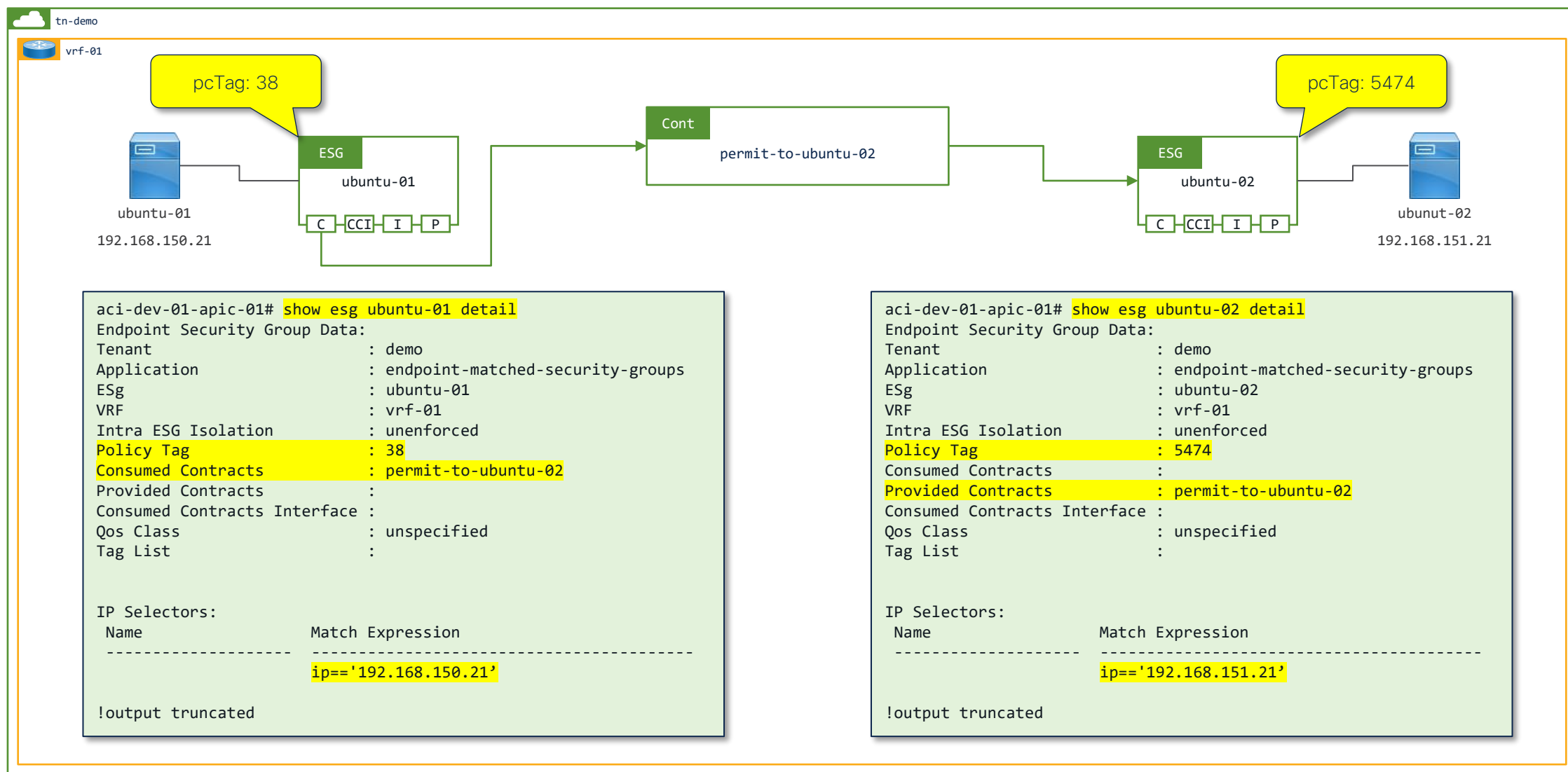
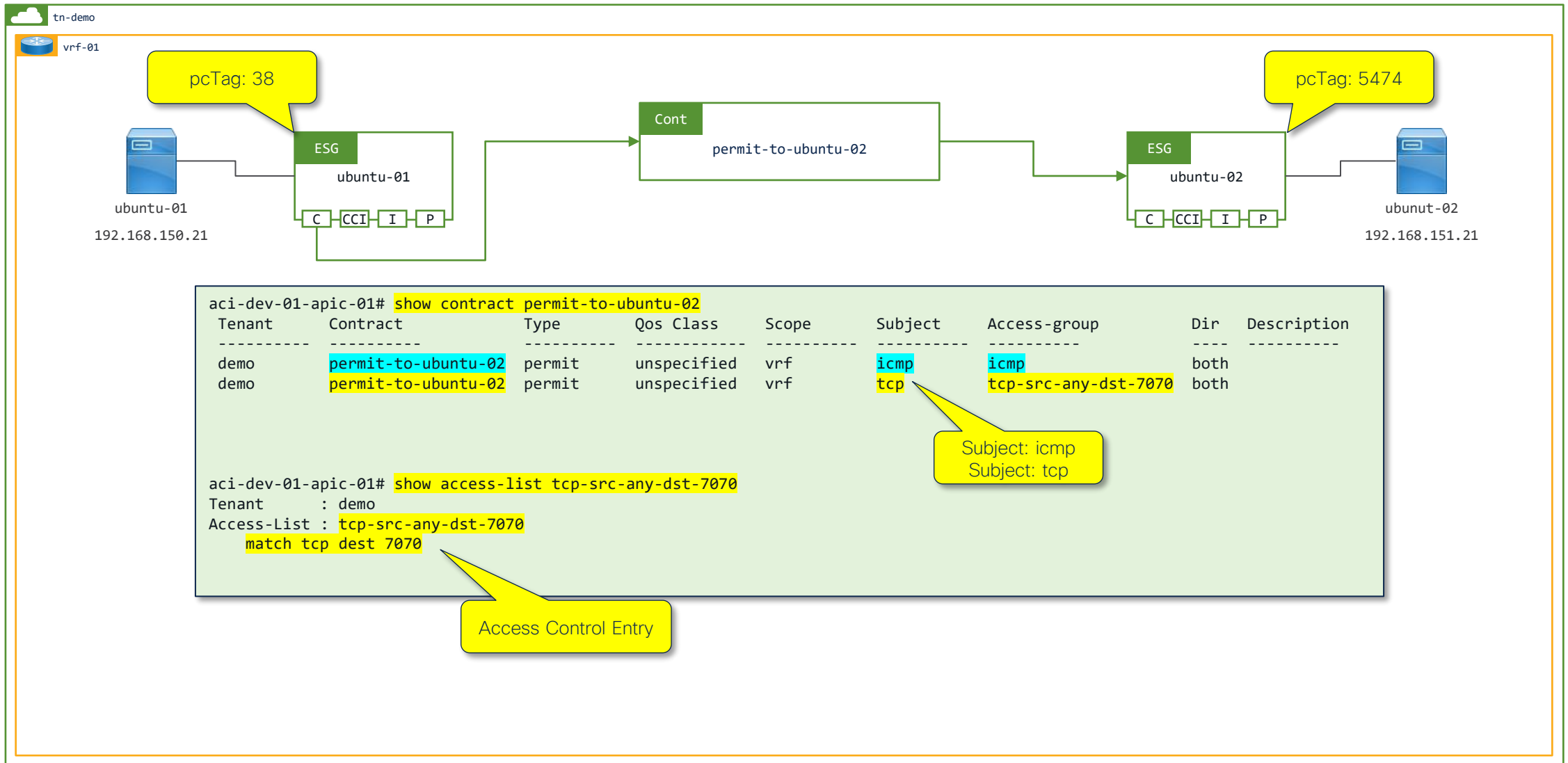


