

CISCO *Live!*

Let's go



The bridge to possible

ACI – “not just another network...”

Steve Sharman – Technical Solutions Architect

CISCO *Live!*

BRKDCN-2984

Agenda

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

Why are you here...?

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

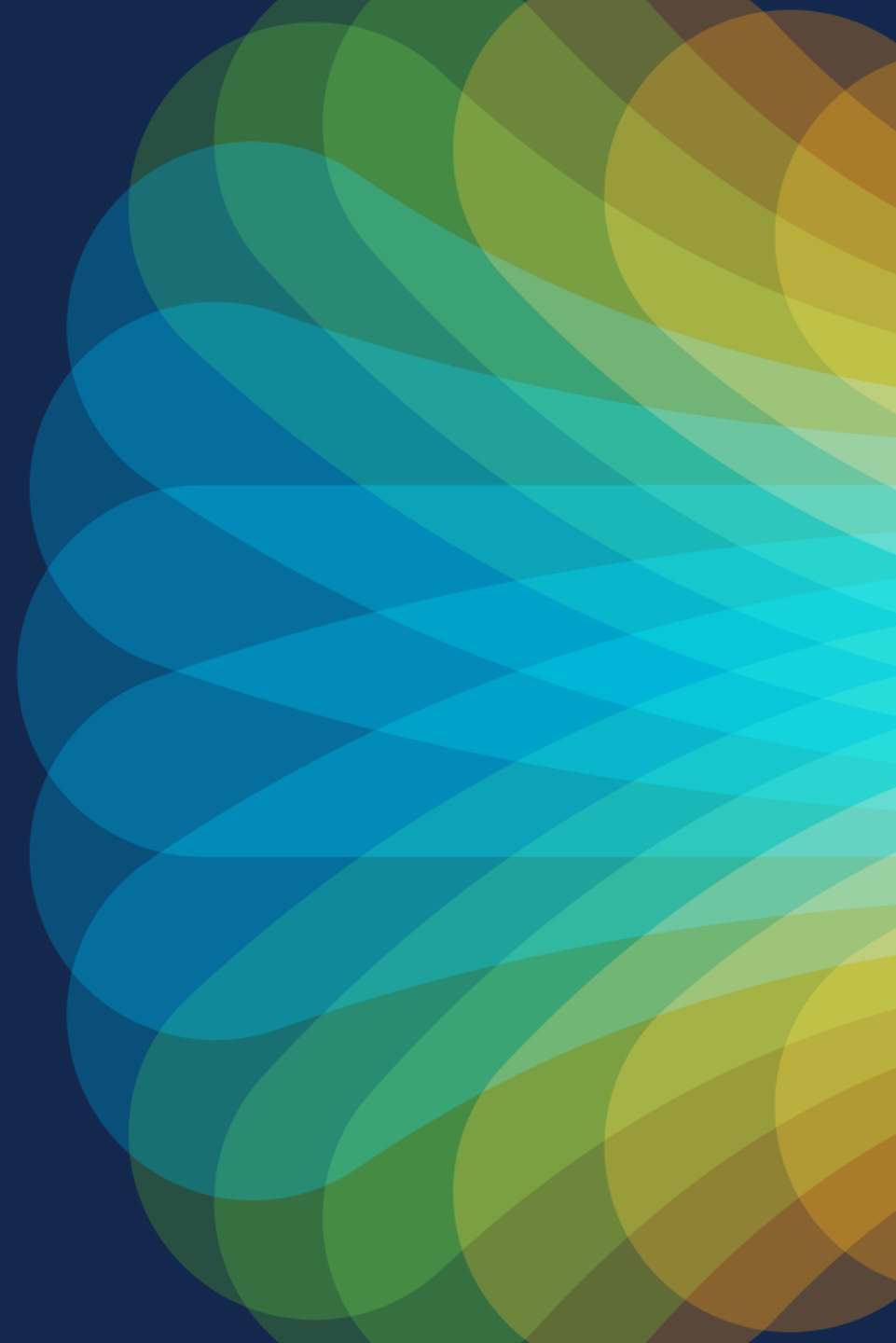
There are thousands of customers globally who have successfully deployed ACI fabrics and operate them as "just another network", but what if you could operate your ACI fabric as programmable private cloud infrastructure?

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...

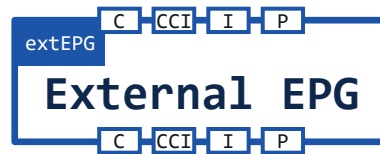
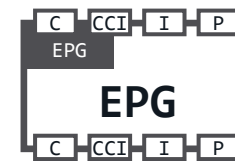
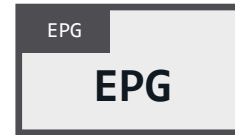


There are lots (and lots) of details in this presentation, please download through the [Cisco Live app](#).

Well unless you have binoculars with you...!



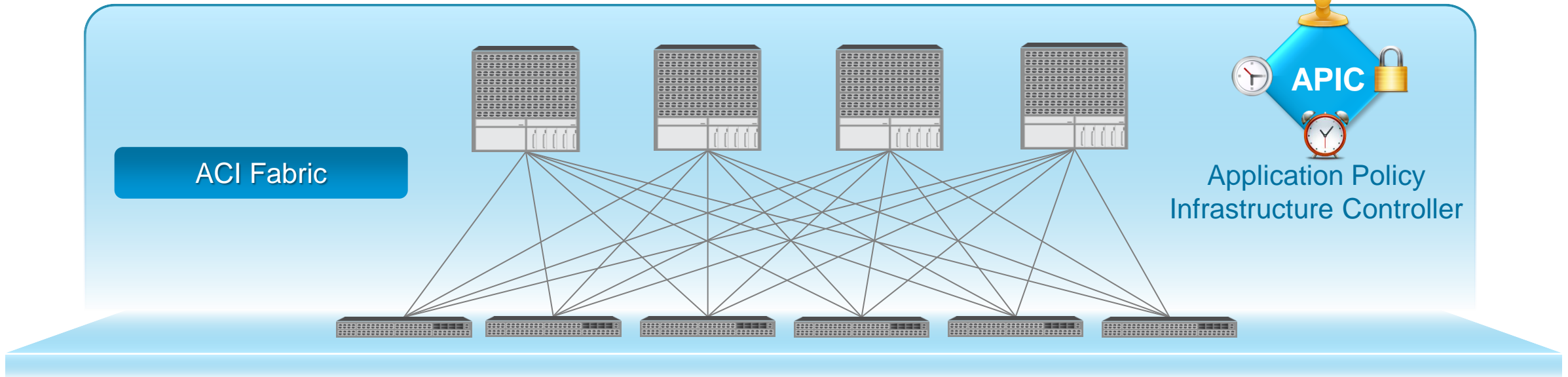
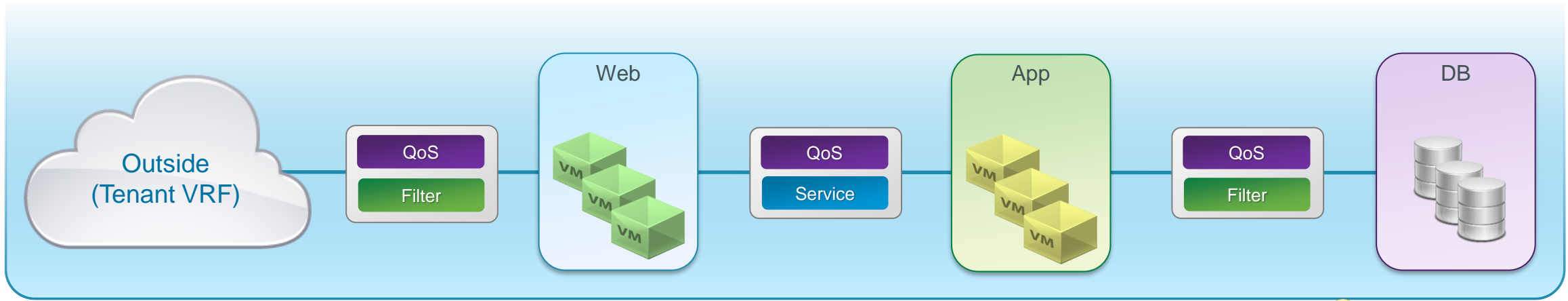
Icons



*arrows indicate expected direction of connection 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


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 #2ZVFJ3GM2N | |
| Quantity: 1 | | \$13.79 |
|  | Cabana Shorts SKU #OLICESPC7Z | |
| 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

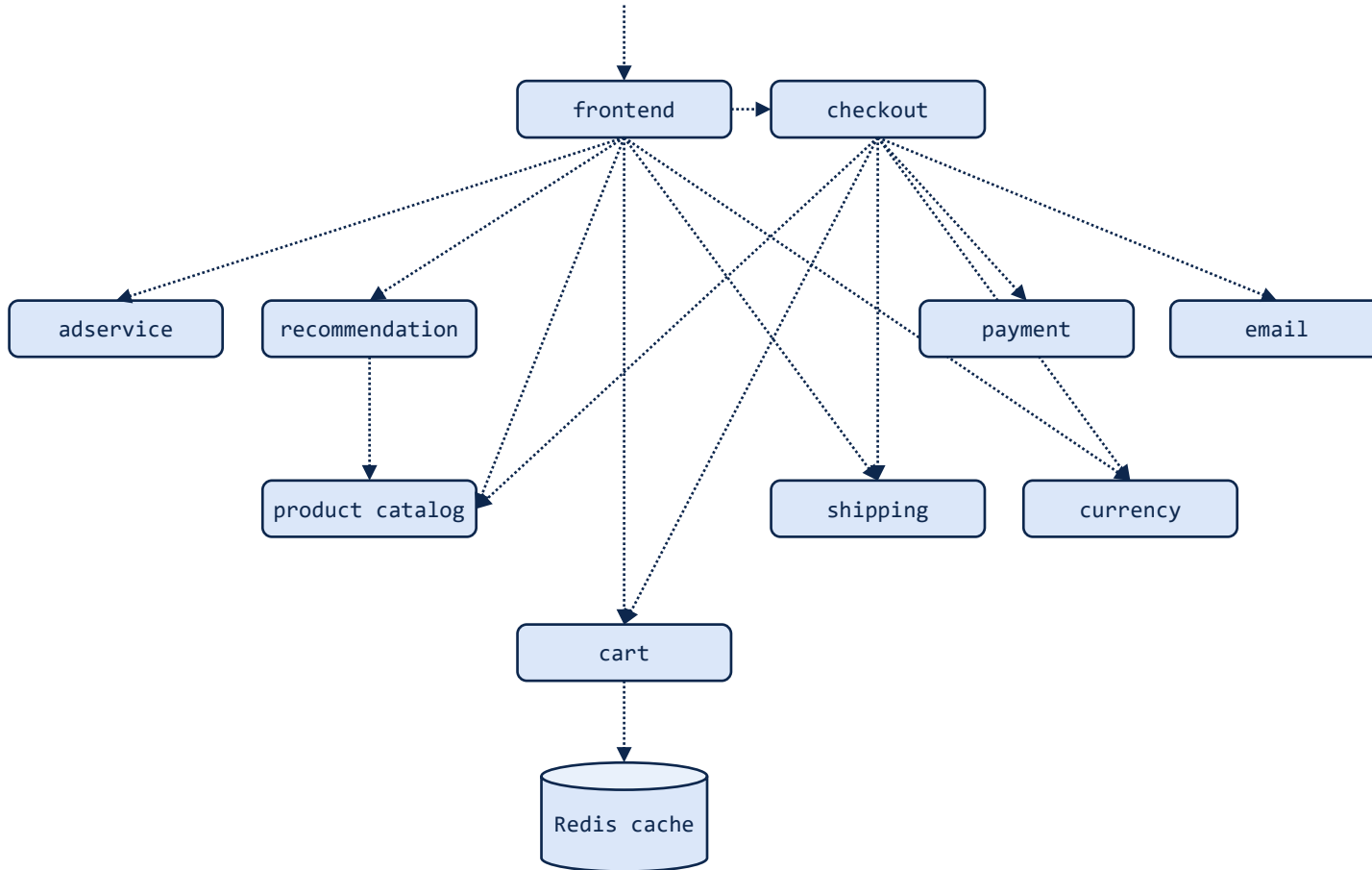
Year
2023

CVV
...

Place Order

Online Boutique

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

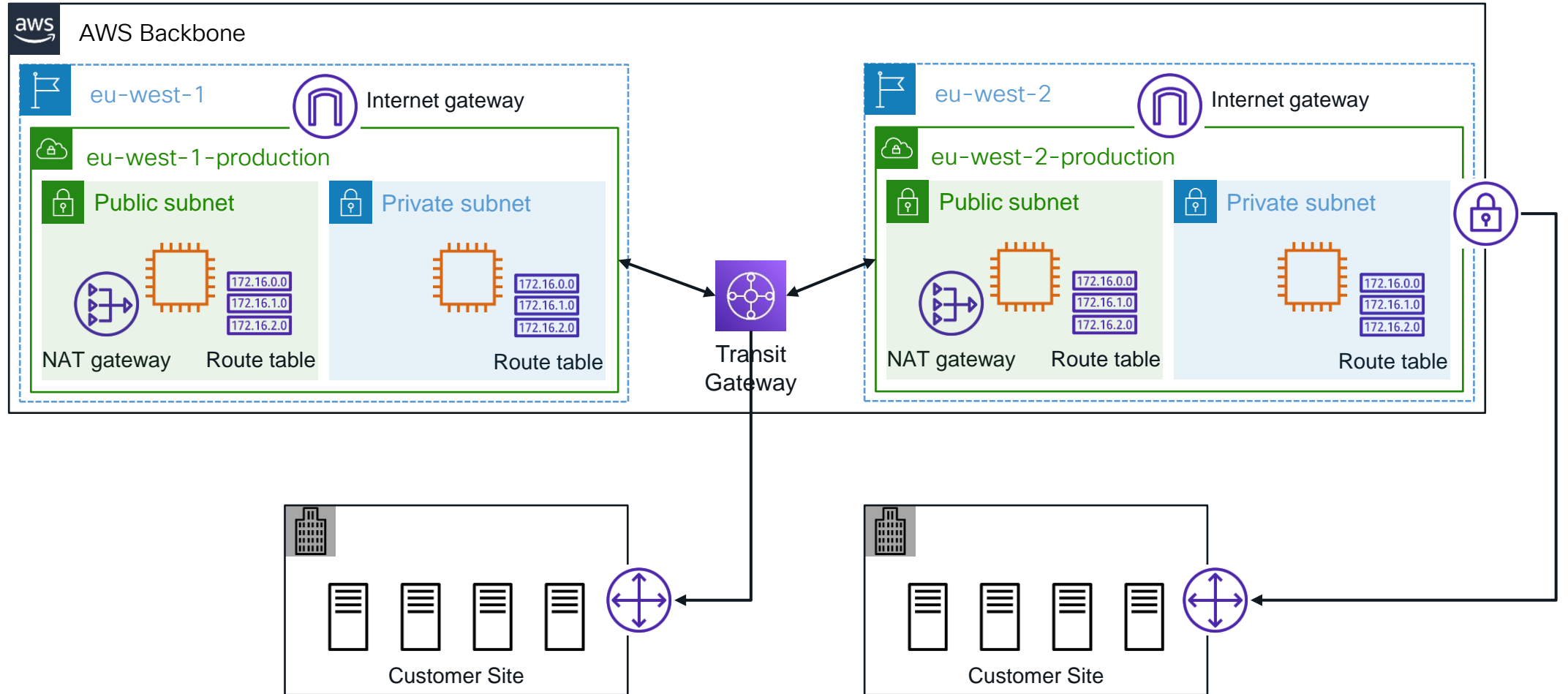


| Source/Consumer | Target/Provider | Target/Provider Port |
|-----------------|-----------------|----------------------|
| cart | Redis cache | TCP 6379 |
| checkout | cart | TCP 7070 |
| | currency | TCP 7000 |
| | email | TCP 8080 |
| | payment | TCP 50051 |
| | product catalog | TCP 3550 |
| | shipping | 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 adaptations). 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. |

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

Google Cloud

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 discovered 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

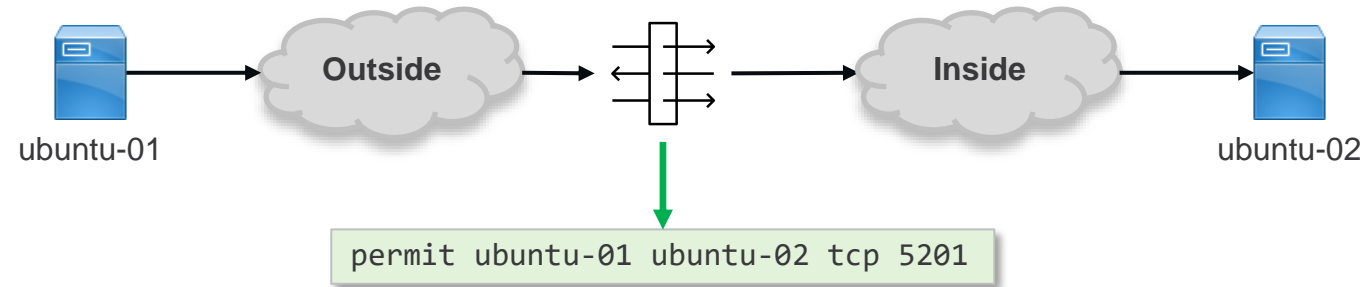
A cloud operating model succeeds best when there is a new organisational culture...

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 a physical firewall which typically becomes a throughput 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



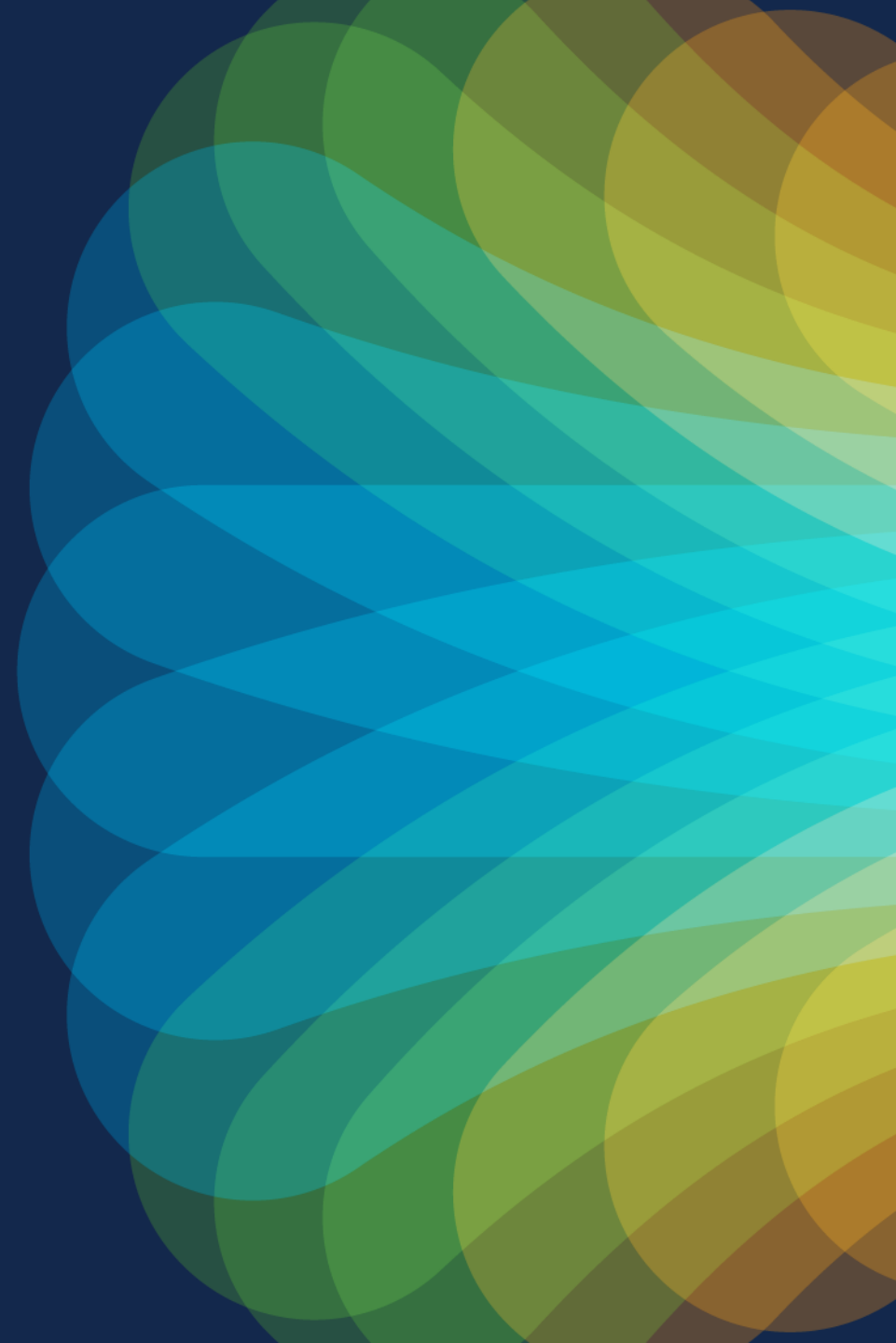
Single API Model for 100s of switches and 1000s of ports; cloud-like consumption model



Infrastructure as Code with Ansible and Terraform

Automation | Classification and Segmentation | Security

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 navigation icons. Below the search bar, there are tabs for "All", "Images", "Videos", "News", "Books", and "More". The search results show "About 157,000 results (0.48 seconds)". A featured snippet from <https://ipwithease.com> titled "Cisco ACI Network Centric vs Application Centric approach" is displayed. Below the snippet, 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 first result is from <https://community.cisco.com> titled "Difference between ACI network centric mode and application ...".

Google search results for "site:cisco.com Cisco ACI what is the difference between network cent". The search bar shows the query and navigation icons. Below the search bar, there are tabs for "All", "Images", "Videos", "News", "Books", and "More". The search results show "About 21,100 results (0.45 seconds)". The first result is from <https://community.cisco.com> titled "Difference between ACI network centric mode and application ...". The second result is from <https://community.cisco.com> titled "ACI network centric vs app centric - Cisco Community". The third result is from <https://www.cisco.com> titled "Cisco ACI - Application Centric Infrastructure". The fourth result is from <https://www.cisco.com> titled "Network Centric to ACI Centric Migration - Cisco". The fifth result is from <https://community.cisco.com> titled "Solved: ACI Network Centric to Application Centric Migration".

Getting with the times...



ChatGPT

As of my last knowledge update in January 2022, Cisco ACI (Application Centric Infrastructure) can operate in two primary modes: Application Centric Infrastructure (ACI) mode and Network Centric Infrastructure (NCI) mode. Let's explore the key differences between these two modes:

1. Application Centric Infrastructure (ACI) Mode:

- **Policy-Driven:** ACI mode is designed with an application-centric approach, where the network is configured and managed based on application requirements.
- **Application Network Profiles:** Administrators define Application Network Profiles (ANP) that encapsulate the requirements and policies of specific applications. This includes networking, security, and other relevant parameters.
- **Automation and Orchestration:** ACI mode emphasizes automation and orchestration. Policies are applied to the entire application infrastructure, allowing for faster deployment and adaptability to changing application needs.
- **Abstraction of Underlying Infrastructure:** ACI abstracts the underlying network infrastructure, enabling administrators to focus on defining and enforcing policies at the application level rather than dealing with specific network configurations.

2. Network Centric Infrastructure (NCI) Mode:

- **Network-Centric Policies:** NCI mode, on the other hand, is more aligned with traditional network-centric configurations. Network administrators can configure and manage the network using familiar networking concepts without the emphasis on application-centric policies.
- **Manual Configuration:** In NCI mode, administrators have more direct control over individual network components and configurations. This can involve manual configuration of networking elements such as VLANs, subnets, and access control lists (ACLs).
- **Familiarity for Network Administrators:** NCI mode is suitable for organizations where network administrators are more comfortable with traditional networking paradigms and want to maintain a higher degree of control over specific network details.

It's important to note that the capabilities and features of Cisco ACI can evolve with software updates and releases. Organizations should refer to the latest Cisco ACI documentation or consult with Cisco support to understand the current state of ACI modes and their capabilities. As of my last update, the information provided here gives a general overview of the concepts associated with ACI modes.



ChatGPT can make mistakes. Consider checking important information. 😊

Message ChatGPT...



ChatGPT can make mistakes. Consider checking important information.

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...

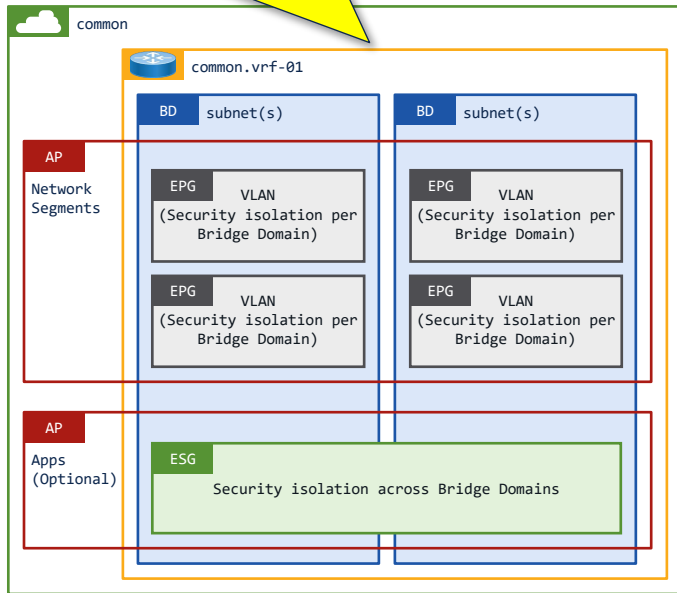
Where should
we start...?



Design Considerations...

Design Patterns

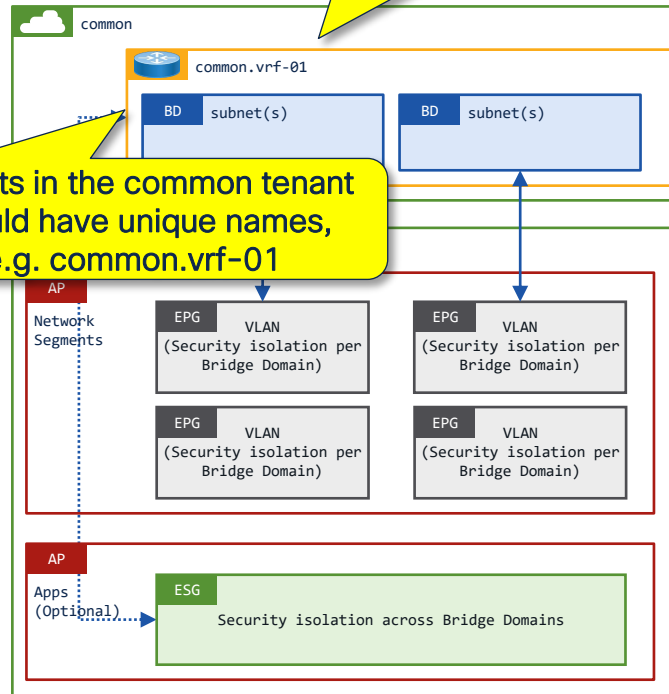
Everything in the "common" Tenant is not typically seen



Used for functions which are accessible from any Tenant

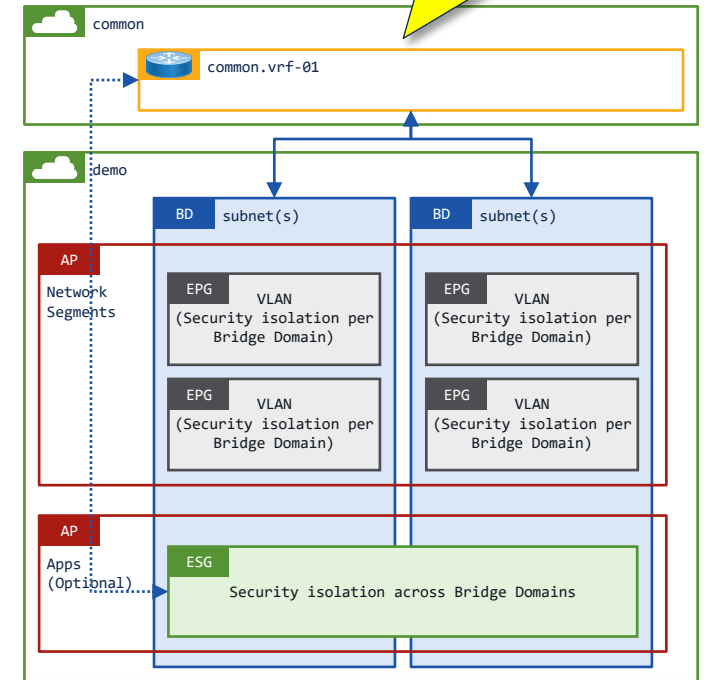
VRFs and BDs in "common" with EPGs and ESGs in the "user" tenant

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



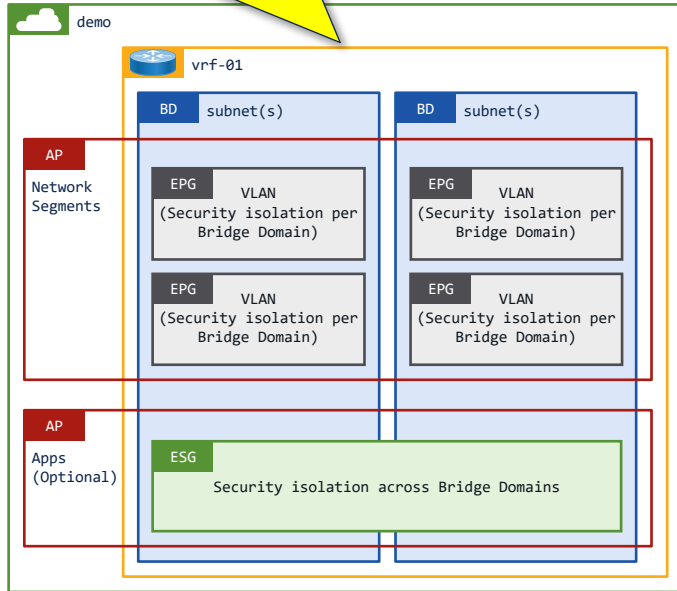
Dedicated subnets for tenants with VRFs that can be (optionally) shared by different Tenants

Design Patterns

All networking constructs contained within a Tenant

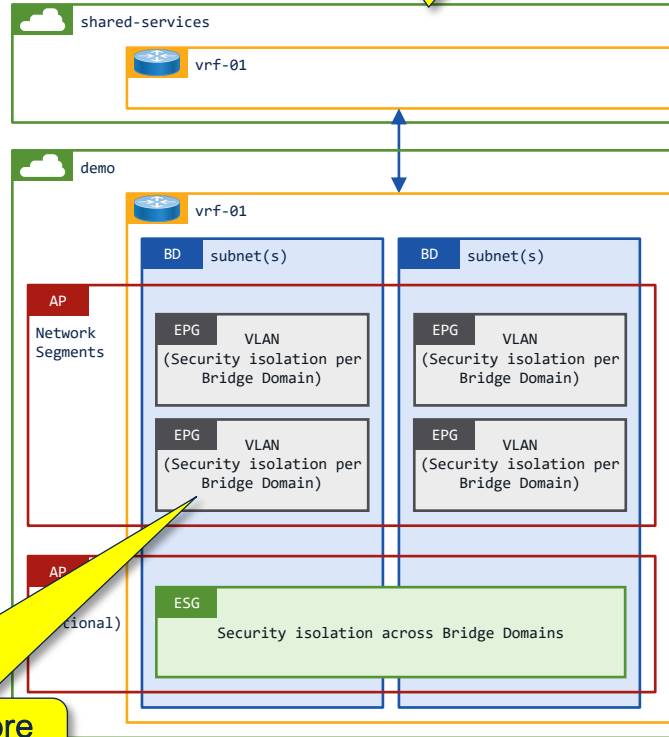
Network team controls inbound/outbound routing

Large subnets can be shared across Tenants



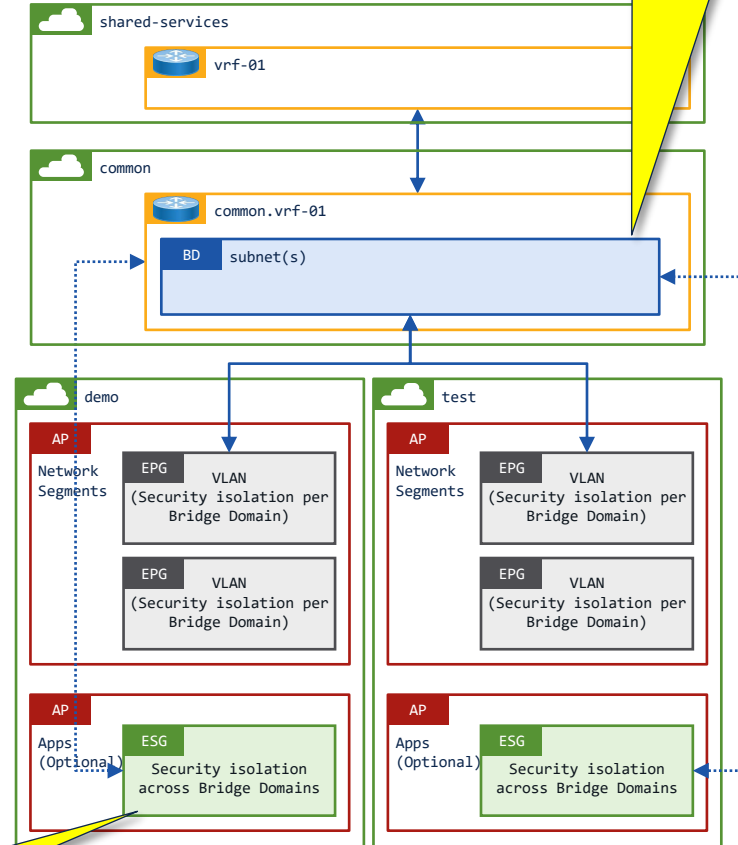
Dedicated VRFs and subnets for each Tenant with Dedicated L3outs

Each Tenant has one or more network security groups



Dedicated VRFs and subnets for each Tenant with Shared L3out

Each Tenant has one or more endpoint security groups



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: name or descr | common | ciscolive-07 | rwhitear | shared-services | ciscolive-08

| 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

Converting 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





Free shipping with \$75 purchase!

cisco-store

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





Hot Products

| | |
|---|--|
|  <p>Cabana Shorts \$39.99</p> |  <p>Cable Knit Blanket \$59.99</p> |
|  |  <p>Save the Bees Bottle SKU #22YFJ3GM2N Quantity: 1 \$13.79</p> |

Free shipping with \$75 purchase!

Cart (2)

[Empty Cart](#) [Continue Shopping](#)

| |
|---|
|  <p>Save the Bees Bottle SKU #22YFJ3GM2N Quantity: 1 \$13.79</p> |
|  <p>Cabana Shorts SKU #OLICESPC7Z Quantity: 1 \$39.99</p> |
| 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

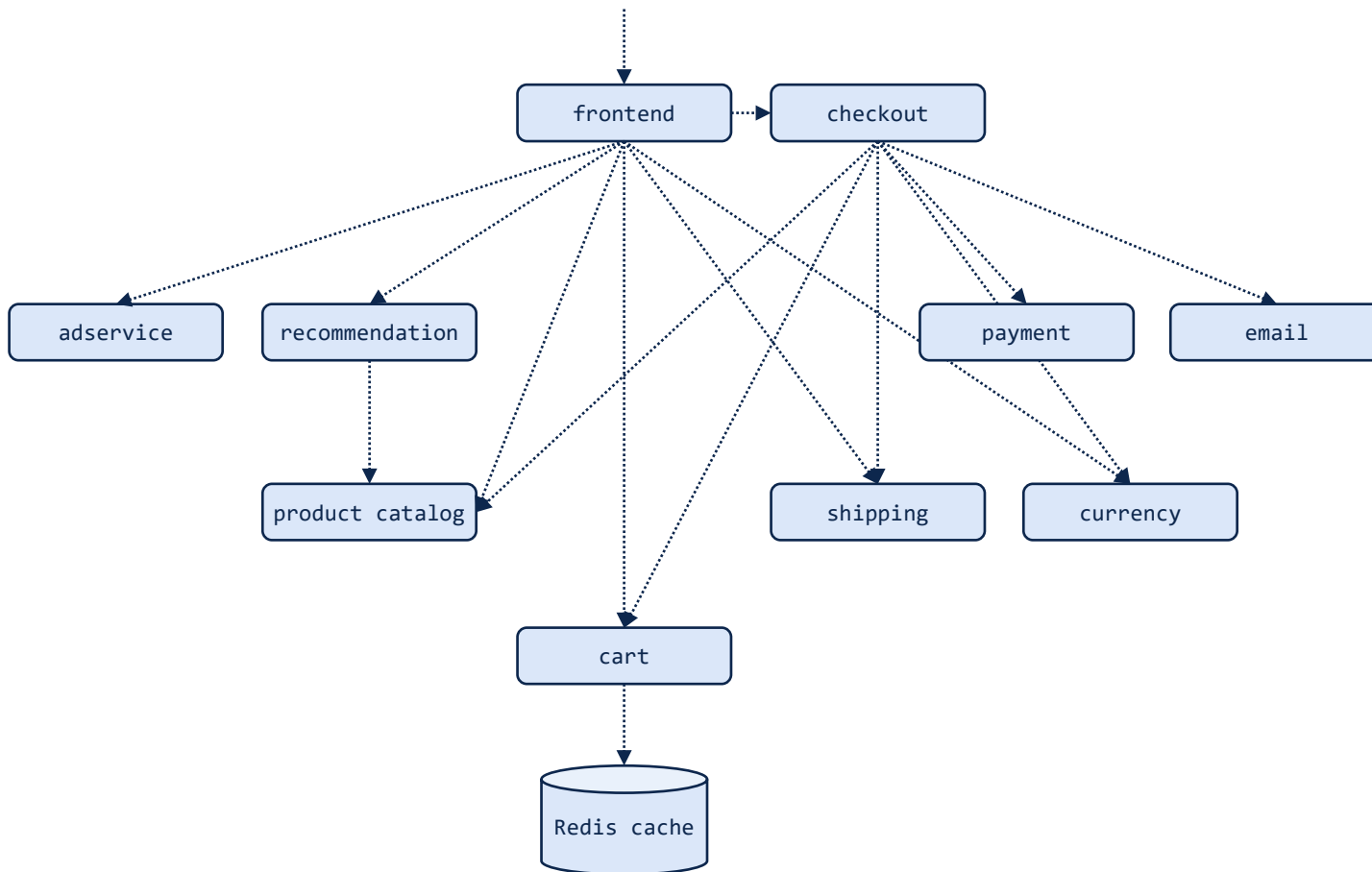
Year
2023

CVV
...

[Place Order](#)

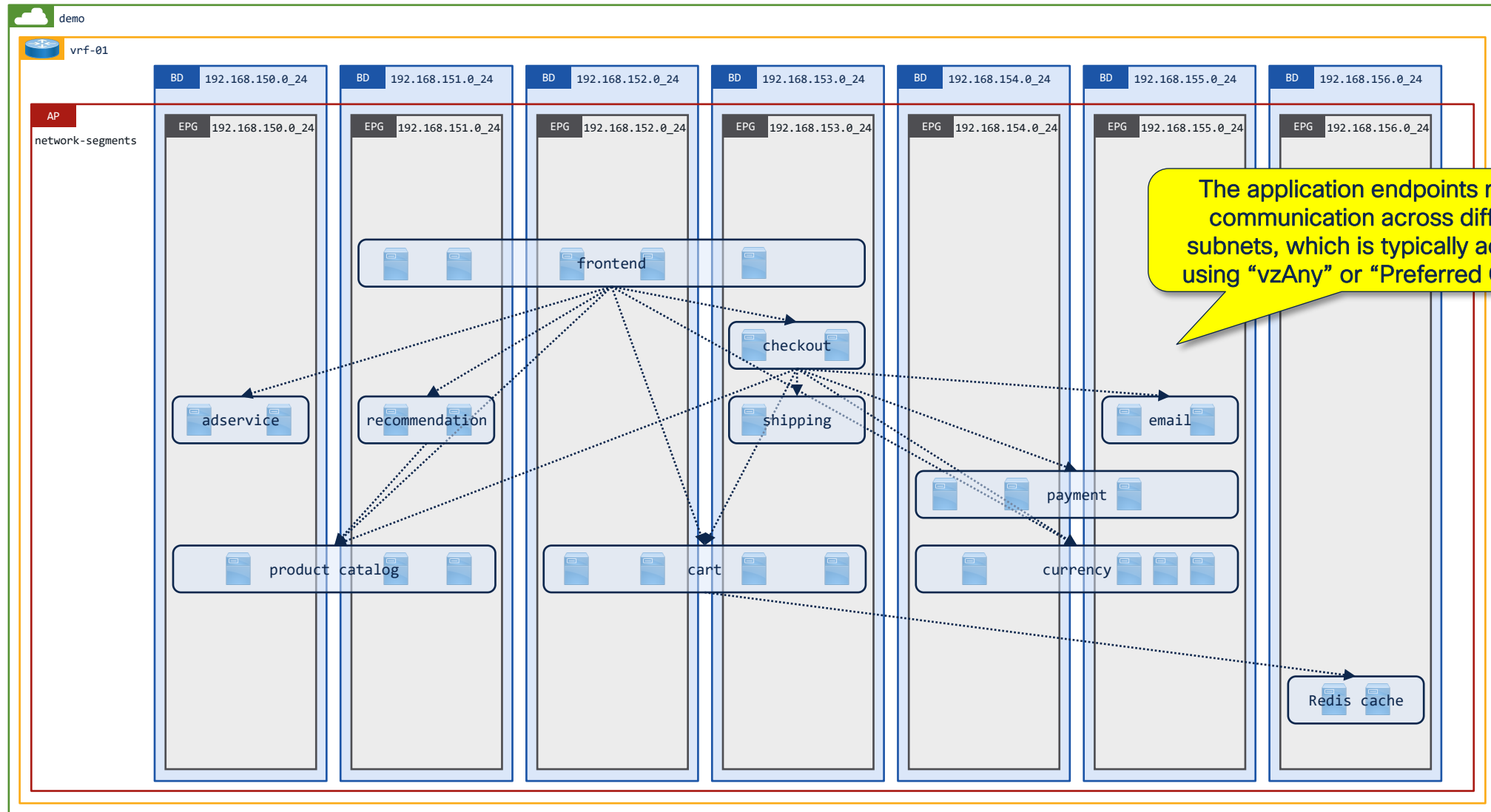
Online Boutique

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

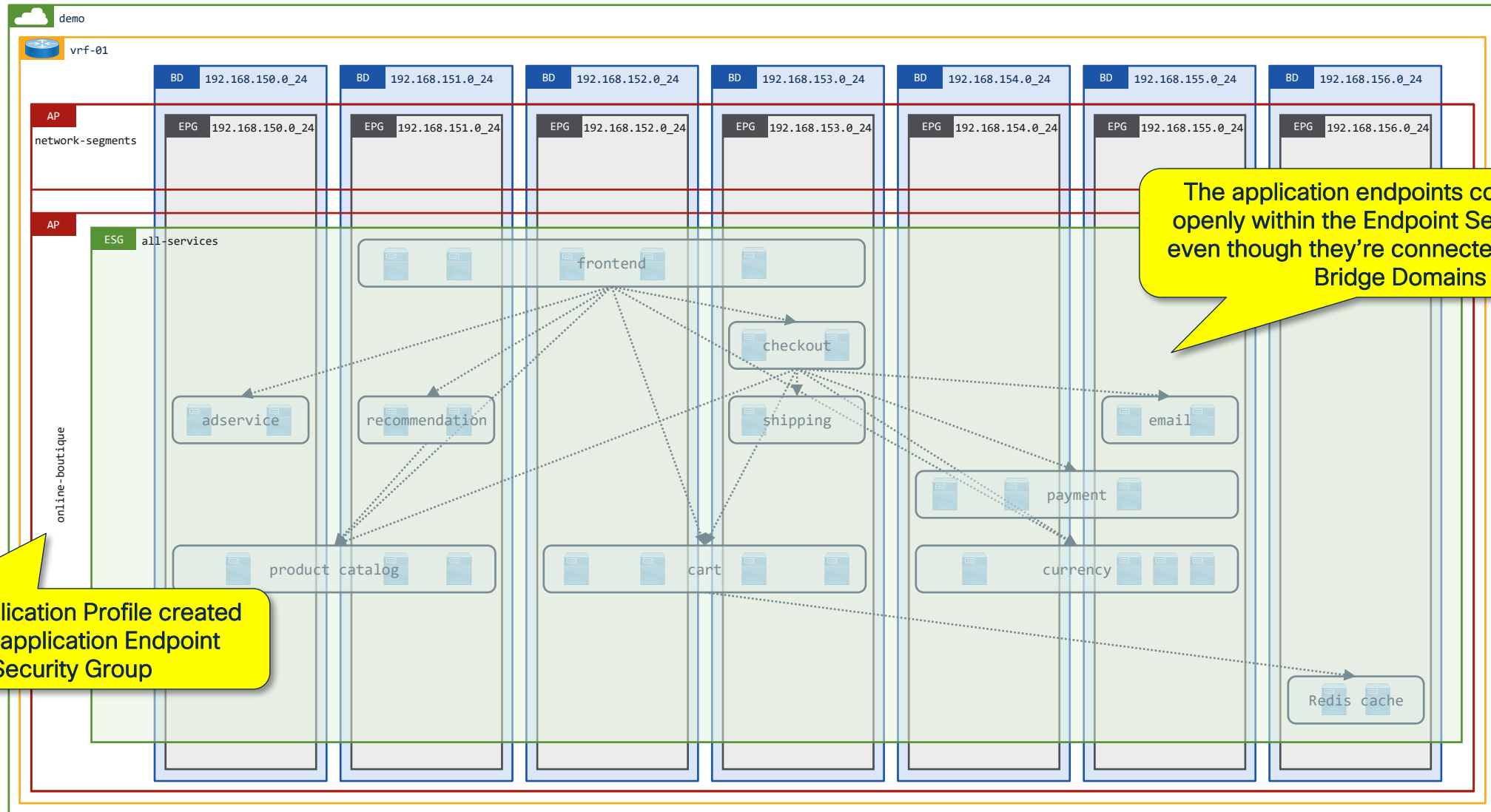


| Source/Consumer | Target/Provider | Target/Provider Port |
|-----------------|-----------------|----------------------|
| cart | Redis cache | TCP 6379 |
| checkout | cart | TCP 7070 |
| | currency | TCP 7000 |
| | email | TCP 8080 |
| | payment | TCP 50051 |
| | product catalog | TCP 3550 |
| | shipping | 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...



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...!

The screenshot displays the Cisco AVC interface for the 'demo' environment, specifically the 'ESG - all-services' view. The interface shows a table of application endpoints with various columns and callouts highlighting specific information.

Table Columns:

- MAC/IP
- Endpoint Name
- Hosting Server
- Interface (learned)
- Encap
- Base EPG
- Policy Tags

Table Data (Sample Rows):

| 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:A1:22:DE 192.168.152.100 | 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-servi 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 | __vmm:vmname tn-demo-online-boutique-shipping-servi 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 | __vmm:vmname tn-demo-online-boutique-product-catalog Function tn-demo-online-boutique-product-catalog-servi |
| 00:50:56:A1:22:DE 192.168.152.100 | tn-demo-online-boutique-cart-service | 10.237.98.166 | 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:A1:84:4D 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 | __vmm:vmname tn-demo-online-boutique-email-service Function tn-demo-online-boutique-email-service |
| 00:50:56:A1:B0:E2 192.168.151.101 | 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-servi |

Callouts:

- Application Endpoint IP and MAC Information:** Points to the MAC/IP column.
- Host Information:** Points to the Hosting Server column.
- VLAN Information:** Points to the Encap column.
- Tag Information:** Points to the Policy Tags column.
- Endpoint names:** Points to the Endpoint Name column.
- Switch and Interface Information:** Points to the Interface (learned) column.
- EPG/Subnet Information:** Points to the Base EPG column.

Page Information: Page 1 of 1, Objects Per Page: 100, Displaying Objects 1 - 11 Of 11.

Correlate Endpoints to Switch Interfaces...

