The bridge to possible

SASE, SSE, and Zero Trust

Anthony Sabella, Principal Architect, CCIE #5374
Enterprise Office of CTO

BRKENT-2002

Cisco Webex App

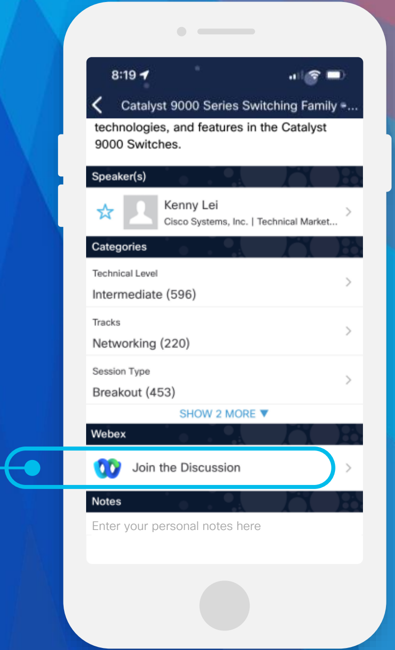
Questions?

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 9, 2023.



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

☆ Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

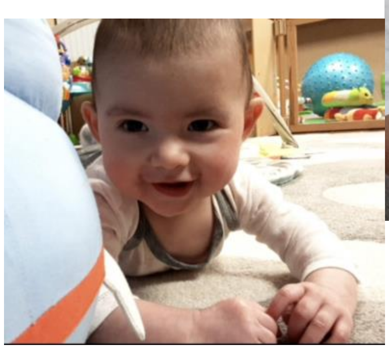
Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-2002

About the Presenter

- Principal Architect for Cisco Systems - Enterprise Office of the CTO
- Specialize in IT transformation strategies (global security & networking)
- Authored several white papers & Cisco/Pearson press “Orchestrating and Automating Security for the Internet of Things”
- Married with 10-month-old daughter



ANSABELL@CISCO.COM

Agenda

- SSE – solution, capabilities, use cases
- SASE – solution, capabilities, use cases
- What is Zero Trust and how it applies to SSE and SASE
- Side by side comparison and when to use/choose each

- Technologies included: FW/IPS, SWG, CASB, DLP, ZTA, ZTNA, SD-WAN, underlay transport technologies, middle-mile optimization, and direct-peering techniques.
- Will not cover: Cisco product roadmap timelines, licensing, pricing
- Housekeeping: Kept 10-15 minutes open at the end for dedicated in-person Q/A

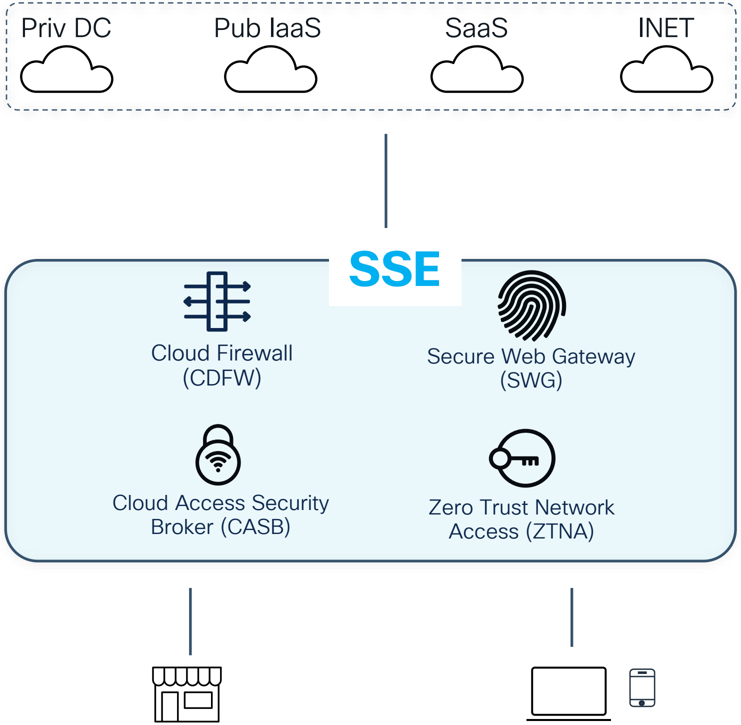
SSE

Gartner

Security service edge (SSE) secures access to the web, cloud services and private applications.

SSE is primarily delivered as a cloud-based service, and may include on-premises or agent-based components.

Typically comprised of firewall, web gateway, cloud access security broker, and ZTNA technologies.



*By 2025, **80%** of organizations seeking to procure SSE-related security services will purchase a **consolidated** SSE solution, rather than stand-alone cloud access security broker, secure web gateway and ZTNA offerings, up from **15%** in 2021.*

Gartner

- *Critical Capabilities for Security Services Edge*

Introducing Cisco Secure Access

SSE Solution (Converged cloud-native security)

Protection for on/off network

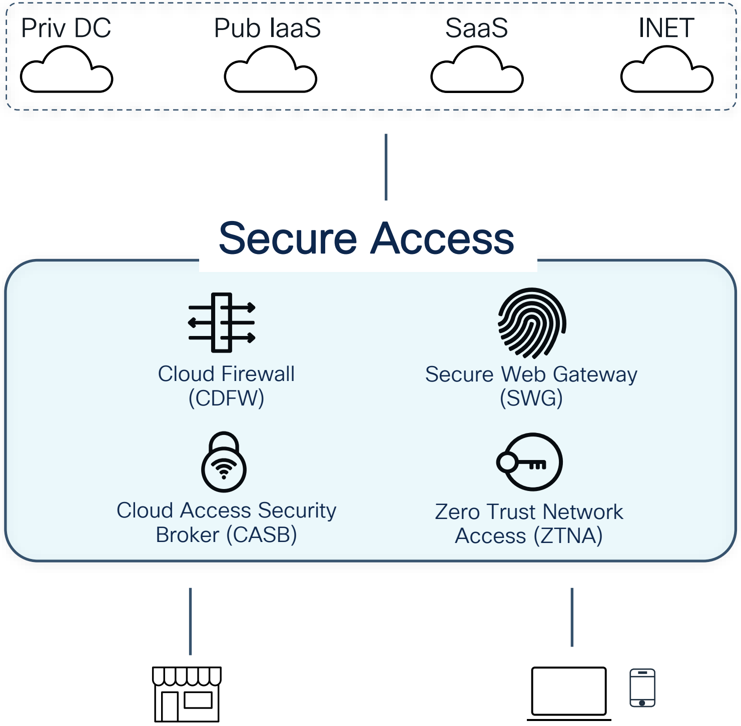
Protect users, applications and resources on or off the network, including contractors/vendors

Simplify Operations

Simplify operations by consolidating security capabilities into one cloud-based tool

Zero Trust

Ensuring zero trust principles with granular controls based on user, device, location, and application



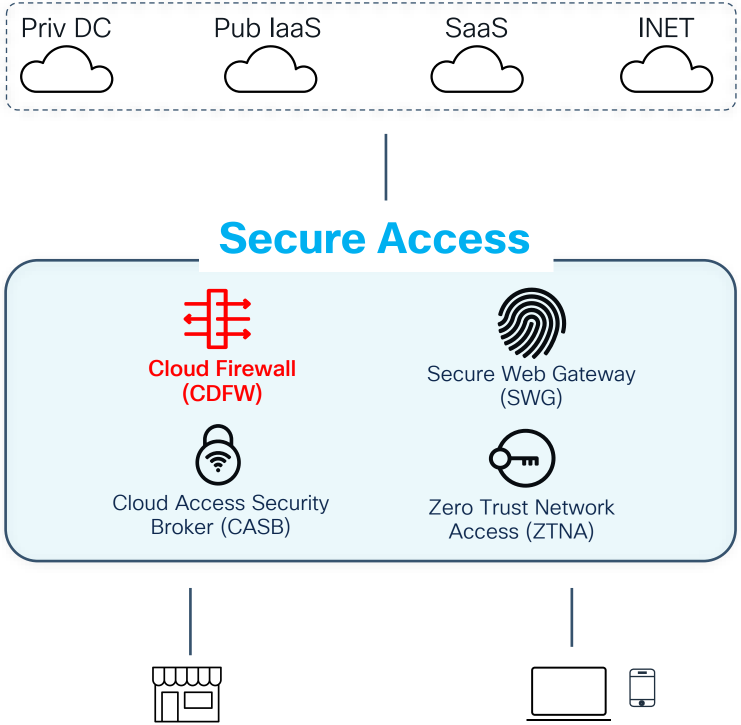
Cisco Secure Access Capabilities

(SSE)

Secure Access (SSE)

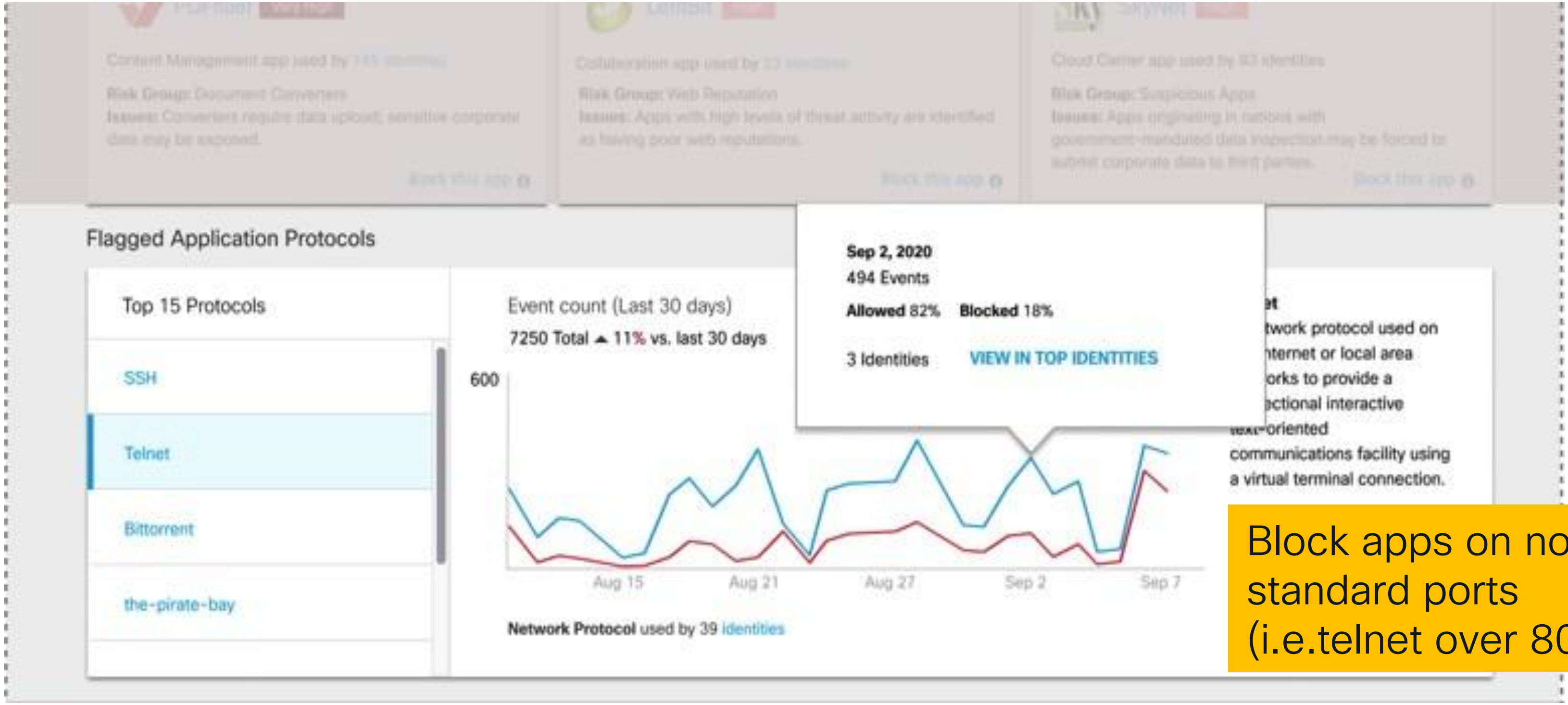
Cloud Firewall

- Port / Protocol Blocking
- Layer 7 Application Control
- IDS / IPS (Snort)
- All tunneled traffic hits **CDFW** first
- Identities: Tunnel, AD group, AD user (supports AD integration with SAML)



Cloud Firewall L7 App Discovery

Provides insight into all apps being used



Content Management app used by 145 identities

Risk Group: Document Converters
Issues: Converters require data upload; sensitive corporate data may be exposed.

