CISCO

Jak zajistit spolehlivou a bezpečnou komunikaci v multicloudovém prostředí?

Miroslav Brzek
Technical Solutions Architect
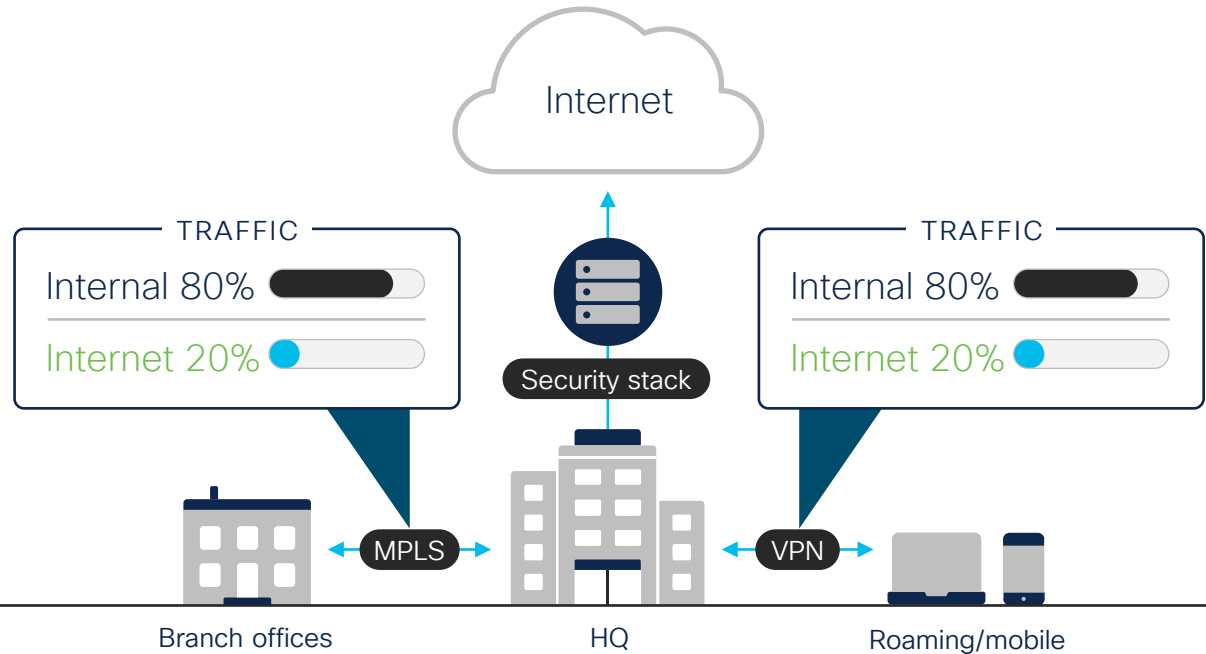
Agenda

1. Today's Security & Networking Trends

2. Cisco SASE: SD-WAN and Umbrella SIG Integration
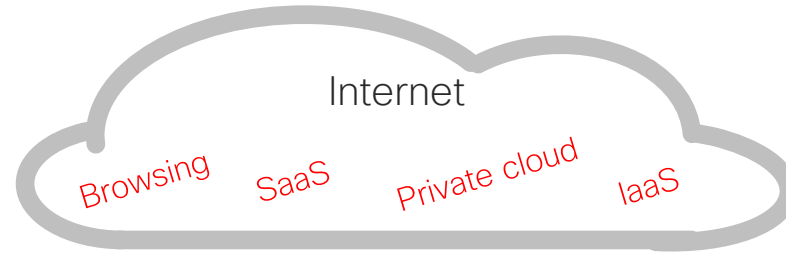
3. Catalyst 8000 Edge Platforms Family

4. Conclusion

Connecting Users to Data Center was the priority of Traditional WAN

Network:
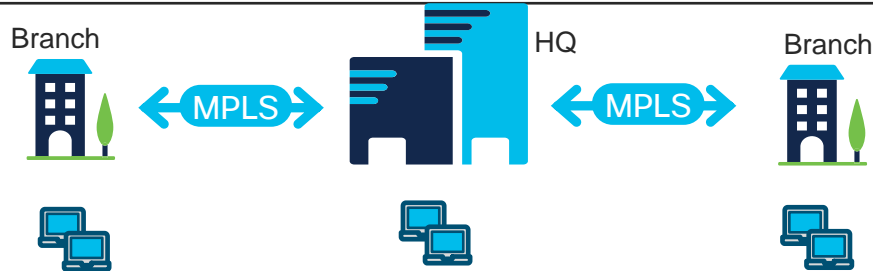Centralized

Security:
Single, on-premise
security stack

Internet

TRAFFIC
Internal 80%
Internet 20%

Security stack

TRAFFIC
Internal 80%
Internet 20%

MPLS

VPN

Branch offices

HQ

Roaming/mobile

Disruption #1 – Cloud App Proliferation
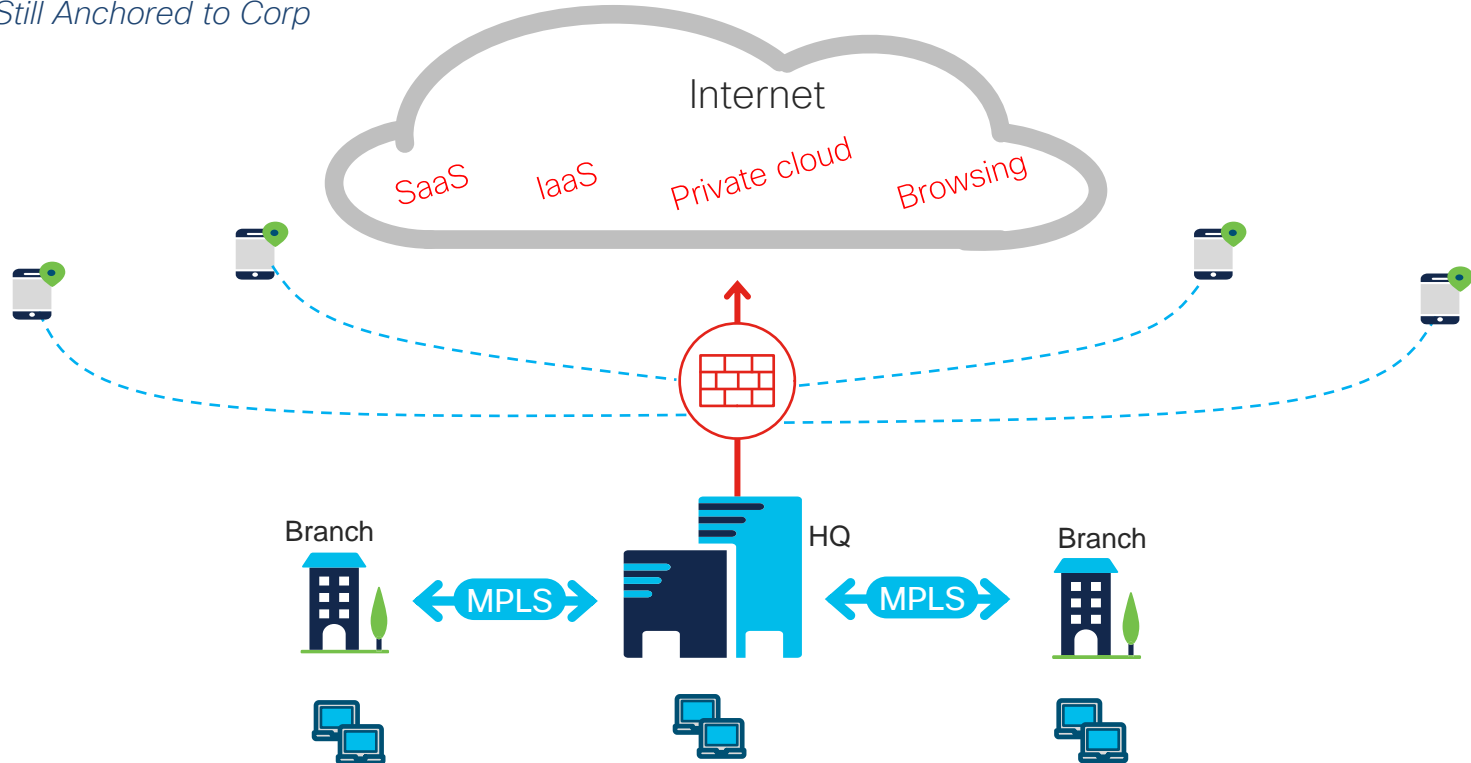
Disruption #2 – User Mobility
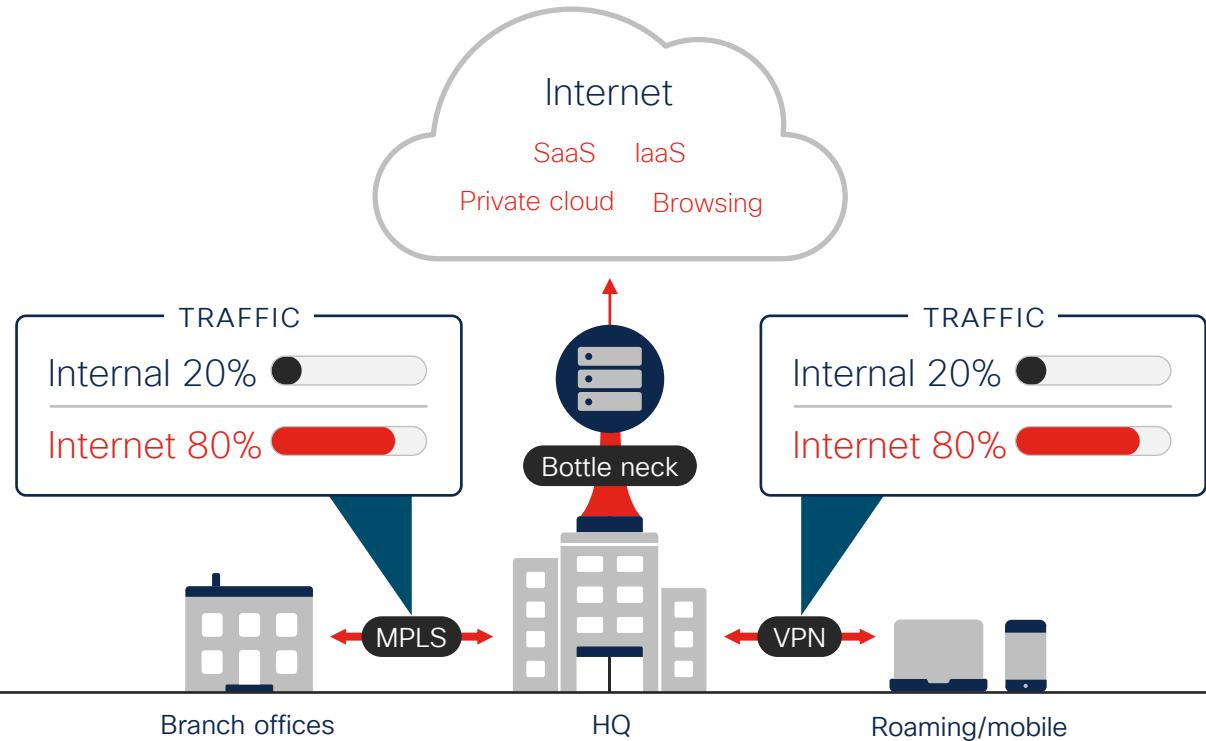
Problem = Still Anchored to Corp

Changes in the types of traffic and destinations
Have inverted the traffic model

Problems:

- Costs
- Performance
- # Tools/vendors
- Integrations
- Maintenance

Internet

SaaS   IaaS

Private cloud   Browsing

TRAFFIC

Internal 20%

Internet 80%

Bottle neck

TRAFFIC

Internal 20%

Internet 80%

Branch offices

MPLS

HQ

VPN

Roaming/mobile

WAN Network Transformation
Internet/Cloud is New "Center of Universe"

DC-Centric

Internet

Perimeter sec appliances to protect network

MPLS

MPLS

Internet/Cloud-Centric

SaaS

WEB

PRIVATE

DIGITAL EXCHANGE

Network architecture is changing

50%

of today's workforce is remote

60%

of orgs' have a majority of apps as SaaS

79%

of orgs shifting to some or all direct internet access

SD-WAN

For remote locations with direct internet access, SD-WAN brings predictable application experience, centralized management, maximum choice and control while cloud security ensures the right security at the right place.

Cloud Security

Cloud-driven security changes

Internet /
SaaS / IaaS

New multi-function
cloud-based security

DNS security

Web gateway

Firewall

CASB

Traditional
on-premise
security stack

○ DNS security

○ Web gateway

○ Firewall

○ CASB

SD-WAN
Direct Internet Access

MPLS

HQ

Branch office
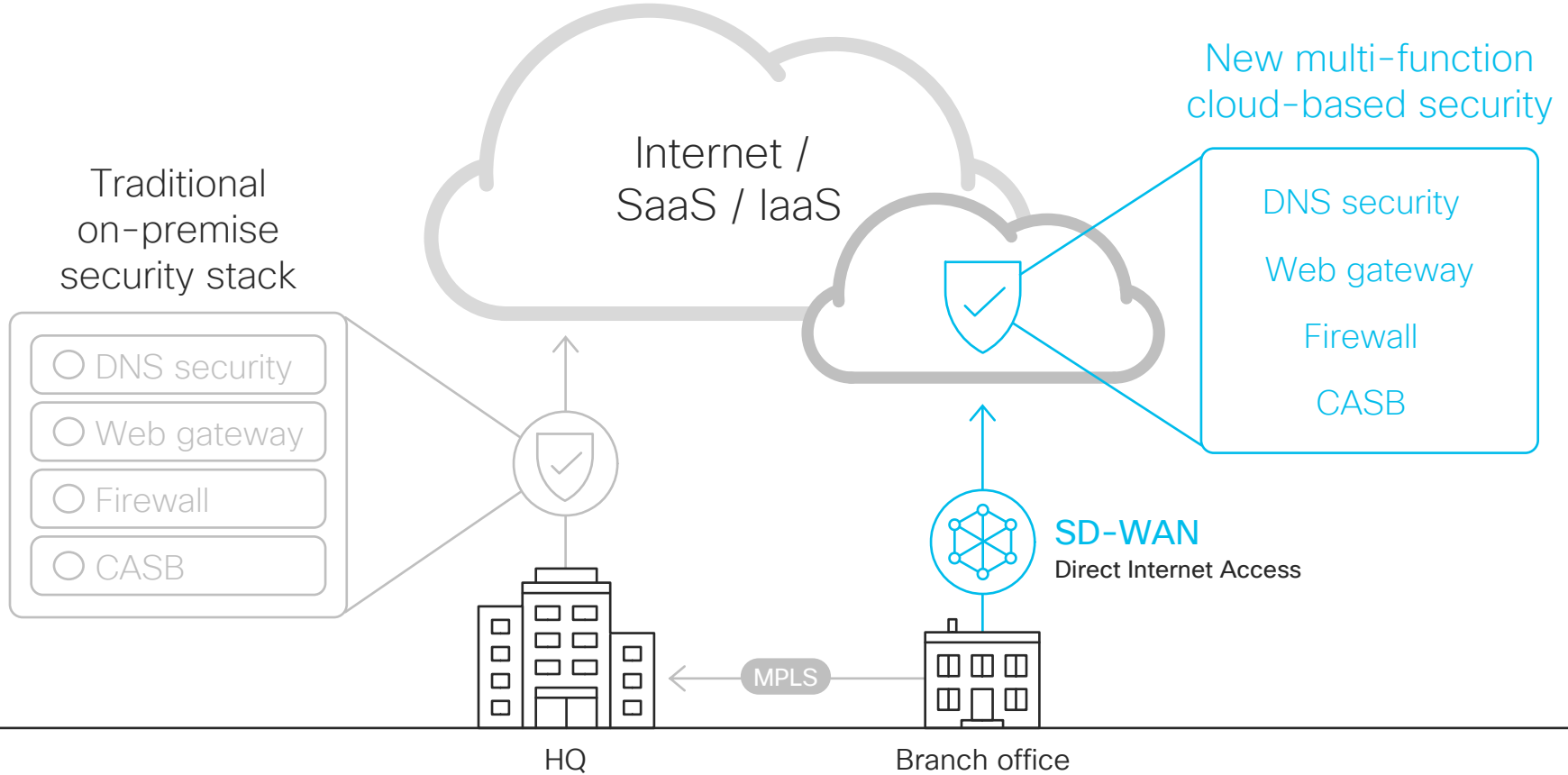
Cloud Driving Major Network Architecture Shift
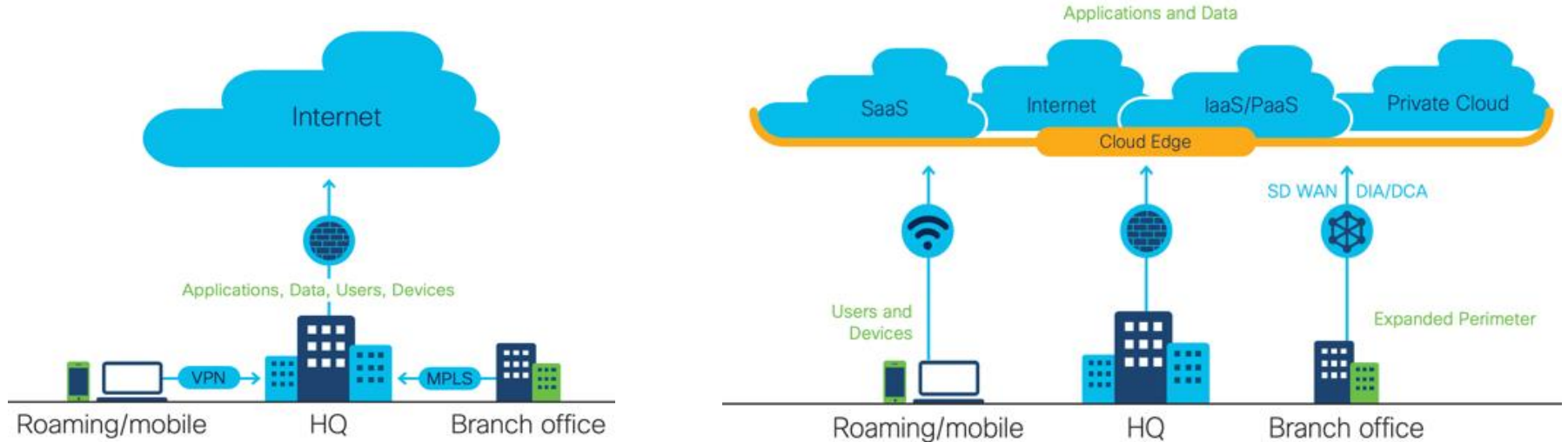
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

We need to reduce complexity and improve performance by **converging** connectivity, security, and identity functions

Different analysts have different names for this multi-function approach...

Gartner®	Secure Access Service Edge (SASE)
	Secure Internet Gateway (SIG)
FORRESTER®	Zero Trust Edge
ESG	Elastic Cloud Gateway

...but full agreement on the move to cloud-native aggregation

"SASE services will converge a number of disparate network and network security services including SD-WAN, DNS protection, secure web gateway, CASB, software defined perimeter (zero trust network access), and firewall as a service."

Gartner
SASE Hype Cycle for Enterprise Networking, Andrew Lerner, 2019

Cisco SASE – Connect, Control, Converge

1 **Connect**

Simple, automated transport from any user , any device, to any application

2 **Control**

Leading threat protection and zero trust access control

3 **Converge**

Integrated networking and security

with automated provisioning

EXTERNAL APPS

INTERNAL APPS

WEB

SaaS

PUBLIC

PRIVATE

Cisco offers the most complete, integrated end-to-end SASE solution

Branch   HQ   Remote   Things   B2B   B2C

Securing your network with Cisco SD-WAN and Umbrella SIG
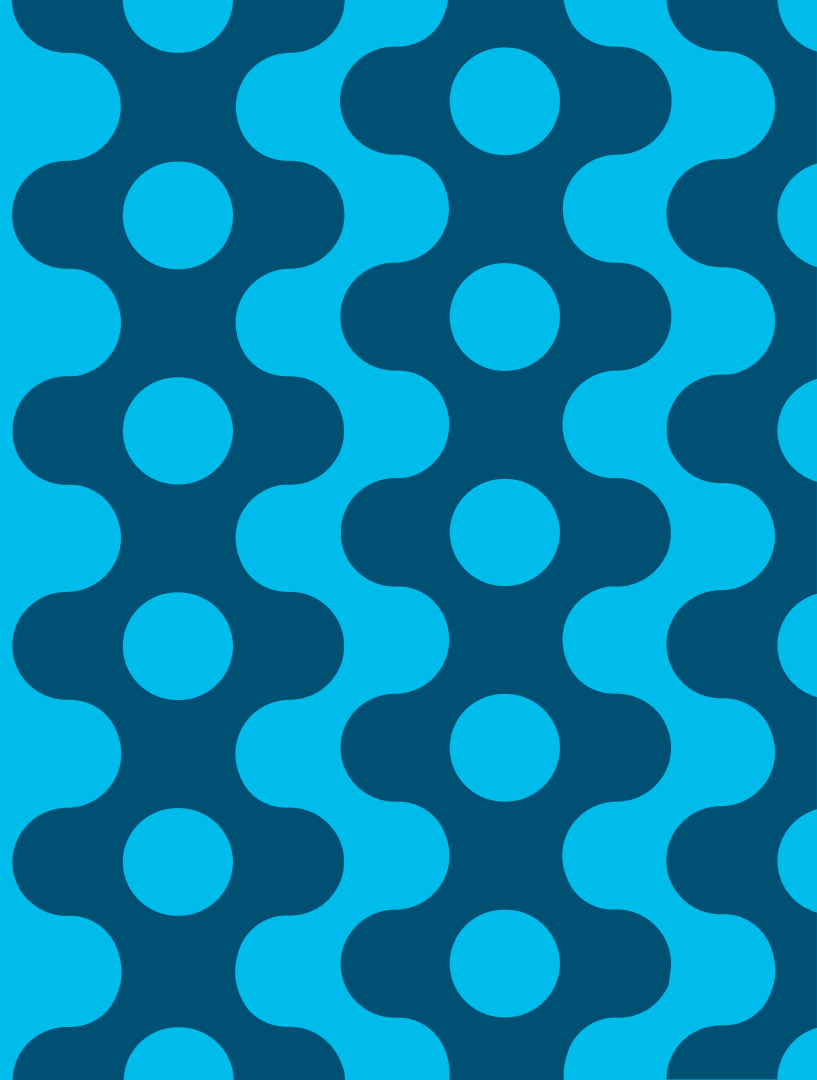
SASE Cloud Adoption with Cisco SD-WAN and Umbrella SIG
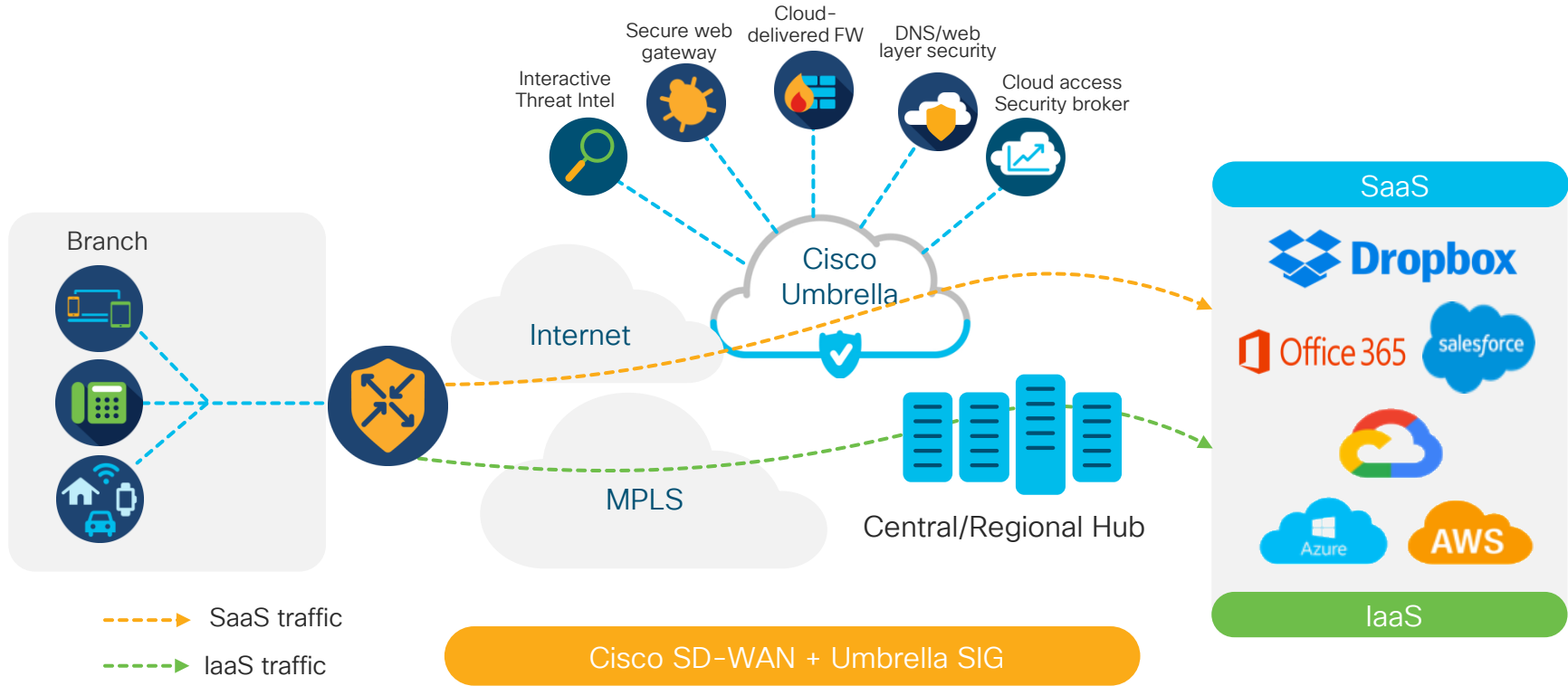
Cisco Umbrella Multi-Function, Cloud Security Solution

Cloud-delivered firewall

Secure web gateway

Cloud access security broker (CASB)

DNS-layer security

Interactive threat intel

Cisco Umbrella

CISCO SecureX

SD-WAN | ON/OFF NETWORK DEVICES
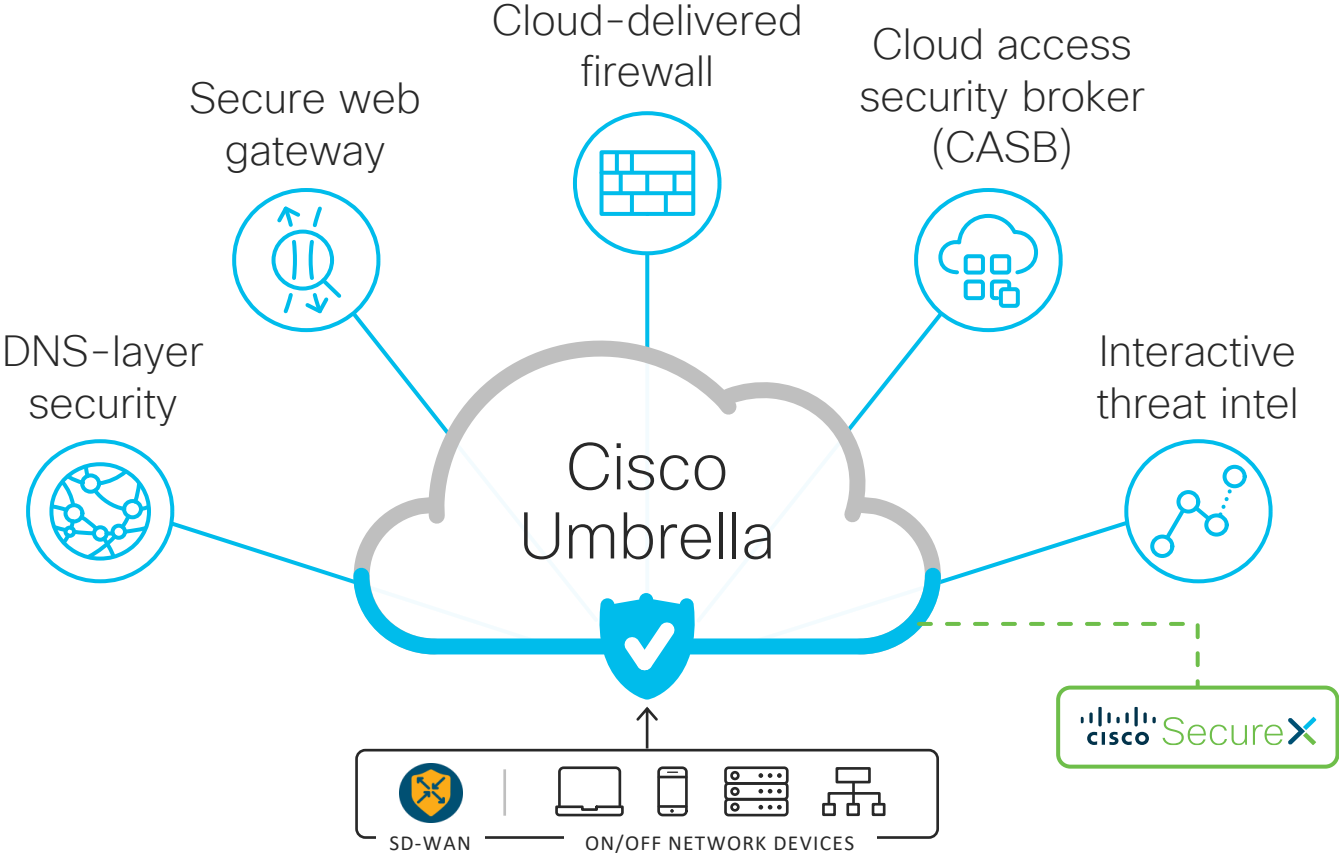
Cisco Umbrella: key capabilities

Secure onramp to the internet, everywhere

Visibility

All internet & web traffic

All apps and all devices

SSL decryption

Other Cisco security and 3rd party data via SecureX

Protection

DNS-layer security

Web inspection

File inspection

Sandboxing

Interactive threat intelligence

File type blocking

Control

URL block/allow lists

Port and protocol rules

Content filtering

Granular app controls

L7 firewall: Non-web app discovery and blocking

Powered by Cisco Talos threat intelligence

Umbrella for Cisco SD-WAN

Fast forward time to value with automated security

Hands-off automation: deploy cloud security across thousands of branches in minutes

Top notch protection: defend against threats at the branch with the leader in security efficacy

Simplified management: single pane of glass across all offices and users

Deeper inspection & controls: SWG and cloud-delivered firewall with IPSec tunnels

Umbrella

DIA

MPLS

Branch

Branch

SD-WAN fabric
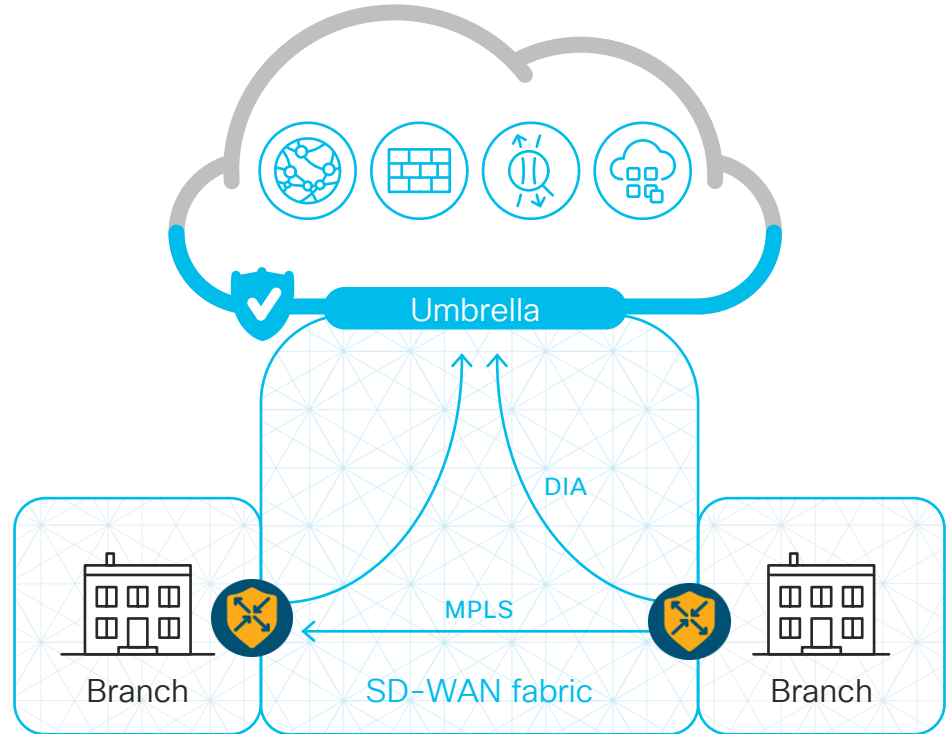
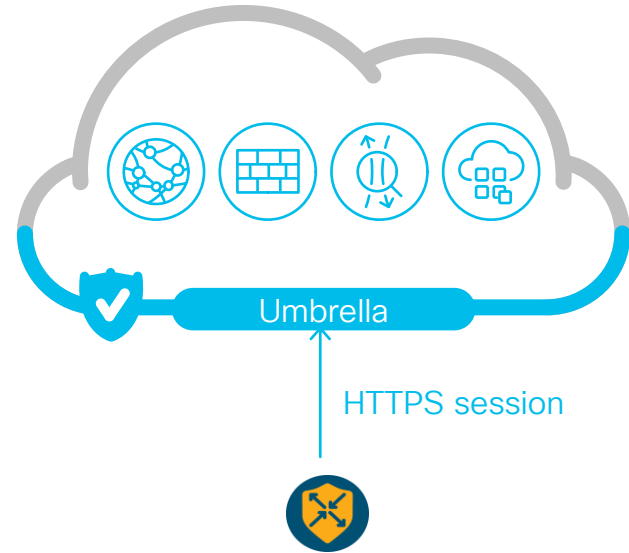# Simple on-boarding: accelerate security & value

Umbrella for Cisco SD-WAN

Deploying Secure SD-WAN no longer takes months:

SD-WAN Edge devices are automatically registered to Umbrella

No need to manually enter API keys

Secure API key is automatically provisioned on the SD-WAN edge device
(via an HTTPS session)

Umbrella

HTTPS session

DNA Premier package

Automated IPsec tunnel creation

Umbrella for Cisco SD-WAN

Distributed organizations with branch offices need to roll-out security fast

Without automation, customers need to manually establish a tunnel for each WAN edge device at the branch

This integration enables customers to:

- Auto-setup with IPSec tunnel to Umbrella SIG using template
- Quickly deploy integrated security across thousands of branches

Internet

Umbrella

vManage
Auto-template
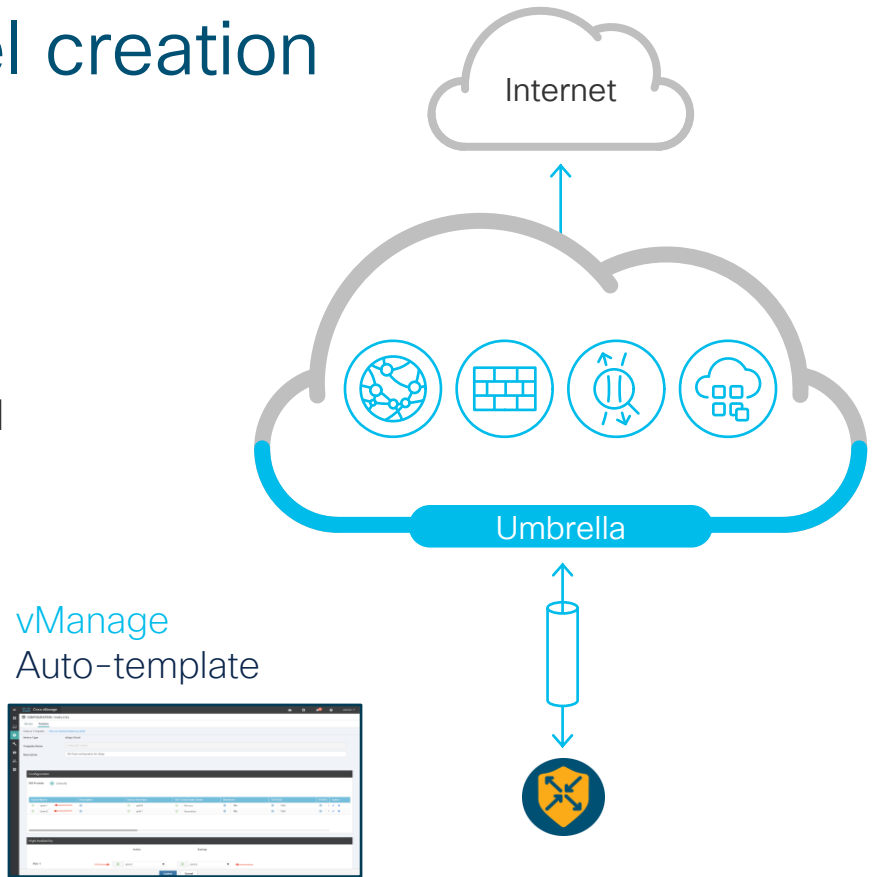
Tunnel capabilities

- vManage auto-templates allow up to active 4 IPSEC tunnels (250Mbps each) from a single SD-WAN edge router

- SD-WAN edge router ECMP load-balances traffic between IPsec tunnels

- Multiple tunnels can be established from a single public IP address (NAT-T)

- You can assign tunnel weights to influence the load-balancing mechanism or to prefer one tunnel over the others

Umbrella

POP1 POP2

ISP1

ISP2

SD-WAN Fabric

Regional Data Center

Data Center

Remote Branch
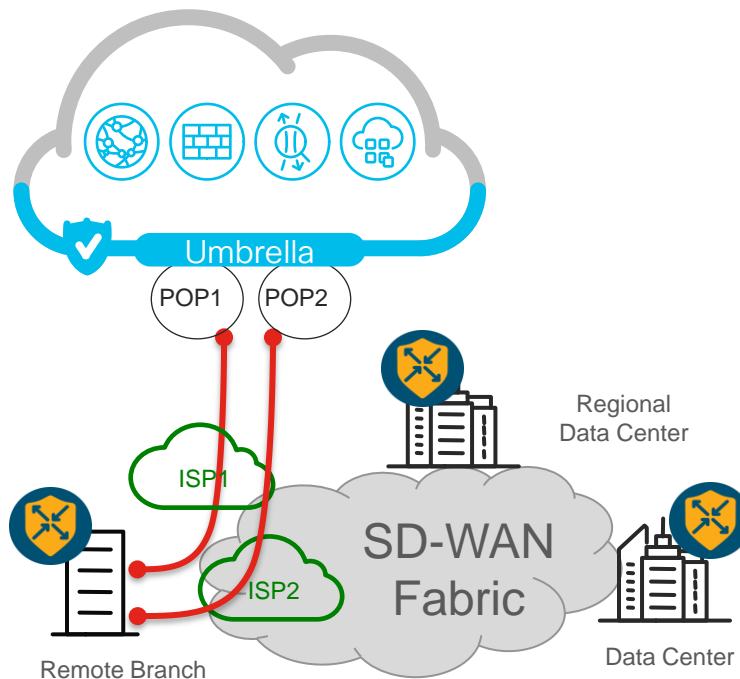
Policy based routing to Cisco Umbrella

Use case

- Centralized Data Policy based" traffic steering to SIG tunnels, which provides more flexibility for a Customer to drive their business intent

- Offers customers flexibility to select which applications send traffic to Umbrella

- Customers can leverage existing data-policy constructs like app-list, prefix-list etc as criteria to steer such traffic/applications to a SIG

- Data policy can be selected per VPN

Umbrella

POP1 POP2

ISP1

ISP2

SD-WAN Fabric

Regional Data Center

Data Center

Remote Branch
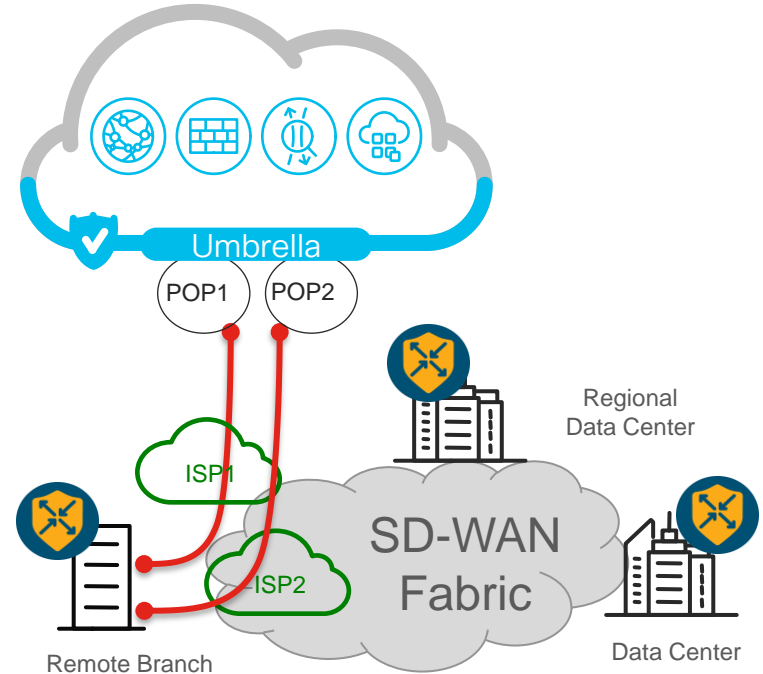
Cisco SD-WAN and Umbrella Integration
Direct Peering – Optimized path from Secure Cloud Gateway to Cloud Workloads

Use case

- As a network admin, I want the best possible application performance across my network

Feature

- Direct peering lowers latency by providing more direct paths
- Global footprint with 20 Regional DCs, expanding to 32+
- Direct peering from Regional DCs to more than 1,000 organizations including leading SaaS and IaaS providers
- Up to 50% performance increase with key applications

SPs	IaaS	SaaS
· AT&T (Global)	· Alibaba	· Apple
· Bell	· Amazon	· Baidu
· Bharti Airtel Limited	· Dell Services	· Box
· BT	· Digital Ocean	· Microsoft MSN
· Charter	· Equinix	· Netflix
· China Mobile	· Fastly	· Salesforce
· Google Fiber	· Go Daddy	· Yahoo!
· KDDI	· Google	· Webex
· Rogers	· Huawei Cloud	· Blizzard
· Swisscom	· Microsoft	· Dropbox
· Telkom	· Rackspace	· Facebook
· Verzion		
· Vodafone		

Current data centers as of January 2021

DNS	SWG	CDFW & IPSec tunnel termination
Miami, US	Miami, FL, US	
Milan, IT	Milan, IT	Milan, IT
Mumbai, IN	Mumbai, IN	
New York, US	New York, NY, US	New York, NY
Palo Alto, US		
Paris, FR	Paris, FR	Paris, FR
Prague, CZ	**Prague, CZ**	**Prague, CZ**
Rio de Janeiro, BR	Rio de Janeiro, BR	Rio de Janeiro, BR
	Santa Clara, CA, US	Santa Clara, CA
Sao Paulo, BR	Sao Paulo, BR	São Paulo, BR
Seattle, US		
Singapore, SG	Singapore, SG	Singapore, SG
Stockholm, SW	Stockholm, SW	
Sydney, AU	Sydney, AU	Sydney, AU
Tokyo, JP	Tokyo, JP	Tokyo, JP
Toronto, CA	Toronto, ON, CA	Toronto, CA
Vancouver, CA	Vancouver, BC, CA	Vancouver, CA
Warsaw, PL		

DNS	SWG	CDFW & IPSec tunnel termination
Amsterdam, NL	Amsterdam, NL	
Ashburn, US	Ashburn, VA, US	Ashburn, VA
Atlanta, US	Atlanta, US	
Bucharest, RO		
Chicago, US	Chicago, IL, US	
Copenhagen, DK		
Dallas, US	Dallas, TX, US	
Denver, US	Denver, US	
Dubai, AE		
Dublin, IE		
Frankfurt, DE	Frankfurt, DE	Frankfurt, DE
Hong Kong, CN	Hong Kong, CN	
Johannesburg, ZA	Johannesburg, ZA	
London, GB	London, UK	London, UK
Los Angeles, US	Los Angeles, CA, US	Los Angeles, CA, US
Melbourne, AU	Melbourne, AU	Melbourne, AU

Cisco Vision for SDWAN and Umbrella integration

Connect it + Secure it

Internet/SaaS — SaaS

IaaS

Data Center

Optimized Routing

Reliability — ON

Secure Internet Gateway

Remote Access

Branch-to-Branch

Visibility

Security as a Service — SASE — Networking as a Service

Remote Workers

CISCO
Customer CPE

Unified Endpoint
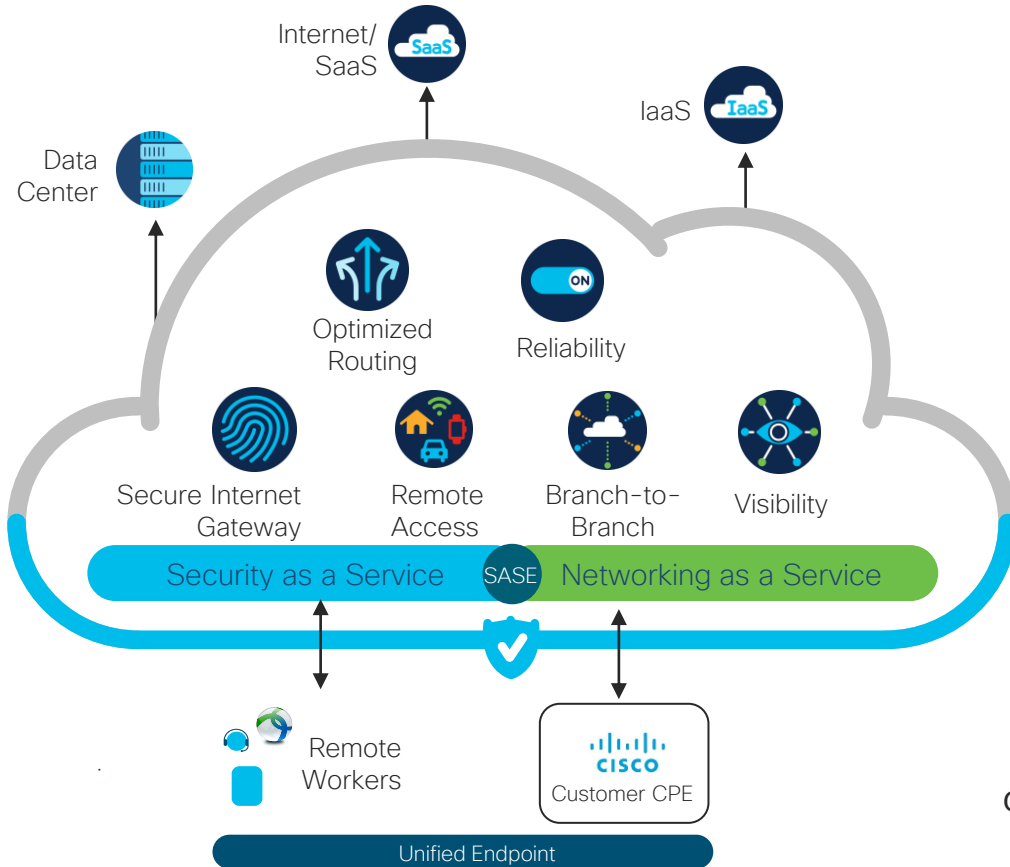
✓ Easily onboard any "branch," from a remote worker to a regional office
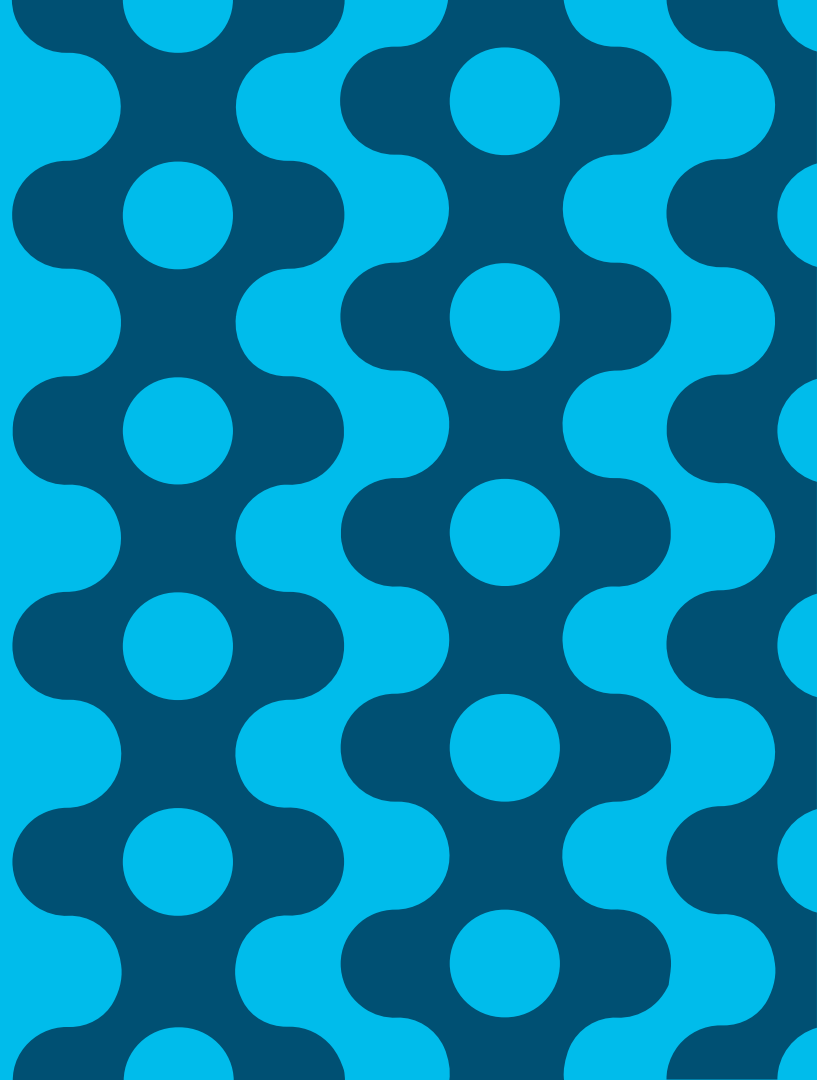
✓ Consistent security across all traffic sources

