Cisco SD-WAN:
Poprawa wydajności aplikacji

Rafał Telbusiewicz
Technical Solution Architect SD-WAN
rafal.telbusiewicz@cisco.com

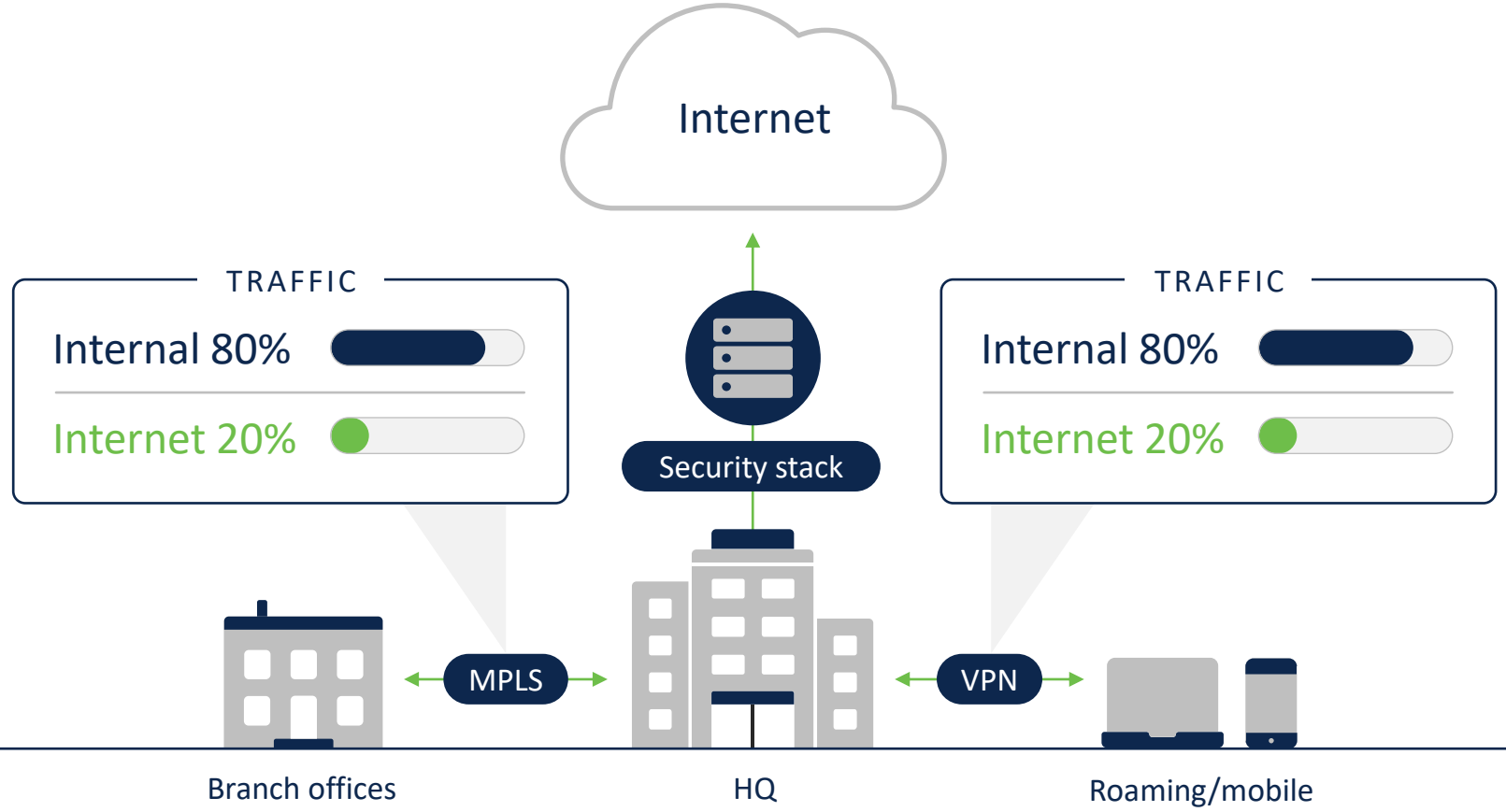
You make networking **possible**

Kiedyś...

Bezpieczeństwo realizowane na perymetrze sieci

Sieć:
Scentralizowana

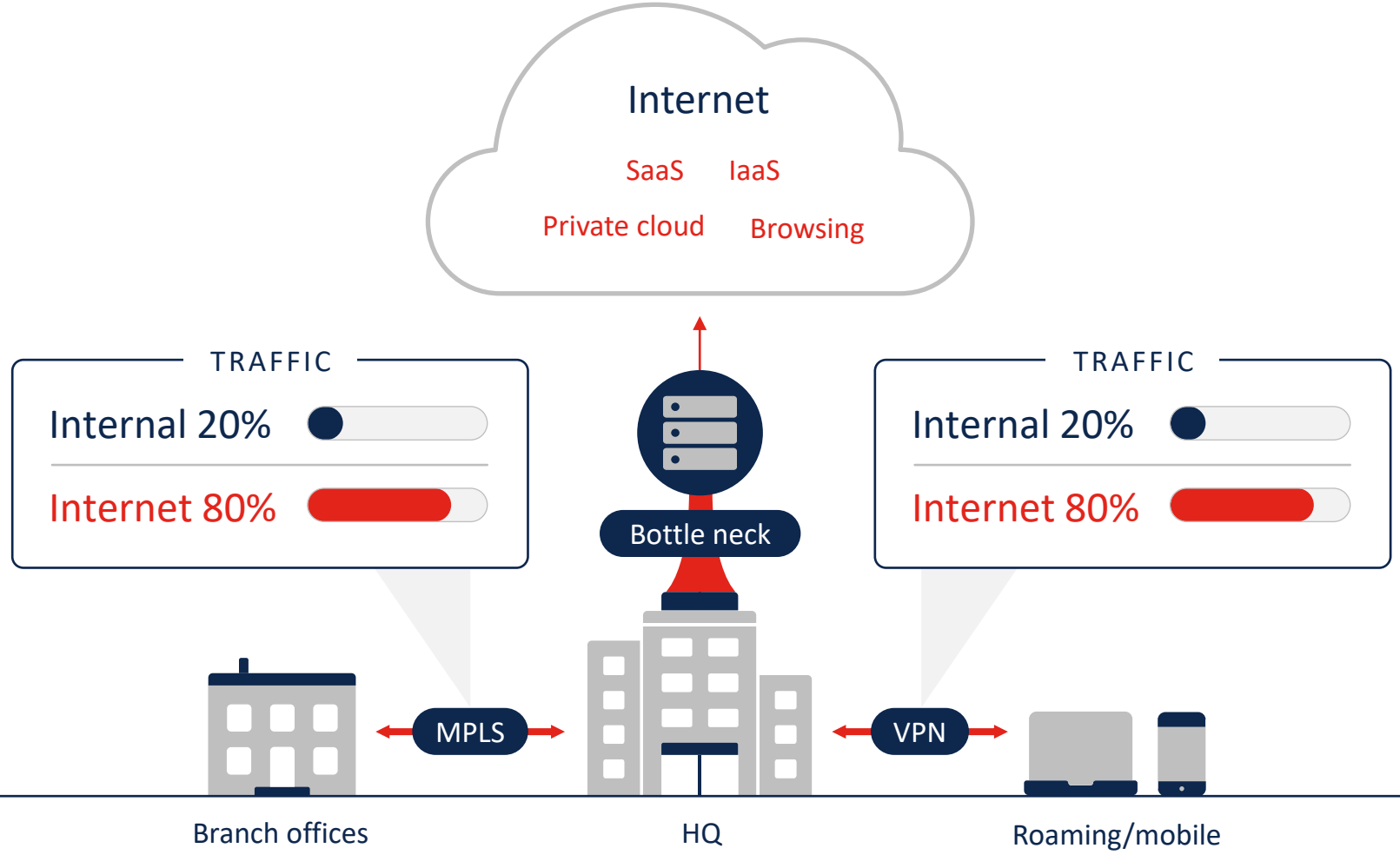
Bezpieczeństwo:
On-prem, centralnie realizowane środki kontroli



Zmiany... zmiany... zmiany...

Wyzwania:

- Wydajność aplikacji
- User experience
- Skuteczność rozwiązań bezpieczeństwa
- # Narzędzi/dostawców
- Integracje



Jak opanować użytkowników i aplikację będące **wszędzie**?

Cisco SD-WAN wyznacza nowe standardy

Multicloud

Multicloud Access

SDCI/Cloud Backbone

App Experience

Voice Optimization

SaaS Optimization M365, Webex

AppQoE – TCP Opt, FEC, Duplication, DRE, etc.

Security

Embedded Security

Segmentation

SSE

AI/ML Ops

Analytics and Visibility

WAN Insights

Intuitive Experience

Simplified UX

Enhanced Upgrade

Self Service Portal

Cloud Managed Cisco SD-WAN

DevOps

App Automation

Intent Automation

API/SDK

MSP

Multi-tenant SD-WAN Edge

Multi-Region Fabric

Co-managed SD-WAN Service

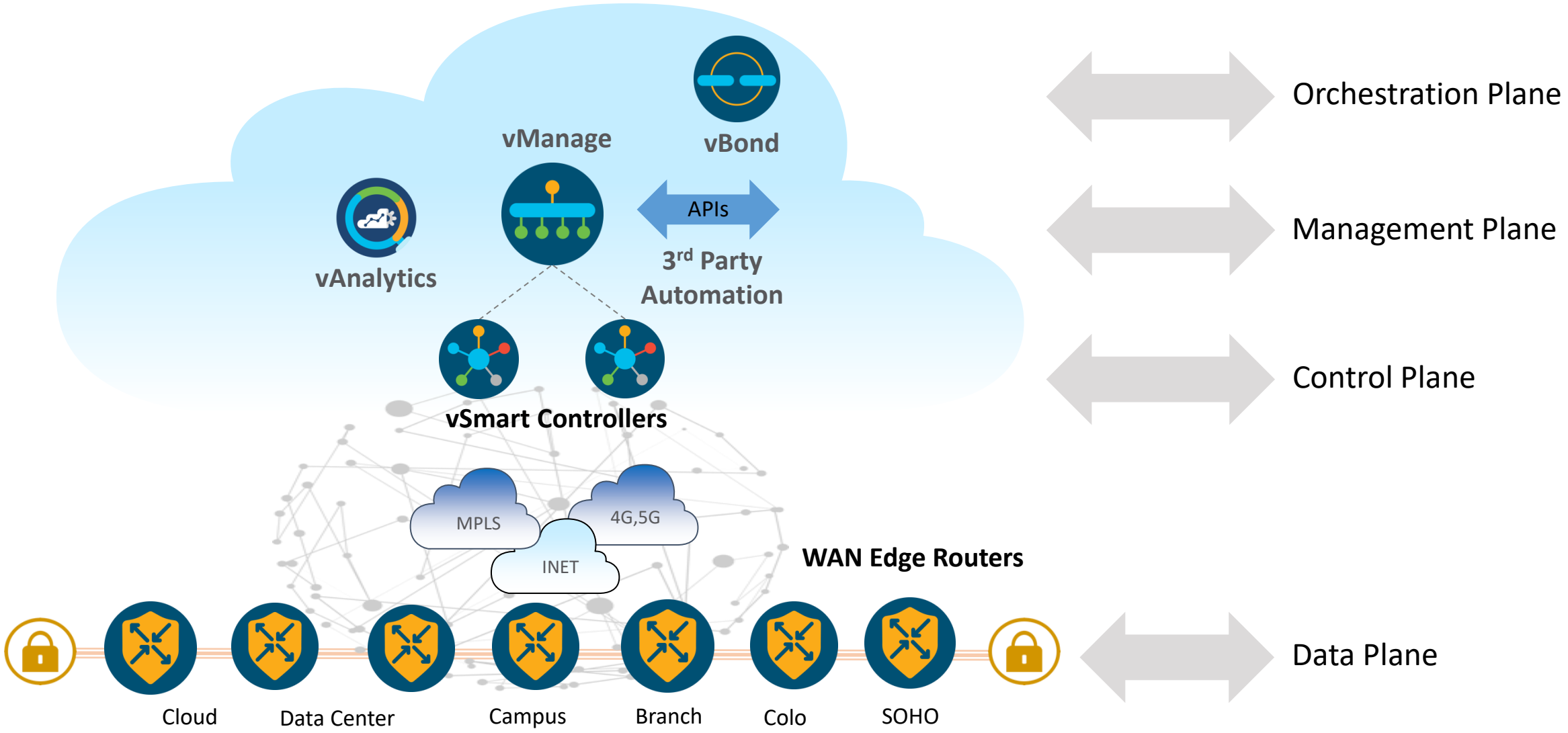
Platforms

SD-WAN Remote Access

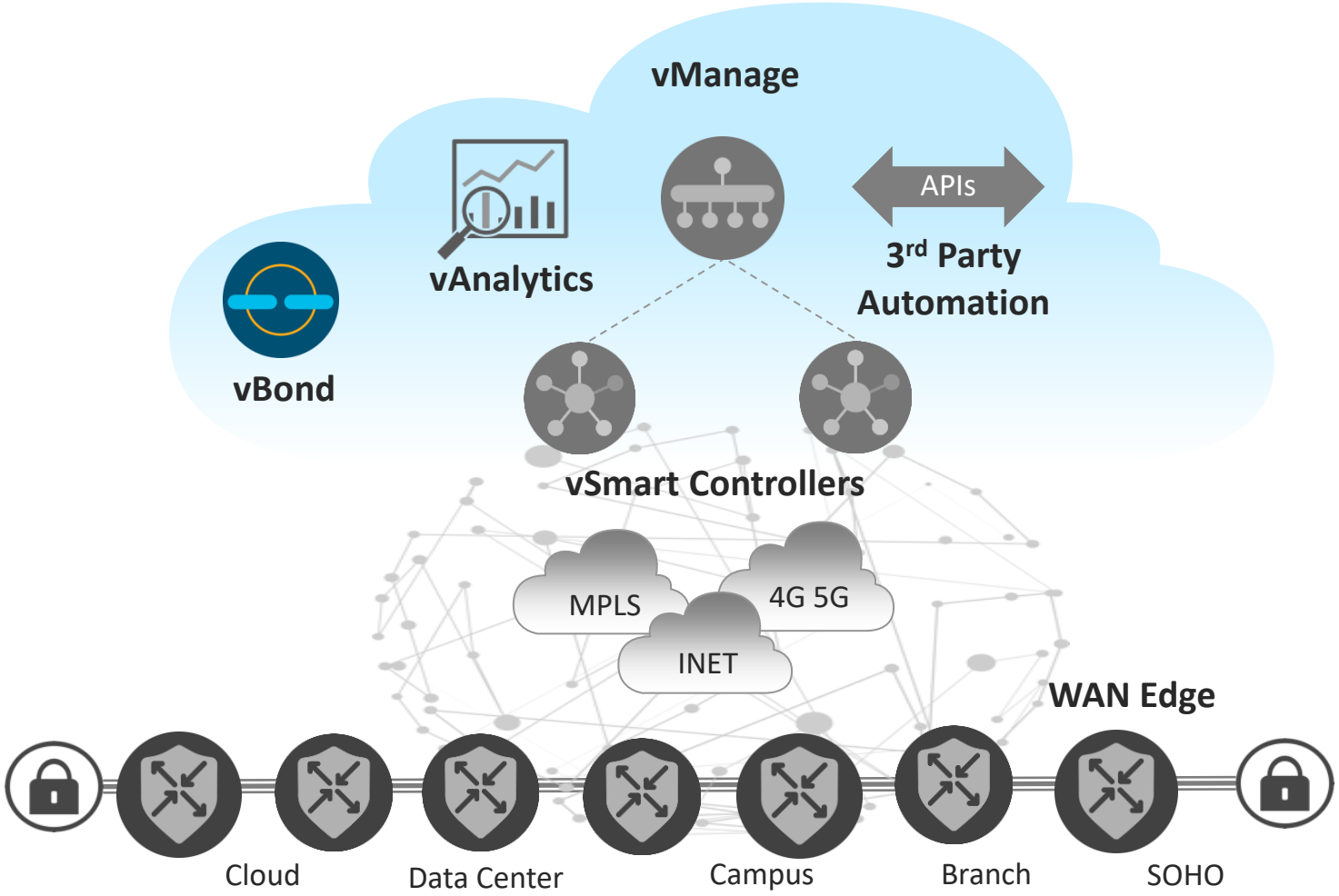
Scalability

Most Powerful Cat8K 100Gbps imix

Architektura Cisco SD-WAN



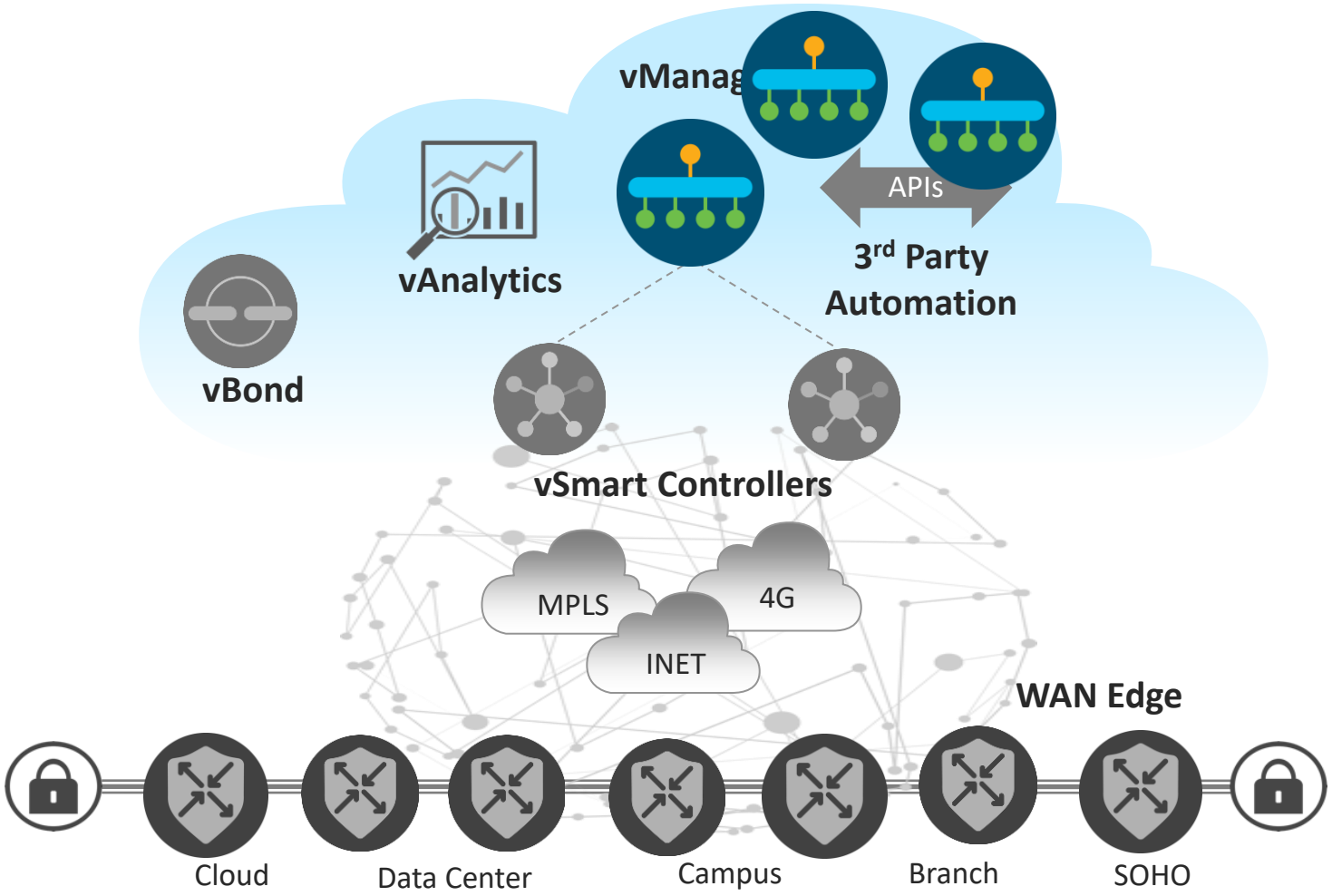
Orchestration Plane



Cisco vBond

- „Bramkarz”
- Orkiestruje warstwą control plane i data plane
- Pierwszy punkt uwierzytelnienia (model white-list)
- Dystrybuuje listę vSmart/vManage do wszystkich Edgy
- Funkcja NAT traversal
- Zalecany publiczny ip adres lub NAT 1:1
- HA

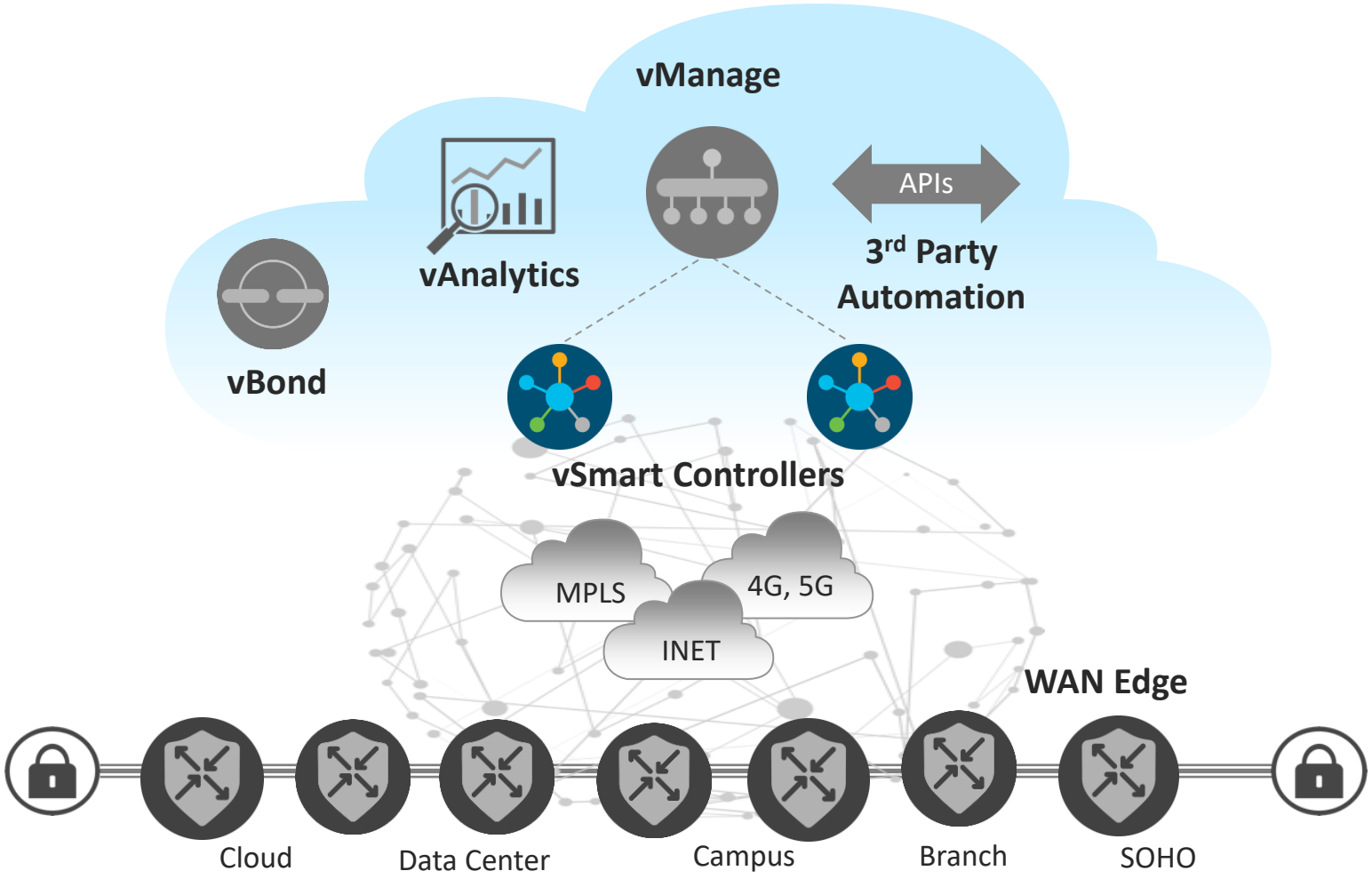
Management Plane



vManage

- „Single panel of glass” for Day0, Day1 and Day2
- Centralny punkt dla administratora
- Troubleshooting, monitoring
- Zarządzanie warstwą data plane oraz control plane
- RBAC
- Udostępnia pełne API
- HA

Control Plane



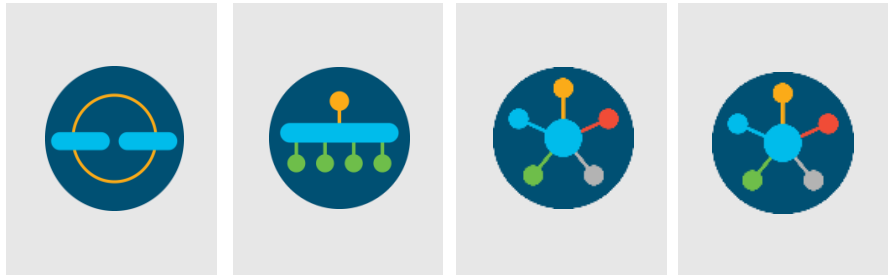
Cisco vSmart

- „Mózg sieci”
- Dystrybuuje warstwę data plane do urządzeń Edge – informacje o routingu i szyfrowaniu
- Implementuje polityki
- Znacznie zmniejsza złożoność control plane
- HA