Block this app

Collaboration app used by 23 identities

Risk Group: Web Reputation
Issues: Apps with high levels of threat activity are identified as having poor web reputations.

Block this app

Skynet

Cloud Carrier app used by 93 identities

Risk Group: Suspicious Apps
Issues: Apps originating in nations with government-mandated data inspection may be forced to submit corporate data to third parties.

Block this app

Flagged Application Protocols

Top 15 Protocols

- SSH
- Telnet
- Bittorrent
- the-pirate-bay

Event count (Last 30 days)

7250 Total ▲ 11% vs. last 30 days

Network Protocol used by 39 identities

Sep 2, 2020
494 Events

Allowed 82% Blocked 18%

3 Identities VIEW IN TOP IDENTITIES

...et
...twork protocol used on
...nternet or local area
...orks to provide a
...ctional interactive
text-oriented
communications facility using
a virtual terminal connection.

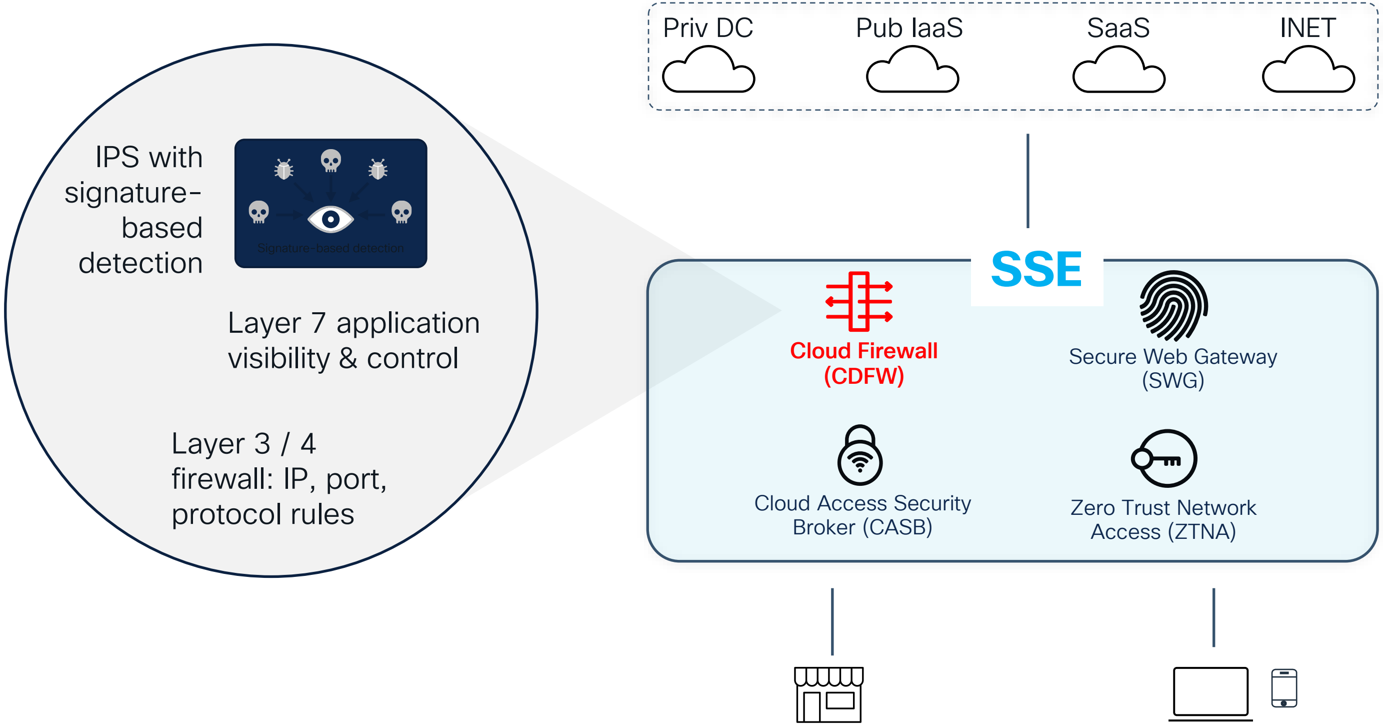
Block apps on non-standard ports (i.e.telnet over 8080)

Umbrella Intrusion Prevention System (IPS)

Compliance

Detecting vulnerabilities

Snort 3 Signatures From Talos



IPS with signature-based detection

Layer 7 application visibility & control

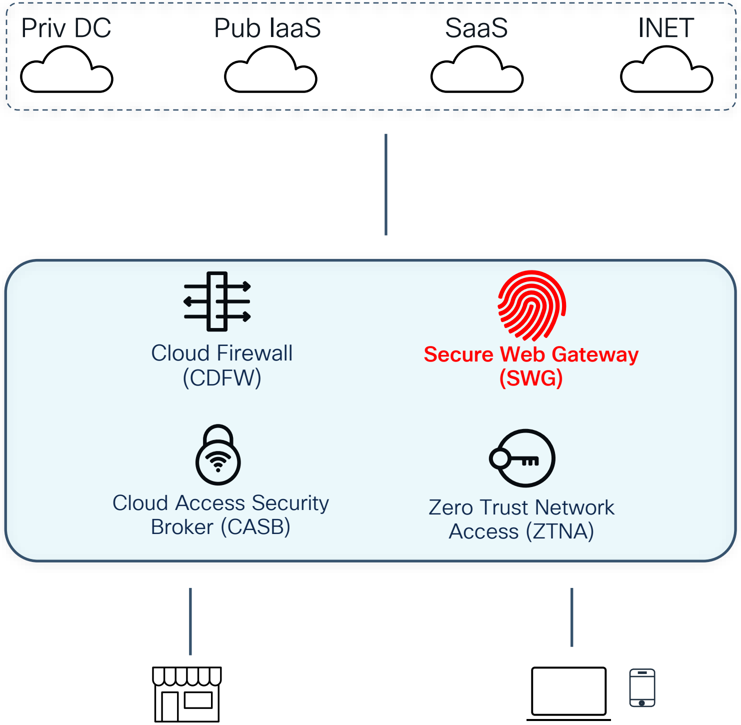
Layer 3 / 4 firewall: IP, port, protocol rules

Signature-based detection
Priv DC
Pub IaaS
SaaS
INET
SSE
Cloud Firewall (CDFW)
Secure Web Gateway (SWG)
Cloud Access Security Broker (CASB)
Zero Trust Network Access (ZTNA)

Secure Access (SSE)

Secure Web Gateway

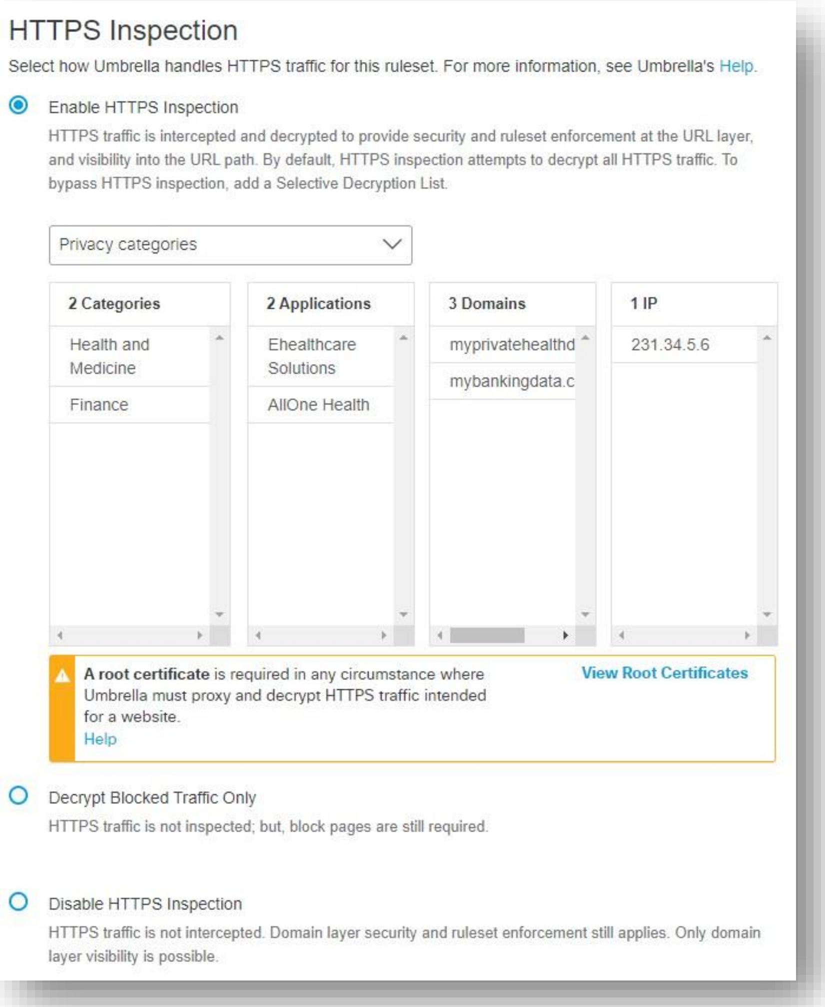
- SSL Decrypt
- Category / Content Control
- Application Control
- File type Controls
- Remote Browser Isolation
- AMP / TG / AV



Selective decryption

Except – based on categories, specific apps, domains, etc

To get full logging – Decrypt, apply policy, log, re-encrypt



HTTPS Inspection

Select how Umbrella handles HTTPS traffic for this ruleset. For more information, see Umbrella's Help.

● Enable HTTPS Inspection

HTTPS traffic is intercepted and decrypted to provide security and ruleset enforcement at the URL layer, and visibility into the URL path. By default, HTTPS inspection attempts to decrypt all HTTPS traffic. To bypass HTTPS inspection, add a Selective Decryption List.

Privacy categories

2 Categories	2 Applications	3 Domains	1 IP
Health and Medicine	Ehealthcare Solutions	myprivatehealthd	231.34.5.6
Finance	AllOne Health	mybankingdata.c	

⚠ **A root certificate** is required in any circumstance where Umbrella must proxy and decrypt HTTPS traffic intended for a website.
Help

View Root Certificates

○ Decrypt Blocked Traffic Only

HTTPS traffic is not inspected; but, block pages are still required.

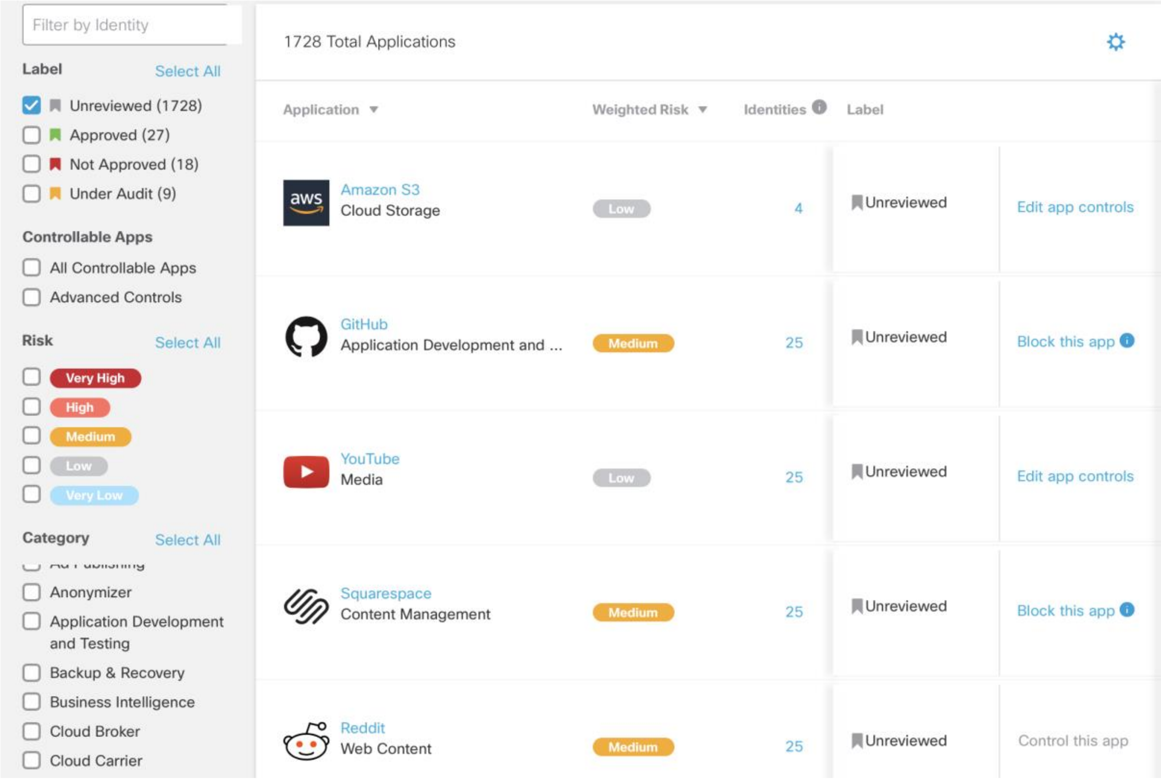
○ Disable HTTPS Inspection

HTTPS traffic is not intercepted. Domain layer security and ruleset enforcement still applies. Only domain layer visibility is possible.

App discovery and controls

Visibility into shadow IT and control of cloud apps

- Full list of cloud apps in use (great for Shadow IT)
- Workflow to block/control
- Number of users and amount of incoming and outgoing traffic



Filter by Identity

Label Select All

☑ Unreviewed (1728)
□ Approved (27)
□ Not Approved (18)
□ Under Audit (9)

Controllable Apps

□ All Controllable Apps
□ Advanced Controls

Risk Select All

□ Very High
□ High
□ Medium
□ Low
□ Very Low

Category Select All

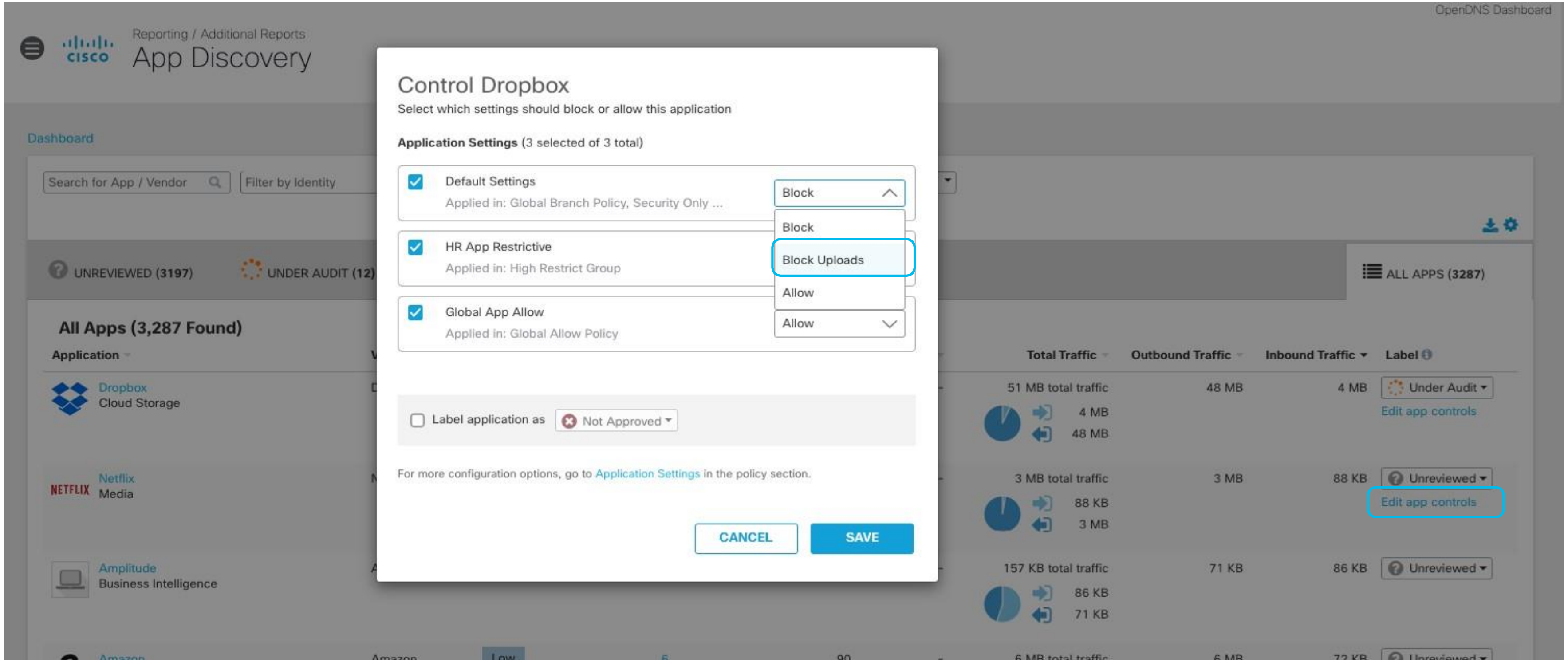
□ Ad Publishing
□ Anonymizer
□ Application Development and Testing
□ Backup & Recovery
□ Business Intelligence
□ Cloud Broker
□ Cloud Carrier

1728 Total Applications

Application ▼	Weighted Risk ▼	Identities	Label	
Amazon S3 Cloud Storage	Low	4	Unreviewed	Edit app controls
GitHub Application Development and ...	Medium	25	Unreviewed	Block this app
YouTube Media	Low	25	Unreviewed	Edit app controls
Squarespace Content Management	Medium	25	Unreviewed	Block this app
Reddit Web Content	Medium	25	Unreviewed	Control this app

Granular app controls

Block uploads (i.e. Dropbox/Box)
Block attachments (i.e. webmail)



App Discovery

Control Dropbox

Select which settings should block or allow this application

Application Settings (3 selected of 3 total)

☑ Default Settings
Applied in: Global Branch Policy, Security Only ...
Block

- Block
- Block Uploads
- Allow

☑ HR App Restrictive
Applied in: High Restrict Group

☑ Global App Allow
Applied in: Global Allow Policy
Allow

□ Label application as: Not Approved

For more configuration options, go to Application Settings in the policy section.

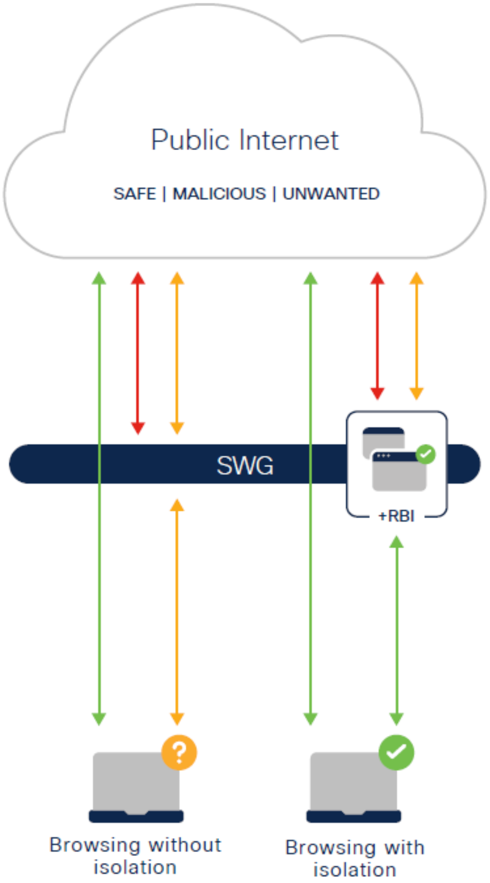
CANCEL SAVE

All Apps (3,287 Found)

Application	V				Total Traffic	Outbound Traffic	Inbound Traffic	Label
Dropbox Cloud Storage	D				51 MB total traffic 4 MB 48 MB	48 MB	4 MB	Under Audit Edit app controls
Netflix Media	N				3 MB total traffic 88 KB 3 MB	3 MB	88 KB	Unreviewed Edit app controls
Amplitude Business Intelligence	A				157 KB total traffic 86 KB 71 KB	71 KB	86 KB	Unreviewed
Amazon	Amazon	Low	6	90	6 MB total traffic	6 MB	72 KB	Unreviewed

Remote Browser Isolation (RBI)

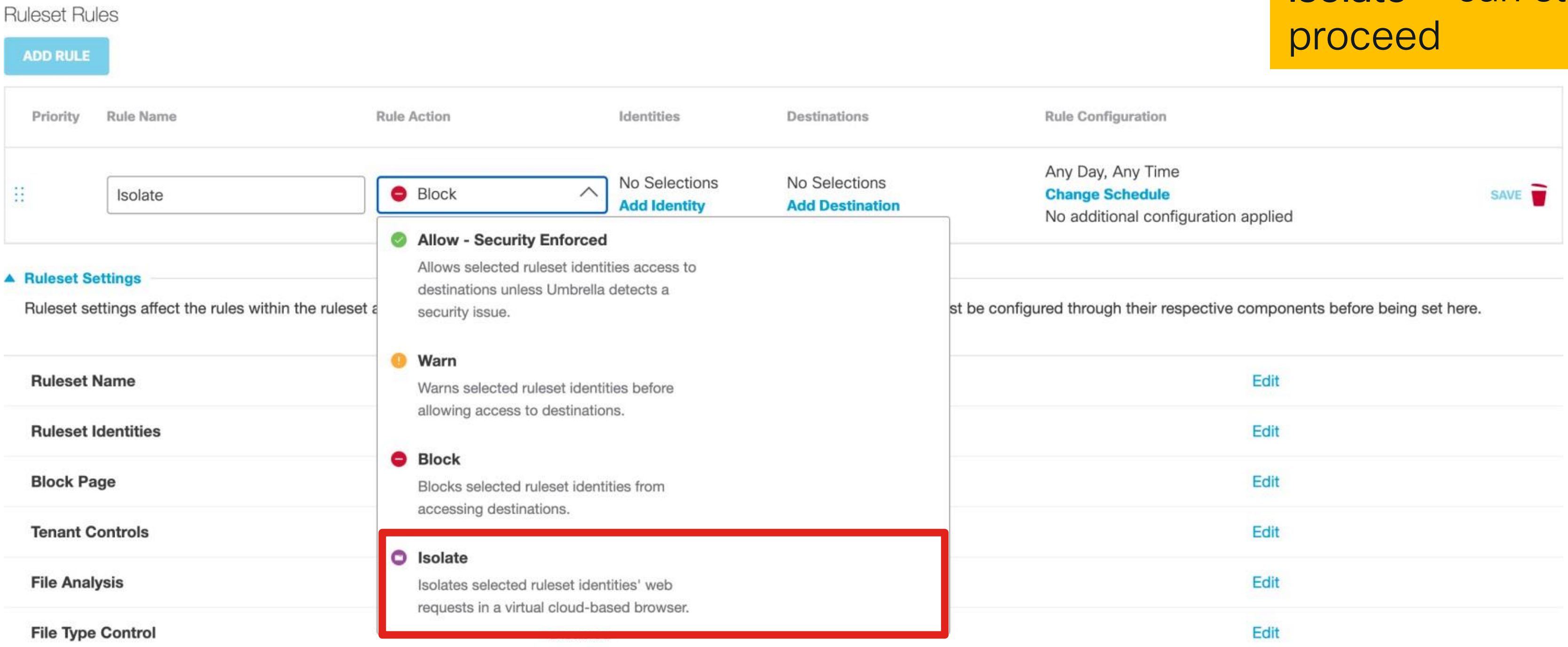
- Provide air gap between user, device and browser-based threats
- Deployed rapidly without changing existing configuration
- We deploy virtual browsers in our cloud to deliver a secure browsing experience
  with protection from zero-day threats
- Offload risk, threats won't be included in restructured browser session
- Fully integrated in policy and reporting



RBI integrated in a very simple way

Block = user can’t proceed

Isolate = can still proceed



Ruleset Rules

ADD RULE

Priority	Rule Name	Rule Action	Identities	Destinations	Rule Configuration	
	Isolate	Block	No Selections **Add Identity**	No Selections **Add Destination**	Any Day, Any Time **Change Schedule** No additional configuration applied	SAVE

- **Allow - Security Enforced**
  Allows selected ruleset identities access to destinations unless Umbrella detects a security issue.
- **Warn**
  Warns selected ruleset identities before allowing access to destinations.
- **Block**
  Blocks selected ruleset identities from accessing destinations.
- **Isolate**
  Isolates selected ruleset identities' web requests in a virtual cloud-based browser.

