Delivering Cisco Next Generation SD-WAN with Viptela (Addendum)

Nikolai Pitaev, Senior Technical Marketing Engineer, ENB
@pitaev
DGTL-BRKCRS-2110

Agenda

- SD-WAN Fundamentals @ CL Barcelona '20
- New since January 2020:
    - Cloud: Google Cloud, TGW, vWAN
    - Security: SSL Proxy, Umbrella Automation
    - Voice and UC
    - Multicast
    - Infrastructure
- Conclusion

SD-WAN
fundamentals recap

SD-WAN fundamentals in CL On-Demand Library

1. Find DGTL-BRKCRS-2110:

Filters   Clear   "BRKCRS-2110" ✕   2020 Barcelona ✕

BRKCRS-2110 🔍

2 sessions

Delivering Cisco Next Generation SD-WAN with Viptela - BRKCRS-2110 ☆

Event: 2020 Barcelona

SPEAKERS
Nikolai Pitaev, Technical Marketing Engineer - **Distinguished Speaker**

EVENT ⌃
☐ 2020 APJC Virtual
☑ 2020 Barcelona

2. Learn in 90 Minutes:

- Building Blocks: controllers and routes
- Deployments: cloud-based and on-prem
- Use cases: DIA, Security, Colocation

- Cloud: SaaS and IaaS
- Application Quality of Experience
- Demonstration

CISCO *Live!*

New since CL Barcelona 2020

Summary of new topics since January 2020

New topics:

- Cloud: SaaS, Google Cloud, AWS TGW, Azure vWAN

- Security: SSL Proxy, Umbrella automation

- Unified Communications

- Multicast

- SD-WAN Infrastructure features

Cloud

Cloud-related SD-WAN topics

1. Cloud onRamp for SaaS Innovations: Microsoft365
2. Cloud onRamp for IaaS: TGW and vWAN automation
3. Google Cloud

SD-WAN SaaS Innovation with Microsoft 365

Use Case: access to cloud-based Office 365 Apps

Key Problem: what is the best way to the App?

Before: active probing on all paths

After:
17.3 (July) identification based on MSFT published categories
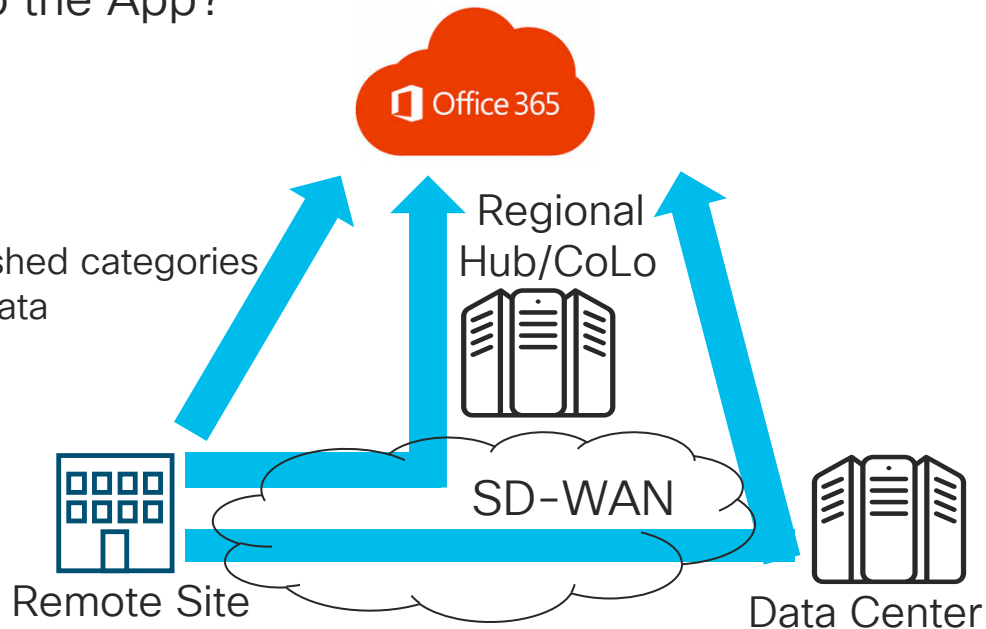17.4 (Nov.) user can rely on MSFT telemetry data
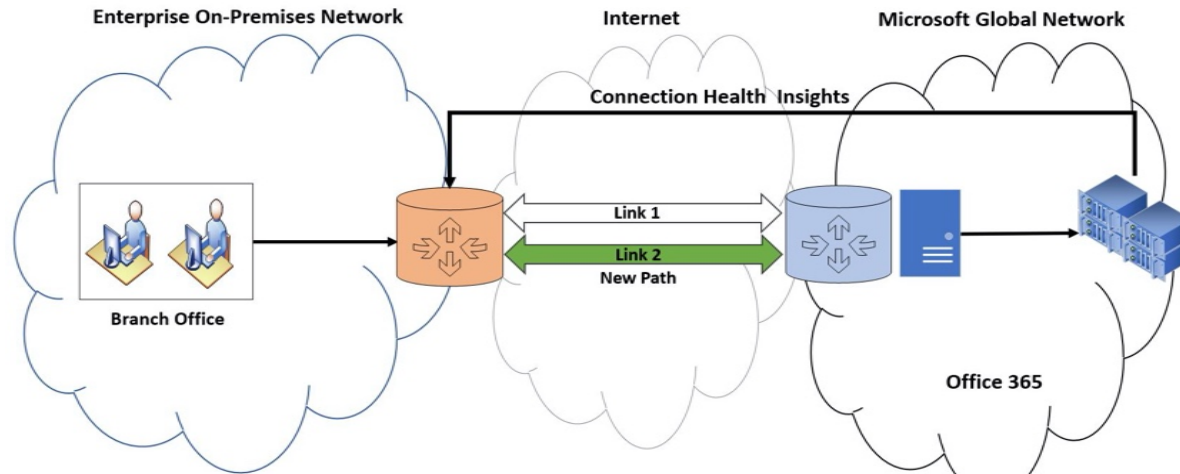
Benefits:

improved application performance

support for new O365 categories

Key message:
Better O365 user experience with Cisco SD-WAN and application infused path selection

How it works

- Microsoft shares Office 365 connection health insights (aka Telemetry data).
- Cisco SD-WAN devices consumes the insights to make intelligent routing decisions by sending key O365 traffic on alternate paths.
- Microsoft-Cisco collaboration enables improved O365 user experiences such as Outlook search, SharePoint document collaboration and Teams conferencing.
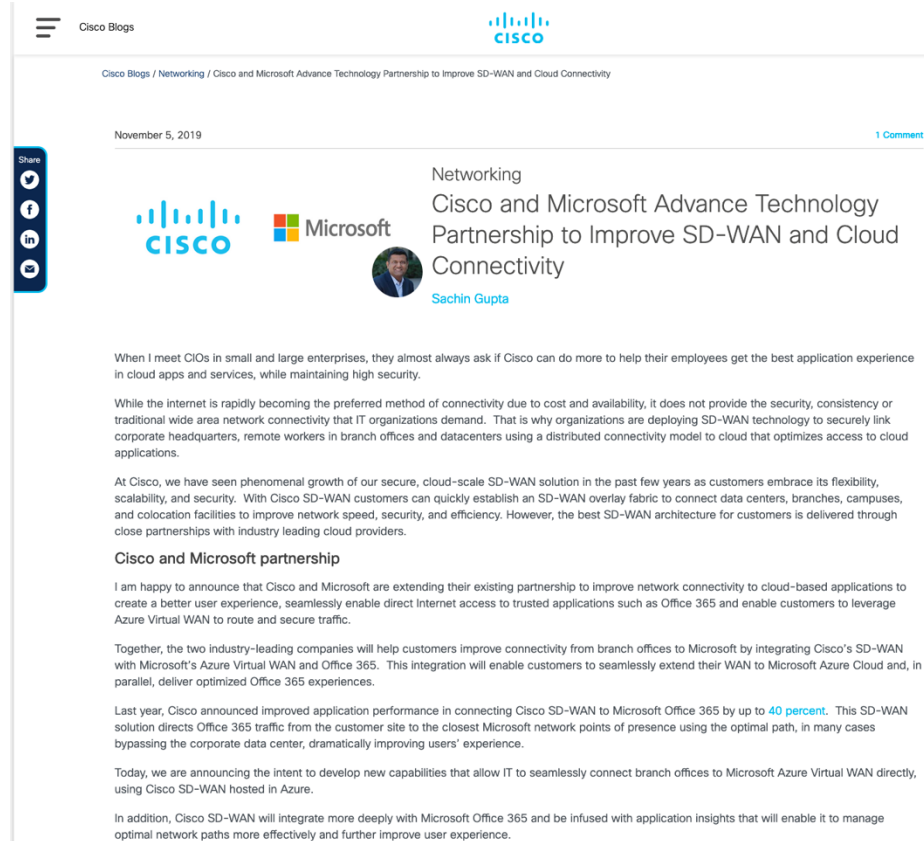
Key Message: this is the first app-driven SD-WAN solution, where route selection is based on telemetry info injected directly from the cloud.

Announcement in November 2019

Last year, Cisco announced improved application performance in connecting Cisco SD-WAN to Microsoft Office 365 by up to 40 percent. This SD-WAN solution directs Office 365 traffic from the customer site to the closest Microsoft network points of presence using the optimal path, in many cases bypassing the corporate data center, dramatically improving users' experience.

Today, we are announcing the intent to develop new capabilities that allow IT to seamlessly connect branch offices to Microsoft Azure Virtual WAN directly, using Cisco SD-WAN hosted in Azure.

