

The background of the slide is a vibrant, abstract graphic. It features a series of overlapping, wavy bands of color in a rainbow spectrum, transitioning from red and orange on the left to yellow and green on the right. On the right side, there is a bright, multi-colored sunburst or starburst effect that radiates outwards, with colors ranging from blue and purple to yellow and green. The overall composition is dynamic and energetic.

cisco *Live!*

Let's go

#CiscoLive



The bridge to possible

Evolution of Cisco Catalyst SD-WAN Security and Journey Towards SASE

Prashanth Raghavendra, Technical Marketing Engineer Technical Leader
BRKENT-2312

CISCO *Live!*

#CiscoLive

Cisco Webex App

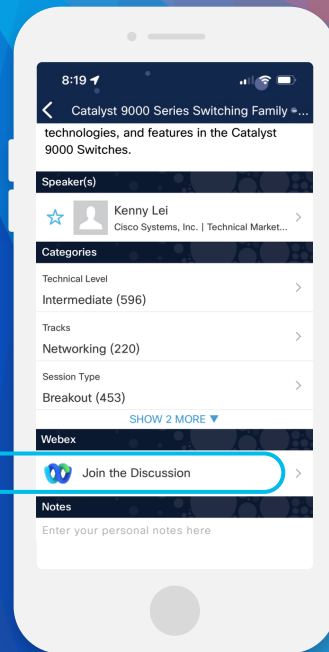
Questions?

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 December 22, 2023.



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

About me



Prashanth
Raghavendra

SD-WAN
Technical Marketing
since 2020

Focus areas:

- User/Application Experience
- Operational features
- Security Policies
- Analytics

Presented sessions at various Cisco events:

- Cisco Live Melbourne/Amsterdam
- Cisco EN SEVT
- APJC SD-WAN Roadshows

Cisco Catalyst SD-WAN innovations driving the new norm

Multicloud



Multicloud
Access



SDCI/Cloud
Backbone

App Experience



Voice
Optimization



SaaS
Optimization
M365, Webex



AppQoS - TCP Opt,
FEC, DRE, etc.

Security



Embedded Security



Segmentation



Cisco+
Secure
Connect



Compliance

AIOps



Analytics and
Visibility



WAN
Insights



Intuitive Experience



Simplified UX



Enhanced
Upgrade



Self Service
Portal



Cloud-delivered
Cisco Catalyst SD-WAN

DevOps



App
Automation



Intent
Automation



API/SDK

MSP



Multitenant
SD-WAN
Edge



Multi-Region
Fabric



Co-managed
SD-WAN Service

Platforms



SD-WAN
Remote
Access



400G IP CEF
Aggregation
Platform



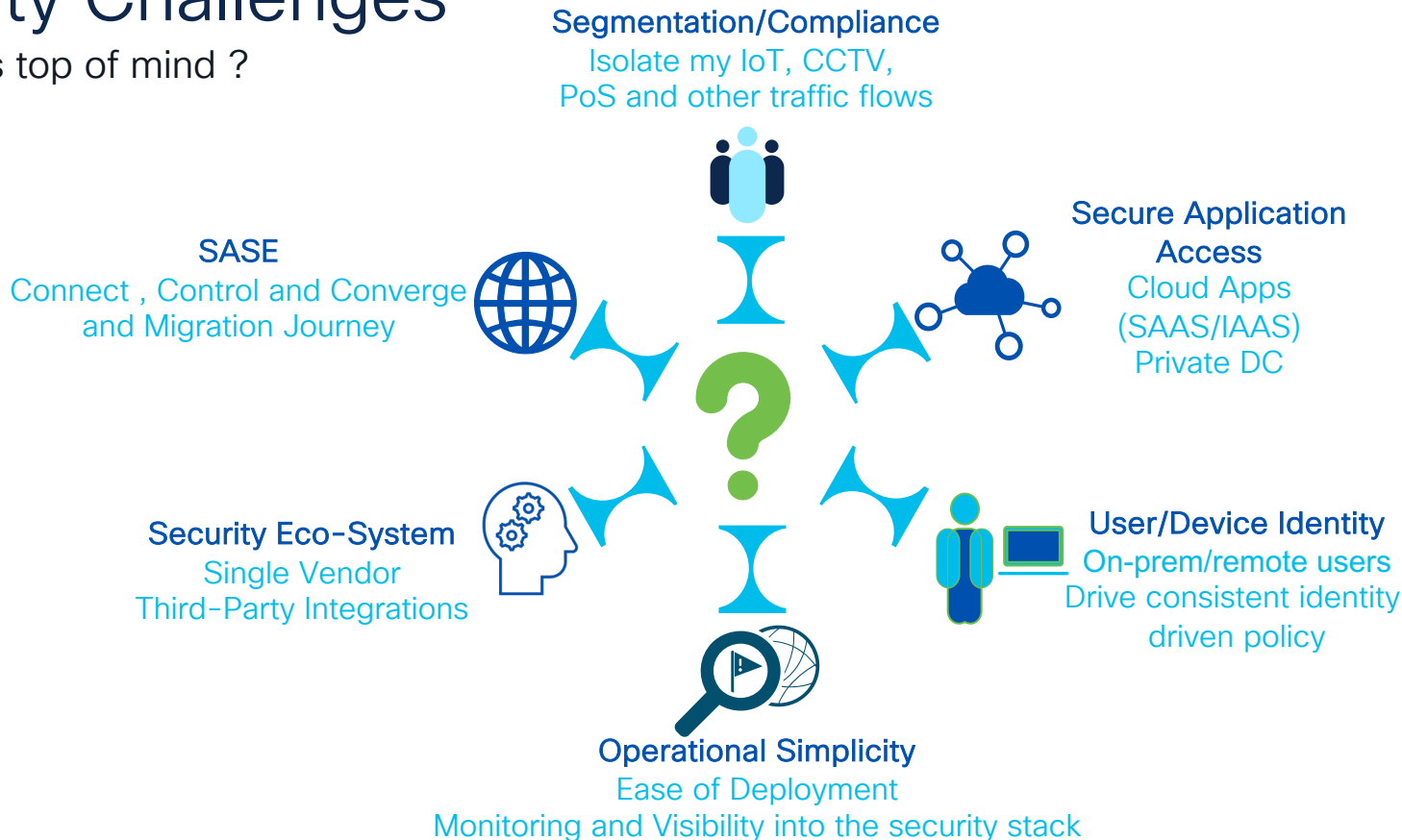
Higher C8K
Dataplane
Performance



C8500-
20X6C

Security Challenges

What's top of mind ?



Key Message

By the end of this session, you will get a holistic understanding about Cisco Catalyst SD-WAN's security capabilities and features, whether you are looking for Integrated security or SASE, you will be able to apply this knowledge for your organizations or clients.

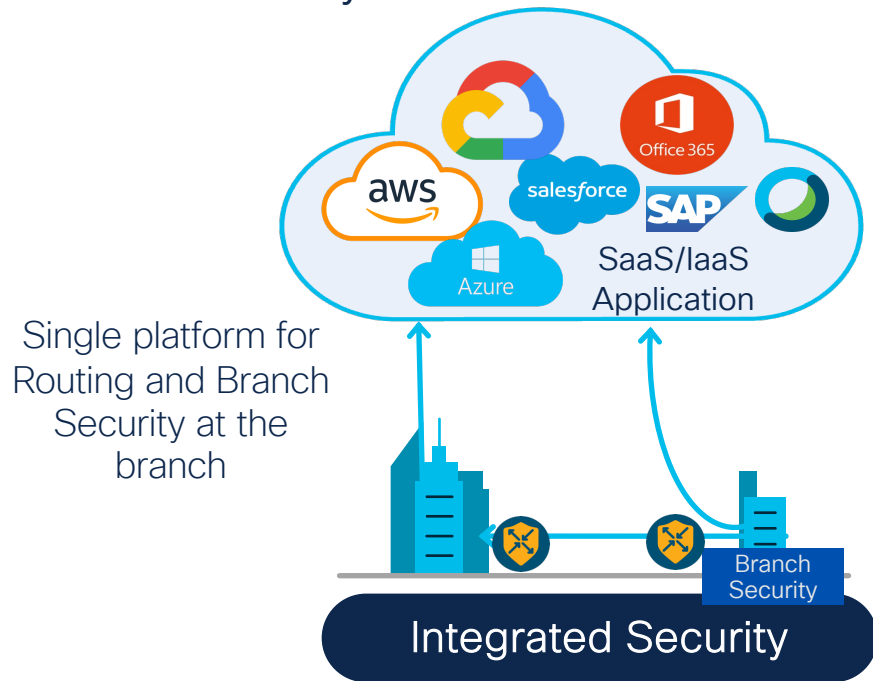
Think Secure WAN, Think about Cisco Catalyst SD-WAN

Agenda

- Section 1 : Integrated Security
 - A look at current capabilities
 - What's New ?
- Section 2 : SASE
 - A look at current capabilities
 - What's New ?
- Demo