▲ **Ruleset Settings**

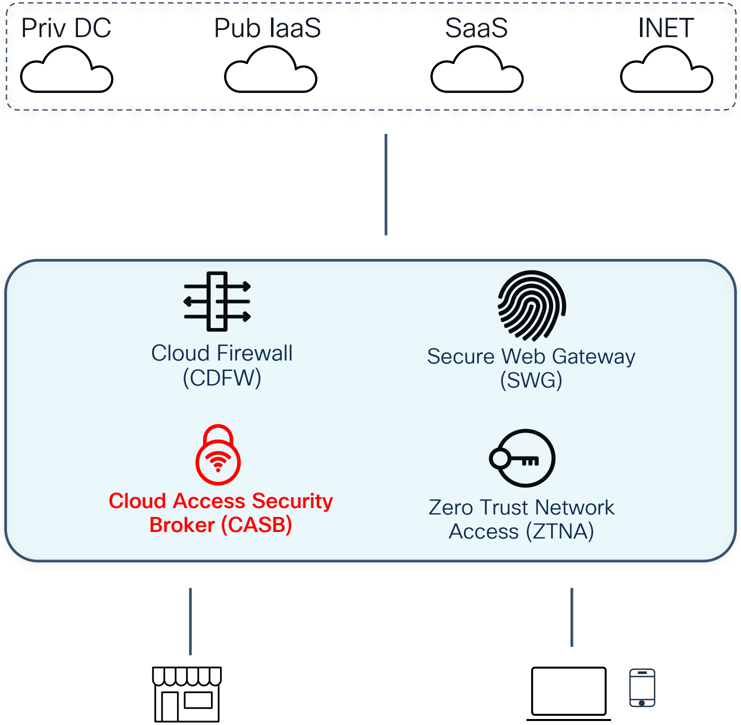
Ruleset settings affect the rules within the ruleset a … st be configured through their respective components before being set here.

Ruleset Name	Edit
Ruleset Identities	Edit
Block Page	Edit
Tenant Controls	Edit
File Analysis	Edit
File Type Control	Edit

Secure Access (SSE)

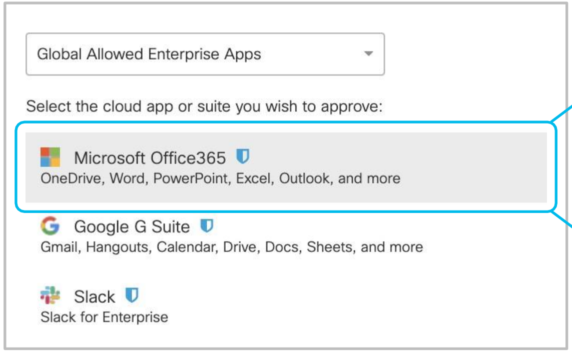
CASB / DLP

- Tenant Controls
- Application Control
- Data Loss Prevention
- Cloud Malware



Tenant controls

Select the instance(s) of Core SaaS applications that can be accessed by all users or by specific groups/individuals



Global Allowed Enterprise Apps

Select the cloud app or suite you wish to approve:

Microsoft Office365
OneDrive, Word, PowerPoint, Excel, Outlook, and more

Google G Suite
Gmail, Hangouts, Calendar, Drive, Docs, Sheets, and more

Slack
Slack for Enterprise

✓ cisco.com (Corp.
✗ instance) Jan Park (Personal
✗ instance) Ron Jamet (Personal
instance)

Configure
Tenant domain

Key Use Cases

Productivity
Only provide access to corporate instances of core SaaS apps

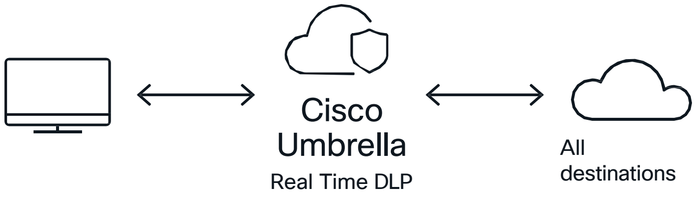
Security
Ensure, sensitive data is created and stored in approved instances of cloud apps

Multimode Cloud Data Loss Prevention (DLP)

Unified policies and reporting for a simplified experience

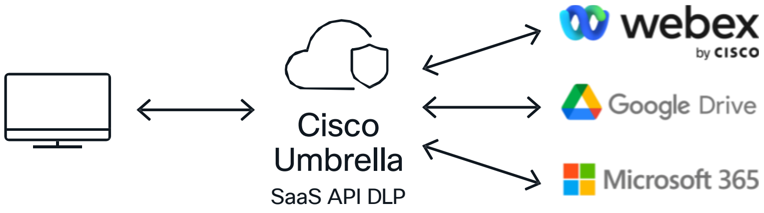
Real-time (inline) DLP

- Analyze data in transit via SWG
- Monitor & block file uploads
- All application coverage: Sanctioned and unsanctioned



SaaS API (out-of-band) DLP

- Analyze data-at-rest via public APIs
- Policy enforcement via continuous scans
- Sanctioned app coverage

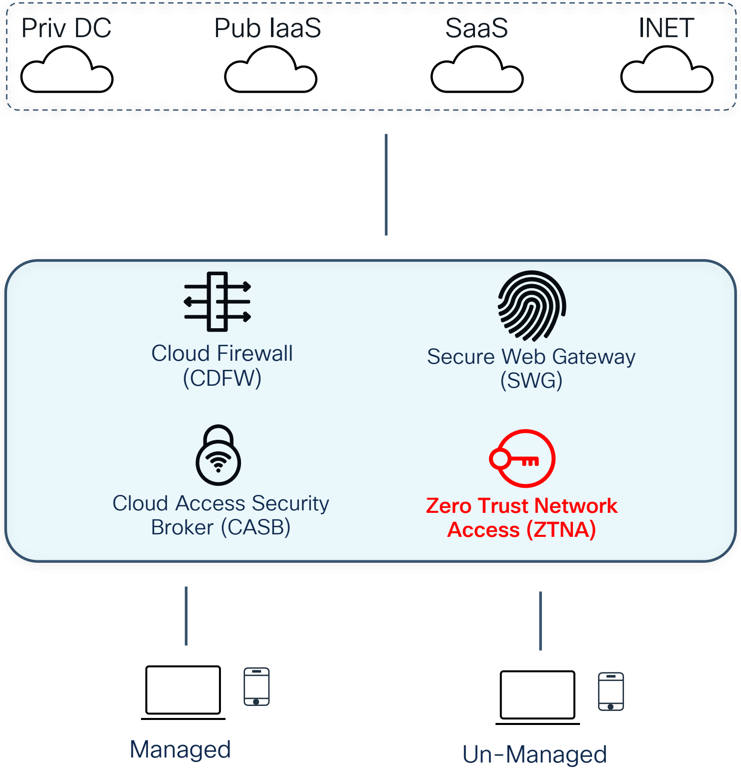


Same management interface

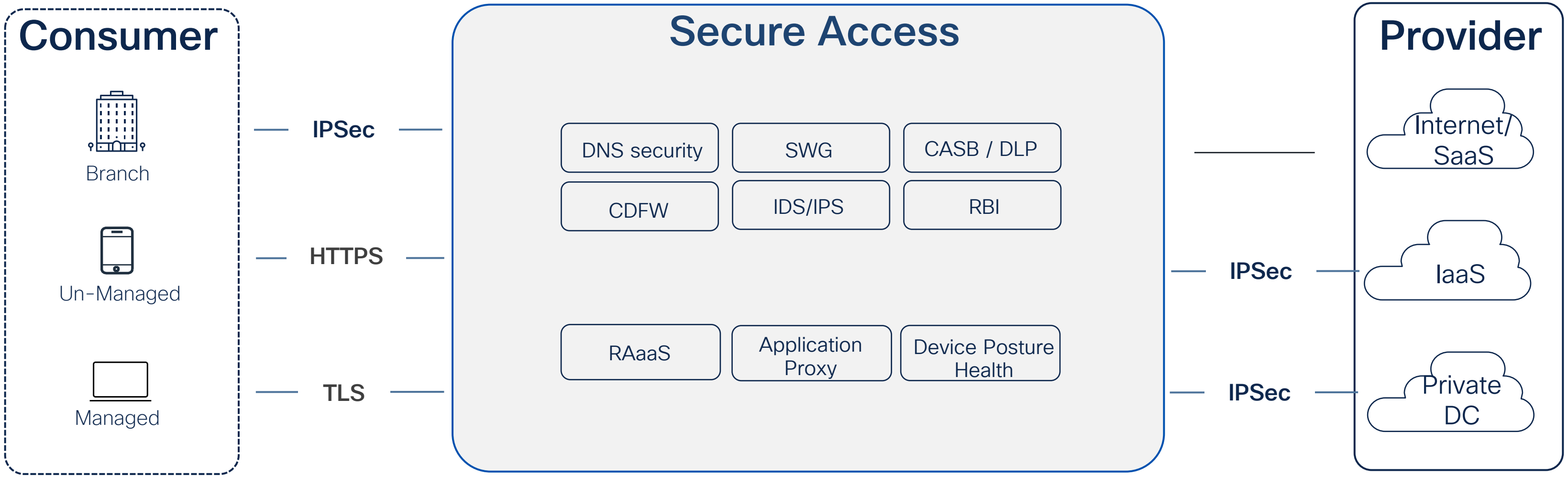
Secure Access (SSE)

Zero Trust Network Access (ZTNA)

- Verify user and device before granting access to resources
- Secure internet access, secure private access
- Managed and unmanaged devices



