Say hello
to the future.

Cisco Connect 2019

Hanoi, Vietnam. 4th April 2019

#CiscoConnectVN

Cisco SD-WAN: Unrivalled Flexibility and Security at the Network Edge

Rajinder Singh

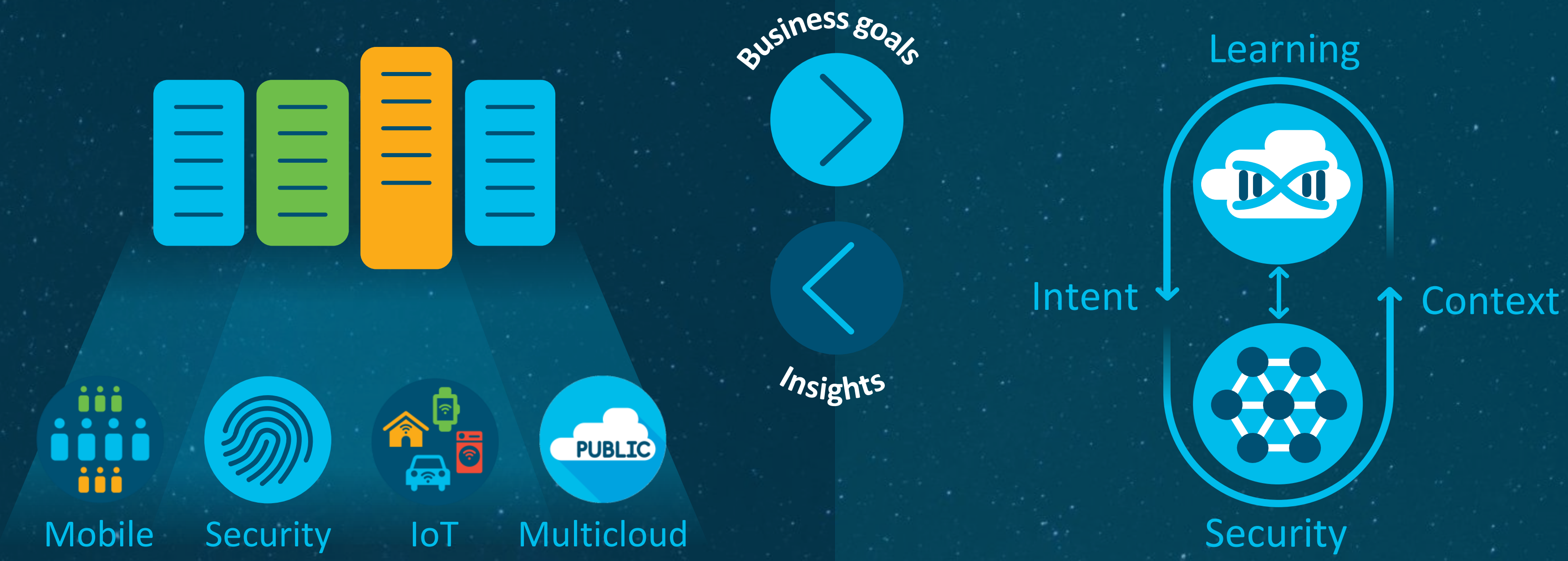
Product Sales Specialist

Cisco ASEAN

Intent-based networking with Cisco

Digital business

Network



Business goals

Insights

Mobile

Security

IoT

Multicloud

Learning

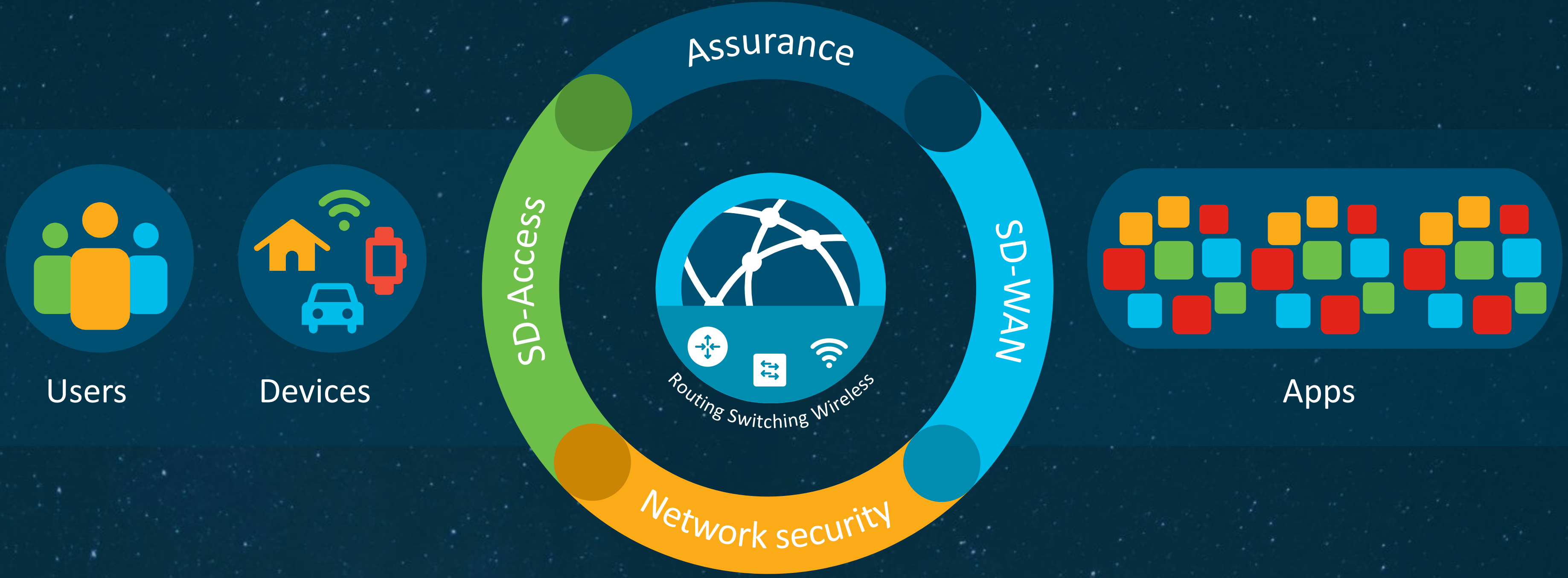
Intent

Context

Security

Powered by intent. Informed by context.

Cisco intent-based networking solutions



Connecting trusted users to trusted devices with an uncompromised experience

The Cisco SD-WAN portfolio

Powered By

cisco Meraki

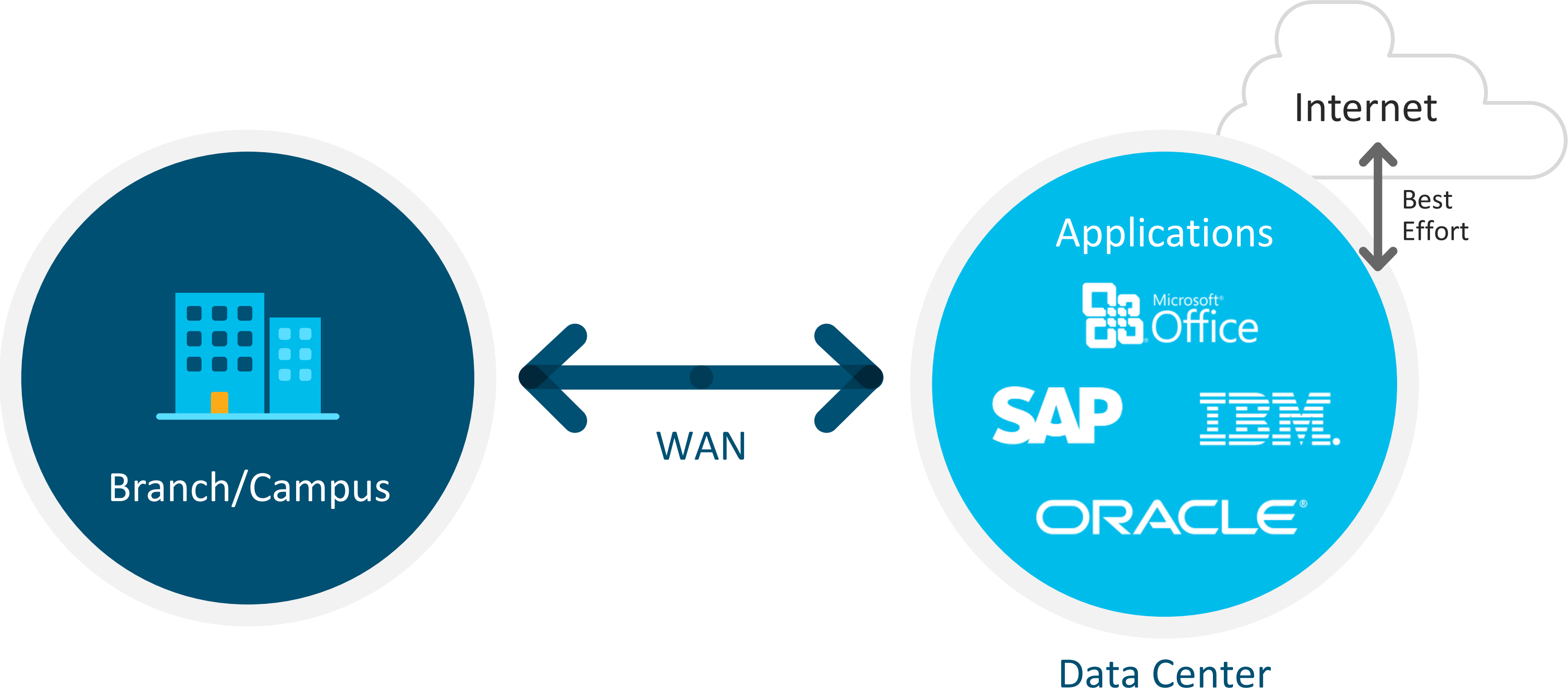
Full stack branch management for Lean IT

