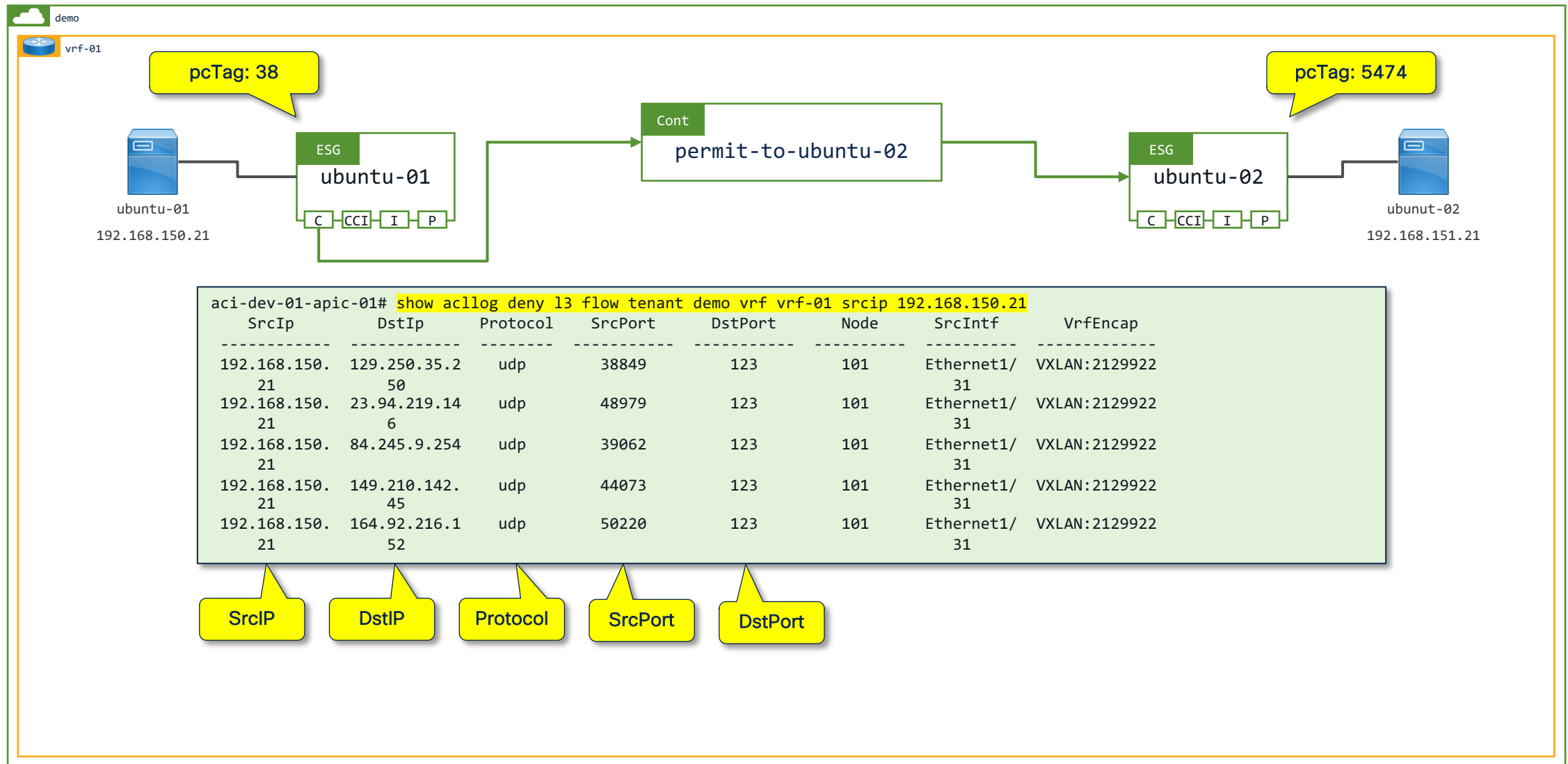
Verifying Contract Operation: Contract details



Verifying Contract operation with netcat – Stateful = Yes



Verifying Contract Operation: Drop details



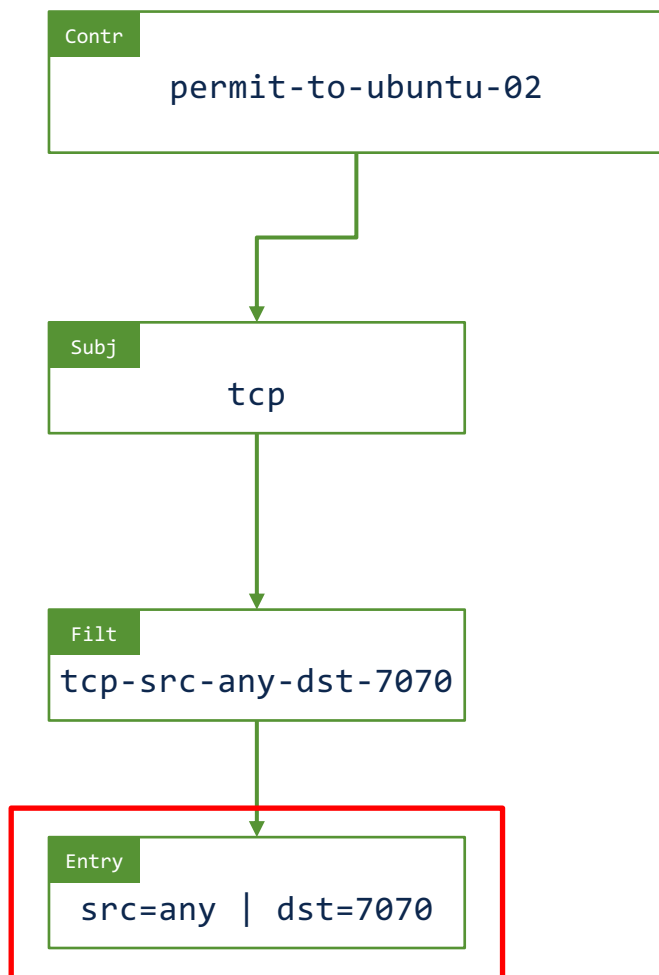
Verifying Contracts with Syslog and ELAM

The image displays two overlapping screenshots. The background screenshot is the Graylog web interface, showing a search for the message "demo:vrf-01". The foreground screenshot is the Cisco APIC (aci-dev-605) interface, specifically the ELAM Assistant page. The ELAM Assistant page shows the configuration for capturing a packet with ELAM (Embedded Logic Analyzer Module). The configuration includes the following parameters:

Status	Node	Direction	Source I/F	Parameters	VxLAN (outer) header
Report Ready	node-101	from downlink	any	src ip 192.168.150.100 dst ip 192.168.156.155	
Report Ready	node-102	from downlink	any	src ip 192.168.150.100 dst ip 192.168.156.155	

Below the configuration, the Packet Forwarding Information is displayed:

Forward Result	
Destination Type	To SUP/CPU
SUP Redirect Reason (SUP code)	NONE The packet was not sent to CPU.
Contract	
Destination EPG pcTag (dclass)	0x1574 / 5492 (null)
Source EPG pcTag (sclass)	0x157A / 5498 (demo:ftdv-02-eth7-gig-0-4ctxvrf-01:gig-0-4)
Contract was applied	1 (Contract was applied on this node)
Drop	
Drop Code	no drop

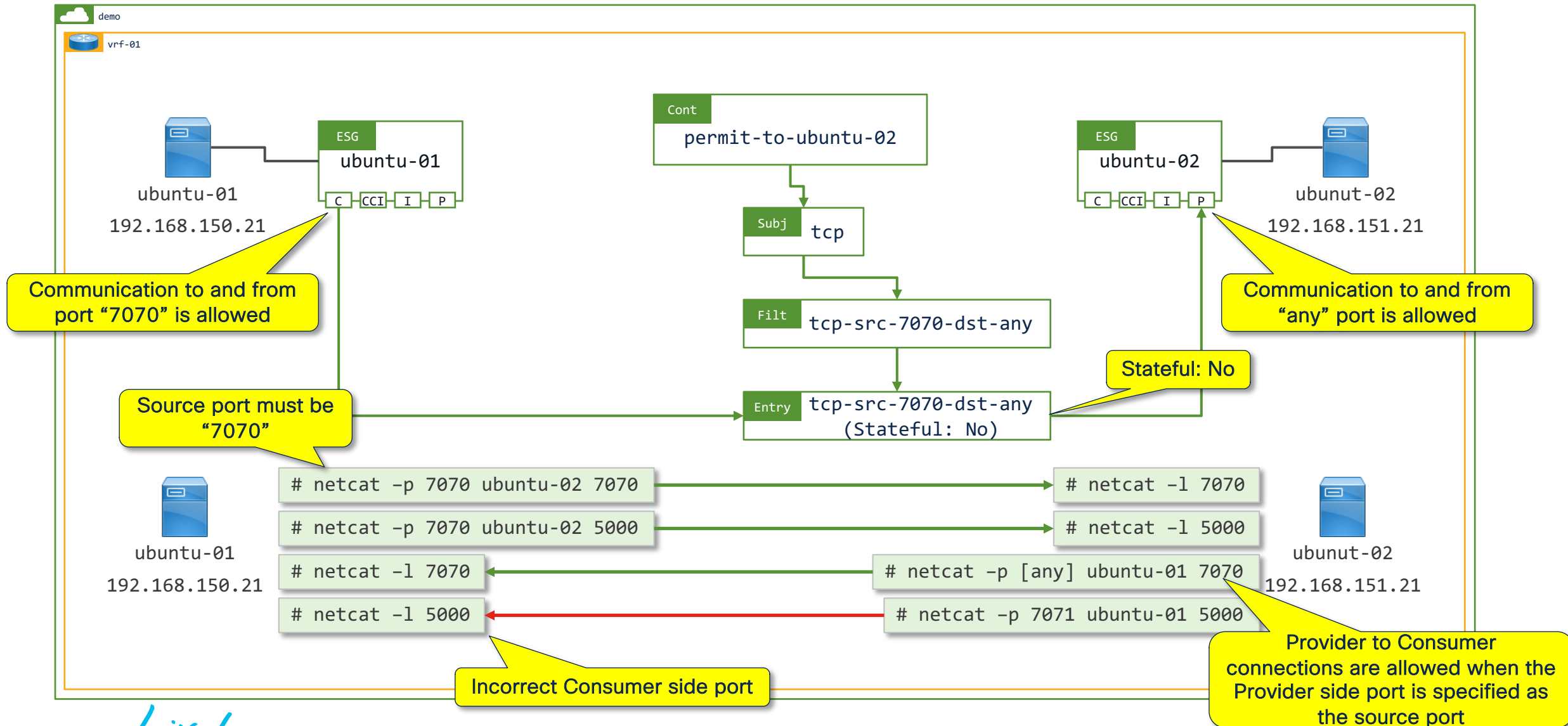


Filter Entry source port =
port opened on the consumer EPG/ESG

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



Reversing the Filter ports - Stateful = No

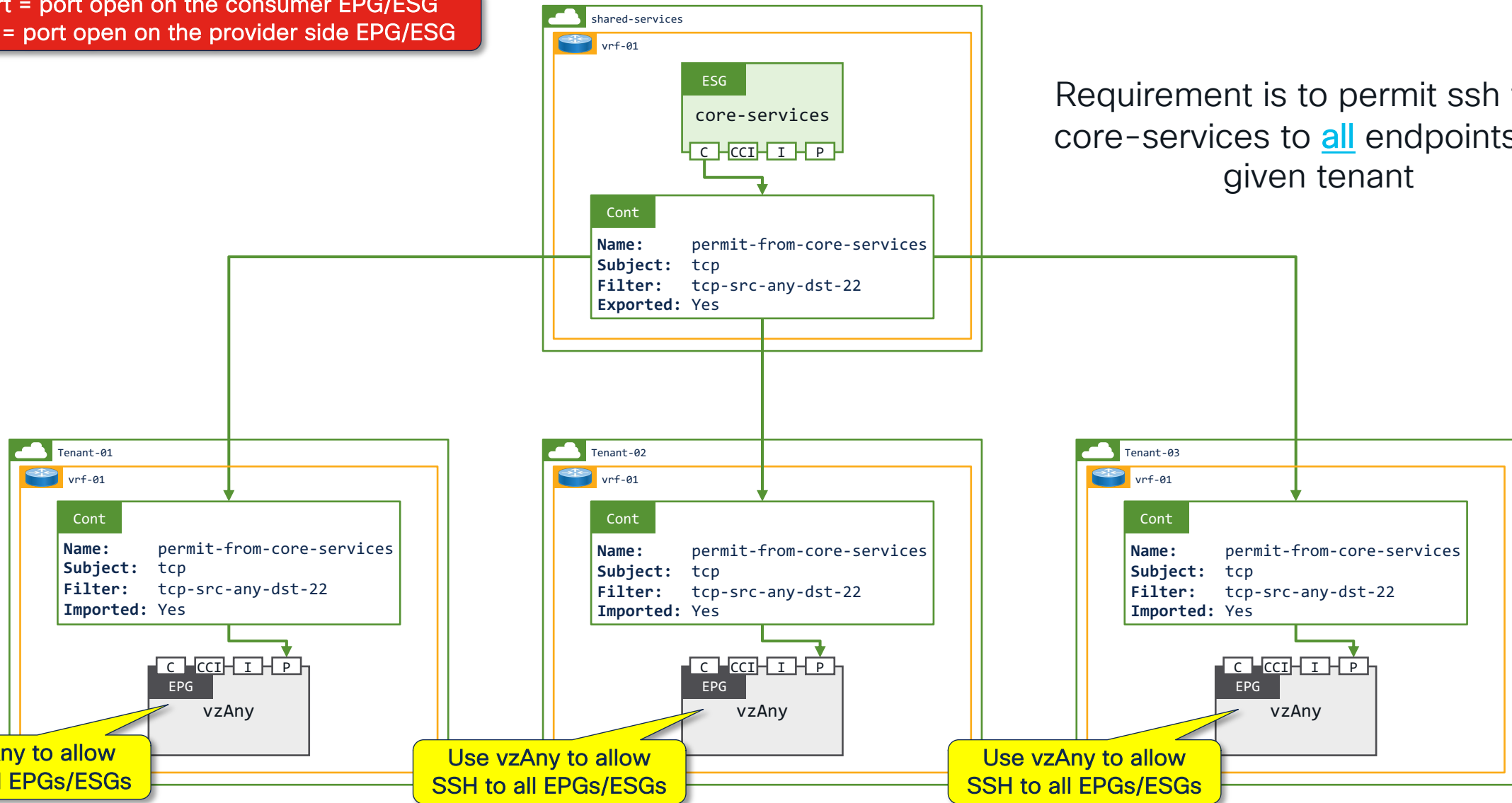


Why would you want to reverse the Consumer and Provider Filters...?

vzAny as a contract Provider

src_port = port open on the consumer EPG/ESG
dsr_port = port open on the provider side EPG/ESG

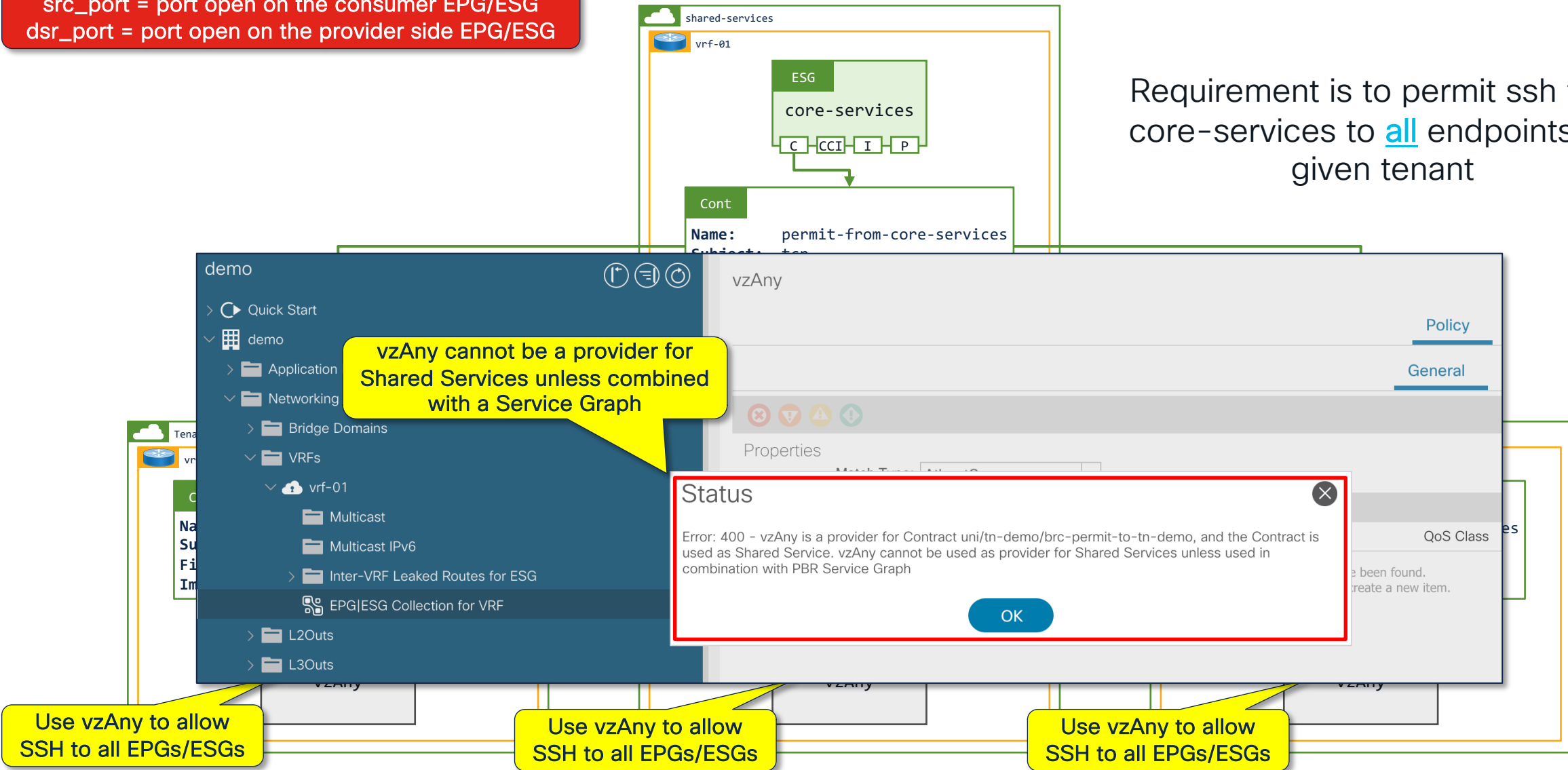
Requirement is to permit ssh from core-services to all endpoints in a given tenant



vzAny as a contract Provider

src_port = port open on the consumer EPG/ESG
dsr_port = port open on the provider side EPG/ESG

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



vzAny as a contract Consumer – Filters Reversed

src_port = port open on the consumer EPG/ESG
dsr_port = port open on the provider side EPG/ESG

Reverse the Filter ports
in the Contract

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

Provide the Contract

Consume the Contract

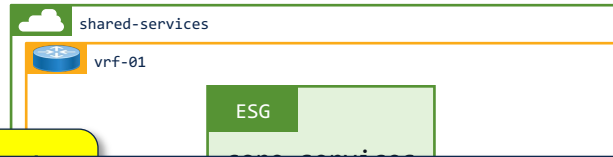
Use vzAny to allow
SSH to all EPGs/ESGs

Use vzAny to allow
SSH to all EPGs/ESGs

Use vzAny to allow
SSH to all EPGs/ESGs

vzAny as a contract Consumer – Filters Reversed

src_port = port open on the consumer EPG/ESG
dsr_port = port open on the provider side EPG/ESG



Requirement is to permit ssh from
s in a

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:

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 Interface

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

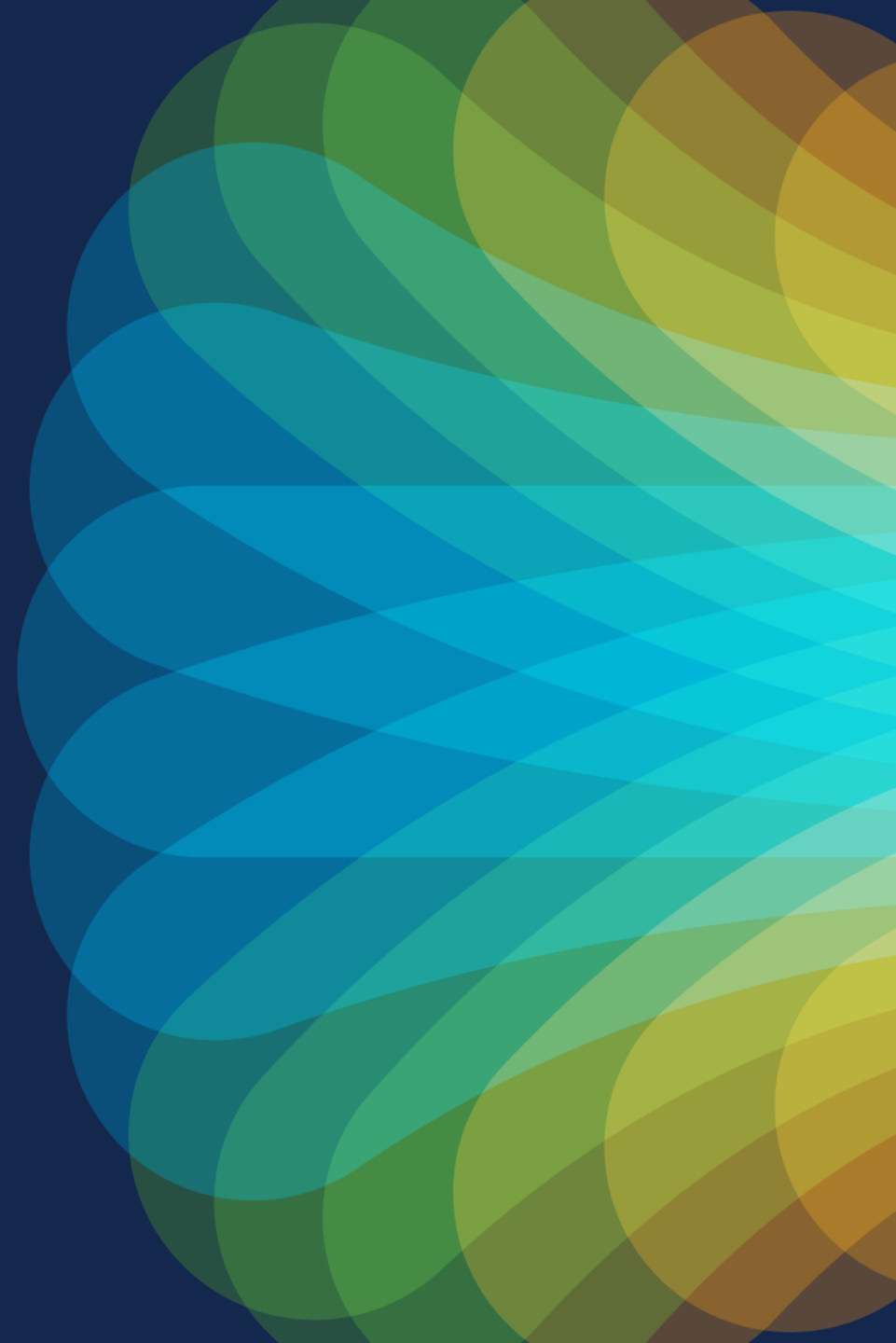
Consume the exported contract(s)

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

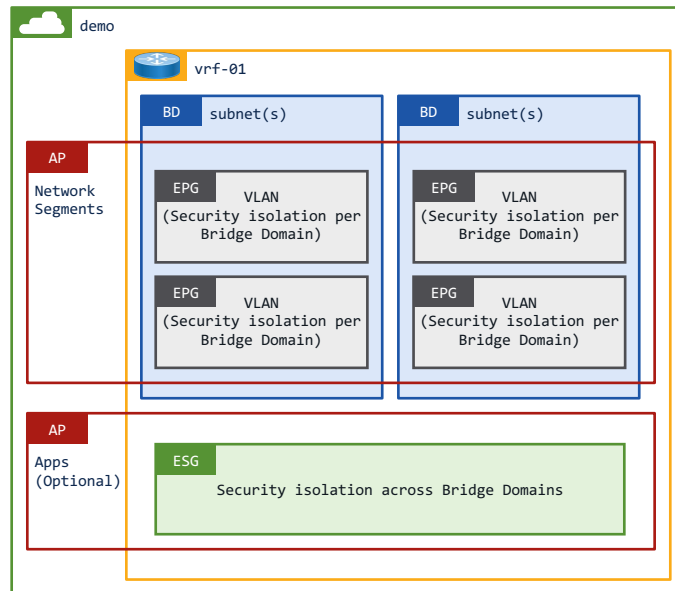
External Connectivity...



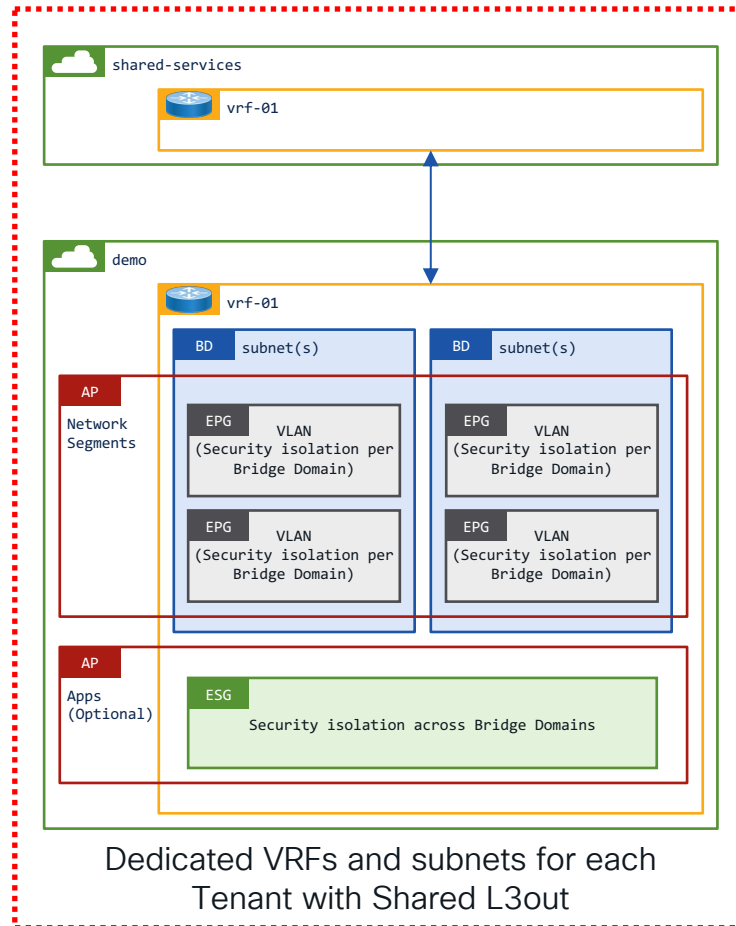
Where should you place your L3outs...?

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

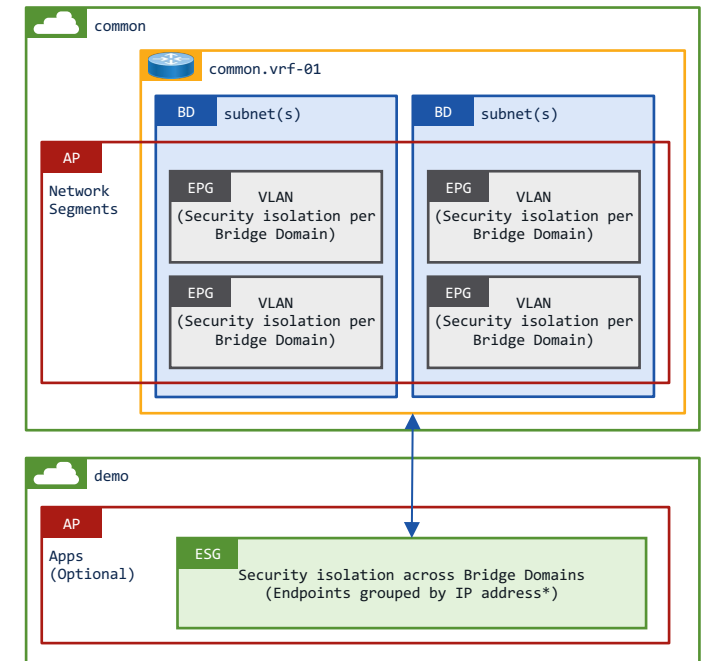
External Connectivity



Dedicated VRFs and subnets for each Tenant with Dedicated L3outs

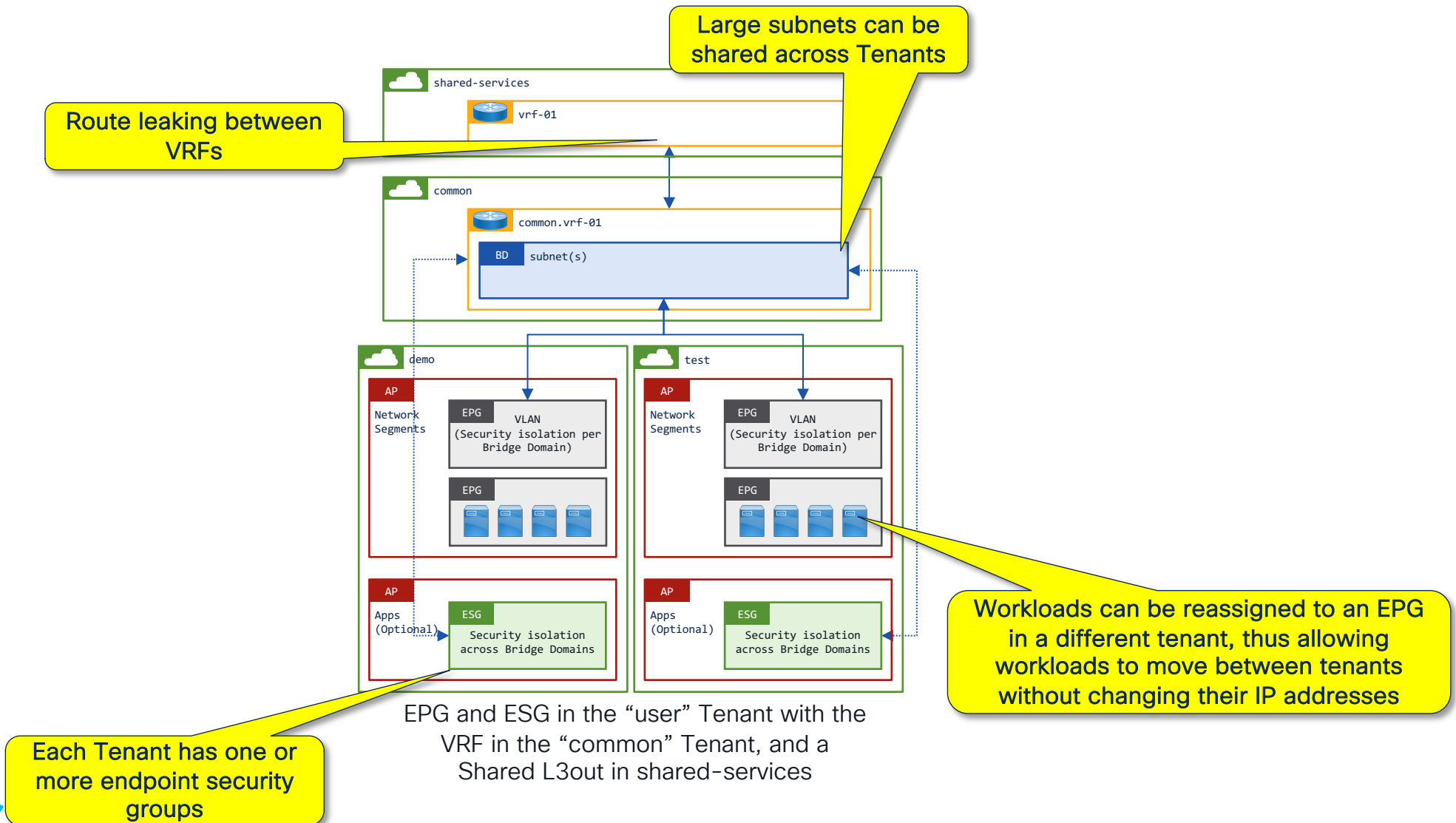


Dedicated VRFs and subnets for each Tenant with Shared L3out



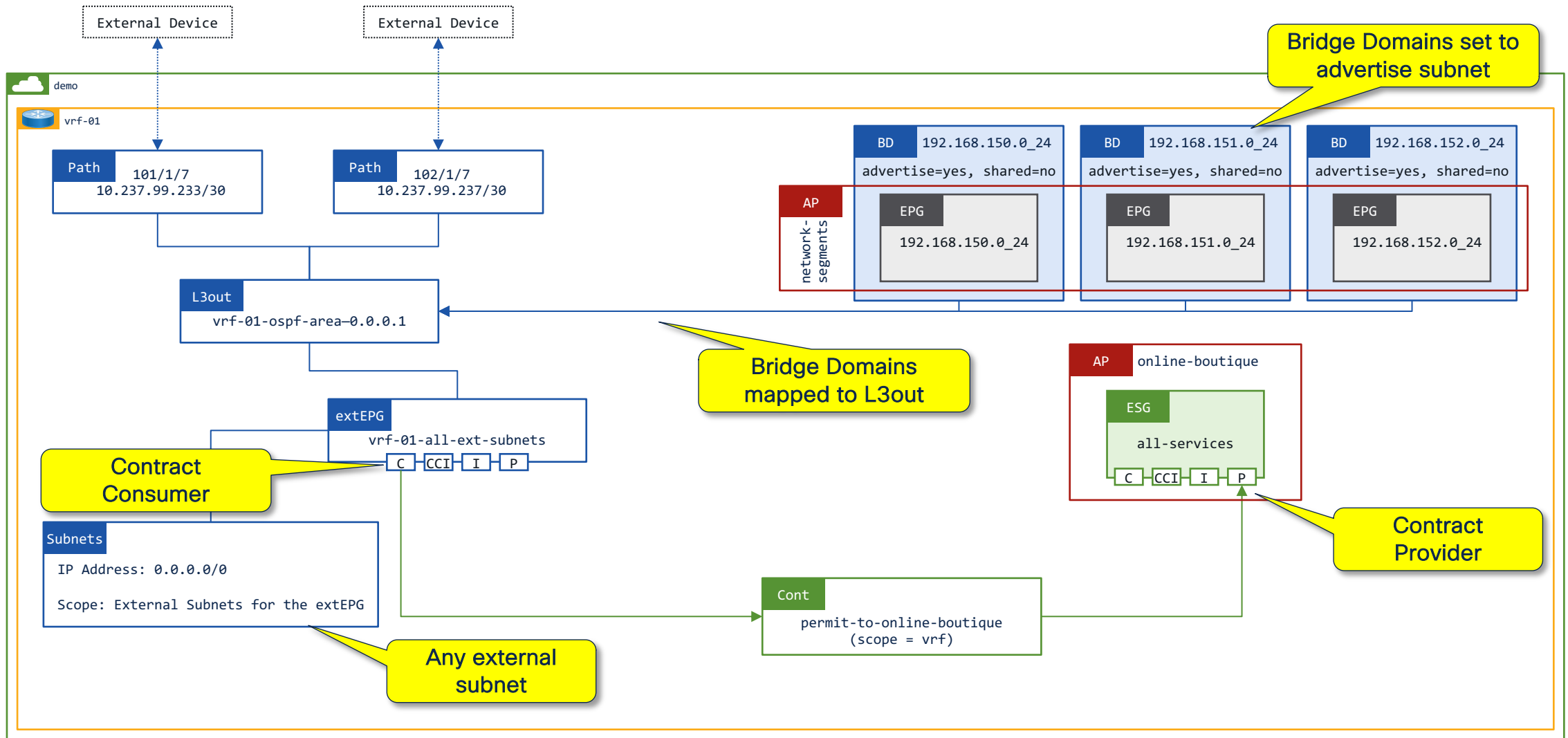
Shared networking with isolated security

External Connectivity with shared subnets...



Option 1 – Dedicated L3out per Tenant

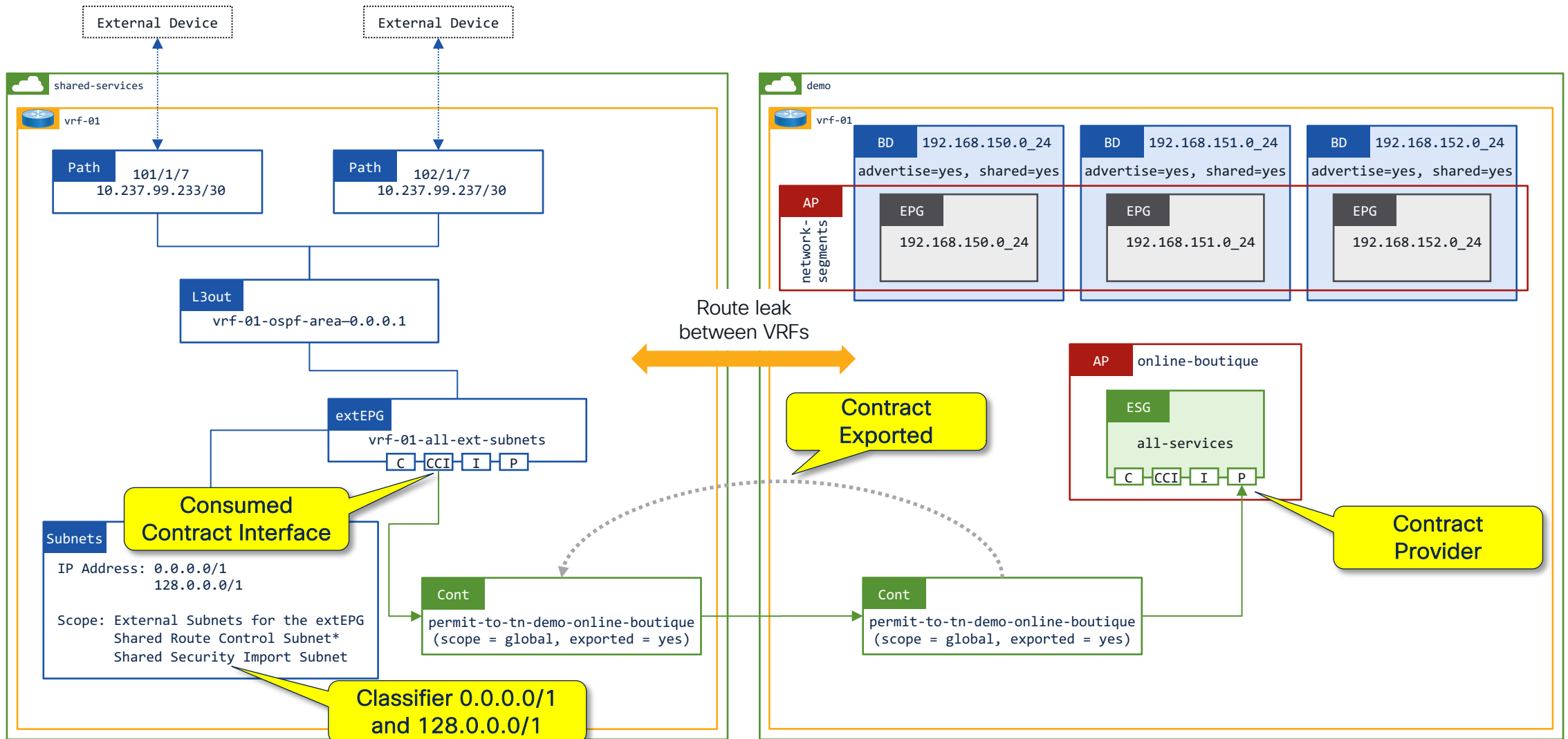
Dedicated L3out



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

Option 2 – Shared L3out

Shared L3out 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...?

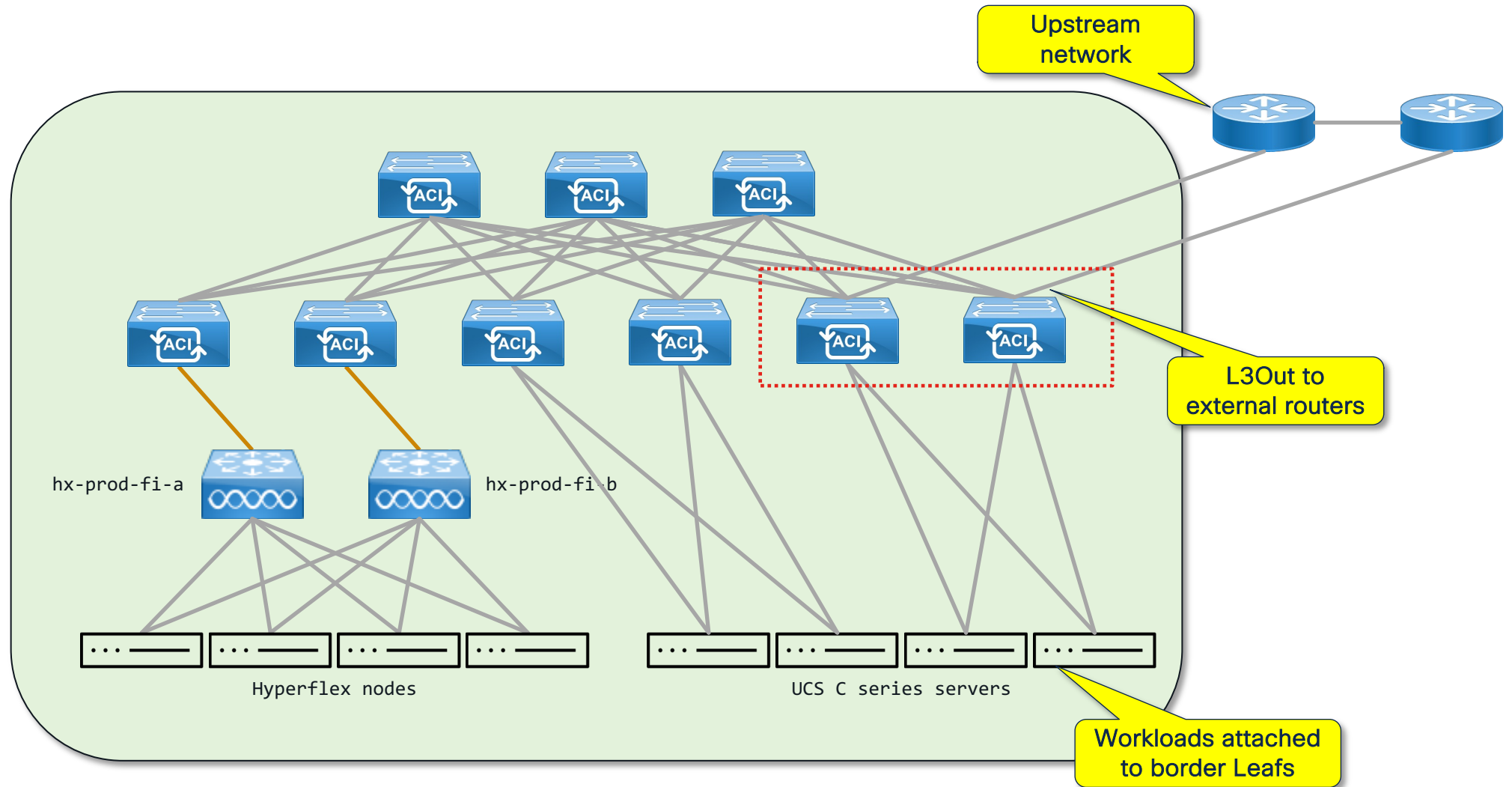


How does ACI Route Leaking work...?

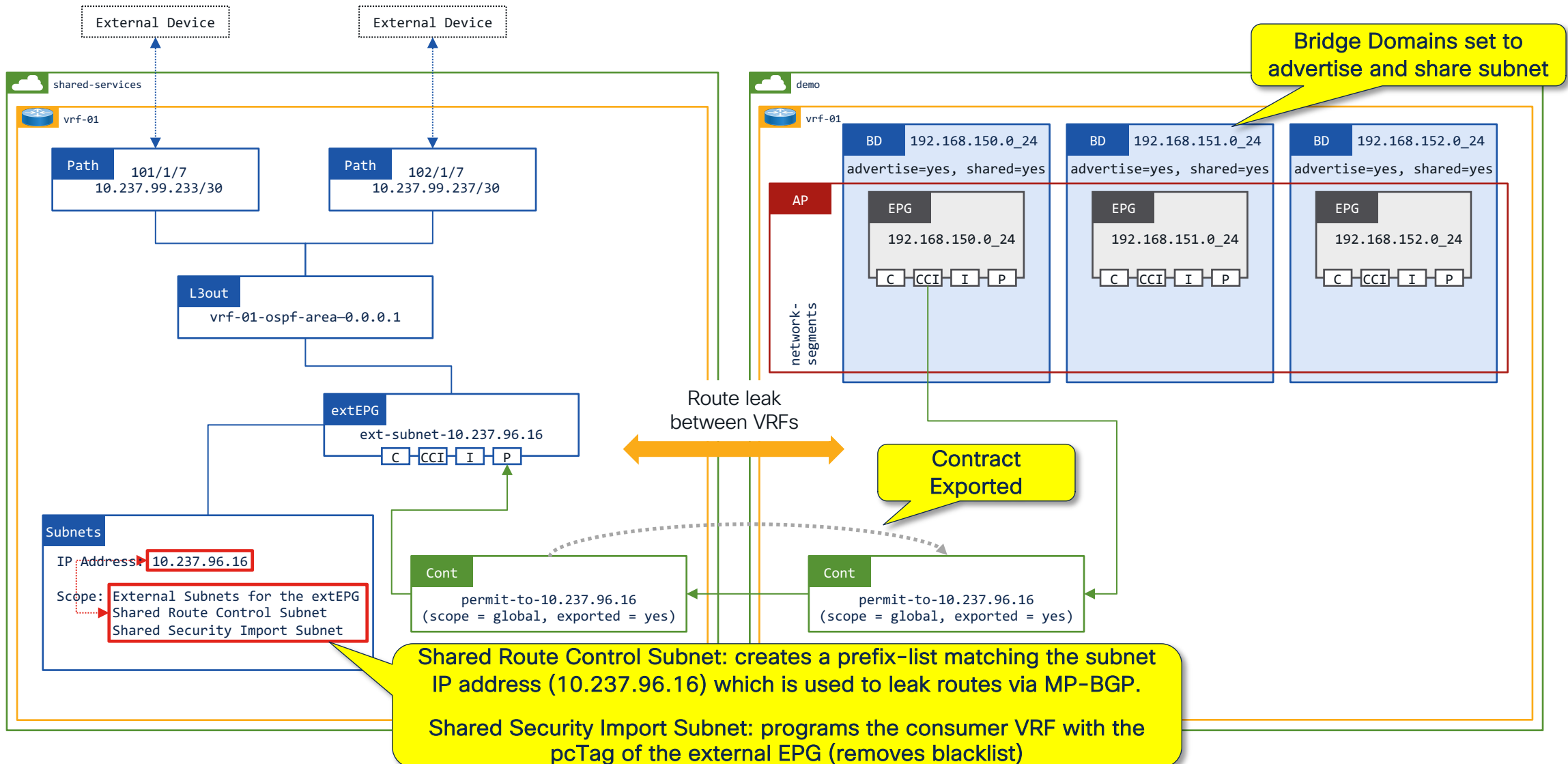
Dedicated or shared border Leaf switches...?

Who is the Consumer and who is the Provider...?

Non dedicated border Leafs

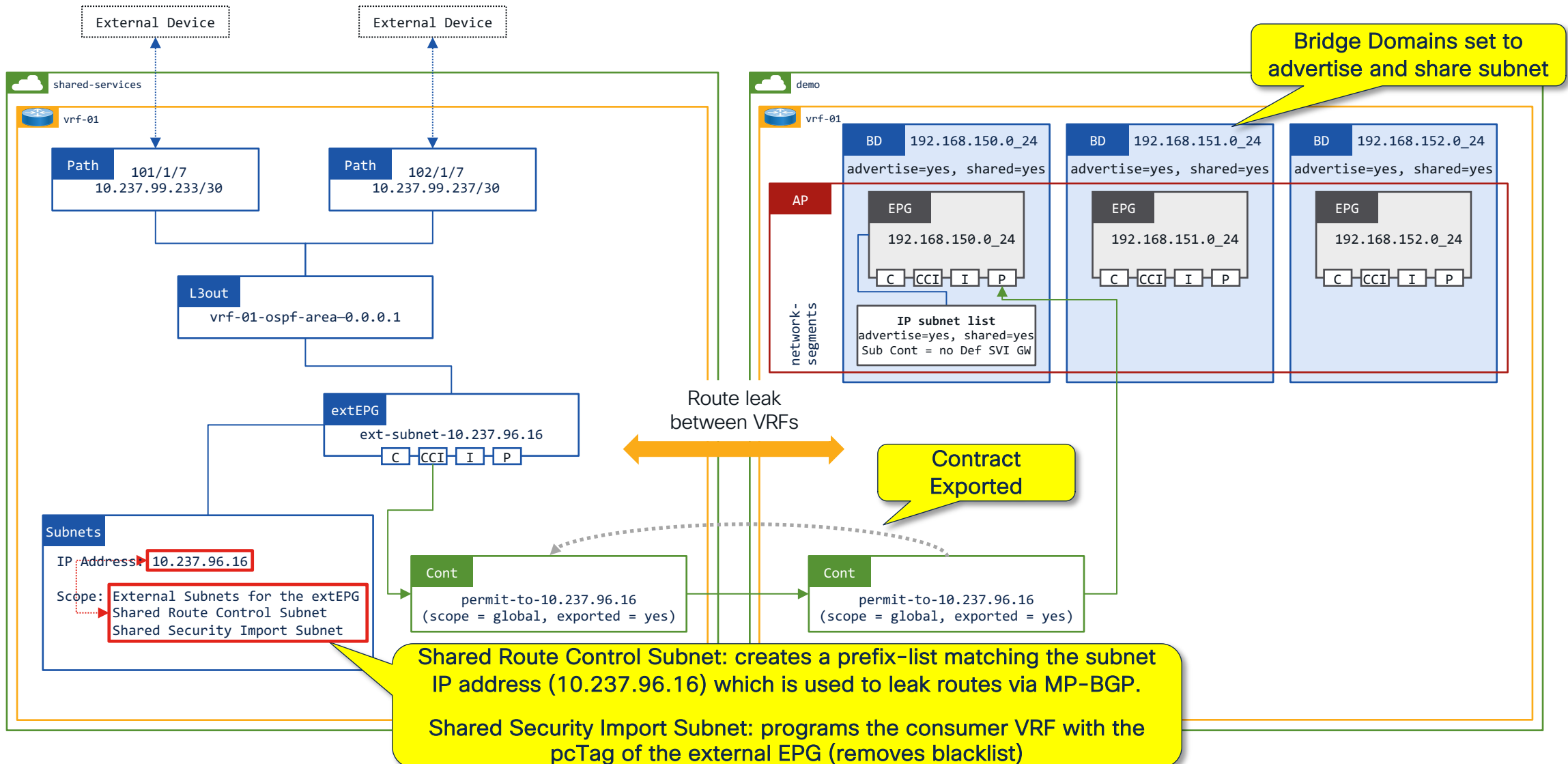


“Original” Route Leaking method – L3out is the Provider



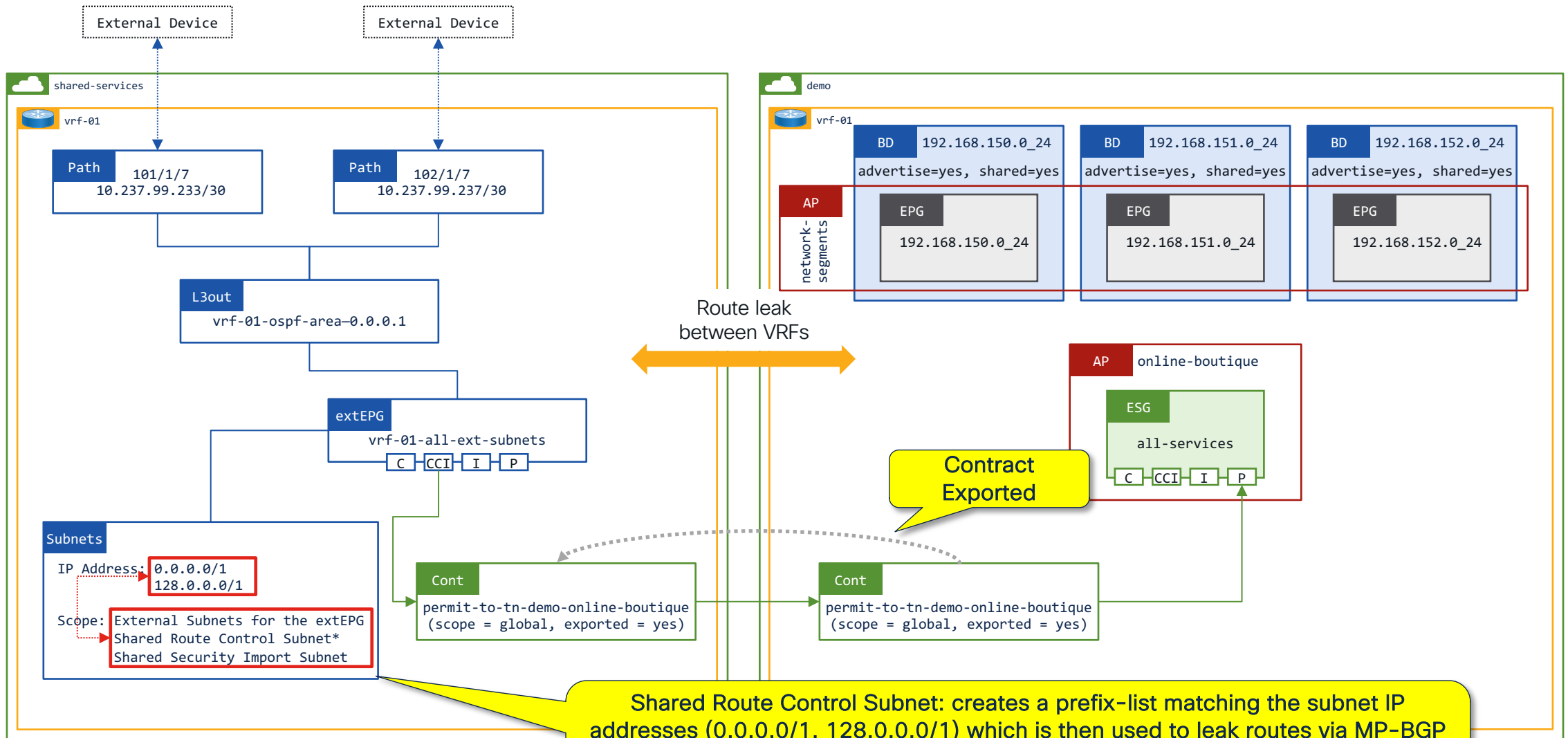
*arrows indicates direction of traffic flow i.e. from consumer to provider

“Original” Route Leaking method – L3out is the Consumer



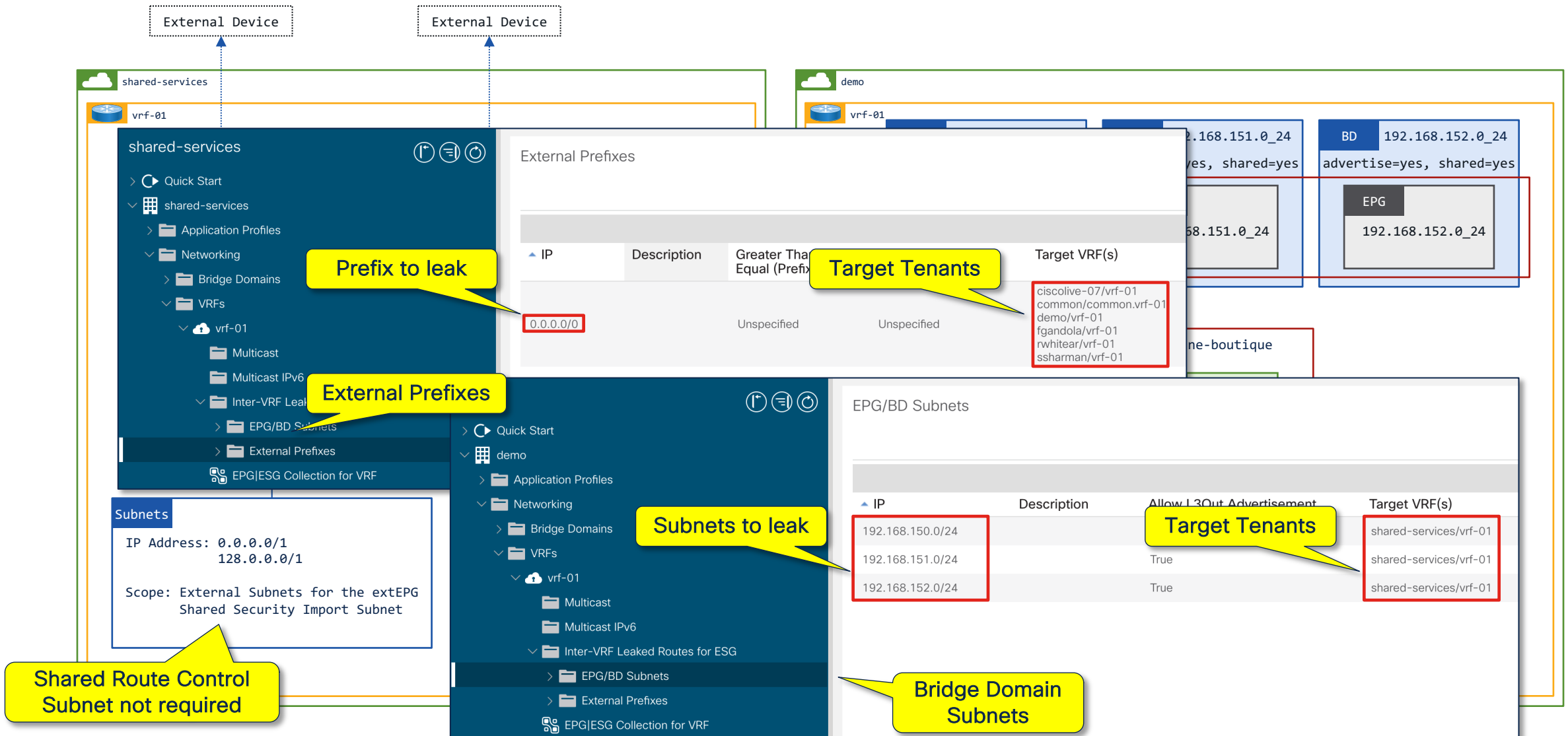
*arrows indicates direction of traffic flow i.e. from consumer to provider

Note: Prefix matching is critical



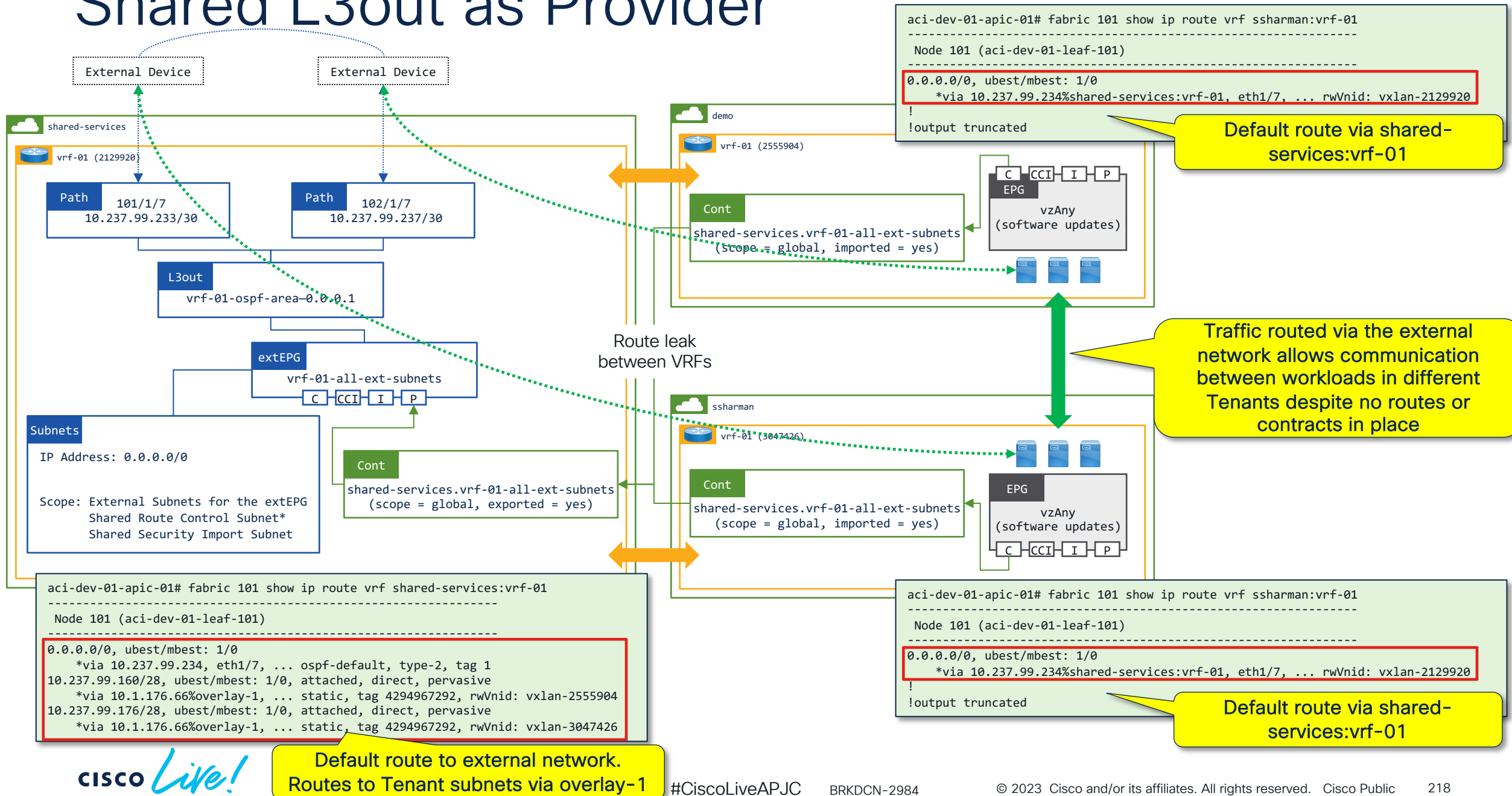
*arrows indicates direction of traffic flow i.e. from consumer to provider

“New” Shared L3out Route Leaking

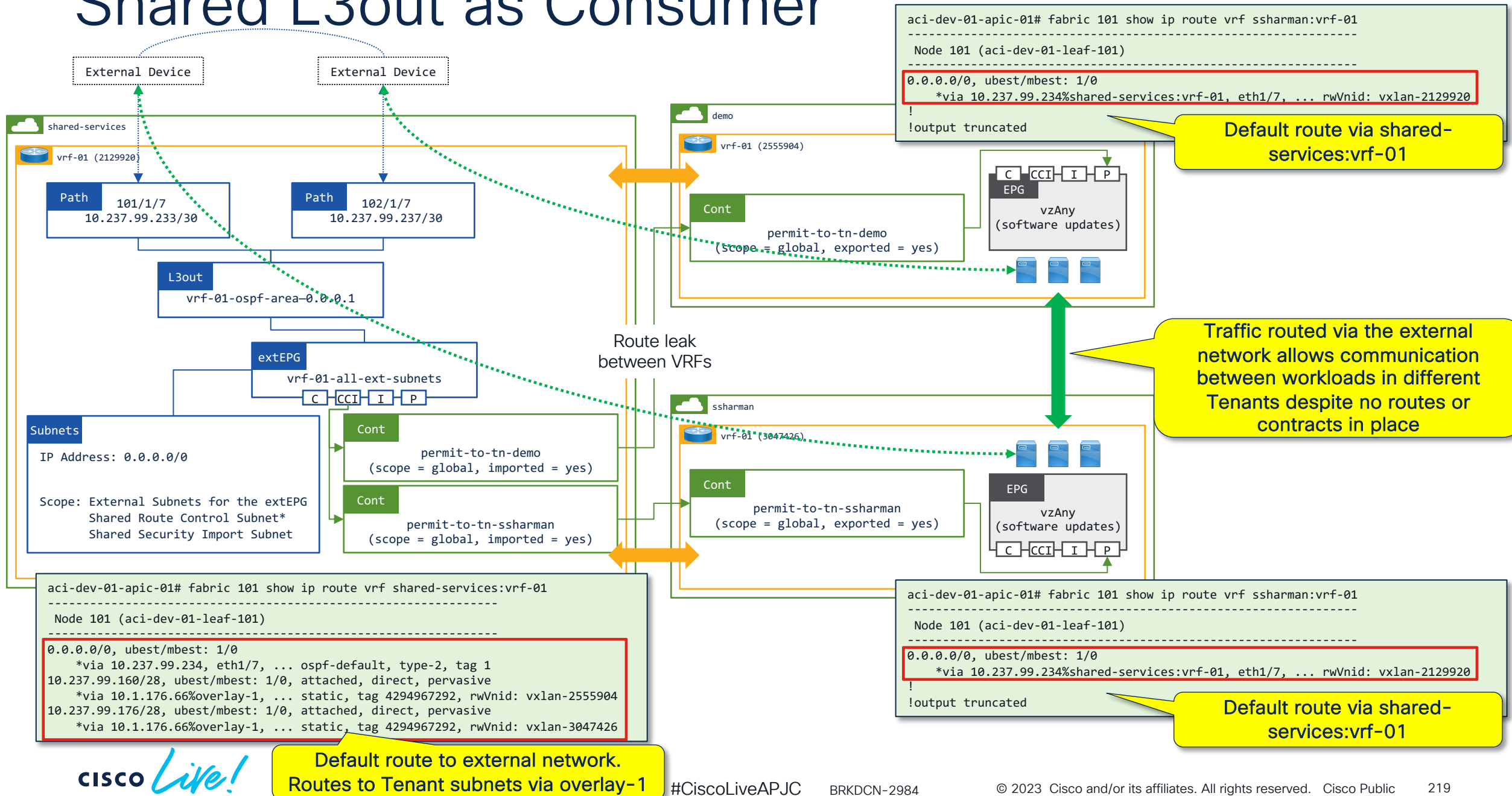


Why are we classifying with 0.0.0.0/1 and 128.0.0.0/1...?

Shared L3out as Provider



Shared L3out as Consumer



Let's understand what's happening...

First, we need the ClassIDs / pcTags so that we can understand the zoning-rules...

Get Class IDs / pcTags

Tenant > Operational > Resources IDs

Resource IDs are visible
in the GUI

Summary				Dashboard		Policy		Operational		Stats		Health		Alerts		History	
				Endpoints		Flows		Packets		Policy Tags		Resource IDs					
				Bridge Domains		VRFs		EPGs		ESGs		L3Outs		External Networks (Bridged)			
<div>Healthy</div>																	
EPG Name		EPG Alias				Class ID				Scope							
all-external-subnets						41				2129920							

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

System: Reserved range
Global: Globally significant range
Local: Locally significant range to the VRF

Get Class IDs / pcTags from the CLI

```
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	Consumed Contracts
shared-services-	vrf-01	2129920	enforced	46	-

shared-services:vrf-01 uses
VXLAN Encap/Scope 2129920
and pcTag 46 (Globally significant)

```
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/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 ext EPG
uses VXLAN Encap/Scope 2129920
and pcTag 41 (Globally significant)

```
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	Consumed Contracts
demo	vrf-01	2555904	enforced	49153	-

demo:vrf-01 uses VXLAN
Encap/Scope 2555904 and pcTag
49153 (Locally significant)

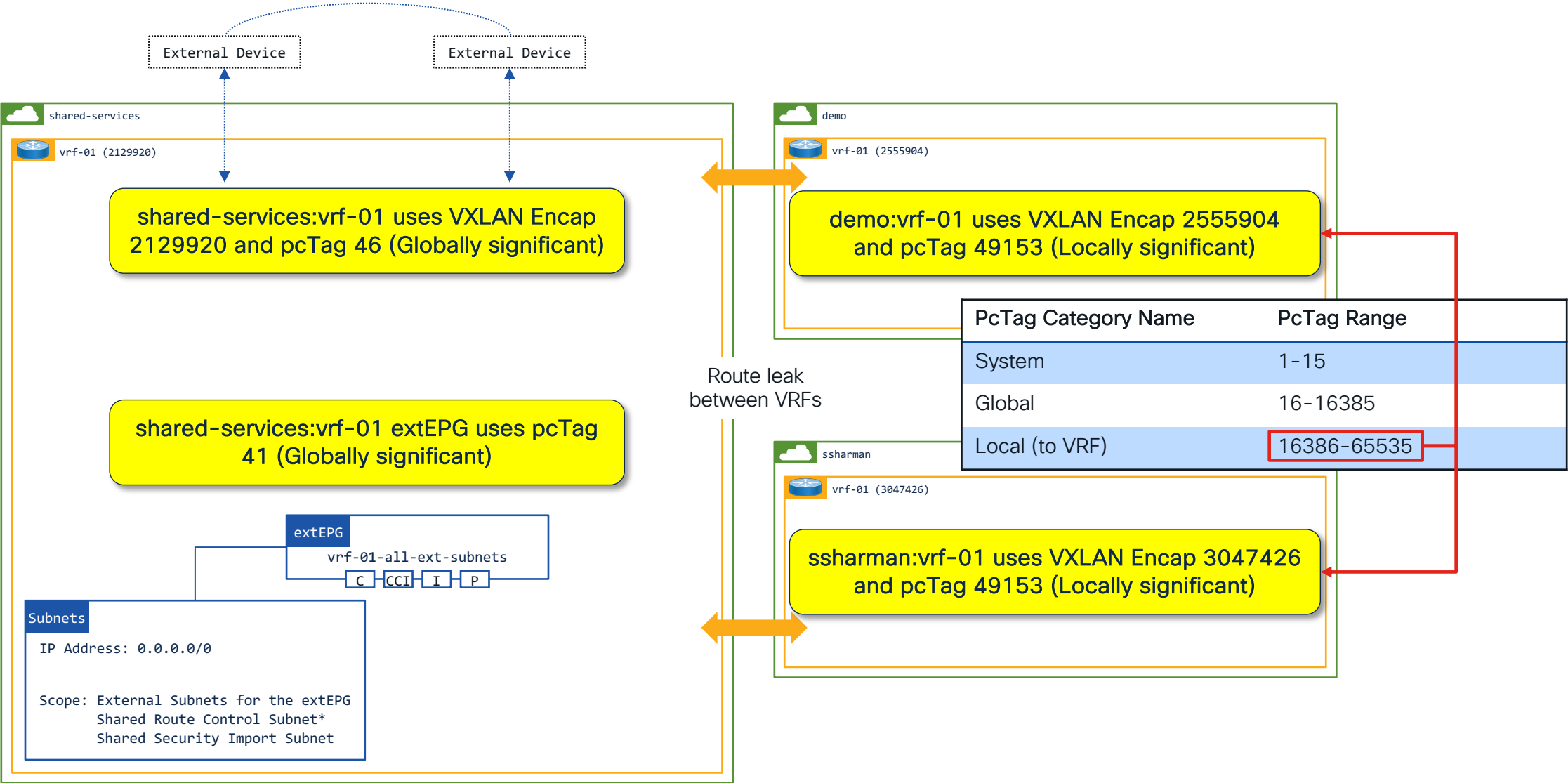
```
aci-dev-01-apic-01# show vrf vrf-01 detail | grep ssharman -B 4 A 1
```

VRF Information:

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

ssharman:vrf-01 uses VXLAN
Encap/Scope 3047426 and pcTag
49153 (Locally significant)

Shared L3out as Consumer



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

Shared L3out as Consumer – extEPG zoning-rules

```
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

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

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

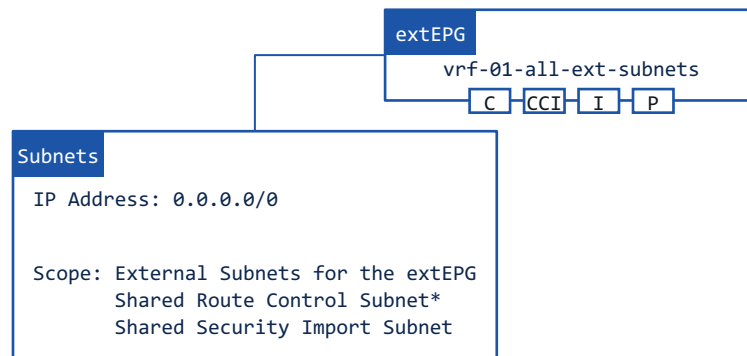
Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope

If there are no zoning-rules from the extEPG – how is traffic flowing between Tenants/VRFs?

demo:vrf-01 uses VXLAN Encap 2555904 and pcTag 49153 (Locally significant)

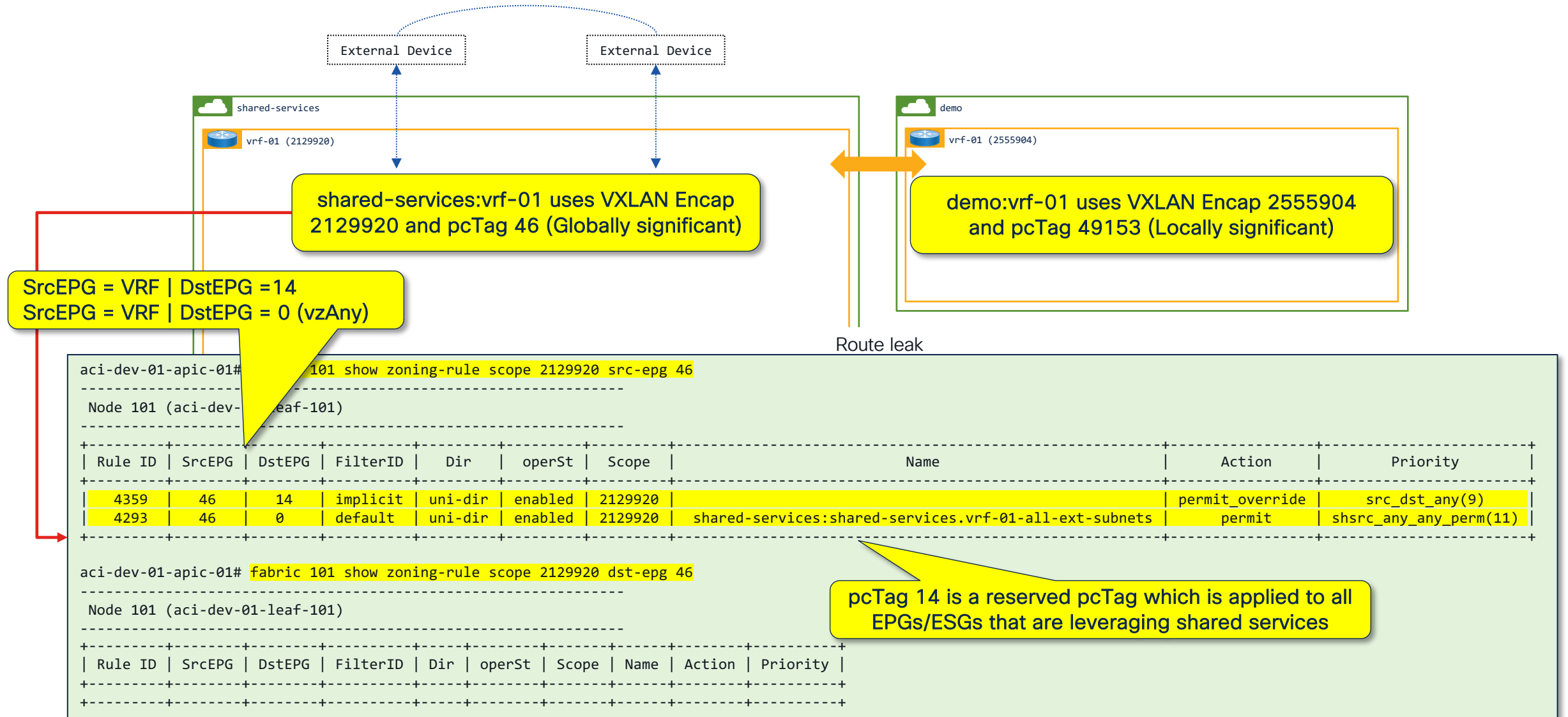
Route leak between VRFs

shared-services:vrf-01 extEPG uses pcTag 41 (Globally significant)



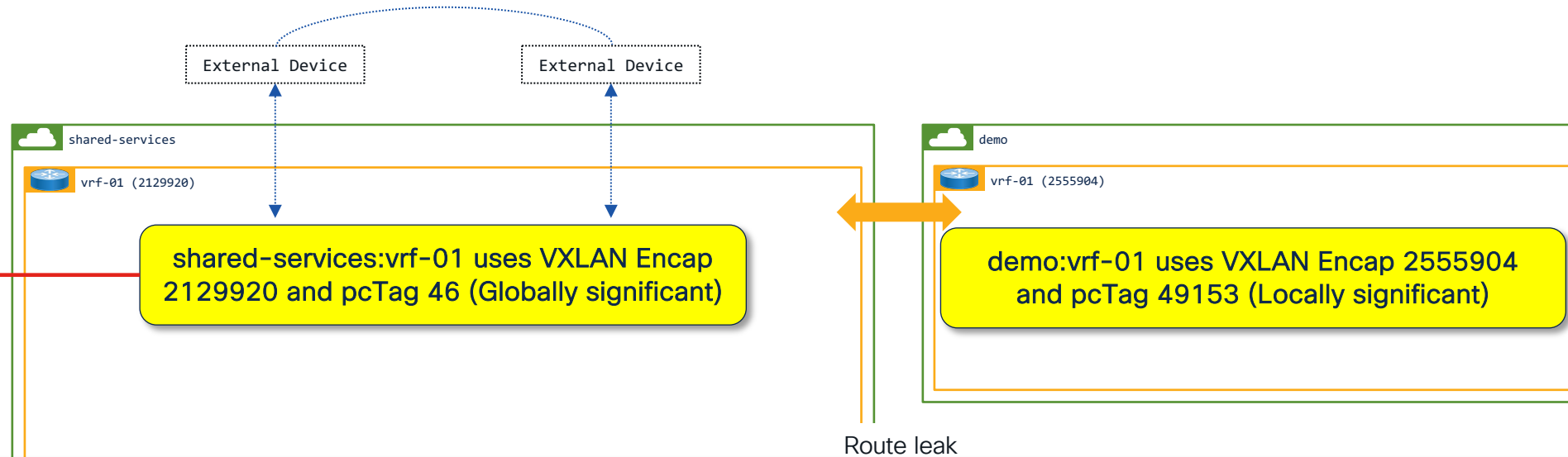
ssharmarman:vrf-01 uses VXLAN Encap 3047426 and pcTag 49153 (Locally significant)

Shared L3out as Consumer – VRF zoning-rules



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
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)

SrcEPG = 0 (vzAny)
DstEPG = 15 (extEPG with 0.0.0.0/0)

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

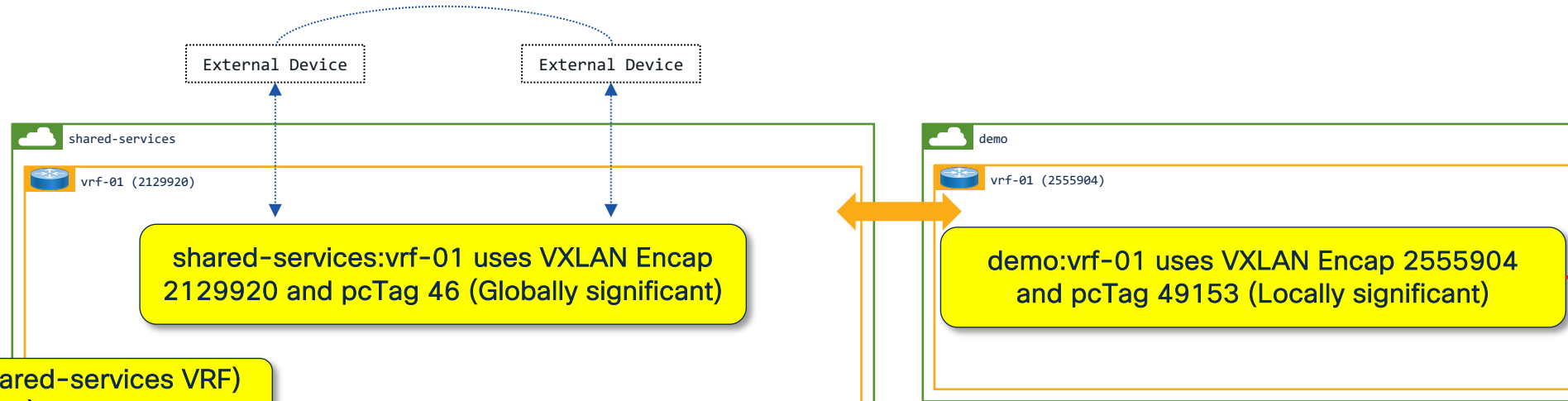
```
Node 101 (aci-dev-01-leaf-101)
```

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

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

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



SrcEPG = 46 (shared-services VRF)
DstEPG = 0 (vzAny)

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

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 15

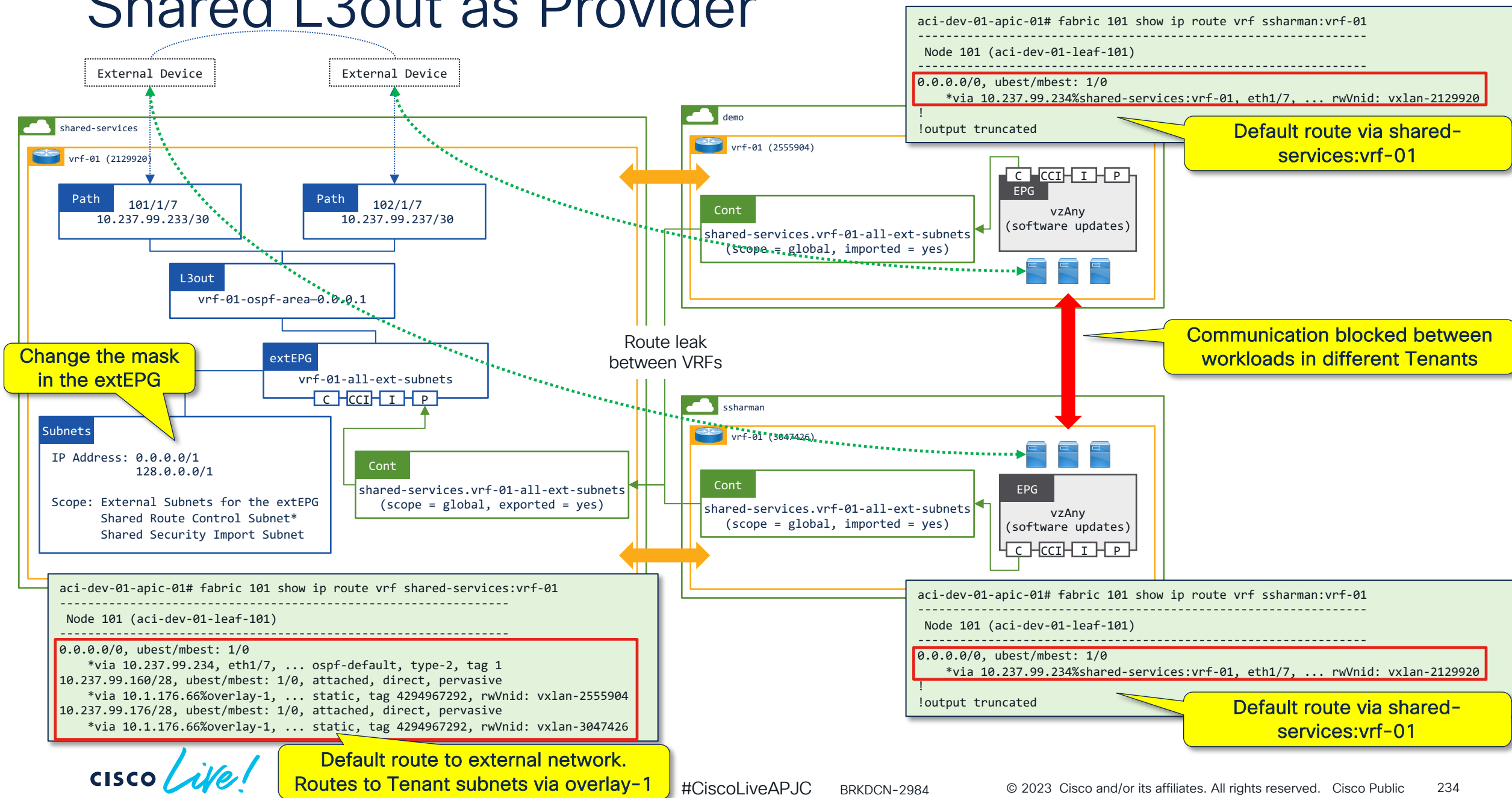
aci-dev-01-apic-01#

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)

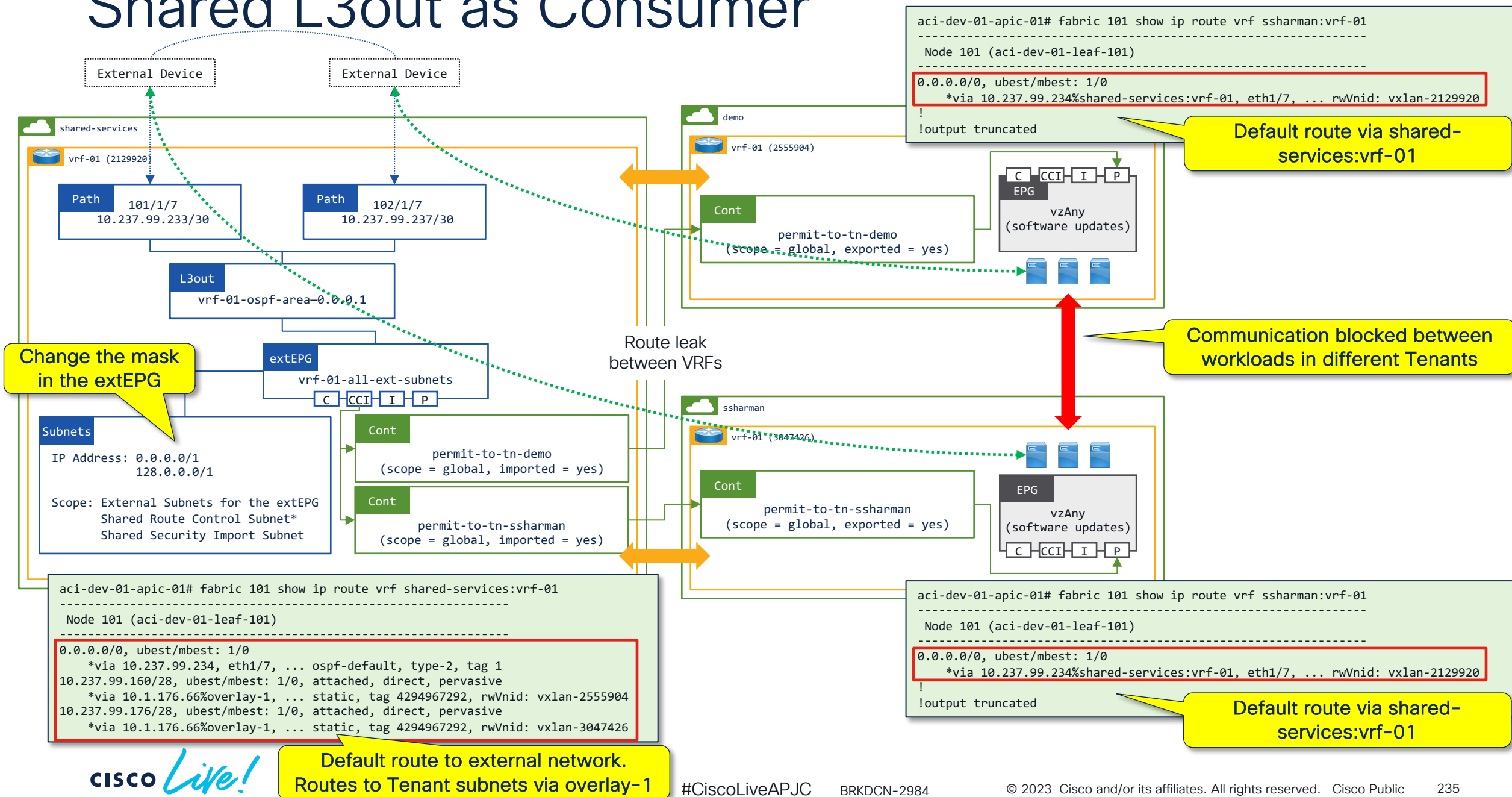
SrcEPG = 0 (vzAny)
DstEPG = 15 (extEPG with 0.0.0.0/0)

How do we resolve the unexpected communication...?

Shared L3out as Provider



Shared L3out as Consumer



So, what's changed...?

Get Class IDs / pcTags

```
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	Consumed Contracts
shared-services-	vrf-01	2129920	enforced	16386	-

shared-services:vrf-01 uses
VXLAN Encap/Scope 2129920 and
pcTag 16386 (Locally significant)

```
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/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 ext EPG
uses VXLAN Encap/Scope 2129920
and pcTag 41 (Globally significant)

```
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	Consumed Contracts
demo	vrf-01	2555904	enforced	49153	-

demo:vrf-01 uses VXLAN
Encap/Scope 2555904 and pcTag
49153 (Locally significant)

```
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	Consumed Contracts
ssharman	vrf-01	3047426	enforced	49153	-

ssharman:vrf-01 uses VXLAN
Encap/Scope 3047426 and pcTag
49153 (Locally significant)

Shared L3out as Consumer – extEPG zoning-rules

```
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

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

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

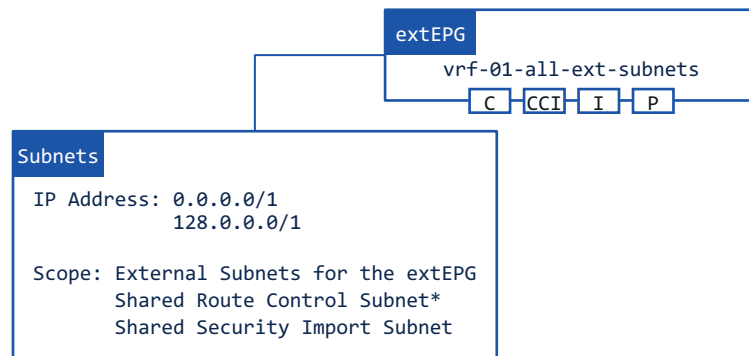
Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope
4487	0	41	default	bi-dir	enabled	2129920

The zoning rules now use the ClassID of the extEPG rather than the VRF ClassID

demo:vrf-01 uses VXLAN Encap 2555904 and pcTag 49153 (Locally significant)

Route leak between VRFs

shared-services:vrf-01 extEPG uses pcTag 41 (Globally significant)



ssharmar:vrf-01 uses VXLAN Encap 3047426 and pcTag 49153 (Locally significant)

What's the bottom line...

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

Prepare the fabric for L4-L7 Service Insertion

ACI Endpoint Update App (optional)

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

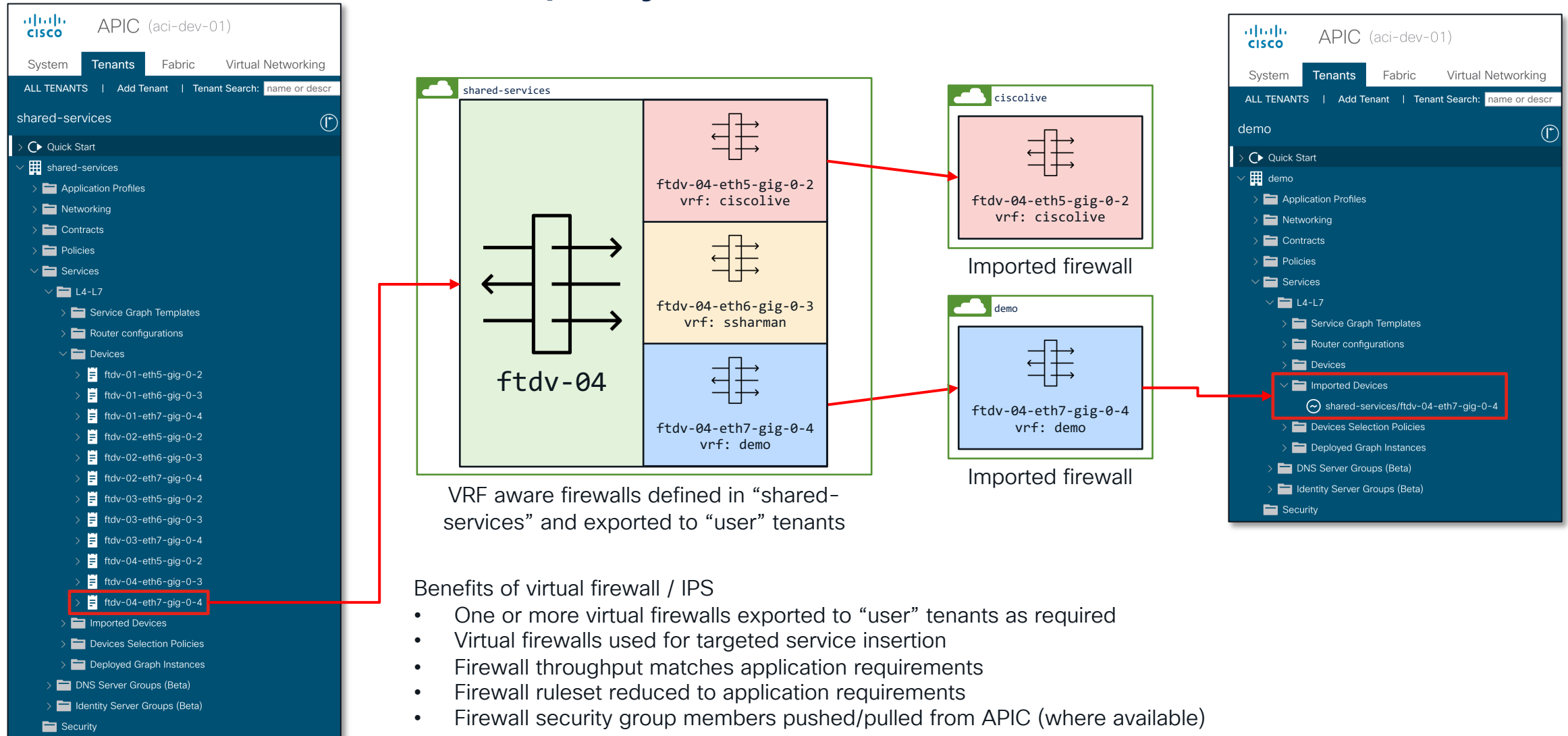
The screenshot displays the Cisco APIC (aci-dev-01) interface. The 'Apps' tab is selected, showing three applications: ELAM Assistant, ACI Endpoint Update, and Nexus Insights Cloud Connector. The 'ACI Endpoint Update' app is highlighted with a red box. A red line connects this box to the 'External Attributes' menu item in the Firewall Management Center (FMC) interface, which is also highlighted with a red box. The FMC interface shows the 'Dynamic Objects' table with the following data:

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...?

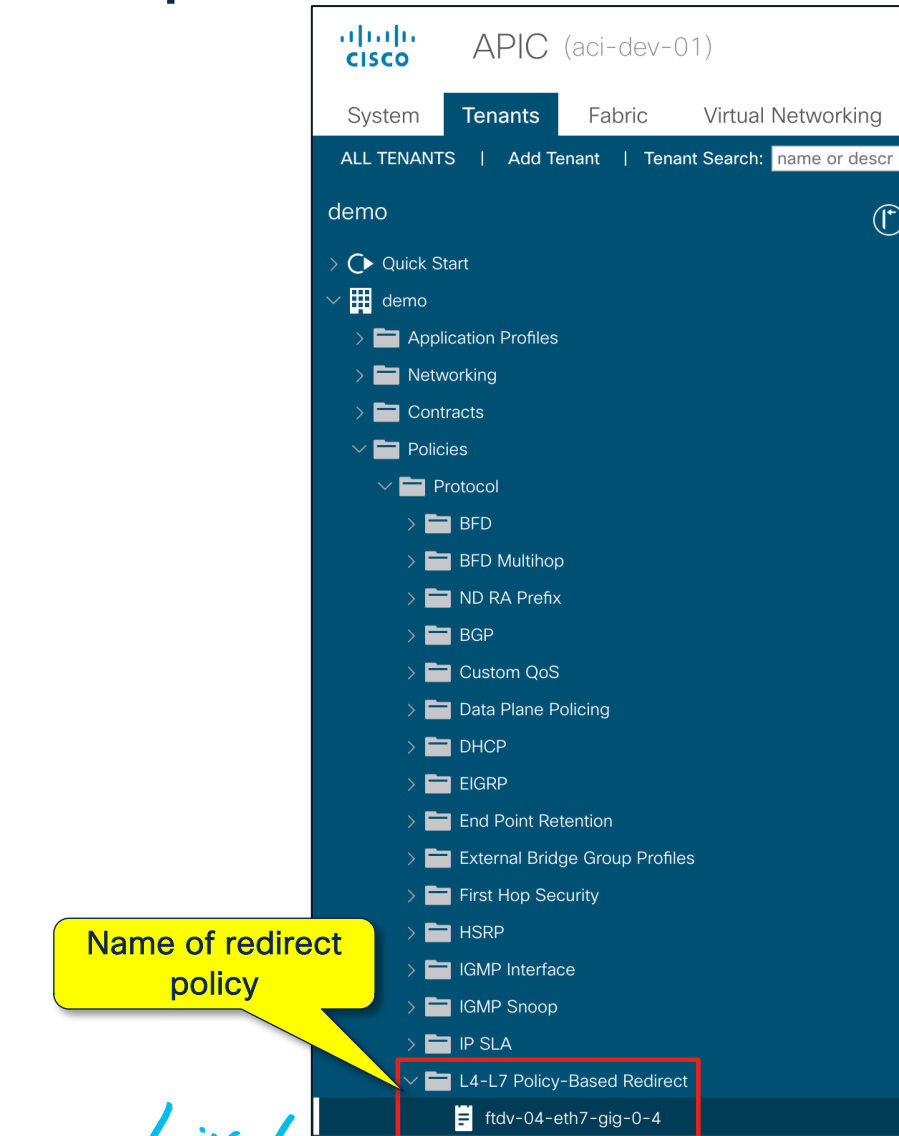
“common” tenant, “shared-services” tenant, or
“workload/user” tenant...

Virtual firewall deployment



Setting up PBR to a one arm attached firewall...

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 Template** and **Device Selection Policy**.

Service Graph Template: The left pane shows the **demo** tenant under the **Services** tab. A red box highlights the **redirect-to-ftdv-04-gig-0-4** service graph template. Below it, a diagram shows the **Consumer** EPG connected to the **Provider** EPG via a **Function Node - N1**. The **ftdv-04-eth7-gig-0-4** information is shown below the diagram, indicating **Firewall: Routed** and **Route Redirect: true**.

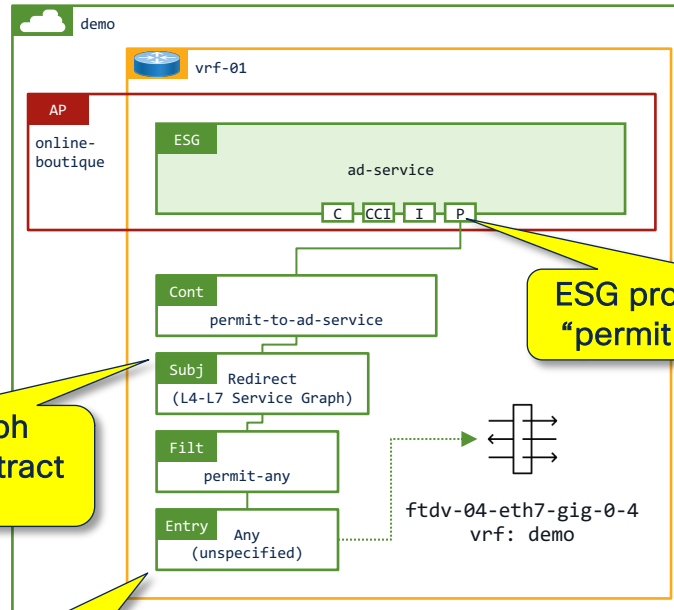
Device Selection Policy: The right pane shows the **demo** tenant under the **Services** tab. A red box highlights the **any-redirect-to-ftdv-04-gig-0-4-N1** device selection policy. Below it, a diagram shows the **Consumer** EPG connected to the **Provider** EPG via a **Function Node - N1**. The **ftdv-04-eth7-gig-0-4** information is shown below the diagram, indicating **Firewall: Routed** and **Route Redirect: true**.

Configuration Details: The right pane shows the configuration for the **any-redirect-to-ftdv-04-gig-0-4-N1** device selection policy. The 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

Yellow callouts highlight the **Firewall interface and Bridge Domain for the Consumer interface** and **Firewall interface and Bridge Domain for the Provider interface**. A red box highlights the **PBR target** configuration.

Step 3: Apply Service Graph to Contract Subject



Service Graph applied to contract subject

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

Service Graph is deployed once the contract is consumed

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

Contract Scope

Property

Name: permit-to-ad-service

Alias:

Global Alias:

Scope: VRF

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

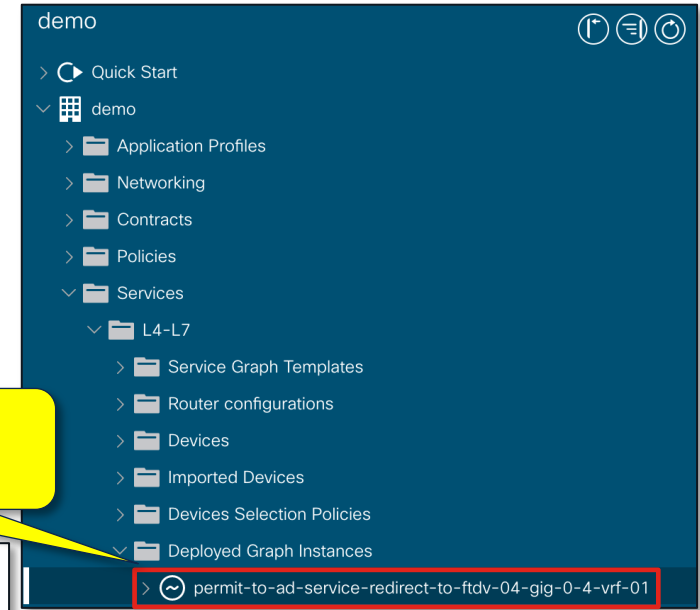
Contract and Subject

permit-to-ad-service

redirect

Contract and Subject

Service Graph redirect

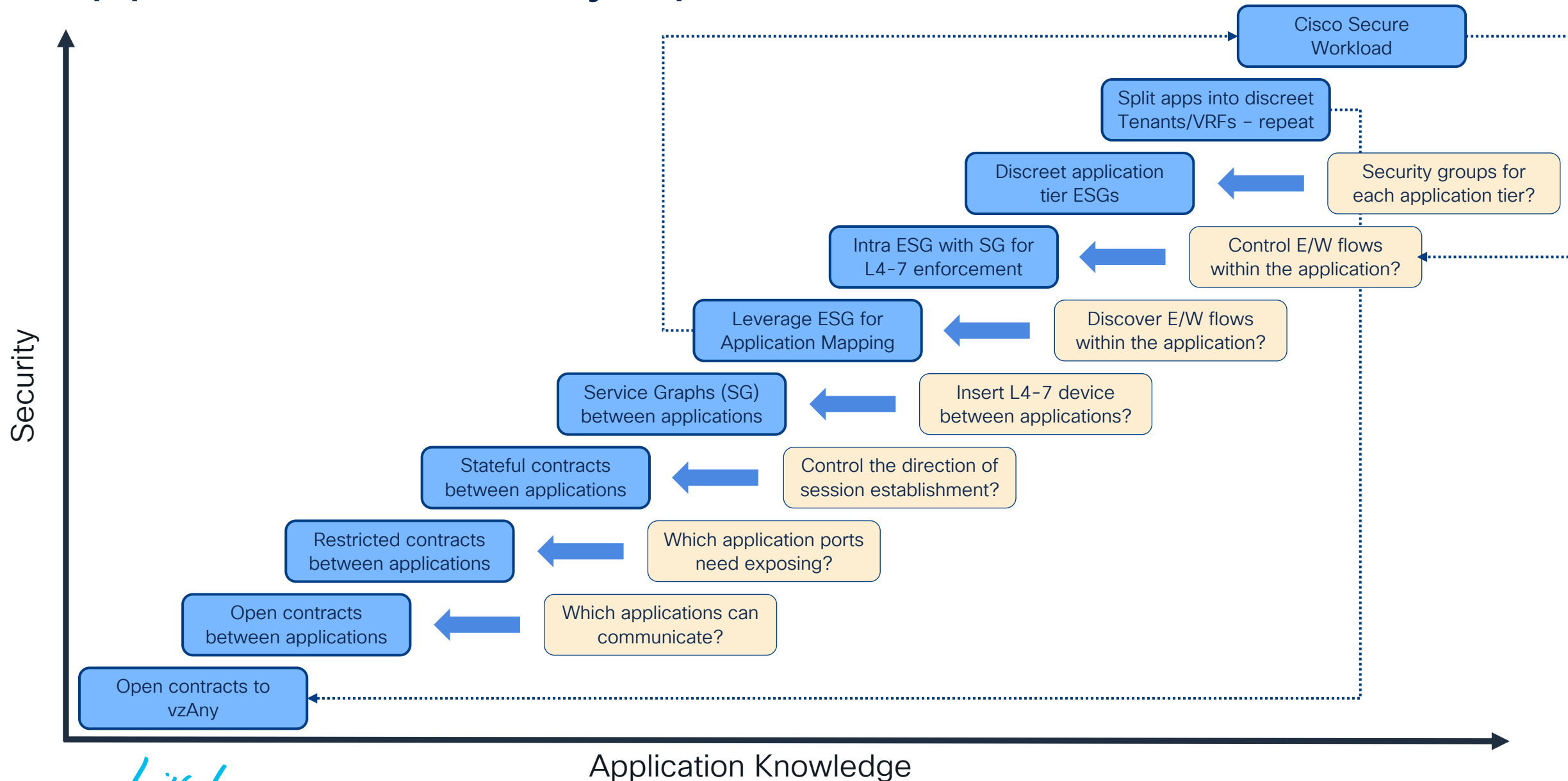


Tightening Security...

How would you like to secure your applications...?

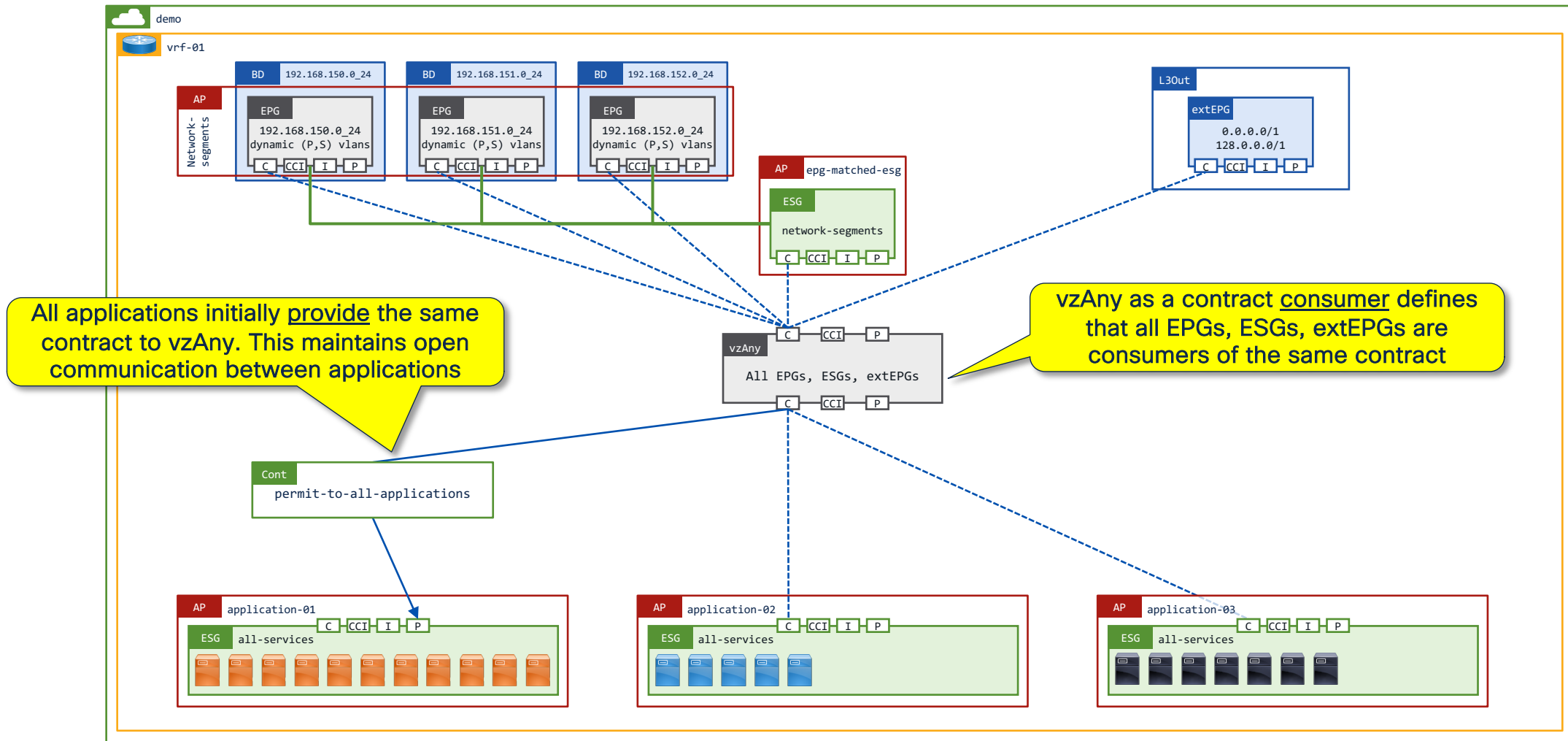


Application security options...



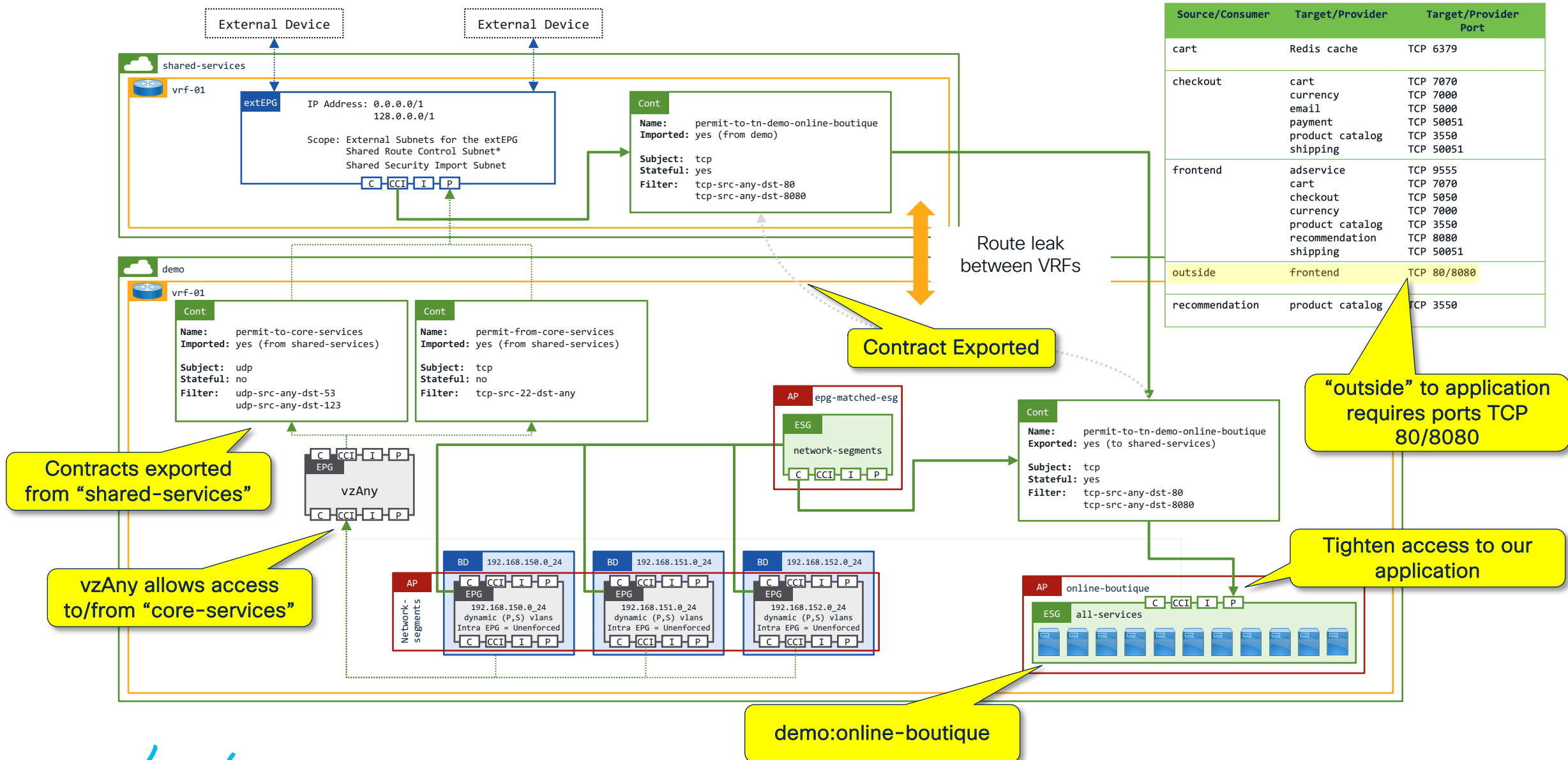
Assign endpoints to the correct security groups...

Assign endpoints by Tagging the IP to the correct group...

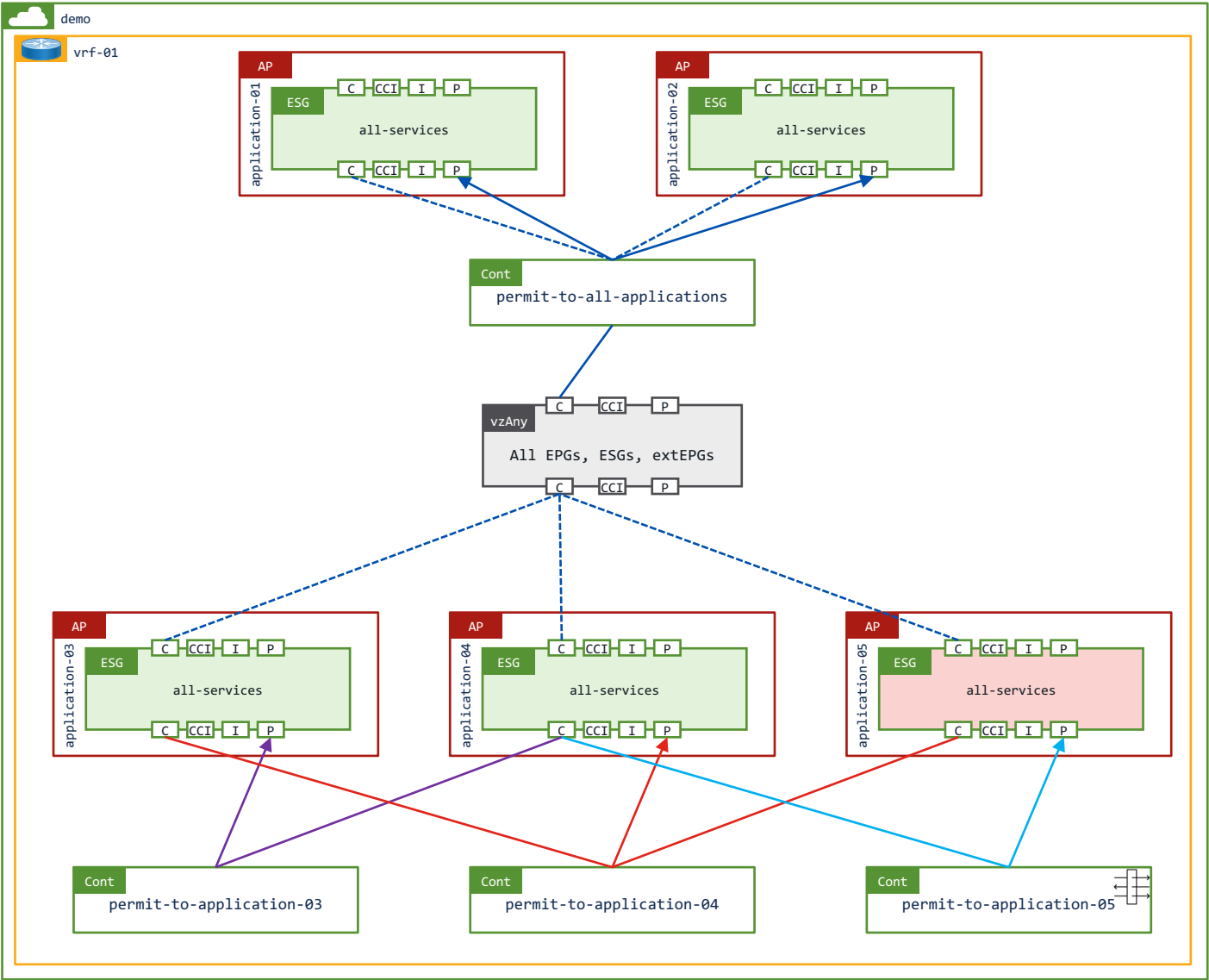


Let's tighten the contract to our online-boutique application...

Tighten access to our online-boutique application...



Defining application security

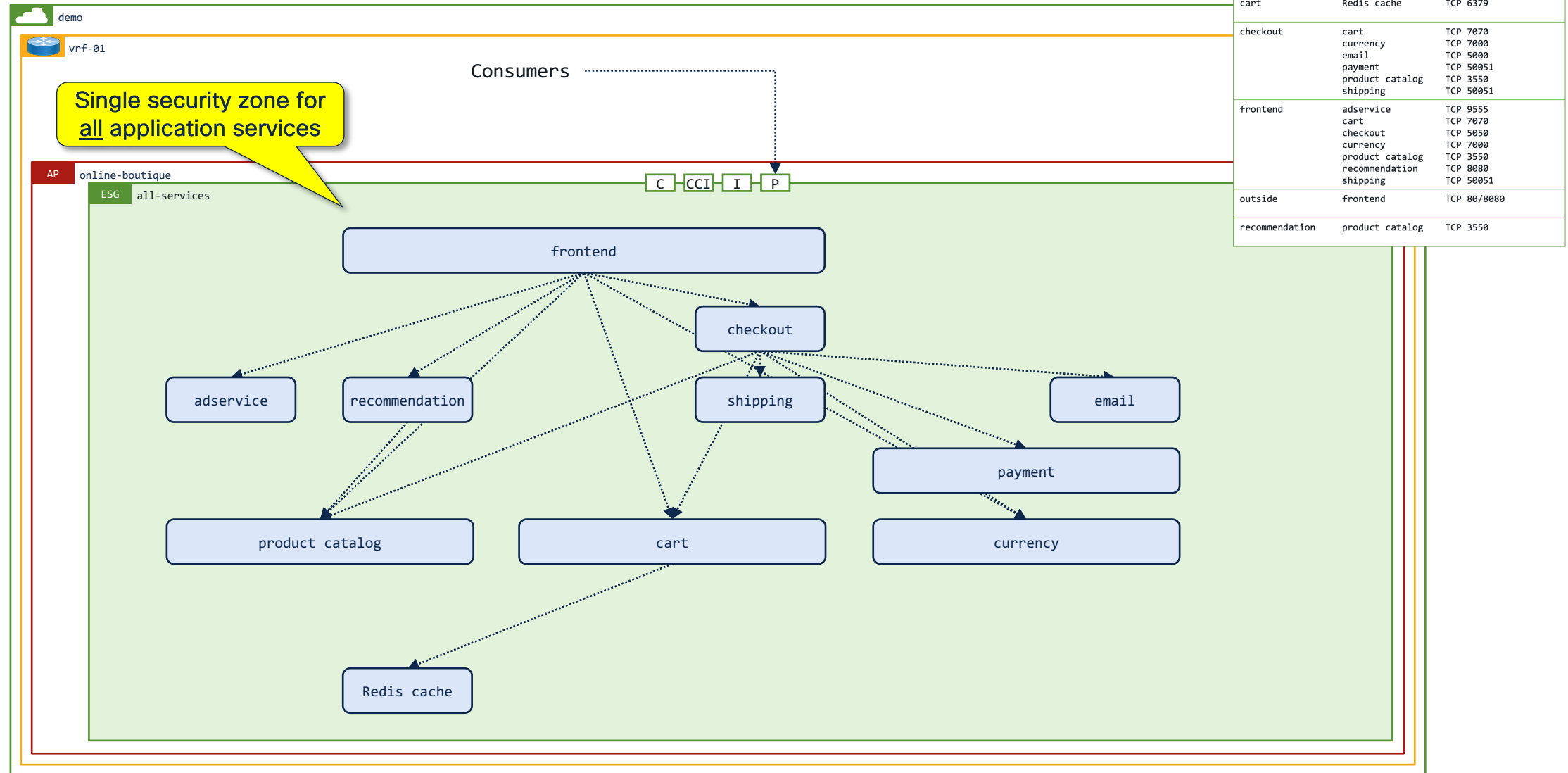


Application Name	Contract	Application Name
application-01	permit-to-all-applications (vzAny)	application-02
	Filter: permit-any	application-03
		application-04
		application-05
application-02	permit-to-all-applications (vzAny)	application-01
	Filter: permit-any	application-03
		application-04
		application-05
application-03	permit-to-application-03	application-04
	Filter: permit-any	
application-04	permit-to-application-04	application-03
	Filter: tcp-src-any-dst-443	application-05
application-05	permit-to-application-05	application-04
	(Service graph to FTD for inter and intra application flows)	
	Filter: permit-any	

Blueprints

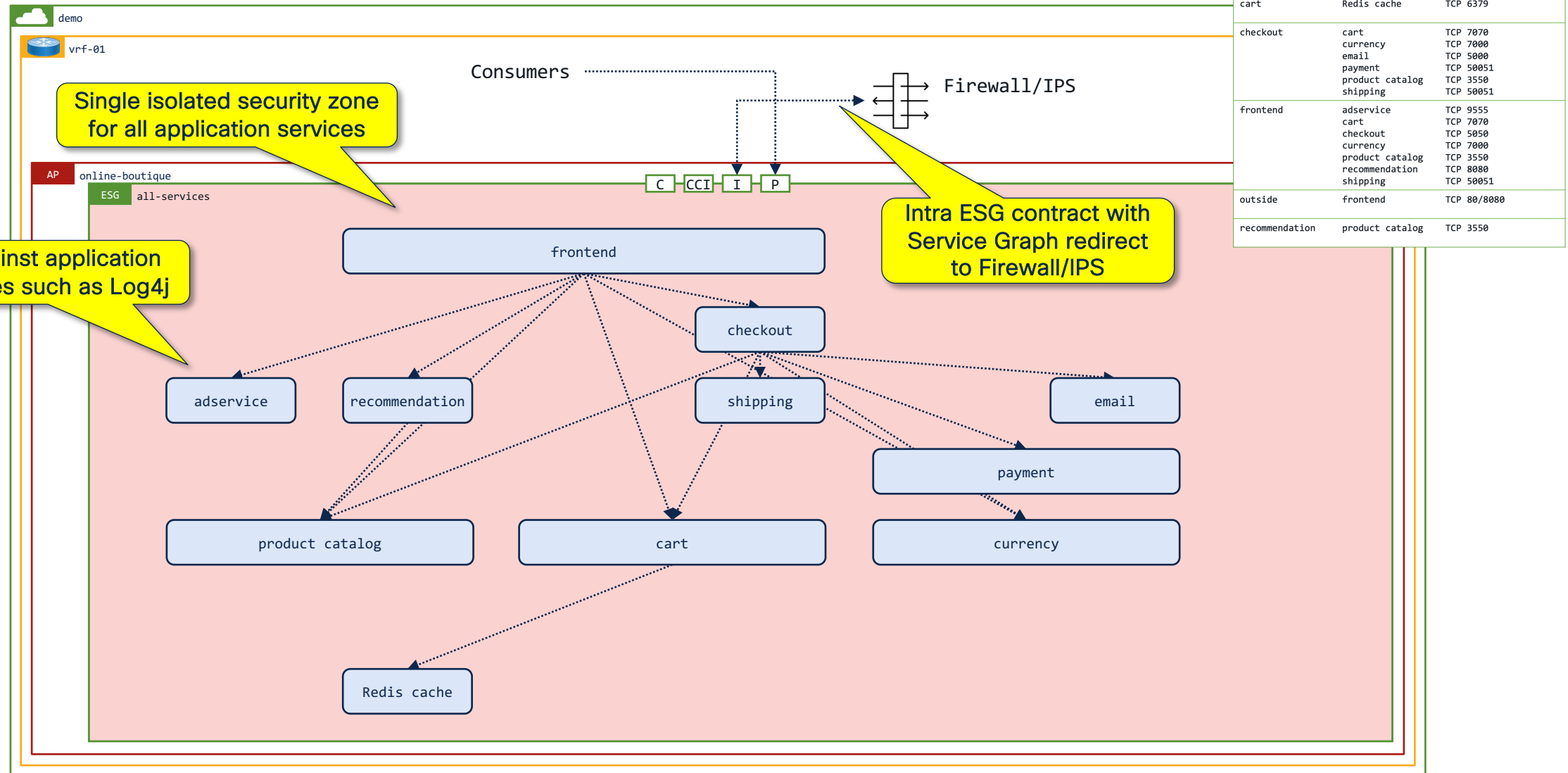
Application tiers across subnets

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



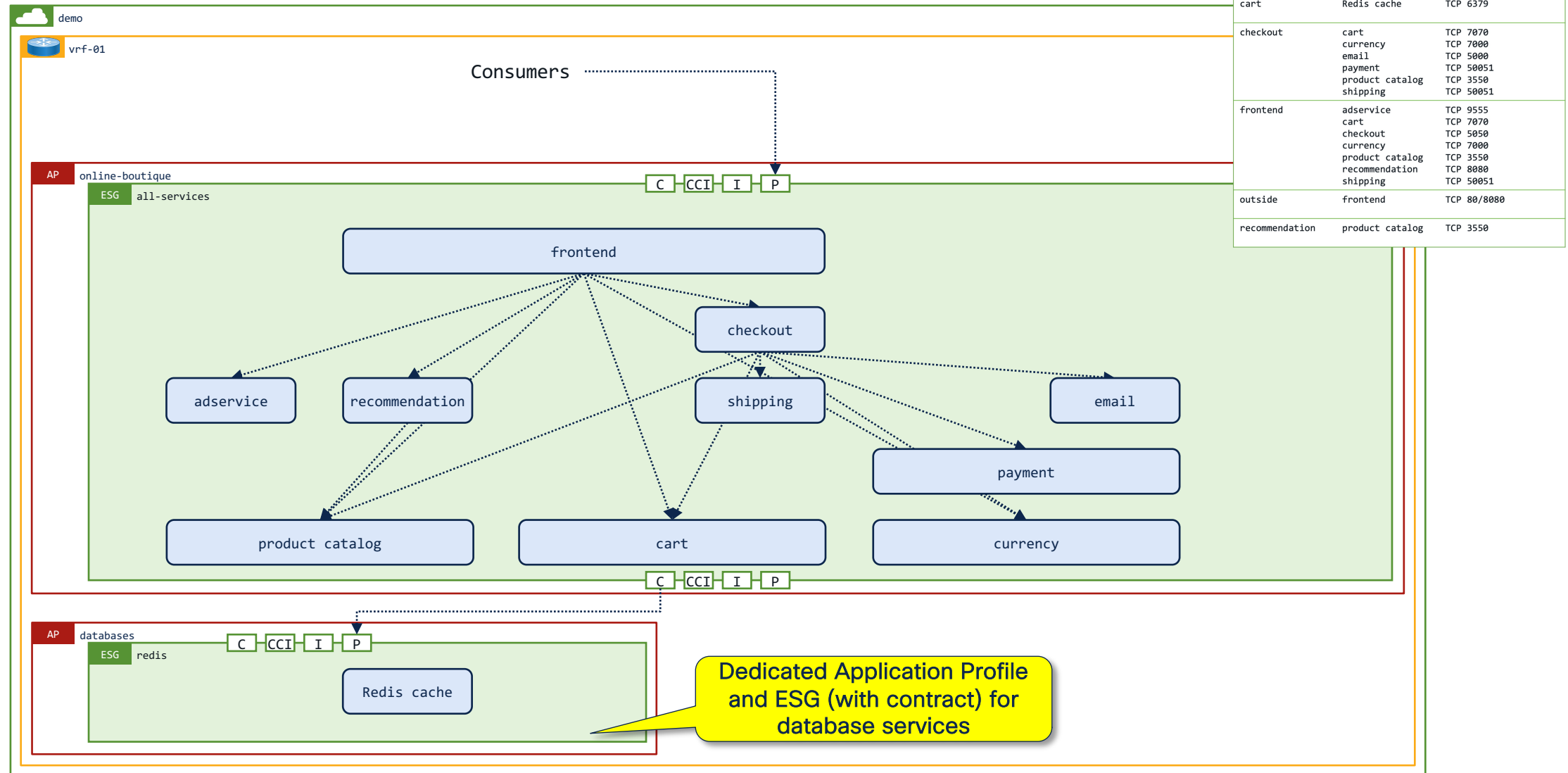
Application tiers across subnets

Application Centric Blueprint #2 – Intra ESG Isolation



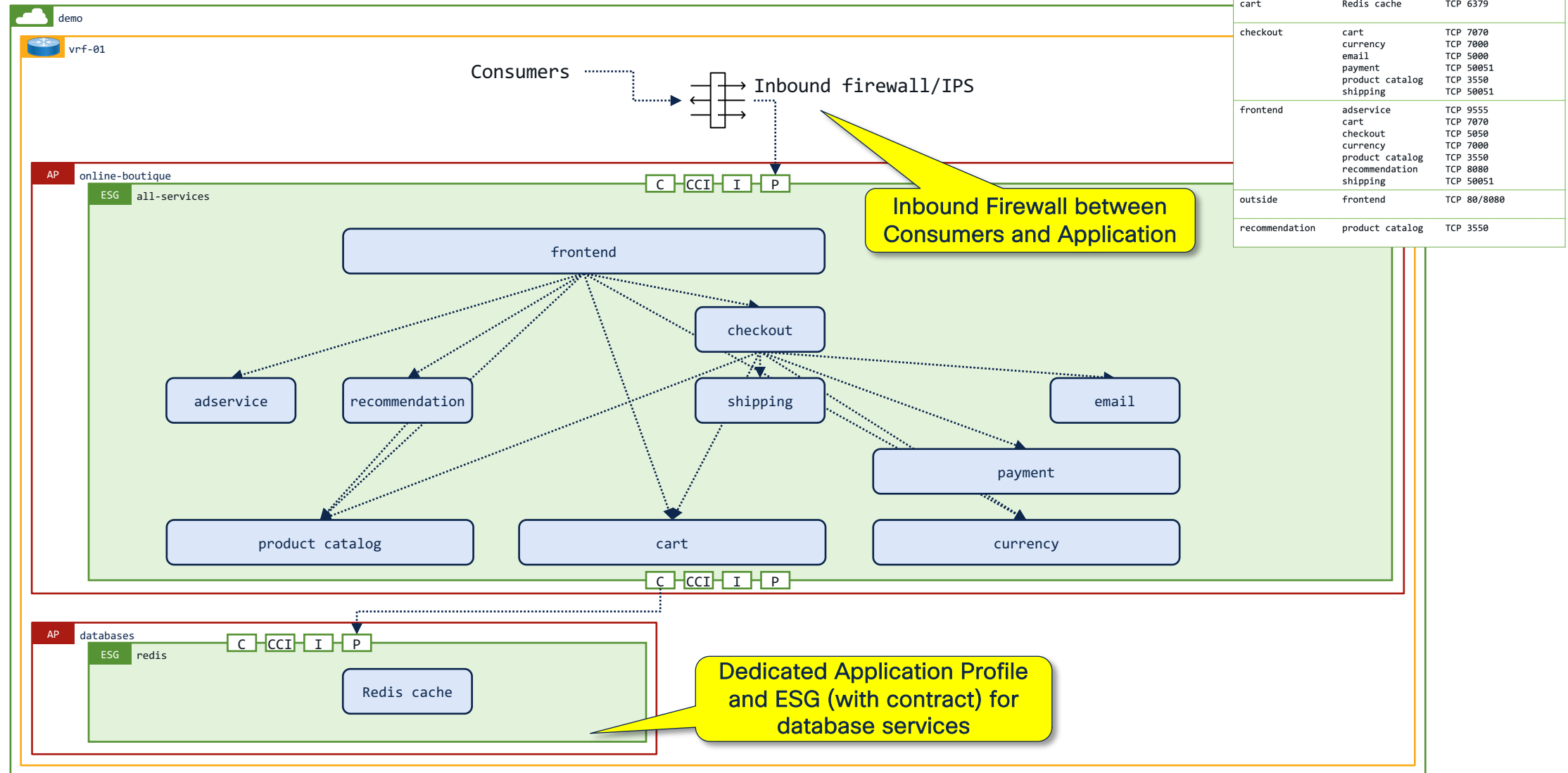
Application tiers across subnets

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



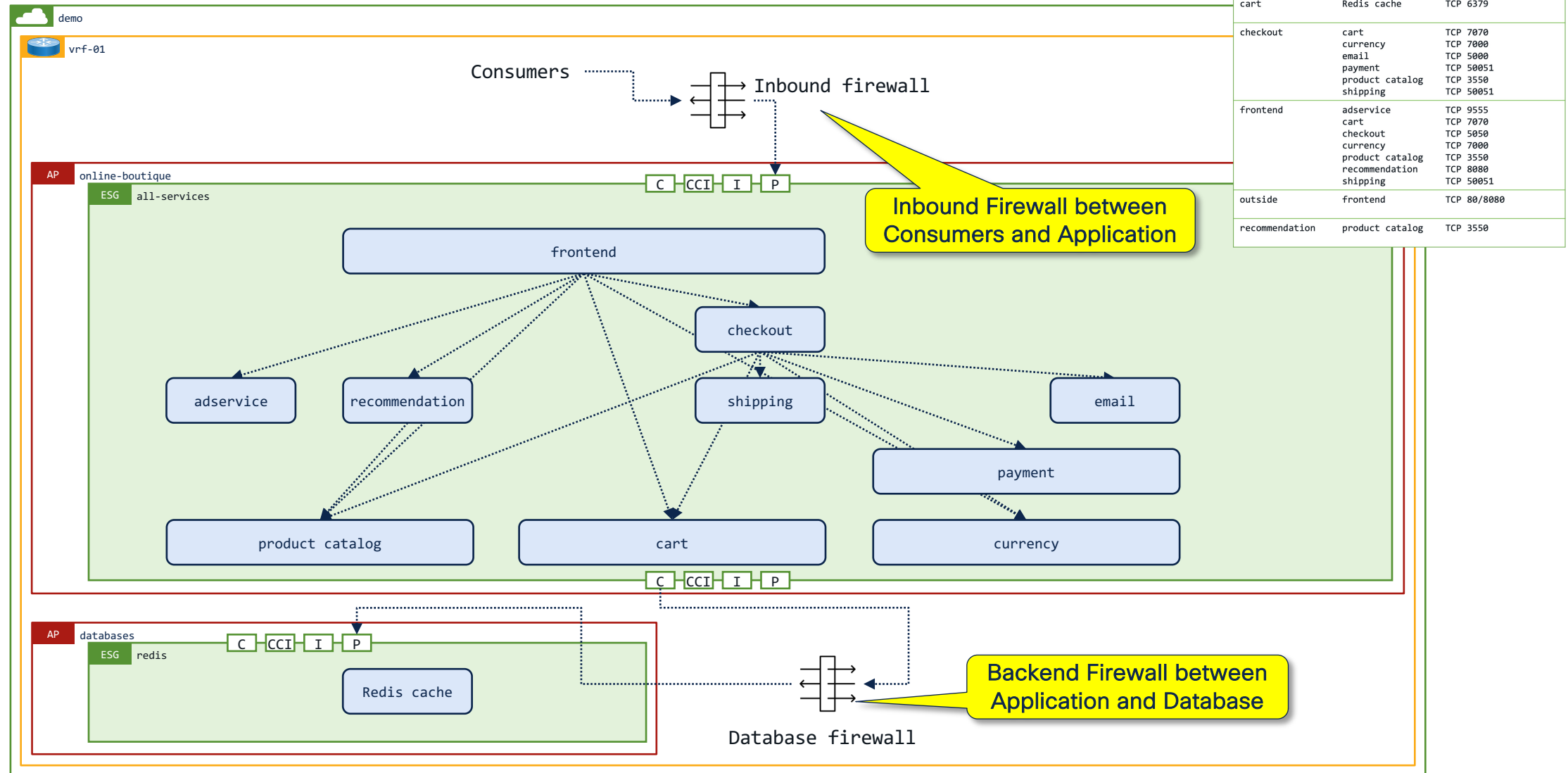
Application tiers across subnets

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



Application tiers across subnets

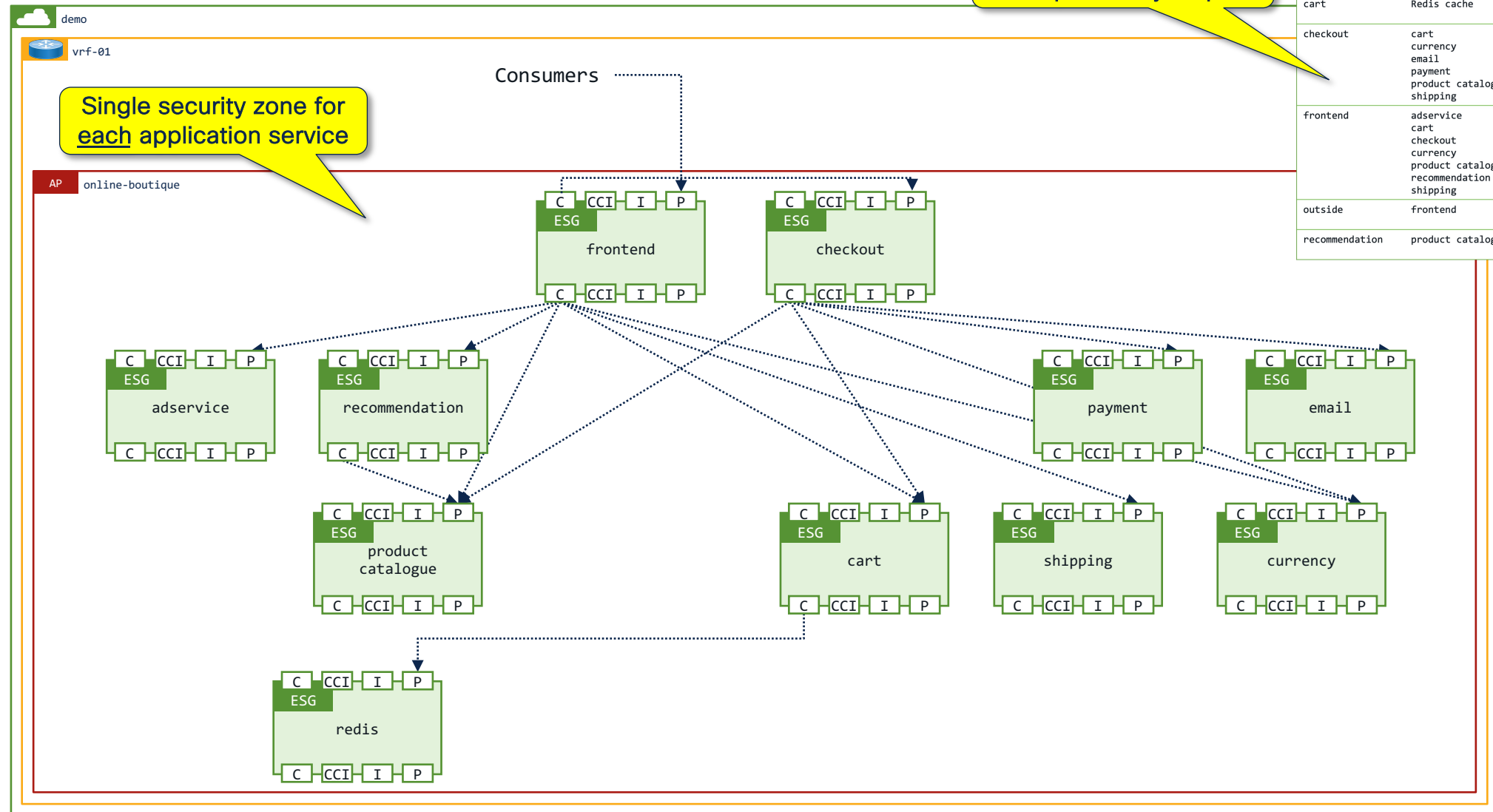
Application Centric Blueprint #5 – Inbound firewall/IPS + backend firewall/IPS



Application tiers across subnets

Application Centric Blueprint #6 – ESG per application tier

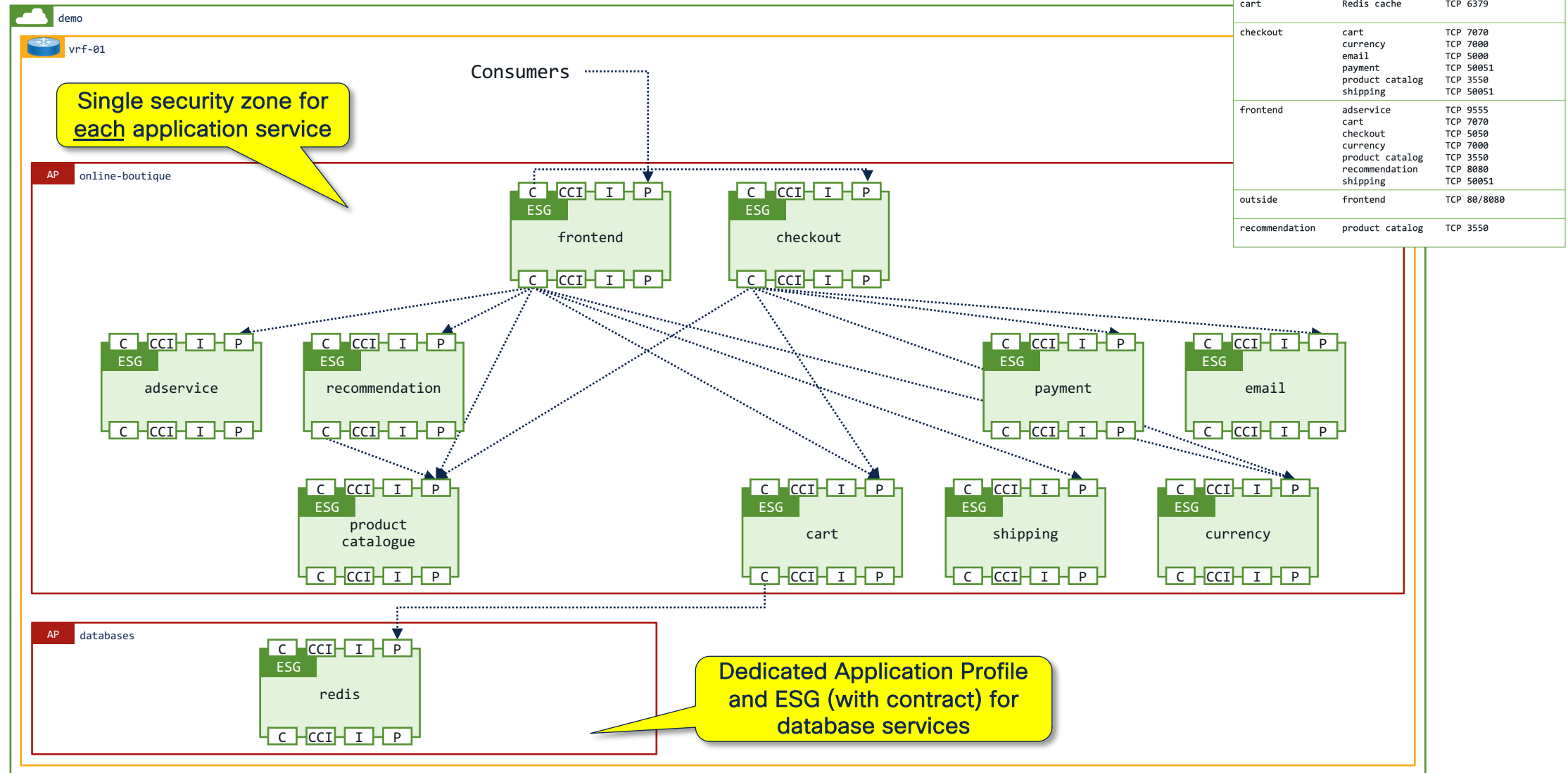
Requires application dependency map



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
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP 3550
outside	recommendation	TCP 8080
	shipping	TCP 50051
recommendation	product catalog	TCP 3550

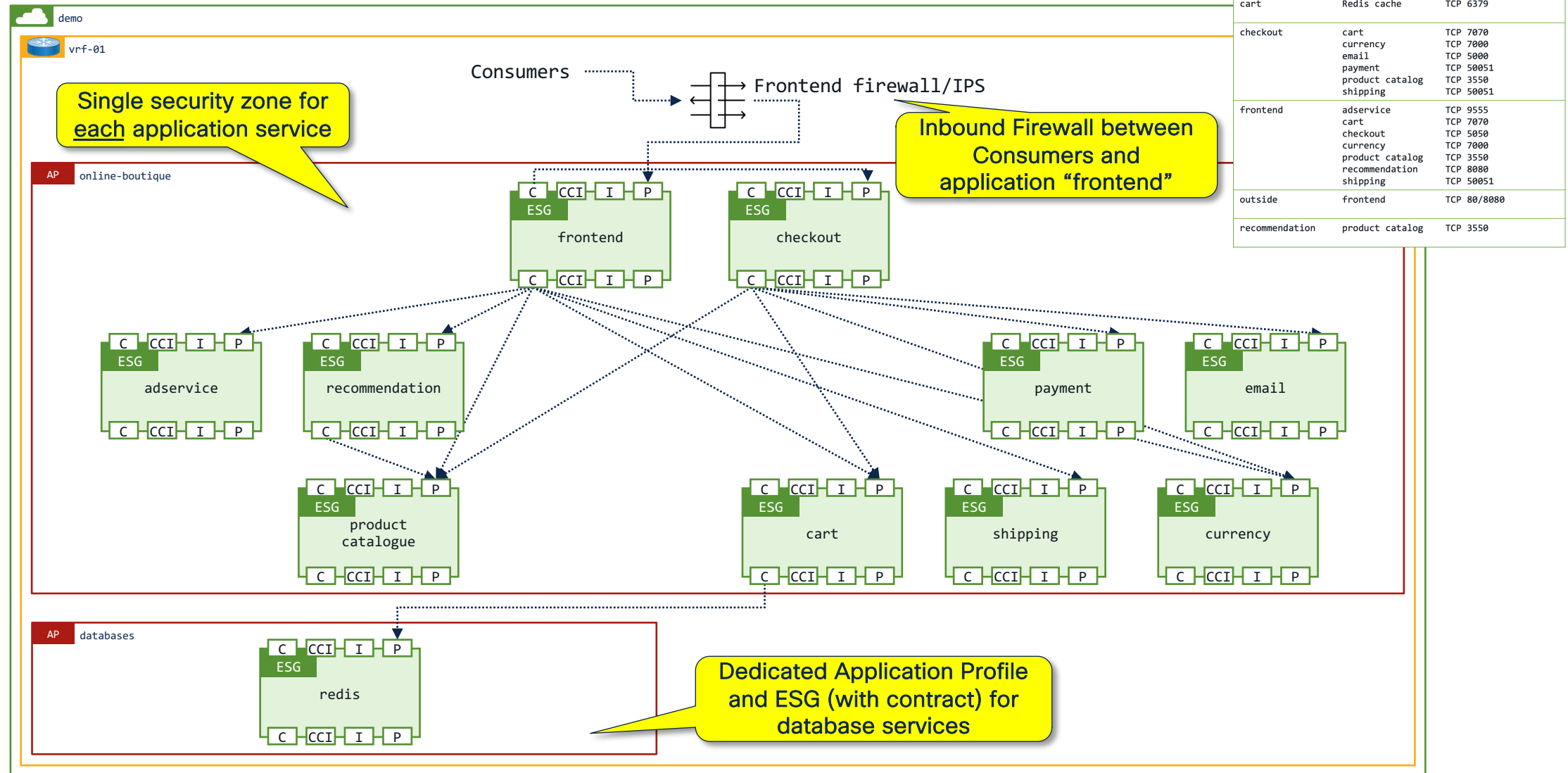
Application tiers across subnets

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



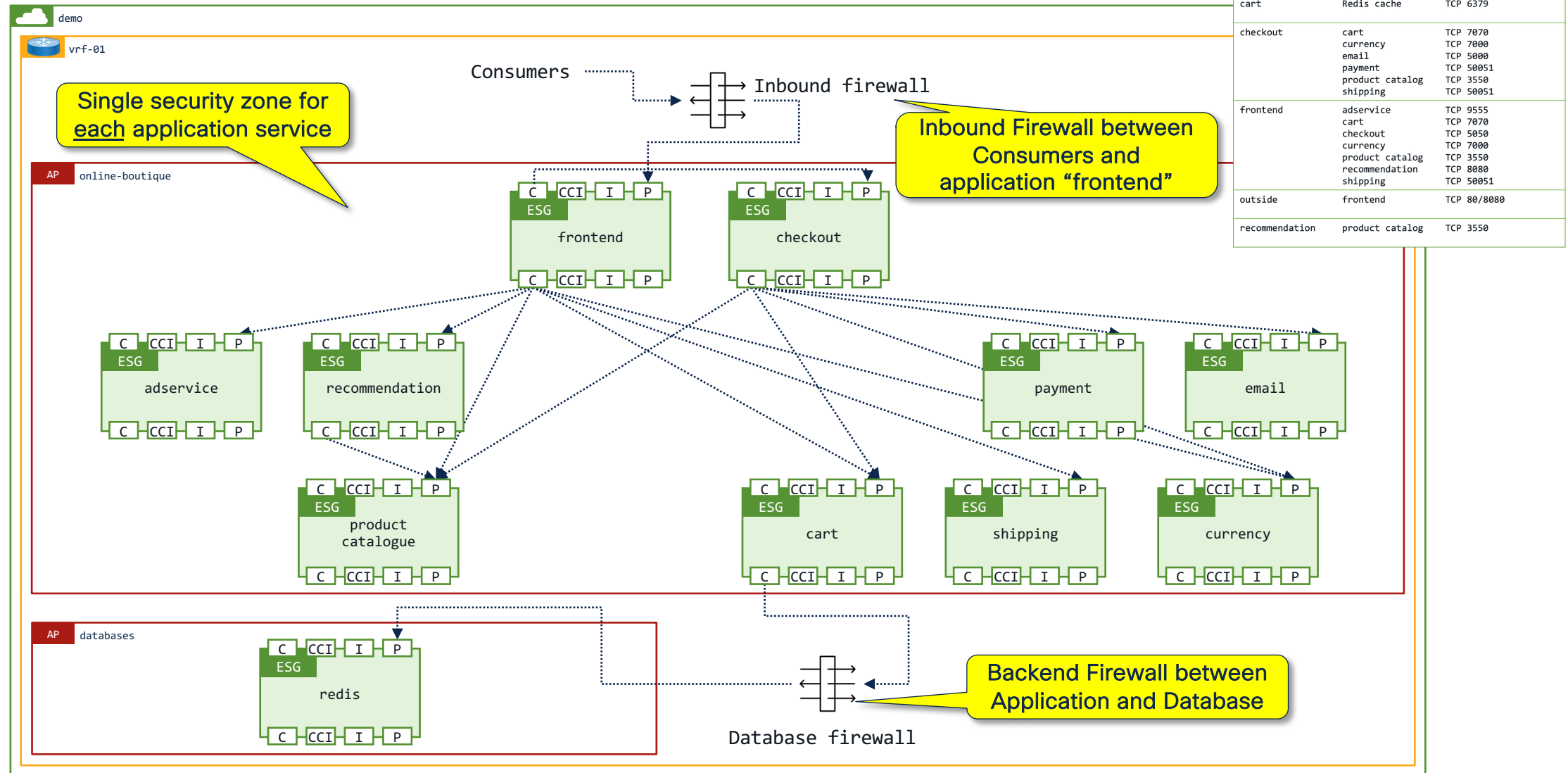
Application tiers across subnets

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



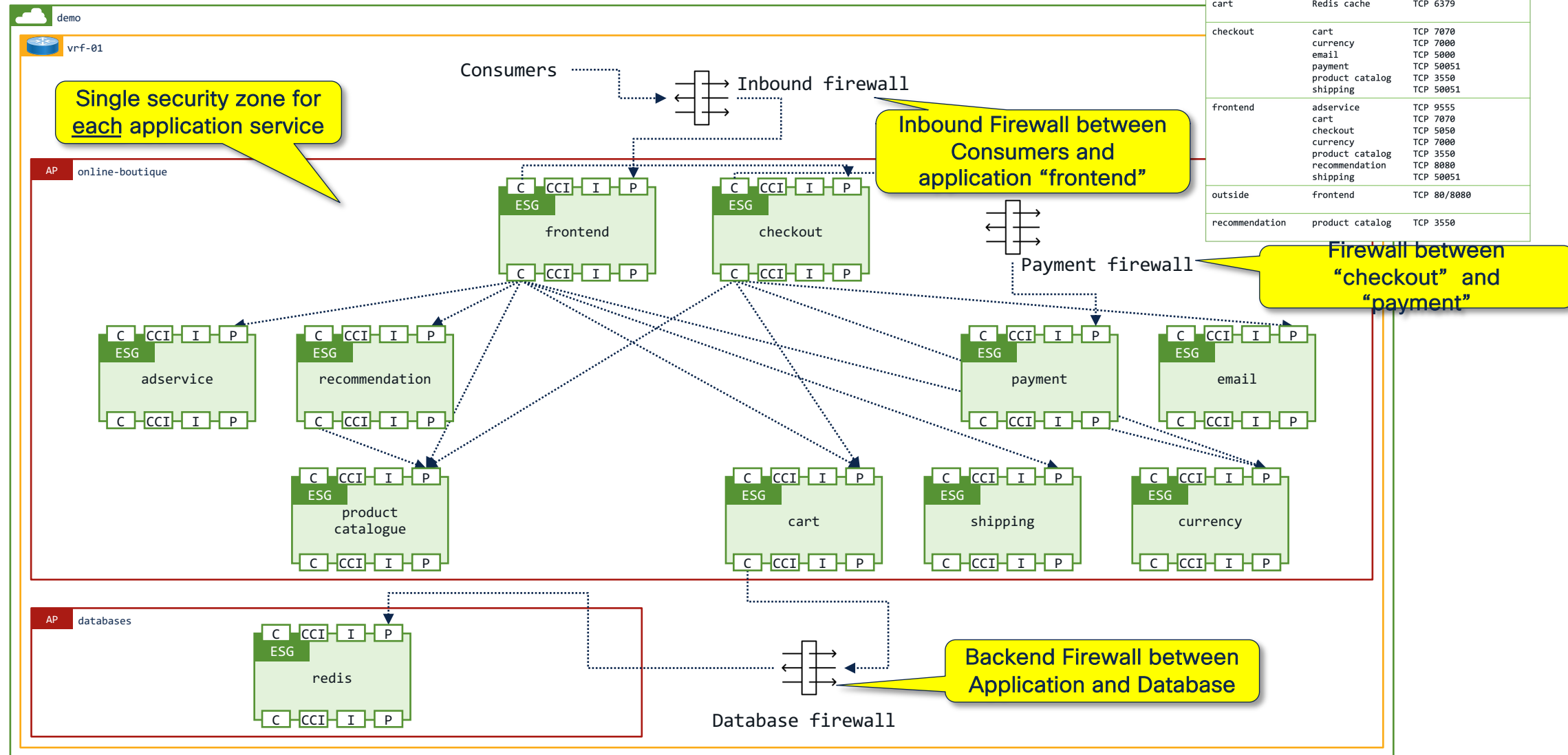
Application tiers across subnets

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



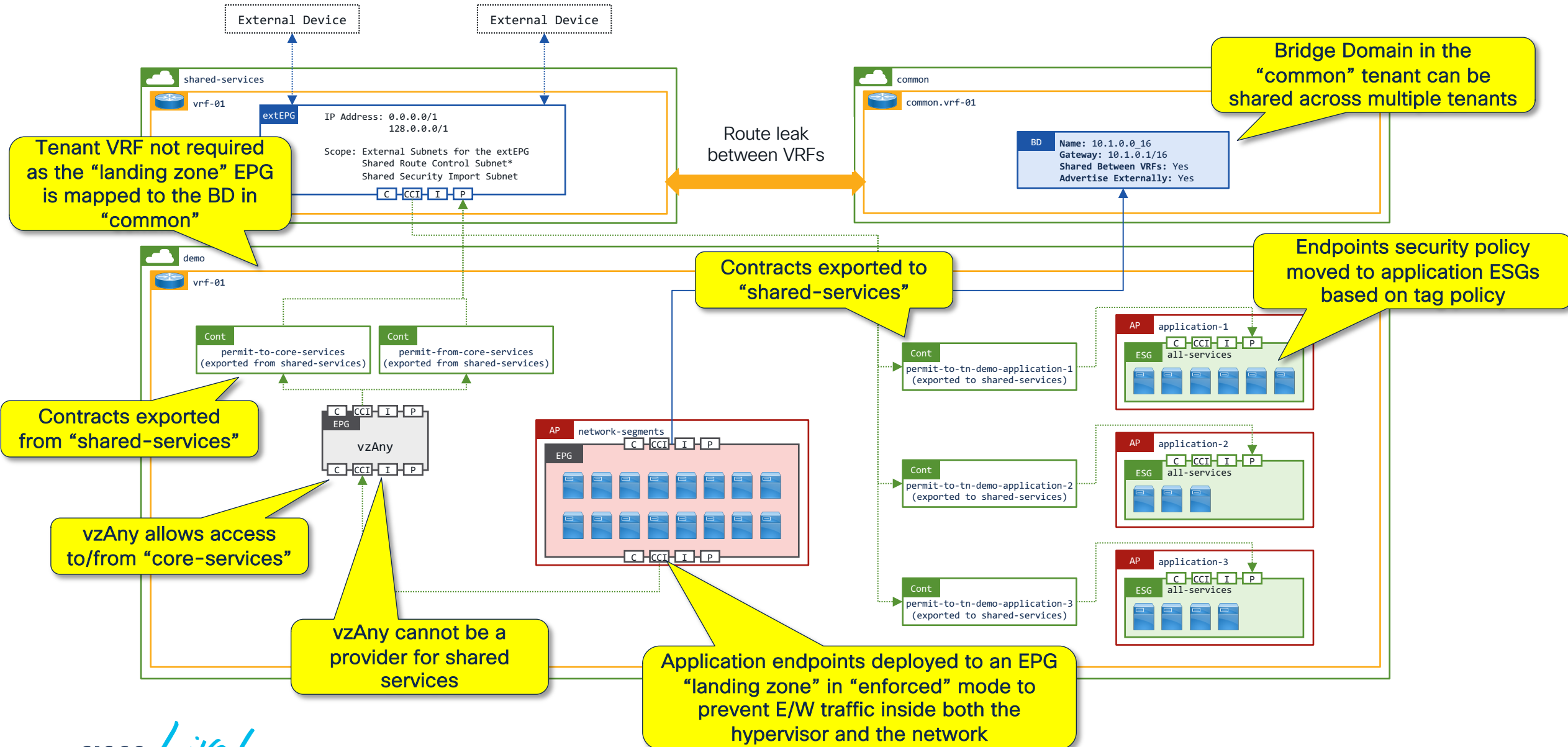
Application tiers across subnets

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

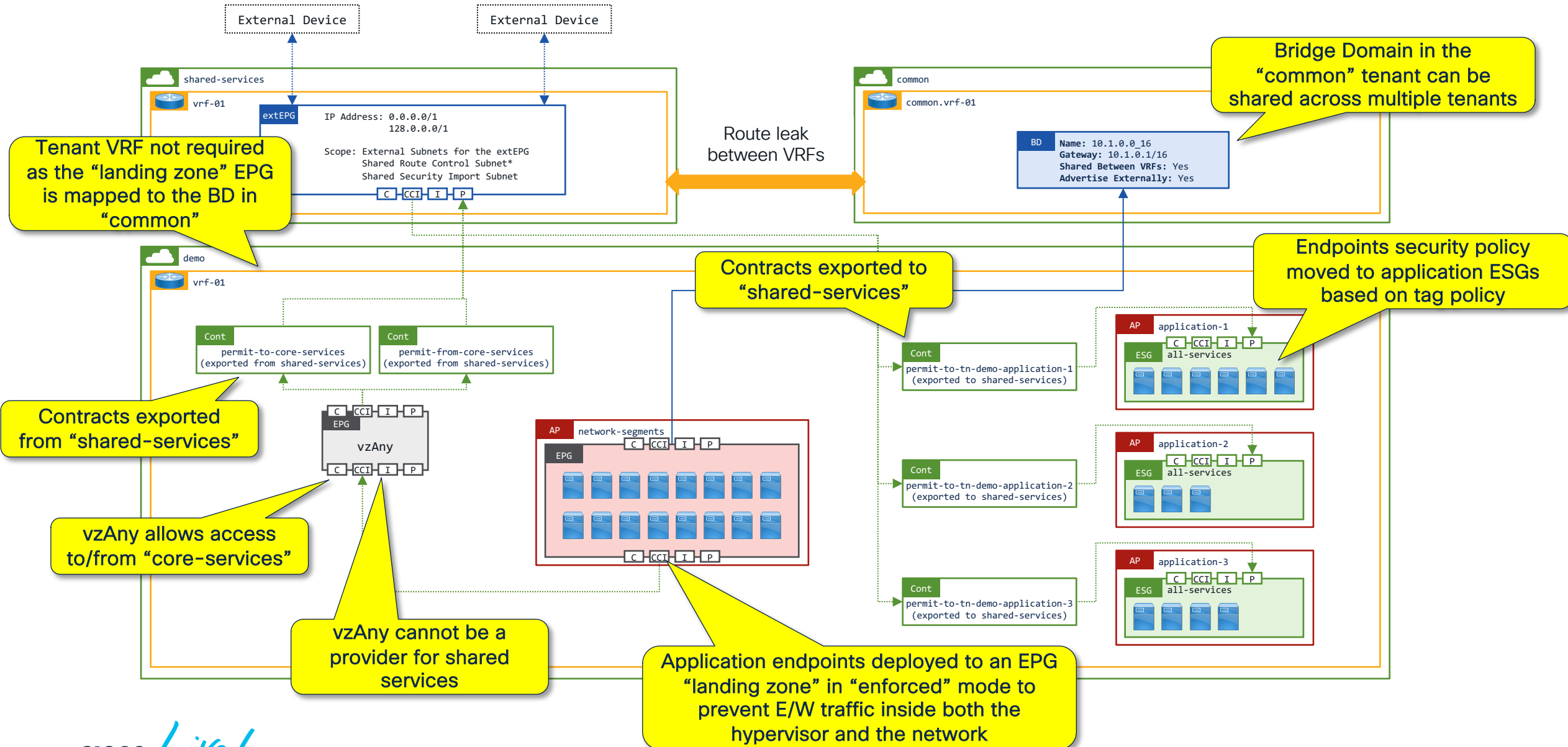


The ultimate aim is to provide a fully consumable fabric where resources are automated on demand...

Example Internal Private Cloud Design – shared subnet(s)



Example Internal Private Cloud Design – Auto Cleanup Isolation



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)
- Contract scopes
- External EPG with the classifier 0.0.0.0/0

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](#)

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

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

ESG Design Guide

<https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-aci-esg-design-guide.html?cachemode=refresh>

Cisco ACI Endpoint Security Group (ESG) Design Guide

Updated: May 25, 2023

[Bias-Free Language](#) [Contact Cisco](#) ✓

Goals of this document ^ Q

Table of Contents

Goals of this document

Prerequisites

Terminology

Introduction

Network-centric to Application-centric Migration Story: Pseudo Co +

ESG Design Examples +

Appendix: Cisco ACI Tenant D... +

FAQ

See Also

Contents

Goals of this document

Prerequisites

Terminology

Introduction

Network-centric to Application-centric Migration Story: Pseudo Co

Overview of Pseudo Company's Cisco ACI Deployment

Network Deployment

Reference Application

Endpoint Group vs Endpoint Security Group

Design Blueprint-Single ESG per Application

Migration Steps

Step 1: Implement a single ESG for open communication between subnets (EPG selectors)

Save

Download

Print

Now available on dCloud

<https://dcloud2-sjc.cisco.com/content/demo/333928?returnPathTitleKey=content-view>

Segmenting your ACI Fabric with ESGs and Secure Firewalls

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

Overview

In this demonstration we review how PseudoCo can convert its Cisco ACI fabric from a network-centric design to an application-centric design via the use of EndPoint Security Groups (ESGs).

PseudoCo has deployed its Cisco ACI fabric in what is commonly described as a network-centric design where there is a 1:1 mapping of Bridge Domains to (Endpoint Groups) EPGs. As part of the network implementation, PseudoCo chose to implement a VMM domain to simplify the management of VLANs between the Cisco ACI fabric and the ESXi hosts.

The focus of this demo is PseudoCo's multi-tier reference application (online-boutique). The online boutique application has been deployed across the different network segments (subnets) within the "demo" tenant. The demonstration reviews various design blueprints which can be used to secure the application using ESGs by introducing the use of contracts, service graphs and next generation firewalls.

When you run this demonstration an instance of the online-boutique application is deployed on VMs connected to a real ACI fabric.

This demonstration should be used in combination with these supporting materials:

- White Paper: [Cisco ACI Endpoint Security Group \(ESG\) Design Guide](#)
- Introduction to Application-Centric design using ESGs: [Endpoint Groups vs Endpoint Security Groups](#)
- Demo instructions: [Guided Walk-through](#)



Try the Walk in Lab in the World of Solutions...

cisco *Live!*

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

CISCO *Live!*

Let's go

#CiscoLiveAPJC