In addition, Cisco SD-WAN will integrate more deeply with Microsoft Office 365 and be infused with application insights that will enable it to manage optimal network paths more effectively and further improve user experience.

https://blogs.cisco.com/enterprise/cisco-and-microsoft-advance-technology-partnership-to-improve-sd-wan-and-cloud-connectivity

Cloud-related SD-WAN topics

1. Cloud onRamp for SaaS Innovations: Microsoft365
2. Cloud onRamp for IaaS: TGW and vWAN automation
3. Google Cloud

Cloud onRamp for IaaS: TGW Innovations

Use Case: connect IaaS infra via TGW to SD-WAN

Key Problem: fast and reliable interconnection

Before: manual interconnection

After: automated interconnection from vManage

Benefits: fast and reliable config from single UI
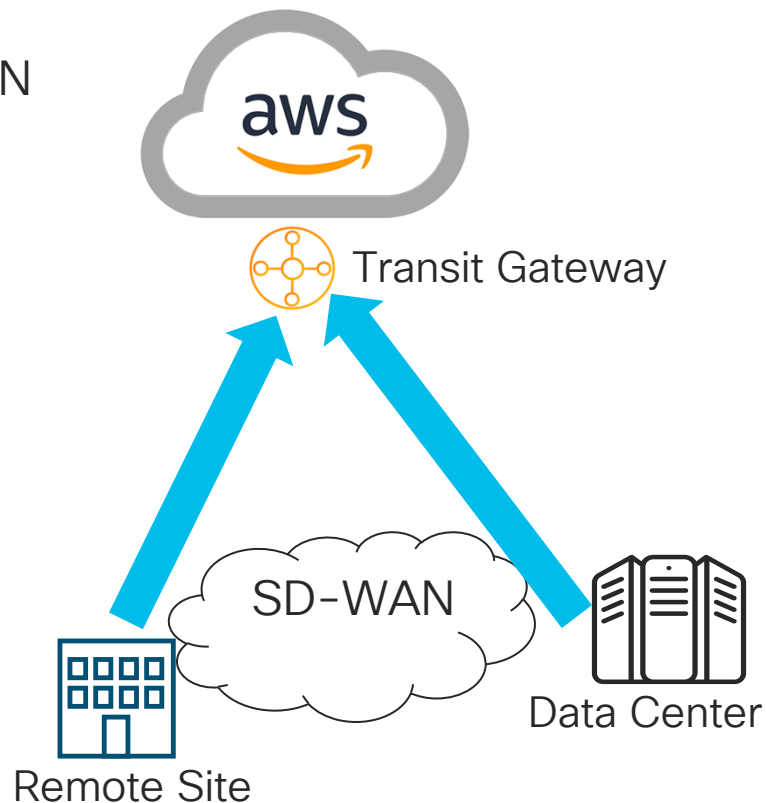
Cloud: SD-WAN & AWS TGW Automation

- Automation is targeted for 2nd half of 2020 with 2 options:

1. Branch connect:
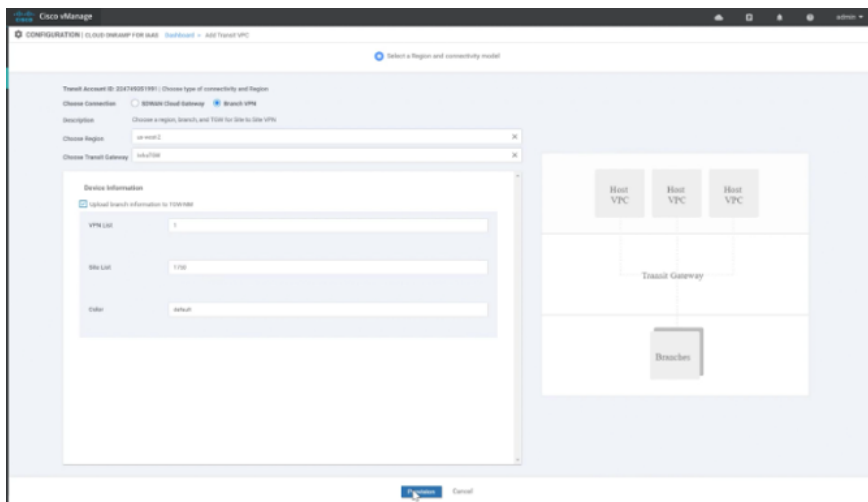
Direct connection from branches to TGW

2. SD-WAN Cloud Gateway:
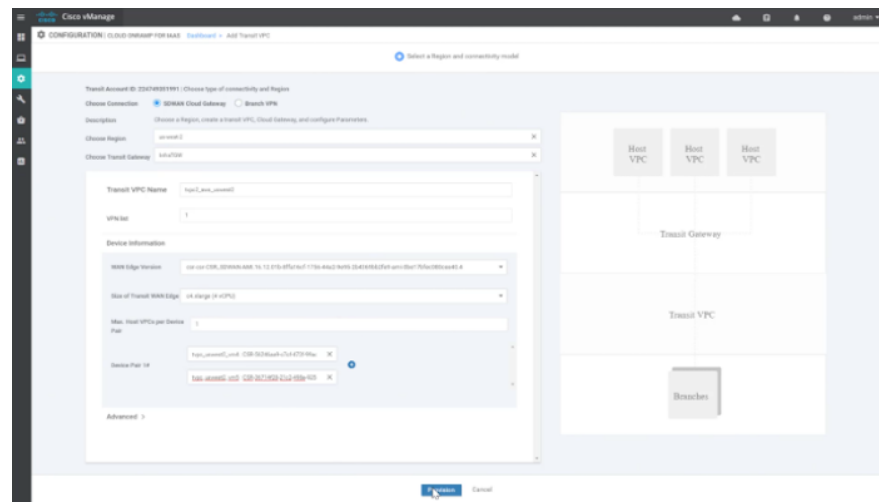
Branches connect to SD-WAN Edge Router in SD-WAN VPC first

AWS TGW Demo: Step 1

- Duration of the whole demo: 12 Min

- Creation of the 1st TGW in us-west1
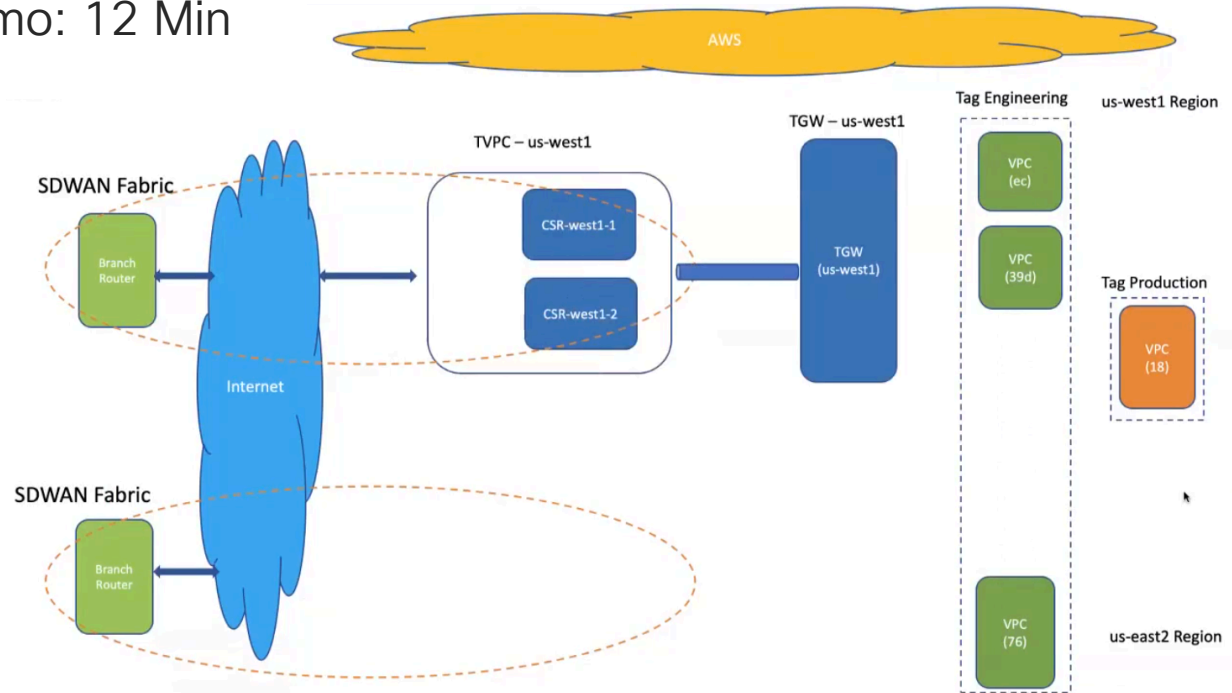
AWS TGW Demo: Step 2