SD-WAN

viptela

Flexible and sophisticated with secure segmentation and advanced routing

Connecting Users to the Data Center was the Priority



Internet

Best Effort

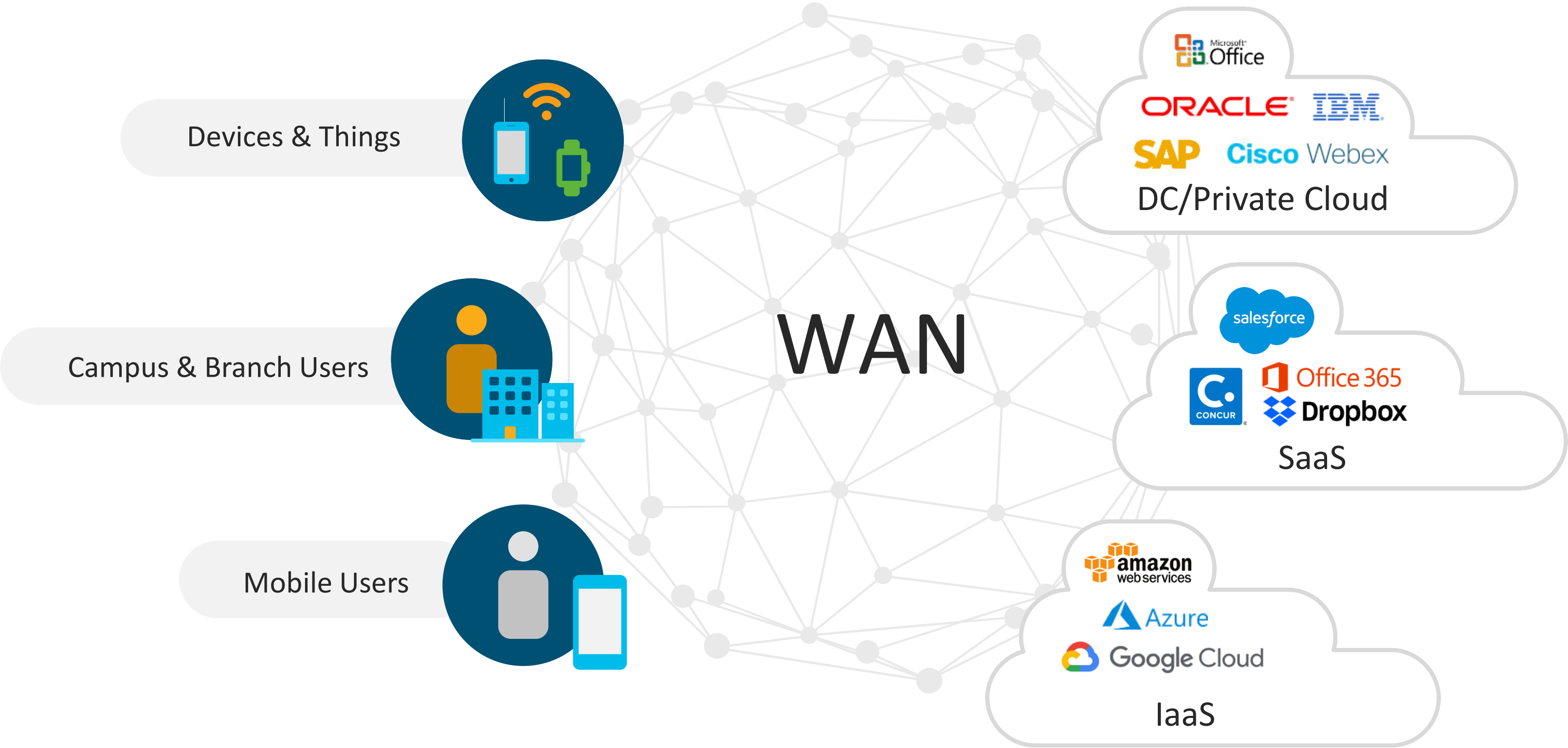
Branch/Campus

WAN

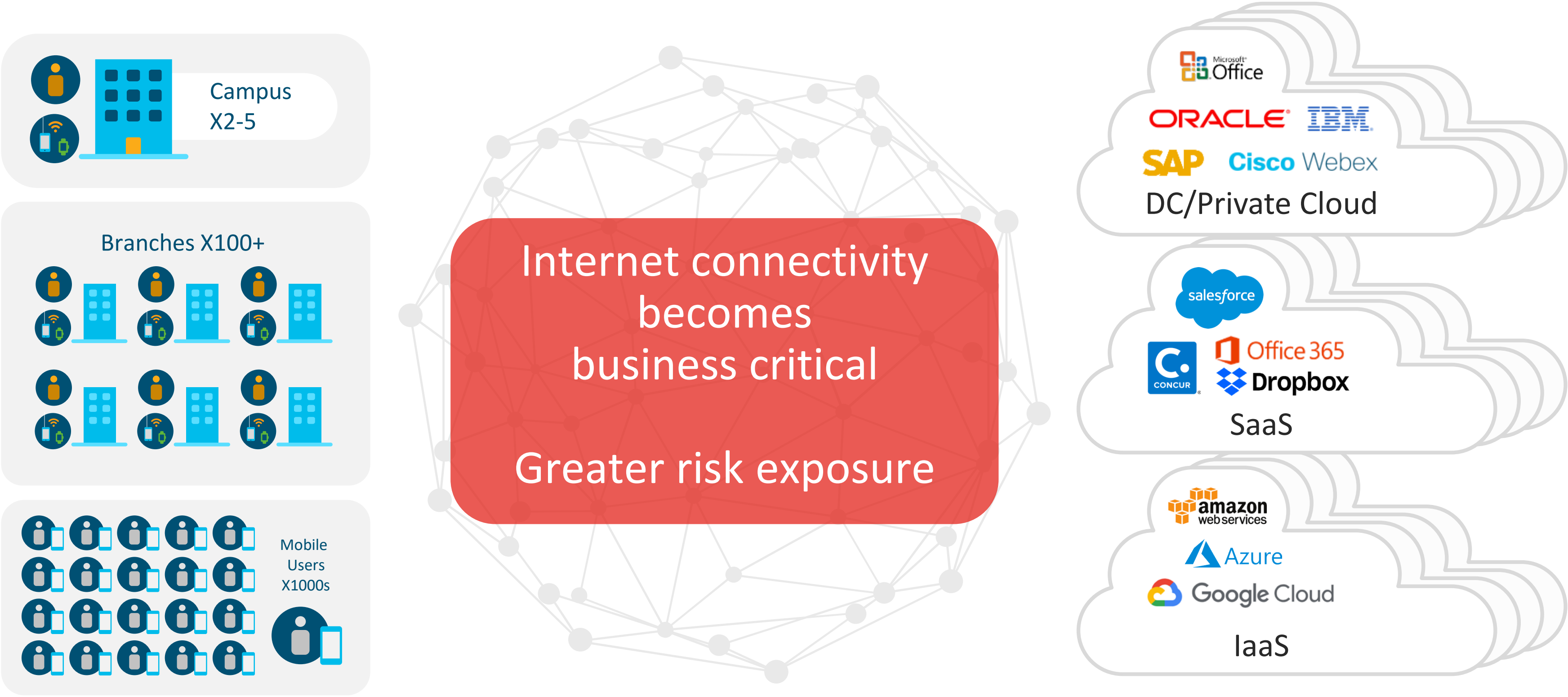
Applications

Data Center

Applications Moving to Not One Cloud, But Many



Resulting a highly complex and dynamic network



Campus X2-5

Branches X100+

Mobile Users X1000s

Internet connectivity becomes business critical

Greater risk exposure

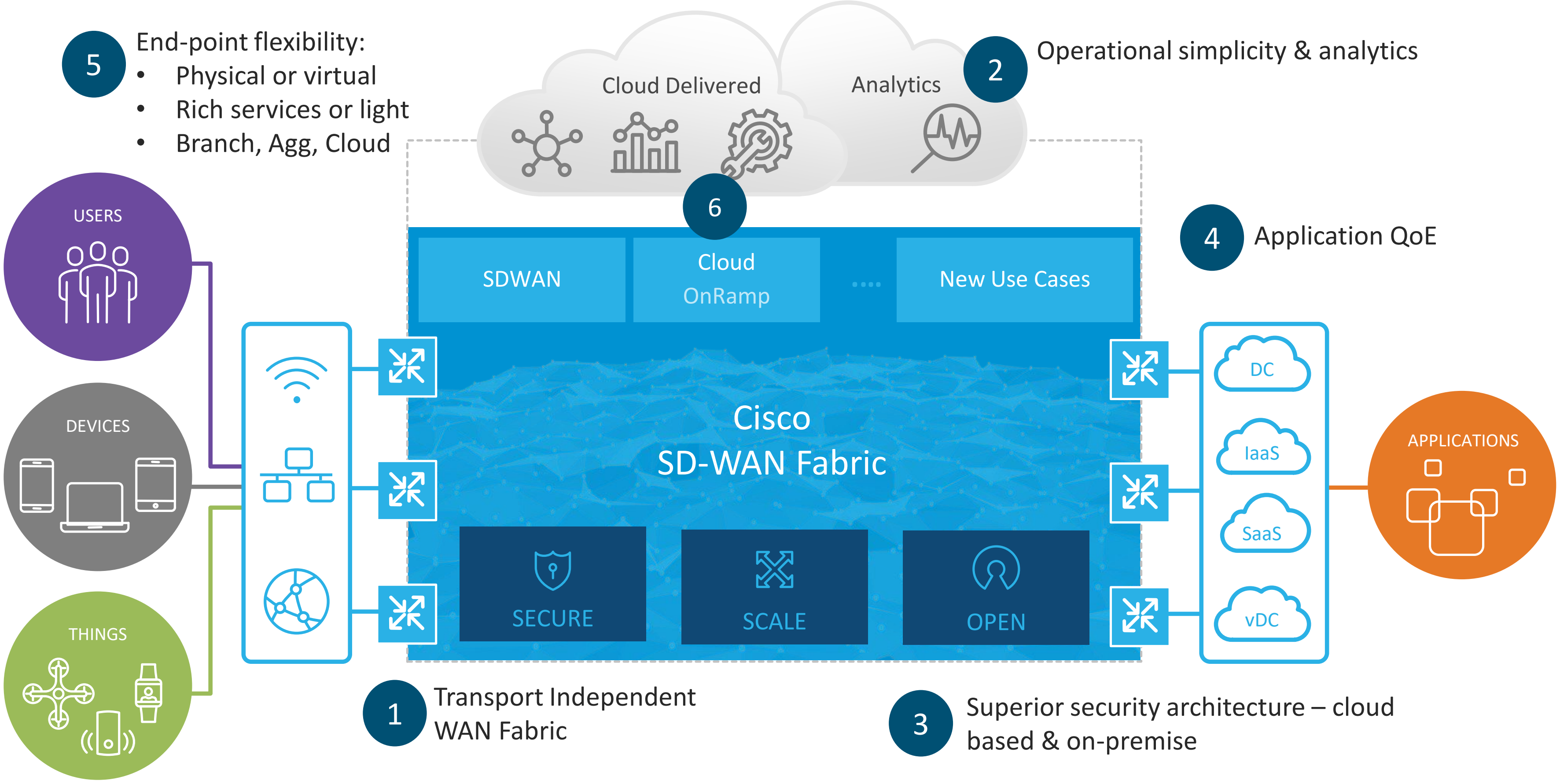
DC/Private Cloud

SaaS

IaaS

More user, things and applications, everywhere

Cisco SD-WAN Solution Differentiation



5 End-point flexibility:

- Physical or virtual
- Rich services or light
- Branch, Agg, Cloud

2 Operational simplicity & analytics

4 Application QoE

1 Transport Independent WAN Fabric

3 Superior security architecture – cloud based & on-premise

Cisco SD-WAN: Cloud Architecture

Management Plane

- Single pane of glass
- Monitoring and Troubleshooting
- RBAC and APIs

Control Plane

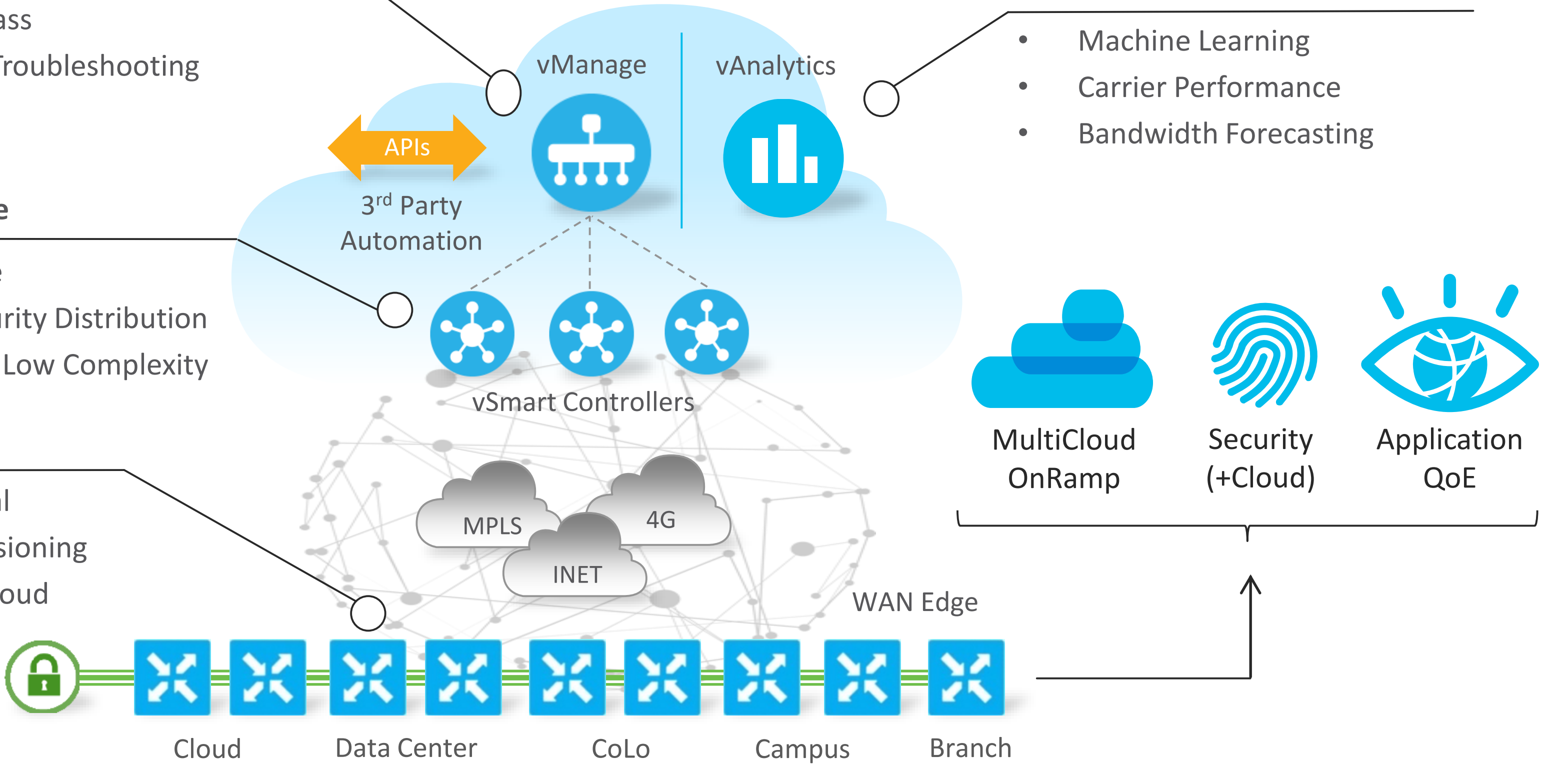
- SDN Architecture
- Routing and Security Distribution
- Horizontal Scale, Low Complexity

Data Plane

- Physical of Virtual
- Zero Touch Provisioning
- On-Premise or Cloud

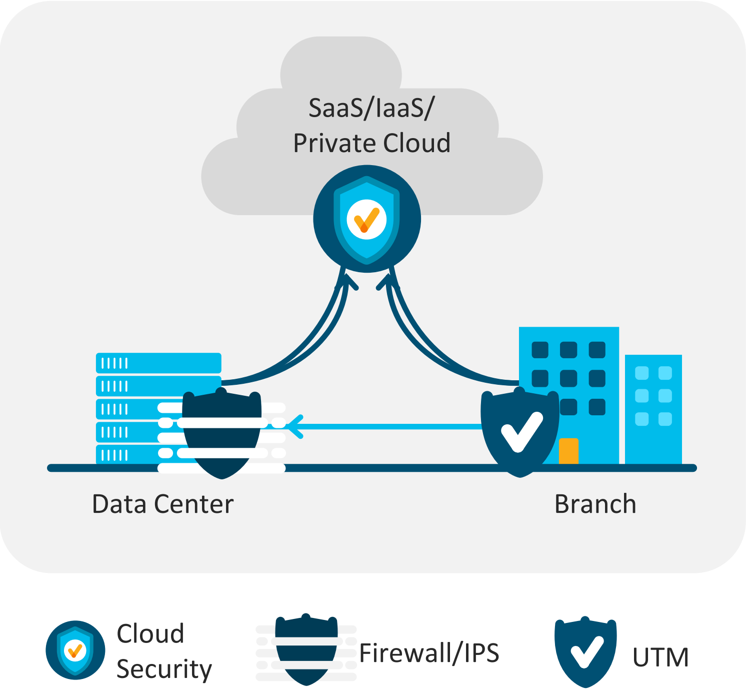
Analytics

- Machine Learning
- Carrier Performance
- Bandwidth Forecasting



SD-WAN Security

Challenges balancing security and user experience



1. Continue Backhauling

Pro: Security is simple

Con: Poor user experience

2. DIA via Cloud Security

Pro: Improves user experience

Con: Limited control

3. DIA via UTM

Pro: Improves user experience

Con: Complex to manage

4. Security Everywhere

Pro: Efficient traffic flows for experience

Con: Difficult to maintain policy

How can IT maintain choice and control connecting a cloud-first world?

Introducing new Cisco SD-WAN software

Full-Stack Security

Integrated Firewall, IPS and URL-Filtering on SD-WAN platforms

Simplified Cloud Security

Cisco Umbrella

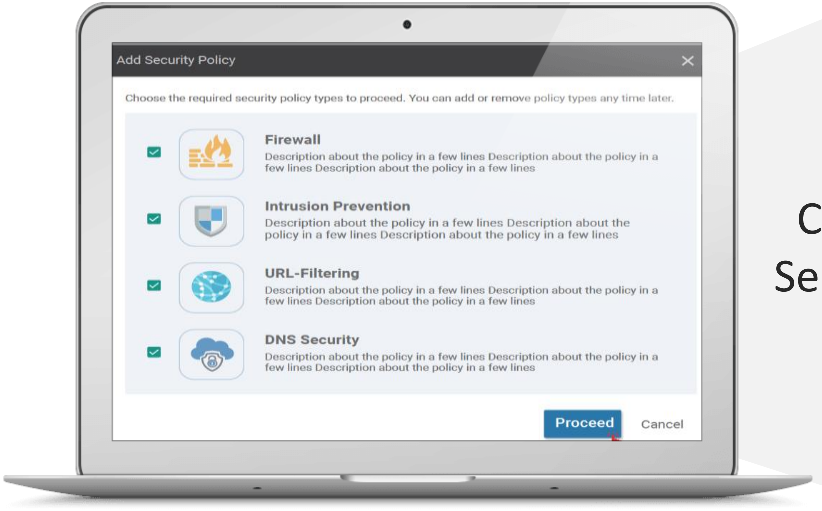
Faster deployment and greater visibility with Cisco Umbrella