Cisco Catalyst SD-WAN Security Models

Flexible Security based on customer needs



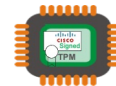
Encrypted
Tunnels



TLS control
plane



Fabric Security



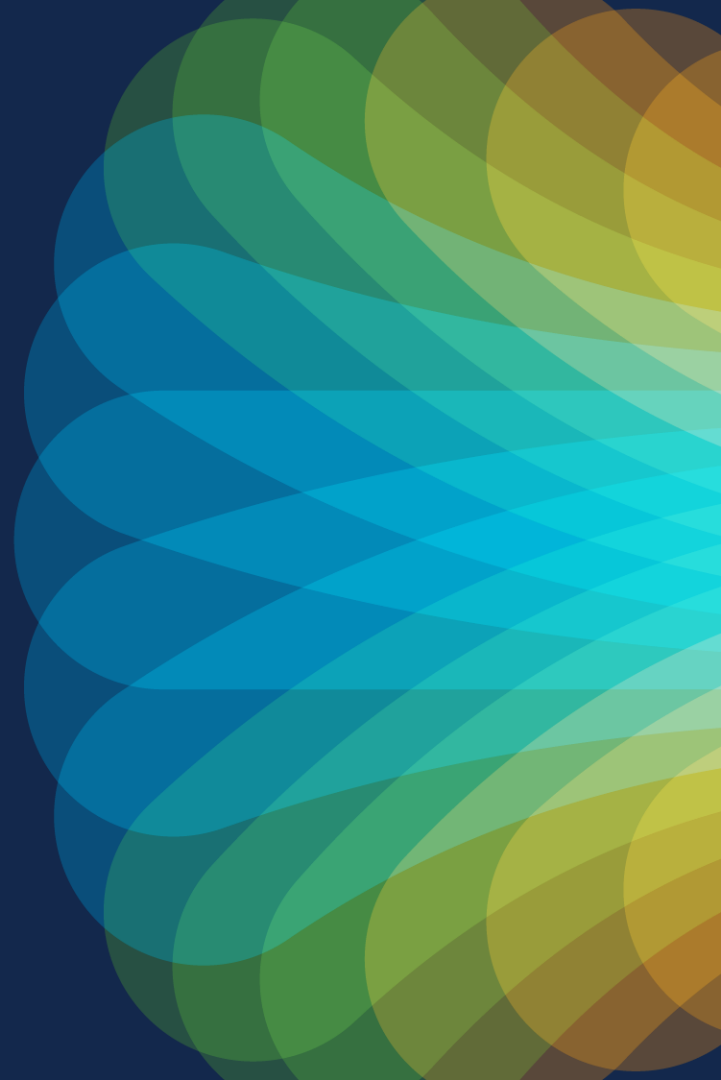
Embedded
Certs



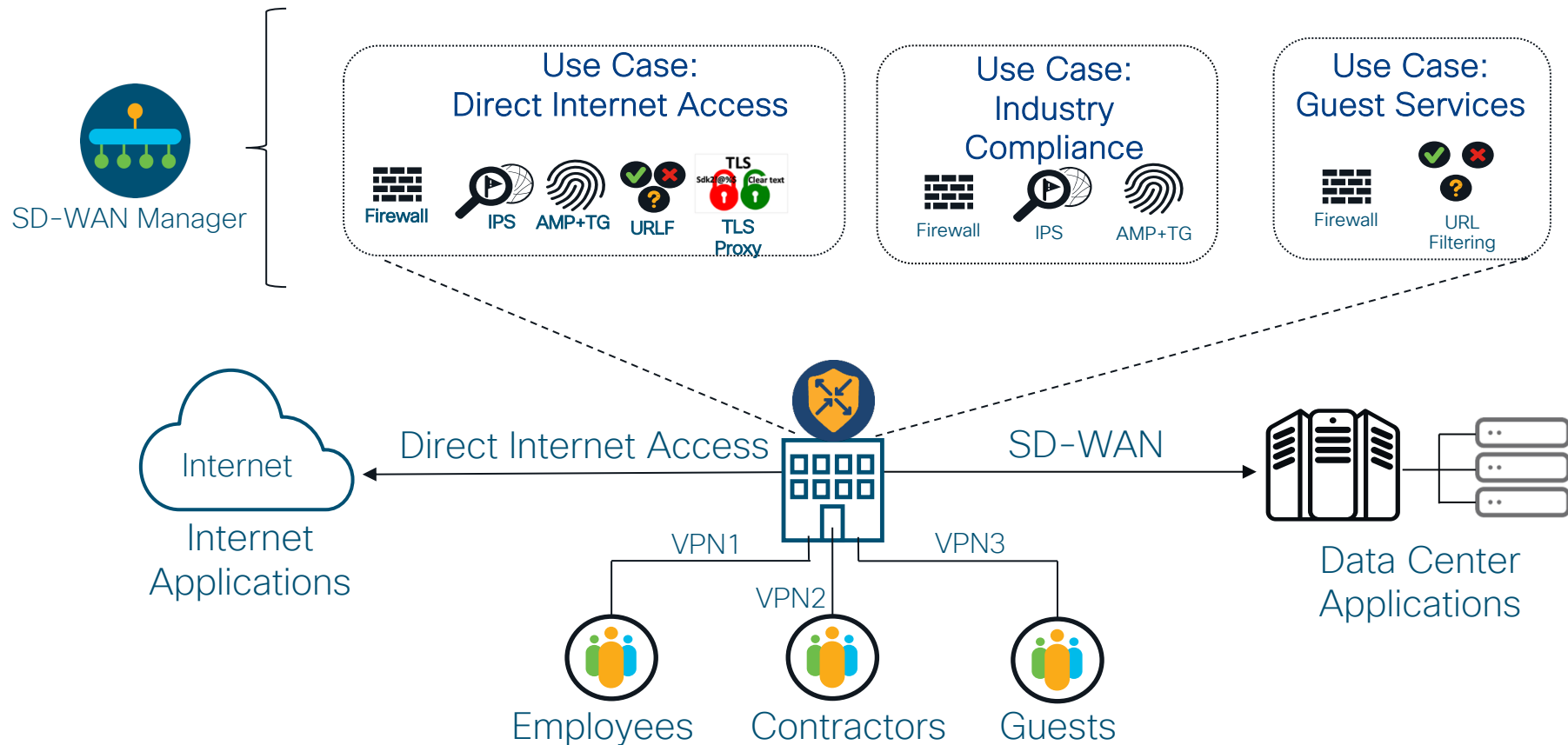
Segmentation

Section1 :

Cisco Catalyst SD-WAN Integrated Security

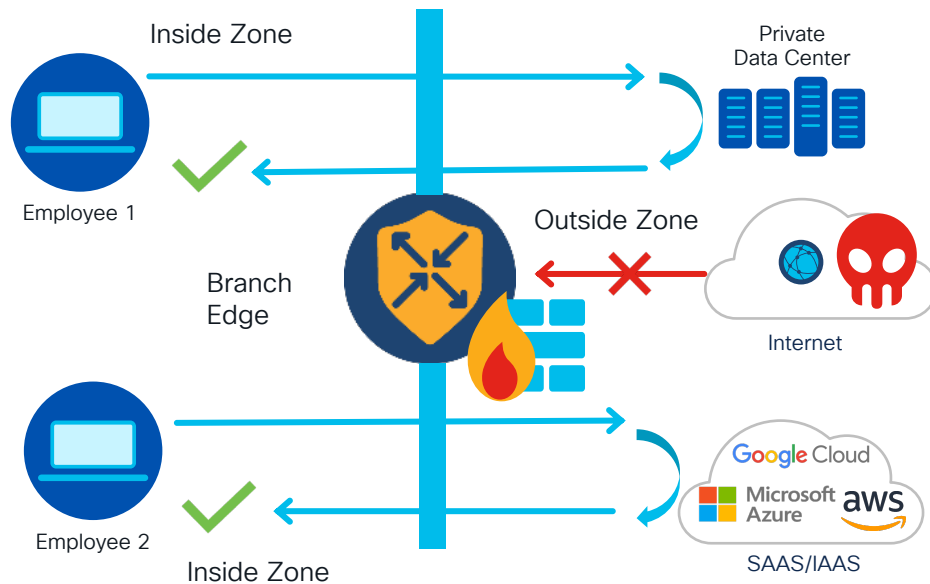


SD-WAN Security Use Cases

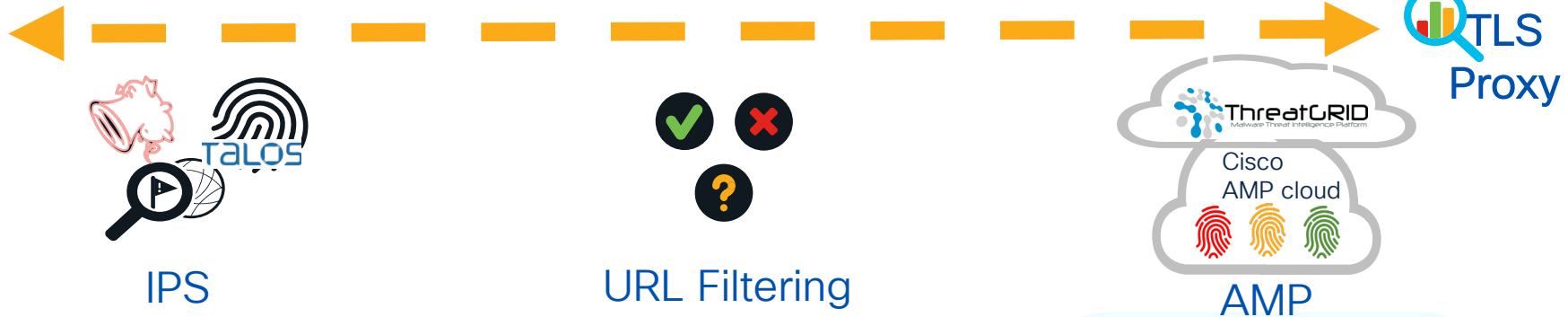


Cisco Enterprise Firewall with App-awareness

- Stateful Zone based Firewall
- Object-groups/Rules/Rules-set/variable support
- App-aware using NBAR2 (Layer 3-7 visibility)
- ALG support (FTP,SIP etc)
- VPNs (VRFs) / Interfaces as Zones
- Self-Zones/Default-Zones
- HSL logging, netflow to multiple collectors
- FQDN Support
- Geo-IP Support
- **IPV6 support* (17.11)**
- Flood attack prevention



Advance Protection Stack



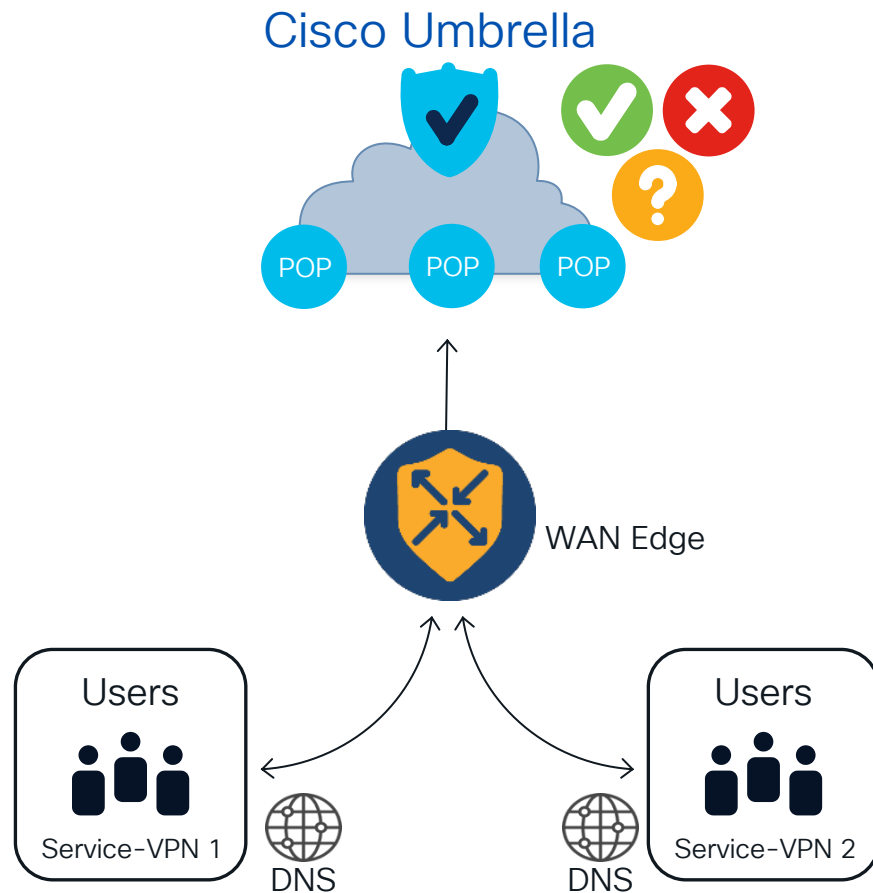
- Detection or Prevention
- **Snort 2.0->3.0 Engine (17.12)**
- Signature Auto-update
- Talos Threat intelligence
- Signature allow-list support
- Security-levels (Conn, Bal, Sec)
- Customize log level

