
cisco Live!
ALL IN

The bridge to possible

Cisco SD-WAN Security Evolution to SASE

Rohan Naggi – Engineering Product Manager
@lifeboy
Kureli Sankar – Leader, Technical Marketing
BRKENT-2312

Cisco Webex App

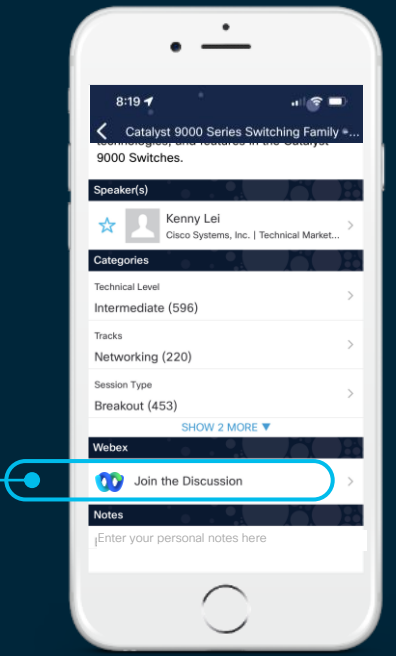
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

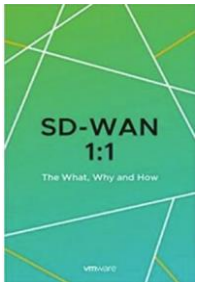
Webex spaces will be moderated by the speaker until June 17, 2022.

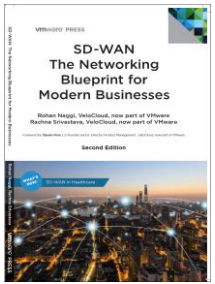


https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-2312

About Me

- Rohan Naggi – Twitter @lifeboy
- Product Manager @Cisco SDWAN BU
- Author for SD-WAN, SASE books
- Podcaster, Technology Influencer , Video Blogger
- Mountain biker





About Me

- BS in Electrical and Electronics Engineering
- 2006 – 2013 TAC Engineer
  - CCIE Security #35505
- 2013 – 2018 Technical Marketing Engineer
- 2019 – Present Leader, Technical Marketing
- Areas of expertise
  - IOS and IOS-XE security features
  - SD-WAN Security solutions
- 2018 – 2x Distinguished Speaker Cisco Live