Controller Deployment Methodology

On-Premise

vBond vManage vSmart vSmart

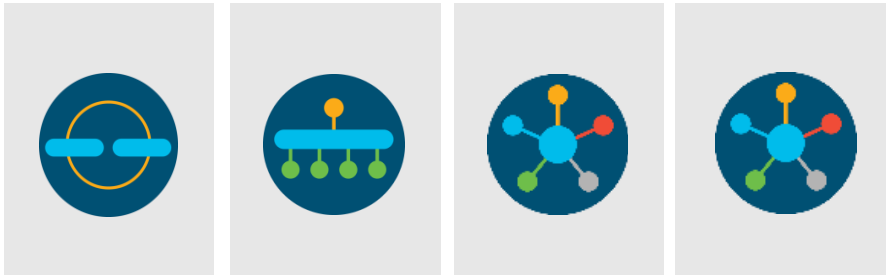


ESXi or KVM

Physical Servers

Cisco or MSP/Customer Hosted

vBond vManage vSmart vSmart



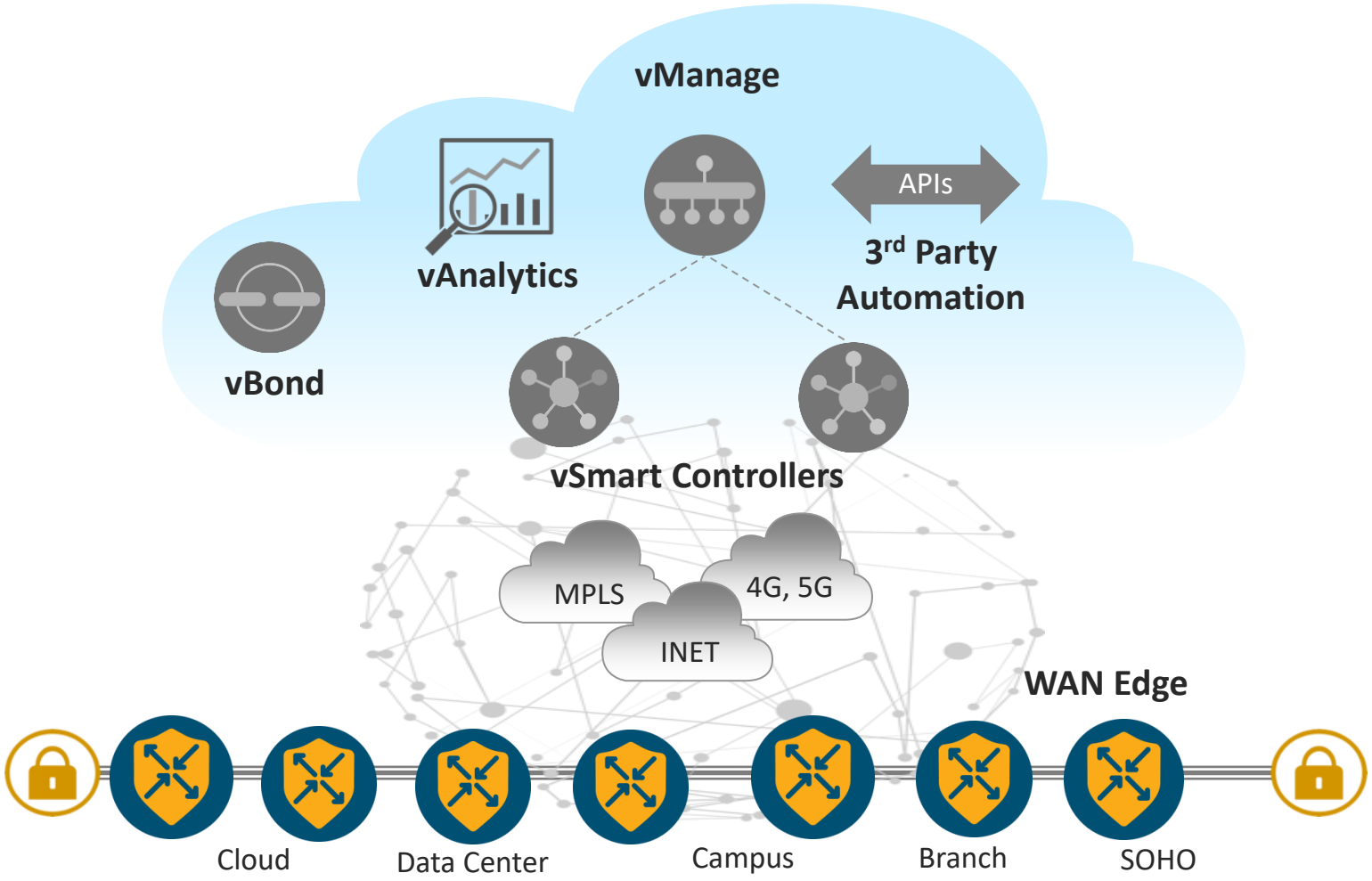
AWS or Azure

Certified Cloud (PCI, SOC2/ISO/C5)*

Gov. Cloud (FedRAMP)*

*Only Cisco hosted

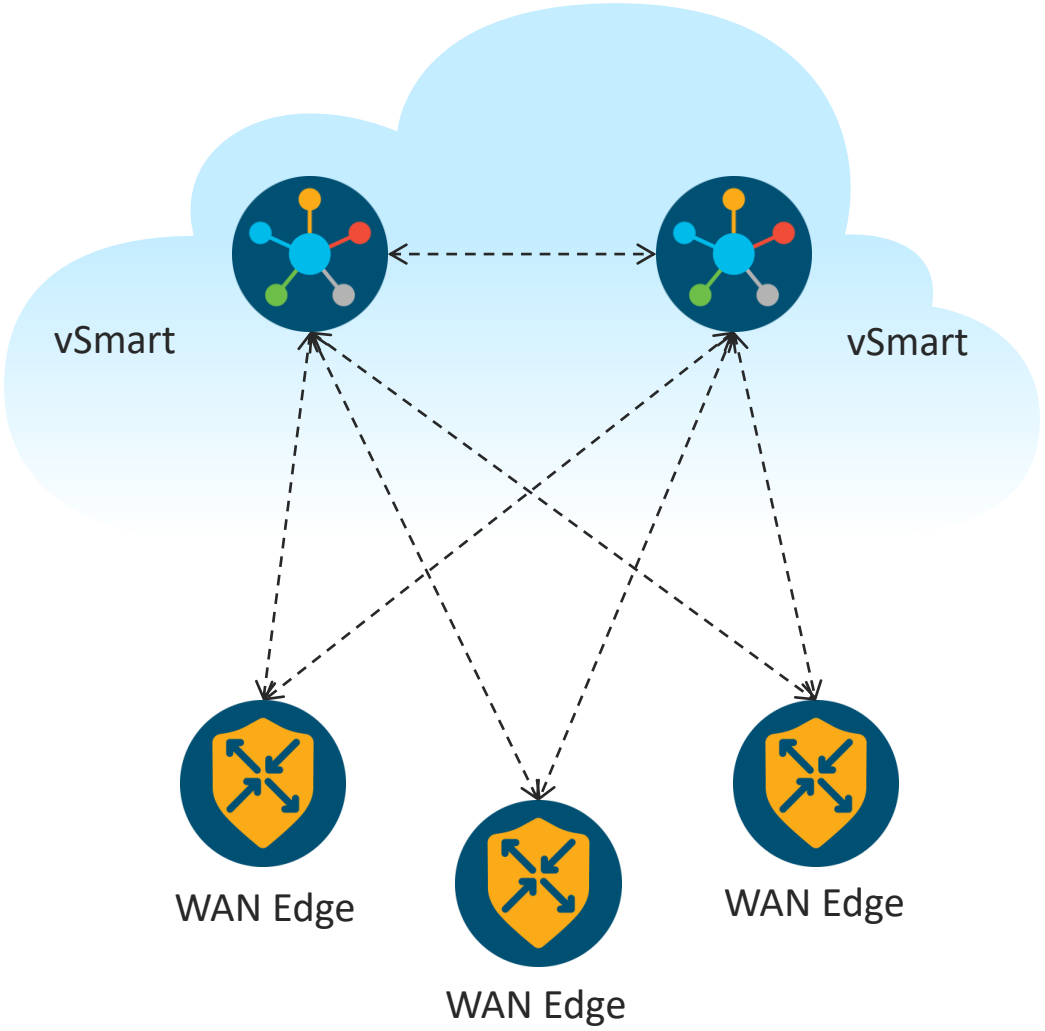
Data Plane



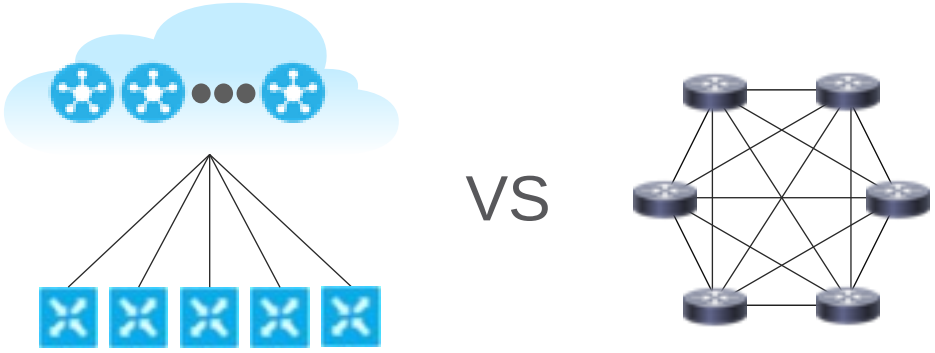
Cisco WAN Edge

- Cisco ISR1K, ISR4K, ASR1K, C8000, NFV, CSR1Kv
- Zapewnia bezpieczny data plane między Edge'ami
- Ustanawia bezpieczny control plane z vSmartami (OMP)
- Implementuje polityki data plane o Application Avare Routing
- Eksportuje statystyki wydajności
- Wykorzystuje tradycyjne protokoły routingu takie jak OSPF, BGP, EIGRP
- Zapewnia całkowity Zero Touch Provisioning
- Obsługa standardów 10GE, 40GE i 100GE

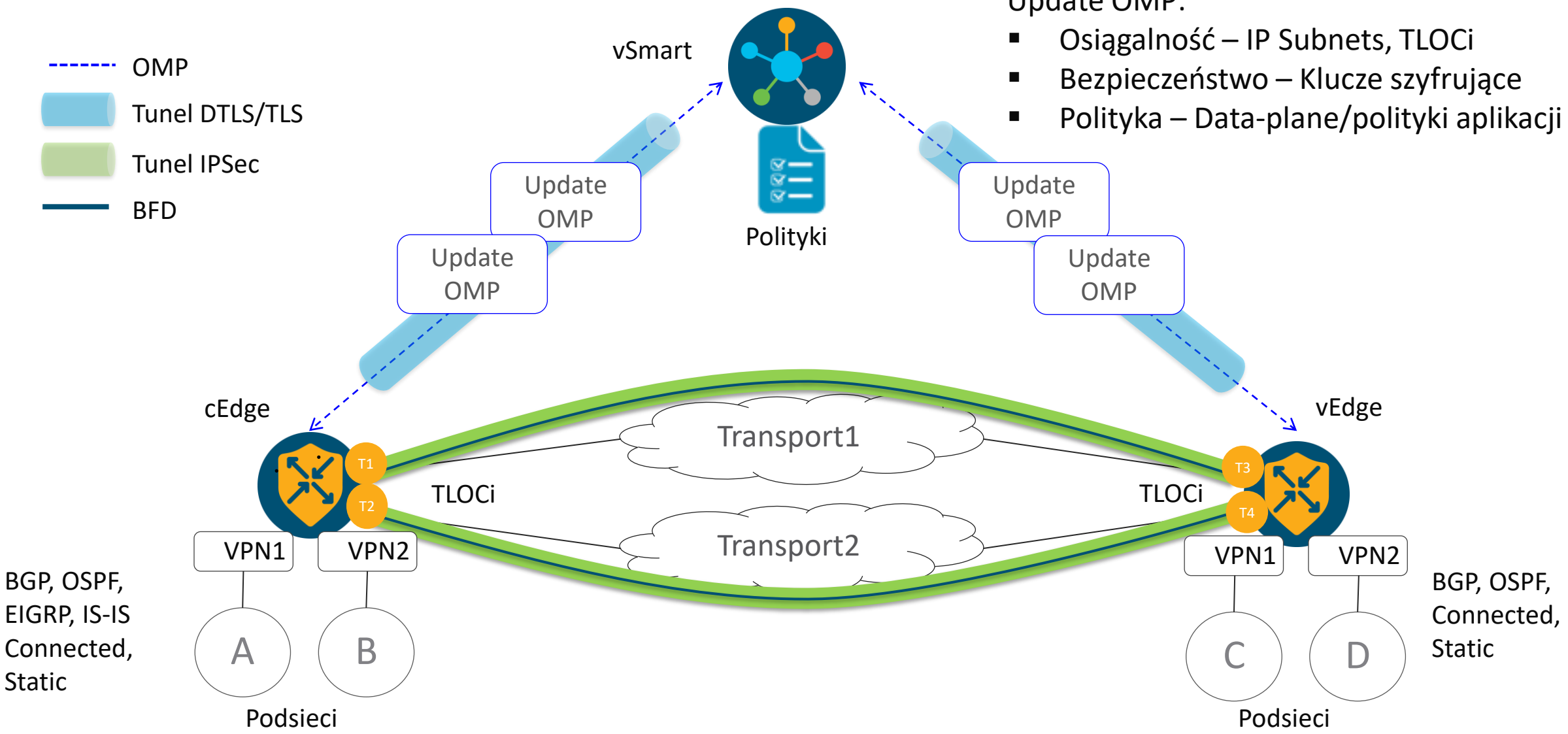
Control Plane - Overlay Management Protocol (OMP)



- OMP jest oparty o TCP, zapewnia control plane, podobny do BGP
- Działa między routerami i kontrolerem vSmart oraz między nimi (vSmartami)
  - zabezpieczony przez DTLS/TLS
- OMP propaguje informacje między data plane i control plane
- OMP niweluje liczbę stanów i skomplikowanie systemu – zwiększając znacząco skalowalność



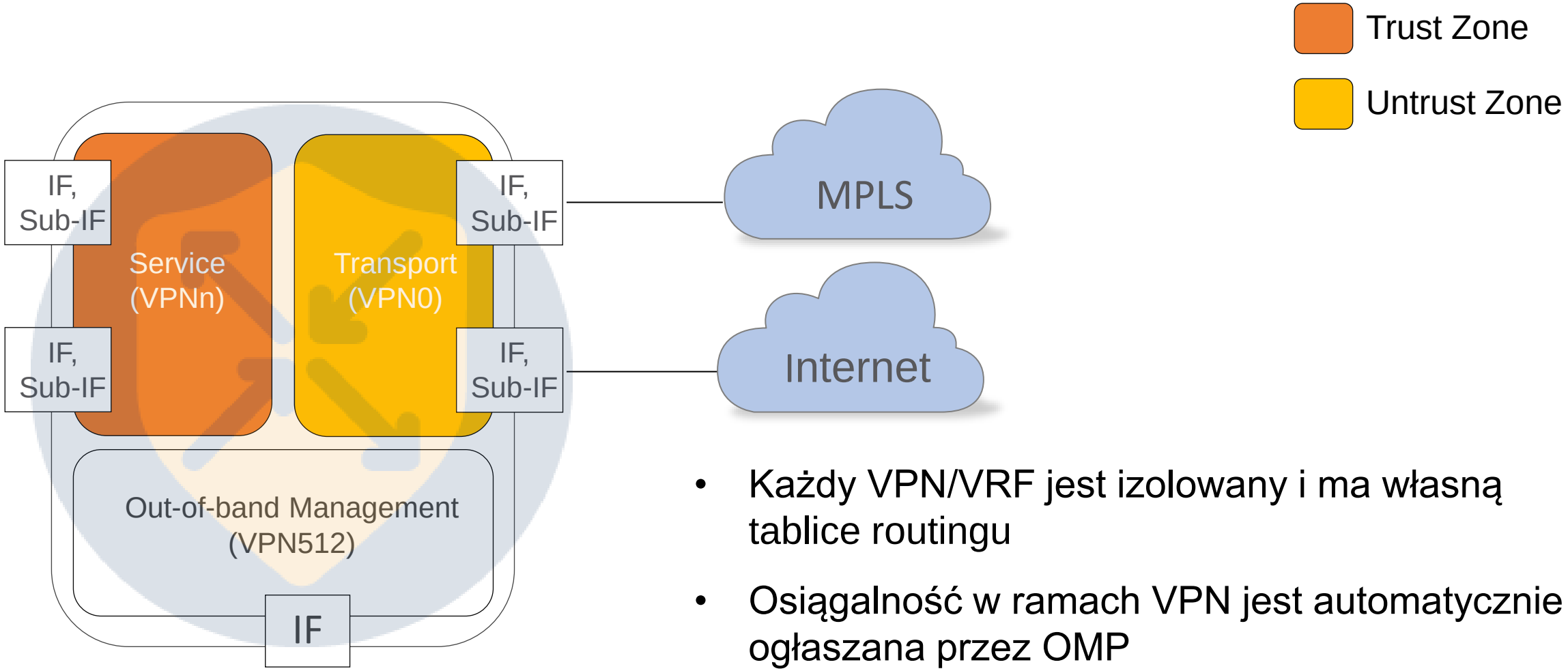
Funkcjonowanie SD-WAN



Update OMP:

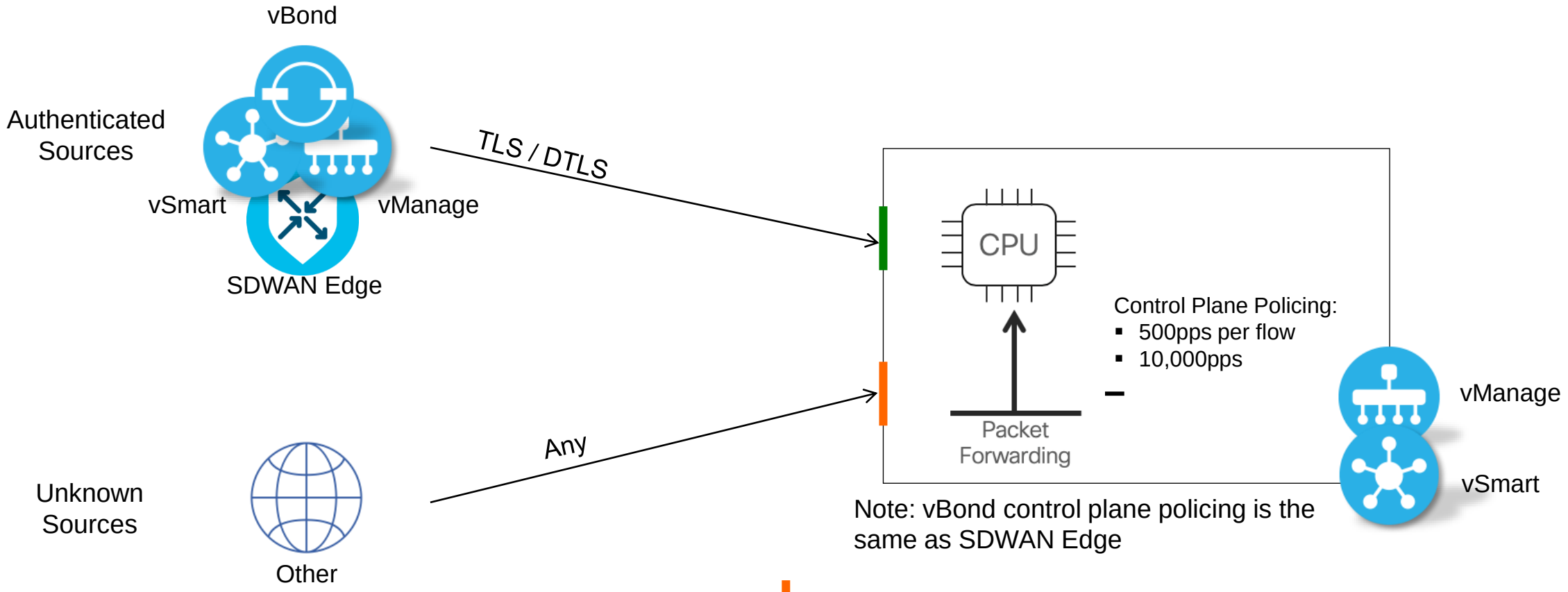
- Osiągalność – IP Subnets, TLOCi
- Bezpieczeństwo – Klucze szyfrujące
- Polityka – Data-plane/polityki aplikacji

Strefy bezpieczeństwa w SD-WAN VPN/VRF

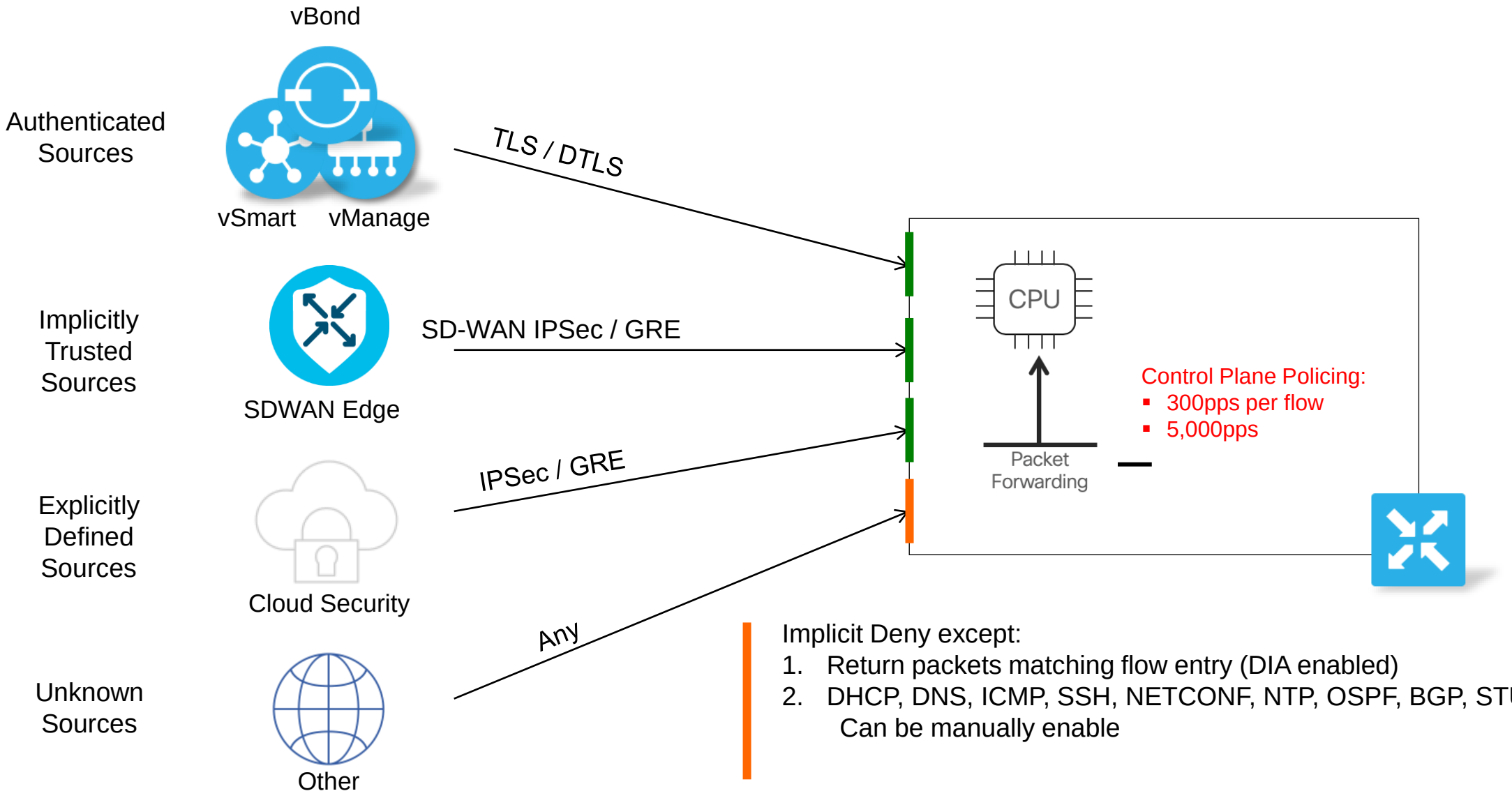


- Każdy VPN/VRF jest izolowany i ma własną tablice routingu
- Osiągalność w ramach VPN jest automatycznie ogłaszana przez OMP

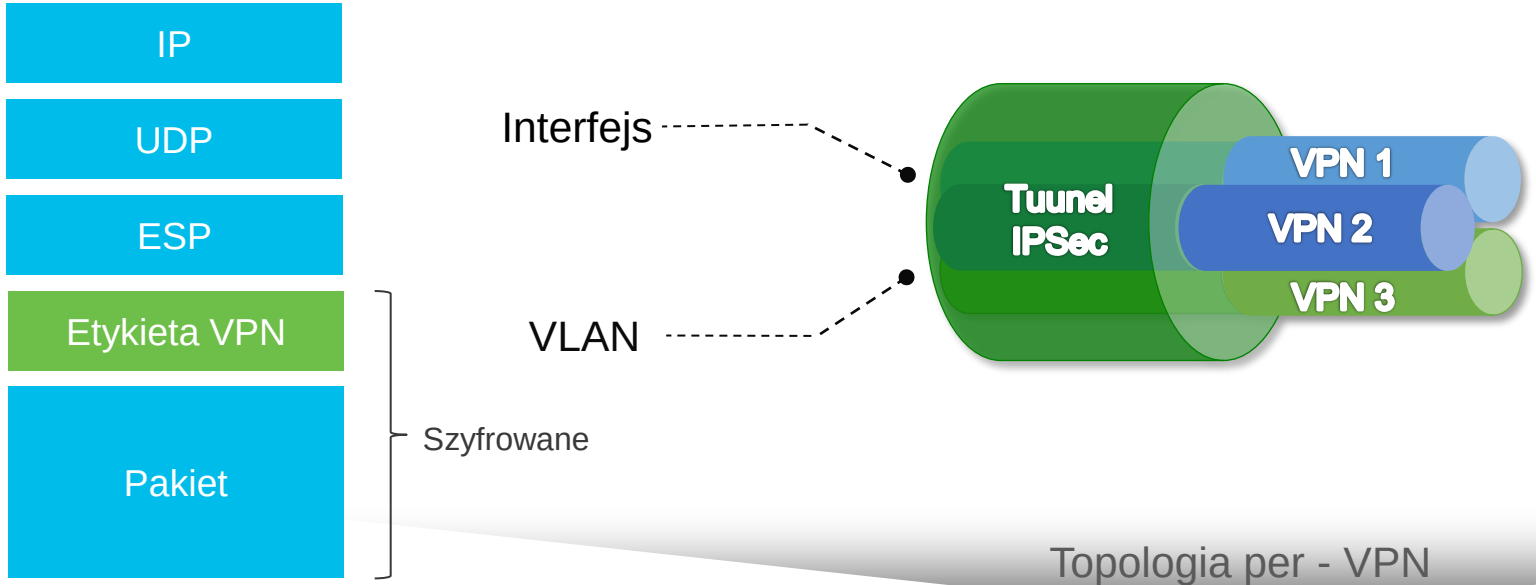
DDoS Protection for Controllers



DDoS Protection for SDWAN Edge Routers



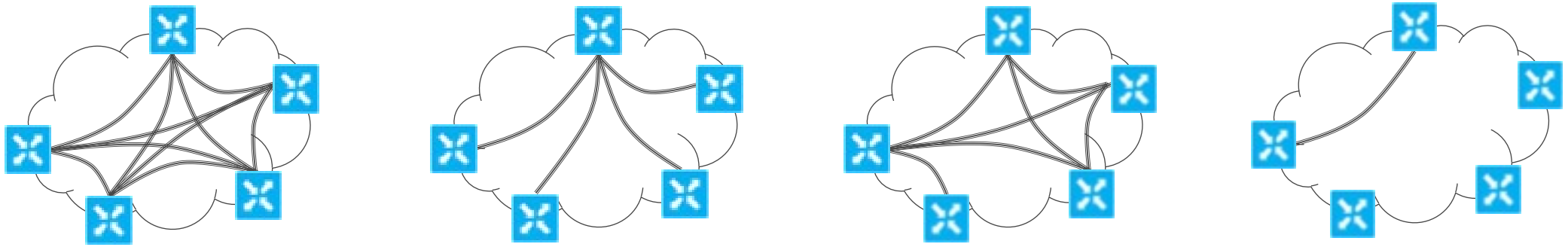
Segmentacja sieci



- Tworzenie ”stref”
- Wymuszanie izolacji
- Gościnne WiFi
- Spółki-córki
- Extranet

https://www.ietf.org/rfc/rfc4023.txt

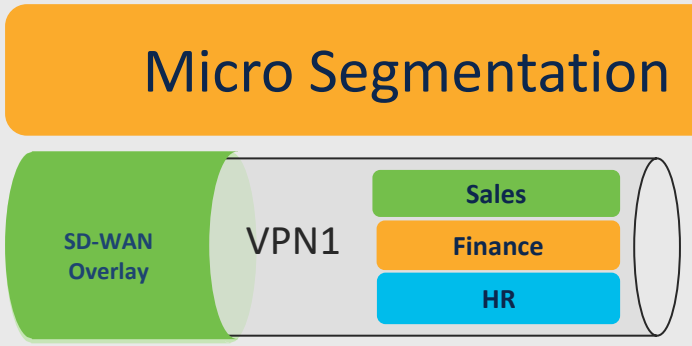
Topologia per - VPN



Full-Mesh | Hub-and-Spoke | Partial Mesh | Point-to-Point

SD-WAN Segmentation

Granular Segmentation Policy



Group/Identity Level Segmentation of Employee VPN1

- Sales, Corporate Laptop
- Finance, BYOD
- HR, Desktop

Identity based

Granular Access to Application Workloads

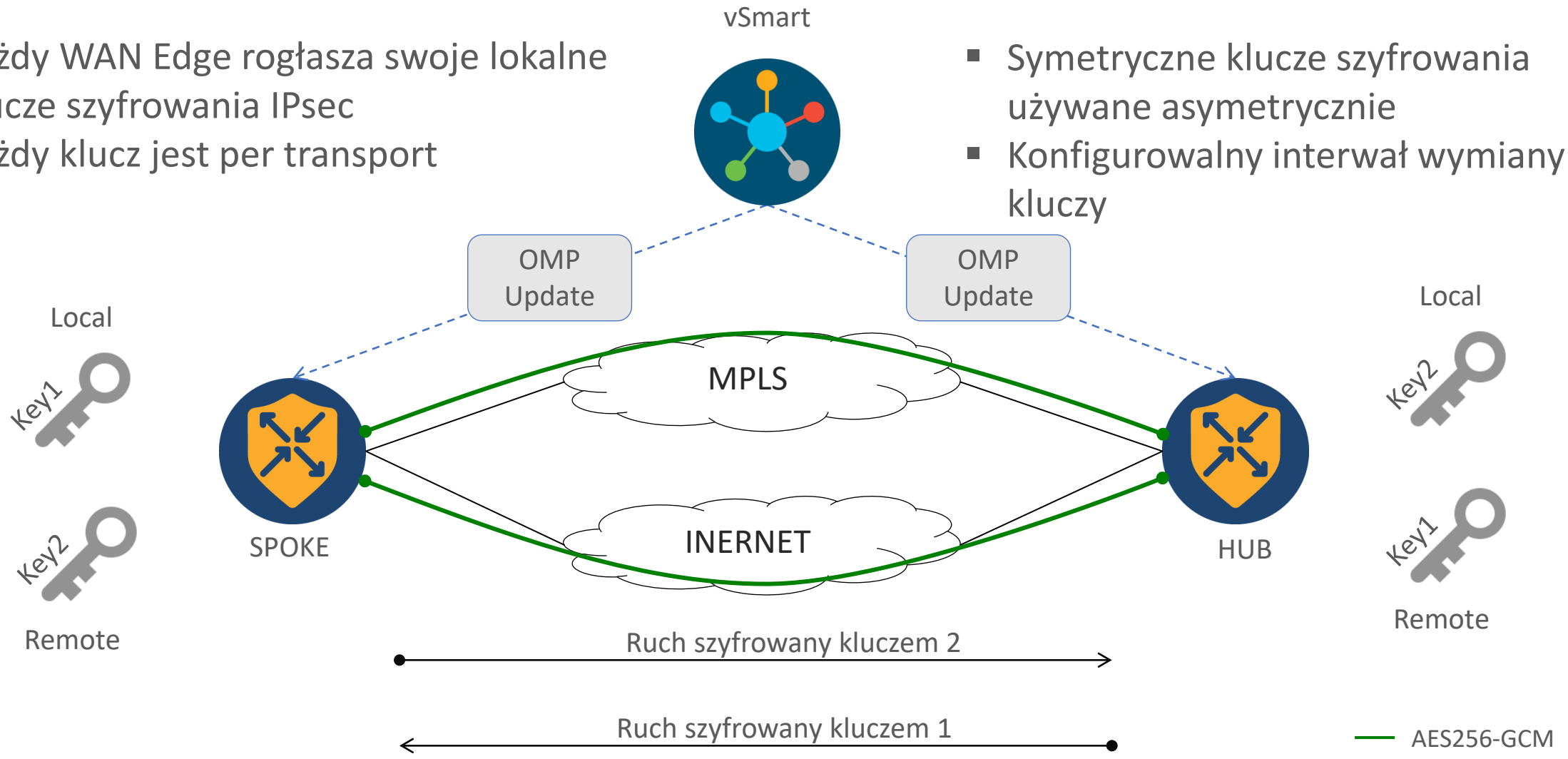
Micro-segmentation and identity-based policy management with Cisco TrustSec®

Duo Zero Trust

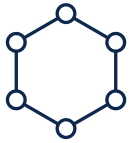
Bezpieczeństwo w warstwie Data Plane

- Każdy WAN Edge rogłasza swoje lokalne klucze szyfrowania IPsec
- Każdy klucz jest per transport

- Symetryczne klucze szyfrowania używane asymetrycznie
- Konfigurowalny interwał wymiany kluczy



Cisco SD-WAN

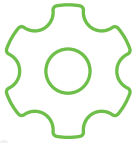


Day 0: Wdrożenie

Routery SD-WAN można bezpiecznie wdrożyć przez proste podłączenie ich na miejscu do przewodu.