Cisco Secure Access (SSE) – Use cases



Consumer

Branch

Un-Managed

Managed

IPSec

HTTPS

TLS

Secure Access

DNS security

SWG

CASB / DLP

CDFW

IDS/IPS

RBI

RAaaS

Application Proxy

Device Posture Health

IPSec

IPSec

Provider

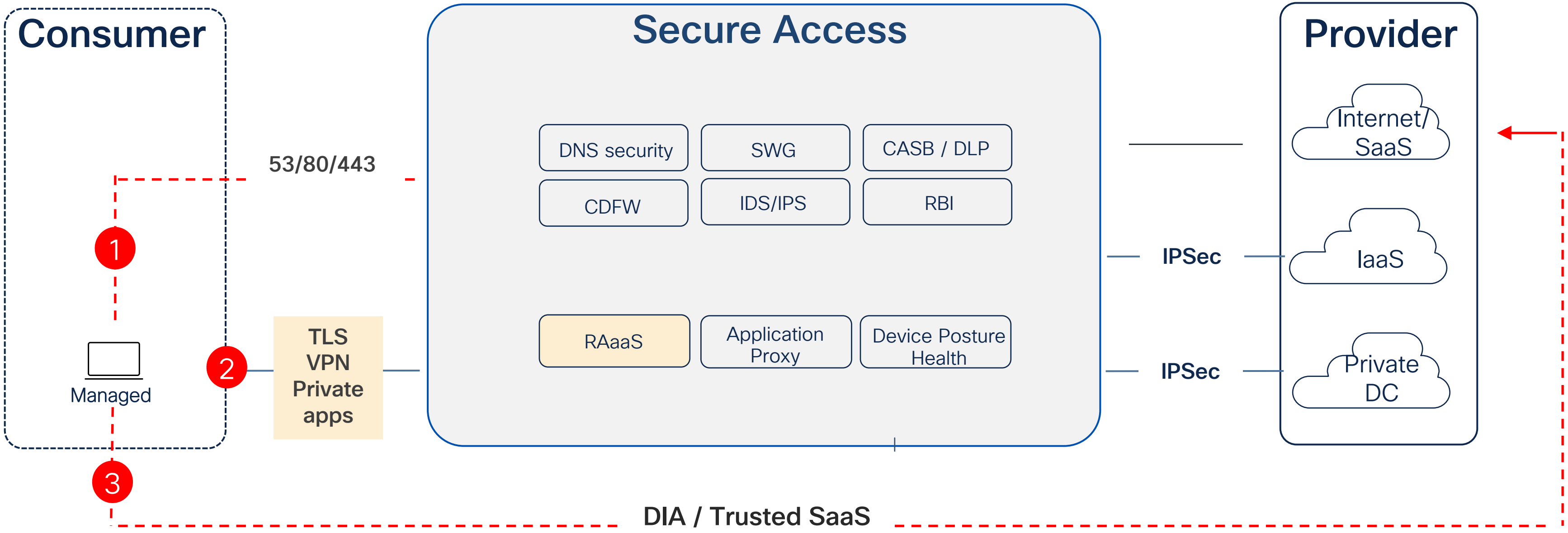
Internet/ SaaS

IaaS

Private DC

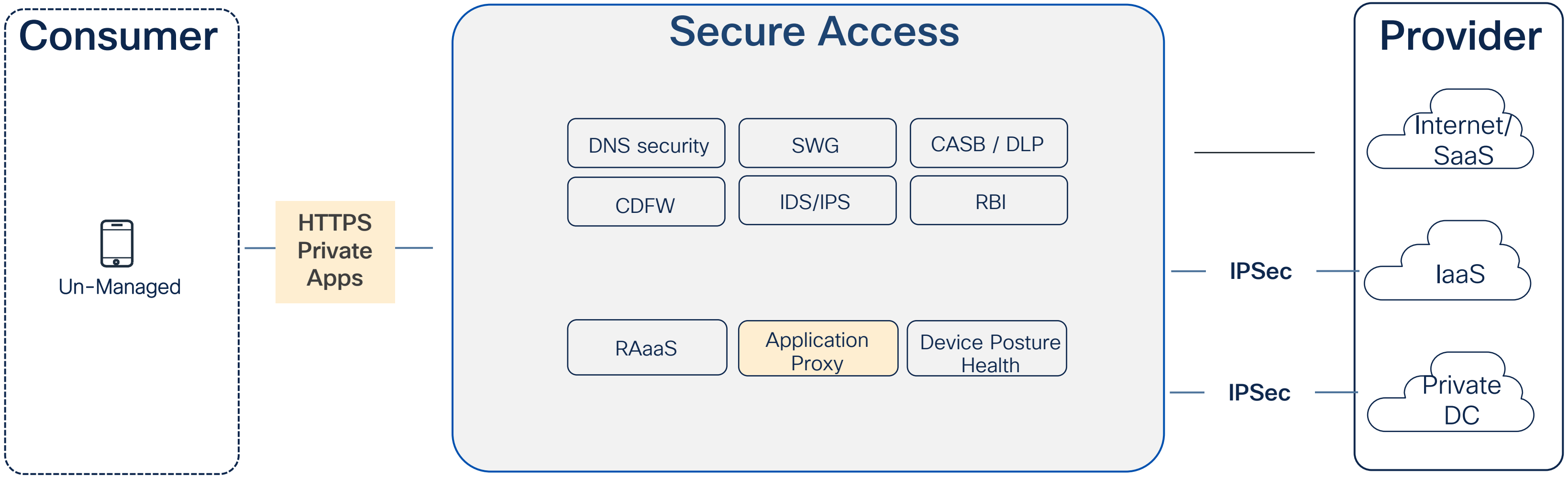
Cisco Secure Access (SSE)

Managed endpoint detail



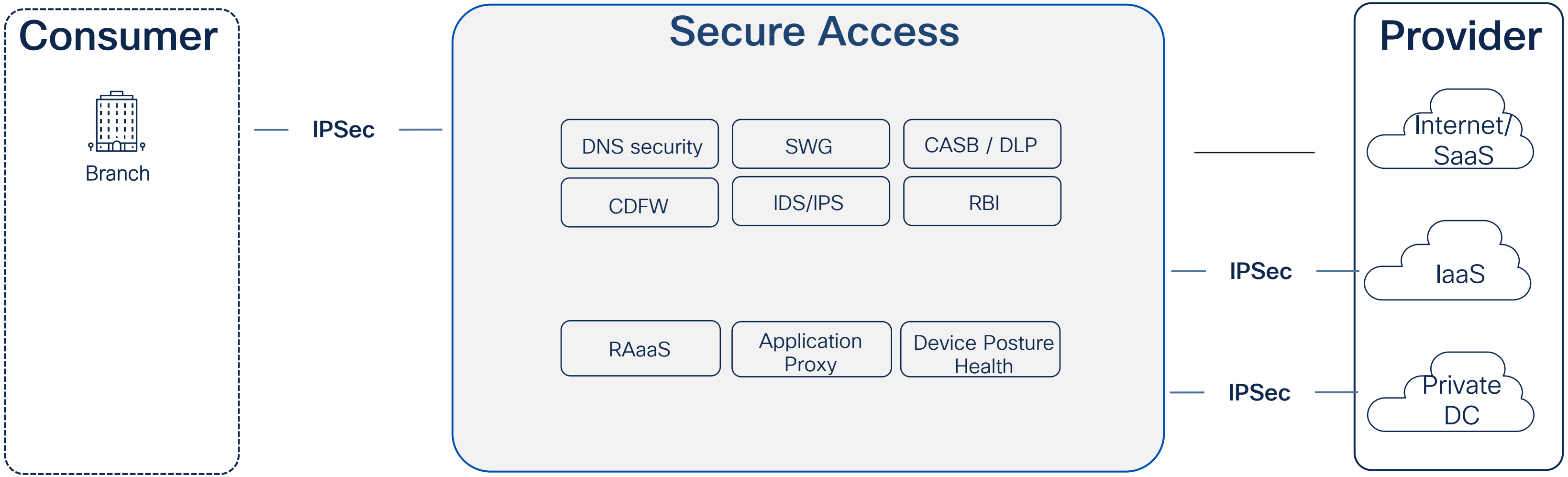
Cisco Secure Access (SSE)

Unmanaged endpoint detail



Cisco Secure Access (SSE)

Branch access detail



- Supports Cisco and 3rd party devices via IPSec
- Cisco = config templates with ZTP (drop ship routers), smart licensing “get keys”

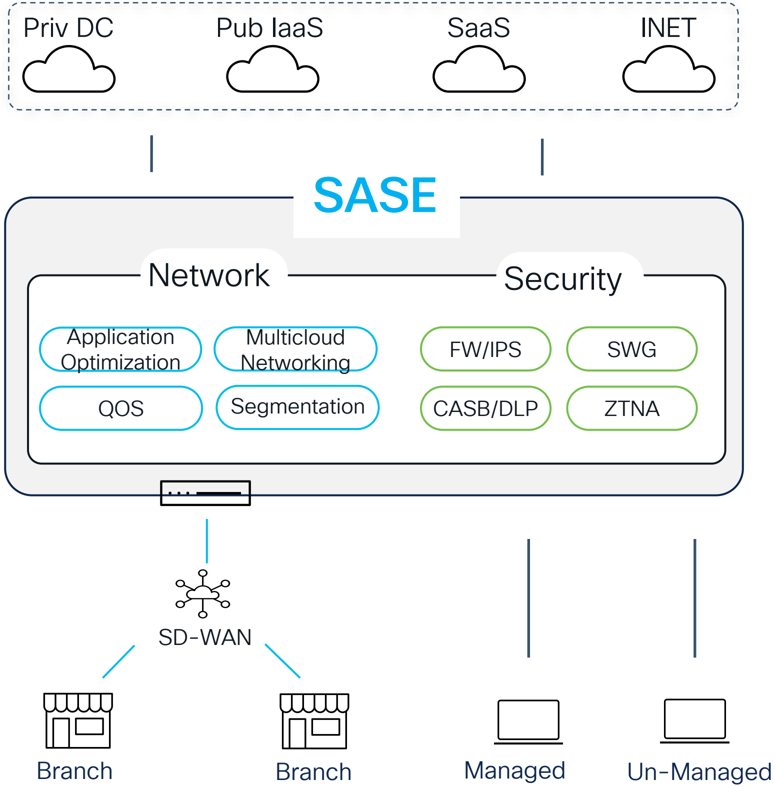
SASE

SASE
Gartner

“Secure access service edge (SASE) delivers converged network and security as a service capabilities, including SD-WAN, SWG, CASB, NGFW and zero trust network access (ZTNA).

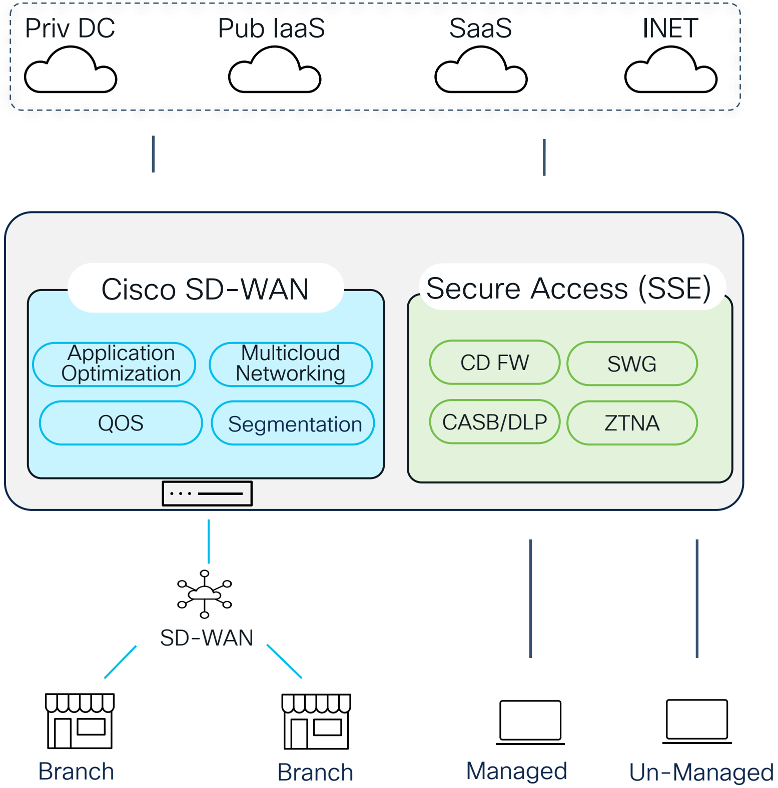
SASE supports branch office, remote worker and on-premises secure access use cases.

