

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



ACI – The Foundation of an Internal Private Cloud

(aka “not just another network...”)

BRKDCN-2984

Steve Sharman – Solutions Engineer
BRKDCN-2984

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 November 15, 2024.



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

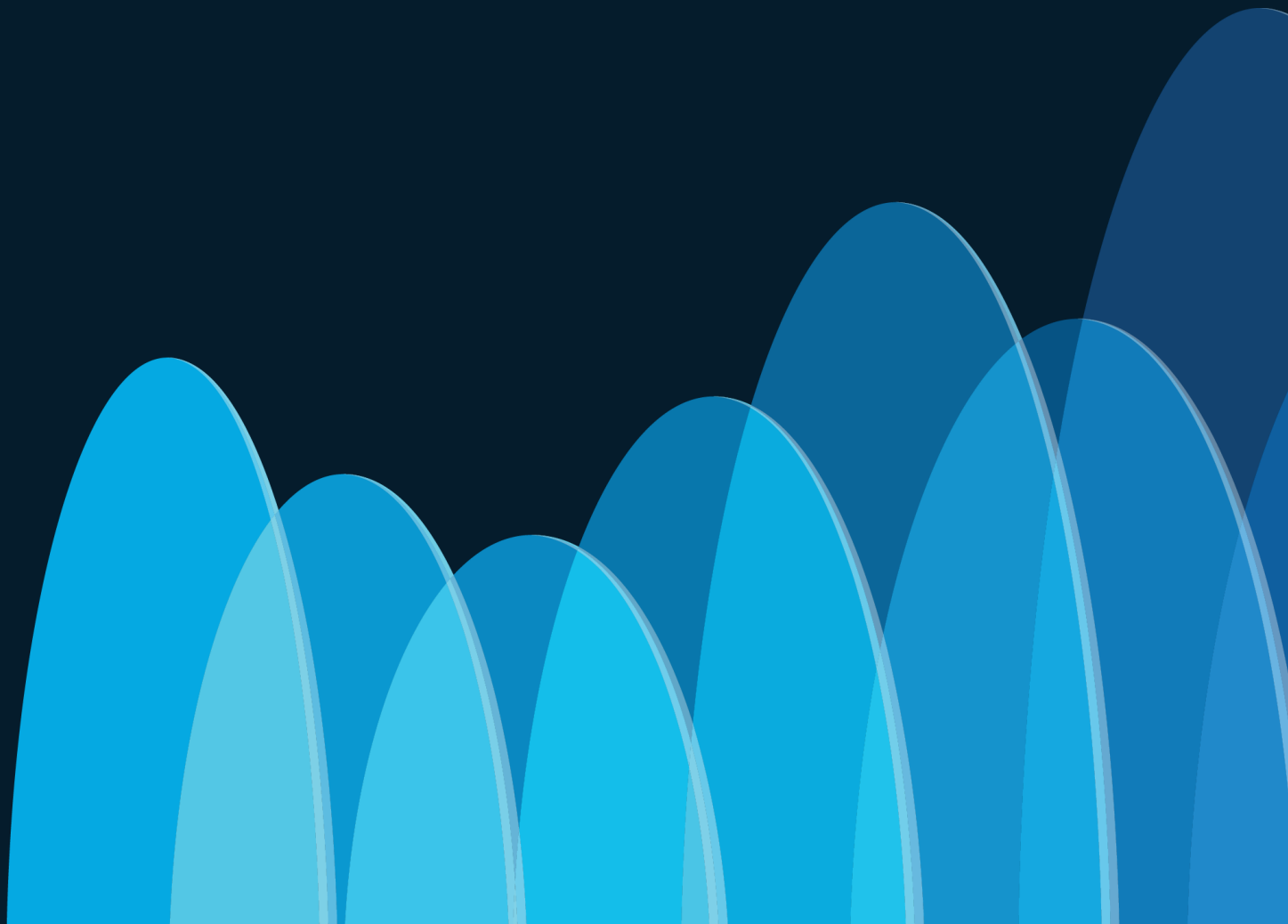


At little bit of background to this session...

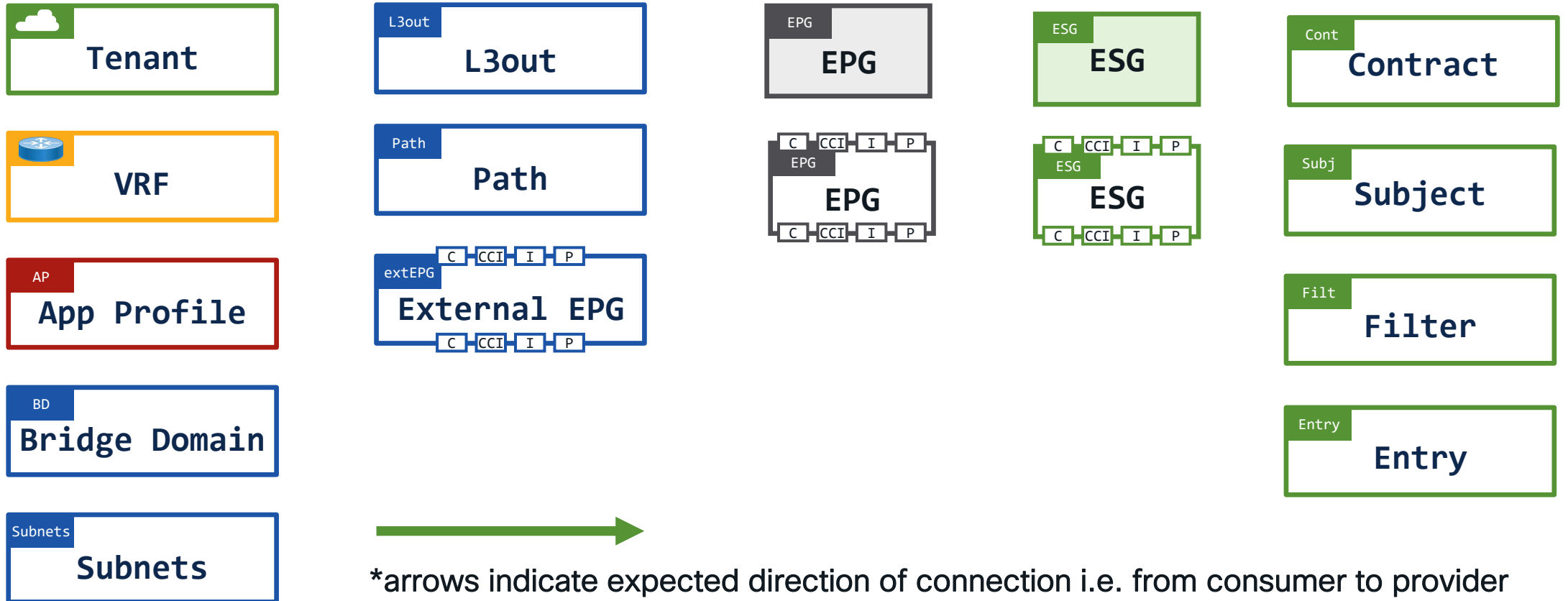
Agenda

- Setting the scene
- Converting your fabric into Application Centric “mode”
- Working with ESGs
- Understanding ACI Security
- External Connectivity
- Increasing Security
- Automation Blueprints

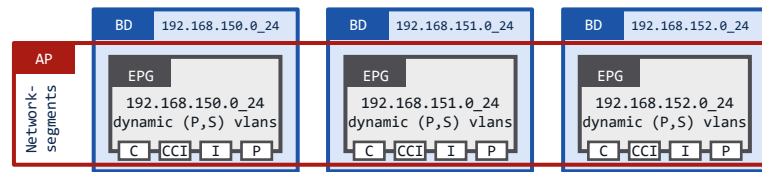
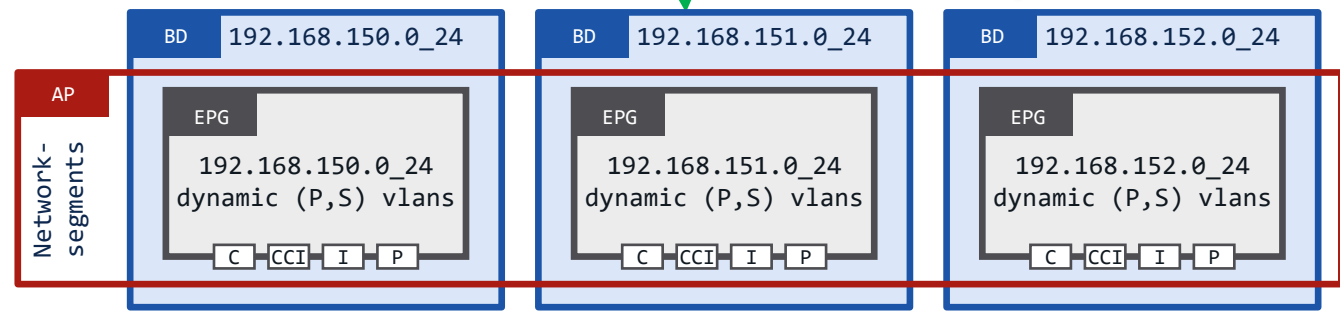
Before we get
started...



Icons



You are going to see lots (and lots) of diagrams...



The details are there for your reference so that you can rebuild in your own environment

Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

Understanding ACI security...

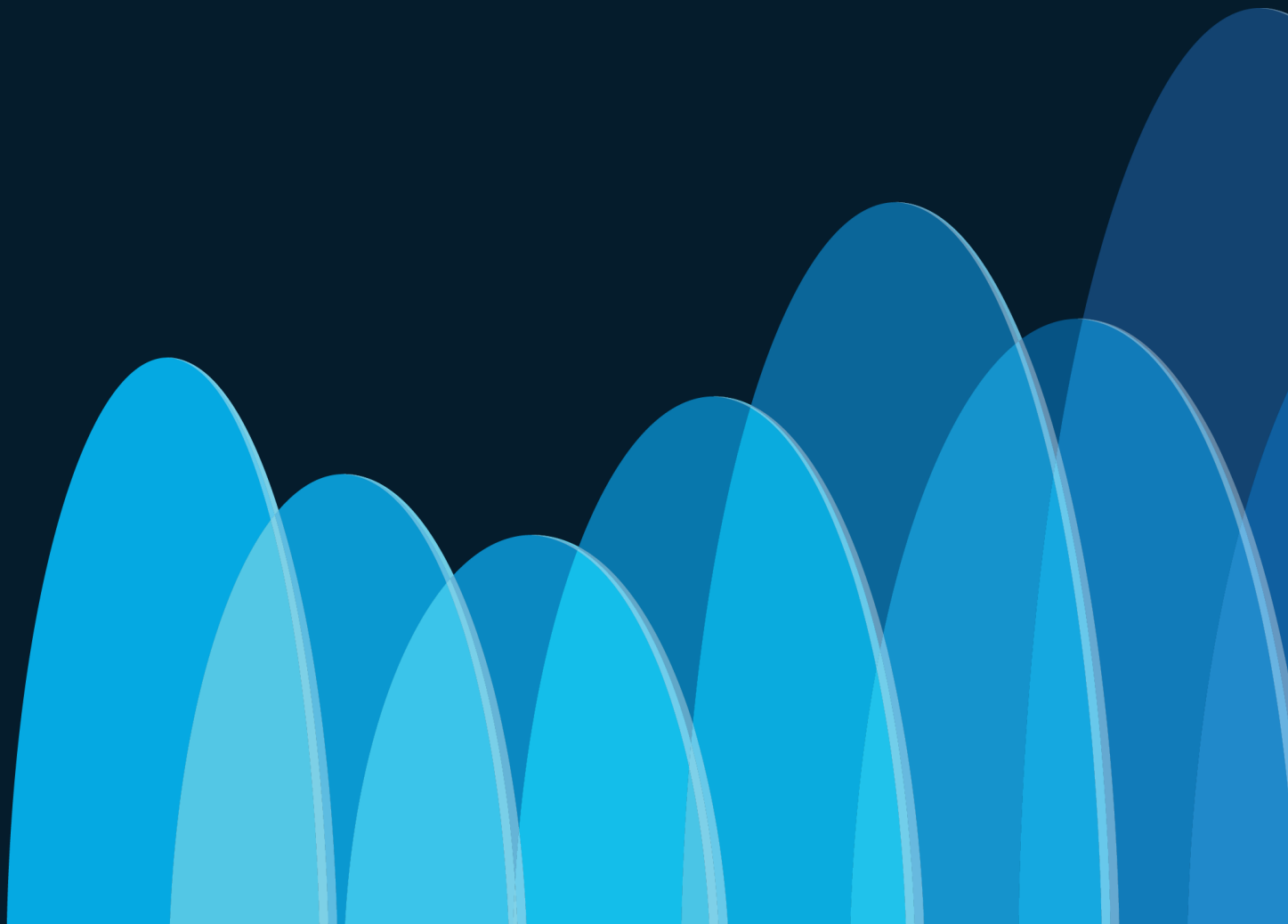
External Connectivity...

Increasing Security...

Automation Blueprints...

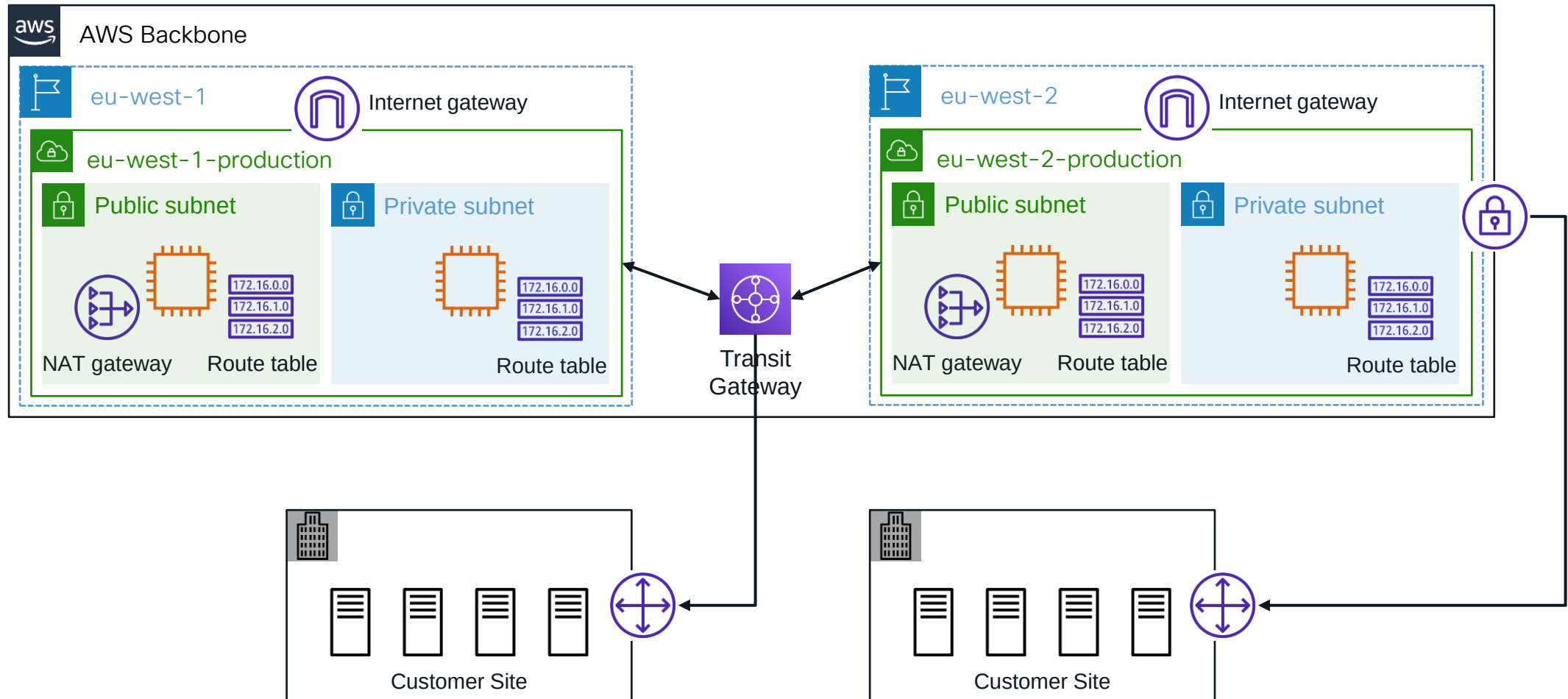
Wrapping up...

Public Cloud
infrastructure...



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.

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

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



Executive
Sponsorship



New Talent
Attraction



New Culture



Evolution Instead
of Revolution



Cross Functional
Teams



Scaling



Think Agile



Partnerships 2.0

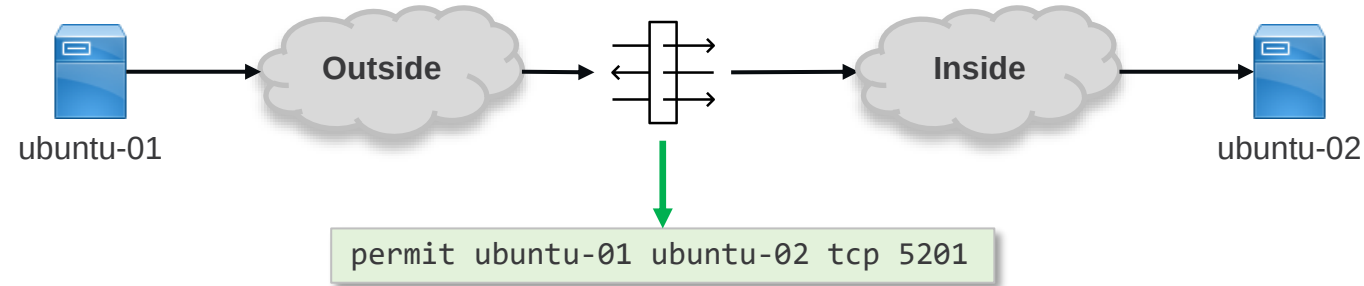
A cloud operating model succeeds best when there is a new organizational culture...

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

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

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

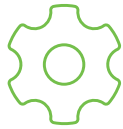
Traditional Enterprise Security Model



Traffic is routed through a firewall which typically becomes a pinch point with thousands of rules

What are the network characteristics required to enable us to operate in a cloud like manner...?

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



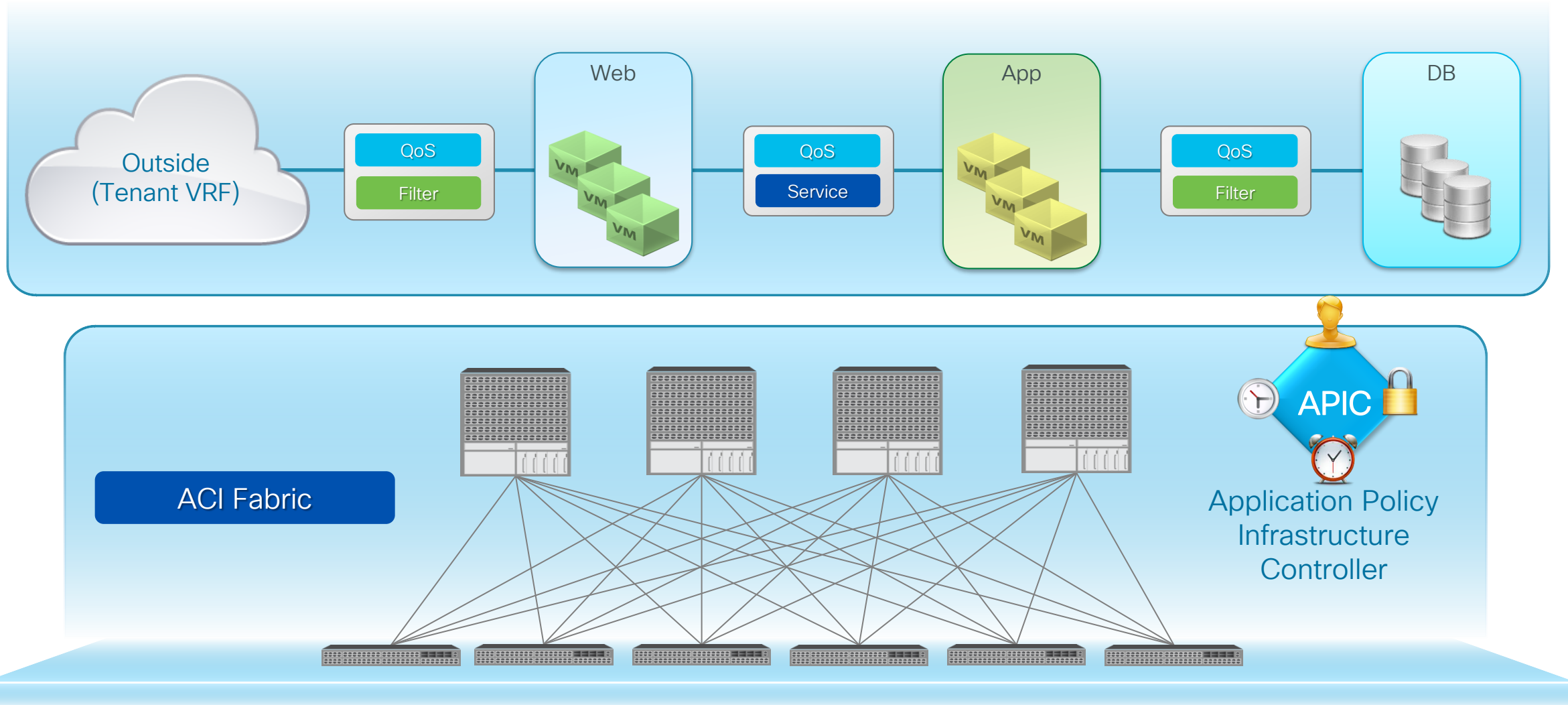
Infrastructure as Code with Ansible and Terraform

Automation | Classification and Segmentation | Security

The ACI Vision...

The ACI reference application from circa 2014...

The mythical three tier application...



Our reference application for this presentation...

Online Boutique

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

Free shipping with \$75 purchase!

 cisco-store

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



Hot Products



Cabana Shorts
\$39.99



Cable Knit Blanket
\$59.99





Free shipping with \$75 purchase!

Cart (2)

Empty Cart Continue Shopping



Save the Bees Bottle
SKU #2ZYFJ3GM2N

Quantity: 1

\$13.79



Cabana Shorts
SKU #OLJCESPC7Z

Quantity: 1

\$39.99

Shipping

\$8.99

Total

\$62.77

Shipping Address

E-mail Address
someone@example.com

Street Address
1600 Amphitheatre Parkway

Zip Code
94043

City
Mountain View

State
CA

Country
United States

Payment Method

Credit Card Number
4432-8015-6152-0454

Month
January

Year
2023

CVV
...

Place Order

cisco Live!

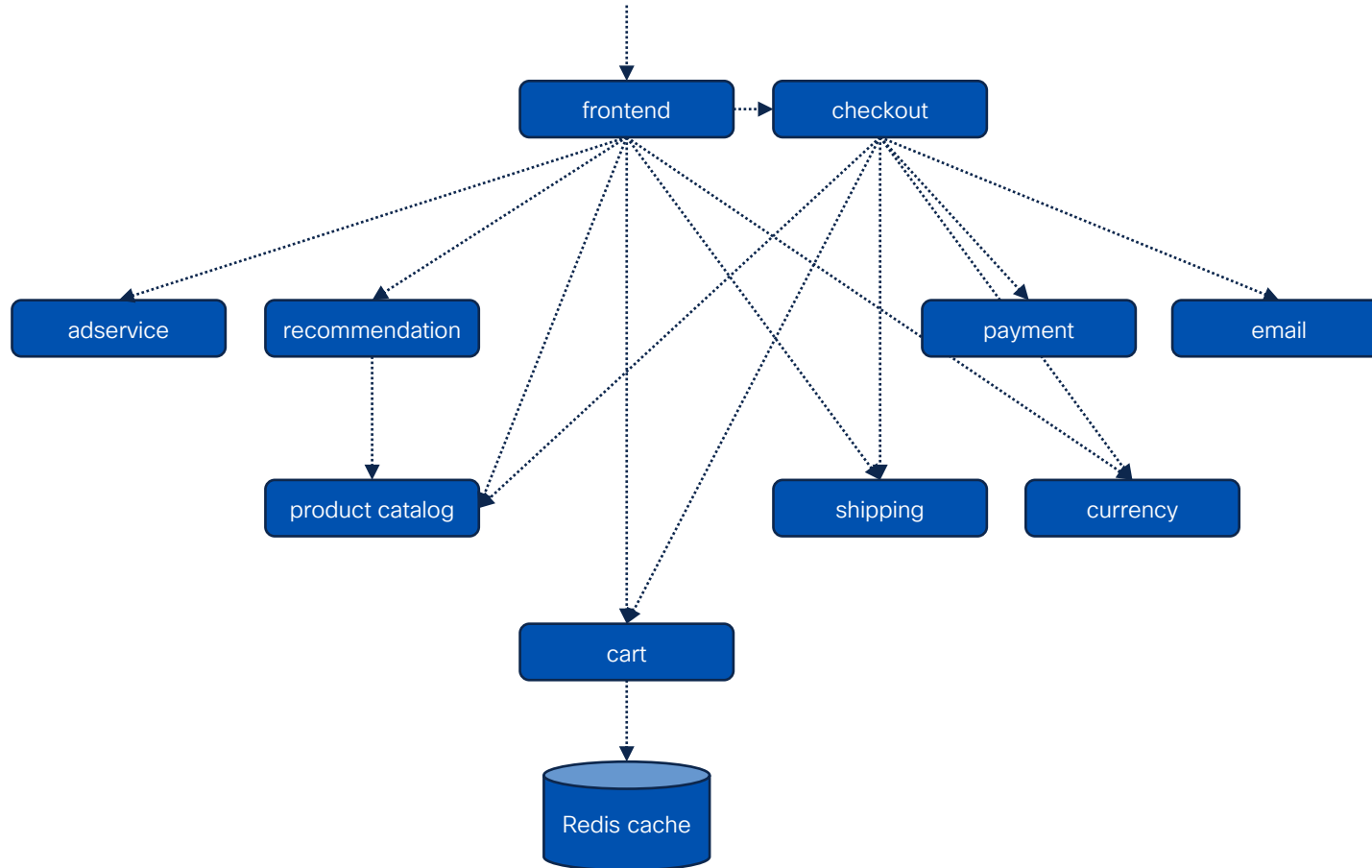
#CiscoLiveAPJC BRKDCN-2984

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

29

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

Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

Understanding ACI security...

External Connectivity...

Increasing Security...

Automation Blueprints...

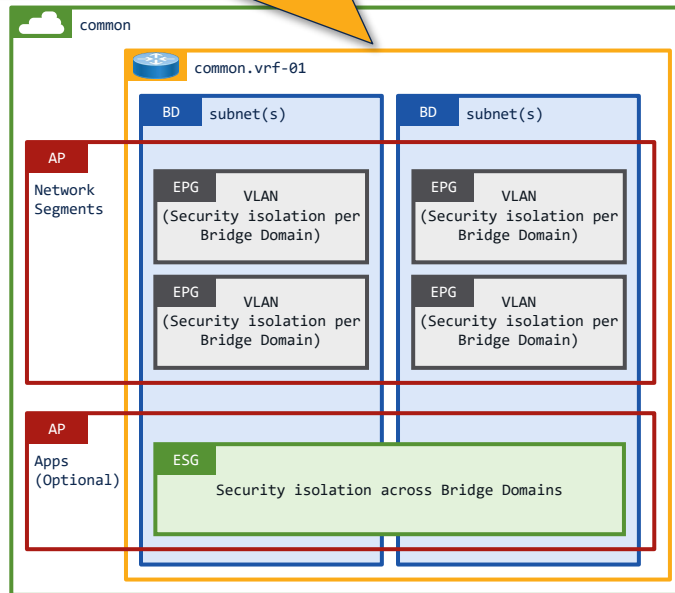
Wrapping up...



Design Considerations...

Design Patterns

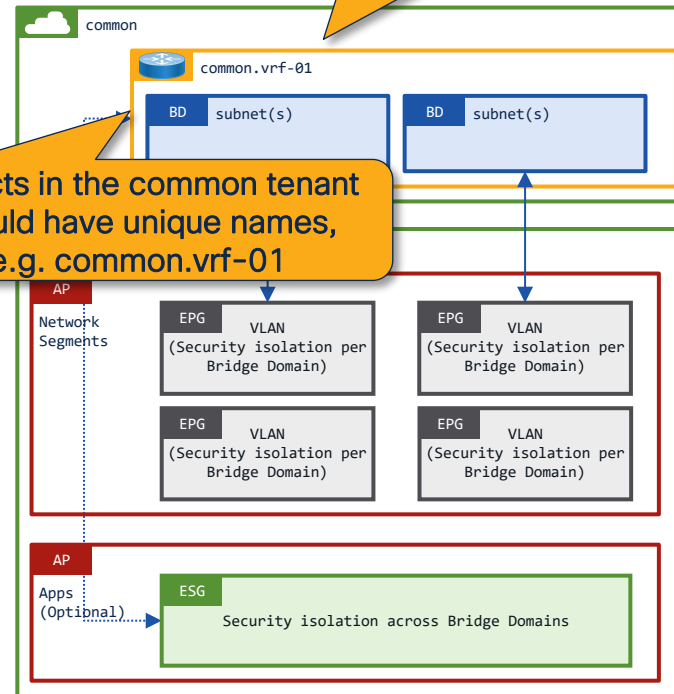
Everything in the “common” Tenant is not typically seen



Used for functions which are accessible from any Tenant

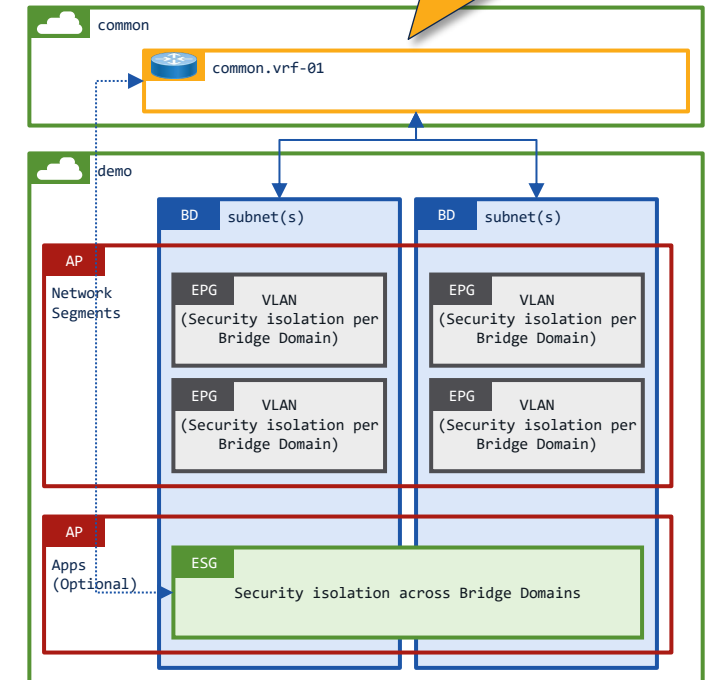
VRFs and BDs in “common” with EPGs and ESGs in the “user” tenant

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

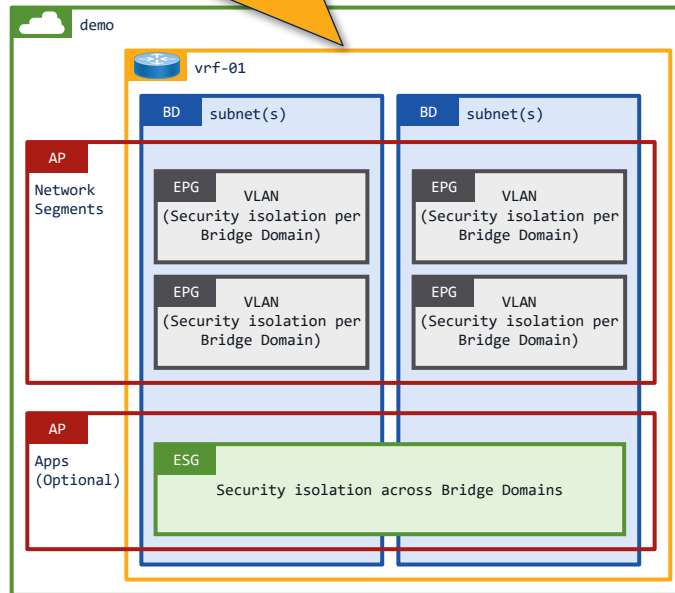
VRFs in “common” with BDs, EPGs and ESGs in the “user” tenant



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

Design Patterns

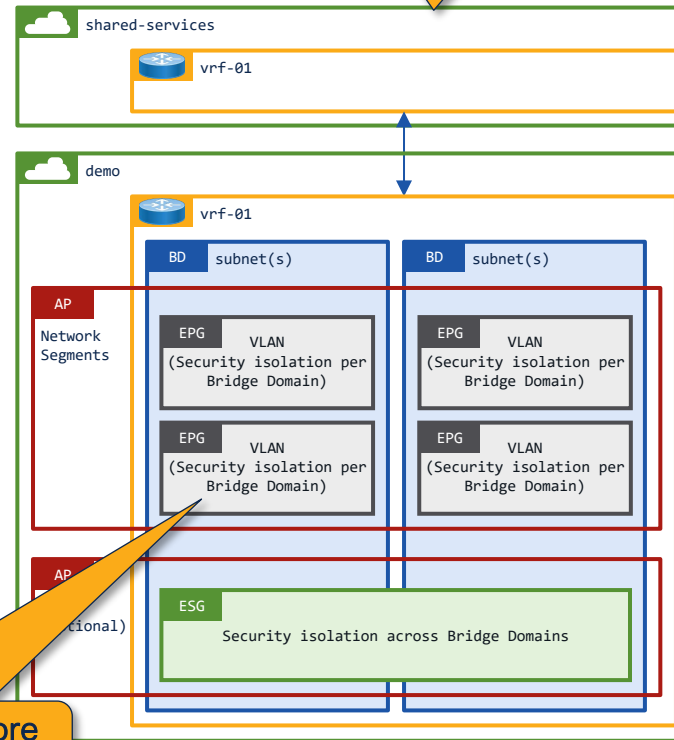
All networking constructs contained within a Tenant



Dedicated VRFs and subnets for each Tenant with Dedicated L3outs

Each Tenant has one or more network security groups

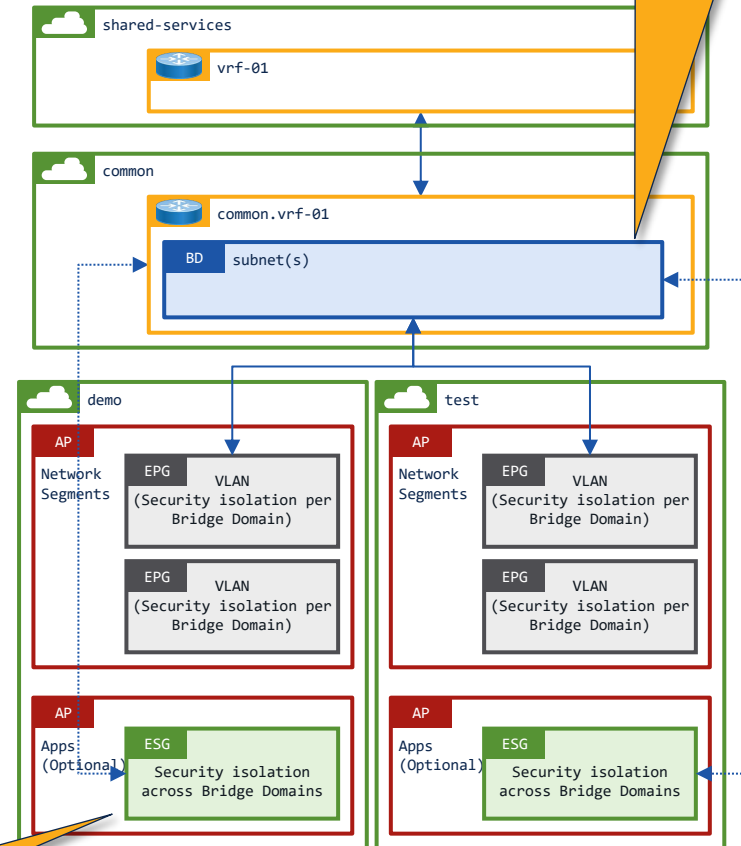
Network team controls inbound/outbound routing



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: | common | ciscolive-07 | rwhitear | shared-services | ciscolive-08

All Tenants

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

Page 1 Of 1

Objects Per Page: 100

Displaying Objects 1 - 32 Of 32

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

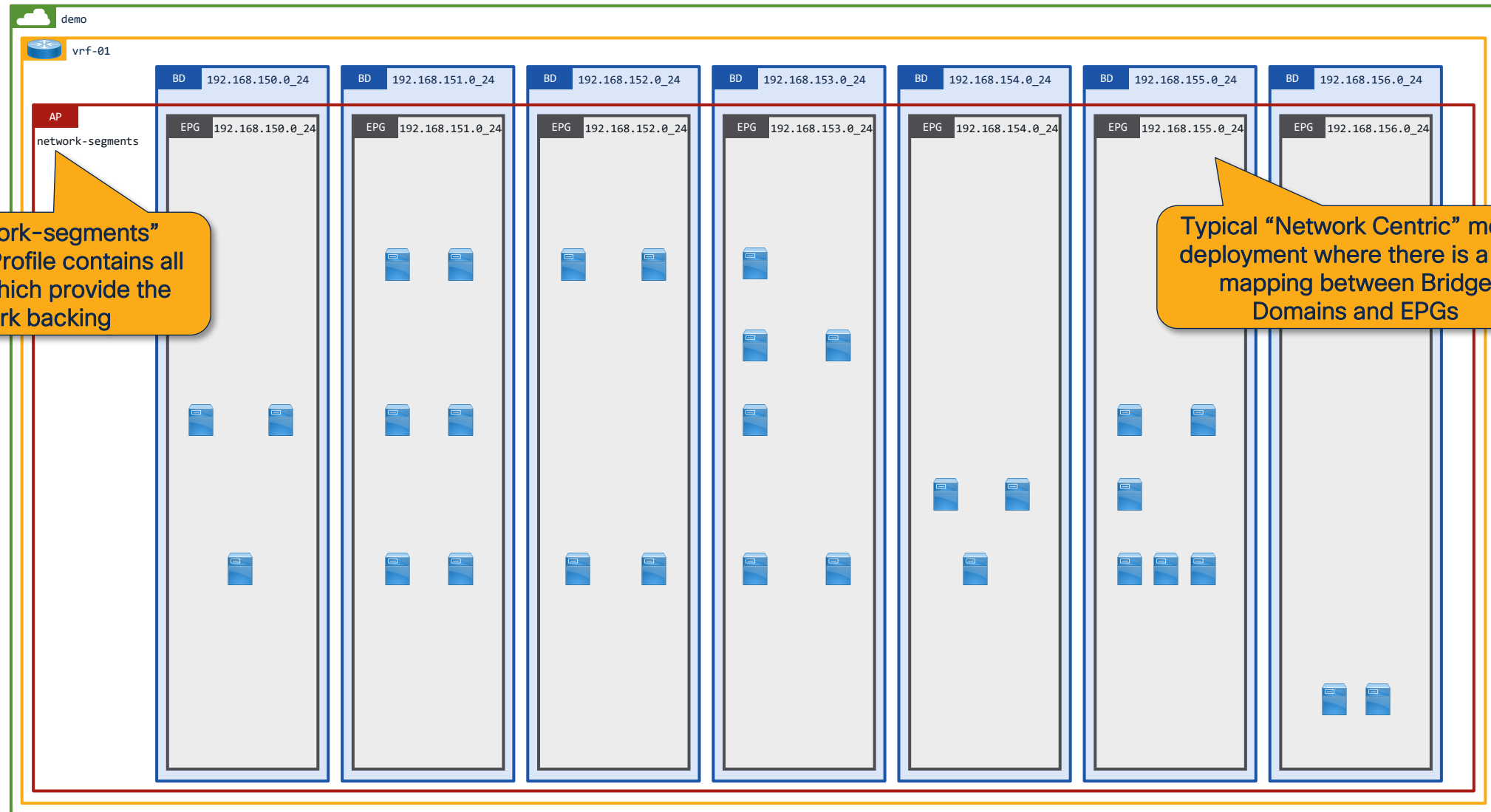
Current System Time: 2022-11-26T07:58 UTC+00:00

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

IP range per Tenant

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>

Free shipping with \$75 purchase!

 cisco-store

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



Hot Products



Cabana Shorts
\$39.99



Cable Knit Blanket
\$59.99





Free shipping with \$75 purchase!

Cart (2)

Empty Cart Continue Shopping



Save the Bees Bottle
SKU #2ZYFJ3GM2N

Quantity: 1

\$13.79



Cabana Shorts
SKU #OLJCESPC7Z

Quantity: 1

\$39.99

Shipping

\$8.99

Total

\$62.77

Shipping Address

E-mail Address
someone@example.com

Street Address
1600 Amphitheatre Parkway

Zip Code
94043

City
Mountain View

State
CA

Country
United States

Payment Method

Credit Card Number
4432-8015-6152-0454

Month
January

Year
2023

CVV
...

Place Order

cisco Live!

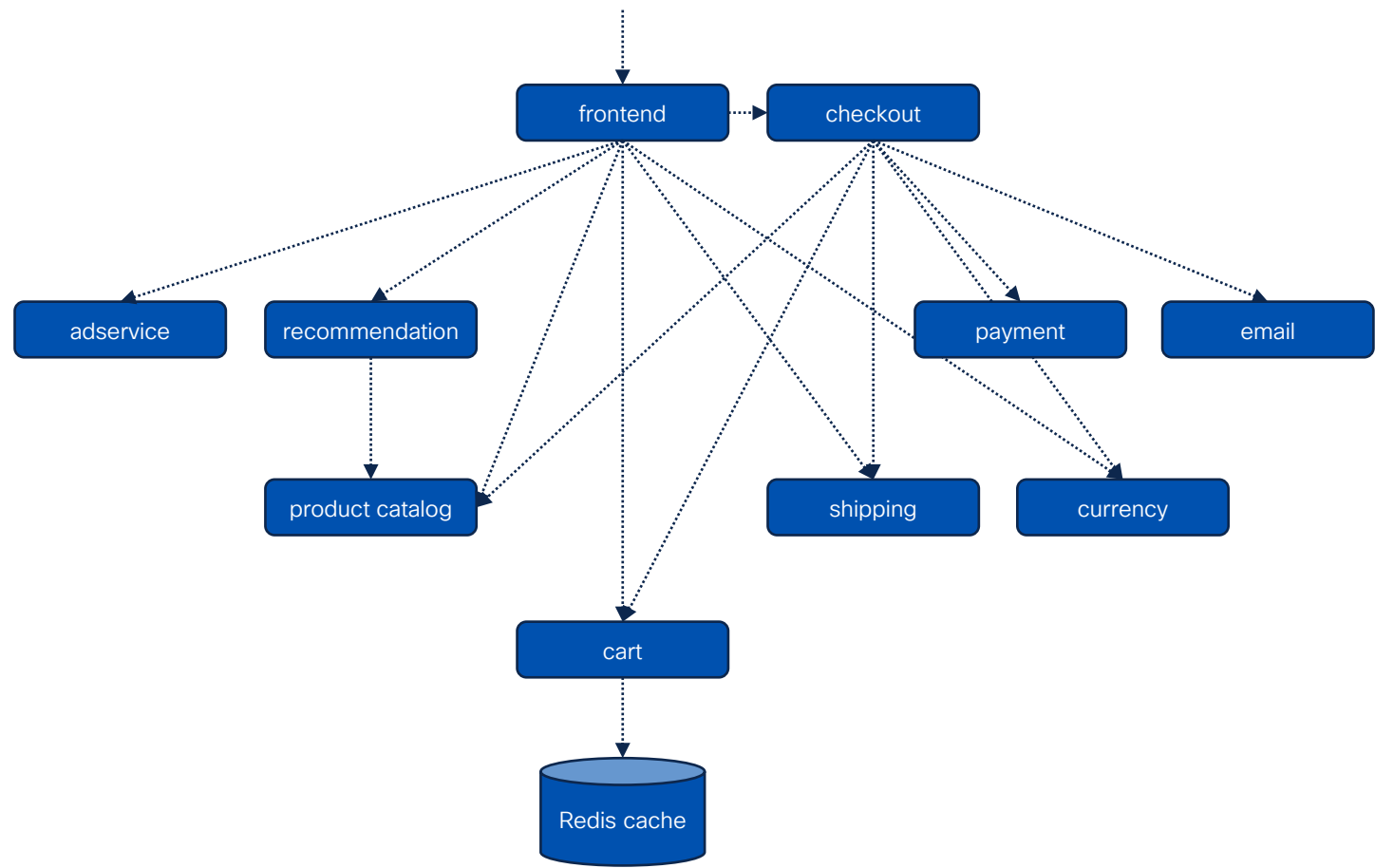
#CiscoLiveAPJC BRKDCN-2984

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

47

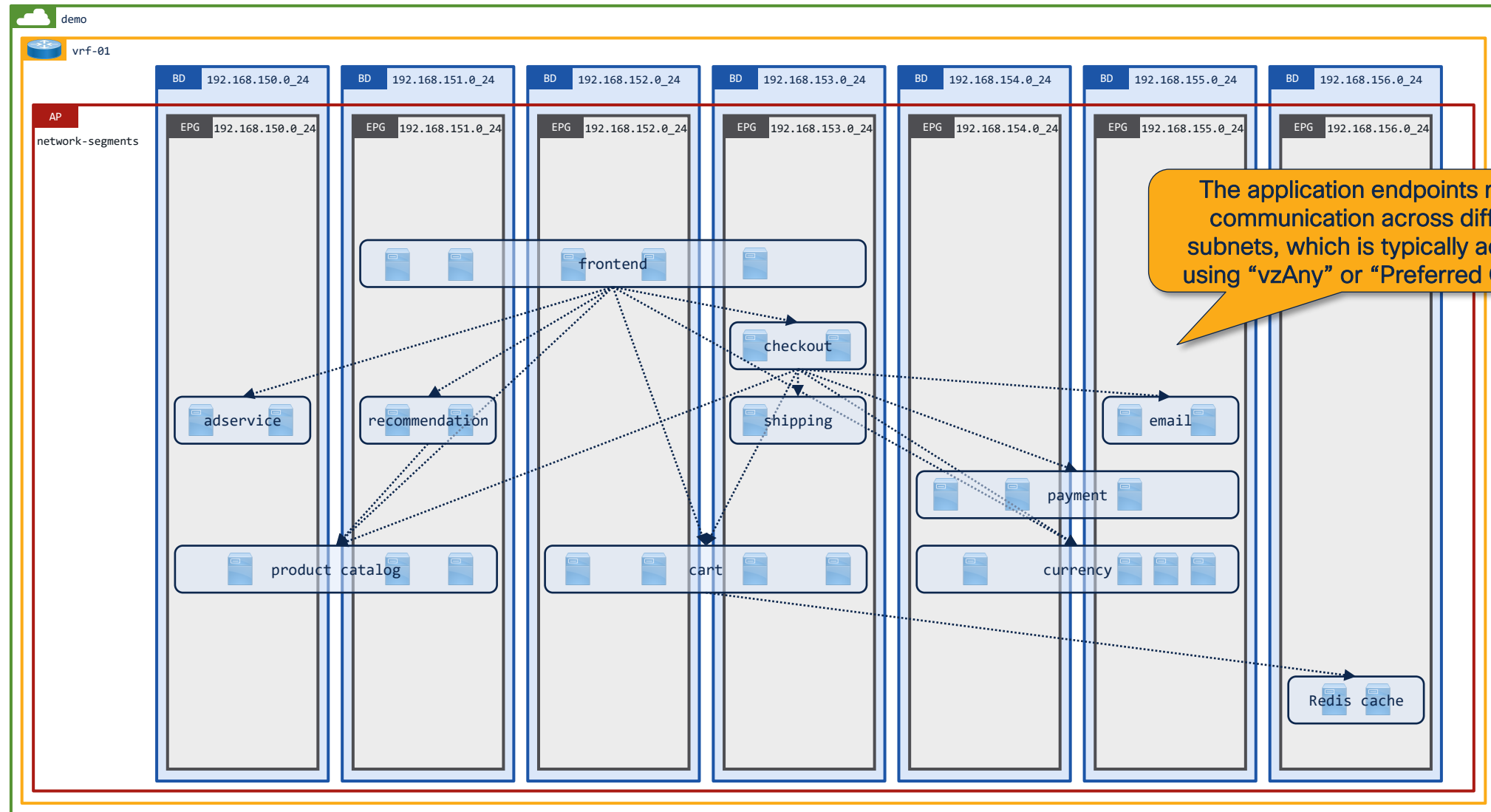
Online Boutique

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

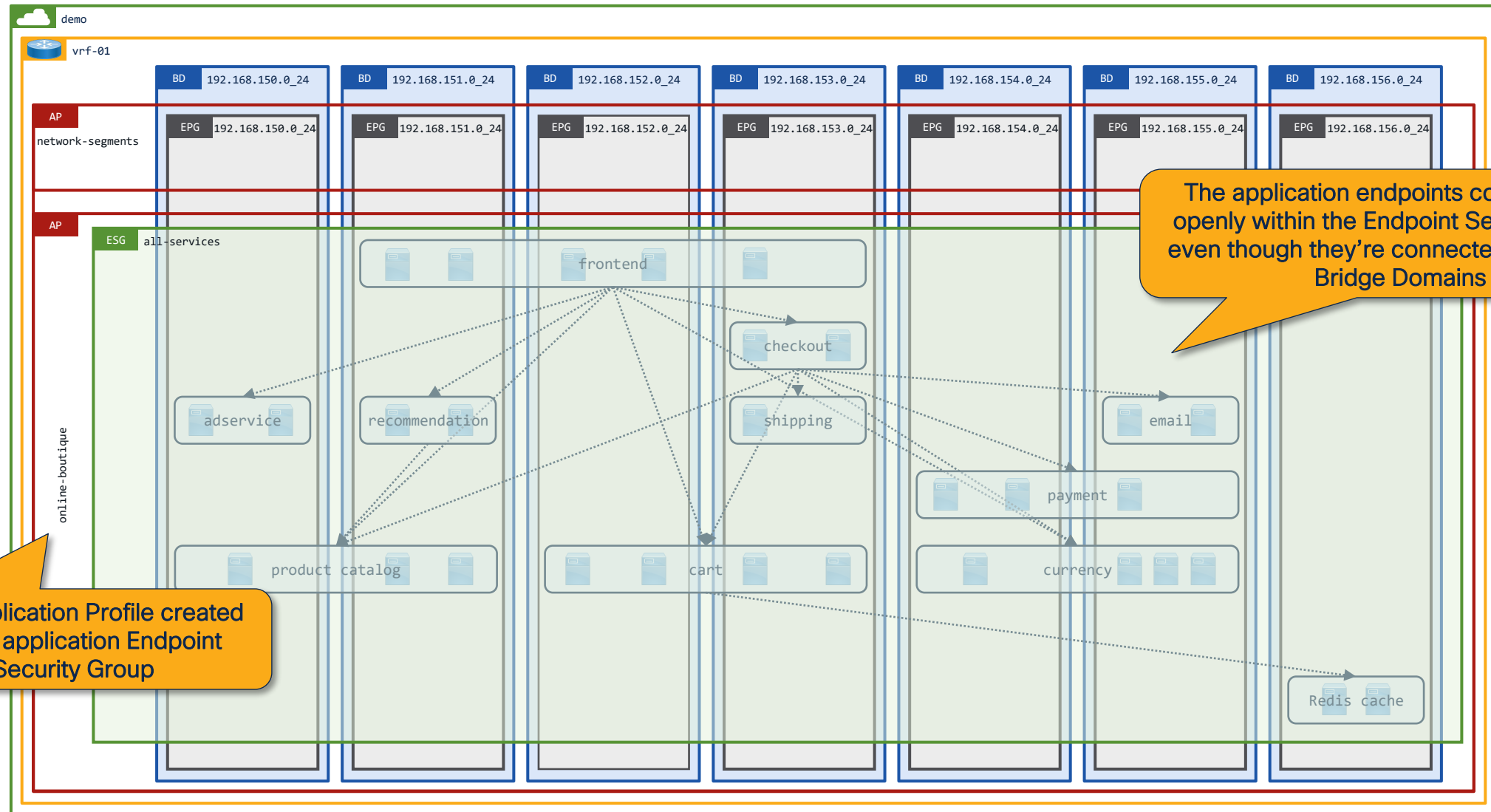


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart currency email payment product catalog shipping	TCP 7070 TCP 7000 TCP 8080 TCP 50051 TCP 3550 TCP 50051
frontend	adservice cart checkout currency product catalog recommendation shipping	TCP 9555 TCP 7070 TCP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

Where is our application running...?



Let's convert to "Application Centric" mode...



New Application Profile created for the application Endpoint Security Group

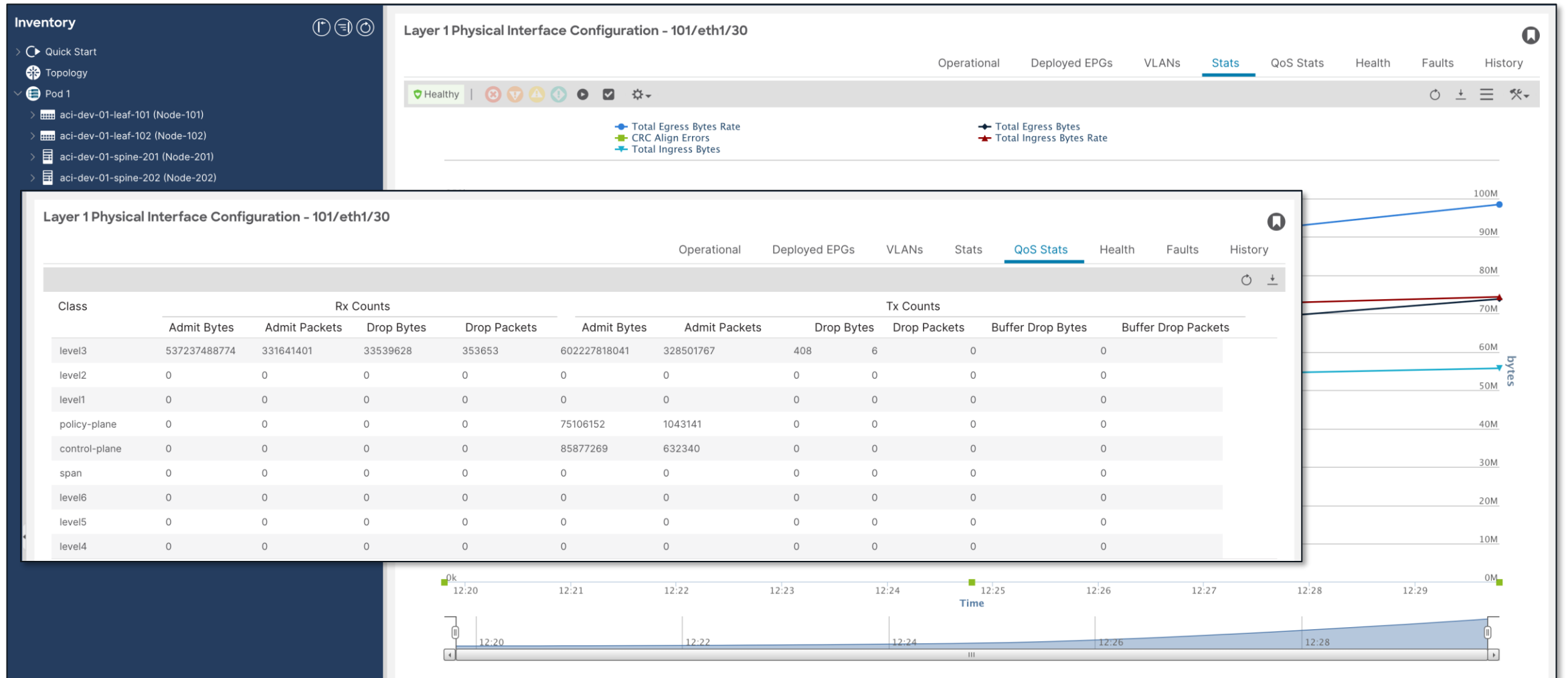
The application endpoints communicate openly within the Endpoint Security Group even though they're connected to different Bridge Domains

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

Application Visibility...!

