Turbo charge your ACI Segmentation and Visibility

Steve Sharman – Solutions Engineer DCN

Fabien Gandola – Solutions Engineer Security

BRKDCN-2959

Zero Trust requirements

For **reference** only

Network Segmentation (Macro Requirements)

Business Unit Segmentation

- Segment BU resources within Data Center into “Tenants”
- Enforce policy into the Data Center via Highly Available Firewalls, to restrict access to only BU users (branch or remote)
- Access managed via User Identity
- All flows into and out of the Tenant will be inspected by L4-7 firewalls as required
- A “Shared Services” will provide services to multiple different tenants

Data Center “Environments”

- Within BU Tenant, we will segment into Environments by either leveraging VRFs, alternatively each BU function will have a dedicated Tenant and VRF
- All flows into and out of an Environment will be L7 inspected by firewalls as required
- VLANs within environments will be used to group resources (applications)
- No enforcement within or between VLANs in same Environment, however there is a requirement to dynamically insert L4-7 firewalls as required

© 2025 Cisco and/or its affiliates. All rights reserved.

Zero Trust requirements

For **reference** only

Network Segmentation Principles

- Users in a BU, can **only access systems within the BU tenant**, as well as shared services in DC
- Users in a BU are **identified by Identity**, not a fixed IP
- Traffic inbound to the tenant will traverse a **Core Firewall which is the enforcement point**
- Production environment includes all production workloads within a single VRF
- Non-Production environment includes all no-prod workloads within a single VRF
- There maybe more than one Non-Production environment, i.e. DEV, UAT, SIT, etc
- DMZ network requires updating as the (aging) firewall provides the default gateway for all subnets
- **Explicit Trust** model between Prod & Non-Prod workloads within/across tenants depending on the model
- **Explicit Trust** model for BU-to-BU and User to App (ZTNA)
- **Implicit Trust** model between Production workloads within same VRF
- **Implicit Trust** model between Non-Prod workloads within same VRF
- **Layer 7 firewall** inspection in place between systems requiring **explicit** trust

© 2025 Cisco and/or its affiliates. All rights reserved.

Zero Trust requirements

For **reference** only

Expected Outcomes

- Prepare a **modern network infrastructure and security posture for next 5+ years**
- Replace existing on-premise Edge Firewalls located in each Data Centre
- **Align on-premise and Cloud Firewall platform**
- Provide the **foundation for a Zero Trust Architecture** moving from IP based security policies to a user and application-based security policy
- Provide **dynamic security and network capabilities for an evolving threat landscape**
- **Eliminate implicit trust** in application access
- **Limit lateral movement** across the network to **reduce the blast radius** of attacks
- **Simplify our overall architecture**
- **Simplify the management and visibility of policy and enforcement**
- **Selectively identify what traffic traverses the firewalls**
- **Implement a modern DMZ design for selective redirection and endpoint security**

© 2025 Cisco and/or its affiliates. All rights reserved.

Customers require:

The coming together of networking and security...

Dividing into multiple tenants and VRFs...

Security control over inbound traffic...

Explicit trust within and between tenants and VRFs...

Zero trust application-based security...

Layer 7 security inspection...

Modern DMZ design with selective redirection...

Reducing operational complexity of segmentation

Implement Zero trust Micro-segmentation

© 2025 Cisco and/or its affiliates. All rights reserved.

Agenda

01 Where networking and security come together...

02 Customer's current network design...

03 Security control over inbound traffic...

04 Understanding ACI security...

05 Zero trust application-based security...

06 Layer 7 security integration...

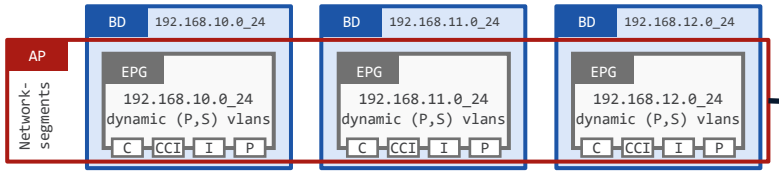
07 DMZ redesign...

08 Reducing segmentation operational complexity...

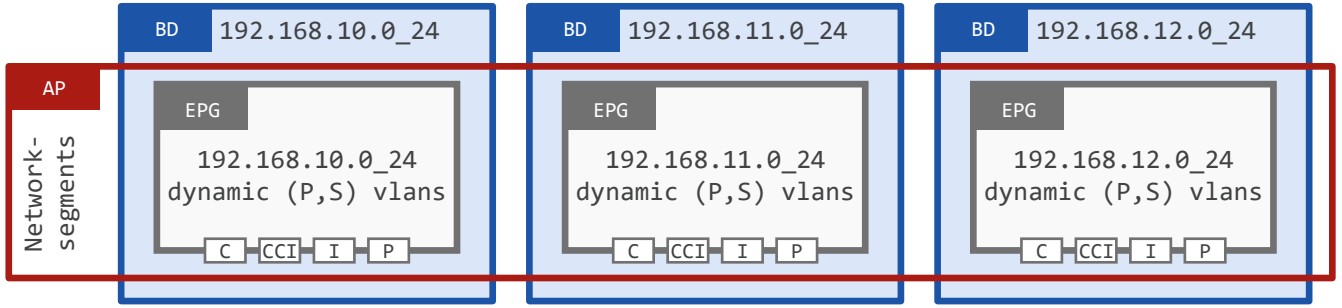
09 Zero trust micro-segmentation...

© 2025 Cisco and/or its affiliates. All rights reserved.

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



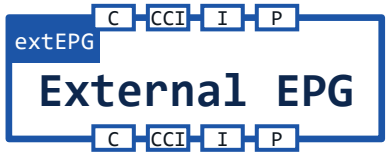
The details are there for your reference so that you can rebuild in your own environment

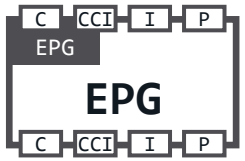


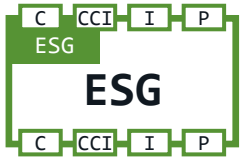
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Icons







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

© 2025 Cisco and/or its affiliates. All rights reserved.

Everything is built using “Network as Code”

https://netascode.cisco.com/

```
~/Github/repositories/public/aci-dev-01/BRKDCN-2959-DMZ  main ⇡6 !10  tree -L 2
.
├── data
│   ├── 01-dmz-design-firewall-outside-one-ha-pair-peering-to-fabric-vrf.nac.yaml
│   ├── 02-dmz-design-firewall-outside-two-ha-pairs-peering-to-fabric-vrf.nac.yaml
│   ├── 03-dmz-design-firewall-cluster.nac.yaml
│   ├── 04-dmz-design-firewall-cluster-independent-mode.nac.yaml
│   ├── 05-dmz-current-design-firewall-provides-default-gateway.nac.yaml
│   ├── 06-dmz-design-firewall-provides-default-gateway-peering-to-fabric-vrf.nac.yaml
│   ├── 07-dmz-design-initial-bd-peering-to-fabric-vrf.nac.yaml
│   └── 08-dmz-design-dual-bd-peering-to-fabric-vrf.nac.yaml
├── LICENSE
├── main.tf
├── README.md
├── terraform.tfstate
├── terraform.tfstate.backup
├── terraform.tfvars
└── variables.tf

2 directories, 15 files

~/Github/repositories/public/aci-dev-01/BRKDCN-2959-DMZ  main ⇡6 !10
```

© 2025 Cisco and/or its affiliates. All rights reserved.

About me

Fabien Gandola

fgandola@cisco.com

TSA Cyber Security EMEA

26 years in Cisco

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

About me

Steve Sharman

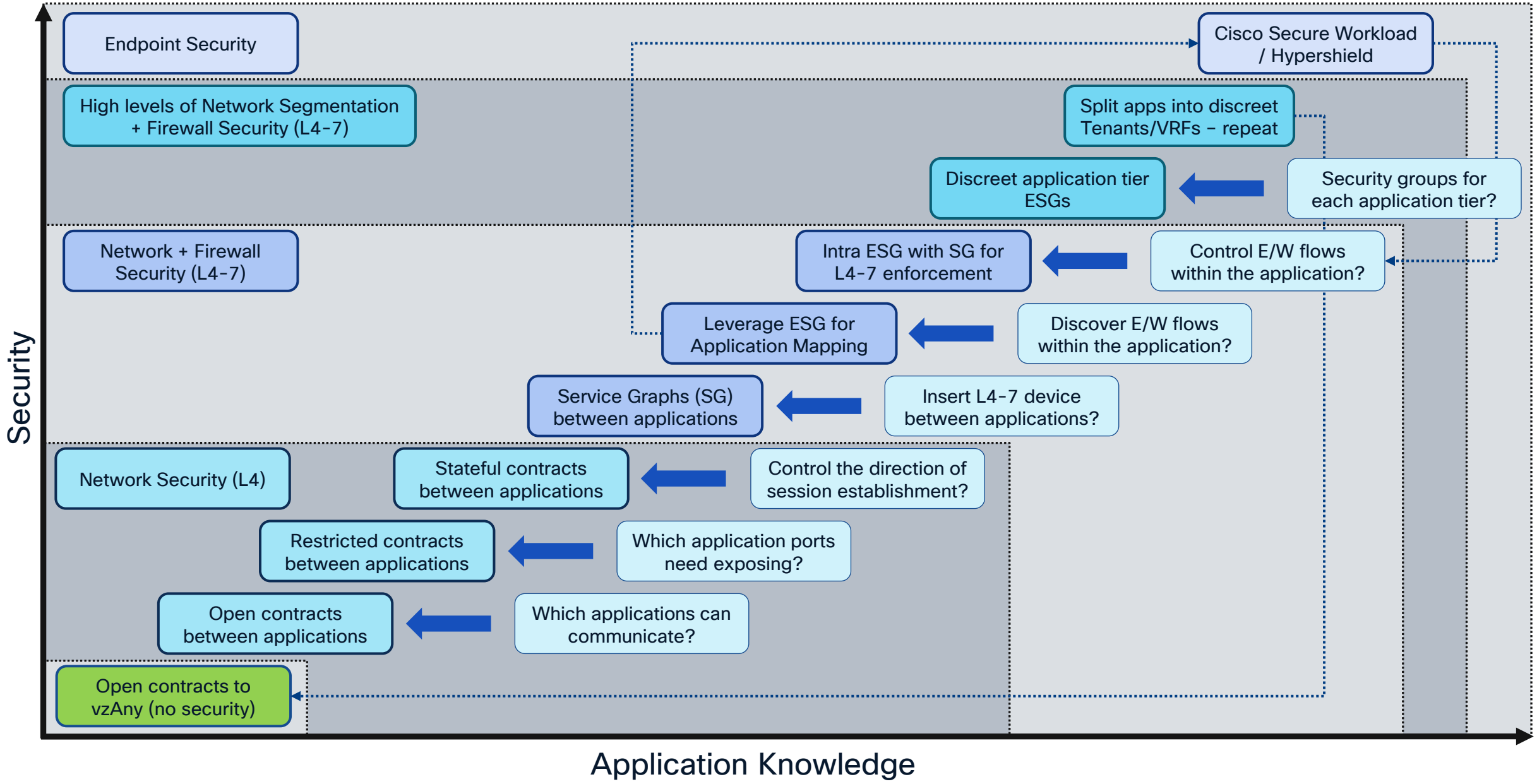
ssharman@cisco.com
SE WW DCN Sales
27 years in Cisco

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Where networking and security come together...

- **Where networking and security come together...**
- Customer's current network design...
- Security control over inbound traffic...
- Understanding ACI security...
- Zero trust application-based security...
- Layer 7 security integration...
- DMZ redesign...
- Reducing operational complexity of segmentation
- Implement Zero trust Micro-segmentation

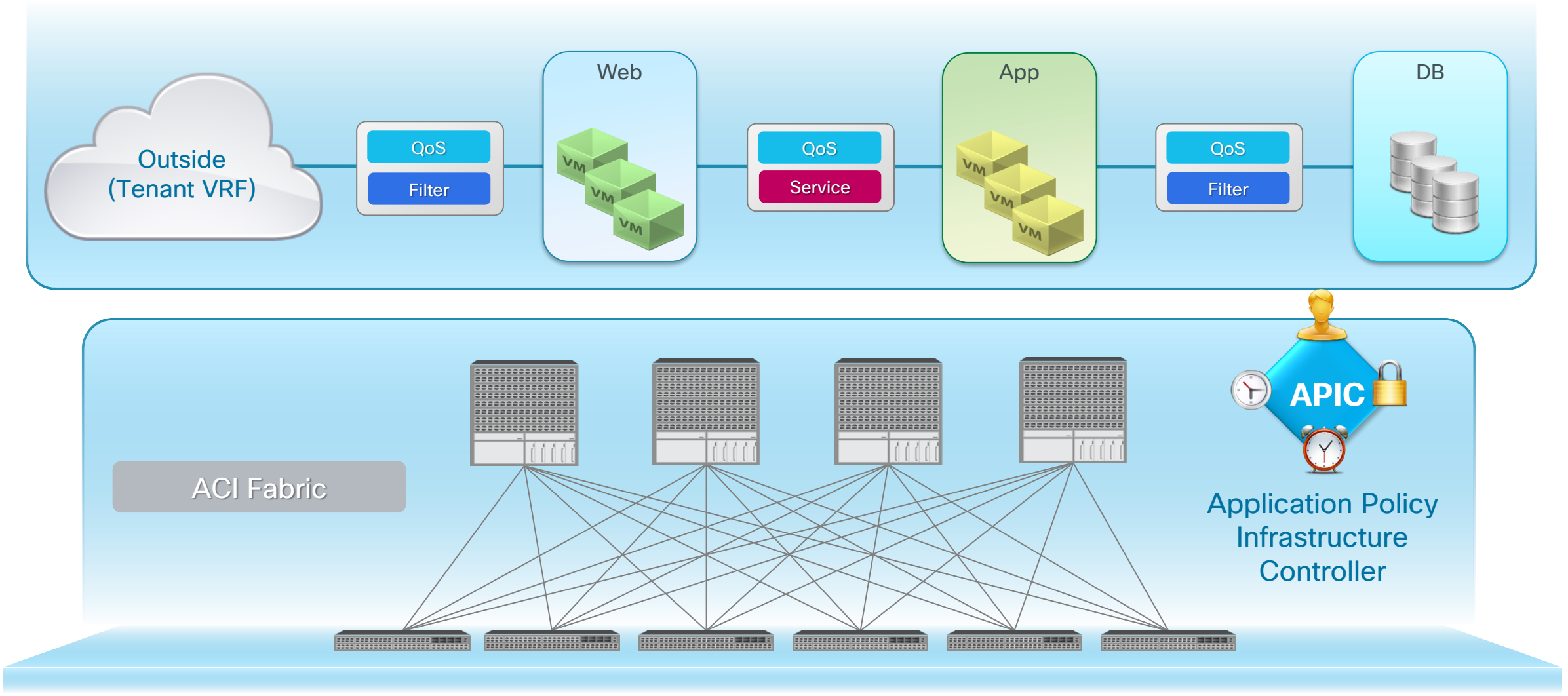


© 2025 Cisco and/or its affiliates. All rights reserved.

Any idea what a modern application looks like?

© 2025 Cisco and/or its affiliates. All rights reserved.

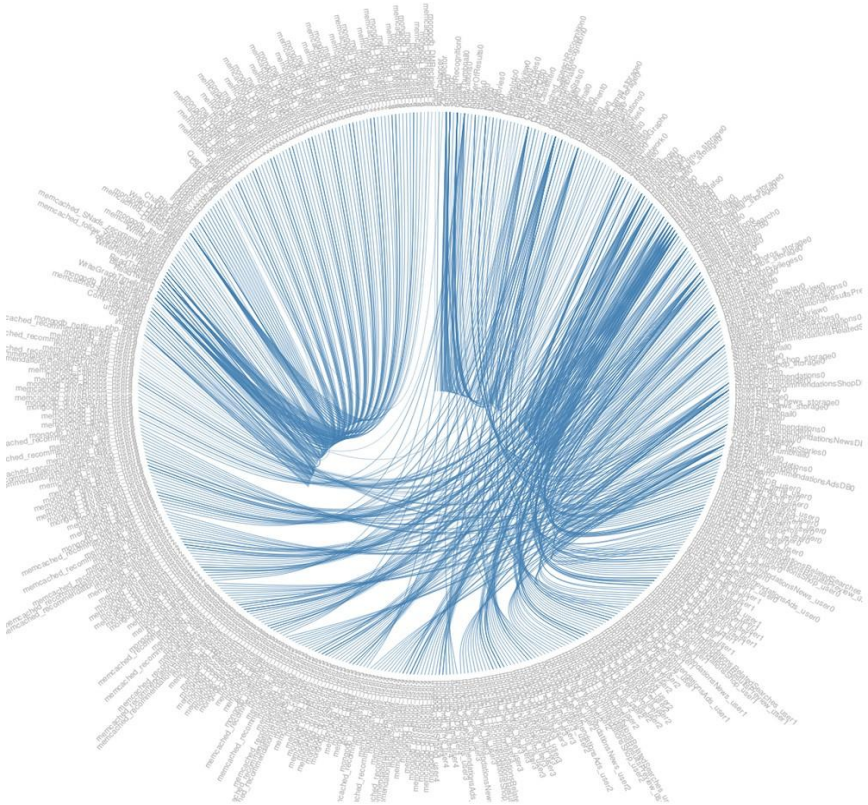
Mythical three tier design

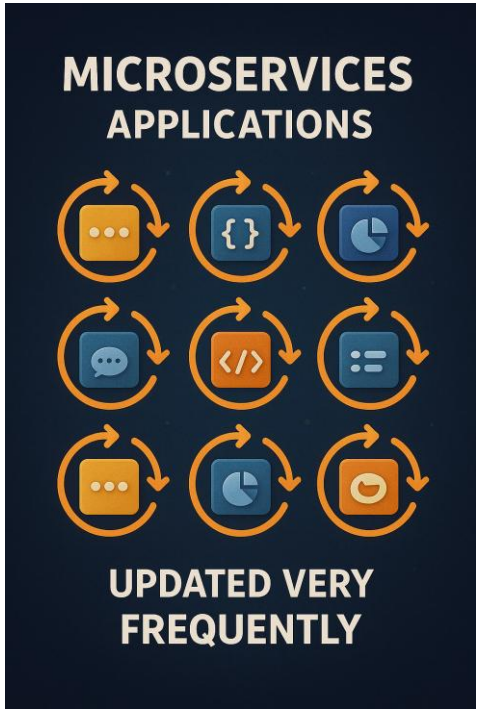


© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Applications have dramatically evolved

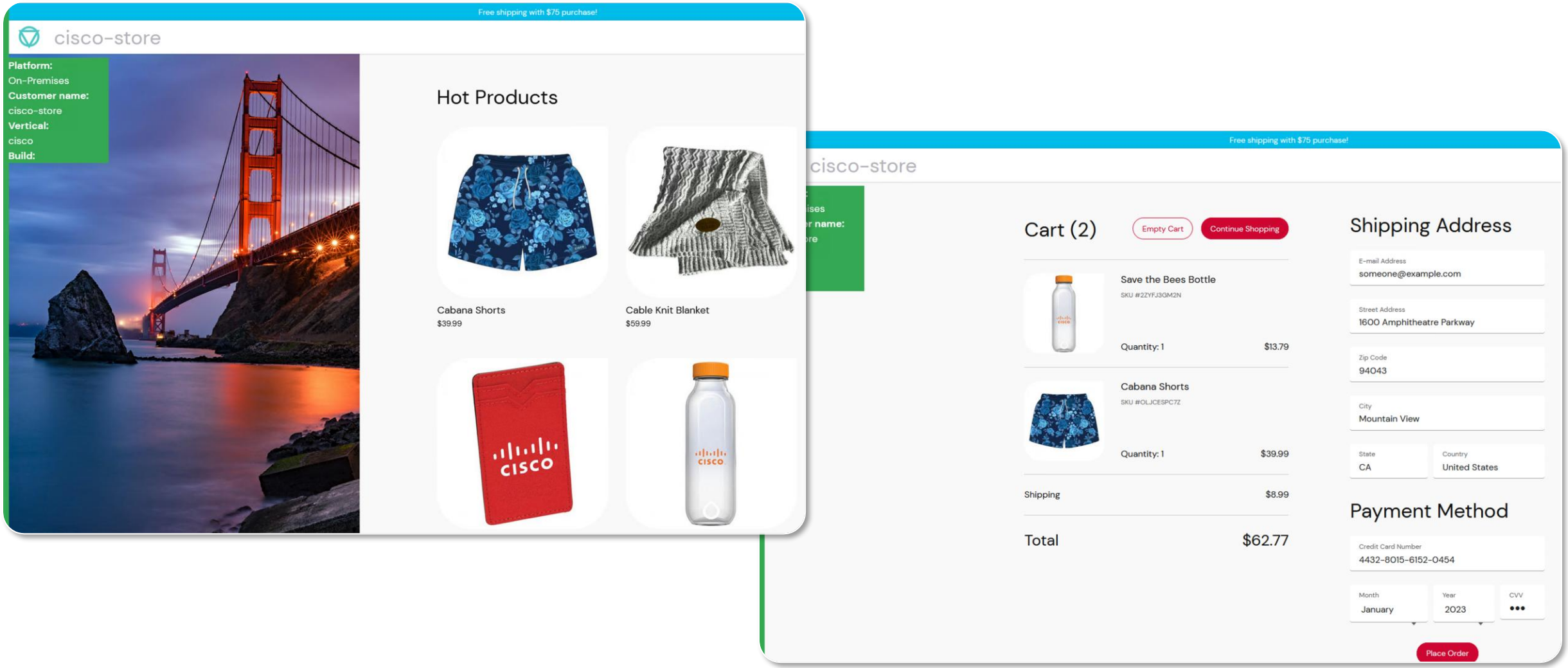




© 2025 Cisco and/or its affiliates. All rights reserved.

Online boutique

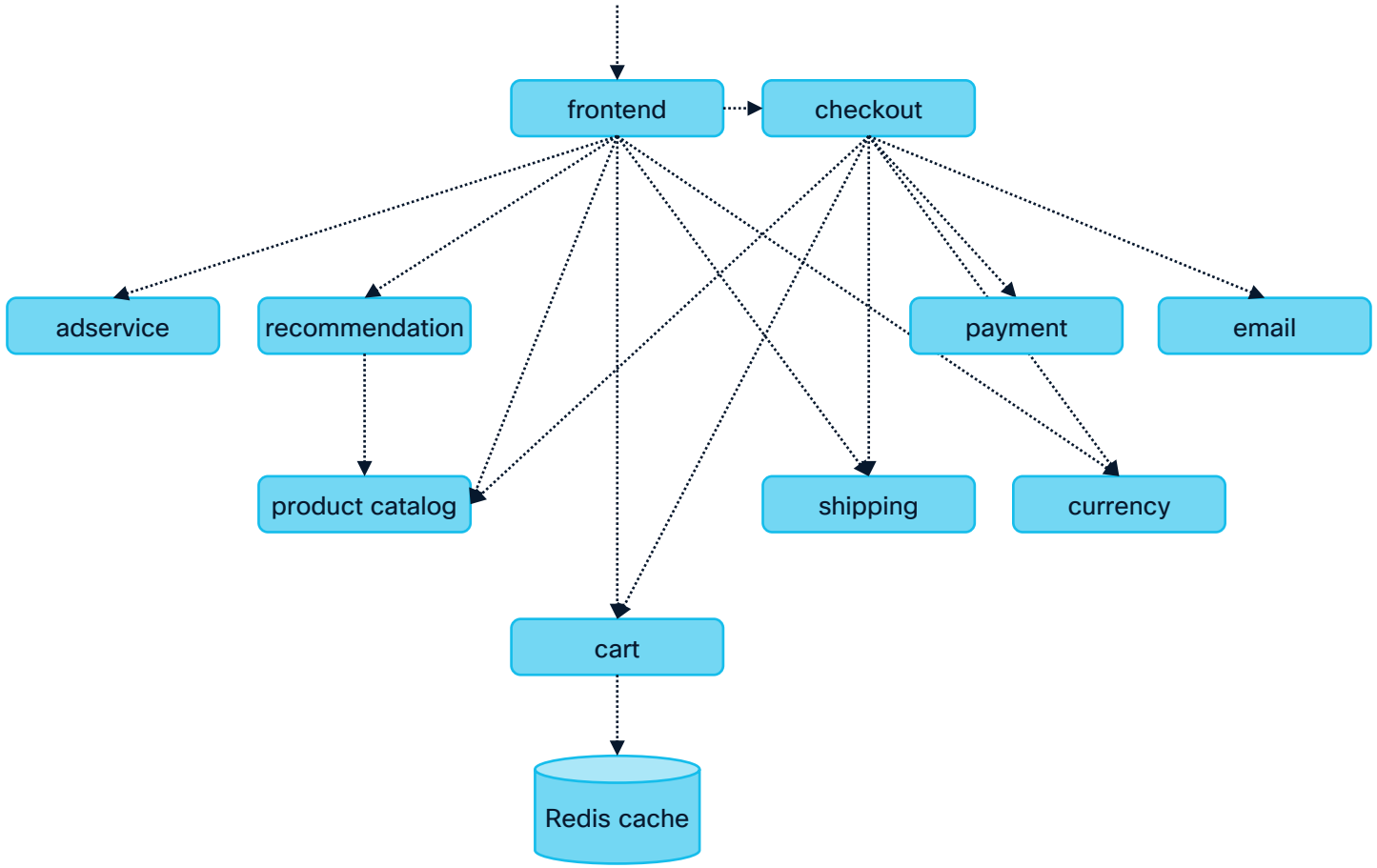
https://github.com/GoogleCloudPlatform/microservices-demo



© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Customer requirement

Multiple Tenants, (at least) one for each BU, security control for BU to BU traffic, and E/W control within a BU...

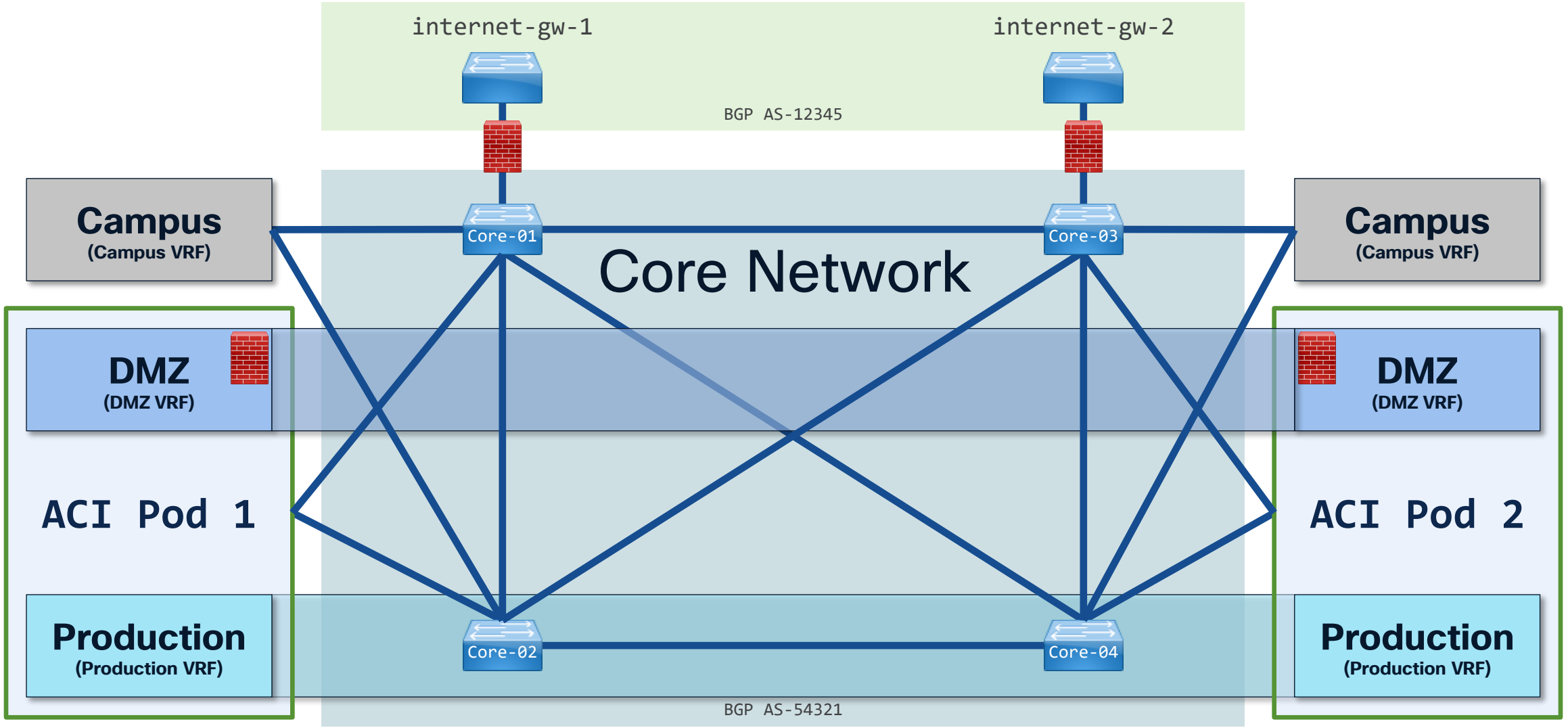
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

What does the Customer’s current network design look like…?

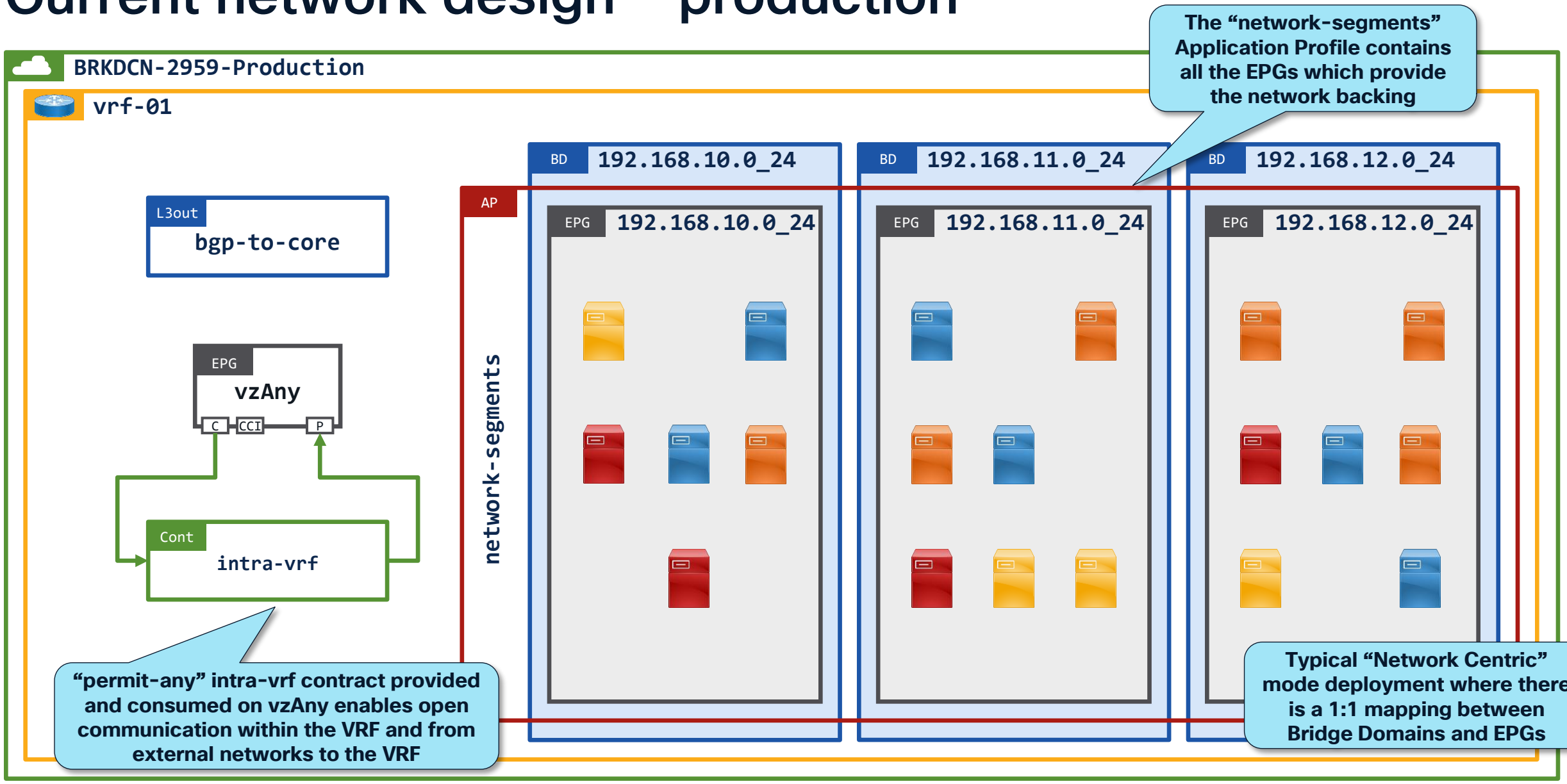
- Where networking and security come together…
- **Customer’s current network design…**
- Security control over inbound traffic…
- Understanding ACI security…
- Zero trust application-based security…
- Layer 7 security integration…
- DMZ redesign…
- Reducing operational complexity of segmentation
- Implement Zero trust Micro-segmentation

High level network overview



© 2025 Cisco and/or its affiliates. All rights reserved.

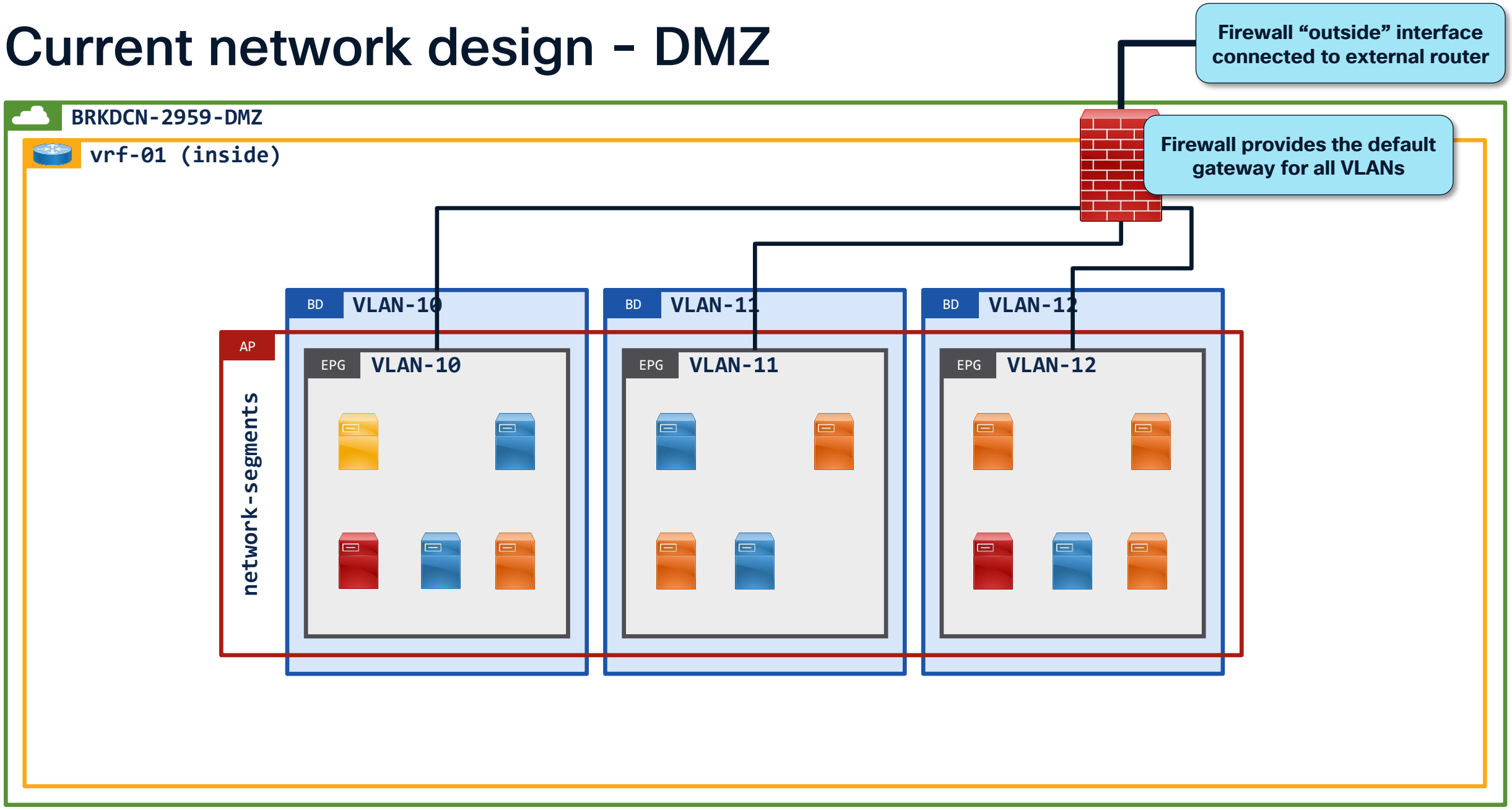
Current network design – production



© 2025 Cisco and/or its affiliates. All rights reserved.

https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959/data/01-production-current-design-l3out-consumer.nac.yaml

Current network design – DMZ



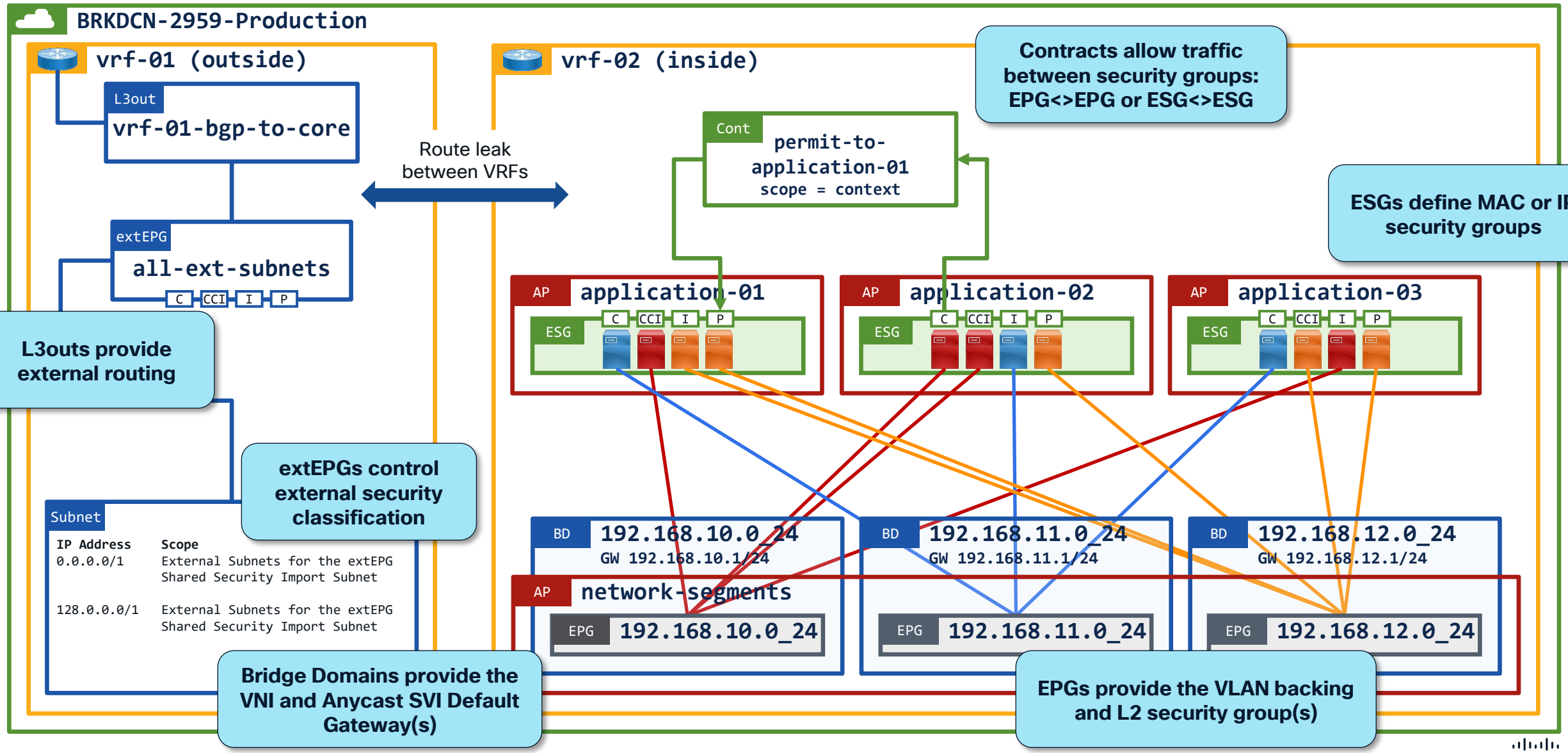
© 2025 Cisco and/or its affiliates. All rights reserved.

What’s clear is that
the customer needs to
re-architect their network...

© 2025 Cisco and/or its affiliates. All rights reserved.

ACI building blocks and design patterns...

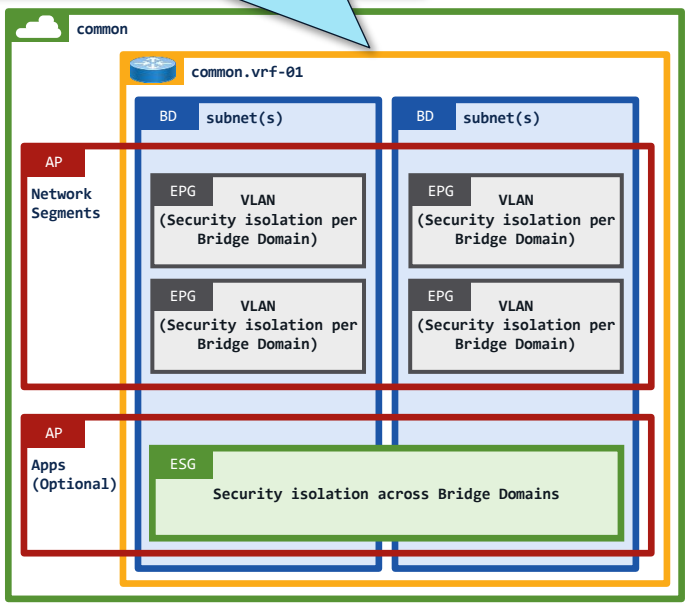
ACI building blocks



© 2025 Cisco and/or its affiliates. All rights reserved.

Design patterns

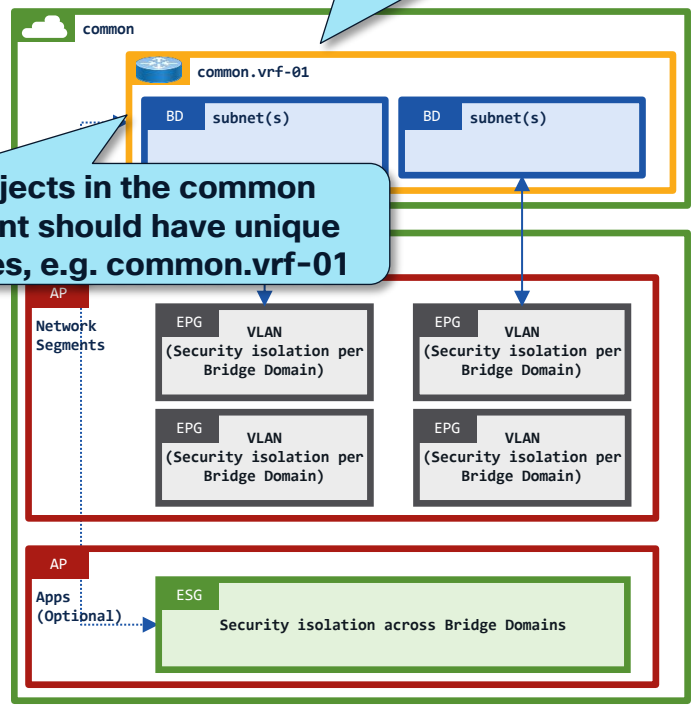
Everything in the “common” Tenant is not typically seen



Used for functions which are accessible from any Tenant

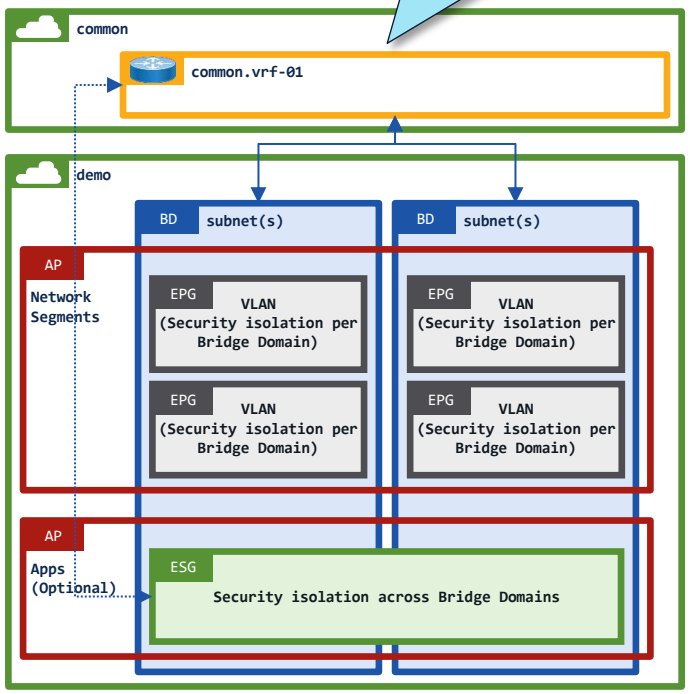
VRFs and BDs in “common” with EPGs and ESGs in the “user” tenant

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

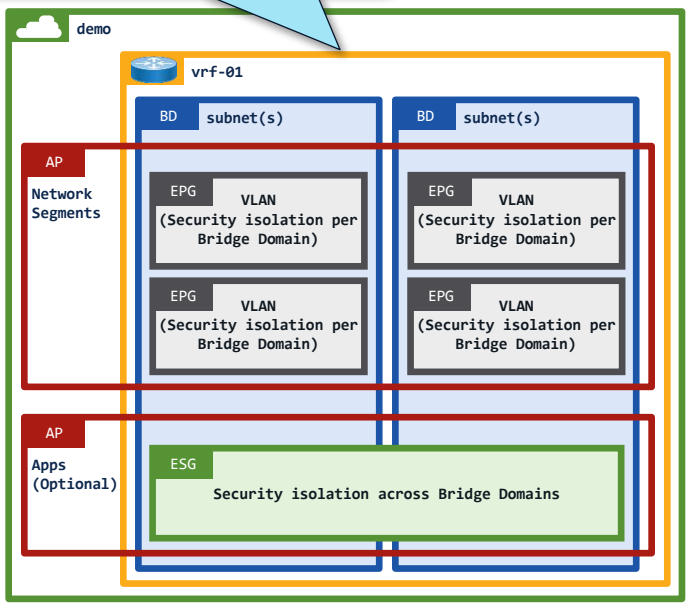


Dedicated subnets for tenants with VRFs that can be (optionally) shared by different Tenants

© 2025 Cisco and/or its affiliates. All rights reserved.

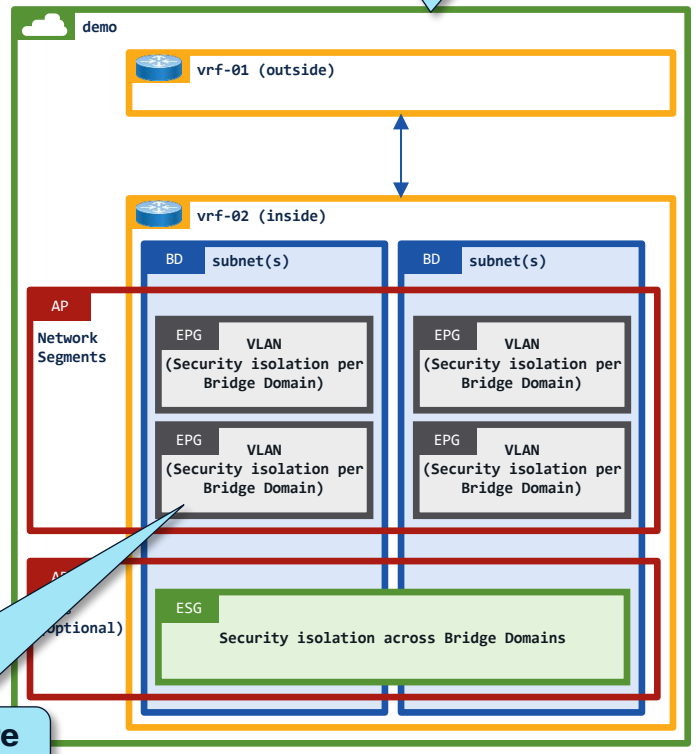
Design patterns

All networking constructs contained within a Tenant



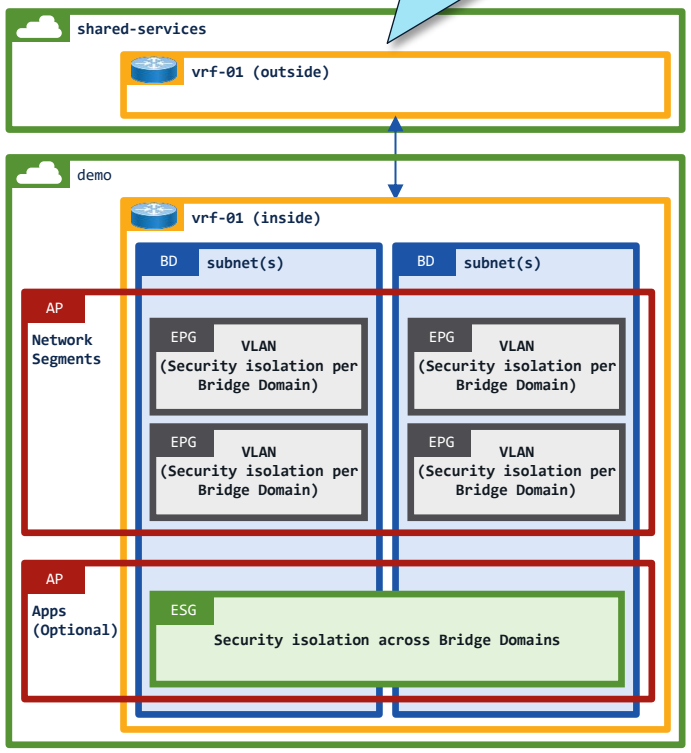
Dedicated VRFs and subnets for each Tenant with Dedicated L3outs

Network team controls inbound/outbound routing



Dedicated VRFs and subnets for each Tenant with Dedicated L3out

Shared L3out



Dedicated VRFs and subnets for each Tenant with Shared L3out

Each Tenant has one or more network security groups

Each Tenant has one or more endpoint security groups

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

The customer had previously deployed option 3 i.e. single tenant with a single VRF...

© 2025 Cisco and/or its affiliates. All rights reserved.

Customer Requirement

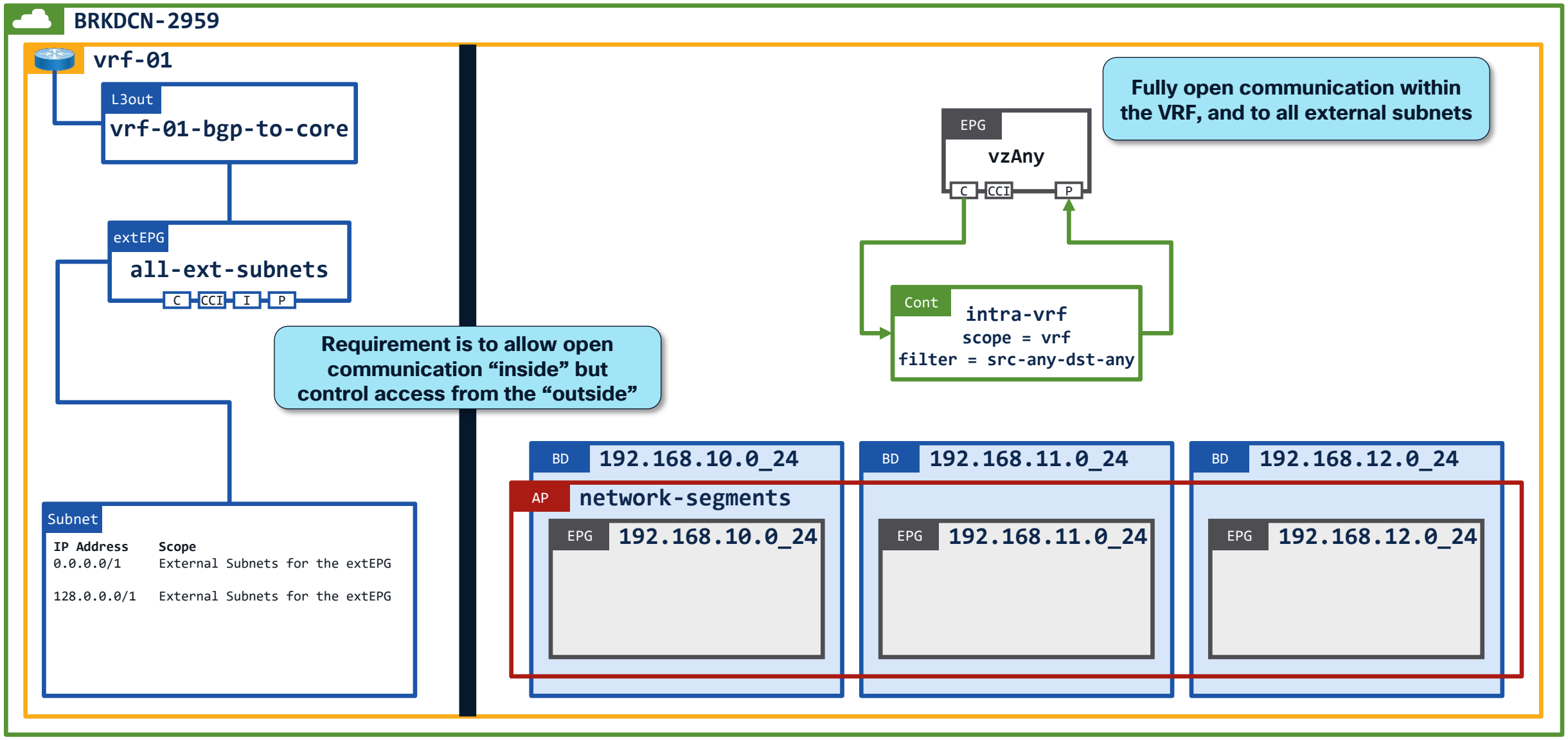
Traffic into, and within a tenant must be controlled...

© 2025 Cisco and/or its affiliates. All rights reserved.

Security control over inbound traffic...

