The bridge to possible

Integrating Cisco Campus, SD-WAN, and Firepower in IPv6 Enterprise Networks

Winston Tsang
Technical Leader

BRKIPV6-2015

cisco Live!

#CiscoLive

Abstract

- Discuss a validated design that integrates Cisco campus, SD-WAN, and Firepower for IPv6 networks
- Explore the two approaches to deploying the campus and branches using either Cisco SD-Access Campus or traditional campus architecture to support IPv6-only clients
- Examine Cisco Firepower implementation for traffic filtering between the shared services block in the data center, campus and branch sites, and the internet.
- Look into using DNS64 and NAT64 services to enable IPv6-only hosts to communicate with IPv4-only servers
- Prerequisite: A good understanding of IPv6 fundamentals is expected

Your Speaker

- Winston Tsang, Technical Leader
  - 15+ years with Cisco
  - Cisco TAC Security, Solution Validation Services, Network Engineering, Solutions Engineering
- IPv6 Work
  - Designed and implemented solution to carry mobile IPv6 traffic over the IPv4 MPLS Core
  - Standardized IPv6 deployment procedure to onboard VPN customers
  - Produced Cisco Validated Profiles
    - IPv6 Integration with Cisco SD-Access, SD-WAN, and Firepower
    - IPv6 Traditional Campus Integration with Cisco SD-WAN and Cisco Firepower
- Hobbies
  - Playing chess and watching NBA basketball

Key Driver

- Enterprise IPv6 Adoption
  - Private IP addressing and Network Address Translation have delayed transition to IPv6
- New Driver: 2020 Government IPv6 Mandate
  - Requirement to migrate to an IPv6-only network and be 80% complete by the end fiscal 2025
- For certain enterprises, the cost of maintaining an IPv4 network will eventually outweigh the cost of transitioning to IPv6
- Let’s plan to deploy IPv6 today!

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKIPV6-2015

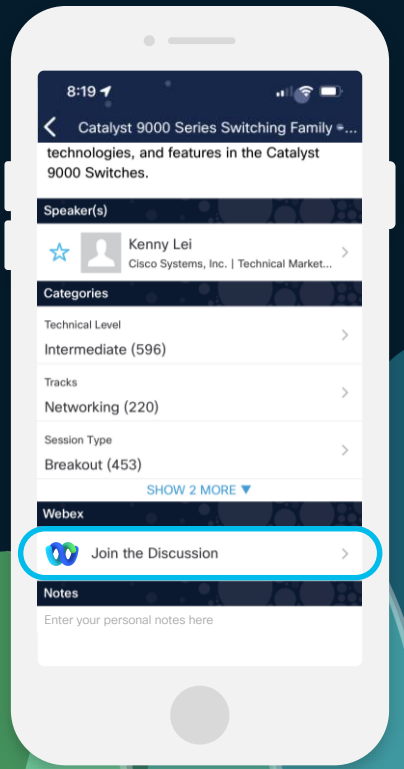
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

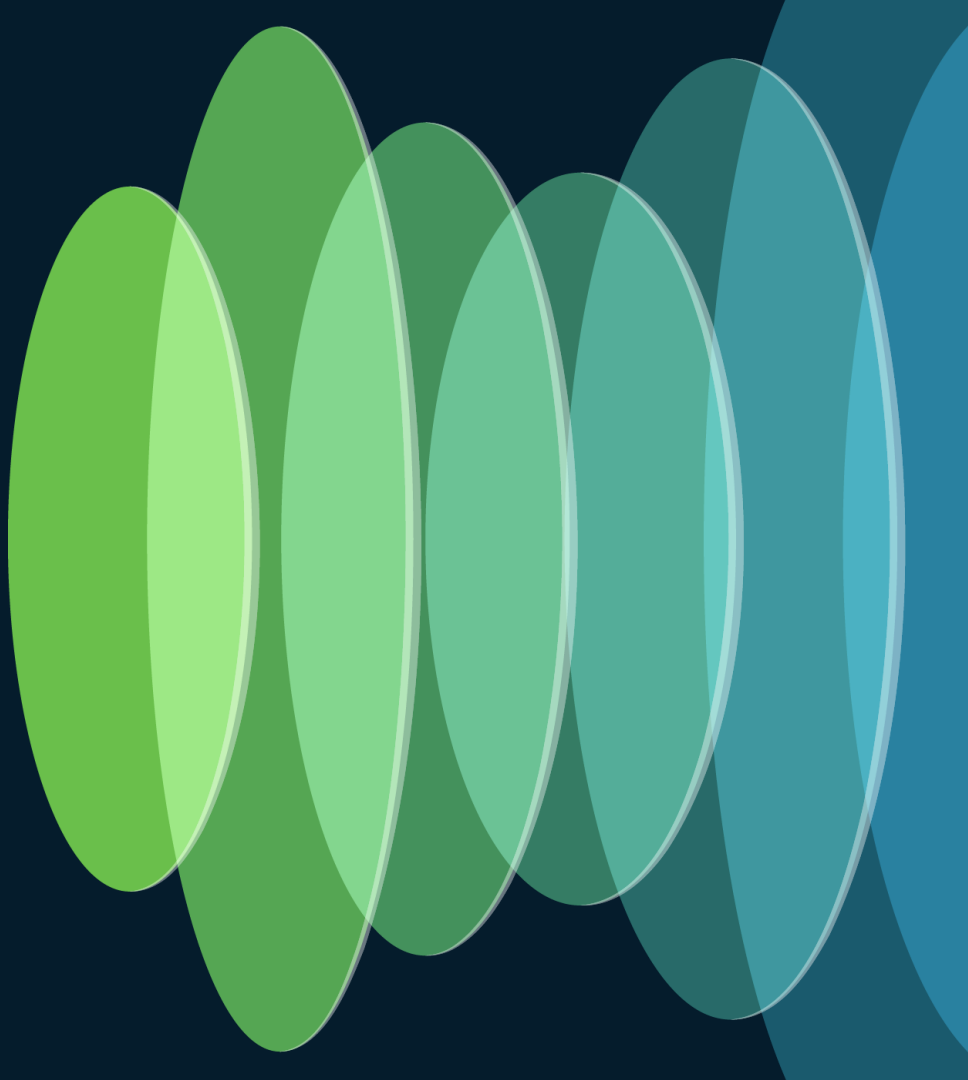
Webex spaces will be moderated by the speaker until June 7, 2024.



Agenda

- IPv6 Integration with **SD-Access Campus Deployment**
  - SD-Access and SD-WAN Integration
  - Main Campus Integration with Firepower
  - Branch Site Design
  - DNS64 and NAT64
  - IPv6 Wireless Guest
- IPv6 Integration with **Traditional Campus Deployment**

IPv6 Integration with SD-Access Campus Deployment

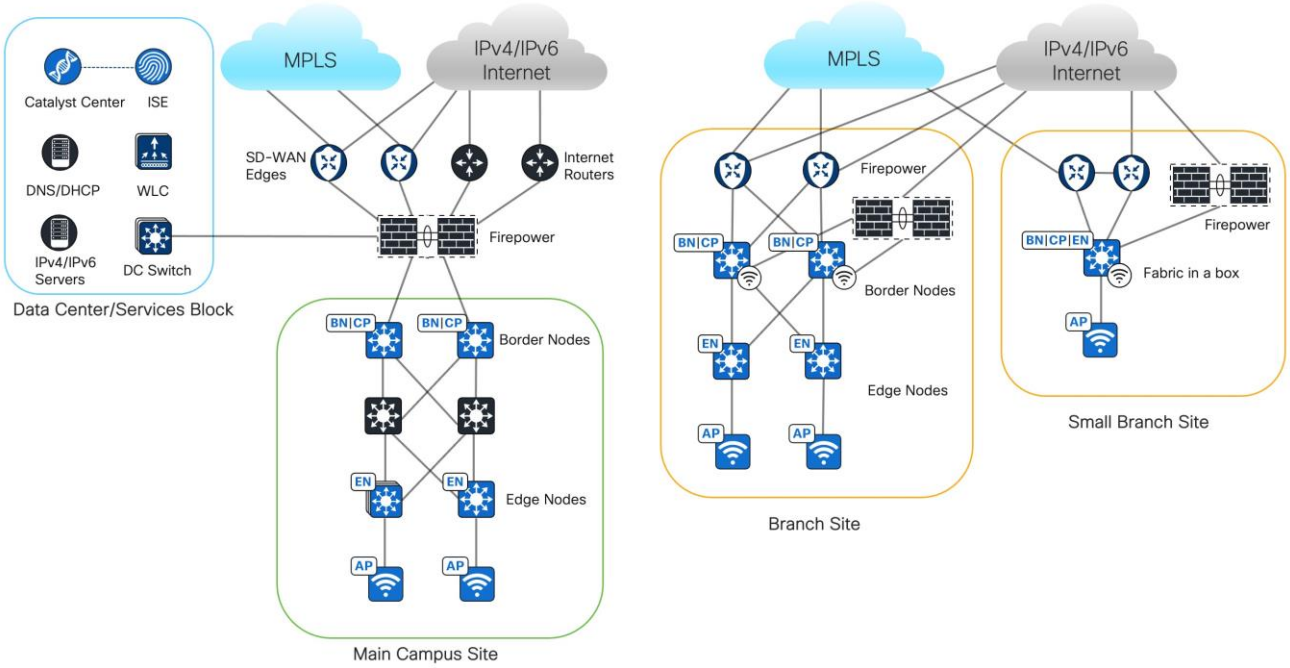


cisco Live!

IPv6 Integration with SD-Access Campus Deployment

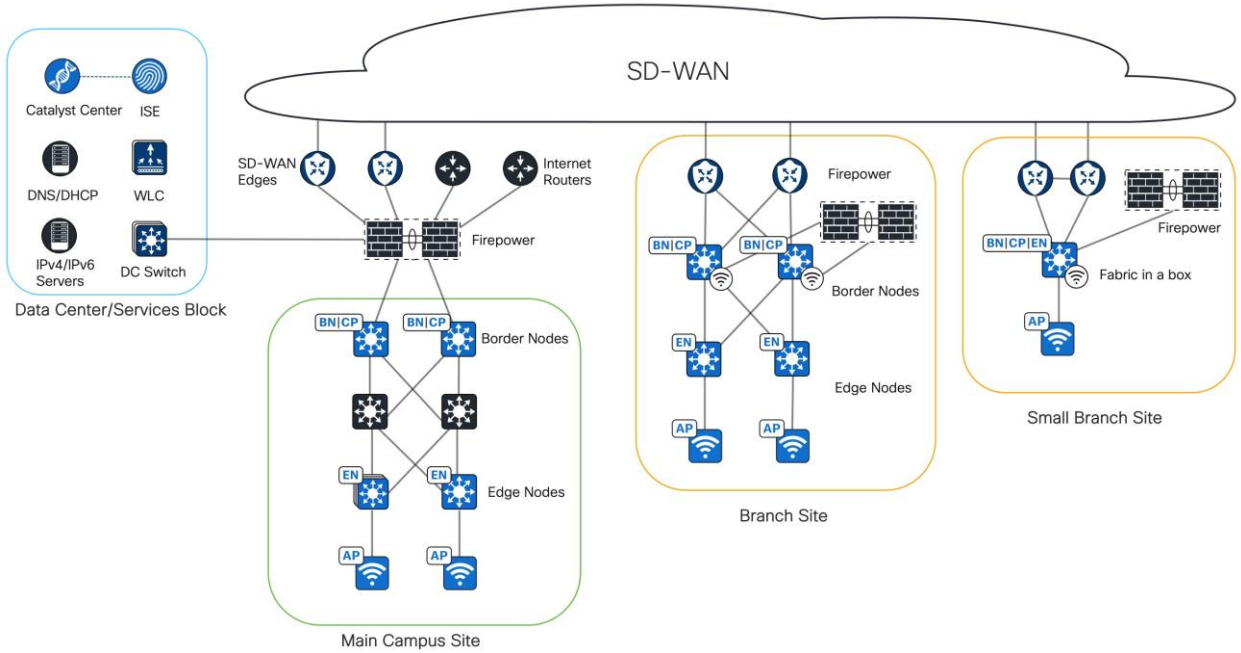
Highlights

- SD-Access + SD-WAN + Firepower
- Catalyst Center for network automation and assurance
- IPv6-Only Wired and Wireless Clients
- IPv6 Wireless Guest Flow
- Security
  - Macro-segmentation
  - Micro-segmentation

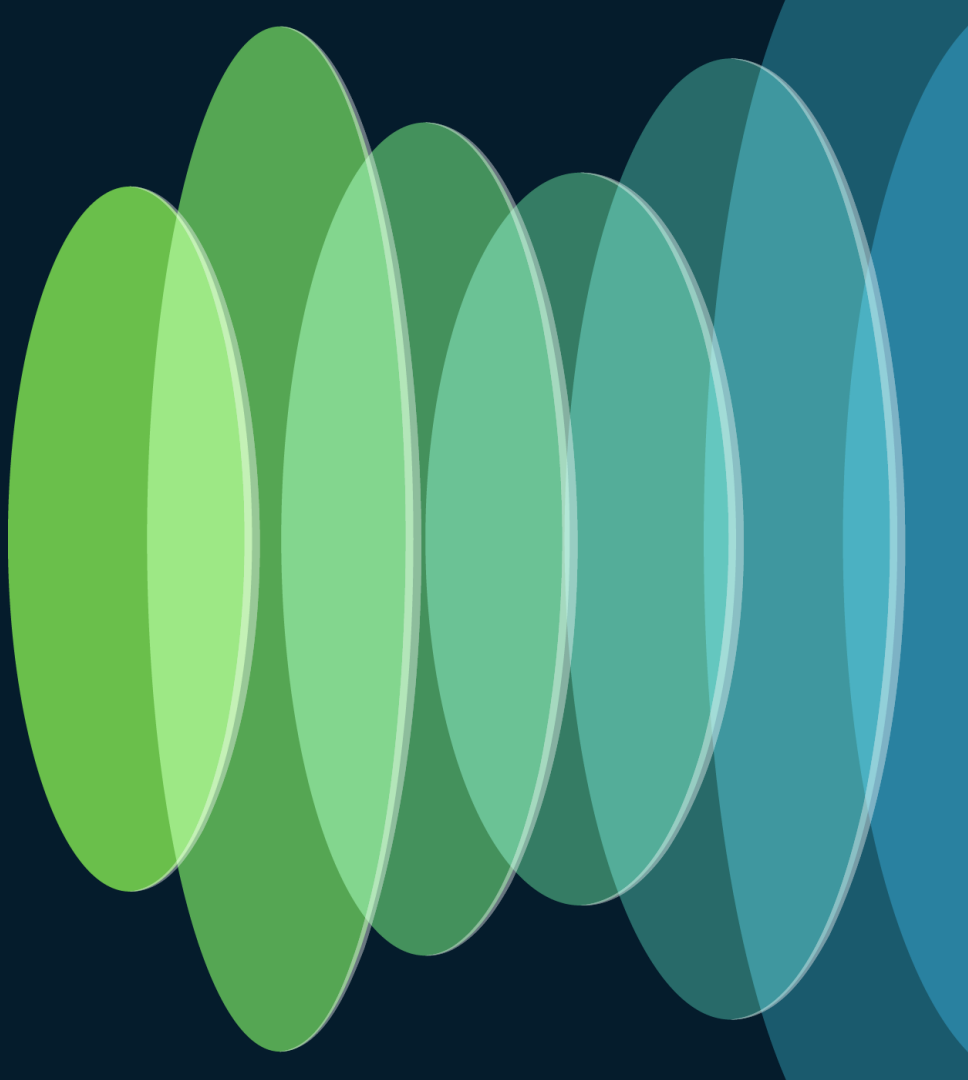


IPv6 Integration with SD-Access Campus Deployment

- SD-WAN Fabric connects Main Campus to Branch sites
- Shared services in Datacenter
- Main Site Firepower
  - Traffic Filtering
  - Route Leak between Global and VRF
  - NAT64



Current IPv6 Capabilities

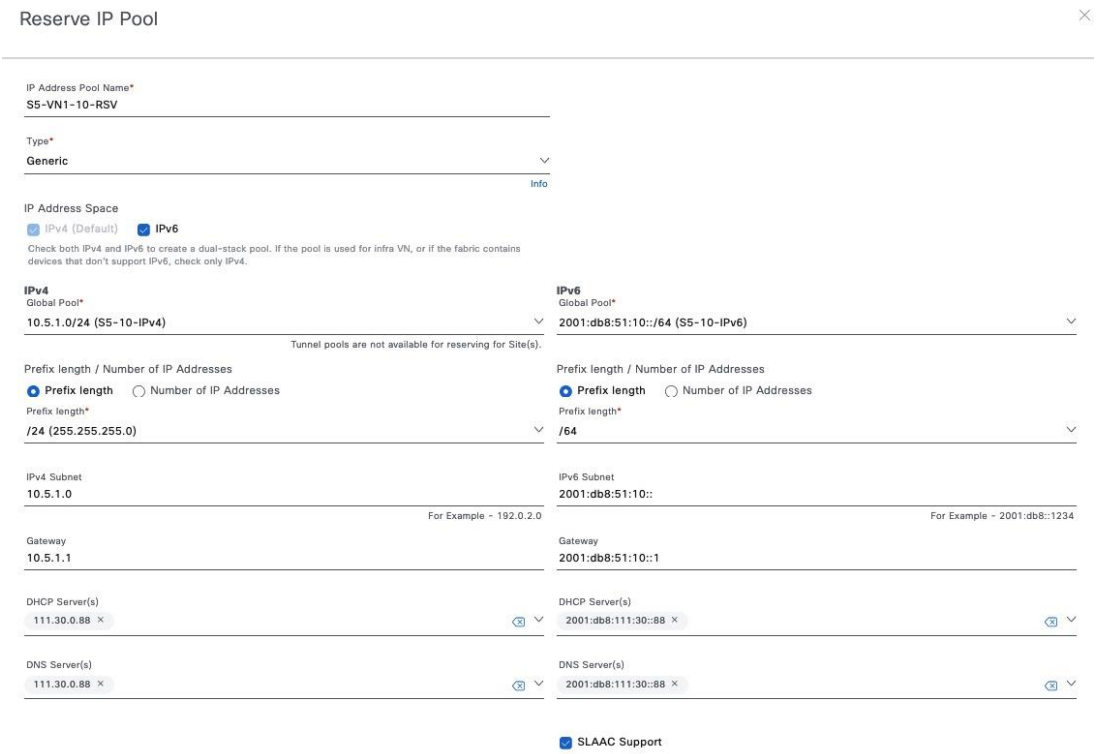


IPv6 in SD-Access

- Currently, SD-Access is only supported in the IPv4 underlay
  - Catalyst Center, ISE, and device communications occur in the IPv4 underlay
- IPv6 overlay traffic is carried over the IPv4 VXLAN Tunnel
- OSPFv3 used for Interior Gateway Protocol (IGP) for underlay, which supports both IPv4 and IPv6 address families