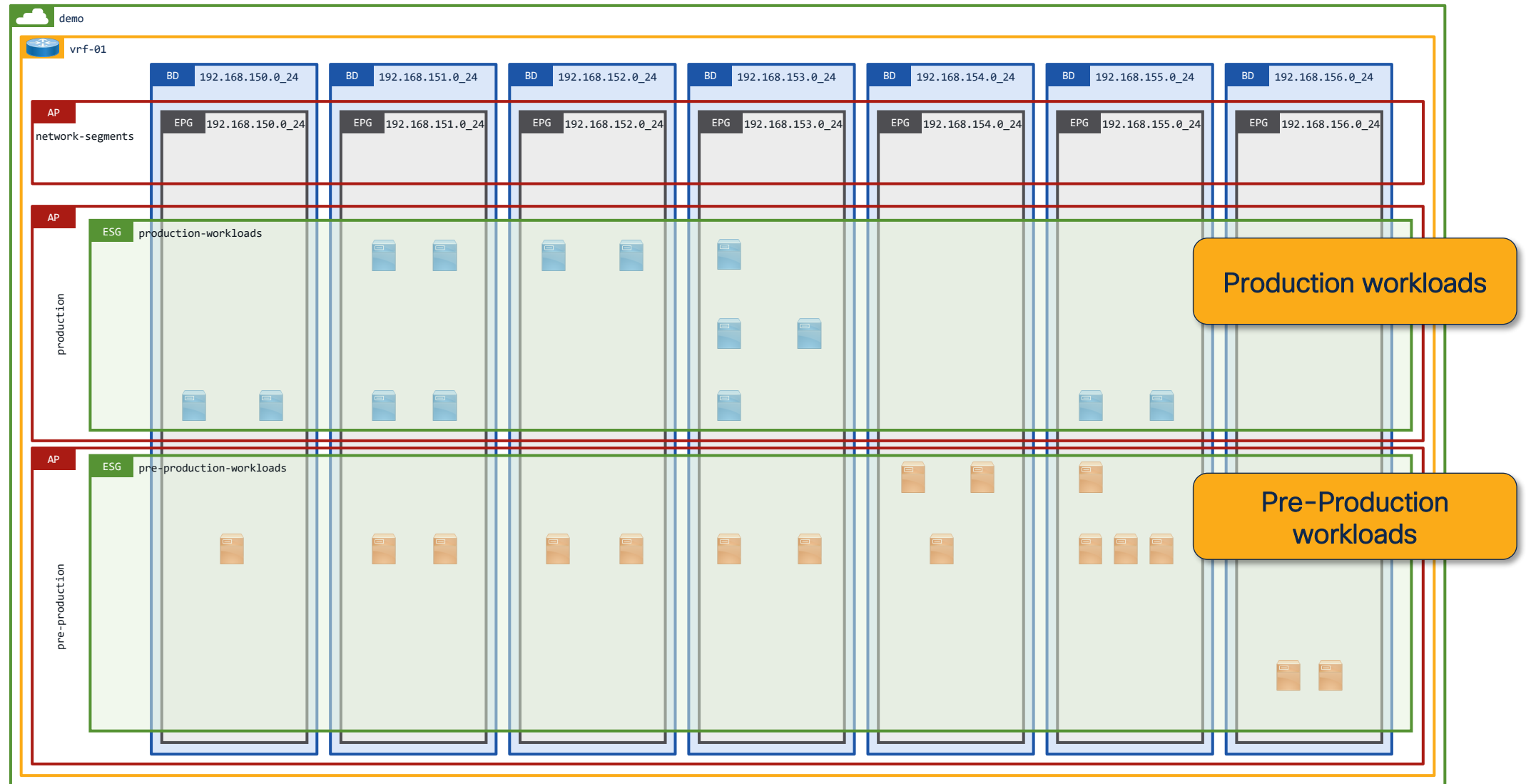
MAC/IP	Endpoint Name	Hosting Server	Interface (learned)	Encap	Base EPG	Policy Tags
00:50:56:A1:1A:60 192.168.150.100	tn-demo-online-boutique-ad-service	10.237.98.165	Pod-1/Node-102/eth1/29 (learned,vm...	vlan-1146(P) vlan-1147(S)	demo:network-segments:192.168.150.0_24 demo:network-segments:192.168.150.0_24	_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 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 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 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 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:A1:8F:09 192.168.153.156	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 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:A1:09:2F 192.168.150.101	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 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:A1:22:DE 192.168.152.100	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 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:A1:84:4D 192.168.155.155	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 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 192.168.151.0_24	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 demo:network-segments:192.168.151.0_24	_vmm:vmname tn-demo-online-boutique-recommendatio Function tn-demo-online-boutique-recommendation-servic

Correlate Endpoints to Switch Interfaces...



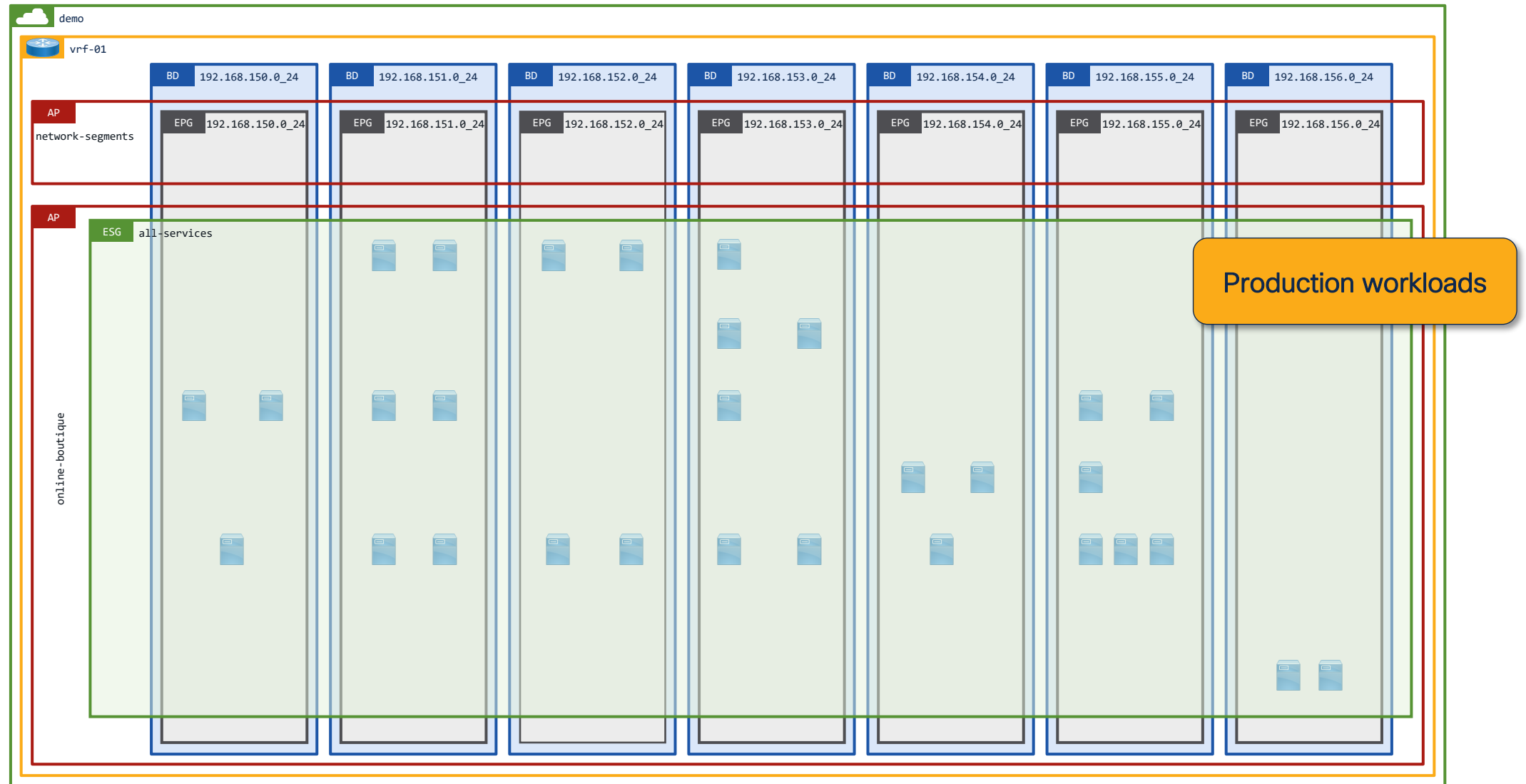
What if don't want my classification to be this granular...?

Broad-brush classification...

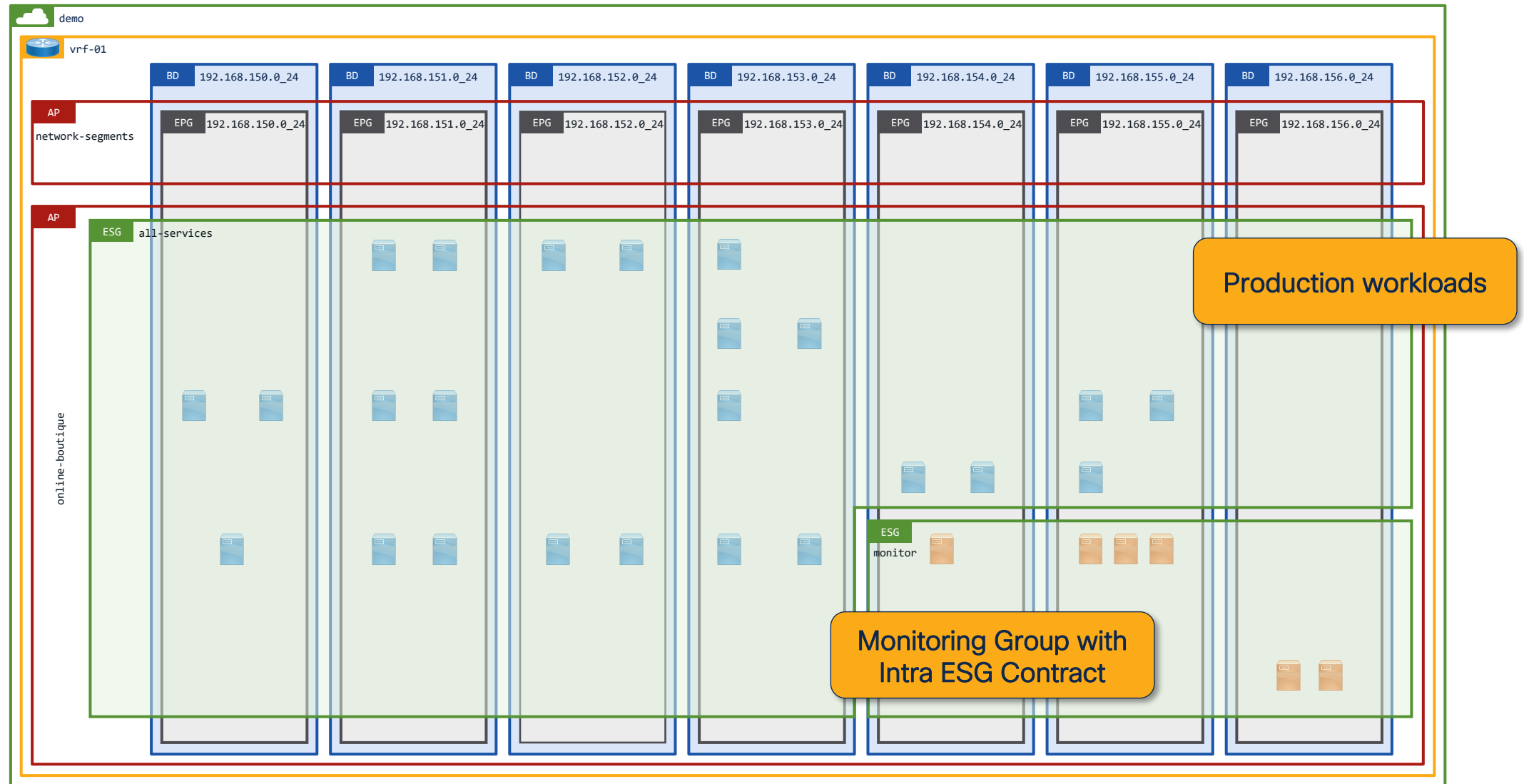


What if I'd like to gather data on a specific group of endpoints...?

Endpoint classification for monitoring...



Endpoint classification for monitoring...



Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

Understanding ACI security...

External Connectivity...

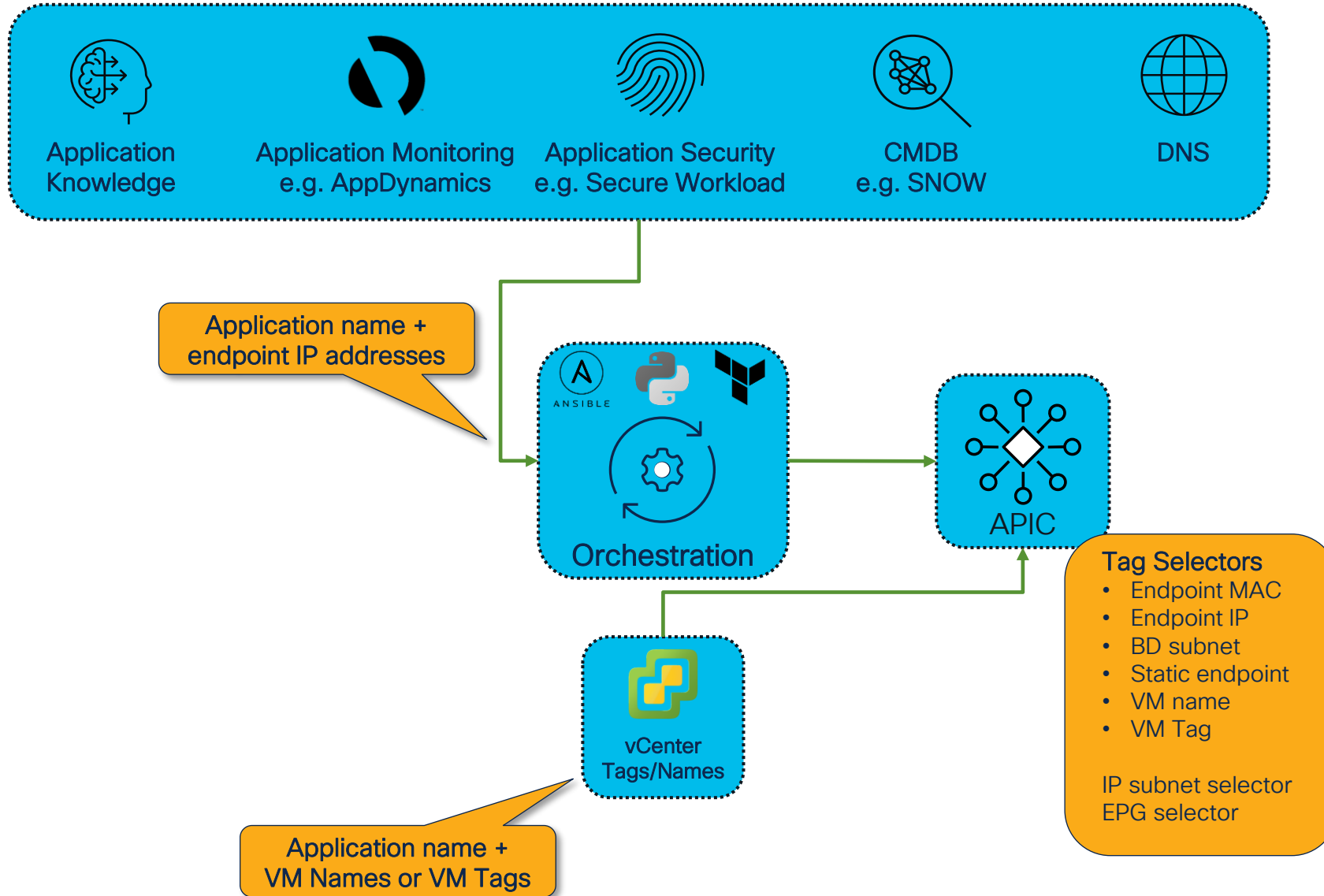
Increasing Security...

Automation Blueprints...

Wrapping up...

All we need are the application names and the associated IP addresses...!

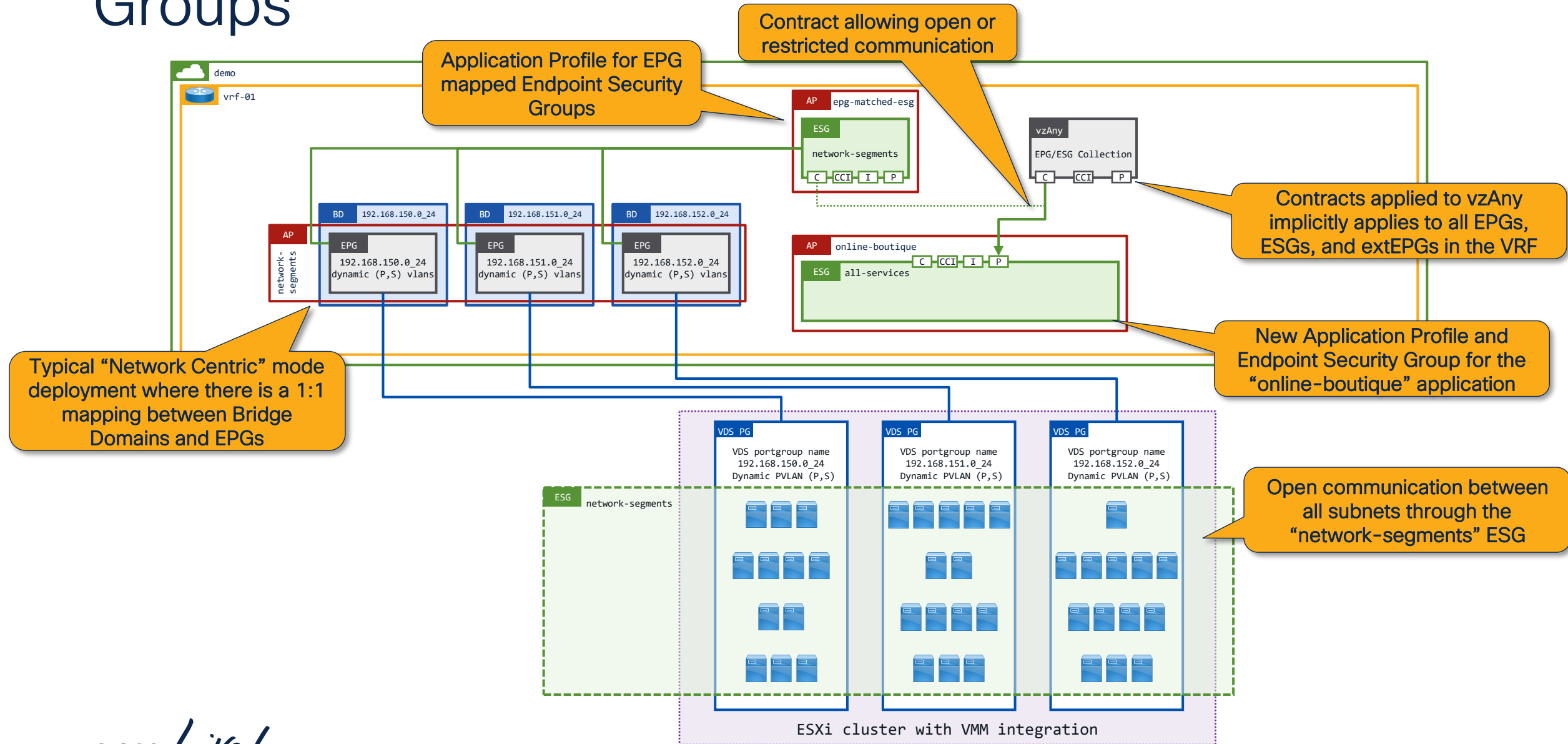
Application Knowledge taken from any source



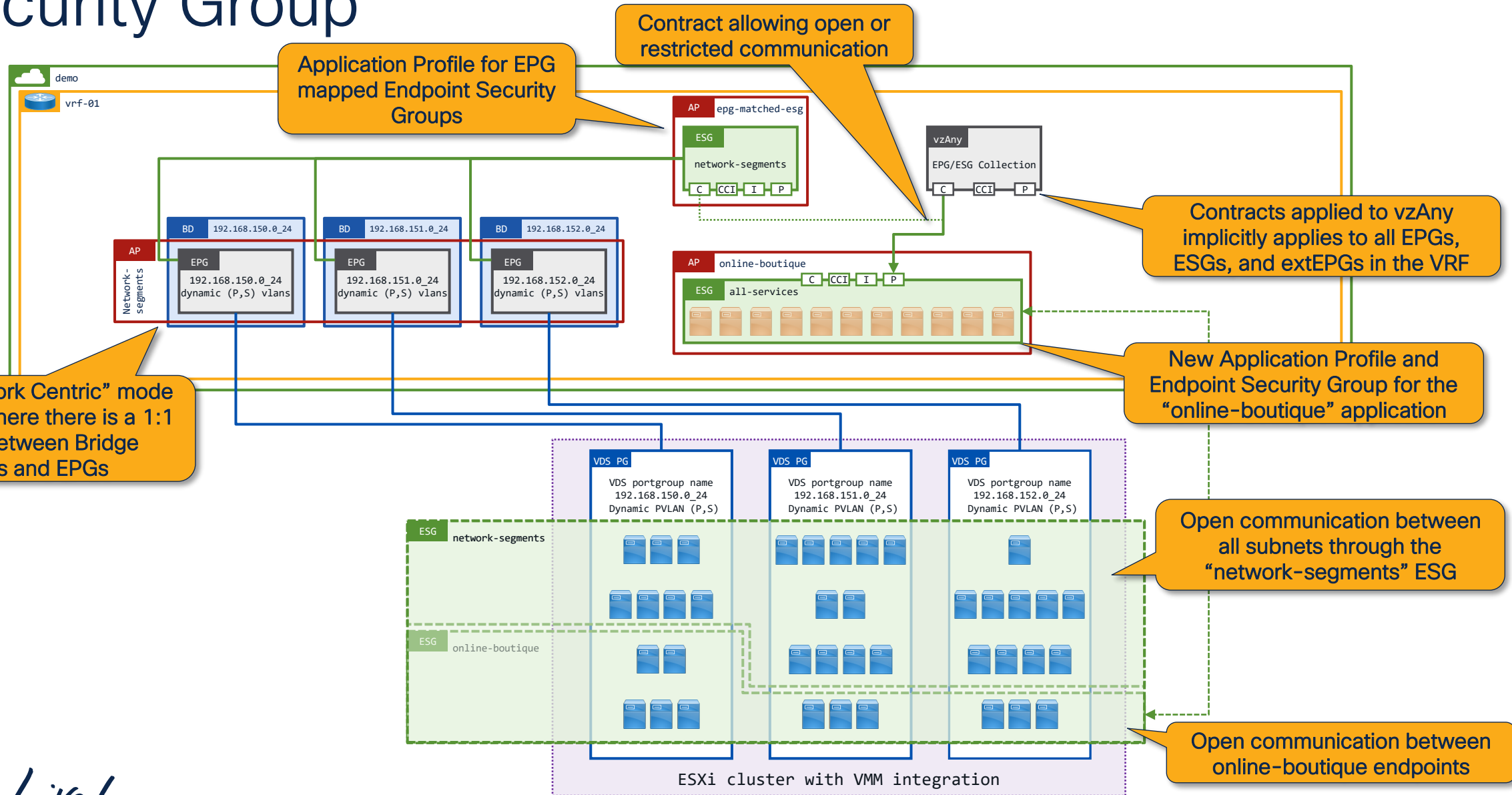
Physical or virtual workloads, with or without VMM Integration...!

You can convert 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 (manual/automated)

The screenshot displays the Cisco ACI configuration interface for a 'demo-non-vmm' environment. The left sidebar shows a navigation tree with categories like Application Profiles, Endpoint Security Groups, and Tag Selectors. The main panel is divided into two sections: 'Tag Selectors' and 'Endpoint MAC'.

Tag Selectors: A table with columns 'Tag Key', 'Value Operator', and 'Tag Value'. A single entry is shown: 'ApplicationName' with operator 'Equals' and value 'online-boutique'. A red box highlights this entry, with an arrow pointing to a blue callout box.

Endpoint MAC: A table with columns 'MAC Address', 'Bridge Domain', 'VRF', 'Tags', and 'Matching Tag Selector'. It lists several MAC addresses, all associated with 'vrf-01' and the 'online-boutique' application. A red box highlights the first row, with an arrow pointing to a blue callout box.

Callout Boxes:

- Define ESG Tag Selector:** ApplicationName = online-boutique
- Map MAC or IP address to Tag Value:** 00:50:56:A1:0A:90 = ApplicationName online-boutique

Annotations:

- An orange callout bubble points to the 'Tag Selectors' table with the text: **ACI Application Workload Tags**
- An orange callout bubble points to the 'Endpoint MAC' table with the text: **Match Endpoints to Workload Tags**

Automated conversion to “Application Centric”



Tagging Option 2: VMM Tag Mapping

The image shows a workflow for mapping vCenter tags to ACI tags. On the left, the vCenter interface displays a folder hierarchy for 'tn-demo-online-boutique', with 'tn-demo-online-boutique-frontend-service' selected. A context menu is open, showing 'Assign Tag...'. A yellow callout bubble points to this menu with the text 'vCenter Application Workload Tags'. On the right, the 'Assign Tag' dialog is open, showing a list of available tags. The tag 'tn-demo-online-boutique-frontend-service' is selected. A red box highlights the list of tags, and a red arrow points from this box to a yellow callout bubble at the bottom right that says 'ACI Application Workload Tags match vCenter Application Workload Tags'. On the bottom left, the ACI interface shows the 'Tag Selectors' table, which lists various tags and their values. A yellow callout bubble points to this table with the text 'ACI Application Workload Tags'.

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”

This object was created from the Terraform orchestrator. It is recommended to only make changes from the Terraform orchestrator.

demo

- Quick Start
- demo
 - Application Profiles
 - epg-matched-esg
 - Application EPGs
 - uSeg EPGs
 - Endpoint Security Groups
 - network-segments
 - network-segments
 - Networking
 - Contracts
 - Policies
 - Services
 - Security

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

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

Page 1 Of 1

Objects Per Page: 100

Displaying Objects 1 - 11 Of 11

Last Login Time: 2023-02-03T07:03 UTC+00:00

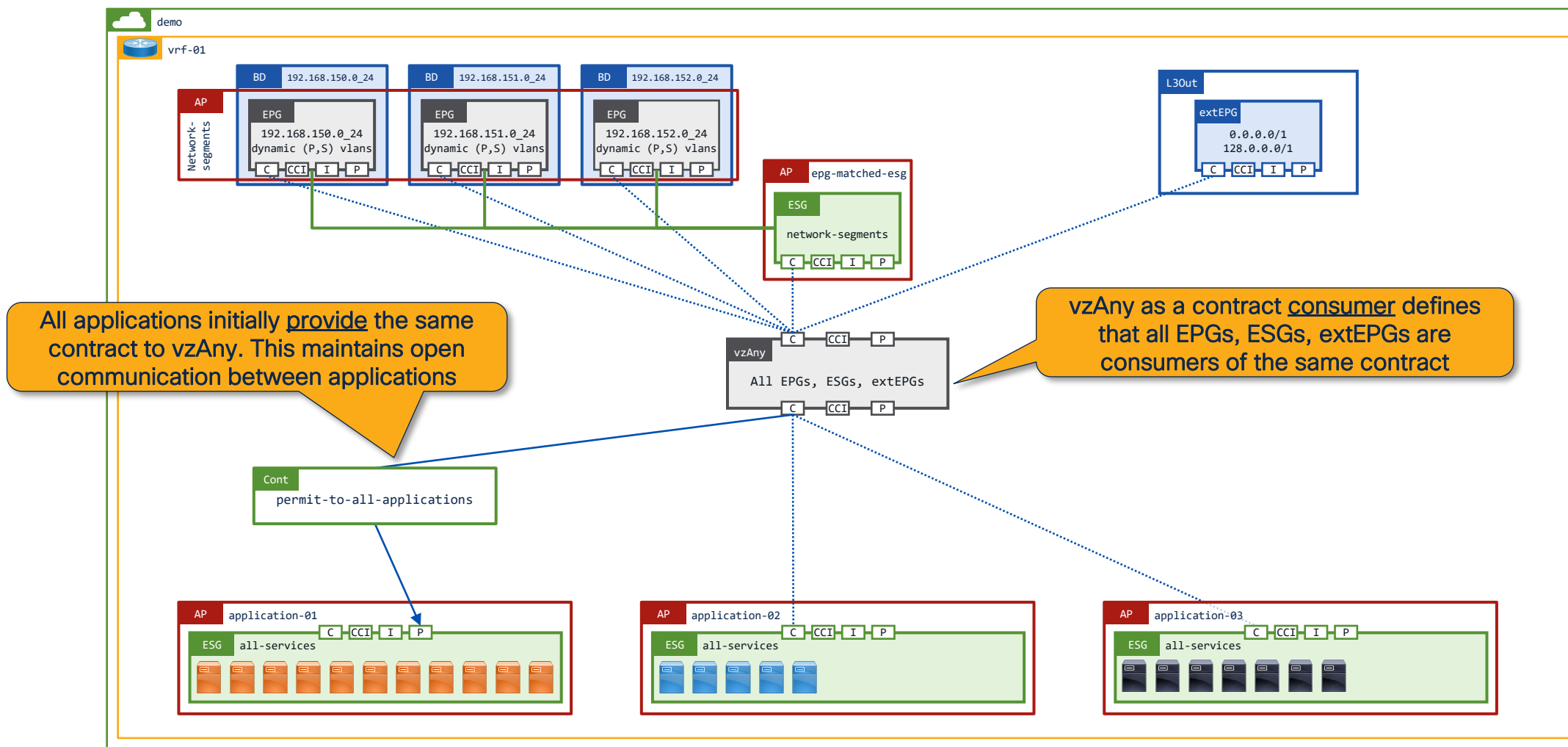
Current System Time: 2023-02-03T08:07 UTC+00:00

ssharmar@ssharmar-jumphost:~

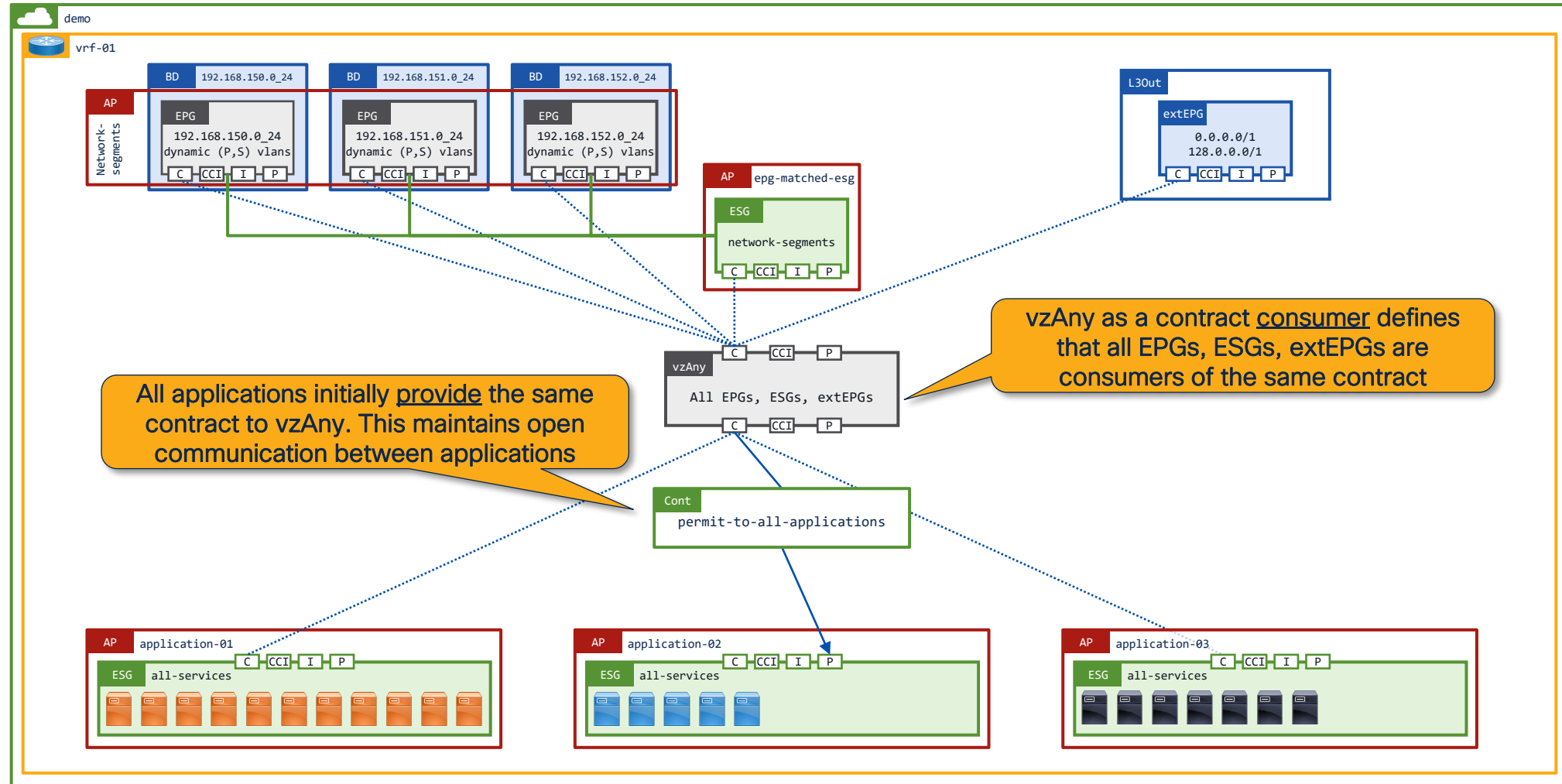
```
ssharmar-jumphost:~$ ping 192.168.152.101
```

Scaling application connectivity with vzAny...

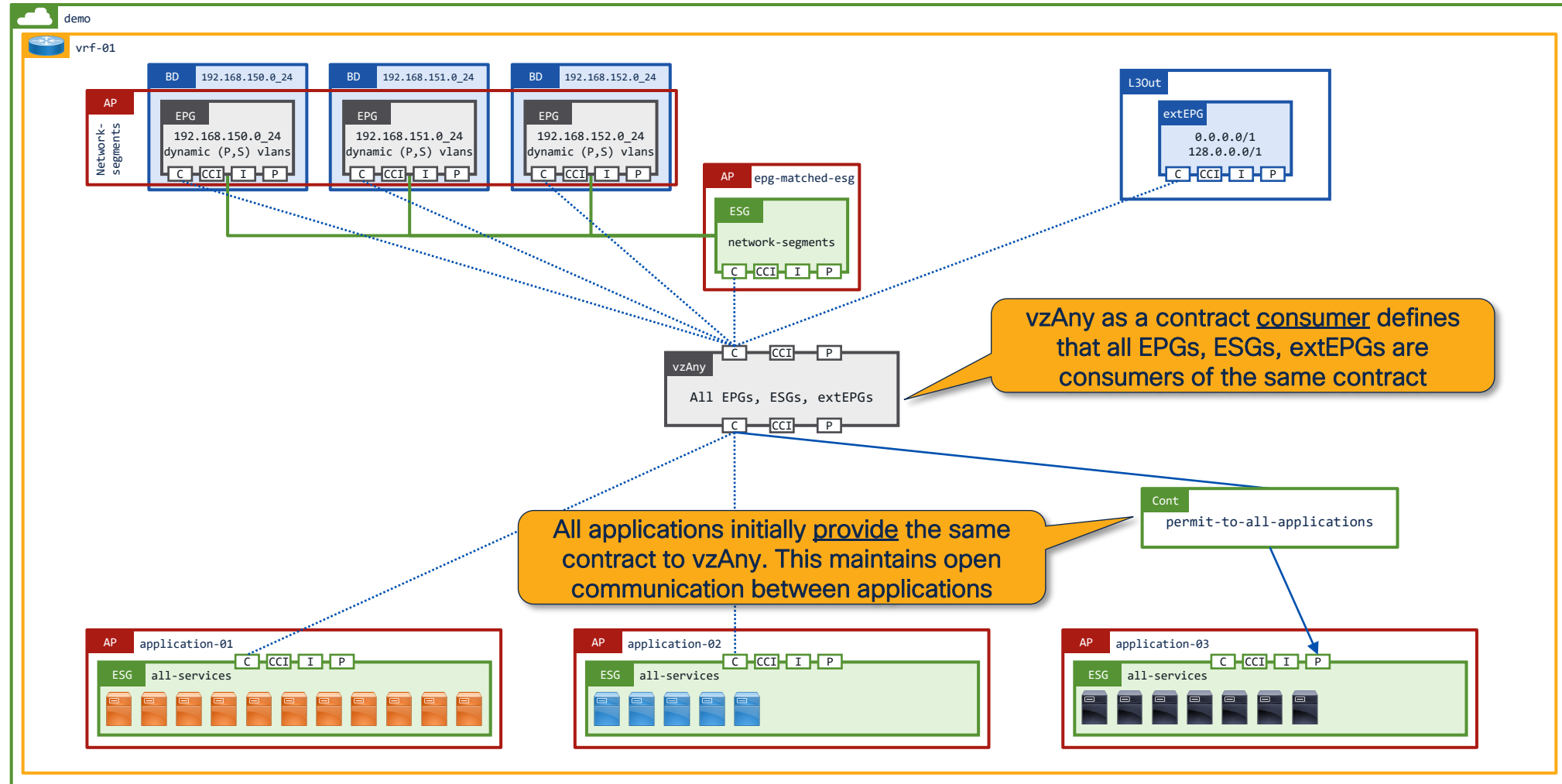
Scaling connectivity to “application-01”



Scaling connectivity to “application-02”



Scaling connectivity to “application-03”



Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

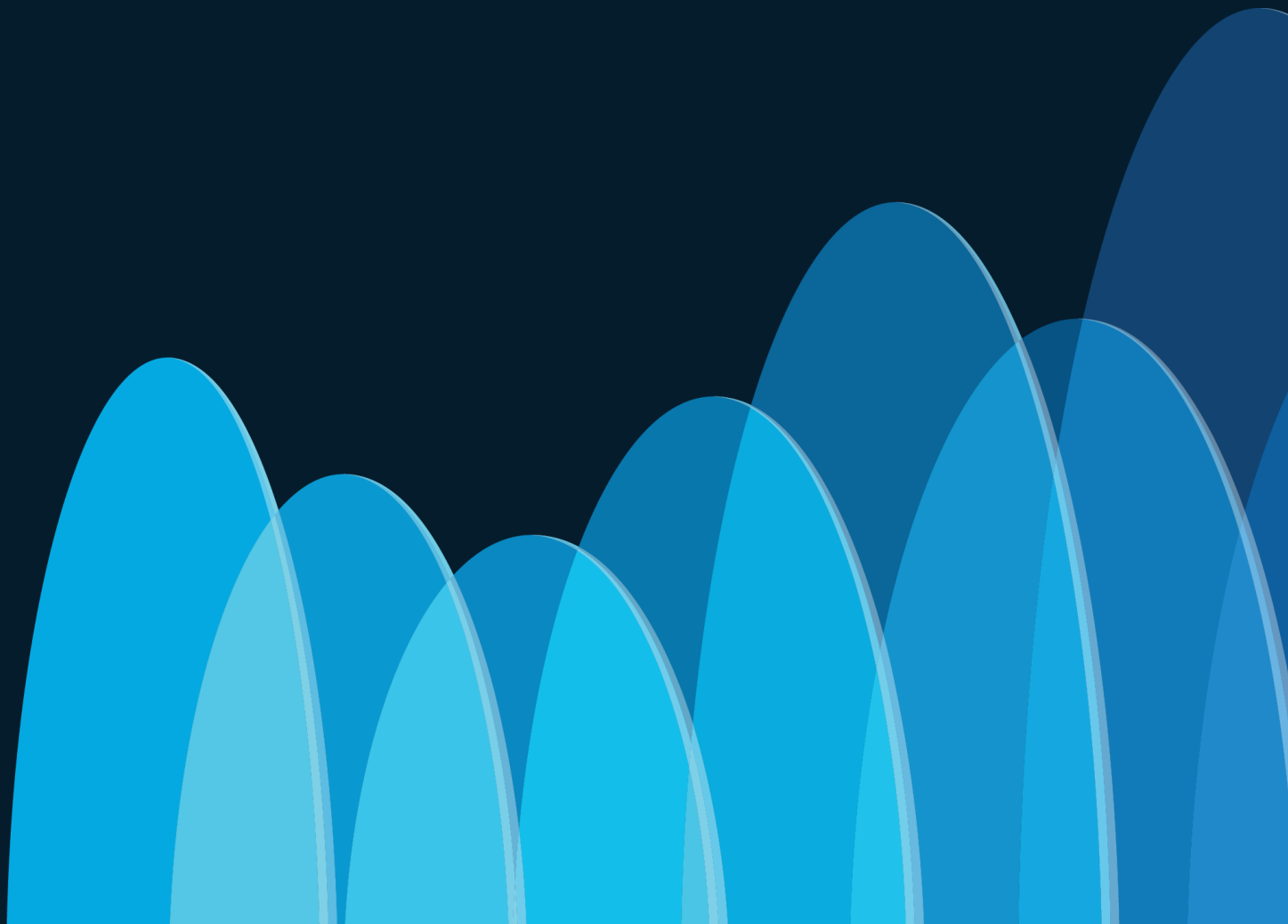
Understanding ACI security...

External Connectivity...

Increasing Security...

Automation Blueprints...

Wrapping up...



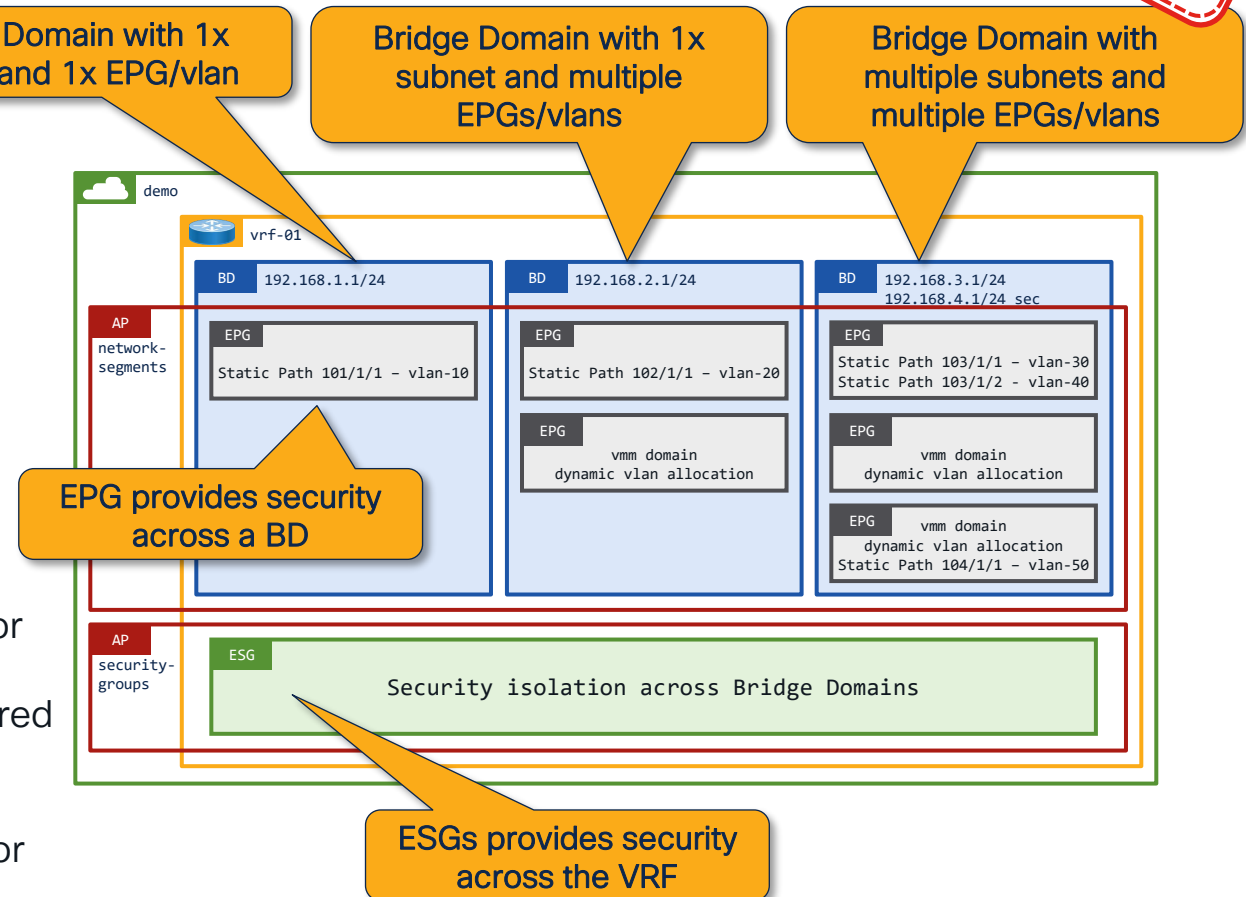
Why are ESGs a better classification option...?

EPG Security vs ESG Security

For your
reference

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

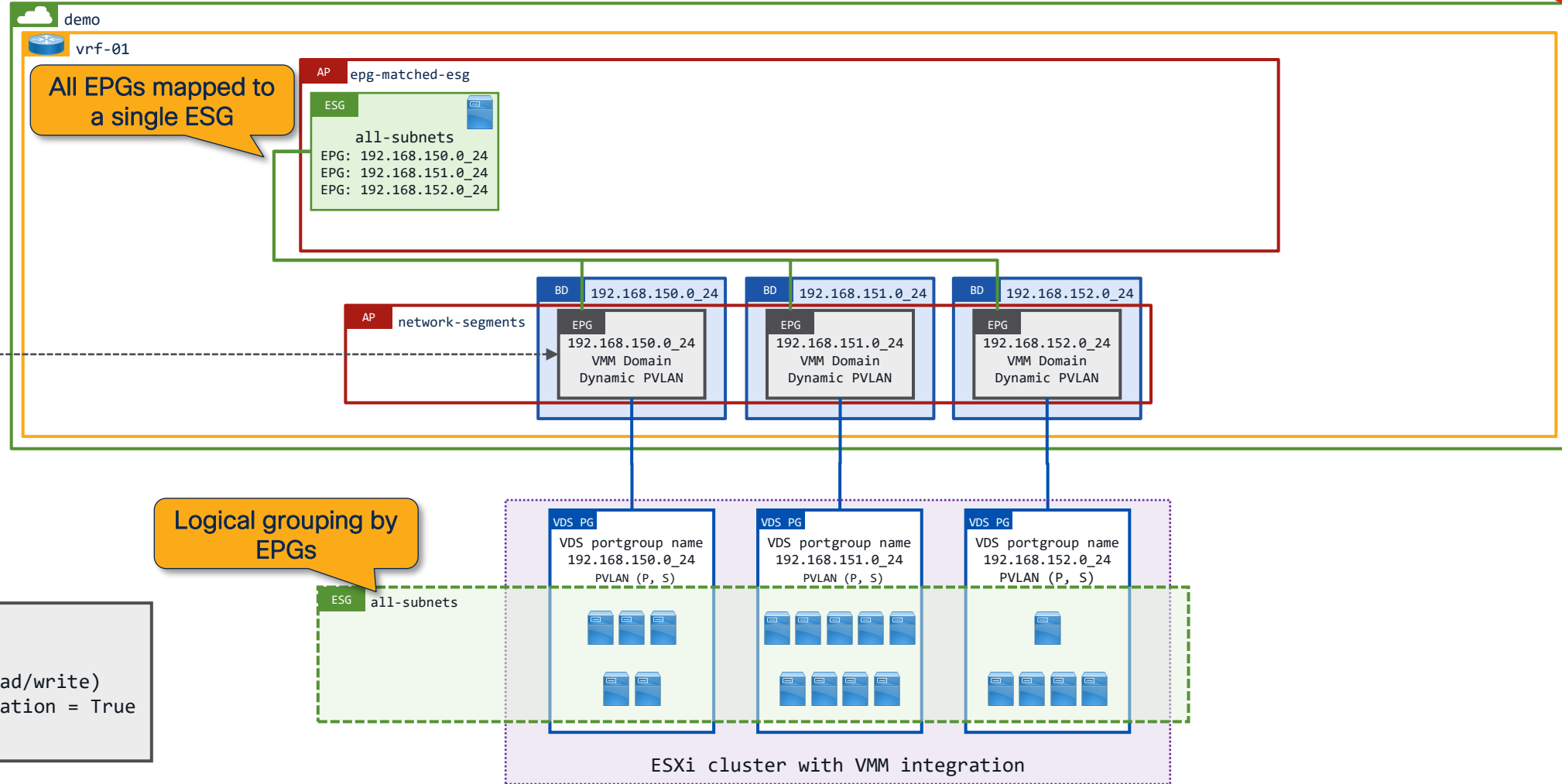


What are our endpoint mapping options...?

