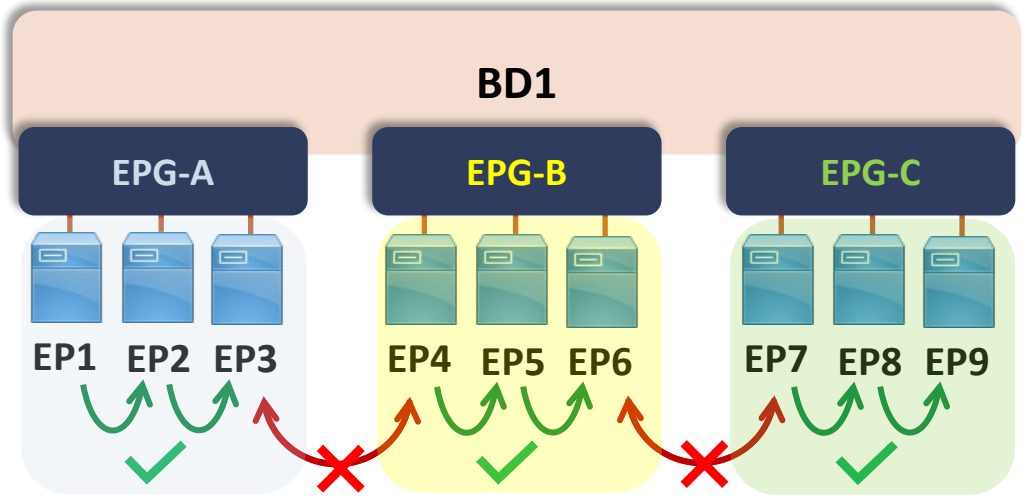
Cisco Data Centers

ACI CORE

ACI Security Policy Deployment Overview

ACI Policy Deployment Overview

- By default, ACI uses a whitelist security model:
  - Traffic within the EPG is allowed.
  - Traffic between EPGs is not allowed without a contract.
  - Contracts are deployed between EPGs, EPGs & L3Outs (Ext-EPG), or ESGs.
  - Contracts are applied on unicast traffic only.
- ACI policy is created based on contracts between EPGs supporting L2-4 filters (like ACLs).
  - Each EPG is assigned a unique pcTag value used in policy deployment (pcTag = Source Group/sClass).
  - The ACI policy is enforced between the source and the destination EPGs.
  - The ACI policy can be enforced at the ingress or egress leaf switches.
  - By default, an EPG and its associated contracts are programmed in a leaf switch only if EPs related to that EPG are locally attached to the leaf.
  - Static path binding: Deployment Immediacy: Immediate | On Demand



(**Tenant1** >> **Operational** >> **Resource IDs** >> **EPGs**)

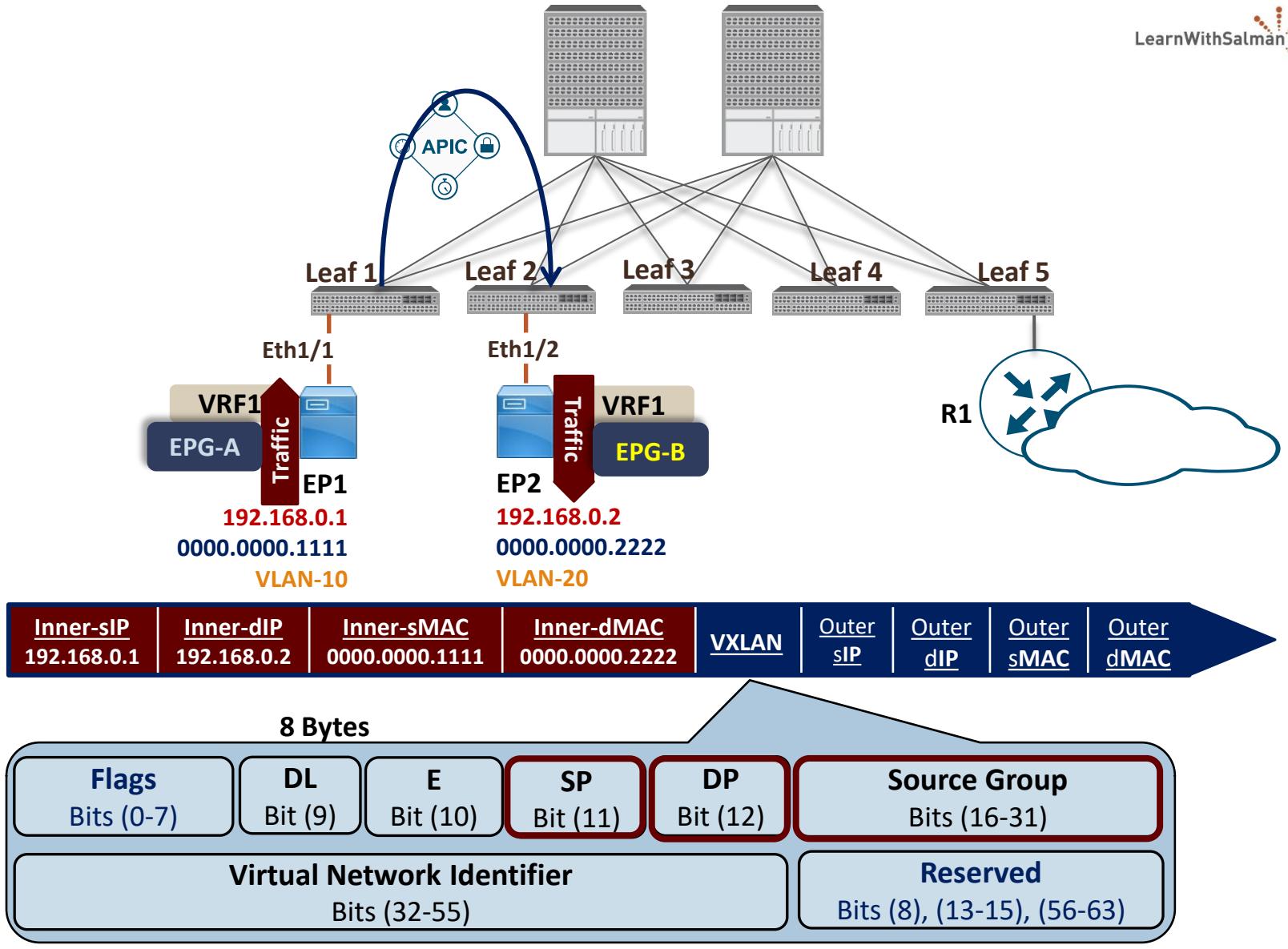
Application Profile Name	EPG Name	Class ID	Scope
App-X	EPG-A	16389	2293765
App-X	EPG-B	32771	2293765
App-X	EPG-C	32770	2293765
App-Y	EPG-D	16388	2293765

```
apic-1# moquery -c fvAEPg -f 'fv.AEPg.name=="EPG-A"' | egrep 'pcTag '
pcTag                : 16389
```

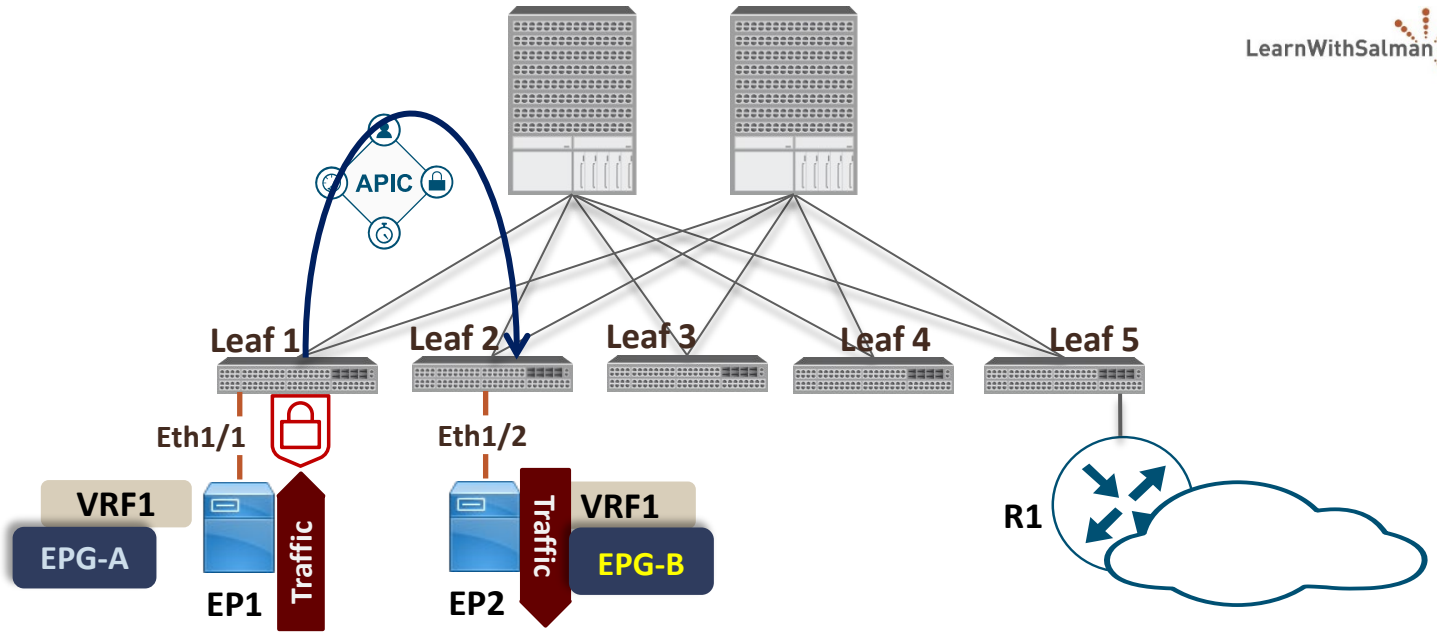
ACI Policy Identification

- Leaf derives **Src EPG pcTag**:
  - Match in **EP table**: src MAC for L2 traffic or src IP for L3 traffic.
  - **Longest prefix match** against src IP (L3Out external EPG).
  - Ingress **port** + **encap VLAN**.
  - **Source Group** value in the iVXLAN header (for egress leaf only).
- Leaf derives **Dst EPG pcTag**:
  - Match in **EP table**: dst MAC for L2 traffic or dst IP for L3 traffic.
  - **Longest prefix match** against dst IP (L3Out external EPG).
- ACI policy rules are programmed within the VRF scope.
  - Policy lookup parameters are: (**VRF**, **Src-pcTag**, **Dst-pcTag**, **Filter**).

CREATED BY SALMAN ALHIARY, CCIE #56363



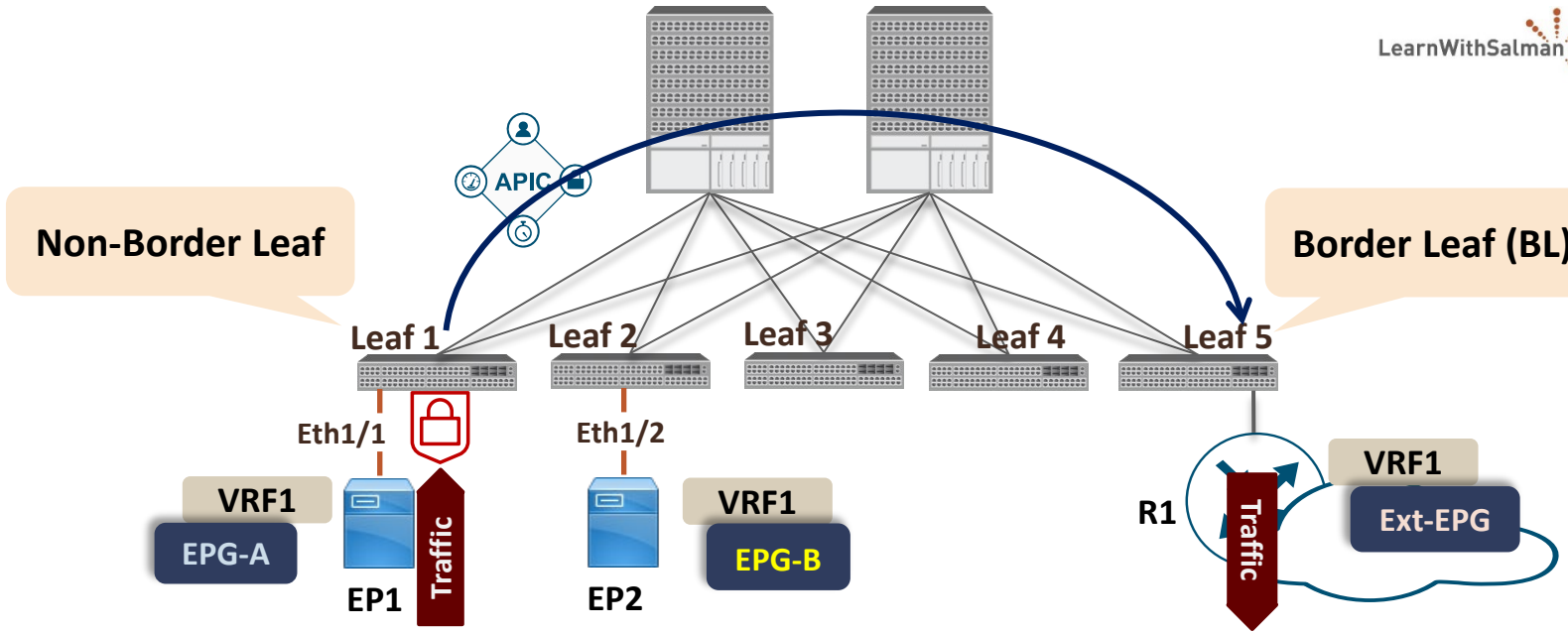
Where is the policy Applied?



Policy Control Enforcement Direction: Egress | **Ingress**

Enforcement Direction	Consumer	Provider	Policy Enforced On
Ingress or **Egress**	**EPG**	**EPG**	**Ingress Leaf**: if dst EP is learned. **Egress Leaf**: if dst EP is not learned.

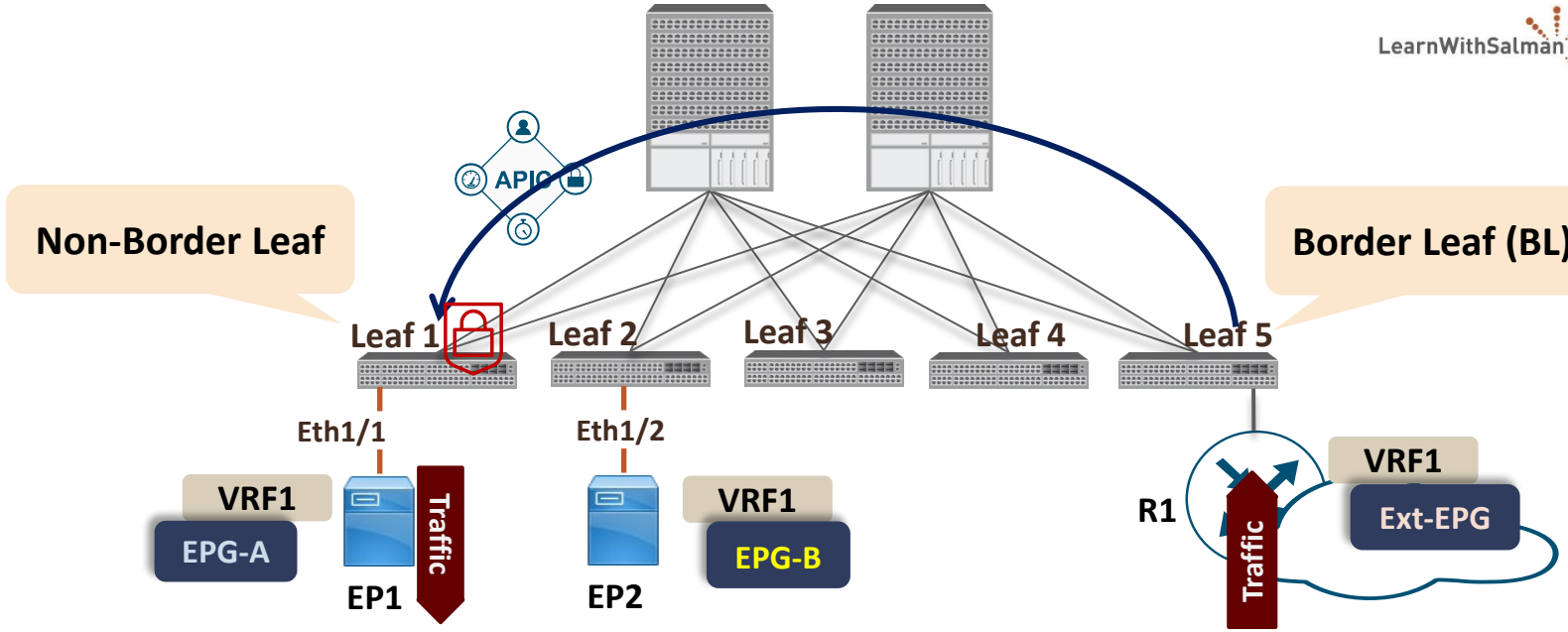
Where is the policy Applied?



Policy Control Enforcement Direction: Egress | Ingress

Enforcement Direction	Consumer	Provider	Policy Enforced On
Ingress or **Egress**	**EPG**	**EPG**	**Ingress Leaf**: if dst EP is learned. **Egress Leaf**: if dst EP is not learned.
Ingress	**EPG**	**L3OUT EPG**	**Consumer Leaf** (non-Border Leaf)

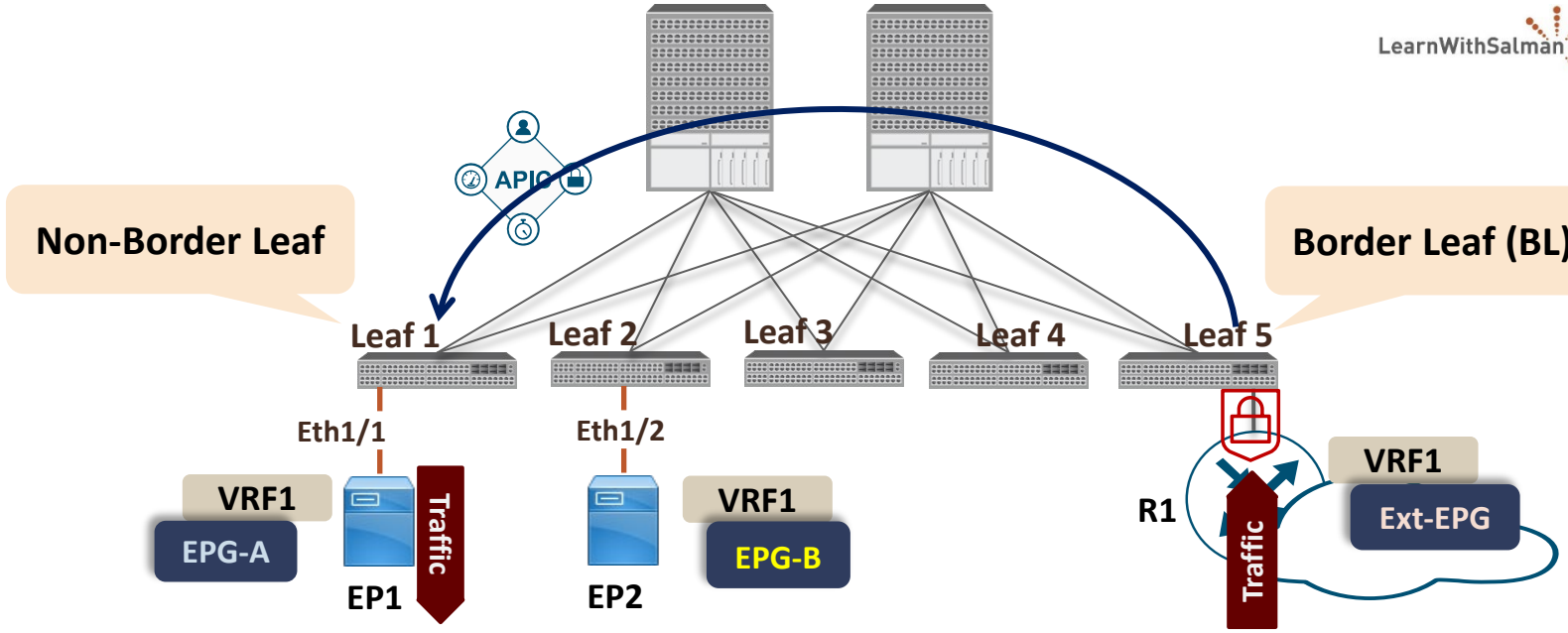
Where is the policy Applied?



Policy Control Enforcement Direction: Egress | Ingress

Enforcement Direction	Consumer	Provider	Policy Enforced On
Ingress or **Egress**	**EPG**	**EPG**	**Ingress Leaf**: if dst EP is learned. **Egress Leaf**: if dst EP is not learned.
Ingress	**EPG**	**L3OUT EPG**	**Consumer Leaf** (non-Border Leaf)
Ingress	**L3Out EPG**	**EPG**	**Provider Leaf** (non-Border Leaf)

