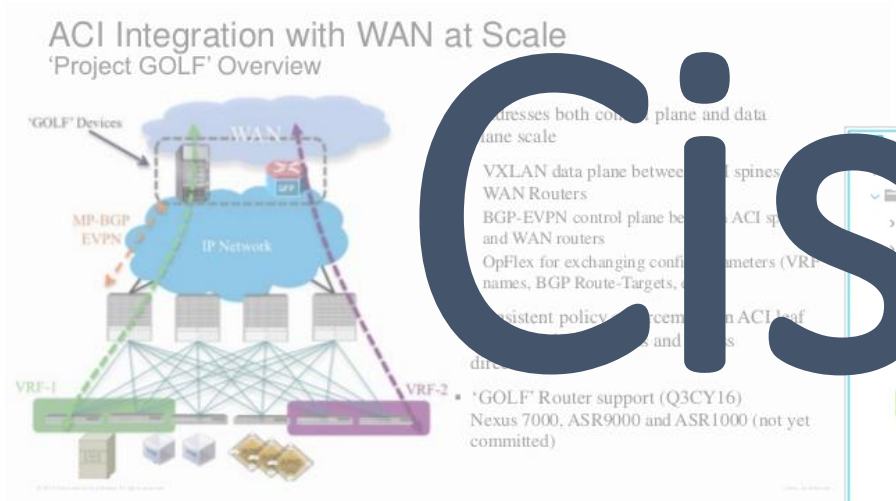
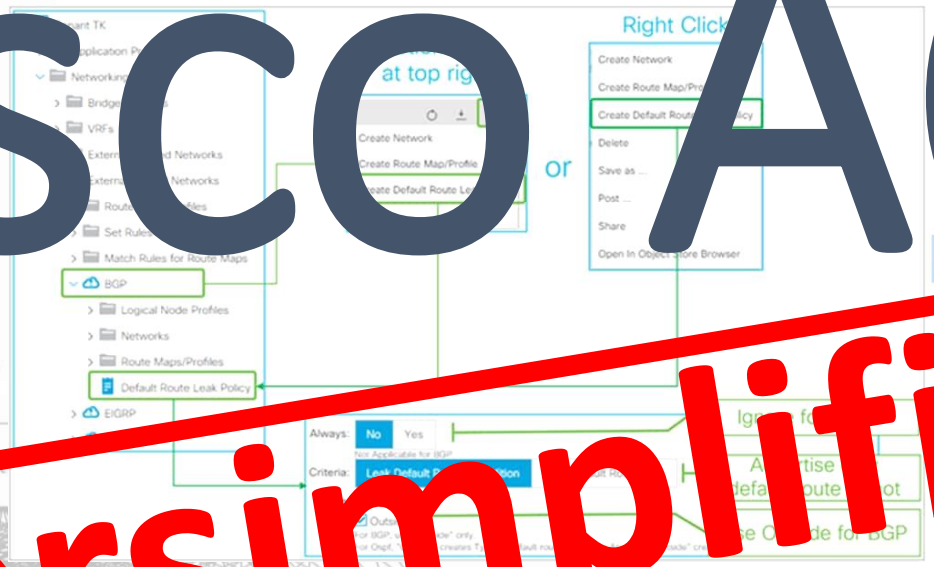
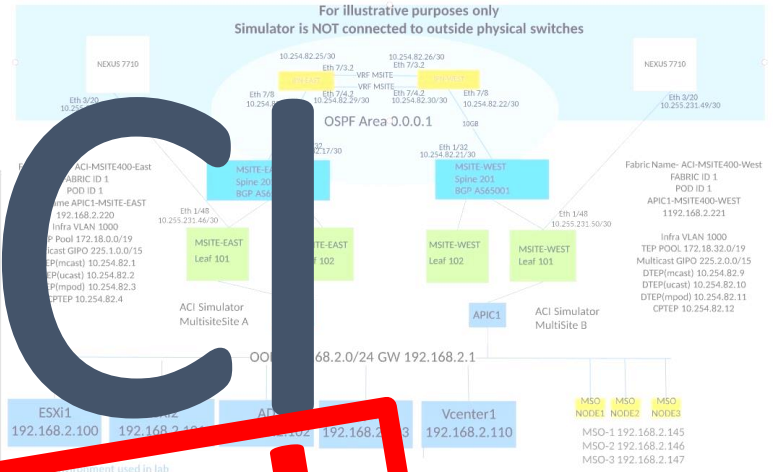
Cisco ACI