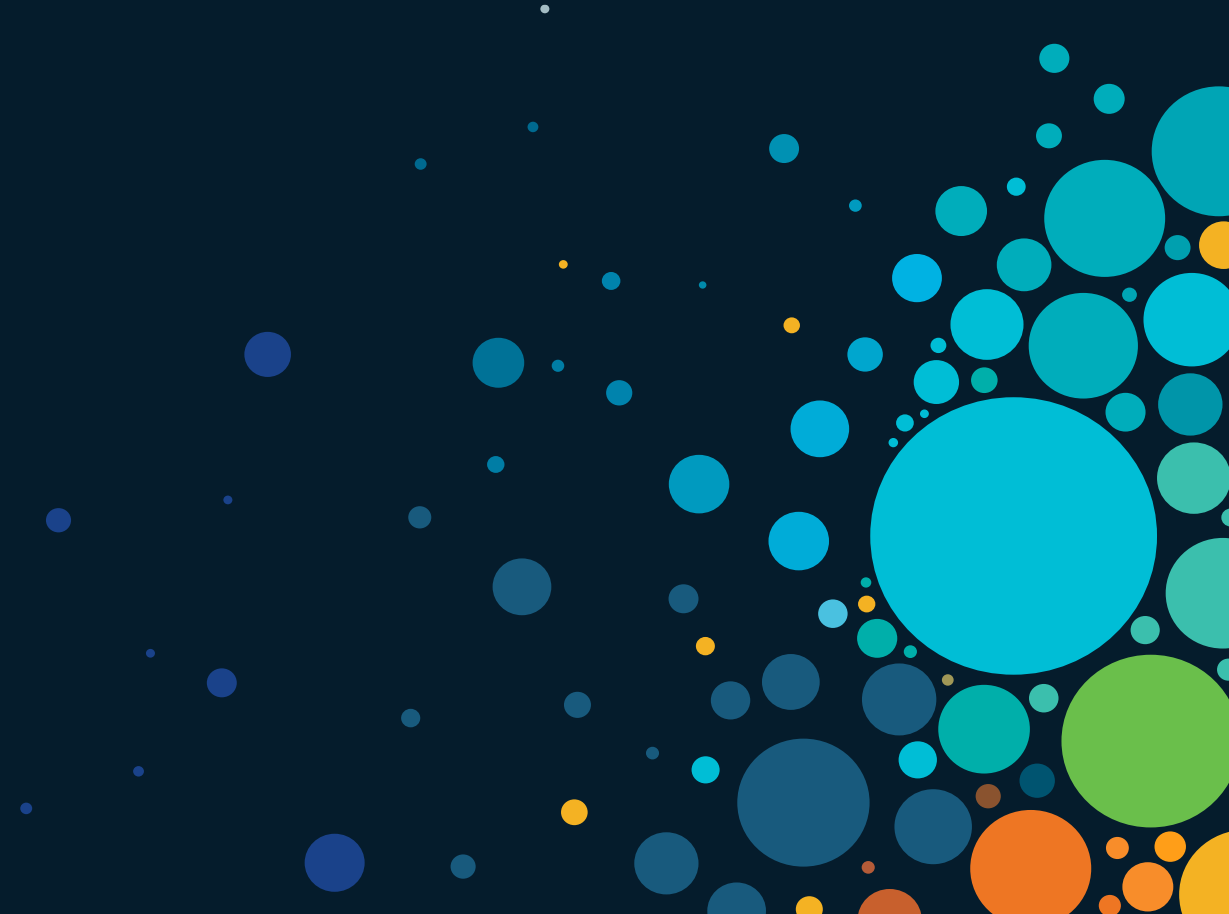
35505

2018
CL EUR and CL MEL

Agenda

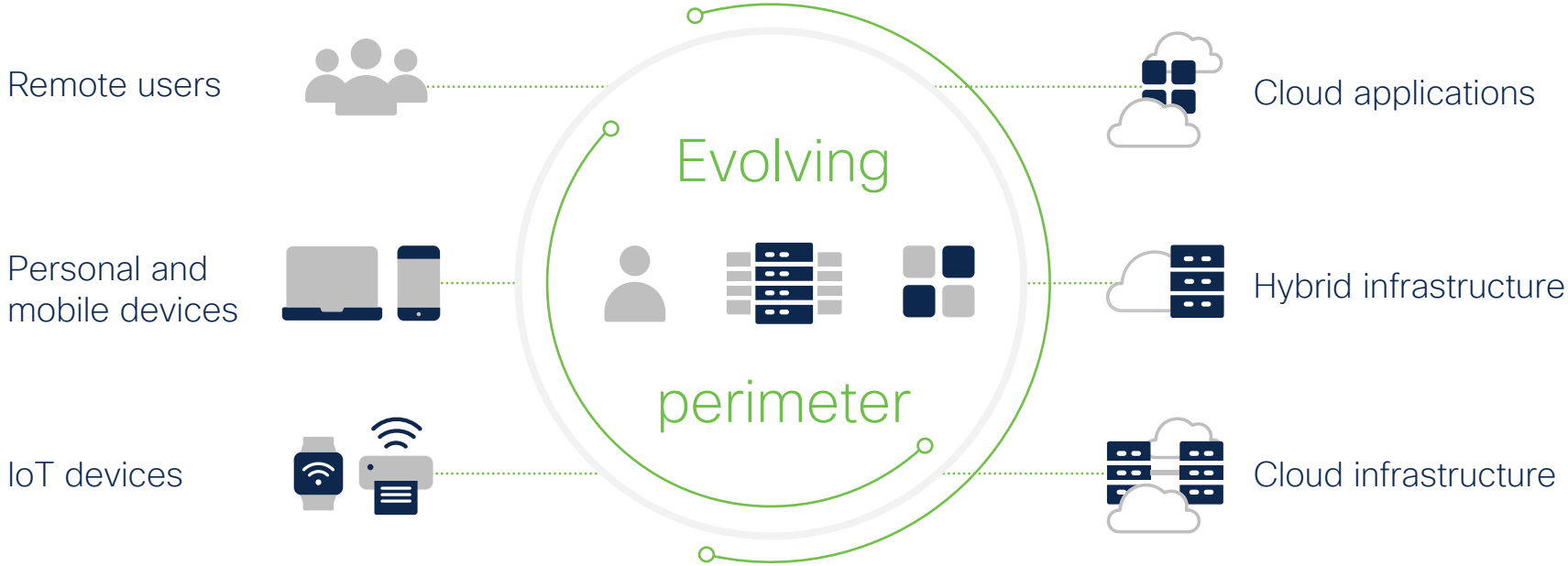
- Market Landscape
- Cisco SD-WAN Innovation
- SD-WAN with Distributed Security Today
- Embedded Security enhancements
- Cloud security enhancements
- Demo time
- By END of this session you will get an overview of all the offering within SD-WAN security which helps in completing SASE journey

Market Landscape



Shift in IT landscape

Users, devices, and apps are everywhere



Cisco SD-WAN Innovations

cisco Live!

Cisco SD-WAN Innovations driving the new norm

Multicloud

Multicloud Access

SDCI / Cloud Backbone

Security

Enterprise FW, IPS, SIG, Adv Malware Protection

Security and Segmentation

Umbrella – SWG, FW, DNS Sec, Zero Trust

zscaler

Cisco+ Secure Connect

AIOps

Analytics and Visibility

WAN Insights

Intuitive Experience

Simplified UX

Enhanced Upgrade

Self Service Portal

App Experience

Voice Optimization

SaaS Optimization M365, Webex

AppQoE – TCP Opt, FEC, DRE, etc.

MSP

Multi-tenant SD-WAN Edge

Multi-Region Fabric

Co-managed SD-WAN Service

Platforms

SD-WAN Remote Access

250GB IP CEF Aggregation Platform

Higher C8K Dataplane Performance

Cisco SD-WAN Security Today

cisco Live!

SD-WAN with Distributed Security Enforcement

SD-WAN Integrated Security

- **Enterprise Firewall –** Stateful Firewall with App Aware
- **IPS** - Intrusion Prevention System
- **URL Filtering** based web reputation categories
- **AMP** - Advanced Malware Protection with File Reputation and Sandboxing from Talos
- **TLS Proxy** – Threat / File Inspection for Encrypted Traffic
- **Unified logging** for Firewall and security components
- Identity based Firewall based on User/User Group (coming in Release 17.9)

Fabric Security

- Encrypted Data Plane and Control Plane
- Enhanced Security with Pairwise keys model
- Hardware Based Device Authentication (SUDI)
- Zero Trust Model for all the fabric component

Cloud Security

- **DNS security** – to block unwanted or malicious content
- Ease of provisioning of either **IPSEC or GRE tunnel** to Secured Internet Gateway
- **Traffic Load balancing (ECMP)** using multiple paths with high performance & lower latency
- **Simplified** Configuration workflow
- **Layer-7 Health Check** for failure detection and resolution

Cisco Umbrella

3rd Party SIG partnership

Granular visibility

Multi-layer insights

Thousand Eyes

Network KPIs

Application performance

Cisco SD-WAN Embedded Security

cisco Live!

Enterprise Firewall

Product Evolution

Zone Based Firewall

- Stateful, zone-based traffic inspection
- VPNs are tied to zones
- Supports Traffic inspection between same VPNs/across different VPNs/to public Internet
- Self Zone protection for targeted attacks to the router interfaces

Layer 7 App Visibility

- Blocks traffic based on applications or application-family
- Application visibility and granular control
- Uses NBAR/SD-AVC integration to match application traffic

HSL Logging

- Firewall logs can be sent to an external third-party collector
- Supports the high-speed logging (HSL) of firewall messages by using NetFlow version 9 as the export format

Enterprise Firewall

Product Evolution

FQDN Support

- Simple and flexible firewall rules based on domain names
- Reduces number of rules created based on IP addresses
- Easy to troubleshoot based on Firewall logs with resolved domain names

Multiple Prefix Lists/Rule Set Support

20.4

- Multiple Prefix List/Ports/Protocols (source/destination) supported
- Rule Set support to group/combine rules to have common allow, drop, or inspect policy

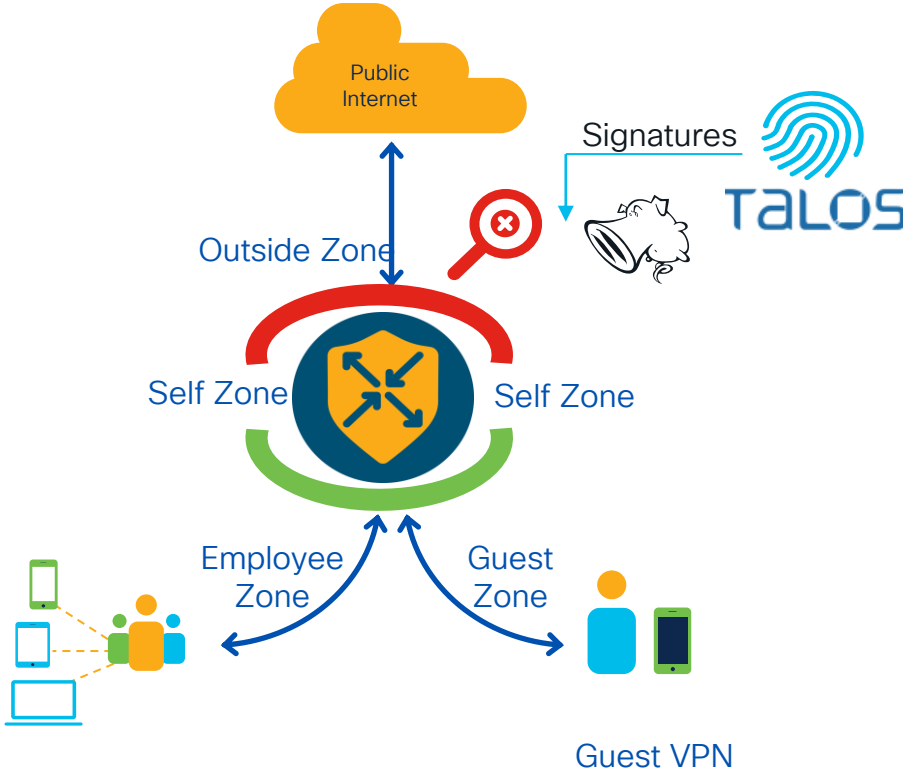
Geo Location Support

20.5

- Allow/block certain geo location and allow traffic from desired location
- Geo information includes list of countries and/or continent
- Geo to IP database mapping from Digital Element (third party)

SD-WAN Unified Security Policy- 17.6

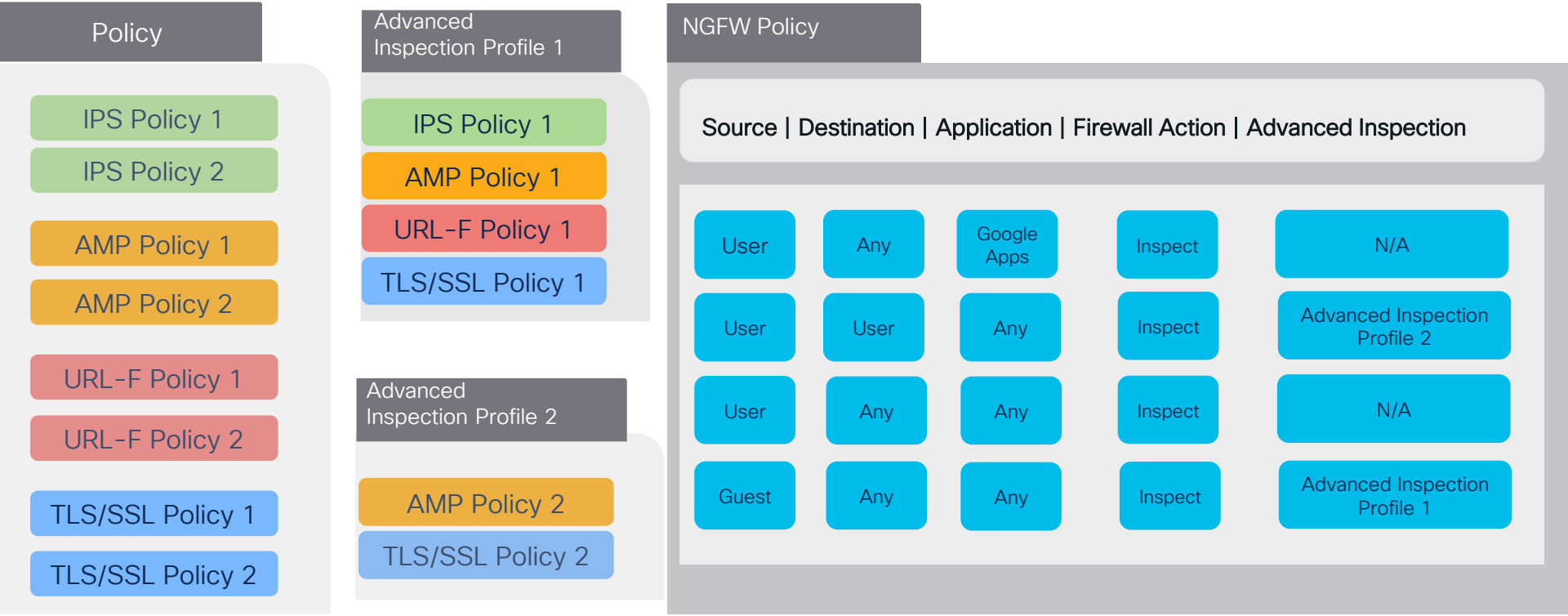
With the introduction of Unified Security Policy in 20.6/17.6, Customers now have the flexibility to configure security policies in a granular fashion and apply advance inspection profiles making the behavior synonymous to a NGFW which is popular in the security industry.



SD-WAN Unified Security

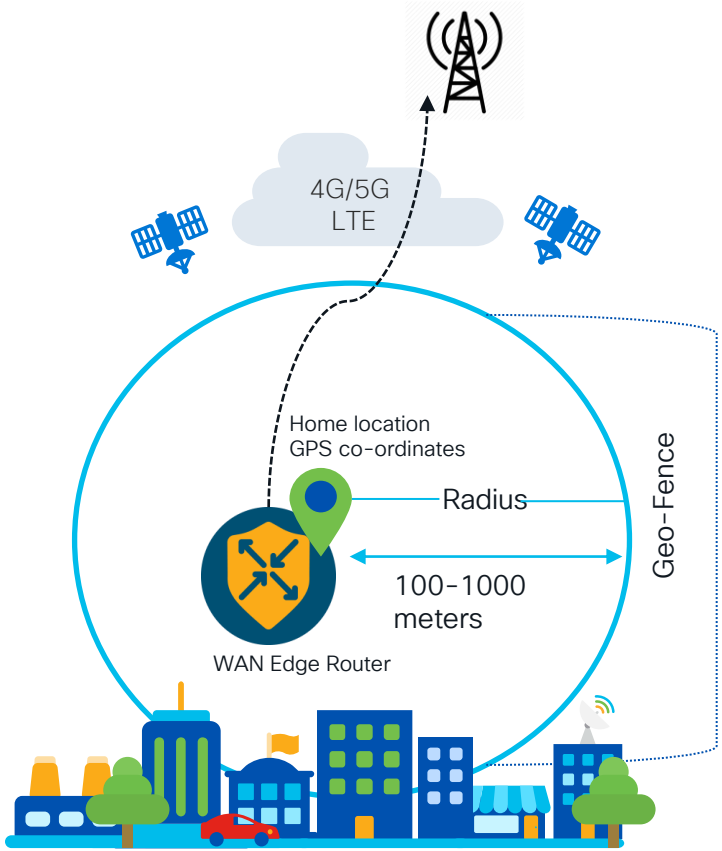
How it works ?