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

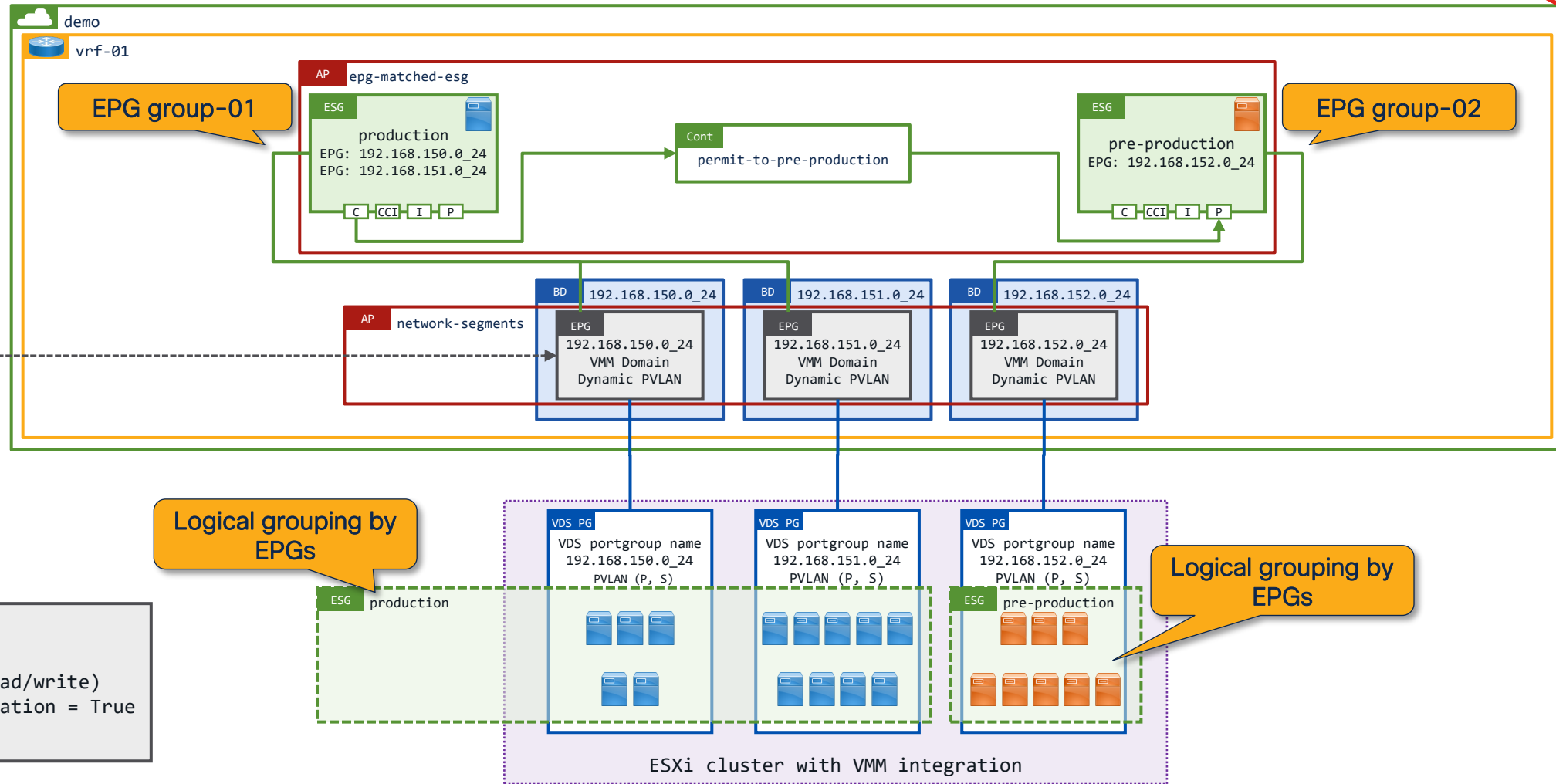
Option 1: EPG mapping to a single security zone

Open security
comparable to vzAny,
excluding the extEPG



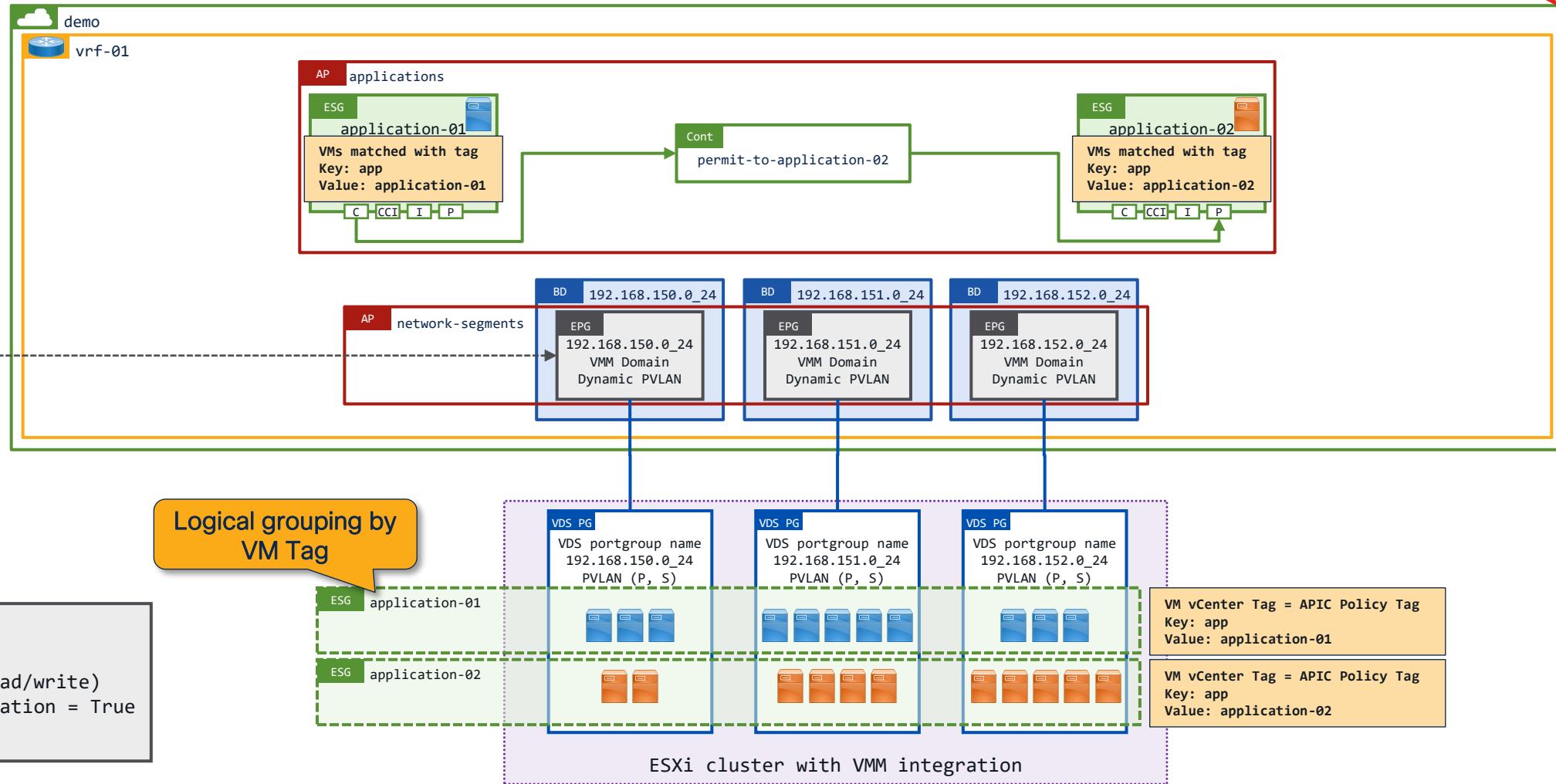
Option 2: EPG mapping for multiple security zones

Two or more security zones, e.g. Production and Pre-Production



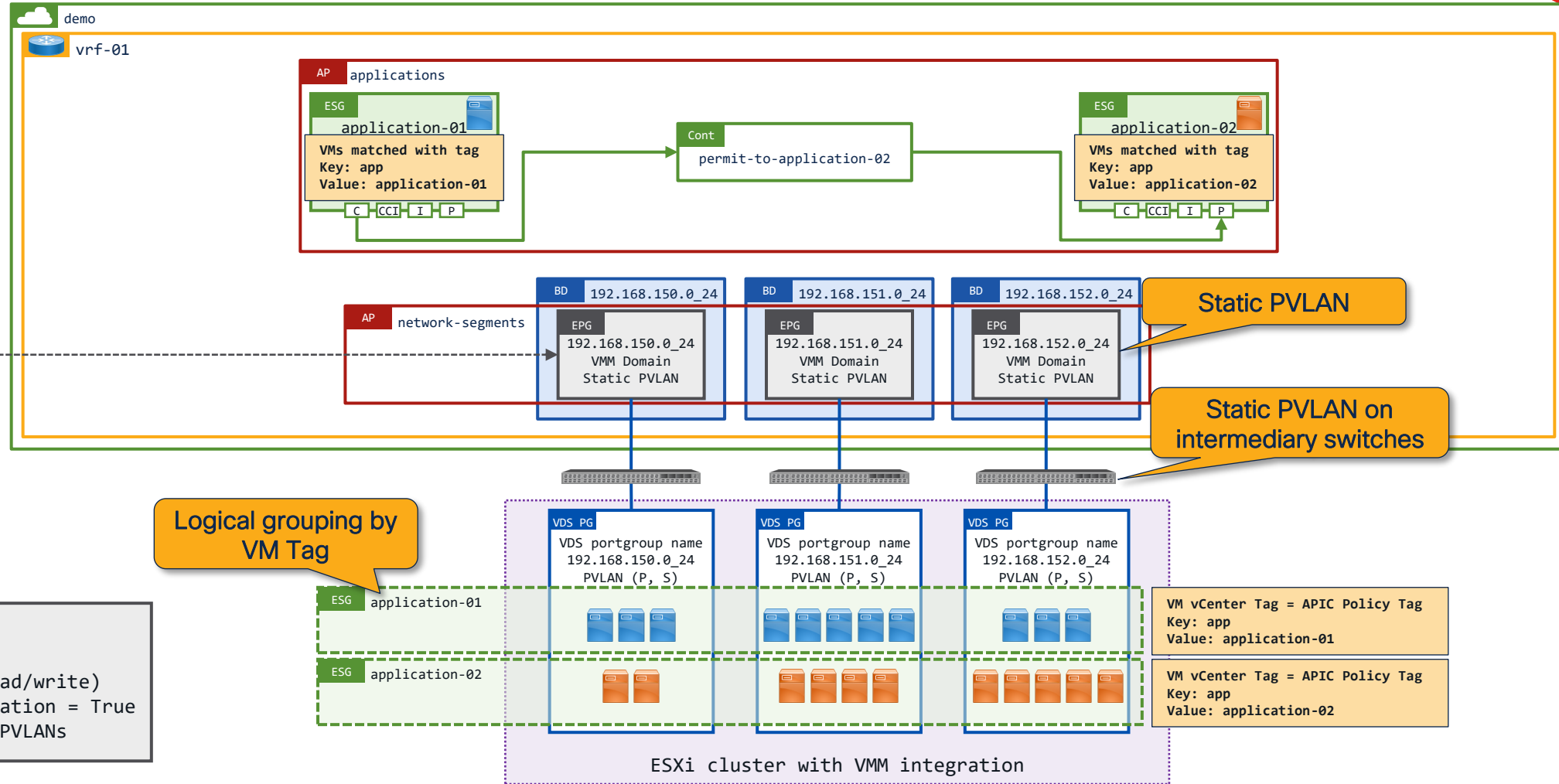
Option 3: Tag selectors with VMM integration

Endpoint assignment
using vCenter Tags.
Requires VMM
read/write integration



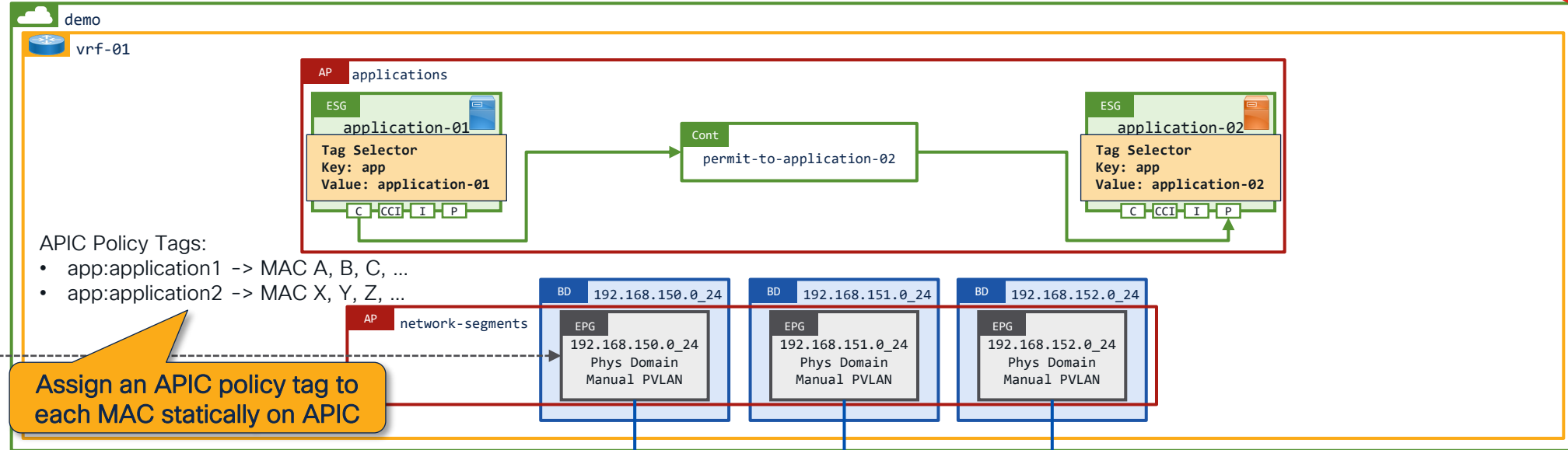
Option 4: Tag selectors with VMM integration and Intermediary switches

Intermediary switches
require PVLAN pre-
provisioning

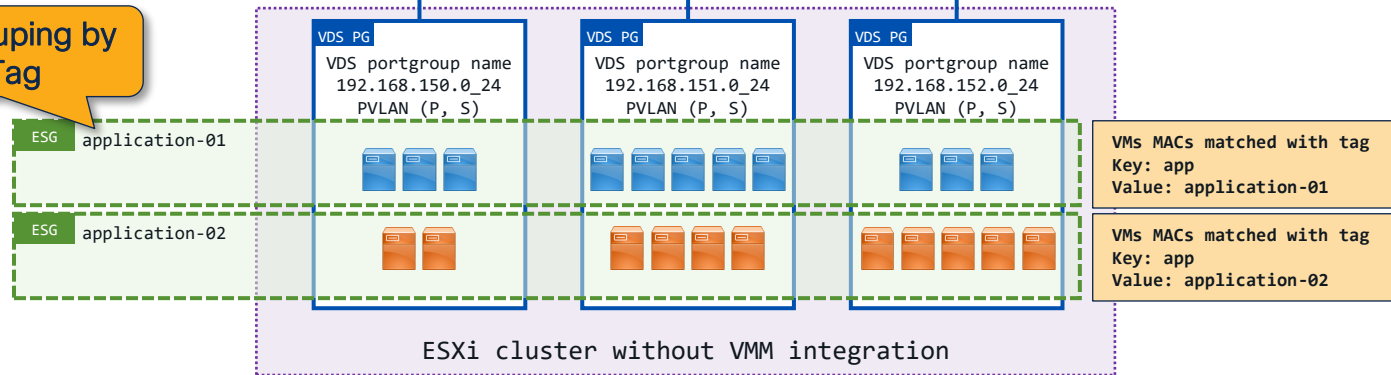


Option 5: MAC selectors, no VMM integration

Endpoint assignment using endpoint MAC addresses. Requires PVLAN on VDS



Logical grouping by MAC Tag



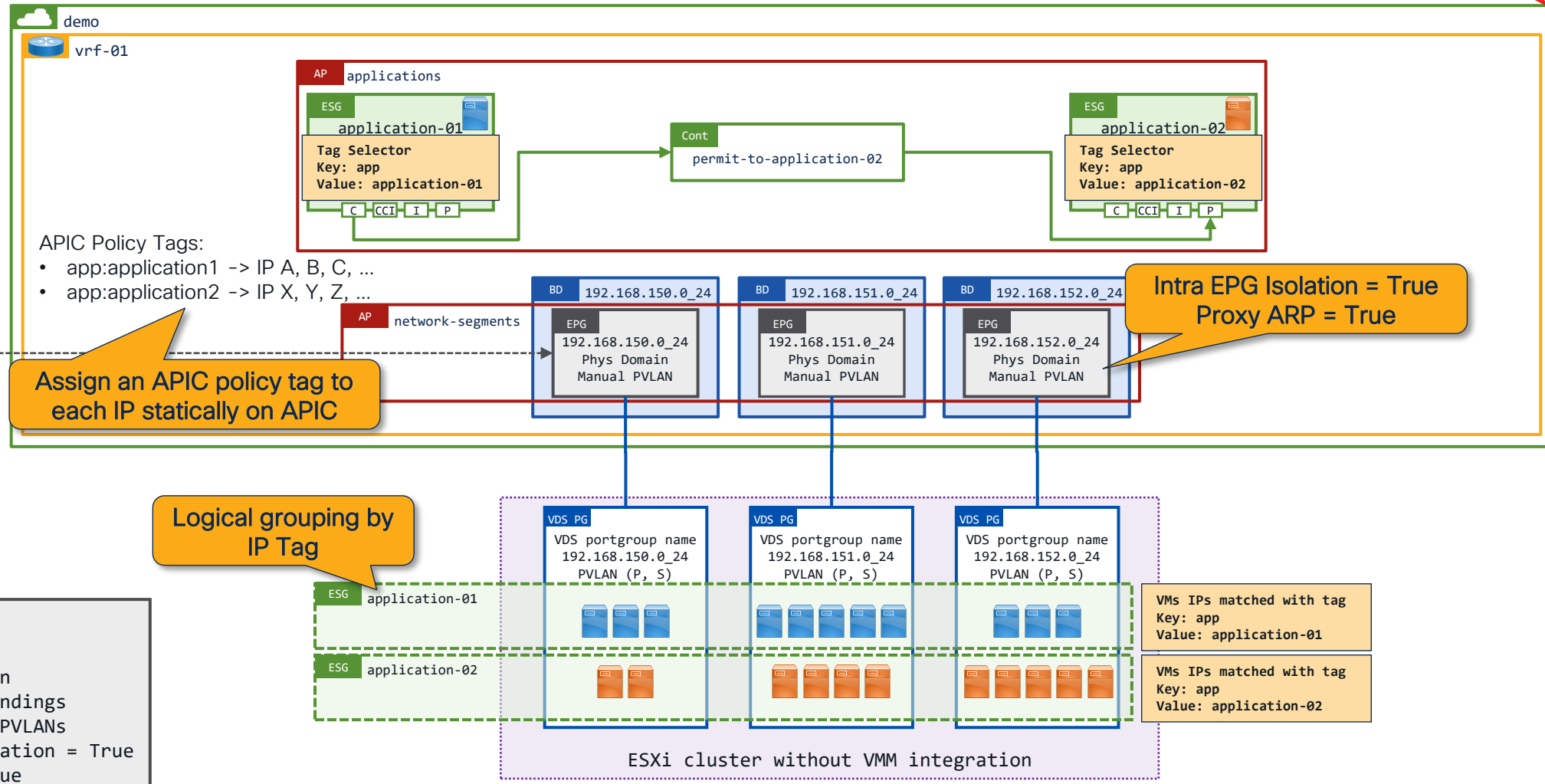
EPG

Settings:

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

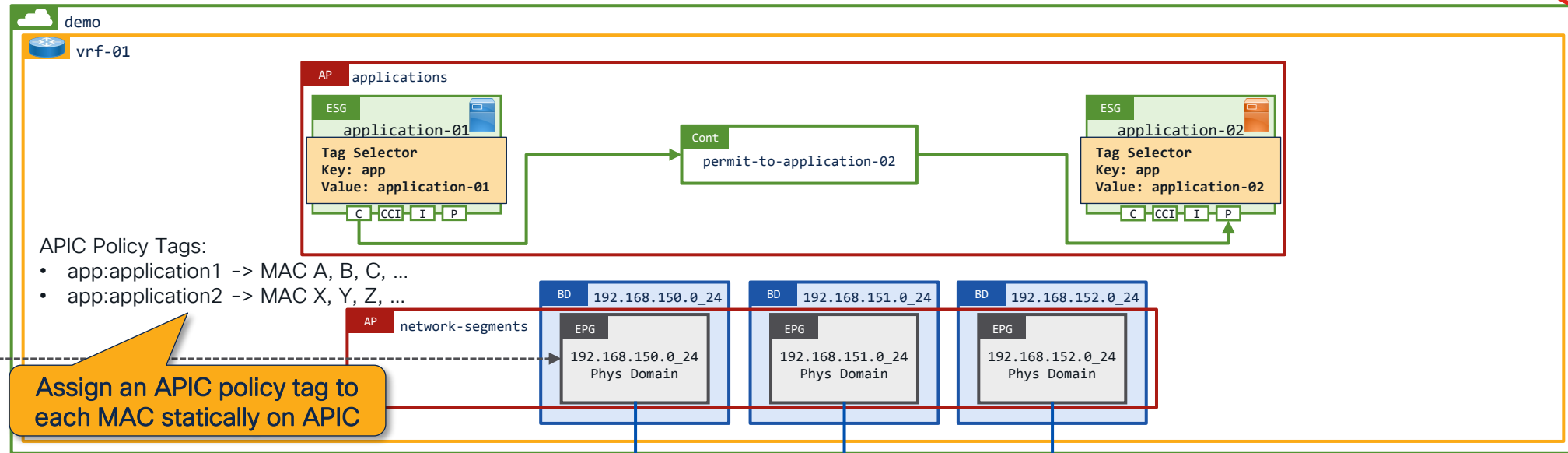
Option 6: IP selectors, no VMM integration

Endpoint assignment
using endpoint IP
addresses. Requires
PVLAN on VDS



Option 7: MAC selectors for bare metal

Endpoint assignment
using endpoint MAC
addresses



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

Assign an APIC policy tag to each MAC statically on APIC

Logical grouping by
MAC Tag

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

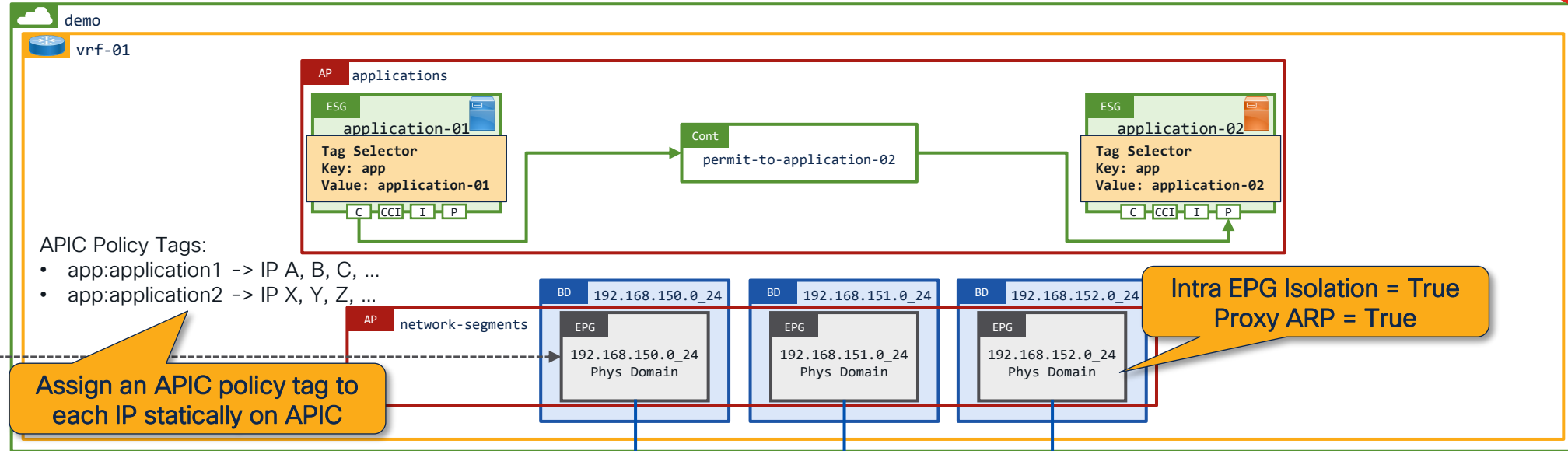
Bare metal MACs matched to the APIC tag
Key: app
Value: application-02

Settings:

- Physical Domain
- Static path bindings

Option 8: IP selectors for bare metal

Endpoint assignment
using endpoint IP
addresses



Assign an APIC policy tag to each IP statically on APIC

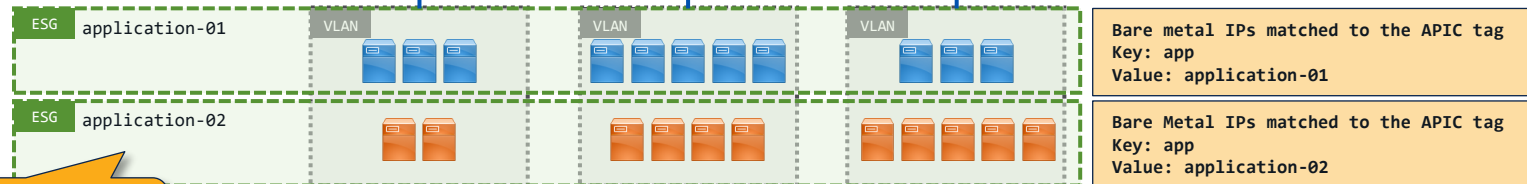
Intra EPG Isolation = True
Proxy ARP = True

EPG

Settings:

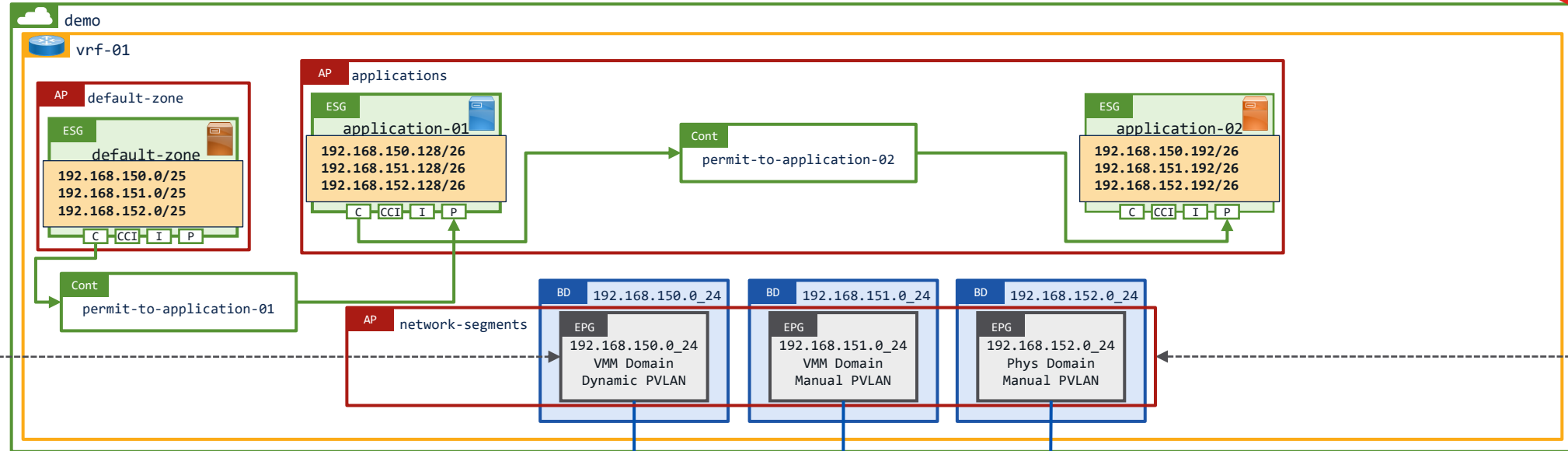
- Physical Domain
- Static path bindings
- Intra EPG Isolation = True
- Proxy ARP = True

Logical grouping by
IP Tag



Option 9: Subnet selectors with mixed Domains

Endpoint assignment
using subnet ranges



Static PVLAN on intermediary switches

EPG

Settings:

- VMM Domain
- Allow uSegmentation = True
- Manual/static PVLANS



Endpoints matched to subnets

Key: app
Value: application-01

Endpoints matched to subnets

Key: app
Value: application-02

Endpoints matched to subnets

Key: default
Value: default-zone

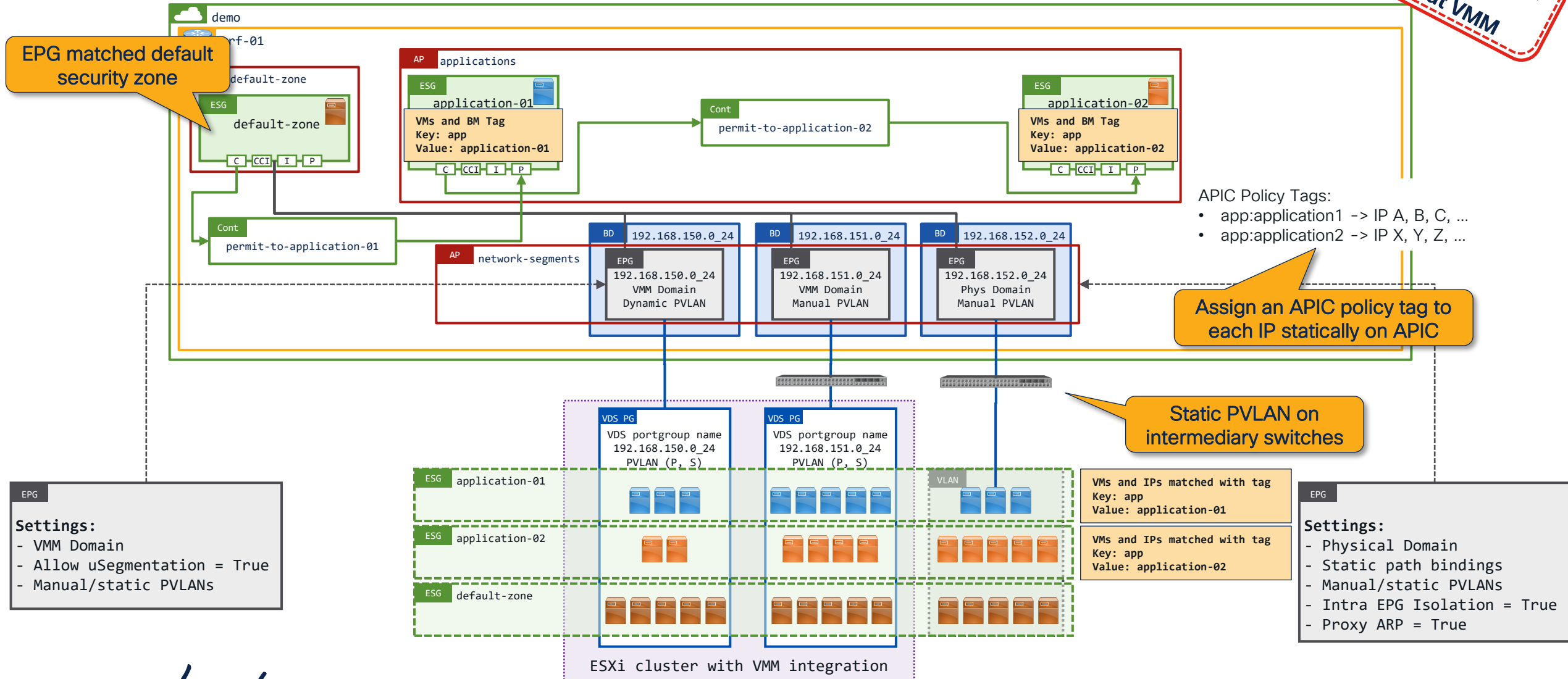
EPG

Settings:

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

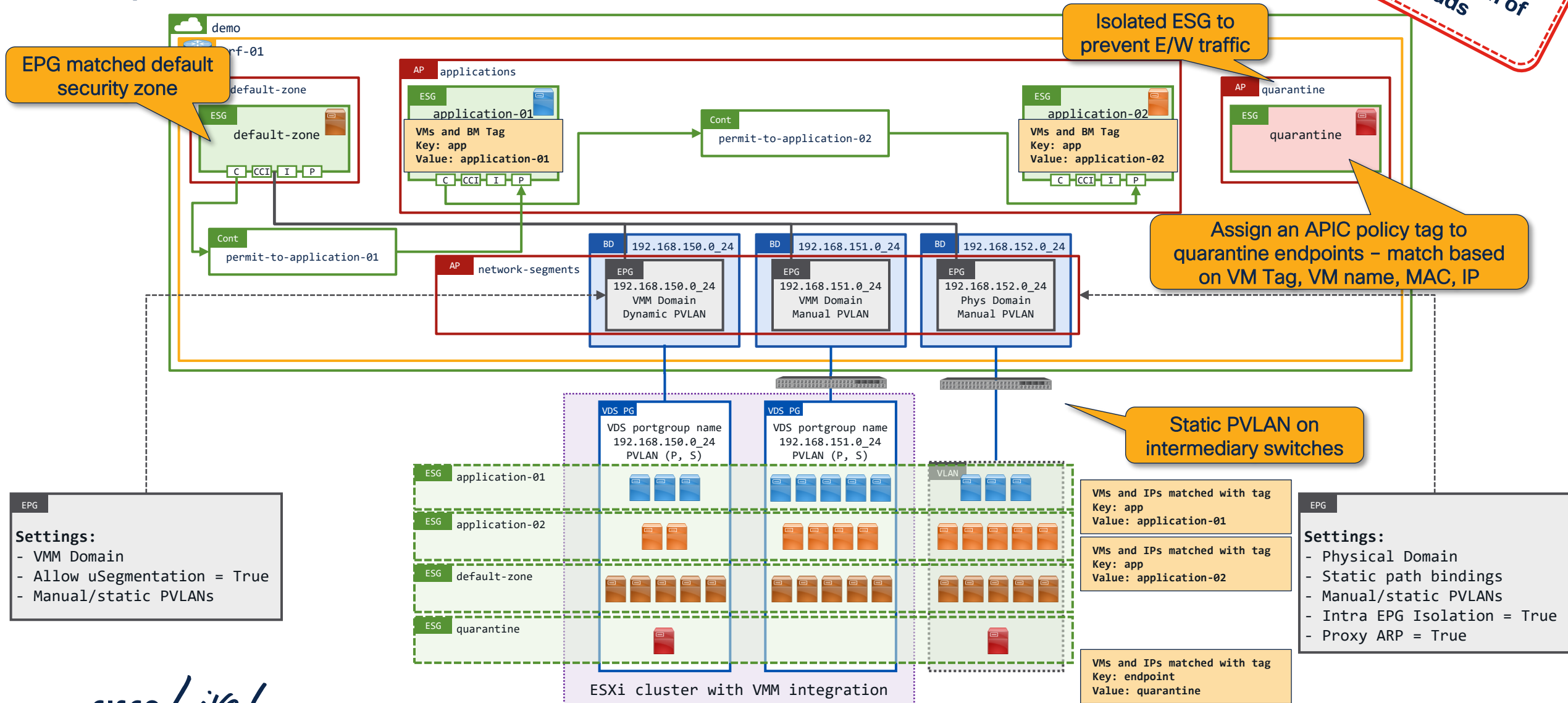
Option 10: Combined solution with/without VMM

Fully integrated solution for bare metal and VM's, with/without VMM



Option 11: Combined solution + Quarantine

Quarantine ESG allows targeted isolation of workloads



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...

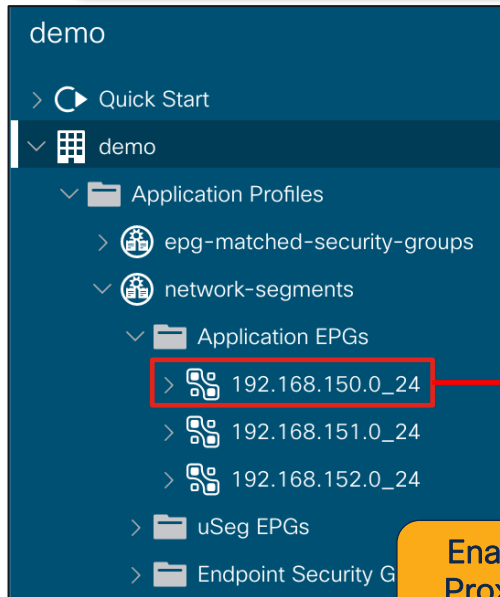
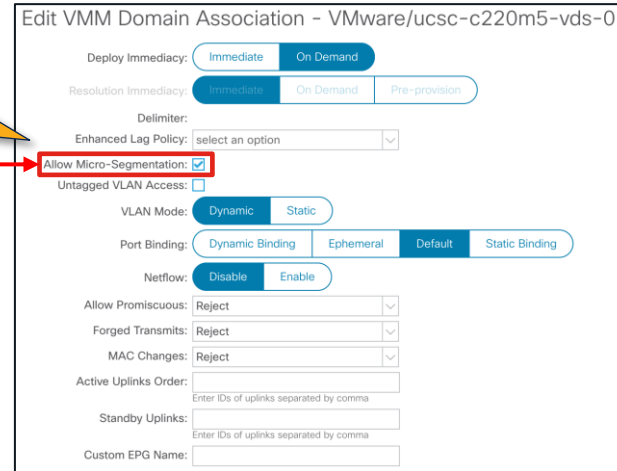
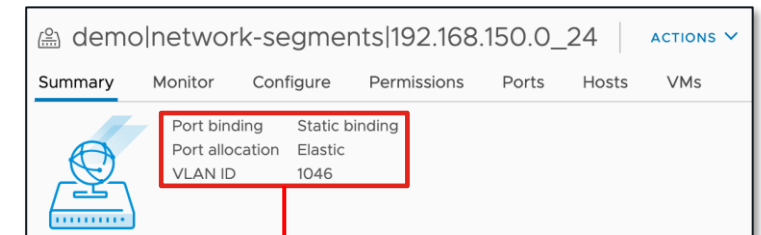
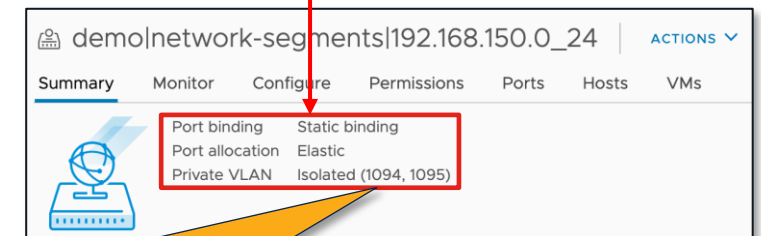
Proxy ARP

Why Proxy ARP...?

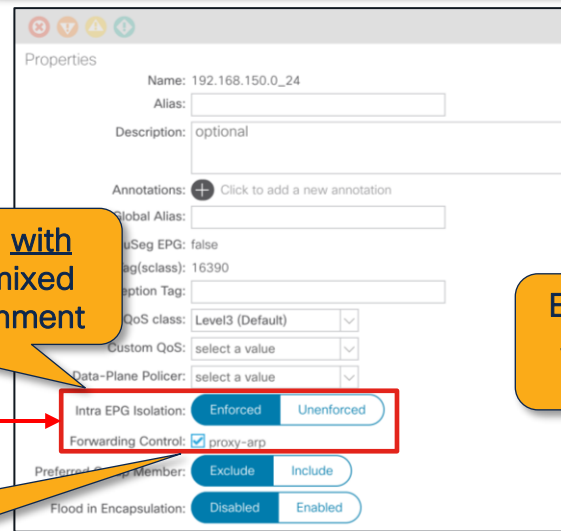


How do you enable Proxy ARP on the Leaf Switches...?

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



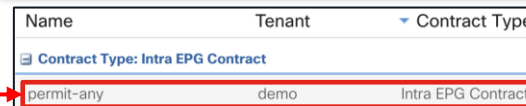
Enable Intra EPG isolation with Proxy ARP if you have a mixed virtual and physical environment



Proxy ARP is only available when Intra ESG isolation is enabled

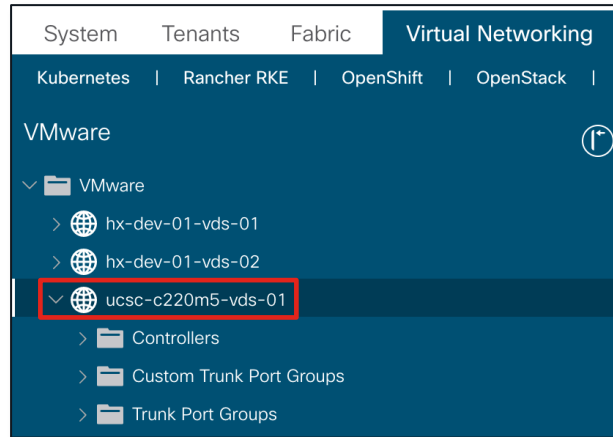
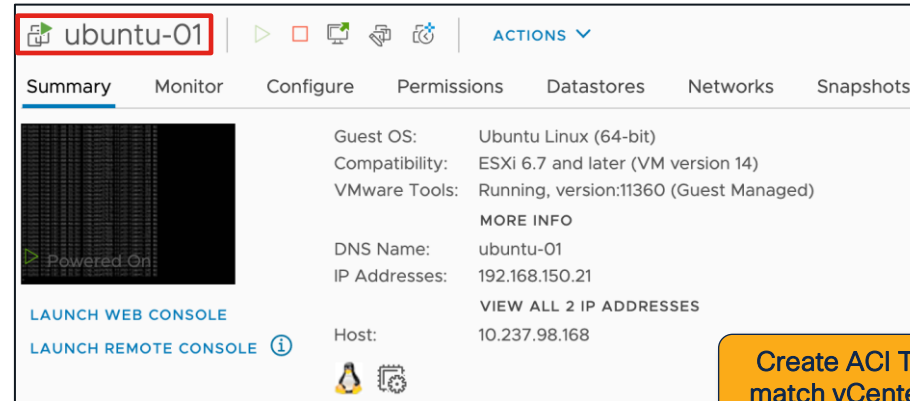
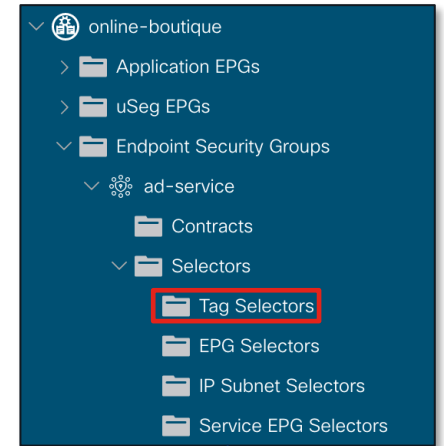
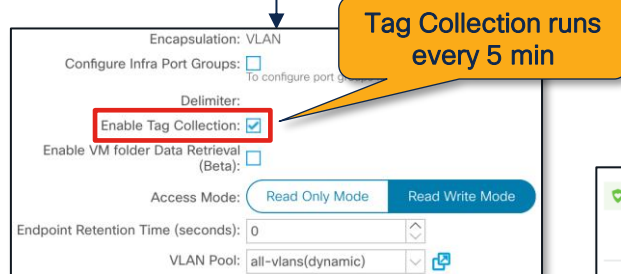
Enabling Intra EPG isolation / Allow Micro-Segmentation configures PVLANS on the port group

Add an Intra EPG Contract



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

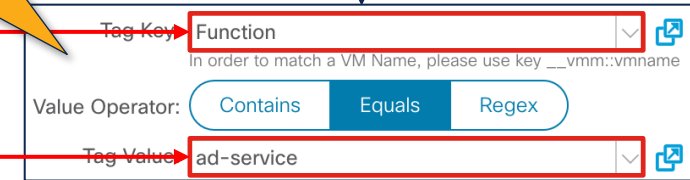
Dynamic Policy Tag matching from vCenter



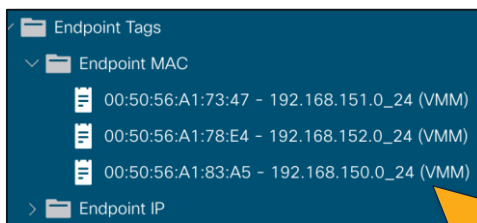
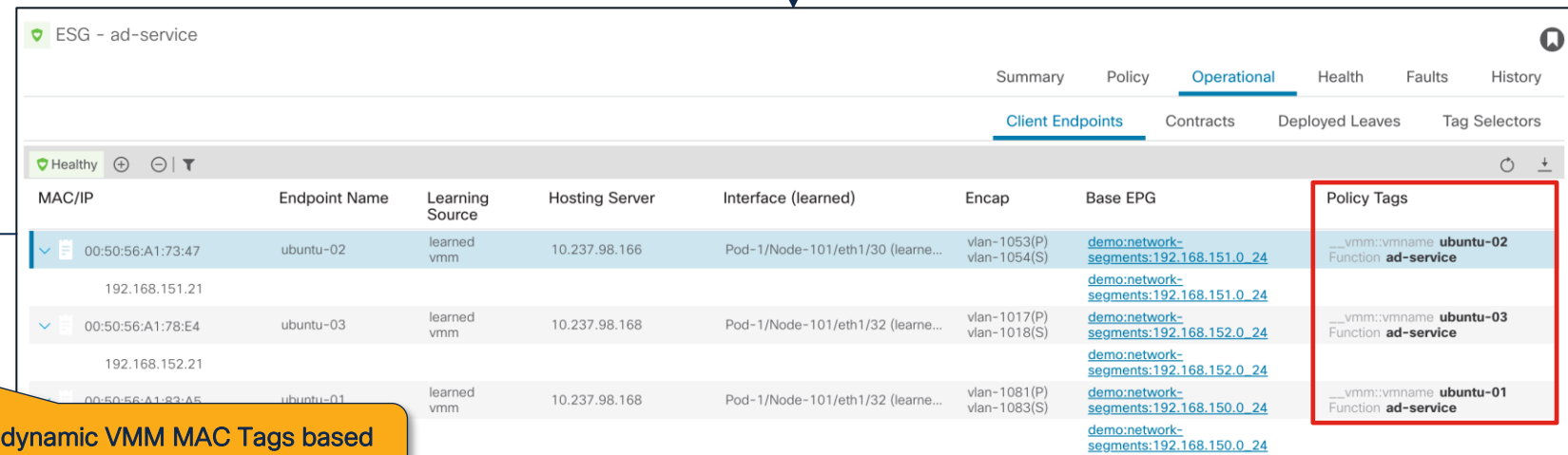
Tag Collection runs every 5 min



Create ACI Tags to match vCenter Tags



Tenant → Policies → Endpoint Tags



CISCO *Live!*

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

Static endpoint mapping...

Static Policy Tags on APIC

Static Endpoints

IP address ranges

MAC addresses

IP addresses

Policy Tags: + Click to add a new tag
Function **ad-service** X

Tag Selectors

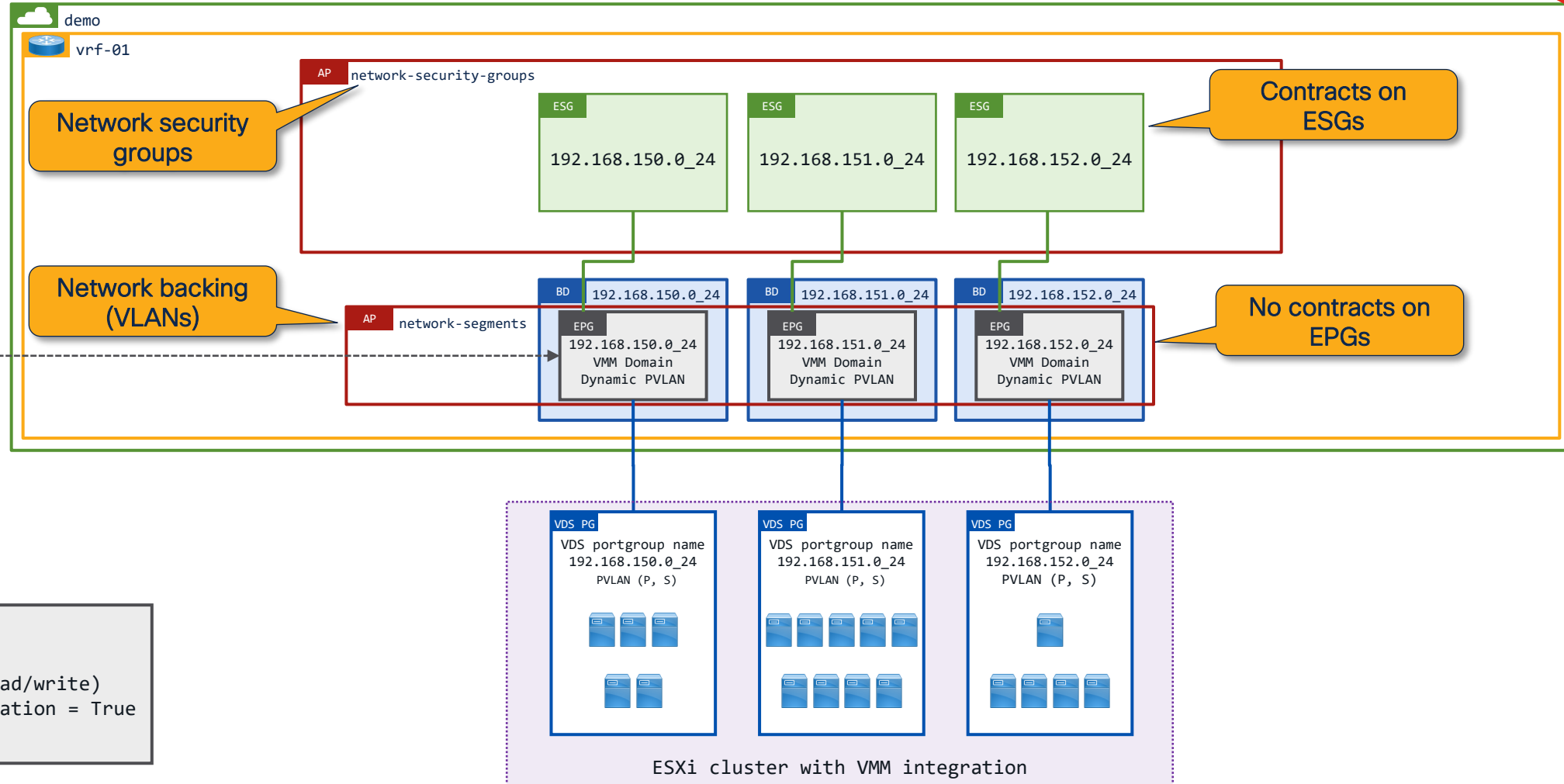
Associated Object

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-[*]

What if you have a Greenfield deployment...?

Greenfield option – 1:1 EPG to ESG mapping

Separate network
backing from
classification/security



Consider automated static MAC tagging derived from the endpoint IP address...

Works for Bare Metal and VMs, with or without VMM Integration...

Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

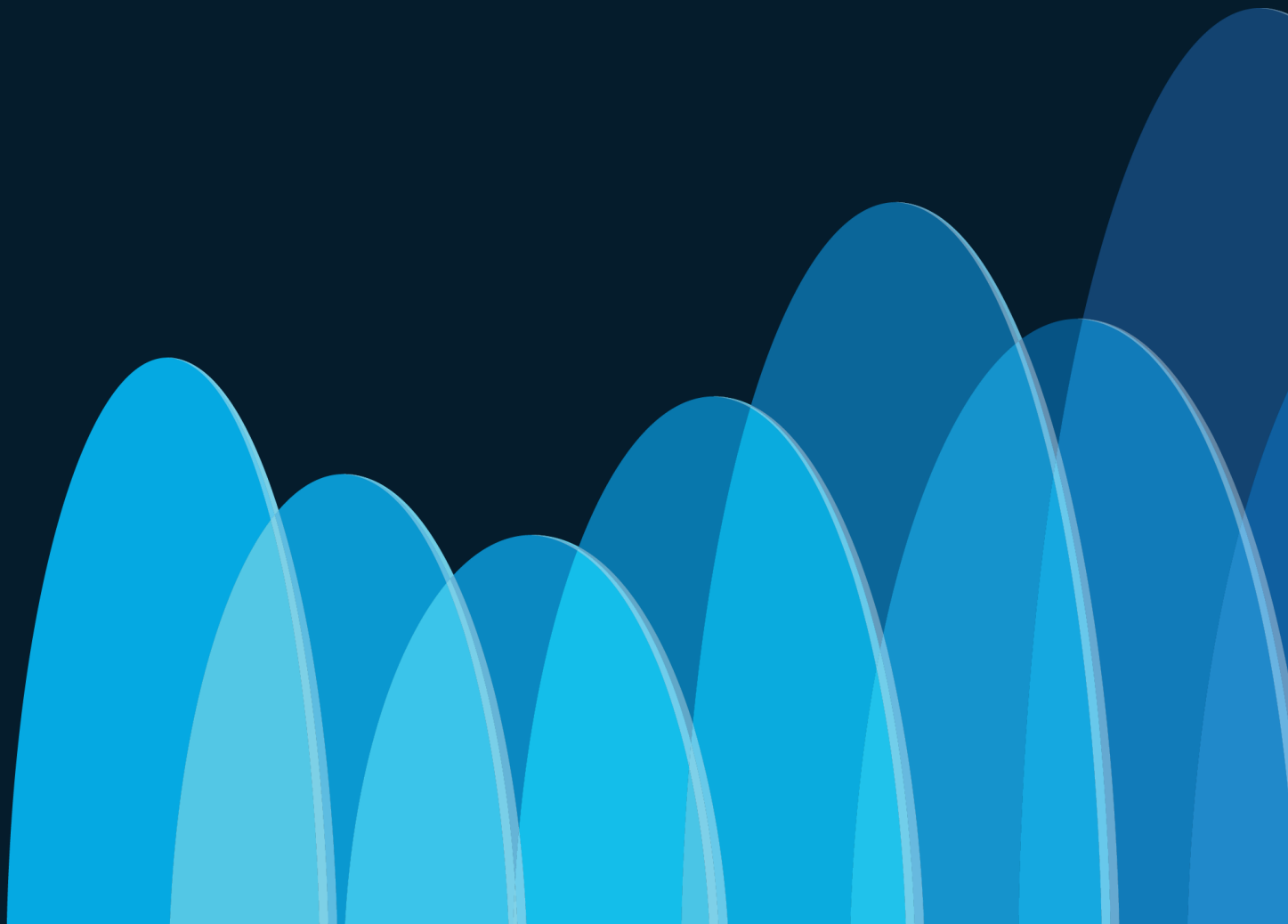
Understanding ACI security...

External Connectivity...

Increasing Security...

Automation Blueprints...

Wrapping up...



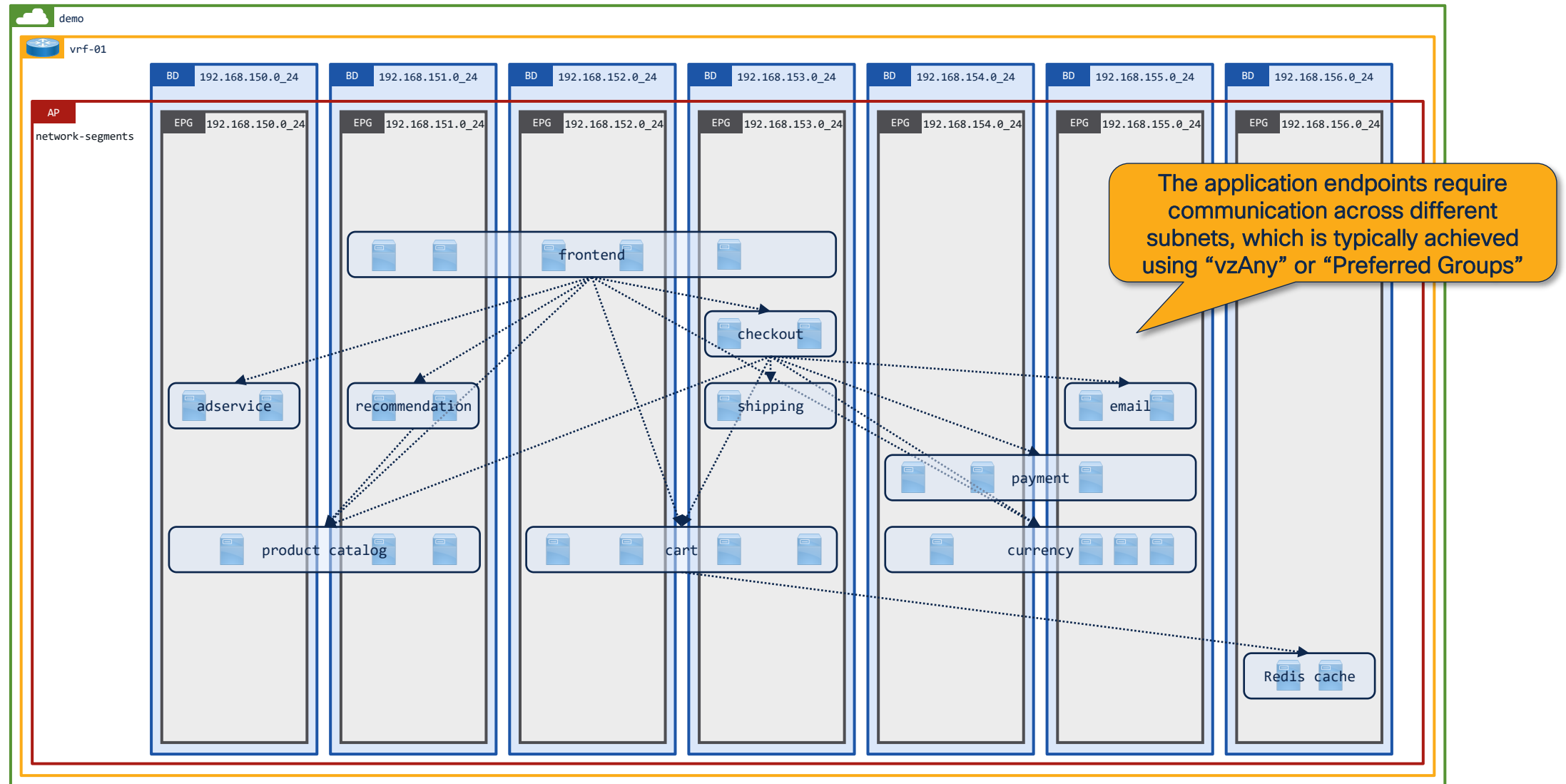
Allowing open
communication...

There are four options to allow open communication...