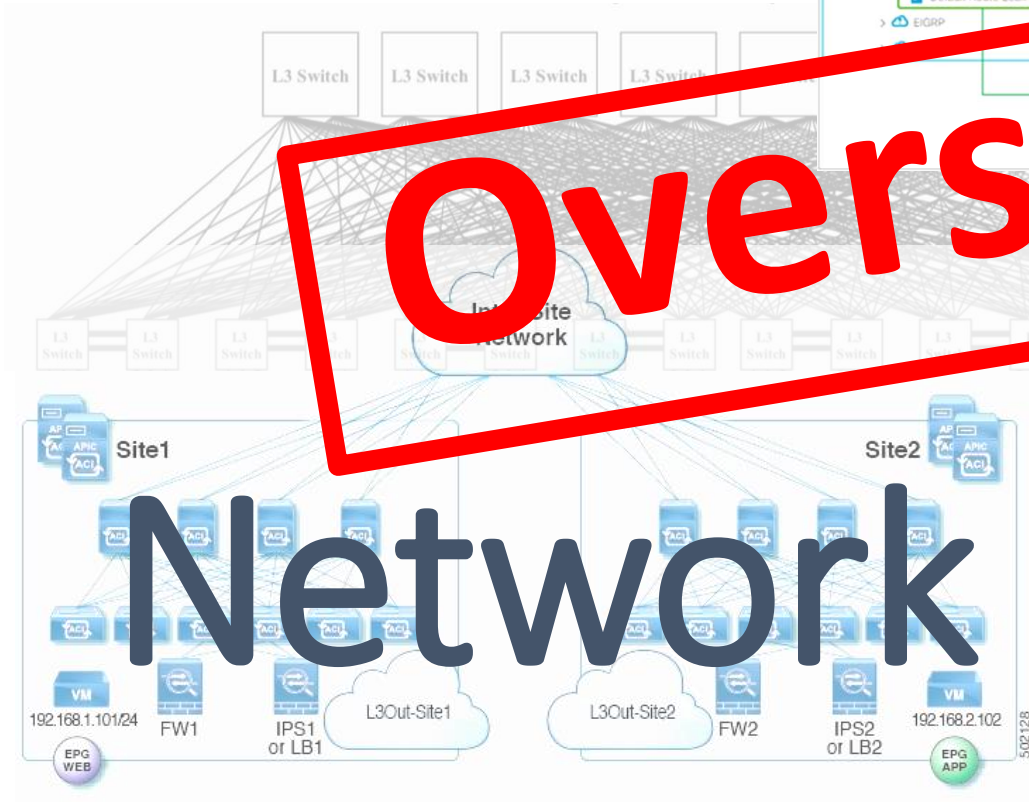
Oversimplified

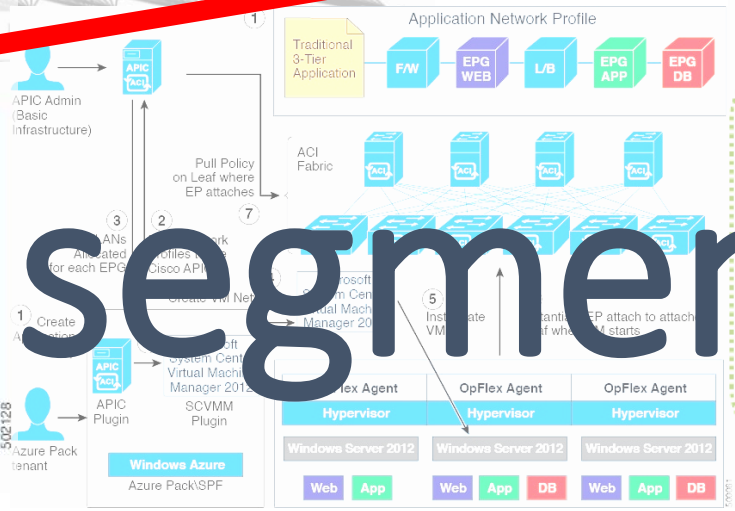
Network segmentation

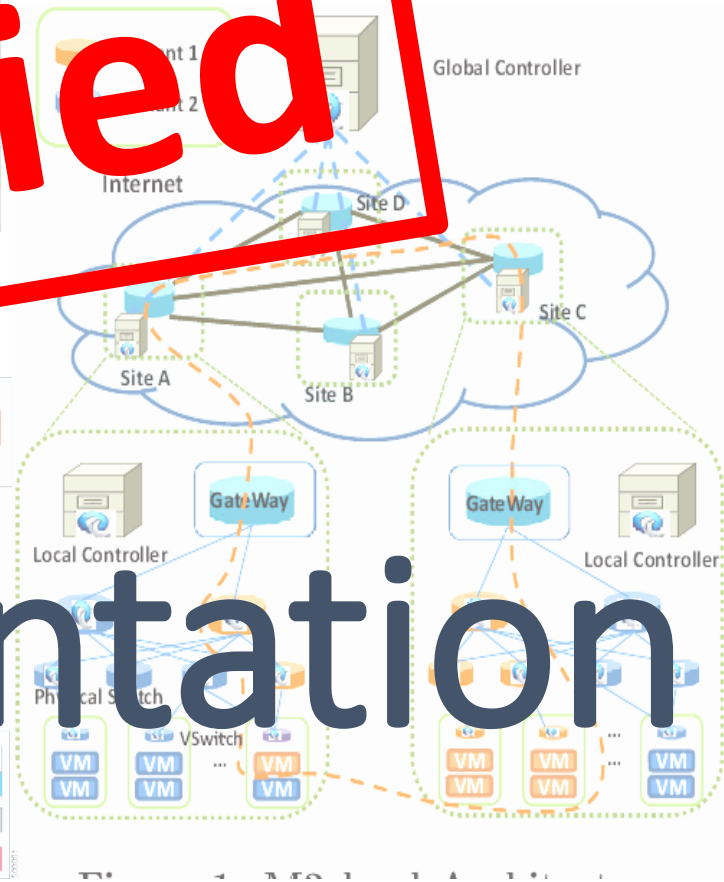












Contracts

- Traffic in ACI between endpoints
  should be explicitly permitted – **whitelist model**
- **Stateless L2-L4** filtering (resembles L3/L4 Network ACLs in AWS)
- **Line-rate** policy, no performance penalty
- These filtering construct in ACI are called **Contracts**
- **No unicast traffic between endpoints** without permitting contract, but BUM traffic is implicitly permitted (as well as PIM, IGMP, DHCP, ARP, ND, OSPF, EIGRP)
- Contacts consists of Actions – basic are **permit** and **deny**, but can do more advanced actions like **redirect** (allows to do flexible traffic engineering FW/LB insertion via Service Graphs – explained later)
- It is possible to disable Contracts – set VRF to unenforced (not recommended)

- **Excellent summary:**
  https://www.networklife.net/images/sheets/Networklife_CheatSheet_ACI_05_Contracts.pdf

Contracts – hardware limitations

- Contracts programmed in hardware – TCAM, so there are **hardware limits**, see here:

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/verified-scalability/Cisco-ACI-Verified-Scalability-Guide-422.html#id_110983