- Creation of the 2nd TGW in us-east2
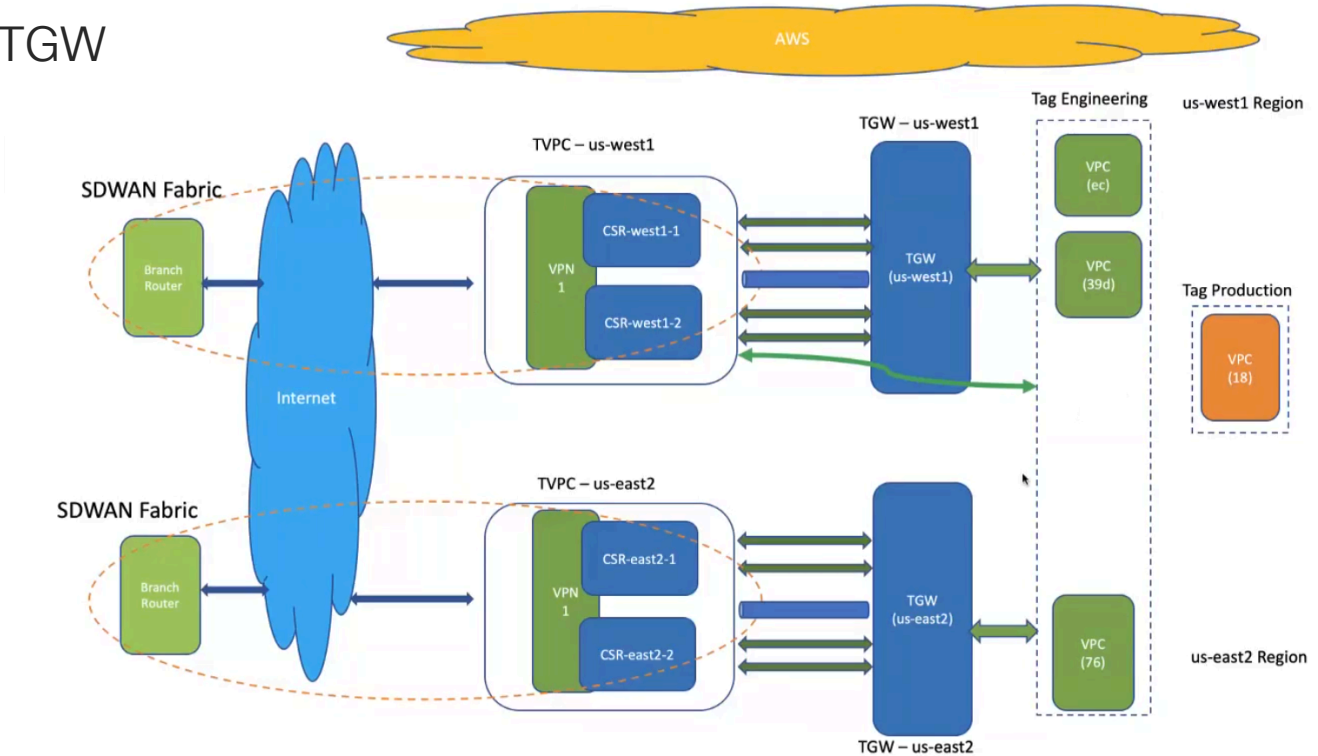
AWS TGW Demo: Step 3

- Moving VPC from "Engineering" to "Production" Tag in us-west1
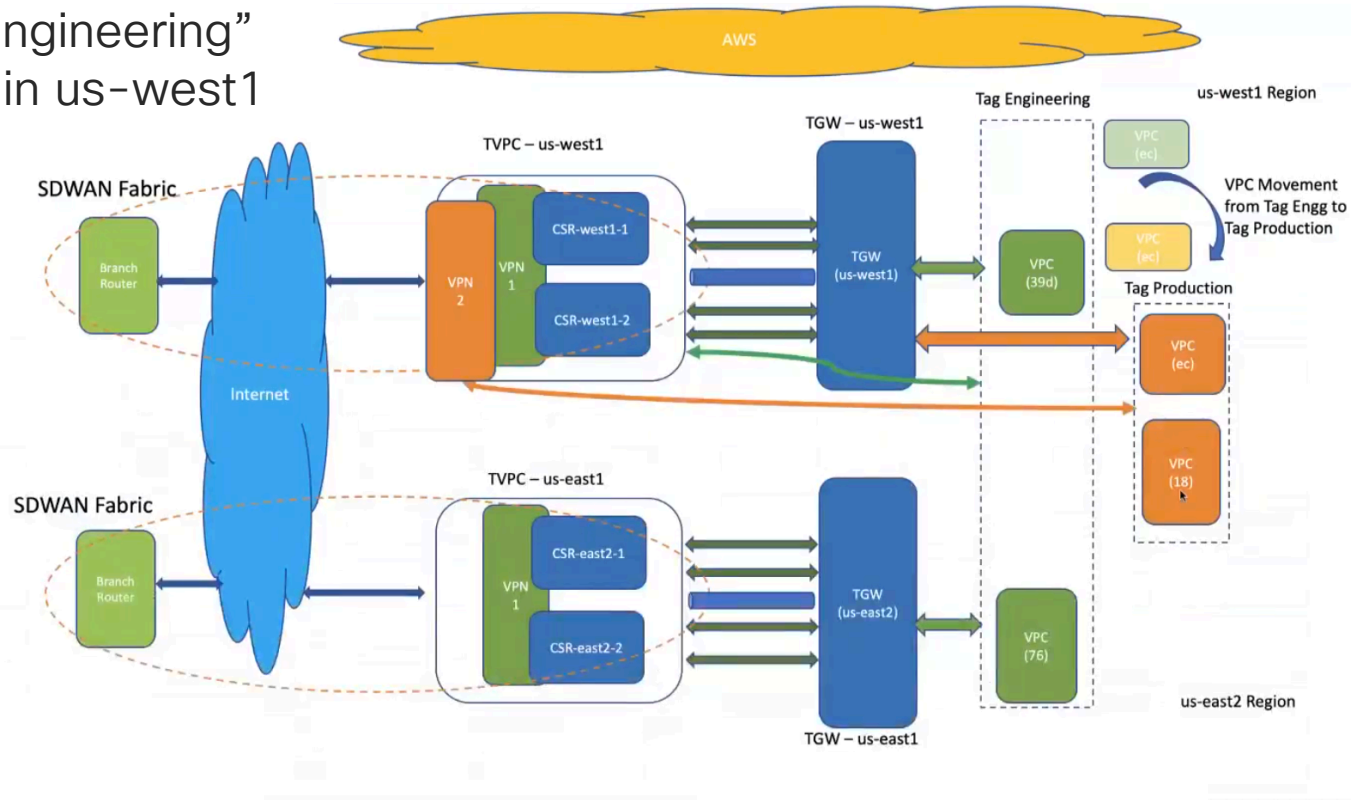
Cloud: Using TGW as underlay

- SD-WAN can use AWS with TGW peering as underlay

- Pros: AWS is just another transport, full visibility and SD-WAN features

- Cons: static routing on the TGW side
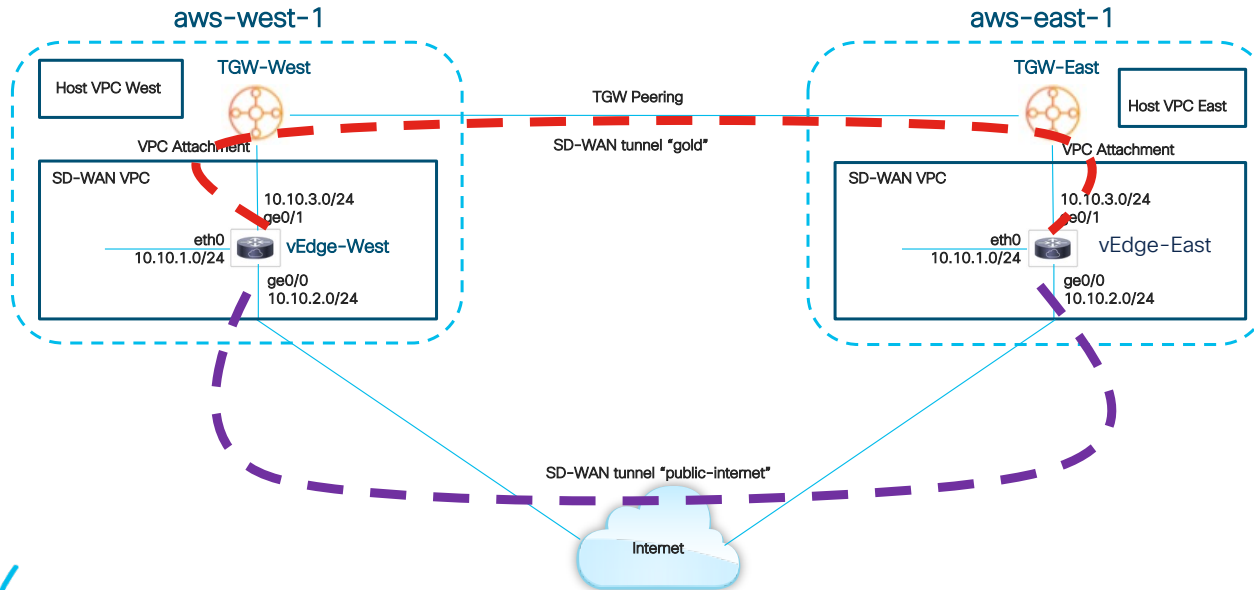
Cloud-related SD-WAN topics

1. Cloud onRamp for SaaS Innovations: Microsoft365
2. Cloud onRamp for IaaS: TGW and vWAN automation
3. Google Cloud

Cloud: SD-WAN & Google Cloud (GCP)