Inventory

- > Quick Start
- > Topology
- > Pod 1
 - > aci-dev-01-leaf-101 (Node-101)
 - > aci-dev-01-leaf-102 (Node-102)
 - > aci-dev-01-spine-201 (Node-201)
 - > aci-dev-01-spine-202 (Node-202)

Layer 1 Physical Interface Configuration - 101/eth1/30

Operational Deployed EPGs VLANs **Stats** QoS Stats Health Faults History

Healthy | ⊛ ⚠ ✔ ⏪ ⏩ ⚙

↗ Total Egress Bytes Rate ↗ Total Egress Bytes
↘ CRC Align Errors ↗ Total Ingress Bytes Rate
↘ Total Ingress Bytes

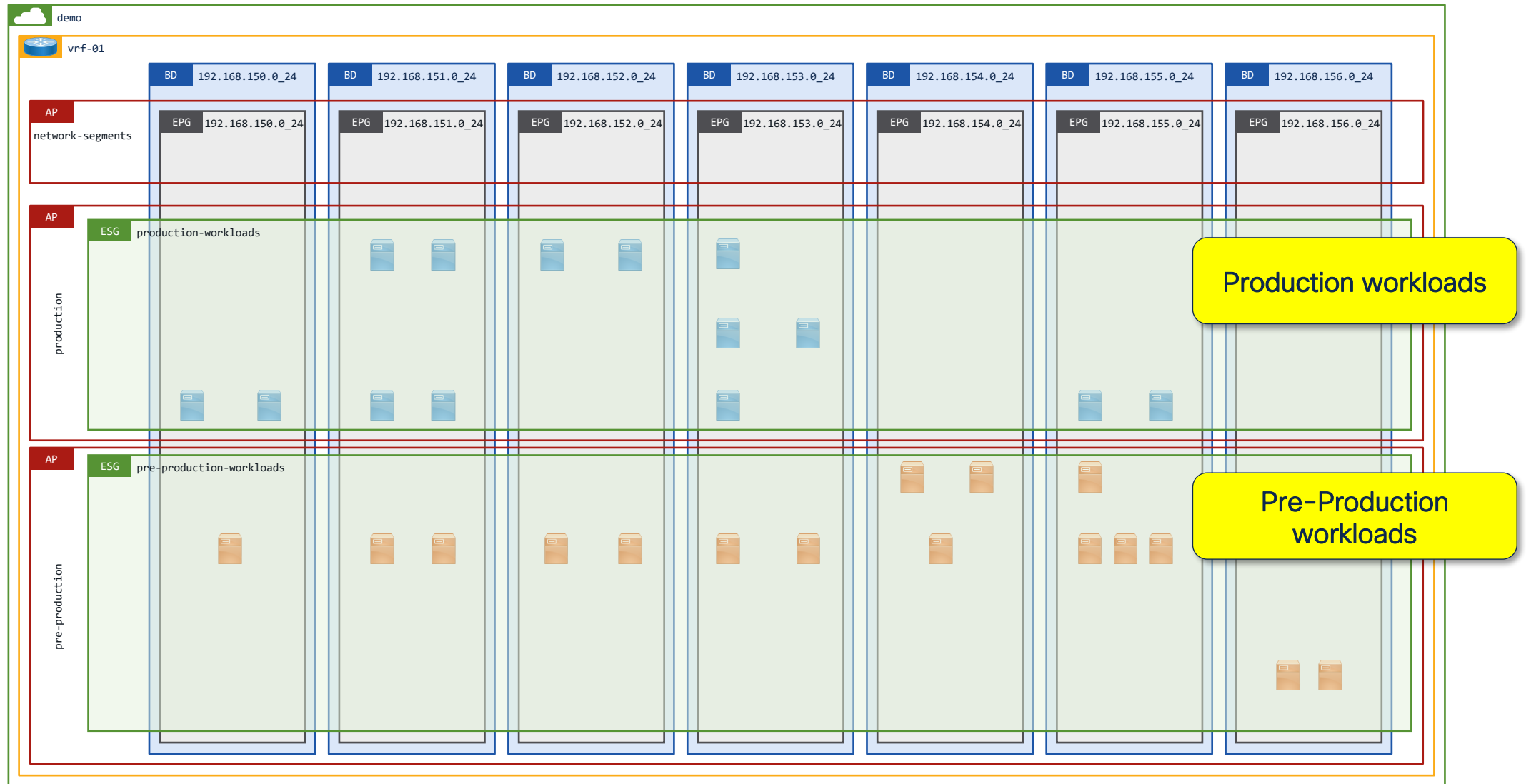
Layer 1 Physical Interface Configuration - 101/eth1/30

Operational Deployed EPGs VLANs Stats **QoS Stats** Health Faults History

| Class | Rx Counts | | | | Tx Counts | | | | | | |
|---------------|--------------|---------------|------------|--------------|--------------|---------------|------------|--------------|-------------------|---------------------|--|
| | Admit Bytes | Admit Packets | Drop Bytes | Drop Packets | Admit Bytes | Admit Packets | Drop Bytes | Drop Packets | Buffer Drop Bytes | Buffer Drop Packets | |
| level3 | 537237488774 | 331641401 | 33539628 | 353653 | 602227818041 | 328501767 | 408 | 6 | 0 | 0 | |
| level2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| level1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| policy-plane | 0 | 0 | 0 | 0 | 75106152 | 1043141 | 0 | 0 | 0 | 0 | |
| control-plane | 0 | 0 | 0 | 0 | 85877269 | 632340 | 0 | 0 | 0 | 0 | |
| span | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| level6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| level5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| level4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |

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

Broad-brush classification...



Switching to “Application
Centric” mode is simple...

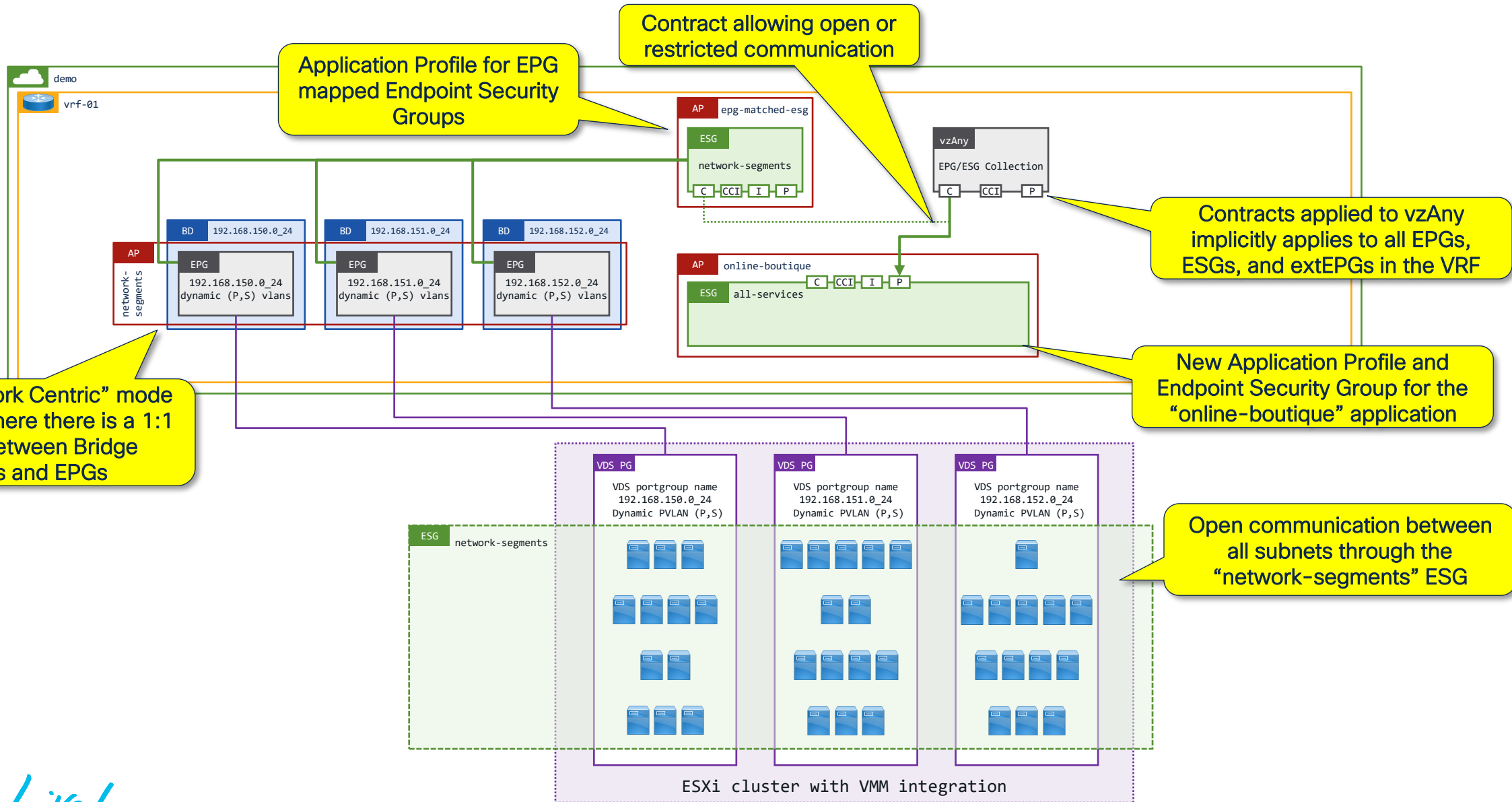
Application name
+
Application IP addresses



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



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

Application Profile for EPG mapped Endpoint Security Groups

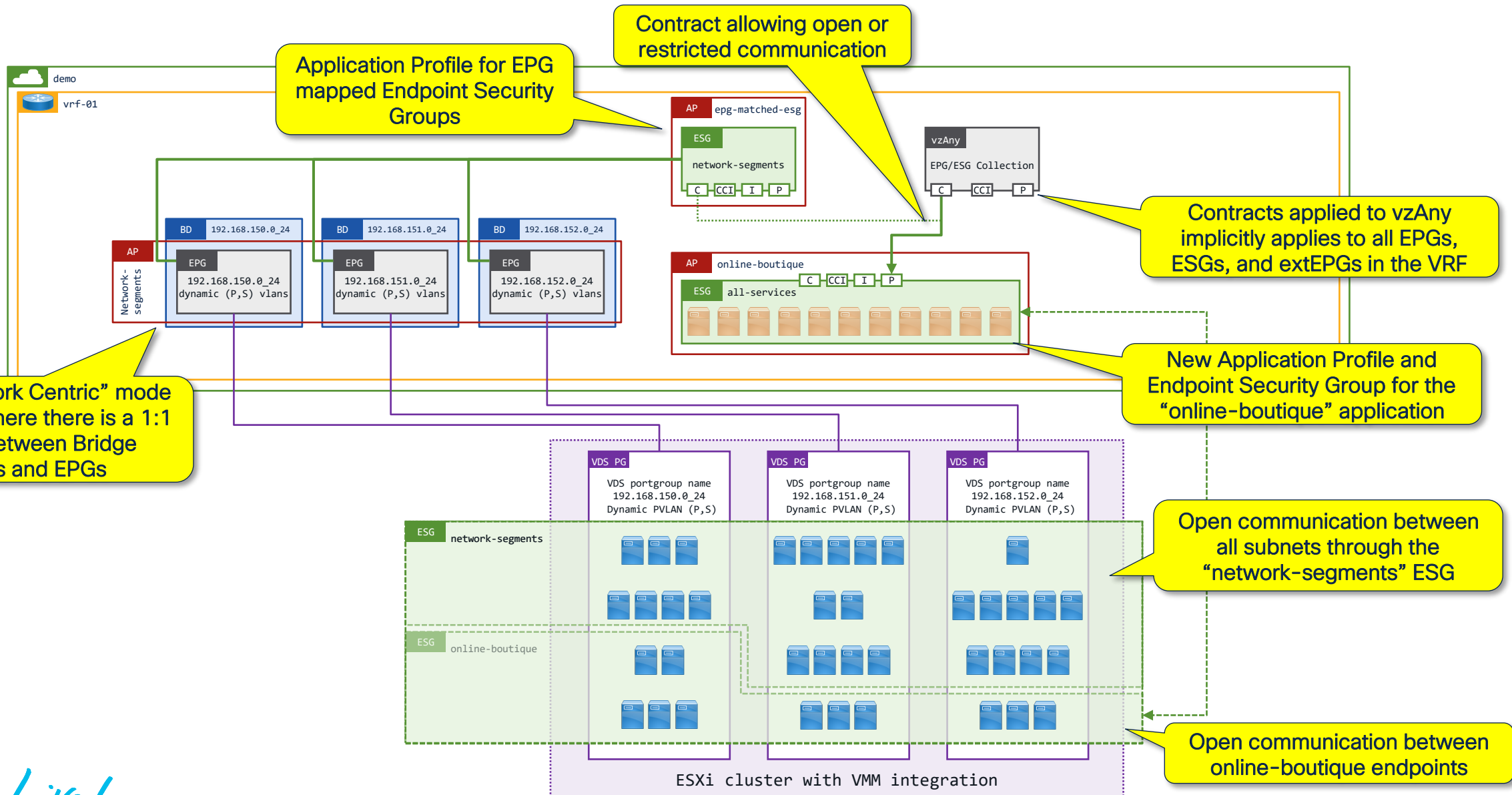
Contract allowing open or restricted communication

Contracts applied to vzAny implicitly applies to all EPGs, ESGs, and extEPGs in the VRF

New Application Profile and Endpoint Security Group for the "online-boutique" application

Open communication between all subnets through the "network-segments" ESG

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



Tagging Option 1: Static Tag Mapping

ACI Application Workload Tags

Define ESG Tag Selector
ApplicationName = online-boutique

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

| MAC Address | Bridge Domain | VRF | Tags | Matching Tag Selector |
|-------------------|---------------|--------|---------------------------------|---|
| 00:50:56:A1:0A:90 | * | vrf-01 | ApplicationName online-boutique | uni/tn-demo-non-vm/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-vm/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-vm/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-vm/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-vm/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-vm/ap-online-boutique/esg-all-services/tagselectorkey-[ApplicationName]-value-[online-boutique] |
| 00:50:56:A1:B8:3B | * | vrf-01 | ApplicationName online-boutique | uni/tn-demo-non-vm/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-vm/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-vm/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 screenshot displays the configuration of vCenter Application Workload Tags and their mapping to ACI Application Workload Tags. A yellow callout points to the vCenter tags, and another points to the ACI tags. A third callout at the bottom right states: "ACI Application Workload Tags match vCenter Application Workload Tags".

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

ADD TAG

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

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 |

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
 - Networking
 - Contracts
 - Policies
 - Services
 - Security

Summary Policy **Operational** Health Faults History

Client Endpoints Contracts Deployed Leaves Tag Selectors

Healthy

| 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- |

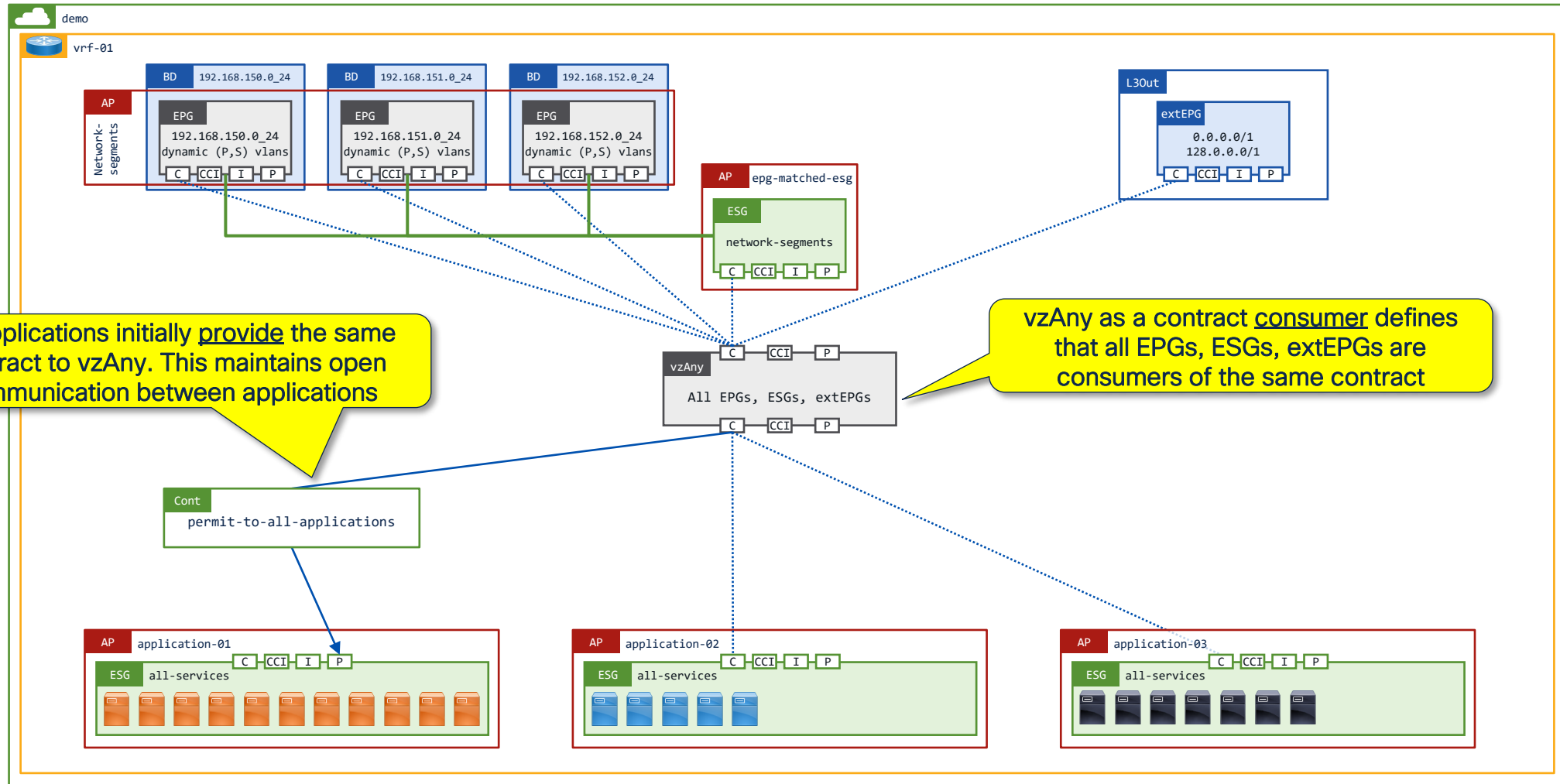
Page 1 Of 1 | Objects Per Page: 100 | Displaying Objects 1 - 11 Of 11

Last Login Time: 2023-02-03T07:03 UTC+00:00 | Current System Time: 2023-02-03T08:07 UTC+00:00

```
sshman@sshman-jumphost:~$ ping 192.168.152.101
```

Scaling application connectivity with vzAny...

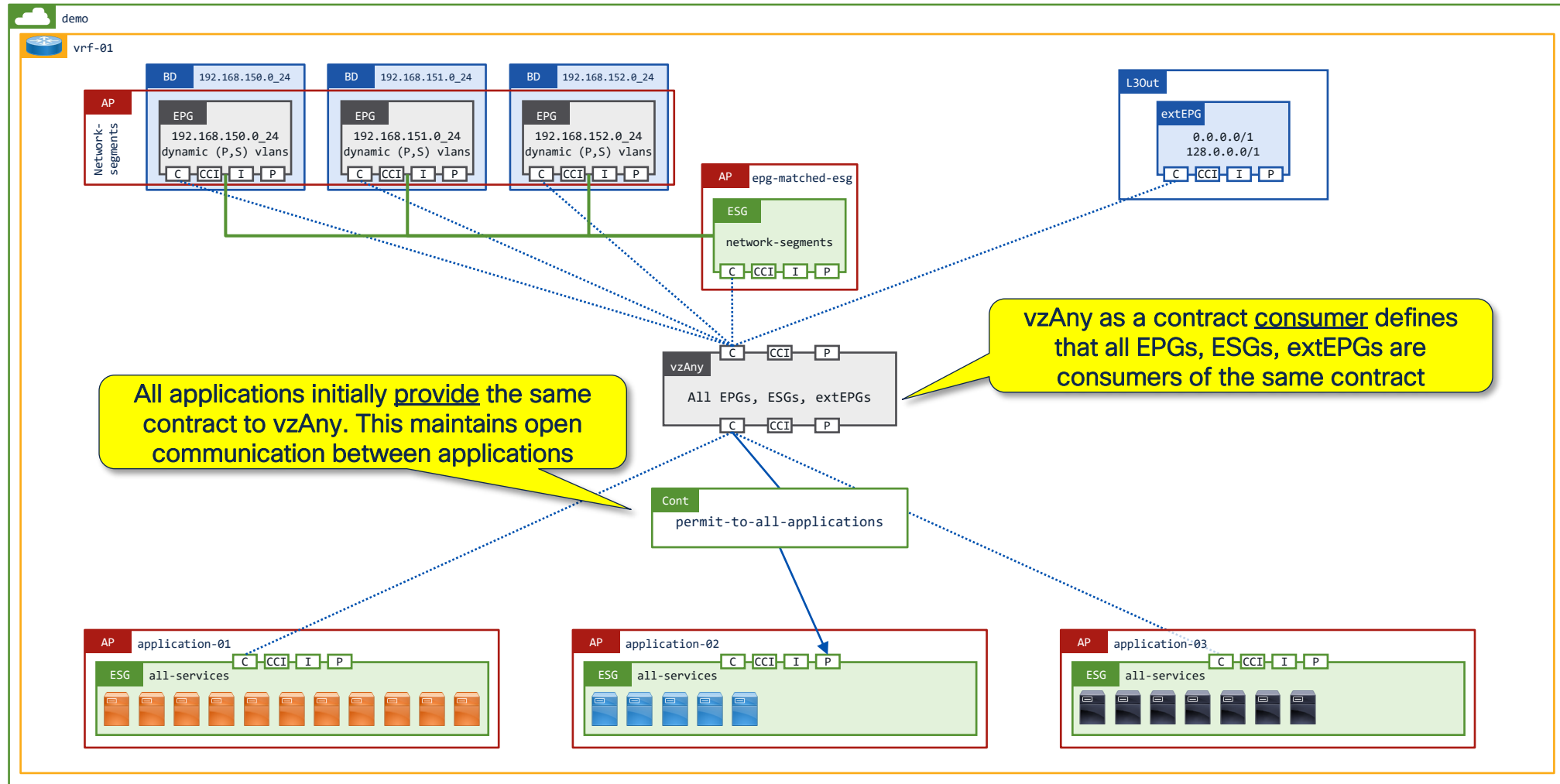
Scaling connectivity to “application-01”



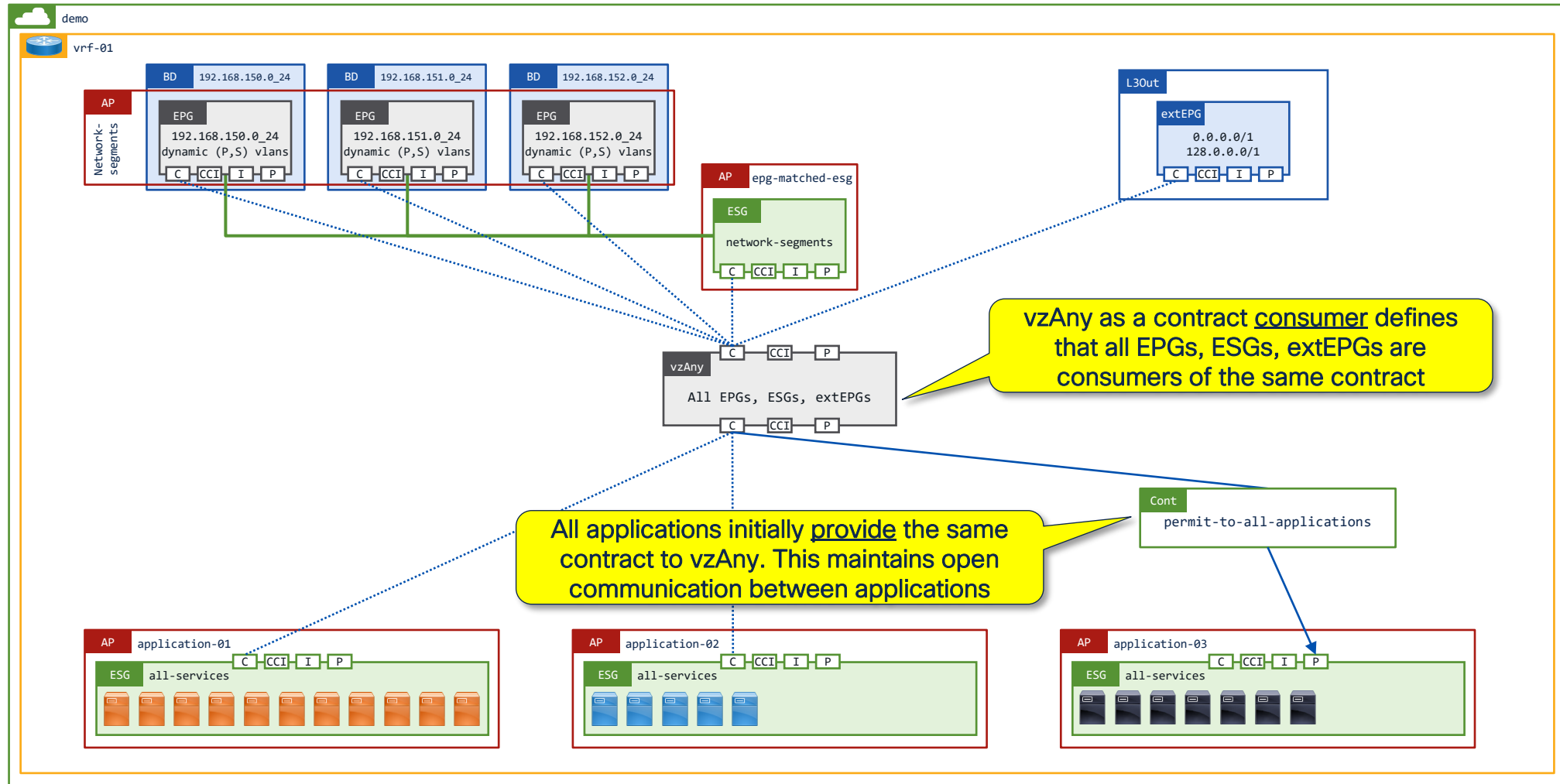
All applications initially provide the same contract to vzAny. This maintains open communication between applications

vzAny as a contract consumer defines that all EPGs, ESGs, extEPGs are consumers of the same contract

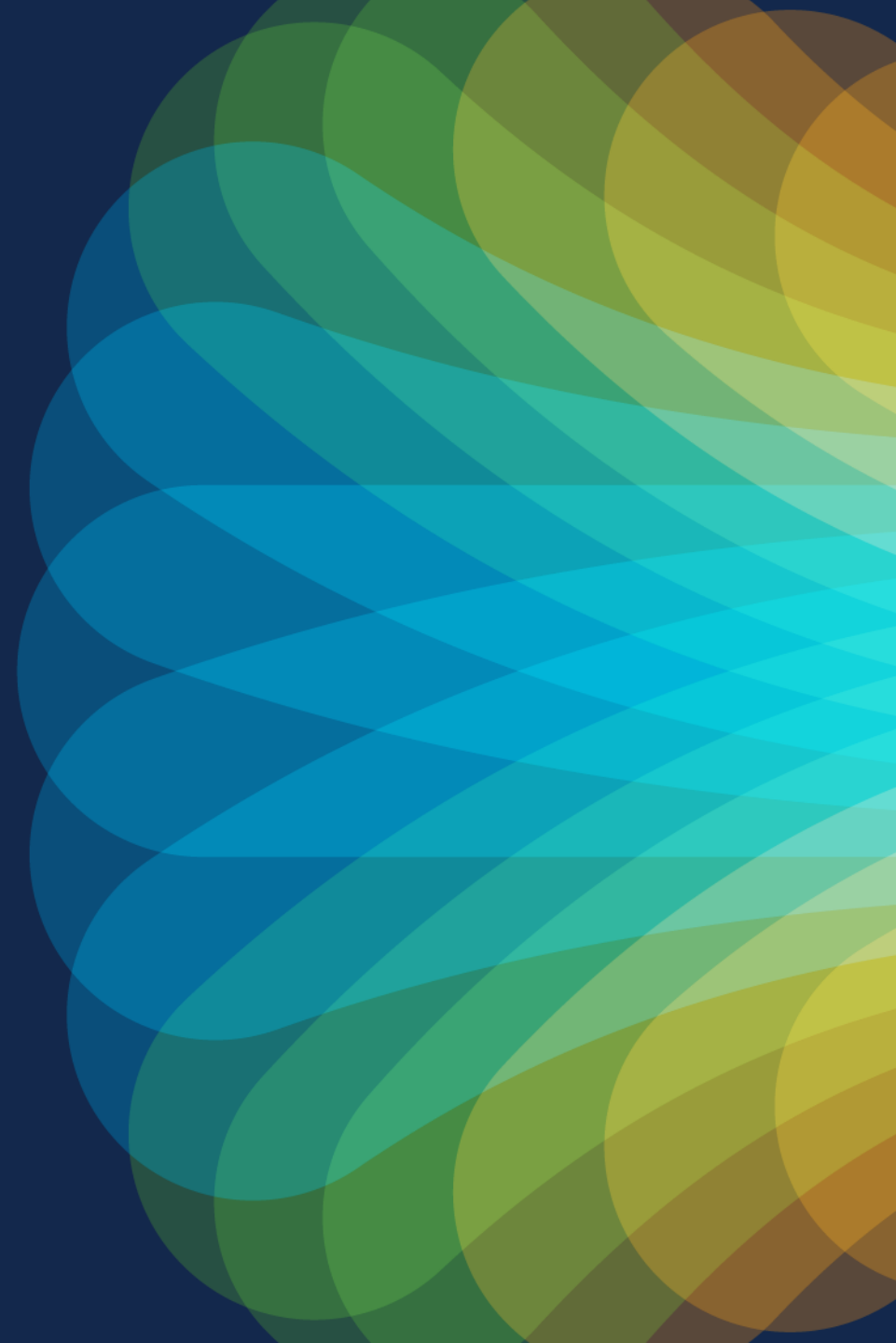
Scaling connectivity to “application-02”



Scaling connectivity to “application-03”



Classification and Segmentation using ESGs

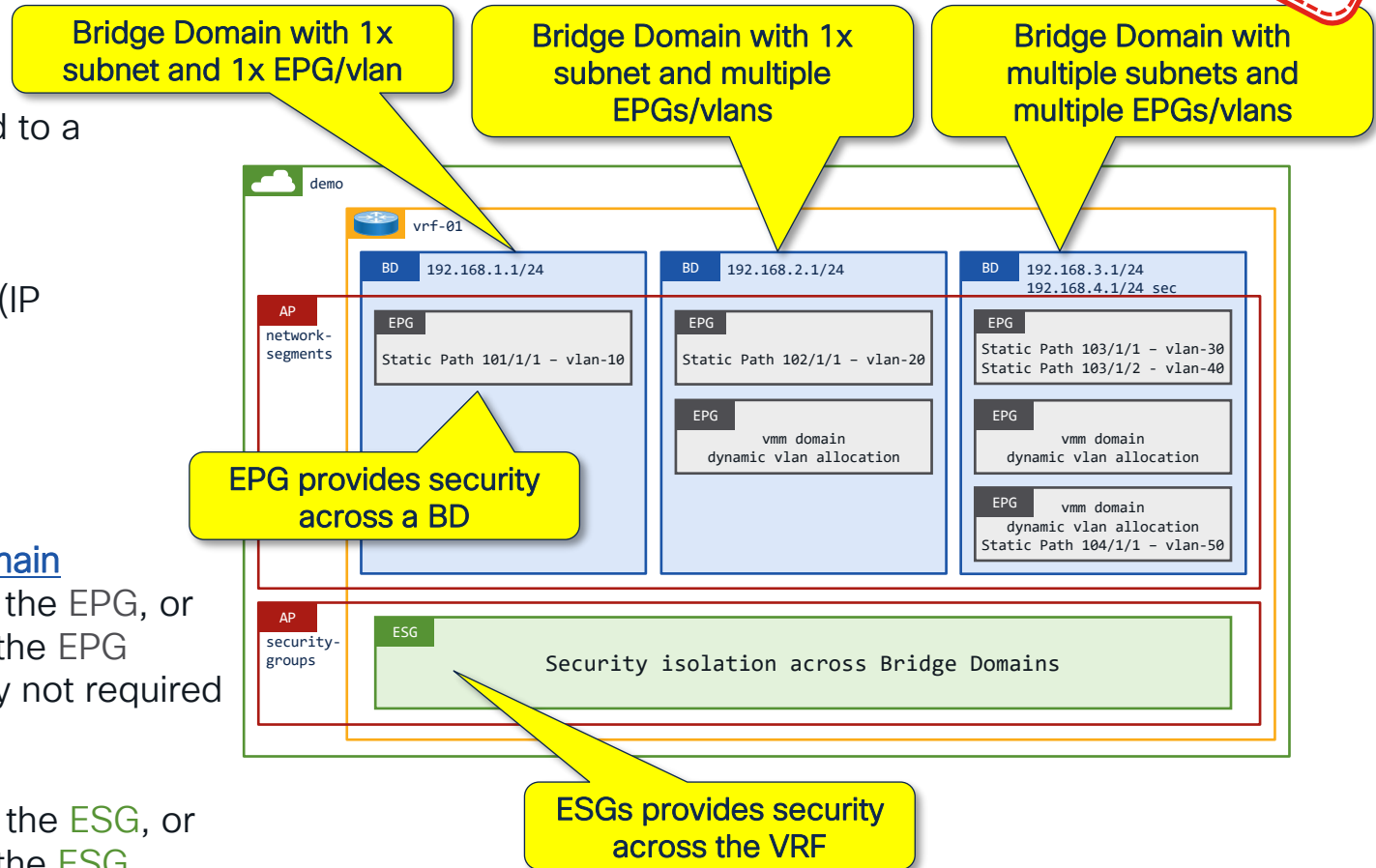


EPG Security vs ESG Security

For your reference

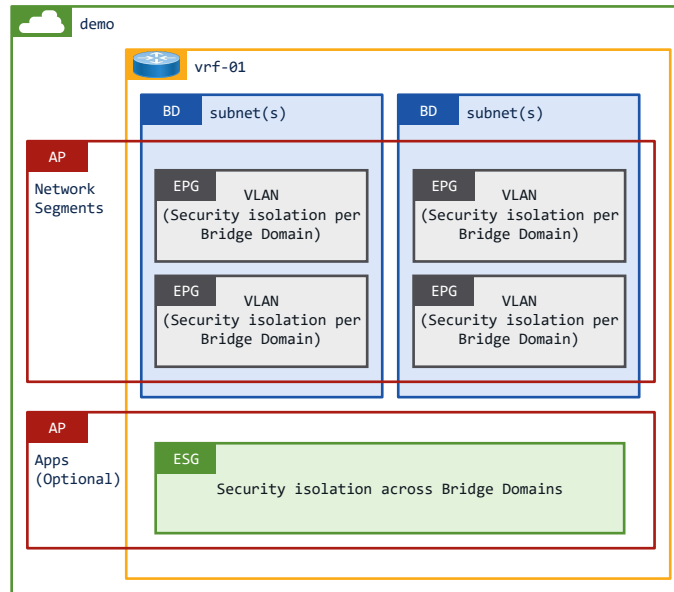
ACI foundational building blocks:

- 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**

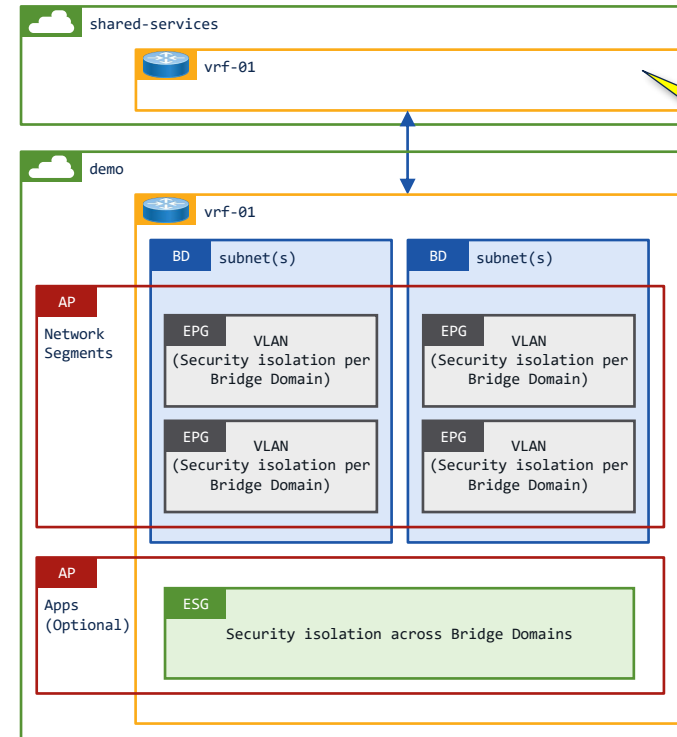


Select a Design Pattern and map your Endpoints to the ESG...

Design Patterns



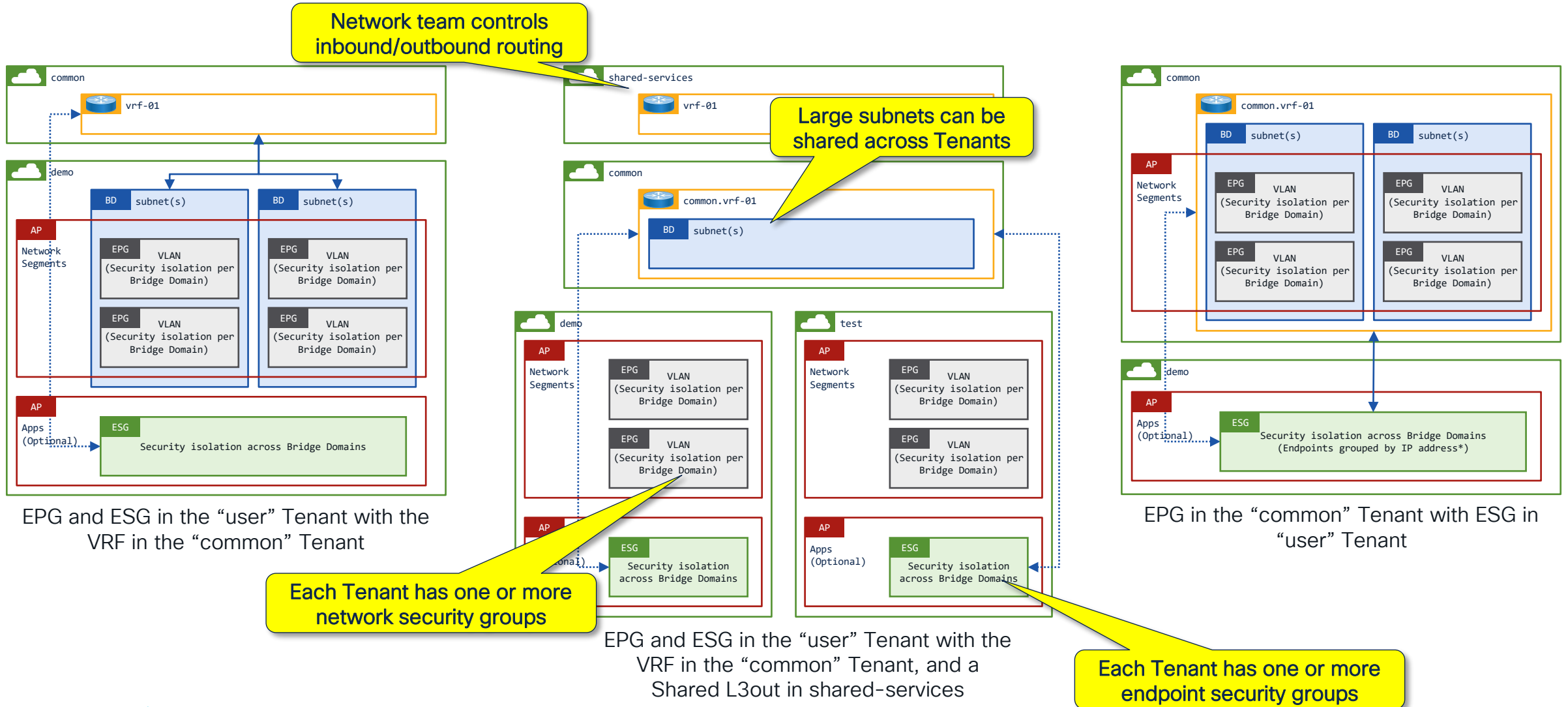
EPG and ESG in the "user" Tenant with a dedicated L3out



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

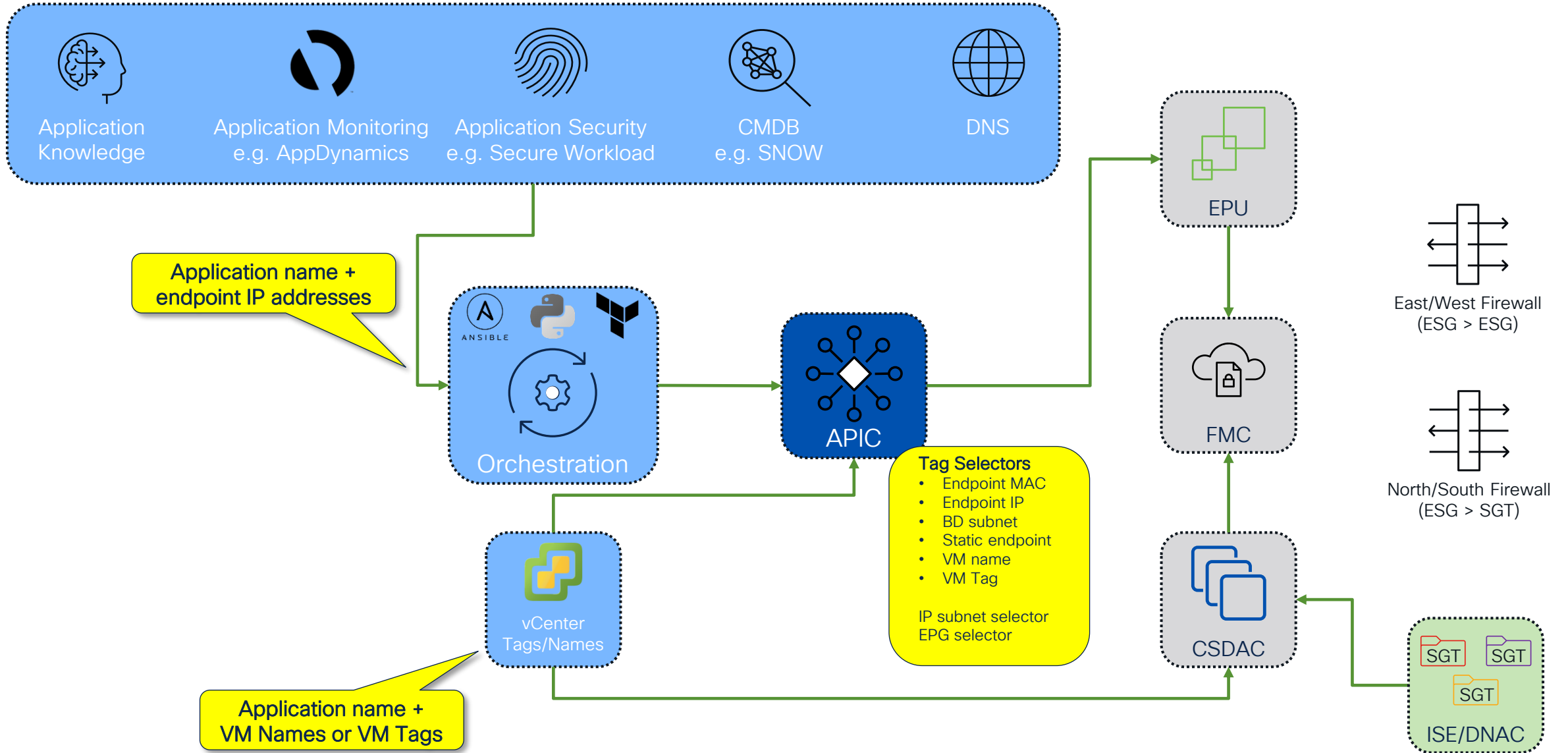
Network team controls inbound/outbound routing

Design Patterns



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

Application Knowledge taken from any source

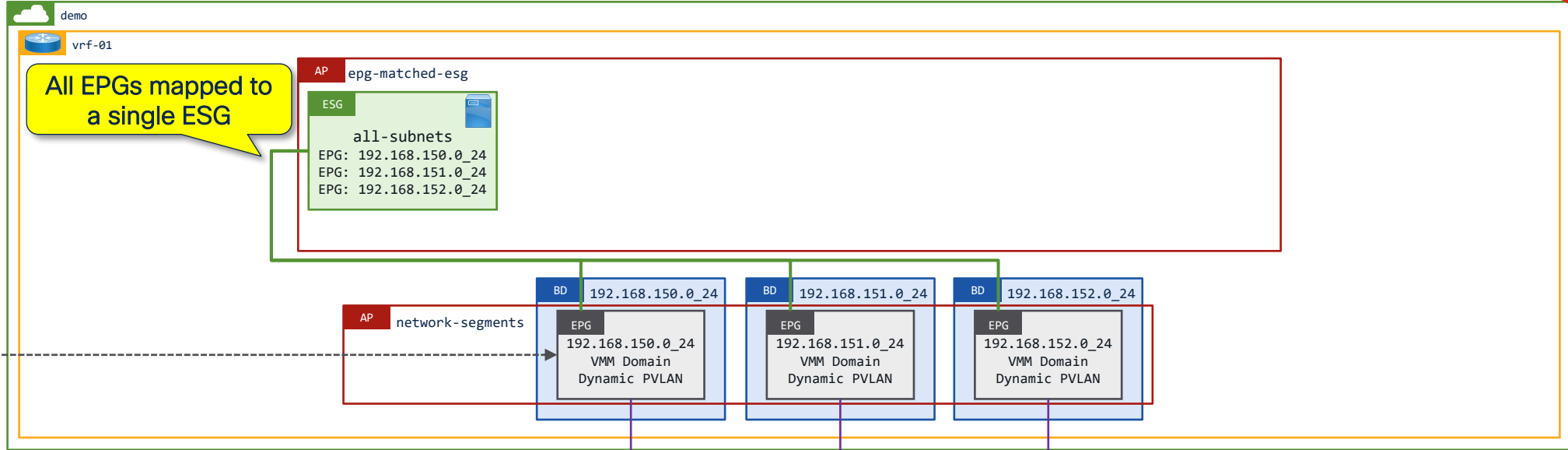


What are our endpoint mapping options...?

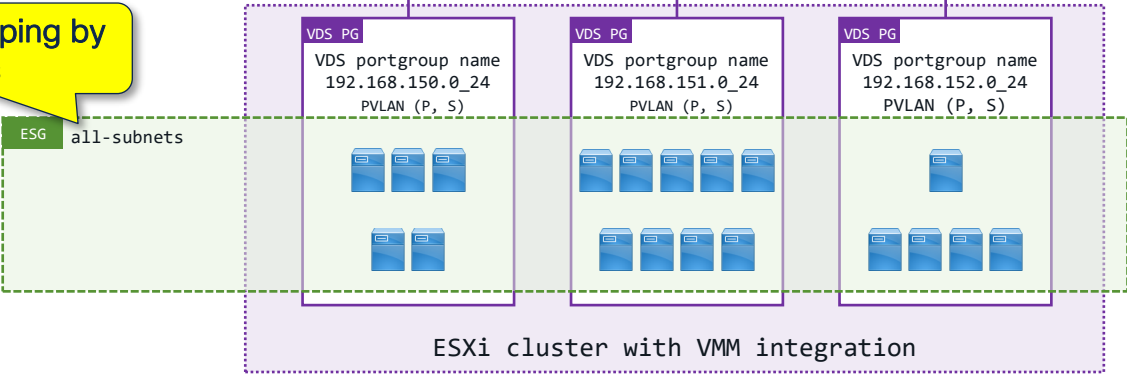
We can use EPGs, Tagged endpoints, Tagged subnets, or simply Static endpoint mapping...