Verifying contracts...

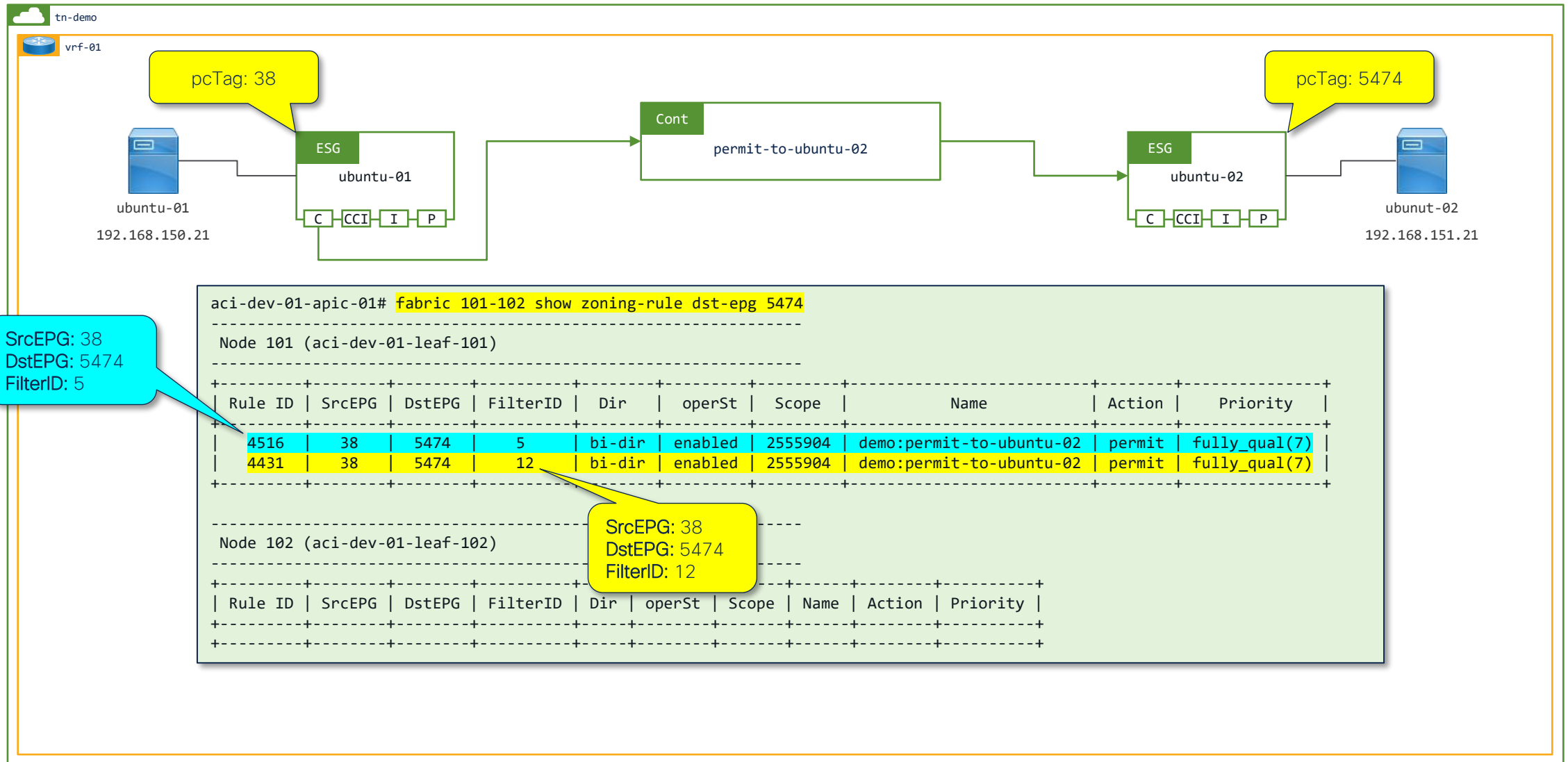
Verifying Contract Operation



Verifying Contract Operation



Verifying Contract Operation



Verifying Contract Operation



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

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

