Cisco SD-Access

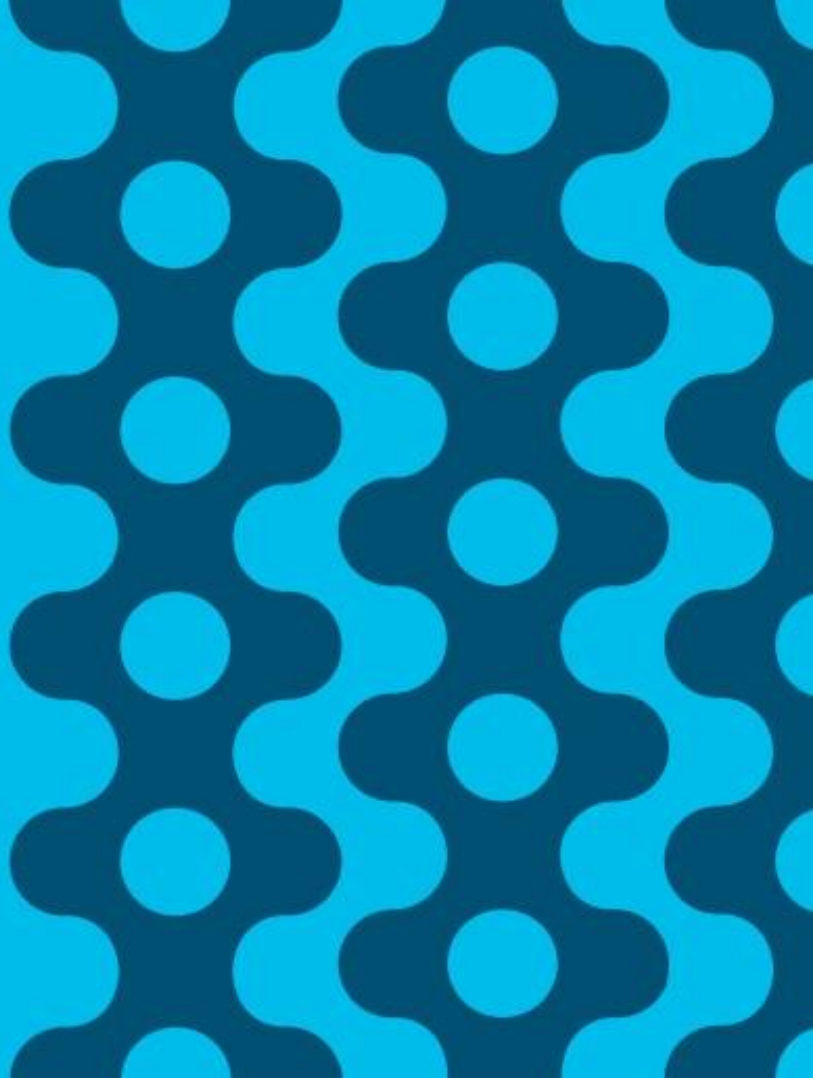
Connecting to the Data Center, Firewall, WAN and More !

Vedran Hafner, vehafner@cisco.com
Systems Engineer Manager

Agenda

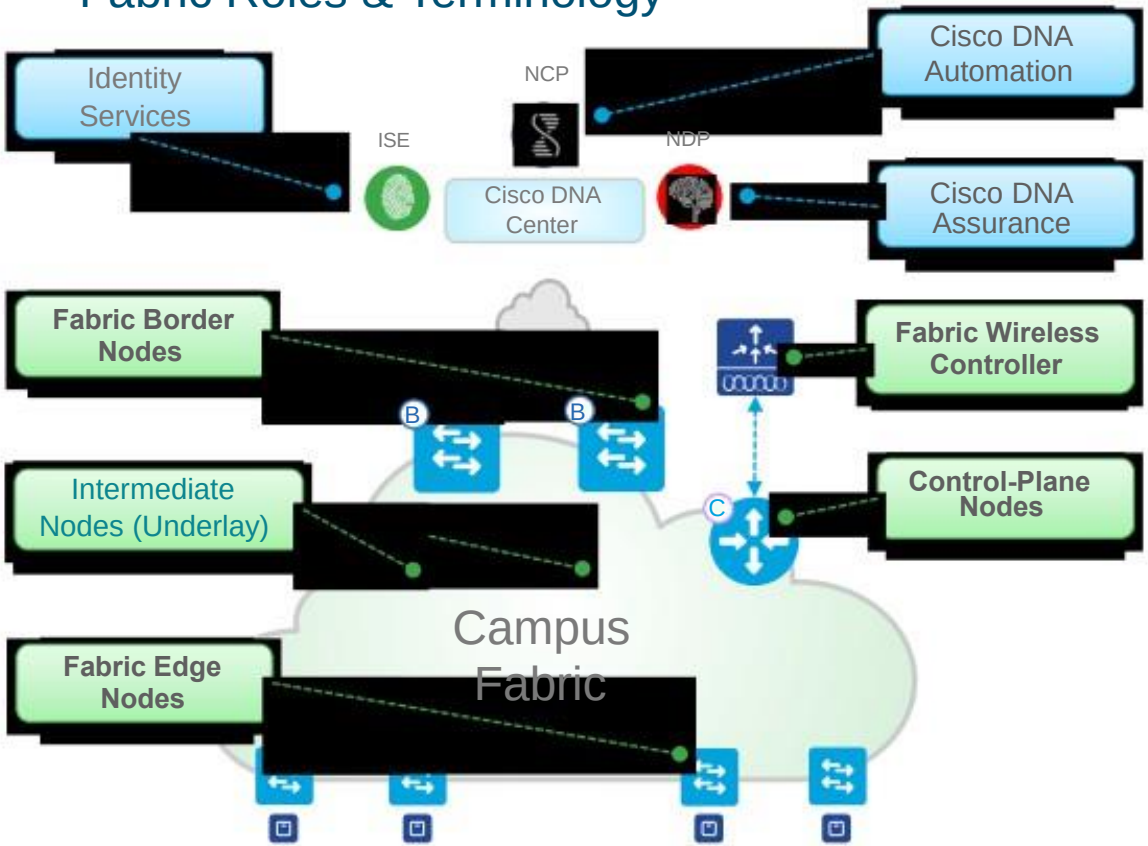
- Introduction to Cisco SD-Access
  - Fabric Roles and Constructs
- Enterprise Network Design
  - Traditional vs Cisco SD-Access Network Design
  - Border Design Options
- Border Connectivity Models
  - Connecting to Internal networks like DC & WAN
  - Connecting to external networks like Internet & Cloud
- Small Enterprise Network Design
  - Traditional vs Cisco SD-Access Network Design
  - Border Design Options
- Conclusion

Fabric Roles and Constructs



Cisco SD-Access

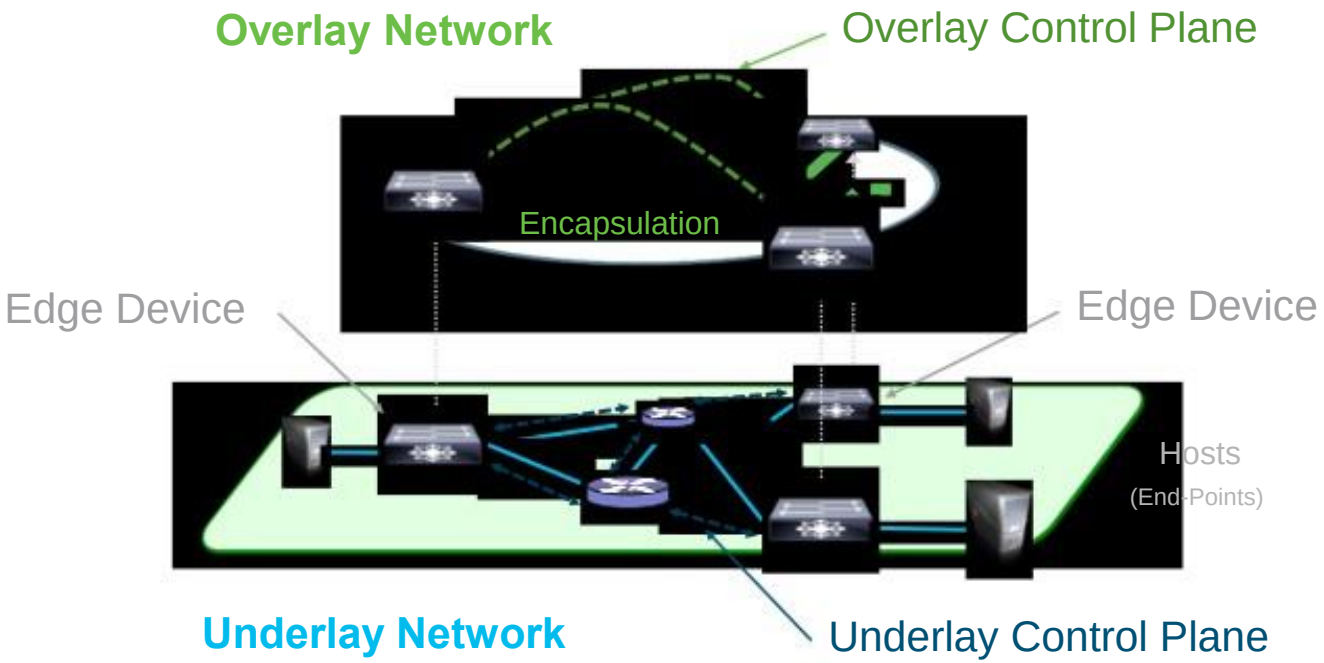
Fabric Roles & Terminology



- **Cisco DNA Automation** - provides simple GUI management and intent based automation (e.g. NCP) and context sharing
- **Cisco DNA Assurance** - Data Collectors (e.g. NDP) analyze Endpoint to App flows and monitor fabric status
- **Identity Services** - NAC & ID Systems (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition
- **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 APs and Wireless Endpoints to the SDA Fabric

Cisco SD-Access

Fabric Terminology

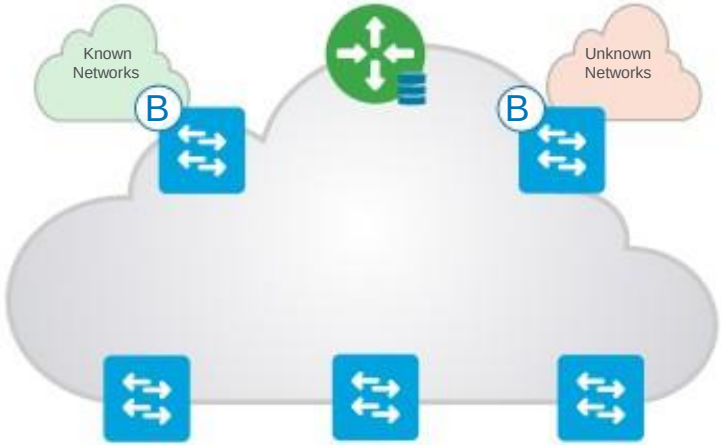


Cisco SD-Access Fabric

Control-Plane Nodes - A Closer Look

Control-Plane Node runs a Host Tracking Database to map location information

- A simple Host Database that maps Endpoint IDs to a current Location, along with other attributes
- Host Database supports multiple types of Endpoint ID lookup types (IPv4, IPv6 or MAC)
- Receives Endpoint ID map registrations from Edge and/or Border Nodes for “known” IP prefixes
- Resolves lookup requests from Edge and/or Border Nodes, to locate destination Endpoint IDs

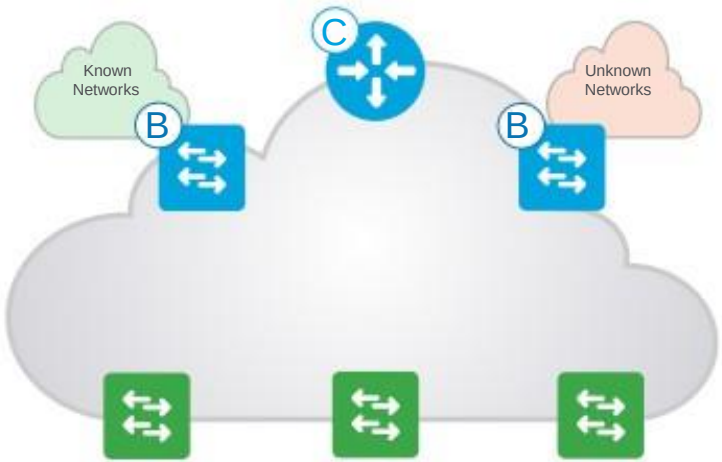


Cisco SD-Access Fabric

Edge Nodes - A Closer Look

Edge Node provides first-hop services for Users / Devices connected to a Fabric

- Responsible for Identifying and Authenticating Endpoints (e.g. Static, 802.1X, Active Directory)
- Register specific Endpoint ID info (e.g. /32 or /128) with the Control-Plane Node(s)
- Provide an Anycast L3 Gateway for the connected Endpoints (same IP address on all Edge nodes)
- Performs encapsulation / de-encapsulation of data traffic to and from all connected Endpoints



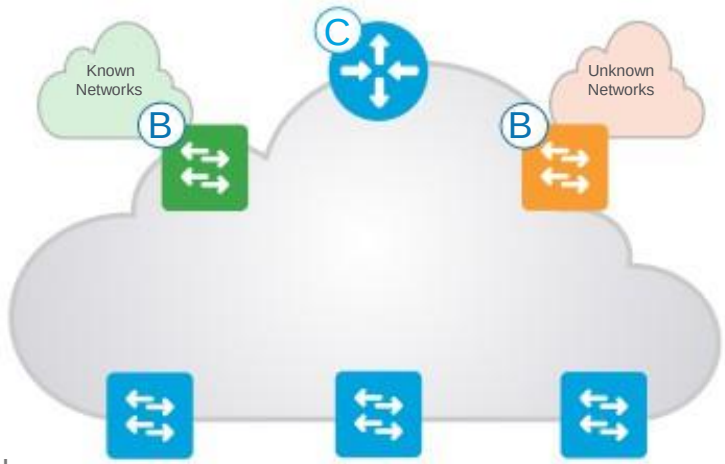
Cisco SD-Access Fabric

Border Nodes

Border Node is an Entry & Exit point for data traffic going Into & Out of a Fabric

There are **3 Types** of **Border Node**!

- **Rest of Company/Internal Border** Used for "Known" Routes inside your company
- **Outside World/External Border** Used for "Unknown" Routes outside your company
- **Anywhere/External + Internal Border** Used for "Known" and "UnKnown" Routes for your company

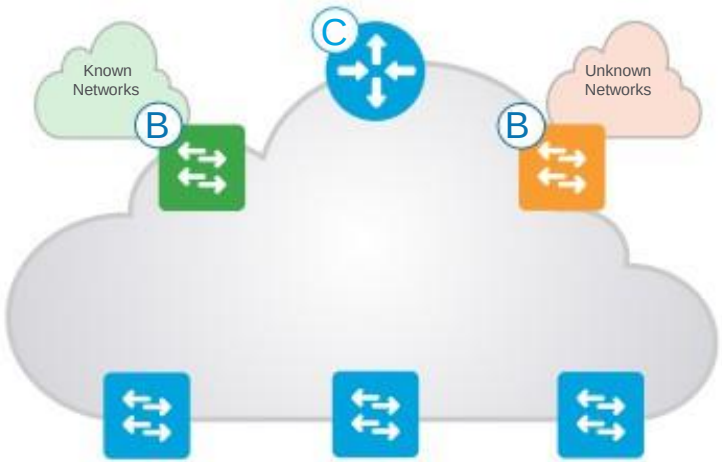


Cisco SD-Access Fabric

Border Nodes - Rest of Company/Internal

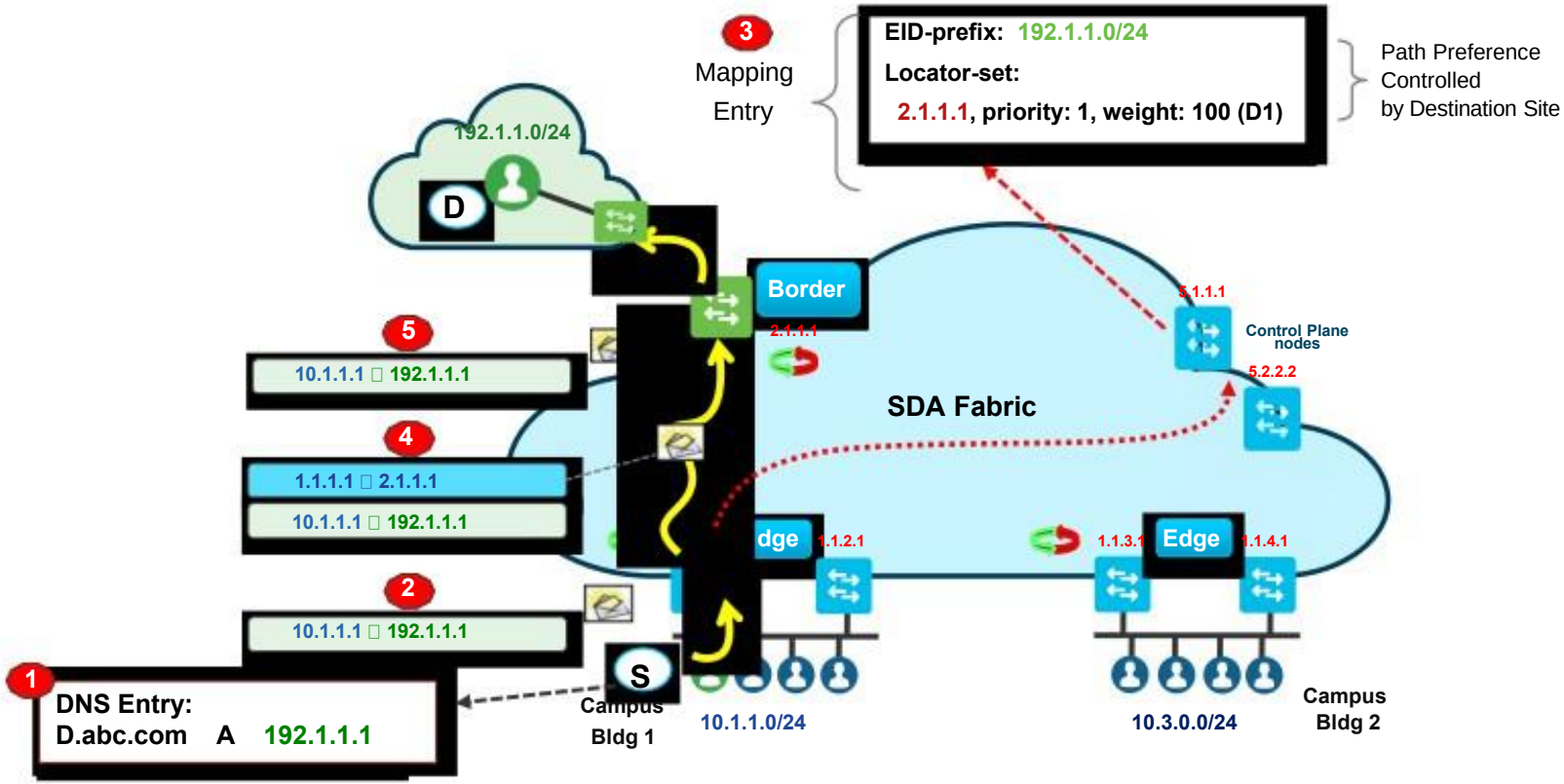
Rest of Company/Internal Border advertises Endpoints to outside, and known Subnets to inside

- Connects to any “known” IP subnets available from 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).
- Importsand registers (known) IP subnets from outside, into the Control-Plane Map System except the default route.
- Hand-off requires mapping the context (VRF & SGT) from one domain to another.



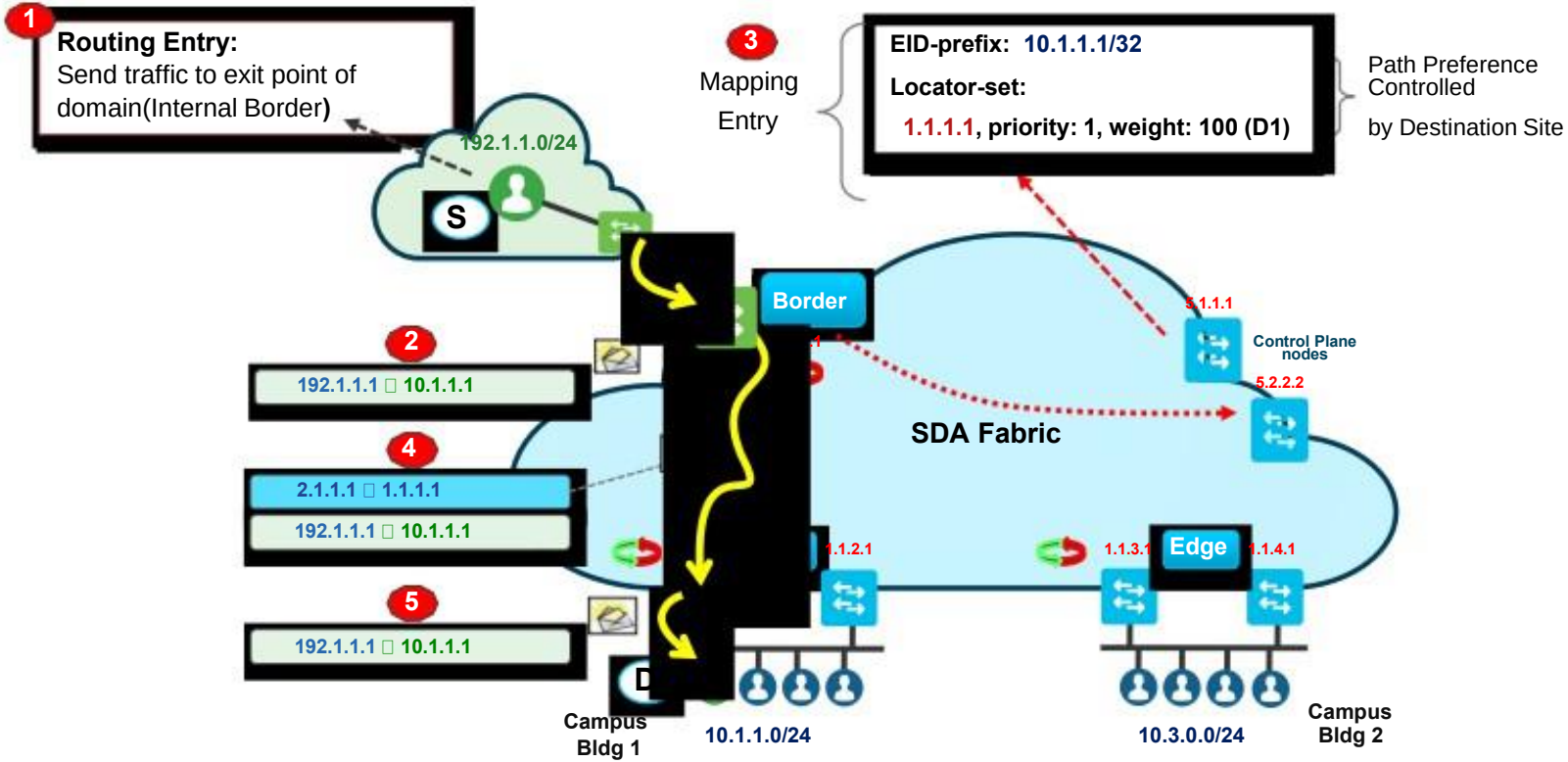
Cisco SD-Access Fabric

Border Nodes - Forwarding from Fabric to External Domain



Cisco SD-Access Fabric

Border Nodes - Forwarding from External to Fabric Domain

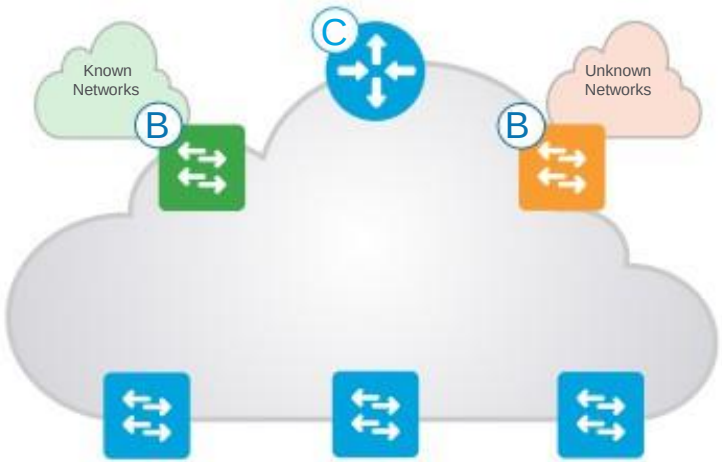


Cisco SD-Access Fabric

Border Nodes - Outside World/External

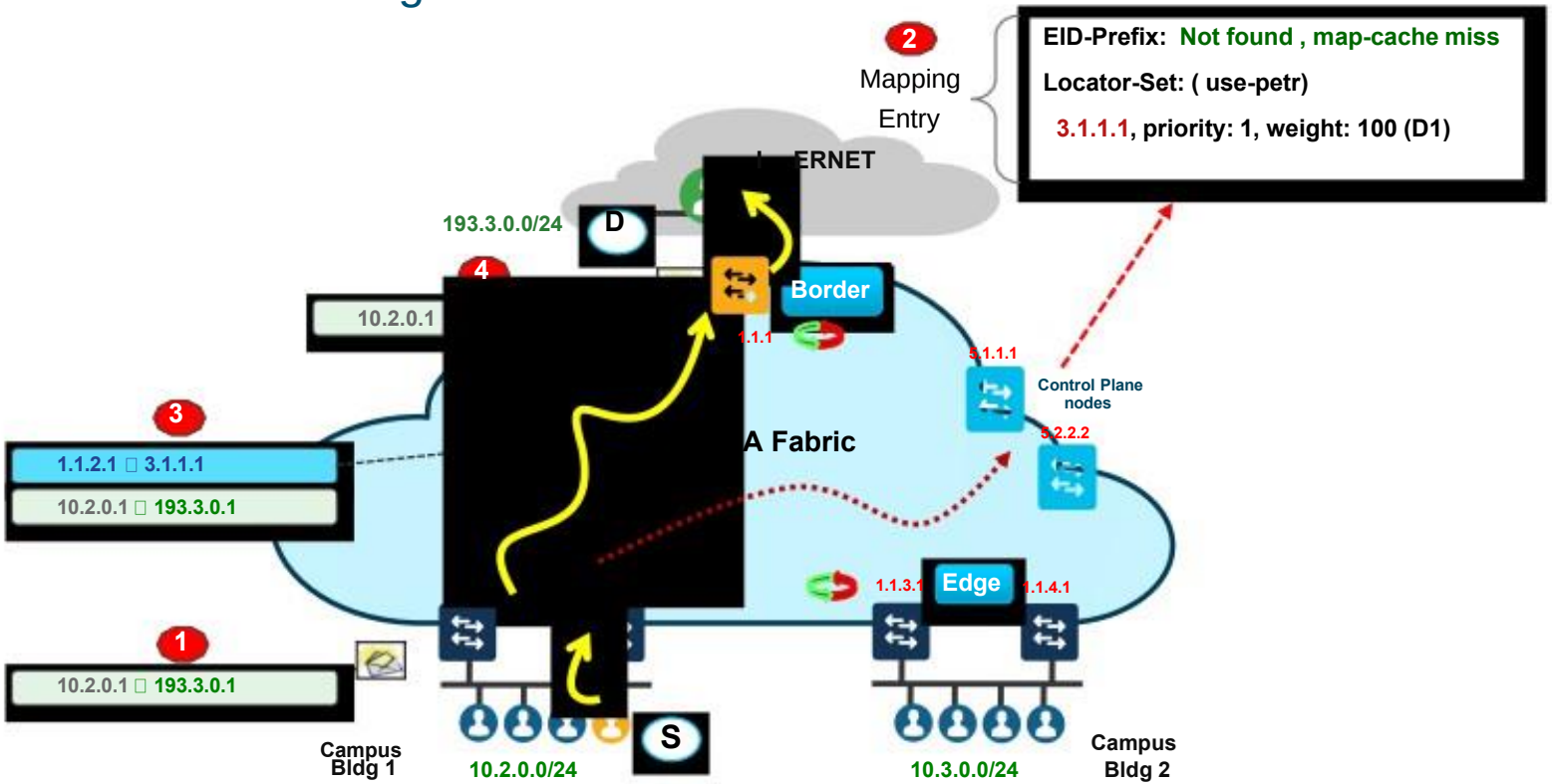
Outside World/External Border is a “Gateway of Last Resort” for any unknown destinations

- Connects to any “unknown” IP subnets, outside of the network (e.g. Internet, Public Cloud)
- Exports all internal IP Pools outside (as aggregate) into traditional IP routing protocol(s).
- Does NOT import any routes! It is a “default” exit, if no entry is available in Control-Plane.
- Hand-off requires mapping the context (VRF & SGT) from one domain to another.



Cisco SD-Access Fabric

Border Nodes - Forwarding from Fabric to External Domain

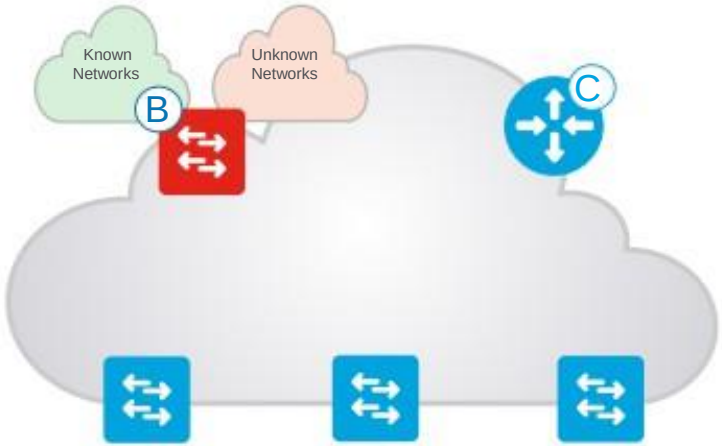


Cisco SD-Access Fabric

Border Nodes - Anywhere/ Internal + External Border

Anywhere/ Internal + External Border is a “One all exit point” for any known and unknown destinations

- Connects to any “unknown” IP subnets, outside of the network (e.g. Internet, Public Cloud) and “known” IP subnets available from the outside network (e.g. DC, WLC, FW, etc.)
- Imports and registers (known) IP subnets from outside, into the Control-Plane Map System except the default route.
- Exports all internal IP Pools outside (as aggregate) into traditional IP routing protocol(s).

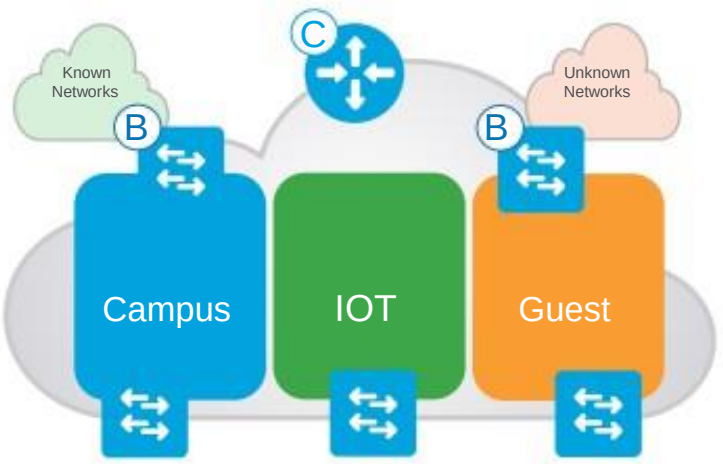


Cisco SD-Access Fabric

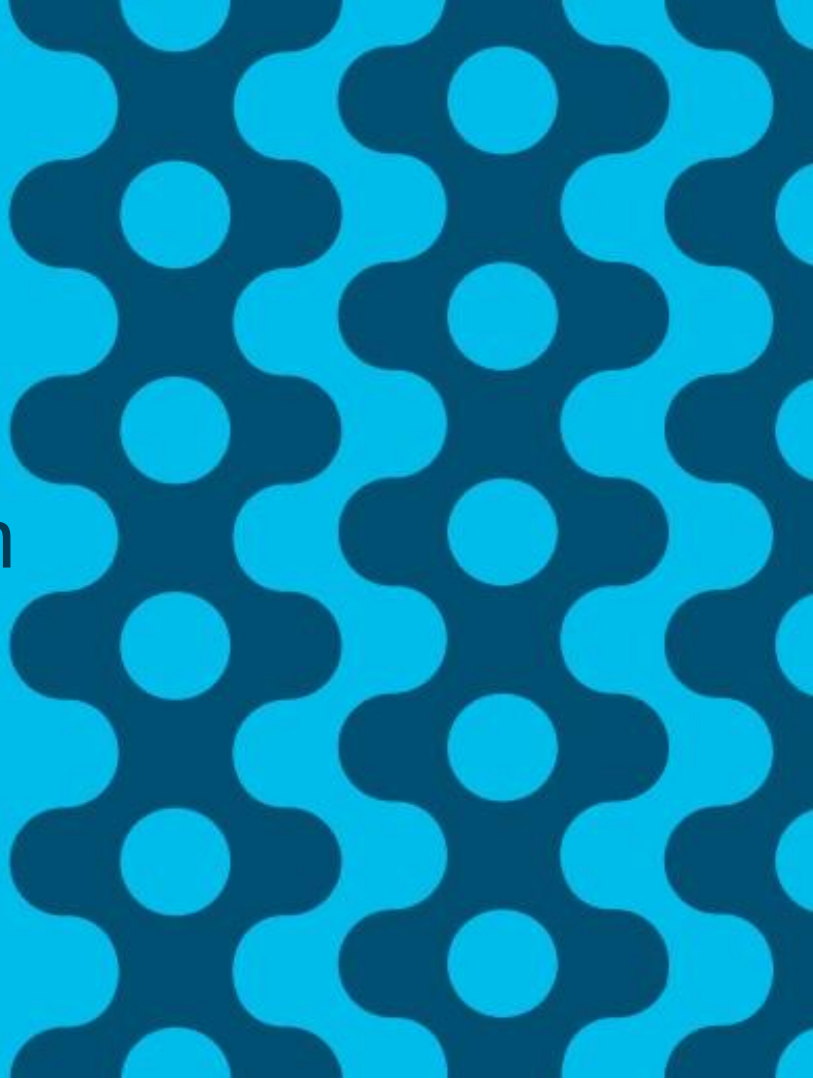
Virtual Network- A Closer Look

Virtual Network maintains a separate Routing & Switching table for each instance

- Control-Plane uses Instance ID to maintain separate VRF topologies (“Default” VRF is Instance ID “4098”)
- Nodes add a VNID to the Fabric encapsulation
- Endpoint ID prefixes (Host Pools) are routed and advertised within a Virtual Network
- Uses standard “vrf definition” configuration, along with RD & RT for remote advertisement (Border Node)



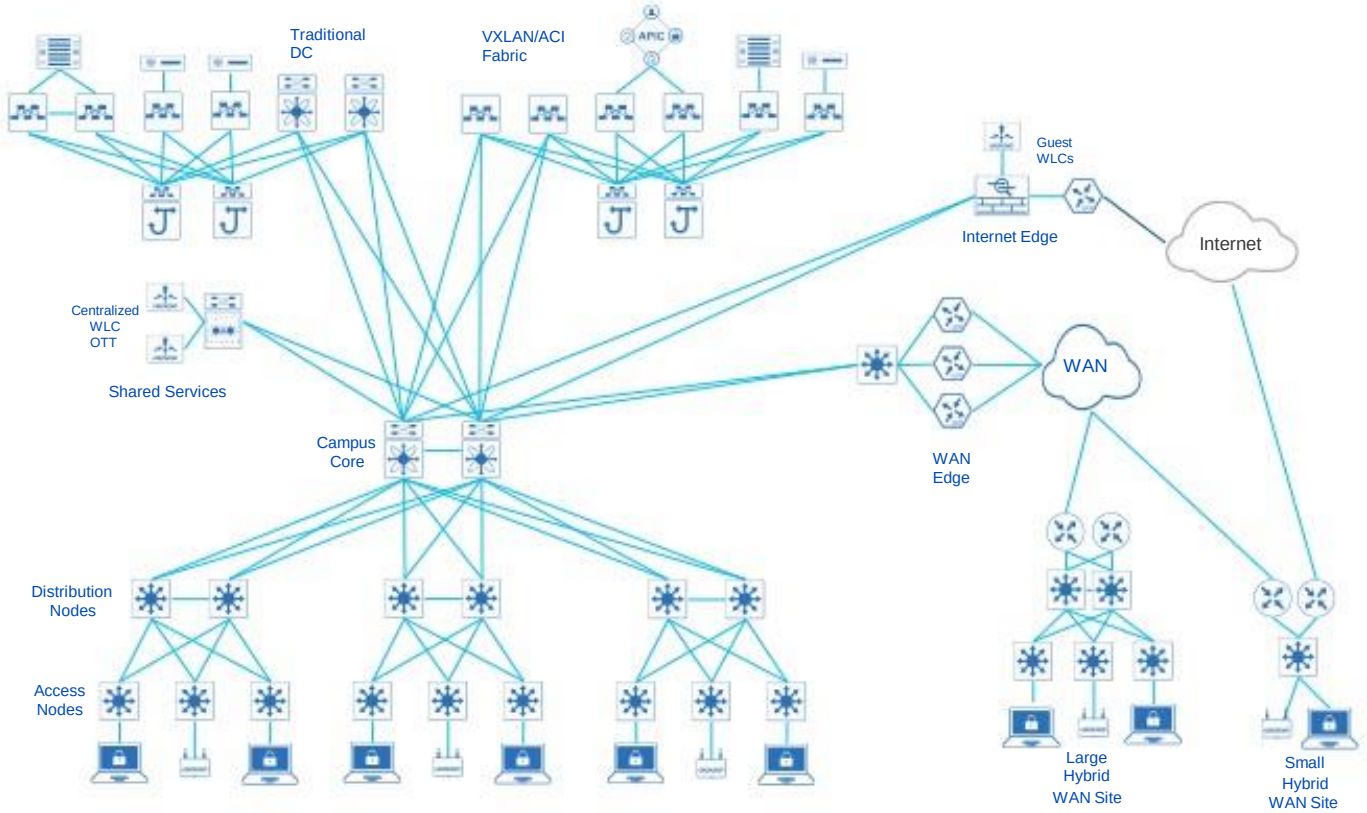
Enterprise Network Design



Traditional Network Design

Cisco SD-Access Fabric

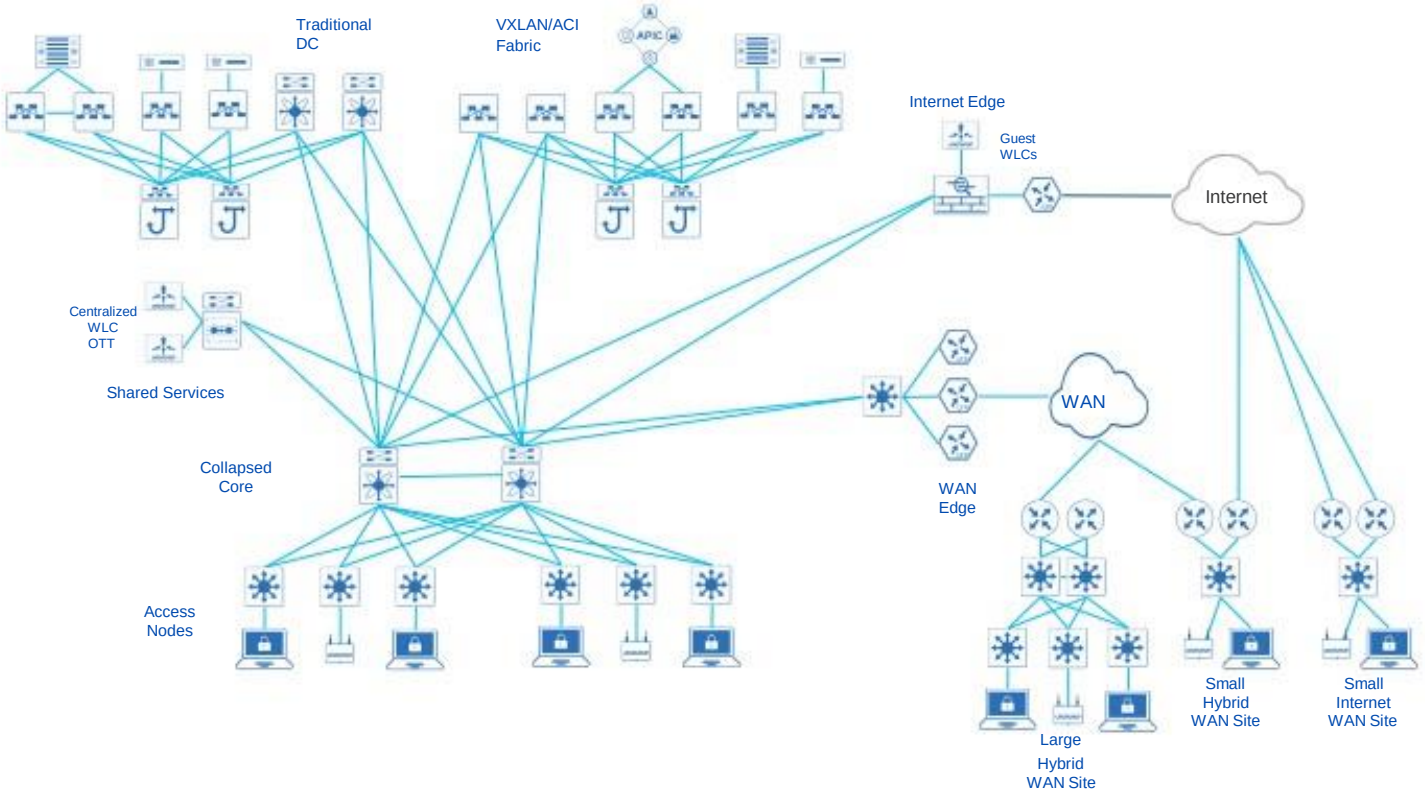
3-Tier Enterprise Network Design - Traditional Network



Role	Platform
Access Node	• Cat3K/9300 • Cat4K/9400
Distribution Node	• Cat3K/9300 • Cat4K/9500 • Cat6K/9500
Core Node	• Cat6K/9500 • NK7K • ASR1K-HX
Centralized WLC	• 8540 • 5520 • x800 APs
WAN HR/MC	• ASR1K • ISR4K
Internet Edge	• ASR1K • ISR4K
Data Center	• N9K - NX-OS • N7K - NX-OS • N9K - ACI
Security	• ISE 2.3 • ASA 55xx • Windows AD

Cisco SD-Access Fabric

Large Enterprise Network Design - Traditional Network

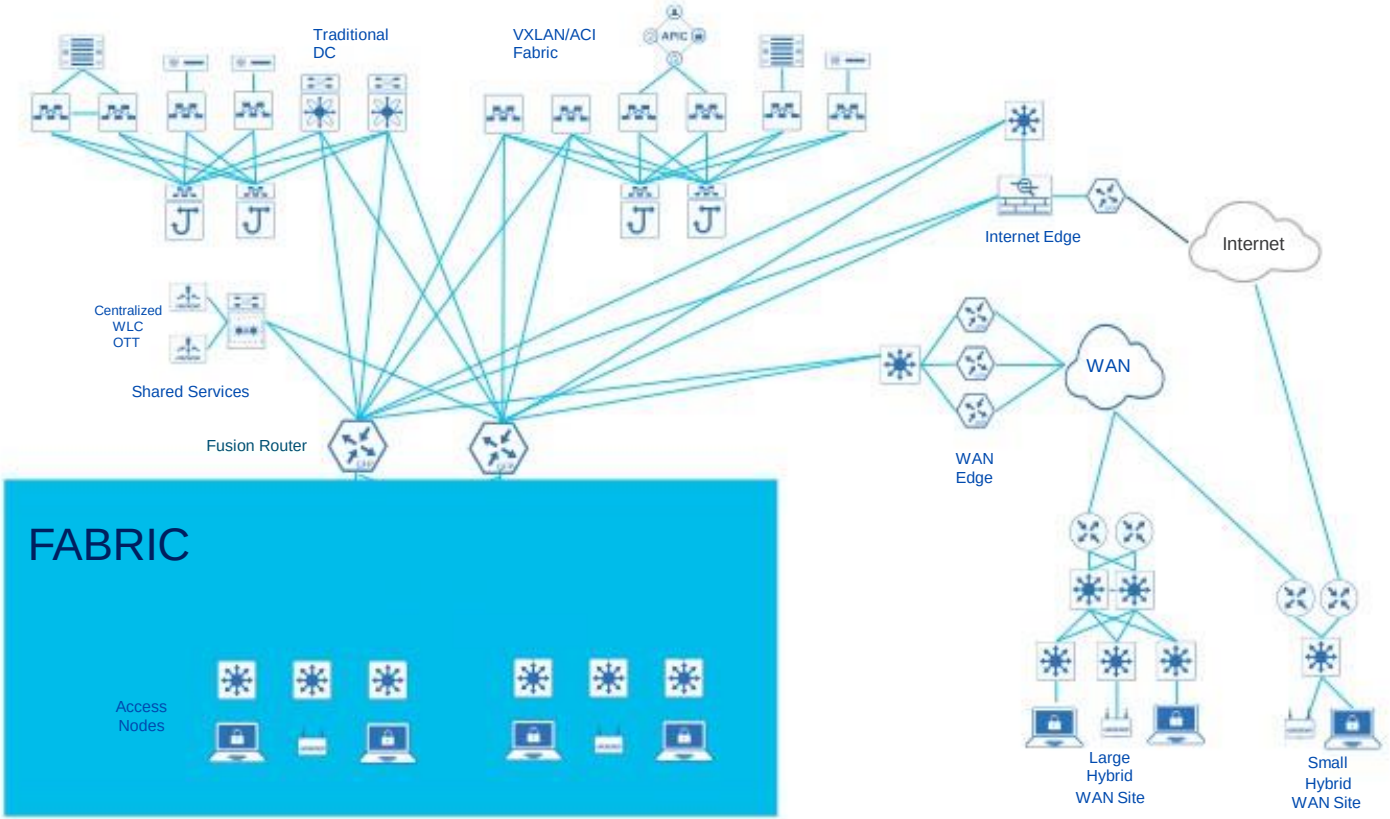


Role	Platform
Access Node	• Cat3K/9300 • Cat4K/9400
Collapsed Core	• Cat6K/9500 • N7K
Centralized WLC	• 5520 • 3504 • x800 APs
WAN HR/MC	• ASR1K • ISR4K
Data Center	• N9K - NX-OS • N7K - NX-OS • N9K - ACI
Security	• ISE 2.3 • ASA 55xx • Windows AD

Cisco SD-Access Network Design

Cisco SD-Access Fabric

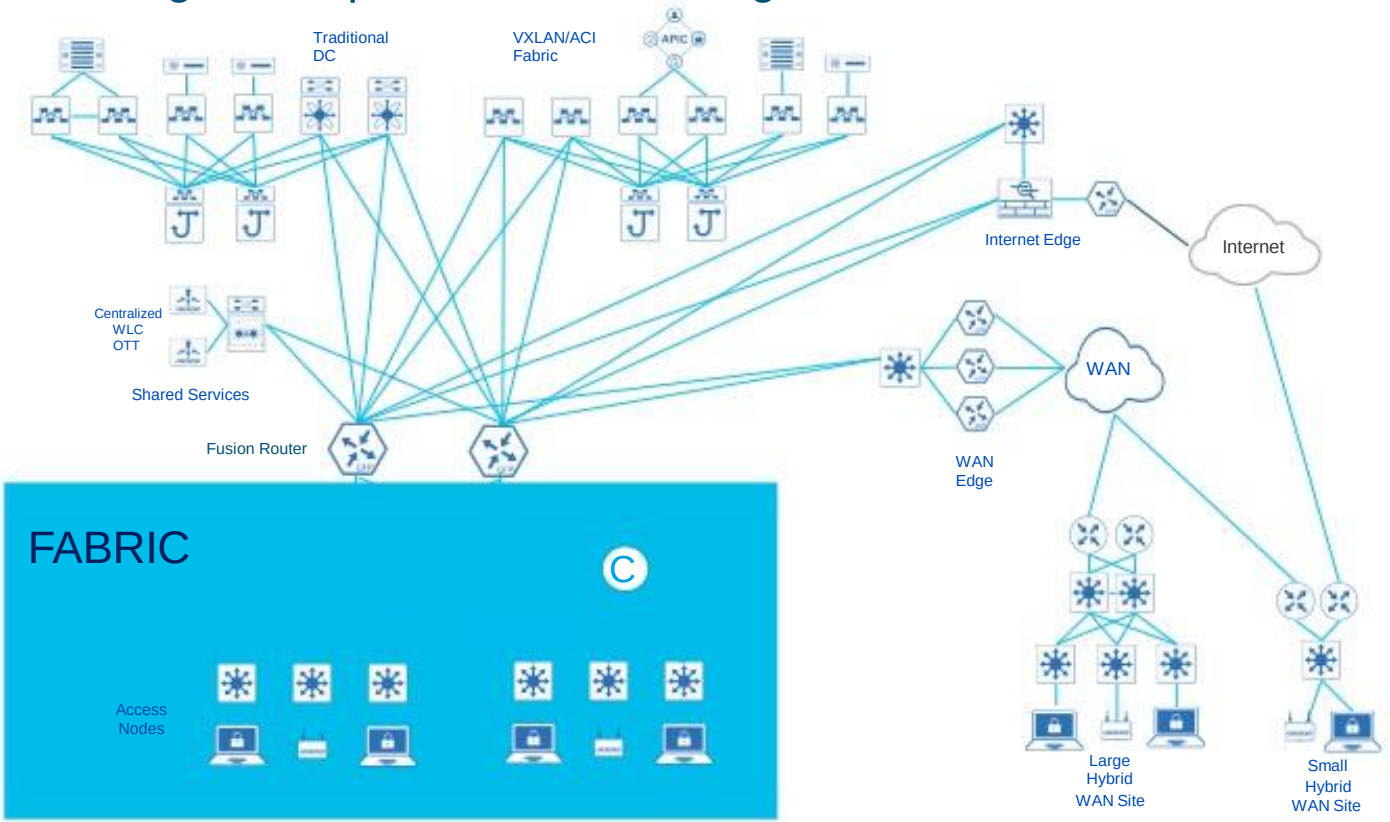
Large Enterprise Network Design - Cisco SD-Access Network



Role	Platform
Access Node	• Cat3K/9300 • Cat4K/9400
Distribution Node	• Cat3K/9300 • Cat4K/9500 • Cat6K/9500
Core Node	• Cat6K/9500 • NK7K • ASR1K-HX
Centralized WLC	• 8540 • 5520 • x800 APs
WAN HR/MC	• ASR1K • ISR4K
Internet Edge	• ASR1K • ISR4K
Data Center	• N9K - NX-OS • N7K - NX-OS • N9K - ACI
Security	• ISE 2.3 • ASA 55xx • Windows AD

Cisco SD-Access Fabric

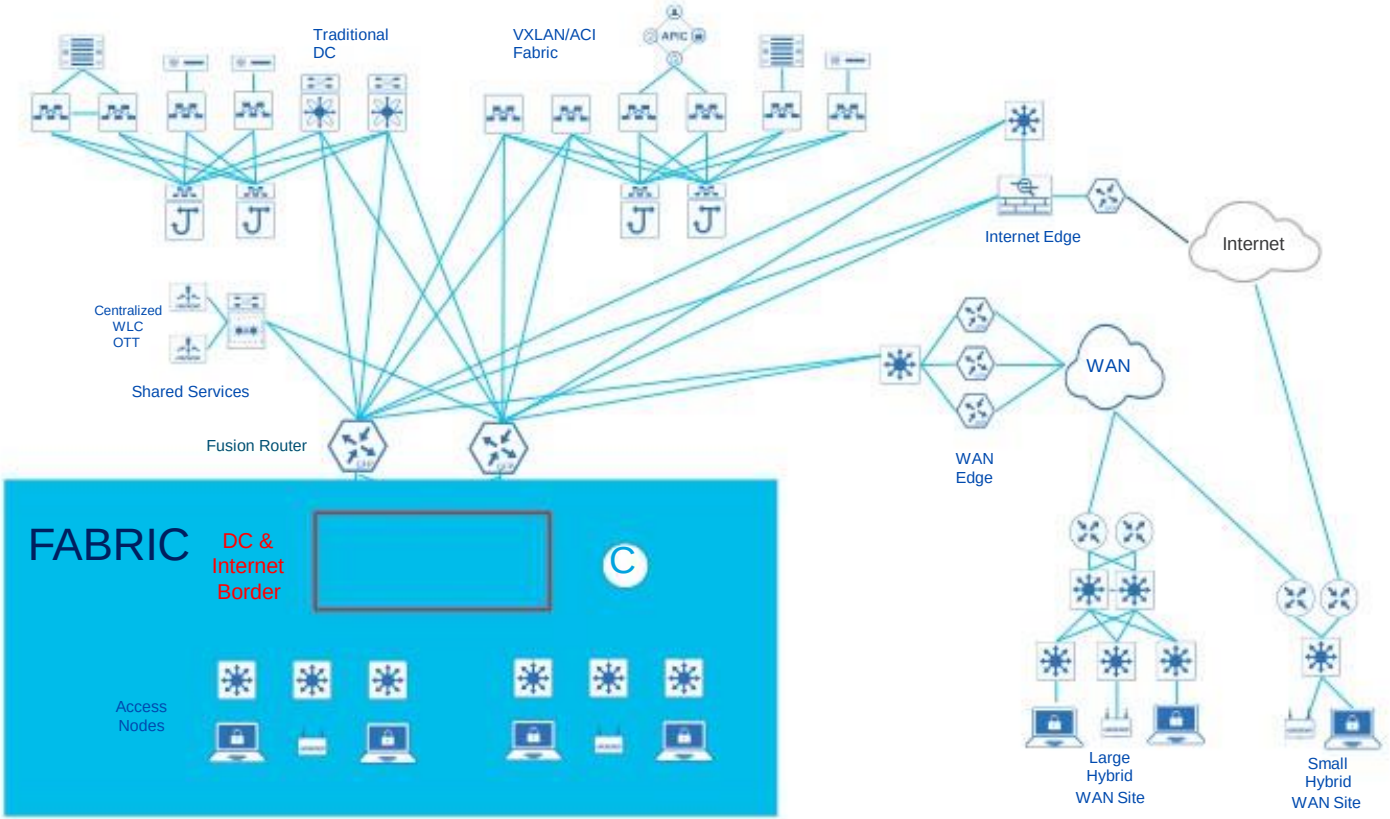
Large Enterprise Network Design - Cisco SD-Access Network



Role	Platform
Access Node	• Cat3K/9300 • Cat4K/9400
Distribution Node	• Cat3K/9300 • Cat4K/9500 • Cat6K/9500
Core Node	• Cat6K/9500 • NK7K • ASR1K-HX
Centralized WLC	• 8540 • 5520 • x800 APs
WAN HR/MC	• ASR1K • ISR4K
Internet Edge	• ASR1K • ISR4K
Data Center	• N9K - NX-OS • N7K - NX-OS • N9K - ACI
Security	• ISE 2.3 • ASA 55xx • Windows AD

Cisco SD-Access Fabric

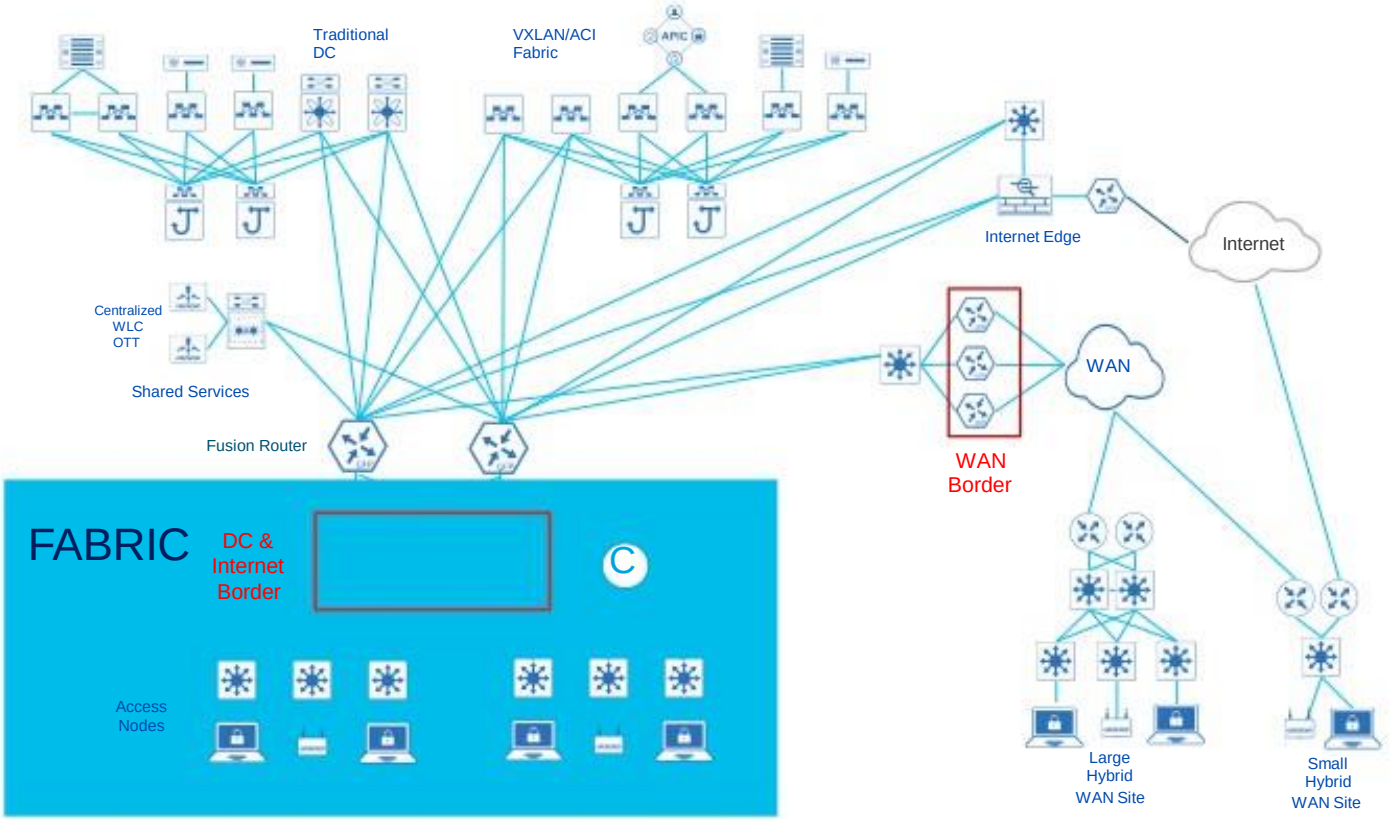
Large Enterprise Network Design - Cisco SD-Access Network



Role	Platform
Access Node	• Cat3K/9300 • Cat4K/9400
Distribution Node	• Cat3K/9300 • Cat4K/9500 • Cat6K/9500
Core Node	• Cat6K/9500 • NK7K • ASR1K-HX
Centralized WLC	• 8540 • 5520 • x800 APs
WAN HR/MC	• ASR1K • ISR4K
Internet Edge	• ASR1K • ISR4K
Data Center	• N9K - NX-OS • N7K - NX-OS • N9K - ACI
Security	• ISE 2.3 • ASA 55xx • Windows AD

Cisco SD-Access Fabric

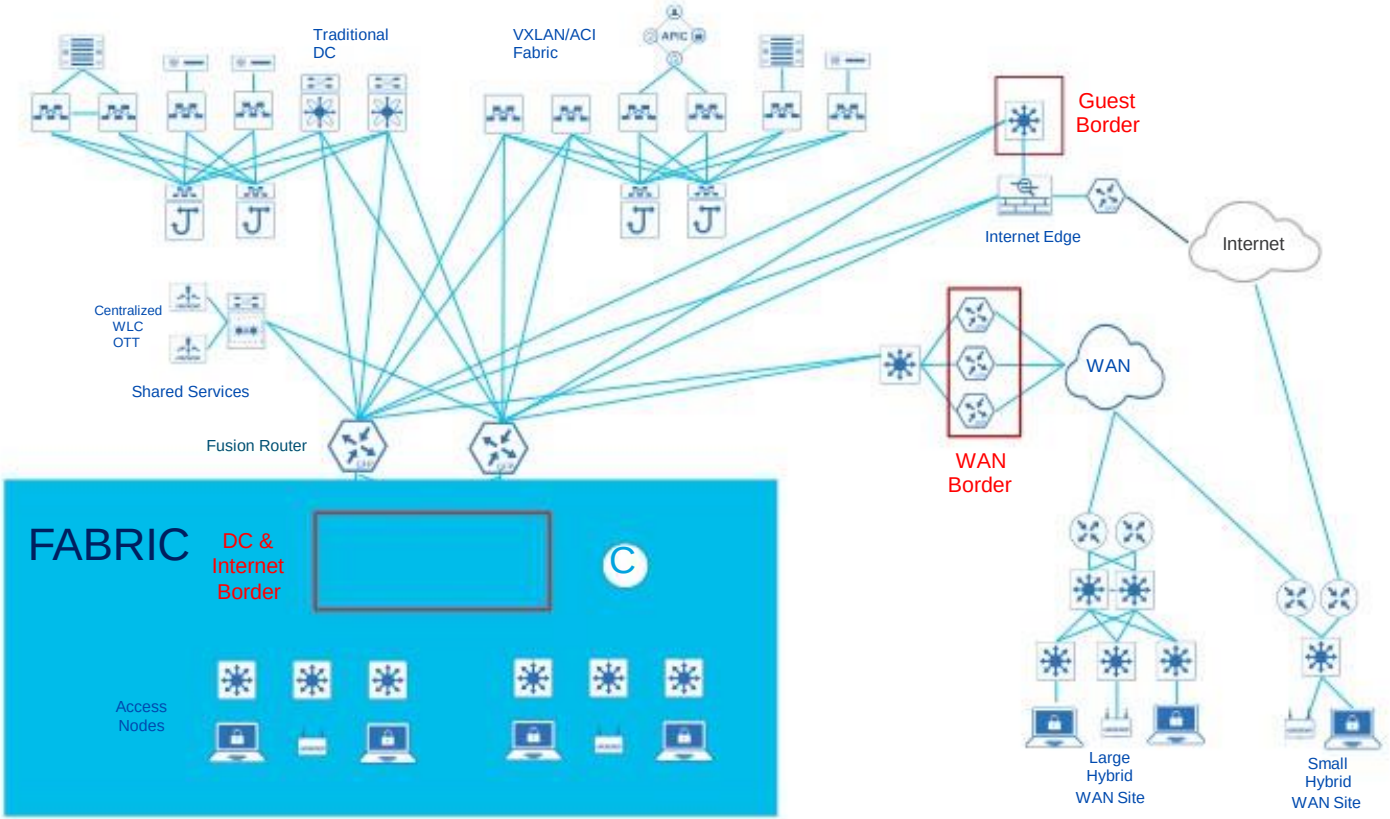
Large Enterprise Network Design - Cisco SD-Access Network



Role	Platform
Access Node	• Cat3K/9300 • Cat4K/9400
Distribution Node	• Cat3K/9300 • Cat4K/9500 • Cat6K/9500
Core Node	• Cat6K/9500 • NK7K • ASR1K-HX
Centralized WLC	• 8540 • 5520 • x800 APs
WAN HR/MC	• ASR1K • ISR4K
Internet Edge	• ASR1K • ISR4K
Data Center	• N9K - NX-OS • N7K - NX-OS • N9K - ACI
Security	• ISE 2.3 • ASA 55xx • Windows AD

Cisco SD-Access Fabric

Large Enterprise Network Design - Cisco SD-Access Network



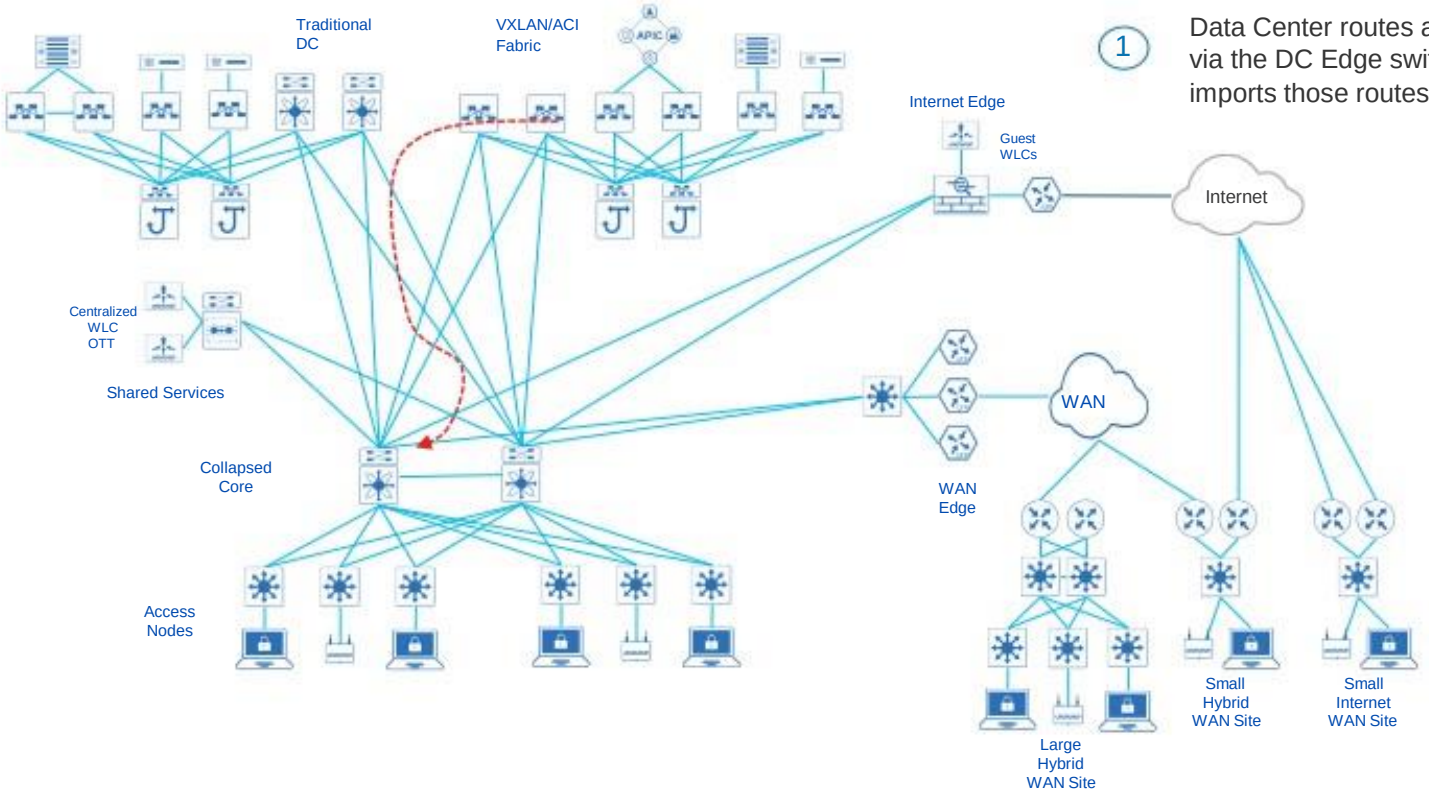
Role	Platform
Access Node	• Cat3K/9300 • Cat4K/9400
Distribution Node	• Cat3K/9300 • Cat4K/9500 • Cat6K/9500
Core Node	• Cat6K/9500 • NK7K • ASR1K-HX
Centralized WLC	• 8540 • 5520 • x800 APs
WAN HR/MC	• ASR1K • ISR4K
Internet Edge	• ASR1K • ISR4K
Data Center	• N9K - NX-OS • N7K - NX-OS • N9K - ACI
Security	• ISE 2.3 • ASA 55xx • Windows AD

Border Connectivity Models

Connectivity to external networks in the traditional design

Cisco SD-Access Fabric

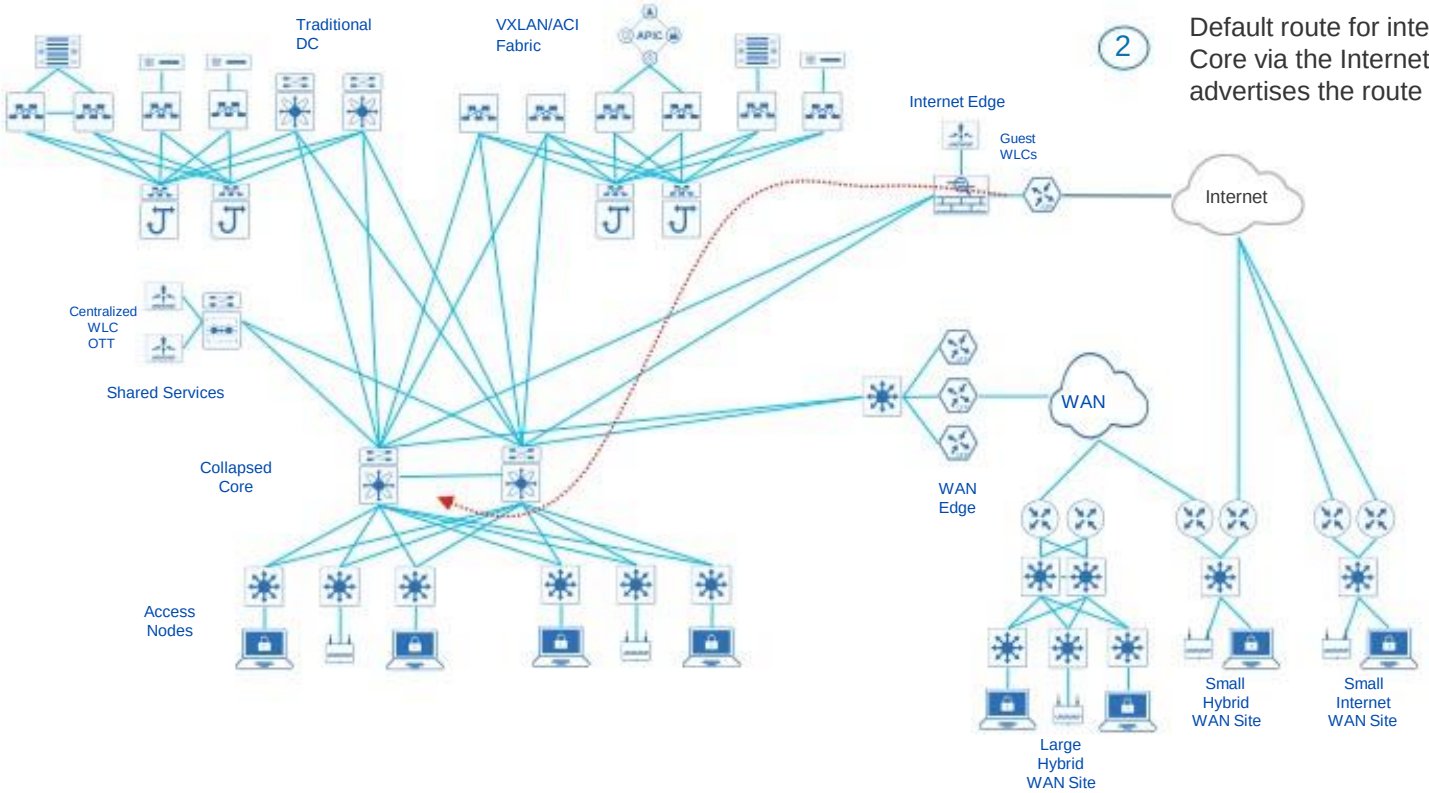
Large Enterprise Network Design - Traditional Network



Data Center routes are advertised to the Campus Core via the DC Edge switch via BGP/IGP. Campus core imports those routes into enterprise network.

Cisco SD-Access Fabric

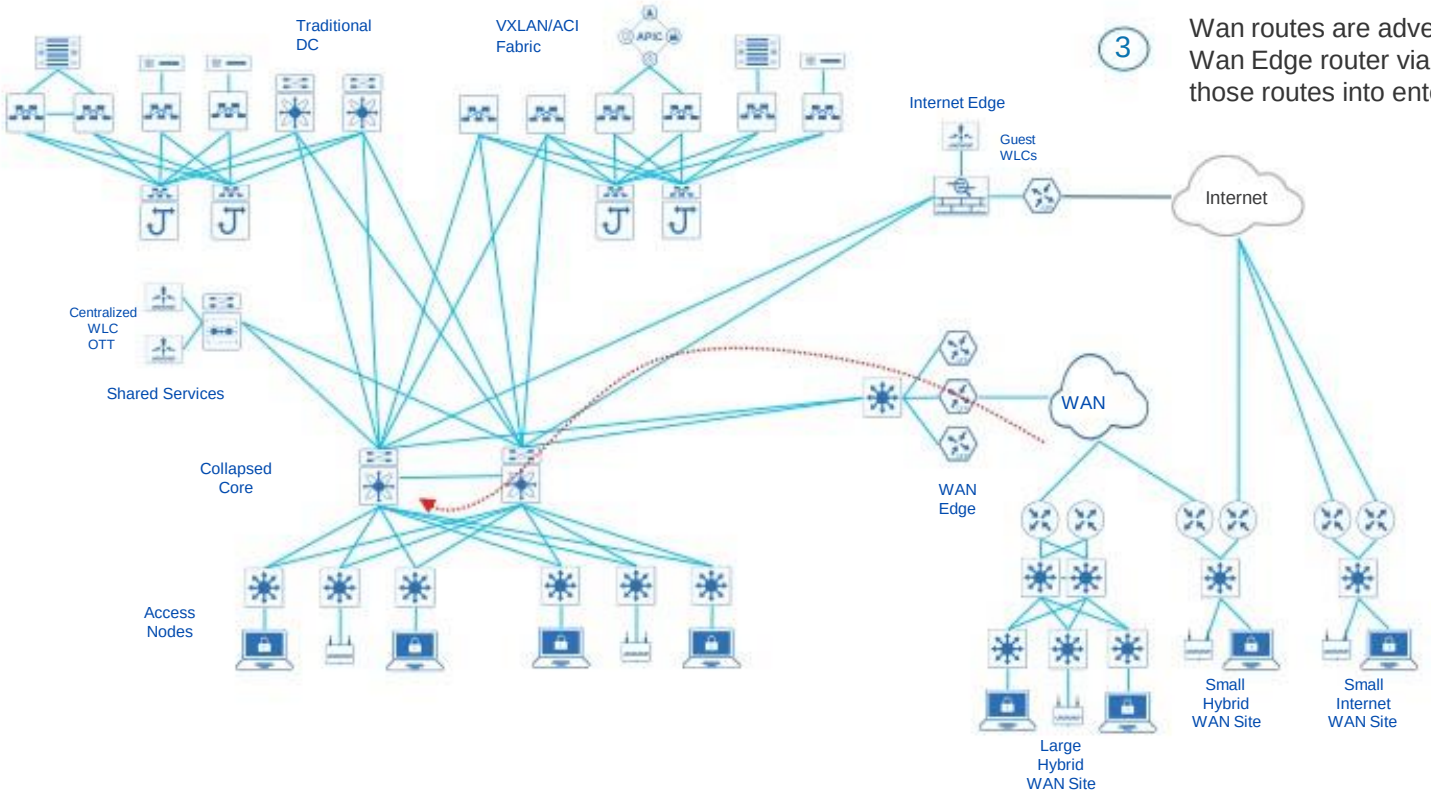
Large Enterprise Network Design - Traditional Network



Default route for internet is advertised to the Campus Core via the Internet Firewall. The campus core in return advertises the route to the enterprise network.

Cisco SD-Access Fabric

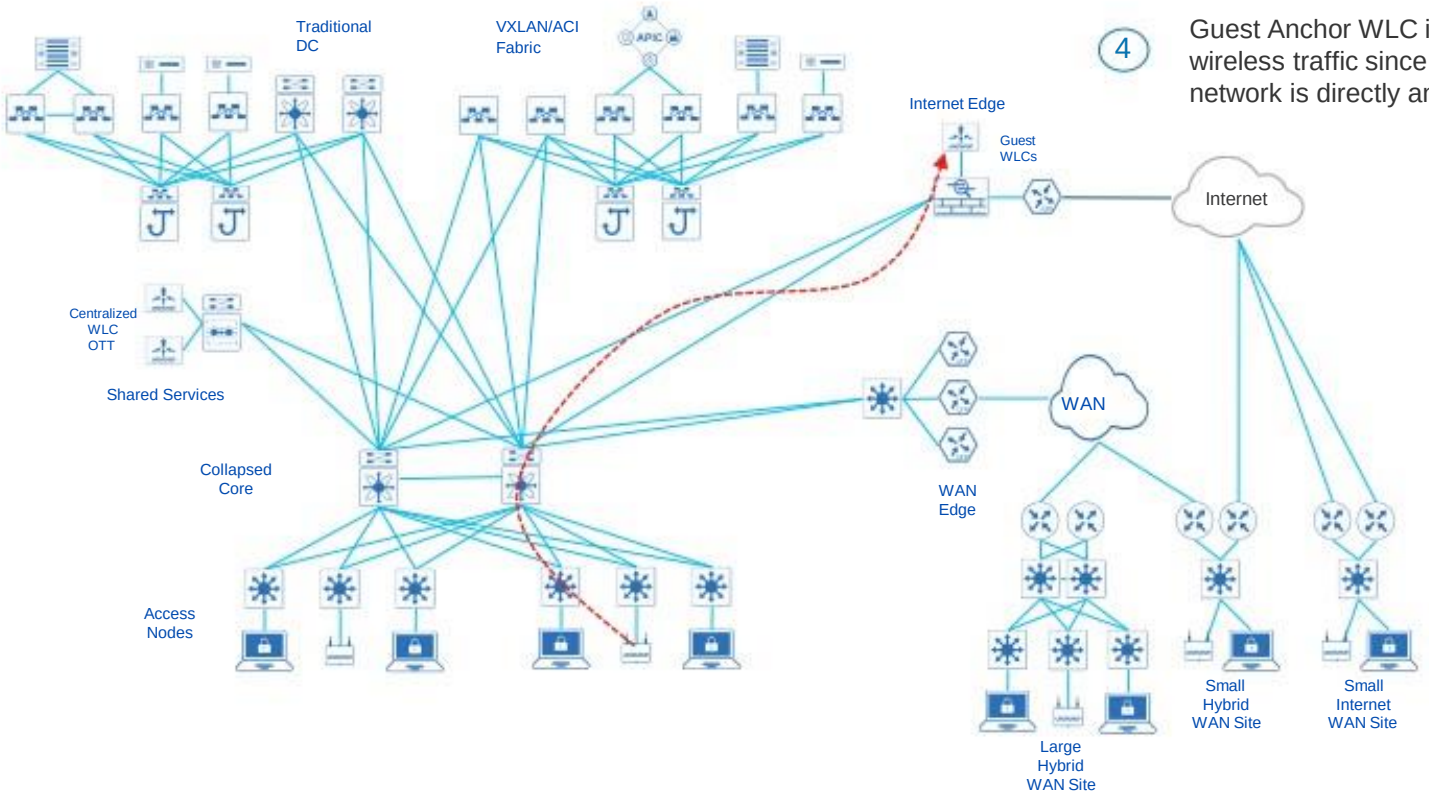
Large Enterprise Network Design - Traditional Network



Wan routes are advertised to the Campus Core via the Wan Edge router via BGP/IGP. Campus core imports those routes into enterprise network.

Cisco SD-Access Fabric

Large Enterprise Network Design - Traditional Network

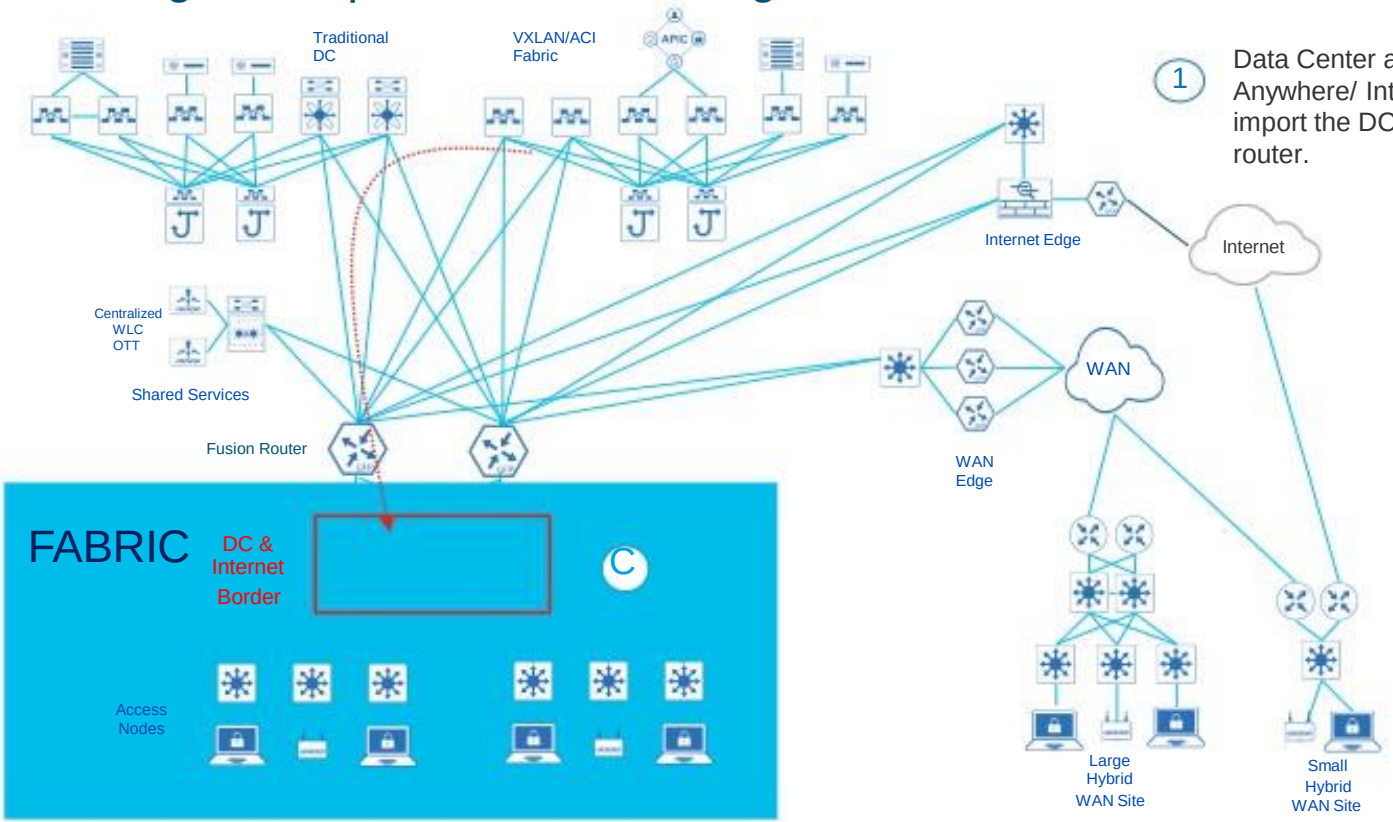


Guest Anchor WLC in the DMZ is responsible for guest wireless traffic since the traffic from the enterprise network is directly anchored to it.

Connectivity to external networks in the Cisco SD-Access design using the Border Node

Cisco SD-Access Fabric

Large Enterprise Network Design - Cisco SD-Access Network

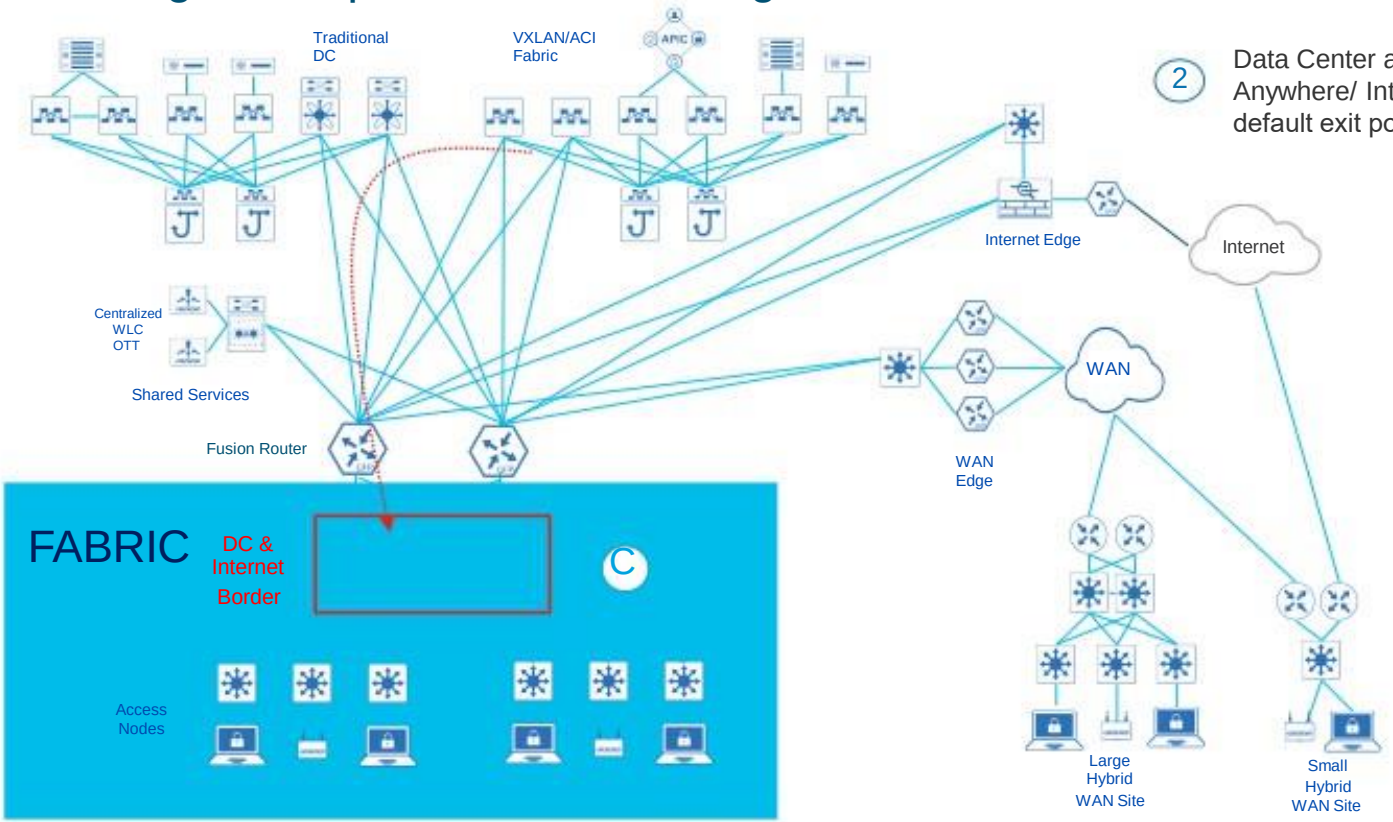


1

Data Center and Internet Border needs to be a Anywhere/ Internal + External Border as it has to import the DC routes into the fabric through the fusion router.

Cisco SD-Access Fabric

Large Enterprise Network Design - Cisco SD-Access Network

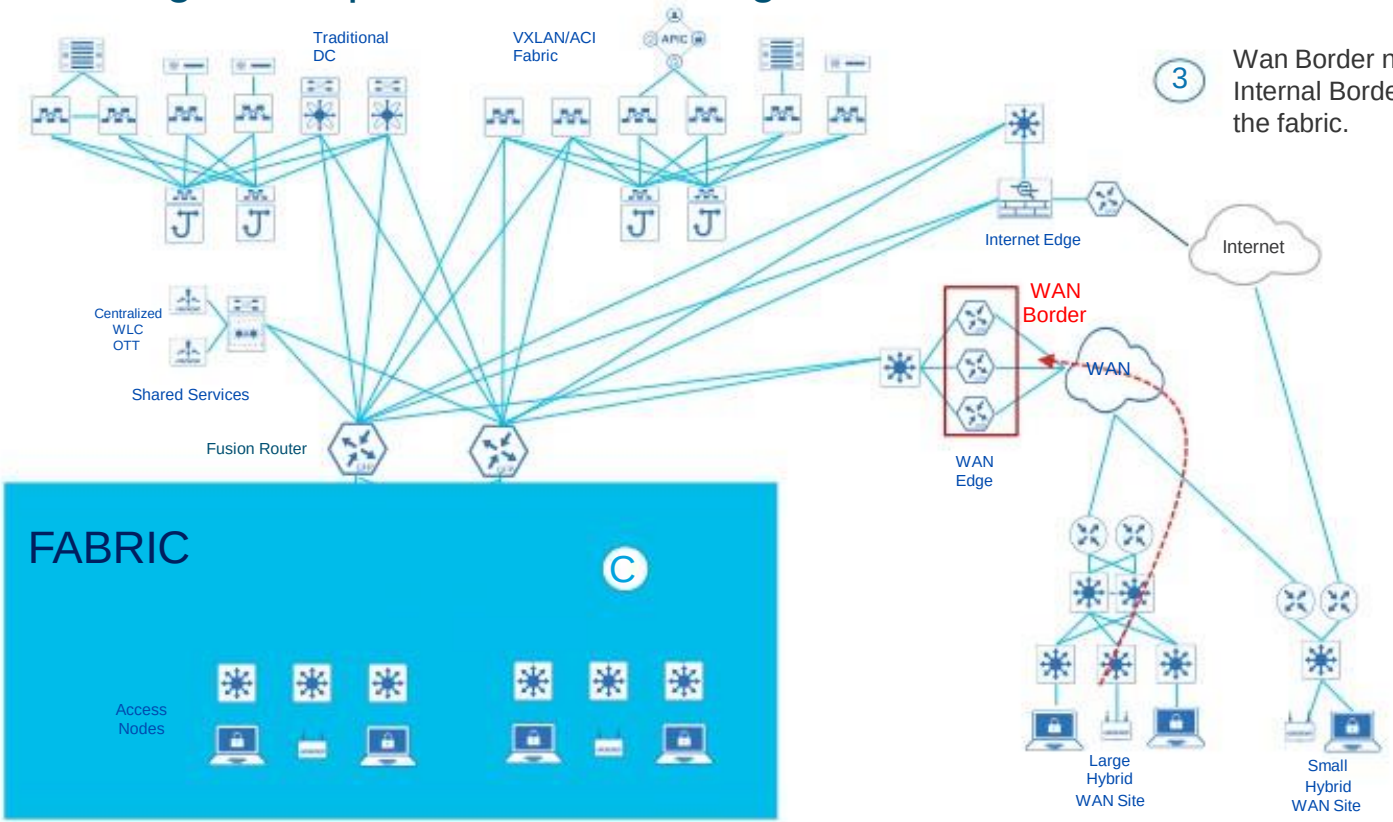


2

Data Center and Internet Border needs to be a Anywhere/ Internal + External Border as it also is the default exit point out of the fabric aka “ Default route”.

Cisco SD-Access Fabric

Large Enterprise Network Design - Cisco SD-Access Network

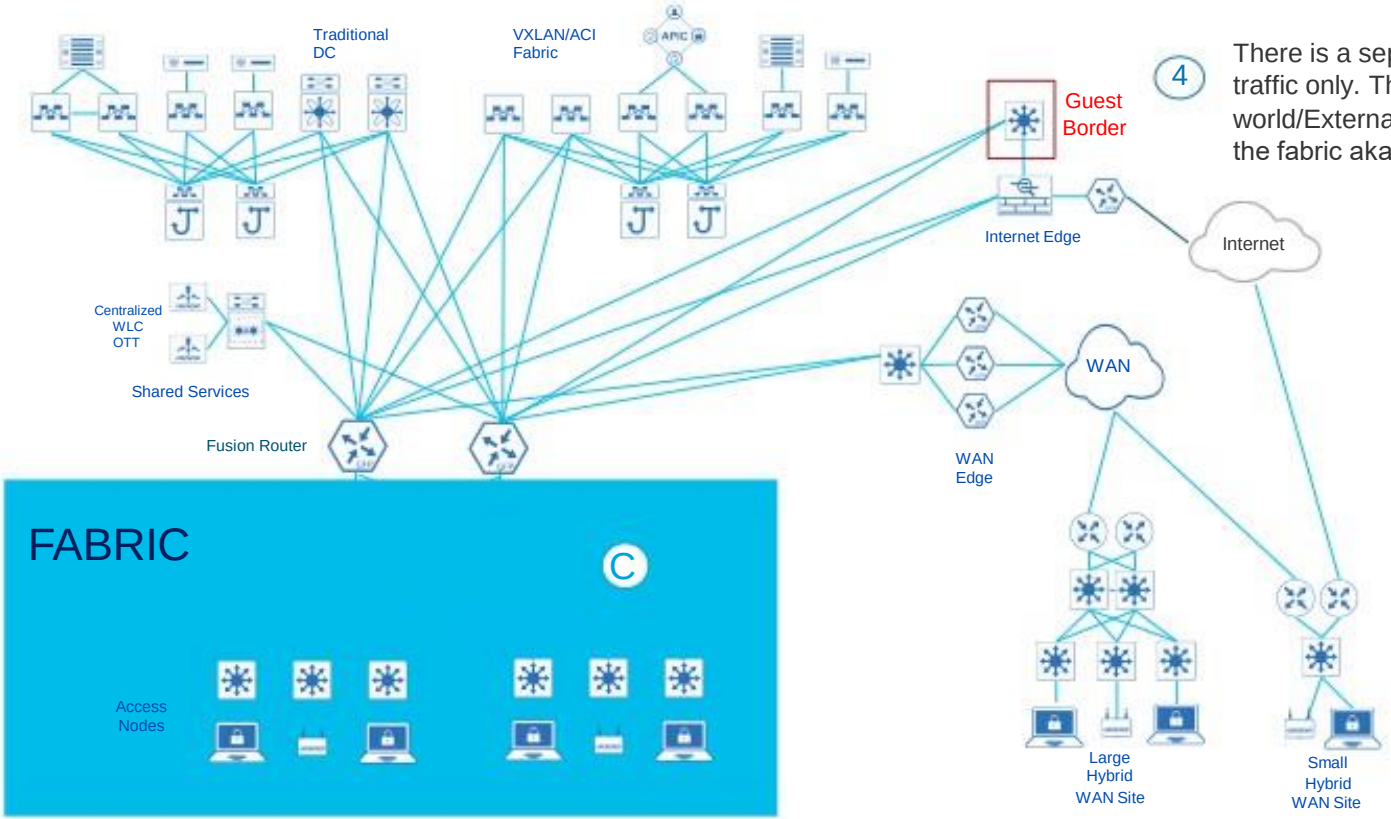


3

Wan Border needs to be a Rest of the Company/ Internal Border as it has to import the WAN routes into the fabric.

Cisco SD-Access Fabric

Large Enterprise Network Design - Cisco SD-Access Network

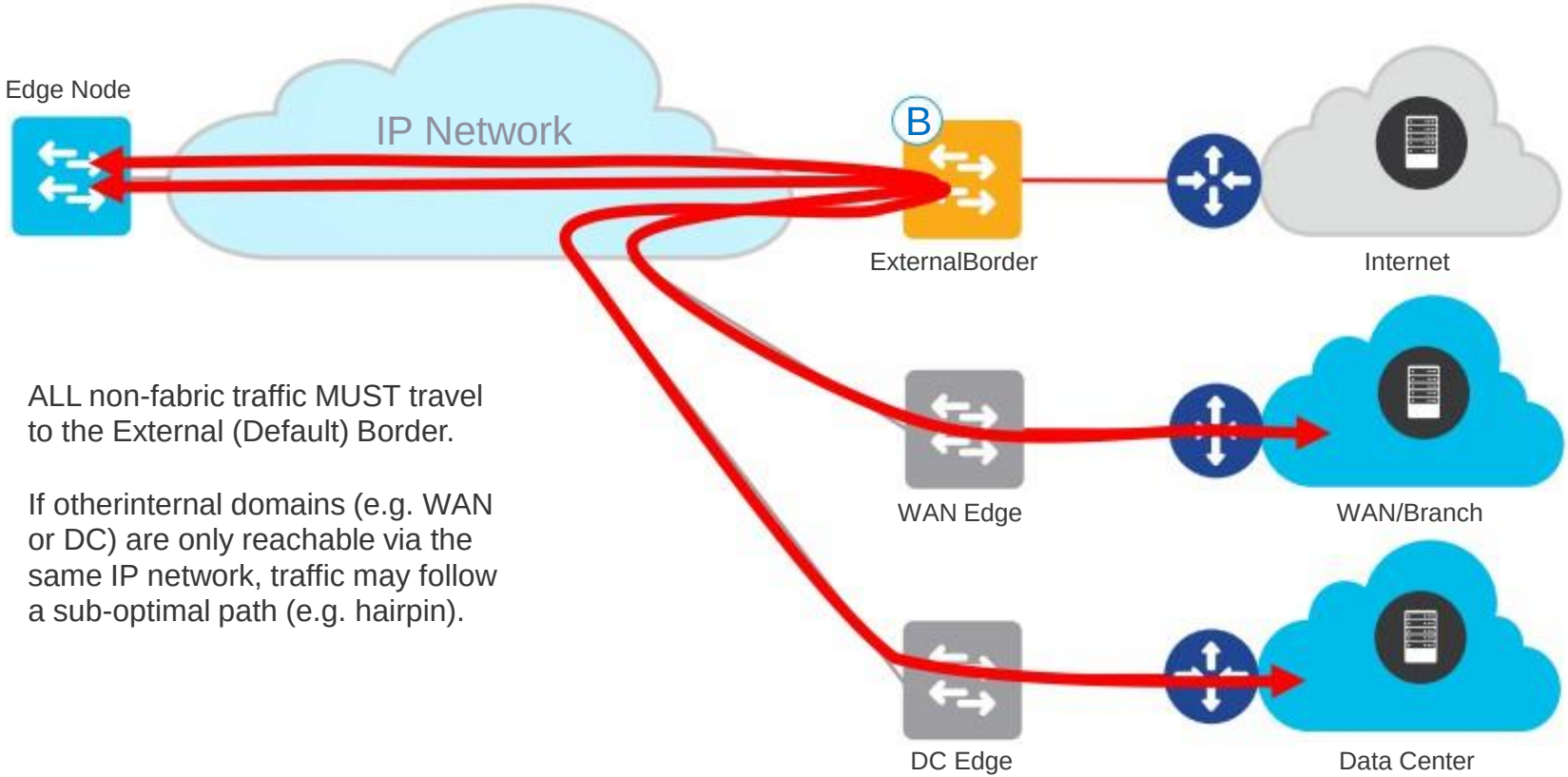


There is a separate Guest Border in fabric for Guest VN traffic only. This Border needs to be a Outside world/External border as it is the default exit point out of the fabric aka “ Default route” for the Guest VN.

Why Internal (Rest of Company) vs External (Outside World) Border

Cisco SD-Access - Border Deployment

Why? Internal Traffic with External Borders

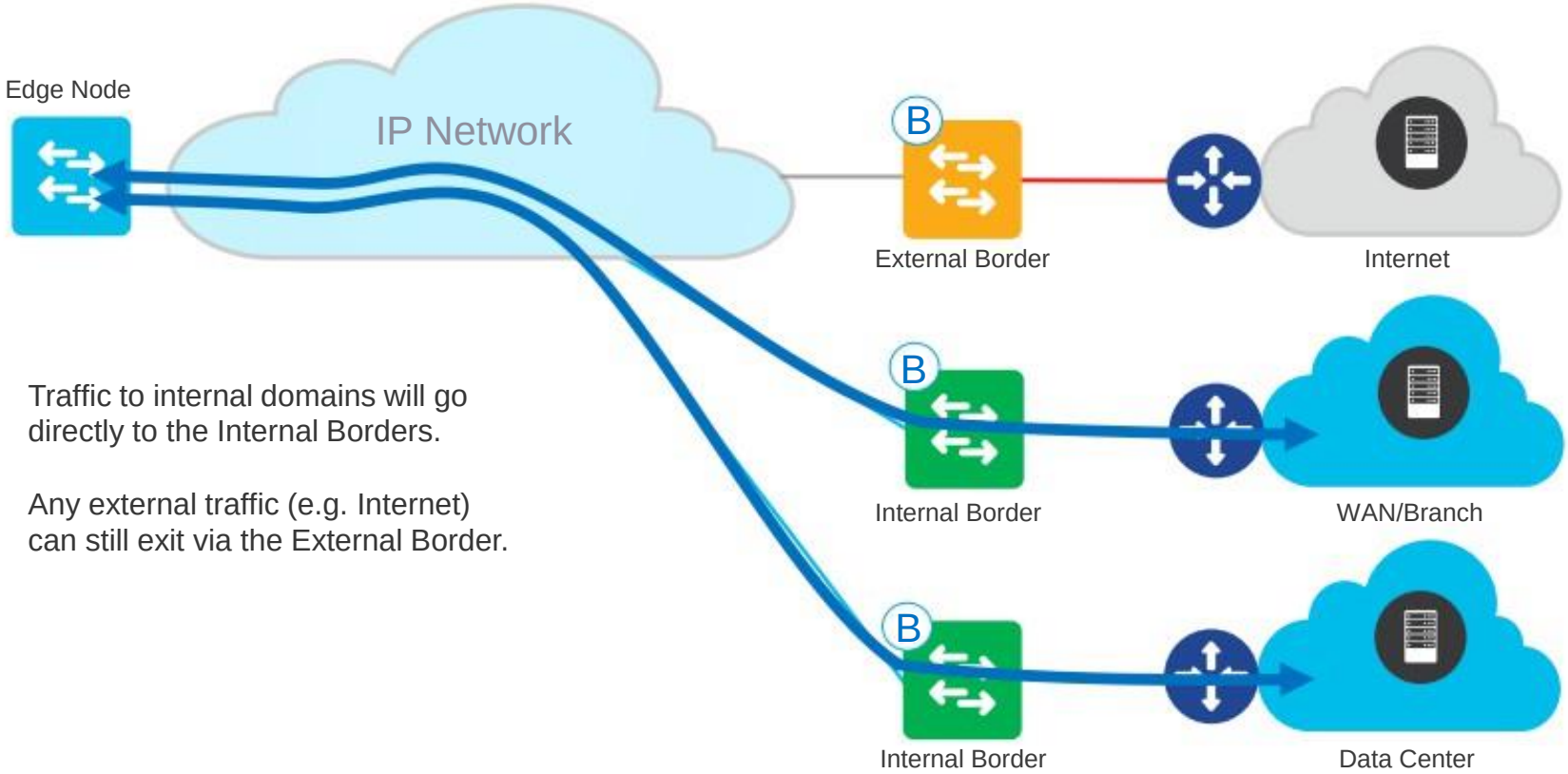


ALL non-fabric traffic MUST travel to the External (Default) Border.

If otherinternal domains (e.g. WAN or DC) are only reachable via the same IP network, traffic may follow a sub-optimal path (e.g. hairpin).

Cisco SD-Access - Border Deployment

Why? Internal Traffic with Internal Borders



Traffic to internal domains will go directly to the Internal Borders.

Any external traffic (e.g. Internet) can still exit via the External Border.

Cisco SD-Access Platforms

Fabric Control Plane

For more details: cs.co/sda-compatibility-matrix

Catalyst 9300

- Catalyst 9300
- 1/mG RJ45
- 10/25/40/mG NM

Catalyst 9400

- Catalyst 9400
- Sup1/Sup1XL
- 9400 Cards

Catalyst 9500

- Catalyst 9500
- 40/100G QSFP
- 1/10/25G SFP

Cisco SD-Access Platforms

Fabric Control Plane

For more details: cs.co/sda-compatibility-matrix

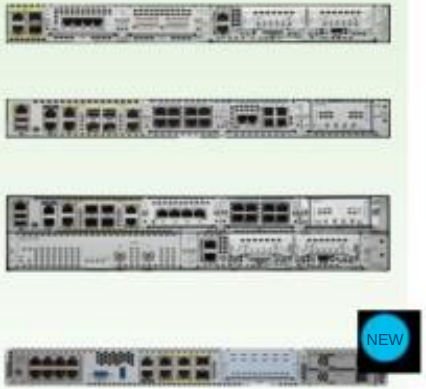
Catalyst 3K

- Catalyst 3650/3850
- 1/mG RJ45
- 1/10G SFP
- 1/10/40G NM Cards

Catalyst 6K

- Catalyst 6500/6800
- Sup2T/Sup6T
- C6800 Cards
- C6880/6840-X

ISR 4K & ENCS



- ISR 4430/4450
- ISR 4330/4450
- ENCS 5400
- ISRv / CSRv

ASR1K

- ASR 1000-X
- ASR 1000-HX
- 1/10G RJ45
- 1/10G SFP

Cisco SD-Access Platforms

Fabric Border Node

For more details: cs.co/sda-compatibility-matrix

Catalyst 9300

- Catalyst 9300
- 1/mG RJ45
- 10/25/40/mG NM

Catalyst 9400

- Catalyst 9400
- Sup1/Sup1XL
- 9400 Cards

Catalyst 9500

- Catalyst 9500
- 1/10/25G SFP
- 40/100G QSFP

Cisco SD-Access Platforms

Fabric Border Node

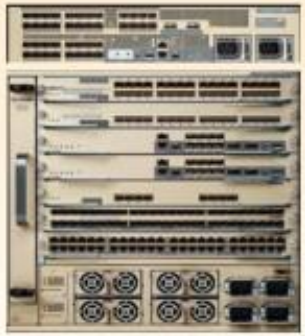
For more details: cs.co/sda-compatibility-matrix

* EXTERNAL ONLY

Catalyst 3K

- Catalyst 3650/3850
- 1/mG RJ45
- 1/10G SFP
- 1/10/40G NM Cards

Catalyst 6K

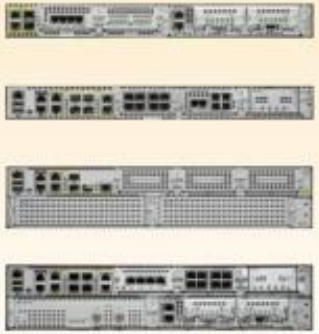


- Catalyst 6500/6800
- Sup2T/Sup6T
- C6800 Cards
- C6880/6840-X

Nexus 7 *

- Nexus 7700
- Sup2E
- M3 Cards
- LAN1K9 + MPLS

ISR 4K



- ISR 4300/4400
- AppX (AX)
- 1/10G RJ45
- 1/10G SFP

ASR 1K

- ASR 1000-X/HX
- AppX (AX)
- 1/10G ELC/EPA
- 40G ELC/EPA

Cisco SD-Access - Border Deployment

Fabric Border Scale

Fabric Constructs	Catalyst 3850-XS	Catalyst 9300	Catalyst 9400	Catalyst 9500	Catalyst 9500H	Catalyst 6800	Nexus N7700	ASR1K / ISR4K	CSR1Kv
Virtual Networks	64	256	256	256	256	500	500	4K	n.a.
SGT/DGT Table	4K	8K	8K	8K	8K	30K	16K	62K	n.a.
SGACLs (Security ACEs)	1500	5K	18K	18K	18K	12K 30K (XL)	16K	64K	n.a.
Control Plane Entries with Co-Located Border	3K	16K	SUP1 = 50K SUP1XL=80K	80K	80K	25K	Not Supported	200K / 100K (16GB) 100K / 50K (8GB)	200K
IPv4 Fabric Routes	8K	4K	SUP1 = 10K SUP1XL=20K	48K	48K	256K 1M (XL)	500K	4M (16GB) 1M (8GB)	n.a.
IPv4 Fabric Host Entries	16K	16K	SUP1 = 50K SUP1XL=80K	96K	96K		32K		

Cisco SD-Access - Border Deployment

Which Border to pick ?

Outside world(External)	Connect to the unknown part of company like internet or is the only exit point from fabric
Rest of Company (Internal)	Connect to known part of the company like DC, WAN etc.
Anywhere(Internal +External)	Connect to the internet and also known part of the company like DC, WAN etc.

Cisco SD-Access - Border Deployment

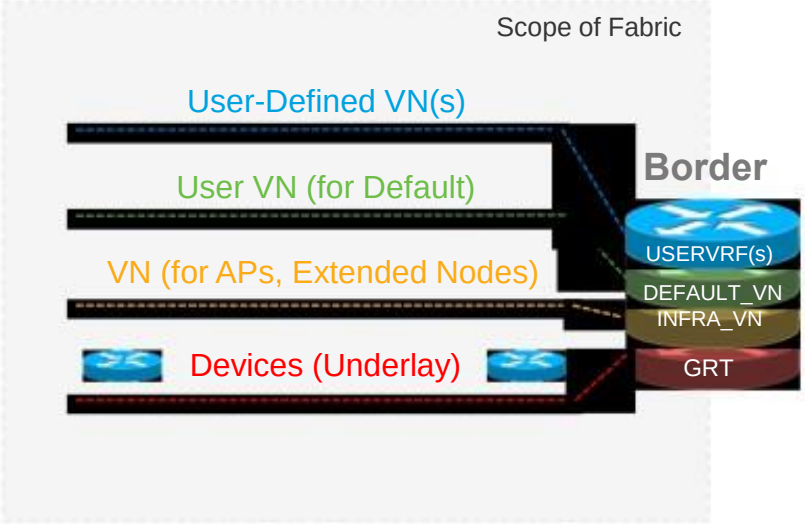
Fabric Border Support Matrix

SDA Border Node	Rest of Company (Internal)	Outside World (External)	Anywhere (Internal + External)
C9K	YES	YES	YES
ASR1K/ISR4K	YES	YES	YES
C6K	YES	YES	YES
N7K	NO	YES	NO

Cisco SD-Access - Border Deployment

How VNs work in SD-Access

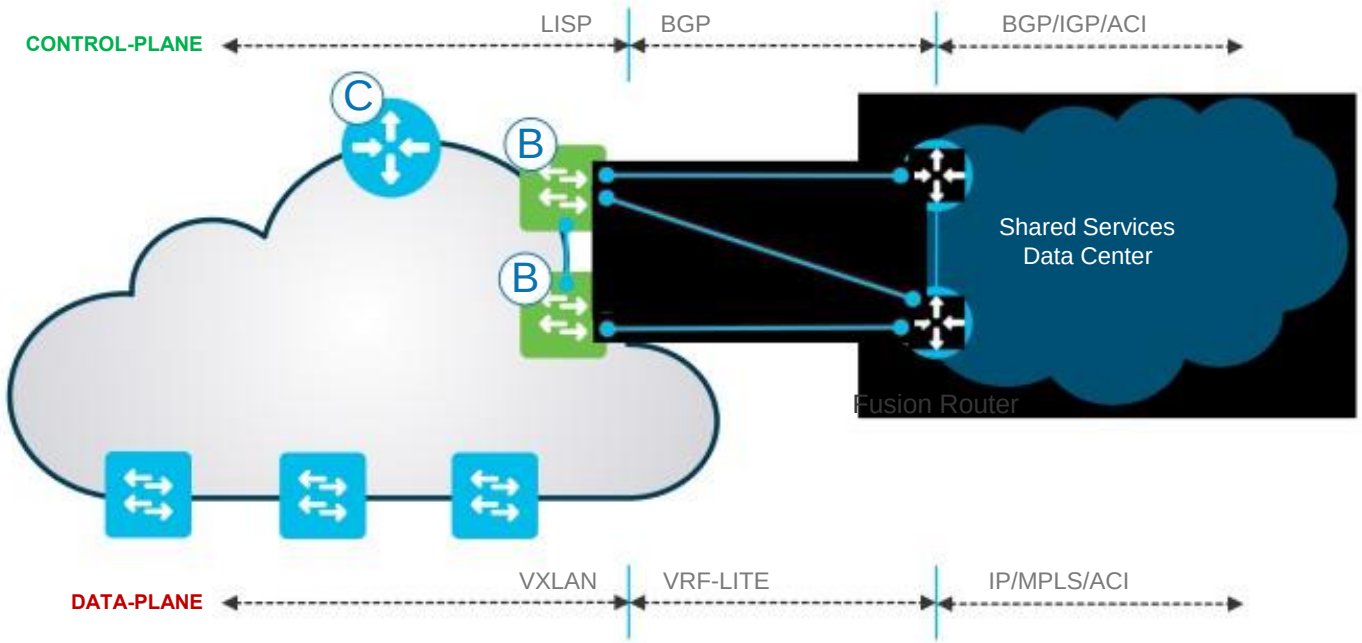
- **Fabric Devices (Underlay)** connectivity is in the Global Routing Table
- **INFRA_VN** is only for Access Points and Extended Nodes in GRT
- **DEFAULT_VN** is an actual "User VN" provided by default
- **User-Defined VNs** can be added or removed on-demand



Connectivity to Known Networks like DC & WAN via the Anywhere/Rest of Company Border

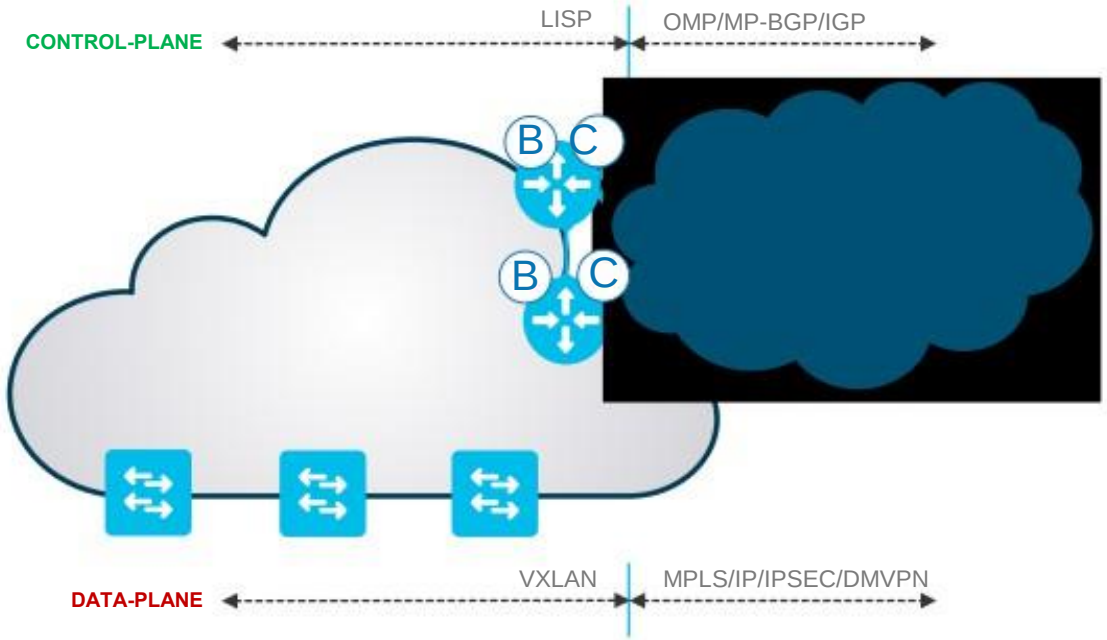
Border Deployment Options

Anywhere/Rest of Company for Shared Services and DC - VRF LITE



Border Deployment Options

Anywhere/Rest of Company Border WAN Connectivity



Cisco SD-Access Fabric

Border Nodes - One Box vs. Two Box

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 ExternalDomain

Two Box Design

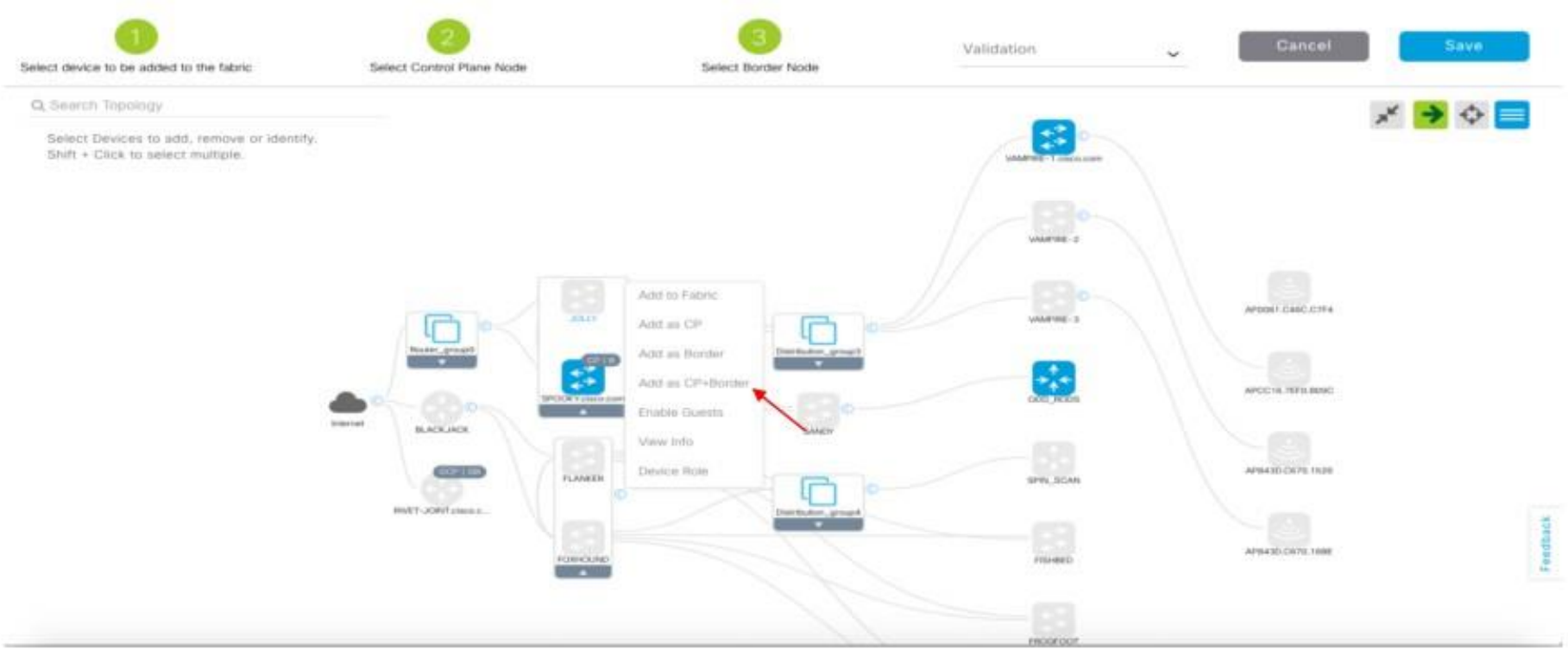
Internal and External domain routing are on **different devices**

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.)

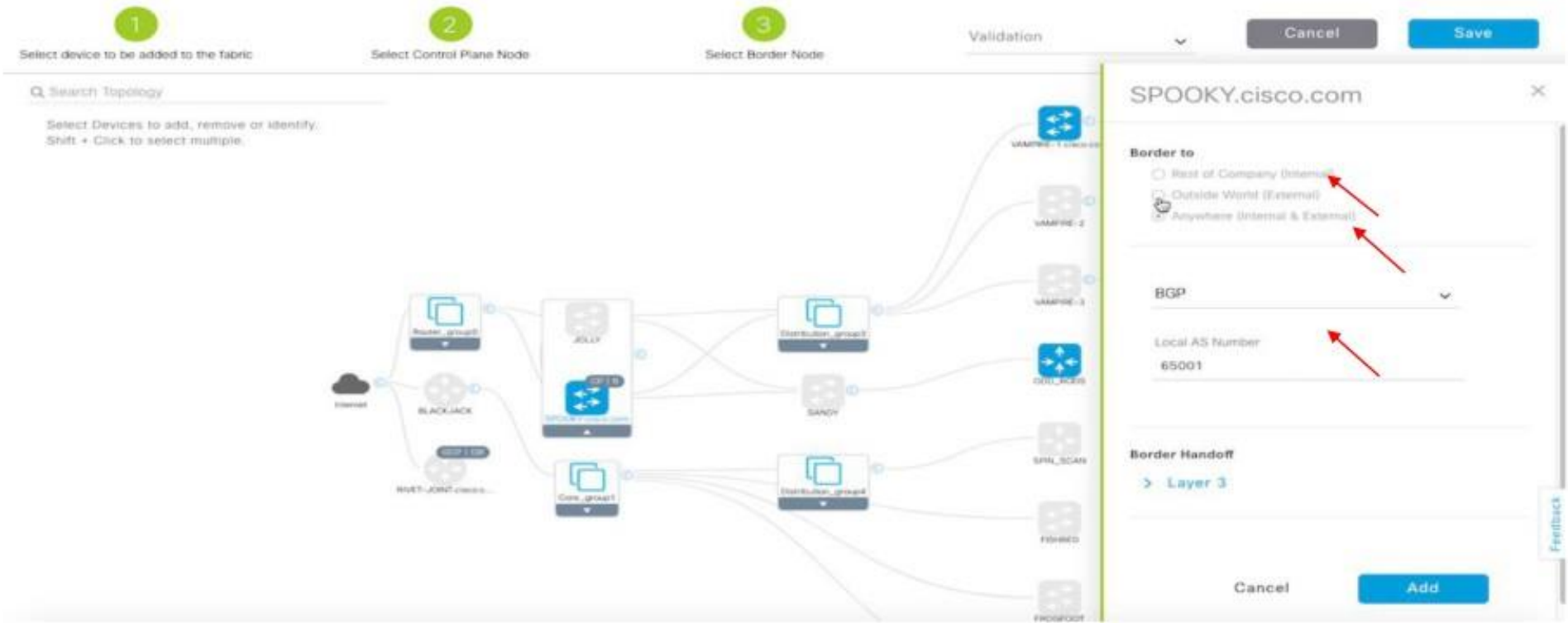
Border Deployment Options

Anywhere/Rest of Company Border



Border Deployment Options

Anywhere/Rest of Company Border



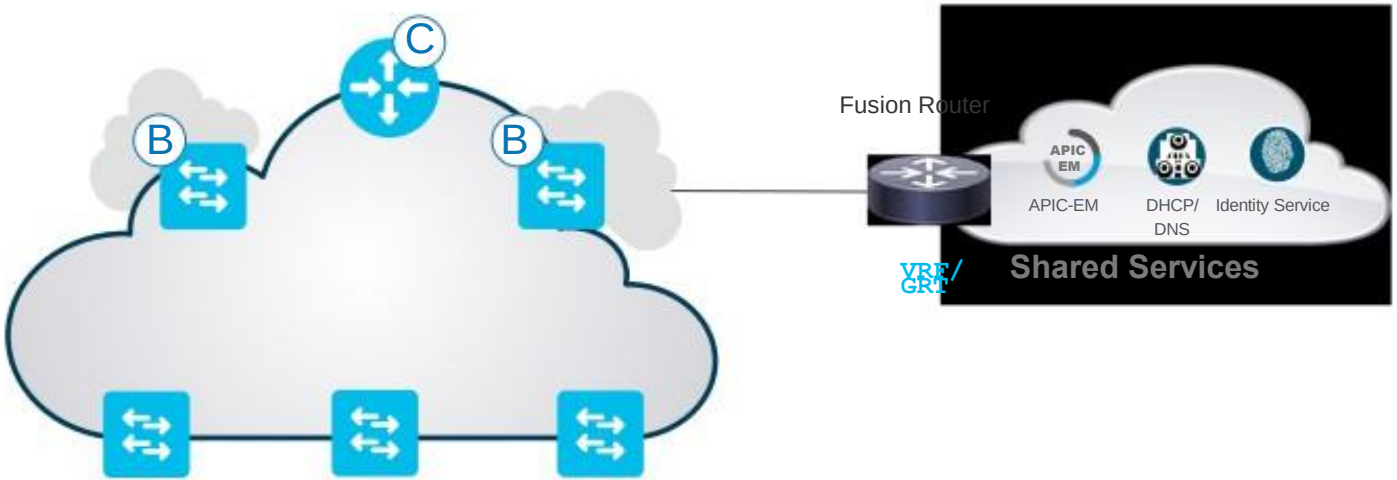
Border Deployment Options

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.

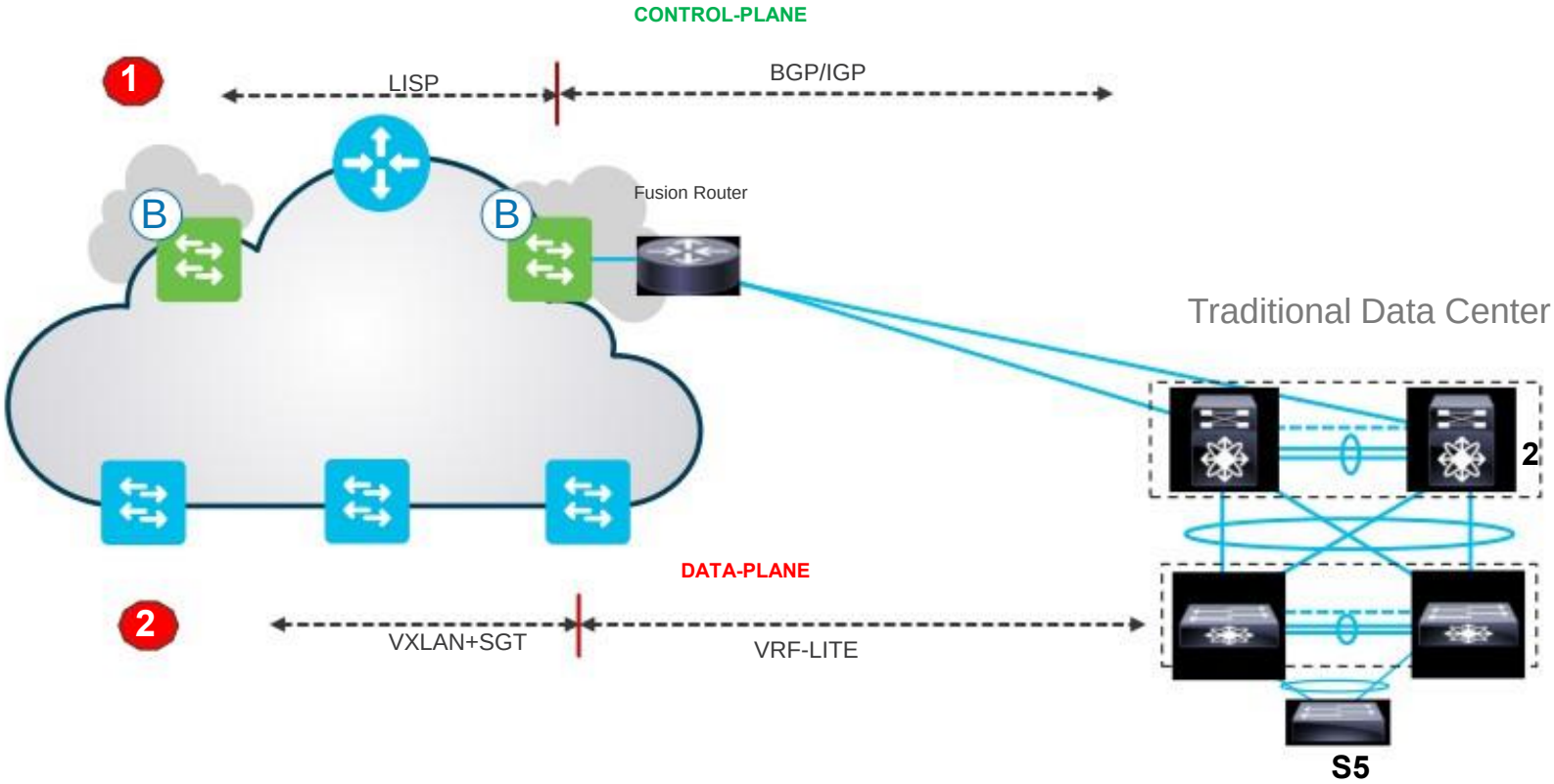
Border Deployment Options

Shared Services (DHCP, AAA, etc.) with Border



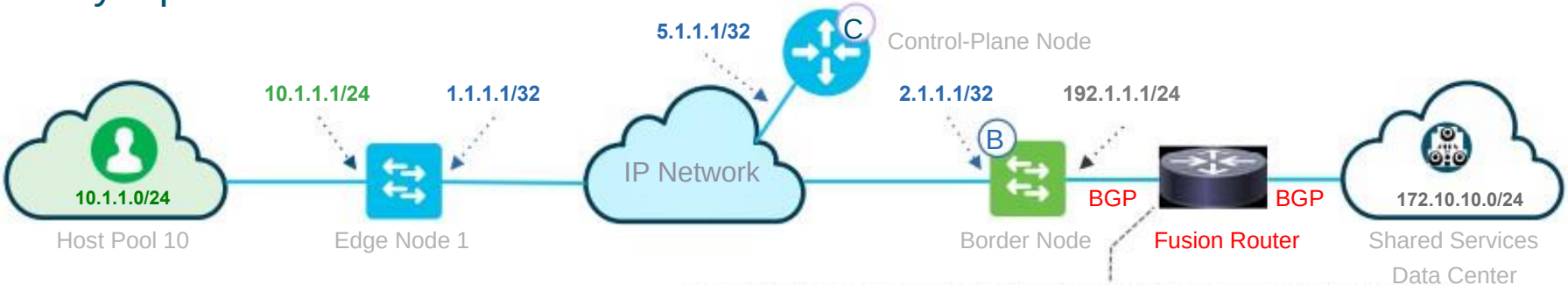
Border Deployment Options

Data Center Connectivity With Border - Traditional DC



Border Deployment Options

Policy Options for Shared Services and Traditional Data Center

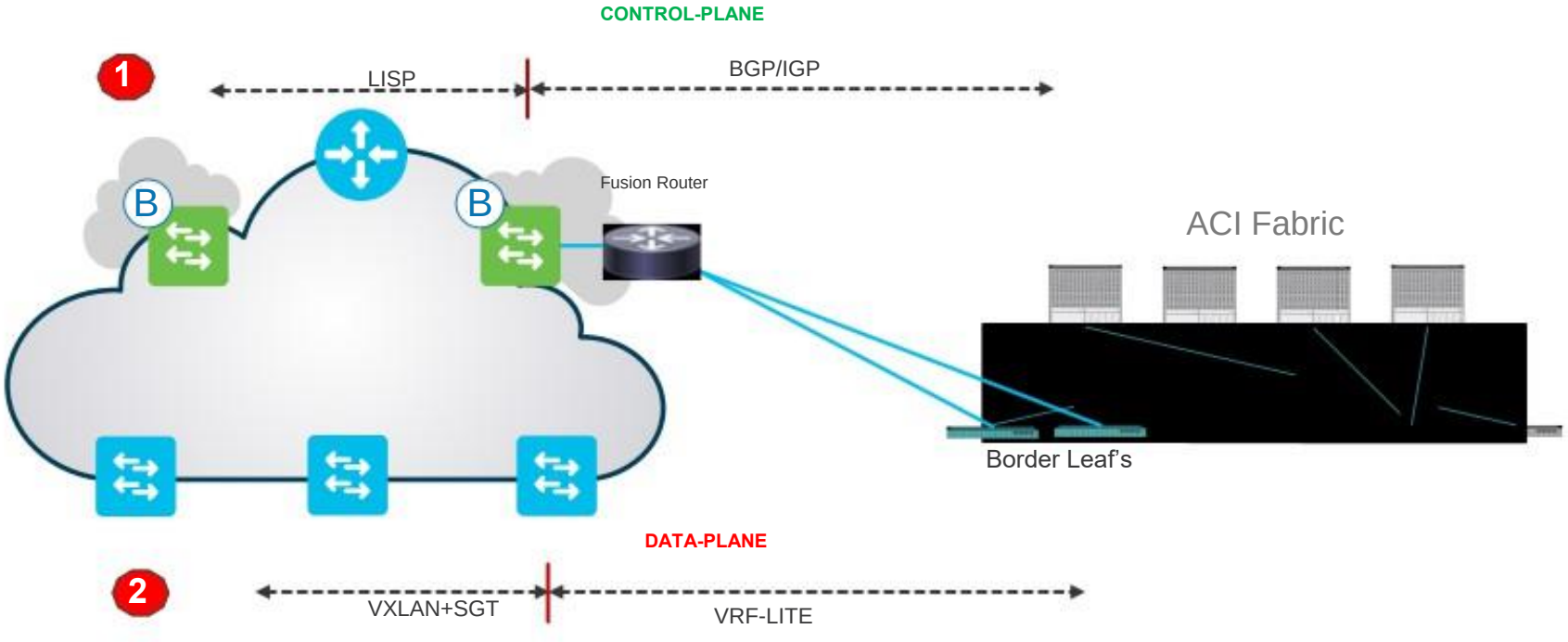


- Destination IP subnets are statically mapped to SGT's in ISE.
- SXP from ISE to fusion router to download the IP to SGT bindings for the destination IP subnets.
- SG ACLS's are enforced at the Fusion router

Source			Destination			Action
IP	Group/User	Security Group	IP	Security Group	Port	Action
ANY	ANY	Employees on Corporate Assets	ANY	ACI_Intranet_Servers_EPG	Any tcp	Allow
ANY	ANY	Senior Execs on registered BYOD devices	ANY	ACI_Finance_Servers_EPG	http, https	Allow
ANY	ANY	Contractors on unmanaged devices	ANY	ACI_Citrix_VDI_EPG	RDP, ICA	Allow
ANY	ANY	Divested Business - Employees	ANY	Divested Business Servers	ANY	Allow
ANY	ANY	ANY	ANY	ANY	ANY	DENY

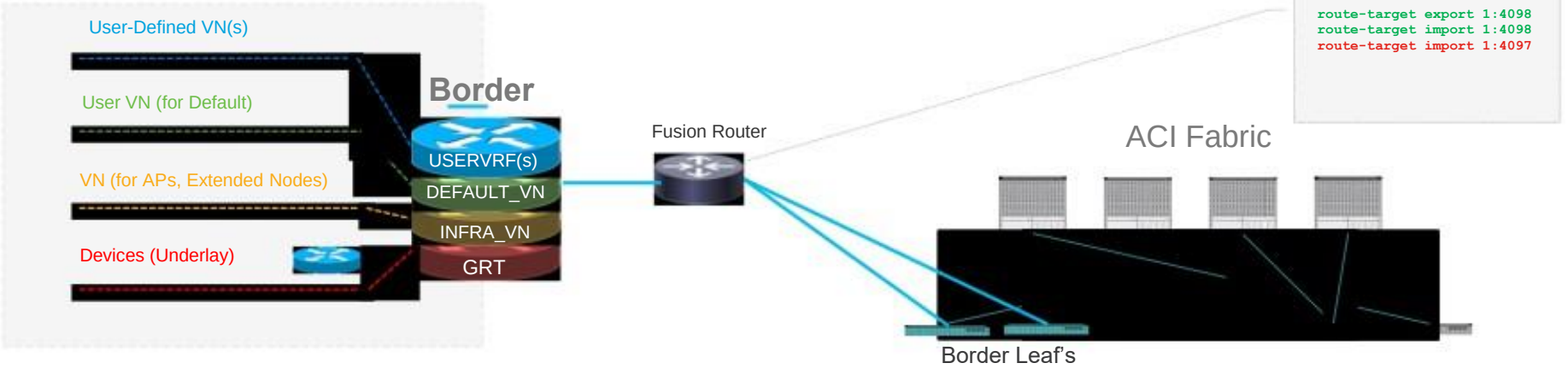
Border Deployment Options

Data Center Connectivity With Border - VXLAN/ACI Fabric



Border Deployment Options

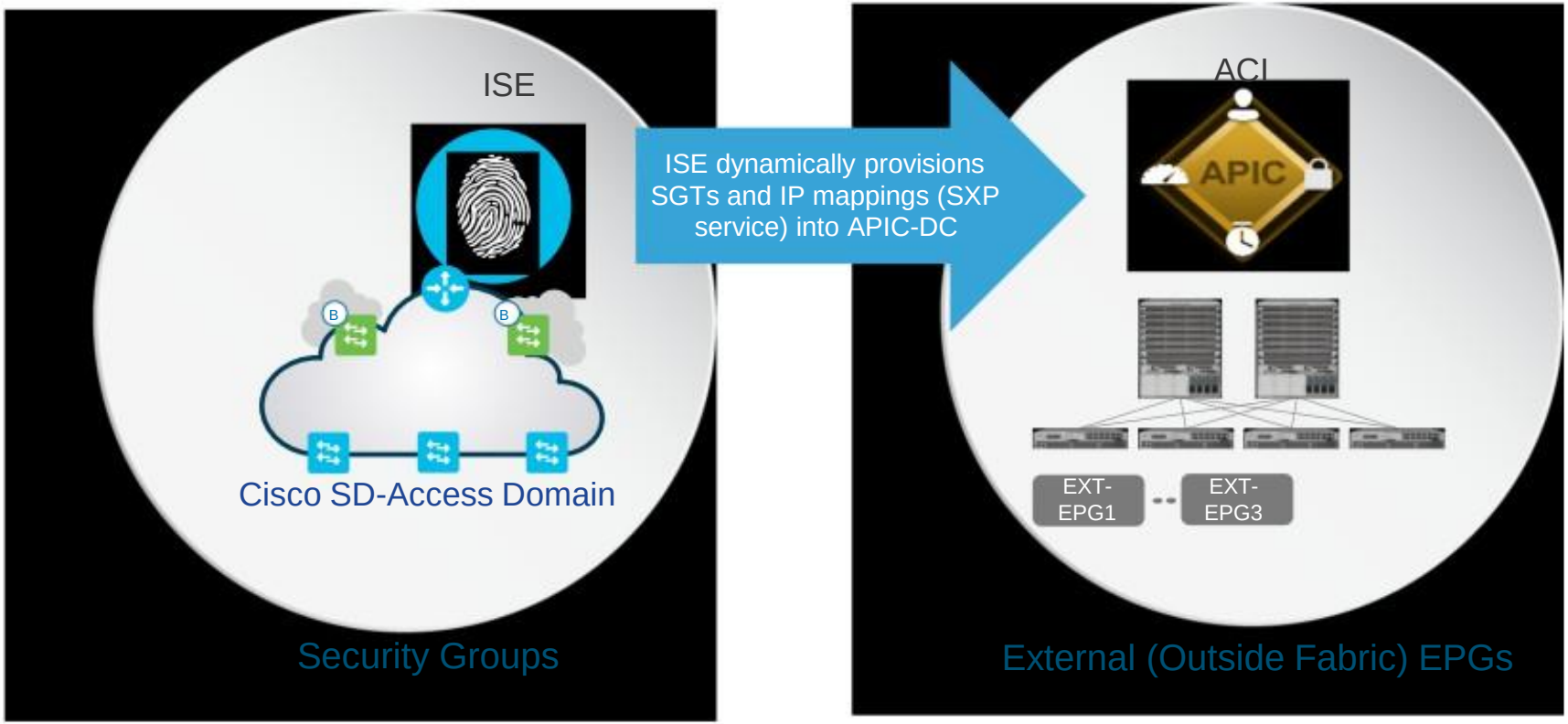
Data Center Connectivity With Border - ACI Fabric



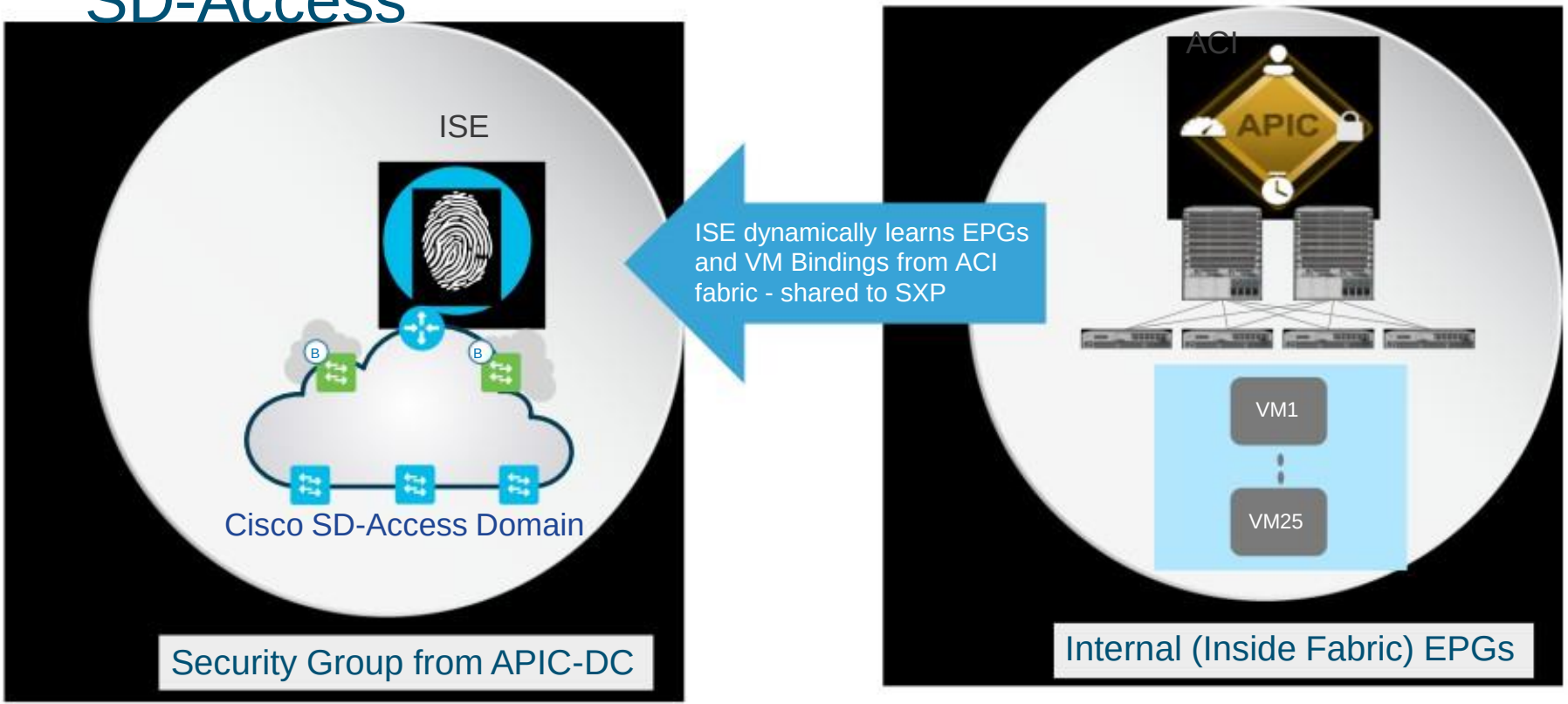

```
ip vrf CAMPUS
 rd 1:4099
 route-target export 1:4099
 route-target import 1:4099
 route-target import 1:4098
!
ip vrf ACI
 rd 1:4098
 route-target export 1:4098
 route-target import 1:4098
 route-target import 1:4097
```

- SD-Access Border merge the VRF's A , B , C and so on to a common VRF D using a fusion router.
- The Common VRF D will connect to ACI VRF on the other side.
- We need access-lists/distribute lists on the fusion router to ensure that VRF A , B and C do not talk to each other. This can also be achieved using VRF import and export maps.

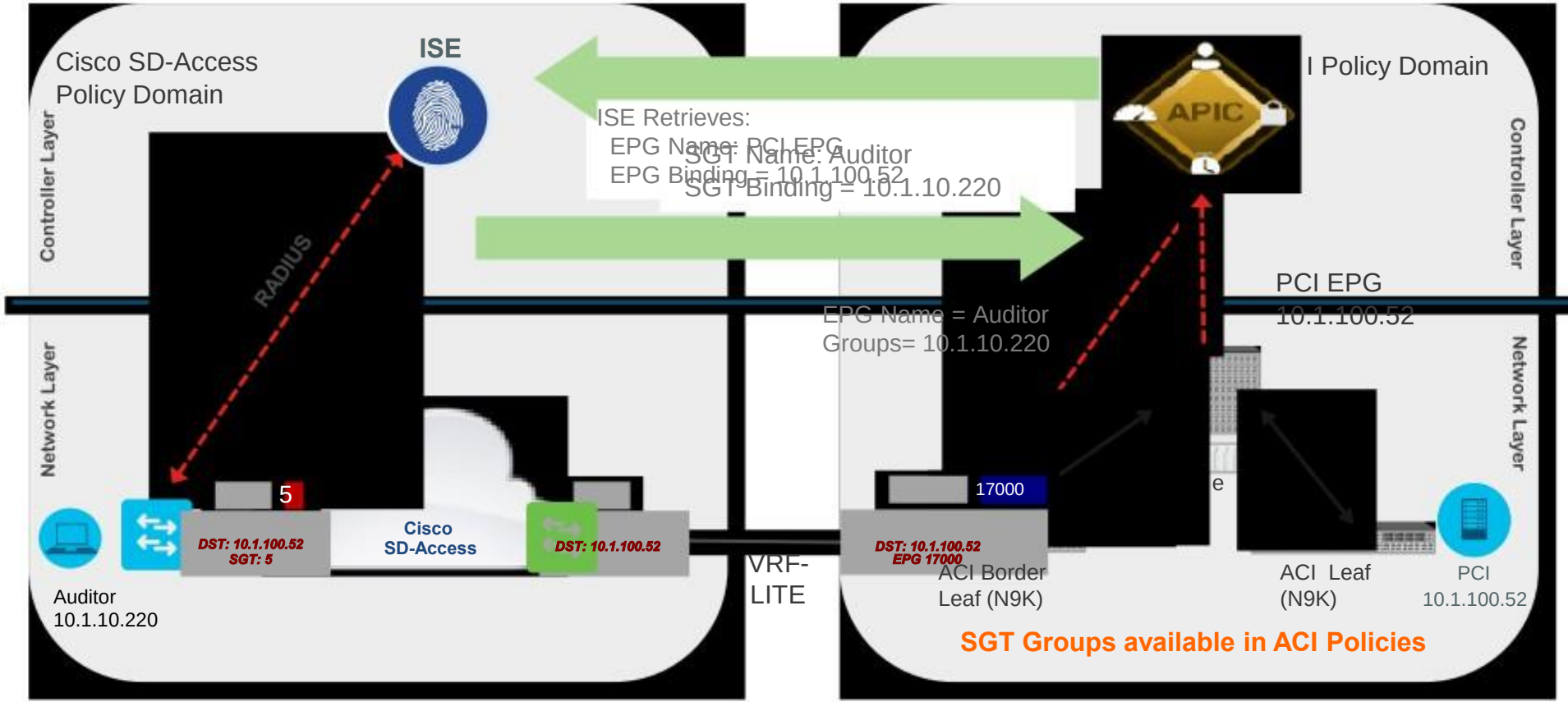
Cisco SD-Access SGTs Provisioned in ACI



ACI EPGs Automatically Propagated into Cisco SD-Access



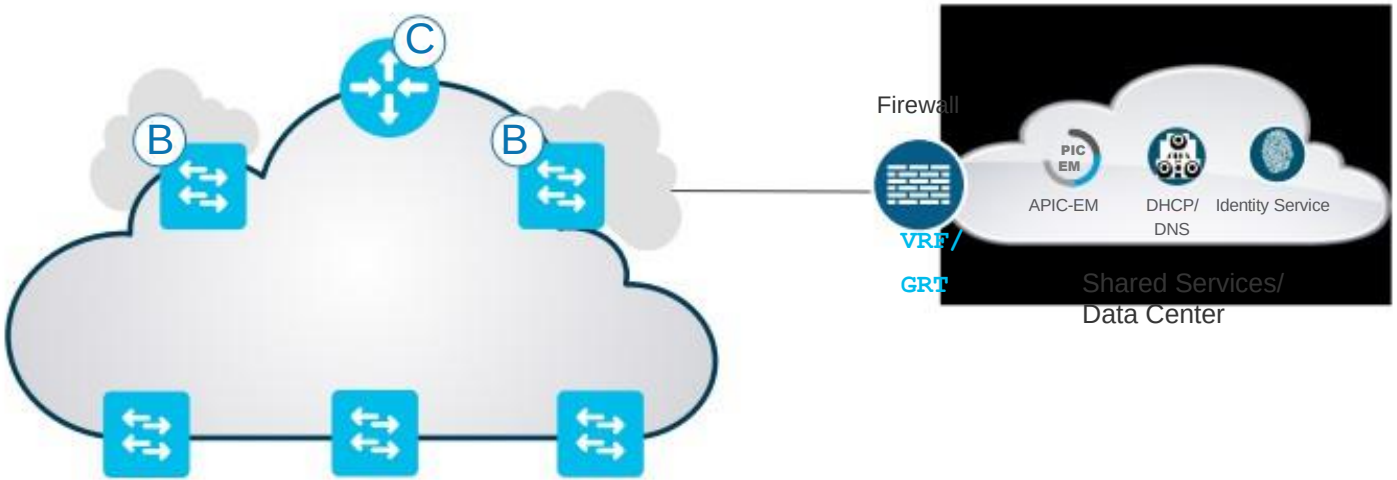
Cisco SD-Access SGT Info Used in ACI Policies



Alternate Design Option for fusion Router

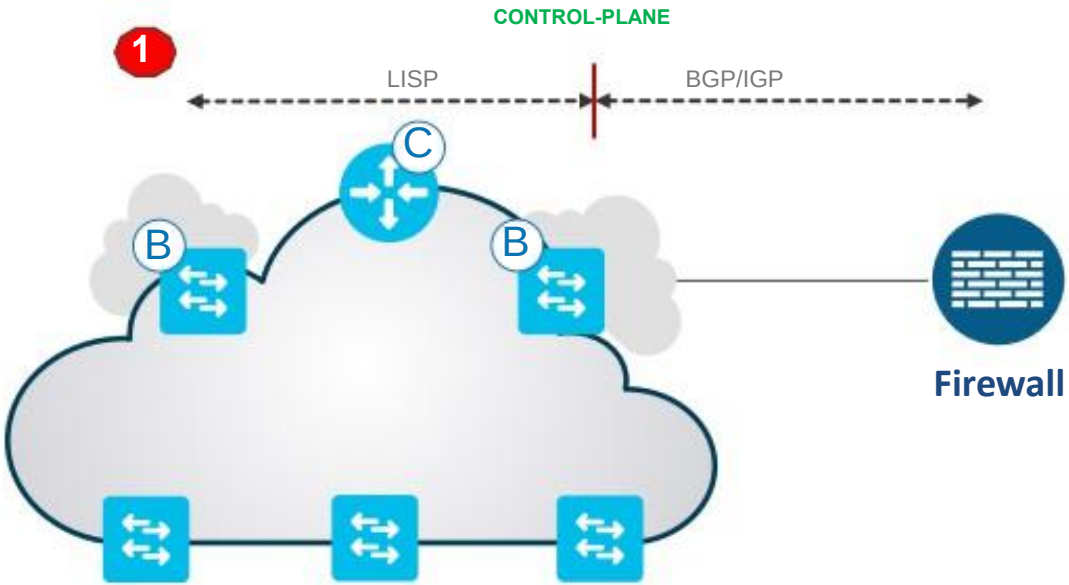
Border Deployment Options

Firewall as fusion router



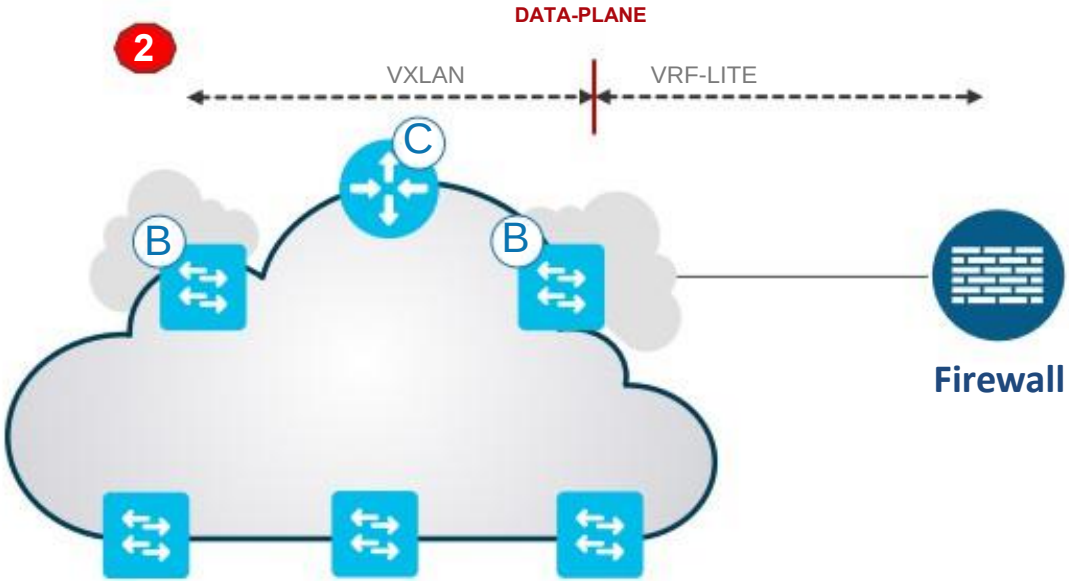
Border Deployment Options

Firewall as fusion router



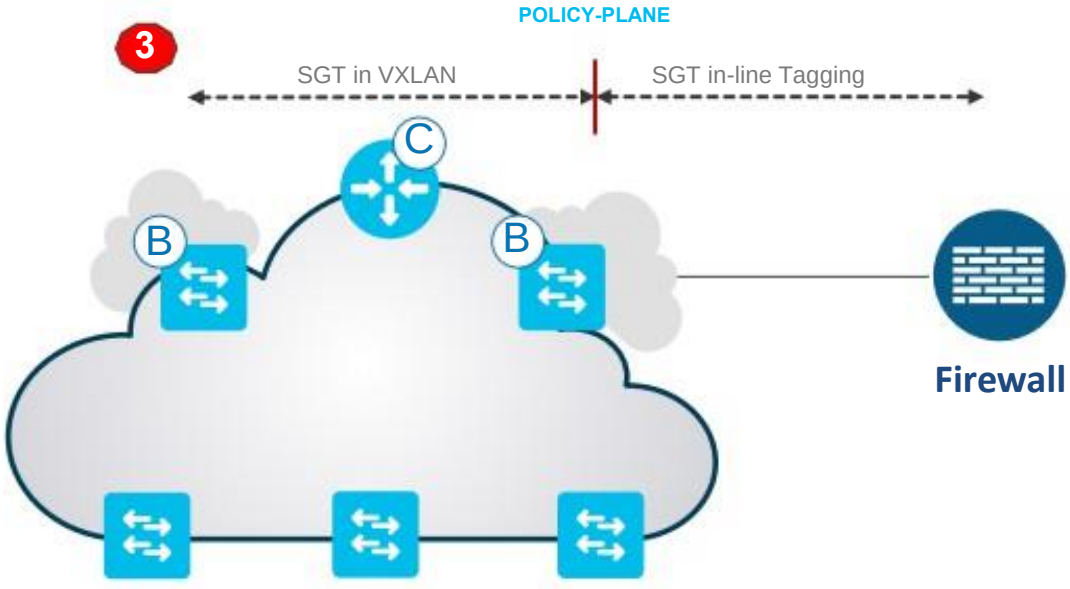
Border Deployment Options

Firewall as fusion router



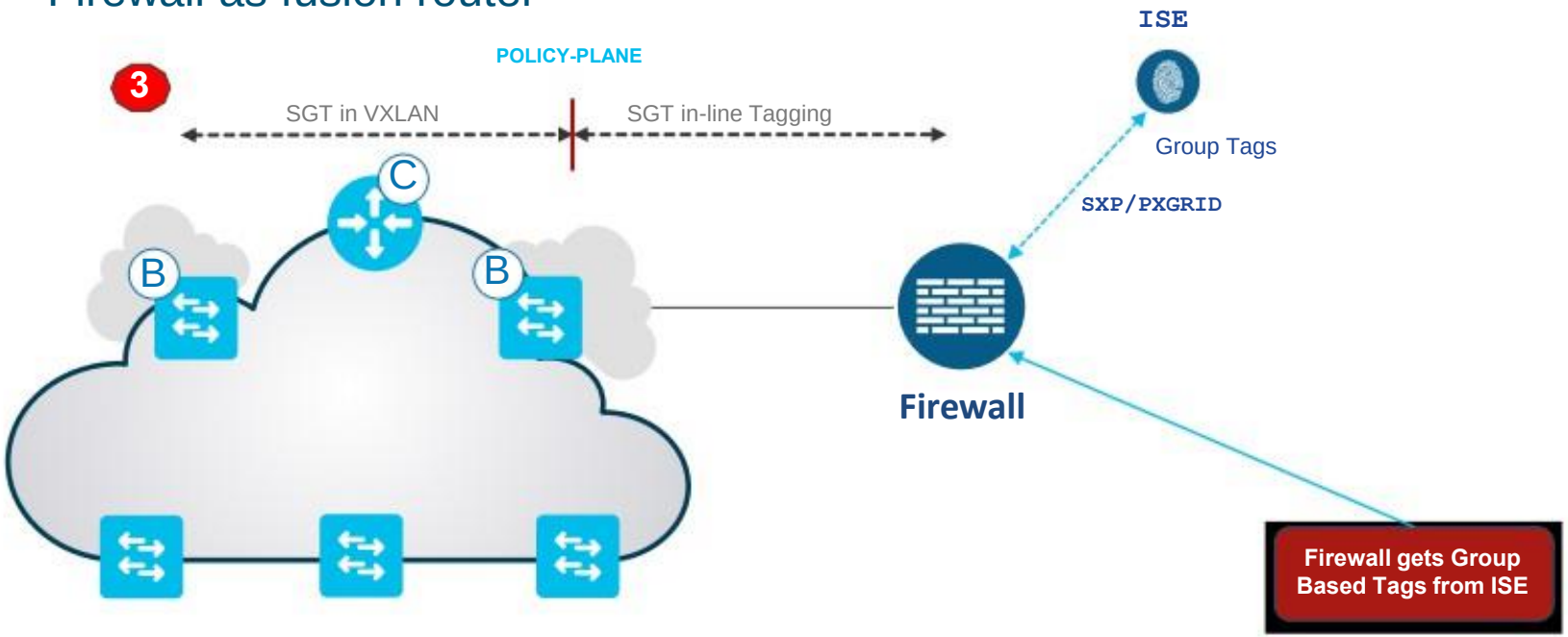
Border Deployment Options

Firewall as fusion router



Border Deployment Options

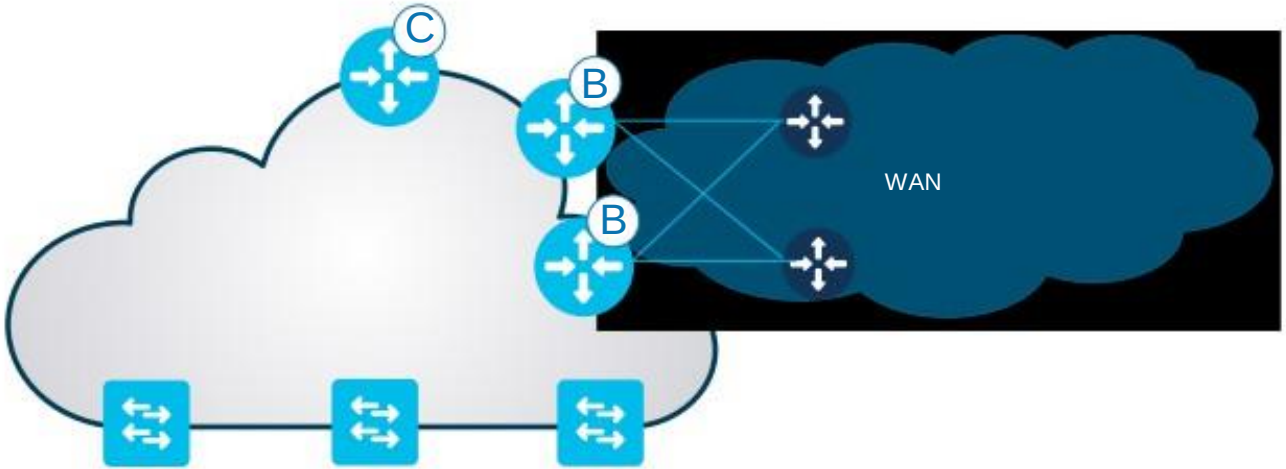
Firewall as fusion router



WAN Connectivity with Rest of Company /Internal Border

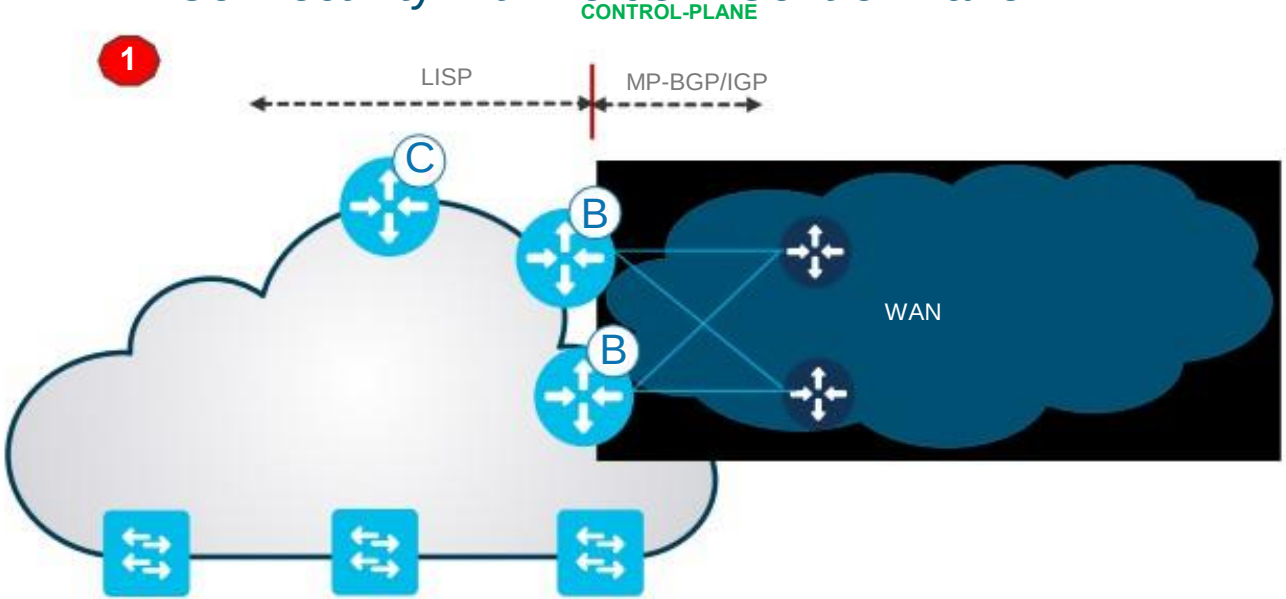
Border Deployment Options

WAN Connectivity with Border- WAN (MPLS/DMVPN)



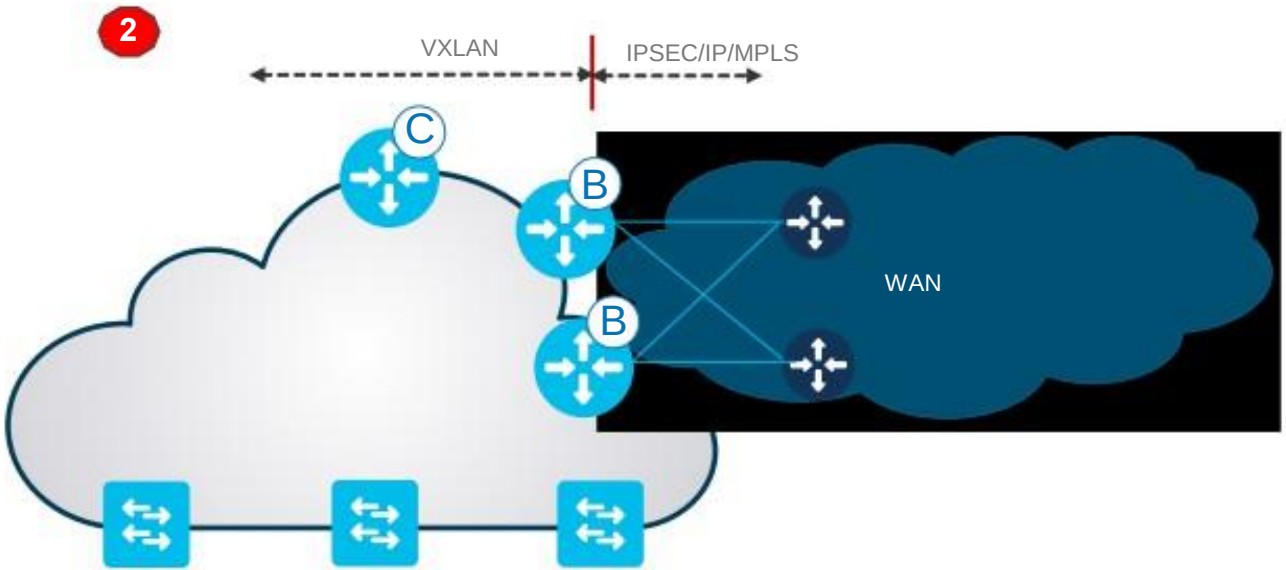
Border Design Options

WAN Connectivity with Border - Control Plane



Border Design Options

WAN Connectivity with Border - Data Plane



Cisco SD-Access - Connecting to the DataCenter, Firewall, WAN and More!

Conclusion

Session Summary

RECAP

For more details: cs.co/sda-compatibility-matrix

Cisco SD-Access Support

Digital Platforms for your Cisco Digital Network Architecture

Switching

NEW Catalyst 9500

Catalyst 9300

NEW Catalyst 9200

Catalyst 9400

Catalyst 4500E

Catalyst 6800

Nexus 7700

Catalyst 3650 & 3850

Routing

ASR-1000-HX

ASR-1000-X

ISR 4451

ISR 4430

ISR 4330

NEW

ENCS 5400

Wireless

Catalyst 9800

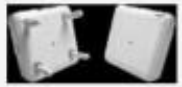
NEW

AIR-CT8540

AIR-CT5520

AIR-CT3504

NEW 4800



Wave 2 APs (1800,2800, 3800)

Wave 1 APs[*] (1700,2700,3700)

Extended BETA

Cisco Digital Building

Catalyst 3560-CX

NEW

Cisco IE 4K/5K

What to Do Next?

Refresh your Hardware & Software

Get **Cisco SD-Access Capable Devices** with **Cisco DNA Advantage OS License**

Deploy the Cisco DNA Center

Get **Cisco DNA Center Appliances** with **Cisco DNA Center Software**

Engage with Cisco Services

Cisco Services can help you **Test** - **Migrate** - **Deploy** - **Manage**

Cisco SD-Access Resources

Would you like to know more?

cisco.com/go/dna

cisco.com/go/sdaccess

- SD-Access At-A-Glance
- SD-Access Ordering Guide
- SD-Access Solution Data Sheet
- SD-Access Solution White Paper

cisco.com/go/cvd

- SD-Access Design Guide
- SD-Access Deployment Guide
- SD-Access Segmentation Guide

cisco.com/go/dnacenter

- Cisco DNA Center At-A-Glance
- Cisco DNA ROI Calculator
- Cisco DNA Center Data Sheet
- Cisco DNA Center 'How To' Video Resources

Thank you

cisco

INTUITIVE