- Enforce Acceptable Use Controls
- Custom regex Allow/Block lists
- Web Reputation score
- Web Categories (82+)
- Redirect or block page
- Customized log types

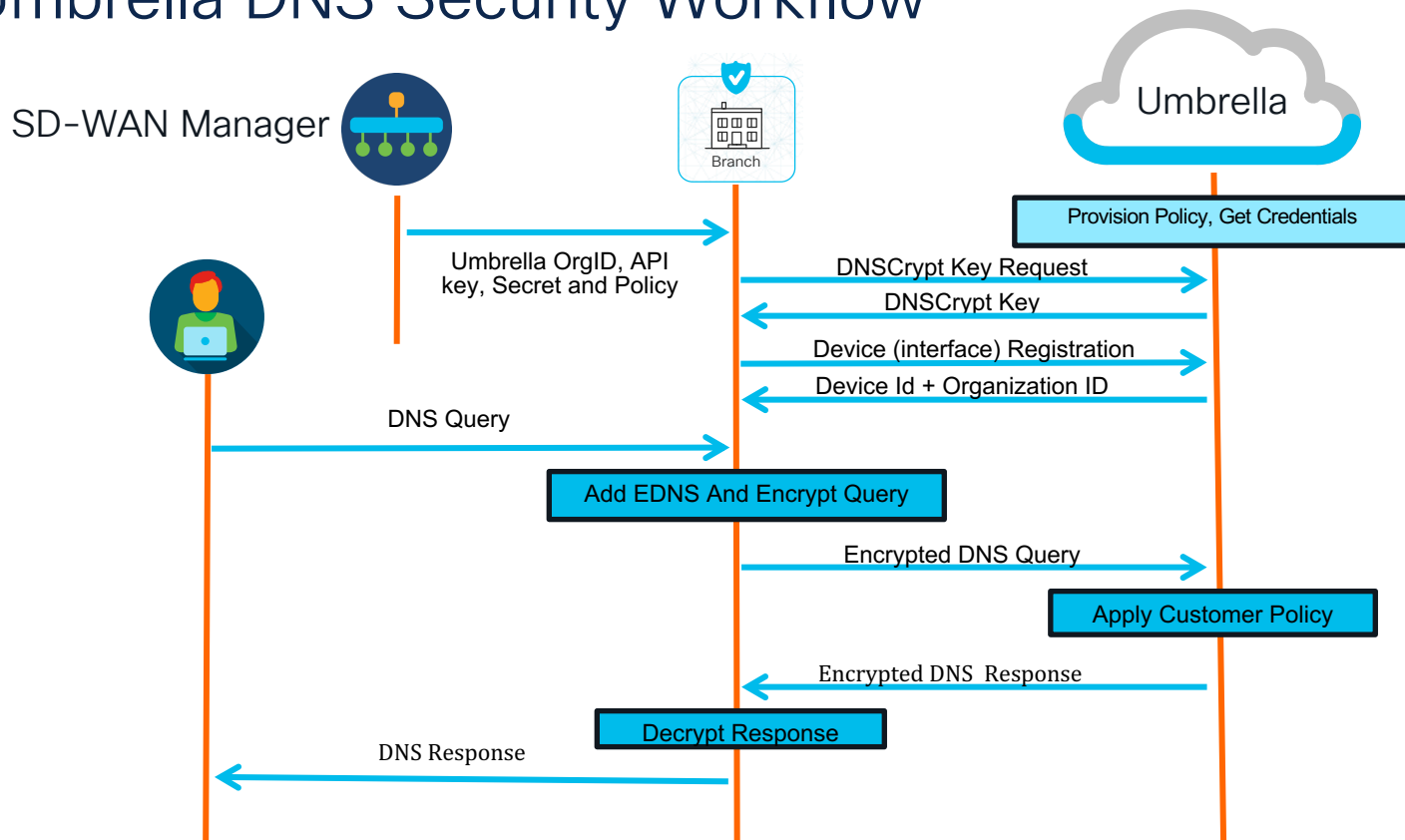
- Integration with AMP Cloud
 - File Reputation
 - File Retrospection
- Integration with Threat Grid
 - File Analysis(sandboxing)
- Customize log level

DNS/Web-layer security

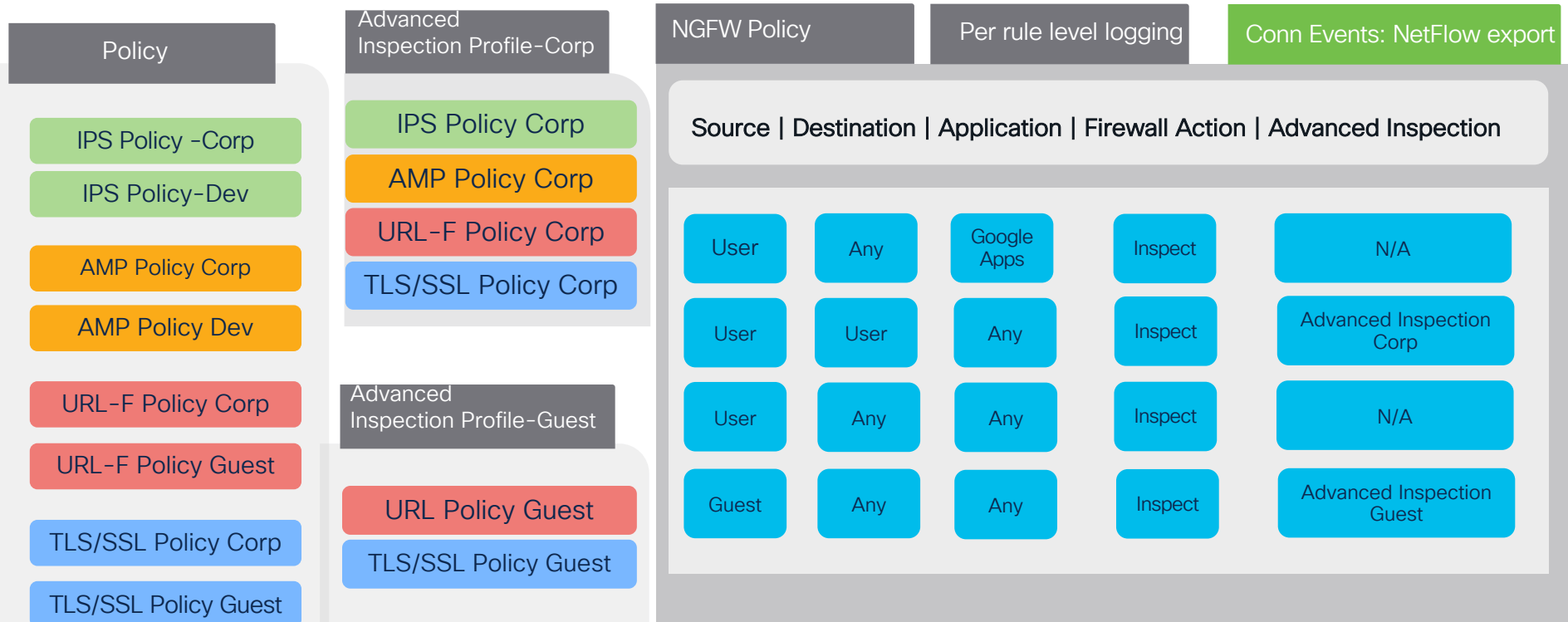
- Cloud-only DNS based inspection
- Automatic API Key registration
- VPN-aware policies
- Global points of presence and anycast IP for fastest response and high availability
- Block malware, phishing, and non-compliance domain requests
- Supports DNSCrypt
- Local Domain-bypass option