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

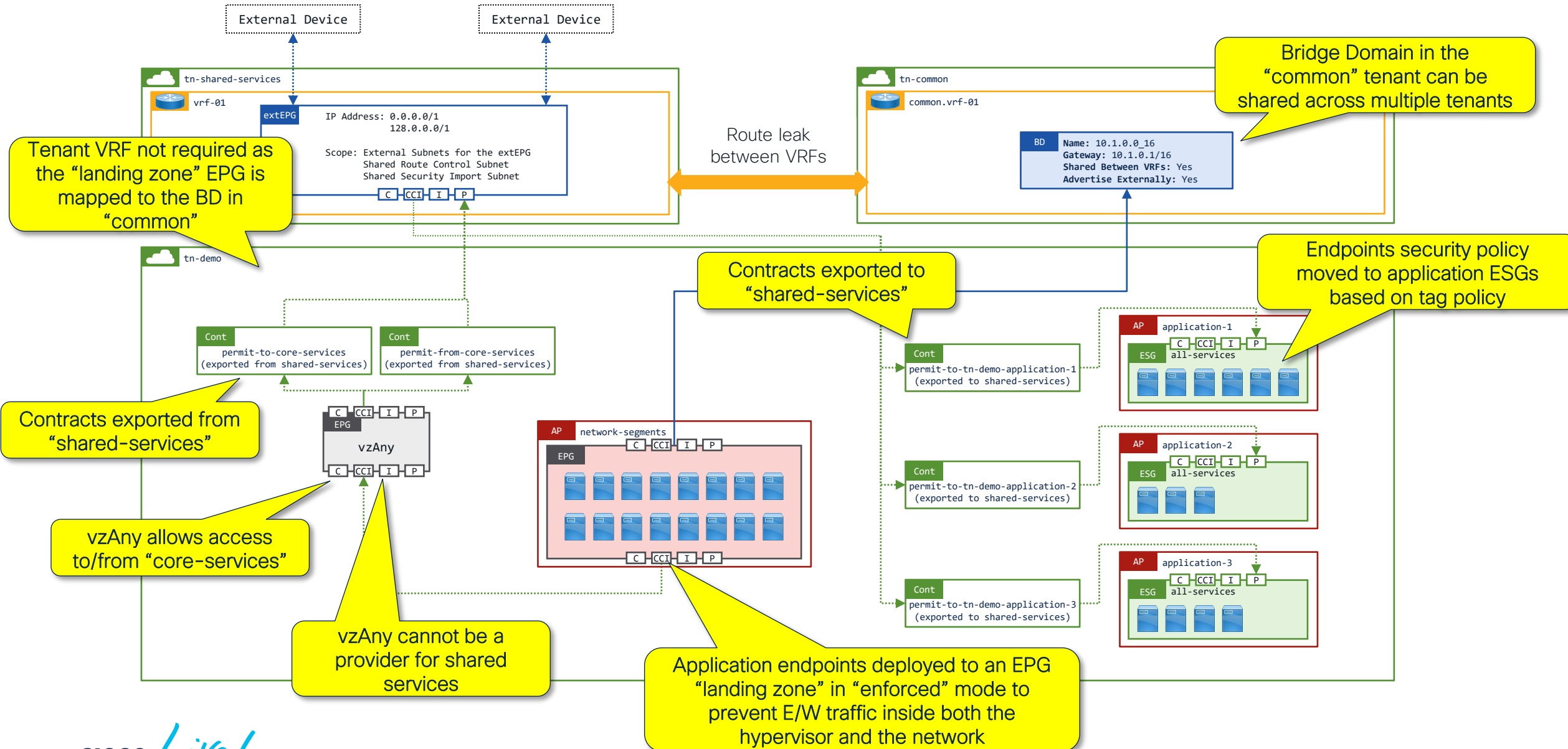
```
Node 102 (aci-dev-01-leaf-102)
```

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

Blueprints

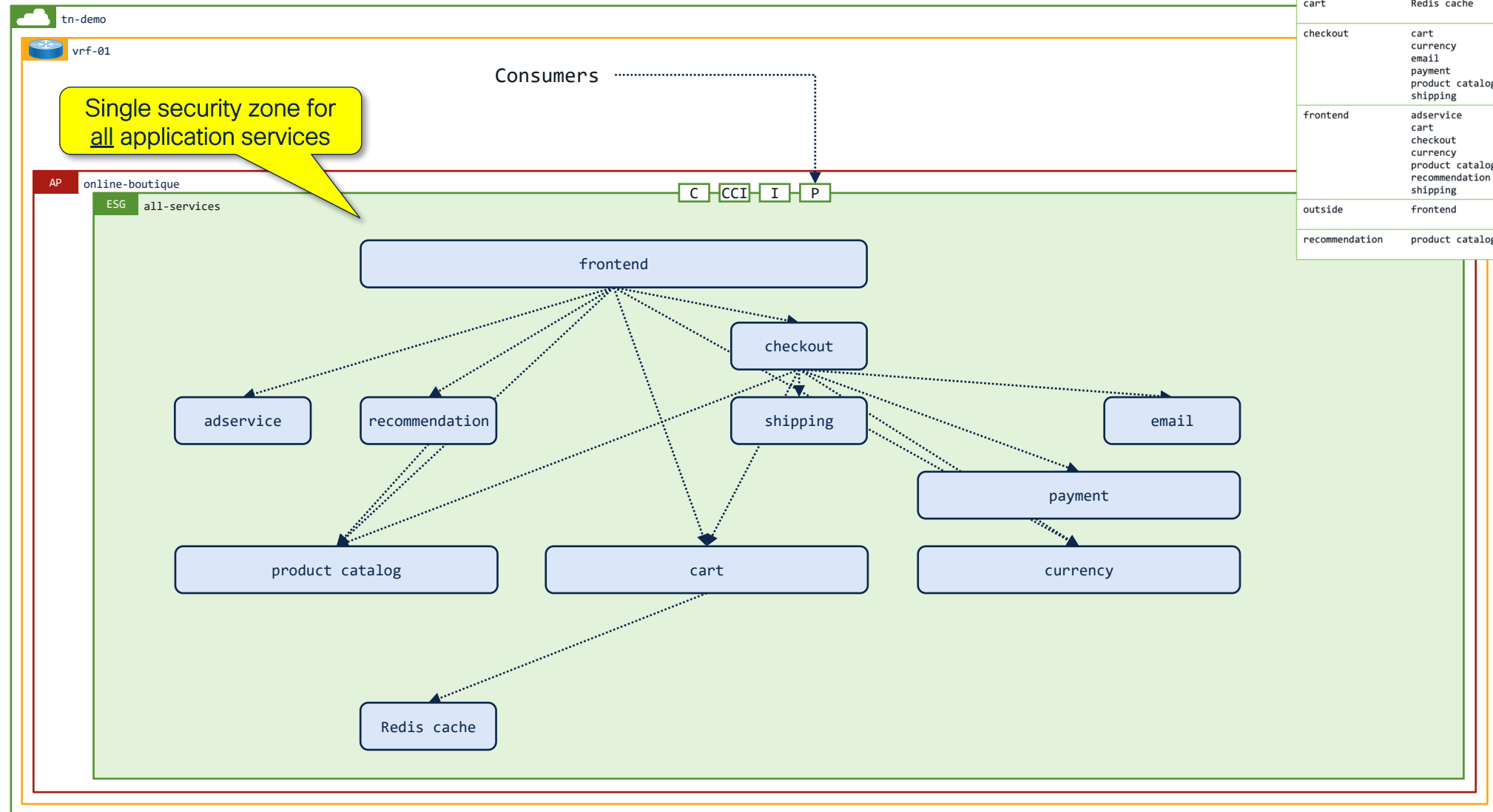


Example Internal Private Cloud Design – shared subnet(s)