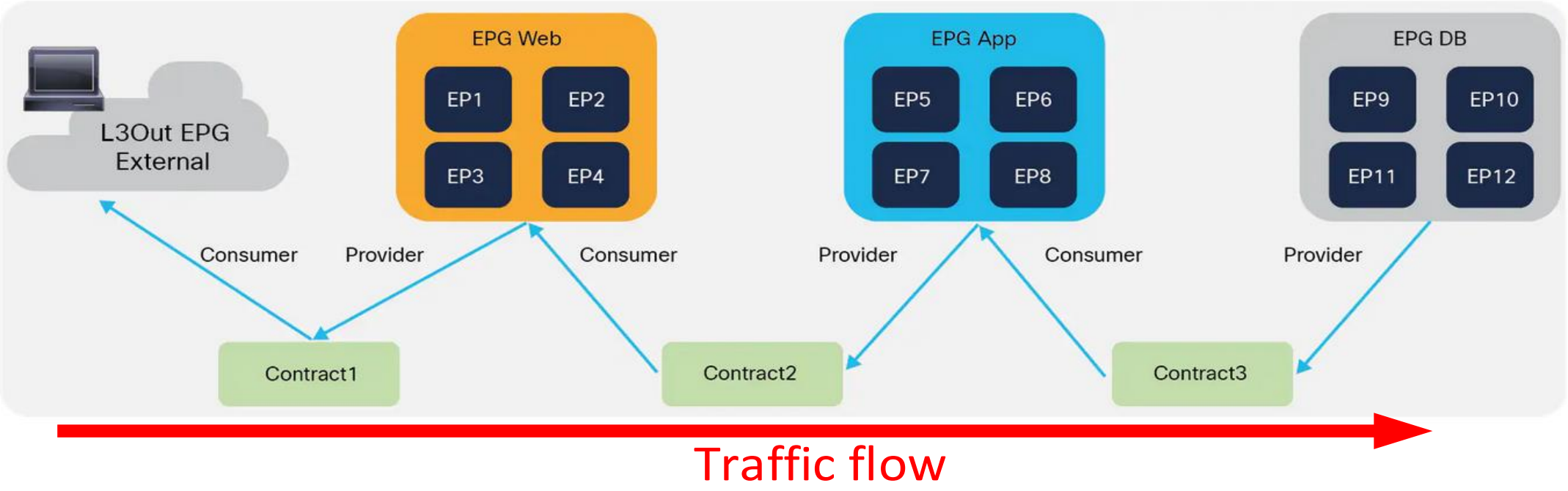
Configurable Options	Per Leaf Scale
Security TCAM size	Default scale profile: • For ALE v1: 4,000 • For ALE v2: 40,000 • For LSE and LSE2: 64,000

Approximate TCAM calculator given contracts and their use by EPGs	Number of entries in a contract X Number of Consumer EPGs X Number of Provider EPGs X 2
Maximum number of EPGs providing the same contract	100
Maximum number of EPGs consuming the same contract	100
Maximum number of consumers from a single EPG and single contract	1000

- Various methods how to reduce or optimize TCAM Utilization:
  - Policy compression
  - vzAny (any endpoints in a VRF)
  - Accurate grouping of endpoints
  - Using TCP established flags -> https://community.cisco.com/t5/application-centric/aci-contract/td-p/3855931

Contracts

- Contracts consist of **Providers** and **Consumers** - these are EPG – **Endpoint groups** (not individual objects as it's possible in FWs, always groups)
- Contracts can be applied either between Endpoint Groups or between Endpoint Group and external (L3Out)
- In documentation you'll see the references like **EPG provides** or **consumes** contracts.
- Usually Provider/Consumer relationships is shown like below, note the actual traffic flow is 'opposite'