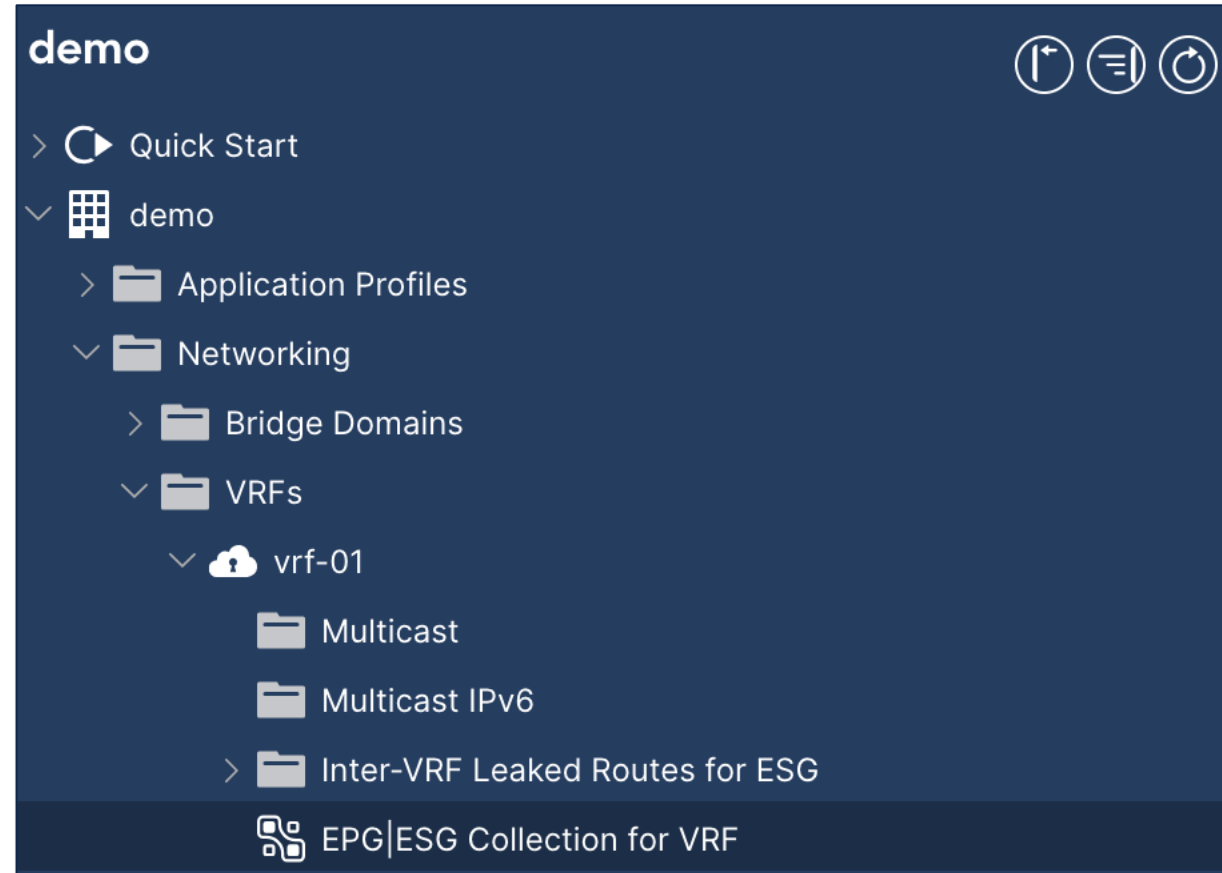
<https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-743951.html#Migrationexample>

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

Existing applications typically require unrestricted communication



vzAny

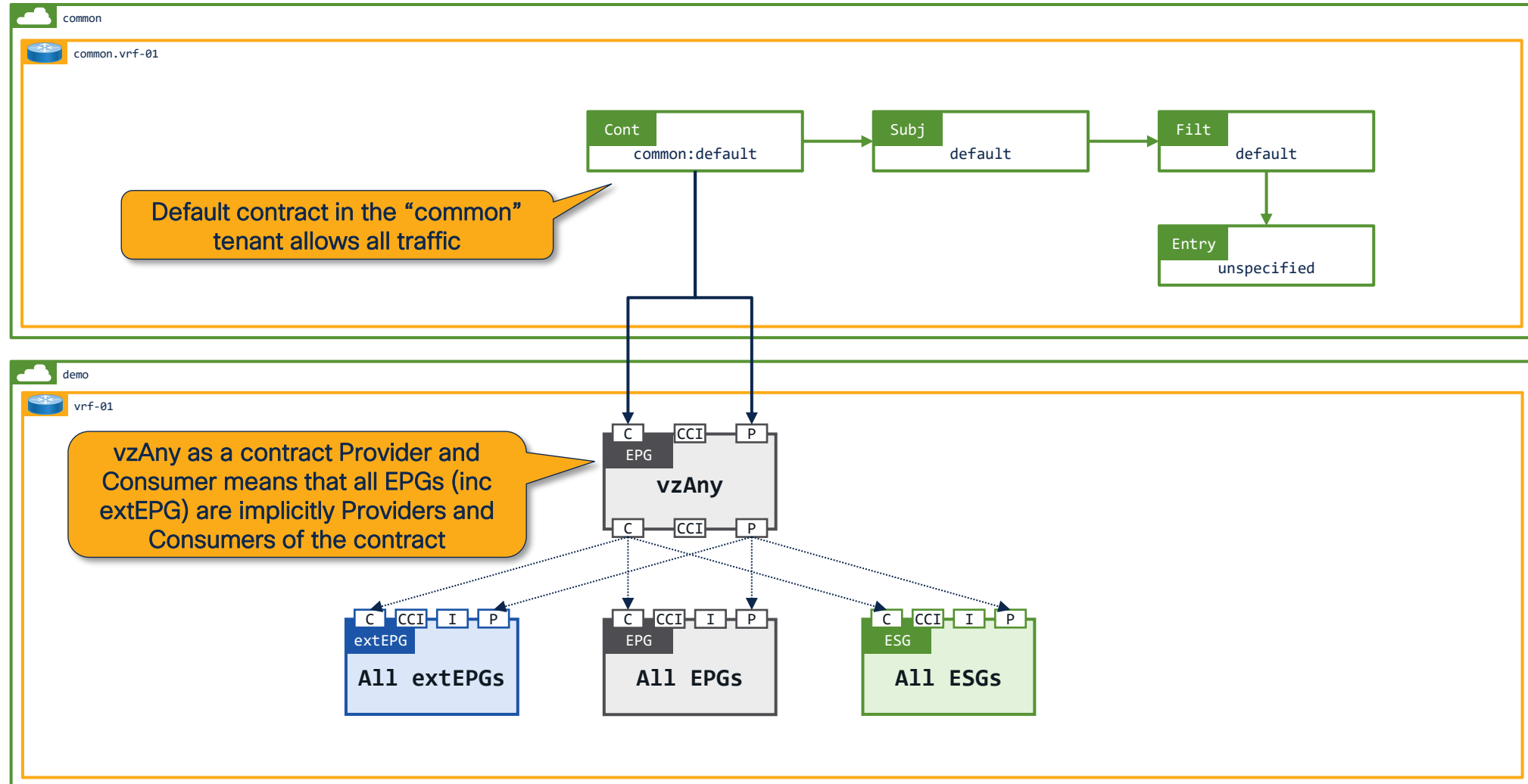


The great thing about vzAny provide/consume is that it allows open communication between all endpoints...

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

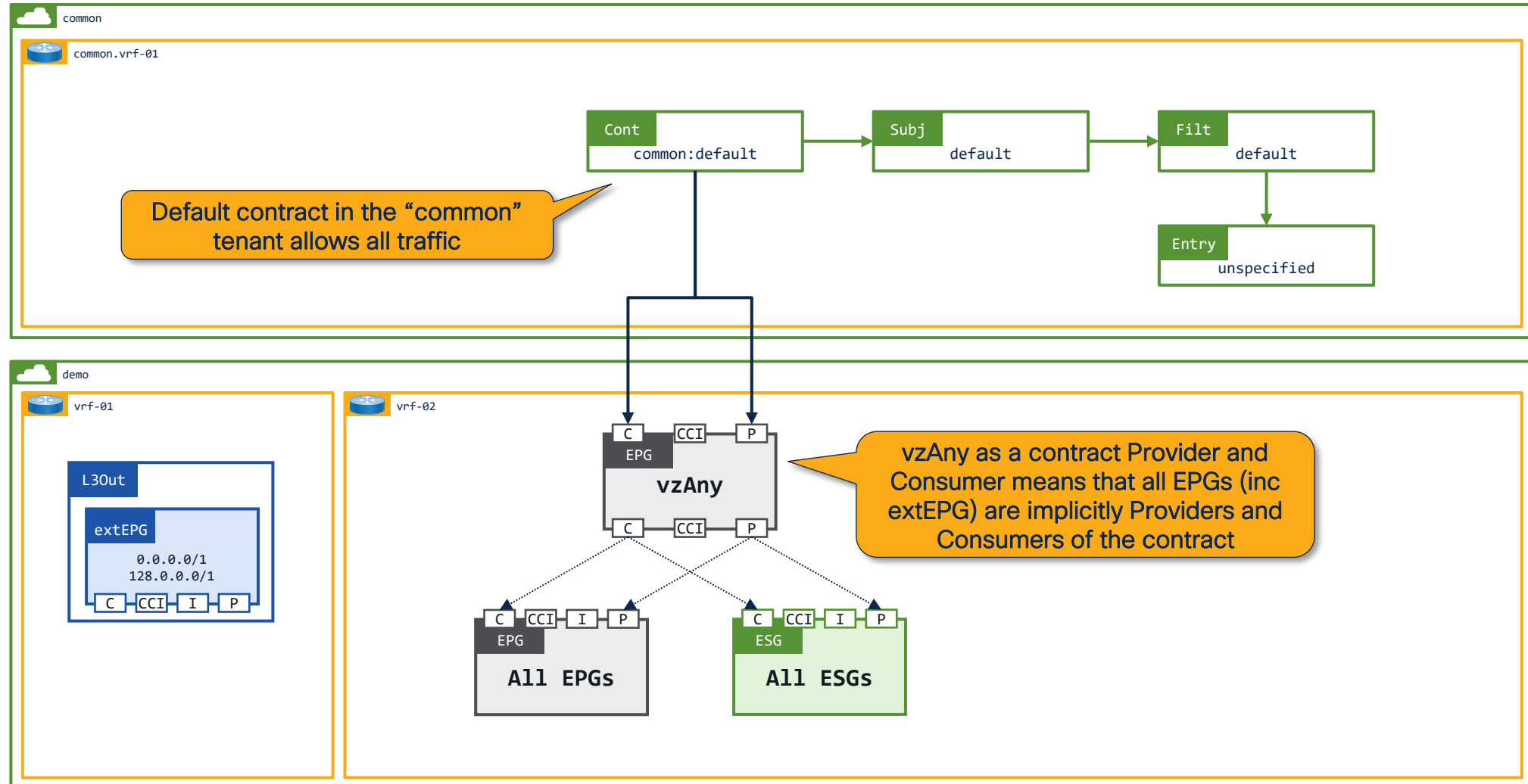
vzAny Operation – Consumer and Provider

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



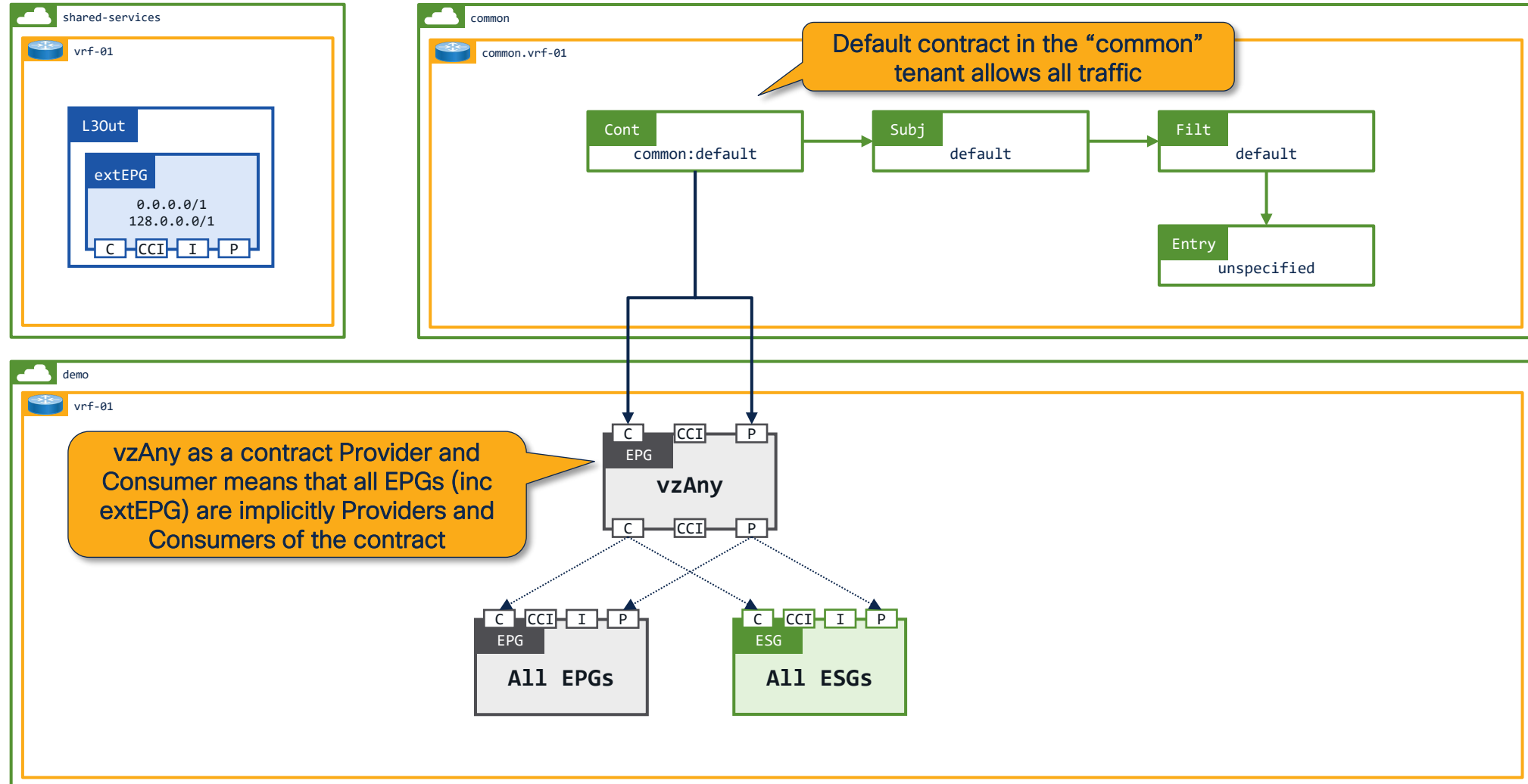
vzAny Operation – Consumer and Provider

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



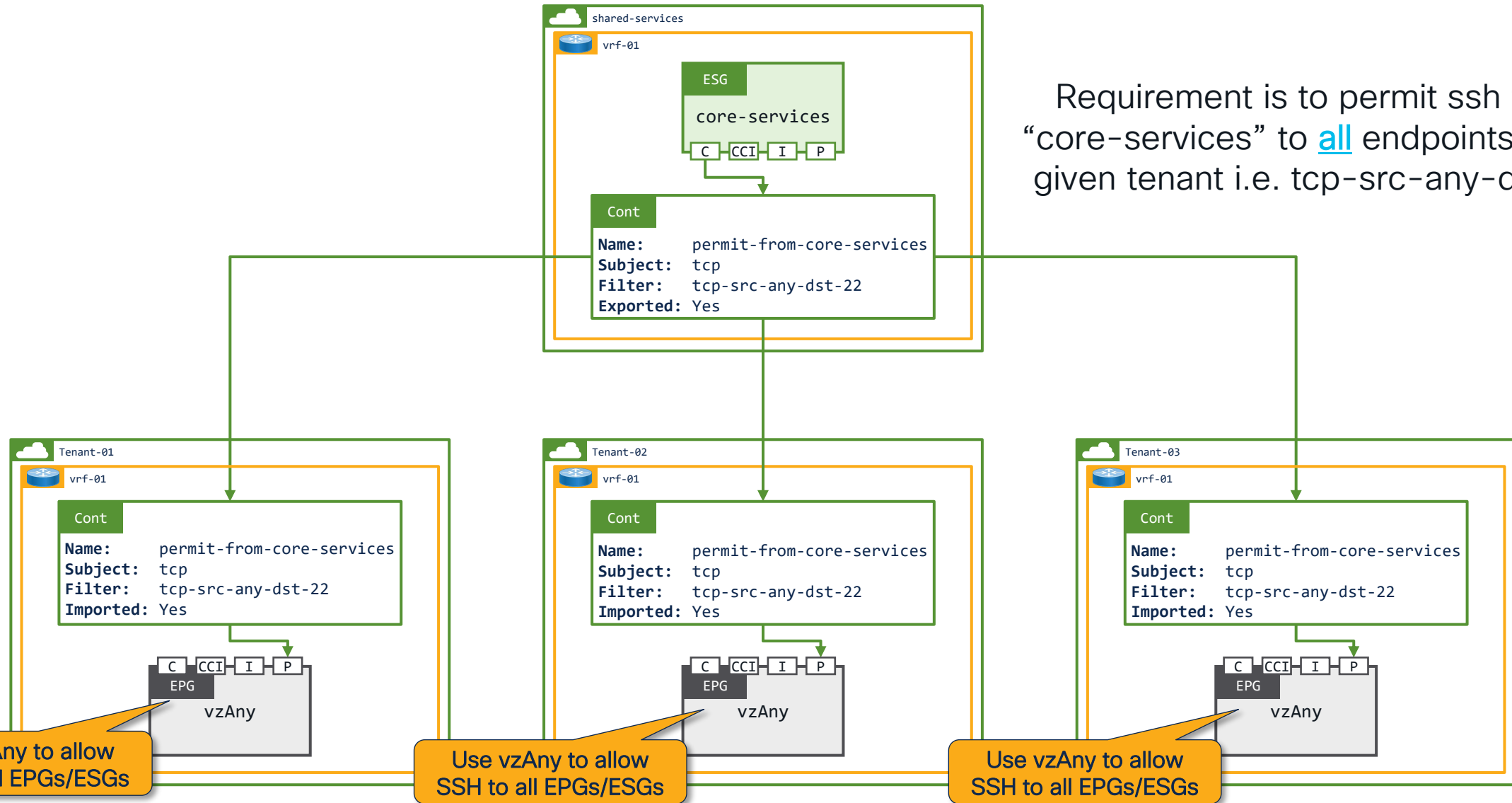
vzAny Operation – Consumer and Provider

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



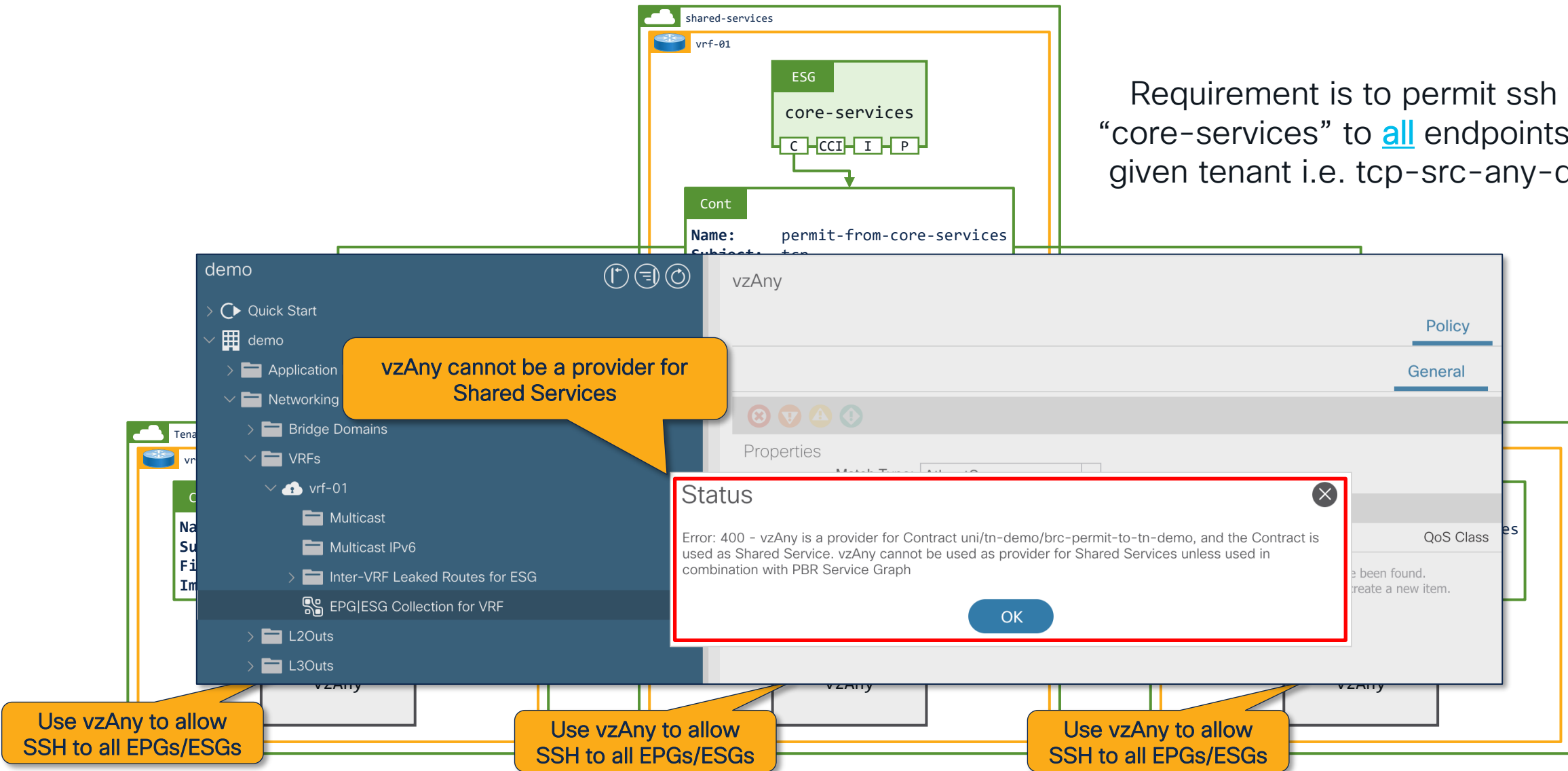
vzAny cannot be a Provider for Shared Services

Requirement is to permit ssh from “core-services” to [all](#) endpoints in any given tenant i.e. tcp-src-any-dst-22



vzAny cannot be a Provider for Shared Services

Requirement is to permit ssh from “core-services” to [all](#) endpoints in any given tenant i.e. tcp-src-any-dst-22



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: select a value



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

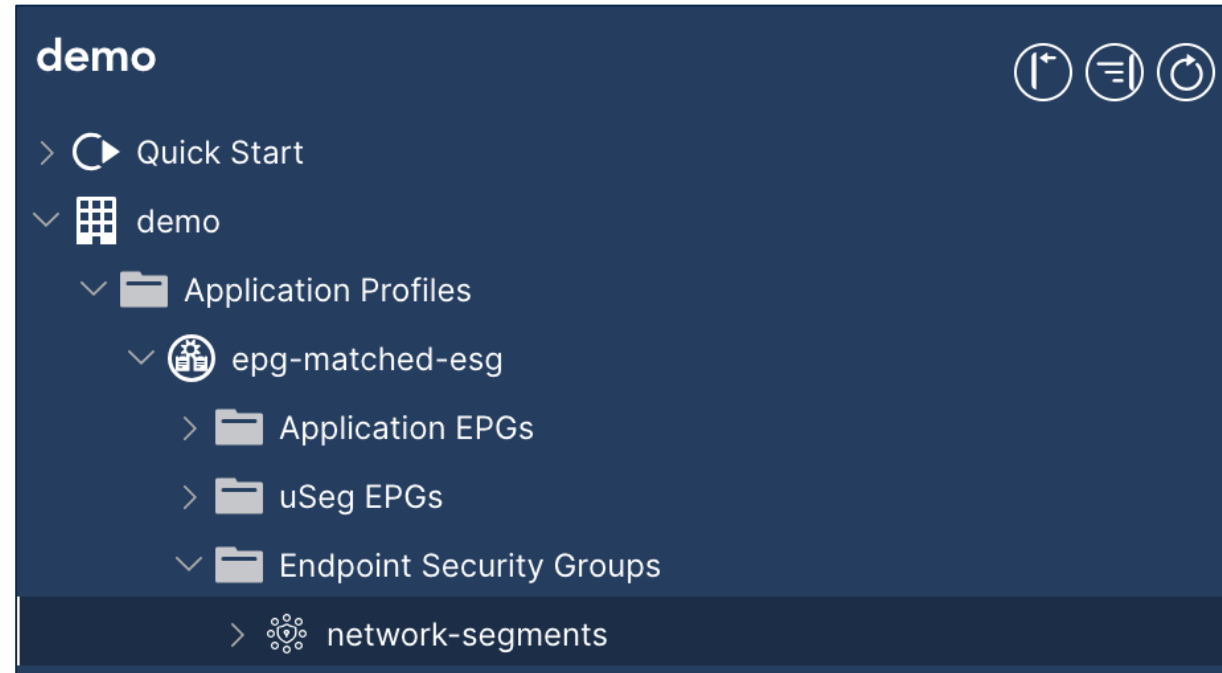
pcTag 16393

Include EPG in Preferred Group

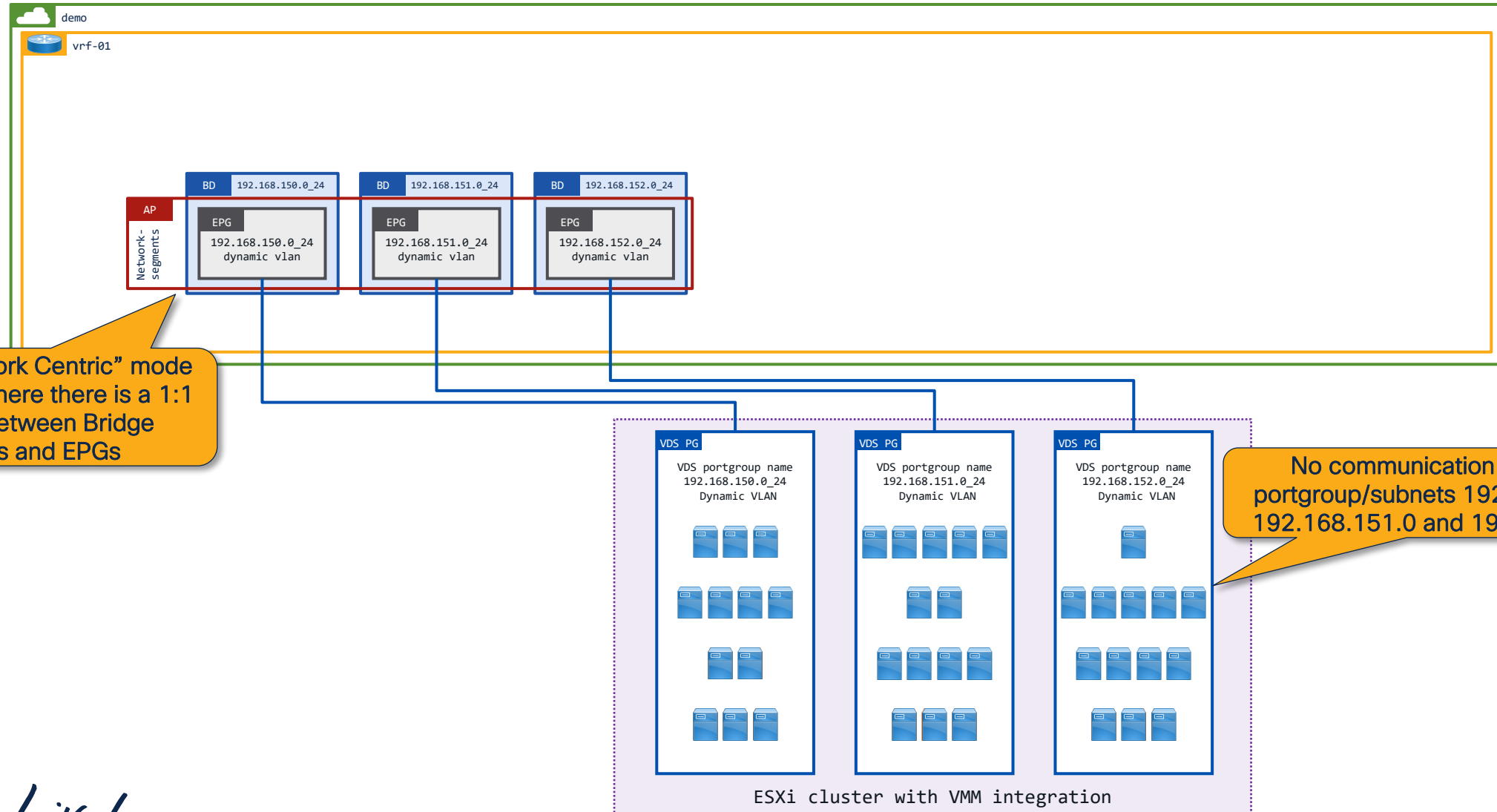
There can only be one “Preferred Group” per VRF...

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

All EPGs mapped to a single ESG



Initial state: Isolated groups of workloads



Enable Endpoint Security Groups

The image displays three screenshots of the Cisco ISE GUI, illustrating the configuration of Endpoint Security Groups (ESGs) for different network topologies. Each screenshot shows the 'Domains (VMs and Bare-Metals)' table, with the 'Allow Micro-Segmentation' checkbox and the 'Primary VLAN' and 'Port Encap' columns highlighted. The callouts provide context for when static VLANs are required.

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

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		

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

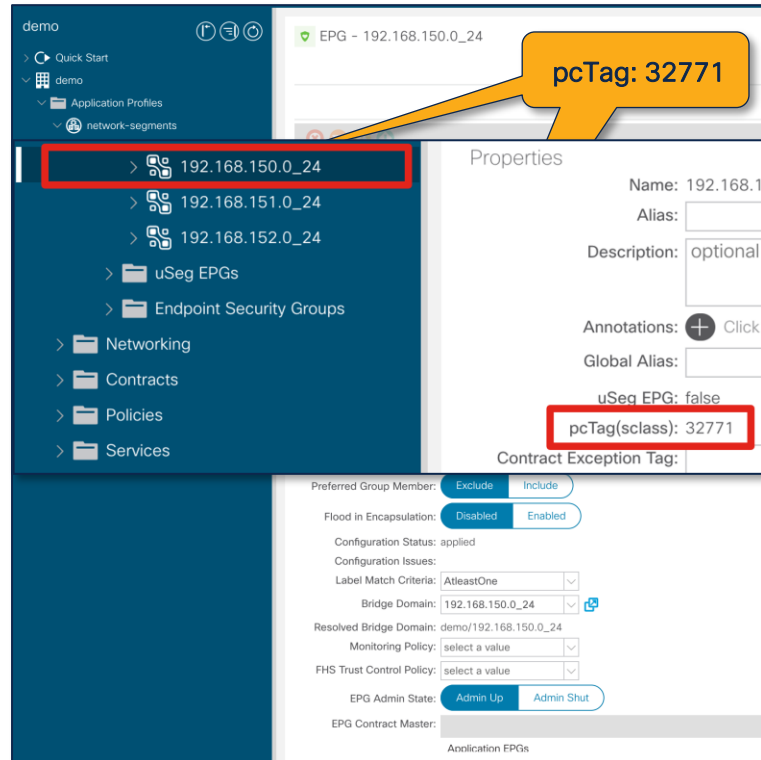
Port binding Static binding
Port allocation Elastic
Private VLAN Isolated (1157, 1158)

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)

Each EPG has a unique security Tag (pcTag)



demo

EPG - 192.168.150.0_24

pcTag: 32771

Properties

Name: 192.168.150.0_24

Alias:

Description: optional

Annotations: + Click

Global Alias:

uSeg EPG: false

pcTag(sclass): 32771

Contract Exception Tag:

Preferred Group Member: Exclude Include

Flood in Encapsulation: Disabled Enabled

Configuration Status: applied

Configuration Issues:

Label Match Criteria: AtleastOne

Bridge Domain: 192.168.150.0_24

Resolved Bridge Domain: demo/192.168.150.0_24

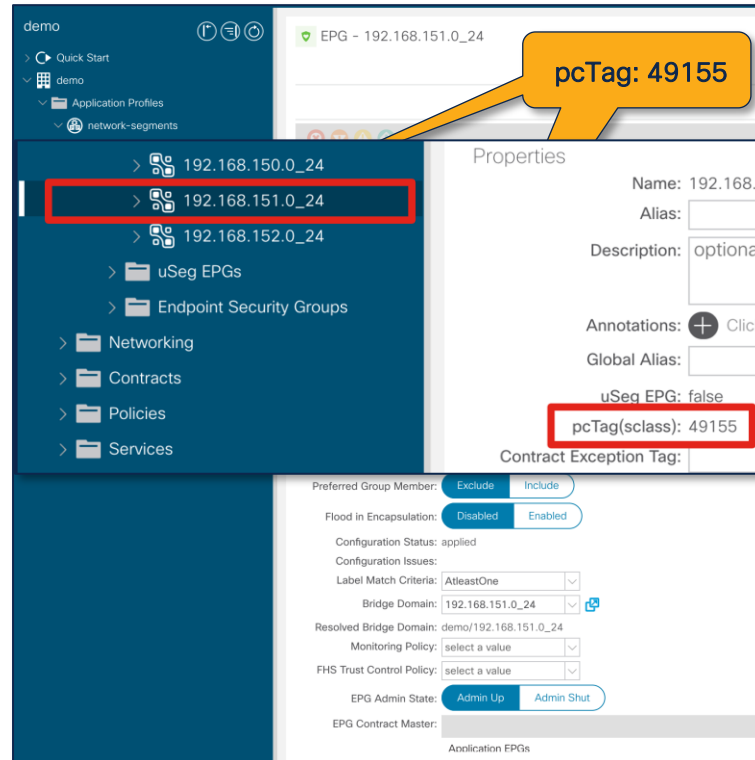
Monitoring Policy: select a value

FHS Trust Control Policy: select a value

EPG Admin State: Admin Up Admin Shut

EPG Contract Master:

Application EPGs



demo

EPG - 192.168.151.0_24

pcTag: 49155

Properties

Name: 192.168.151.0_24

Alias:

Description: optional

Annotations: + Click

Global Alias:

uSeg EPG: false

pcTag(sclass): 49155

Contract Exception Tag:

Preferred Group Member: Exclude Include

Flood in Encapsulation: Disabled Enabled

Configuration Status: applied

Configuration Issues:

Label Match Criteria: AtleastOne

Bridge Domain: 192.168.151.0_24

Resolved Bridge Domain: demo/192.168.151.0_24

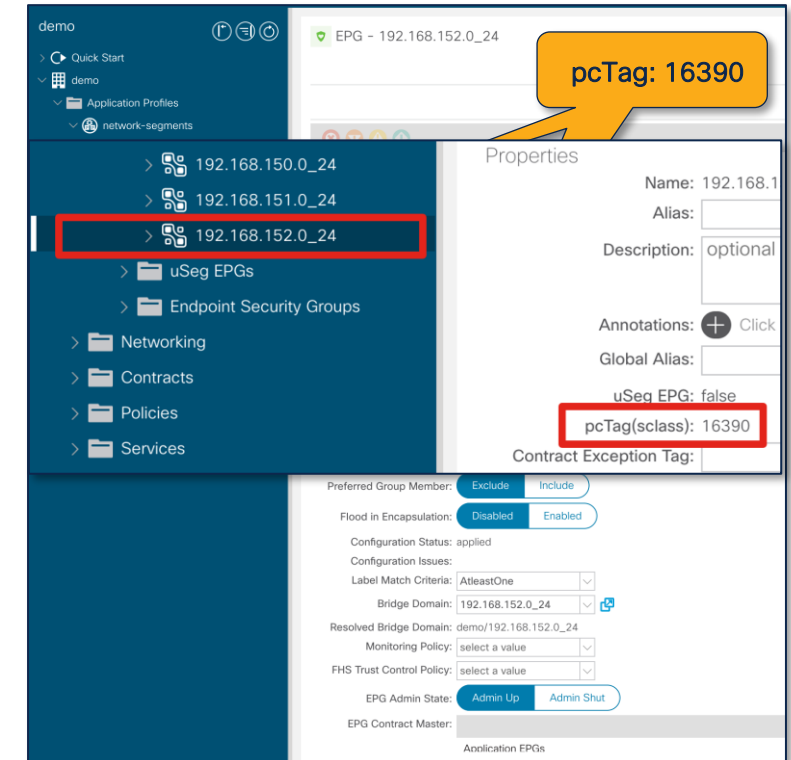
Monitoring Policy: select a value

FHS Trust Control Policy: select a value

EPG Admin State: Admin Up Admin Shut

EPG Contract Master:

Application EPGs



demo

EPG - 192.168.152.0_24

pcTag: 16390

Properties

Name: 192.168.152.0_24

Alias:

Description: optional

Annotations: + Click

Global Alias:

uSeg EPG: false

pcTag(sclass): 16390

Contract Exception Tag:

Preferred Group Member: Exclude Include

Flood in Encapsulation: Disabled Enabled

Configuration Status: applied

Configuration Issues:

Label Match Criteria: AtleastOne

Bridge Domain: 192.168.152.0_24

Resolved Bridge Domain: demo/192.168.152.0_24

Monitoring Policy: select a value

FHS Trust Control Policy: select a value

EPG Admin State: Admin Up Admin Shut

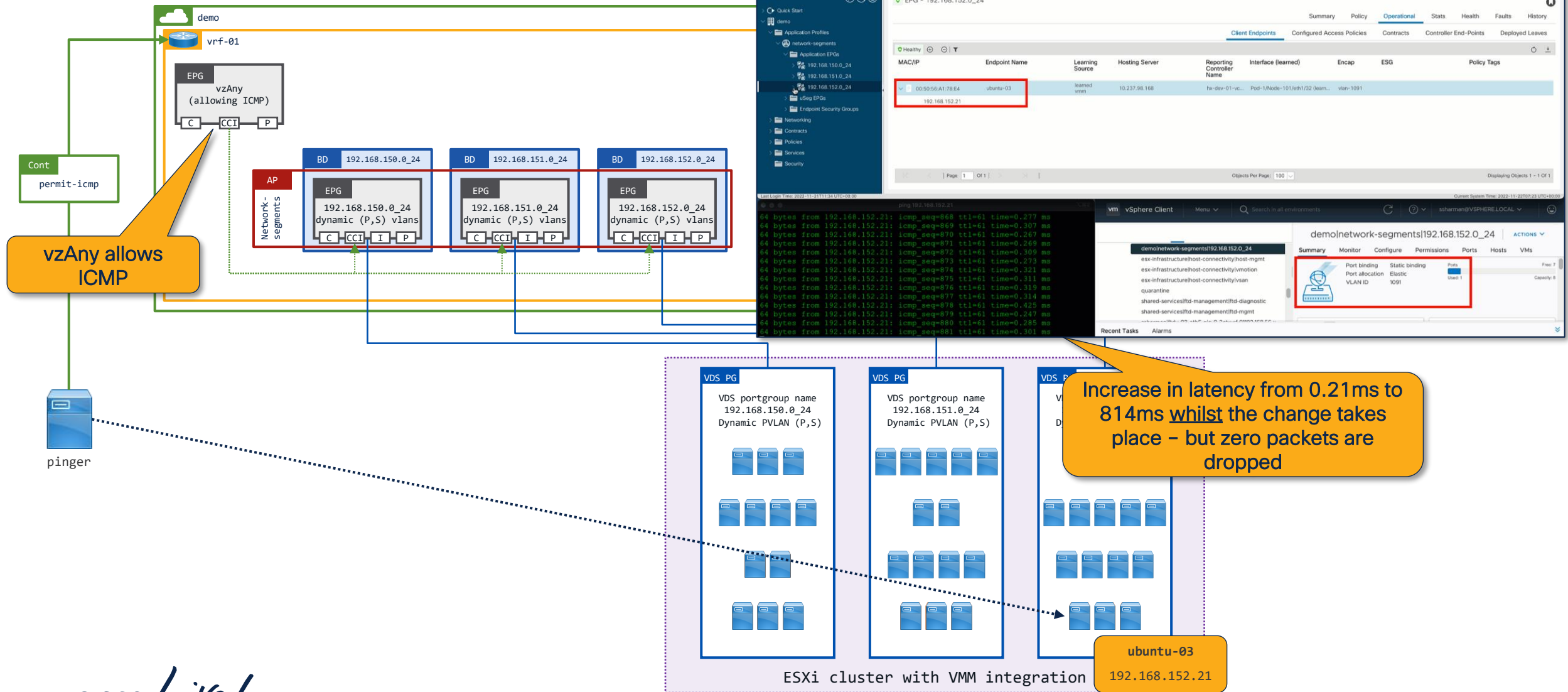
EPG Contract Master:

Application EPGs

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

plus, micro segmentation also enables Proxy ARP and dynamic endpoint MAC Tagging...

What's the impact to traffic when we enable uSegmentation...



Let's map our EPGs to an ESG...

Create an 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** | ciscolive-07 | ciscolive-08

demo

Application Profiles

Create Application Profile

epg-matched-security-groups

Do not create EPGs

Create Application Profile

Name: epg-matched-security-group

Alias:

Description: optional

Annotations: Click to add a new annotation

Monitoring Policy: select a value

EPGs

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

Cancel Submit

Create a new ESG for Network Segments (EPGs)

Create new ESG

Enter ESG name "group-01"

Select the VRF for the ESG to be applied against

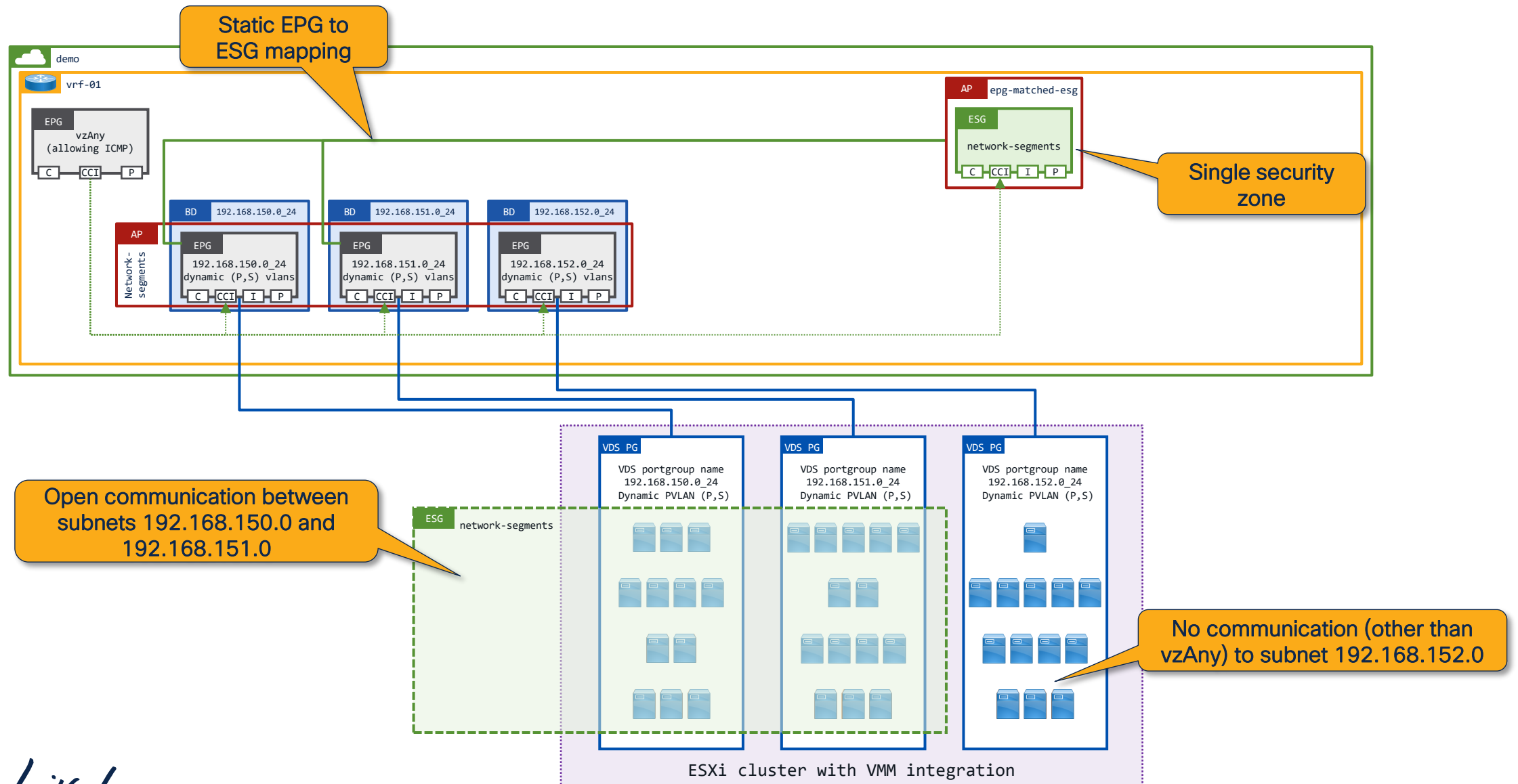
Add EPGs

Select one or more EPGs

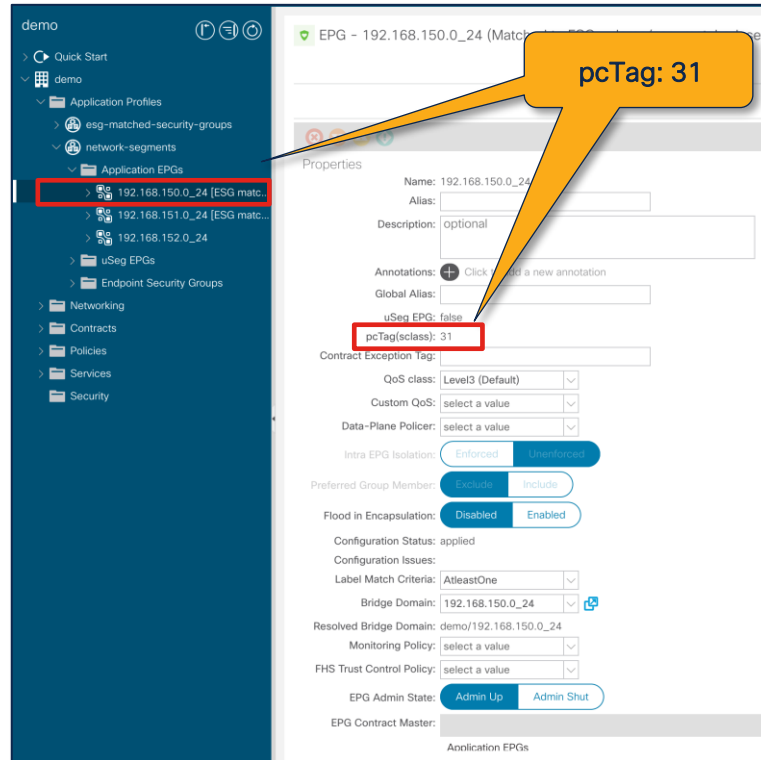
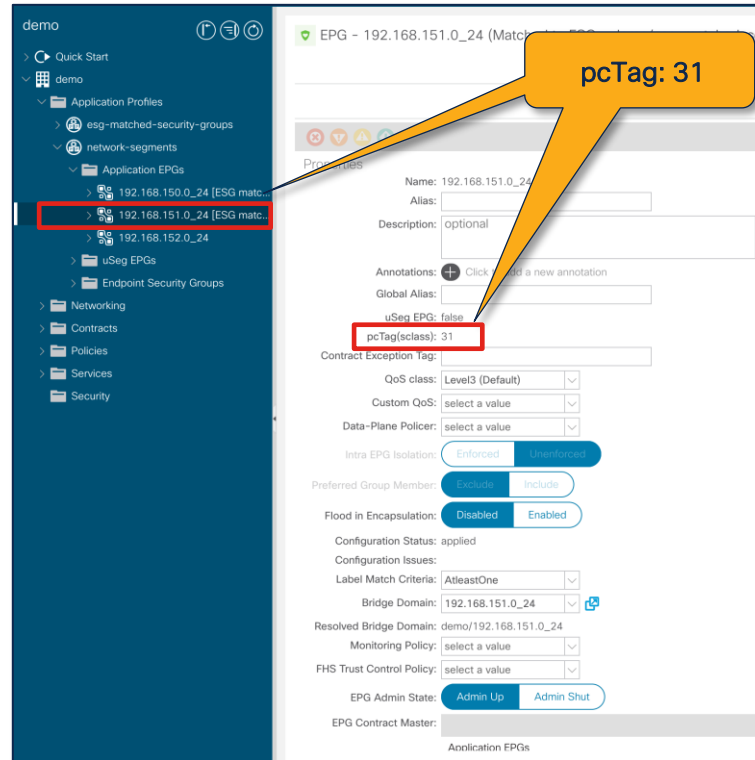
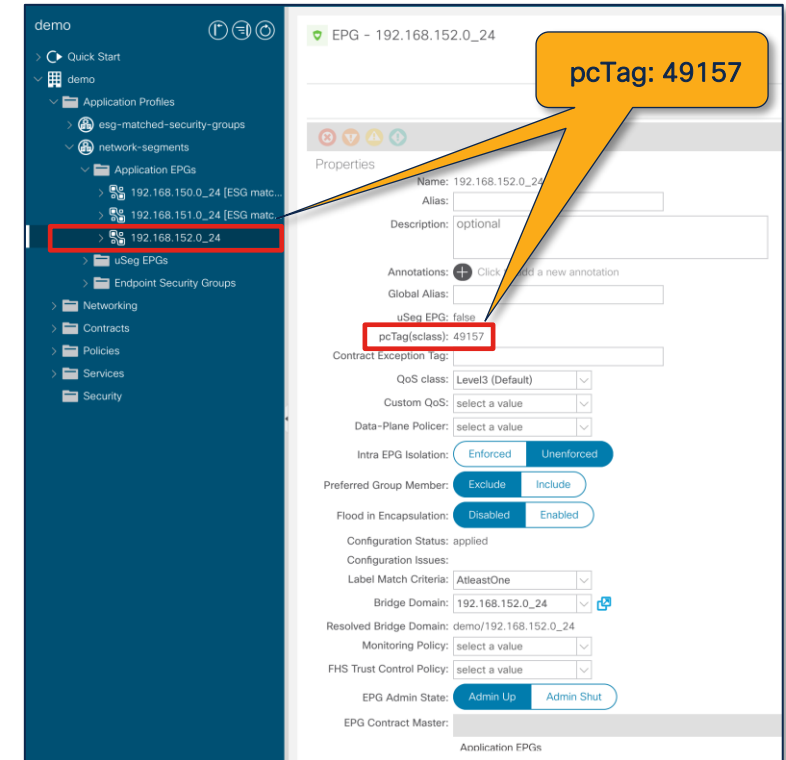
Allow Intra ESG traffic i.e. permit traffic between EPGs

Finish

Open communication within the ESG...

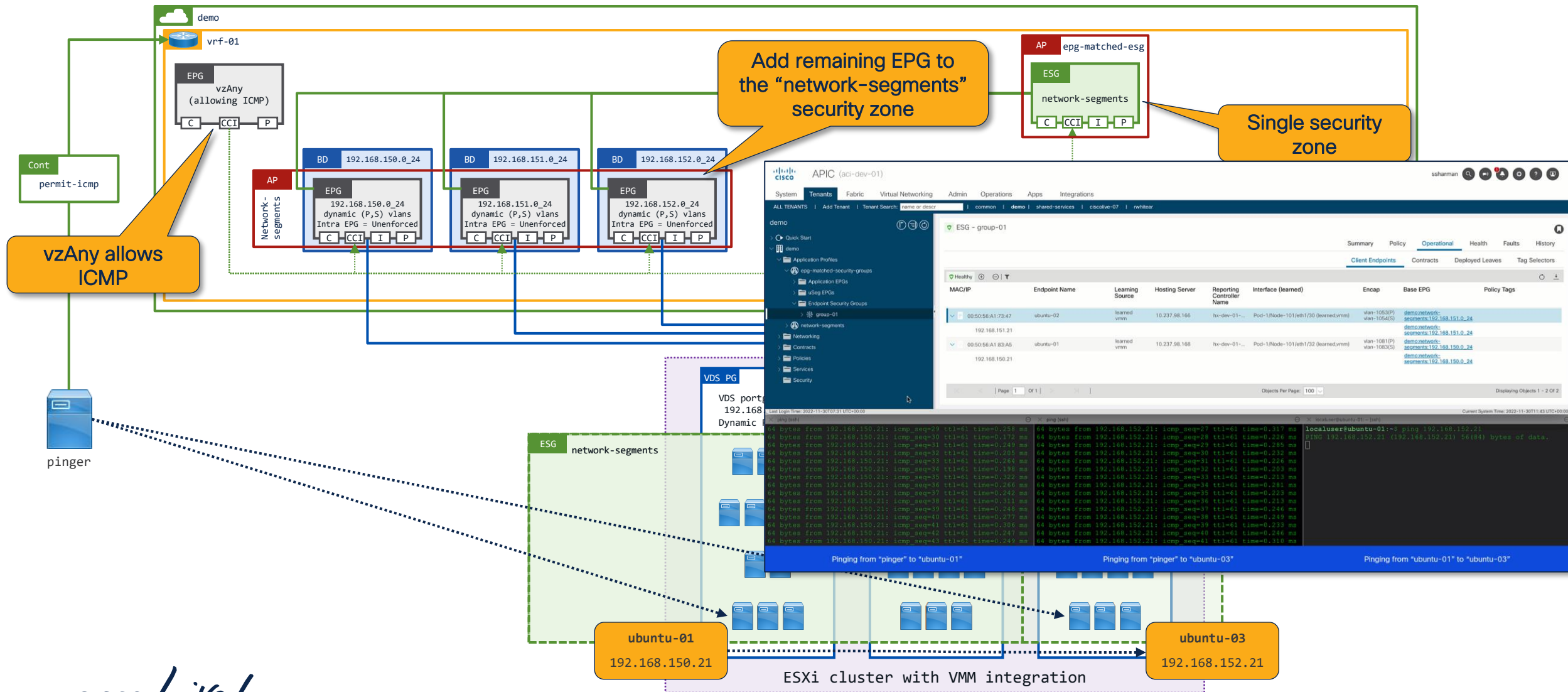


Matched EPGs now classified with a common pcTag

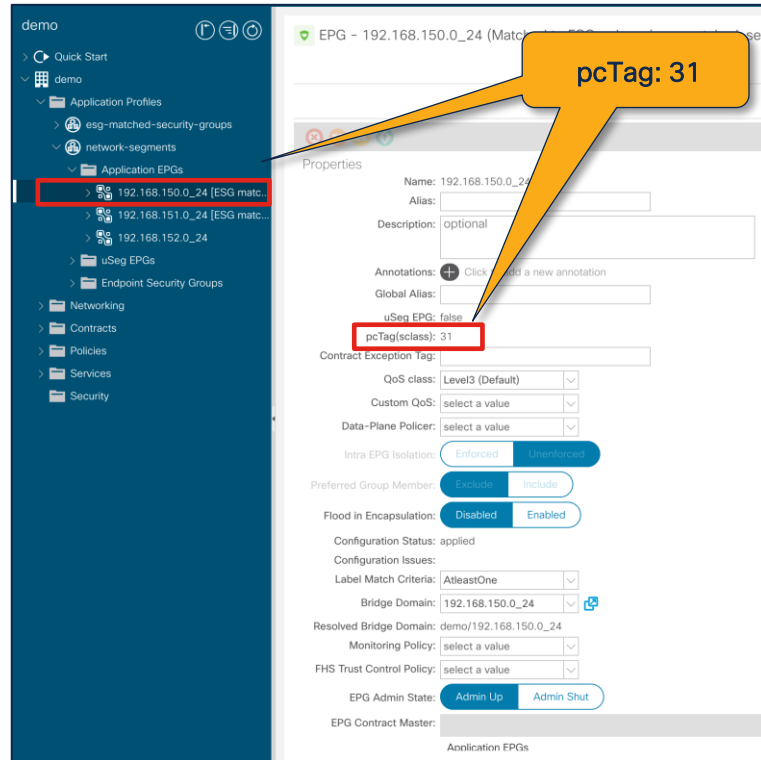
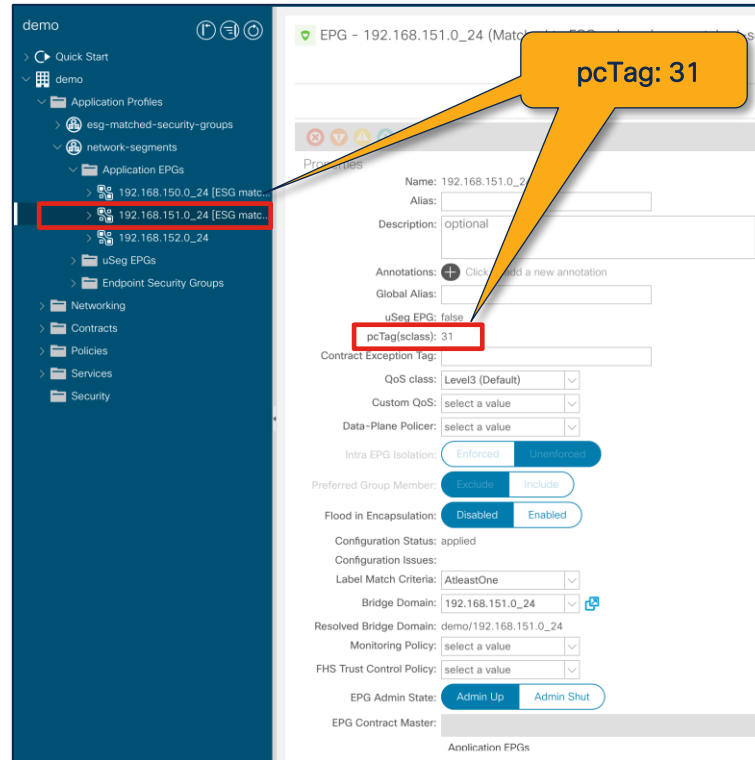
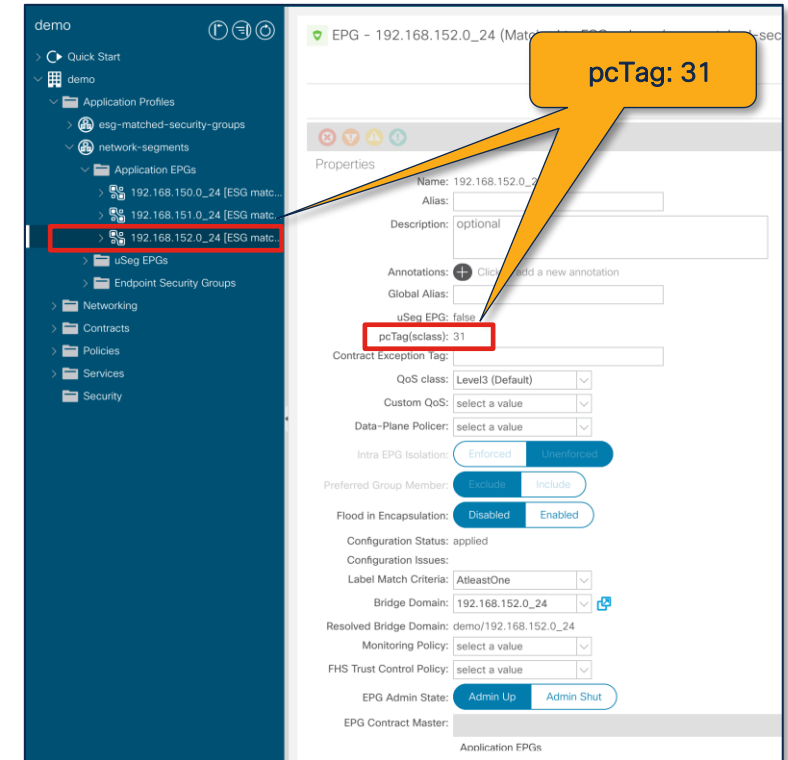


Let's consider any impact to traffic when adding the remaining EPG to the Security Group...

