ARCEP/IDATE

Table ronde IPv6

Fayçal HADJ MOHAMED
IOT/IPv6 Solution Architect
Decembre 2023

IPv6 …
…pour garantir l’expérience utilisateur !!

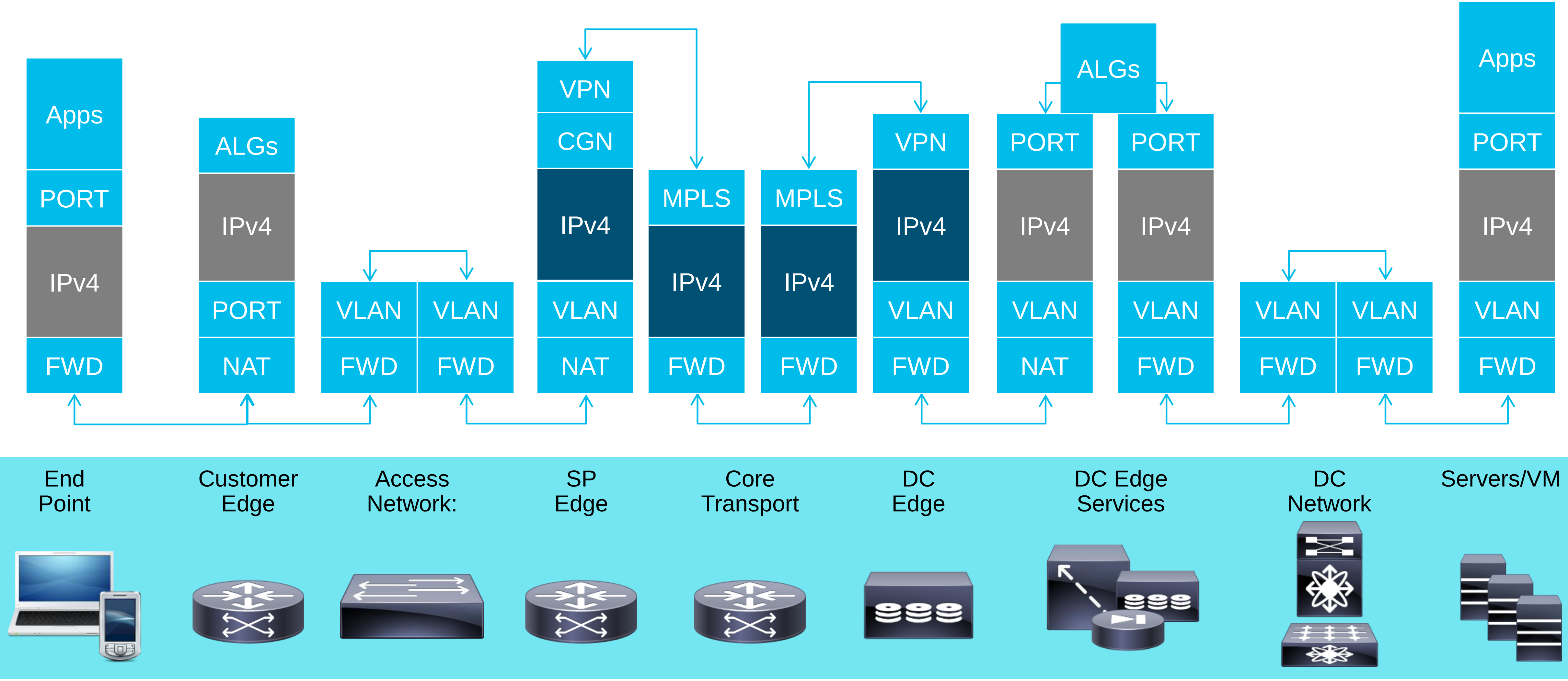
The World Today

Client OS	Enterprise Network	ISP	Internet
✓	✗	✓	✓

IPv6 adoption

- Why ?