Hierarchy

Filter

Single ACL entry

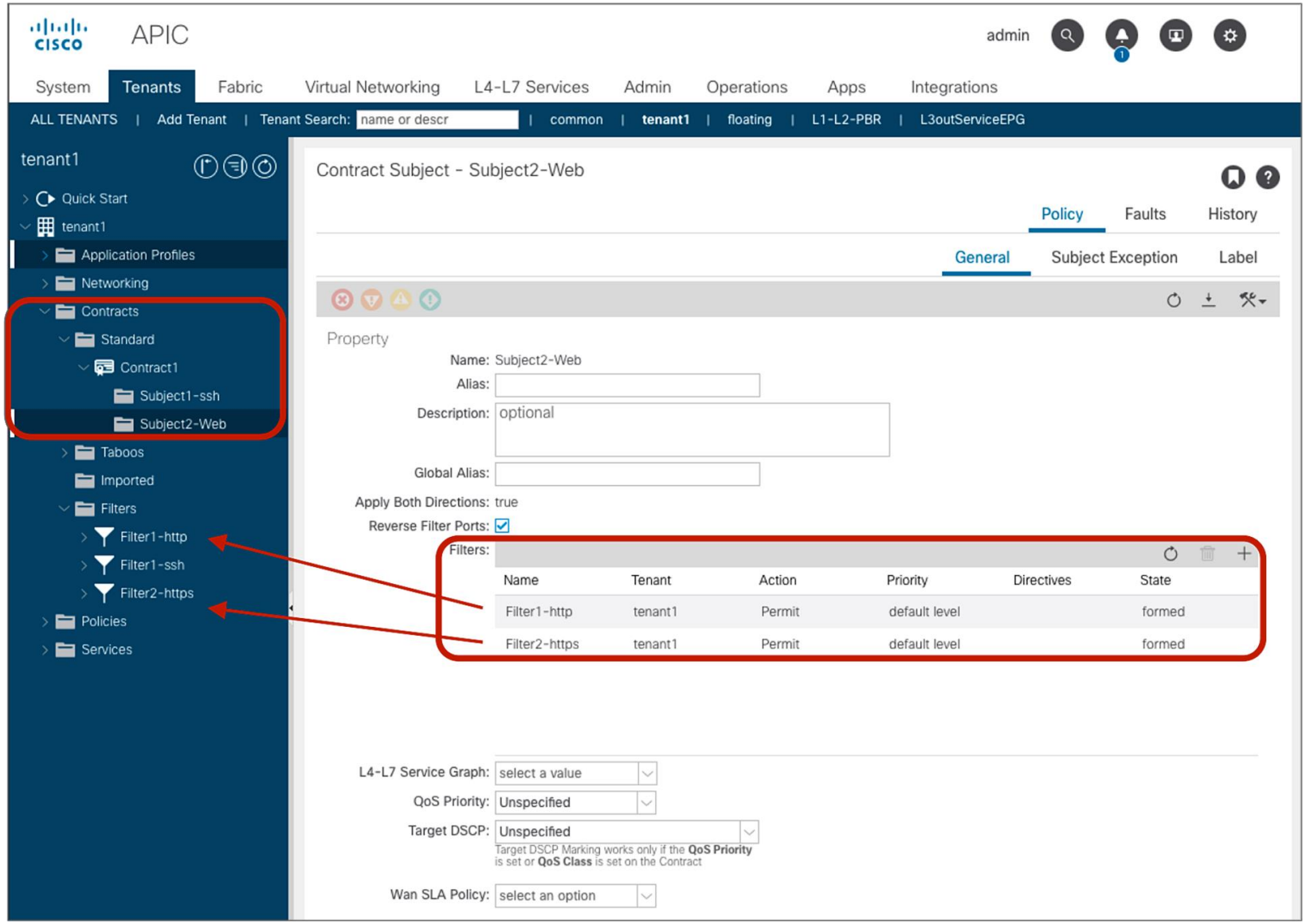
Subject

Multiple ACL entries – filters

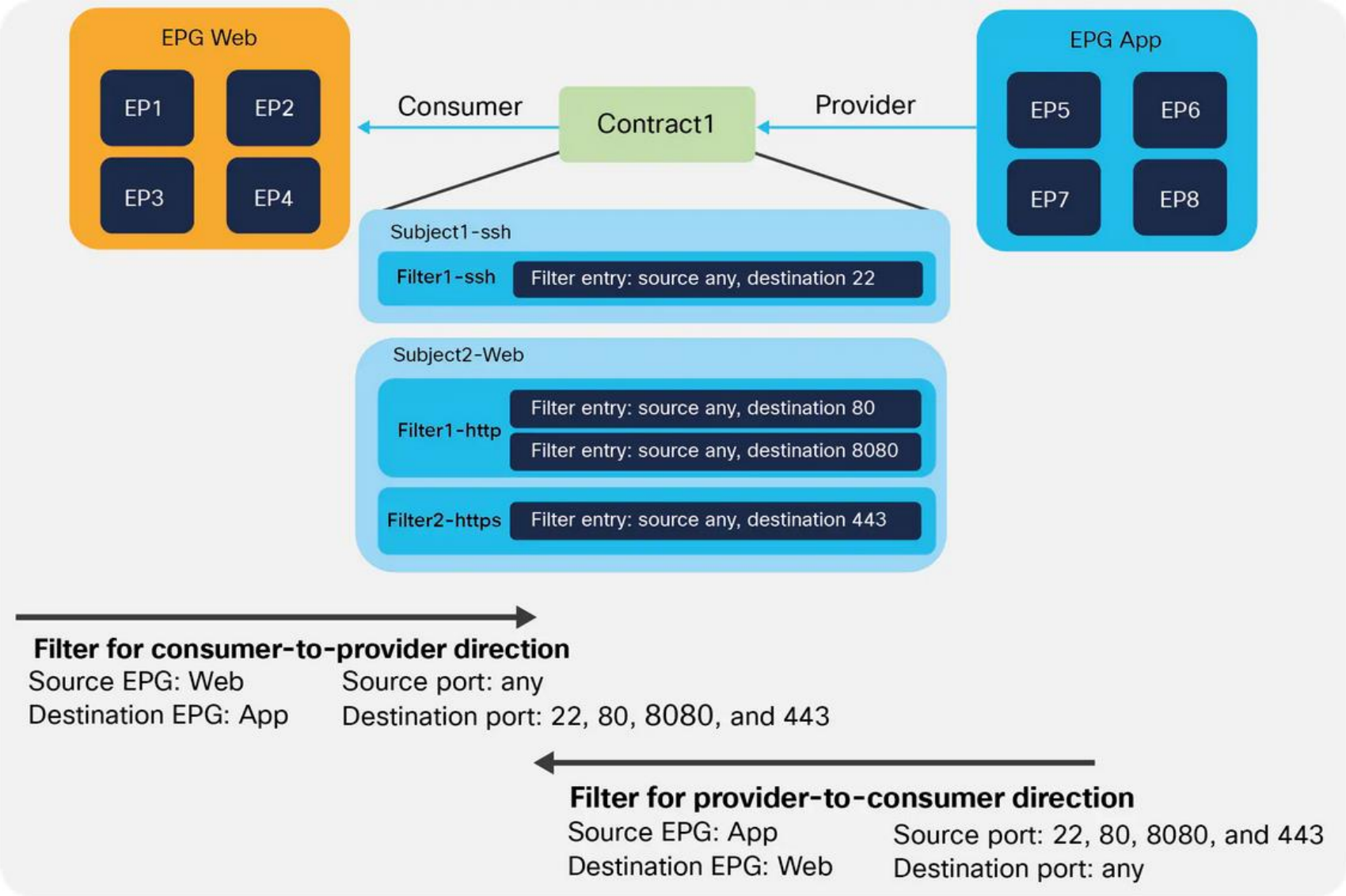
Contract

Multiple subjects – defining all traffic flows between groups

Contracts then **assigned to EPGs** as Provided or Consumed contracts



Subjects and filters – How contracts work



Check the source:

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/cisco-aci-contract-guide-wp.html#Howcontractswork

Endpoint Groups

- Group of objects sharing the same policies – similar to normal FW
- Endpoints inside an EPG can talk to each other
- Endpoints in different EPGs cannot communicate with each other without a contract
- EPG ID (**pcTag**) is carried in VXLAN header (which makes it proprietary iVXLAN)
- Easiest case: **Endpoint group = VLAN** – the same is traditional L3 networks, no filtering in the same broadcast domain, often called Network-centric approach
- Group endpoints based on purpose/functions **irrespectively of their network attributes, such as MAC,VLAN/IP**, etc – Application-centric approach
- Multiple EPGs per BD segmenting Broadcast domain (each EPG belongs to 1 BD)
- Specific cases - Endpoint Security Groups (ESG) and uEPG (microEPG) for micro segmentation for ESXi-hosted VMs

Endpoint Groups – how to assign EP to EPG

- **External EPG** used for L3Out – **based on network prefixes**, like in traditional routers (10.9.8.0/25)
- **ACI internal endpoints** – multiple ways - based on Endpoint attributes (VLAN, MAC, IP, VM name, etc):
- Simplest – static assignment: port + VLAN = EPG
- IP or MAC address of physical EP
- If integrated with vCentre, possible to build uEPG (microsegmentation) based on:
  - VM name
  - VM tags or customer attributes
  - Guest OS
  - AD Group
  - VM Folder
  - Combination with AND/OR of the above attributes

Three approaches to using EPGs in ACI

EPG/BD = VLAN

Create a BD and one EPG for each existing VLAN.

Common strategy to lift-and-shift traditional configurations.

Simpler for migration, complex for Micro Segmentation.

EPG = App Tier

Create one EPG for each application Tier.

Flat-network design, many apps can share a single BD.

Fantastic for GreenField and automated deployments.

Hybrid (Combination)

New Apps and Legacy Apps share the same Fabric.

Tenant and VRF sharing.

or

Dedicated Tenant/VRF and leaking.