Zero konfiguracji, zero troubleshootingu w oddziale.

Bez względu na łącze – MPLS, Internet, 4G/5G



Day 1: Konfiguracja

Szybkie podłączenie – kontrolery z chmury gotowe dla klienta zanim dotrą routery lub czekająca usługa

Konfiguracja hurtowa na bazie wzorców. Brak potrzeby konfiguracji pojedynczych urządzeń.

Podłączenie do IaaS – pojedyncza, krótka konfiguracja dla setek oddziałów

Day 2: Utrzymanie

Potrzeba dostosowania konfiguracji - > zmiany w pojedynczym miejscu kontrolera zamiast na wielu routerach

Problemy z siecią? Proste i skuteczne narzędzia pokazujące GDZIE DOSZŁO DO PROBLEMu i jaka **jest przyczyna**

Technical Marketing Engineers

demo

Cisco vManage | Select Resource Group | Monitor · Overview

Overview | Devices | Tunnels | Security | VPN | Logs | Multicloud

CONTROLLERS
1 vBond
2 vSmart
1 vManage

WAN Edges
4 Reachable
2 Unreachable

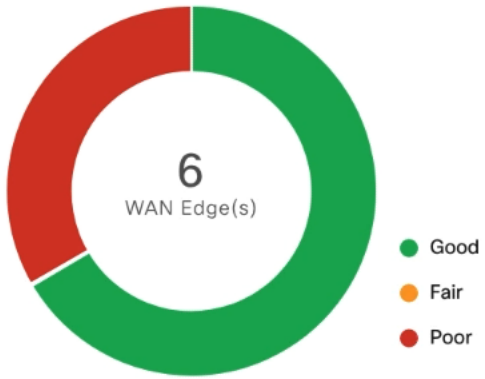
CERTIFICATE STATUS
0 Warning

LICENSING
0 Assigned
12 Unassigned

REBOOT
9 Last 24 hrs

Actions

WAN Edge Health



Geography | All WAN Edges

Site BFD Connectivity (4)

BFD Connectivity	Site
Full	3
Partial	0
Unavailable	1

Transport Interface Distribution

< 10 Mbps	6
10 Mbps - 100 Mbps	0
100 Mbps - 500 Mbps	0
> 500 Mbps	0

View Details

WAN Edge Inventory

Total	62

Transport Health

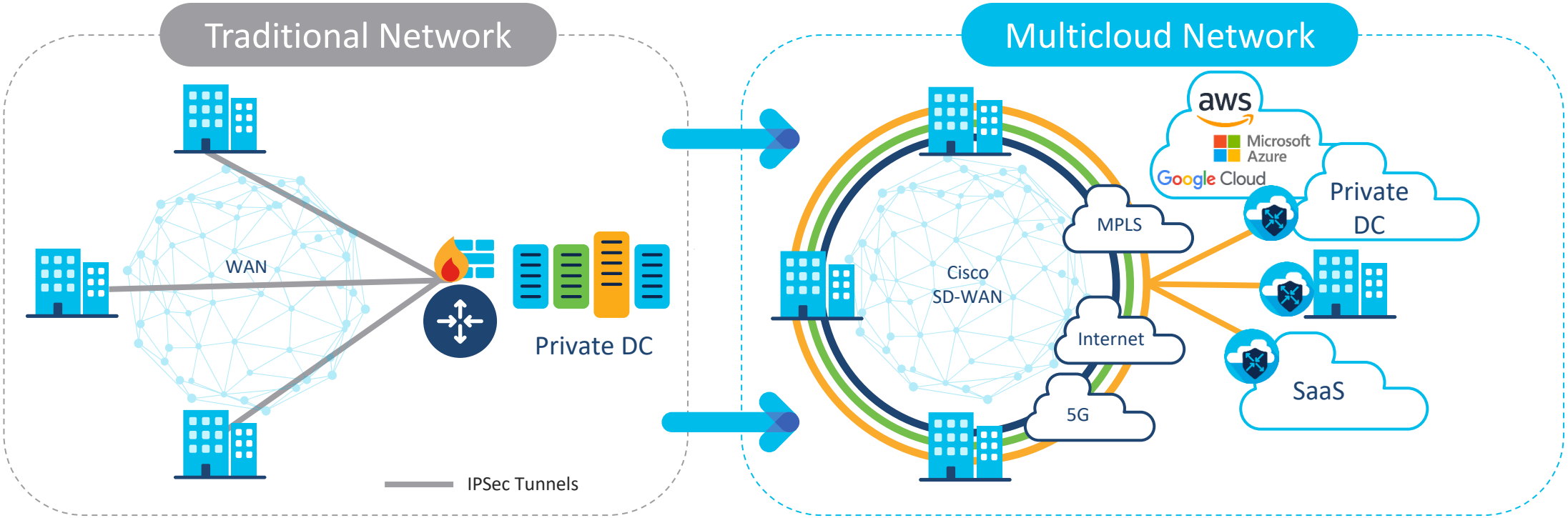
By Loss | 24 Hours

Top Applications

VPN - All | 24 Hours

TECENT-3377

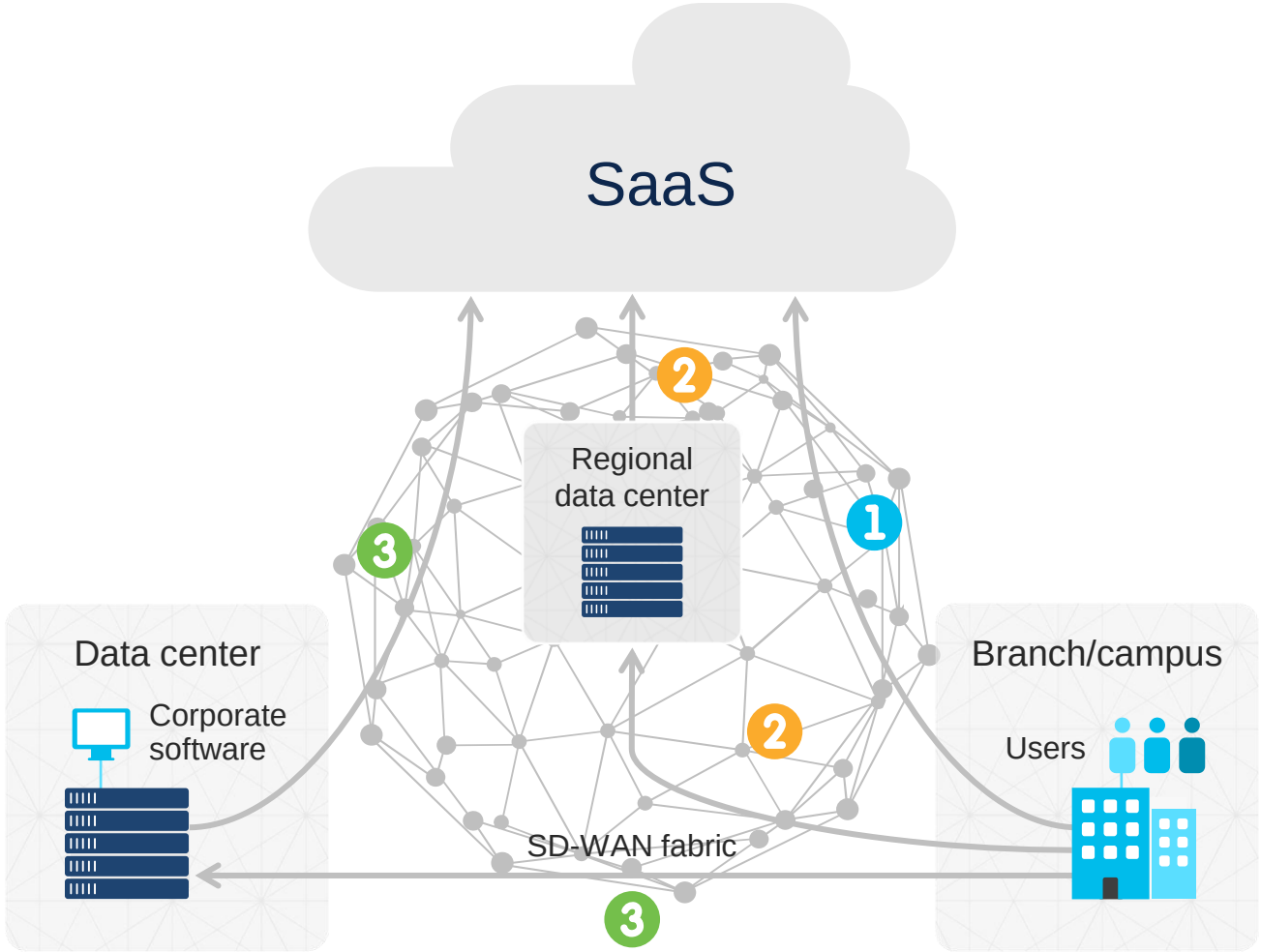
Sieć musi ewoluować aby spełnić kolejne wymagania



Cloud networking is different from traditional networking

COR for SaaS

Dlaczego Cloud OnRamp dla SaaS?
Co realnie daje?



Which path do I use for SaaS applications?

1 Direct internet access	2 Regional breakout	3 Data center backhaul
		
Best quality	Medium quality	Poor quality

Która ścieżka ma lepsze SLA dla M365?

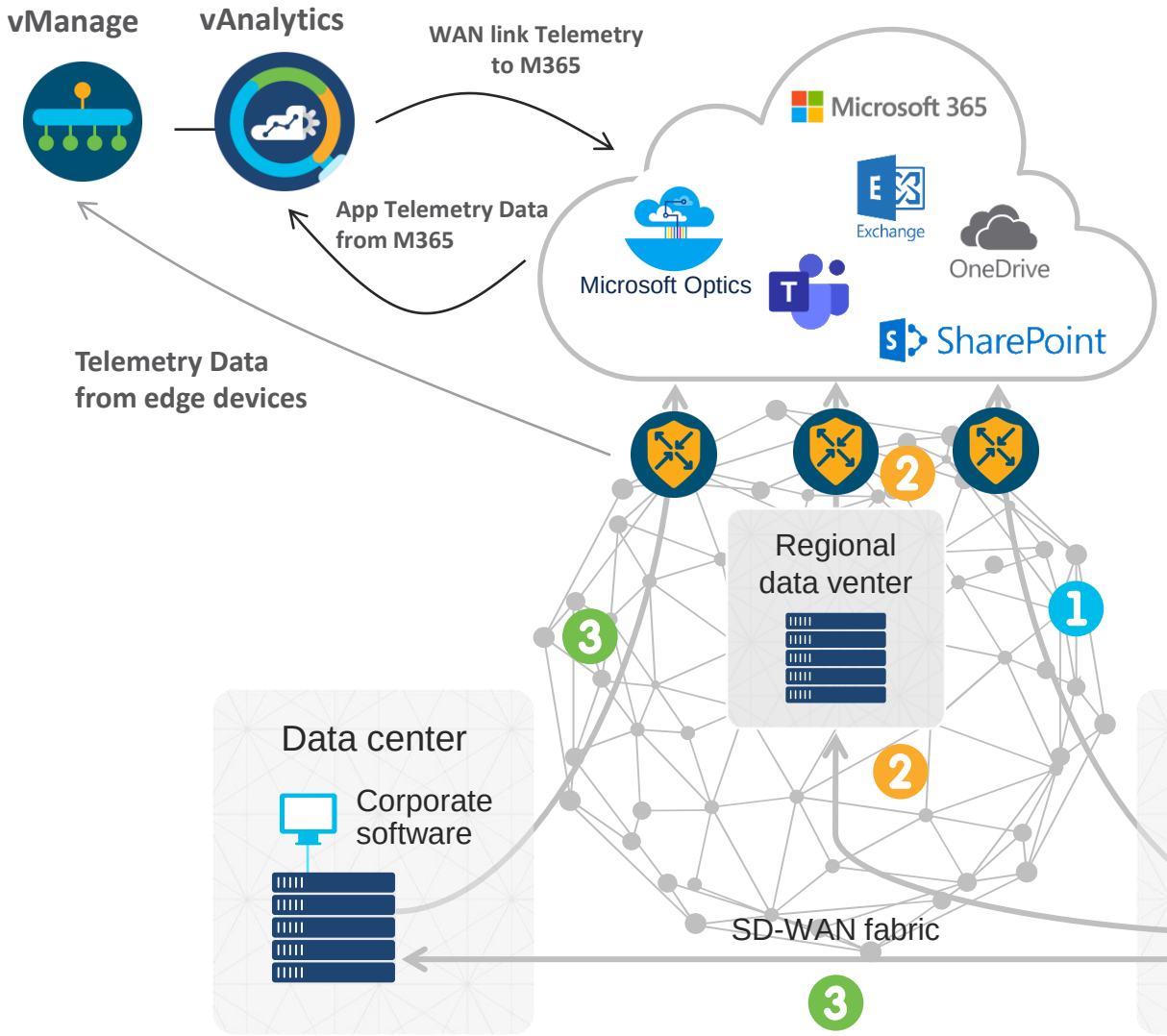
Czy zaufane aplikacje jak M365 mogą wyjść lokalnie?

Czy wszystkie aplikację powinny iść najpierw do DC?

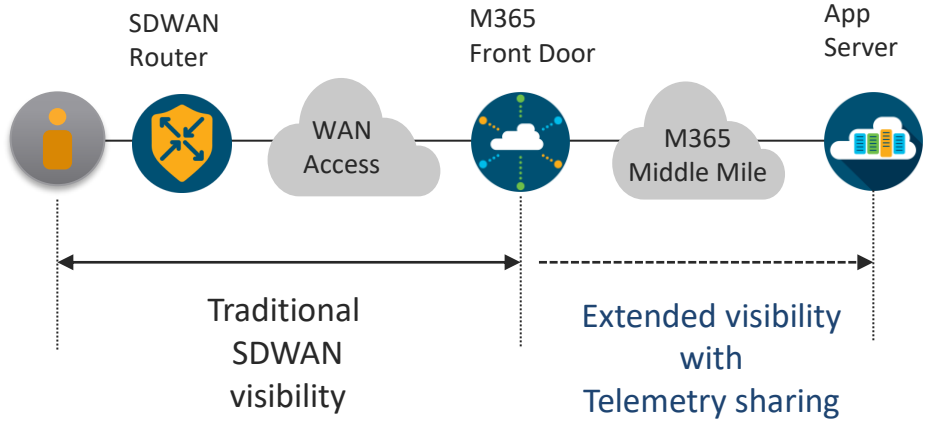
Jak automatycznie sterować ruchem między ścieżkami?

COR for SaaS

Cloud OnRamp for SaaS dla Microsoft 365
Strategiczne partnerstwo z Microsoftem

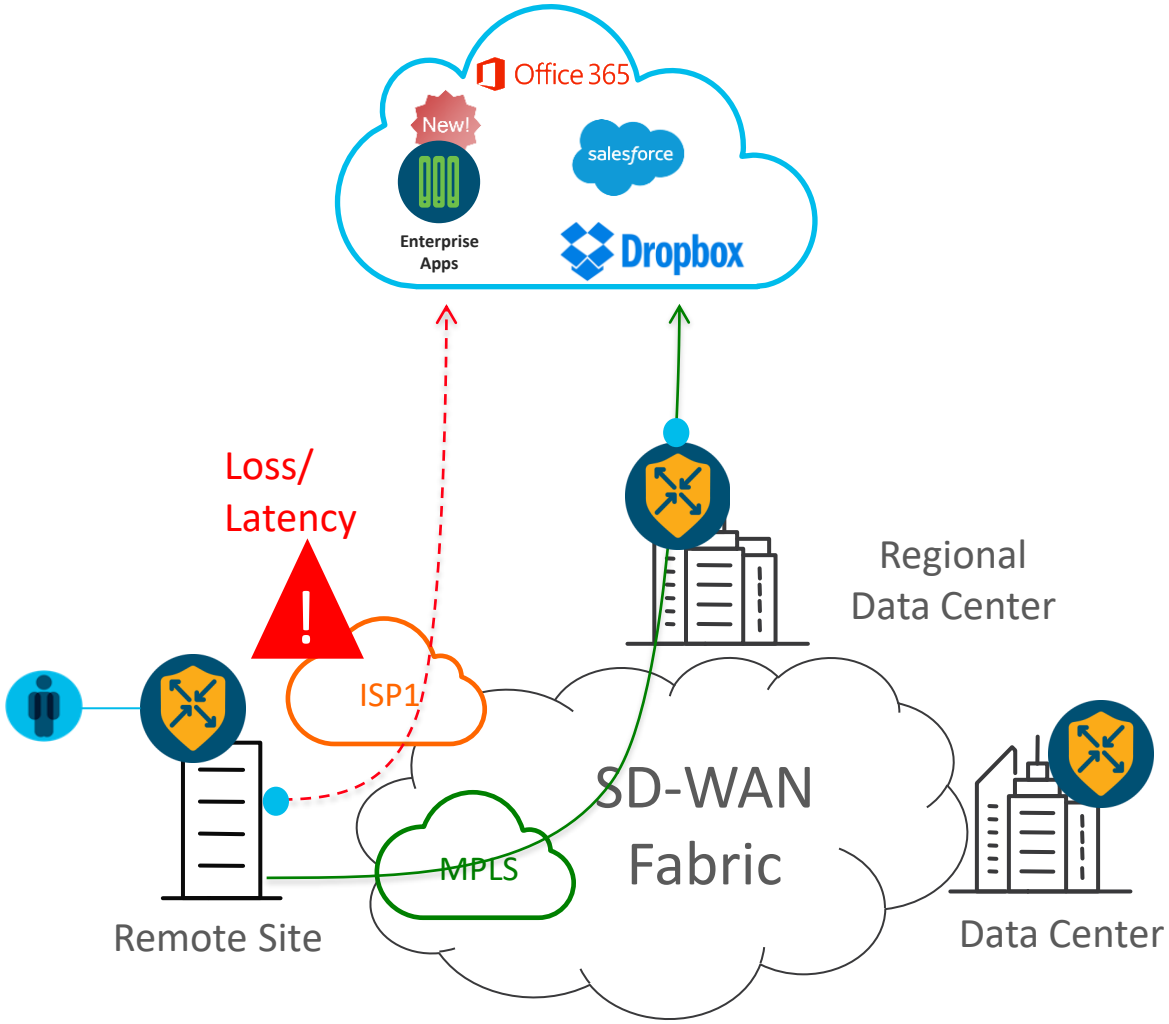


- Jedyny certyfikowa nypartner sieciowy
- Pierwszy vendor SD-WAN otrzymujące telemetrie z M365 – Informed Network Routing
- Routowanie aplikacji w oparciu o działanie łączy i samej aplikacji
- Granularne polityki ruchowe per aplikacja



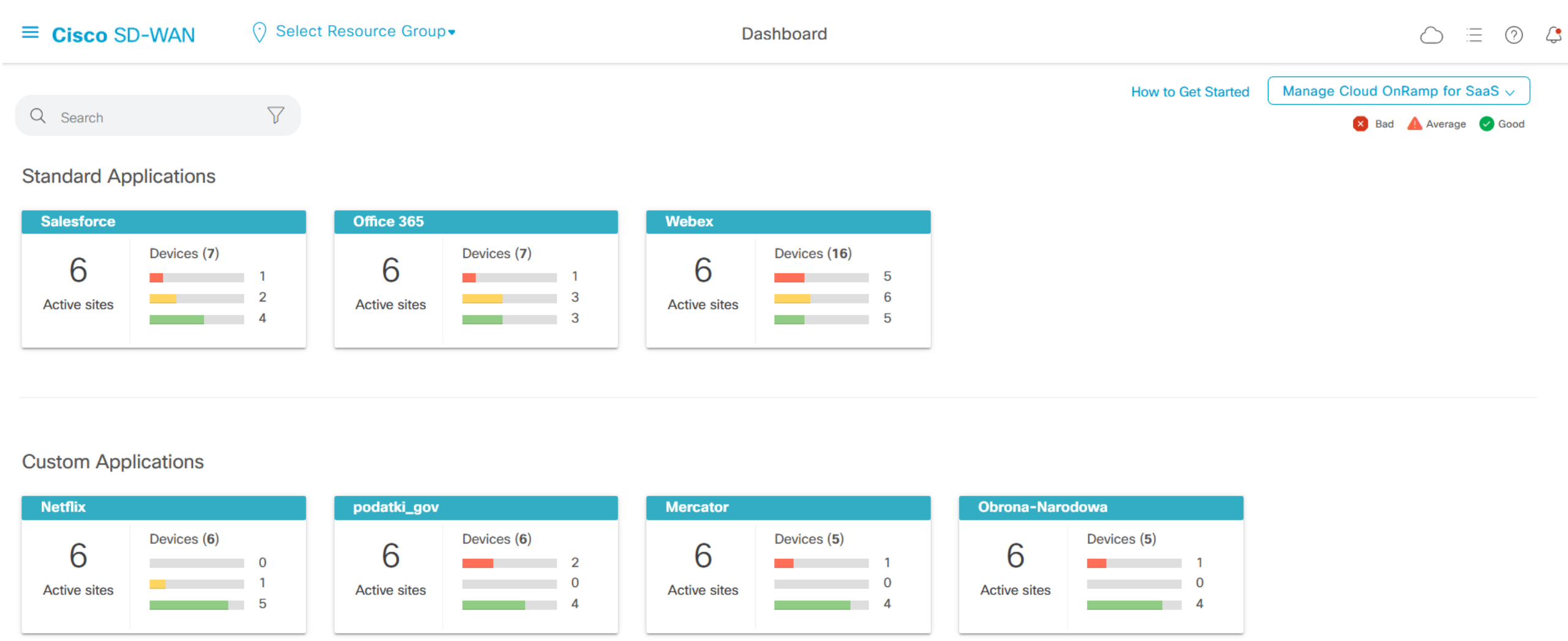
Cloud OnRamp for Applications

- Zapewnienie, że ruch SaaS i Enterprise Apps przechodzi przez najbardziej wydajną ścieżkę.
- Router wysyła próbki HTTP lub HTTPS do zdefiniowanych przez użytkownika punktów końcowych sondy (adres IP lub FQDN lub URL) i oblicza najlepiej działającą ścieżkę dla odpowiednich aplikacji SaaS i Enterprise.
- Na podstawie wyników próbek HTTP/HTTPS ruch aplikacji SaaS i Enterprise jest wysyłany przez najlepiej działającą ścieżkę.



Technical Marketing Engineers

Cloud onRamp for SaaS



Technical Marketing Engineers

Cisco SD-WAN | Select Resource Group | Dashboard

Cloud onRamp for SaaS > Office 365

How to Get Started | Manage Cloud OnRamp for SaaS

Bad (0-5) | Average (5-8) | Good (8-10)

Search

VPN List All

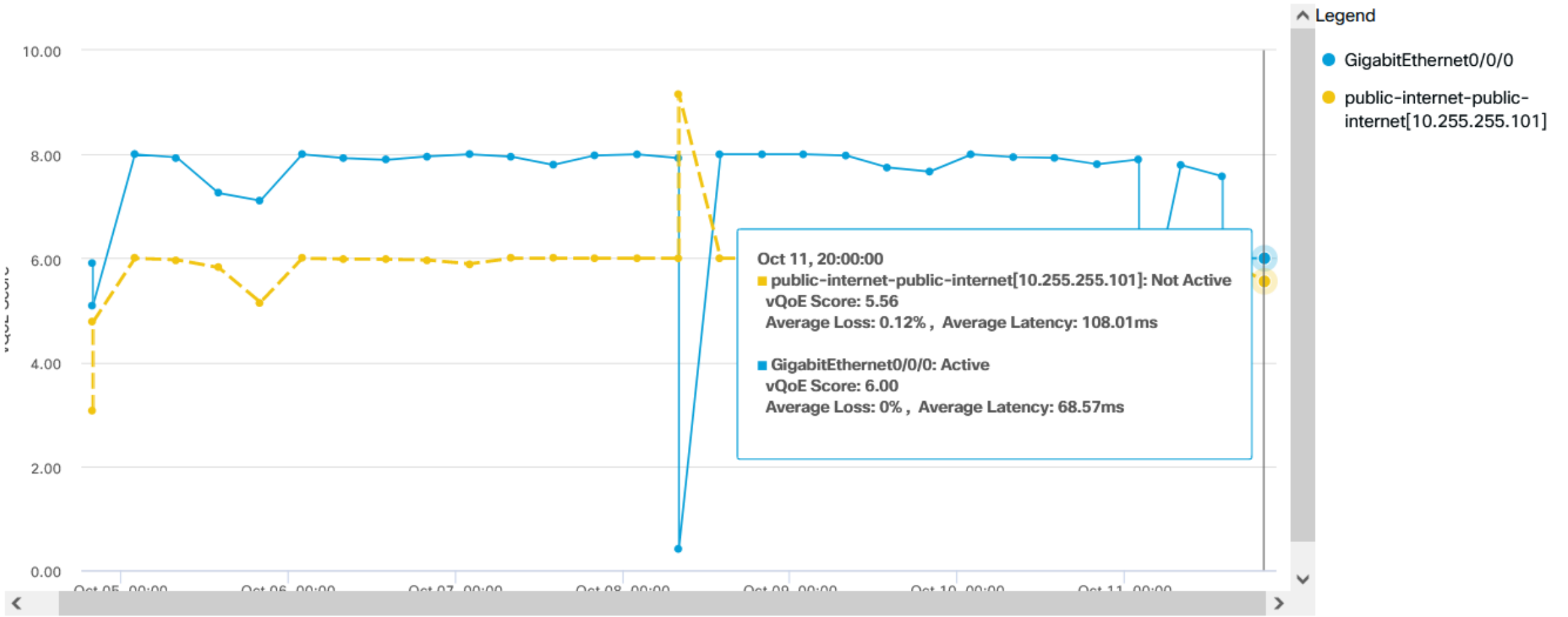
Total Rows: 7

Sites List	Hostname	vQoE Status	vQoE Score	DIA Status	Selected Interface	Activated Gateway	Local Color	Remote Color	Application Usage
100	C8000v-HUB		10.0	local	GigabitEthernet1	N/A	N/A	N/A	View Usage
38	c4331-Warsaw-corpo		8.0	local	GigabitEthernet0/0/0	N/A	N/A	N/A	View Usage
22	makrupin-ISR4321		8.0	gateway	N/A	10.255.255.101	public-internet	public-internet	View Usage
53	c1131X-rtelbusi_ho...		10.0	local	GigabitEthernet0/0/0	N/A	N/A	N/A	View Usage
31	makrupin-CoLoBR1-...		8.0	gateway	N/A	10.255.255.101	public-internet	public-internet	View Usage
56	c1111_LTE_WiFi		7.0	local	GigabitEthernet0/0/0	N/A	N/A	N/A	View Usage
21	makrupin-C1111X-8P		9.0	gateway	N/A	10.255.255.101	public-internet	public-internet	View Usage

vQoE Score History (office365,c4331-Warsaw-corpo)

Service Area: CoR SaaS Probe

1h 3h 6h 12h 24h 7days Custom



How to Get Started | Manage Cloud OnRamp for SaaS

Bad (0-5) Average (5-8) Good (8-10)