- Where networking and security come together...
- Customer's current network design...
- **Security control over inbound traffic...**
- Understanding ACI security...
- Zero trust application-based security...
- Layer 7 security integration...
- DMZ redesign...
- Reducing operational complexity of segmentation
- Implement Zero trust Micro-segmentation

Protect access from the “outside”



https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959/data/01-production-current-design-l3out-consumer.nac.yaml

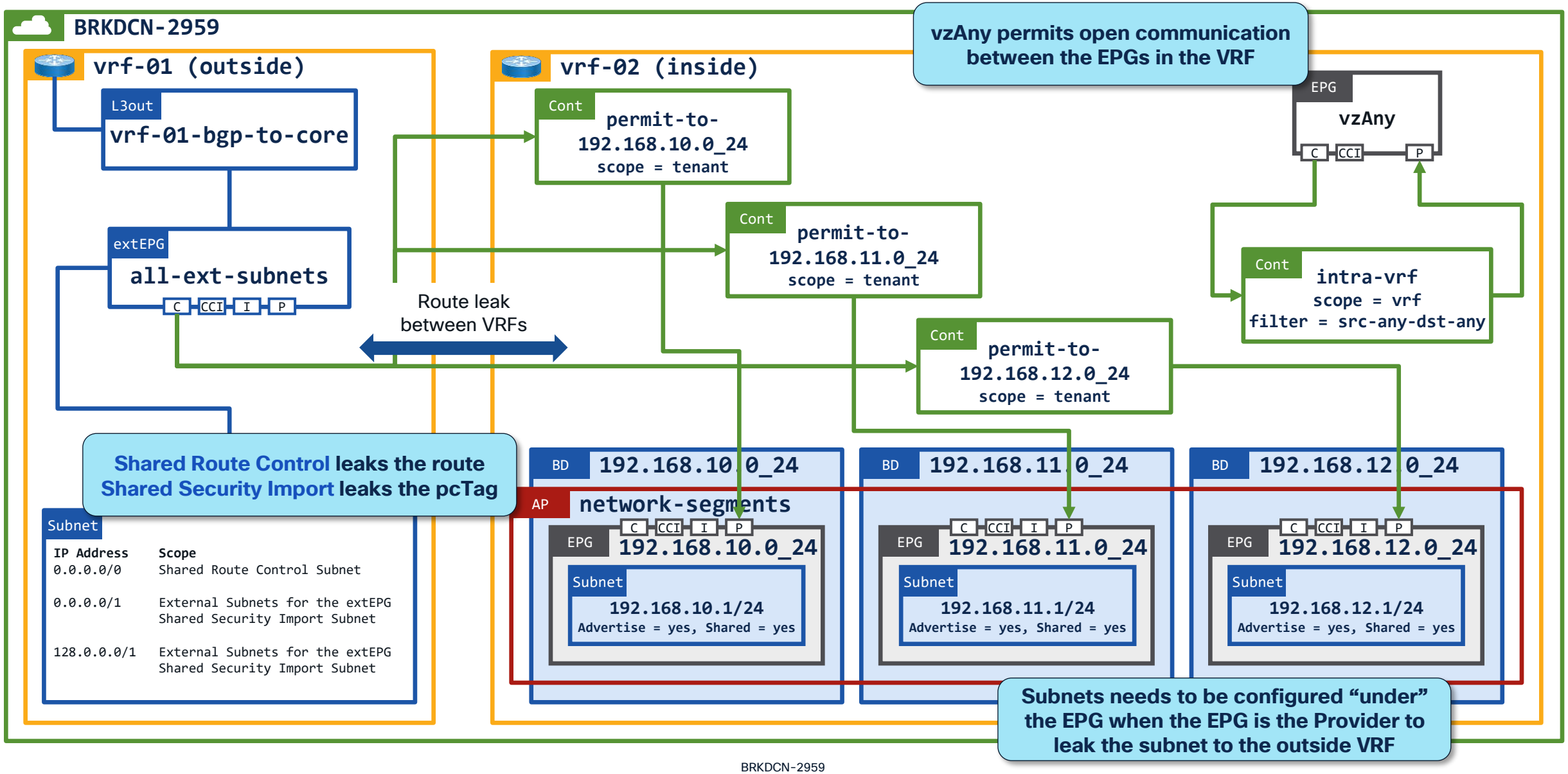
Three options to “manage” access to vzAny...?

Option 1

Single tenant, dual VRF design

© 2025 Cisco and/or its affiliates. All rights reserved.

Single tenant, dual VRF – L3out is the contract consumer



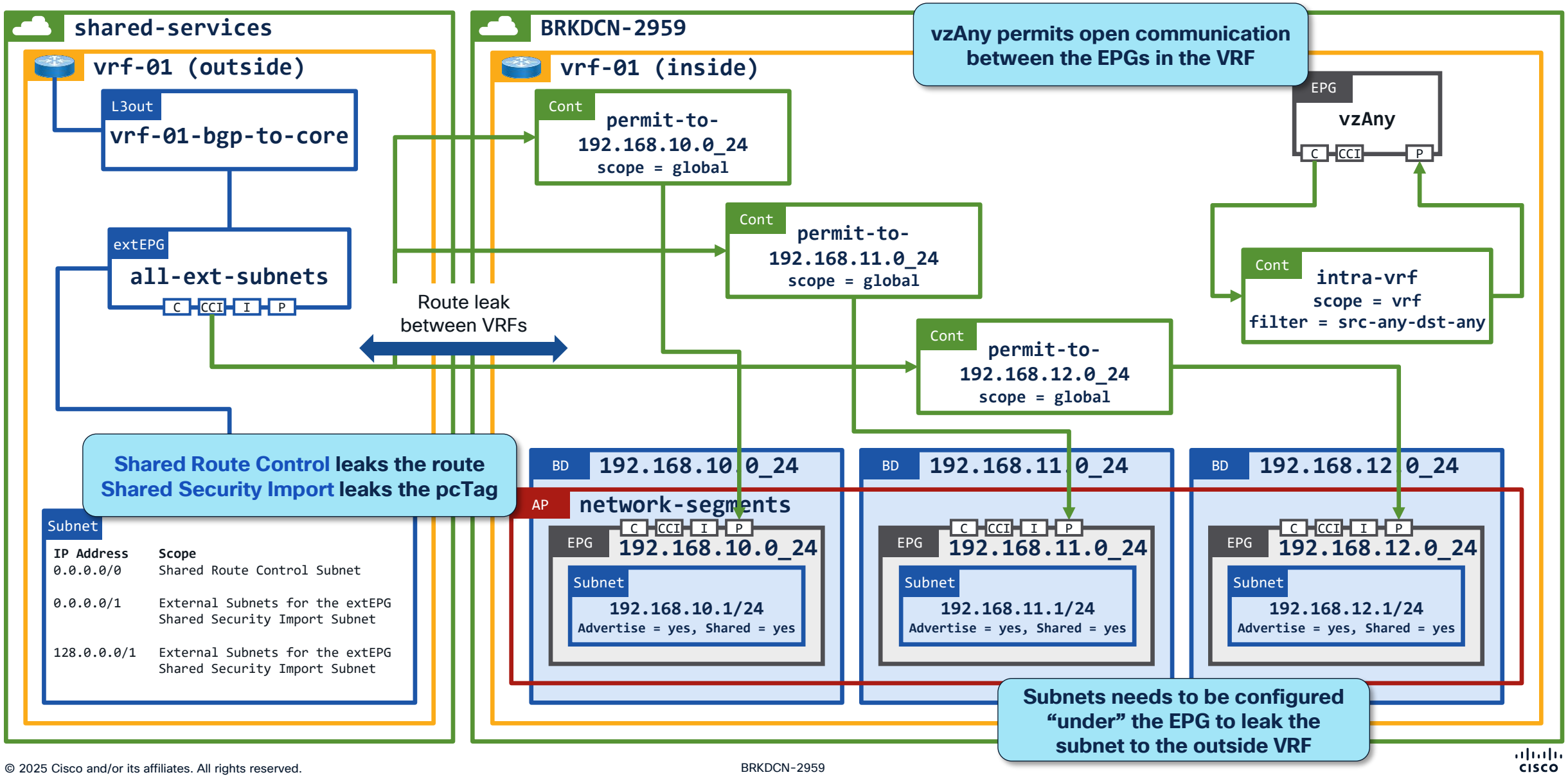
https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959/data/02-production-dual-vrf-design-l3out-consumer.nac.yaml

Option 2

Shared services tenant with dual VRF design, aka a shared L3out

© 2025 Cisco and/or its affiliates. All rights reserved.

Dual tenant, dual VRF – Shared L3out is the contract consumer



© 2025 Cisco and/or its affiliates. All rights reserved.

https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959/data/05-production-shared-l3out-design-l3out-consumer.nac.yaml

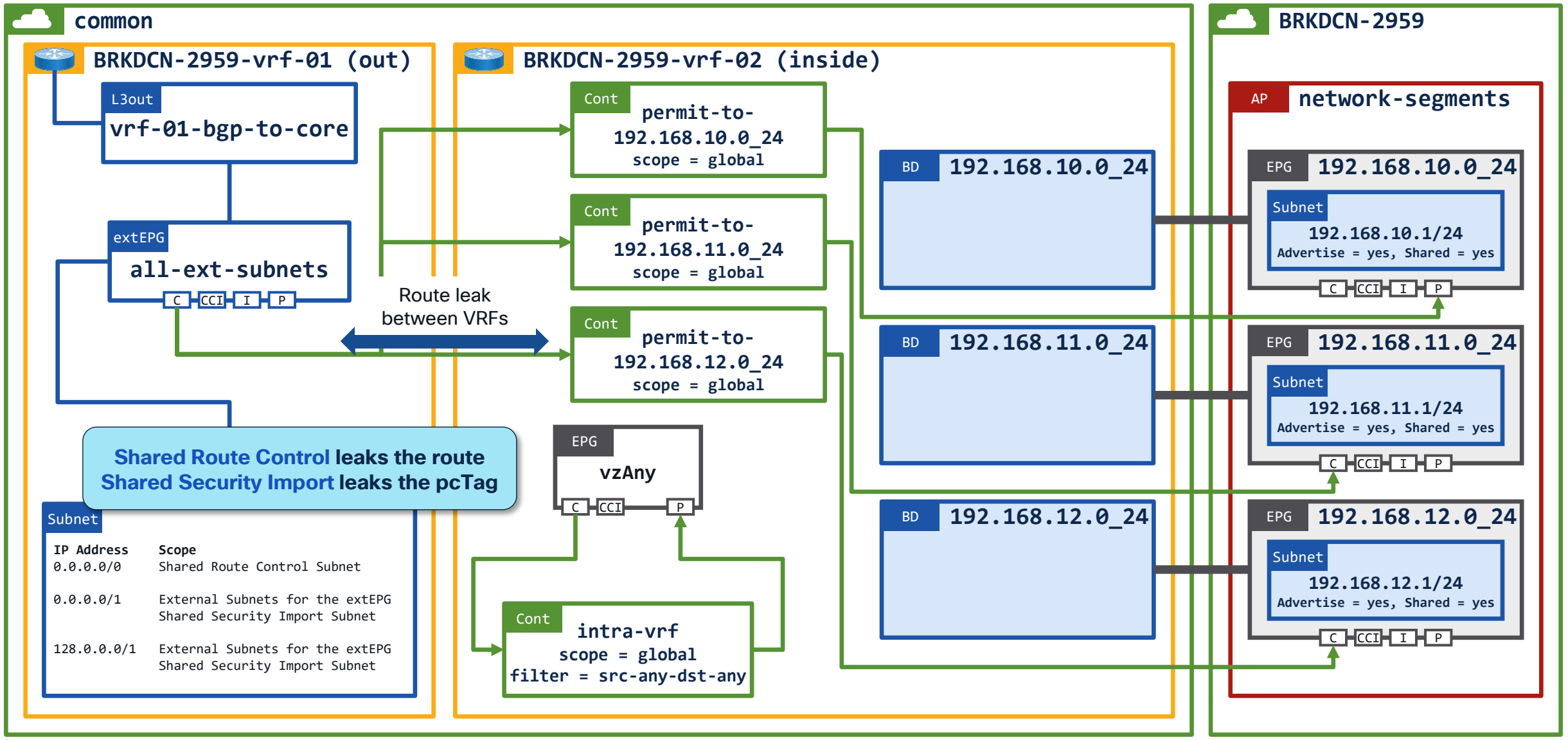
Option 3

Shared services using tenant common with dual VRF, aka a shared L3out in common

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

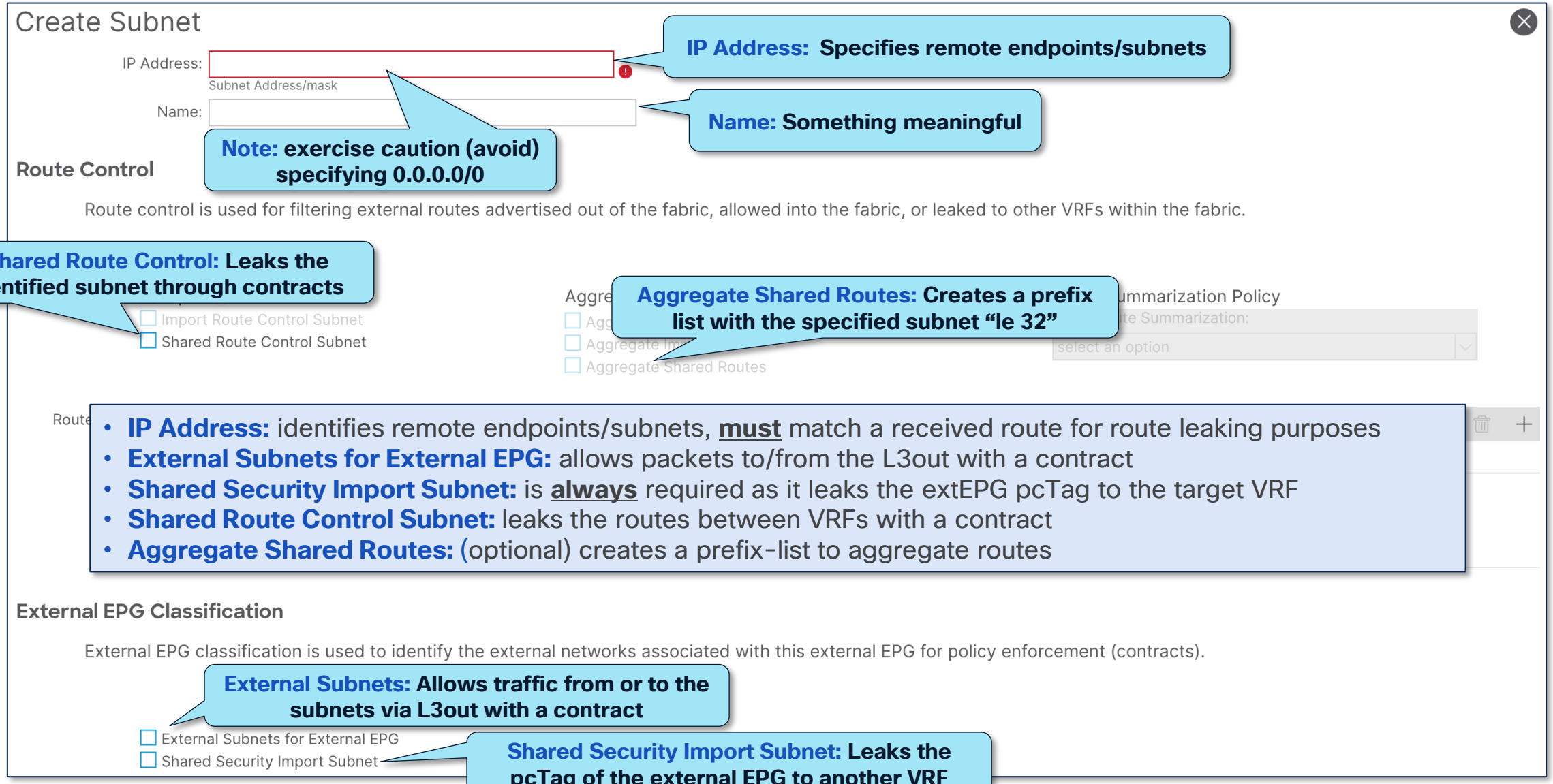
Dual tenant, dual VRF – Shared L3out is the contract consumer



© 2025 Cisco and/or its affiliates. All rights reserved.

https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959/data/07-production-dual-vrf-design-in-common-l3out-consumer.nac.yaml

Subnet classification and route leaking for EPGs...



© 2025 Cisco and/or its affiliates. All rights reserved.

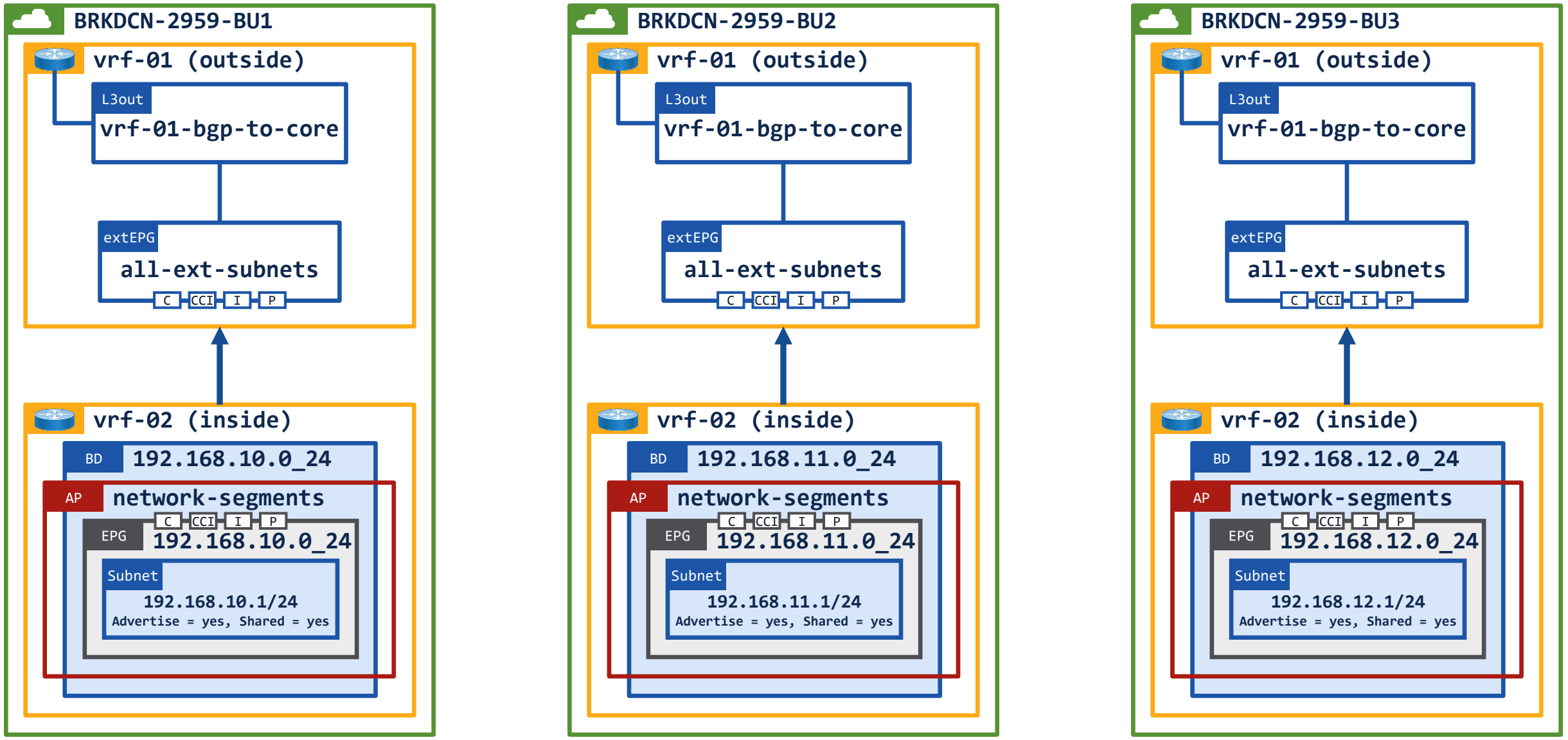
No time to get into the weeds on extEPG knobs...

© 2025 Cisco and/or its affiliates. All rights reserved.

L3out option summary...

© 2025 Cisco and/or its affiliates. All rights reserved.

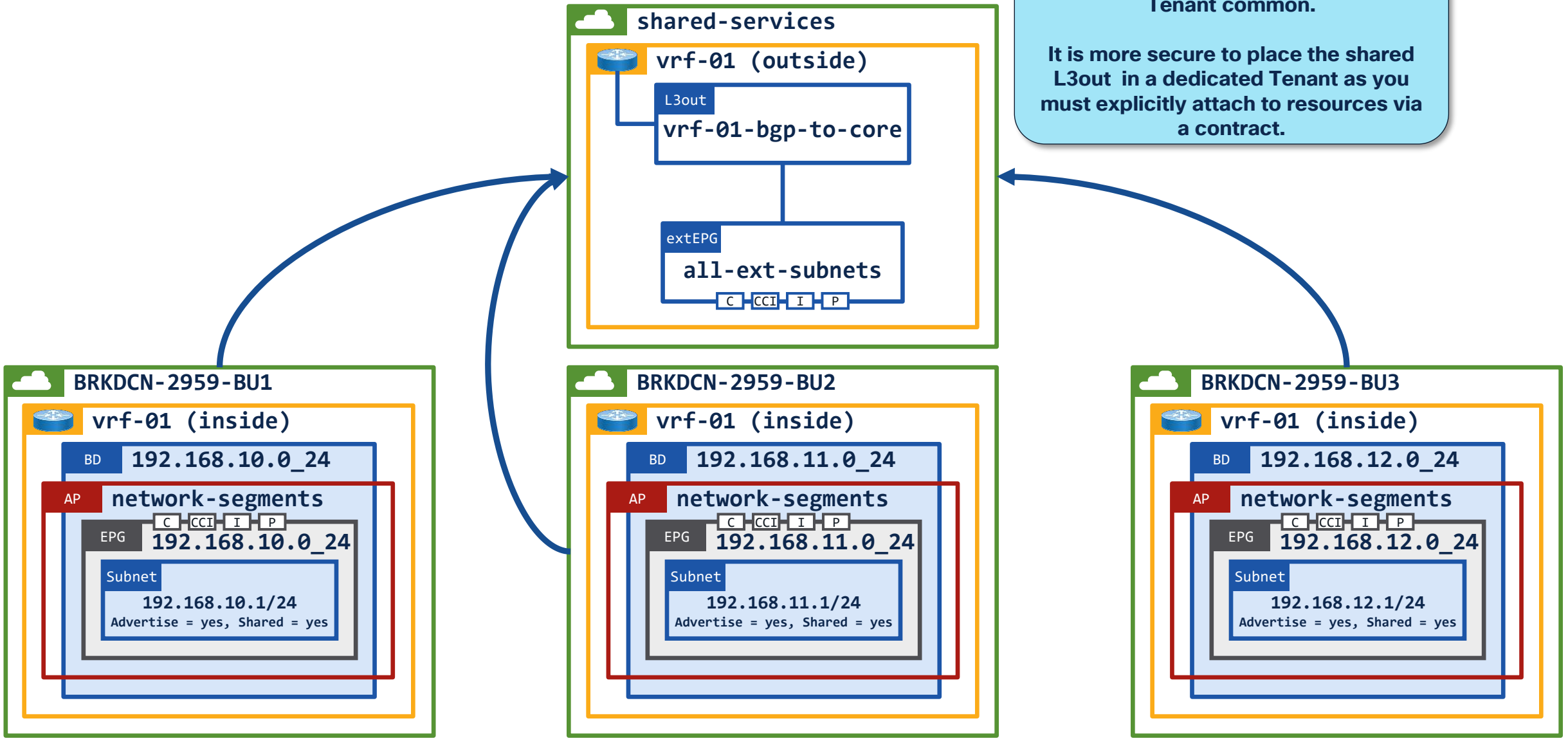
Dedicated L3out per tenant



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Shared L3out



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Customer requirement

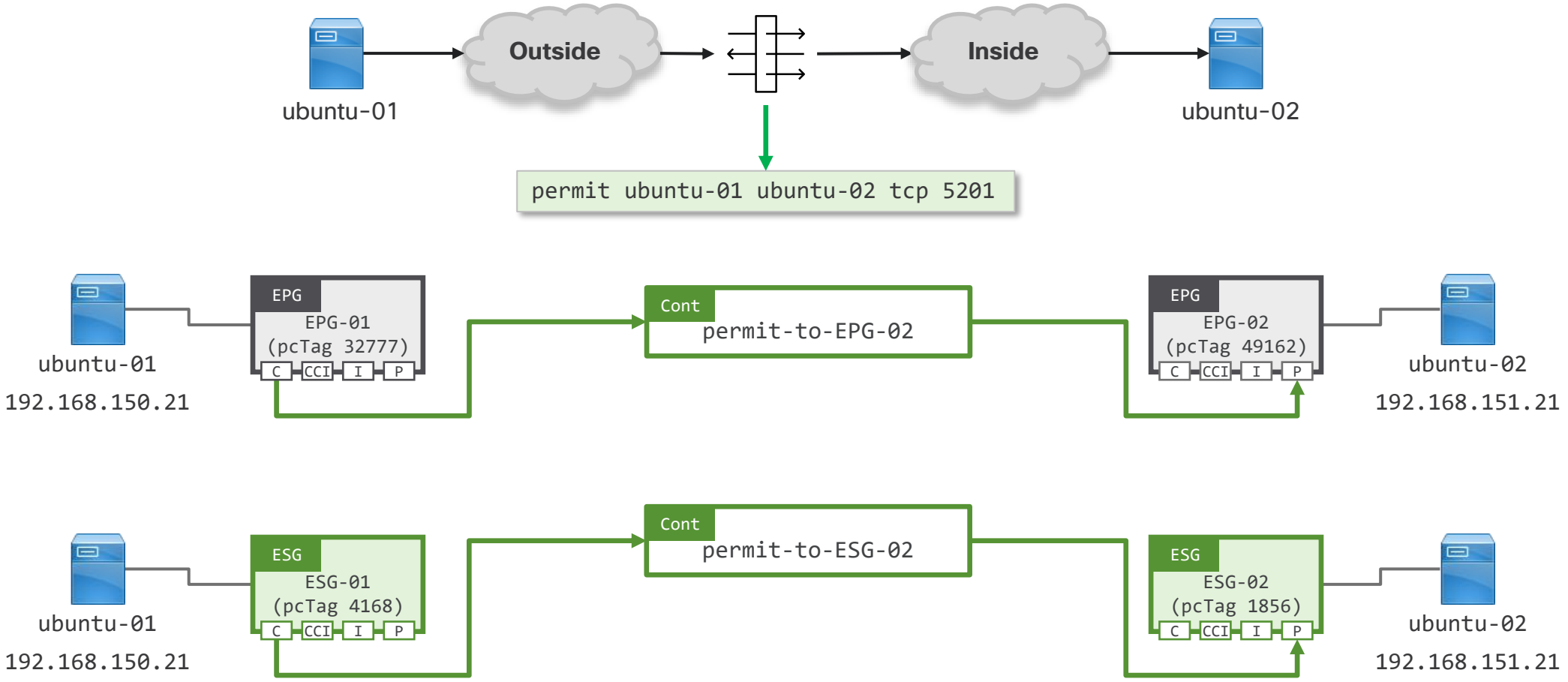
Explicit trust model between prod and non-prod workloads within/across tenants

© 2025 Cisco and/or its affiliates. All rights reserved.

Understanding ACI security...

- Where networking and security come together...
- Customer's current network design...
- Security control over inbound traffic...
- **Understanding ACI security...**
- Zero trust application-based security...
- Layer 7 security integration...
- DMZ redesign...
- Reducing operational complexity of segmentation
- Implement Zero trust Micro-segmentation

How do contracts work...?



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

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Consumer and provider relationships are there to help you visualize the traffic flow direction i.e. (typically) from the consumer to the provider

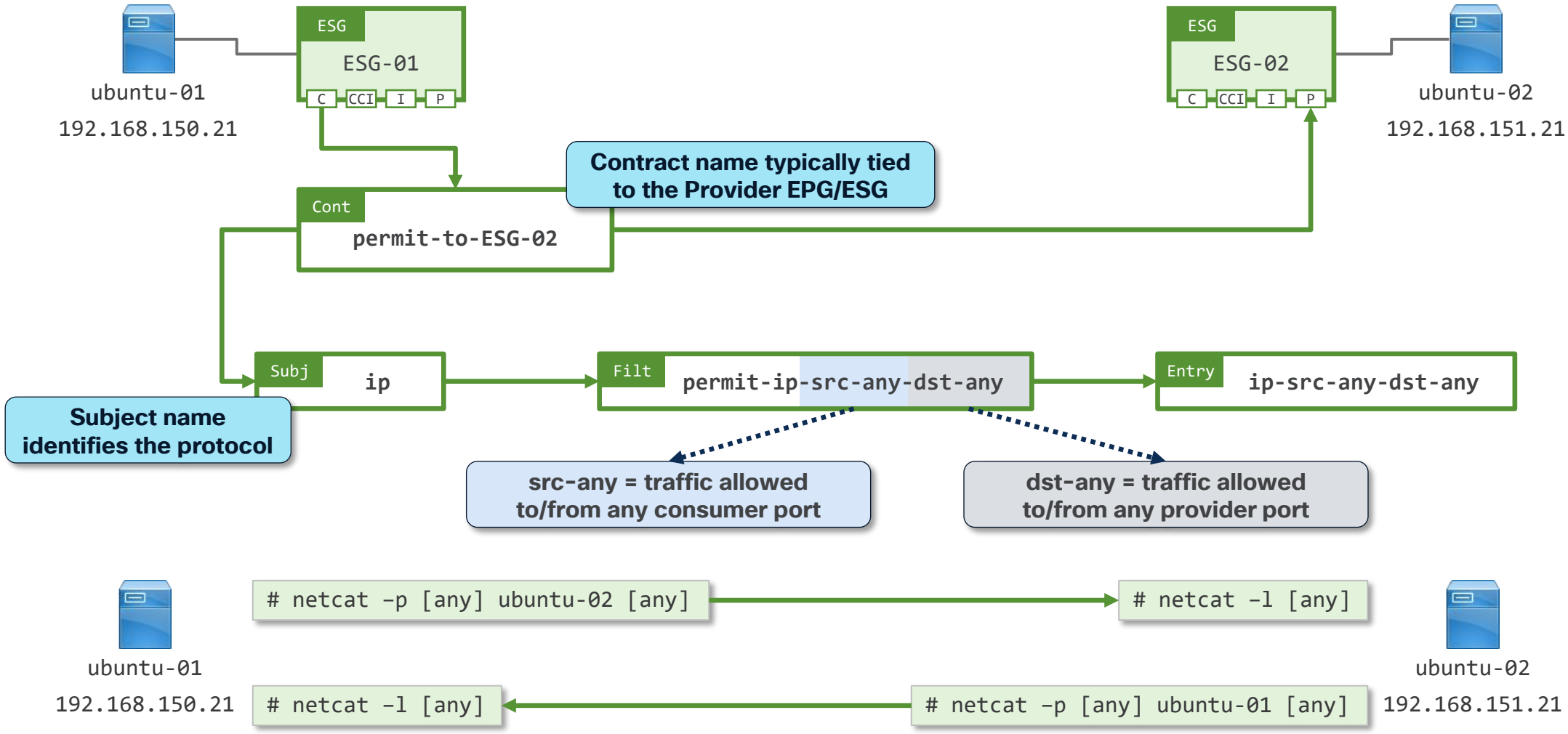
Consumer and provider relationships do not (by default) prevent TCP connections being established from the provider to the consumer

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Contract structure...

Use clear and explicit naming for filters and entries

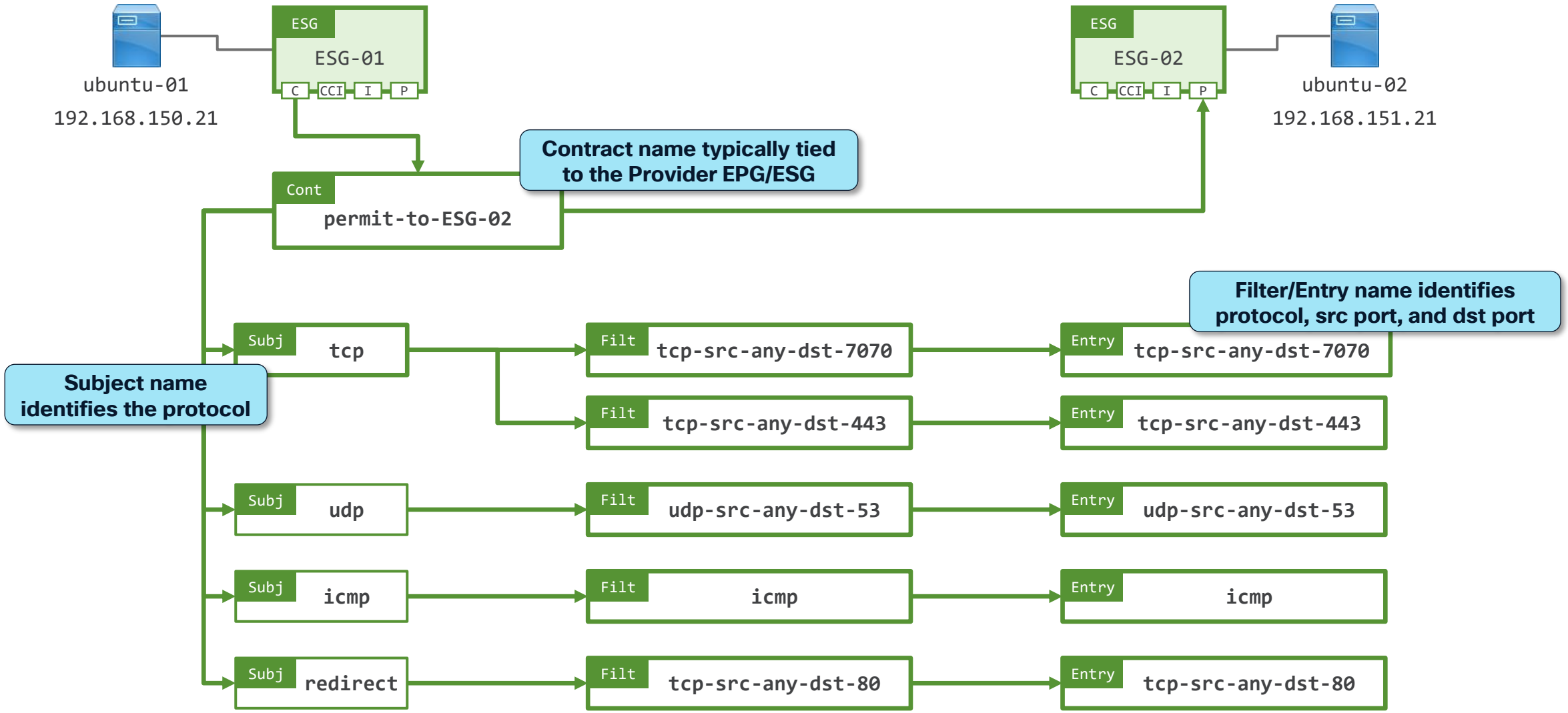


© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Contract structure...

Use clear and explicit naming for filters and entries



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Getting into the weeds on Contracts...

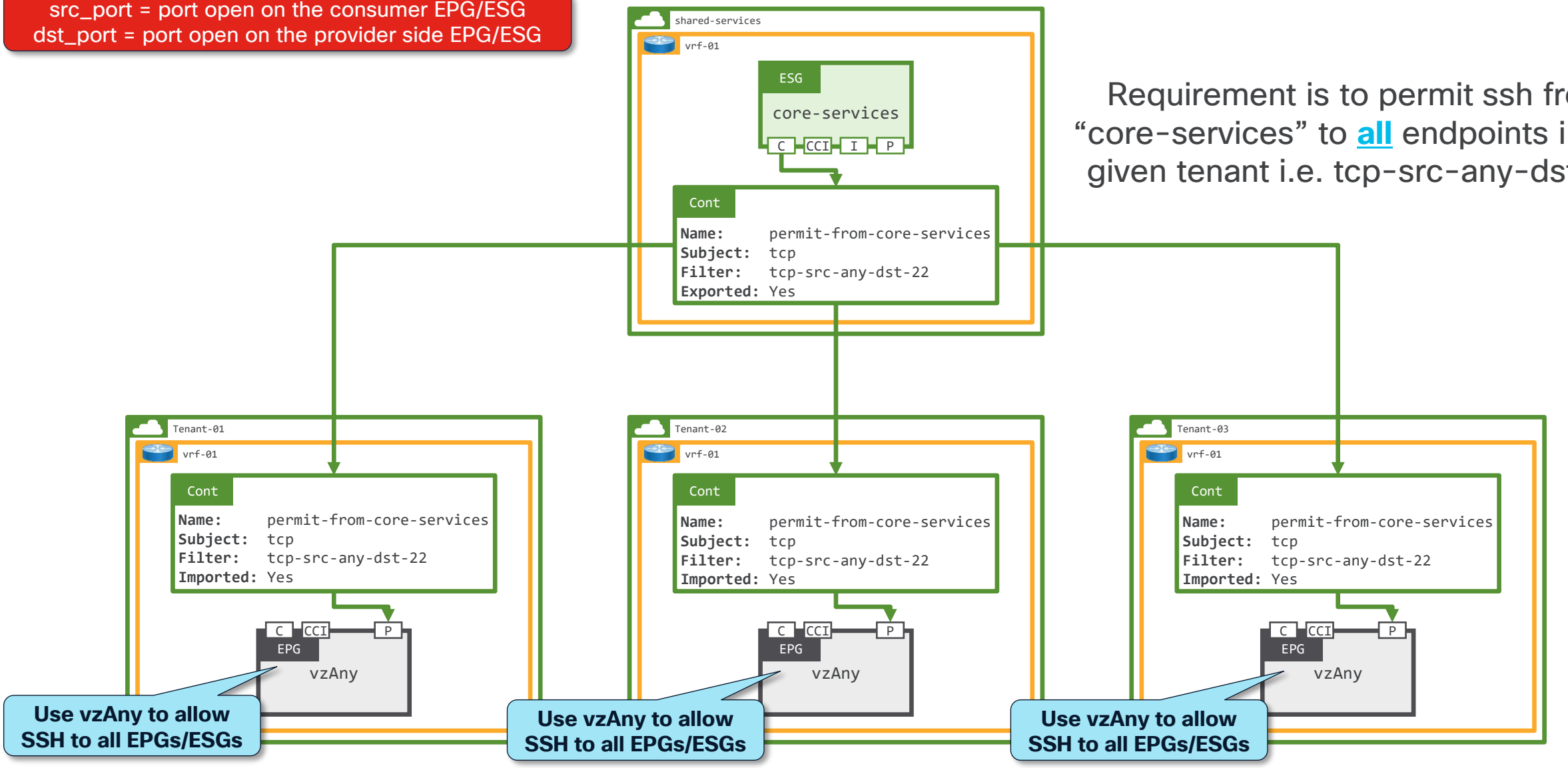
© 2025 Cisco and/or its affiliates. All rights reserved.

I want to be able to ssh to all the endpoints in my network from my management network...

© 2025 Cisco and/or its affiliates. All rights reserved.

Dual VRF – vzAny is the contract provider

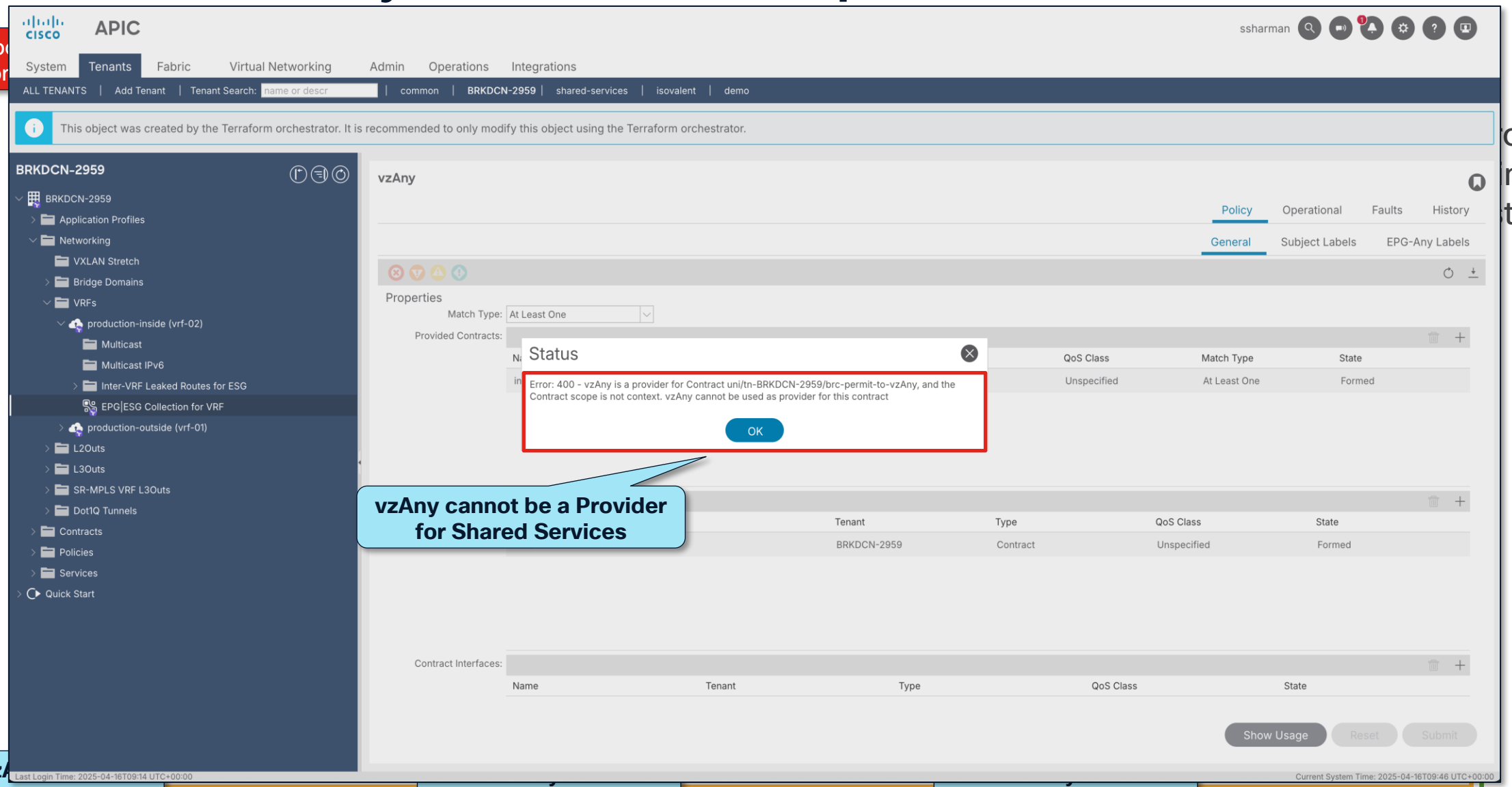
src_port = port open on the consumer EPG/ESG
dst_port = port open on the provider side EPG/ESG



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

© 2025 Cisco and/or its affiliates. All rights reserved.

Dual VRF – vzAny is the contract provider

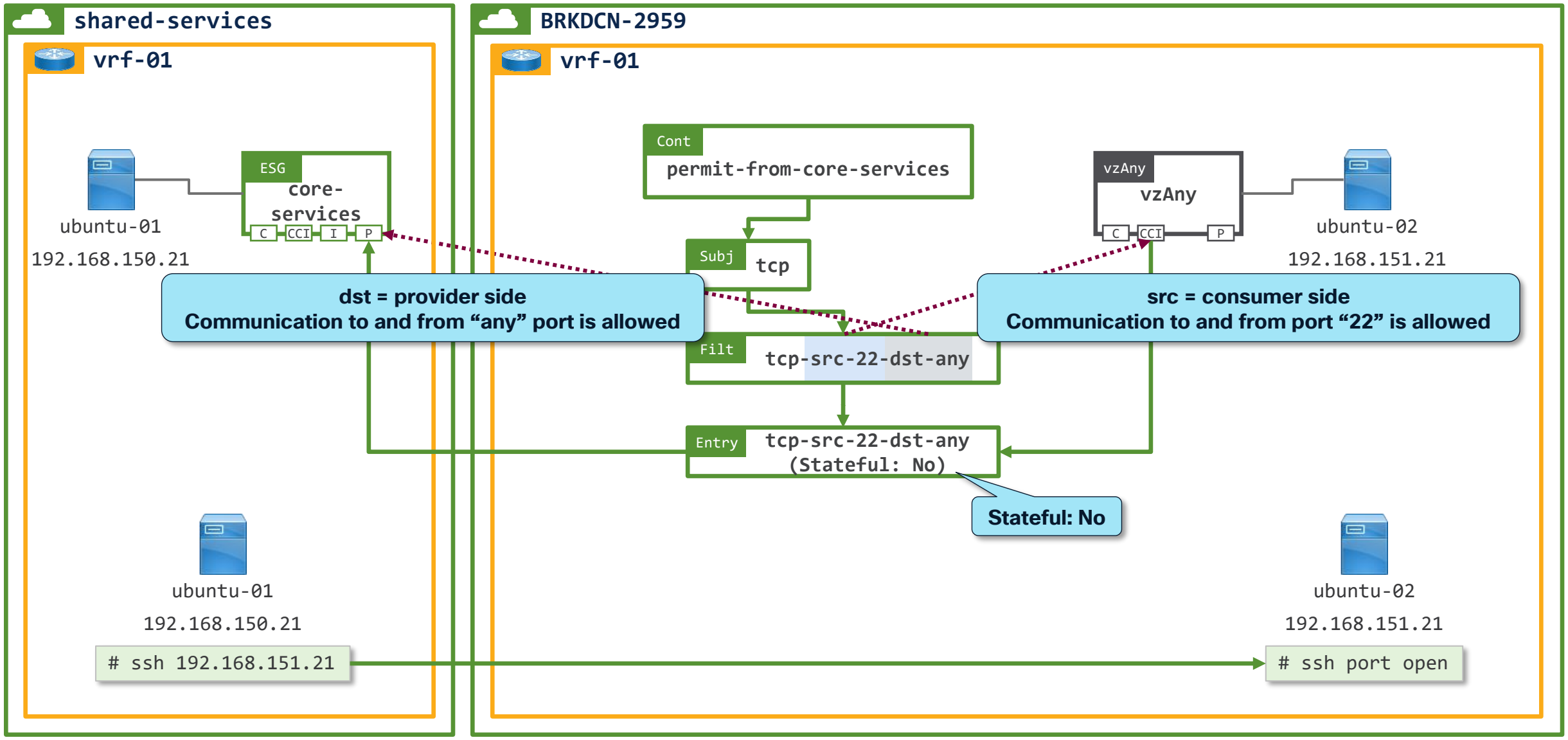


© 2025 Cisco and/or its affiliates. All rights reserved.

How can I use vzAny as a shared services Provider...?

© 2025 Cisco and/or its affiliates. All rights reserved.

Reversing filter ports – stateful = no

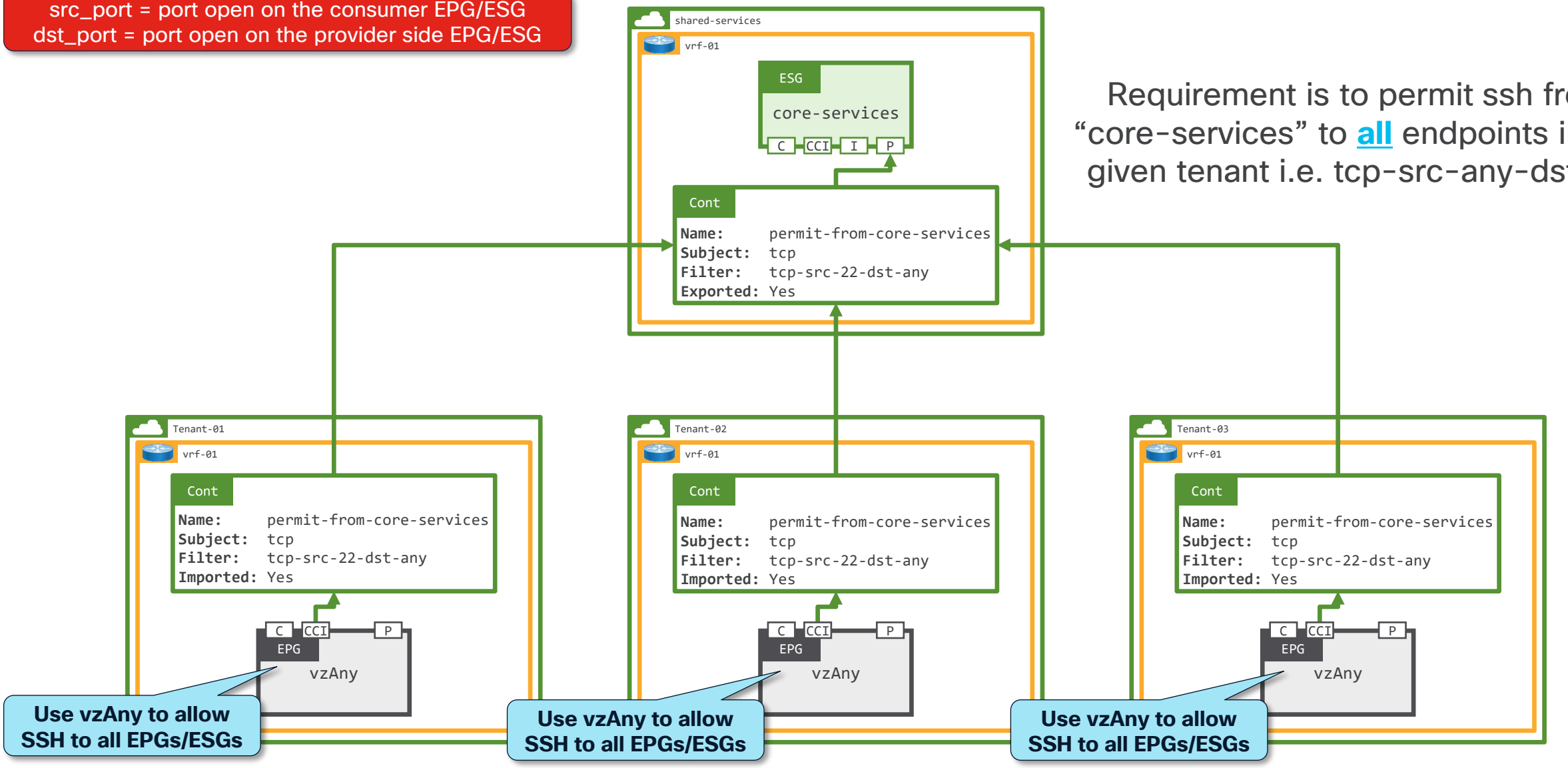


© 2025 Cisco and/or its affiliates. All rights reserved.

https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959/data/09-production-shared-l3out-design-l3out-provider-ssh-to-vzAny.nac.yaml

vzAny as a contract consumer – Filters reversed

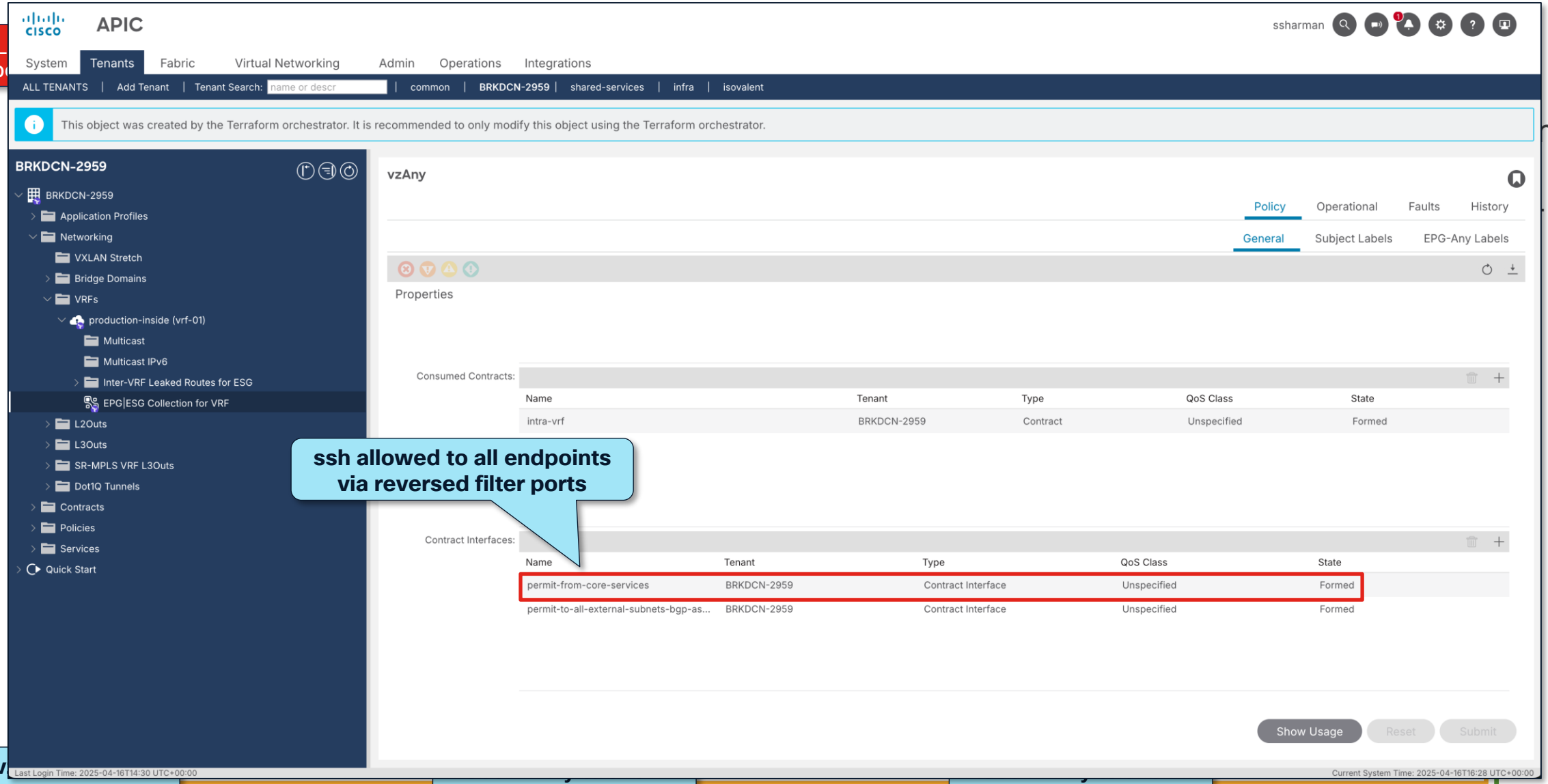
src_port = port open on the consumer EPG/ESG
dst_port = port open on the provider side EPG/ESG



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

© 2025 Cisco and/or its affiliates. All rights reserved.

vzAny as a contract consumer – Filters reversed



SSH to all EPGs/ESGs

SSH to all EPGs/ESGs

SSH to all EPGs/ESGs

© 2025 Cisco and/or its affiliates. All rights reserved.

Customer requirement

Migrate from IP based security policies to user and application-based security policies

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

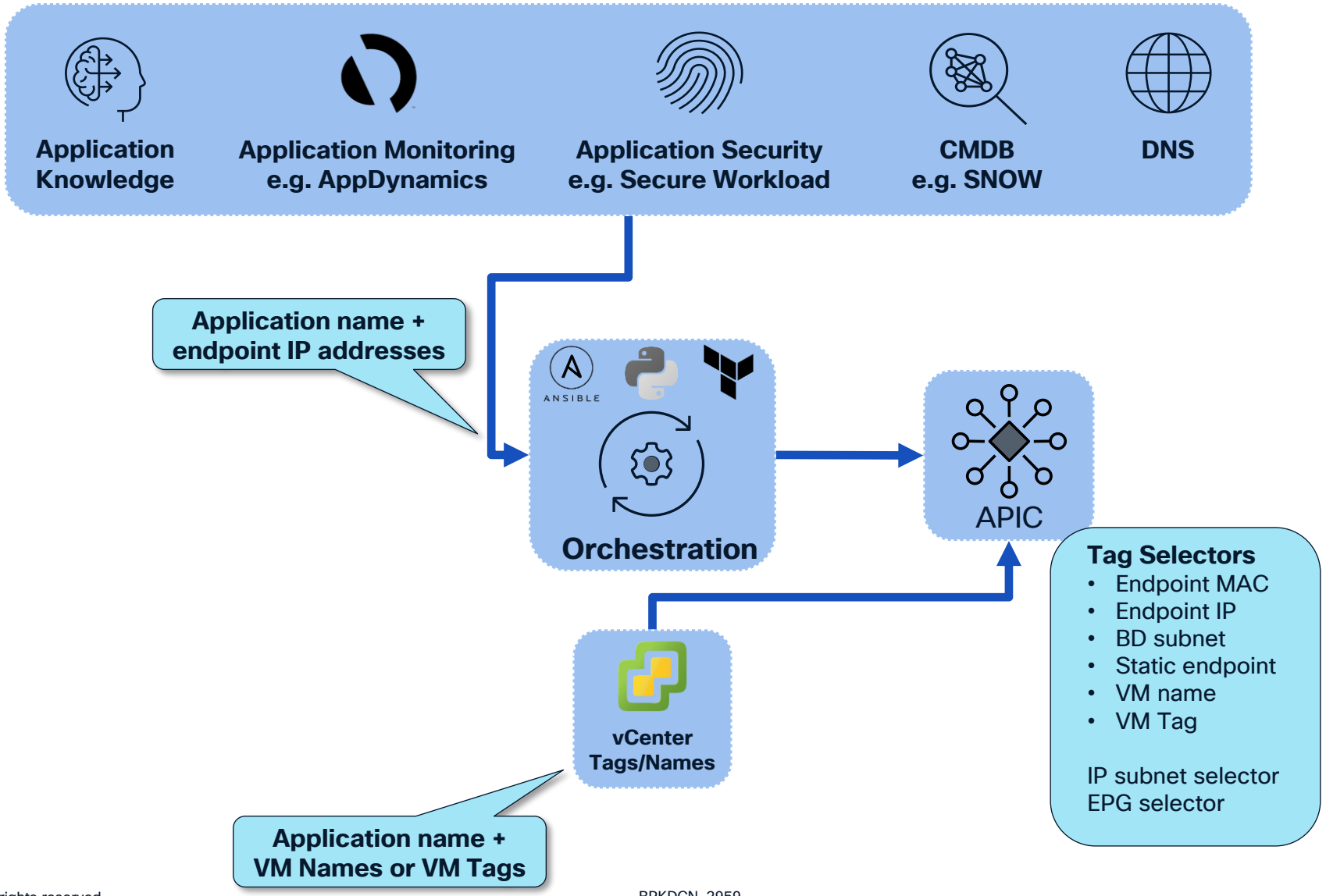
Zero trust application based security…

- Where networking and security come together…
- Customer’s current network design…
- Security control over inbound traffic…
- Understanding ACI security…
- **Zero trust application-based security…**
- Layer 7 security integration…
- DMZ redesign…
- Reducing operational complexity of segmentation
- Implement Zero trust Micro-segmentation

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

© 2025 Cisco and/or its affiliates. All rights reserved.