IPv4 Complexity



Apps
PORT
IPv4
FWD

ALGs
IPv4
PORT
NAT

VLAN
FWD

VLAN
FWD

VPN
CGN
IPv4
VLAN
NAT

MPLS
IPv4
FWD

MPLS
IPv4
FWD

VPN
IPv4
VLAN
FWD

ALGs

PORT
IPv4
VLAN
NAT

PORT
IPv4
VLAN
FWD

VLAN
FWD

VLAN
FWD

Apps
PORT
IPv4
VLAN
FWD

End Point

Customer Edge

Access Network:

SP Edge

Core Transport

DC Edge

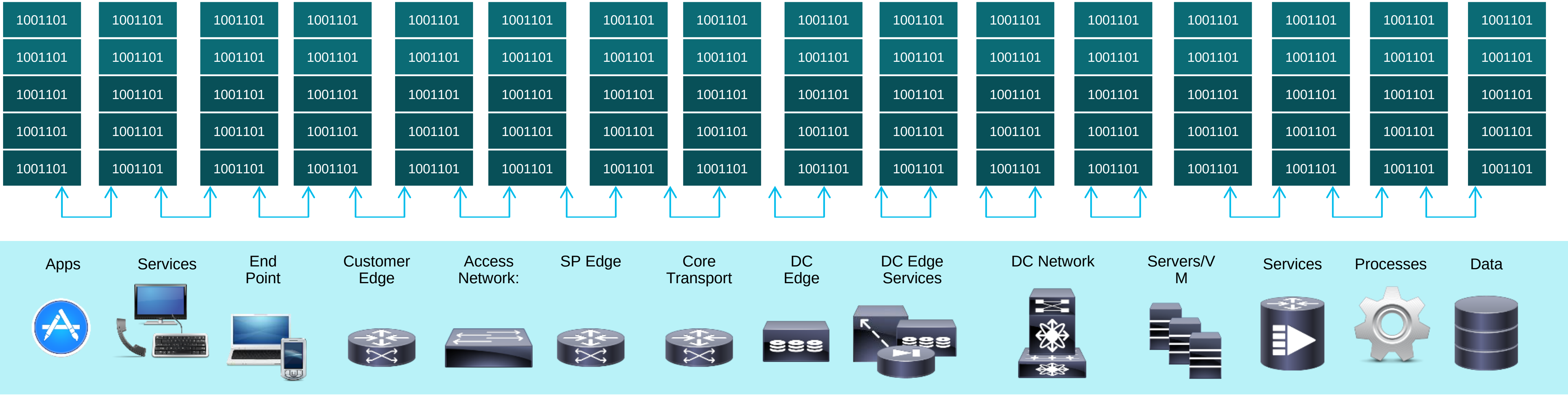
DC Edge Services

DC Network

Servers/VM

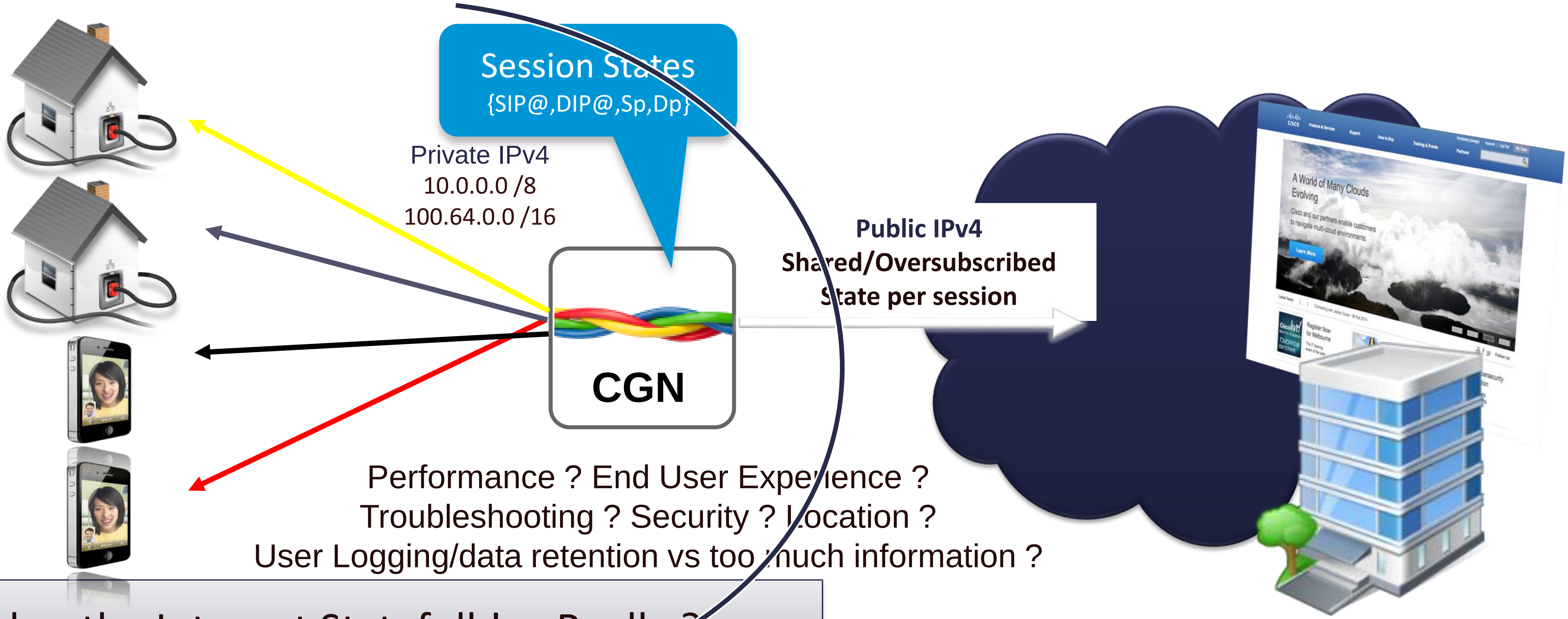
IPv6-Centric Networking – Simplicity & Opportunity

Creating a global conduit of shared information touching applications, services, networks, processes, data…



1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101
1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101
1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101
1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101
1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101	1001101