Option 1: EPG mapping to a single security zone

Open security comparable to vzAny, excluding the extEPG



Logical grouping by EPGs

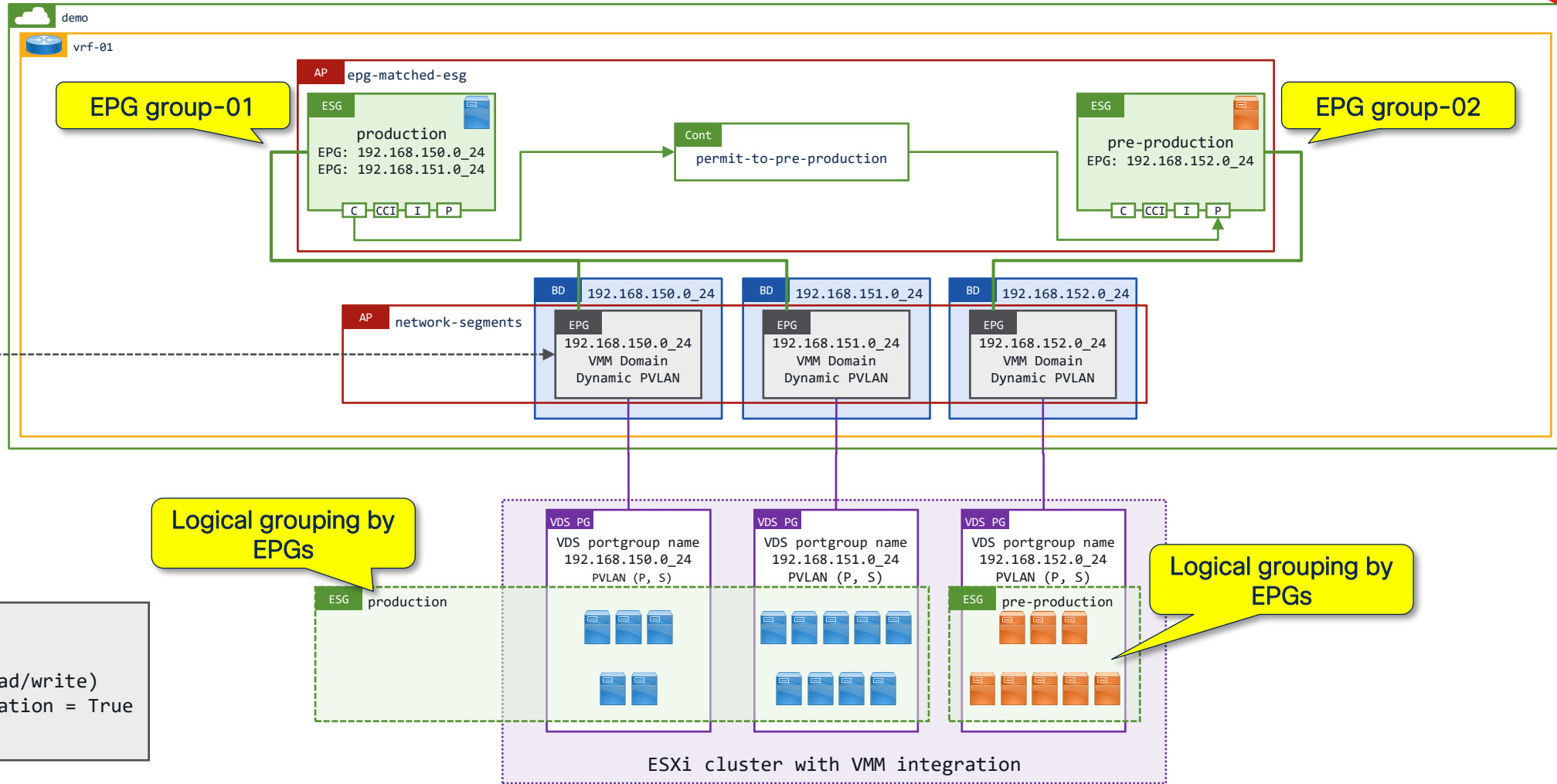


EPG Settings:

- VMM Domain (read/write)
- Allow uSegmentation = True
- Dynamic PVLANS

Option 2: EPG mapping for multiple security zones

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

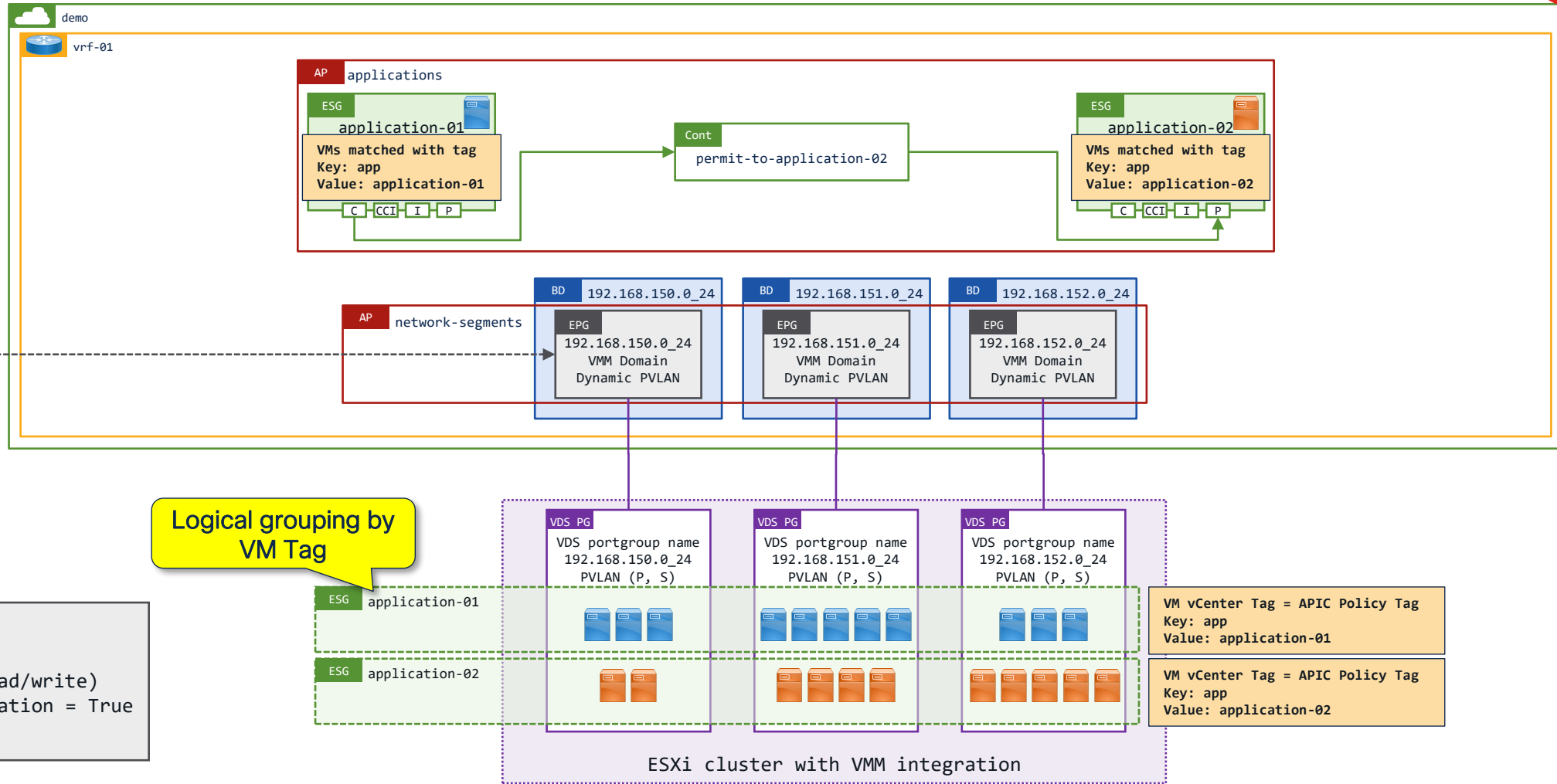


EPG Settings:

- VMM Domain (read/write)
- Allow uSegmentation = True
- Dynamic PVLANS

Option 3: Tag selectors with VMM integration

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



Logical grouping by VM Tag

Settings:

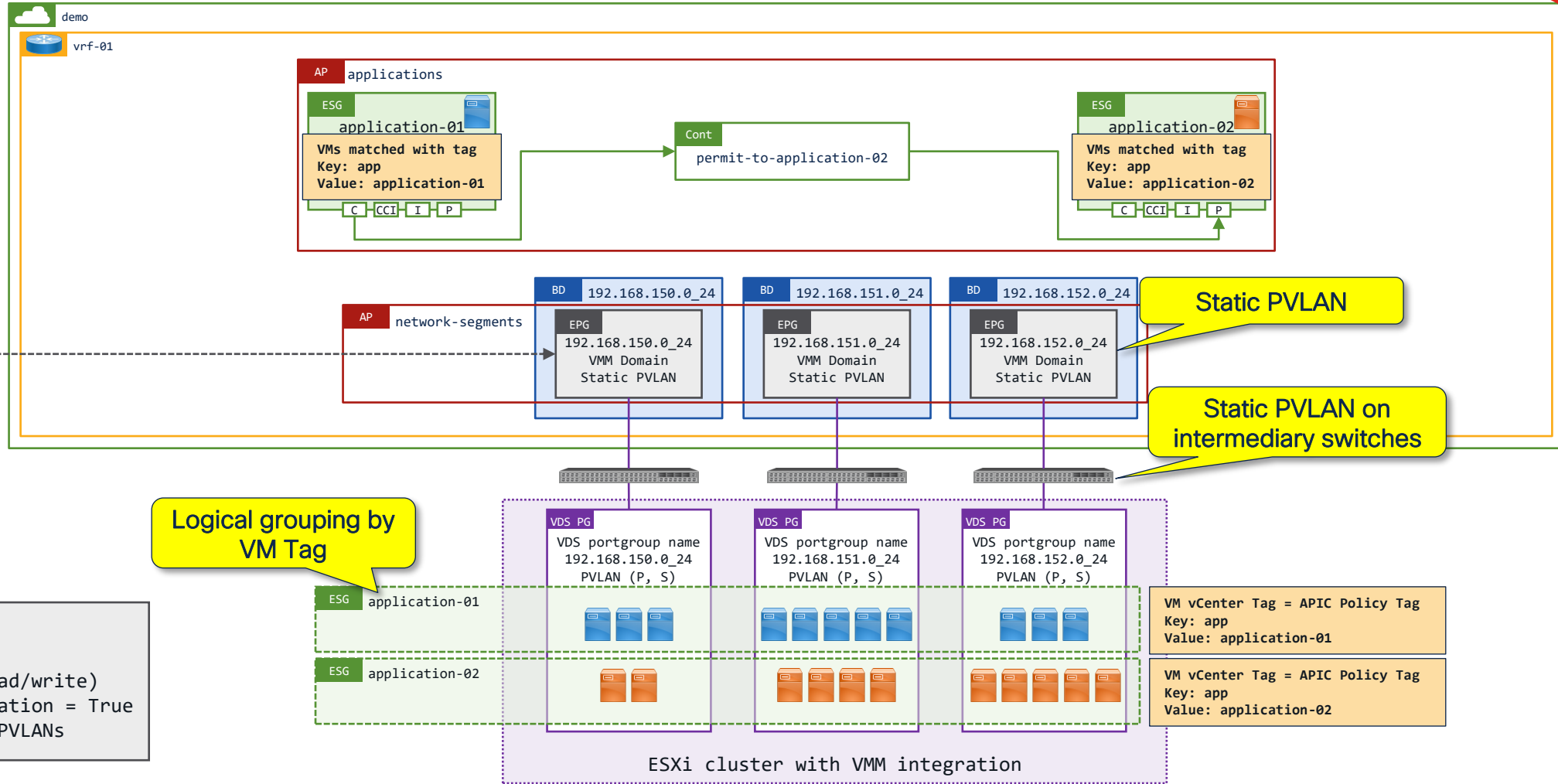
- VMM Domain (read/write)
- Allow uSegmentation = True
- Dynamic PVLANS

VM vCenter Tag = APIC Policy Tag
Key: app
Value: application-01

VM vCenter Tag = APIC Policy Tag
Key: app
Value: application-02

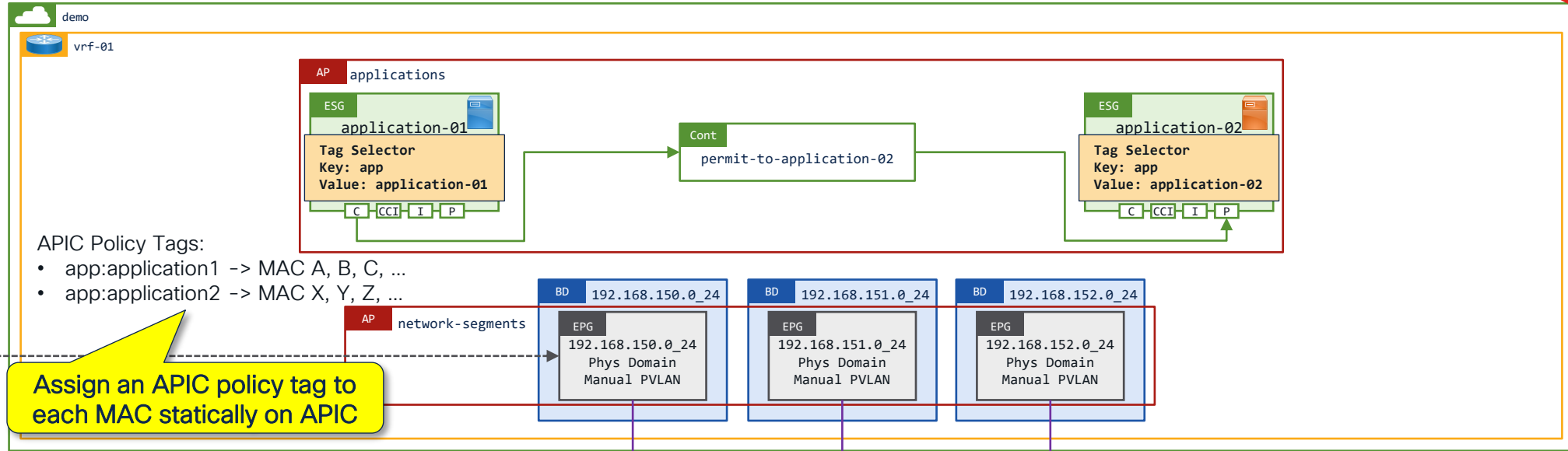
Option 4: Tag selectors with VMM integration and Intermediary switches

Intermediary switches require PVLAN pre-provisioning



Option 5: MAC selectors, no VMM integration

Endpoint assignment using endpoint MAC addresses. Requires PVLAN on VDS

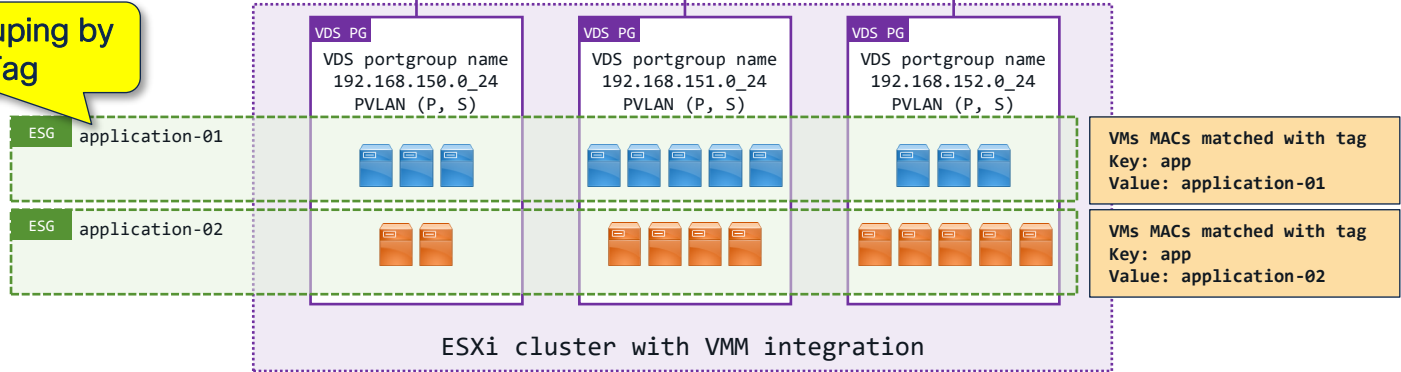


- APIC Policy Tags:
- app:application1 -> MAC A, B, C, ...
 - app:application2 -> MAC X, Y, Z, ...

Assign an APIC policy tag to each MAC statically on APIC

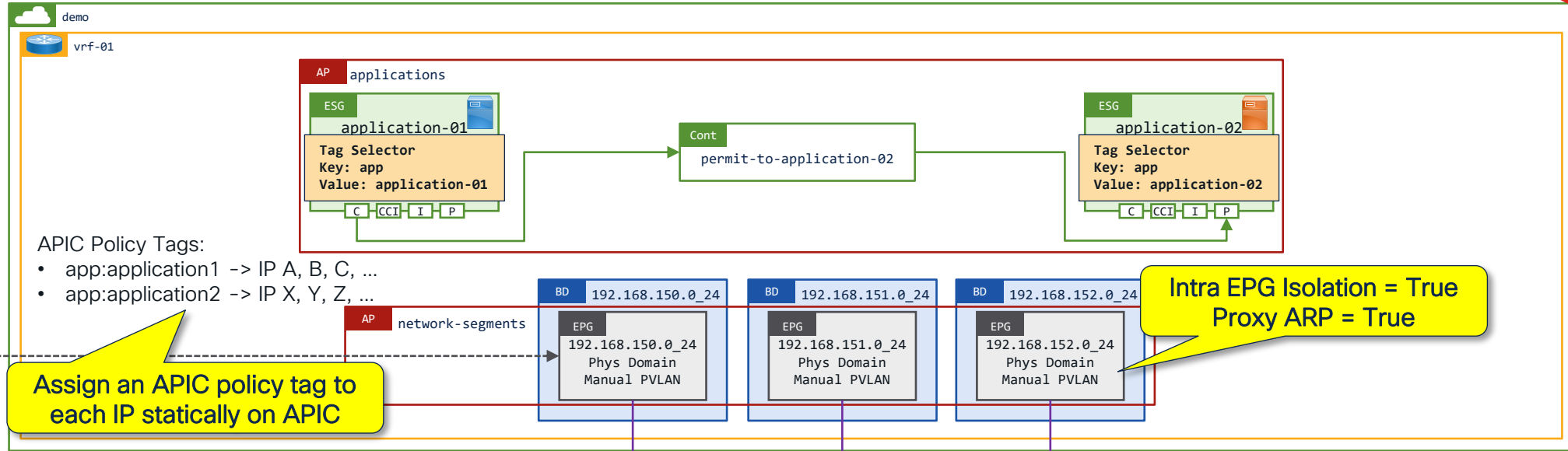
Logical grouping by MAC Tag

- 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

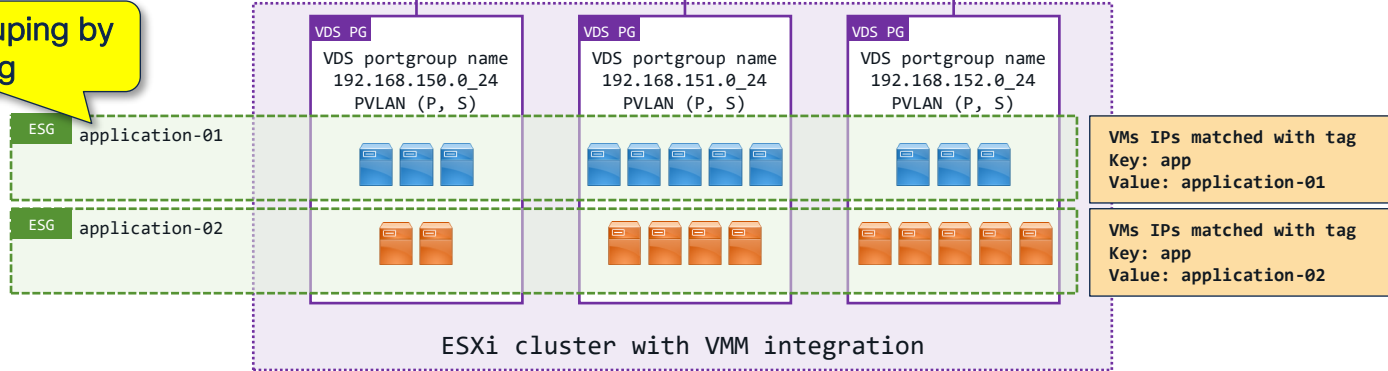


Assign an APIC policy tag to each IP statically on APIC

Intra EPG Isolation = True
Proxy ARP = True

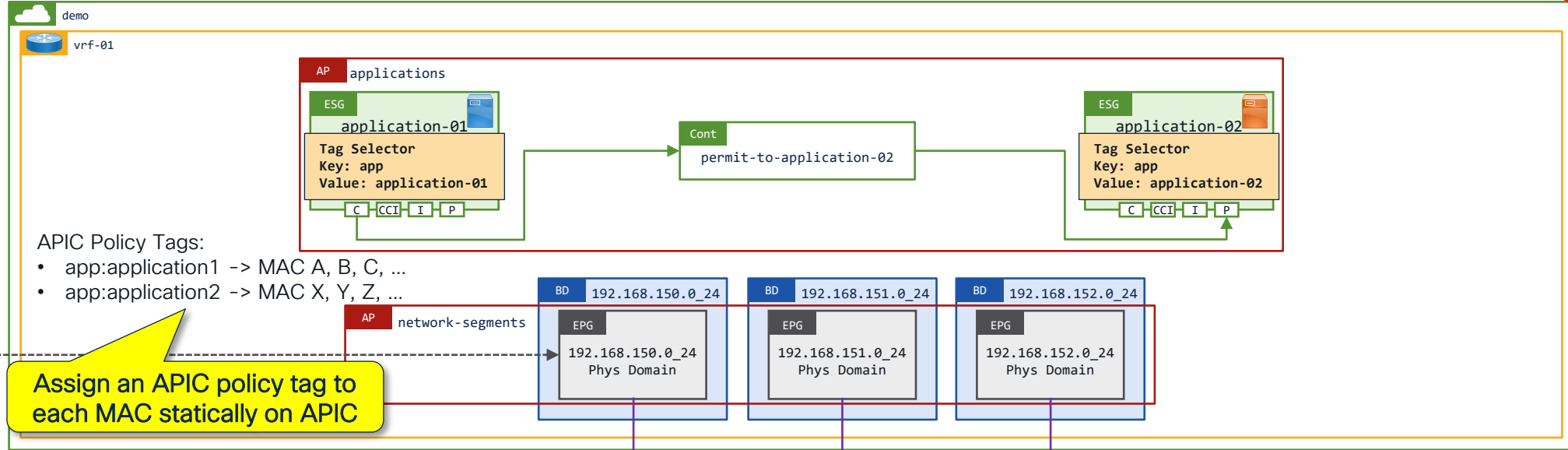
Logical grouping by IP Tag

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



Option 7: MAC selectors for bare metal

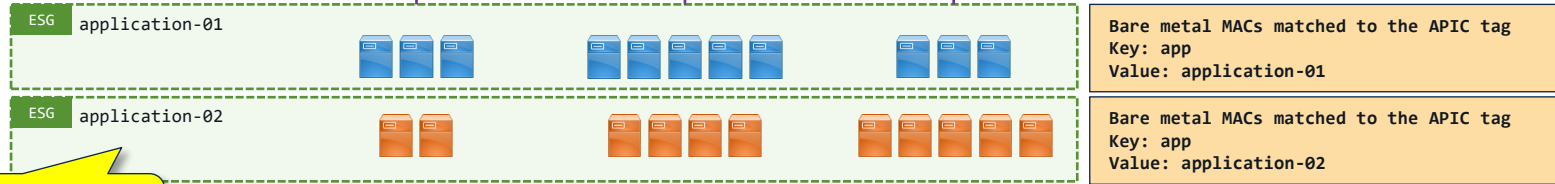
Endpoint assignment using endpoint MAC addresses



EPG Settings:

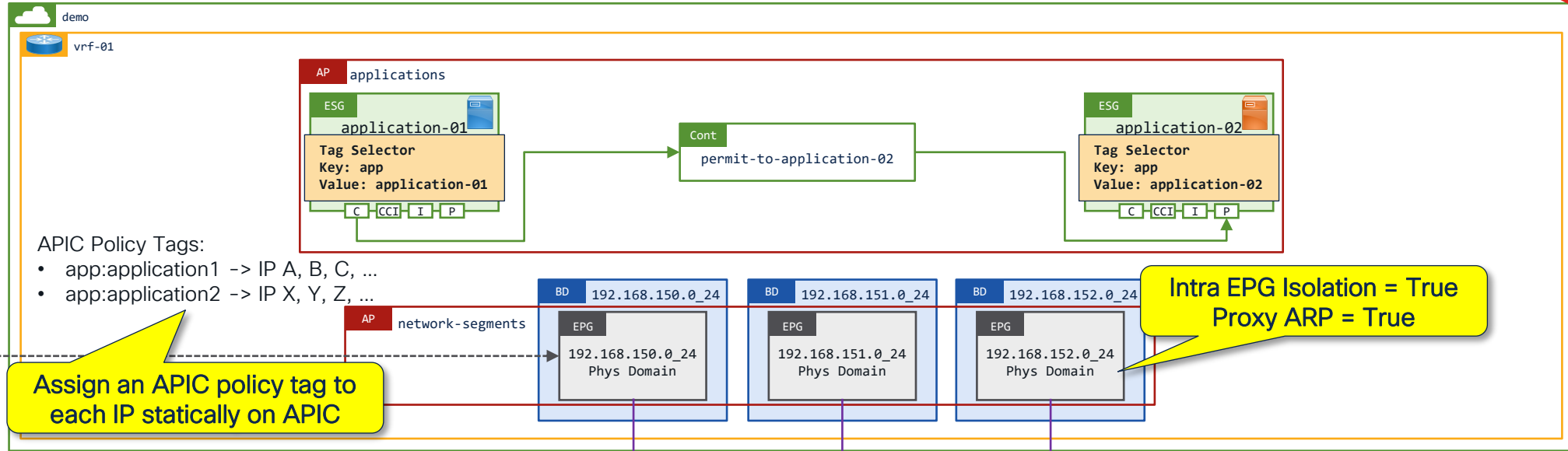
- Physical Domain
- Static path bindings

Logical grouping by MAC Tag



Option 8: IP selectors for bare metal

Endpoint assignment using endpoint IP addresses



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

Assign an APIC policy tag to each IP statically on APIC

Intra EPG Isolation = True
Proxy ARP = True

Logical grouping by IP Tag

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

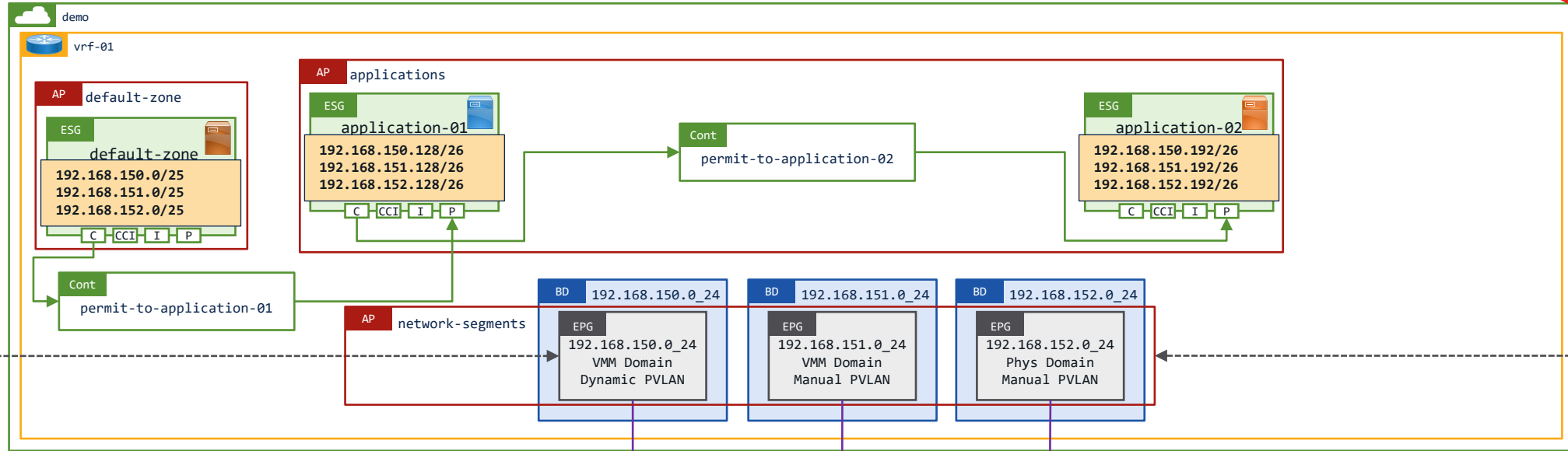
EPG

Settings:

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

Option 9: Subnet selectors

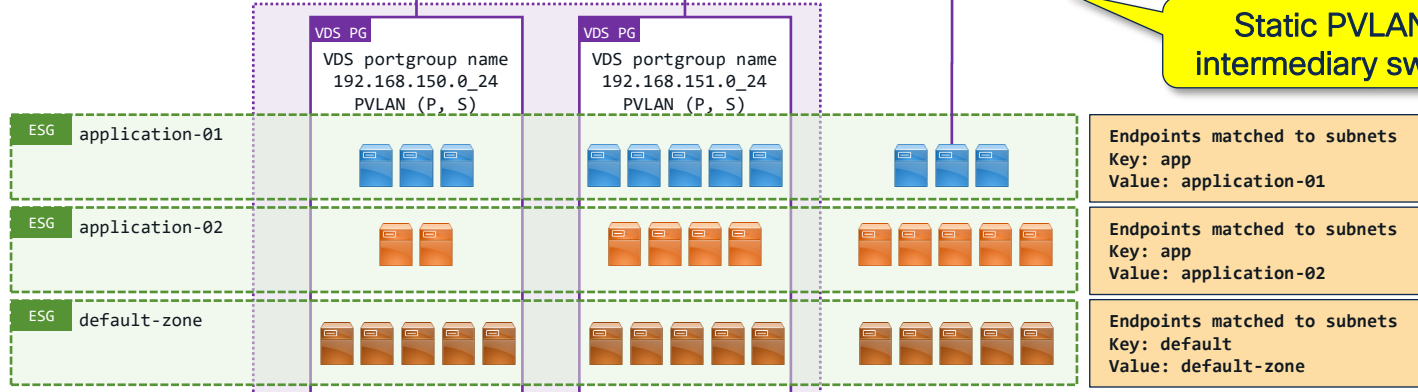
Endpoint assignment using subnet ranges



Static PVLAN on intermediary switches

EPG Settings:

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



EPG Settings:

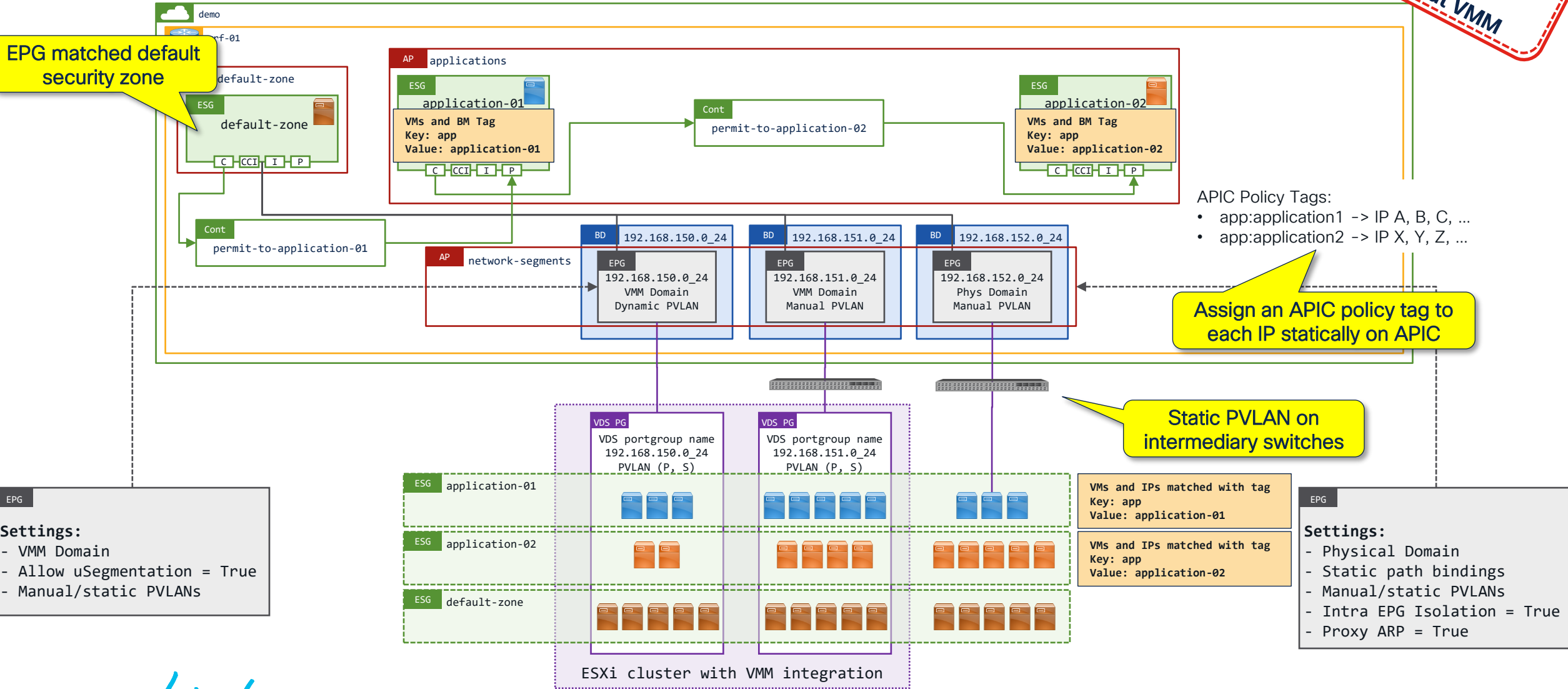
- Physical Domain
- Static path bindings
- Manual/static PVLANS
- Intra EPG Isolation = True
- Proxy ARP = True

ESXi cluster with VMM integration

Option 10: Combined solution with/without VMM

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

EPG matched default security zone



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

Assign an APIC policy tag to each IP statically on APIC

Static PVLAN on intermediary switches

Settings:

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

VMs and IPs matched with tag
Key: app
Value: application-01

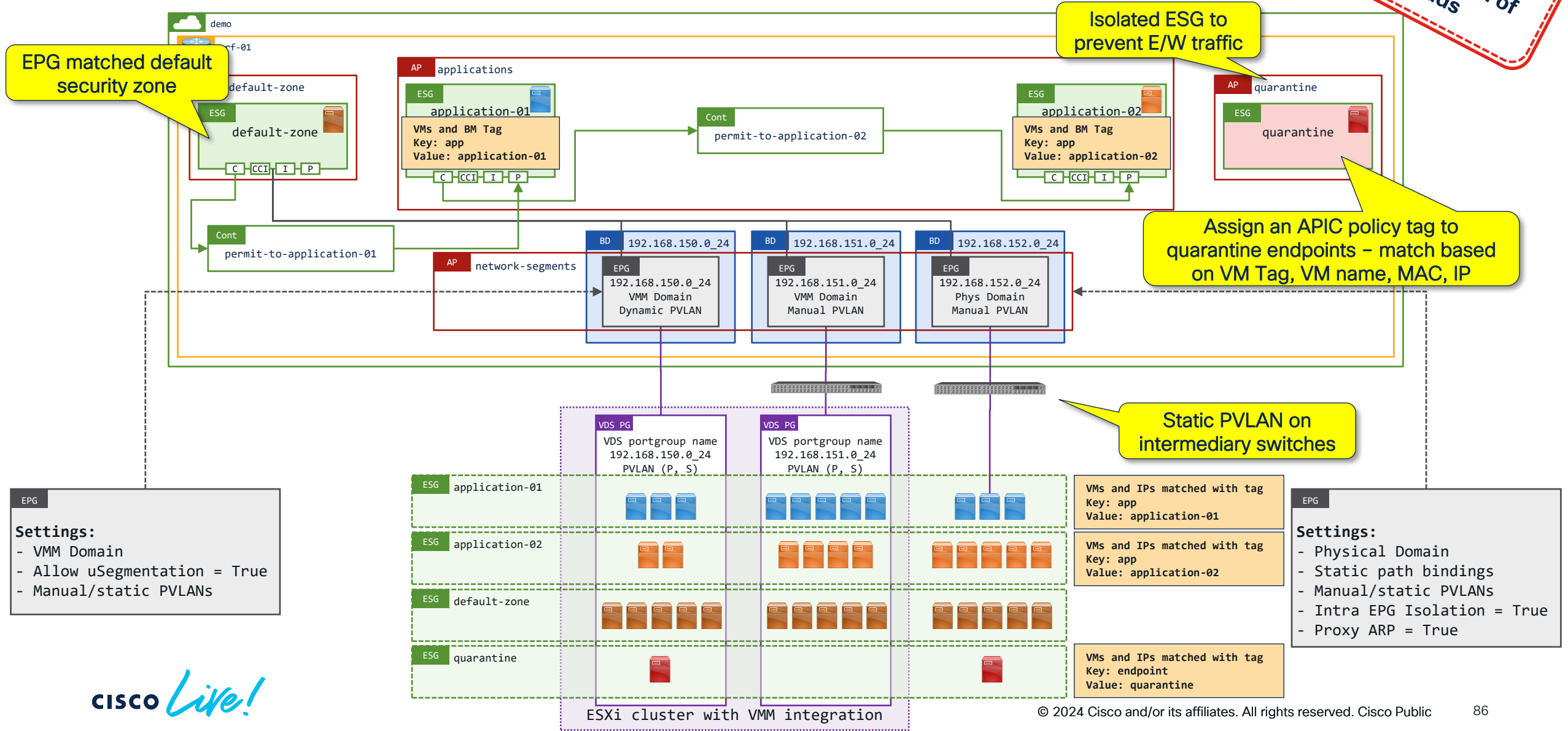
VMs and IPs matched with tag
Key: app
Value: application-02

Settings:

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

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...

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 G

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:

demo|network-segments|192.168.150.0_24

Summary Monitor Configure Permissions Ports Hosts VMs

Port binding: Static binding

Port allocation: Elastic

VLAN ID: 1046

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

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

demo|network-segments|192.168.150.0_24

Summary Monitor Configure Permissions Ports Hosts VMs

Port binding: Static binding

Port allocation: Elastic

Private VLAN: Isolated (1094, 1095)

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

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

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

Dynamic Policy Tag matching from vCenter

System Tenants Fabric **Virtual Networking**

Kubernetes | Rancher RKE | OpenShift | OpenStack |

VMware

- VMware
 - hx-dev-01-vds-01
 - hx-dev-01-vds-02
 - ucsc-c220m5-vds-01**
 - Controllers
 - Custom Trunk Port Groups
 - Trunk Port Groups

ubuntu-01

Summary Monitor Configure Permissions Datastores Networks Snapshots

Guest OS: Ubuntu Linux (64-bit)
 Compatibility: ESXi 6.7 and later (VM version 14)
 VMware Tools: Running, version:11360 (Guest Managed)

DNS Name: ubuntu-01
 IP Addresses: 192.168.150.21

Host: 10.237.98.168

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

Tag Collection runs every 5 min

Encapsulation: VLAN

Configure Infra Port Groups: To configure port groups

Delimiter:

Enable Tag Collection:

Enable VM folder Data Retrieval (Beta):

Access Mode: Read Only Mode Read Write Mode

Endpoint Retention Time (seconds): 0

VLAN Pool: all-vlans(dynamic)

Create ACI Tags to match vCenter Tags

| Assigned Tag | Category | Description |
|--------------|----------|-------------|
| ad-service | Function | |

Tag Key:

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

Value Operator: Contains Equals Regex

Tag Value:

Tenant → Policies → Endpoint Tags

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

ESG - ad-service

Summary Policy **Operational** Health Faults History

Client Endpoints Contracts Deployed Leaves Tag Selectors

| MAC/IP | Endpoint Name | Learning Source | Hosting Server | Interface (learned) | Encap | Base EPG | Policy Tags |
|-------------------|---------------|-----------------|----------------|-----------------------------------|------------------------------|--|--|
| 00:50:56:A1:73:47 | ubuntu-02 | learned vmm | 10.237.98.166 | Pod-1/Node-101/eth1/30 (learne... | vlan-1053(P) vlan-1054(S) | demo:network-segments:192.168.151.0_24 | __vmm::vmname ubuntu-02 Function ad-service |
| 192.168.151.21 | | | | | | demo:network-segments:192.168.151.0_24 | |
| 00:50:56:A1:78:E4 | ubuntu-03 | learned vmm | 10.237.98.168 | Pod-1/Node-101/eth1/32 (learne... | vlan-1017(P) vlan-1018(S) | demo:network-segments:192.168.152.0_24 | __vmm::vmname ubuntu-03 Function ad-service |
| 192.168.152.21 | | | | | | demo:network-segments:192.168.152.0_24 | |
| 00:50:56:A1:83:A5 | ubuntu-01 | learned vmm | 10.237.98.168 | Pod-1/Node-101/eth1/32 (learne... | vlan-1081(P) vlan-1083(S) | demo:network-segments:192.168.150.0_24 | __vmm::vmname ubuntu-01 Function ad-service |
| | | | | | | demo:network-segments:192.168.150.0_24 | |

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

Static endpoint mapping...

Static Policy Tags on APIC

Static Endpoints

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

IP address ranges

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

MAC addresses

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

IP addresses

- Endpoint IP
 - 192.168.150.21
 - 192.168.151.21
 - 192.168.152.21

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

online-boutique

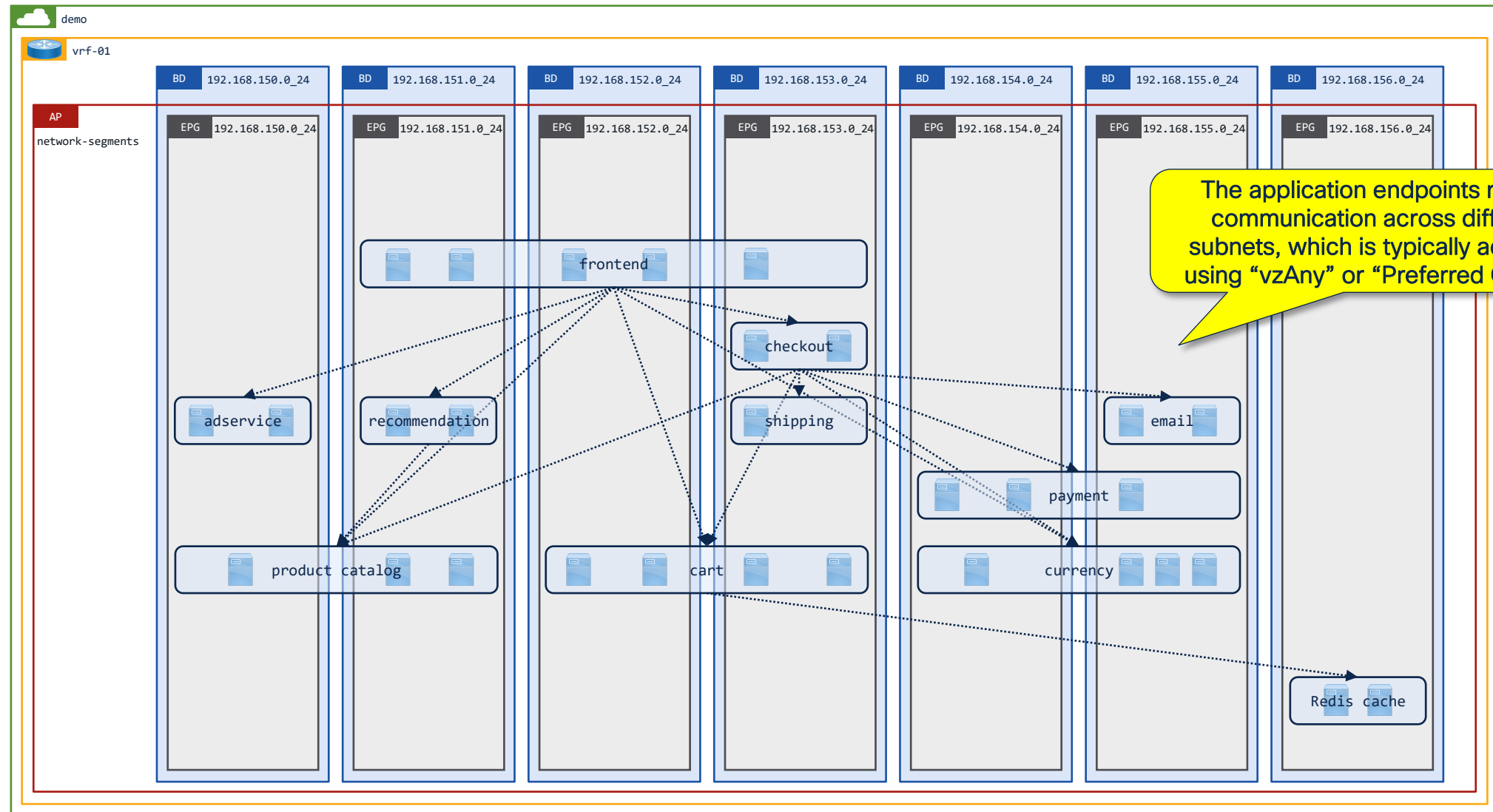
- Application EPGs
- uSeg EPGs
- Endpoint Security Groups
 - ad-service
 - Contracts
 - Selectors
 - Tag Selectors
 - EPG Selectors
 - IP Subnet Selectors
 - Service EPG Selectors

| Associated Object |
|---|
| 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-[*] |

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

Allowing open
communication...

Existing applications typically require unrestricted 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...?)

vzAny

demo ⏪ ☰ 🔄

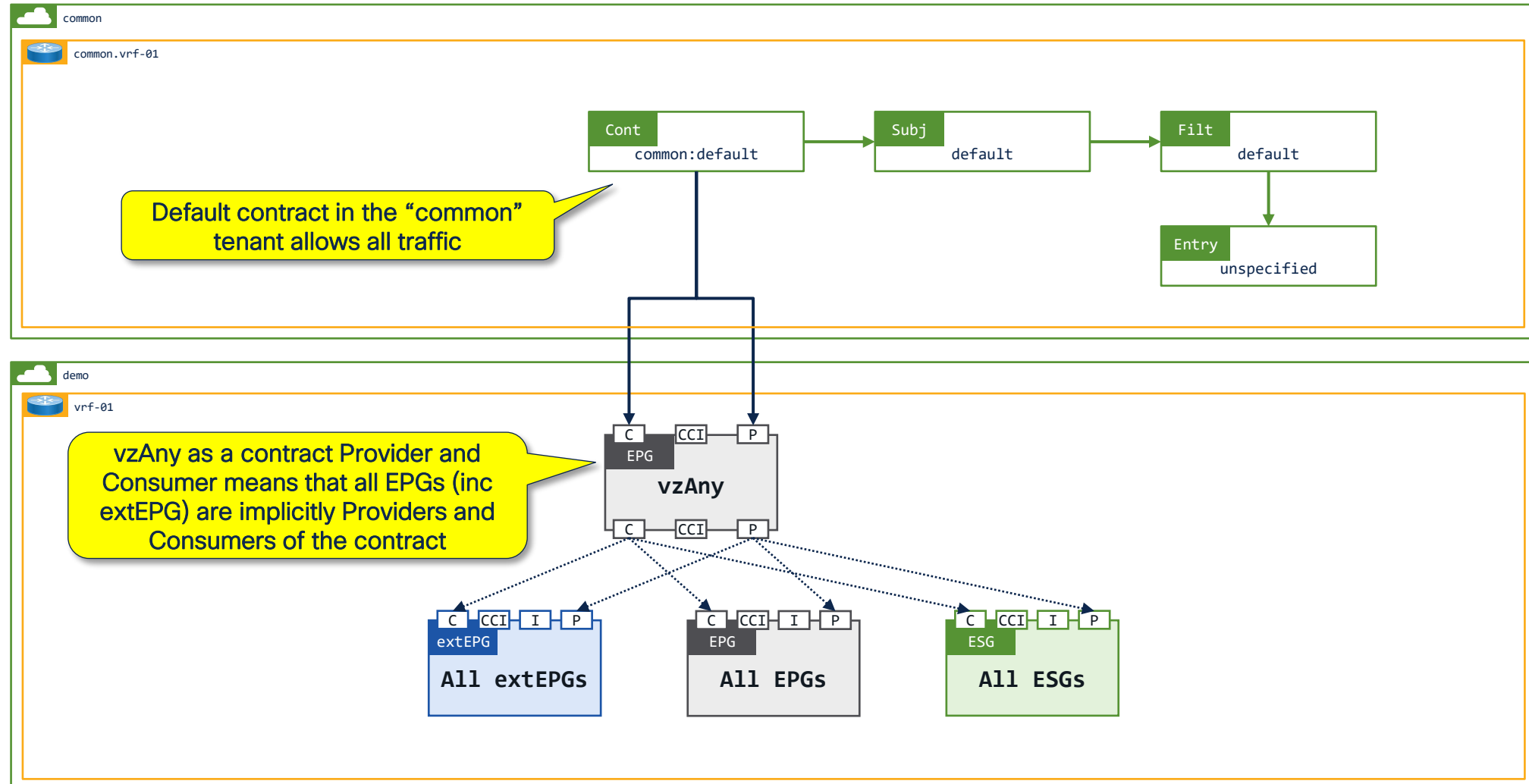
- > 🎬 Quick Start
- ▼ 🏠 demo
 - > 📁 Application Profiles
 - ▼ 📁 Networking
 - > 📁 Bridge Domains
 - ▼ 📁 VRFs
 - ▼ ☁️ vrf-01
 - 📁 Multicast
 - 📁 Multicast IPv6
 - > 📁 Inter-VRF Leaked Routes for ESG
 - 🔗 EPG|ESG Collection for VRF

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...!