Application tiers across subnets

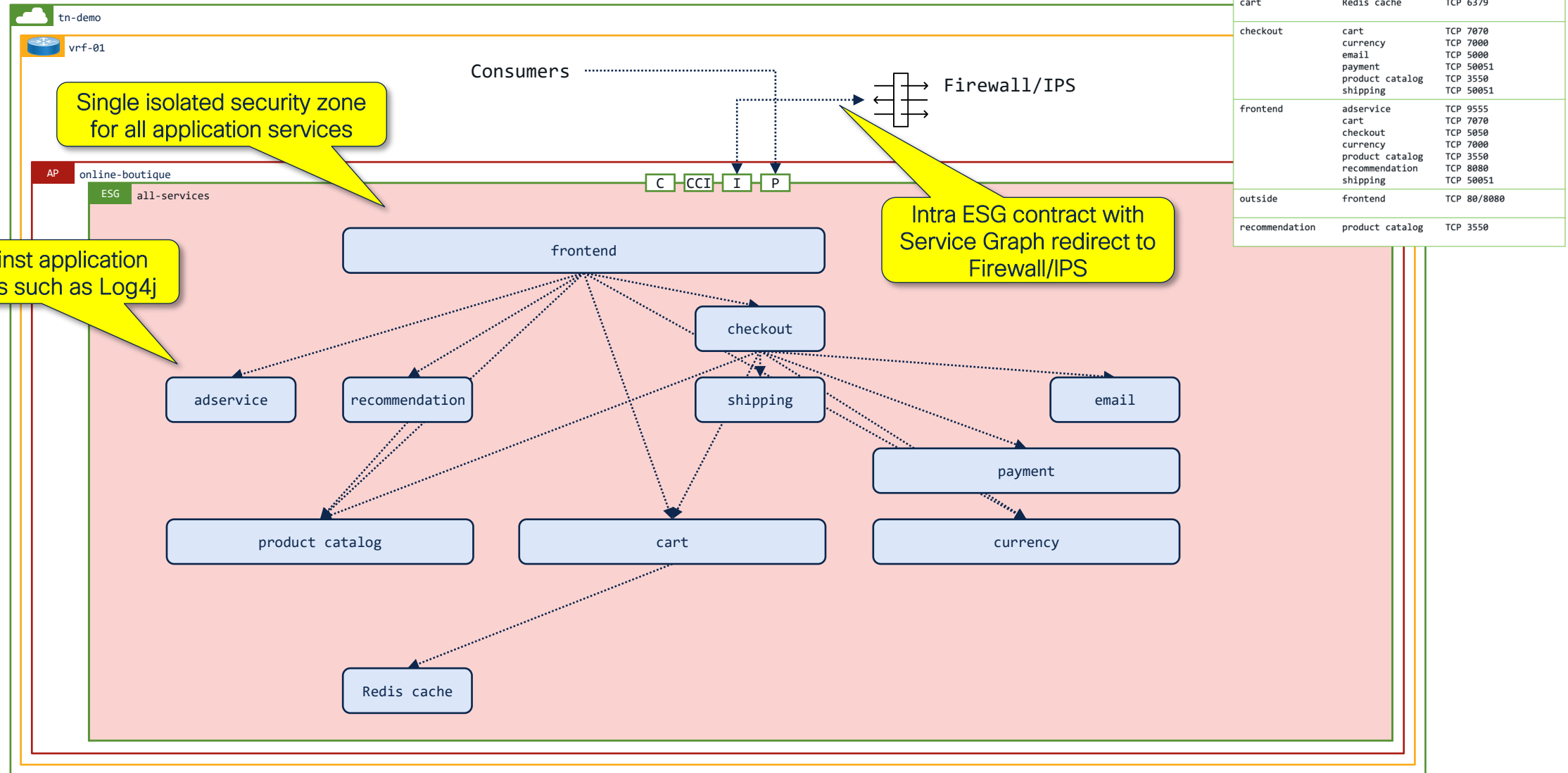
Application Centric Blueprint #1 – ESG “wrapper” for all services