40% Faster Office 365 performance

Increased reliability and utilization of all available paths with OnRamp

One console for SD-WAN and network security simplifies management

Combining Best of Breed in Security and SD-WAN



Add Security Policy ✕

Choose the required security policy types to proceed. You can add or remove policy types any time later.

☑ **Firewall**
Description about the policy in a few lines Description about the policy in a few lines Description about the policy in a few lines

☑ **Intrusion Prevention**
Description about the policy in a few lines Description about the policy in a few lines Description about the policy in a few lines

☑ **URL-Filtering**
Description about the policy in a few lines Description about the policy in a few lines Description about the policy in a few lines

☑ **DNS Security**
Description about the policy in a few lines Description about the policy in a few lines Description about the policy in a few lines

Cisco SD-WAN

Cisco Security

Enterprise Firewall
+1400 layer 7 apps classified

Intrusion Protection System
Most widely deployed IPS engine in the world

URL-Filtering
Web reputation score using 82+ web categories

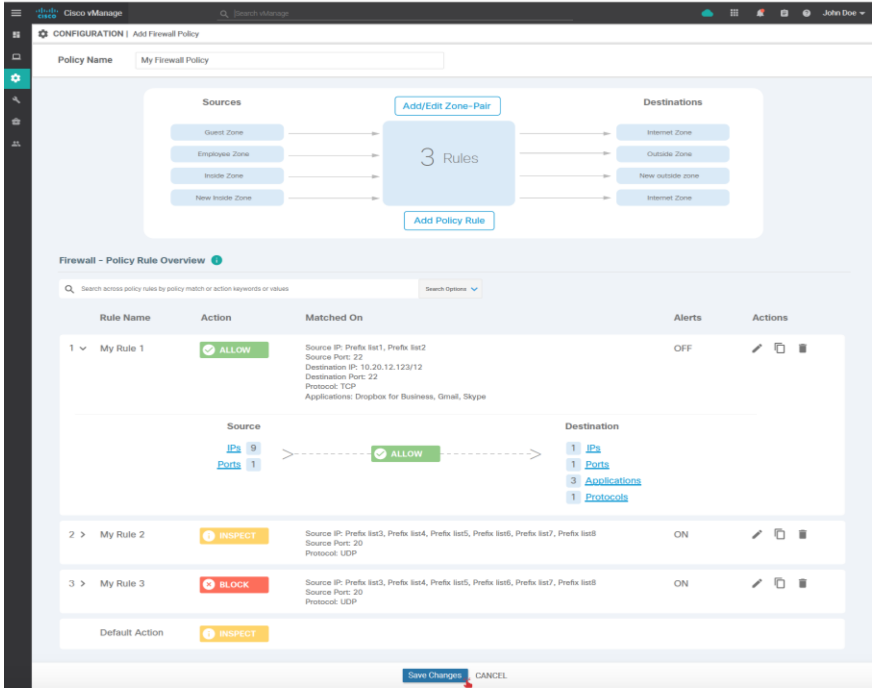
Adv. Malware Protection*
With File Reputation and Sandboxing

Simplified Cloud Security
Easy Deployment for Cisco Umbrella

*Roadmap Mar ‘19

One security architecture across Viptela and Meraki powered by TALOS

Simplify Management and Configuration

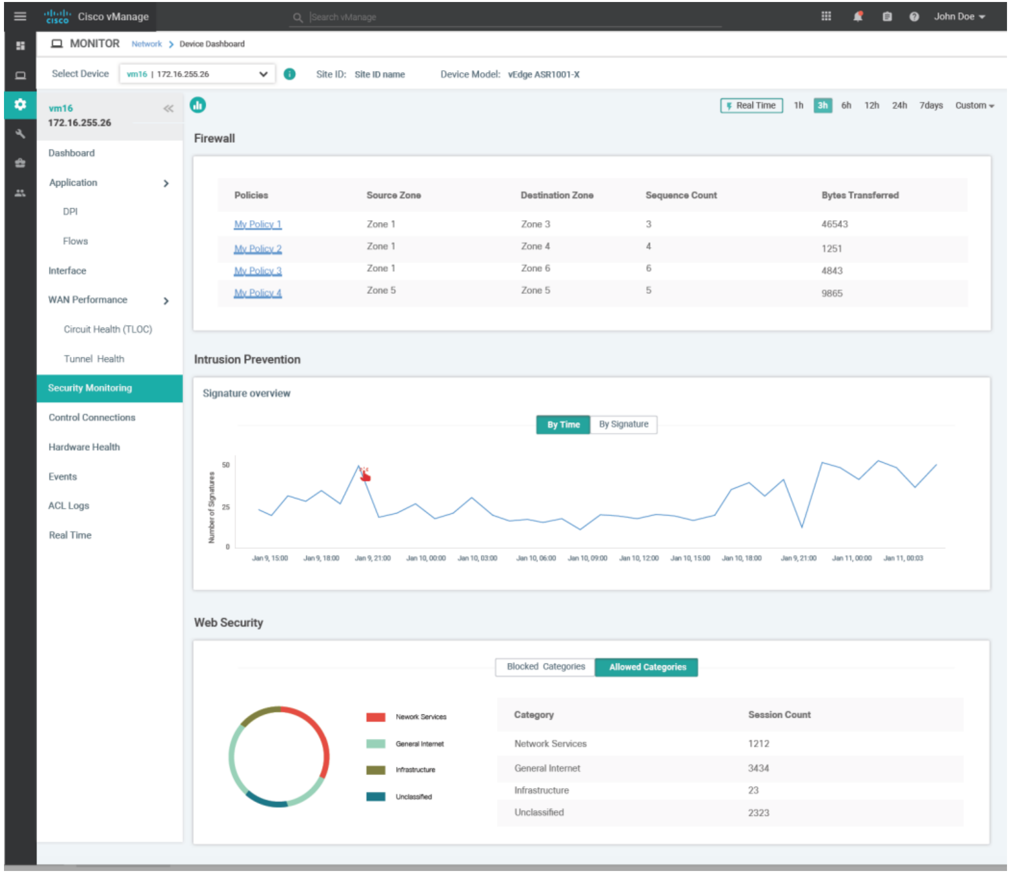


Policy Name: My Firewall Policy

Firewall – Policy Rule Overview

	Rule Name	Action	Matched On	Alerts
1	My Rule 1	ALLOW	Source IP: Prefix list1, Prefix list2 Source Port: 22 Destination IP: 10.20.12.123/12 Destination Port: 22 Protocol: TCP Applications: Dropbox for Business, Gmail, Skype	OFF
2	My Rule 2	INSPECT	Source IP: Prefix list3, Prefix list4, Prefix list5, Prefix list6, Prefix list7, Prefix list8 Source Port: 20 Protocol: UDP	ON
3	My Rule 3	BLOCK	Source IP: Prefix list3, Prefix list4, Prefix list5, Prefix list6, Prefix list7, Prefix list8 Source Port: 20 Protocol: UDP	ON
	Default Action	INSPECT		