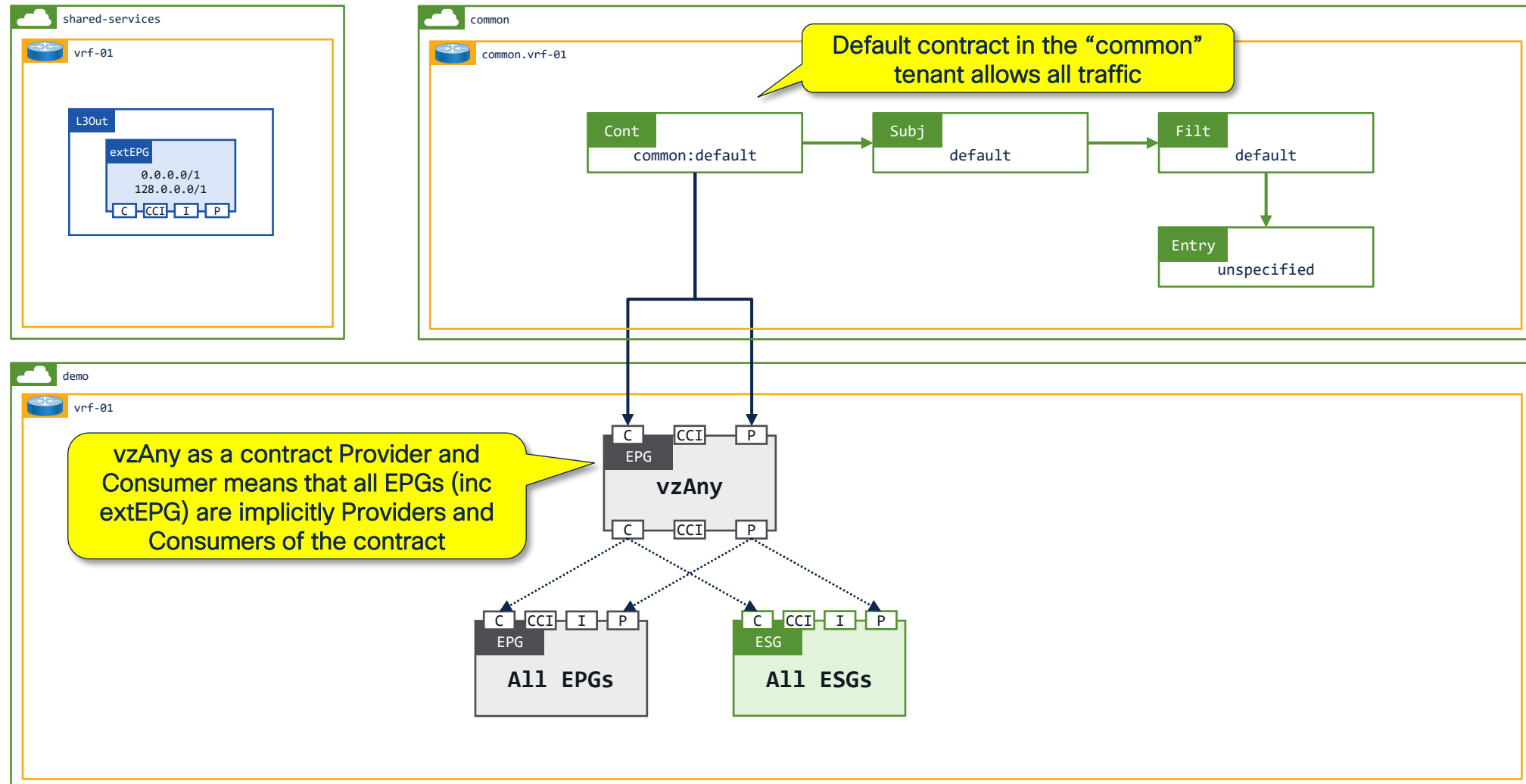
vzAny operation – consumer and provider

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



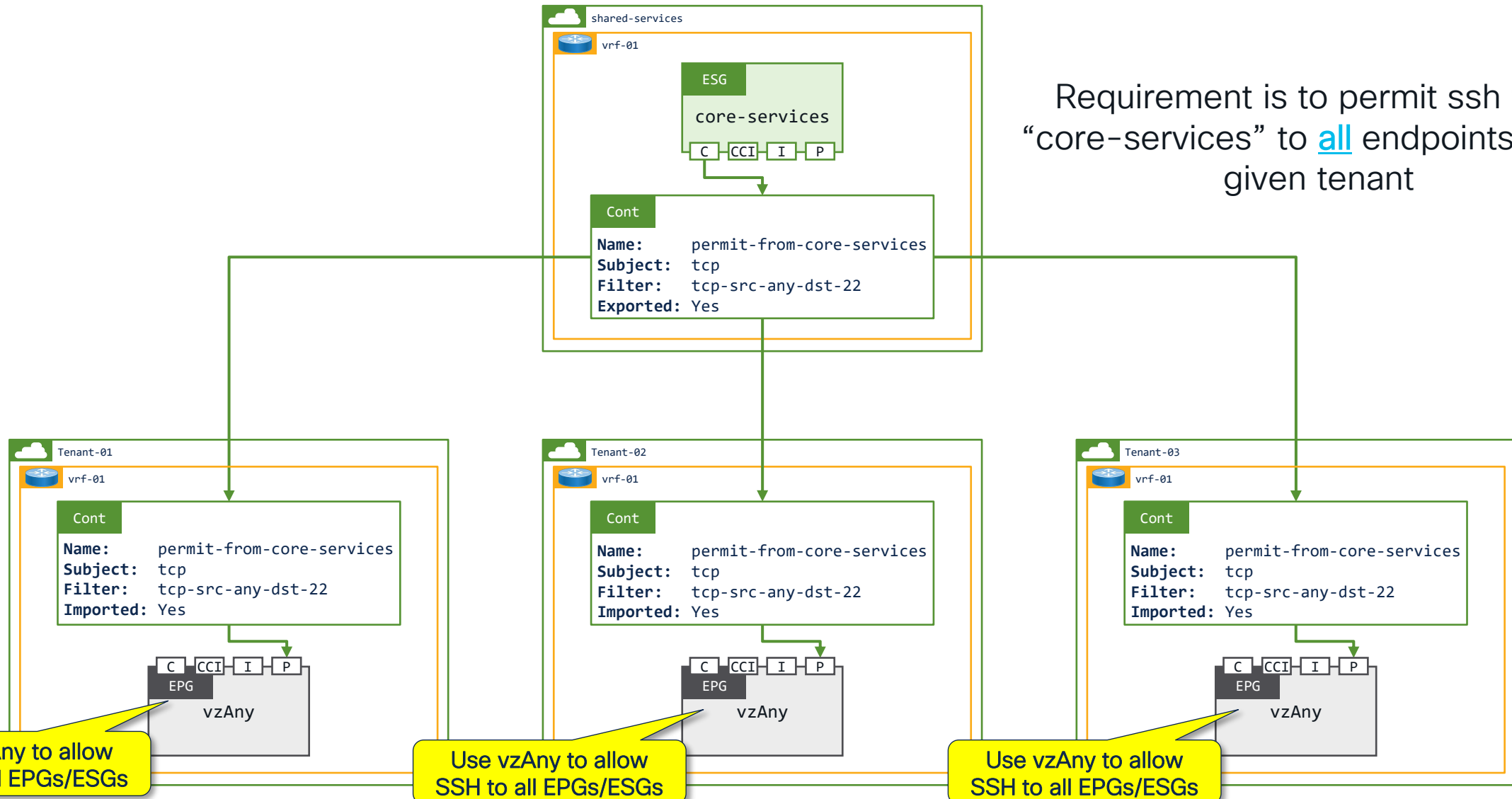
vzAny operation – consumer and provider

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



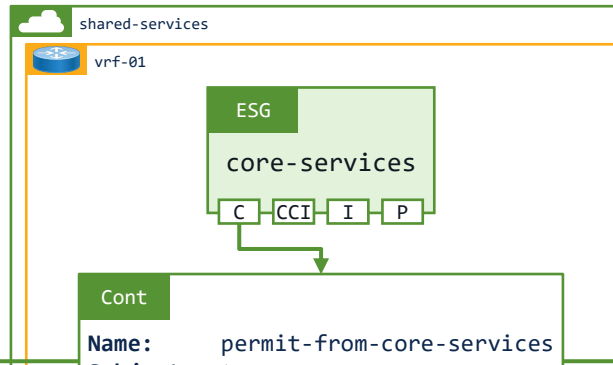
vzAny cannot be a Provider for Shared Services

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



vzAny cannot be a Provider for Shared Services

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



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 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:

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

This block contains two screenshots from the Cisco GUI. The left screenshot shows a VRF named 'vrf-01' with a 'Preferred Group' containing three Bridge Domains (BDs) and their corresponding EPGs. A yellow callout bubble points to this group with the text: "There is only one preferred group per VRF". The right screenshot shows the 'VRF - vrf-01' configuration page. The 'Preferred Group' setting is highlighted with a red box and a yellow callout bubble that says: "Enable Preferred Group on VRF".

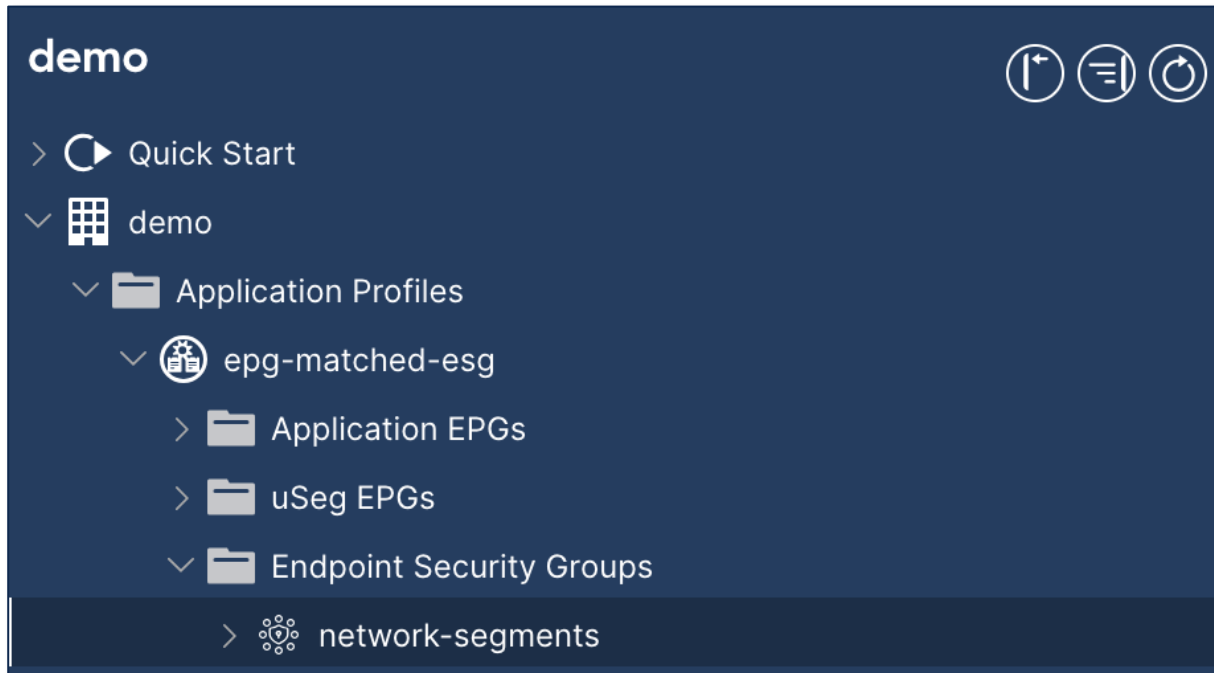
Typical "Network Centric" mode deployment where there is a 1:1 mapping between Bridge Domains and EPGs

This block contains three screenshots of EPG configuration pages. Each screenshot shows the 'Preferred Group Member' setting with the 'Include' option selected. Yellow callout bubbles identify the 'pcTag' values for each EPG: 'pcTag 49160' for the first EPG, 'pcTag 49159' for the second, and 'pcTag 16393' for the third. A yellow callout bubble also points to the 'Include' selection in the first screenshot with the text: "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”

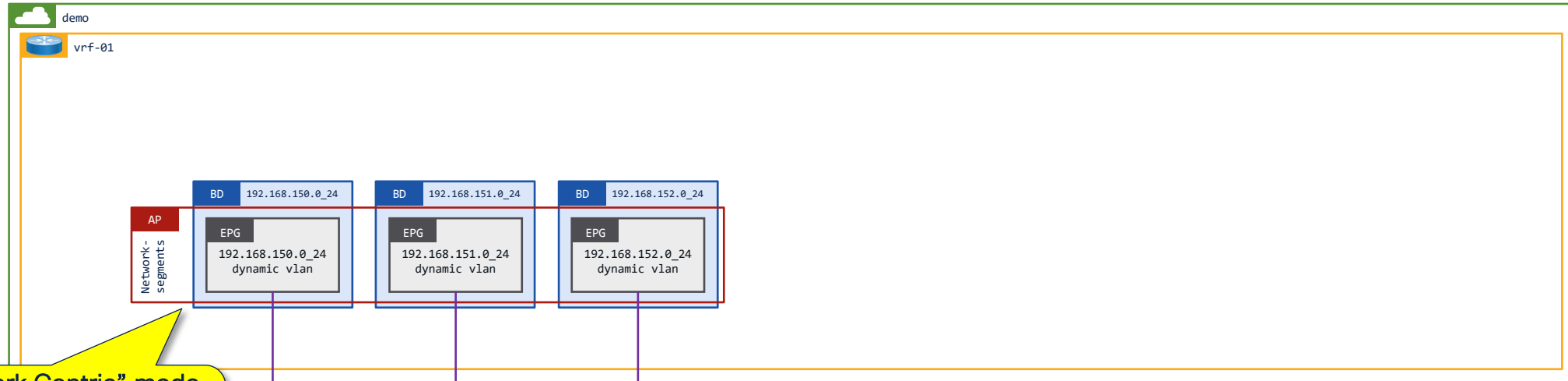
All EPGs mapped to a single ESG



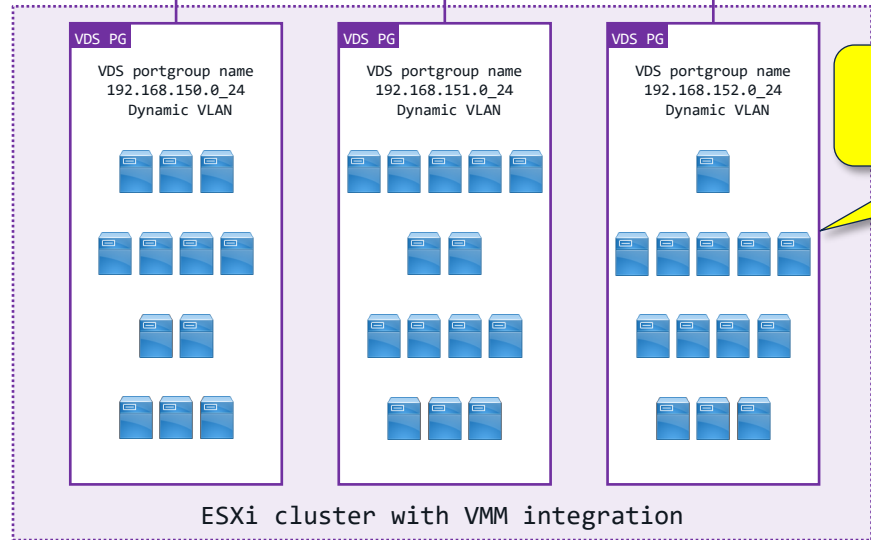
Two step process...

1) Enable uSegmentation, 2) Map EPGs to a 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

Enable Endpoint Security Groups

The image displays three screenshots of the Cisco ICM GUI, illustrating the configuration of Endpoint Security Groups for different host types. Each screenshot shows a table of domains with columns for Domain, Type, Deployment, Resolution, Allow Micro-Segmentation, Primary VLAN, Port Encap, Switching Mode, Encap Mode, Cos Value, Enhanced Lag Policy, and Custom EPG Name.

Top Screenshot: Shows a domain configuration where 'Allow Micro-Segmentation' is set to 'True'. A yellow callout points to the 'Port Encap' column, stating: "Primary/Port Encap VLANs not required for directly attached hosts".

Middle Screenshot: Shows a similar domain configuration. A yellow callout points to the 'Primary VLAN' column, stating: "Static Primary / Encap VLANs are required when there is an intermediary switching layer such as UCS FIs".

Bottom Screenshot: Shows a domain configuration where 'Allow Micro-Segmentation' is set to 'True'. A yellow callout points to the 'Primary VLAN' column, stating: "Static Primary / Encap VLANs are required when there is an intermediary switching layer such as UCS FIs".

Each EPG has a unique security Tag (pcTag)

The screenshot shows the configuration page for EPG - 192.168.150.0_24. A yellow callout bubble points to the EPG name in the left sidebar, labeled "pcTag: 32771". Another yellow callout bubble points to the "pcTag(sclass)" field in the Properties section, which is highlighted with a red box and contains the value "32771". The "uSeg EPG" field is set to "false".

The screenshot shows the configuration page for EPG - 192.168.151.0_24. A yellow callout bubble points to the EPG name in the left sidebar, labeled "pcTag: 49155". Another yellow callout bubble points to the "pcTag(sclass)" field in the Properties section, which is highlighted with a red box and contains the value "49155". The "uSeg EPG" field is set to "false".

The screenshot shows the configuration page for EPG - 192.168.152.0_24. A yellow callout bubble points to the EPG name in the left sidebar, labeled "pcTag: 16390". Another yellow callout bubble points to the "pcTag(sclass)" field in the Properties section, which is highlighted with a red box and contains the value "16390". The "uSeg EPG" field is set to "false".

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

plus, it 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

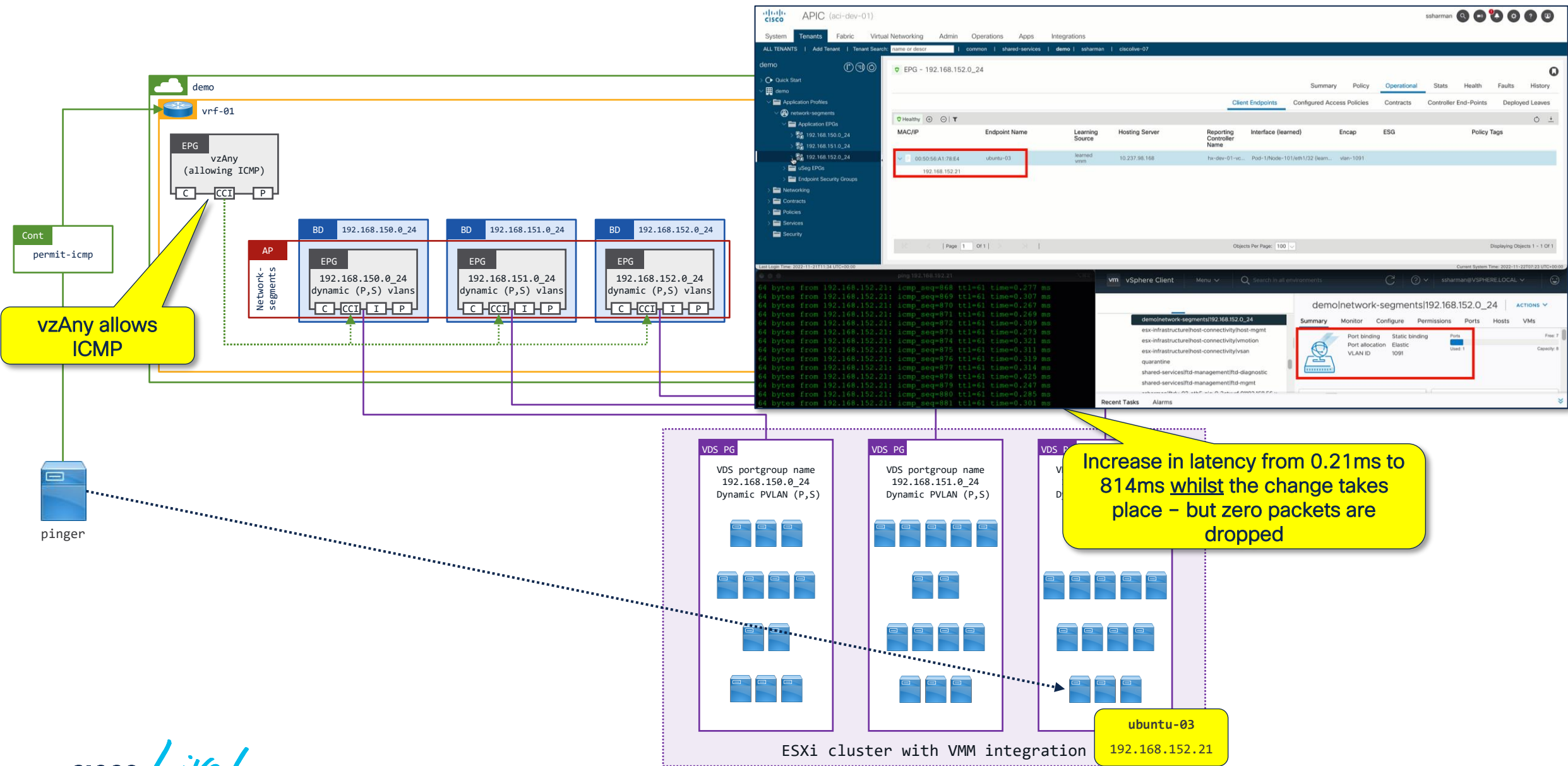
Distributed switch ucsc-c220m5-vds-01

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 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 | ssharman | ciscolive-07 | ciscolive-08

demo

Application Profiles

Quick Start

demo

Application Profiles

network-segments

Networking

Contracts

Policies

Services

Security

Create Application Profile

Delete

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 | ssharman

demo

Application Profiles

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 |
|------|-------|----|--------|----------------|-------------|------------------|-------------------|-------------------|
|------|-------|----|--------|----------------|-------------|------------------|-------------------|-------------------|

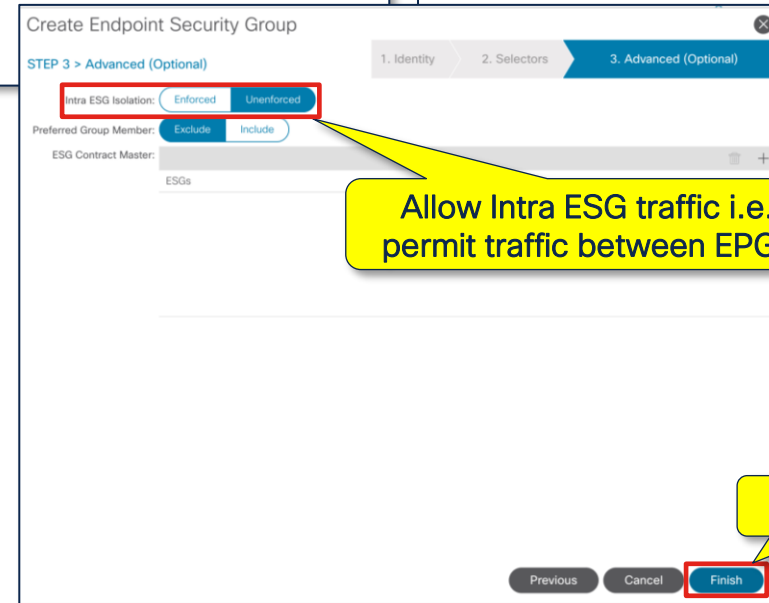
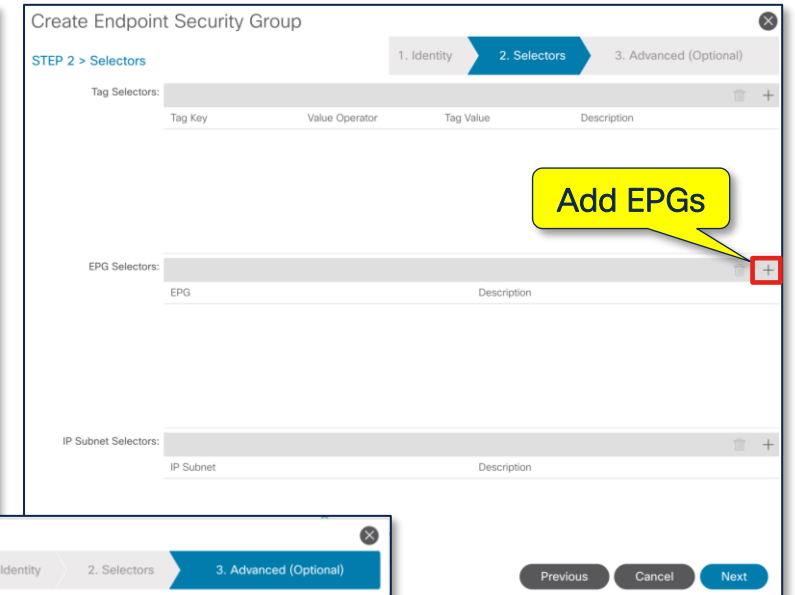
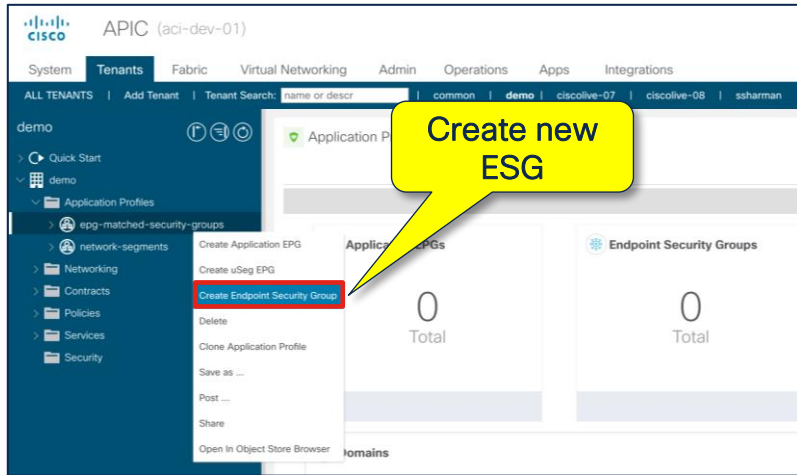
Cancel Submit

New Application Profile for Security Groups

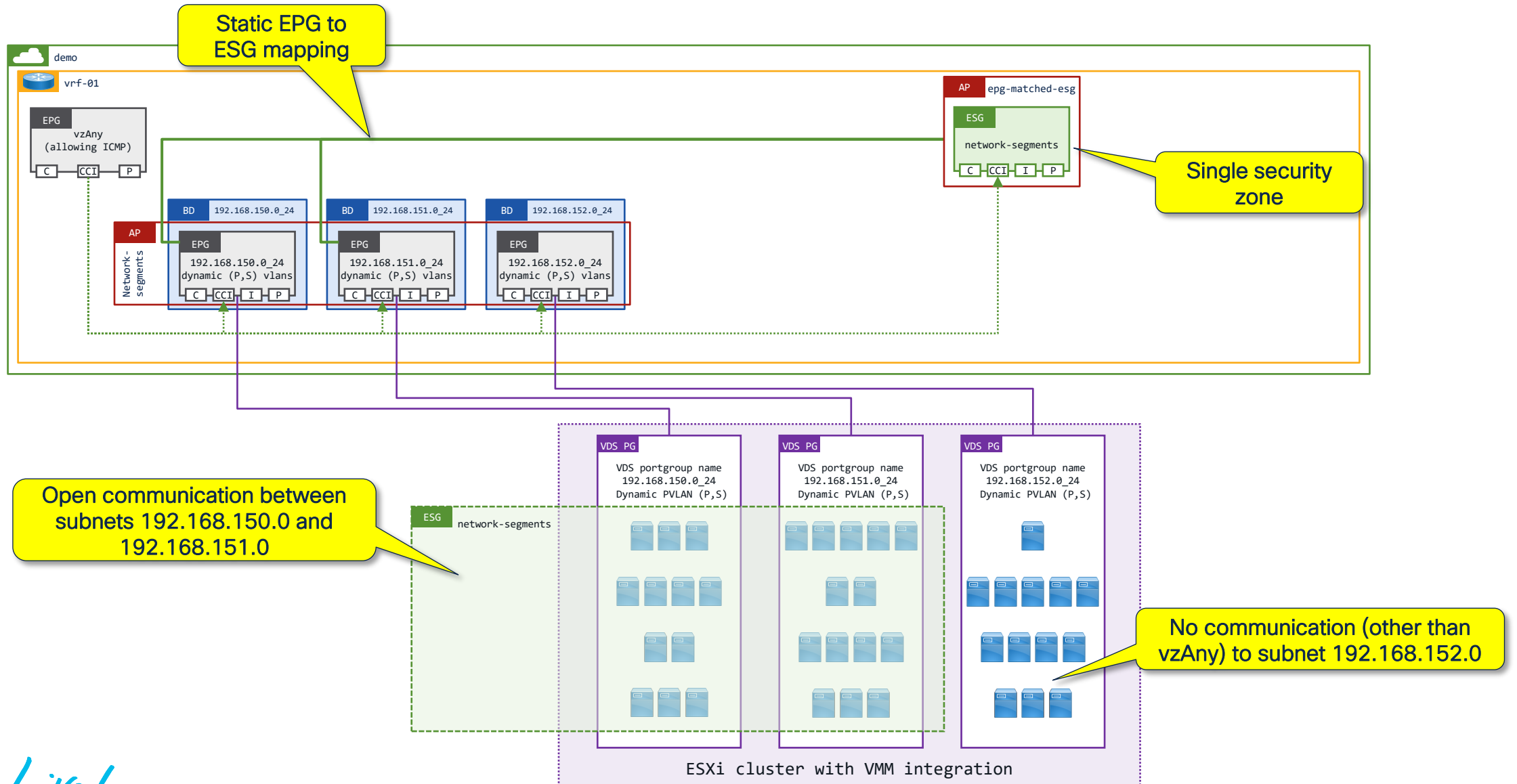
epg-matched-security-groups

Do not create EPGs

Create a new ESG for Network Segments (EPGs)



Open communication within the ESG...



Matched EPGs now classified with a common pcTag

demo

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

EPG - 192.168.150.0_24 (Matched)

Properties

Name: 192.168.150.0_24

Alias:

Description: optional

Annotations: Click to add a new annotation

Global Alias:

uSeg EPG: false

pcTag(class): 31

Contract Exception Tag:

QoS class: Level3 (Default)

Custom QoS: select a value

Data-Plane Policer: select a value

Intra EPG Isolation: Enforced Unenforced

Preferred Group Member: Exclude Include

Flood in Encapsulation: Disabled Enabled

Configuration Status: applied

Configuration Issues:

Label Match Criteria: AtleastOne

Bridge Domain: 192.168.150.0_24

Resolved Bridge Domain: demo/192.168.150.0_24

Monitoring Policy: select a value

FHS Trust Control Policy: select a value

EPG Admin State: Admin Up Admin Shut

EPG Contract Master:

Application EPGs

pcTag: 31

demo

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

EPG - 192.168.151.0_24 (Matched)

Properties

Name: 192.168.151.0_24

Alias:

Description: optional

Annotations: Click to add a new annotation

Global Alias:

uSeg EPG: false

pcTag(class): 31

Contract Exception Tag:

QoS class: Level3 (Default)

Custom QoS: select a value

Data-Plane Policer: select a value

Intra EPG Isolation: Enforced Unenforced

Preferred Group Member: Exclude Include

Flood in Encapsulation: Disabled Enabled

Configuration Status: applied

Configuration Issues:

Label Match Criteria: AtleastOne

Bridge Domain: 192.168.151.0_24

Resolved Bridge Domain: demo/192.168.151.0_24

Monitoring Policy: select a value

FHS Trust Control Policy: select a value

EPG Admin State: Admin Up Admin Shut

EPG Contract Master:

Application EPGs

pcTag: 31

demo

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

EPG - 192.168.152.0_24

Properties

Name: 192.168.152.0_24

Alias:

Description: optional

Annotations: Click to add a new annotation

Global Alias:

uSeg EPG: false

pcTag(class): 49157

Contract Exception Tag:

QoS class: Level3 (Default)

Custom QoS: select a value

Data-Plane Policer: select a value

Intra EPG Isolation: Enforced Unenforced

Preferred Group Member: Exclude Include

Flood in Encapsulation: Disabled Enabled

Configuration Status: applied

Configuration Issues:

Label Match Criteria: AtleastOne

Bridge Domain: 192.168.152.0_24

Resolved Bridge Domain: demo/192.168.152.0_24

Monitoring Policy: select a value

FHS Trust Control Policy: select a value

EPG Admin State: Admin Up Admin Shut

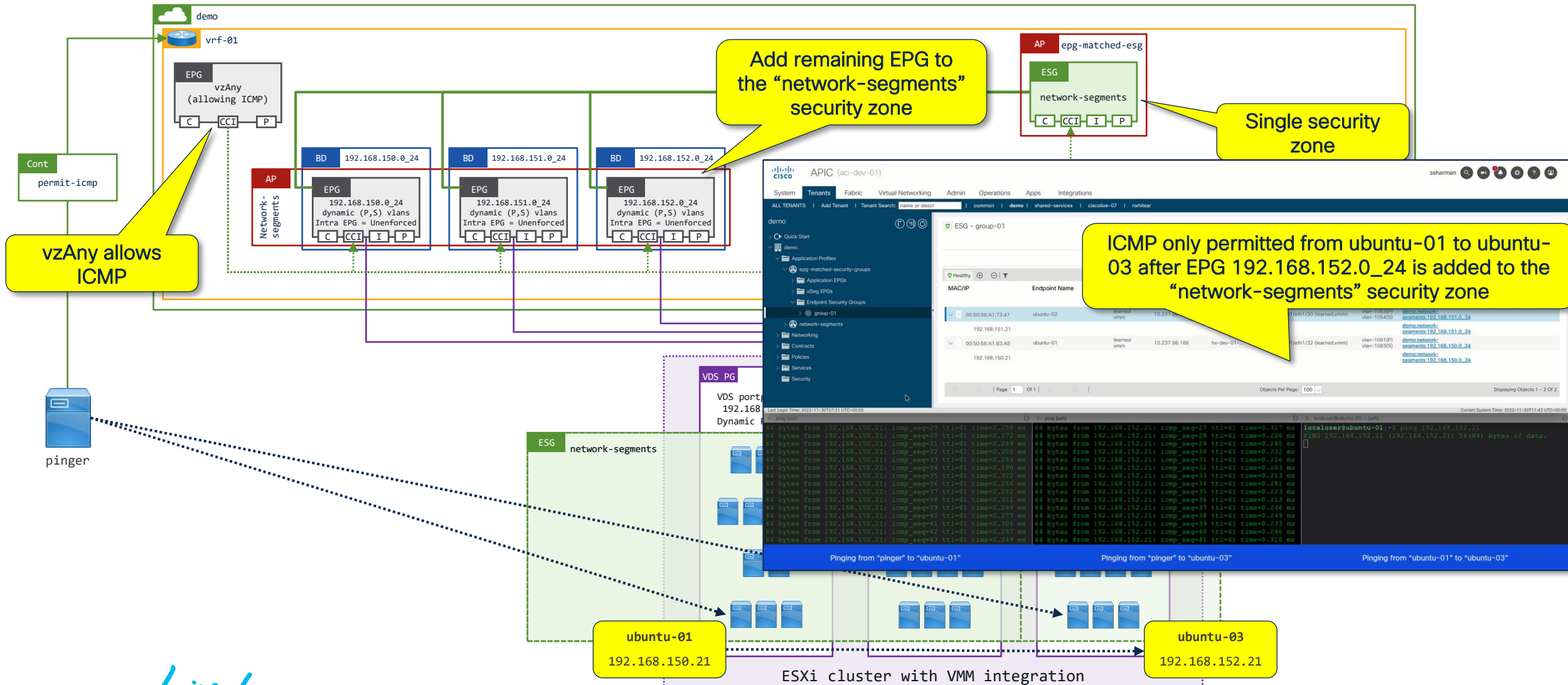
EPG Contract Master:

Application EPGs

pcTag: 49157

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

Add remaining EPG to Single Security Zone



Add remaining EPG to the "network-segments" security zone

Single security zone

vzAny allows ICMP

ICMP only permitted from ubuntu-01 to ubuntu-03 after EPG 192.168.152.0_24 is added to the "network-segments" security zone

All EPGs now classified with a common pcTag

demo

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

EPG - 192.168.150.0_24 (Matched Security Group)

Properties

Name: 192.168.150.0_24

Alias:

Description: optional

Annotations: Click to add a new annotation

Global Alias:

uSeg EPG: false

pcTag(class): 31

Contract Exception Tag:

QoS class: Level3 (Default)

Custom QoS: select a value

Data-Plane Policier: select a value

Intra EPG Isolation: Enforced Unenforced

Preferred Group Member: Exclude Include

Flood in Encapsulation: Disabled Enabled

Configuration Status: applied

Configuration Issues:

Label Match Criteria: AtleastOne

Bridge Domain: 192.168.150.0_24

Resolved Bridge Domain: demo/192.168.150.0_24

Monitoring Policy: select a value

FHS Trust Control Policy: select a value

EPG Admin State: Admin Up Admin Shut

EPG Contract Master:

Application EPGs

demo

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

EPG - 192.168.151.0_24 (Matched Security Group)

Properties

Name: 192.168.151.0_24

Alias:

Description: optional

Annotations: Click to add a new annotation

Global Alias:

uSeg EPG: false

pcTag(class): 31

Contract Exception Tag:

QoS class: Level3 (Default)

Custom QoS: select a value

Data-Plane Policier: select a value

Intra EPG Isolation: Enforced Unenforced

Preferred Group Member: Exclude Include

Flood in Encapsulation: Disabled Enabled

Configuration Status: applied

Configuration Issues:

Label Match Criteria: AtleastOne

Bridge Domain: 192.168.151.0_24

Resolved Bridge Domain: demo/192.168.151.0_24

Monitoring Policy: select a value

FHS Trust Control Policy: select a value

EPG Admin State: Admin Up Admin Shut

EPG Contract Master:

Application EPGs

demo

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

EPG - 192.168.152.0_24 (Matched Security Group)

Properties

Name: 192.168.152.0_24

Alias:

Description: optional

Annotations: Click to add a new annotation

Global Alias:

uSeg EPG: false

pcTag(class): 31

Contract Exception Tag:

QoS class: Level3 (Default)

Custom QoS: select a value

Data-Plane Policier: select a value

Intra EPG Isolation: Enforced Unenforced

Preferred Group Member: Exclude Include

Flood in Encapsulation: Disabled Enabled

Configuration Status: applied

Configuration Issues:

Label Match Criteria: AtleastOne

Bridge Domain: 192.168.152.0_24

Resolved Bridge Domain: demo/192.168.152.0_24

Monitoring Policy: select a value

FHS Trust Control Policy: select a value

EPG Admin State: Admin Up Admin Shut

EPG Contract Master:

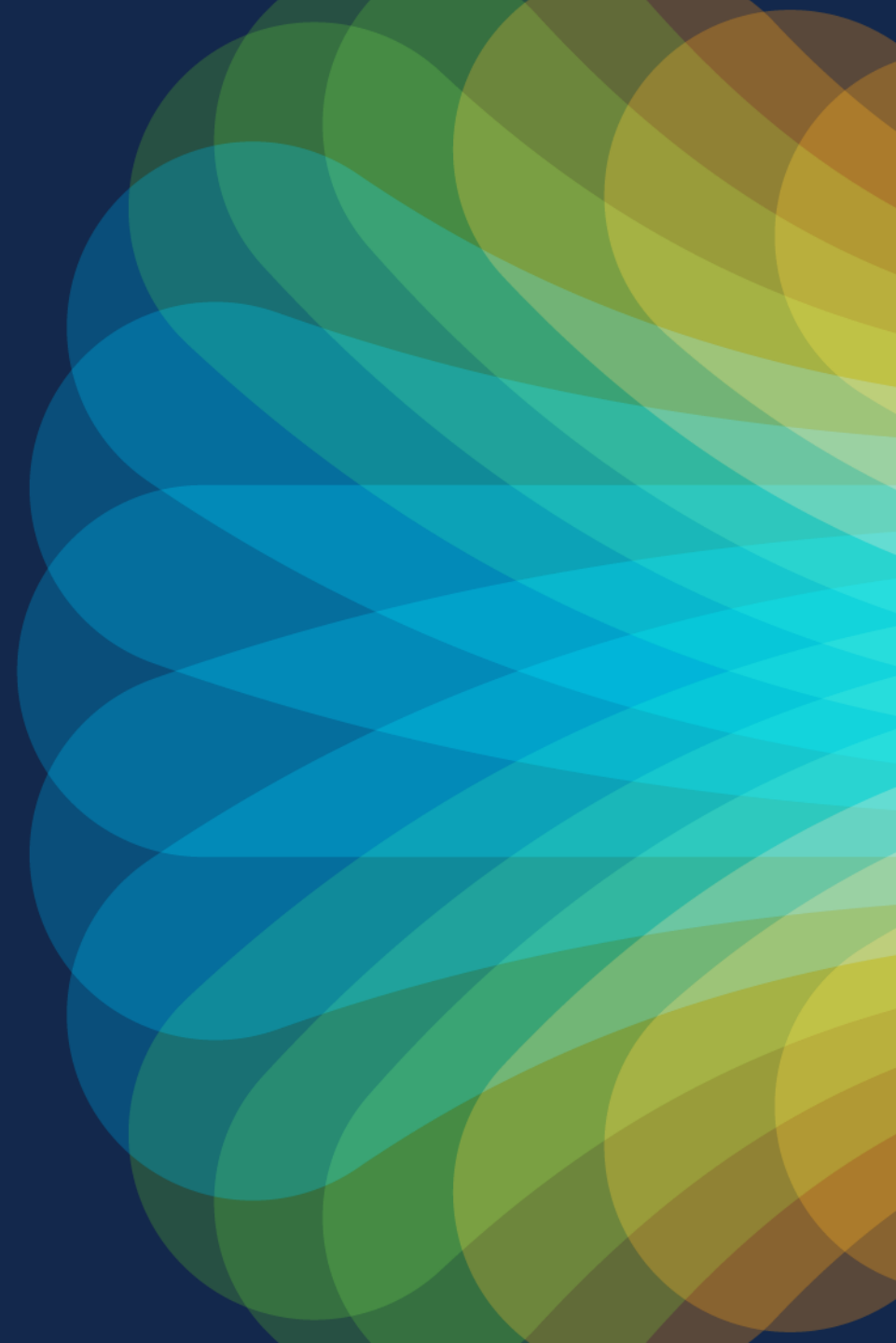
Application EPGs

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

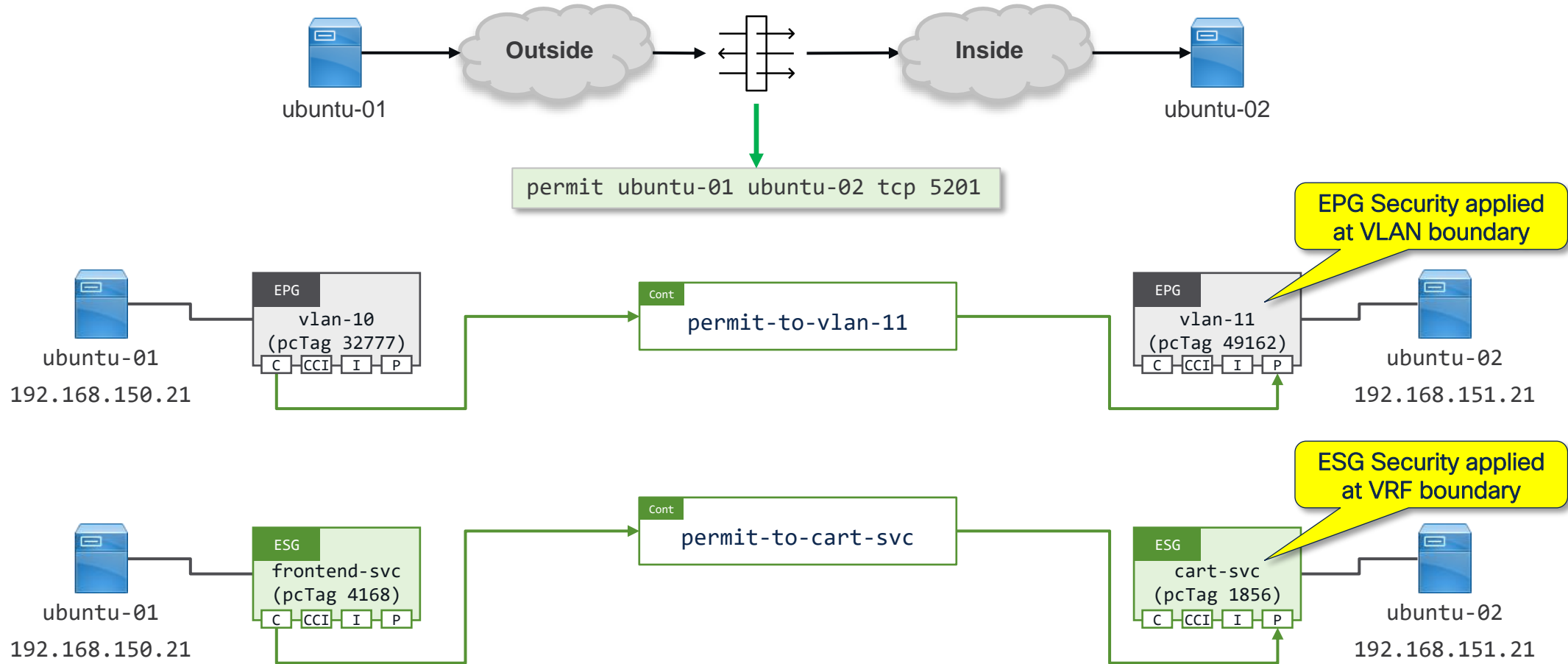
* Assumes 1:1 mapping between Bridge Domain and EPG. ESGs can mapping can also be performed on IP subnets

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

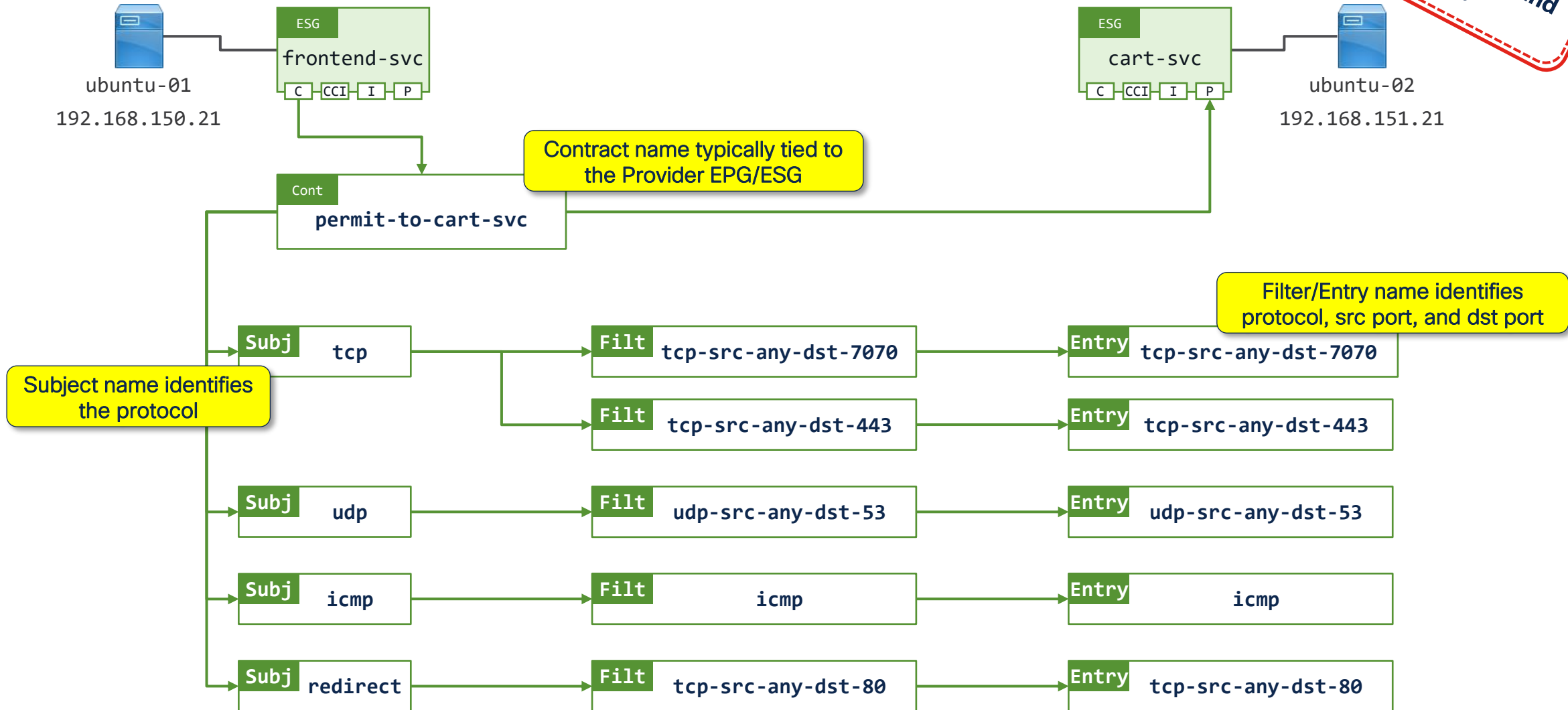
Consumer and Provider relationships are there to help you visualize the traffic flow direction