- CSR1000v running non SD-WAN image is supported on GCP

- CSR1000v SD-WAN Image is targeted for 2nd half of 2020

- Example of joint innovation:
  - Interaction between SD-WAN and Service Directory
  - App Metadata translated to SD-WAN SLA/Policies
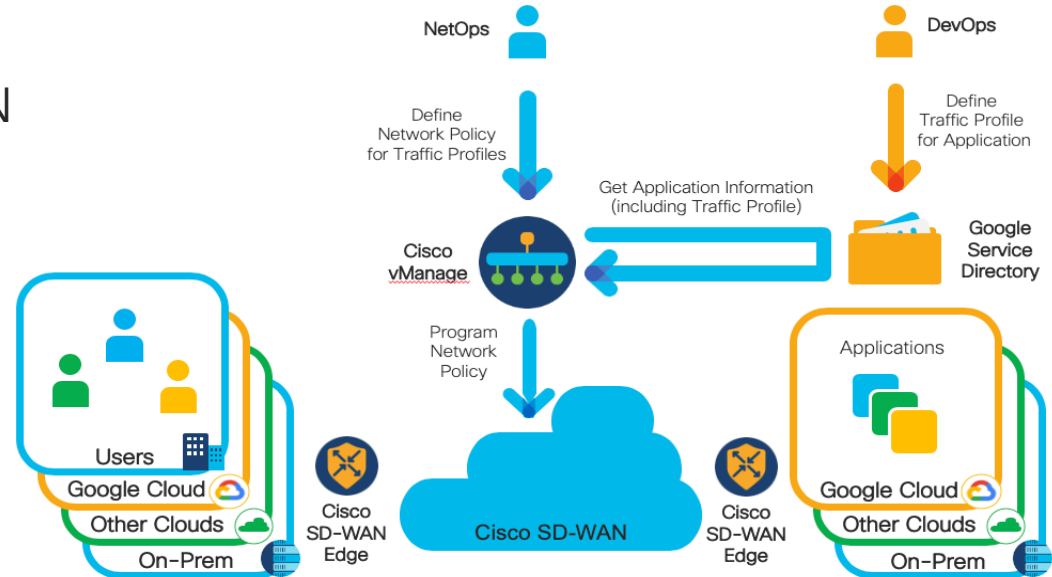
Architecture
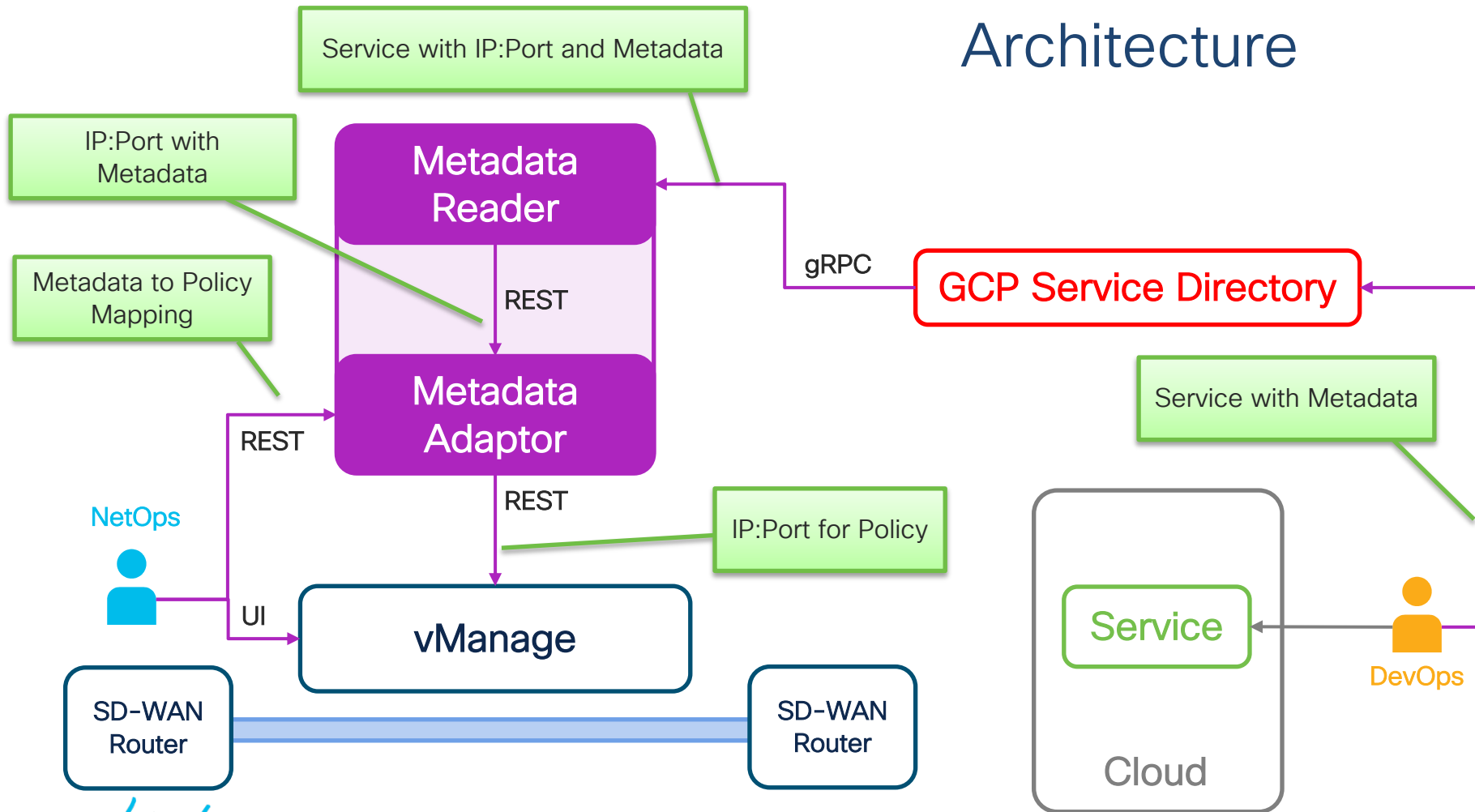
Demo Setup Topology
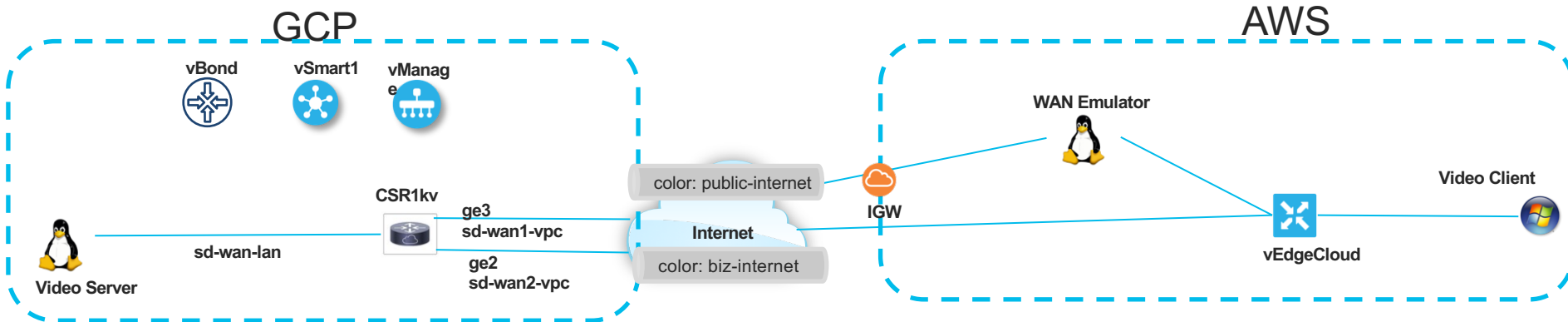
Demo Steps:

1. Video runs over public-internet with bad quality

2. Video Server App registers in Google Service Directory

3. Script polls Service Directory, reads metadata and activates SD-WAN policy

4. SD-WAN switches traffic to a better biz-internet path. Video quality is improved!

Cloud: Summary

1. Cloud onRamp for SaaS Innovations Microsoft365: endpoint category support, telemetry influenced routing

2. Cloud onRamp for IaaS – TGW and vWAN automation: segmentation use case automated, cloud provider backbone is just an additional transport

3. Google Cloud:
Service Directory creates a bridge between Devops (app metadata) and Netops (network policy)

Security

TLS/SSL Proxy Support with SD-WAN

SSL Proxy will help customers decrypt and inspect network traffic for malware

Cisco SD-WAN SSL Proxy…
- Intercepts/Redirects SSL traffic to ISR
- Decrypts packet and inspects
- Re-encrypts packet and sends
- Intercepts response
- Decrypts packet and inspects
- Re-encrypts packet and forwards to end user

HTTPS traffic

Inspect Traffic

| SSL Proxy Decrypts | FW IPS/IDS URLF AMP (Security Features for inspection) | SSL Proxy Encrypts |

Router

HTTPS traffic
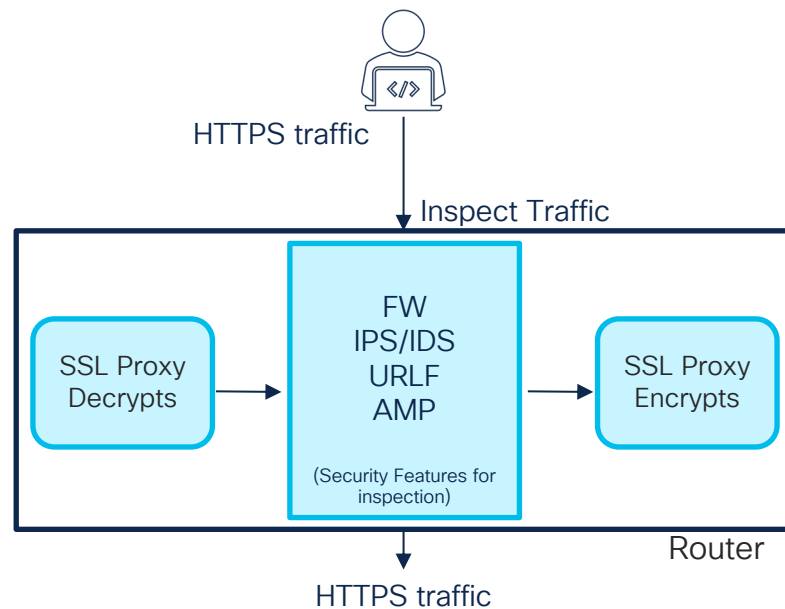
"At the start of 2019, 87% of Web traffic was encrypted"