My Rule 1 — Source: IPs 9, Ports 1 → ALLOW → Destination: 1 IPs, 1 Ports, 3 Applications, 1 Protocols



Select Device: vm16 | 172.16.255.26   Site ID: Site ID name   Device Model: vEdge ASR1001-X

Firewall

Policies	Source Zone	Destination Zone	Sequence Count	Bytes Transferred
My Policy 1	Zone 1	Zone 3	3	46543
My Policy 2	Zone 1	Zone 4	4	1251
My Policy 3	Zone 1	Zone 6	6	4843
My Policy 4	Zone 5	Zone 5	5	9865

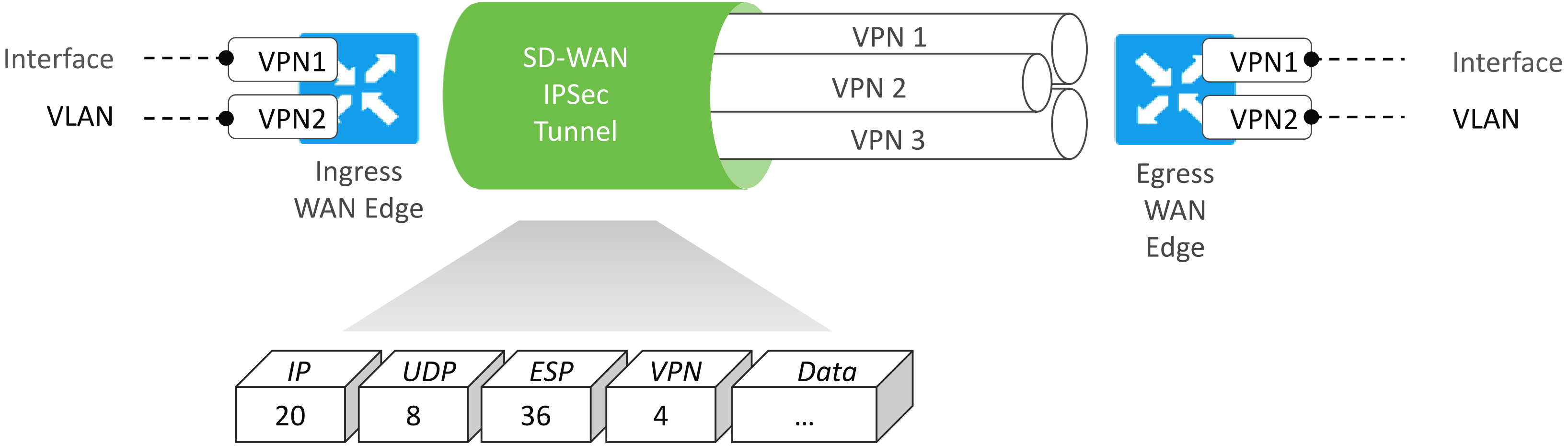
Intrusion Prevention

Signature overview

Web Security

Category	Session Count
Network Services	1212
General Internet	3434
Infrastructure	23
Unclassified	2323

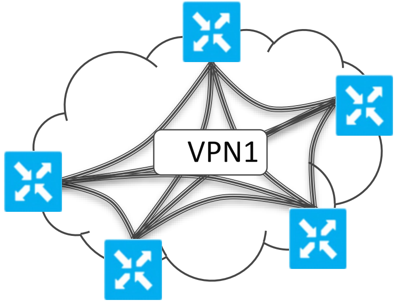
End-to-End Segmentation



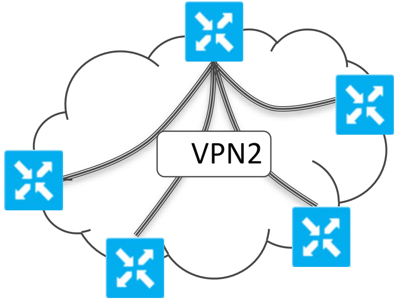
- Segment connectivity across fabric w/o reliance on underlay transport
- WAN Edge routers maintain per-VPN routing table
- Labels are used to identify VPN for destination route lookup
- Interfaces and sub-interfaces (802.1Q tags) are mapped into VPNs

Arbitrary VPN Topologies

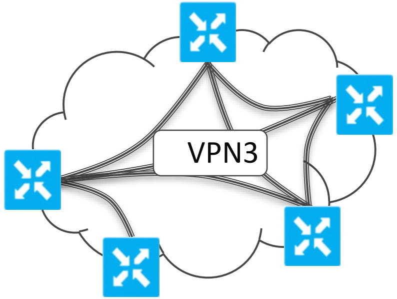
Full-Mesh



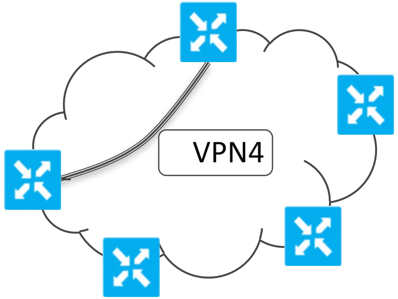
Hub-and-Spoke



Partial Mesh



Point-to-Point



- Each VPN can have it’s own topology
  - Full-mesh, hub-and-spoke, partial-mesh, point-to-point, etc…
- VPN topology can be influenced by leveraging control policies
  - Filtering TLOCs or modifying next-hop TLOC attribute for OMP routes
- Applications can benefit from shortest path, e.g. voice takes full-mesh topology
- Security compliance can benefit from controlled connectivity topology, e.g. PCI data takes hub-and-spoke topology

Cloud Innovations

How are customers accessing SaaS today

No DIA

Users have to back-haul for internet access

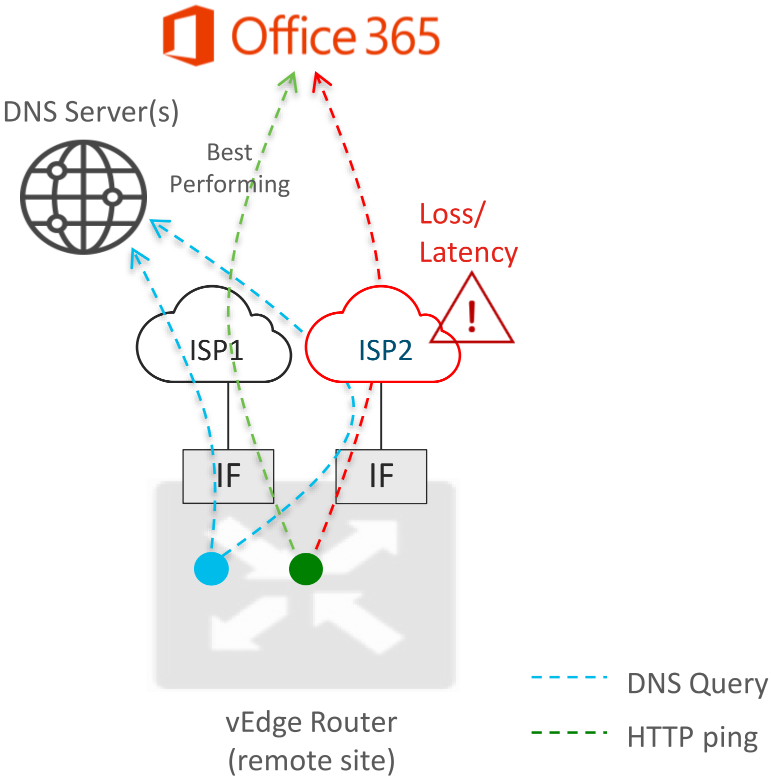
Dual DIA

Dual DIA paths for SaaS, providing additional bandwidth and availability

Single DIA

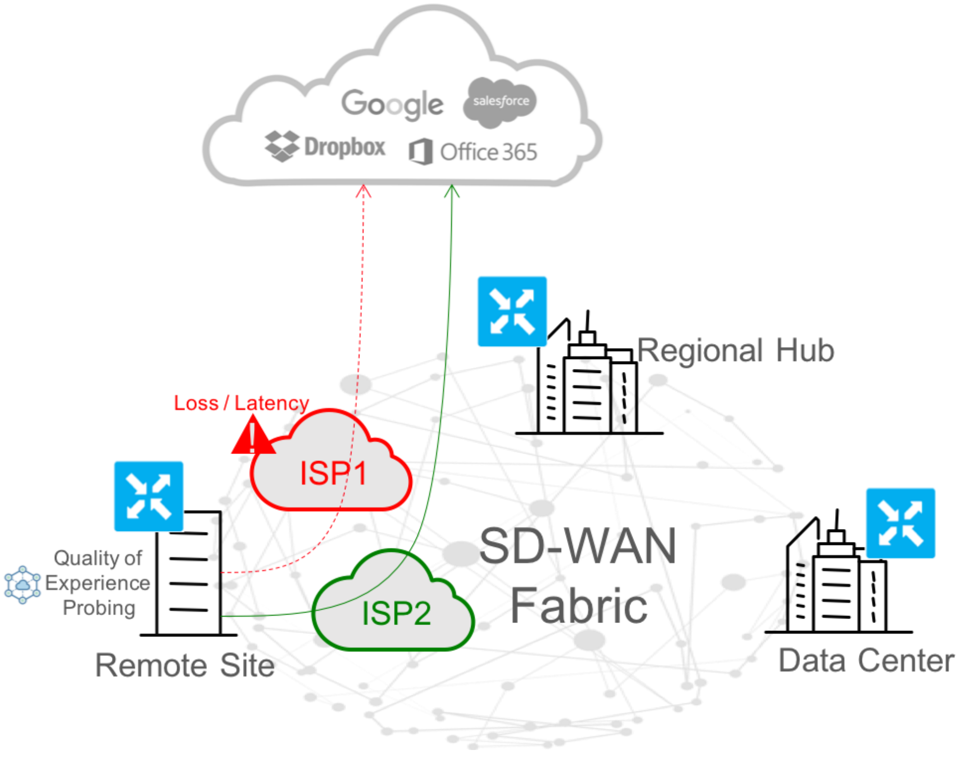
SaaS applications can take the DIA path from branch