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

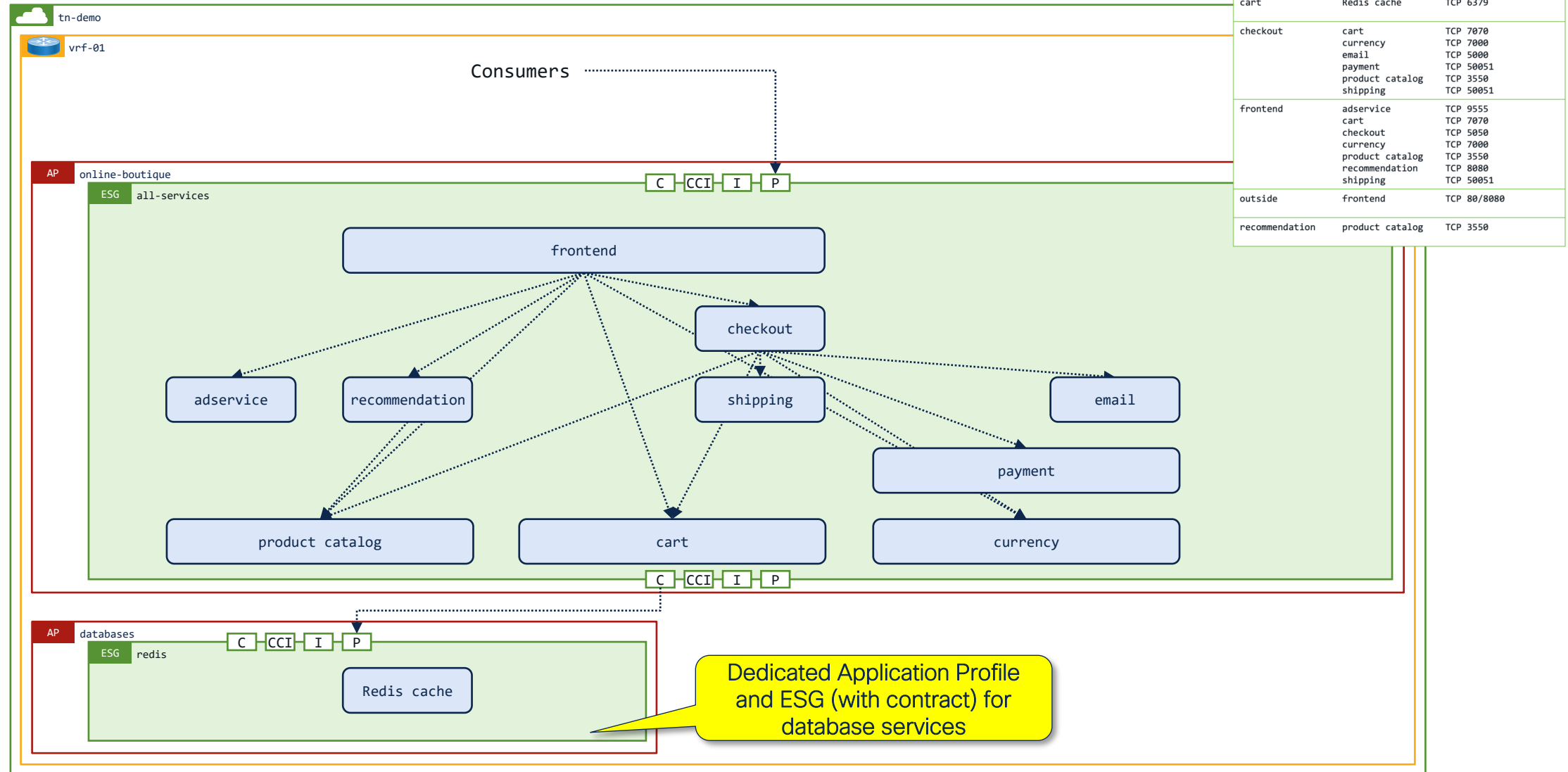
Application tiers across subnets

Application Centric Blueprint #2 – Intra ESG Isolation



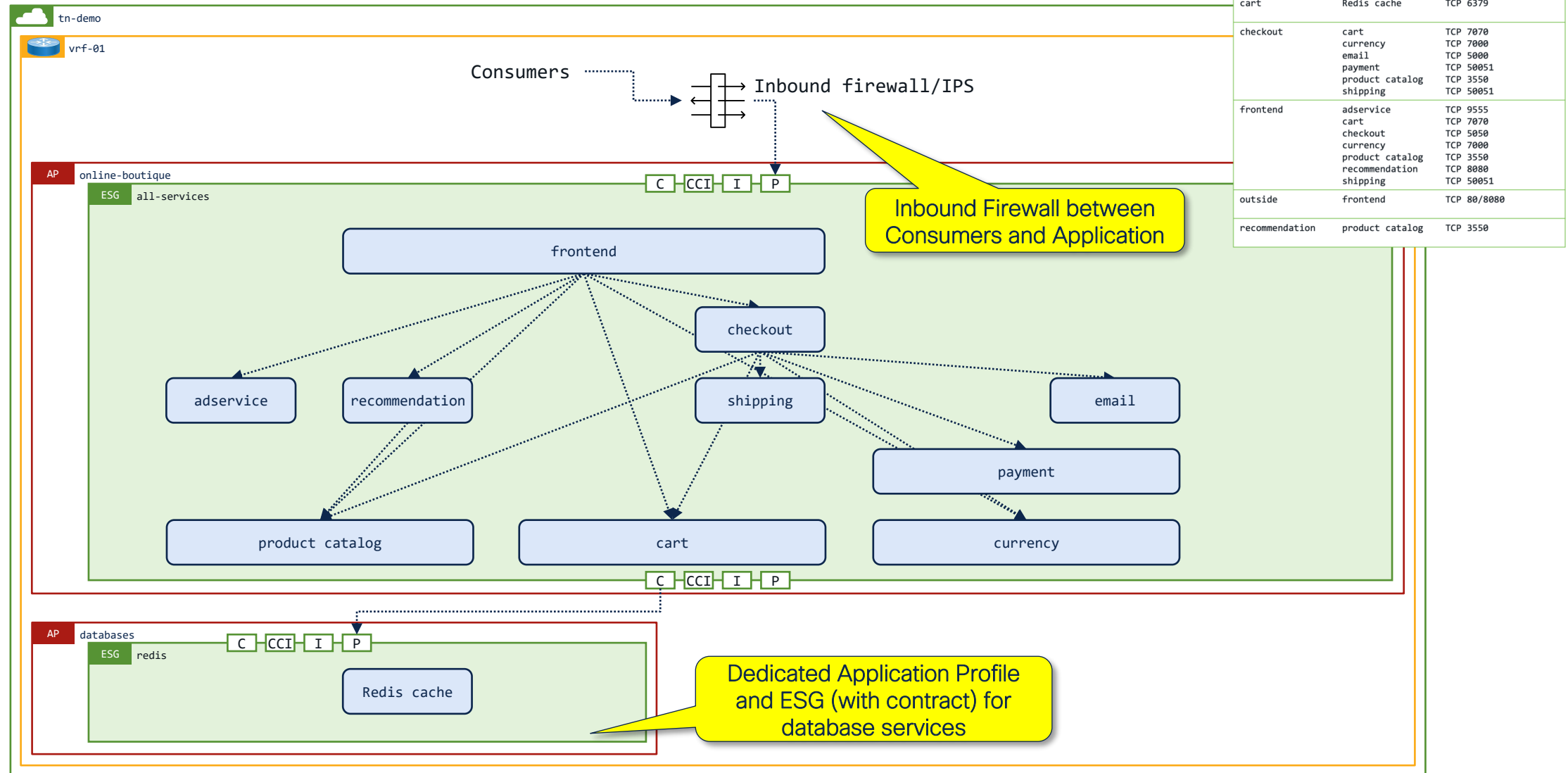
Application tiers across subnets

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