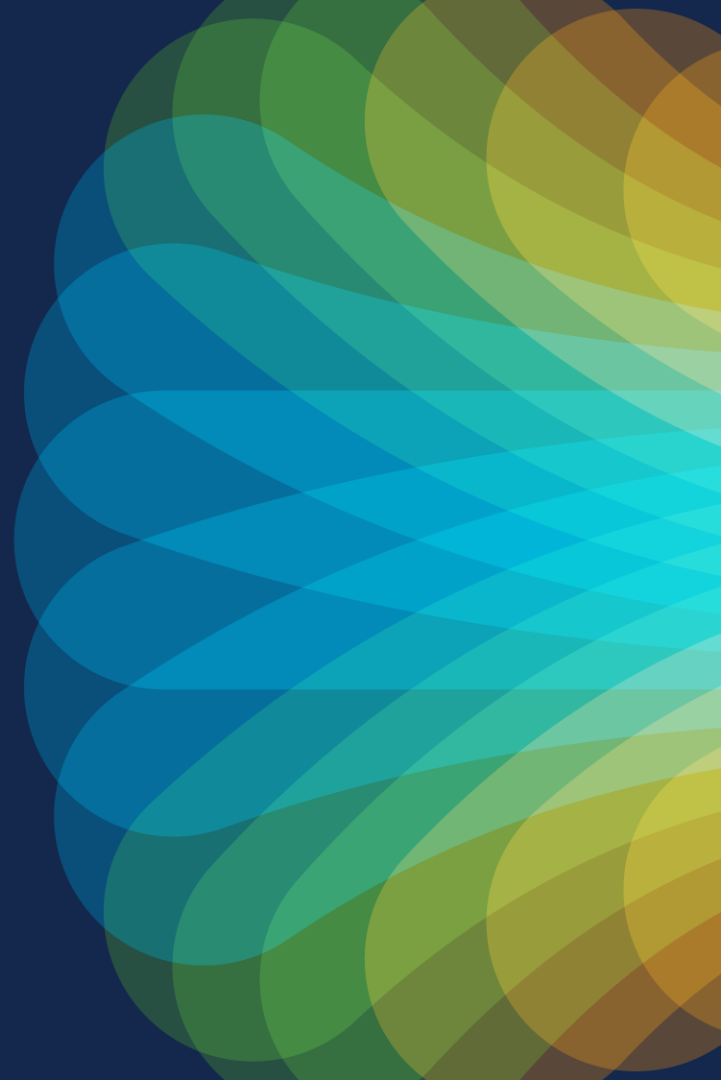
Umbrella DNS Security Workflow



SD-WAN Unified Security Policy and Logging

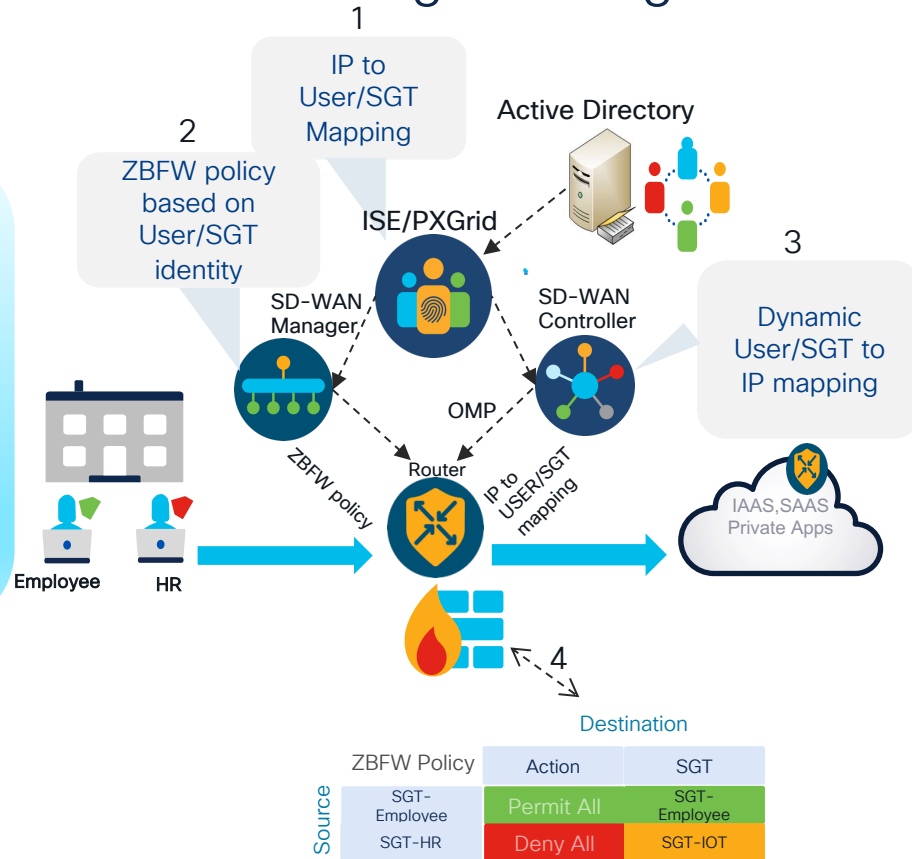


What's New?

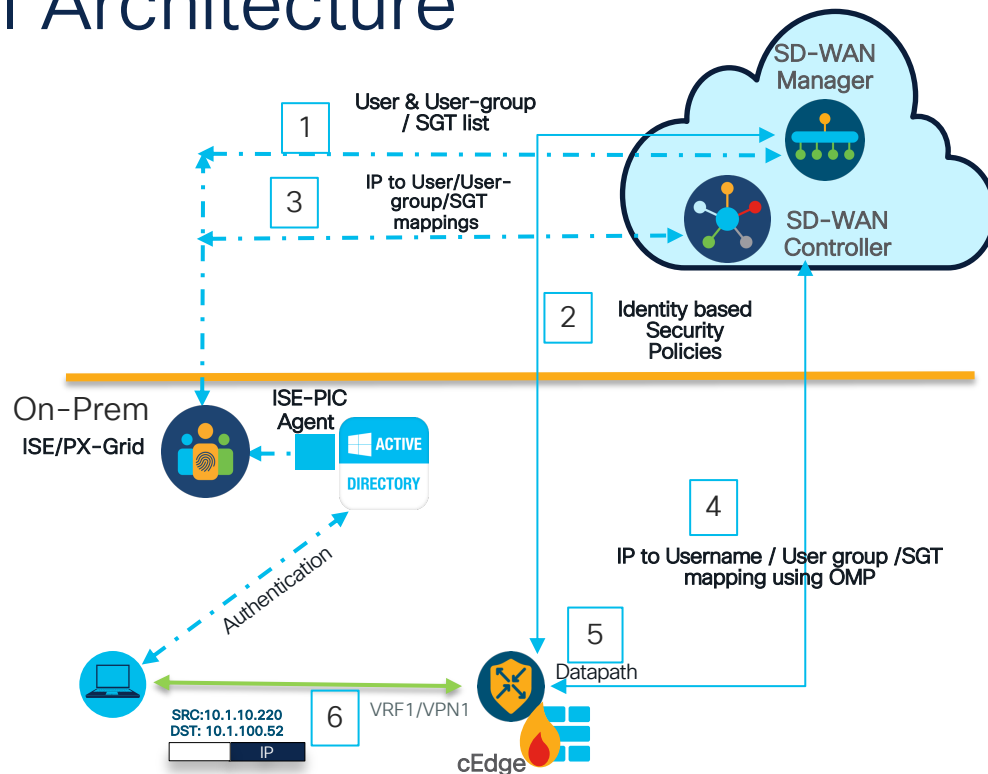


Cisco catalyst SD-WAN Identity-based Firewall using ISE integrations

- Identity as part of Security Policies
- User/User-Group (20.9)
- Security Group Tag (SGT)(20.10)
- Security Compliance throughout the network
- Ease of Configuration



High Level Architecture

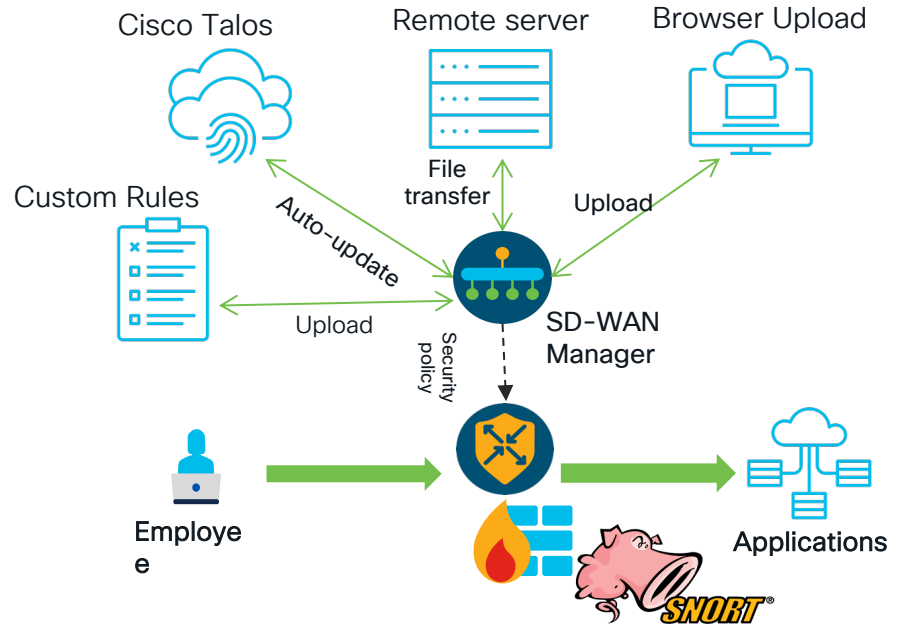


Custom IPS Signature and Offline updates

Starting 20.10/17.10

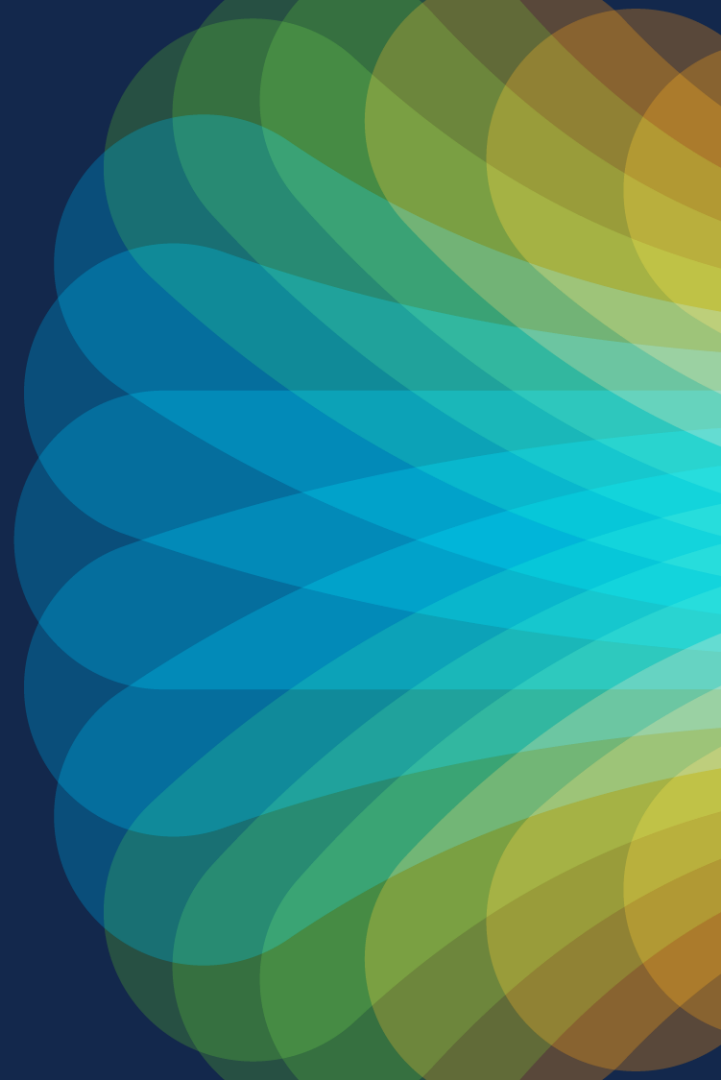
- Design for Air-gapped Network
- Customers can upload signatures packages to SD-WAN Manager using:
 - File upload
 - Remote server (FTP, SCP etc.)
- Ability to upload custom rules for day-2 customization

Operational Simplicity and Enhanced Security
Control for Cisco catalyst SD-WAN NGFW



IPS Policy	
	Match rules
Enterprise App	Allow
Exploit	Deny

Configuration Simplicity And Visibility



Simplified UX for SD-WAN Security Management



Security Policy
Workflow



Simple Navigation



Abstractions of
Objects



Smart Default
policies



User to App
Policies



Dynamic
rules/qualifier

Cisco SD-WAN Select Resource Group Create Security Policy

4 of 5 steps
Test-policy (Total Source Zones: 2)

[Add Sub-Policy](#) [Additional Settings](#)

Source Zone: **Employee** [Add Rule](#) [Delete Sub-Policy](#)

Search Table

Order	Name	Destination Zone	Traffic Source	Traffic Destination	User/User Group	Application	Protocol	Advanced Inspection Profile	Log	Action
1	Internet	Untrusted	Data Prefix: Site2-LAN,Site1-L...	All	All	Productivity	Internet	AMP_IPS_URLF_NGFW	☒	Inspect
2	All-Traffic	Untrusted	All	All	All	All	All	-	☐	Drop

2 Records Items per page: 25 1 - 2 of 2

Source Zone: **Guest** [Add Rule](#) [Delete Sub-Policy](#)

Search Table

Order	Name	Destination Zone	Traffic Source	Traffic Destination	User/User Group	Application	Protocol	Advanced Inspection Profile	Log	Action
1	Rule1	Untrusted	All	All	All	All	All	-	☐	Inspect

[Exit](#) [Next](#)

Streamlining Security Experience:

- Transforming Intent into Action
- Combine multiple security features into one access policy for seamless integration
- Eliminate manual policy configurations