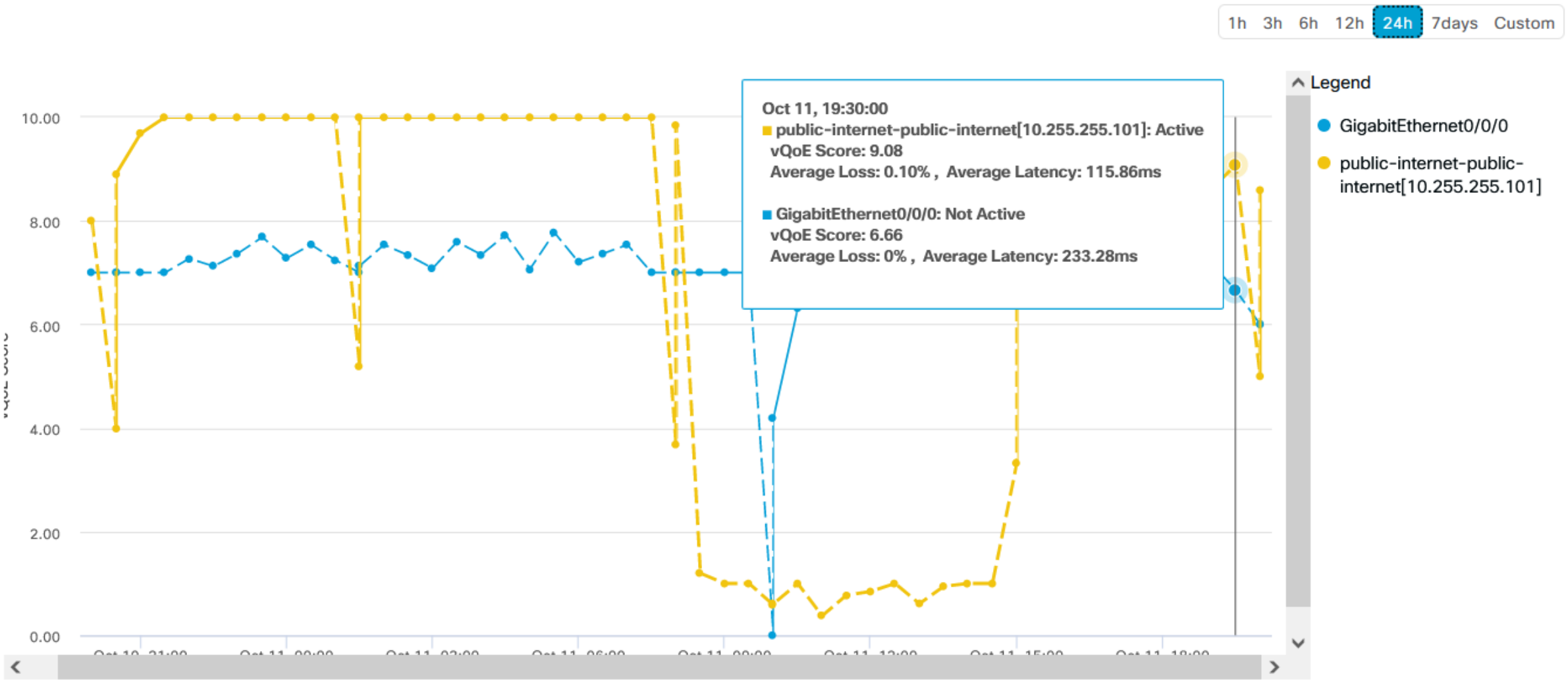
Search

VPN List All

Total Rows: 6

Sites List	Hostname	vQoE Status	vQoE Score	DIA Status	Selected Interface	Activated Gateway	Local Color
100	C8000v-HUB		10.0	local	GigabitEthernet1	N/A	N/A
38	c4331-Warsaw-corpo		3.0	gateway	N/A	10.255.255.101	public-internet
56	c1111_LTE_WiFi		1.0	local	GigabitEthernet0/0/0	N/A	N/A
53	c1131X-rtelbusi_home		10.0	local	GigabitEthernet0/0/0	N/A	N/A
31	makrupin-CoLoBR1-v8000		10.0	gateway	N/A	10.255.255.101	public-internet
21	makrupin-C1111X-8P		10.0	local	GigabitEthernet0/0/0	N/A	N/A

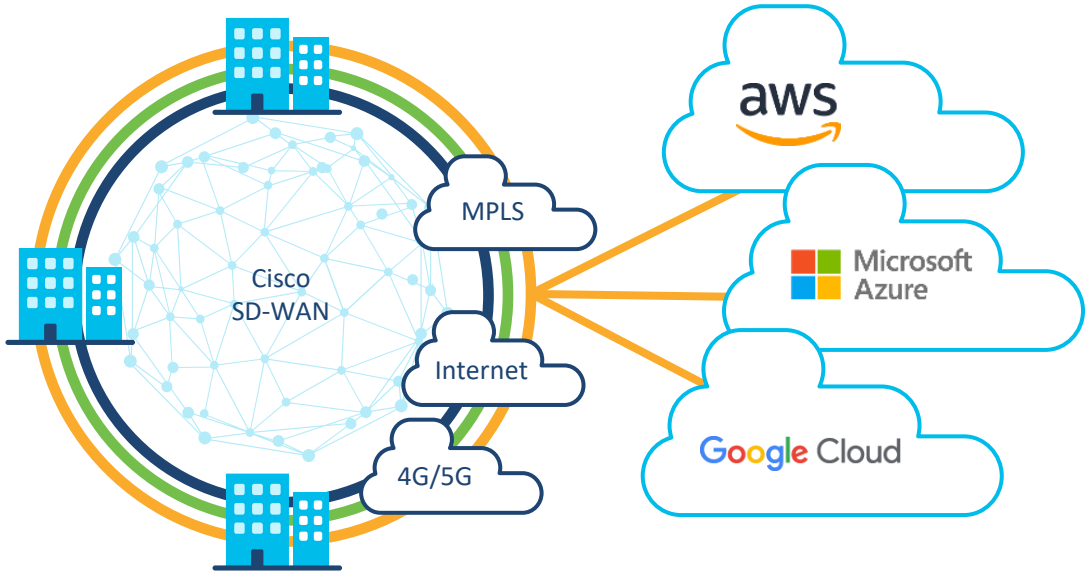
vQoE Score History (podatki_gov,c4331-Warsaw-corpo)



Cloud OnRamp for IaaS

Automatyzacja i ujednolicona konfiguracja dla różnych usług IaaS

Obsługa 3 głównych usługodawców – AWS, Azure, GCP



Automatyzacja
Cztero-krokowy workflow

Ujednolicony sposób konfiguracji
To samo GUI i te same procesy konfiguracyjne dla usługodawców

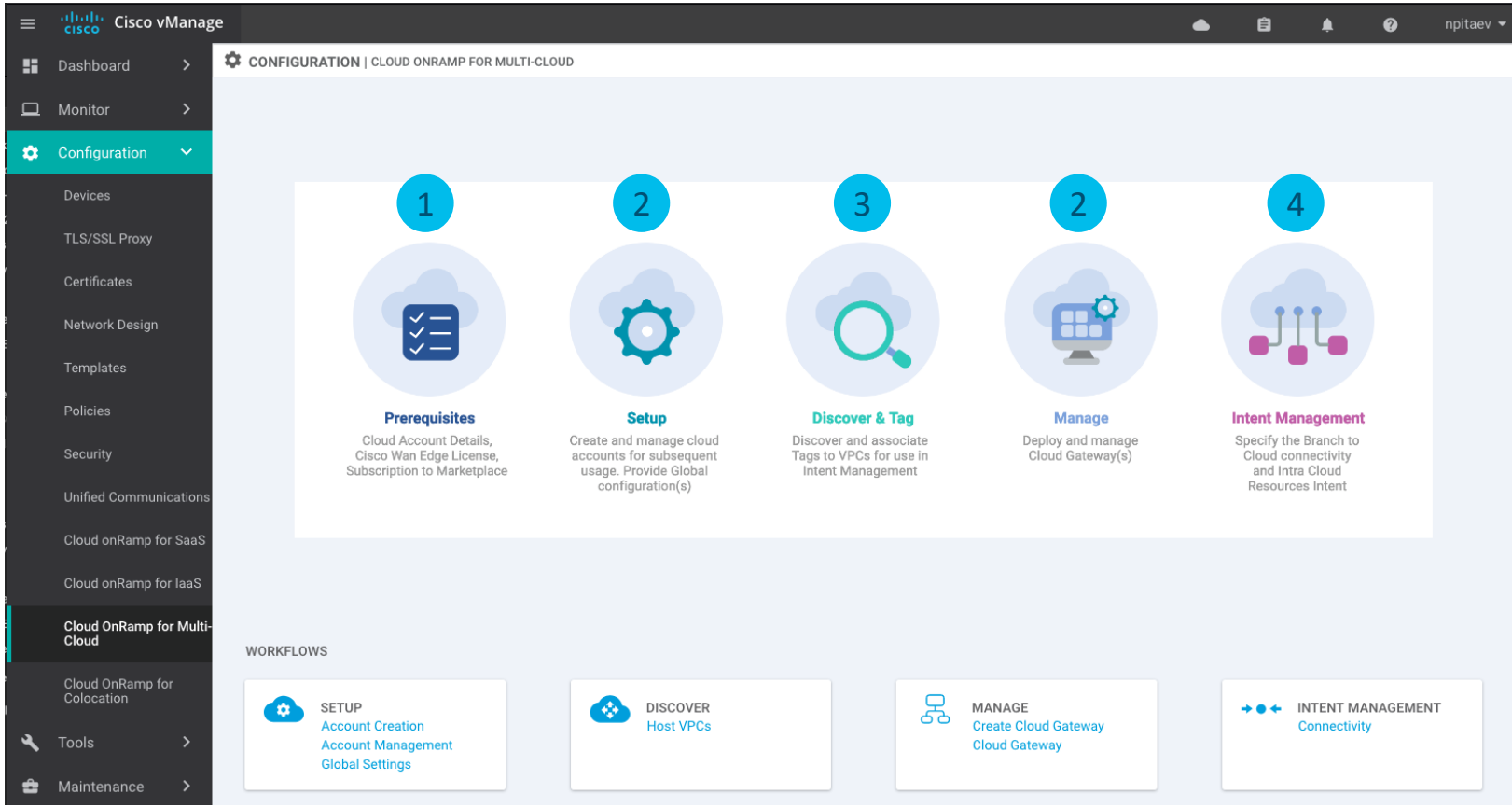
Jednolite polityki bezpieczeństwa
Umożliwiają rociągnięcie segmentacji i NGFW do chmury

Proste zmiany konfiguracji
Wszystko zarządzane z poziomu vManage

Cloud OnRamp Automation on vManage

Ten sam sposób konfiguracji 3 CSP (AWS, Azure, Google Cloud)

1. Credentiale do chmury
2. Provisioning Cloud routerów
3. Sprawdzenie sieci w chmurze
4. Mapowanie segmentów



Tworzymy most między światem chmurowym a tym na ziemi

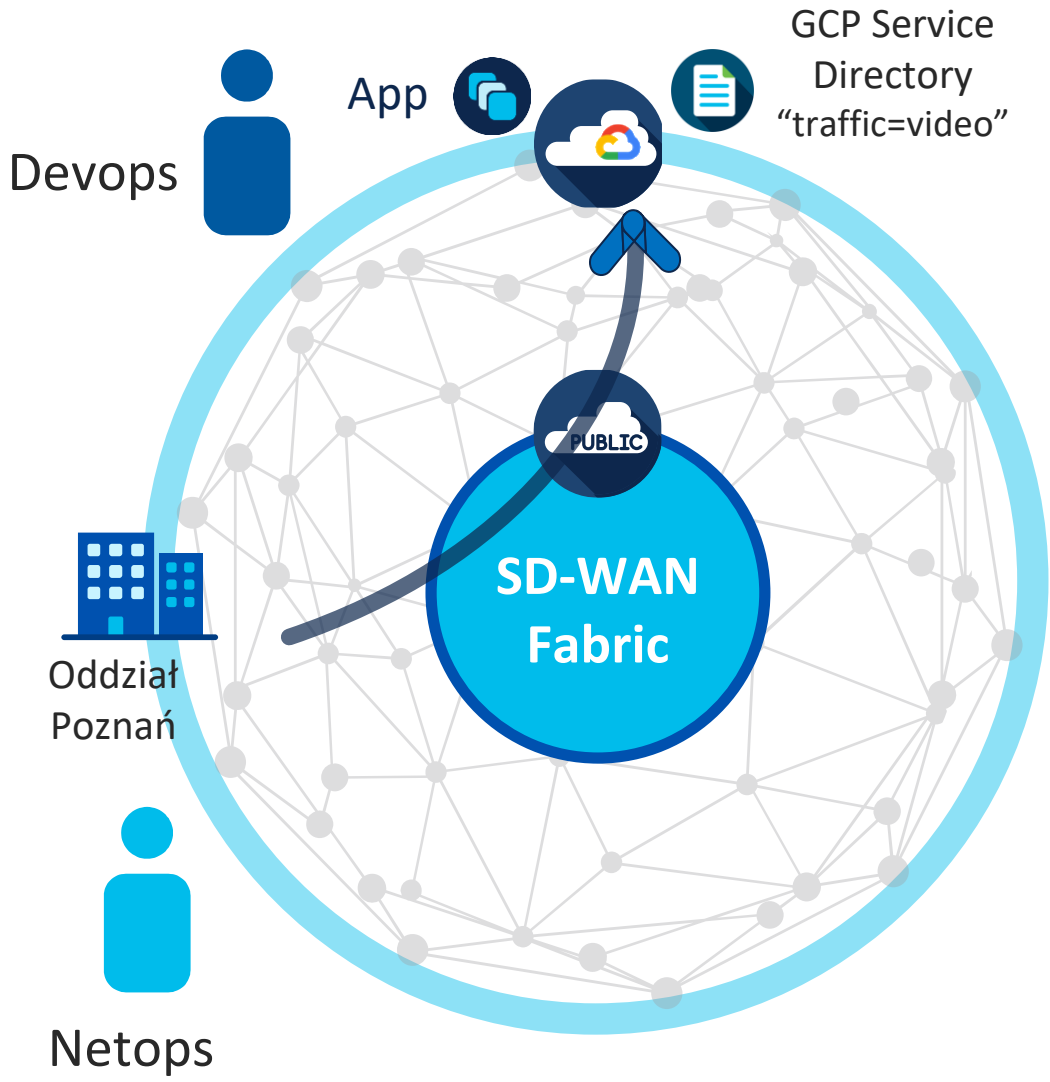
Use Case

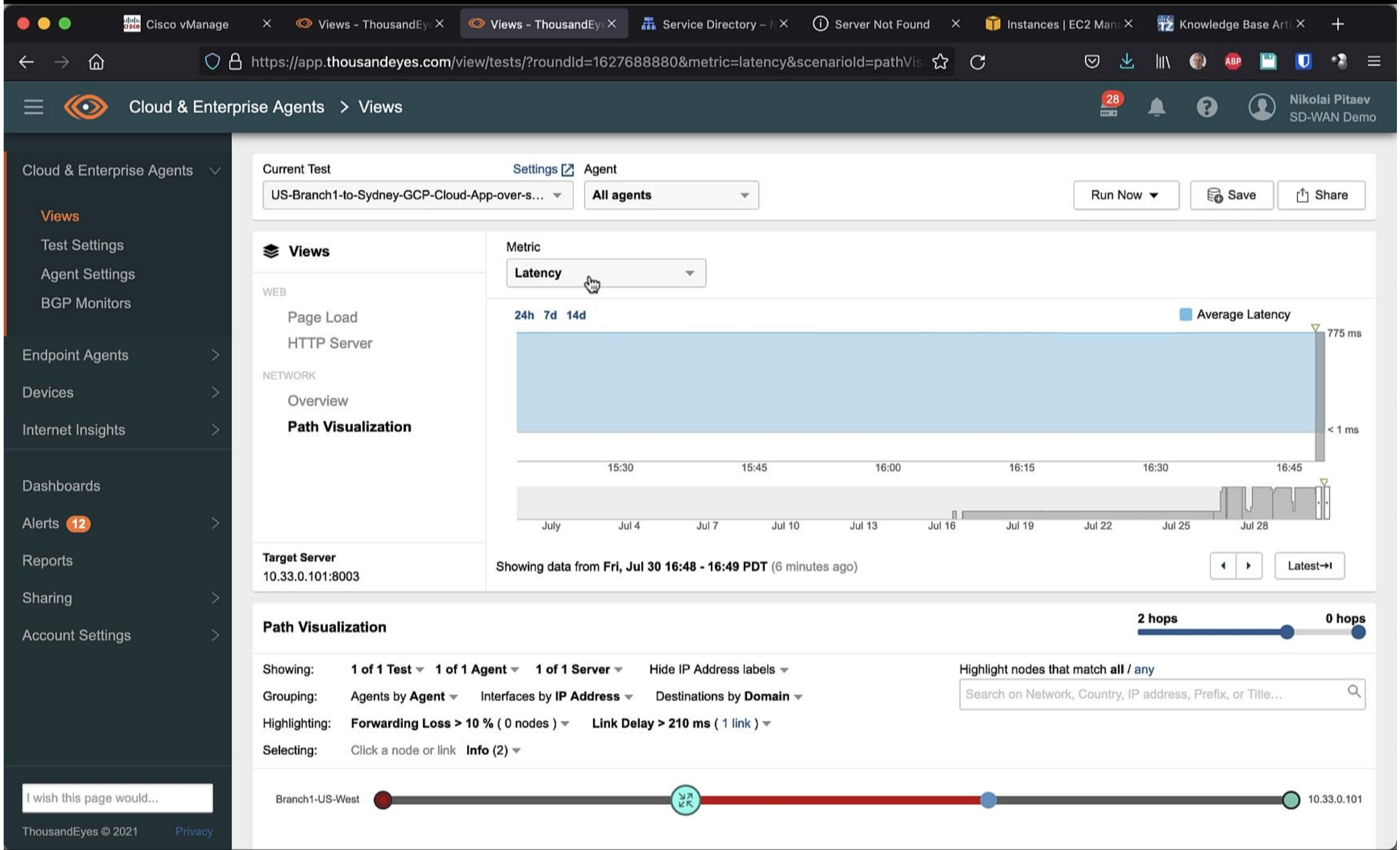
Zespół Devops rejestruje aplikacje cloudową w GCP Service Directory

vManage samodzielnie wykrywa tą aplikację

Zespół Netops tworzy w vManage odpowiednią politykę sieciową zapewniającą jakość działania tej aplikacji

Następnie ktoś usuwa konfiguracje sieciową w chmurze



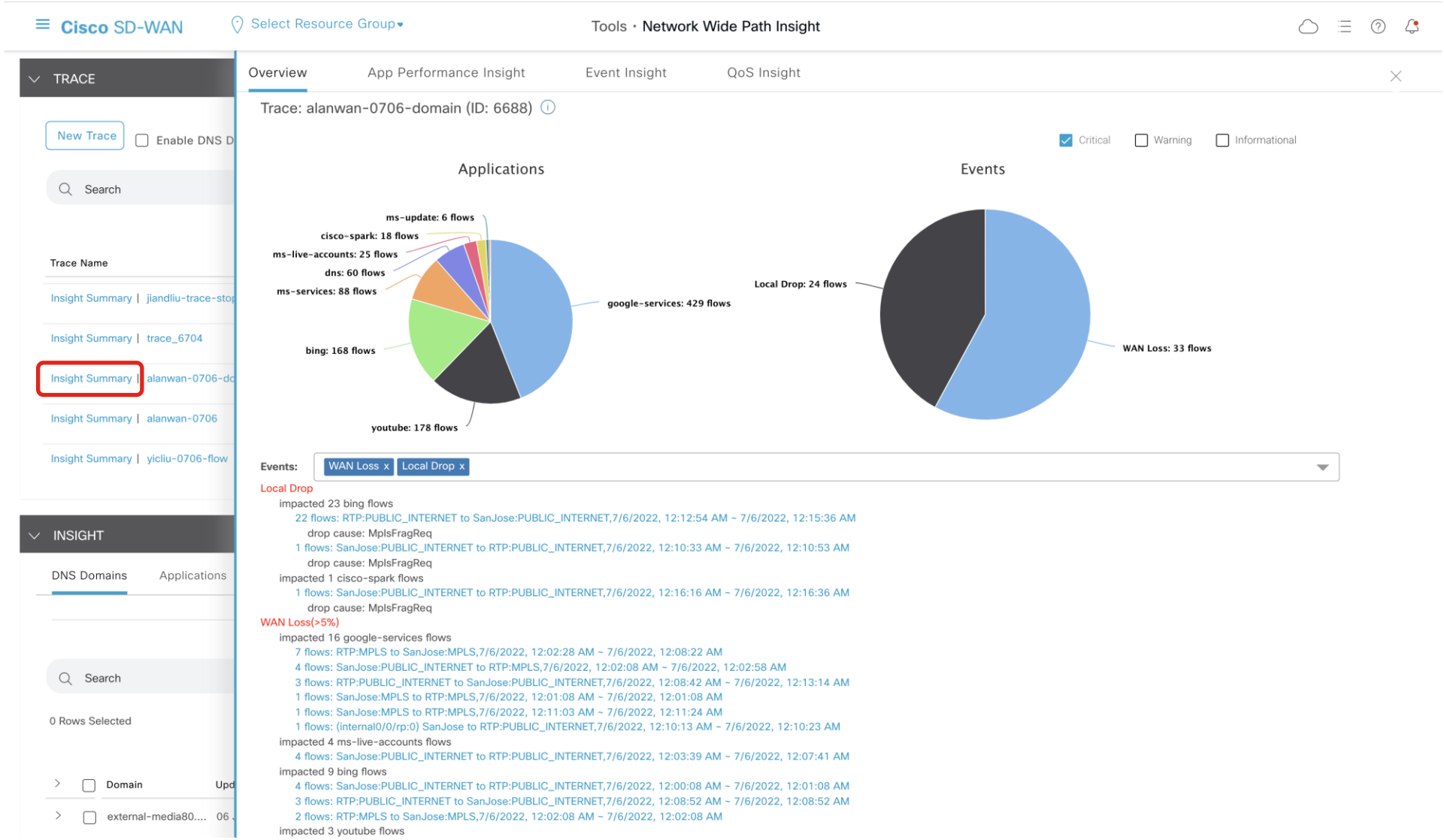

Cisco vManage
Views - ThousandEy
Views - ThousandEy
Service Directory – N
Server Not Found
Instances | EC2 Man
Knowledge Base Arti
https://app.thousandeyes.com/view/tests/?roundId=1627688880&metric=latency&scenarioId=pathVis
Cloud & Enterprise Agents > Views
28
Nikolai Pitaev
SD-WAN Demo
Cloud & Enterprise Agents
Views
Test Settings
Agent Settings
BGP Monitors
Endpoint Agents
Devices
Internet Insights
Dashboards
Alerts 12
Reports
Sharing
Account Settings
I wish this page would...
ThousandEyes © 2021
Privacy
Current Test
Settings
US-Branch1-to-Sydney-GCP-Cloud-App-over-s...
Agent
All agents
Run Now
Save
Share
Views
WEB
Page Load
HTTP Server
NETWORK
Overview
Path Visualization
Metric
Latency
24h 7d 14d
Average Latency
775 ms
< 1 ms
15:30
15:45
16:00
16:15
16:30
16:45
July
Jul 4
Jul 7
Jul 10
Jul 13
Jul 16
Jul 19
Jul 22
Jul 25
Jul 28
Target Server
10.33.0.101:8003
Showing data from Fri, Jul 30 16:48 - 16:49 PDT (6 minutes ago)
Latest
Path Visualization
2 hops
0 hops
Showing: 1 of 1 Test 1 of 1 Agent 1 of 1 Server Hide IP Address labels
Grouping: Agents by Agent Interfaces by IP Address Destinations by Domain
Highlighting: Forwarding Loss > 10 % (0 nodes) Link Delay > 210 ms (1 link)
Selecting: Click a node or link Info (2)
Highlight nodes that match all / any
Search on Network, Country, IP address, Prefix, or Title...
Branch1-US-West
10.33.0.101

Rozwiązywanie problemów zanim się pojawią

Day 2 - utrzymanie

- Zarządzanie politykami
- Zarządzanie template’ami
- NWPI,
- vAnalytics
- WAN Insights
- ThousandEyes

NWPI Insight Summary

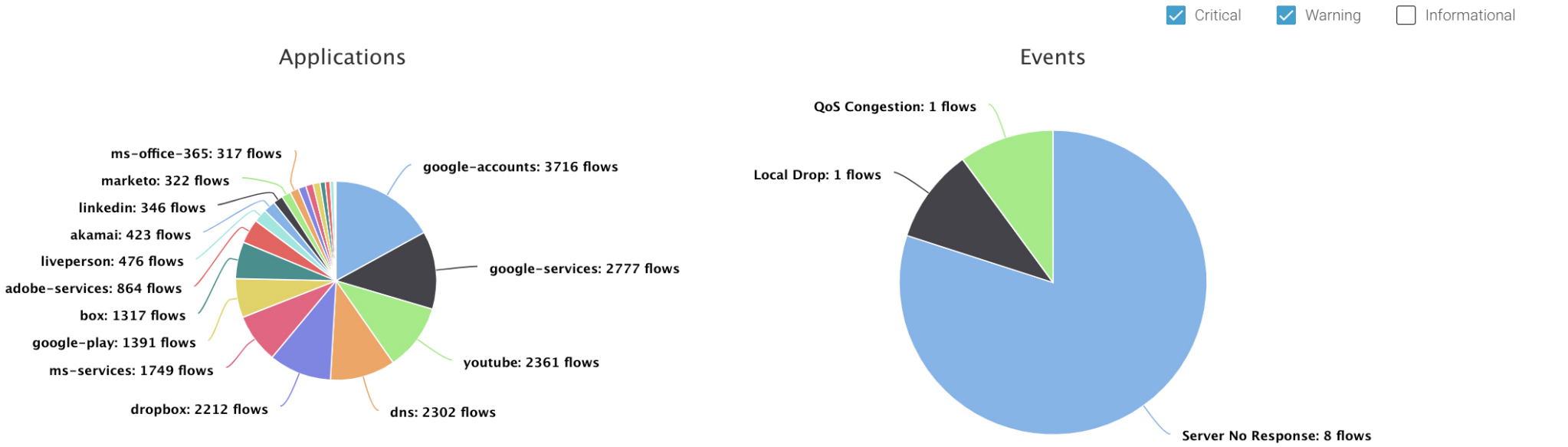


Technical Marketing Engineers

Insight Summary - Overview

Overview | App Performance Insight | Event Insight | QoS Insight

Trace: alanwan-0723-domain2 (ID: 8624)



Events: Server No Response x | Local Drop x | QoS Congestion x

What

Server No Response
impacted 7 unknown flows
4 flows: SJC-Branch:MPLS to RTP-Hub1:MPLS,7/23/2022, 2:27:16 PM ~ 7/23/2022, 2:28:23 PM
3 flows: SJC-Branch:MPLS to RTP-Hub1:MPLS,7/23/2022, 2:43:01 PM ~ 7/23/2022, 2:43:25 PM
4 flows: RTP-Hub1:PUBLIC_INTERNET to SHN-Branch1:PUBLIC_INTERNET,7/23/2022, 2:27:16 PM ~ 7/23/2022, 2:28:15 PM
3 flows: RTP-Hub1:PUBLIC_INTERNET to SHN-Branch1:PUBLIC_INTERNET,7/23/2022, 2:43:01 PM ~ 7/23/2022, 2:43:25 PM

Who

impacted 1 adobe-services flows
1 flows: SJC-Branch:MPLS to RTP-Hub1:MPLS,7/23/2022, 2:43:58 PM ~ 7/23/2022, 2:44:57 PM

When

Where

1 flows: RTP-Hub1:PUBLIC_INTERNET to SHN-Branch1:PUBLIC_INTERNET,7/23/2022, 2:43:58 PM ~ 7/23/2022, 2:44:57 PM

Local Drop
impacted 1 box flows
1 flows: SJC-Branch:MPLS to RTP-Hub1:MPLS,7/23/2022, 2:18:19 PM ~ 7/23/2022, 2:18:40 PM

Why

drop cause: TailDrop

QoS Congestion
impacted 1 box flows
1 flows: SJC-Branch:MPLS to RTP-Hub1:MPLS,7/23/2022, 2:18:19 PM ~ 7/23/2022, 2:18:40 PM
policy: qos_template, type: qosMap, queue: 1

Hyperlink

Hyperlink will help user quickly spot impacted flows in one click and drill down to deeper understanding of **“Why”.**

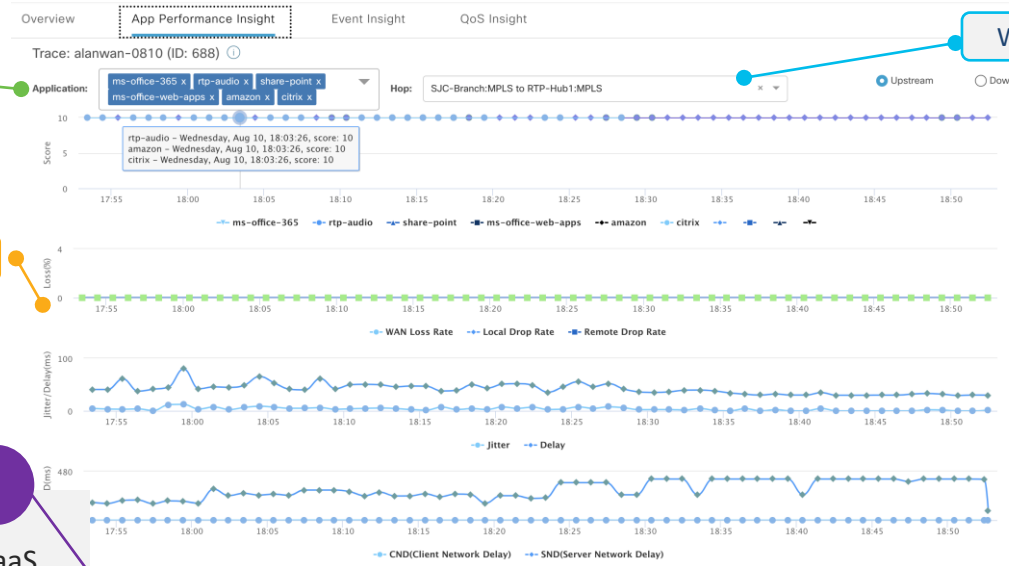
Insight Summary - App Performance Insight

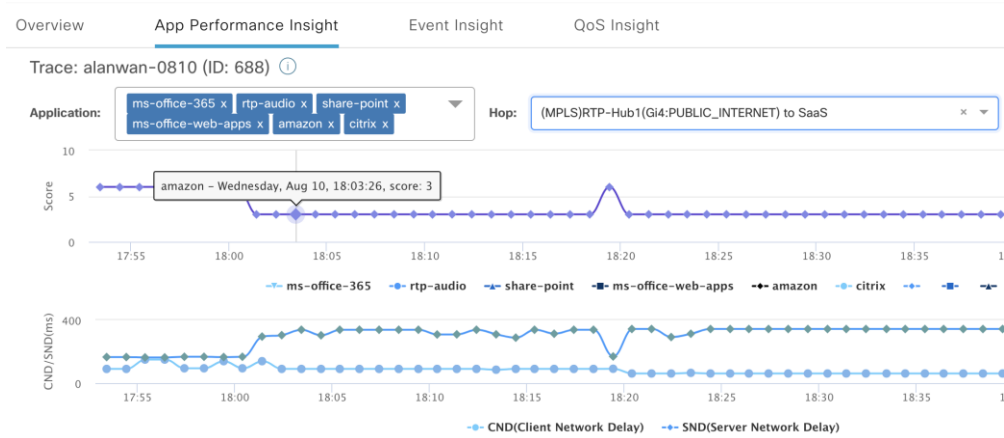
Who

What

When

Where





Readout

M365: SJC-Branch local breakout to SaaS Cloud via INET(DIA).