SASE is primarily delivered as a service and enables zero trust access based on the identity of the device or entity, combined with real-time context and security and compliance policies”

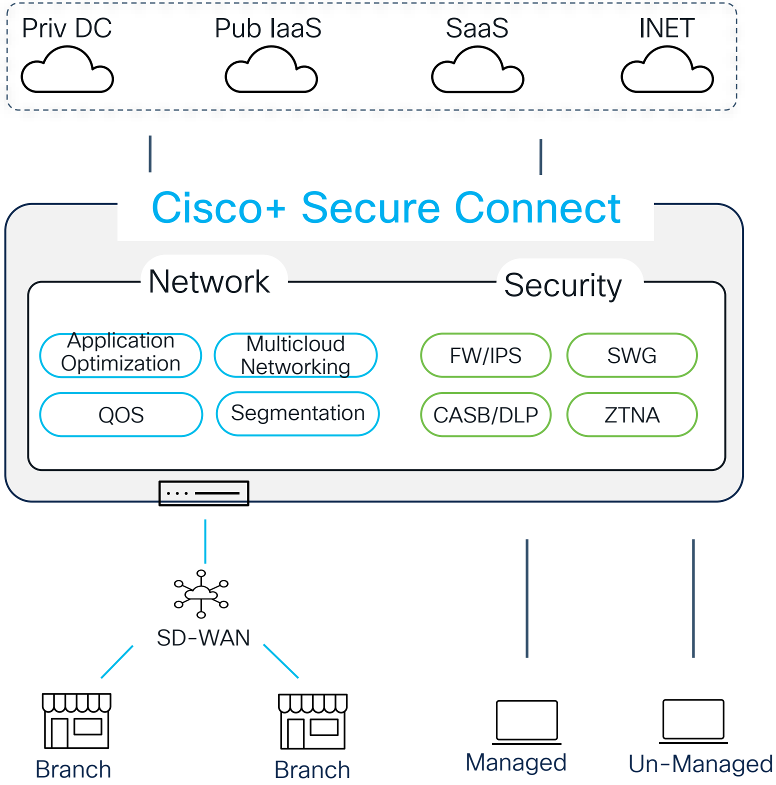


SASE Flavors

Modular



Unified



Cisco+ Secure Connect

Unified SASE Solution

Unified Dashboard

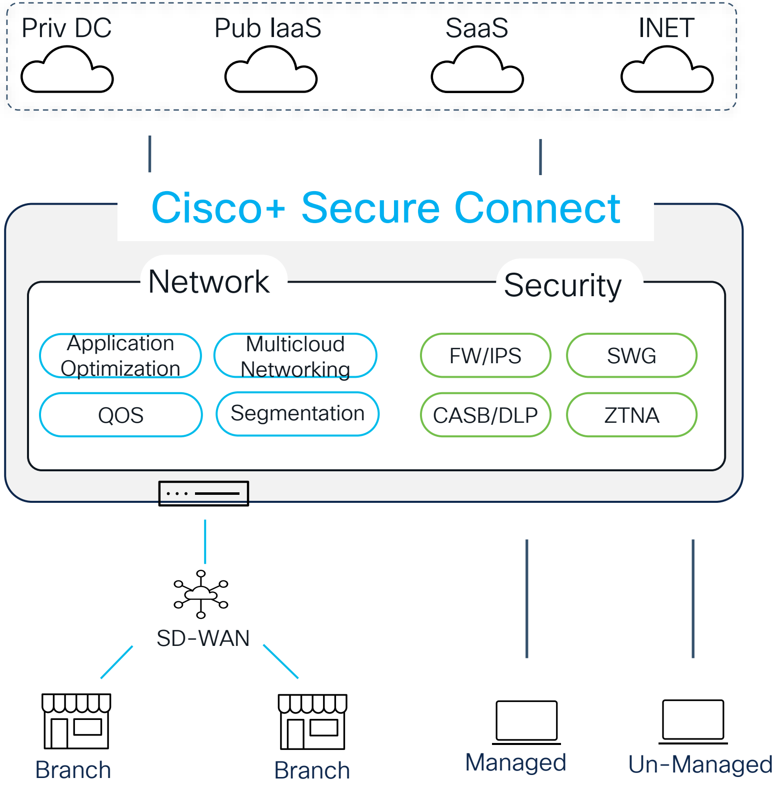
Provides a unified IT experience that is easy to deploy and operate, without complex engineering

Unified Support

The Unified Support for Secure Connect has its own team working 24/7 via email or phone.

Turnkey Operations

Solution comes pre-integrated with minimal work needed from the customer



Why use SD-WAN? Why can’t we just use our ZTNA solution?

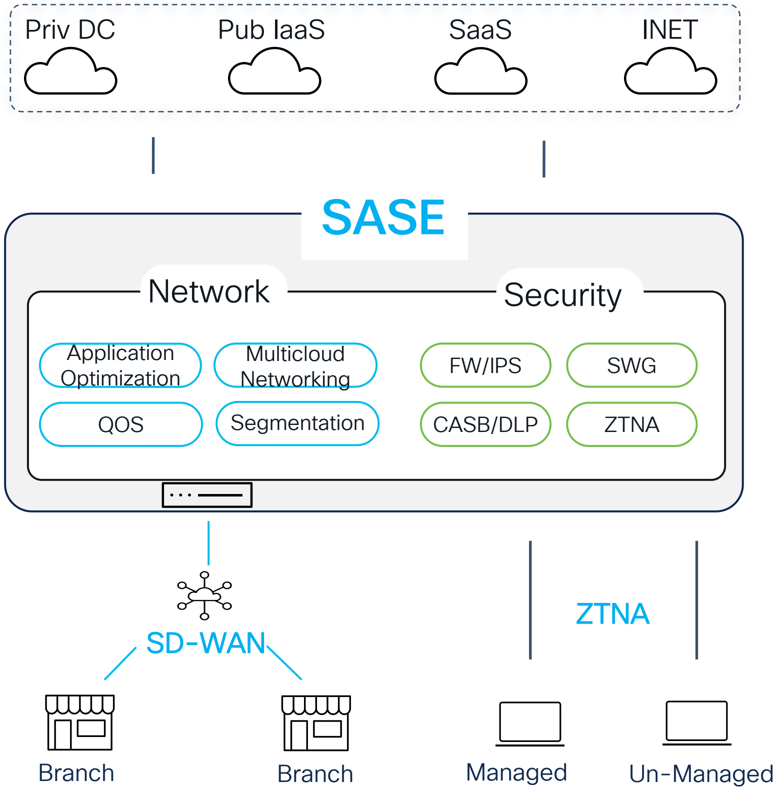
Customer

ZTNA / SD-WAN

ZTNA solutions provide secure remote access to applications

SD-WAN provides traffic optimization, application performance monitoring, path selection

Different networking technologies – not either/or but BOTH



Benefits of Network / SD-WAN for SASE

Using SD-WAN to help meet strict application SLAs

Use Case = branch employee to AWS application

First mile

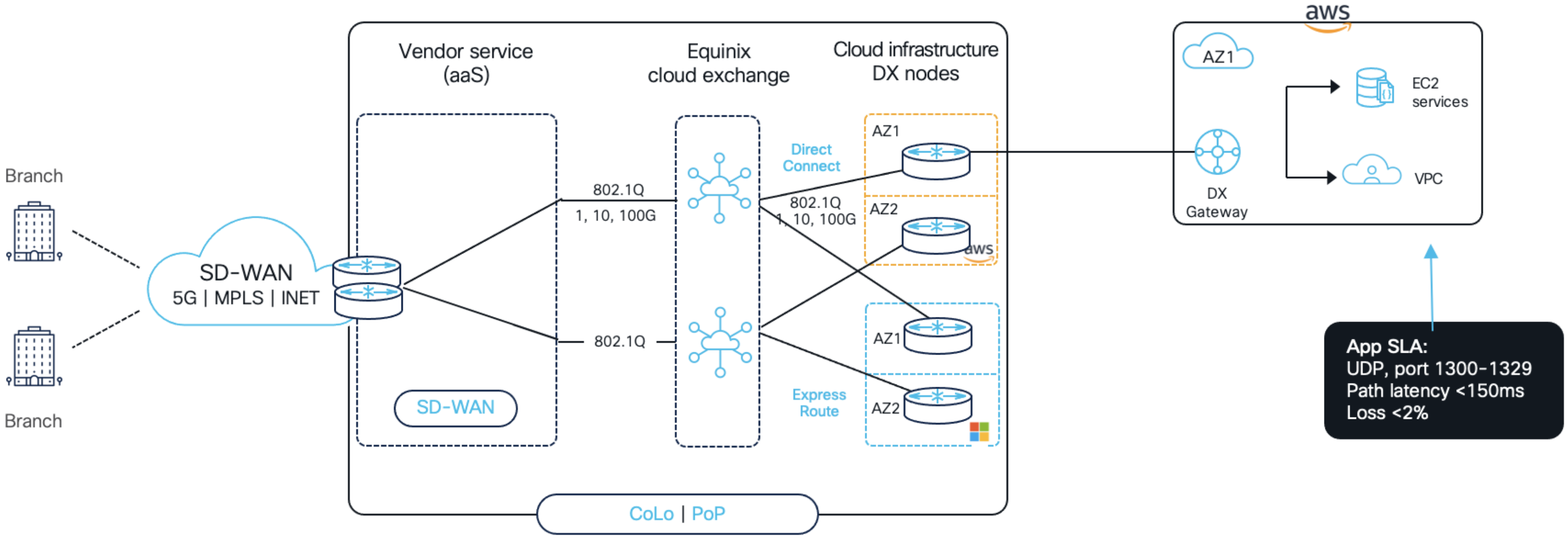
WAN service, internet,
or private networks

Middle mile

SP core network,
private network, ASN

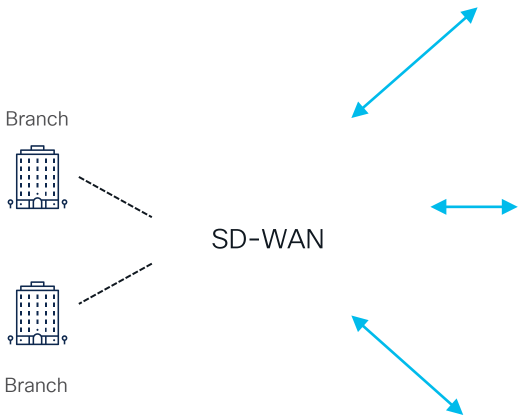
Last mile

CSP network, ASN,
or private networks



App SLA:
UDP, port 1300-1329
Path latency <150ms
Loss <2%

First mile – underlay options



MPLS

- Was gold standard for private connections
- Packet prioritization, guarantee on availability/performance
- It’s a VPN so segmented from public Internet

