cisco Live!

GO BEYOND

#CiscoLiveAPJC

ACI – The Foundation of an Internal Private Cloud

(aka “not just another network…”)

BRKDCN-2984

Steve Sharman – Solutions Engineer
BRKDCN-2984

Cisco Webex App

Questions?

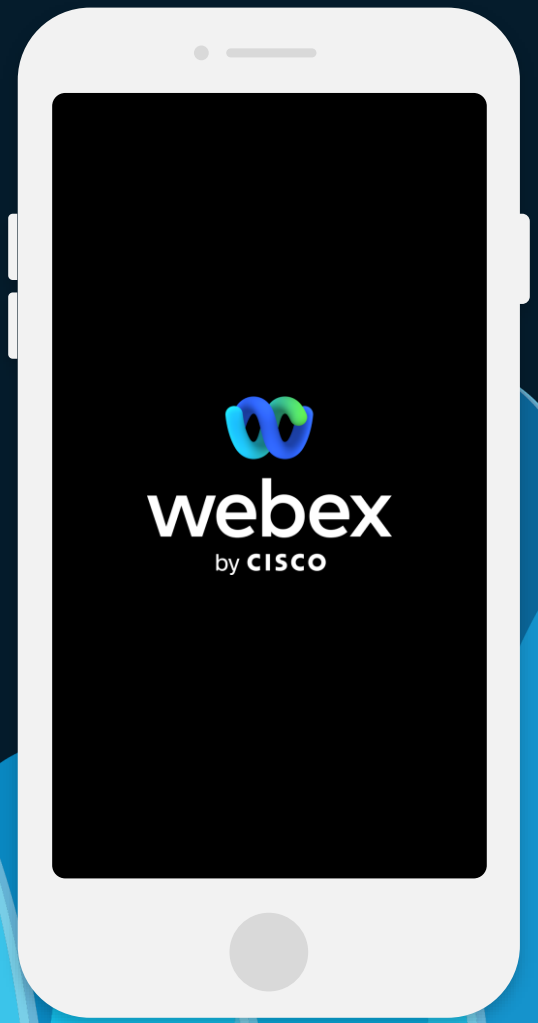
Use Cisco Webex App to chat
with the speaker after the session

How

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

Webex spaces will be moderated by the speaker until November 15, 2024.

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



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

At little bit of background to this session...

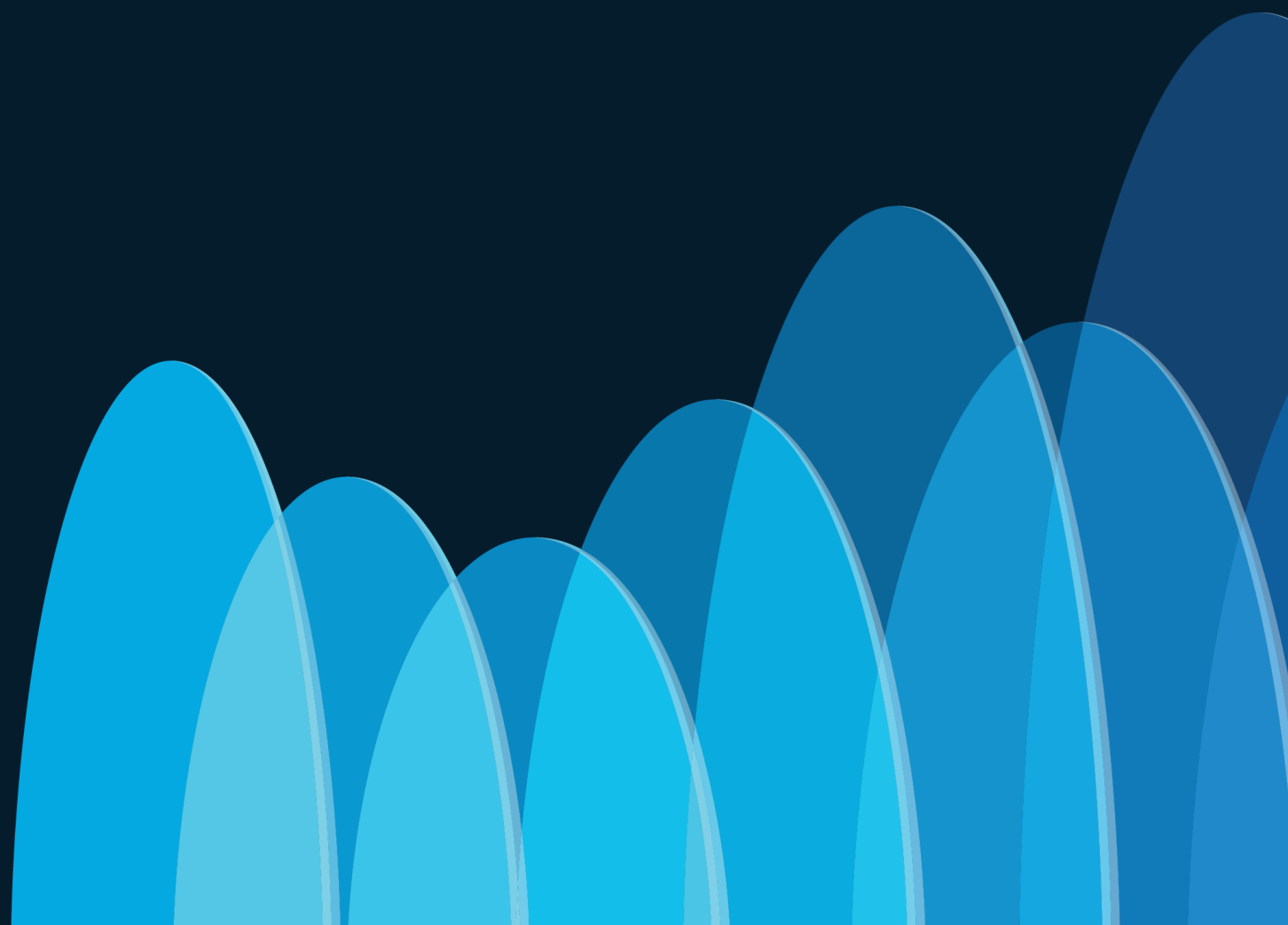
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

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

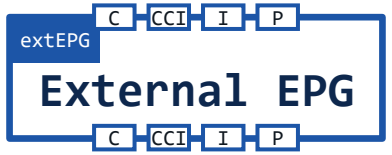
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

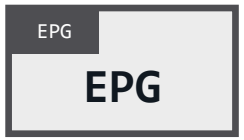
Before we get started...

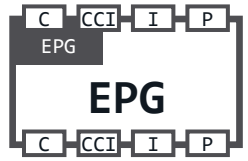


cisco Live!

Icons



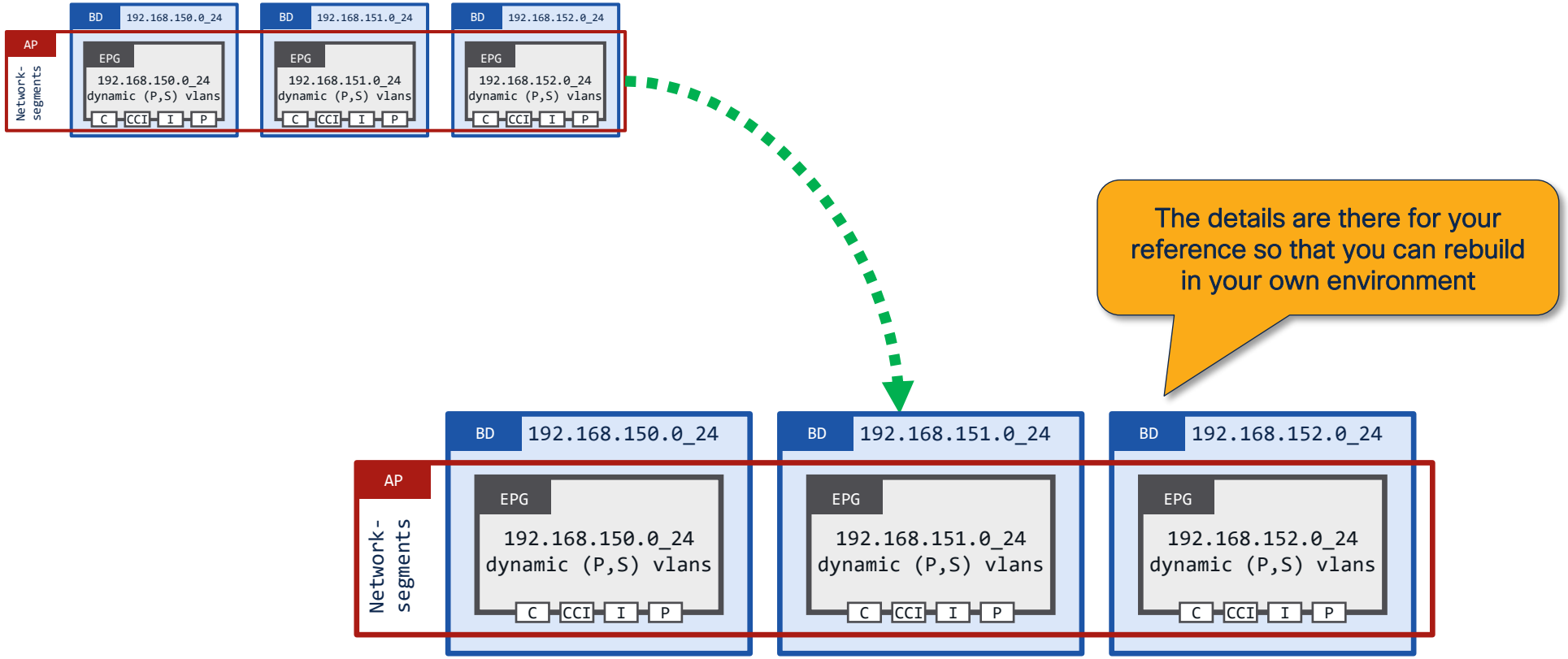




*arrows indicate expected direction of connection i.e. from consumer to provider

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

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



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

Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

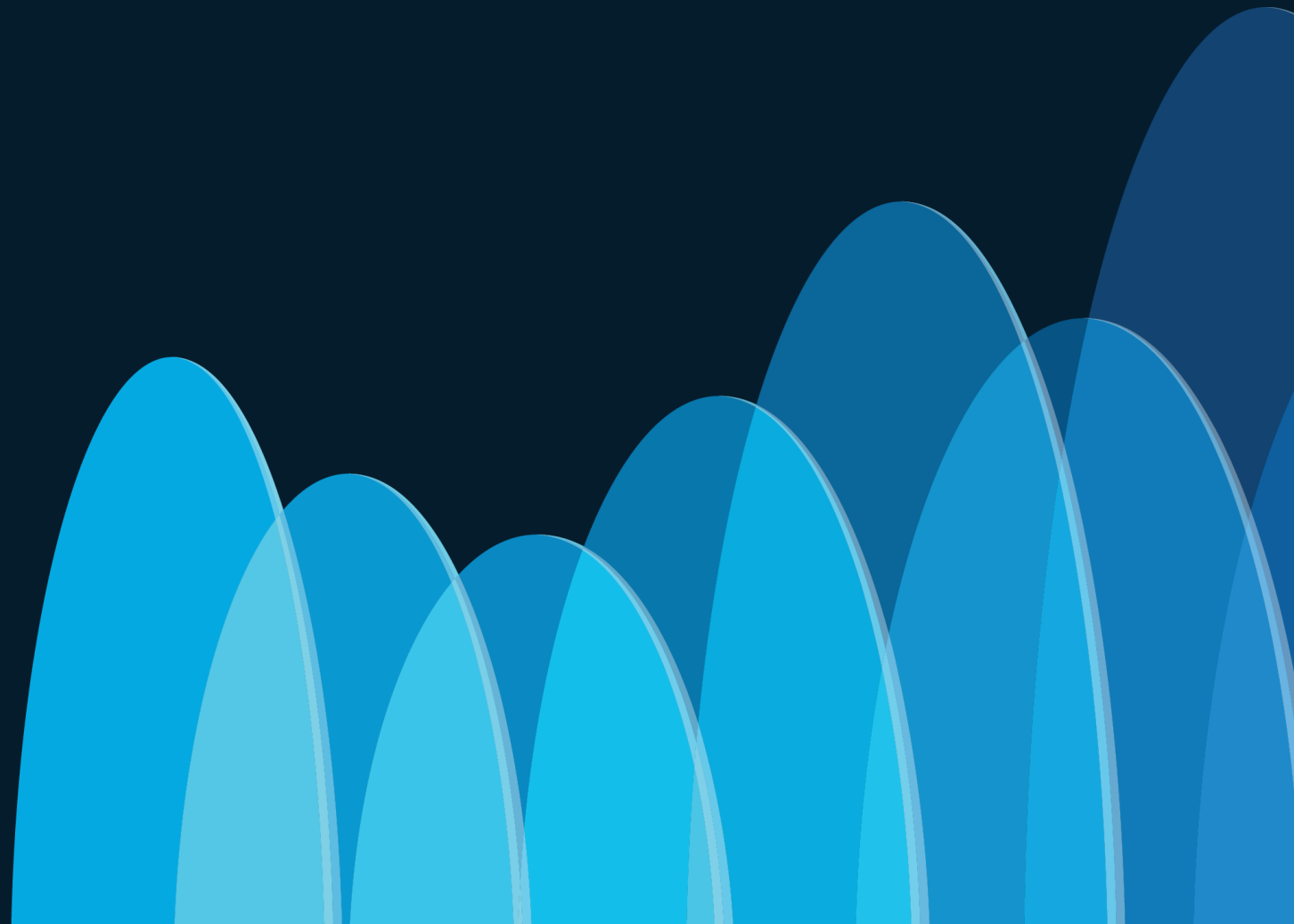
Understanding ACI security...

External Connectivity...

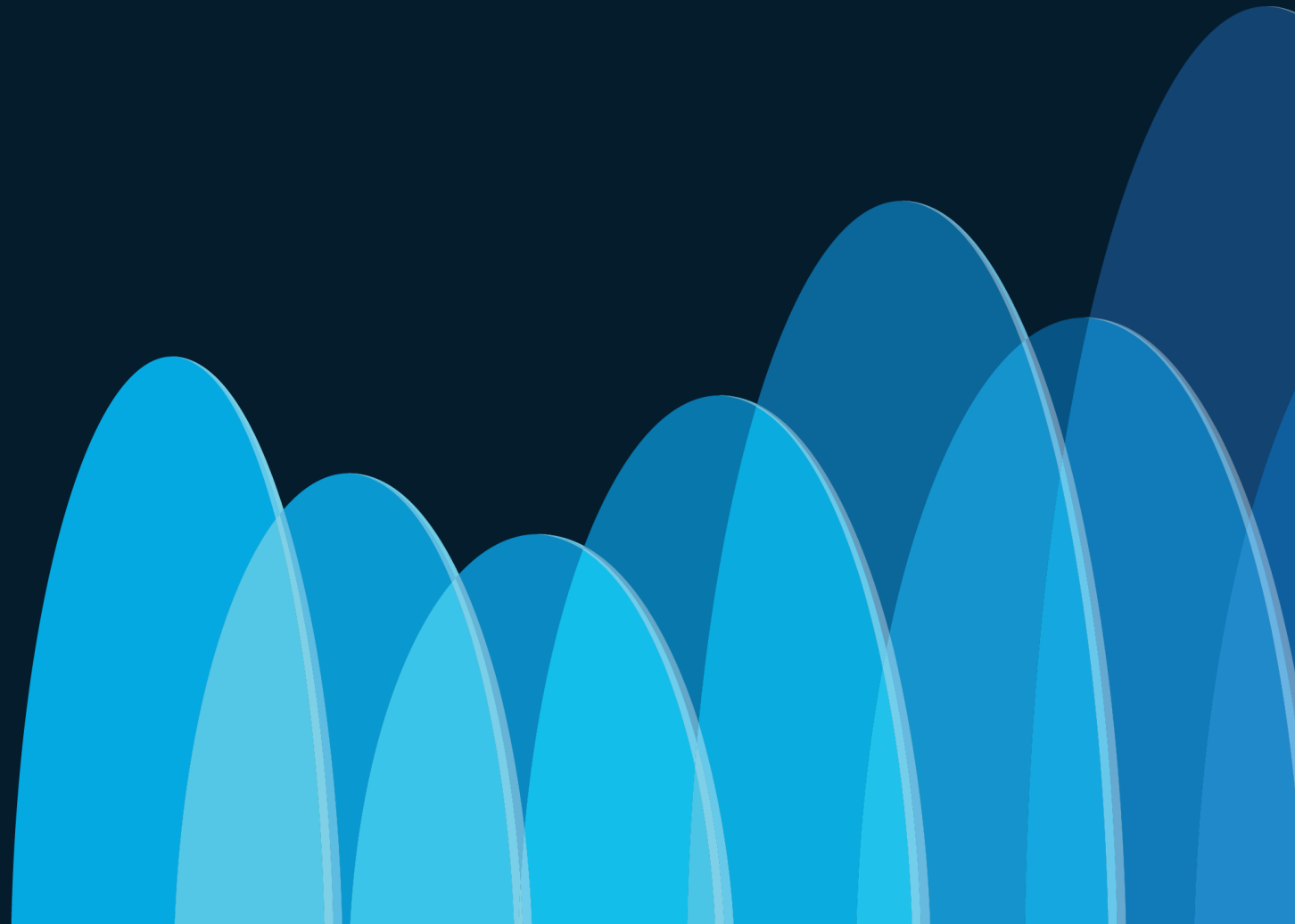
Increasing Security...

Automation Blueprints...

Wrapping up...

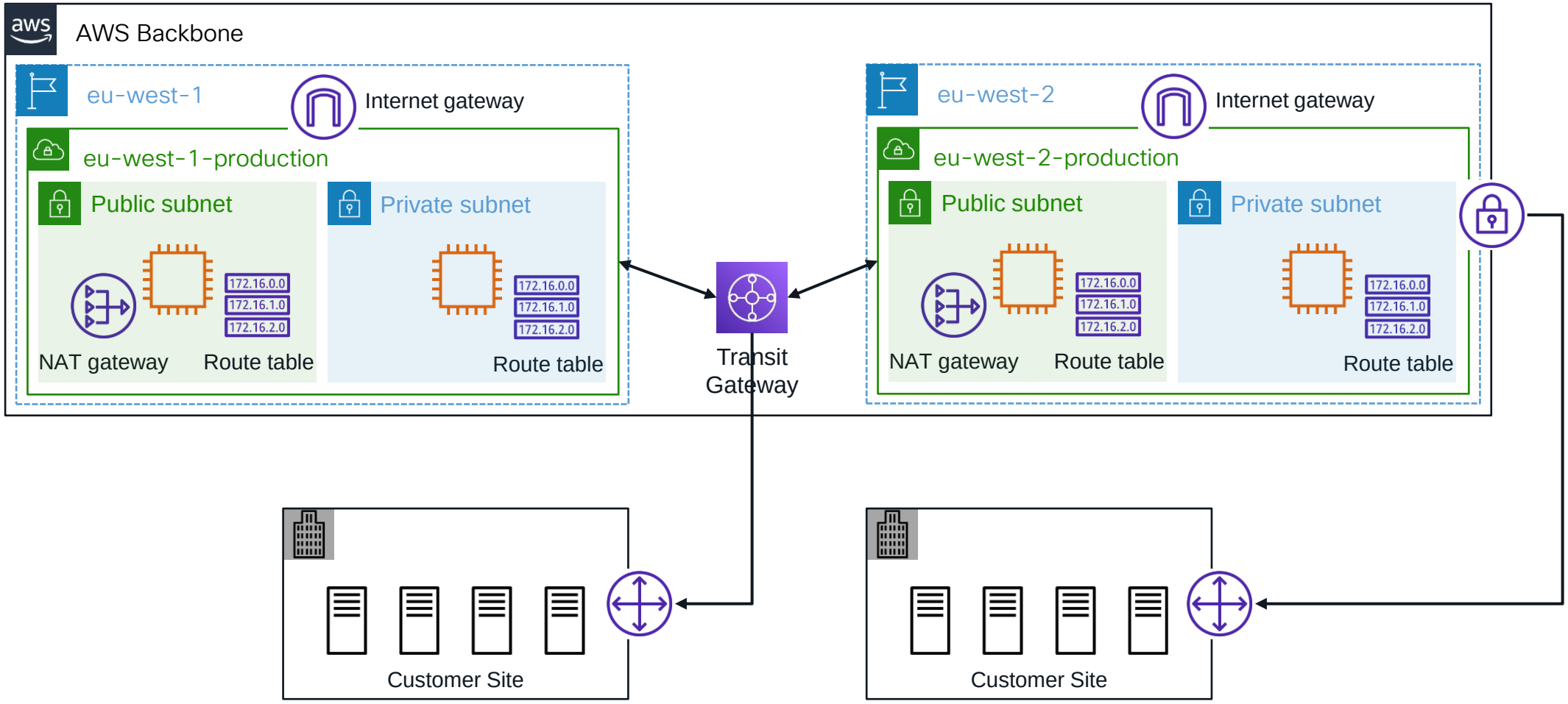


Public Cloud infrastructure...



AWS reference architecture

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

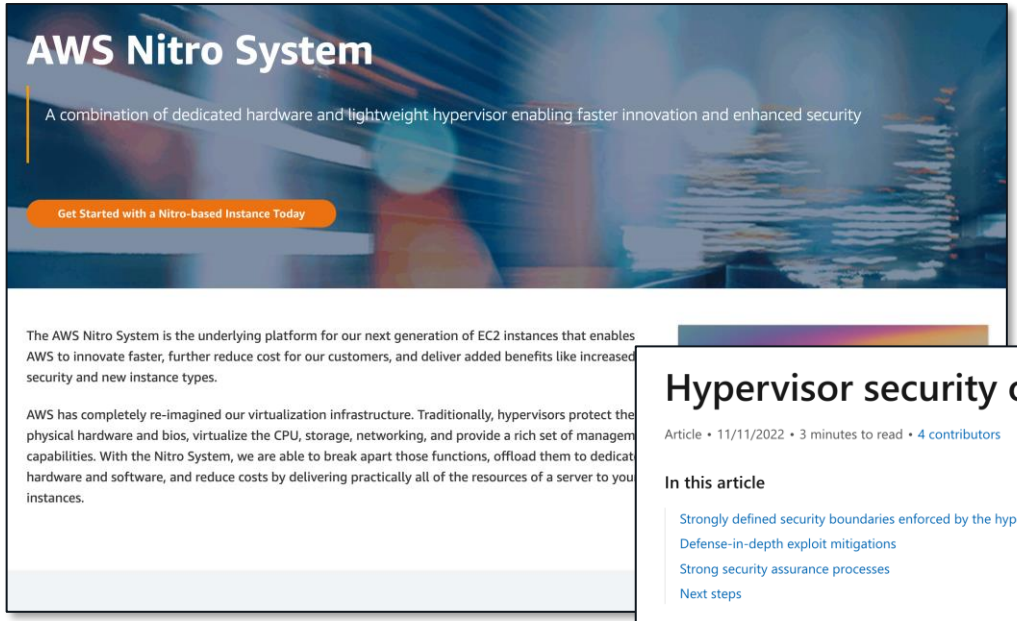


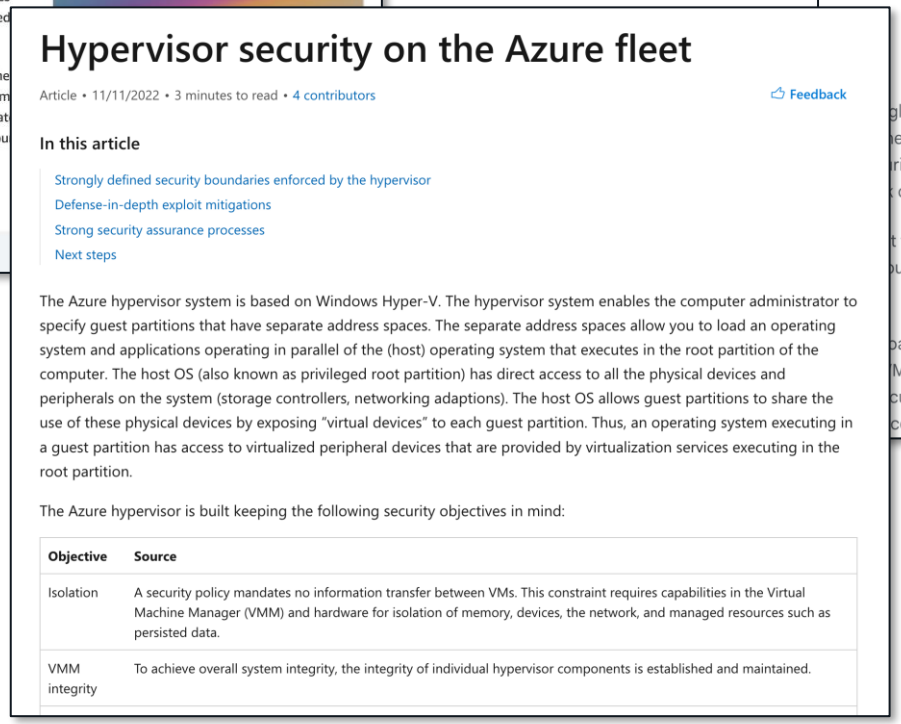
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

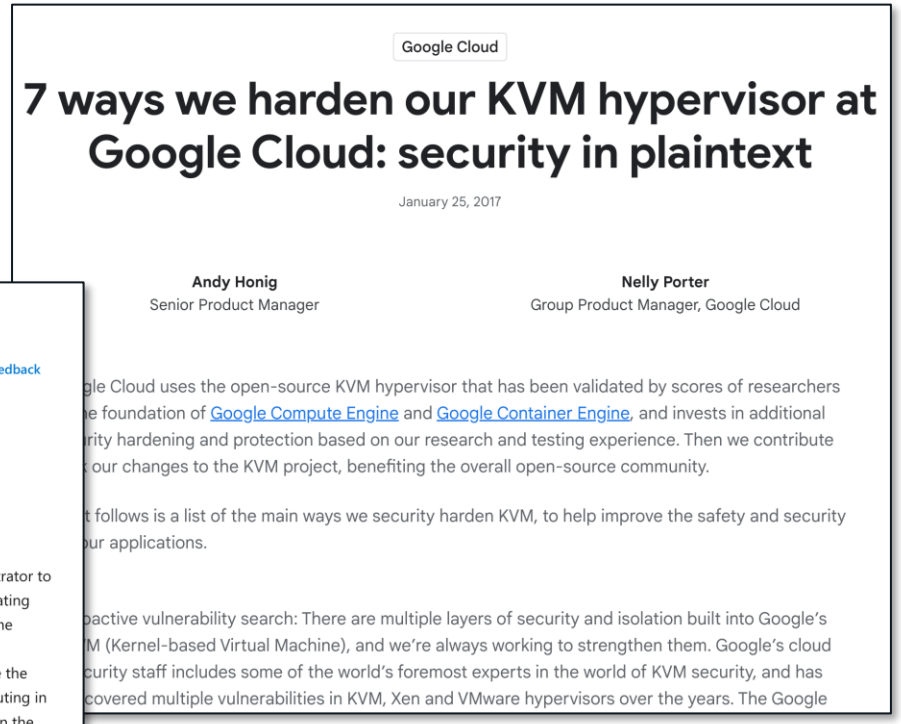
Network Connectivity and Security are mandatory in the cloud...

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

Different clouds run different hypervisors







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

- Executive Sponsorship
- Cross Functional Teams
- New Talent Attraction
- Scaling
- New Culture
- Think Agile
- Evolution Instead of Revolution
- Partnerships 2.0

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

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

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

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

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

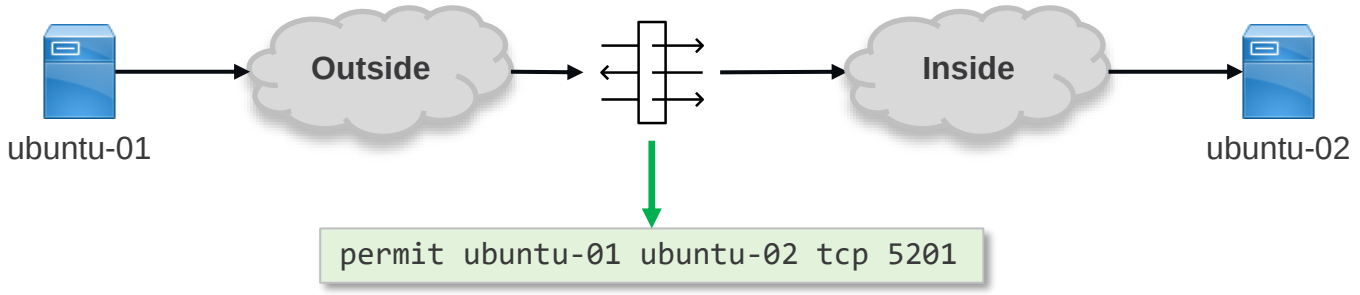
With a cloud operating model, security rules are typically declared with the application constructs...

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

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

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

Traditional Enterprise Security Model



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

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

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

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

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

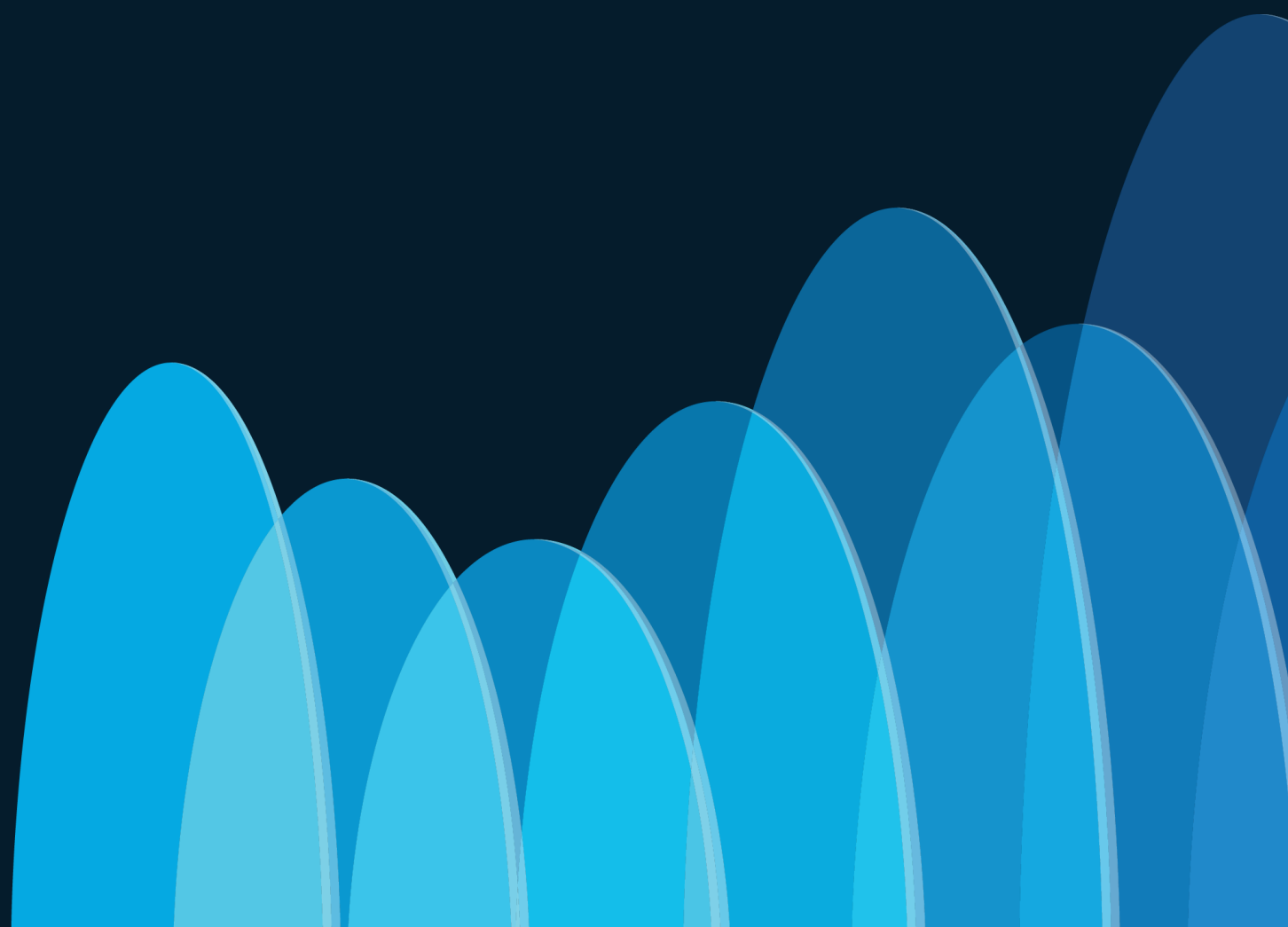
Single API Model for 100s of switches and 1000s of ports; cloud-like consumption model

Infrastructure as Code with Ansible and Terraform

Automation | Classification and Segmentation | Security

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

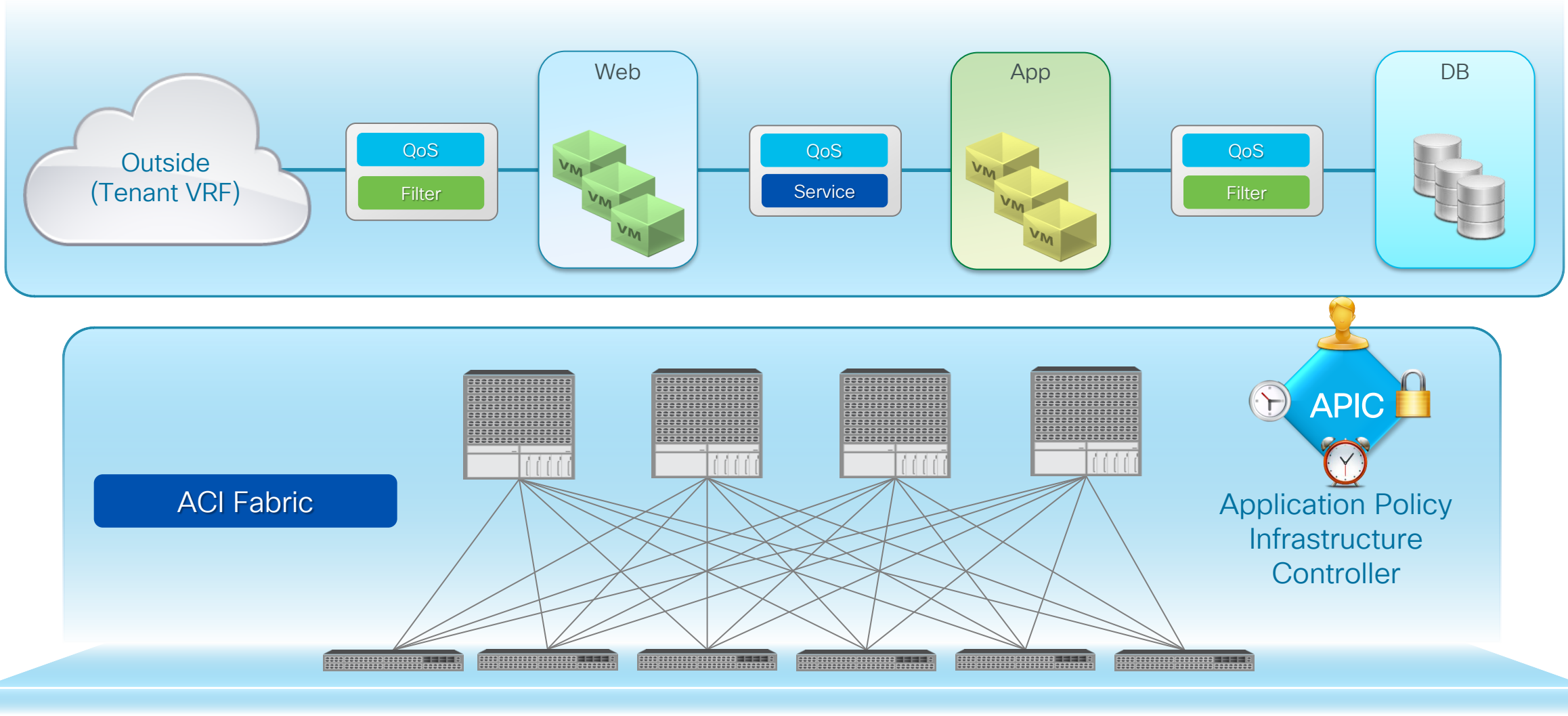
The ACI Vision...



The ACI reference application from circa 2014...

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

The mythical three tier application...!



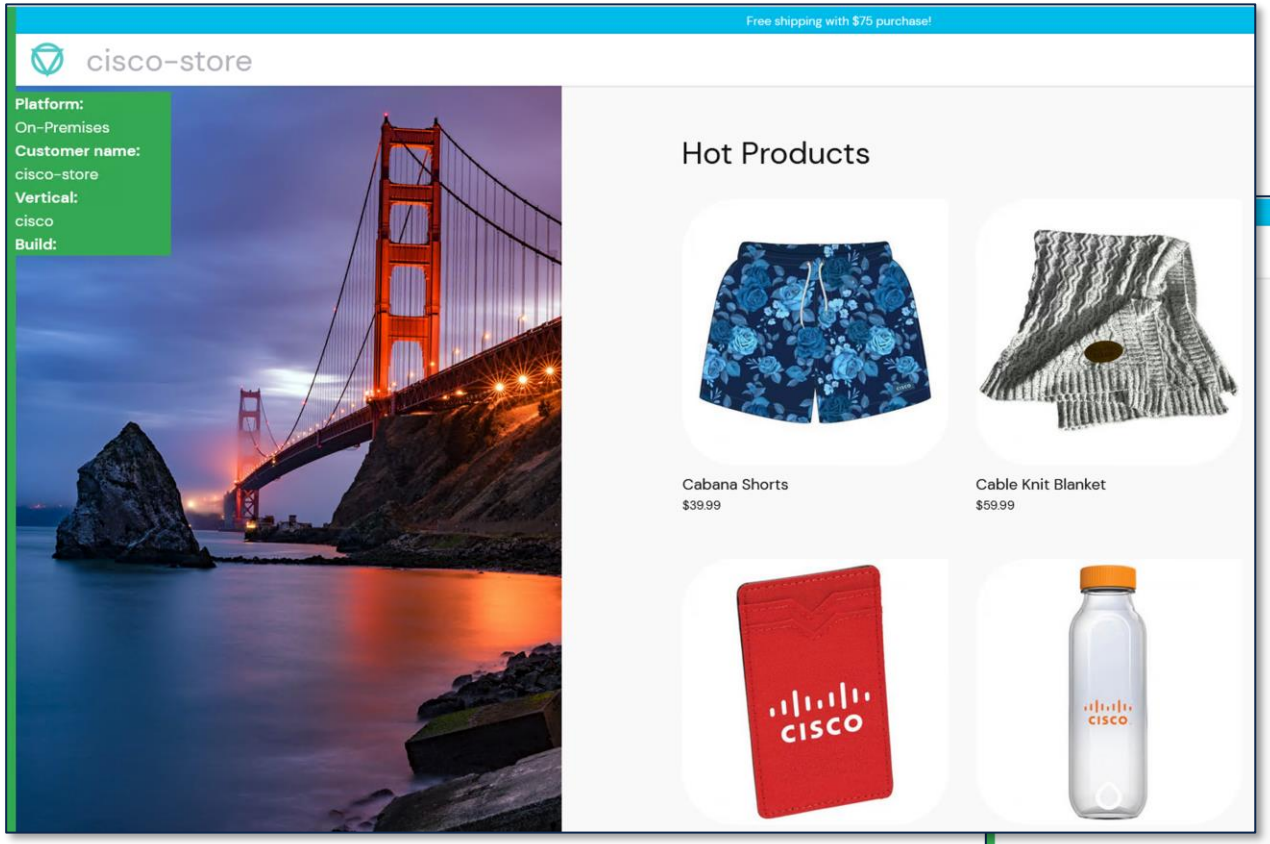
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

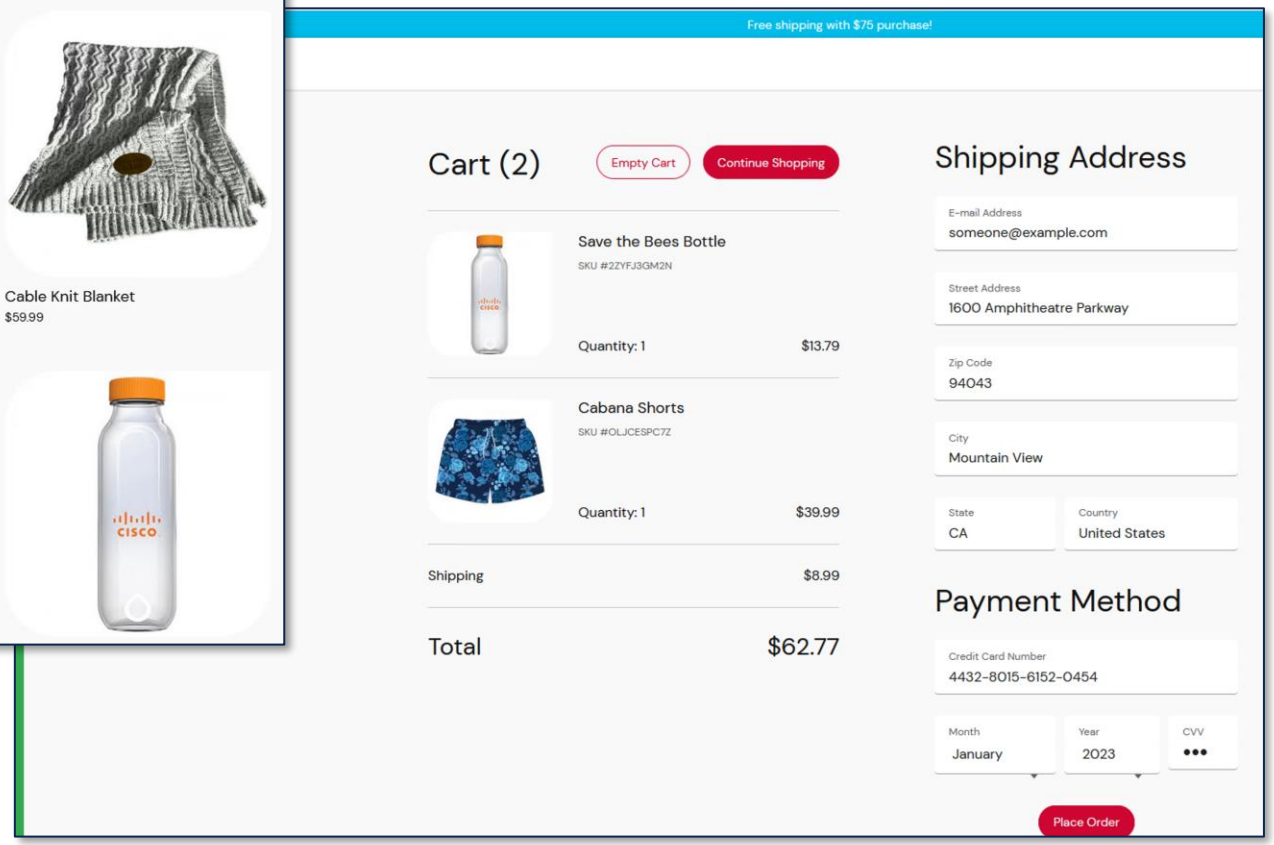
Our reference application for this presentation...

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

Online Boutique

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

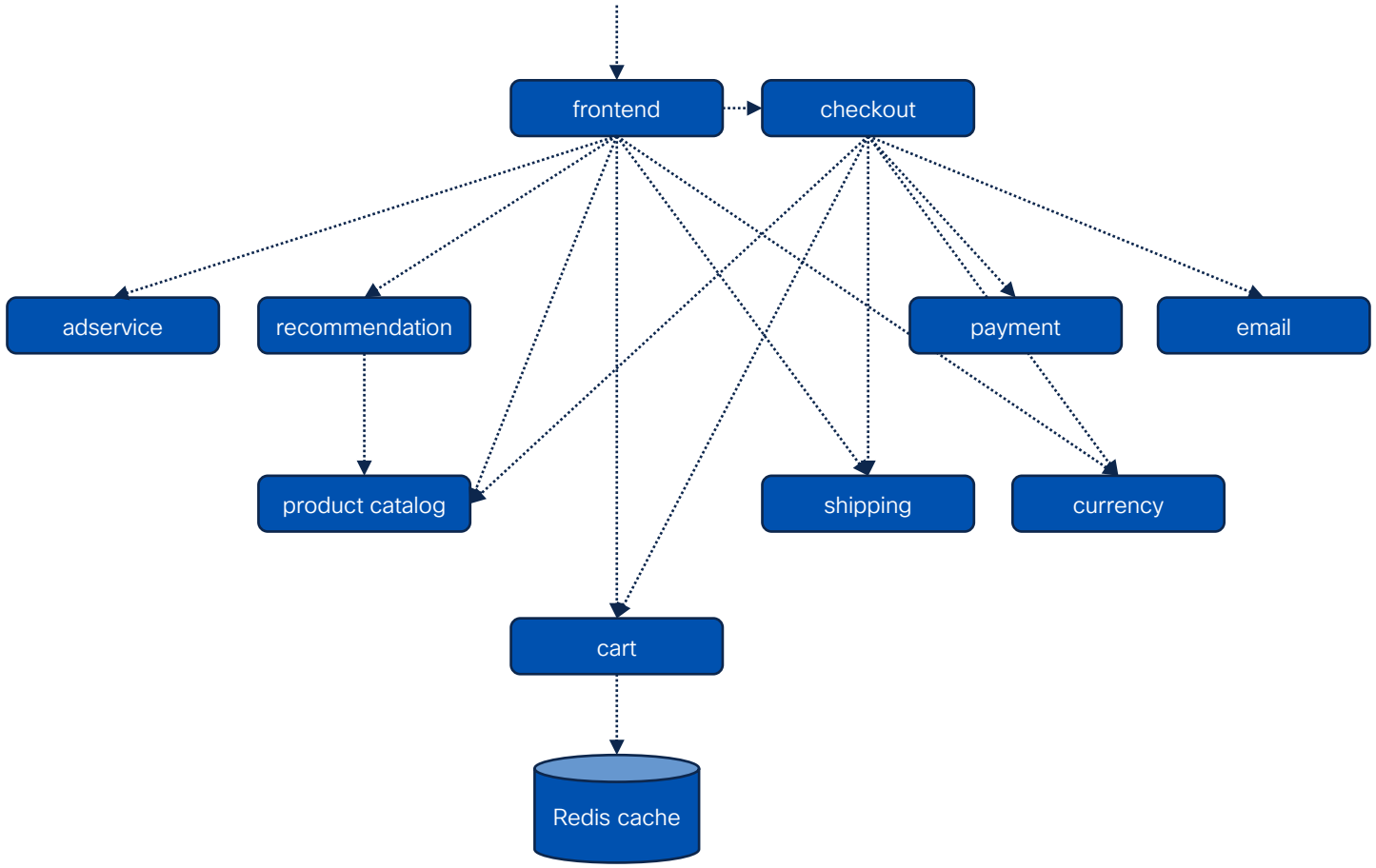




© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Online Boutique

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



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

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

Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

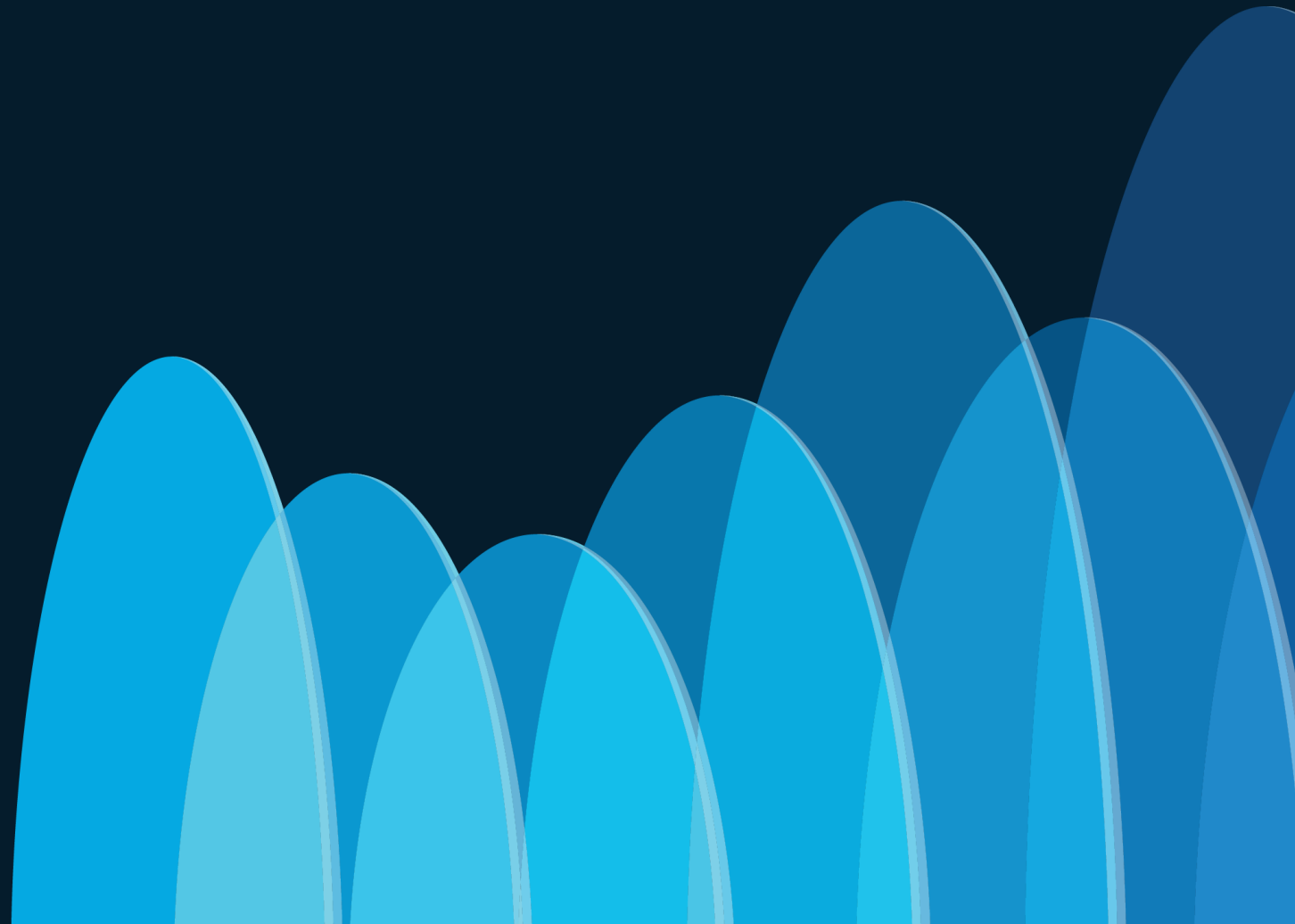
Understanding ACI security...

External Connectivity...

Increasing Security...

Automation Blueprints...

Wrapping up...



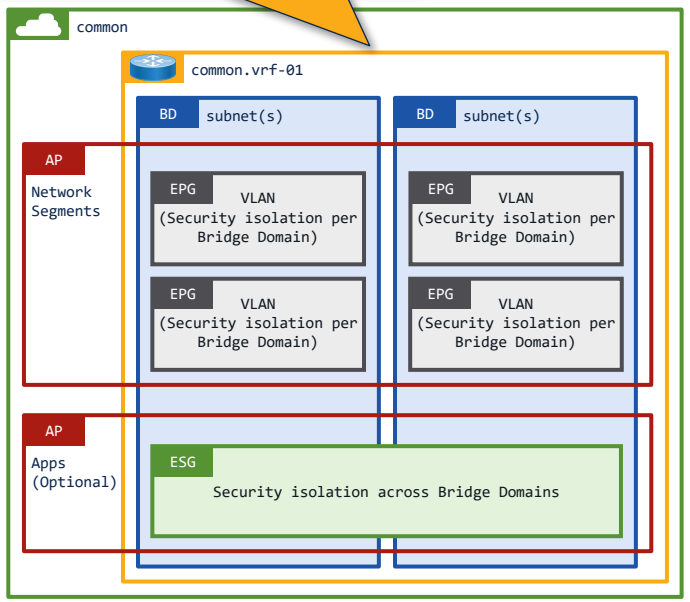
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Design Considerations...

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

Design Patterns

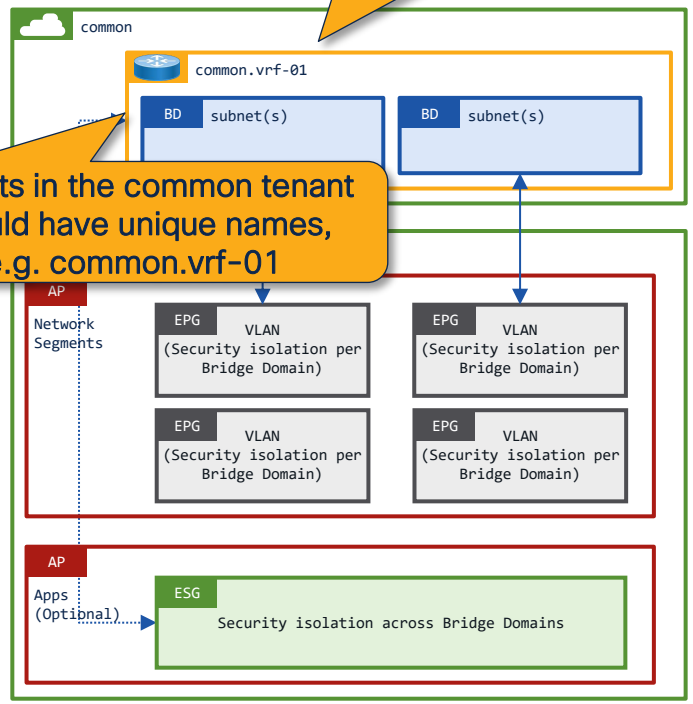
Everything in the “common” Tenant is not typically seen



Used for functions which are accessible from any Tenant

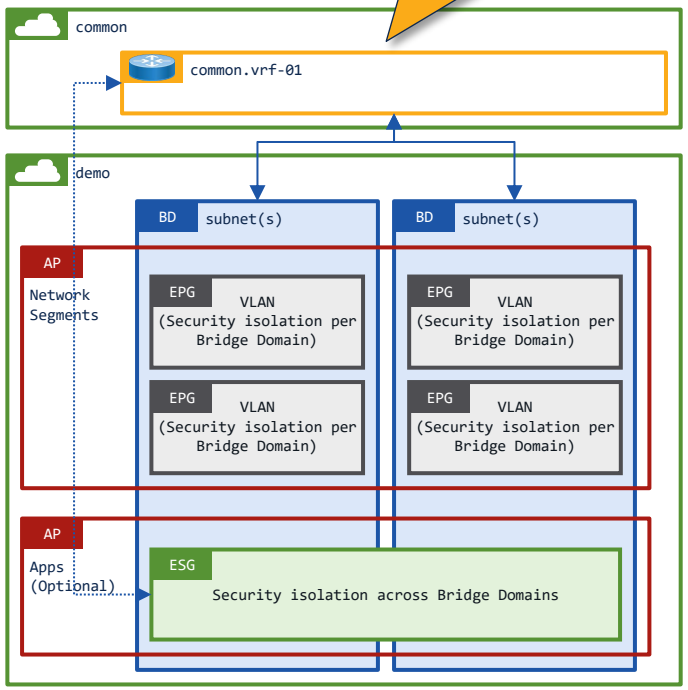
VRFs and BDs in “common” with EPGs and ESGs in the “user” tenant

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

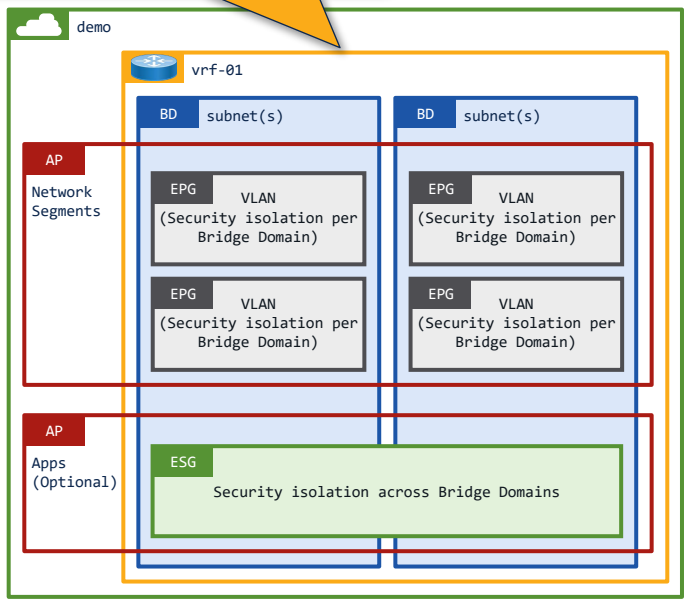


Dedicated subnets for tenants with VRFs that can be (optionally) shared by different Tenants

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

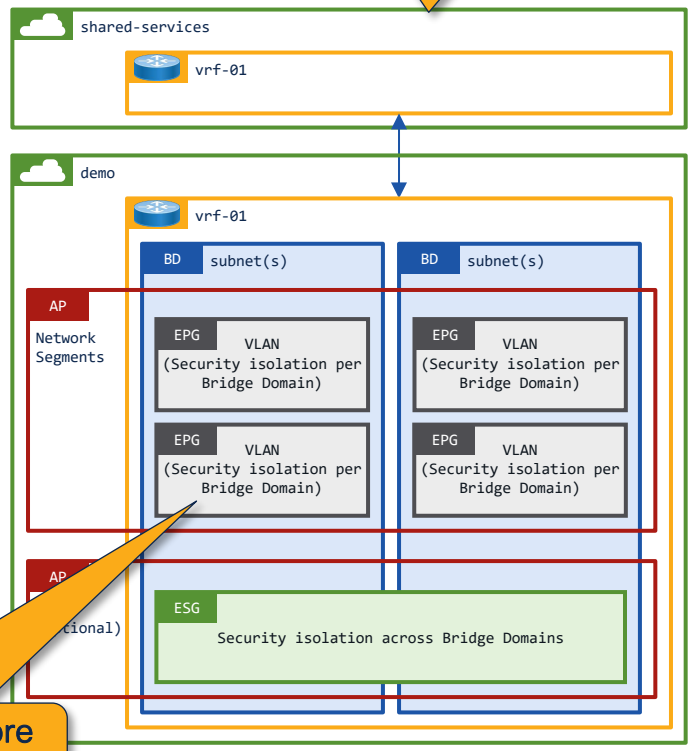
Design Patterns

All networking constructs contained within a Tenant



Dedicated VRFs and subnets for each Tenant with Dedicated L3outs

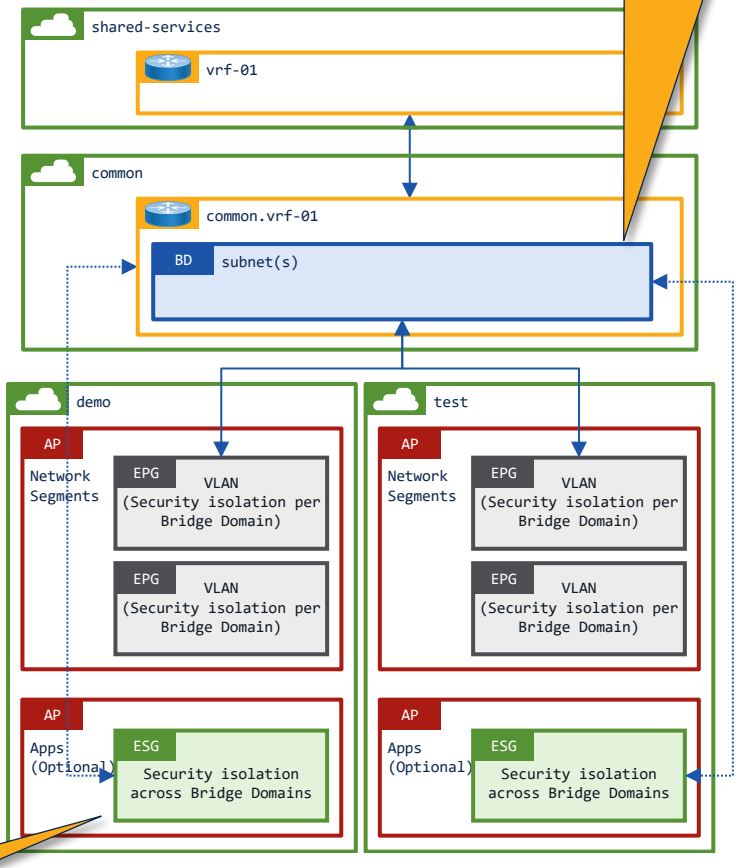
Network team controls inbound/outbound routing



Each Tenant has one or more network security groups

Dedicated VRFs and subnets for each Tenant with Shared L3out

Large subnets can be shared across Tenants

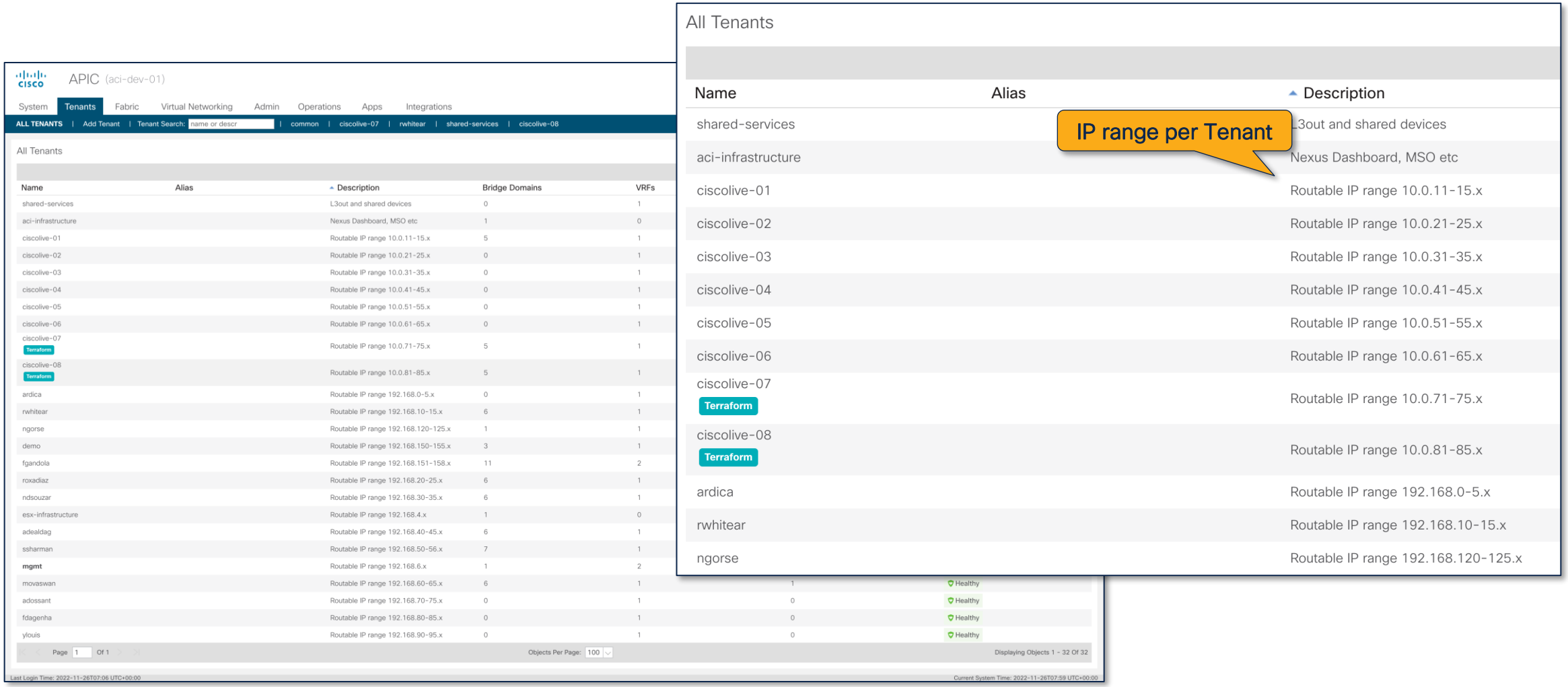


Each Tenant has one or more endpoint security groups

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

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

Each Tenant has their own IP Range

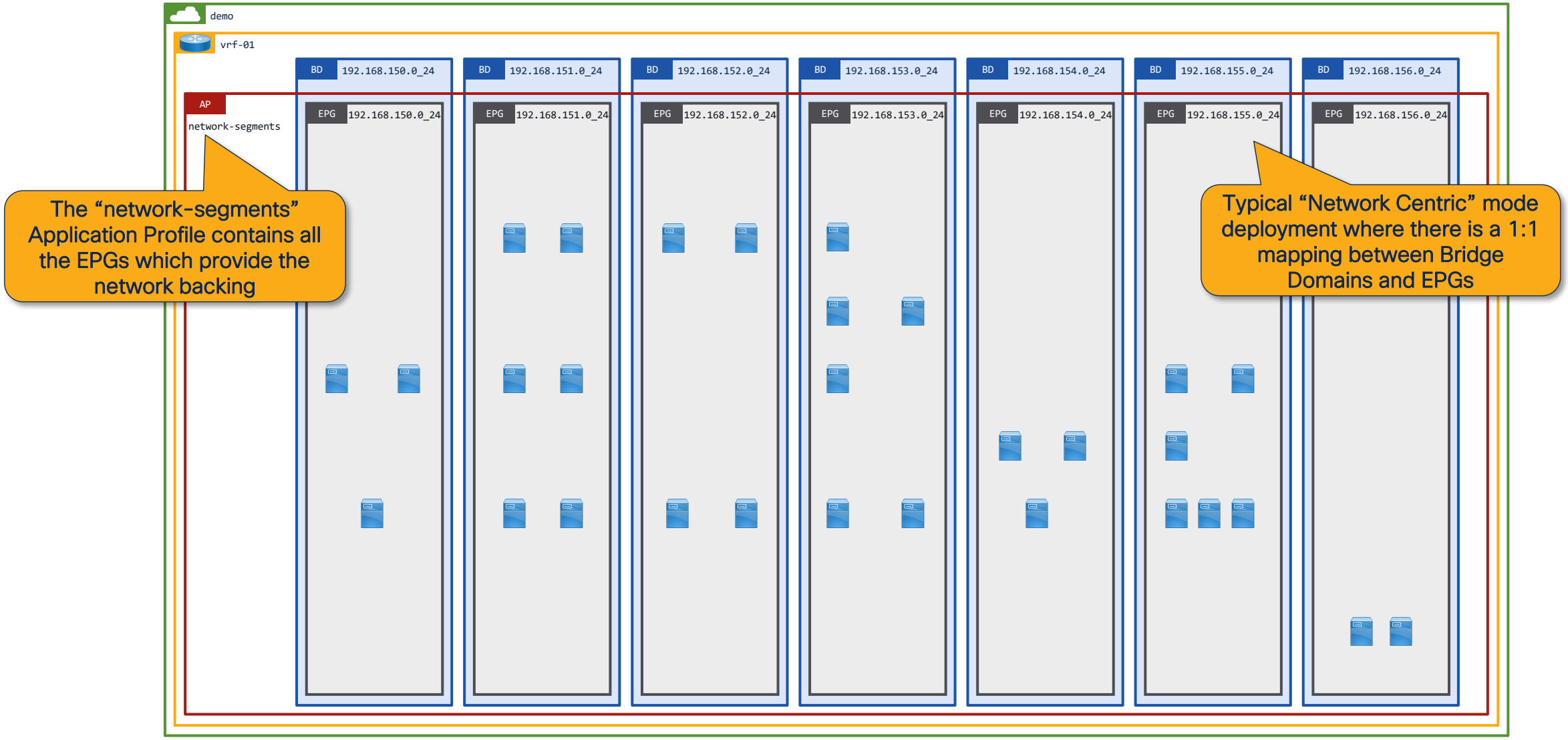


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

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

Workloads identified by IP and Mac address



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

What does the application owner care about...?