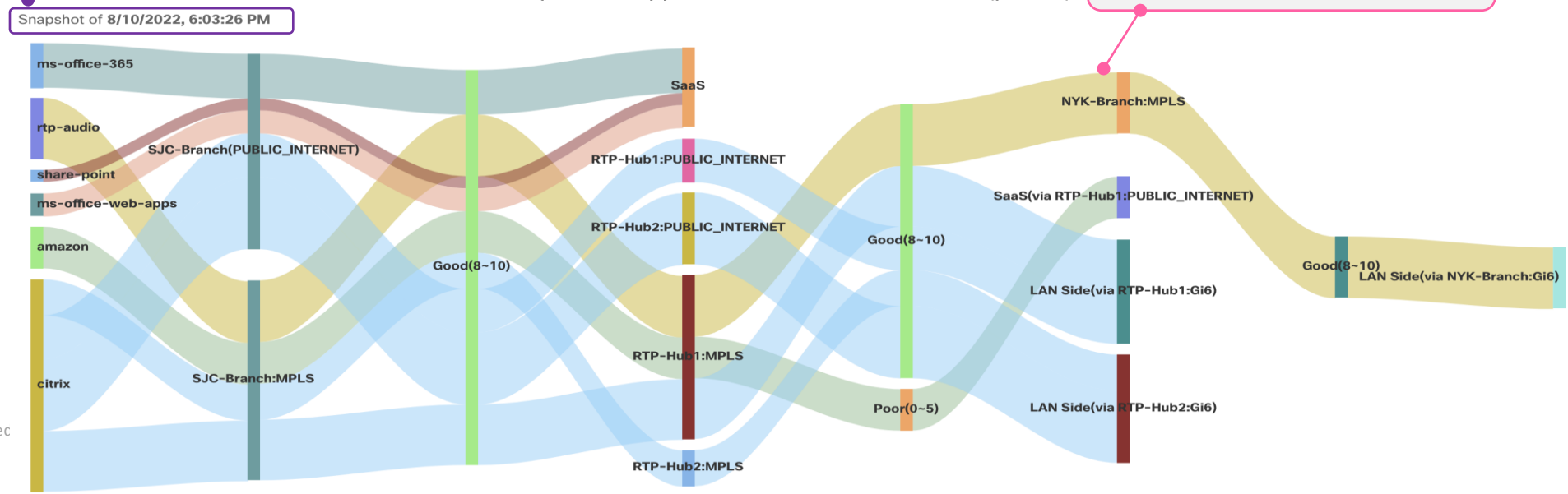
Amazon: Backhaul from SJC-branch to RTP-Hub1 via MPLS, then breakout to SaaS Cloud via INET(DIA).
Poor performance on the hop:
RTP-Hub1 to SaaS (via INET)
high server network delay, score 3

rtp-audio: SJC-Branch to NYK-Branch via RTP-Hub1 (MPLS)

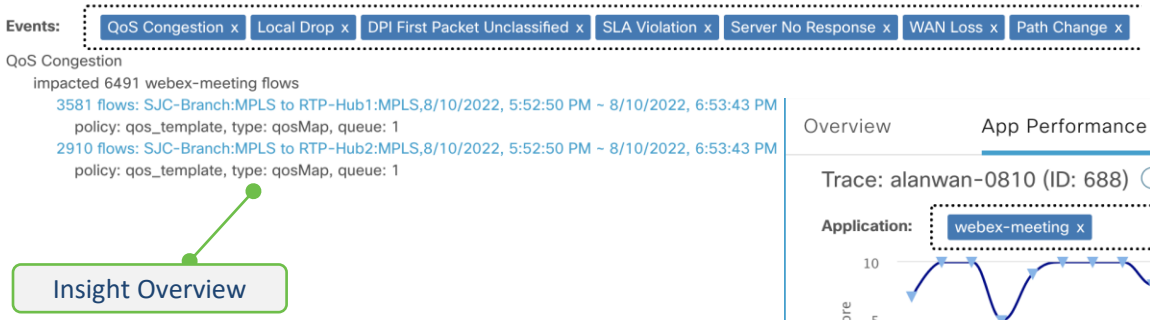
Citrix: Load balance from SJC-branch to RTP-Hub1/Hub2 via MPLS/INET, then toward Campus/DC via LAN.

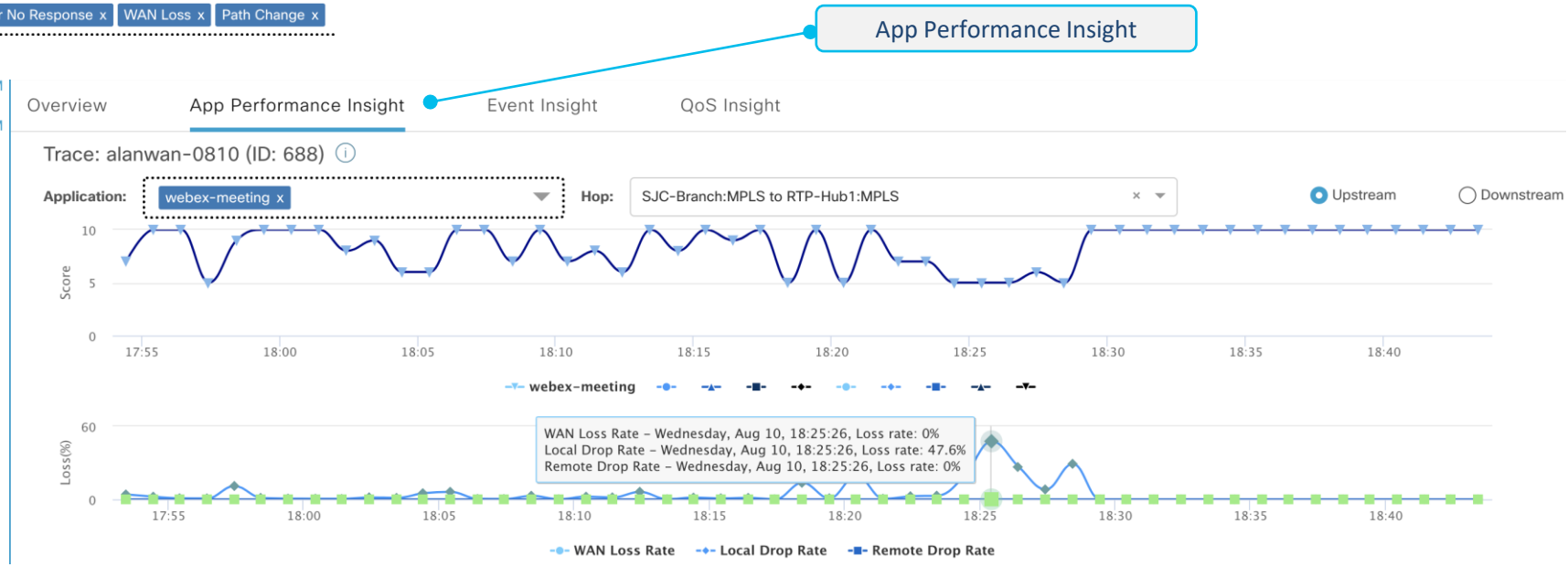
Upstream Applications Path & Performance (packet)

App Centric Topology & Paths
- Discovered by interested traffic



Insight Summary - App Performance Insight

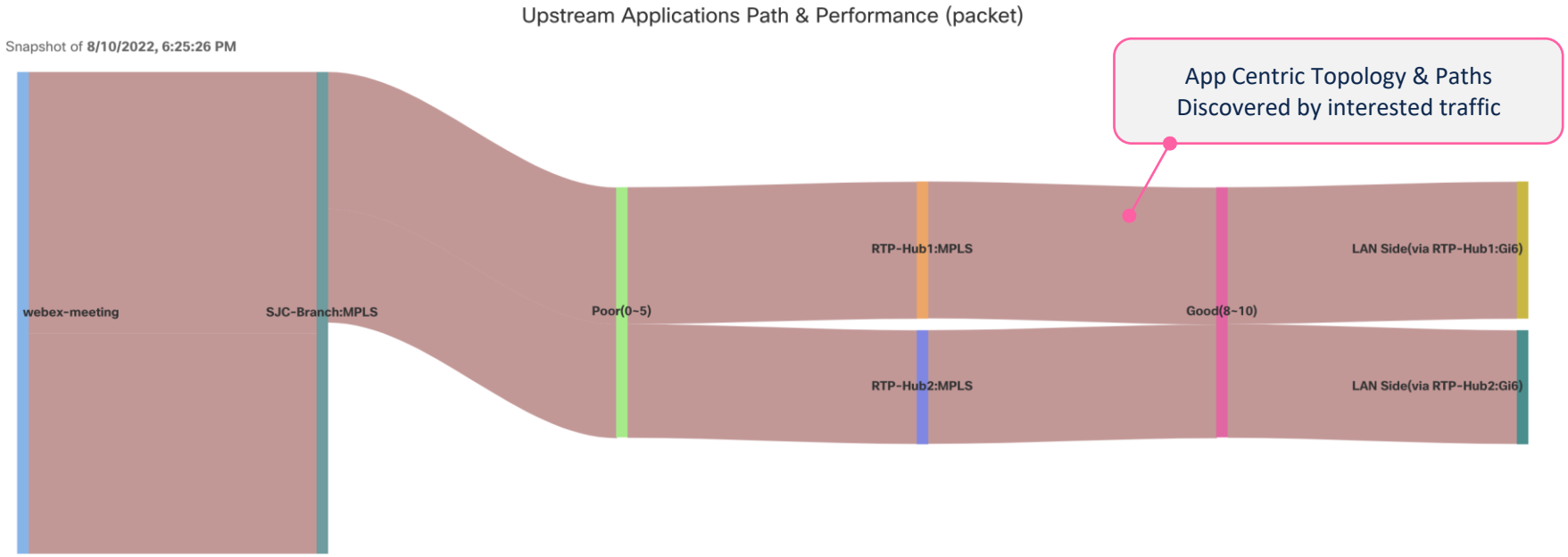




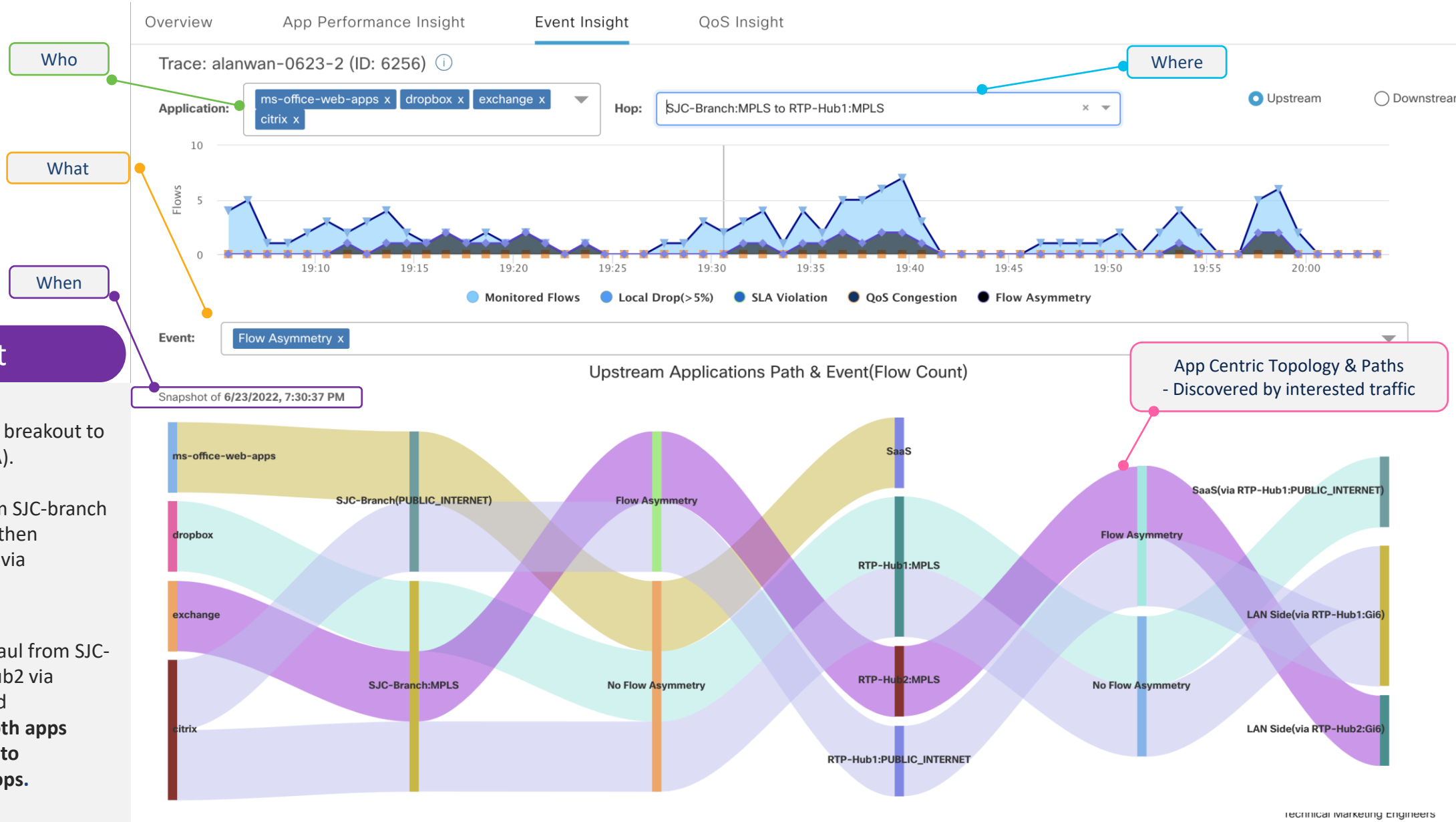
Readout

Webex-meeting: Load balance from SJC-branch to RTP-Hub1/Hub2 via MPLS, then toward Campus/DC via LAN.

Poor performance on the hops:
SJC-branch to RTP-Hub1/2 as QoS congestion caused local drop on SJC-branch's MPLS link.



Insight Summary - Event Insight



Readout

Office: SJC-Branch local breakout to SaaS Cloud via INET(DIA).

Dropbox: Backhaul from SJC-branch to RTP-Hub1 via MPLS, then breakout to SaaS Cloud via INET(DIA).

Exchange/Citrix: Backhaul from SJC-branch to RTP-Hub1/Hub2 via MPLS/INET, then toward Campus/DC via LAN. **Both apps have some flows run into asymmetry on some hops.**

Insight Summary - QoS Insight

Queue	Application	Bandwith
Queue0	Voice, Video	15%
Queue1	Webex	20%
Queue2(Default)	HTTP, SSL ,Adobe-service etc.	20%
Queue3	SaaS(Box/Dropbox/Google/Office365/Amazon etc.) SMTP, POP3 ,Citrix, Exchange	45%

Tips

QoS Insight – Use case 1

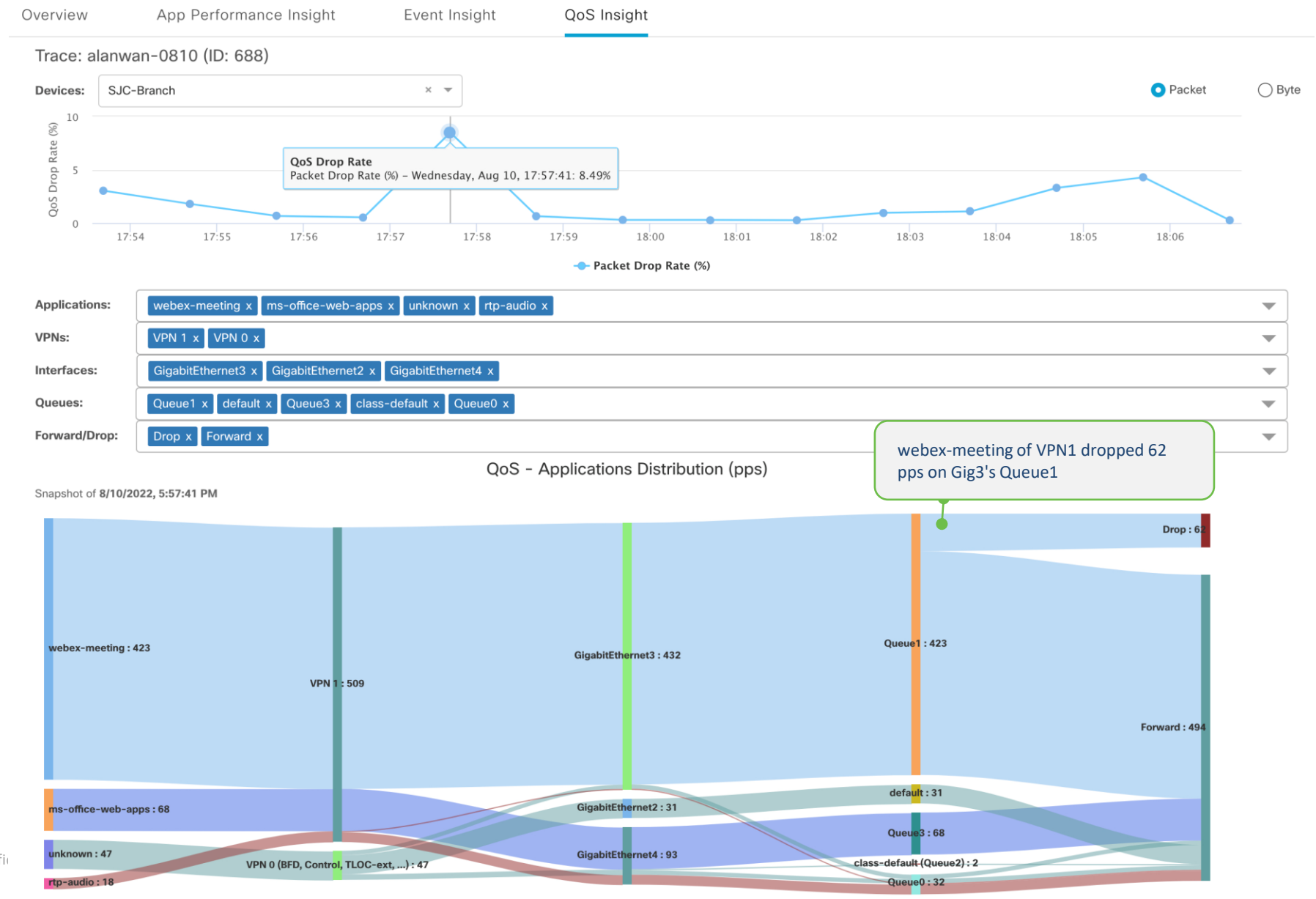
CIO's Webex meeting run into bad quality. Finally, root cause was:

More attendees joined the Webex meeting from same site and run out of planned bandwidth.

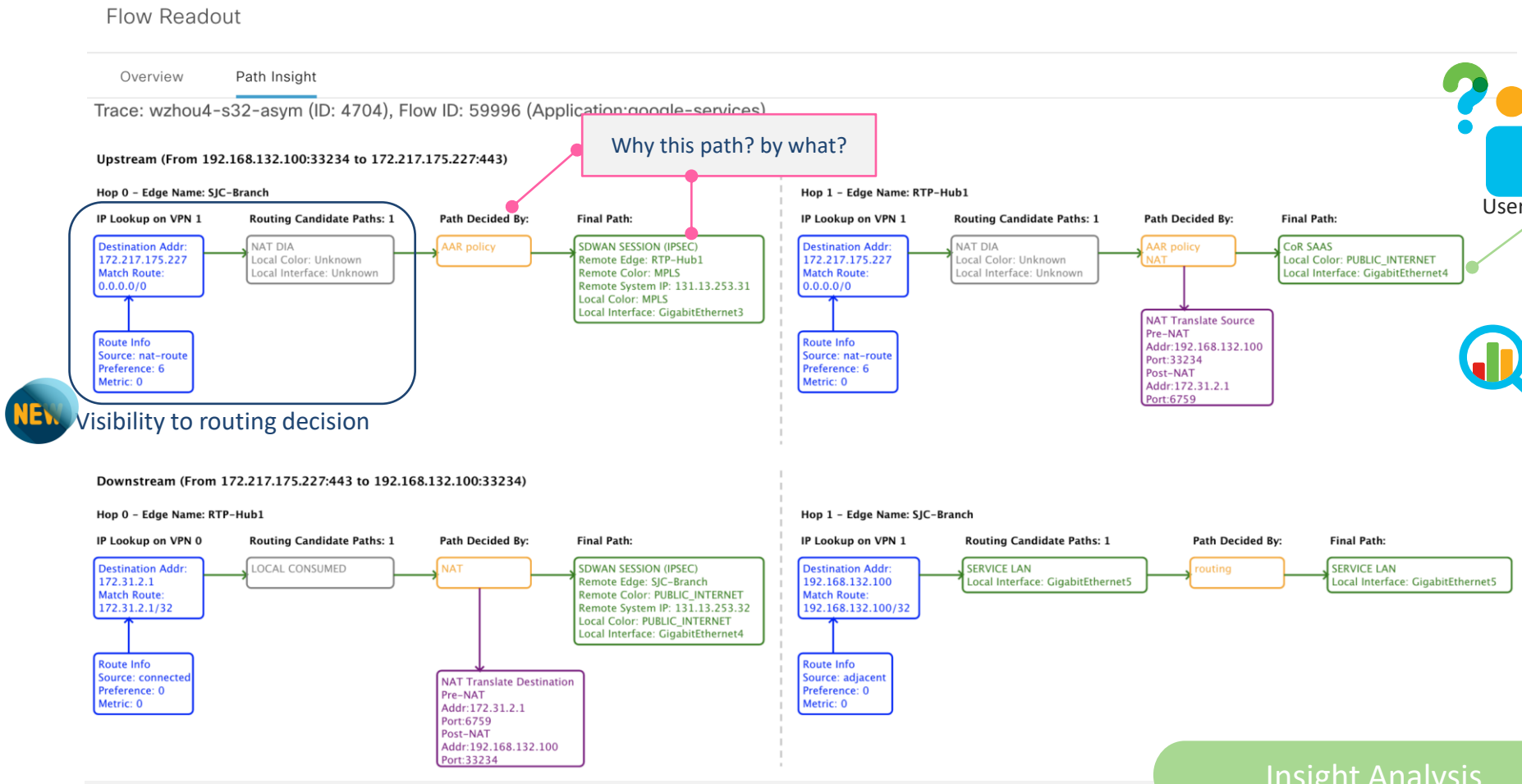
"QoS insight", for QoS congestion debug or bandwidth capacity planning.

Remediation Actions:

1. Allocate more bandwidth for Webex/Queue1
2. Buy more bandwidth for circuit Gig3.
3. Allocate other apps to different queue if competing bandwidth is in same queue
4. Revisit traffic steering policy, for example not to prefer MPLS, load-balance to other WAN circuits.



Path Insight at Flow Level



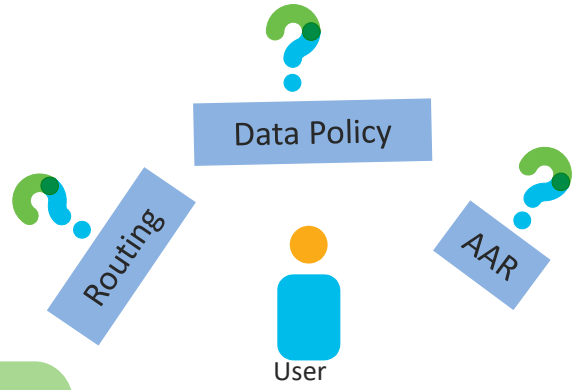
NEW Visibility to routing decision

Insight Level 1- What

Office 365 takes Internet path

User

Insight Level 2- Why

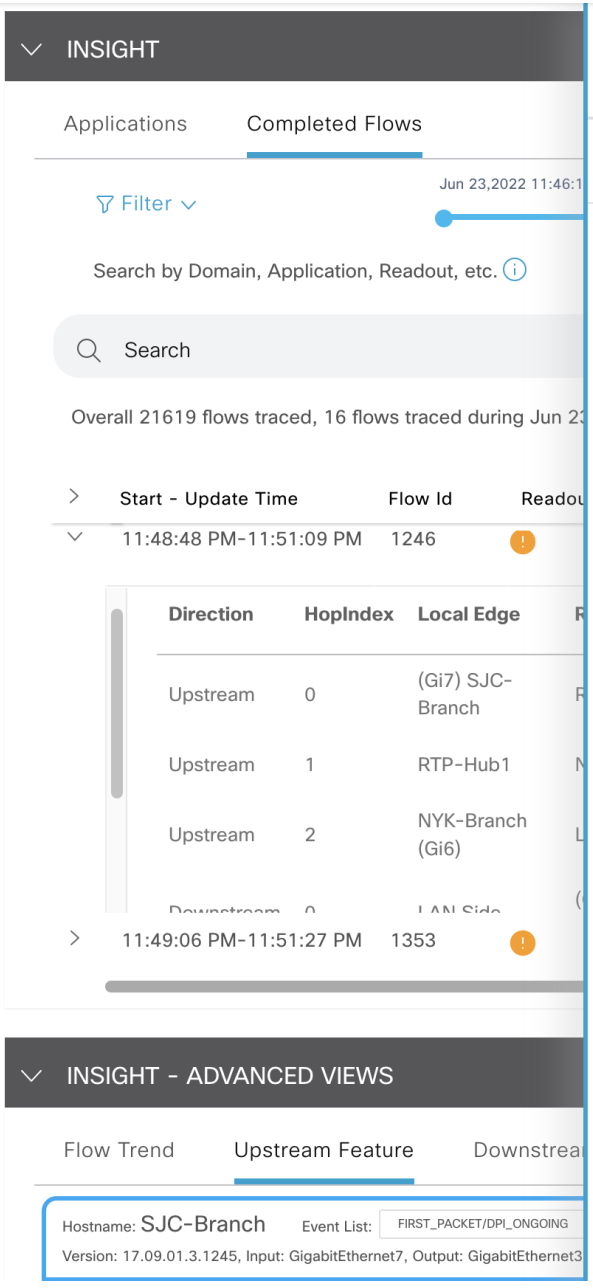


Insight Analysis

Google services application took the path decided by CoR-SaaS from SJC-Banch to RTP hub, then to Internet.