Application tiers across subnets

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



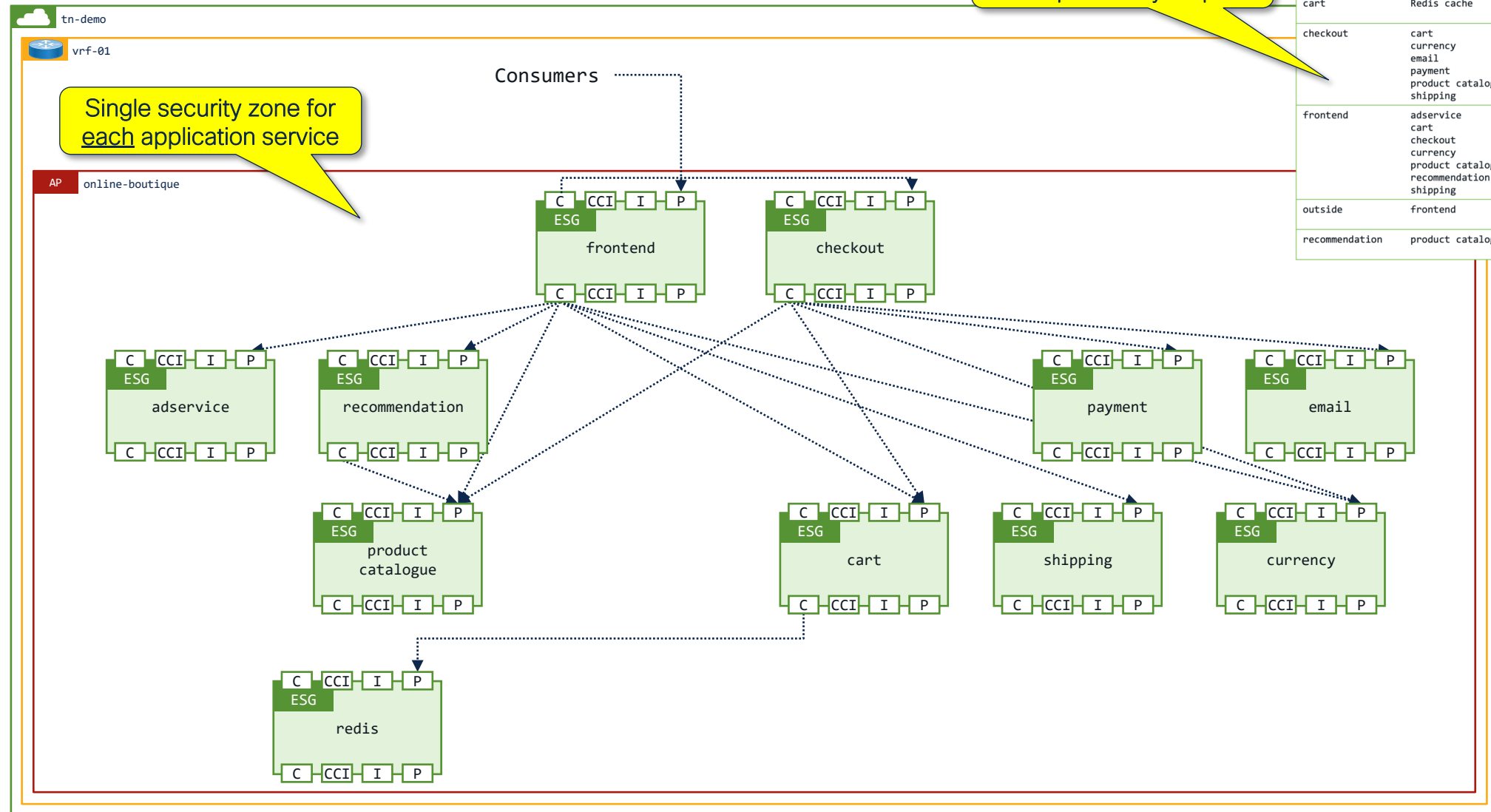
Application Centric Blueprint #5 – Inbound firewall/IPS + backend firewall/IPS



Application tiers across subnets

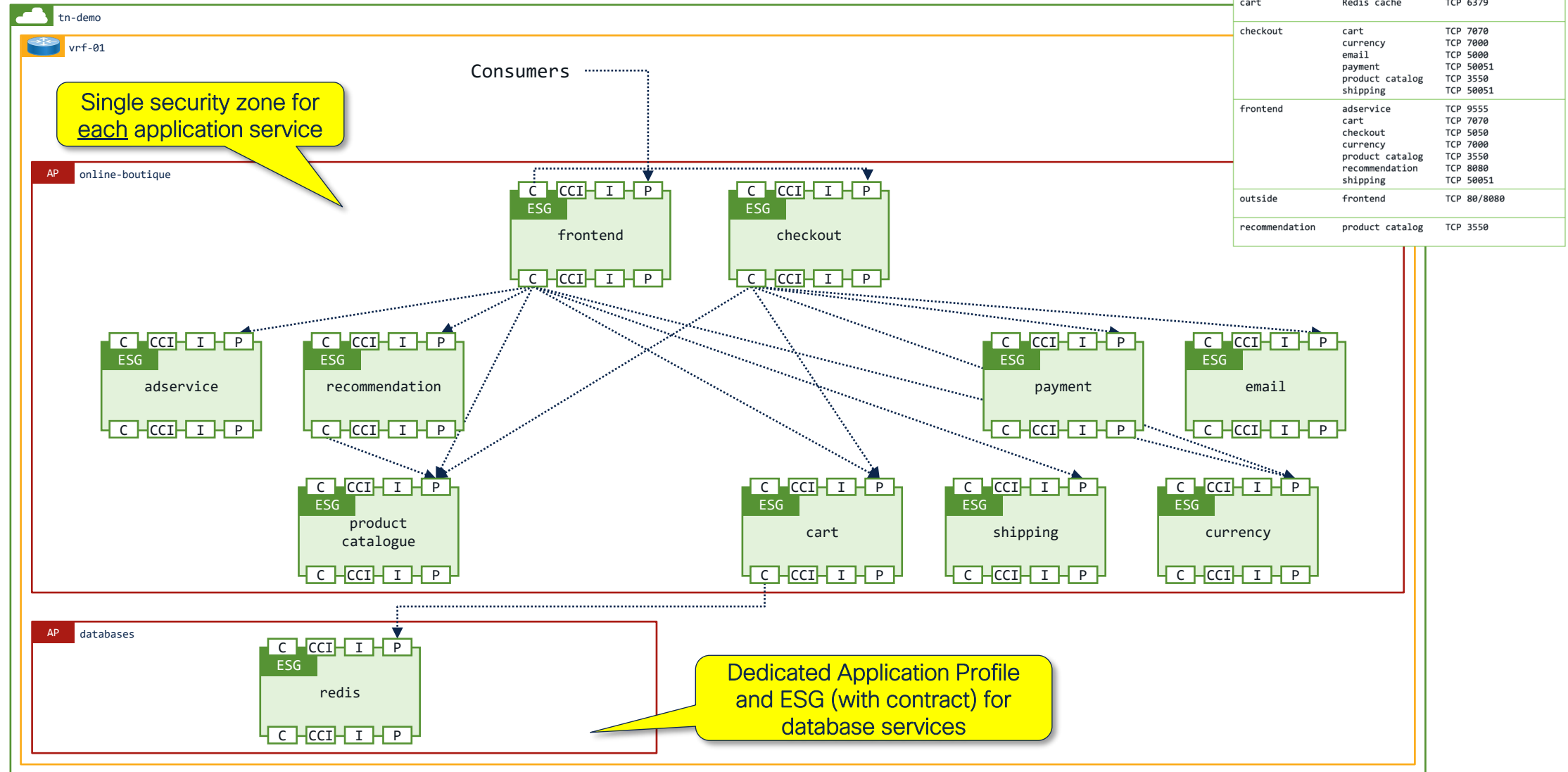
Application Centric Blueprint #6 – ESG per application tier