- Advanced Inspection Profile (AIP) can now be applied for each use case, can be reused across multiple policies.
- AppFW now supports Inspect, Drop and Pass.
- AppFW is now implemented as a filter.
  Datapath now uses all filters including application to filter traffic.

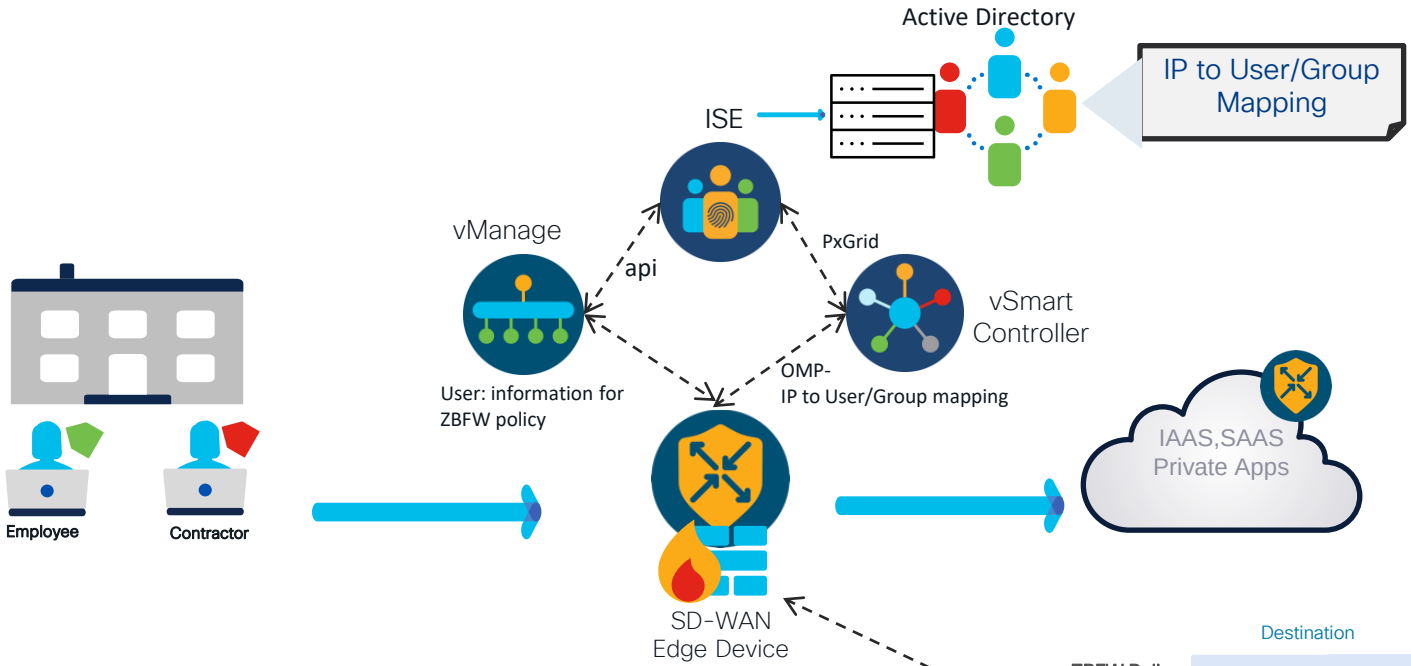


Geo Fencing with SD-WAN Edge Devices -17.6

- Geo Fencing feature can be enabled on the WAN edge routers
- Utilizing location-based services (GPS) to track the assets
- Provide real time alerts on vManage/SMS to registered mobile numbers if the device moves out of the authorized geographical boundary
- Supported actions - Device invalidation, stop the data traffic and factory reset



Identity Based Firewall (17.9)



Destination

Source \ ZBFW Policy	Employee	Contractor
Employee	Permit All	Deny All
PLC	Permit All	Deny All
Contractor	Deny All	Permit All

- Granular Security Control at User/Group Level
- Unified Security policy and intent

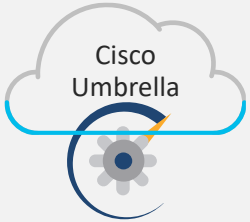
Cisco SD-WAN SASE SIG Innovation Journey

cisco Live!

SIG Integrations

Product Evolution (Before-20.5/17.5)

Rapid-Onboarding



- SD-WAN Edge devices are automatically registered to Umbrella
- No need to manually enter API keys
- Secure API key is automatically provisioned on the edge device via an HTTPS session

SIG Template

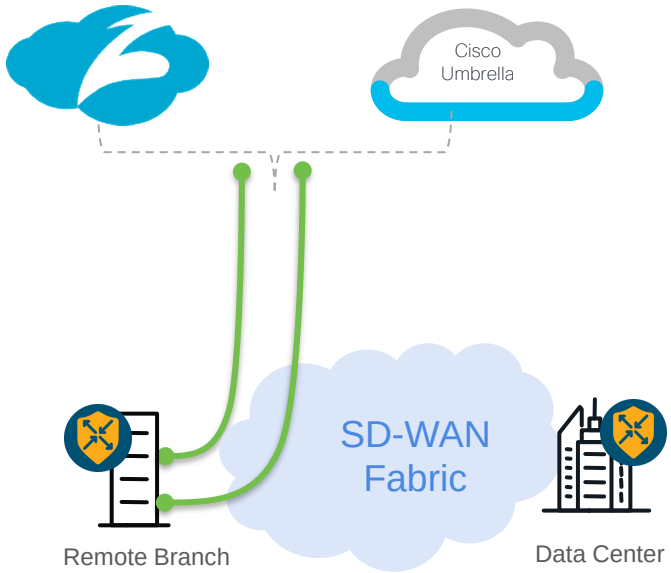
vManage

- By pushing the SIG feature template, a customer can now setup an IPsec tunnel to Umbrella SIG
- Consistent Tunnel Design
- Automatic Tunnel Creation

Increased Throughput Capabilities and Traffic Engineering

- Multiple Tunnels (4-Active/ 4 backup Through template)
- ECMP Load balancing
- Weighted load balancing
- Data-policy support for selective Traffic re-direction based on app-classification

Unified Secure-Internet Gateway(SIG) Workflow



Summary

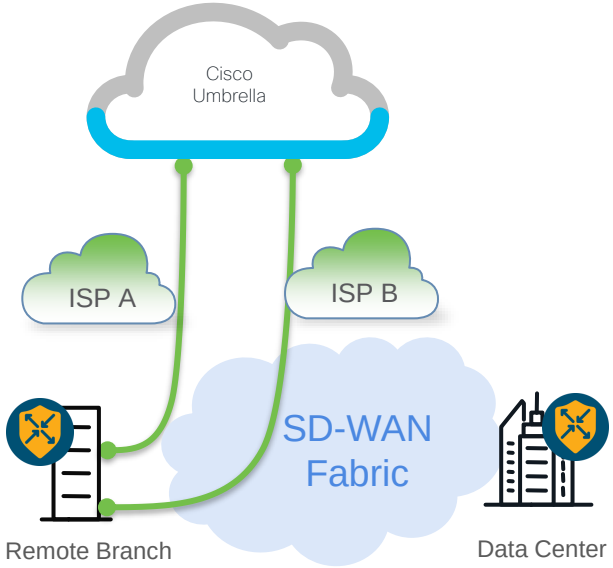
Multiple vManage SIG workflows exist today for Umbrella and Third Party. Various deployment models exits for SIG as one could create the tunnels on both Service and Transport side.