✓ Access to applications wherever they reside

Create a strong and differentiated SASE offer to deliver unparalleled value to customers through a simple, seamless, and tight integration between SDWAN and Umbrella

Catalyst 8000 Edge Platforms Family

Introducing Catalyst 8000 Edge Platforms Family

Built for the cloud edge

Catalyst 8000v Edge Software/
Catalyst 8200 Edge uCPE

Catalyst 8300/8200 Series Edge Platforms

Catalyst 8500 Series Edge Platforms

Secure, connected experience

- SD-WAN ready
- Cloud-scale multi-layer security
- 256-bit WAN MACSec

Cloud-native agility

- 2-5x throughput improvement
- 10G in access to 40G/100G in edge
- Integration with leading cloud providers

Business-first resiliency

- Built-in edge compute resources
- End-to-end analytics and assurance

Why Catalyst 8000?

Cloud Native Agility	SASE	Connected Experiences	Business First Resiliency
Higher Scale for Distributed Services Integration with leading Cloud Providers	Support for Cisco Umbrella's cloud security services Integrated security and advanced segmentation to contain threats	Enhanced Wireless capabilities for IoT Scale Improved applications performance – User to Cloud	Resource elasticity for edge compute and virtualization Built to produce massive and rich telemetry capabilities

- Next Generation QFP3.0
- Higher SD-WAN Performance
- Open and programmable IOS XE
- Future Proofed – 5G Ready

Easy Operations with Single Image

Single Image
universalk9

IOS XE 'Autonomous' mode

IOS XE SD-WAN 'Controller' mode

Accelerate SD-WAN

Simplify Deployments

Cloud-scale Applications

Cisco Catalyst 8500 Platforms
Powerful SD-WAN 1RU Platform with 100G, 40G ports

01 Improved Data Plane

02 Accelerated SD-WAN Services

03 High Speed Multicloud Access

04 Highly Scalable Control Plane

3rd Generation Quantum Flow Processor

QFP

Hardware Accelerated Services

Up to 8000 SD-WAN IPsec Tunnels

High Speed DIA, DCA 100/40/10/1G Ports

Cisco Catalyst 8500 Series Edge Platforms
Highly Capable 1RU SD-WAN Headend

Integrated Rich Services

NBAR2, NAT, Firewall, QoS, etc.
Industry's Leading Service Edge Platforms

Edge Intelligence

Compute
Container based Apps

Scale

Up to 8000 SD-WAN Tunnel Aggregation
High Speed 100/40 Gigabit Ethernet Ports
High Density 10/1 Gigabit Ethernet Ports

Multi-layer Security

High Throughput MACsec and IPsec
Trustworthy Solutions
Umbrella SIG

Built-in Port Flexibility

Highlights

All Ports Built-in	WAN MACsec	Third Generation QFP	Up to 200Gbps CEF	5G Ready

Manageability

vManage | DNA Center
Open APIs | Analytics
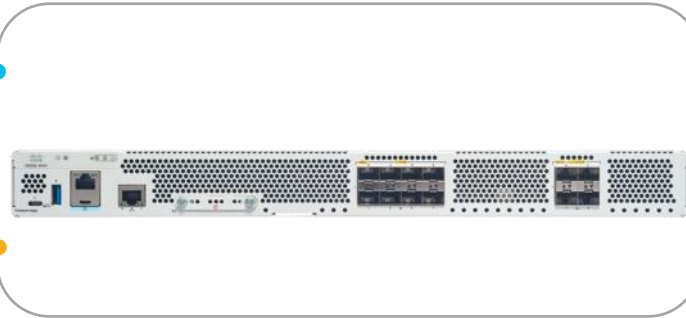
Cisco Catalyst 8500L Edge Platform
Re-Imagined x86 based powerful SD-WAN Headend

Multi-services Support

NBAR2, NAT, Firewall, QoS, etc.
Industry's Leading Service Edge Platforms

Edge Intelligence

Compute
Container based Apps

Scale

Up to 8000 SD-WAN Tunnel Aggregation
High Density 10/1 Gigabit Ethernet Ports

Multi-layer Security

High Throughput MACsec and IPSec
Trustworthy Systems
Umbrella SIG

✓ Core Allocation Flexibility

Connectivity

| All Ports Built-in | WAN MACsec | x86 Advanced Flow Forwarding | Up to 20 Gbps CEF | 5G Ready |

Manageability

vManage | DNA Center

Open APIs | Analytics

Cisco Catalyst 8300 Series Edge Platforms
Multi Gig SD-WAN branch with Accelerated Services

5x Data plane Performance

4x Services Performance

Gigabit+ Cellular, 5G Ready

SD-WAN Voice Integration

SoC Architecture for Dynamic Core allocations

x86

Hardware Accelerated Services

Up to 6000 SD-WAN IPsec Tunnels

High Speed Cloud Access With 10/1G Ports

Cisco Catalyst 8300 Series Edge Platforms
Foundation for the Secure Cloud Scale SD-WAN branch

Integrated Rich Services

Voice Survivability, Forward Error Correction & Packet Duplication, TCP Optimization

Edge Intelligence

Compute
Container based Apps

Scale

Up to 5x IPsec and IP CEF Performance
Core Availability for 3-4x Services
Performance

Multi-layer Security

SSL Acceleration
Application Firewall
IPS/IDS, URL Filtering
AMP, Threat Grid
Umbrella SIG

✔ YES Modularity

Connectivity

Higher WAN Port density	Default 8G DRAM	10G w/ MACsec	Pluggable NVMe Storage	5G Ready

Manageability

vManage | DNA Center

Open APIs | Analytics

Cisco Catalyst 8200 Series Edge Platforms
Foundation for the Secure Cloud Scale SD-WAN branch

Integrated Rich Services

Voice Survivability, Forward Error Correction & Packet Duplication, TCP Optimization

Edge Intelligence

Container based Apps

Performance & Scale

Up to 2x IPSec and CEF Performance
Core Availability for 2x Services Performance
Up to 2x higher IPSEC tunnel Scale

Multi-layer Security

SSL Acceleration
Application Firewall
IPS/IDS, URL Filtering
AMP, Threat Grid
Umbrella SIG

YES Modularity

Connectivity

| Higher WAN Port density | Default 8G DRAM | PIM Support | Pluggable NVMe Storage | 5G Ready |

Manageability

vManage | DNA Center
Open APIs | Analytics
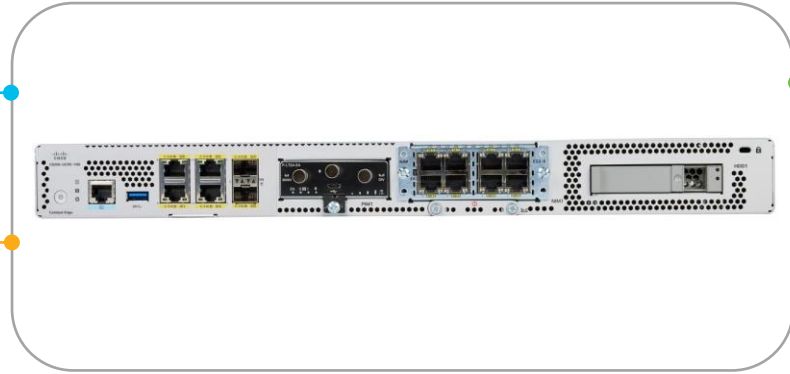
Cisco Catalyst 8200uCPE
uCPE designed for Service Providers

Rich Service Chain
Routing and security functions on one platform
SD-WAN Routing, Security, WLC VNFs

Performance Elasticity
Scale throughput according to branch requirements
Up to 500 Mbps IPsec with QAT & 2 Gbps CEF

Edge Intelligence
AI/ML Analytics
IoT and Business Applications

Compact and Secure
Cisco Trustworthy Solution
Hardware Anchor Module
Less than 12-inch depth

Highlights

8 Core CPU Up to 4 VNFs	WAN/LAN Module Diversity	5G Ready	Higher WAN Port Density	Up to 4TB Storage

Manageability

vManage
NSO
MSX
Analytics

Catalyst 8300/8200 Edge Platforms Family – SoC

x86

X86 Multi-core CPU

WIRESHARK

iPerf

DPDK
DATA PLANE DEVELOPMENT KIT

Hosted App1	Hosted App2

IPS	URL-F	AMP

UTD Engine

KVM – Hypervisor

LXC Container

Quick Assist Technology (QAT)

PPE	SP	SP	I/O
PPE	SP	CP	I/O

Service Plane Optimized

Dynamic Allocation

PPE	PPE	PPE	I/O
PPE	PPE	CP	I/O

Data Plane Optimized
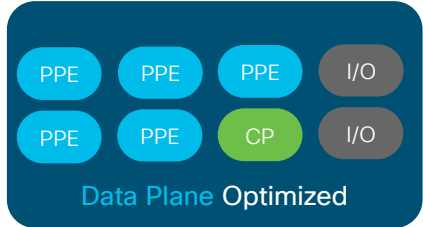
I/O	I/O Core
PPE	Data Plane Core
CP	Control Plane Core
SP	Service Plane Core

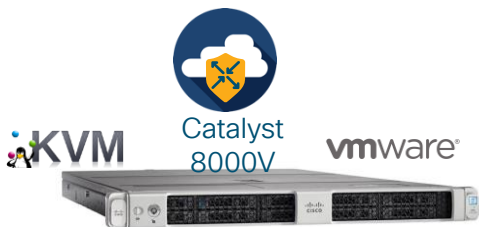**Dynamic Core allocation – meet throughput and services demand**