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



Contract Scope

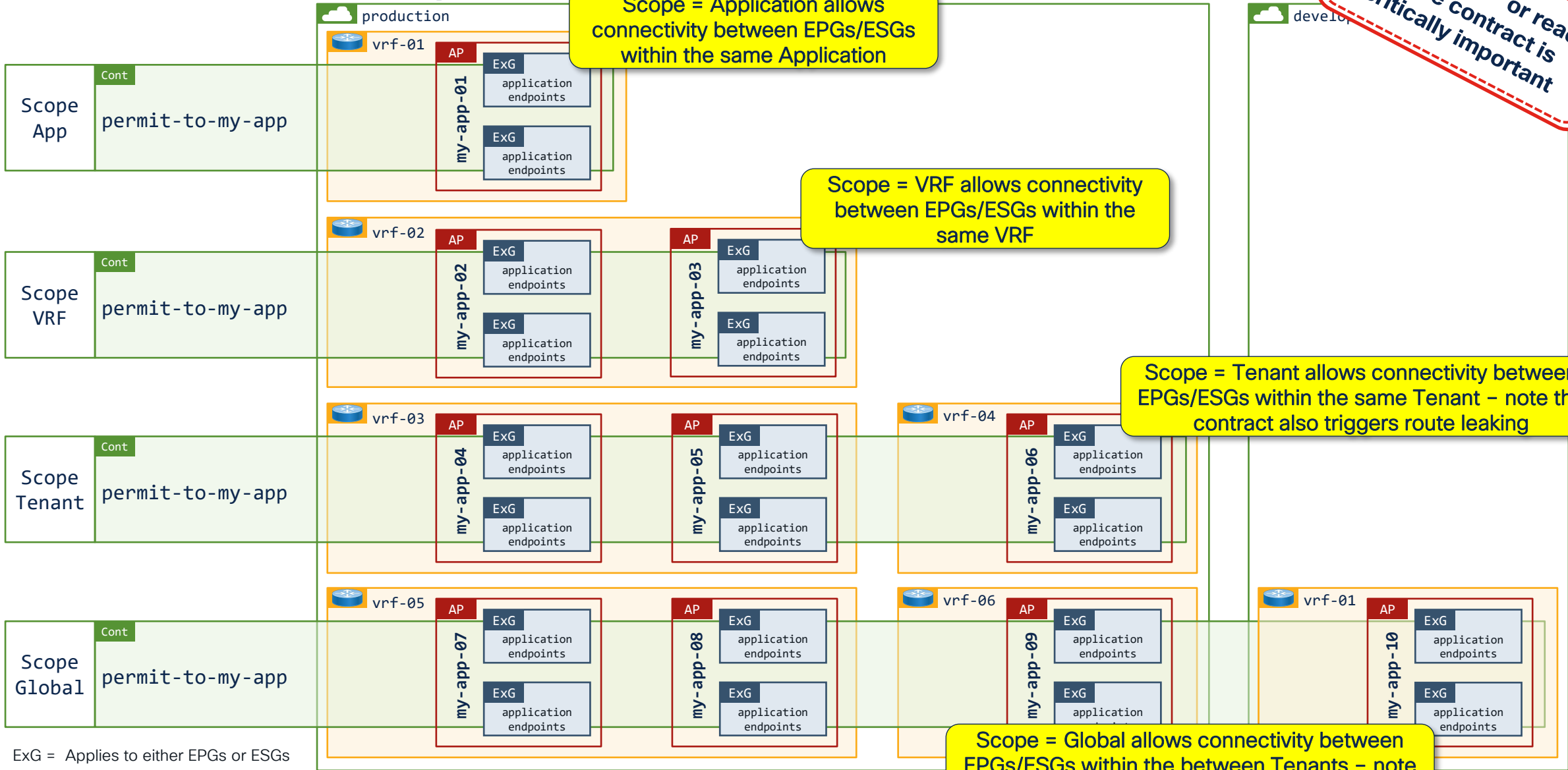
The "Scope" or reach of the contract is critically important

Scope = Application allows connectivity between EPGs/ESGs within the same Application

Scope = VRF allows connectivity between EPGs/ESGs within the same VRF

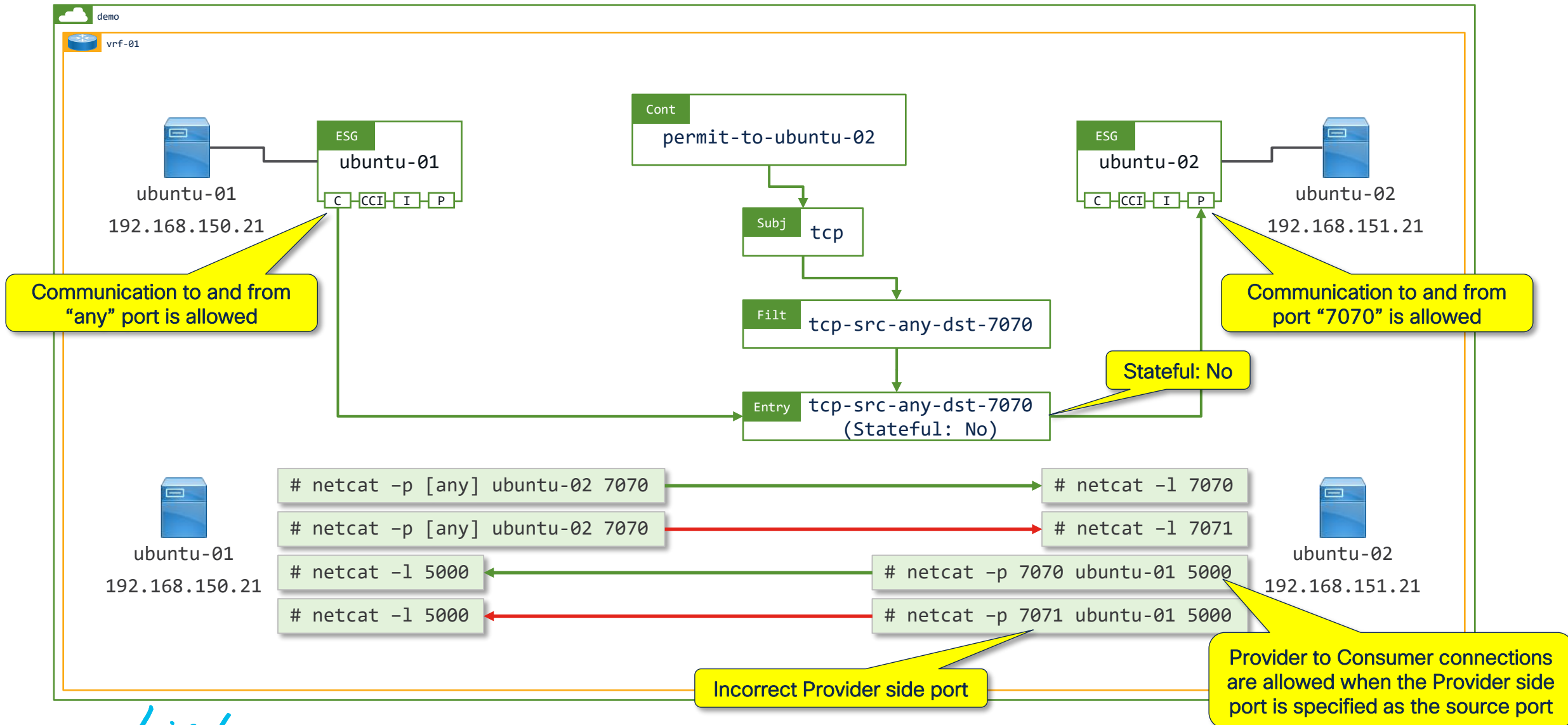
Scope = Tenant allows connectivity between EPGs/ESGs within the same Tenant - note the contract also triggers route leaking

Scope = Global allows connectivity between EPGs/ESGs within the between Tenants - note the contract also triggers route leaking

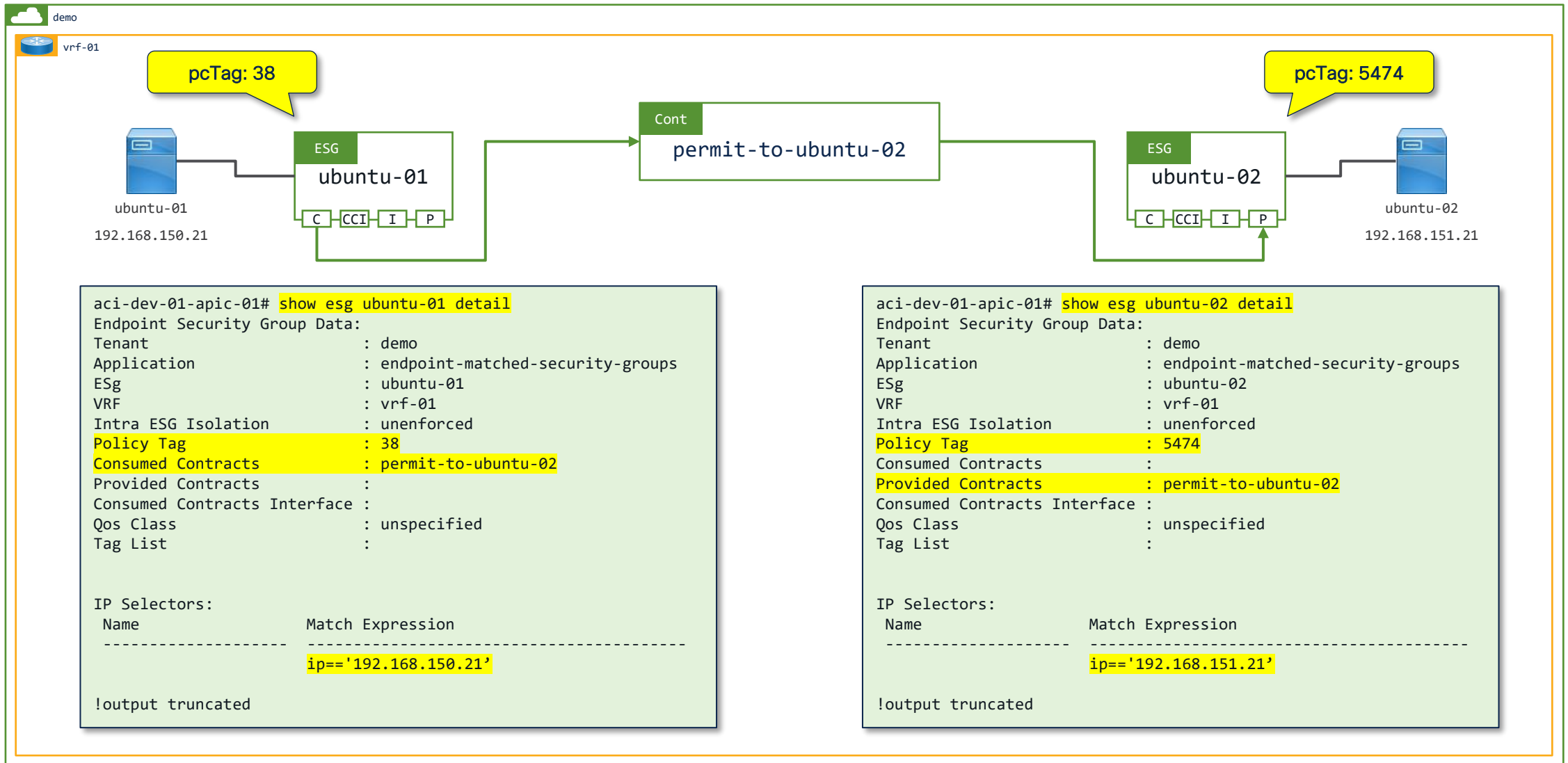


ExG = Applies to either EPGs or ESGs

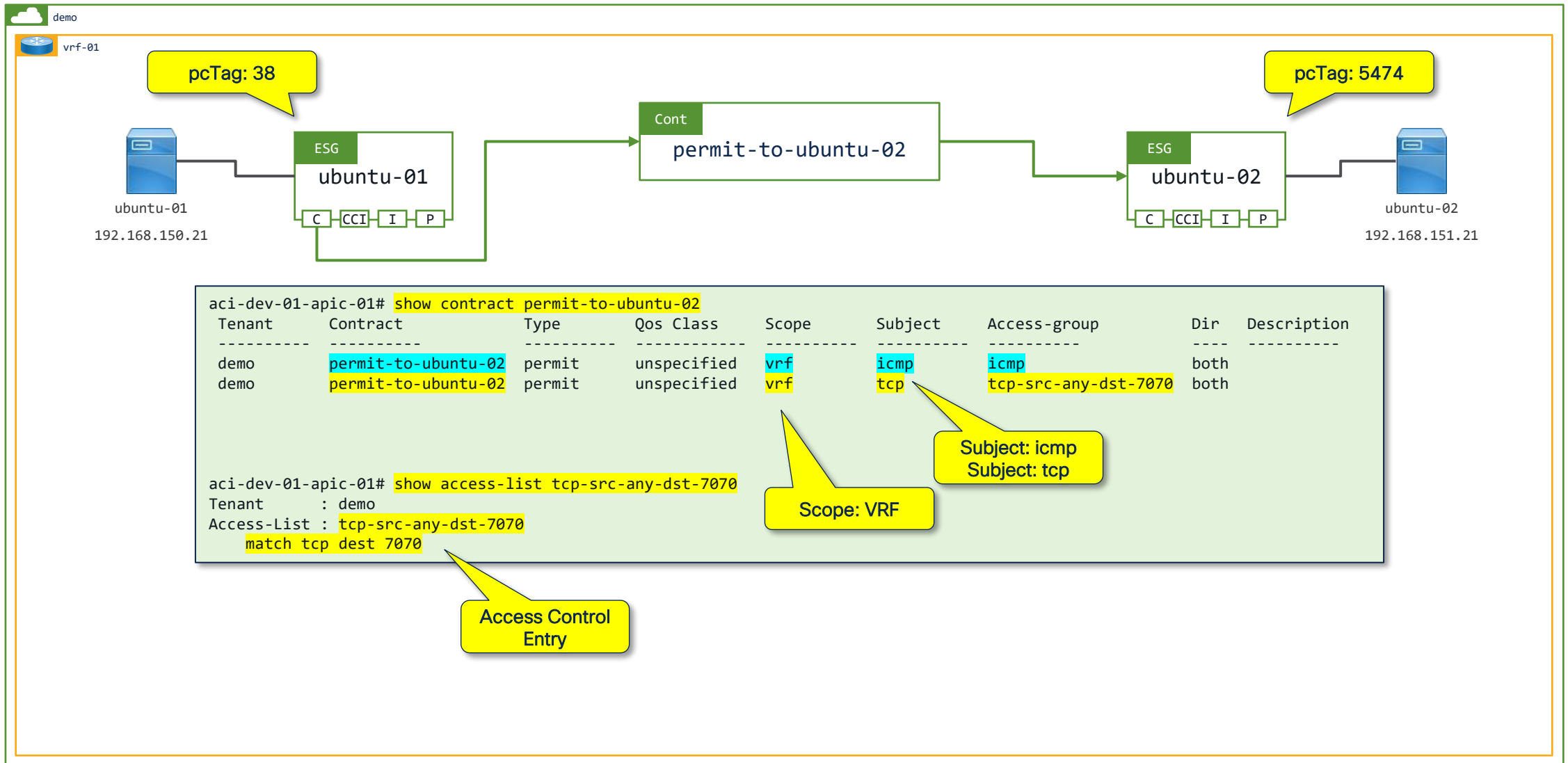
Verifying Contract operation with netcat – Stateful = No



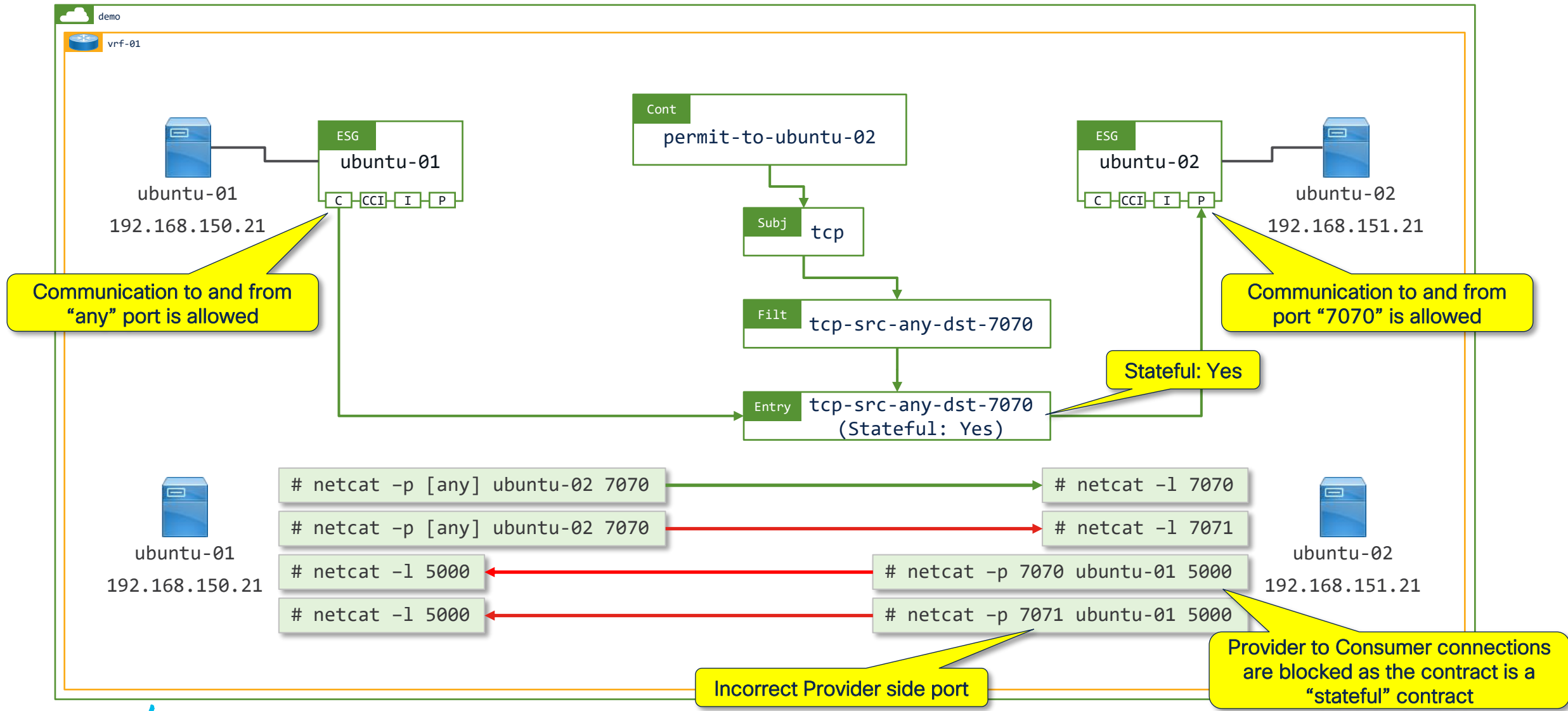
Verifying Contract Operation: EPG/ESG details



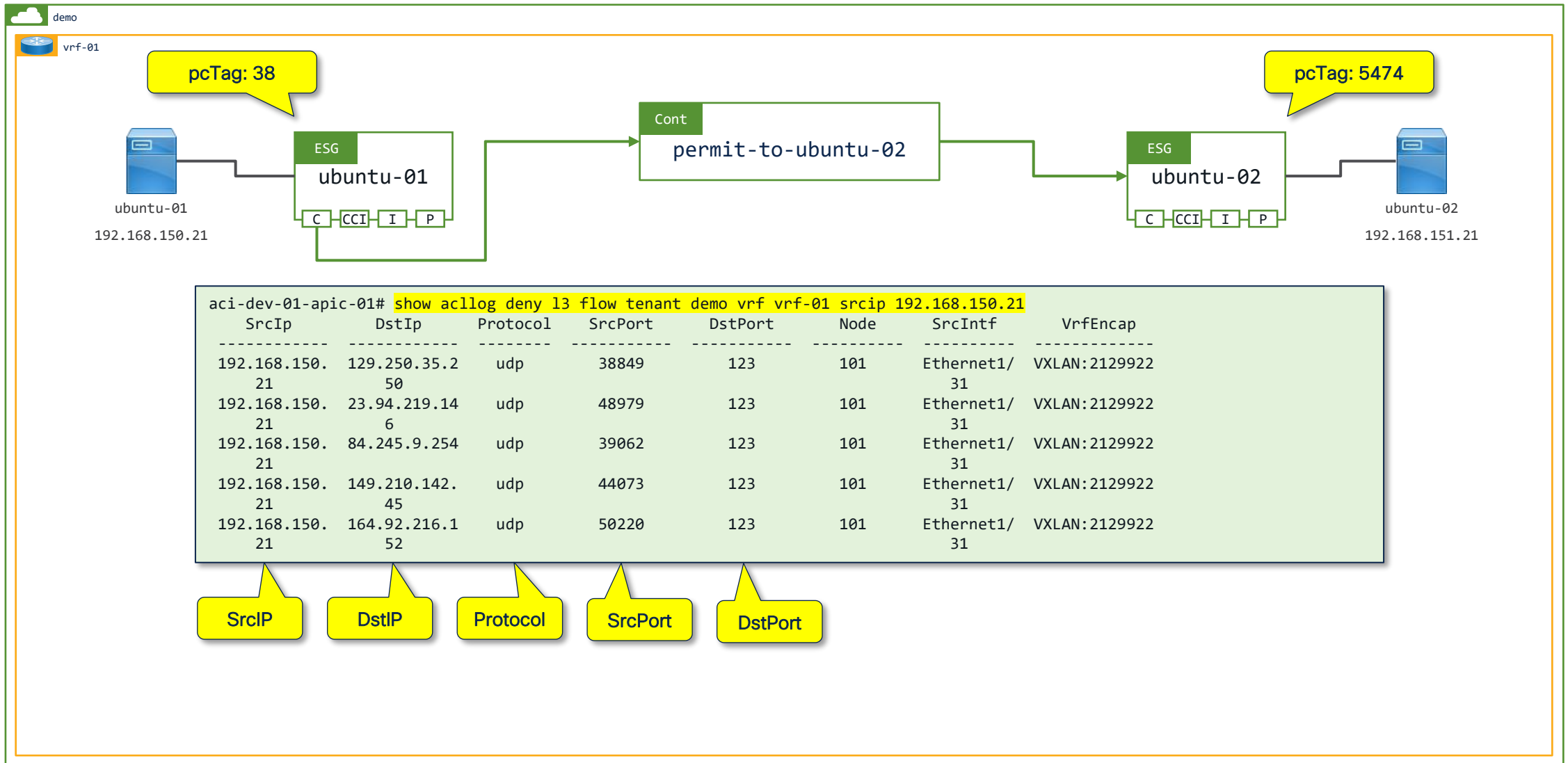
Verifying Contract Operation: Contract details



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 interface, showing a search for messages with the filter "message: 'demo:vrf-01'". A message count graph and a list of messages are visible, with one message selected and its details shown in a table.

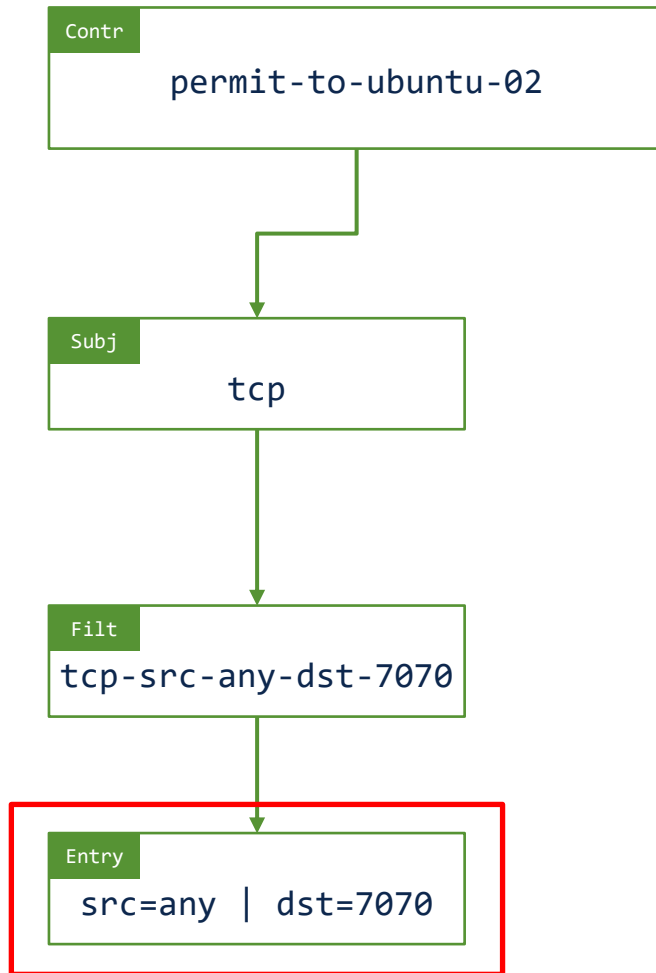
The foreground screenshot is the Cisco APIC (aci-dev-605) interface, specifically the ELAM Assistant configuration page. It shows the configuration for capturing a packet with ELAM (Embedded Logic Analyzer Module) on nodes node-101 and node-102. The configuration includes a search filter "tn-demo-online-boutique" and a table of VxLAN (outer) headers.

| 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, a "Packet Forwarding Information" window is open, showing the following details:

| 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...!



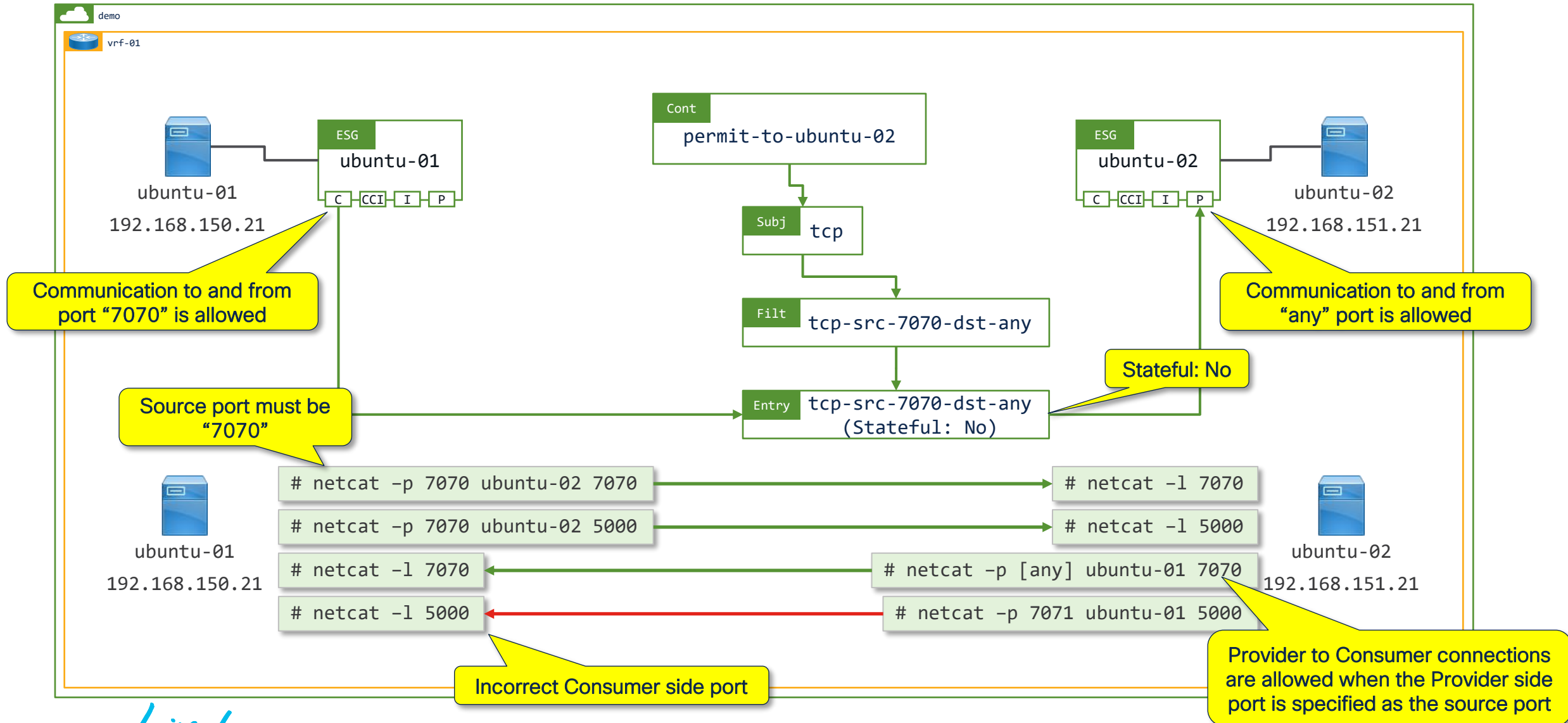
Filter Entry source port =
port opened on the consumer EPG/ESG

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



**Getting into
the weeds...!**

Reversing the Filter ports - Stateful = No

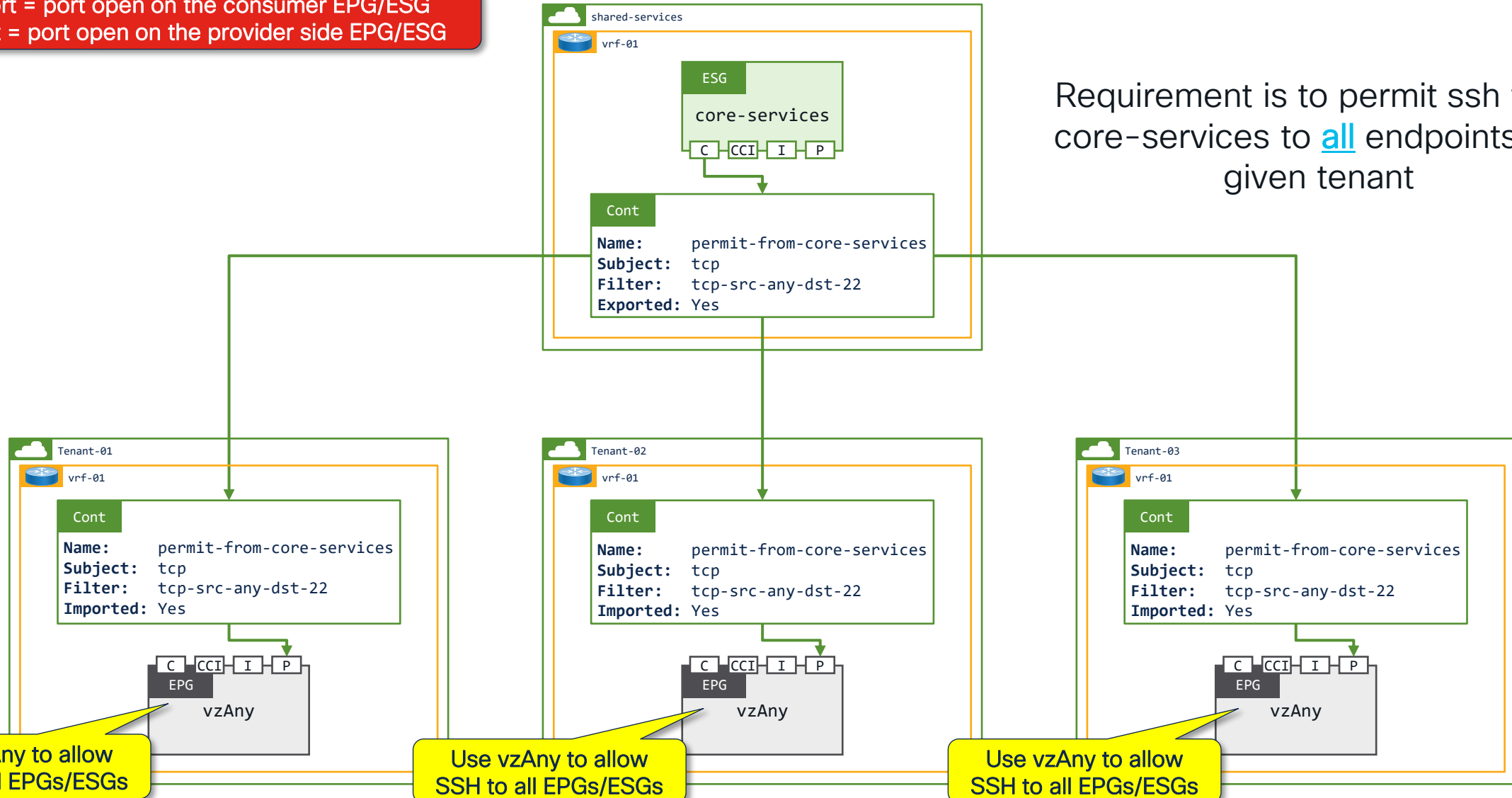


Why would you want to reverse the Consumer and Provider Filters...?

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 a given tenant



Use vzAny to allow SSH to all EPGs/ESGs

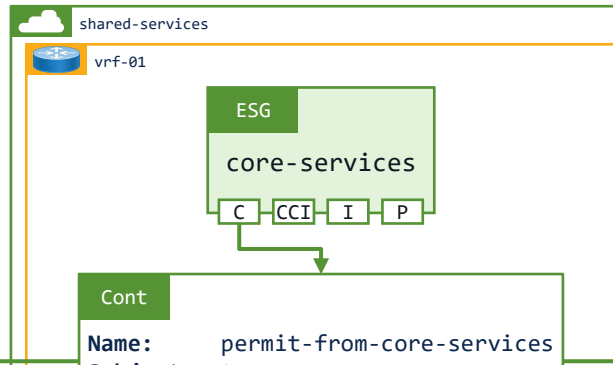
Use vzAny to allow SSH to all EPGs/ESGs

Use vzAny to allow SSH to all EPGs/ESGs

vzAny as a contract 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



The screenshot shows the Cisco GUI configuration page for 'vzAny'. The 'Policy' tab is selected, and the 'General' sub-tab is active. A 'Status' dialog box is open, displaying an error message: 'Error: 400 - vzAny is a provider for Contract uni/tn-demo/brc-permit-to-tn-demo, and the Contract is used as Shared Service. vzAny cannot be used as provider for Shared Services unless used in combination with PBR Service Graph'. The dialog has an 'OK' button.

vzAny cannot be a provider for Shared Services unless combined with a Service Graph

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
dst_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

tcp-src-22-dst-any means any TCP port is open on the Provider side

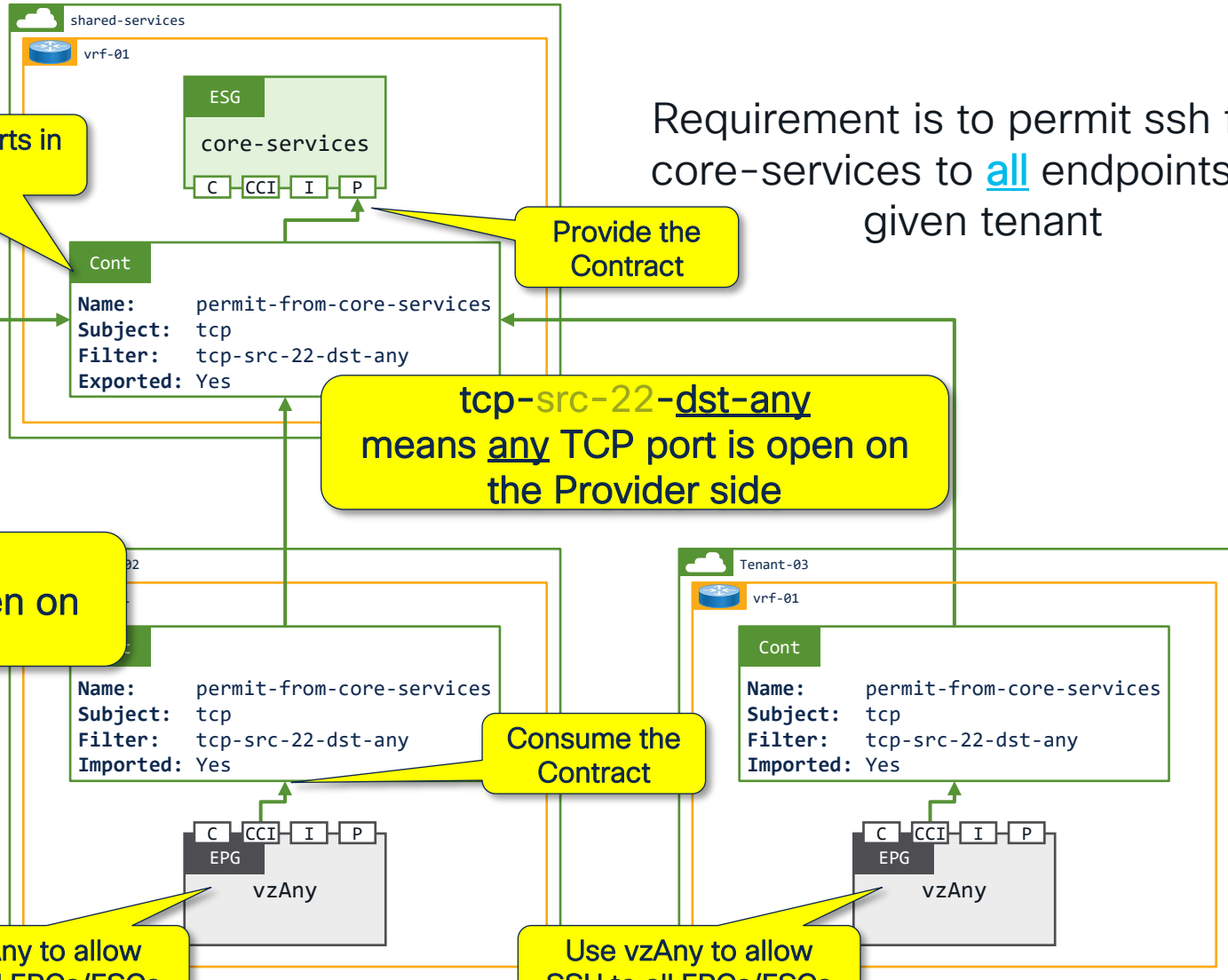
tcp-src-22-dst-any means TCP port 22 is open on the Consumer side

Consume the Contract

Use vzAny to allow SSH to all EPGs/ESGs

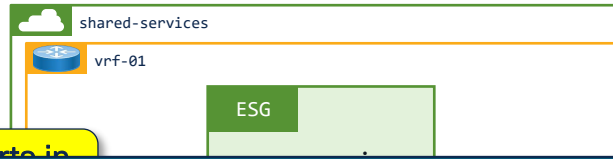
Use vzAny to allow SSH to all EPGs/ESGs

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
dst_port = port open on the provider side EPG/ESG



Requirement is to permit ssh from [redacted] in a [redacted]

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

Reverse the Filter ports in

Requirement is to permit ssh from [redacted] in a [redacted]

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 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 |

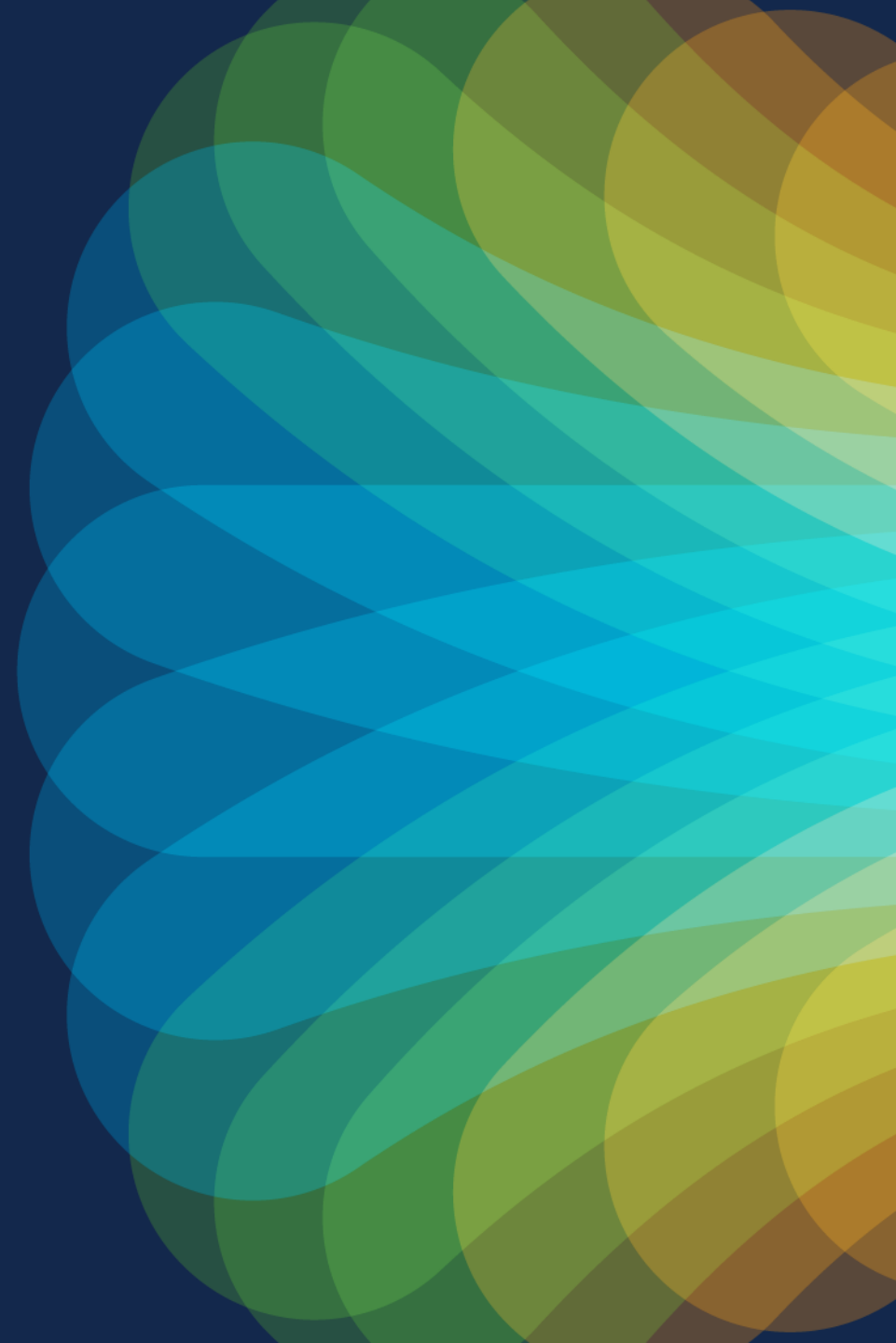
Consume the exported contract(s)

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

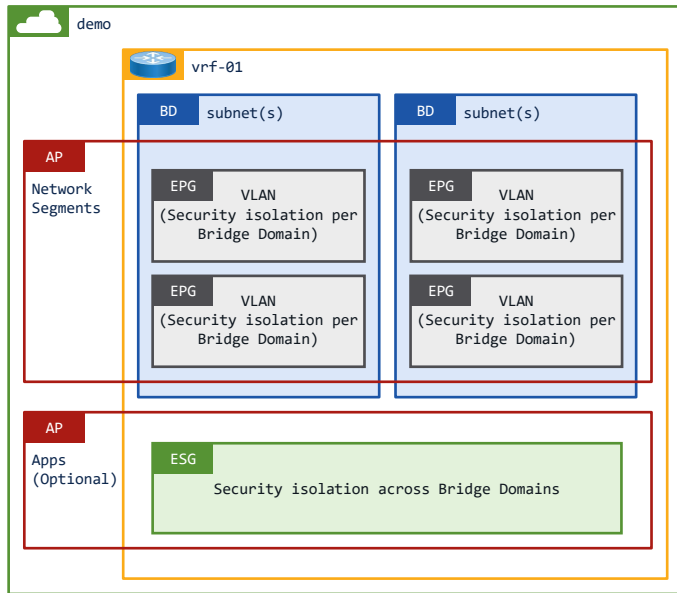
Controlling external connectivity...



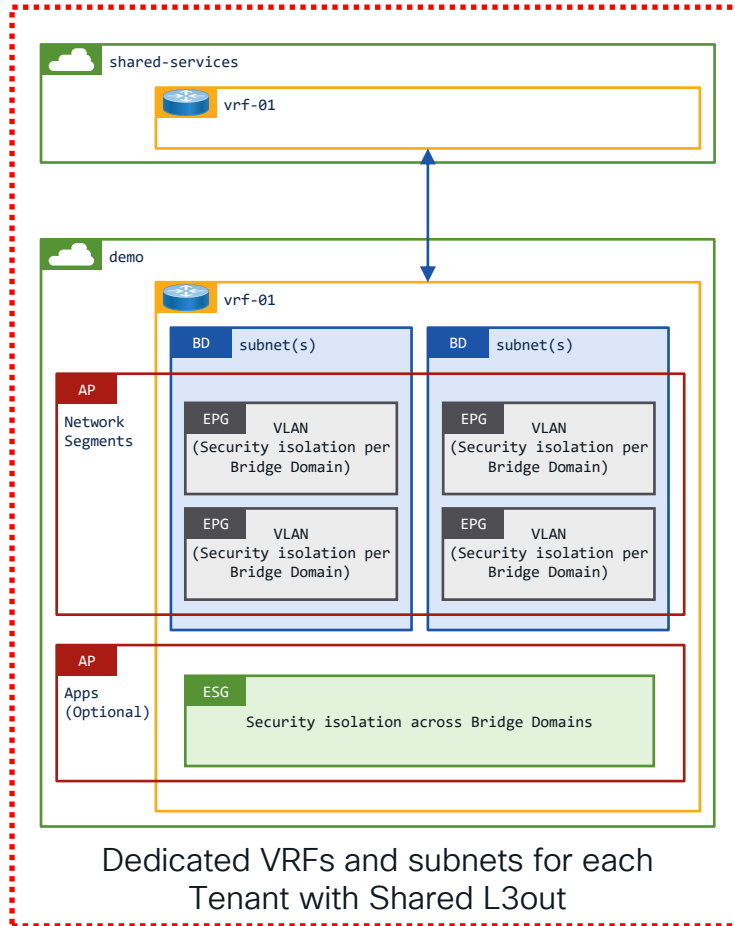
Where should you place your L3outs...?