Quality of Experience Probing



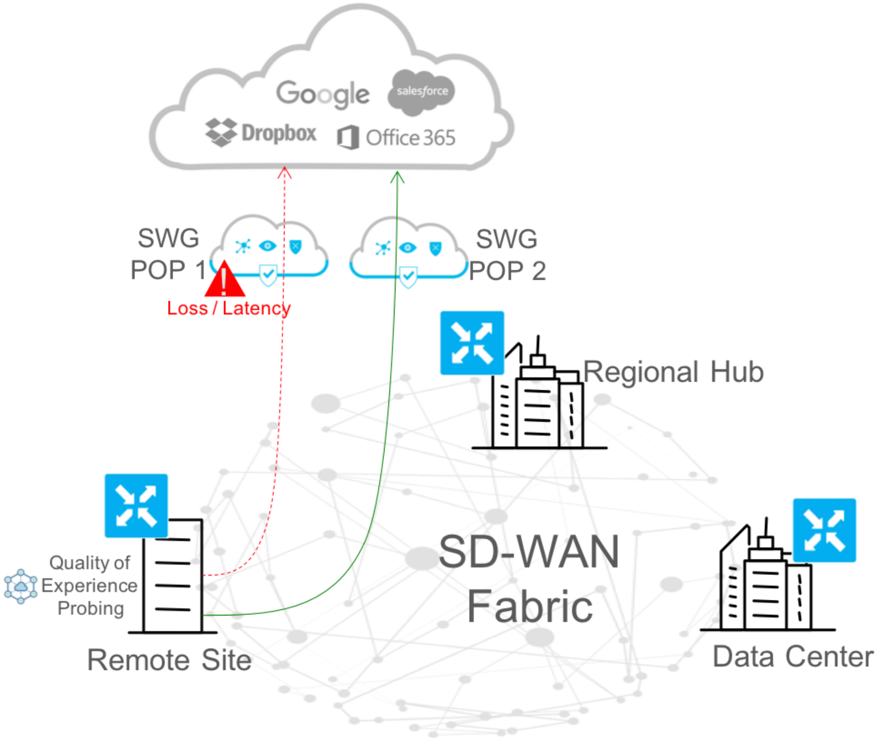
- vEdge router performs DNS resolution for the configured Cloud onRamp SaaS application
  - Done separately over each ISP circuit
  - Public DNS servers are defined and used
- vEdge router initiates periodic HTTP pings toward the configured SaaS application
  - Done separately over each ISP circuit
- vEdge router determines best performing circuit based on loss and latency characteristics reported by the HTTP pings

Branch Direct Internet Access



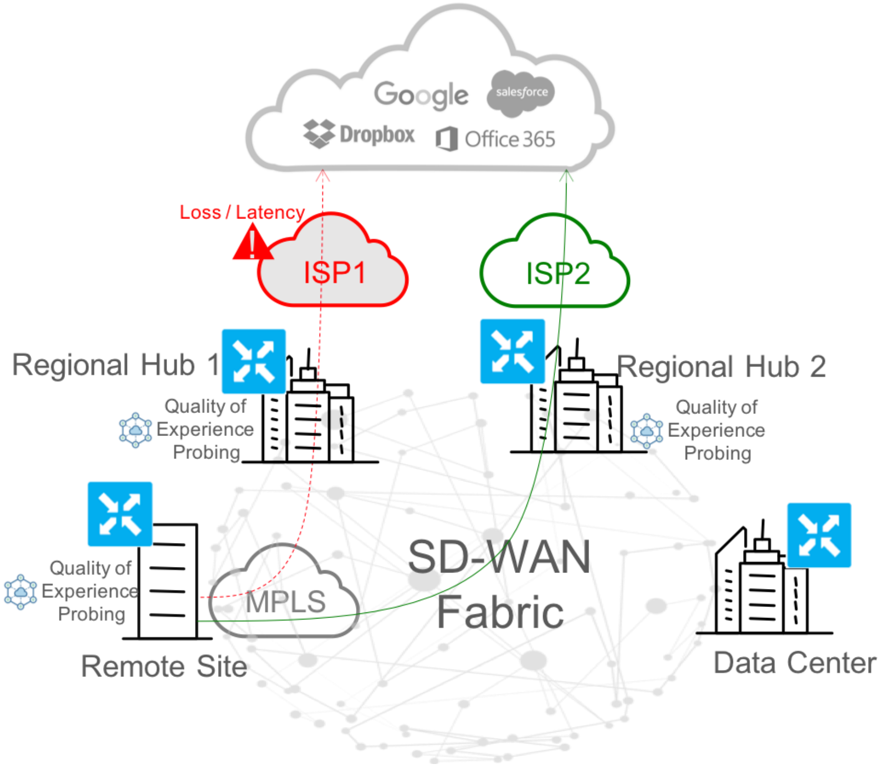
- Monitor SaaS application performance across multiple local internet breakouts
- Local edge router periodically polls and records per application performance
- Edge router determines best performing circuit based on loss and latency characteristics reported by application polling.
- Dynamic identification of end user application flows and steering to optimal local path

Internet Access via Secure Web Gateway



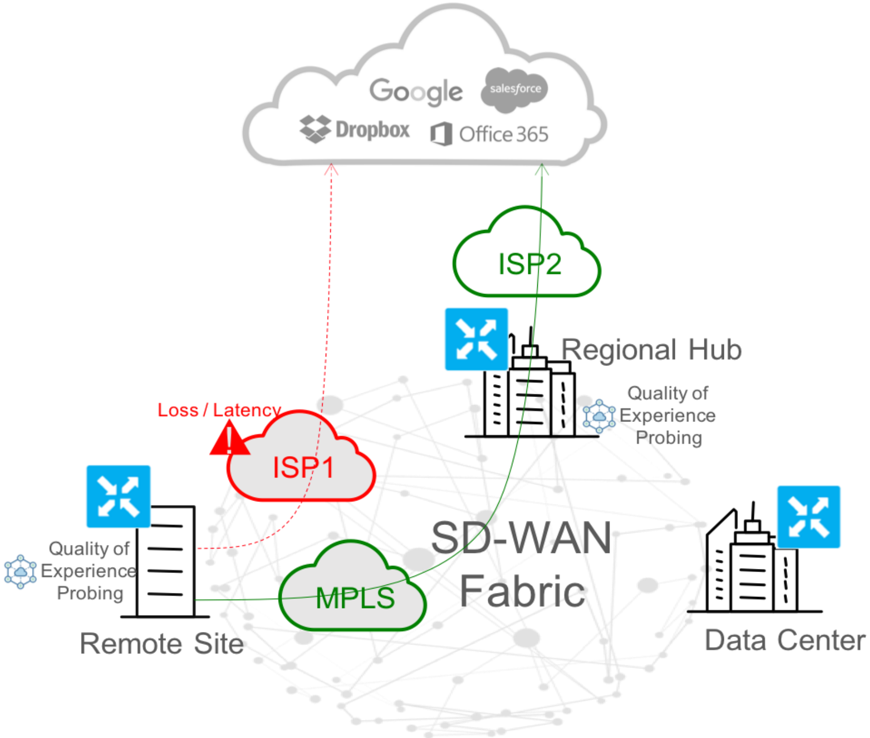
- Monitor SaaS application performance across multiple SWG pops
- Edge router periodically polls and records per application performance
- Edge router determine best performing SWG pop based on loss and latency characteristics reported by application polling.
- Dynamic identification of end user application flows and steering to optimal SWG pop

Regionalised / Centralised Internet Access



- Monitor SaaS application performance across multiple remote internet breakouts
- Remote edge routers periodically poll and record per application performance
- Remote edge routers determine best performing circuit based on loss and latency characteristics reported by application polling.
- Dynamic identification of end user application flows and steering to optimal remote path

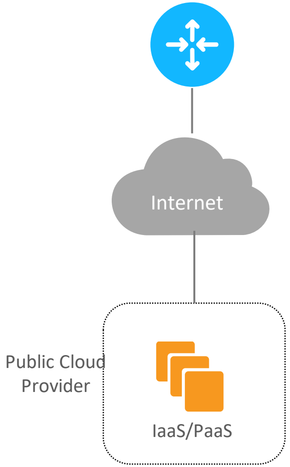
Regionalised & Direct Internet Access



- Monitor SaaS application performance across local and remote internet breakouts
- Local and remote edge routers periodically poll and record per application performance
- Local and remote edge routers determine best performing circuit based on loss and latency characteristics reported by application polling.
- Dynamic identification of end user application flows and steering to optimal local or remote path

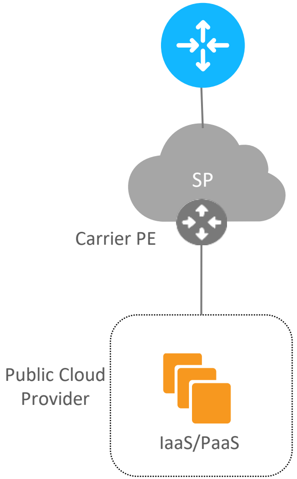
Public Cloud Connectivity Options

Option 1: Internet connection to Public cloud



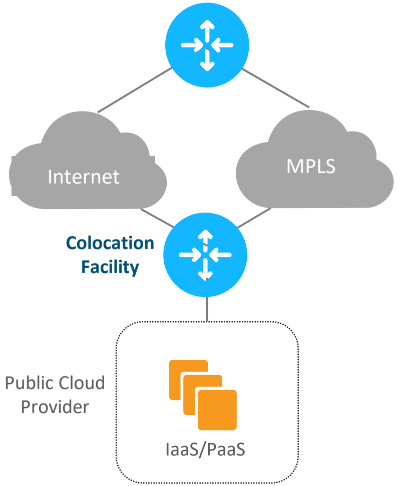
Internet only for connectivity.

Option 2: Direct Connect to Public Cloud through SP



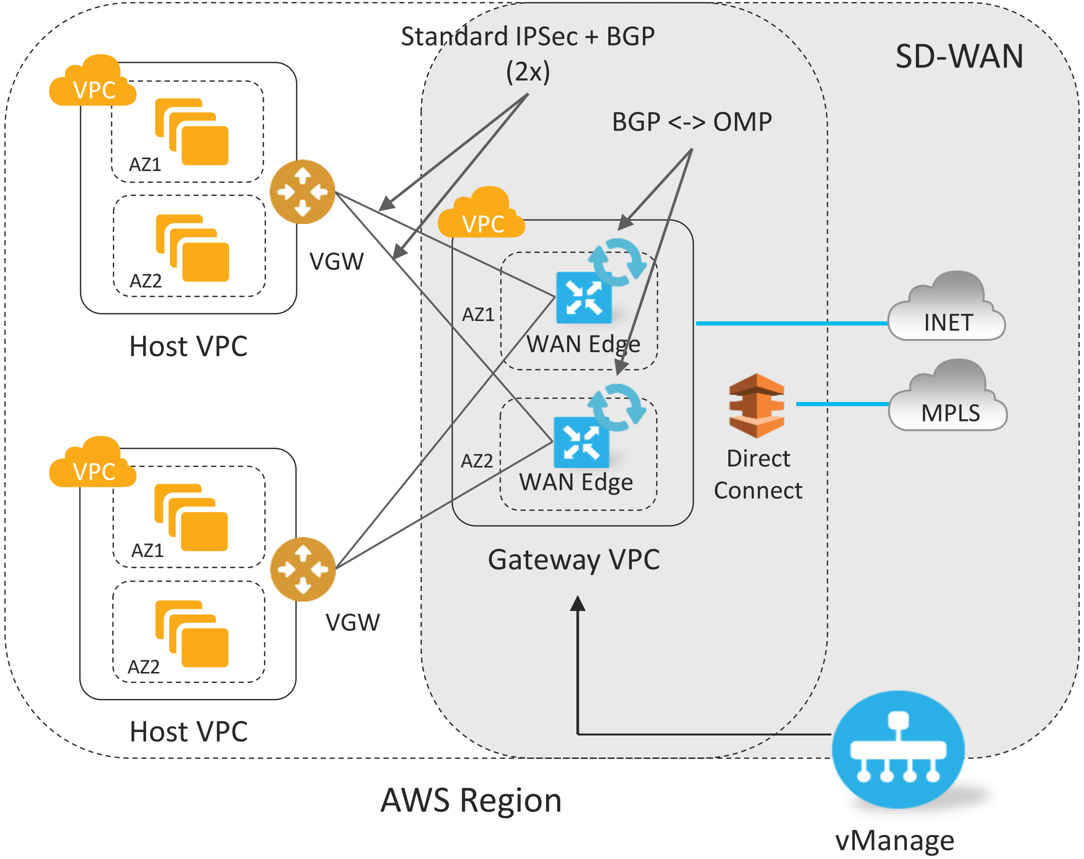
MPLS carriers offers direct connect into public cloud provider

