

Cisco ACI EPGs vs. ESGs: Comparison and Use Cases for Each

cisco Live !

Joe Rinehart
Content Advocate, Data Center & AI
CCIE #14256
@jjrinehart

Cisco Webex App

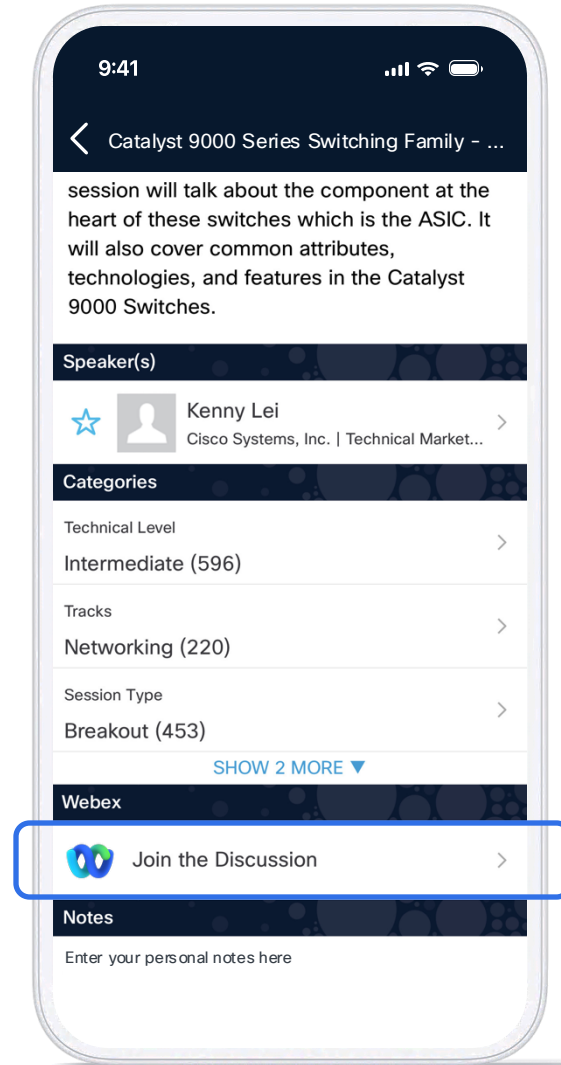
Questions?

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 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#CISCOU-2652>

Agenda

- 01 Introduction
- 02 Review of Endpoint Groups (EPGs)
- 03 Overview of Endpoint Security Groups (ESGs)
- 04 EPGs and ESGs Side by Side
- 05 Use Cases
- 06 Conclusion

Introduction

Introduction

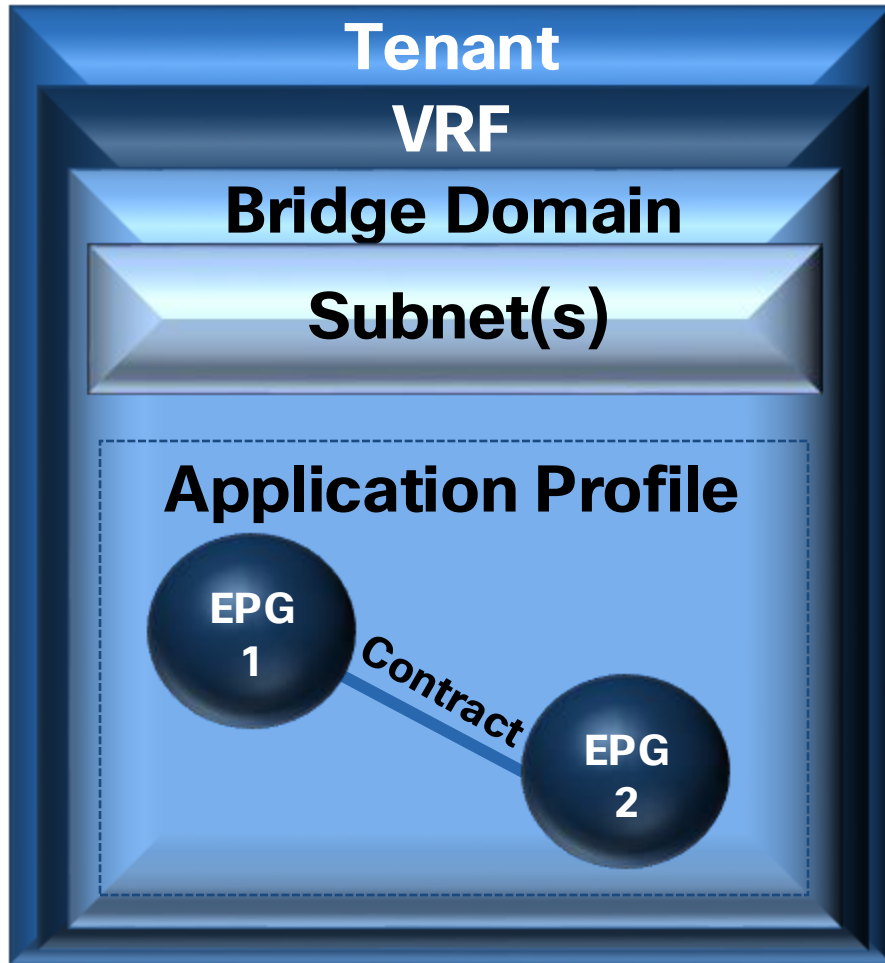
Some Thoughts

- The basic security model for ACI has not changed much since it was introduced
- EPGs and contract relationships can get complex over time
- Cisco introduced Endpoint Security Groups (ESGs) in ACI code 5.0(1)
- Questions come up often about how EPGs and ESGs differ
- This session will provide a brief overview of each and clarify which work better in which situations (use cases)

Review of Endpoint Groups (EPGs)

Review of Endpoint Groups (EPGs)

What Is An Endpoint Group?