Shared Internet

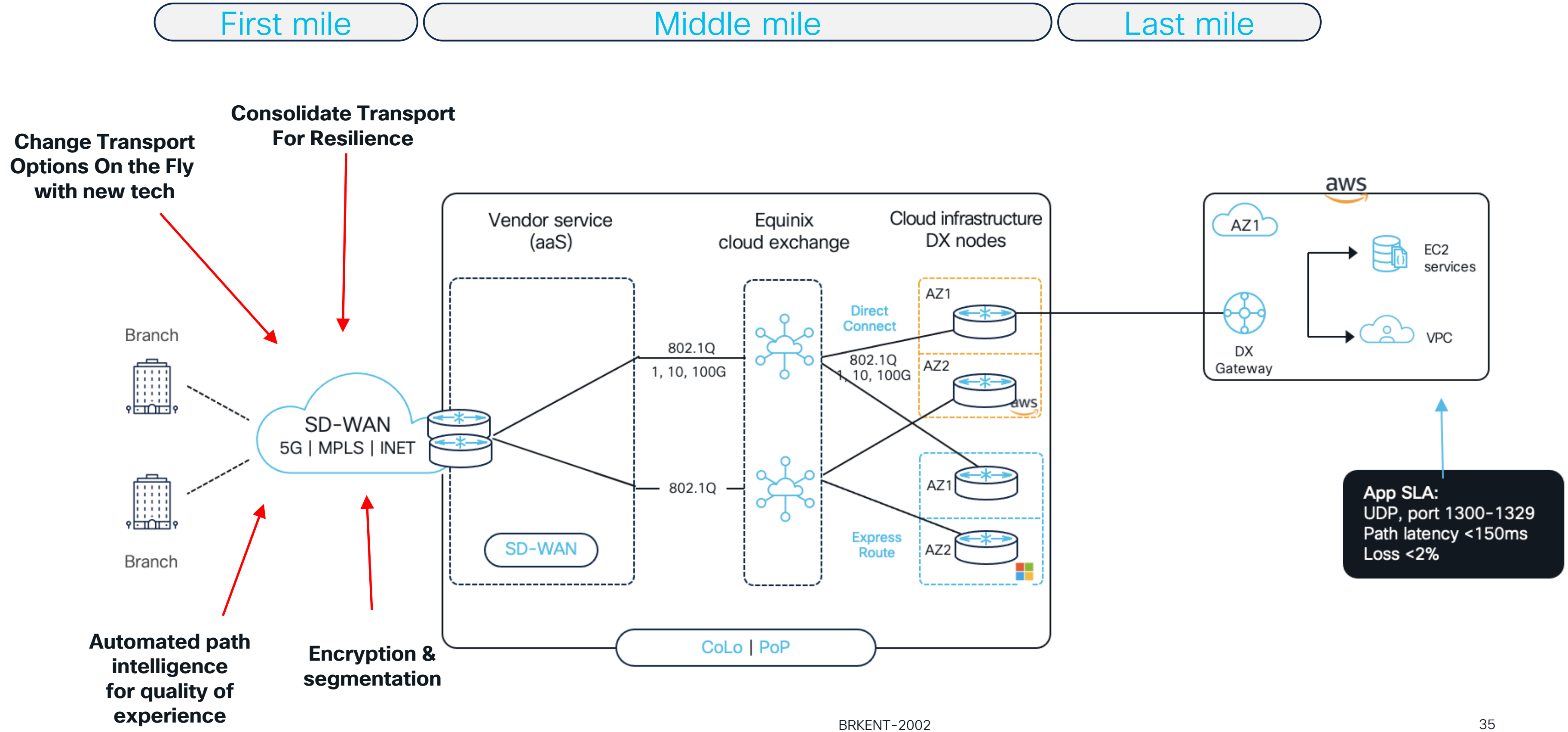
- Broadband, 5G, etc
- Infra is shared, availability & performance not guaranteed by SLA (no CoS), asynchronous comms

Dedicated Internet

- T1, Ethernet over Copper, Ethernet over Fiber, etc
- CoS options, synchronous comms

Using SD-WAN to help meet strict application SLAs

First mile benefits



Change Transport Options On the Fly with new tech

Consolidate Transport For Resilience

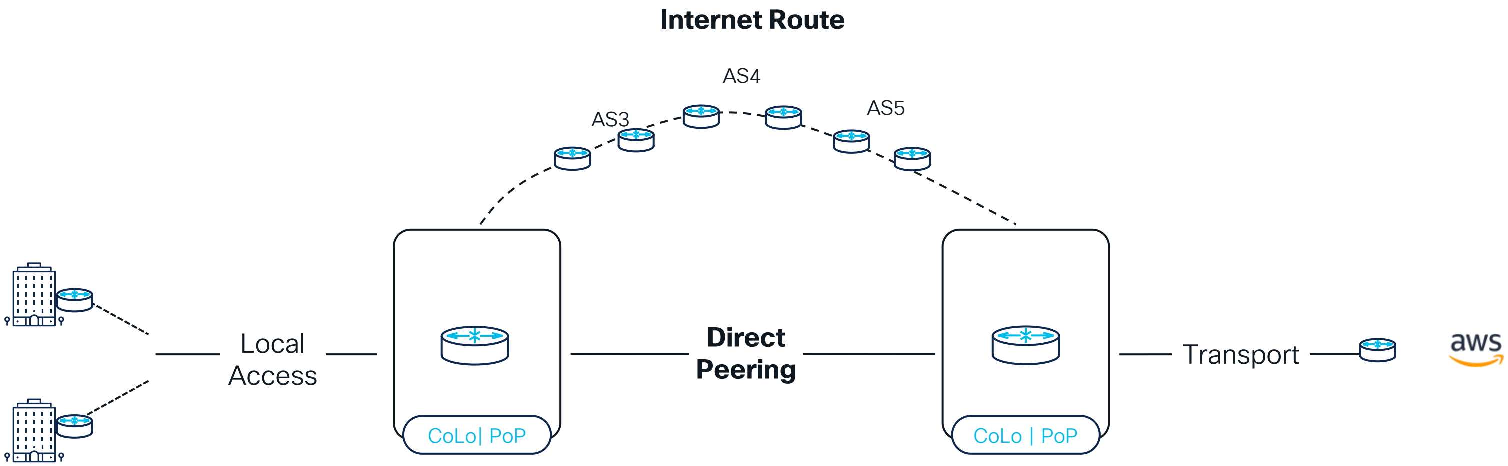
Automated path intelligence for quality of experience

Encryption & segmentation

App SLA:
UDP, port 1300-1329
Path latency <150ms
Loss <2%

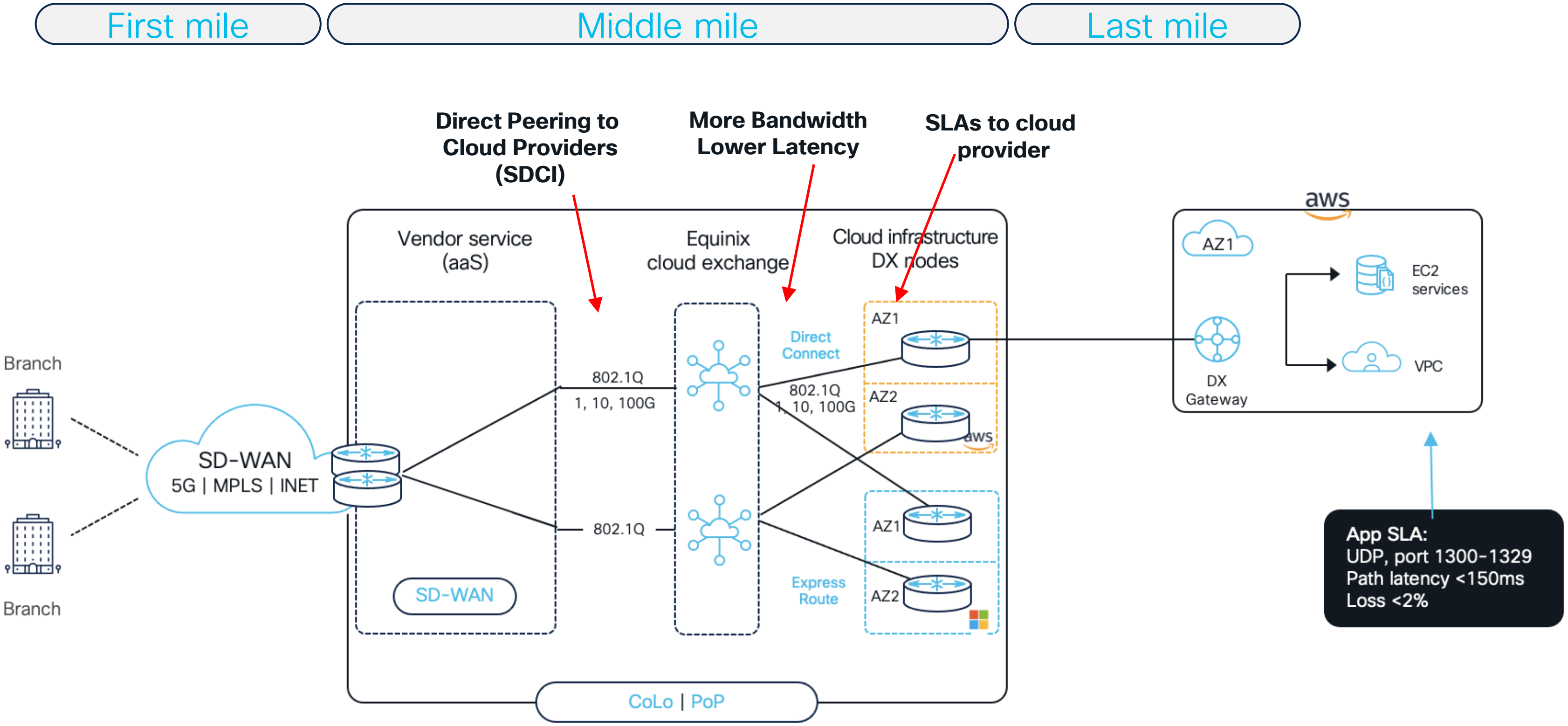
Middle Mile Optimization

First mile	Middle mile	Last mile
WAN service, internet, or private networks	SP core network, private network, ASN	CSP network, ASN, or private networks



Using SD-WAN to help meet strict application SLAs

Middle & Last mile benefits



Direct Peering to Cloud Providers (SDCI)

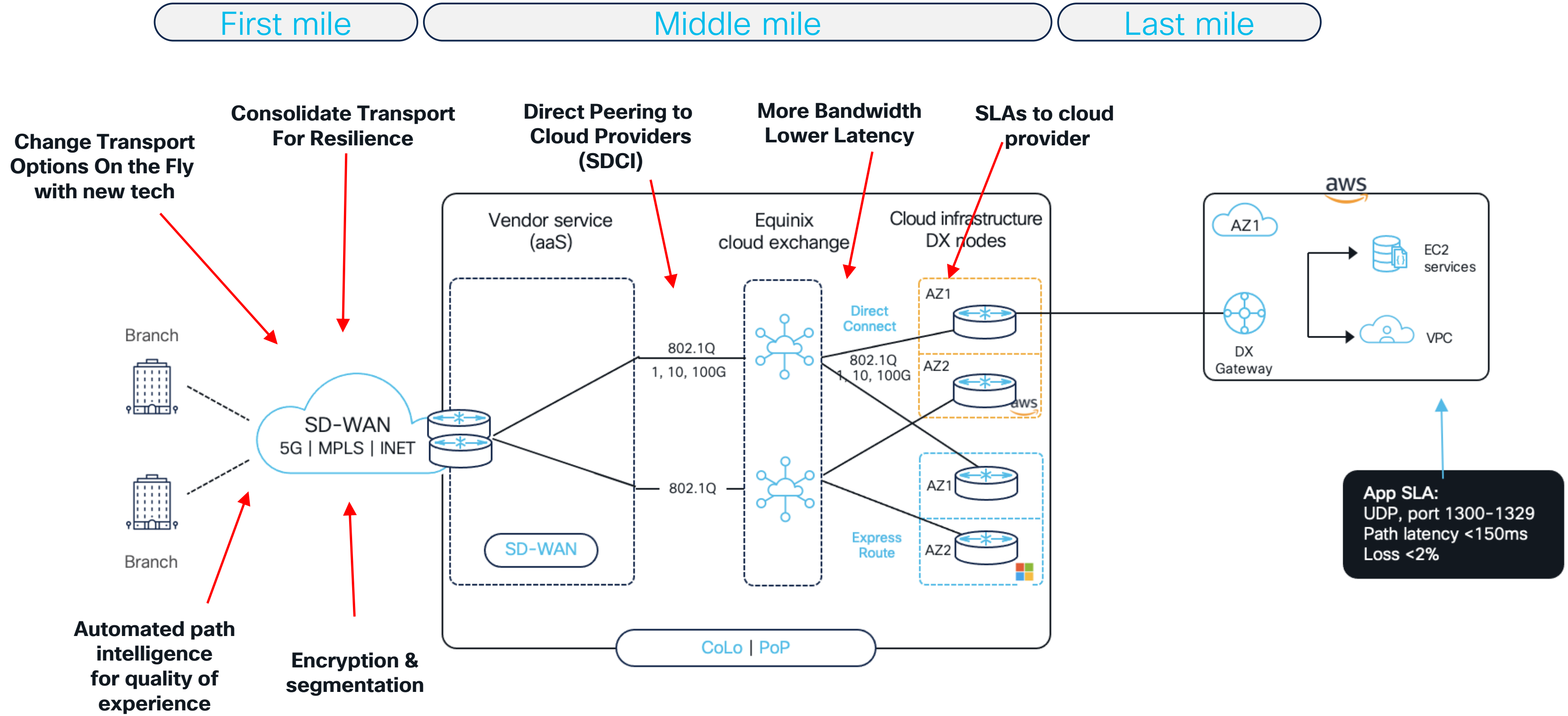
More Bandwidth Lower Latency

SLAs to cloud provider

App SLA:
UDP, port 1300-1329
Path latency <150ms
Loss <2%

Using SD-WAN to help meet strict application SLAs

Use Case = branch employee to AWS application



Change Transport Options On the Fly with new tech

Consolidate Transport For Resilience

Direct Peering to Cloud Providers (SDCI)