- *Mary Meeker, Internet Trends*

Security: Umbrella integration

Auto-Registration to Cisco Umbrella based on Smart Account credentials:

- Registration of Edge Devices to Umbrella is automatically done

- Secure API key is automatically provisioned on the Edge Device through HTTPS session

IPSec Auto-Tunnel to Cisco Umbrella:

- By pushing the SIG Feature template, a customer can now setup an IPSec tunnel to Umbrella SIG

- Without this solution, customer would need to manually establish the tunnel for each WAN Edge device at branch

INTERNET

- Cloud Firewall
- DNS Security
- Secure Web Gateway

UMBRELLA

Edge Device
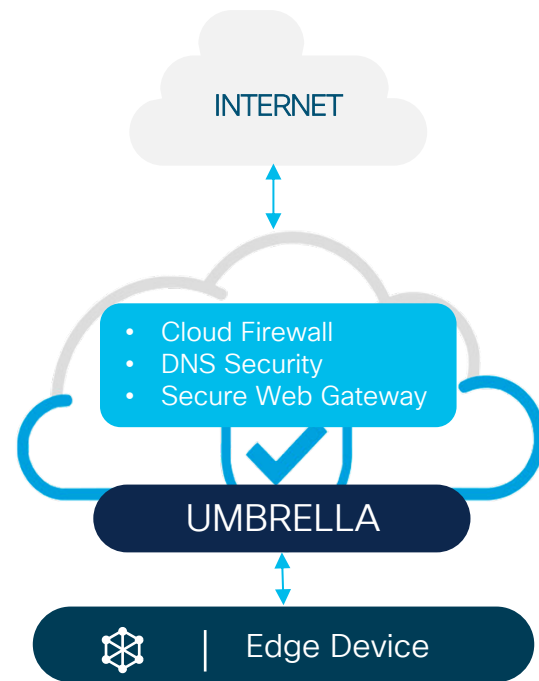
Layer 7 health check to ZScaler

- Redundant IPsec/GRE tunnels to ZScaler now support dynamic best path selection

- No longer reliant on IKE DPD for tunnel failure

- Supported on both vEdge and cEdge

- Ensures traffic takes the best path when redundant paths are available

Region 1   Region 2

HTTP Probe:
http://gateway.zscalerbeta.net/vpntest

Gi0/0

cEdge

Transport (VPN0)

| Service (VPN1) | Mgmt (VPN512) | Service (VPN2) |

Gi0/1   Gi0   Gi0/3

CISCO Live!
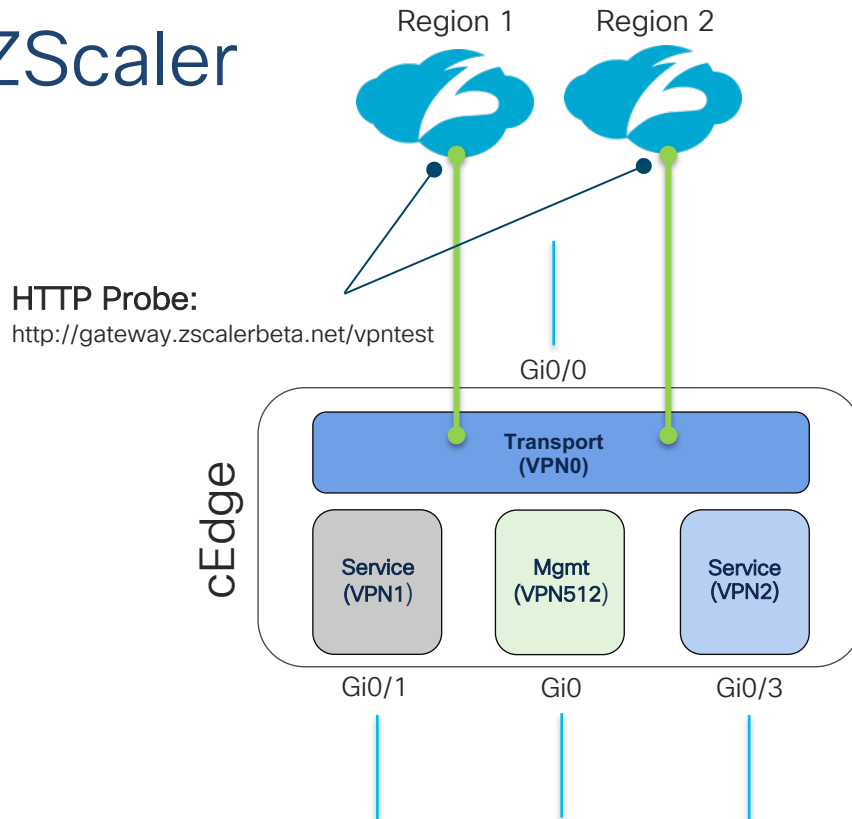
Transport-side IPsec/GRE Tunnels

- IPsec/GRE tunnels to 3rd party devices can now be sourced from VPN0 interfaces

- Supported on both vEdge and cEdge

- Conserves hardware resources

- Simplifies design

3rd Party

Gi0/0

cEdge

Transport (VPN0)

Service (VPN1)   Mgmt (VPN512)   Service (VPN2)

Gi0/1   Gi0   Gi0/3
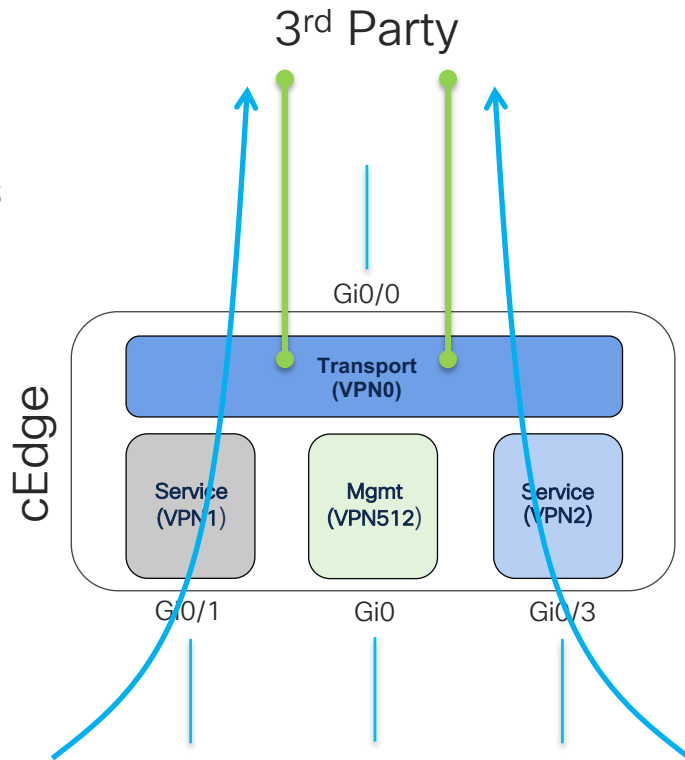
SD-WAN Security - Summary

Latest innovations:

- SSL Proxy

- Cisco Umbrella automation

- Layer 7 health check to ZScaler

- Transport-side IPsec/GRE Tunnels

Unified Communications

Key use cases

On-Premise UCM

UCM Cloud

WebEx Calling

3rd Party
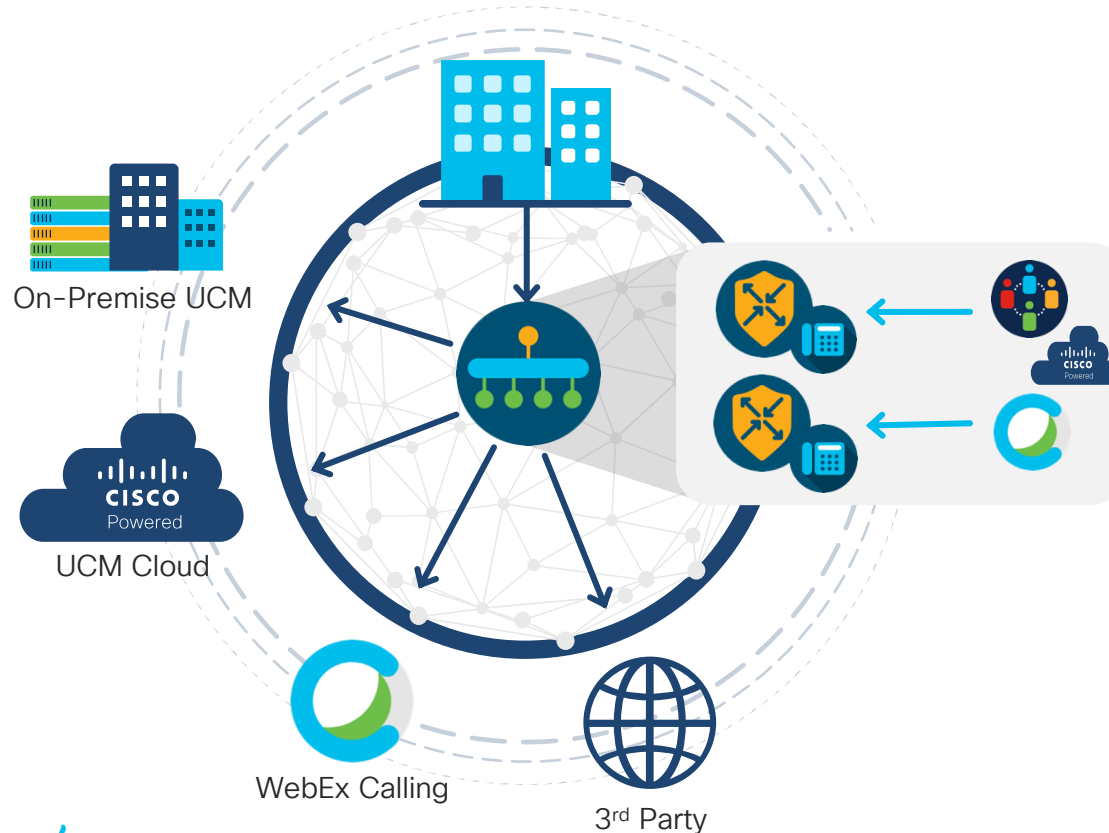
Flexible Connectivity

Directly connect with Cloud or On-Premise call control with improved user experience while positioning for the future