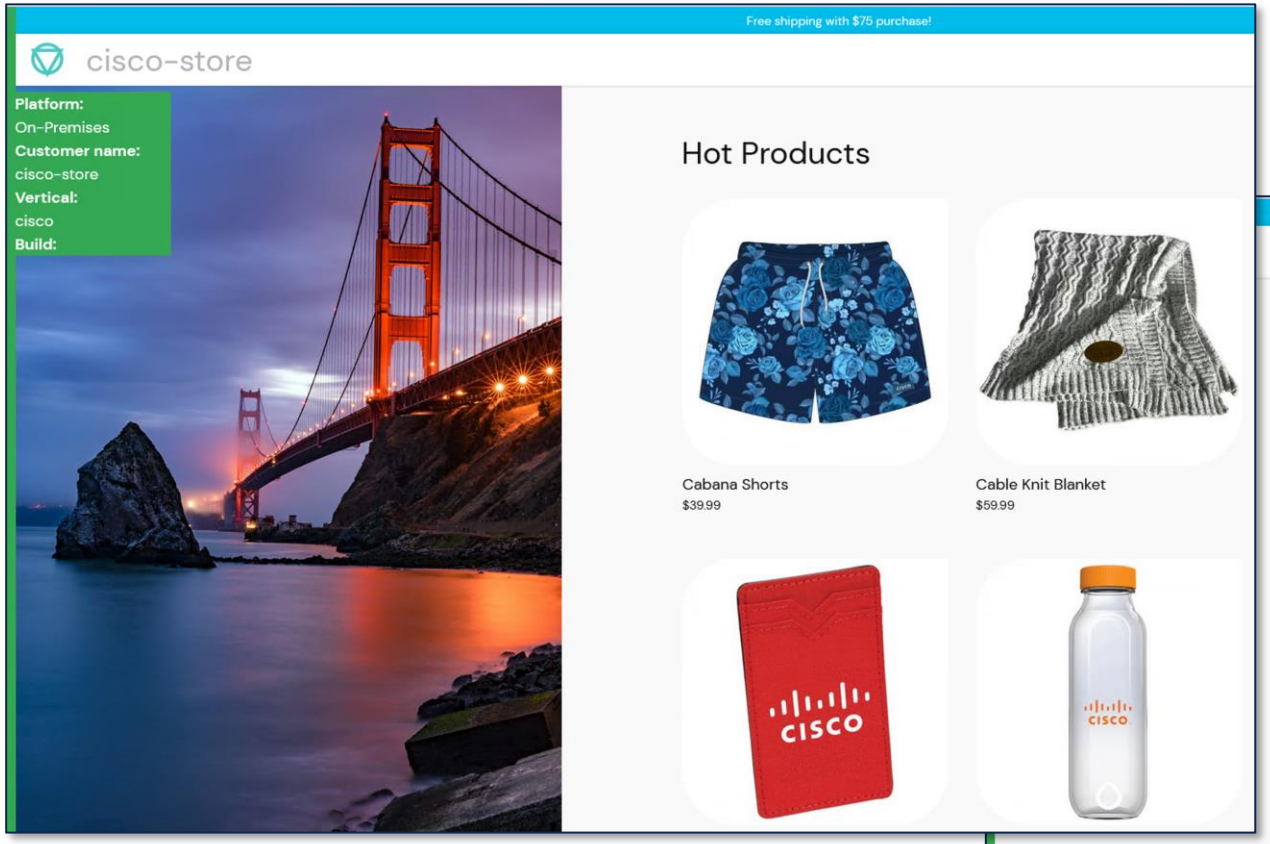
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

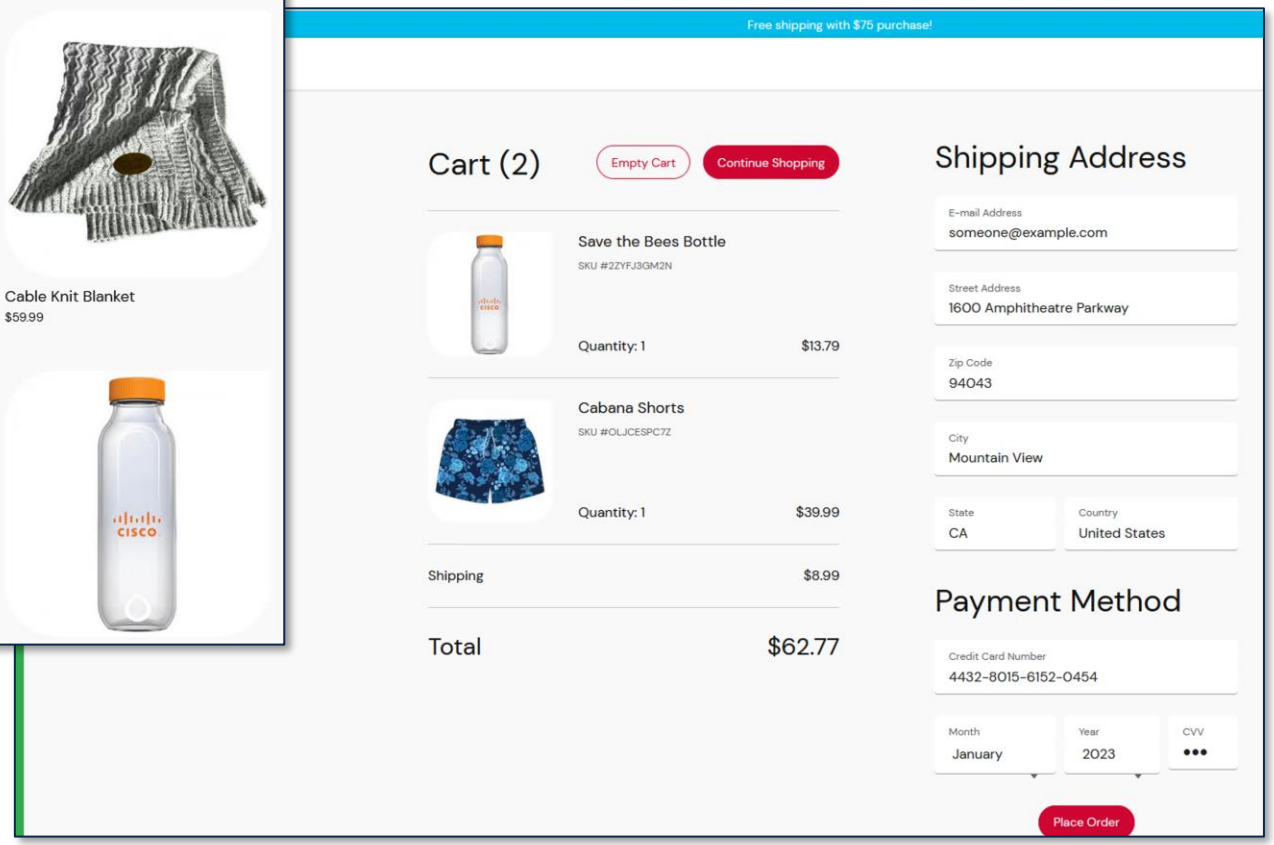
DNS names, IP addresses, Default Gateways, and Security Rules...

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

Online Boutique

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

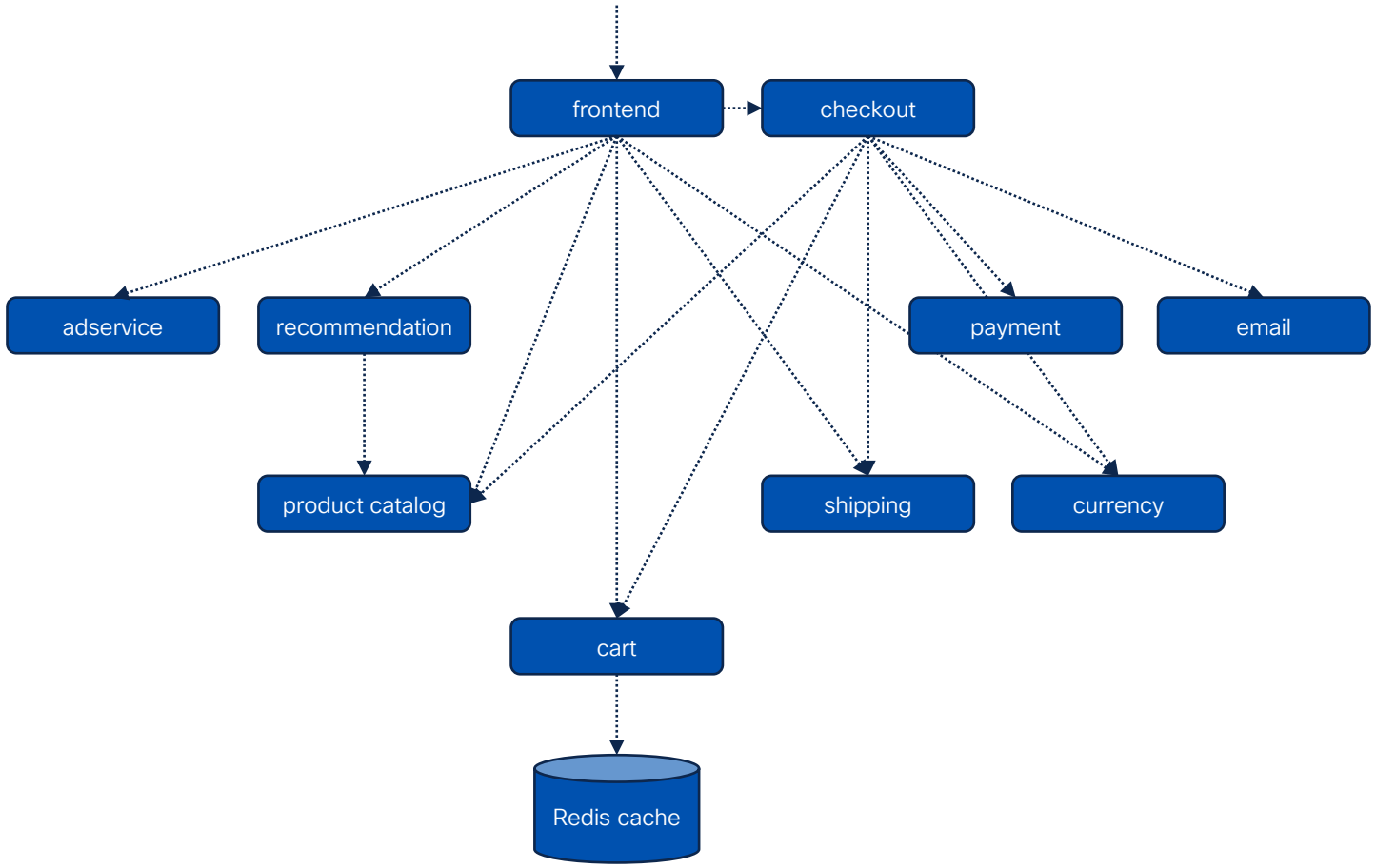




© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Online Boutique

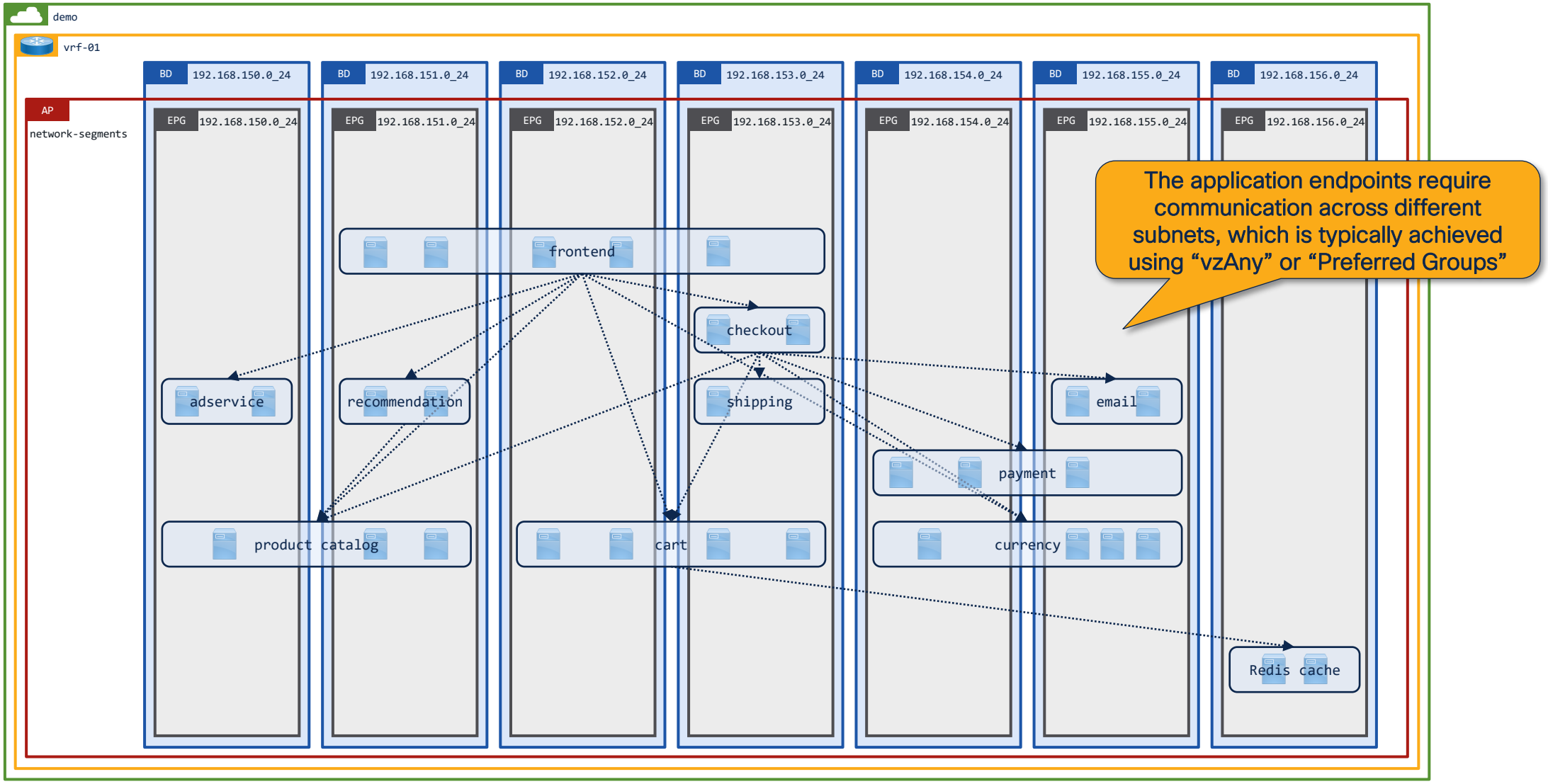
https://github.com/GoogleCloudPlatform/microservices-demo



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

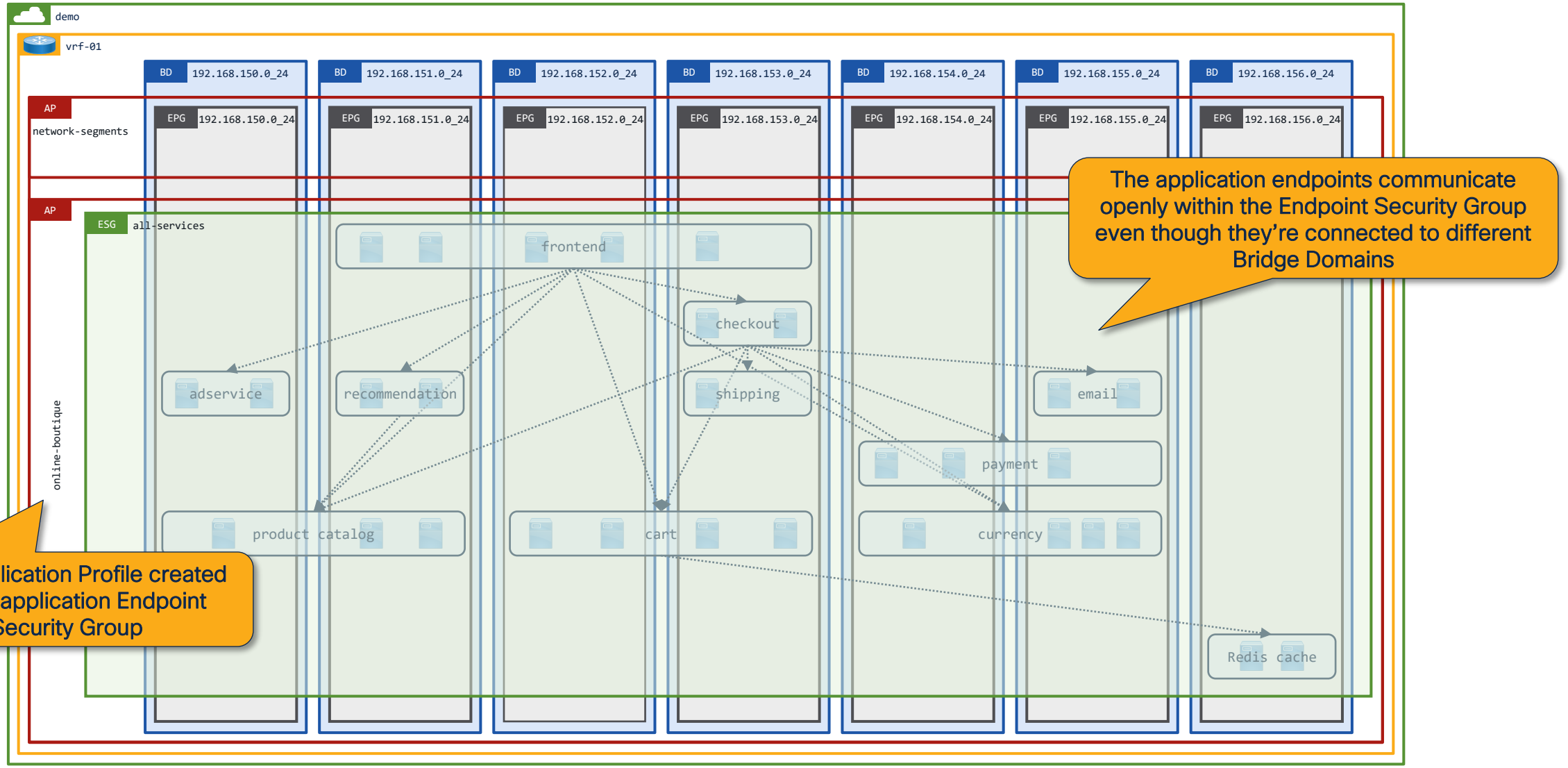
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Where is our application running...?



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

Let’s convert to “Application Centric” mode...

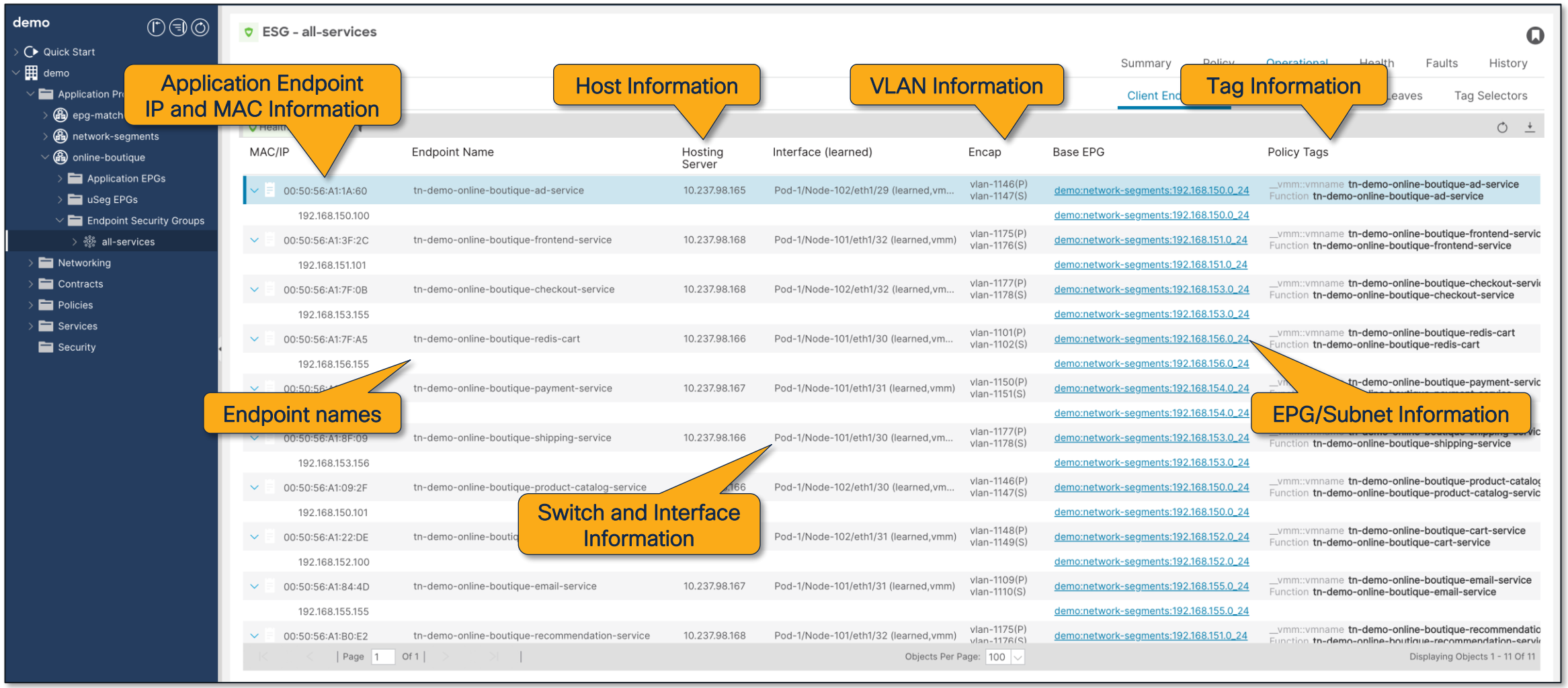


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

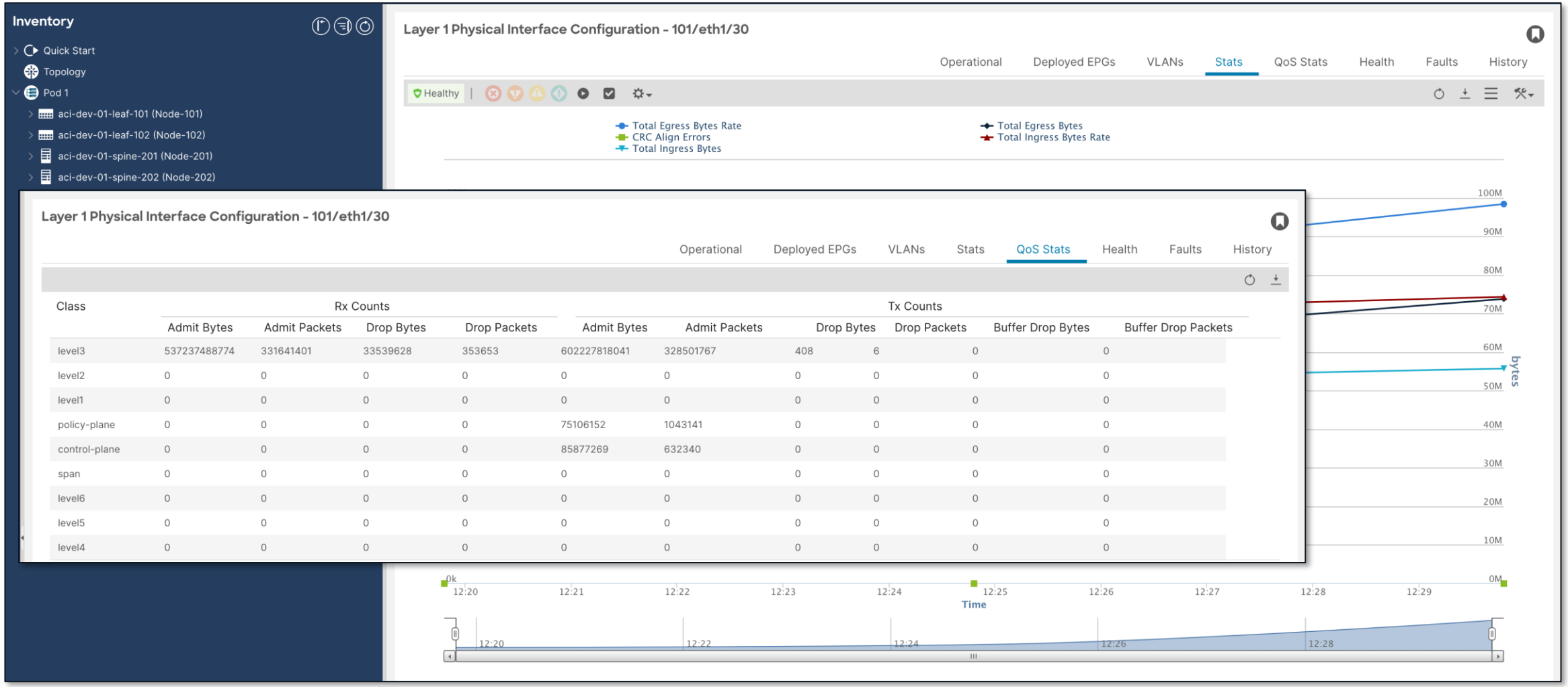
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Application Visibility...!



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

Correlate Endpoints to Switch Interfaces...



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

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

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

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

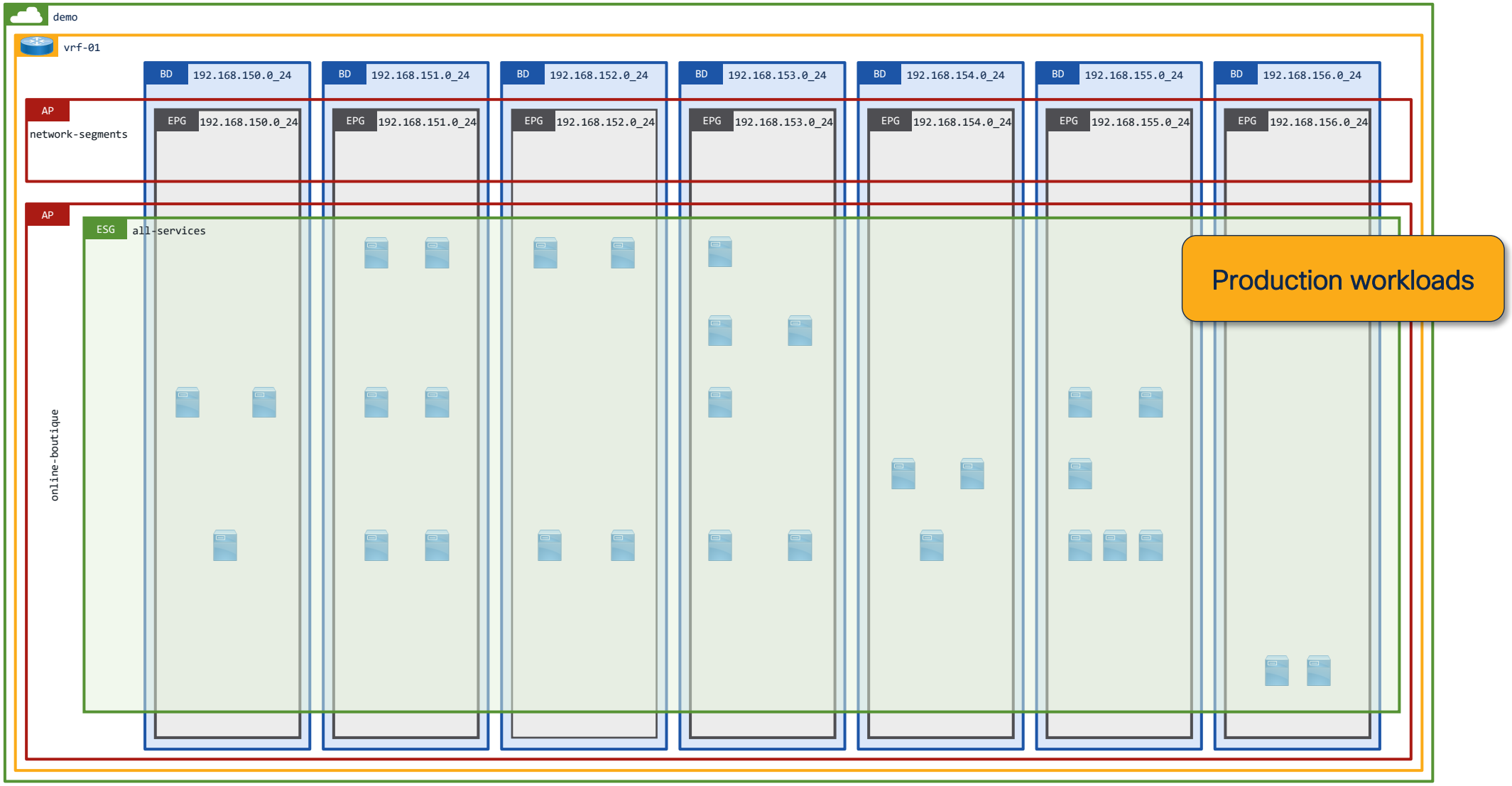
Broad-brush classification...

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

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

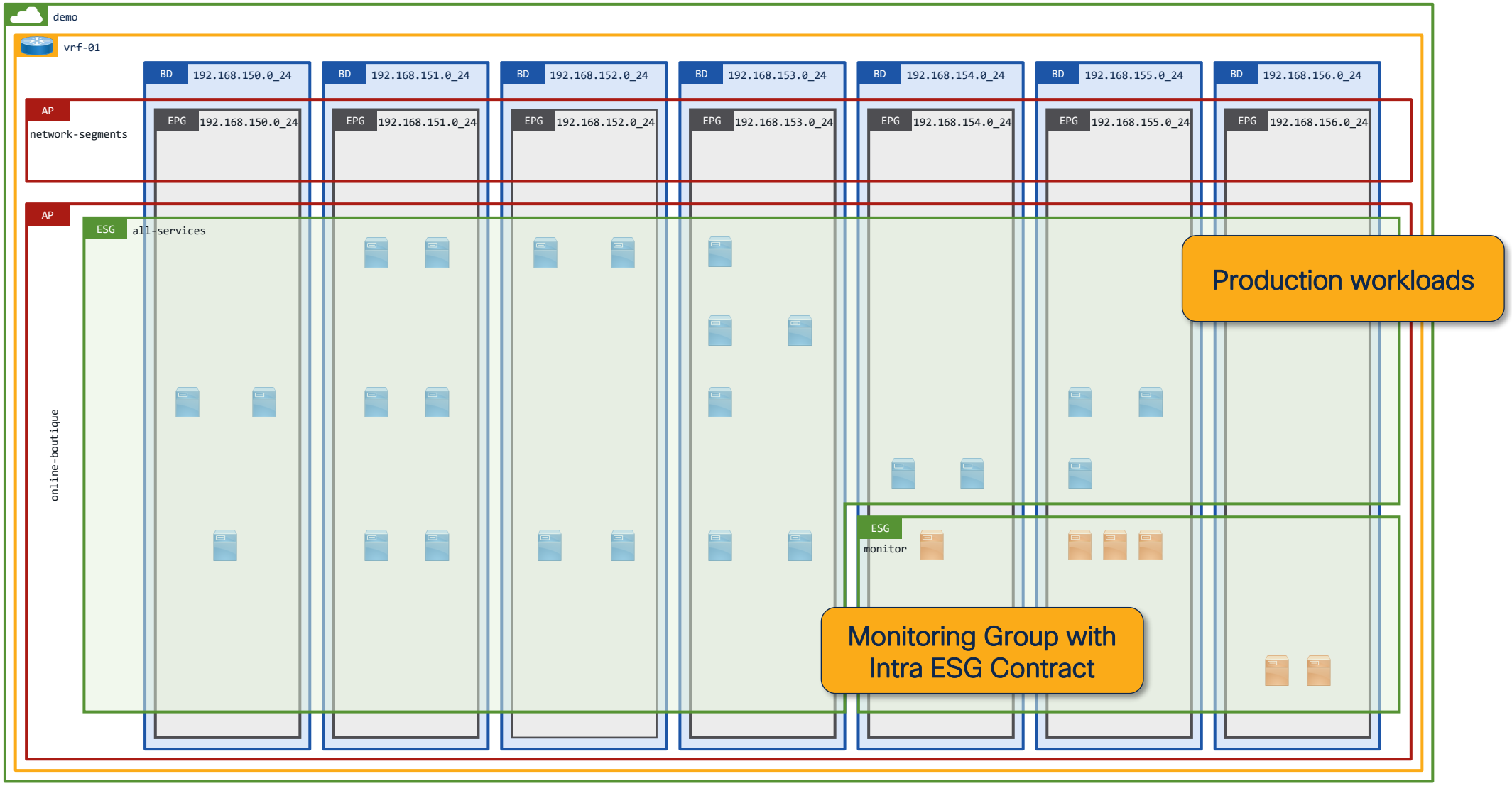
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Endpoint classification for monitoring...



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

Endpoint classification for monitoring...



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

Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

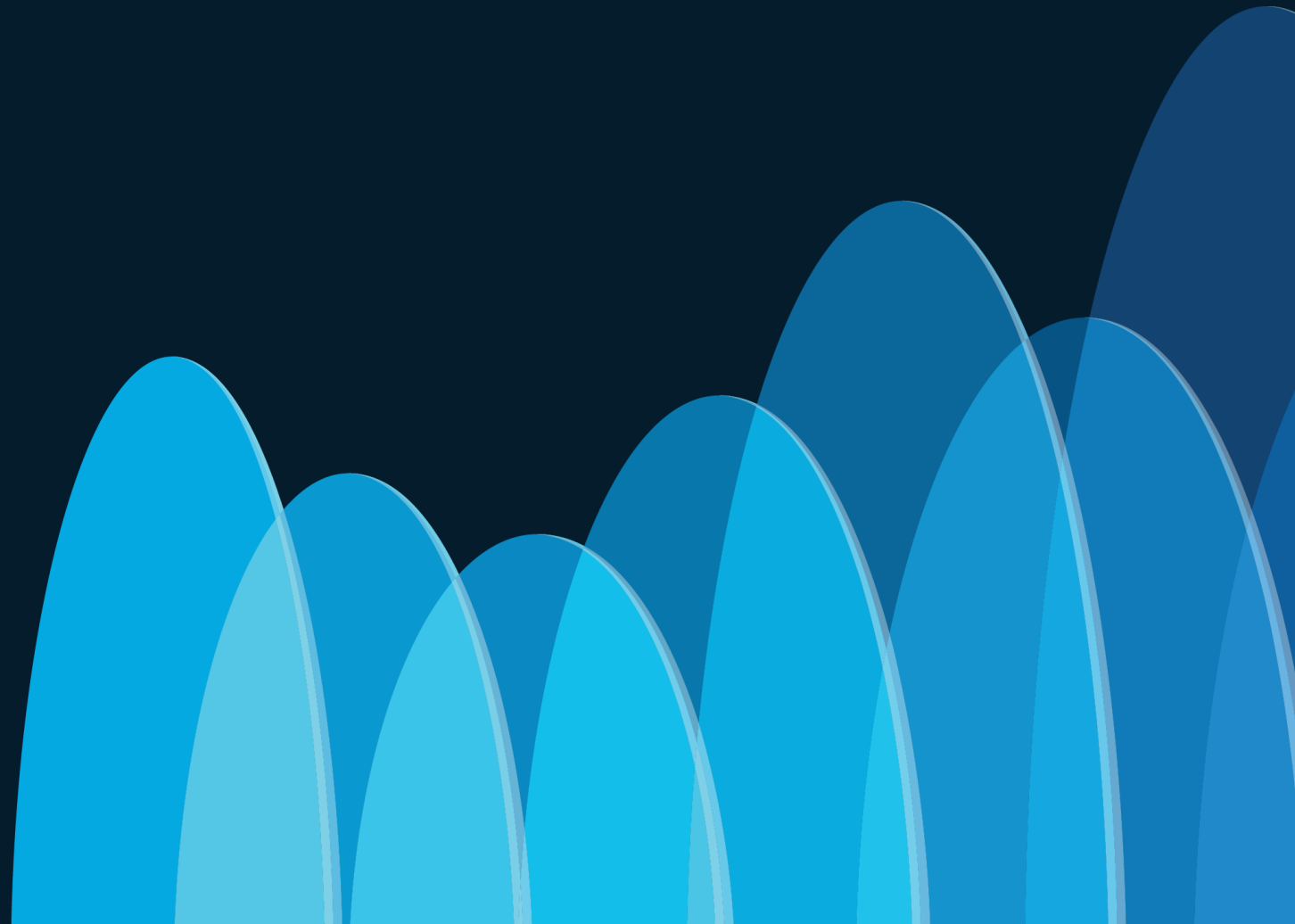
Understanding ACI security...

External Connectivity...

Increasing Security...

Automation Blueprints...

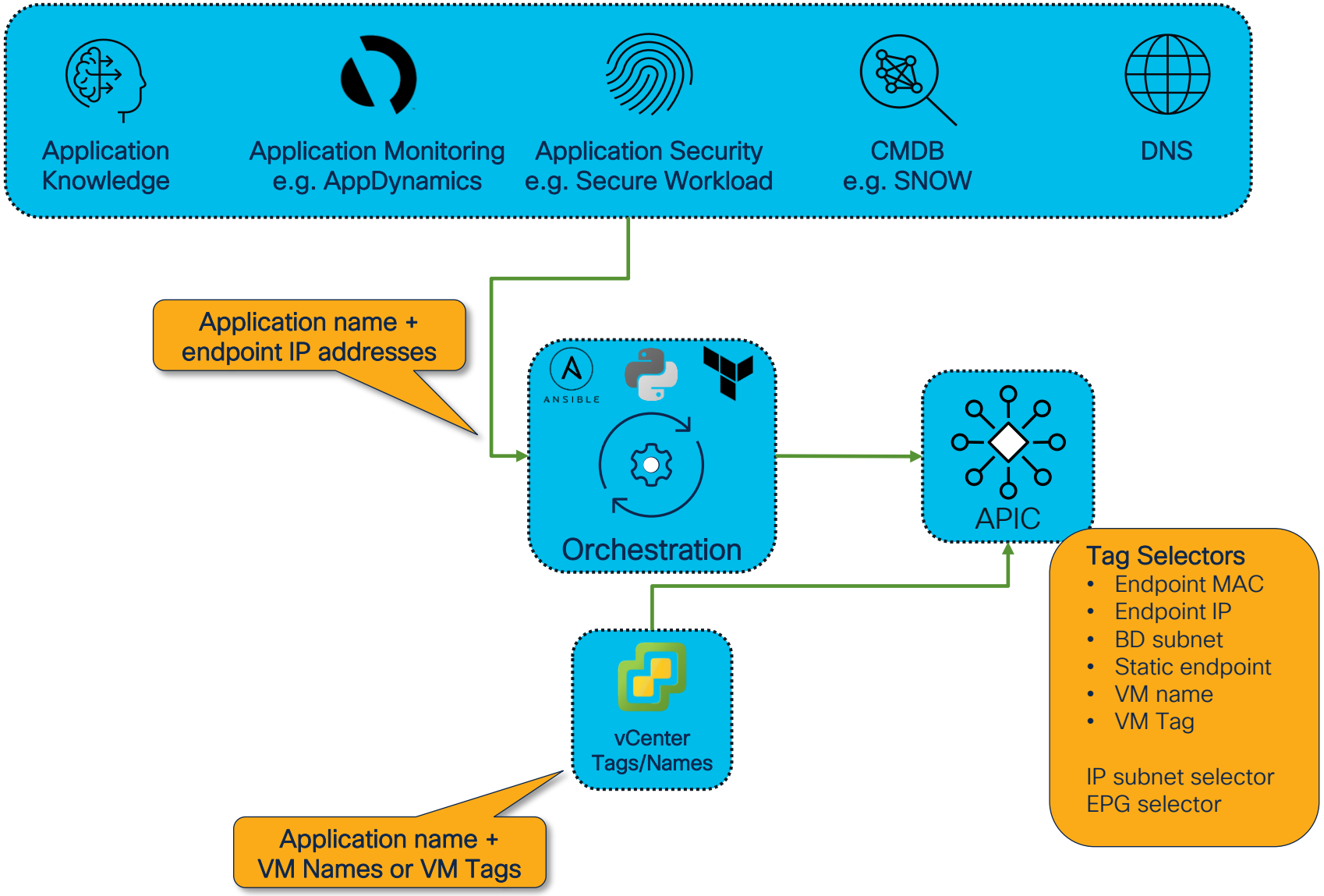
Wrapping up...



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

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

Application Knowledge taken from any source



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

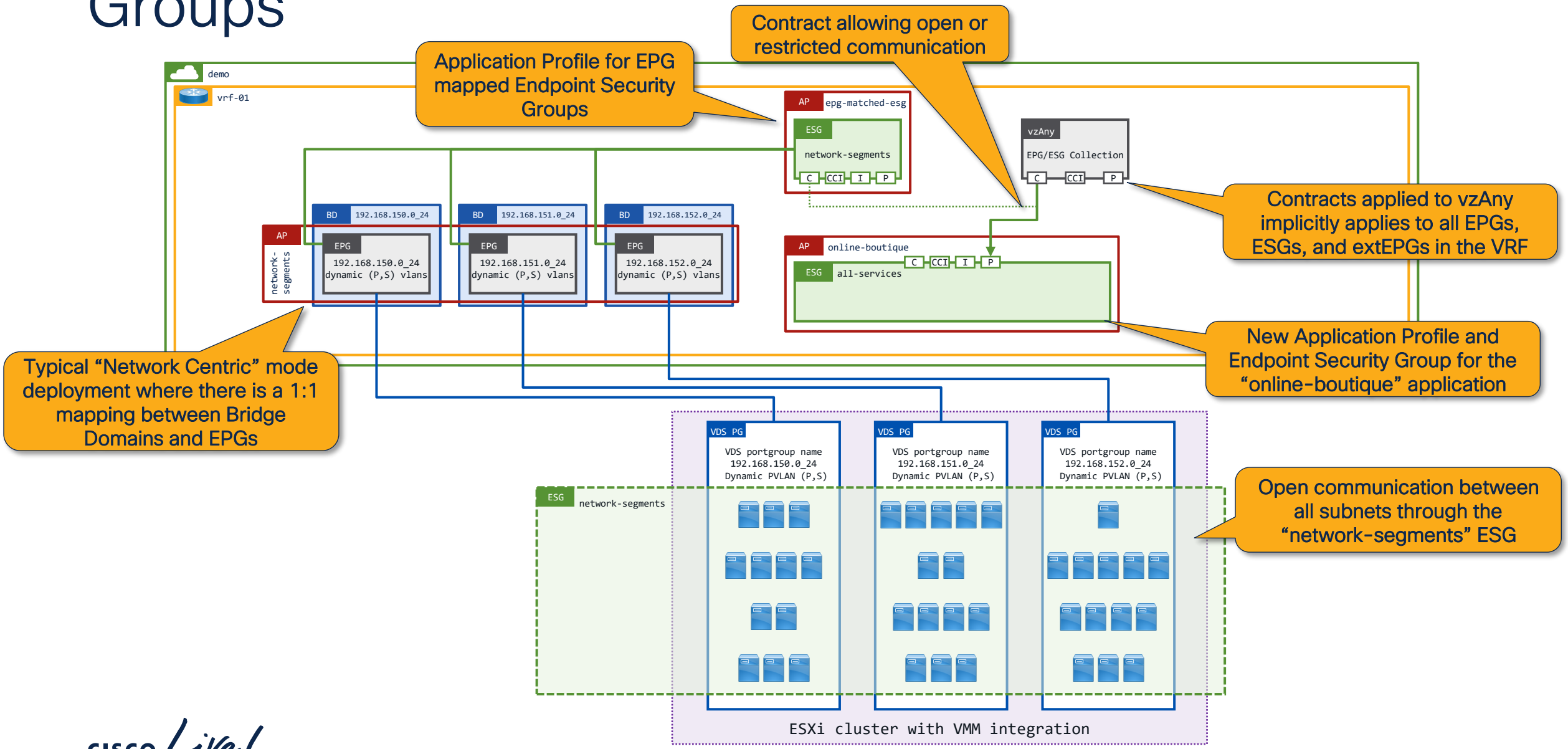
Physical or virtual workloads, with or without VMM Integration...!

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

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

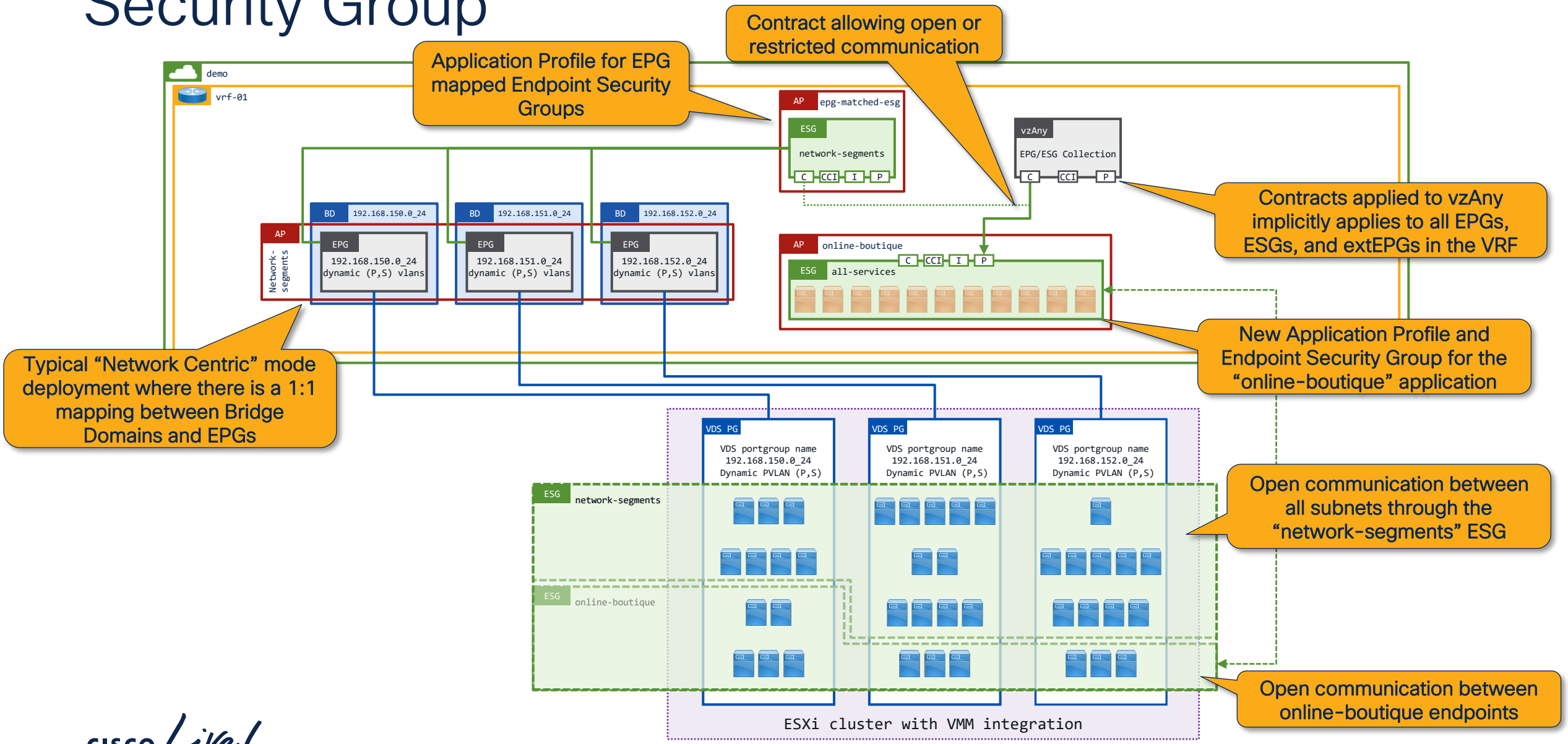
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 1: Create Application Profiles and Security Groups



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

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



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

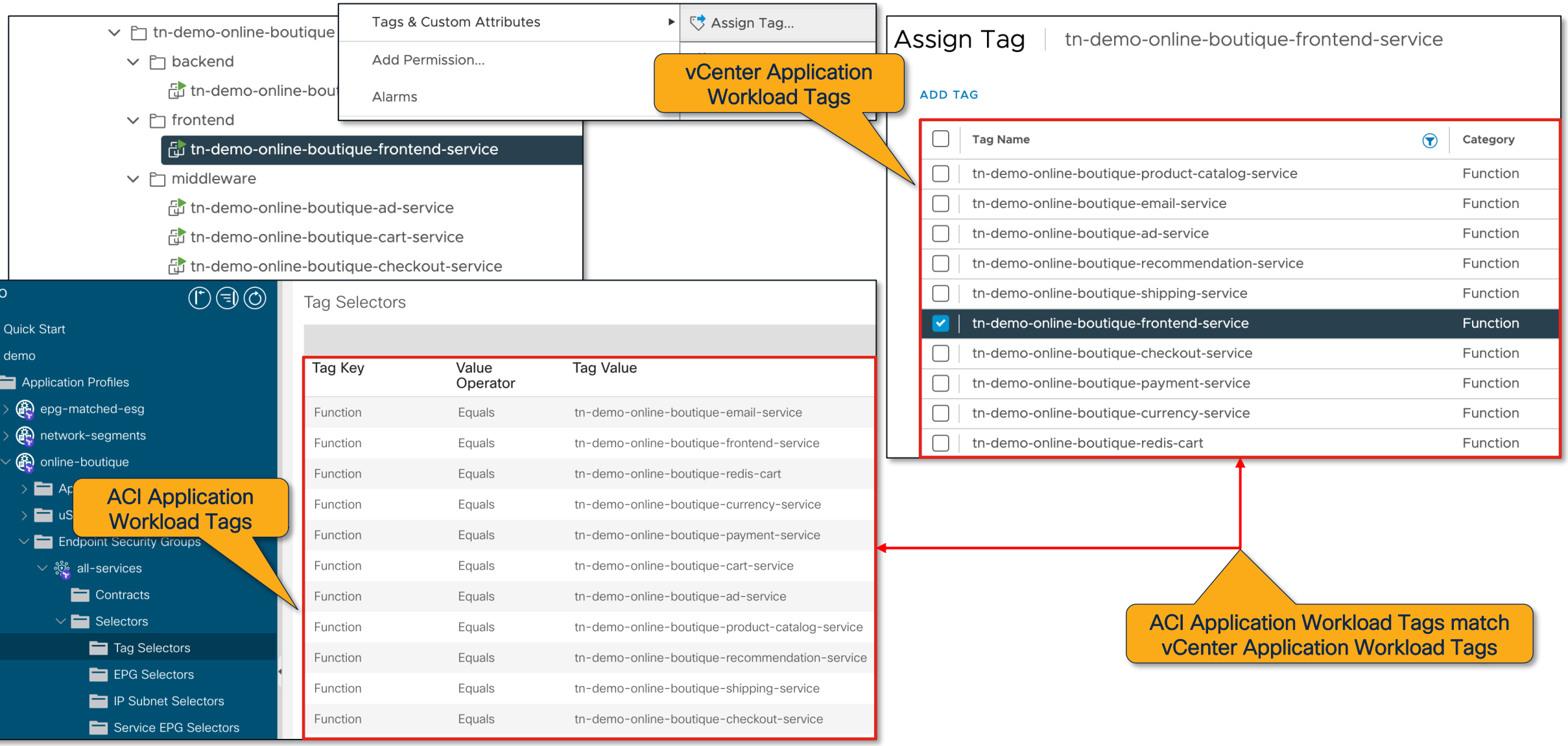
Tagging Option 1: Static Tag Mapping (manual/automated)

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

Automated conversion to “Application Centric”

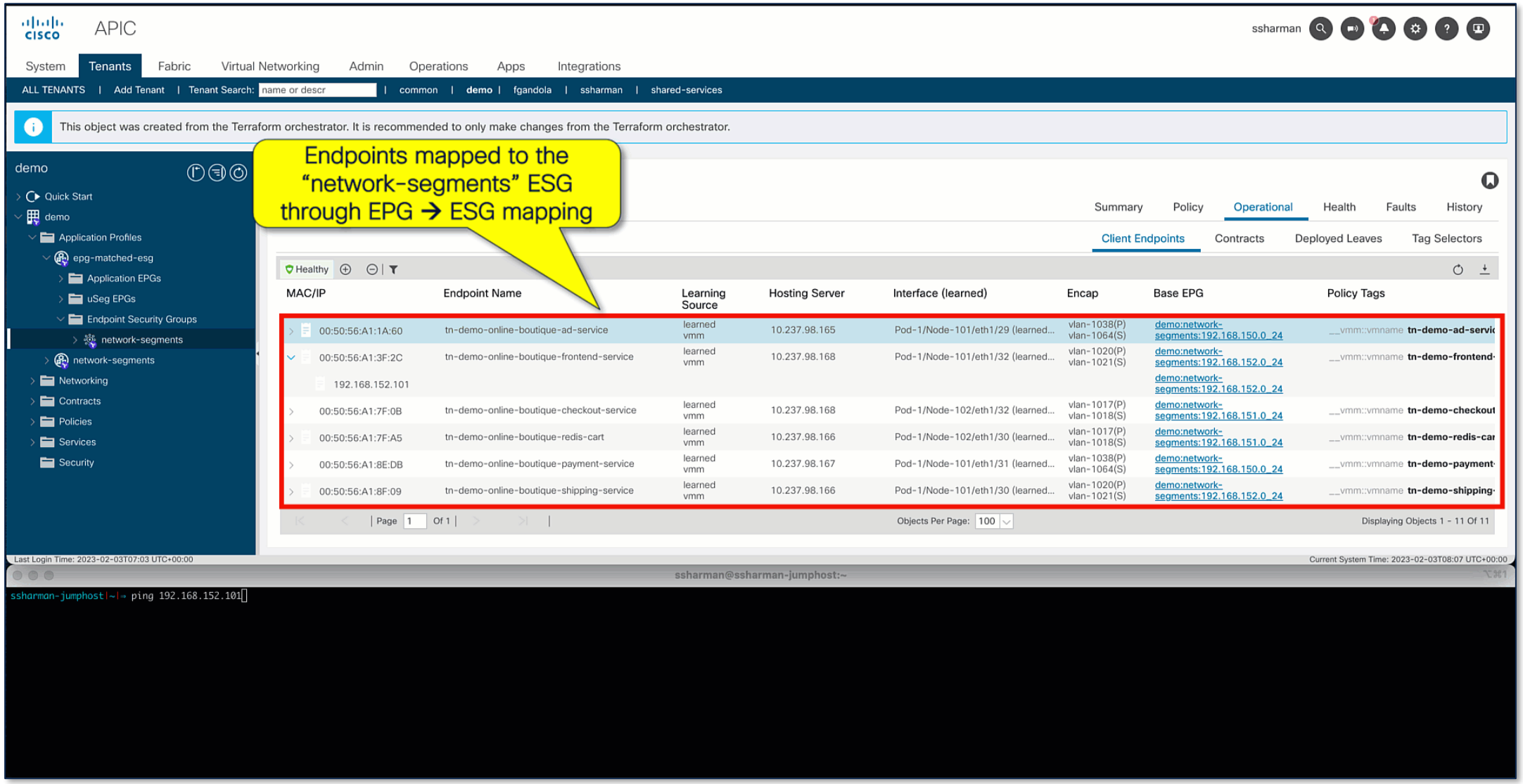
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Tagging Option 2: VMM Tag Mapping



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

Automated conversion to “Application Centric”

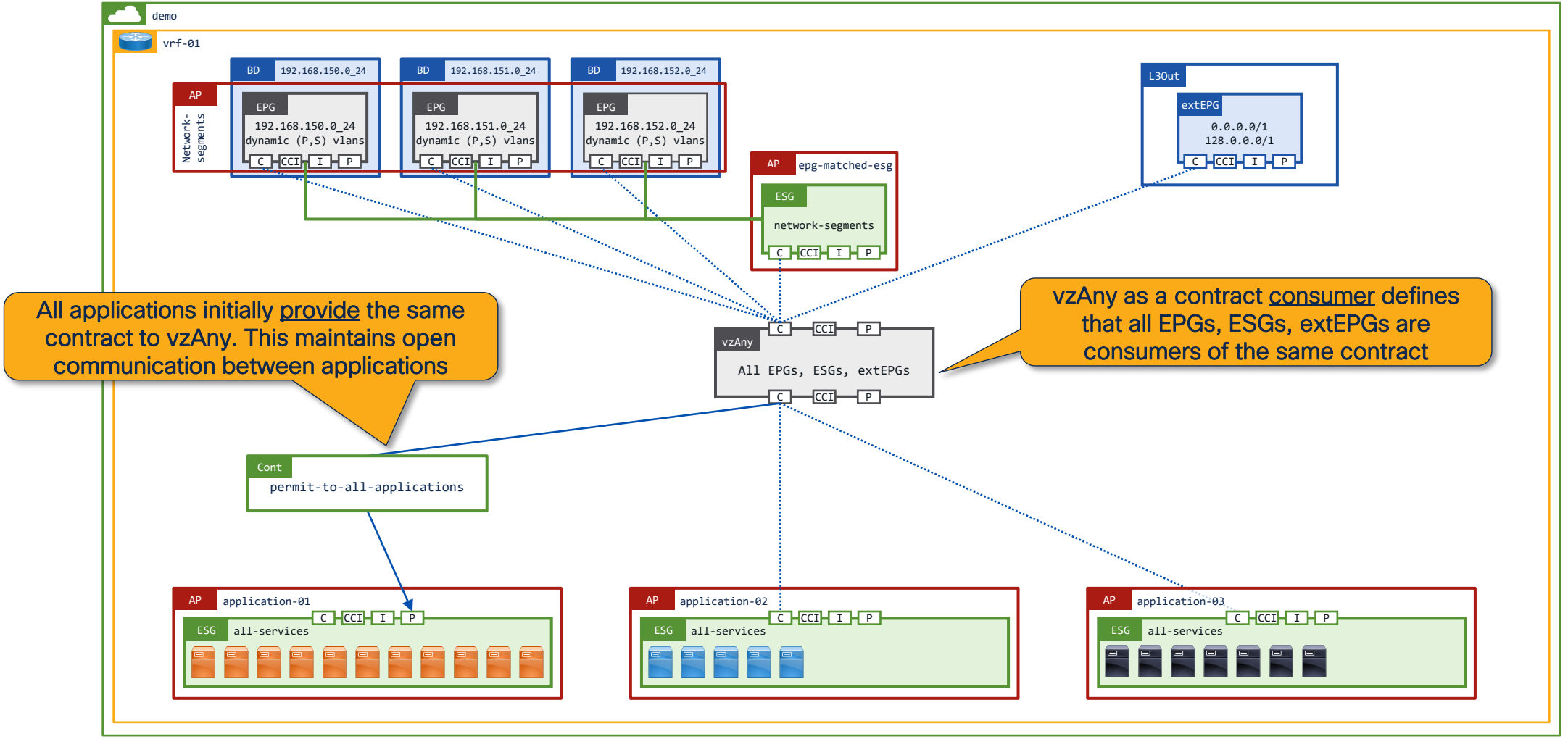


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling application connectivity with vzAny...

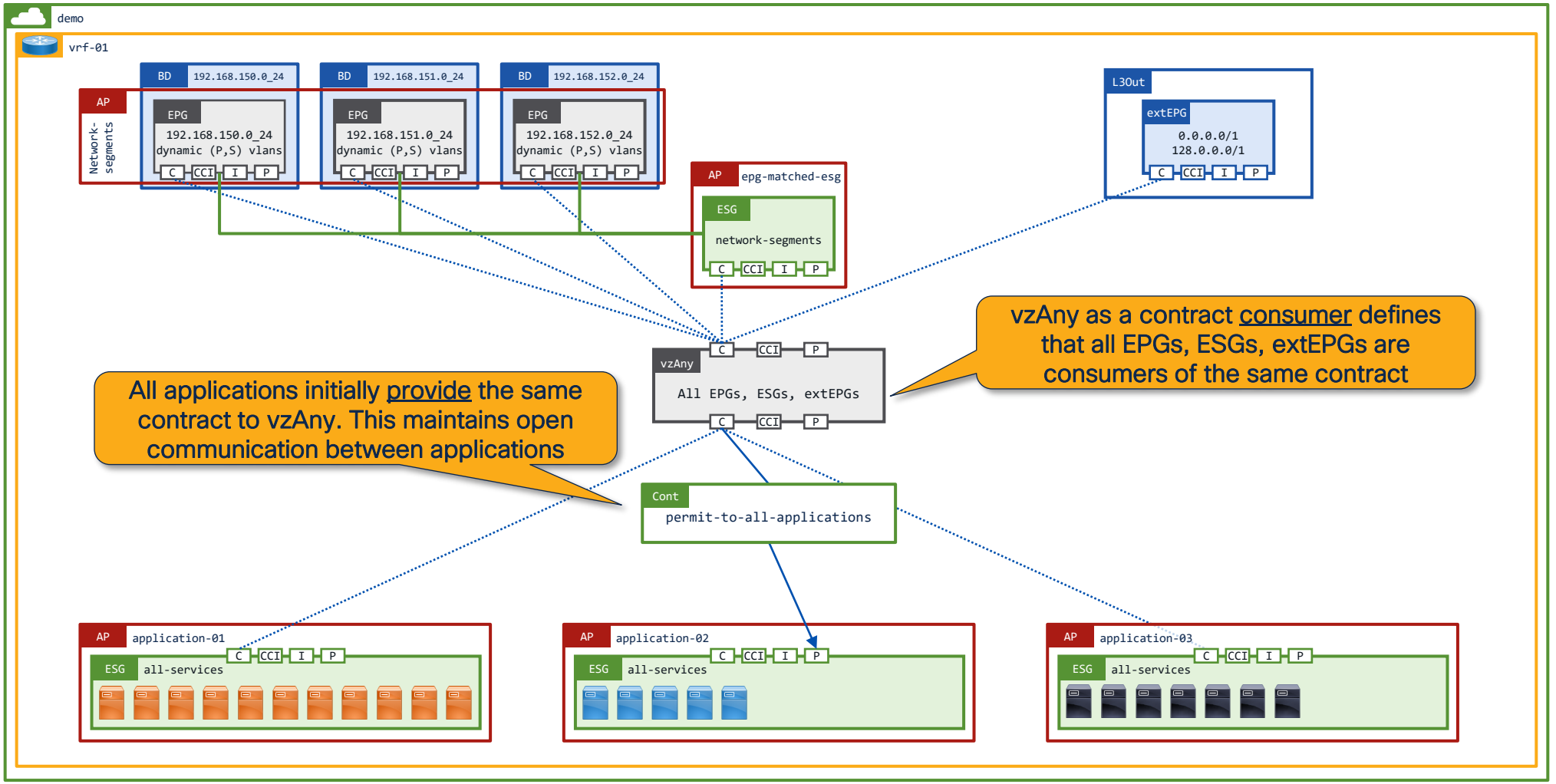
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling connectivity to “application-01”



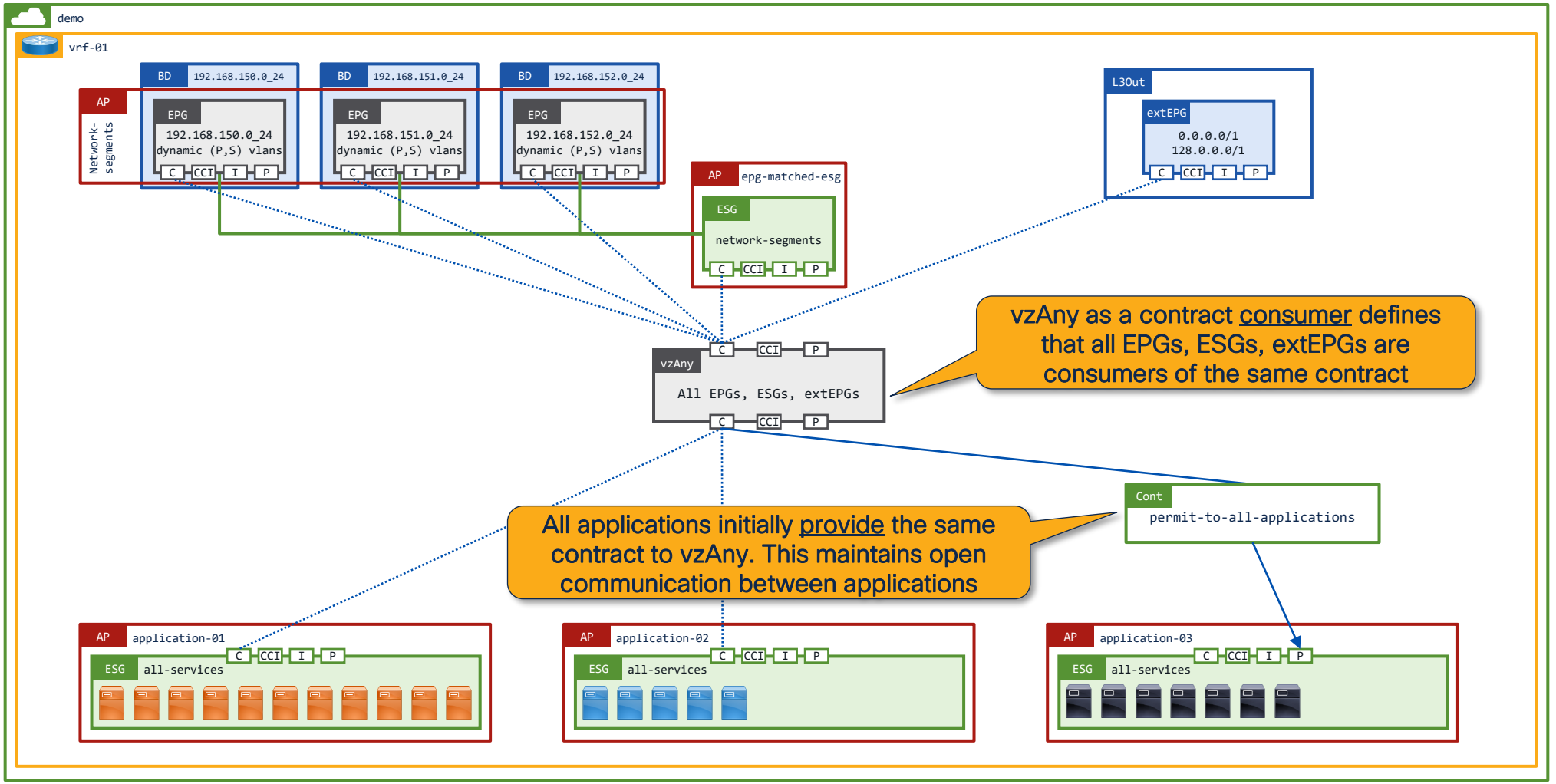
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scaling connectivity to “application-02”



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

Scaling connectivity to “application-03”



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

Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

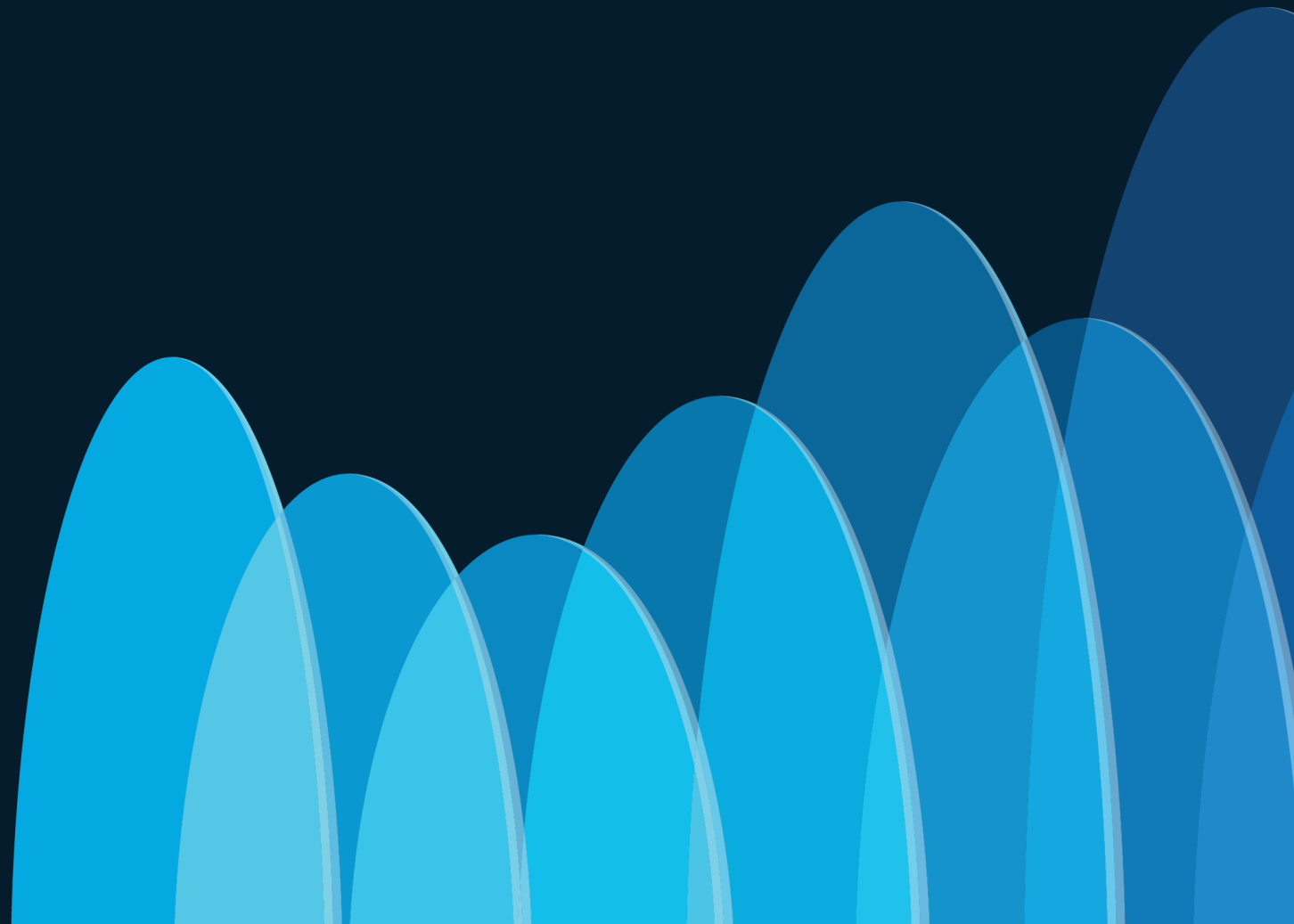
Understanding ACI security...