Carrier Grade NAT: Sharing public IPv4 addresses



Session States
{SIP@,DIP@,Sp,Dp}

Private IPv4
10.0.0.0 /8
100.64.0.0 /16

CGN

Public IPv4
Shared/Oversubscribed
State per session

Performance ? End User Experience ?
Troubleshooting ? Security ? Location ?
User Logging/data retention vs too much information ?

Makes the Internet Statefull ! … Really ?

IPv6 deployment

- Cisco Methodology

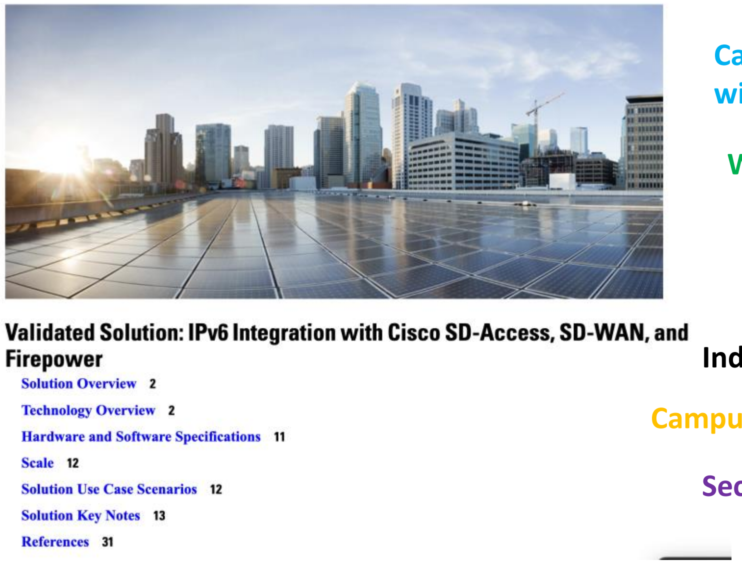
Cisco Validated Design (CVD) & Validated profiles (CVP)

Updated: November 14, 2023

- Validated Solution: 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

The objective is to enable IPv6-only clients while keeping the underlay infrastructure dual stack during transition. Migrating to a single-stack IPv6 architecture for both overlay and underlay will be performed when an end-to-end, IPv6-only environment is fully supported.

33 pages



Validated Solution: IPv6 Integration with Cisco SD-Access, SD-WAN, and Firepower

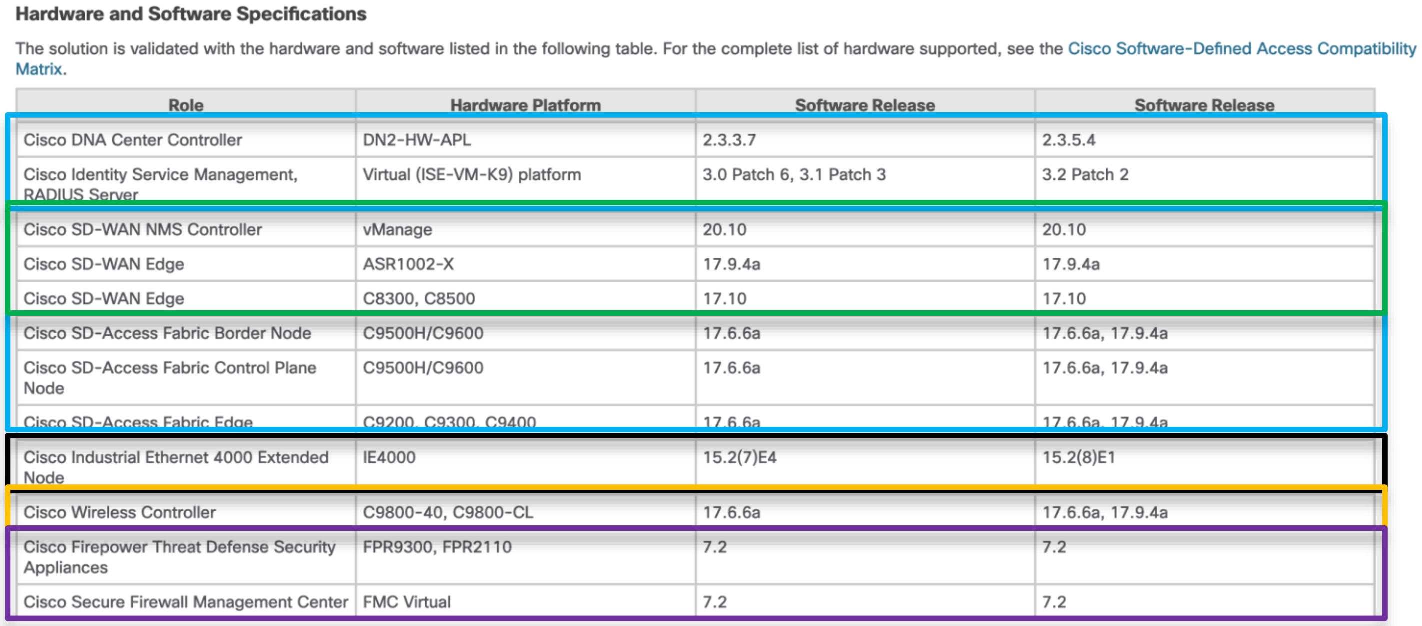
Campus wired

Wan

Industrial

Campus Wifi

Security



Hardware and Software Specifications

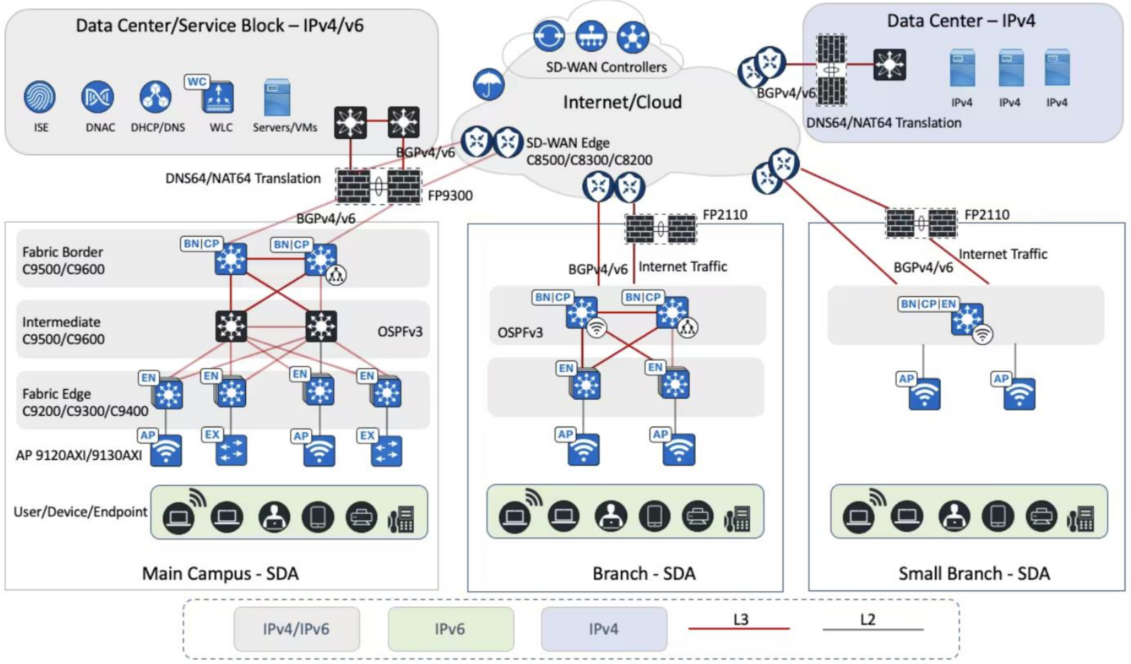
The solution is validated with the hardware and software listed in the following table. For the complete list of hardware supported, see the Cisco Software-Defined Access Compatibility Matrix.

Role	Hardware Platform	Software Release	Software Release
Cisco DNA Center Controller	DN2-HW-APL	2.3.3.7	2.3.5.4
Cisco Identity Service Management, RADIUS Server	Virtual (ISE-VM-K9) platform	3.0 Patch 6, 3.1 Patch 3	3.2 Patch 2
Cisco SD-WAN NMS Controller	vManage	20.10	20.10
Cisco SD-WAN Edge	ASR1002-X	17.9.4a	17.9.4a
Cisco SD-WAN Edge	C8300, C8500	17.10	17.10
Cisco SD-Access Fabric Border Node	C9500H/C9600	17.6.6a	17.6.6a, 17.9.4a
Cisco SD-Access Fabric Control Plane Node	C9500H/C9600	17.6.6a	17.6.6a, 17.9.4a
Cisco SD-Access Fabric Edge	C9200, C9300, C9400	17.6.6a	17.6.6a, 17.9.4a
Cisco Industrial Ethernet 4000 Extended Node	IE4000	15.2(7)E4	15.2(8)E1
Cisco Wireless Controller	C9800-40, C9800-CL	17.6.6a	17.6.6a, 17.9.4a
Cisco Firepower Threat Defense Security Appliances	FPR9300, FPR2110	7.2	7.2
Cisco Secure Firewall Management Center	FMC Virtual	7.2	7.2

Cisco Validated Design (CVD) & Validated profiles (CVP)

- **IPv6 in Cisco SD-Access (Campus)**
  - Over time Cisco DNA Center architecture has evolved from traditional campus LAN designs to the Cisco SD-Access design architecture. Cisco SD-Access uses Cisco DNA Center to design, provision, and apply policies, as well as provide wired and wireless network assurance for an intelligent campus network. In this solution, the Cisco SD-Access fabric **underlay uses IPv4 addressing**.In the Cisco SD-Access fabric, **overlay IPv6 traffic is transported in IPv4 Virtual Extensible LAN (VXLAN) tunnels.**