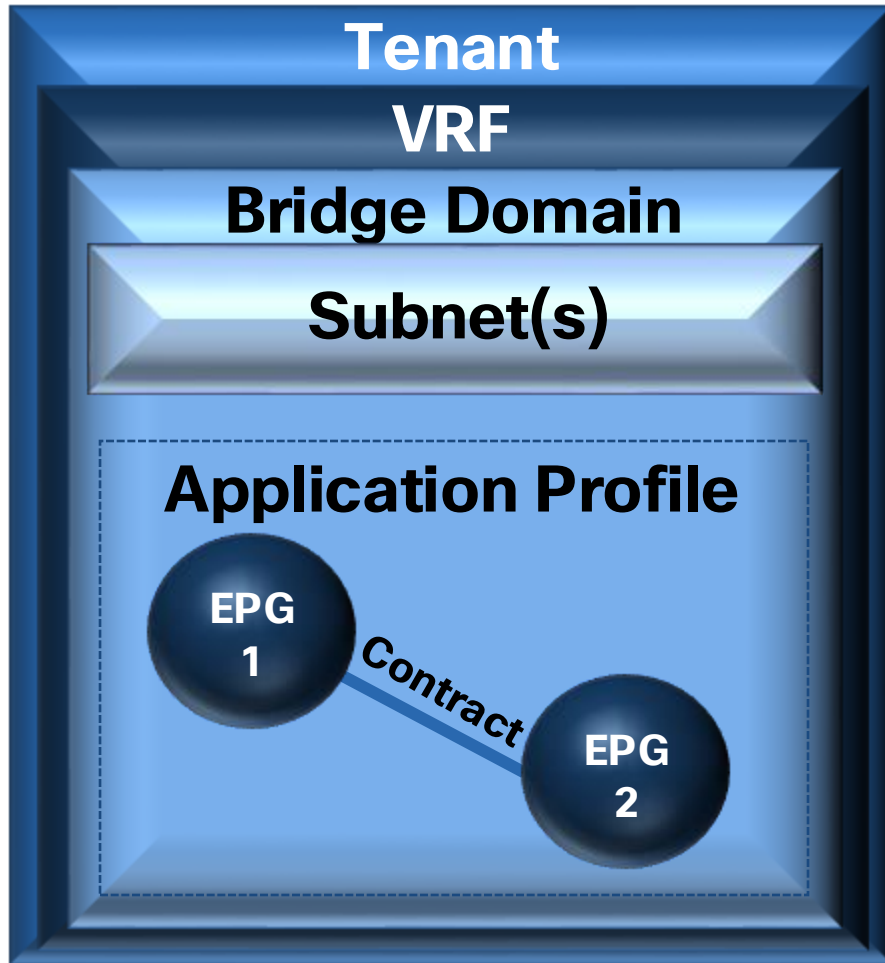


- ACI uses a hierarchy of logical constructs to organize network resources:
 - **Tenant**
 - **VRF**
 - **Bridge Domain**
 - **Subnet(s)**
 - **Application Profile**
 - **Endpoint Groups:**
 - **Endpoints:** Physical or virtual device represented by a MAC and IP address.*
 - **Endpoint Groups:** Collection of endpoints with similar connections and/or policies

** While most endpoints will have an IP address there are some cases where they may not*

Review of Endpoint Groups (EPGs)

Key Aspects of EPGs



- **Membership:**

- EPGs belong to only **one** bridge domain, and by extension, one VRF and tenant

- **Connectivity:**

- EPGs map to a single external VLAN (network centric mode)
- Physical mapping of EPGs are static or dynamic

- **Communication:**

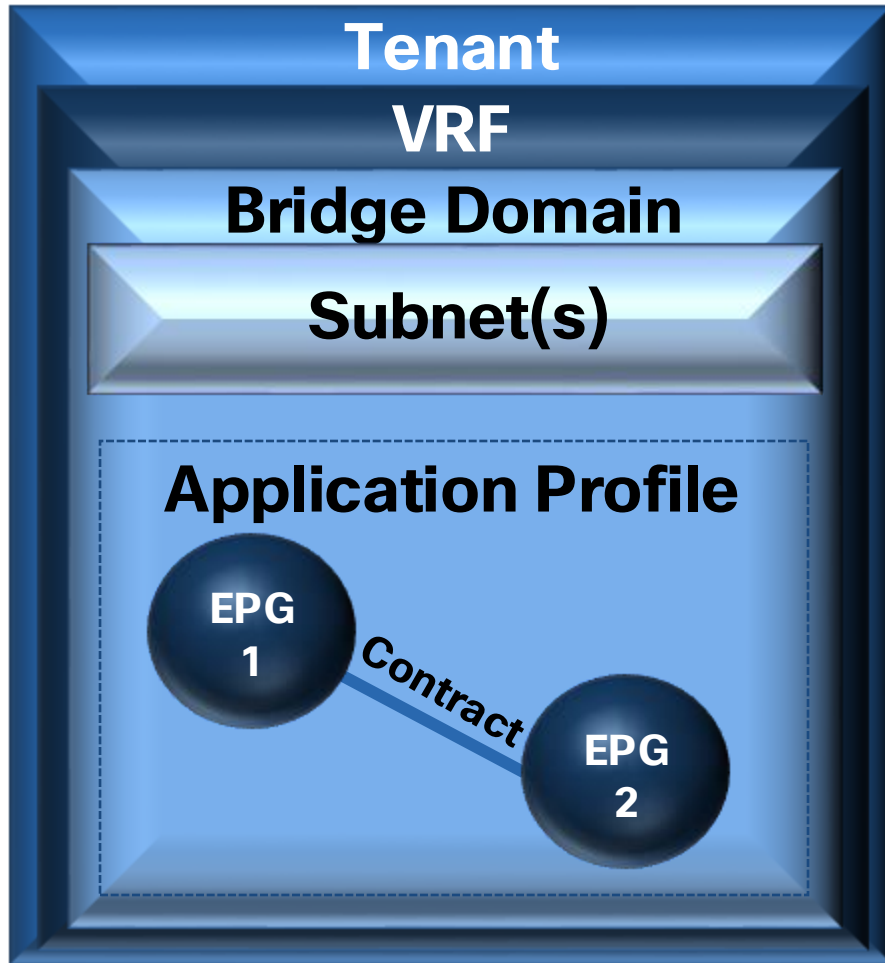
- Traffic within an EPG is permitted by default
- Traffic between EPGs requires a contract (not permitted by default)

- **Feature Availability:**

- EPGs have been supported since ACI 1.0

Review of Endpoint Groups (EPGs)

Key Aspects of EPGs



- **Functionality:**

- Combines **forwarding** and **security segmentation**.
- Requires contracts for inter-EPG communication.
- Used for VLAN bindings and network configurations.

DEMO: Contract Setup & Testing with EPGs





Sales



> Quick Start

> Sales

- > Application Profiles
- > Networking
- > Contracts
- > Policies
- > Services
- > Security (Beta)