Solution

Introduce a consistent SIG workflow experience to our customers by enhancing SIG templates as a deployment model to provision tunnels for Umbrella and 3rd party including Zscaler.

Supported Platforms	XE SD-WAN	Viptela OS

Active-Active SIG Tunnels



Summary

As of 20.3/17.3, you can only deploy SIG tunnels in an Active/Backup mode.
With more and more compute shifting to cloud, customers require throughout beyond 250mbps.

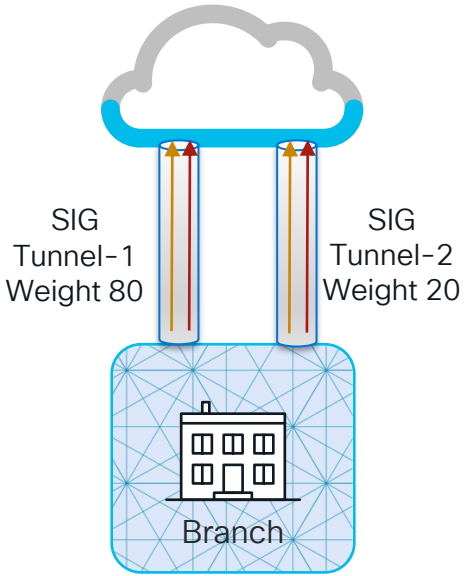
Solution

Effective 20.4/17.4, Users will now be able to configure up to 4 active tunnel pairs to get the benefit of ECMP load-balancing across multiple tunnels. You can assign tunnel weights to influence the load-balancing mechanism or to prefer one tunnel over the others.

Supported Platforms	XE SD-WAN	Viptela OS

Weighted Load-Balancing

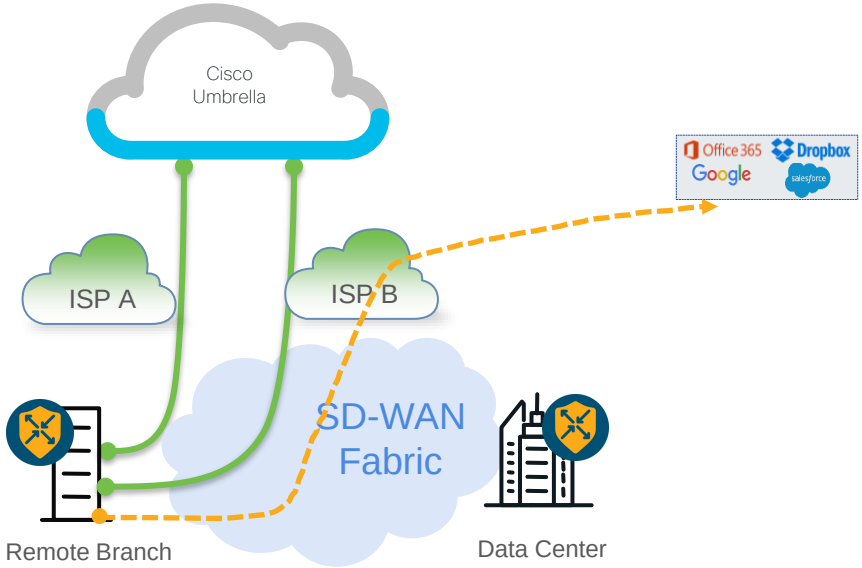
Load balancing is done by flow pinning, where a flow is dictated by hashing the 4 Tuple (Source IP + Destination IP + Source Port + Destination Port).



Active-Active SIG Tunnels

Traffic will be load-balanced across SIG tunnels in a 80:20 ratio

SIG Data-Policy



Summary

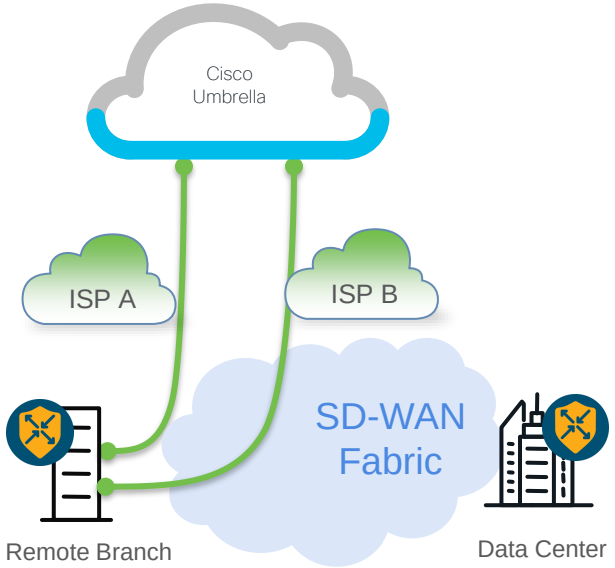
Currently traffic steering to SIG (Umbrella/Zscaler) is achieved via “service-route”. This workflow doesn’t allow customers to selectively steer certain applications/traffic of interest to SIG; instead, it’s a catch-all policy which applies to “every” traffic from the WAN edge.

Solution

Introduce “Centralized Data Policy based” traffic steering to SIG tunnels, which provides more flexibility for a Customer to drive their business intent, where one can leverage existing data-policy constructs like app-list, prefix-list etc as criteria to steer such traffic/applications to a SIG tunnel