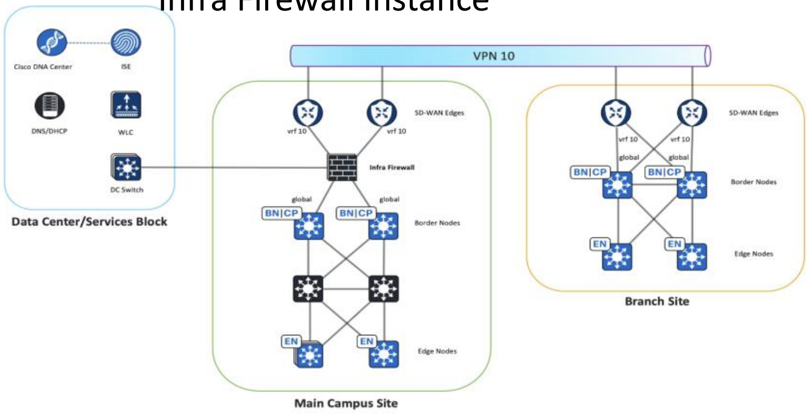
Figure 1. Solution Testbed Logical Topology



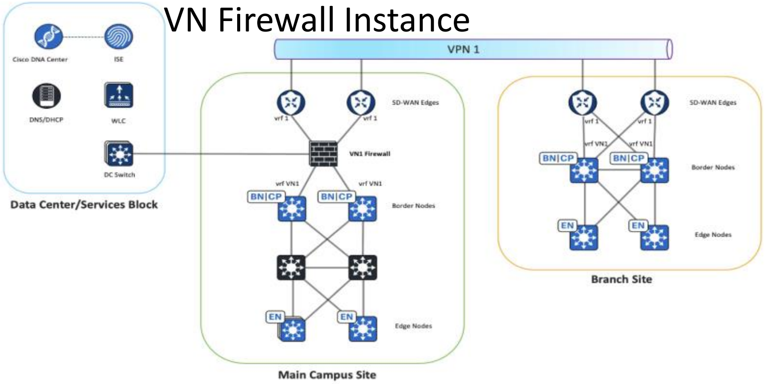
Firewall Instance Types

- At the main site, three types of firewall instances are deployed: Infra Firewall, VN Firewall, and Internet Firewall.
- The **Infra Firewall instance** provides Cisco SD-Access underlay connectivity for Cisco DNA Center to discover Cisco SD-Access fabric devices at the main site and remote branch sites.
- The **VN Firewall instance** connects the Cisco SD-Access VN to the Cisco SD-WAN VPN and provides VN connectivity to the shared-services network in the data center.
- The **Internet Firewall** instance provides internet access to the Cisco SD-Access VN hosts
  - The Internet Firewall instance receives IPv4 and IPv6 default routes from the internet router through the eBGP.
  - The Internet Firewall instance advertises IPv4 and IPv6 default routes to fabric borders through the eBGP
  - The Internet Firewall instance denies traffic between different VNs to maintain macrosegmentation
  - The Internet Firewall instance allows outbound traffic to IPv4 and IPv6 internet.
  - The Internet Firewall instance performs NAT64 function to allow IPv6 clients reachability to the IPv4 internet.