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

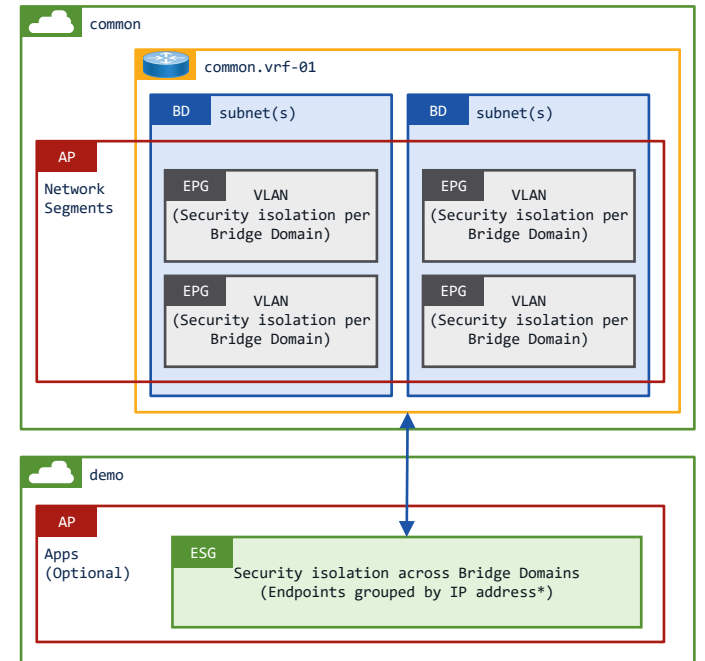
External Connectivity



Dedicated VRFs and subnets for each Tenant with Dedicated L3outs

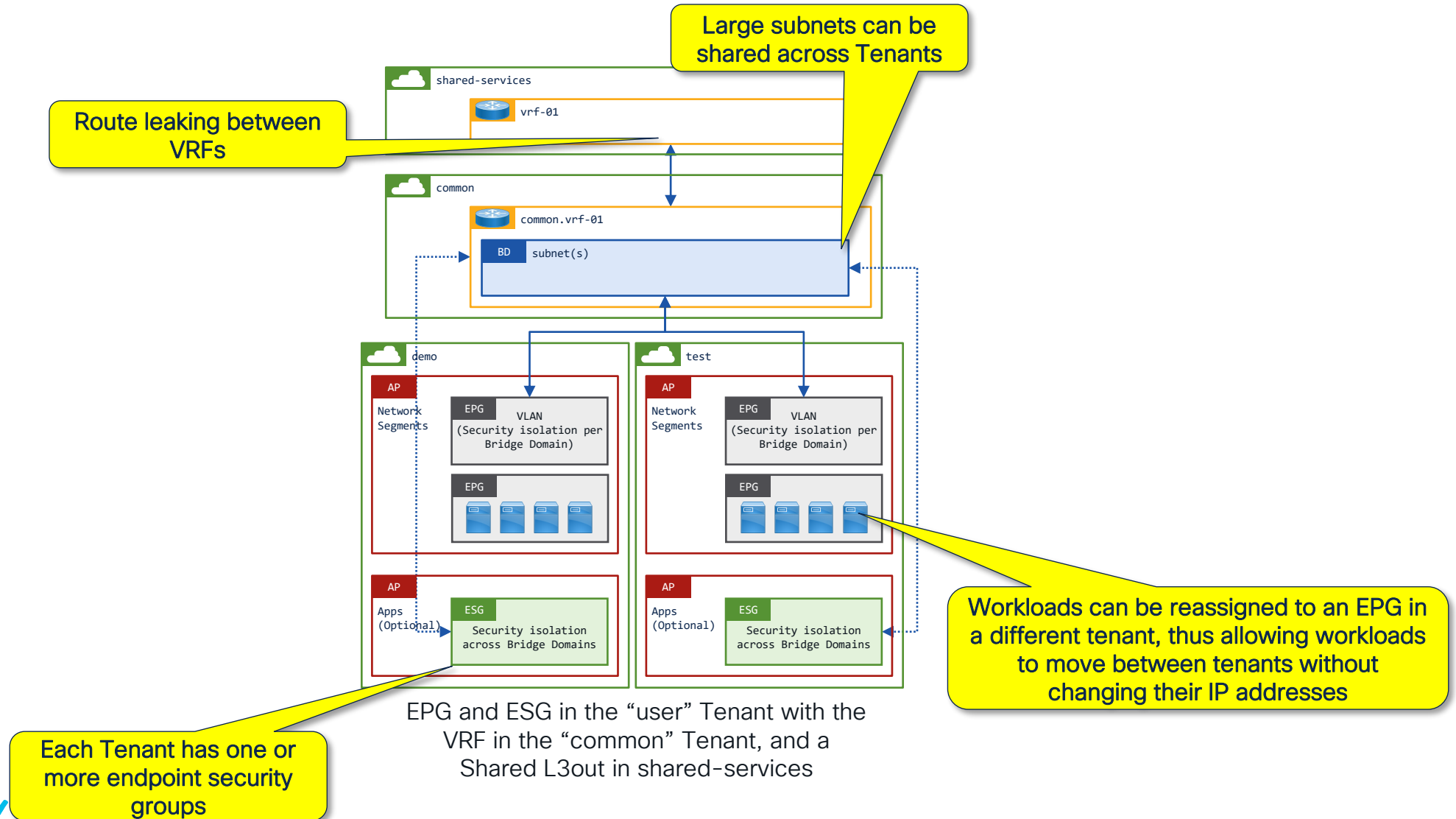


Dedicated VRFs and subnets for each Tenant with Shared L3out

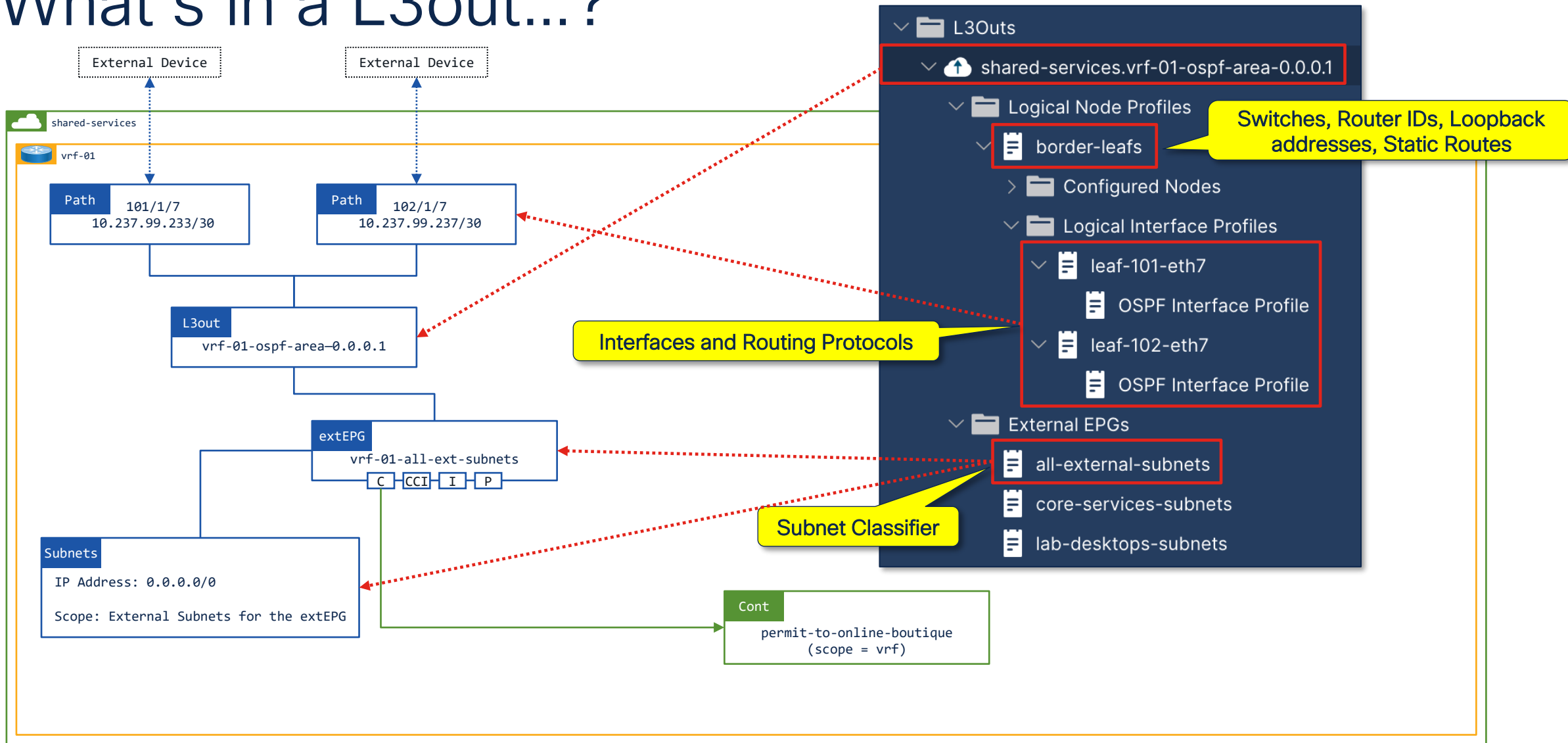


Shared networking with isolated security

External Connectivity with shared subnets...



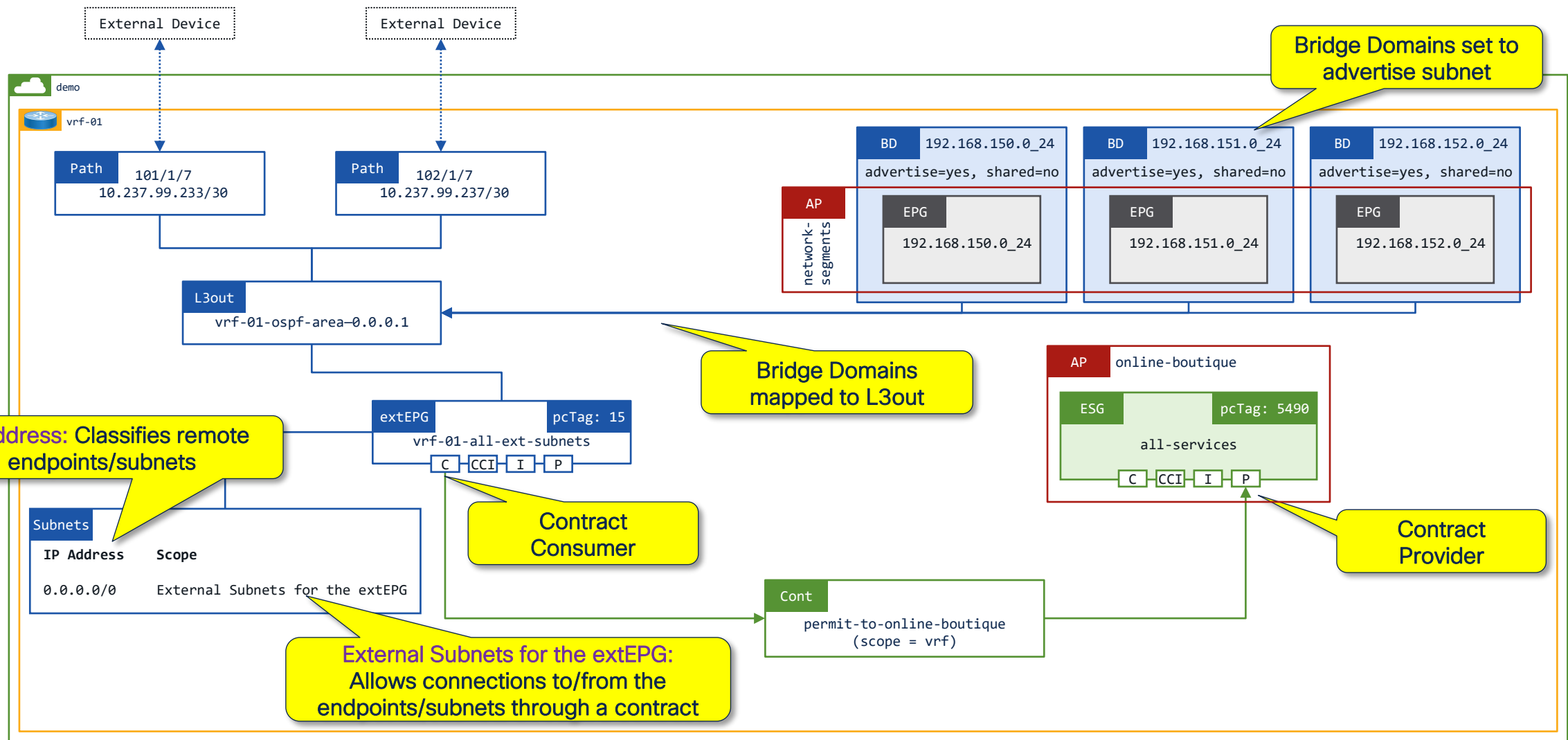
What's in a L3out...?



*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).

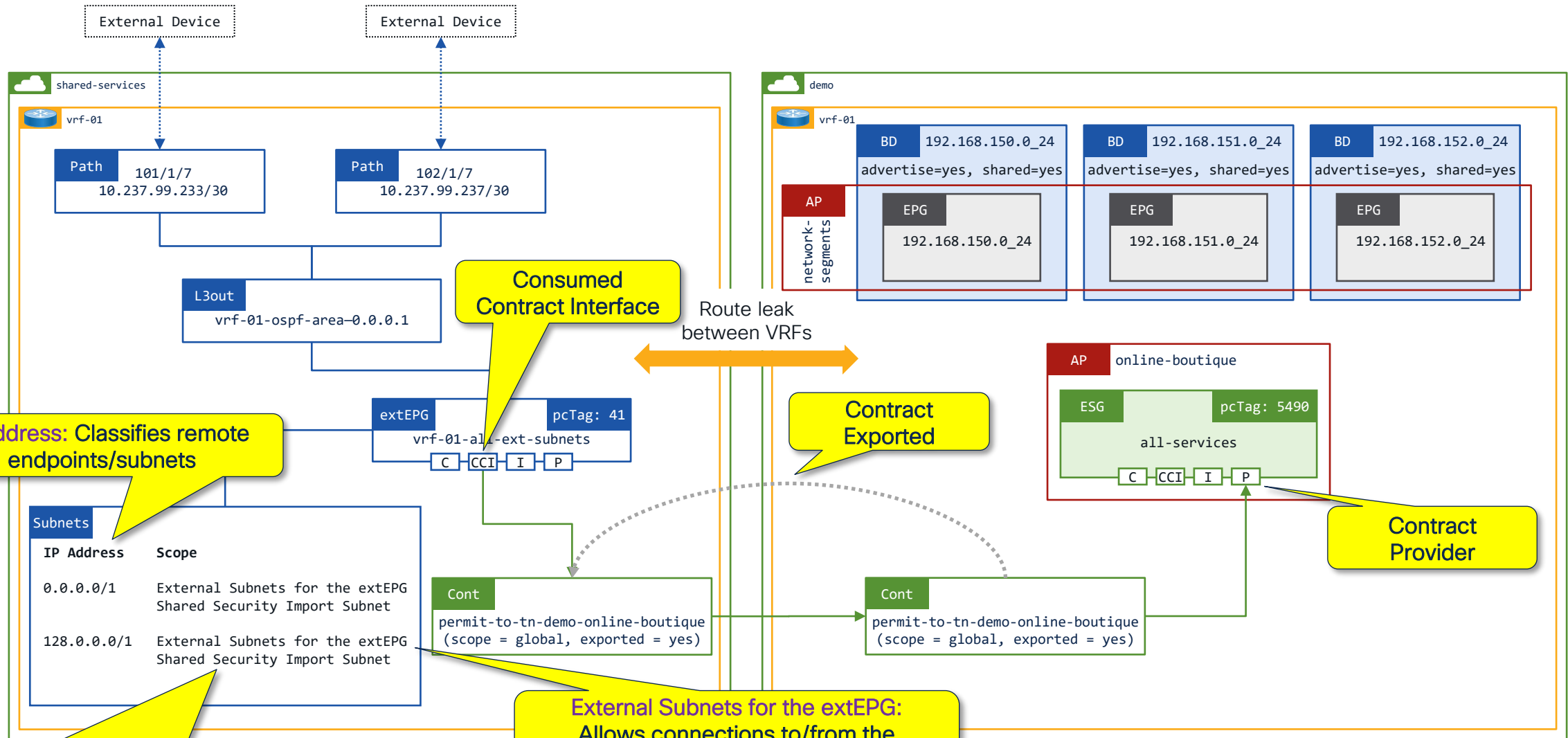
External Subnets for External EPG
 Shared Security Import Subnet

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



IP address: Classifies remote endpoints/subnets

Consumed Contract Interface

Contract Exported

Contract Provider

Shared Security Import Subnet: Leaks the pcTag of the extEPG between VRFs

External Subnets for the extEPG: Allows connections to/from the endpoints/subnets through a contract

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

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

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

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

Control Profile:

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

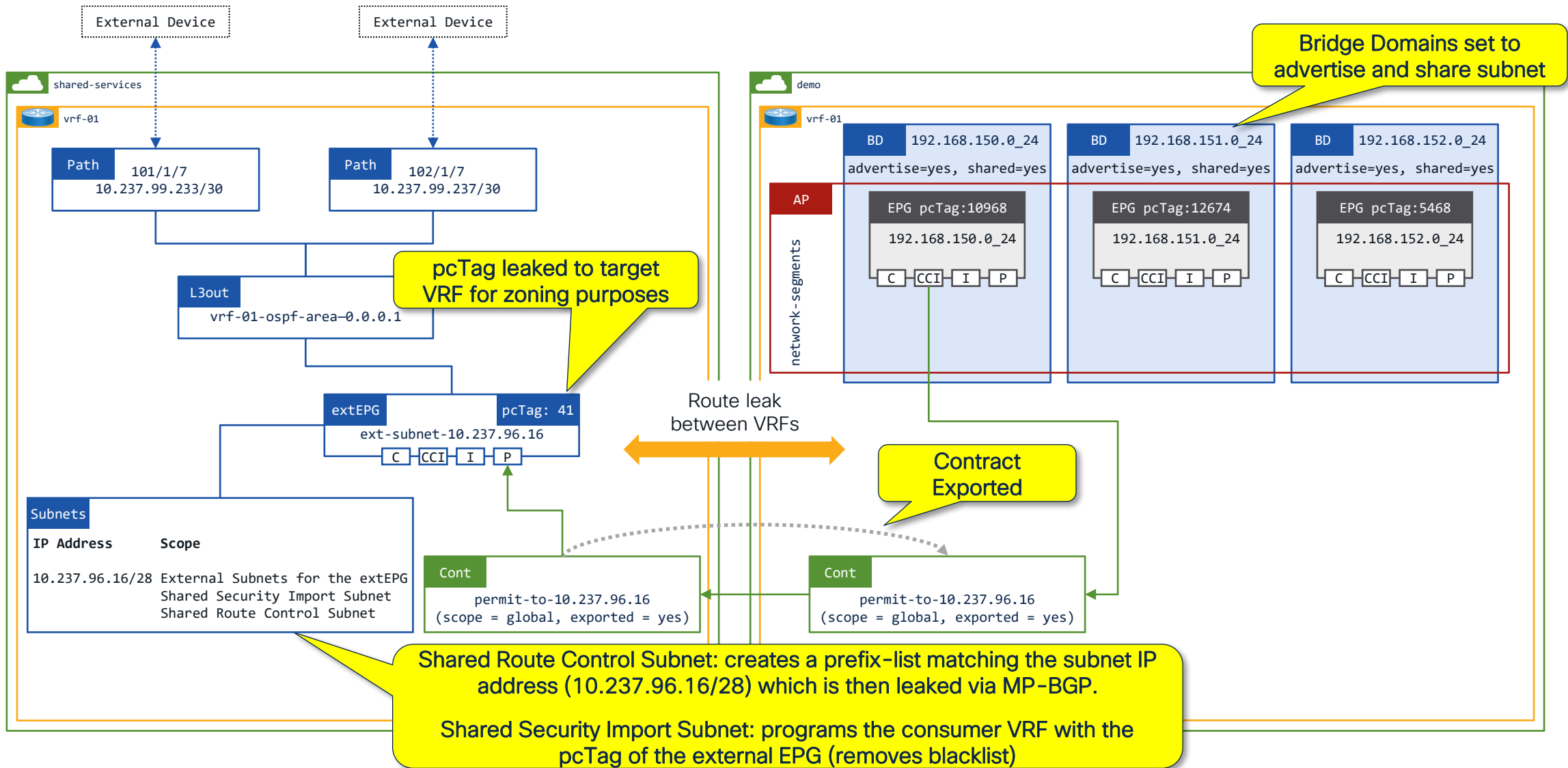
- **IP Address:** identifies remote endpoints/subnets, **must** match a received route for route leaking purposes
- **External Subnets for External EPG:** allows packets to/from the L3out with a contract
- **Shared Security Import Subnet:** is **always** required as it leaks the extEPG pcTag to the target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

A close-up, low-angle shot of a dense field of weeds. The plants have green, serrated leaves and thin, upright stems. Many stems are topped with small, yellow, daisy-like flowers or dark, developing seed heads. The background is slightly blurred, showing more of the same vegetation under bright, natural light.

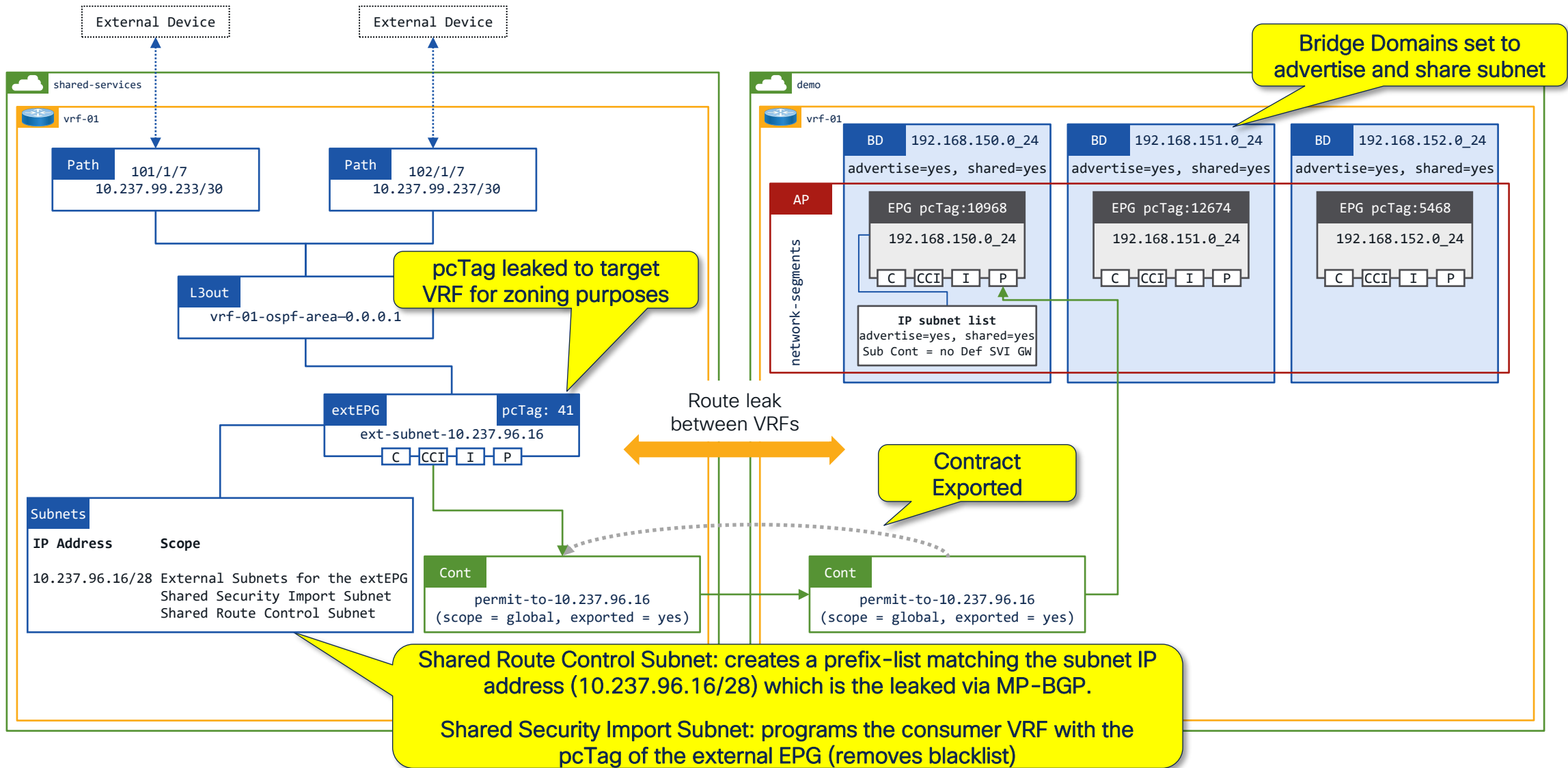
**Getting into
the weeds...!**

How does ACI Route Leaking work...?

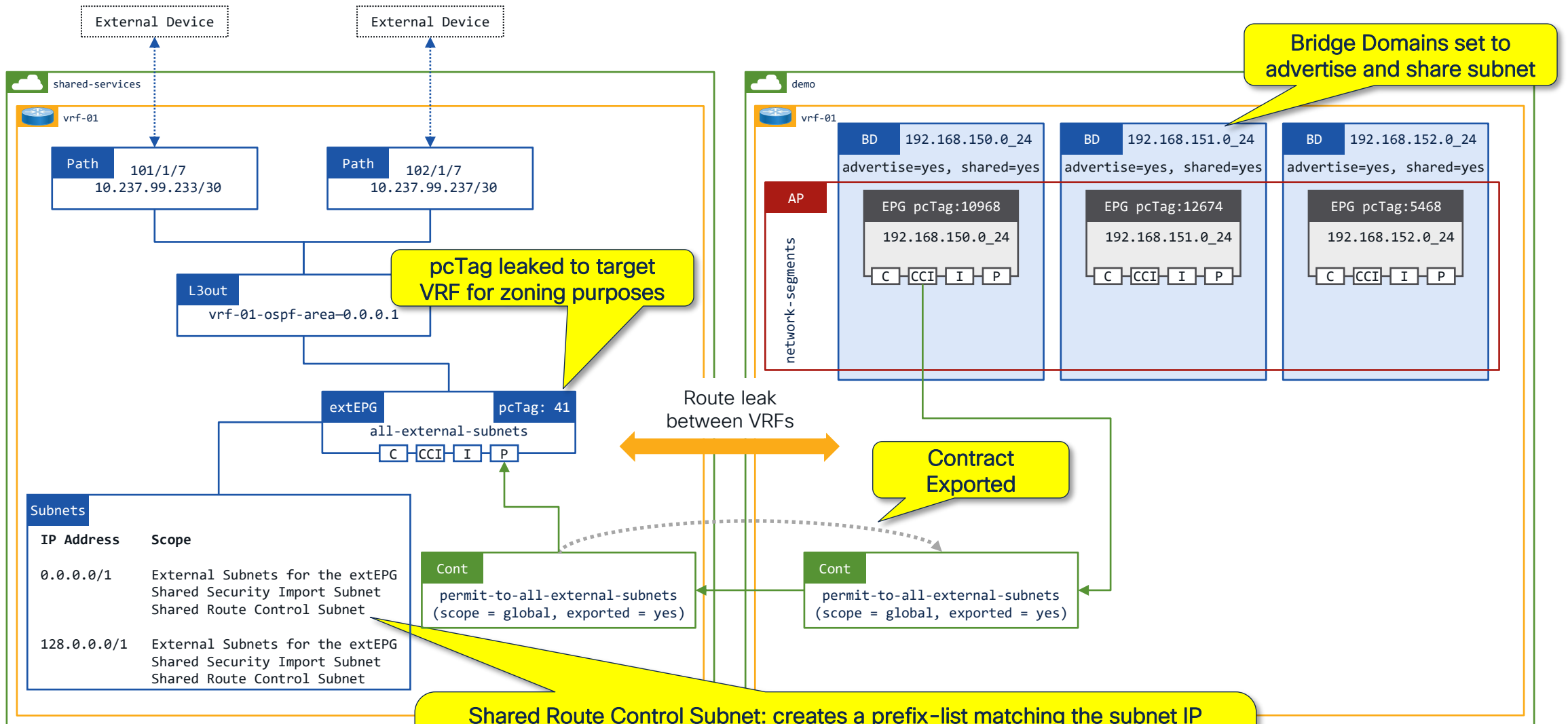
“Original” Route Leaking method – L3out is the Provider



“Original” Route Leaking method – L3out is the Consumer



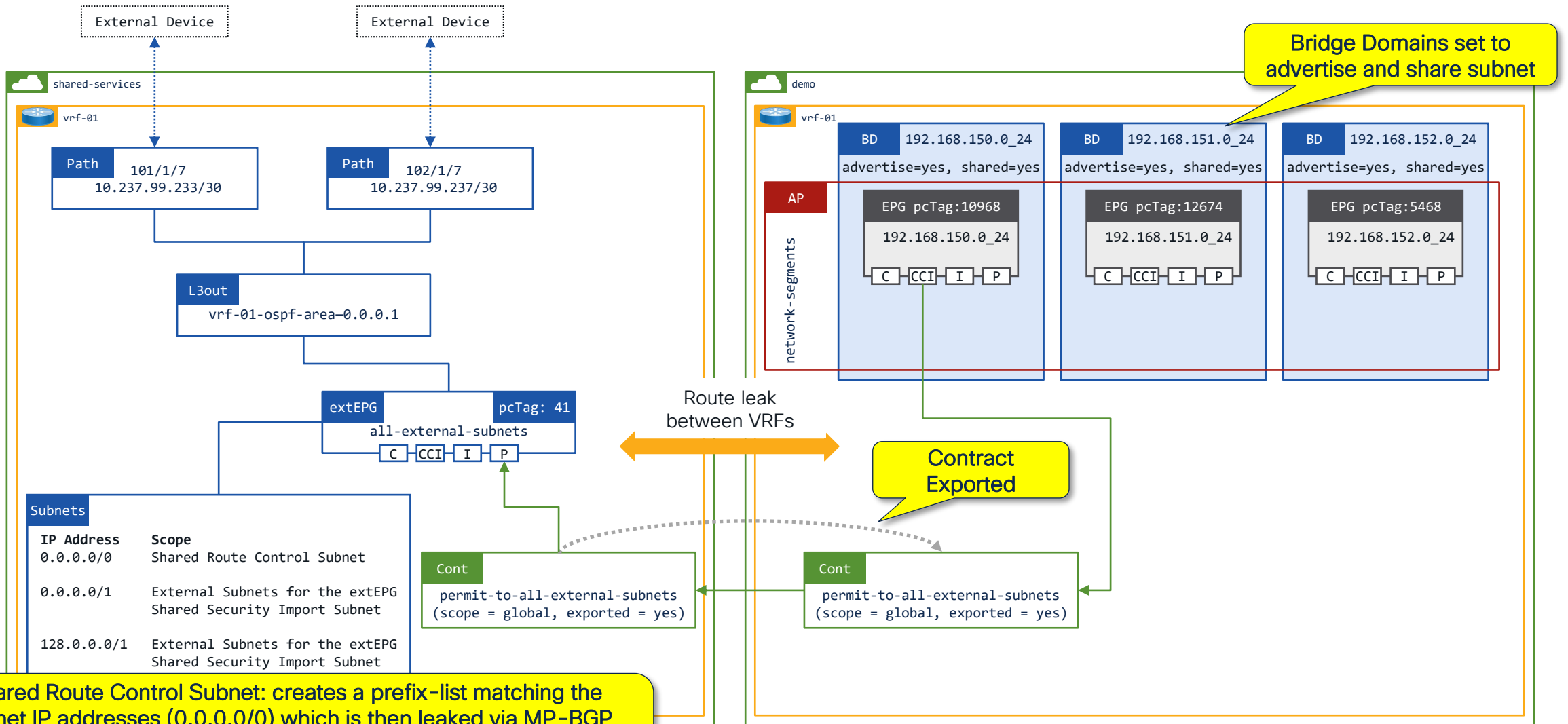
“Shared Route Control Subnet” must match a received route



Shared Route Control Subnet: creates a prefix-list matching the subnet IP addresses (0.0.0.0/1, 128.0.0.0/1) which is then leaked via MP-BGP

THESE ROUTES WILL NEVER MATCH, AND THEREFORE WILL NEVER LEAK...!

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

“New” (and improved) Route Leaking method

shared-services

vrf-01

External Device

External Device

shared-services

demo

vrf-01

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 |

Prefix to leak

External Prefixes

Subnets

| IP Address | Scope |
|-------------|---|
| 0.0.0.0/1 | External Subnets for the extEPG Shared Security Import Subnet |
| 128.0.0.0/1 | External Subnets for the extEPG Shared Security Import Subnet |

Subnets to leak

EPG/BD Subnets

| 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 |

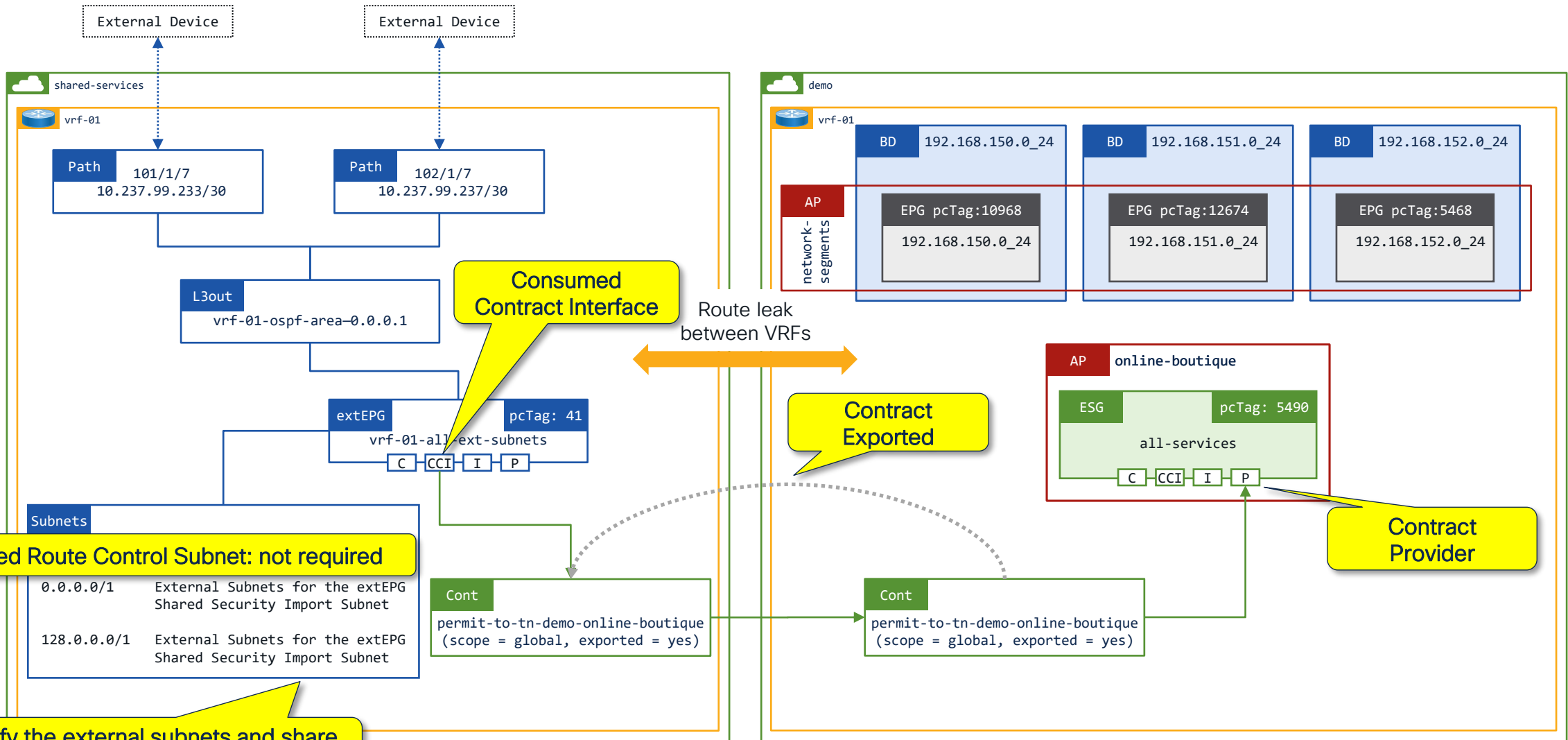
Bridge Domain Subnets

Target Tenants

Target Tenants

Classify the external subnets and share the extEPG pcTag between VRFs

“New” (and improved) Route Leaking method

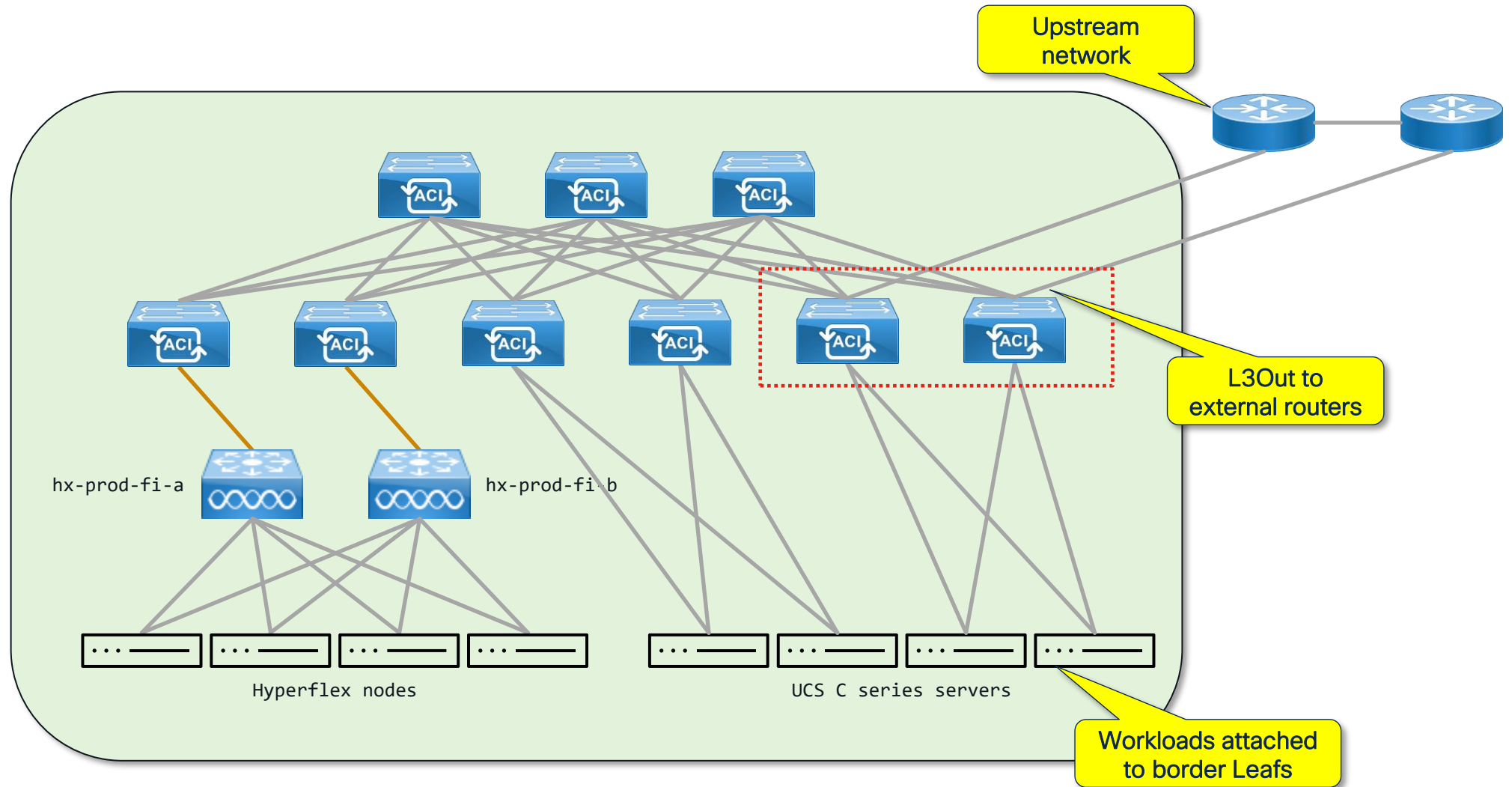


Shared Route Control Subnet: not required

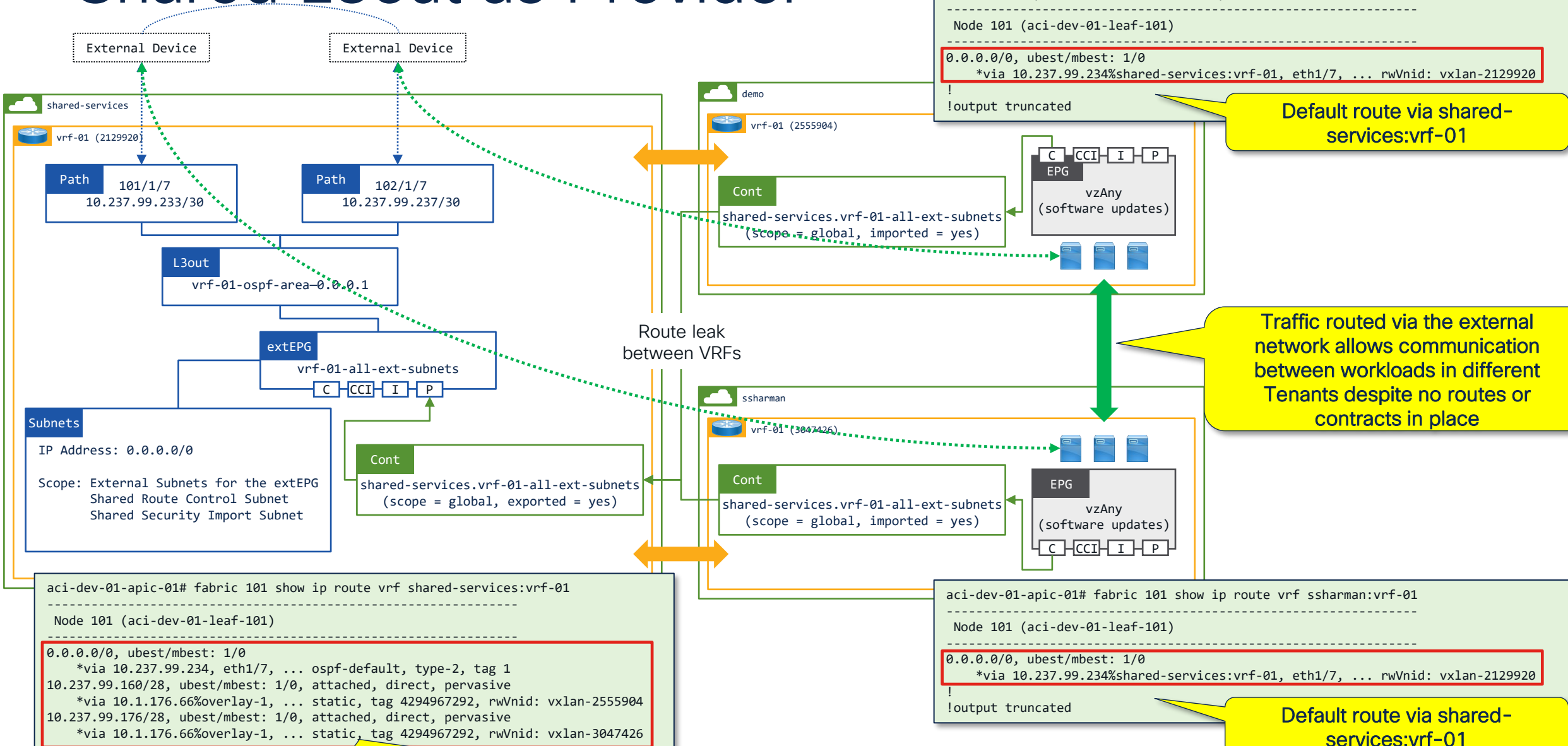
Classify the external subnets and share the extEPG pcTag between VRFs

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

Non dedicated border Leafs



Shared L3out as Provider



```
aci-dev-01-apic-01# fabric 101 show ip route vrf ssharman:vrf-01
-----
Node 101 (aci-dev-01-leaf-101)
-----
0.0.0.0/0, ubest/mbest: 1/0
  *via 10.237.99.234%shared-services:vrf-01, eth1/7, ... rwVnid: vxlan-2129920
!
!output truncated
```

Default route via shared-services:vrf-01

Traffic routed via the external network allows communication between workloads in different Tenants despite no routes or contracts in place

```
aci-dev-01-apic-01# fabric 101 show ip route vrf ssharman:vrf-01
-----
Node 101 (aci-dev-01-leaf-101)
-----
0.0.0.0/0, ubest/mbest: 1/0
  *via 10.237.99.234%shared-services:vrf-01, eth1/7, ... rwVnid: vxlan-2129920
!
!output truncated
```

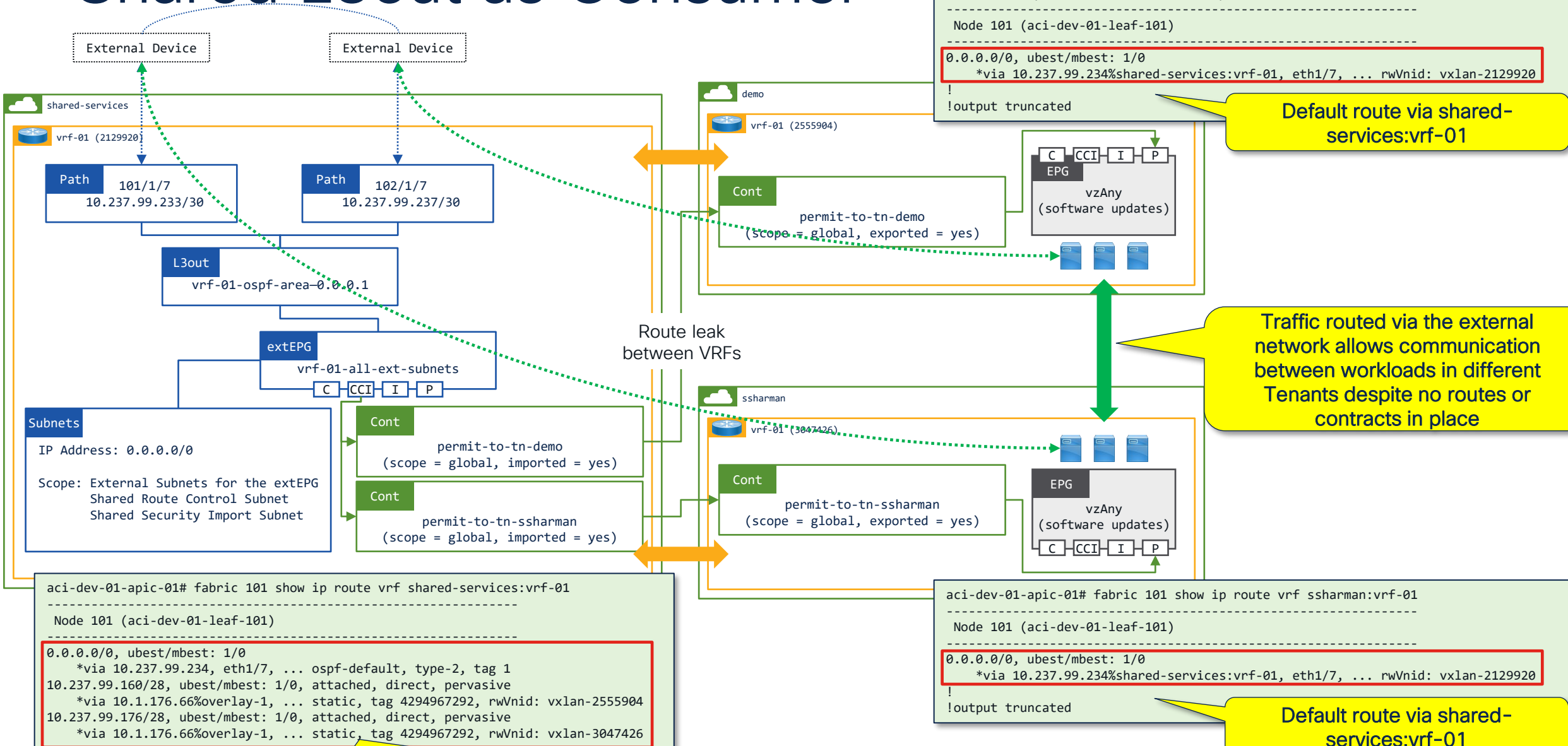
Default route via shared-services:vrf-01

```
aci-dev-01-apic-01# fabric 101 show ip route vrf shared-services:vrf-01
-----
Node 101 (aci-dev-01-leaf-101)
-----
0.0.0.0/0, ubest/mbest: 1/0
  *via 10.237.99.234, eth1/7, ... ospf-default, type-2, tag 1
  10.237.99.160/28, ubest/mbest: 1/0, attached, direct, pervasive
  *via 10.1.176.66%overlay-1, ... static, tag 4294967292, rwVnid: vxlan-2555904
  10.237.99.176/28, ubest/mbest: 1/0, attached, direct, pervasive
  *via 10.1.176.66%overlay-1, ... static, tag 4294967292, rwVnid: vxlan-3047426
```

Default route to external network. Routes to Tenant subnets via overlay-1



Shared L3out as Consumer



```
aci-dev-01-apic-01# fabric 101 show ip route vrf ssharman:vrf-01
-----
Node 101 (aci-dev-01-leaf-101)
-----
0.0.0.0/0, ubest/mbest: 1/0
  *via 10.237.99.234%shared-services:vrf-01, eth1/7, ... rwVnid: vxlan-2129920
!
!output truncated
```

Default route via shared-services:vrf-01

Traffic routed via the external network allows communication between workloads in different Tenants despite no routes or contracts in place

```
aci-dev-01-apic-01# fabric 101 show ip route vrf shared-services:vrf-01
-----
Node 101 (aci-dev-01-leaf-101)
-----
0.0.0.0/0, ubest/mbest: 1/0
  *via 10.237.99.234, eth1/7, ... ospf-default, type-2, tag 1
  10.237.99.160/28, ubest/mbest: 1/0, attached, direct, pervasive
  *via 10.1.176.66%overlay-1, ... static, tag 4294967292, rwVnid: vxlan-2555904
  10.237.99.176/28, ubest/mbest: 1/0, attached, direct, pervasive
  *via 10.1.176.66%overlay-1, ... static, tag 4294967292, rwVnid: vxlan-3047426
```

Default route to external network. Routes to Tenant subnets via overlay-1

```
aci-dev-01-apic-01# fabric 101 show ip route vrf ssharman:vrf-01
-----
Node 101 (aci-dev-01-leaf-101)
-----
0.0.0.0/0, ubest/mbest: 1/0
  *via 10.237.99.234%shared-services:vrf-01, eth1/7, ... rwVnid: vxlan-2129920
!
!output truncated
```

Default route via shared-services:vrf-01

Recommendation

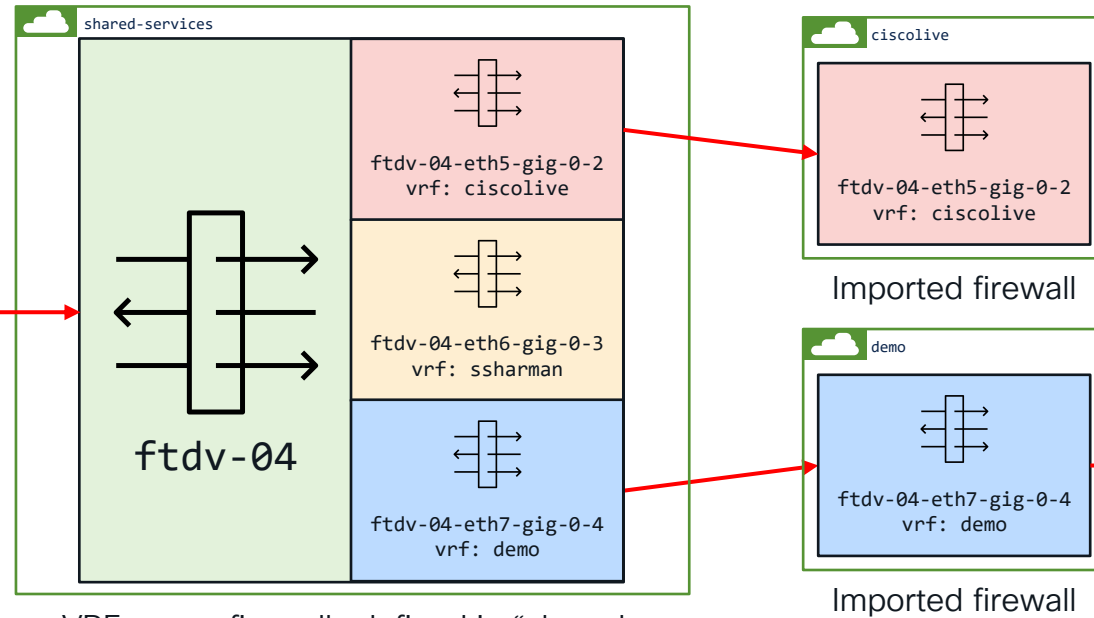
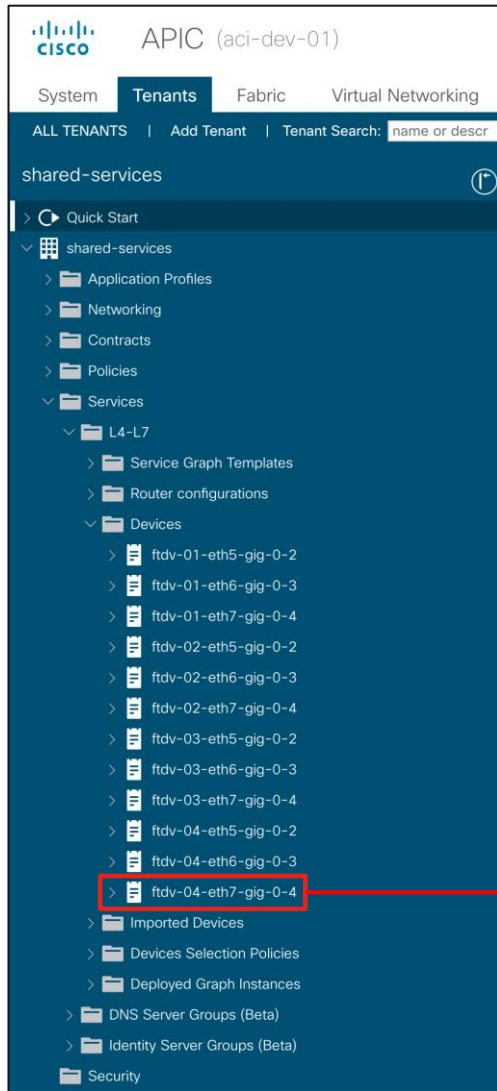
Do not use 0.0.0.0/0 in route leaking design...!