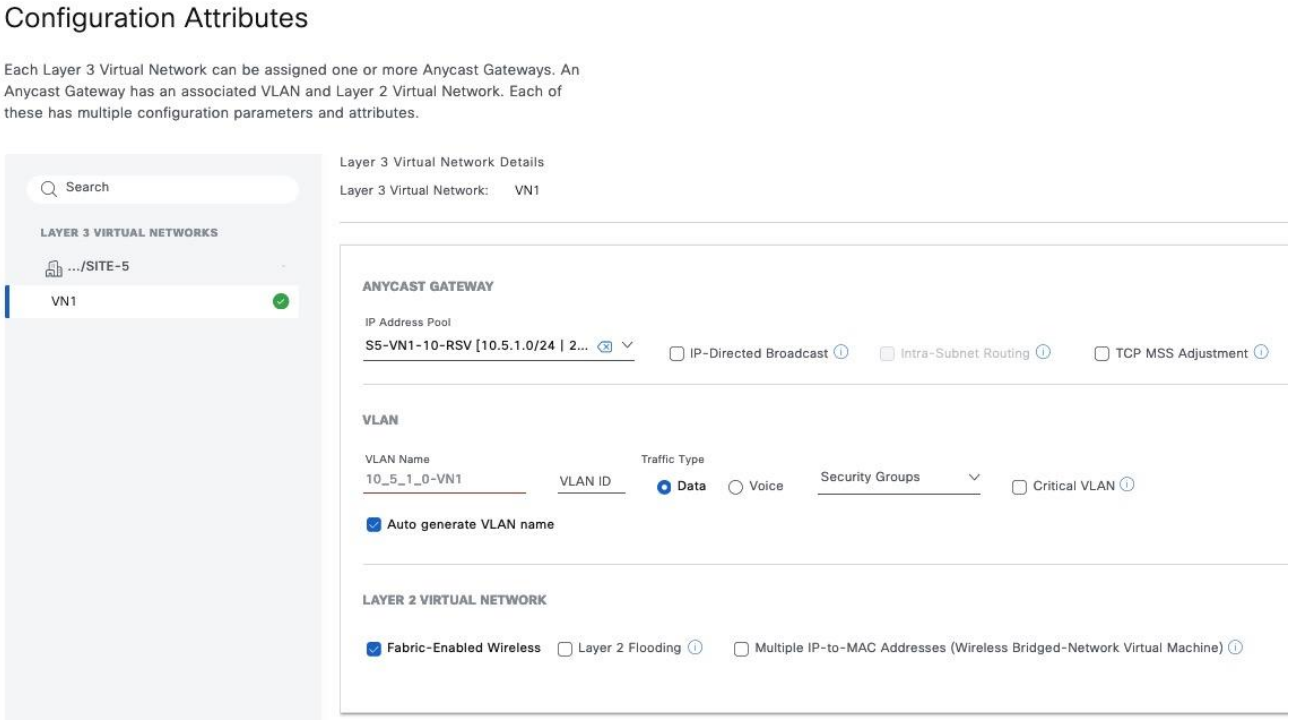
IPv6 in SD-Access

- Catalyst Center IP pool is dual stacked IPv4/IPv6 pool
  - IPv4 pool must be enabled with IPv6 pool
  - To ‘enforce’ IPv6-only
    - Use dummy IPv4 address for the IPv4 pool/ IPv4 dhcp server
  - For the IPv6 pool, a client can obtain IPv6 addresses from DHCPv6 and/or SLAAC



Example Fabric Edge SVI Configuration

- Dual Stack IP Pool is applied to Anycast Gateway configuration in a Virtual Network under Fabric Sites



Example Fabric Edge SVI Configuration

- Switch Virtual Interface (SVI) configuration pushed by Catalyst Center to Fabric Edges in the site
- Wired/wireless clients associated with the IP Pool are placed on this VLAN via the host onboarding procedure

SD-Access Fabric Edge

```
interface Vlan1026
 description Configured from Catalyst Center
 mac-address 0000.0c9f.f5e1
 vrf forwarding VN1
 ip address 10.5.1.1 255.255.255.0
 ip helper-address 111.30.0.88
 no ip redirects
 ip route-cache same-interface
 ipv6 address 2001:DB8:51:10::1/64
 ipv6 enable
 ipv6 nd dad attempts 0
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 nd router-preference High
 ipv6 dhcp relay destination 2001:DB8:111:30::88
 ipv6 dhcp relay source-interface Vlan1026
 ipv6 dhcp relay trust
 no lisp mobility liveness test
 lisp mobility 10_5_1_0-VN1-IPV4
 lisp mobility 10_5_1_0-VN1-IPV6
```

IPv6 in SD-WAN

- Control and Data plane sessions can be carried over IPv4 or IPv6 WAN transports
- If using dual-stack on transport interface, IPv4 transport takes precedence
- SD-WAN 20.10/IOS-XE 17.10 versions or later, enable ipv6-strict-control to prefer the IPv6 transport carrying Control plane and Data plane sessions.

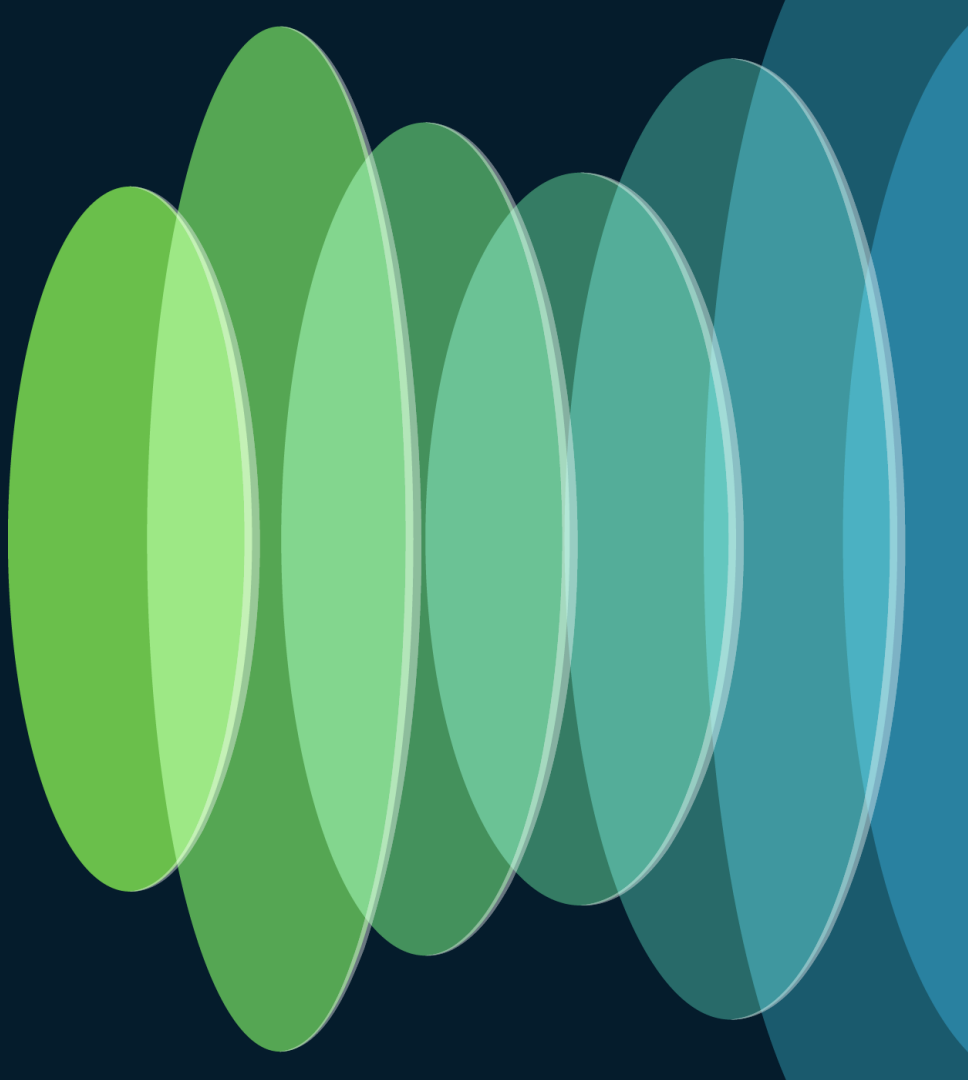
SD-WAN Edge

```
system
 system-ip            1.1.1.11
 overlay-id           1
 site-id              1
 ipv6-strict-control  true
 no transport-gateway enable
 port-offset          0
 control-session-pps  300
 admin-tech-on-failure
 sp-organization-name  SJC-SDWAN-LAB-IPv6
 organization-name     SJC-SDWAN-LAB-IPv6
 port-hop
 track-transport
 track-default-gateway
 console-baud-rate     9600
 no on-demand enable
 on-demand idle-timeout 10
 vbond 2001:DB8:170:10::201 port 12346
```

IPv6 in Firepower

- Provides dual-stack IPv4/IPv6 support
- Network Segmentation
  - Firewall Instances(Logical Firewalls)
  - Virtual Routers(VRFs in a single firewall)
    - Supports BGPv6 in user-defined virtual router in version 7.1 or later
    - Supports IPv6 Route leaking in version 7.1 or later
- Filter Inter-site and Internet IPv6 Traffic
- Provide NAT64 services

SD-Access and SD-WAN Integration



cisco Live!

SD-Access and SD-WAN Integration

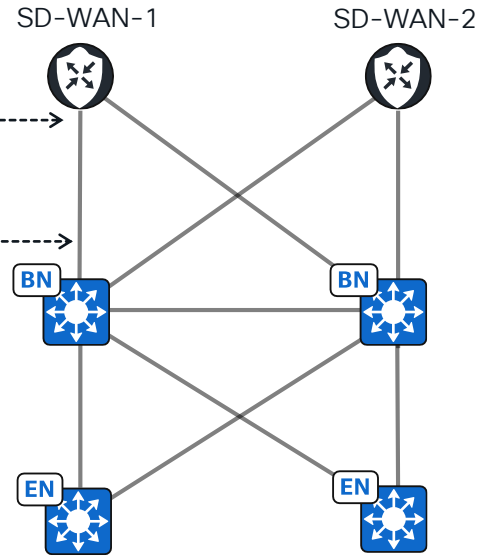
- Extend Data-plane, control-plane and policy-plane from campus to branch
- Between SD-Access Fabric Border and SD-WAN Edge:
  - Enable VRF-LITE
  - Enable eBGP peering
  - Enable Inline Security Group Tag (SGT)

SD-Access and SD-WAN Integration – VRF-LITE

- SD-WAN Edge subinterface is placed in VRF belonging to SD-WAN VPN and assigned an IPv6 address
- Fabric Border SVI is placed in VRF belonging to SD-Access Virtual Network(VN) and assigned an IPv6 address
- SD-WAN Edge subinterface dot1q # matches Fabric Border SVI vlan # to connect SD-WAN VPN to SD-Access VN

```
interface GigabitEthernet0/0/0.3001
 encapsulation dot1Q 3001
 vrf forwarding 1
 ipv6 address 2001:DB8:1::2/127
```

```
interface Vlan3001
 vrf forwarding VN1
 ipv6 address 2001:DB8:1::3/127
 ipv6 enable
```



SD-Access and SD-WAN Integration – eBGP

- Enable eBGP Peering between SD-WAN Edge and SD-Access Fabric Border
- On SD-WAN Edge, perform mutual route redistribution between BGP and Overlay Management Protocol (OMP)

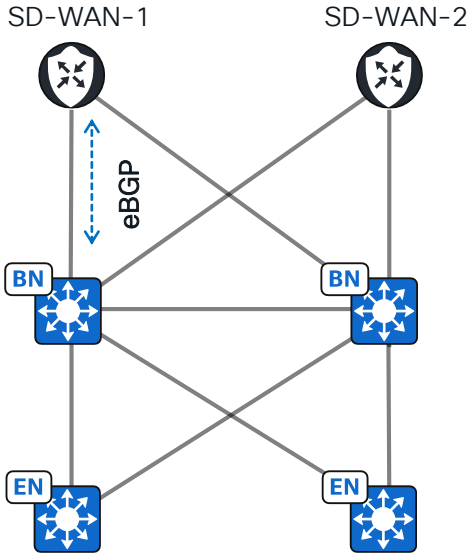
[SD-WAN-1]

```
router bgp 61021
 address-family ipv6 vrf 1
  redistribute omp
  maximum-paths eibgp 2
  distance bgp 20 200 20
  neighbor 2001:DB8:1::3 remote-as 61002
  neighbor 2001:DB8:1::3 activate

 sdwan
  omp
   address-family ipv6 vrf 1
    advertise bgp
```

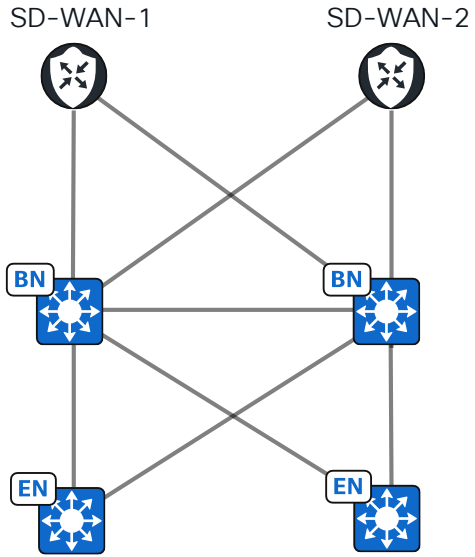
[BN]

```
router bgp 61002
 address-family ipv6 vrf VN1
  neighbor 2001:DB8:1::2 remote-as 61021
  neighbor 2001:DB8:1::2 update-source Vlan3001
  neighbor 2001:DB8:1::2 activate
```



SD-Access and SD-WAN Integration – Inline SGT

- Security Group Tag (SGT) classifies traffic in a Cisco TrustSec network
- User/device traffic can be identified by SGT instead of IPv4/IPv6 address
- Apply policy enforcement based on SGTs
- SGTs are carried in Layer2 encapsulation
- Enabling Inline SGT allows the ethernet interface to carry the SGT value in the CMD field of the ethernet header



SD-Access and SD-WAN Integration – Inline SGT

- On SD-WAN Edge, enable inline SGT on both physical interfaces and subinterfaces connected to the Fabric Border Nodes
- Enable SGT propagation on SD-WAN Tunnel interfaces. Disabled by default since SD-WAN 20.6.1/IOS-XE 17.6.1
- Enable inline SGT on Fabric Border Node trunk interface connected to SD-WAN Edge

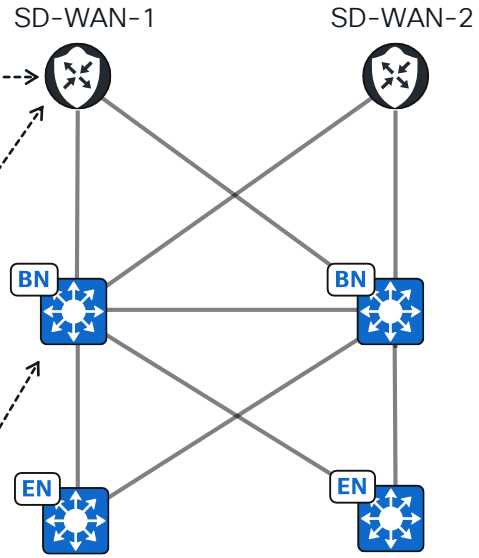
```
interface GigabitEthernet0/0/0
 cts manual

interface GigabitEthernet0/0/0.3001
  cts manual
  policy static sgt 2 trusted
```

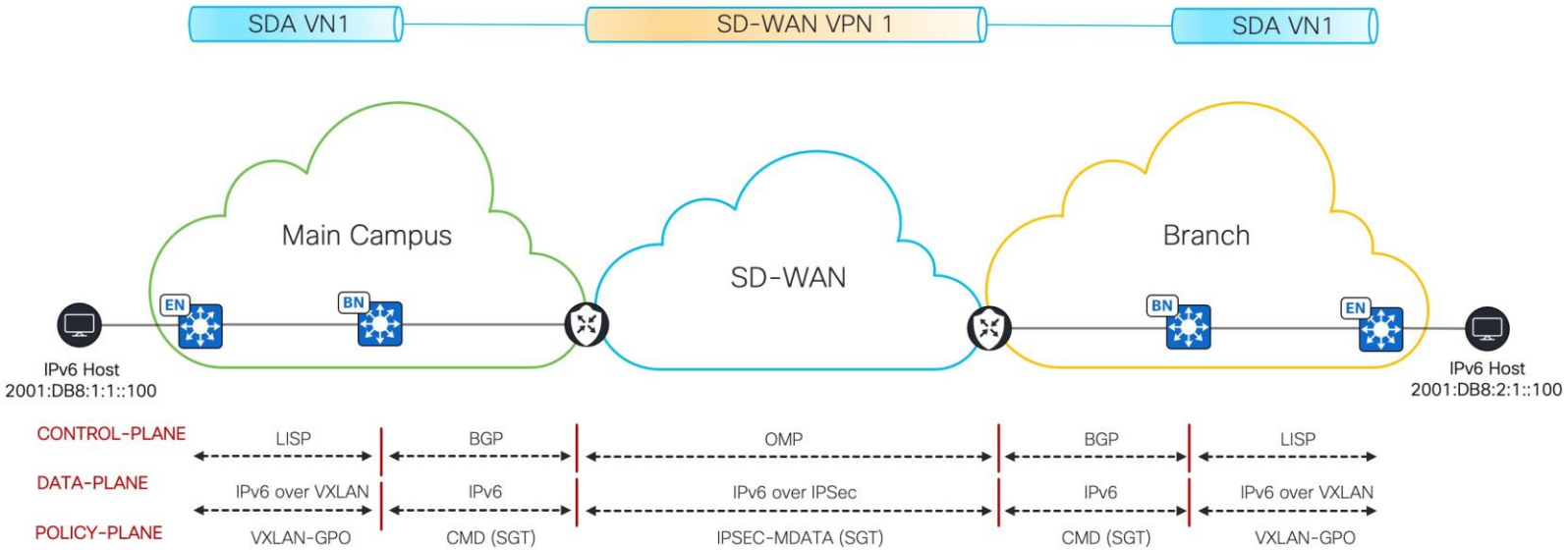
```
interface Tunnel3
cts manual

interface Tunnel4
cts manual
```