Best-in-Class Security Controls: Elevate Your Protection

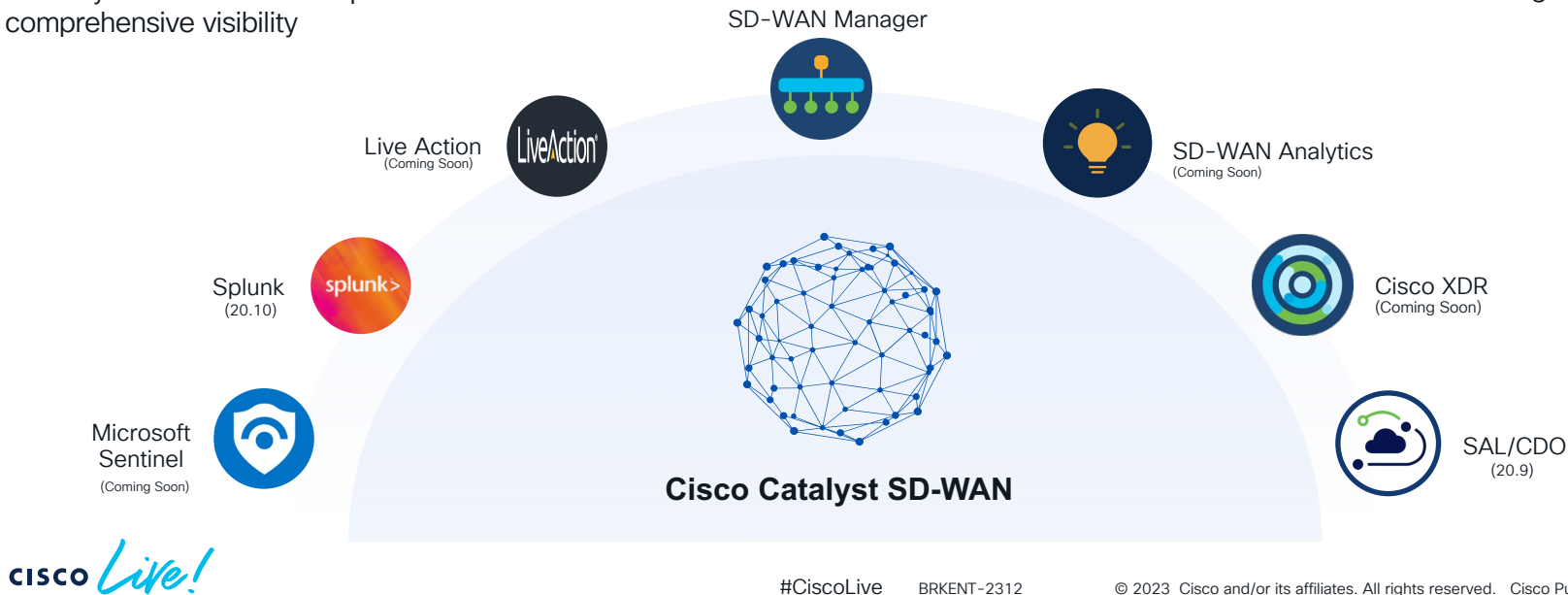
Security – Monitoring & Visibility Ecosystem

Why this Ecosystem?

- ✓ Different market segments with different requirements
- ✓ Security Stack is never complete without comprehensive visibility

Benefits to the Customer

- ✓ Comprehensive security visibility
- ✓ Drill down to device and flow for immediate troubleshooting



Cisco Catalyst SD-WAN Manager Security Dashboard

1

Firewall Rule counter

Overview of top rule hits within network with an ability to drill down to individual device level

2

Top Threats

Overview of the critical threats (IPS/AMP) in the network

3

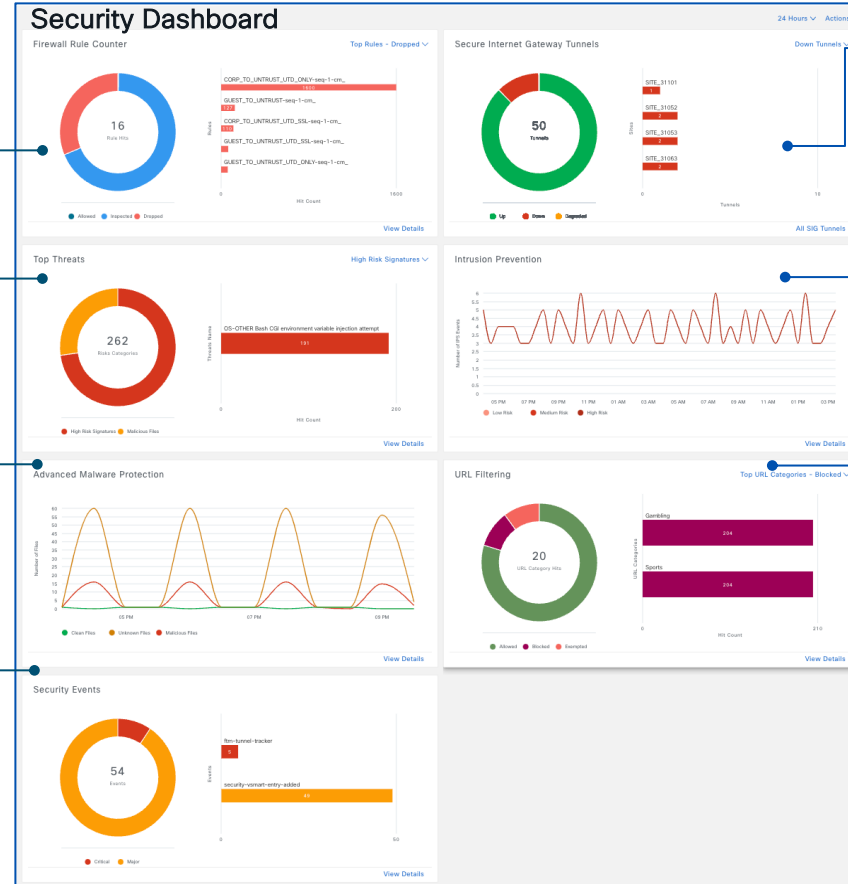
Advanced Malware Protection

Trend of incoming files in the network. Categorized into clean, unknown and malicious

4

Security Events

Displays raw events captured in the network



5

Secure Service Edge (Cisco Catalyst SD-WAN secure internet gateway - SIG)

Provides the status of each SIG tunnel hosted by the SD-WAN routers

6

Intrusion Prevention

Trend of IPS events in the network with an ability to view event details and associated devices

7

URL Filtering

Displays web categories accessed by the user

Customers can customize the dash-let on this security dashboard

Cisco Catalyst SD-WAN / Splunk Integration - Use Cases

SoC Dashboard

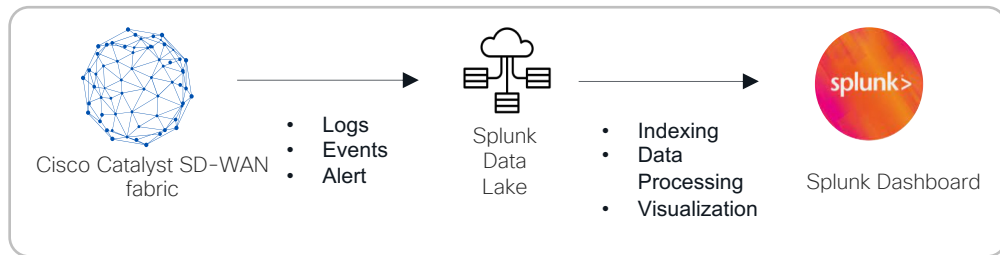
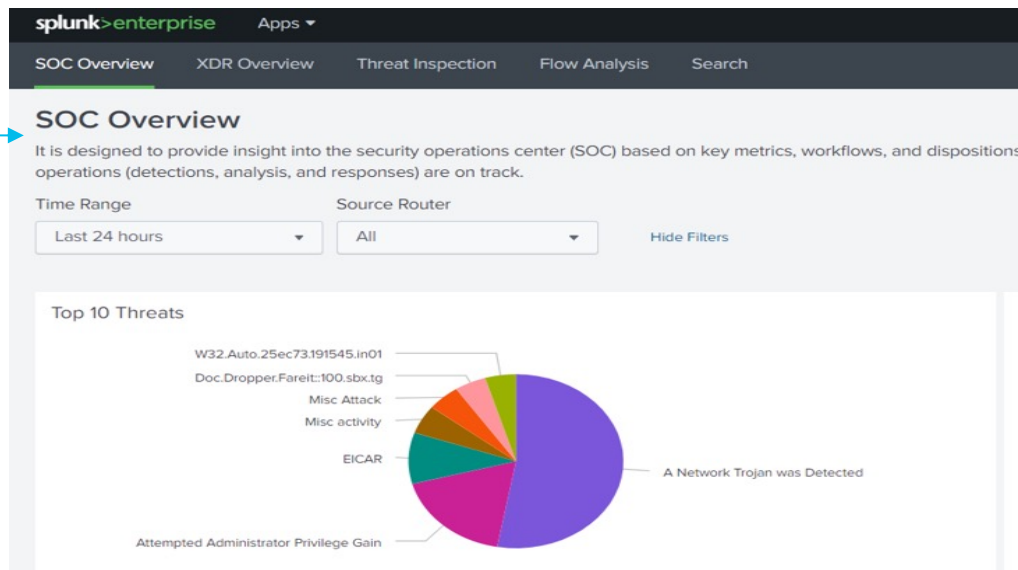
- Holistic view of all security events
 - Top Threats & Policy Hits
 - Overall Application Traffic
- Drill down to device level from any security widget (user/sgt)

Threat Management

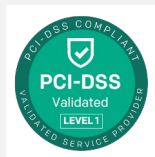
- List all IPS events in the network
- List all Malware events in the network
- View which devices are impacted by threat events

Flow Analysis

- View device network patterns
- Top applications accessed
- Top website domains visited
- Generate reports



Cisco Catalyst SD-WAN Certifications



PCI-DSS

Securing SD-WAN infrastructure and simplifying customer journey to compliance

20.6 and 20.9



SOC2/SOC3

Validates following controls with-in trust services criteria (TSC)

Security, Availability, Processing Integrity, Confidentiality and Privacy

20.6 and 20.9



FIPS 140-2

Validation of the Approved Cryptographic algorithms for SD-WAN

[SD-WAN Manager/SD-WAN Validator/SD-WAN Controller/vEdge]

20.6 and 20.9



FedRAMP*

Uniform evaluation and authorization of cloud information security controls for federal agencies utilizing SD-WAN

20.9



ISO

International Standards to manage information security Governance risk, Security Technique, Protection of Privacy, and Protection of PII

20.11



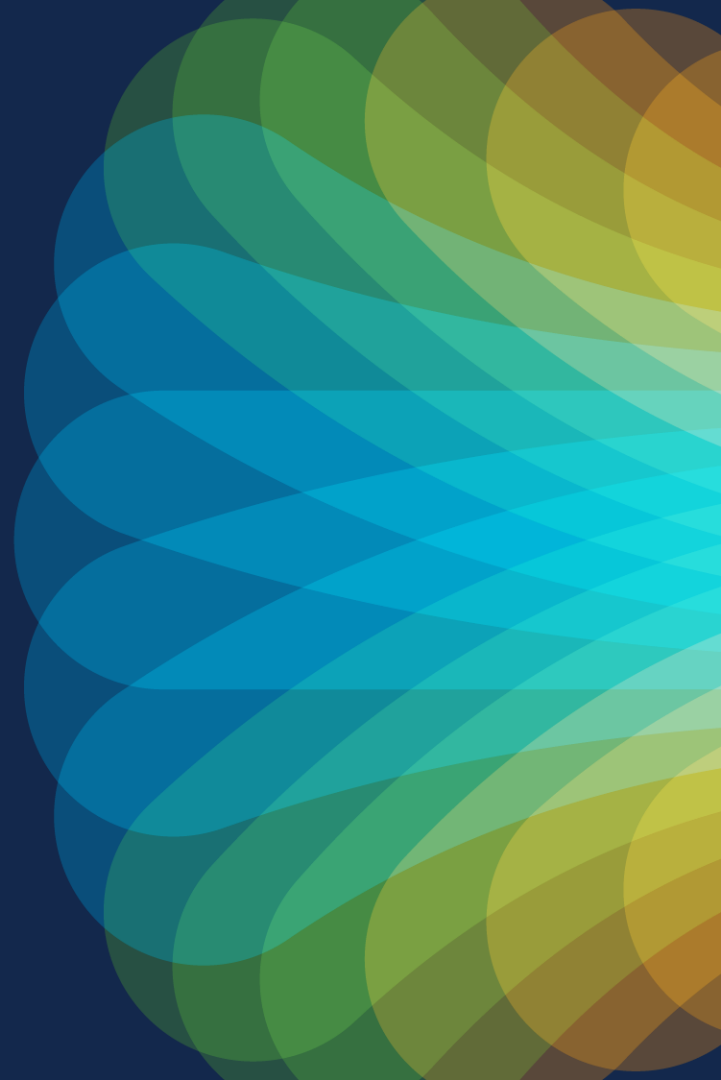
C5

Evaluation of operational security against cyber-attacks when using cloud services within the context of German Government's Security recommendations for SD-WAN

20.11

Certified overlays are limited to controllers purchased via certified controller SKUs

Section 2 :SASE



SASE Solution Your Way...