Add remaining EPG to Single Security Zone



All EPGs now classified with a common pcTag

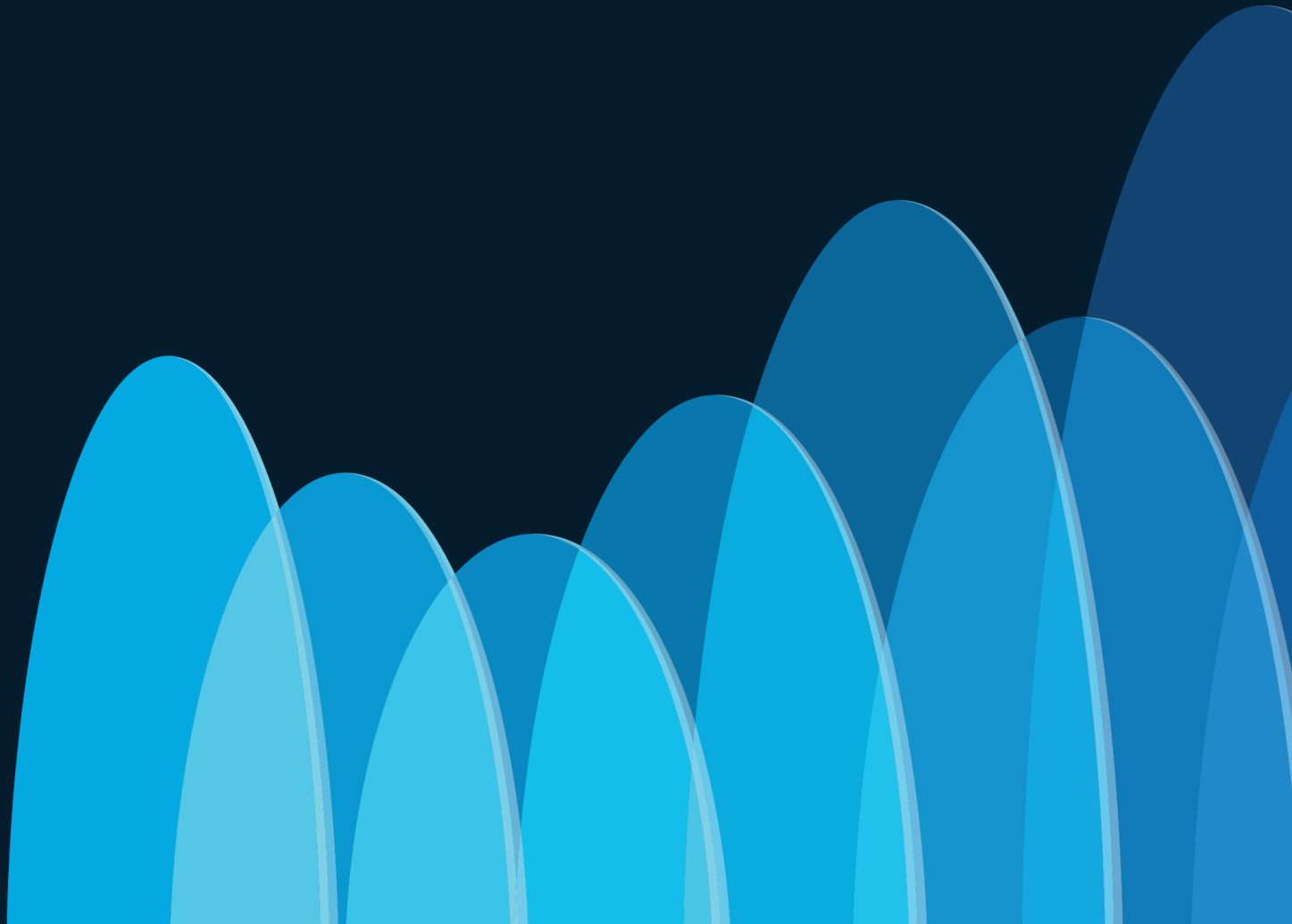


Benefits of EPG to ESG Mapping

- 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

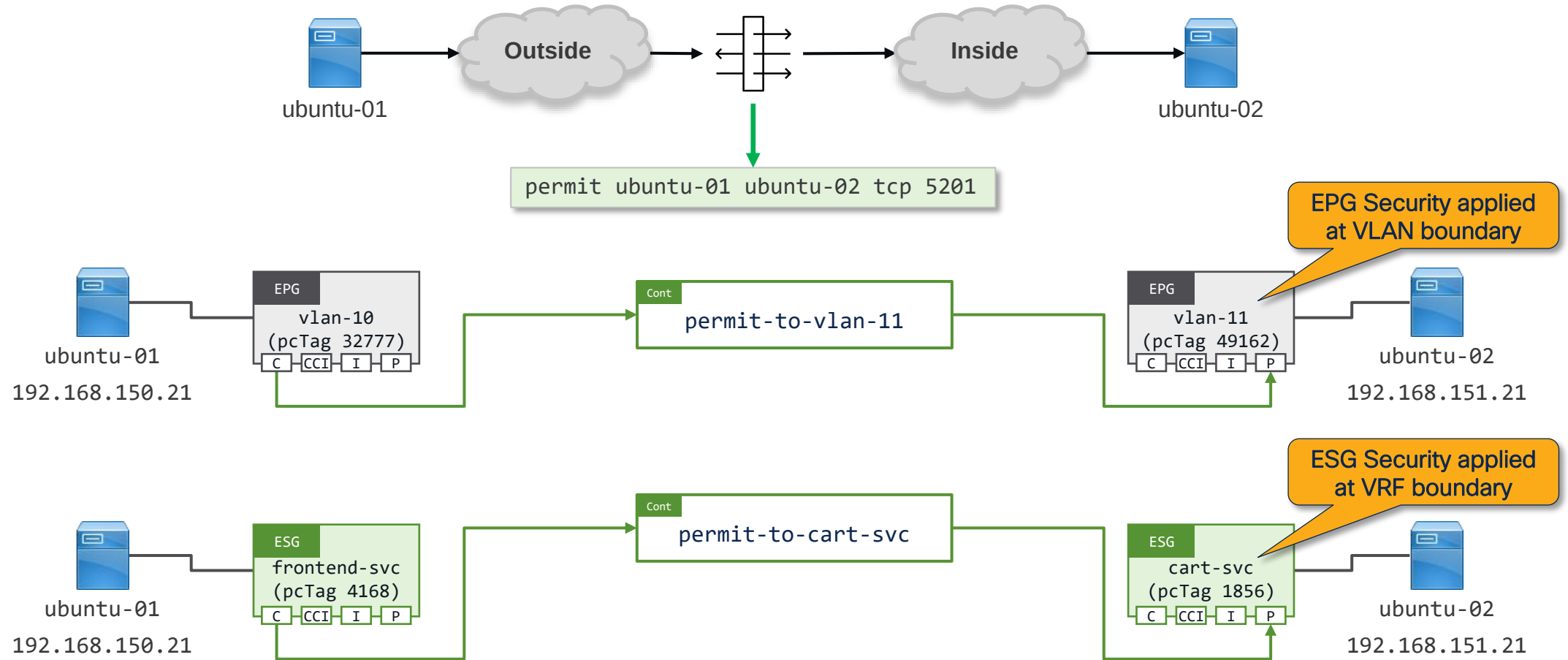
* Assumes 1:1 mapping between Bridge Domain and EPG. ESGs can mapping can also be performed on IP subnets

Allowing restricted
communication...



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

How do contracts work...?



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

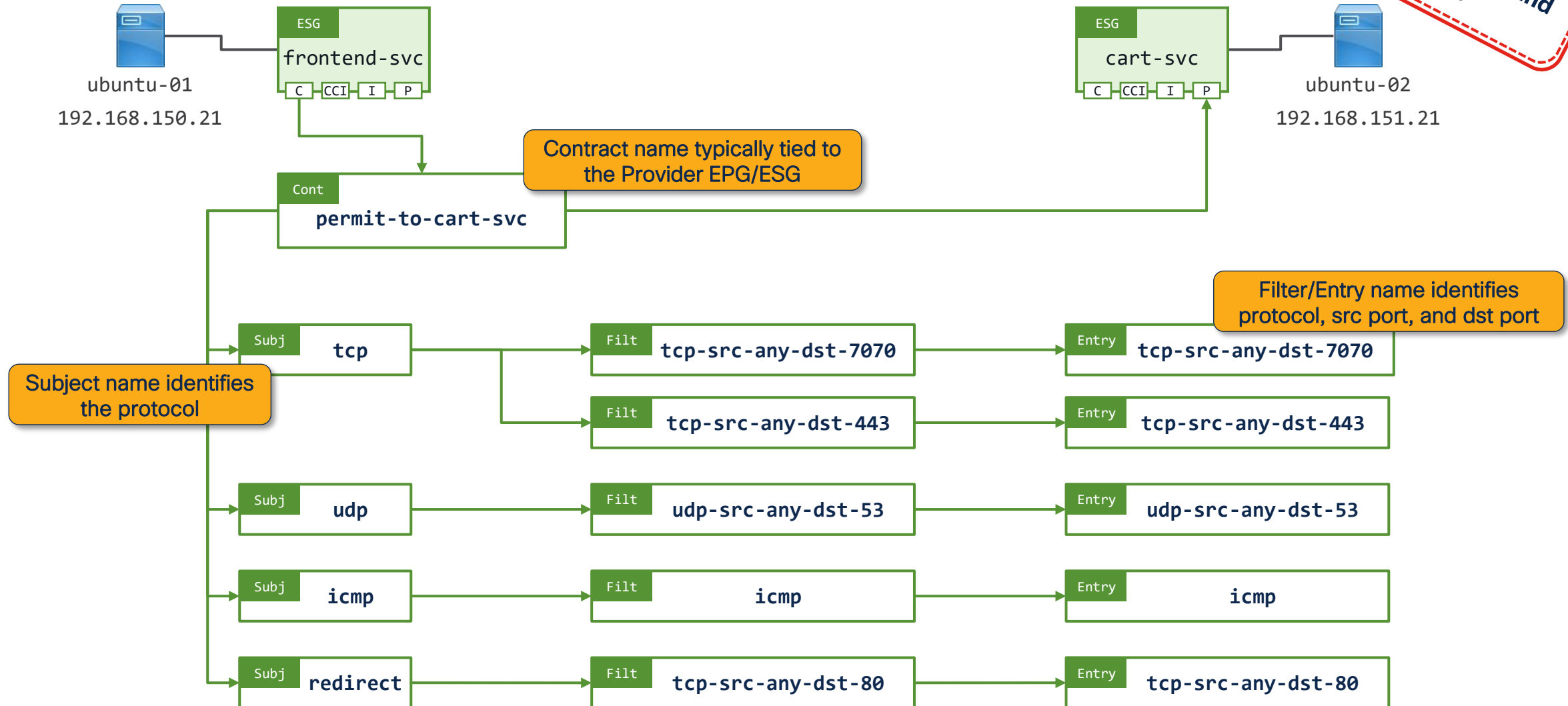
Consumer and Provider relationships are there to help you visualize the traffic flow direction

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

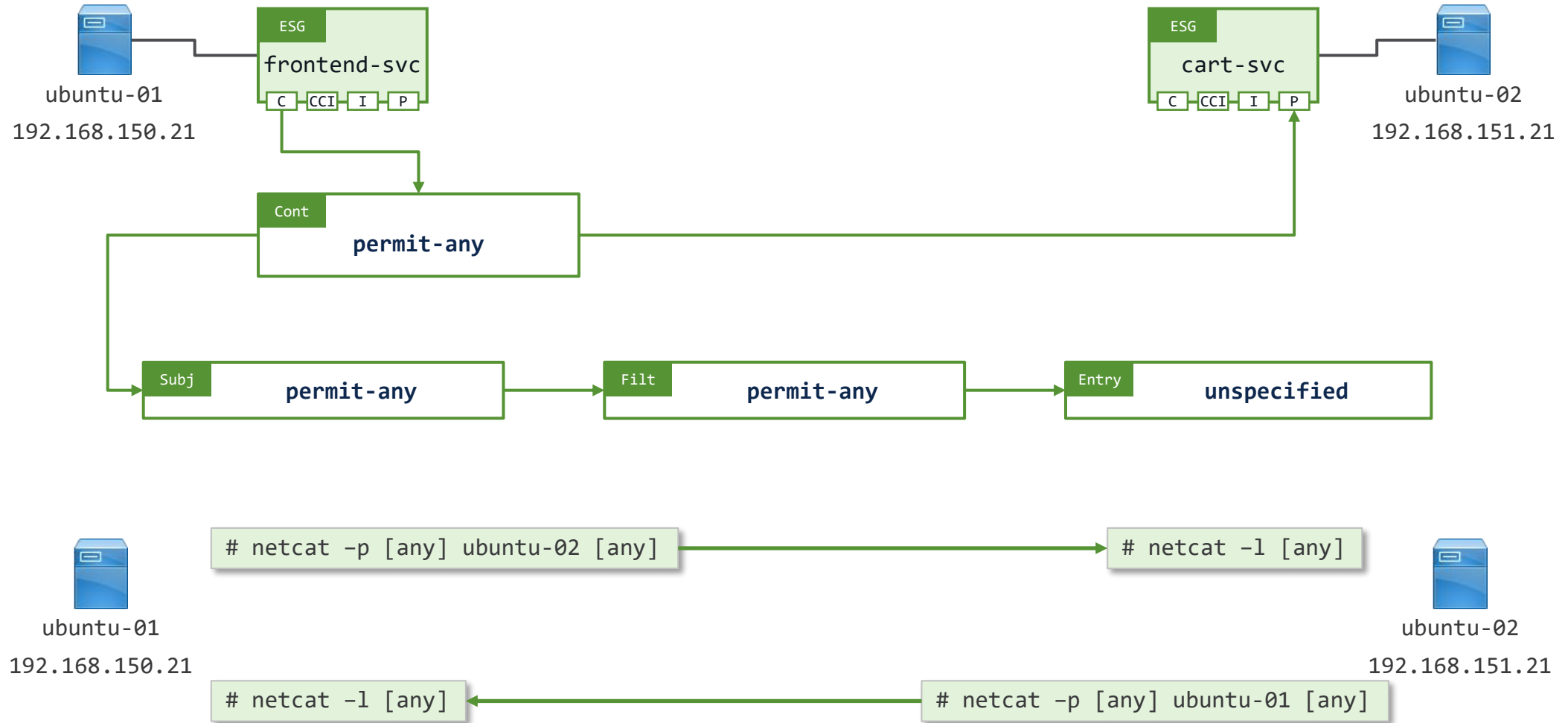
Contract Structure...

Use clear and explicit naming for filters and entries



Who hasn't simply done this...

permit any/any

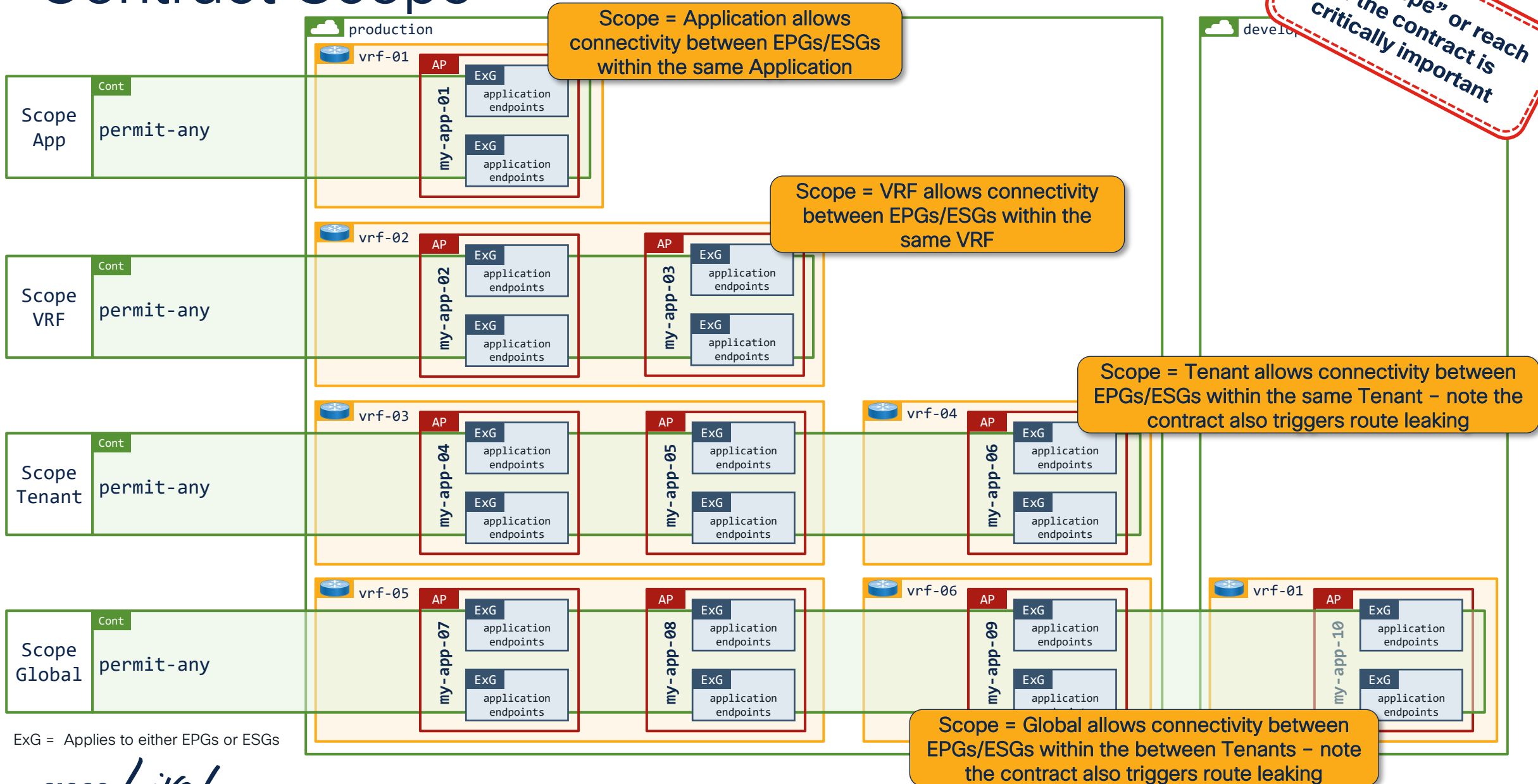


Important...

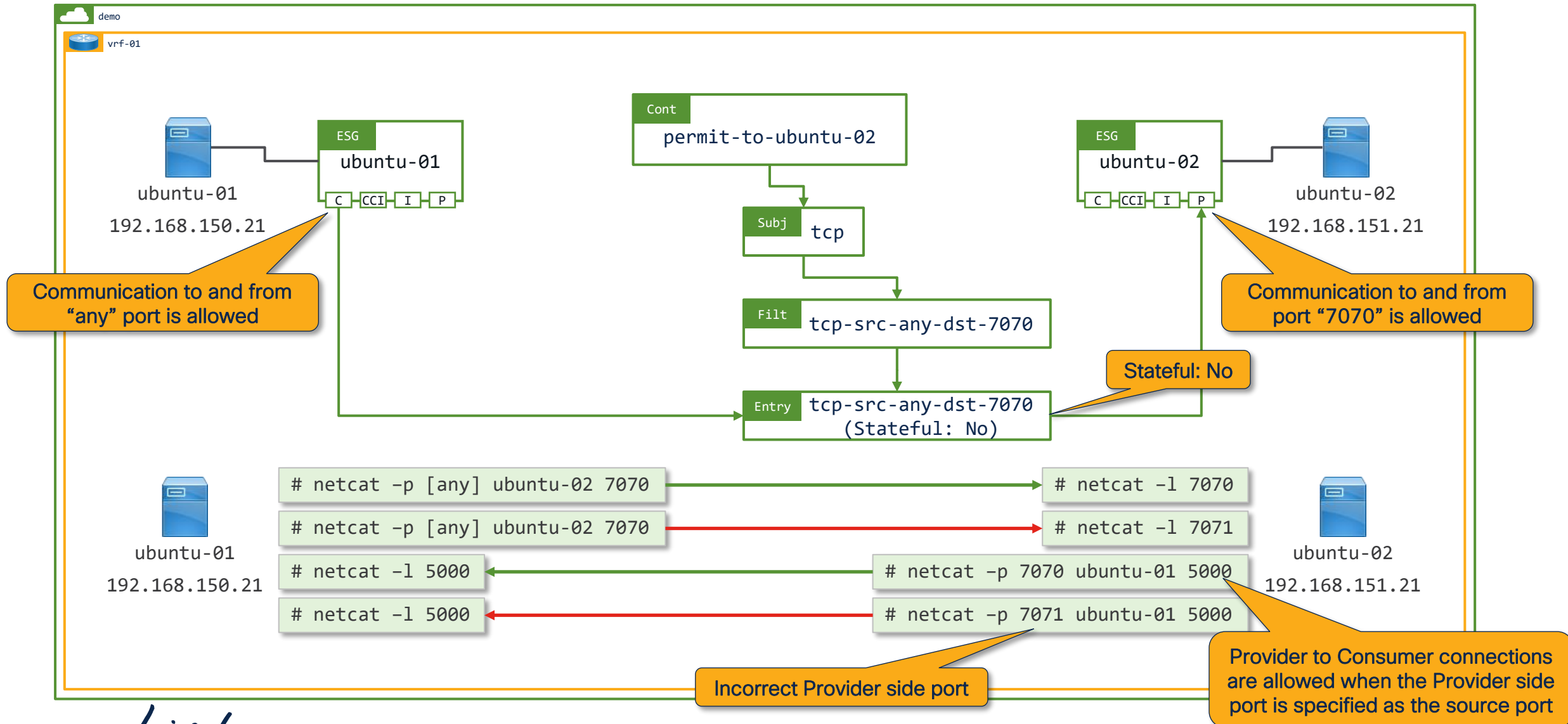
Contracts also trigger route leaking for EPGs...

Contract Scope

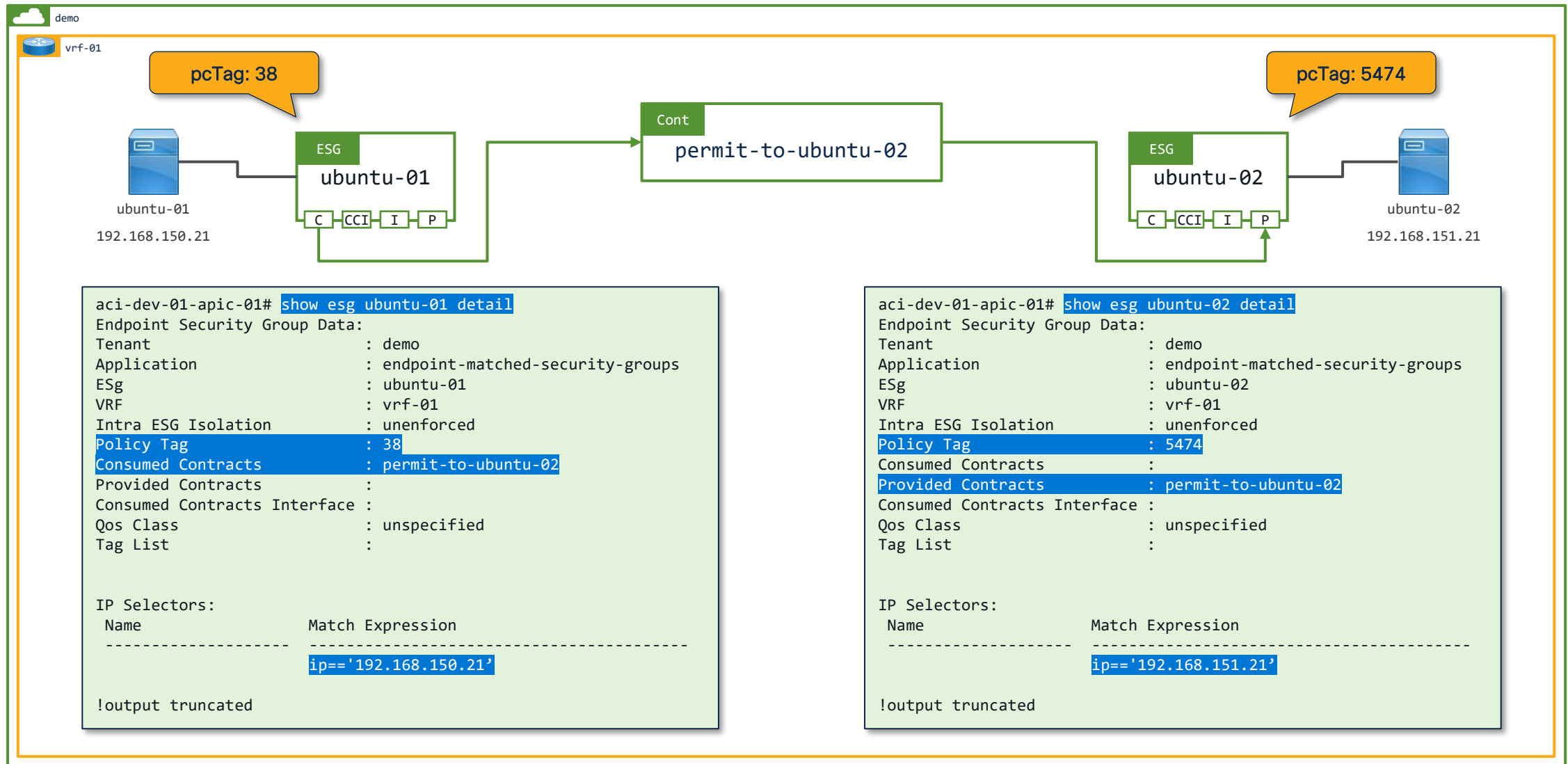
The "Scope" or reach of the contract is critically important



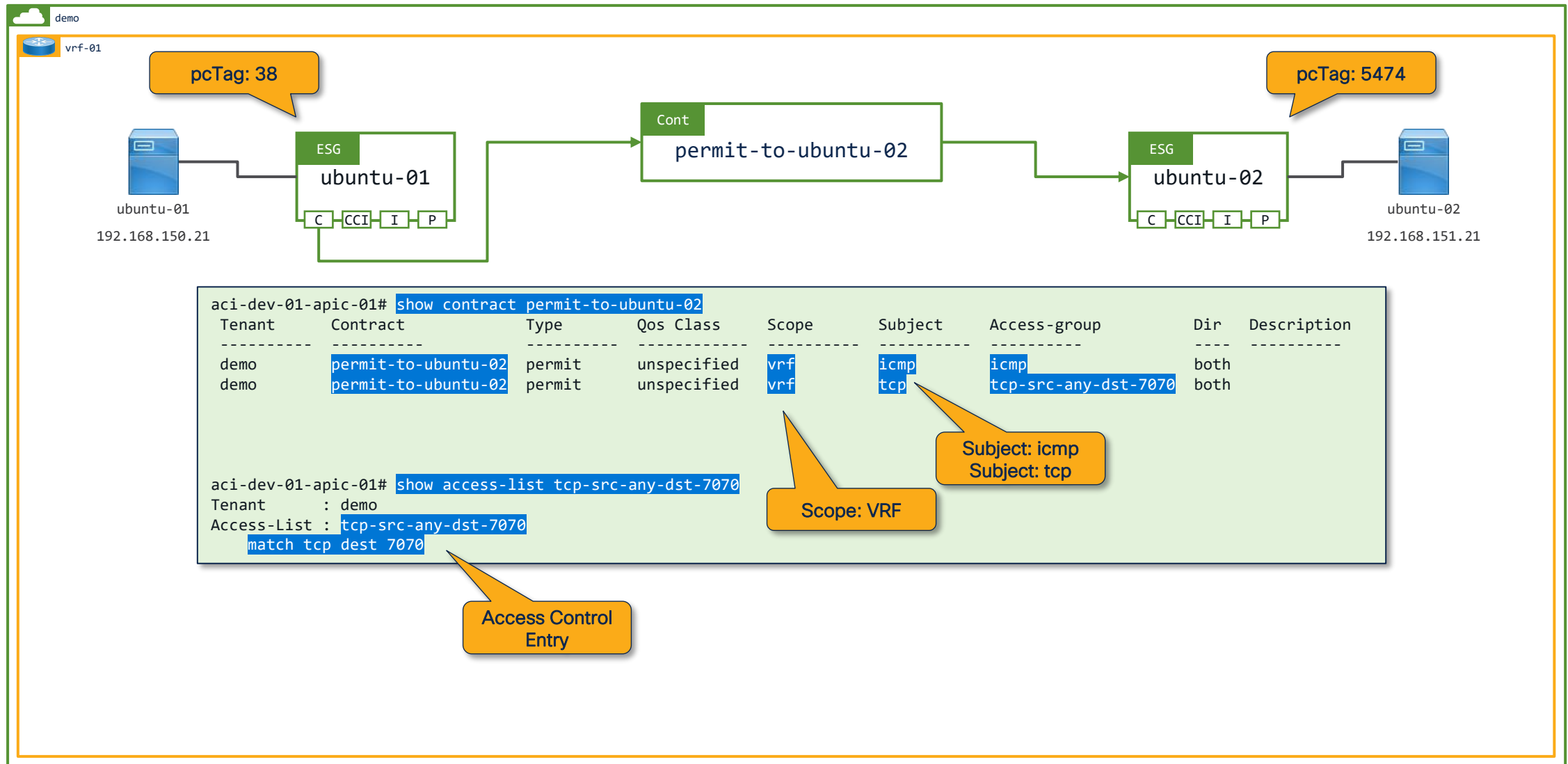
Verifying Contract operation with netcat – Stateful = No



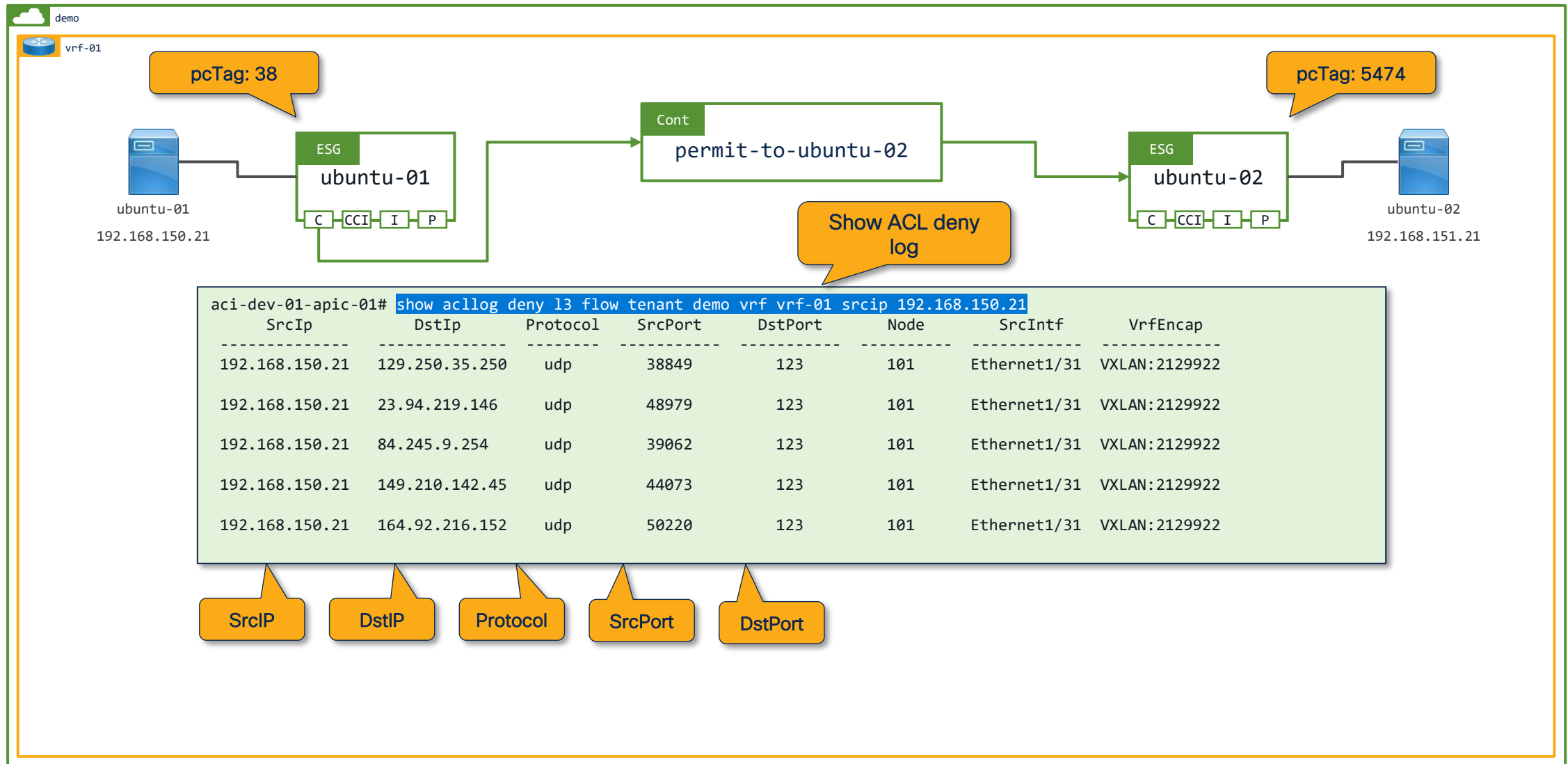
Verifying Contract Operation: EPG/ESG details



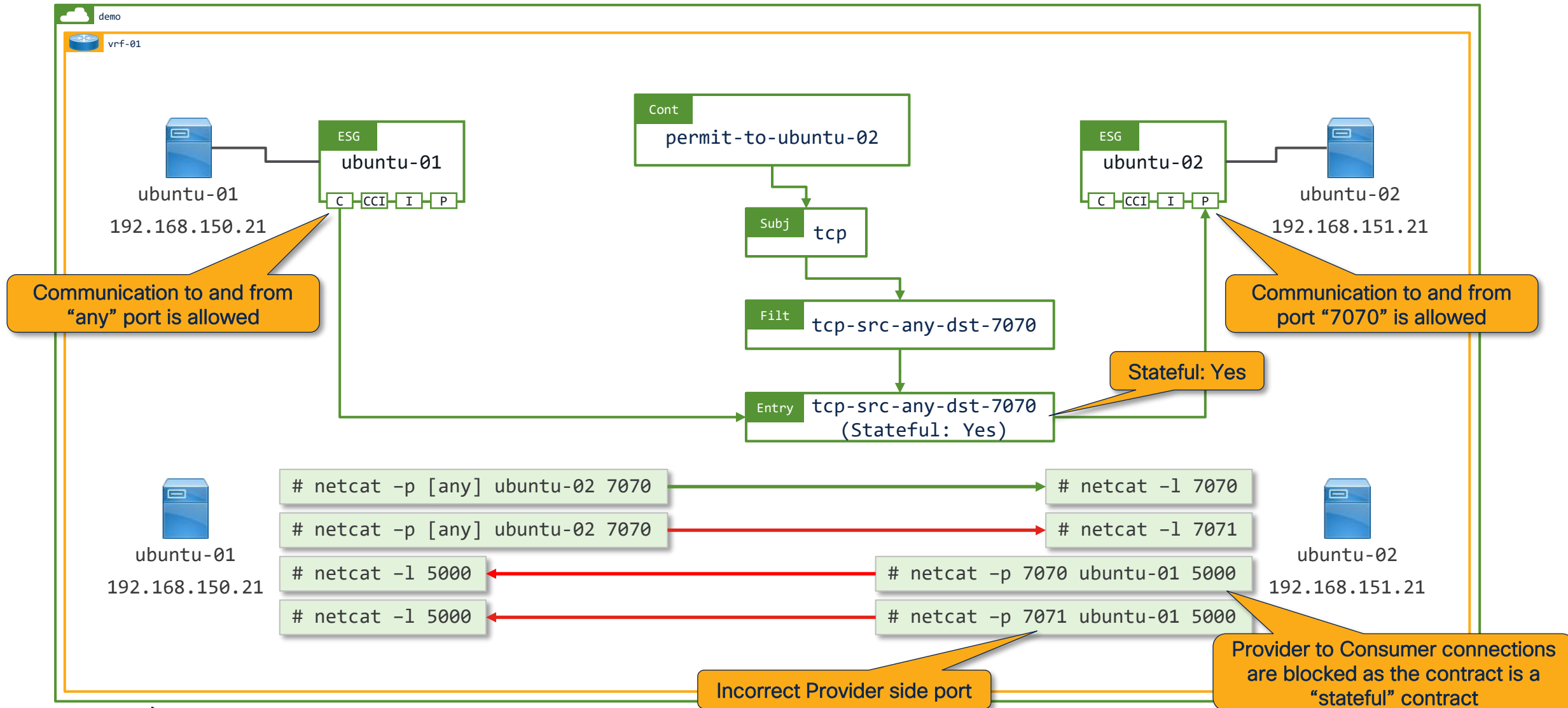
Verifying Contract Operation: Contract details



Verifying Contract Operation: Drop details



Verifying Contract operation with netcat – Stateful = Yes



Verifying Contracts with Syslog and ELAM

The image displays two overlapping screenshots from a network management environment. The background screenshot is the Graylog web interface, showing a search for the message "demo:vrf-01". The search results show a message count graph and a list of messages. The foreground screenshot is the Cisco APIC (aci-dev-605) interface, specifically the ELAM Assistant page. It shows the configuration for capturing a packet with ELAM (Embedded Logic Analyzer Module) on node-101 and node-102. The ELAM Parameters section shows the configuration for capturing traffic from the tn-demo-online-boutique. The Packet Forwarding Information section shows the Forward Result, Contract, and Drop information for the captured packet.

Graylog Search Results:

Search: message: "demo:vrf-01"

Message Count:

3,000,000
2,000,000
1,000,000
0

Oct 2021 Jan 2022 Apr 2022 Jul 2022

All Messages

timestamp 1f

2023-06-03 00:25:32.930 +00:00

Jun 03 01:25:32 BST aci-dev-01-leaf-102 : %LOG_LOCAL7-6-SYSTEM_MSG: [E4204936][transition][D_VLAN, Vlan-Id: 83, SMac: 0x005056a122de, DMac: 0x0022bdf819ff, SIP: 192.168.152.100, DIP: 10.0.73.67, SPort: 38232, DPort: 6379, Seq: 2823] it cnt: 1

26ec0e20-01a5-11ee-ba3b-00505686785c

Timestamp: 2023-06-03 00:25:32.930

Received by: Syslog UDP port 5140 on 0ceff33a / syslog

Stored in index: graylog_3

Routed into streams: All messages

Facility: local7

Facility_num: 23

Level: 6

Message: Jun 03 01:25:32 BST aci-dev-01-leaf-102 : %LOG_LOCAL7-6-SYSTEM_MSG: [E4204936][transition][D_VLAN, Vlan-Id: 83, SMac: 0x005056a122de, DMac: 0x0022bdf819ff, SIP: 192.168.152.100, DIP: 10.0.73.67, SPort: 38232, DPort: 6379, Seq: 2823] it cnt: 1

Sequence_number: 0

Source: 2823

Cisco APIC ELAM Assistant:

APIC (aci-dev-605)

System Tenants Fabric Virtual Networking Admin Operations Apps Integrations

Installed Apps Faults Downloads

Apps ELAM Assistant

Capture a packet with ELAM (Embedded Logic Analyzer Module)

ELAM Parameters

tn-demo-online-boutique

Quick Add Add Node

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	

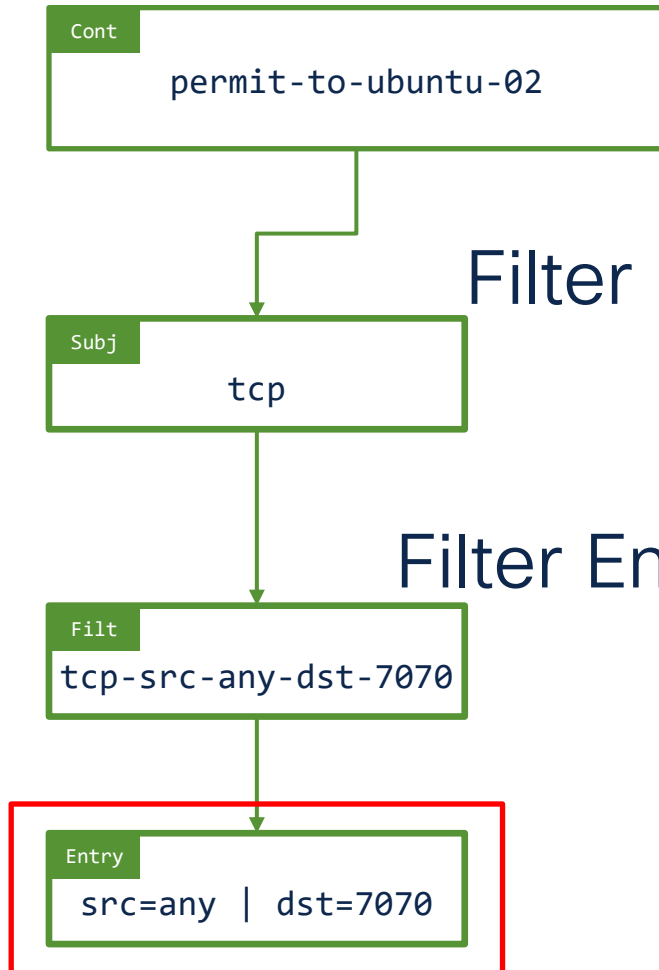
Packet Forwarding Information

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)

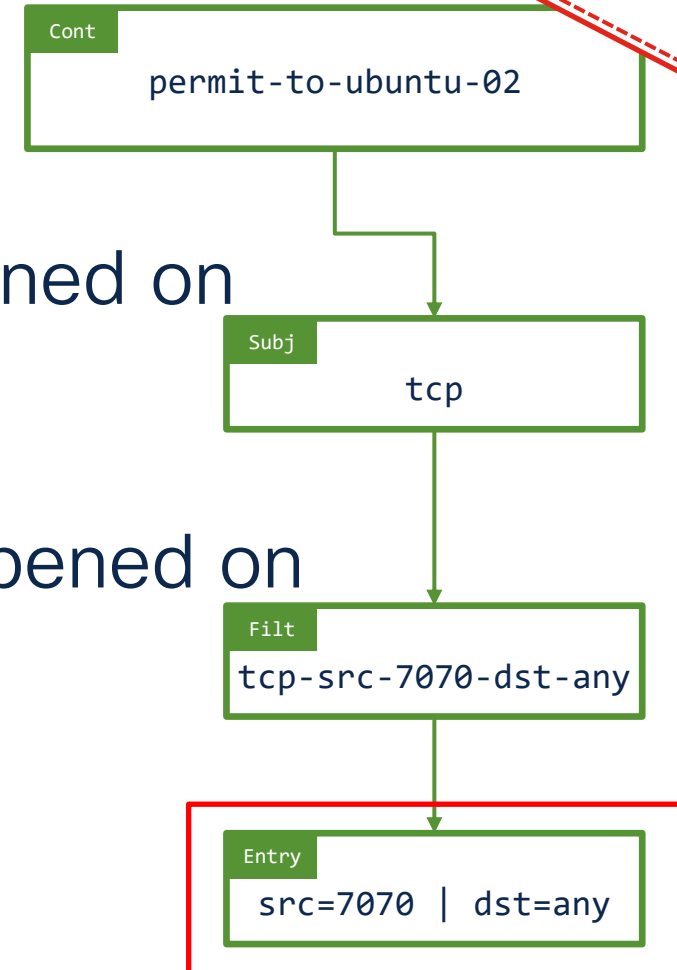
Drop	
Drop Code	no drop

Remember...!



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

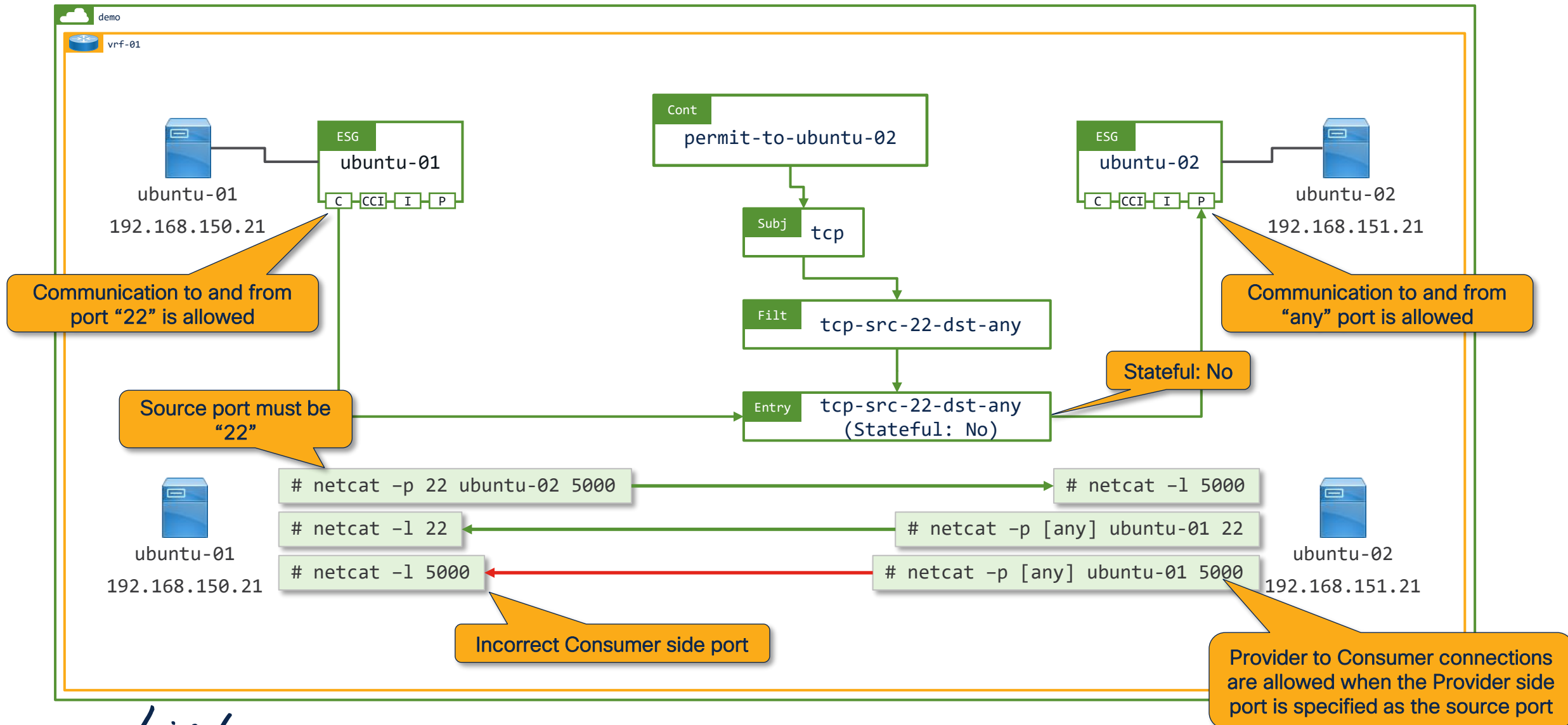
Filter Entry destination port = port opened on the provider EPG/ESG





Getting into the weeds...!

Reversing the Filter ports – Stateful = No

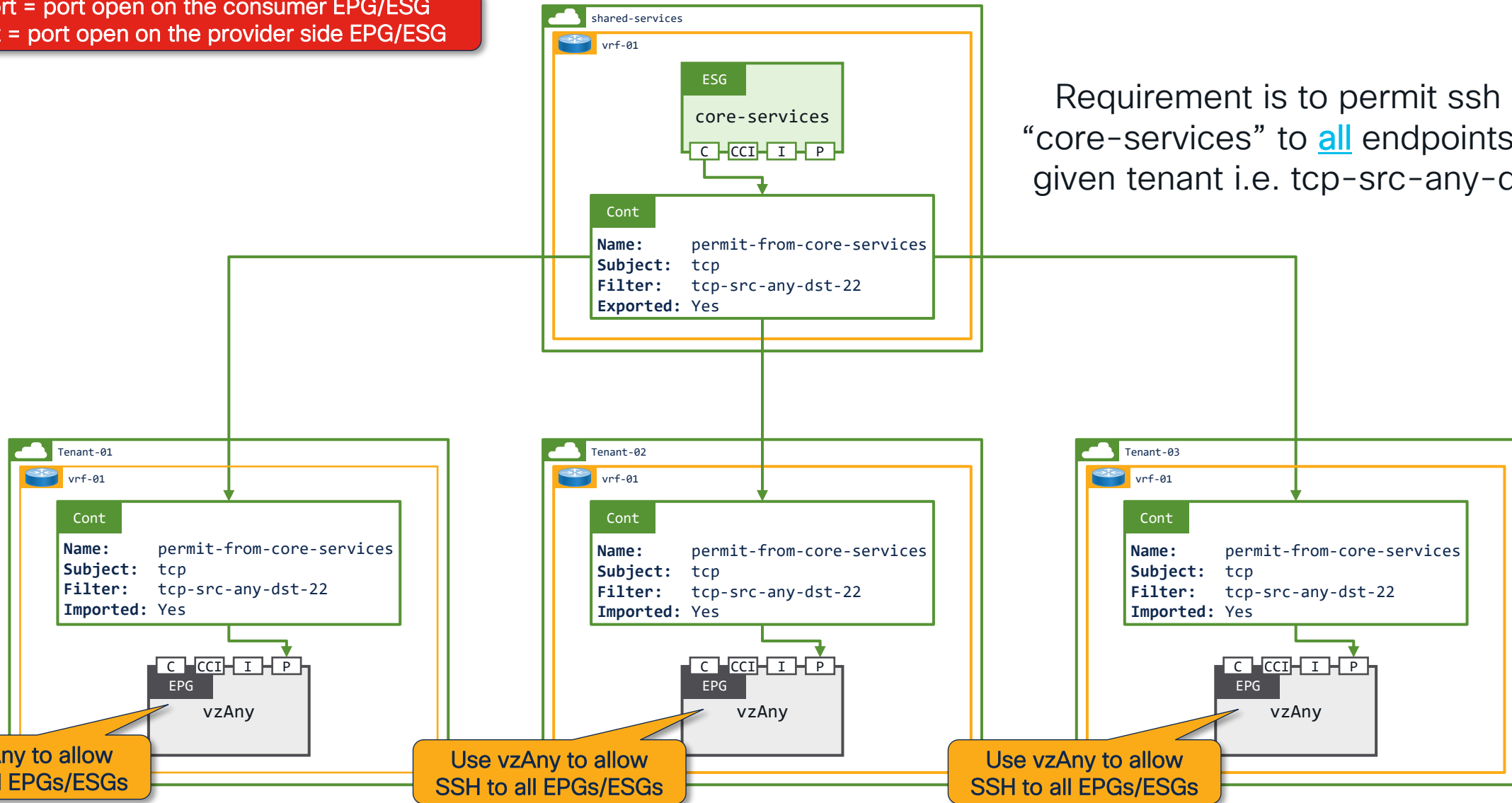


Why would you want to reverse the Consumer and Provider Filters...?

vzAny as a contract Provider

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

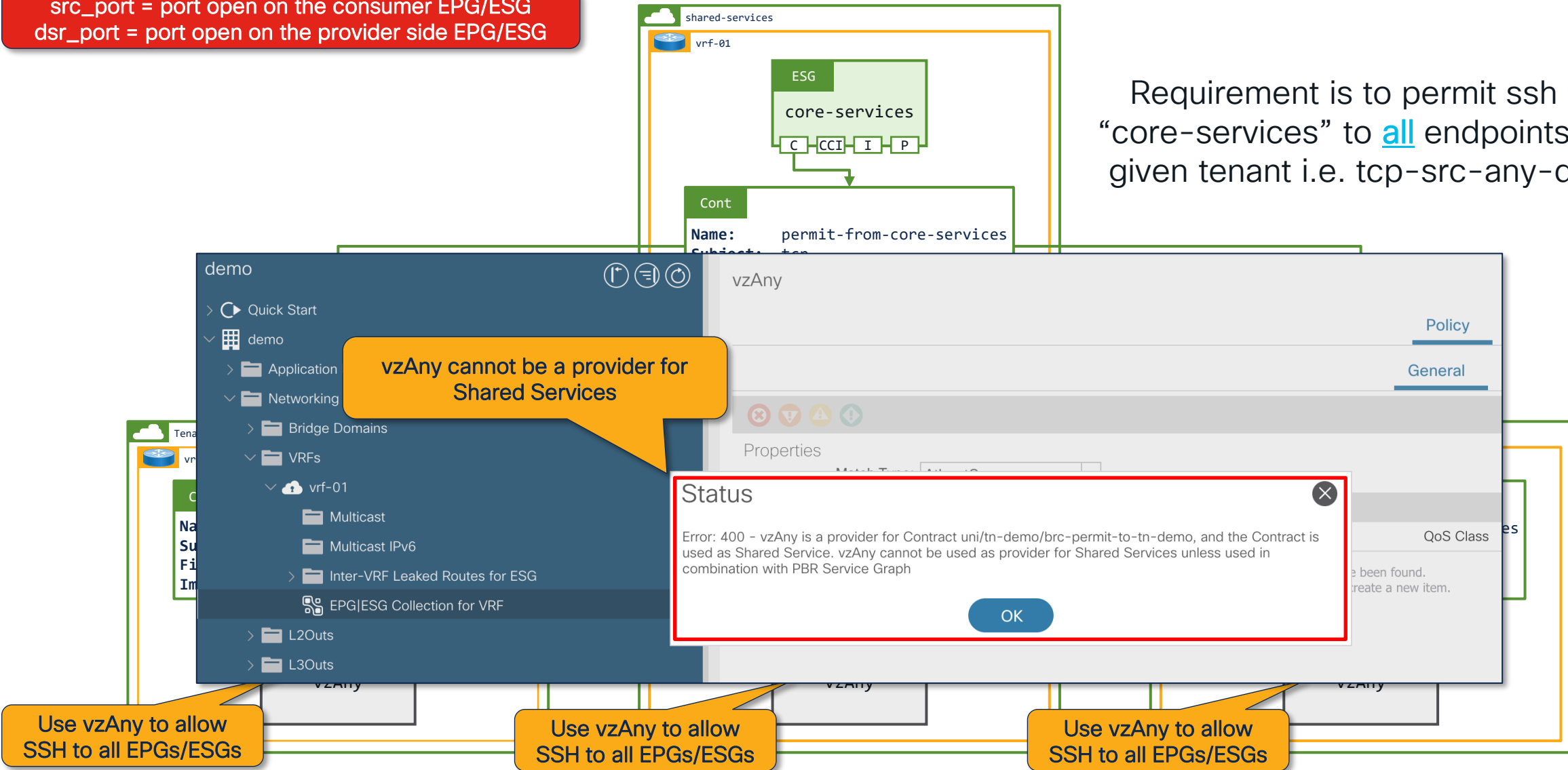
Requirement is to permit ssh from
“core-services” to [all](#) endpoints in any
given tenant i.e. tcp-src-any-dst-22



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 any
given tenant i.e. tcp-src-any-dst-22



vzAny as a contract Consumer – Filters Reversed

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

Reverse the Filter ports in

Requirement is to permit ssh from
s in any
dst-22

demo

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

vzAny

Policy Operational

General Subject Labels

Properties

Match Type: AtleastOne

Provided Contracts:

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

Consumed Contracts:

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

Contract Interfaces:

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

Consume the exported contract(s)

Use vzAny to allow SSH to all EPGs/ESGs

Use vzAny to allow SSH to all EPGs/ESGs

Use vzAny to allow SSH to all EPGs/ESGs

Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

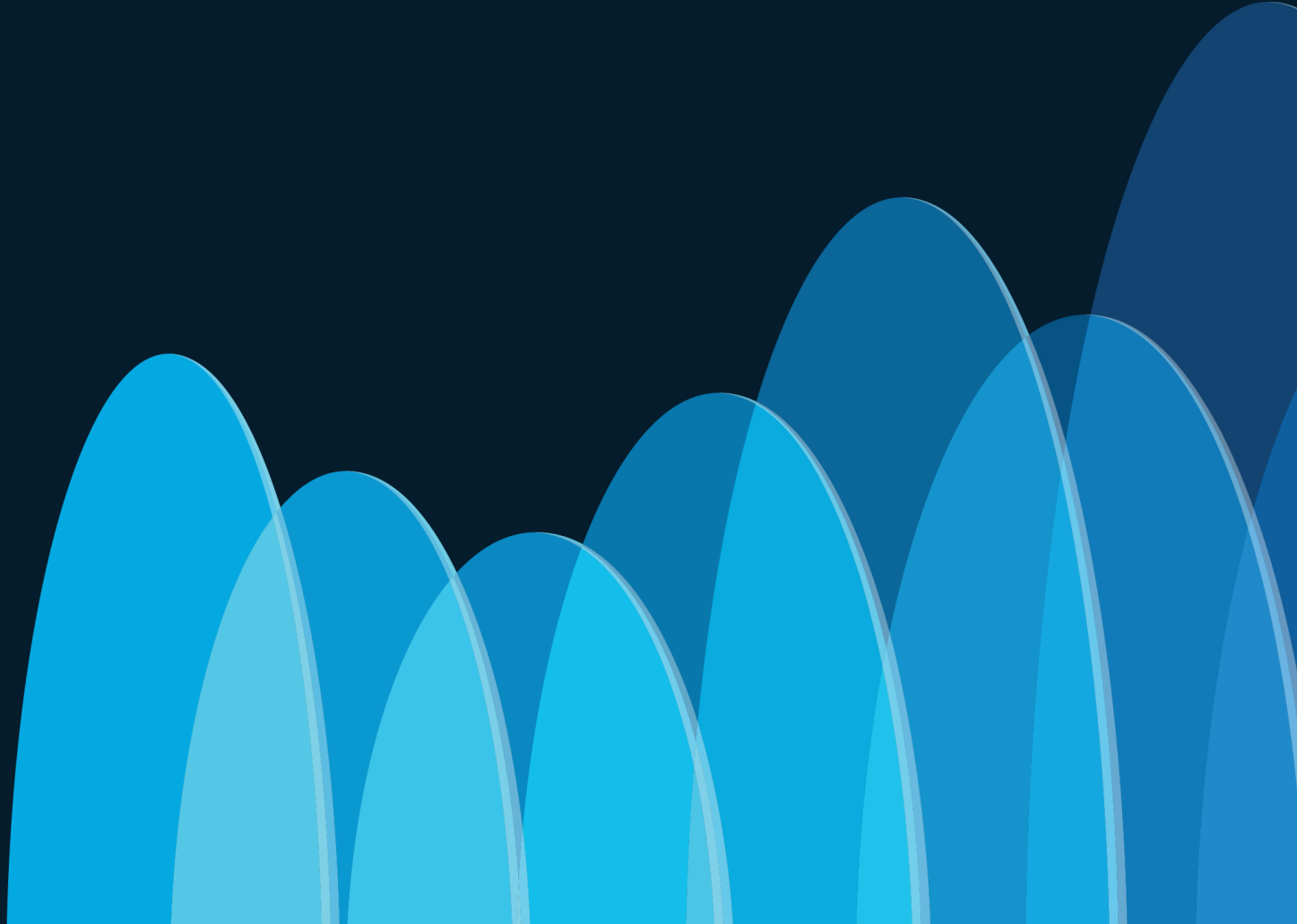
Understanding ACI security...