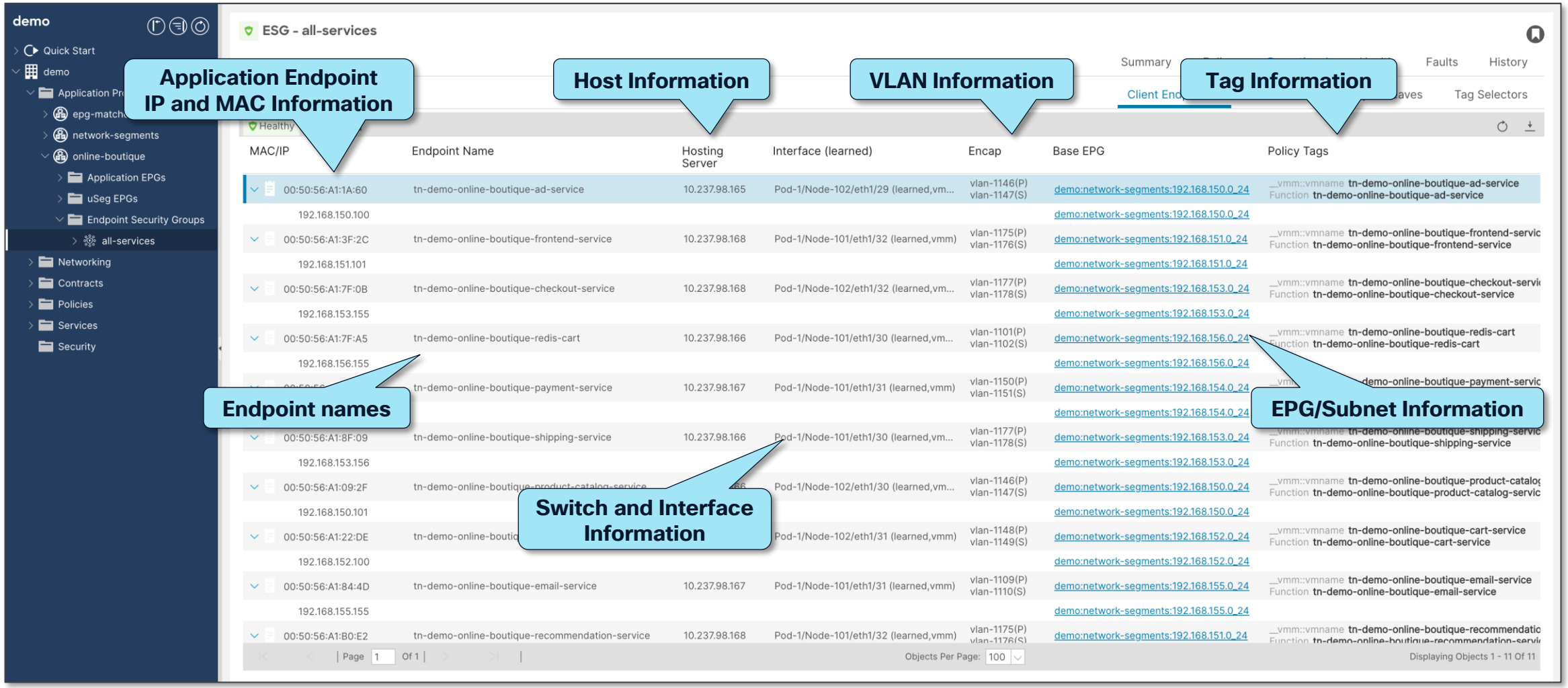
Application IP address details from any source



© 2025 Cisco and/or its affiliates. All rights reserved.

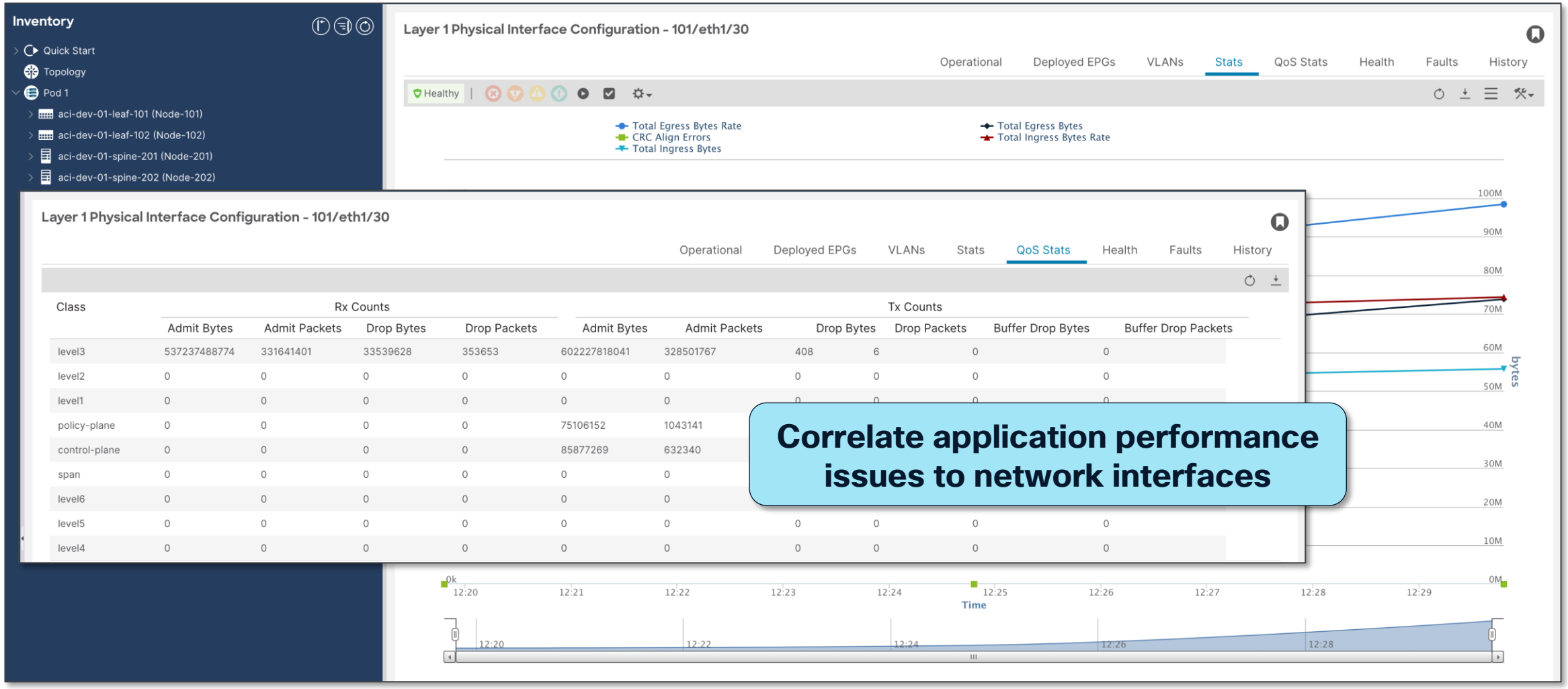
cisco

Understand where your application is running on the network



© 2025 Cisco and/or its affiliates. All rights reserved.

Are there errors or excessive drops, affecting the application...?



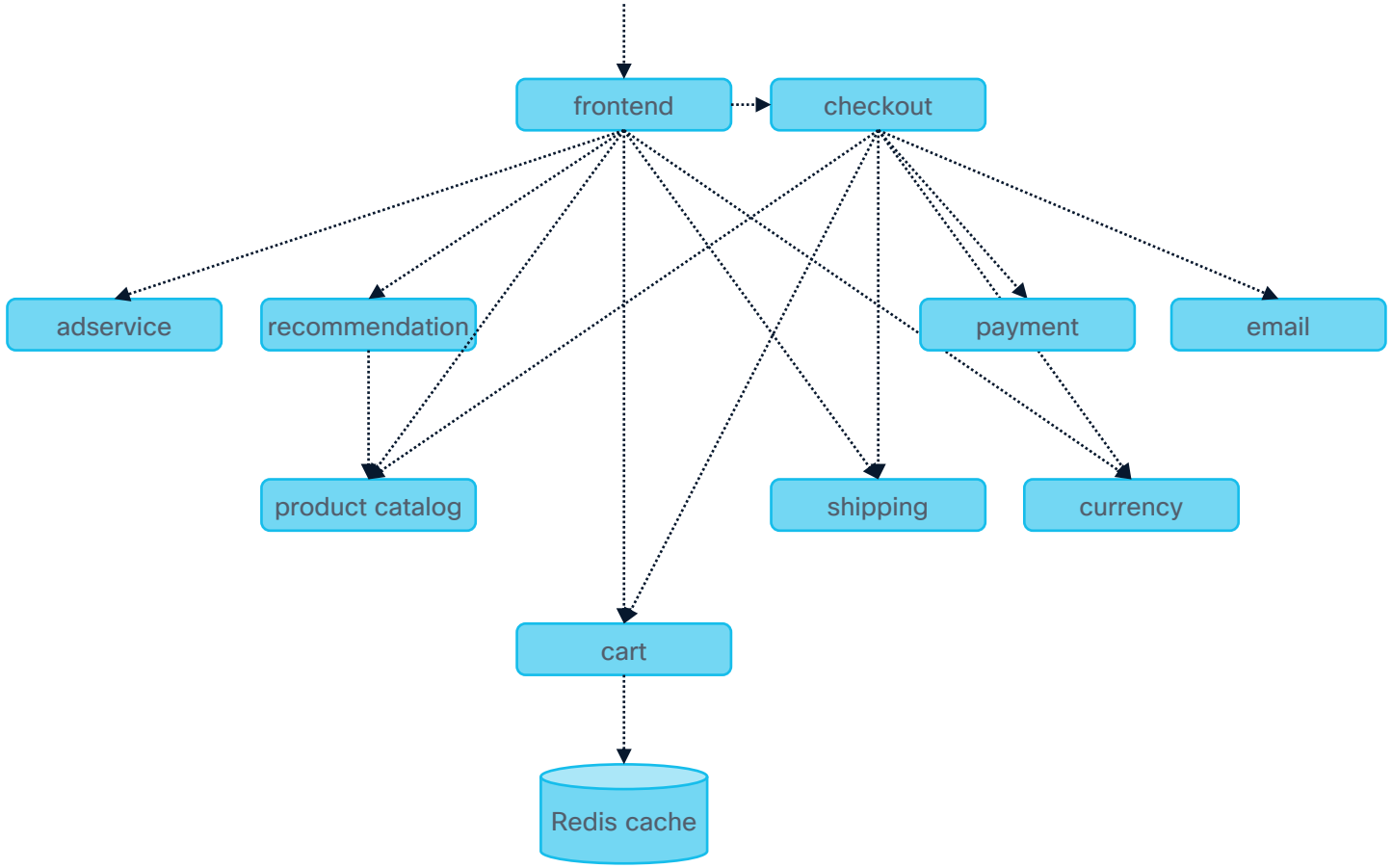
© 2025 Cisco and/or its affiliates. All rights reserved.

Option 1

Application segmentation and visibility with EPGs...

Online Boutique

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

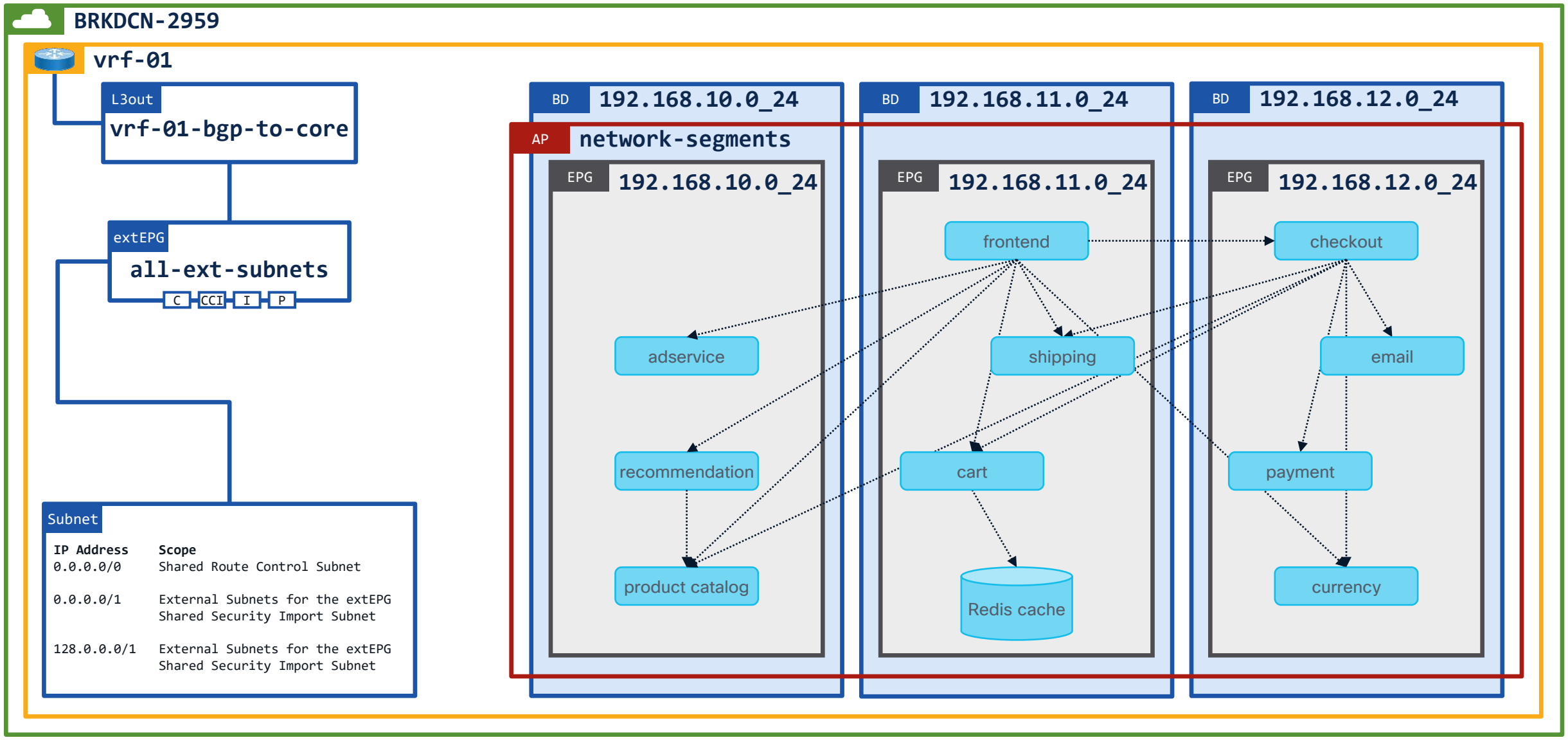


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart currency email payment product catalog shipping	TCP 7070 TCP 7000 TCP 8080 TCP 50051 TCP 3550 TCP 50051
frontend	adservice cart checkout currency product catalog recommendation shipping	TCP 9555 TCP 7070 TCP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

© 2025 Cisco and/or its affiliates. All rights reserved.

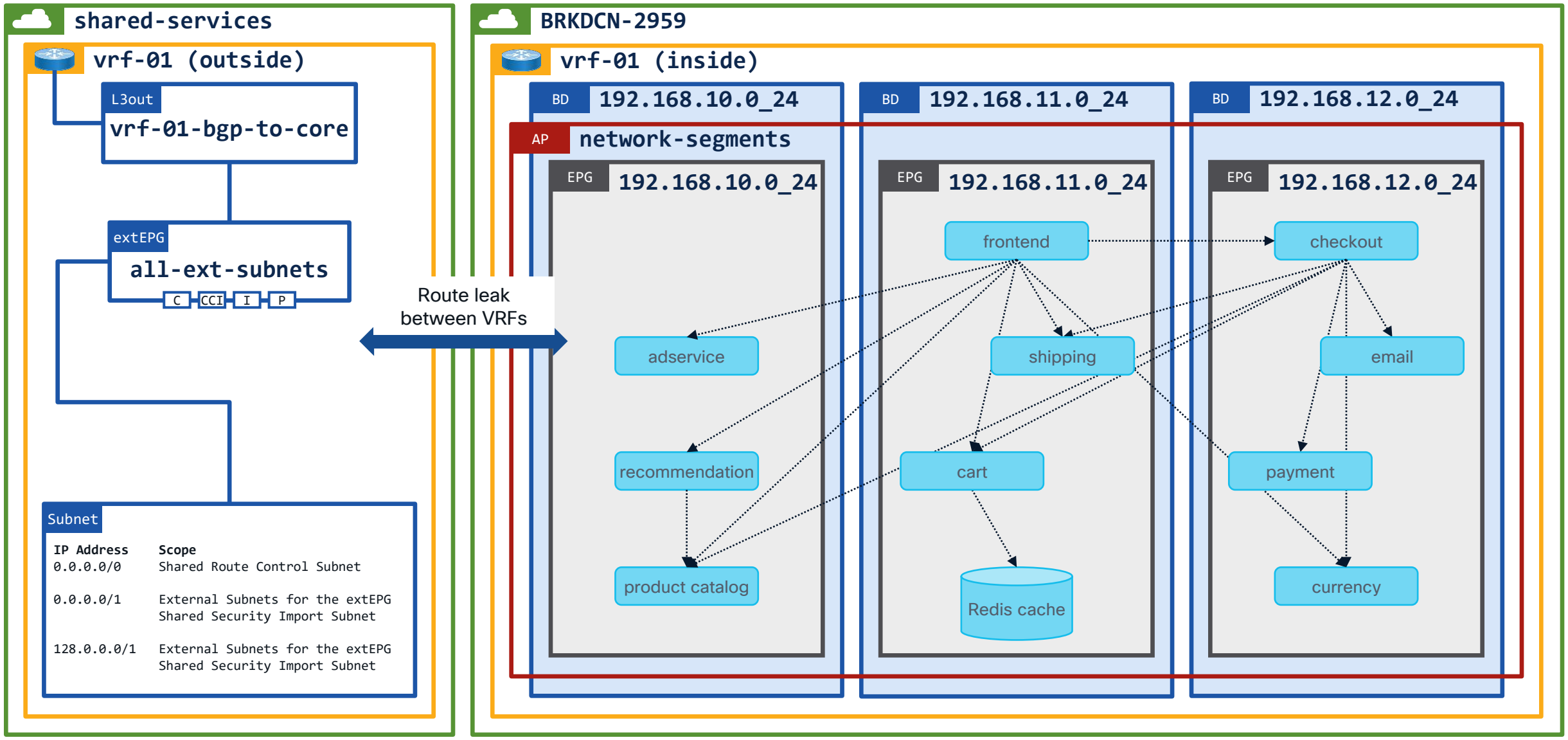
cisco

Application tiers are spread across EPGs



© 2025 Cisco and/or its affiliates. All rights reserved.

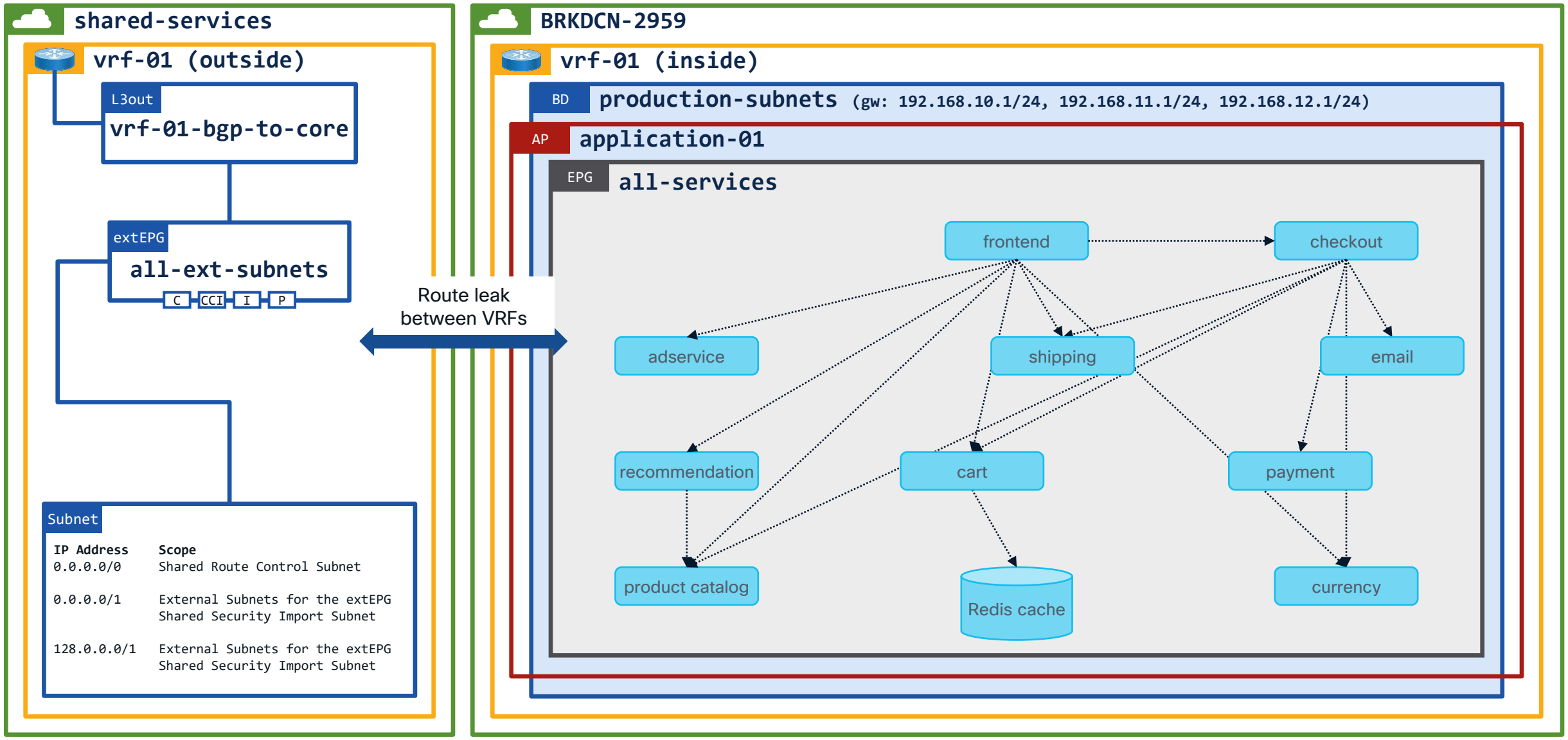
Migrate to a “shared-services” split VRF design



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

End goal is a single EPG (VLAN) per application



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

No time to get into the weeds on how to migrate...

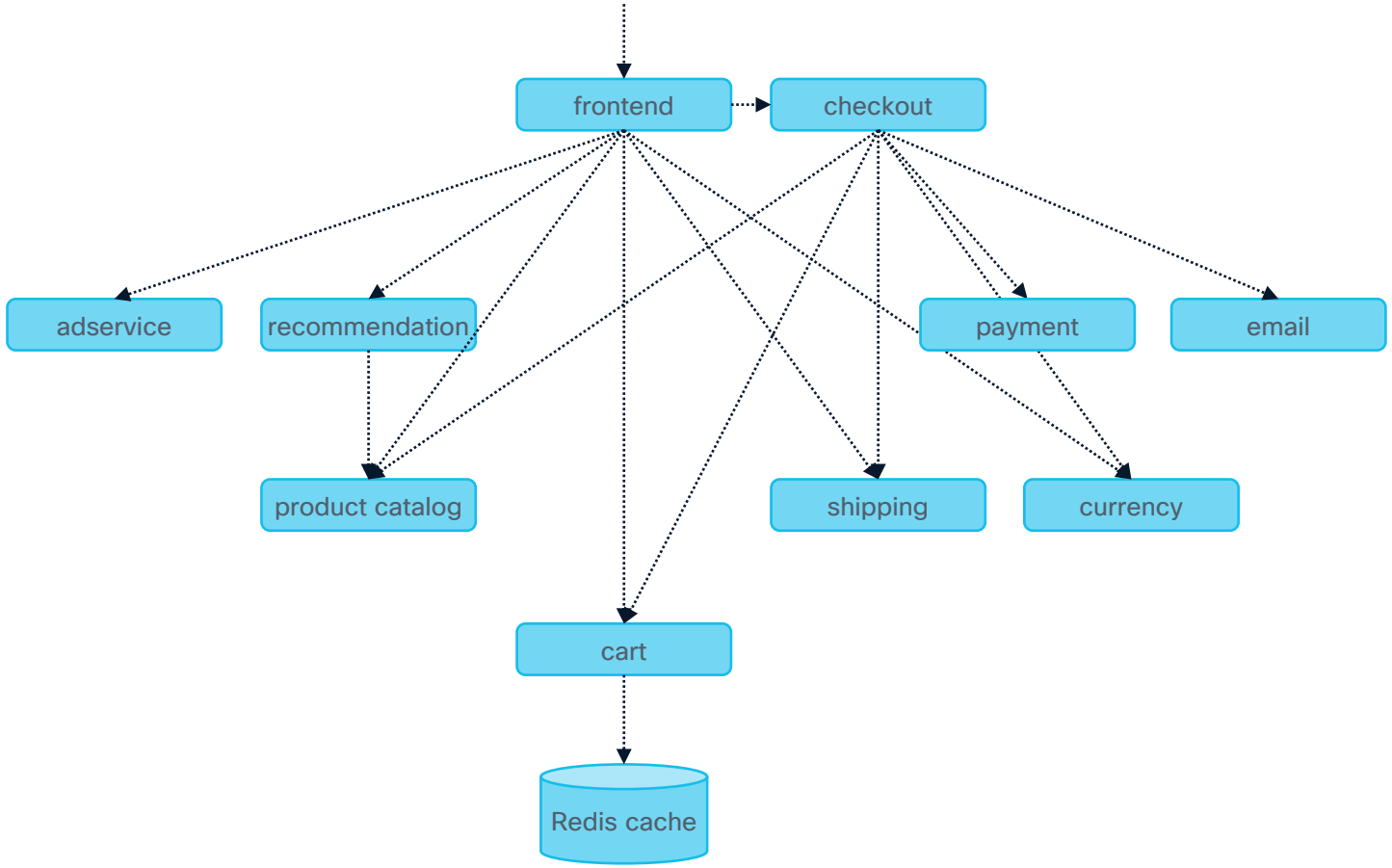
© 2025 Cisco and/or its affiliates. All rights reserved.

Option 2

Application segmentation and visibility with ESGs...

Online Boutique

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

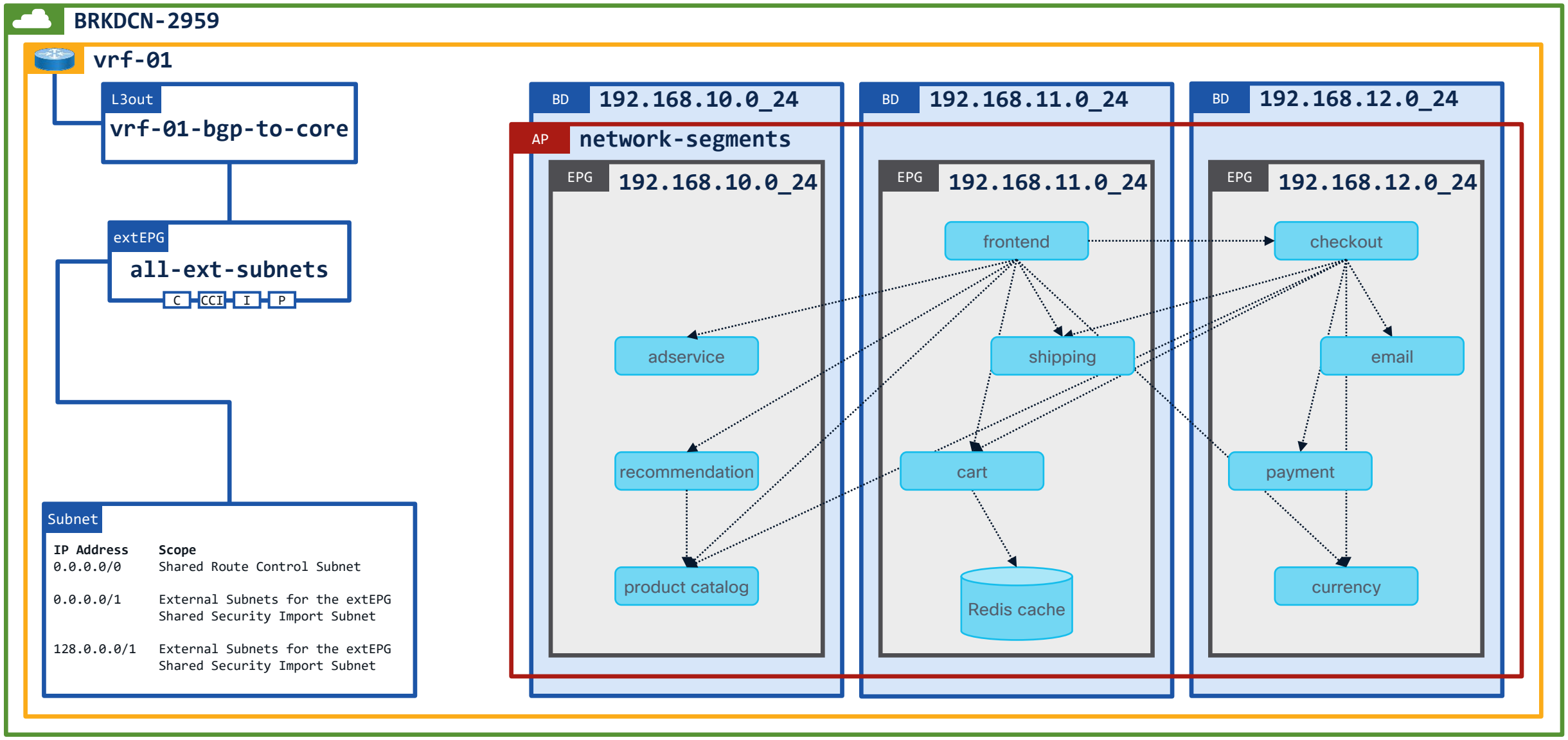


Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart currency email payment product catalog shipping	TCP 7070 TCP 7000 TCP 8080 TCP 50051 TCP 3550 TCP 50051
frontend	adservice cart checkout currency product catalog recommendation shipping	TCP 9555 TCP 7070 TCP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

© 2025 Cisco and/or its affiliates. All rights reserved.

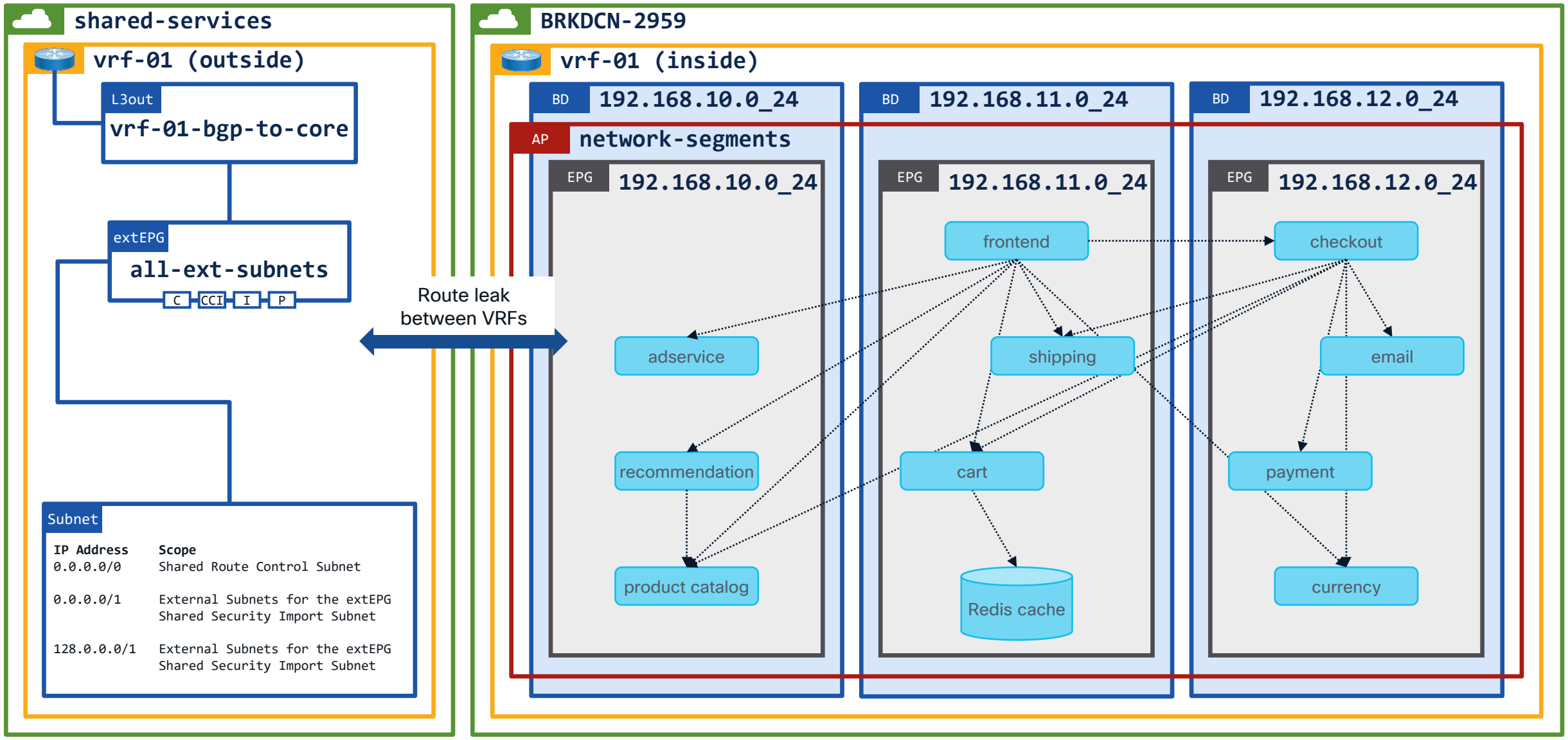
cisco

Application tiers are spread across EPGs



© 2025 Cisco and/or its affiliates. All rights reserved.

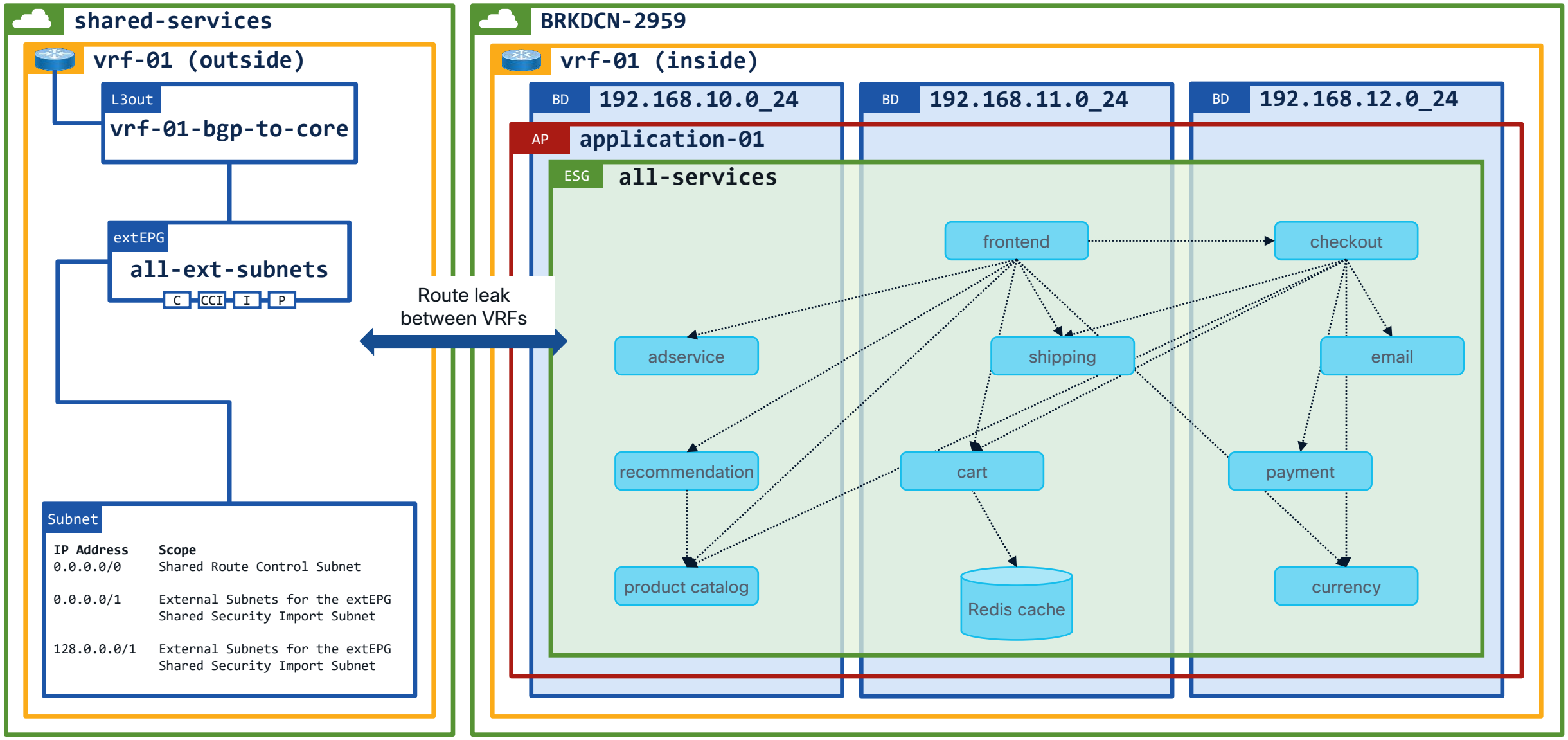
Migrate to a “shared-services” split VRF design



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Single ESG per application



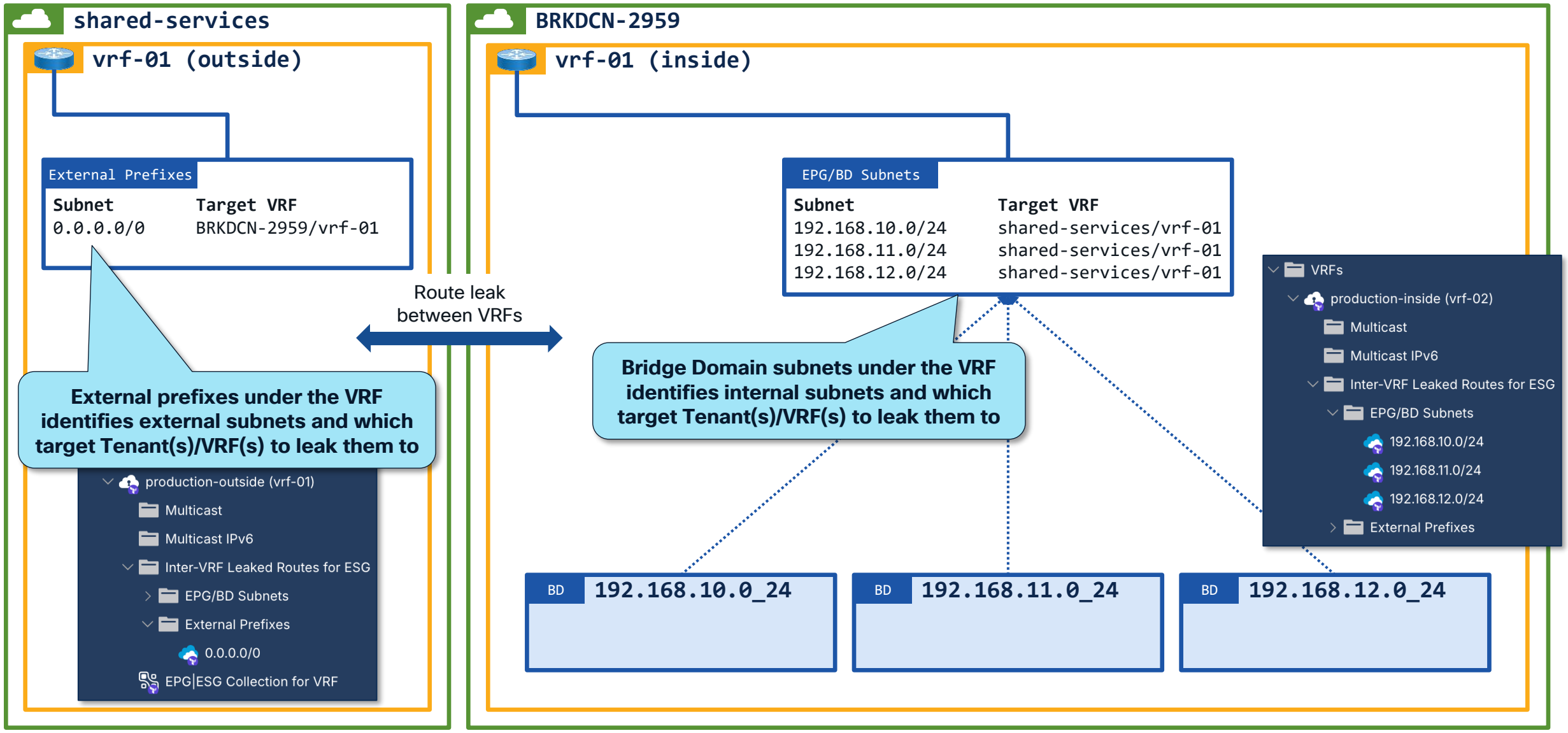
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

What are the migration steps...?

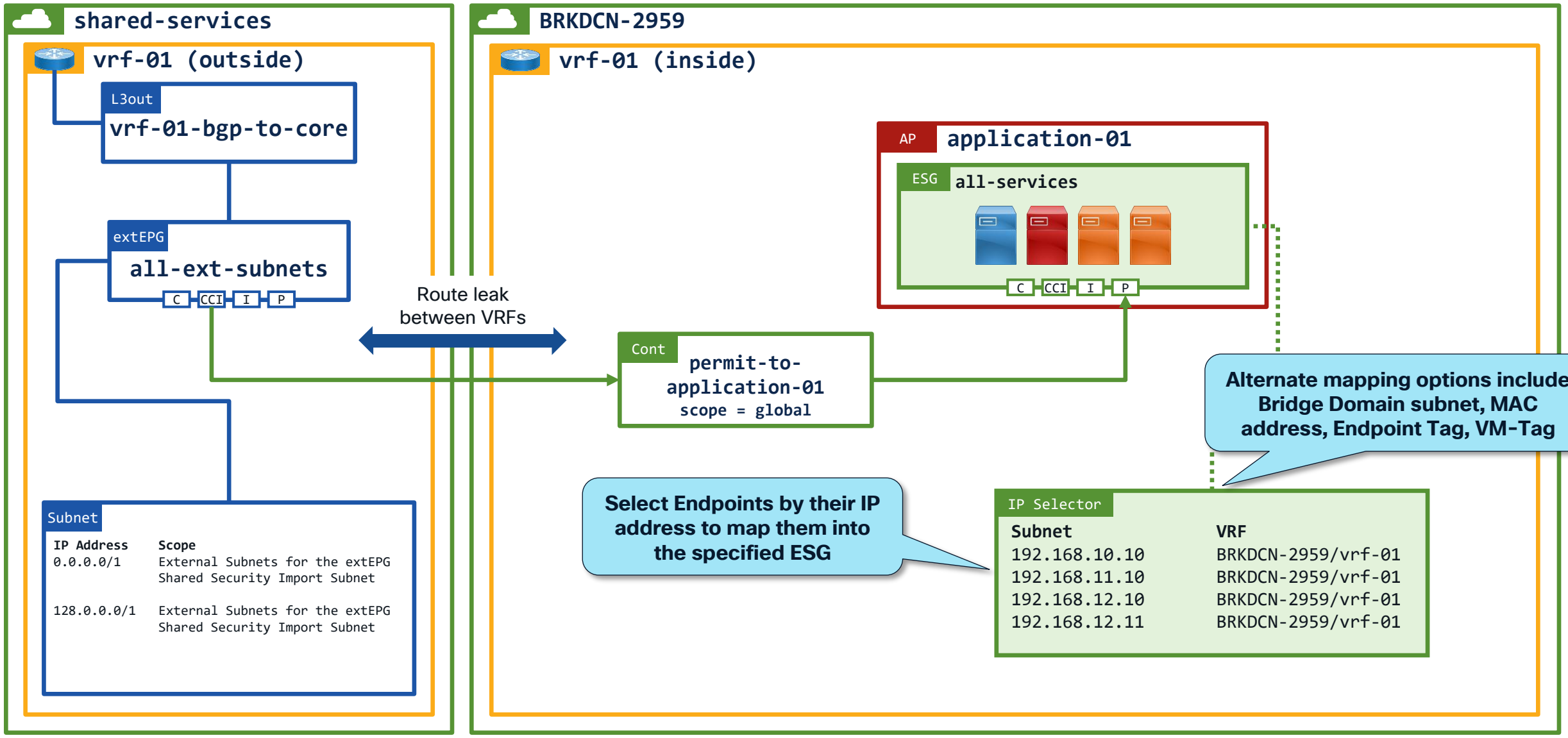
© 2025 Cisco and/or its affiliates. All rights reserved.

Leak Routes between VRFs for ESGs



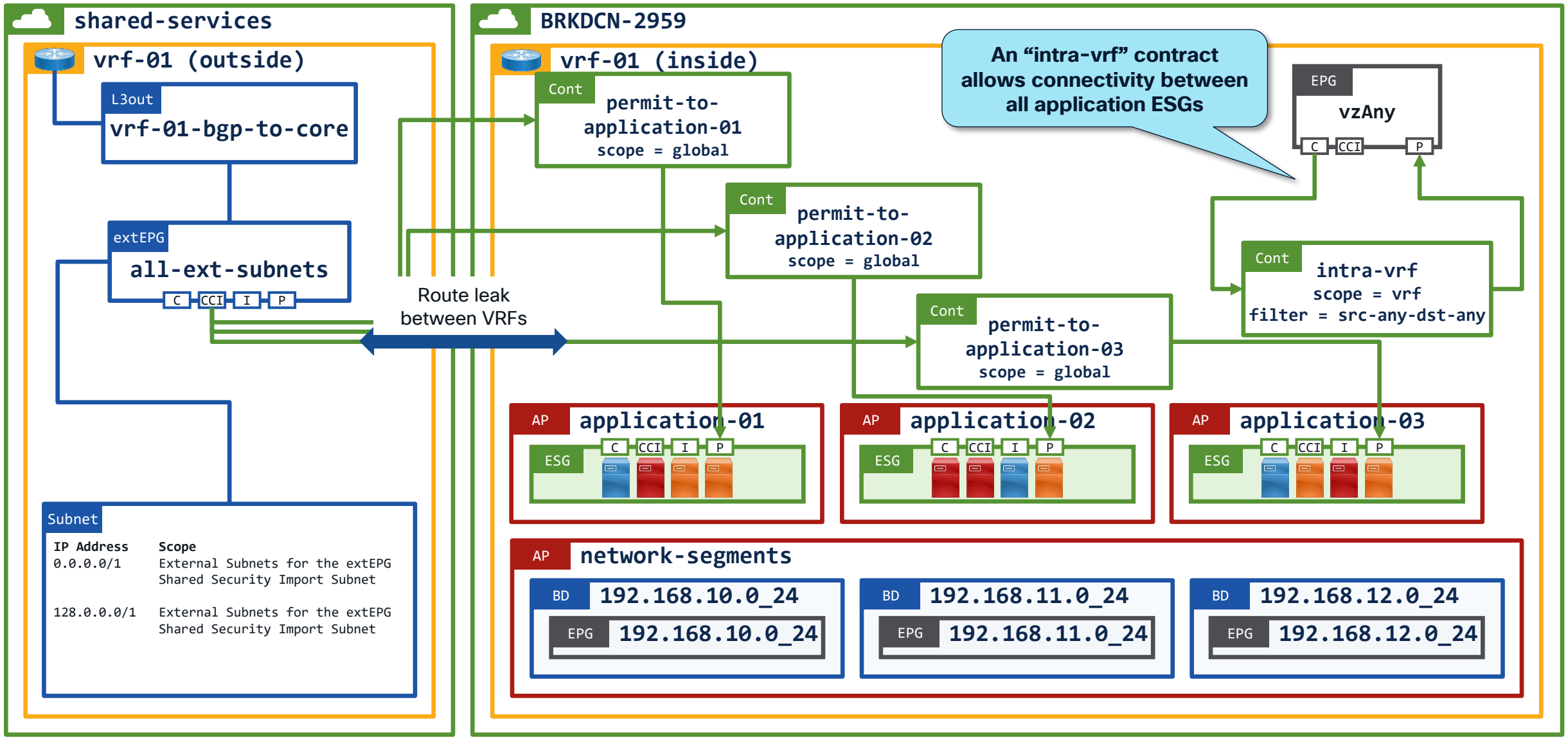
© 2025 Cisco and/or its affiliates. All rights reserved.

Map endpoints to an ESG



© 2025 Cisco and/or its affiliates. All rights reserved.

Endpoint security decoupled from BD/EPG boundary



© 2025 Cisco and/or its affiliates. All rights reserved.

https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959/data/13-production-shared-l3out-design-esg-l3out-consumer.nac.yaml

Considerations

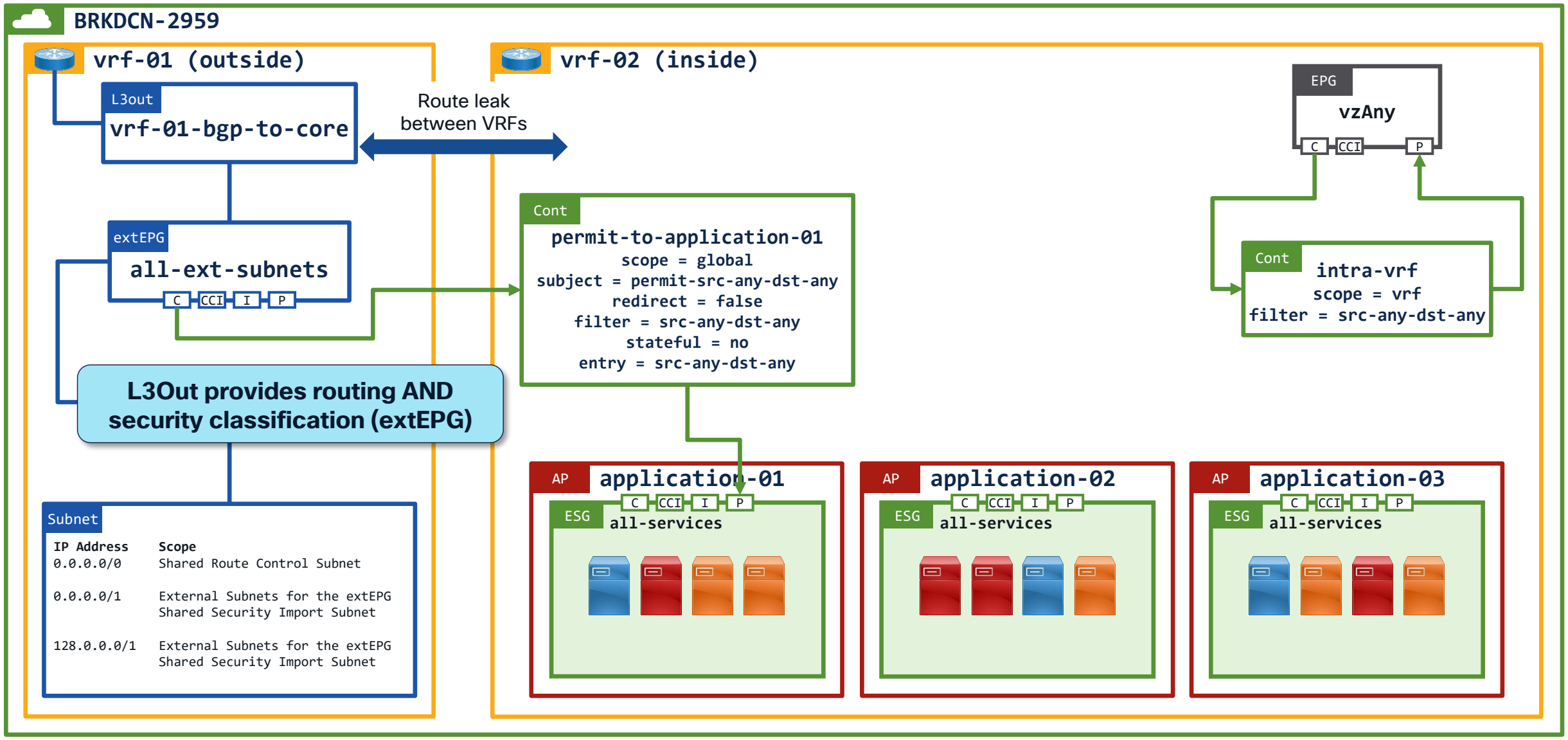
- No changes to Bridge Domains i.e. 1x Bridge Domain mapped to 1x EPG
- Bridge Domains can support one or more gateways
- DHCP allowed
- IGMP snooping policy applied to Bridge Domain
- Private VLANs used to control East / West traffic in the Hypervisor
- Proxy ARP required on the leaf switches
- Minimal traffic interruption whilst Proxy ARP and PVLANs are enabled (change window required)
- Endpoints retain their existing EPG mapping
- **6.1.4 added a new feature allowing external subnets to be classified directly into ESGs**

© 2025 Cisco and/or its affiliates. All rights reserved.

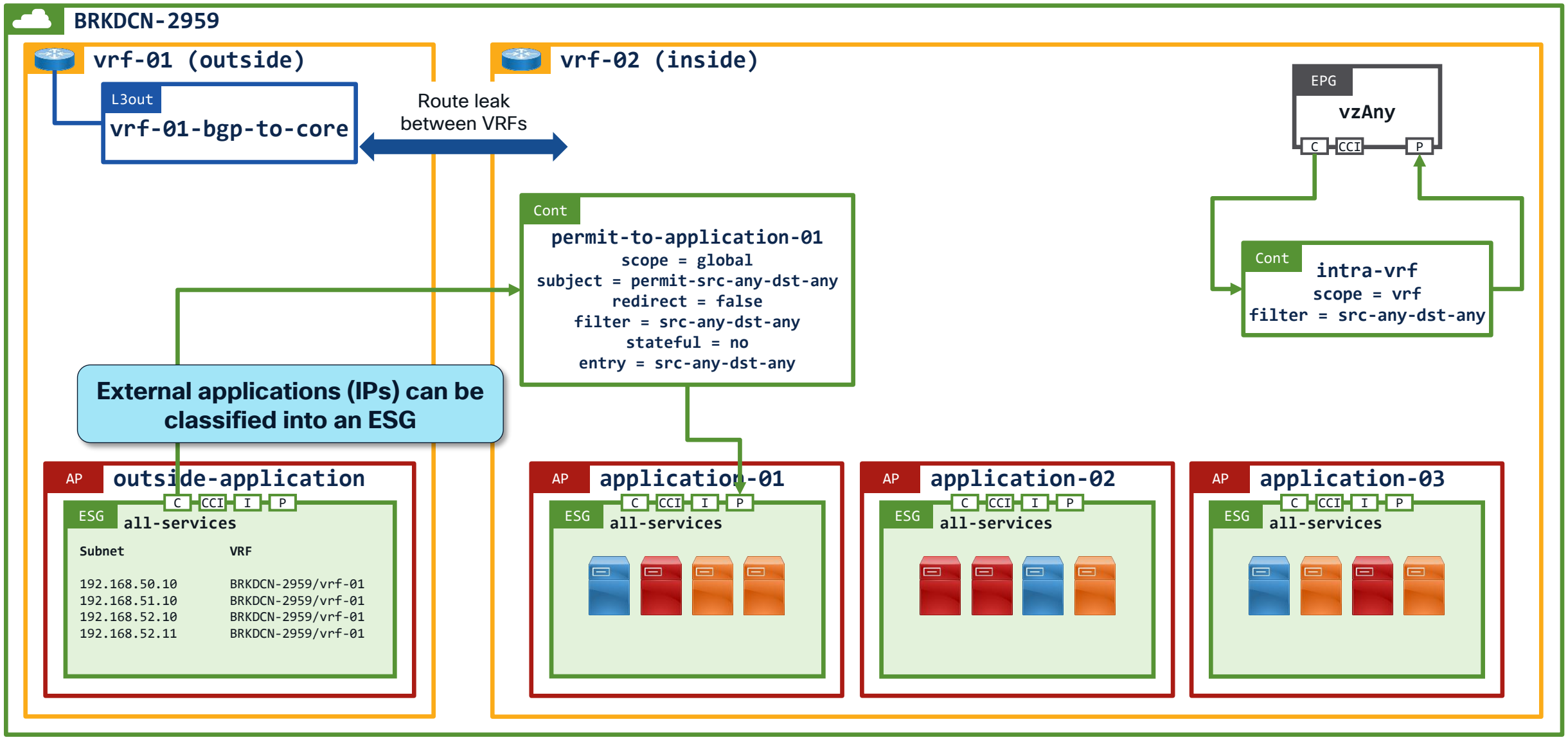
cisco

What’s new with ESGs...