Technical Marketing Engineers

Flow level readout - Overview



Flow Readout

Overview | Path Insight

Trace: alanwan-0623-3 (ID: 6304), Flow ID: 1246 (Application:sip)
Upstream From 49.16.0.255:6094 to 17.16.0.255:5060
Downstream From 17.16.0.255:5060 to 49.16.0.255:6094

Overall Status

SLA Violation From BFD Measurement: Yes
* Upstream hop((Gi7) SJC-Branch:MPLS -> RTP-Hub1:MPLS)
request SLA Voice-And-Video defined in policy AAP_COLOR_3G-yicliu-cxp can not meet.
BFD measurement:
please check Dashboard-> Main Dashboard-> Application-Aware Routing for detail.

* Upstream hop(RTP-Hub1:MPLS -> NYK-Branch:MPLS)
request SLA Voice-And-Video defined in policy AAP_COLOR_3G-yicliu-cxp can not meet.
BFD measurement:
please check Dashboard-> Main Dashboard-> Application-Aware Routing for detail.

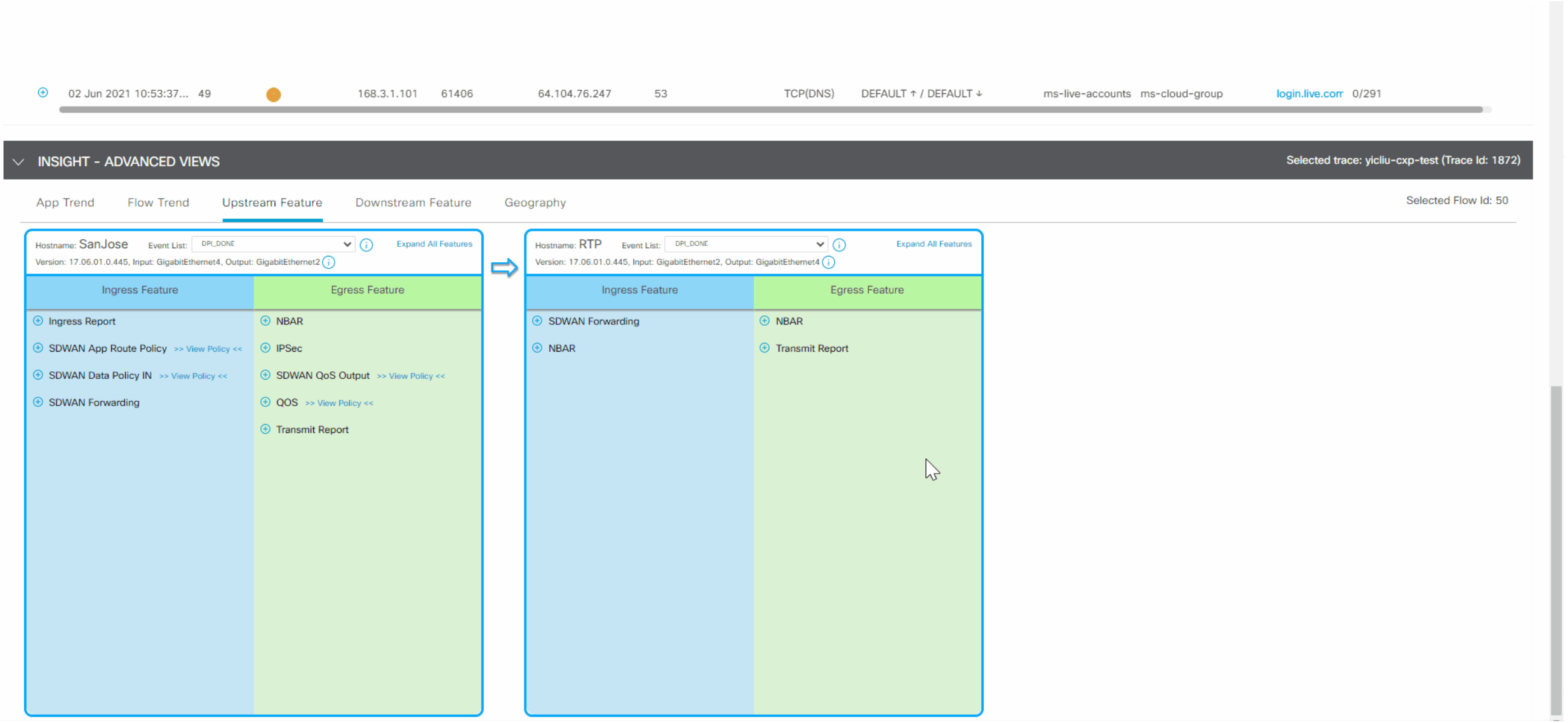
* Downstream hop(RTP-Hub2:MPLS -> SJC-Branch(Gi7) :MPLS)
request SLA Voice-And-Video defined in policy AAP_COLOR_3G-yicliu-cxp can not meet.
BFD measurement:
please check Dashboard-> Main Dashboard-> Application-Aware Routing for detail.

==========

Flow Asymmetry: Possible (Reverse flow traffic not detected, UDP flow's asymmetry can not be determined)
Upstream: (Gi7) SJC-Branch:MPLS --> RTP-Hub1:MPLS
Upstream: RTP-Hub1:MPLS --> NYK-Branch:MPLS
Upstream: NYK-Branch (Gi6):Service LAN --> LAN Side:N/A
Downstream: LAN Side:N/A --> (Gi6)NYK-Branch:Service LAN
Downstream: NYK-Branch:MPLS --> RTP-Hub2:MPLS
Downstream: RTP-Hub2:MPLS --> SJC-Branch(Gi7) :MPLS

Technical Marketing Engineers

ADVANCED VIEWS – Up/Downstream Feature

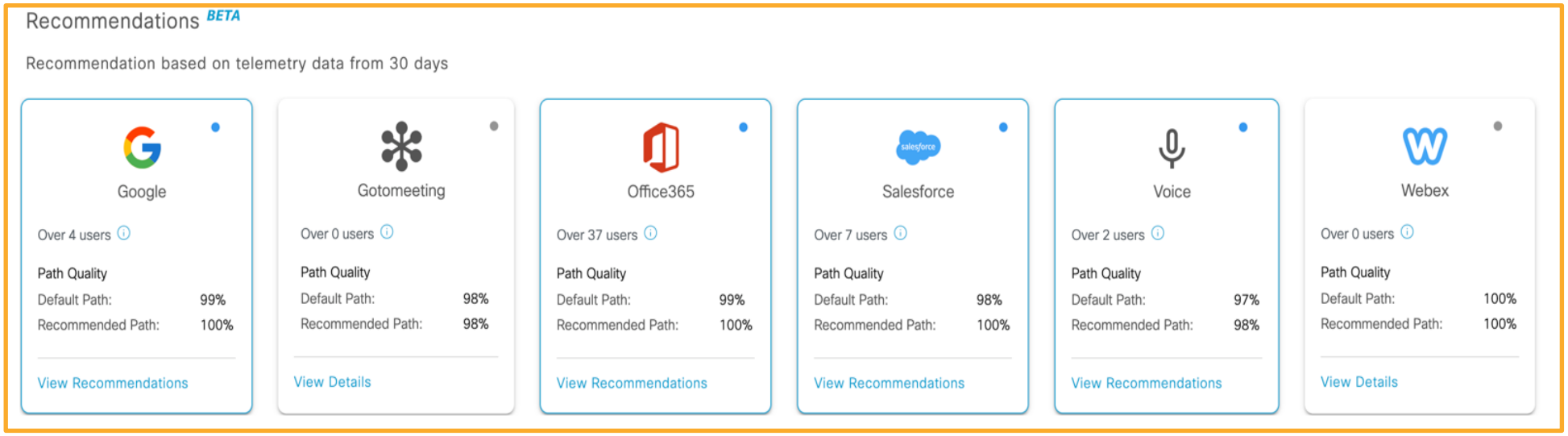


Proactive Path Recommendations to improve App Experience

Powered by ThousandEyes WAN Insights

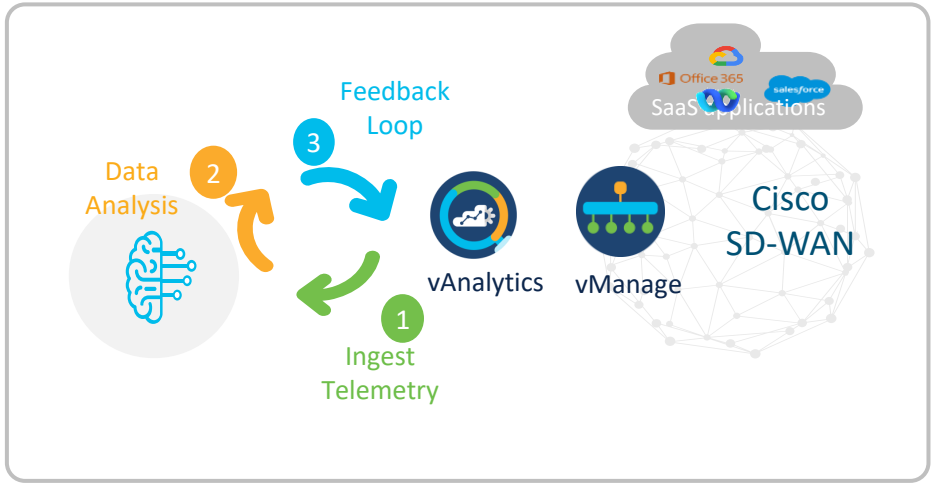
New!

Forecast path performance issues and make recommendations –
Transforming SD-WAN operations from a reactive to a predictive model



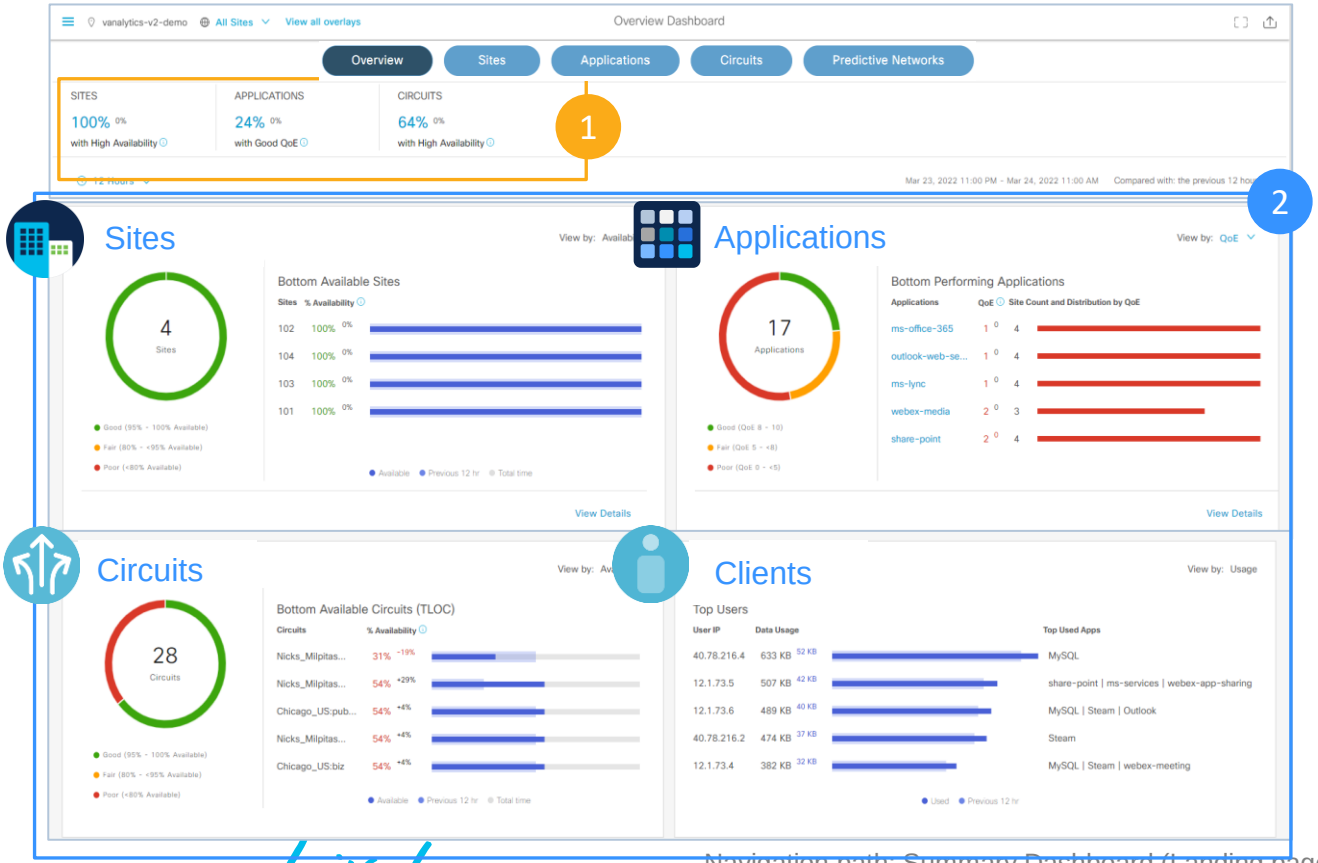
1. Ingest Telemetry: Collect network telemetry data through vAnalytics
2. Data Analysis: Apply predictive models to forecast issues & make path recommendations
3. Feedback Loop: Fine-tune SD-WAN policies (initially manual, automated in future) to implement path recommendation and improve App experience

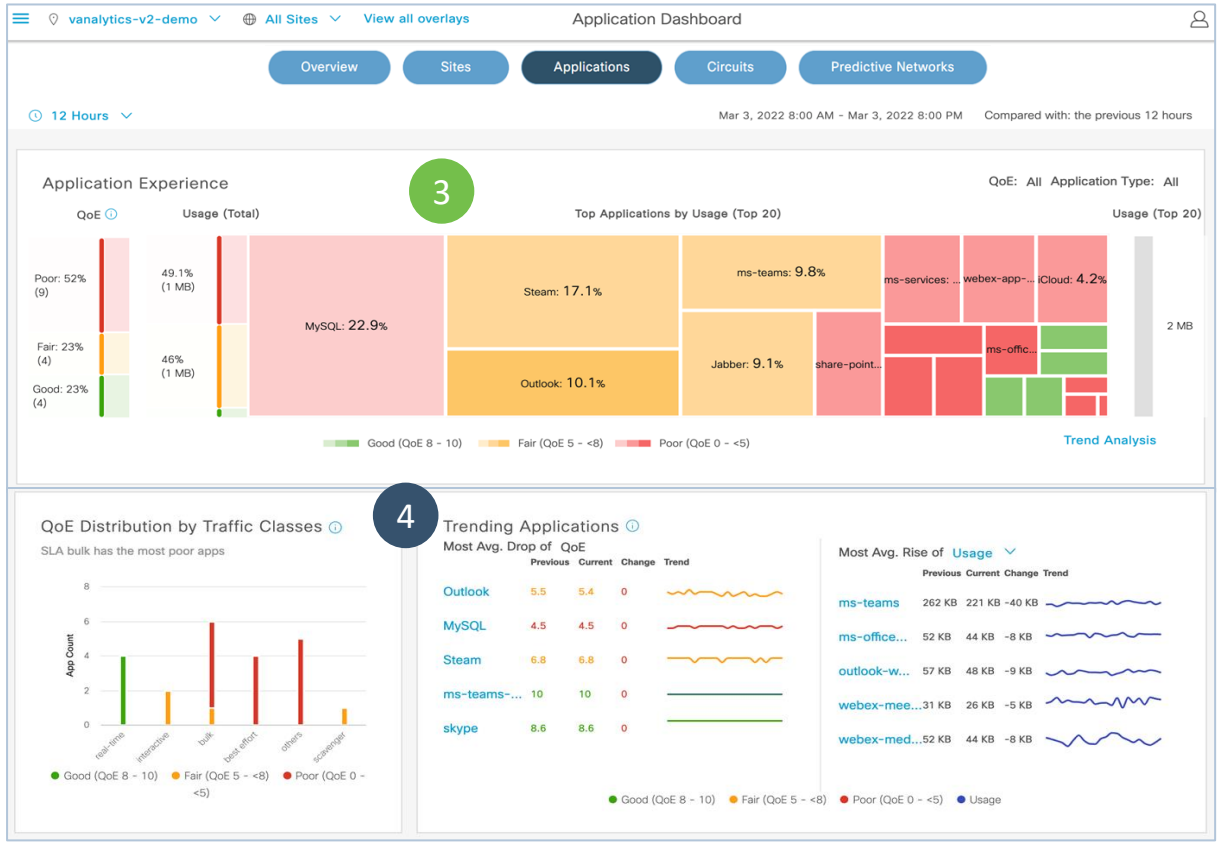
- Included with SD-WAN DNA Advantage & above license; ThousandEyes Agent not necessary
- Limited availability for private preview customers (w/ vAnalytics deployment in Americas region)



Operational Insights of your network and applications

1. Snapshot of the overall network and application health
2. Summary widgets for 4 key elements – Sites, Apps, Circuits, & Clients
3. Application health (QoE) and magnitude of its impact
4. Trending Apps – by usage, health, loss



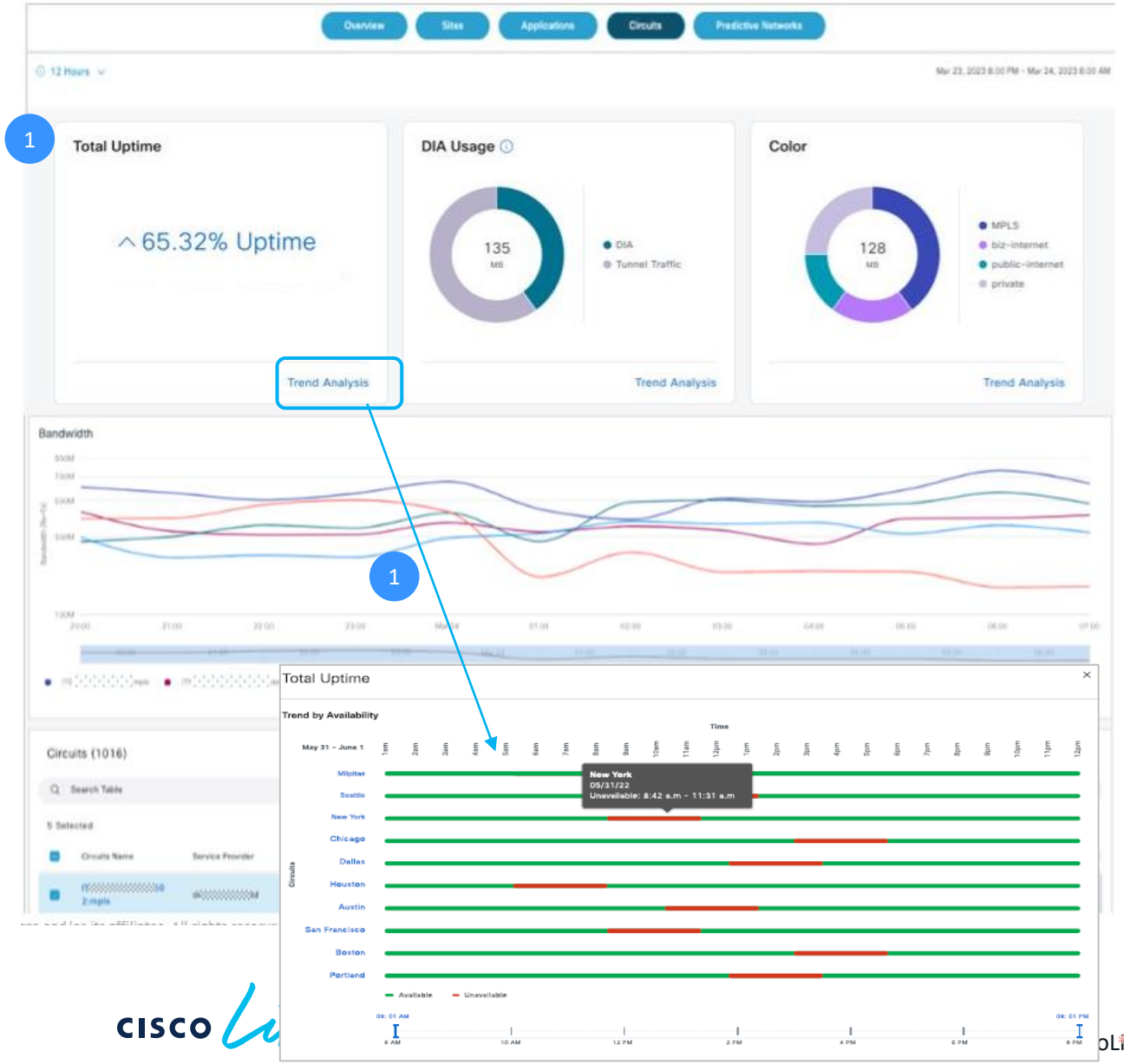


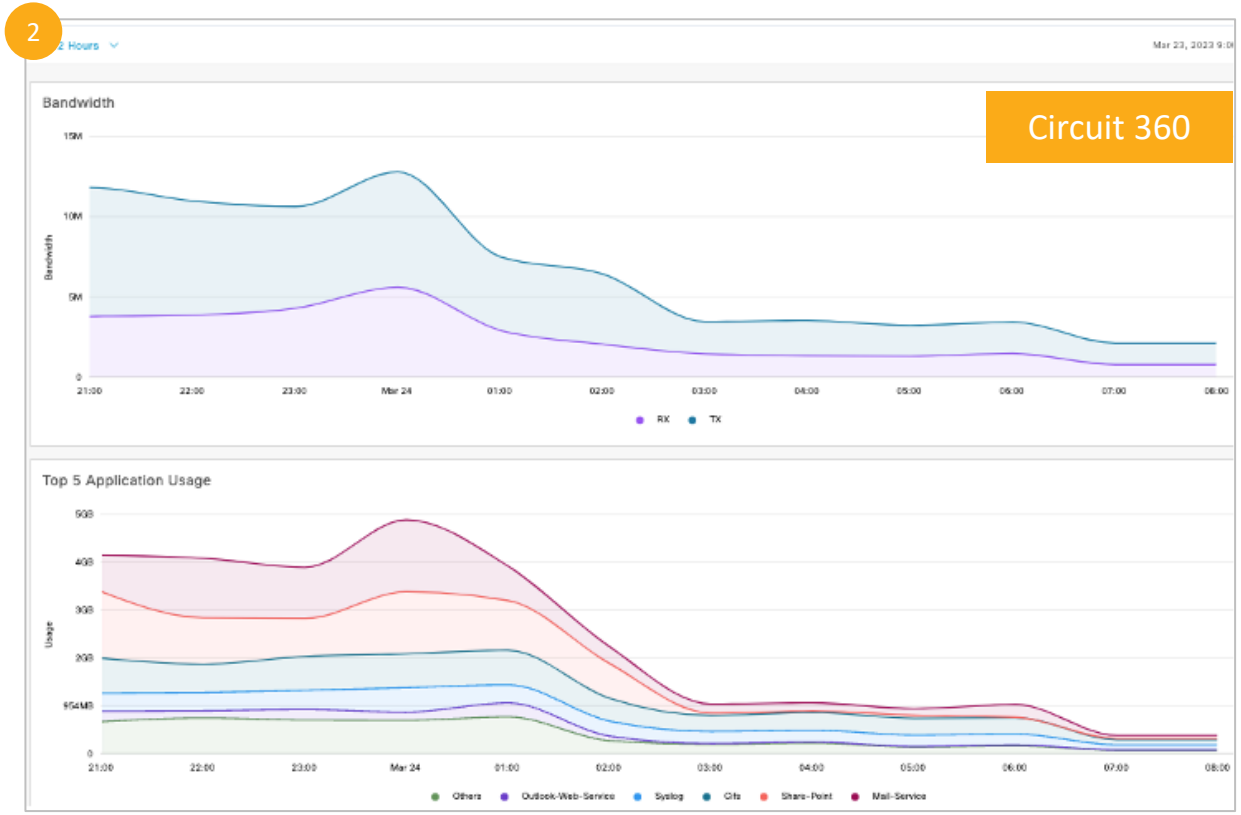
Navigation path: Summary Dashboard (Landing page)

Navigation path: Summary Dashboard -> Applications

Circuit Dashboard

New!





1 **Comprehensive visibility into WAN circuits**
- Circuit uptime and availability trends
- Traffic distribution - DIA vs Tunnel and by Color

2 **Top used circuits and usage trends (Circuit360 page)**
- RX and TX bandwidth rate
- Top Applications & Top Flows

Monitor - Overview Cisco SDW

Not Secure | https://tme-demo-vmanage.cisco.com/#/app/monitor2/overview

Cisco SD-WAN | Select Resource Group | All Sites | Monitor · Overview

Overview | Devices | Tunnels | Applications | Security | VPN | Logs | Multicloud

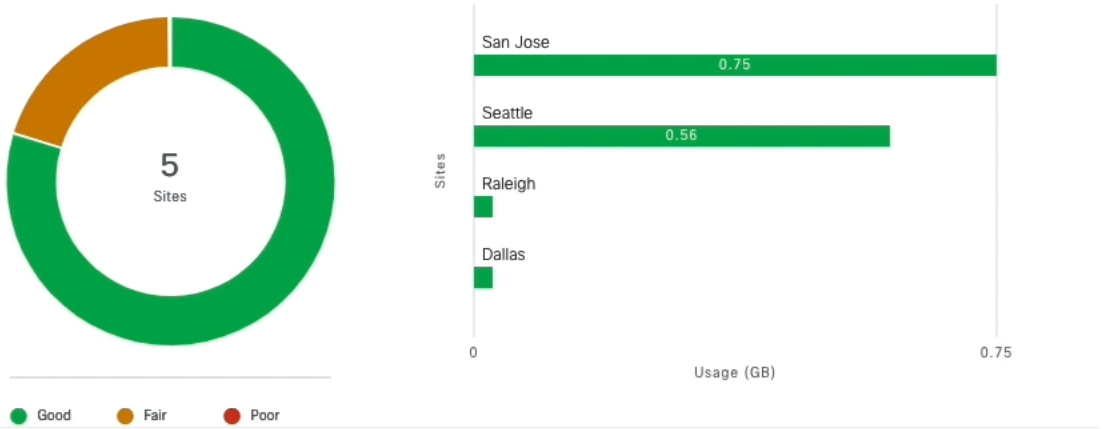
Overview

CONTROLLERS			WAN Edges	CERTIFICATE STATUS	LICENSING	REBOOT
1	1	1	5	0	0	0
vBond	vSmart	vManage	Reachable	Warning	Assigned	Last 24 hrs
					5 Unassigned	