External Connectivity...

Increasing Security...

Automation Blueprints...

Wrapping up...



Why are ESGs a better classification option...?

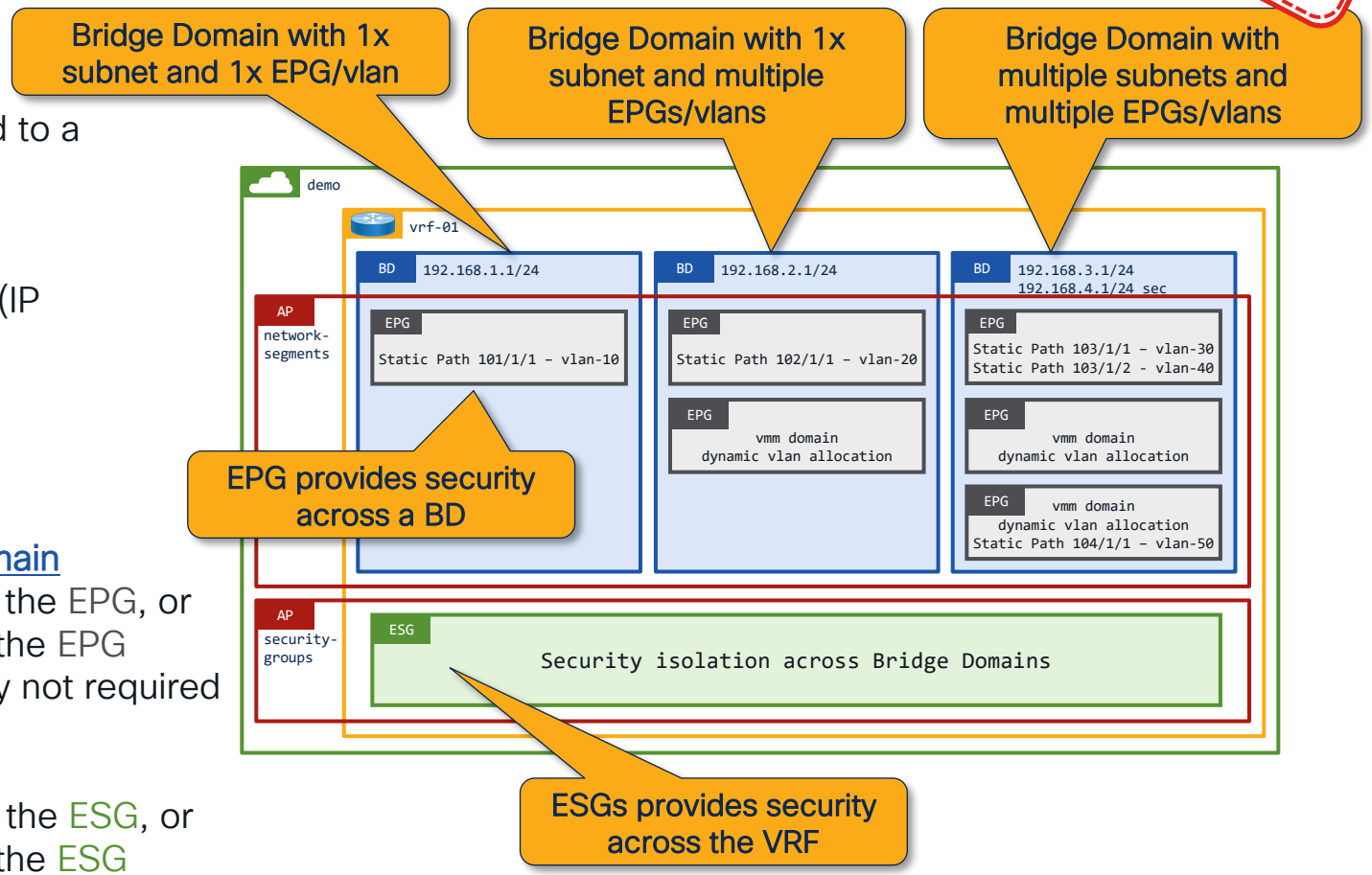
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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



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

What are our endpoint mapping options...?

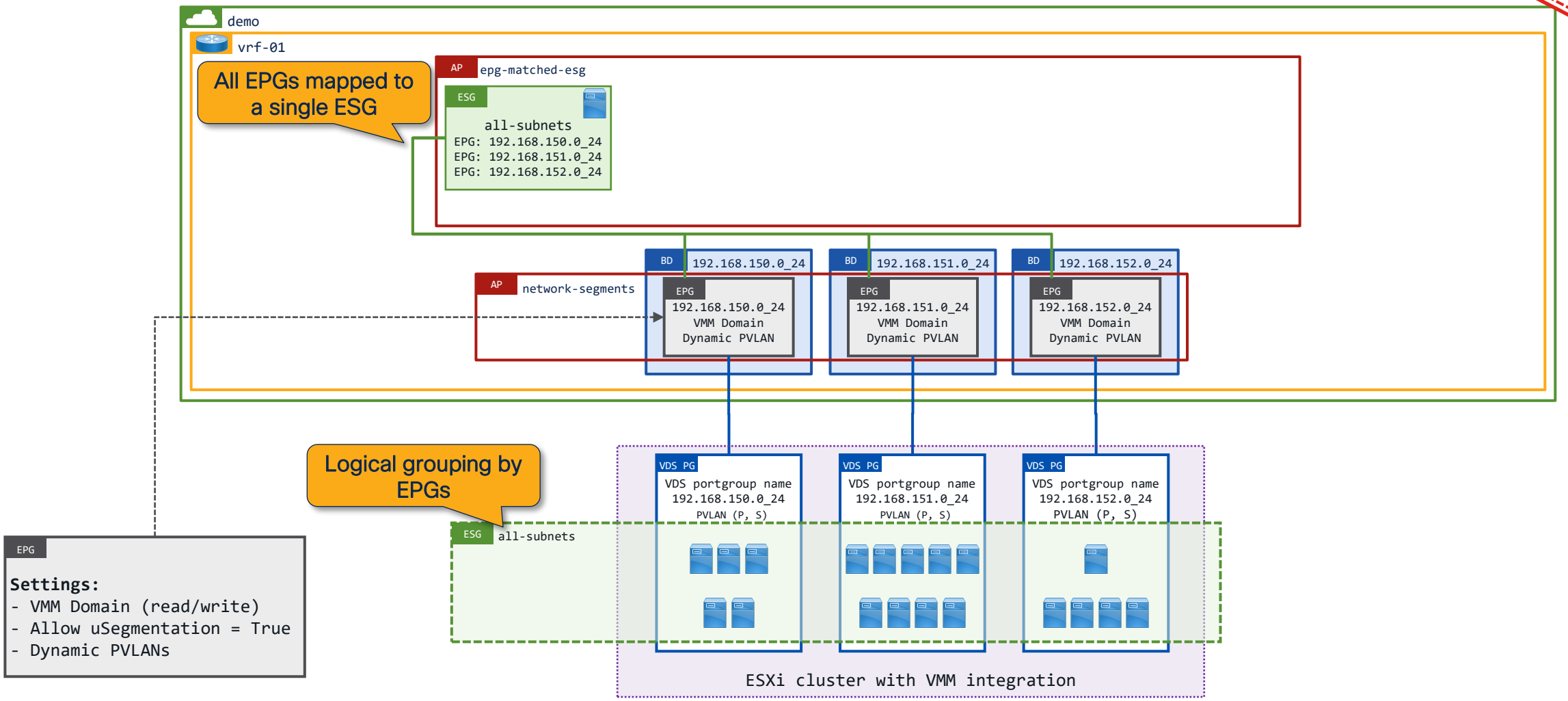
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

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

Option 1: EPG mapping to a single security zone

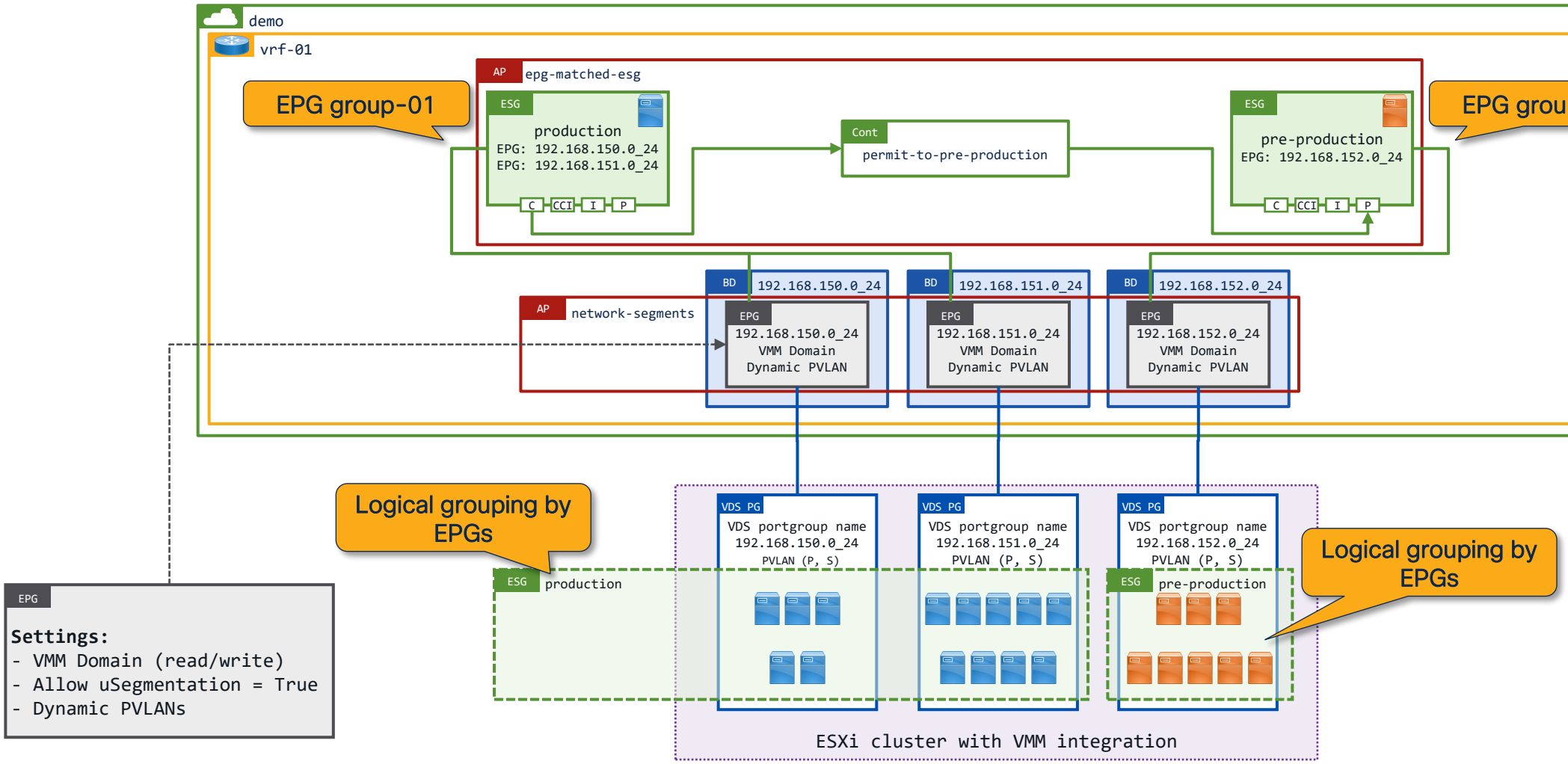
Open security comparable to vzAny, excluding the extEPG



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

Option 2: EPG mapping for multiple security zones

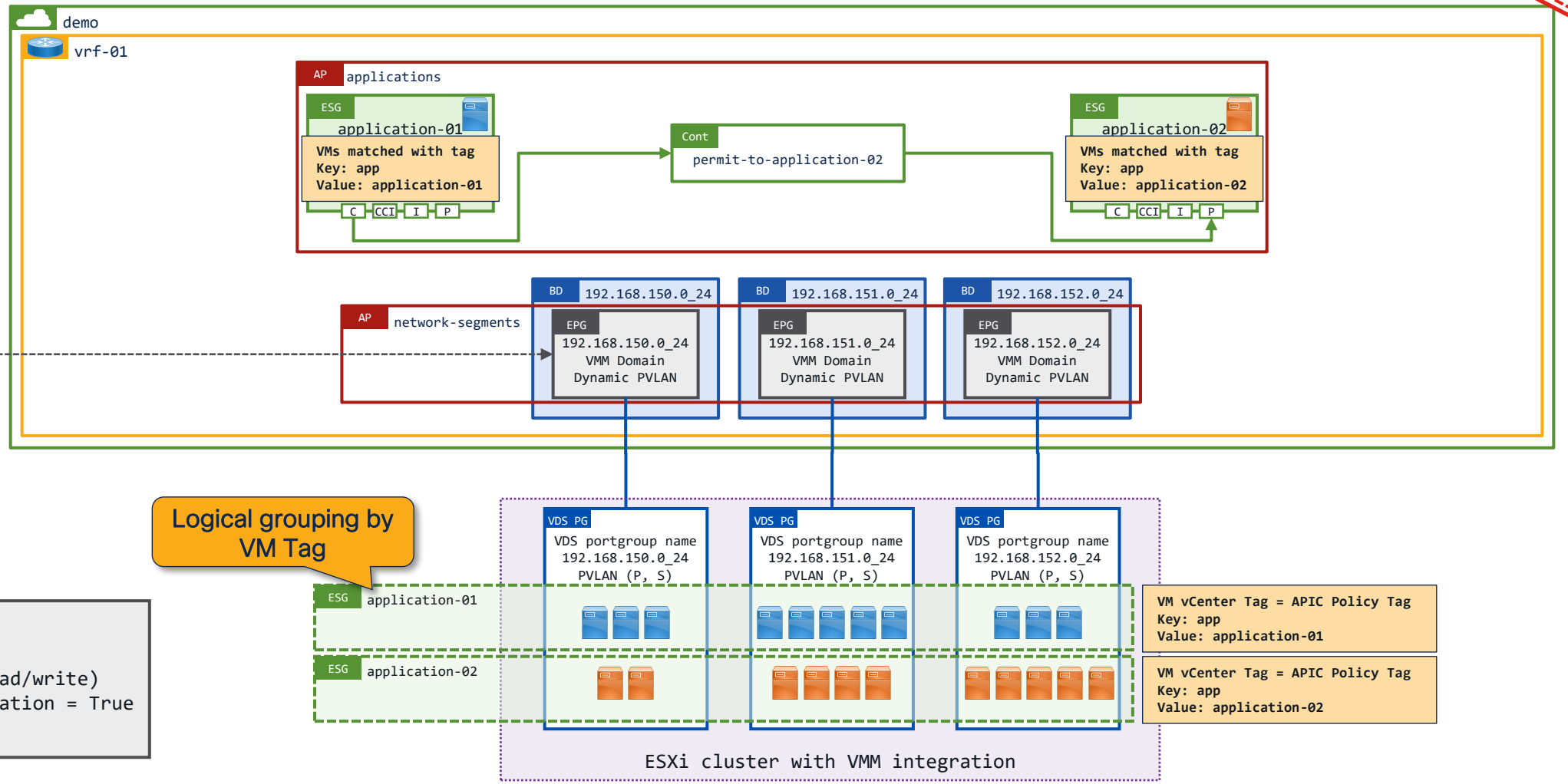
Two or more security zones, e.g. Production and Pre-Production



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

Option 3: Tag selectors with VMM integration

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



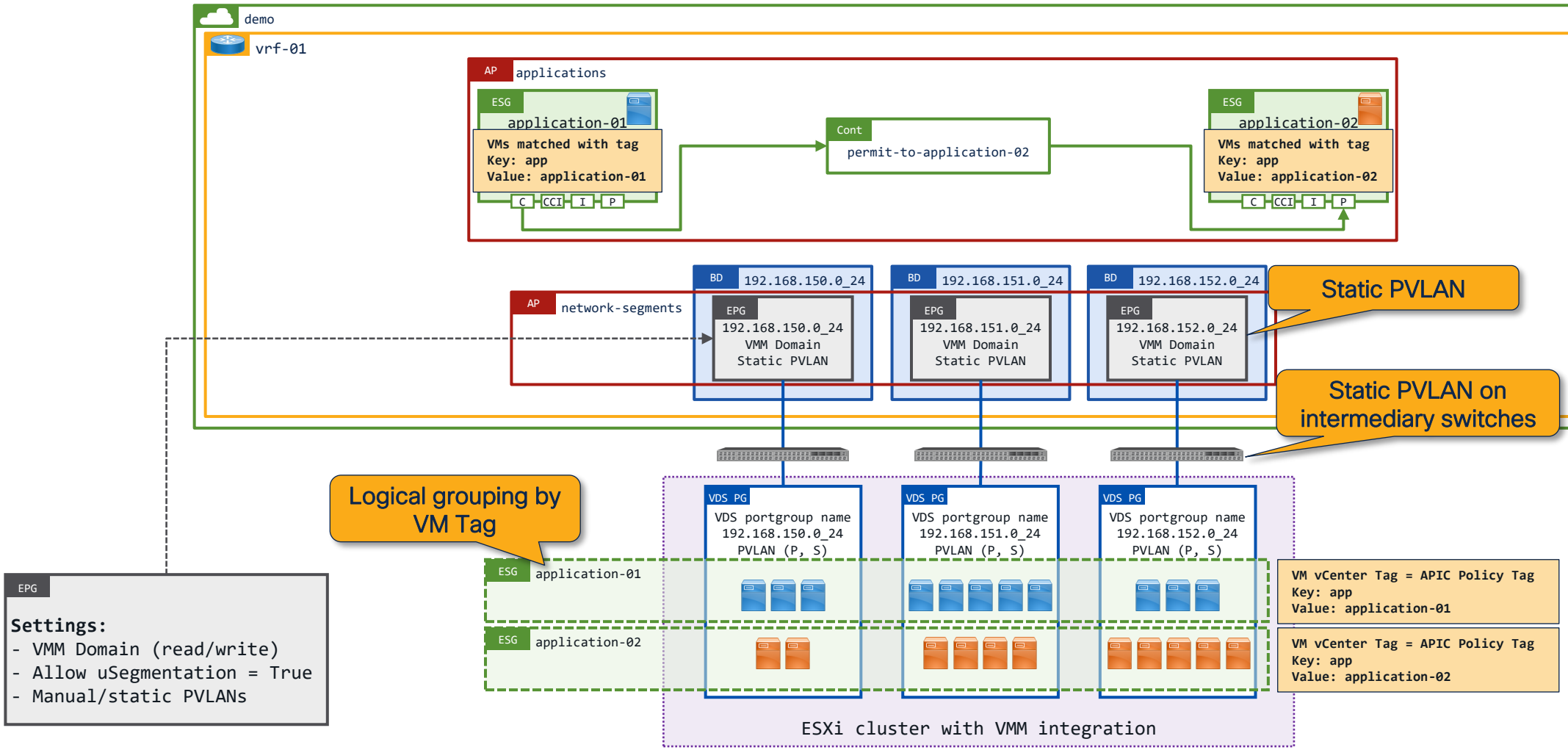
EPG

Settings:
- VMM Domain (read/write)
- Allow uSegmentation = True
- Dynamic PVLANs

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

Option 4: Tag selectors with VMM integration and Intermediary switches

Intermediary switches require PVLAN pre-provisioning



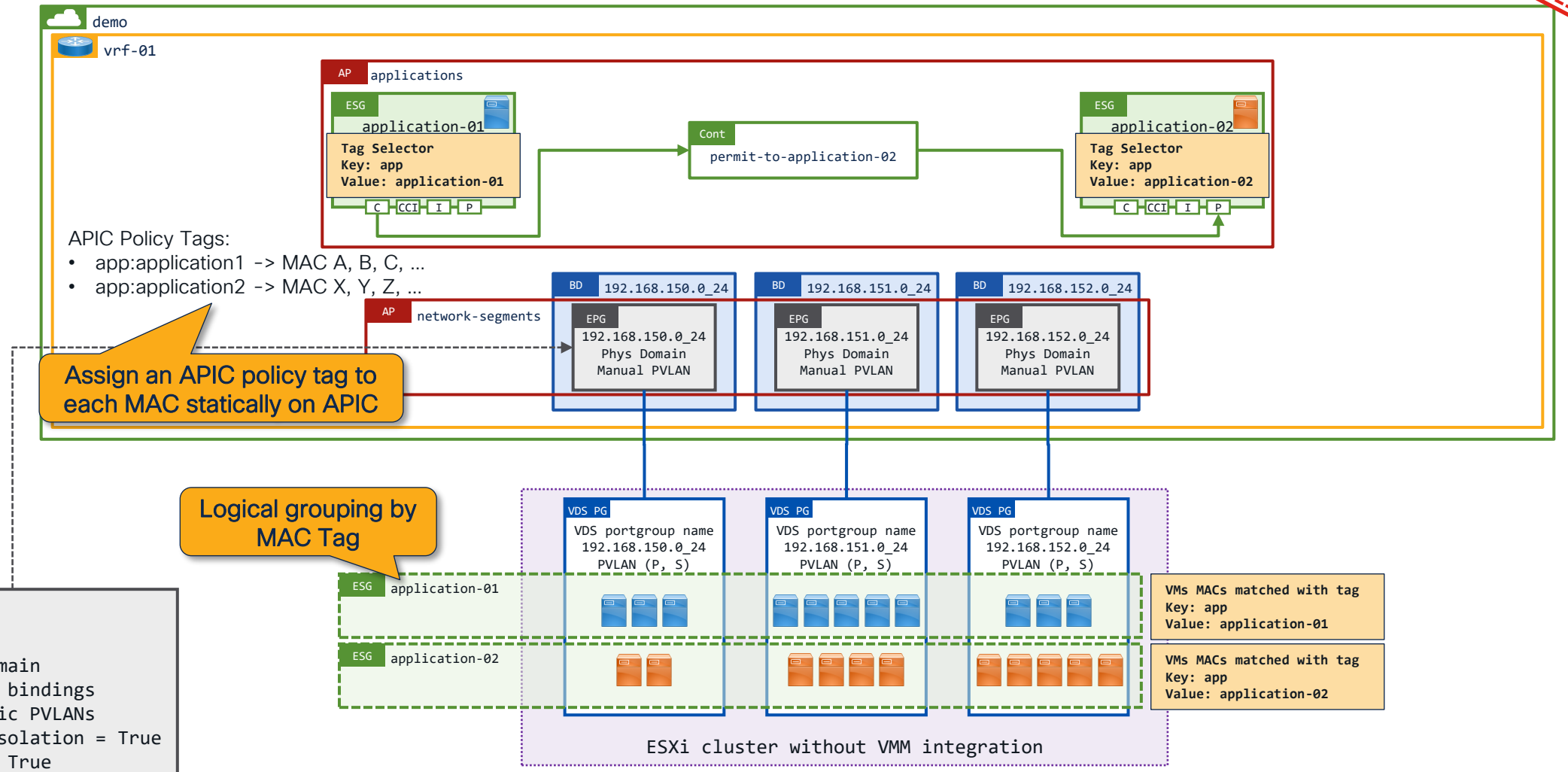
EPG

Settings:
- VMM Domain (read/write)
- Allow uSegmentation = True
- Manual/static PVLANs

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

Option 5: MAC selectors, no VMM integration

Endpoint assignment using endpoint MAC addresses. Requires PVLAN on VDS



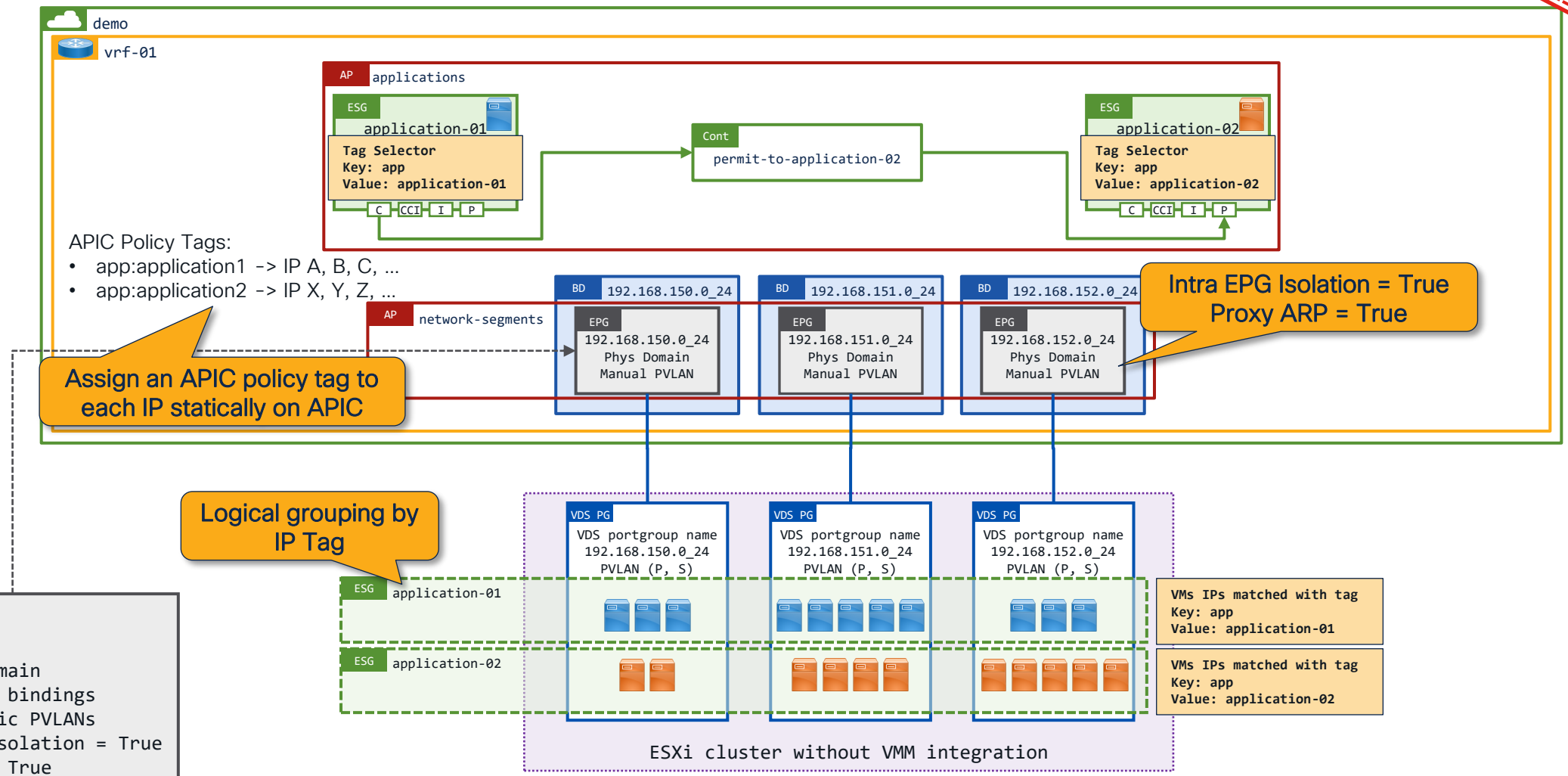
EPG

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

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

Option 6: IP selectors, no VMM integration

Endpoint assignment using endpoint IP addresses. Requires PVLAN on VDS



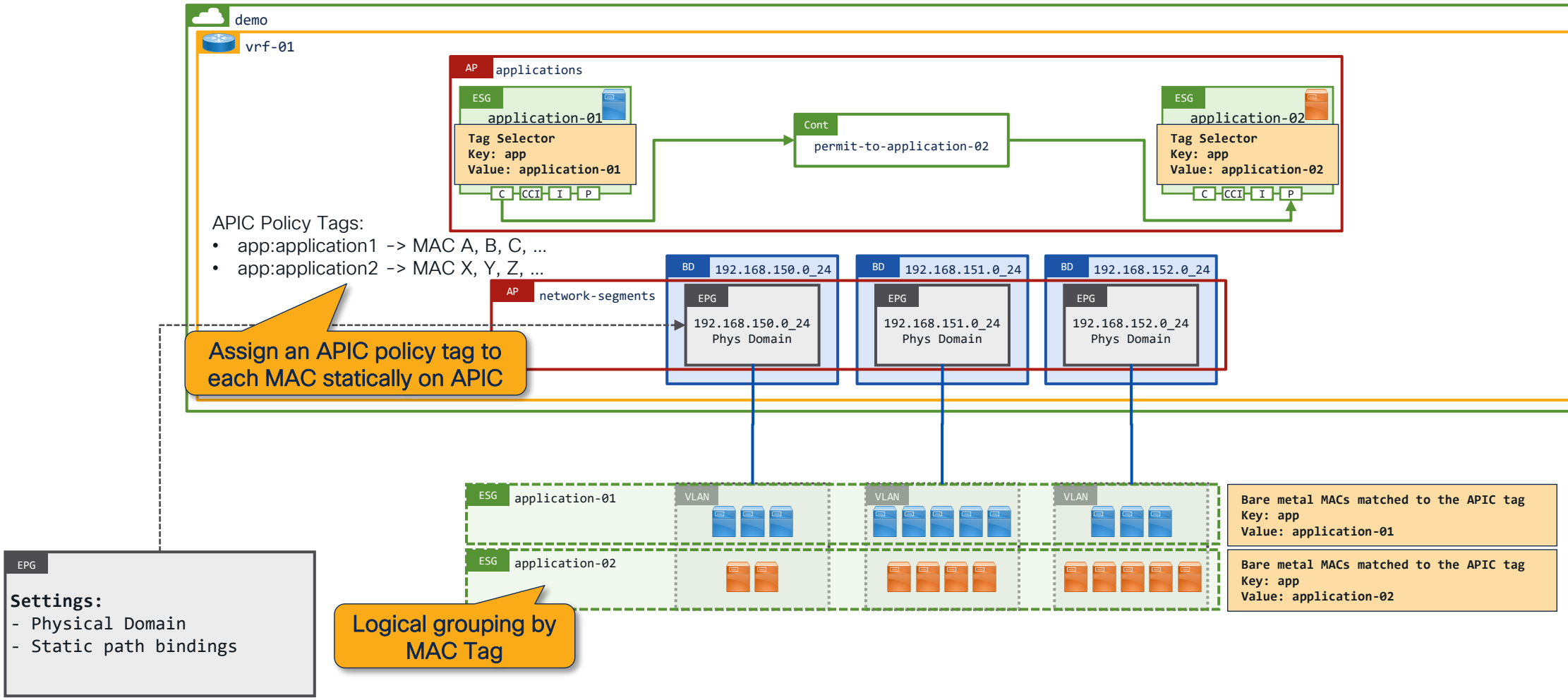
EPG

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

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

Option 7: MAC selectors for bare metal

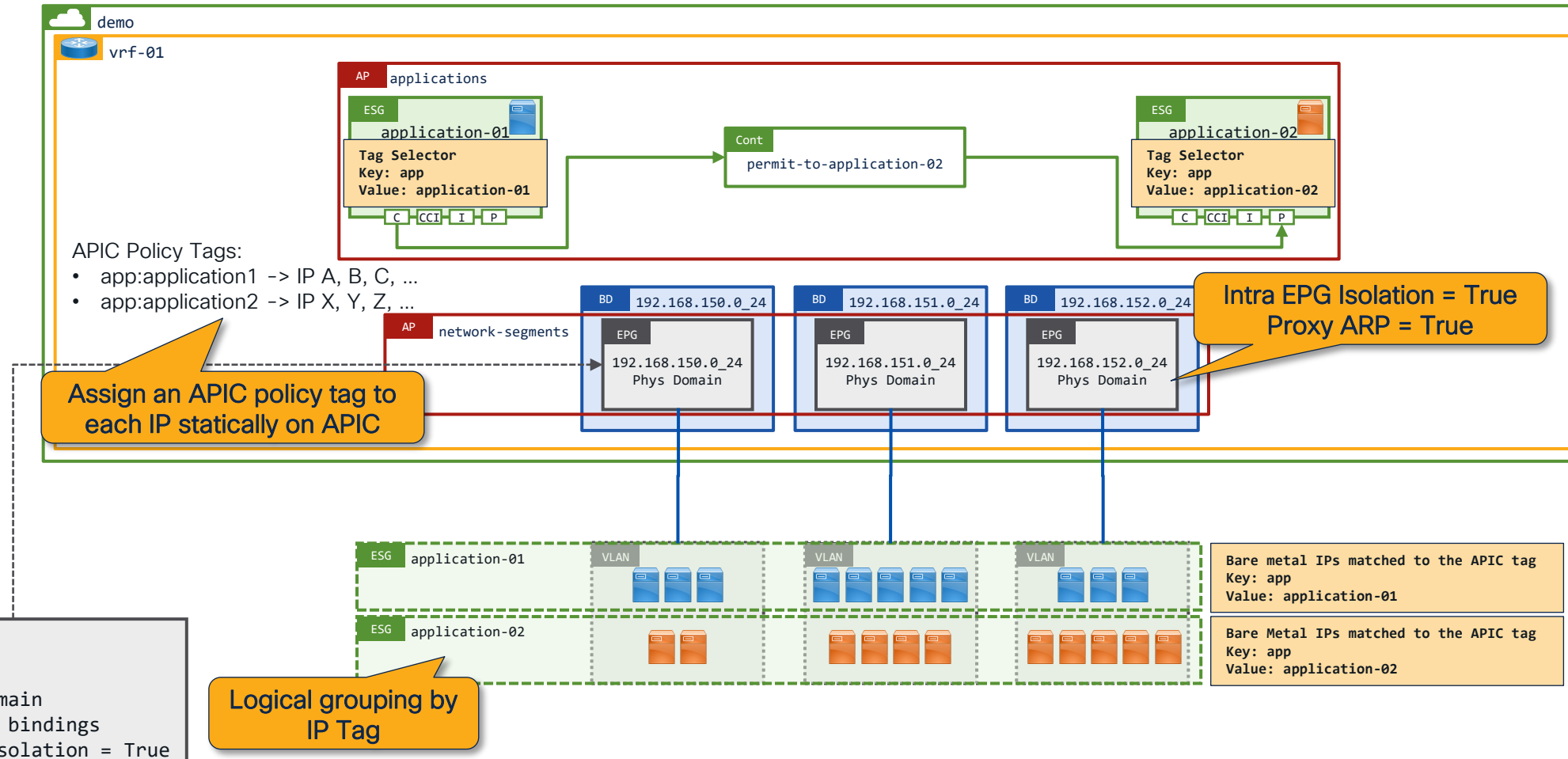
Endpoint assignment using endpoint MAC addresses



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

Option 8: IP selectors for bare metal

Endpoint assignment using endpoint IP addresses



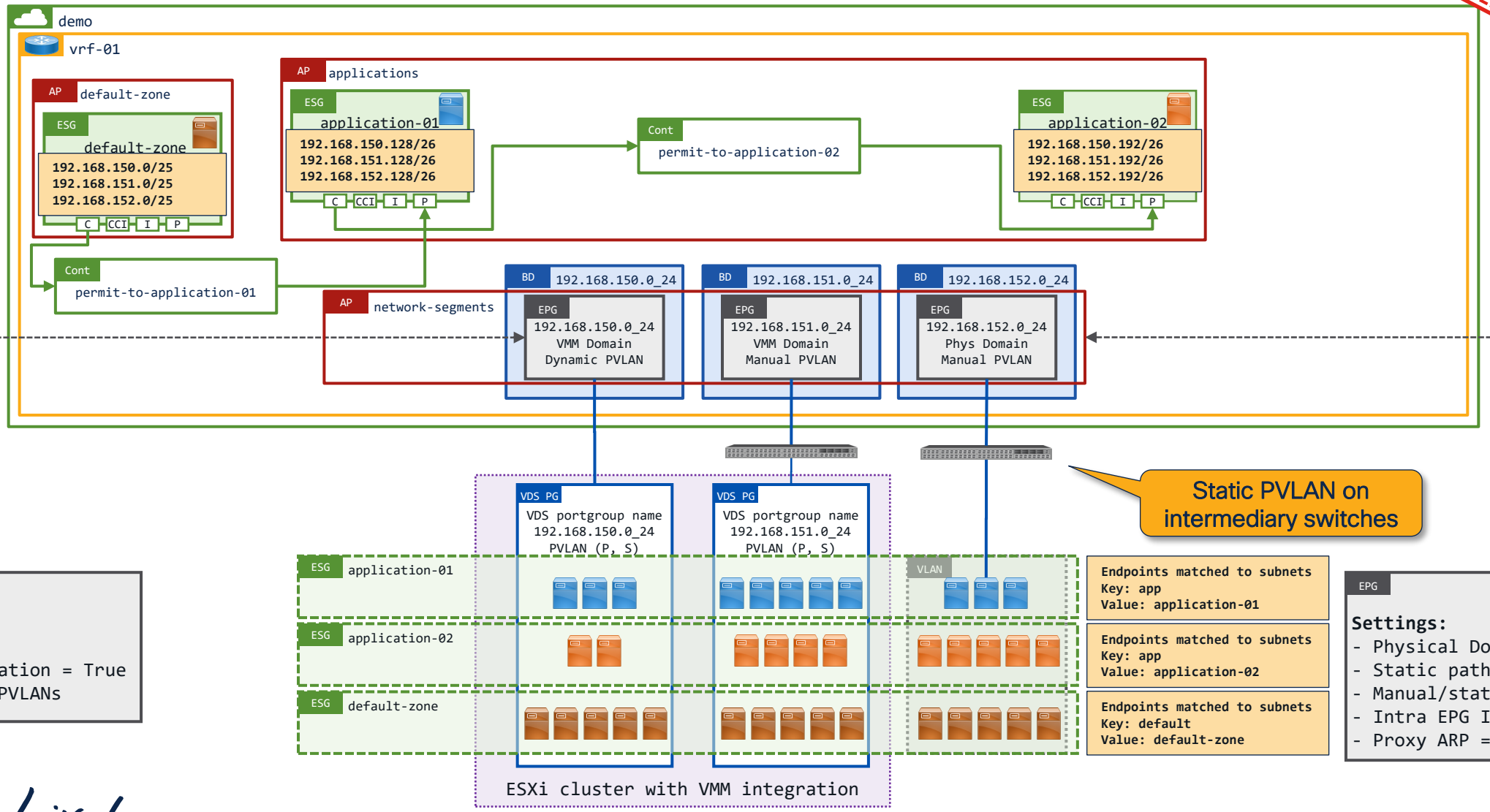
EPG

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

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

Option 9: Subnet selectors with mixed Domains

Endpoint assignment using subnet ranges



EPG

Settings:
- VMM Domain
- Allow uSegmentation = True
- Manual/static PVLANs

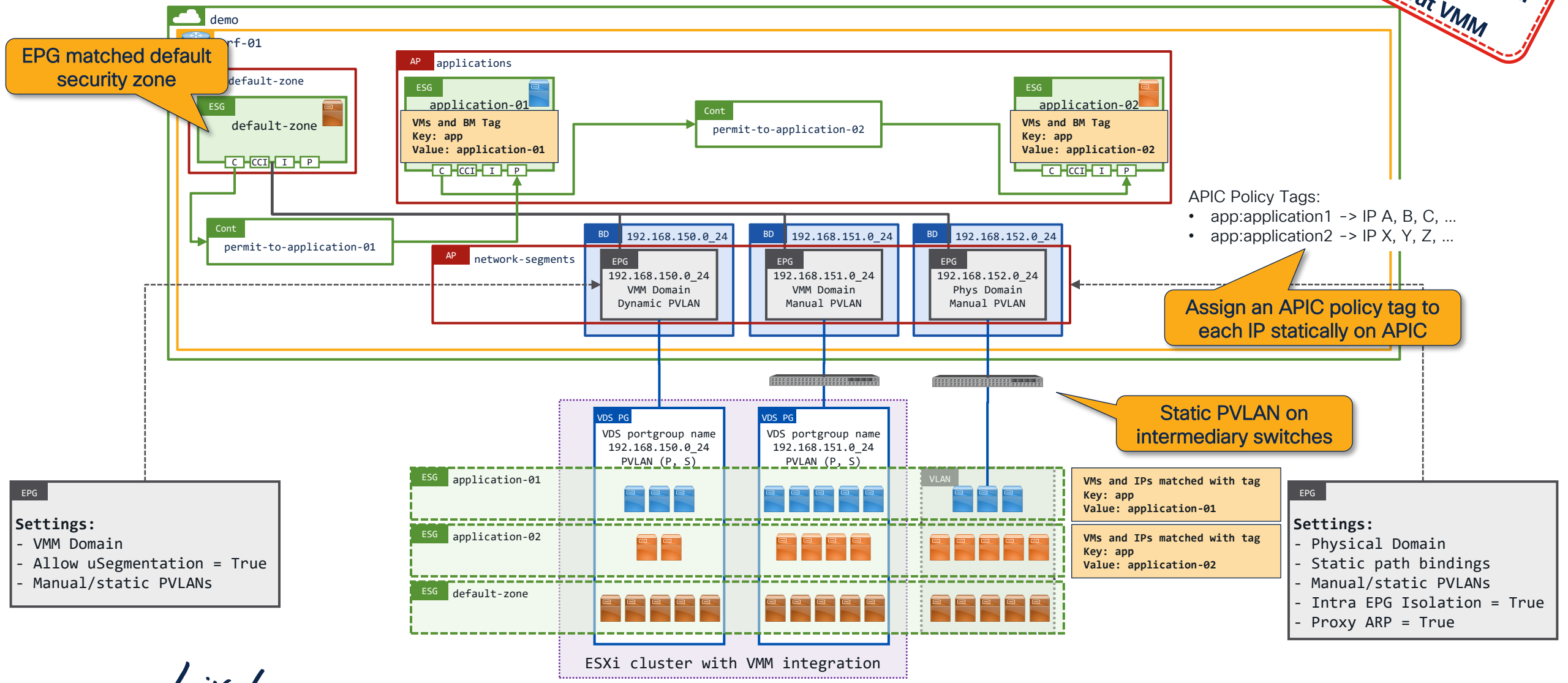
EPG

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

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

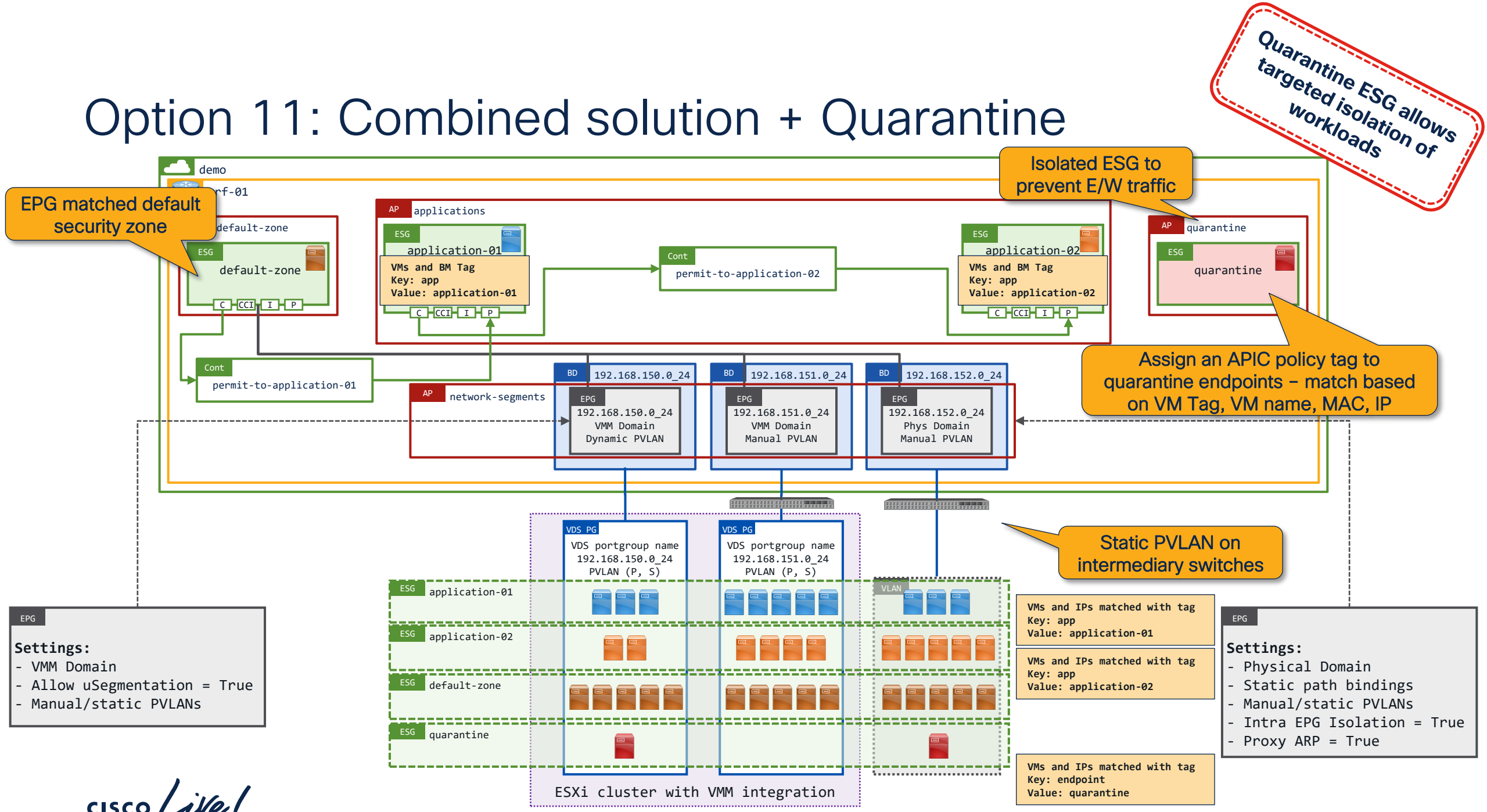
Option 10: Combined solution with/without VMM

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



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

Option 11: Combined solution + Quarantine



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

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

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

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...

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

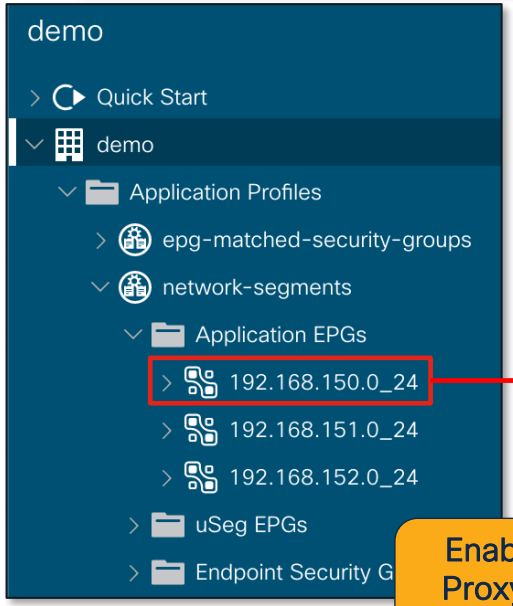
Proxy ARP

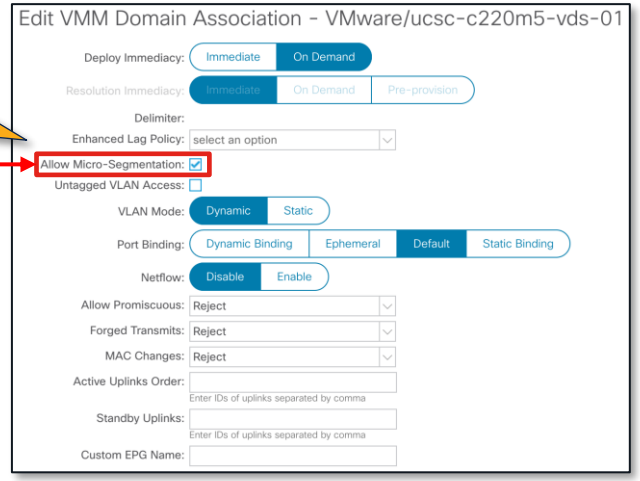
Why Proxy ARP...?

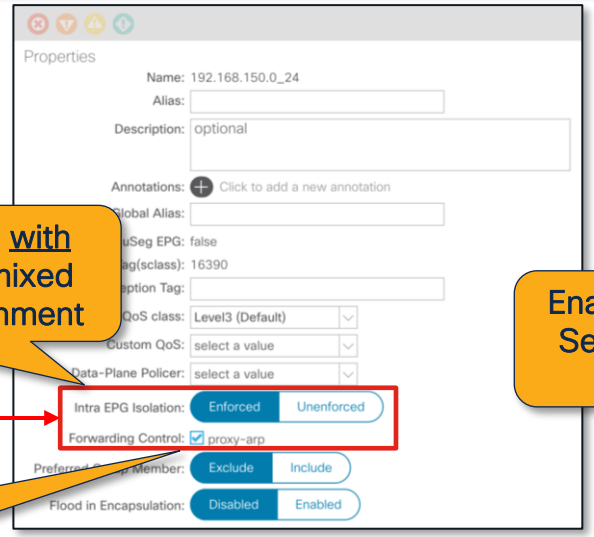
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

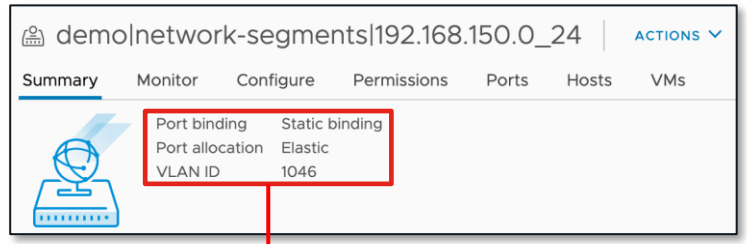
How do you enable Proxy ARP on the Leaf Switches…?

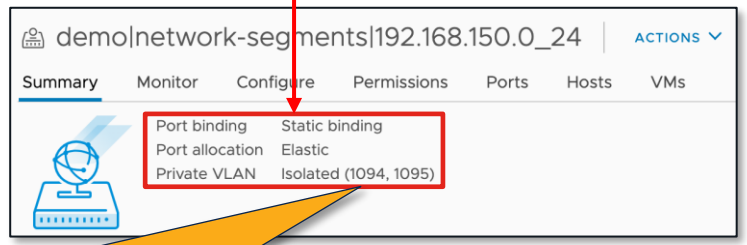
Enabling “Allow Micro-Segmentation” automatically enables Proxy ARP. Option in a 100% virtual deployment, use with or without Intra EPG isolation









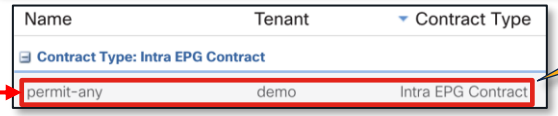


Enable Intra EPG isolation with Proxy ARP if you have a mixed virtual and physical environment

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

Proxy ARP is only available when Intra ESG isolation is enabled

Add an Intra EPG Contract

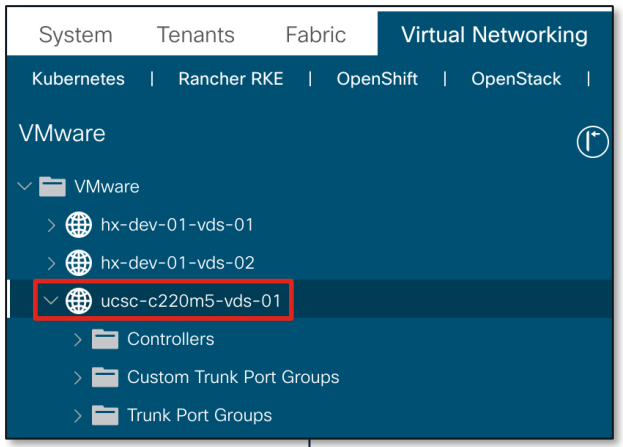


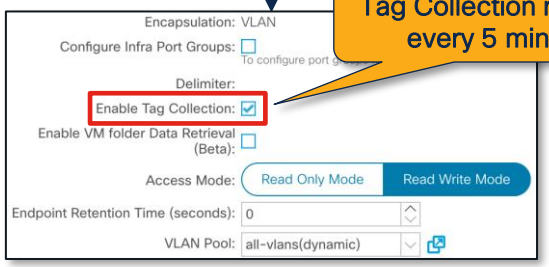
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

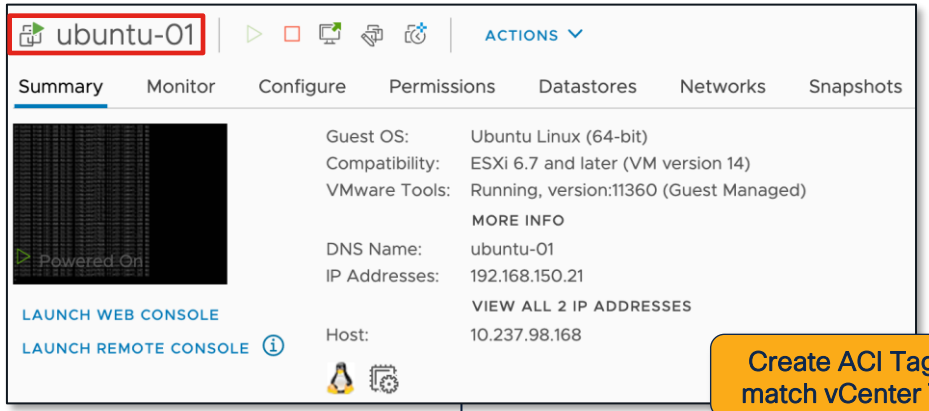
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

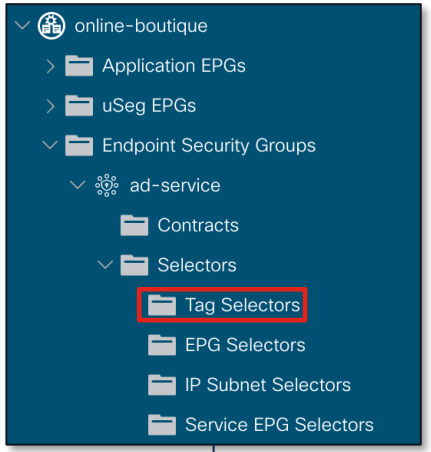
Dynamic Policy Tag matching from vCenter



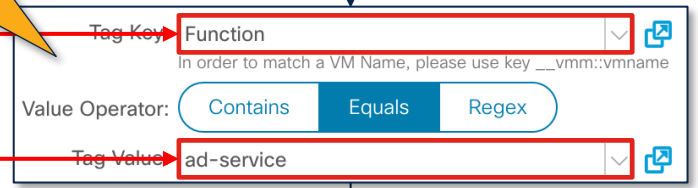


Tag Collection runs every 5 min

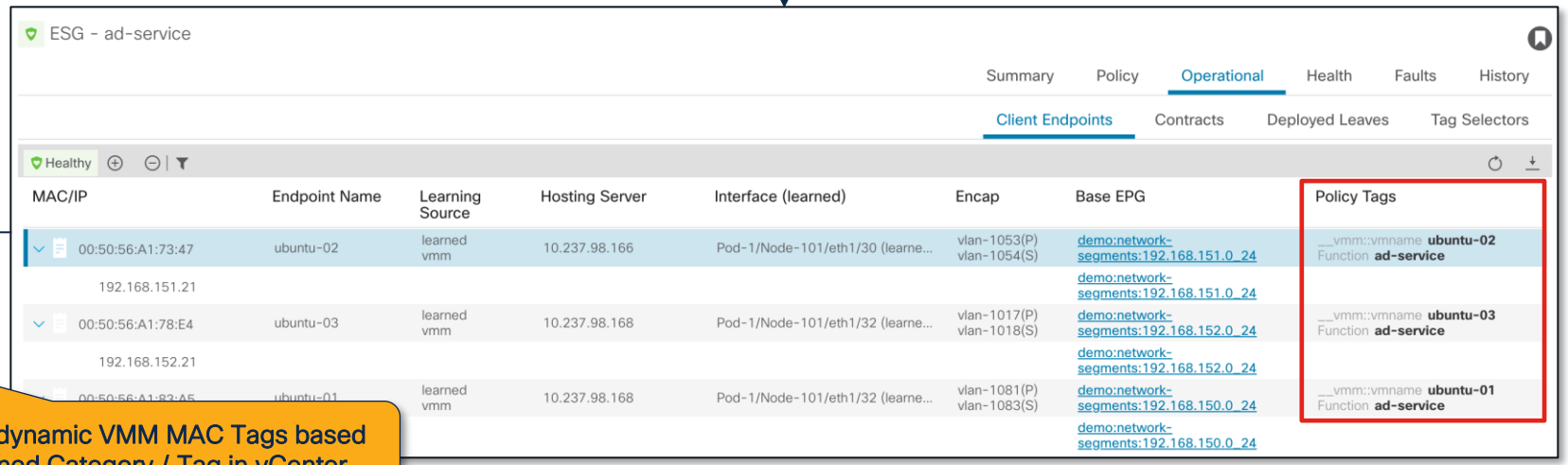




Create ACI Tags to match vCenter Tags



Tenant → Policies → Endpoint Tags



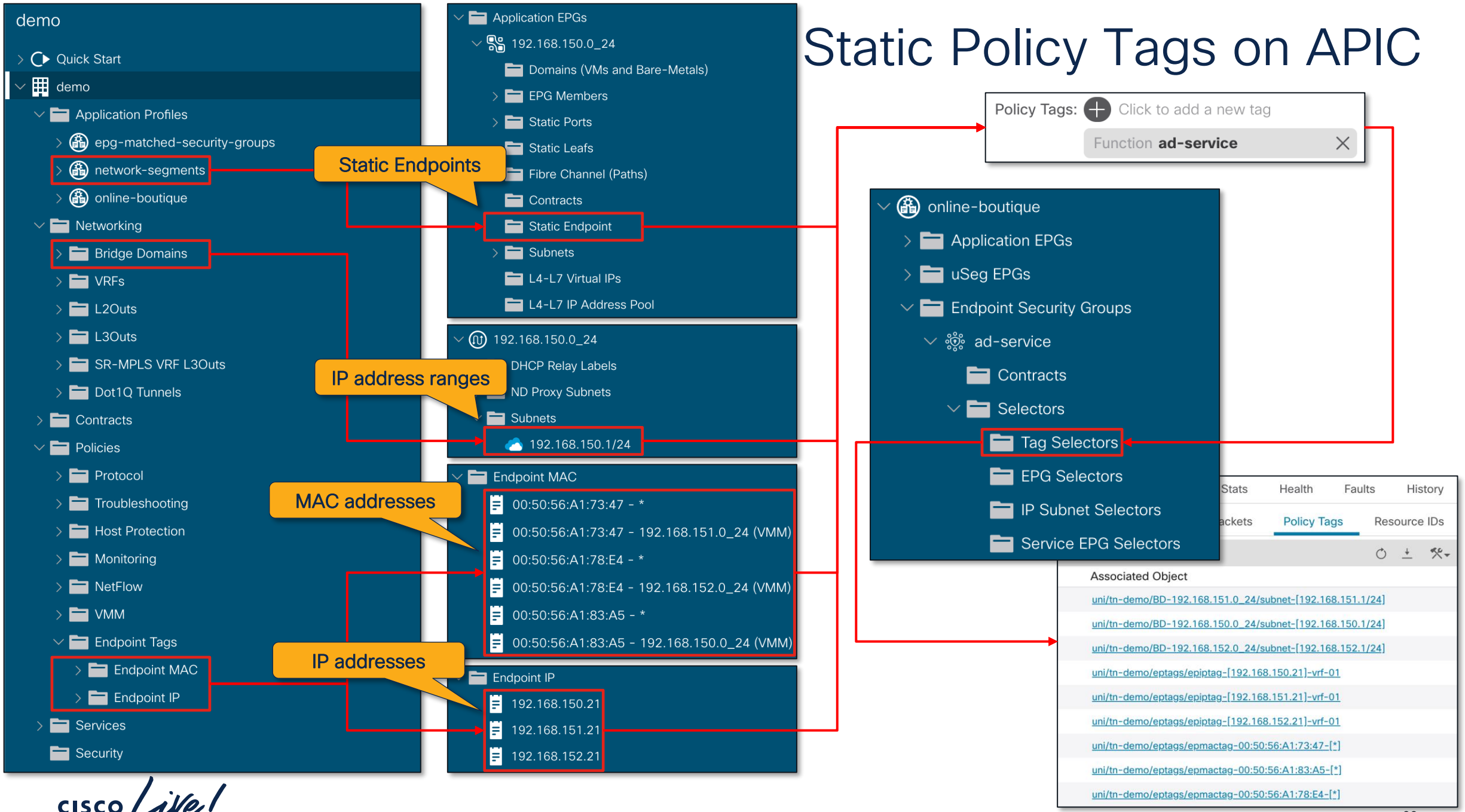
APIC creates dynamic VMM MAC Tags based on the assigned Category / Tag in vCenter

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

Static endpoint mapping...

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

Static Policy Tags on APIC



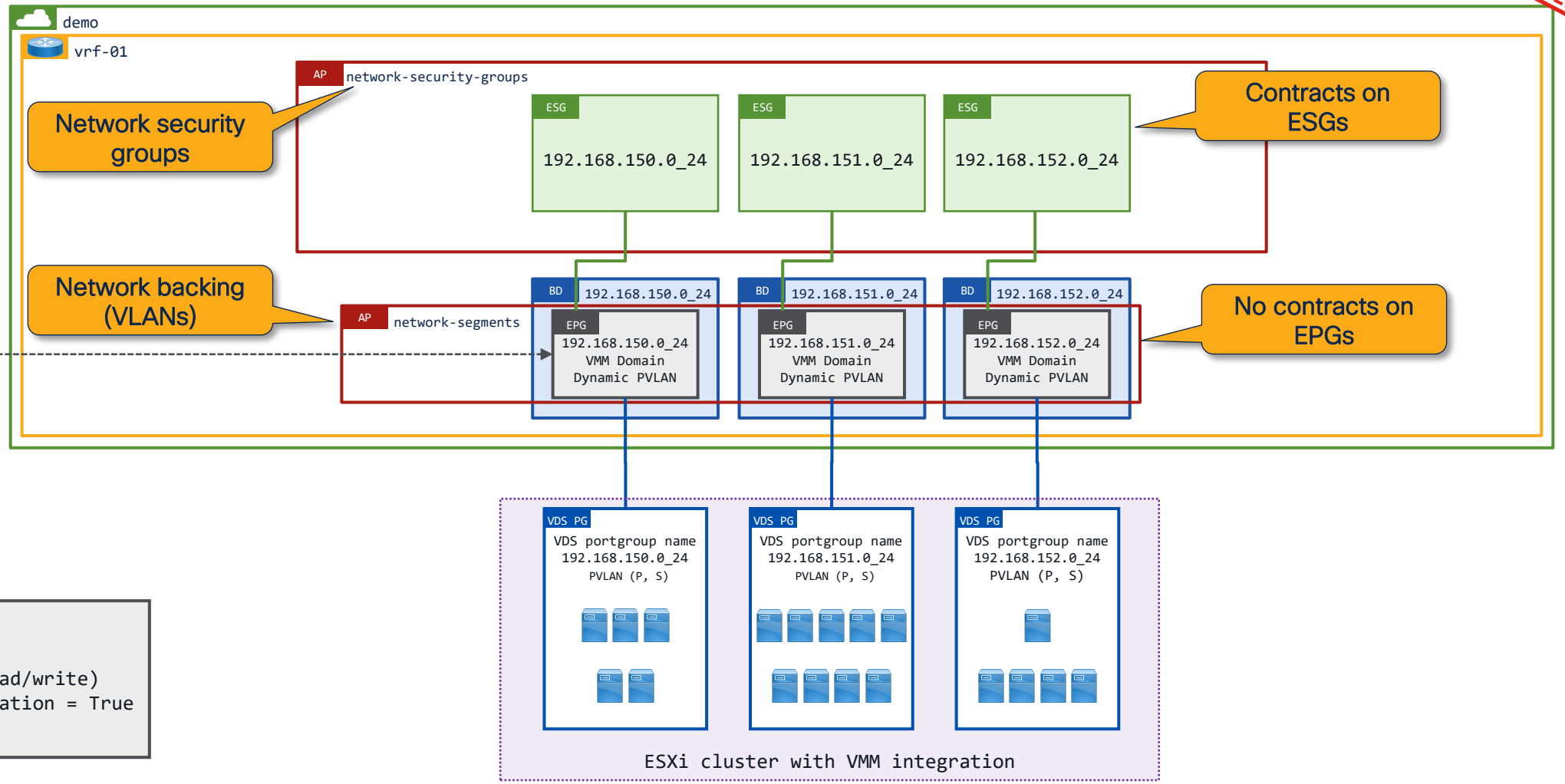
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What if you have a Greenfield deployment...?

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

Greenfield option – 1:1 EPG to ESG mapping

Separate network backing from classification/security



EPG

Settings:
- VMM Domain (read/write)
- Allow uSegmentation = True
- Dynamic PVLANs

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

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

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

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

Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

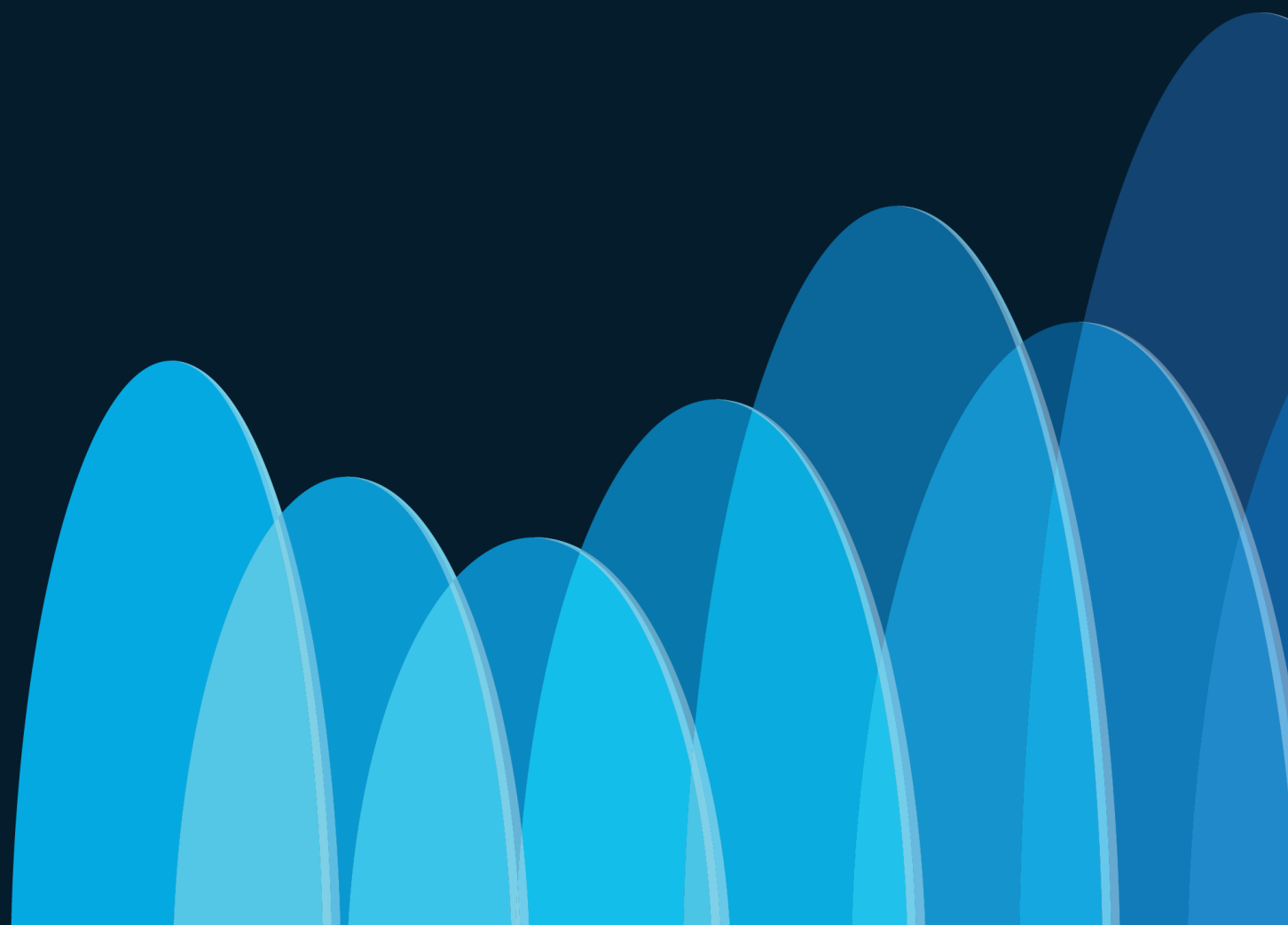
Understanding ACI security...

External Connectivity...

Increasing Security...

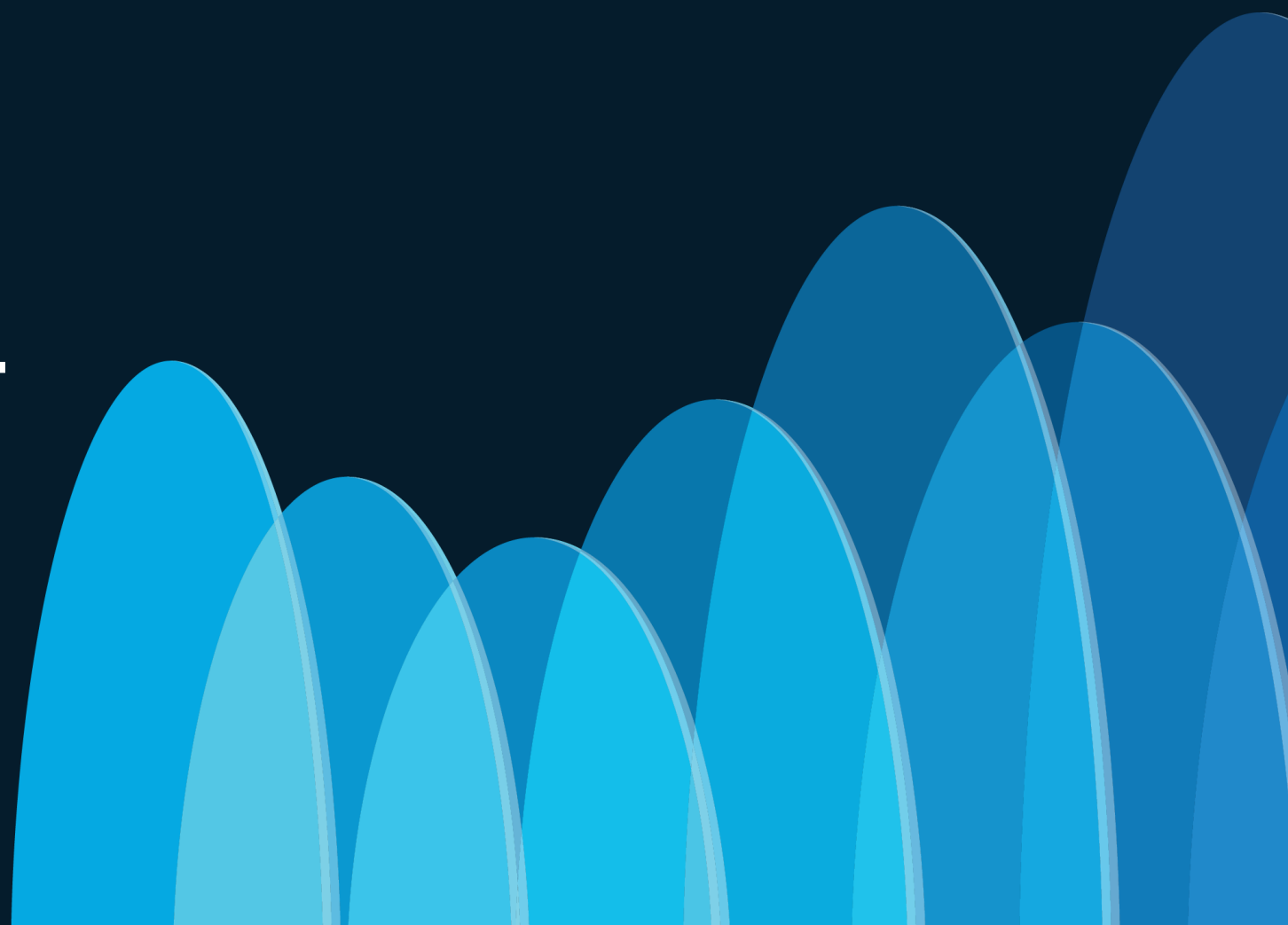
Automation Blueprints...

Wrapping up...



cisco Live!

Allowing open communication...



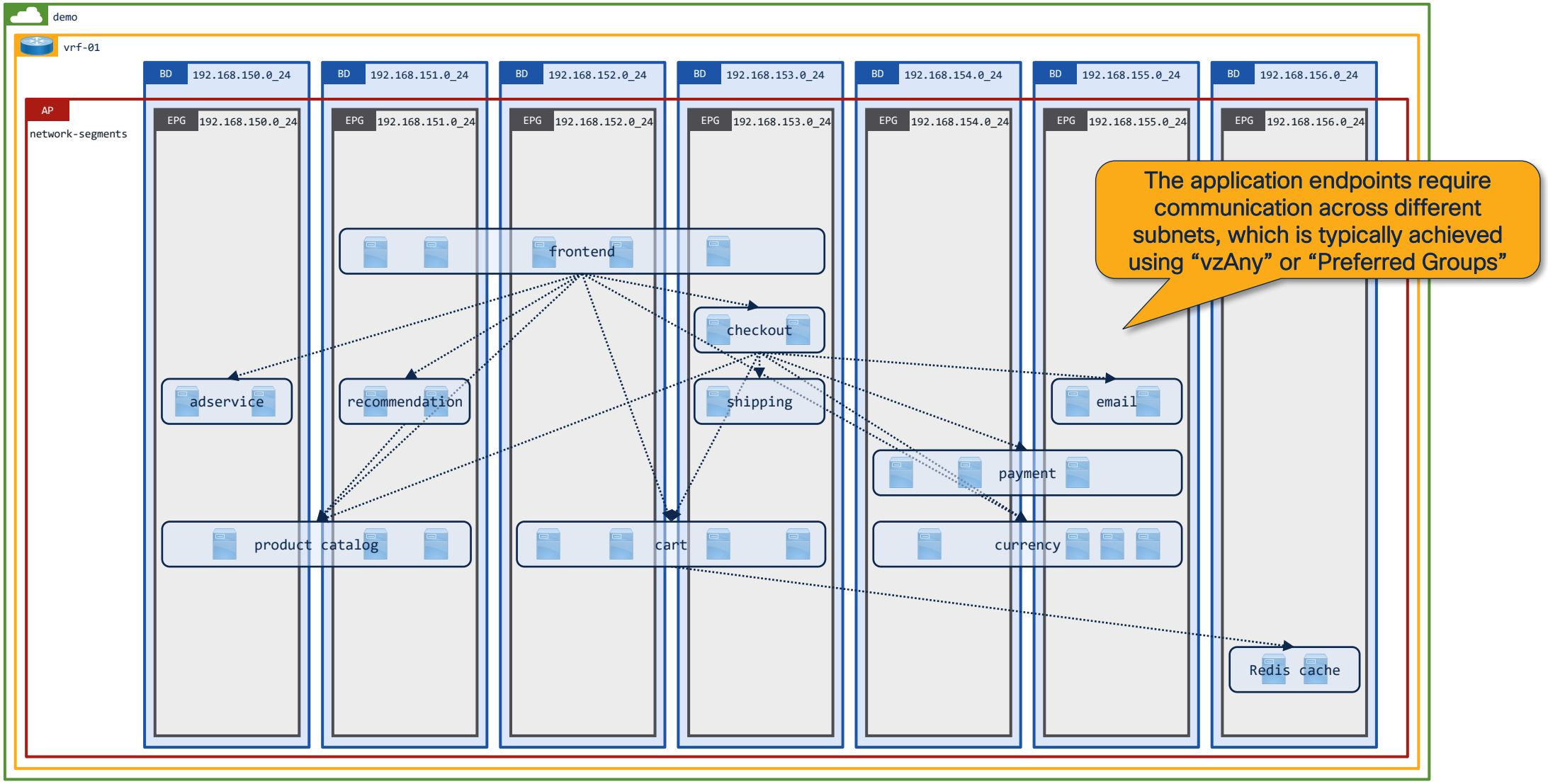
There are four options to allow open communication...

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

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

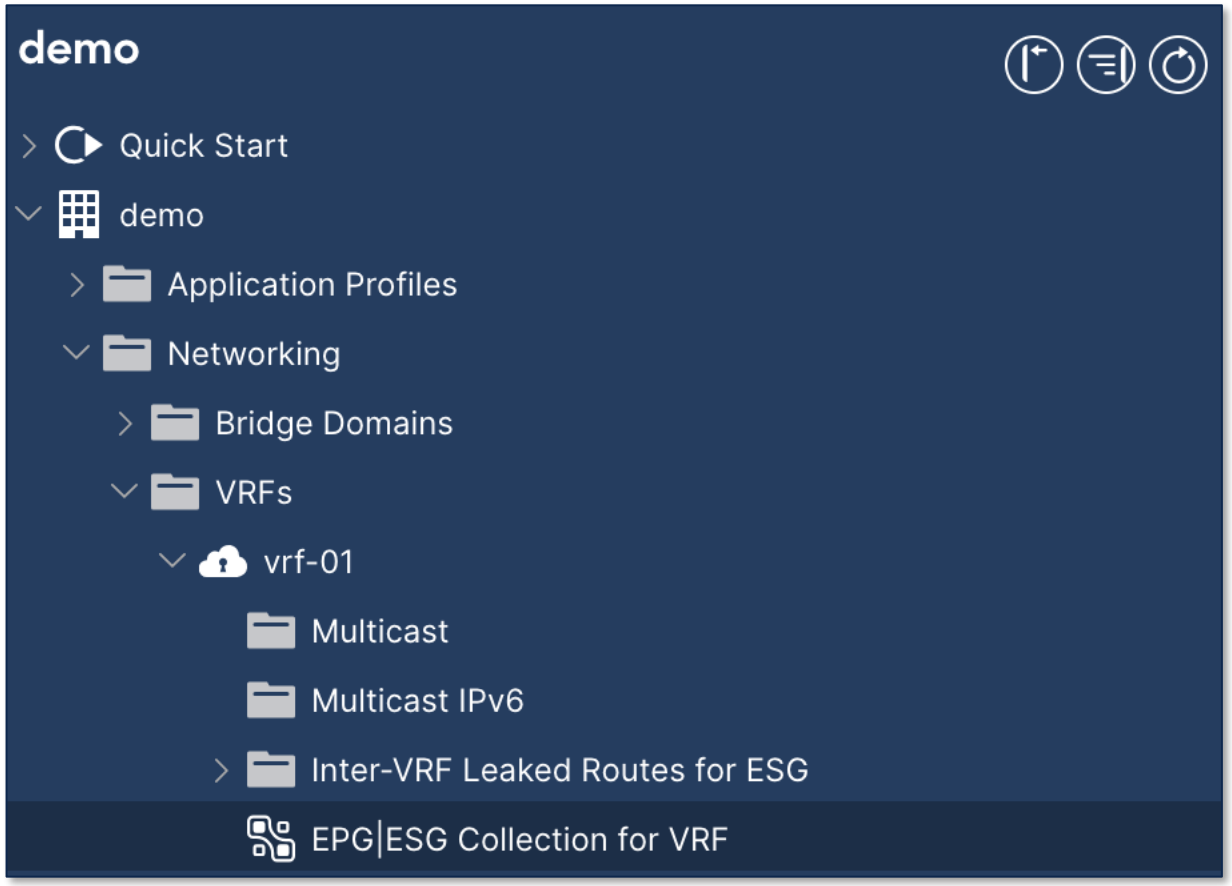
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Existing applications typically require unrestricted communication



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

vzAny



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

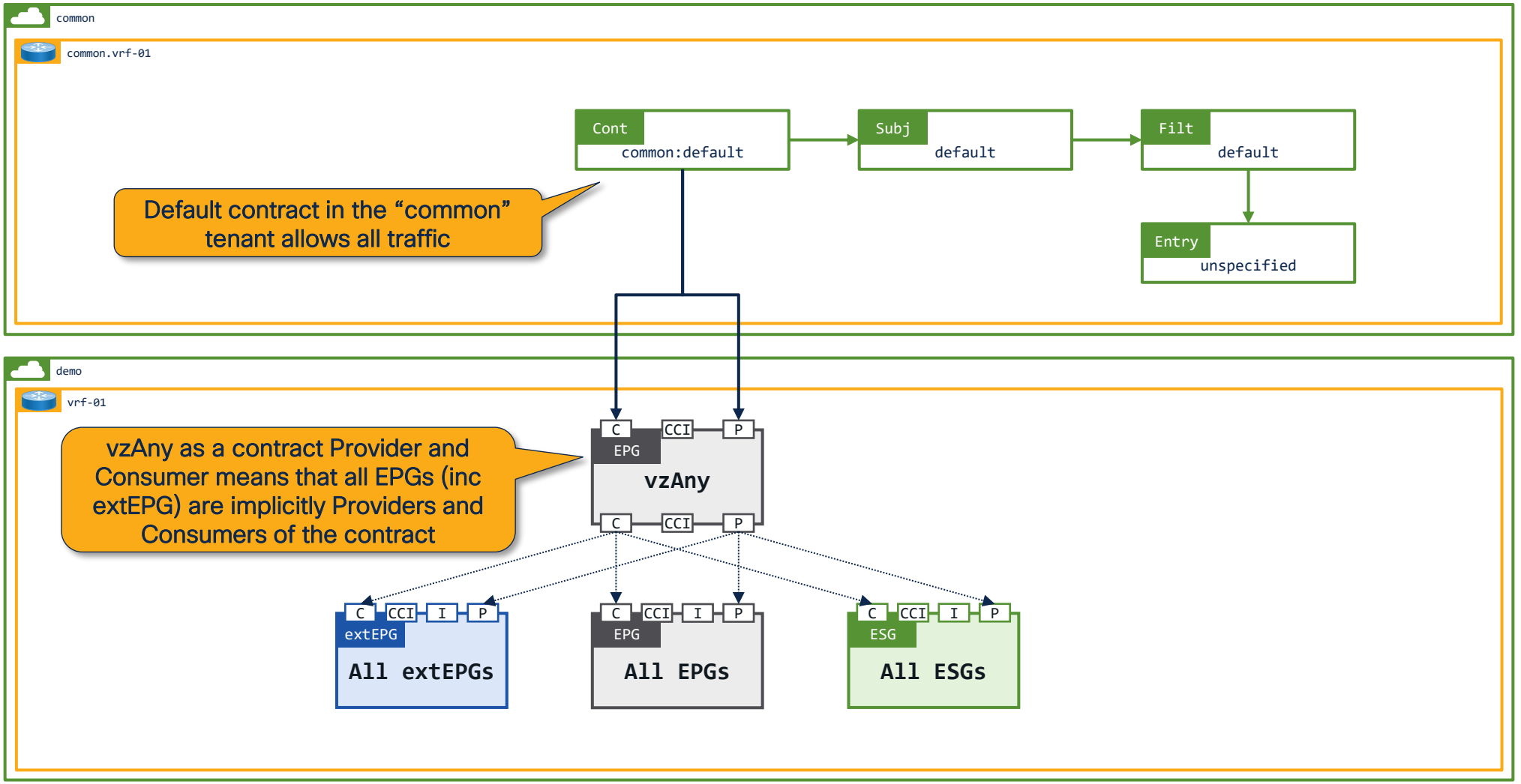
The great thing about vzAny provide/consume is that it allows open communication between all endpoints...

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

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

vzAny Operation – Consumer and Provider

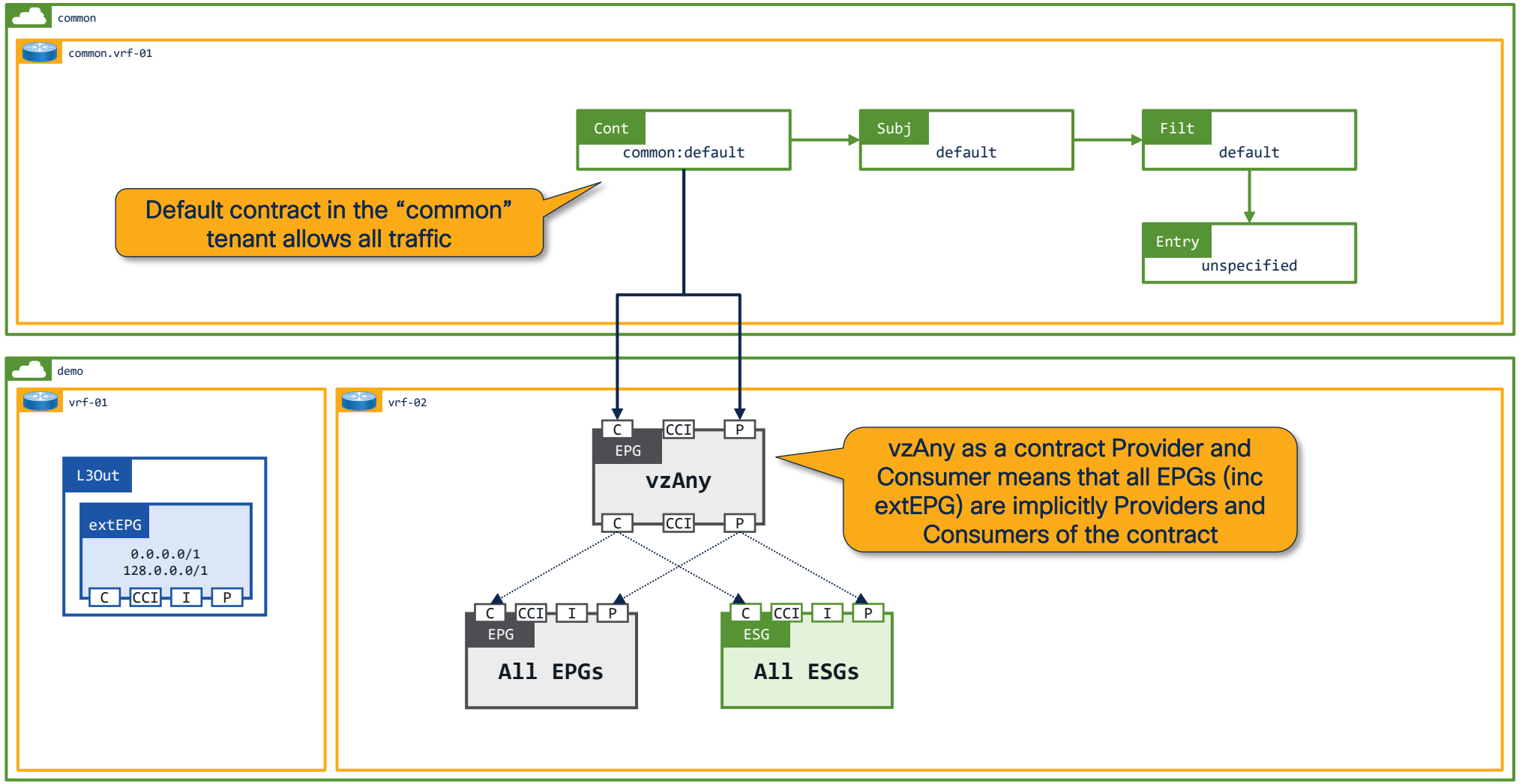
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_KB_Use_vzAny_to_AutomaticallyApplyCommunicationRules_toEPGs.html



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

vzAny Operation – Consumer and Provider

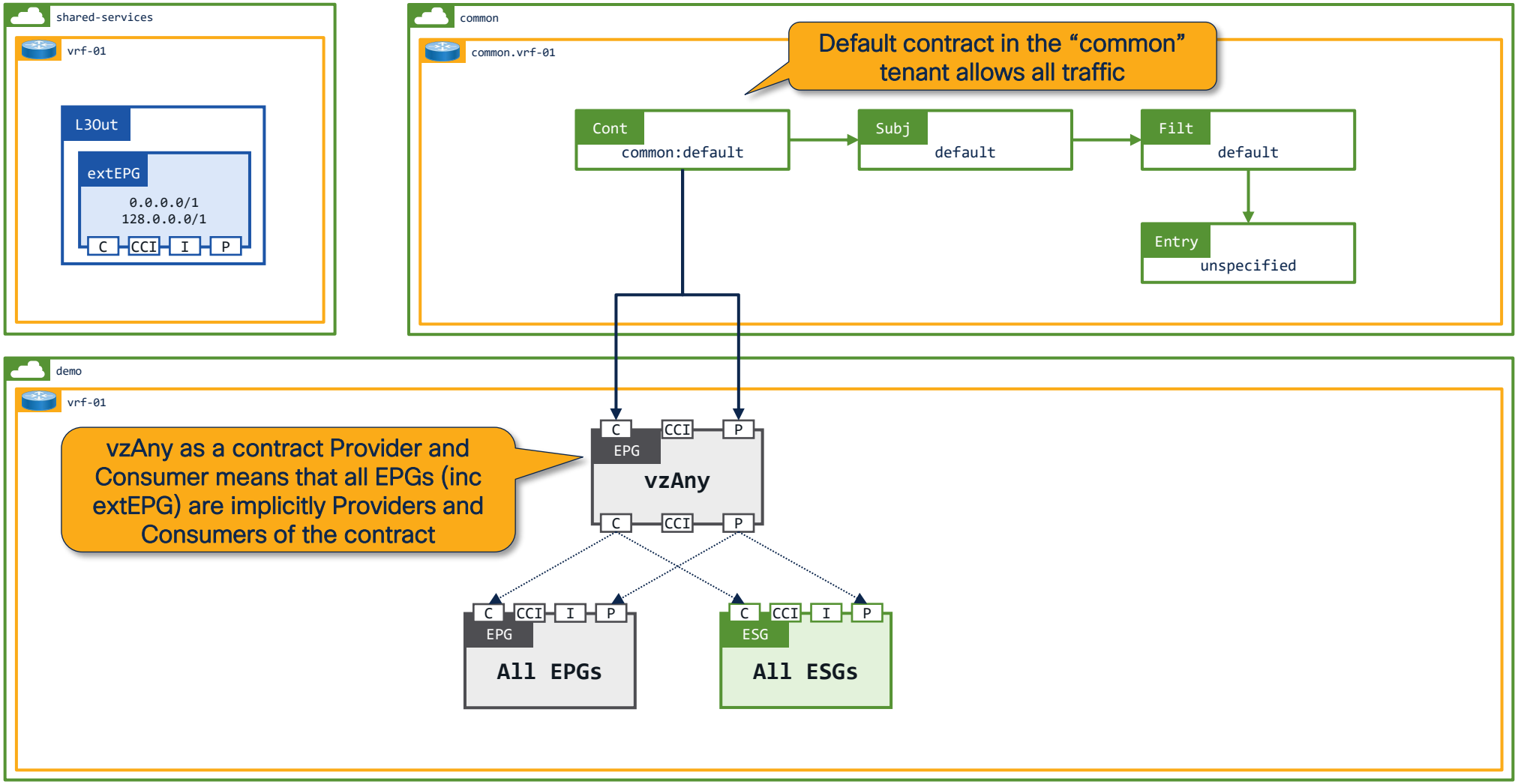
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_KB_Use_vzAny_to_AutomaticallyApplyCommunicationRules_toEPGs.html



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

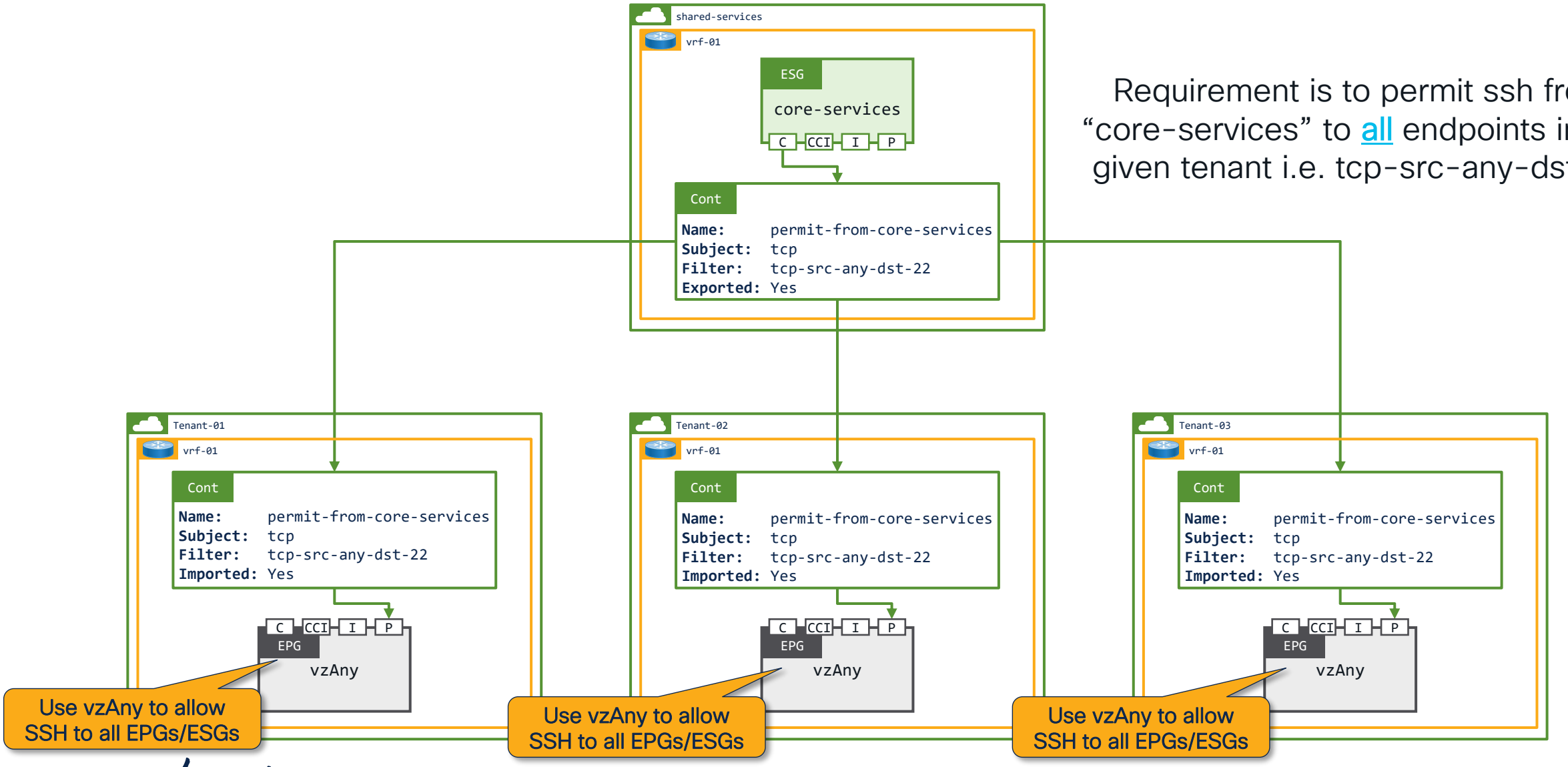
vzAny Operation – Consumer and Provider

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



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

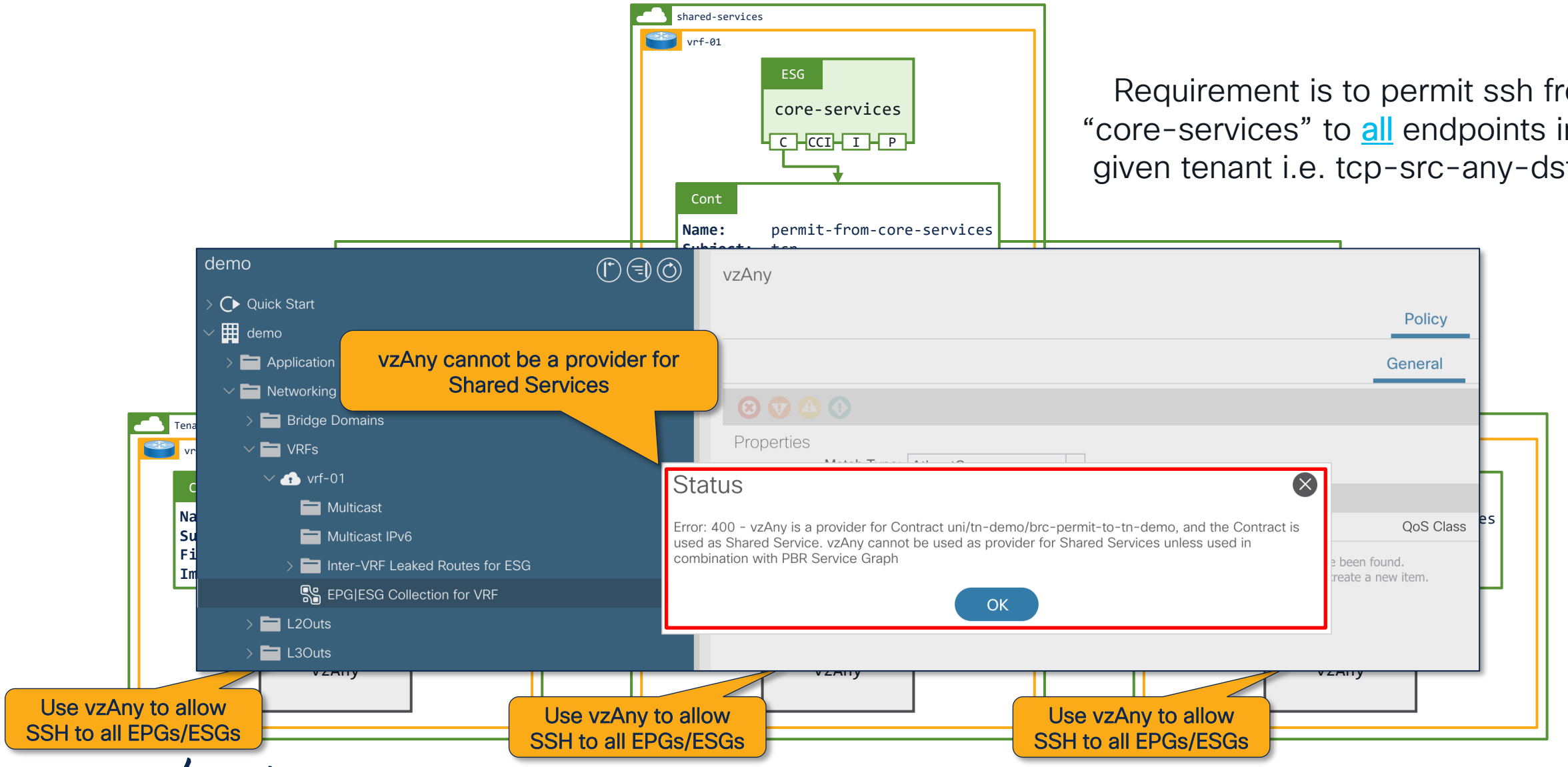
vzAny cannot be a Provider for Shared Services



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

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

vzAny cannot be a Provider for Shared Services



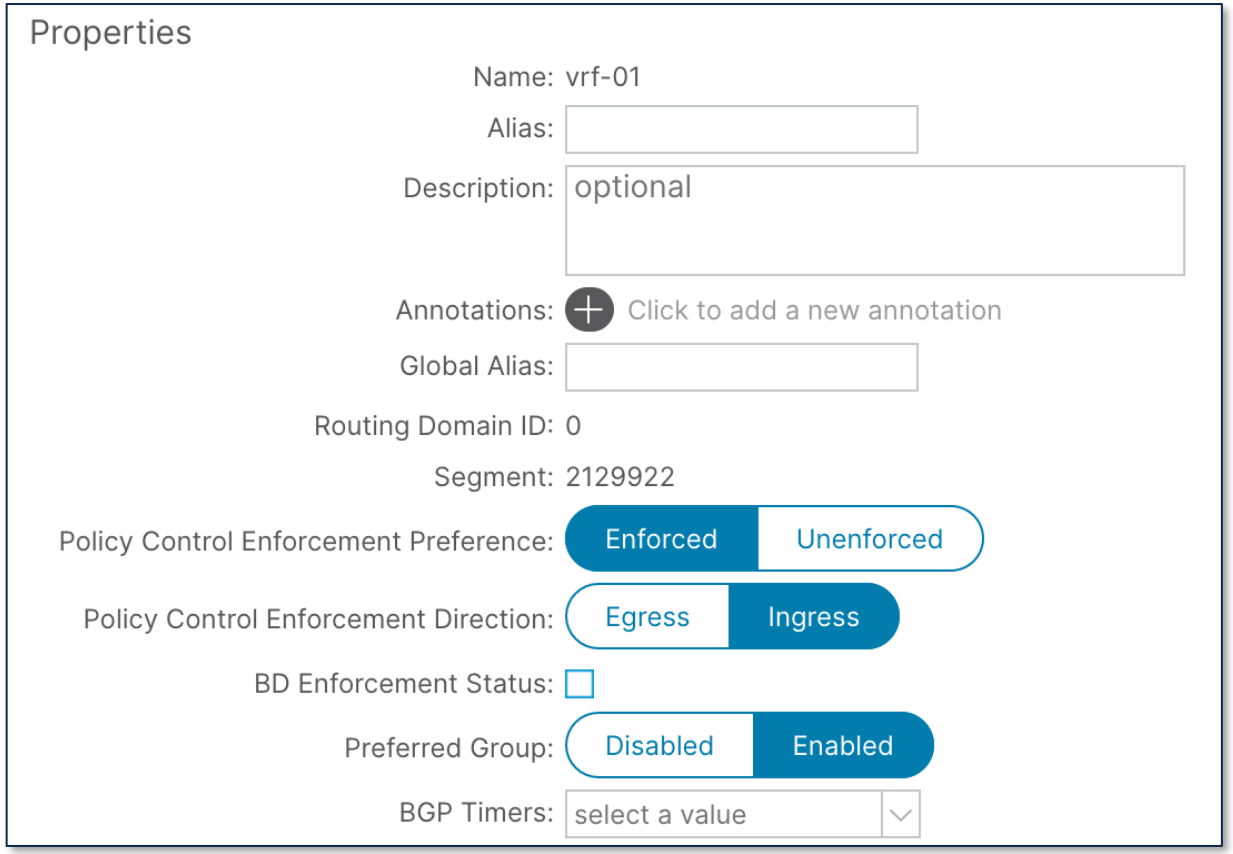
Requirement is to permit ssh from "core-services" to all endpoints in any given tenant i.e. tcp-src-any-dst-22

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

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

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

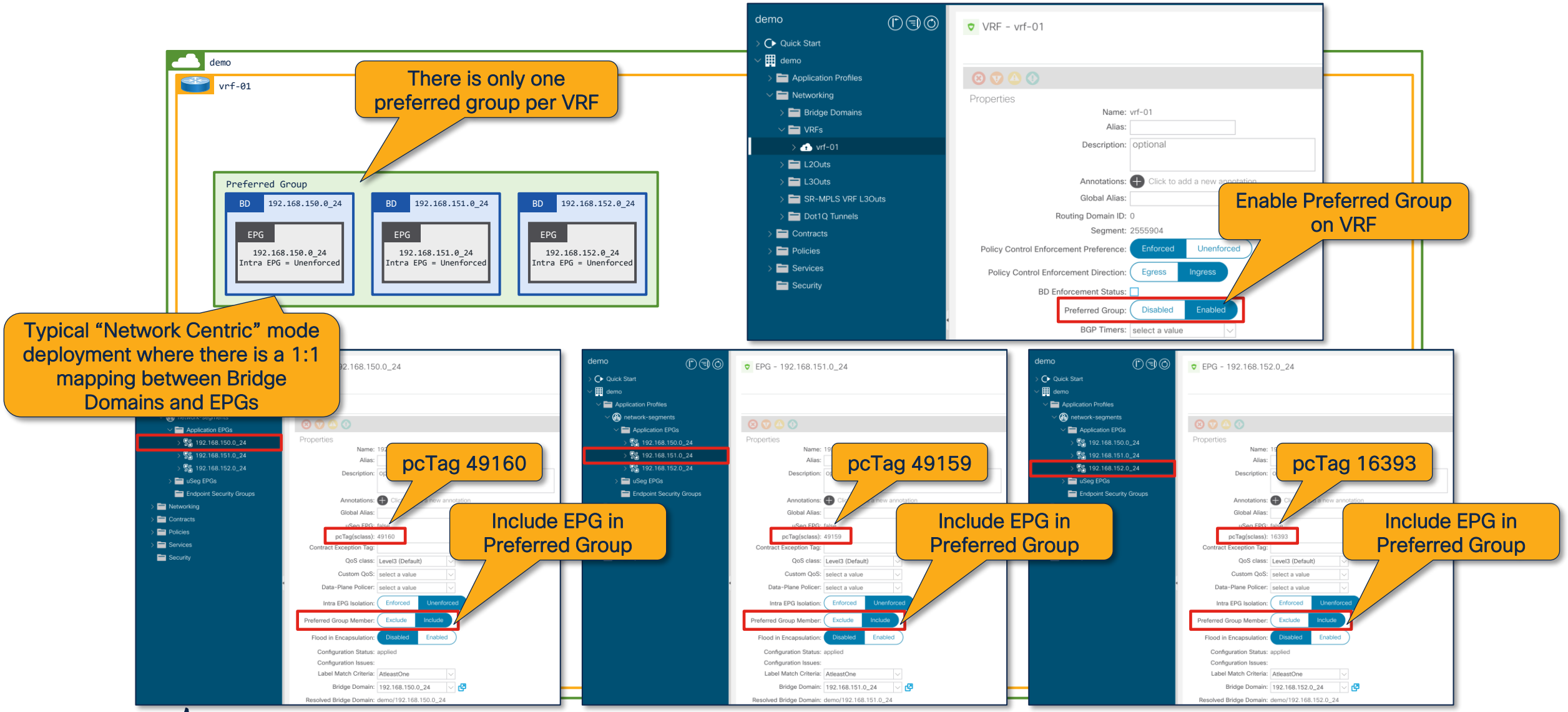
Preferred Groups



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

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



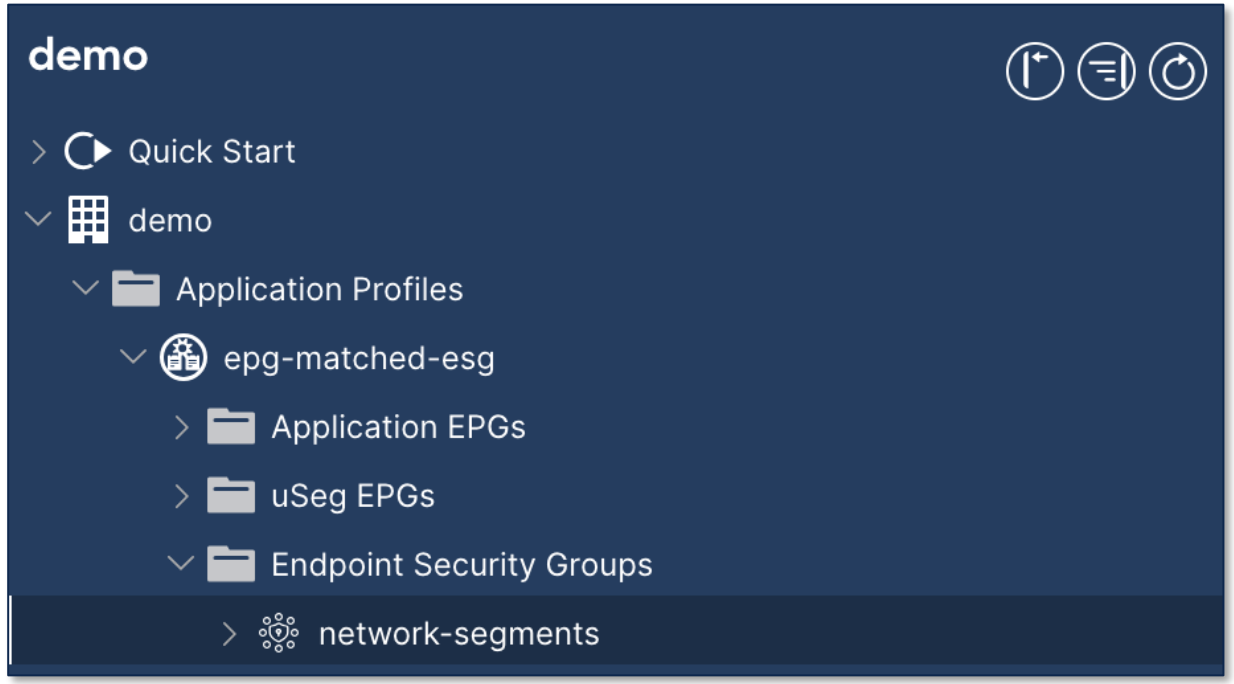
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

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

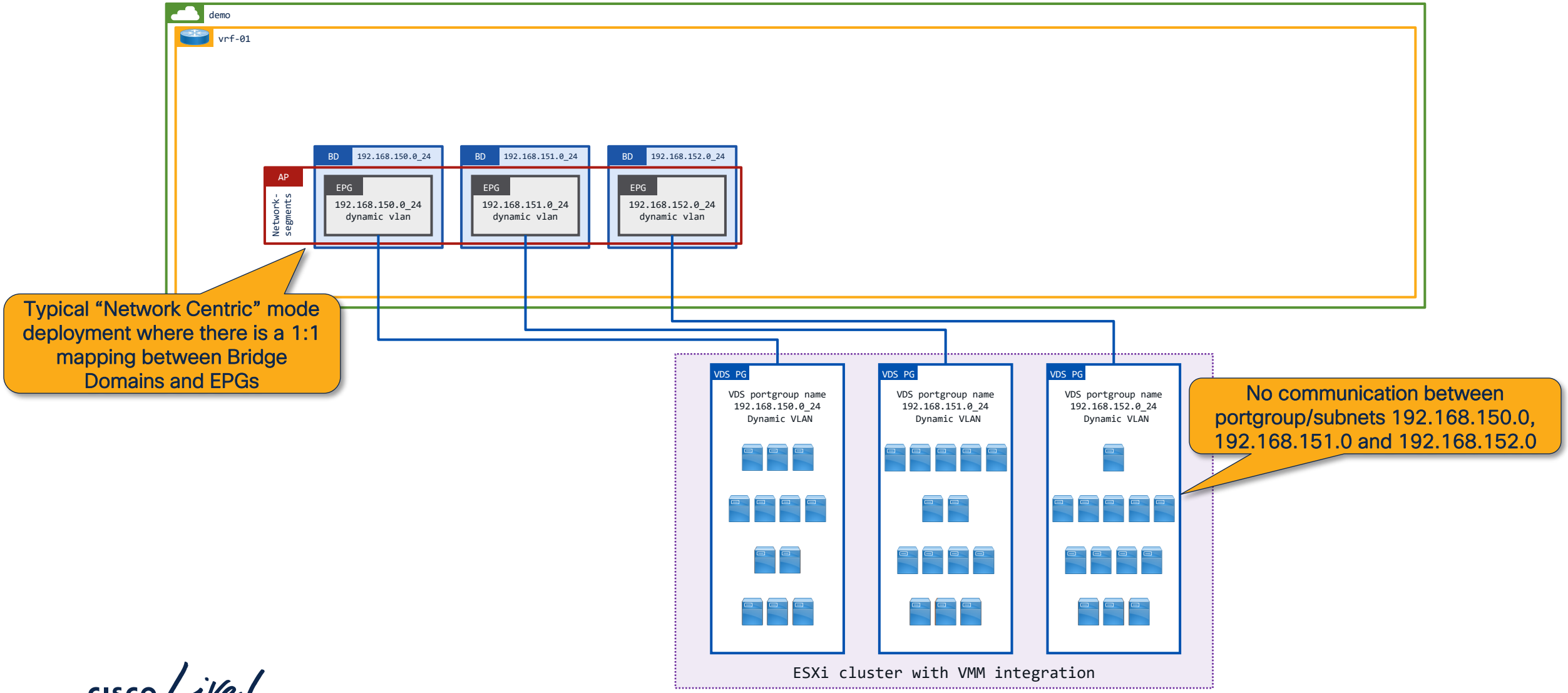
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

All EPGs mapped to a single ESG



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

Initial state: Isolated groups of workloads

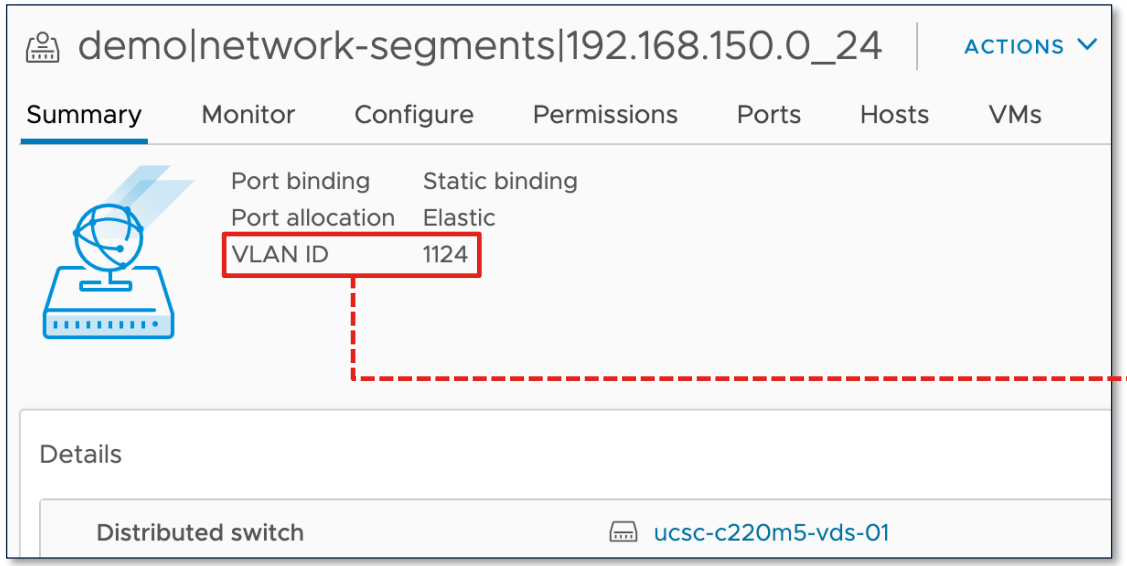


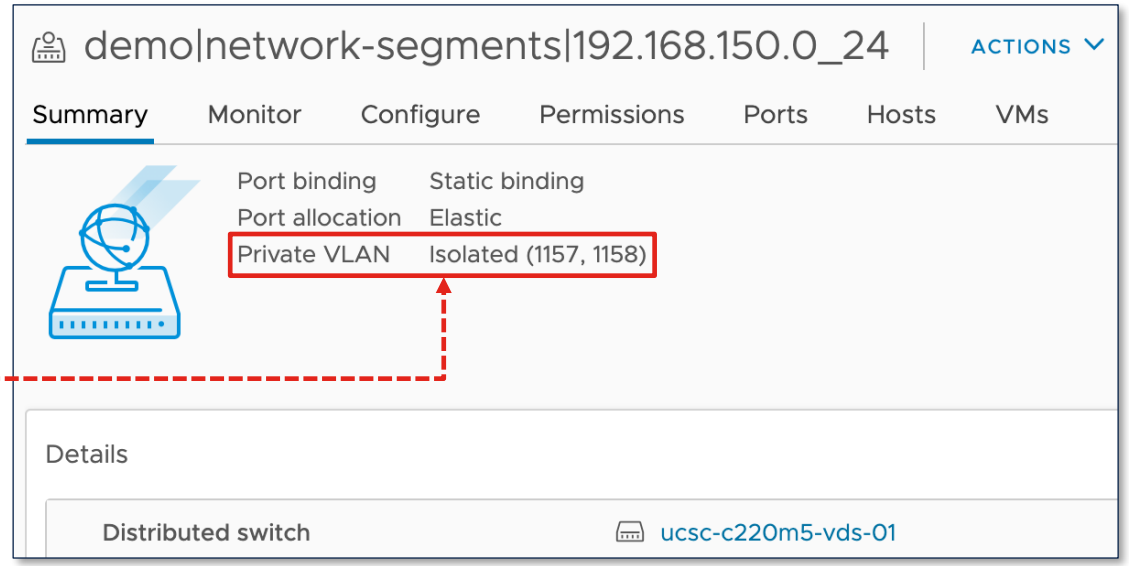
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

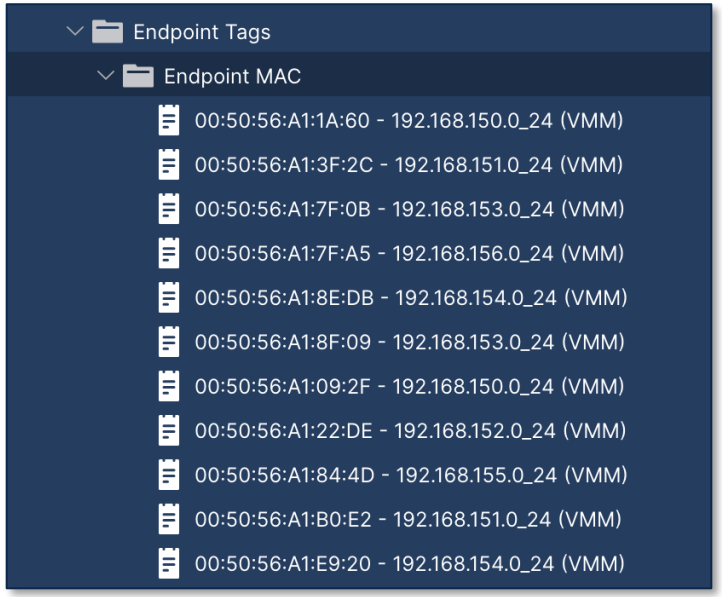
Enable Endpoint Security Groups

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

PVLAN and MAC Tagging

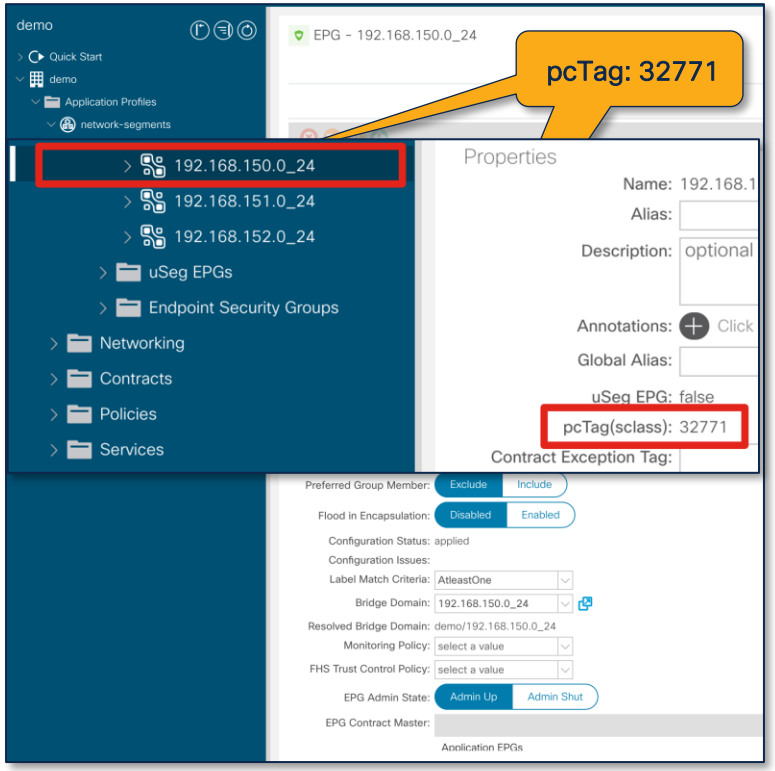


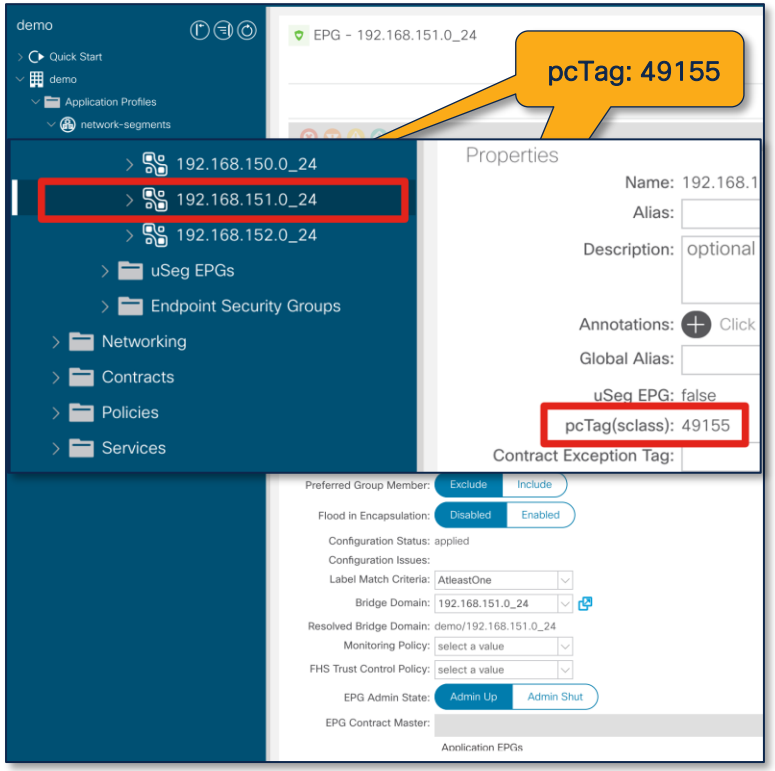


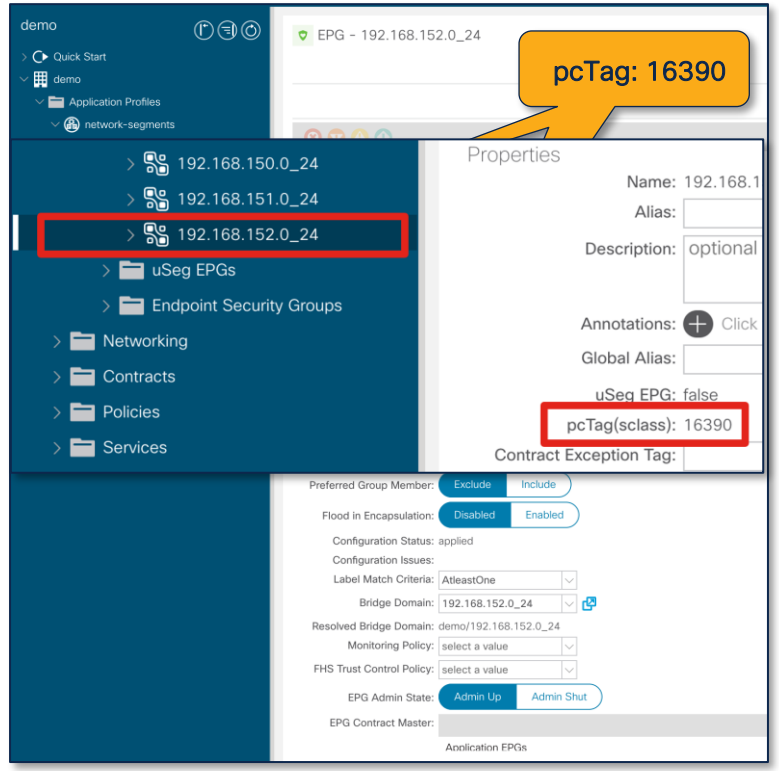


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Each EPG has a unique security Tag (pcTag)







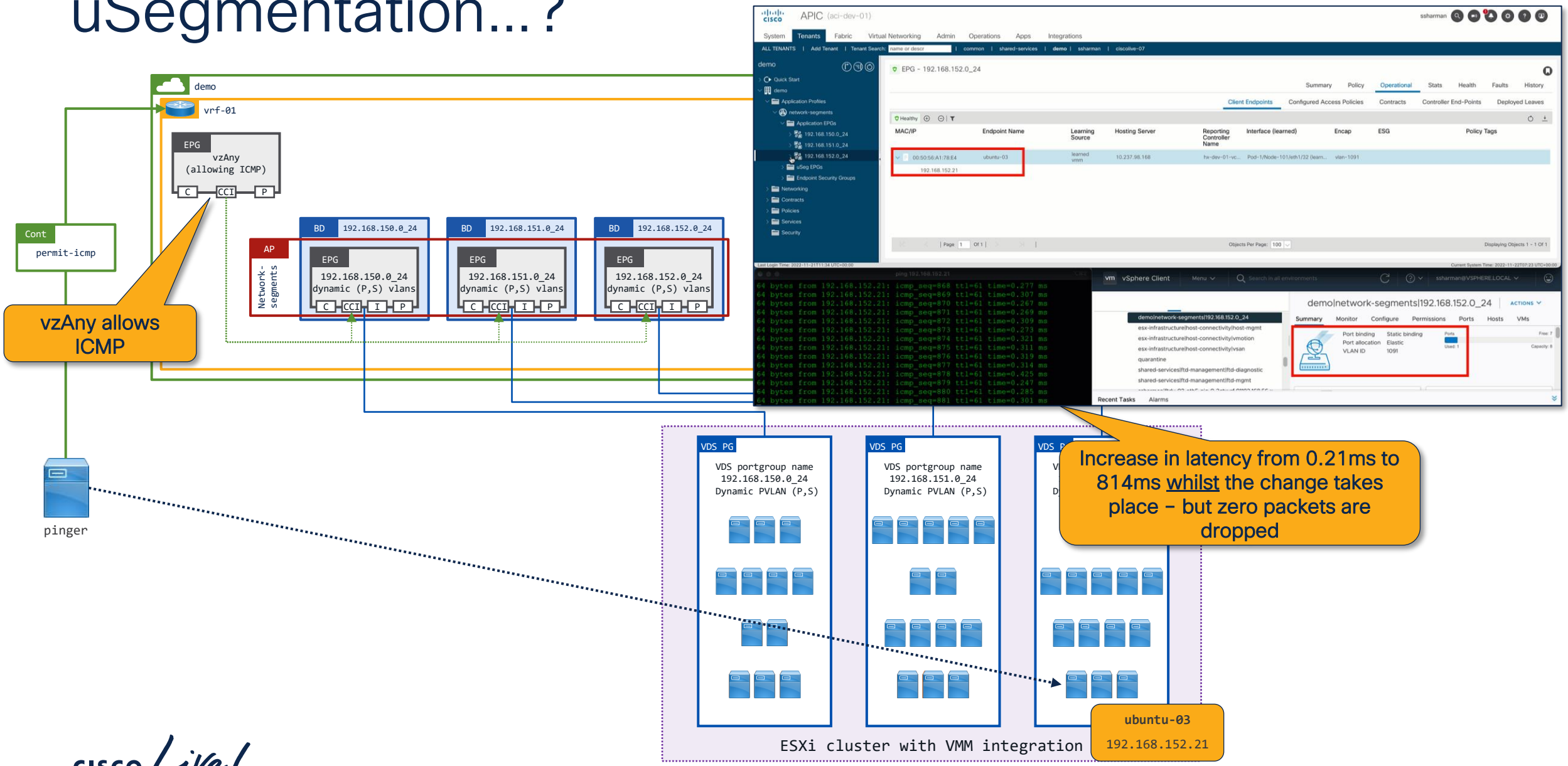
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

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

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

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

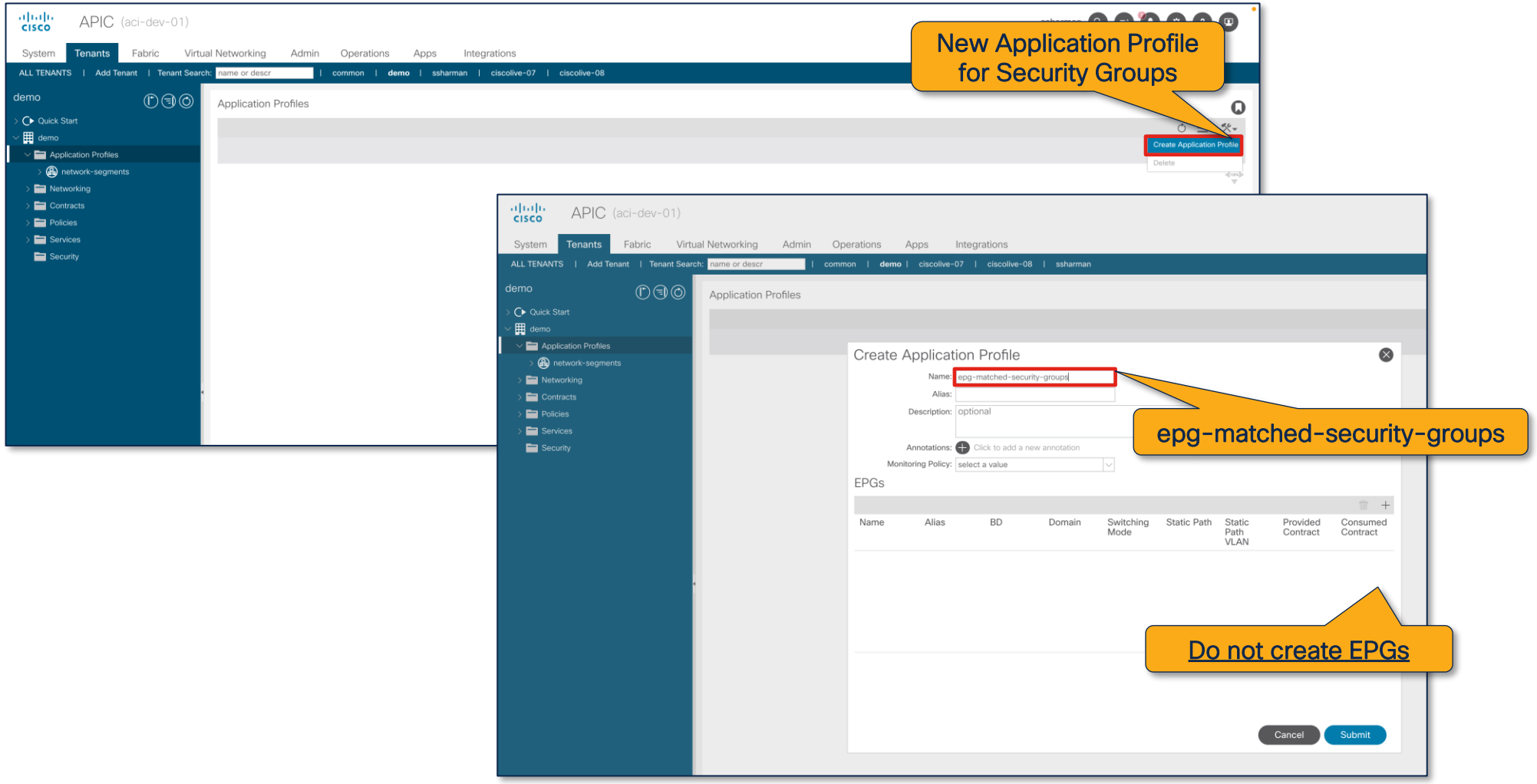


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Let’s map our EPGs to an ESG…

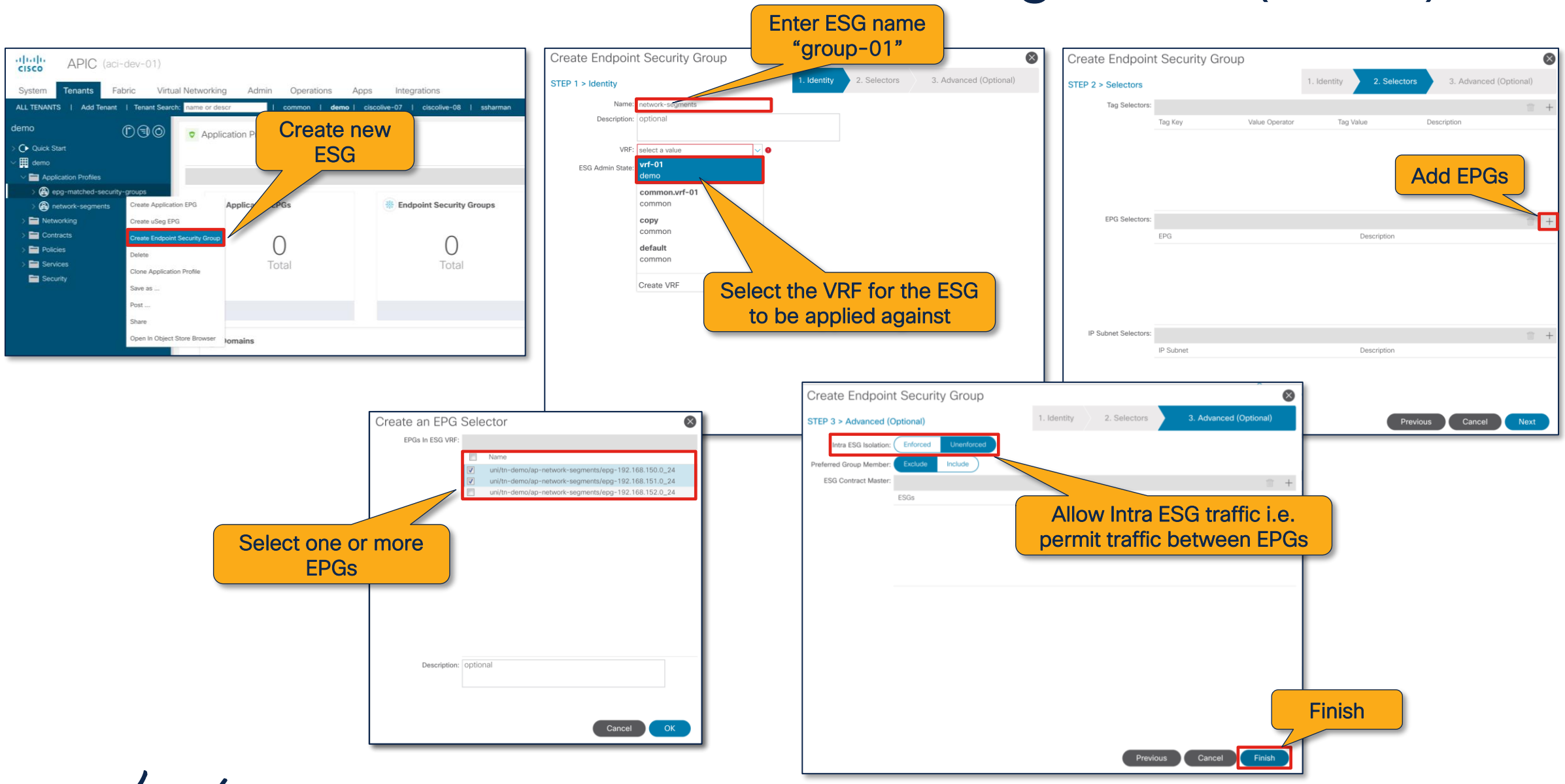
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Create an Application Profile for Security Groups



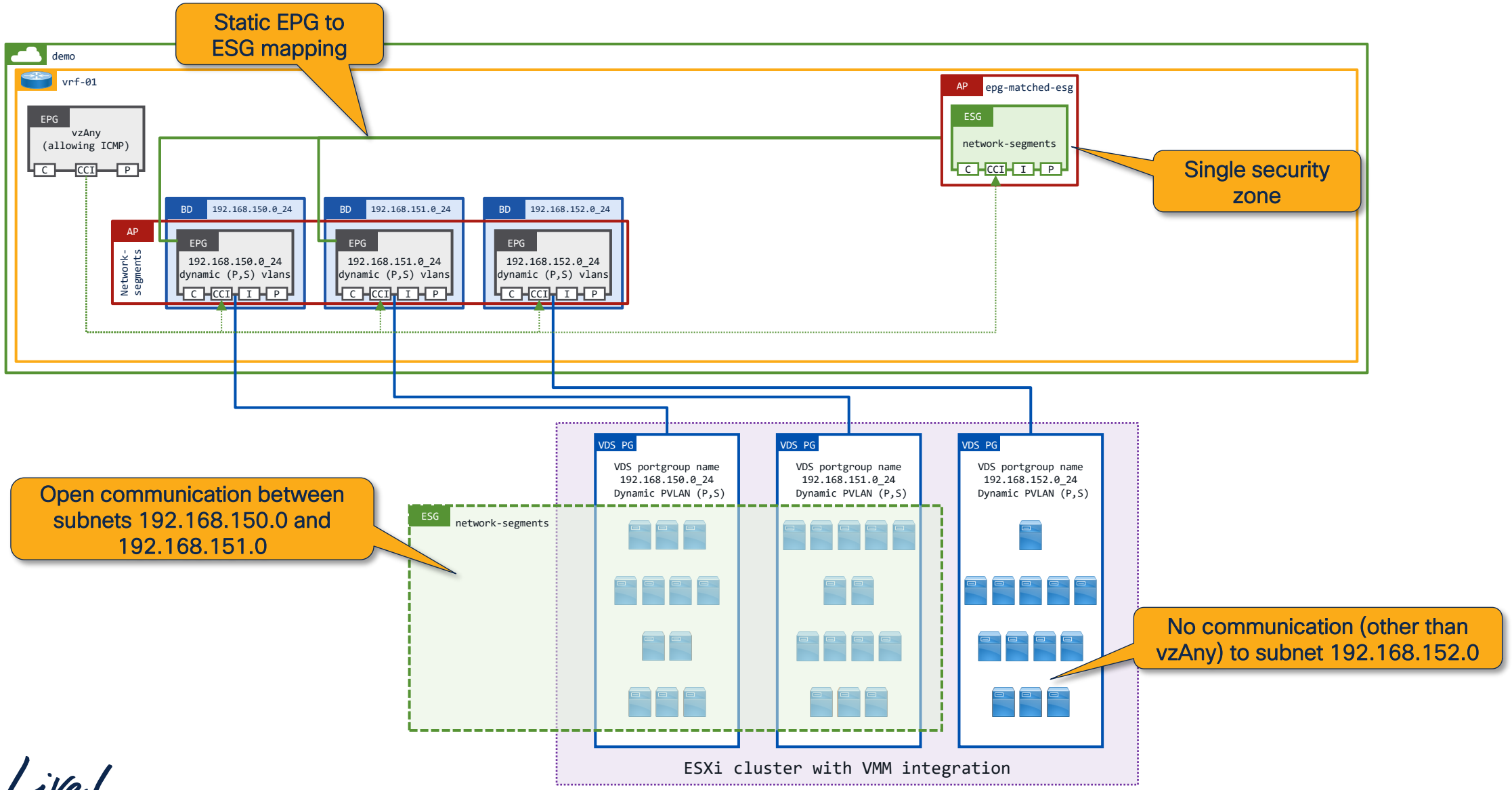
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Create a new ESG for Network Segments (EPGs)



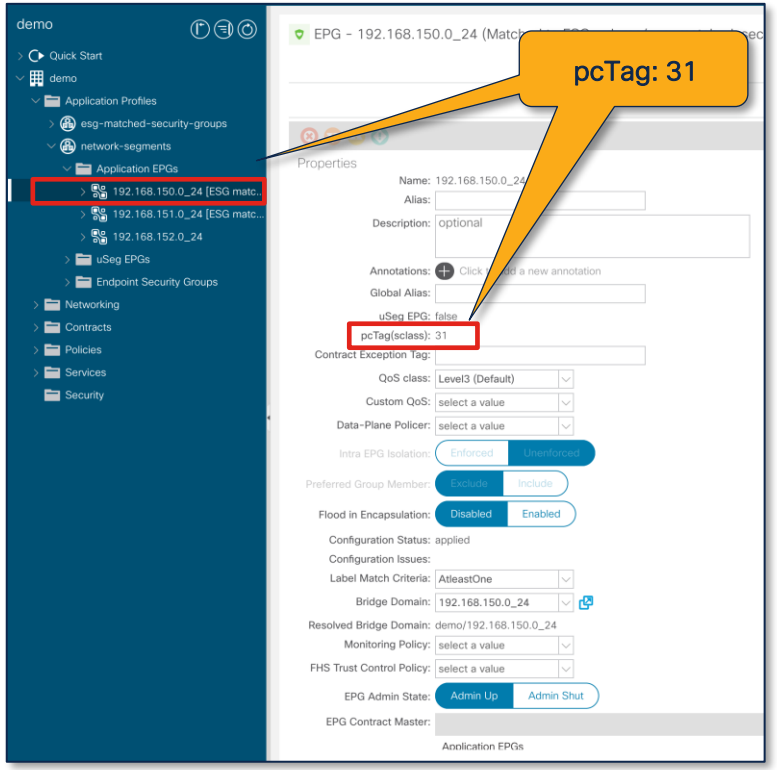
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

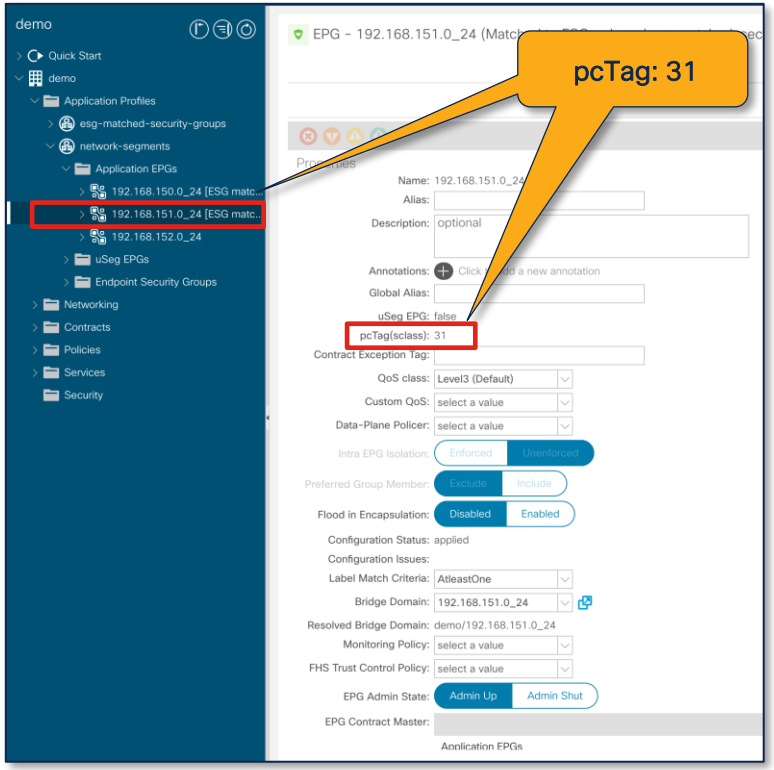
Open communication within the ESG...

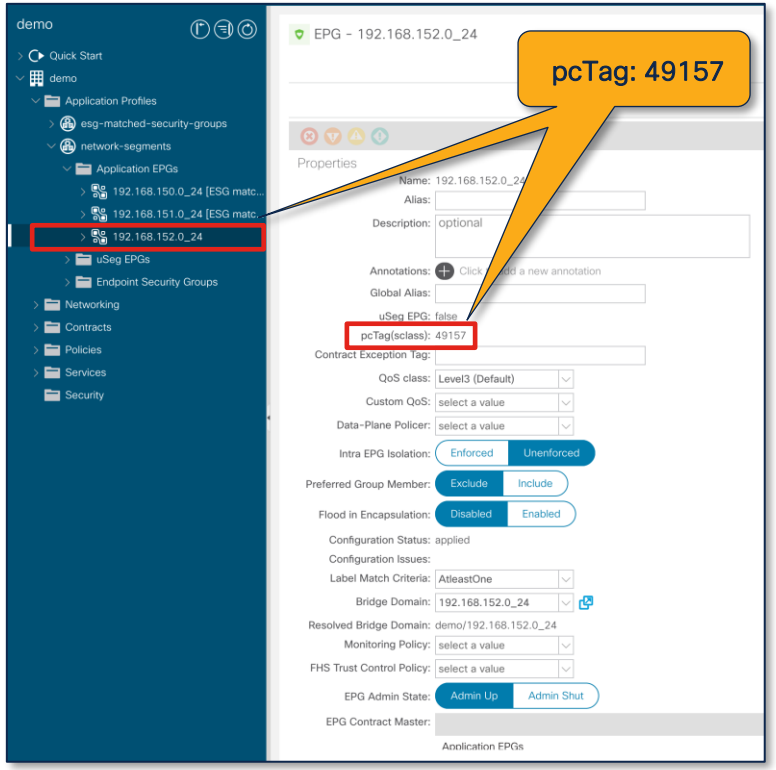


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Matched EPGs now classified with a common pcTag





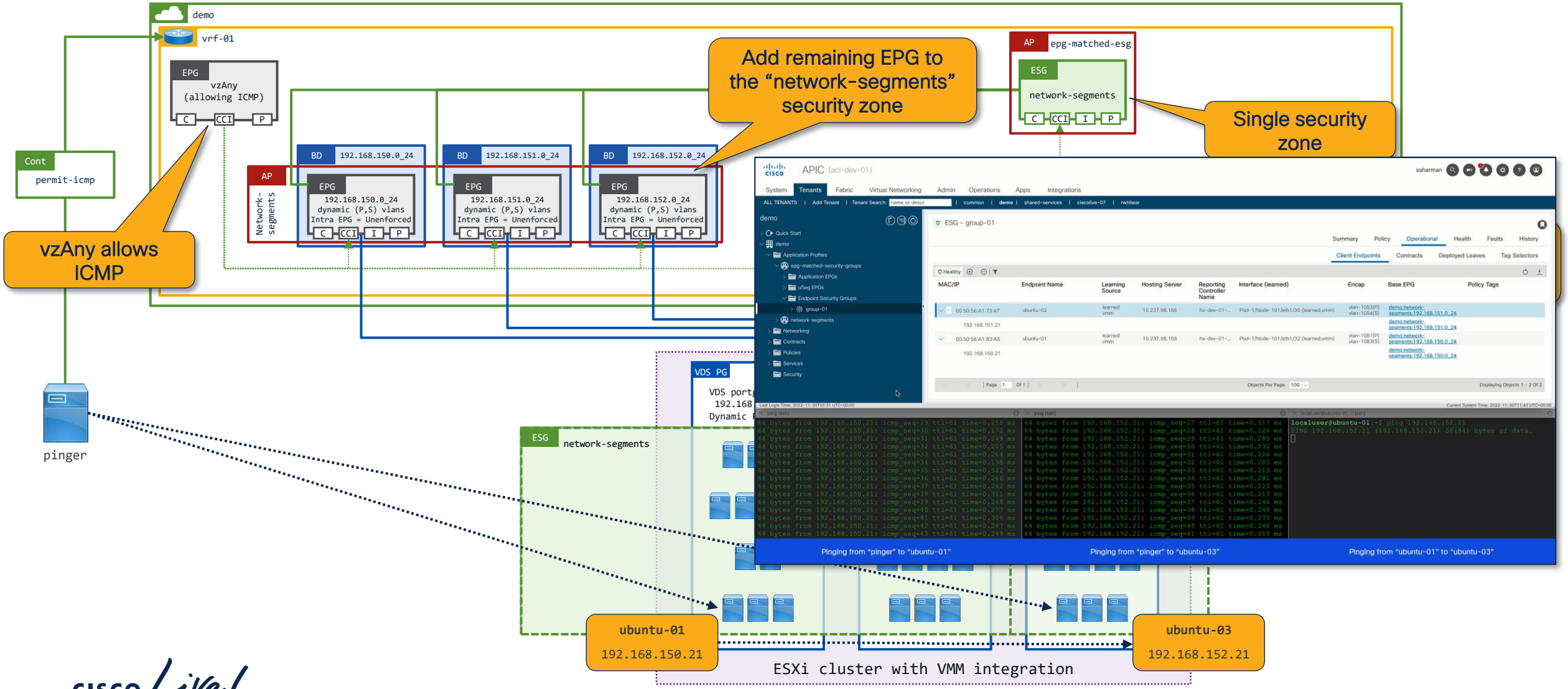


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Let’s consider any impact to traffic when adding the remaining EPG to the Security Group…

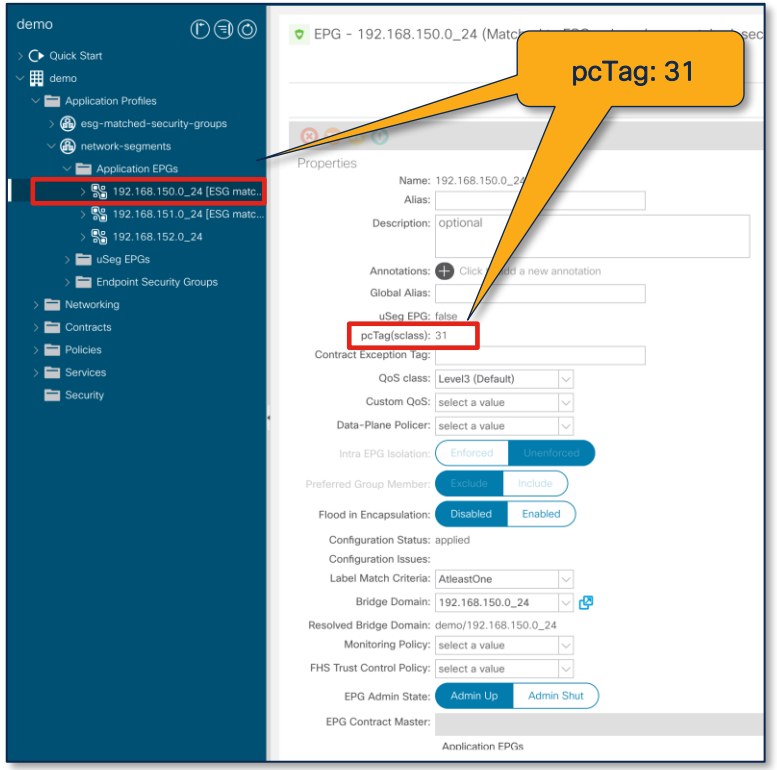
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

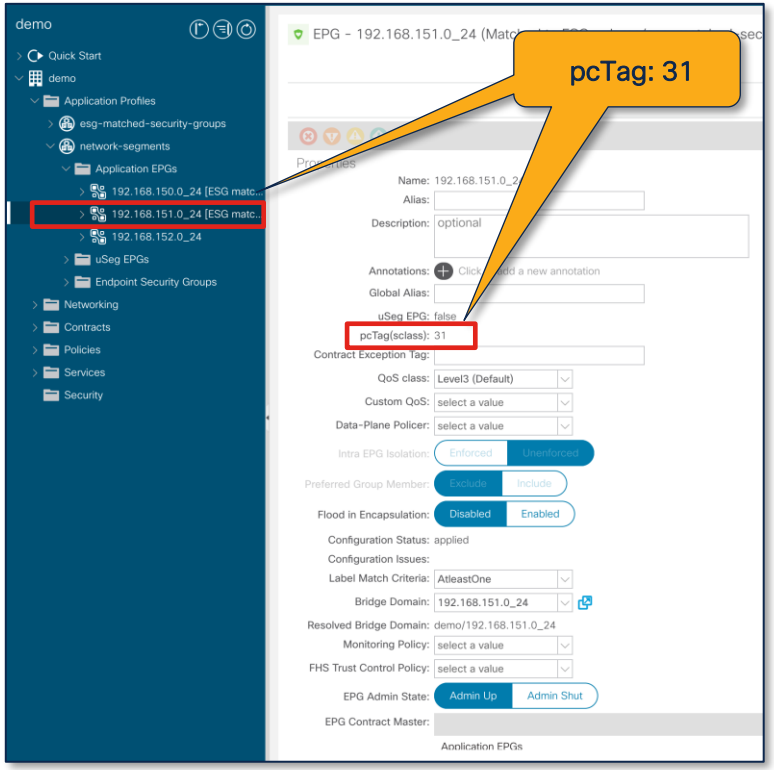
Add remaining EPG to Single Security Zone

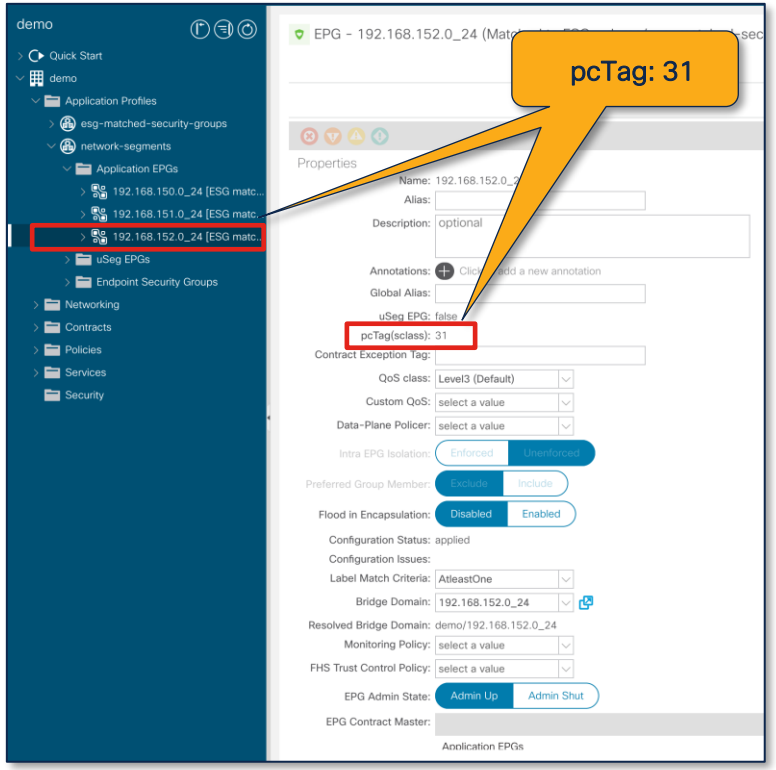


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

All EPGs now classified with a common pcTag







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

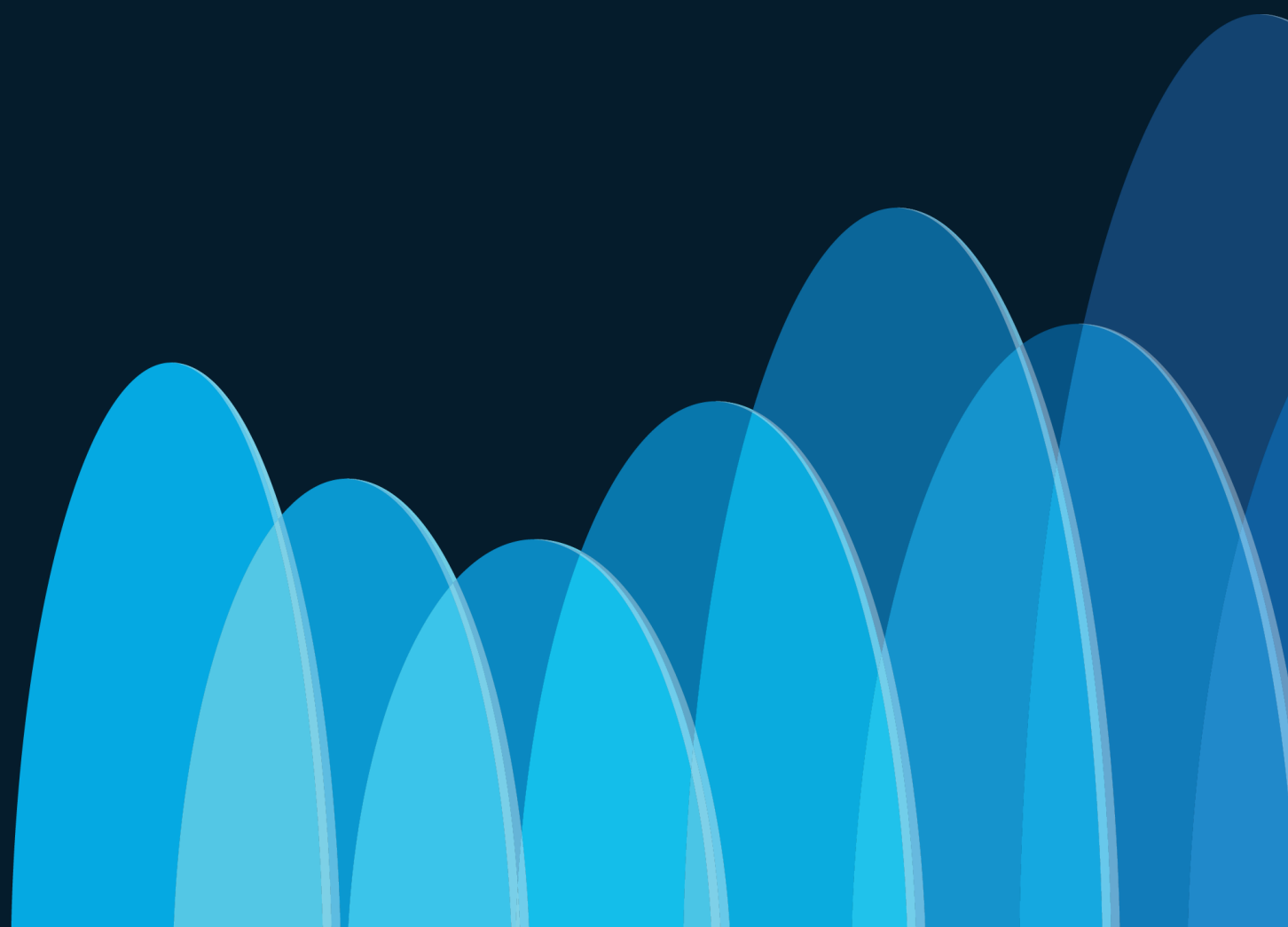
Benefits of EPG to ESG Mapping

- 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

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

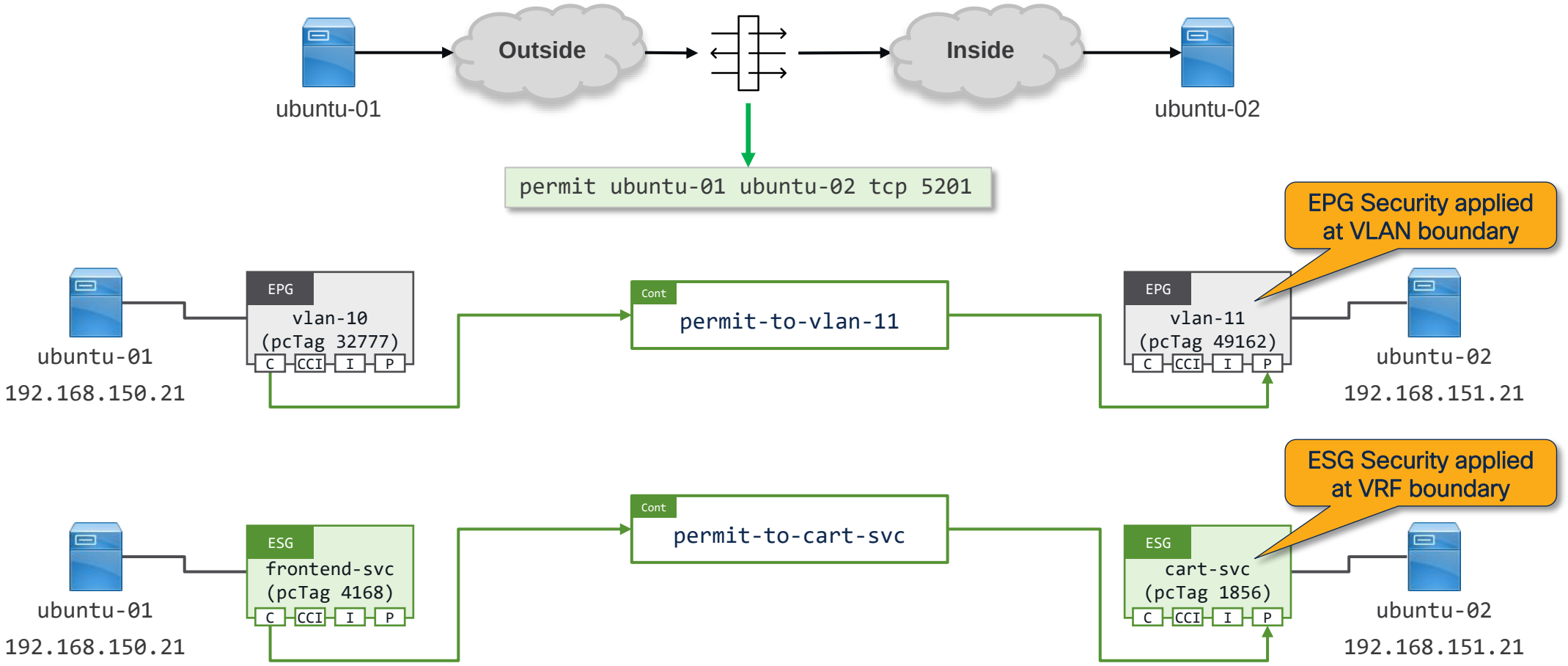
Allowing restricted communication...



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

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

How do contracts work...?



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

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

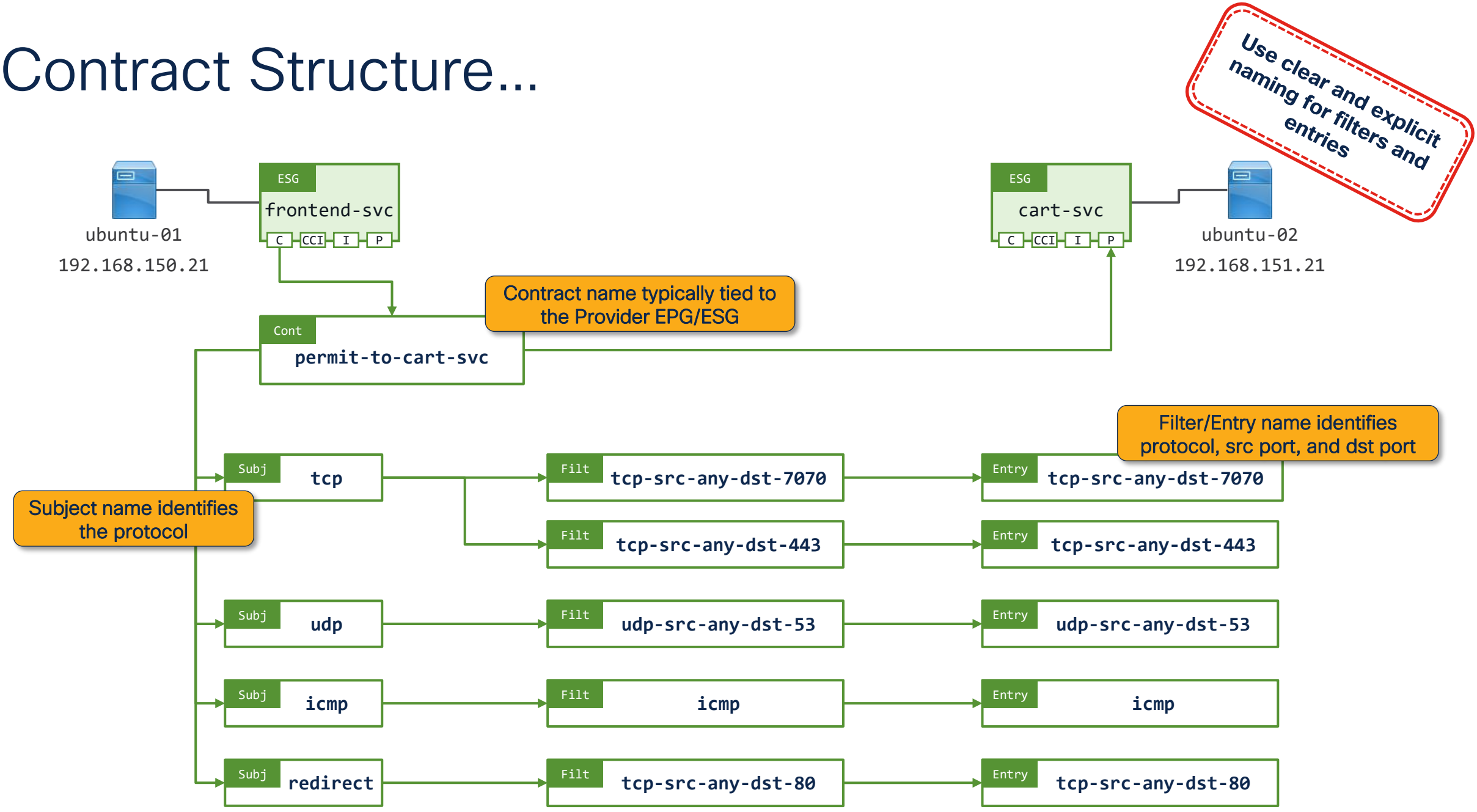
Consumer and Provider relationships are there to help you visualize the traffic flow direction

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

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

Contract Structure...

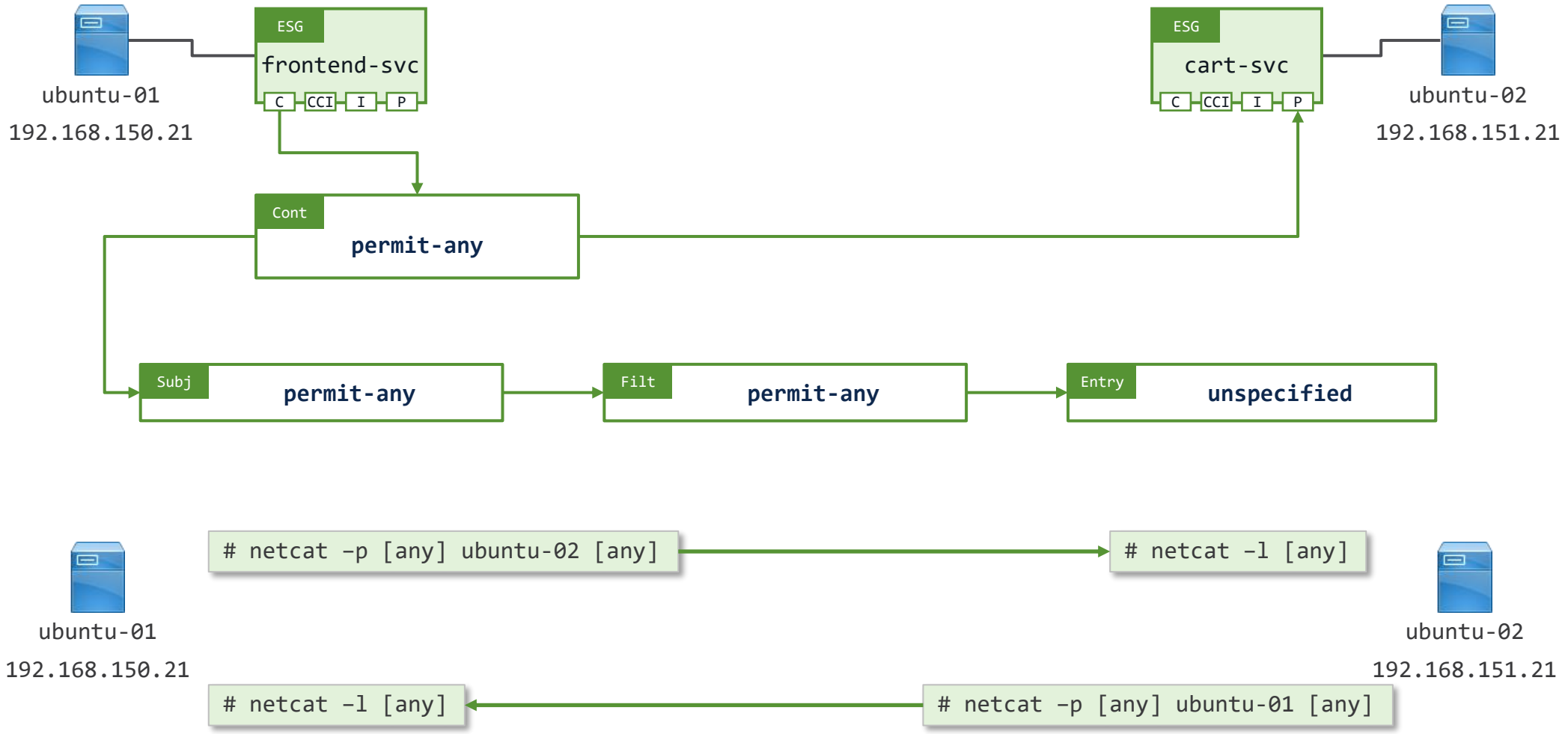


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Who hasn’t simply done this...

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

permit any/any

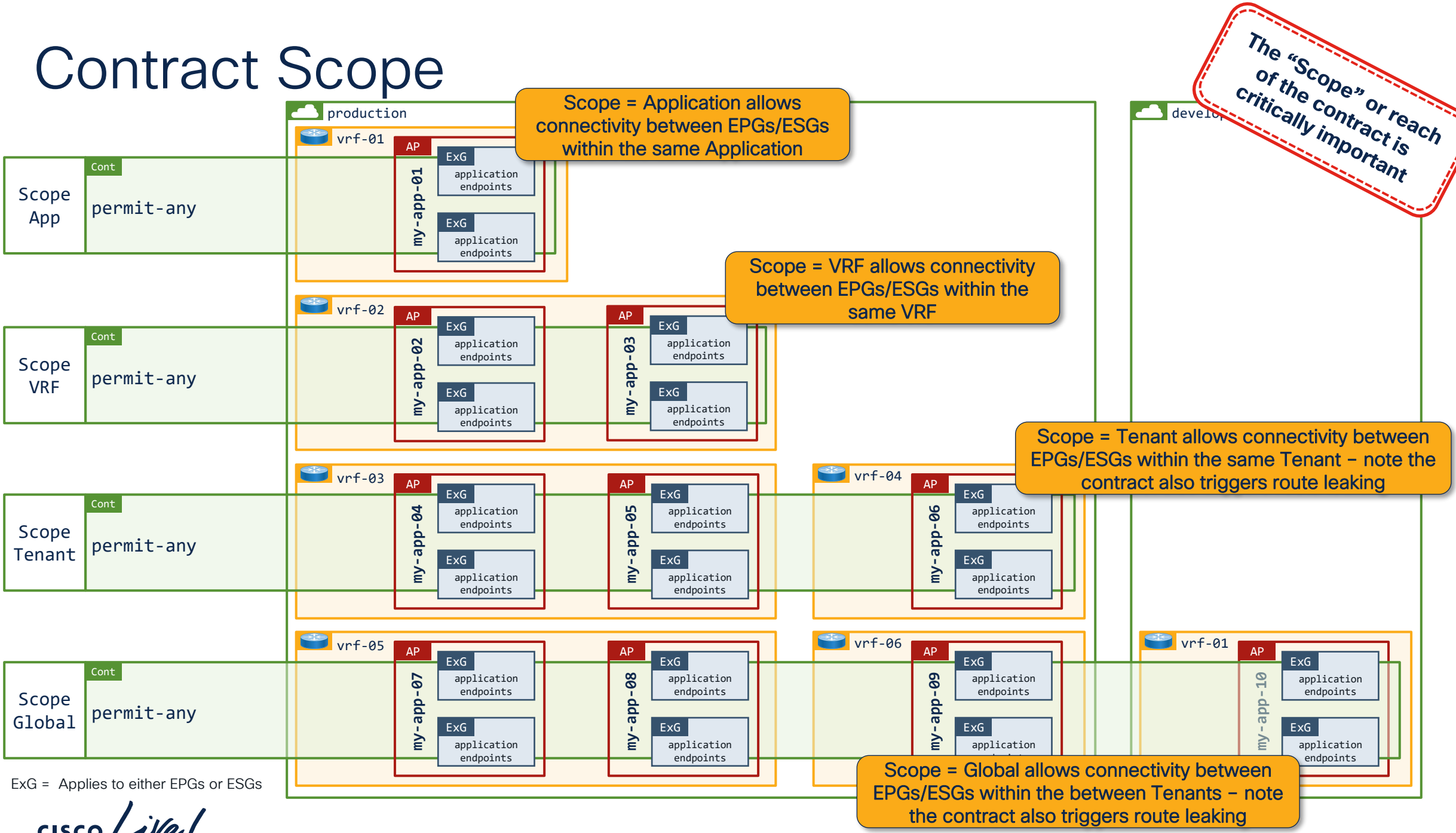


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Contracts also trigger route leaking for EPGs...

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

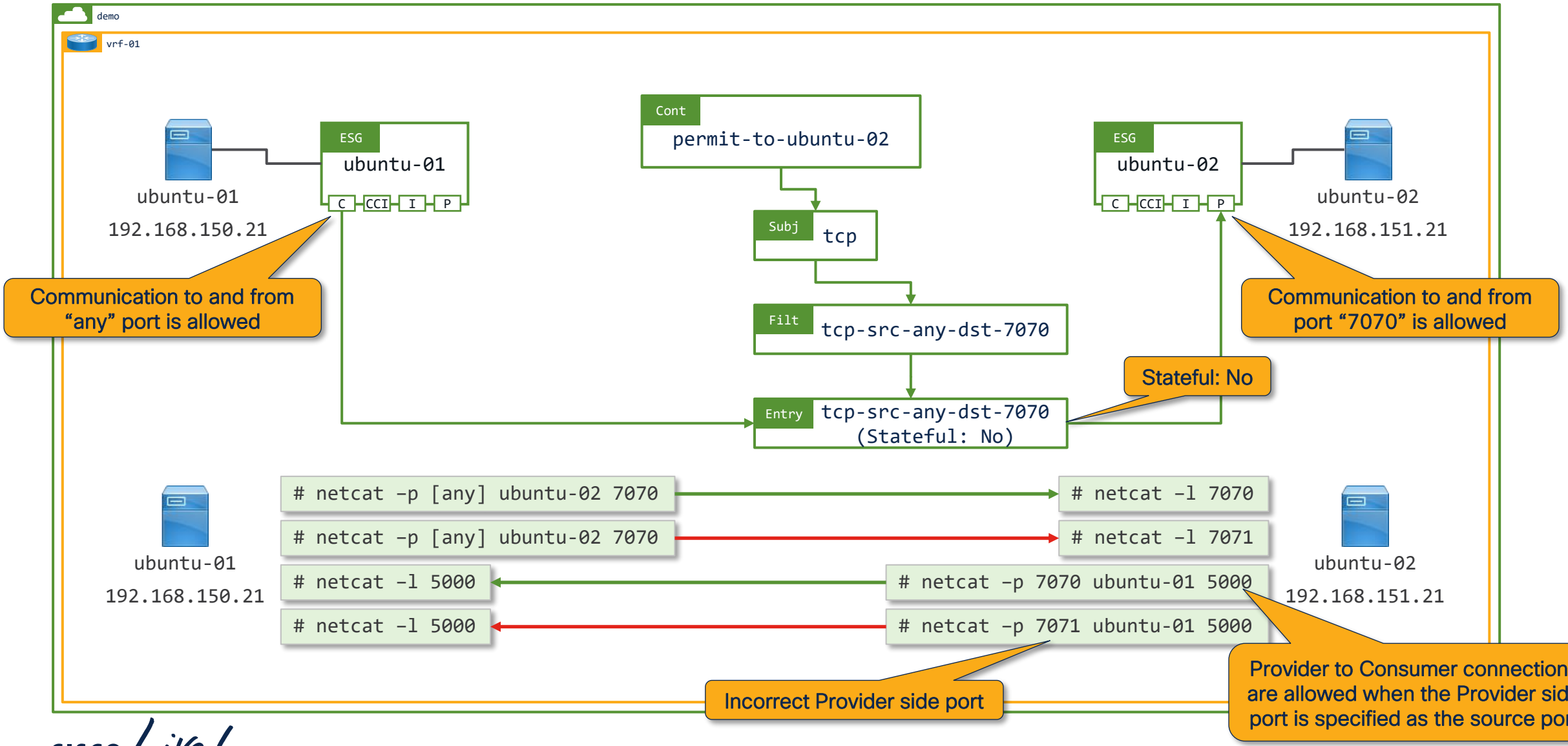
Contract Scope



ExG = Applies to either EPGs or ESGs

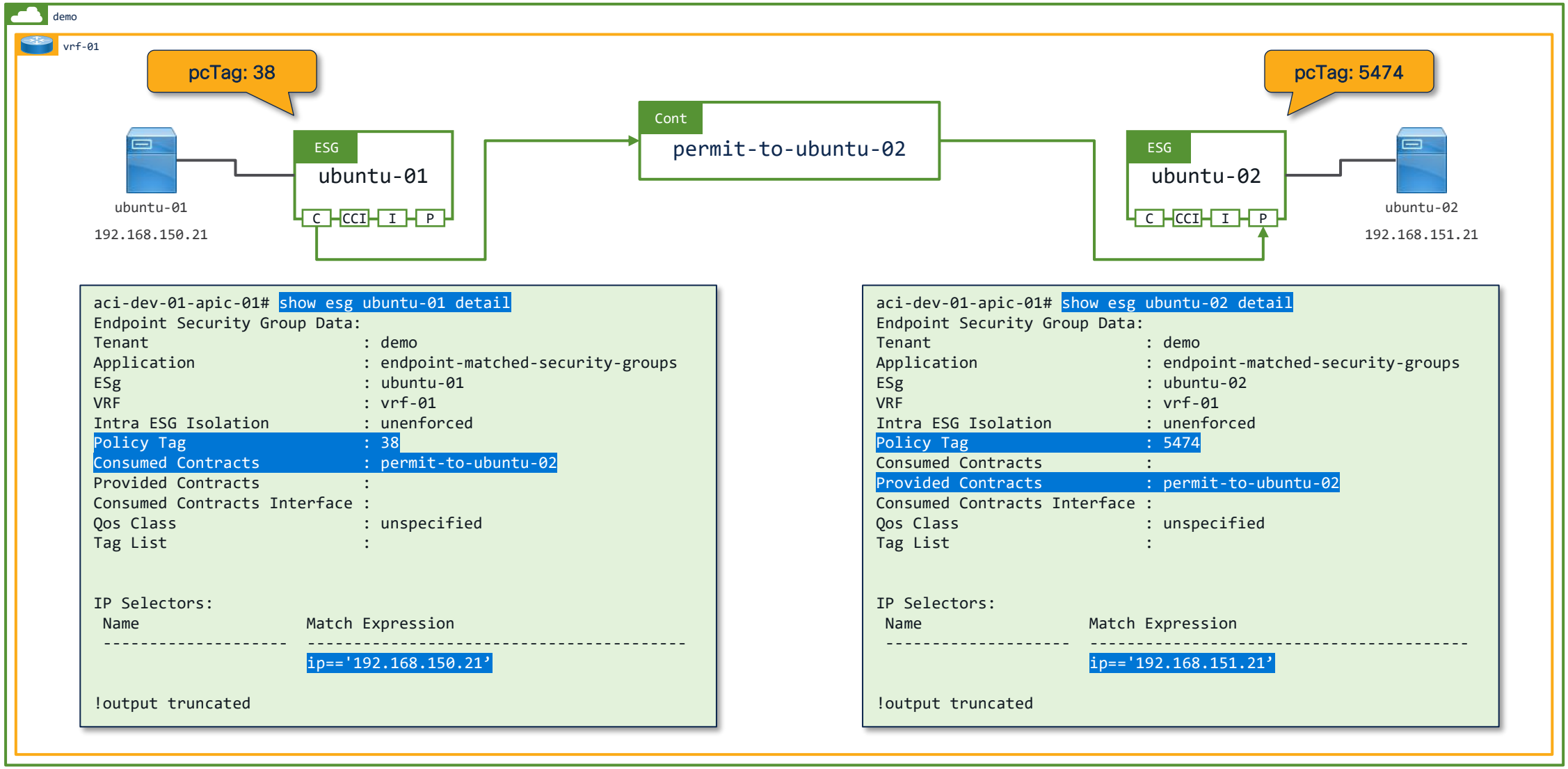
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Verifying Contract operation with netcat – Stateful = No



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

Verifying Contract Operation: EPG/ESG details




```
aci-dev-01-apic-01# show esg ubuntu-01 detail
Endpoint Security Group Data:
Tenant                          : demo
Application                     : endpoint-matched-security-groups
ESg                             : ubuntu-01
VRF                             : vrf-01
Intra ESG Isolation             : unenforced
Policy Tag                      : 38
Consumed Contracts              : permit-to-ubuntu-02
Provided Contracts              :
Consumed Contracts Interface    :
Qos Class                       : unspecified
Tag List                        :


IP Selectors:
 Name                   Match Expression
 --------------------   ----------------------------------------
                        ip=='192.168.150.21'

!output truncated
```

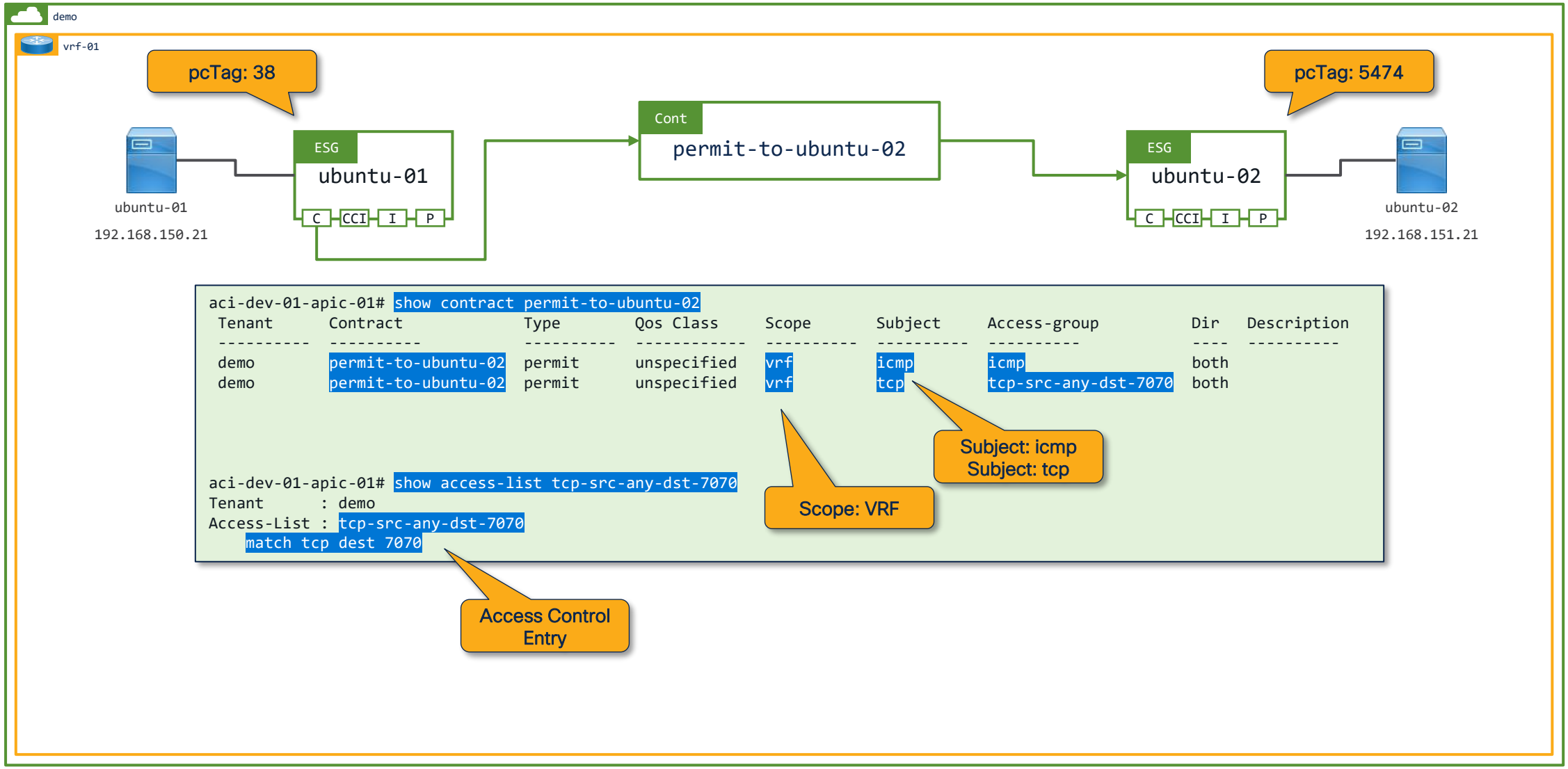
```
aci-dev-01-apic-01# show esg ubuntu-02 detail
Endpoint Security Group Data:
Tenant                          : demo
Application                     : endpoint-matched-security-groups
ESg                             : ubuntu-02
VRF                             : vrf-01
Intra ESG Isolation             : unenforced
Policy Tag                      : 5474
Consumed Contracts              :
Provided Contracts              : permit-to-ubuntu-02
Consumed Contracts Interface    :
Qos Class                       : unspecified
Tag List                        :


IP Selectors:
 Name                   Match Expression
 --------------------   ----------------------------------------
                        ip=='192.168.151.21'

!output truncated
```

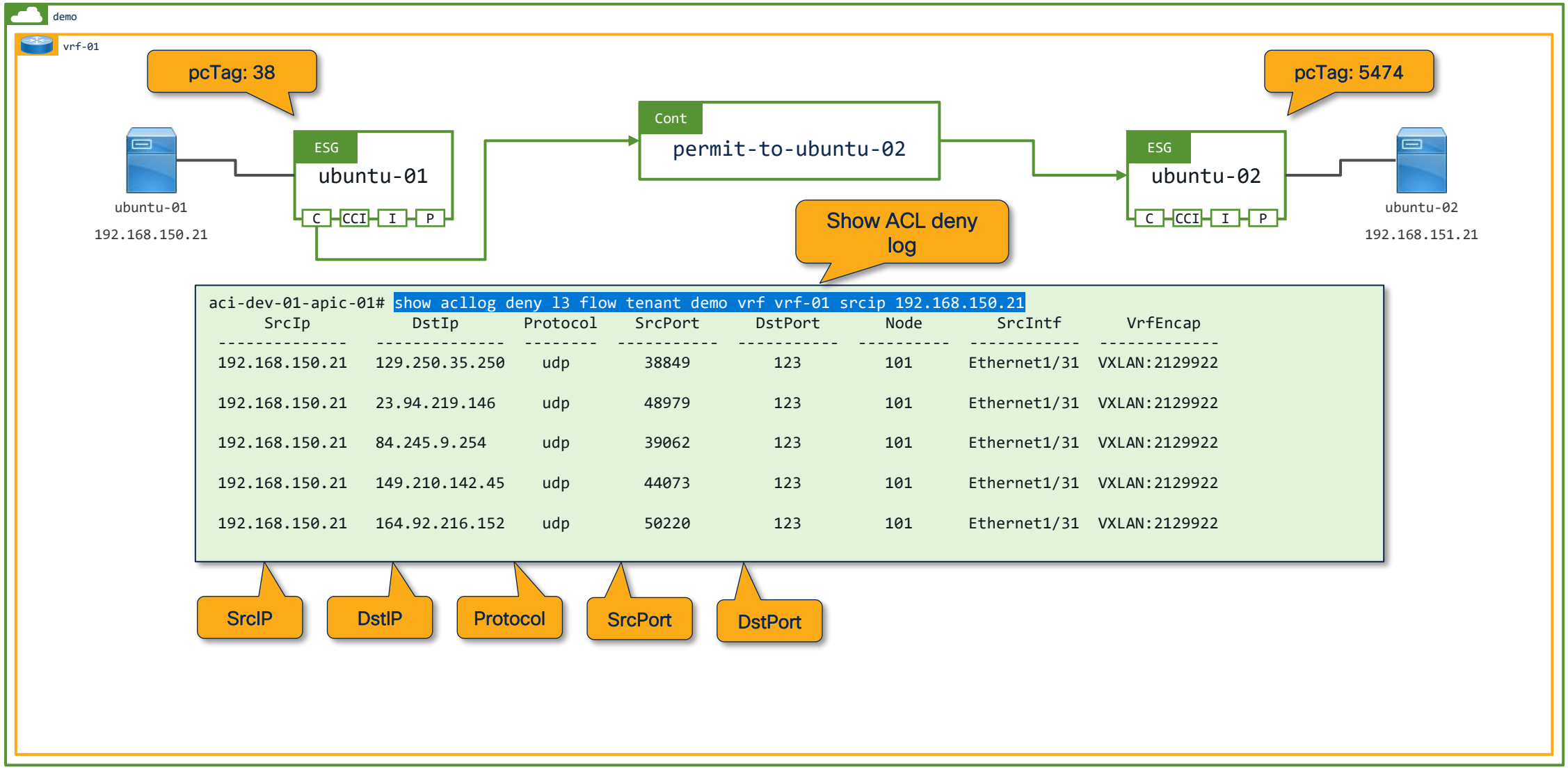

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Verifying Contract Operation: Contract details



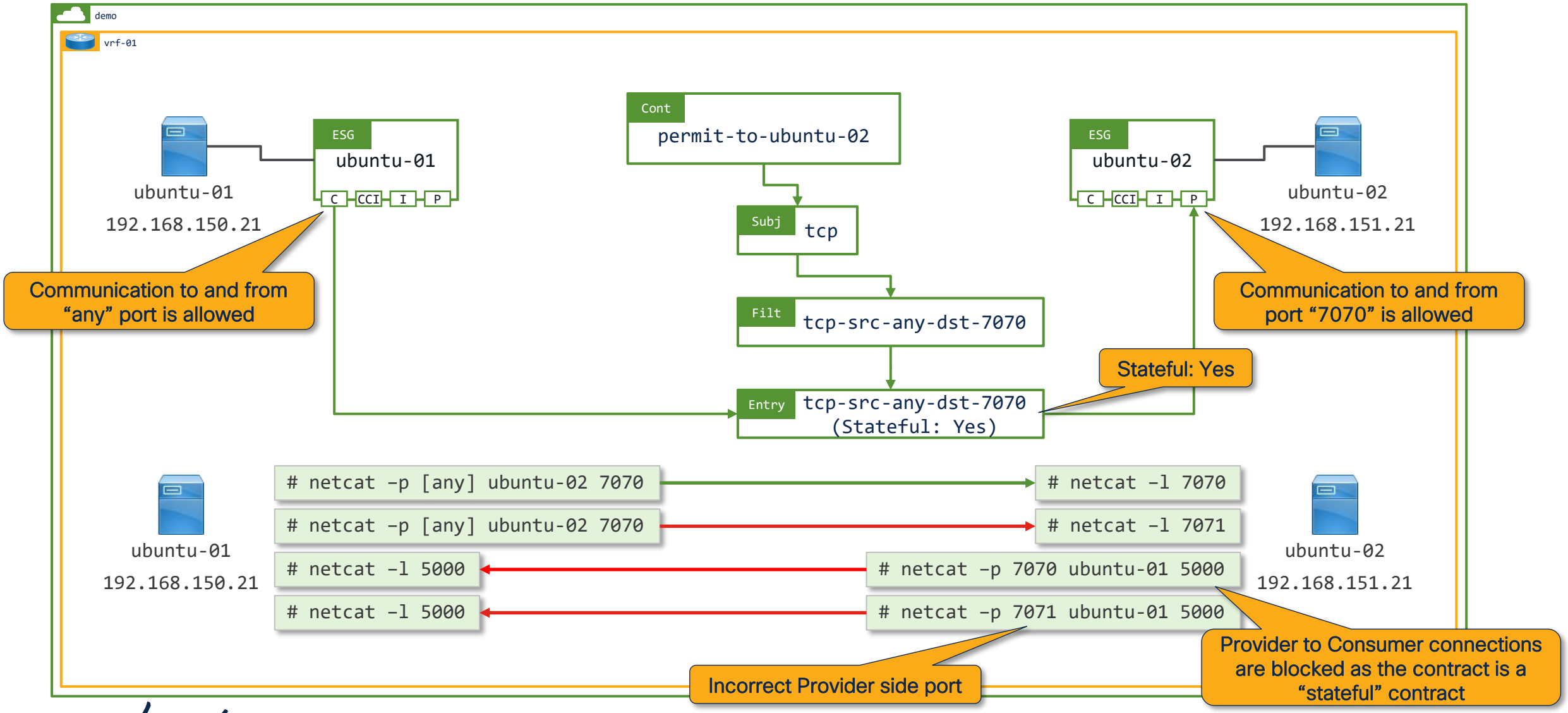
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Verifying Contract Operation: Drop details



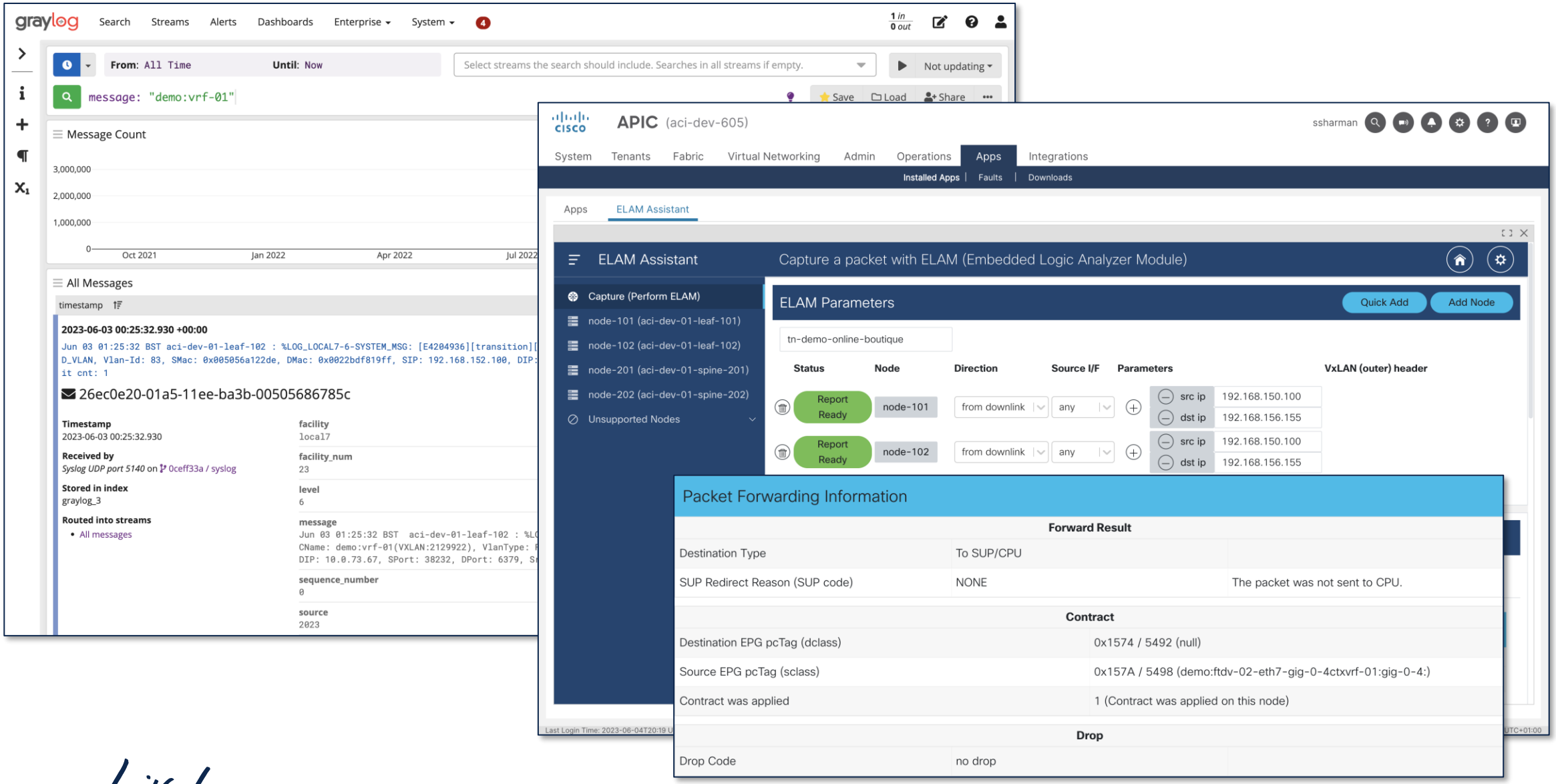
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Verifying Contract operation with netcat – Stateful = Yes

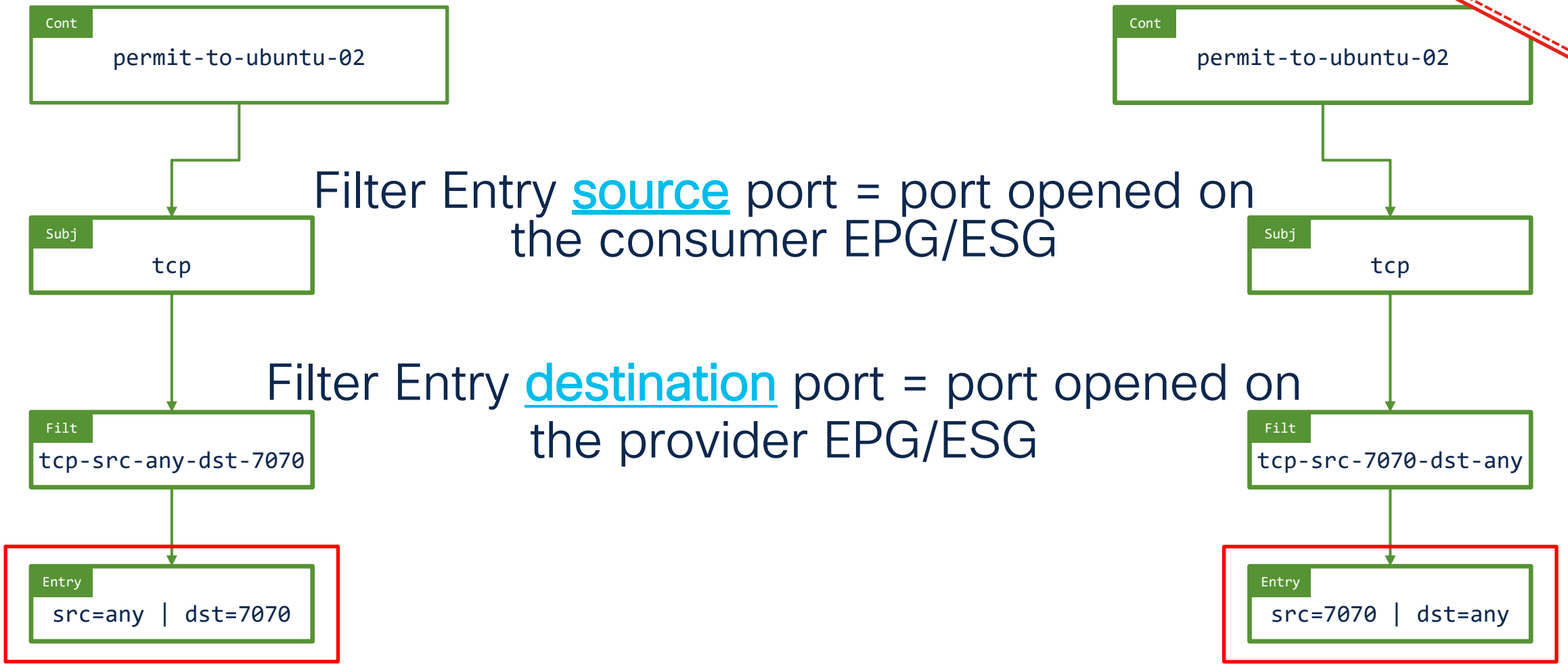


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Verifying Contracts with Syslog and ELAM



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

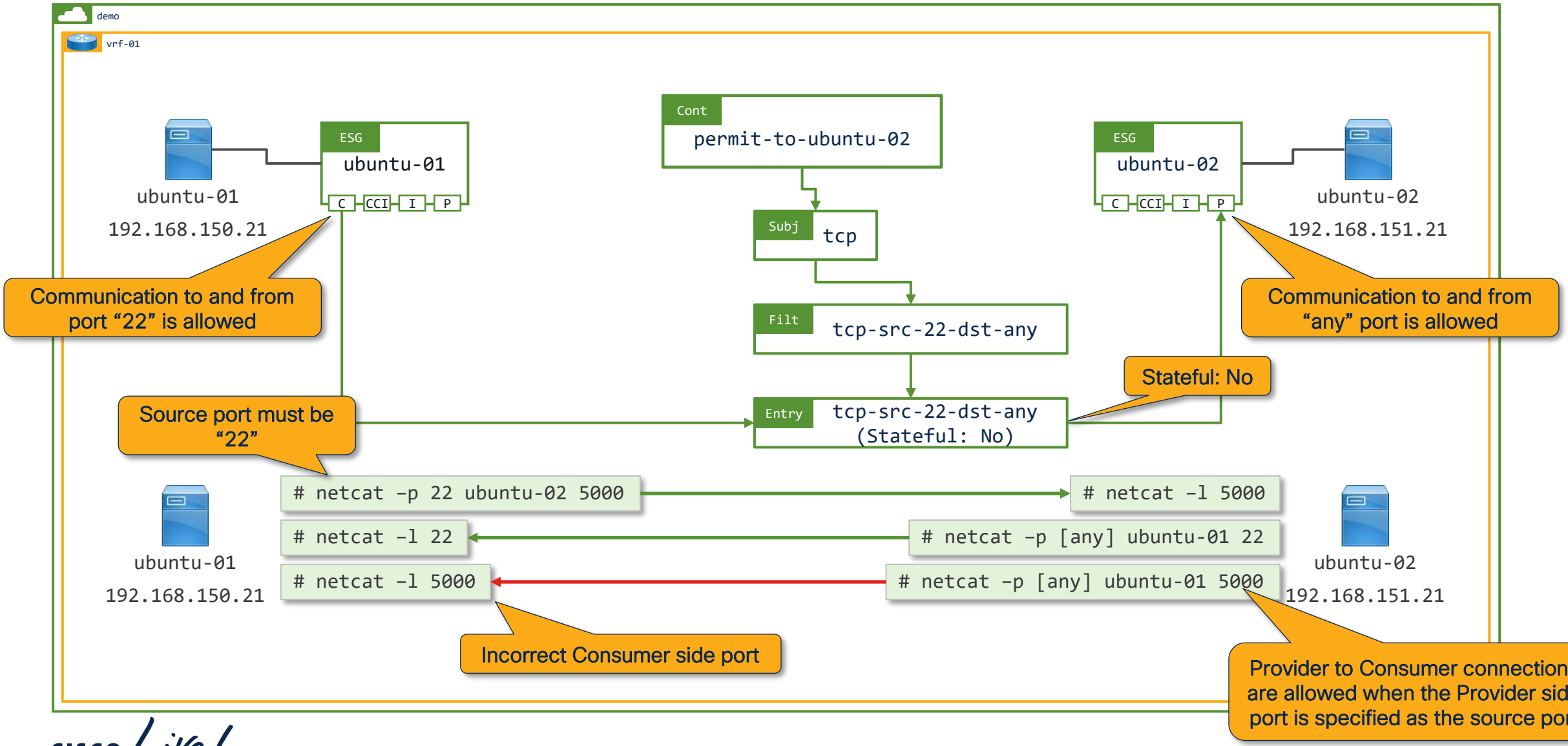


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Getting into the weeds...!

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

Reversing the Filter ports – Stateful = No



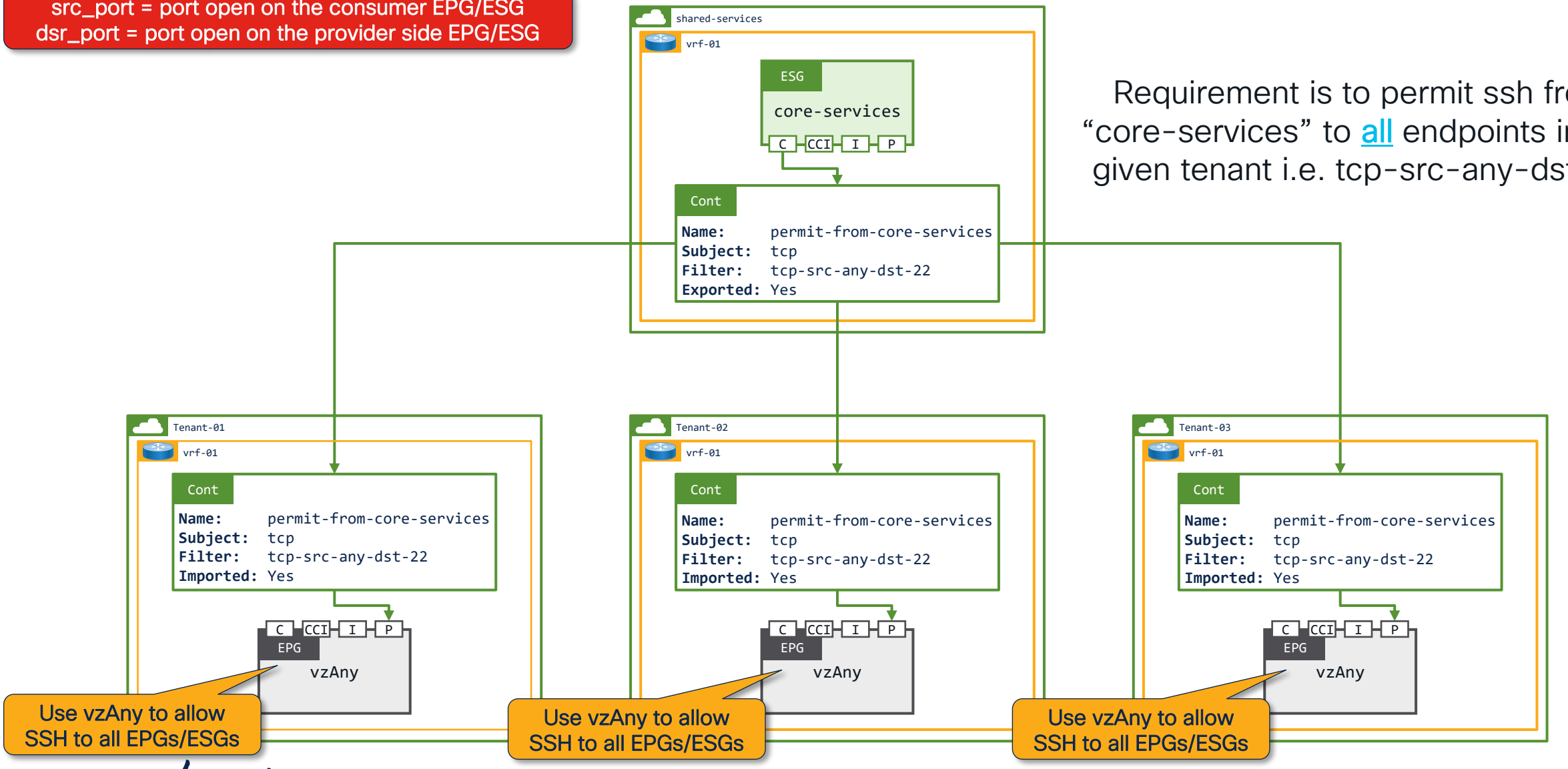
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

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

vzAny as a contract Provider

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

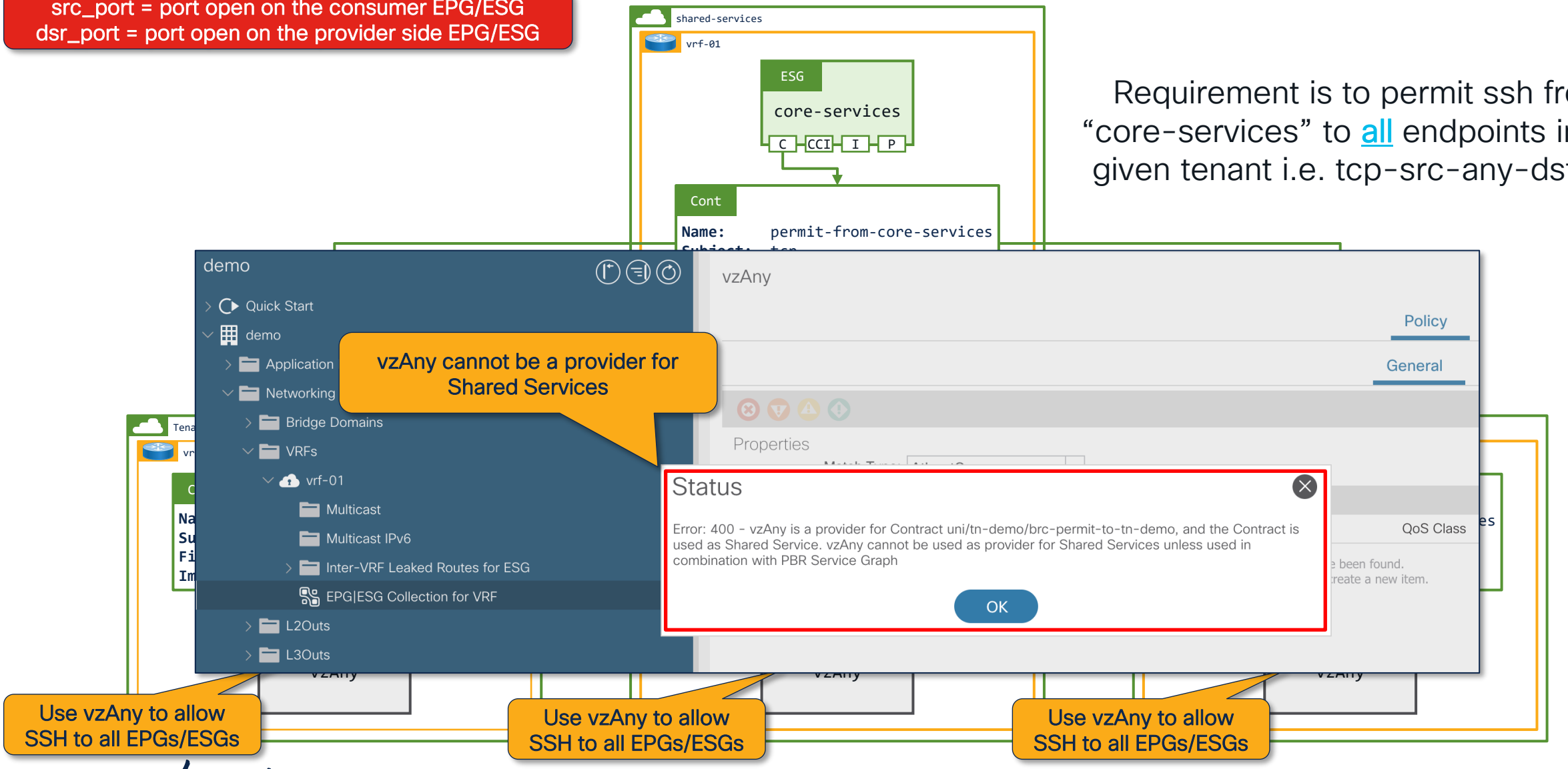


Requirement is to permit ssh from "core-services" to all endpoints in any given tenant i.e. tcp-src-any-dst-22

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

vzAny as a contract Provider

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

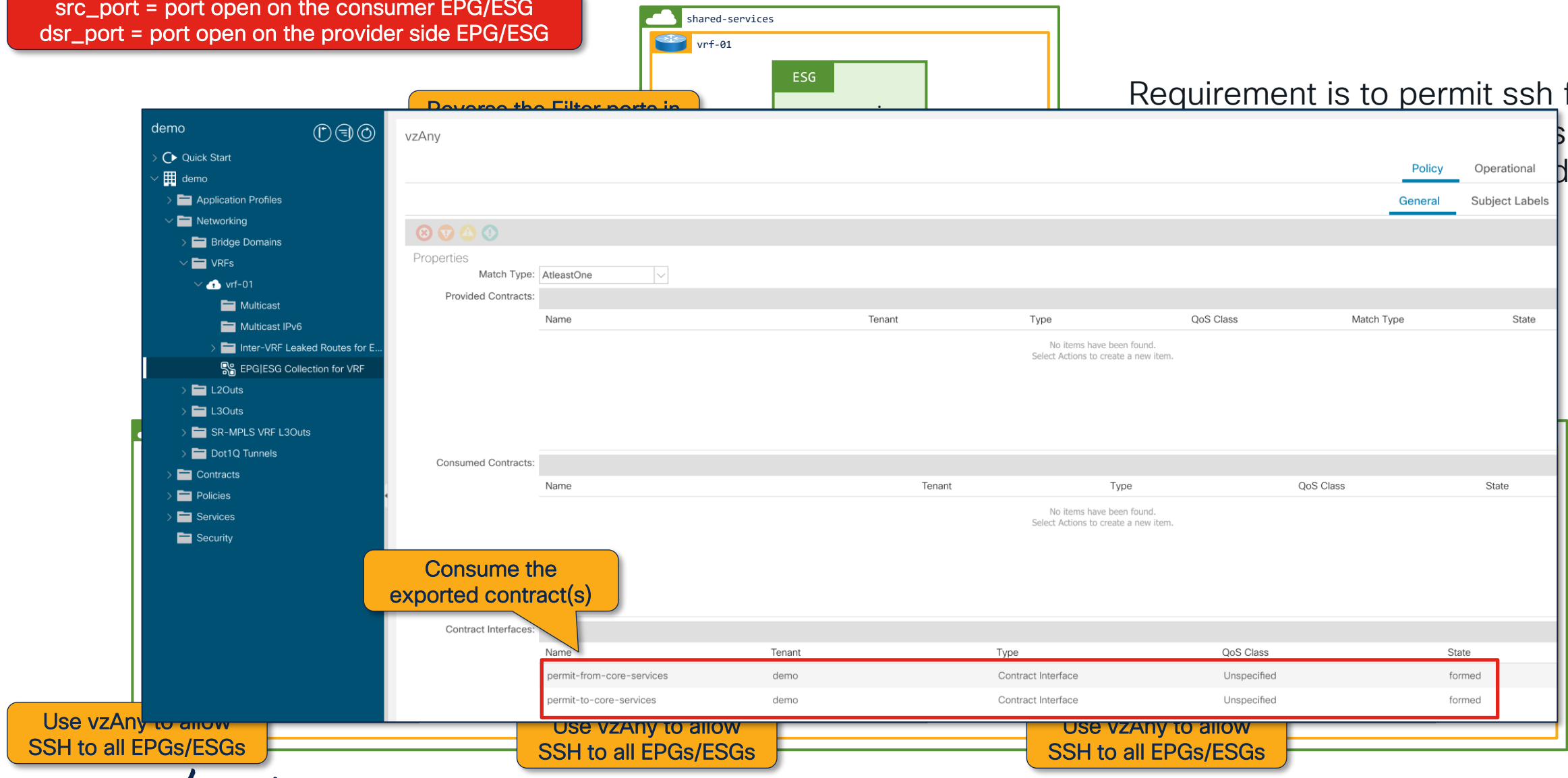


Requirement is to permit ssh from “core-services” to all endpoints in any given tenant i.e. tcp-src-any-dst-22

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

vzAny as a contract Consumer – Filters Reversed

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



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

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

Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

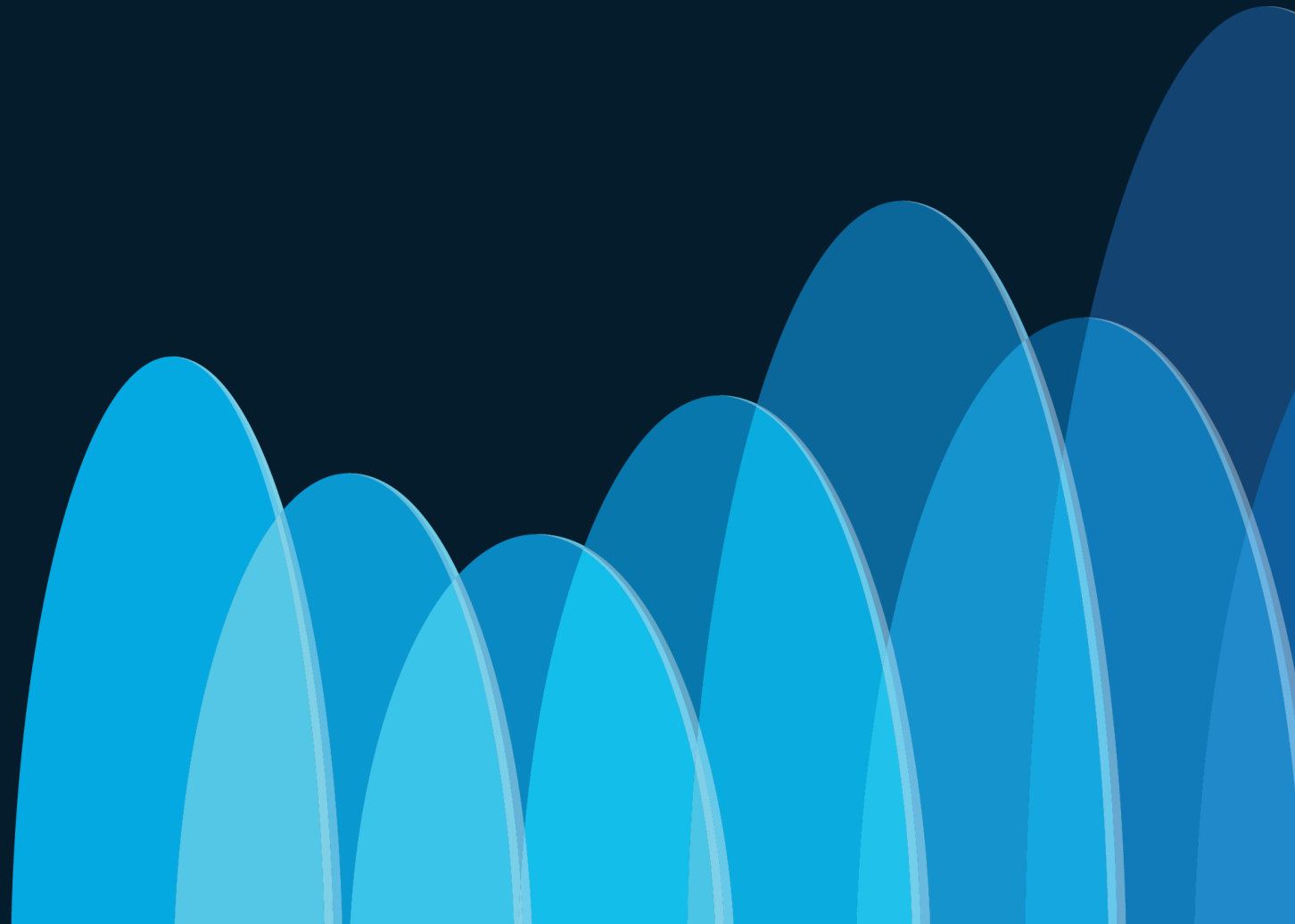
Understanding ACI security...

External Connectivity...

Increasing Security...

Automation Blueprints...

Wrapping up...



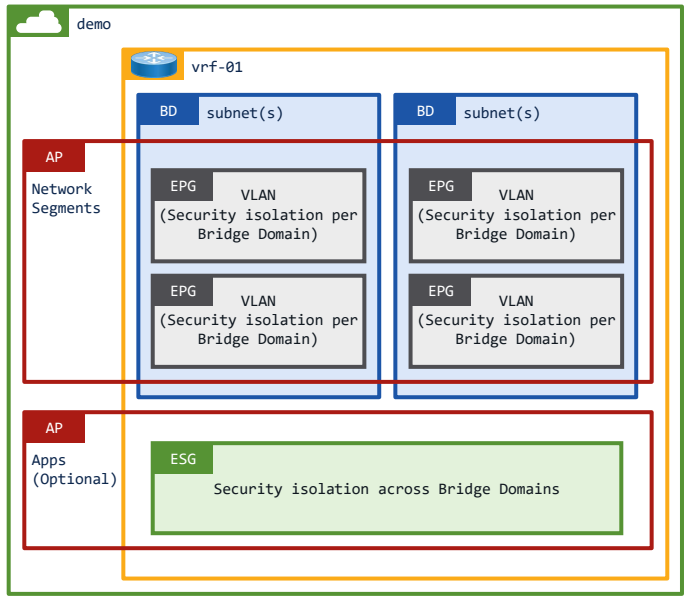
Where should you place your L3outs…?

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

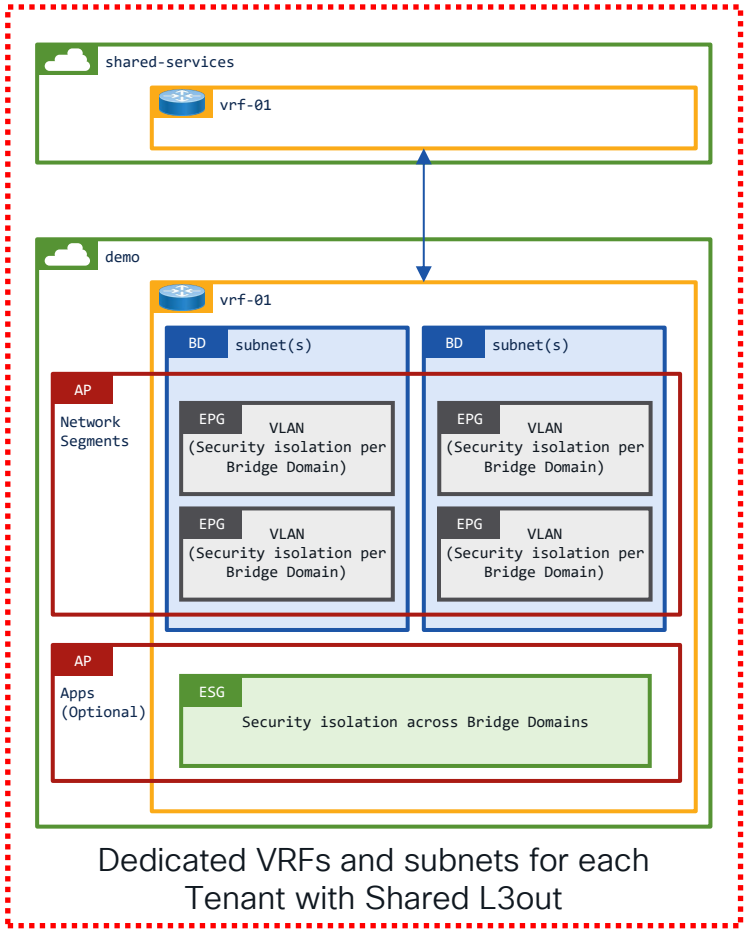
tenant “common”, “shared-services”, or in the “workload/user” tenant…

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

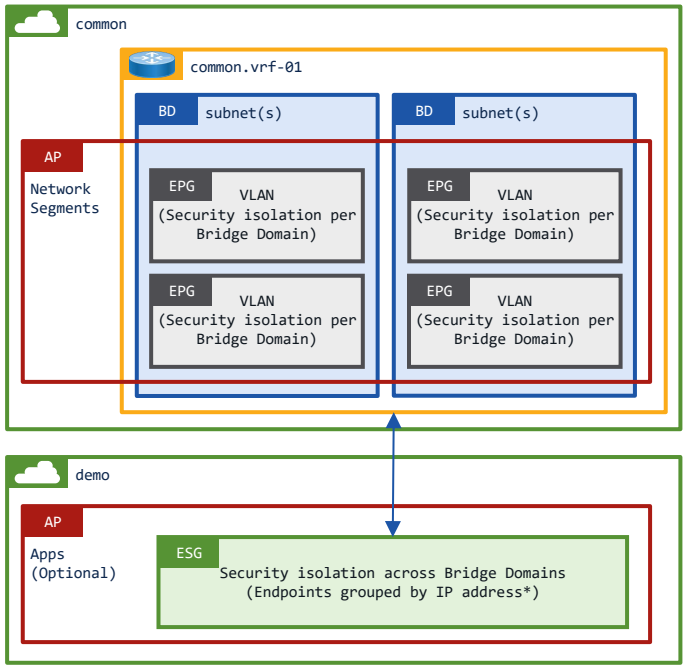
External Connectivity



Dedicated VRFs and subnets for each Tenant with Dedicated L3outs



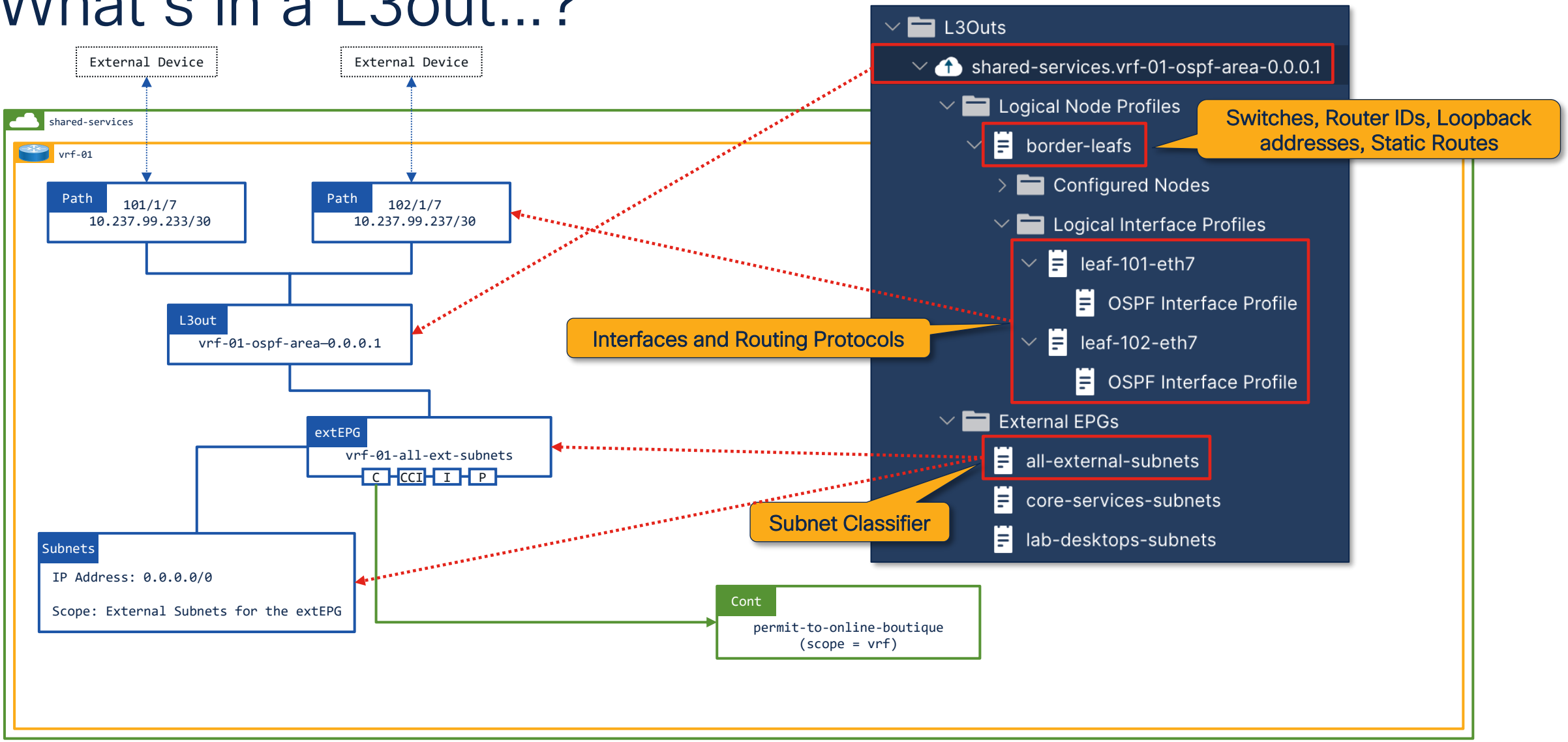
Dedicated VRFs and subnets for each Tenant with Shared L3out



Shared networking with isolated security

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

What's in a L3out...?



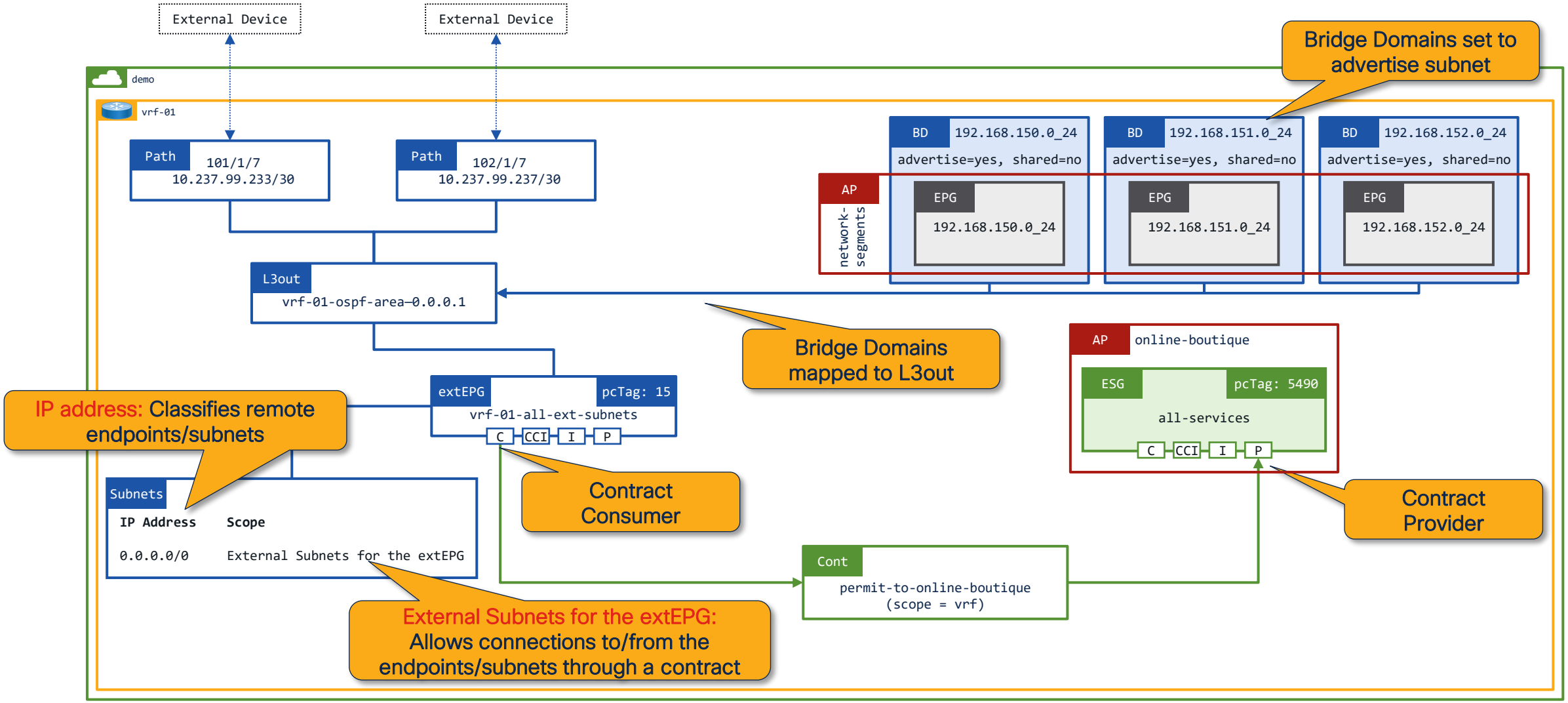
*arrows indicates direction of traffic flow i.e. from consumer to provider

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

Option 1 – Dedicated L3out per Tenant

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

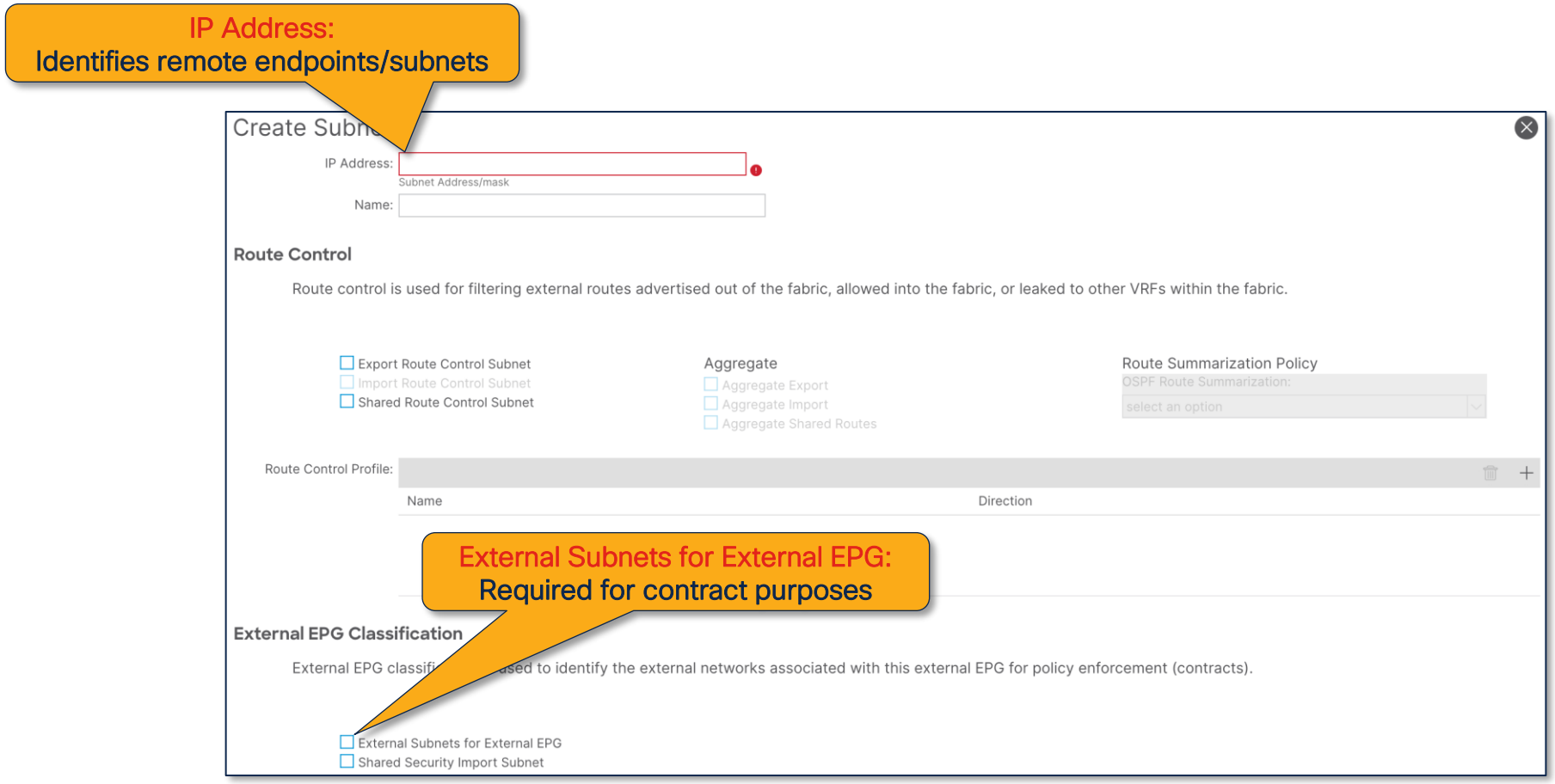
Dedicated L3out



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

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

External Classification



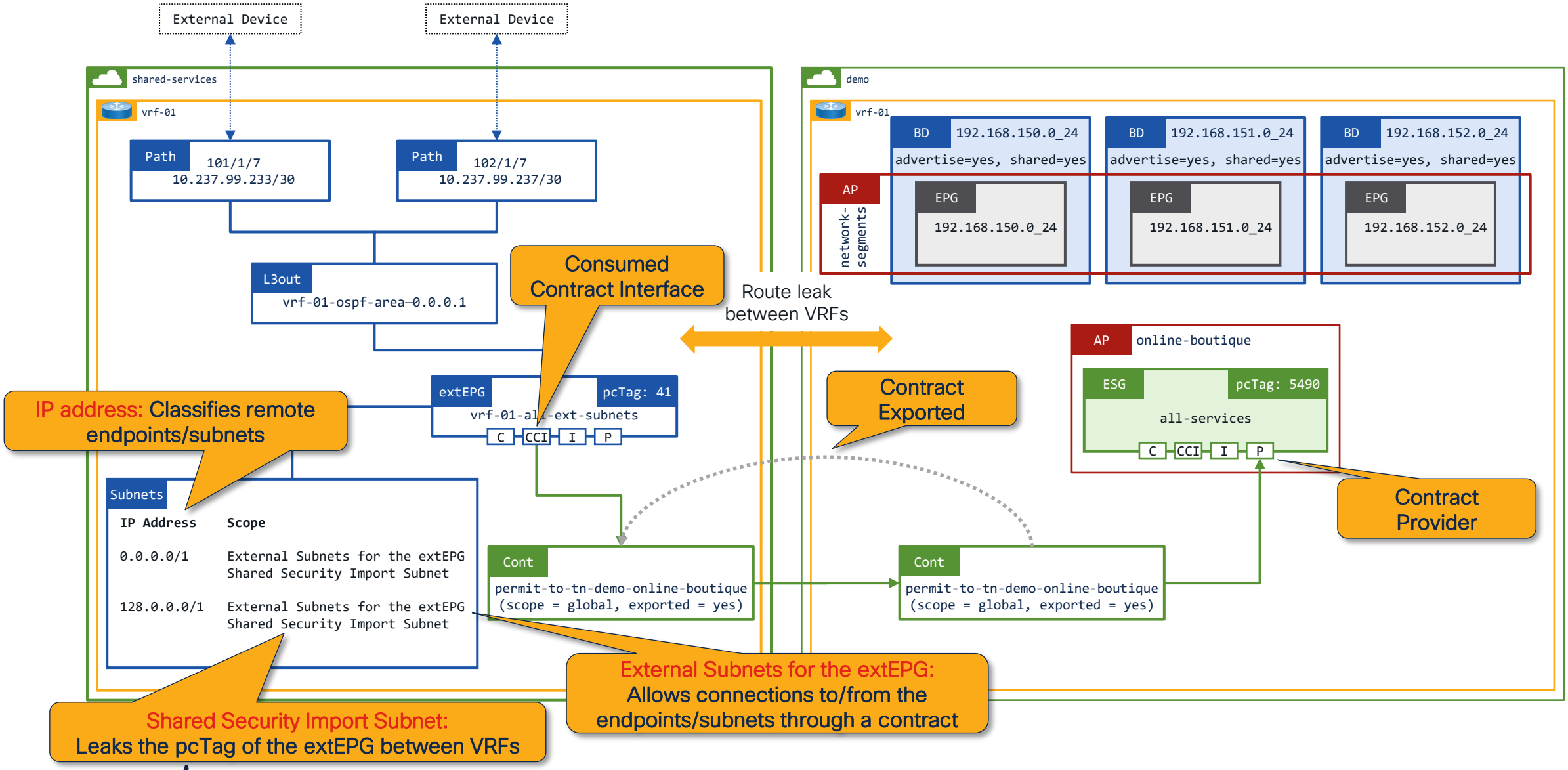
- **IP Address:** identifies remote endpoints/subnets
- **External Subnets for External EPG:** allows packets to/from the L3out with a contract

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

Option 2 – Shared L3out

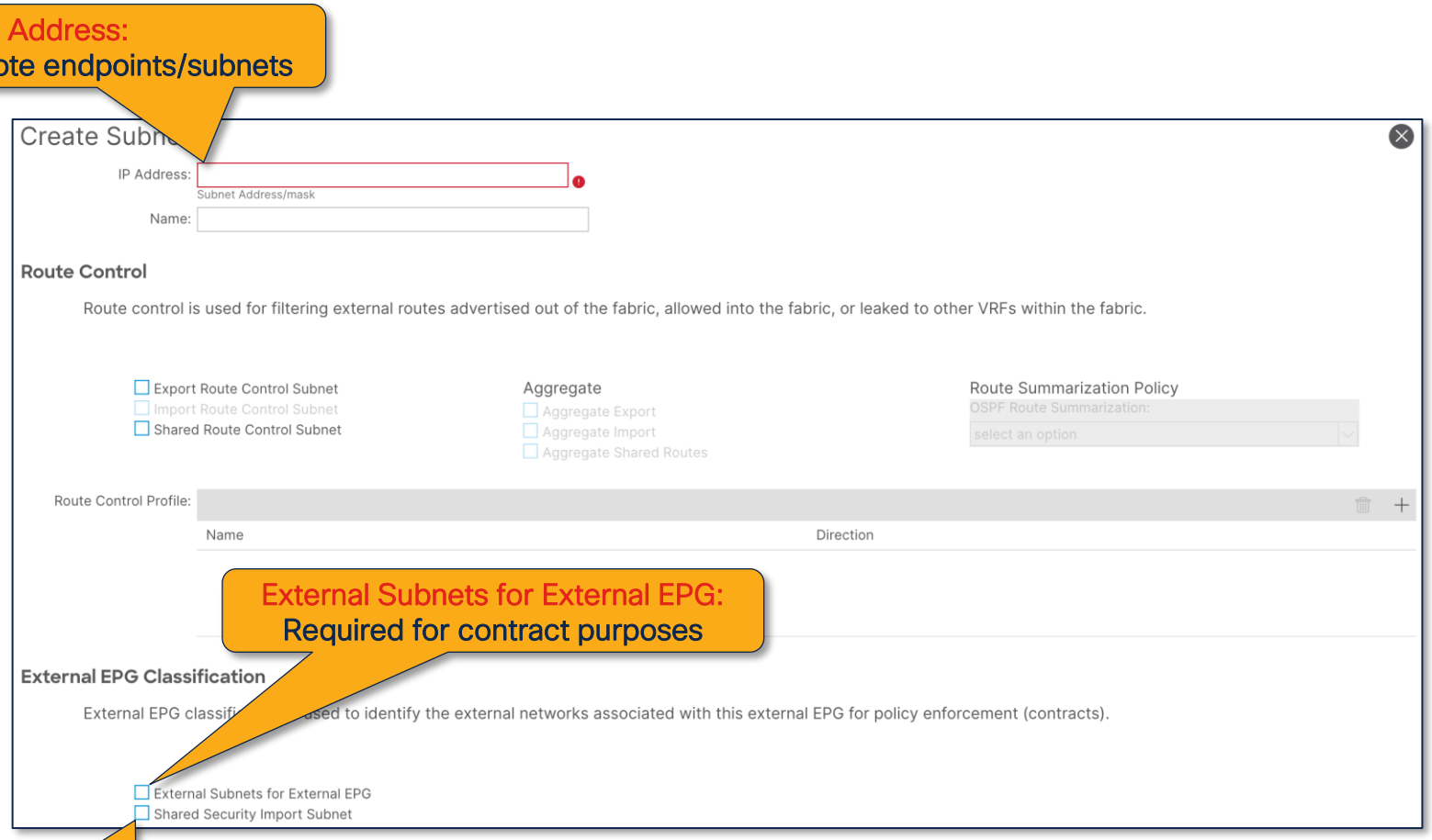
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Shared L3out – Route Leaking between VRFs (ESGs)



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

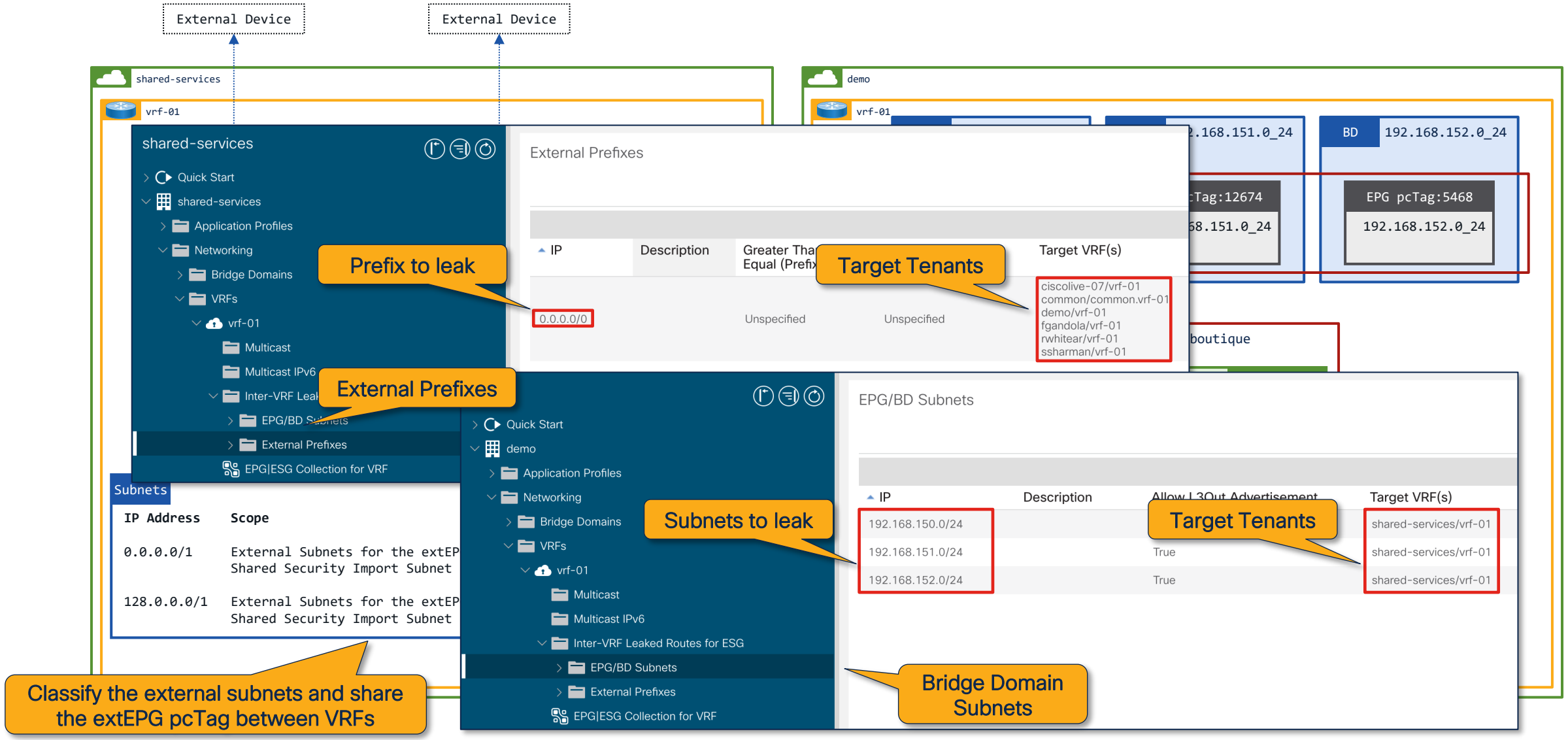
External Classification and Route Leaking



- **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

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

Shared L3out – Route Leaking between VRFs (ESGs)



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

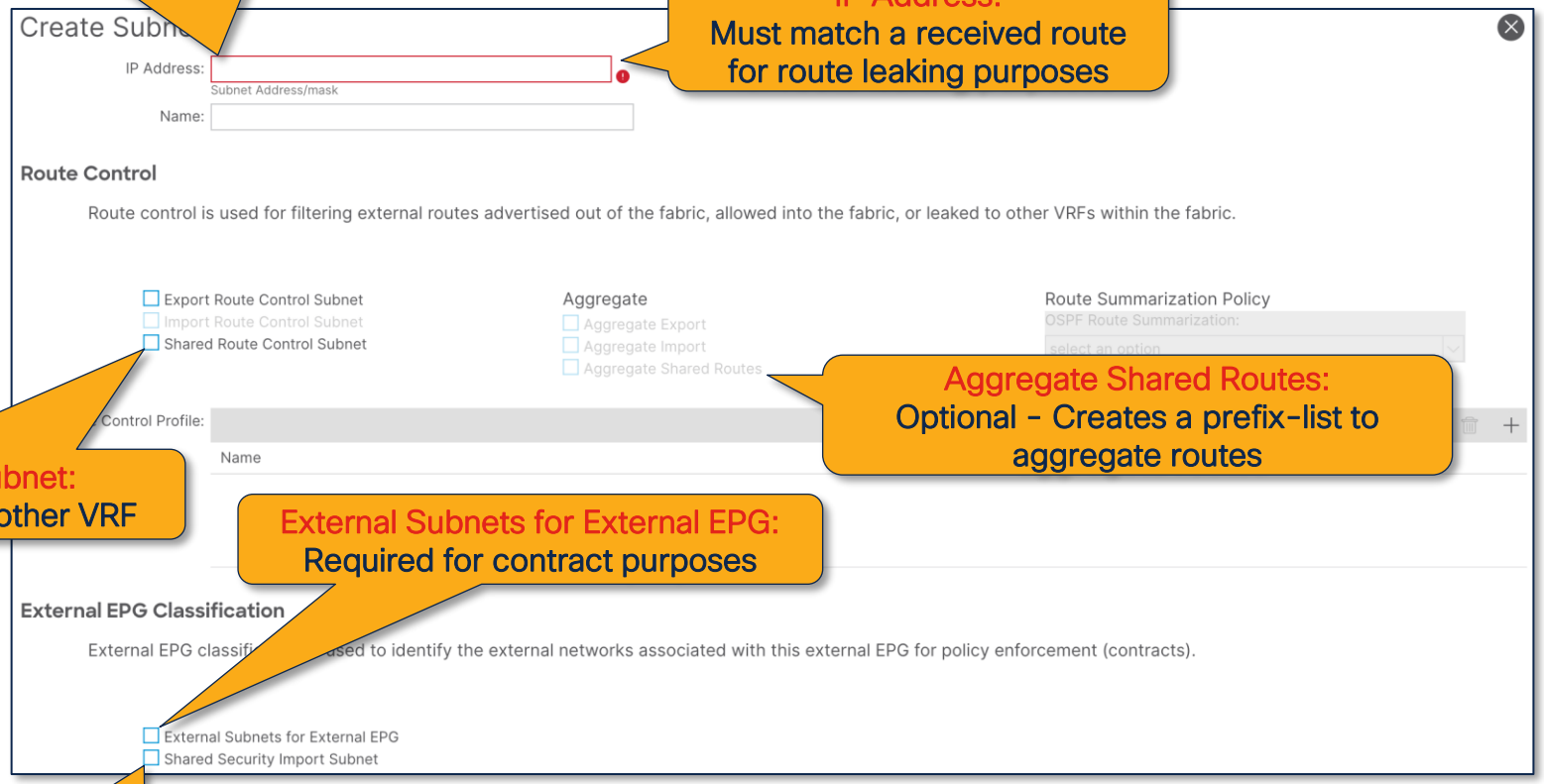
Getting into the weeds...!

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

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

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

External Classification and Route Leaking

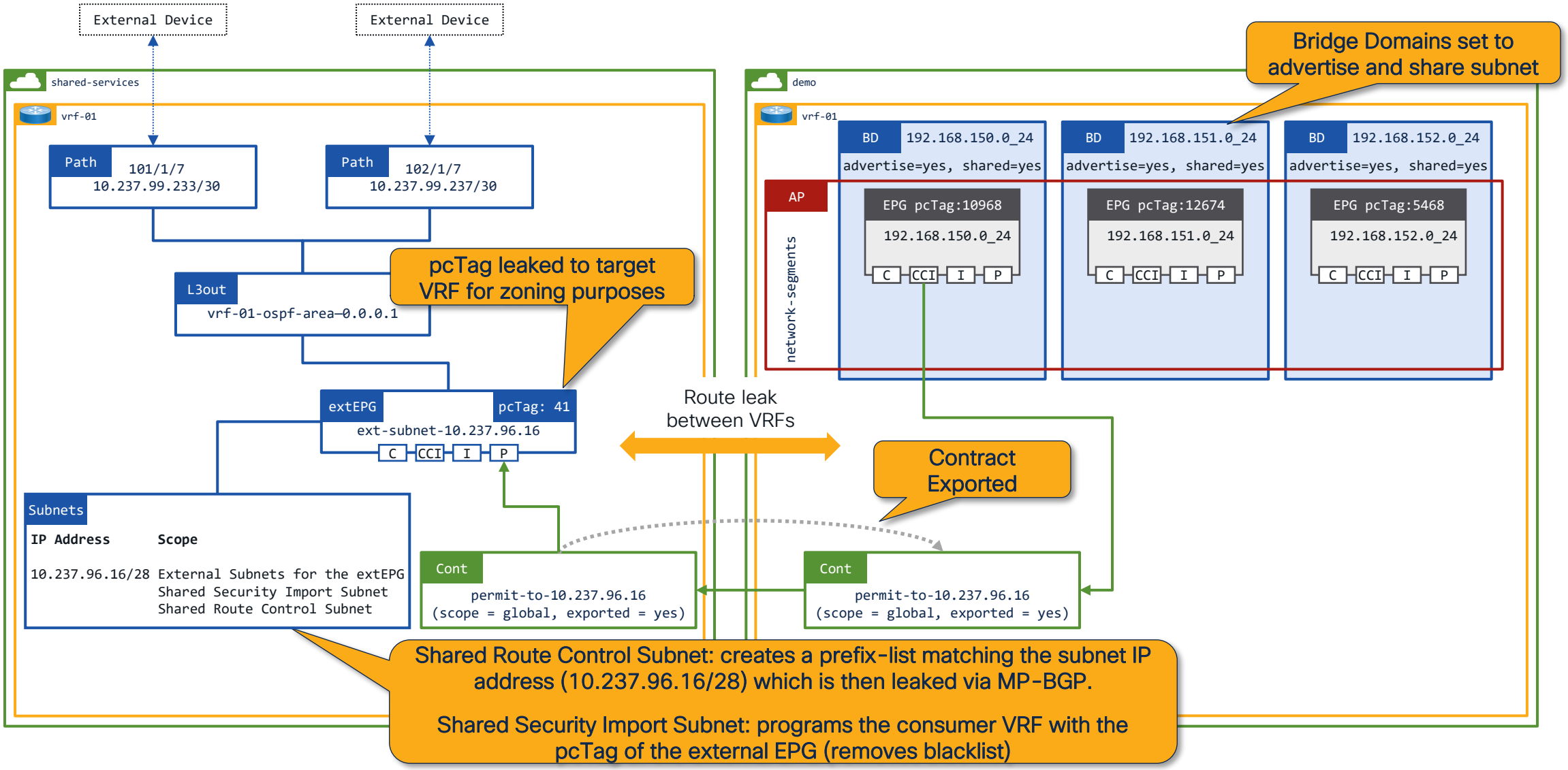


- **IP Address:** identifies remote endpoints/subnets, **must** match a received route for route leaking purposes
- **External Subnets for External EPG:** allows packets to/from the L3out with a contract
- **Shared Security Import Subnet:** is **always** required as it leaks the extEPG pcTag to the target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

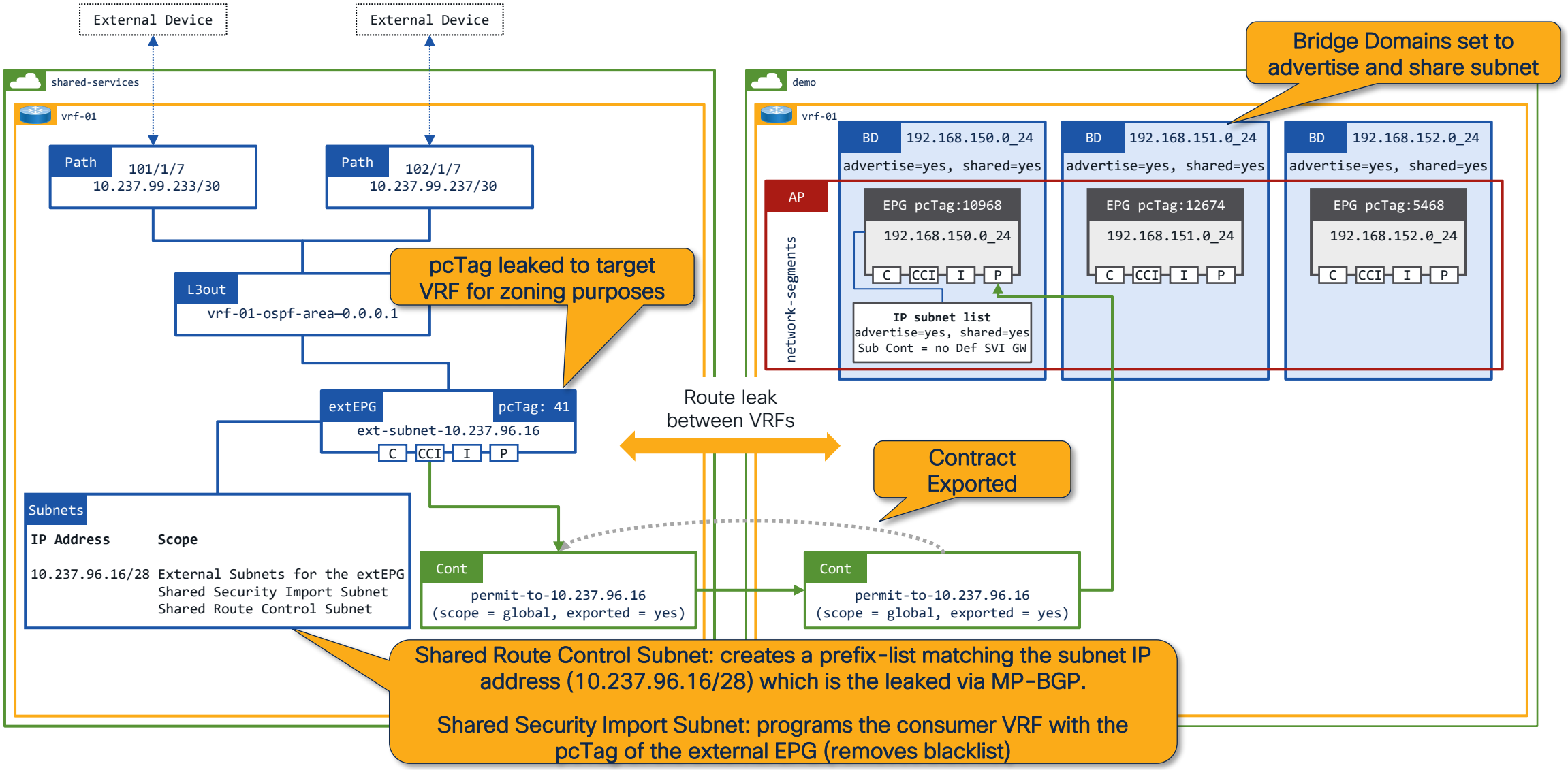
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

EPG Route Leaking – L3out is the Provider



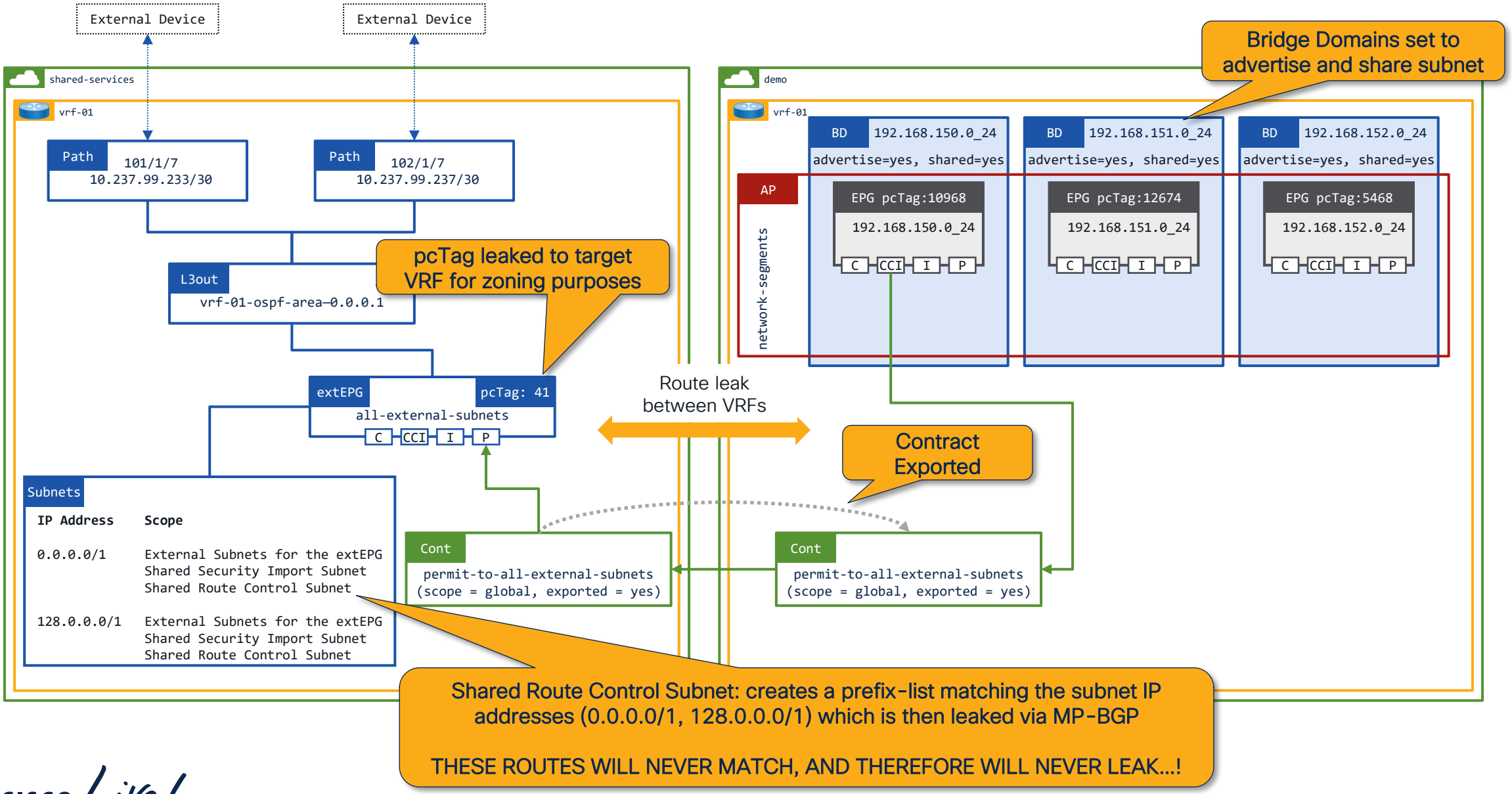
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

EPG Route Leaking – L3out is the Consumer



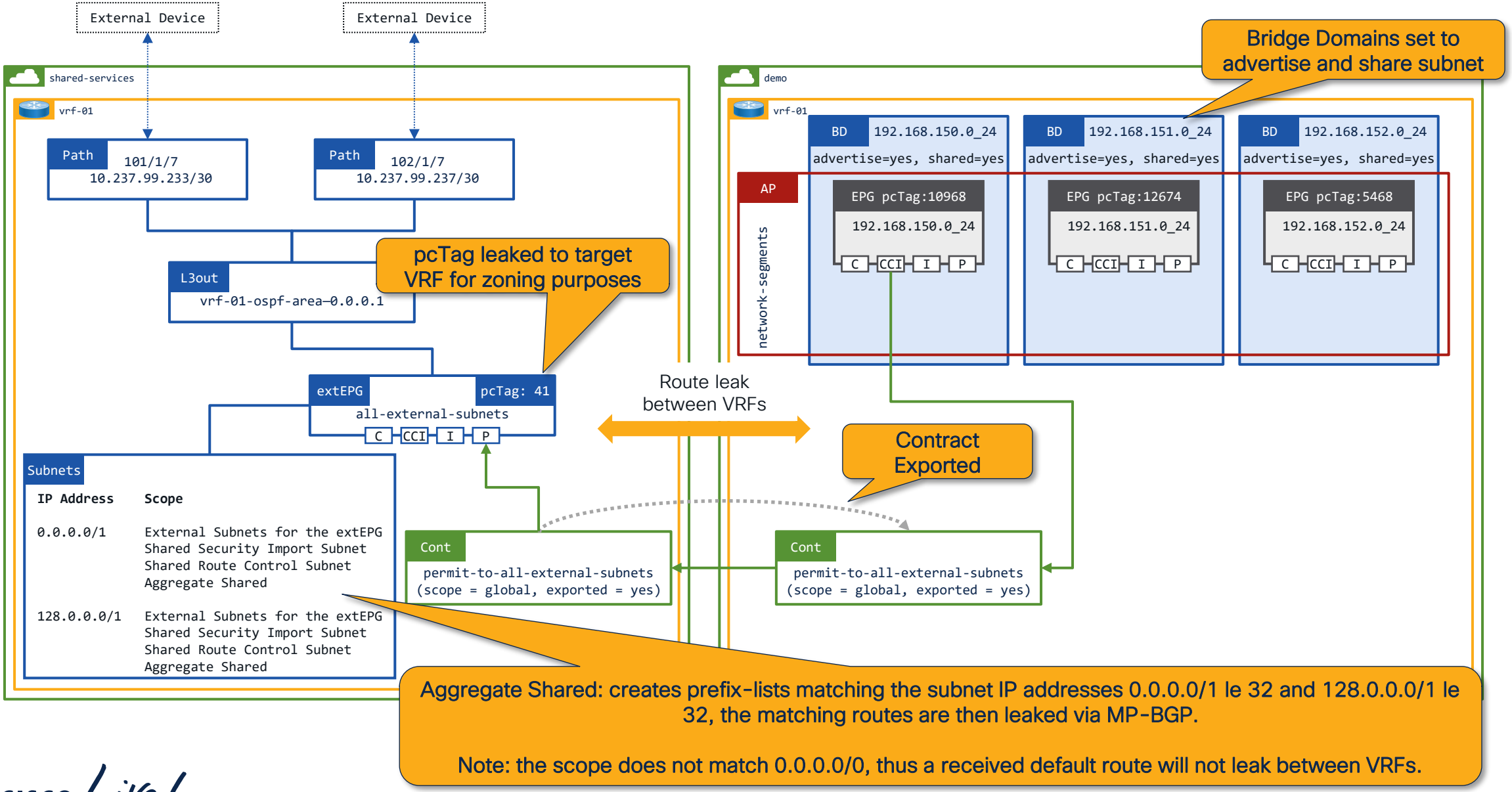
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

“Shared Route Control Subnet” **must** match a received route



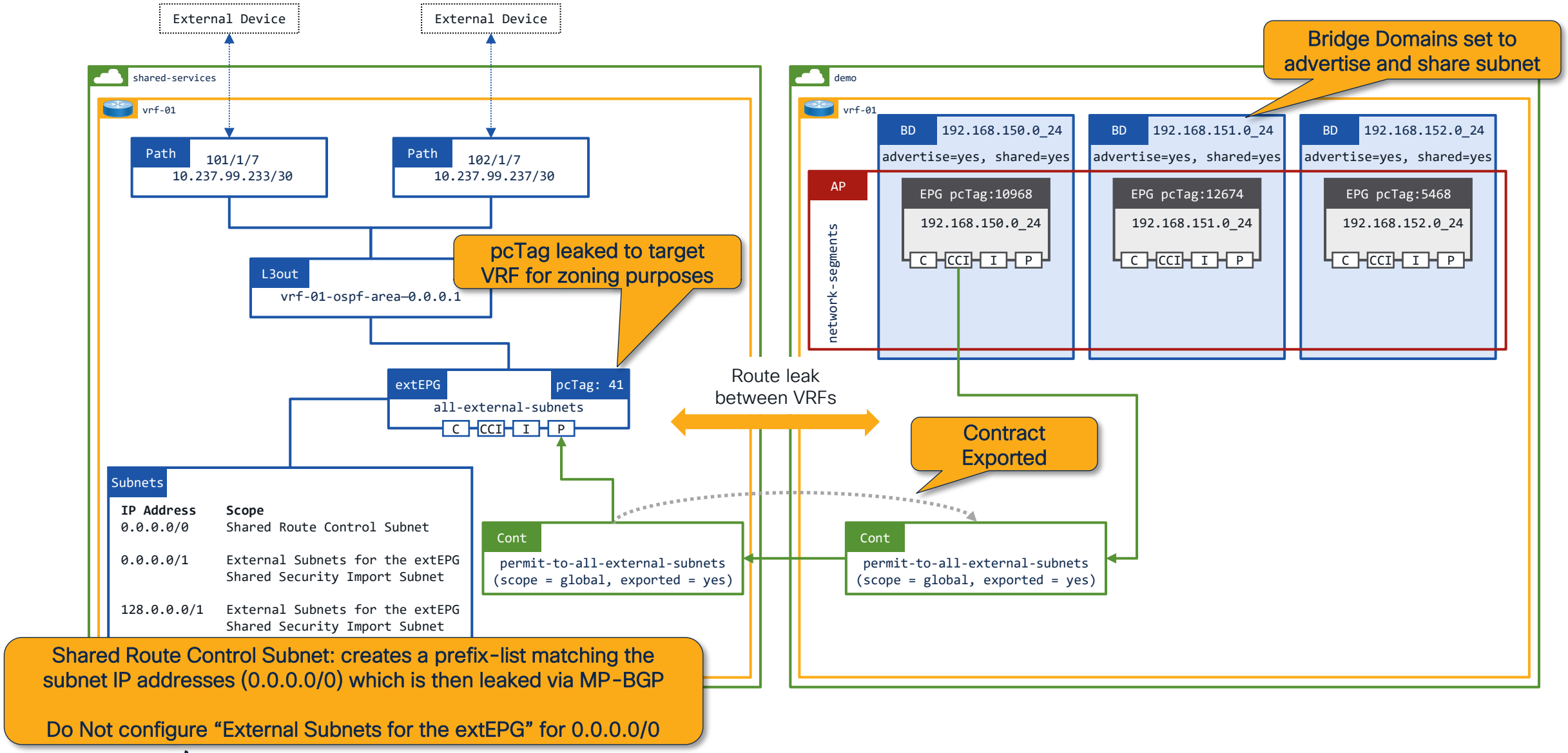
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Leaking all received routes



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

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

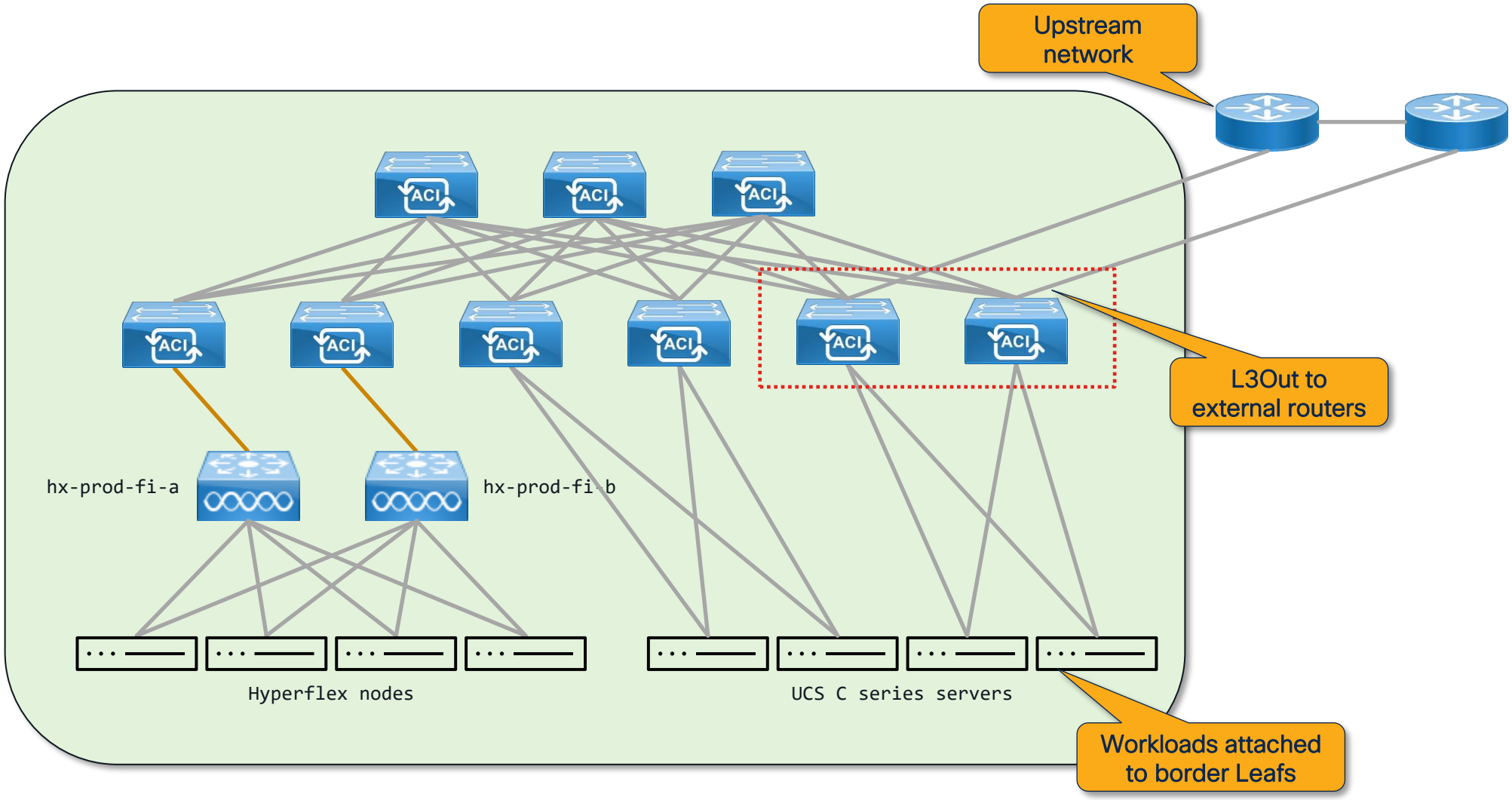
Do Not configure “External Subnets for the extEPG” for 0.0.0.0/0

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

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

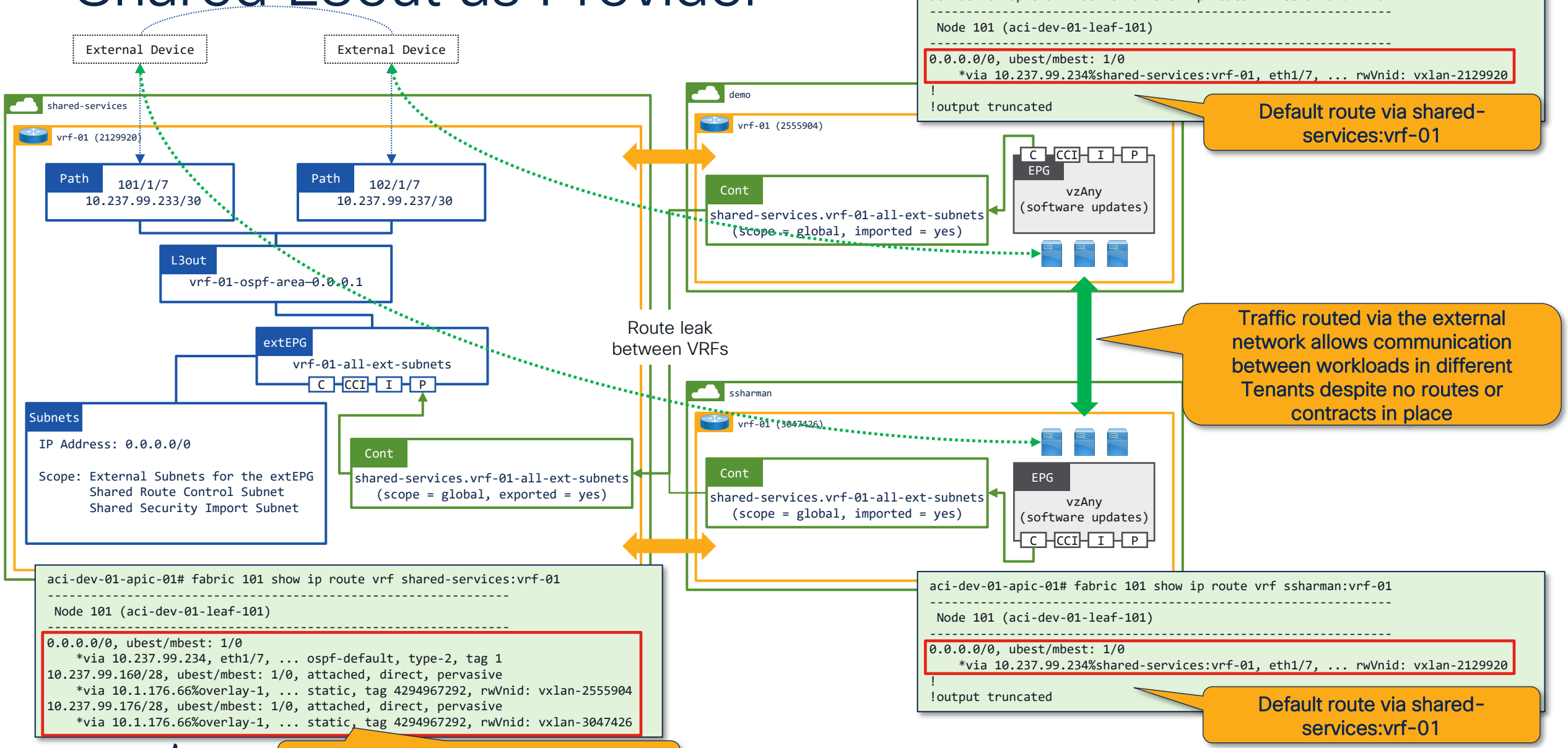
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Non dedicated border Leafs



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

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 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
```

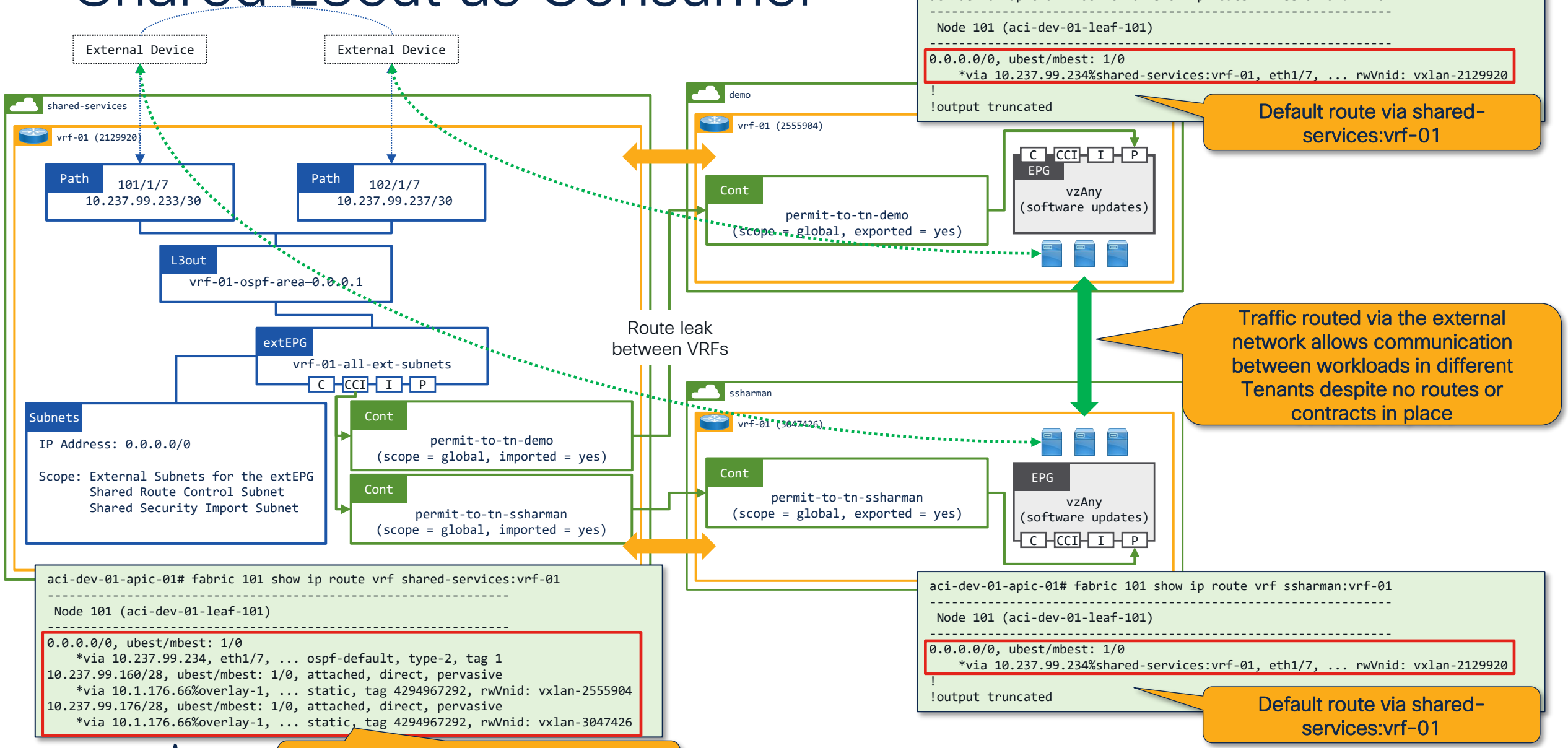
Default route to external network. Routes to Tenant subnets via overlay-1

```
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

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

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

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

Recommendation

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

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

Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

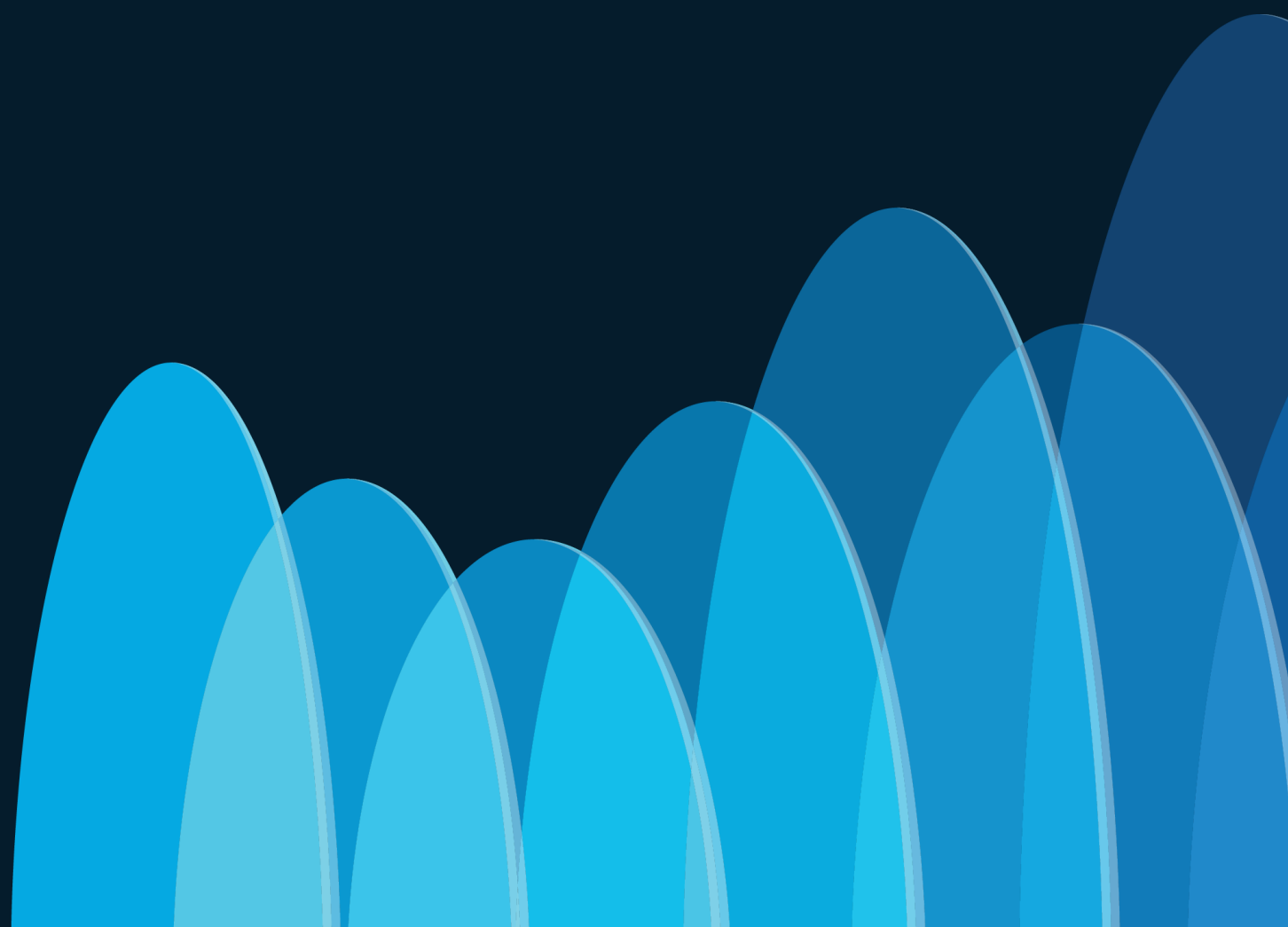
Understanding ACI security...

External Connectivity...

Increasing Security...

Automation Blueprints...

Wrapping up...



cisco Live!

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

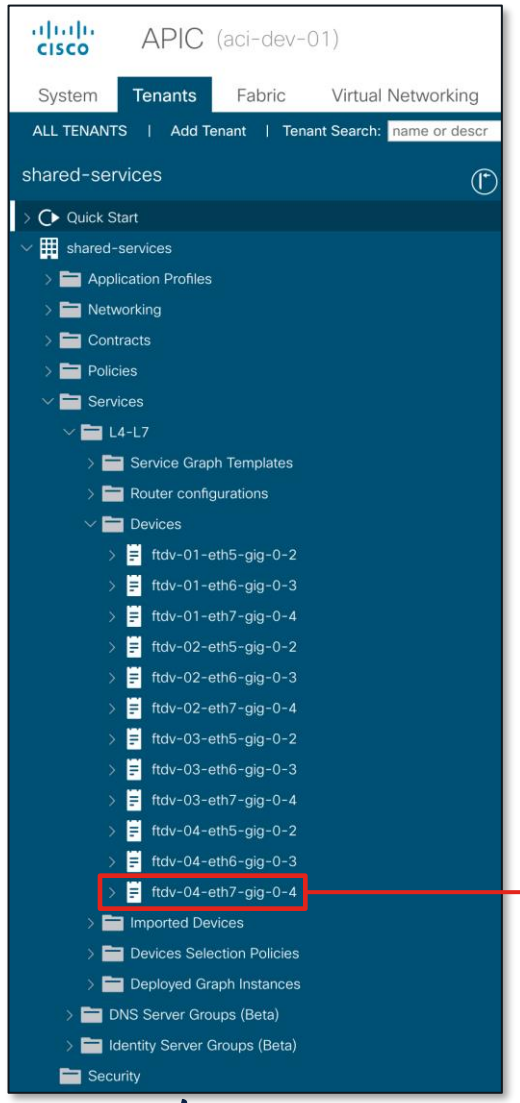
Do you want to use Layer 2 or Layer 3 redirects for service insertion...?

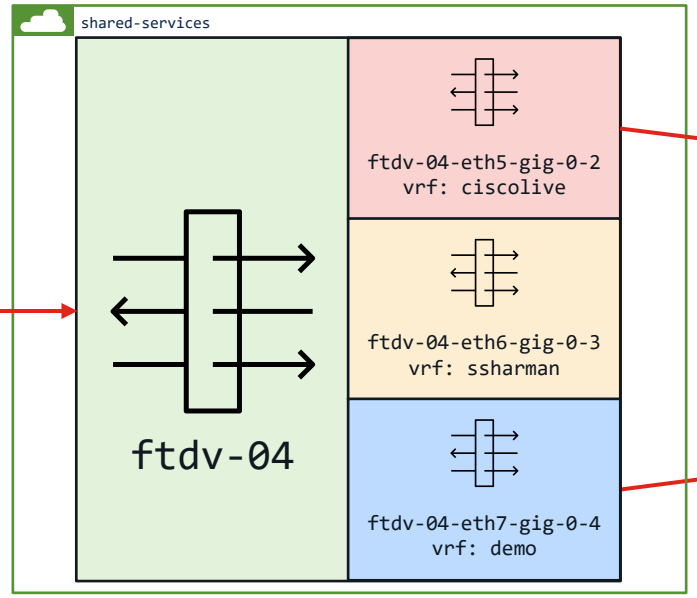
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

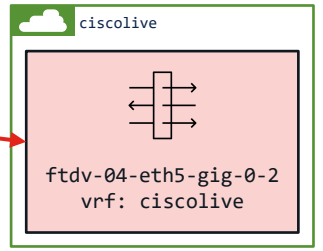
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Virtual firewall deployment

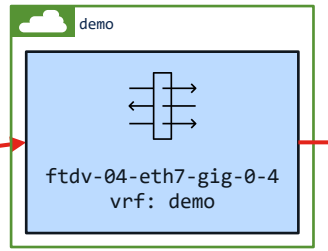




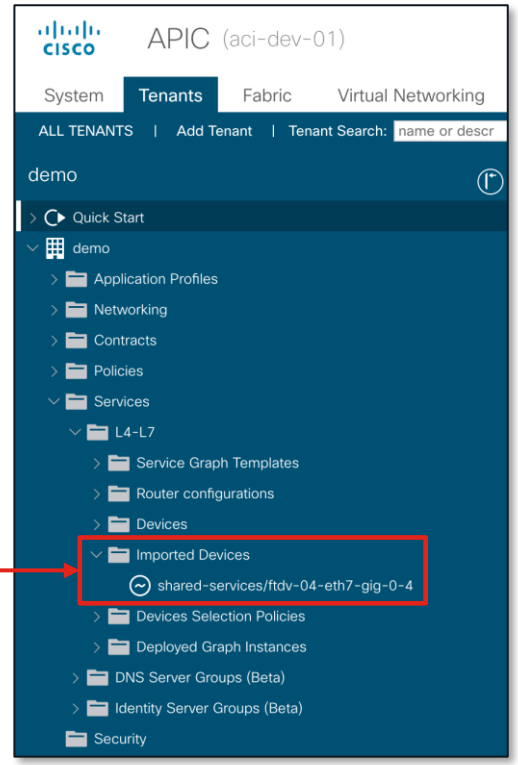
VRF aware firewalls defined in “shared-services” and exported to “user” tenants



Imported firewall



Imported firewall



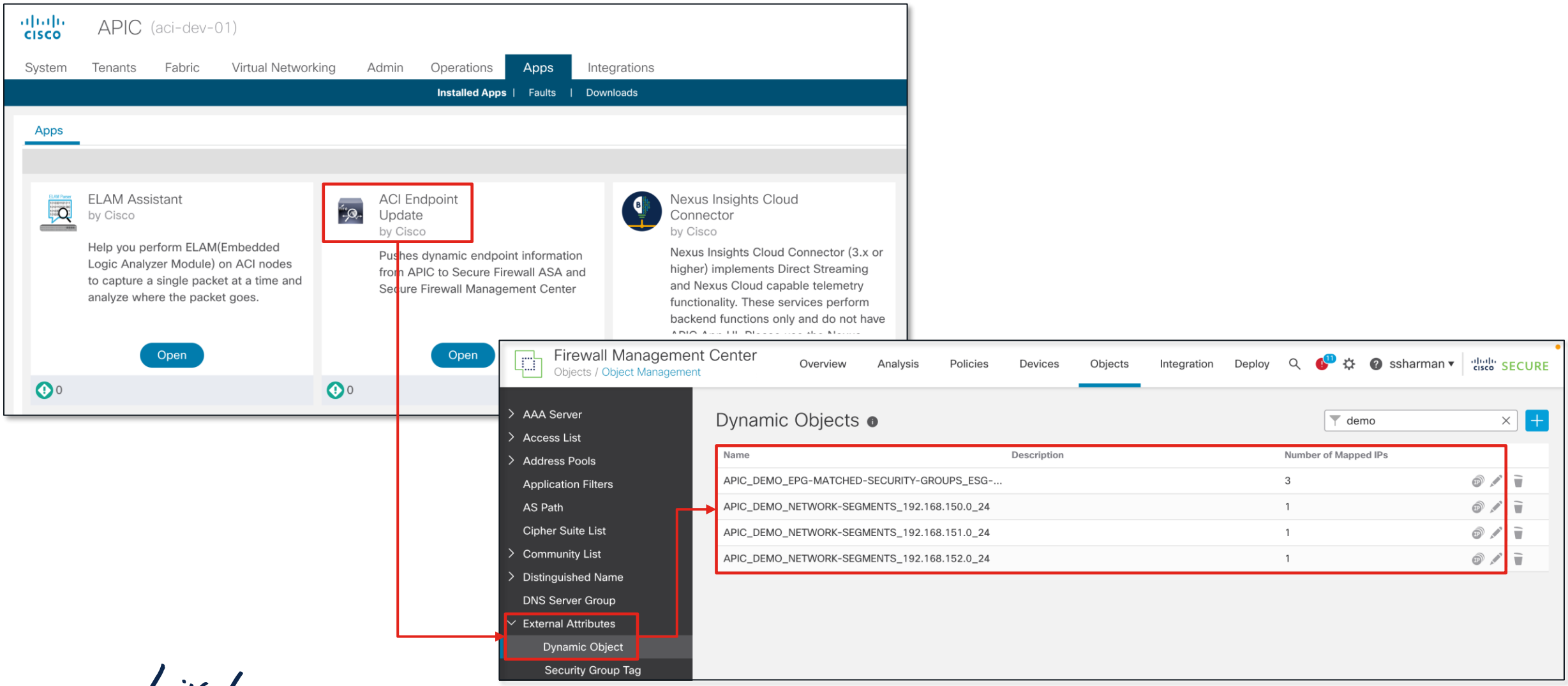
Benefits of virtual firewall / IPS

- 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)

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

ACI Endpoint Update App (optional)

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

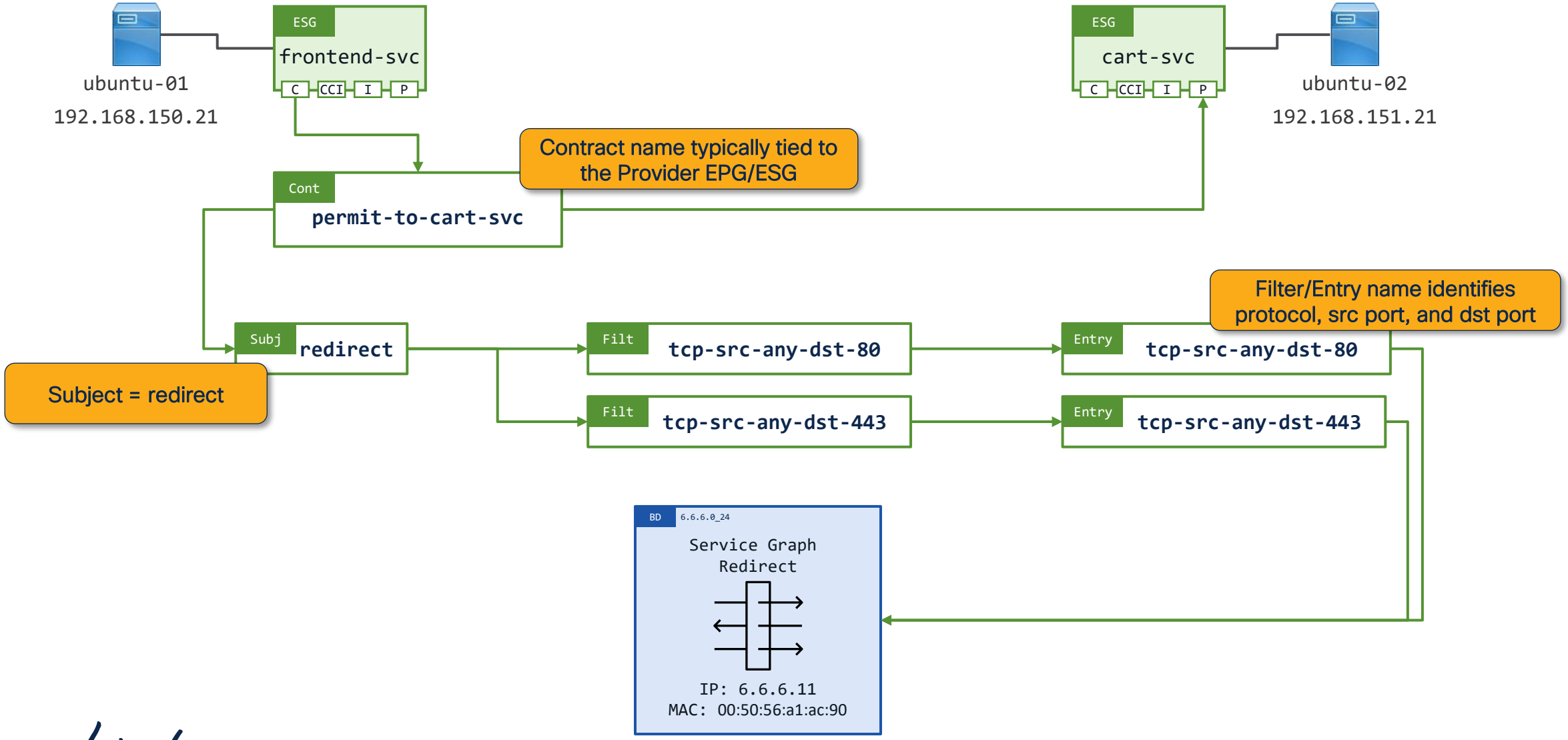


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

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

Redirect applied to all Filters under the Subject...

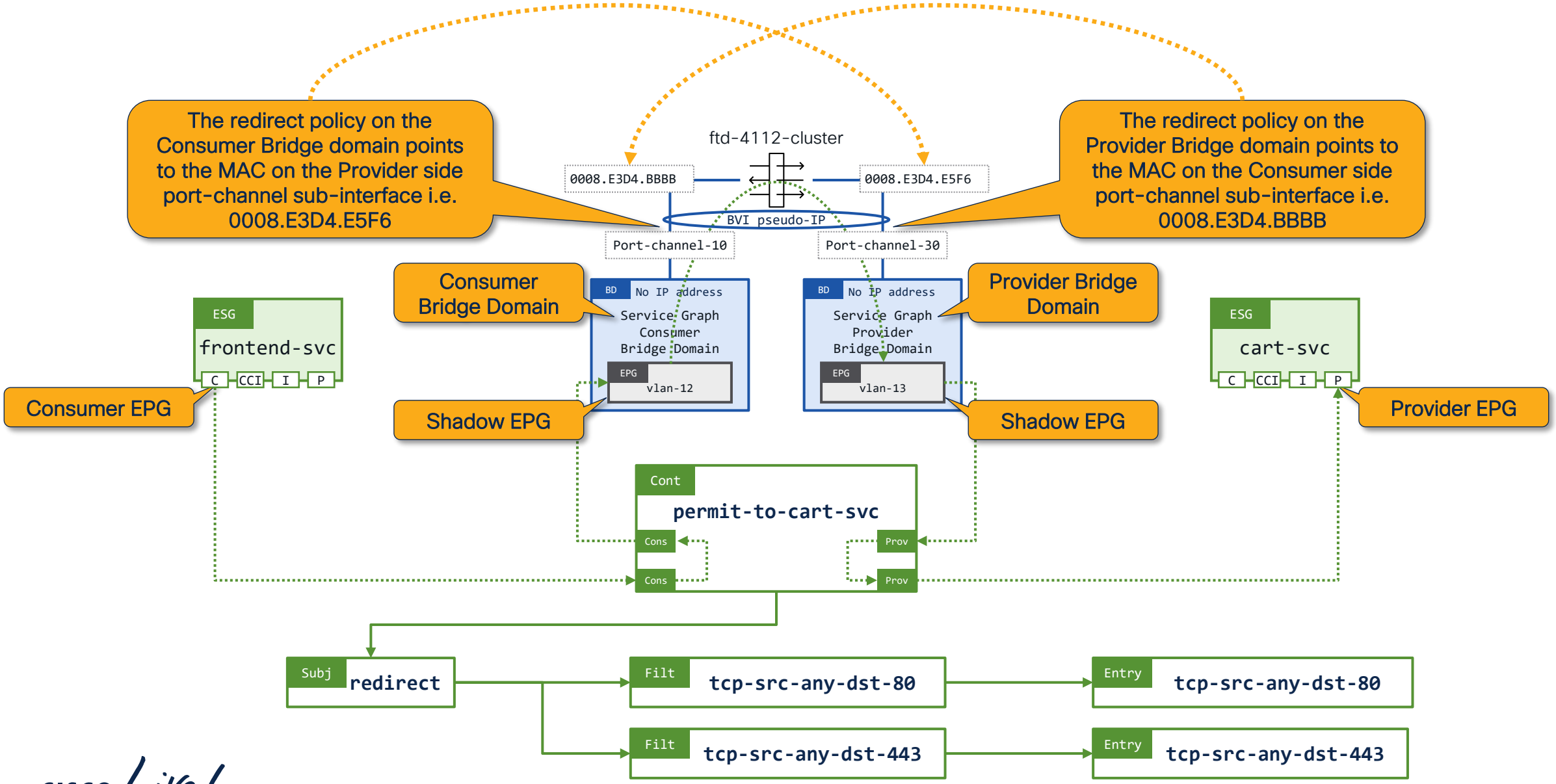


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

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

Two arm service graph – L2

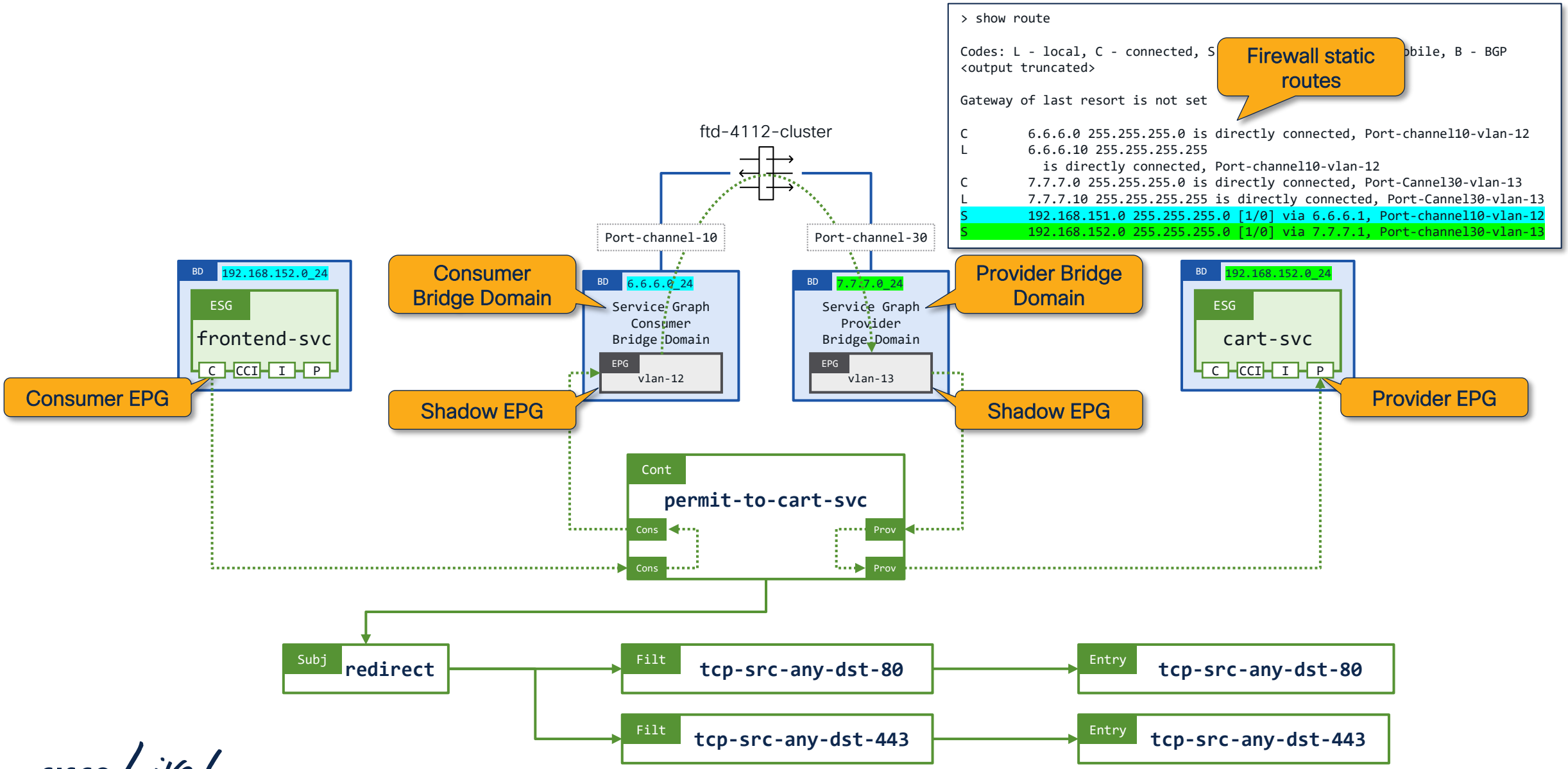


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Do not use Two Arm with L3 redirect...

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

Two arm service graph – L3 Cons to Prov



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

Two arm service graph – L3 Prov to Cons

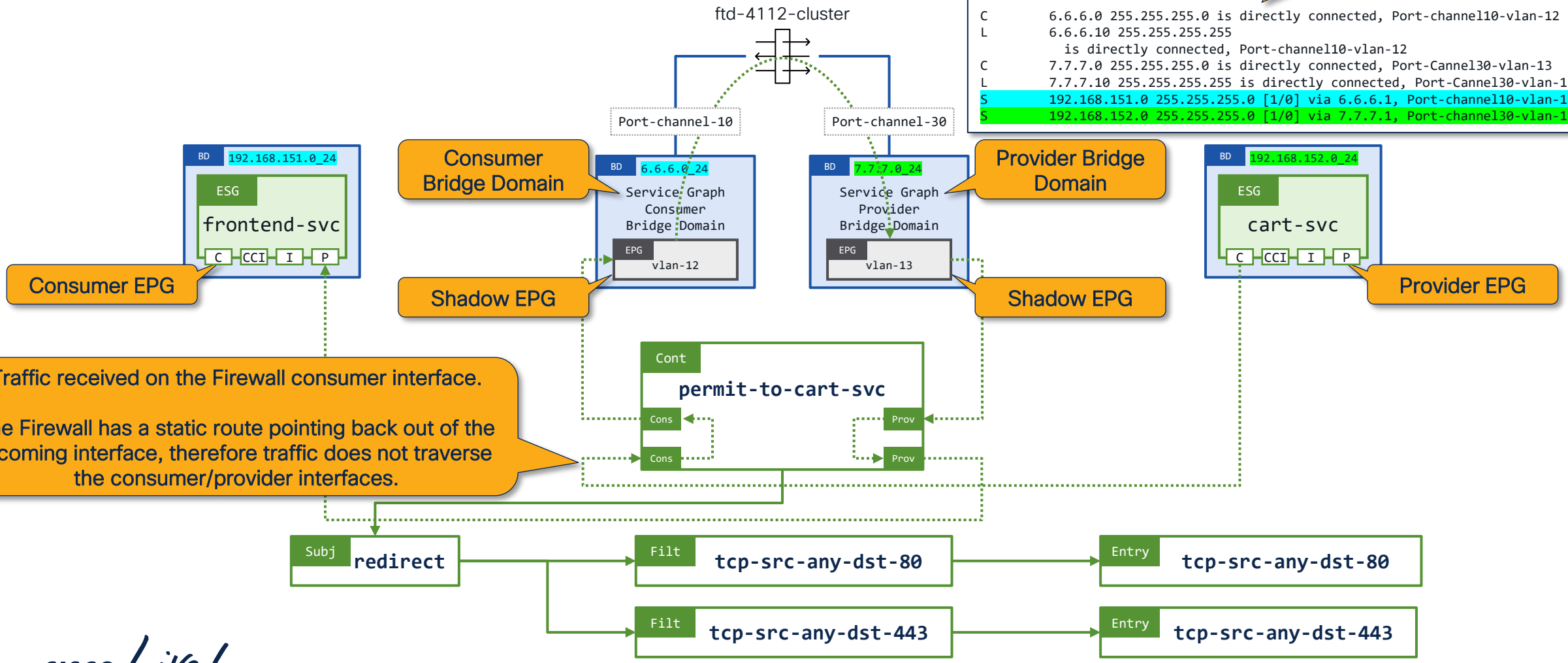
```
> show route

Codes: L - local, C - connected, S                    obile, B - BGP
<output truncated>

Gateway of last resort is not set

C        6.6.6.0 255.255.255.0 is directly connected, Port-channel10-vlan-12
L        6.6.6.10 255.255.255.255
           is directly connected, Port-channel10-vlan-12
C        7.7.7.0 255.255.255.0 is directly connected, Port-Cannel30-vlan-13
L        7.7.7.10 255.255.255.255 is directly connected, Port-Cannel30-vlan-13
S        192.168.151.0 255.255.255.0 [1/0] via 6.6.6.1, Port-channel10-vlan-12
S        192.168.152.0 255.255.255.0 [1/0] via 7.7.7.1, Port-channel30-vlan-13
```

Firewall static routes



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

Layer 2 vs Layer 3 firewall insertion

Layer 2 – two arm attached

- Transparent IPS mode
- Slightly higher throughput
- No routing

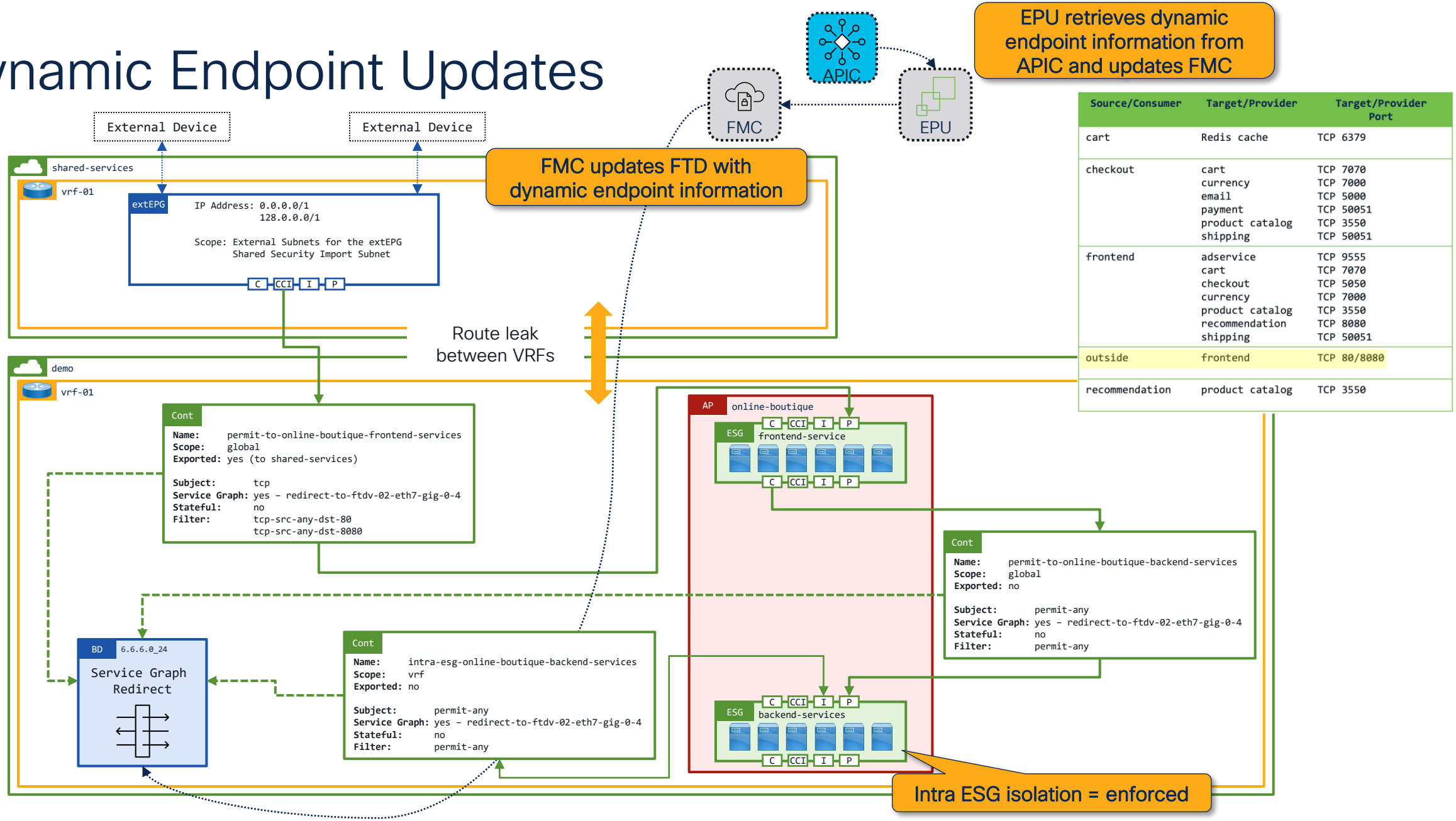
- **Layer 3 – one arm attached**
- Simple “default” routing
- Easier installation method
- Used by more than 95% of customers

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

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

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

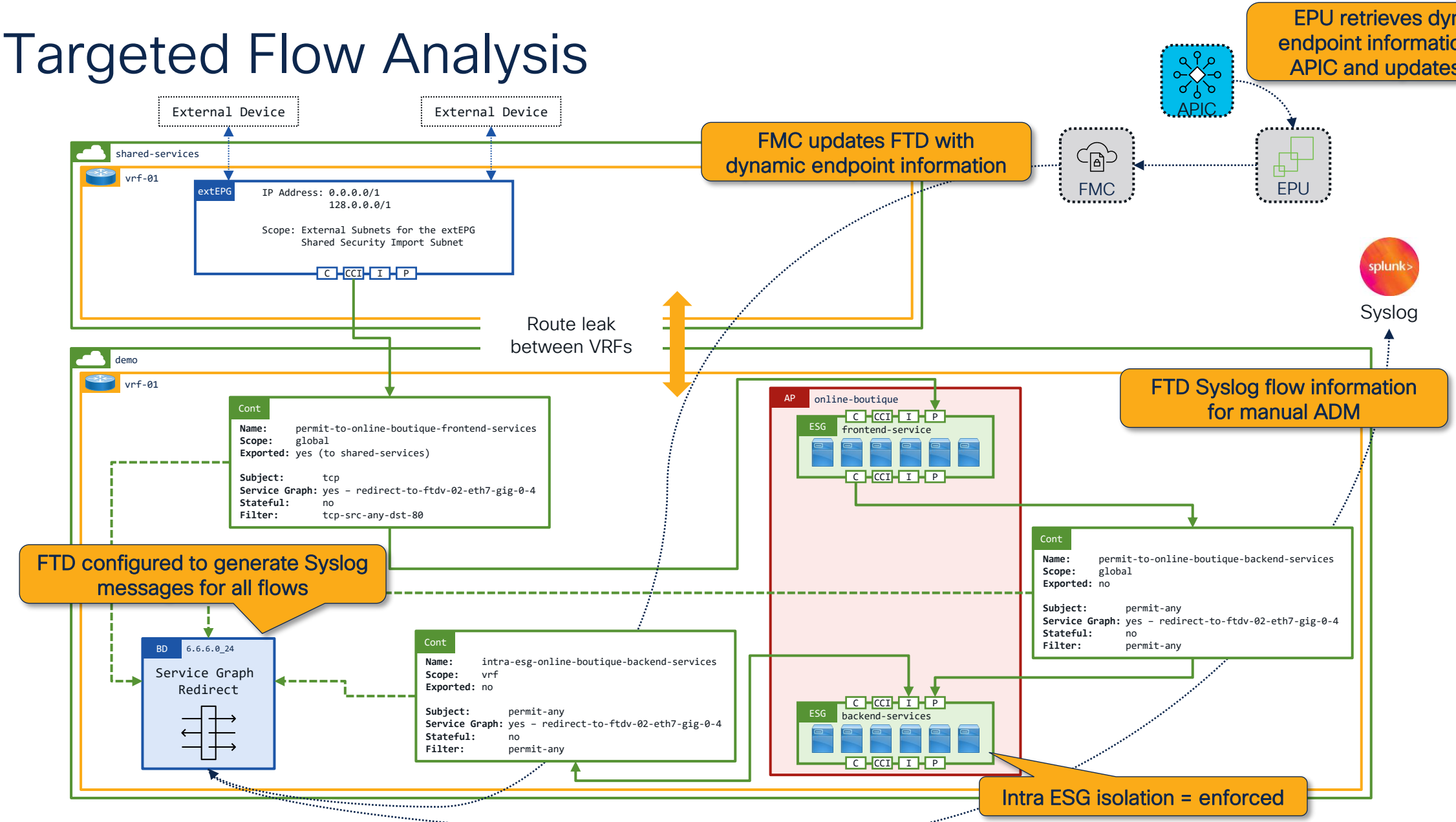
Dynamic Endpoint Updates



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

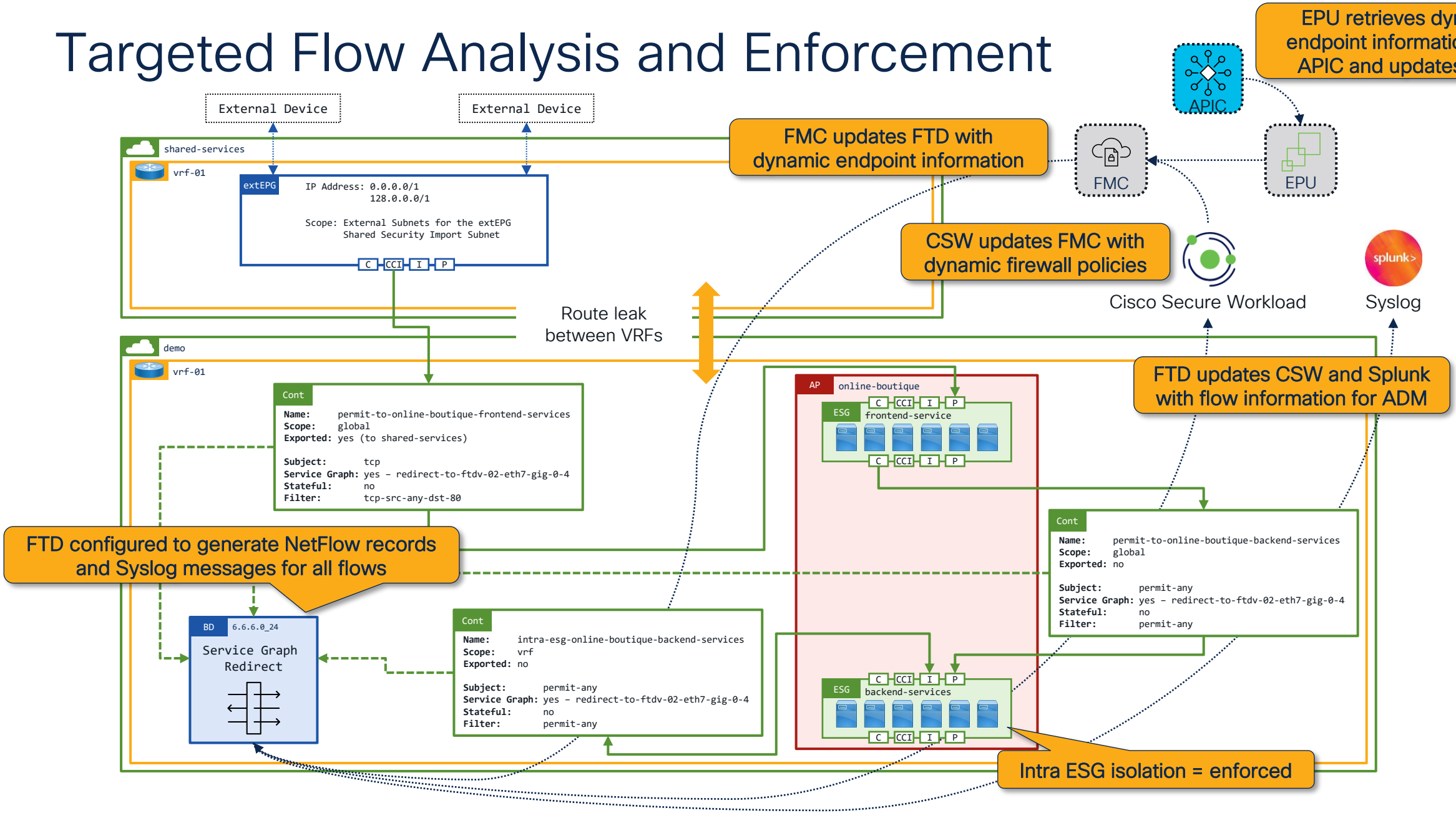
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Targeted Flow Analysis



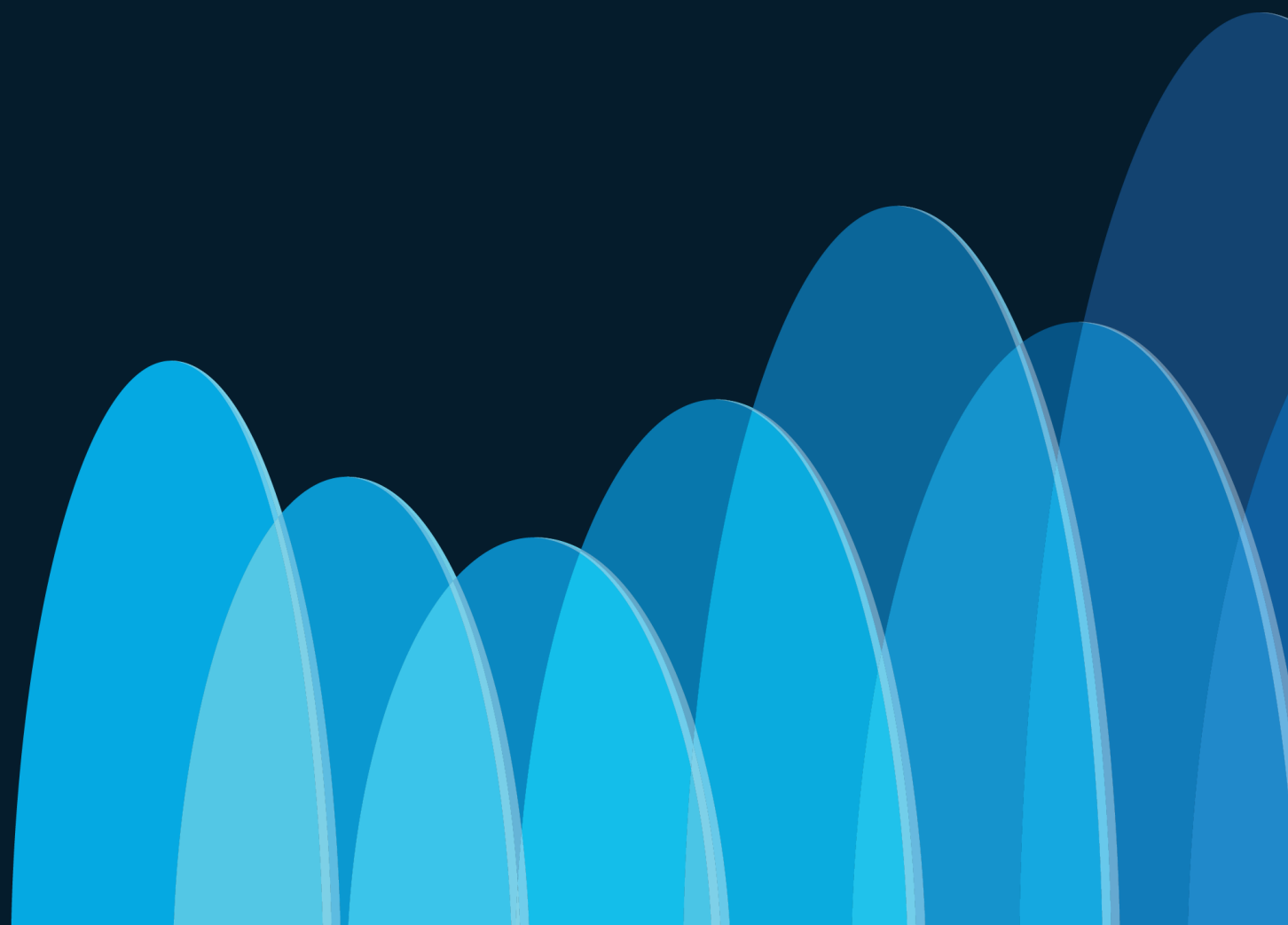
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Targeted Flow Analysis and Enforcement



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

Tightening Security...

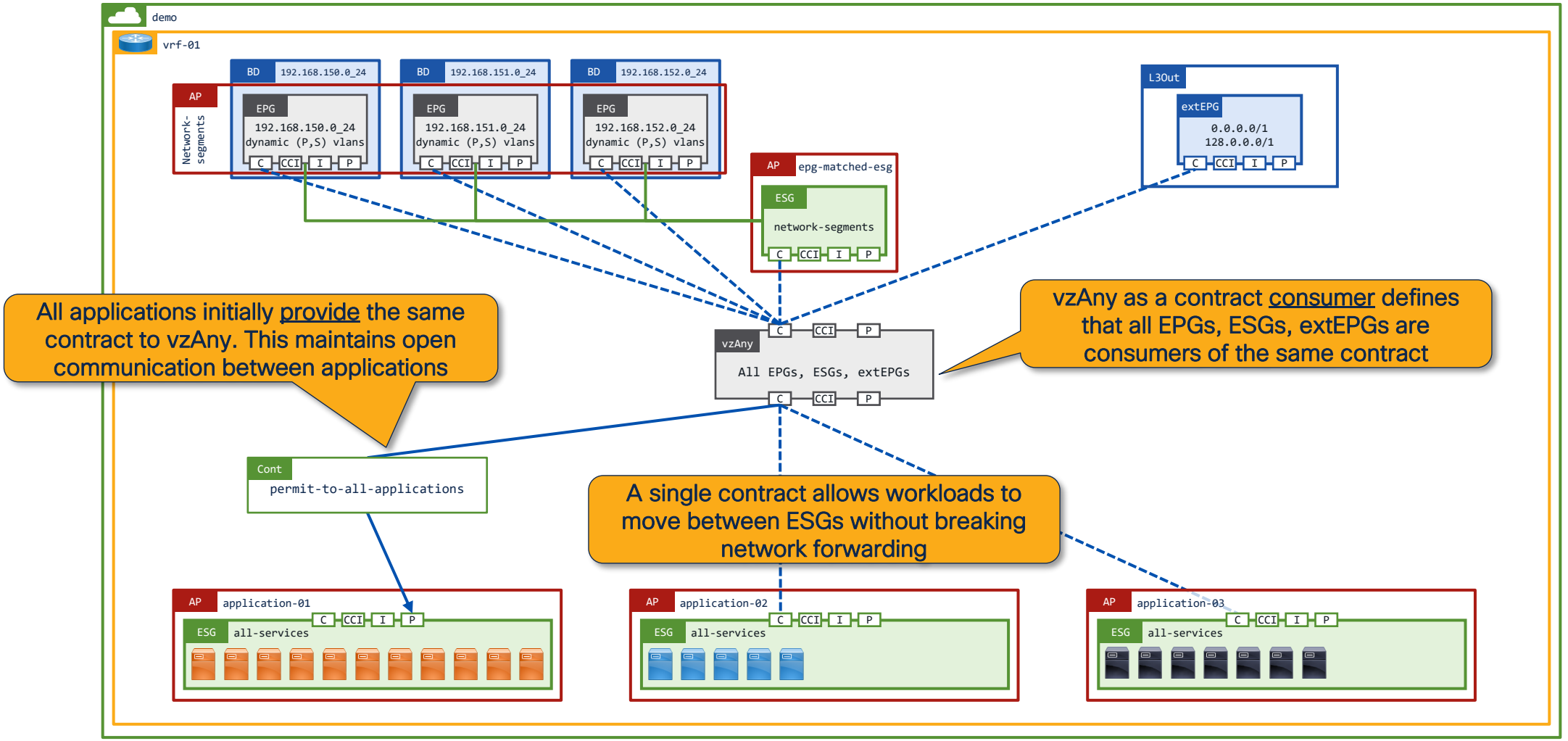


cisco Live!

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

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

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

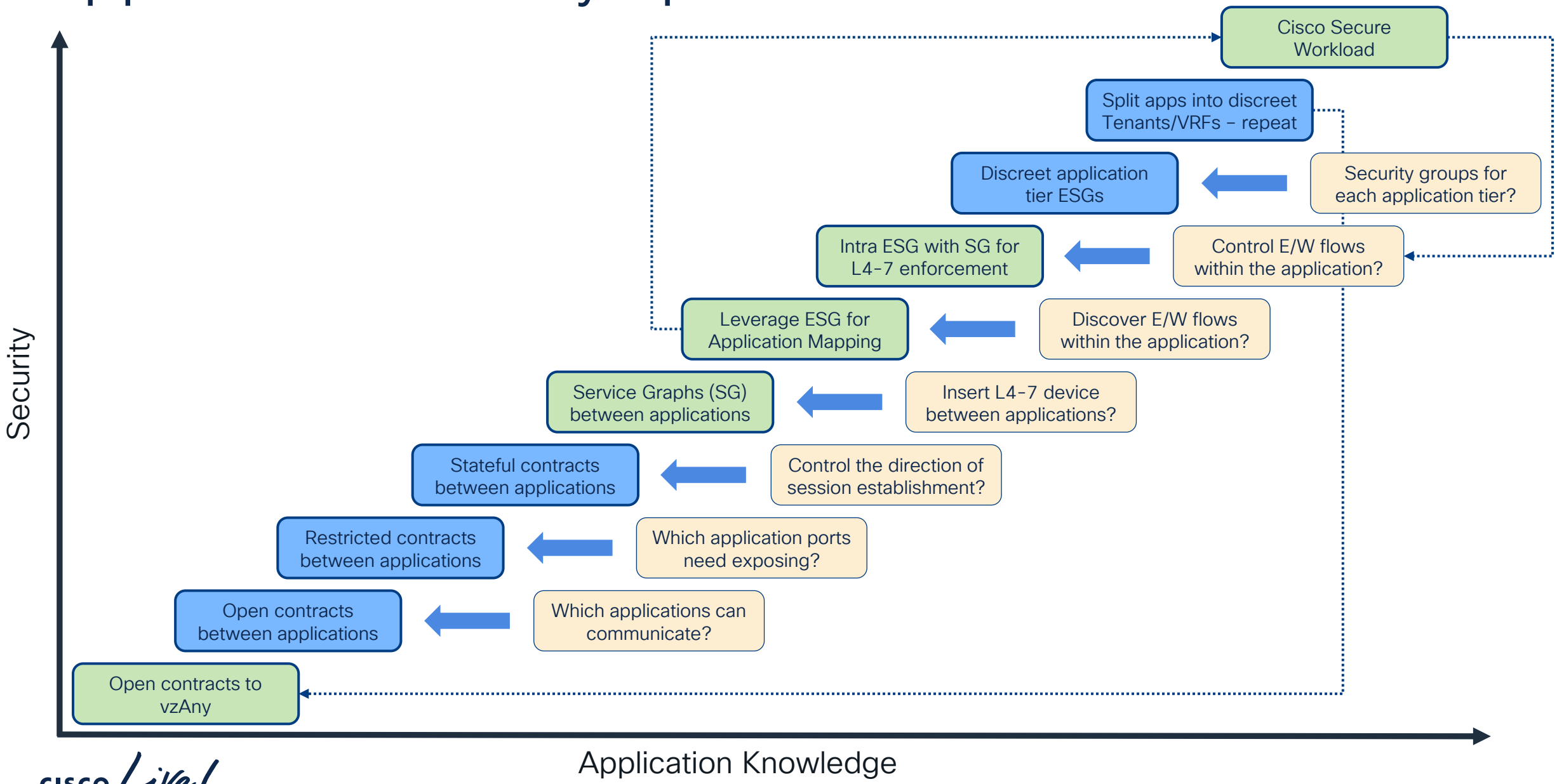


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 2: Decide how to tighten security…

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

Application security options...

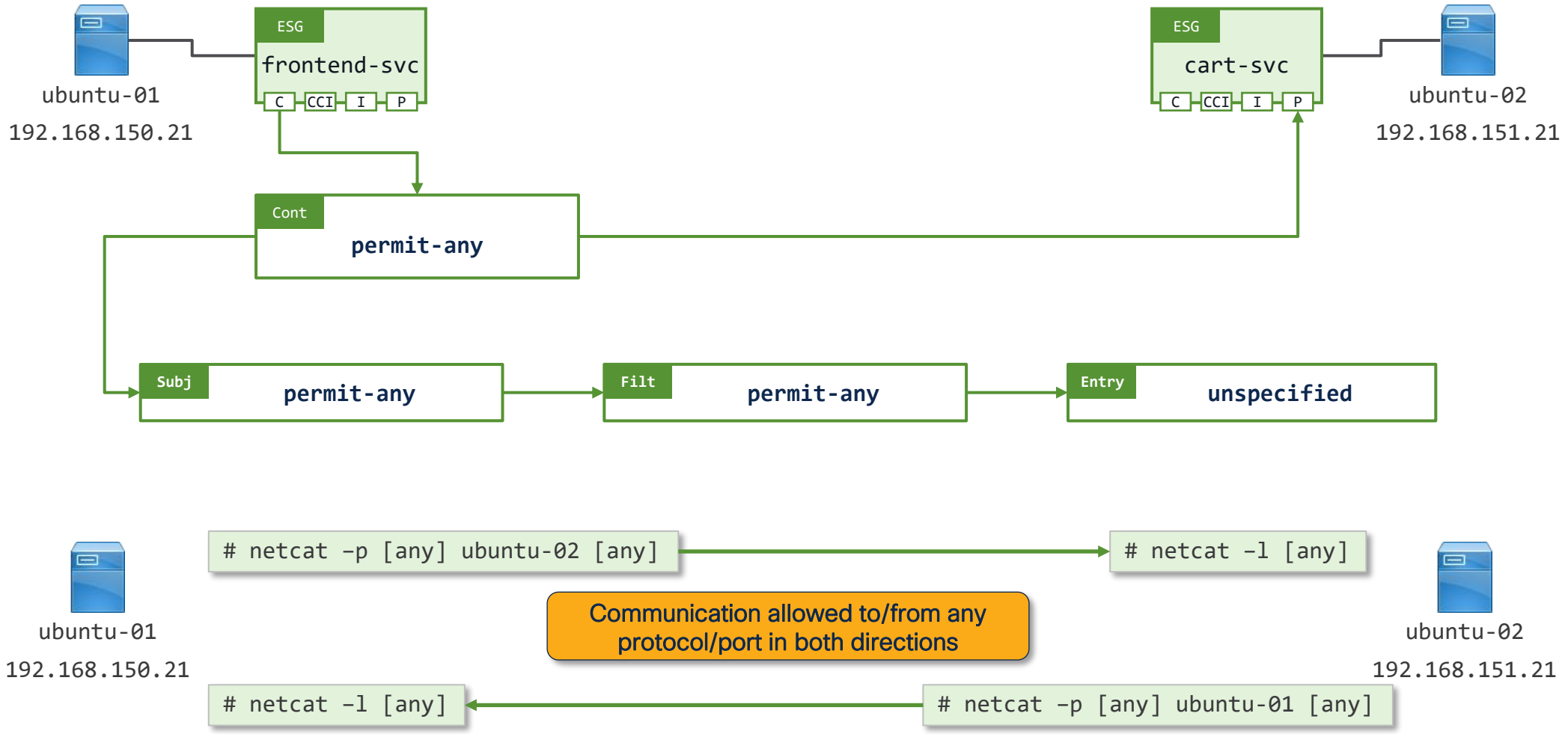


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Remember this from a little earlier...

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

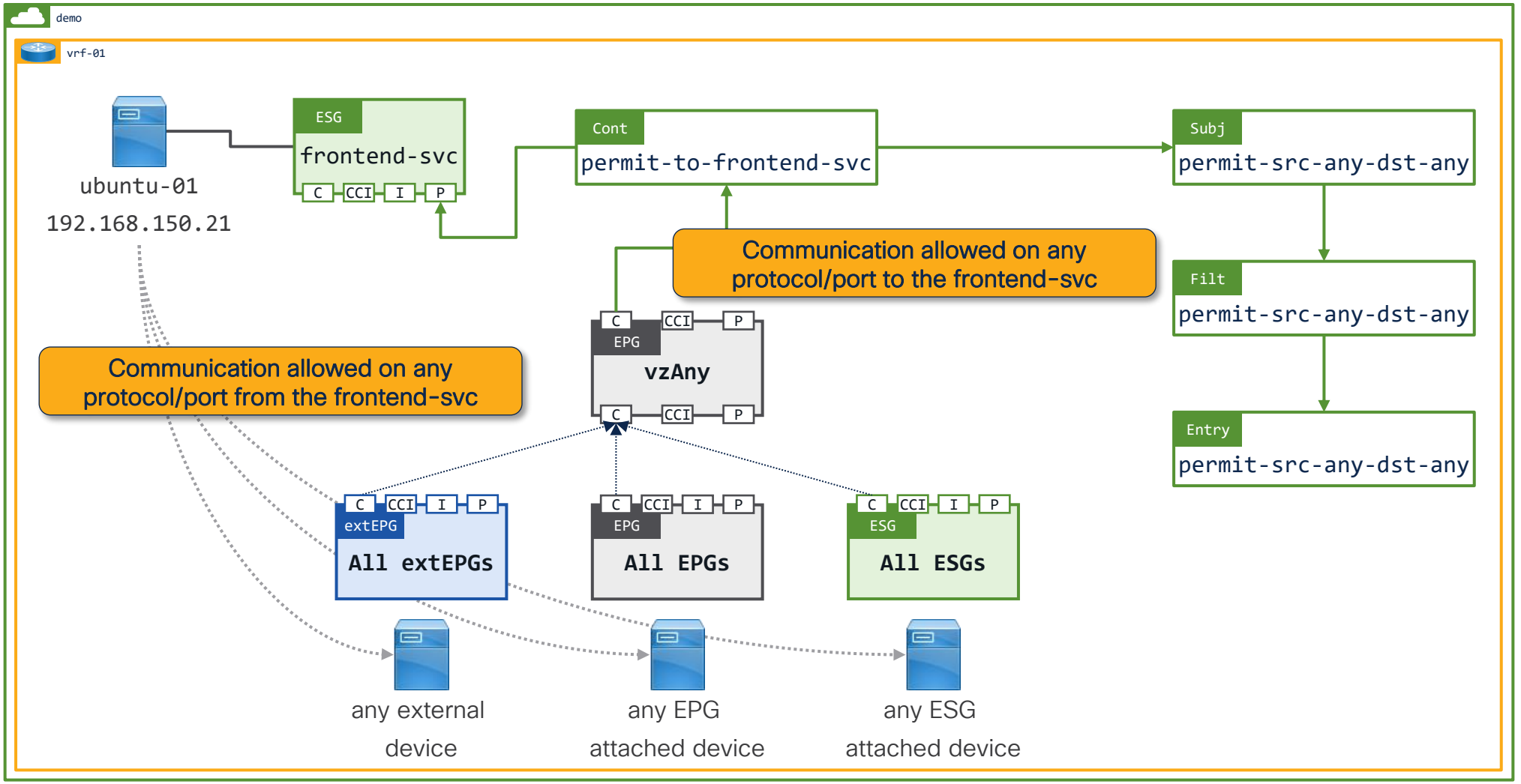
permit any/any



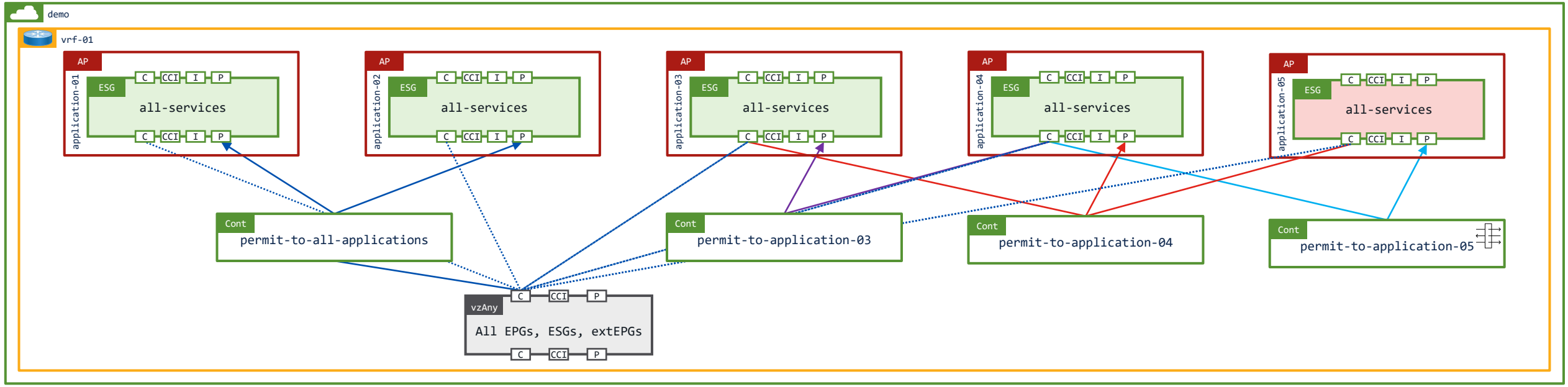
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

permit any/any with vzAny

Exercise caution when using vzAny...!



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



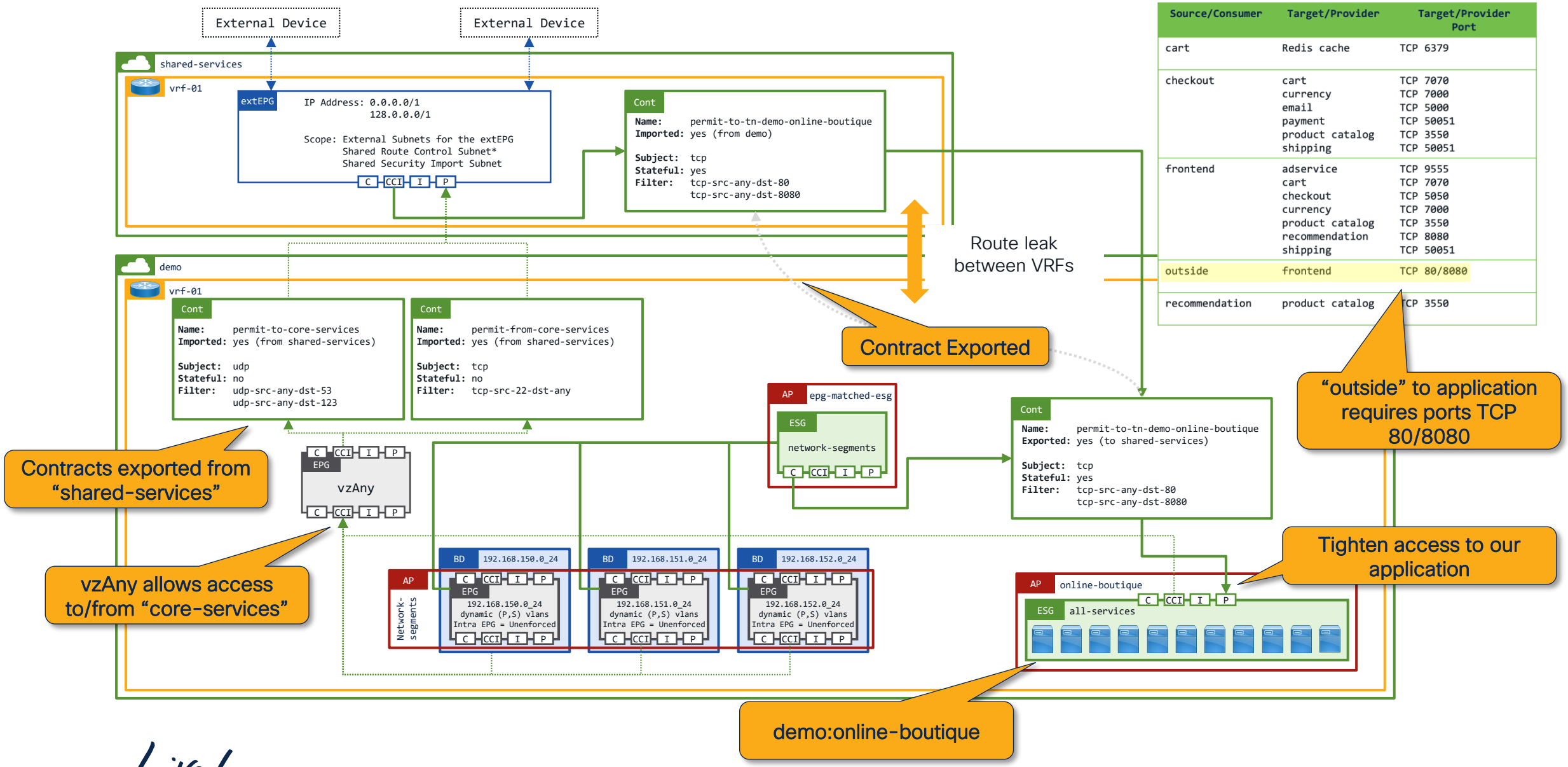
Consumer	Contract	Filter	Provider	Notes
vzAny (all EPGs/ESGs/extEPGs)	permit-to-all-applications	permit-src-any-dst-any	application-01	vzAny with permit-src-any-dst-any allows bi-directional communication on any port between **all** applications
vzAny (all EPGs/ESGs/extEPGs)	permit-to-all-applications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

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

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

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

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
	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

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

Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

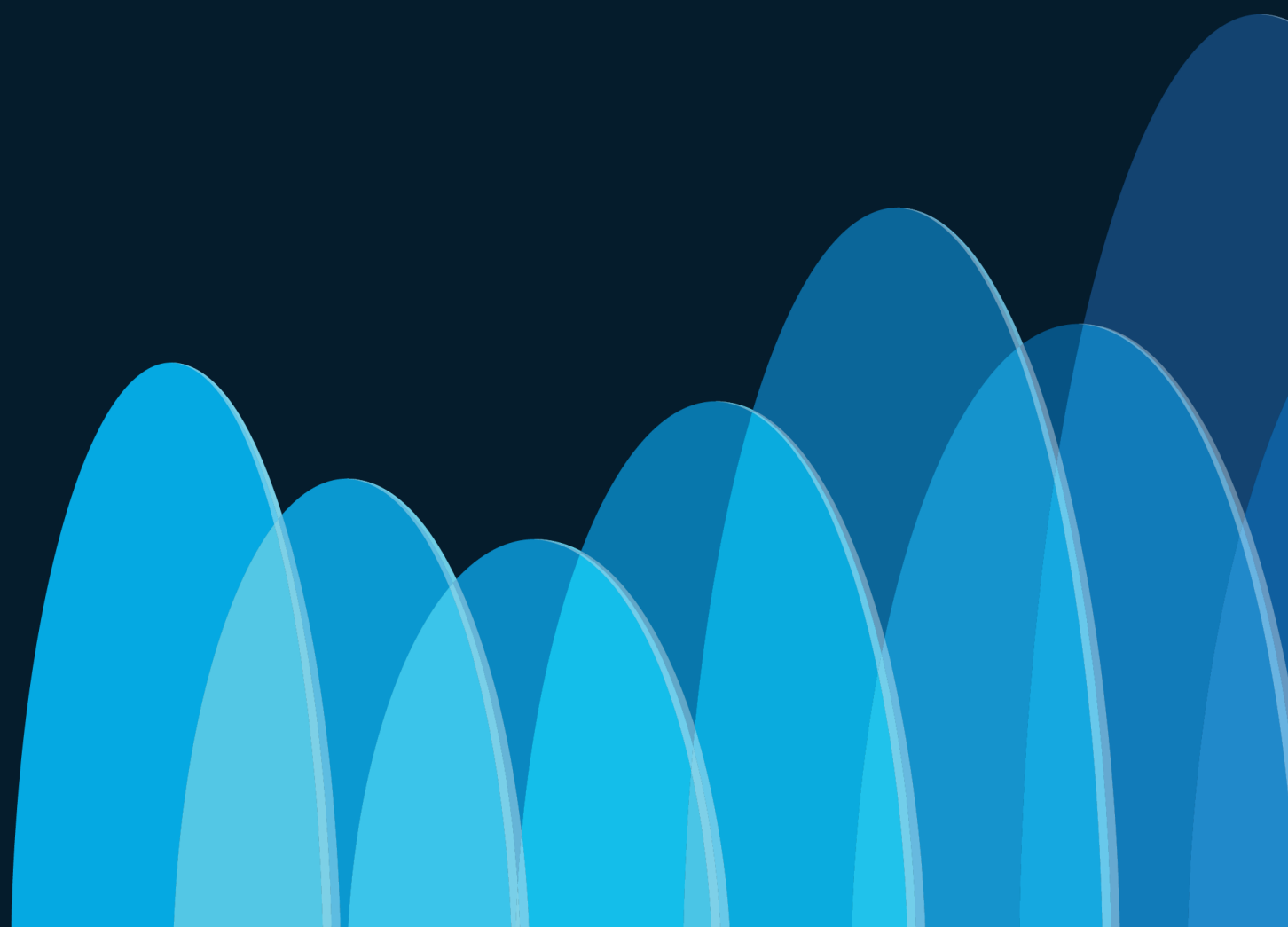
Understanding ACI security...

External Connectivity...

Increasing Security...

Automation Blueprints...

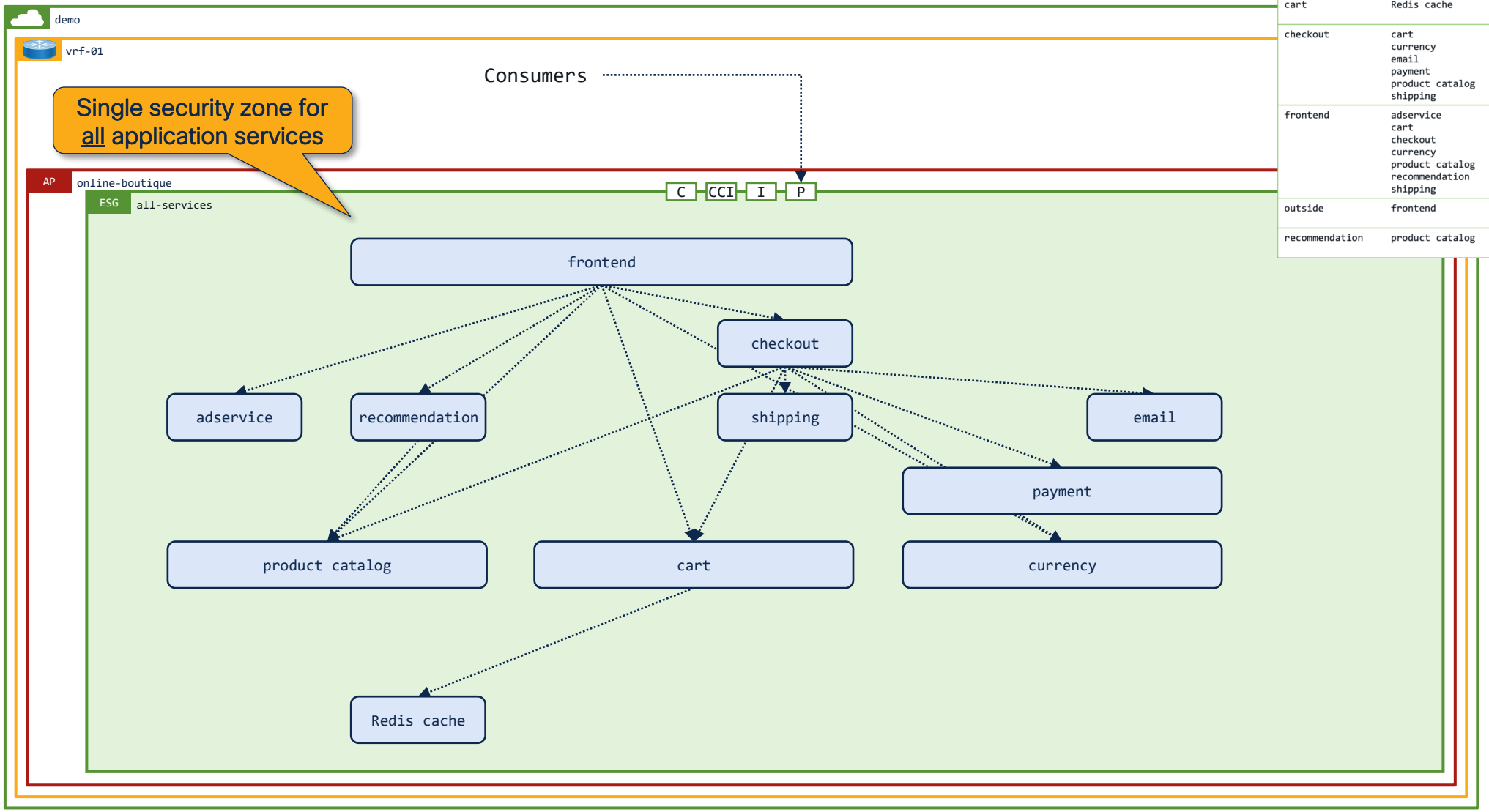
Wrapping up...



cisco Live!

Application tiers across subnets

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

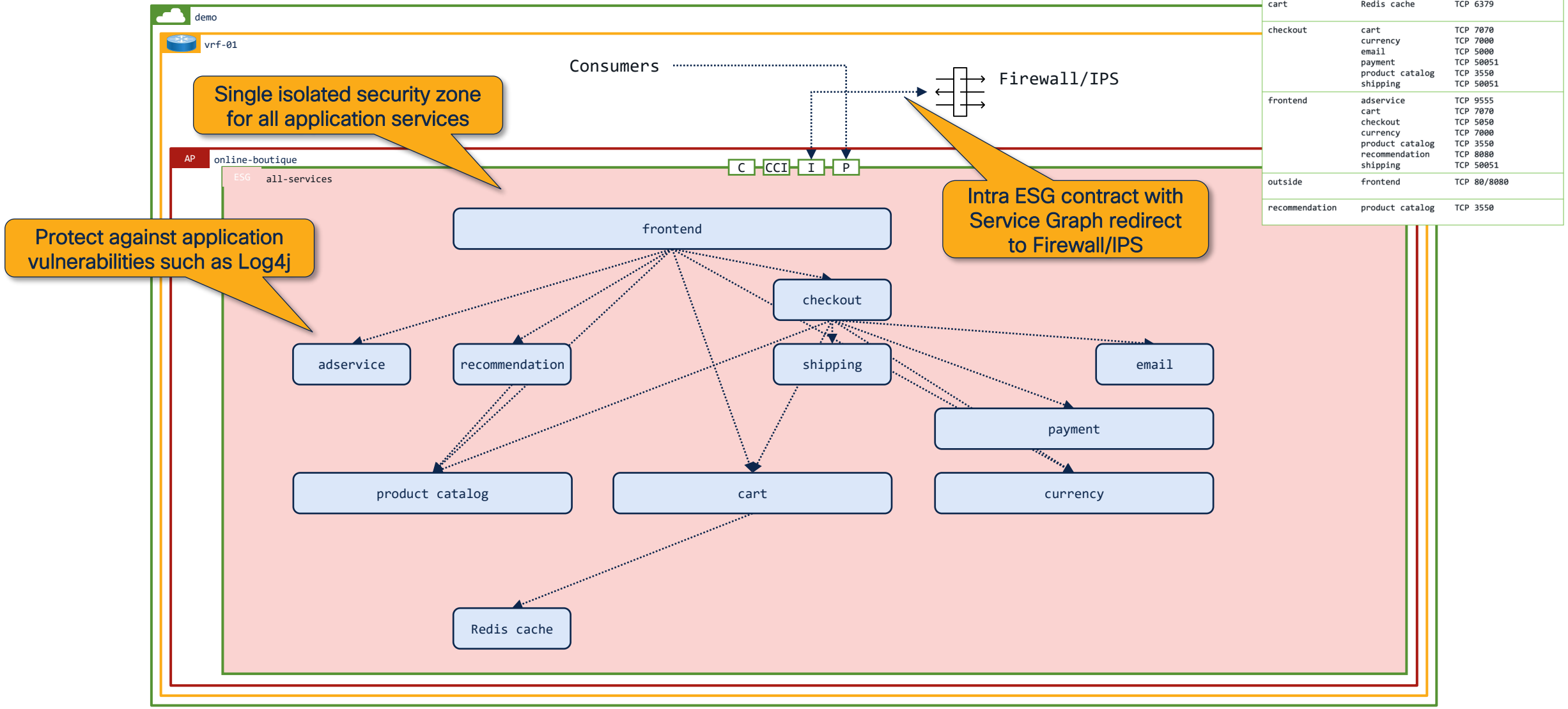


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP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

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

Application tiers across subnets

Application Centric Blueprint #2 – Intra ESG Isolation

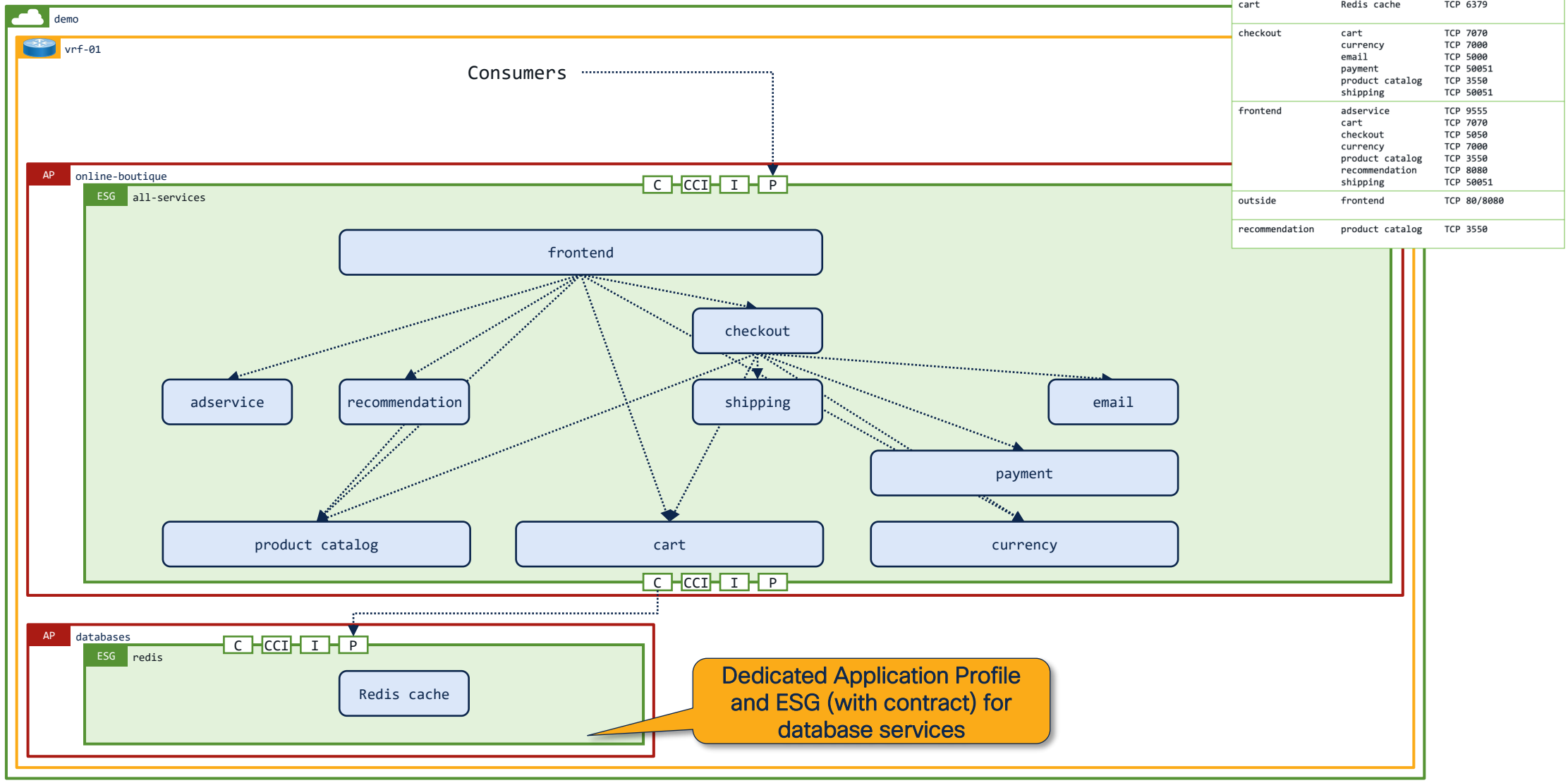


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP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

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

Application tiers across subnets

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

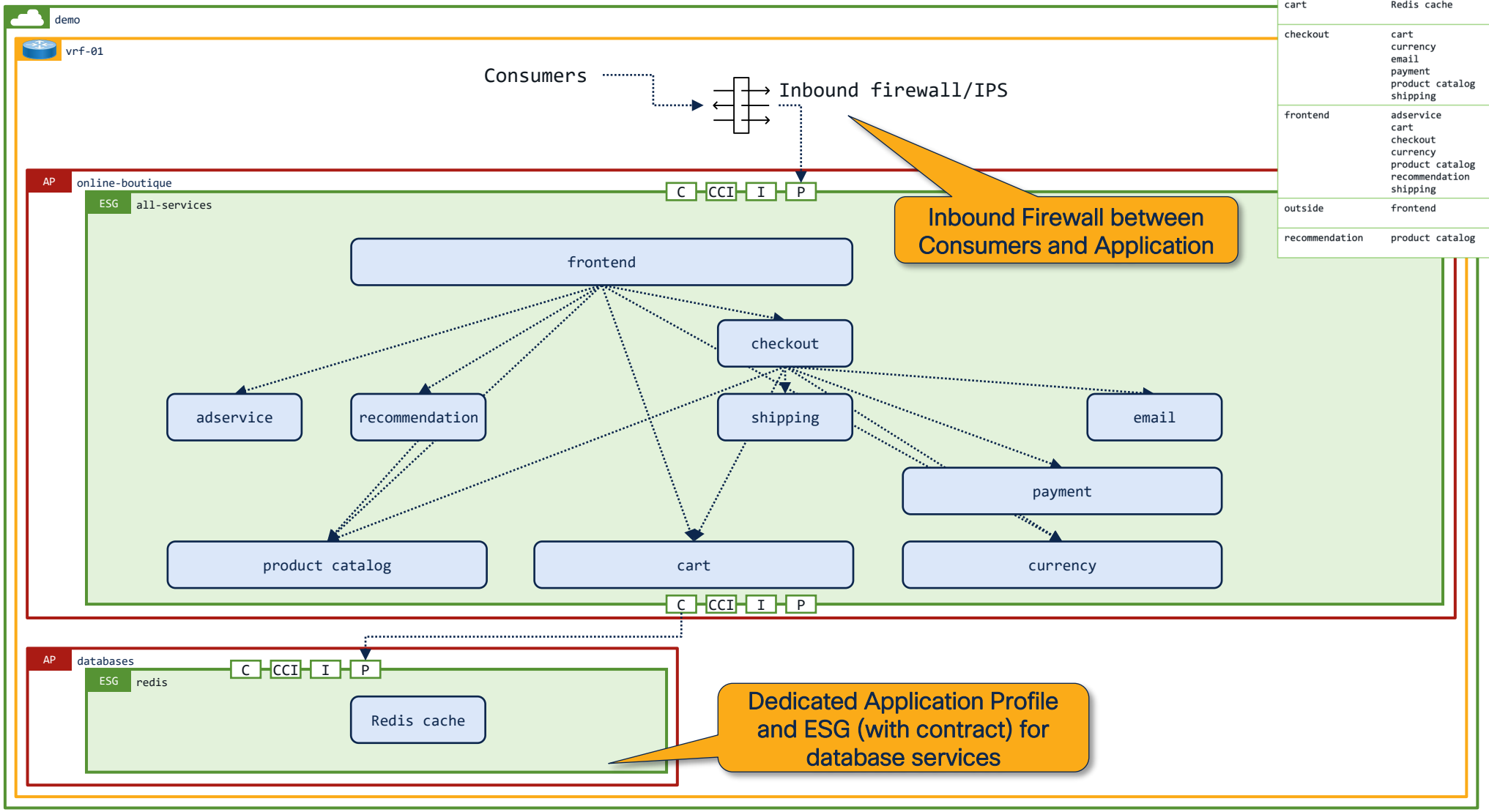


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP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

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

Application tiers across subnets

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

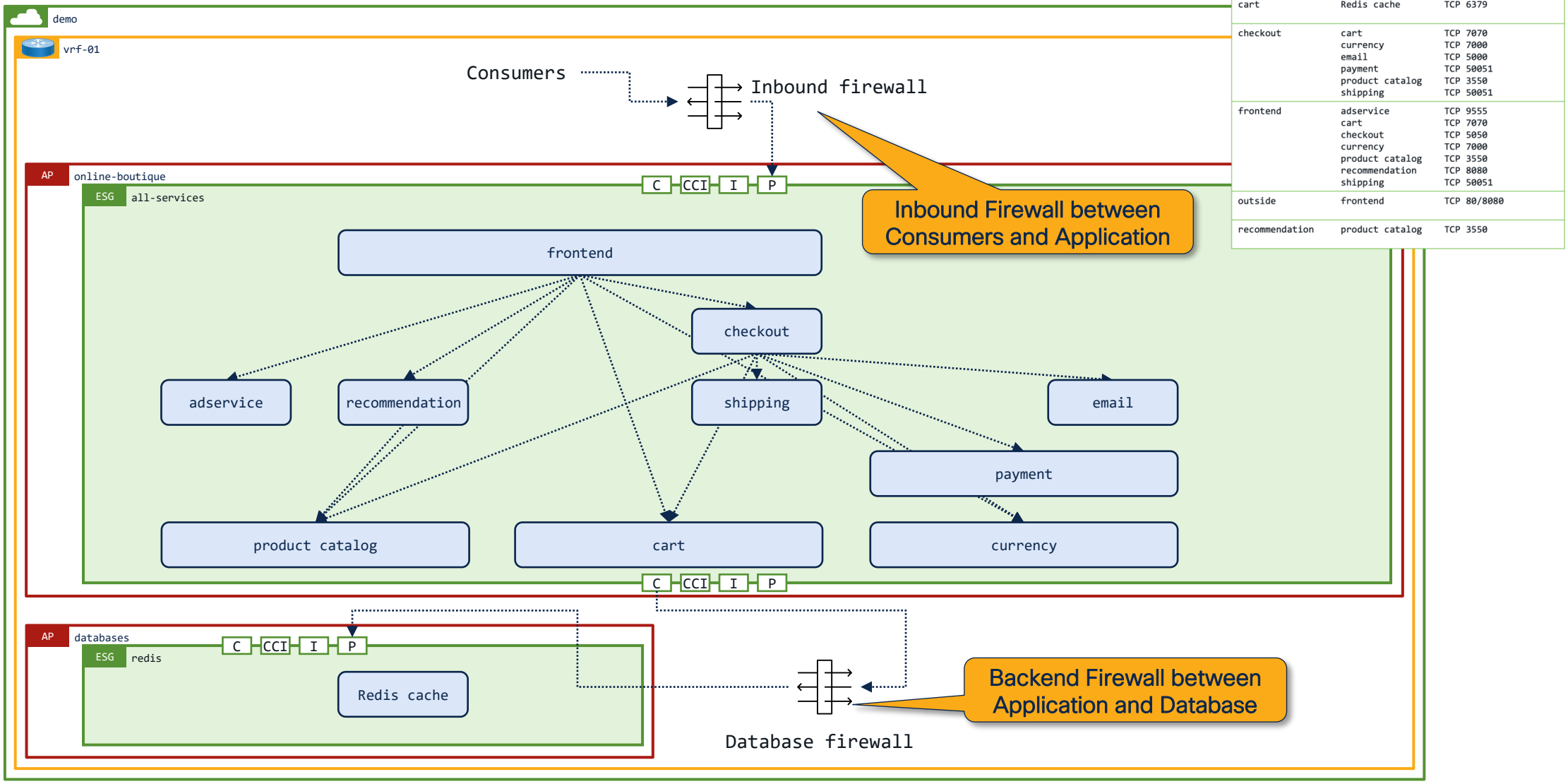


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP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

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

Application tiers across subnets

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

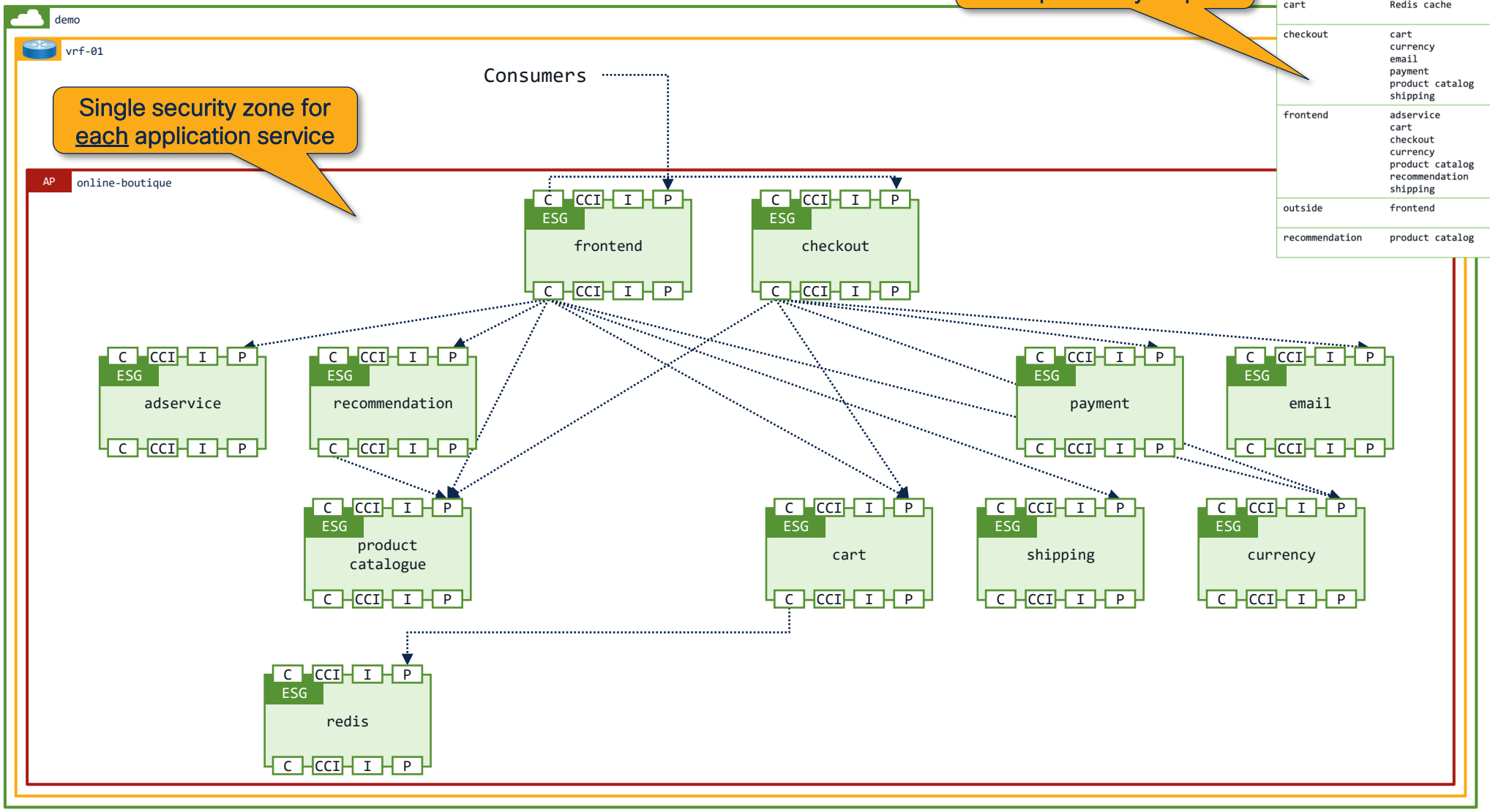


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP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

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

Application tiers across subnets

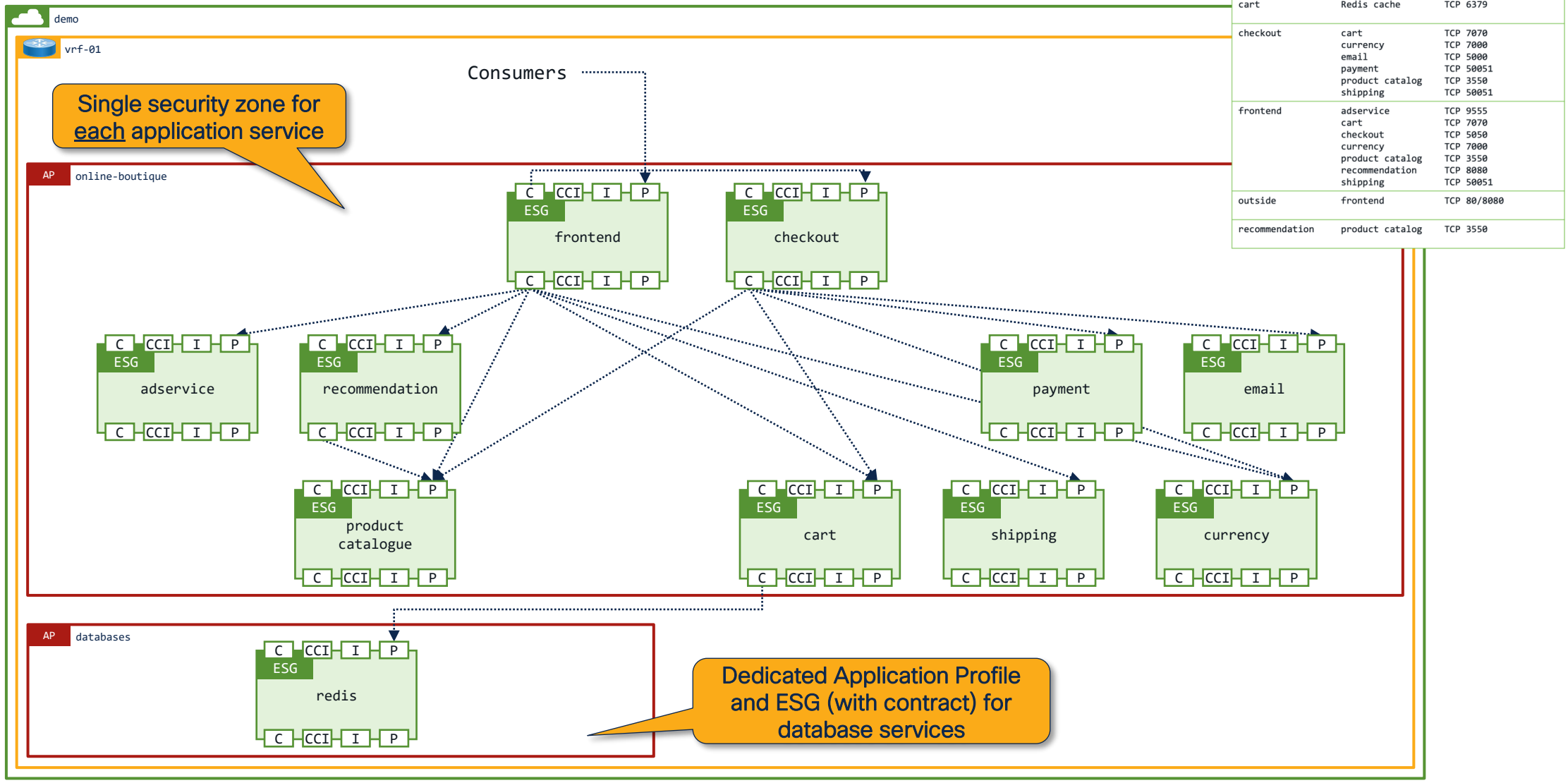
Application Centric Blueprint #6 – ESG per application tier



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

Application tiers across subnets

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

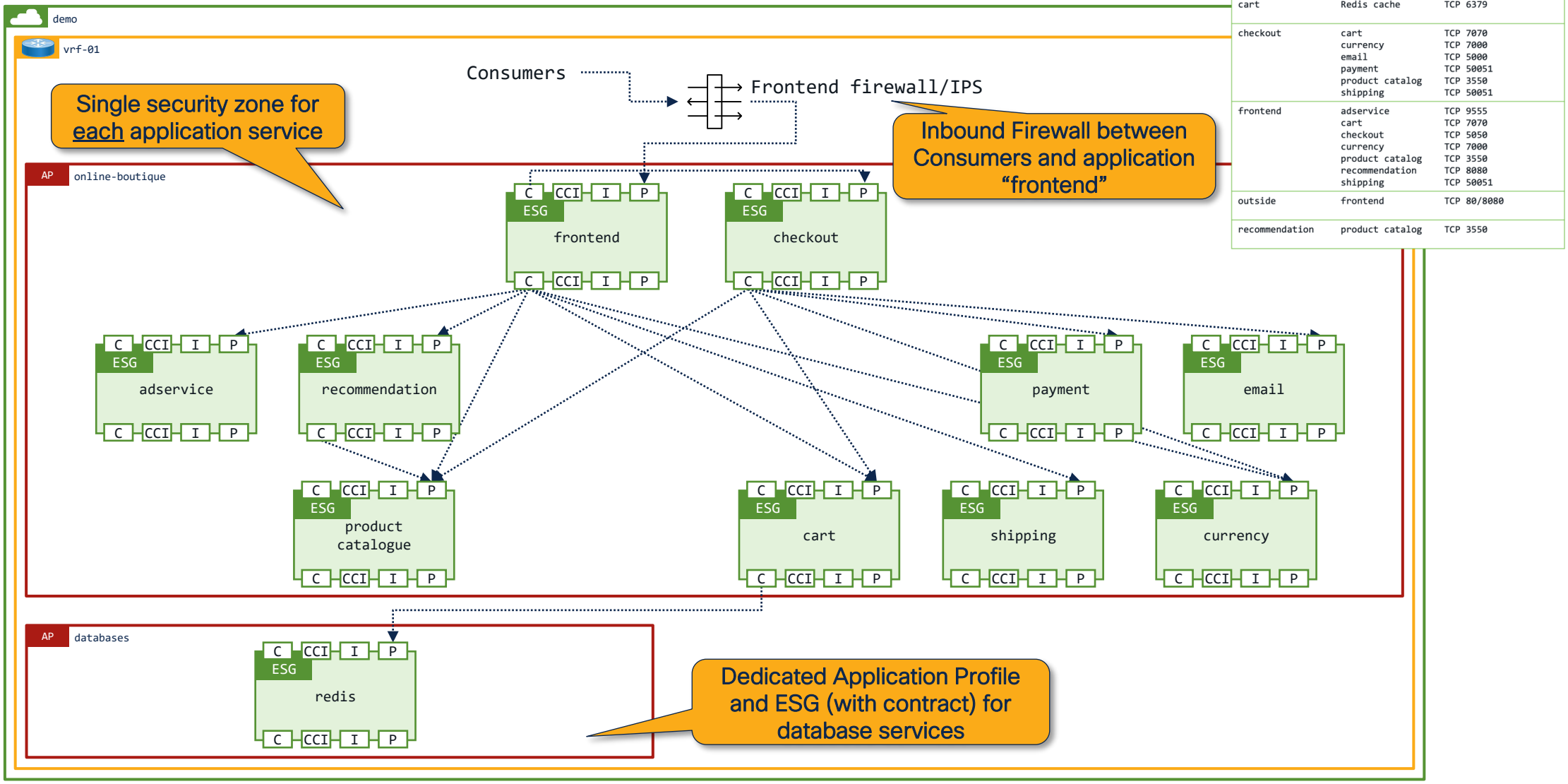


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP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

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

Application tiers across subnets

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

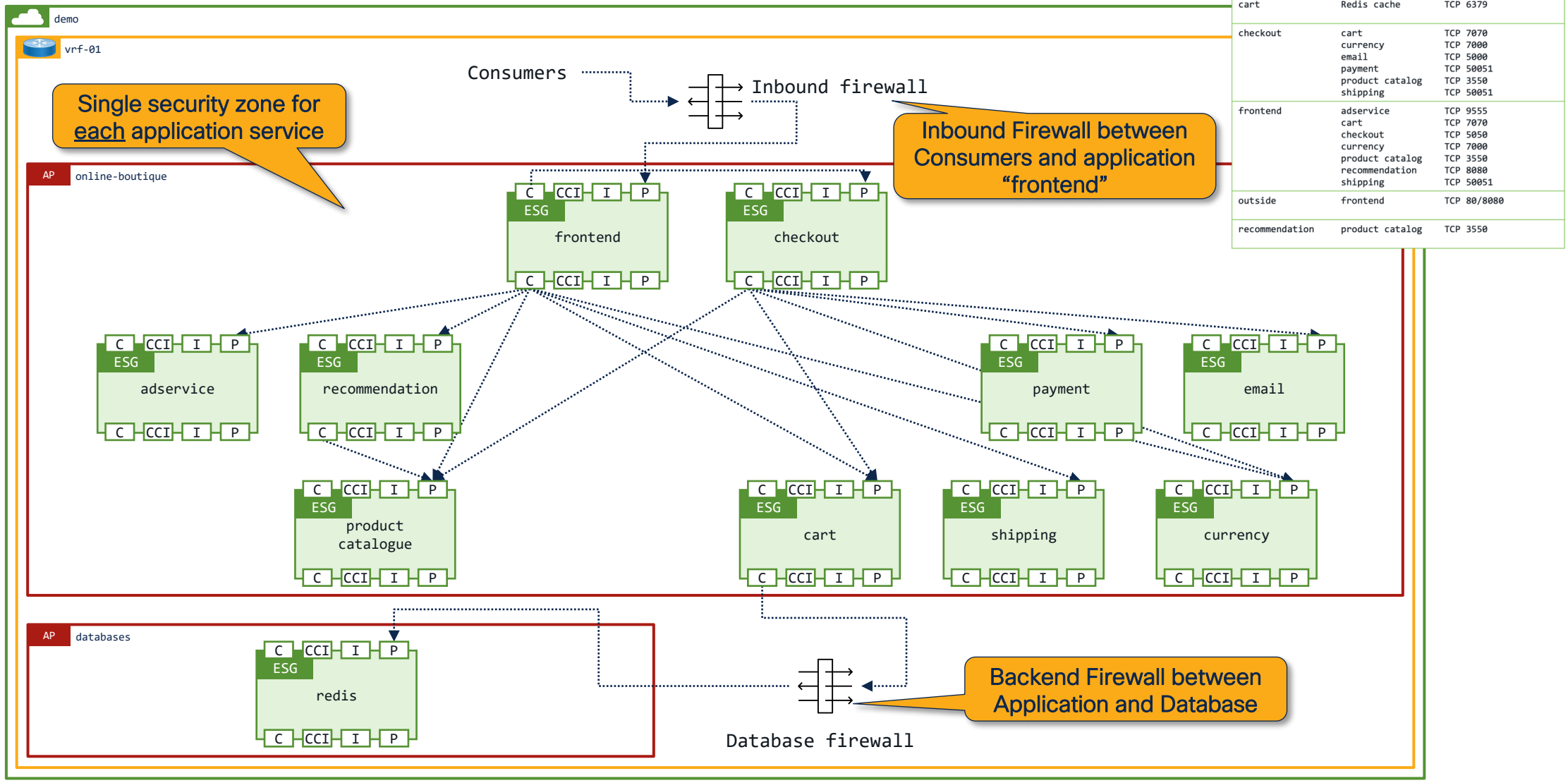


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP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

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

Application tiers across subnets

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

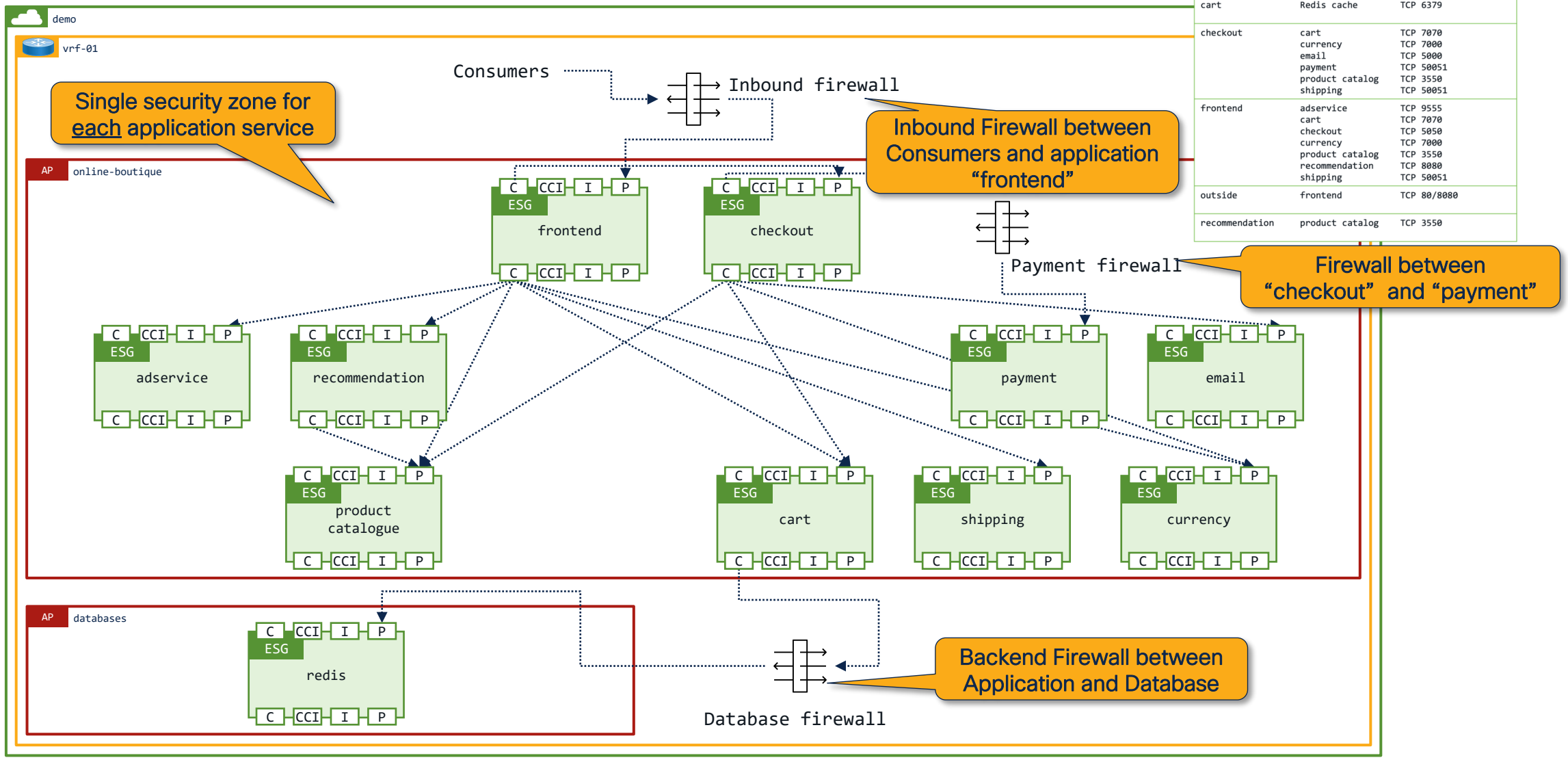


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP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

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

Application tiers across subnets

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



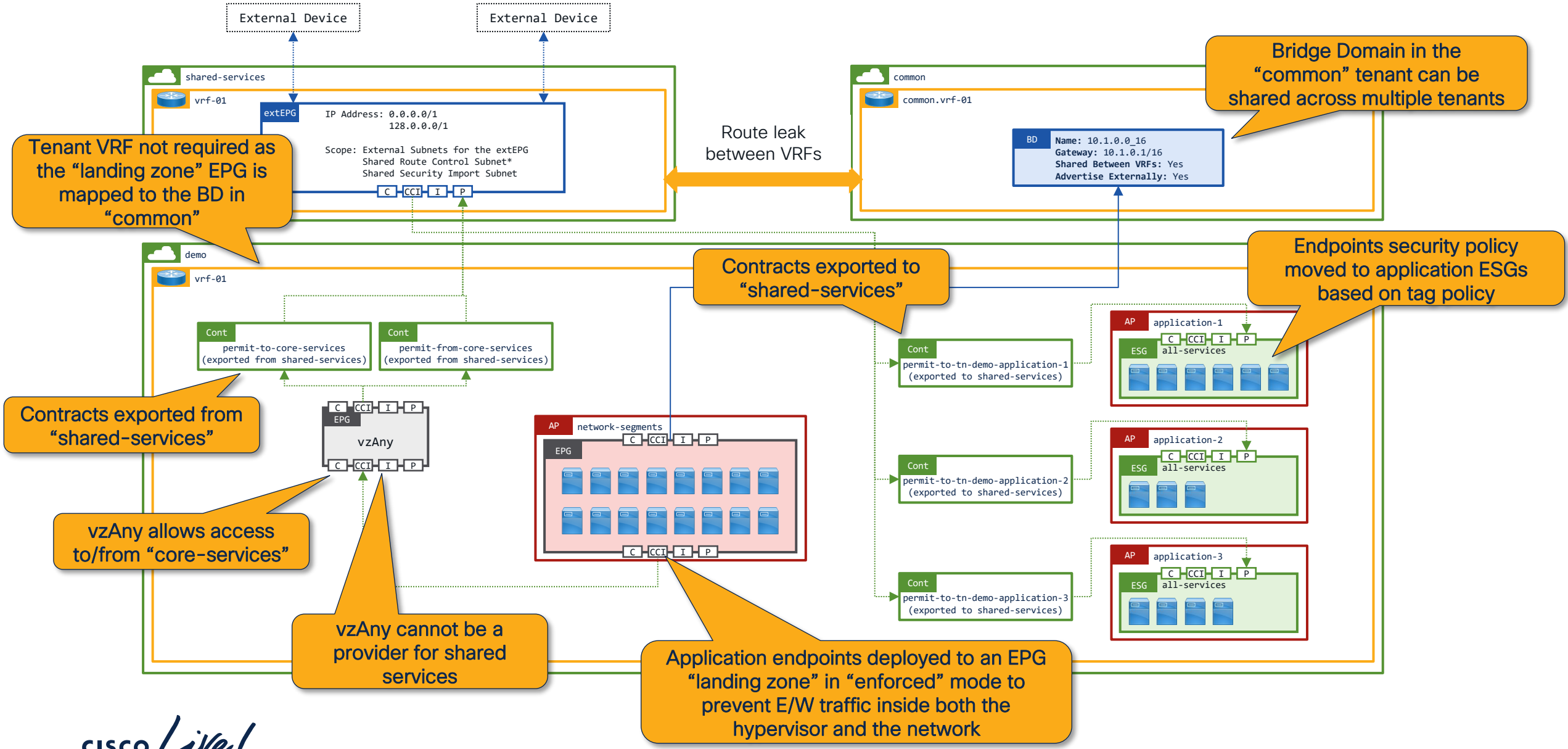
Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart	TCP 7070
	currency	TCP 7000
	email	TCP 5000
	payment	TCP 50051
	product catalog	TCP 3550
	shipping	TCP 50051
frontend	adservice	TCP 9555
	cart	TCP 7070
	checkout	TCP 5050
	currency	TCP 7000
	product catalog	TCP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

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

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

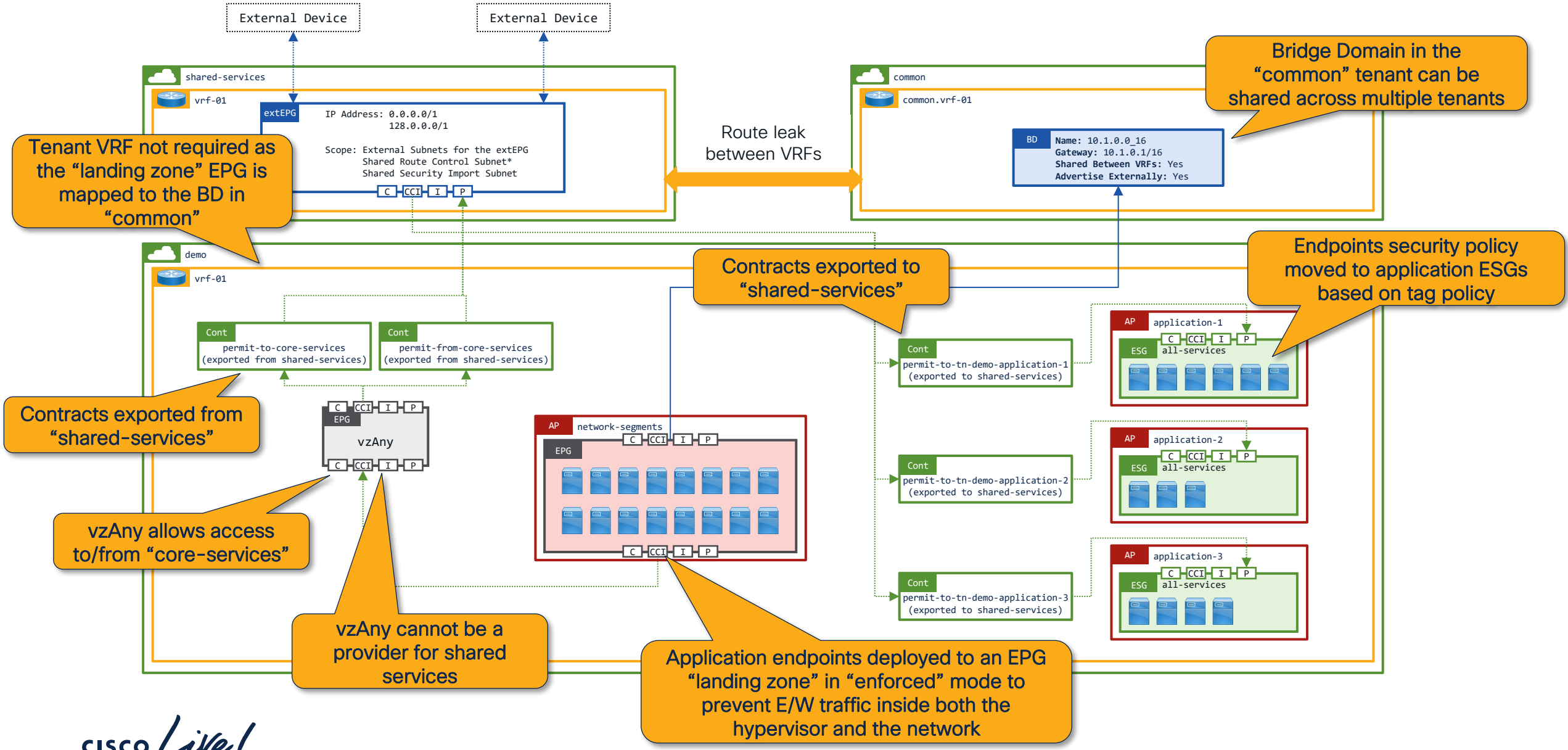
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Example Internal Private Cloud Design – shared subnet(s)



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

Example Internal Private Cloud Design – Auto Cleanup Isolation



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

Setting the scene...

Designing your Tenants...

Switching to Application Centric mode...

Working with ESGs...

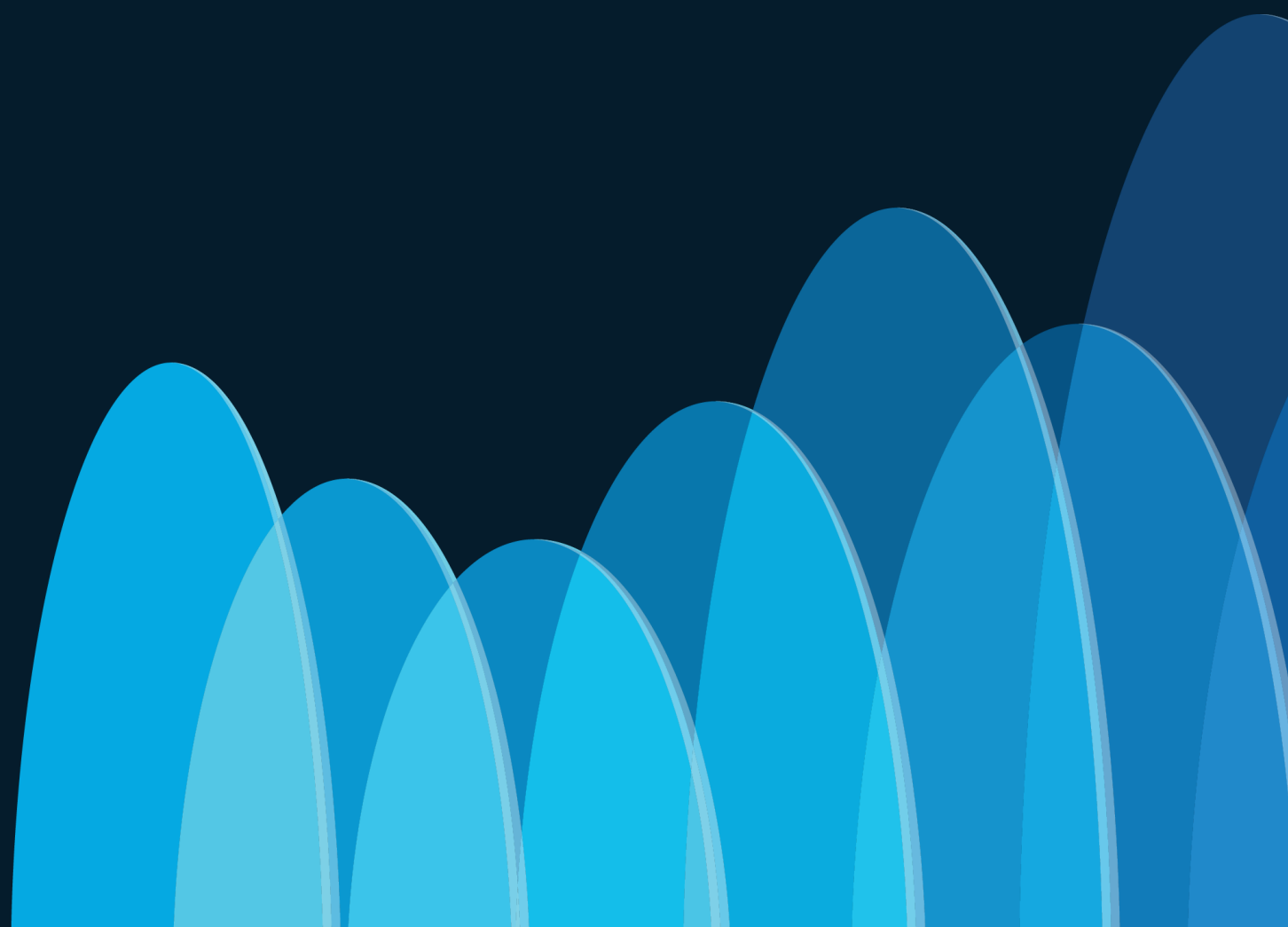
Understanding ACI security...

External Connectivity...

Increasing Security...

Automation Blueprints...

Wrapping up...



cisco Live!

Select one or more Design Patterns…

Carefully consider the use of:

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

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

Benefits of Shared Service model...

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

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

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

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

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

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

Getting started resources

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

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

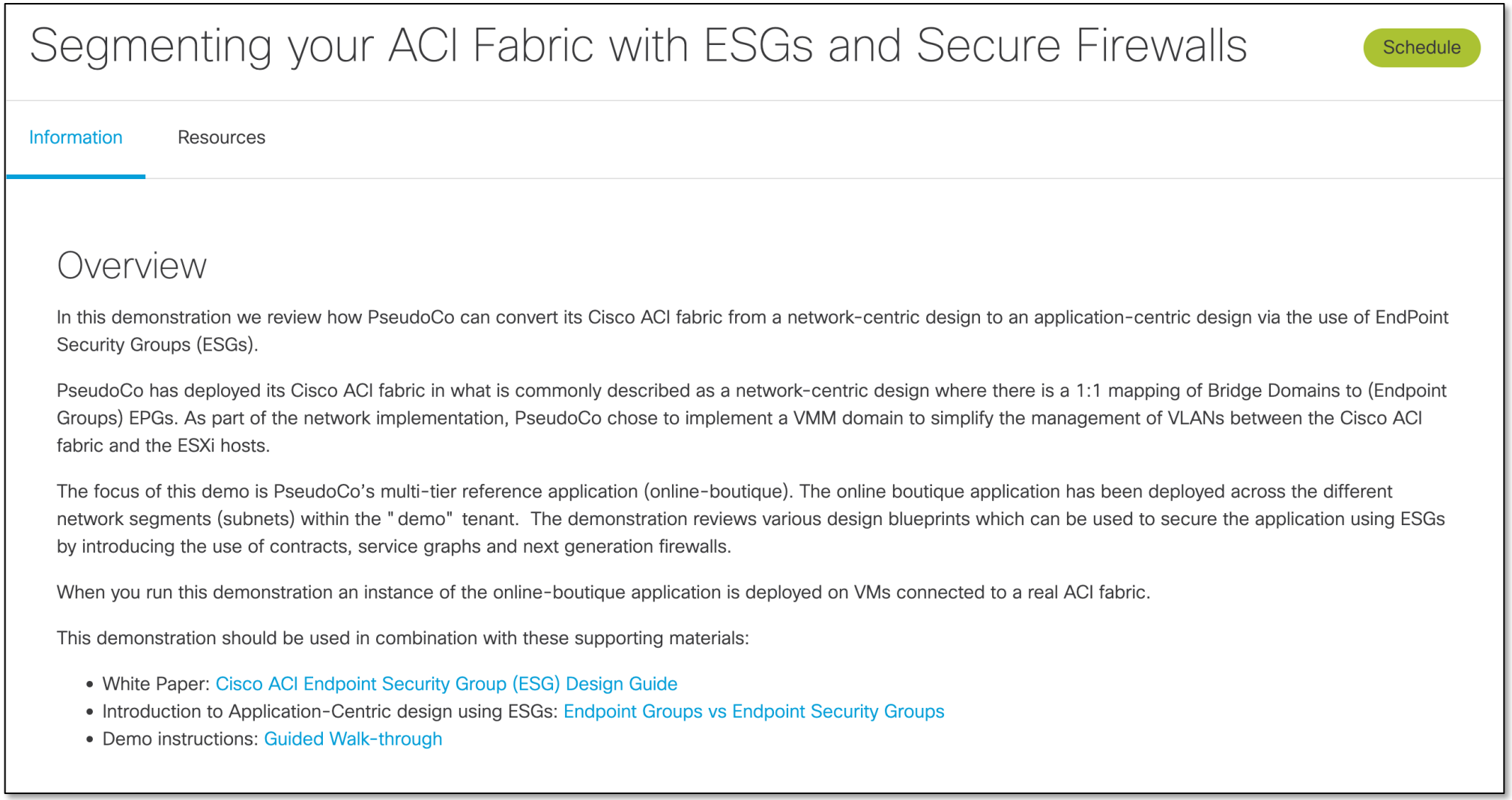
ESG Design Guide

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

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

Now available on dCloud

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



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

Try the Walk in Lab (LABDCN-2287) in the World of Solutions...

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

Complete Your Session Evaluations

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

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

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

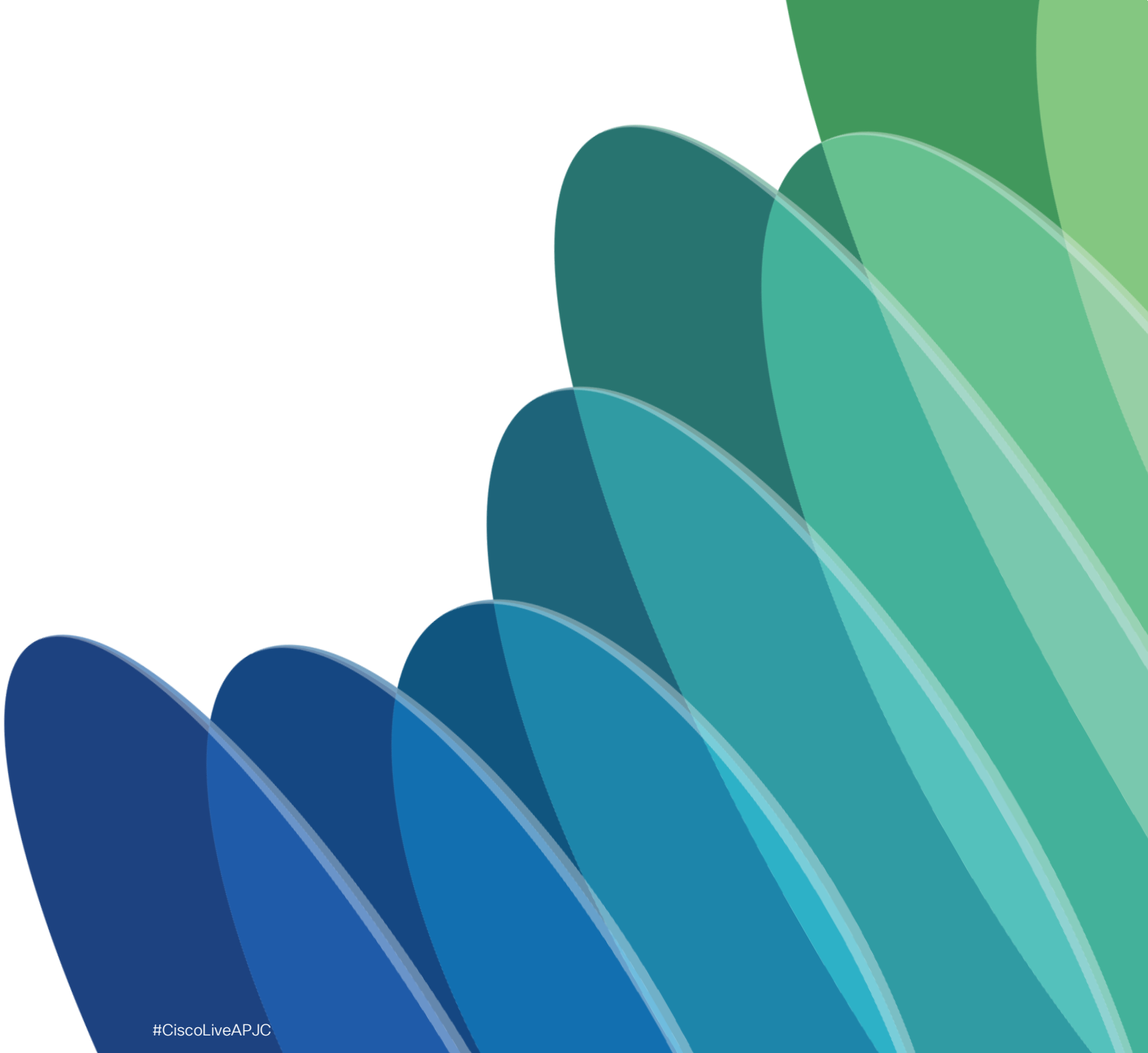
Continue your education

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

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

Contact me at: ssharman@cisco.com

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



Thank you

cisco Live!

GO BEYOND

#CiscoLiveAPJC