External Connectivity...

Increasing Security...

Automation Blueprints...

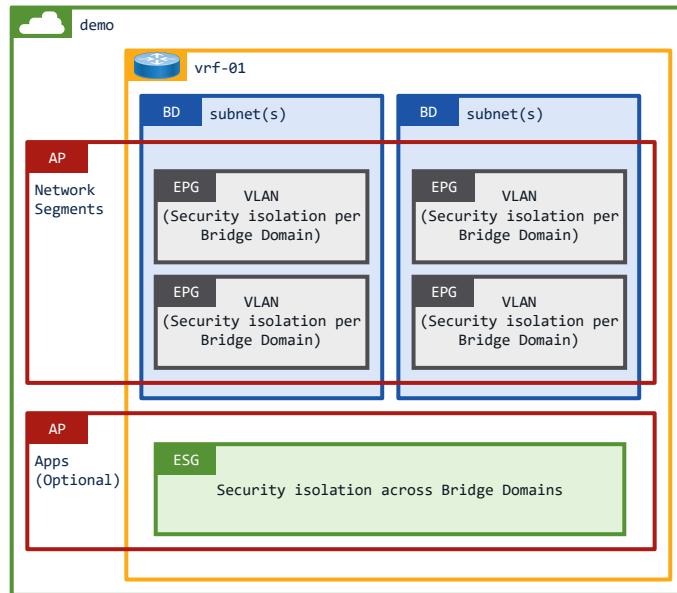
Wrapping up...



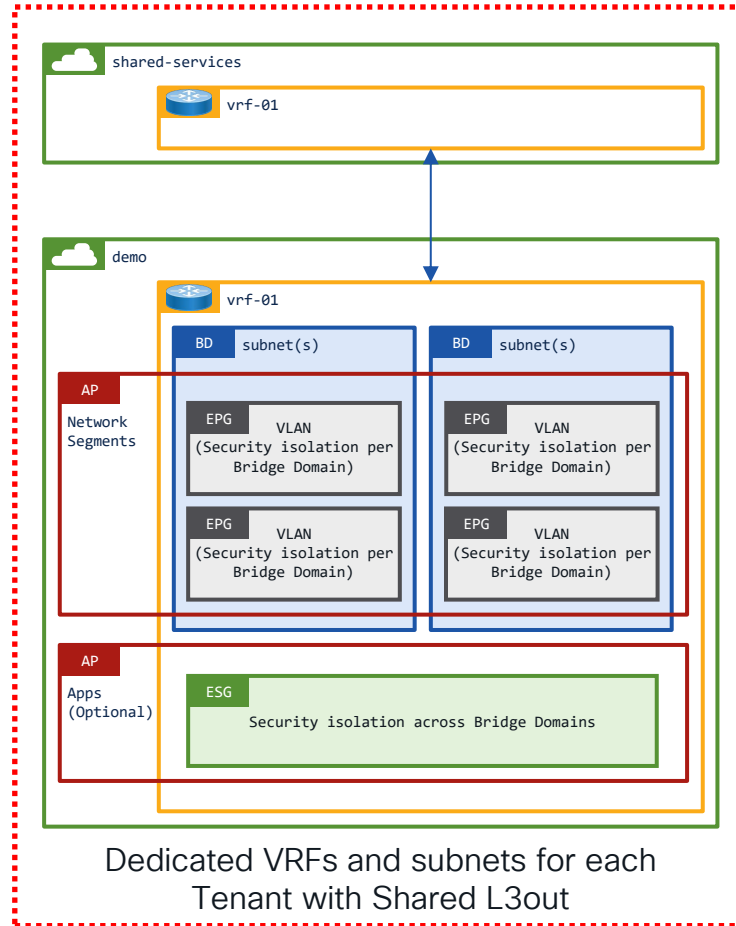
Where should you place your L3outs...?

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

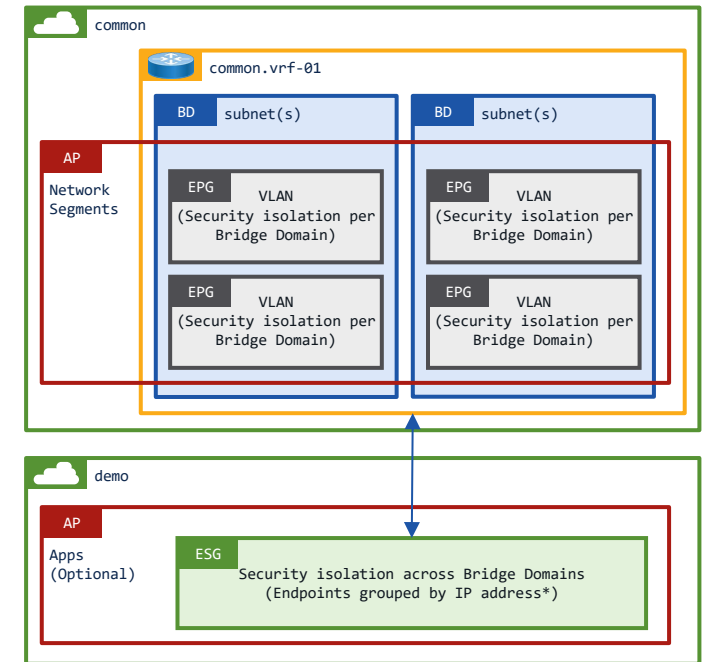
External Connectivity



Dedicated VRFs and subnets for each Tenant with Dedicated L3outs

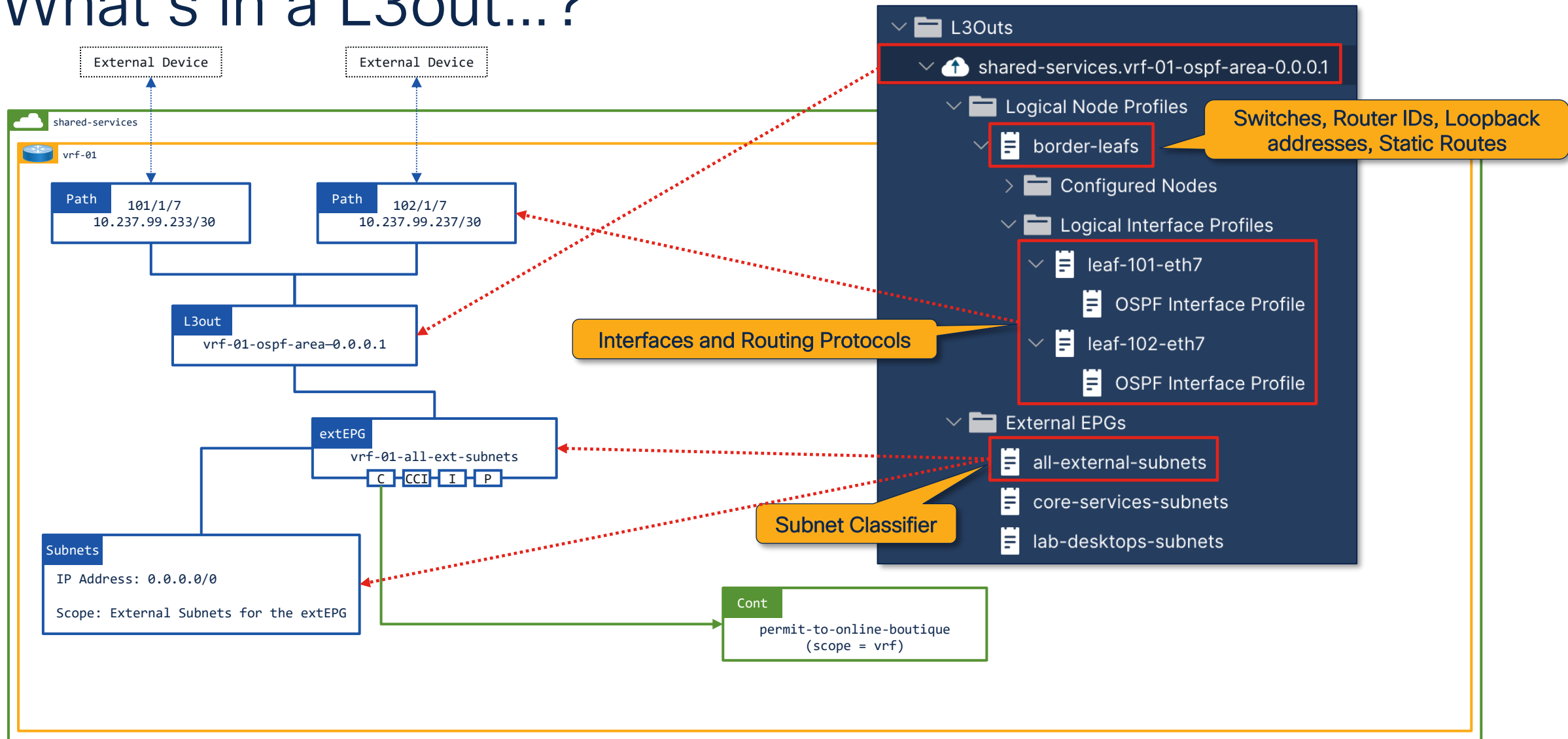


Dedicated VRFs and subnets for each Tenant with Shared L3out



Shared networking with isolated security

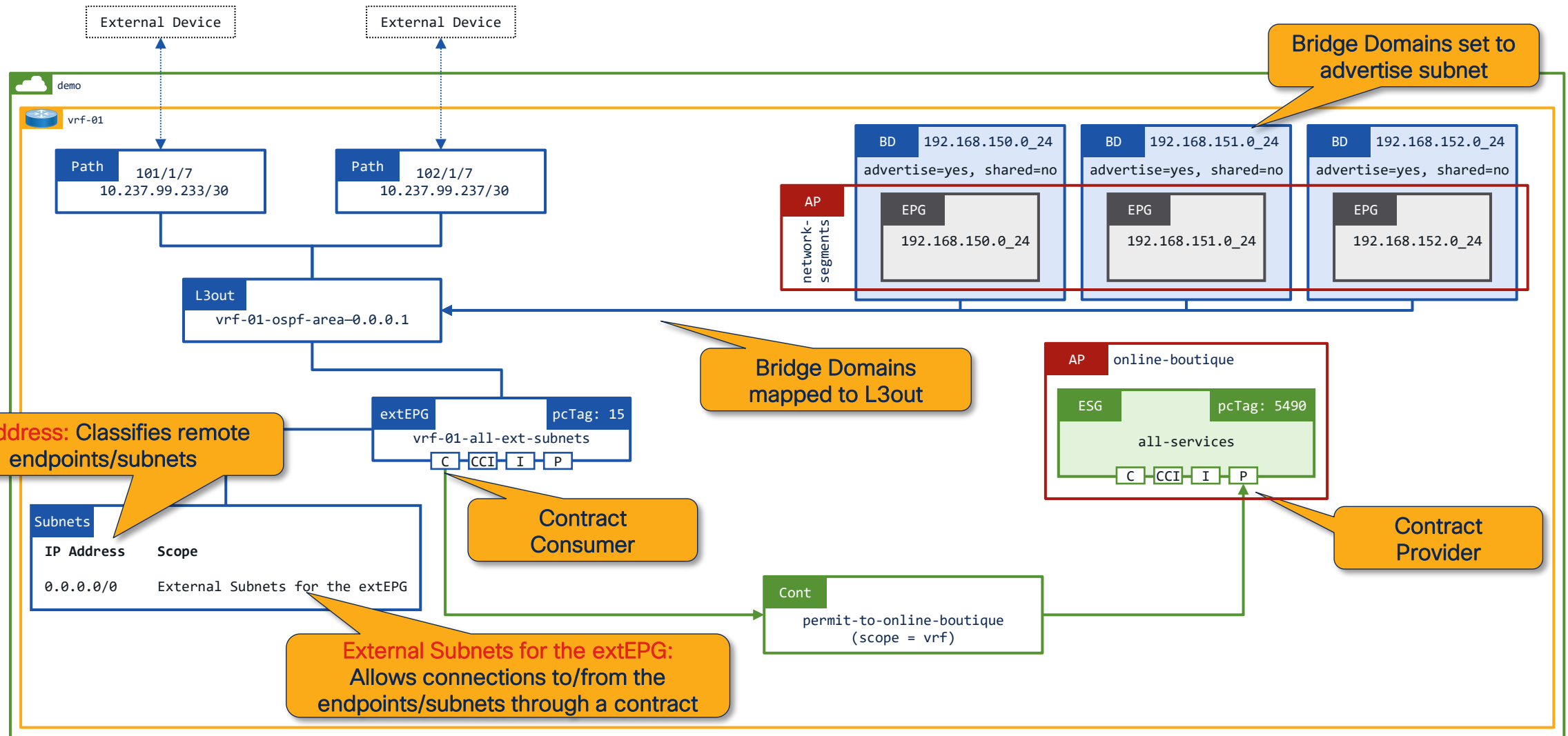
What's in a L3out...



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

Option 1 – Dedicated L3out per Tenant

Dedicated L3out



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

External Classification

IP Address:
Identifies remote endpoints/subnets

Create Subnet

IP Address:

Subnet Address/mask

Name:

Route Control

Route control is used for filtering external routes advertised out of the fabric, allowed into the fabric, or leaked to other VRFs within the fabric.

☐ Export Route Control Subnet

☐ Import Route Control Subnet

☐ Shared Route Control Subnet

Aggregate

☐ Aggregate Export

☐ Aggregate Import

☐ Aggregate Shared Routes

Route Summarization Policy

OSPF Route Summarization:

select an option

Route Control Profile:

Name

Direction

External EPG Classification

External EPG classification is used to identify the external networks associated with this external EPG for policy enforcement (contracts).

☐ External Subnets for External EPG

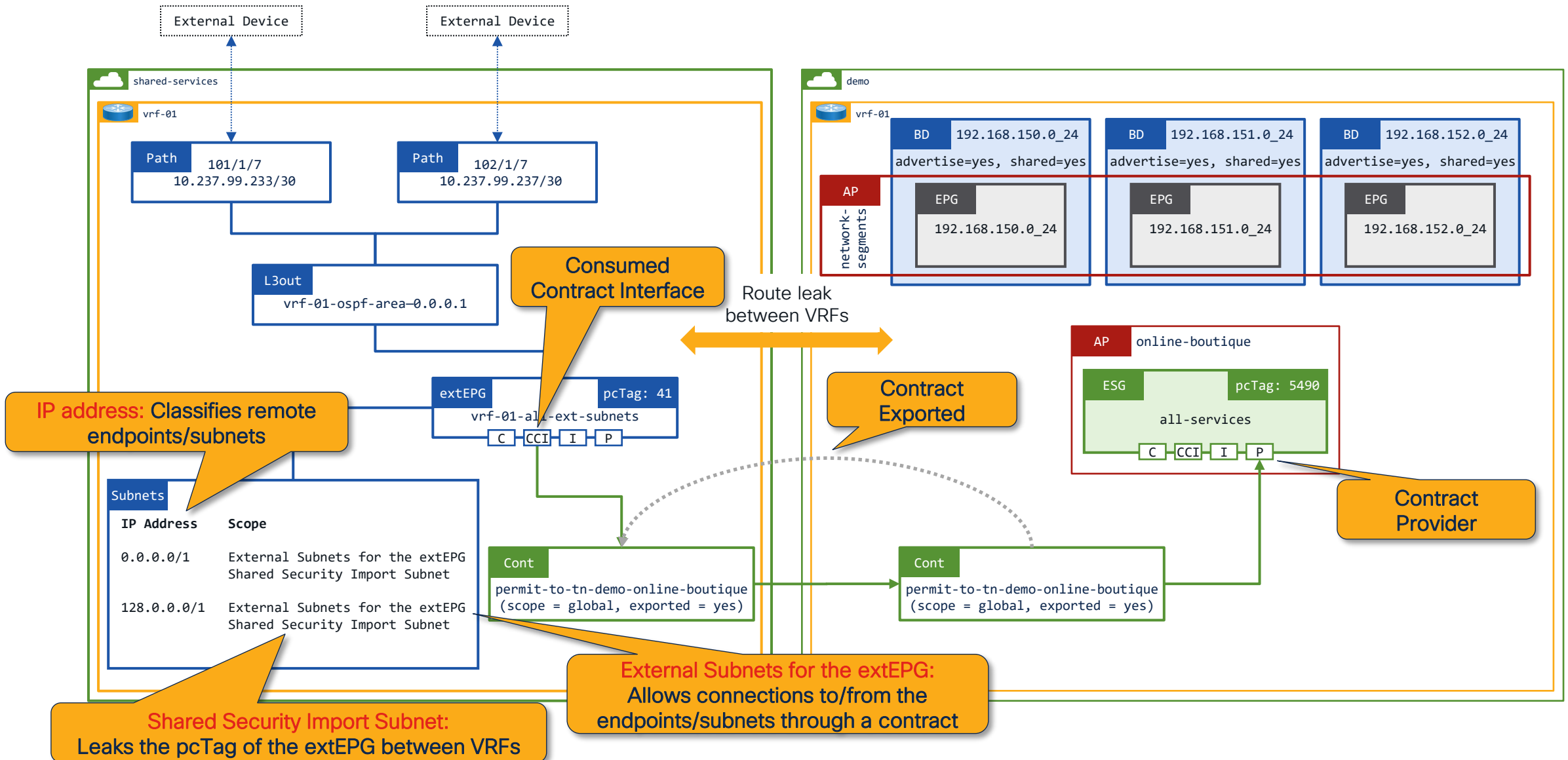
☐ Shared Security Import Subnet

External Subnets for External EPG:
Required for contract purposes

- **IP Address:** identifies remote endpoints/subnets
- **External Subnets for External EPG:** allows packets to/from the L3out with a contract

Option 2 – Shared L3out

Shared L3out – Route Leaking between VRFs (ESGs)



External Classification and Route Leaking

IP Address:
Identifies remote endpoints/subnets

Create Subnet

IP Address: Subnet Address/mask: Name:

Route Control

Route control is used for filtering external routes advertised out of the fabric, allowed into the fabric, or leaked to other VRFs within the fabric.

☐ Export Route Control Subnet
☐ Import Route Control Subnet
☐ Shared Route Control Subnet

Aggregate

☐ Aggregate Export
☐ Aggregate Import
☐ Aggregate Shared Routes

Route Summarization Policy

OSPF Route Summarization:
select an option

Route Control Profile:

Name	Direction
------	-----------

External EPG Classification

External EPG classification is used to identify the external networks associated with this external EPG for policy enforcement (contracts).

☐ External Subnets for External EPG
☐ Shared Security Import Subnet

External Subnets for External EPG:
Required for contract purposes

Shared Security Import Subnet:
Leaks the pcTag/Class ID between VRFs

- **IP Address:** identifies remote endpoints/subnets, must match a received route for route leaking purposes
- **External Subnets for External EPG:** allows packets to/from the L3out with a contract
- **Shared Security Import Subnet:** is always required as it leaks the extEPG pcTag to the target VRF

Shared L3out – Route Leaking between VRFs (ESGs)

Prefix to leak

External Prefixes

IP	Description	Greater Than Equal (Prefix)	Target VRF(s)
0.0.0.0/0	Unspecified	Unspecified	ciscolive-07/vrf-01 common/common.vrf-01 demo/vrf-01 fgandola/vrf-01 rwhitear/vrf-01 ssharman/vrf-01

Subnets to leak

IP	Description	Allow L3Out Advertisement	Target VRF(s)
192.168.150.0/24			shared-services/vrf-01
192.168.151.0/24		True	shared-services/vrf-01
192.168.152.0/24		True	shared-services/vrf-01

Bridge Domain Subnets

Classify the external subnets and share the extEPG pcTag between VRFs



Getting into the weeds...!

How does ACI Route Leaking work for EPGs...?

External Classification and Route Leaking

IP Address:
Identifies remote endpoints/subnets

IP Address:
Must match a received route
for route leaking purposes

Shared Route Control Subnet:
Leaks a received route to another VRF

External Subnets for External EPG:
Required for contract purposes

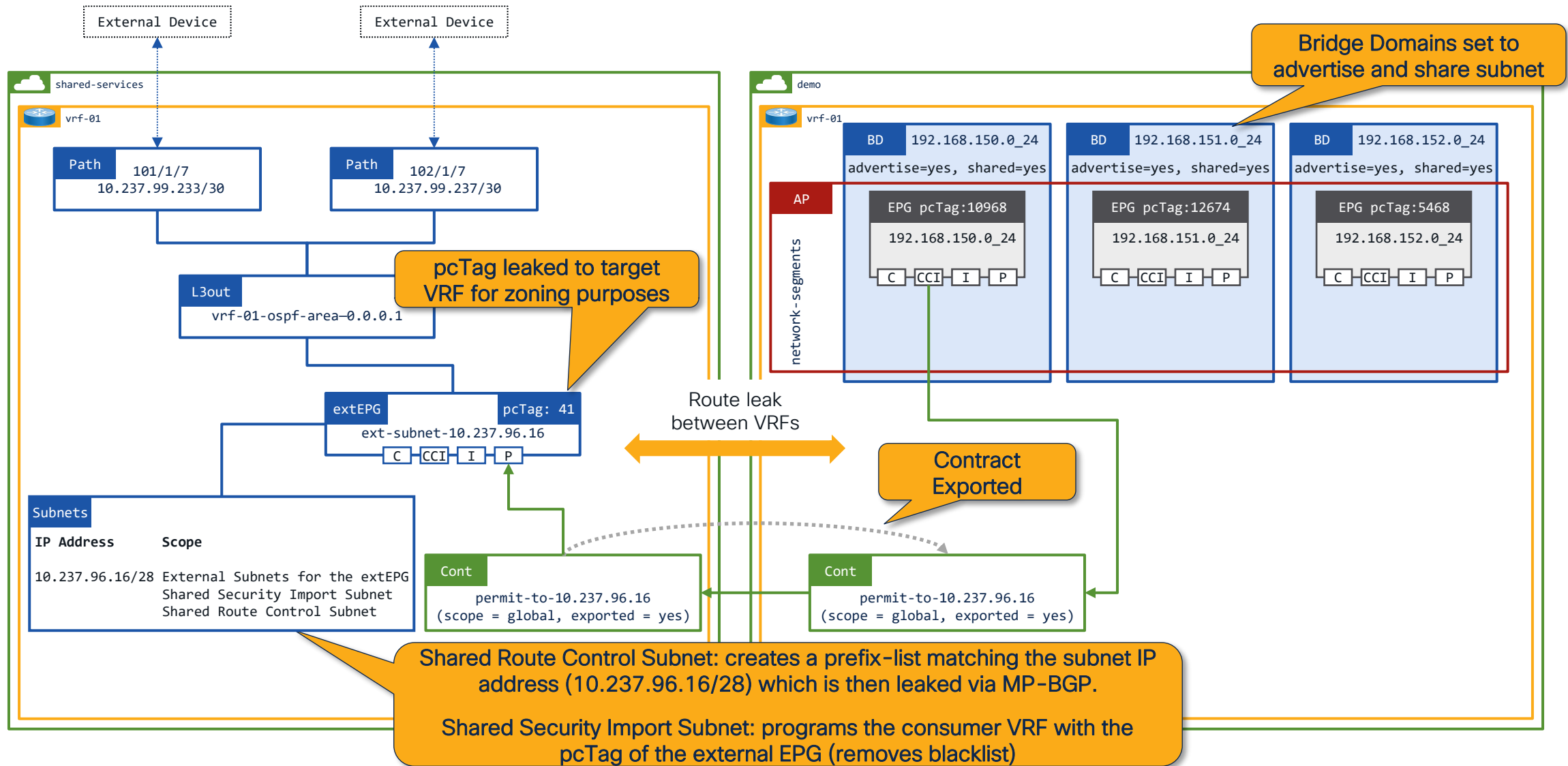
Aggregate Shared Routes:
Optional - Creates a prefix-list to
aggregate routes

Shared Security Import Subnet:
Leaks the pcTag/Class ID between VRFs

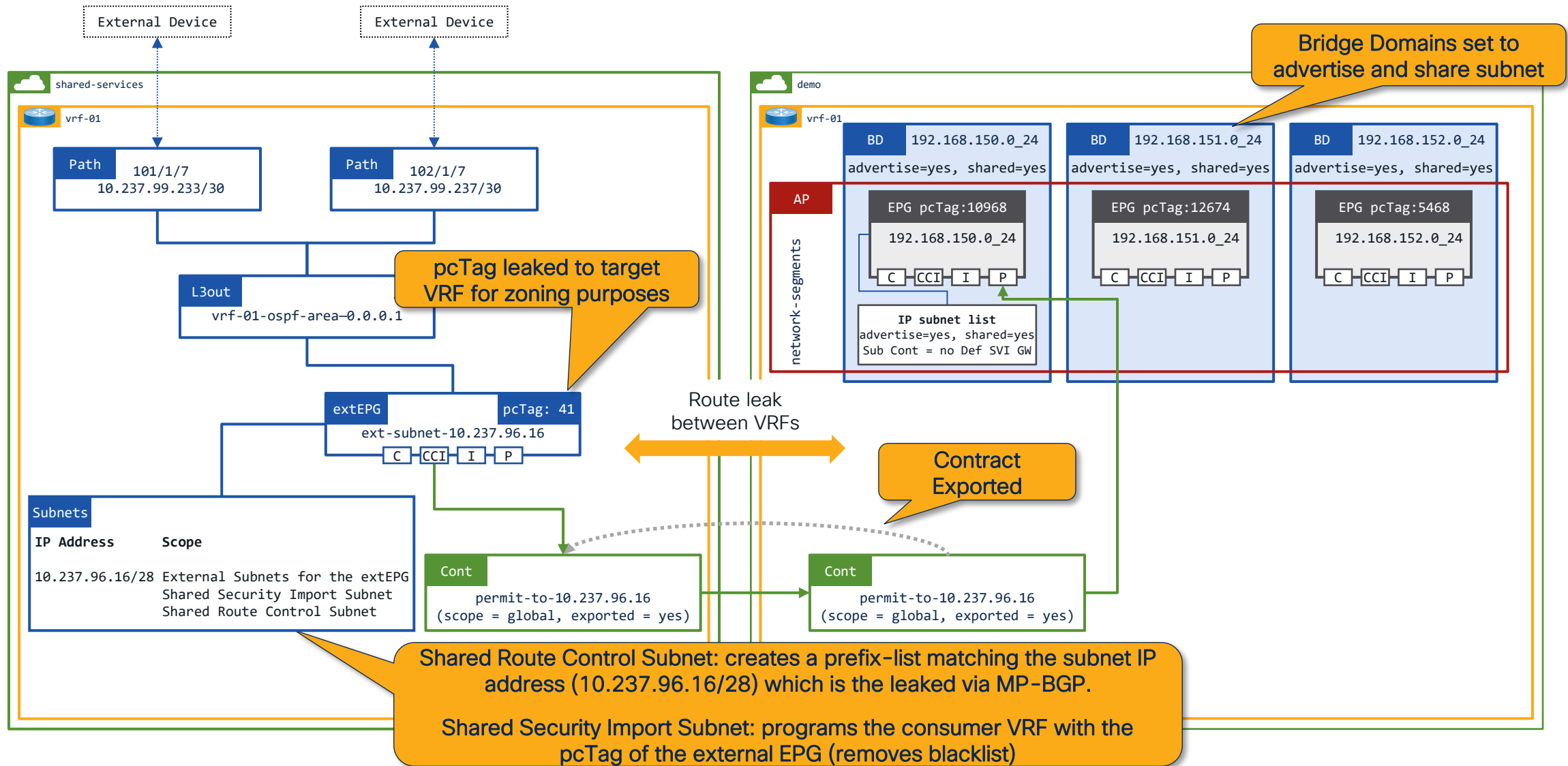
The screenshot shows the 'Create Subnet' configuration page. At the top, there are fields for 'IP Address' and 'Subnet Address/mask'. Below this is the 'Name' field. The 'Route Control' section contains three checkboxes: 'Export Route Control Subnet', 'Import Route Control Subnet', and 'Shared Route Control Subnet'. To the right of these are 'Aggregate' checkboxes: 'Aggregate Export', 'Aggregate Import', and 'Aggregate Shared Routes'. Further right is the 'Route Summarization Policy' section with a dropdown for 'OSPF Route Summarization'. Below these is the 'Control Profile' section with a 'Name' field. At the bottom is the 'External EPG Classification' section with two checkboxes: 'External Subnets for External EPG' and 'Shared Security Import Subnet'. Several orange callout boxes with white text are overlaid on the page, providing additional context for specific fields and options.

- **IP Address:** identifies remote endpoints/subnets, must match a received route for route leaking purposes
- **External Subnets for External EPG:** allows packets to/from the L3out with a contract
- **Shared Security Import Subnet:** is always required as it leaks the extEPG pcTag to the target VRF
- **Shared Route Control Subnet:** not required when route leaking is configured under the VRF
- **Aggregate Shared Routes:** creates a prefix-list to aggregate routes

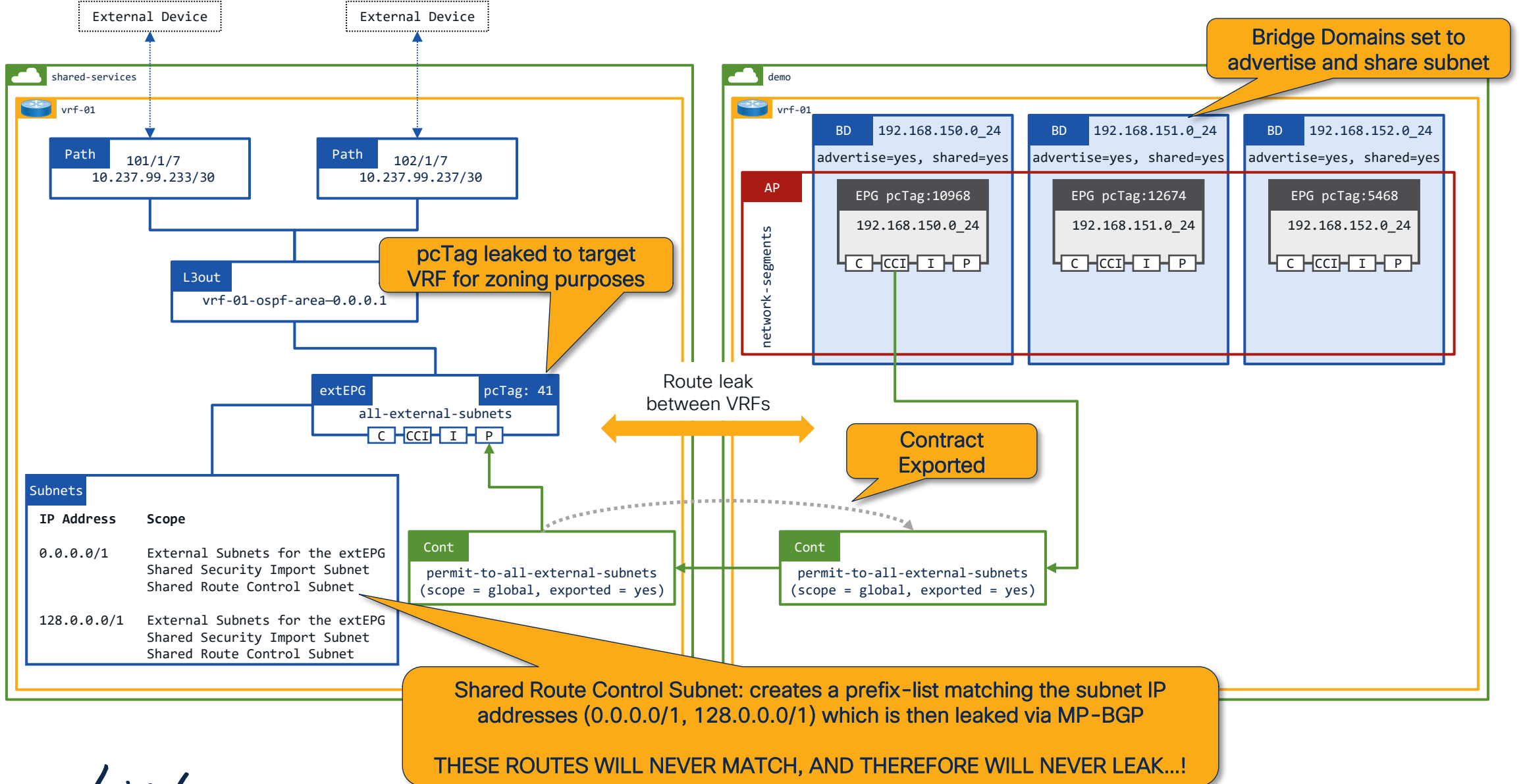
EPG Route Leaking – L3out is the Provider



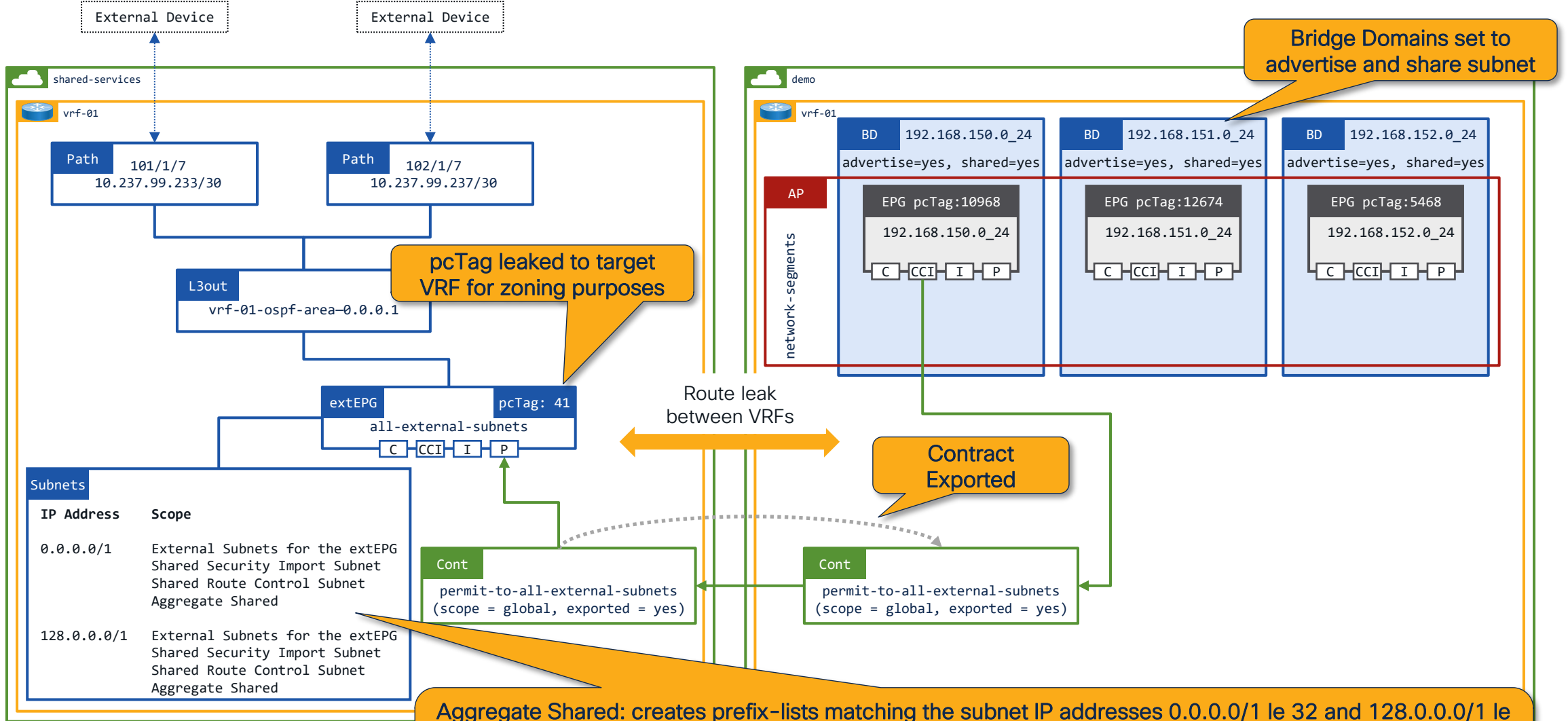
EPG Route Leaking - L3out is the Consumer



“Shared Route Control Subnet” must match a received route



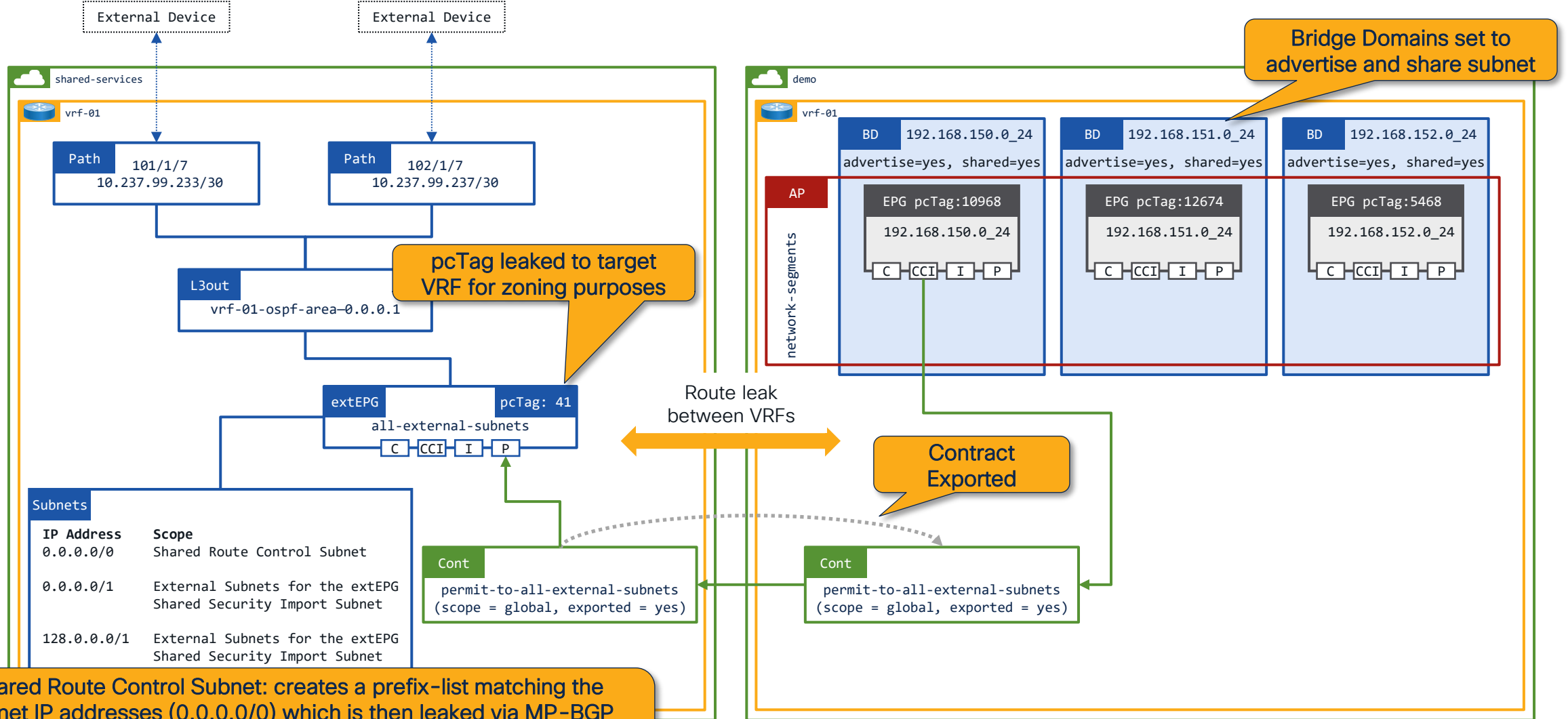
Leaking all received routes



Aggregate Shared: creates prefix-lists matching the subnet IP addresses 0.0.0.0/1 le 32 and 128.0.0.0/1 le 32, the matching routes are then leaked via MP-BGP.

Note: the scope does not match 0.0.0.0/0, thus a received default route will not leak between VRFs.

Leaking a default route

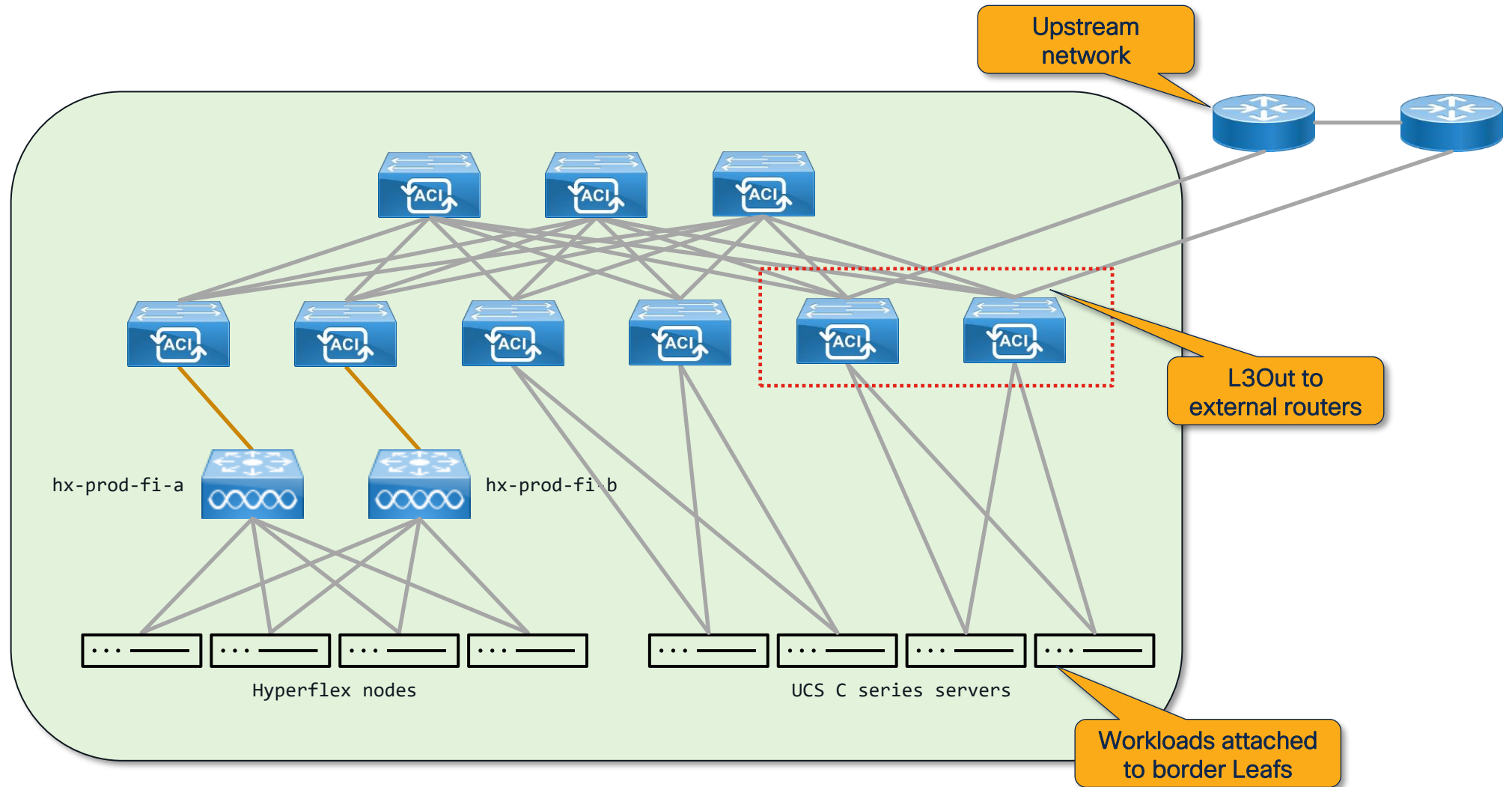


Shared Route Control Subnet: creates a prefix-list matching the subnet IP addresses (0.0.0.0/0) which is then leaked via MP-BGP

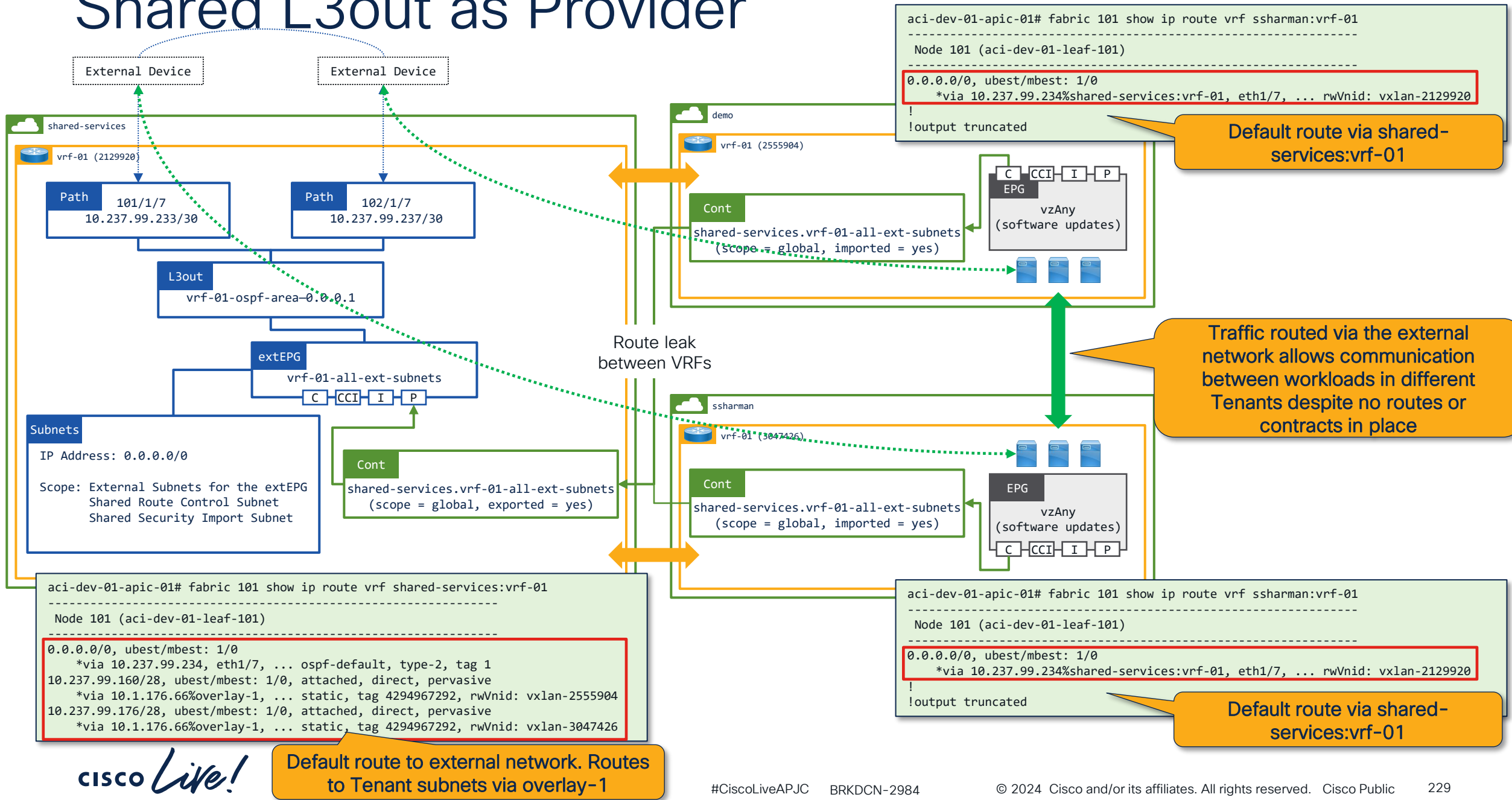
Do Not configure "External Subnets for the extEPG" for 0.0.0.0/0

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

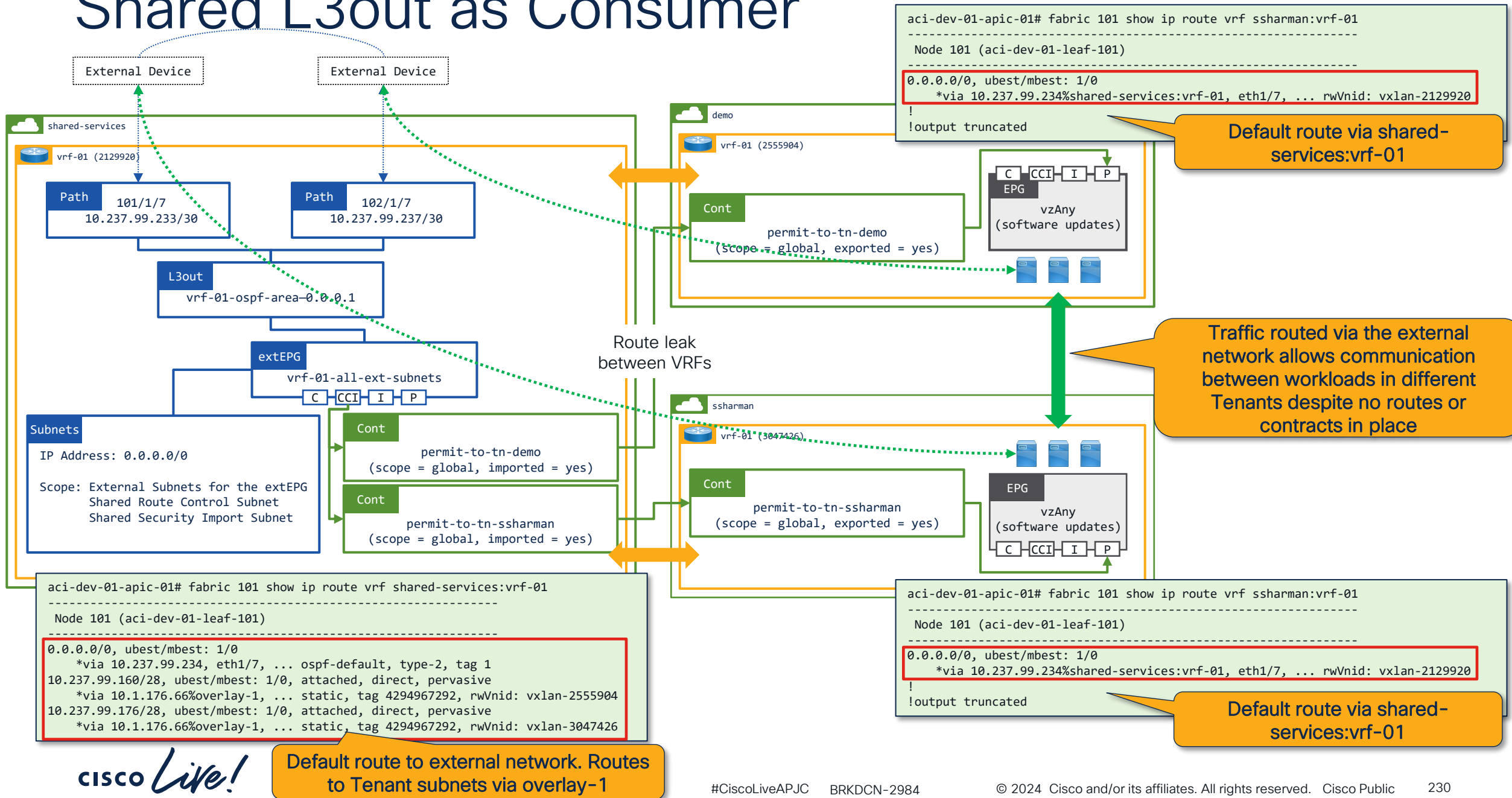
Non dedicated border Leafs



Shared L3out as Provider



Shared L3out as Consumer



Recommendation

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

Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

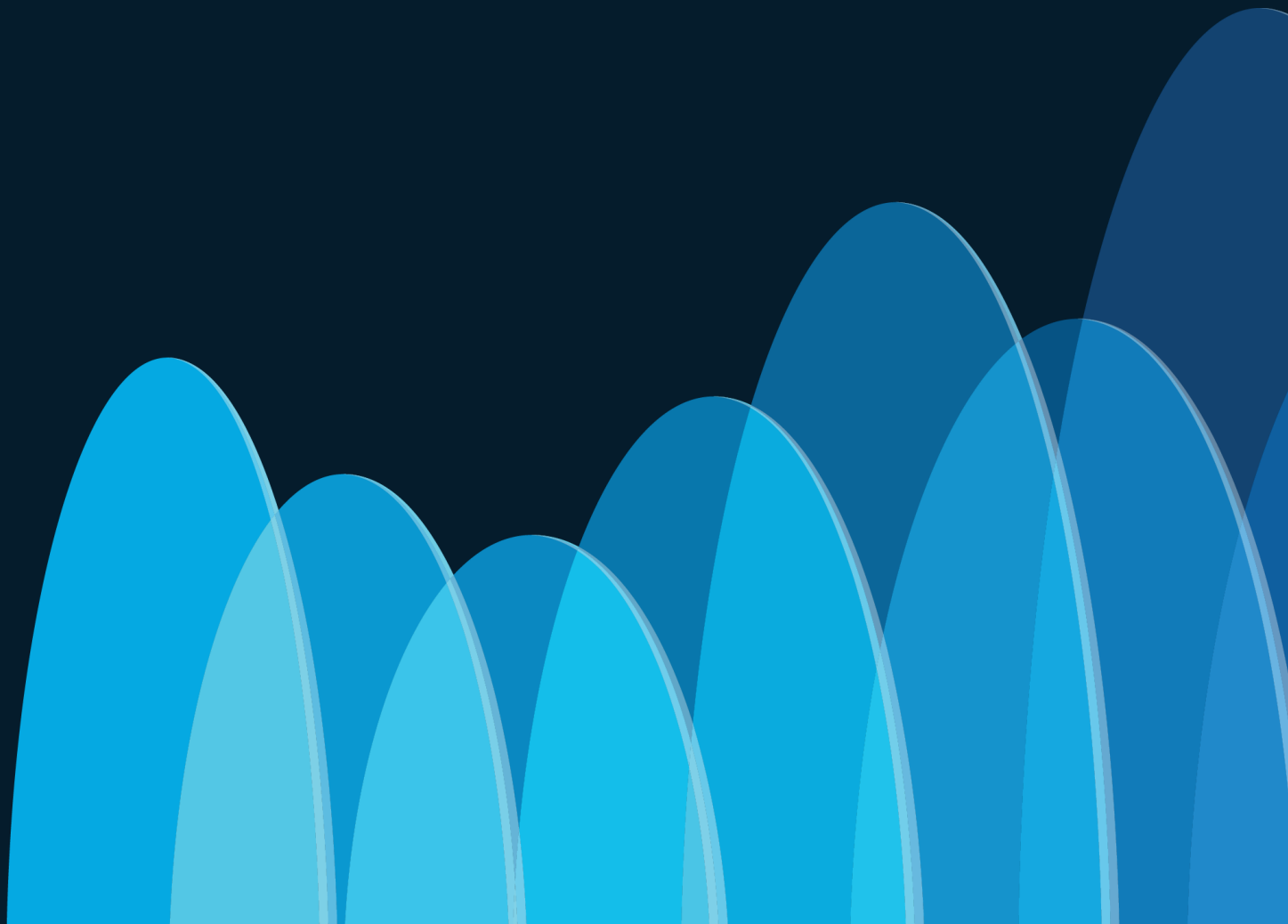
Understanding ACI security...