Requires application dependency map



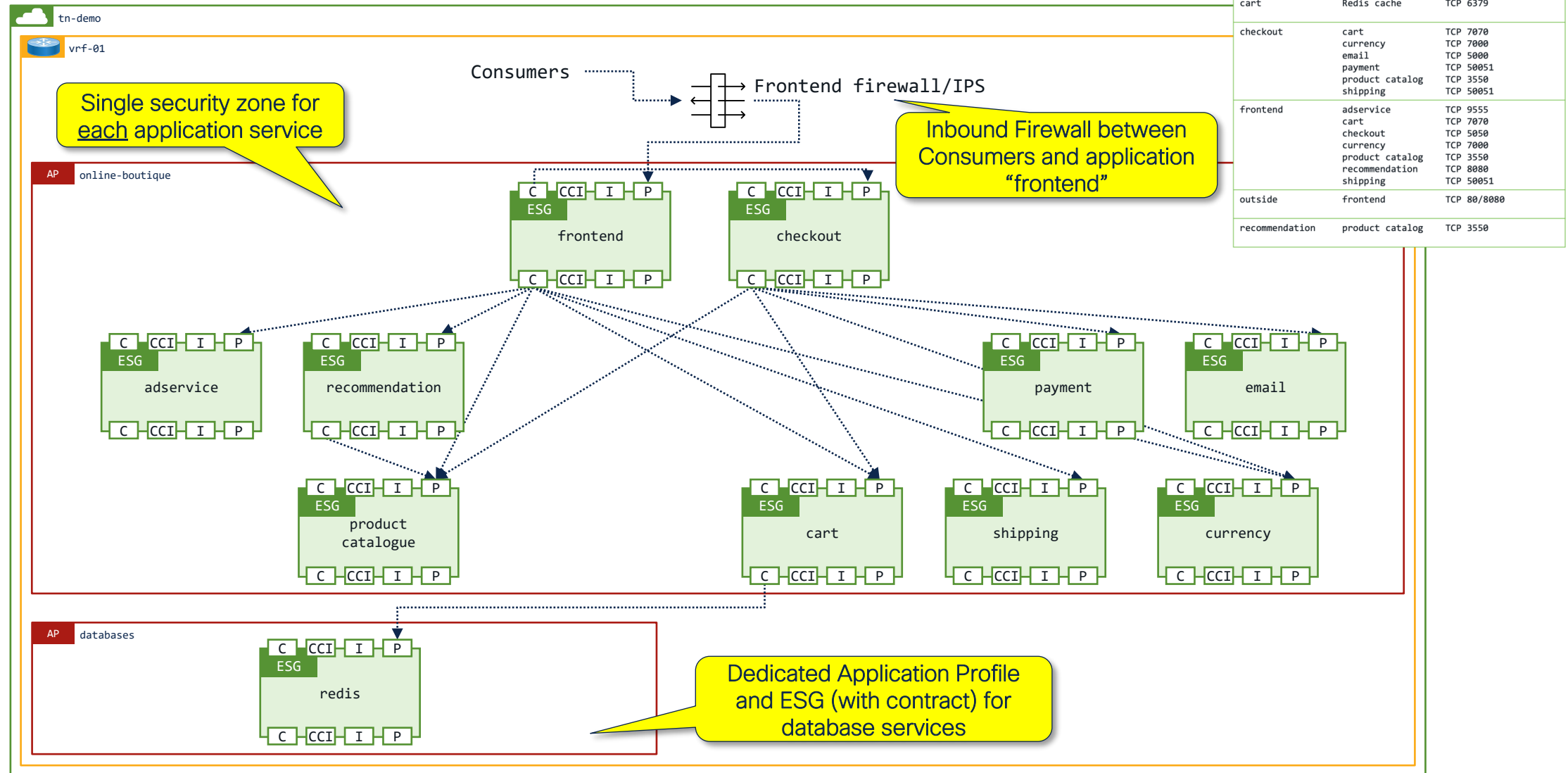
Application tiers across subnets

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



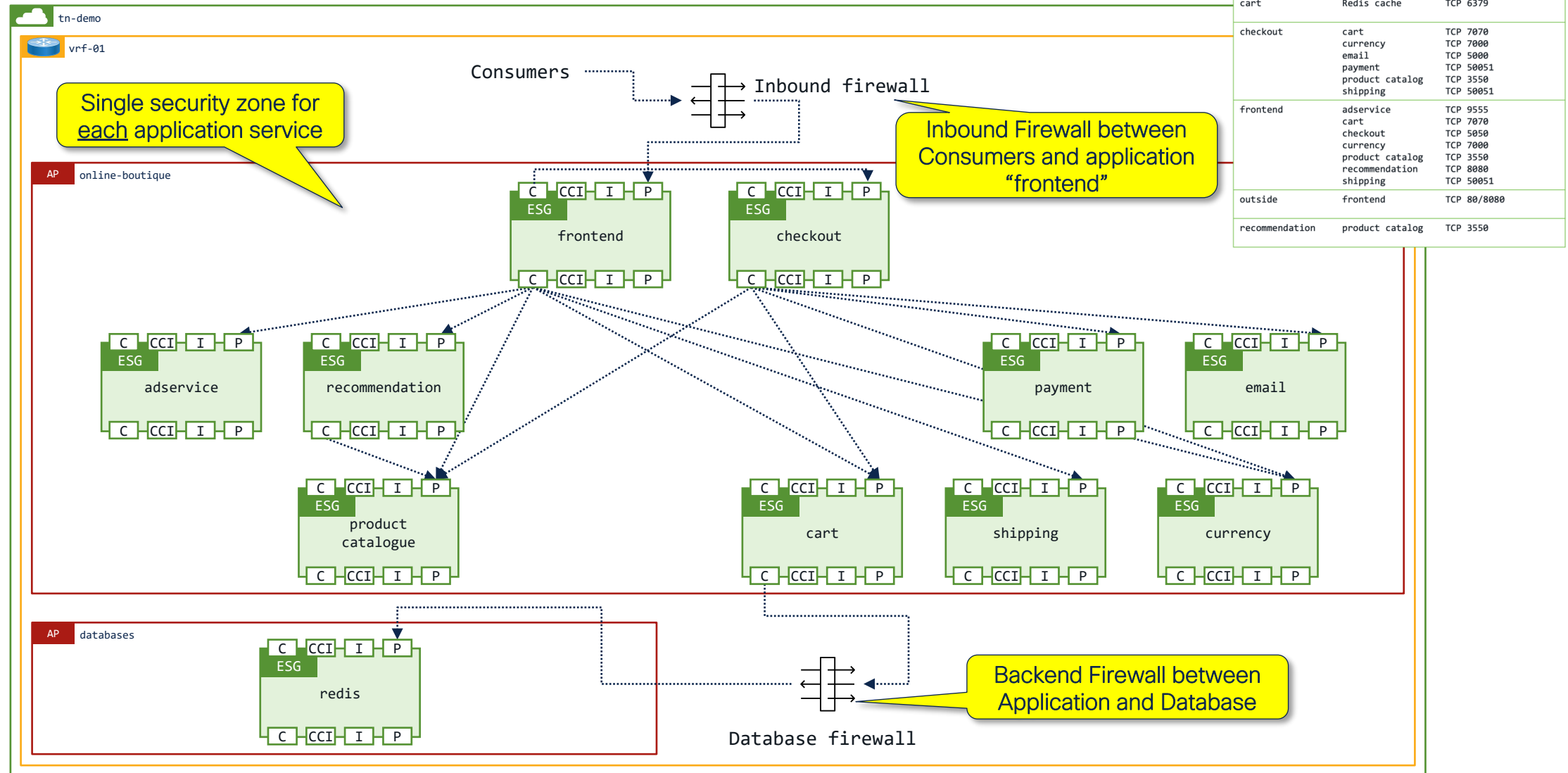
Application tiers across subnets

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



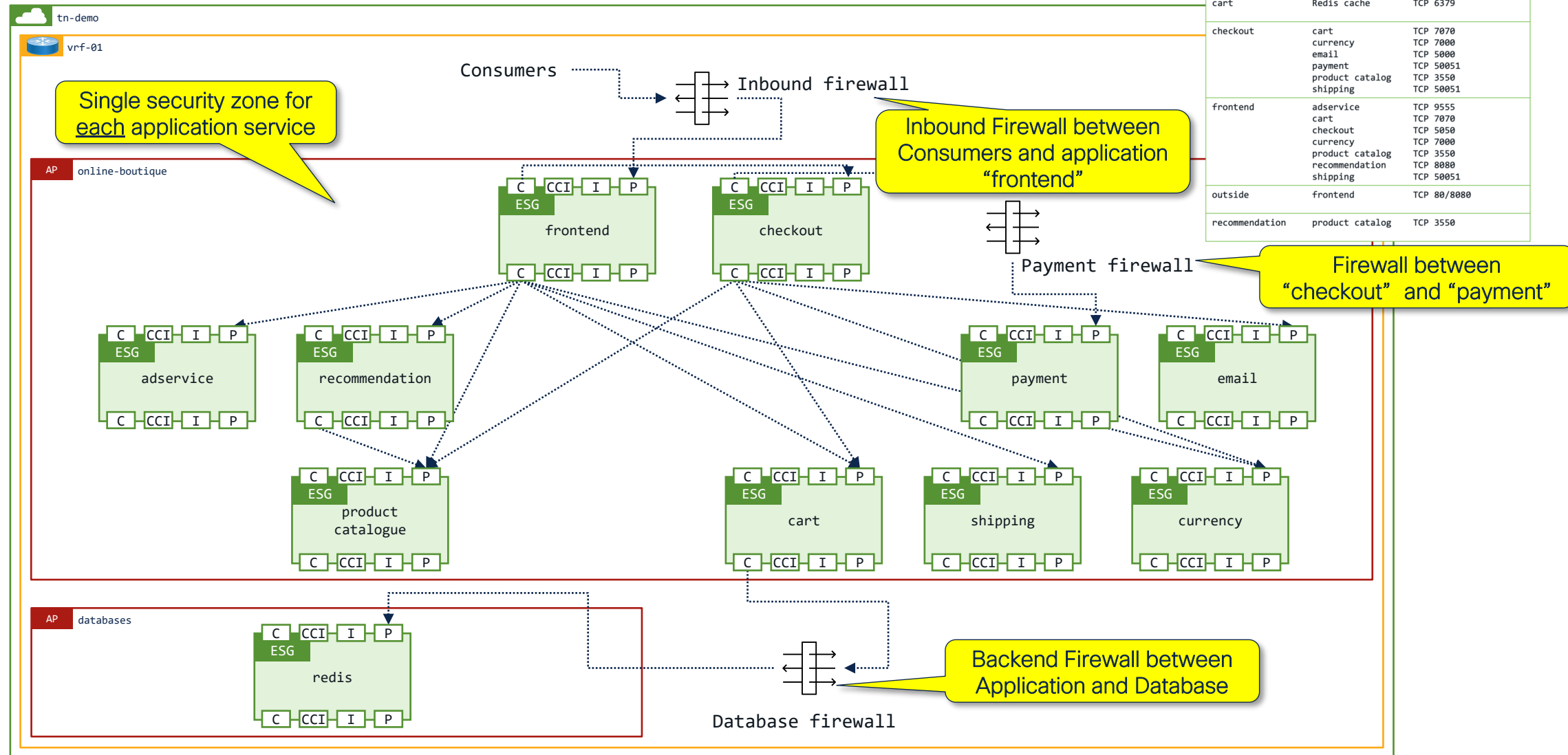
Application tiers across subnets

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



Application tiers across subnets

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



Wrapping up...



Select one or more Design Patterns...

Carefully consider the use of:

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

Implement ESG “wrappers” ...

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

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

Benefits of Shared Service model...

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

Automation Considerations...

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

Now available on dCloud