Tenant - Sales



Summary

Dashboard

Policy

Operational

Stats

Health

Faults

History



Application EPGs

3
Total



0

100



Endpoint Security Groups

0
Total



Bridge Domains

2
Total



0

100



VRFs

1
Total



0

100



L2Outs

0
Total



L3Outs

1
Total



0

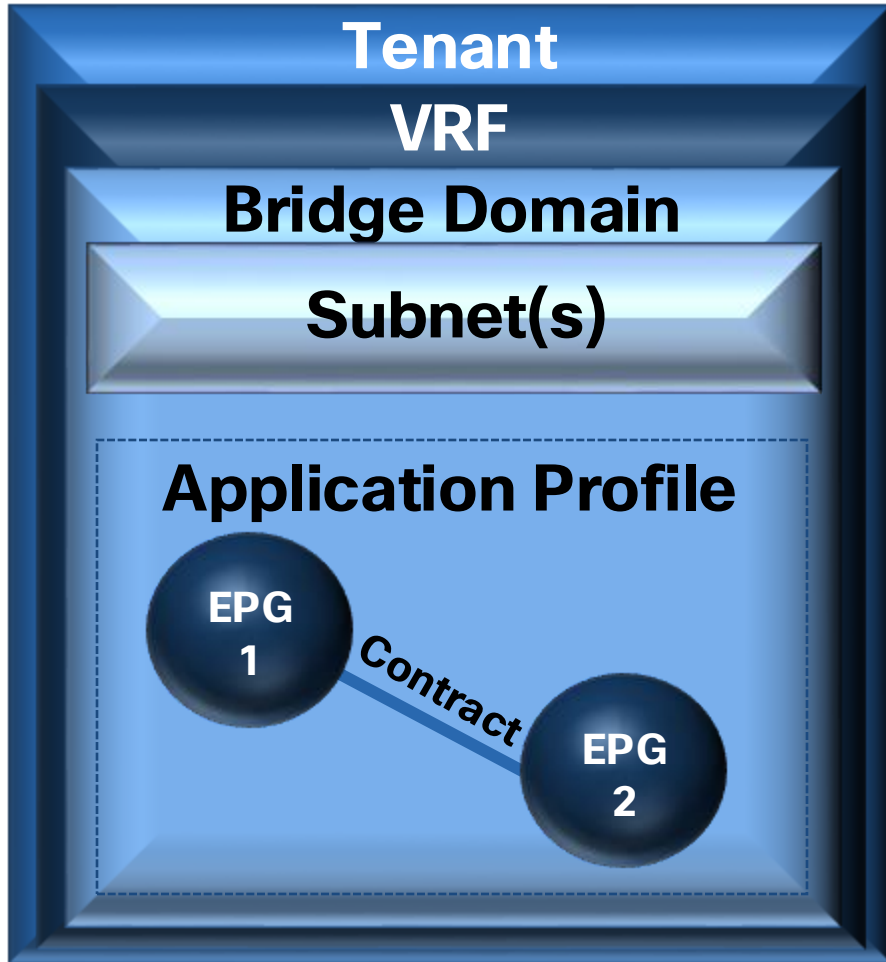
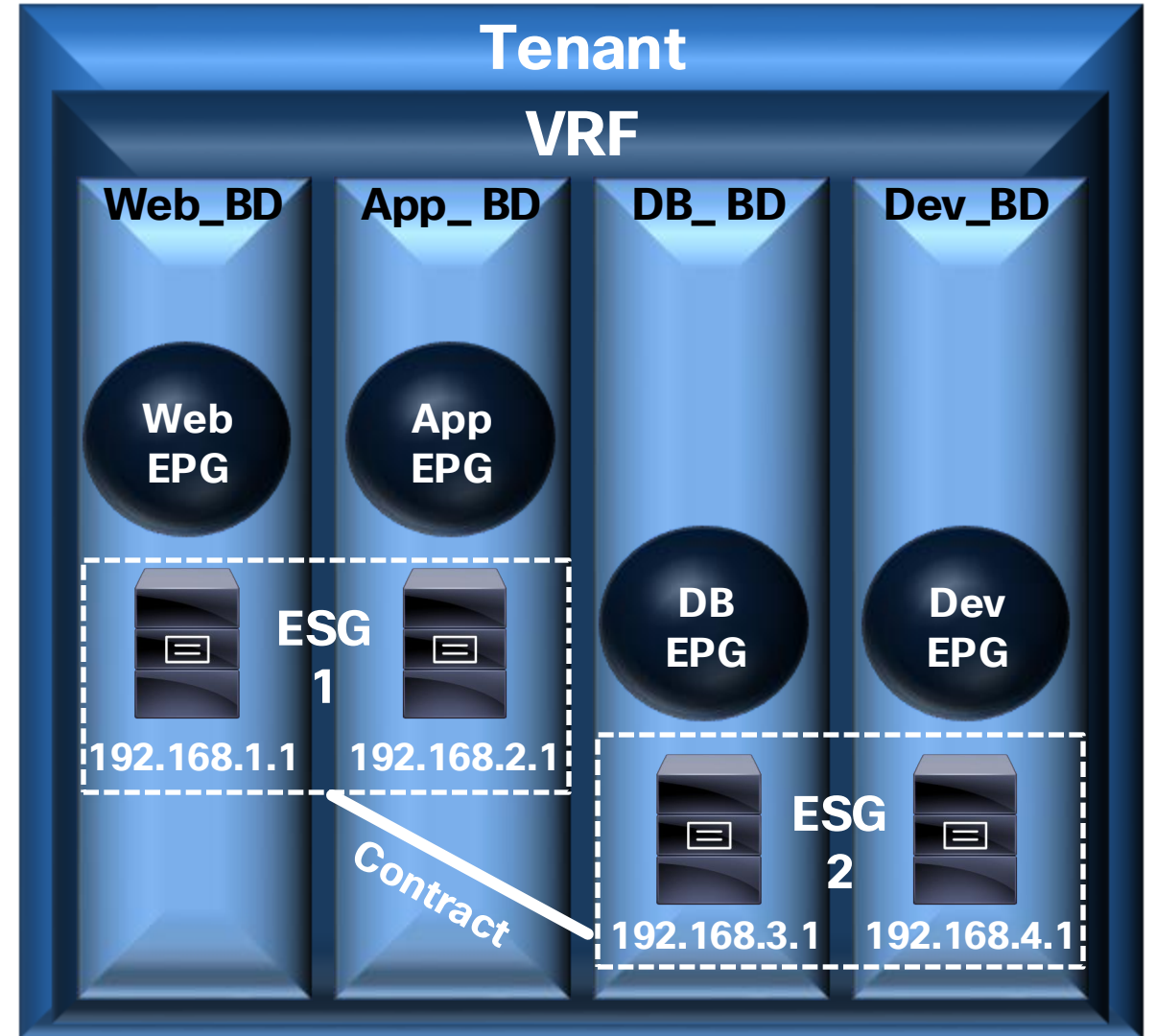
100



Overview of Endpoint Security Groups (ESGs)

Overview of Endpoint Security Groups (ESGs)