Large Scale VoIP Provisioning

Leverage the power of vManage Templating and Policy orchestration to provision scalable, consistent UC across the enterprise

Hardware Consolidation

Reduce CapEx and OpEx by consolidating UC and SD-WAN into a single CPE

Voice Module Support

Digital Voice Modules

Phase 2 (July)

- T1E1 Multiflex Trunk NIM Modules 1 - 8 Port
- PVDM4 – Packet Voice DSP Modules (DSPs) with 32 - 256 sessions
- High Density DSP Service Modules (SM–X–PVDMs)
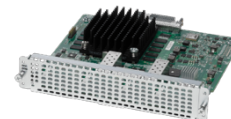
Analog Voice Modules

Phase 1 (April)

- FXS / FXO Voice NIM Modules 2 - 6 Ports
- High Density Analog Voice Service Modules
- BRI Voice NIM Modules 2 - 4 Ports
- E/M NIM Modules 4 Ports

UC Portfolio Summary

20Gb+

4400 / ASR architecture
Dedicated CPU sockets for Control & Data Plane

ISR 4461

1/10Gb

ISR 4451

1Gb

4300 architecture
Single socket CPU Multiple CPU cores

ISR 4431

ISR 4351

ISR 4331

100Mb

ISR 4321

Small Office | Branch Campus | Midsize Campus | Large Campus | Data Center | Cloud/Virtual
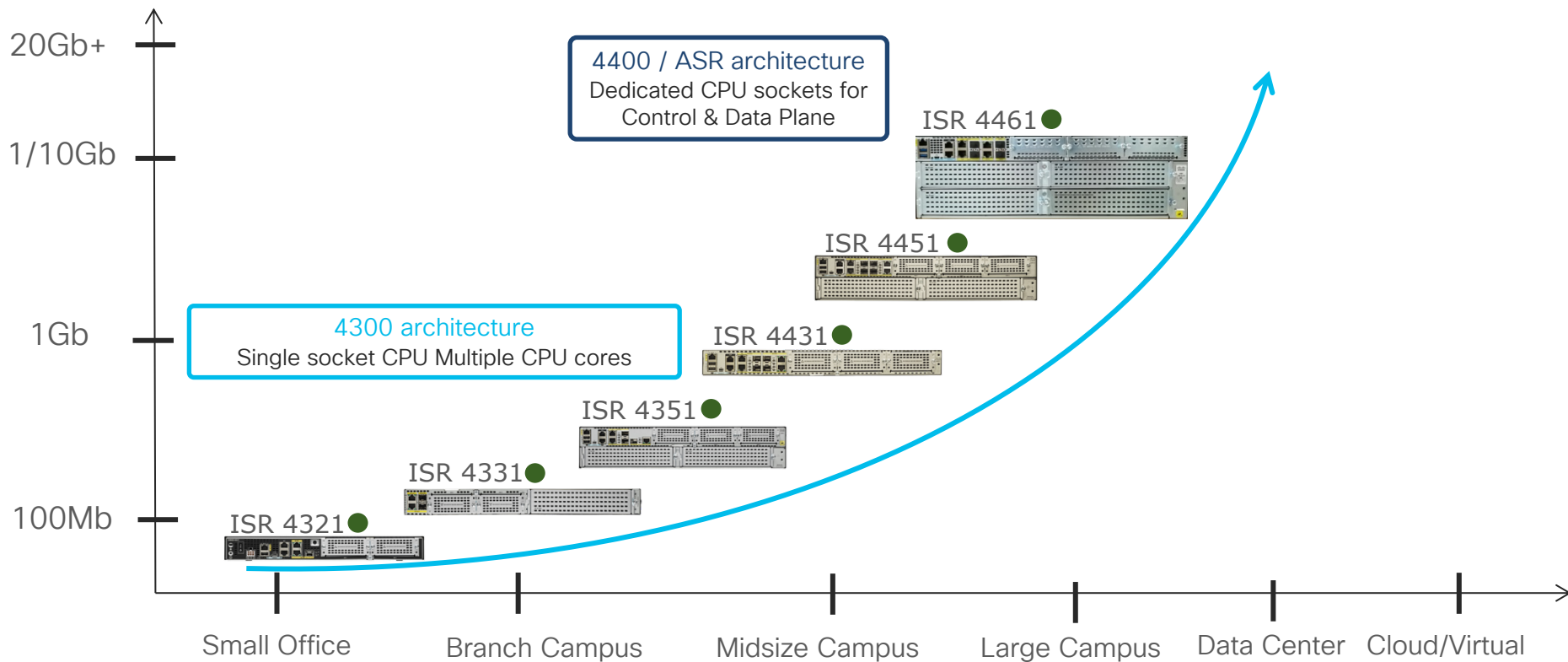
UC Configuration and Policy

vManage/vSmart

Does not participate in Call Routing

Provisions ISR for UC
- Distributed Dial Plan (SIP Dial Peer)
- Call Manipulation (Translation)
- Media/Codec Selection
- SRST

Management/Control Plane

Data Plane

Participates in Data Plane

Provides extended Dial Plan support
- Enterprise call routing
- Media Termination
- SIP

Does not invoke configuration change

Call Control

PSTN

Basic Workflow

①

Feature Template
- ✓ Call Routing
- ✓ Voice Card
- ✓ SRST

②

Voice-Policy
- ✓ Translation-Profile
- ✓ Line Parameters
- ✓ SIP Media Profile

③

Device Template
- ✓ Map Feature Templates
- ✓ Map Voice-Policy Elements

Configuration Snippet

```
voice register pool 1
 voice-class codec 1
 dtmf-relay rtp-nte sip-notify
!
```

```
sip-ua
voice class codec 1
 codec preference 1 g722-64 bytes 160
 codec preference 2 g729r8
 codec preference 3 g711ulaw bytes 160
!
voice class codec 2
 codec preference 1 g722-64 bytes 160
 codec preference 2 g729r8
 codec preference 3 g711ulaw bytes 160
!
```

```
voice-card 0/2
 no local-bypass
```

```
dial-peer voice 2 voip
 voice-class codec 2
 session protocol sipv2
 dtmf-relay rtp-nte digit-drop sip-notify
!
dial-peer voice 100 voip
 destination-pattern .T
 no shutdown
 session protocol sipv2
 session target ipv4:10.21.24.35
!
dial-peer voice 101 pots
 incoming called-number .
 port     0/2/0
 no shutdown
!
dial-peer voice 911 pots
 destination-pattern 911
 forward-digits all
 port          0/2/0
 no shutdown
!
```

Voice Policy

SIP Template

```
voice service voip
 allow-connections sip to sip
 no supplementary-service sip handle-replaces
 no supplementary-service sip moved-temporarily
 no supplementary-service sip refer
 sip
  registrar server expires max 300 min 200
  bind control source-interface GigabitEthernet0/0/0
  bind media source-interface GigabitEthernet0/0/0
 !
 ip address trusted list
  ipv4 10.0.0.0 255.0.0.0
 !
 fax protocol t38
!
```

```
voice register global
 max-dn   48
 max-pool 24
 system message "SRST Mode"
!
```

SRST Template

Voice-Card Template

```
voice-port 0/2/0
 caller-id enable
 secondary dialtone
!
```

UC Call Flow Review (CLI)

show voip rtp connections

```
ROUTER# show voip rtp connections
VoIP RTP Port Usage Information:
Max Ports Available: 19999, Ports Reserved: 101, Ports in Use: 1
Port range not configured
Min Max Ports Ports Ports
Media-Address Range Port Port Available Reserved In-use
----------------------------------------------------------------------
Global Media Pool 8000 48198 19999 101 1
----------------------------------------------------------------------
VoIP RTP active connections :
No. CallId dstCallId LocalRTP RmtRTP LocalIP RemoteIP MPSS VRF
1 439 440 8018 32398 10.104.55.216 10.104.55.62 NO NA
Found 1 active RTP connections
```

show voice call status

```
ROUTER# show voice call status
CallID   CID   ccVdb        Port       Slot/DSP:Ch   Called #        Codec      MLPP Dial-peers
0x3B5    1C2D  0x1B7F03C8   50/0/115.0               0502289600     g711alaw   20114/102
0x6EF    2525  0x1B996AB0   50/0/130.0               0554322189     g711alaw   20129/102
2 active calls found
```

debug ccapi calls

```
ROUTER# debug voice ccapi calls
Call 23 set InfoType to SPEECH
*Mar 4 11:53:26.605: //-1/xxxxxxxxxxx/SIP/Info/ccsip_process_tcp_queue_event: Event type: send msg, connid: 6, fd: 0
ACK sip:7002@10.104.55.65:5060 SIP/2.0
Via: SIP/2.0/TCP 10.104.55.55:5060;branch=z9hG4bK974E
From: <sip:10.104.55.55>;tag=21A32655-182
To: <sip:7002@10.104.55.65>;tag=31978359
Date: Wed, 04 Mar 2020 11:53:26 GMT
Call-ID: 979D8058-5D4511EA-8049E498-283111D1@10.104.55.55
Max-Forwards: 70
CSeq: 101 ACK
Allow-Events: telephone-event
Session-ID: 00000000000000000000000000000000;remote=83b54a01625b52269d3f4987ea9ce152
Content-Length: 0
```