Getting Started with Cisco ACI 6.0 v1

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

Overview

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

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

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

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

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

Cisco Webex App

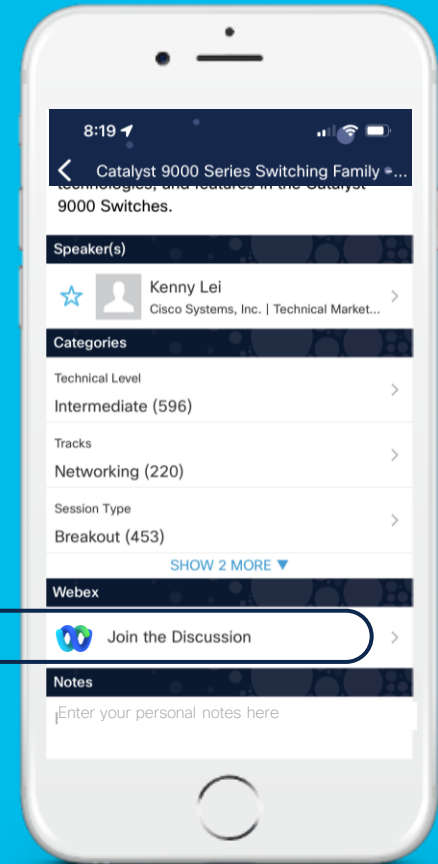
Questions?

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

How

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

Webex spaces will be moderated until February 24, 2023.



Complete your Session Survey

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



Continue Your Education



Visit the Cisco Showcase for related demos.



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



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



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



The bridge to possible

Thank you

CISCO *Live!*

ALL

IN