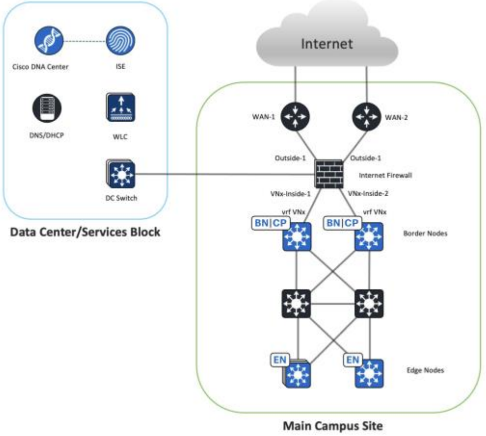
Infra Firewall Instance



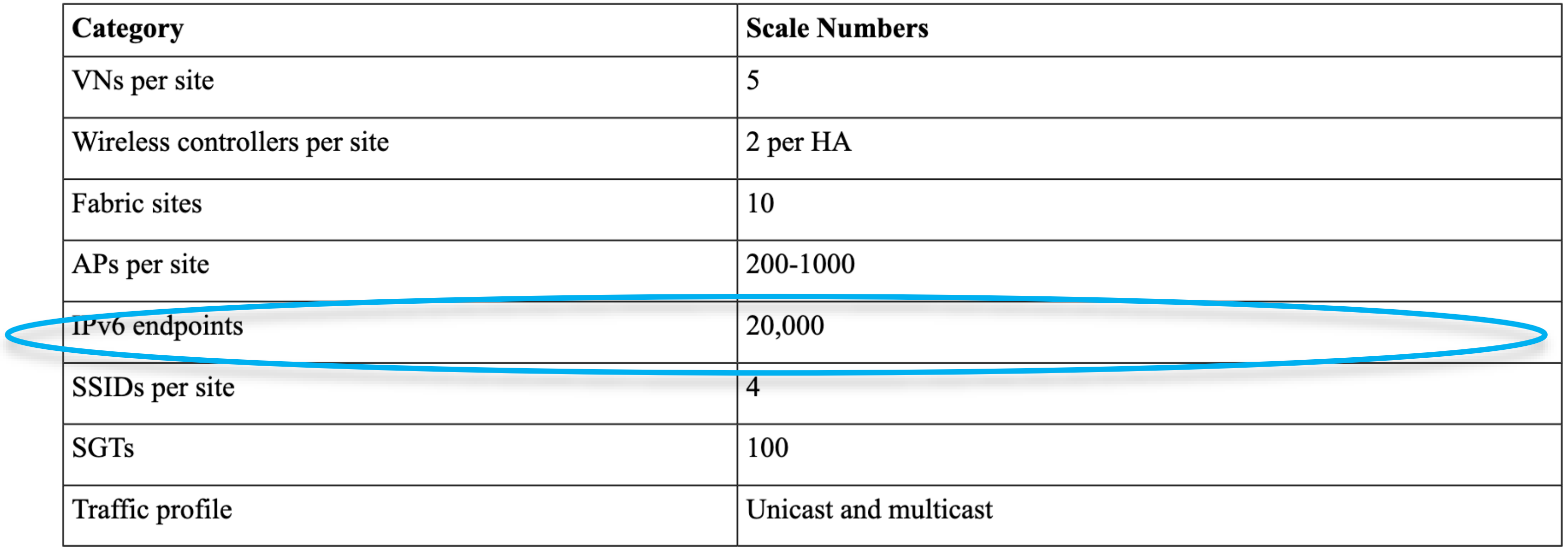
VN Firewall Instance



Internet Firewall Instance



Scale



Category	Scale Numbers
VNs per site	5
Wireless controllers per site	2 per HA
Fabric sites	10
APs per site	200-1000
IPv6 endpoints	20,000
SSIDs per site	4
SGTs	100
Traffic profile	Unicast and multicast

Use cases

- Automated secure Cisco SD-WAN transporting IPv4 and **IPv6 traffic**
- Fabric-enabled wireless deployment for **IPv6** Enterprise users
- Network visibility, monitoring, and troubleshooting for **IPv6** devices and endpoints
- **IPv6** application visibility and health
- Network robustness for **IPv6** networks
- Secure onboarding for various **IPv6-only endpoints**
- End-to-end **IPv6** traffic and secure internet access
- End-to-end inline SGT traffic enforcement between Cisco SD-Access sites across Cisco SD-WAN
- **IPv6-only clients access of IPv6 application**s and legacy IPv4 applications
- **IPv6 application performance optimization** with quality of service (QoS) and path selection
- **IPv6 endpoints** and addresses scale
- Day-n operations for the following operations: Image Upgrade, Configuration Management, Backup and Restore, and Network Expansion.