Supported Platforms	XE SD-WAN	Viptela OS

Design Considerations - SIG Baseline

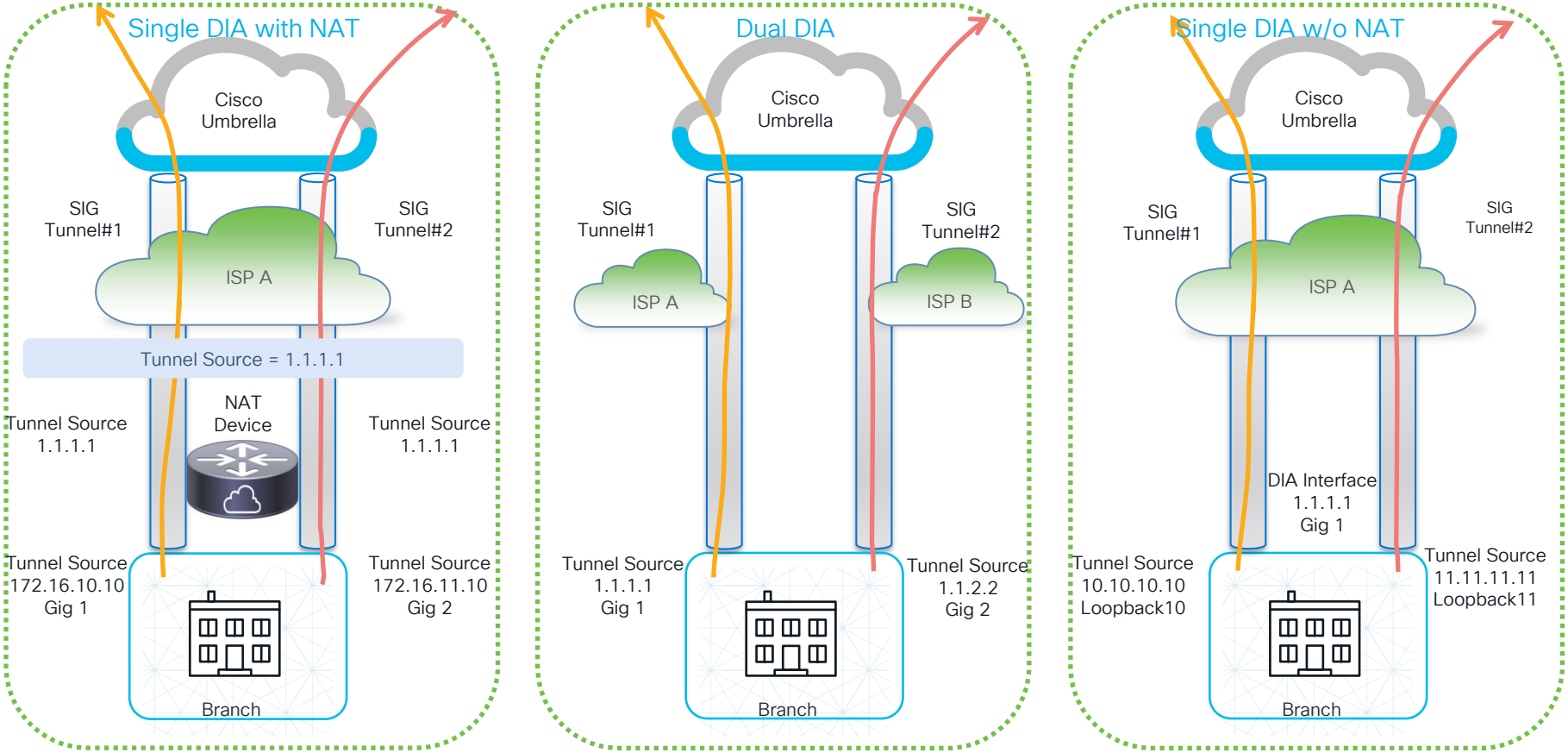


Considerations

- Umbrella requires that the Service VPN address-space falls within RFC1918
- Both Umbrella and Zscaler support NAT-T
- When Onboarding multiple Active-Active tunnels, each tunnel 4-Tuple should be unique for the tunnel to be UP and Operational
- NAT on DIA interface is a must requirement.
- DNS Web-Security over SIG Tunnels is a No-Go

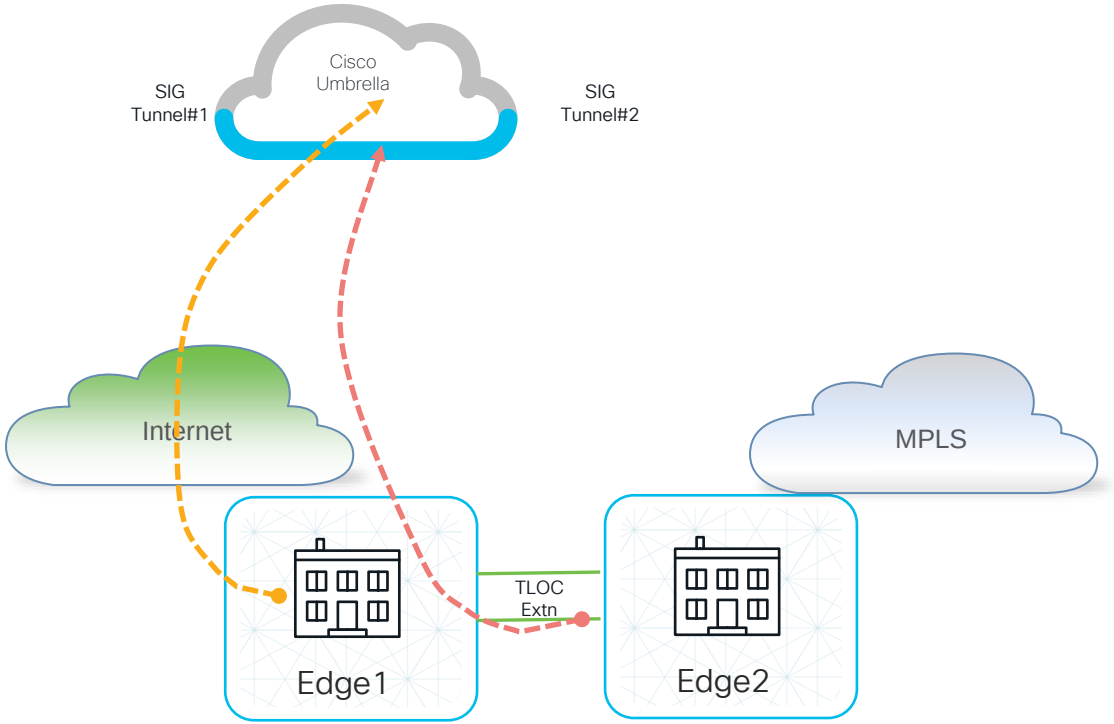
Secure Internet Gateway (SIG) Deployment Use Cases