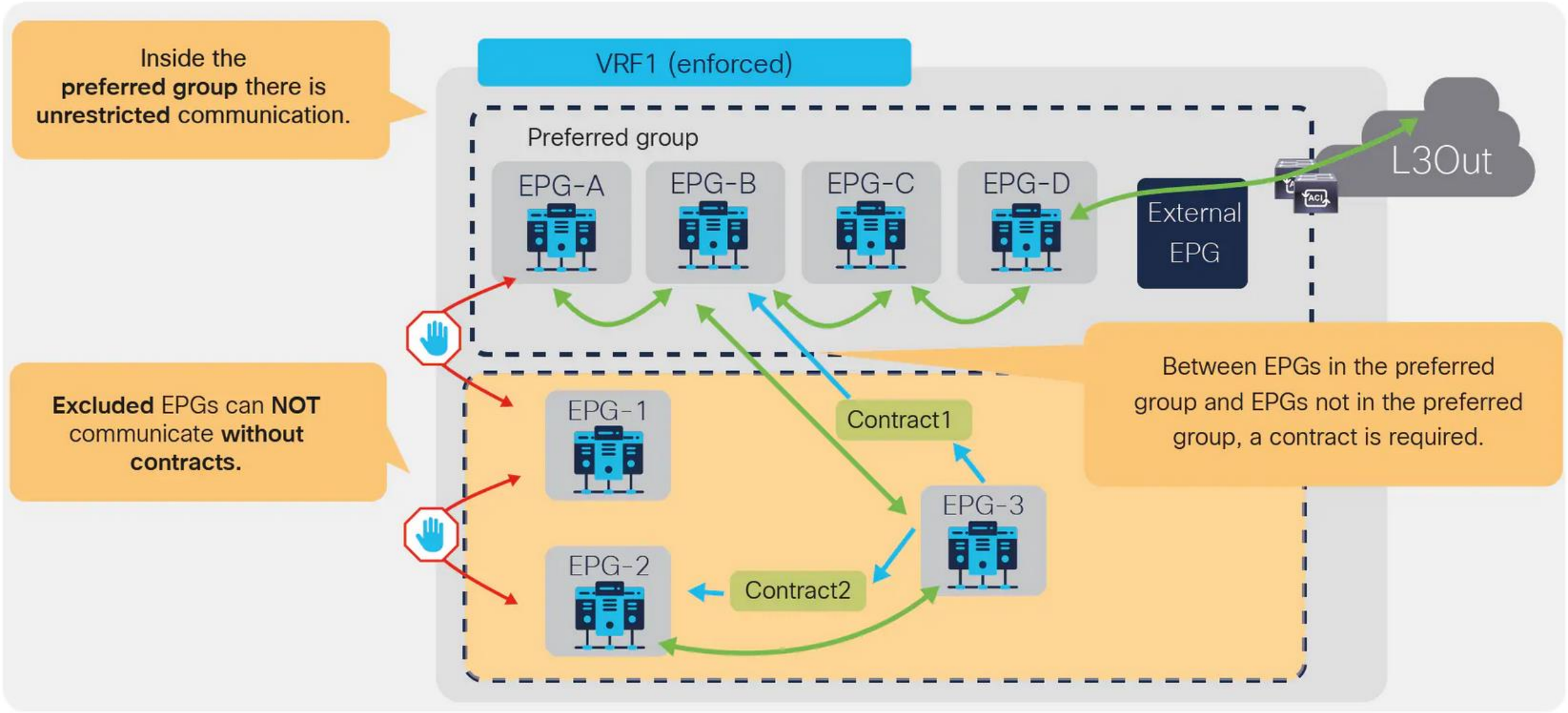
Migration from the existing network

The following list summarizes the options provided by Cisco ACI to simplify the adoption of contracts:

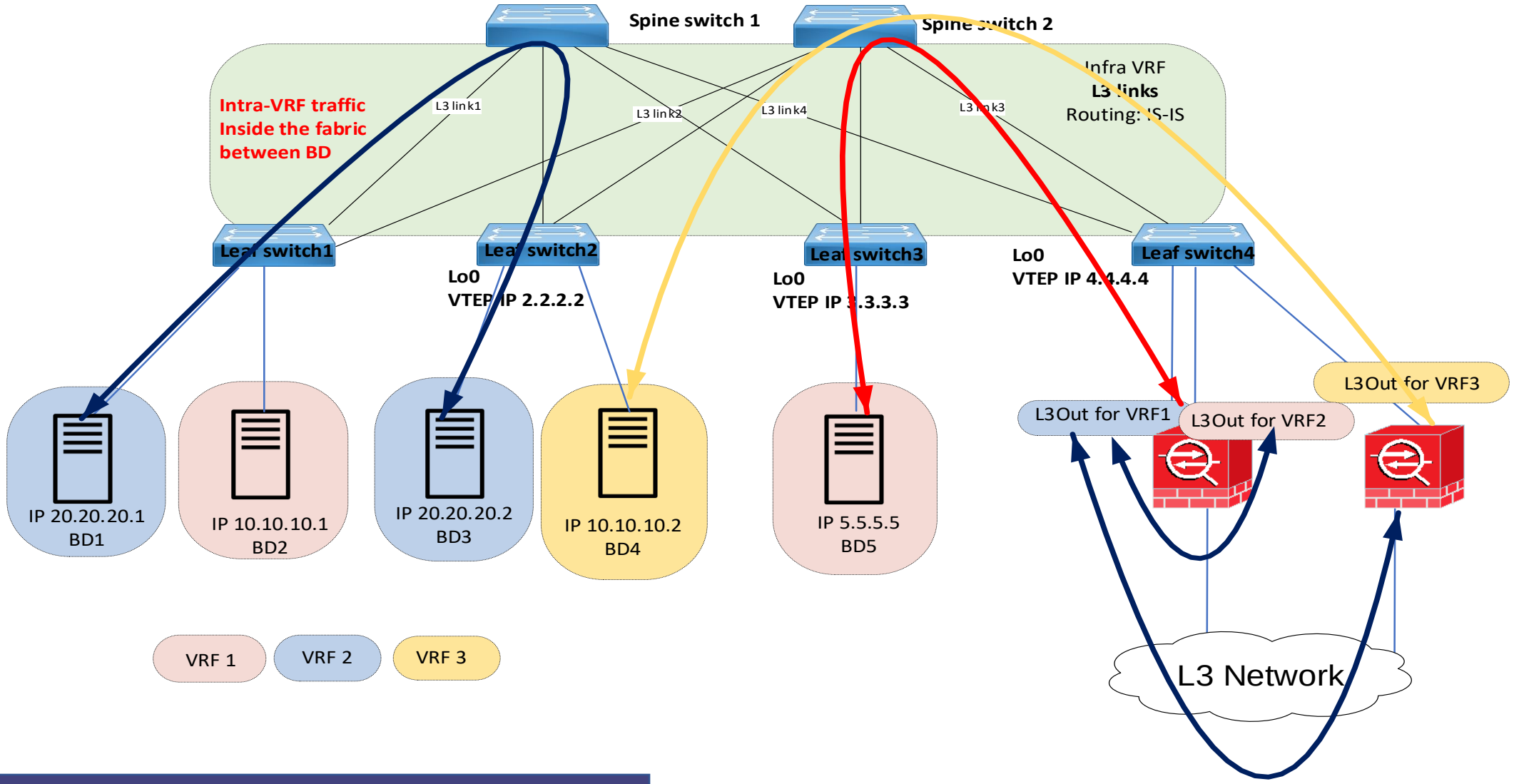
- Unenforced mode: All EPGs members in the VRF can communicate freely. This is a per-VRF configuration.
- Preferred groups: a group of EPGs per VRF where EPGs can communicate freely. Other EPGs still require contracts to communicate. Each VRF can have one preferred group.
- vzAny: vzAny represents all EPGs in the VRF. This option is also referred to as an "EPG Collection." By applying contracts to vzAny, the administrator can create security rules that apply to all the EPGs in the VRF.
- EPG contract inheritance: This feature allows the administrator to configure an EPG to inherit the contracts of other EPGs, which are used as a "master." This feature allows organizing contracts in a more manageable way for complex configuration.

Check the source: https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/cisco-aci-contract-guide-wp.html#Contractdesignoptionsformigrationandoperationalsimplification