Prepare the fabric for L4-L7 Service Insertion

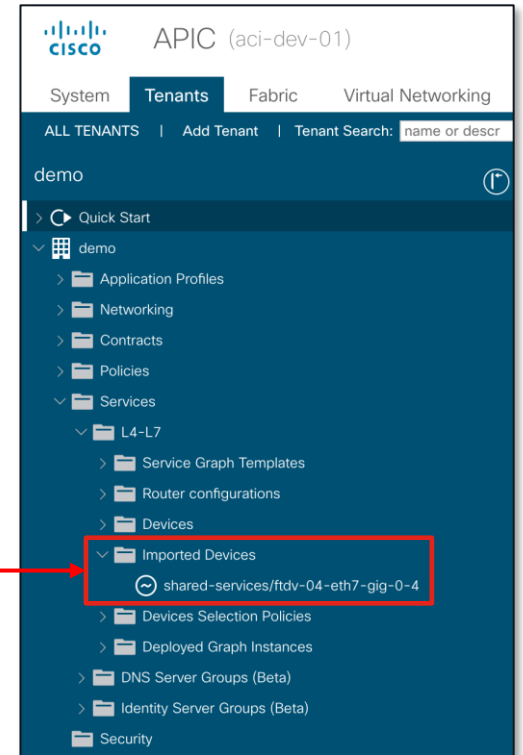
Where should you place your L4-7 devices...?

“common” tenant, “shared-services” tenant, or
“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>

APIC (aci-dev-01)

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

Installed Apps | Faults | Downloads

Apps

ELAM Assistant by Cisco
Help you perform ELAM(Embedded Logic Analyzer Module) on ACI nodes to capture a single packet at a time and analyze where the packet goes.

ACI Endpoint Update by Cisco
Pushes dynamic endpoint information from APIC to Secure Firewall ASA and Secure Firewall Management Center

Nexus Insights Cloud Connector by Cisco
Nexus Insights Cloud Connector (3.x or higher) implements Direct Streaming and Nexus Cloud capable telemetry functionality. These services perform backend functions only and do not have...

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration Deploy

Dynamic Objects

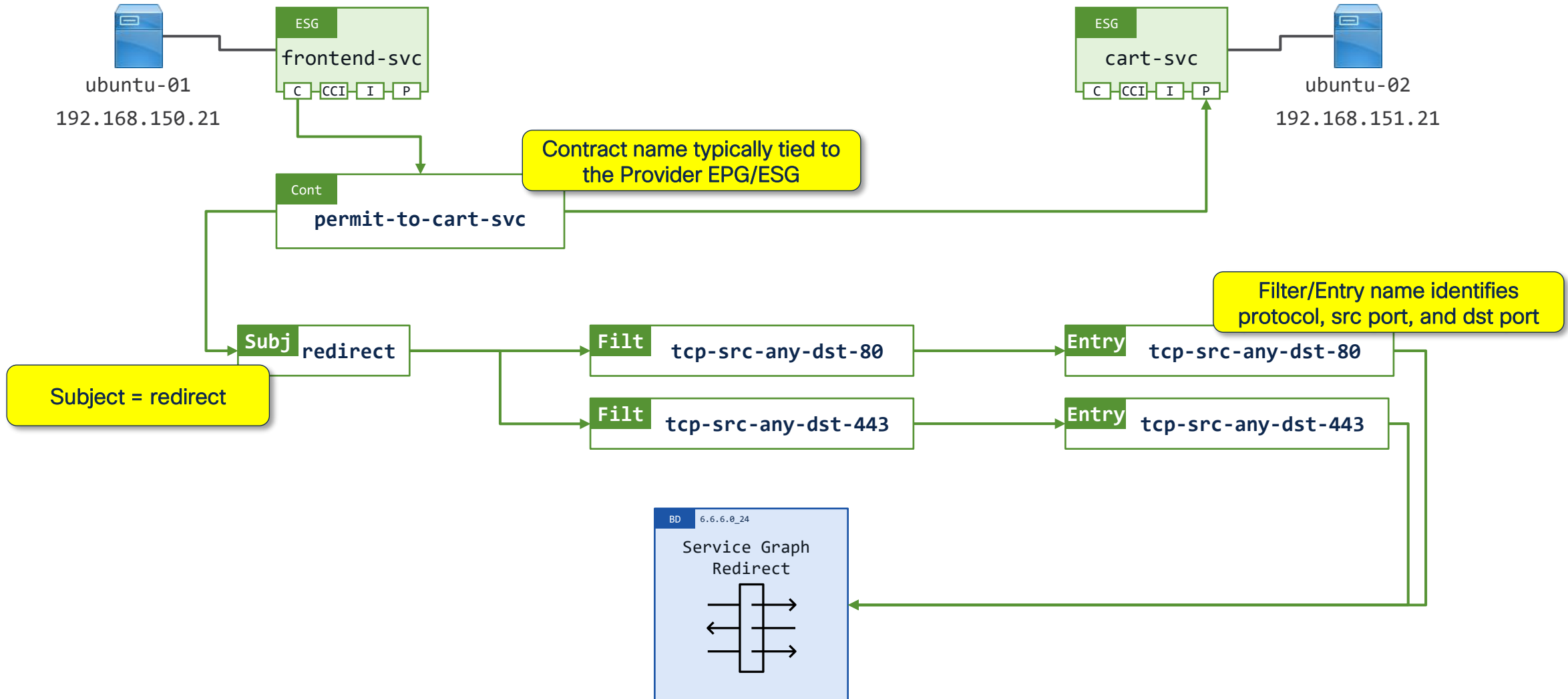
| Name | Description | Number of Mapped IPs |
|---|-------------|----------------------|
| APIC_DEMO_EPG-MATCHED-SECURITY-GROUPS_ESG-... | | 3 |
| APIC_DEMO_NETWORK-SEGMENTS_192.168.150.0_24 | | 1 |
| APIC_DEMO_NETWORK-SEGMENTS_192.168.151.0_24 | | 1 |
| APIC_DEMO_NETWORK-SEGMENTS_192.168.152.0_24 |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

External Attributes

Dynamic Object

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

Redirect applied to all Filters under the Subject...



Step 1: Define the Policy Based Redirect Target

APIC (aci-dev-01)

System **Tenants** Fabric Virtual Networking

ALL TENANTS | Add Tenant | Tenant Search: name or descr

demo

- Quick Start
- demo
 - Application Profiles
 - Networking
 - Contracts
 - Policies
 - Protocol
 - BFD
 - BFD Multihop
 - ND RA Prefix
 - BGP
 - Custom QoS
 - Data Plane Policing
 - DHCP
 - EIGRP
 - End Point Retention
 - External Bridge Group Profiles
 - First Hop Security
 - HSRP
 - IGMP Interface
 - IGMP Snoop
 - IP SLA
 - L4-L7 Policy-Based Redirect**
 - ftdv-04-eth7-gig-0-4

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

Step 2: Define Service Graph Template and Device Selection Policy

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

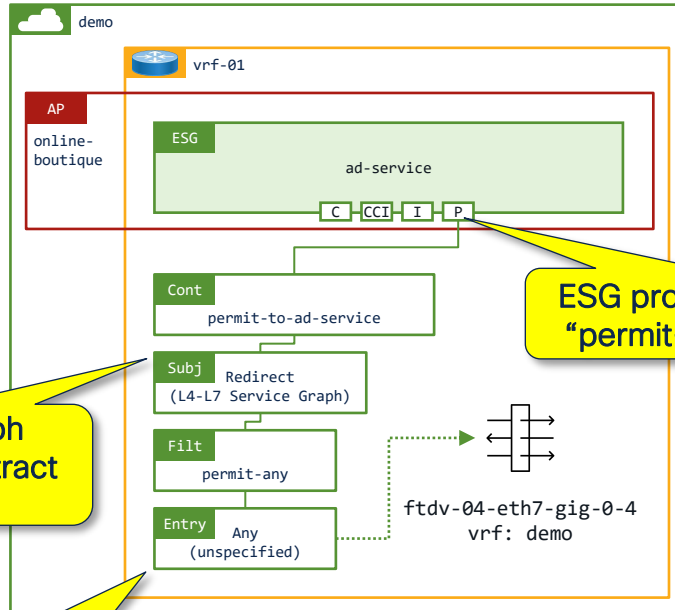
Service Graph Template Configuration:

- Service Graph Template:** A template named "redirect-to-ftdv-04-gig-0-4" is shown, containing a Function Node - N1 with three endpoints: "consumer", "provider", and "ftdv-04-eth7-gig-0-4".
- Endpoint Information:** A box titled "ftdv-04-eth7-gig-0-4 Information" shows "Firewall: Routed" and "Route Redirect: true".

Device Selection Policy Configuration:

- Policy:** A policy named "any-redirect-to-ftdv-04-gig-0-4-N1" is shown, targeting "consumer" and "provider" devices.
- Configuration Details:** Two configuration boxes are shown, one for the "consumer" connector and one for the "provider" connector. Both boxes are highlighted with red boxes and callouts:
 - Firewall interface and Bridge Domain for the Consumer/Provider interface:** Points to the "Cluster Interface" (gig-0-4) and "Associated Network" (Bridge Domain, L3Out) fields.
 - PBR target:** Points to the "L3 Destination (VIP)" field, which is checked and set to "ftdv-04-eth7-gig-0-4".

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

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

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 Subject and Filter

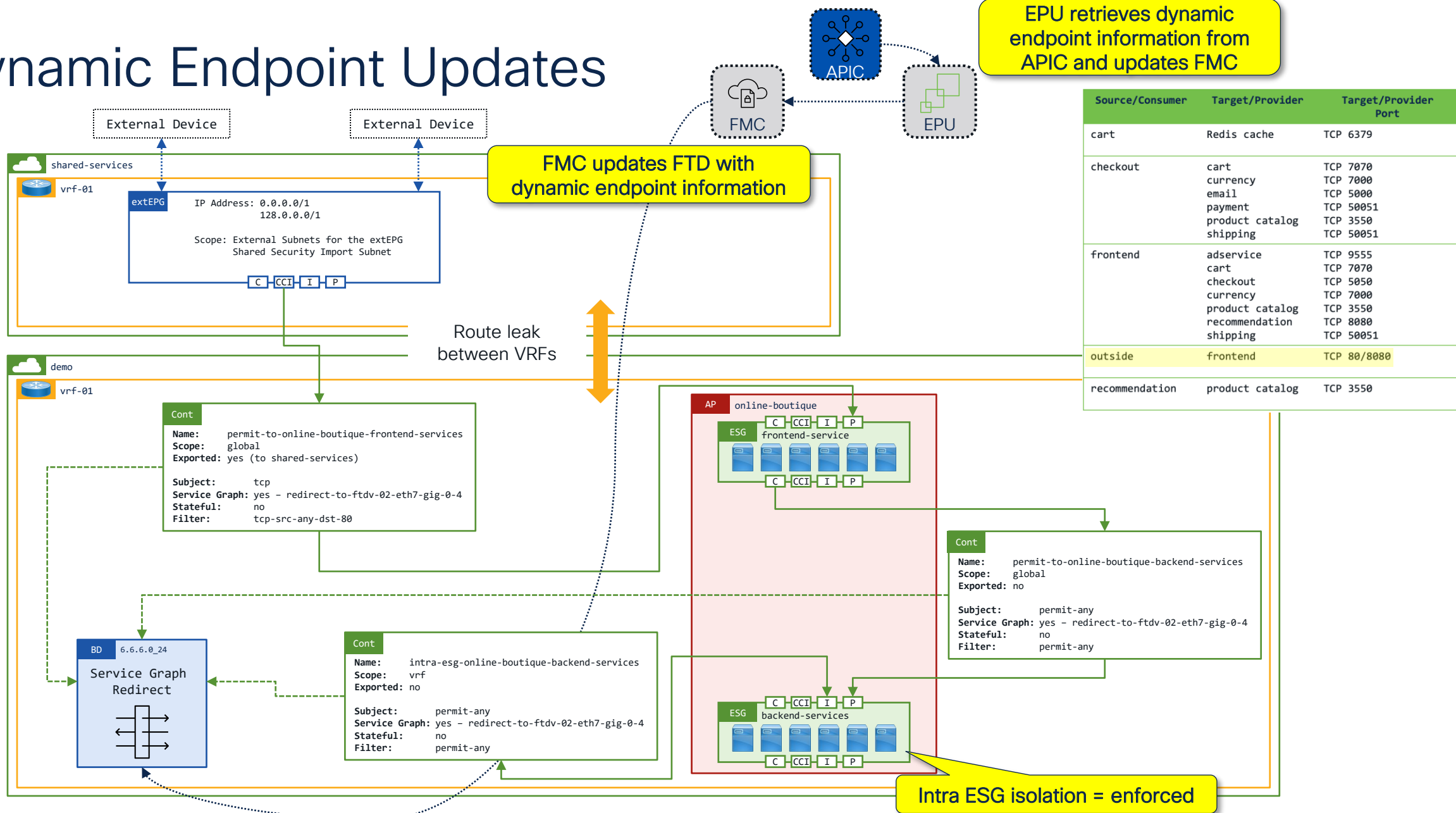
Service Graph redirect

- permit-to-ad-service
- redirect

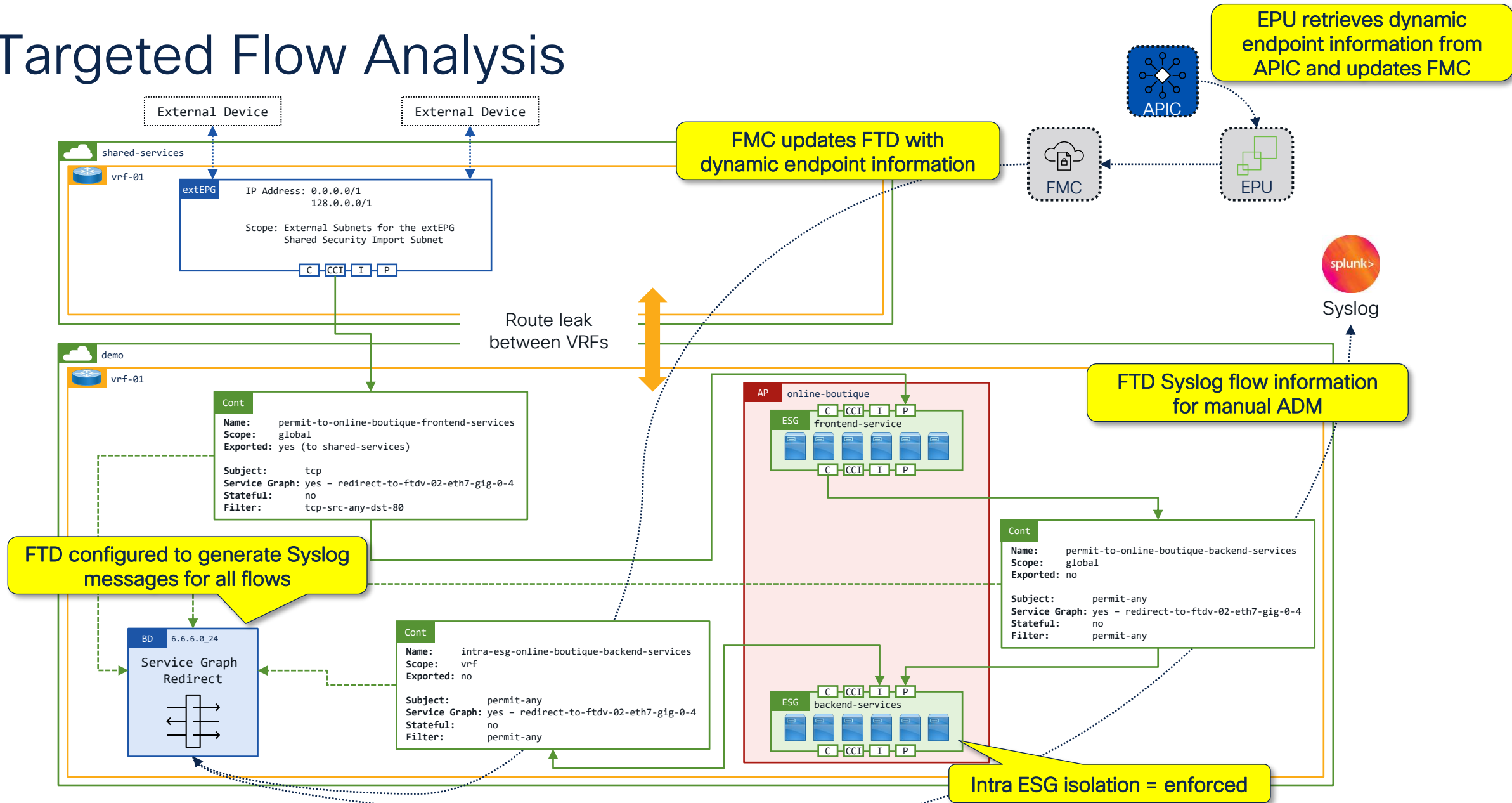
Contract and Subject

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

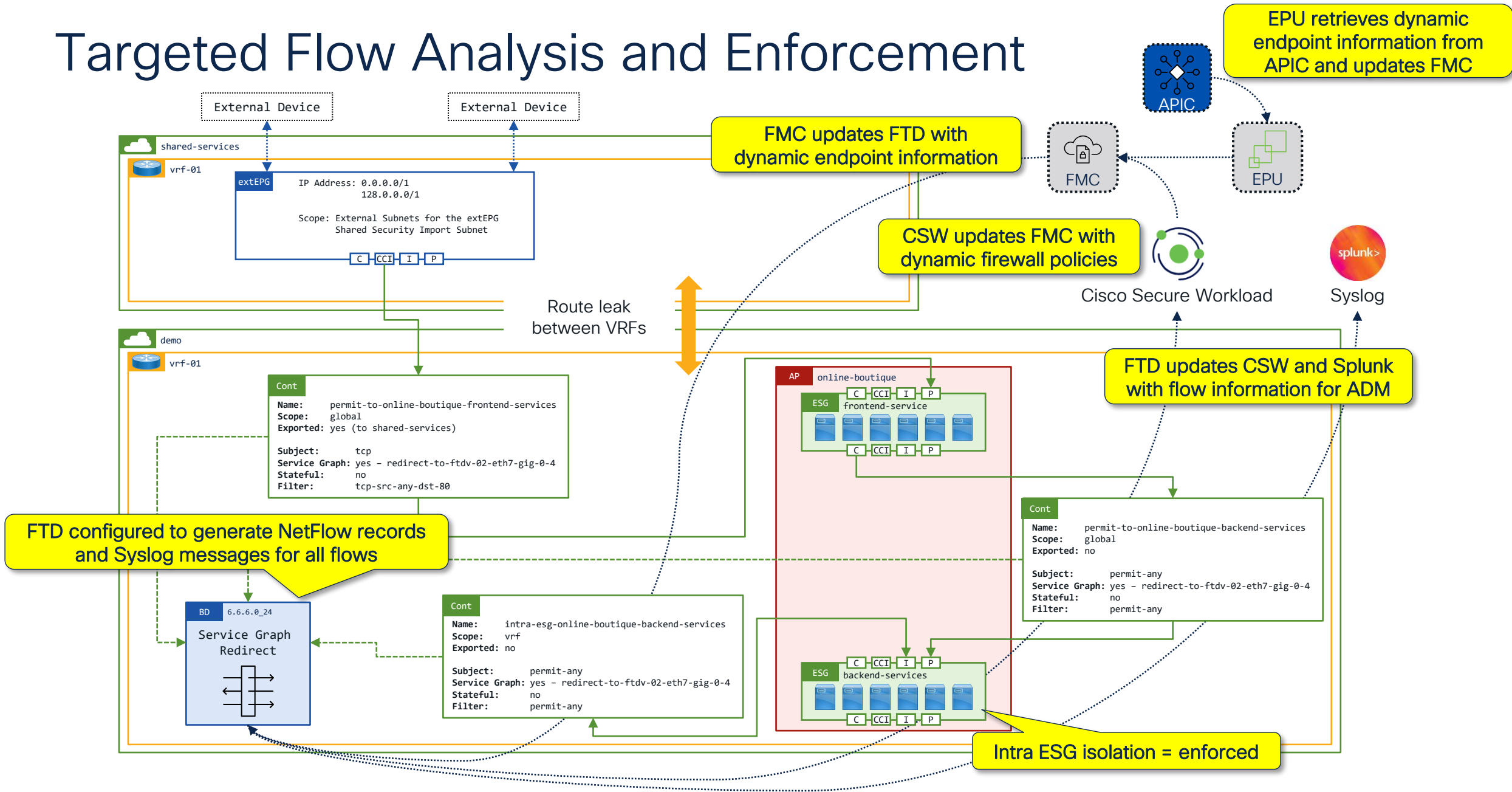
Dynamic Endpoint Updates



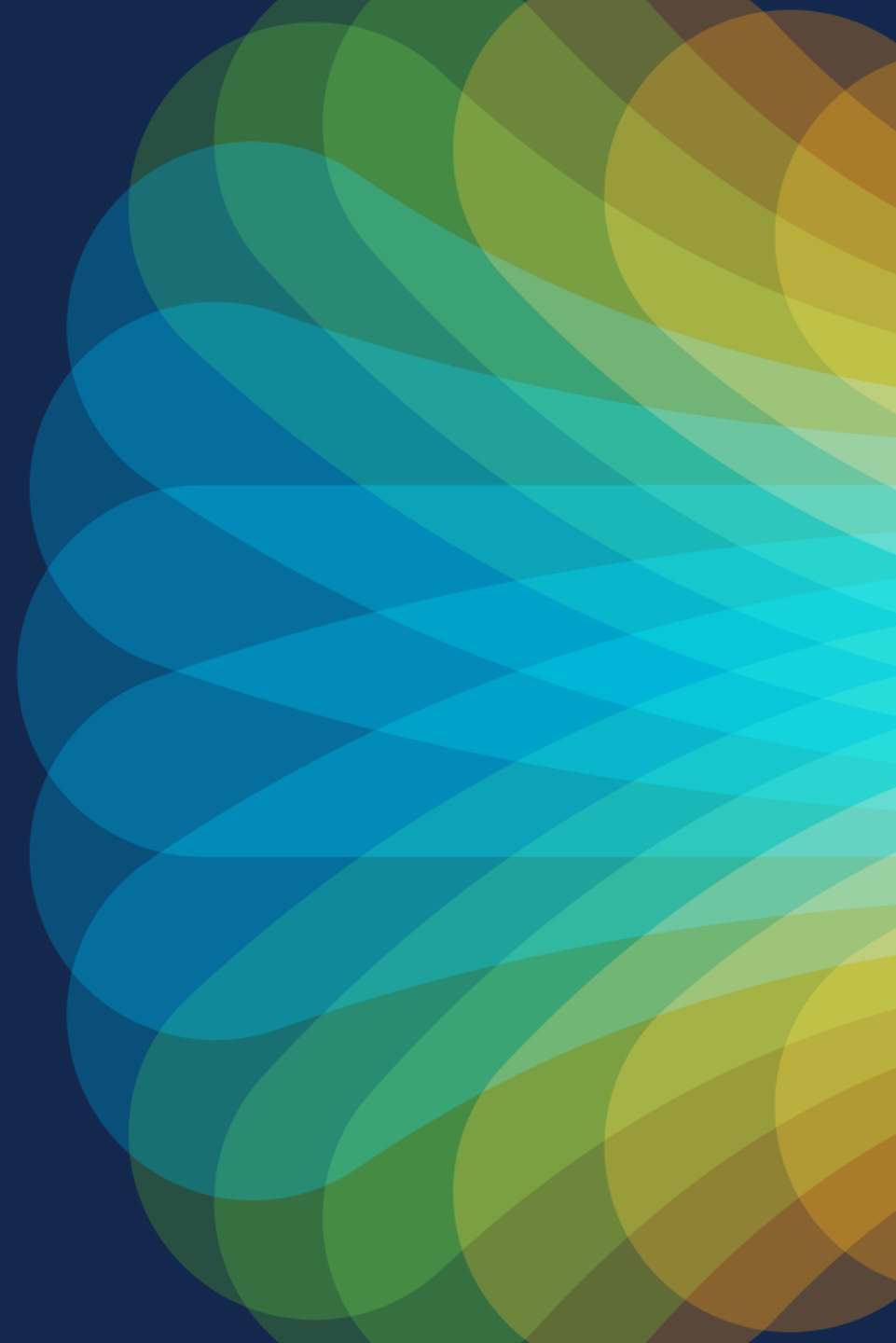
Targeted Flow Analysis



Targeted Flow Analysis and Enforcement

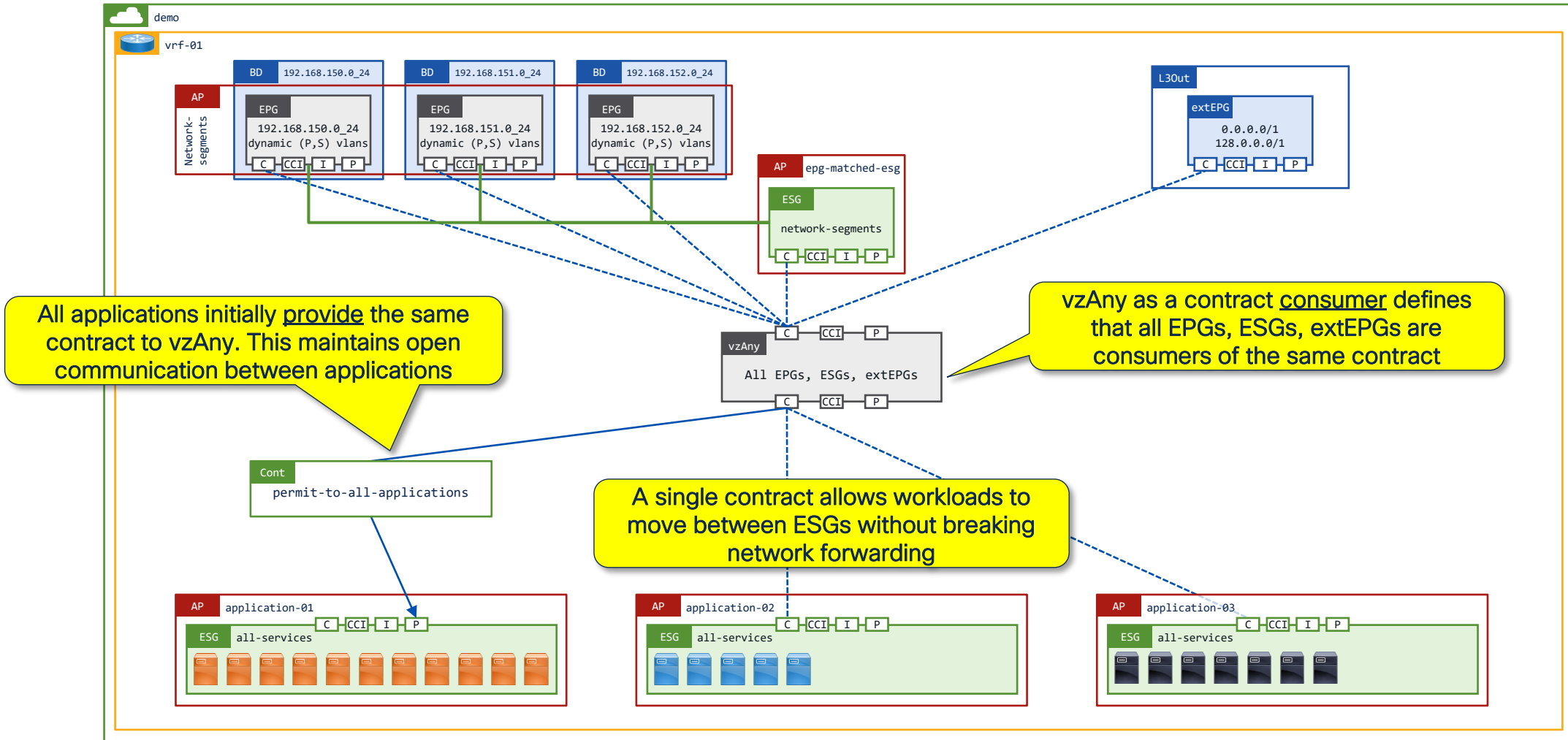


Tightening Security...



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

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



All applications initially provide the same contract to vzAny. This maintains open communication between applications

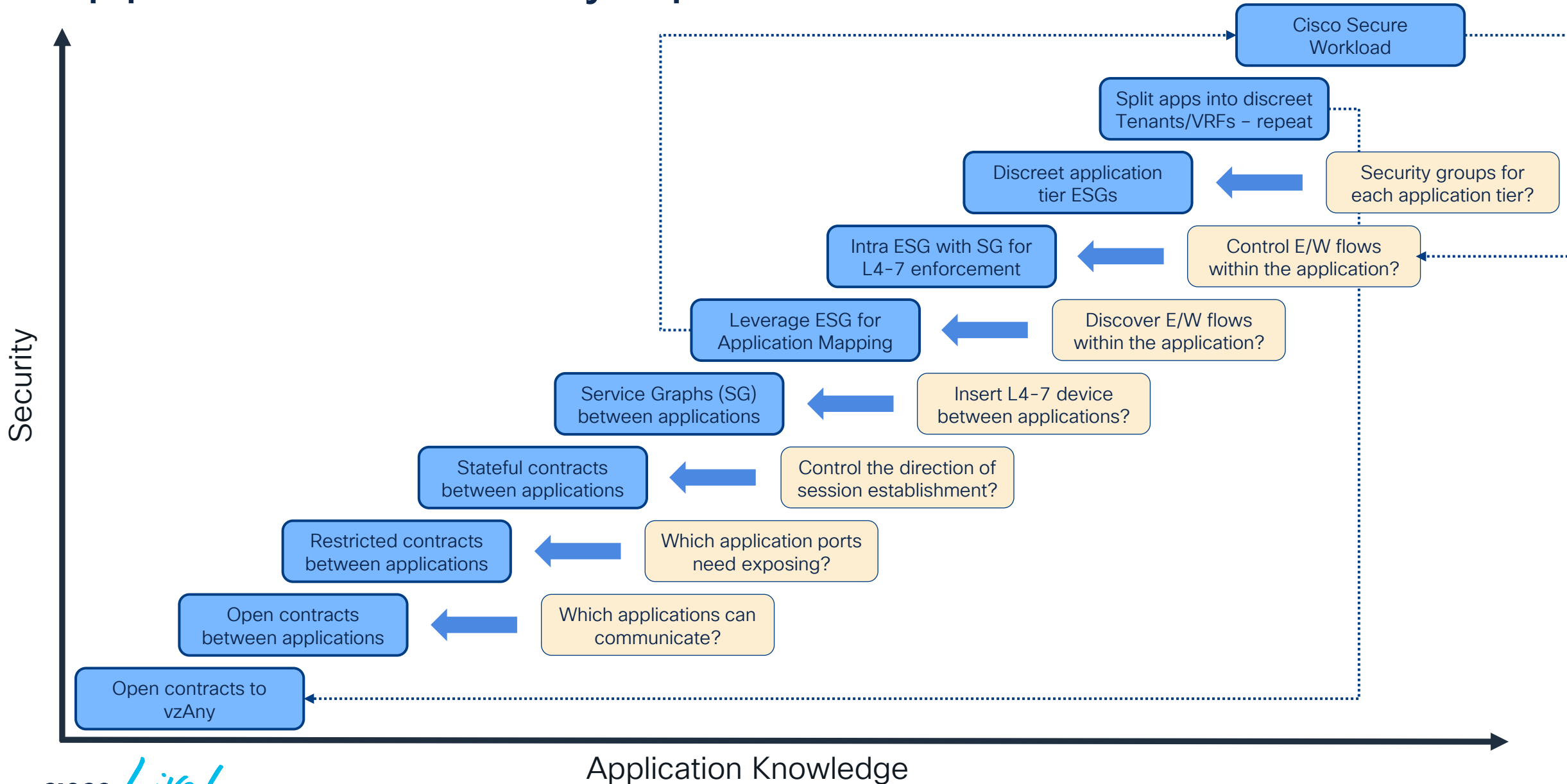
vzAny as a contract consumer defines that all EPGs, ESGs, extEPGs are consumers of the same contract

A single contract allows workloads to move between ESGs without breaking network forwarding

Step 2: ...

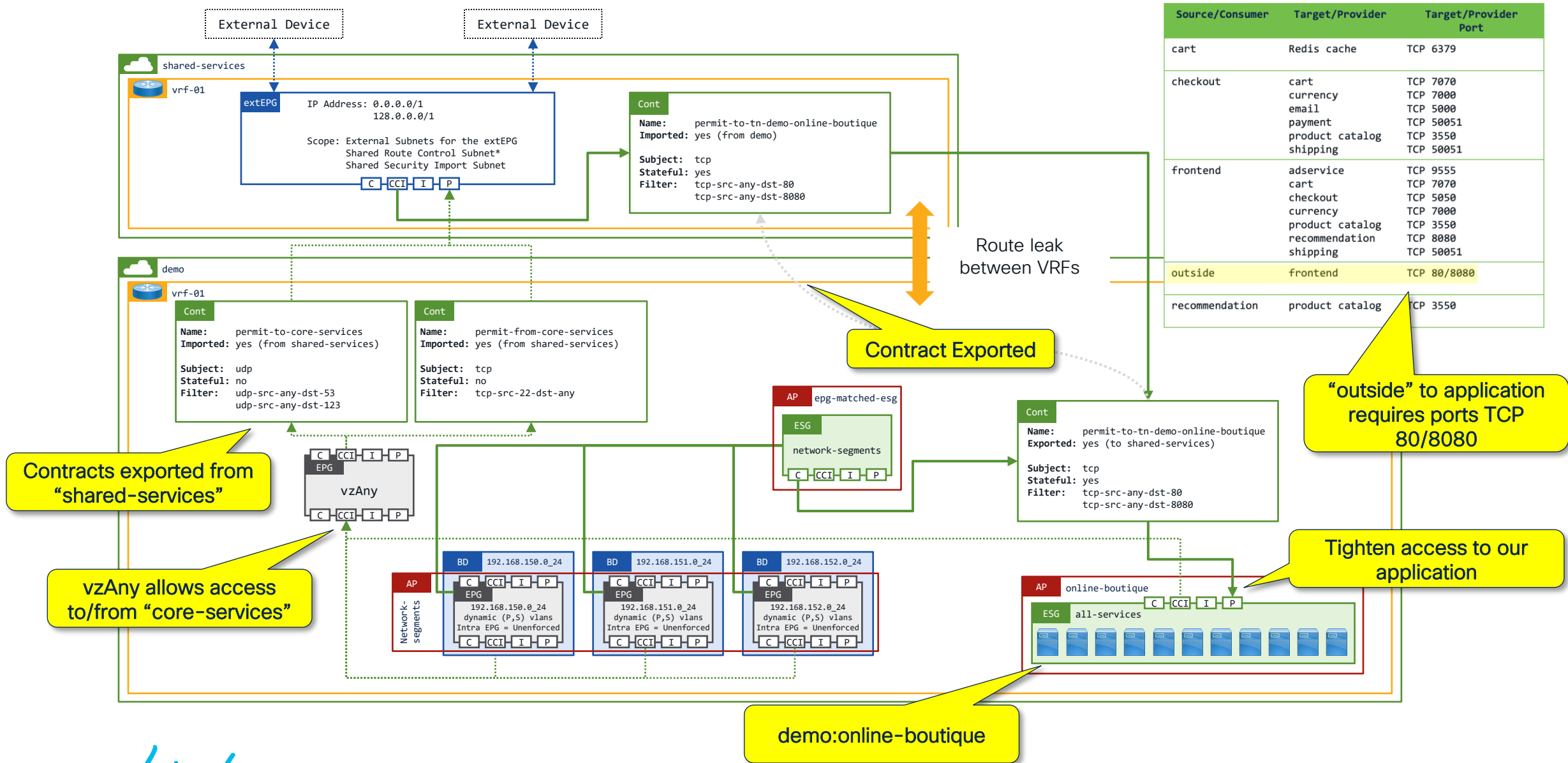


Application security options...



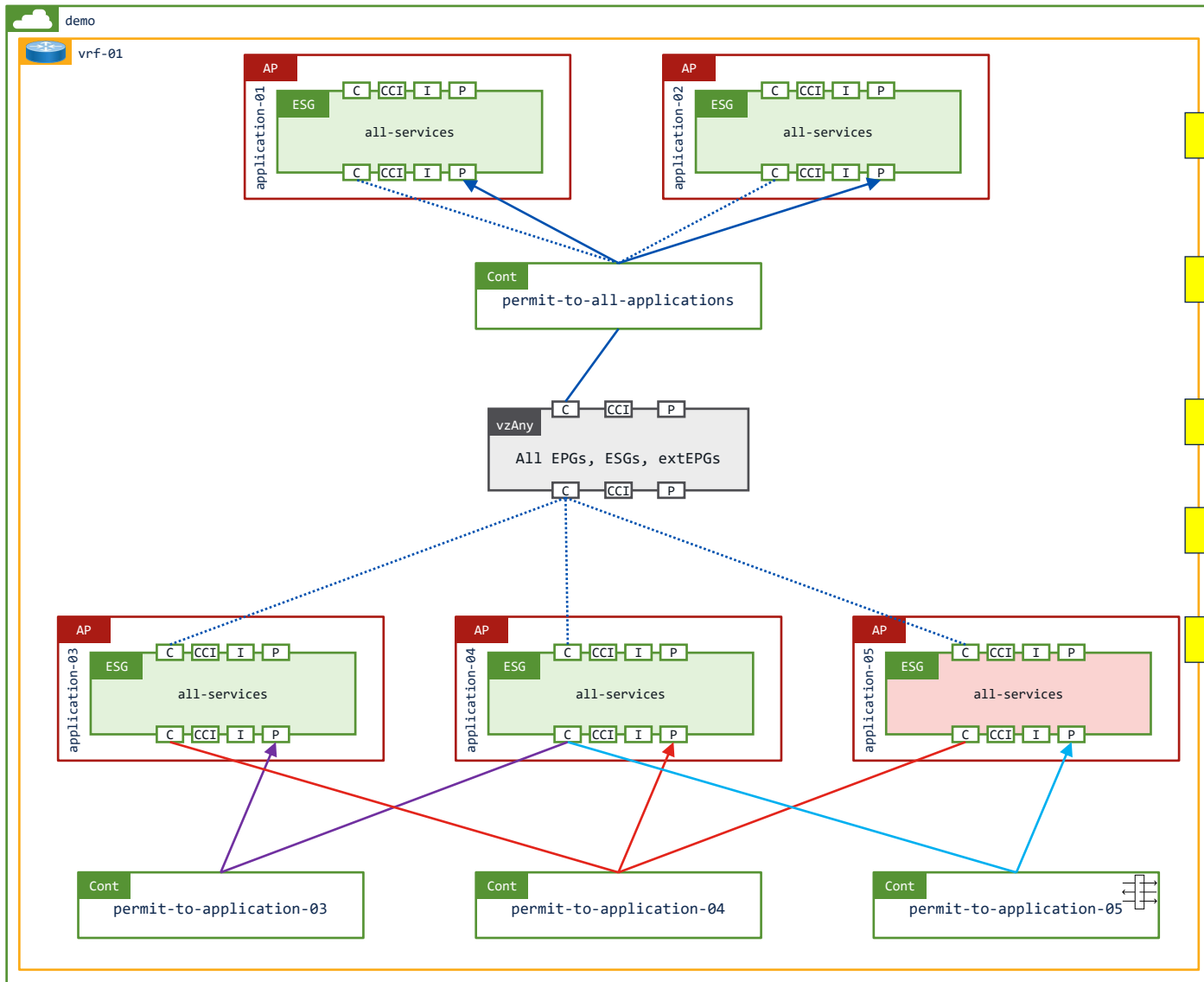
Let's tighten the contract to our online-boutique application...

Tighten access to our online-boutique application...



| 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 | shipping | TCP 50051 |
| | adservice | TCP 9555 |
| | cart | TCP 7070 |
| | checkout | TCP 5050 |
| | currency | TCP 7000 |
| recommendation | product catalog | TCP 3550 |
| | recommendation | TCP 8080 |
| | shipping | TCP 50051 |
| | shipping | TCP 50051 |
| outside | frontend | TCP 80/8080 |
| recommendation | product catalog | TCP 3550 |

Defining application security...

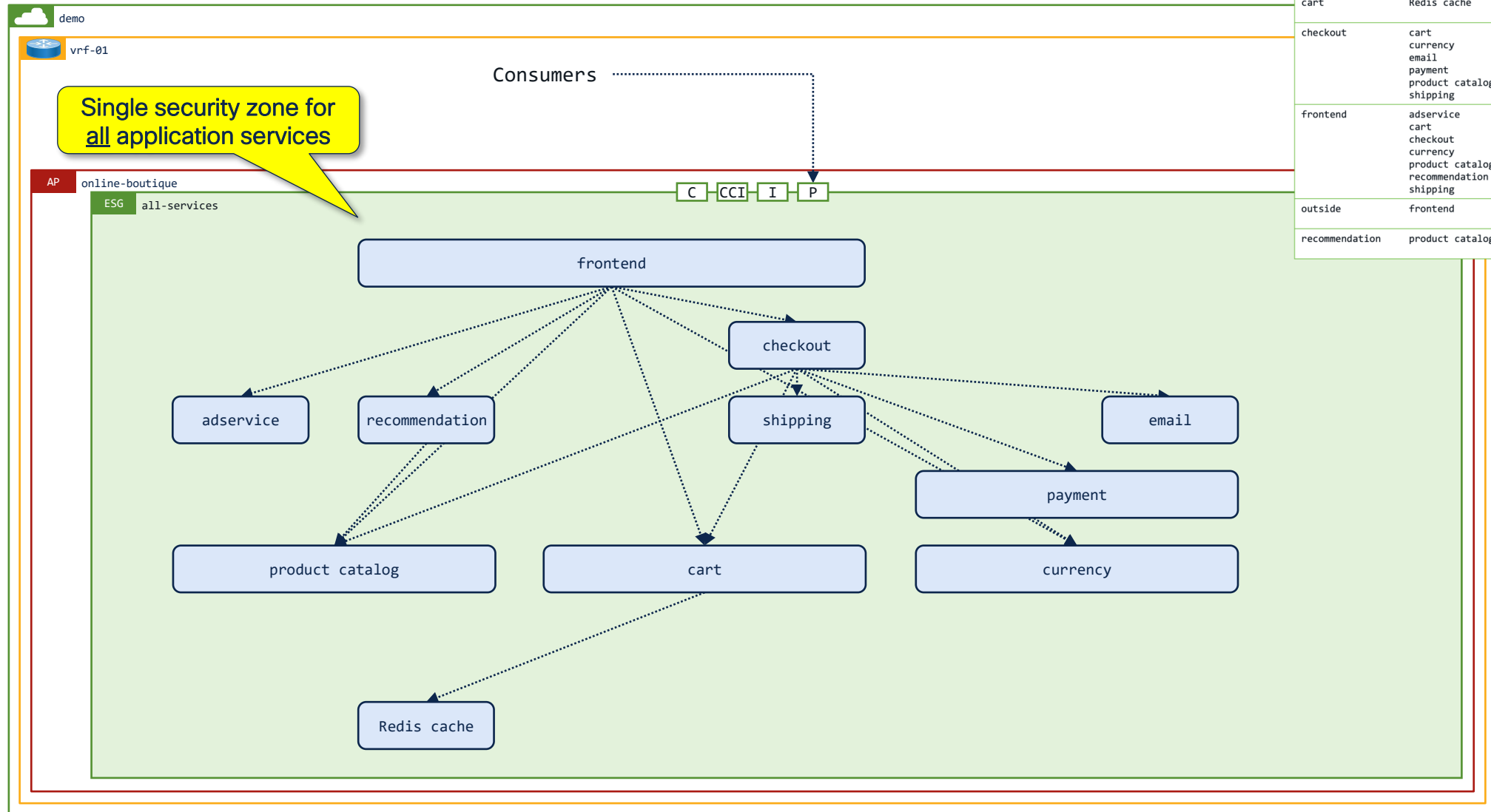


| Application Name | Contract | Application Name |
|------------------|--|--|
| application-01 | permit-to-all-applications (vzAny) | application-02 application-03 application-04 application-05 |
| | Filter: permit-any | |
| application-02 | permit-to-all-applications (vzAny) | application-01 application-03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

Automated Application Blueprints...