Unified SASE



Cisco+ Secure Connect

Unified solution on converged platform with turnkey operations



Integrated SASE

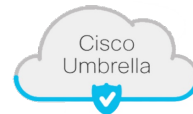


SASE A-la-carte

Build-your-own SASE approach



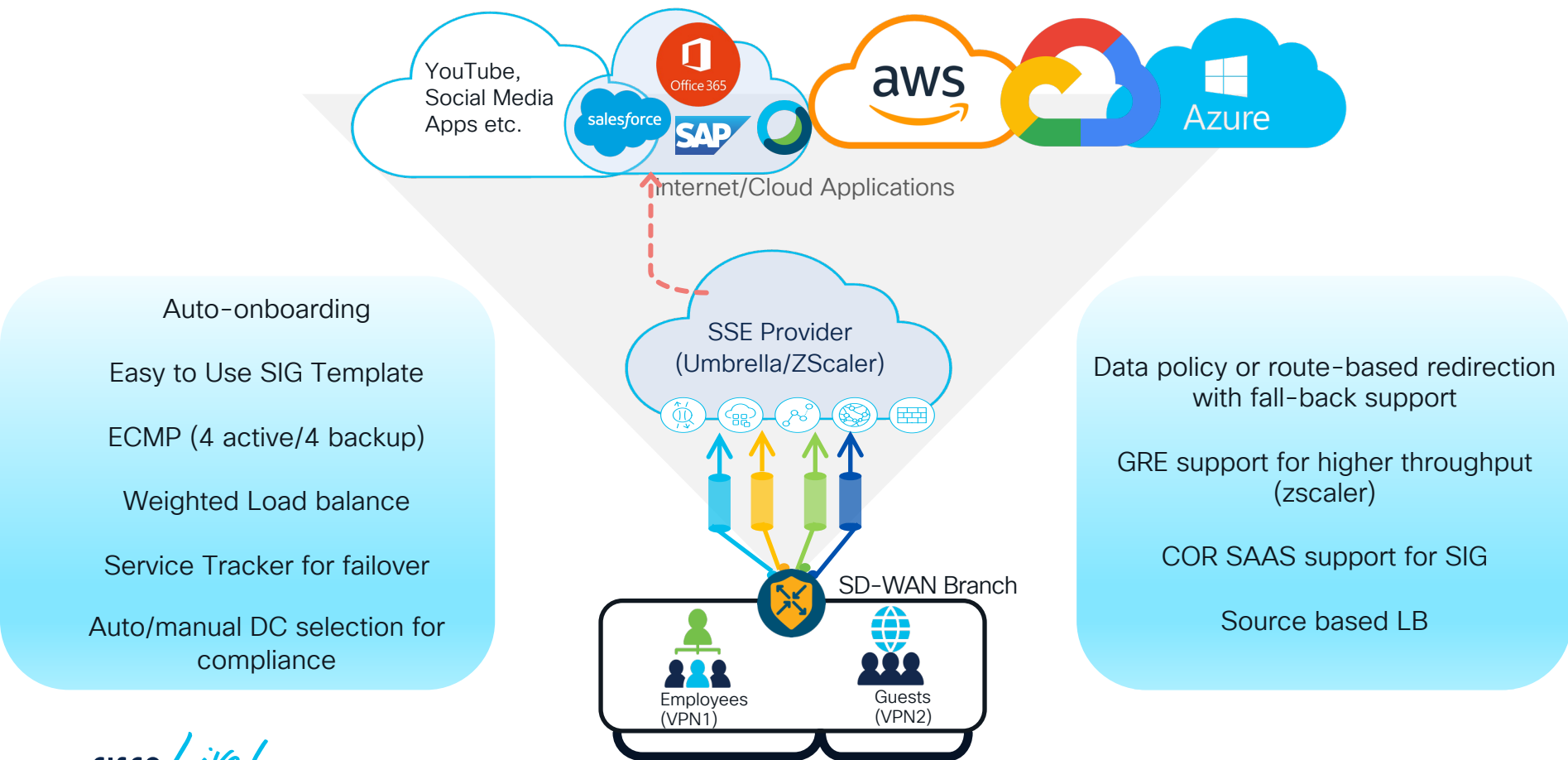
+



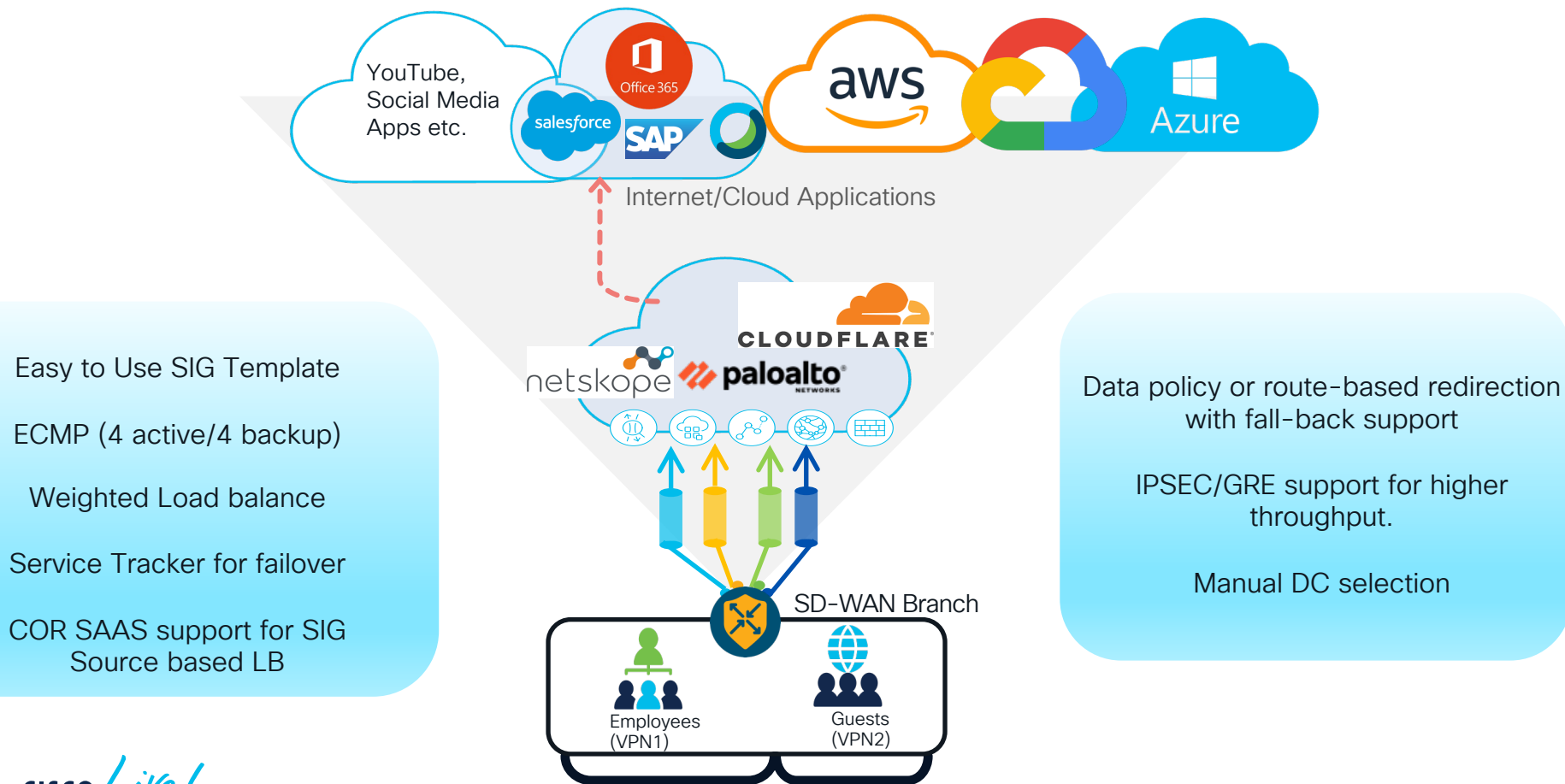
Cisco Catalyst SD-WAN

Cloud Security (SSE) Vendors

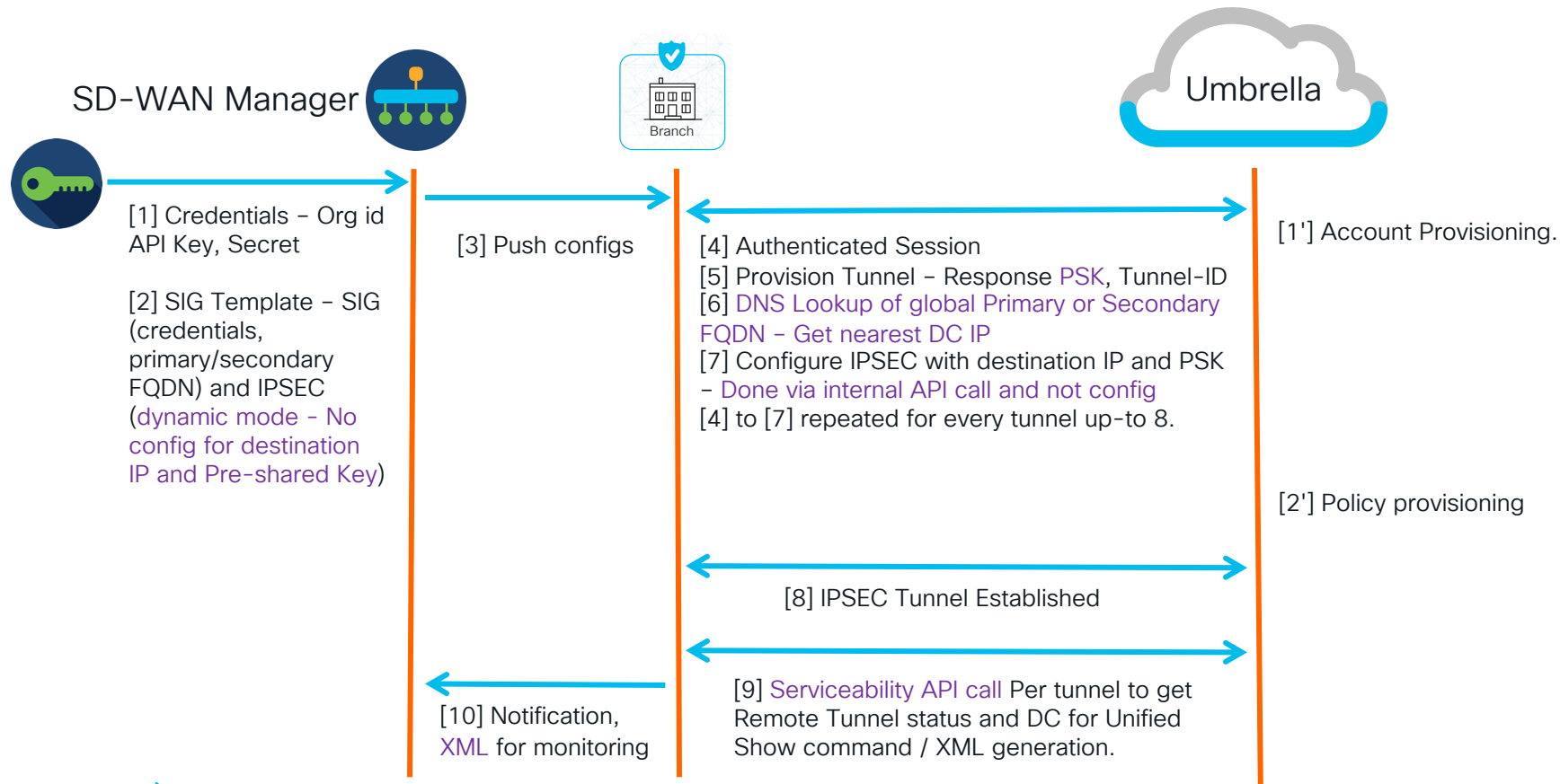
SD-WAN - Auto SIG Capabilities



SD-WAN - SIG Capabilities - Manual



SD-WAN / Umbrella - Auto Tunnel Provisioning



Tunnel Monitoring Fields

- 1) Tunnel id
- 2) Tunnel name
- 3) Tunnel Status – Local & remote
- 4) Type of ha-pair (Active/Backup)
- 5) SIG Provider
- 6) Destination Data Center
- 7) Transport Type – IPSec / GRE
- 8) Events/Notifications
- 9) Tracker
- 10) Site ID
- 11) Host Name
- 12) Packets In/Out (Local device)

Cisco vManage Select Resource Group Monitor · Tunnels

Overview Devices **Tunnels** Security VPN Logs Multicloud

SD-WAN Tunnels SIG Tunnels

24 Hours

SIG Tunnels (4) [Export](#)

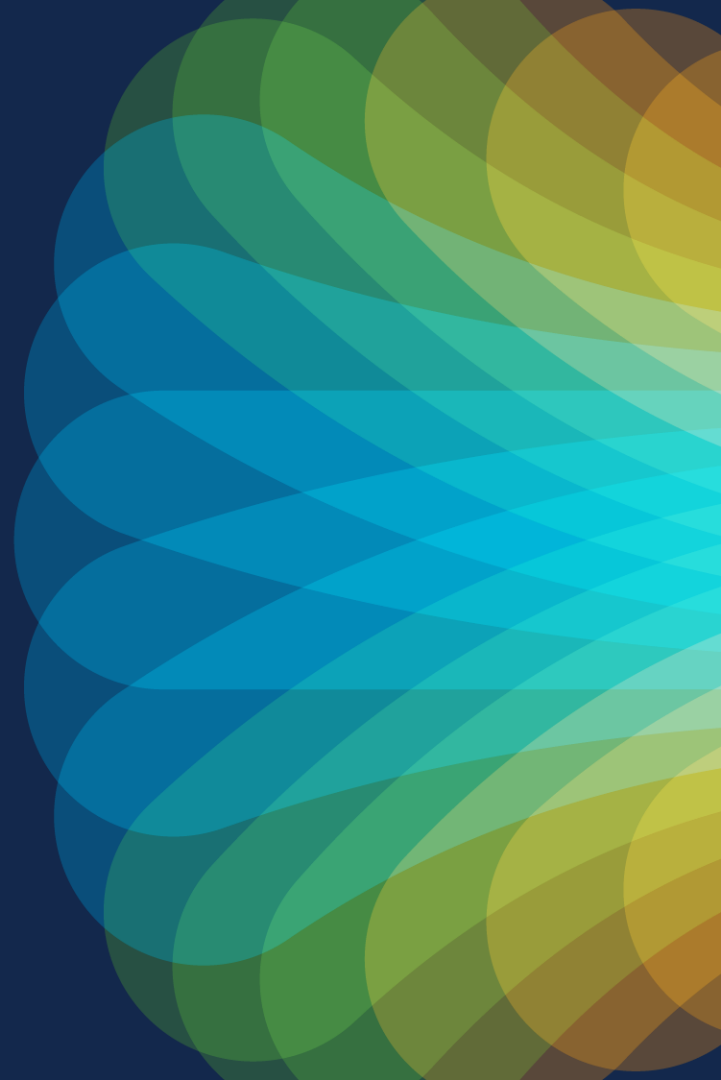
Search Table

As of: Sep 12, 2022 05:49 PM

Host Name	Site ID	Tunnel ID	Transport Type	Tunnel Name	HA Pair	Provider	Destination Data Center	Tunnel Status(Local)	Tunnel Status(Remote)	Events	Tracker	Packets In/Out (Local Device)
R2-ER3-C8Kv	3	74340	GRE	173.37.56.165_Tunnel100512	Active	zScaler	NA	Up	NA	14	Enabled	654 / 879
R1-ER2-12X	2	0	IPsec	SITE2SYS2x2x21IFTunnel100001	Active	Umbrella	-	-	-	0	Enabled	0 / 0
BR2-4331-E2	-	0	-	SITE2SYS2x2x22IFTunnel100001	-	-	-	-	-	0	-	0 / 0
R1-ER1-C8Kv	1	11257756	IPsec	site1sys1x1x11IFTunnel100001	Active	zScaler	NA	Up	NA	30	Enabled	12808 / 17782

Items per page: 25 1 - 4 of 4

What's New

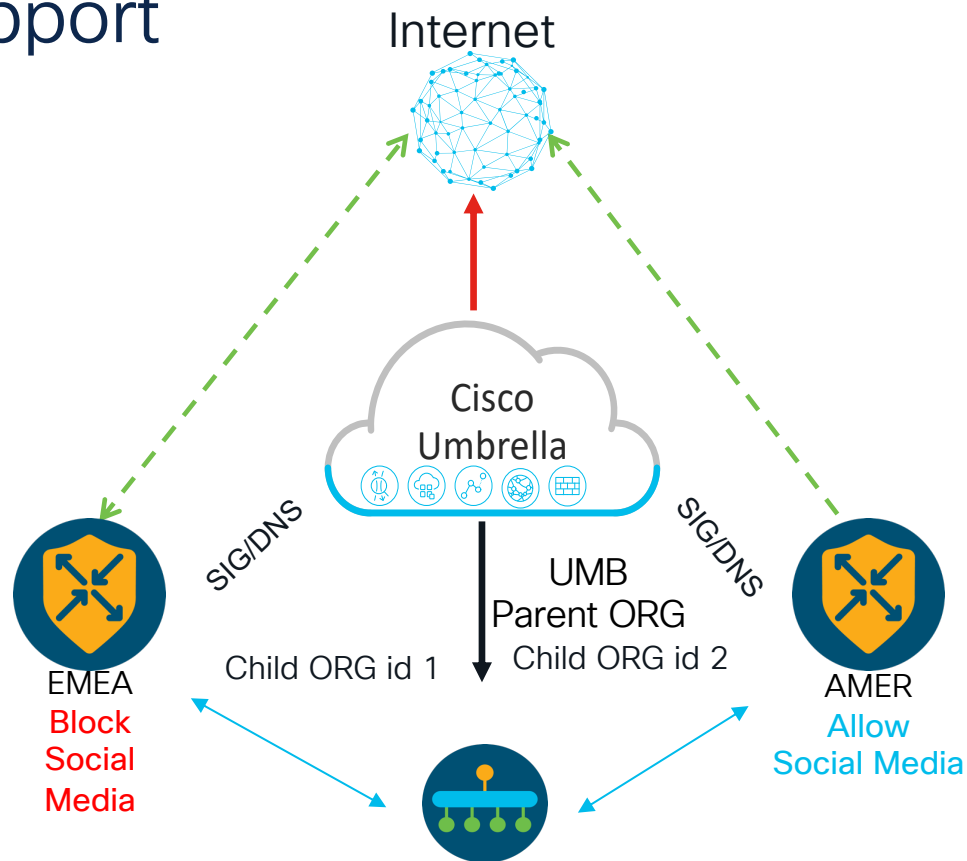


Umbrella Multi-ORG support

20.11/17.11 Cisco vManage –Umbrella Integration:

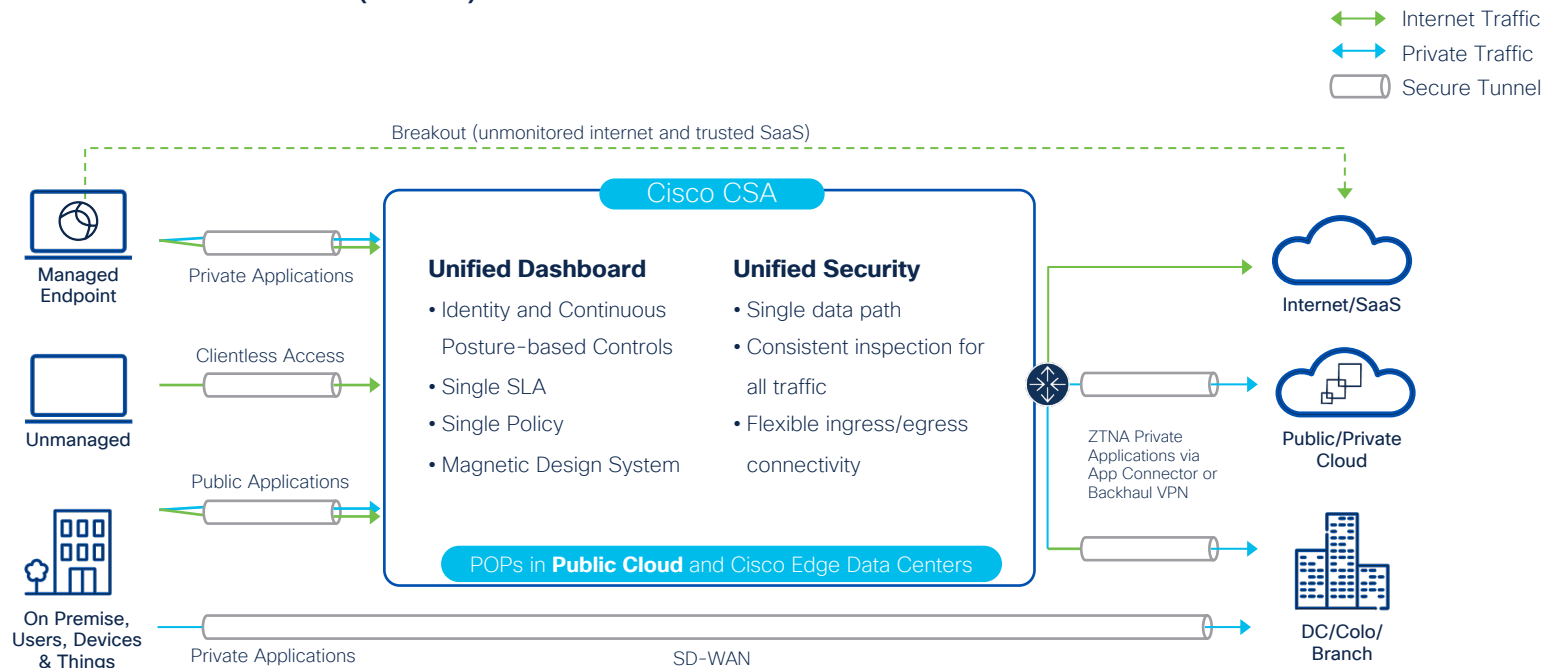
- Ability to select multiple child org
- Simple integration using parent org id
- SIG tunnel support
- DNS Security

Flexibility to deploy distributed cloud security enforcement policies and compliance



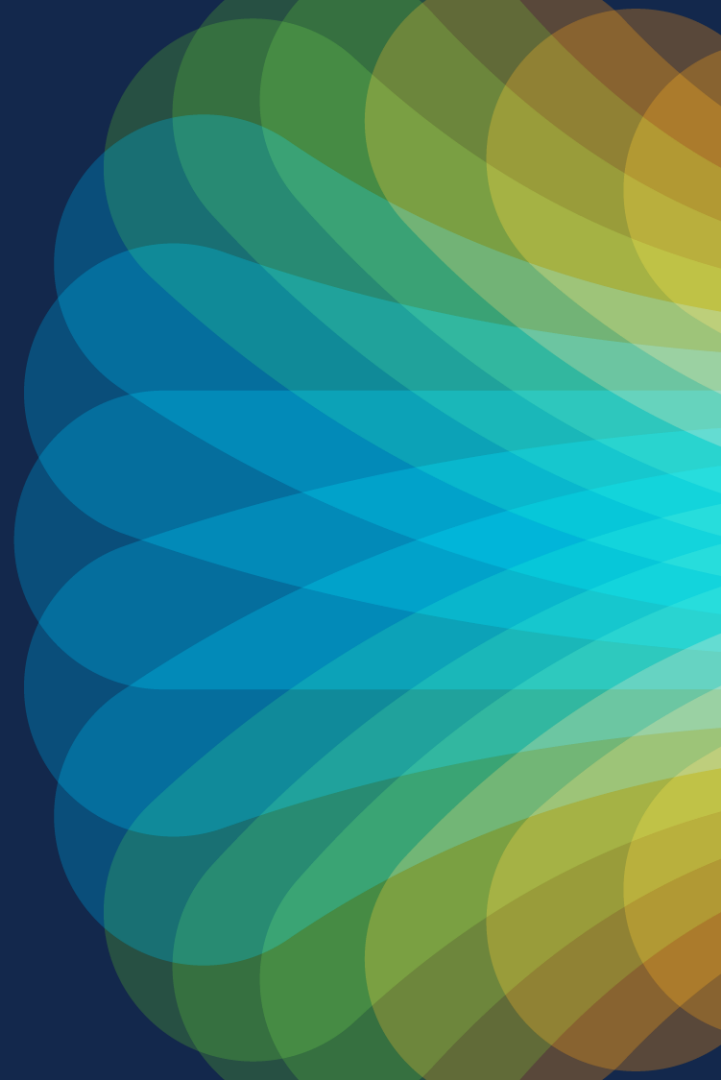
Architecture Overview

Cisco Secure Access (CSA)



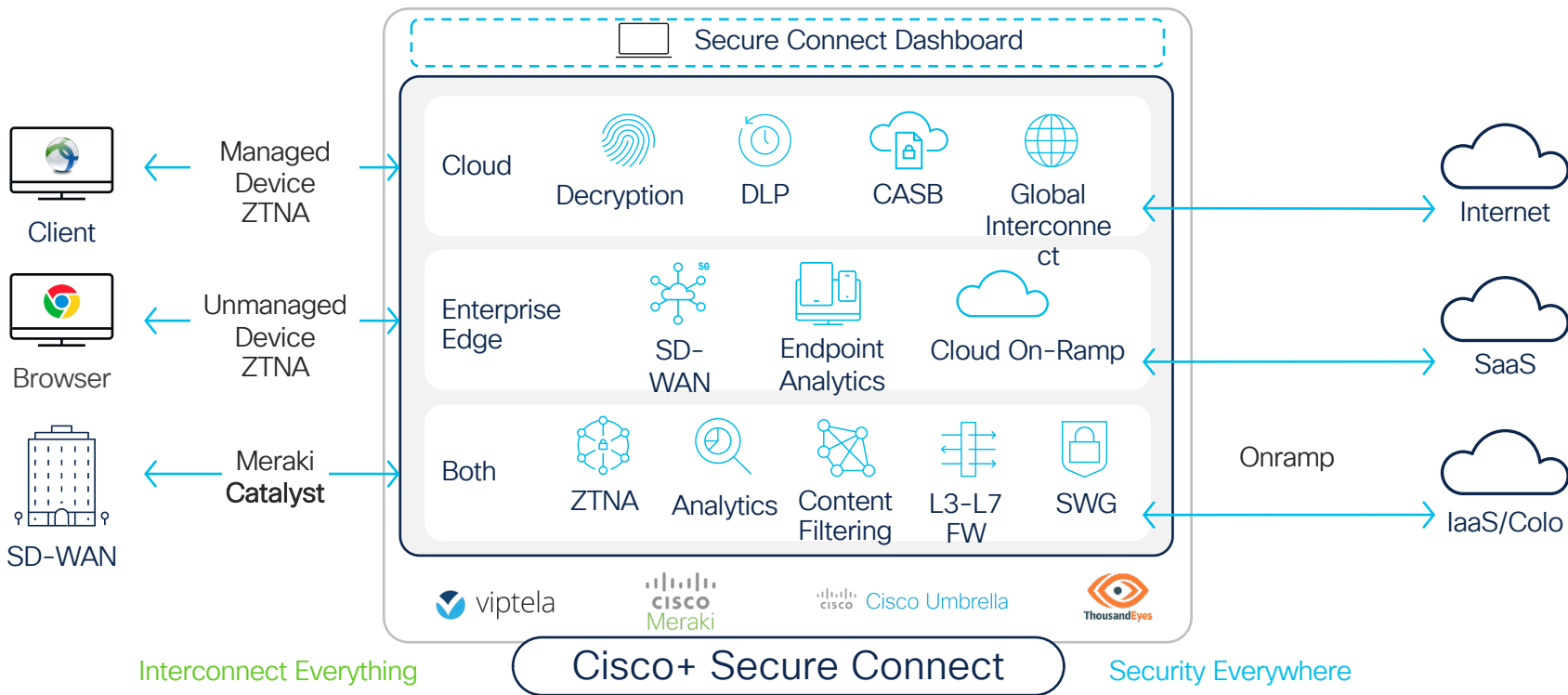
Who How What

Unified SASE



Unified SASE

Centralized Management, Distributed Enforcement



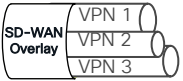
Demo UX 2.0 Security Policies and Dashboard

Key Take-away

Embedded Security




Next-Gen Firewall
Stateful & App-aware NGFW
IPv6 support


Segmentation
Micro & Macro Segmentation


AMP (by Talos)
File Reputation


Threat Grid Sandboxing
Unknown file to Malicious file scan


IPS (Snort)
Protection against complex threats


Unified Policy
Single simplified workflow to apply security


URL F
Category & Reputation score


Zero Trust
Protection extended with Identity & Security Tags

SD-WAN Integration with Cloud Security (SSE)




Tunnel


Umbrella Automation


Simplified Configuration


Layer-7 Health Check


Traffic Load Balancing


Active Standby Tunnel


Multi-Tunnel support

Cisco Integration



3rd Party Integration



Fabric Security




Encrypted
Control Plane


HW Based
Device Authentication (SUDI)


Encrypted
Data Plane


Enhanced Security
Pairwise keys

Certification & Compliance

Commercial

PCI-DSS, SOC2/SOC3, C5
ISO27001, 27017, 27018, 27701

Federal

FedRAMP Moderate* (Pending PMO review),
FIPS 140-2

Monitoring & Visibility


SD-WAN Manager
SecOps Dashboard


Microsoft Sentinel
splunk > **LiveAction**

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session and the overall event surveys to claim a Cisco Live merchandise.

Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert 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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive

The background is a vibrant, abstract graphic. It features a series of overlapping, wavy bands of color in a rainbow spectrum, transitioning from red and orange on the left to yellow and green on the right. On the right side, there is a bright, multi-colored sunburst or starburst effect that radiates outwards, creating a sense of energy and movement. The overall composition is dynamic and celebratory.

cisco *Live!*

Let's go

#CiscoLive