SIG Deployment Use-Cases



Branch with Single DIA

Use-Case 4



Deployment Overview

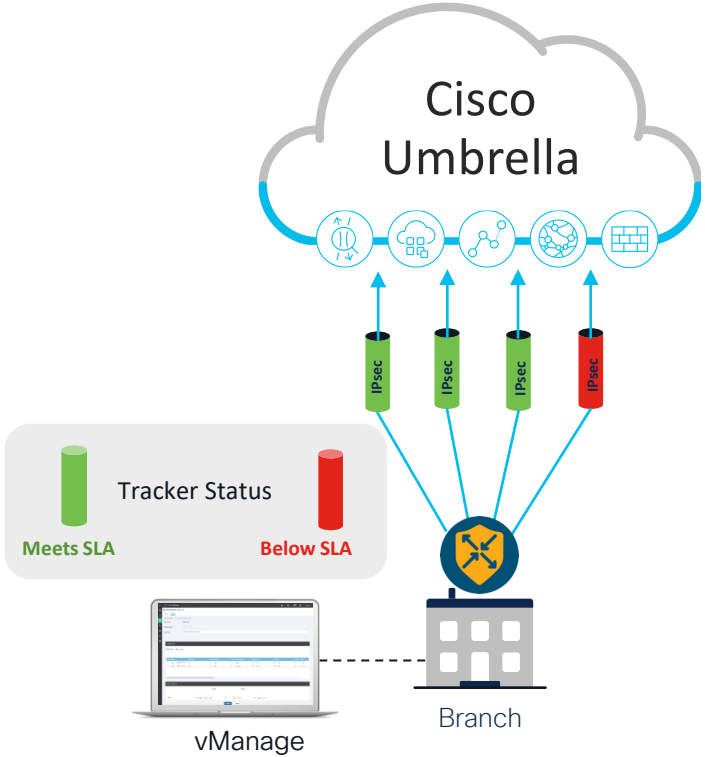
- Branch with two Edges, where one Edge has a MPLS breakout and the other one has an Internet breakout
- TLOC Extension is configured between the routers
- No NAT device in front of Edge router
- Branch aggregate traffic throughput requirement > 250Mbps
- Customer can onboard first SIG tunnel sourcing the DIA interface of Edge1
- Second SIG tunnel can be created sourcing the TLOC Extn interface of Edge2

Layer7 Health Check 17.6.2

vEdge(20.5) ✓

cEdge ✓

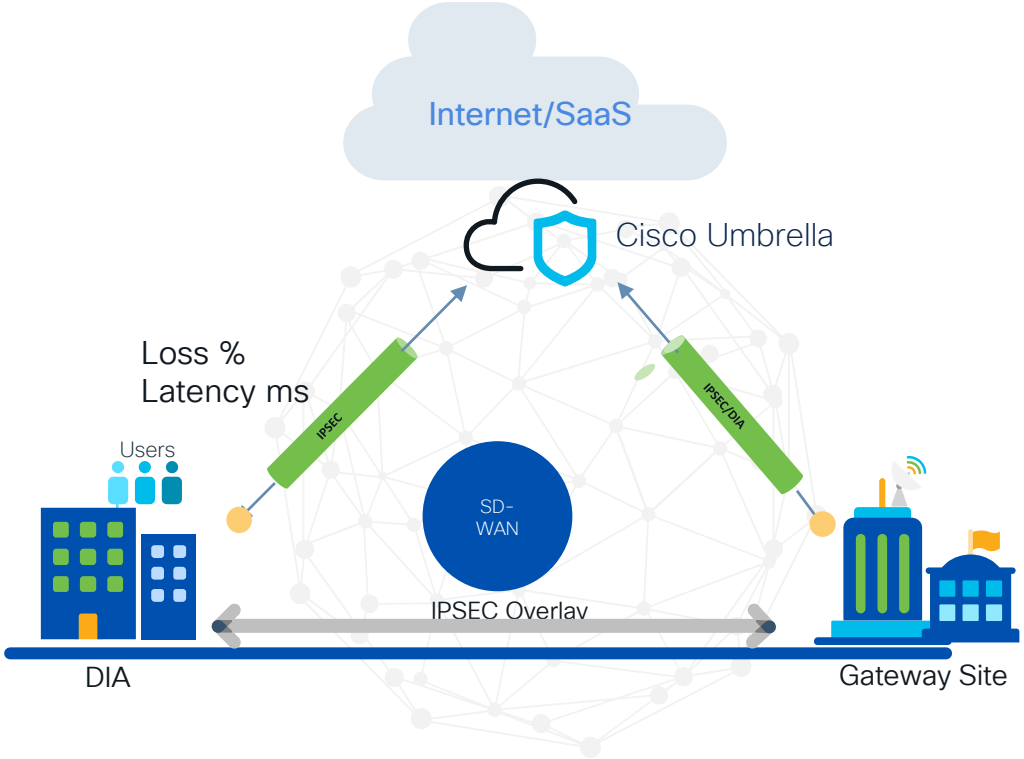
Tracking SIG Tunnel Health



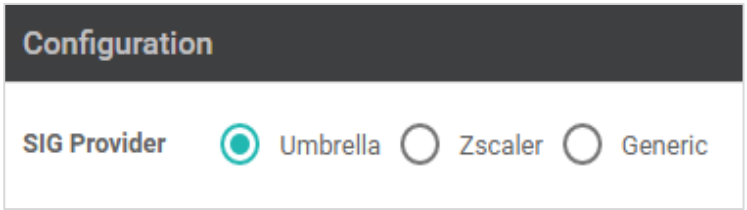
- Default tracker sends HTTPing request to the service API, measures the RTT latency and compares with default threshold.
- Tracker status for the tunnels which does not meet the SLA are marked down.
- Optionally Customers can create a custom tracker to override the default parameters or use any service URL of their choice.

Cloud OnRamp for SaaS for SIG- 17.6

Predictable Application Experience, Granular app controls

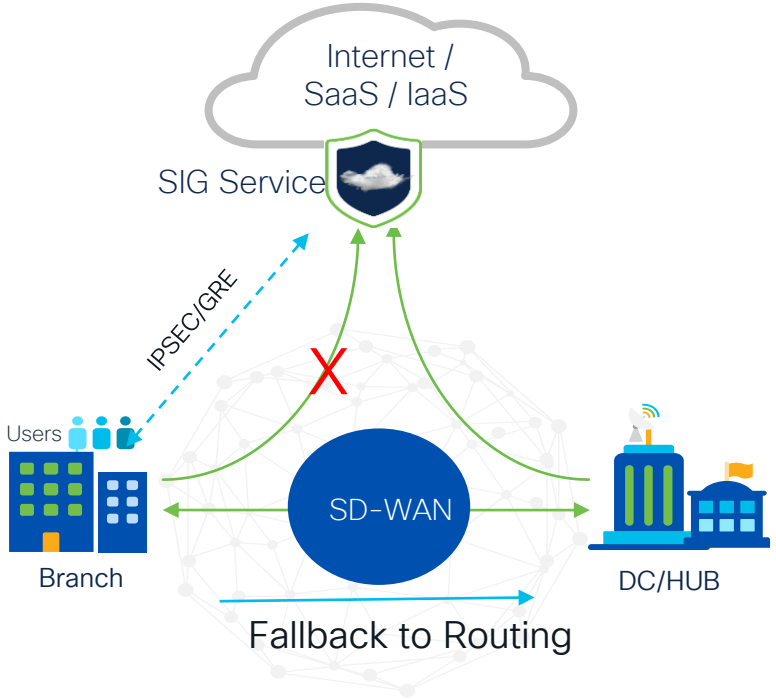


- CoR for SaaS continuously monitors the application performance from SD-WAN Edge to SaaS, and picks the best performing SIG tunnels based on loss, latency metrics.
- Supports CoR for SaaS workflow over Umbrella IPSEC tunnels to get tighter security controls for SaaS access.