Migration from the existing network – preferred group



Simplest config: EPG = BD = VLAN, all in preferred groups, filtering on FW

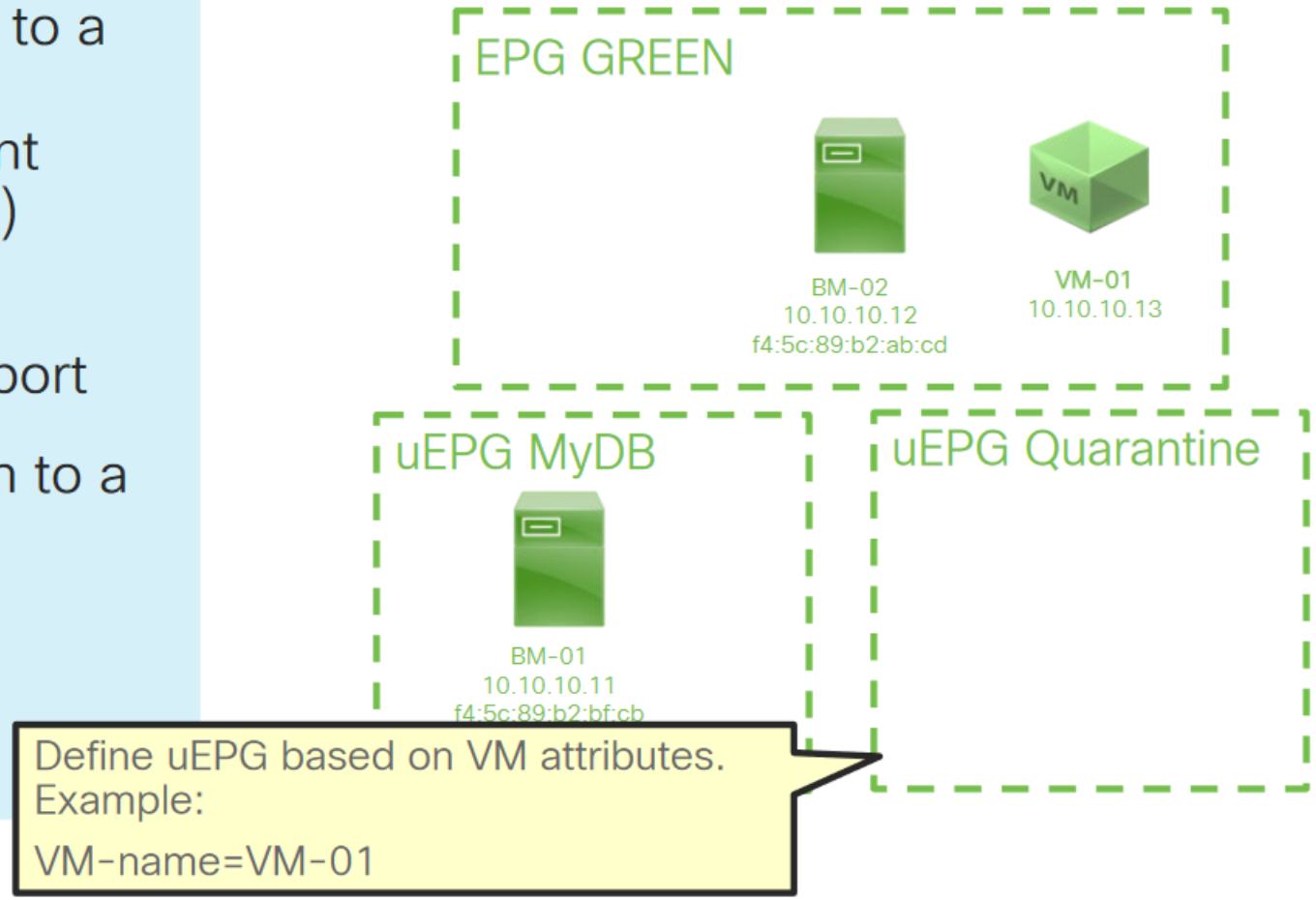


Building EPGs based on functions

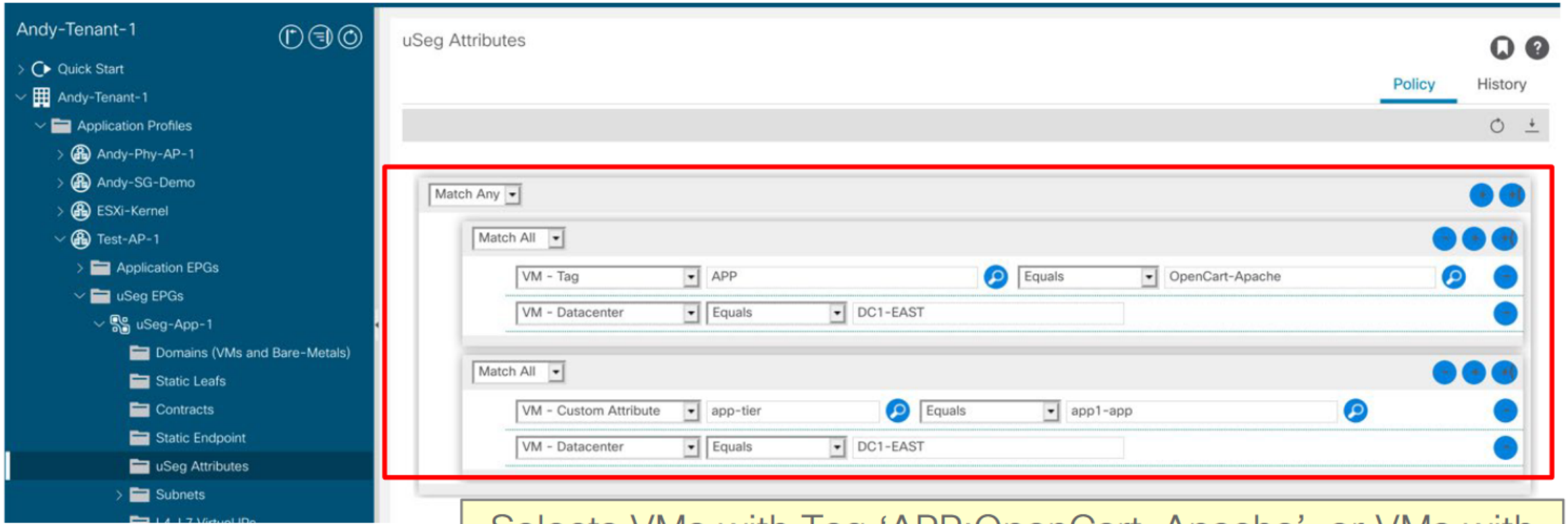
- Security Groups (ESG)
- Microsegmentation

Understanding Micro EPGs

- A MicroEPG (uEPG) is equivalent to a regular EPG for all purposes, but classification is based on endpoint attributes (and dynamic in nature)
- Endpoints assigned to the uEPG regardless of the encapsulation/port
- The endpoint must be first known to a regular EPG, called "**base EPG**"



uEPGs with Attributes and Logical Operators - GUI Configuration (2/2)



Selects VMs with Tag 'APP:OpenCart-Apache', or VMs with 'Custom Attribute app-tier=app1-app' as long as they are running on vCenter DC1-EAST datacenter

Good reading

- **Cisco ACI Contract Guide**

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/applica aci-contract-guide-wp.html

- **Contracts Cheatsheet**

https://www.networklife.net/images/sheets/Networklife_CheatSheet_ACI_05_Contracts.pdf

- **Cisco Live - Practical Applications of Cisco ACI Micro Segmentation**

https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKACI-2301.pdf

Thanks!