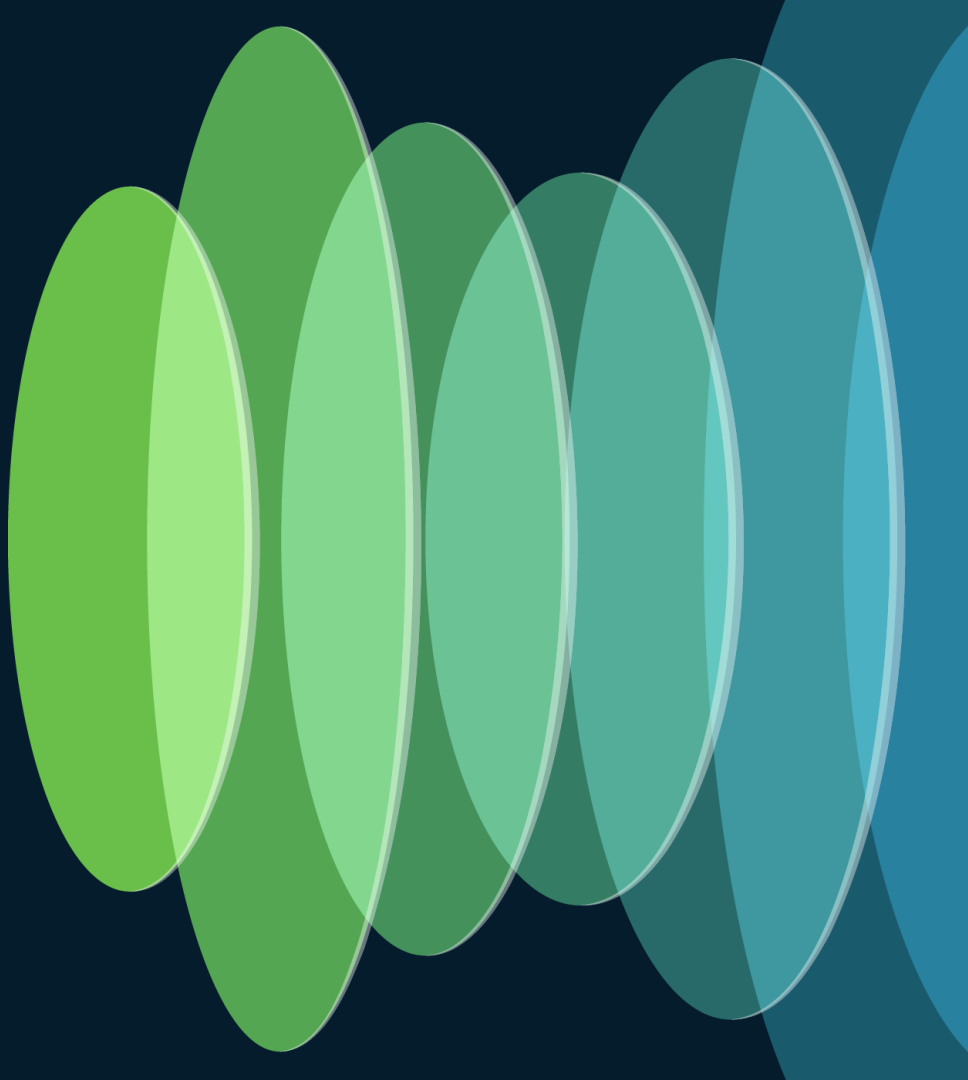
```
interface TenGigabitEthernet1/0/1
 switchport mode trunk
 cts manual
  policy static sgt 2 trusted
```



End-to-End Integration of Data, Control, Policy Planes



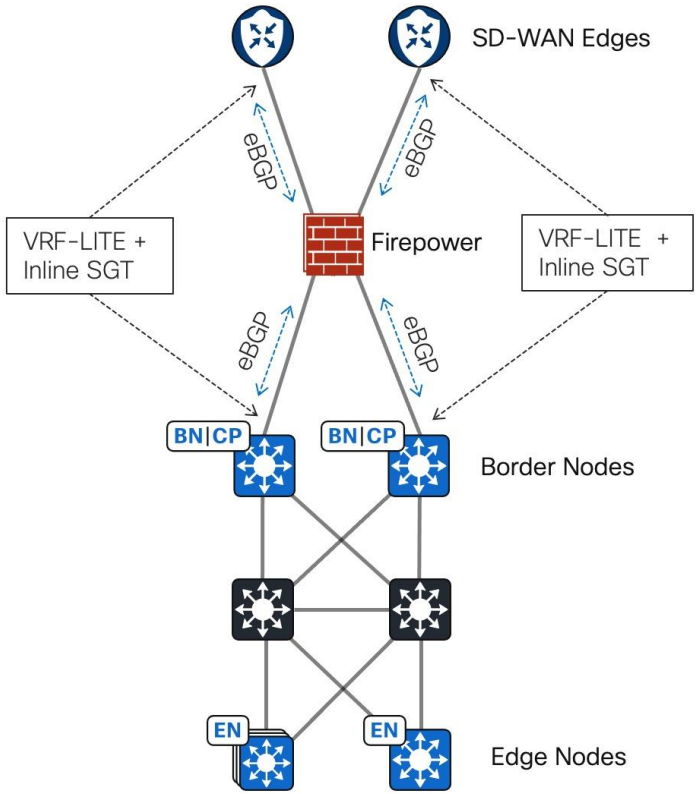
Main Campus Integration with Firepower



cisco Live!

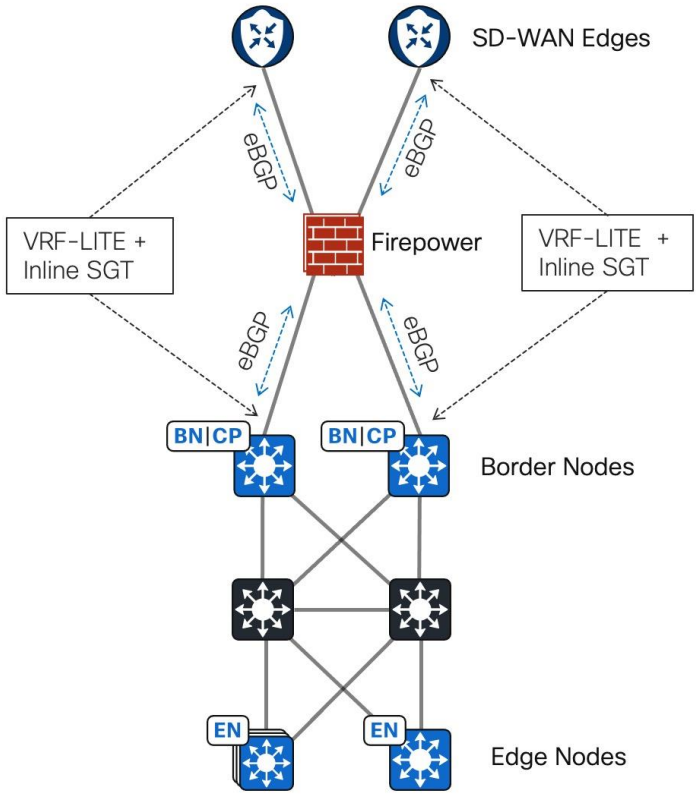
Firepower between SD-Access and SD-WAN

- 1) Between Firepower and SD-WAN Edges
  - Enable VRF-LITE
  - Enable eBGP peering
  - Enable Inline SGT
- 2) Between Firepower and Fabric Borders
  - Enable VRF-LITE
  - Enable eBGP peering
  - Enable Inline SGT

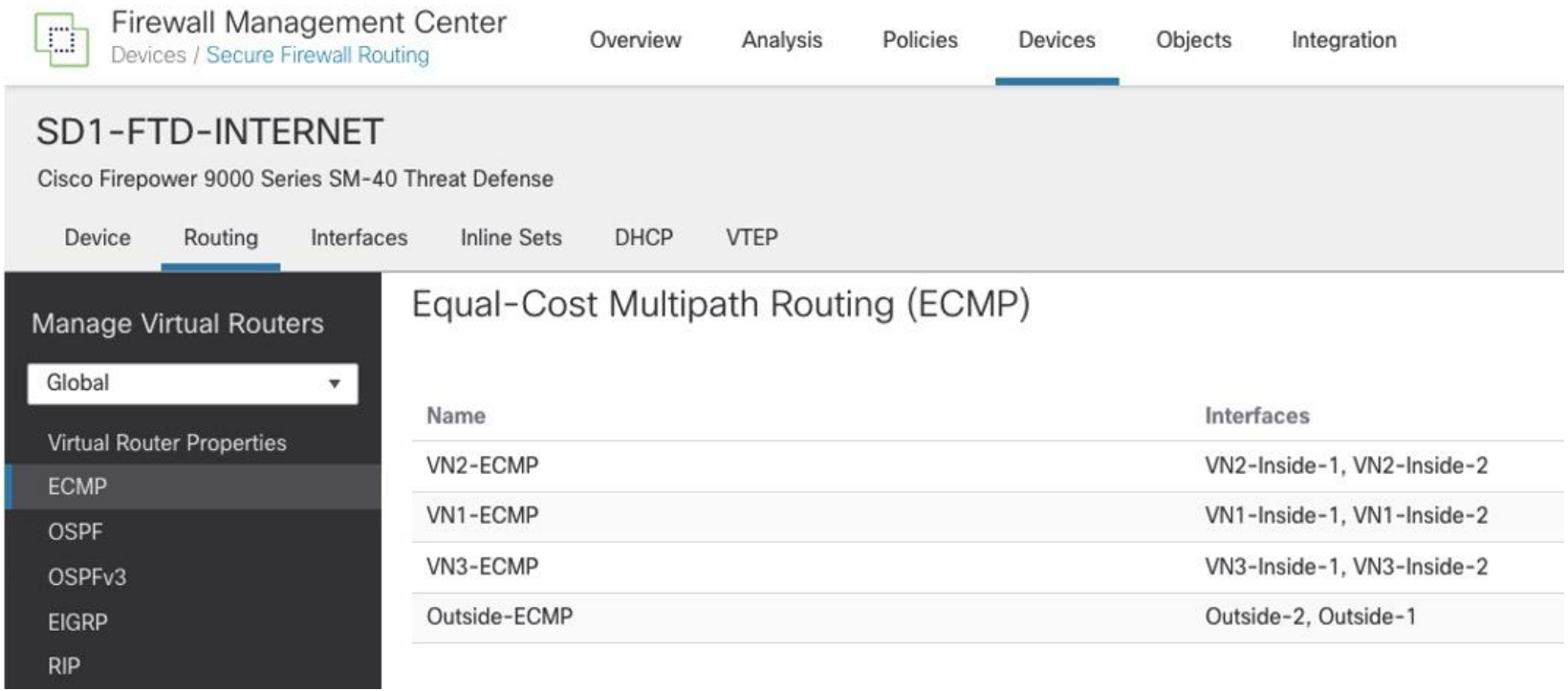


Firepower between SD-Access and SD-WAN

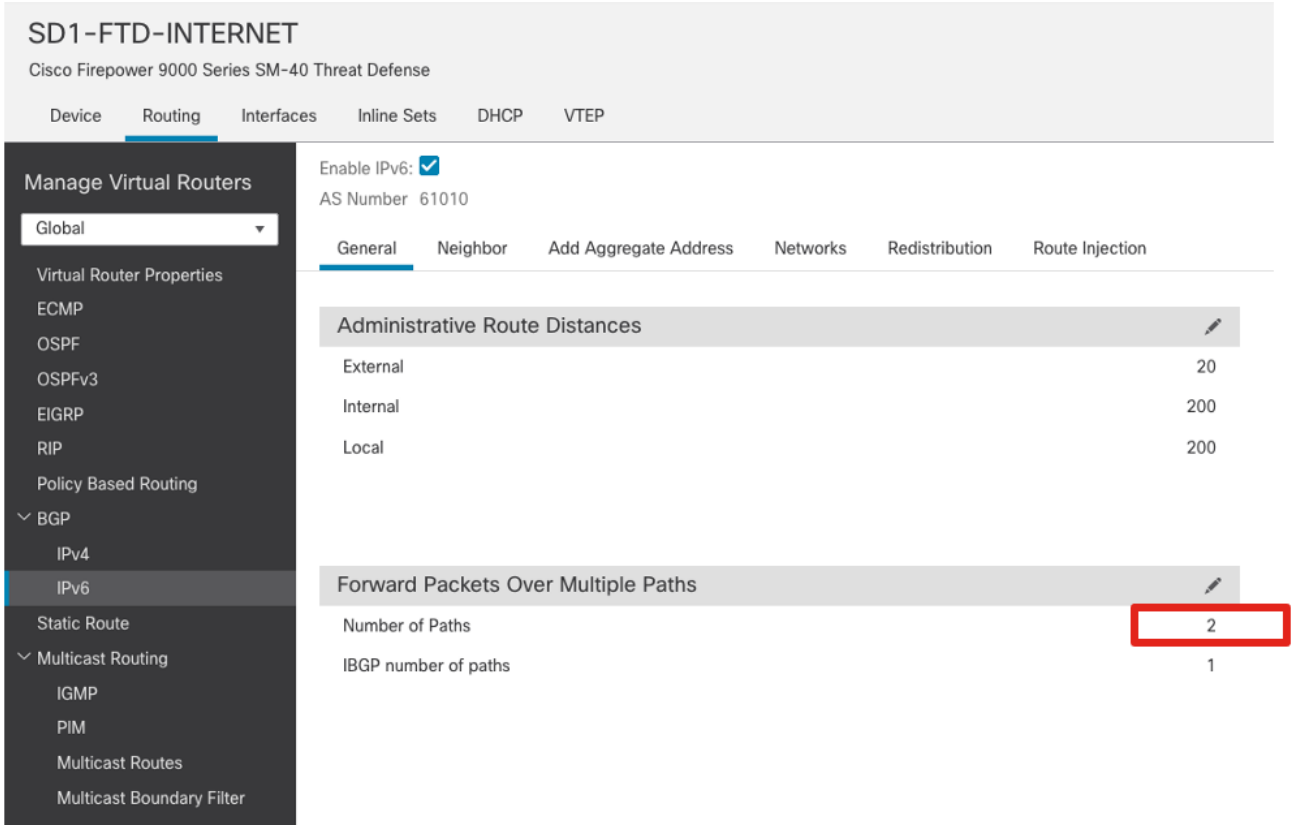
- Dual firewall connections to SD-WAN Edges and SD-Access Fabric Borders
- Traffic egressing one interface and returning on another interface dropped by Firewall Stateful Inspection
- Solution
  - Enable ECMP Zones
    - Place both FW interfaces towards Fabric Border nodes in one ECMP Zone
    - Place both FW interfaces towards SD-WAN edges in another ECMP Zone
  - Set eBGP multipath to 2



