

Symmetric State

Designing for Multi-site Stateful Inspection in the Era of Extended VLANs and VRFs

Tyler Conrad

Principal Engineer

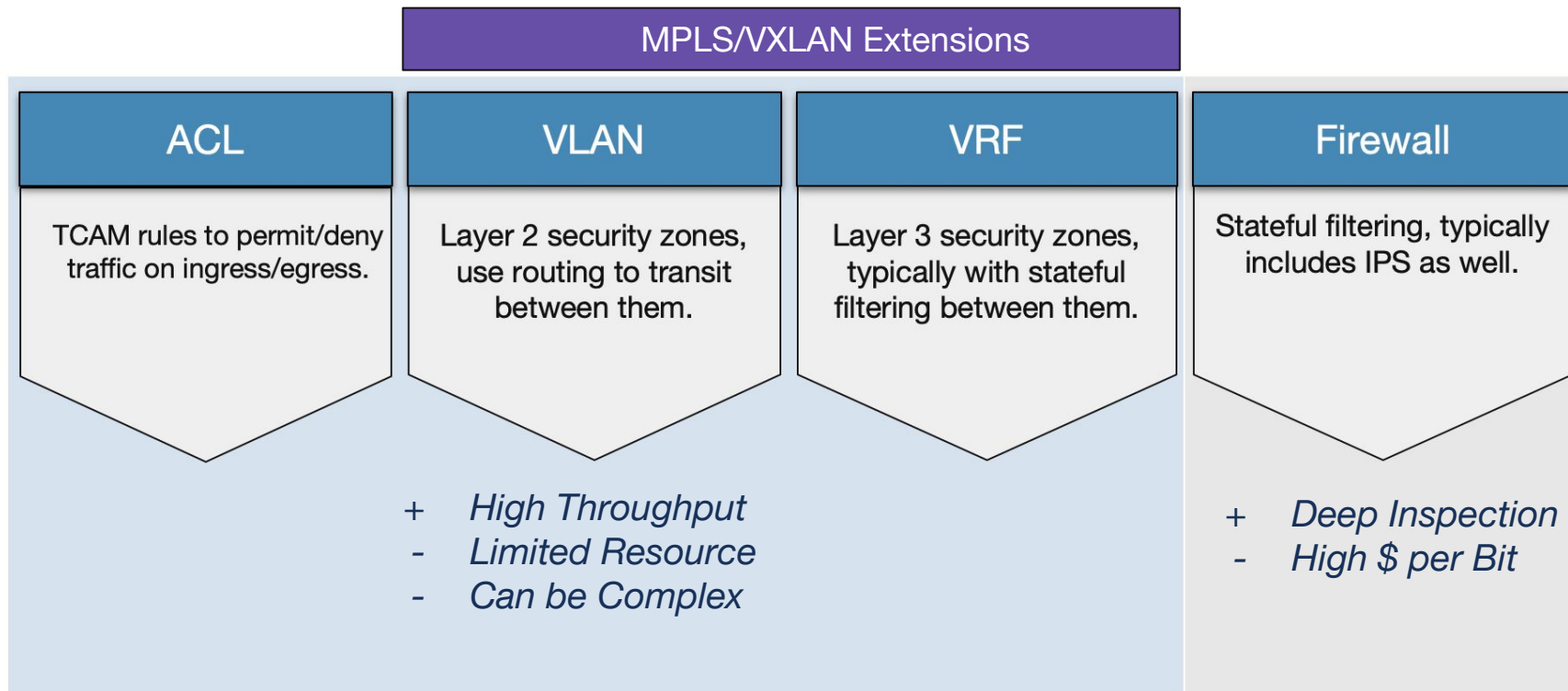
About me?

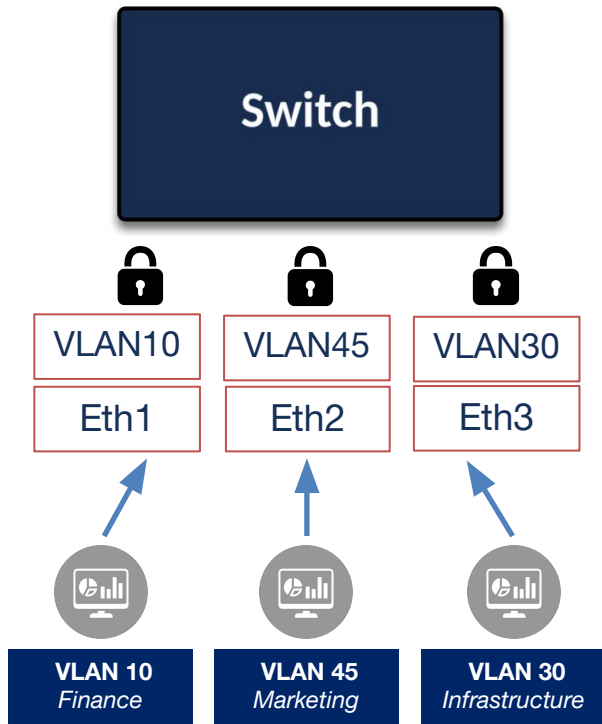
Principal Engineer at Arista
Networks, amateur electrician,
self-proclaimed “DCIE”.

This picture was taken out near
Hood ->



Segmentation Options





VLANs

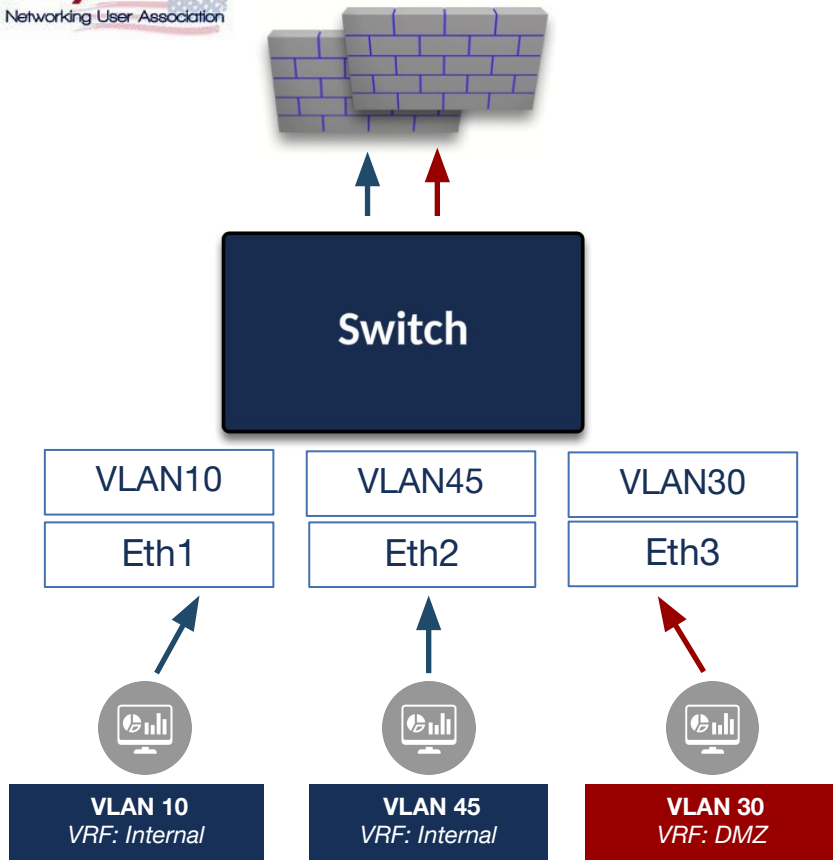
- Can segment a physical switch into multiple logical segments at Layer 2
- VLANs reduce the broadcast domain size
- VLANs can be spanned across the switches using Dot1Q trunk interfaces

```
switch(config)#vlan 45
switch(config-vlan-45)#name Marketing
switch(config-vlan-45)#show vlan 45
```

VLAN	Name	Status	Ports
------	------	--------	-------

45	Marketing	active	Eth1
----	-----------	--------	------

```
switch(config-vlan-45)#
```



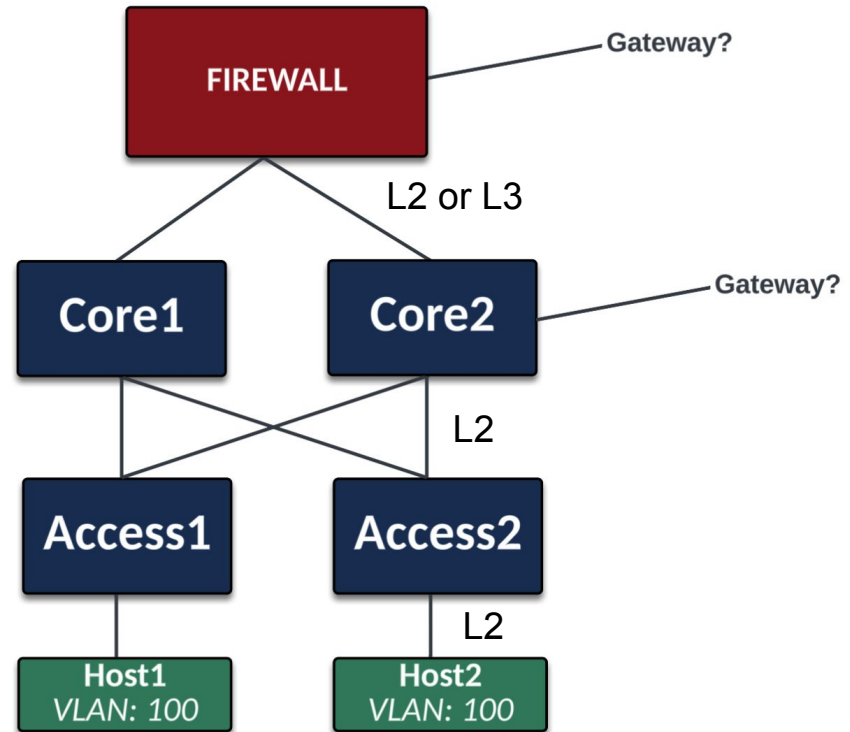
VRFs

- Can segment a physical switch into multiple logical segments at Layer 3
- VRFs carry a vrf-specific routing table
- VRFs can be extended between switches with Layer 3 links, or with encapsulation protocols (VXLAN/MPLS).

Typical Enterprise?

Lots of environments look something like this.

Gateway placement and topology are variable.



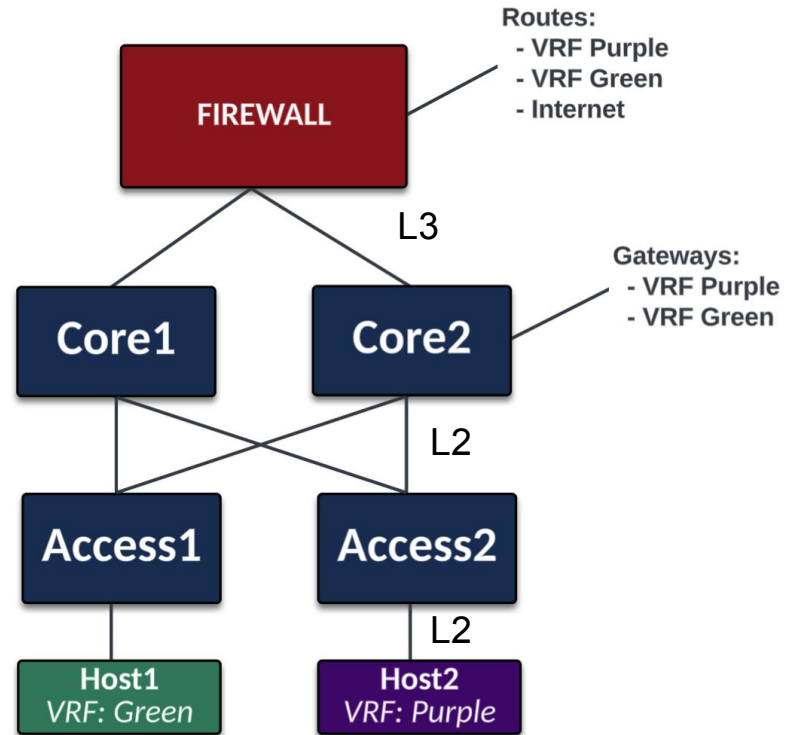
Why use VRFs?

VRF = Separation

Green <-> Firewall <-> Purple

Green <-> Green

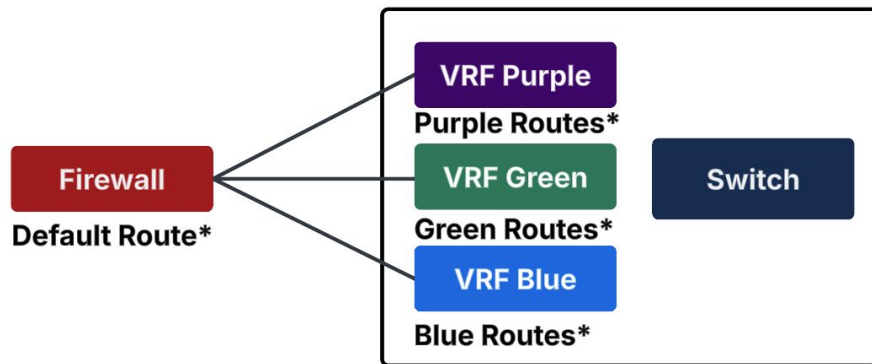
Purple <-> Purple



VRF Routing Approach

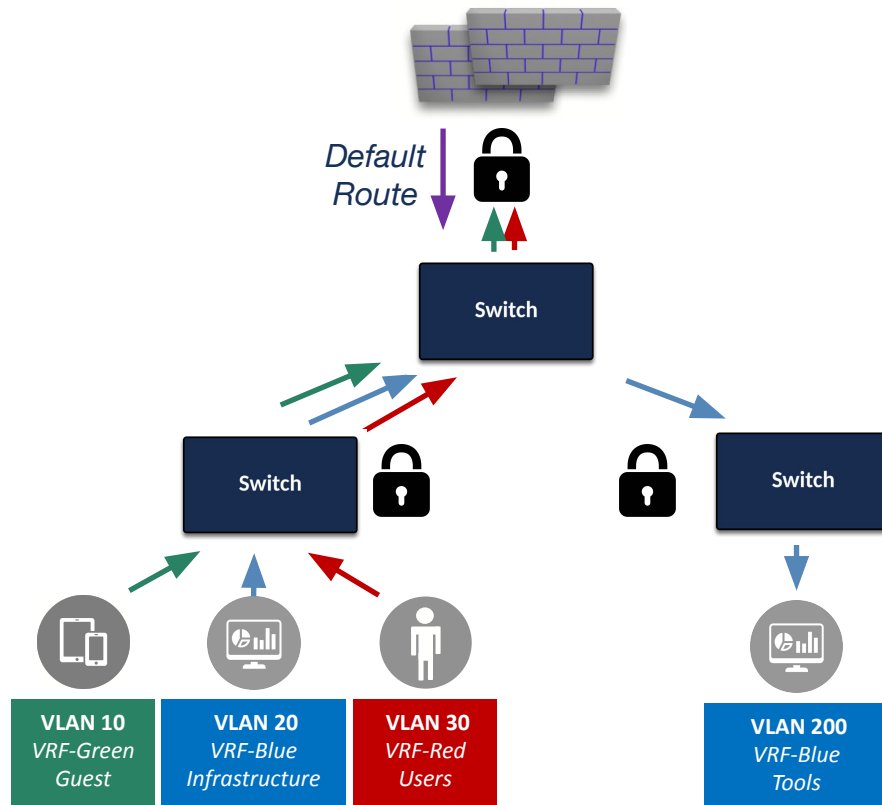
Firewall peering to network fabric.

Default-route-only is a common approach, using the firewall as a core router between VRFs



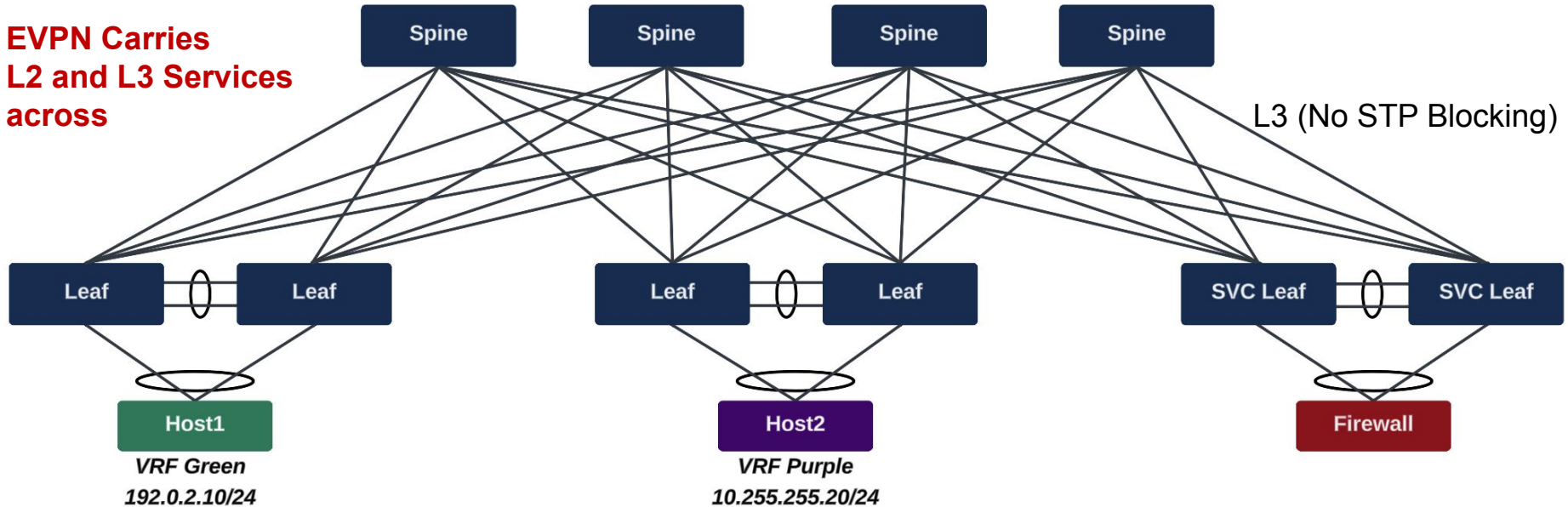
*Denotes Routes sent to peer (BGP or static)

Layering Security



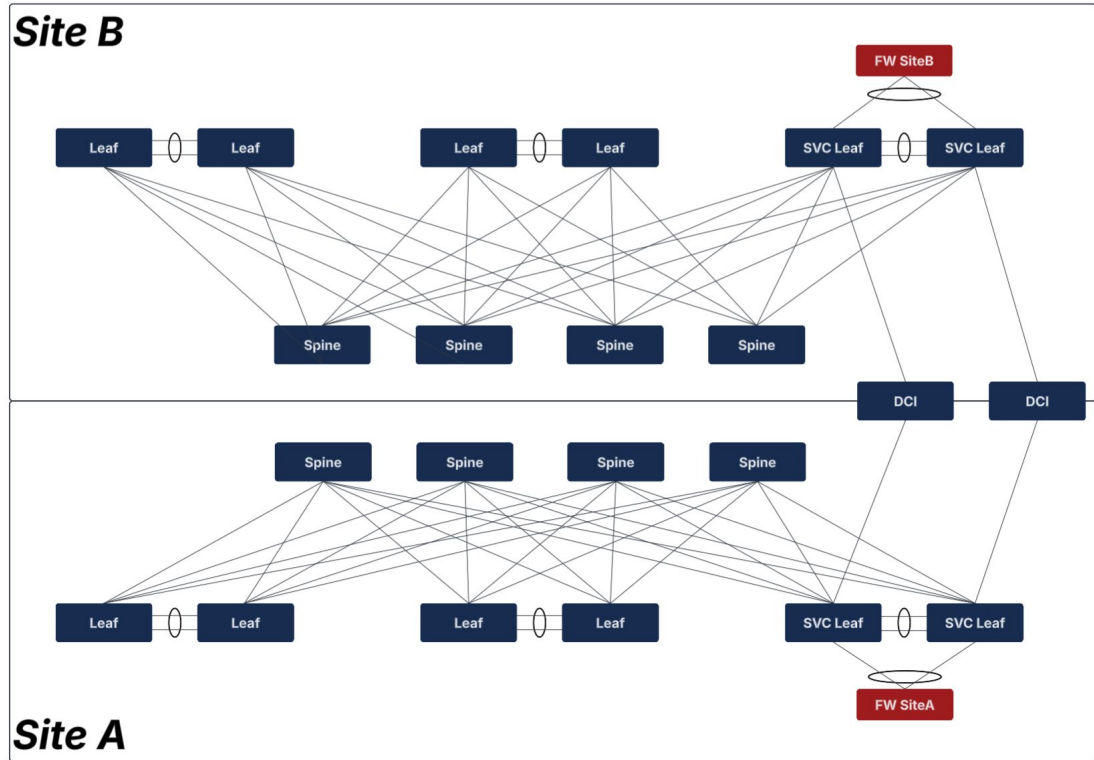
Why EVPN?

**EVPN Carries
L2 and L3 Services
across**



DCI

What happens when
we add a Second
Site/DCI into the mix?

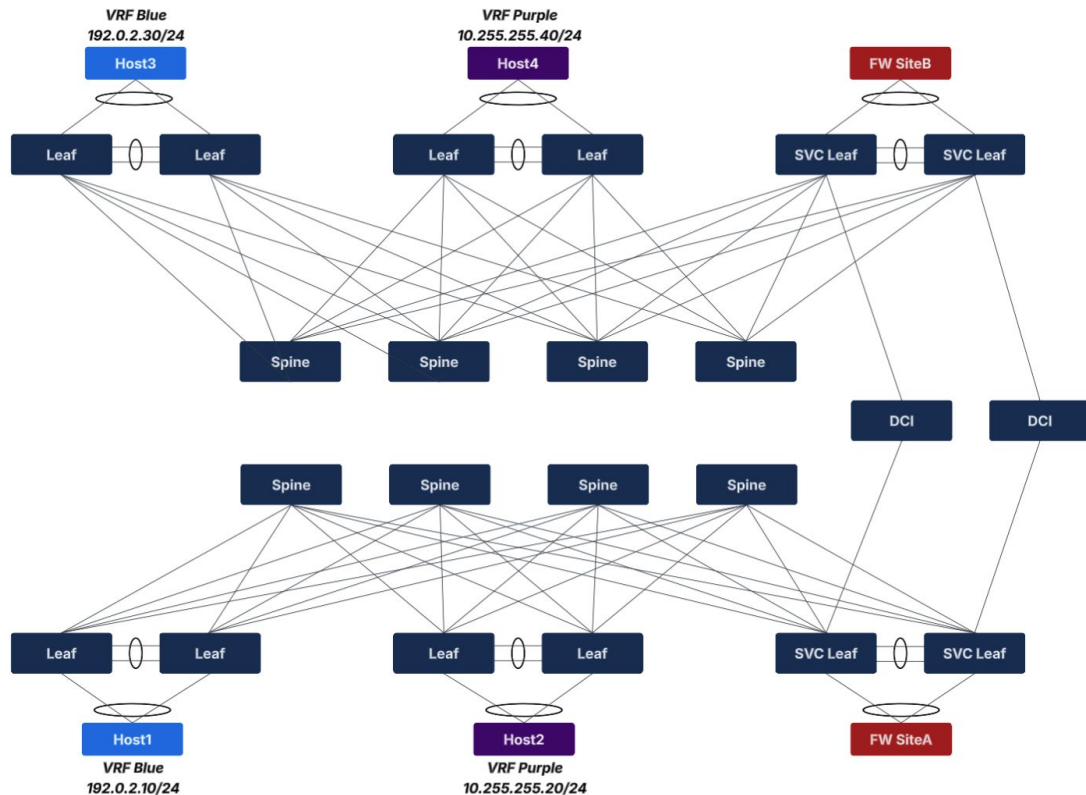


DCI

EVPN End-to-End

- VLANs extended
- VRFs extended

Operating like a
single DC...except
for those Firewalls...

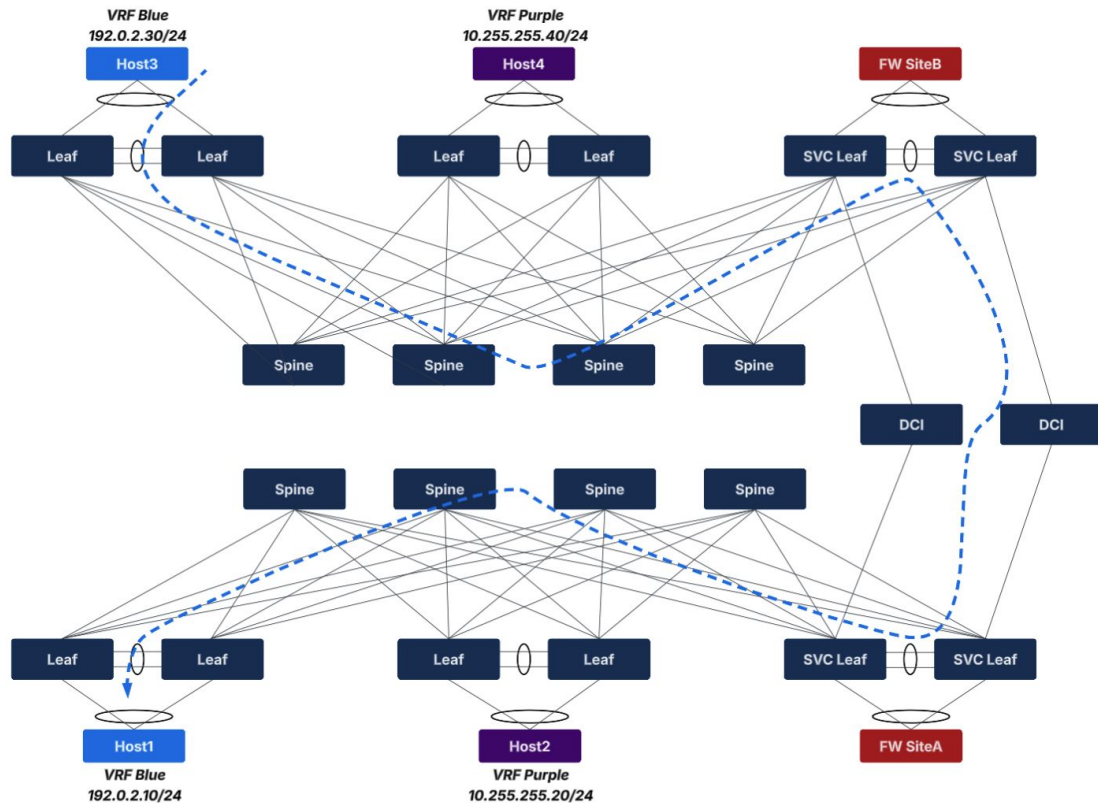


DCI

Example Flow:

- Host3 -> Host1.

So far, so good.

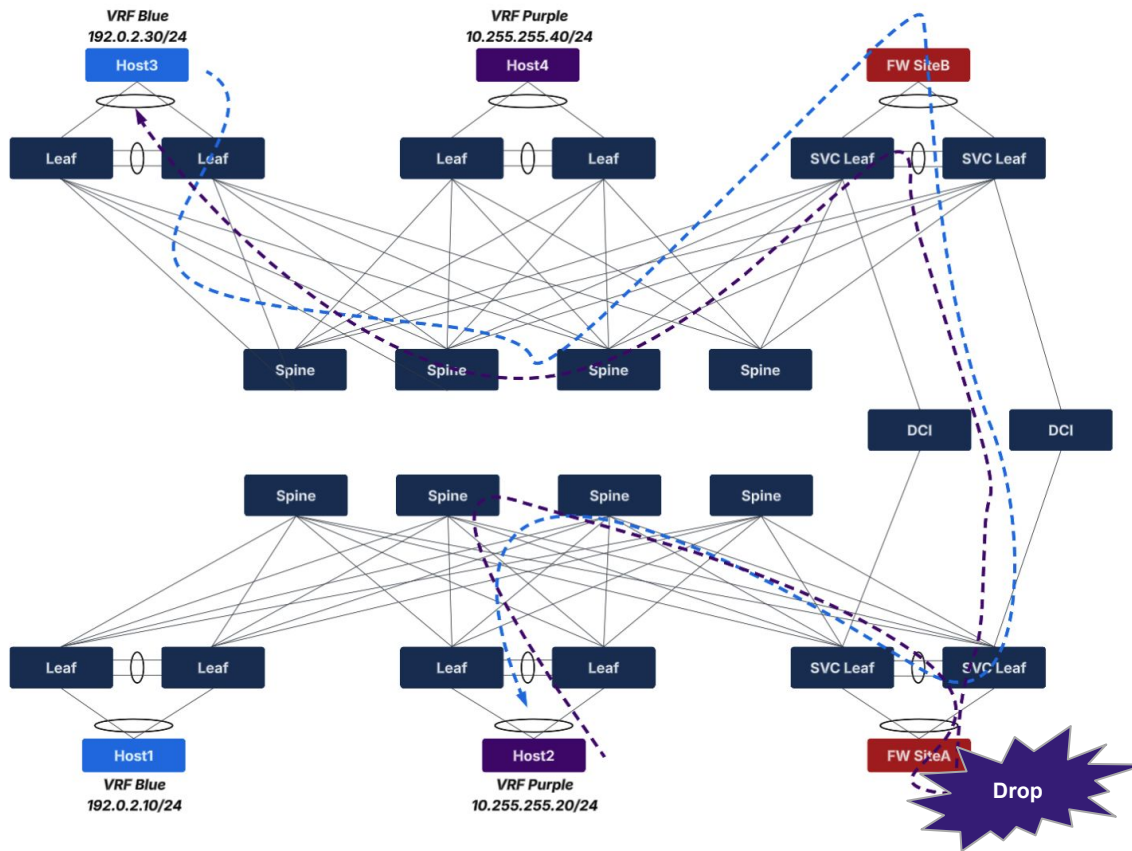


DCI

This is where it falls apart; Inter-Site w/ Inter-VRF

Blue is transmit path from Host3 -> Host2

Purple is return path from Host2 -> Host3



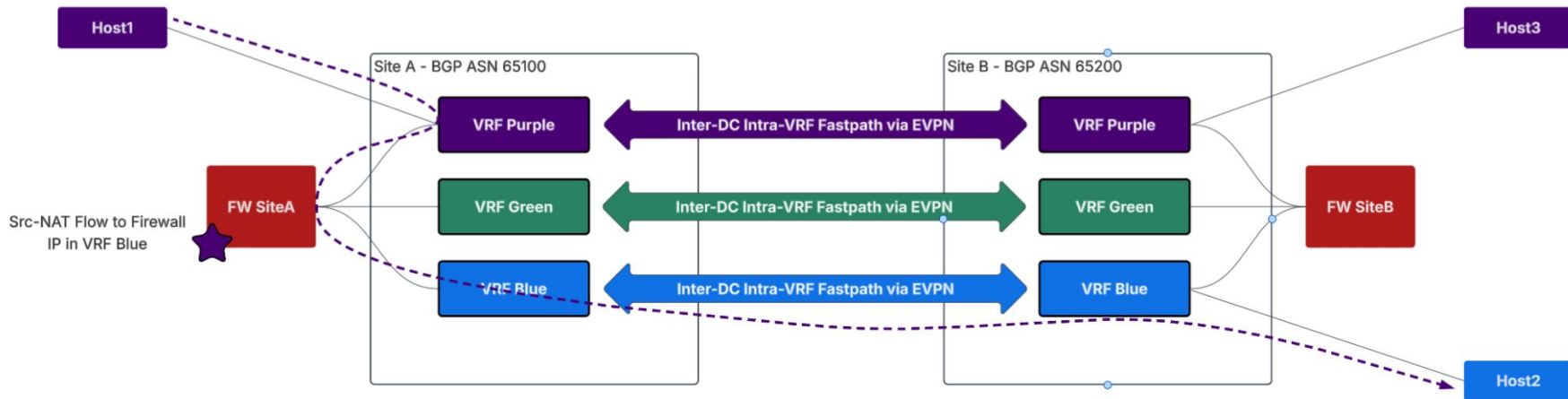
Problem Statement

Cross-Site, Cross-VRF traffic is difficult to maintain symmetric firewall state, leading to dropped traffic.

Solutions

Source-NAT

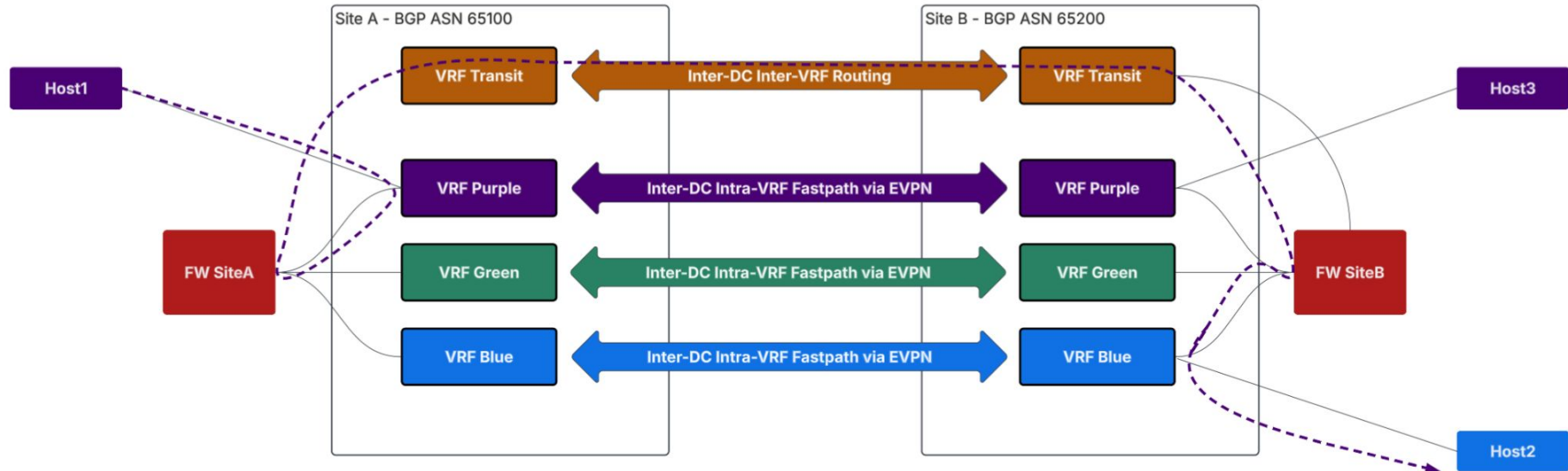
When crossing the firewall boundary, Source-NAT traffic to the firewall IP.
Con: Lose IP address visibility, and some apps break.



Transit VRF

We can instantiate a new vrf called “Transit”, that can carry all Inter-site, Inter-VRF traffic. Both firewalls will see all traffic.

Con: Double-Inspection



Transit VRF

Multiple Sites can participate in VRF Transit.

Not limited to pairs.

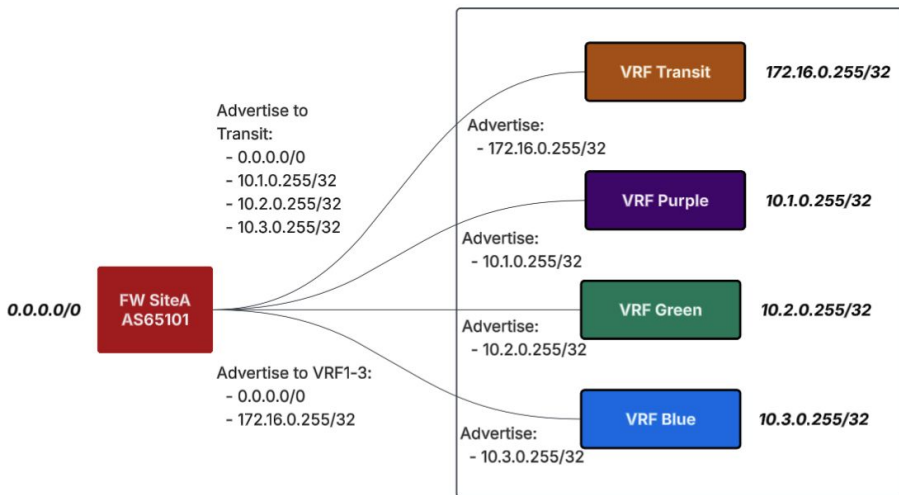
Traffic is always symmetric.



Transit VRF

How do we force routes via Transit?

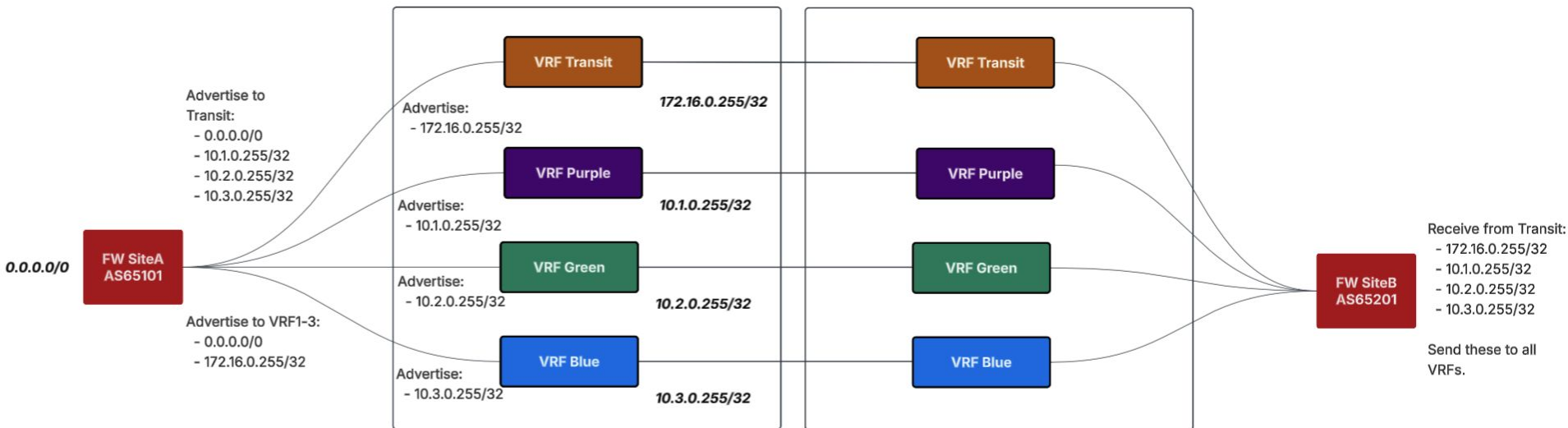
- Allow all routes inside VRF to flow as-is.
- Block local firewall from learning any remote routes inside tenant vrfs.
- Allow all routes from Transit.



VRF1-3 Routes not advertised to each other due to AS-Path Loop Prevention

Transit VRF

Expanded view - from SiteA -> SiteB.



Summary

- Firewalls have to see both directions of a flow, and will drop traffic that's seen as "out-of-state".
- Same-VRF, or single-VRF with multiple sites doesn't hit this problem.
- Not an easy problem to solve without trade-offs.
- BGP as a routing protocol enables predictable steering/filtering that lets this work.