Option 3: Direct Connect to Public Cloud through meet-me locations



Enterprise collocated with public cloud carriers in meet me locations

Cloud onRamp for IaaS - AWS

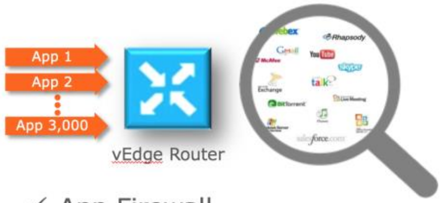


- VGW for host VPCs
- Gateway VPC per-region
  - Multiple for scale
- Standard based IPSec
  - Connectivity redundancy
- BGP across IPSec tunnels for route advertisement
  - Active/active forwarding
  - BGP into OMP redistribution
    Advertise default route to host VPCs
- Optional Direct Connect

SD-WAN Quality of Experience

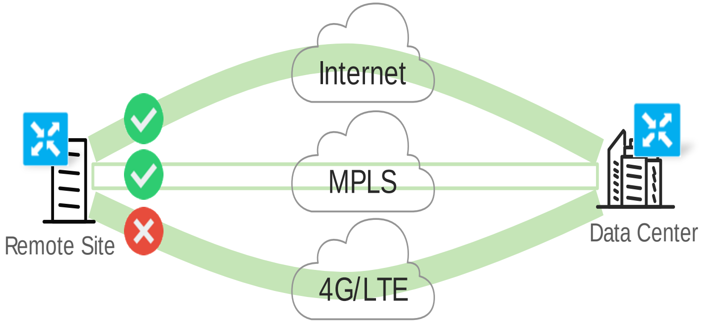
Application Quality of Experience

Application Visibility

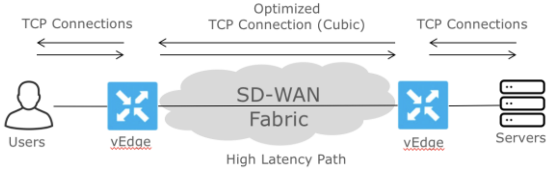


- ✓ App Firewall
- ✓ Traffic prioritization
- ✓ Transport selection

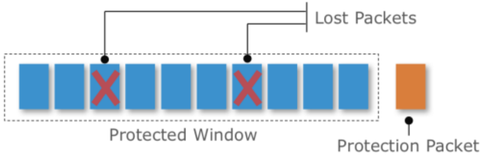
SLA Routing



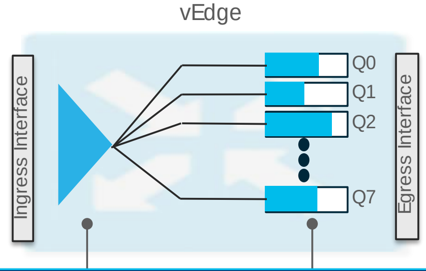
TCP Optimization



FEC



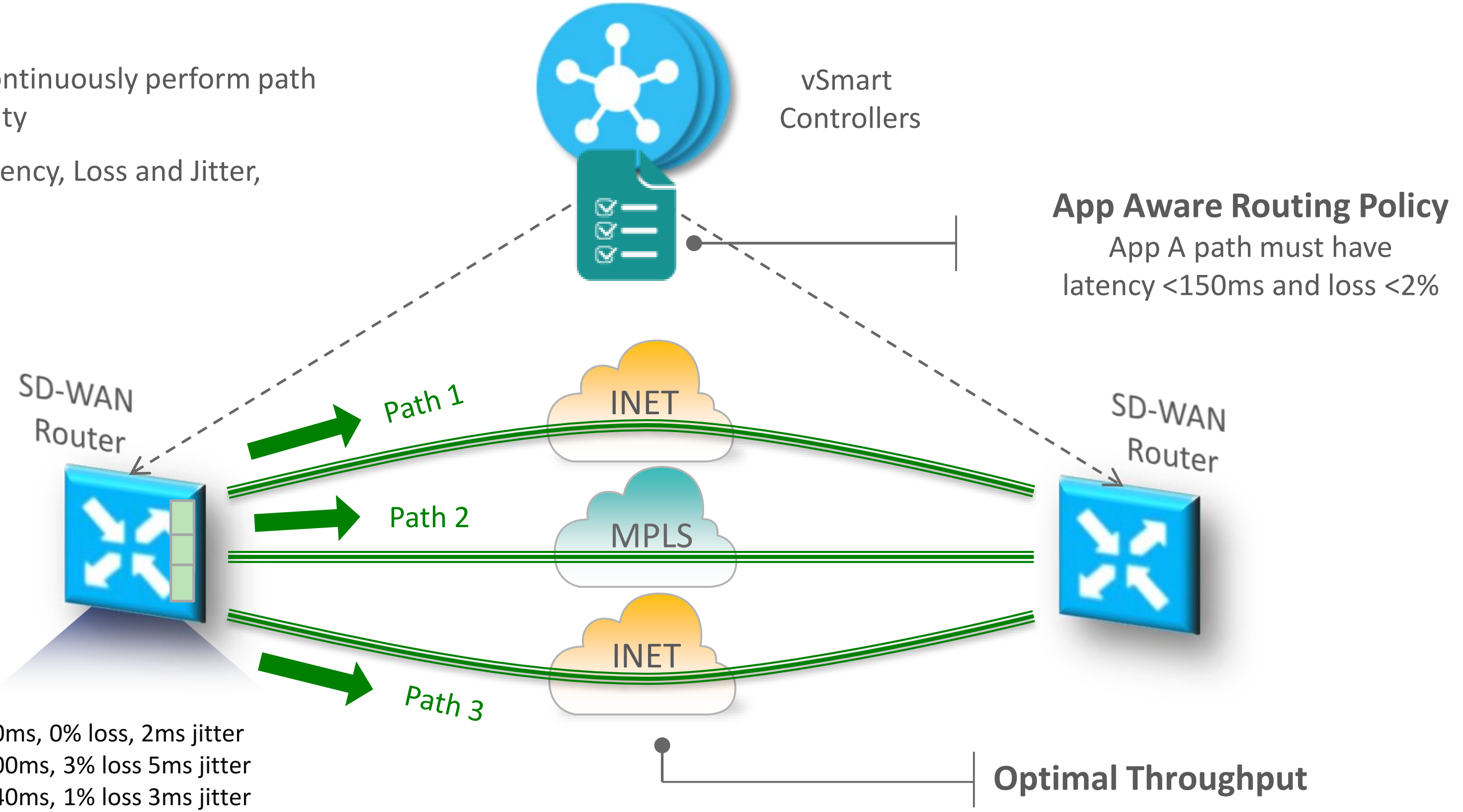
Queuing / Shaping, Marking



Delivering Better Application Quality of Experience

Application Performances and AAR

- SDWAN Routers continuously perform path liveliness and quality
- Measurements Latency, Loss and Jitter,
- Auto Load Balance



App Aware Routing Policy
App A path must have
latency <150ms and loss <2%

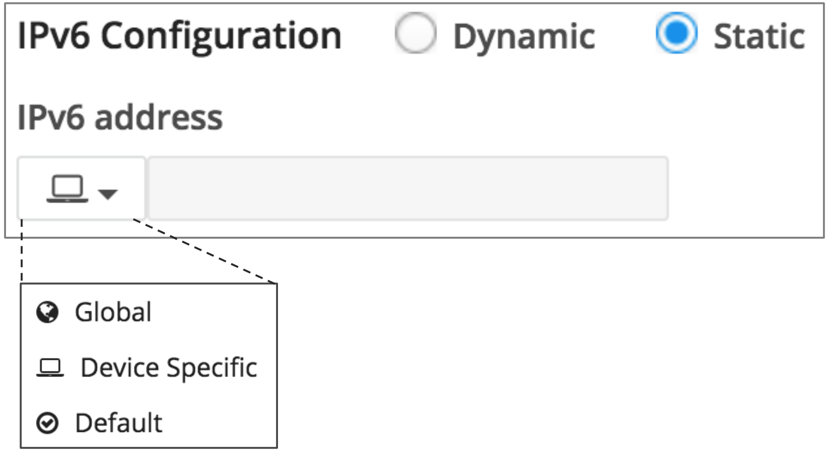
Device QoS
(shaping, policing,
queuing, marking)

Path1: 10ms, 0% loss, 2ms jitter
Path2: 200ms, 3% loss 5ms jitter
Path3: 140ms, 1% loss 3ms jitter

Optimal Throughput

Operational Simplicity

Template-Based Configurations

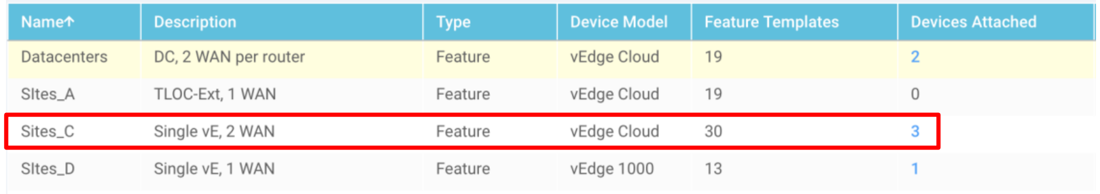


IPv6 Configuration ○ Dynamic ● Static

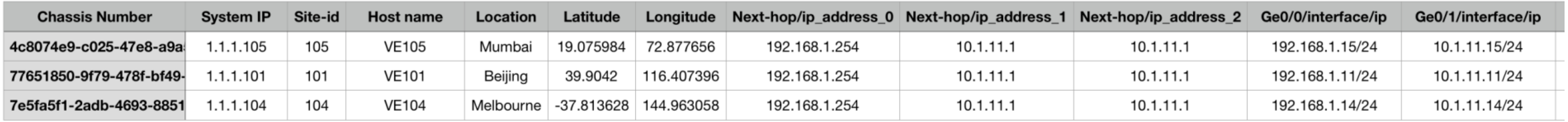
IPv6 address

- Global
- Device Specific
- Default

- Templates are attached to provisioned vEdge routers
- Variables are used for rapid bulk configuration rollout with unique per-device settings
- Local configuration changes are not allowed
  - Prevents configuration drift

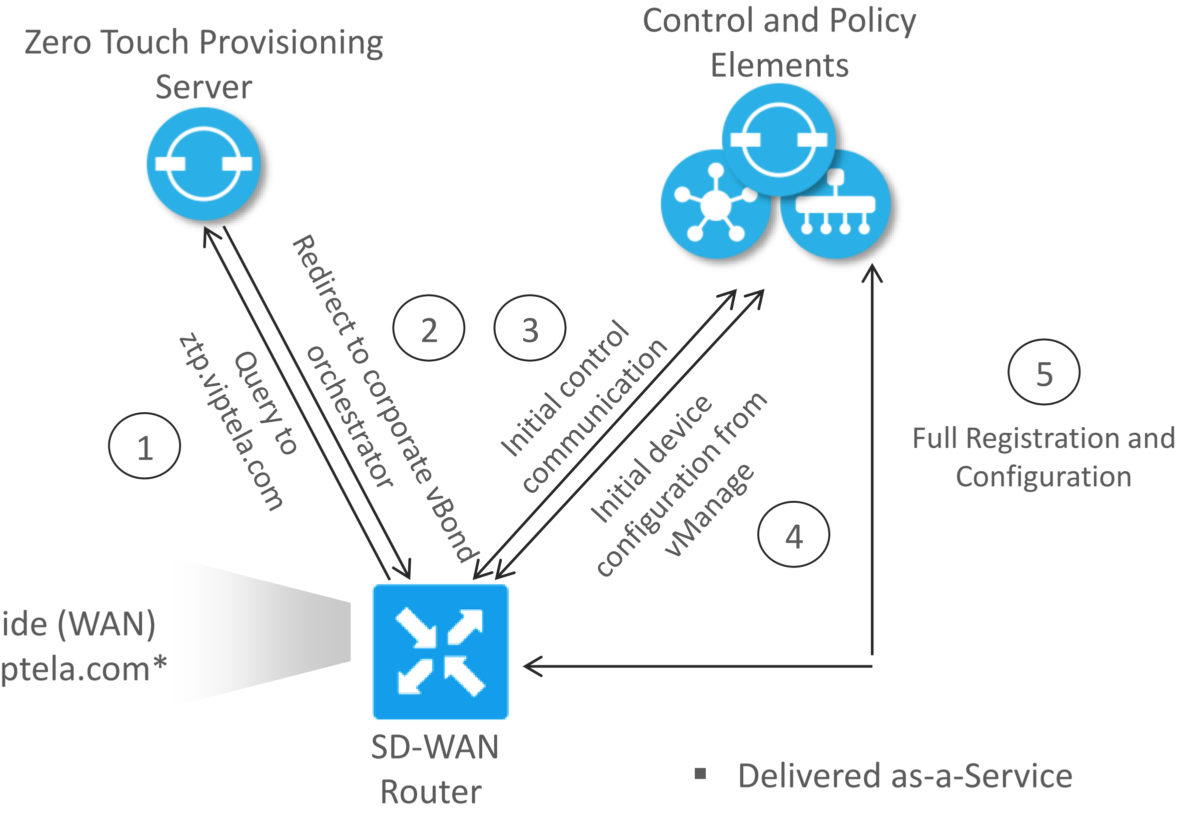


Name↑	Description	Type	Device Model	Feature Templates	Devices Attached
Datacenters	DC, 2 WAN per router	Feature	vEdge Cloud	19	2
SItes_A	TLOC-Ext, 1 WAN	Feature	vEdge Cloud	19	0
Sites_C	Single vE, 2 WAN	Feature	vEdge Cloud	30	3
SItes_D	Single vE, 1 WAN	Feature	vEdge 1000	13	1