Cisco Catalyst 8000V Edge Software

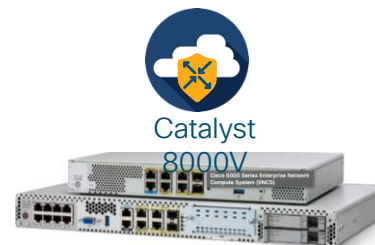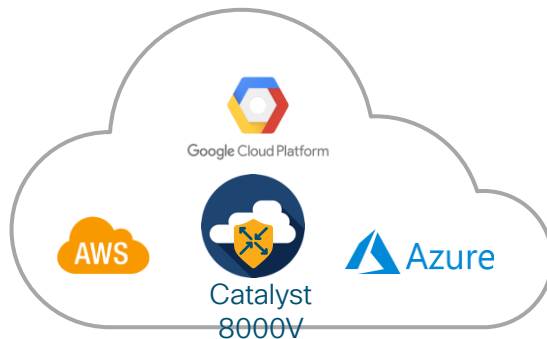Versatile Network Connectivity Options

Seamless SD-WAN Extension in cloud

Infrastructure Agnostic

Service Richness

Catalyst 8000V

KVM   vmware®

Hypervisor
On x86 server

Google Cloud Platform

AWS   Catalyst 8000V   Azure

Catalyst 8000V

NFVIS
on ENCS

Virtual Router Convergence

VNF Convergence Approach

17.1.x and earlier

- ISRv IOS XE
- ISRv XE SD-WAN
- CSR 1000V IOS XE
- CSR 1000V XE SD-WAN
- vEdgeCloud Viptela OS

17.2/17.3

- ISRv on ENCS Unified
- CSR 1000V Unified
- vEdgeCloud Viptela OS

17.4.1

- Catalyst 8000V Unified
- vEdgeCloud Viptela OS

IOS-XE 'Autonomous' Mode

IOS-XE SD-WAN 'Controller' mode

Virtual Router Unified

AWS Azure

CISCO

3rd Party

Network Consistency
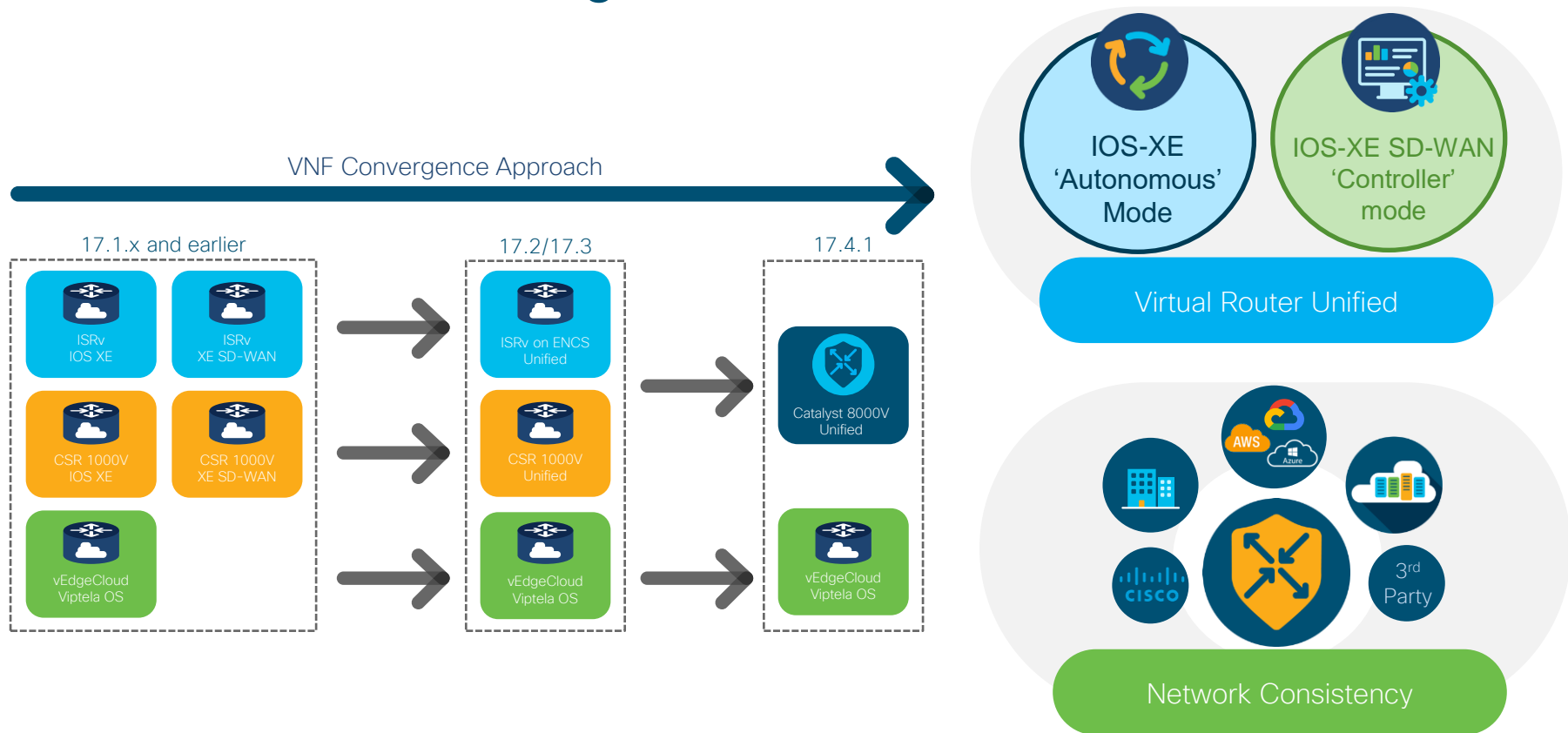
Cisco Catalyst 8000V Edge Software
Enterprise-class networking and Security with flexibility of a x86 based VNF

Multi-Services Support

Feature-rich IOS XE and XE-SD-WAN software
Supported features such as NAT, Firewall, NBAR
QoS, etc.
Runs on any x86 VM platform

Cloud Integration

Extends connectivity, visibility, security into public
and private clouds
Auto-Scaling capability
Integration with Azure vWAN and AWS TGW
Supports wide variety of cloud instances

Performance Elasticity

CPU Hypervisors: 1 – 8 vCPU
Cloud Providers: 1- 16 vCPUs
Memory Scale: 4 – 16Gb

Multi-Layer Security

Secure object storage
High Throughput IPsec
IPS/IDS, URLF, **AMP&TG, TLS Proxy**

Catalyst 8000V

Virtual Switch/SRIOV
Hypervisor/Cloud

Highlights

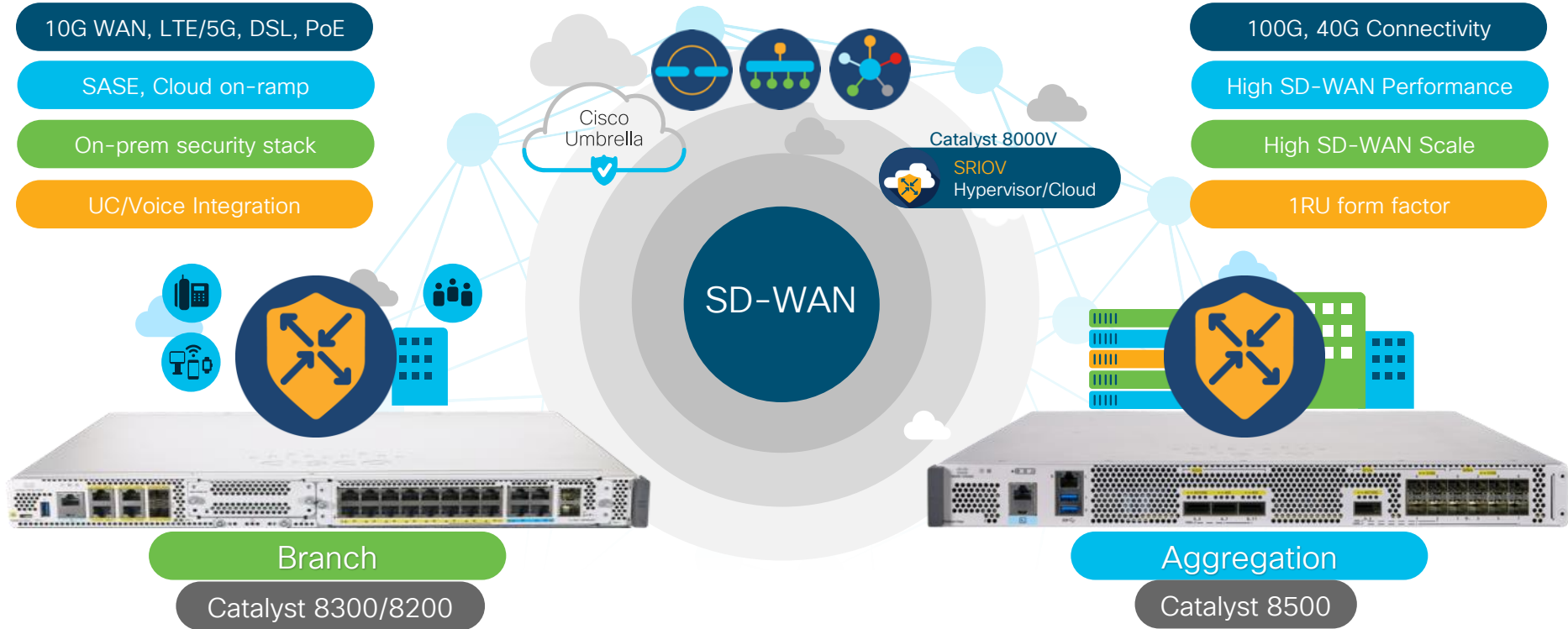| Up to 10 Gbps IPsec in cloud | ENCS NIM support | TGW and vWAN integration | DPDK IO | SD-WAN in AWS, Azure, and GCP |