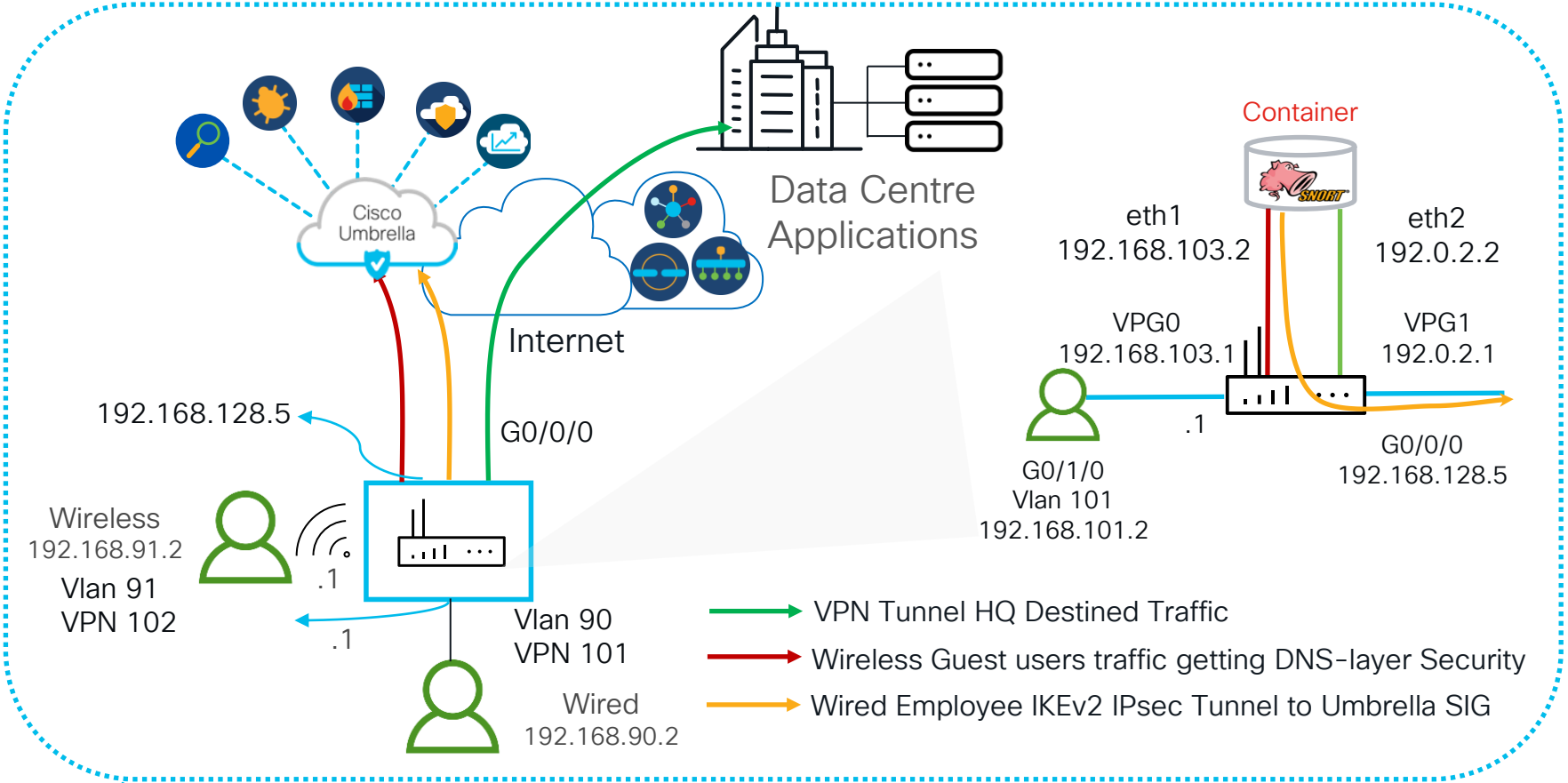
Fall-back Routing for SIG (17.8)

- Traffic Data policy Redirect traffic to SIG
- If SIG tunnel is down, fallback to omp routing to avoid blackholing



Demo

Demo Topology



Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Security Reference Architecture

CISCO SECURE

TALOS — Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

- Managed Detection and Response Services
- Security, Orchestration, Automation and Response
- Incident Response and Remediation Services
- Threat Visibility & Hunting
- Device Insights
- Kenna Vuln Mgmt
- Secure Cloud Insights
- 3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access

Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed

Cisco Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Visibility)

Device Mgmt

Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE) | ZERO TRUST

Threat Protection | Secure Access Control | Managed Remote Access

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

Umbrella/Duo

- ZTNA
- DNS-layer security
- Secure web gateway
- L7 firewall + IPS
- Cloud access security broker/ shadow IT
- RAaaS
- SSL decryption
- Remote browser Isolation
- Data loss prevention
- Cloud malware detection

SDWAN

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes
- Cloud DDoS,WAF

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

- Industrial Router
- Industrial Firewall
- Industrial Switch/AP
- Cyber Vision
- ISE TrustSec

ZERO TRUST

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

- Security Analytics and Logging
- Secure Firewall
- DuoCloud SSO+IDP
- Network Gateway
- Secure DDoS
- Meraki Full Stack
- Secure Network Analytics
- Secure Web Appliance
- ISE TrustSec
- Cisco DNA Center

Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

- Cloud Native Security
- APIC
- Secure Workload
- Secure Application by AppDynamics

App Observability | Detection | Response

- Hybrid Private
- Public Cloud
- Secure Cloud Analytics
- Secure Firewall
- ThousandEyes
- Secure DDoS, WAF/Bot

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Learning Map

Branch and Aggregation Routing Solutions

BRKENT-2312 You are here!

Branch Router Segmentation & Security

TECARC-2407

Architecture, Deployments and Troubleshooting deep dive for Catalyst 8000 Series Edge Platforms

BRKARC-1881

Which one is the perfect ISR1K for me?

BRKXAR-2003

Extending Enterprise Network to the public cloud with Cisco Catalyst 8000V Edge Software

BRKARC-2885

Cisco Catalyst 8500 Series Edge Platform Deep Dive

BRKENT-2809

Untangle Enterprise Direct Cloud Connectivity with Powerful Catalyst 8500 Series Edge Platforms

BRKSEC-2419

Branch Router Segmentation & Security

Thank you


cisco Live!
ALL IN