24 Hours | Actions

Site Health

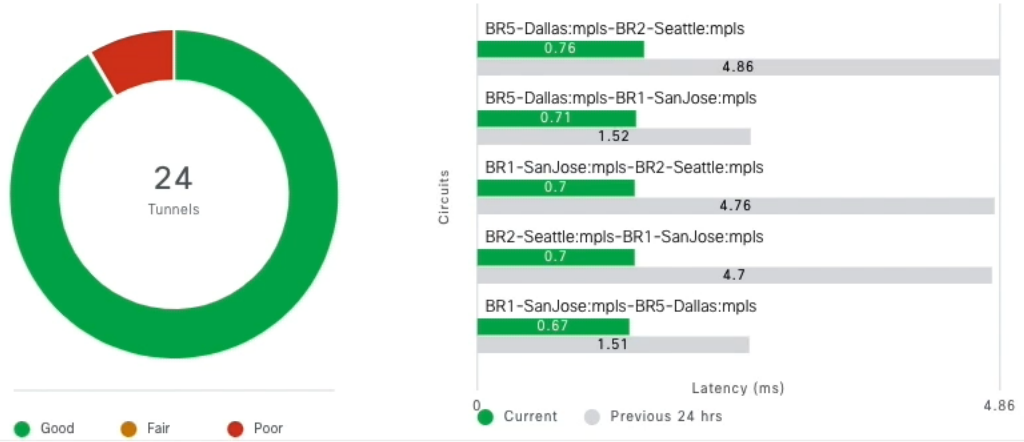
Good Performing Sites



View Details

Tunnel Health

Latency (ms) | Good Tunnels



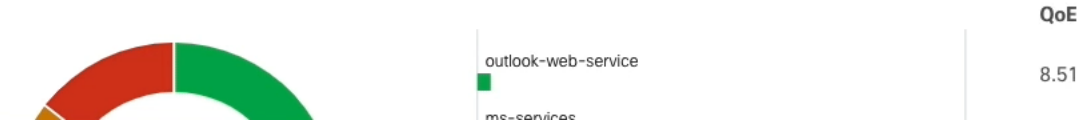
View Details

WAN Edge Health

CPU Load (%) | Fair Devices

Application Health

Good Performing Applications

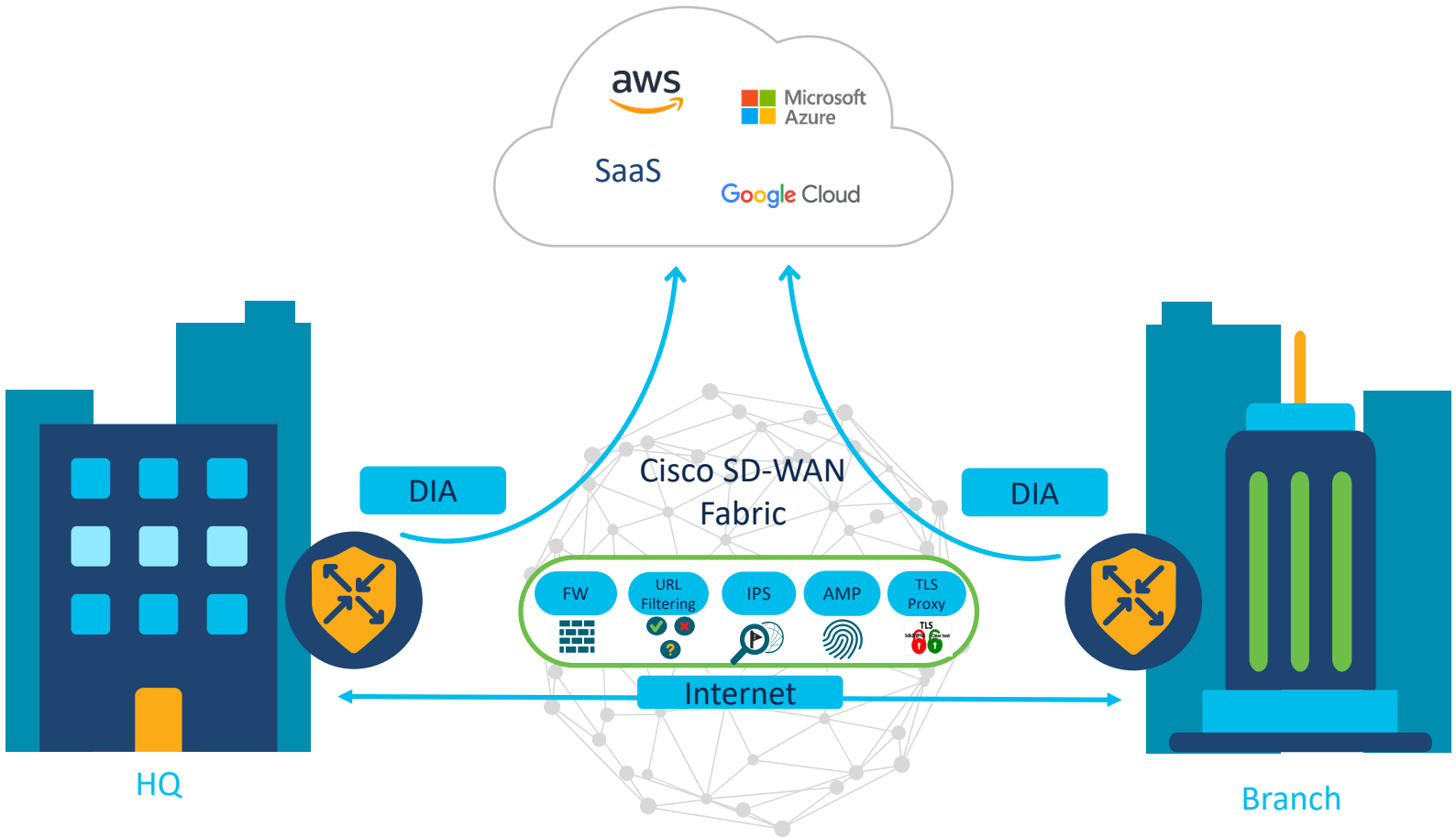


Observability – optymalizacja i widoczność

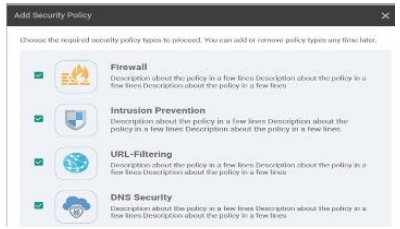
ThousandEyes - Cloud Intelligence

Wydajność aplikacji	Wizualizacja trasy	Status Internetu i WANu	Monitoring BGP	Zdalny pracownik
✓	✓	✓	✓	✓
Izolacja problemów aplikacji od problemów sieciowych	Zweryfikuj czy to problem w sieci, operatora czy aplikacji chmurowej	Internet to nowy WAN– monitoruj jego parametry	Upewnij się, że routing nie powoduje problemów z aplikacją	Aplikacje muszą być dostępne niezależnie od lokalizacji użytkownika

Dzięki Cisco SD-WAN NGFW w każdym oddziale



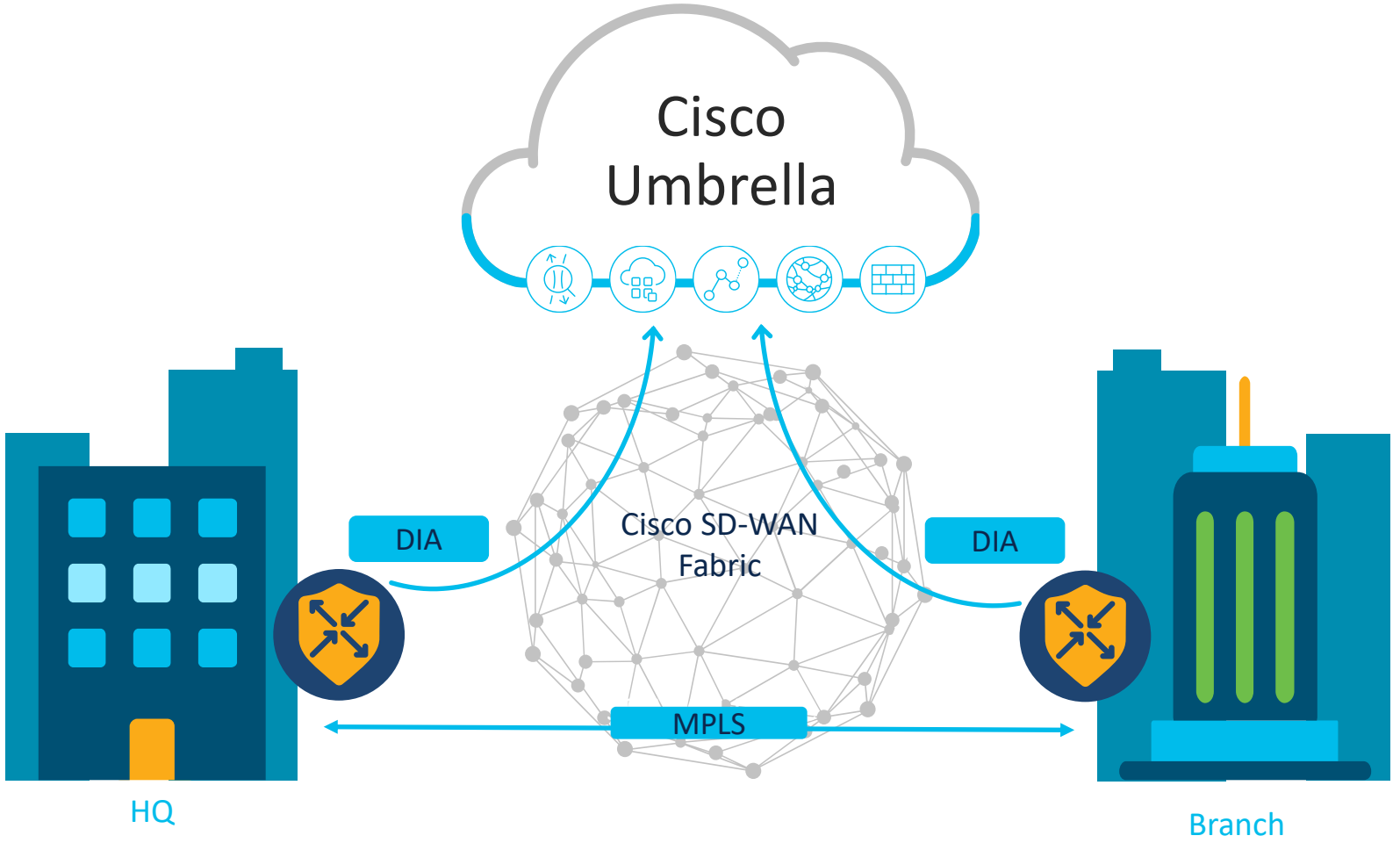
vManage Automated Templates



- Enterprise Firewall
- Intrusion Prevention System
- URL-Filtering
- Advance Malware Protection
- DNS Security
- TLS/SSL Proxy

SD-WAN Cloud Security

Auto Tunnel, Intelligent Traffic Steering



Use-Case

Unified policy for Mobile work force
Branch to Internet
Branch to Cloud(SaaS)

vManage
Auto-Templates

DNS-Layer Security

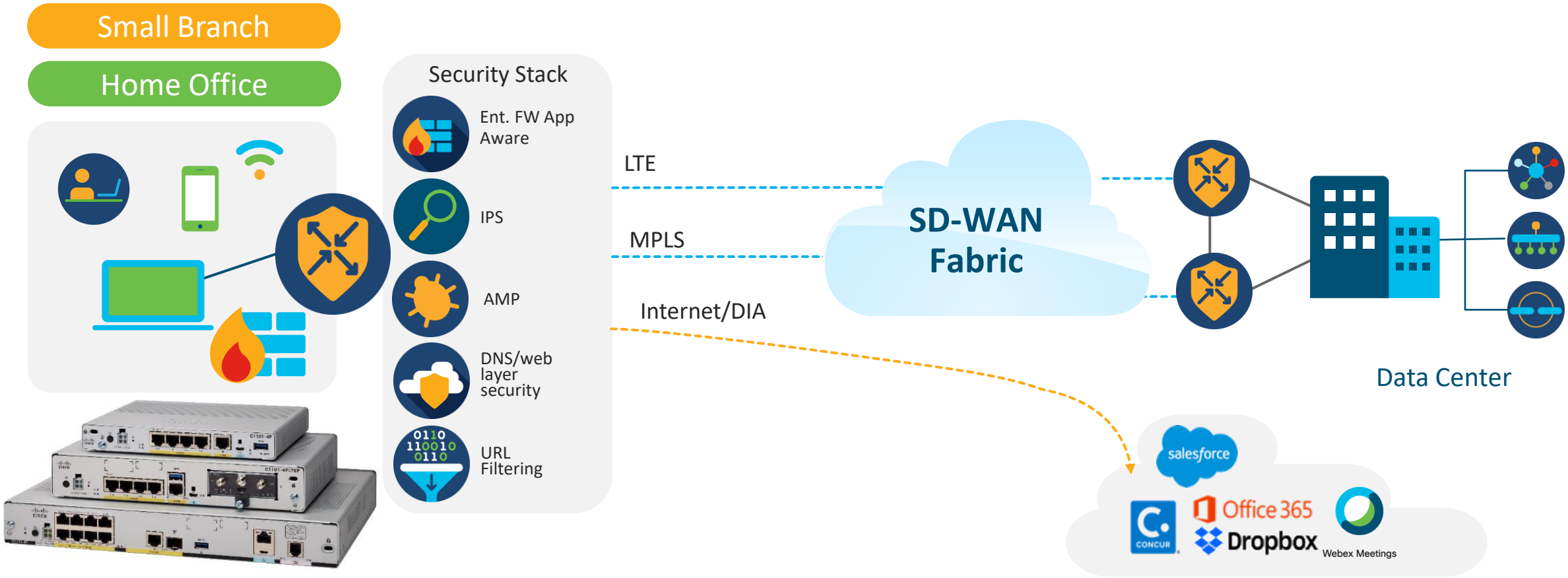
Secure Web Gateway

Cloud-Delivered Firewall

Cloud Access Security Broker

Interactive Threat Intel

Model nowoczesnego oddziału



WiFi6, Next-gen 5G LTE, Integrated Security, Visibility & Analytics, Cloud OnRamp for SaaS, One Box Solution

SASE

Cisco Umbrella

Bezpieczeństwo DNS	Secure Web Gateway	Cloud-delivered Layer 7 firewall	Cloud access security broker (CASB) Inc. DLP	Wiedza o zagrożeniach
✓	✓	✓	✓	✓
Zatrzymaj zagrożenia zanim dotrą do Twojej sieci	Pełna widoczność i kontrola komunikacji WWW Kontrola tenantów	Blokowanie zagrożeń do warstwy 7	Widoczność, raportowanie i kontrola wykorzystania aplikacji chmurowych	Konkteksowa wiedza o zagrożeniach oraz dane dla zespołów analitycznych

XDR

Zintegrowana platforma Cyberbezpieczeństwa

Widoczność i automatyzacja wszystkich rozwiązań cyberbezpieczeństwa

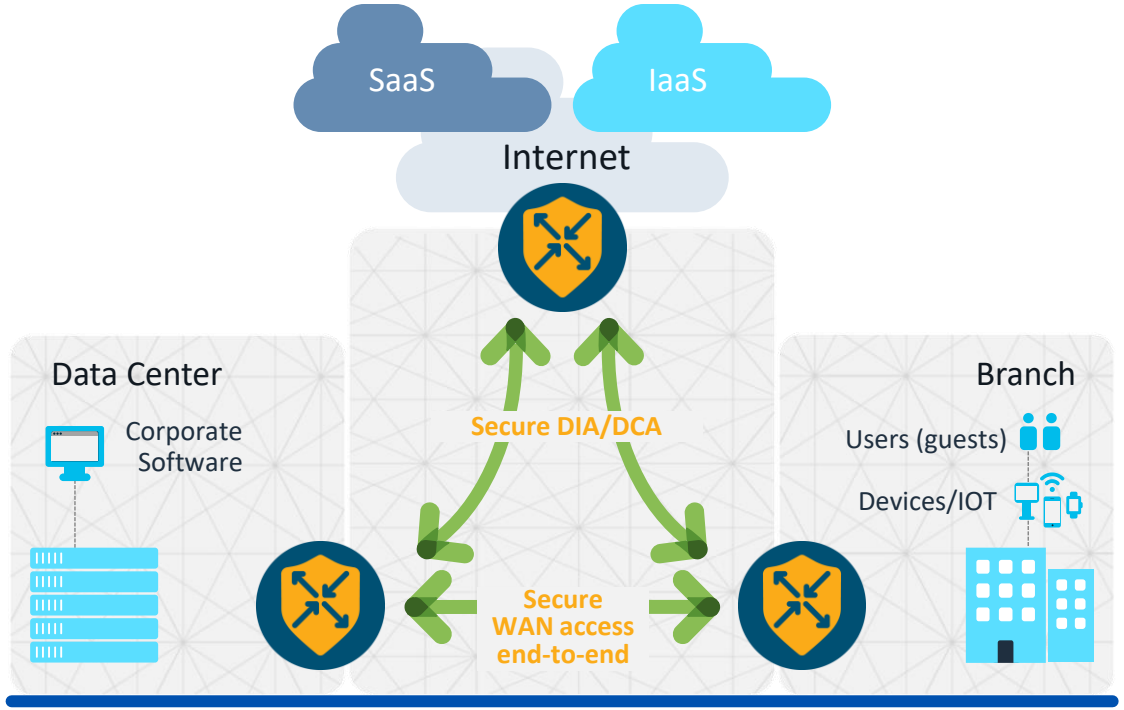
SASE zero trust

Bezpieczny dostęp z DUO

MFA	Sprawdzanie stanu stacji koncowej	Least privileged access	Ciągła weryfikacja	Analiza zachowania
✓	✓	✓	✓	✓
Weryfikacja tożsamości użytkownika	Weryfikacja i wymuszenie	Fundament bezpieczeństwa	Każda próba dostępu jest weryfikana w sposób ciągły	Wykrycie i raportowanie anomalii i nieporządanych zachowań

Dla każdego użytkownika, urządzenia, aplikacji

Benefity z posiadania security everywhere



Cisco catalyst SD-WAN

	Plusy	Minusy
ONLY Cloud Security	Spójna ochrona użytkowników i urządzeń we wszystkich lokalizacjach i skalowanie na żądanie	Brak widoczności i kontroli nad ruchem wewnętrznym i zagrożeniami
ONLY On-Prem Security	Widoczność całego ruchu i ochrona przed zagrożeniami wewnętrznymi i zewnętrznymi	Deszyfrowanie zwiększa obciążenie urządzeń brzegowych
On-Prem and Cloud Security	Najlepsza równowaga między bezpieczeństwem i komfortem użytkowania w przypadku bezpośredniego dostępu do Internetu	Zintegrowane rozwiązanie Cisco eliminuje te wady

You make networking **possible**

Backup slides

You make networking **possible**

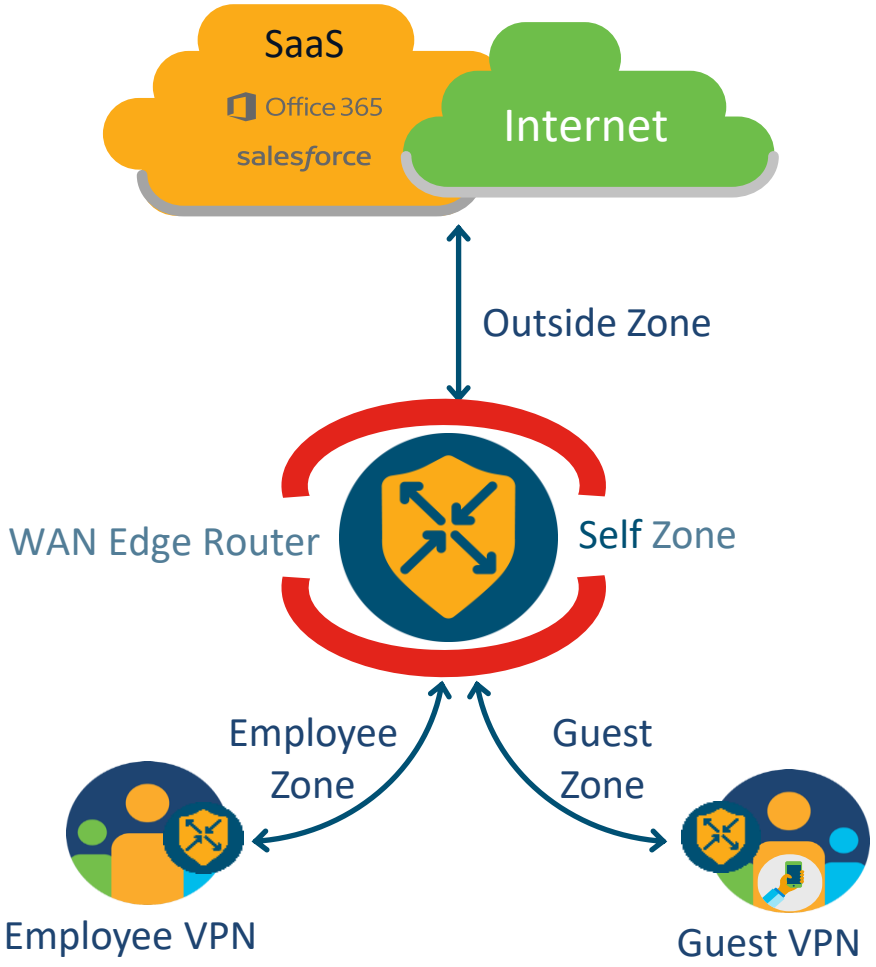
Cisco Enterprise Firewall with Application Aware Policy

Use case

Jako administrator bezpieczeństwa chcę mieć architekturę bezpieczeństwa, która chroni sieci przed coraz bardziej wyrafinowanymi zagrożeniami i zapewnia widoczność end-to-end oraz pojedyncze zarządzanie bezpieczeństwem i egzekwowanie polityki sieciowej.

Features

- Cisco SD-WAN oferuje Enterprise Firewall warstwy 7 aplikacji aby zapewnić stałą ochronę przed wewnętrznymi i zewnętrznymi zagrożeniami z różnych źródeł
- Granularne polityki i kontrola nad aplikacjami
- Scentralizowana widoczność i kontrola całego ruchu wewnętrznego, przychodzącego i wychodzącego
- Single pane of glass - scentralizowana konfiguracja i administracja dla sieci i bezpieczeństwa



Enterprise Firewall

Kluczowe możliwości

Zone Based Firewall

- Stanowy, oparta na strefach inspekcja
- VPNy/VRFy powiązane do stref
- Obsługuje inspekcje ruchu między tymi samymi strefami jak i różnymi
- Self-Zone ochrona routera przed wewnętrznymi atakami

Layer 7 App Visibility

- Blokowanie ruchu w oparciu o aplikacje lub rodziny aplikacji
- Widoczność aplikacji i granularna kontrola
- Wykorzystanie integracji NBAR/SD-AVC do dopasowania ruchu aplikacji

HSL Logging

- Logi firewalla mogą być wysyłane do zewnętrznego kolektora
- Obsługa High-Speed logging (HSL) użycie NetFlow jako formatu eksportu

Enterprise Firewall

Kluczowe możliwości

FQDN Support

- Proste reguły firewall oparte na nazwach domen
- Redukcja reguł tworzonych na podstawie adresów IP
- Ułatwienie monitoringu

Multiple Prefix Lists/Rule Set Support

- Obsługa obiektów tworzonych z prefiksów/portów/protokołów (source/destination)

Geo Location Support

- Filtracja wybranych lokalizacji geograficznych
- Informacje geograficzne obejmują listę krajów i/lub kontynentów
- Dane IP Geo z Digital Element

Geo Location Based Firewall Policy

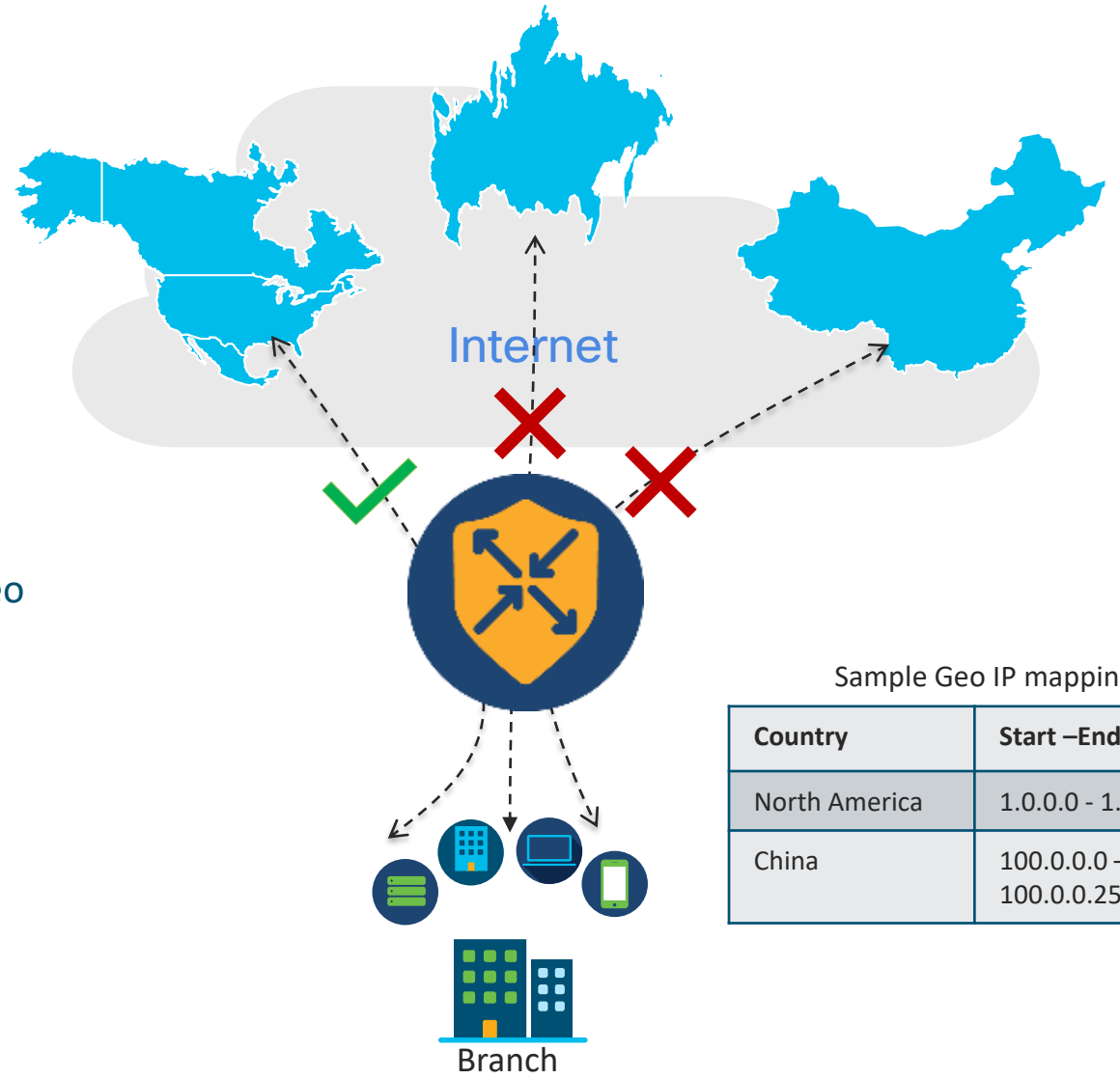
Use case

As a security admin in banking sector, I wants to allow traffic only from our office locations (North America) and block connections to or from other geographical location (China & Russia)

Features

Use ZBFW policy with Geo filtering feature to block certain geo location and allow traffic from desired location

Configure Geo location as source/destination prefix lists and geo location database includes list of countries and/or continents



Sample Geo IP mapping

Country	Start –End IP Address
North America	1.0.0.0 - 1.0.0.0.255
China	100.0.0.0 – 100.0.0.255

Identity based Firewall (using ISE-AD) integrations

vEdge ✗

cEdge ✓

Problem

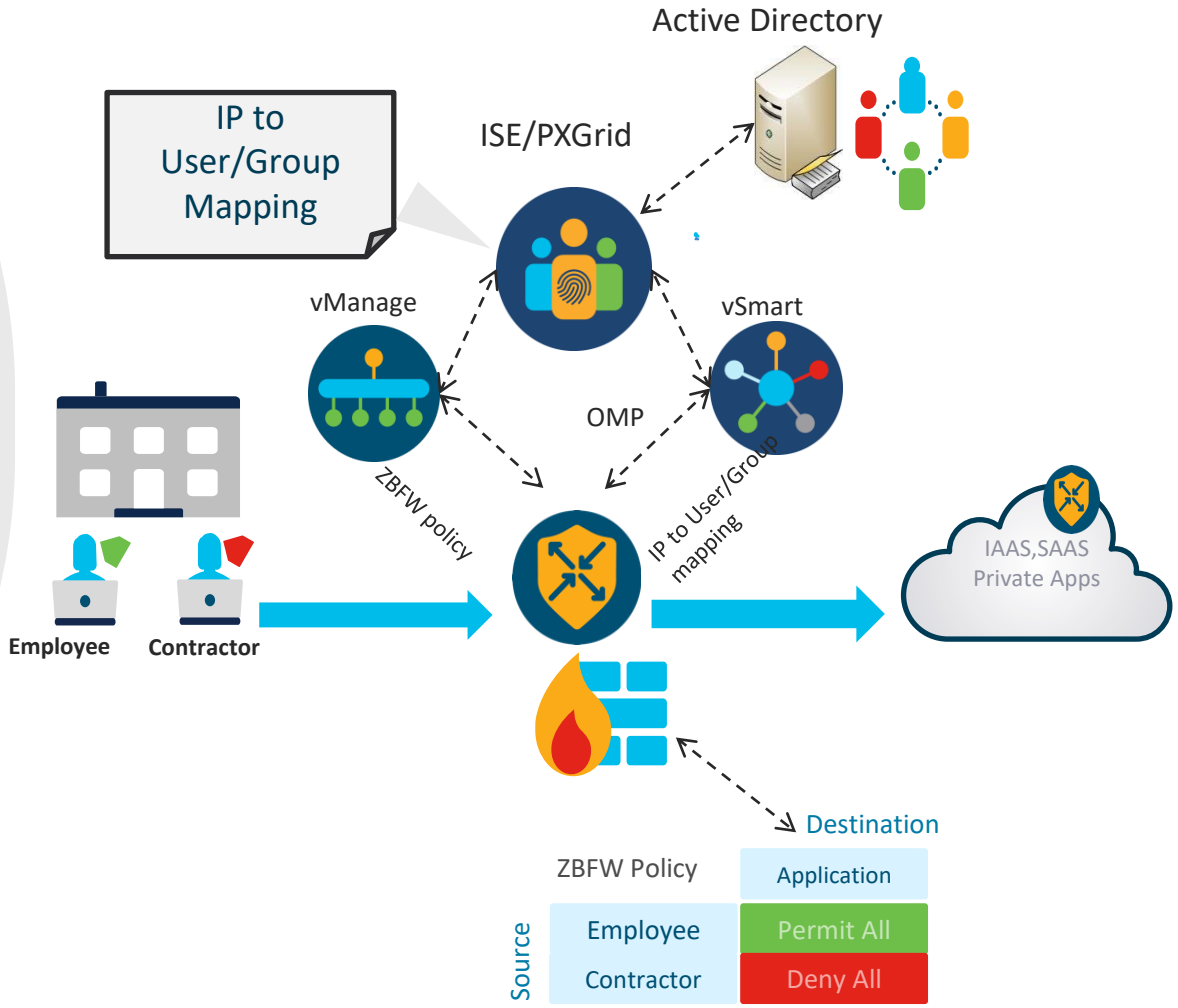
Security policies that align to users and groups rather than to IP addresses give organizations easier, more precise control over who can access the network/applications—and what they can access.
In a hybrid workforce environment, the users can access application from anywhere and from any IP, therefore applying security policy based on prefixes is not enough.
Typically, a SD-WAN embedded security stack is not aware of the users' identities and, therefore, cannot apply security policies based on identities.