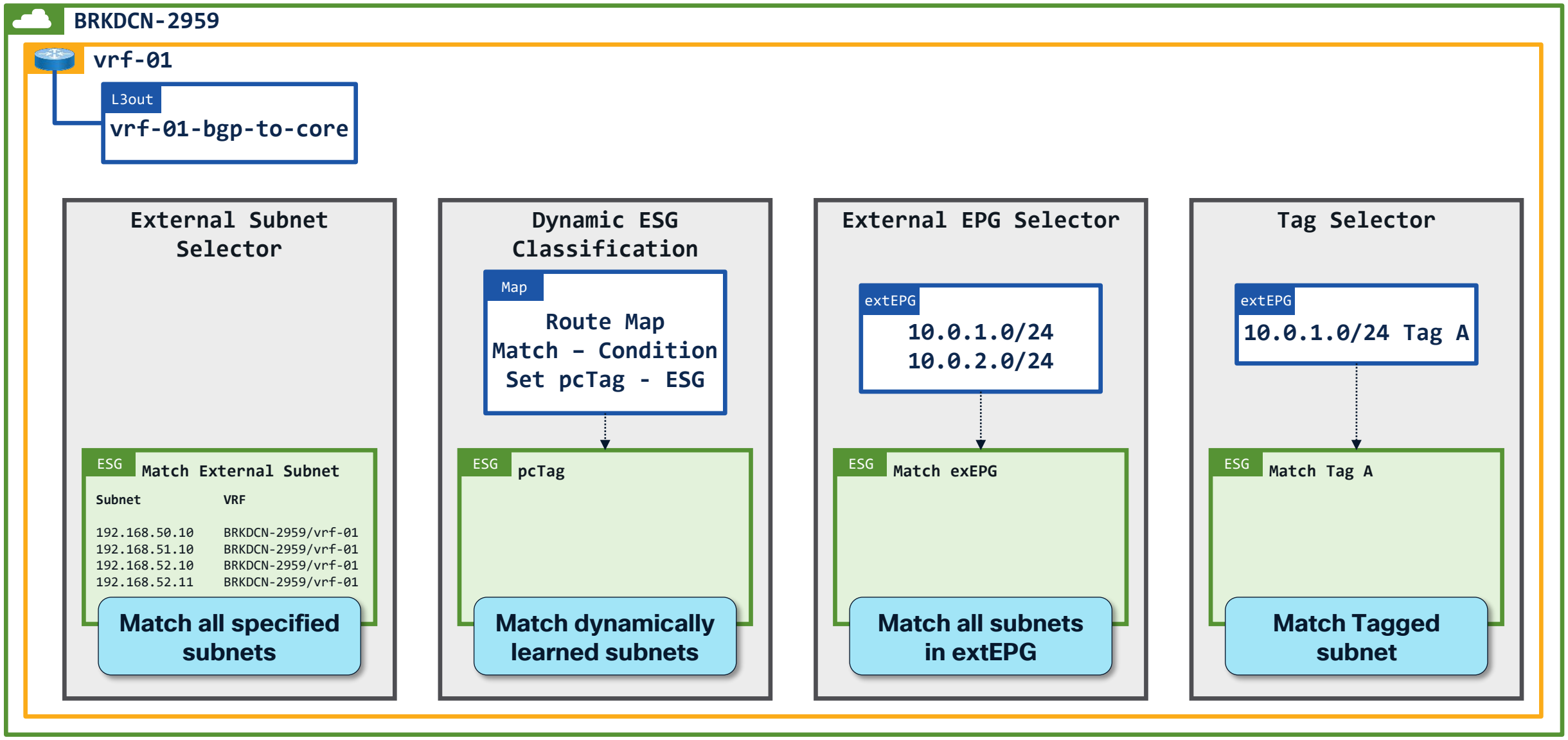
Combined routing and security pre ACI 6.1(4)



Decoupling routing from security – ACI 6.1(4)

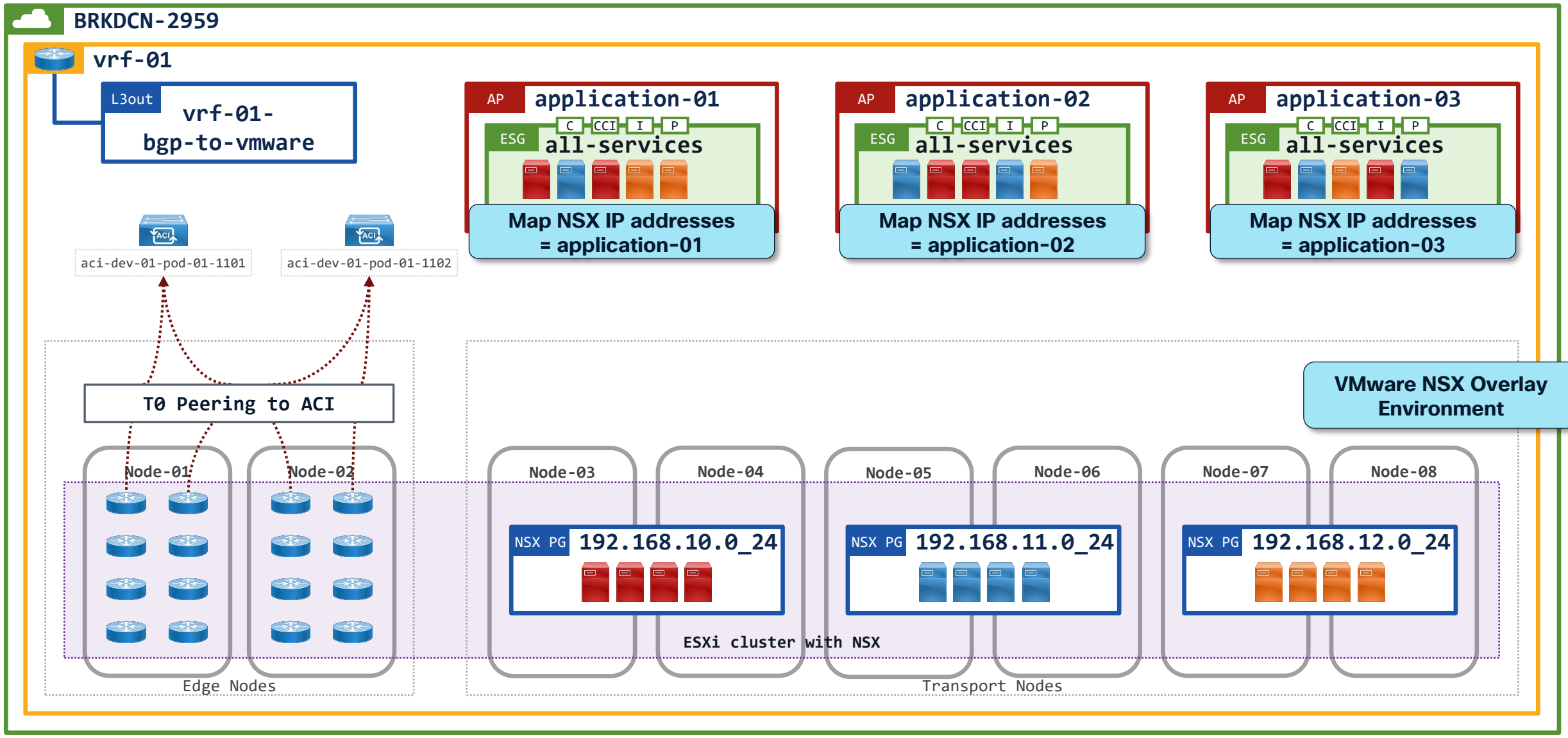


External IP address to ESG classification options



© 2025 Cisco and/or its affiliates. All rights reserved.

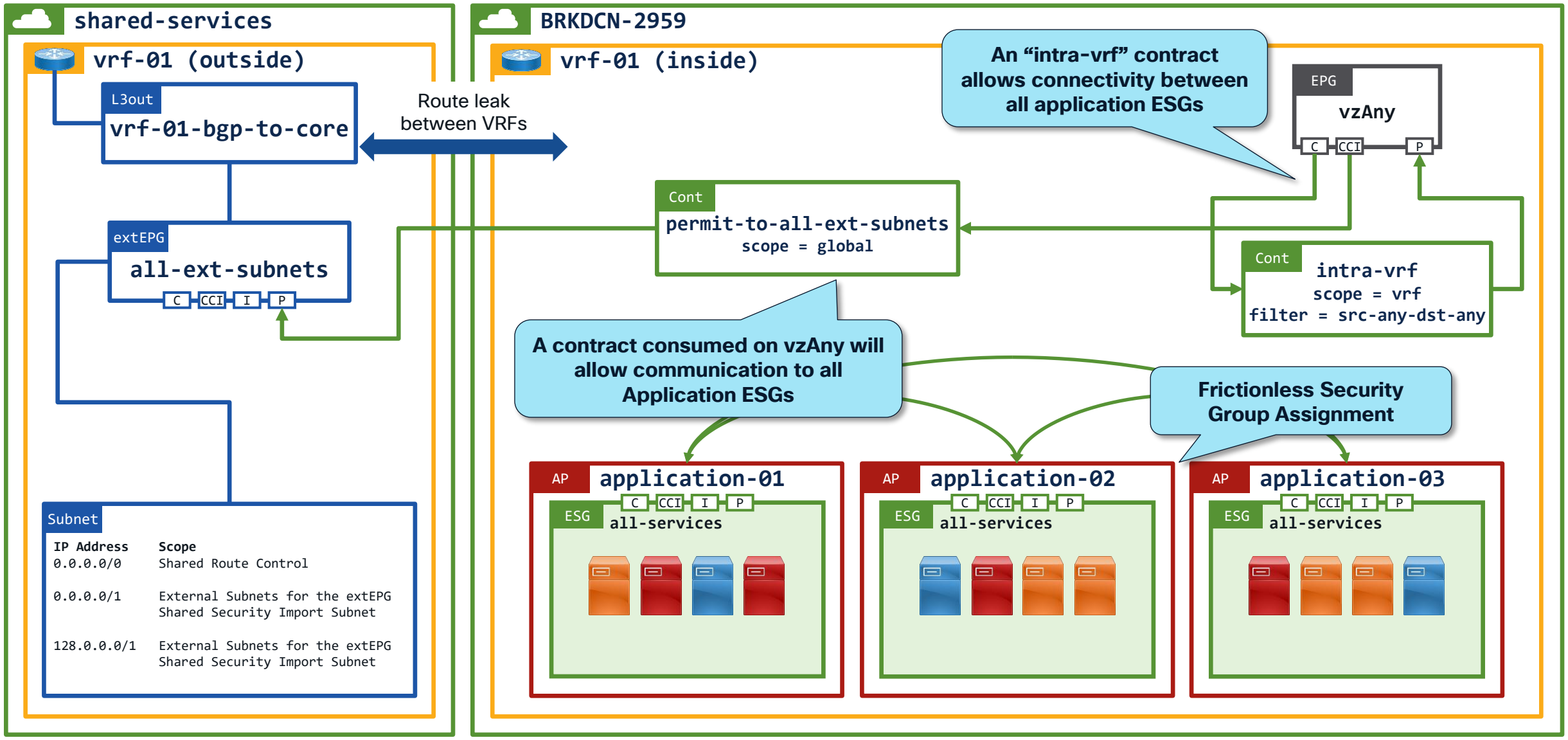
Common classification method from Overlay, Campus, CNI, etc



© 2025 Cisco and/or its affiliates. All rights reserved.

Scaling application connectivity…

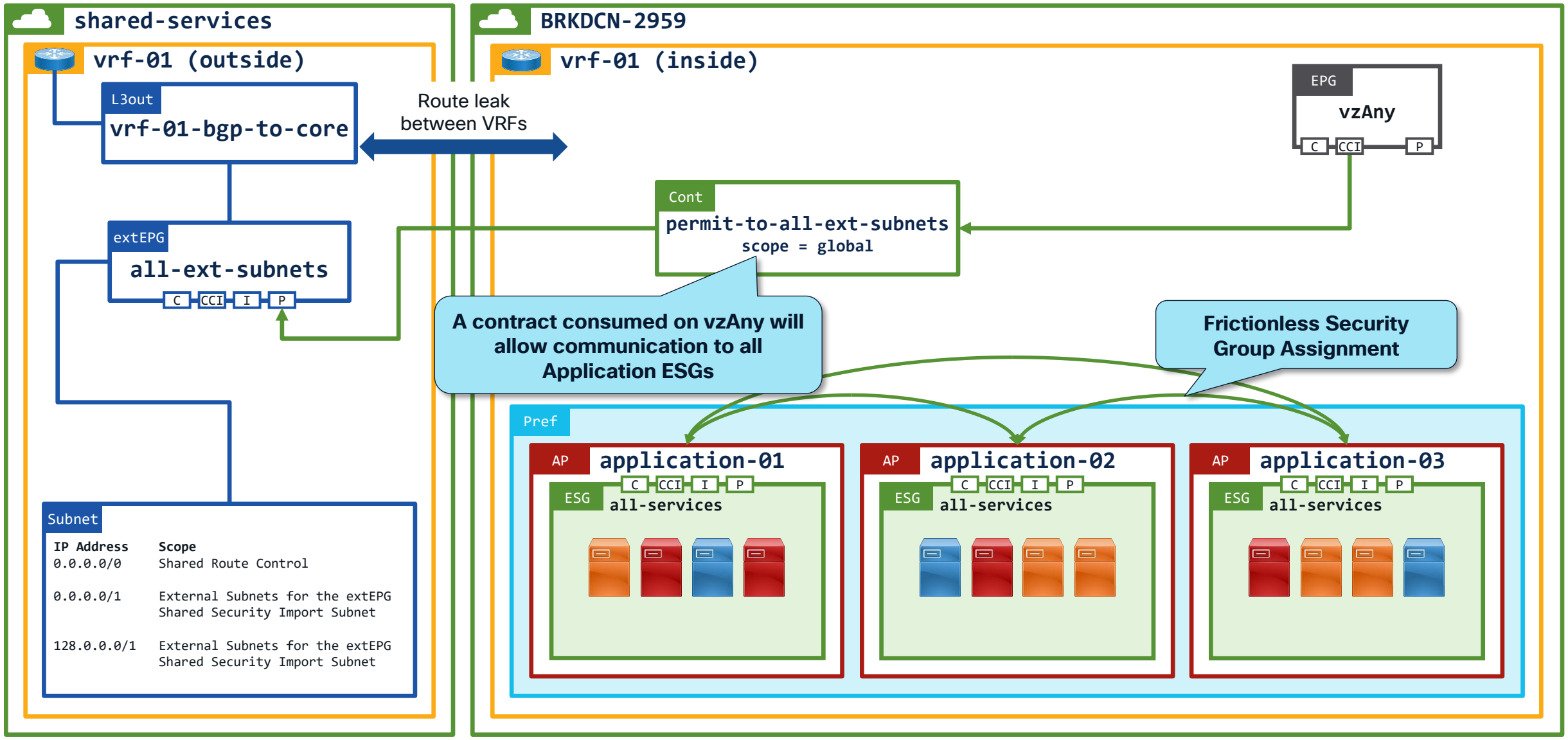
Option 1: Frictionless ESG Assignment with vzAny



© 2025 Cisco and/or its affiliates. All rights reserved.

https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959/data/14-production-shared-l3out-design-esg-l3out-consumer-with-vzAny.nac.yaml

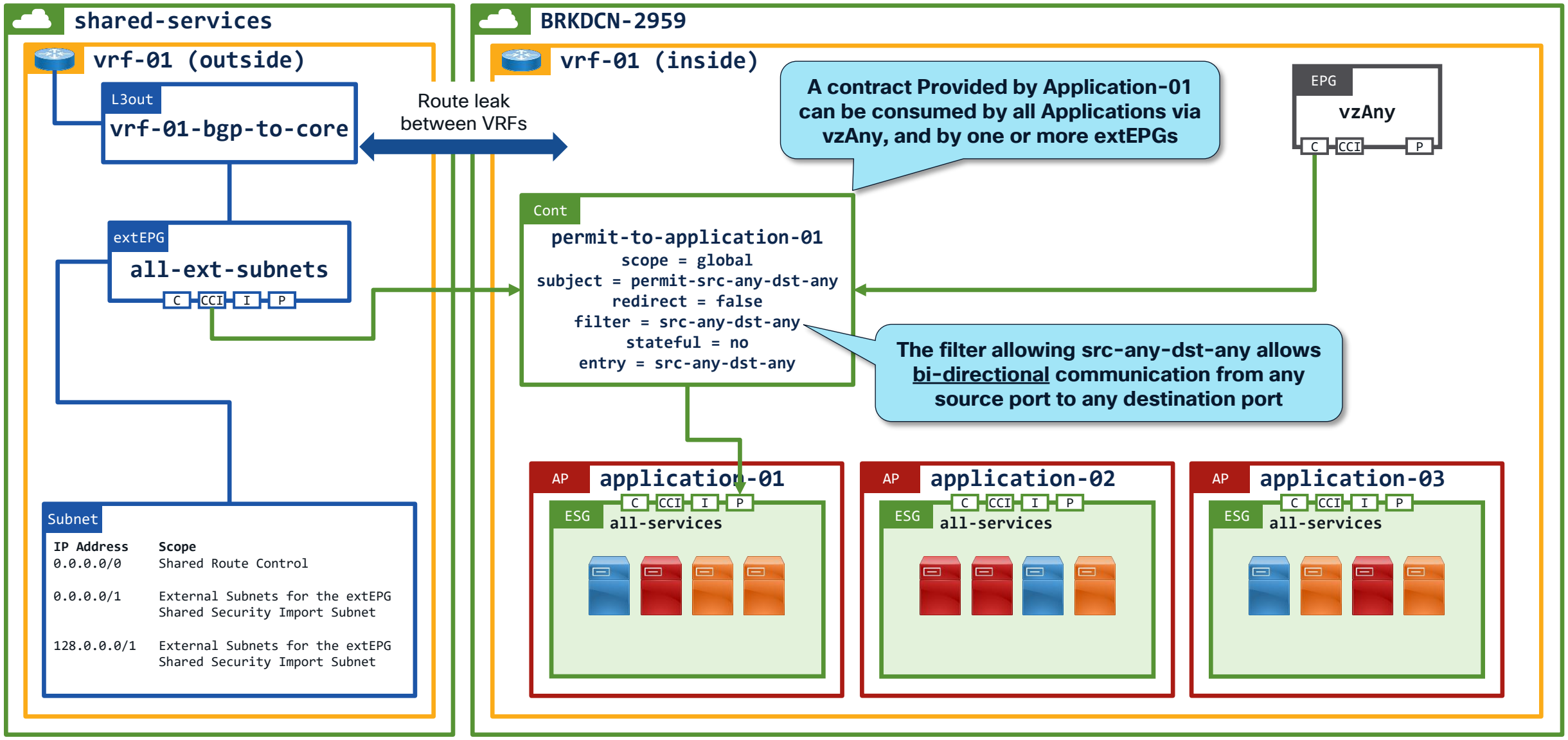
Option 2: Frictionless ESG Assignment with a Preferred Group



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

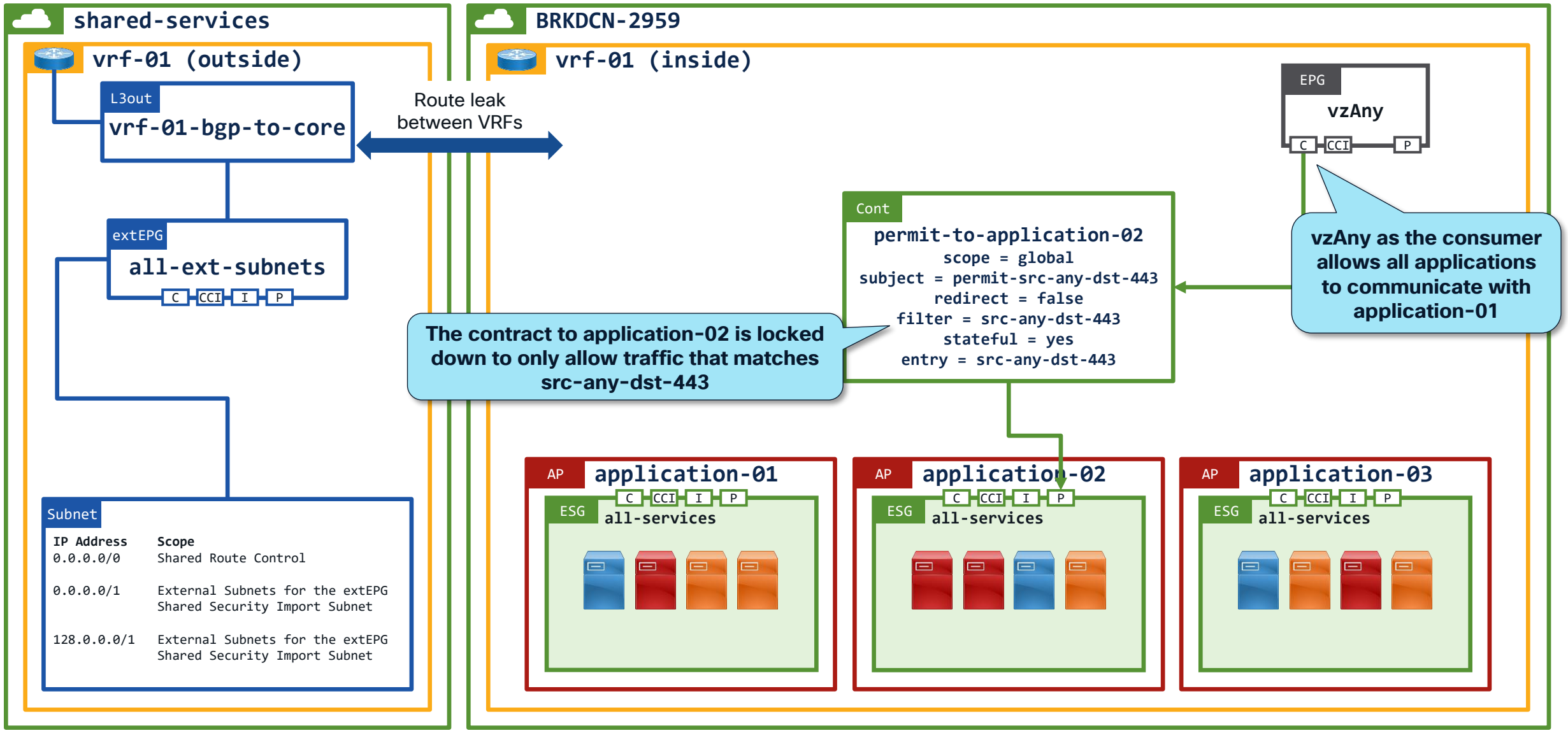
Scaling connectivity to application-01



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

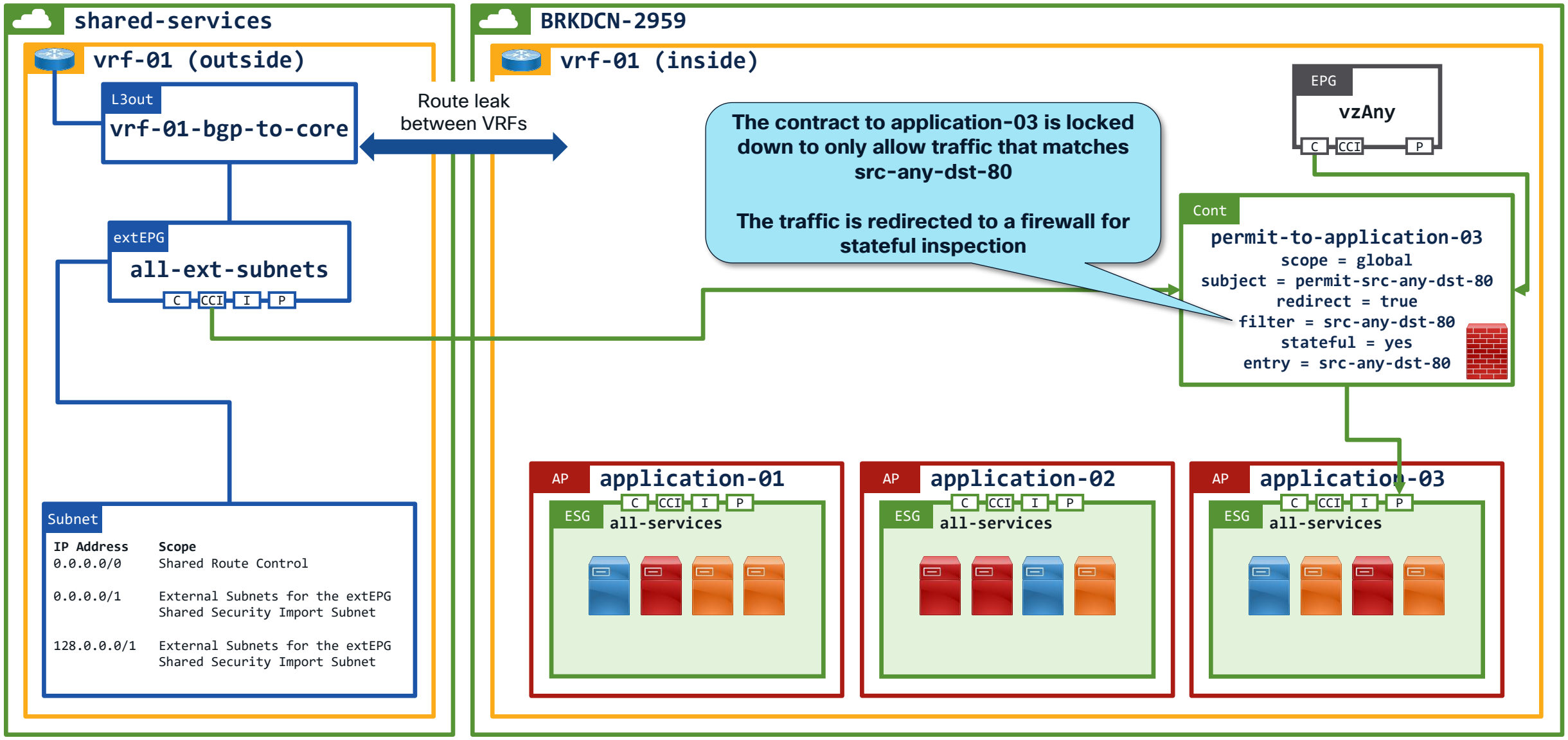
Scaling connectivity to application-02



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

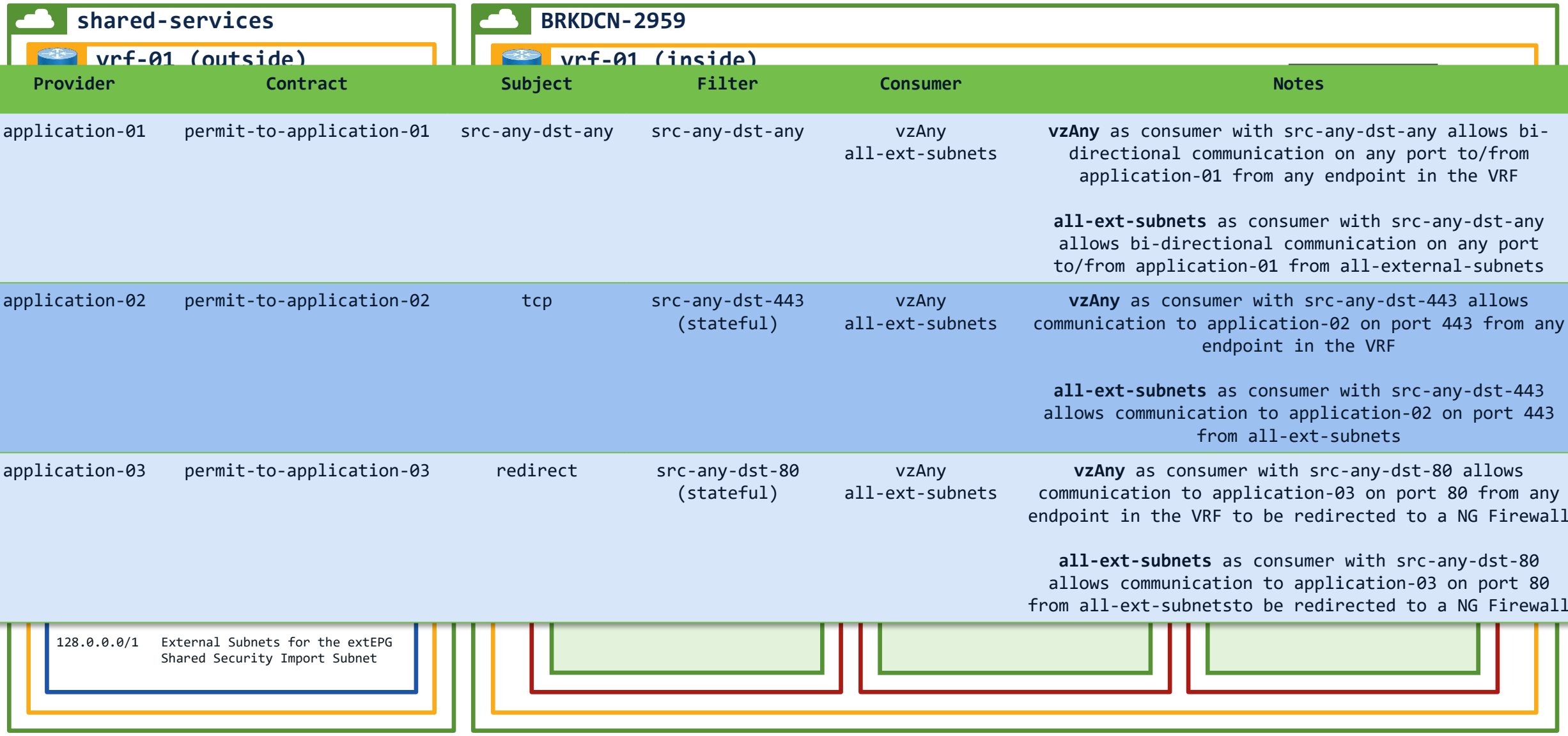
Scaling connectivity to application-03



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Scaling connectivity



Provider	Contract	Subject	Filter	Consumer	Notes
application-01	permit-to-application-01	src-any-dst-any	src-any-dst-any	vzAny all-ext-subnets	**vzAny** as consumer with src-any-dst-any allows bi-directional communication on any port to/from application-01 from any endpoint in the VRF **all-ext-subnets** as consumer with src-any-dst-any allows bi-directional communication on any port to/from application-01 from all-external-subnets
application-02	permit-to-application-02	tcp	src-any-dst-443 (stateful)	vzAny all-ext-subnets	**vzAny** as consumer with src-any-dst-443 allows communication to application-02 on port 443 from any endpoint in the VRF **all-ext-subnets** as consumer with src-any-dst-443 allows communication to application-02 on port 443 from all-ext-subnets
application-03	permit-to-application-03	redirect	src-any-dst-80 (stateful)	vzAny all-ext-subnets	**vzAny** as consumer with src-any-dst-80 allows communication to application-03 on port 80 from any endpoint in the VRF to be redirected to a NG Firewall **all-ext-subnets** as consumer with src-any-dst-80 allows communication to application-03 on port 80 from all-ext-subnetsto be redirected to a NG Firewall

© 2025 Cisco and/or its affiliates. All rights reserved.

Scaling considerations

https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/6x/verified-scalability/cisco-aci-verified-scalability-guide-613.html

- 1 preferred group per VRF
- vzAny supports 70 “provided” contracts per VRF
- vzAny supports 70 “consumed” contracts per VRF
- vzAny supports 16 “consumed contract interface” contracts (shared services) per VRF
- Determine whether restricted contracts, or L4-7 firewalls are the most applicable from a security perspective

© 2025 Cisco and/or its affiliates. All rights reserved.

Customer requirement

Layer 7 firewall inspection in place between systems requiring **explicit** trust

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Layer 7 security integration...

- Where networking and security come together...
- Customer's current network design...
- Security control over inbound traffic...
- Understanding ACI security...
- Zero trust application-based security...
- **Layer 7 security integration...**
- DMZ redesign...
- Reducing operational complexity of segmentation
- Implement Zero trust Micro-segmentation

Fastest introduction ever on Cisco Firepower Threat Defense (in 6 slides)

FTD converged image

For **reference** only

ASA

- L2-L4 Stateful Firewall
- Scalable CGNAT, ACL, routing
- Application inspection

FirePOWER

- Threat-centric NGIPS
- AVC, URL Filtering for NGFW
- Advanced Malware Protection

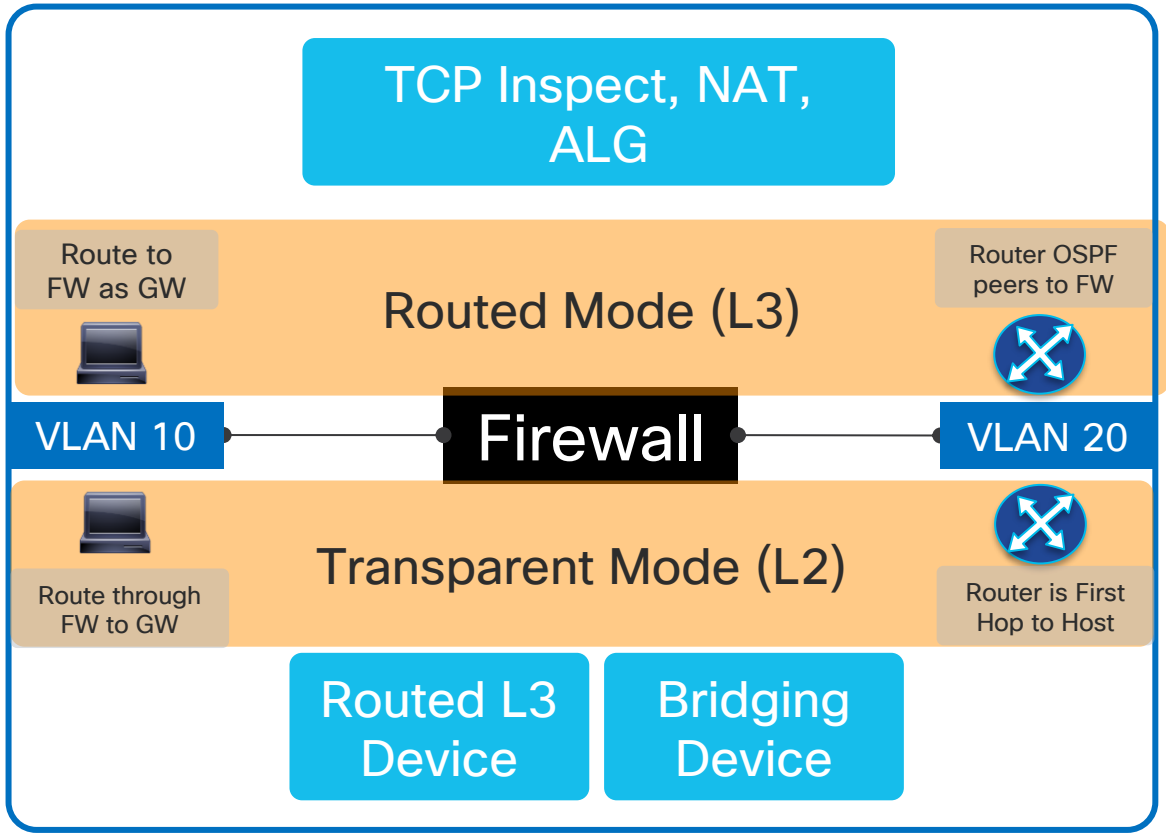
Firepower Threat Defense (FTD)

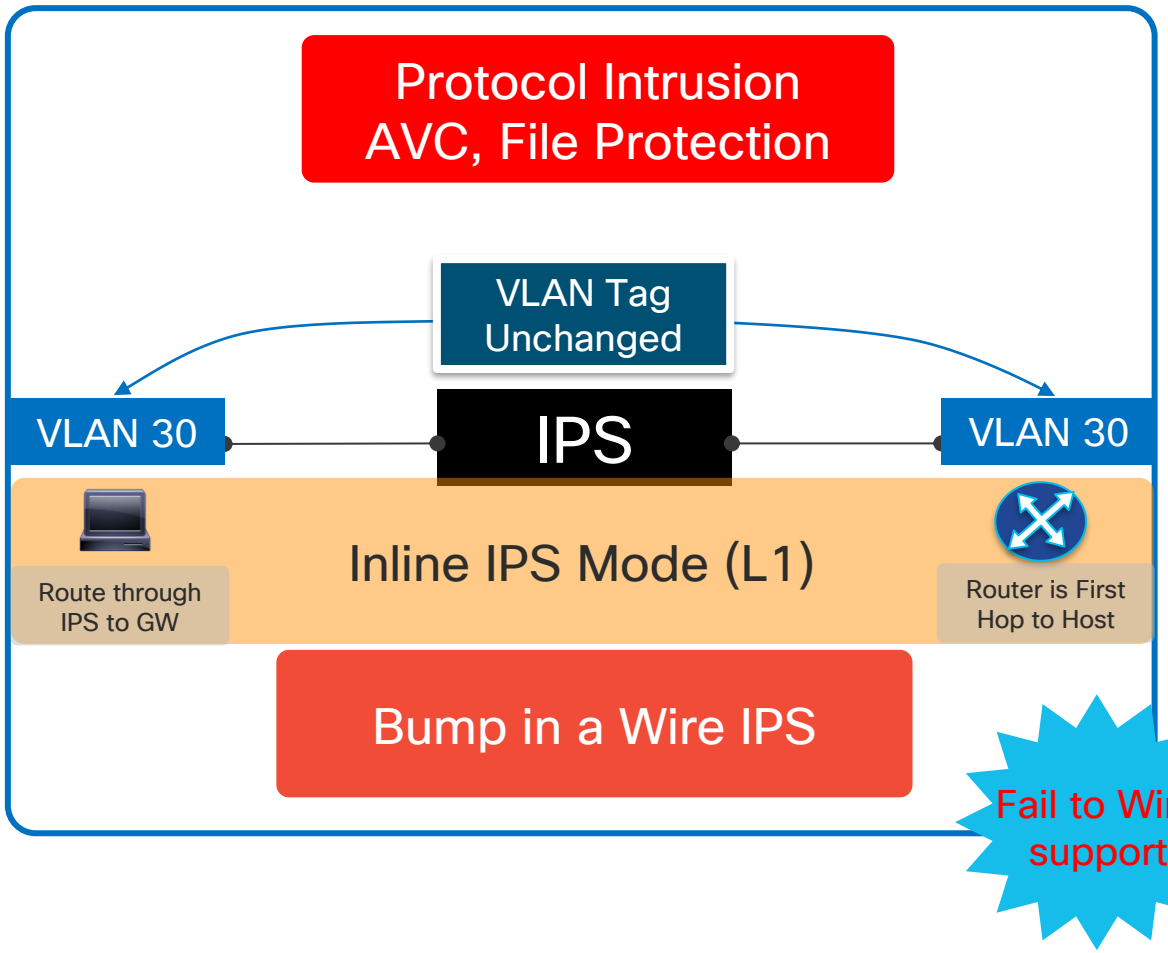
- Converged NGFW/NGIPS image on new Firepower and ASA5500-X platforms
- Single point of management with Firepower Management Center (FMC)
- Full FirePOWER functionality for NGFW/NGIPS deployments
- ASA Data Plane with TCP Normalizer, NAT, ACL, dynamic routing, failover, clustering

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Secure Firewall Modes of Operation

For **reference** only

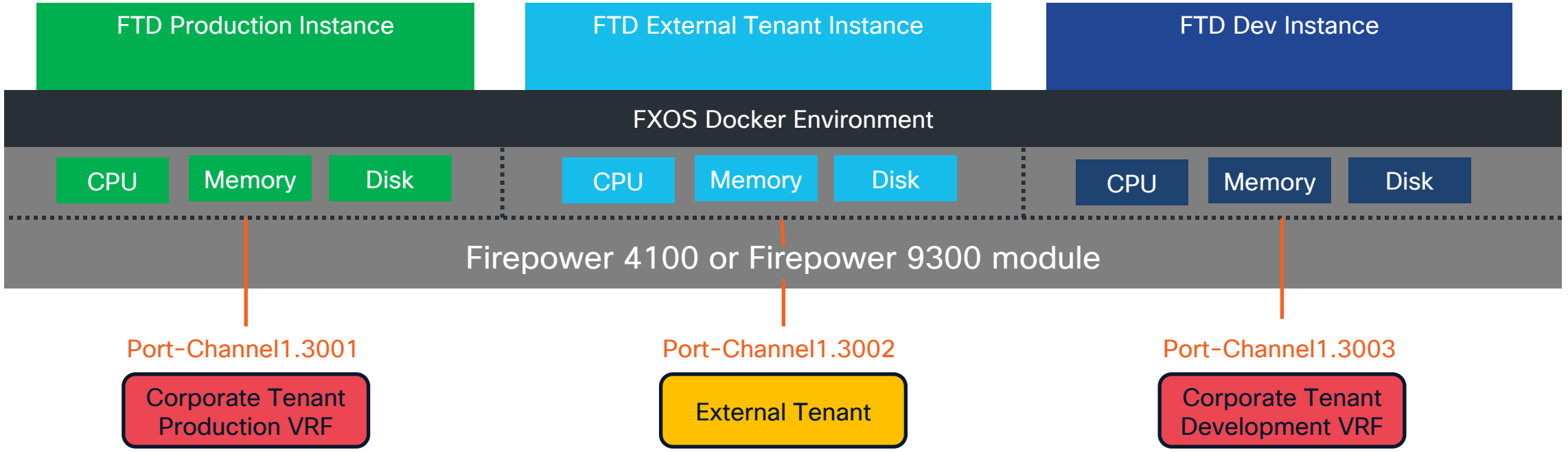




© 2025 Cisco and/or its affiliates. All rights reserved.

FTD Multi-Instance DC use case

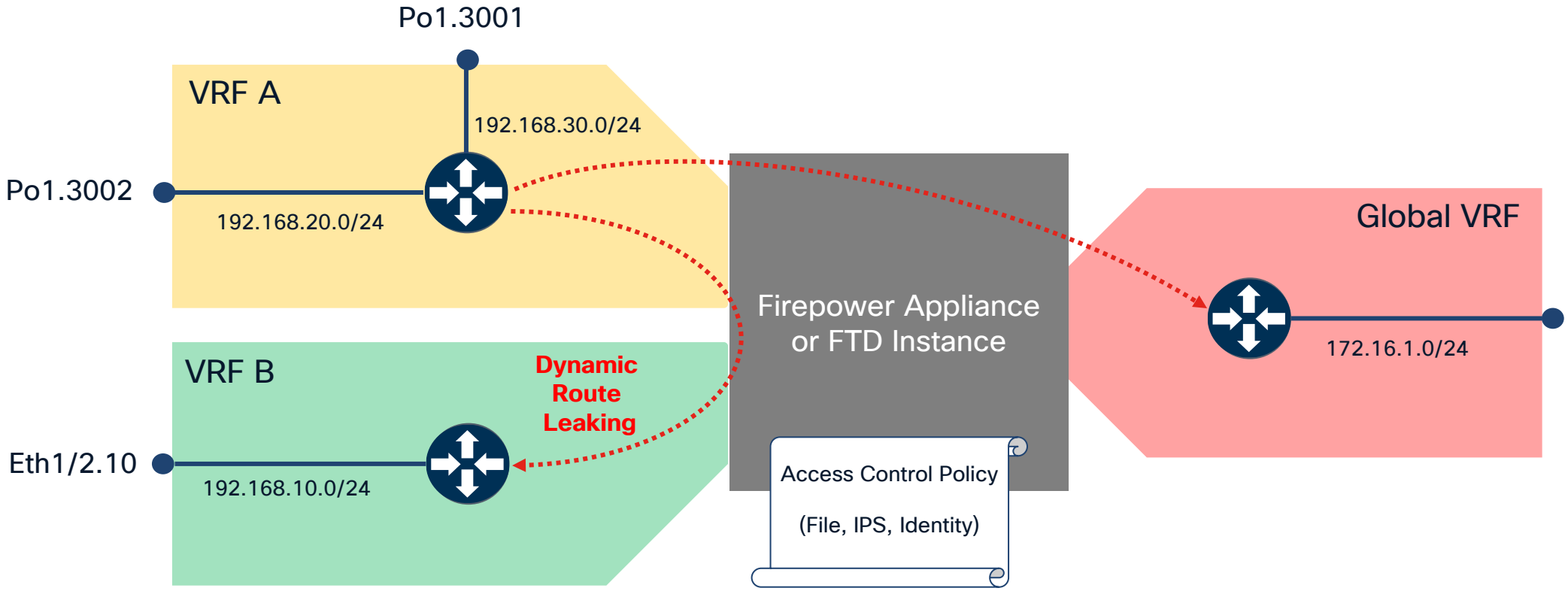
- Create multiple logical FTD devices on a single module or appliance, and use as separate devices in the ACI fabric
- Complete traffic processing and management separation while protecting DC apps
- Supported on Firepower 4100 and 9300 only
- Dev firewall can overload/go offline/upgrade with out any effect on Production or External instances



© 2025 Cisco and/or its affiliates. All rights reserved.

Virtual Routing and Forwarding (VRF) Lite

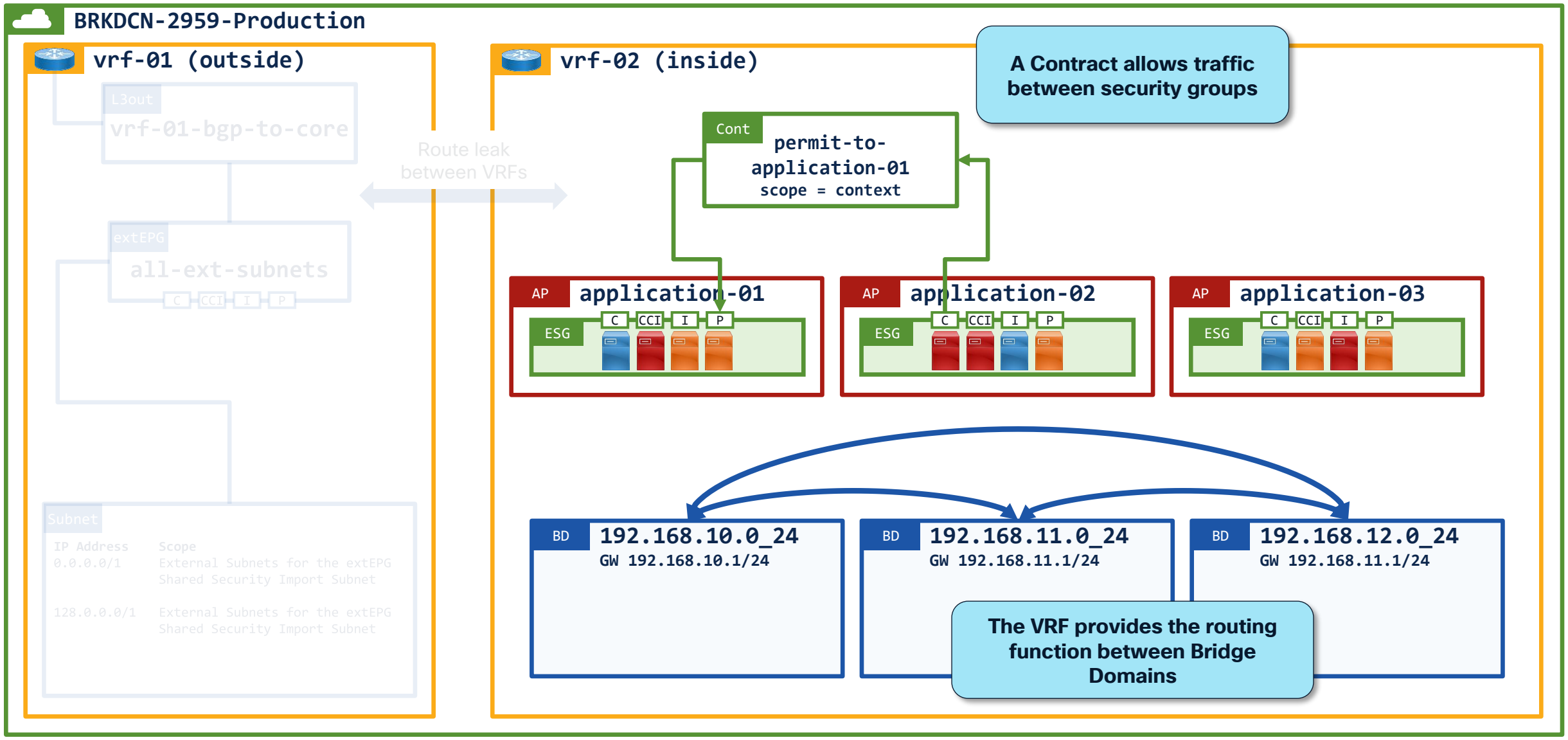
- In FTD 6.6, interfaces can be in different Routing Domains
  (Overlapping IP address support between User and **Global VRF)**
- Allows for easy separation of Service Graphs within the same FTD



© 2025 Cisco and/or its affiliates. All rights reserved.

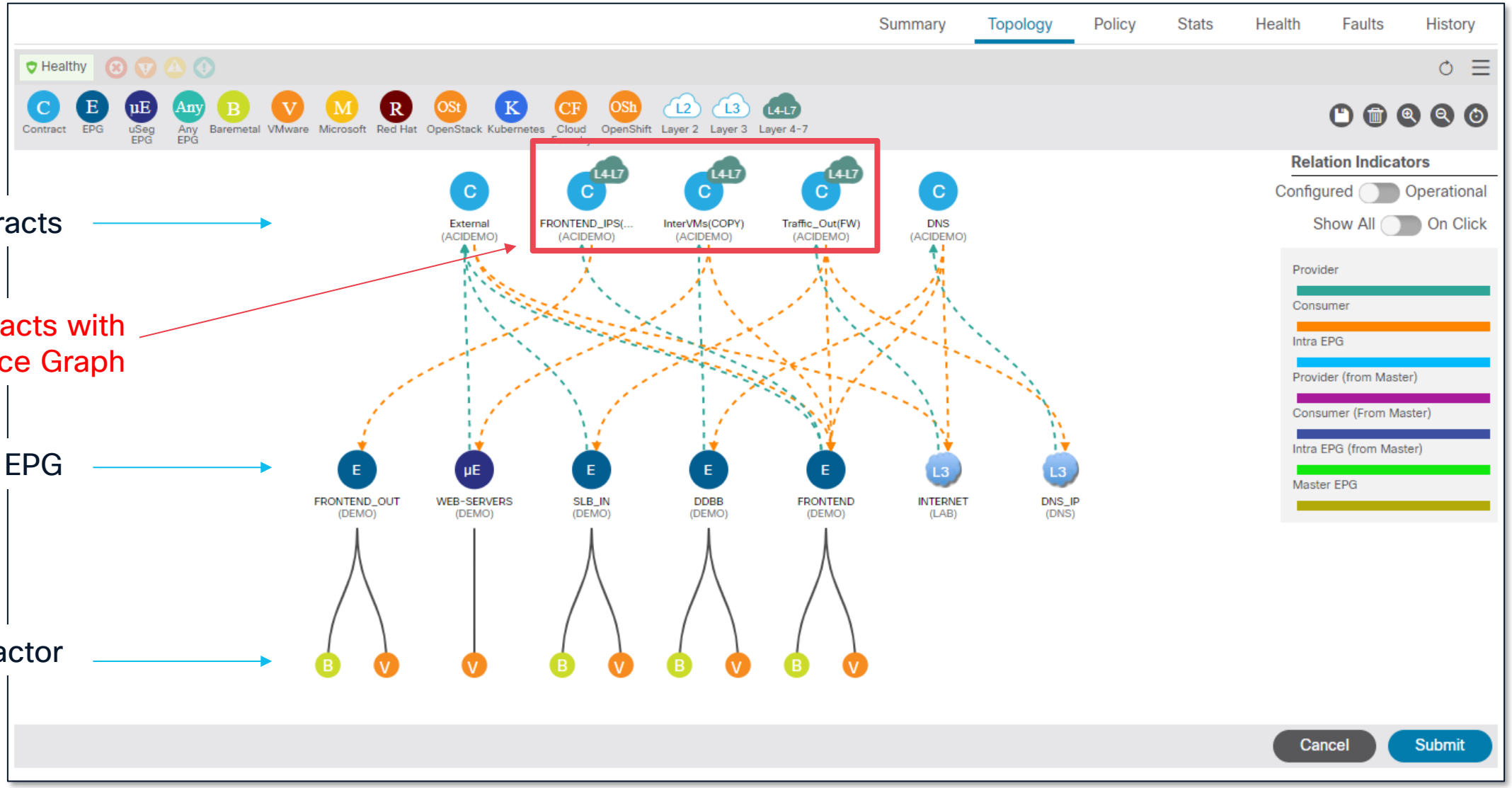
Firewall insertion...

Two requirements for communication: Routing and Contracts



© 2025 Cisco and/or its affiliates. All rights reserved.

Application policy with contract



Contracts

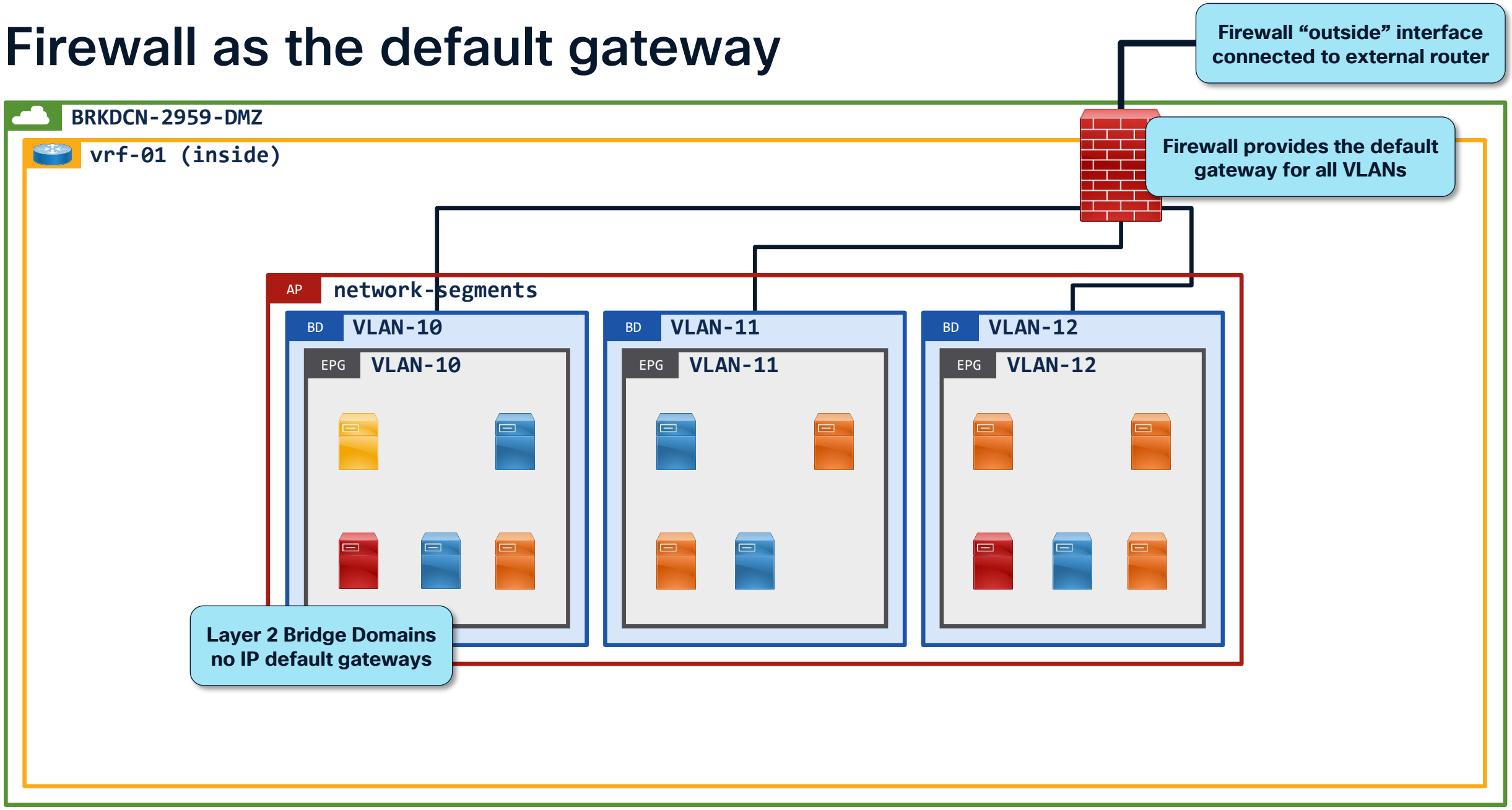
Contracts with Service Graph

EPG

Form Factor

© 2025 Cisco and/or its affiliates. All rights reserved.