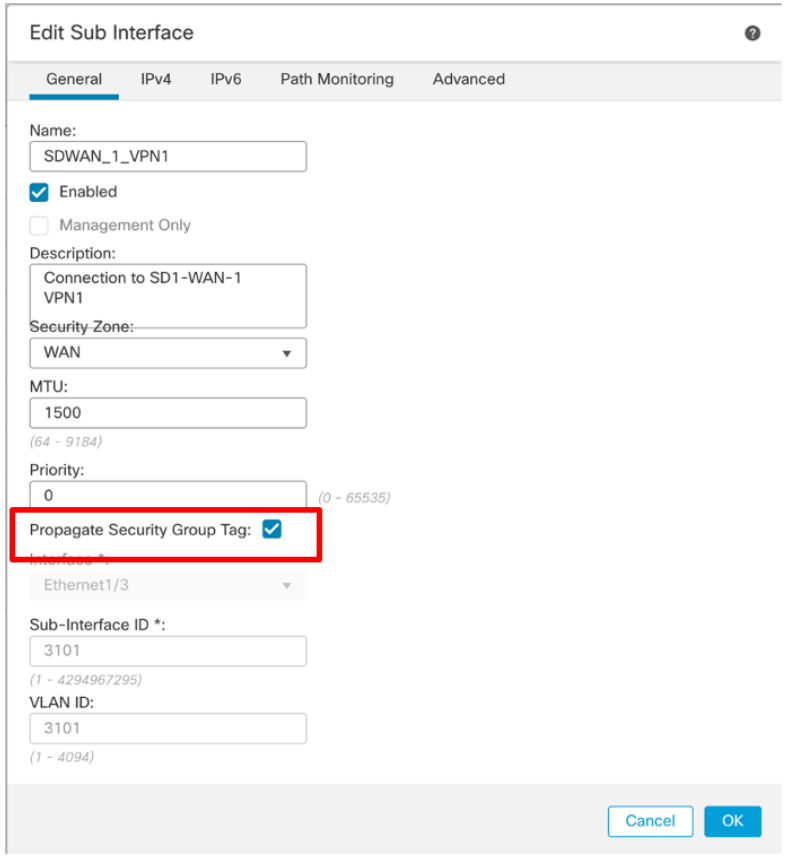
Enable ECMP Zones



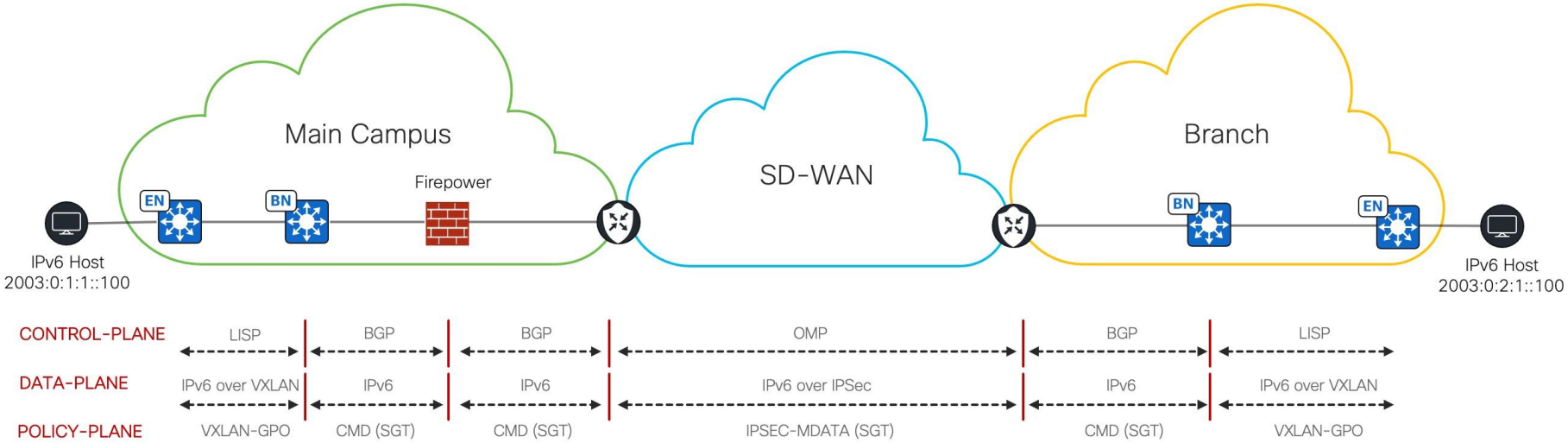
Enable eBGP Multipath



Enable Inline SGT on Firepower Subinterfaces



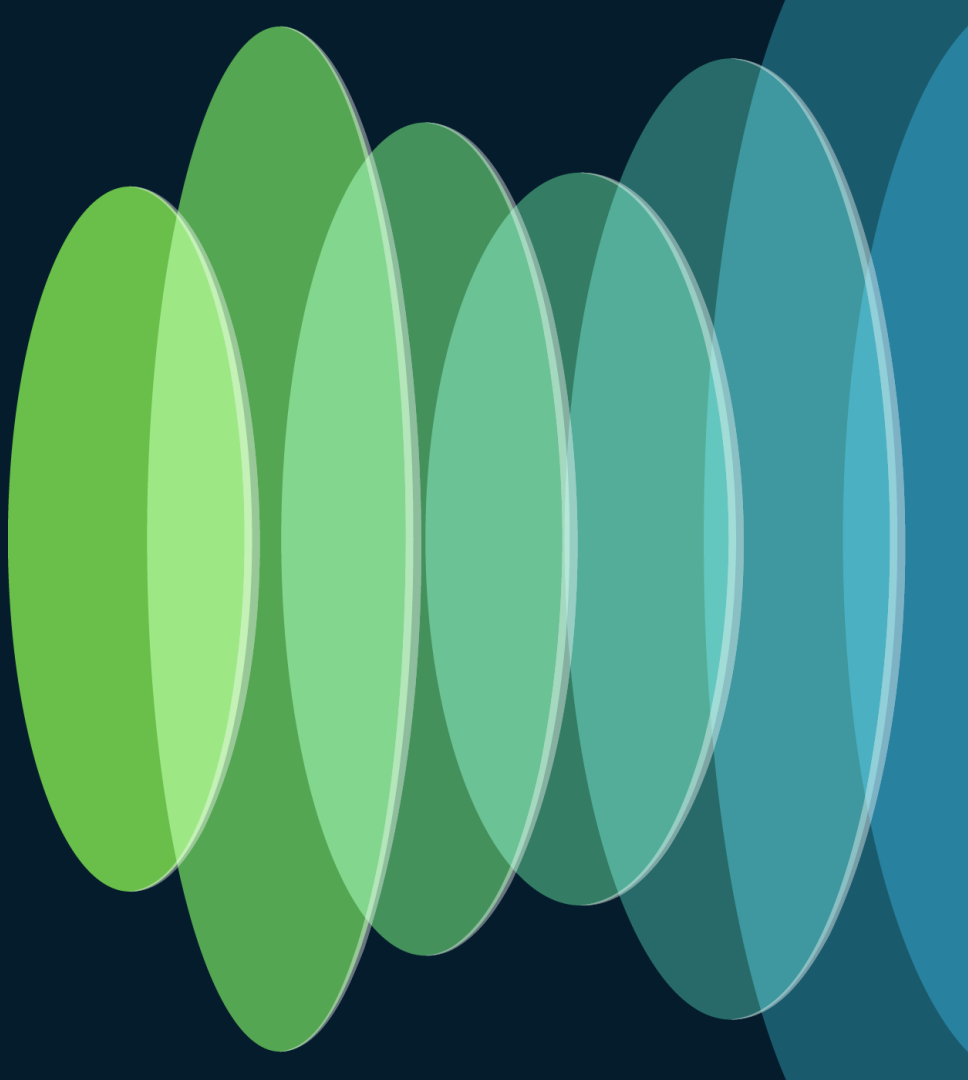
Data, Control, and Policy Plane Integration with Firewall



Firepower – ICMPv6 Filtering Considerations

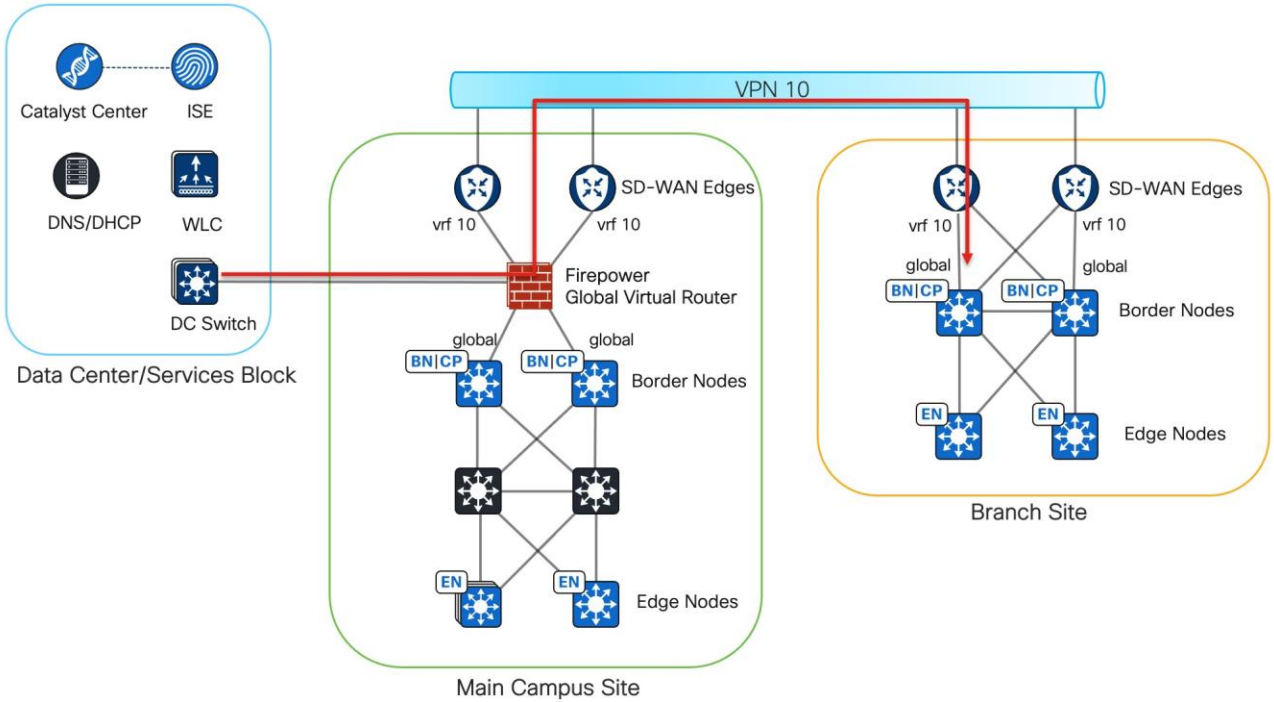
- In IPv6, fragmentation is performed by the source host and not by routers
- Path MTU discovery is used to determine optional MTU for a path
- For Path MTU discovery to function, Firewall must not block ICMPv6 (type 2) packet too big
- Reference RFC 4890 – Recommendations for Filtering ICMPv6 messages in Firewalls > Traffic That Must Not be Dropped
  - Destination Unreachable (Type 1) – All codes
  - Packet Too Big (Type 2)
  - Time Exceeded (Type 3) – Code 0 only
  - Parameter Problem (Type 4) – Codes 1 and 2 only

SD-Access Underlay Traffic through SD-WAN

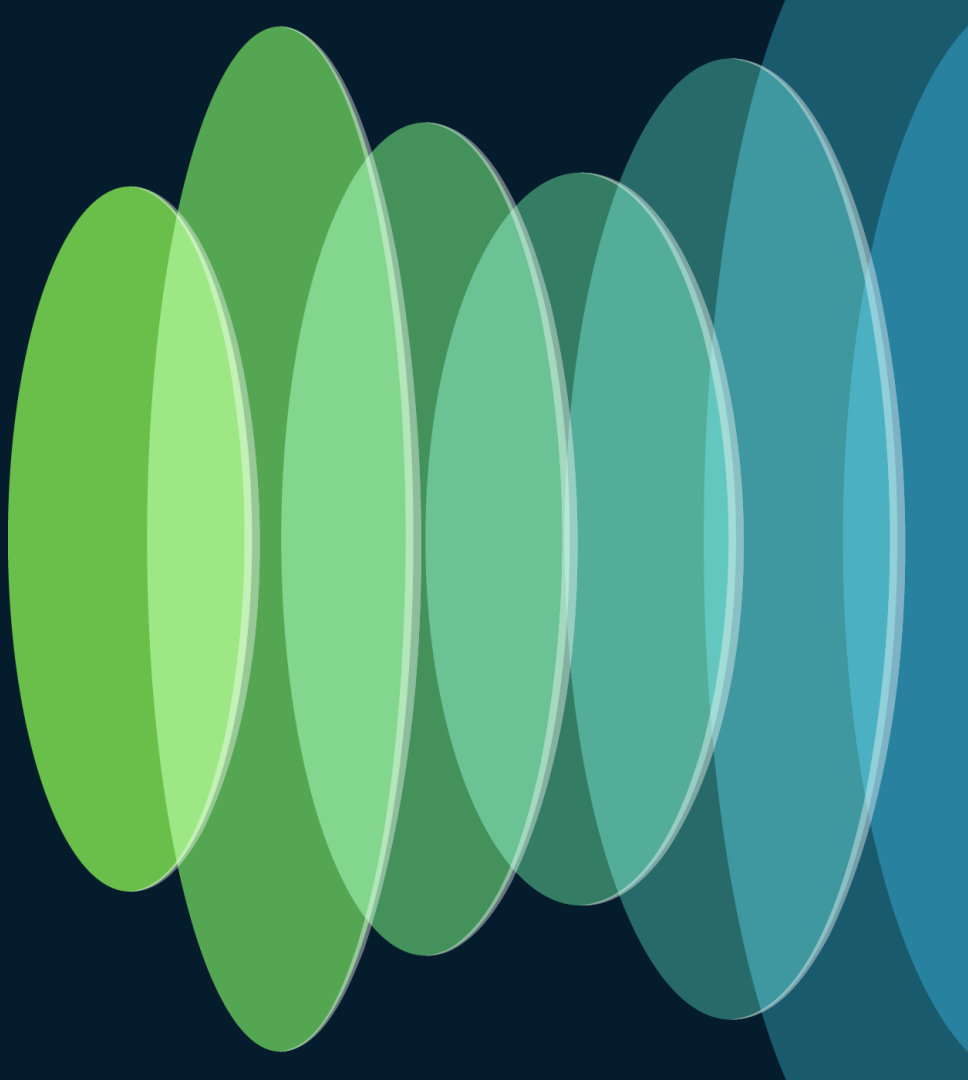


SD-Access Underlay Routing across SD-WAN

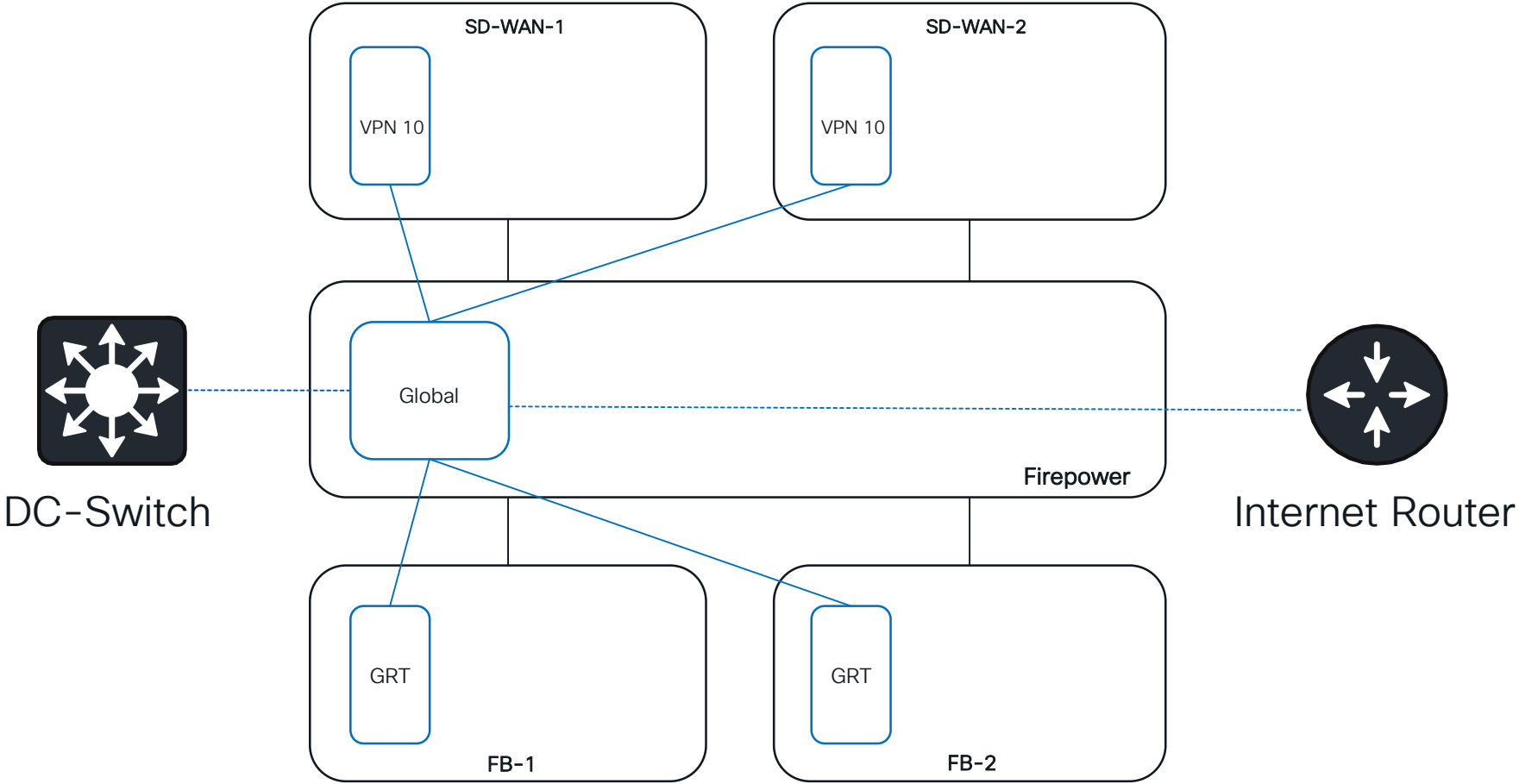
- Catalyst Center needs to reach SD-Access underlay at branch sites
- Use a SD-WAN VPN dedicated for carrying SD-Access Underlay traffic
- At main site, FW global interface connects to SD-WAN service VPN interface
- At branch site, Fabric Border global interface connects to SD-WAN service VPN interface