Summary

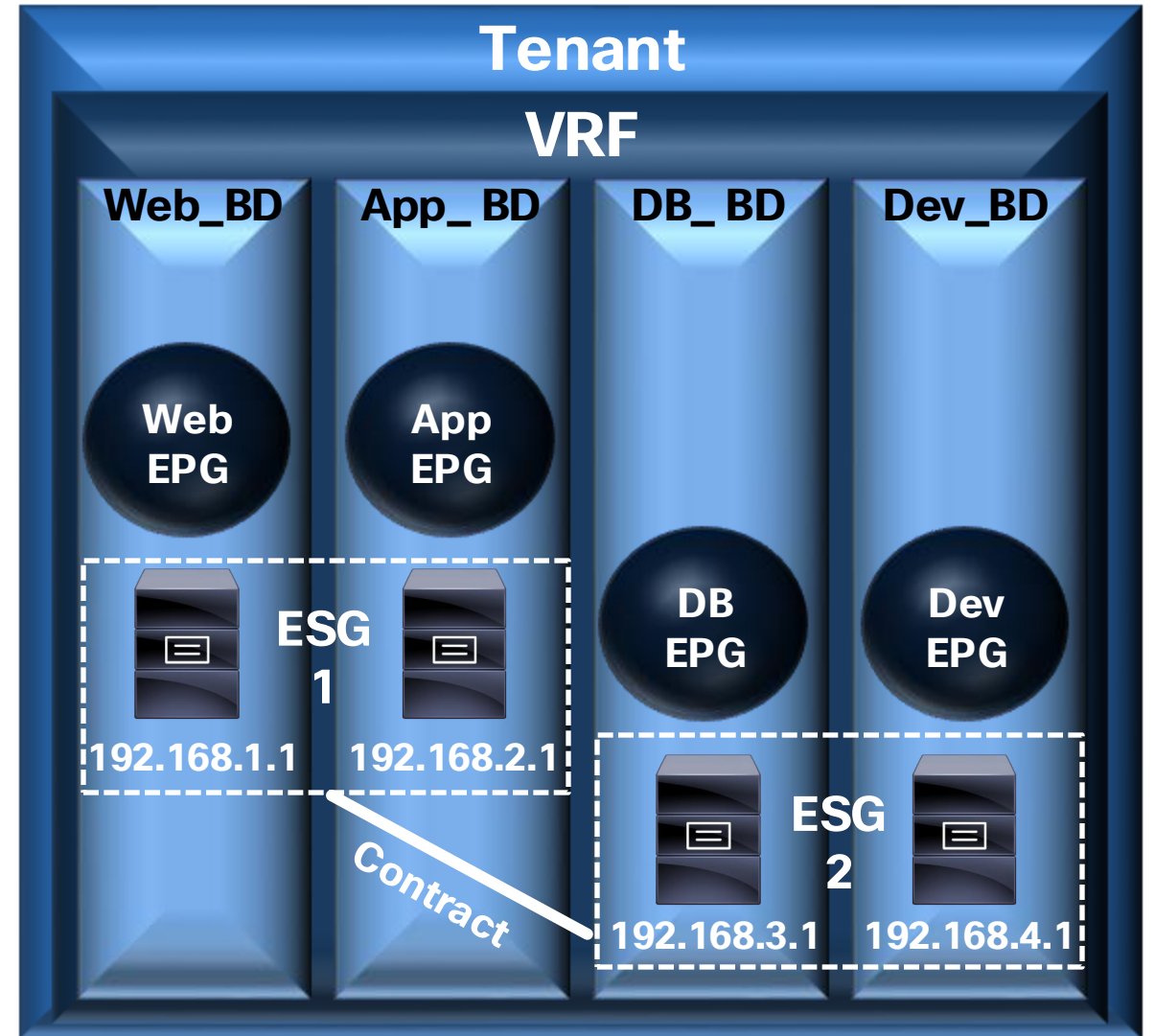


Overview of Endpoint Security Groups (ESGs)

Summary

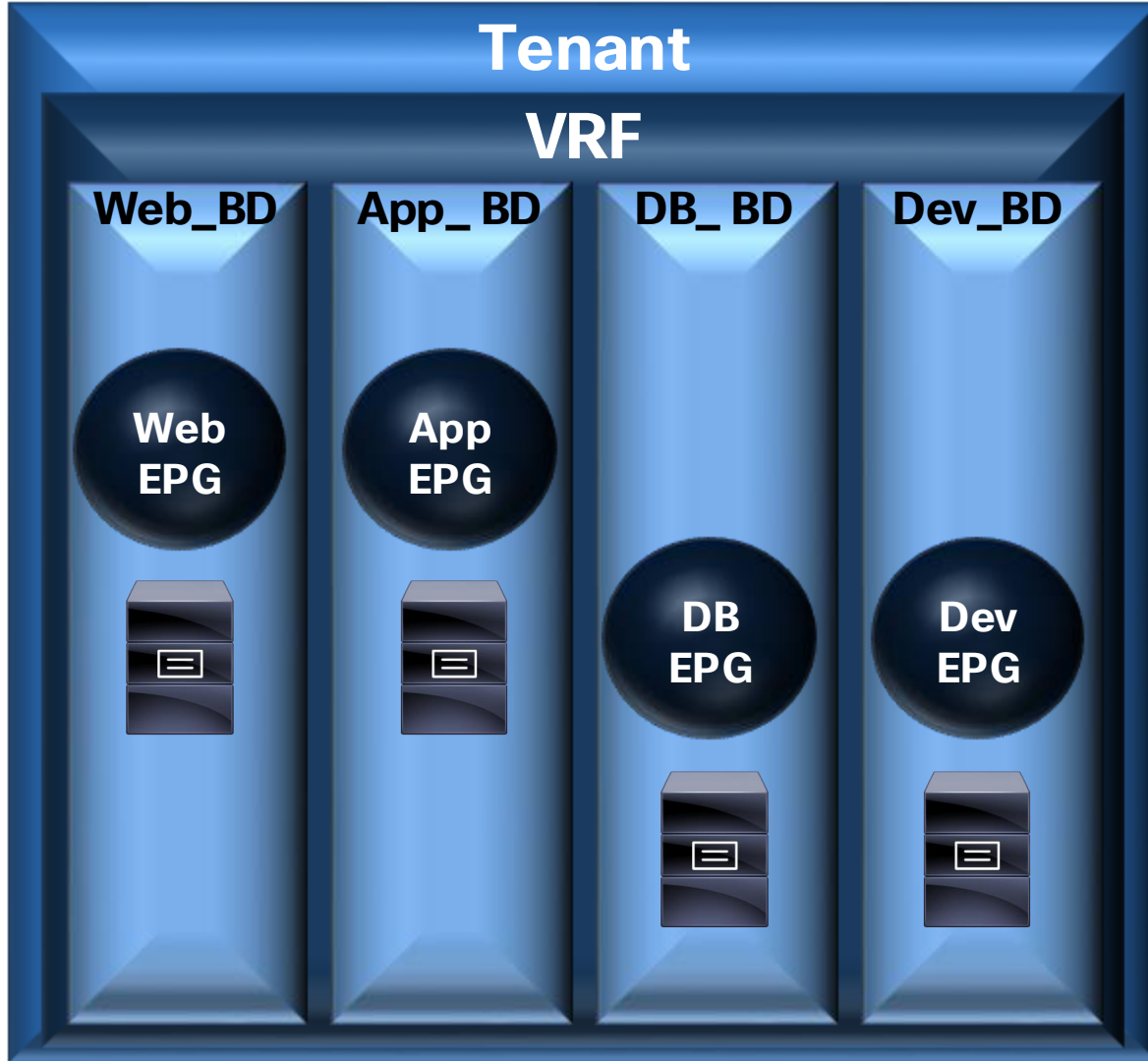
Endpoint Security Group:

- Unlike EPGs, ESGs can span multiple BDs
- Uses endpoint selectors to classify by attributes:
 - IP selector (IPv4/IPv6 subnets)
 - Tag selector (VM attributes, MAC, etc.)
 - EPG selector (assign entire EPG to ESG)
- Contract rules still apply between ESGs
- **Cannot** deploy contracts between EPGs and ESGs
- Can use preferred group with EPGs and ESGs included

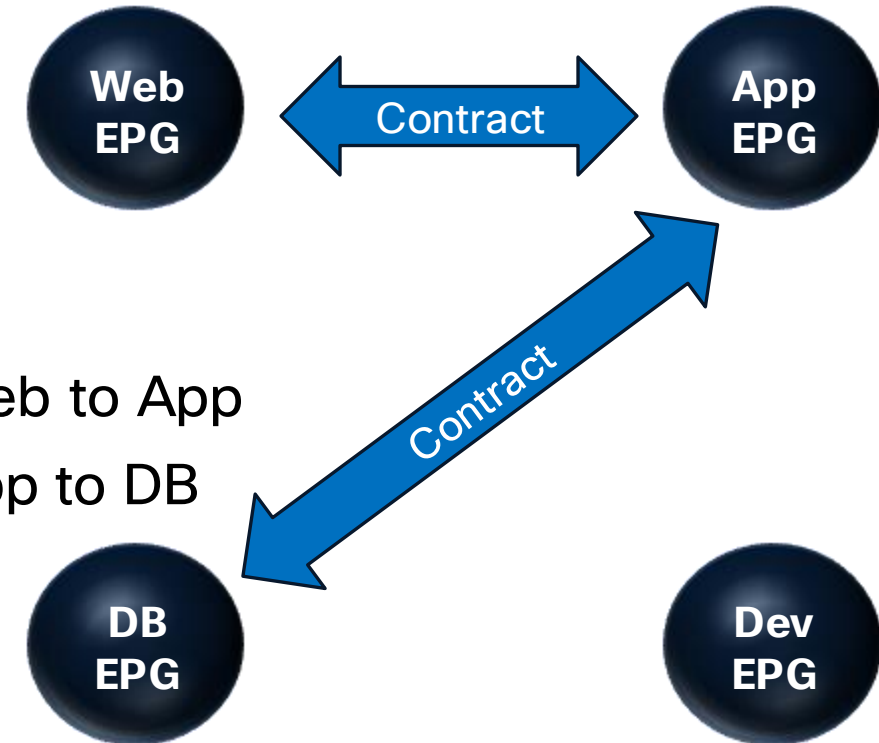


Overview of Endpoint Security Groups (ESGs)

Why You May Want to Use ESGs



Simple Contract Flow with EPGs:

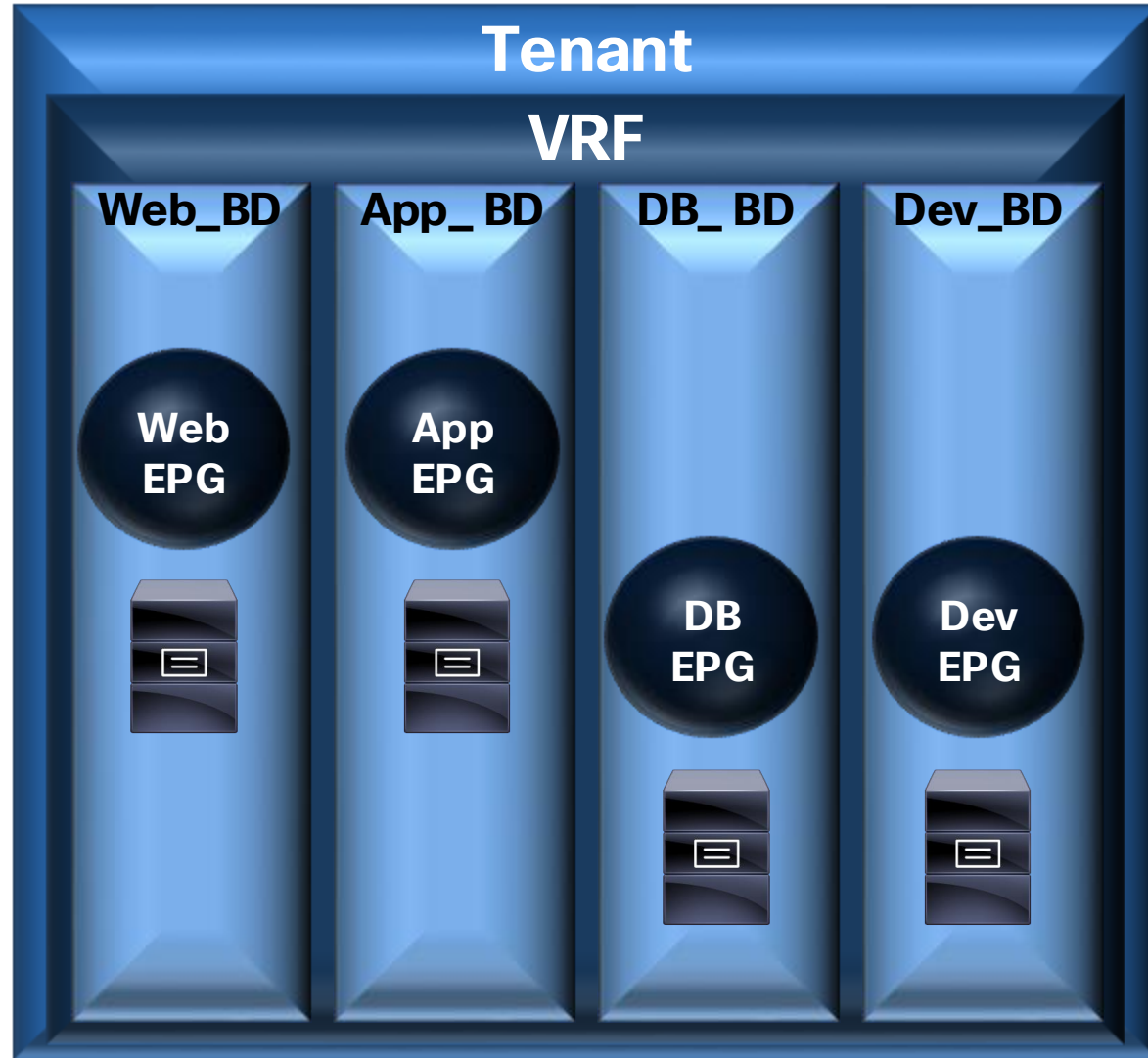


- Web to App
- App to DB

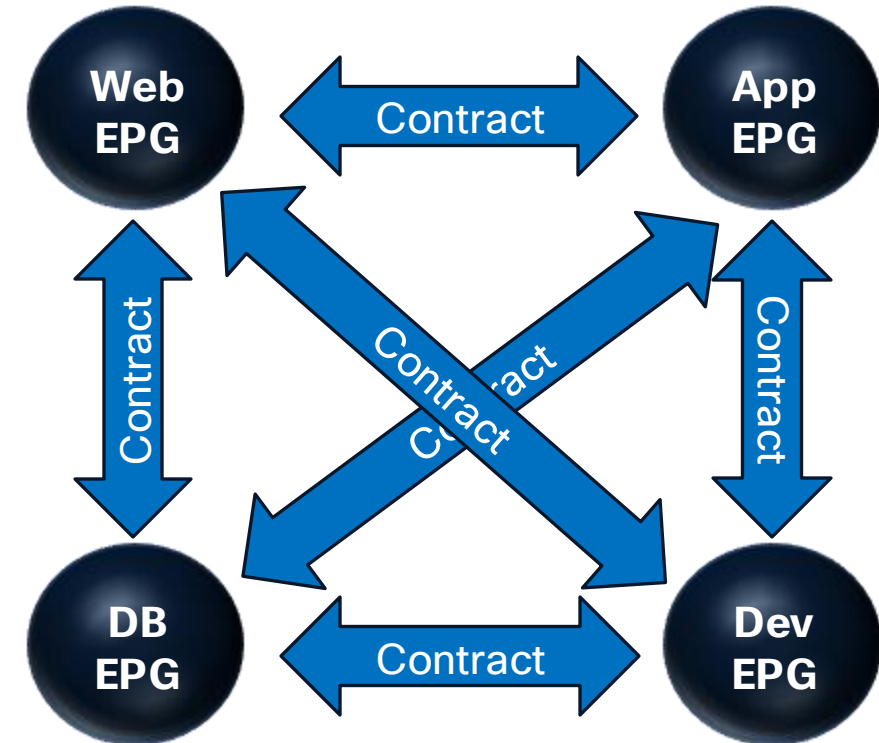
• But what if you needed more?

Overview of Endpoint Security Groups (ESGs)

Why You May Want to Use ESGs



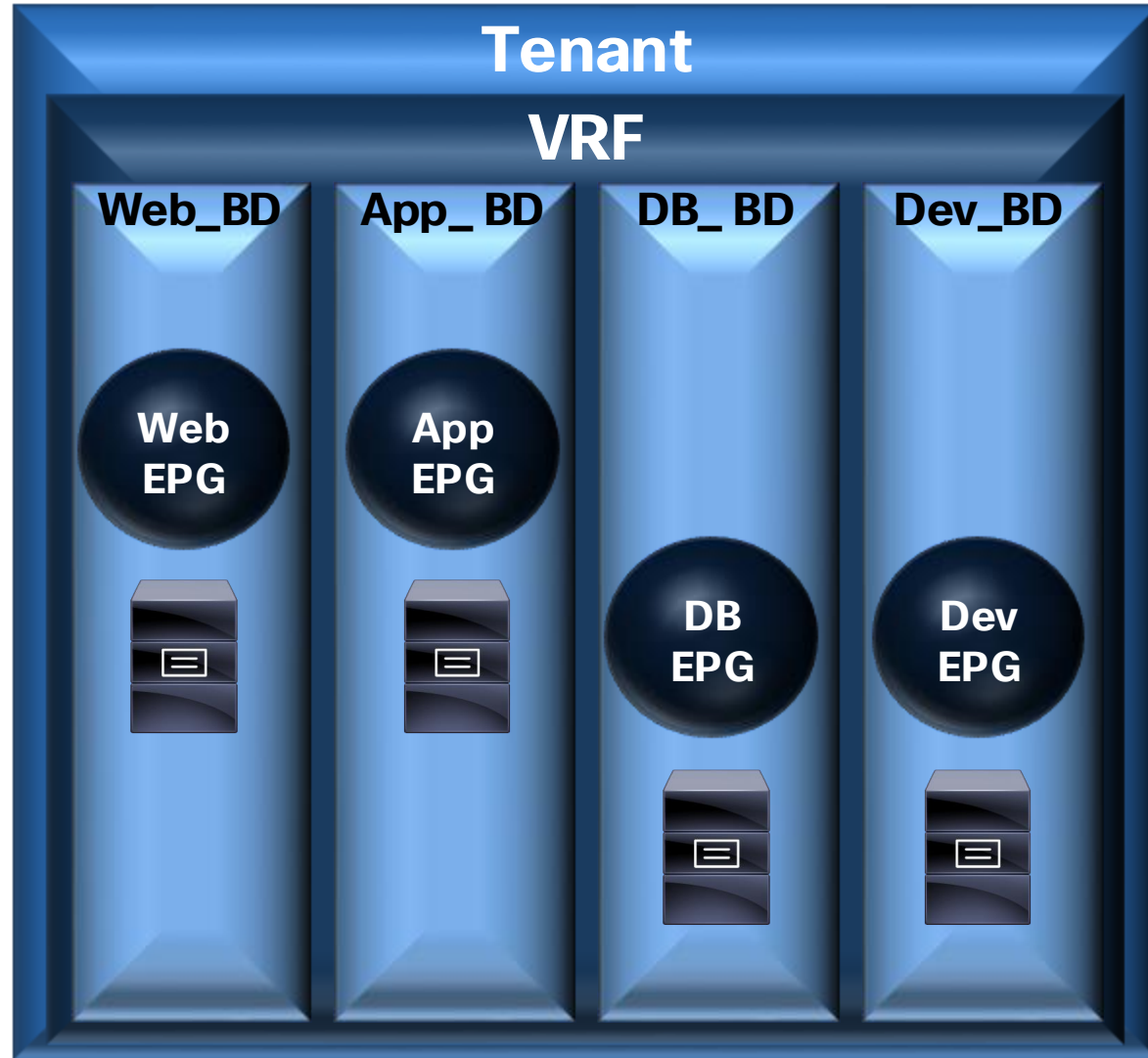
Contracts Needed for Full Mesh:



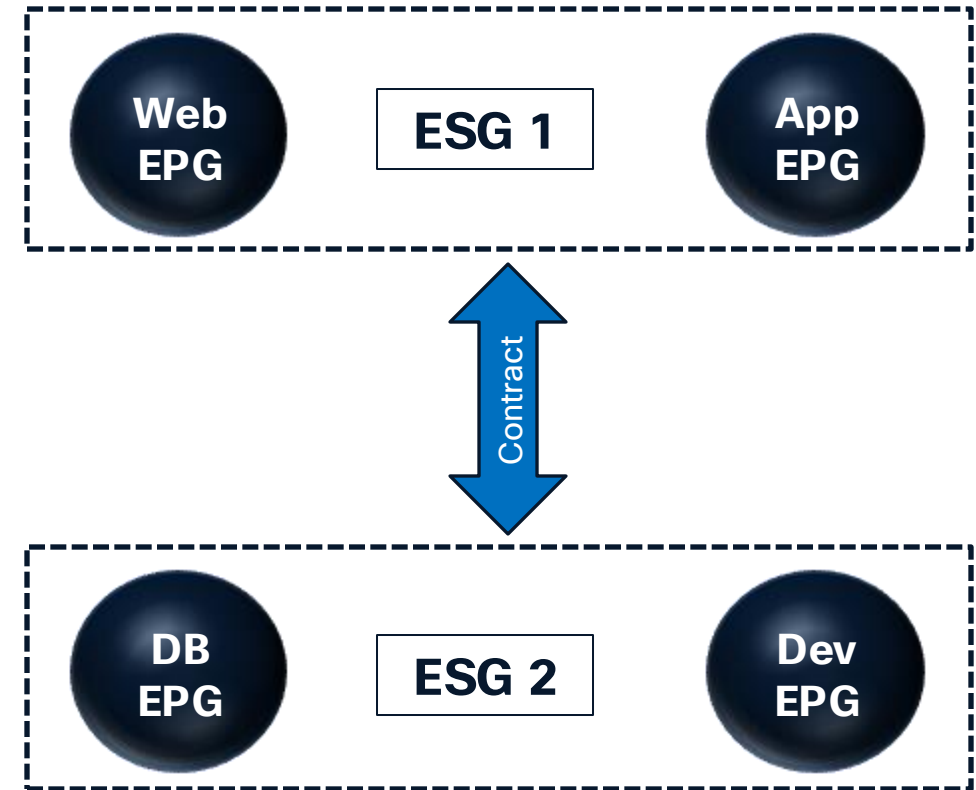
- The number of contracts involved could get complex FAST!

Overview of Endpoint Security Groups (ESGs)

Why You May Want to Use ESGs



ESGs Can Solve This Issue:



- With two ESGs the number of contracts drops to two!

DEMO: Contract Setup & Testing with ESGs





Sales

[Quick Start](#)[Sales](#)[Application Profiles](#)[eCommerce_AP](#)[Application EPGs](#)[App_EPG](#)[DB_EPG](#)[Web_EPG](#)[uSeg EPGs](#)[Endpoint Security Groups](#)[Networking](#)[Contracts](#)[Standard](#)[FileServices_Ct](#)[WebServices_Ct](#)[Taboos](#)[Imported](#)[Filters](#)[Policies](#)[Services](#)[Security \(Beta\)](#)[Application Profile - eCommerce_AP](#)[Summary](#)[Topology](#)[Policy](#)[Stats](#)[Health](#)[Faults](#)[History](#)[Application EPGs](#)3
Total

0

100

[Endpoint Security Groups](#)0
Total[uSeg EPGs](#)0
Total[Contracts Relations](#)0
Total

EPGs and ESGs Side by Side

EPGs and ESGs Side by Side

Comparison

Criteria	Endpoint Groups	Endpoint Security Groups
Scope	Bridge Domain	VRF
Function	Combines forwarding and security	Security segmentation only
Endpoint Classification	Used for VLAN bindings and interface configurations	Supports dynamic endpoint classification using selectors (e.g., IP, MAC, tags)
Class ID	Local, Global with inter-VRF contracts	Global
Preferred Group Support	Yes	Yes
vzAny Support	Yes	Yes
Multi-Pod Support	Yes	Yes
Multi-Site Support	Yes	No (as of 6.0)

EPGs and ESGs Side by Side

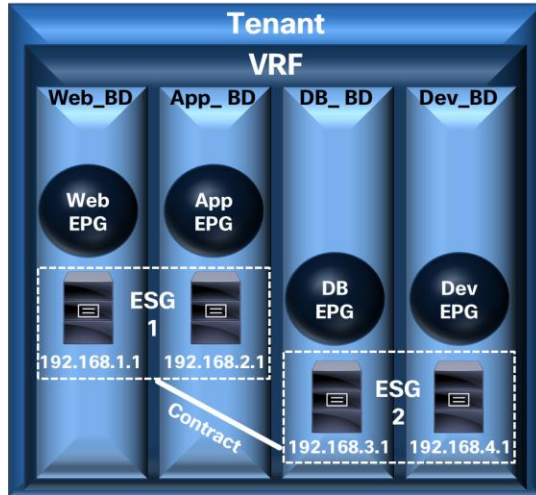
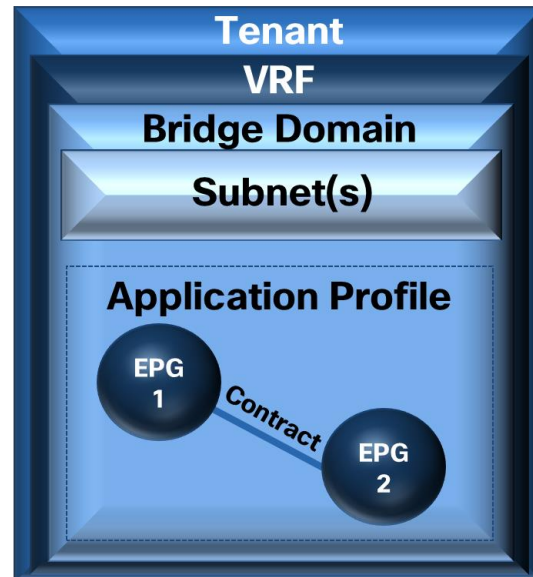
Things to Remember

1. ESGs rely on EPGs for port/VLAN mapping.
2. ESG contracts and BD subnets are deployed on all nodes where the VRF is deployed.
3. ESG contracts supersede EPG contracts.
4. EPG to ESG contracts NOT supported.
5. Contracts between ESG and L3Out are supported.
6. With ESGs there is no automatic route leaking based on contracts.
7. EPGs are supported on first generation hardware but ESGs are not.

Use Cases

Use Cases

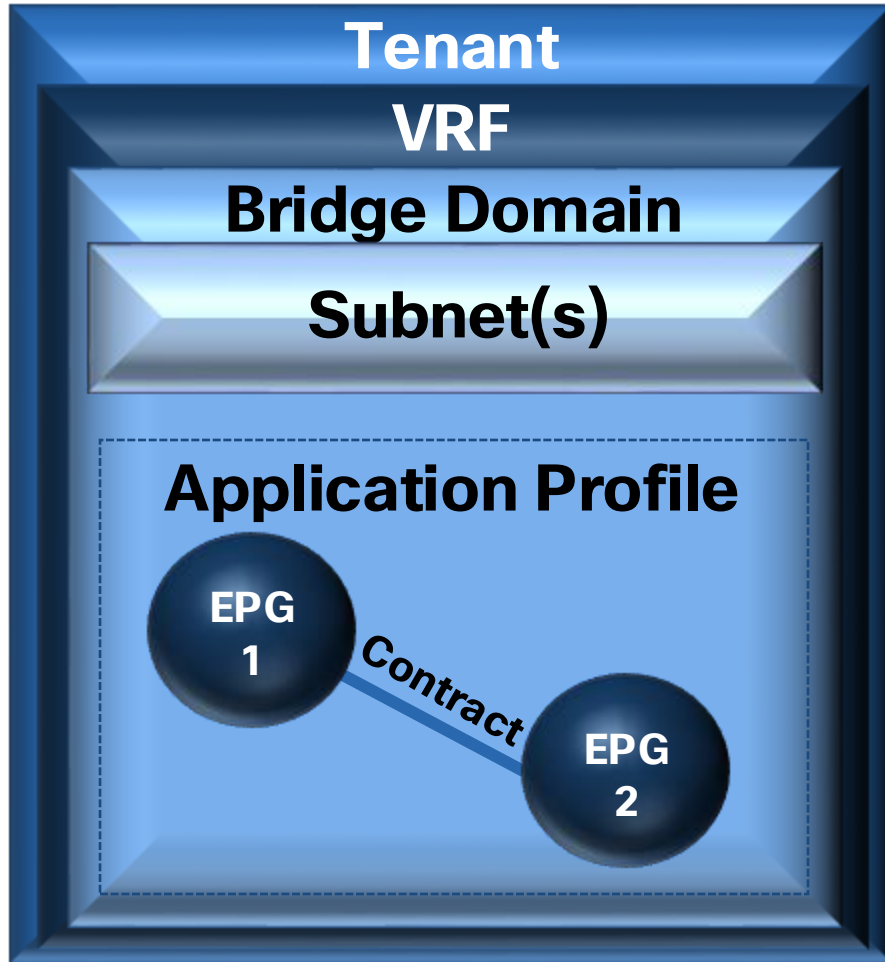
Keep in Mind...