Application tiers across subnets

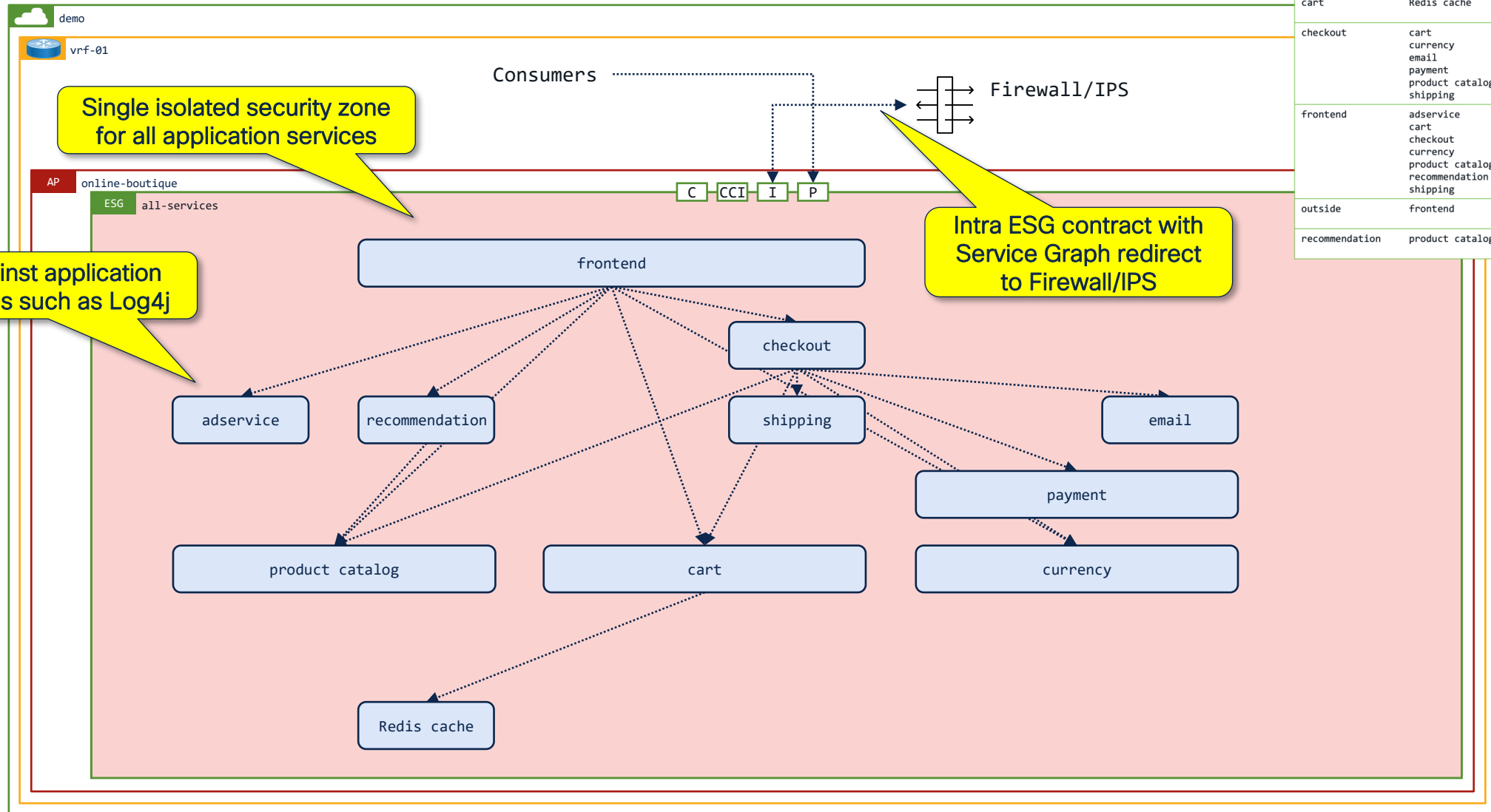
Application Centric Blueprint #1 – ESG “wrapper” for all services



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

Application tiers across subnets

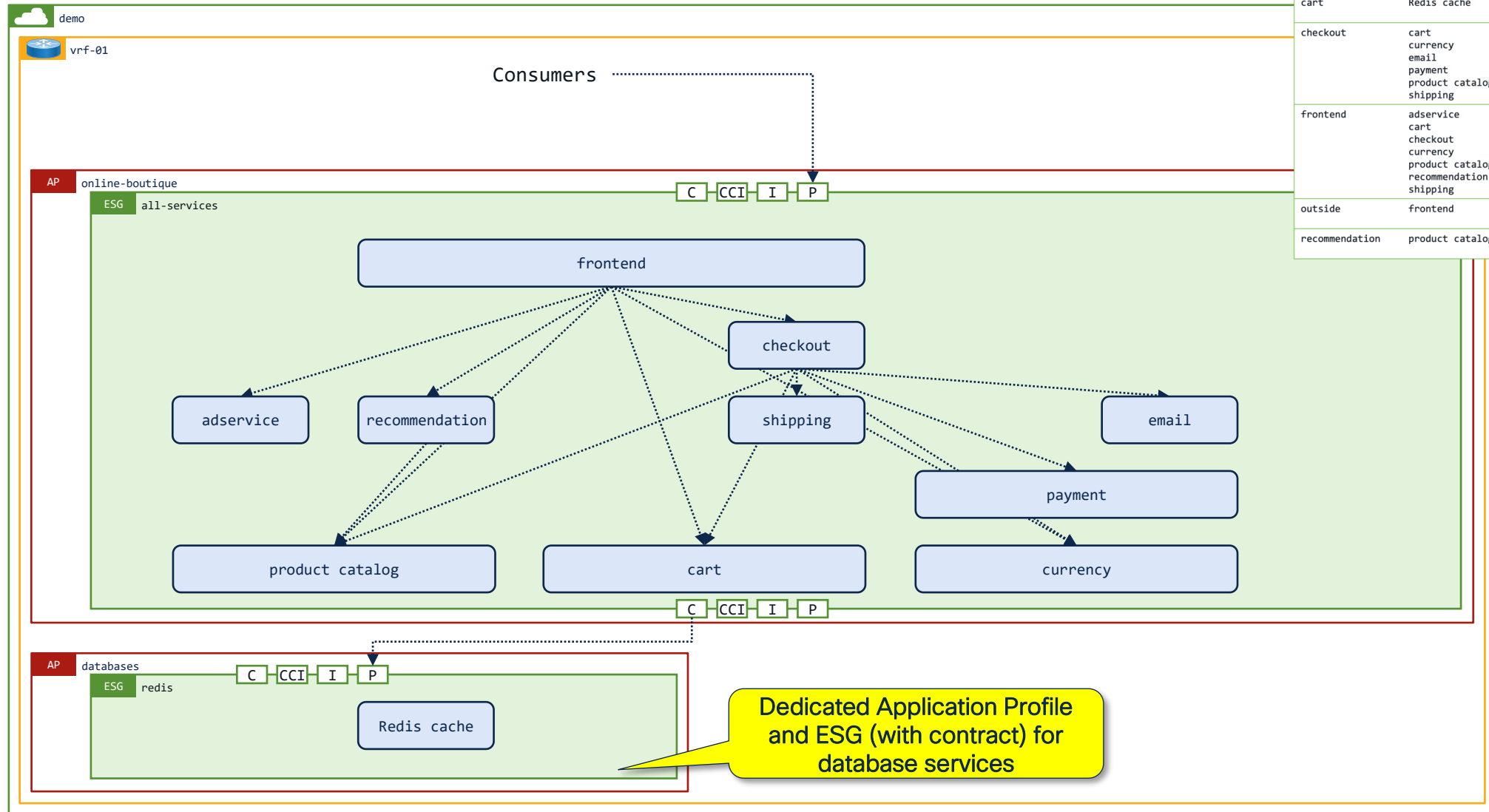
Application Centric Blueprint #2 – Intra ESG Isolation



| Source/Consumer | Target/Provider | Target/Provider Port |
|-----------------|-----------------|----------------------|
| cart | Redis cache | TCP 6379 |
| checkout | cart | TCP 7070 |
| | currency | TCP 7000 |
| | email | TCP 5000 |
| | payment | TCP 50051 |
| | product catalog | TCP 3550 |
| 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

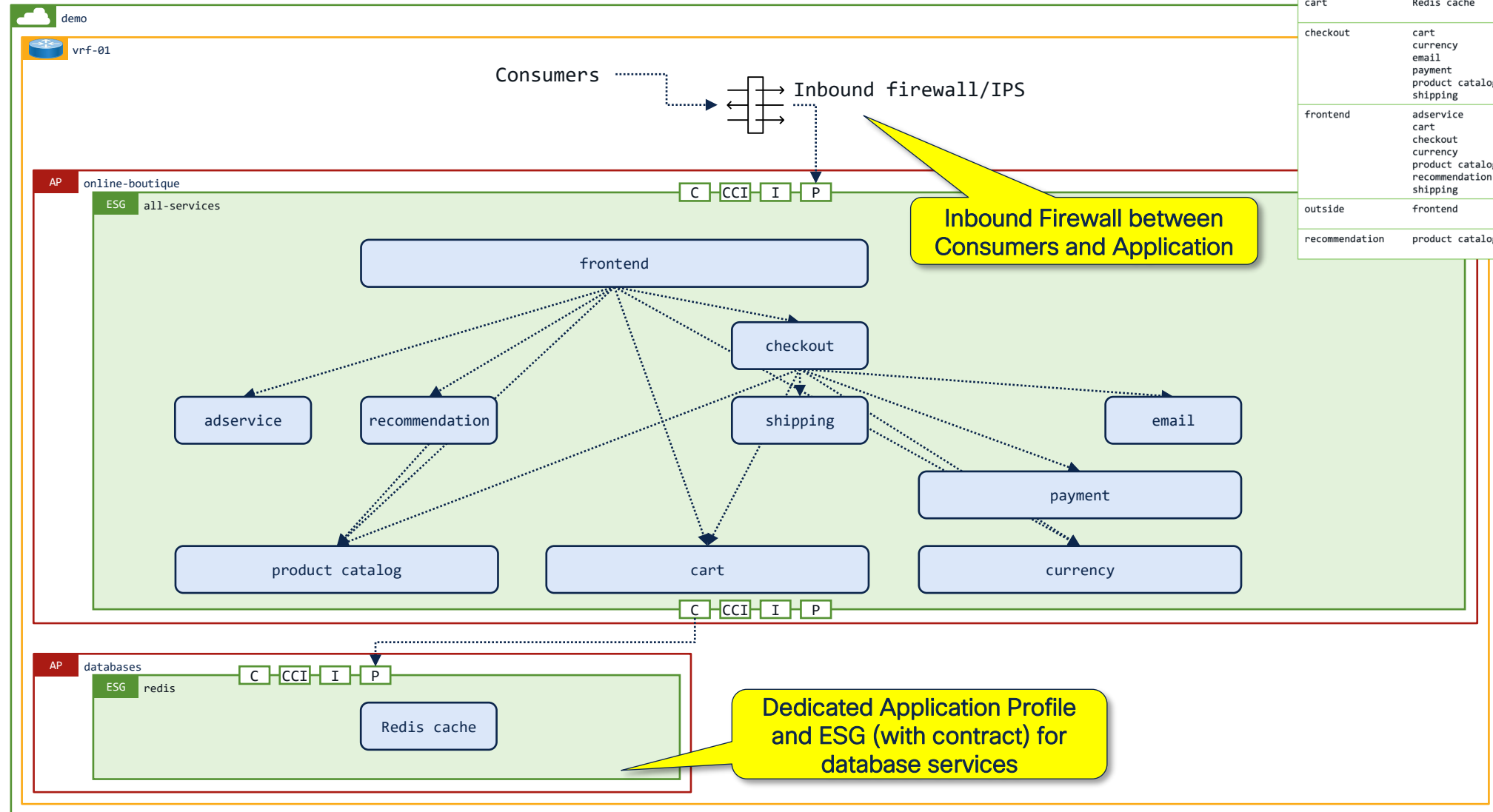
Application Centric Blueprint #3 – Dedicated AP/ESG for backend database



| 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

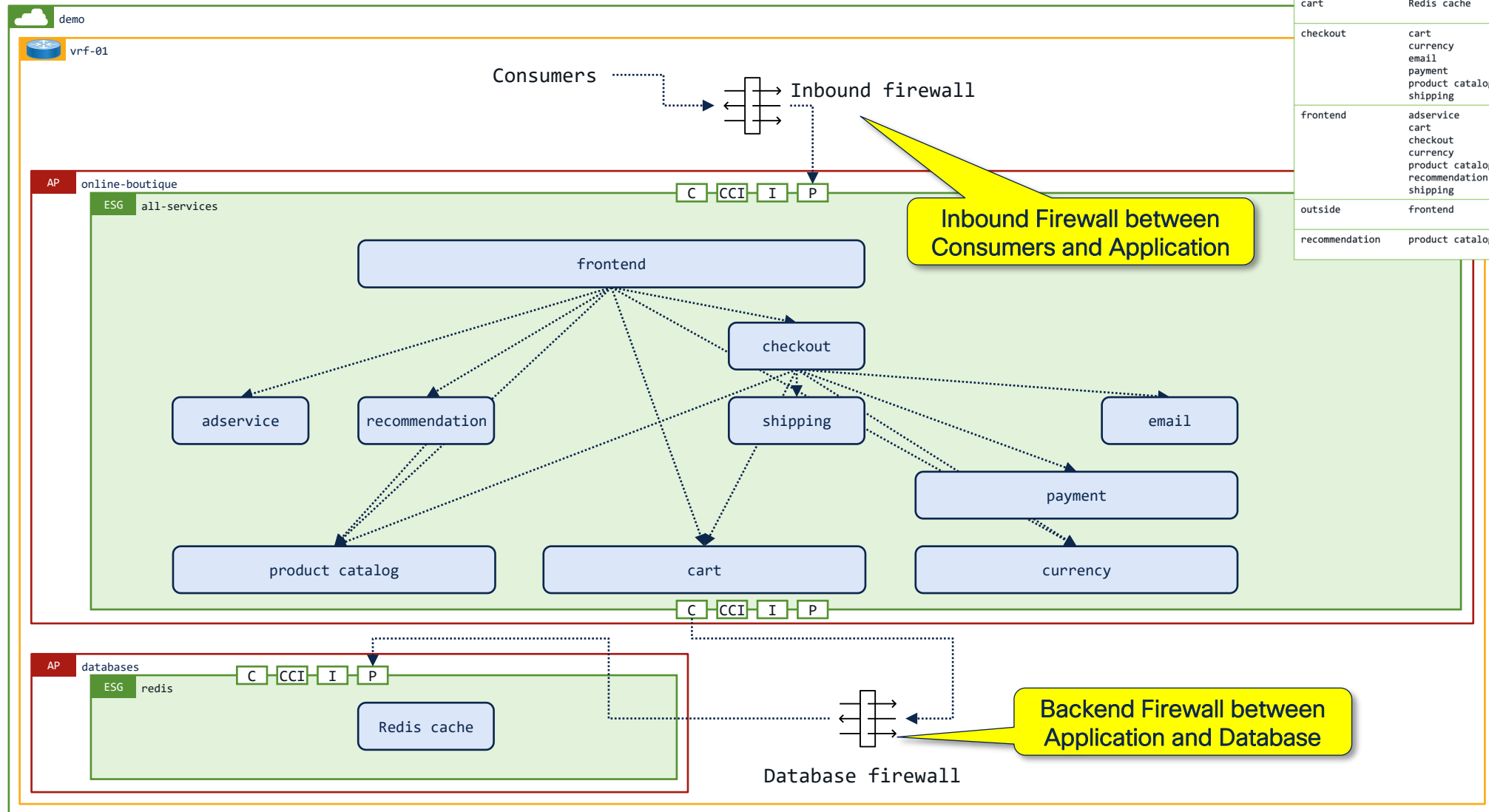
Application Centric Blueprint #4 – Inbound firewall/IPS + backend contract



| 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 | product catalog | TCP 3550 |
| | shipping | TCP 50051 |
| | adservice | TCP 9555 |
| | cart | TCP 7070 |
| | checkout | TCP 5050 |
| recommendation | 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 #5 – Inbound firewall/IPS + backend firewall/IPS

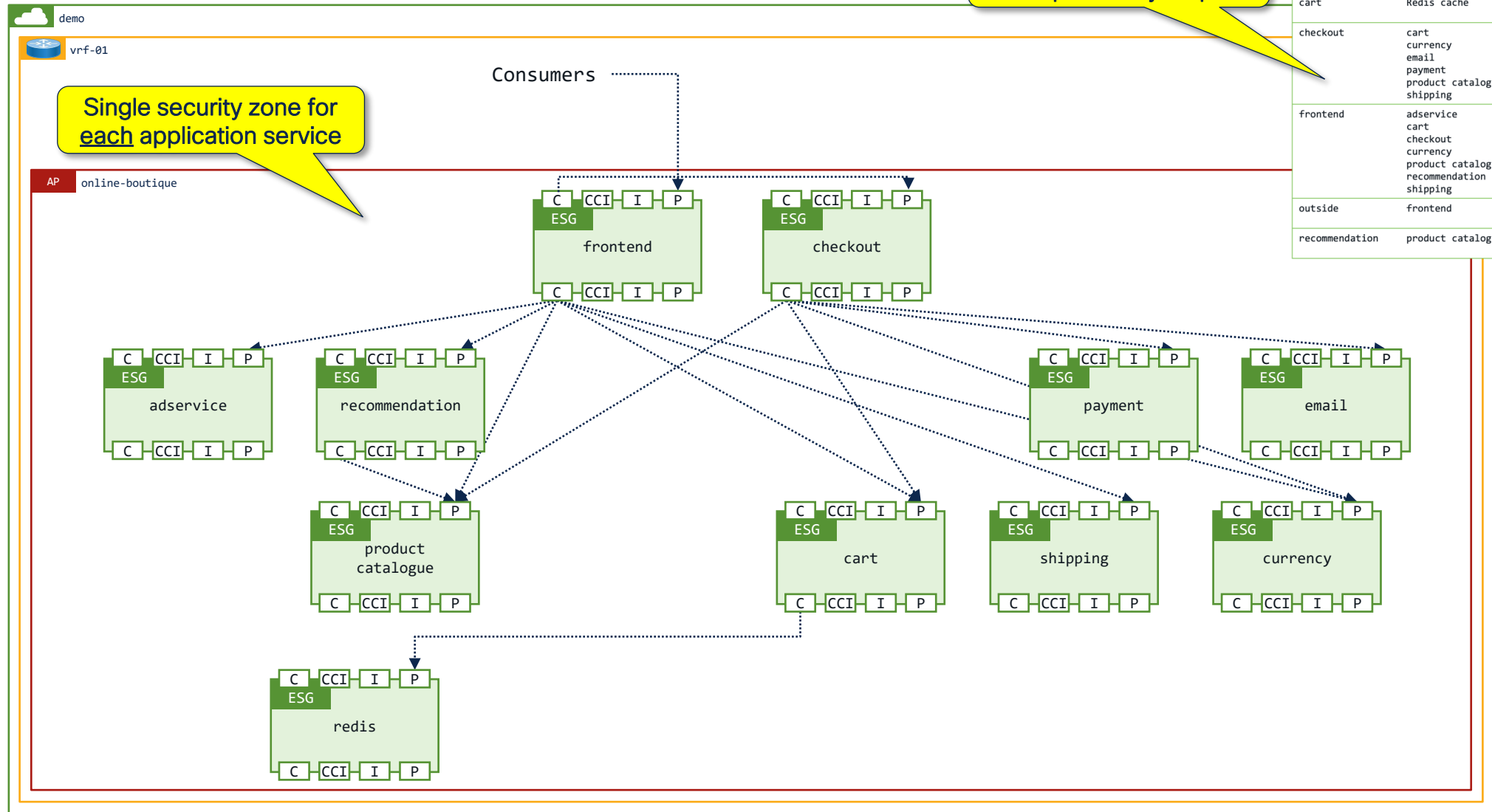


| Source/Consumer | Target/Provider | Target/Provider Port |
|-----------------|-----------------|----------------------|
| cart | Redis cache | TCP 6379 |
| checkout | cart | TCP 7070 |
| | currency | TCP 7000 |
| | email | TCP 5000 |
| | payment | TCP 50051 |
| | product catalog | TCP 3550 |
| frontend | product catalog | TCP 3550 |
| | shipping | TCP 50051 |
| | adservice | TCP 9555 |
| | cart | TCP 7070 |
| | checkout | TCP 5050 |
| recommendation | 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 #6 – ESG per application tier

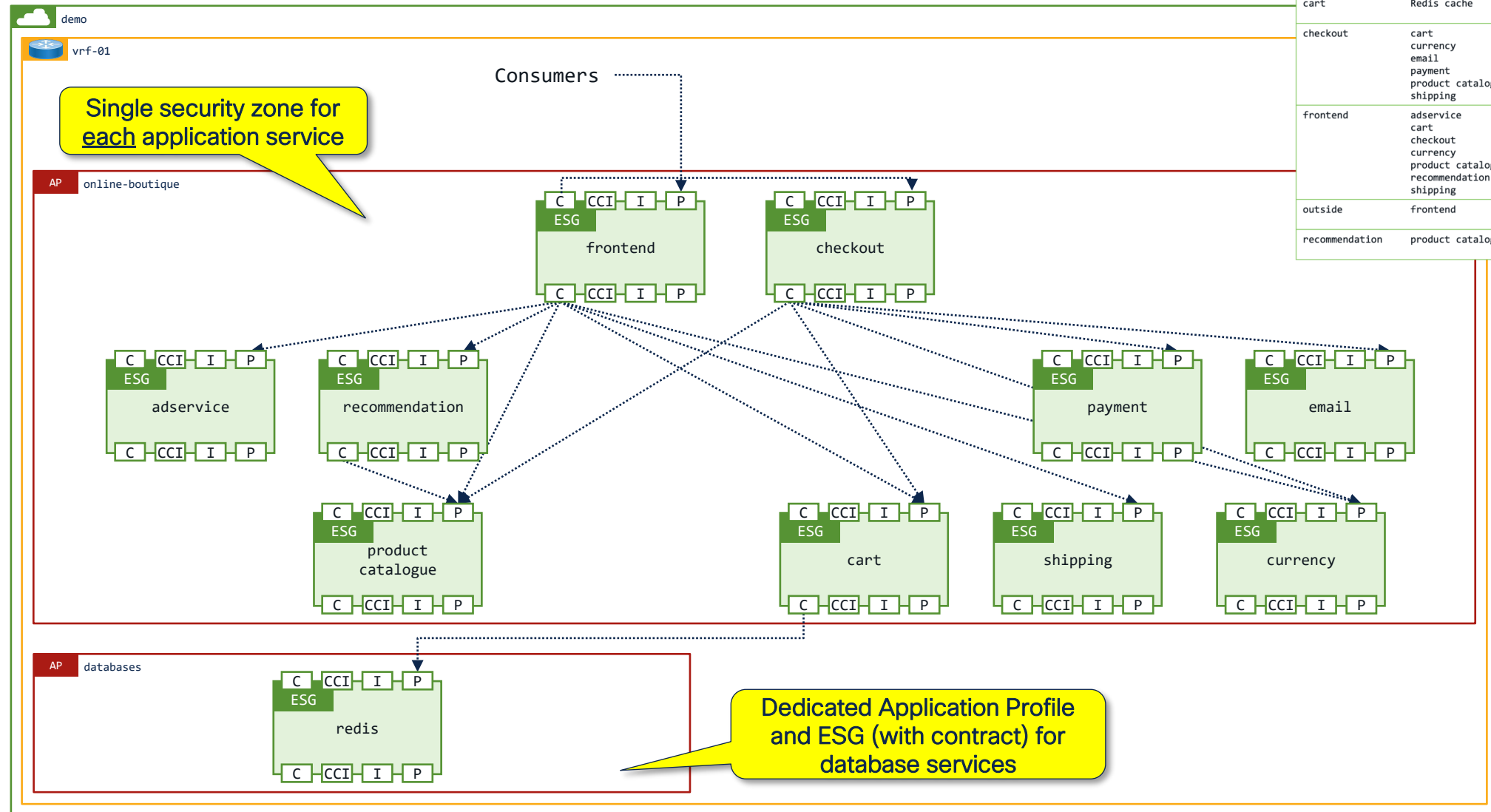
Requires application dependency map



| 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

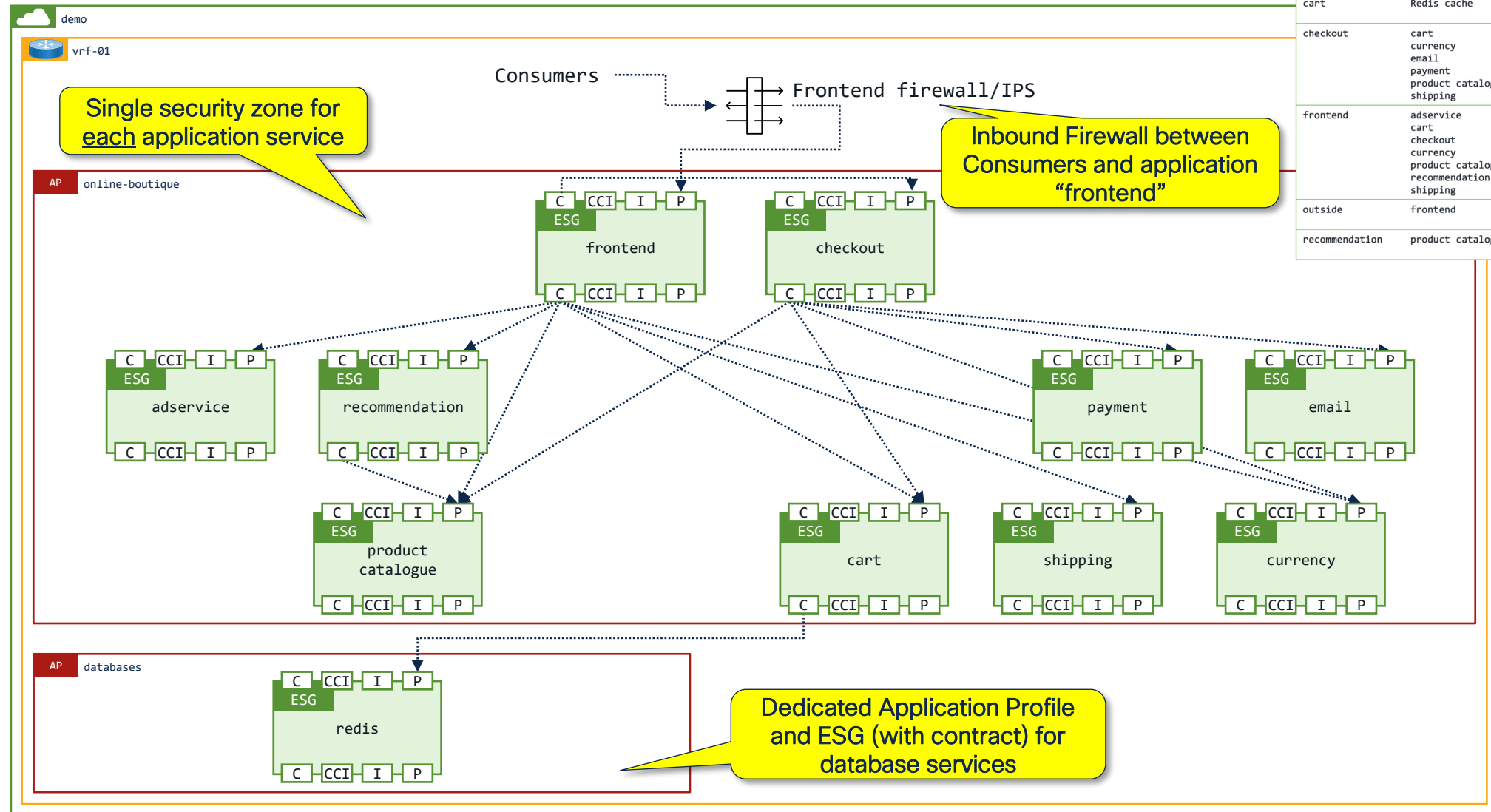
Application Centric Blueprint #7 – Dedicated AP/ESG for backend database



| 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

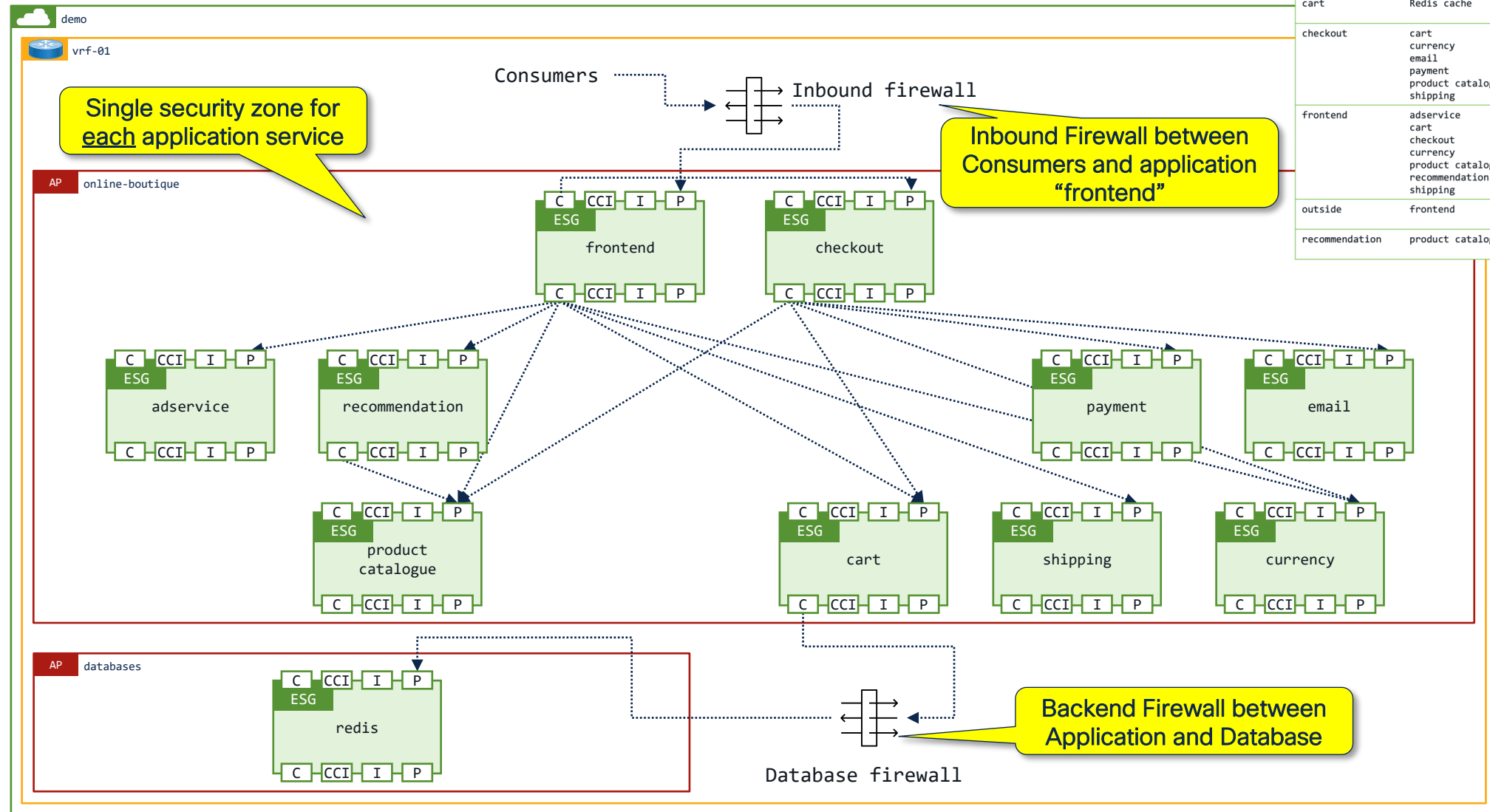
Application Centric Blueprint #8 – ESG per application tier + frontend firewall/IPS



| 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 | product catalog | TCP 3550 |
| | shipping | TCP 50051 |
| | adservice | TCP 9555 |
| | cart | TCP 7070 |
| | currency | TCP 7000 |
| recommendation | currency | TCP 7000 |
| | product catalog | TCP 3550 |
| | shipping | TCP 8080 |
| outside | frontend | TCP 80/8080 |
| recommendation | product catalog | TCP 3550 |

Application tiers across subnets

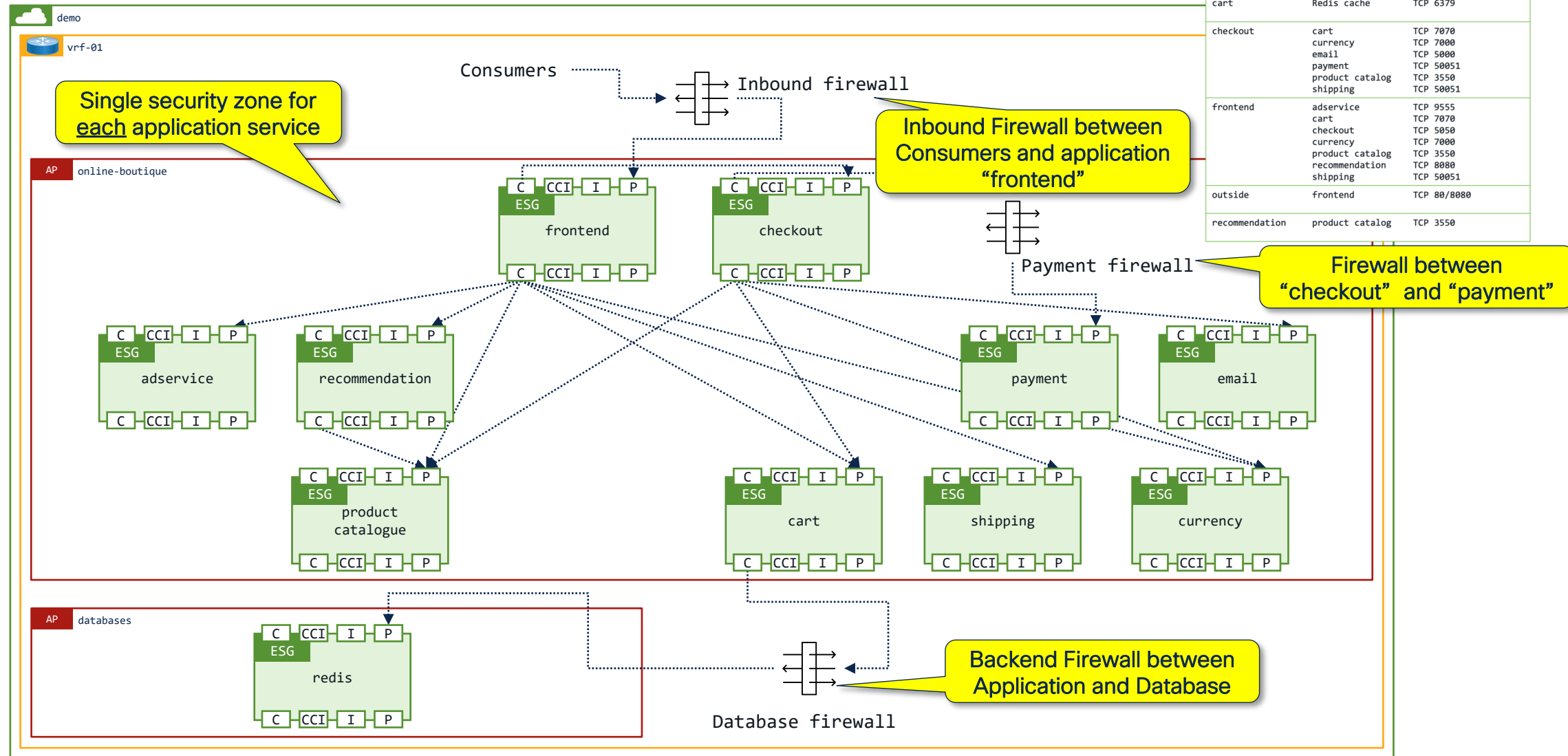
Application Centric Blueprint #9 – ESG per application tier + frontend firewall/IPS + backend firewall/IPS



| 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 |
| outside | frontend | TCP 80/8080 |
| recommendation | product catalog | TCP 3550 |

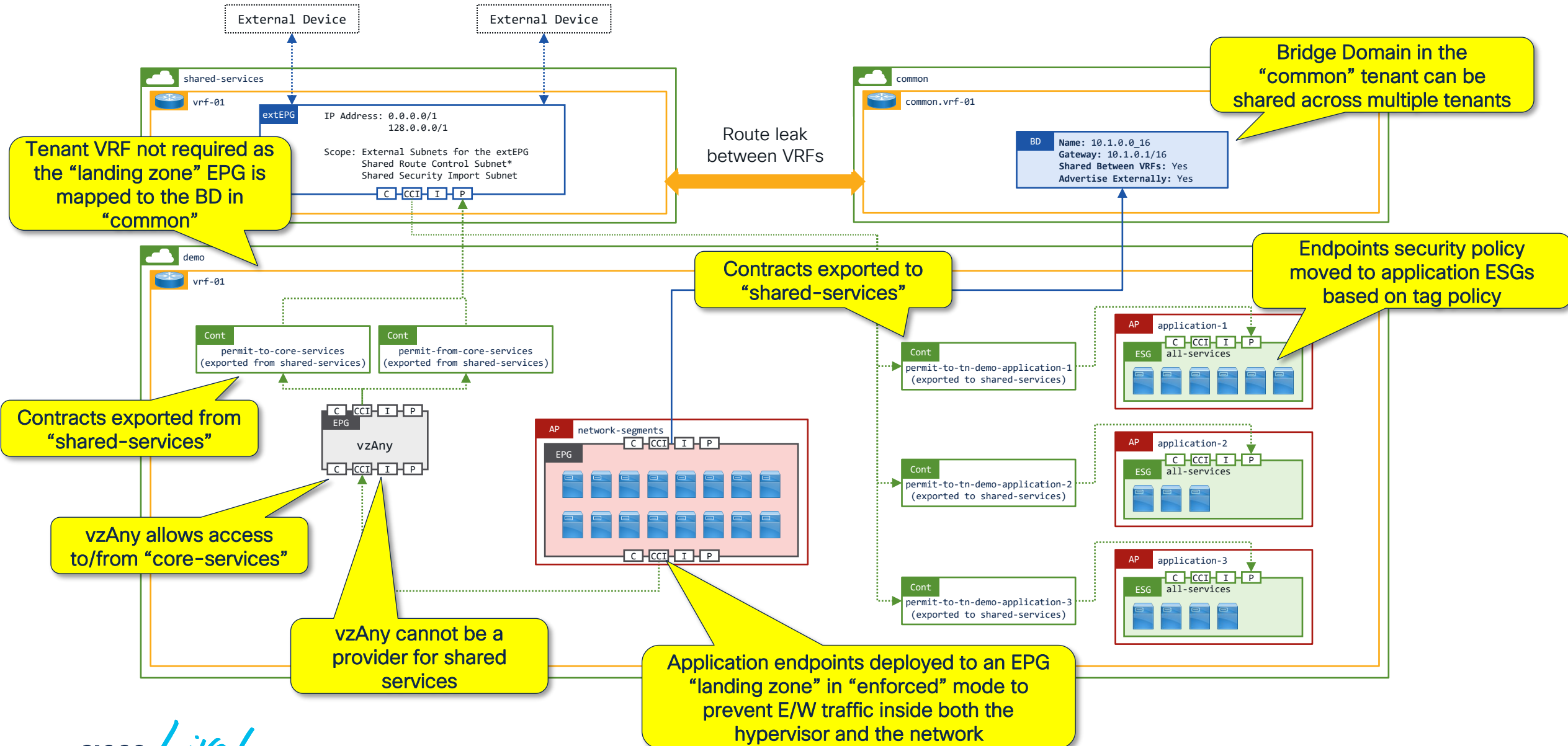
Application tiers across subnets

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

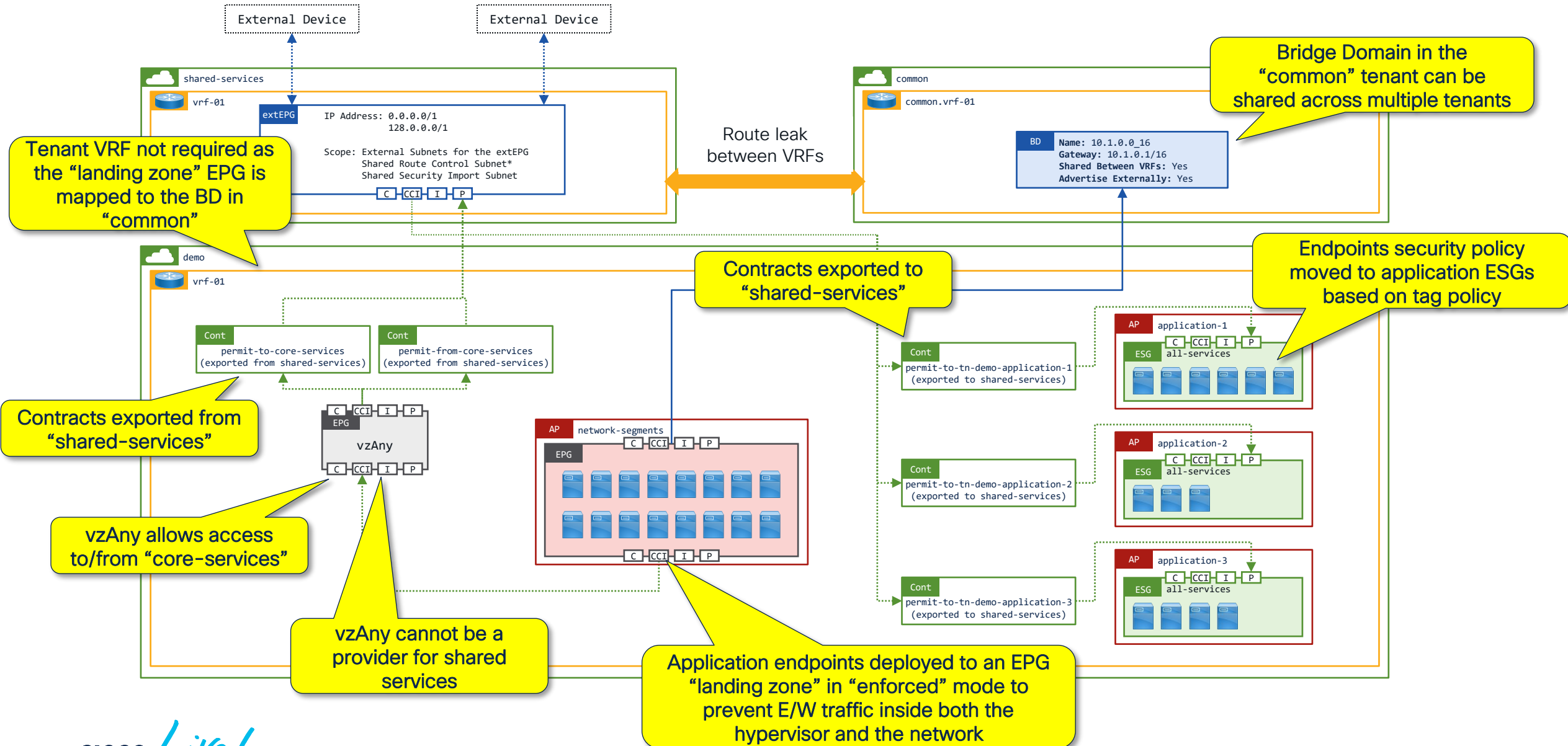


The ultimate aim is to provide a fully consumable fabric where resources are automated on demand...

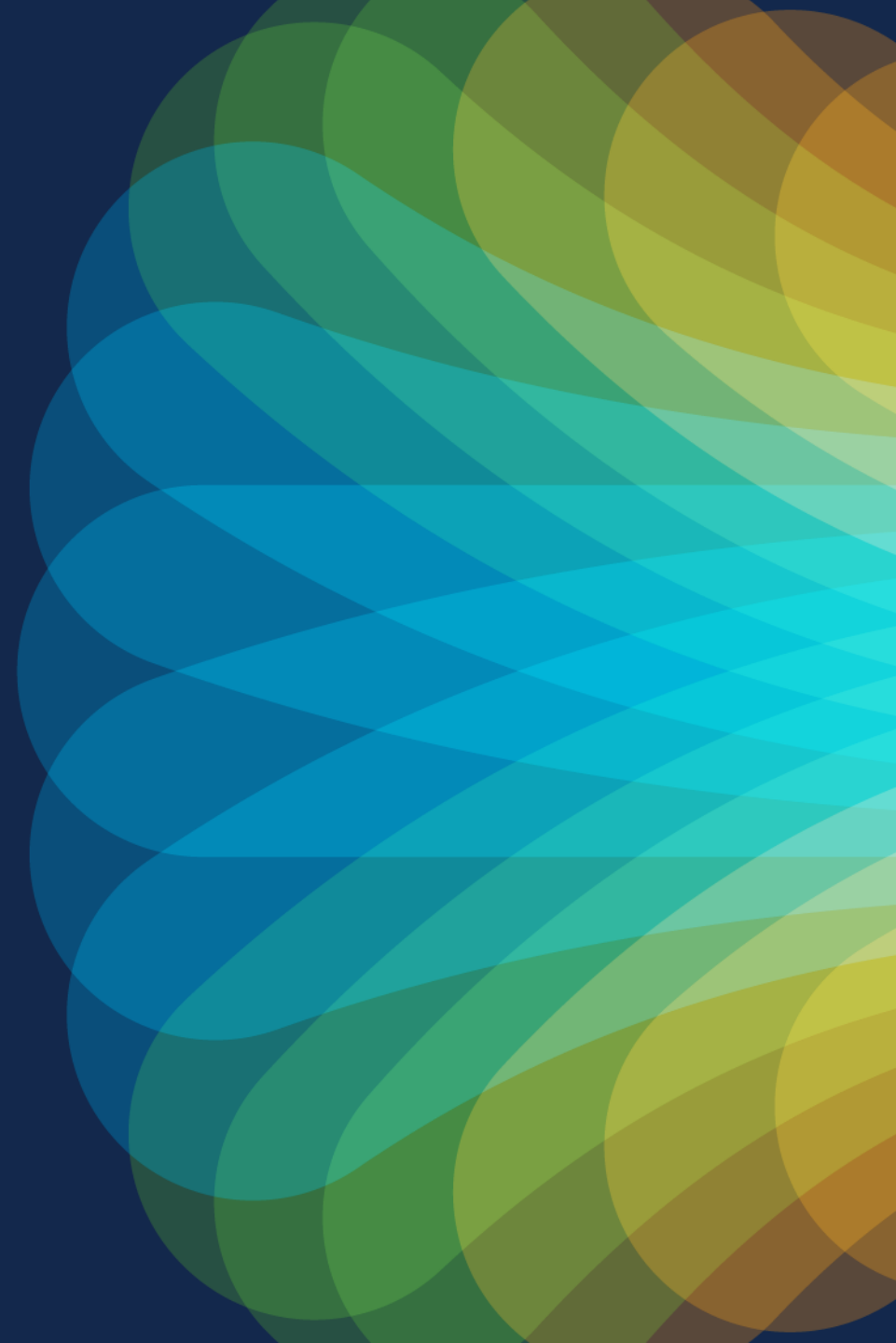
Example Internal Private Cloud Design – shared subnet(s)



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
- 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

Save Download Print

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)

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...



The bridge to possible

Thank you

CISCO *Live!*

The Cisco Live! logo features the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, cursive script font.

CISCO *Live!*

The text "Let's go" is displayed in a dark blue, sans-serif font. The background behind the text is a vibrant, multi-colored geometric pattern of overlapping triangles and lines, transitioning from red and orange on the left to blue and green on the right, with a bright white light source on the right side.

Let's go