Chassis Number	System IP	Site-id	Host name	Location	Latitude	Longitude	Next-hop/ip_address_0	Next-hop/ip_address_1	Next-hop/ip_address_2	Ge0/0/interface/ip	Ge0/1/interface/ip
4c8074e9-c025-47e8-a9a	1.1.1.105	105	VE105	Mumbai	19.075984	72.877656	192.168.1.254	10.1.11.1	10.1.11.1	192.168.1.15/24	10.1.11.15/24
77651850-9f79-478f-bf49-	1.1.1.101	101	VE101	Beijing	39.9042	116.407396	192.168.1.254	10.1.11.1	10.1.11.1	192.168.1.11/24	10.1.11.11/24
7e5fa5f1-2adb-4693-8851	1.1.1.104	104	VE104	Melbourne	-37.813628	144.963058	192.168.1.254	10.1.11.1	10.1.11.1	192.168.1.14/24	10.1.11.14/24

Zero Touch Provisioning


Zero Touch Provisioning Server
Control and Policy Elements
1
Query to ztp.viptela.com
2
Redirect to corporate vBond orchestrator
3
Initial control communication
Initial device configuration from vManage
4
5
Full Registration and Configuration
SD-WAN Router

Assumption:

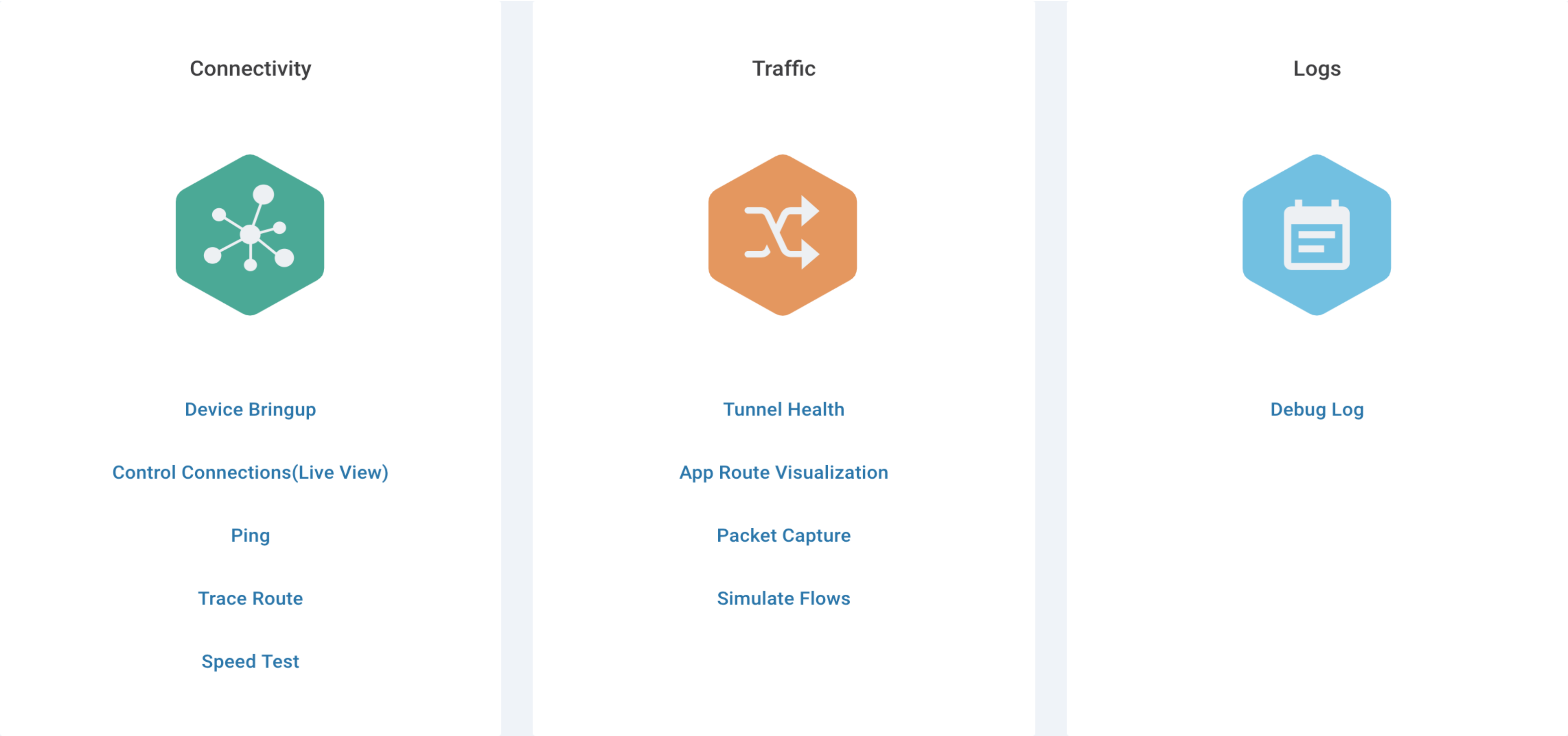
- DHCP on Transport Side (WAN)
- DNS to resolve ztp.viptela.com*

* Factory default config

- Delivered as-a-Service

Troubleshooting and Verification

Transparent Operations



Connectivity

- Device Bringup
- Control Connections(Live View)
- Ping
- Trace Route
- Speed Test

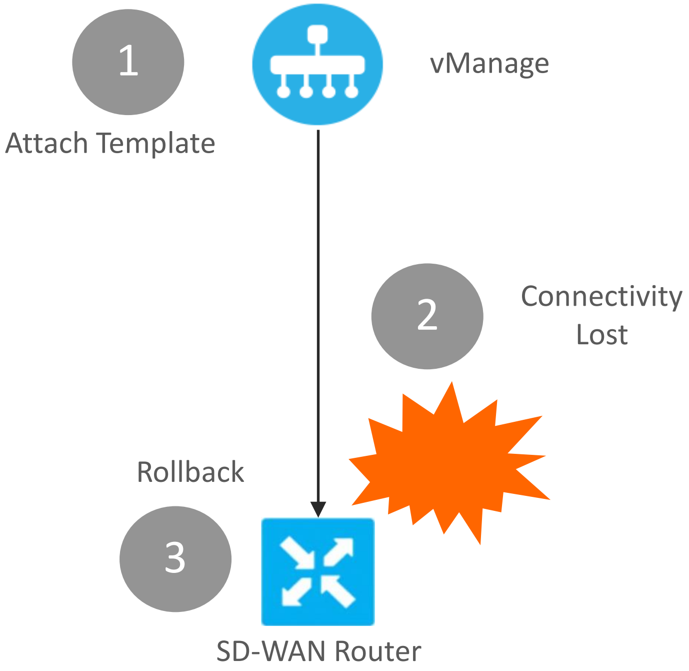
Traffic

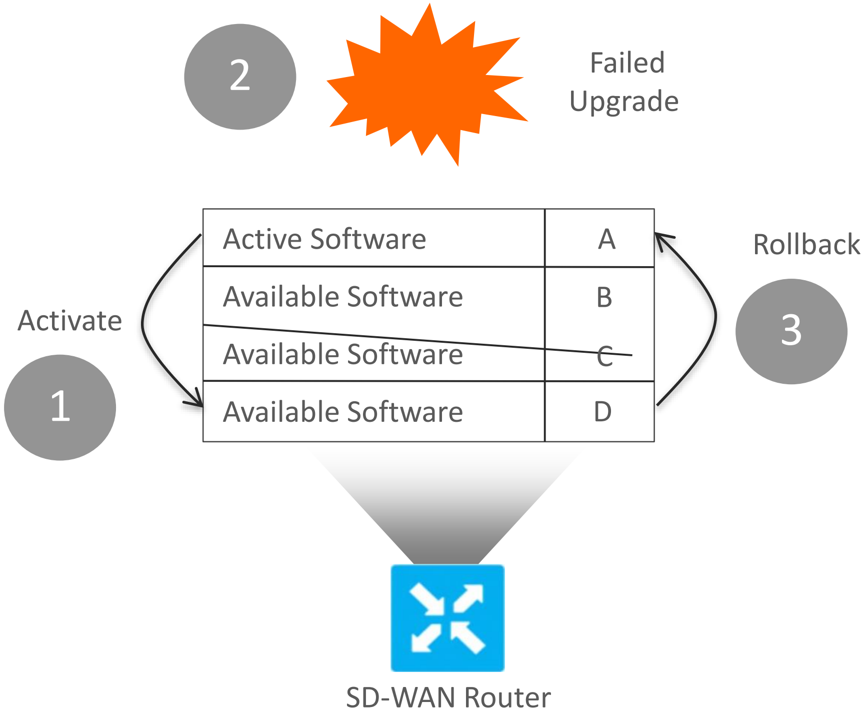
- Tunnel Health
- App Route Visualization
- Packet Capture
- Simulate Flows

Logs

- Debug Log

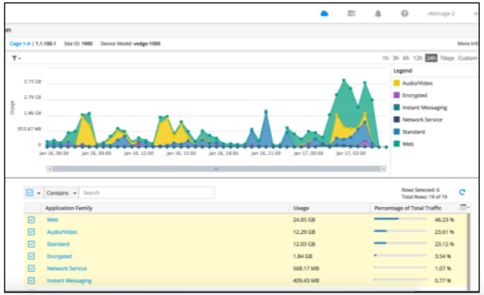
Self Healing Capabilities





Active Software	A
Available Software	B
~~Available Software~~	~~C~~
Available Software	D

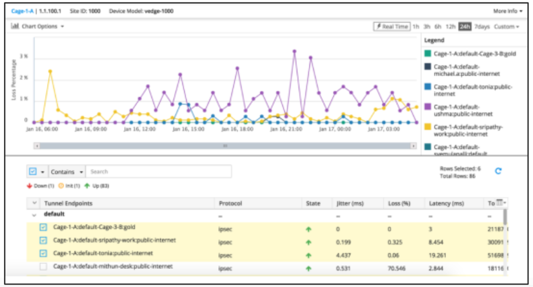
Centralize Management & Monitoring



☑ Contains Search

Rows Selected: 6
Total Rows: 19 of 19

	Application Family	Usage	Percentage of Total Traffic
☑	Web	24.05 GB	46.23 %
☑	Audio/Video	12.29 GB	23.61 %
☑	Standard	12.03 GB	23.12 %
☑	Encrypted	1.84 GB	3.54 %
☑	Network Service	568.17 MB	1.07 %
☑	Instant Messaging	409.43 MB	0.77 %