Cisco Cloud UC (UCaaS) Overview

- Enterprise unified communications and collaboration as a service from the Cloud

- Powered by Cisco's Unified Communications Manager and Webex in the cloud

- Hosted and operated by Cisco

- Webex Teams, Webex Meetings, Jabber, and all Cisco collaboration endpoints supported

- Cloud Calling option in Collaboration FLEX Plan
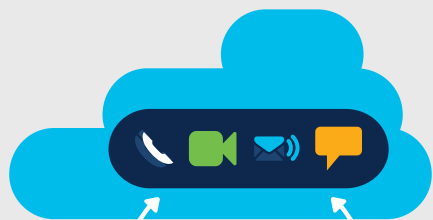
Cisco UCM Cloud

Cisco UCOne

Cisco Webex Teams

Cisco Webex Meetings

Cisco Webex Calling

UC: key takeaways

- Phase 1 introduces SIP only support for SRST and analog

- SD-WAN + UC enhances VoIP provisioning and consistency

- SD-WAN + UC will position for the future (UCaaS)

- SD-WAN + UC consolidates hardware

Multicast

Multicast support comes to SD-WAN

IOS XE SD-WAN's multicast supports sending data to multiple destinations
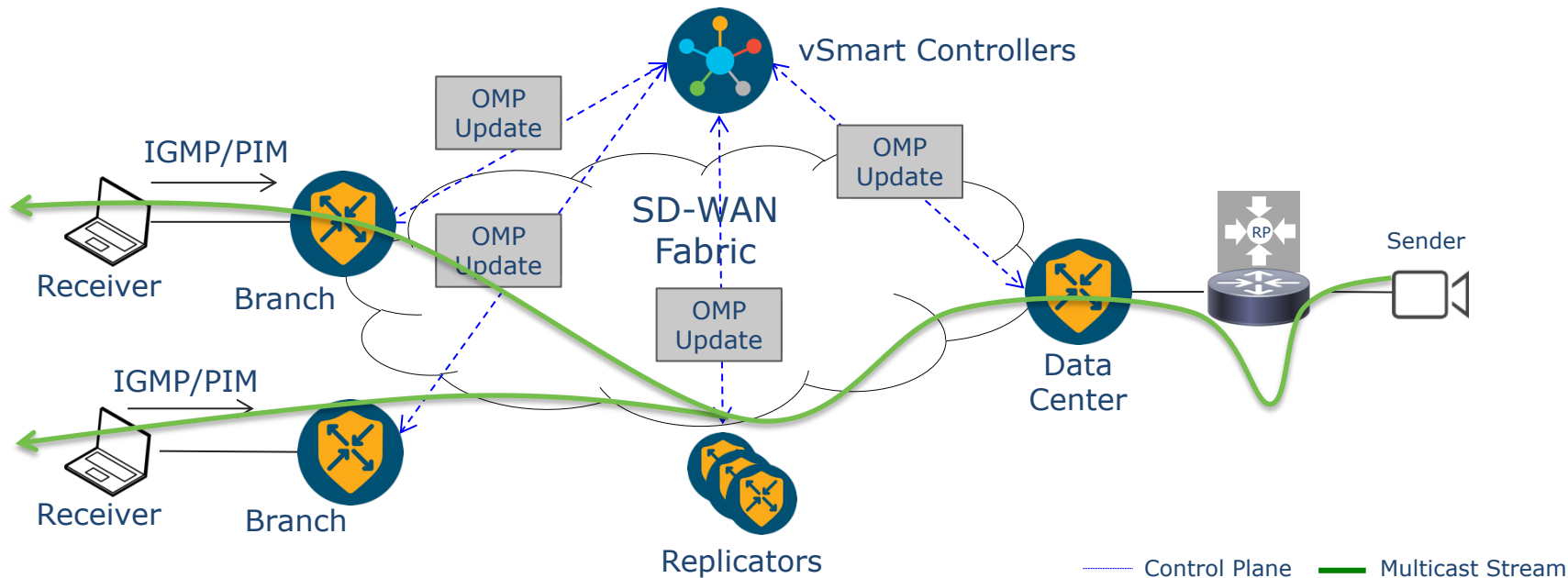
- cEdges interoperate with IGMP v2/v3 and PIM on the service side
- cEdges advertise receiver multicast groups using OMP
- cEdge Replicators replicate multicast stream to receivers
- Multicast is encapsulated in point-to-point tunnels

SDWAN Overlay Multicast – vEdge vs cEdge – 20.1/17.2

Feature	vEdge	cEdge
Overlay Multicast – PIM ASM		
Replicator		
Auto RP – Proxy		
IGMP V2		
IPSec and GRE Encapsulation		
ECMP across multiple TLOCs		
Overlay Multicast – PIM SSM		
WAN Edge RP Functionality		
Static RP		
Auto-RP (Candidate RP and Mapping-Agent)		
IGMP V3		

Caveats

SD-WAN Feature Limitation (17.2)

× SD-WAN Application Aware Routing
× TLOC-Extension with Multicast

Multicast Features - Unsupported

× PIM Bidir
× AnycastRP/MSDP(Across WAN)
× Multicast BSR
× IPv6 Overlay Multicast
× IPv6 underlay Multicast

Multicast: key takeaways

- Cisco ISRs/ASRs now support multicast

- SD-WAN XE introduces support for PIM, IGMPv3 and RP

- Cisco SD-WAN now fully supports IPv4 multicast across all platforms

SD-WAN Infra features

Summary of the key infra SD-WAN features

- Single Image for IOS-XE and IOS-XE SD-WAN

- CLI add-on templates

- Per-Tunnel QoS support on SD-WAN

- AppNav-XE with SD-WAN

Single Image for IOS-XE and IOS-XE SD-WAN

IOS-XE
'Autonomous'
mode

SINGLE
IMAGE

IOS-XE
SD-WAN
'Controller'
mode
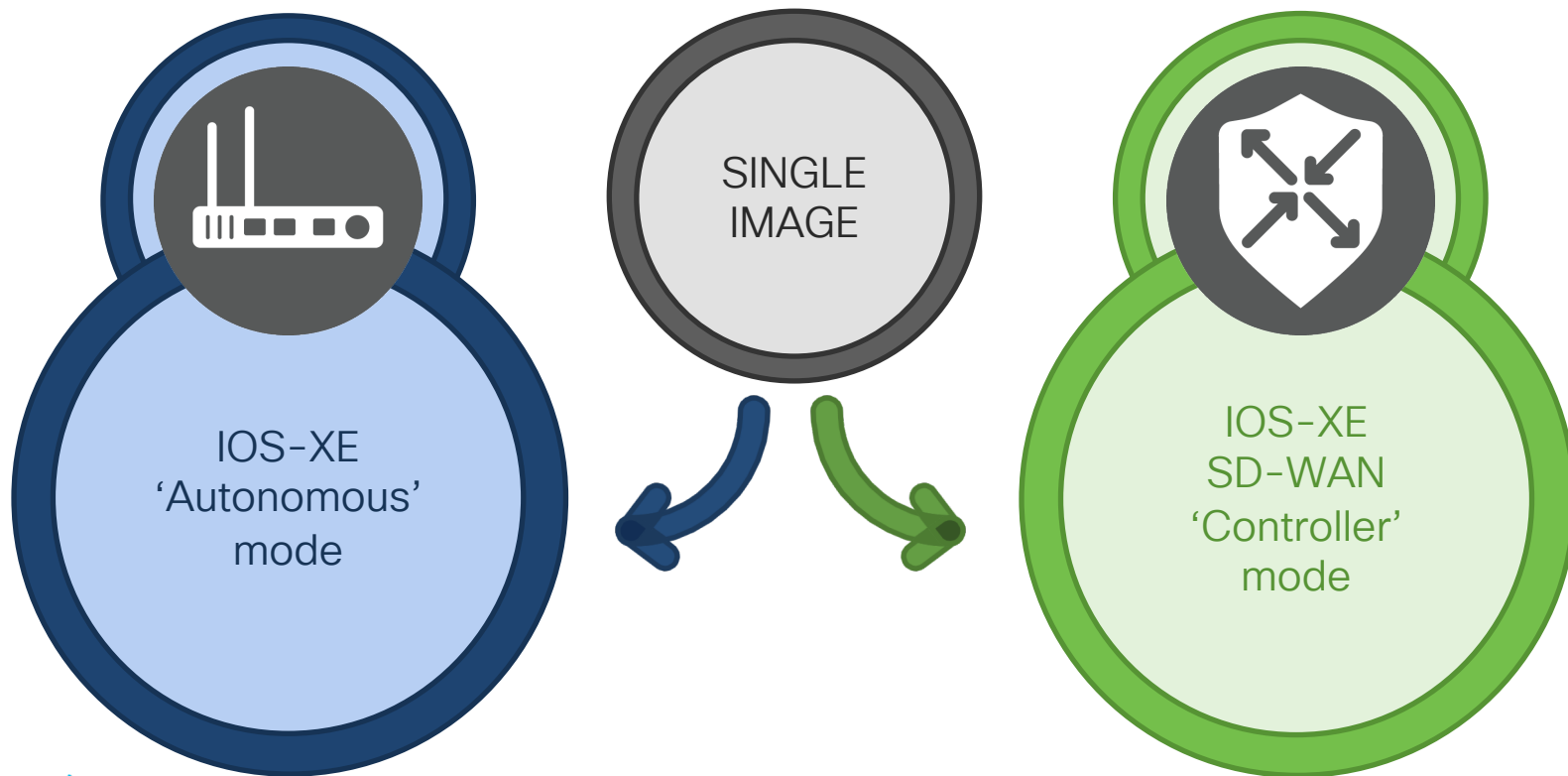
IOS XE vs IOS XE SD-WAN