External Connectivity...

Increasing Security...

Automation Blueprints...

Wrapping up...

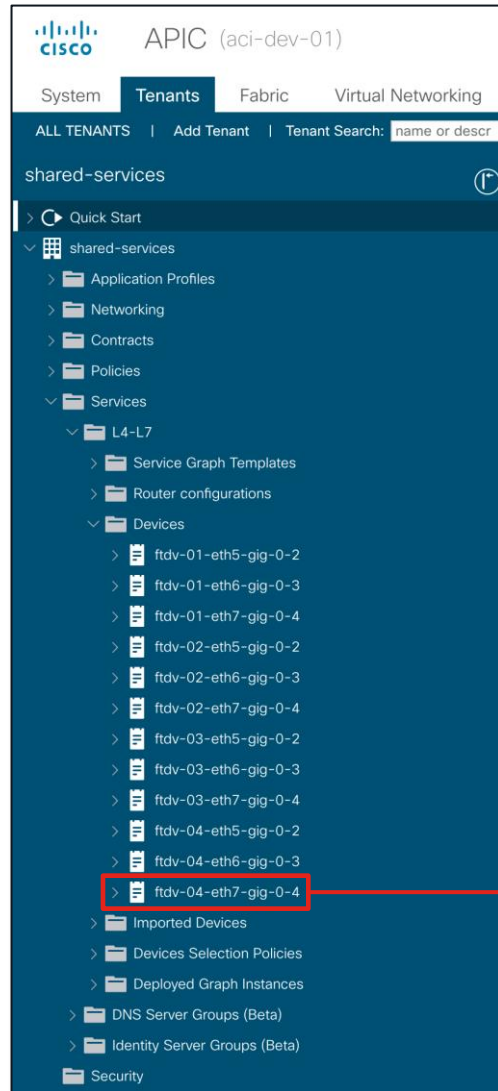
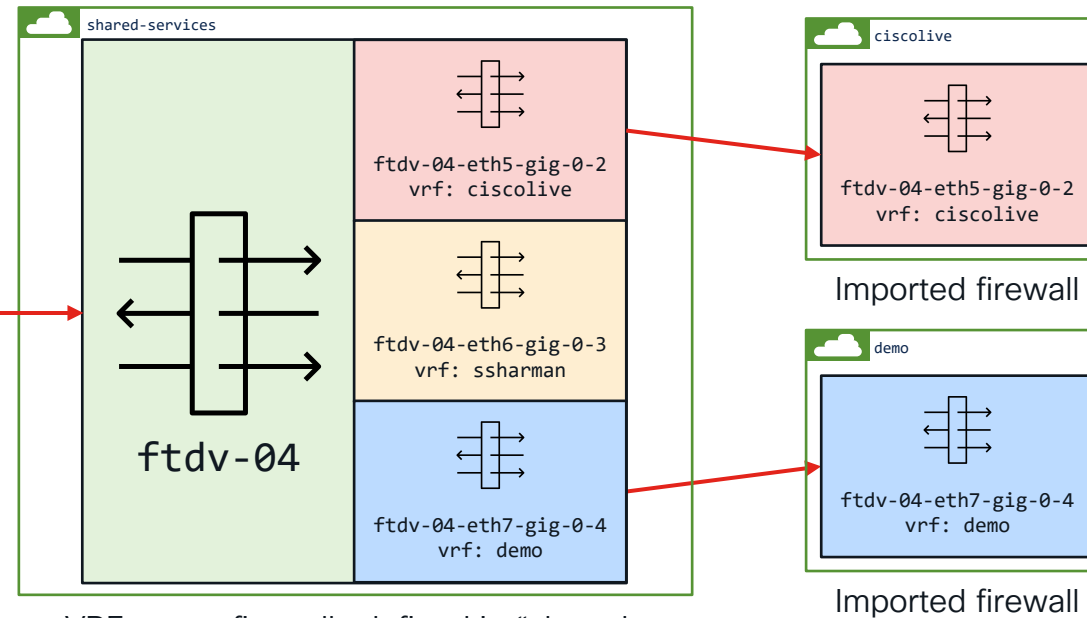


Where should you place your L4-7 devices...?

Do you want to use Layer 2 or Layer 3 redirects for service insertion...?

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

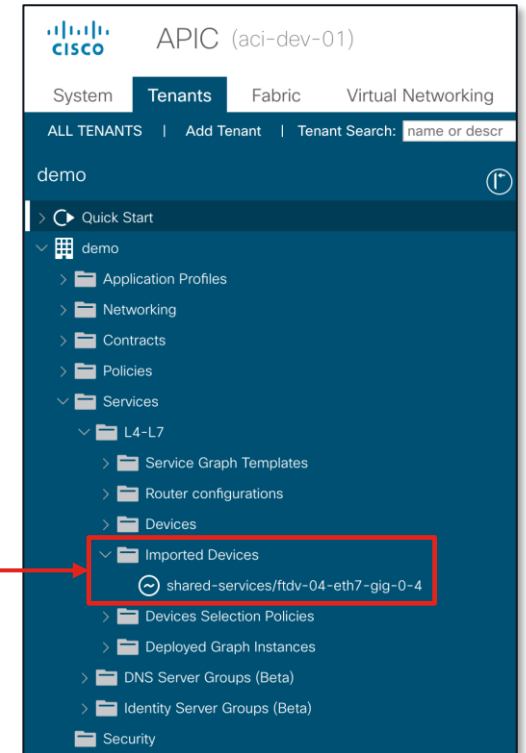
Virtual firewall deployment



VRF aware firewalls defined in “shared-services” and exported to “user” tenants

Benefits of virtual firewall / IPS

- One or more virtual firewalls exported to “user” tenants as required
- Virtual firewalls used for targeted service insertion
- Firewall throughput matches application requirements
- Firewall ruleset reduced to application requirements
- Firewall security group members pushed/pulled from APIC (where available)



ACI Endpoint Update App (optional)

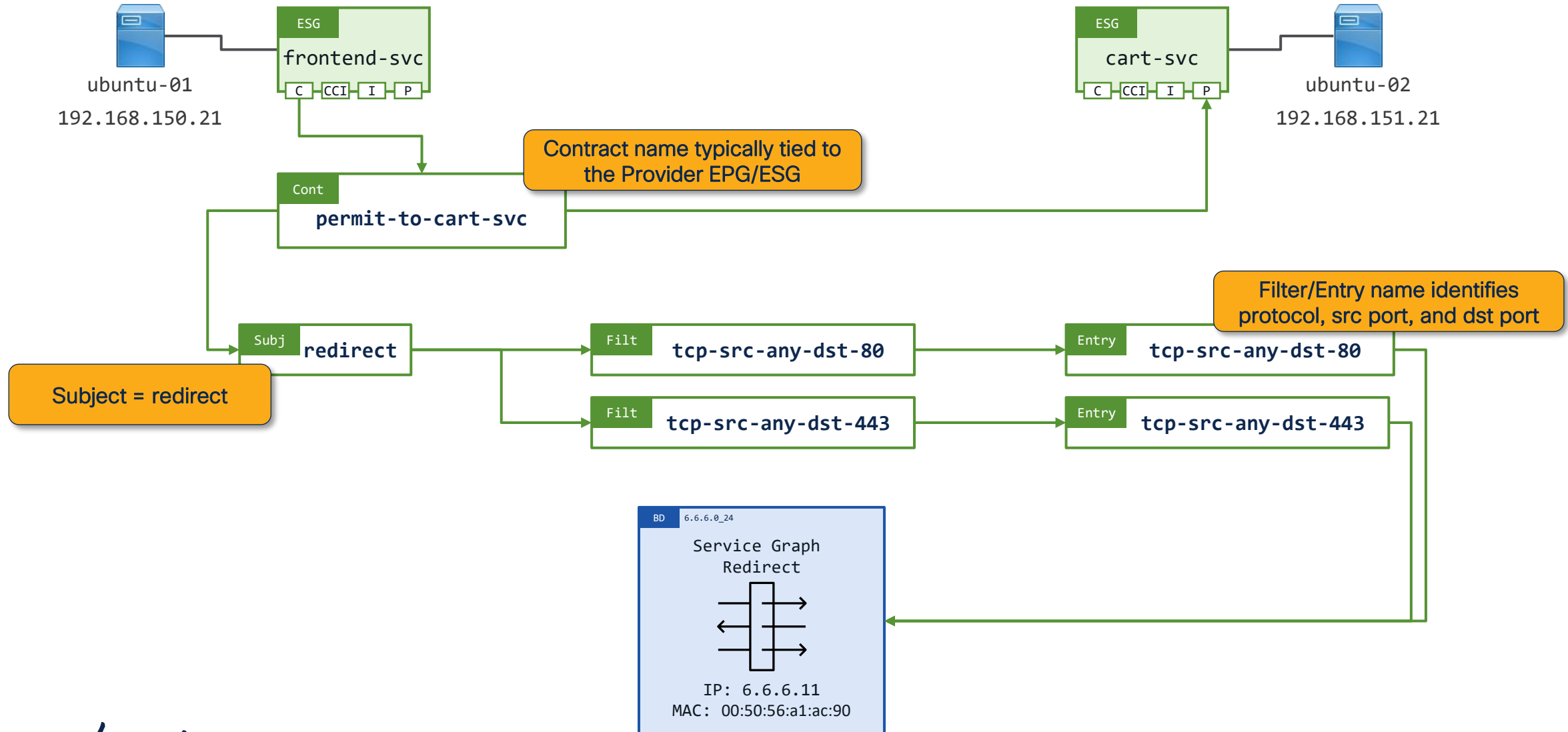
<https://dcappcenter.cisco.com/aci-endpoint-update.html>

The screenshot displays two interfaces. The top interface is the APIC (aci-dev-01) 'Apps' page, showing three installed apps: ELAM Assistant, ACI Endpoint Update (highlighted with a red box), and Nexus Insights Cloud Connector. The bottom interface is the Firewall Management Center 'Objects / Object Management' page. A red line connects the 'ACI Endpoint Update' app to the 'External Attributes' menu item in the left sidebar. The main content area shows a table of dynamic objects.

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

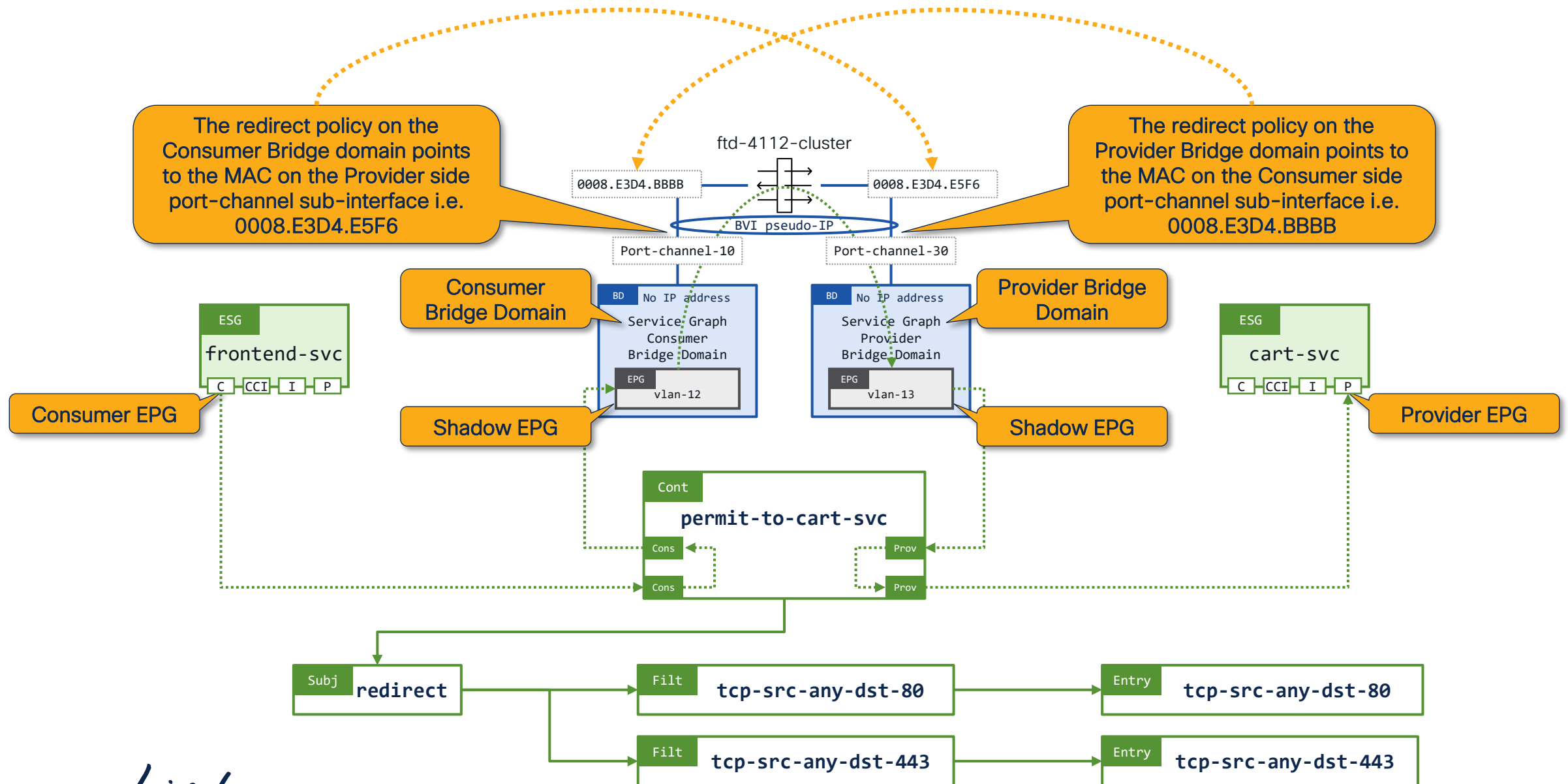
Setting up PBR to a one arm attached firewall...

Redirect applied to all Filters under the Subject...



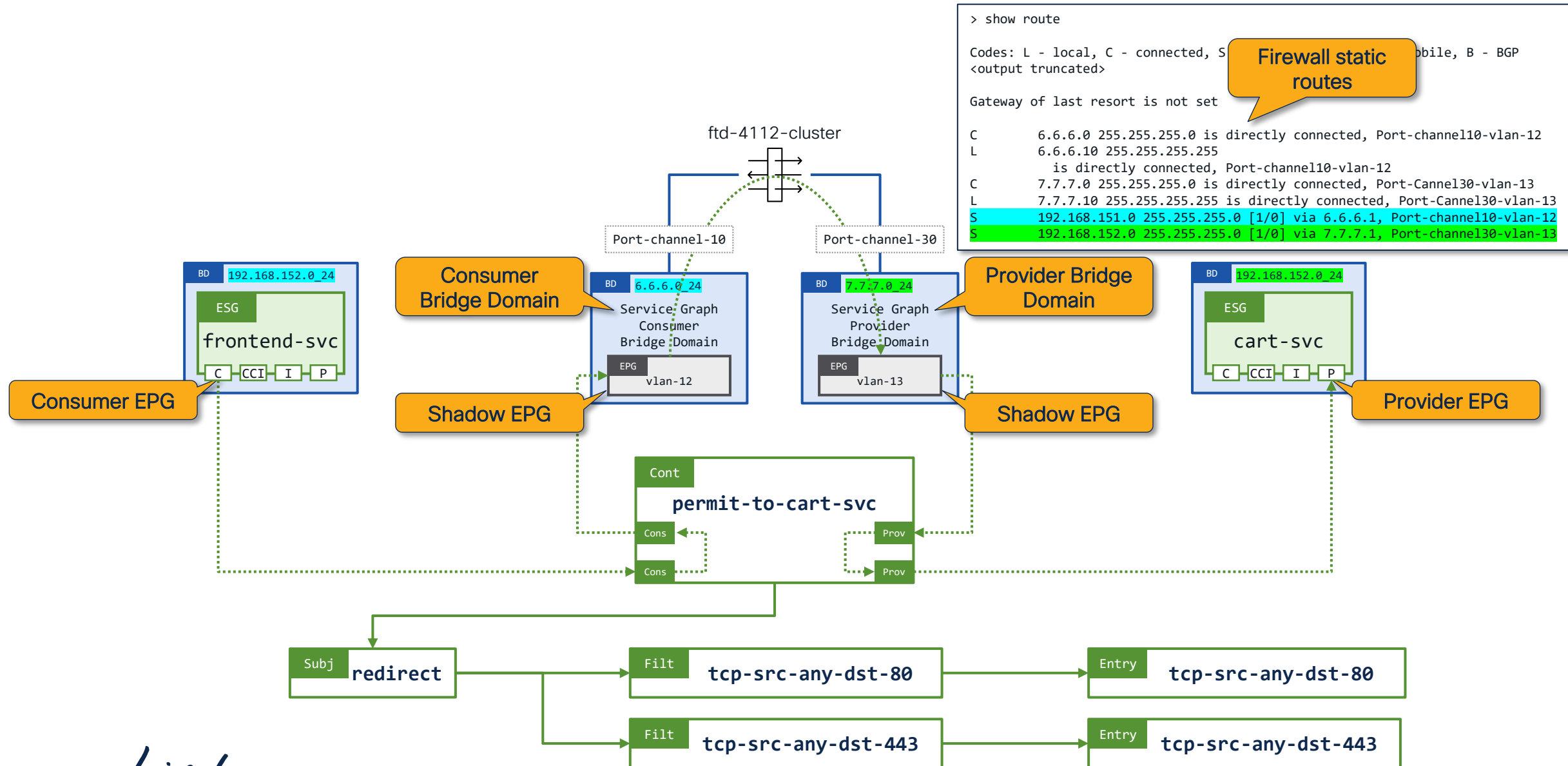
Setting up PBR to a two arm attached firewall...

Two arm service graph - L2

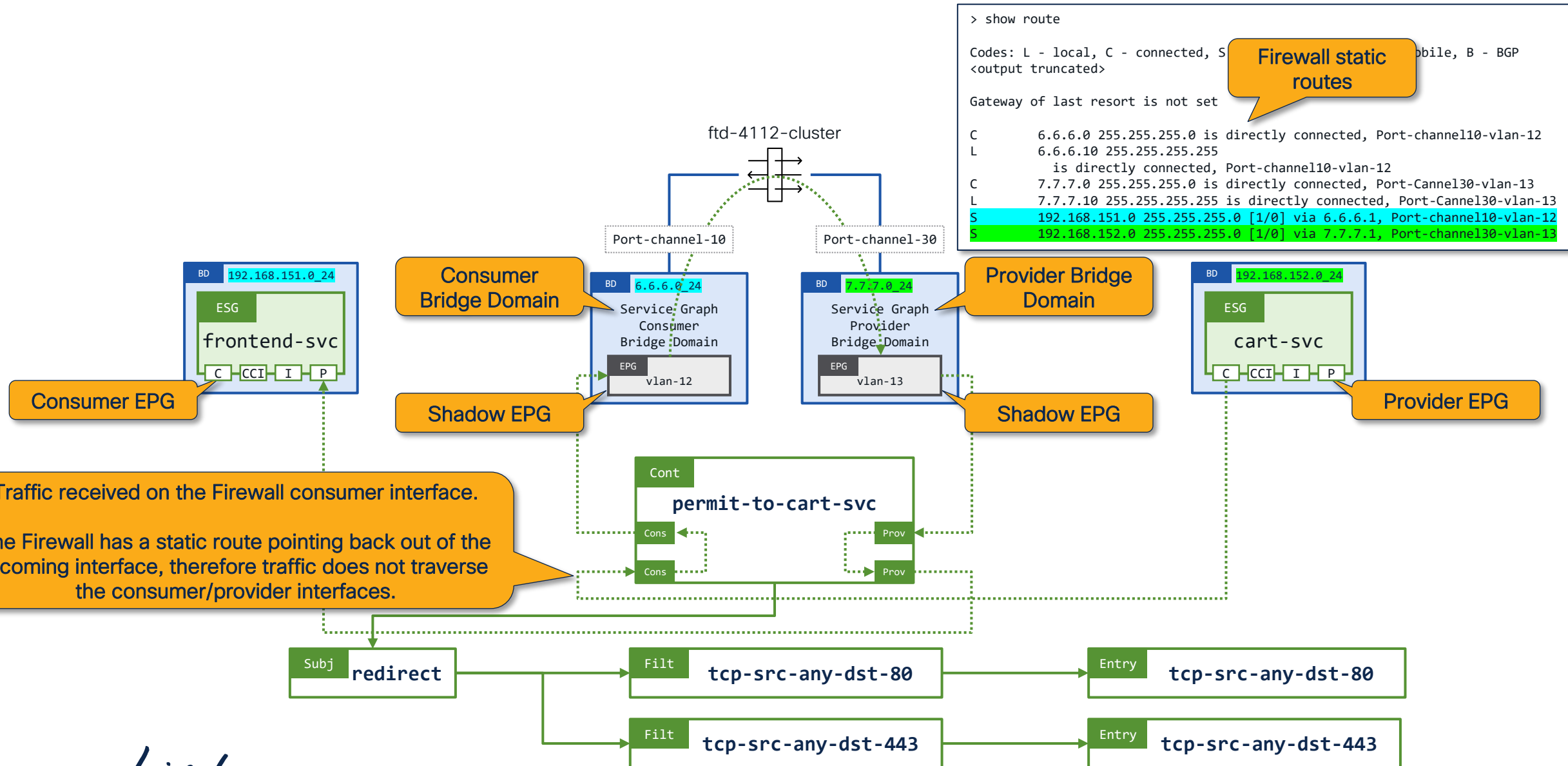


Do not use Two Arm with L3 redirect...

Two arm service graph - L3 Cons to Prov



Two arm service graph - L3 Prov to Cons



Layer 2 vs Layer 3 firewall insertion

Layer 2 – two arm attached

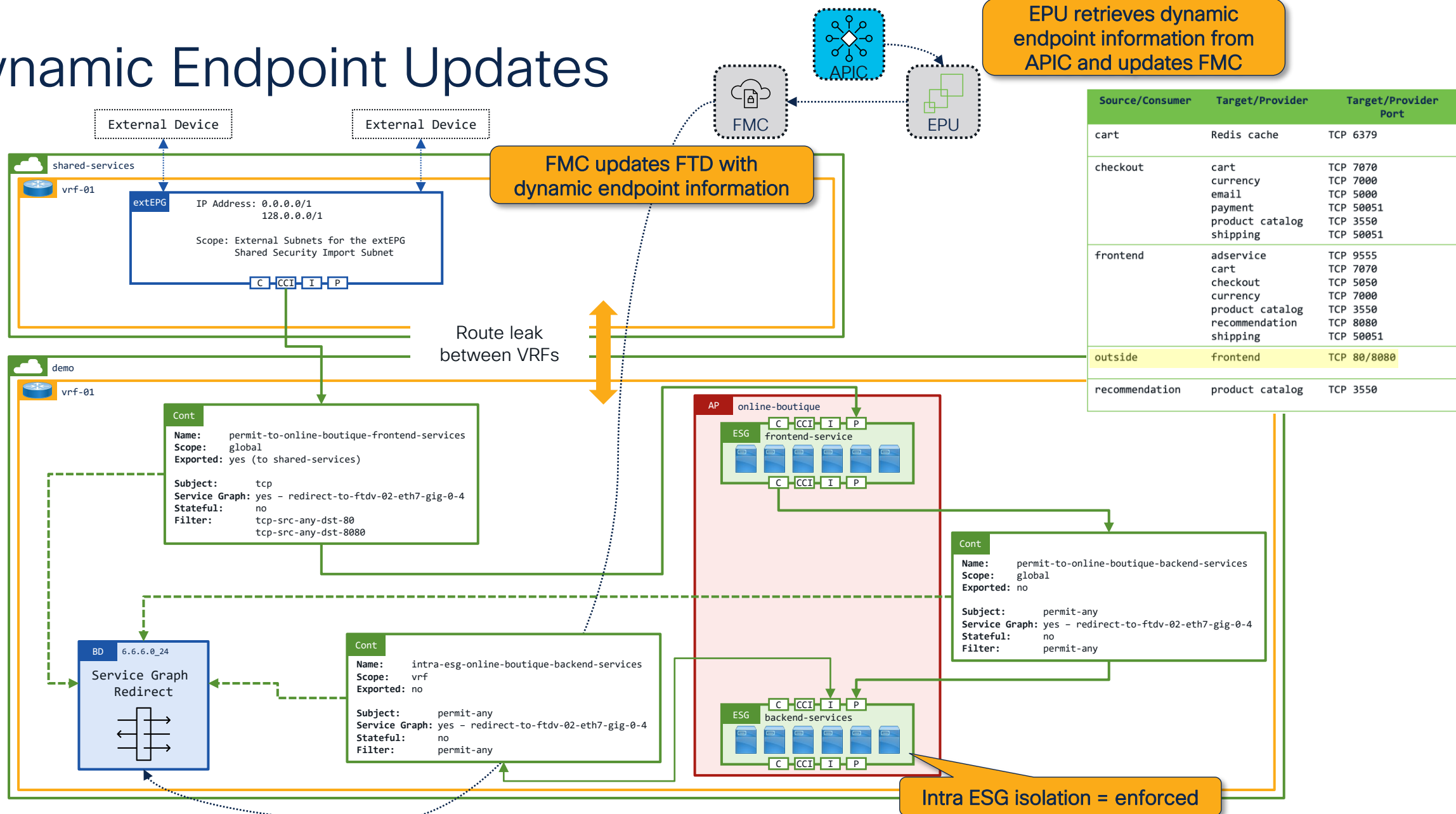
- Transparent IPS mode
- Slightly higher throughput
- No routing

• Layer 3 – one arm attached

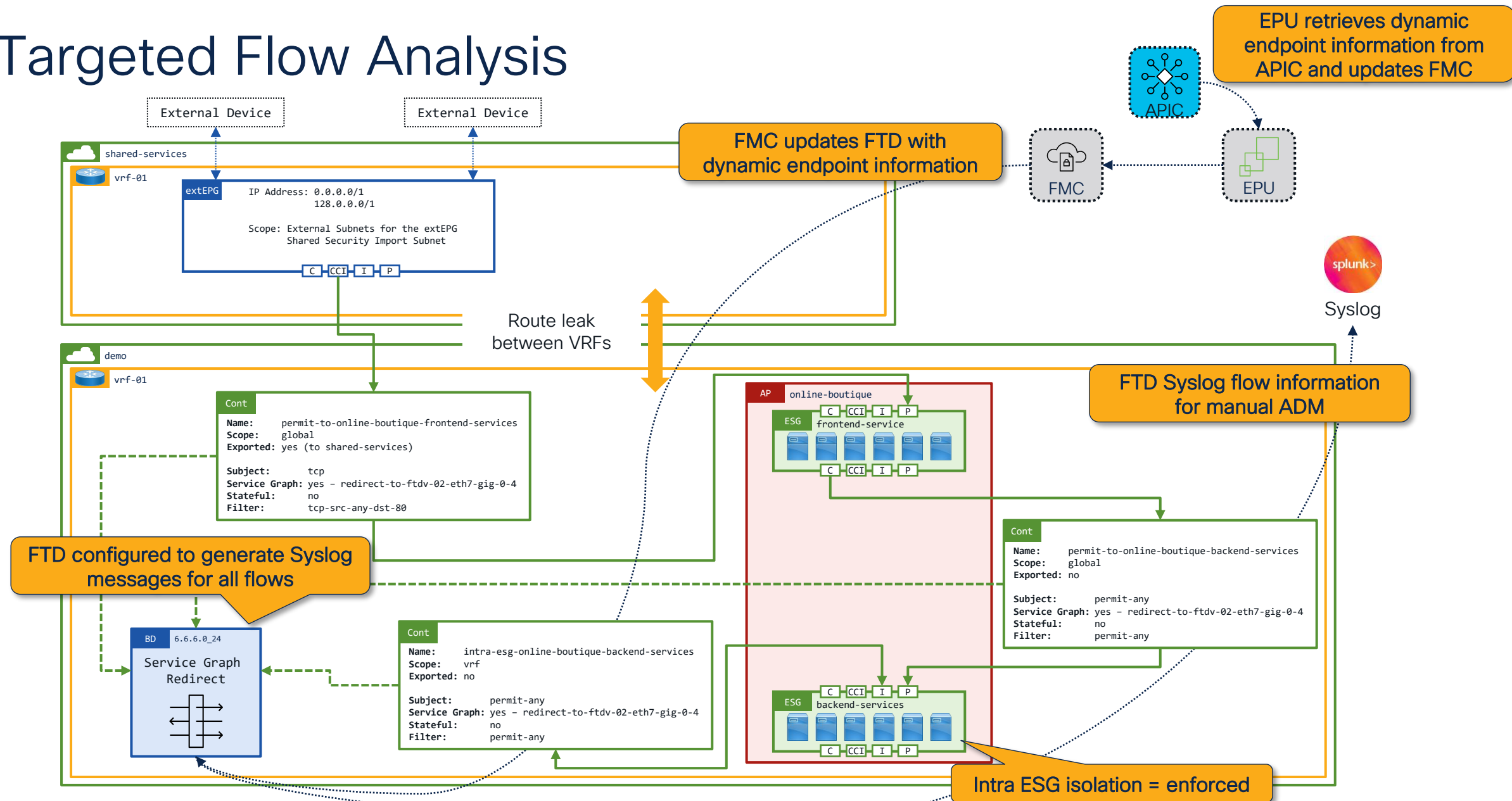
- Simple “default” routing
- Easier installation method
- Used by more than 95% of customers

Using Service Graphs for Security Enforcement and/or Application Dependency Mapping...

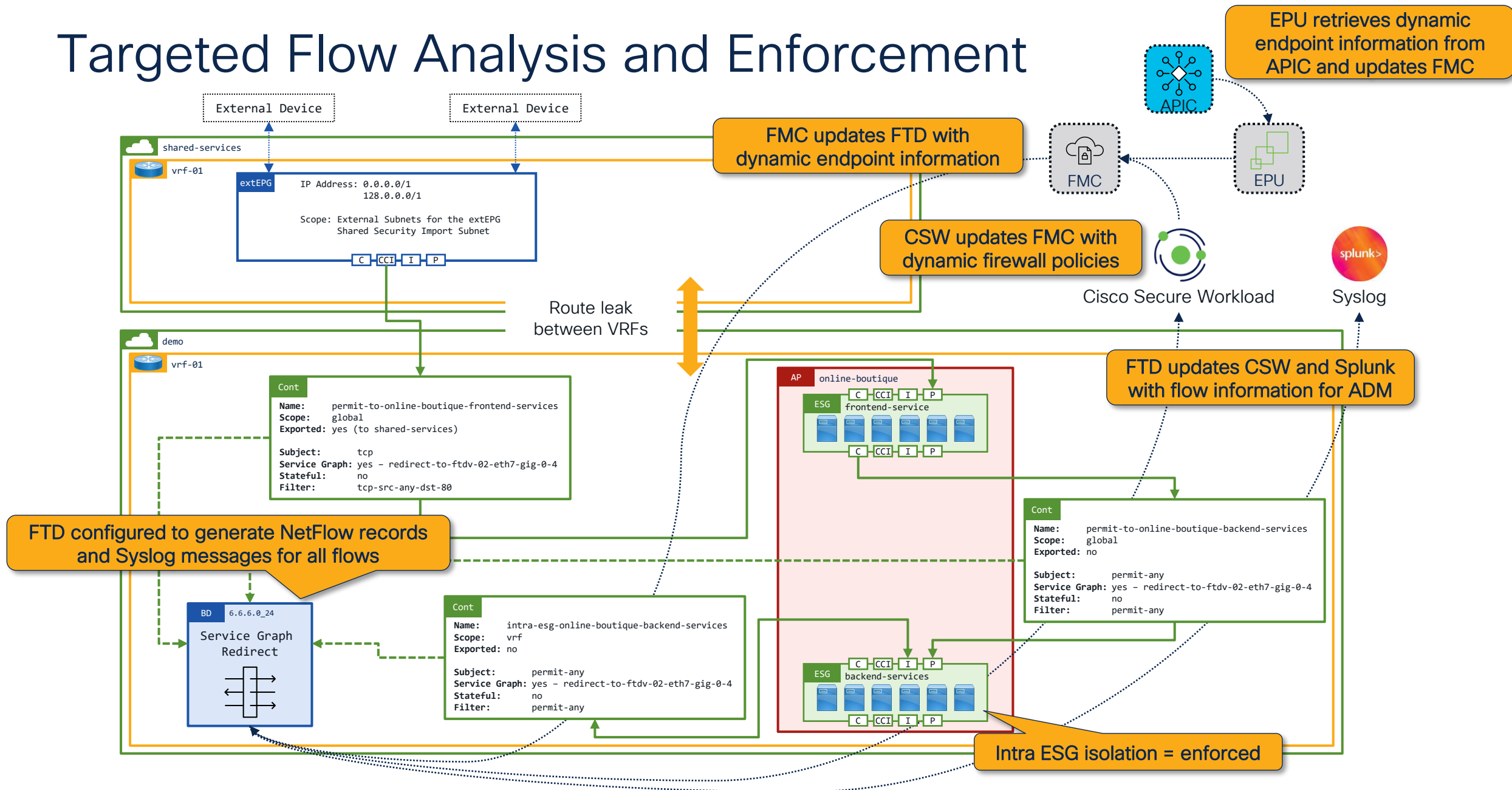
Dynamic Endpoint Updates



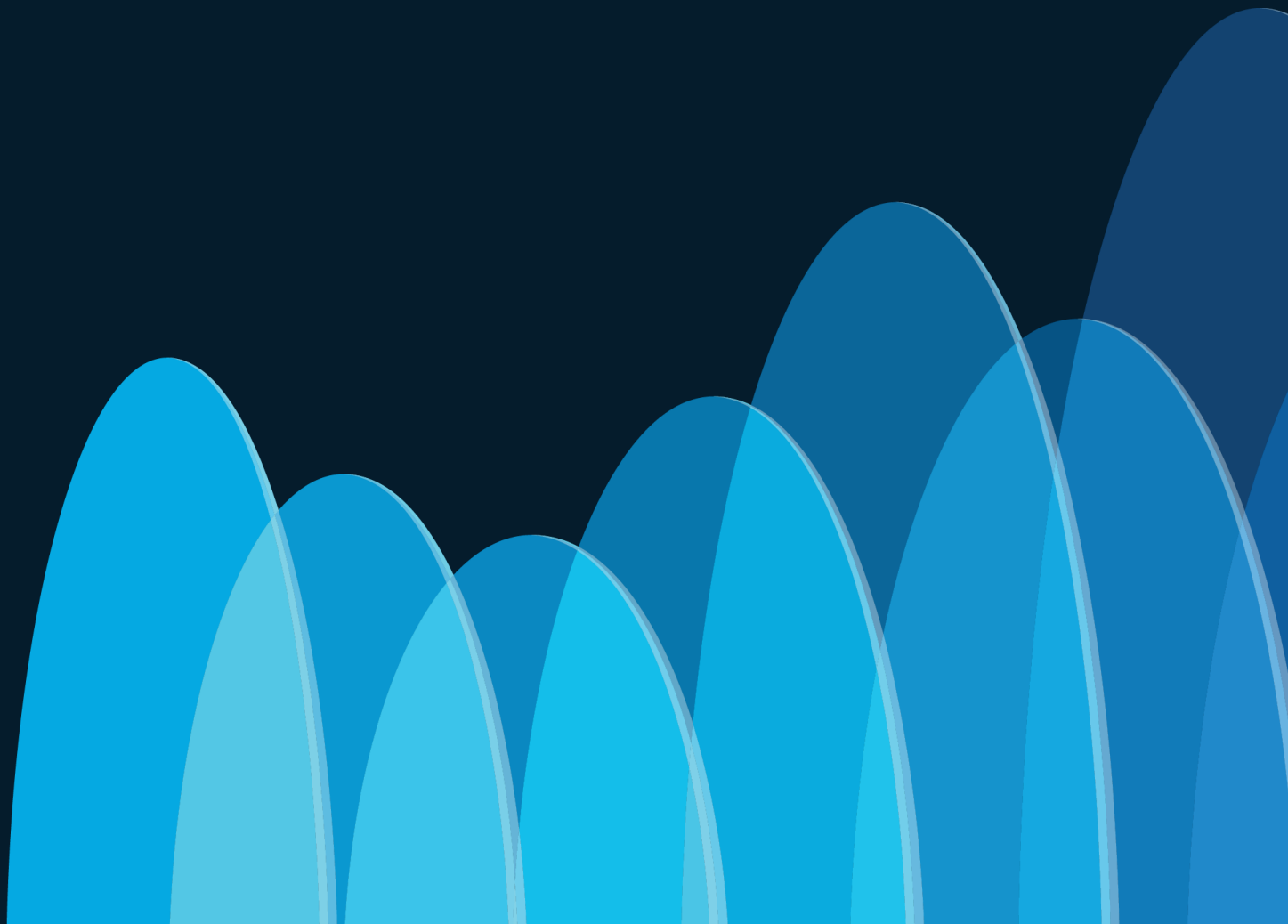
Targeted Flow Analysis



Targeted Flow Analysis and Enforcement

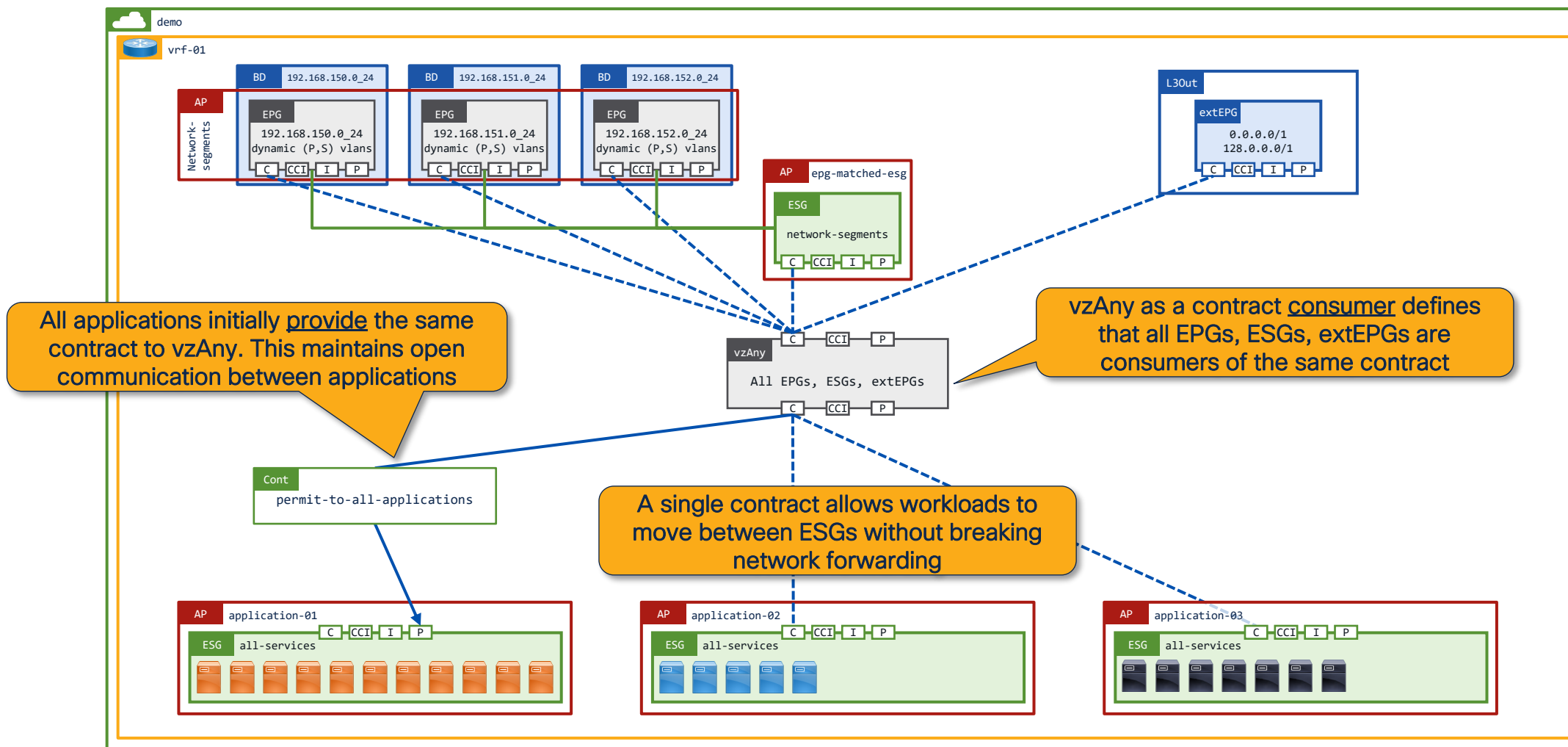


Tightening Security...



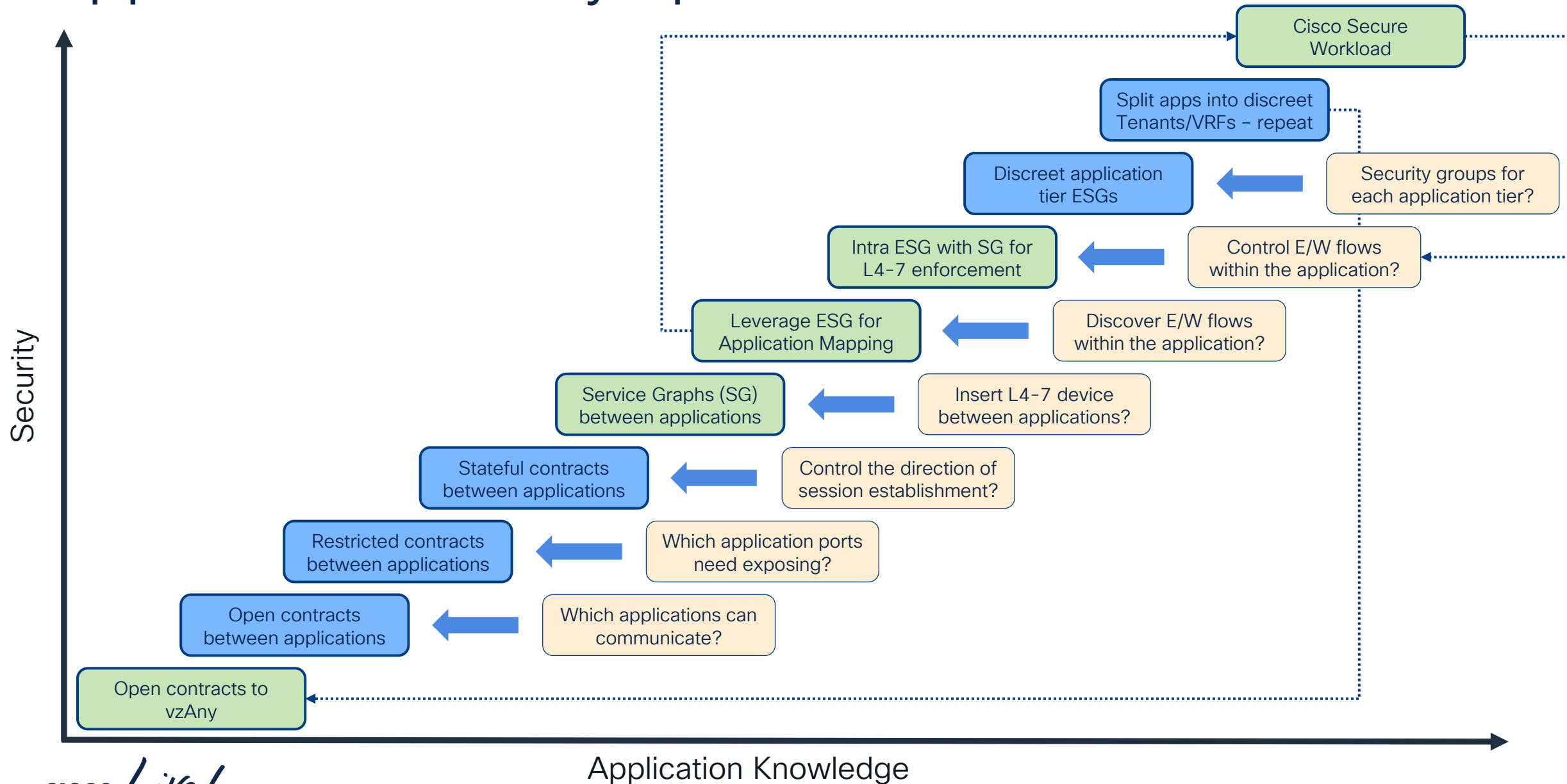
Step 1: Assign Endpoints to the “correct” ESG...

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



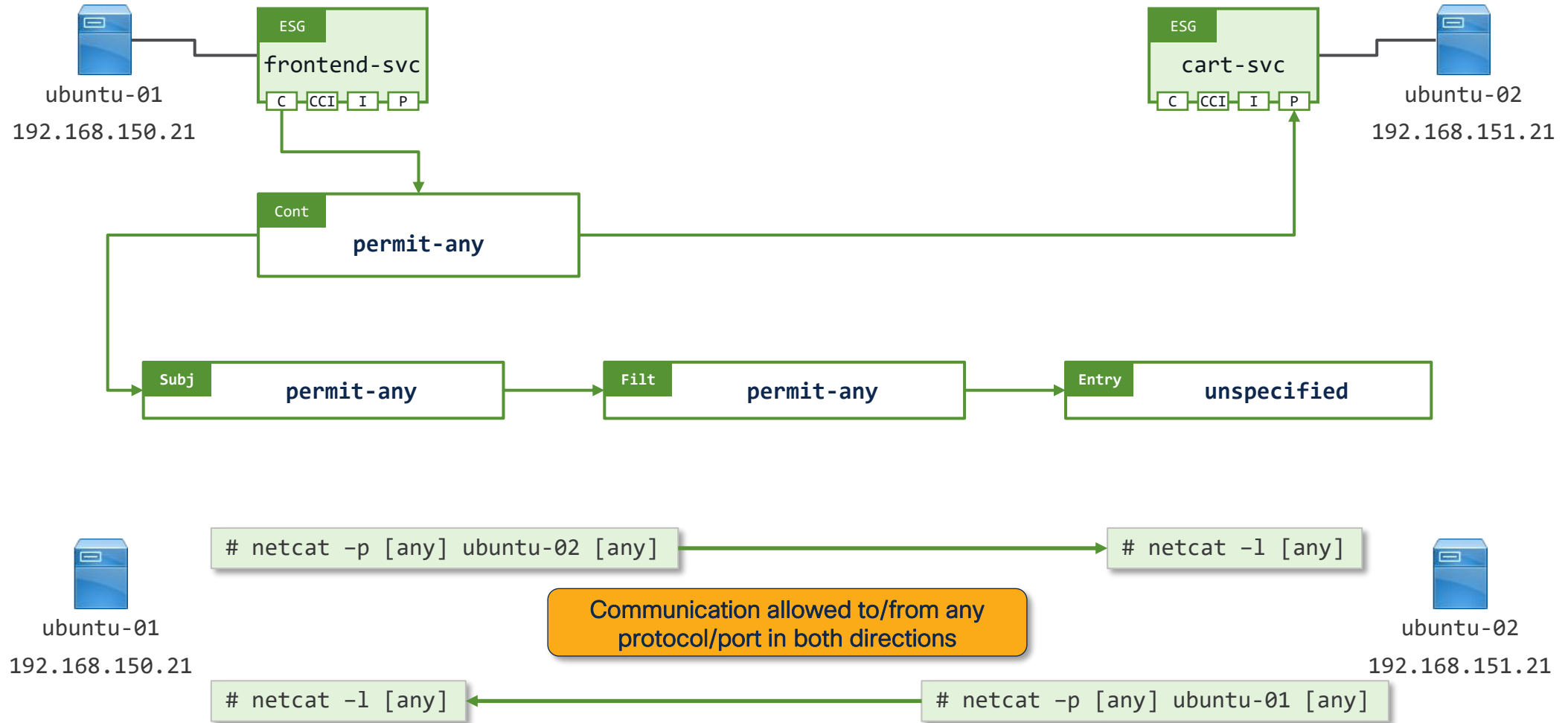
Step 2: Decide how to tighten security...

Application security options...