Manageability

vManage | Multi-tenant

Open APIs | Analytics

Catalyst 8000 - SD-WAN Hub, Branch and Cloud

10G WAN, LTE/5G, DSL, PoE

SASE, Cloud on-ramp

On-prem security stack

UC/Voice Integration

100G, 40G Connectivity

High SD-WAN Performance

High SD-WAN Scale

1RU form factor

Cisco Umbrella

Catalyst 8000V

SRIOV
Hypervisor/Cloud

SD-WAN

Branch

Catalyst 8300/8200

Aggregation

Catalyst 8500

AppQoE with SD-WAN

Branch

DIA

MPLS

SD-WAN Fabric

Office 365

Google salesforce Webex Meetings Dropbox

ISP2

Regional Data center

Critical Applications

Data Center

Catalyst 8300/8200

TCP Optimization

Forward Error Correction (FEC)

Packet Duplication

DRE & Caching *

Enhanced Application Quality experience
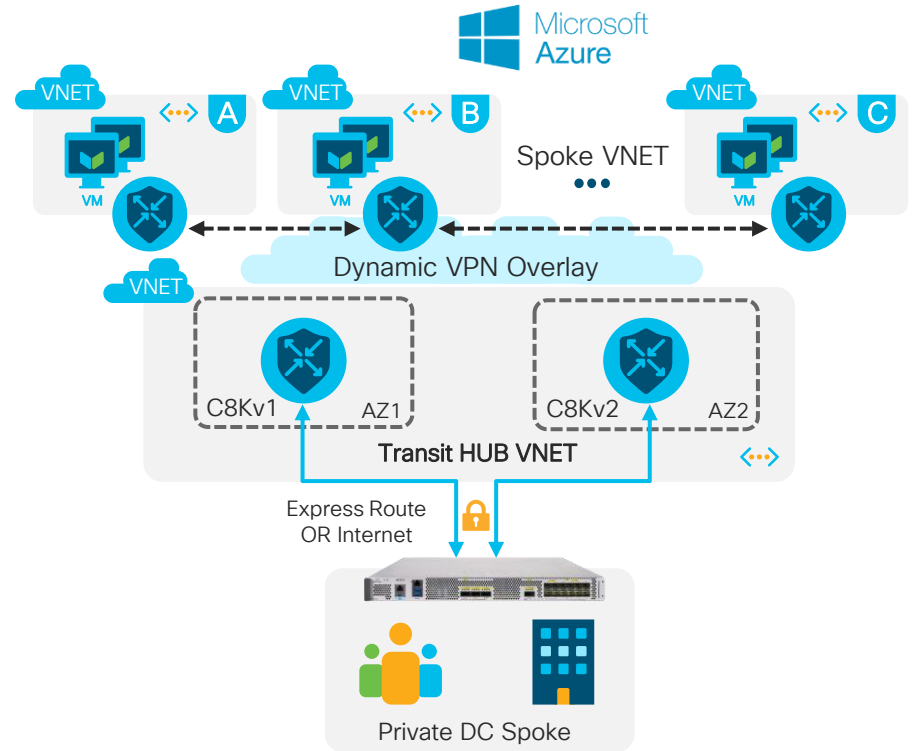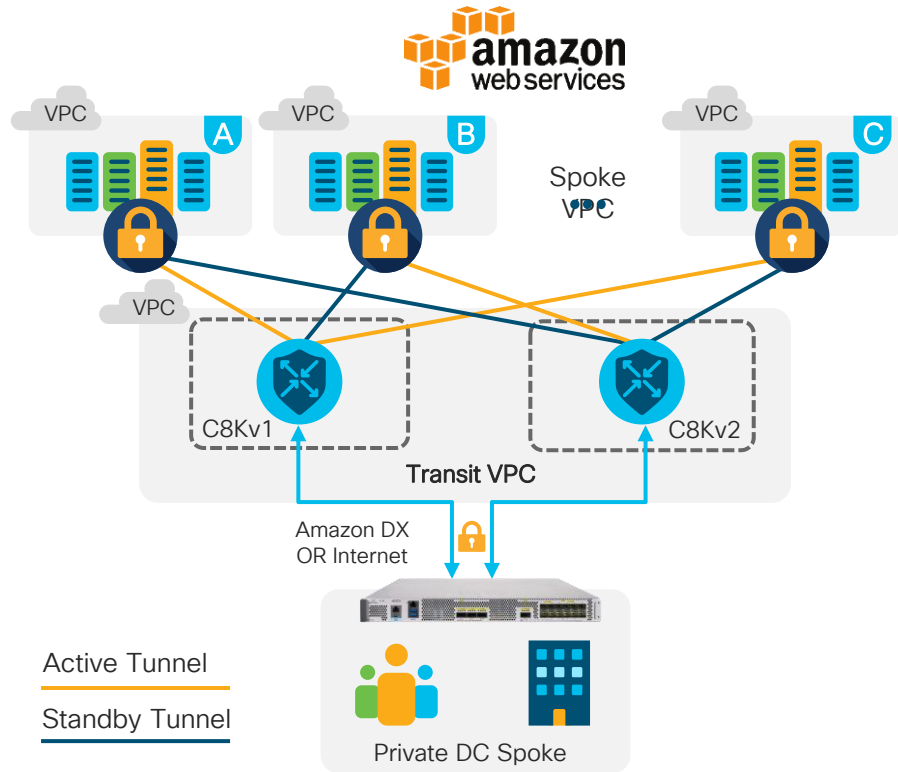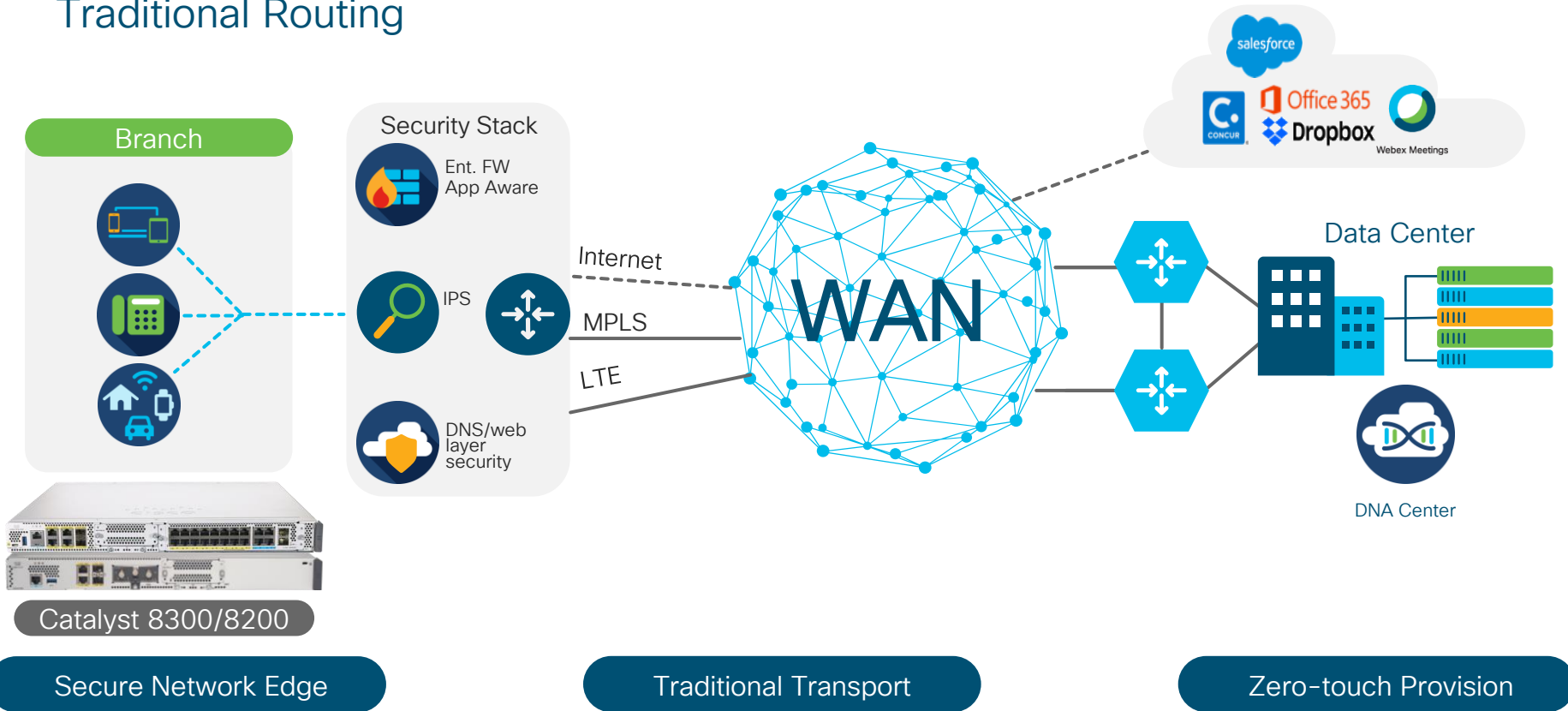
Public Cloud Applications
AWS Transit VPC, Azure Transit VNET

Enterprise Branch Office
Traditional Routing

Branch

Security Stack

Ent. FW
App Aware

IPS

DNS/web
layer
security

Internet

MPLS

LTE

WAN

salesforce

CONCUR

Office 365

Dropbox

Webex Meetings

Data Center

DNA Center

Catalyst 8300/8200

Secure Network Edge

Traditional Transport

Zero-touch Provision

SASE Cloud Adoption with SD-WAN

Branch

Catalyst 8300/8200

Interactive Threat Intel

Secure web gateway

Cloud-delivered FW

DNS/web layer security

Cloud access Security broker

Cisco Umbrella

Internet

SD-WAN

Regional Hub/Co-lo

SaaS

Dropbox

Office 365

salesforce

Webex Meetings

Azure

AWS

IaaS

Cisco SD-WAN + Umbrella SIG = SASE

Seamless cloud access for SASE applications

Key Takeaways

- SASE – a modern approach to building secure networks in multicloud world

- Cisco SASE solution delivers superior connectivity with complete protection

- New Catalyst 8000 Platform Optimized for SASE and Cloud-scale SD-WAN solutions