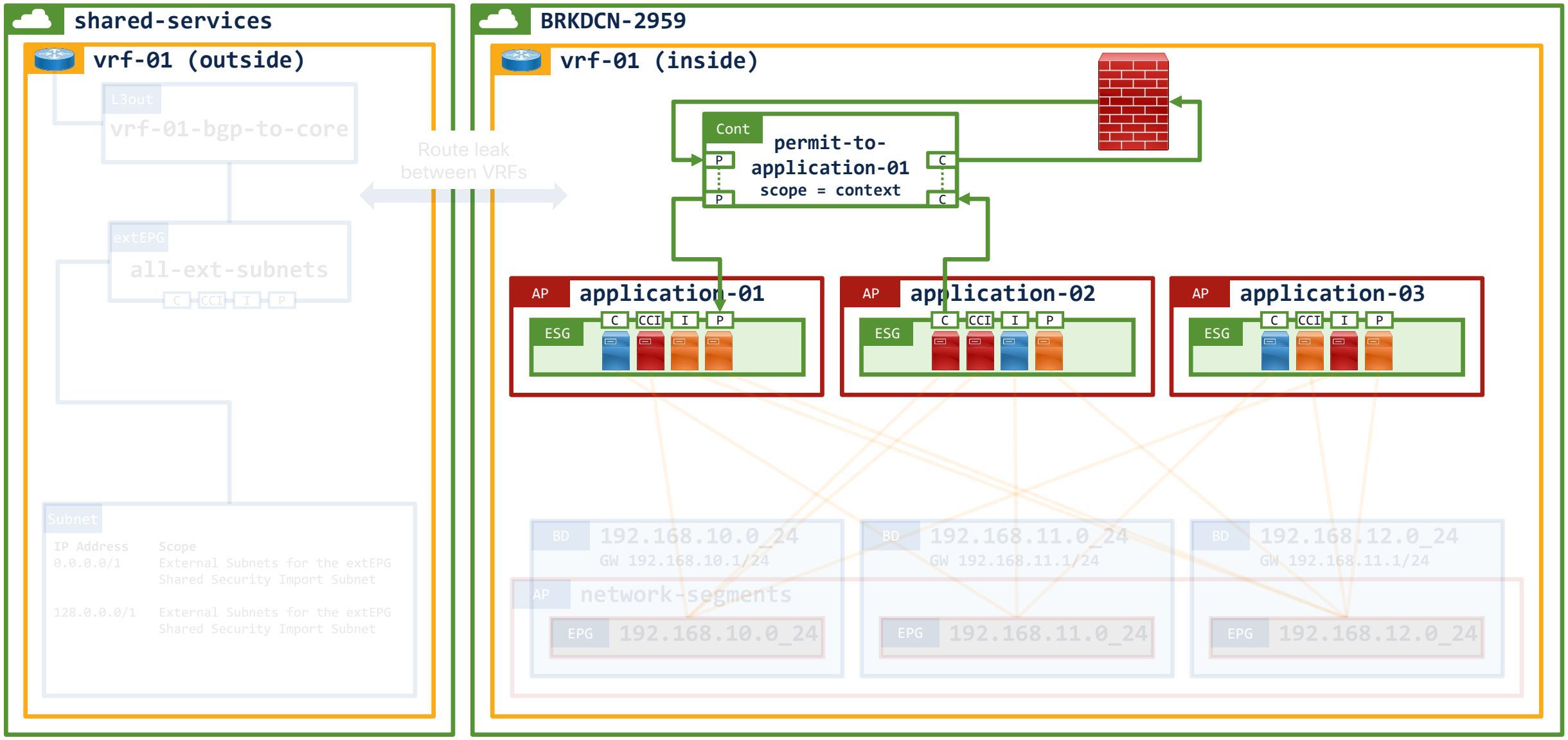
Firewall as the default gateway



© 2025 Cisco and/or its affiliates. All rights reserved.

https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959-DMZ/data/07-dmz-current-design-firewall-provides-default-gateway.nac.yaml

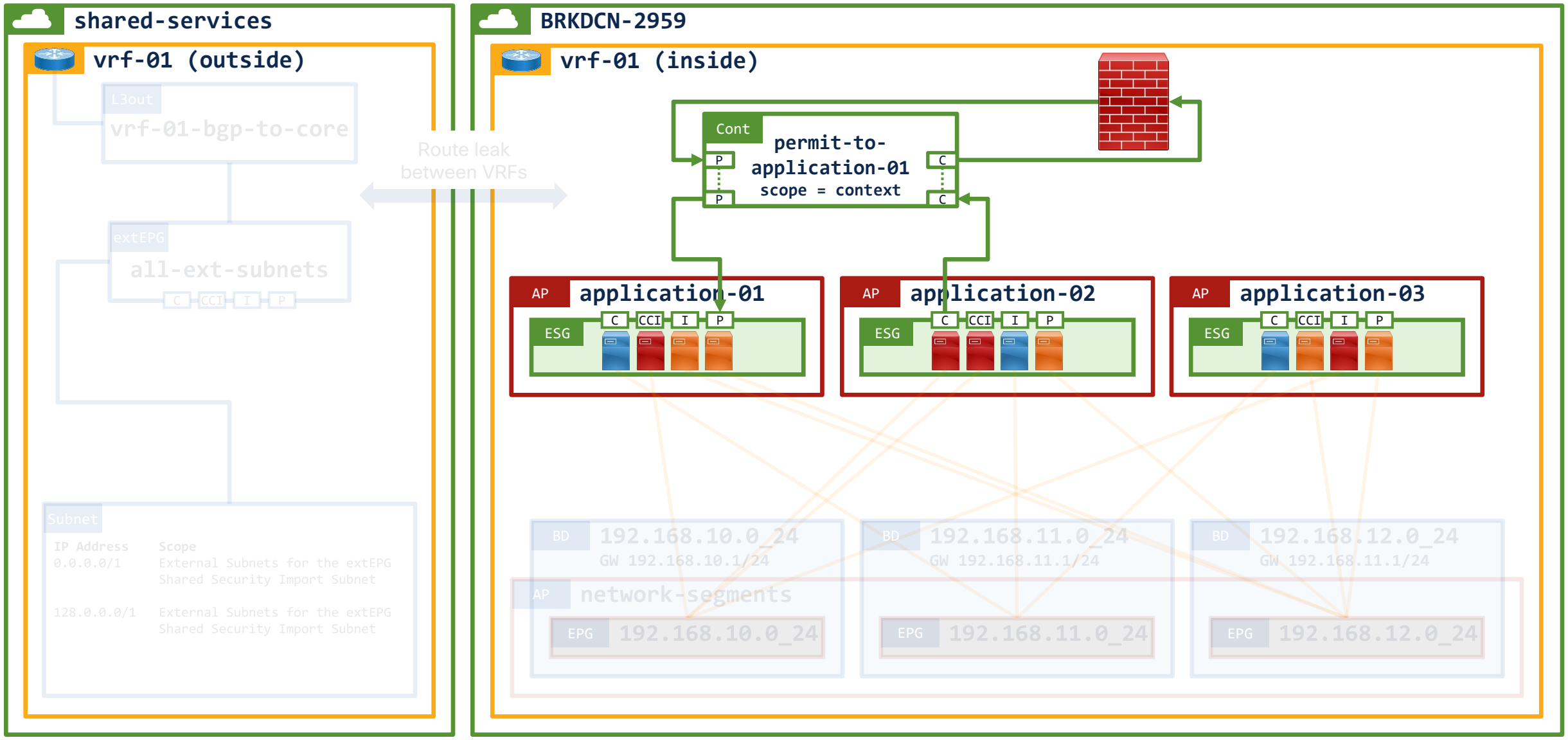
Policy Based Redirect is your Best Friend



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Policy Based Redirect is your Best Friend

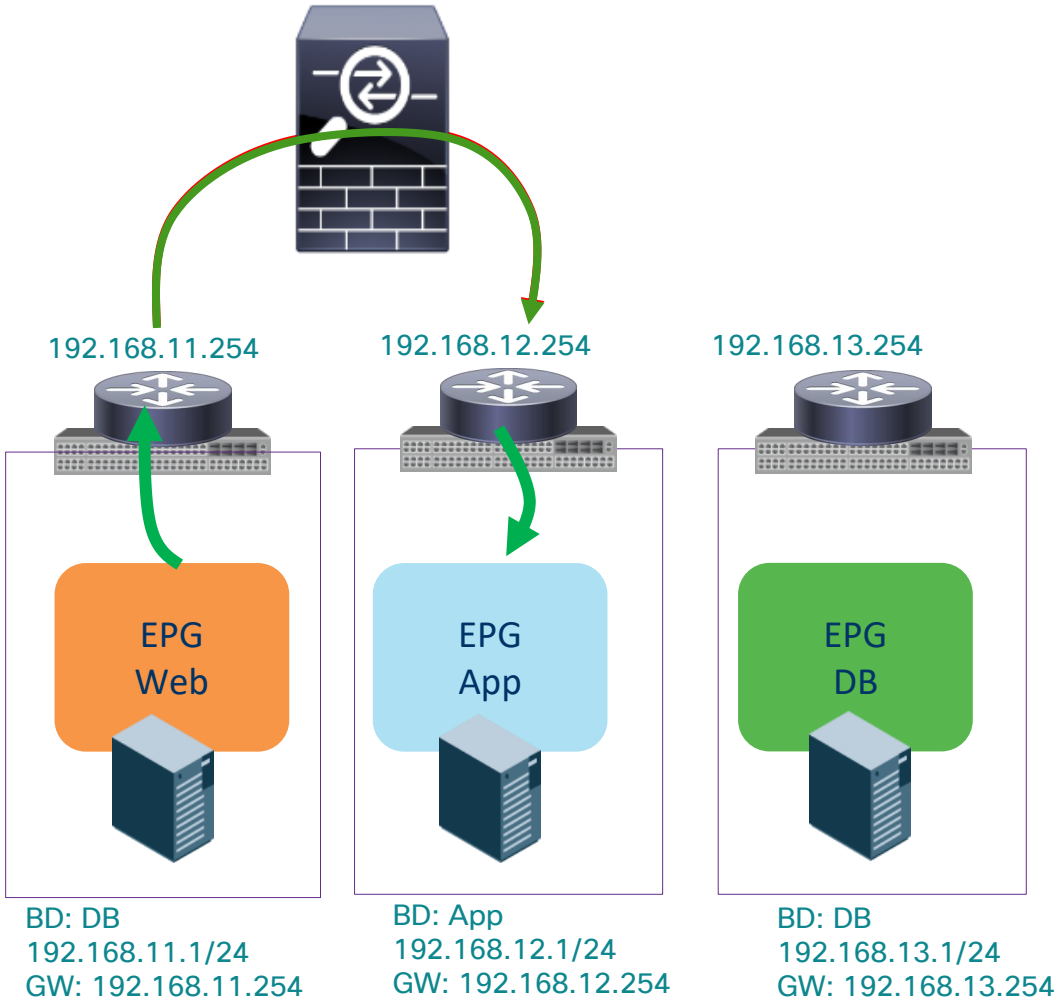


© 2025 Cisco and/or its affiliates. All rights reserved.

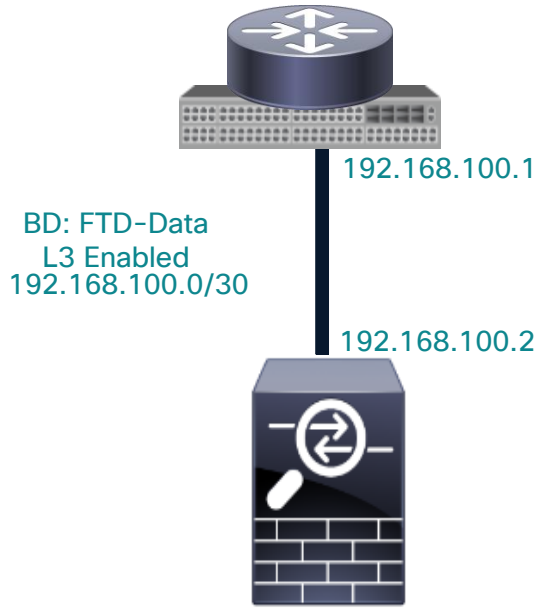
cisco

Policy Based Redirect is your Best Friend

With PBR Service Graph



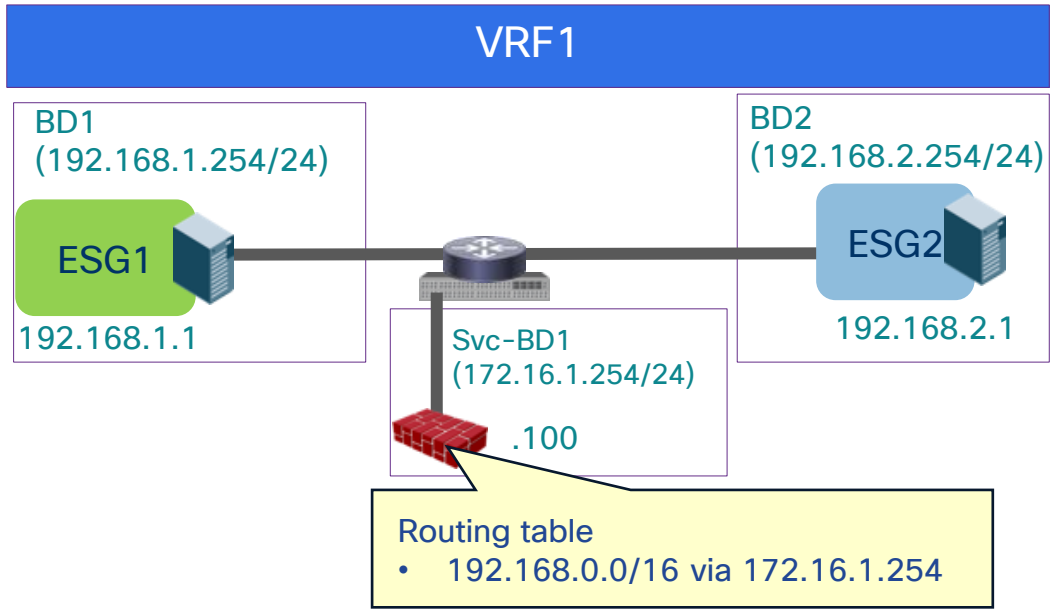
PBR redirects the traffic matching the contract to the **Security Service**



© 2025 Cisco and/or its affiliates. All rights reserved.

One-arm vs. Two-arm?

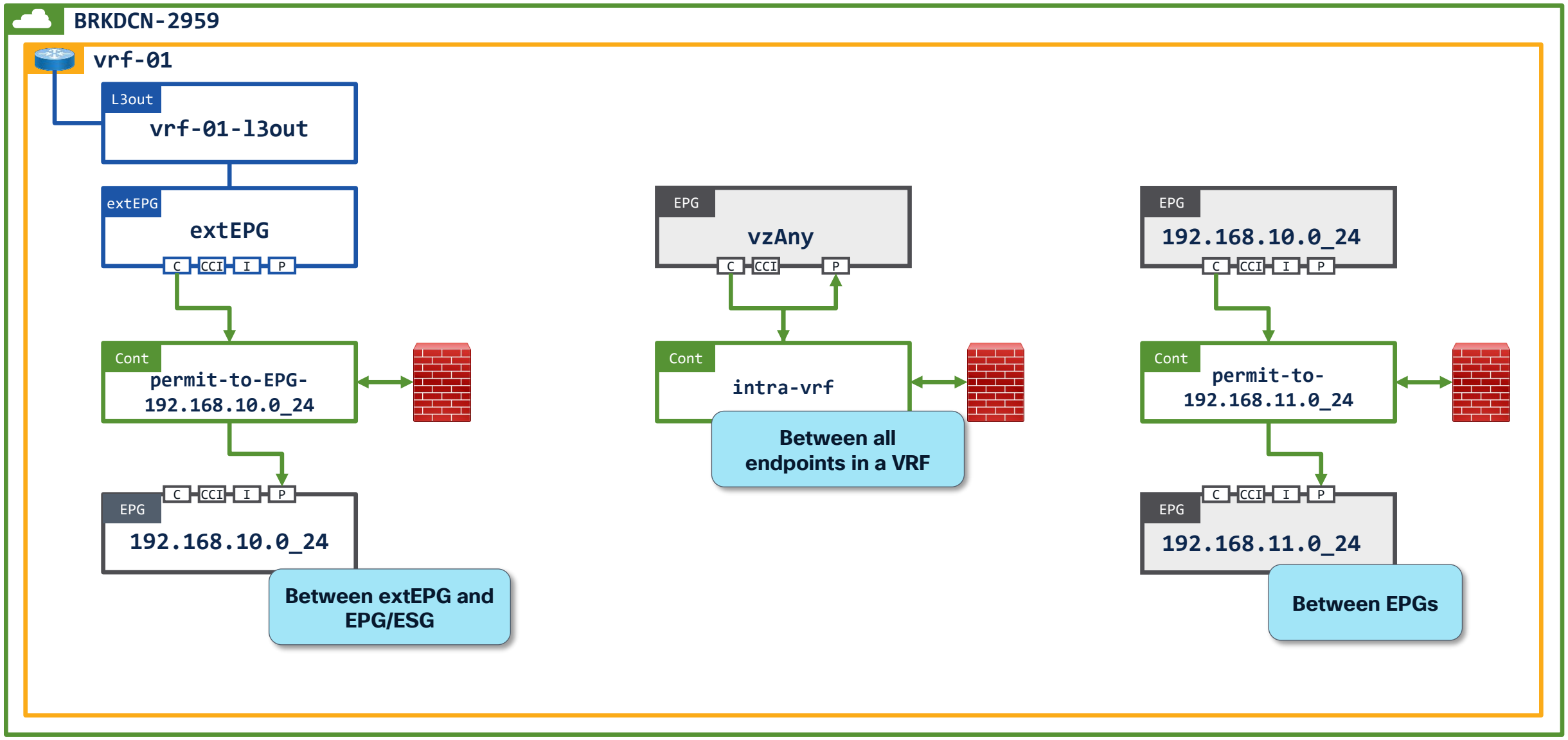
- One-arm
  - Simple routing design on service node.
  - One-arm must be used for intra-subnet or intra-EPG/ESG contract.
  - Some firewall doesn't allow intra-interface traffic by default.



- Two-arm
  - Need to manage routing design on service node.
  - Different security level on each interface.
  - If in transparent mode (PBR L2)

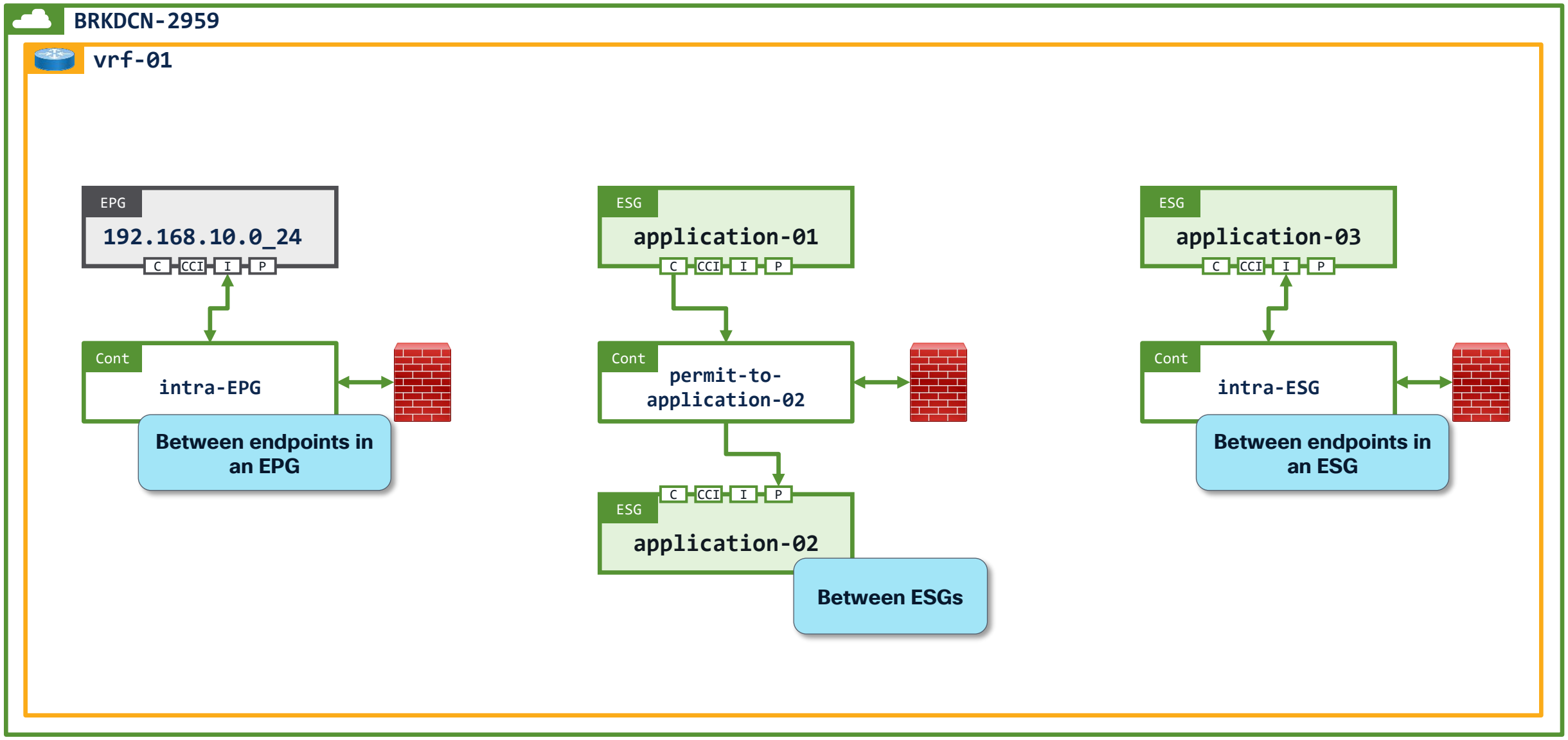
© 2025 Cisco and/or its affiliates. All rights reserved.

Where can we use PBR...?



© 2025 Cisco and/or its affiliates. All rights reserved.

Where can we use PBR...?

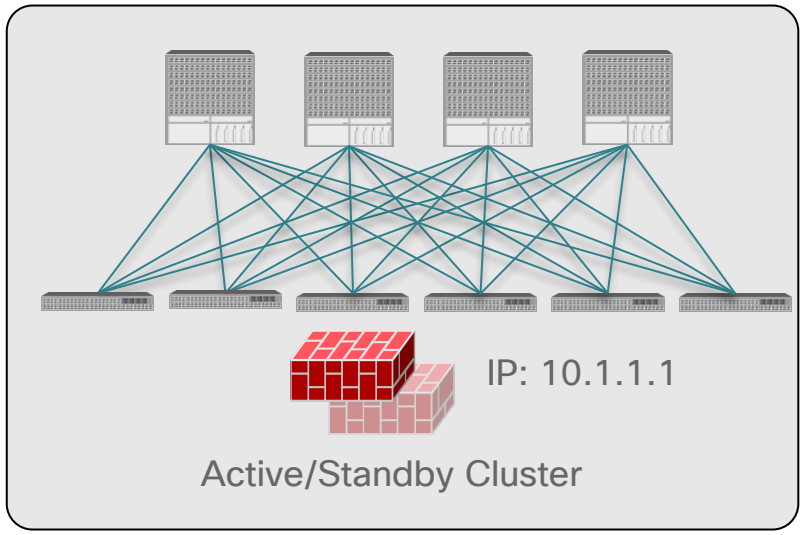


© 2025 Cisco and/or its affiliates. All rights reserved.

What are the Stateful HA options ?

One PBR destination IP
One Logical device with two concrete devices

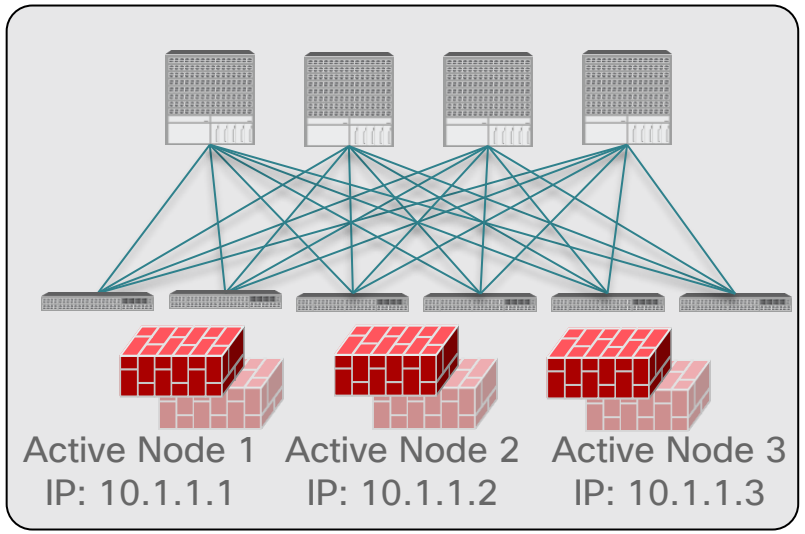
Single A/S Failover Node



- PBR is not mandatory
- The Active/Standby pair represents a single MAC/IP entry.

Multiple PBR destination IPs (Symmetric PBR)
One Logical device with multiple concrete devices

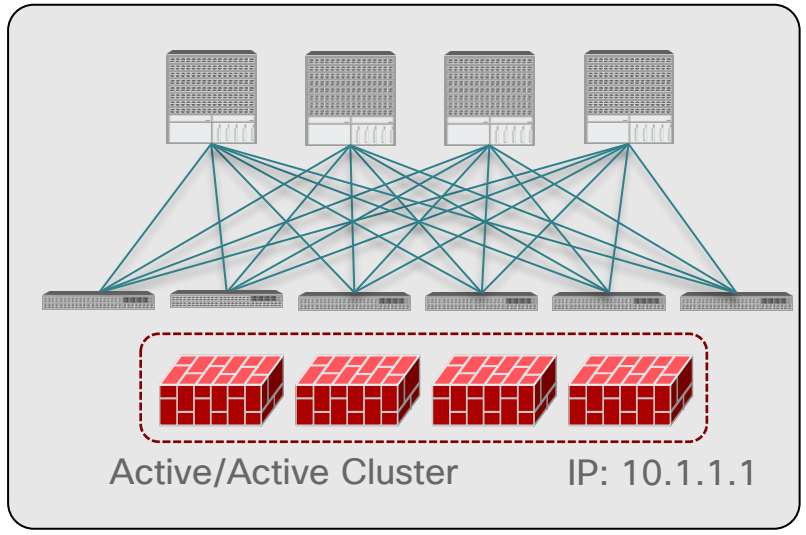
Several A/S Nodes



- PBR is required.
- Each Active node represent a unique MAC/IP entry.
- Use of Symmetric PBR to ensure each flow is handled by the same Active node in both directions

One PBR destination IP
One Logical device with one concrete device

Active/Active Cluster



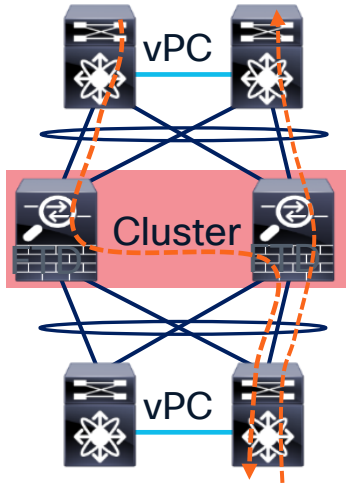
- PBR is required if the cluster is stretched across pods.
- The Active/Active cluster represents a single MAC/IP entry.
- Spanned Ether-Channel Mode supported with Cisco ASA/FTD platforms

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Firewall Clustering...

ASA and FTD clustering

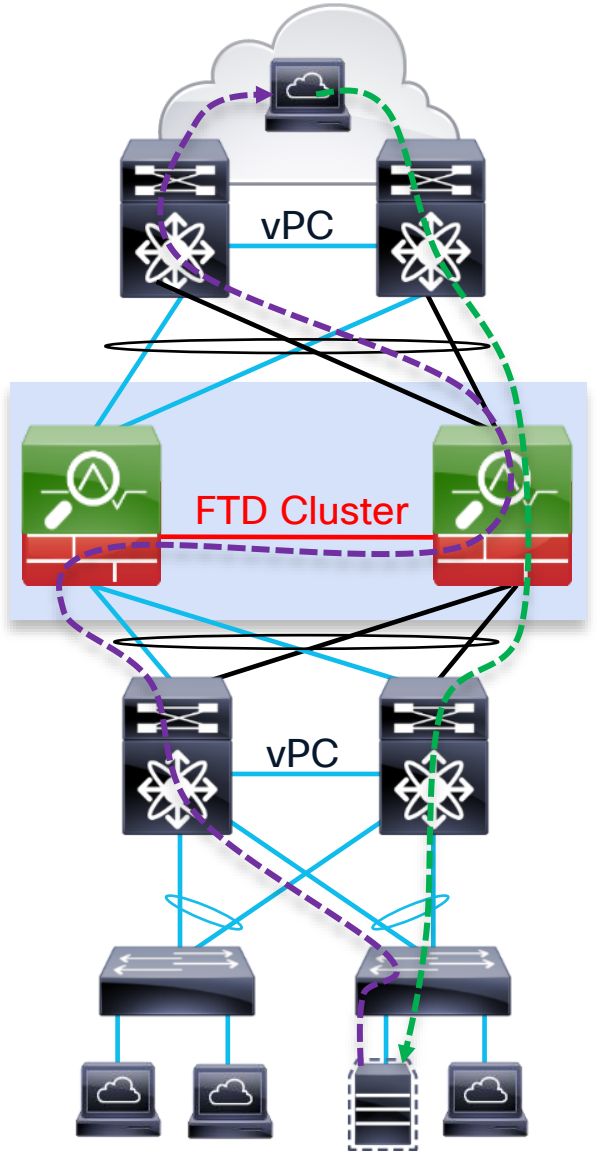
- **Up to 16** appliances or modules combine in one traffic processing system
- Preserve the benefits of failover
  - All members are managed as a single entity
  - Virtual IP and MAC addresses for first-hop redundancy
  - Connection states are preserved after a single member failure
- Implement true **scalability** in addition to high availability
  - Fully distributed data plane for new and existing connections
  - Elastic scaling of throughput and maximum concurrent connections
  - Stateless external load-balancing through standard Etherchannel or routing
  - Out-of-band Cluster Control Link for **asymmetry normalization**
  - No member-to-member communication on data interfaces



© 2025 Cisco and/or its affiliates. All rights reserved.

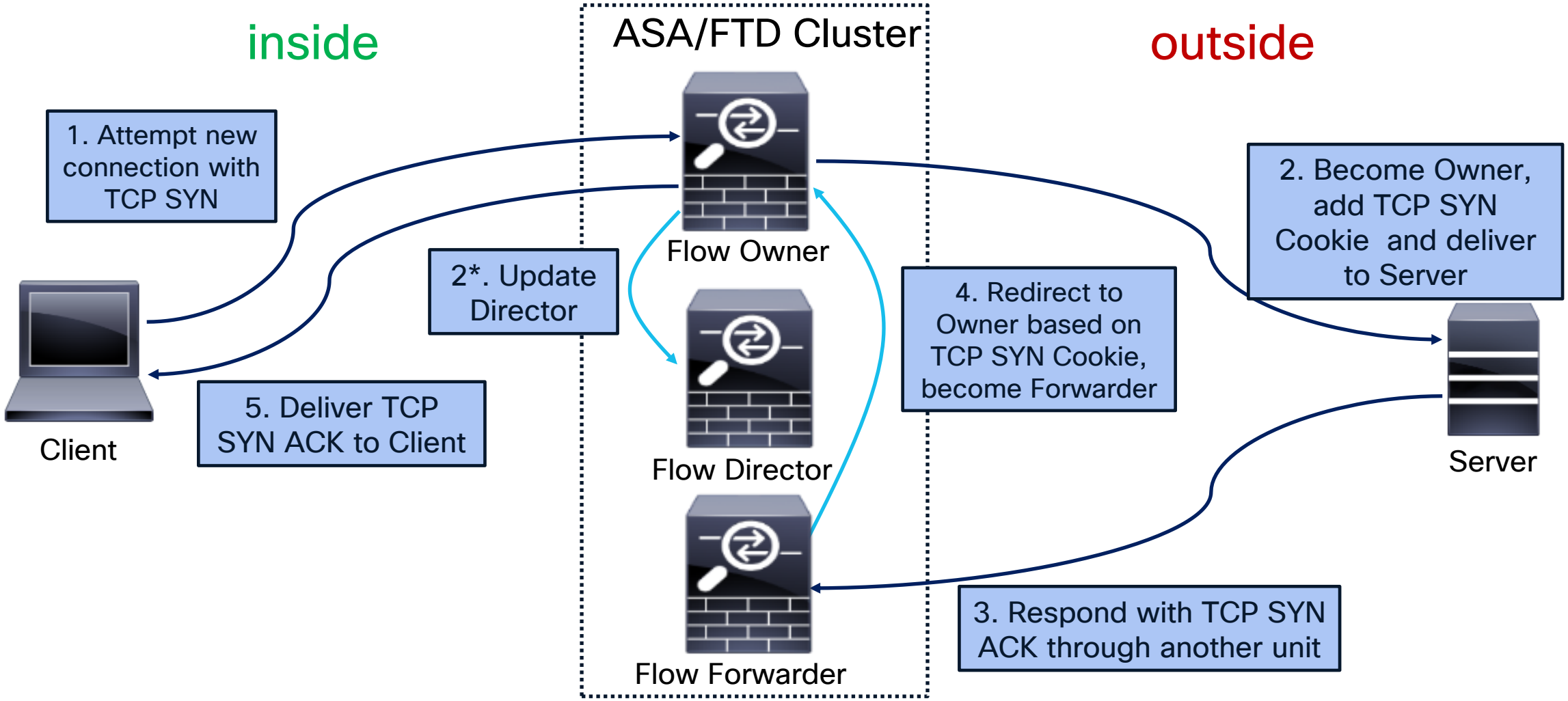
Clustering concepts – Physical and virtual

- Cluster roles
  - Control Node – synchronizes cluster configuration
  - Data Node – Cluster member other than the Control Node
- Flow roles
  - Flow Director (deterministic) – keeps track of owner
  - Flow Owner (nondeterministic) – receiver of first packet of flow
  - Flow Forwarder – forward the traffic to owner in case of asym traffic
- Cluster Control Link (CCL)
  - Internode communication
  - Asymmetric traffic redirection to flow owner
- State sharing
  - Cluster nodes share connection state
  - Cluster nodes do not share IPS state



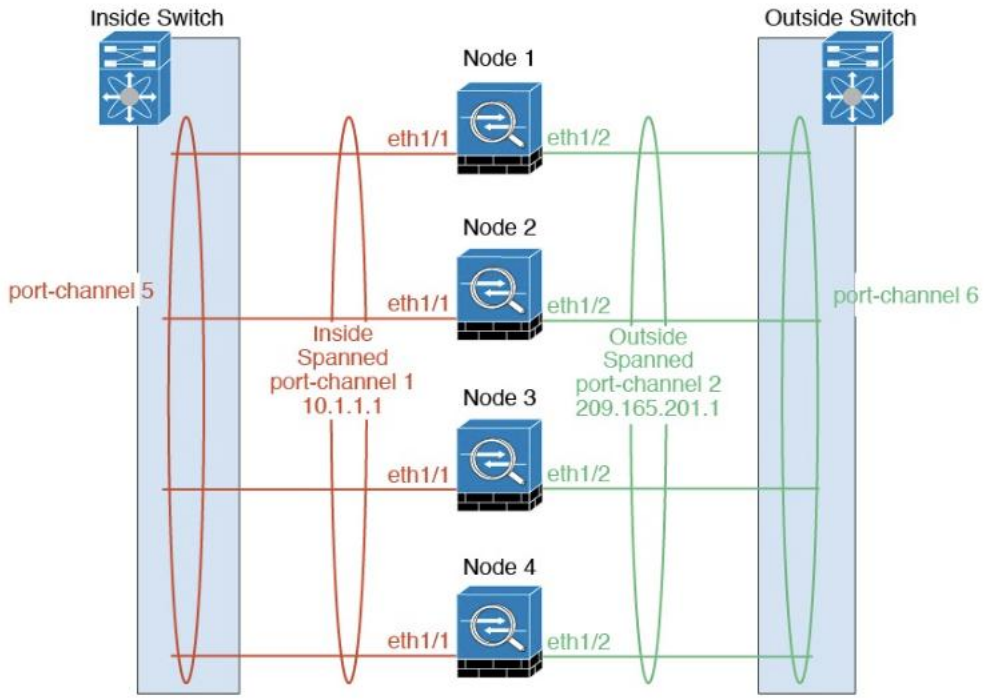
© 2025 Cisco and/or its affiliates. All rights reserved.

New TCP connection



© 2025 Cisco and/or its affiliates. All rights reserved.

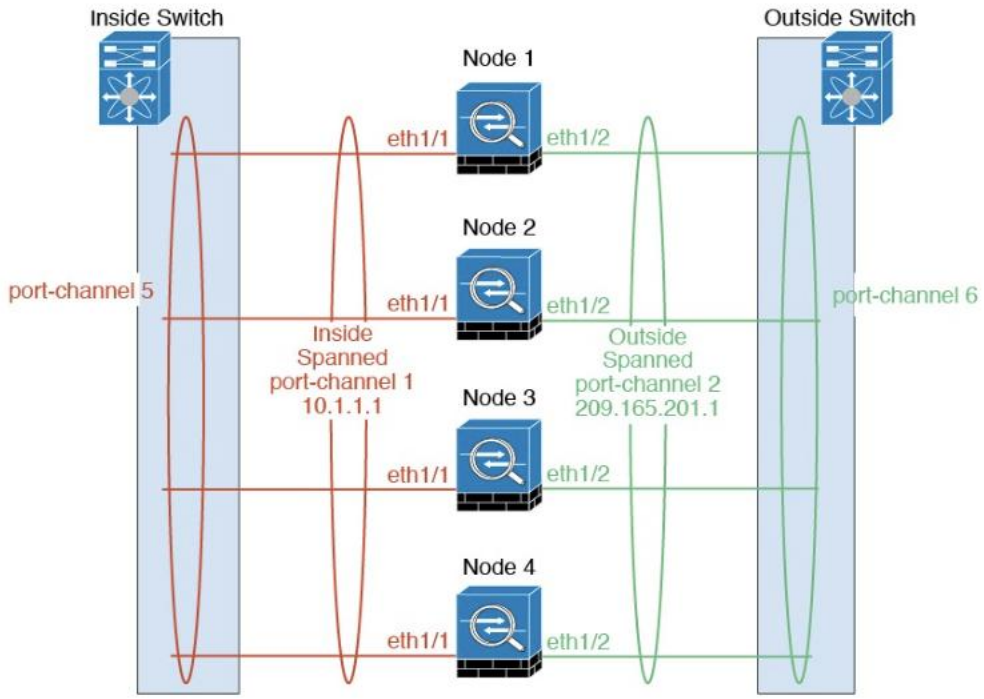
Two interface modes possible

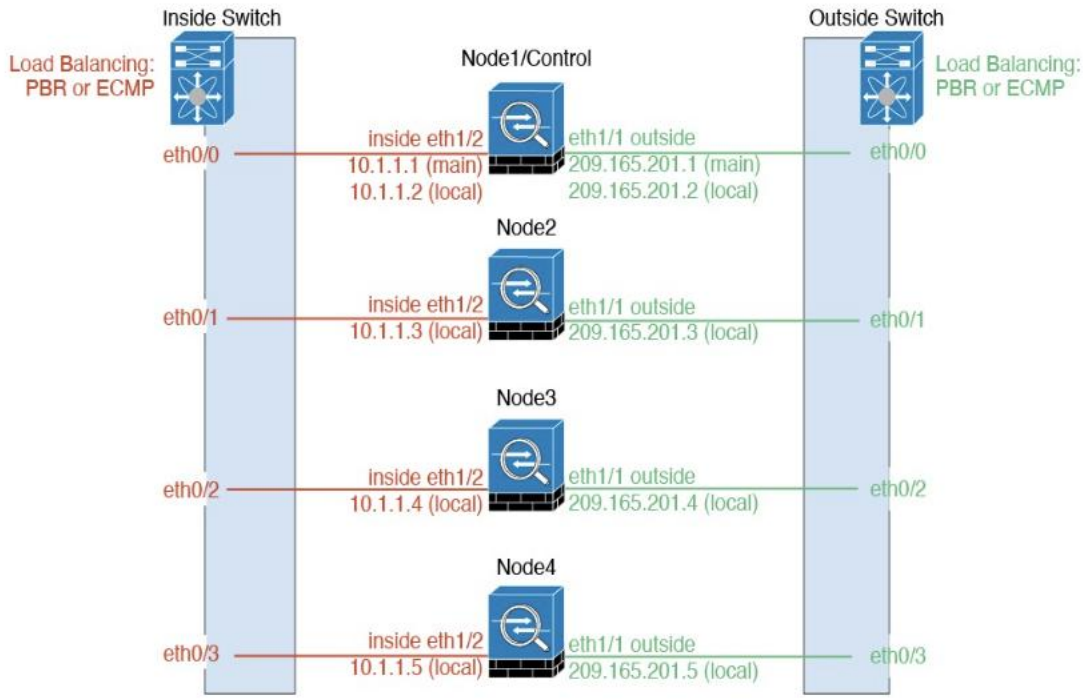


Spanned Mode

© 2025 Cisco and/or its affiliates. All rights reserved.

Two interface modes possible





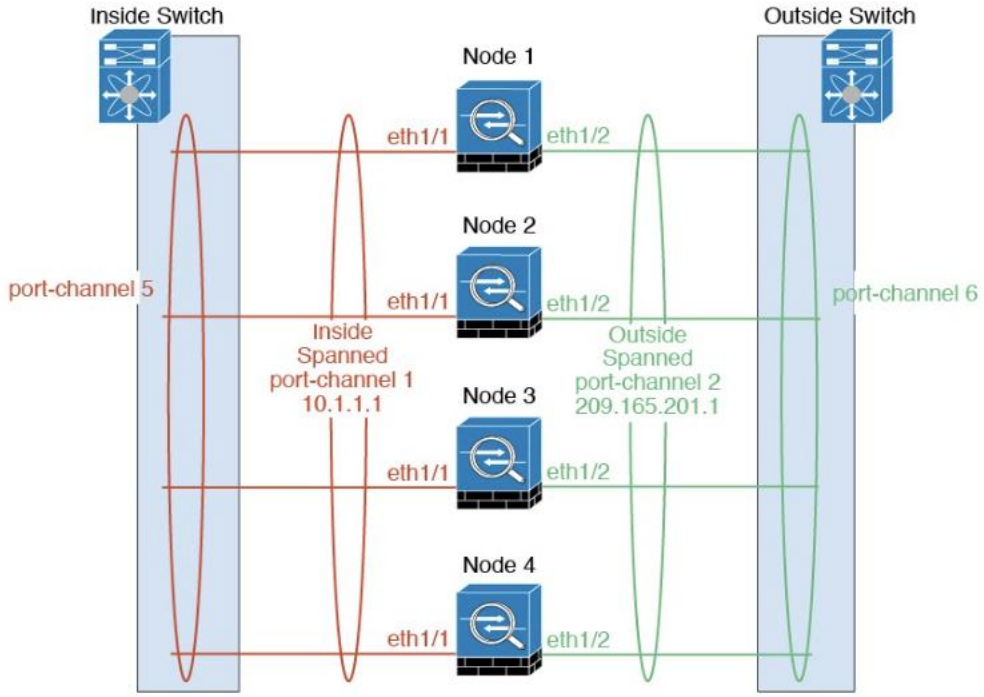
Spanned Mode

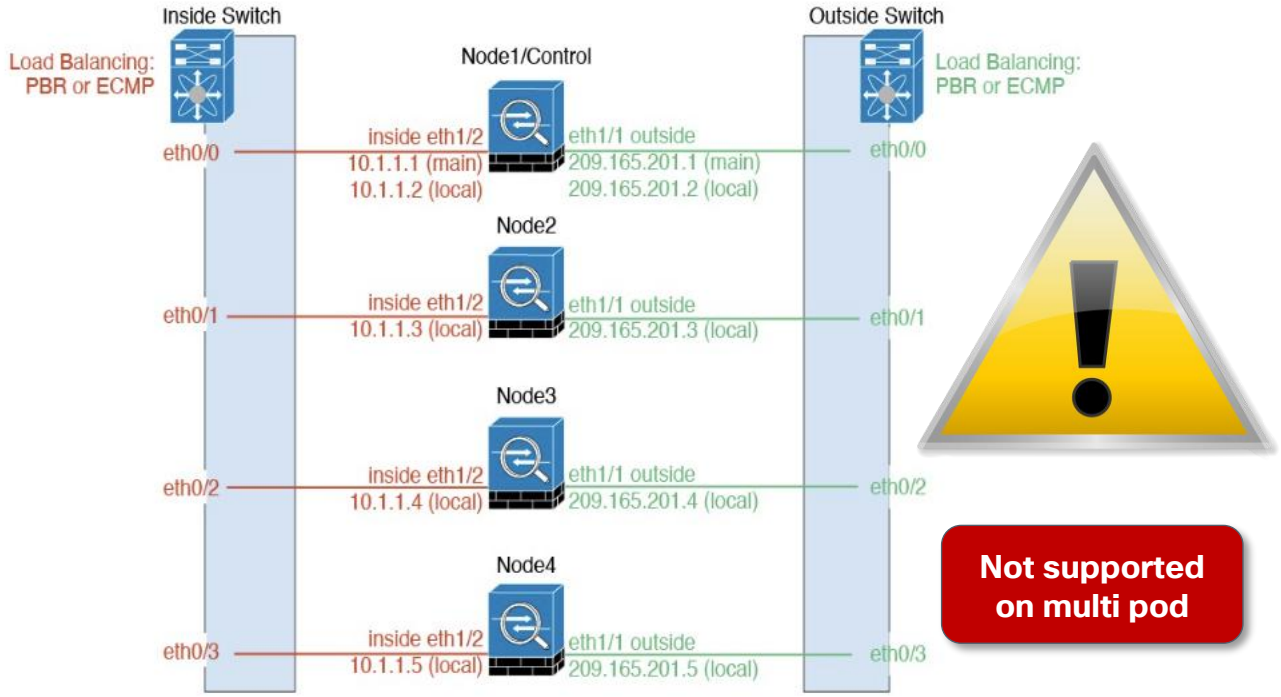
Individual Mode

	Individual Mode	Spanned Mode
FTDv	Default	Not Supported
4100/9300 Series	Not Supported	Default
3100/4200	*New in 7.6*	Default

© 2025 Cisco and/or its affiliates. All rights reserved.

Two interface modes possible





Not supported on multi pod

Spanned Mode

Individual Mode

	Individual Mode	Spanned Mode
FTDv	Default	Not Supported
4100/9300 Series	Not Supported	Default
3100/4200	*New in 7.6*	Default

© 2025 Cisco and/or its affiliates. All rights reserved.

Create an FTD cluster in FMC

For **reference** only

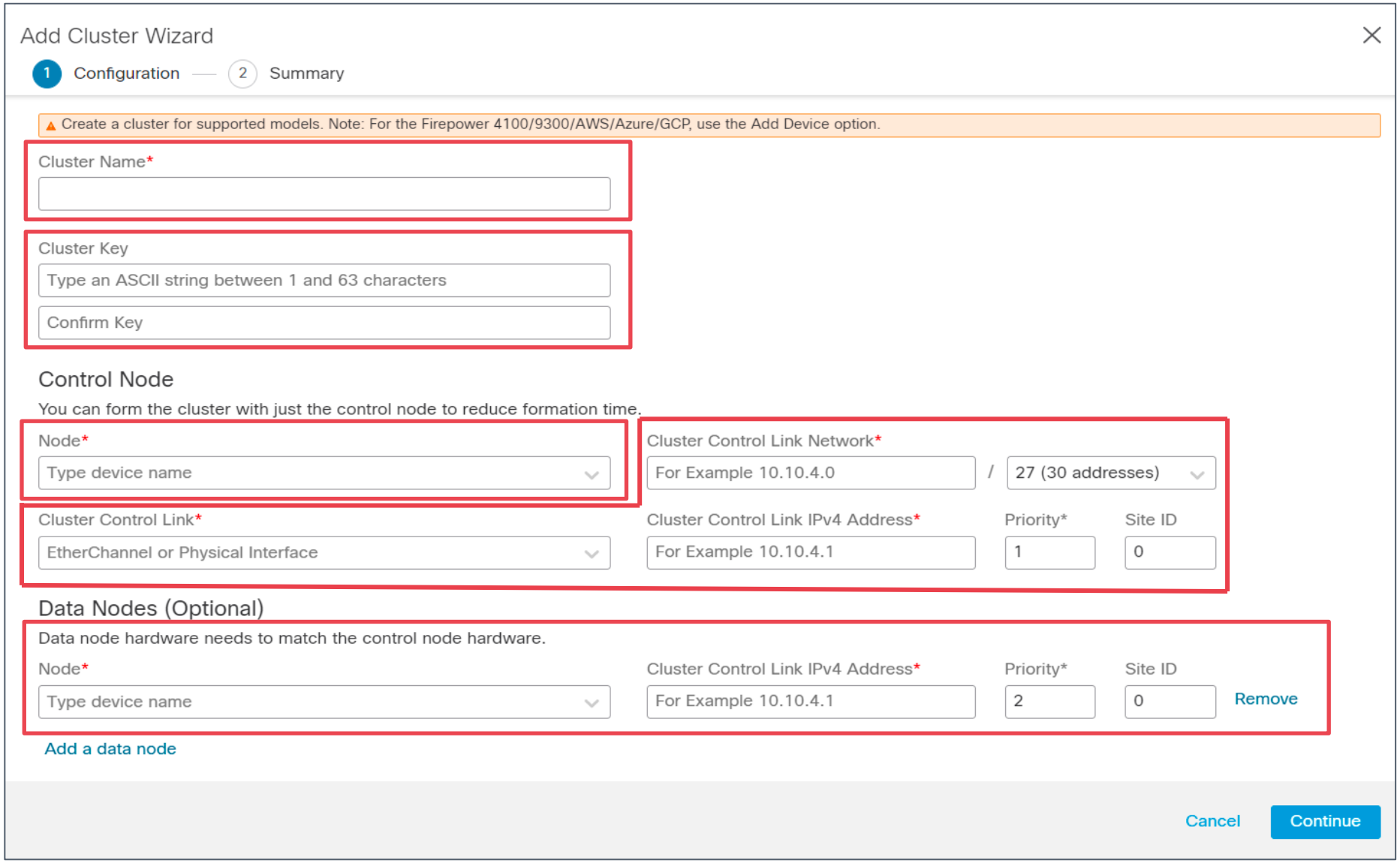
Name

Secret Key

First Cluster Node

CCL Information

Add cluster members



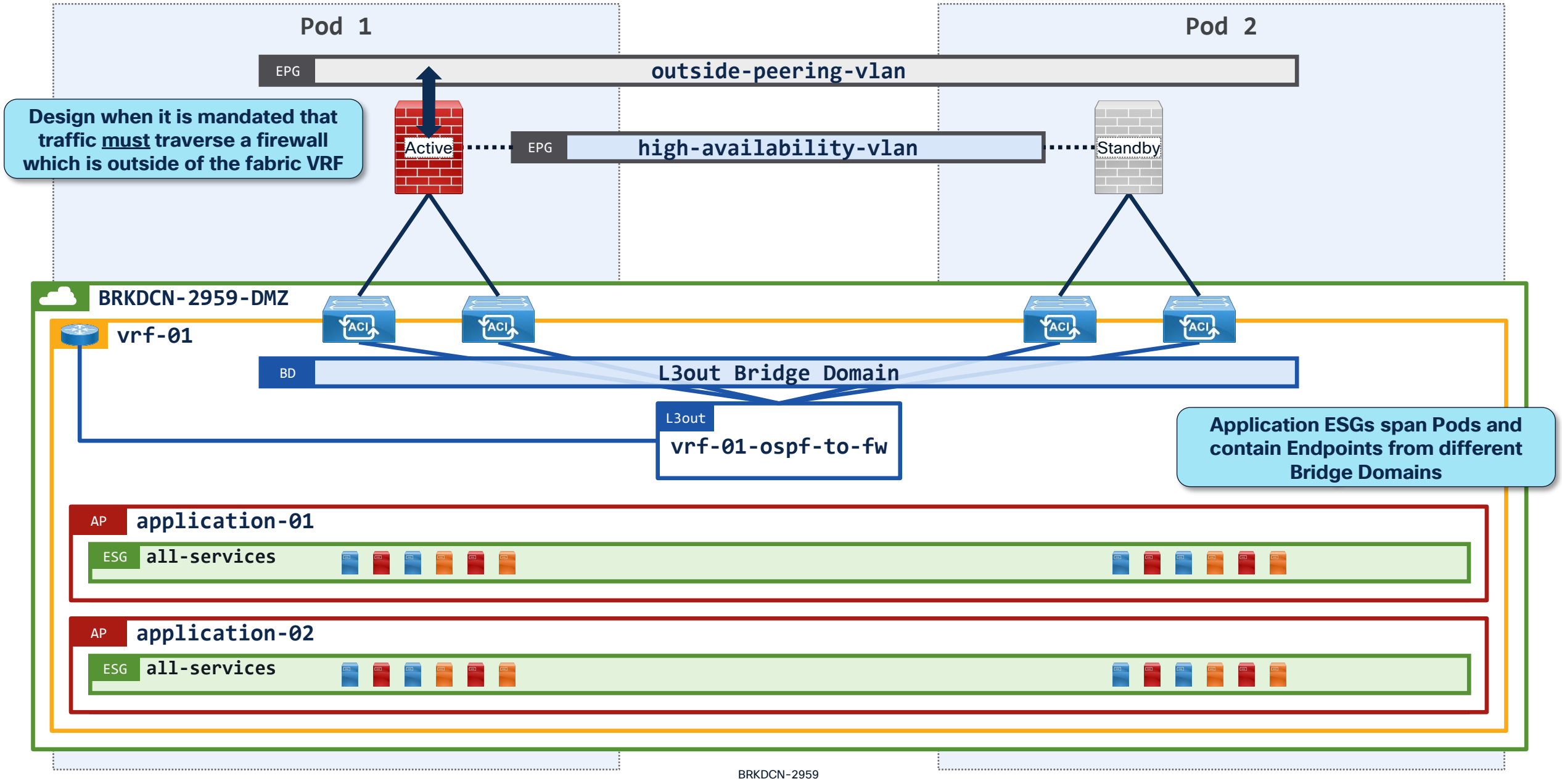
© 2025 Cisco and/or its affiliates. All rights reserved.

Firewall placement options...

Would you like your
firewall outside of the fabric,
or inside the fabric...?

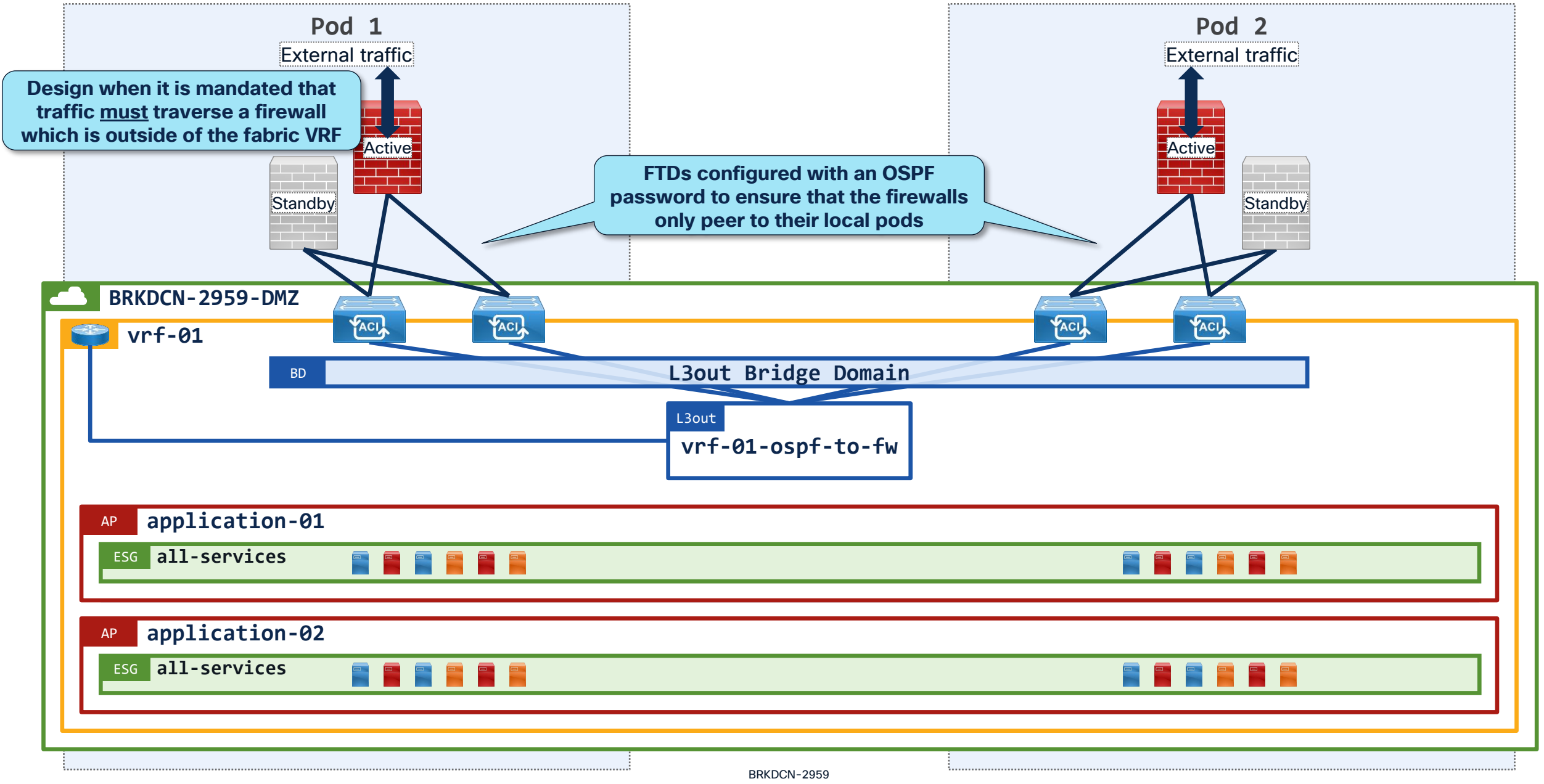
© 2025 Cisco and/or its affiliates. All rights reserved.

Option 1: Firewall outside - Active/standby across pods

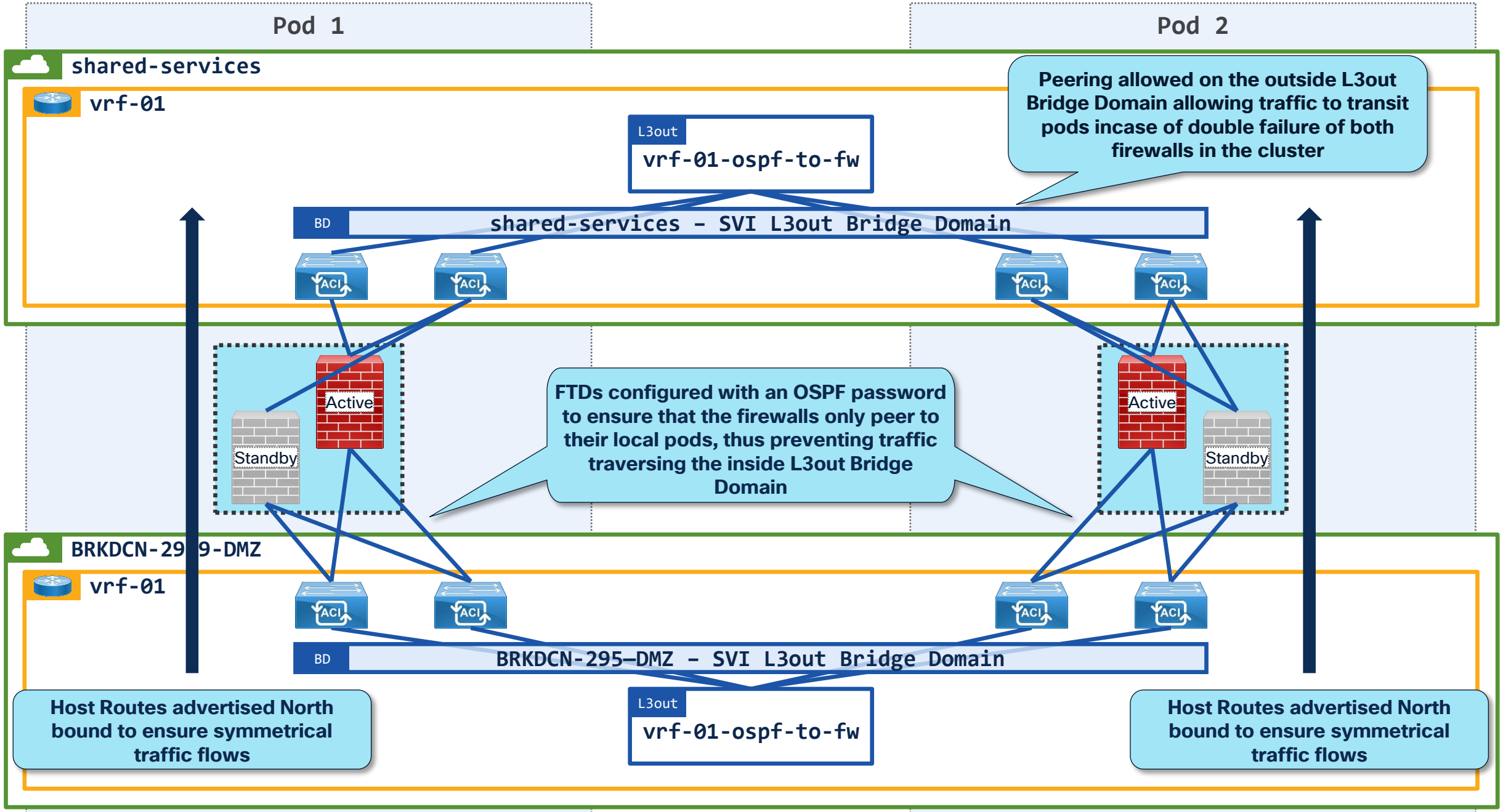


https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959-DMZ/data/01-dmz-design-firewalls-outside-one-ha-pair.nac.yaml

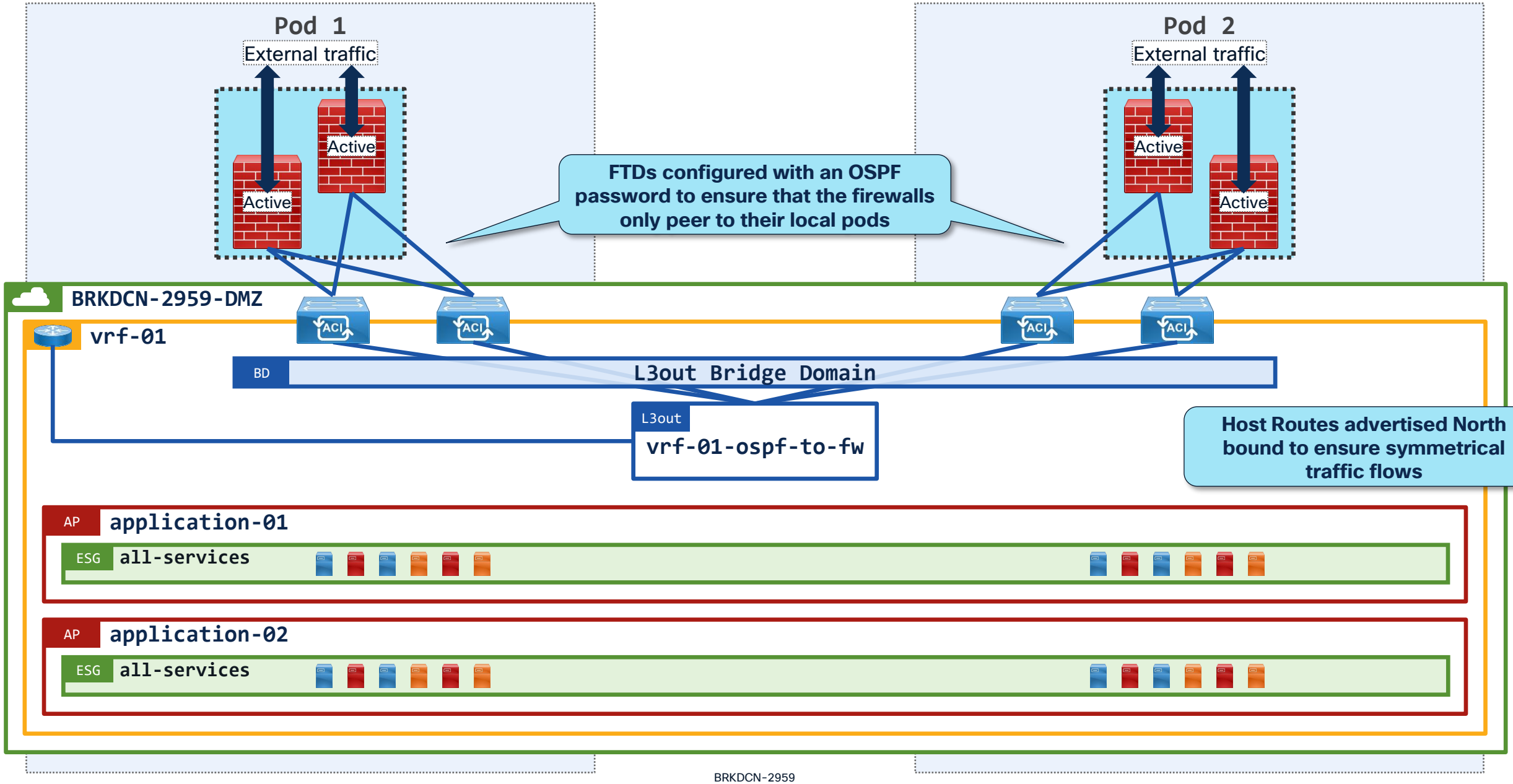
Option 2: Firewalls outside - Active/standby in both pods



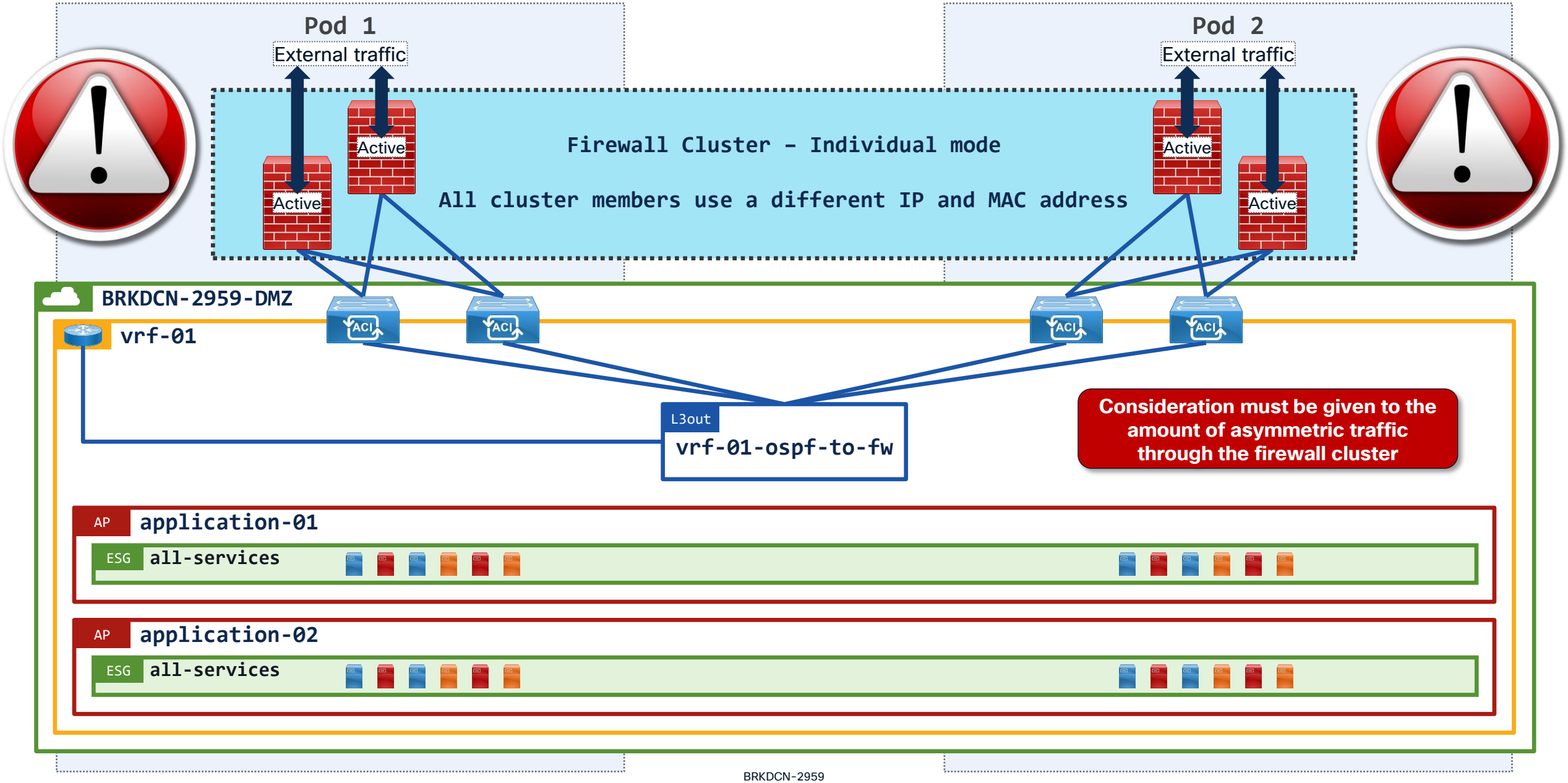
https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959-DMZ/data/02-dmz-design-firewalls-outside-two-ha-pairs.nac.yaml


Pod 1
Pod 2
shared-services
vrf-01
L3out
vrf-01-ospf-to-fw
Peering allowed on the outside L3out Bridge Domain allowing traffic to transit pods incase of double failure of both firewalls in the cluster
BD
shared-services – SVI L3out Bridge Domain
ACI
Active
Standby
FTDs configured with an OSPF password to ensure that the firewalls only peer to their local pods, thus preventing traffic traversing the inside L3out Bridge Domain
BRKDCN-29 9-DMZ
vrf-01
BD
BRKDCN-295–DMZ – SVI L3out Bridge Domain
L3out
vrf-01-ospf-to-fw
Host Routes advertised North bound to ensure symmetrical traffic flows
Host Routes advertised North bound to ensure symmetrical traffic flows

Option 3: Firewalls outside – Dual clusters

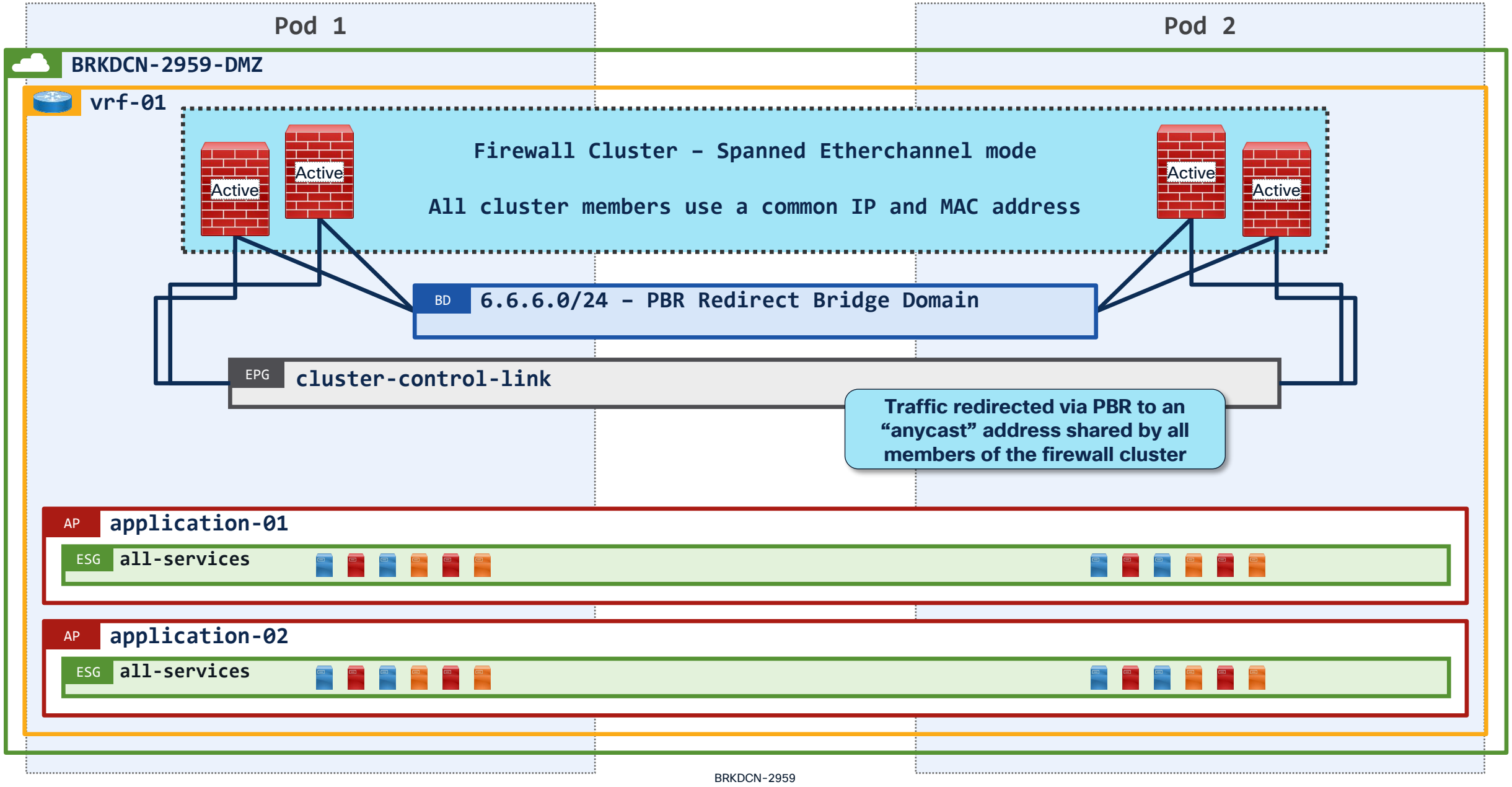


Option 4: Firewalls outside – Single “individual” mode cluster



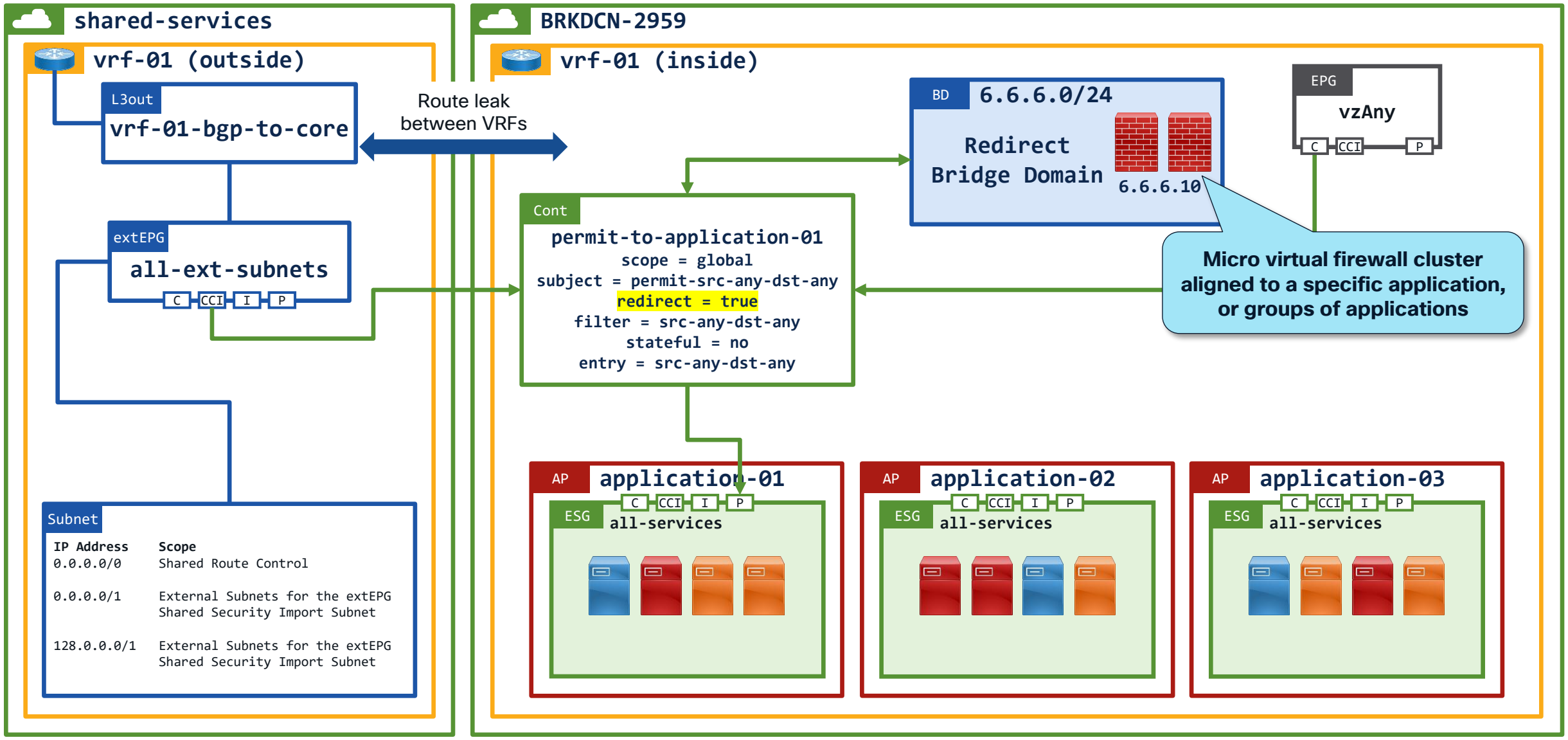
https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959-DMZ/data/03-dmz-design-firewalls-outside-dual-clusters-independent-mode.nac.yaml

Option 5: Firewall inside – Layer 3 PBR for N/S or E/W traffic



https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959-DMZ/data/05-dmz-design-firewalls-inside-single-cluster.nac.yaml

Option 6: Firewall insertion – Micro cluster firewall

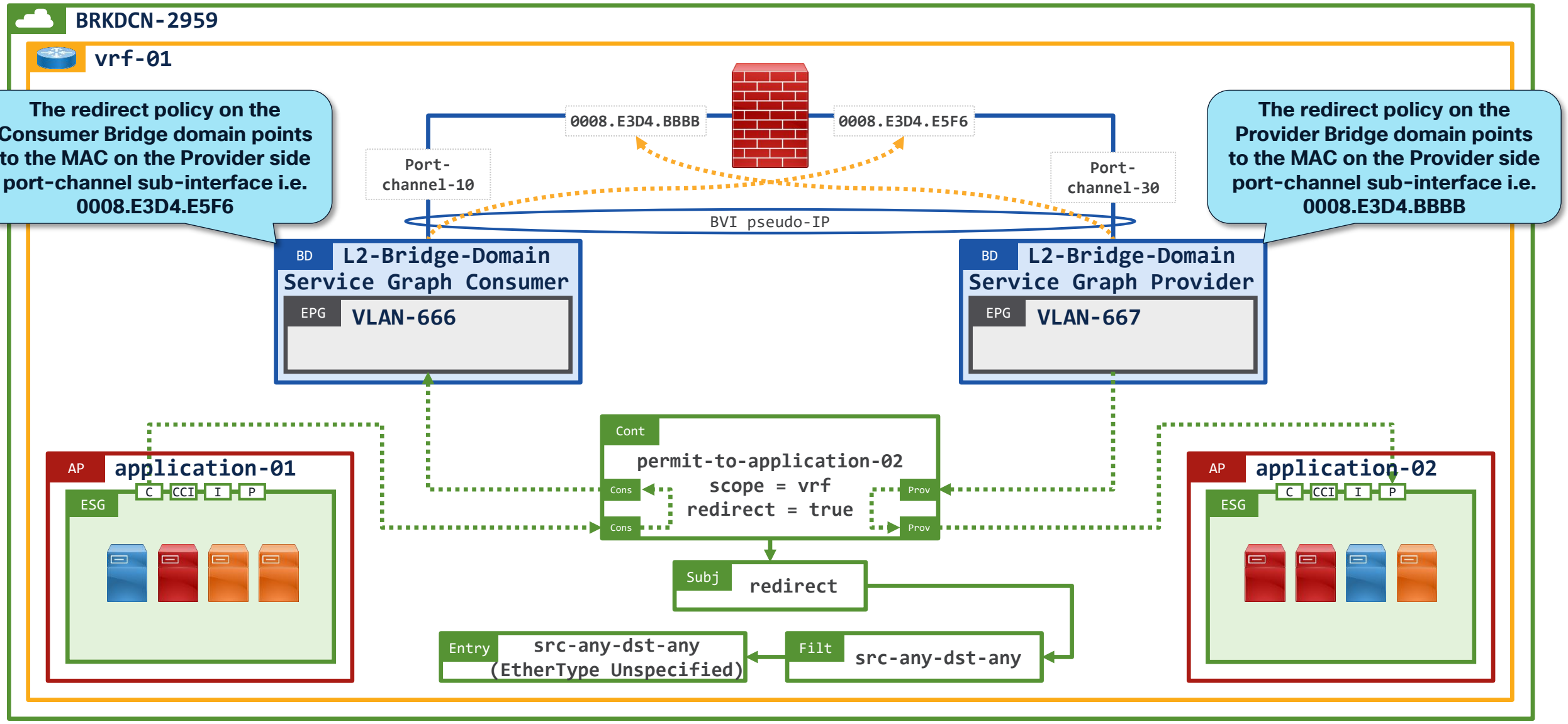


© 2025 Cisco and/or its affiliates. All rights reserved.

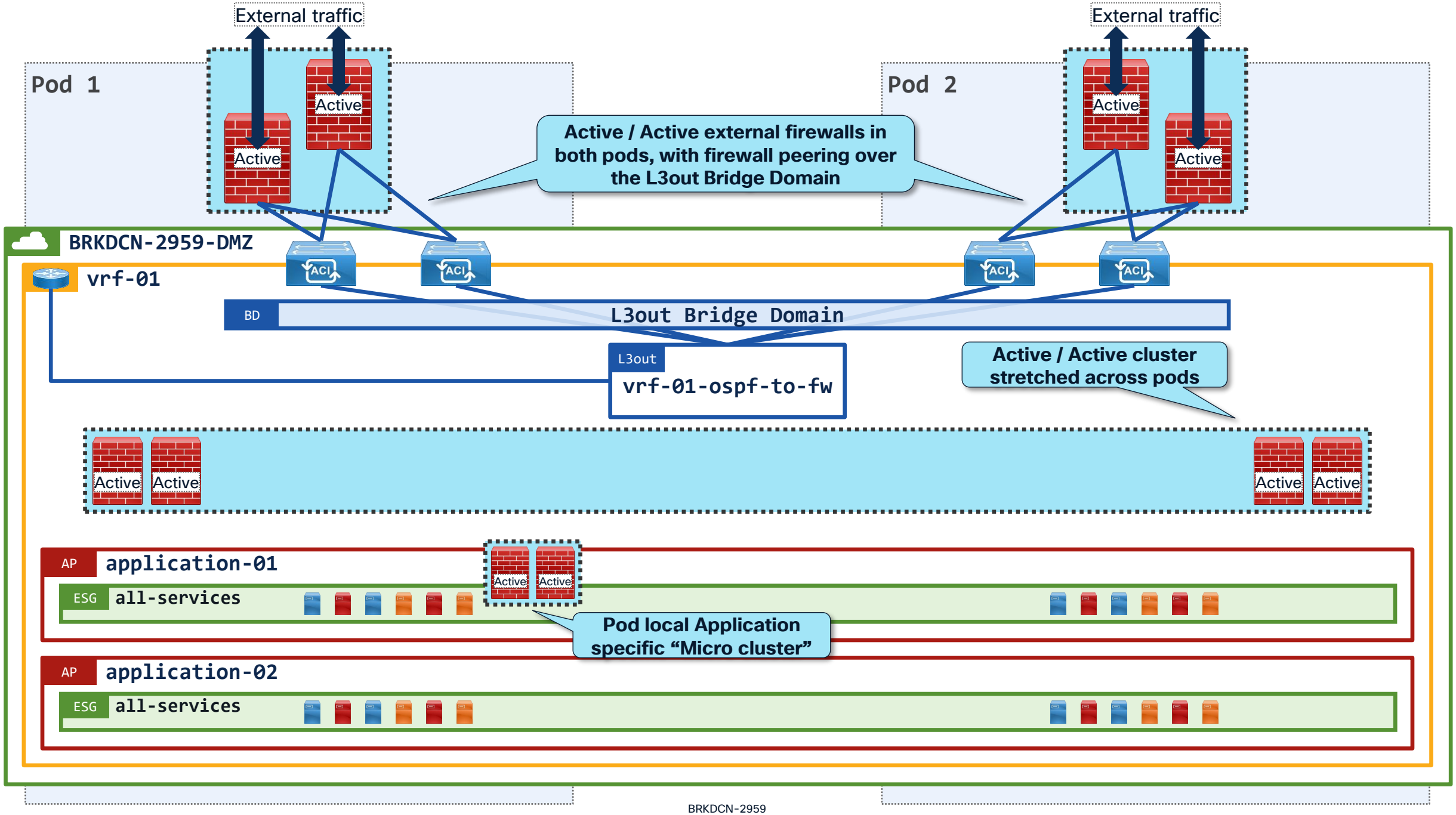
https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959-DMZ/data/06-dmz-design-firewalls-inside-micro-cluster.nac.yaml

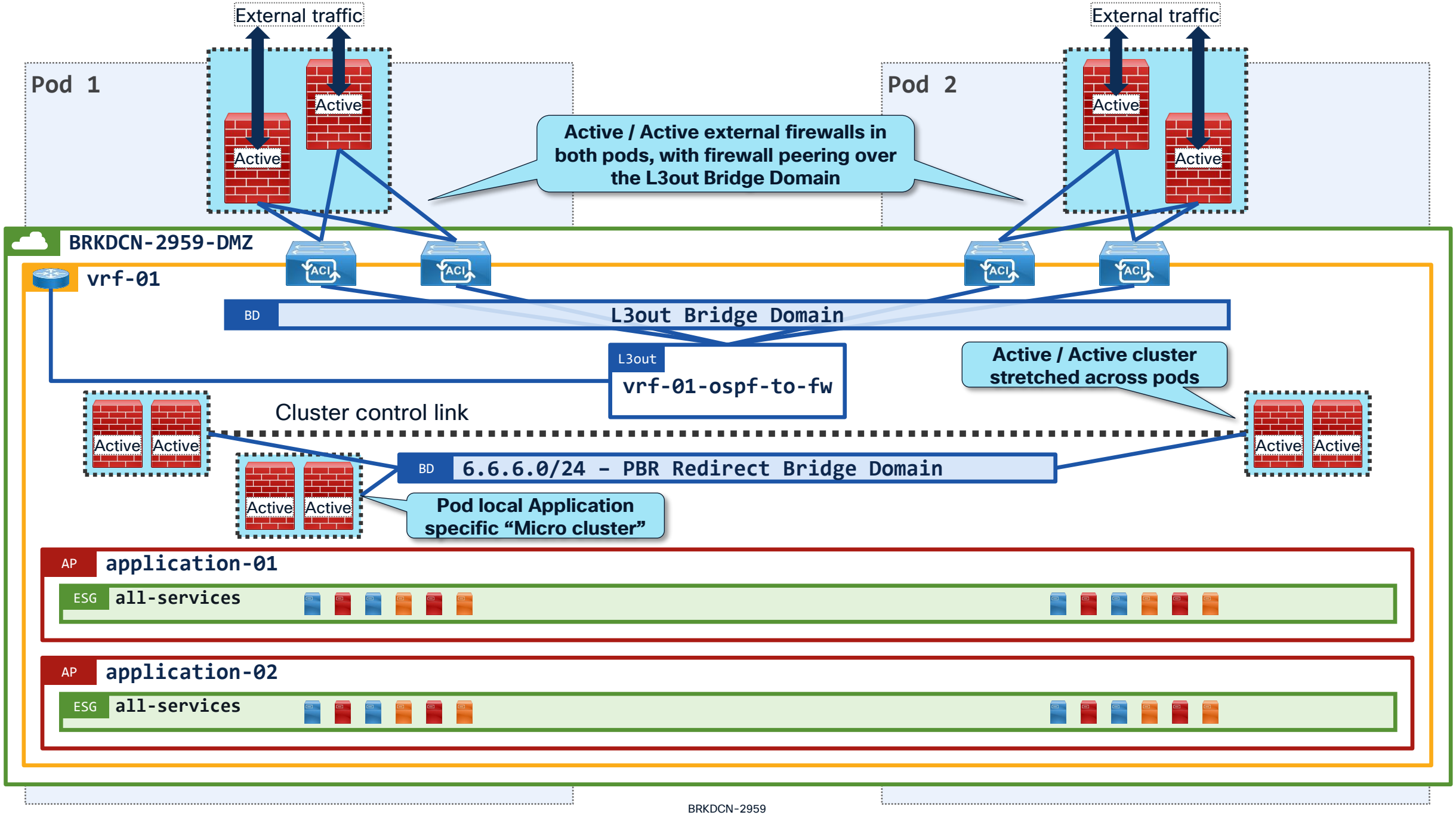
Layer 2 PBR (E/W) – single pod only

For **reference** only



© 2025 Cisco and/or its affiliates. All rights reserved.


External traffic
External traffic
Pod 1
Pod 2
Active
Active
Active
Active
Active / Active external firewalls in both pods, with firewall peering over the L3out Bridge Domain
BRKDCN-2959-DMZ
vrf-01
ACI
ACI
ACI
ACI
BD
L3out Bridge Domain
L3out
vrf-01-ospf-to-fw
Active / Active cluster stretched across pods
Active
Active
Active
Active
AP
application-01
ESG
all-services
Active
Active
Pod local Application specific “Micro cluster”
AP
application-02
ESG
all-services


External traffic
External traffic
Pod 1
Pod 2
Active
Active
Active
Active
Active / Active external firewalls in both pods, with firewall peering over the L3out Bridge Domain
BRKDCN-2959-DMZ
vrf-01
ACI
ACI
ACI
ACI
BD
L3out Bridge Domain
L3out
vrf-01-ospf-to-fw
Active / Active cluster stretched across pods
Cluster control link
Active
Active
Active
Active
Active
Active
BD
6.6.6.0/24 – PBR Redirect Bridge Domain
Pod local Application specific “Micro cluster”
AP
application-01
ESG
all-services
AP
application-02
ESG
all-services

Recommendation summary

- PBR L3 is number one choice.
  - with FTD Cluster for Active active HA, scalability and Asymetric traffic
  - with a single pair Active/Standby for HA (no asymmetrical traffic)
  - with several pairs of FTDs Active/Stanby for HA and scalability

- If PBR is not possible (like North/South Traffic)
  - cluster active/active is possible BUT might be impacted in term of performance by asymmetrical traffic
  - Pair of FTD active/Standby but need to be sized with scaling in mind

© 2025 Cisco and/or its affiliates. All rights reserved.

Customer requirement

Implement a modern DMZ design for selective redirection and endpoint security

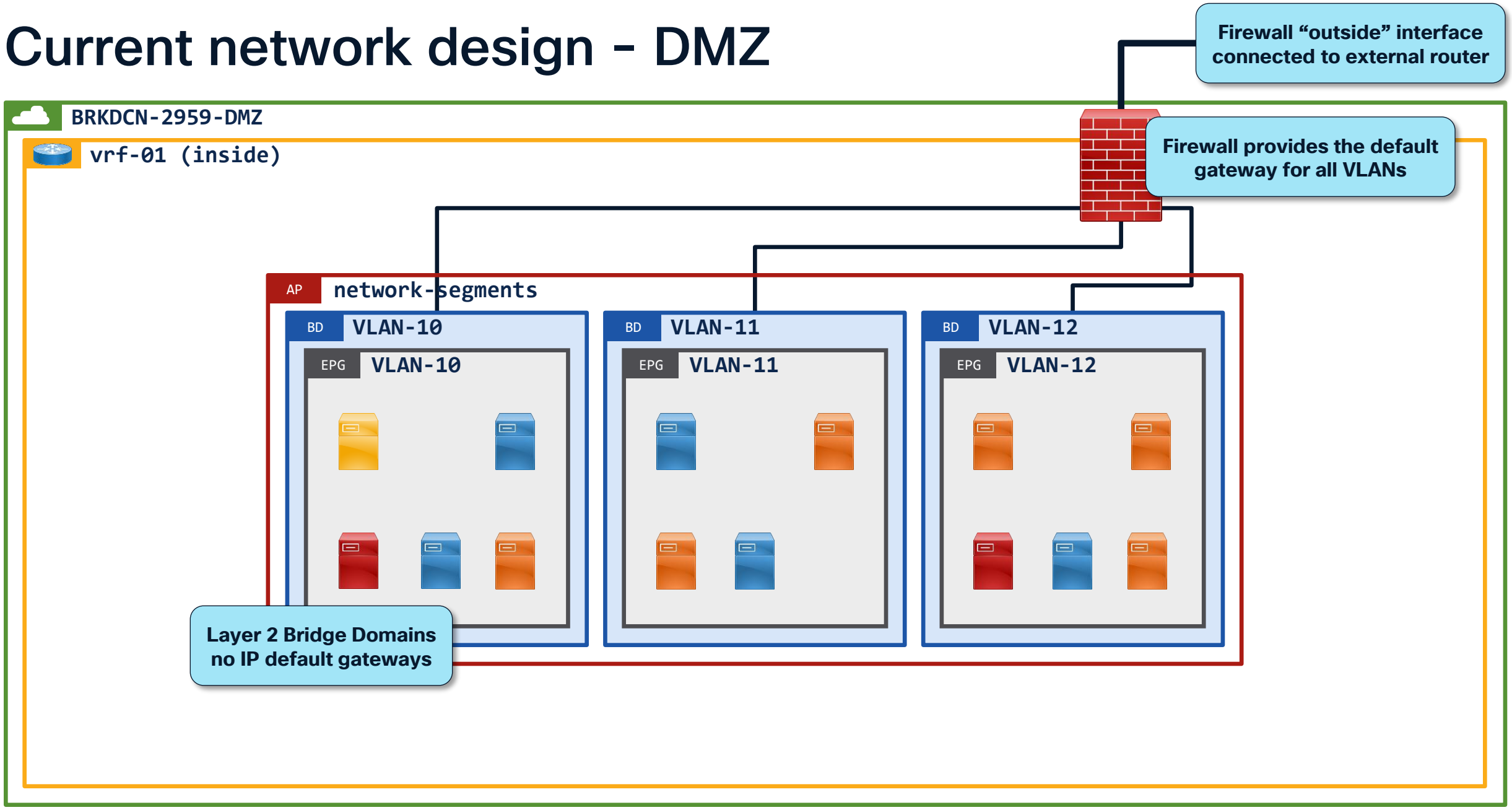
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

DMZ redesign...

- Where networking and security come together...
- Customer's current network design...
- Security control over inbound traffic...
- Understanding ACI security...
- Zero trust application-based security...
- Layer 7 security integration...
- **DMZ redesign...**
- Reducing operational complexity of segmentation
- Implement Zero trust Micro-segmentation

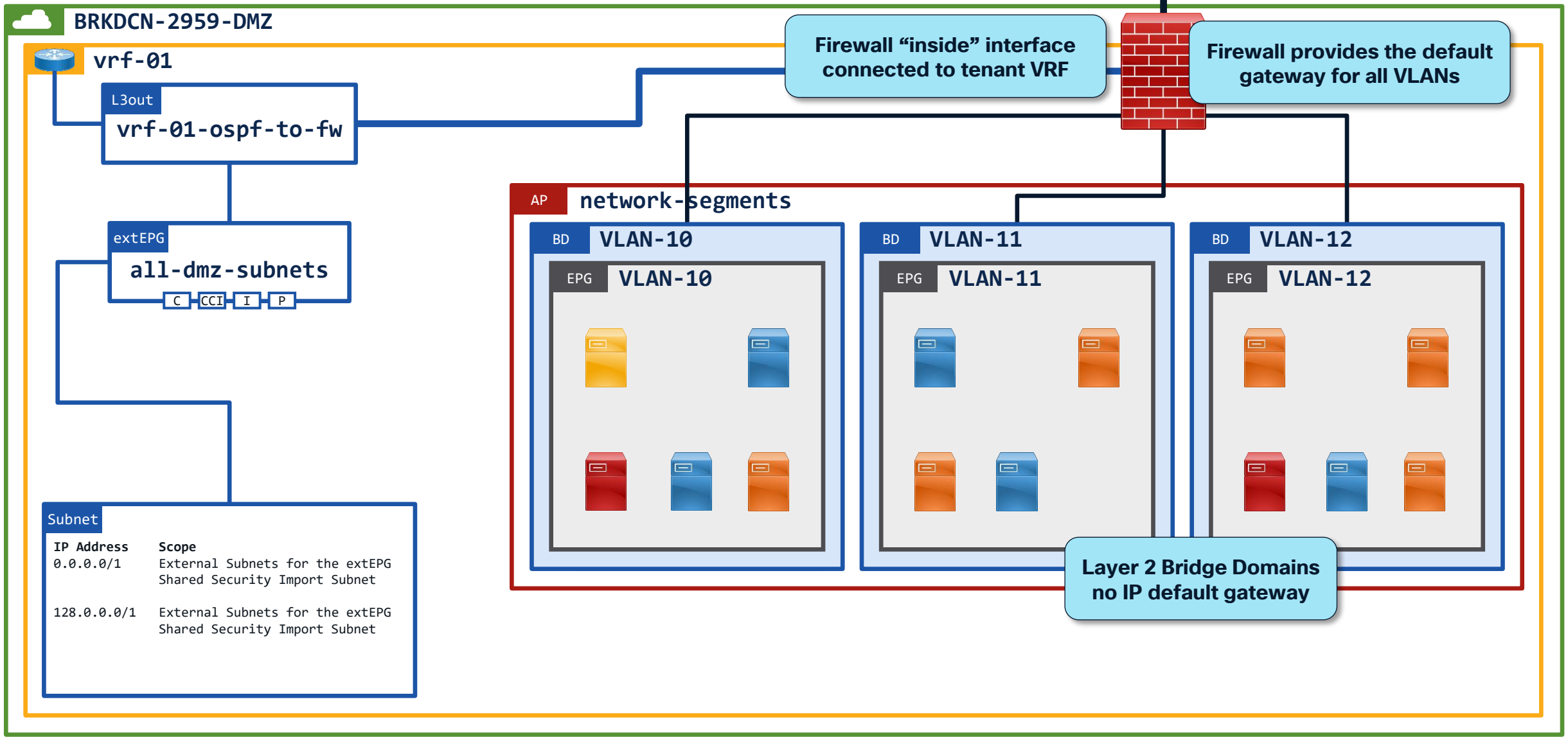
Current network design - DMZ



© 2025 Cisco and/or its affiliates. All rights reserved.

https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959-DMZ/data/07-dmz-current-design-firewall-provides-default-gateway.nac.yaml

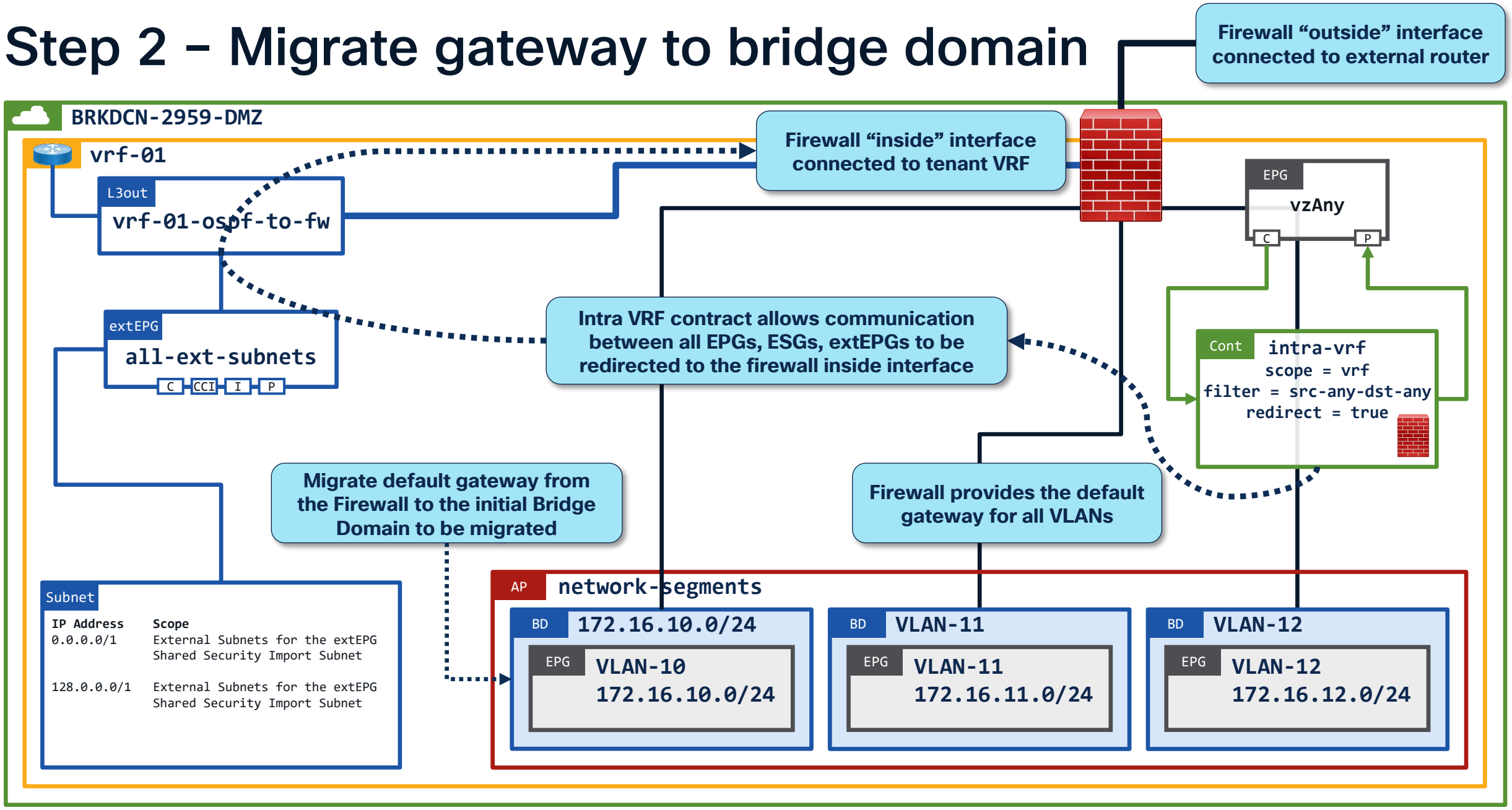
Step 1 – Peer from DMZ VRF to firewall



© 2025 Cisco and/or its affiliates. All rights reserved.

https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959-DMZ/data/08-dmz-design-firewall-provides-default-gateway-peering-to-fabric-vrf.nac.yaml

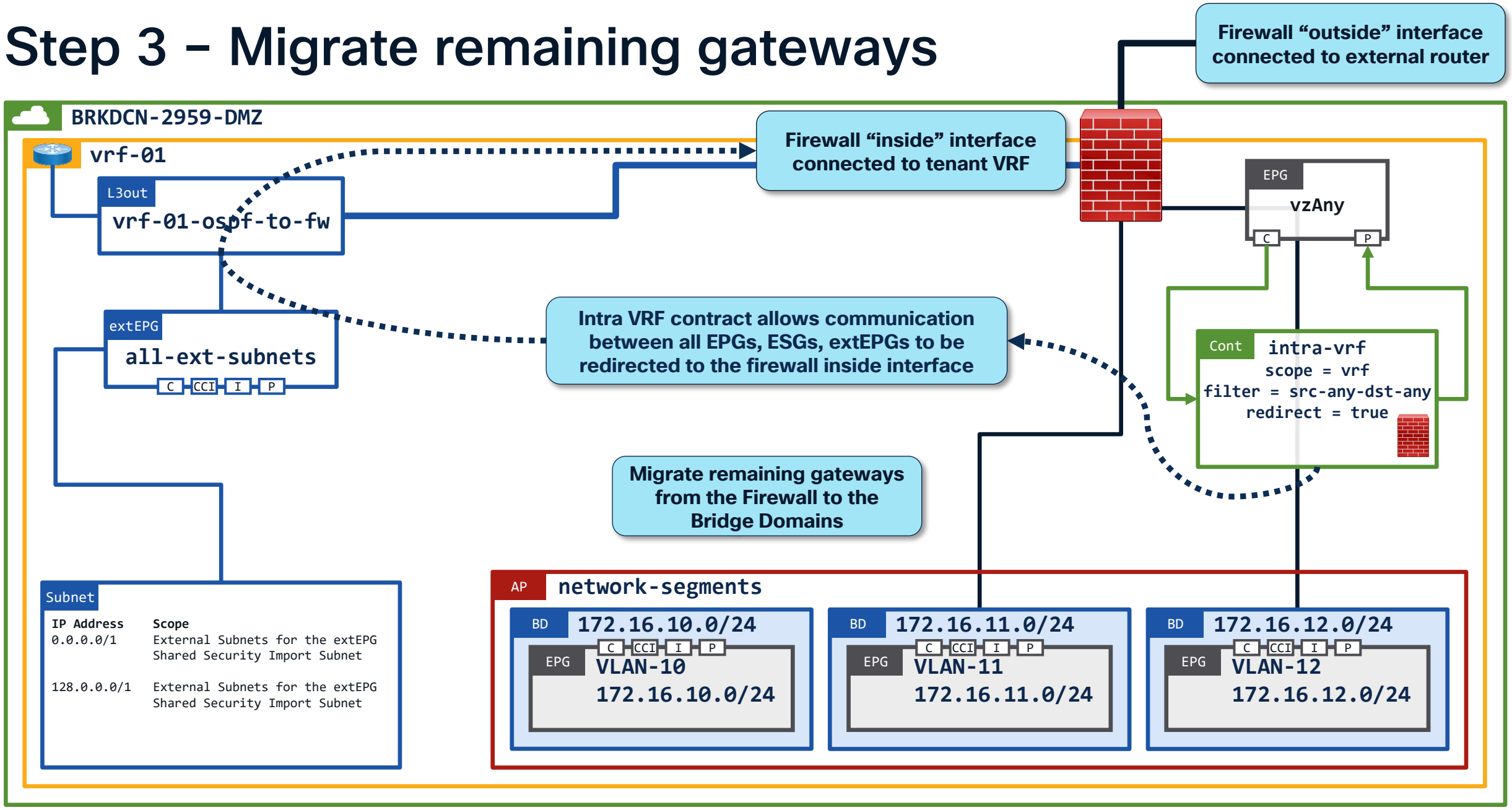
Step 2 – Migrate gateway to bridge domain



© 2025 Cisco and/or its affiliates. All rights reserved.

https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959-DMZ/data/09-dmz-design-initial-bd-peering-to-fabric-vrf.nac.yaml

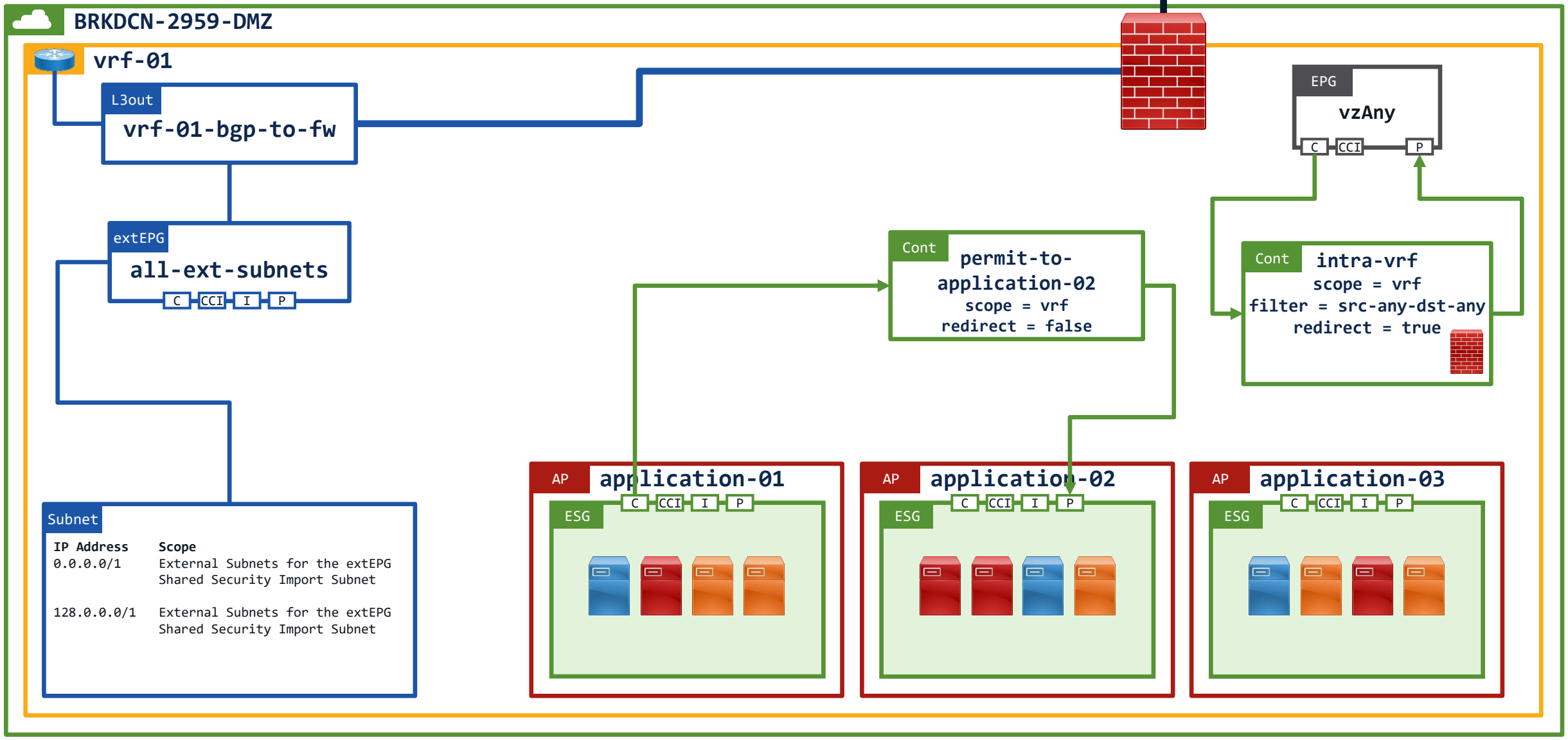
Step 3 – Migrate remaining gateways



© 2025 Cisco and/or its affiliates. All rights reserved.

https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959-DMZ/data/10-dmz-design-dual-bd-peering-to-fabric-vrf.nac.yaml

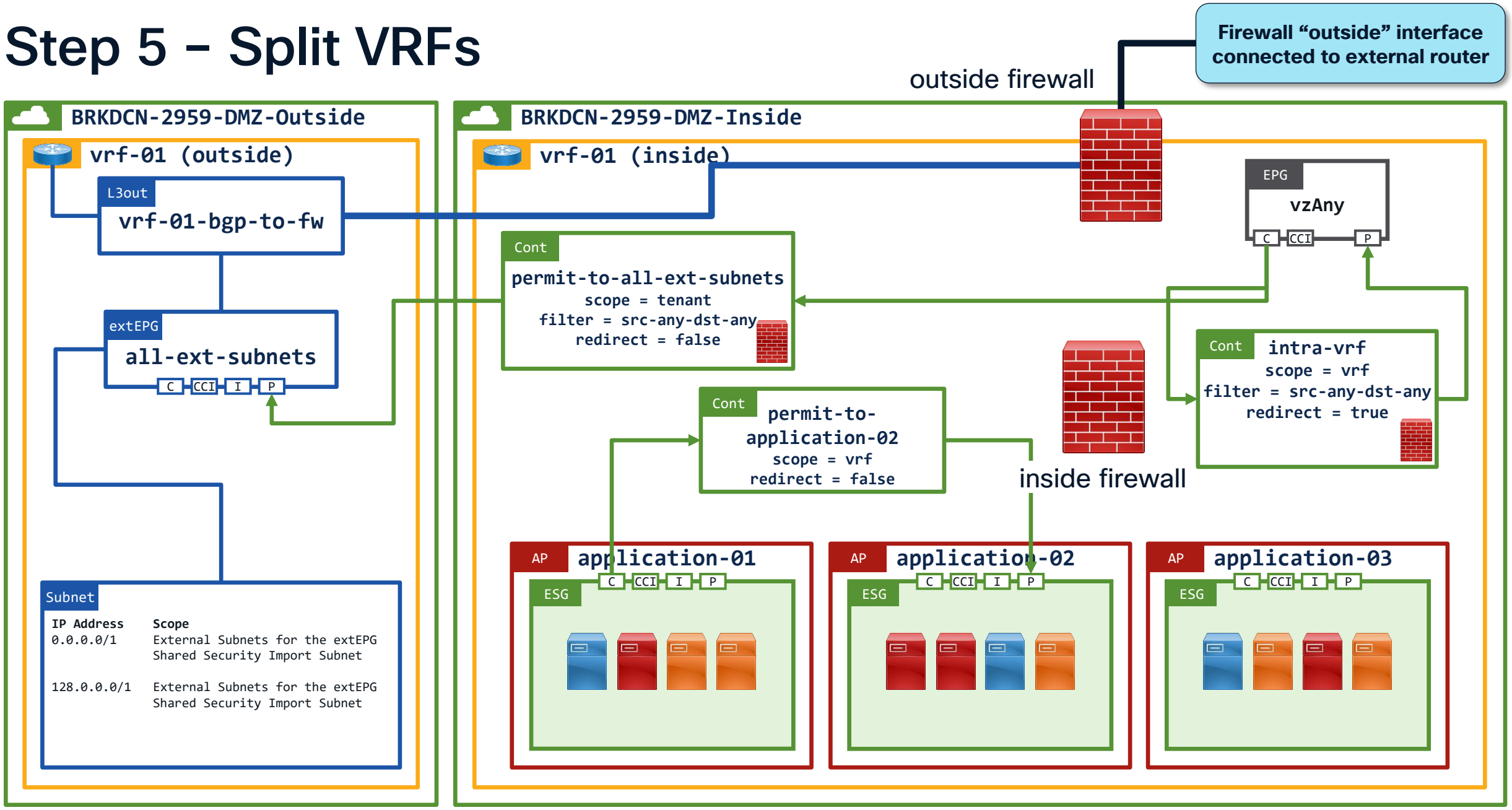
Step 4 – Add application groups



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Step 5 – Split VRFs

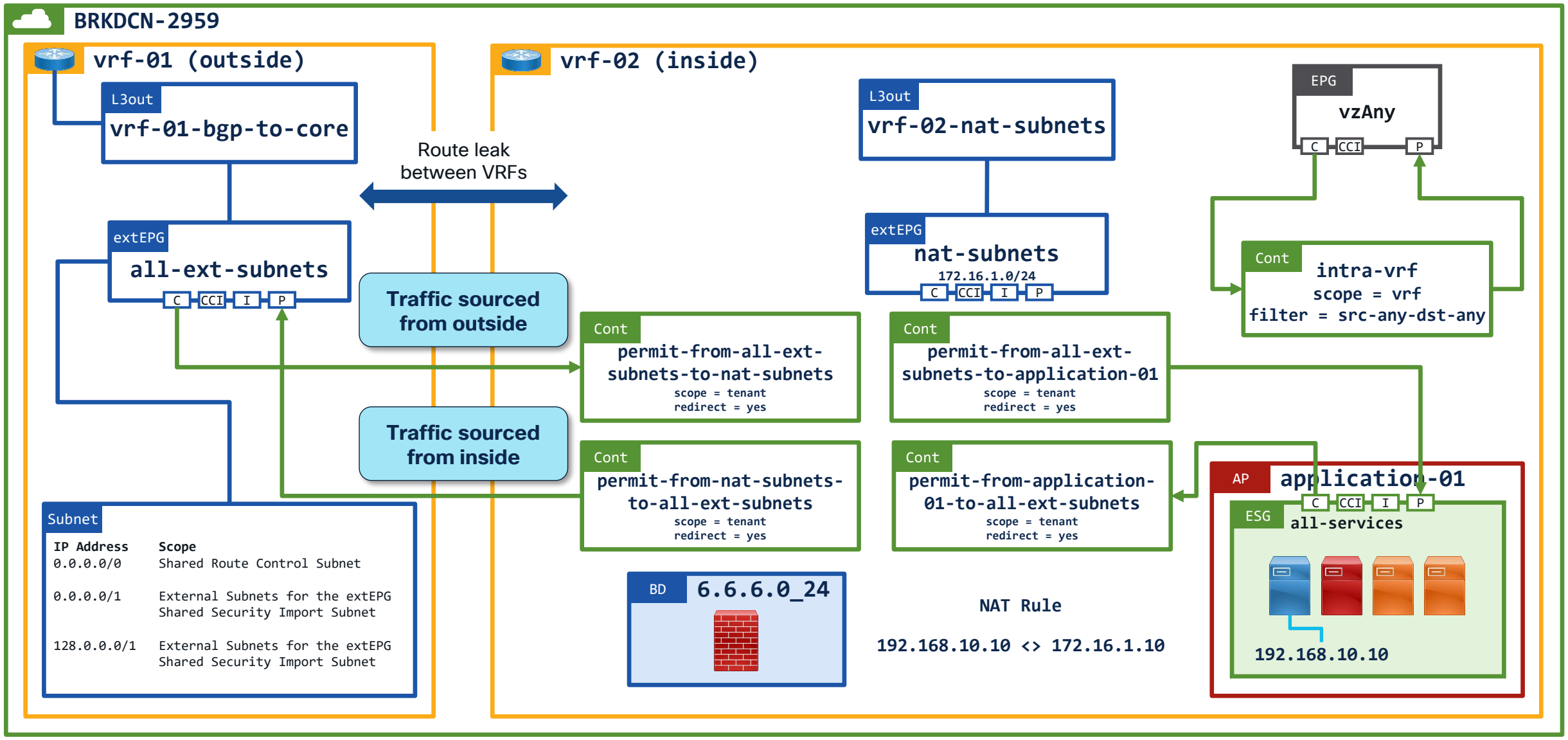


© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

What about PBR for NAT...?

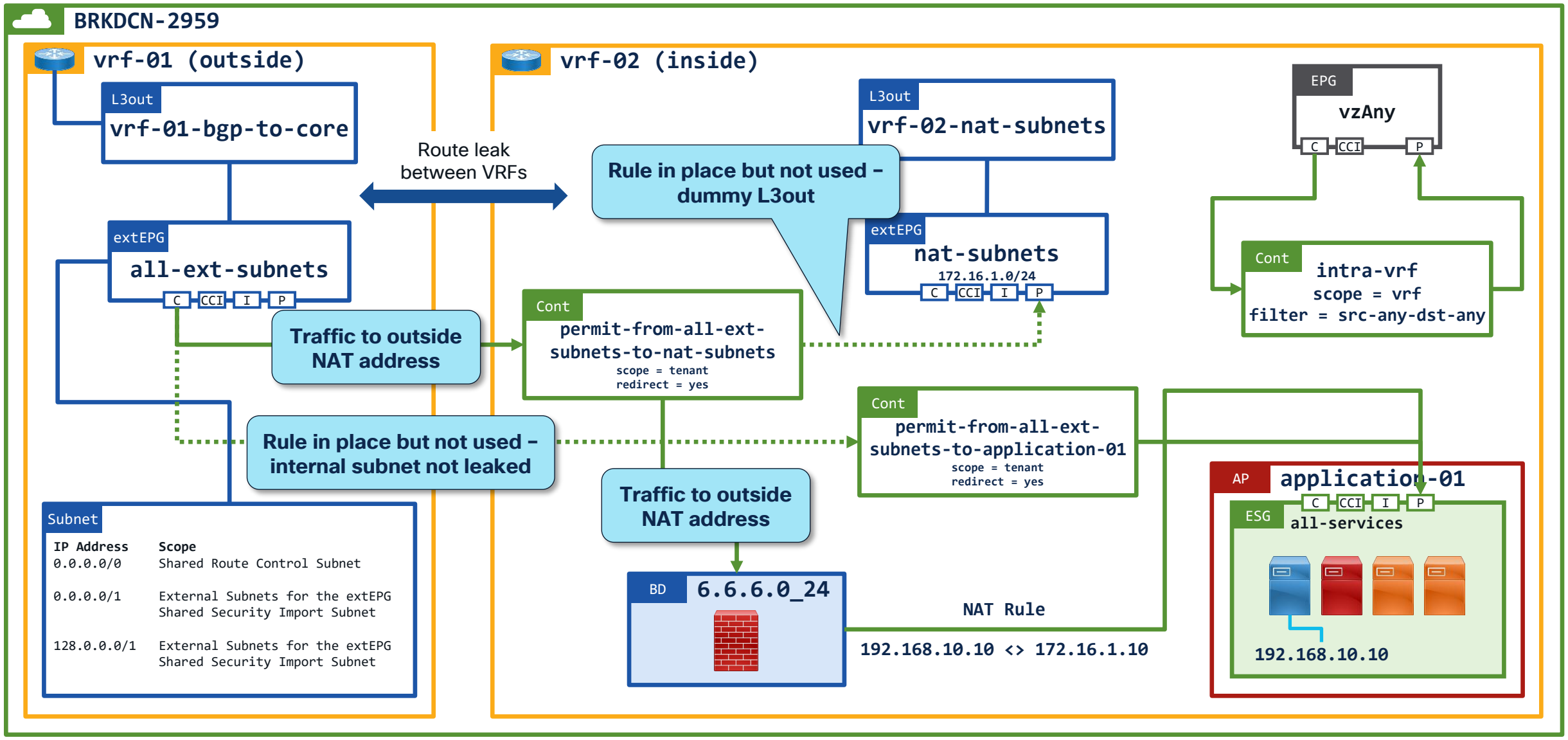
Topology – High Level Overview



© 2025 Cisco and/or its affiliates. All rights reserved.

https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959/data/18-production-dual-vrf-l3out-design-with-nat.nac.yaml

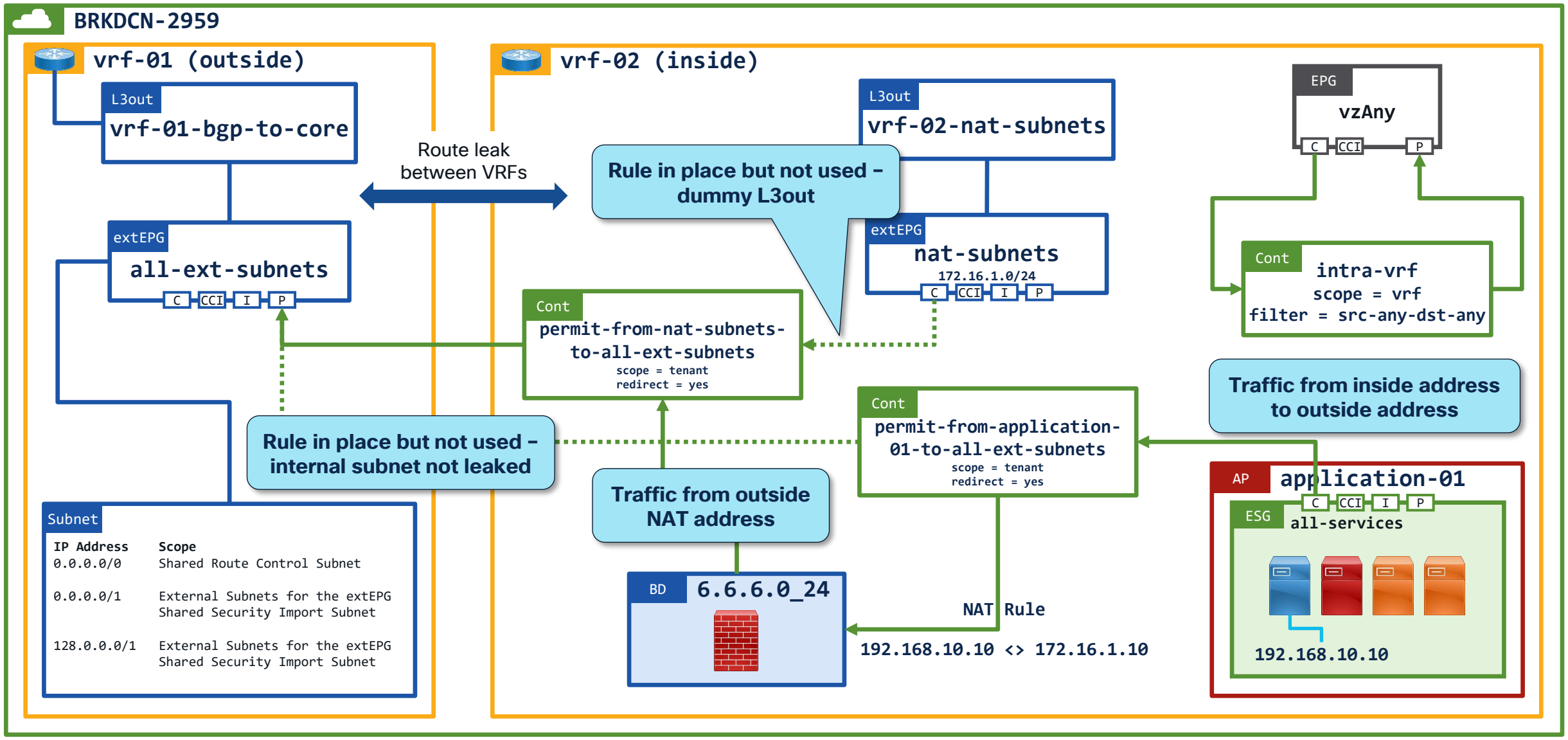
Traffic from “external” endpoints to application “outside” NAT IP



© 2025 Cisco and/or its affiliates. All rights reserved.

https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959/data/18-production-dual-vrf-l3out-design-with-nat.nac.yaml

Traffic from application “inside” IP to external IP addresses



© 2025 Cisco and/or its affiliates. All rights reserved.

https://github.com/spsharman/aci-dev-01/blob/main/BRKDCN-2959/data/18-production-dual-vrf-l3out-design-with-nat.nac.yaml

Customer requirement

Implement an intent-based security policy leveraging dynamic groups while reducing operational complexity

© 2025 Cisco and/or its affiliates. All rights reserved.

Reducing segmentation operational complexity...

- Where networking and security come together...
- Customer's current network design...
- Security control over inbound traffic...
- Understanding ACI security...
- Zero trust application-based security...
- Layer 7 security integration...
- DMZ redesign...
- **Reducing operational complexity of segmentation**
- Implement Zero trust Micro-segmentation

The problem statement

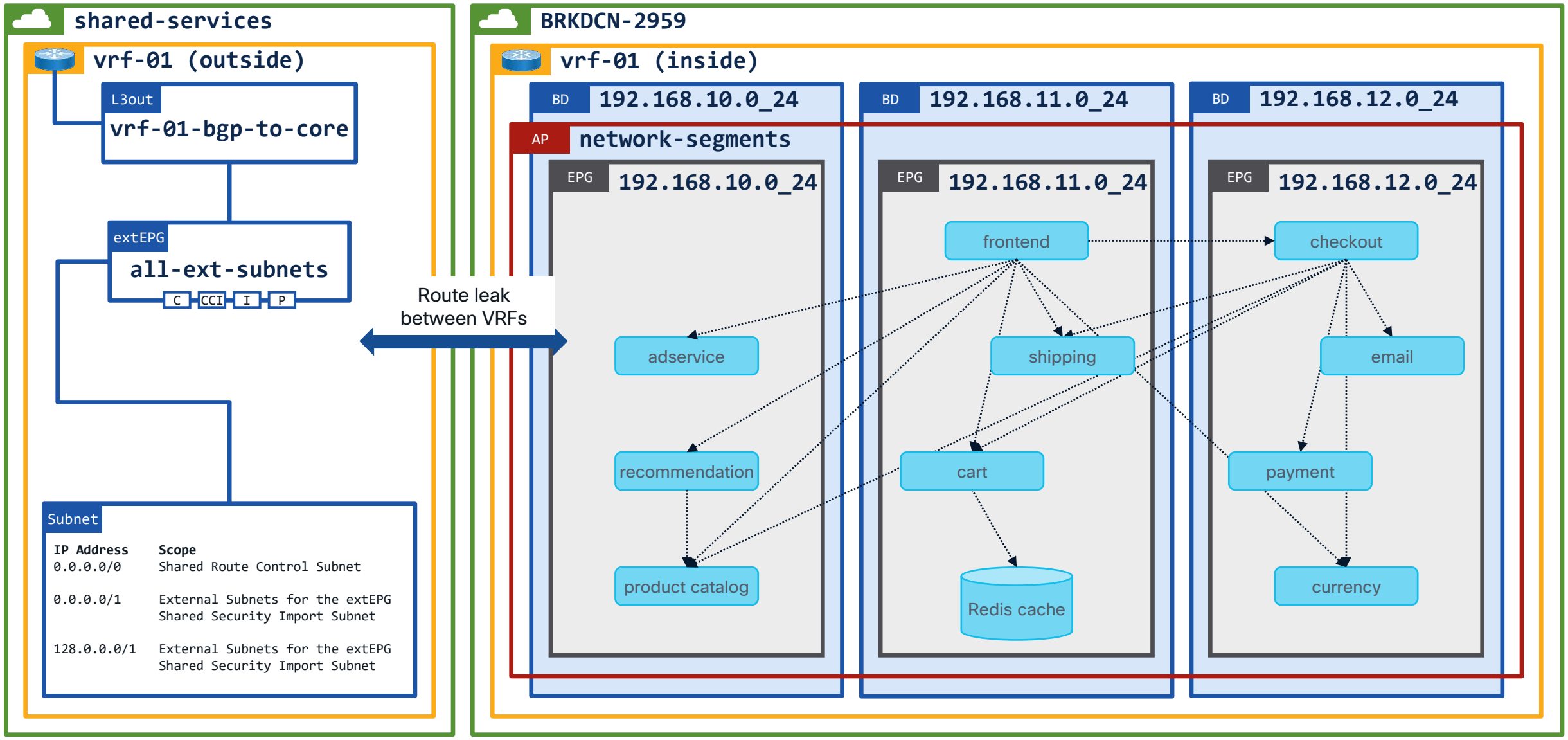
How to build a policy based on intent instead of static IPs?

How to reduce changes on enforcement point?

How to build a policy with cross security Domain?

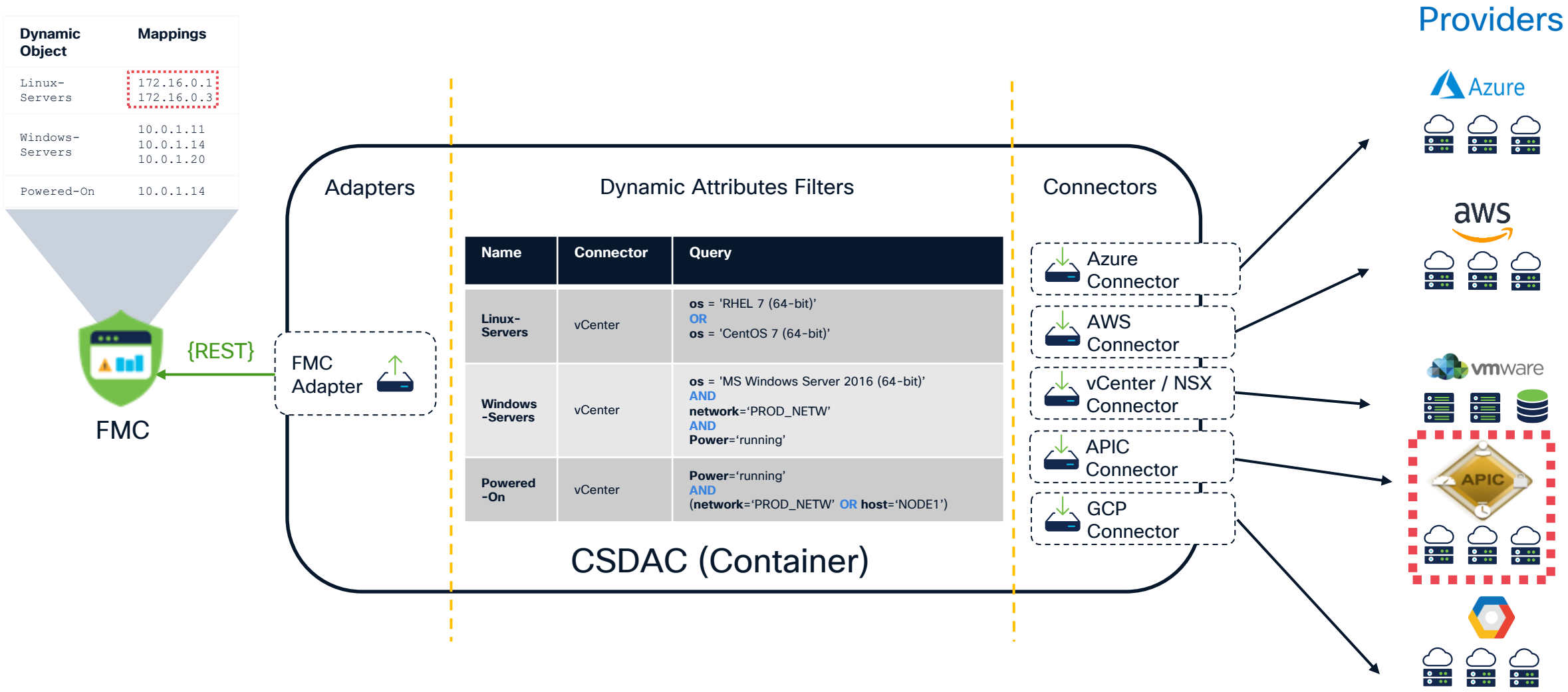
© 2025 Cisco and/or its affiliates. All rights reserved.

Where is our application running...?



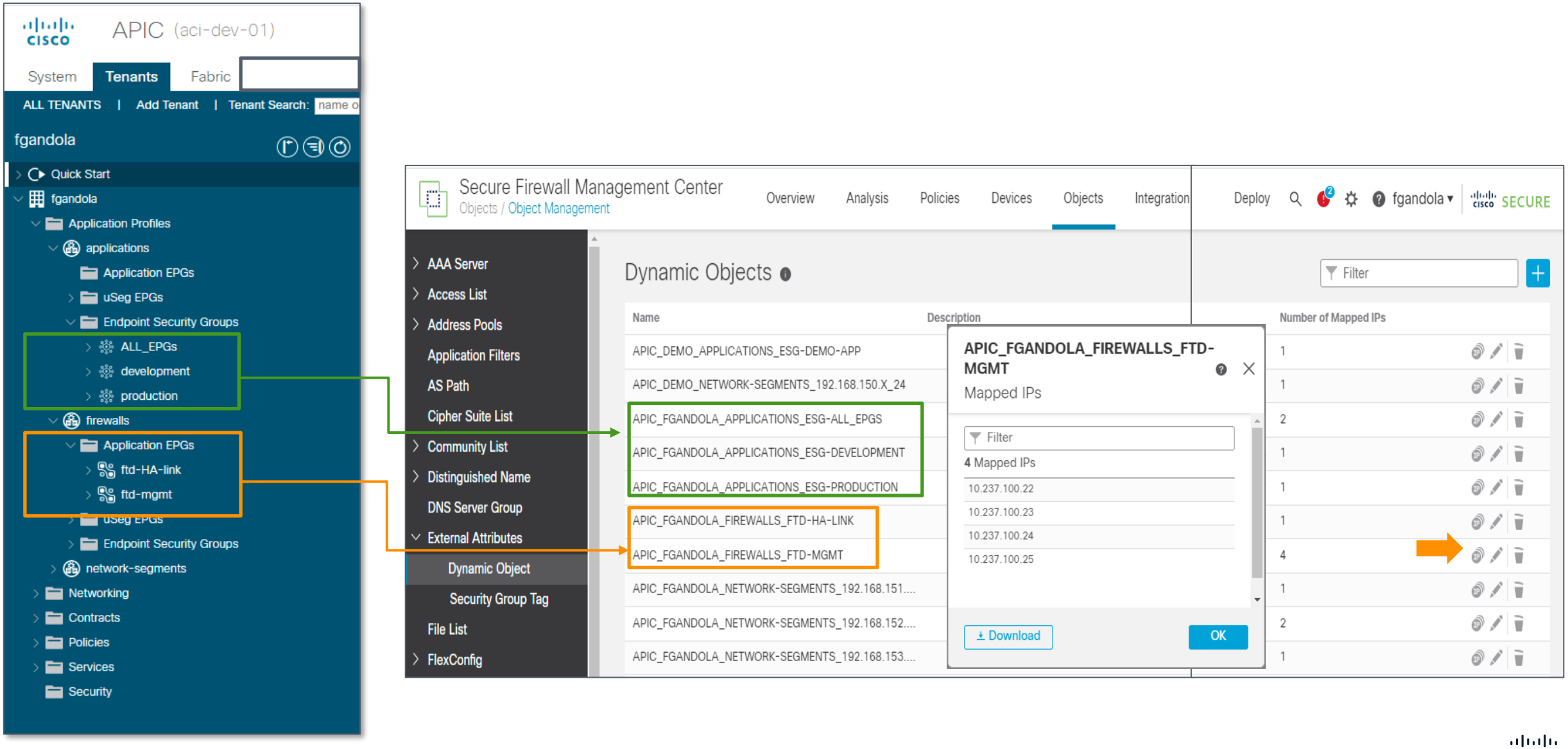
© 2025 Cisco and/or its affiliates. All rights reserved.

Architecture of the Dynamic Attributes Connector



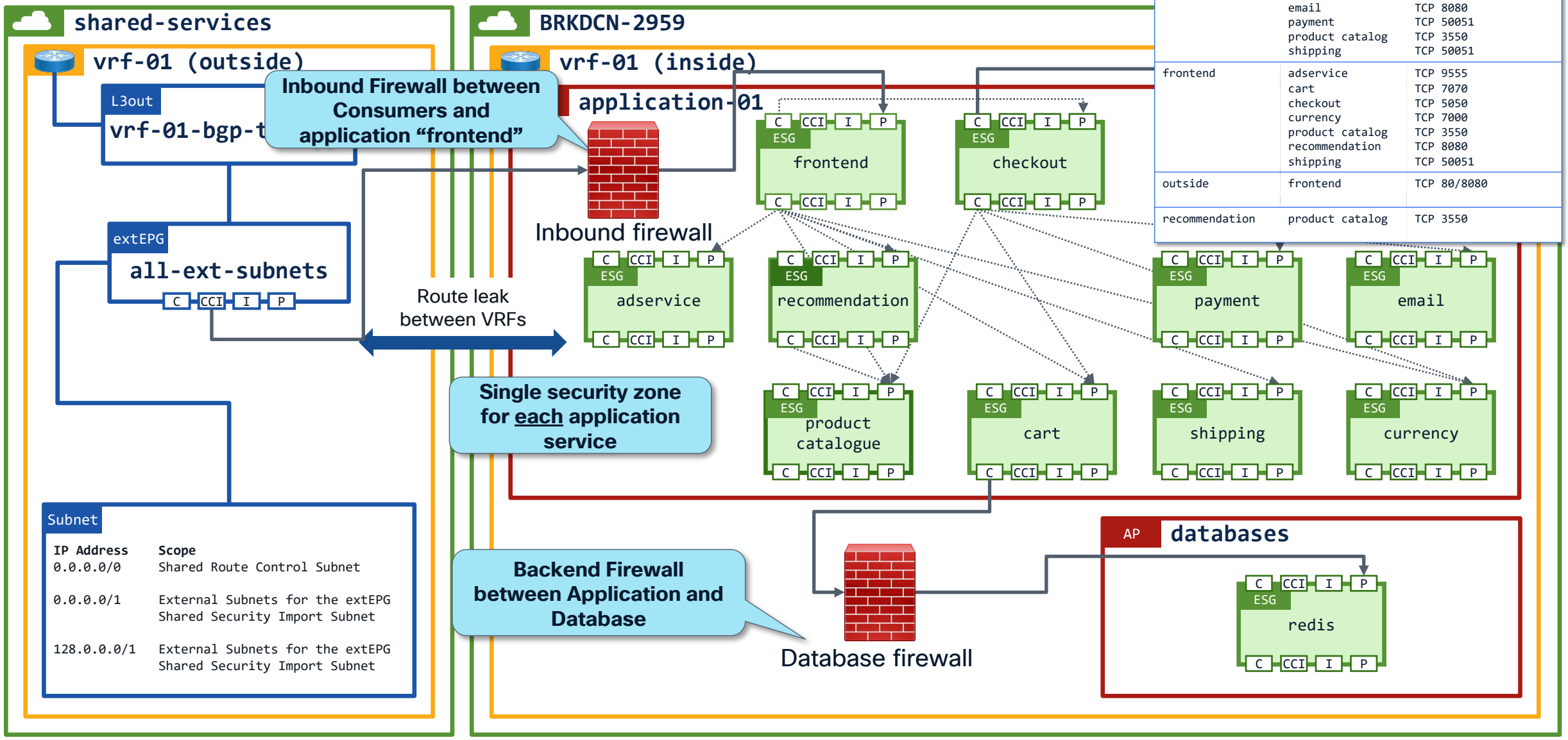
© 2025 Cisco and/or its affiliates. All rights reserved.

FMC Learns EPGs/ESGs as Dynamic Attributes



© 2025 Cisco and/or its affiliates. All rights reserved.

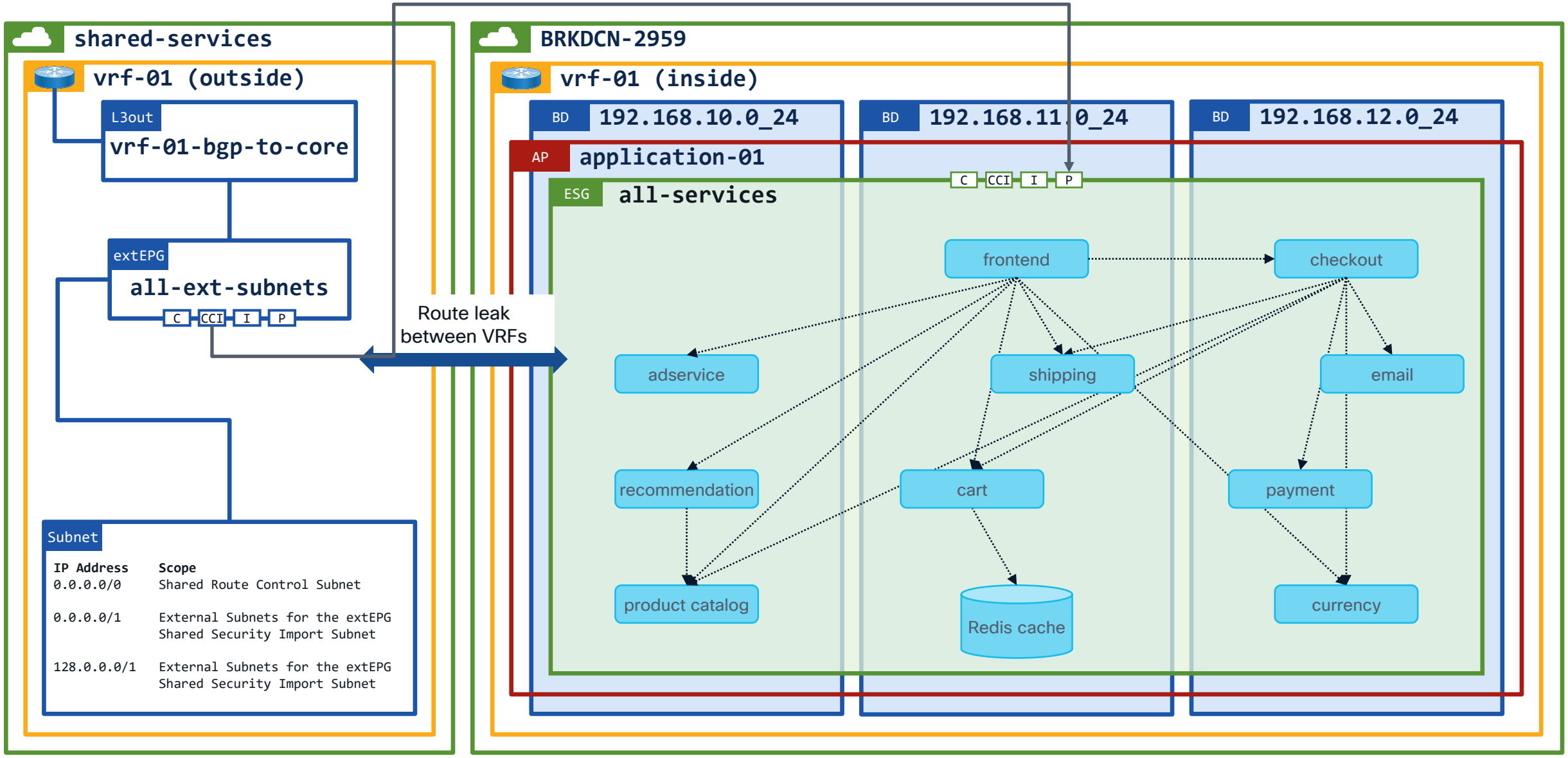
Tiered security approach



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

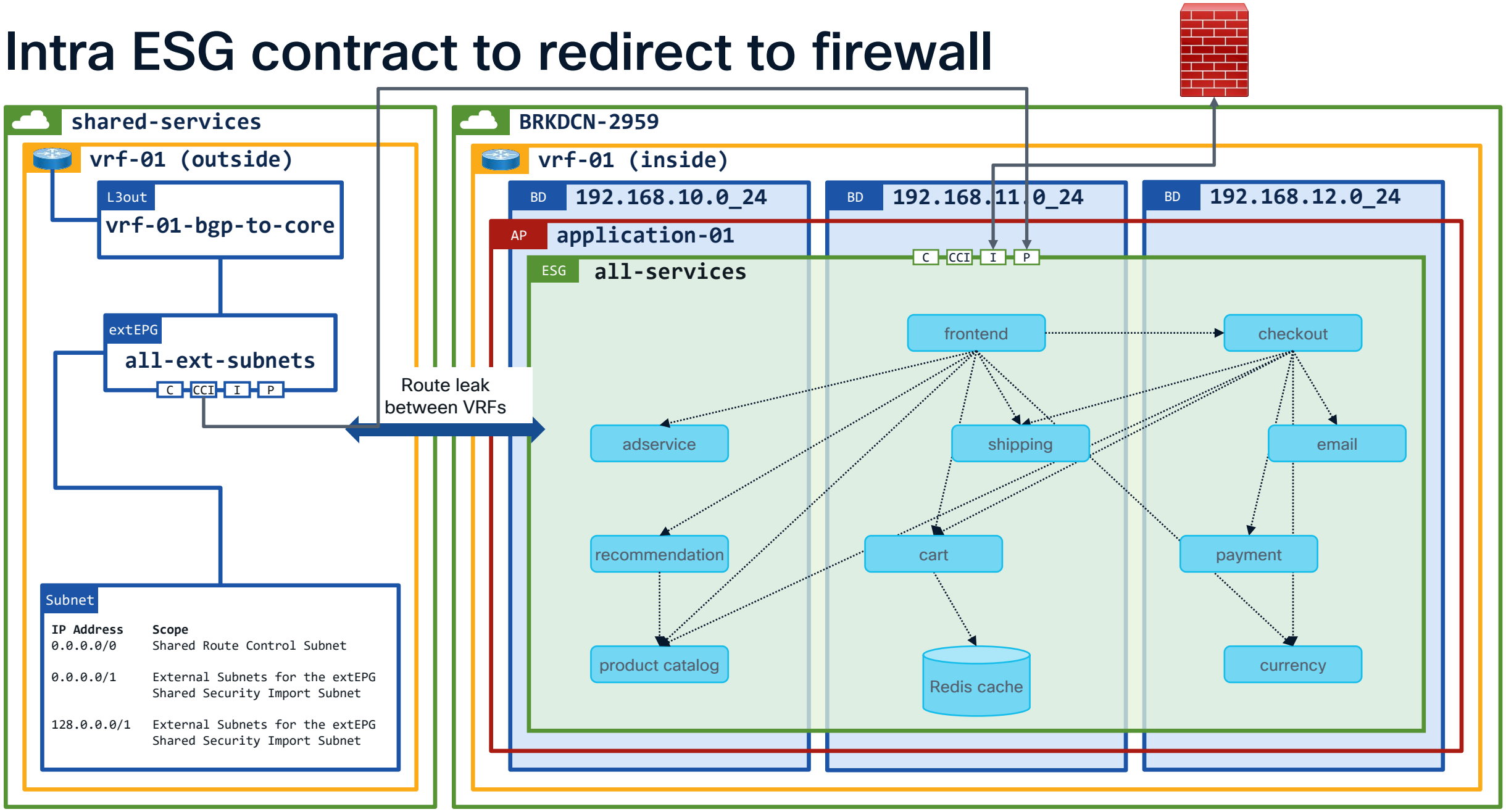
© 2025 Cisco and/or its affiliates. All rights reserved.

Single ESG per application is preferred



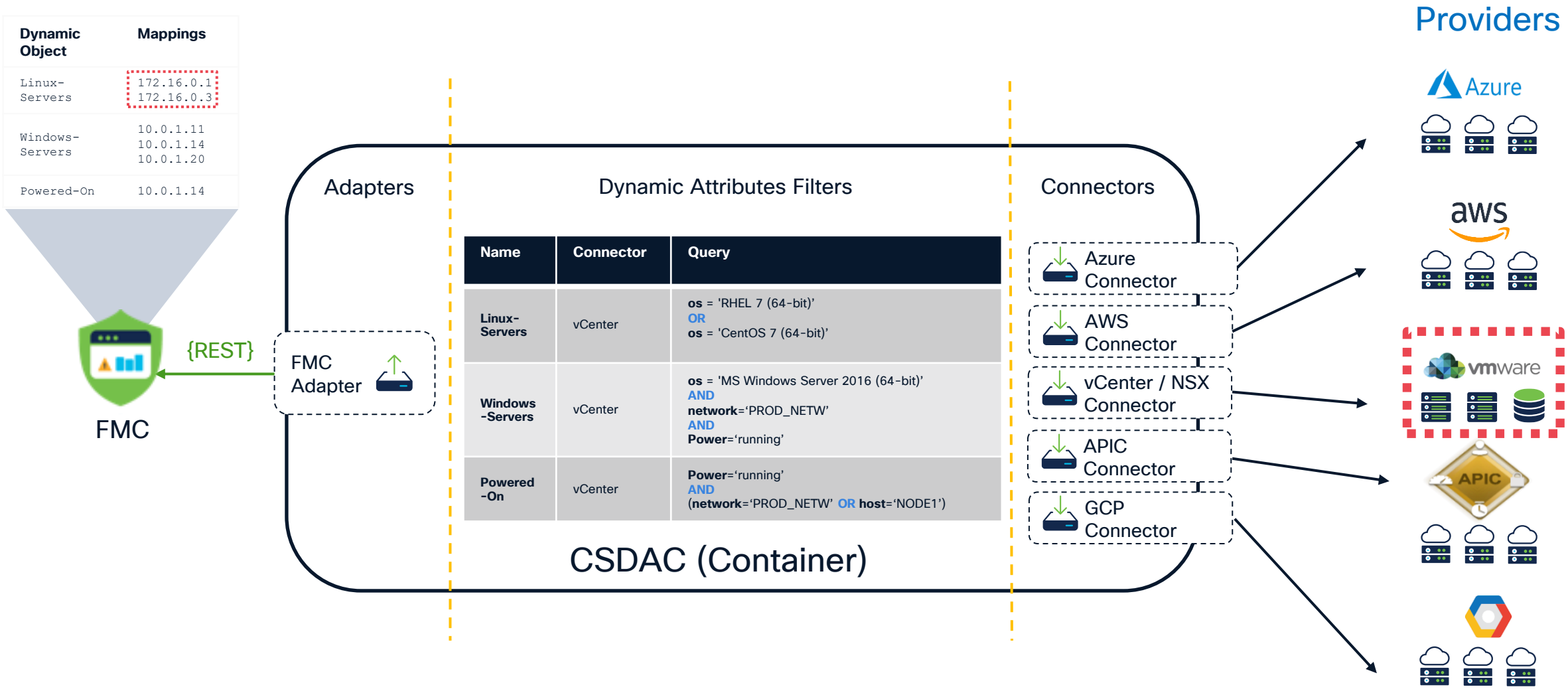
© 2025 Cisco and/or its affiliates. All rights reserved.

Intra ESG contract to redirect to firewall



© 2025 Cisco and/or its affiliates. All rights reserved.

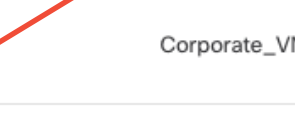
Architecture of the Dynamic Attributes Connector

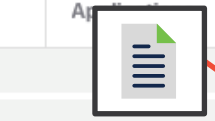


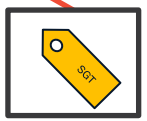
© 2025 Cisco and/or its affiliates. All rights reserved.

Attribute Based Policy

#	Name	Source Zones	Dest Zones	Users	Ap...	Dest Ports	Source Dynamic Attributes	Destination Dynamic ...es	Action
>	Mandatory - Attribute-Based Policy (-)								
v	Default - Attribute-Based Policy (1-9)								
1	Workload_1	Any	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	A...
2	IoT Support Service	External	IoT_VN	Any	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Pri...	Corporate_VN	Data_Center_Edge	Any	Any	SNMP ICMP-PING Spooler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	Allow
5	Block Social Media	...VN	External	Any	Facebook Google+ Instagram Tinder Twitter	Any	Contractors Branch_Locations	Any	Block
6	o365 Access	Corporate_VN	External	lab-local/Domain Users	Any	HTTPS HTTP	Any	o365_Common o365_Exchange o365_SharePoint	Allow
7	SecureX Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	SecureX_Quarantined_IPs SecureX_Suspicious_IPs	Honeypot_Service	Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Quarantined_Systems	Honeypot_Service	Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow



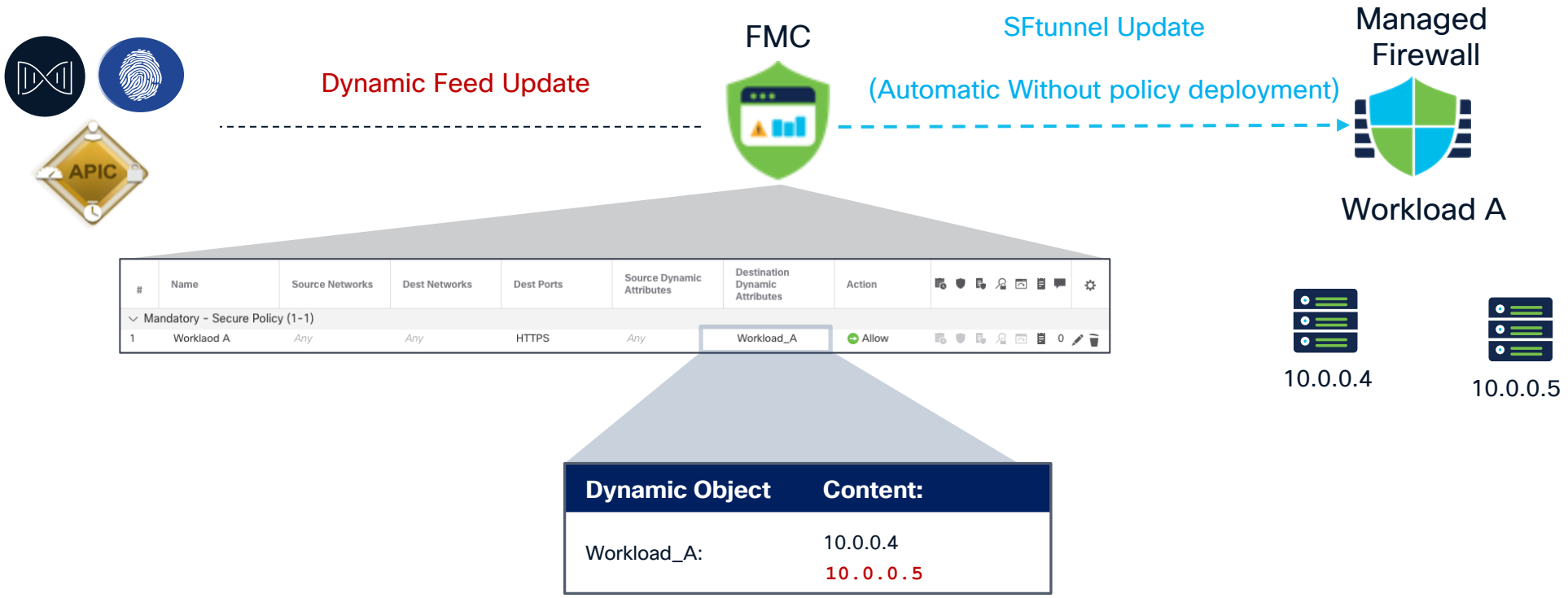




© 2025 Cisco and/or its affiliates. All rights reserved.

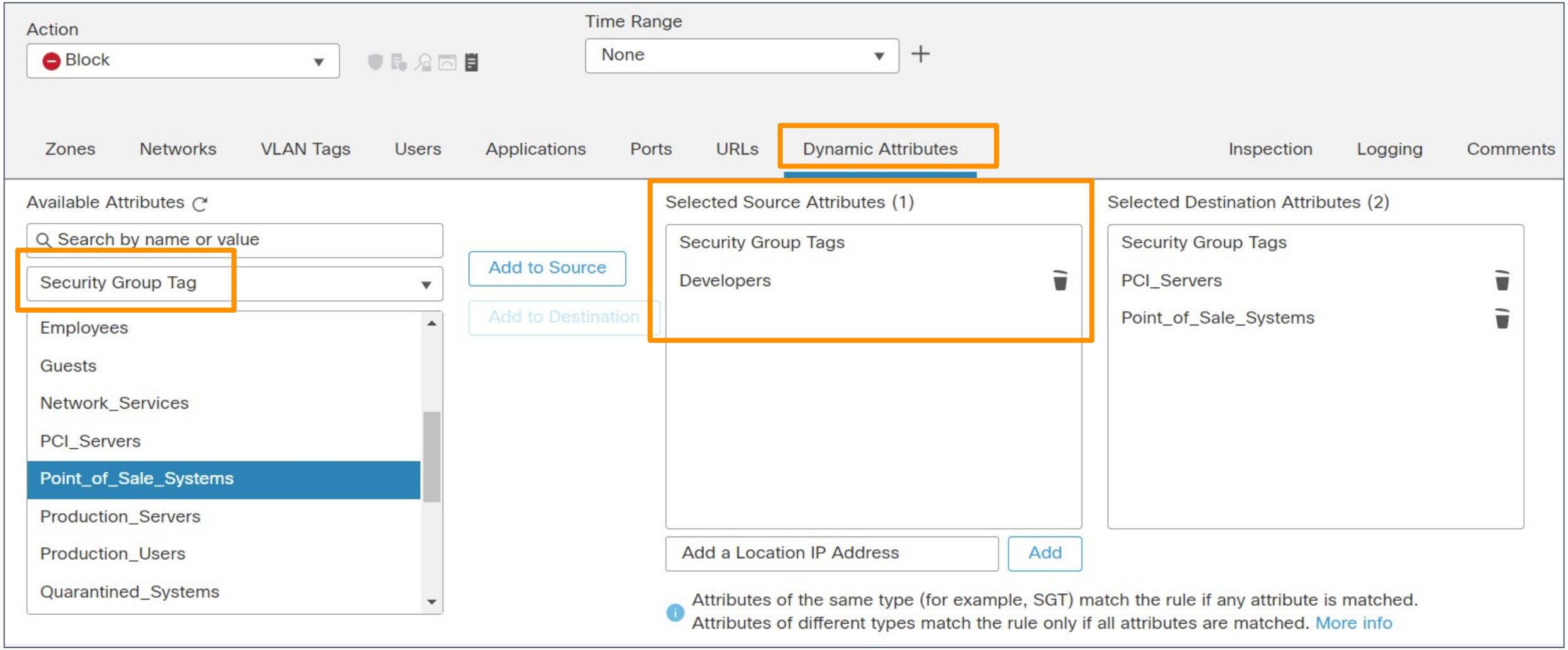
Dynamic Objects in action

Automatic without policy deployment



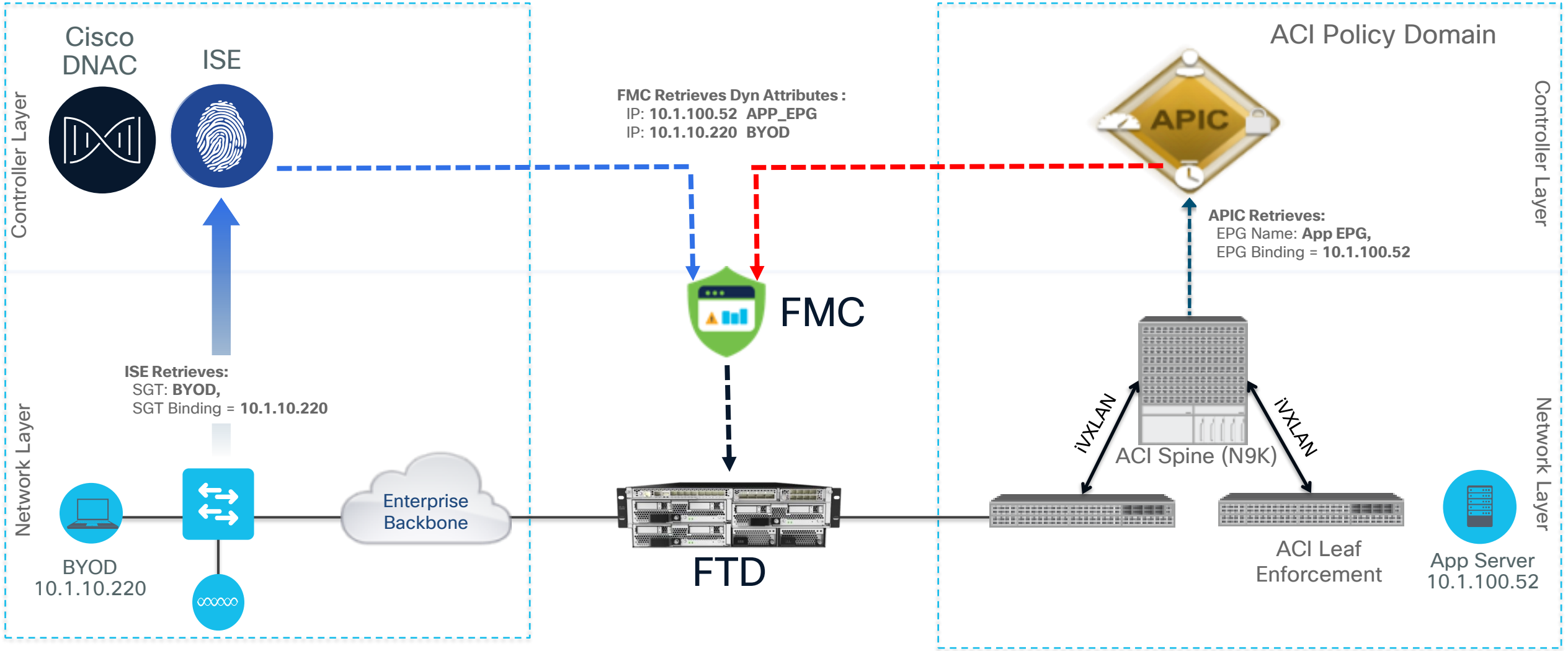
© 2025 Cisco and/or its affiliates. All rights reserved.

FTD and ASA can leverage SGTs



© 2025 Cisco and/or its affiliates. All rights reserved.

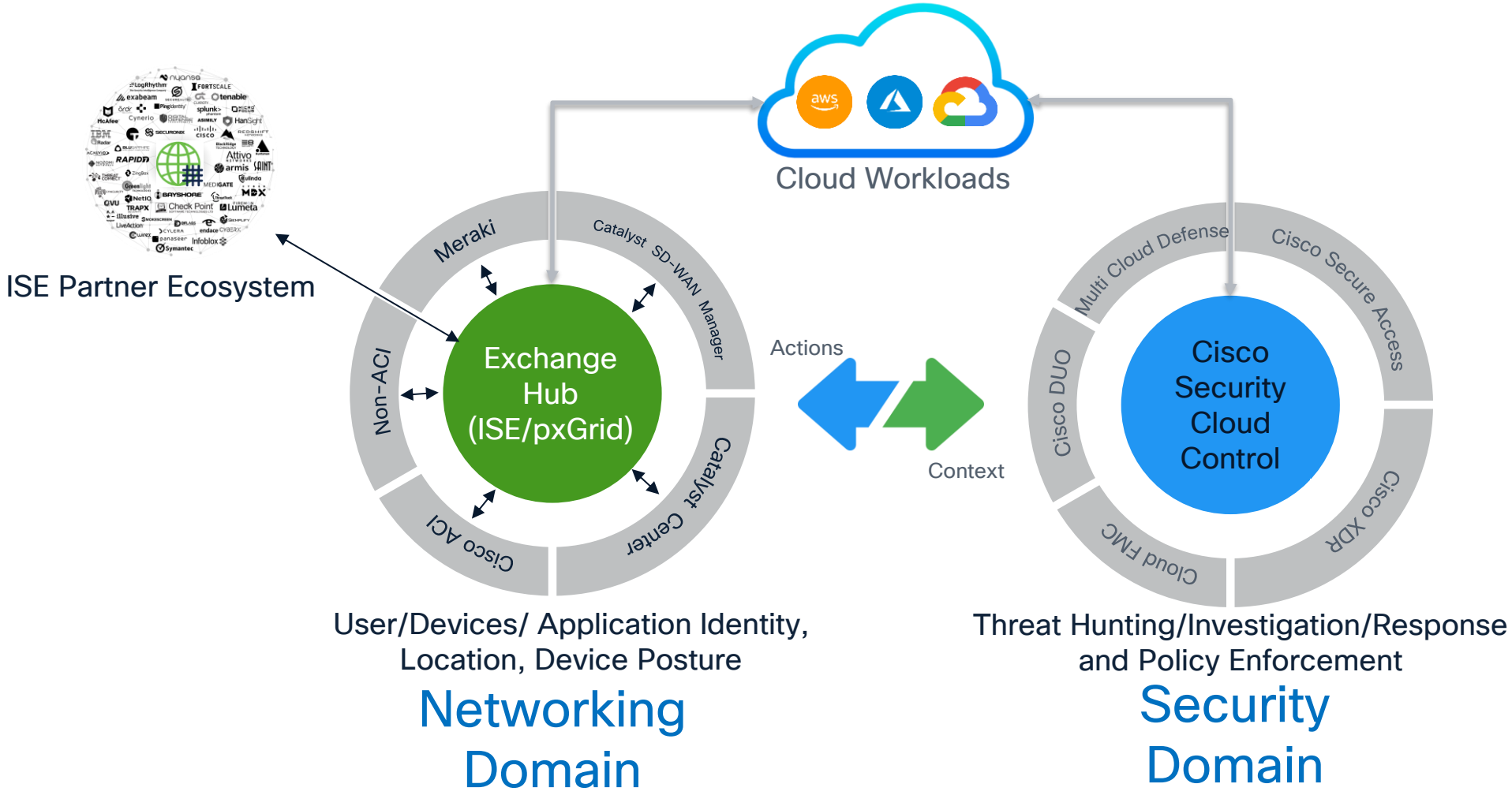
SGT/ACI Firepower Integration



© 2025 Cisco and/or its affiliates. All rights reserved.