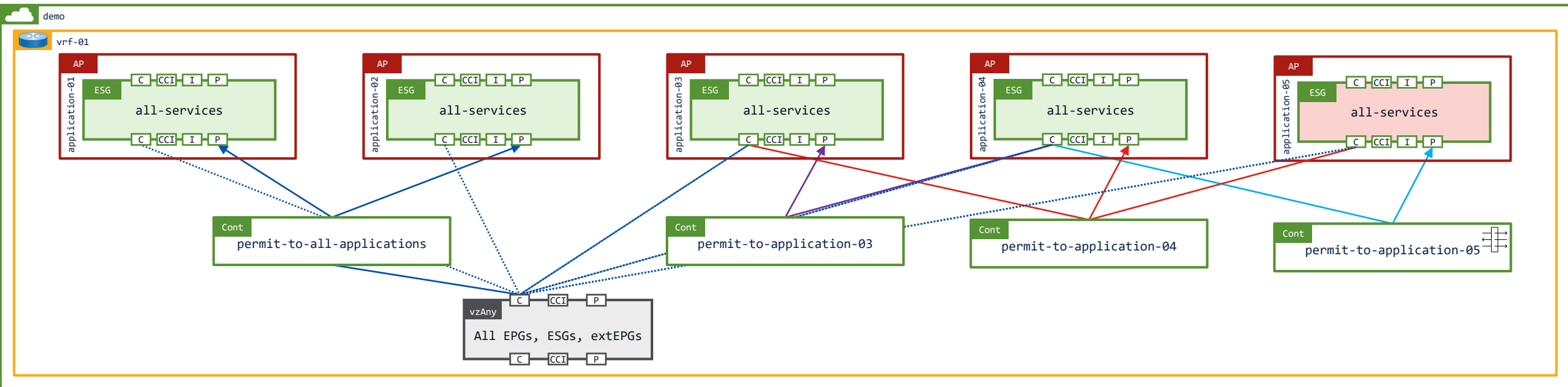
Remember this from a little earlier...

permit any/any



**Exercise caution when
using vzAny....!**

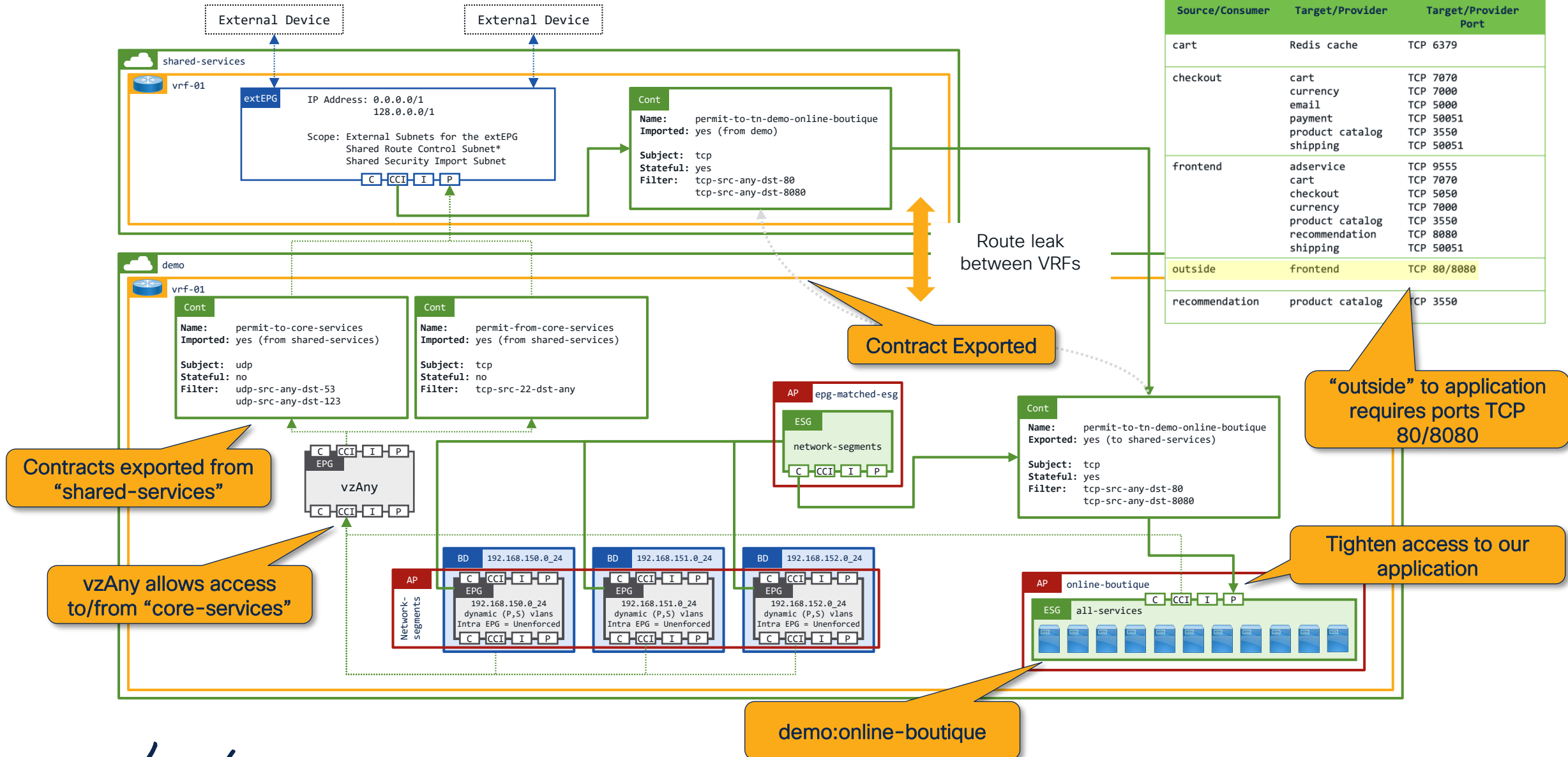




Consumer	Contract	Filter	Provider	Notes
vzAny (all EPGs/ESGs/extEPGs)	permit-to-all-applications	permit-src-any-dst-any	application-01	vzAny with permit-src-any-dst-any allows bi-directional communication on any port between all applications
vzAny (all EPGs/ESGs/extEPGs)	permit-to-all-applications	permit-src-any-dst-any	application-02	vzAny with permit-src-any-dst-any allows bi-directional communication on any port between all applications
application-04	permit-to-application-03	permit-src-any-dst-any	application-03	Bi-directional communication on any port between application-04 and application-03
application-03 application-05	permit-to-application-04	permit-tcp-src-any-dst-443	application-04	Communication from application-03 and application-05
application-04	permit-to-application-05 (Service graph to FTD for inter and intra application flows)	permit-src-any-dst-any	application-05	Bi-directional communication on any port via firewall between application-04 and application-05

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

Tighten access to our online-boutique application...



Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

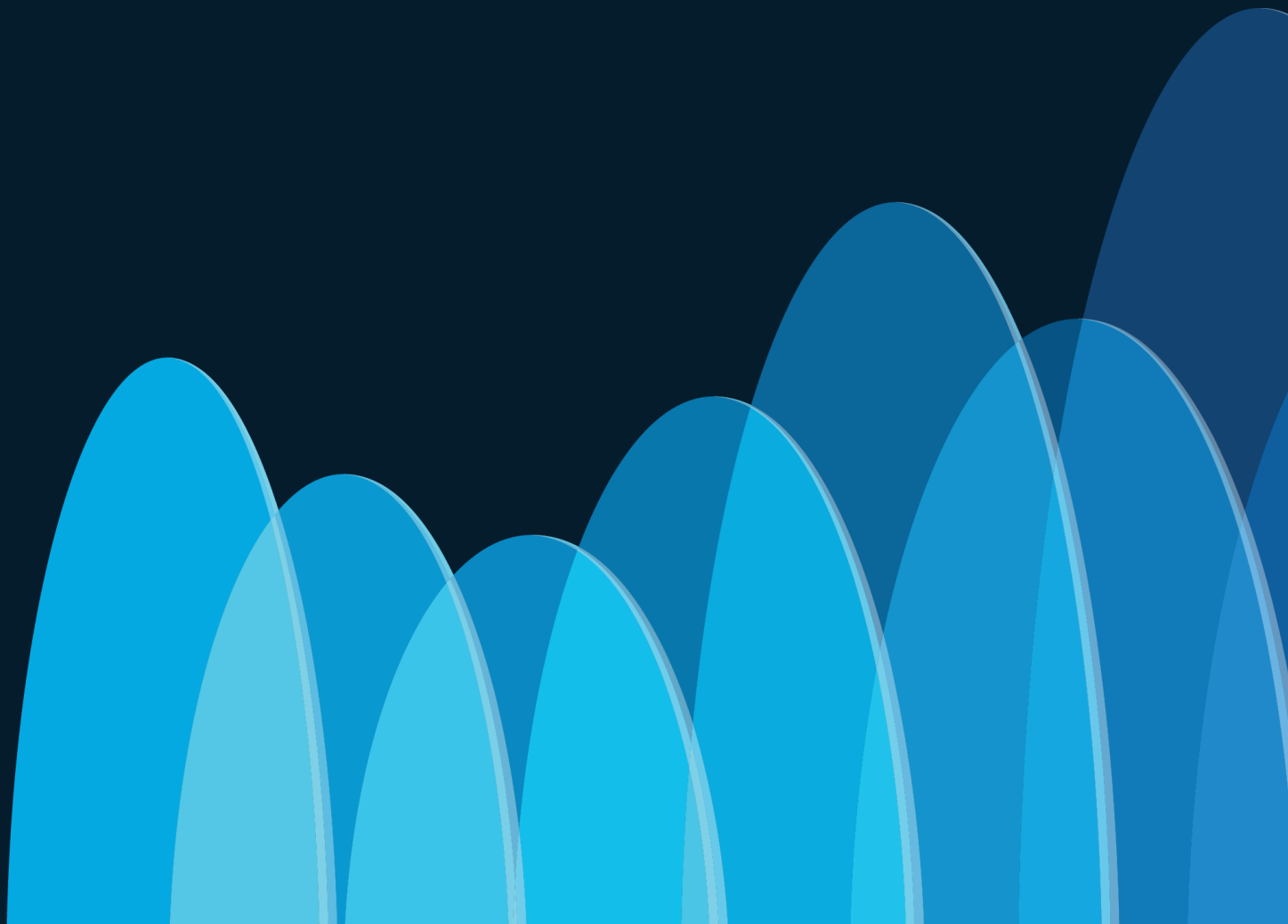
Understanding ACI security...

External Connectivity...

Increasing Security...

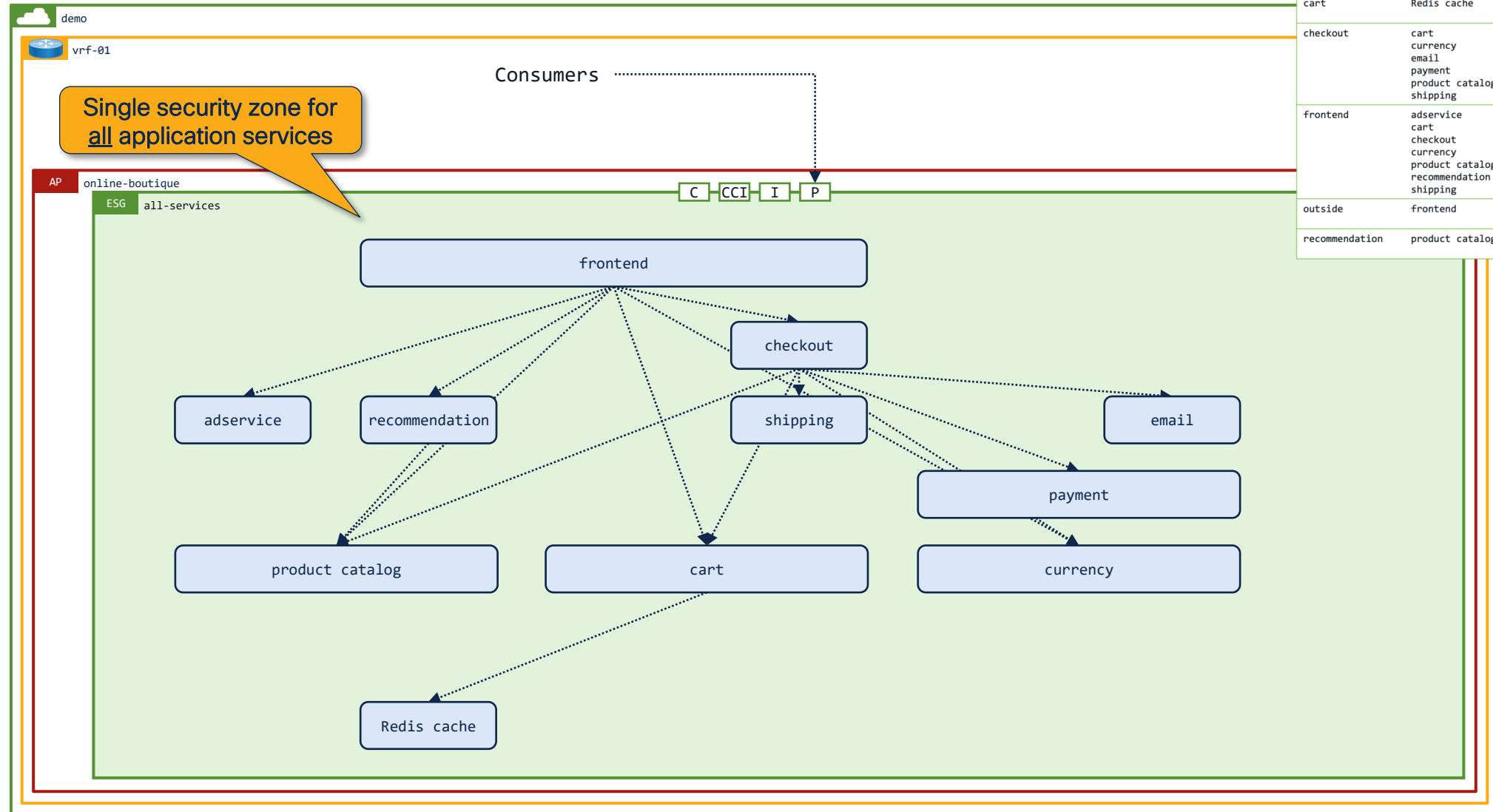
Automation Blueprints...

Wrapping up...



Application tiers across subnets

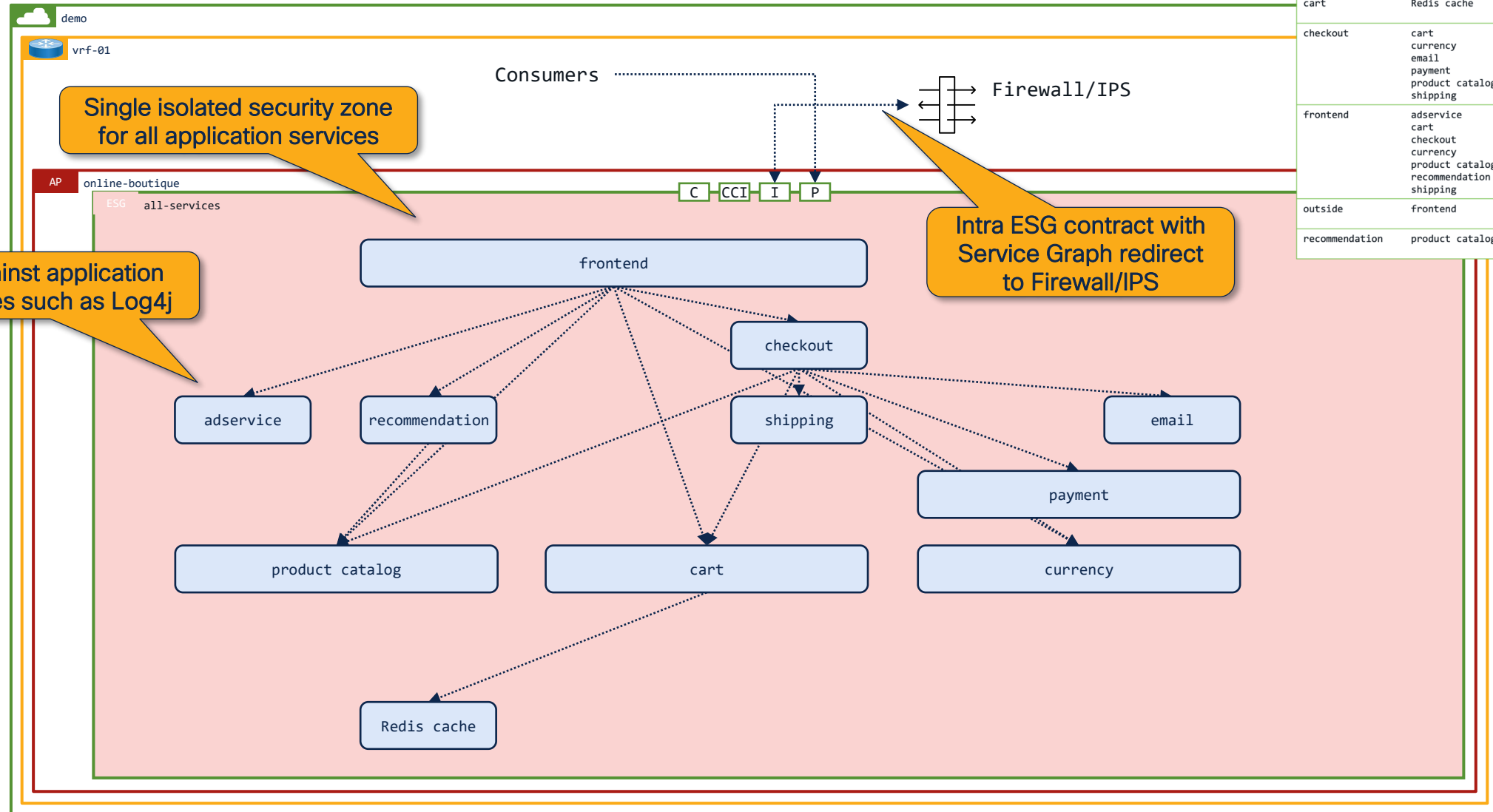
Application Centric Blueprint #1 – ESG “wrapper” for all services



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

Application tiers across subnets

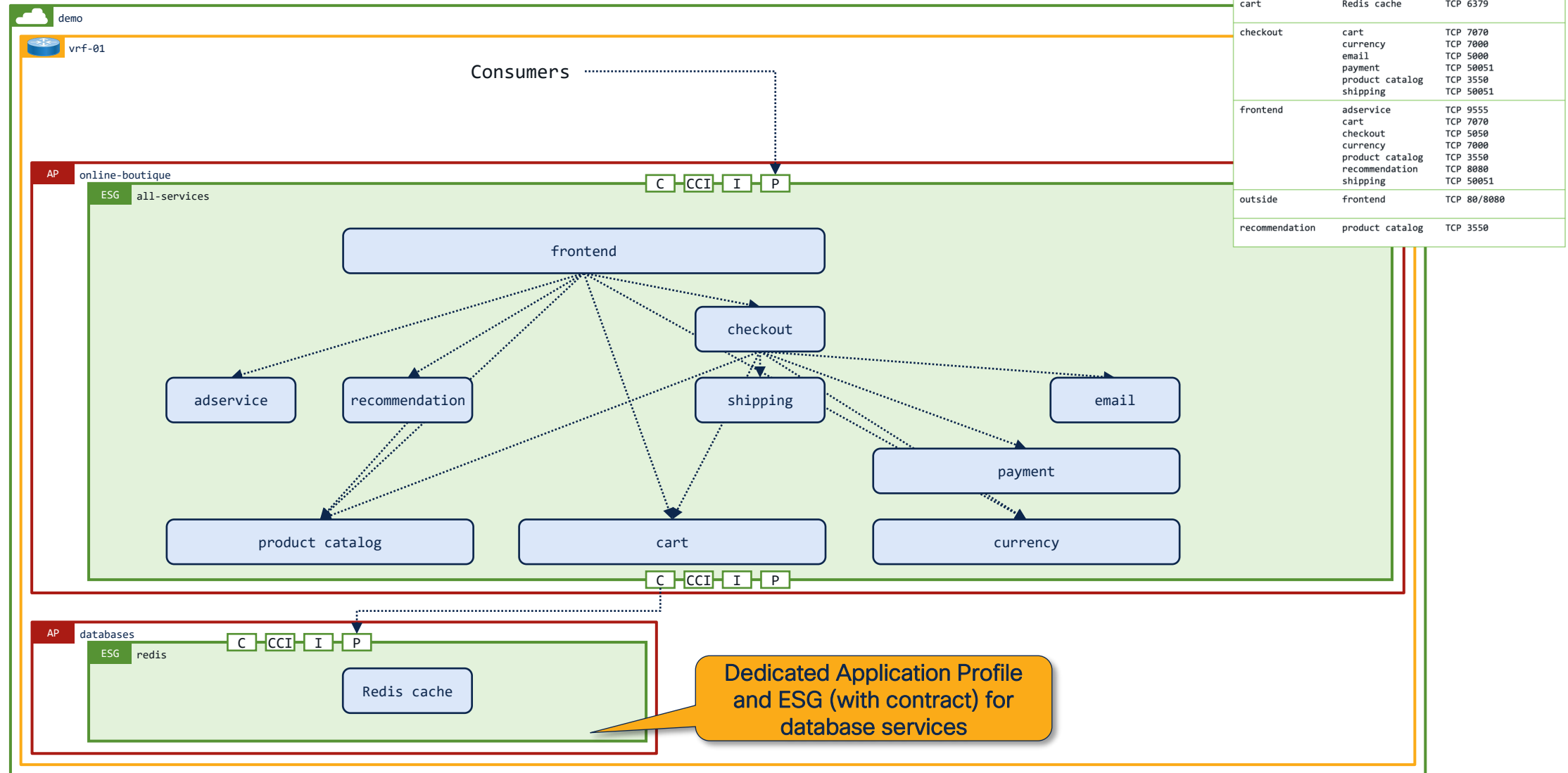
Application Centric Blueprint #2 – Intra ESG Isolation



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

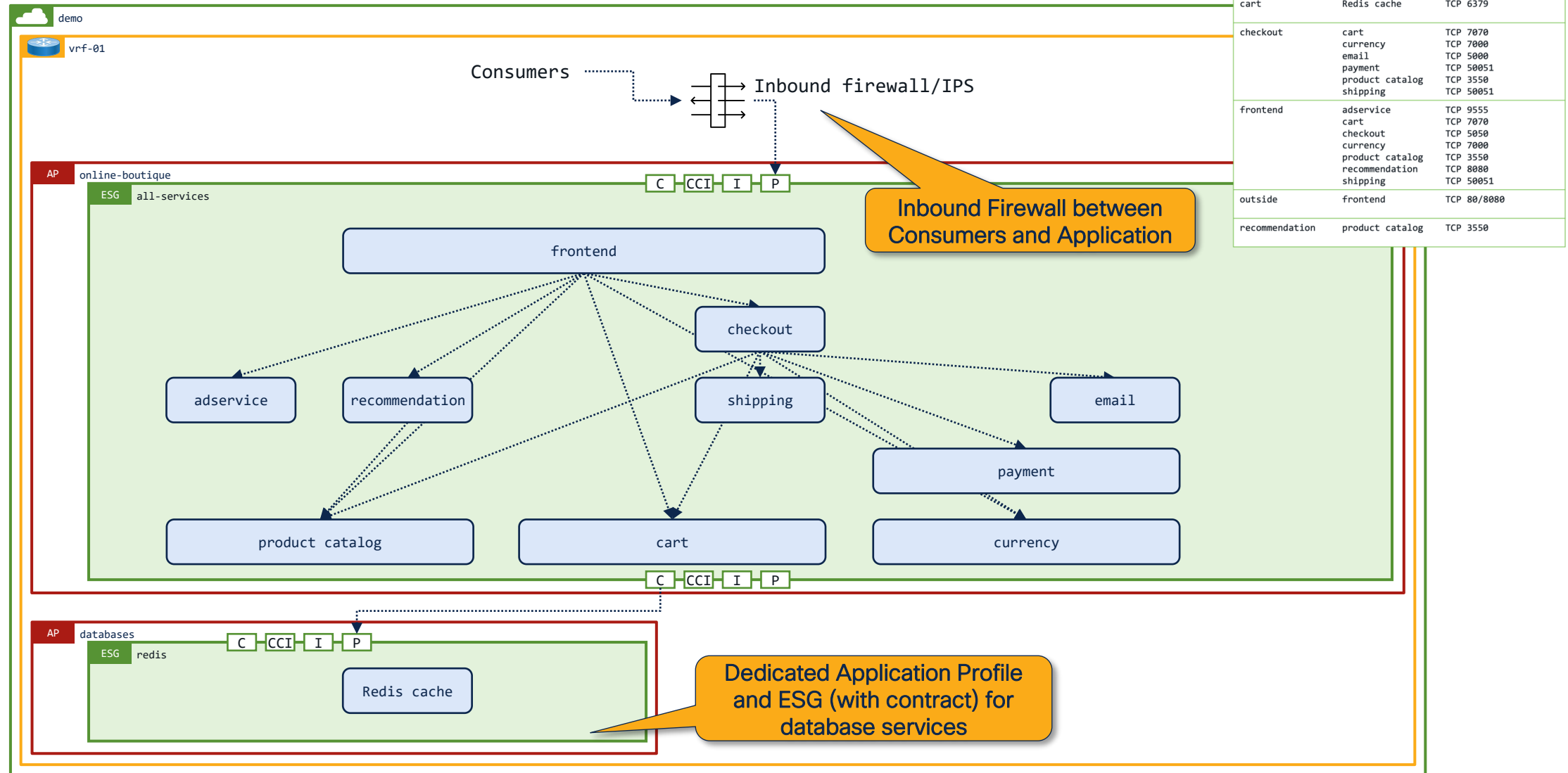
Application tiers across subnets

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



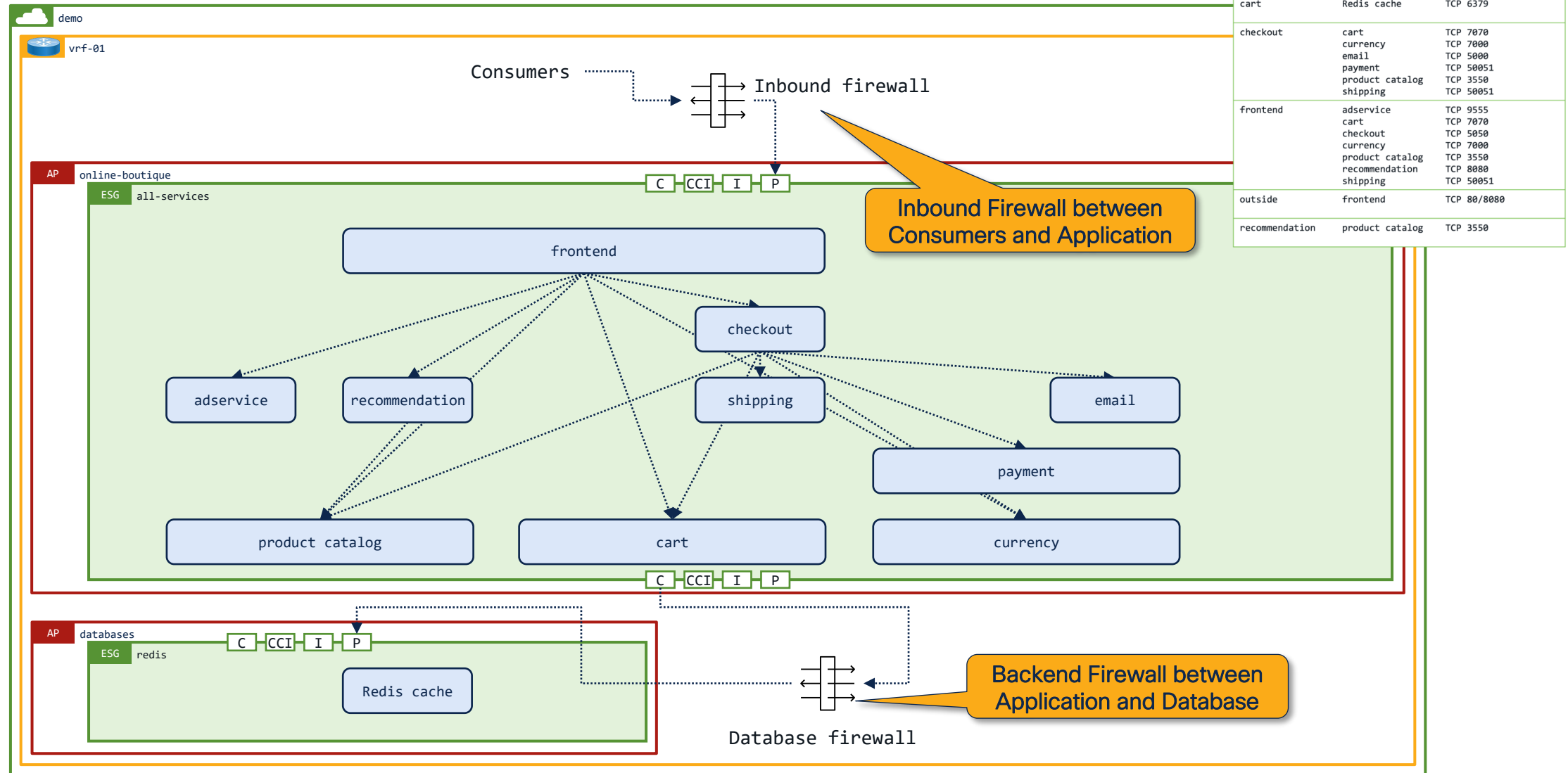
Application tiers across subnets

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



Application tiers across subnets

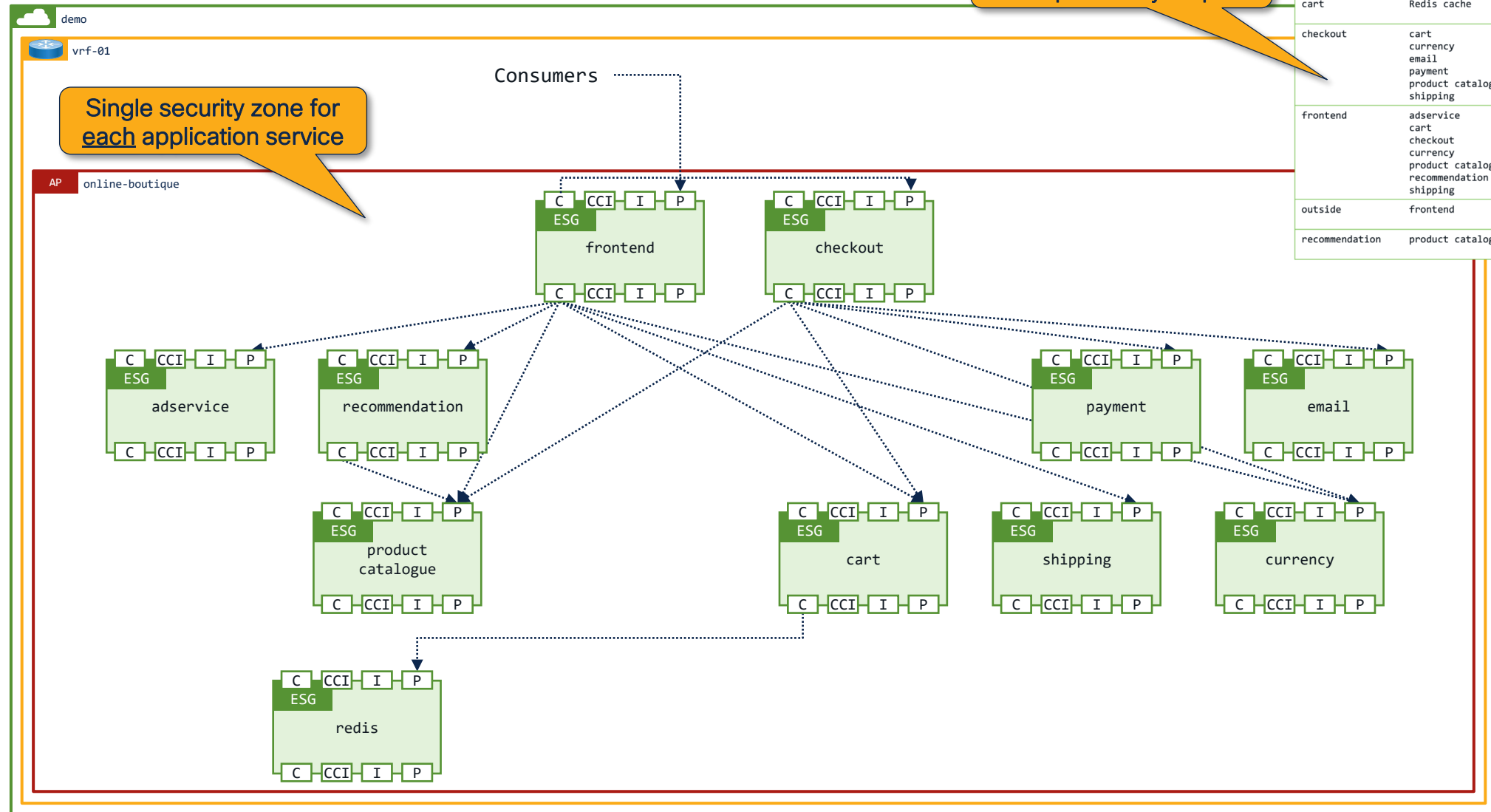
Application Centric Blueprint #5 – Inbound firewall/IPS + backend firewall/IPS



Application tiers across subnets

Application Centric Blueprint #6 – ESG per application tier

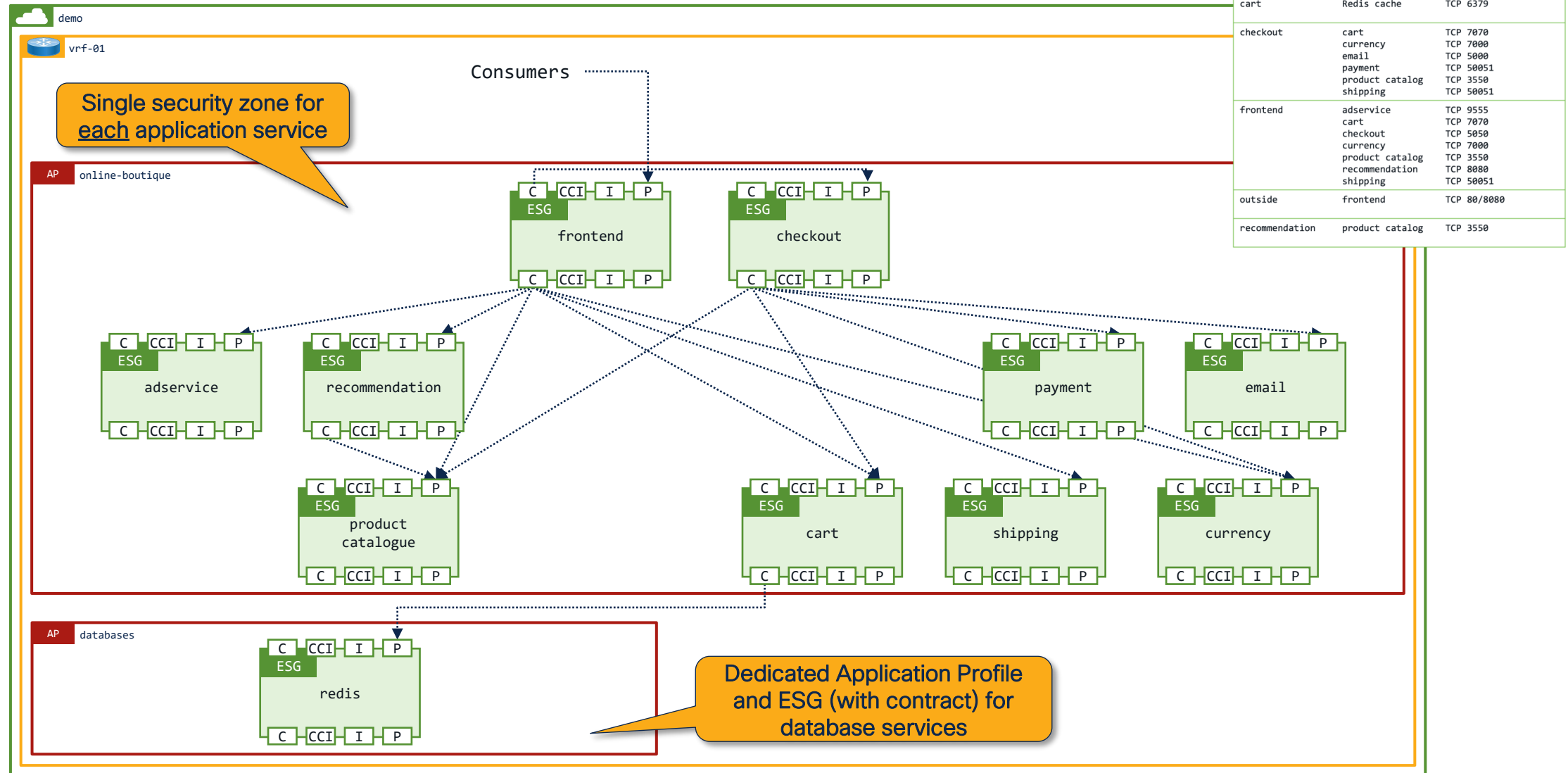
Requires application dependency map



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
recommendation	recommendation	TCP 8080
	shipping	TCP 50051
outside	frontend	TCP 80/8080
recommendation	product catalog	TCP 3550

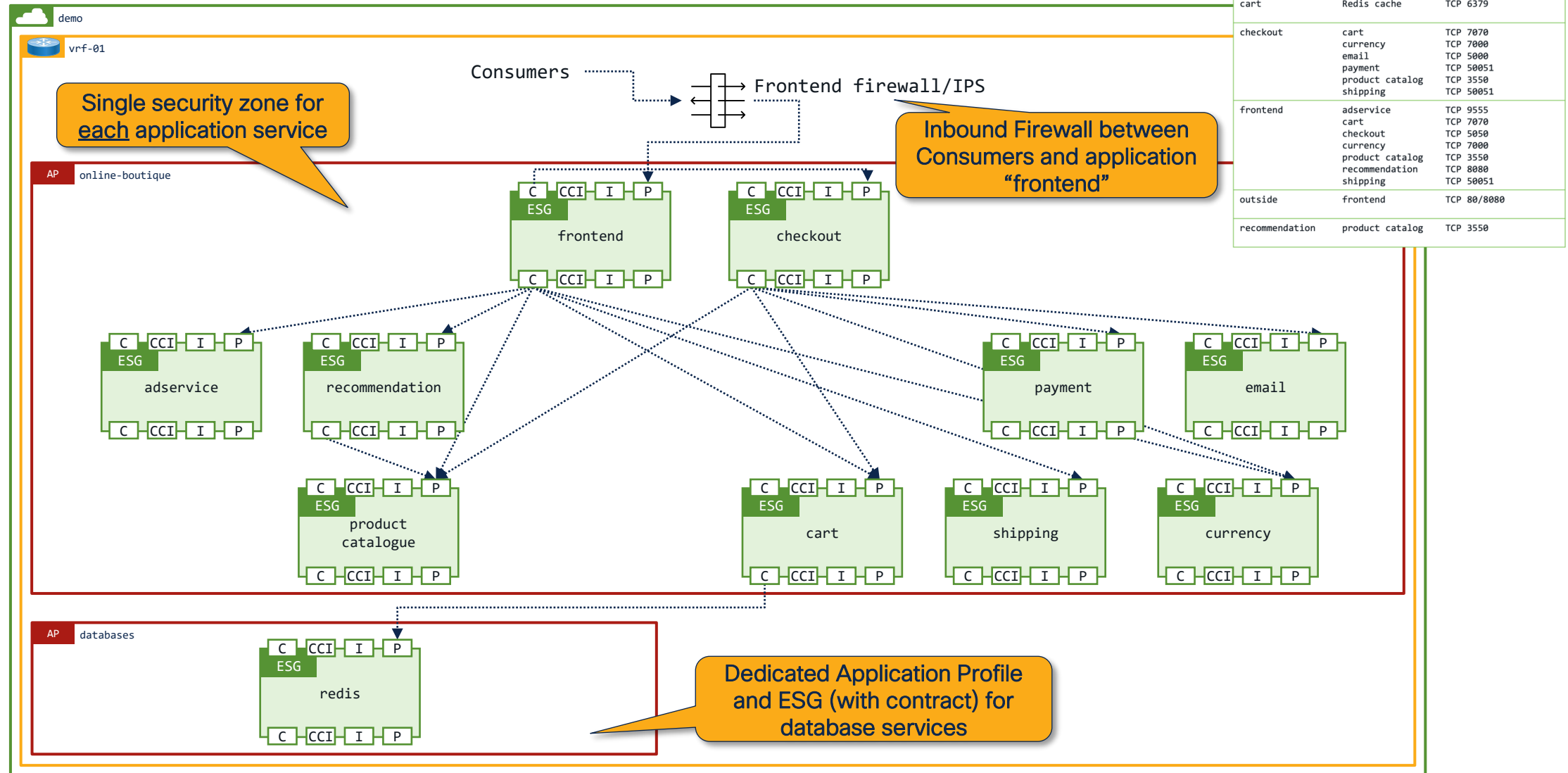
Application tiers across subnets

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



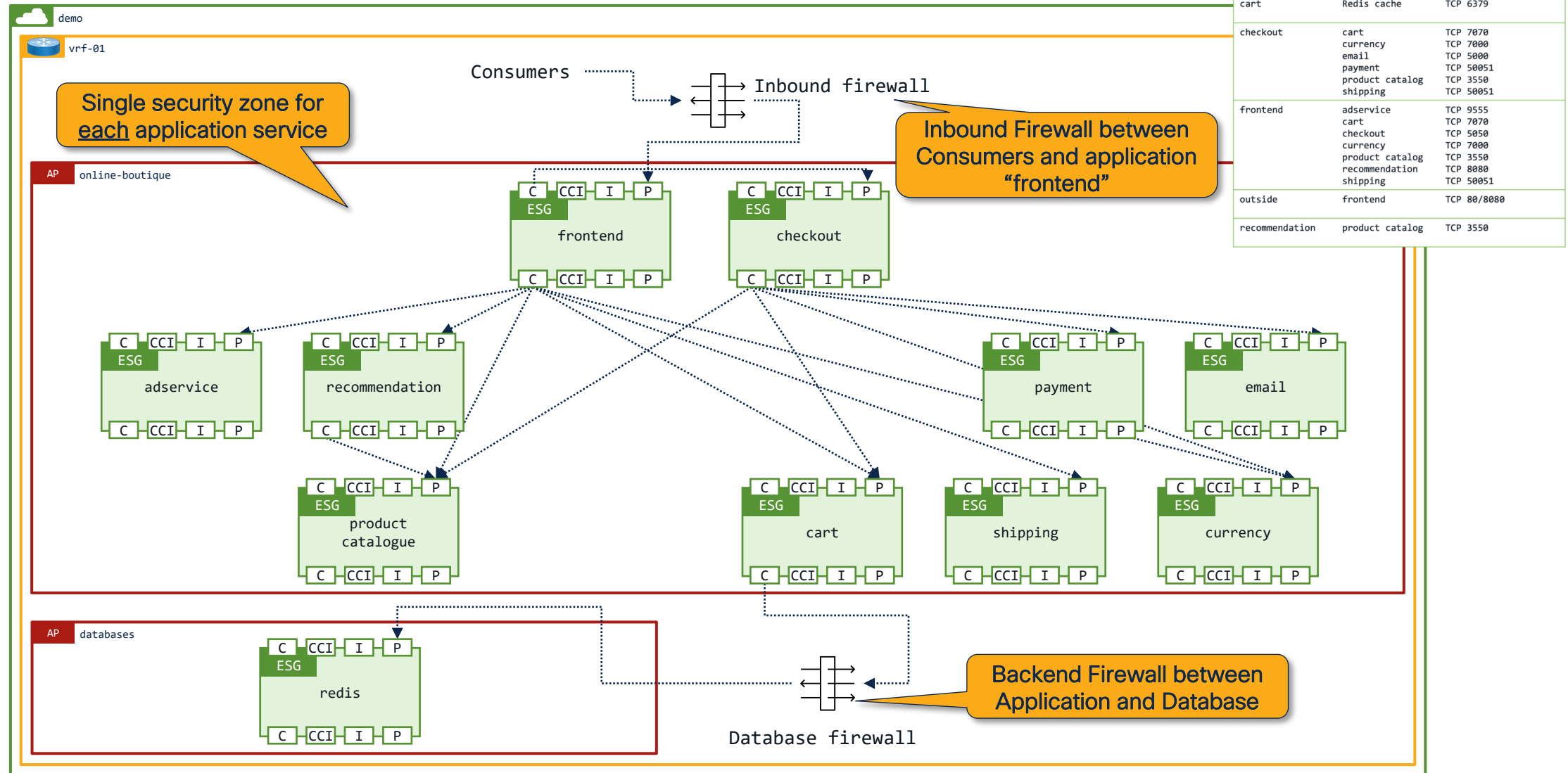
Application tiers across subnets

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



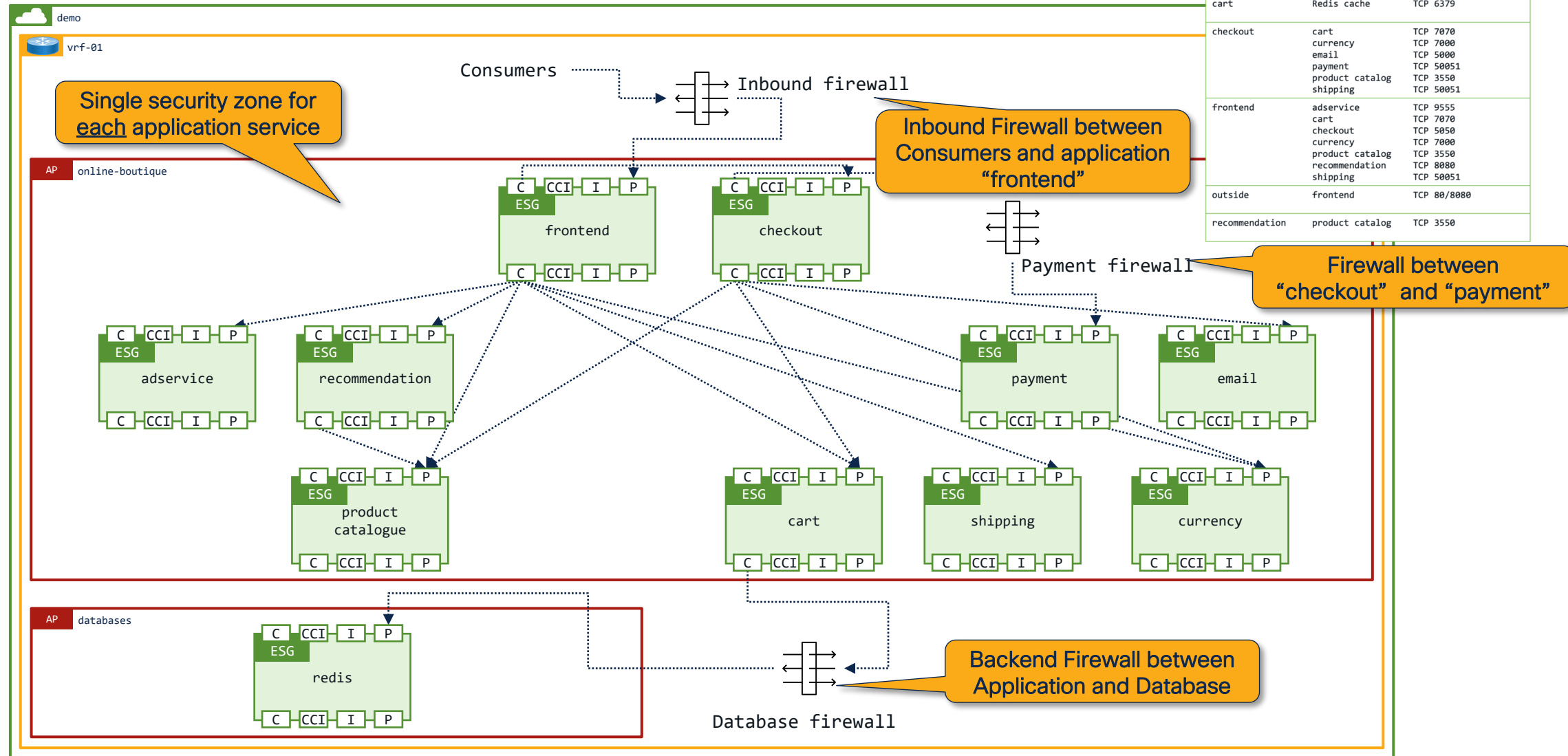
Application tiers across subnets

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



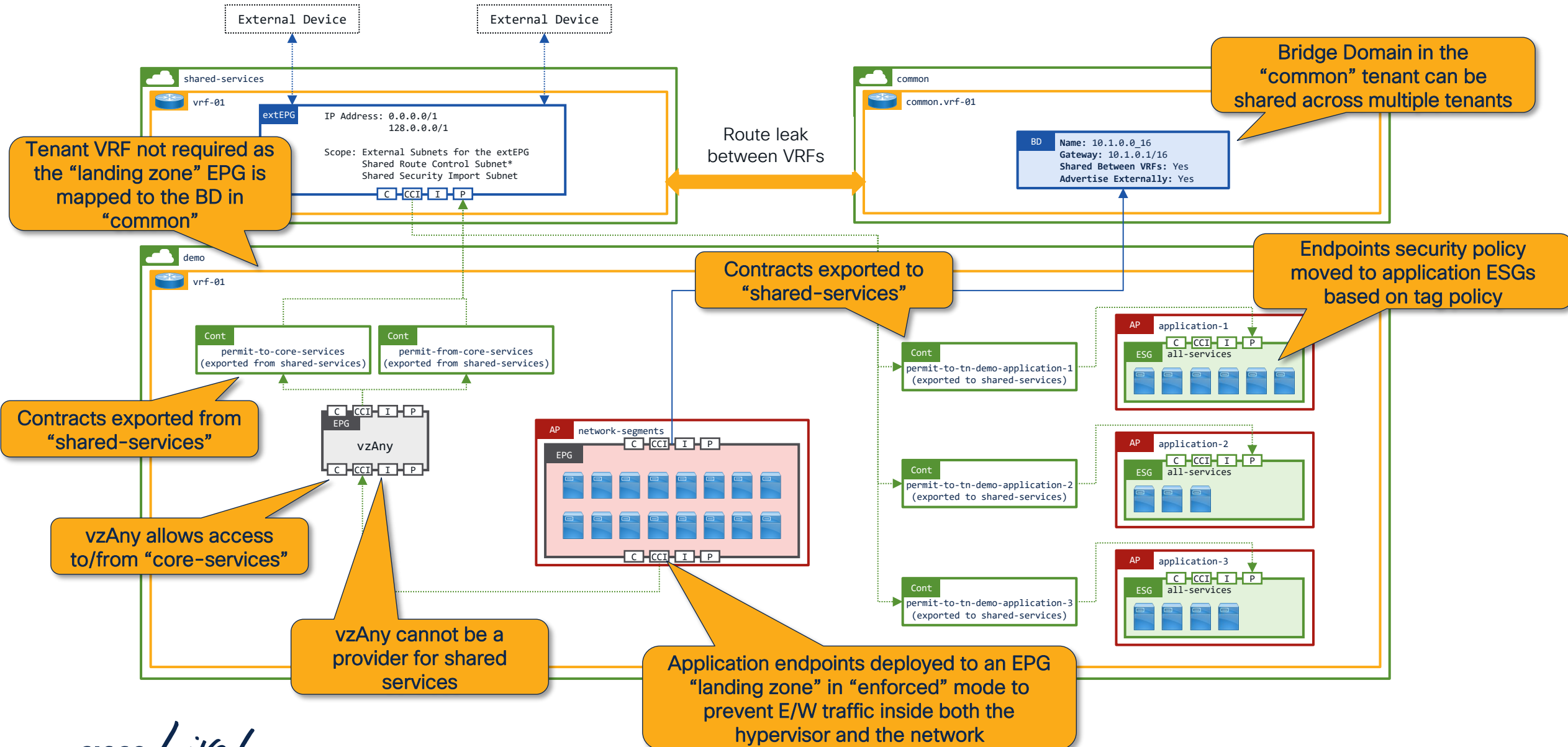
Application tiers across subnets

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

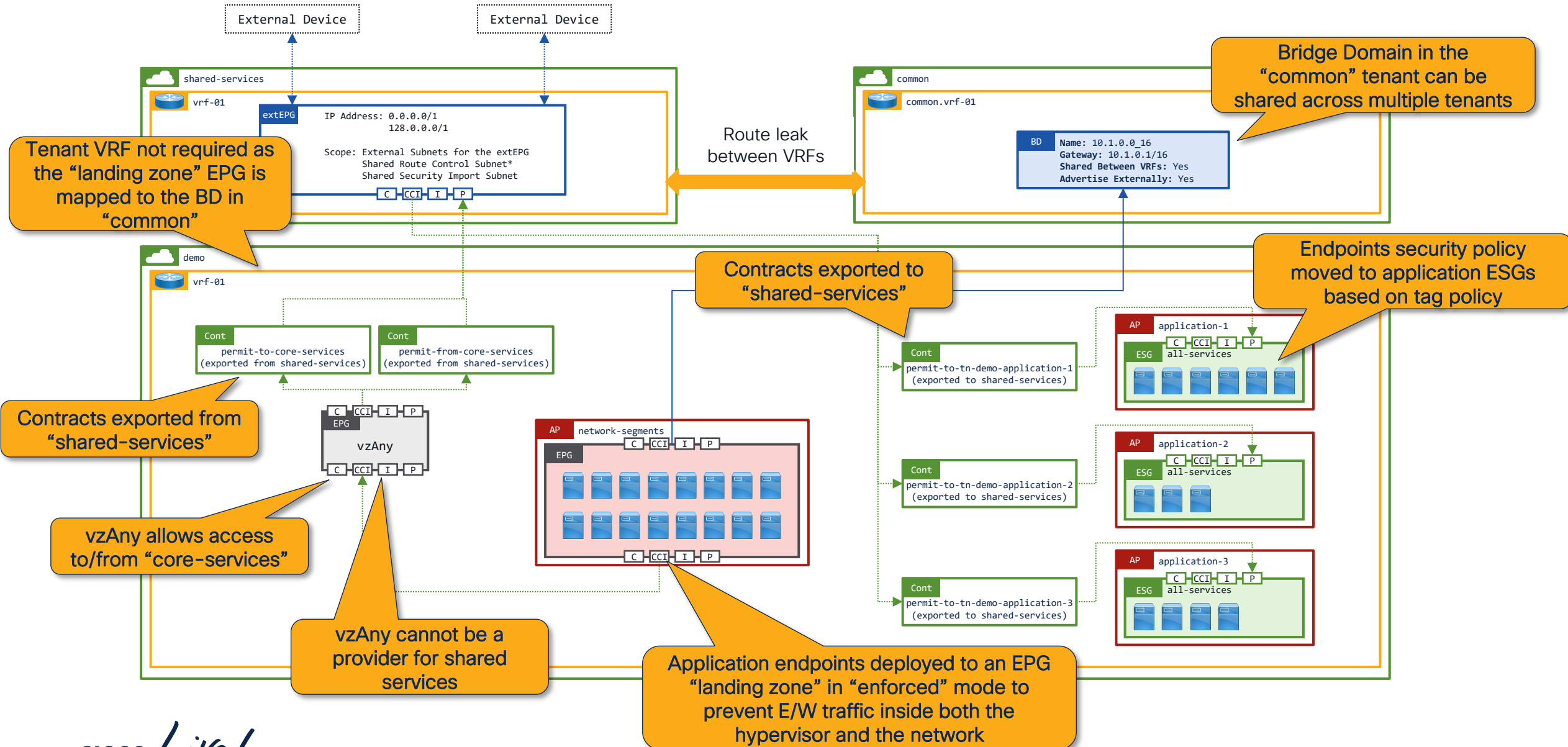


The ultimate aim is to provide a fully consumable fabric where resources are automated on demand...

Example Internal Private Cloud Design – shared subnet(s)



Example Internal Private Cloud Design – Auto Cleanup Isolation



Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

Understanding ACI security...

External Connectivity...

Increasing Security...

Automation Blueprints...

Wrapping up...

Select one or more Design Patterns...

Carefully consider the use of:

- Tenant “common”
- 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 in a shared model](#)

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

Getting started resources

- Visual Studio Code with extensions
 - Yaml
 - Indent Rainbow
 - Hashi Terraform
- <https://netascode.cisco.com/solutions/aci/terraform/overview>
- <https://developer.cisco.com/docs/nexus-as-code/introduction/>
- <https://github.com/netascode/terraform-aci-nac-aci/tree/main>
- <https://github.com/netascode/nac-aci-simple-example>
- <https://github.com/netascode/nac-aci-comprehensive-example>
- <https://github.com/spsharman/CiscoLive2024>
- <https://github.com/spsharman/aci-prod>
- <https://github.com/spsharman/aci-dev-01>
- <https://tl10k.dev/categories/terraform/nexus-as-code-architecture/>

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 ^ 🔍

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 (LABDCN-2287) in the World of Solutions...

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education

LABDCN-2287 – ACI Segmentation...
BRKDCN-2634 – Deploying EVPN G/W...
BRKDCN-2673 – Nexus-as-Code...
BRKDCN-2910 – Upgrading ACI...
BRKDCN-2949 – ACI Multi-Pod...
BRKDCN-2980 – ACI Multi-Site...
BRKDCN-3900 – ACI Forwarding...
BRKDCN-3982 – ACI PBR Deep Dive...

- 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

Contact me at: ssharman@cisco.com



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC