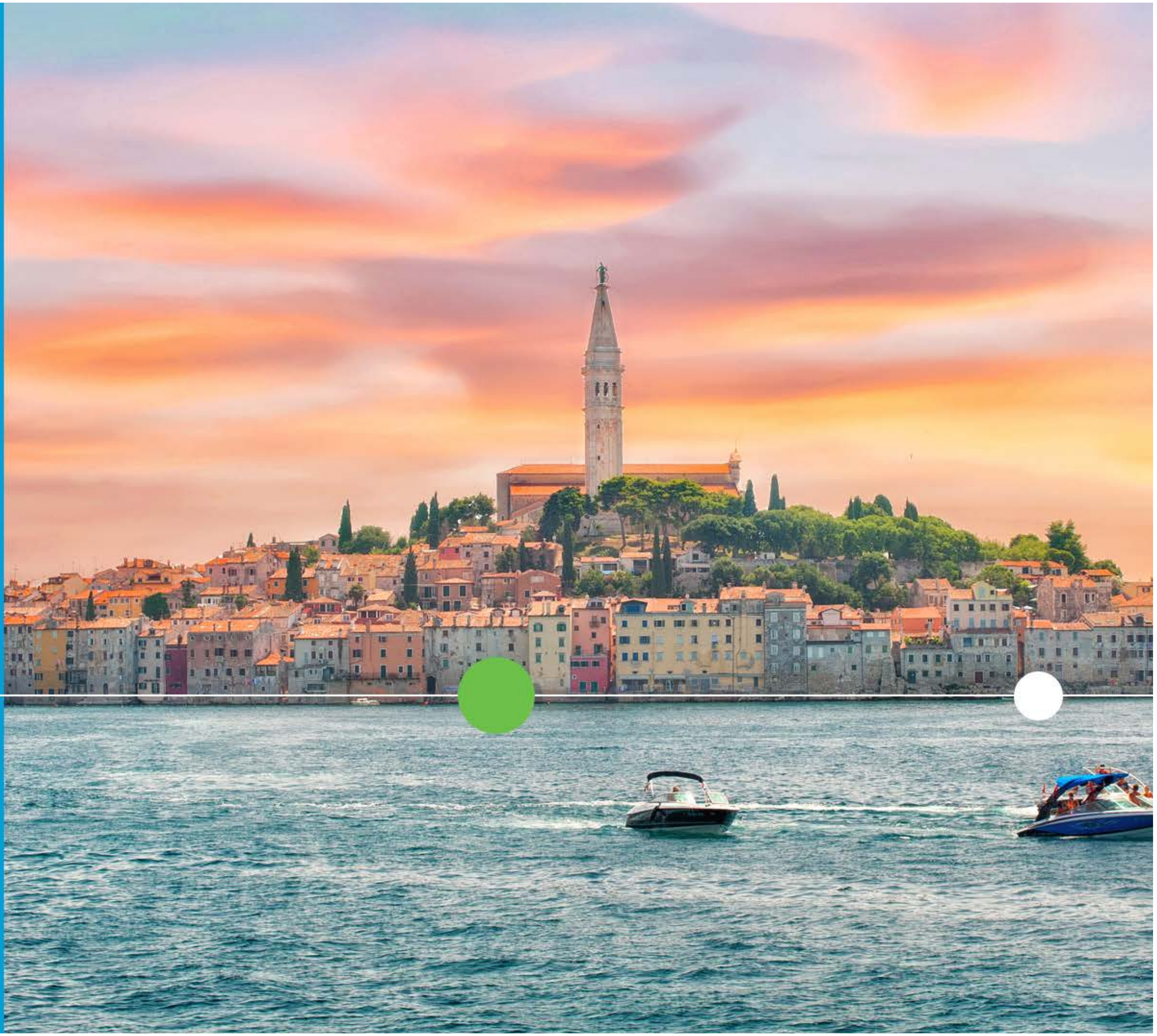
Cisco Connect

19 - 21 March, 2018
Rovinj, Croatia

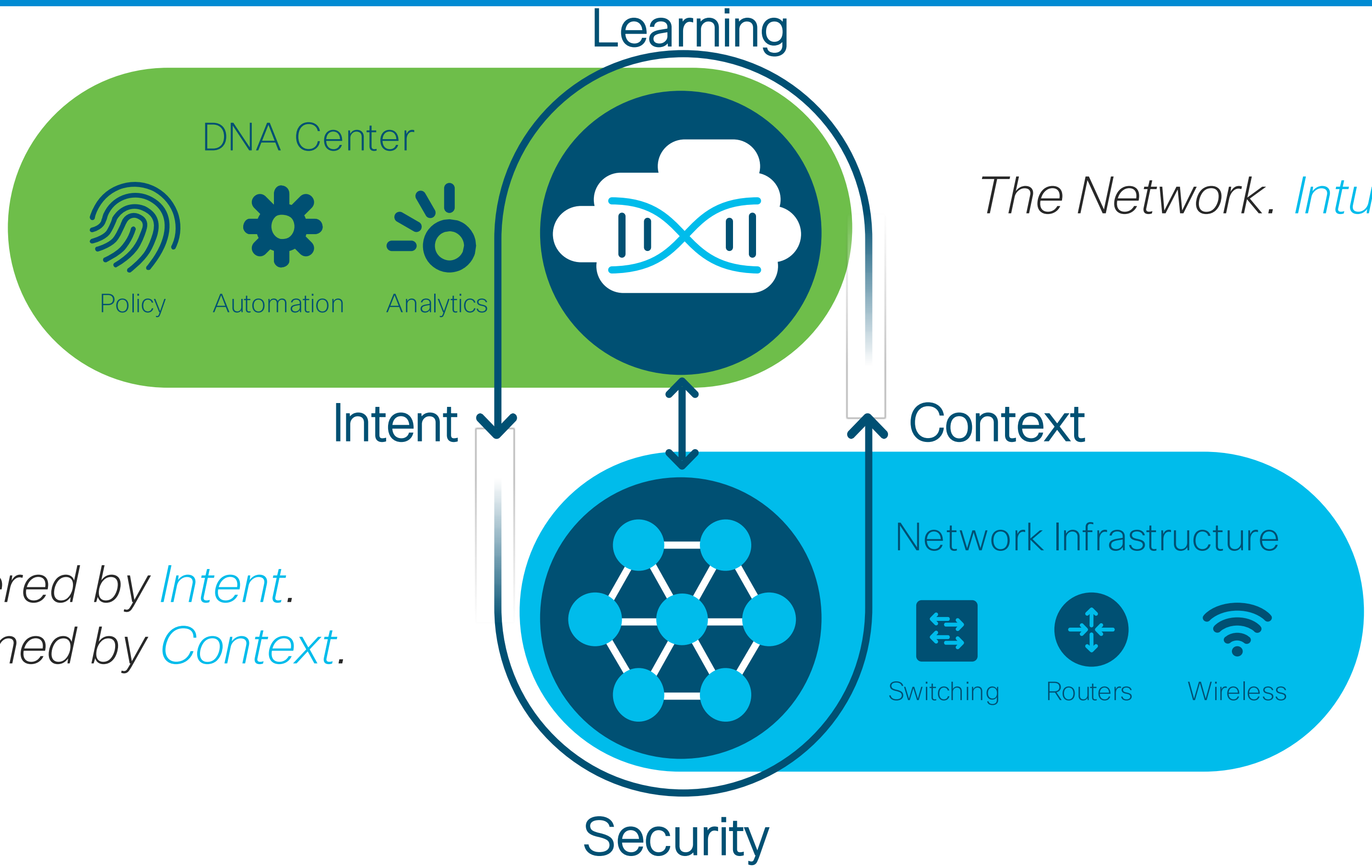


Cisco SD-Access - Connecting the Fabric to External Networks

Vedran Hafner, Systems Engineer

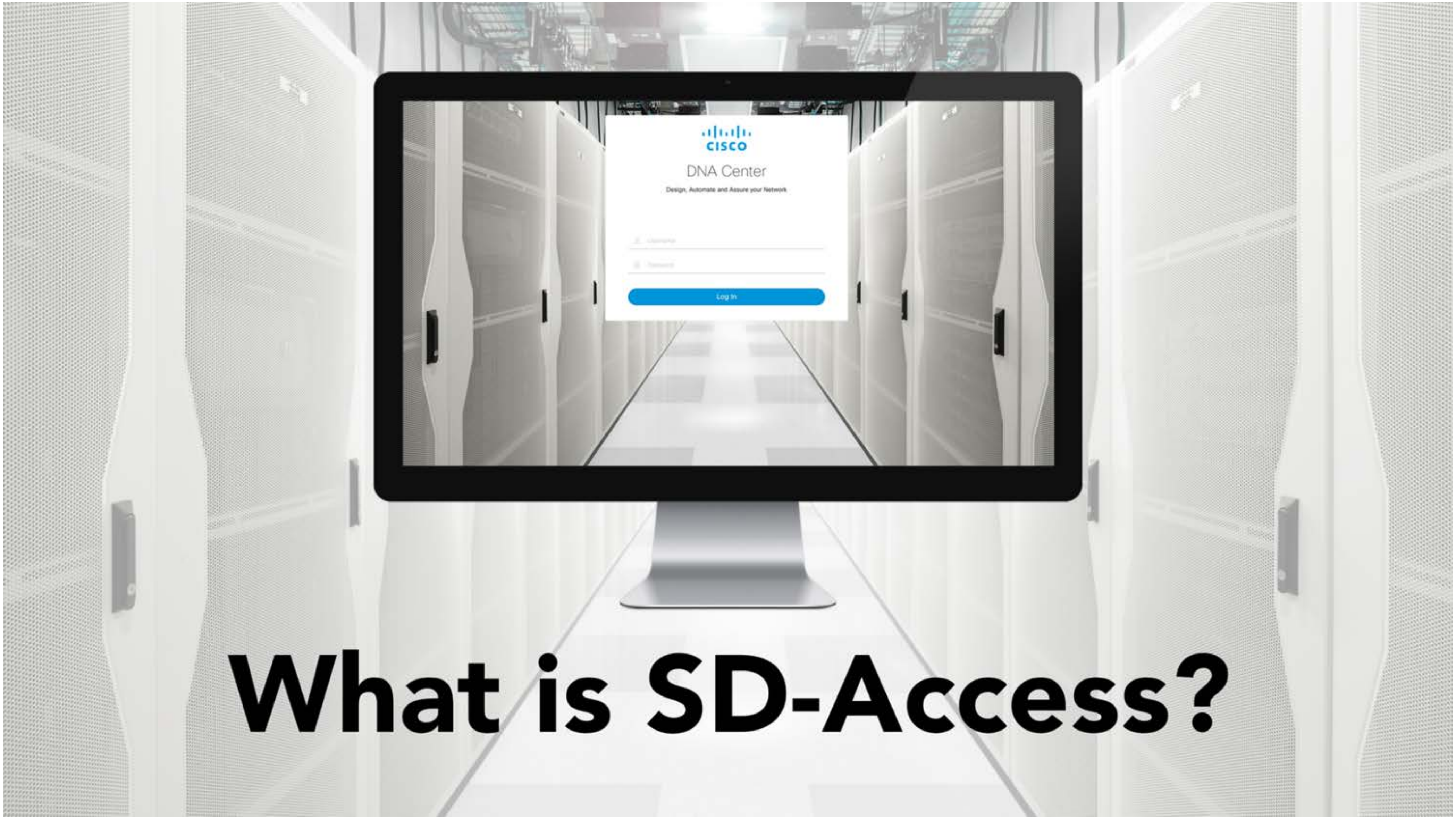
Cisco's Intent-based Networking

Cisco Connect



The Network. Intuitive.

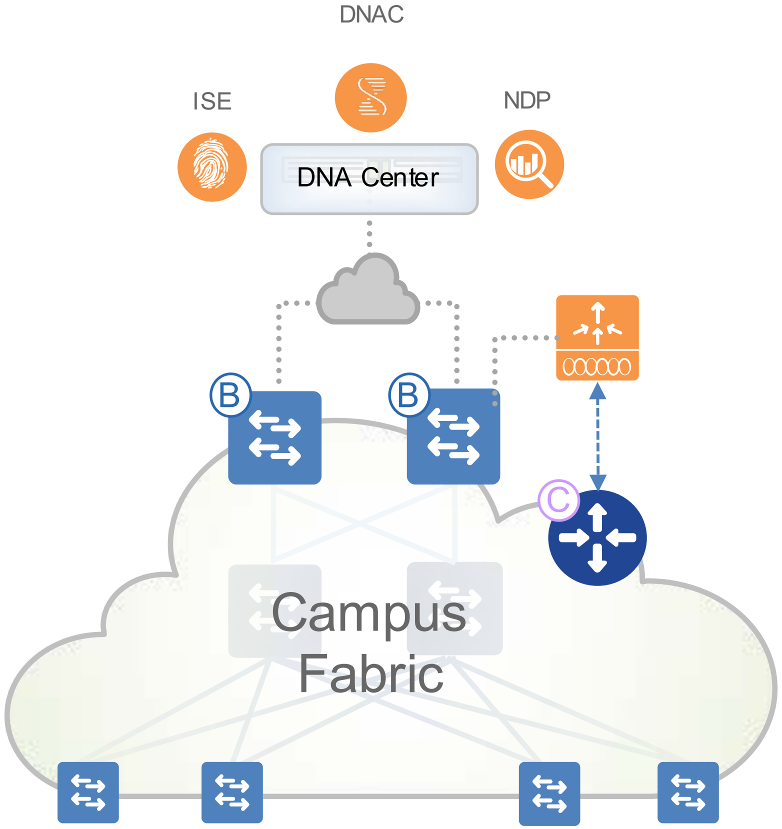
Powered by Intent.
Informed by Context.



What is SD-Access?

What is SD-Access?

Campus Fabric + DNA Center (Automation & Assurance)



- **SD-Access** – ***Available Aug 2017***

  GUI approach provides automation & assurance of all Fabric configuration, management and group-based policy.

  Leverages DNA Center to integrate external Service Apps, to orchestrate your entire LAN, Wireless LAN and WAN access network.

- **Campus Fabric** – ***Shipping Now***

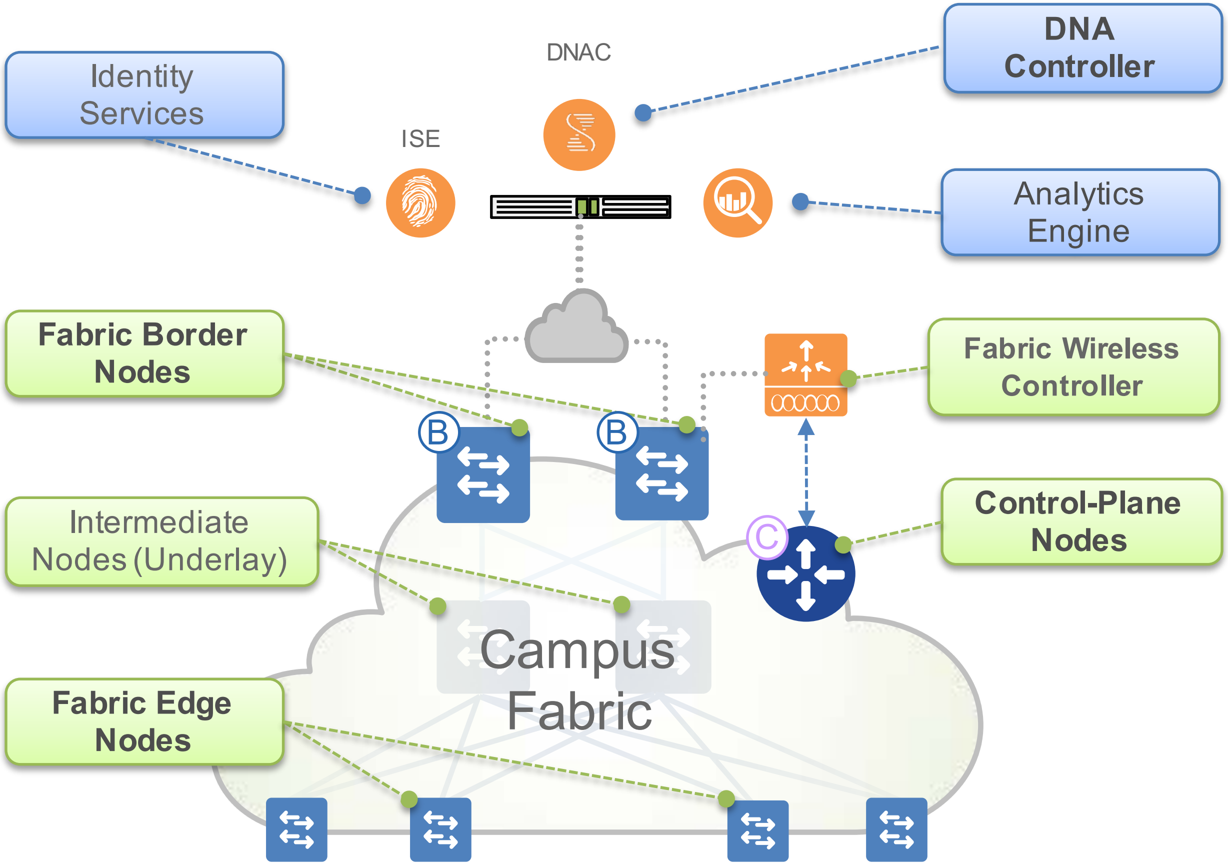
  CLI or API form of the new overlay Fabric solution for your enterprise Campus access networks.

  CLI approach provides backwards compatibility and customization, Box-by-Box. API approach provides automation via NETCONF / YANG.

  APIC-EM, ISE, NDP are all separate.

What is SD-Access?

Fabric Roles & Terminology



- **DNA Controller** – Enterprise SDN Controller (e.g. DNA Center) provides GUI management and abstraction via Apps that share context
- **Identity Services** – External ID System(s) (e.g. ISE) are leveraged for dynamic Endpoint to Group mapping and Policy definition
- **Analytics Engine** – External Data Collector(s) (e.g. NDP) are leveraged to analyze Endpoint to App flows and monitor fabric status

- **Control-Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A Fabric device (e.g. Core) that connects External L3 network(s) to the SDA Fabric
- **Fabric Edge Nodes** – A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric
- **Fabric Wireless Controller** – A Fabric device (WLC) that connects Wireless Endpoints to the SDA Fabric

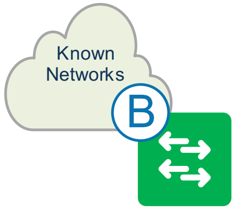
Cisco
Connect

SDA Fabric Border Functionality
What do customers need to know about the Fabric Border?

SD-Access Border

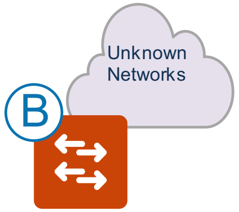
Border Nodes – Border and Default Border

Cisco Connect



Border

- Connects the Campus Fabric to **Known networks**. (Use case 2.1 and 2.2)
  - part of your company network
- **Known networks are generally WAN, DC, Shared Services, etc.**
- Responsible for advertising prefixes **to (import)** and **from (export)** the local fabric and external domain.



Default Border

- Connects the Campus Fabric to **Un-Known networks** (Use case 1)
  - not part of the company network
- **Un-known networks are generally the Internet and/or Public Cloud.**
- Responsible for advertising prefixes **only from (export)** the local fabric to external domain.

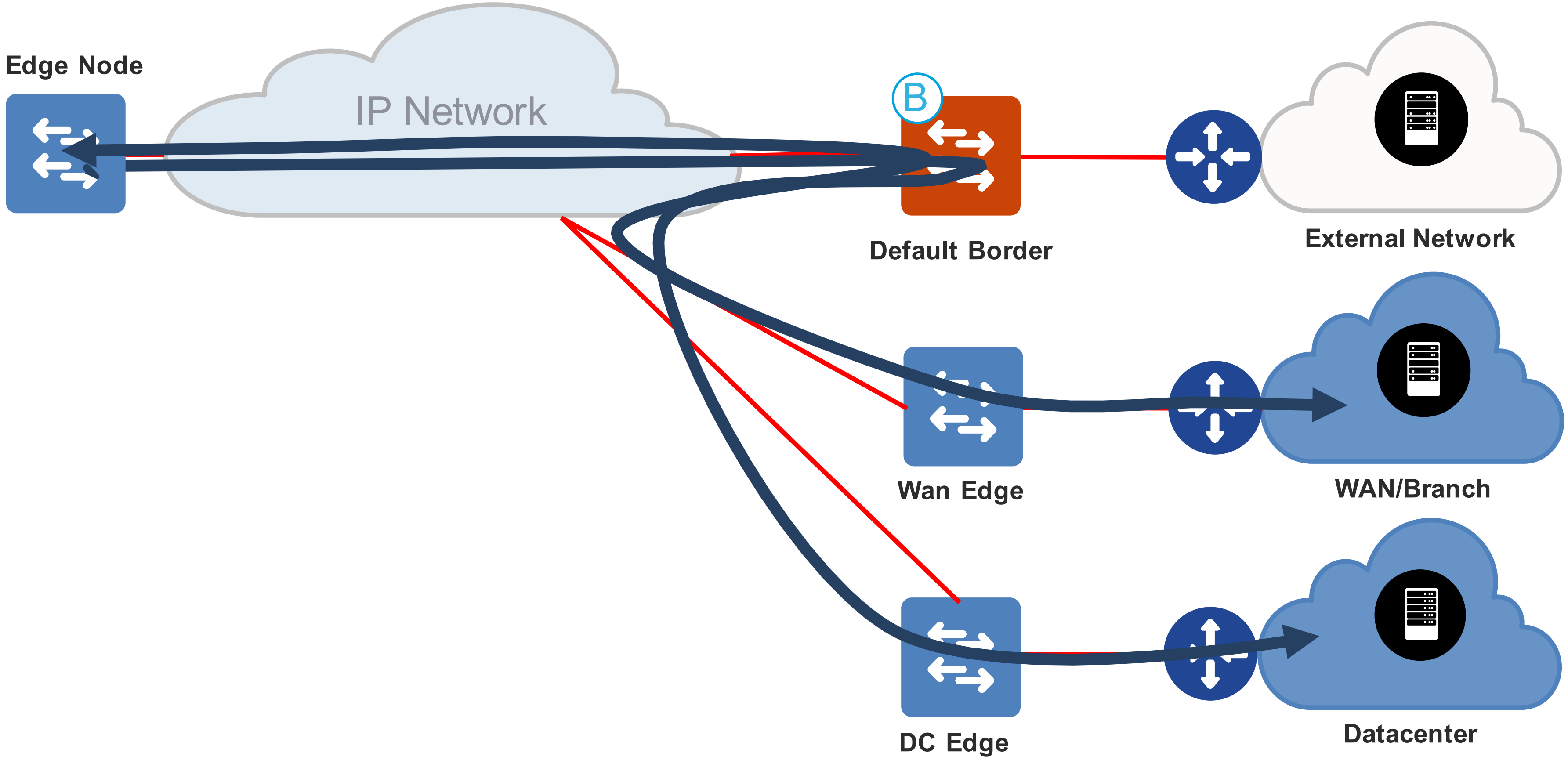
Cisco
Connect

Why Border Vs Default Border

SD-Access Fabric

Why Border vs Default Border?

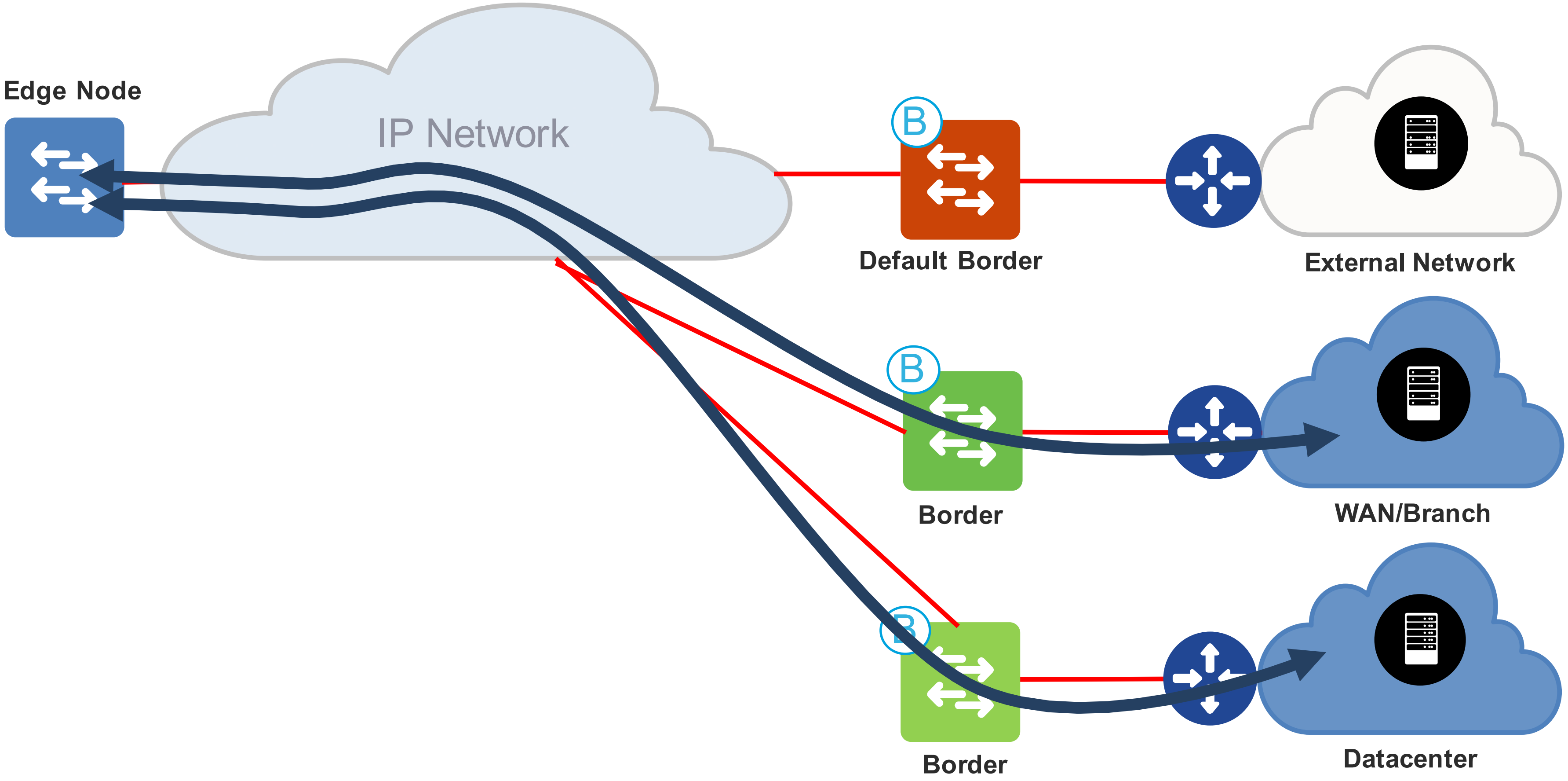
Cisco Connect



SD-Access Fabric

Why Border vs Default Border?

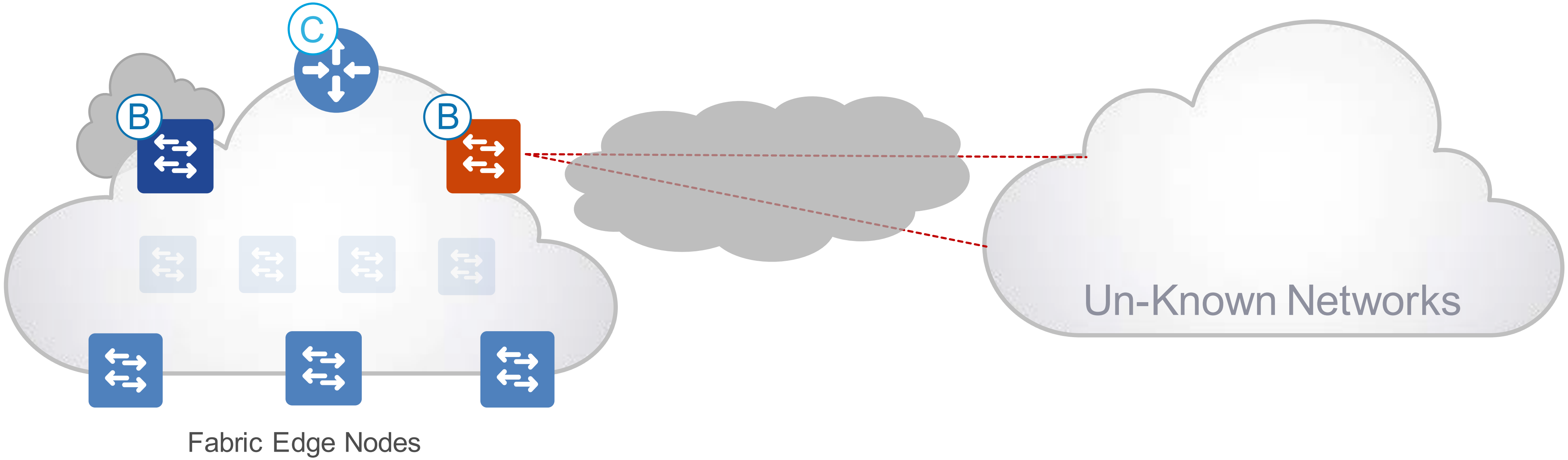
Cisco Connect



SD-Access Border Deployment Options

Use Case 1 : SDA fabric Connecting to Unknown Networks

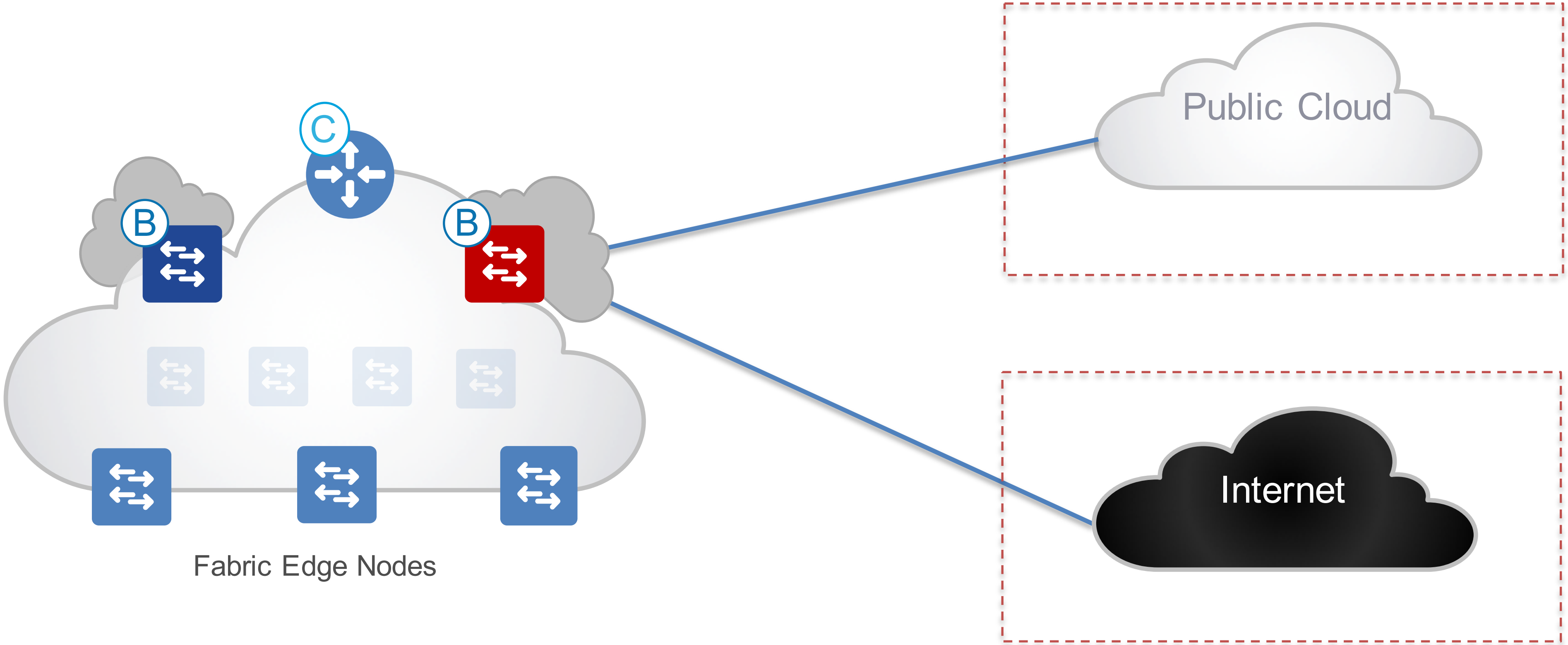
Cisco Connect



SD-Access Border Deployment Options

Use Case 1: SDA fabric Connecting to Unknown Networks – A Closer Look

Cisco Connect

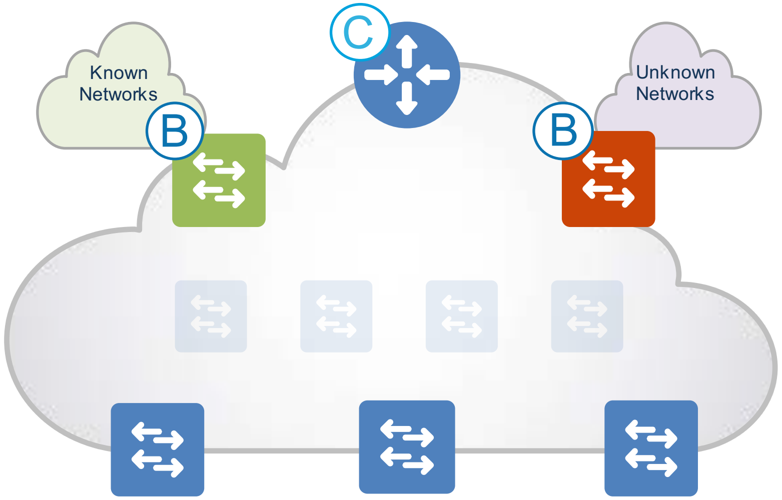


SD-Access Border

Use Case 1 : SDA fabric Connecting to Unknown Networks

Cisco Connect

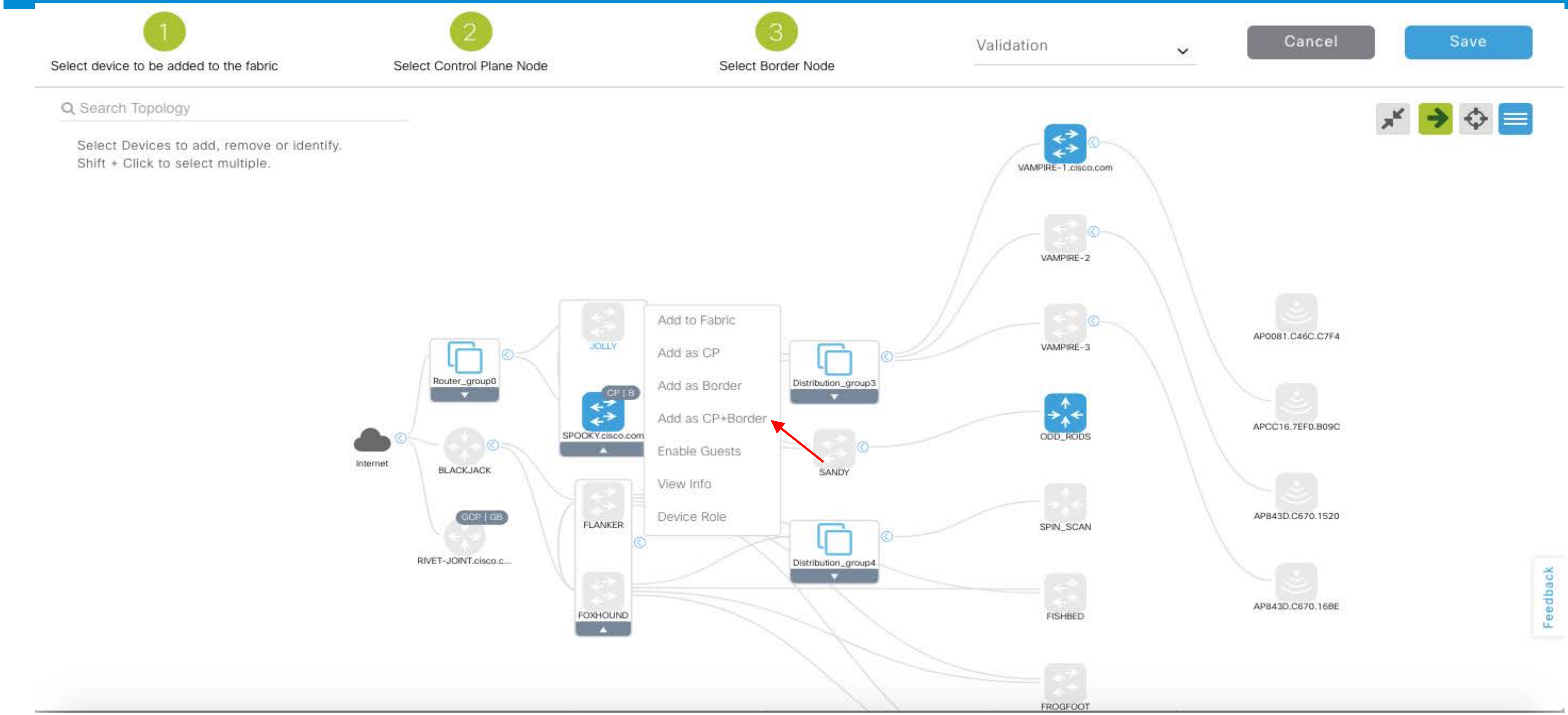
- **Default Border** is a "Gateway of Last Resort" for unknown destinations
- Connects to any "unknown" IP prefixes (e.g. Internet, Public Cloud, 3rd Party, etc.)
- Exports all internal IP Pools outside (as aggregate) into traditional IP routing protocol(s).
- Default Border is a "default" domain exit point, if no other (specific) entry present in Map System.
- Outside hand-off requires mapping the prefix context (VRF & SGT) from one domain to another.



Fabric Edge Nodes

SD-Access Border Deployment Options

Use Case 1 : SDA fabric Connecting to Unknown Networks – Automation



1 Select device to be added to the fabric

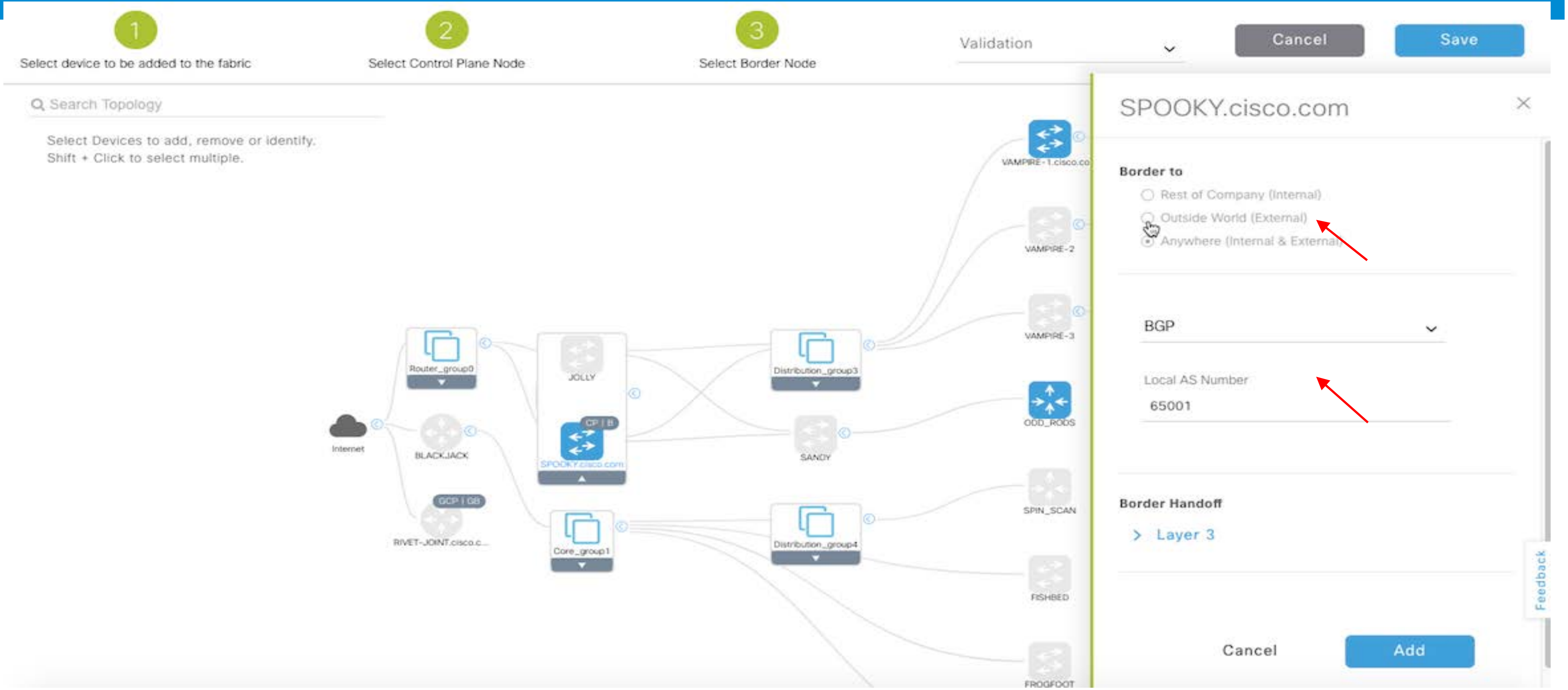
2 Select Control Plane Node

3 Select Border Node

Select Devices to add, remove or identify.
Shift + Click to select multiple.

SD-Access Border Deployment Options

Use Case 1 : SDA fabric Connecting to Unknown Networks – Automation



1 Select device to be added to the fabric

2 Select Control Plane Node

3 Select Border Node

Select Devices to add, remove or identify.
Shift + Click to select multiple.

SPOOKY.cisco.com

Border to

- ○ Rest of Company (Internal)
- ○ Outside World (External)
- ● Anywhere (Internal & External)

BGP

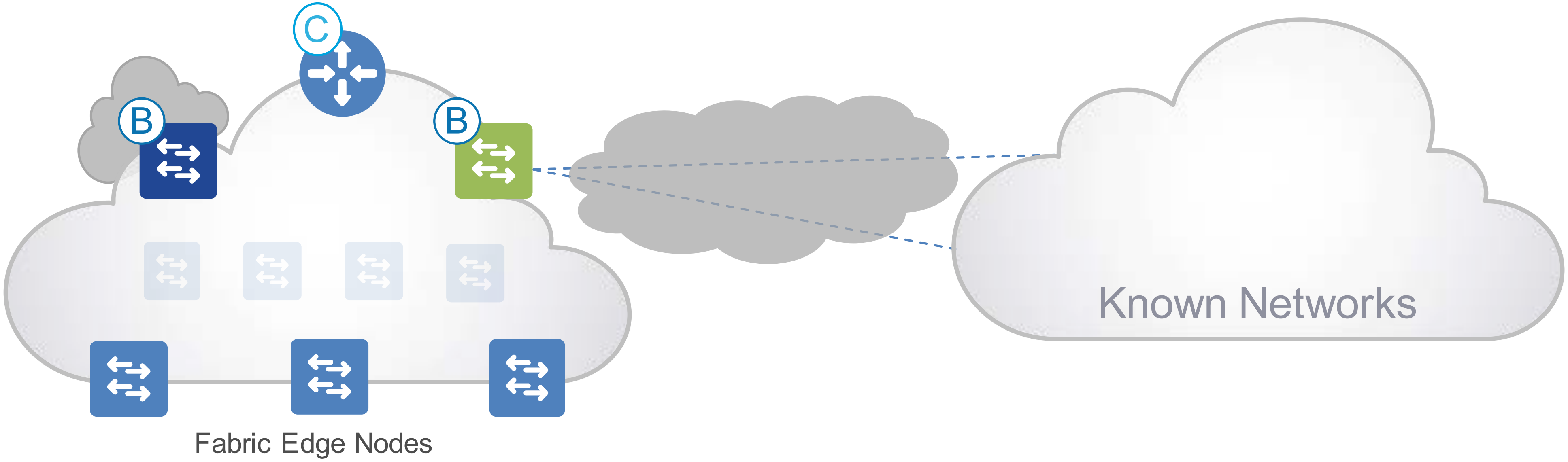
Local AS Number: 65001

Border Handoff

> Layer 3

SD-Access Border Deployment Options

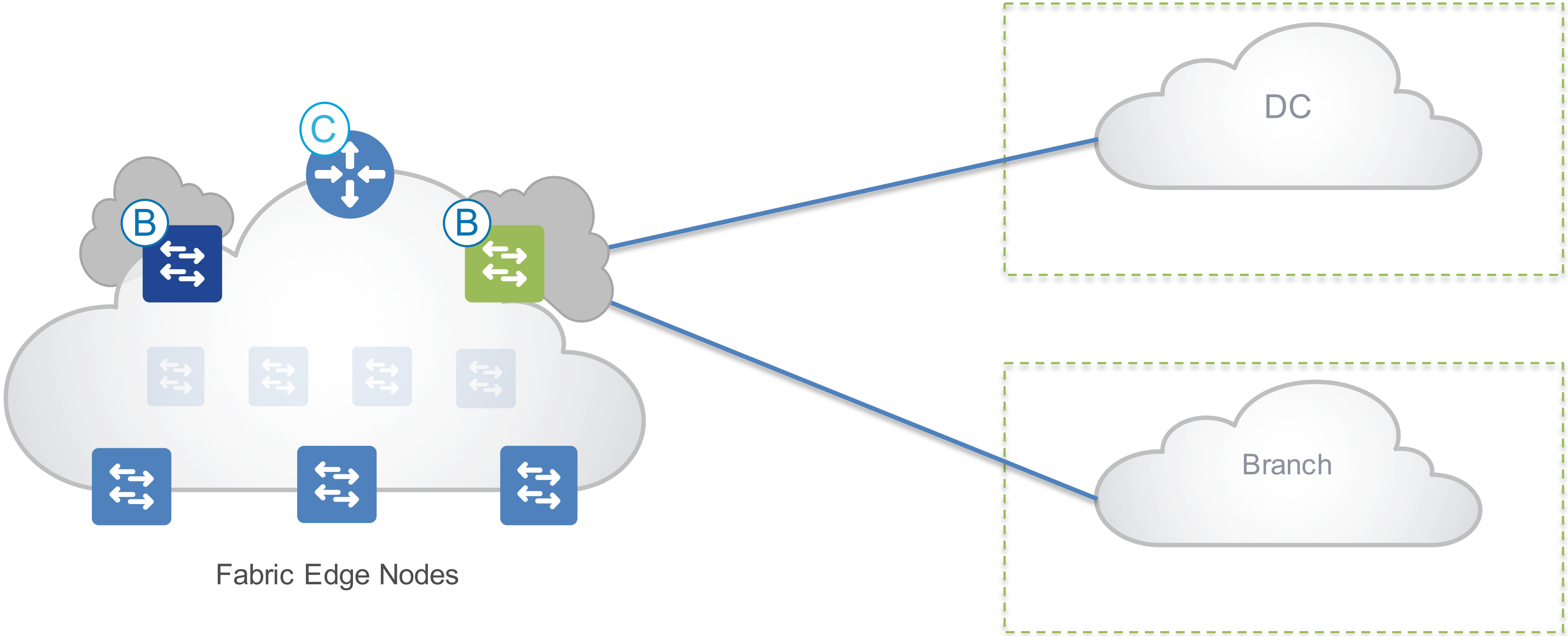
Use Case 2.1 : SDA fabric Connecting to known Networks



SD-Access Deployment Options

Use Case 2.1 : SDA fabric Connecting to known Networks – A Closer Look

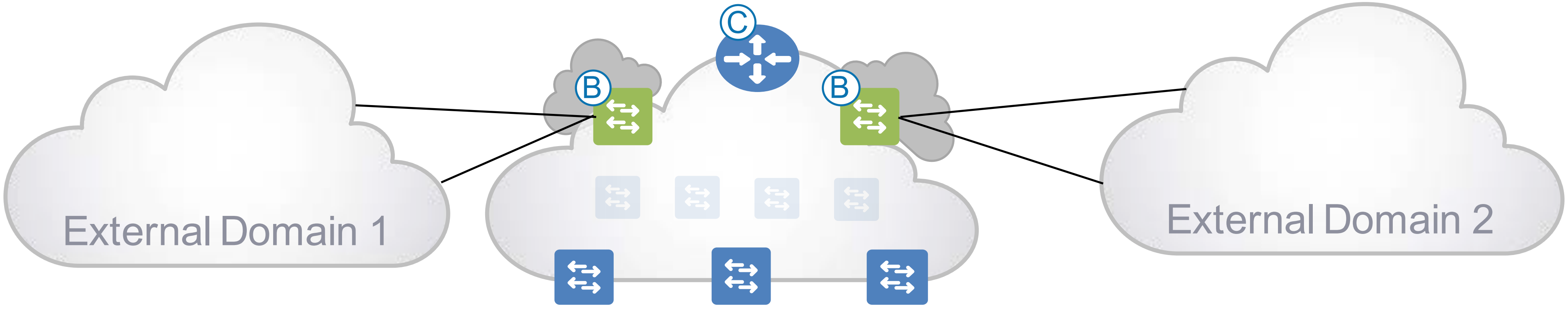
Cisco Connect



SD-Access Border Deployment Options

Use Case 2.2 : SDA fabric as a Transit Network

Cisco Connect



Fabric Edge Nodes

SD-Access Border

Use Case 2 : SDA fabric Connecting to known Networks

Cisco Connect

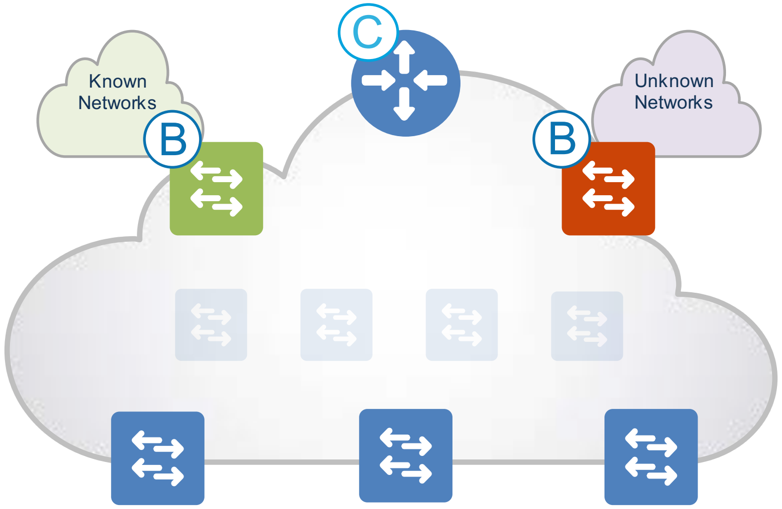
- **Border**

- Connects to any “known” IP subnets attached to the outside network (e.g. DC, WLC, FW, etc.)

- Exports all internal IP Pools to outside (as aggregate), using a traditional IP routing protocol(s).

- Imports and registers (known) IP subnets from outside, into the Fabric Control Plane System

- Outside hand-off requires mapping the prefix context (VRF & SGT) from one domain to another.

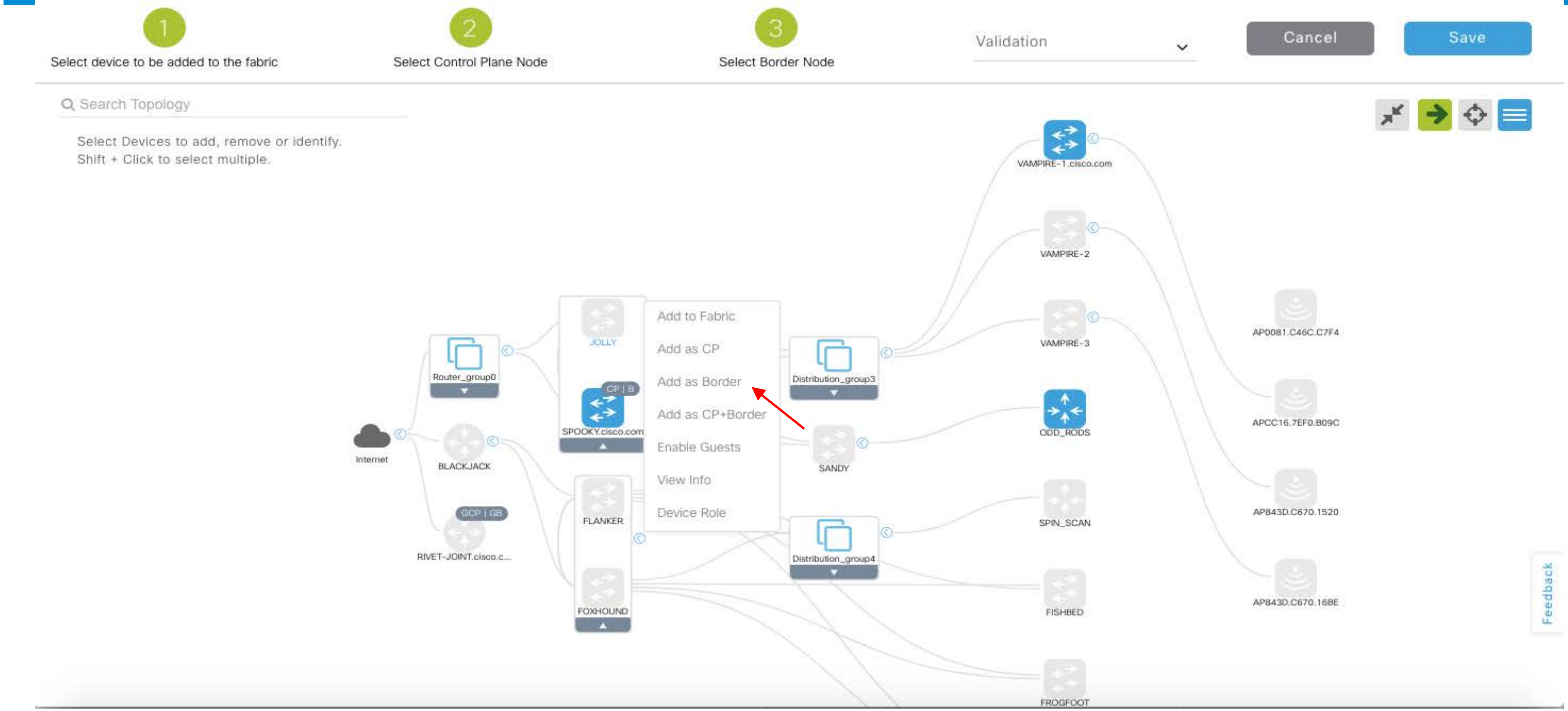


Fabric Edge Nodes

SD-Access Border Deployment Options

Use Case 2 : SDA fabric Connecting to known Networks – Automation

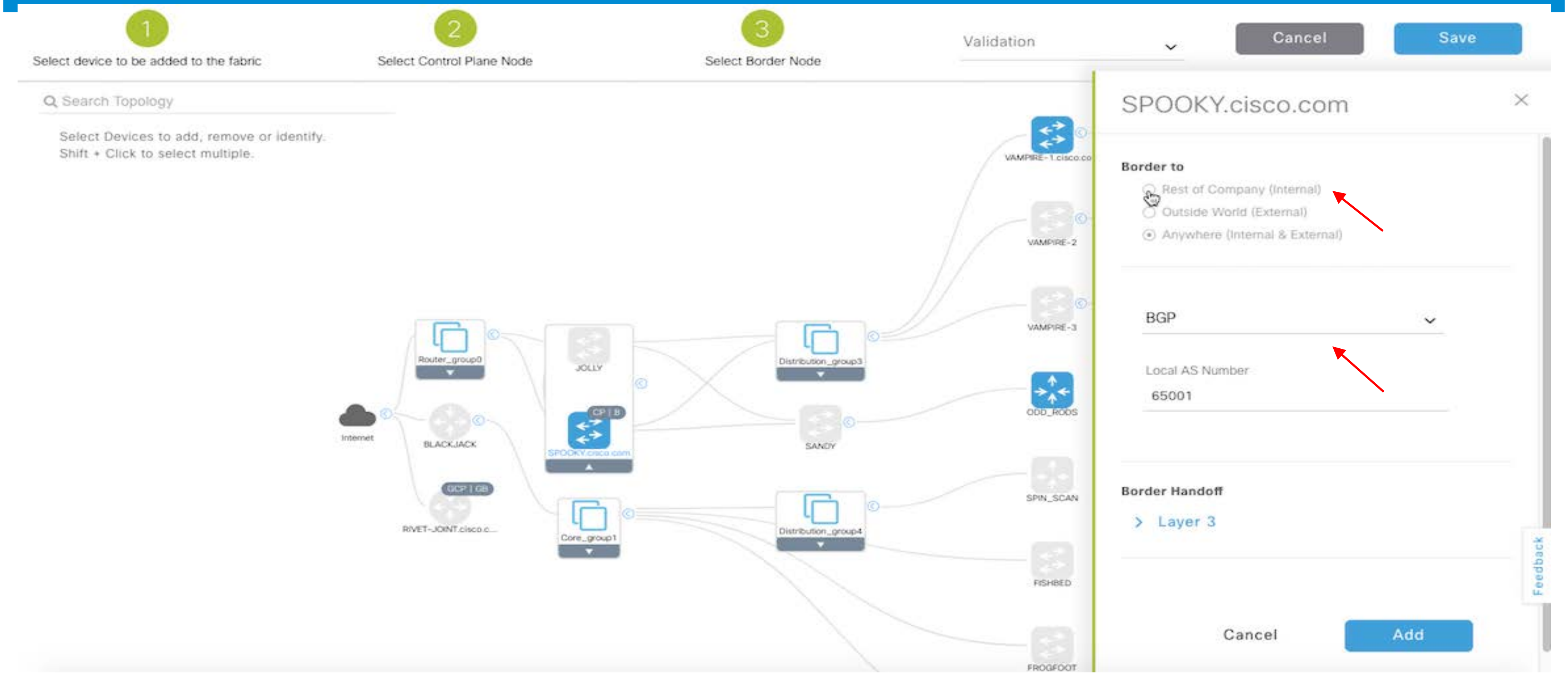
Cisco Connect



SD-Access Border Deployment Options

Use Case 2 : SDA fabric Connecting to known Networks – Automation

Cisco Connect



1 Select device to be added to the fabric

2 Select Control Plane Node

3 Select Border Node

Validation ⌄

Cancel

Save

Search Topology

Select Devices to add, remove or identify.
Shift + Click to select multiple.

SPOOKY.cisco.com

Border to

○ Rest of Company (Internal)

○ Outside World (External)

● Anywhere (Internal & External)

BGP ⌄

Local AS Number

65001

Border Handoff

› Layer 3

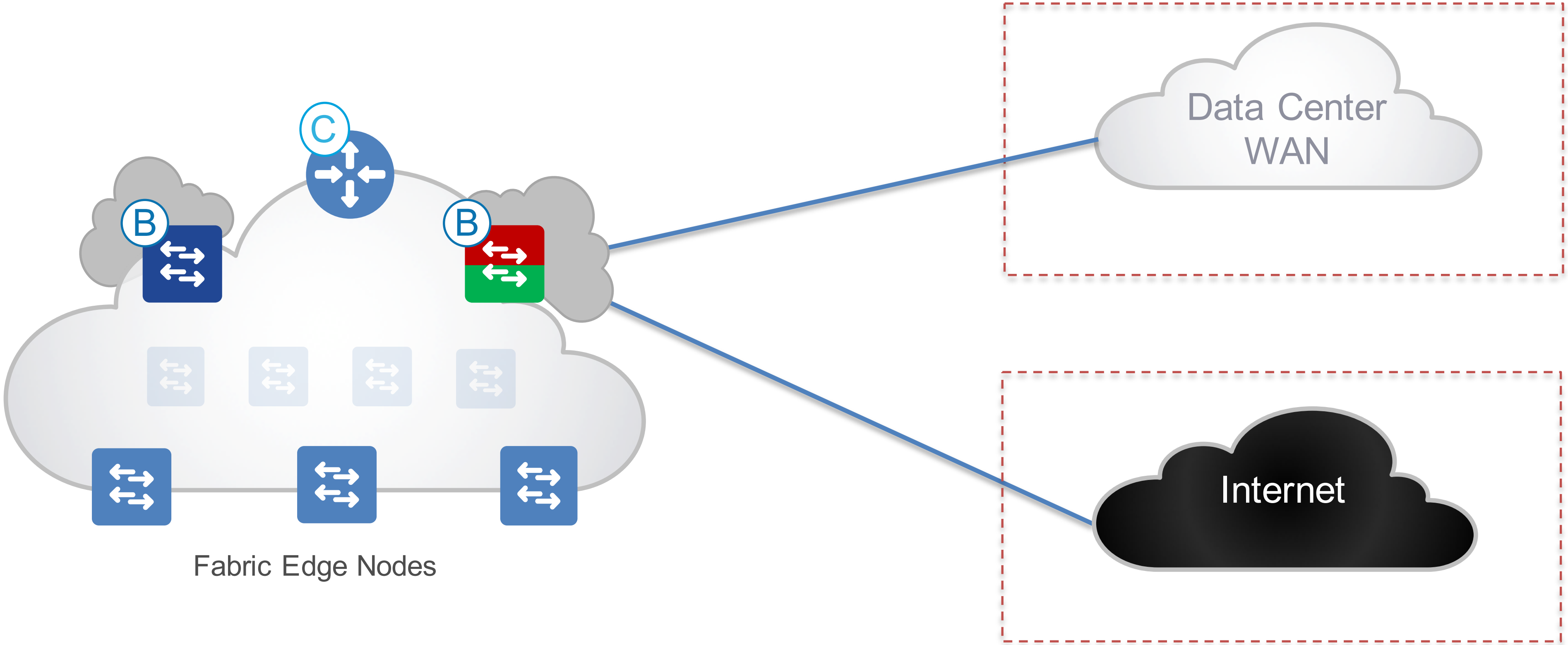
Cancel

Add

SD-Access Border Deployment Options

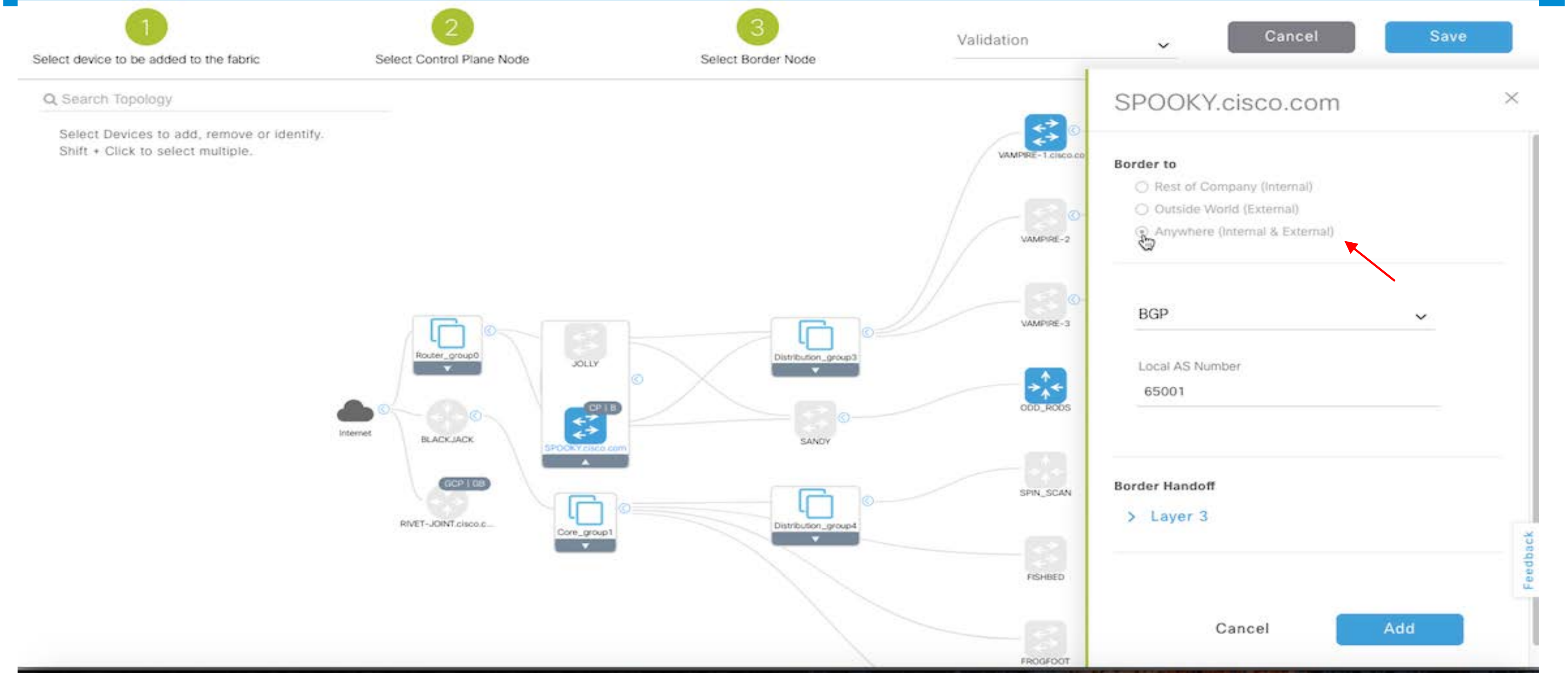
Use Case 3 : SDA fabric Connecting to known and Un-known Networks

Cisco Connect



SD-Access Border Deployment Options

Use Case 3 : SDA fabric Connecting to Everything– Automation



SPOOKY.cisco.com

Border to

- ○ Rest of Company (Internal)
- ○ Outside World (External)
- ● Anywhere (Internal & External)

BGP

Local AS Number: 65001

Border Handoff

> Layer 3

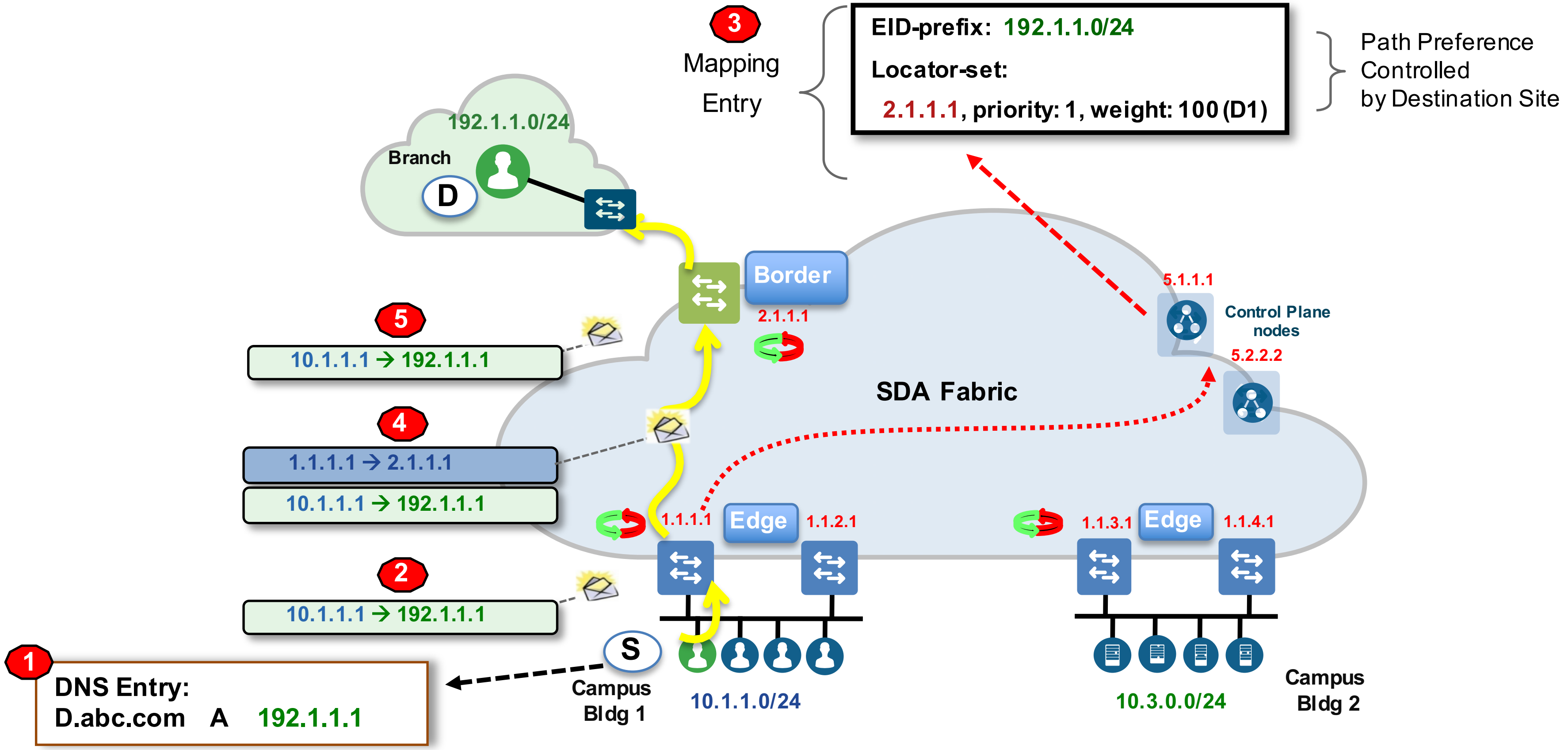
Cancel | Add

Fabric Border (Internal)

SD-Access Border

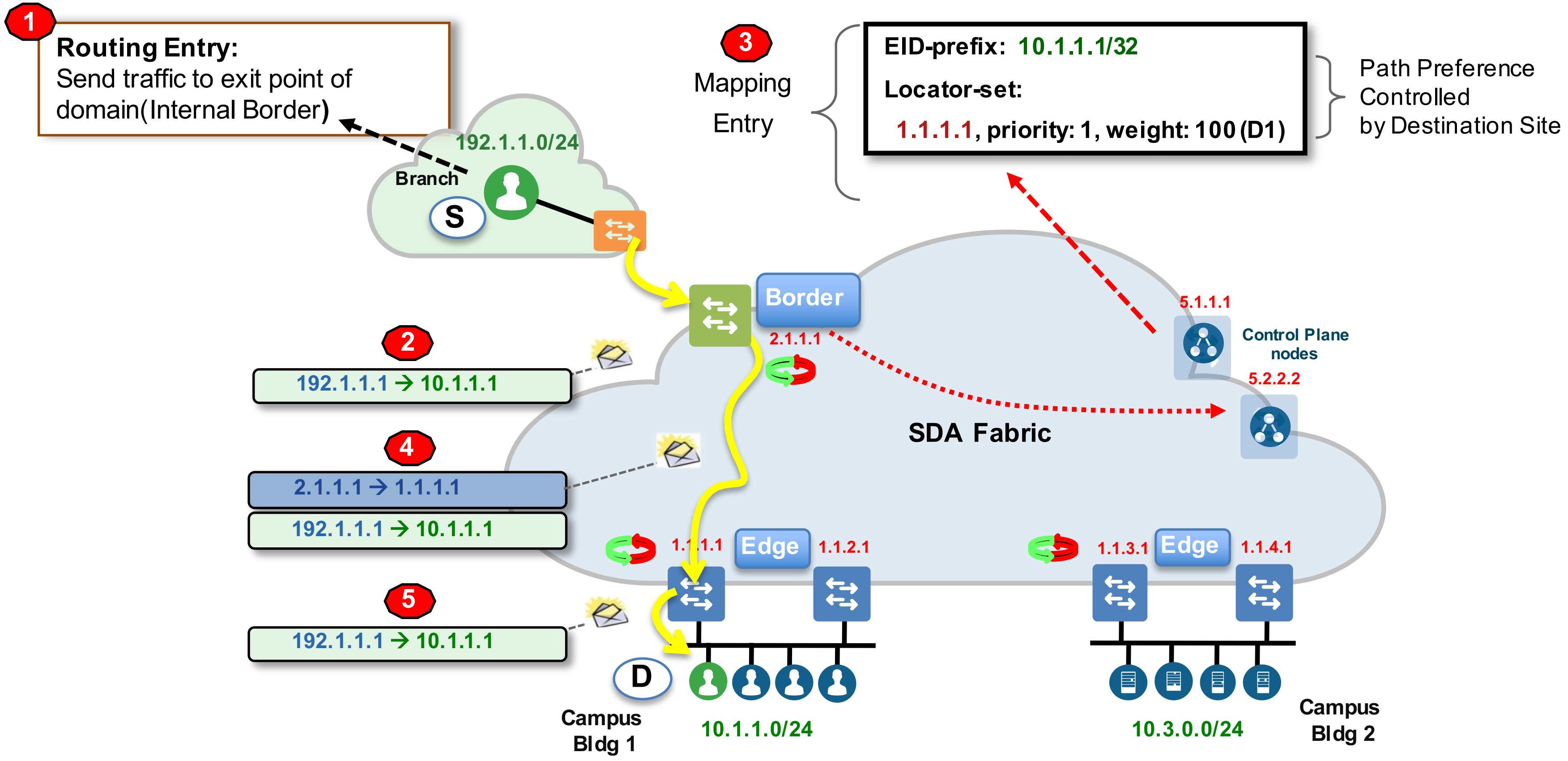
Border - Forwarding from Fabric Domain to External Domain

Cisco Connect



SD-Access Border

Border - Forwarding from External Domain to Fabric Domain



1 **Routing Entry:** Send traffic to exit point of domain(Internal Border)

3 Mapping Entry

EID-prefix: 10.1.1.1/32

Locator-set:

1.1.1.1, **priority: 1, weight: 100 (D1)**

Path Preference Controlled by Destination Site

2 192.1.1.1 → 10.1.1.1

4 2.1.1.1 → 1.1.1.1

192.1.1.1 → 10.1.1.1

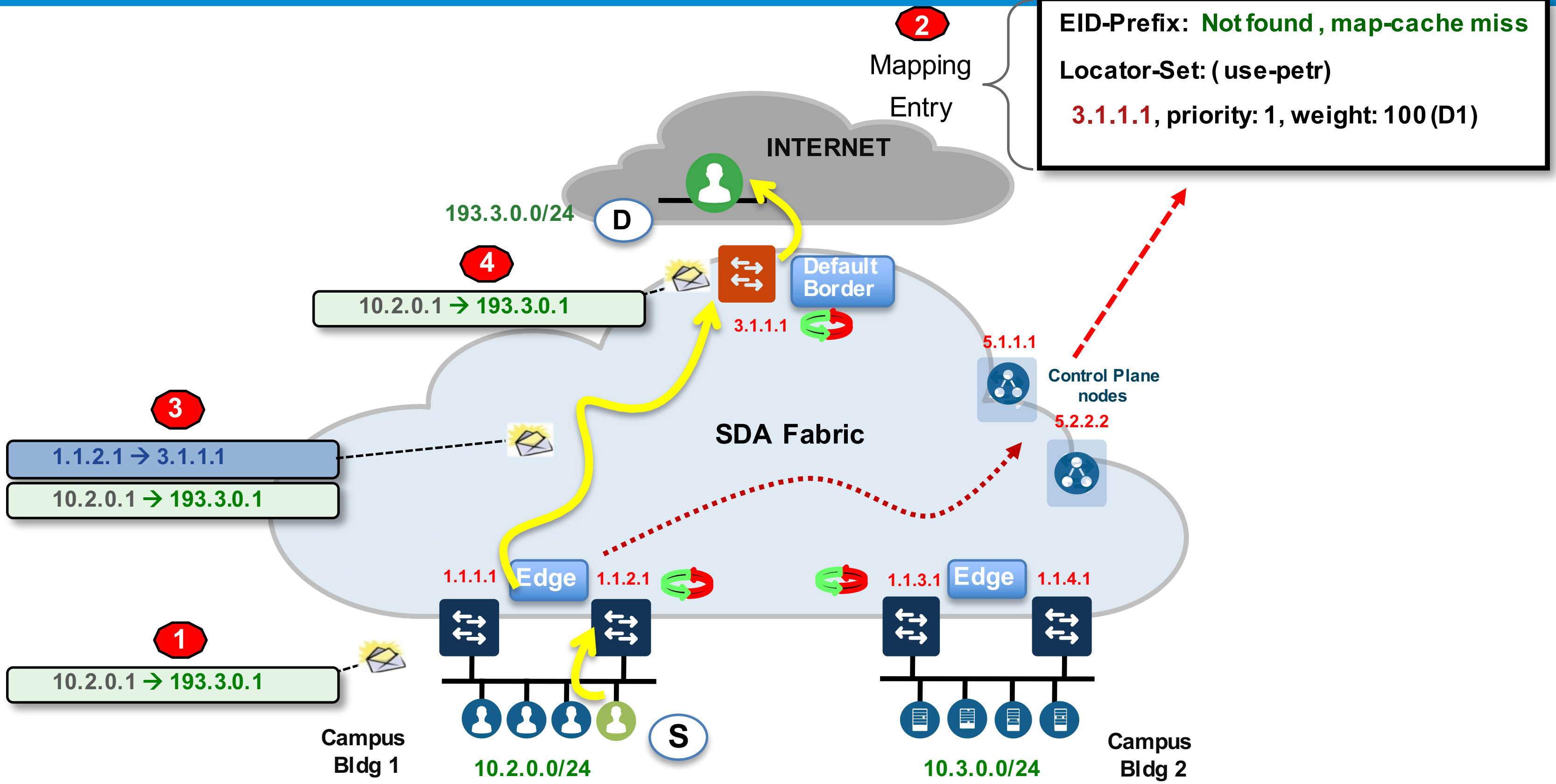
5 192.1.1.1 → 10.1.1.1

Default Border (External)

SD-Access Border

Default Border - Forwarding to External Domain

Cisco Connect



2 Mapping Entry

EID-Prefix: Not found , map-cache miss

Locator-Set: (use-petr)

3.1.1.1, priority: 1, weight: 100 (D1)

Cisco
Connect

SDA Fabric Border Design Considerations

Cisco
Connect

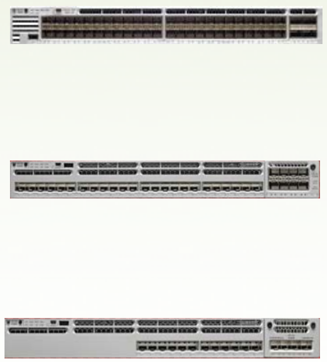
Fabric Border Platform Support and Recommendations

SD-Access – Border Node

Platform Support

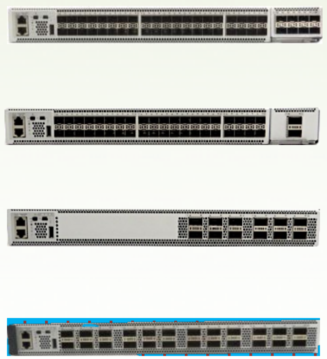
Cisco Connect

Catalyst 3K



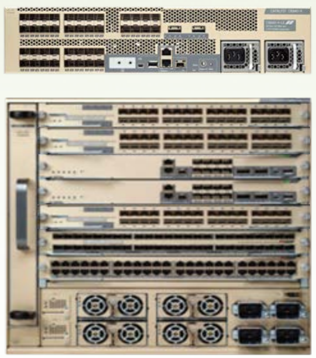
- **Catalyst 3850**
- 1/10G SFP+
- 10/40G NM Cards
- **IOS-XE 16.6.1+**

Catalyst 9K



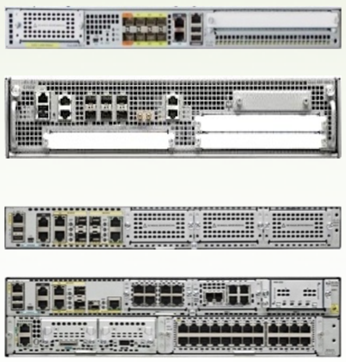
- **Catalyst 9300**
- **Catalyst 9400**
- **Catalyst 9500**
- 40G QSFP
- 10/40G NM Cards
- **IOS-XE 16.6.1+**

Catalyst 6K



- **Catalyst 6800**
- **Catalyst 6500**
- Sup2T/6T
- 6880-X or 6840-X
- **IOS 15.5.1SY+**

ASR1K & ISR4K



- **ASR 1000-X/HX**
- **ISR 4451/4431**
- 1/10G/40G
- **IOS-XE 16.6.1+**

Nexus 7K

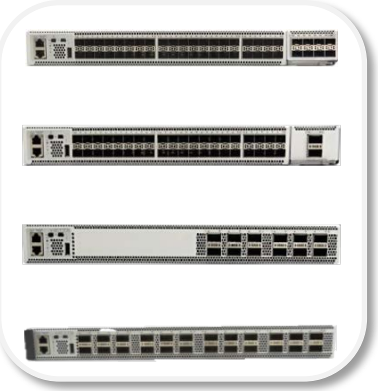
- **Nexus 7700**
- Sup2E
- M3 Cards
- **NXOS 7.3.2+**

SD-Access – Border Node Scale

Platform Scale

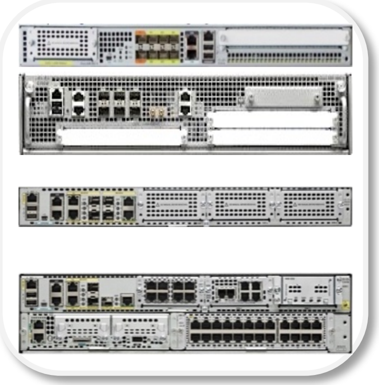
Catalyst 3850

Catalyst 9500



Catalyst 6K

ASR1K & ISR4K



Nexus 7K

	Catalyst 3850	Catalyst 9500	Catalyst 6K	ASR1K & ISR4K	Nexus 7K
Virtual Networks:	64	256	512	4K	500
SGT's in Fabric:	4K	32K	30K	64K	64K
SGT ACL's:	1350	32K	30K	64K	64K
Security ACL's:	3K	18K	32K	4K	128K
IPv4 TCAM:	16K/8K	96K/48K	256K	1M	1M

- **Numbers listed are HW scale limits , SW numbers might be different**

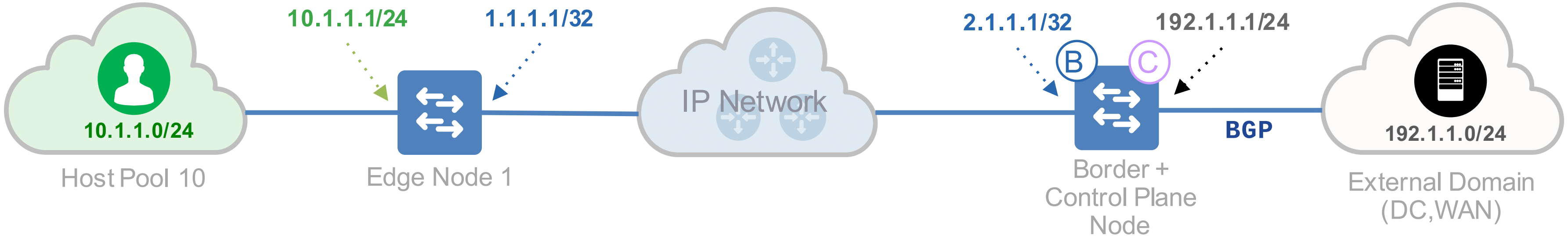
Cisco
Connect

Fabric Border Design Options

Border Design Options

Use case 1: Border with Collocated Control Plane Node

Cisco Connect



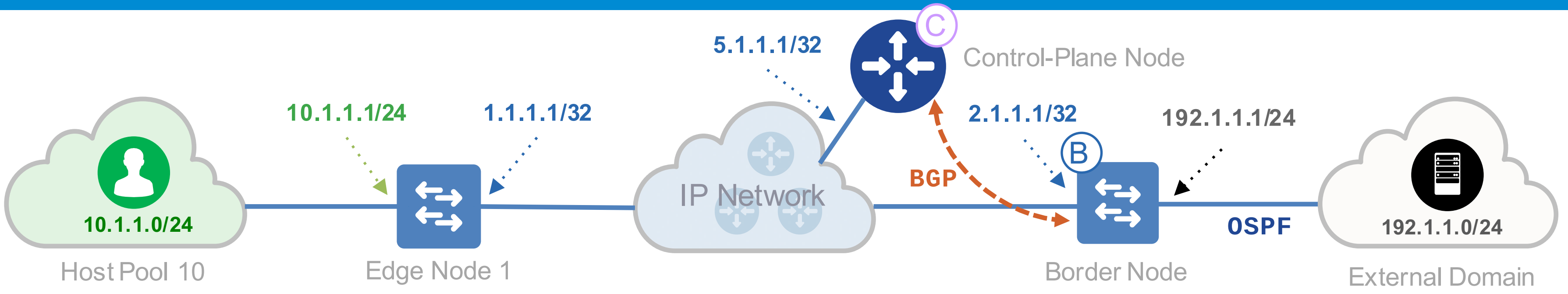
- Border node must perform export (and/or import) of routes between domains
- Control Plane node maintains the database of every prefix/subnet in the Fabric Domain

- **Simplified Design (no additional configuration)**
  - No additional routing protocols needed to synch Border & Control Plane
- **Best when only a few Border nodes are used** (e.g. 2 to 4 per Domain)

NOTE: Control Plane node scale is different on different platforms (select accordingly)

Border Design Options

Use case 2: Border with Distributed Control Plane Node

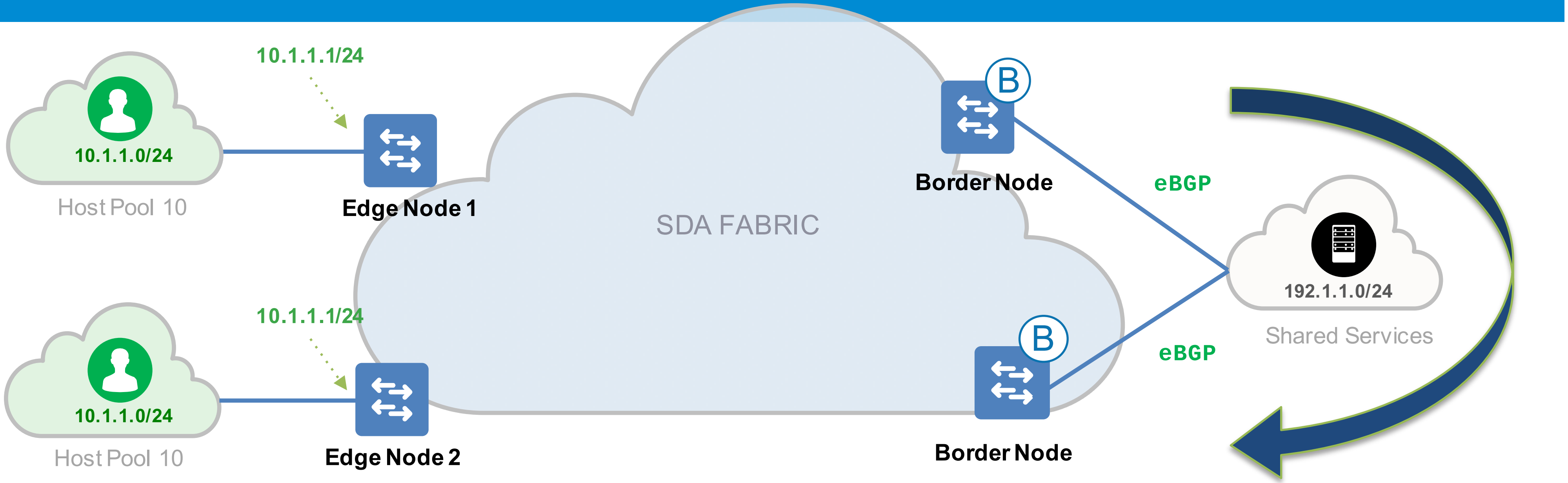


- **The Border node and Control plane node are *different devices***
  - Device 1 - Border node must perform export (and/or import) of routes between domains
  - Device 2 - Control Plane node maintains the database of every prefix/subnet in the Fabric Domain
- **Additional configurations are required**
  - Need additional protocol (iBGP) to share EID mapping information from Border to Control Plane node.
- **Multiple Border nodes can connect to the same Control Plane nodes** (single or set of)

NOTE: Control Plane node scale is different on different platforms (select accordingly)

Border Resiliency Options

Multiple Borders - Loop Prevention



- **eBGP is preferred to break any loops caused by the bidirectional advertisement (redistribution) of routes** from the fabric to external domain (and vice-versa), when using multiple Internal Borders for redundancy.
  - eBGP uses AS-Path loop prevention.
- **If you are using any other protocol than eBGP, some appropriate loop prevention mechanism needs to be used** (distribute-list, prefix-list, or route tags with route-map, etc).

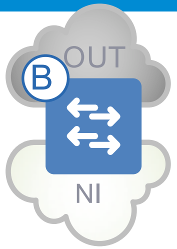
Cisco
Connect

Fabric Border
One Box -vs- Two Box

SD-Access Fabric

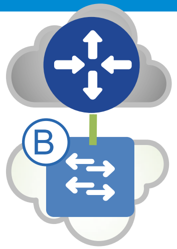
Border Nodes – One Box vs. Two Box

Cisco Connect



One Box Design

- Internal and External domain routing is on the **same device**
- Simple design, without any extra configurations between the Border and outside routers
- The Border device will advertise routes to and from the Local Fabric domain to the External Domain



Two Box Design

Internal and External domain routing are on **different devices**

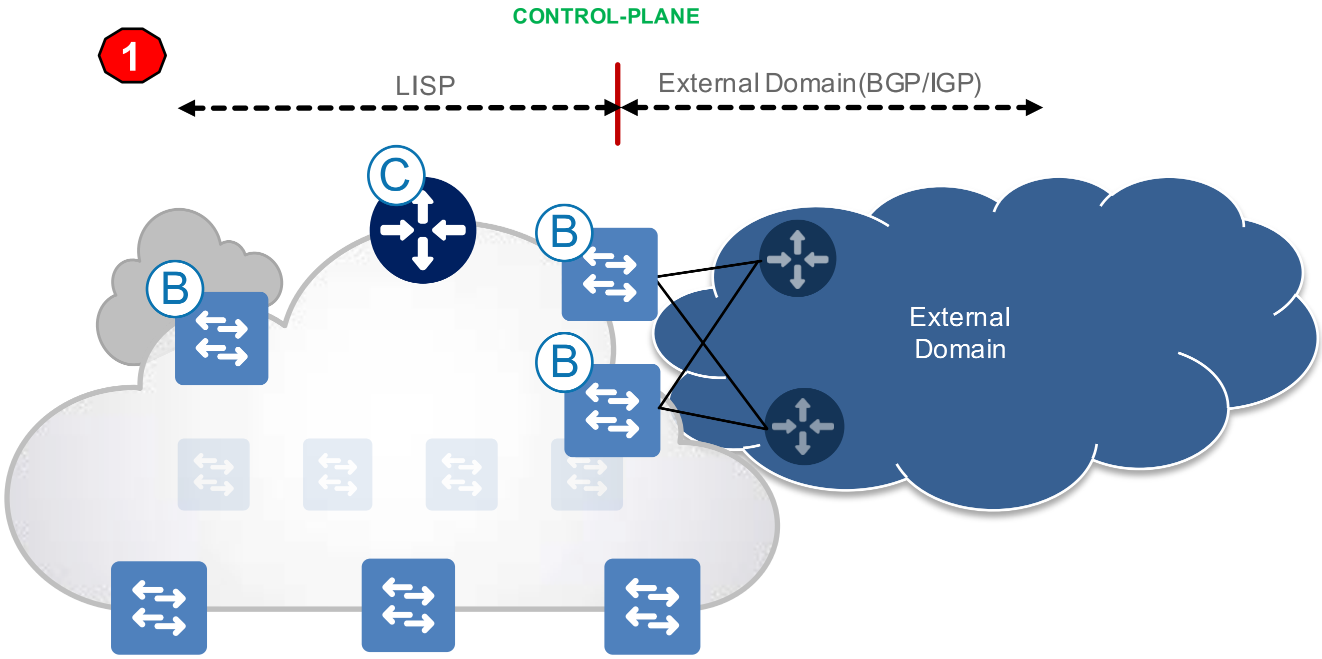
Requires two Devices with BGP in between to exchange connectivity and reachability information

This model is chosen if the Border does not support the functionality (This can due to hardware or software support on the device) to run the external domain on the same device (e.g. DMVPN, EVPN, etc.)

Border Design Options

One Box Border - Control Plane

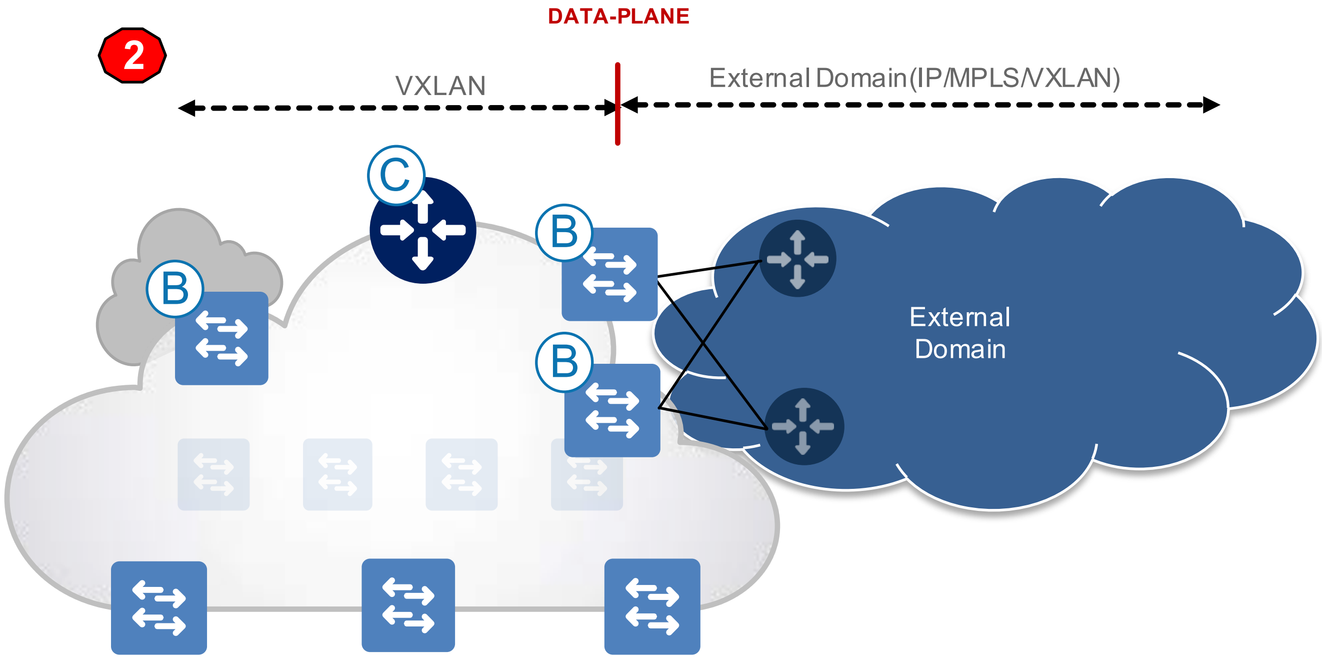
Cisco Connect



Border Design Options

One Box Border - Data Plane

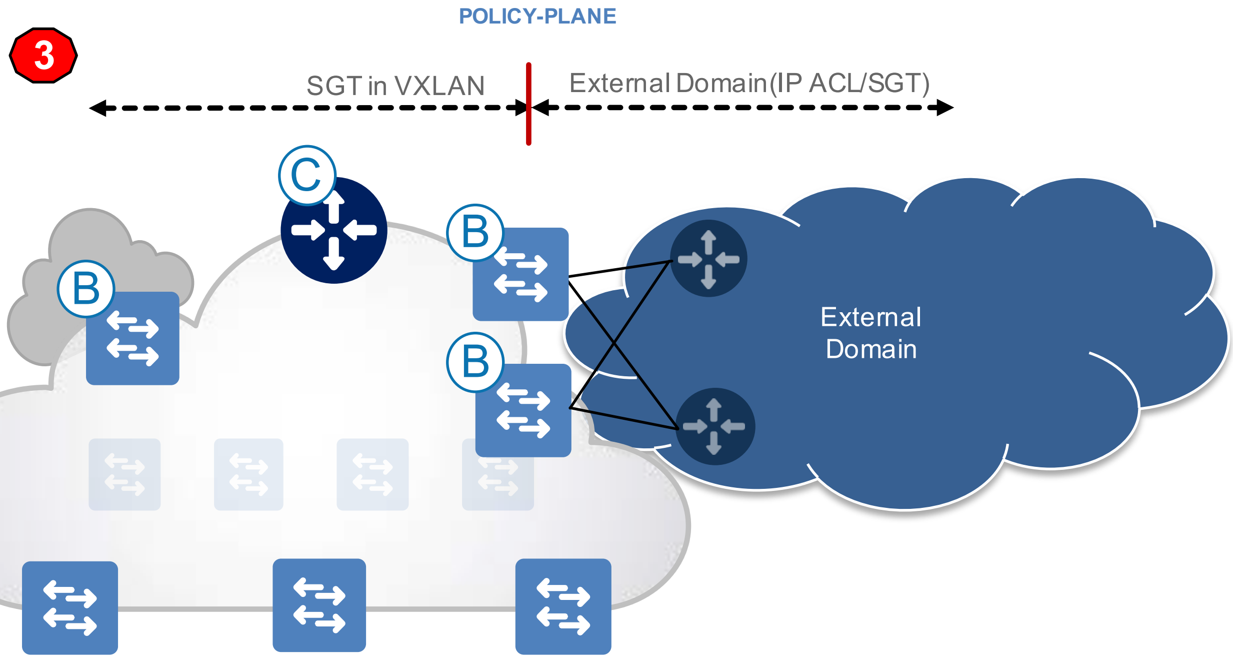
Cisco Connect



Border Design Options

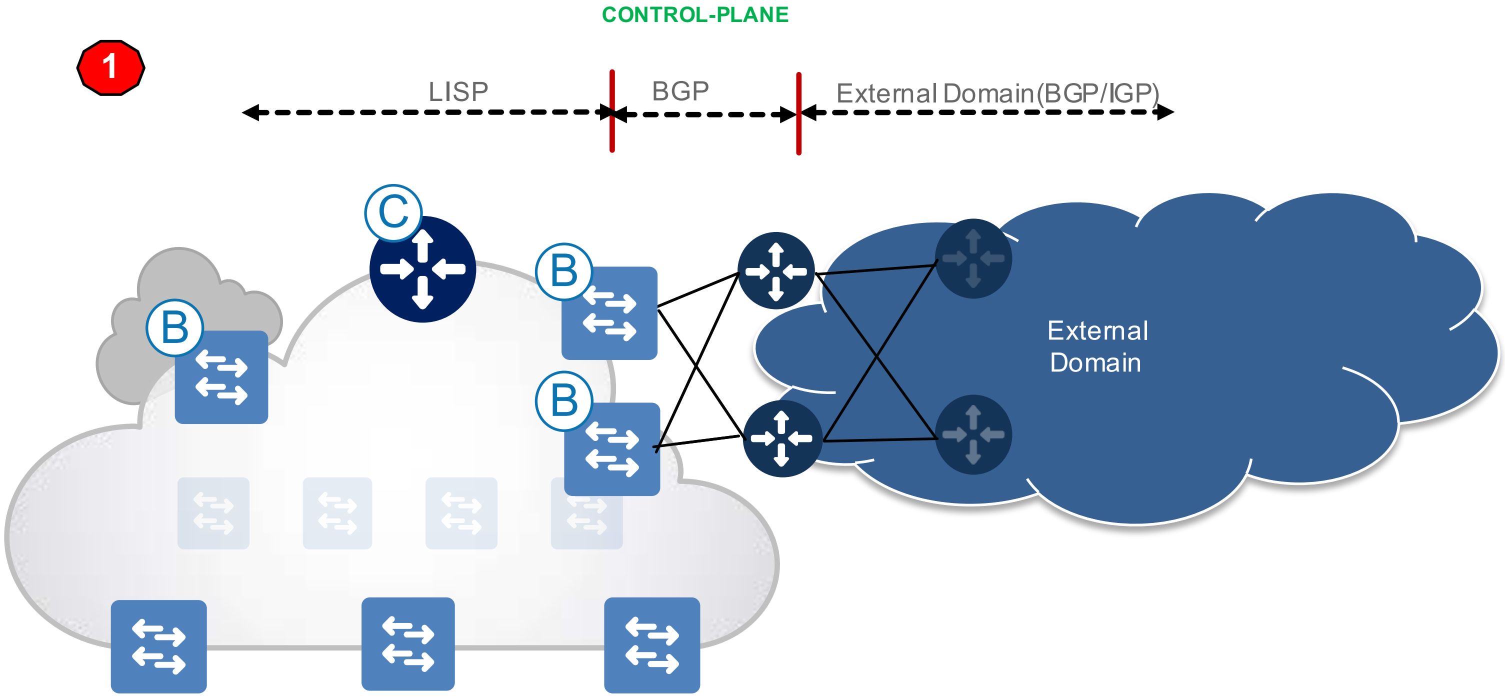
One Box Border - Policy Plane

Cisco Connect



Border Design Options

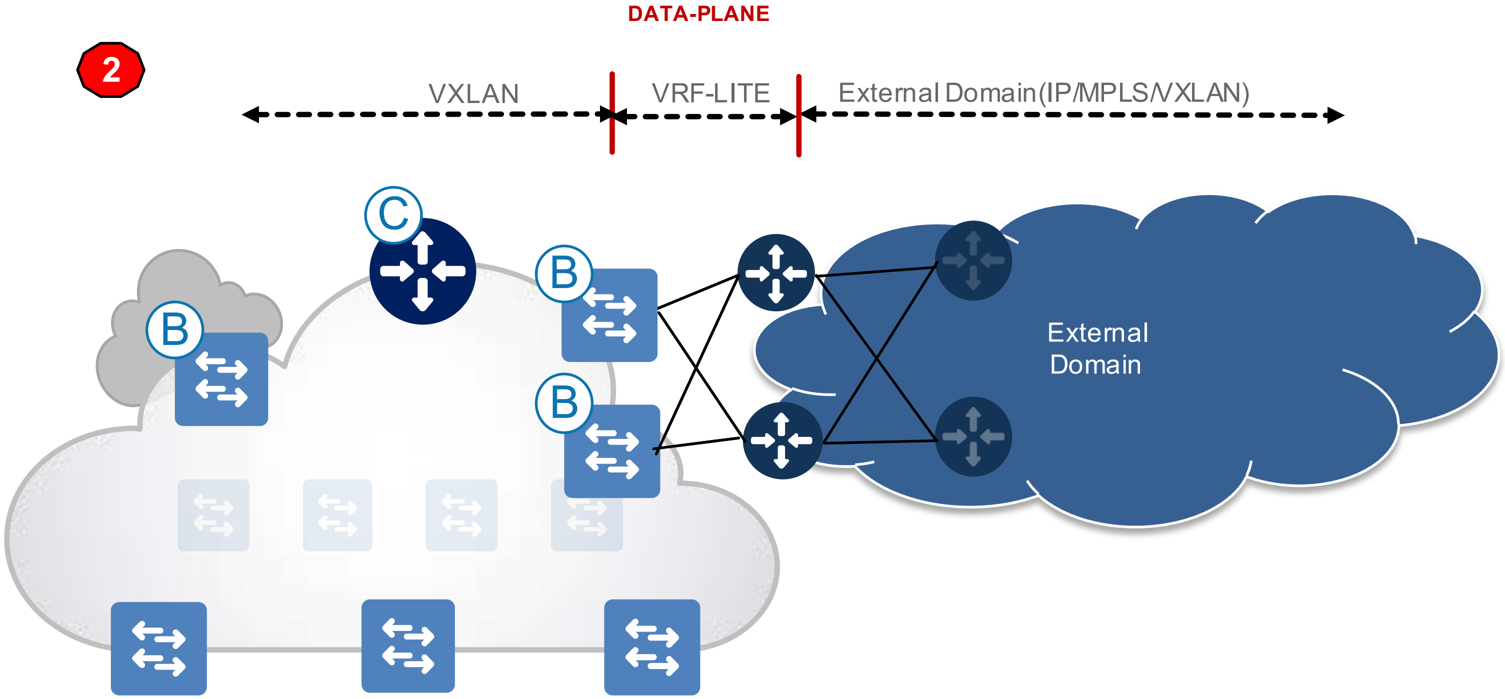
Two Box Border - Control Plane



Border Design Options

Two Box Border - Data Plane

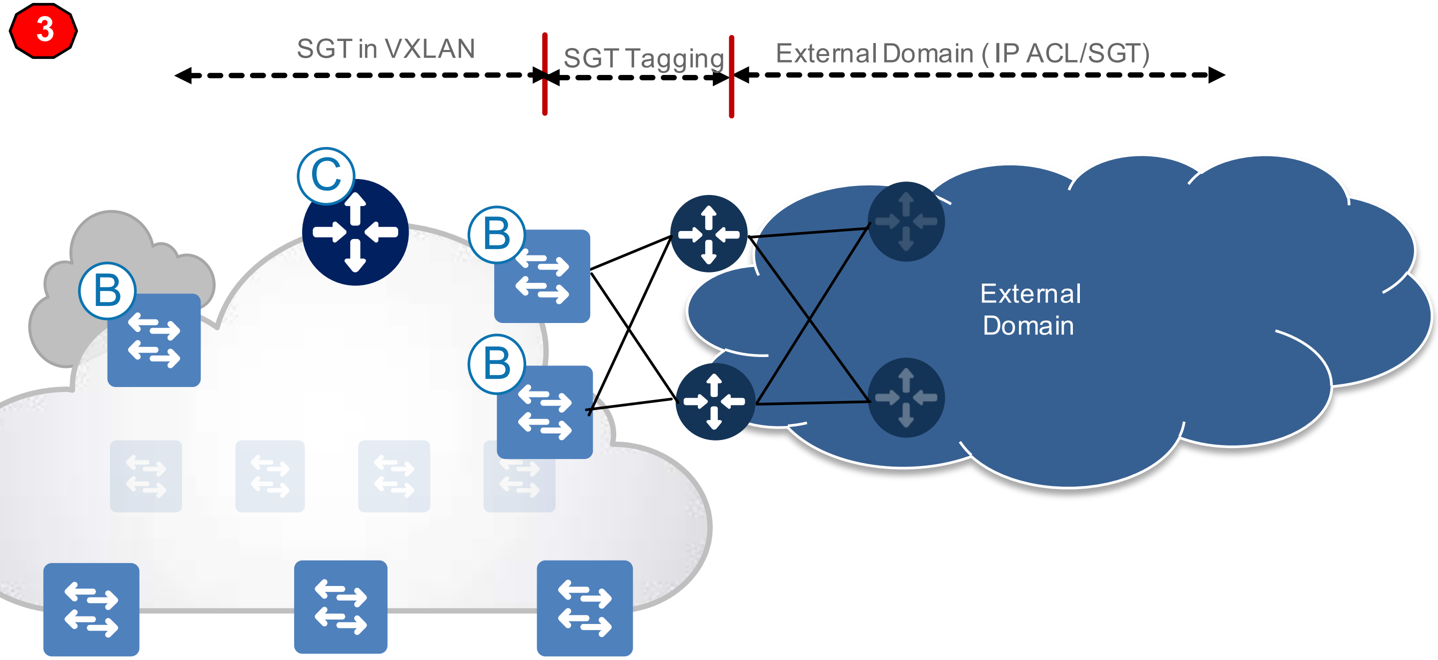
Cisco Connect



Border Design Options

Two Box Border - Policy Plane

POLICY-PLANE

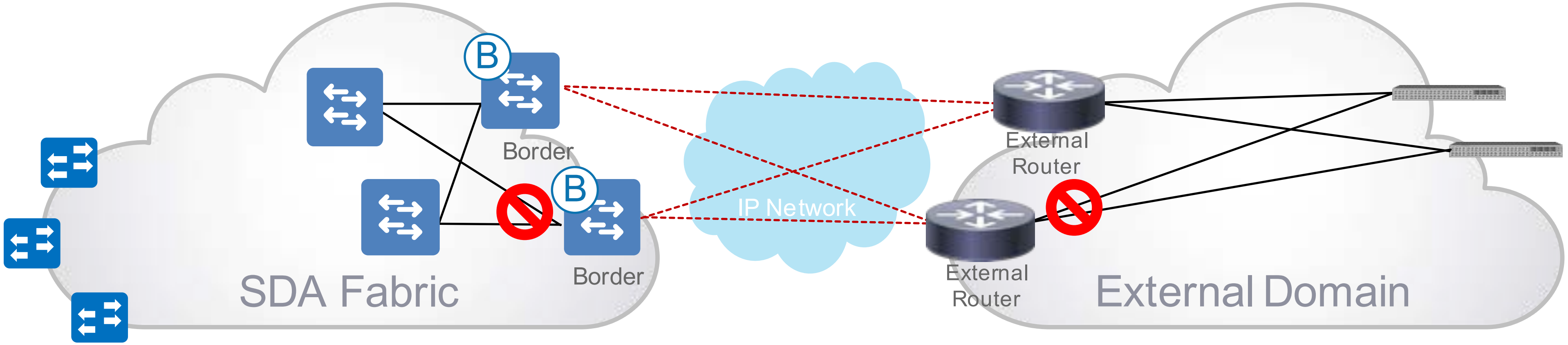


Border Resiliency (HA)

Resiliency at the Border

Track or propagate events across domains

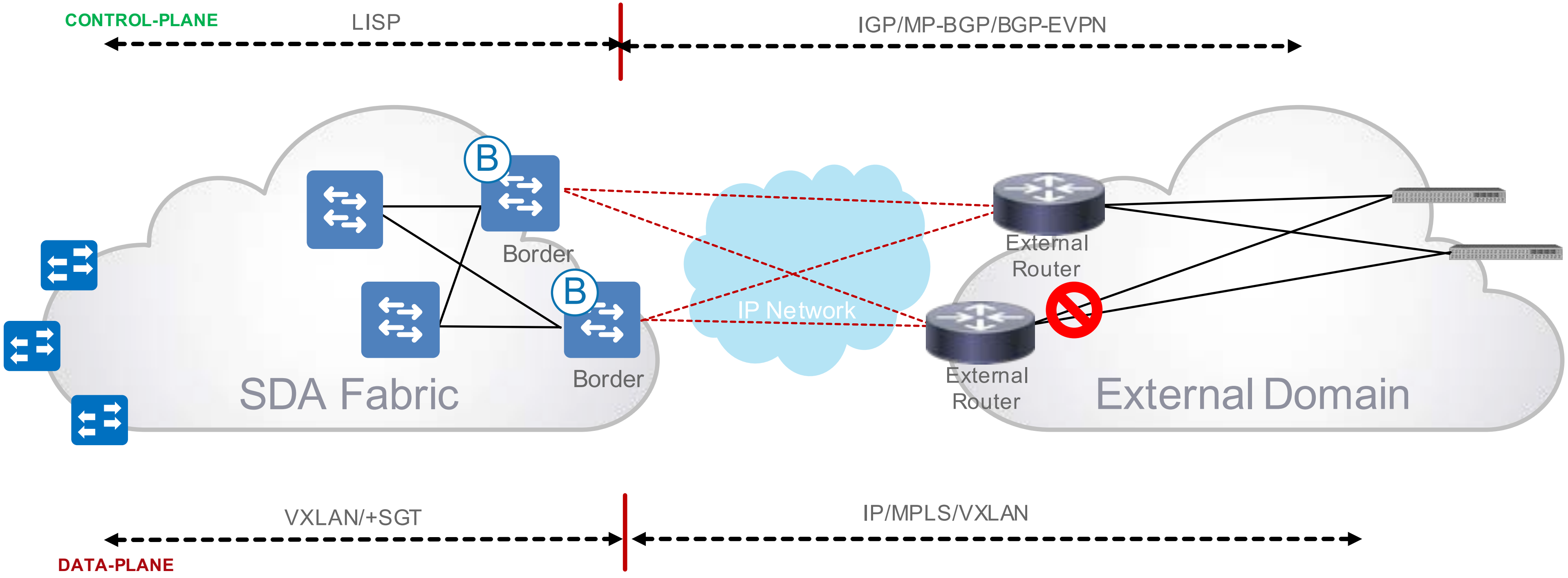
Cisco Connect



Resiliency at the Border

Use Case 1 : Track failures in the External Domain

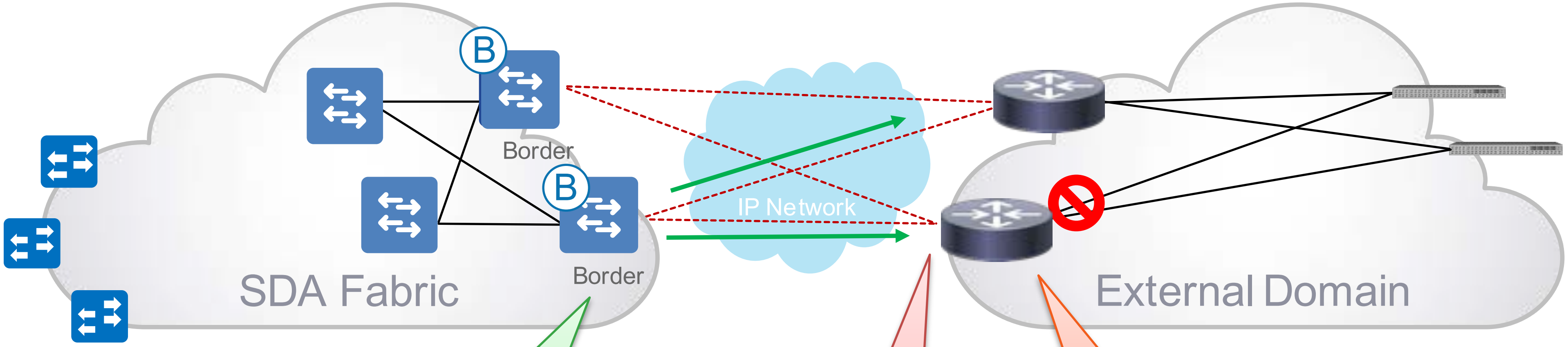
Cisco Connect



Failures & Changes in the External Domain

External advertisements to reflect state of the External Domain

Cisco Connect



Border Routing Tables updated to remove the faulty route(s)

Host advertisements from this router are withdrawn

Host reachability from router is lost or degraded

Resiliency at the Border

Use Case 1 : Track failures in the External Domain

Cisco Connect

❑ No additional configuration is needed on the fabric border to achieve resiliency.

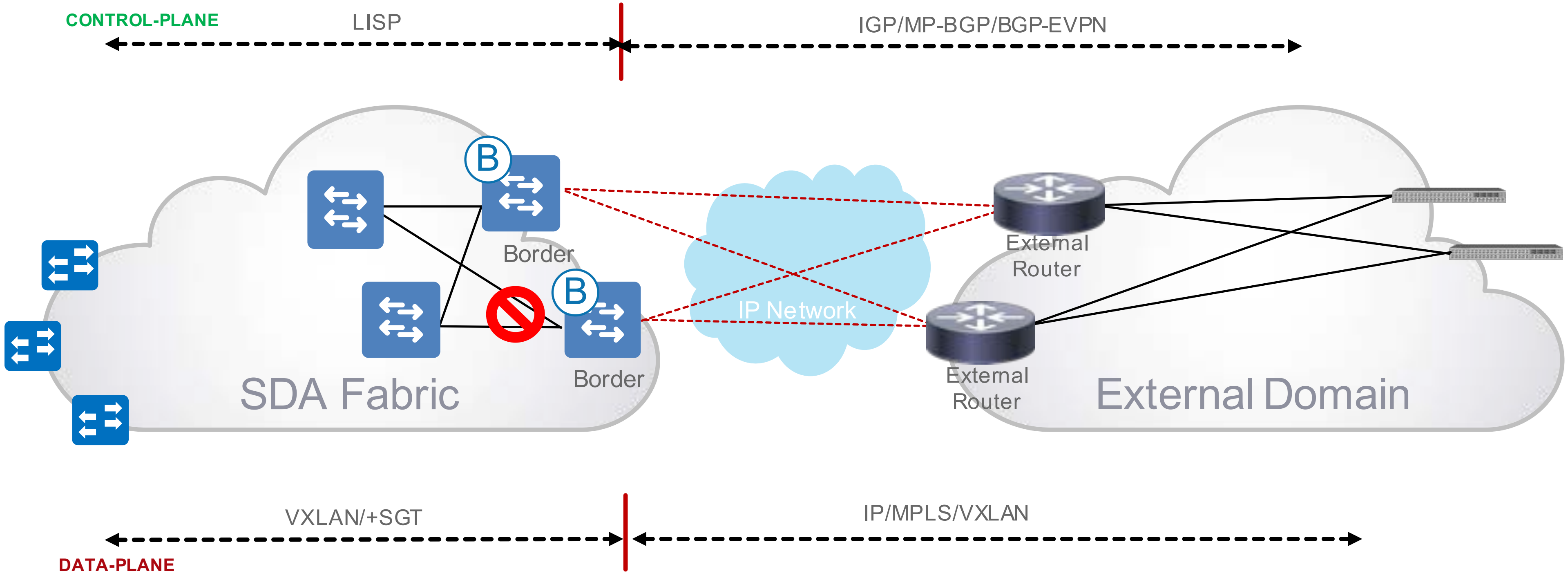
❑ Traffic is re-routed away from the failure point based on routing protocols configured on the fabric border.

❑ Convergence depends on the routing protocols convergence times.

Resiliency at the Border

Use Case 2.1: Track failures in the Fabric Domain @ Border and CP Co-located

Cisco Connect

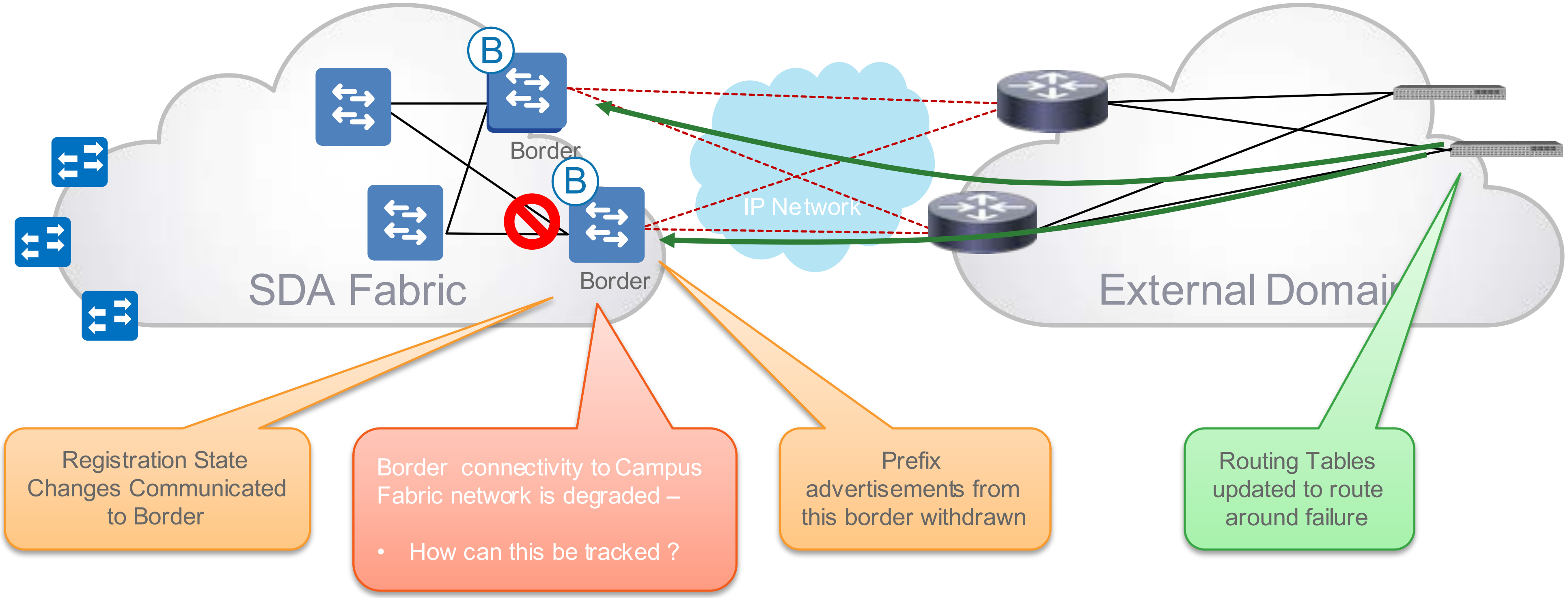


Failures & Changes in the SD-Access Fabric

Internal redistribution of Fabric state into External Domain @ Border and CP Co-located

Cisco Connect

I. Border and Control plane Node Co-located



Registration State Changes Communicated to Border

Border connectivity to Campus Fabric network is degraded –

- How can this be tracked ?

Prefix advertisements from this border withdrawn

Routing Tables updated to route around failure

Failures & Changes in the SD-Access Fabric

Internal redistribution of Fabric state into External Domain @ Border and CP Co-located

❑ Since Border and Control Plane node are Co-located, when a Failure happens the state of the network needs to be tracked and informed to the control plane node so that the fabric border can withdraw its route advertisements.

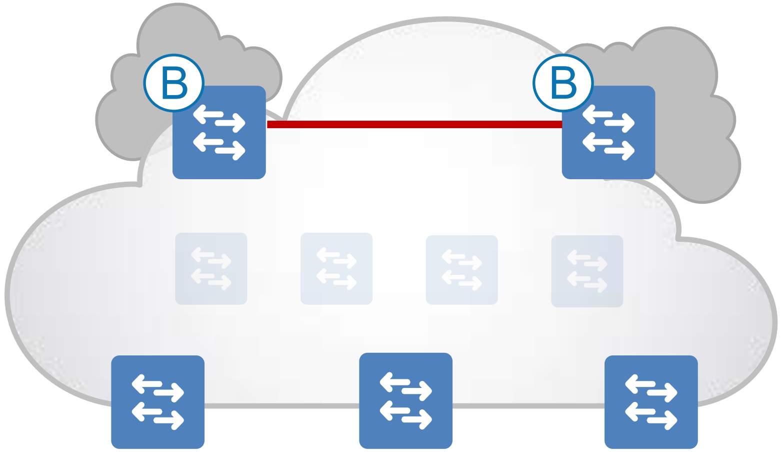
❑ To Track the state of the Network we can use either an EEM script or Object tracking.

❑ Since above requires configuration's on the border nodes an workaround to alleviate this issue is explained in next slide.

Resiliency at the Border

Use Case 2.1 : Track failures in the Fabric Domain @ Border and CP Co-located

Cisco Connect

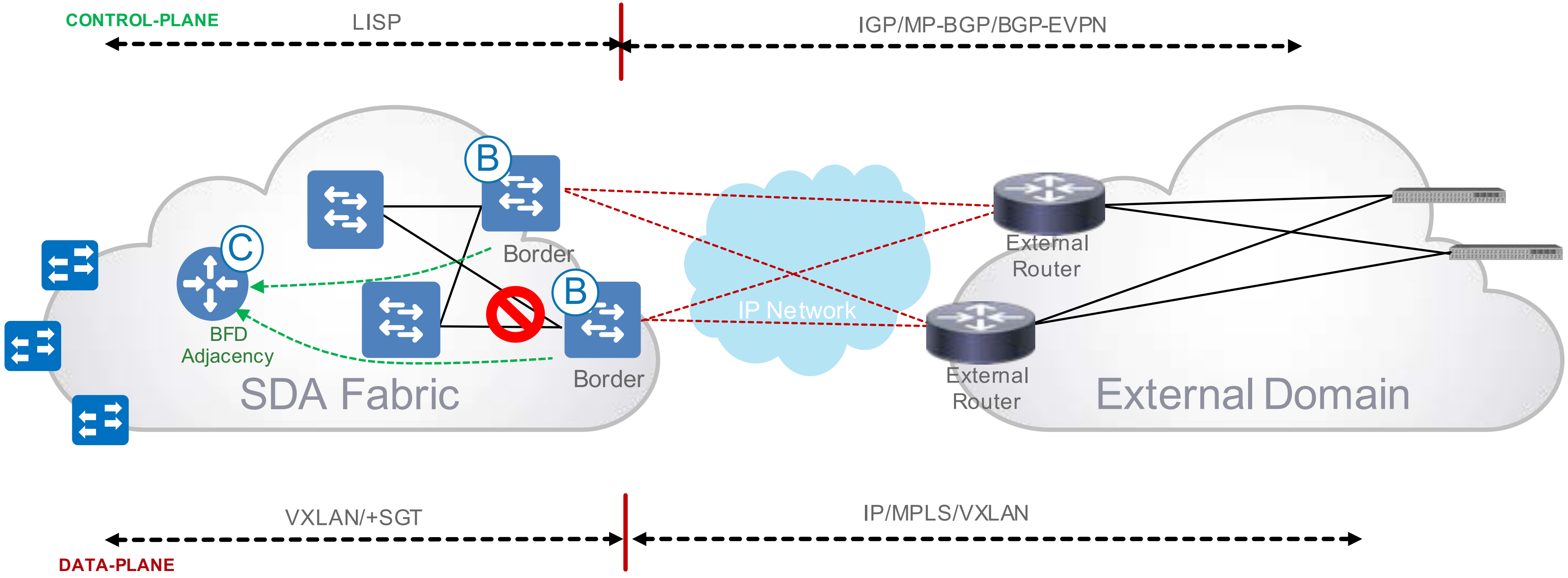


- ❑ As a workaround the border node’s can be Connected via a Layer 3 link.
- ❑ This Layer 3 link/’s will have lesser cost to reach the fabric edge nodes than the underlay , meaning when underlay is available this direct connect link is not used.
- ❑ If one of the border’s connectivity to the underlay is degraded then the traffic from external domain will come to that border and using the Layer 3 link will flow to the other border node and then on to the fabric edge nodes.
- ❑ Convergence times depends on routing protocol between the border nodes

Resiliency at the Border

Use Case 2.2 : Track failures in the Fabric Domain @ Border and CP Distributed

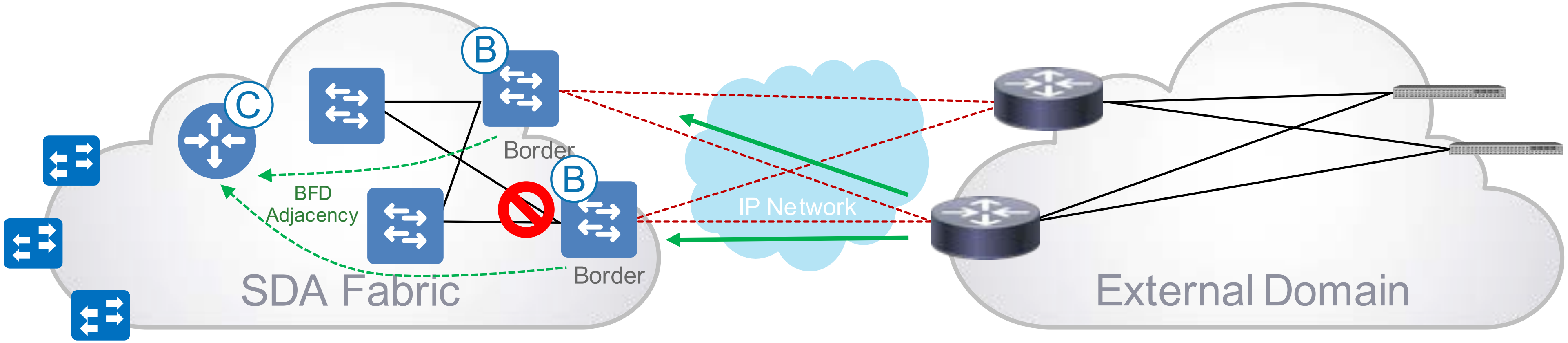
Cisco Connect



Failures & Changes in the SD-Access Fabric

Internal redistribution of Fabric state into External Domain @ Border and CP Distributed

Cisco Connect



- SDA fabric domain prefixes are advertised via BGP from Control Plane node to Border node
- **BGP adjacencies between Control Plane and Border node are monitored with BFD**
- Upon BFD adjacency fail, prefixes associated with the Border are withdrawn immediately
- **Fast Convergence (150-200ms)**

Cisco
Connect

Shared Services with Border

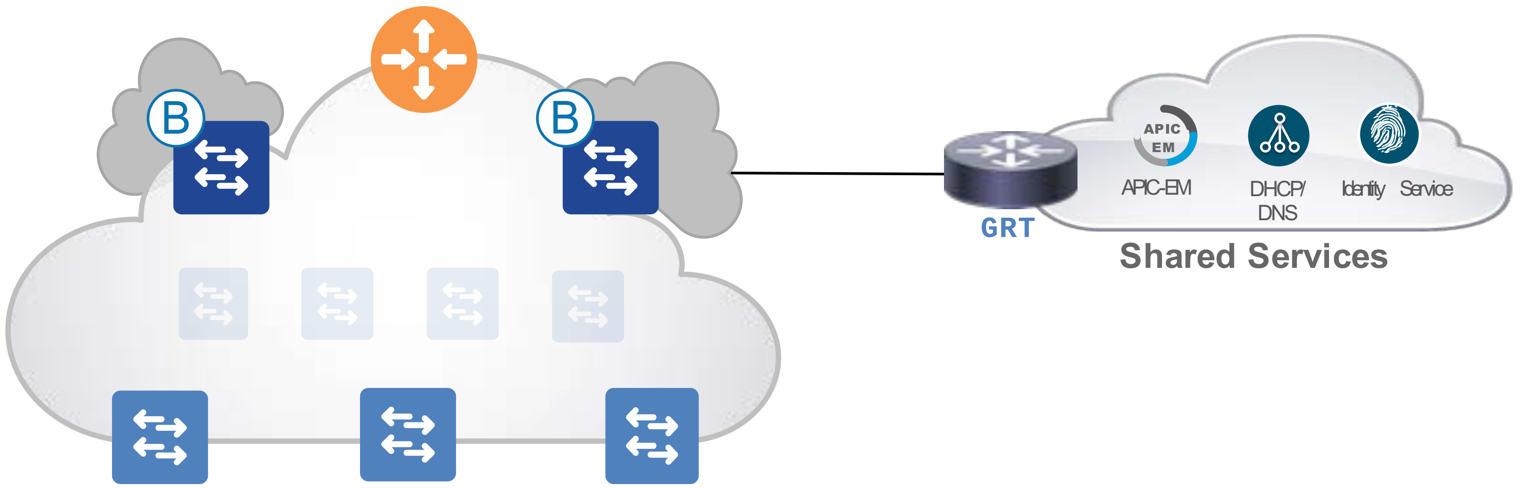
Border Deployment Options

Shared Services (DHCP, AAA, etc) with Border

- Hosts in the fabric domain (in their respective Virtual Networks) will need to have access to common “Shared Services”:
  - **Identity Services** (e.g. AAA/RADIUS)
  - **Domain Name Services** (DNS)
  - **Dynamic Host Configuration** (DHCP)
  - **IP Address Management** (IPAM)
  - **Monitoring tools** (e.g. SNMP)
  - **Data Collectors** (e.g. Netflow, Syslog)
  - **Other infrastructure elements**
- These shared services will *generally* reside *outside* of the fabric domain.

Border Deployment Options

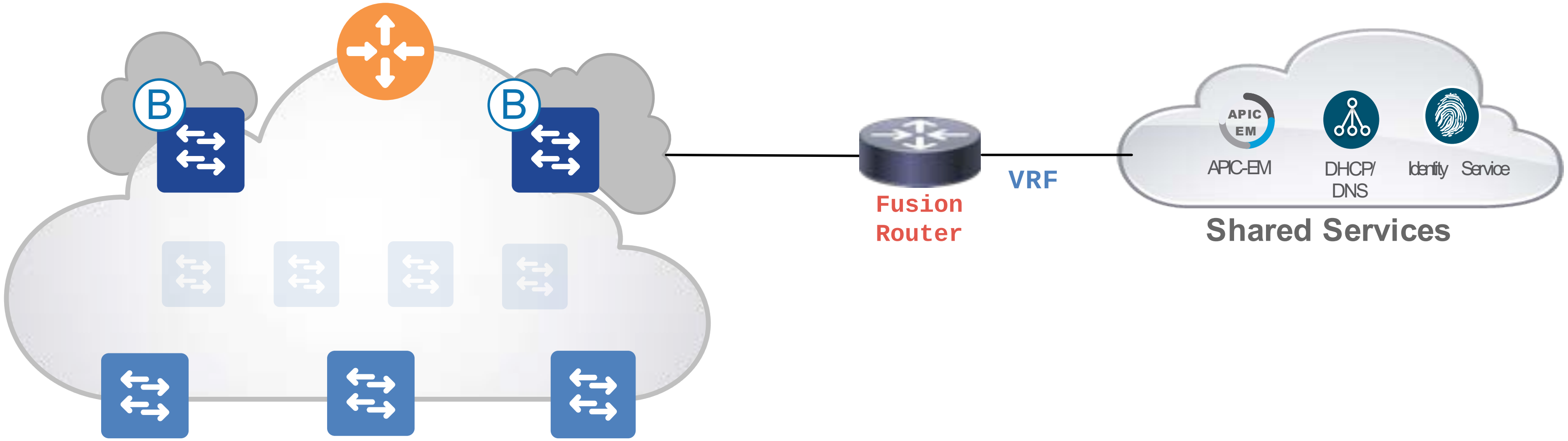
Shared Services (DHCP, AAA, etc) with Border in Global Routing Table



Border Deployment Options

Shared Services (DHCP, AAA, etc) with Border in dedicated VRF

Cisco Connect



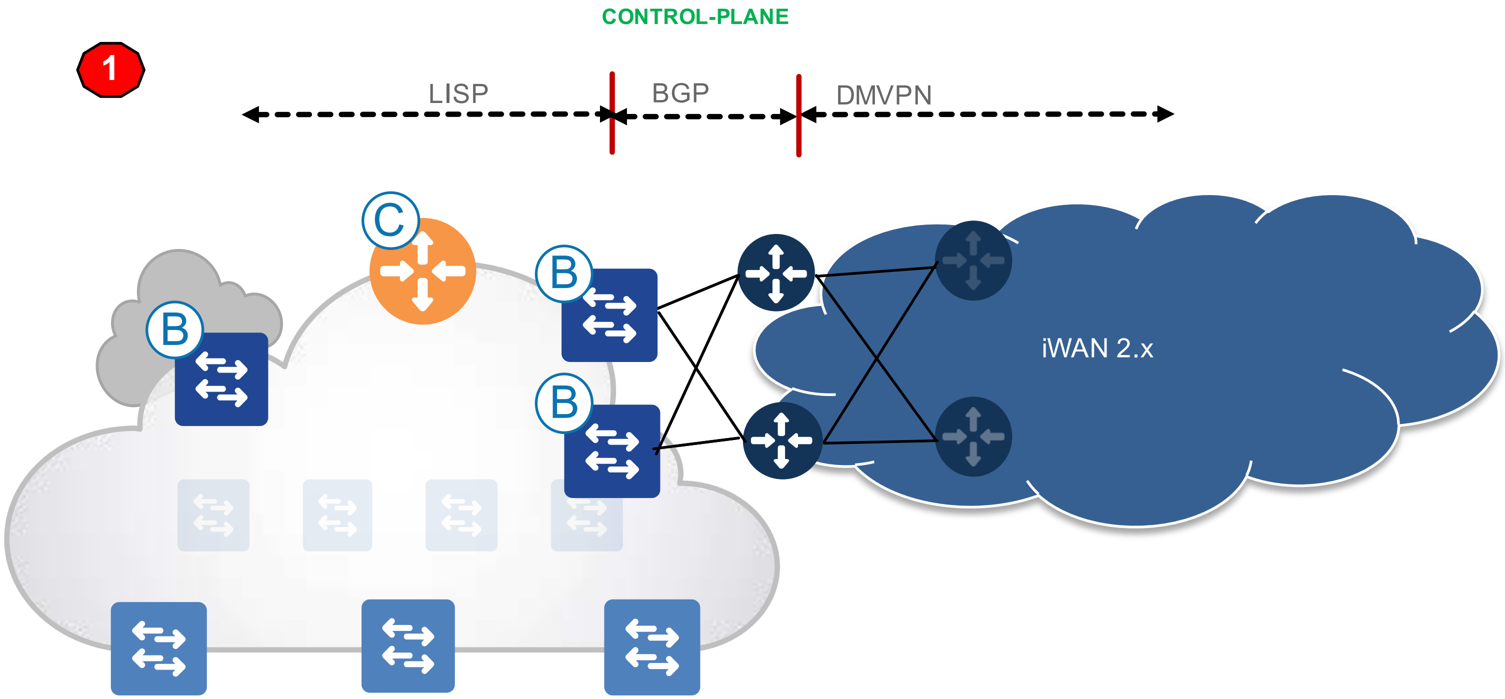
Cisco
Connect

WAN Connectivity with Border

Border Design Options

IWAN2.x Connectivity with Border - Control Plane

Cisco Connect

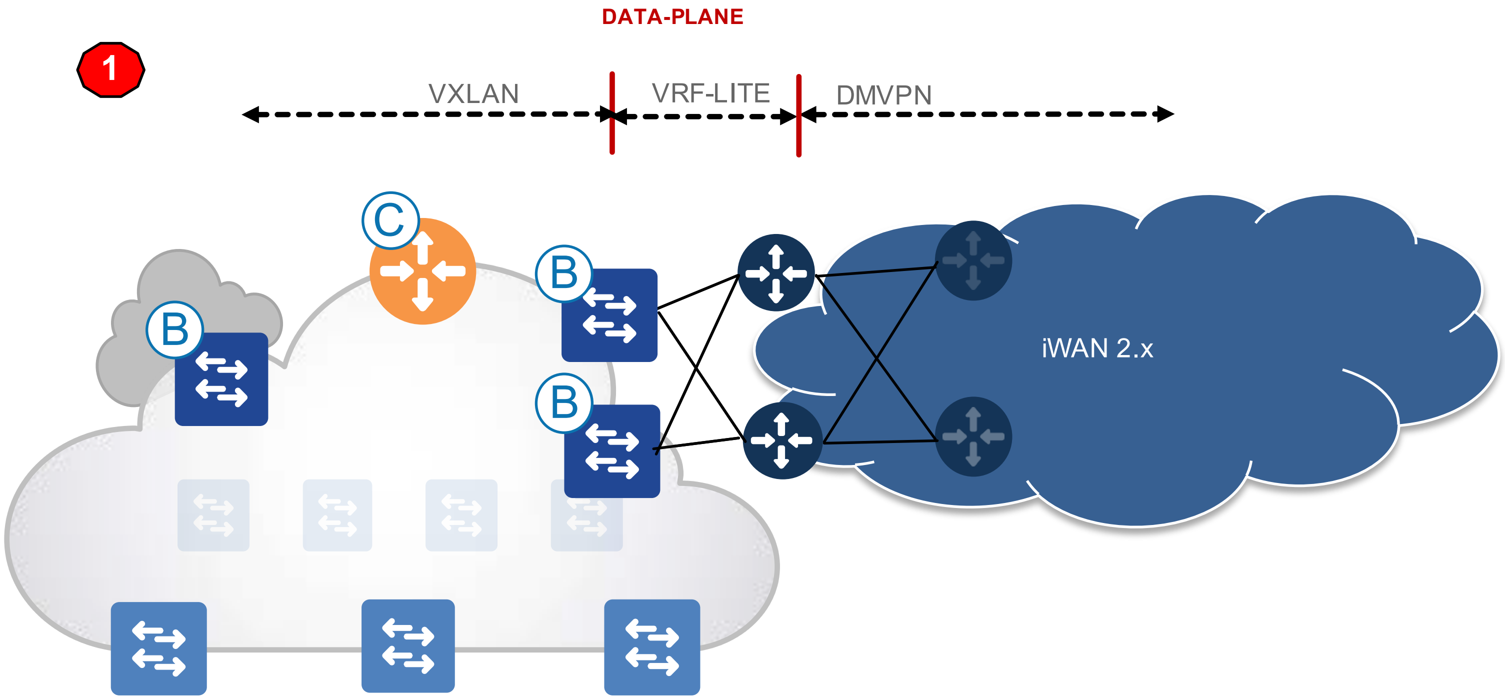


Border Design Options

IWAN2.x Connectivity with Border - Data Plane

Cisco Connect

* **Recap**

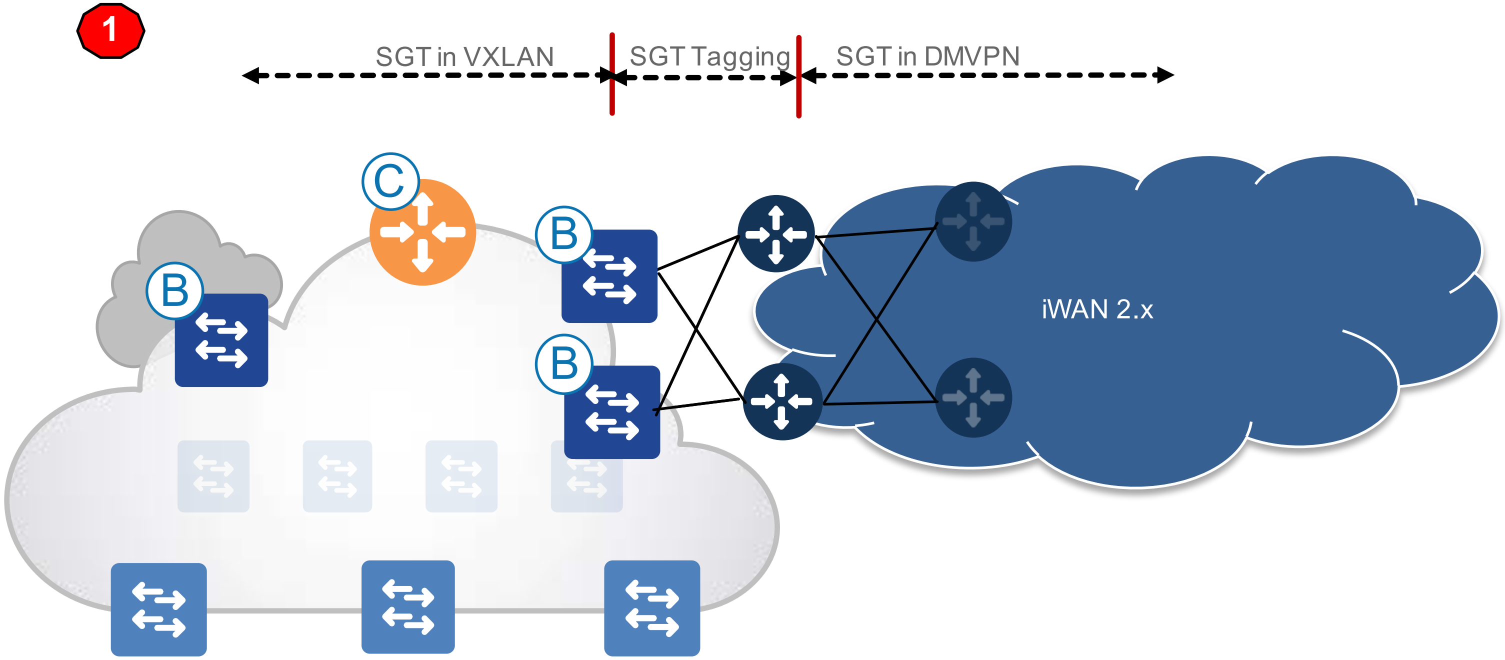


Border Design Options

IWAN2.x Connectivity with Border - Policy Plane

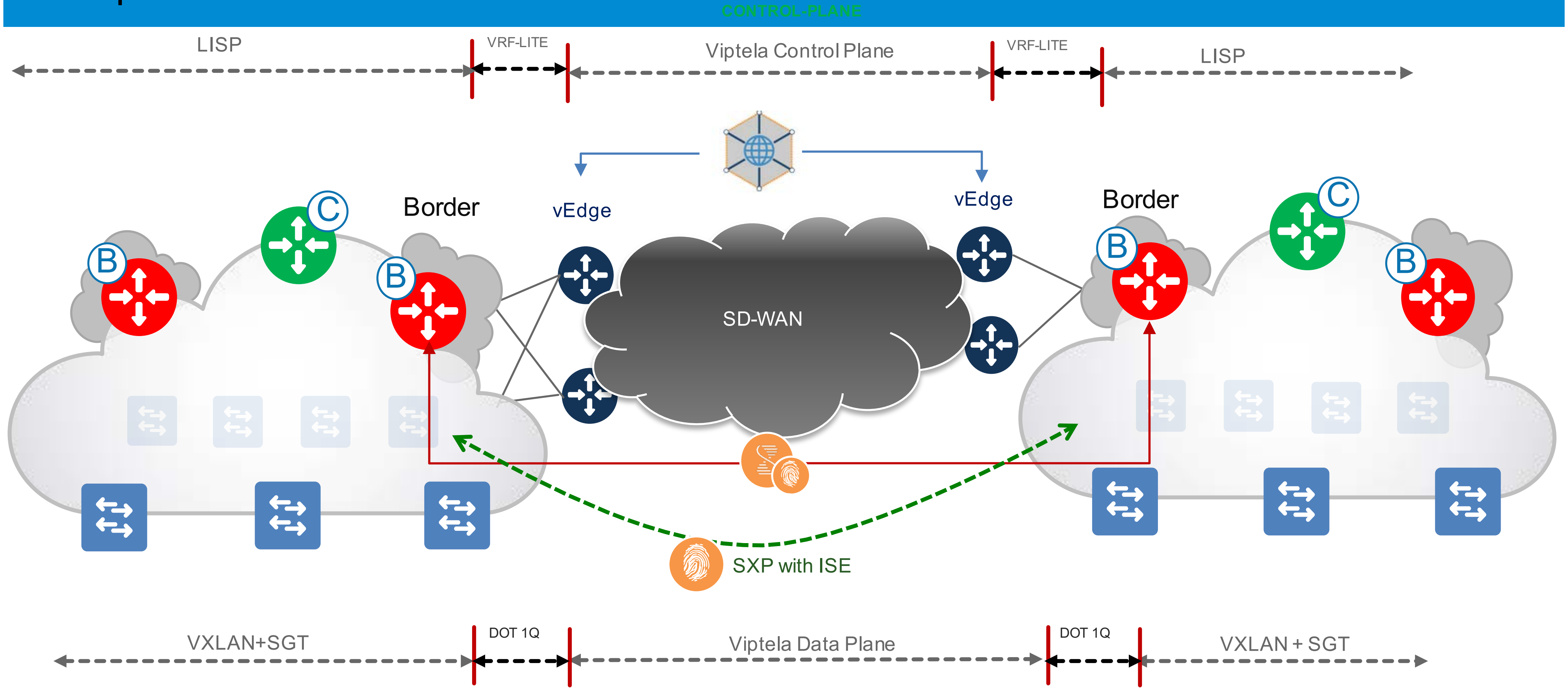
Cisco Connect

POLICY-PLANE



Border Deployment Options
Viptela SD-WAN hand off

Cisco Connect



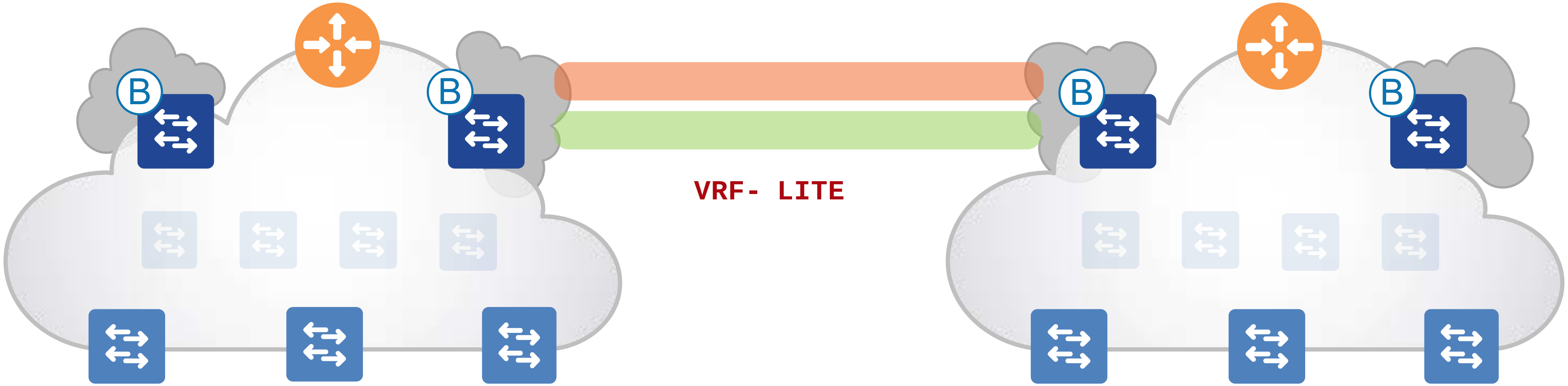
Cisco
Connect

Multiple Fabric Domains Connectivity with Border

Border Deployment Options

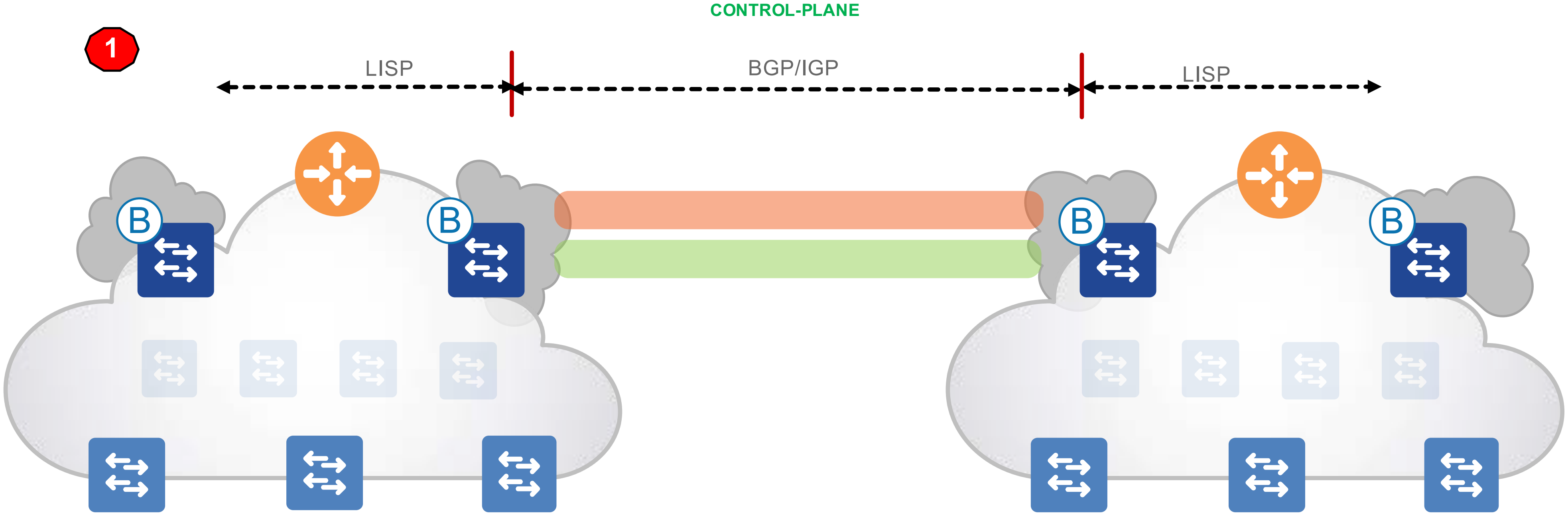
Multiple Fabric Domains

Cisco Connect



Border Deployment Options

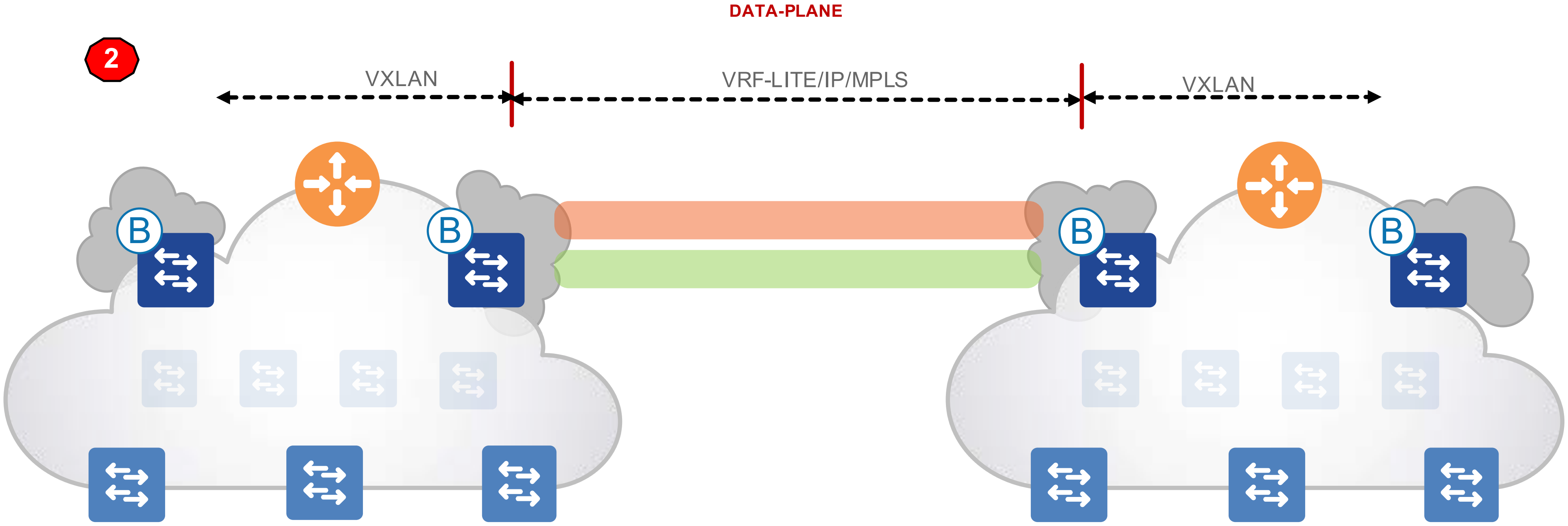
Multiple Fabric Domains



Border Deployment Options

Multiple Fabric Domains

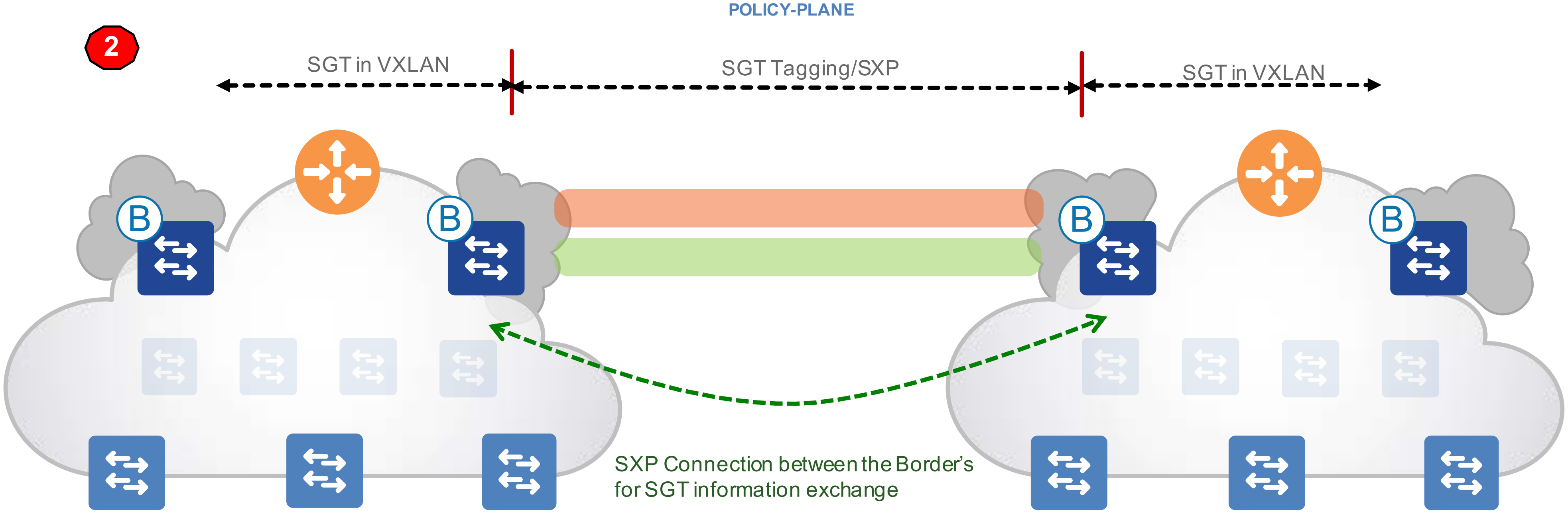
Cisco Connect



Border Deployment Options

Multiple Fabric Domains

Cisco Connect

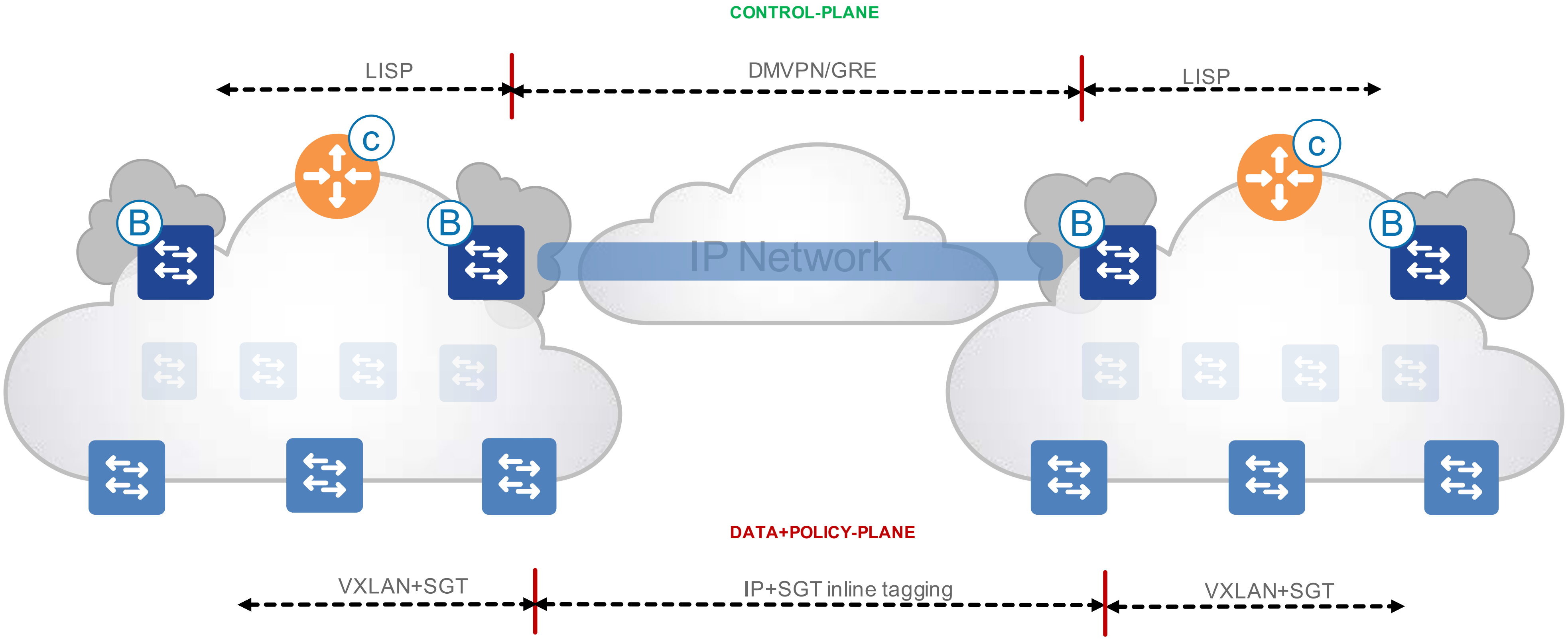

POLICY-PLANE
2
SGT in VXLAN
SGT Tagging/SXP
SGT in VXLAN
B
B
B
B
SXP Connection between the Border's
for SGT information exchange

*** Check Platform support if using the SXP Model**

Border Deployment Options

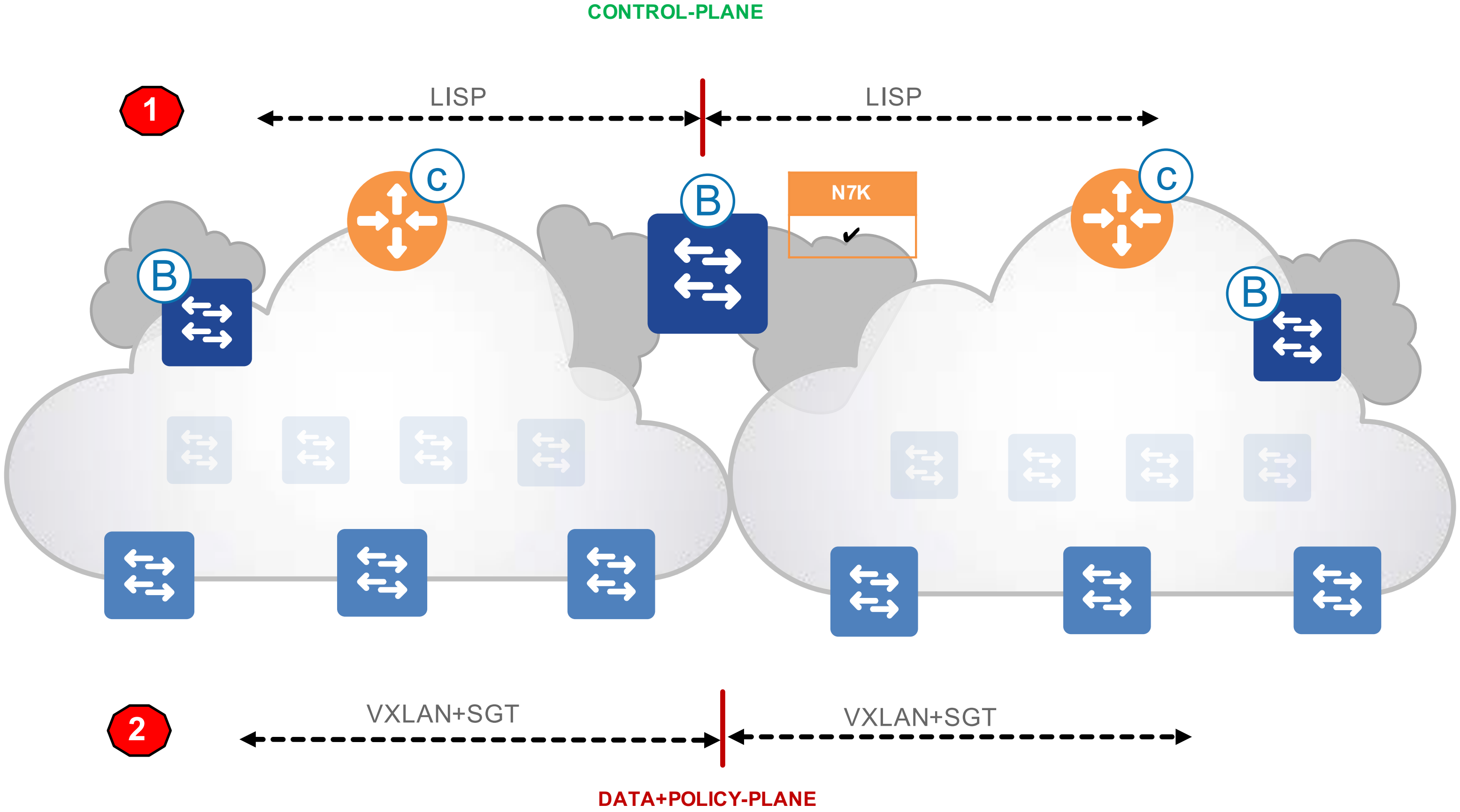
Multiple Fabric Domains

Cisco Connect



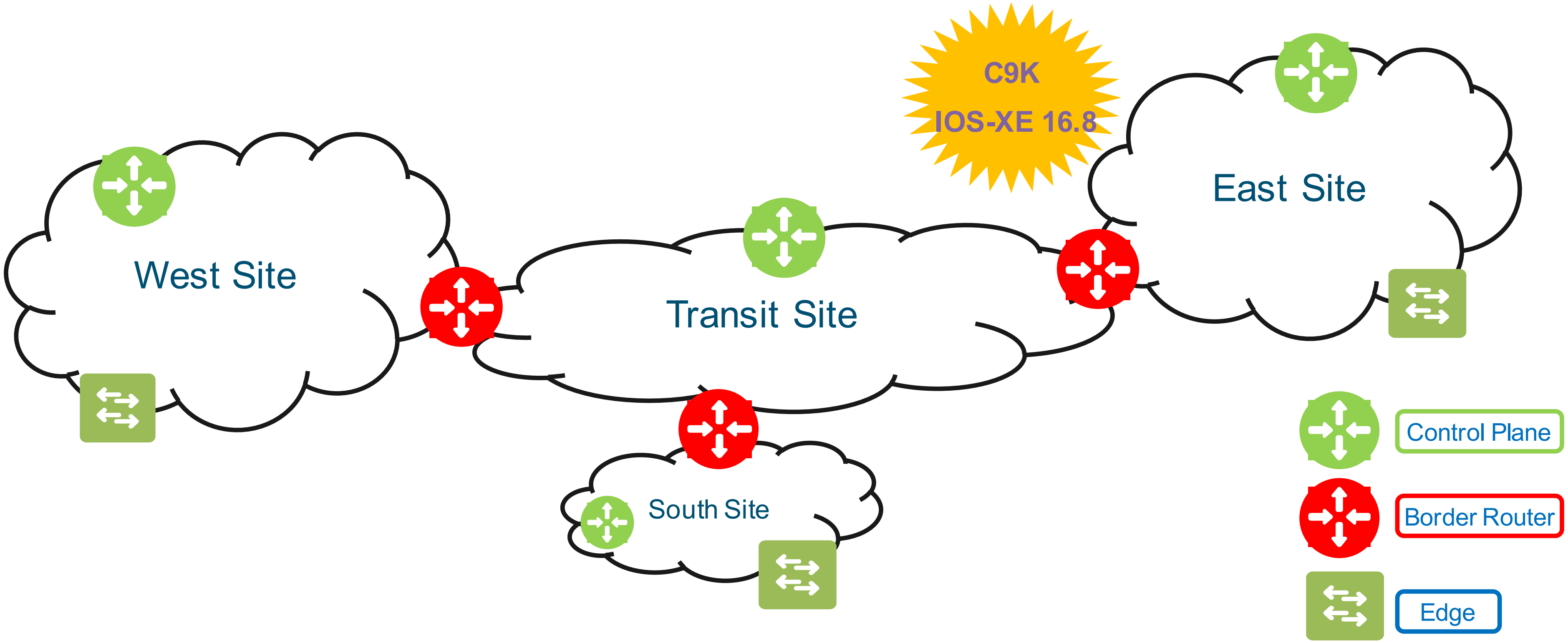
Border Deployment Options

Multiple Fabric Domains



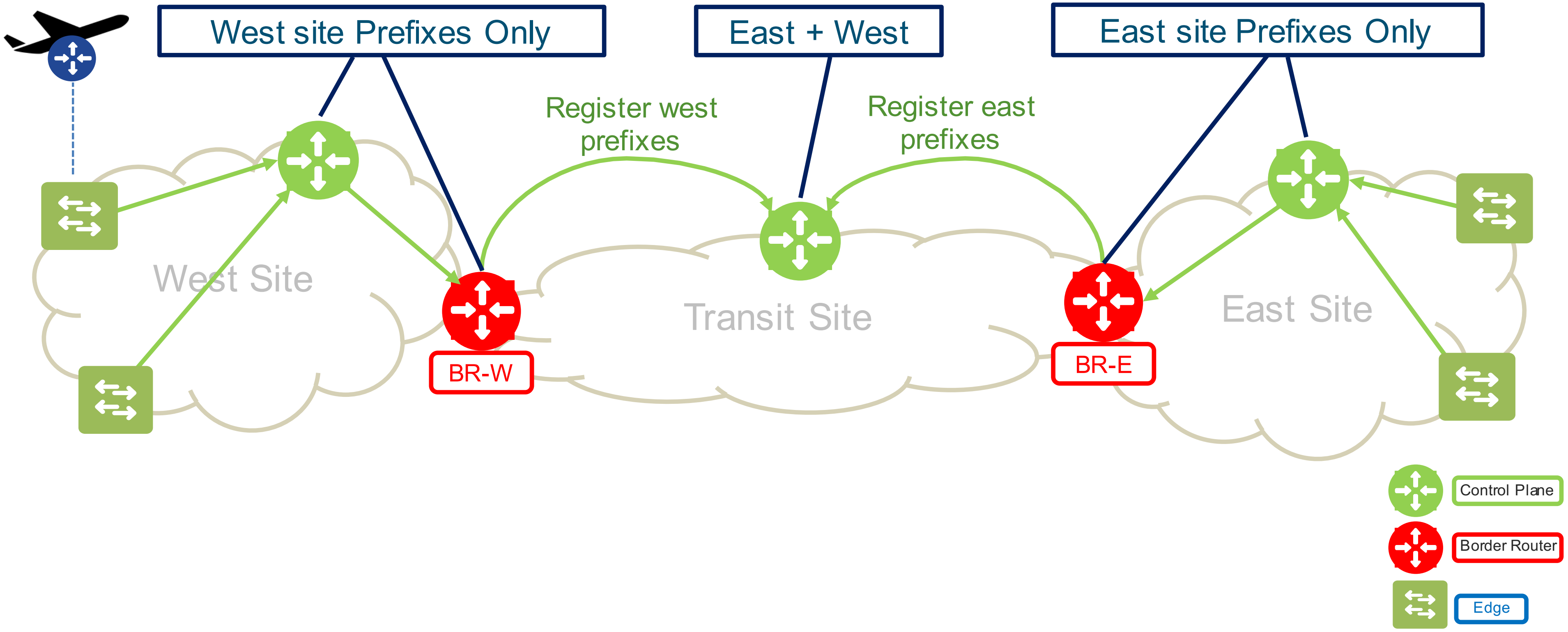
Border Deployment Options

SD-Access Multi-Site



Border Deployment Options

SD-Access Multi-Site



Cisco
Connect

Service Chaining with Border

Border Deployment Options

Service Chaining with Border

Non-Cisco Firewall:

- Firewall is connected externally to the Campus Fabric.
- The prefixes from the local Campus Fabric domain will be advertised to the firewall with a routing protocol of choice.
- **Firewall policy is based Interface or Subnet IP/mask and IP ACL's.**

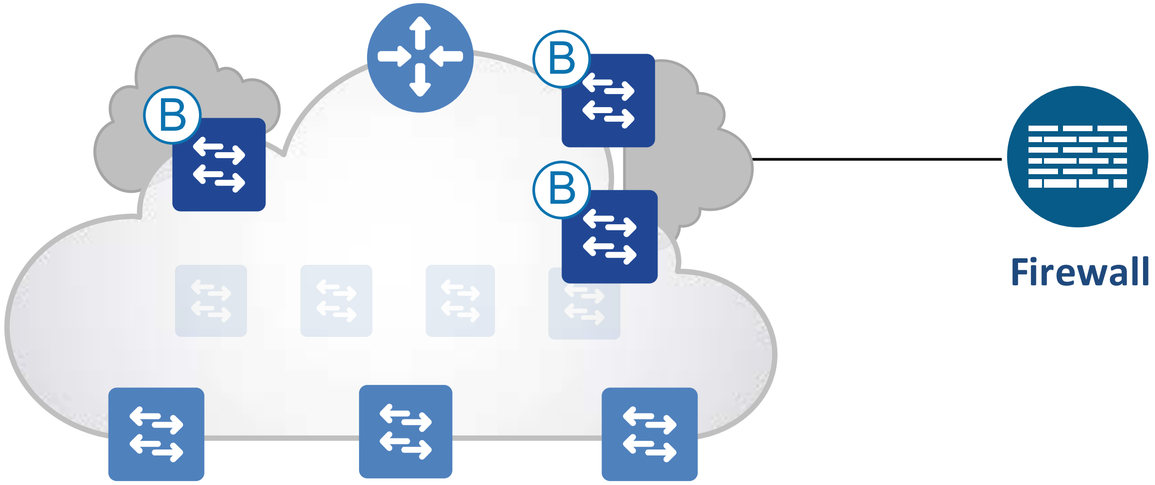
Cisco Firewall :

- Firewall is connected externally to the Campus Fabric.
- The prefixes from the local Campus Fabric domain will be advertised to the firewall with a routing protocol of choice.
- **SXP connection between ISE and Firewall used for derivation of SGTs on the Firewall.**
- **Firewall policy is based on SGT's and SG ACL's (Group based Policy).**
- Firewall also has Interface or Subnet IP based policy, for brownfield integration

Border Deployment Options

Service Chaining with Border - Firewall

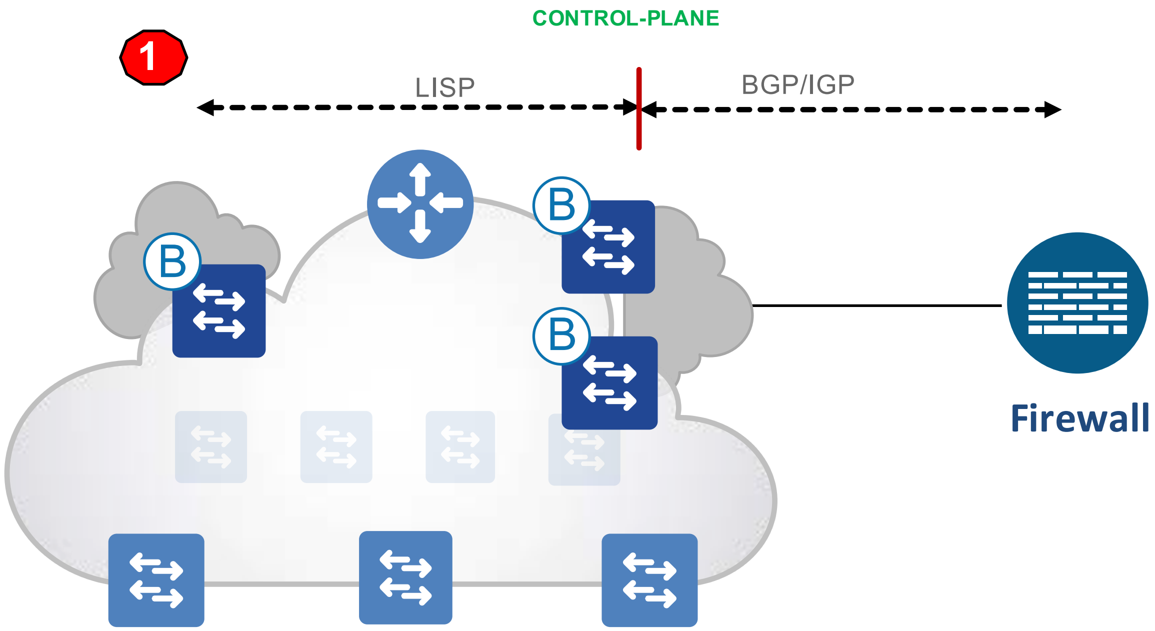
Cisco Connect



Border Deployment Options

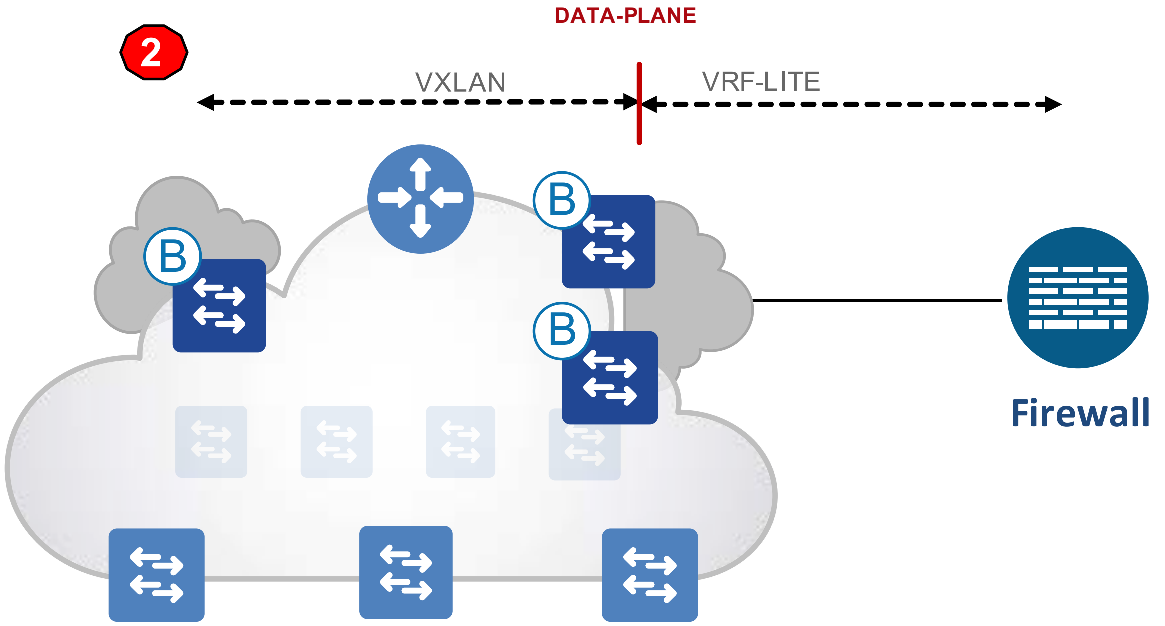
Service Chaining with Border - Firewall

Cisco Connect



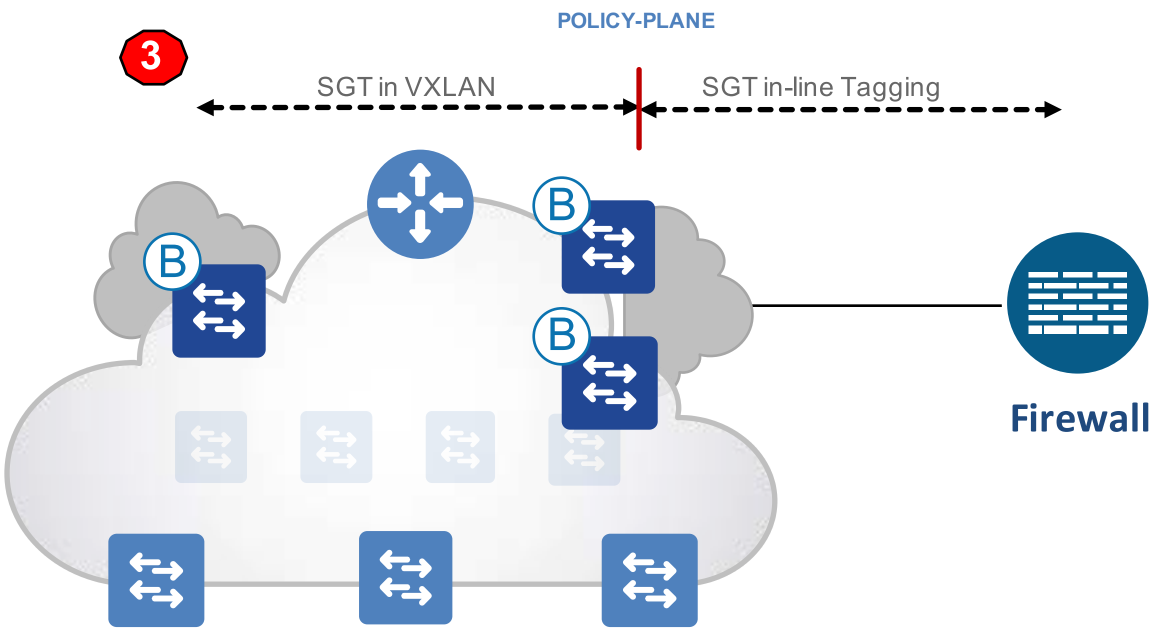
Border Deployment Options

Service Chaining with Border – Data-Plane (Routed firewall)



Border Deployment Options

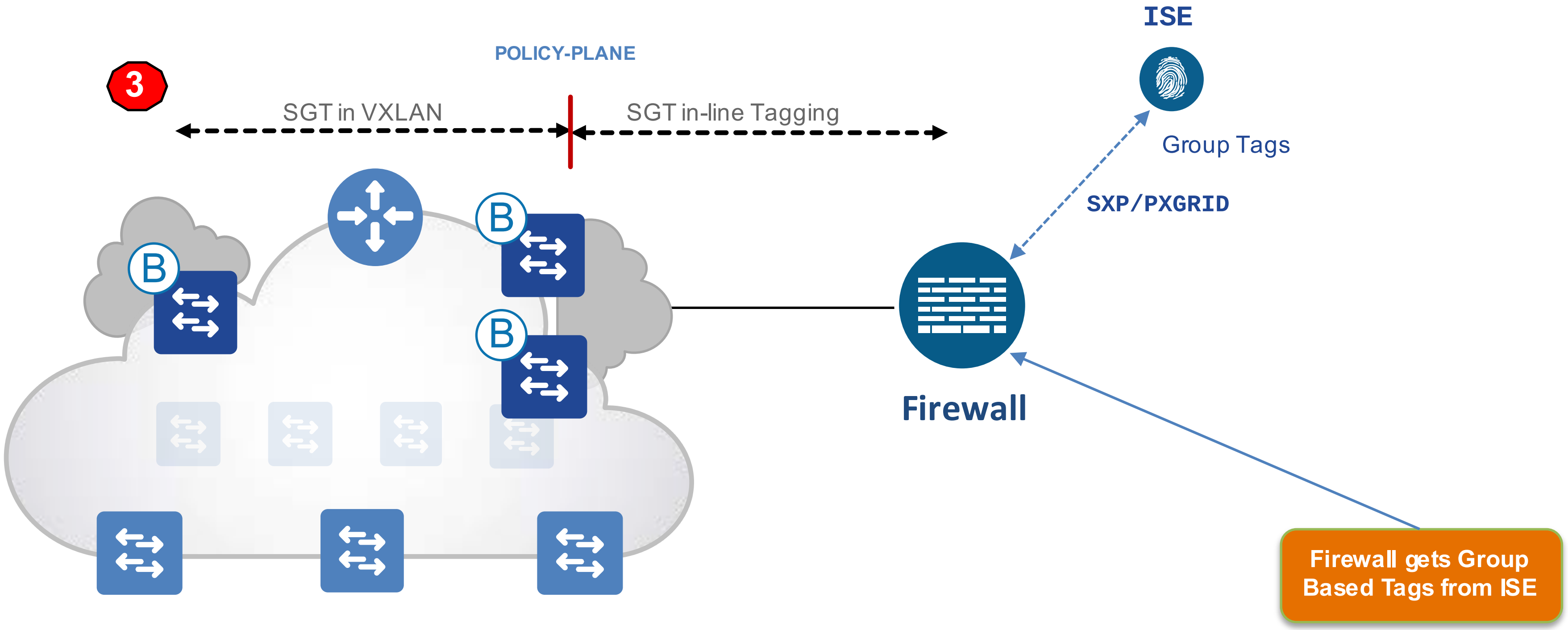
Service Chaining with Border – Policy Plane



Border Deployment Options

Service Chaining with Internal Border – Cisco Firewall, Checkpoint

Cisco Connect



Firewall gets Group Based Tags from ISE

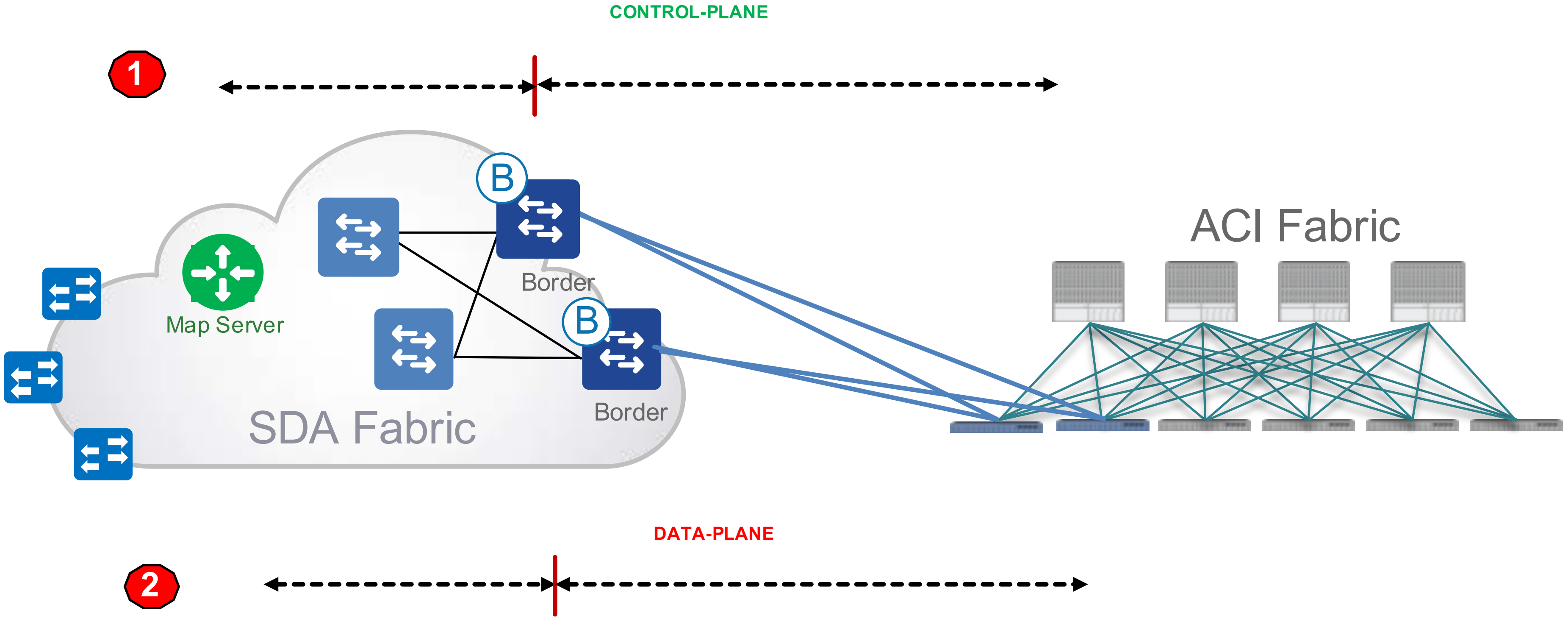
Cisco
Connect

Data Center Connectivity with Border

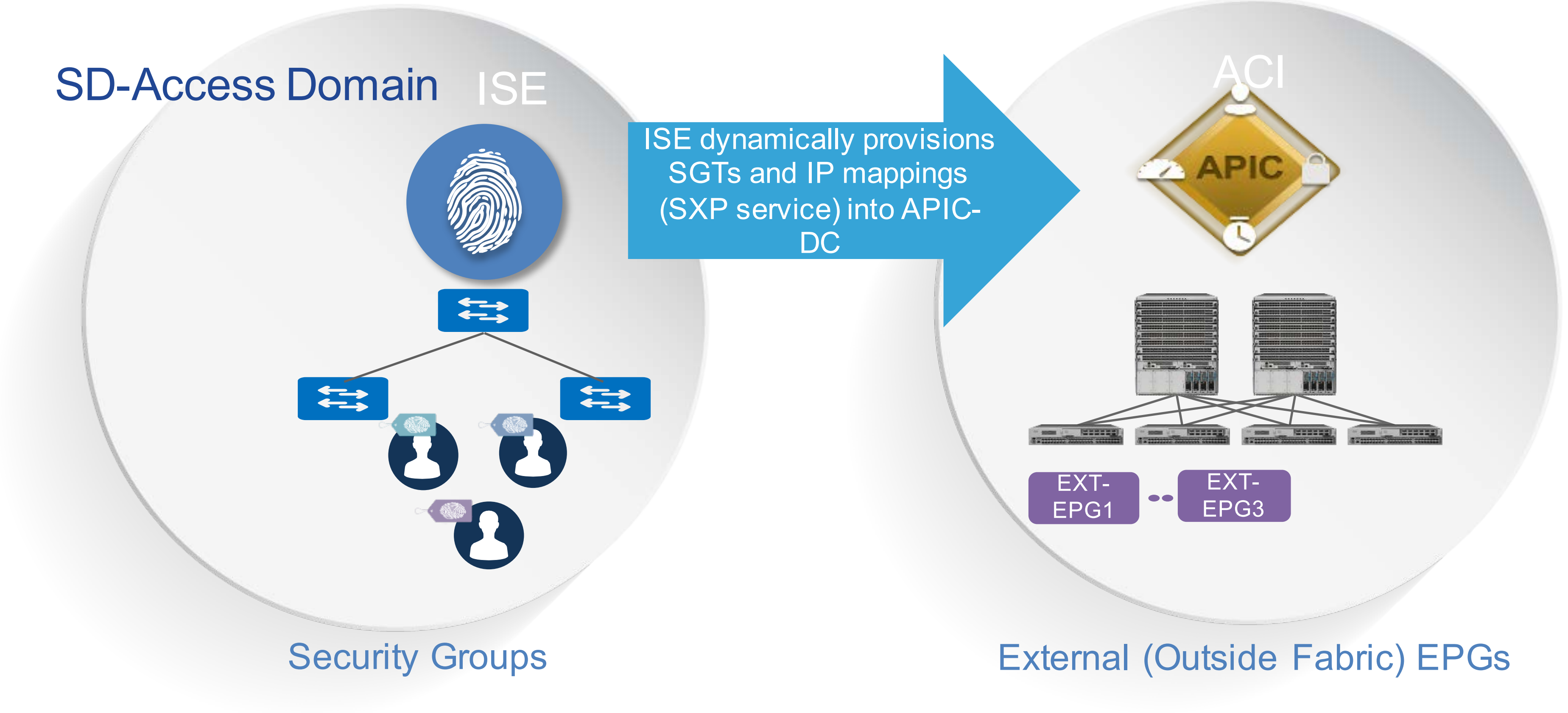
Border Deployment Options

Data Center Connectivity With Border – ACI Fabric

Cisco Connect



SD-Access SGTs Provisioned in ACI



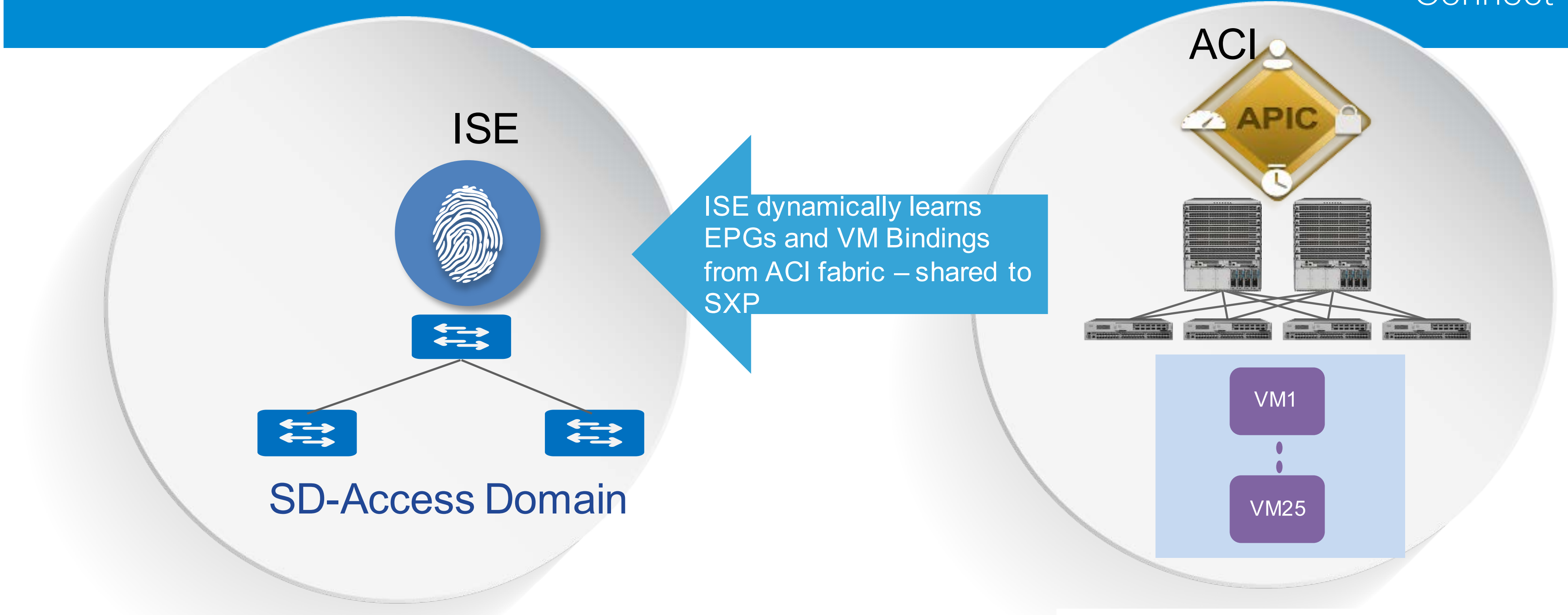
SD-Access Domain

ISE dynamically provisions SGTs and IP mappings (SXP service) into APIC-DC

Security Groups

External (Outside Fabric) EPGs

ACI EPGs Automatically Propagated into SD-Access

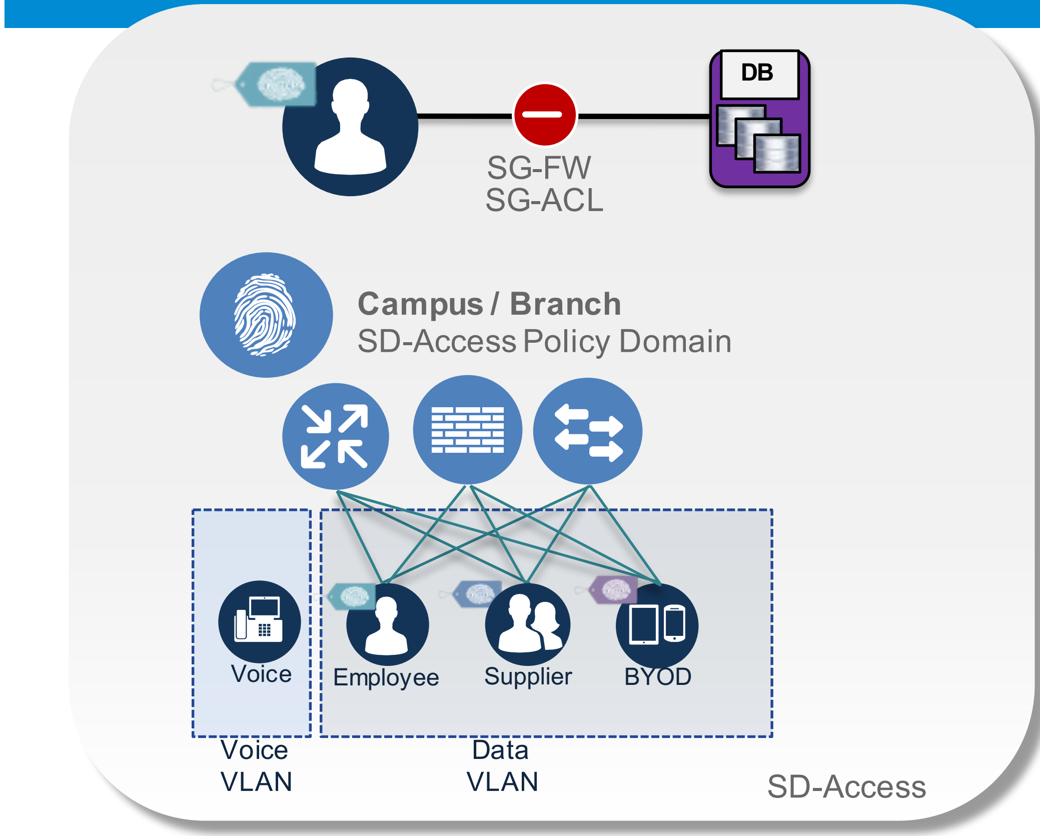


ISE dynamically learns EPGs and VM Bindings from ACI fabric – shared to SXP

Security Group from APIC-DC

Internal (Inside Fabric) EPGs

Enabling Group-based Policy in each Domain



SG-FW
SG-ACL

DB

Campus / Branch
SD-Access Policy Domain

Voice

Employee

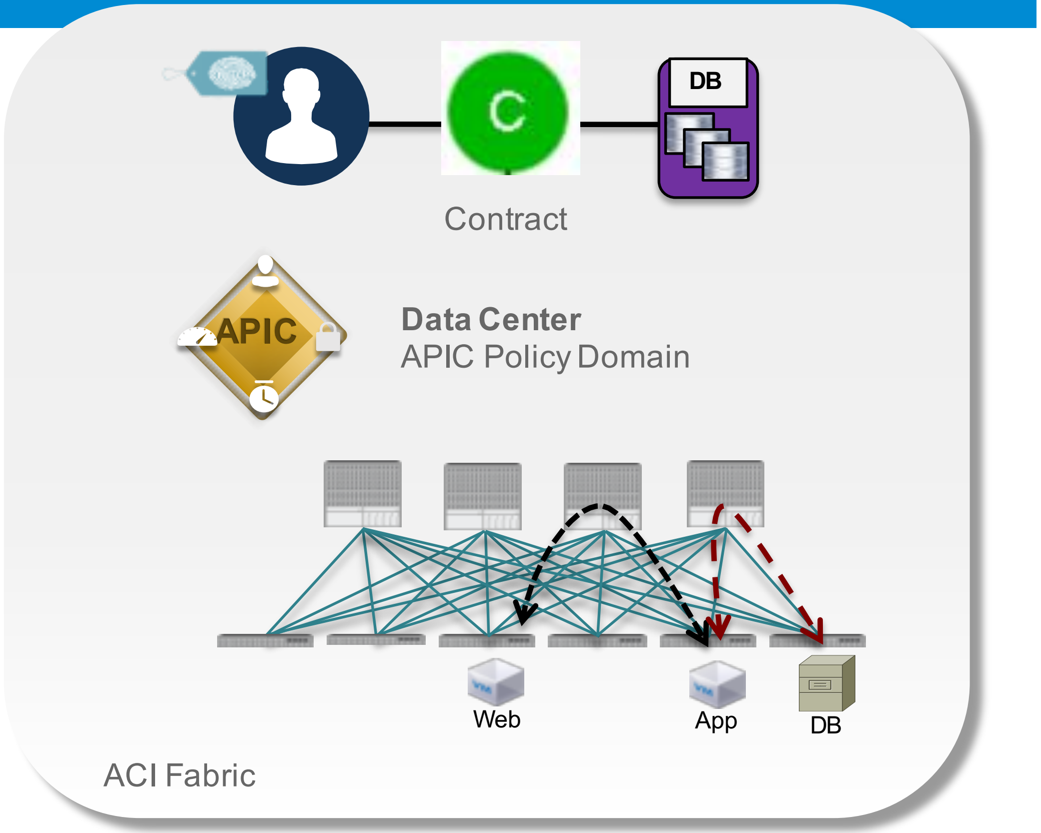
Supplier

BYOD

Voice
VLAN

Data
VLAN

SD-Access



Contract

DB

Data Center
APIC Policy Domain

Web

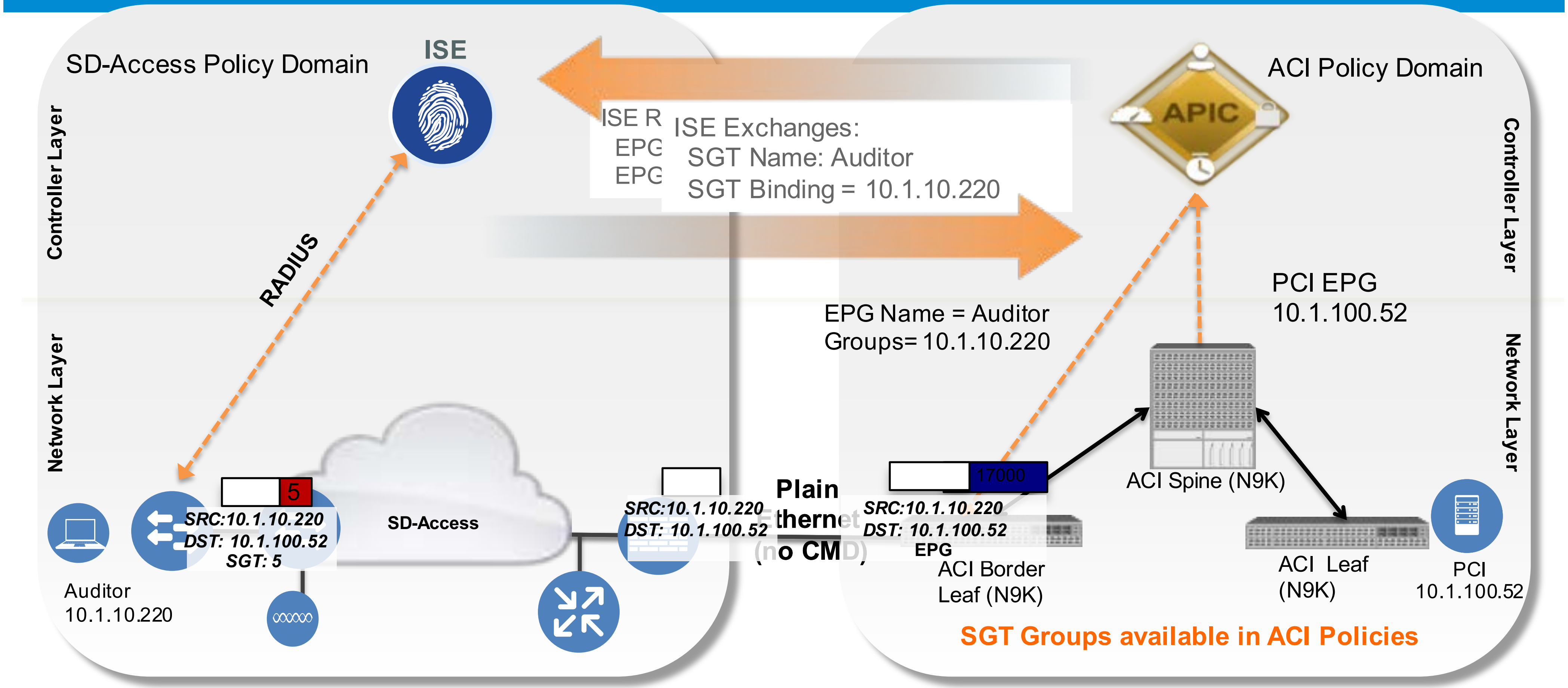
App

DB

ACI Fabric

SD-Access SGT Info Used in ACI Policies

Cisco Connect



SD-Access Policy Domain

ISE

Controller Layer

Network Layer

RADIUS

ISE R
EPG
EPG

ISE Exchanges:
SGT Name: Auditor
SGT Binding = 10.1.10.220

ACI Policy Domain

APIC

Controller Layer

Network Layer

PCI EPG
10.1.100.52

EPG Name = Auditor
Groups= 10.1.10.220

5

SRC:10.1.10.220
DST: 10.1.100.52
SGT: 5

SD-Access

Auditor
10.1.10.220

SRC:10.1.10.220
DST: 10.1.100.52

Plain
Ethernet
(no CMD)

17000

SRC:10.1.10.220
DST: 10.1.100.52
EPG

ACI Spine (N9K)

ACI Border
Leaf (N9K)

ACI Leaf
(N9K)

PCI
10.1.100.52

SGT Groups available in ACI Policies

Cisco
Connect

Take Away
When to get started?

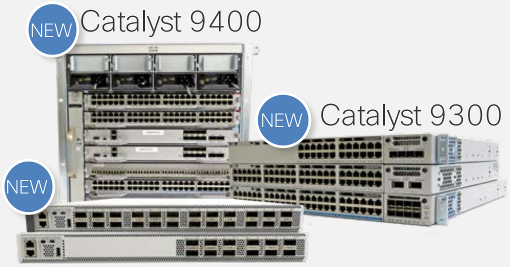
SD-Access Support

Fabric ready platforms for your digital ready network

Cis

Co

Switching


NEW Catalyst 9400

NEW Catalyst 9300

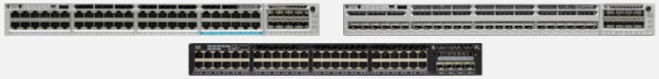
NEW

Catalyst 9500

Catalyst 4500E

Catalyst 6800

Nexus 7700


Catalyst 3650 and 3850

Routing

ASR-1000-X

ASR-1000-HX

ISR 4430

BRKCRS 2811

ISR 4450

ISRv/CSRv

Wireless

AIR-CT5520

AIR-CT8540

NEW

AIR-CT3504

NEW

Wave 2 APs (1800,2800,3800)

Wave 1 APs* (1700,2700,3700)

Extended

NEW

CDB

3560-CX

NEW

IE (2K/3K/4K/5K)

* with Caveats

The First Step...

#NewEra
#CiscoDNA
#NetworkIntuitive

CISCO