Solution

20.9/17.9 introduces capability to match user identity and apply zone-based firewall policy based on identities. vManage and vSmart controllers in this case integrates with ISE/PXGRID which is further integrated with Active Directory. The interested domain is then subscribed to be learned in SD-WAN controllers and thus ip-user and ip-user-group mapping is learned though OMP which is then used for ZBFW policies dynamically

Caveats

Only one ISE instance allowed
Only one domain allowed
Only one identity list per rule
No destination-based identity matching in FW rule
With ISE v3.1 system only allows user-group based configs, ISE-3.2 recommended
No SGT mapping (roadmap)



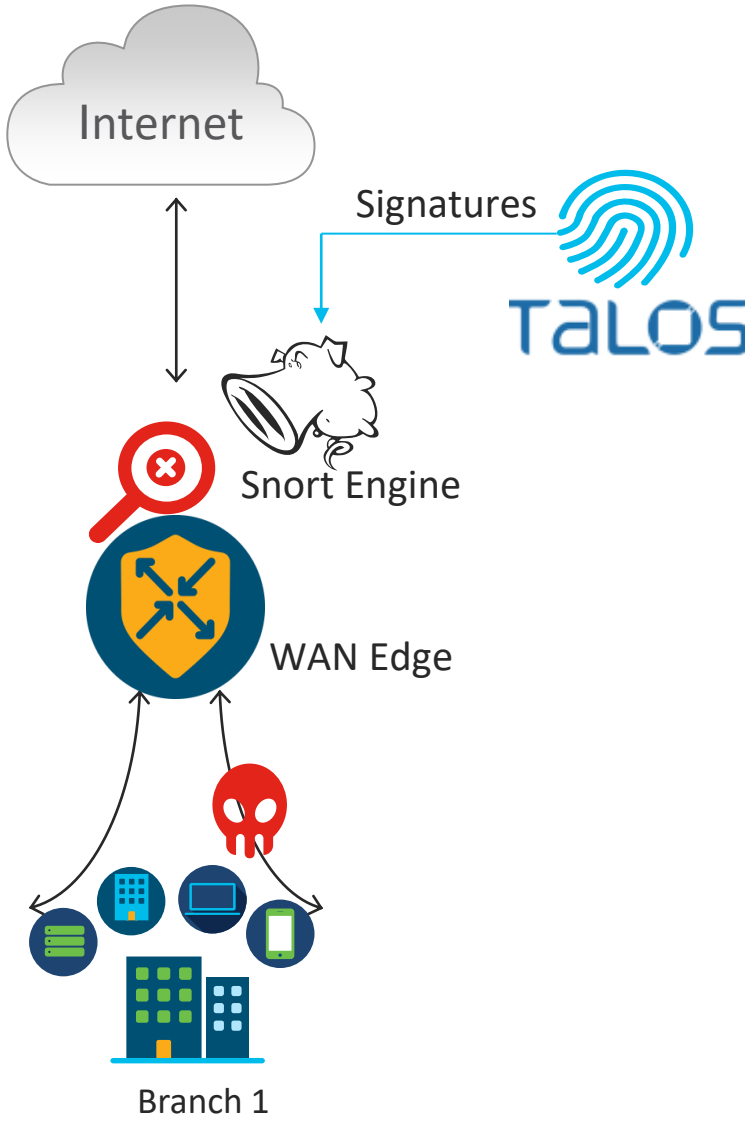
Intrusion Prevention/Detection System (IPS/IDS)

Use case

Jako administrator bezpieczeństwa, chcę blokować znane zagrożenia w całej sieci i poddawać inspekcji ruch internetowy do wykrywania i reagowania na ataki. Łatać luki w krótszym czasie i przy użyciu mniejszych zasobów.

Feature

- Snort IPS jest najczęściej wdrażanym IPSem na świecie
- Cisco TALOS – zespół bezpieczeństwa Cisco – przygotowuje dedykowane sygnatury
- Snort automatycznie aktualizuje sygnatury
- Wsparcie dla whitelisty sygnatur
- Analiza ruchu w czasie rzeczywistym



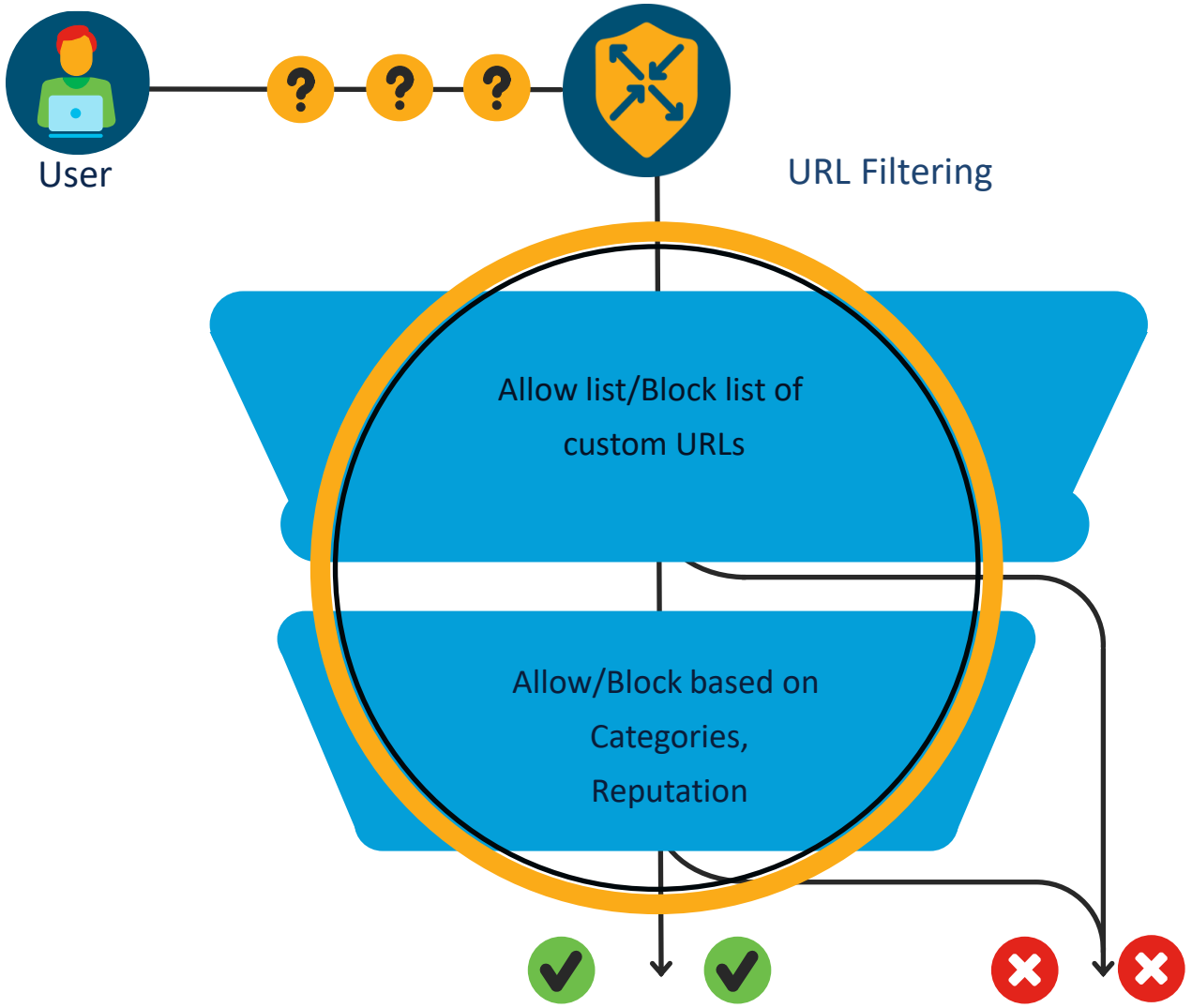
URL-Filtering (URL-F)

Use case

Jako administrator ds. bezpieczeństwa chcę ściślejszej kontroli bezpieczeństwa. Chcę uniemożliwić użytkownikom dostęp do stron, które mogą zakłócić funkcjonowanie firmy - takich jak strony niezwiązane z pracą, strony zawierające treści obraźliwe, nielegalne, strony związane z próbami wyłudzenia informacji, lub strony po prostu niebezpieczne

Feature

- URL-Filtering umożliwia zarządzanie dostępem do stron poprzez blokowanie lub zezwalanie w oparciu o kategorie stron lub jej reputacji
  - Allow List/Block List
  - Kategorie
  - Reputacje
- 82+ kategorii stron z dynamicznymi aktualizacjami



Advanced Malware Protection (AMP)

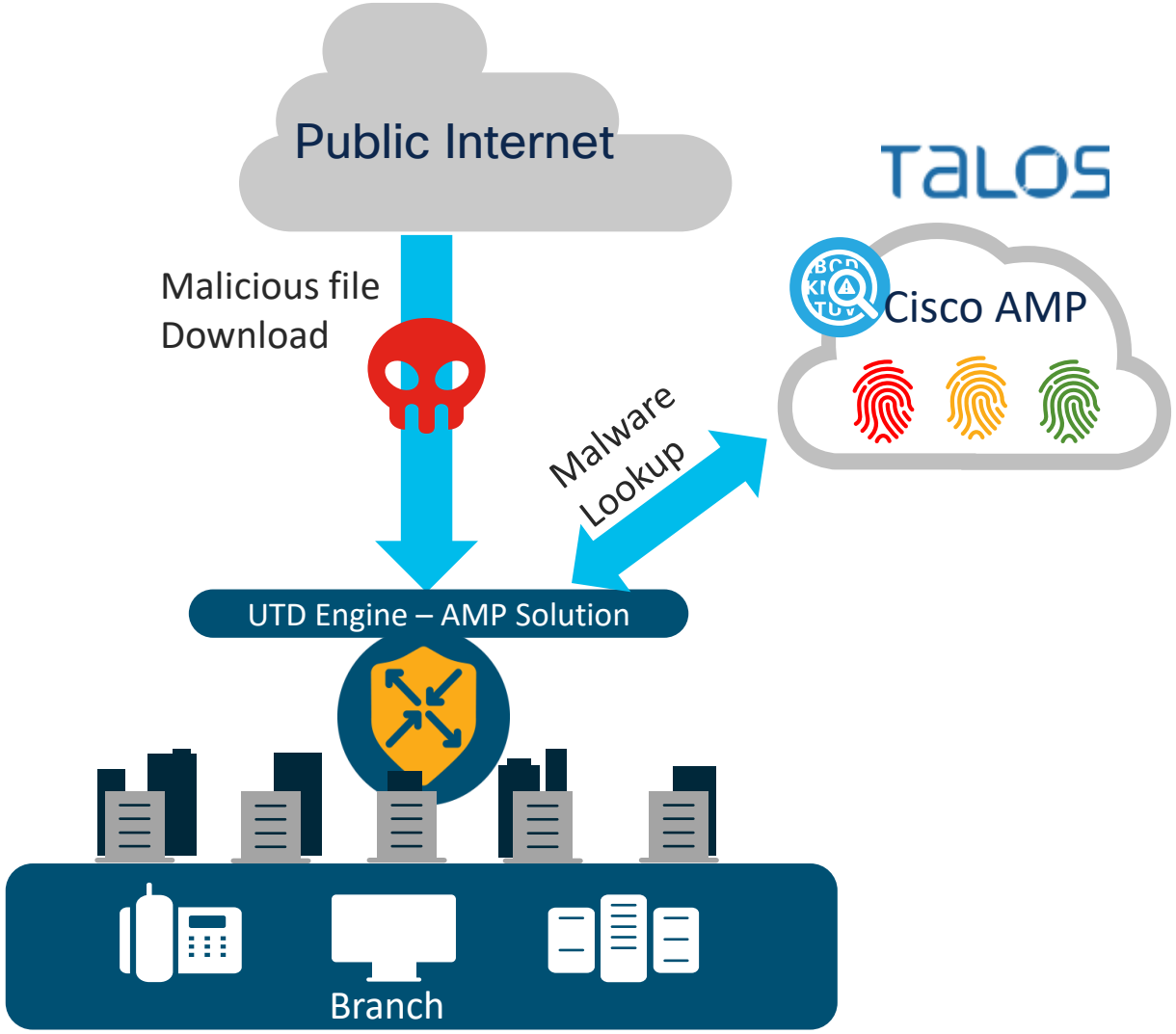
File Reputation & Retrospection

Use case

Jako administrator ds. bezpieczeństwa chcę, aby architektura bezpieczeństwa uwzględniała co raz bardziej wyrafinowane zagrożenia związane z plikami, a także zapewniała możliwość szybkiego śledzenia, powstrzymywania, analizowania i usuwania skutków udanych ataków

Feature

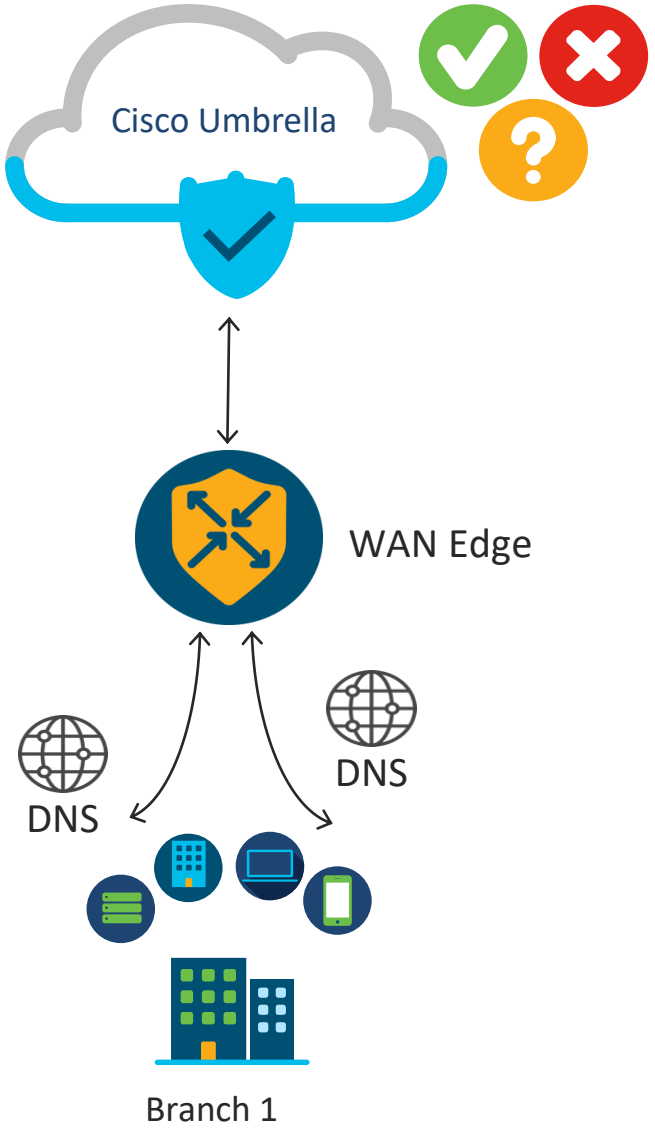
- AMP zapewnia ciągłe śledzenia i analizowania plików oraz aktywności plików podczas ich przemieszczania się w sieci
- Precyzyjne wykrywanie dyspozycji plików (czyste, nieznane lub złośliwe) w oparciu o współprace z TALOS, inteligencję działającą w czasie rzeczywistym
- Ciągłe aktualizacje danych o statusie plików z globalnej bazy danych AMP pomagają wykrywać i chronić przed złośliwym oprogramowaniem



DNS Security

- Cisco Umbrella – lider na rynku bezpieczeństwa DNS
- Blokowanie malware, phishing i nie bezpiecznych stron
- Wsparcie dla DNScrypt
- Bypass dla lokalnych domen
- Wsparcie dla dekrypcji ruchu HTTPS
- Inteligentne Proxy
- Również dla domowych rozwiązań

•208.67.222.222
•208.67.220.220
•2620:119:35::35
•2620:119:53::53



TLS/SSL Proxy

Use case

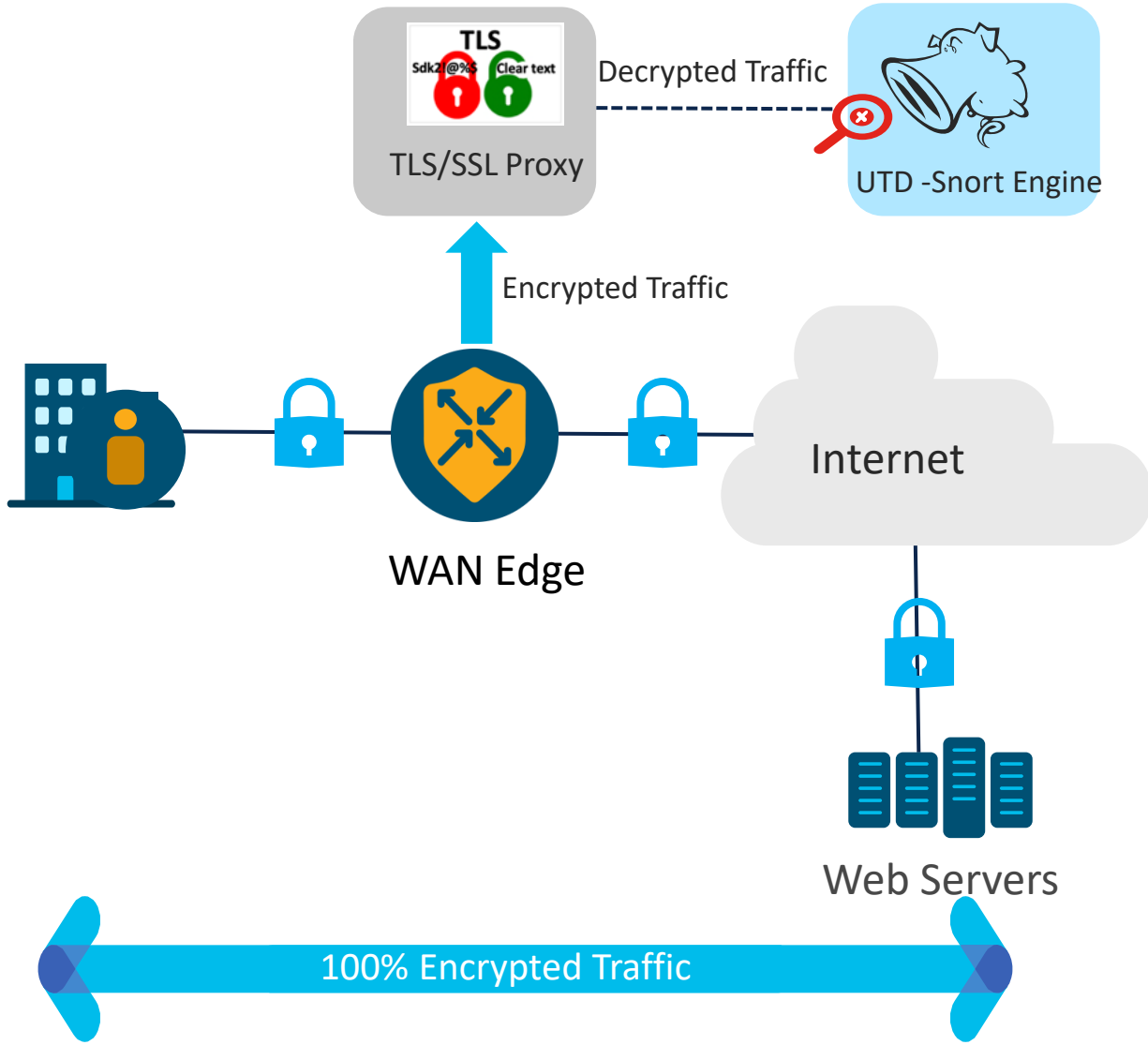
Jako administrator bezpieczeństwa, chcę mieć architekturę bezpieczeństwa, która może zidentyfikować złośliwe oprogramowanie i zagrożenia w zaszyfrowanym ruchu.

Feature

- TLS/SSL Proxy, które działana zasadzie man in the midle, odszyfrowując zaszyfrowany ruch TLS przez Internet i wysyłając go do silnika UTD Snort w celu przeprowadzenia zaawansowanej inspekcji bezpieczeństwa

- Egzekwowanie zasad bezpieczeństwa w oparciu o inspekcję odszyfrowanego ruchu

- Dane są ponownie szyfrowane po inspekcji, zanim zostaną wysłane do miejsca docelowego



Cisco SD-WAN Licensing
Model licencjonowania

Cisco DNA Essentials

Connectivity/Mgmt

- Cloud or On-Prem Management
- Flexible Topology
  - Hub and Spoke
  - Full Mesh/Partial Mesh
- App and SLA based policy
- Dynamic Routing (BGP, OSPF)
- VNF Lifecycle Management

Security

- Enterprise Firewall with Talos-powered IPS and application controls
- Cisco Umbrella DNS Monitoring (visibility only)

SD-WAN Services

- Basic Path optimization with FEC and Packet Duplication
- TCP Optimization

No Site Limit

Cisco DNA Advantage

Cloud/Analytics

- Cloud OnRamp for IaaS and SaaS
- Automated Service Stitching
- Encrypted Traffic Analytics
- vAnalytics

Security

- Segmentation (Unlimited VPNs)
- Cisco AMP and SSL proxy
- URL filtering
- Cisco Umbrella app discovery

X-domain Innovations

- Integrated Border for Campus (SD-Access)
- Integration with ACI for Application SLA

Services

- Web Caching, DRE (incl. SSL proxy)
- Voice Module and SRST Integration
- Multicast

Cisco DNA Essentials

Cisco DNA Premier

Security

Cisco Umbrella SIG Essentials

Transactional

- 5 – 250 Mbps = 1 License per Mbps
- 500 Mbps = 375 Licenses
- 1 Gbps = 500 Licenses
- 2.5, 5, 10 Gbps = 750 Licenses

Enterprise Agreement

- Tier 0: Not Available in Premier
- Tier1: 25 Licenses
- Tier 2: 250 Licenses
- Tier 3: 750 Licenses

- Additional Cisco Umbrella SIG Essentials licenses can be purchased separately.

Cisco Threat Grid

- Provides entitlement for 200 files per day per customer account
- Files sent to Threat Grid cloud for sandboxing. On-premises Threat Grid not available in Premier
- Global entitlement across all customer sites
- Additional Cisco Threat Grid licenses can be purchased separately.

Cisco DNA Advantage

Cisco DNA Essentials

NEW SD-WAN Licensing Enhancements

Availability Dec 11, 2021

Enhancements / Additions

Cisco DNA Essentials

Existing Capabilities +

Cloud Networking

- IaaS: GCP, AWS, Azure
- SaaS: All (M365, Webex …)

Security

- URL Filtering, IPS, AMP, SSL Proxy
- VPN Segments: 2+1 -> 4 +1

Cloud Security:

- Cisco Umbrella app discovery
- Umbrella Connector
- 3rd party Cloud Security Provider

Cisco DNA Advantage

Cloud/Analytics w/ Telemetry

- Advanced Cloud OnRamp for IaaS and SaaS
- Automated Service Stitching
- vAnalytics
- SD-WAN Application Intelligence Engine

Security

- Segmentation (Unlimited VPNs)

X-domain Innovations

- Integrated Border for Campus (SD-Access)
- Integration with ACI for Application SLA

Services

- Web Caching, DRE (incl. SSL proxy)
- Voice Module and SRST Integration1
- Multicast

Cisco DNA Essentials

Cisco DNA Premier

No changes

Cisco DNA Advantage

Cisco DNA Essentials

Consistency and Simplicity of SD-WAN BW Consumption

Cisco Bandwidth Tiers			
Current Tiers	**BW**		**New Tier (EA/MSLA/ALC)**
T0	10M		**T0** **25M (Increase)**
	15M		
	25M		
T1	50M		**T1** **200M (Increase)**
	100M		
	200M		
T2	250M		**T2** 1G
	500M		
	1G		
T3	2.5G		**T3** 10G
	5G		
	10G		

5M Option for IoT/M2M

- Applicable across all consumption models (ALC, EA and MSLA)
- Target Availability:

  Early December 2021
- 5M Targeted for ATM / KIOSKS / IoT use-cases

Networking

SD-WAN

Learn how to confidently adopt Cisco's SD-WAN solution in a new or existing network. These sessions provide an advanced journey through the latest Cisco SD-WAN innovations including recent development and integration with Cloud, SASE and Assurance/Analytics.

START

Feb 6 | 08:30
TECENT-2376
From Zero to SD-WAN Hero: Planning, Designing and Implementing Cisco SD-WAN

Feb 6 | 08:30
TECARC-2407
Architecture, Deployments, and Troubleshooting Deep Dive for Catalyst 8000 Series Edge Platforms

Feb 6 | 14:00
TECTRS-3477
Advanced Troubleshooting SD-WAN

Feb 7 | 08:30
BRKENT-1656
Beginner's Guide to Enterprise Network Monitoring with ThousandEyes

Feb 7 | 11:30
BRKENT-2108
Cisco SD-WAN: Start Here

Feb 7 | 11:30
BRKNWT-2210
Predicting Networks are THERE !!

Feb 7 | 14:00
BRKENT-2628
ThousandEyes with Catalyst 8000 routers: Empowerment from Data in your Pocket

Feb 7 | 15:30
BRKENT-2139
How to Choose the Correct Branch Router

Feb 7 | 17:00
BRKENT-2423
SD-WAN From Design to Reality

Feb 8 | 08:30
BRKENT-2653
All You Need to Know about Forwarding on the Catalyst 8500 and 8500L Platforms

Feb 8 | 08:30
BRKOPS-2857
Deploy Visibility in Your SASE Architecture With ThousandEyes

Feb 8 | 08:30
LTRENT-2052
IPv6 Routing, SD-WAN and Services Lab

If you are unable to attend a live session, you can watch it On Demand after the event

cisco Live!

Feb 8 | 08:30

LTRENT-3615

Cisco SD-WAN Multi-Region Fabric – from Zero to Hero

Feb 8 | 10:30

BRKXAR-2003

Extending Enterprise Network into Public Cloud with Cisco Catalyst 8000V Edge Software

Feb 8 | 12:00

BRKENT-2652

Simplify User Experience through Software defined Interconnect and Public cloud

Feb 8 | 14:30

BRKTRS-3475

Advanced Troubleshooting of cat8k, asr1k, ISR and SD-WAN Edge Made Easy

Feb 8 | 16:30

BRKENT-2060

Cisco SD-WAN Cloud OnRamp for Multicloud – from Connectivity to Application Integration

Feb 8 | 16:30

BRKENT-2651

Migration to Multi-Region Fabric – Transform and Simplify Middle-mile Based Network Designs for Large Scale, Cloud and Colo based SD-WAN Networks

Feb 8 | 16:45

BRKXAR-2001

Cisco Intent Based Cross and Multidomain Integrations for SDA and SD-WAN

Feb 9 | 08:30

BRKARC-2885

Cisco Catalyst 8500 Series Edge Platform Deep Dive

Feb 9 | 10:30

BRKENT-2837

GAME Time ! Will You Be the Networker of the Year ?

Feb 9 | 10:30

BRKENT-3297

Multi-Cloud SD-WAN Design

Feb 9 | 12:00

BRKENT-2312

Evolution of Cisco SD-WAN Security and Journey Towards SASE

Feb 9 | 14:15

BRKENT-3412

How to Optimize SaaS Applications using Cisco SD-WAN

Feb 9 | 15:45

BRKENT-2126

Three Steps to Gain Actionable Visibility in the Cisco SD-WAN Using ThousandEyes

Feb 9 | 15:45

BRKMER-1003

Cisco+ Secure Connect – Connect and Secure with Meraki

Feb 10 | 11:00

BRKTRS-3457

Cross-Domain Integration: Troubleshooting Cisco SD-Access – SD-WAN Integration

Feb 10 | 11:00

BRKTRS-3793

Advanced SD-WAN Routing Troubleshooting

Feb 10 | 11:15

FINISH

BRKOPS-3179

Wide Area Bonjour (mDNS) – Best practices, Design and Deployment

If you are unable to attend a live session, you can watch it On Demand after the event

cisco Live!