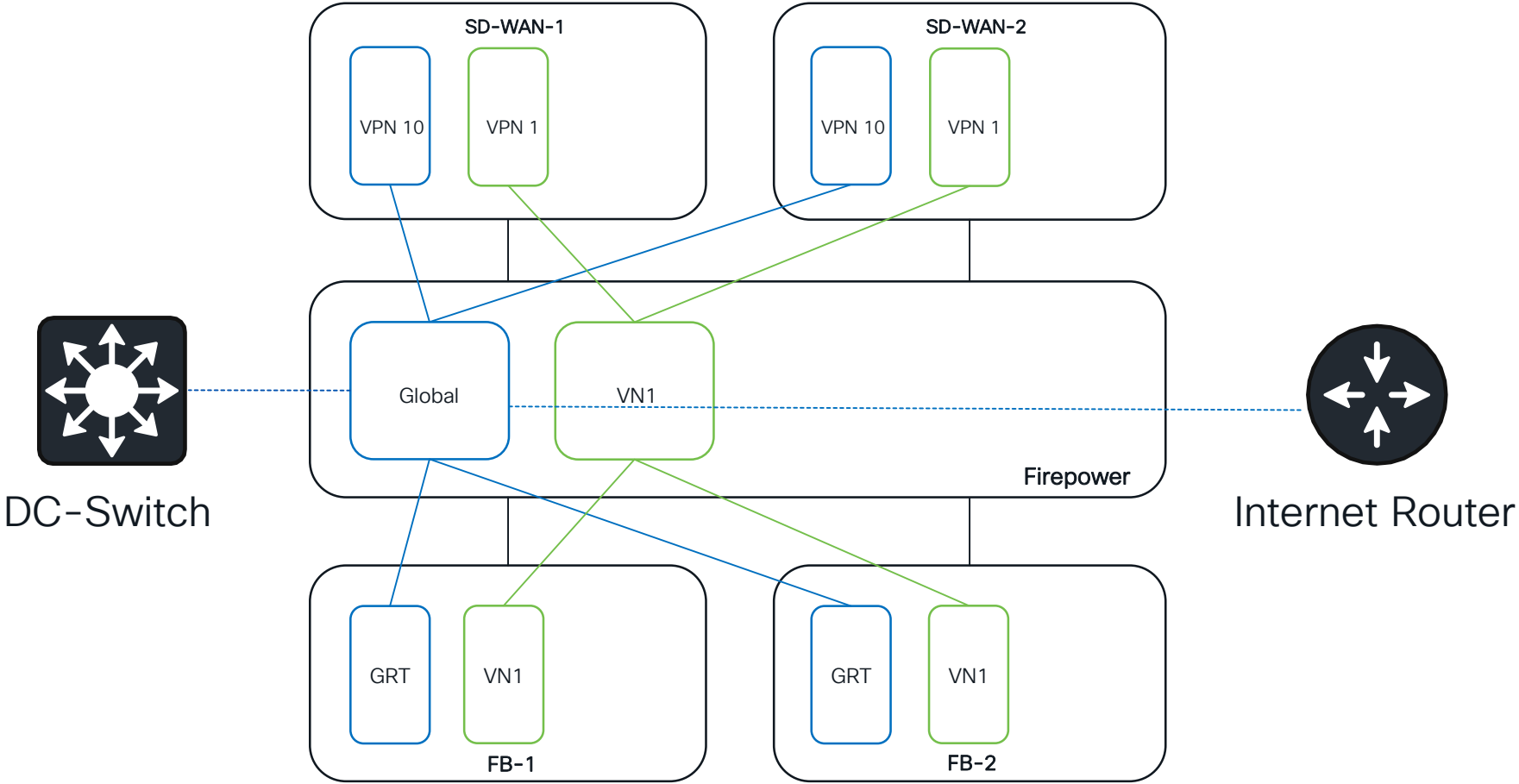
Firepower Logical Segmentation



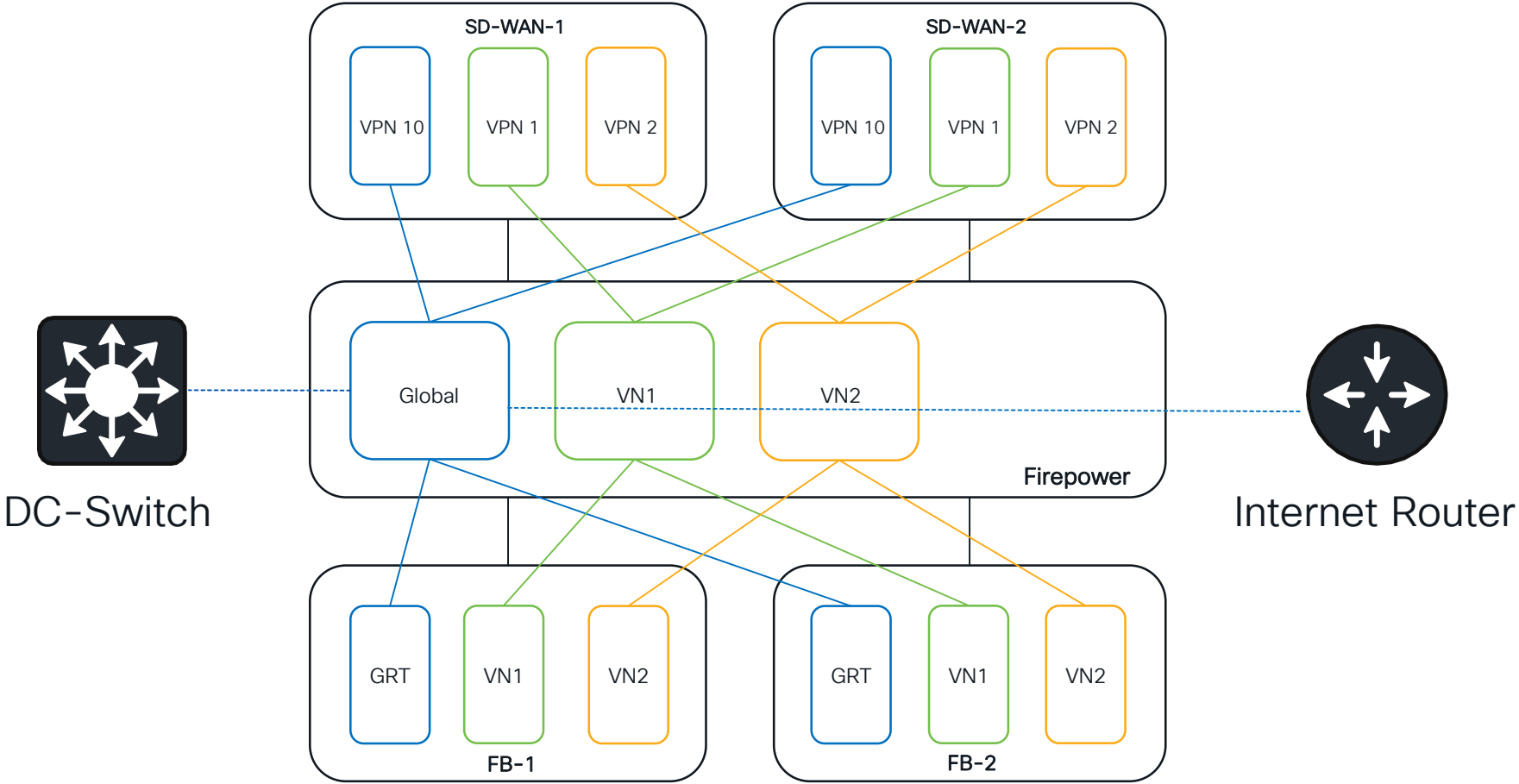
Firewall Virtual Routers



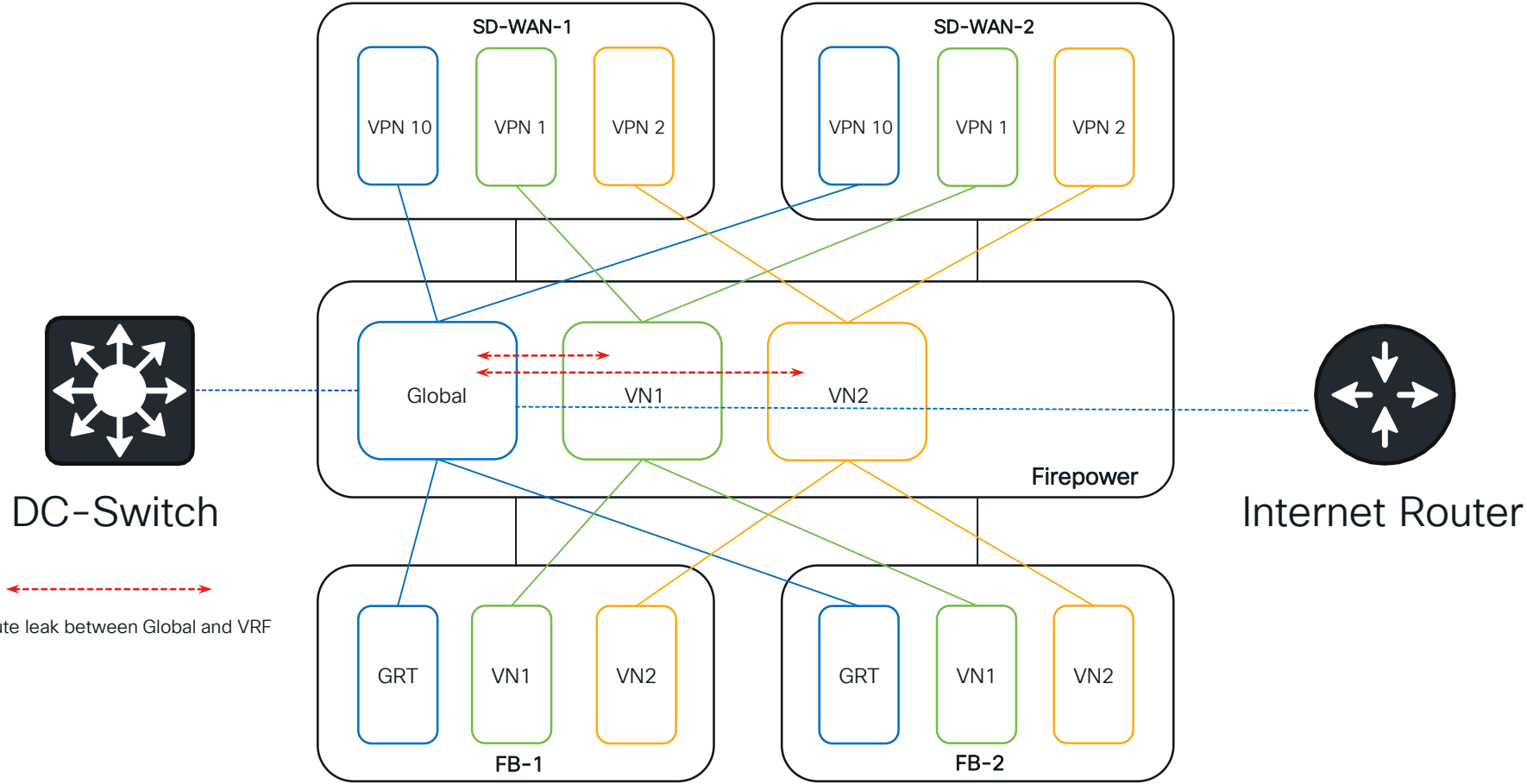
Firewall Virtual Routers



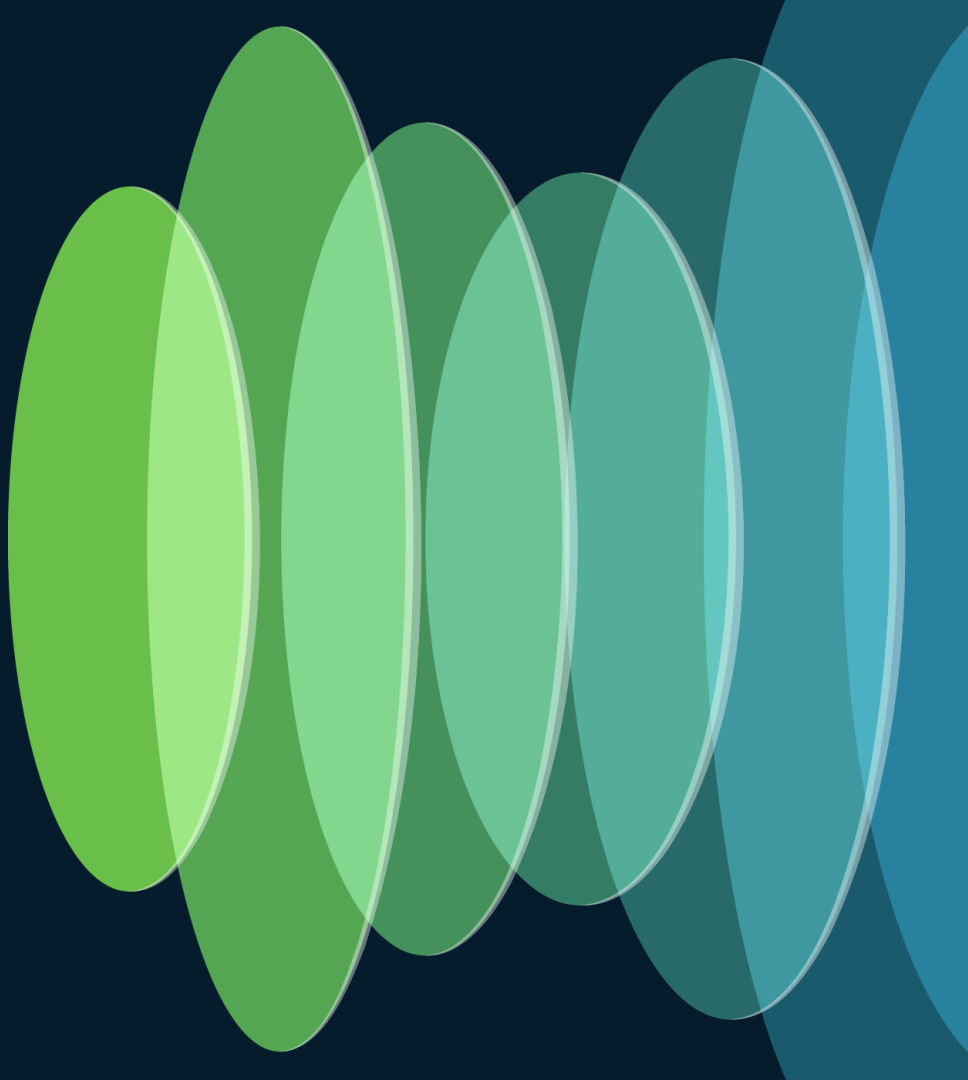
Firewall Virtual Routers



Firewall Virtual Routers



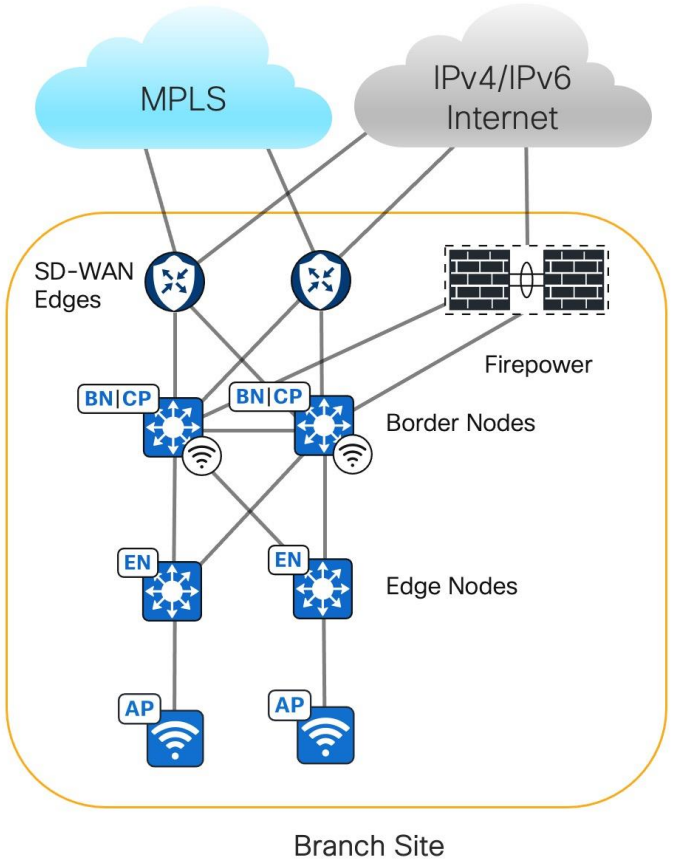
Branch Site Design



cisco Live!

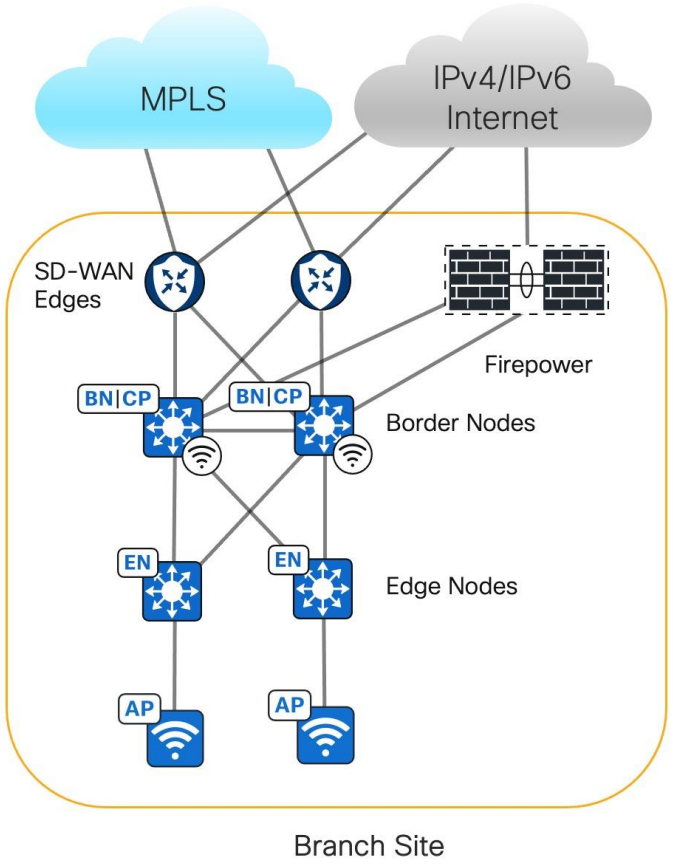
Branch Site Design

- Two SD-WAN Edges connect to the Fabric Borders
- Deploy SD-Access and SD-WAN Integration using VRF-LITE, eBGP, and Inline SGT
- The Branch site design deploys the Firepower strictly as the Internet Firewall
- Embedded Wireless on Border Nodes to manage local Access Points

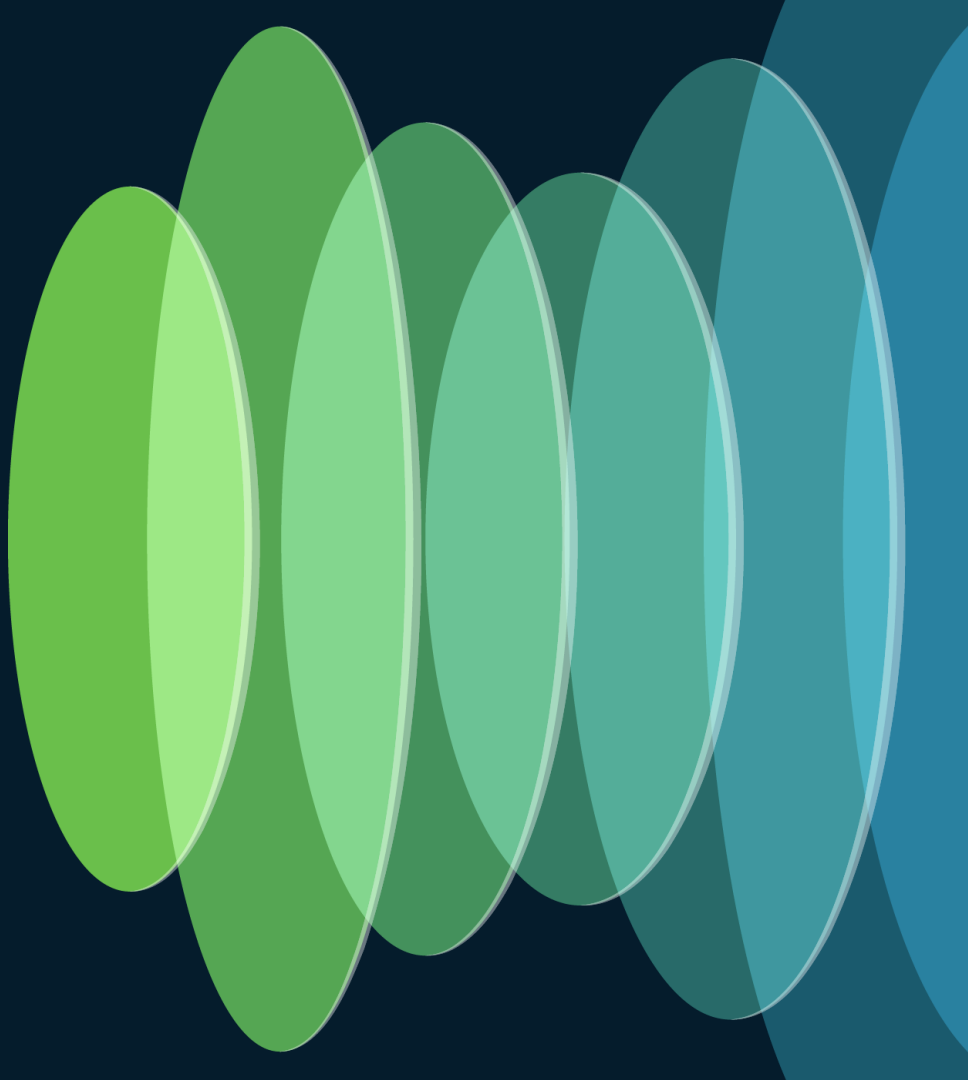


Branch Site Design

- Fabric Border VNs learn default routes from Internet Firewall
- Apply route filter to deny default routes to SD-WAN Edge to prevent this site from becoming transit for Internet traffic

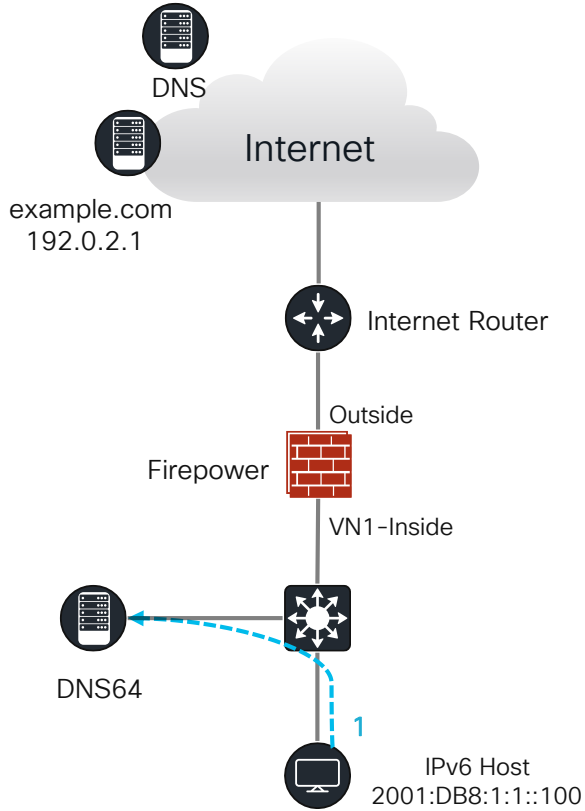


DNS64 and NAT64



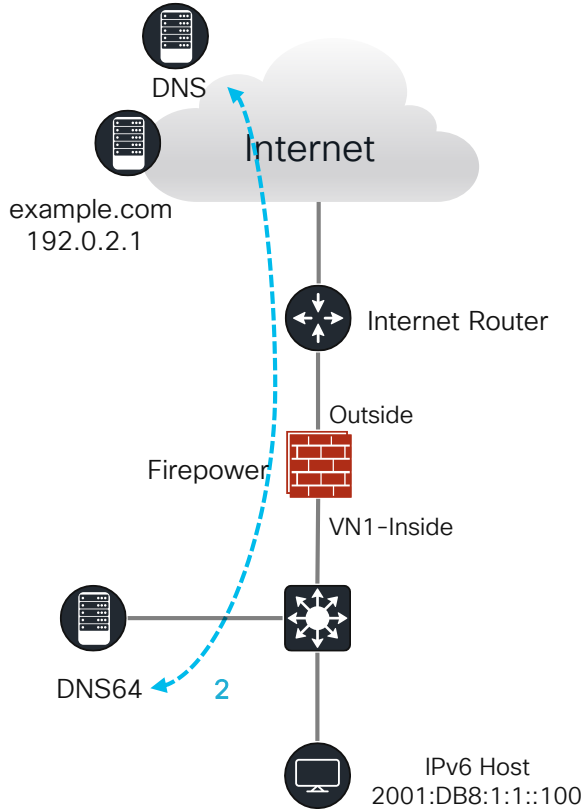
DNS64

1. IPv6-only Client sends AAAA query for example.com



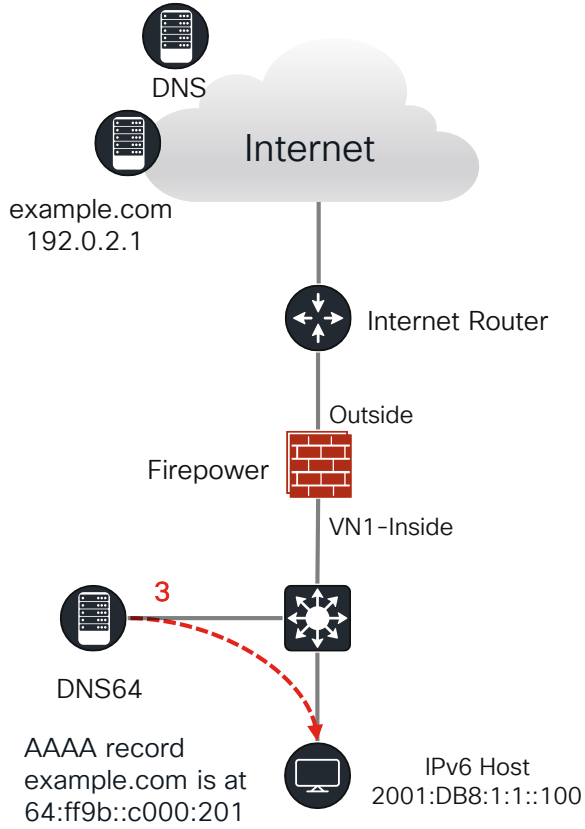
DNS64

2. DNS64 server sends AAAA query to the authoritative name server for example.com. If it receives empty AAAA record in response, it will send A query. The name server responds with A record 192.0.2.1



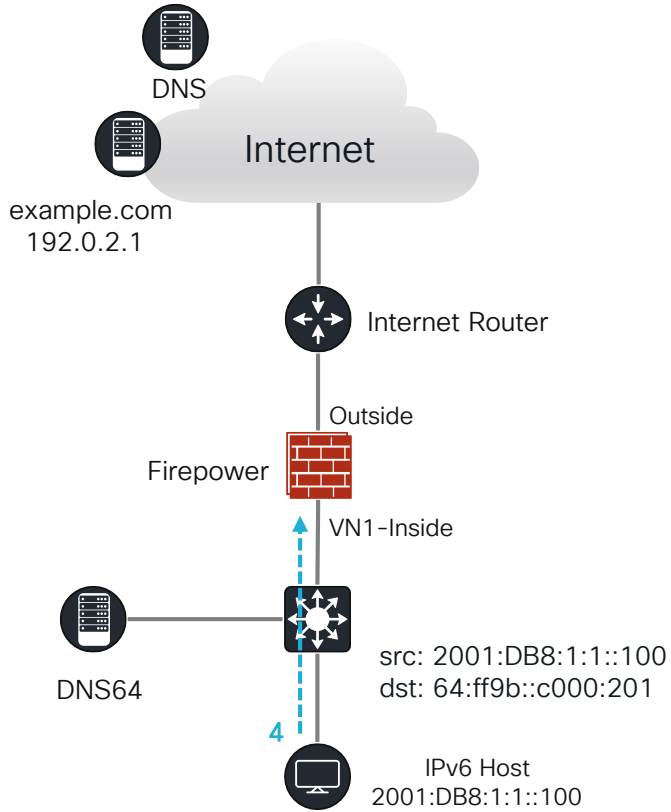
DNS64

3. DNS64 returns a synthetic AAAA record with IPv6 address of NAT64 Well-Known Prefix (64:ff9b::/96) embedded with original 32-bit IPv4 address of the A Record



NAT64

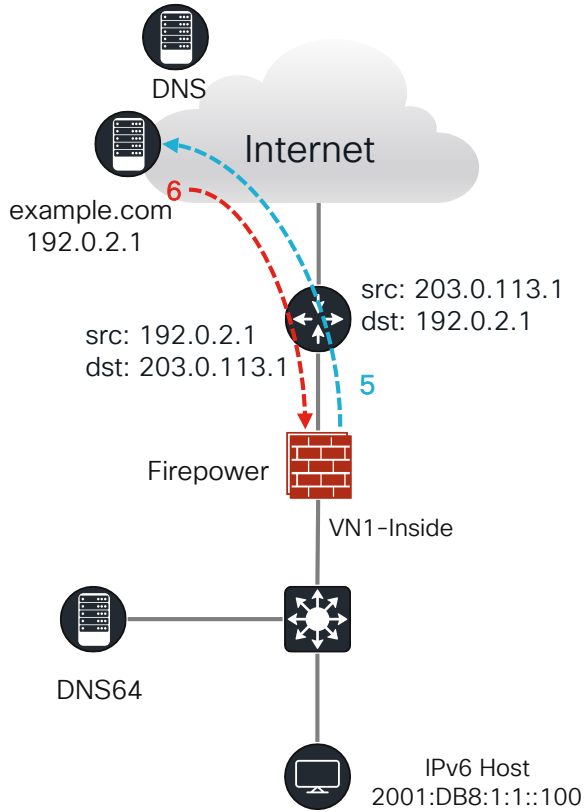
4. Client sends IPv6 packet to synthetic IPv6 address of web server, which is routed to Firewall



NAT64

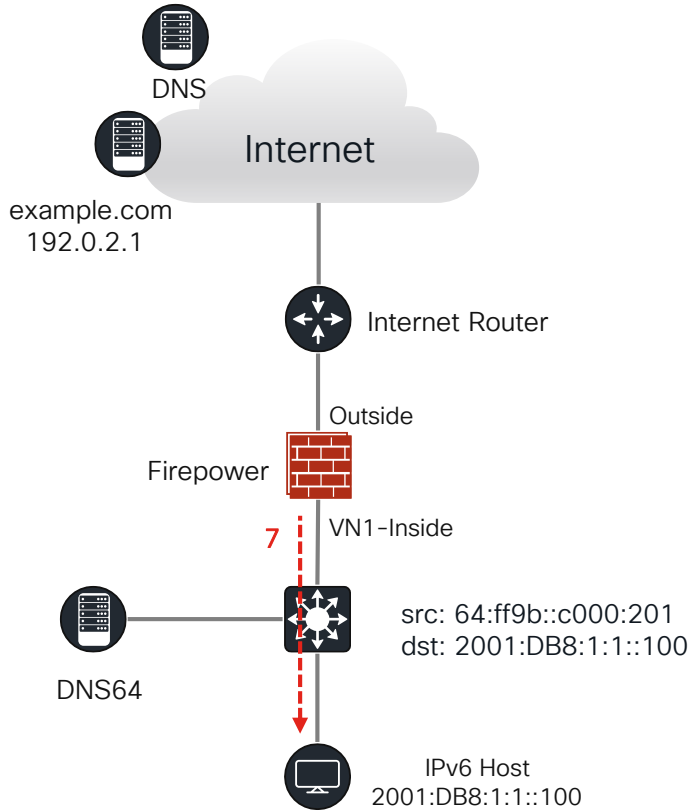
5. Firewall translates source and destination IPv6 addresses to IPv4 addresses and sends packets to the web server

6. IPv4 web server replies over IPv4 to the Firewall



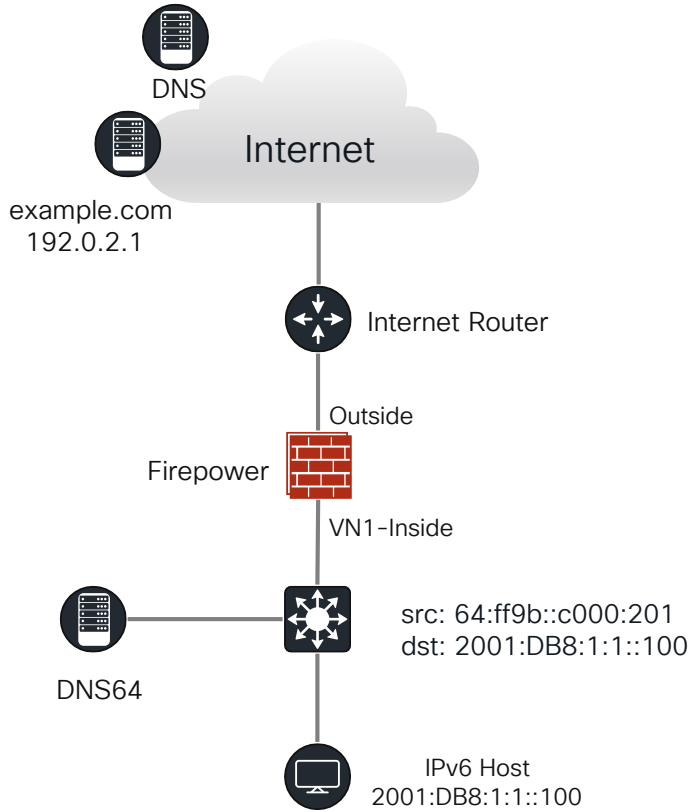
NAT64

7. Firewall translates IPv4 to IPv6 and sends it to IPv6 client



NAT64 on Firepower

- NAT64 has 2 components:
  - Source NAT: Perform dynamic NAT of Source IPv6 address to a public IPv4 address or pool of public IPv4 addresses
  - Destination NAT: Perform static NAT for Any IPv4 address to NAT64-prefix. Entire 32-bit IPv4 Internet address space maps to 32-bit /96 IPv6 address space
  - Example: Synthetic IPv6 address = 64:ff9b::c000:201
  - NAT64-prefix = 64:ff9b::/96
  - c000:201 converts to 192.0.2.1



NAT64 on Firepower

Example Firepower Manual NAT64 Configuration:

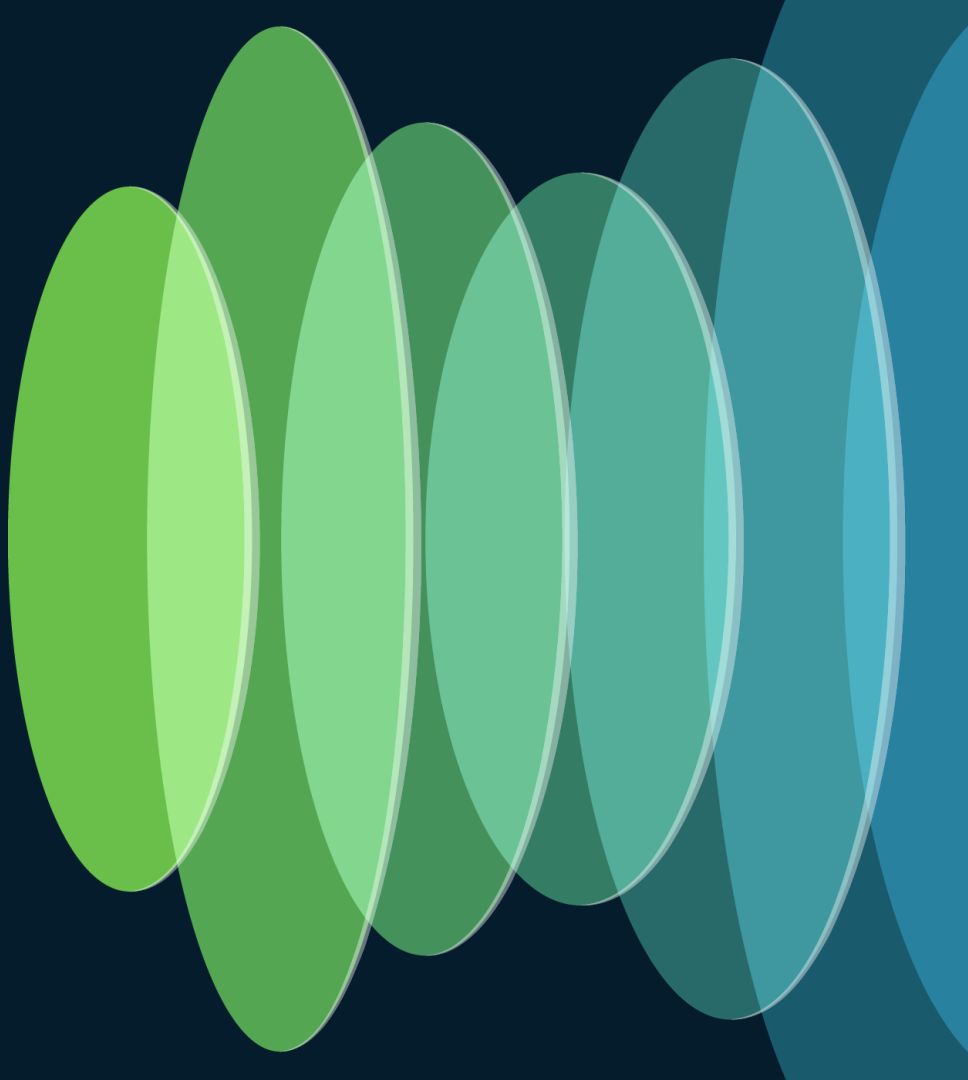
```
###IPv6 Client Network###
object network ipv6_client_net
 subnet 2001:DB8:2:1::/64

###NAT64-Prefix###
object network 4_mapped_to_6
 subnet 64:ff9b::/96

###Any IPv4 Network###
object network any_IPv4
 subnet 0.0.0.0 0.0.0.0

nat (VN1-Inside,Outside) source dynamic ipv6_client_net interface destination
static 4_mapped_to_6 any_IPv4
```

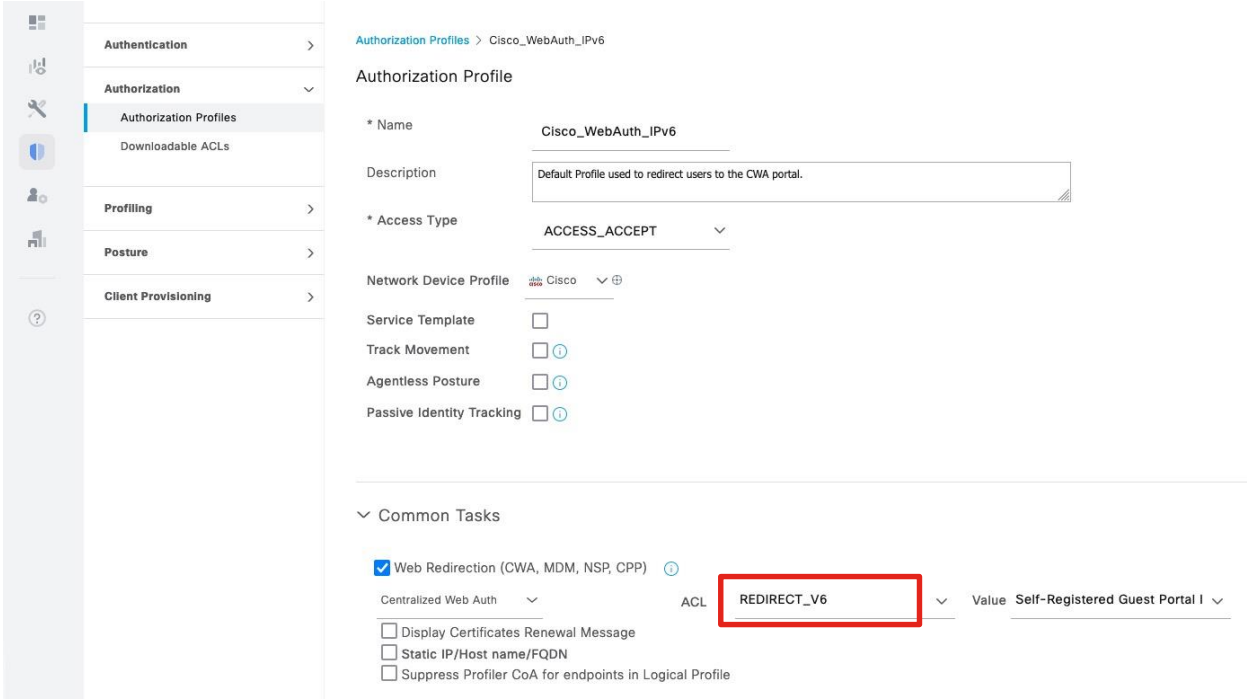
IPv6 Wireless Guest



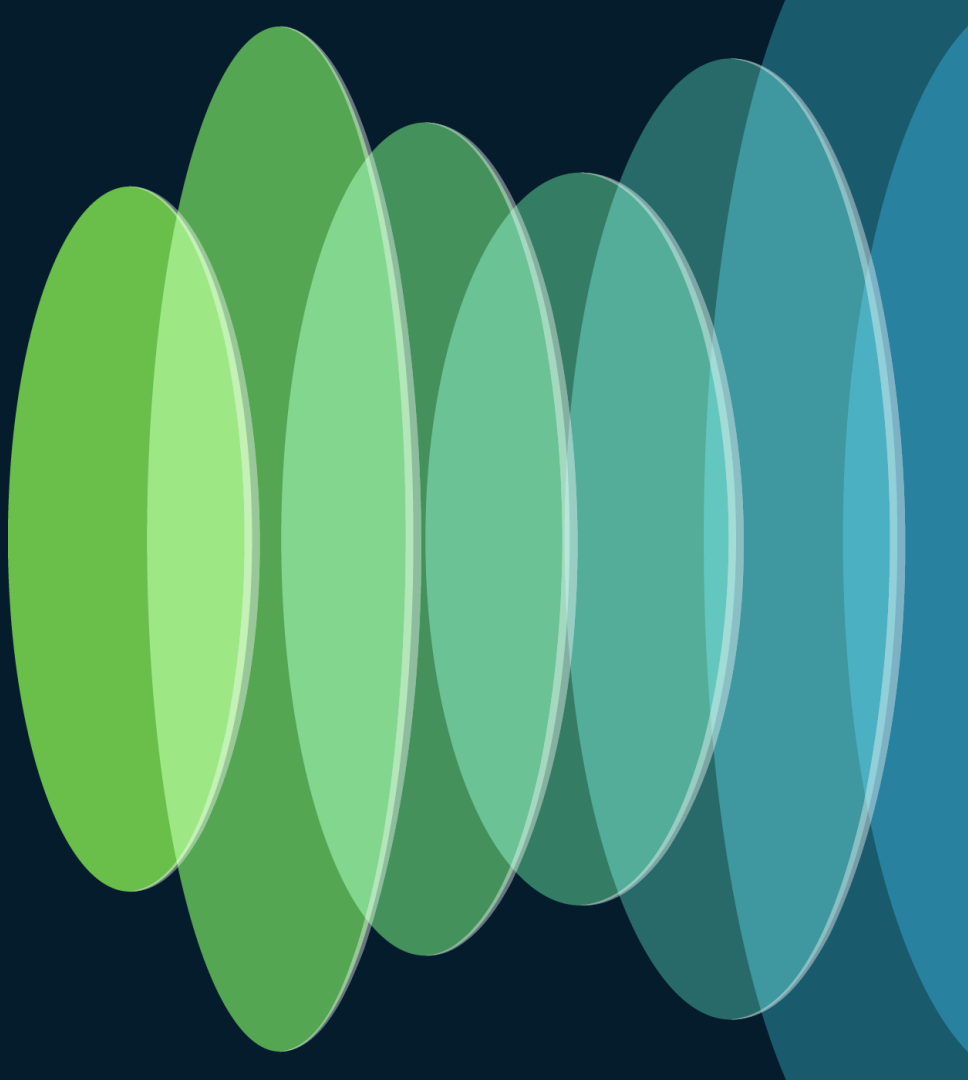
cisco Live!

IPv6 Wireless Guest – Central Web Authentication

- To enable Fabric Enabled Wireless for IPv6 Guests CWA
  - ISE 3.3 introduces support for IPv6 Guest Portal
  - Catalyst 9800 – IOS-XE 17.15 onwards
  - IPv6 Redirect ACL is manually configured on the WLC
  - In Authorization profile used in Guest Authorization policy, the ACL points to the name of IPv6 Redirect ACL that's manually configured on the WLC



IPv6 Integration with Traditional Campus Deployment

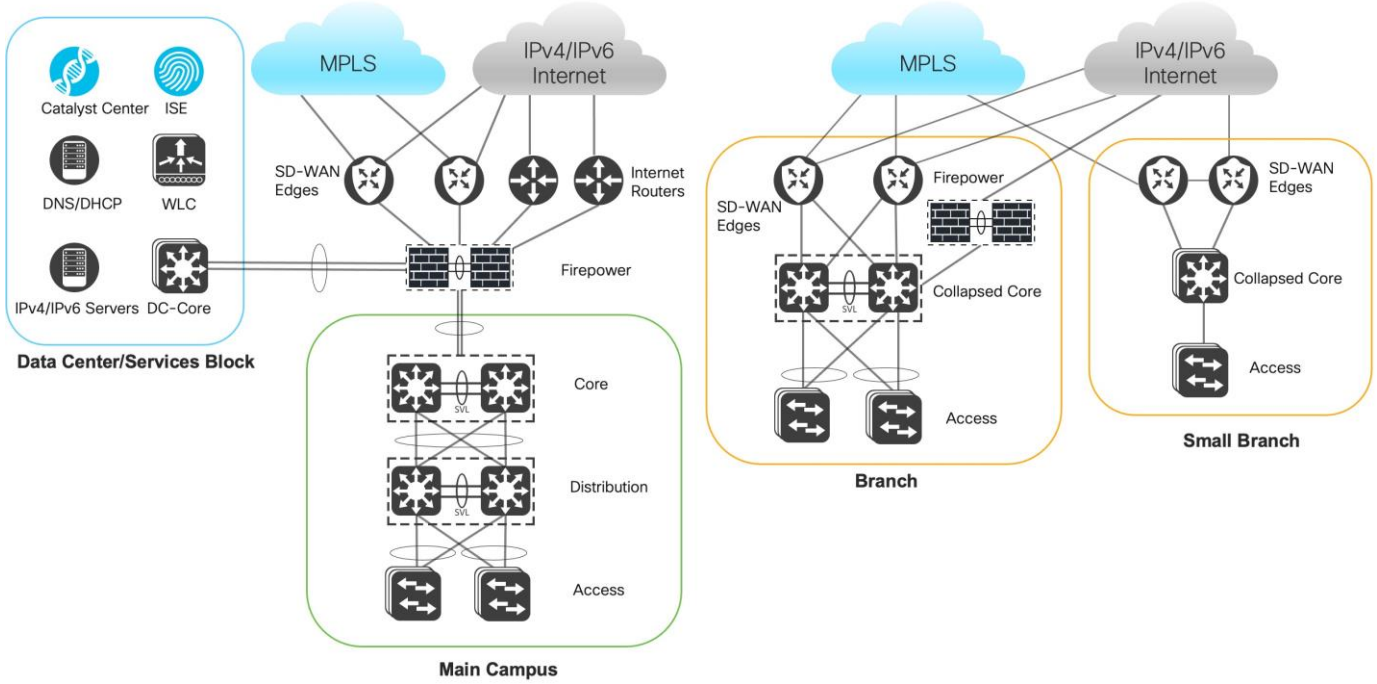


cisco Live!

Traditional Campus IPv6 Deployment

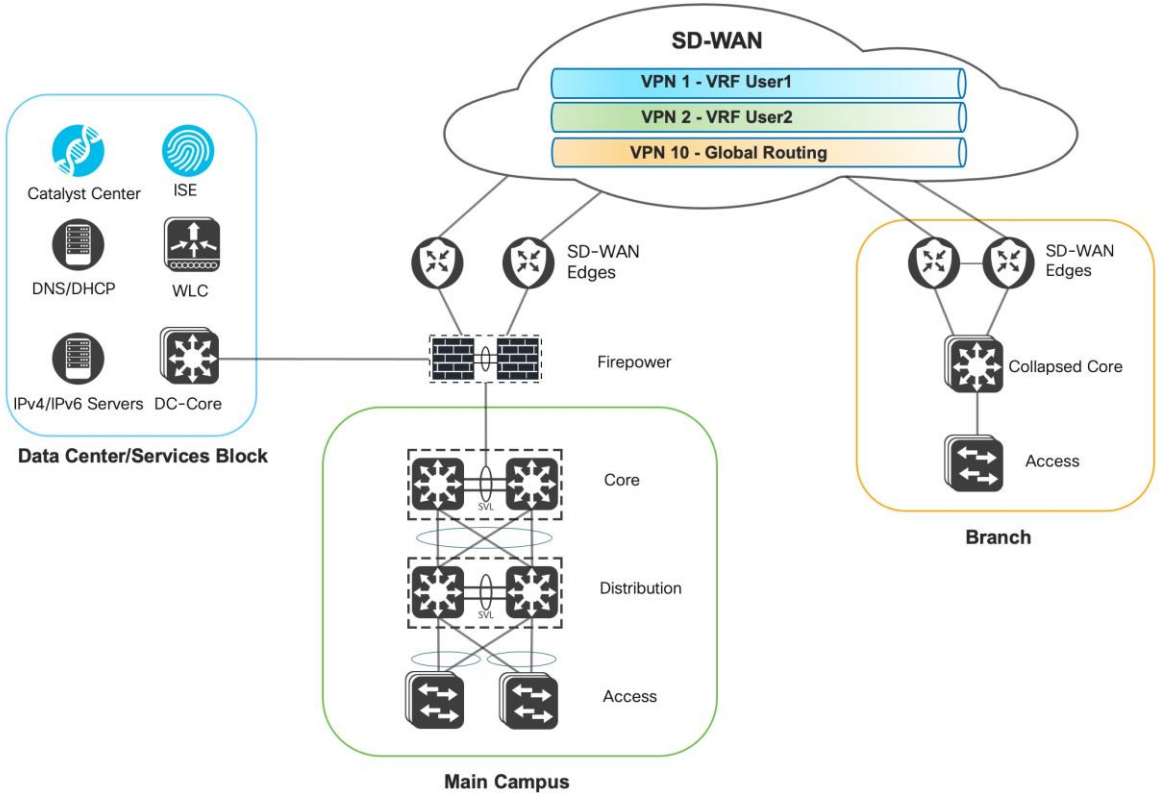
Highlights

- Traditional Campus + SD-WAN + Firepower
- SD-WAN and Firepower deployments remain the same
- Deploy Traditional 3 Tier Architecture of core, distribution, access
- Use IPv6 Transport for networking management communications
- WLC in Datacenter manages all access points



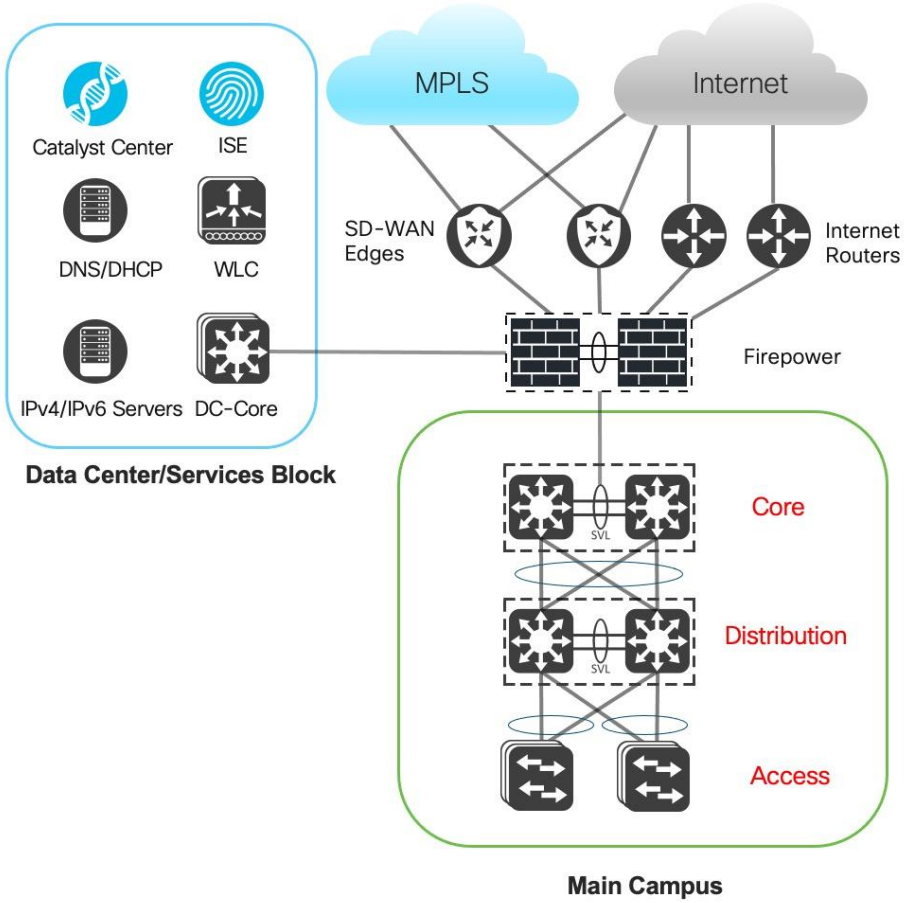
Routing Across SD-WAN

- Dedicated VPN (i.e. VPN10) for carrying global routing traffic
- Other VPNs used for carrying USER VRF traffic



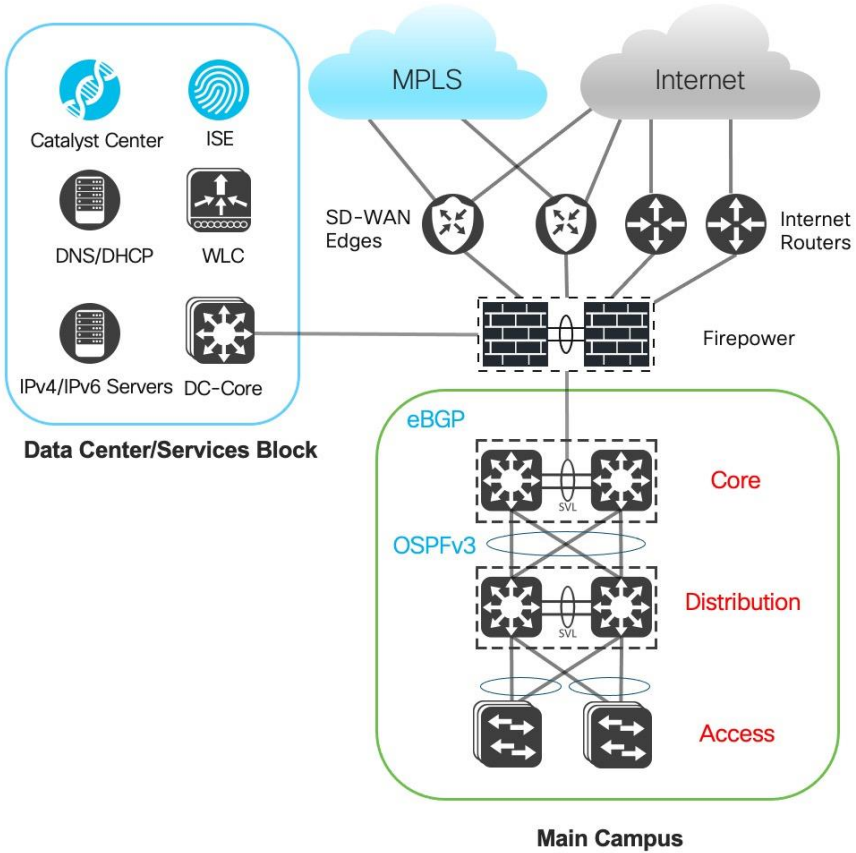
Main Campus

- Deploy Traditional 3 Tier Architecture of core, distribution, access
  - Core and Distribution uses Switch Virtual Link(SVL)
    - Multi-chassis EtherChannel
    - No need for First Hop Redundancy Protocol
- Use IPv6 global routing to carry network management communications
  - RADIUS, TACACS, SNMP, CAPWAP, NetFlow, etc
- Multi-VRF environment using VRF-LITE



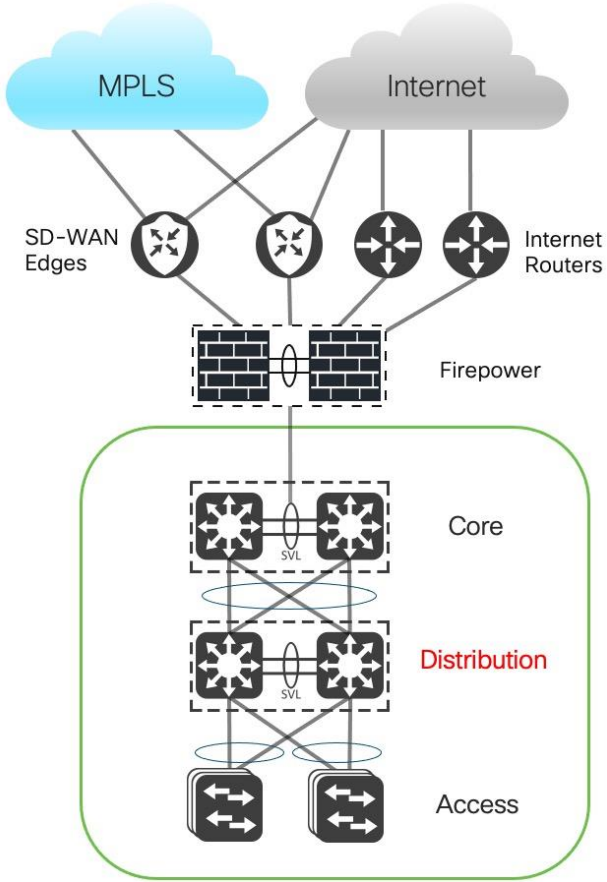
Main Campus – Routing

- Connections between switches are configured as trunks
- Use Switch Virtual Interfaces (SVIs) as transit layer 3 links in global and VRF
- Routing Protocols
  - Between Firepower and Core: BGPv6 in global and VRF
  - Between Core and Distribution: OSPFv3 for IPv6 address families in global and VRF



Main Campus – Distribution

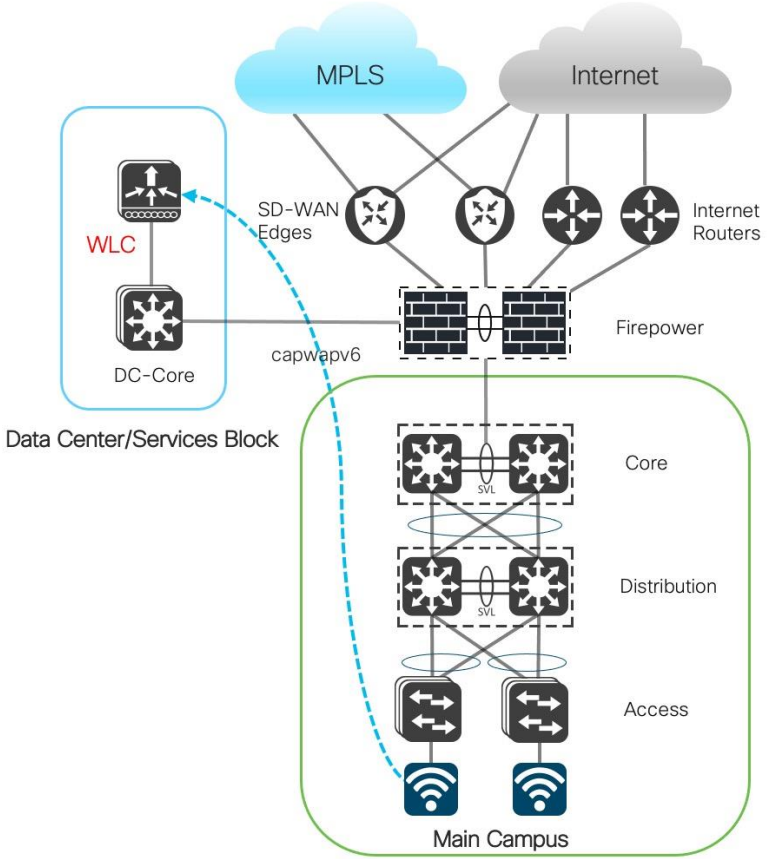
- Distribution switch provides SVI Gateway for user traffic
  - SLAAC only
    - IPv6 Router provides IPv6 prefix in router advertisement and relies on clients to derive IPv6 address
    - Recursive DNS Server (RDNSS) option can be defined
      ipv6 nd ra dns server 2001:DB8:160::161
  - Stateful DHCPv6
    - DHCPv6 server provides IPv6 address
    - DHCPv6 server provides other options (i.e. dns-server)
      ipv6 nd prefix 2001:DB8:11:1031::/64 no-autoconfig
      ipv6 nd managed-config-flag
      ipv6 nd other-config-flag
      ipv6 dhcp relay destination 2001:DB8:160::161
  - Stateless DHCPv6
    - Other options (i.e. dns-server) obtained via DHCPv6
      ipv6 nd other-config-flag



Main Campus

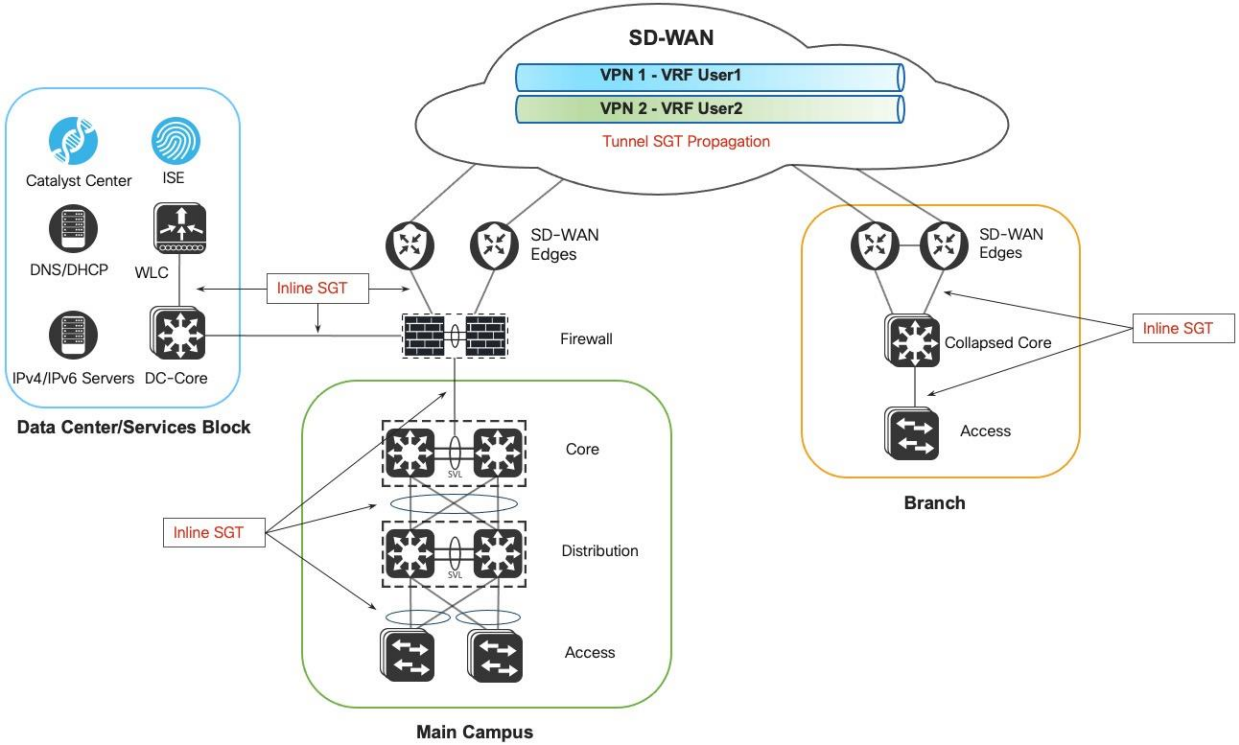
Main Campus – Wireless

- Access Points use DHCPv6 option 52 to find WLC IPv6 address and form capwapv6 tunnel
- Corporate WLAN using Dot1x authentication
- Guest WLAN using Central Web Authentication
- A WLAN is bridged to a VLAN
- DC-Core SW provides SVI Gateway service to WLAN

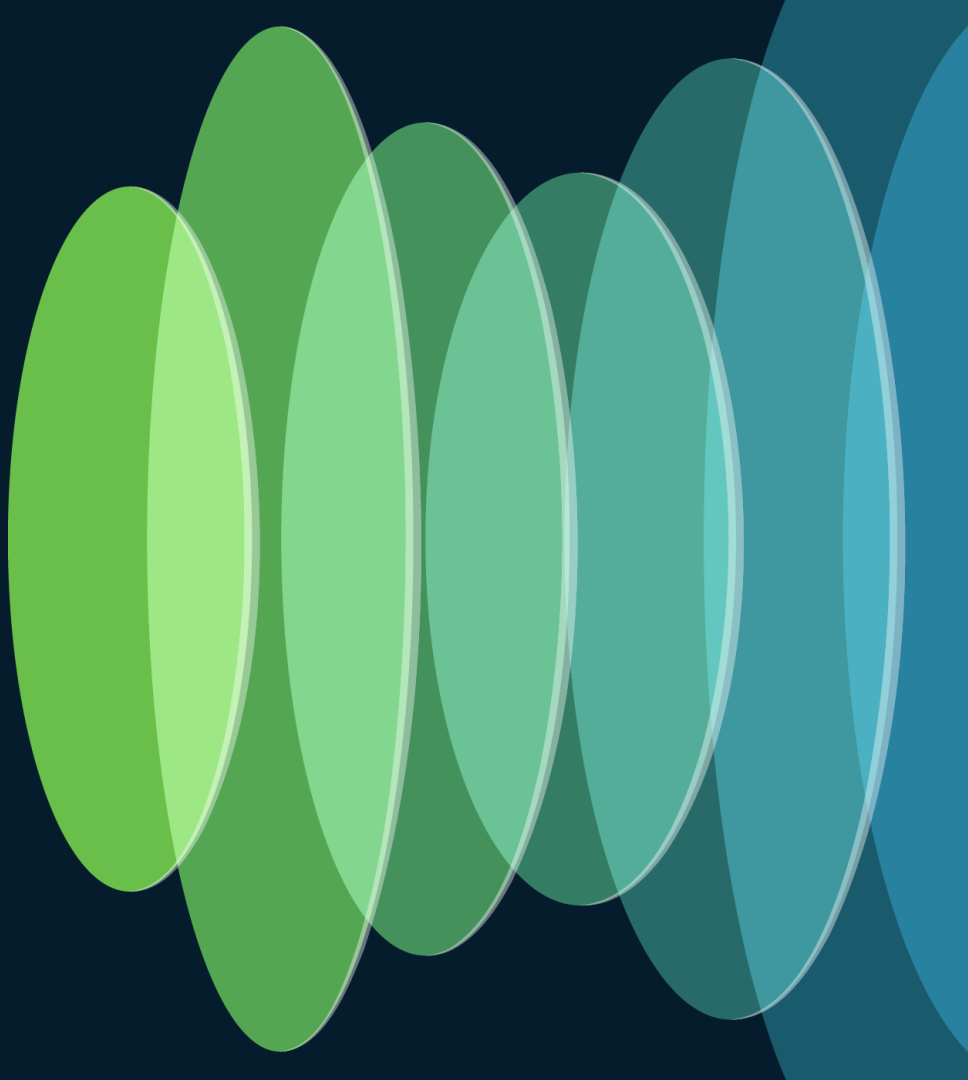


Main Campus – Cisco TrustSec Domain

- Enable Inline SGT
- Enable SGT Propagation across SD-WAN tunnel



Additional Learning



Cisco Validated Profiles

- IPv6 Integration with Cisco SD-Access, SD-WAN, and Firepower
  - https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/Cisco-Validated-Solution-Profiles/b_cisco_validated_solution_ipv6.html
- IPv6 Traditional Campus Integration with Cisco SD-WAN and Cisco Firepower
  - To be published soon!

Cisco Live US IPv6 Learning Map

Sunday–2nd

TECXAR-2000 9AM
Integrating IPv6 Services with SD-WAN

TECIPV-2000 9AM
IPv6 in the Host and in the Local Network

TECIPV-2001 2PM
IPv6 Beyond the Local Network

TECMPL-2119 2PM
SRv6 Tech Update: Use Cases and Operations

Monday–3rd

BRKIPV-2191 8:30AM
IPv6:: It's Happening!

BRKENT-2109 10:30AM
Let's Deploy IPv6 Now

BRKMPL-2203 10:30AM
Introduction to SRv6 uSID Technology

BRKENS-2834 11:00AM
IPv6-Enabled Wireless (Wi-Fi) Access: Design and Deployment Strategies

BRKIPV-1616 1PM
IPv6 – What Do You Mean There Isn't a Broadcast?

BRKENT-3002 1PM
IPv6 Security in the Local Area with First Hop Security

IBOENT-2811 2:30PM
Everything You Wanted to Know about IPv6 but Were Afraid to Ask

Tuesday–4th

IBOIPV-1000 10:30AM
U.S. Government Mandate Driving to 50% IPv6-Only and beyond in 2024

BRKENT-3340 1PM
The Hitchhiker's Guide to Troubleshooting IPv6

BRKENT-2008 2:30PM
Goodbye Legacy, the Move to an IPv6-Only Enterprise

BRKIPV-2418 3PM
Deploying IPv6 Routing Protocols: Specifics and Considerations

Wednesday–5th

CTF-1001 10:15AM
IPv6: The Internet's best kept secret!

IBOIPV-1428 2:30PM
IPv6 Unleashed: Cisco Meraki Cutting-Edge Design Session

Thursday–6th

BRKIPV-2015 8:00AM
Integrating Cisco Campus, SD-WAN and Firepower in IPv6 Enterprise Networks

BRKSEC-2044 9:30AM
Secure Operations for an IPv6 Network

IBOIPV-2000 1PM
Sharing Experience on IPv6 Deployments

Walk in Labs

LABIPV-1639	IPv6 Foundations: A Dive into Basic Networking Concepts
LABIPV-2640	IPv6 Deep Dive: Beyond Basics to Brilliance
LABMPL-1201	SRv6 Basics
LABSP-2129	SRv6 Micro-Segment Basics
LABSP-3393	Implementing Segment Routing v6 (SRv6) Transport on NCS 55xx/5xx and Cisco 8000: Advanced

Instructor-led Labs

LTRENT-2016	Learning IPv6 in the Enterprise for Fun and (Fake) Profit: A Hands-On Lab
LTRSPG-2212	SRv6 and Cloud-Native: A Platform for Network Service Innovation
LTRSPG-2006	Explore the Power of SRv6: Unleashing the Potential of Next-Generation Networking

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: witsang@cisco.com

Complete Your Session Evaluations

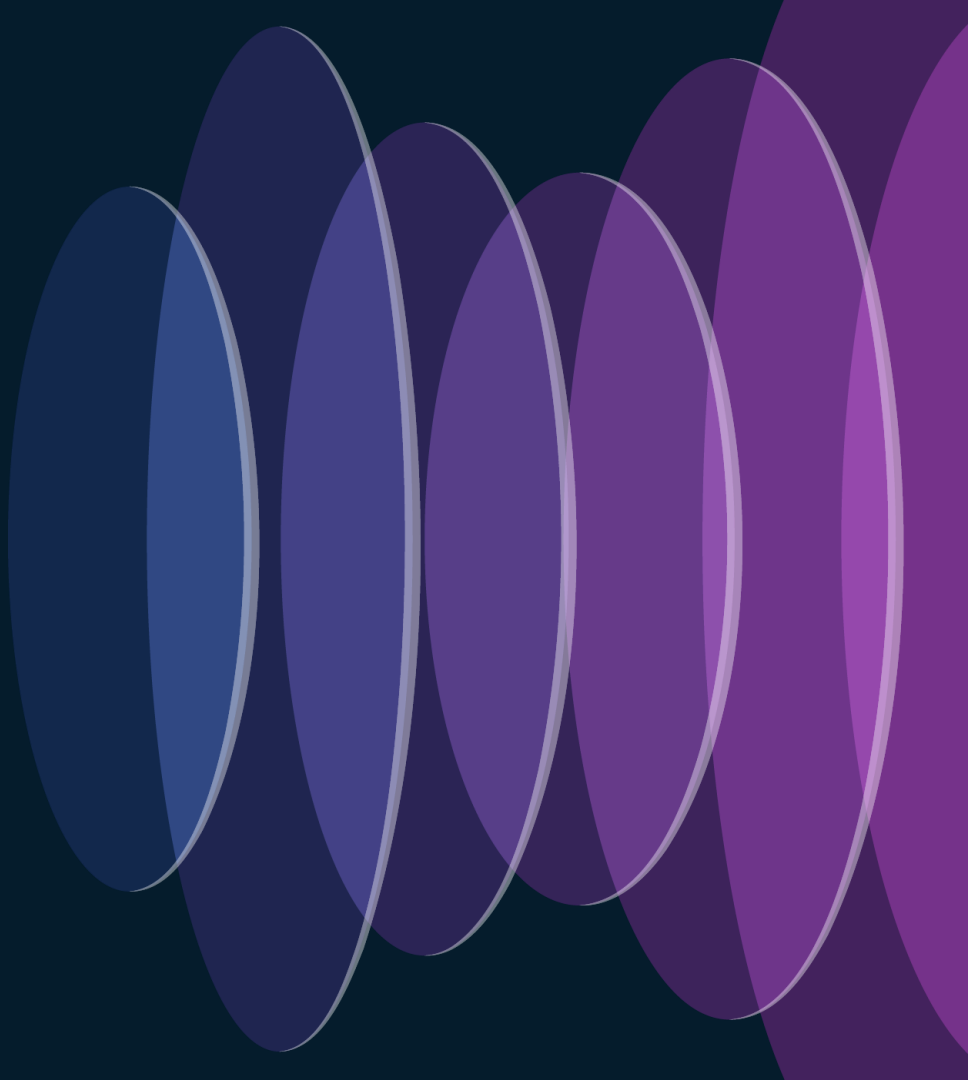
Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

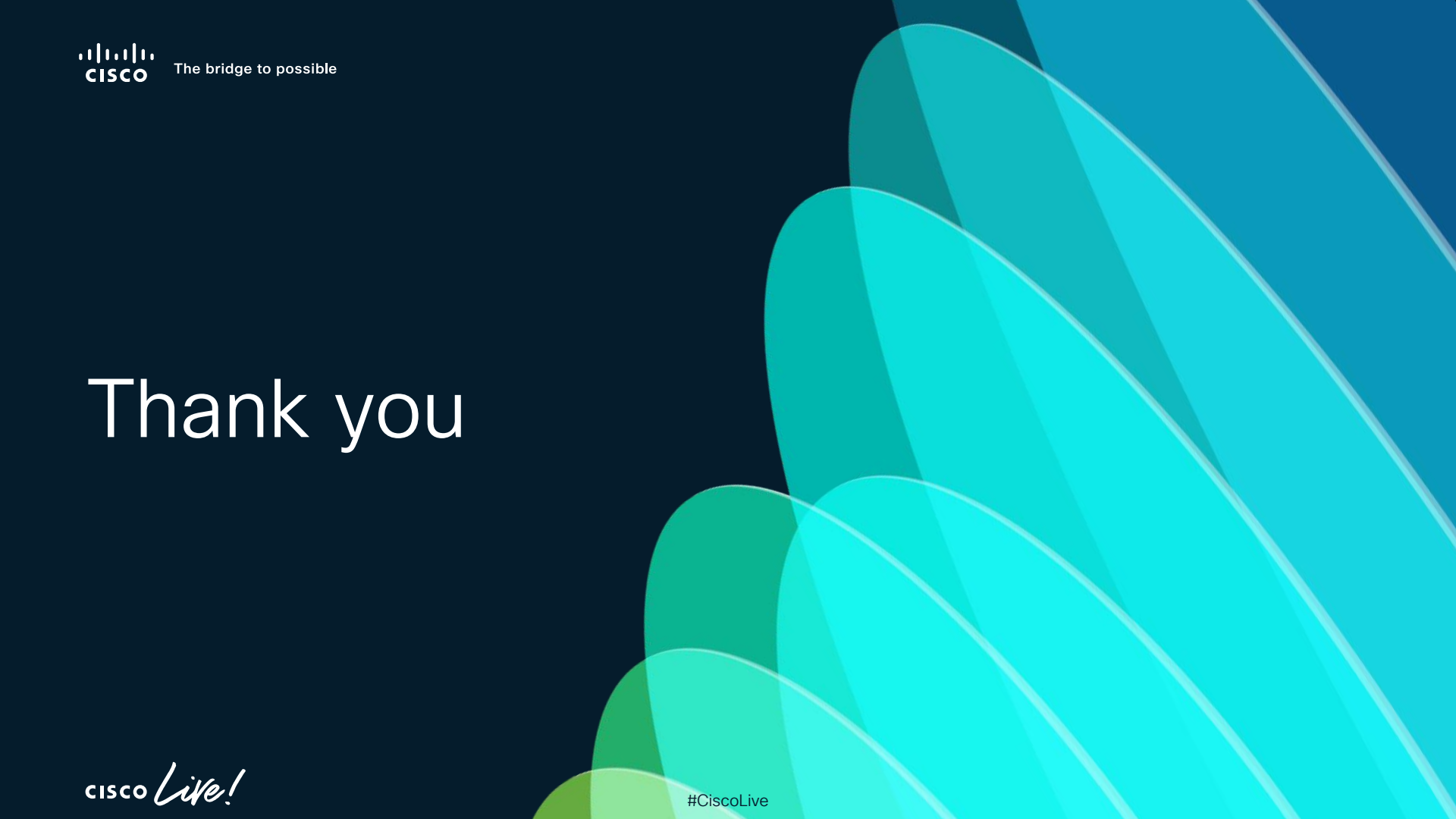
Complete your surveys in the **Cisco Live mobile app.**

Conclusion



Key Takeaways

- Explored two approaches to deploying IPv6 networks
  - Cisco SD-Access, SD-WAN, and Firepower
  - Cisco Traditional Campus, SD-WAN, and Firepower
- We have provided a framework you can use to deploy IPv6 networks
- Let’s plan to deploy IPv6 today!


The bridge to possible
Thank you
cisco Live!
#CiscoLive