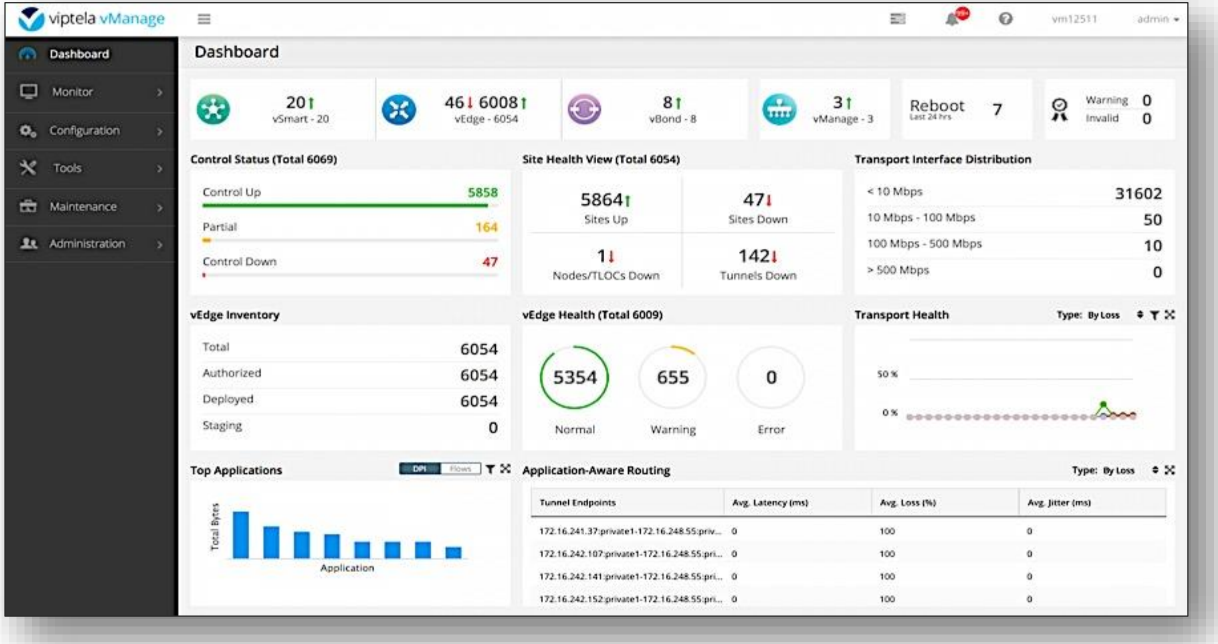
Cage-1-A | 1.1.100.1 Site ID: 1000 Device Model: vedge-1000
More info
Chart Options
Real Time 1h 3h 6h 12h 24h 7days Custom
Loss Percentage
3 %
2 %
1 %
0
Jan 16, 06:00
Jan 16, 09:00
Jan 16, 12:00
Jan 16, 15:00
Jan 16, 18:00
Jan 16, 21:00
Jan 17, 00:00
Jan 17, 03:00
Legend
Cage-1-A:default-Cage-3-B:gold
Cage-1-A:default-michael.a:public-internet
Cage-1-A:default-tonia:public-internet
Cage-1-A:default-ushma:public-internet
Cage-1-A:default-sripathy-work:public-internet
Cage-1-A:default-svemu/anali:default

☑ Contains Search

Down (1) Init (1) Up (83)

Rows Selected: 6
Total Rows: 86

	Tunnel Endpoints	Protocol	State	Jitter (ms)	Loss (%)	Latency (ms)	To
	default	--		--	--	--	--
☑	Cage-1-A:default-Cage-3-B:gold	ipsec	↑	0	0	3	21187
☑	Cage-1-A:default-sripathy-work:public-internet	ipsec	↑	0.199	0.325	8.454	30091
☑	Cage-1-A:default-tonia:public-internet	ipsec	↑	4.437	0.06	19.261	51698
□	Cage-1-A:default-mithun-desk:public-internet	ipsec	↑	0.531	70.546	2.844	18116



Dashboard

20↑ vSmart - 20

46↓ 6008↑ vEdge - 6054

8↑ vBond - 8

3↑ vManage - 3

Reboot 7
Last 24 hrs

Warning 0
Invalid 0

Control Status (Total 6069)

Control Up	5858
Partial	164
Control Down	47

Site Health View (Total 6054)

5864↑ Sites Up	47↓ Sites Down
1↓ Nodes/TLOCs Down	142↓ Tunnels Down

Transport Interface Distribution

< 10 Mbps	31602
10 Mbps - 100 Mbps	50
100 Mbps - 500 Mbps	10
> 500 Mbps	0

vEdge Inventory

Total	6054
Authorized	6054
Deployed	6054
Staging	0

vEdge Health (Total 6009)

5354 Normal

655 Warning

0 Error

Transport Health

Top Applications

Application-Aware Routing

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
172.16.241.37:private1-172.16.248.55:priv...	0	100	0
172.16.242.107:private1-172.16.248.55:pri...	0	100	0
172.16.242.141:private1-172.16.248.55:pri...	0	100	0
172.16.242.152:private1-172.16.248.55:pri...	0	100	0

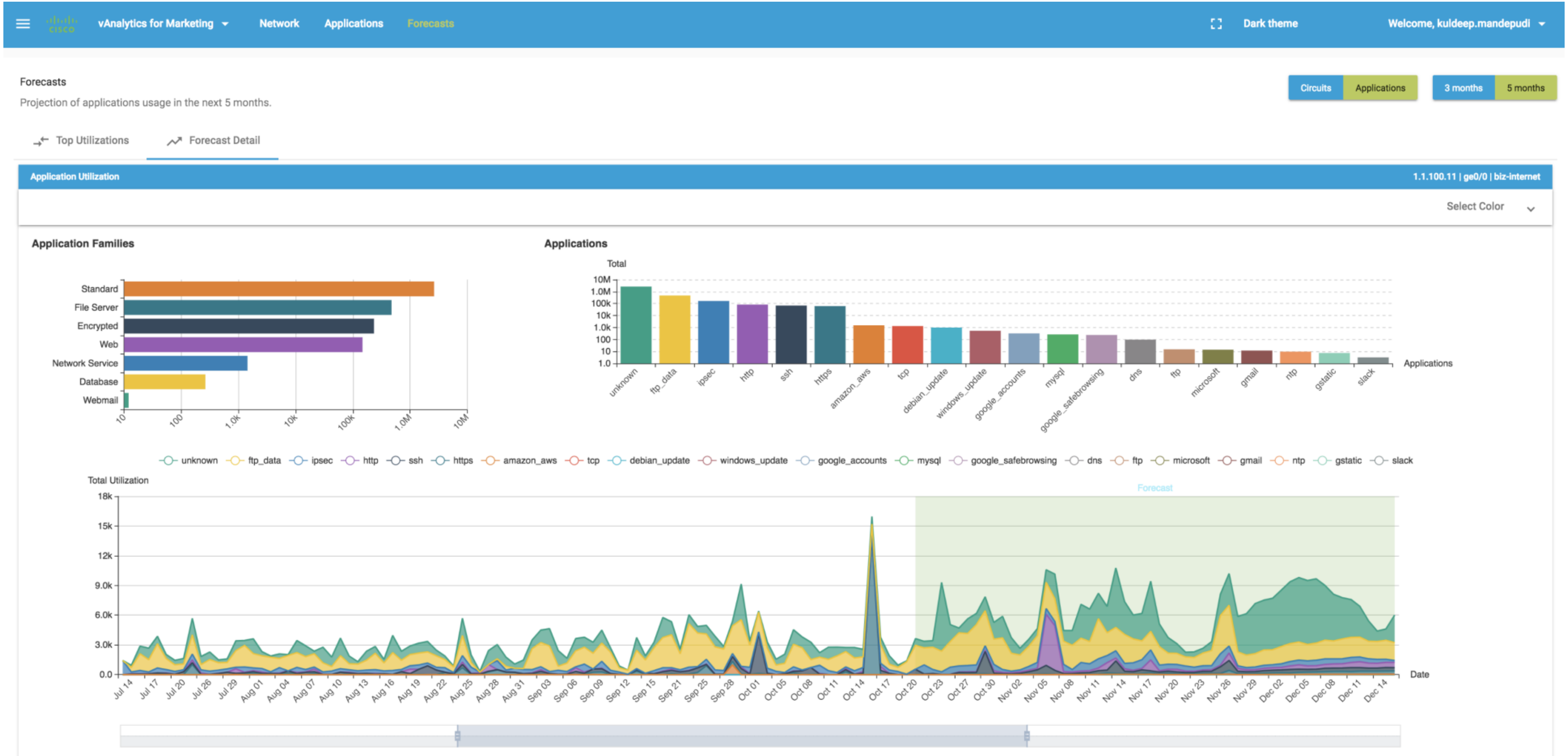
Centralize Configuration

- Security
- Template Configuration
- Policy
- Routing
- QoS, Marking
- ACL
- Application SLA
- .....

Centralize Monitoring

- Devices
- Application
- Bandwidth usage
- Link Performances
- Alerts

Application Forecasting and Analytics



Forecasts

Projection of applications usage in the next 5 months.

Application Utilization — 1.1.100.11 | ge0/0 | biz-internet

SD-WAN Platform Options

Providing for flexibility in deployment

SDWAN and Services

ISR 1000

- 200 Mbps
- Next-gen connectivity
- Performance flexibility

ISR 4000

- Up to 2 Gbps
- Modular
- Integrated service containers
- Compute with UCS-E

ASR 1000

- 2.5-200Gbps
- High-performance service w/hardware assist
- Hardware & software redundancy

Core SD-WAN

vEdge 100

- 100 Mbps
- 4G LTE & Wireless

vEdge 1000

- Up to 1 Gbps
- Fixed

vEdge 2000

- 10 Gbps
- Modular

Virtualization

ENCS 5100

- Up to 250Mbps

ENCS 5400

- 250Mbps – 2GB

Public Cloud

Microsoft Azure

amazon web services

Cisco SD-WAN Powered by Meraki portfolio

Teleworker

Z3

Z3C

~5 users
802.11ac Wave 2 Wireless & PoE+
FW throughput: 100 Mbps
CAT 3 LTE (Z3C)

Small Branch

MX64/65

~50 clients
250 Mbps FW throughput
802.11ac Wireless* & PoE+

MX67/68

~50 clients
450 Mbps FW throughput
802.11ac Wave 2* & PoE+

MX67C/68CW

~50 clients
450 Mbps FW throughput
802.11ac Wave 2* & PoE+
CAT 6 LTE (300 Mbps)

Medium Branch

MX84

~200 clients
500 Mbps FW throughput

MX100

~500 clients
750 Mbps FW throughput

Data Center, Campus or Concentrator

MX250

~2,000 clients
4 Gbps FW throughput

MX450

~10,000 clients
6 Gbps FW throughput

Virtual

vMX100 for AWS & Azure

FW throughput: 750 Mbps
VPN & SD-WAN features

**Available with wireless models*
(MX64W, MX65W, MX67W, MX68W, MX68CW)

Why Cisco?

Choice of any cloud and any connectivity

No matter where you applications are hosted Cisco SD-WAN delivers the best user experience, securely across any cloud.

Security at enterprise scale

Protect all users, devices and applications by deploying the right security, on-premise or cloud delivered, in the right place, quickly.

Unified architecture with no compromise

Leadership in SD-WAN and Security with the best threat intelligence stops threats faster without impacting user experience.

Designed for Intent-Based Networking end-to-end

Say hello
to the future.

Cisco Connect 2019

Hanoi, Vietnam . 4th April 2019
#CiscoConnectVN