- EPGs do not go away when using ESGs:
 - EPGs still define endpoint mapping to BDs:
 - Physical endpoint mapping using static binding
 - Virtual endpoint mapping using VMM domains
 - L3Out external EPG still identifies external traffic
- ESGs take over security configuration:
 - Contract mapping and management
 - ESG Selectors:
 - Tag selector
 - EPG selector
 - IP subnet selector
 - Service EPG selector

Use Cases

When to Use EPGs

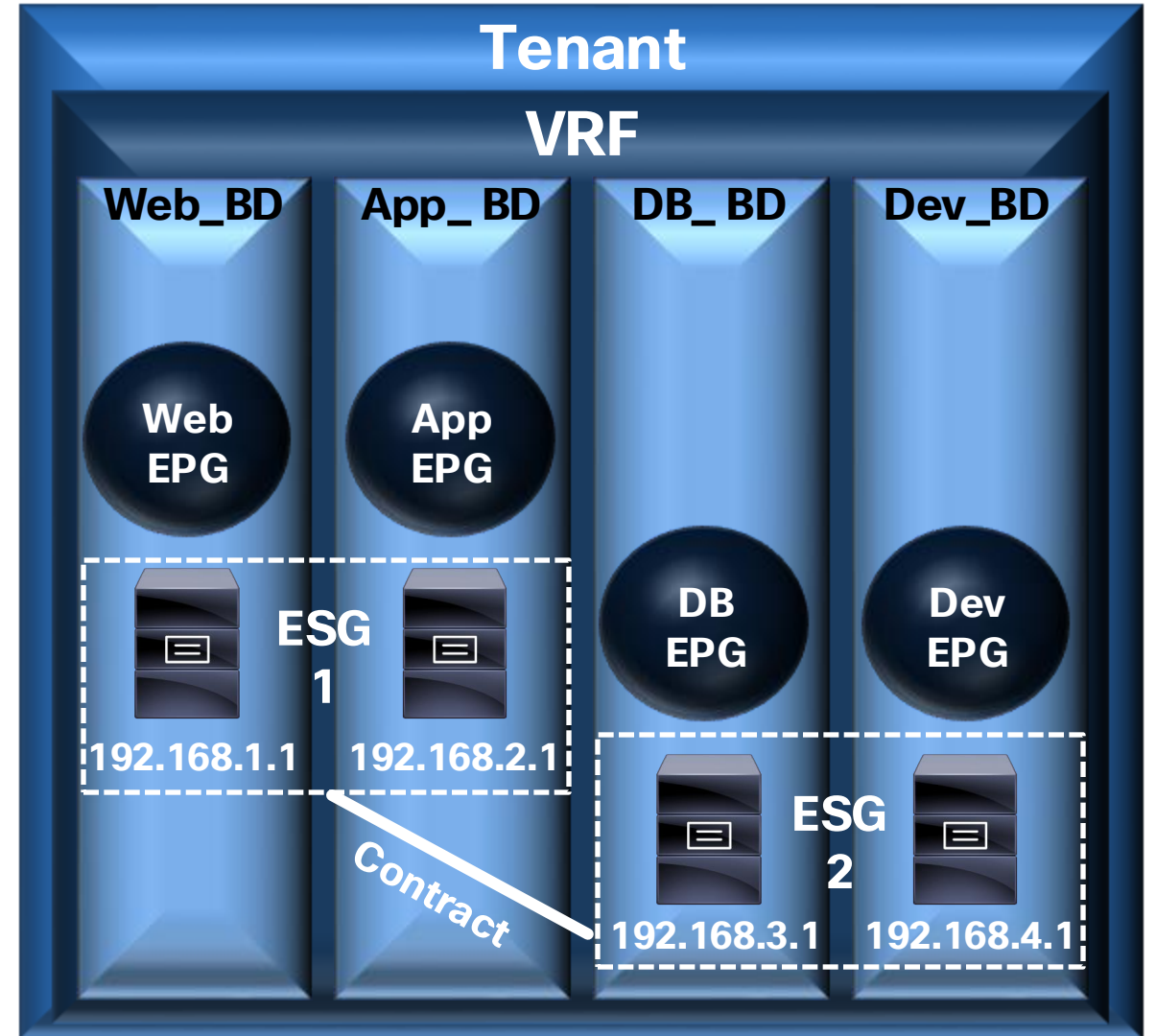


- Use EPGs alone when you need:
 - To enforce simple security within a single bridge domain
 - Simple network segmentation
 - Traditional network centric deployments
 - Mapping of ports and VLANs (this is required no matter which option you use)
 - Straightforward security

Use Cases

When to Use ESGs

- Use ESGs when you need:
 - Consolidated contract relationships (TCAM conservation)
 - Granular security zones across bridge domains
- Application network centric deployments (and migrations to app centric)
- Simplification of brownfield deployments



Conclusion

Conclusion

Final Thoughts

1. While the acronyms look similar, there is a significant difference between EPGs and ESGs.
2. ESGs still depend on EPGs for VLAN and port mappings.
3. EPGs work well when the security requirements are simple and straightforward.
4. ESGs allow for much greater granularity in security enforcement.
5. ESGs can reduce the number of contracts required.
6. ESGs have incredible flexibility.

The Cisco Live! logo is positioned on the right side of a white rectangular area. It consists of the word "CISCO" in a bold, black, sans-serif font, followed by the word "Live" in a lighter weight of the same font, and a large, bold exclamation mark "!" to the right. The background of the slide features a dynamic pattern of flowing, wavy lines in various shades of blue and purple, creating a sense of motion and energy.

CISCO Live !