Common policy for Cisco Networking Cloud

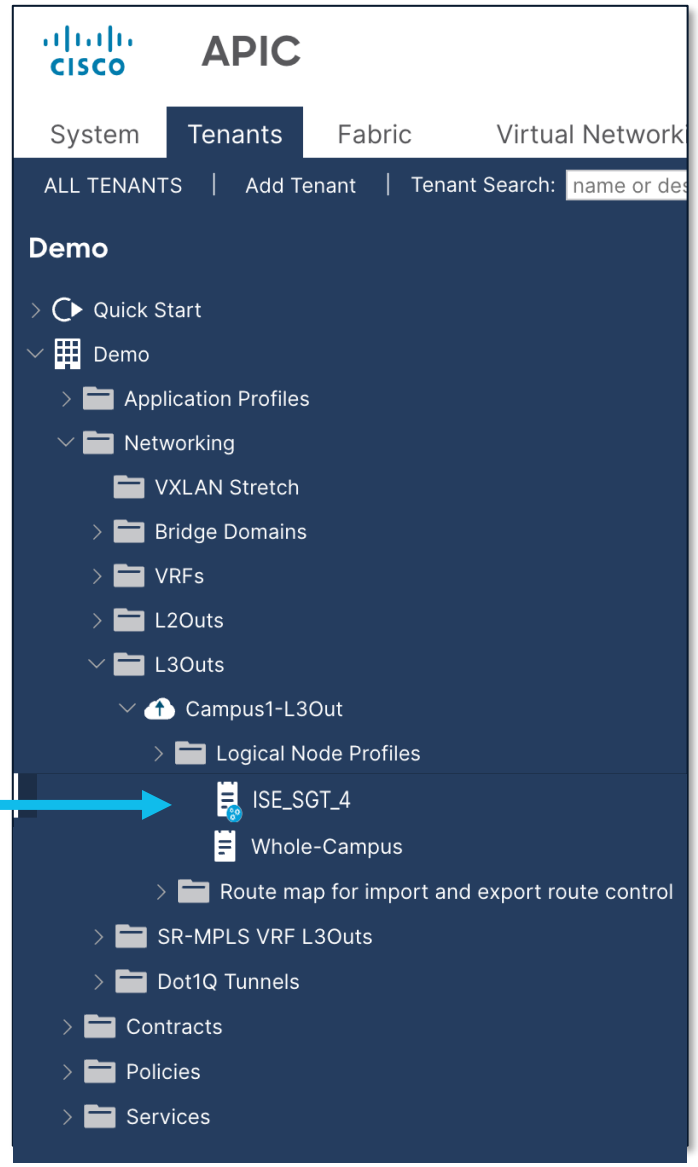
Normalizing and sharing context across domains



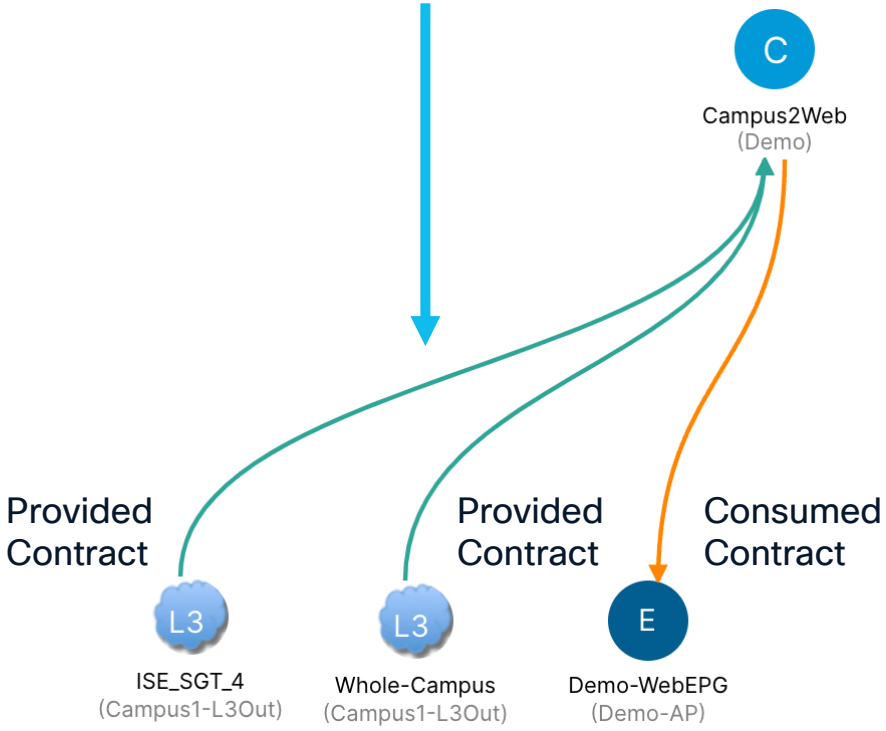
© 2025 Cisco and/or its affiliates. All rights reserved.

Context sent to ACI

SGT added as External EPG



Newly added Group attached to existing Contract in APIC:



© 2025 Cisco and/or its affiliates. All rights reserved.

Customer requirement

Implementing Zero Trust Micro Segmentation

© 2025 Cisco and/or its affiliates. All rights reserved.

Zero trust micro-segmentation...

- Where networking and security come together...
- Customer's current network design...
- Security control over inbound traffic...
- Understanding ACI security...
- Zero trust application-based security...
- Layer 7 security integration...
- DMZ redesign...
- Reducing operational complexity of segmentation
- **Implement Zero trust Micro-segmentation**

Cloud workload protection

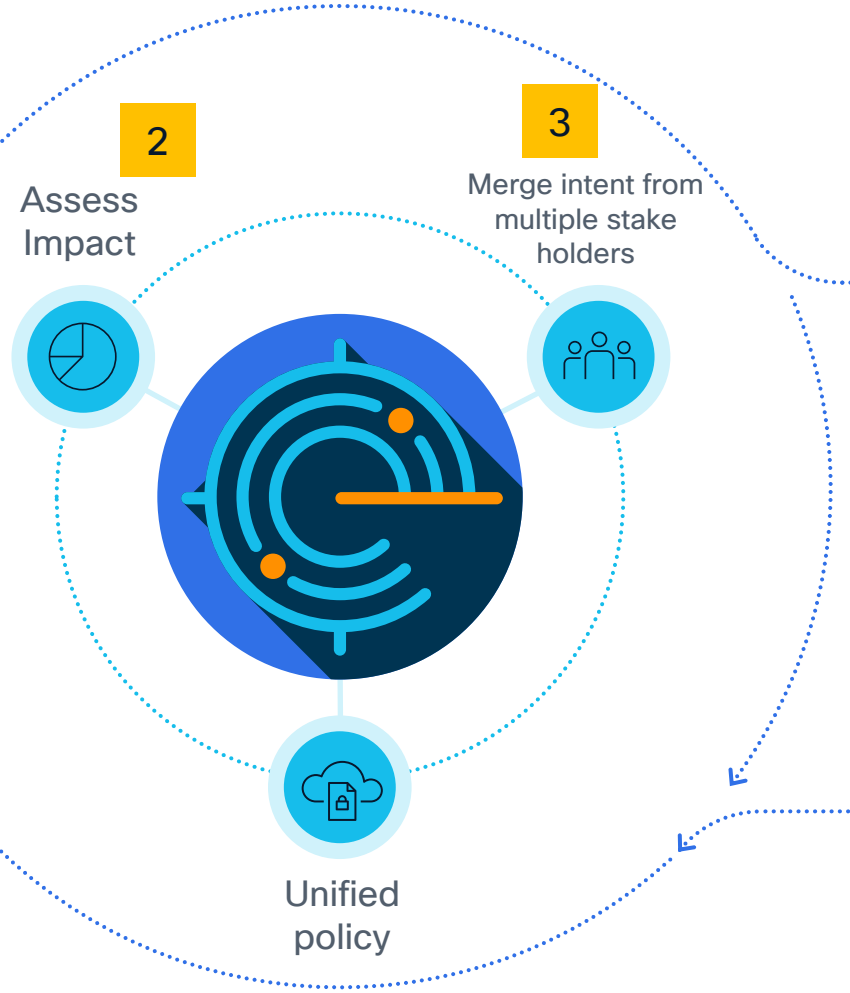
Dynamic attribute & behavior-based security policy and segmentation

1

Baseline workload protection posture

- Network communications
- Process behavior
- SW Vulnerabilities
- Application Insights

Baseline policy



Enforcement

4

Compliance alerts

5

- Threat Intel
- Policy violations
- Risk Reports

© 2025 Cisco and/or its affiliates. All rights reserved.

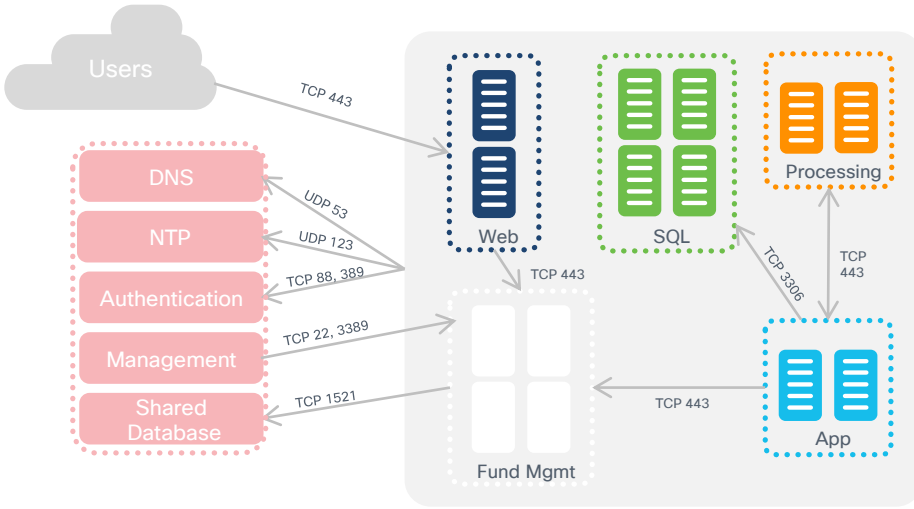
cisco

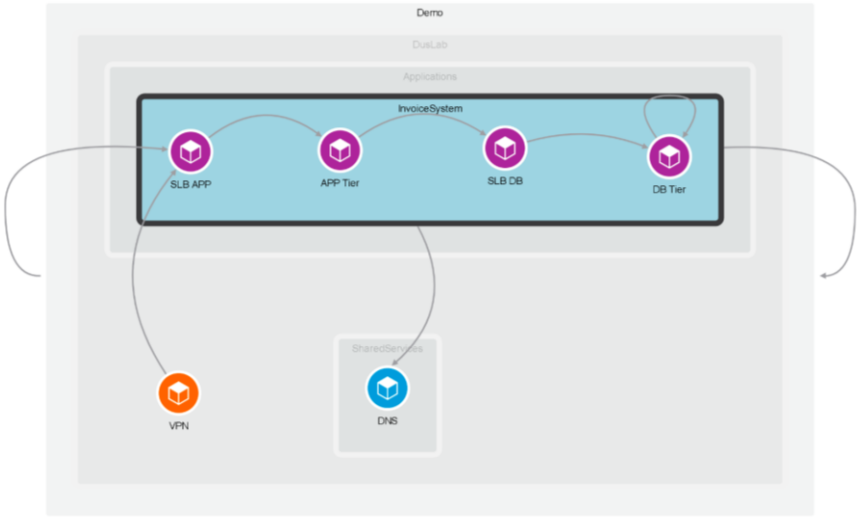
Understand your workloads

Automated discovery, clustering and policy generation

Baseline workload protection posture

- Network communications
- Process behaviour
- Labels



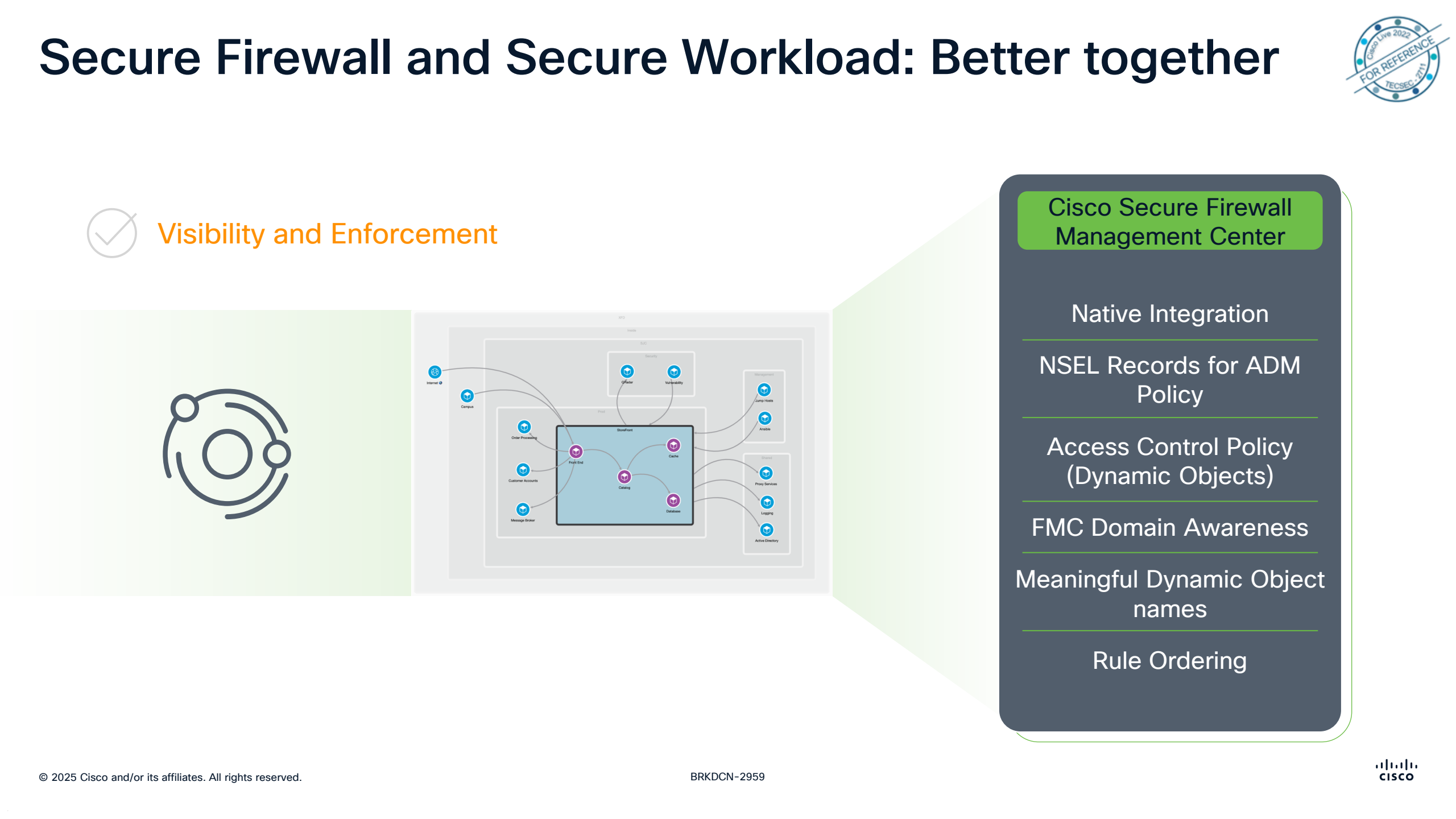


Absolute and Default Policies 13 | Catch All DENY | Grouped | Ungrouped

Rank	Priority	Action	Consumer	Provider	Protocols And Ports
Absolute	100	ALLOW	VPN	SLB APP	TCP : 1936
Default	100	ALLOW	VPN	SLB APP	TCP : 80 (HTTP)
Default	100	ALLOW	SLB DB	DB Tier	TCP : 3306 (MySQL)
Default	100	ALLOW	SLB APP	APP Tier	TCP : 8081
Default	100	ALLOW	Demo : DusLab : Applications : InvoiceSystem	Demo	UDP : 123 (NTP) ...2 more
Default	100	ALLOW	Demo : DusLab : Applications : InvoiceSystem	Demo : DusLab : SharedServices : DNS	UDP : 53 (DNS) ...1 more

© 2025 Cisco and/or its affiliates. All rights reserved.

Secure Firewall and Secure Workload: Better together



Visibility and Enforcement

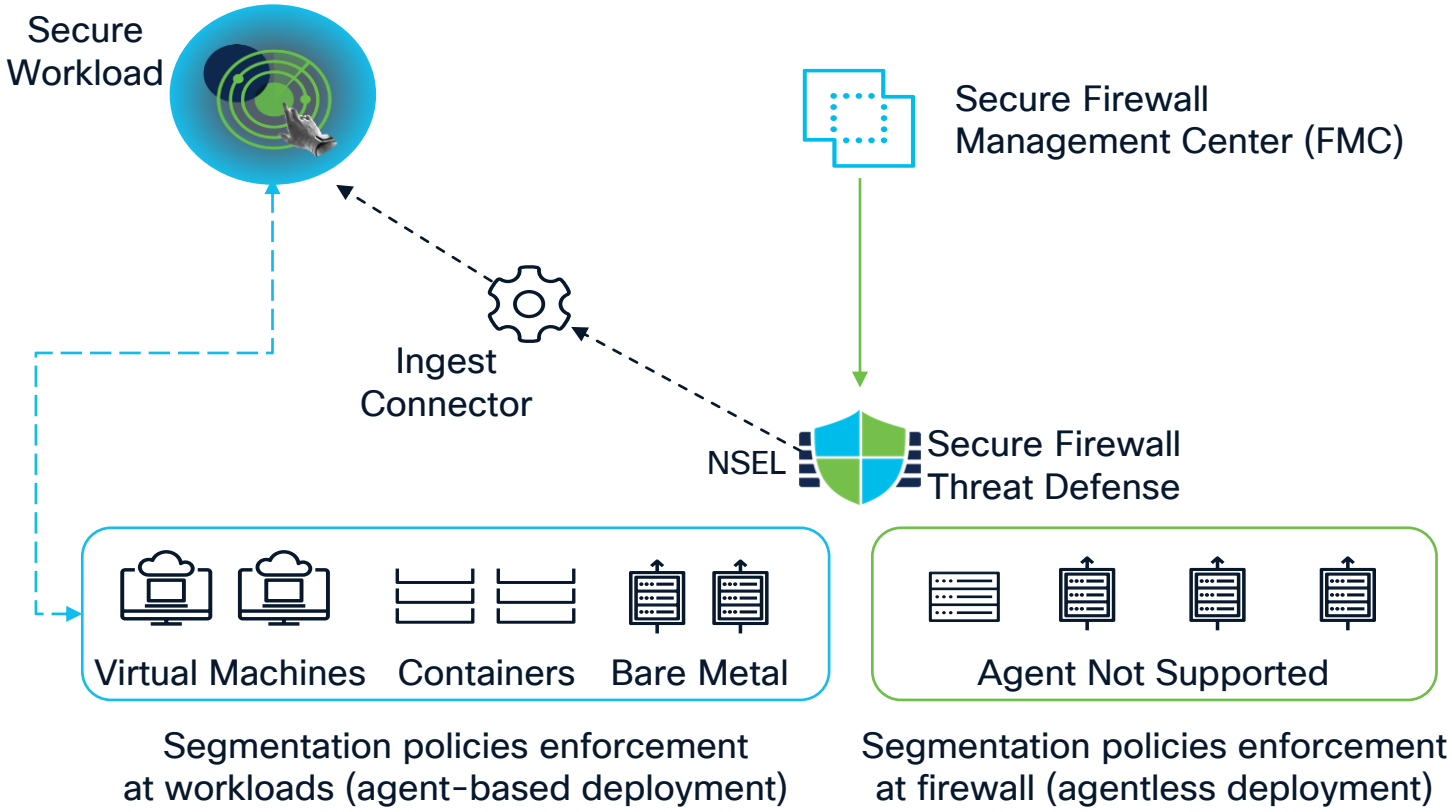
Cisco Secure Firewall Management Center

- Native Integration
- NSEL Records for ADM Policy
- Access Control Policy (Dynamic Objects)
- FMC Domain Awareness
- Meaningful Dynamic Object names
- Rule Ordering

© 2025 Cisco and/or its affiliates. All rights reserved.

CSW-FMC Integration and Enforcement

Defense-in-depth Use Case

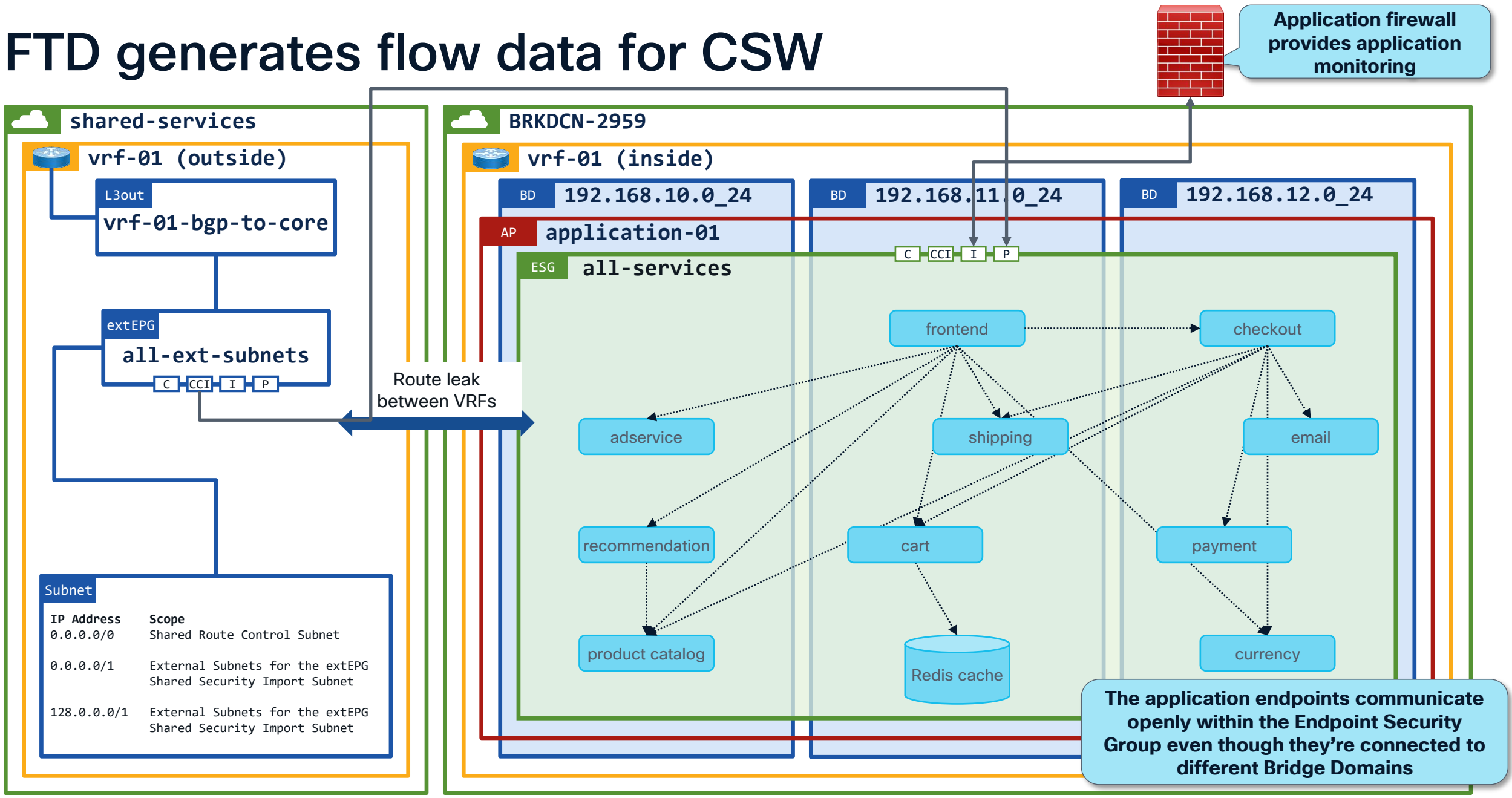


- Defense in depth
- Support access control policy and dynamic object
- Improved rule ordering
- FMC domain awareness
- Topology aware policy enforcement
- Support deployment across multicloud

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

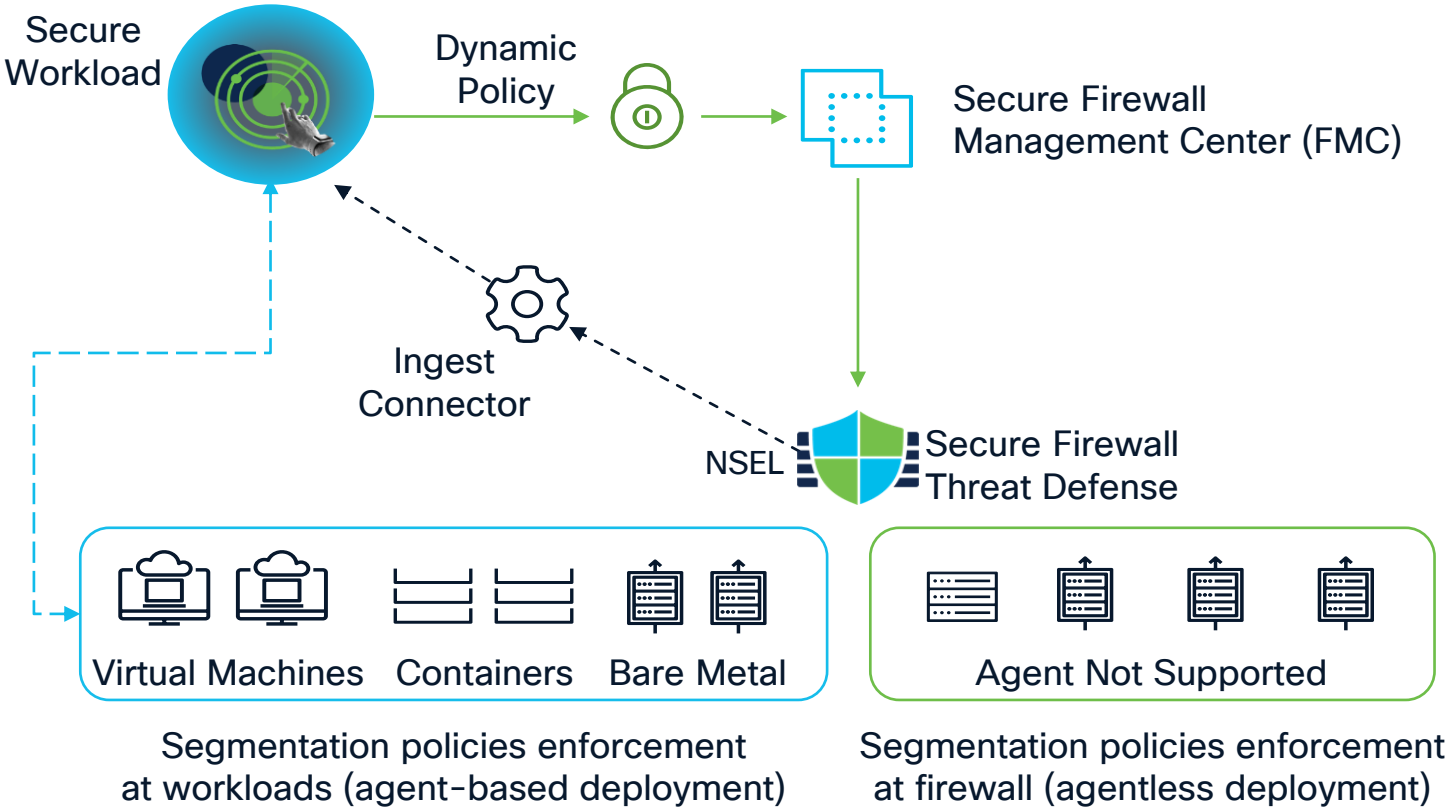
FTD generates flow data for CSW



© 2025 Cisco and/or its affiliates. All rights reserved.

CSW-FMC Integration And Enforcement

Defense-in-depth Use Case

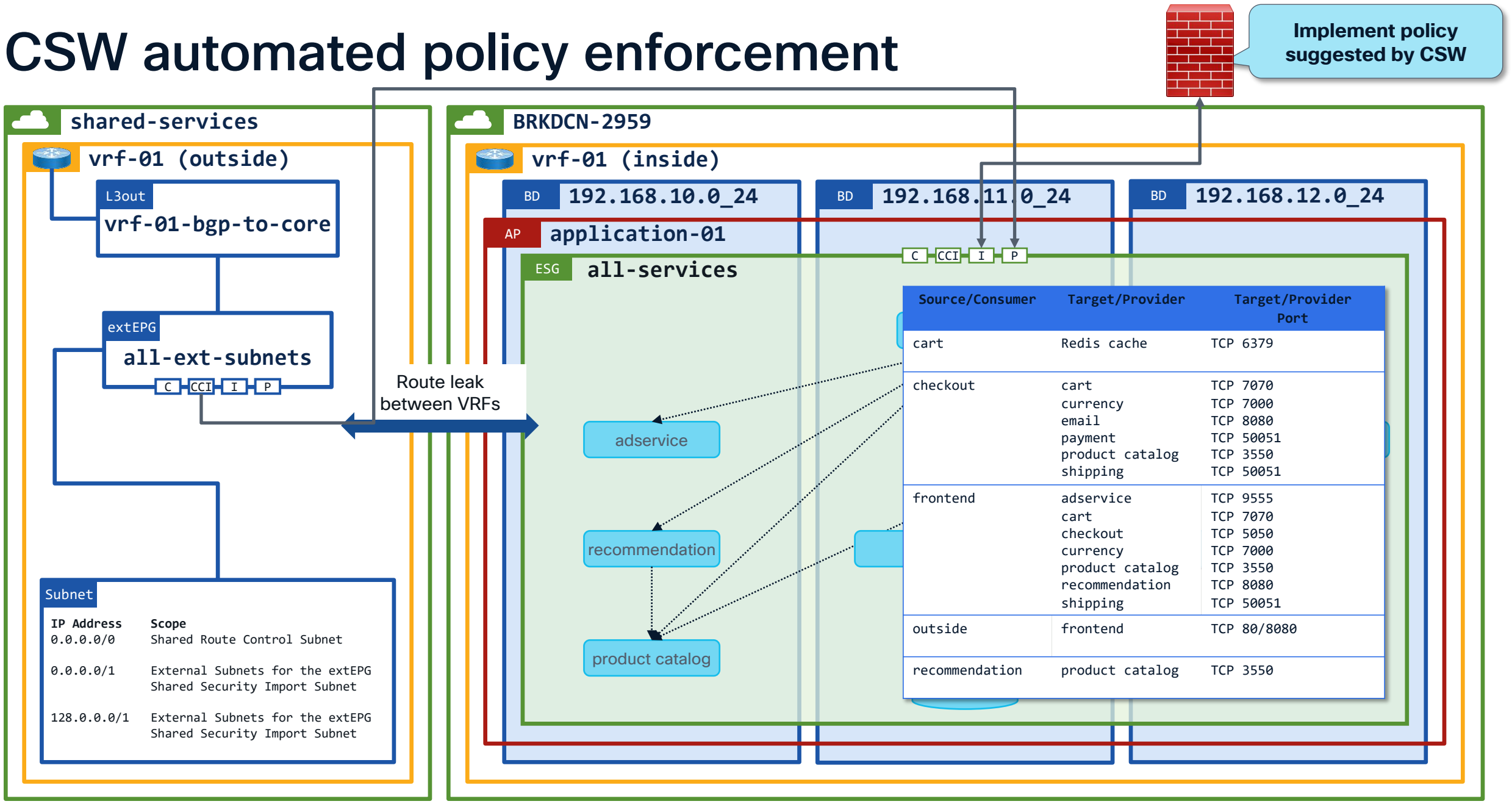


- Defense in depth
- Support access control policy and dynamic object
- Improved rule ordering
- FMC domain awareness
- Topology aware policy enforcement
- Support deployment across multicloud

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

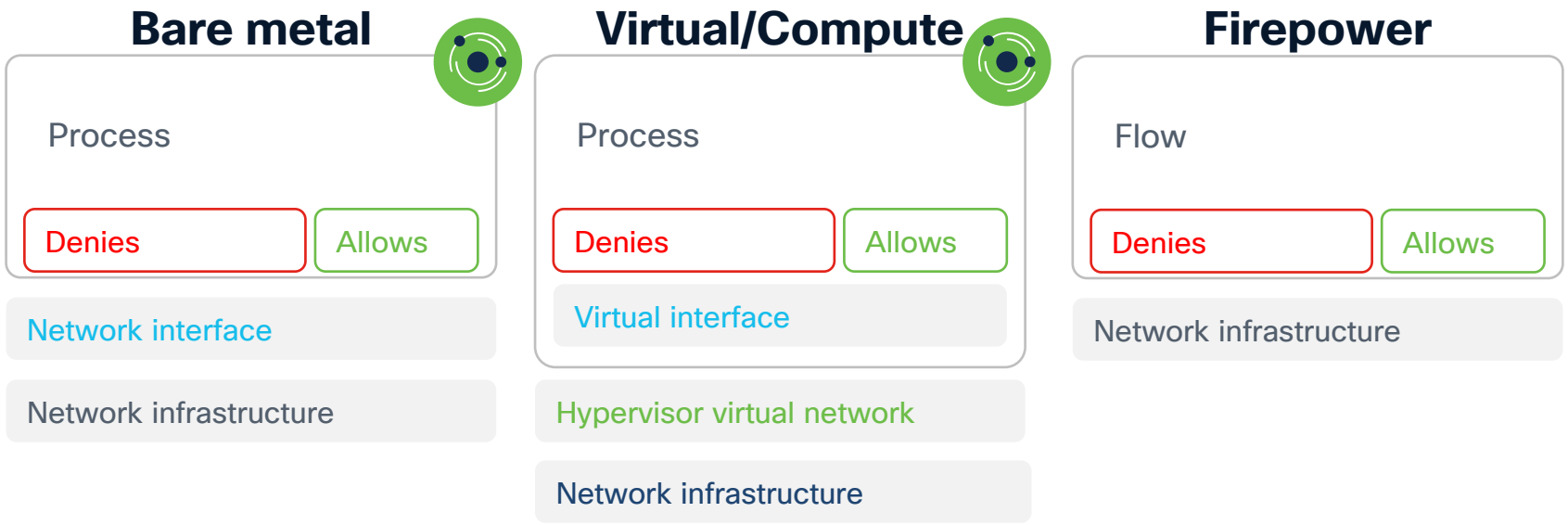
CSW automated policy enforcement



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

How does CSW enforce the policy ?

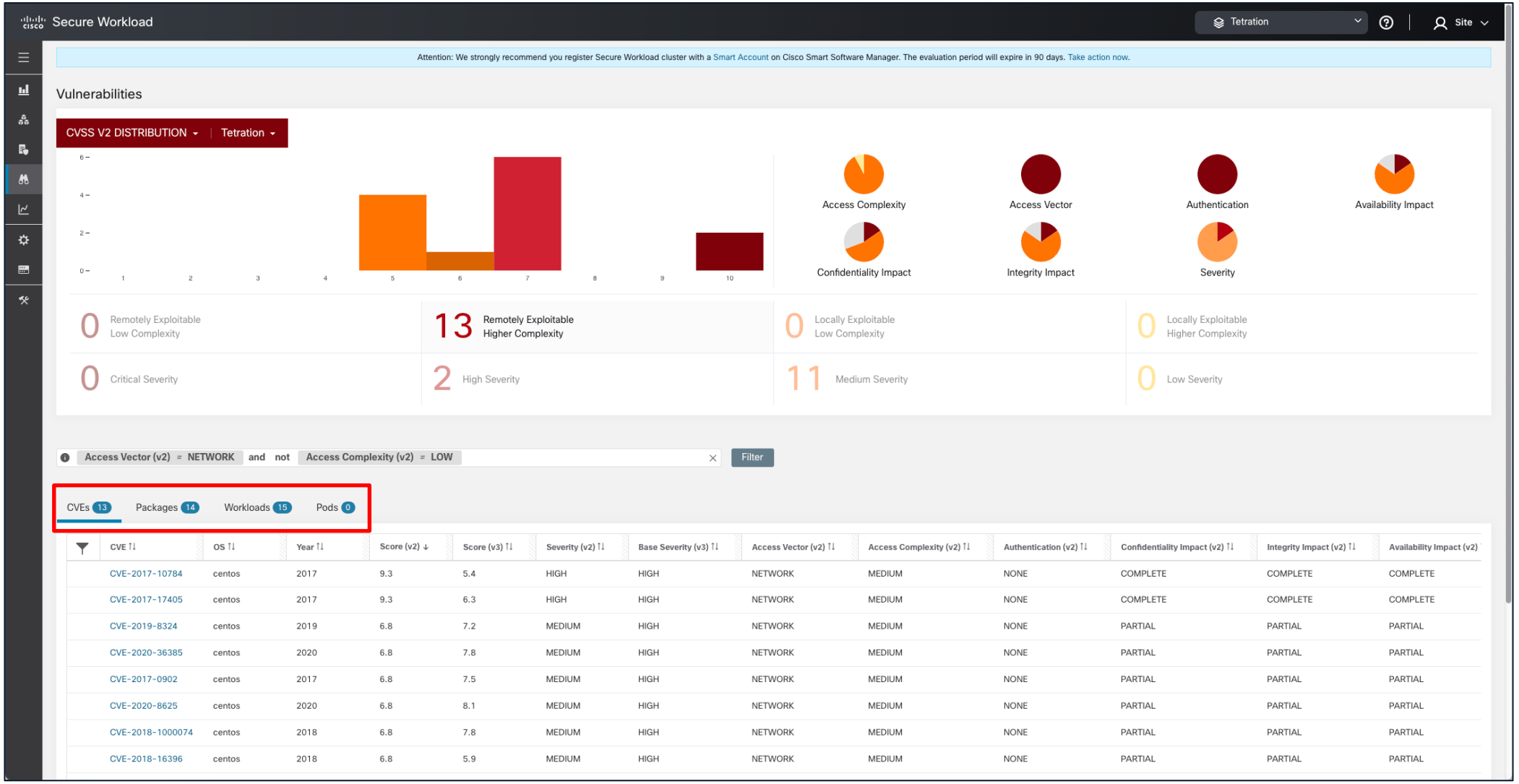


Intent is rendered as security rules in native environment

- IP sets on Linux servers
- Windows Advanced Firewall or Windows Filtering Platform on Windows servers
- Access Policies in Firepower Threat Defense

© 2025 Cisco and/or its affiliates. All rights reserved.

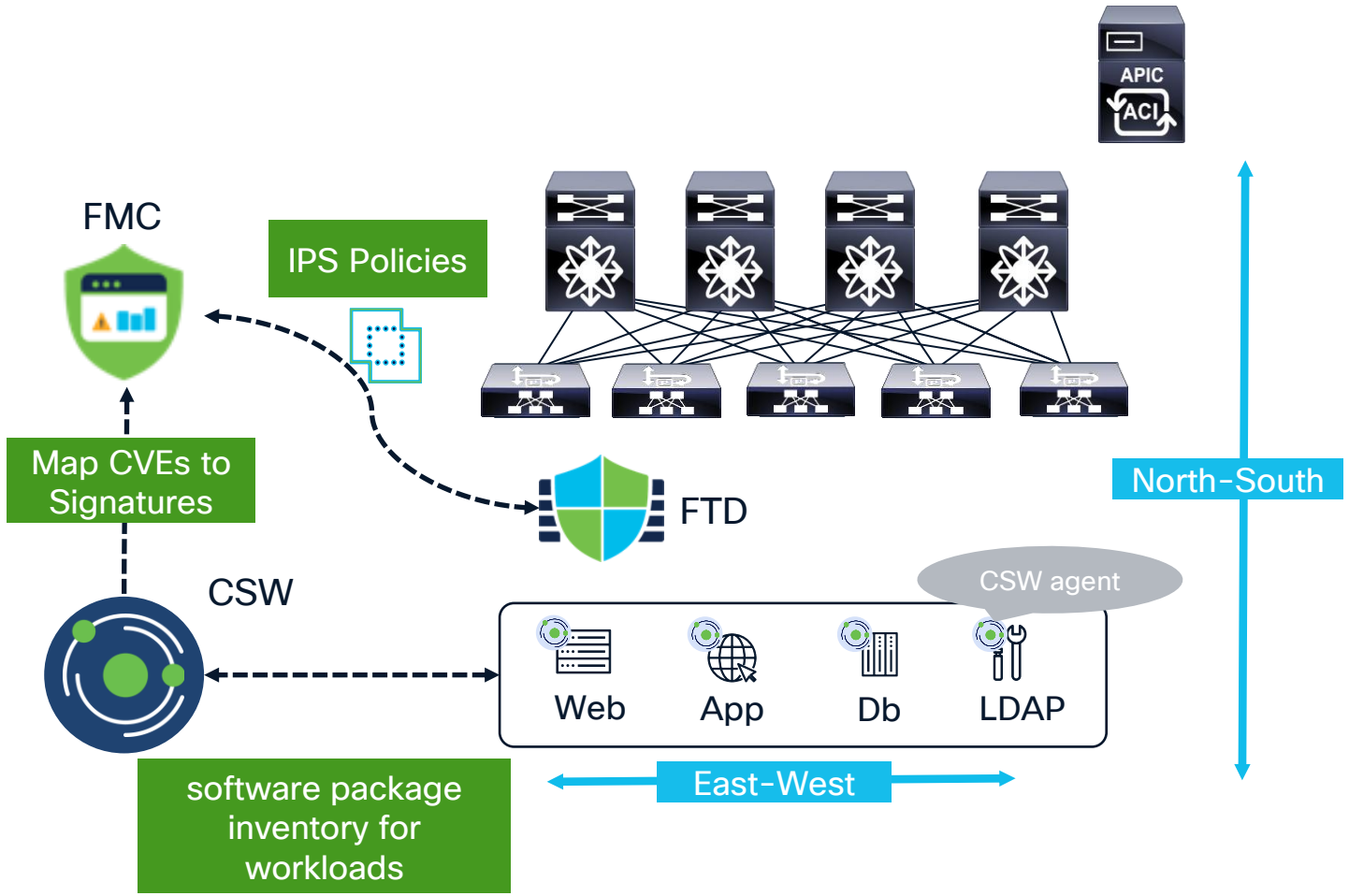
Cisco Secure Workload



CVE	OS	Year	Score (v2)	Score (v3)	Severity (v2)	Base Severity (v3)	Access Vector (v2)	Access Complexity (v2)	Authentication (v2)	Confidentiality Impact (v2)	Integrity Impact (v2)	Availability Impact (v2)
CVE-2017-10784	centos	2017	9.3	5.4	HIGH	HIGH	NETWORK	MEDIUM	NONE	COMPLETE	COMPLETE	COMPLETE
CVE-2017-17405	centos	2017	9.3	6.3	HIGH	HIGH	NETWORK	MEDIUM	NONE	COMPLETE	COMPLETE	COMPLETE
CVE-2019-8324	centos	2019	6.8	7.2	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL
CVE-2020-36385	centos	2020	6.8	7.8	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL
CVE-2017-0902	centos	2017	6.8	7.5	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL
CVE-2020-8625	centos	2020	6.8	8.1	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL
CVE-2018-1000074	centos	2018	6.8	7.8	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL
CVE-2018-16396	centos	2018	6.8	5.9	MEDIUM	HIGH	NETWORK	MEDIUM	NONE	PARTIAL	PARTIAL	PARTIAL

© 2025 Cisco and/or its affiliates. All rights reserved.

Virtual patching – Cisco Secure Firewall

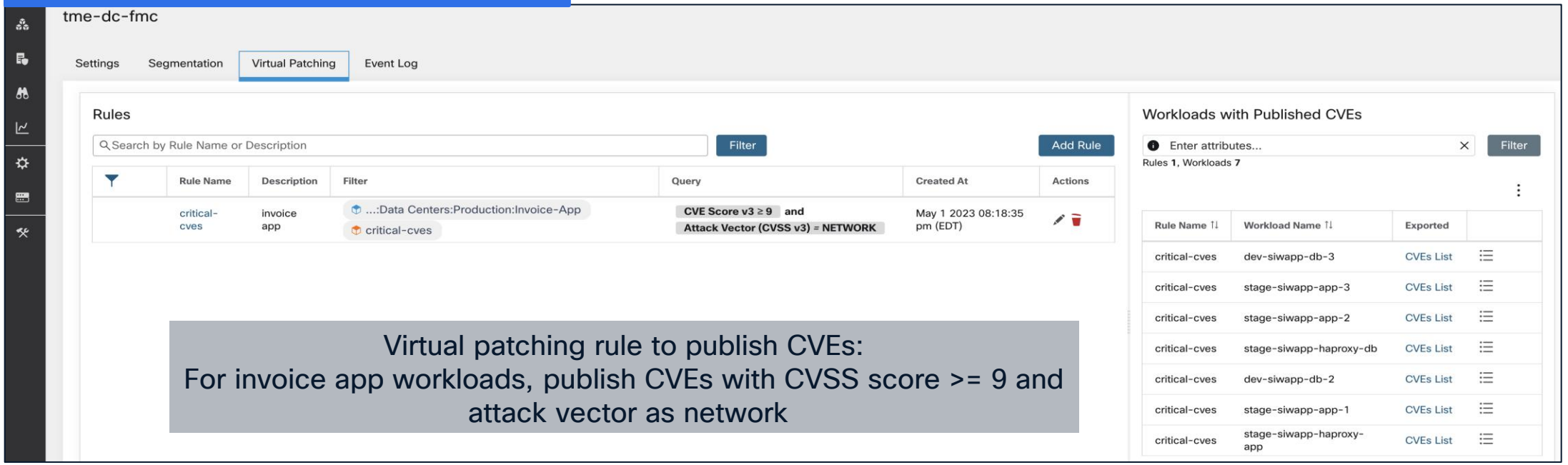


- Secure Workload agents collects CVE data from workloads
- Publish specific CVE data to Firewall Management Center
- Use Firewall recommendations to generate precise IPS policy
- Apply precise IPS policy to protect against CVE exploits

© 2025 Cisco and/or its affiliates. All rights reserved.

Virtual patching – Cisco Secure Firewall

CSW: Manage > Connector > FMC > Virtual Patching



Virtual patching rule to publish CVEs:
For invoice app workloads, publish CVEs with CVSS score >= 9 and attack vector as network

FMC: Analysis > Hosts > Third party vulnerabilities

Vulnerability Source	Vulnerability ID	IP Address	Port	Bugtraq ID	CVE ID	SVID	Snort ID	Title	Description
CSW|d5341dbb-4b4f-31f8-5845-111fb6fbc537|1	2000042	192.168.18.7			2022-1271	12936	300301	2022-1271	CSW-3.8.0.29.devel, 20230502030004Z
CSW|d5341dbb-4b4f-31f8-5845-111fb6fbc537|1	2000073	192.168.18.6			2022-1271	12936	300301	2022-1271	CSW-3.8.0.29.devel, 20230502030004Z
CSW|d5341dbb-4b4f-31f8-5845-111fb6fbc537|1	2000117	192.168.17.10			2022-1271	12936	300301	2022-1271	CSW-3.8.0.29.devel, 20230502030005Z
CSW|d5341dbb-4b4f-31f8-5845-111fb6fbc537|1	2000052	192.168.16.7			2022-1271	12936	300301	2022-1271	CSW-3.8.0.29.devel, 20230502030004Z
CSW|d5341dbb-4b4f-31f8-5845-111fb6fbc537|1	2000027	192.168.16.6			2022-1271	12936	300301	2022-1271	CSW-3.8.0.29.devel, 20230502030004Z
CSW|d5341dbb-4b4f-31f8-5845-111fb6fbc537|1	2000116	192.168.16.5			2022-1271	12936	300301	2022-1271	CSW-3.8.0.29.devel, 20230502030005Z
CSW|d5341dbb-4b4f-31f8-5845-111fb6fbc537|1	2000089	192.168.15.10			2022-1271	12936	300301	2022-1271	CSW-3.8.0.29.devel, 20230502030005Z

© 2025 Cisco and/or its affiliates. All rights reserved.

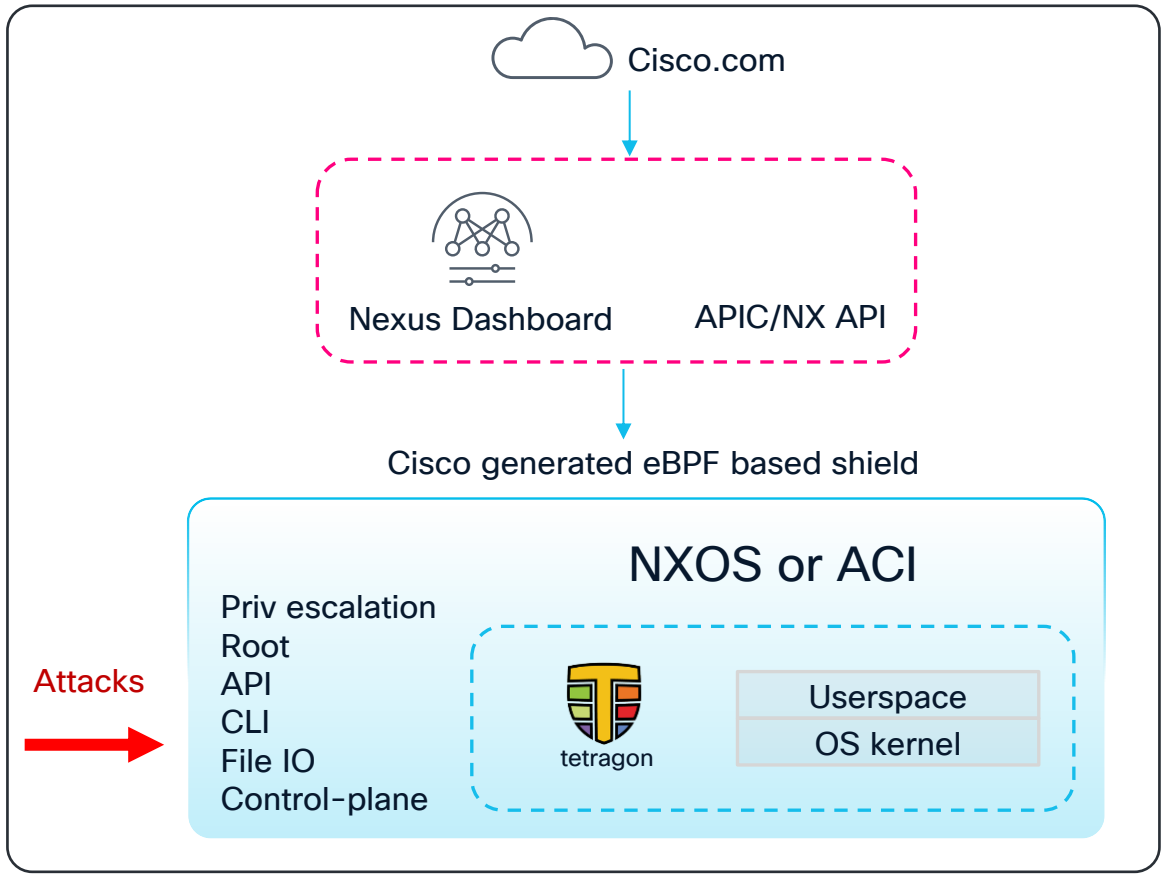
Live Protect

CVE Mitigation for Nexus Switches

Data Center is critical infrastructure:
- PSIRTs require large switch fleet upgrades (100s-1000s)
- Require testing, planning, multiple maintenance windows
- High cumulative downtime - high MTTR

Live Protect workflow:
- Download compensating controls from cisco.com
- Tetragon agent applies eBPF policy CVE shields
  - Monitor mode
  - Enforce mode

Benefits:
- CVE mitigation with no downtime
- Upgrades during regular maintenance window

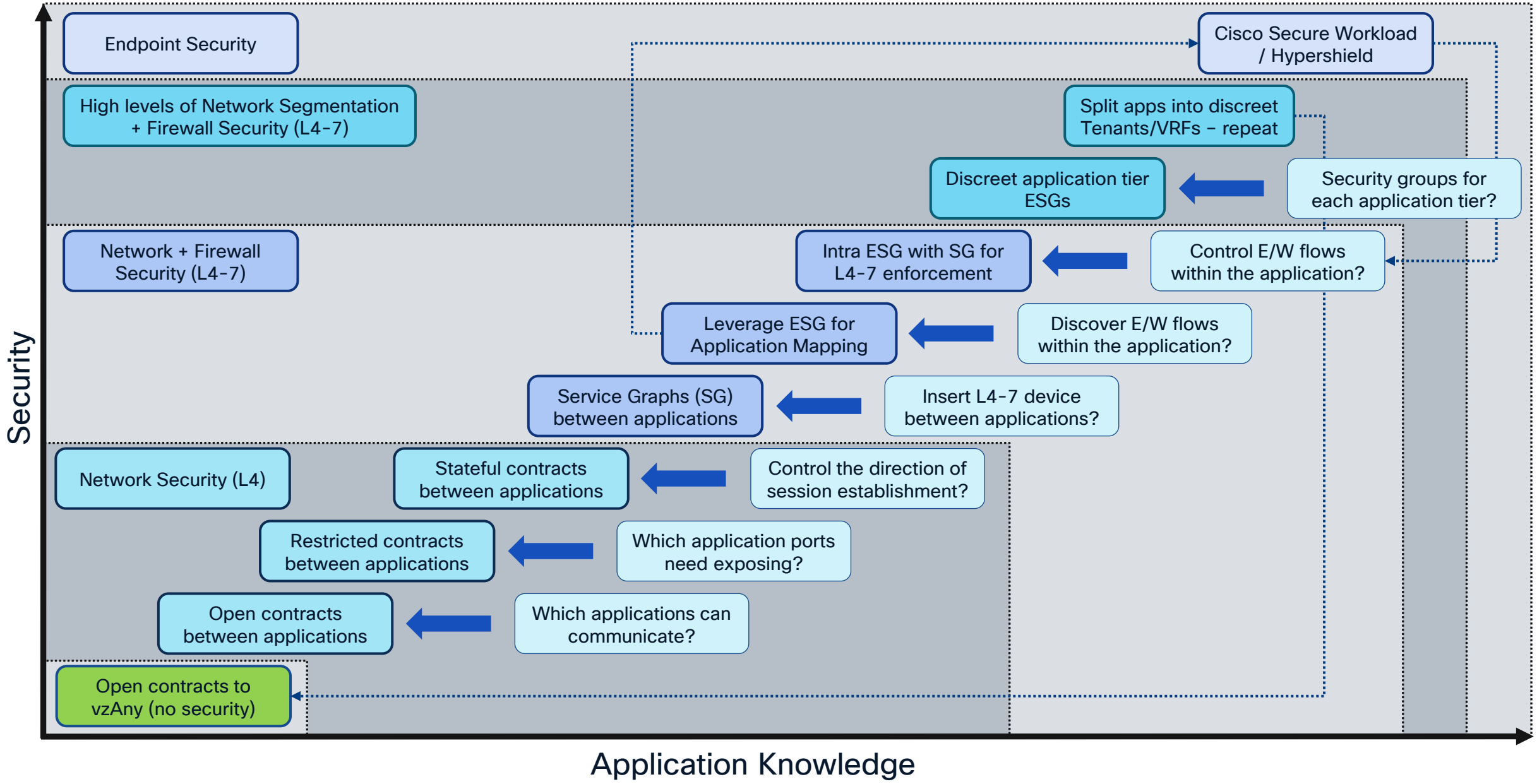


Live Protect Roadmap

Shipping NXOS 10.6(1)	Nov 2025 NXOS 10.6(2)	April 2026 NXOS 10.6(3)	July 2026 ACI 6.2(3)
Observability policy CloudScale	Privilege escalation CloudScale & S1	Network control CloudScale & S1 (Planning)	Live Protect (Planning)

© 2025 Cisco and/or its affiliates. All rights reserved.

Wrapping up...



© 2025 Cisco and/or its affiliates. All rights reserved.

Key takeaway’s

1. Make your life easy, automate and leverage automated automation
2. EPGs and ESGs (preferred) provide both security **and** workload visibility
3. Security can be implemented in different places – network fabric, firewalls, and workloads
4. Application knowledge is key to achieve zero trust micro segmentation
5. Provide flexible application security responses
6. A more secure network can be an evolution rather than a revolution

© 2025 Cisco and/or its affiliates. All rights reserved.

Complete your session evaluations

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

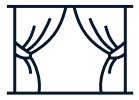
Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

© 2025 Cisco and/or its affiliates. All rights reserved.

Continue your education



Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

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

Contact me at: fgandola@cisco.com, ssharman@cisco.com

© 2025 Cisco and/or its affiliates. All rights reserved.

Thank you

CISCO