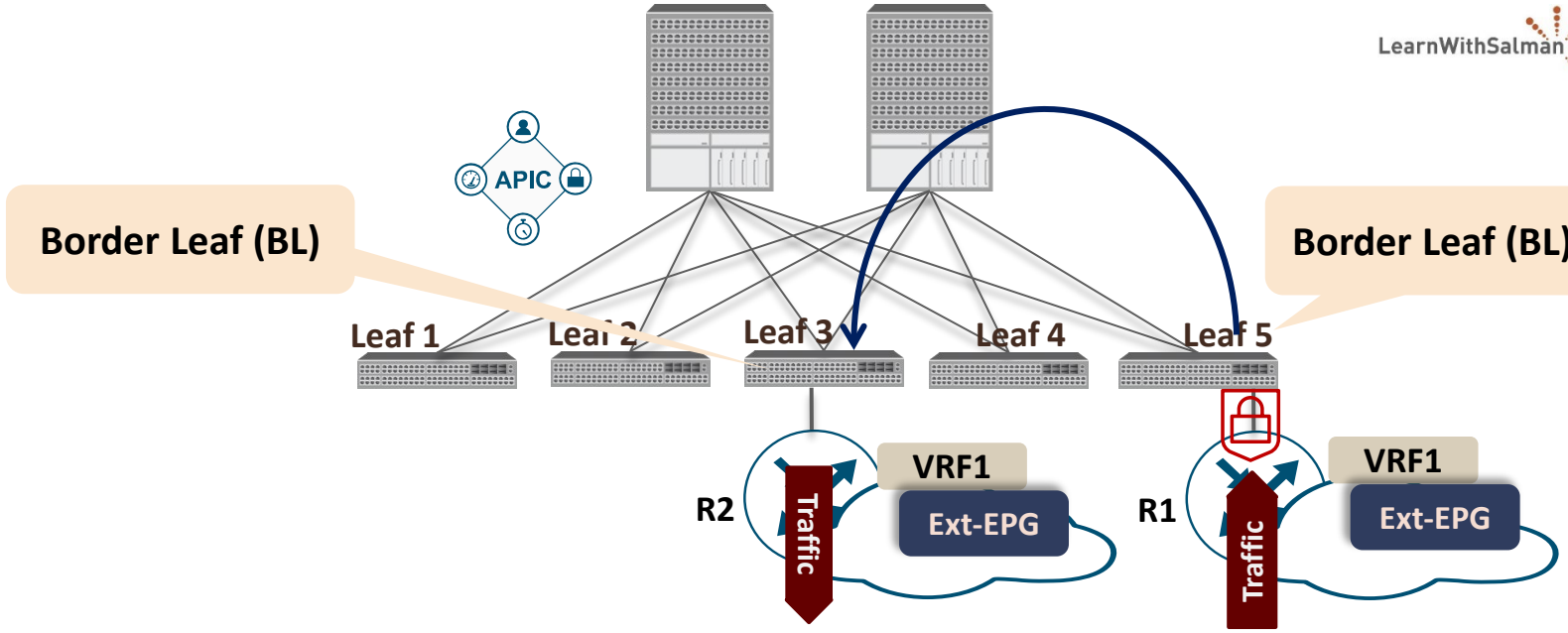
Where is the policy Applied?



Policy Control Enforcement Direction: Egress | **Ingress**

Enforcement Direction	Consumer	Provider	Policy Enforced On
Ingress or **Egress**	**EPG**	**EPG**	**Ingress Leaf**: if dst EP is learned. **Egress Leaf**: if dst EP is not learned.
Ingress	**EPG**	**L3OUT EPG**	**Consumer Leaf** (non-Border Leaf)
Ingress	**L3Out EPG**	**EPG**	**Provider Leaf** (non-Border Leaf)
Egress	**EPG**	**L3Out EPG**	Border Leaf to non-Border Leaf traffic: • **Border Leaf (BL):** if dst EP is learned. • **Non-Border Leaf (BL):** if dst EP is not learned. Non-Border Leaf to Border Leaf traffic: • **Border Leaf (BL)**
Egress	**L3Out EPG**	**EPG**	

Where is the policy Applied?



Policy Control Enforcement Direction: Egress | **Ingress**

Enforcement Direction	Consumer	Provider	Policy Enforced On
Ingress or **Egress**	**EPG**	**EPG**	**Ingress Leaf**: if dst EP is learned. **Egress Leaf**: if dst EP is not learned.
Ingress	**EPG**	**L3OUT EPG**	**Consumer Leaf** (non-Border Leaf)
Ingress	**L3Out EPG**	**EPG**	**Provider Leaf** (non-Border Leaf)
Egress	**EPG**	**L3Out EPG**	Border Leaf to non-Border Leaf traffic: • **Border Leaf (BL):** if dst EP is learned. • **Non-Border Leaf (BL):** if dst EP is not learned. Non-Border Leaf to Border Leaf traffic: • **Border Leaf (BL)**
Egress	**L3Out EPG**	**EPG**	
Ingress or **Egress**	**L3Out EPG**	**L3Out EPG**	Ingress Leaf

Thanks for watching!


LearnWithSalman