'AUTONOMOUS' mode

- Only non SD-WAN use-cases are supported

- Autonomous mode is default mode in boot sequence

- Can be configured using exec CLI
  - 'controller-mode disable'

'CONTROLLER' mode

- Only SD-WAN use-cases are supported

- Controller mode requires a second reboot

- Can be configured using exec CLI
  - 'controller-mode enable'

Operational Mode Change

```
Router# controller-mode ?
    disable    controller-mode disable
    enable     controller-mode enable
    reset      controller-mode reset
```
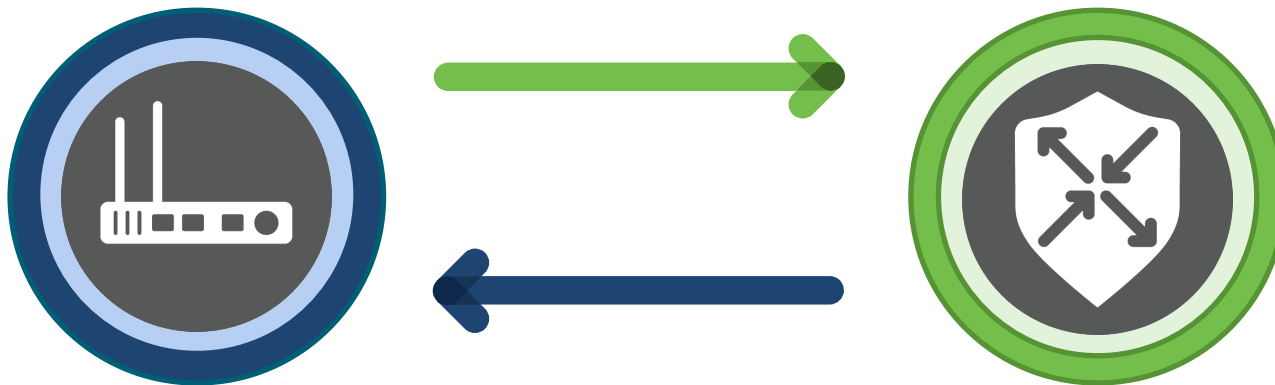

Change to Autonomous Mode
- Config lost, device in day-0

Change to Controller Mode
- Config lost, device in day-0

CLI Add-On Templates

Use Case:

- Needed feature or functionality does not yet exist in a vManage Feature Template

- Caveat or bug workaround

Solution:

- Configure Device Template as normal

- Attach CLI Add-On Template to append configuration

- Supported Commands

CLI Add-On Template

Device Template

Per-Tunnel QoS support on SD-WAN

Per-Tunnel QoS allows a site to dynamically adjust the sending rate of its traffic to accommodate lower bandwidth circuits at remote locations.


```
sdwan
 interface GigabitEthernet2
  tunnel-interface
   encapsulation ipsec
   color Internet restrict
   tunnel-qos spoke
  exit
  bandwidth-downstream 9000
 exit
```
Branch 1

```
sdwan
 interface GigabitEthernet2
  tunnel-interface
   encapsulation ipsec
   color Internet restrict
   tunnel-qos hub
  exit
exit
```
Data Center

```
sdwan
 interface GigabitEthernet2
  tunnel-interface
   encapsulation ipsec
   color Internet restrict
   tunnel-qos spoke
  exit
  bandwidth-downstream 8000
 exit
```
Branch 2

Adaptive QoS introduced in 17.3 IOS XE

Ability to detect the current bandwidth rate for the WAN circuit and dynamically update the interface shaper and egress queue bandwidth values.

Per-tunnel QoS
DC to Branch1 Overlay Shaper:
Range 5000~15000 Kbps
Default 10000 Kbps

Per-tunnel QoS
DC to Branch2 Overlay Shaper:
Range 10000~30000 Kbps
Default 20000 Kbps

Branch1 to DC Physical Shaper:
Range 8000~12000 Kbps
Default 10000 Kbps

Branch2 to DC Physical Shaper:
Range 16000~24000 Kbps
Default 20000 Kbps

```
sdwan
 interface GigabitEthernet1
  qos-adaptive
   period 30
   downstream range 5000 15000
   downstream 10000
   upstream range 8000 12000
   upstream 10000
  !
 !
!
```
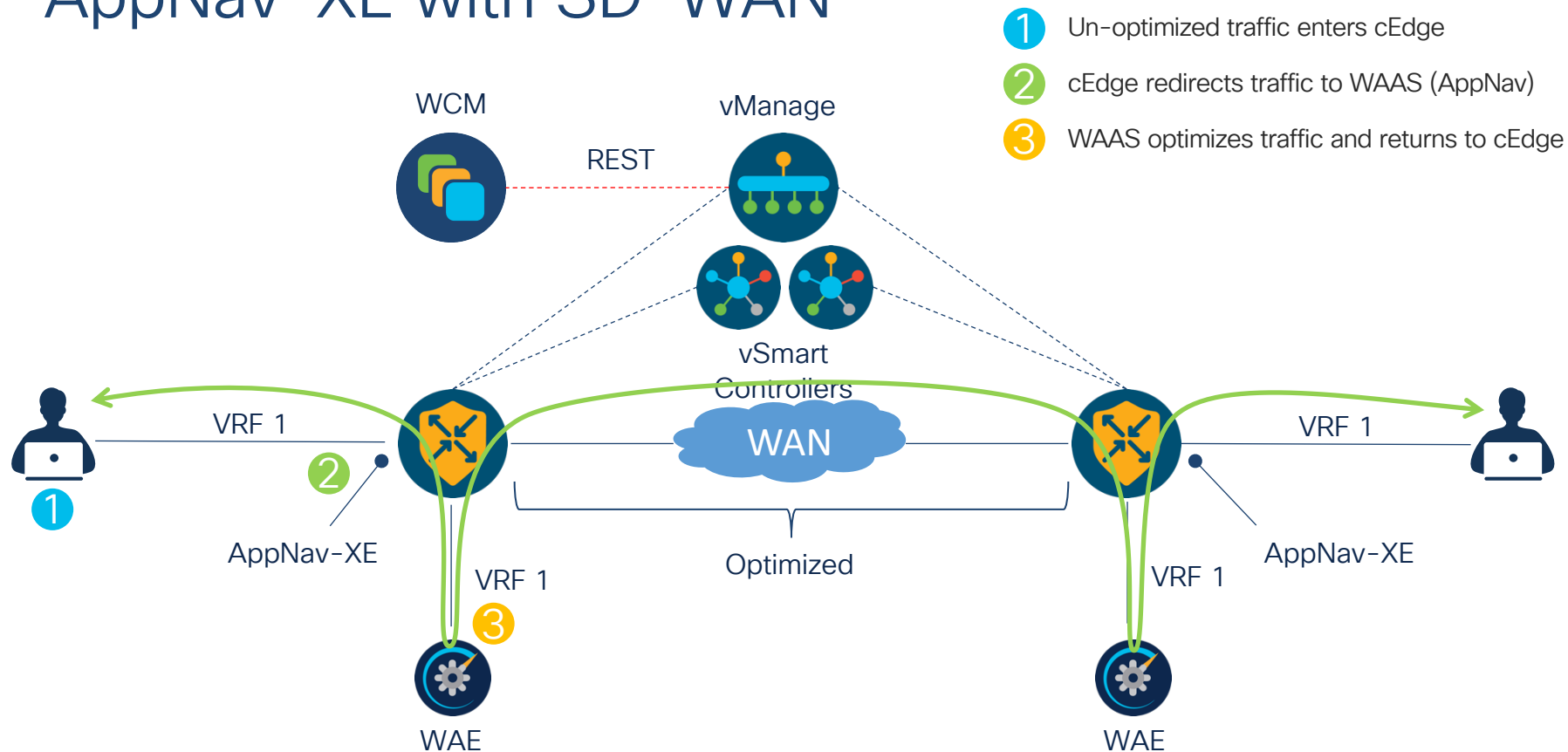
```
sdwan
 interface GigabitEthernet2
  qos-adaptive
   period 60
   downstream range 10000 30000
   downstream 20000
   upstream range 16000 24000
   upstream 20000
  !
 !
!
```

AppNav-XE with SD-WAN

1. Un-optimized traffic enters cEdge
2. cEdge redirects traffic to WAAS (AppNav)
3. WAAS optimizes traffic and returns to cEdge

Summary of the key infra SD-WAN features

- Single Image for IOS-XE and IOS-XE SD-WAN

- CLI add-on templates

- Per-Tunnel QoS support on SD-WAN

- AppNav-XE with SD-WAN

Conclusion

- See DGTL-BRKCRS-2110 from CL Barcelona 2020 for SD-WAN fundamentals available at the on-demand library

- Key SD-WAN innovations since January 2020 are:
  1. Cloud: Google Cloud, AWS TGW and Azure vWAN automation, SaaS
  2. Unified Communication
  3. Security: SSL proxy, Umbrella automation
  4. Multicast
  5. Infra: single image, CLI add-on templates, per tunnel QoS, AppNav

Thank you

#CiscoLive