More Bandwidth Lower Latency

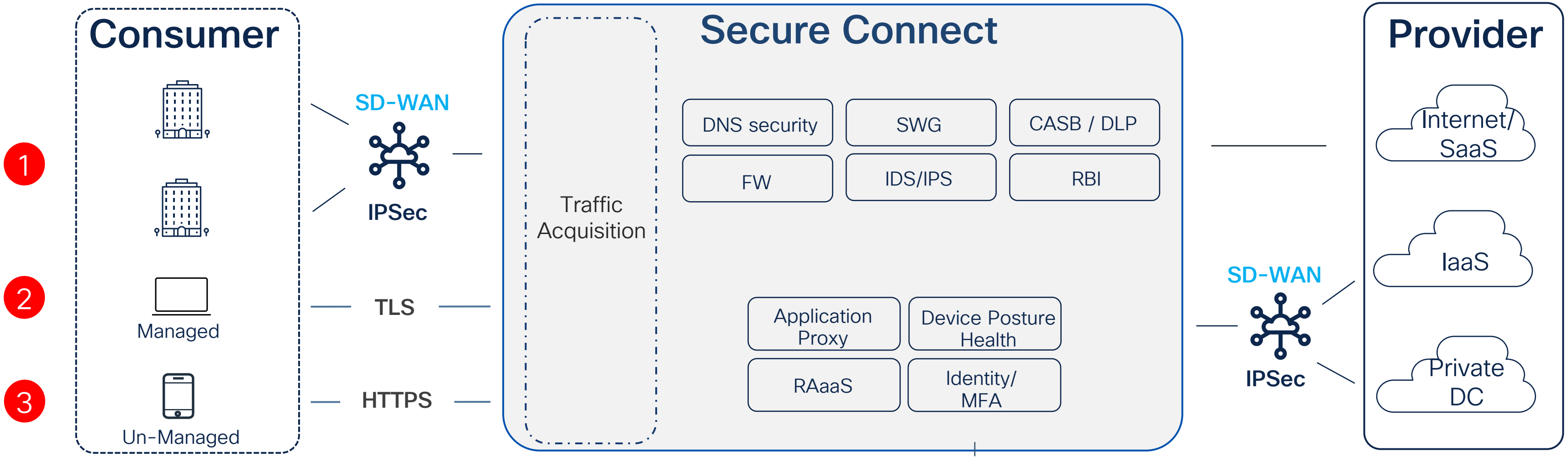
SLAs to cloud provider

Automated path intelligence for quality of experience

Encryption & segmentation

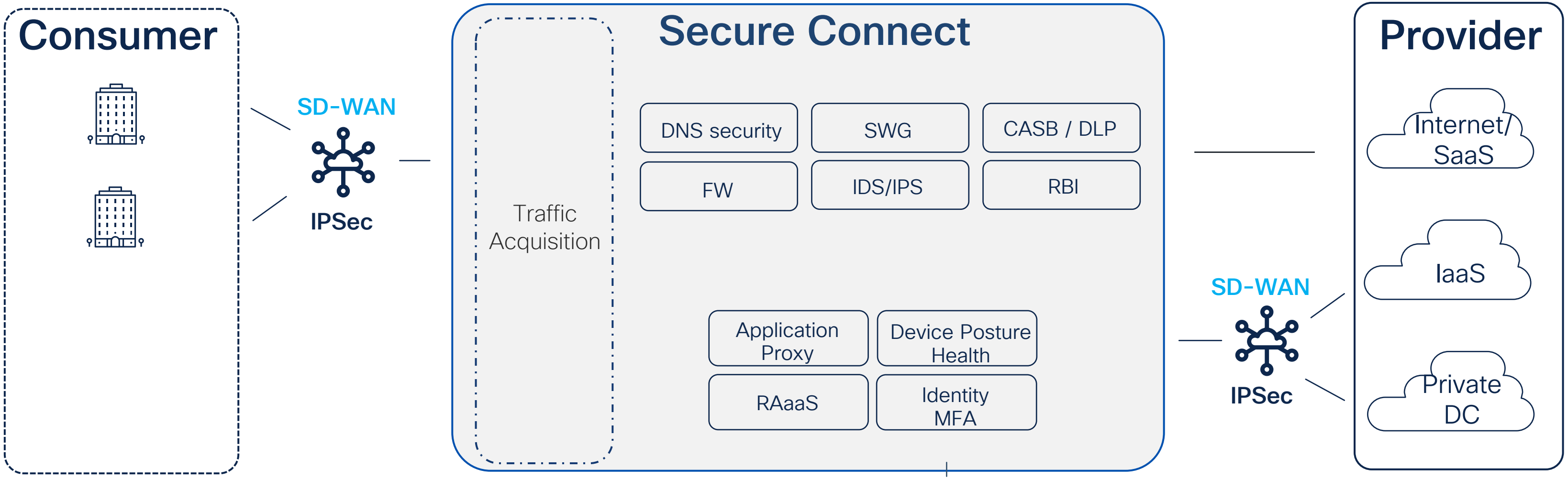
App SLA:
UDP, port 1300-1329
Path latency <150ms
Loss <2%

Cisco Secure Connect (SASE) – Use cases



Cisco Secure Connect (SASE)

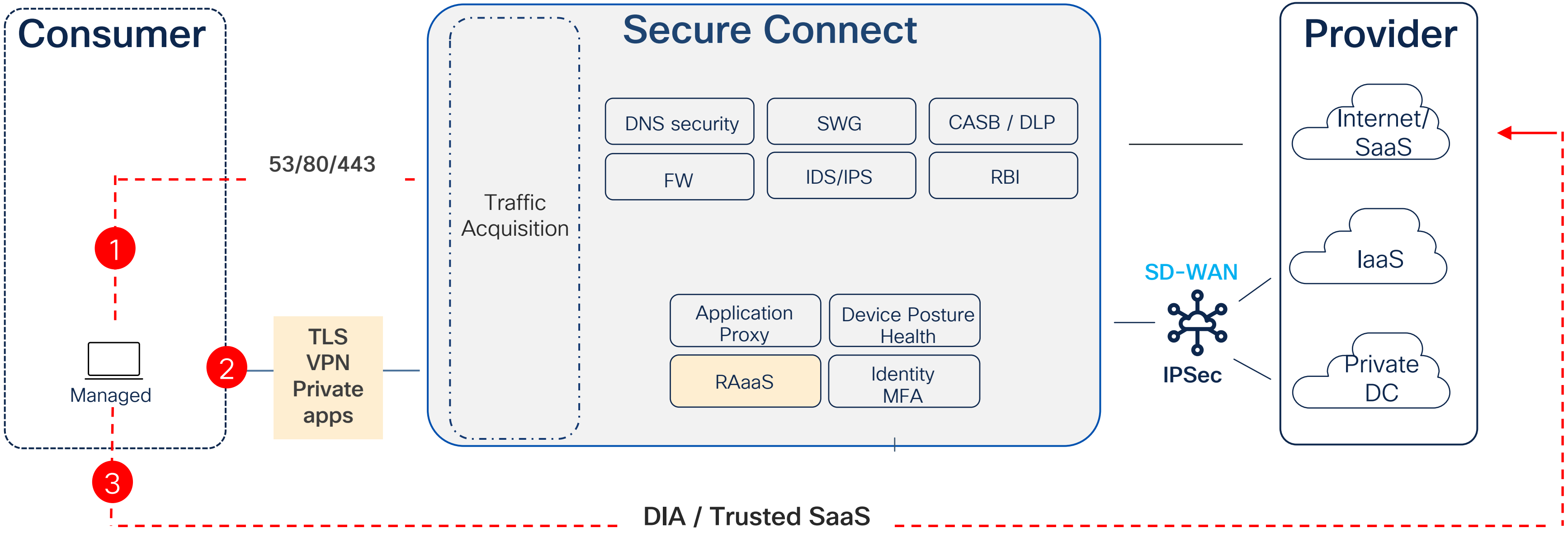
Branch access detail



1. Managing and interconnecting on-premesis sites (branches)
2. Currently supports Meraki SD-WAN (auto-VPN) or 3rd party devices via IPSec
3. Meraki creates 2 auto-VPN tunnels to corresponding DCs (primary/secondary)

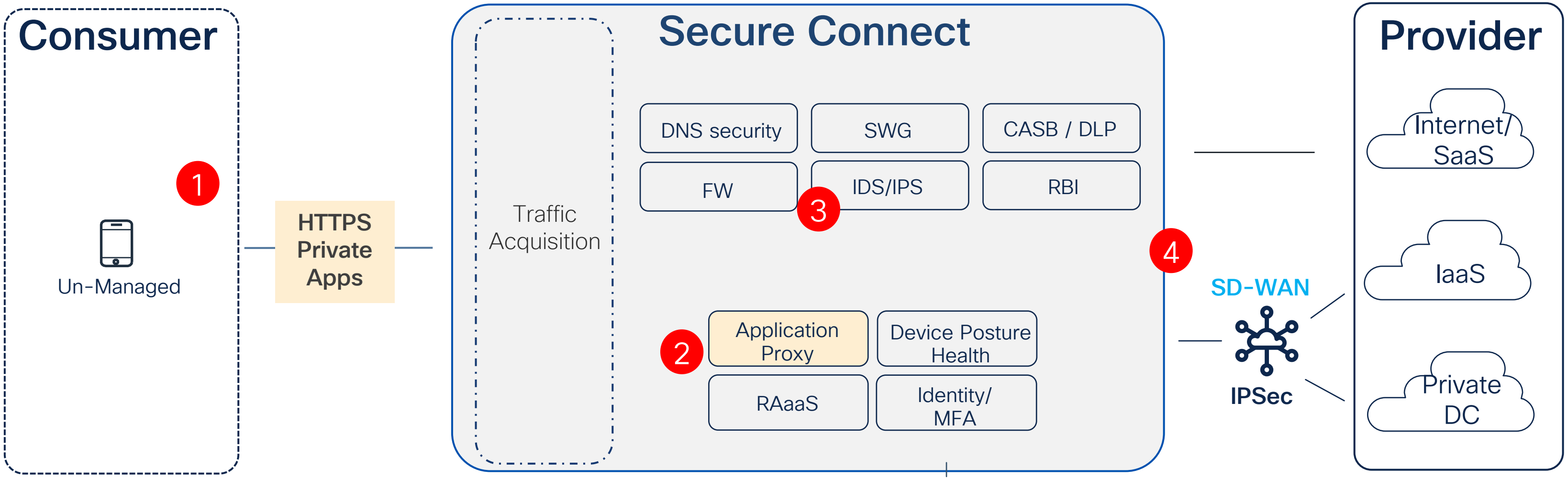
Cisco Secure Connect (SASE)

Managed endpoint detail



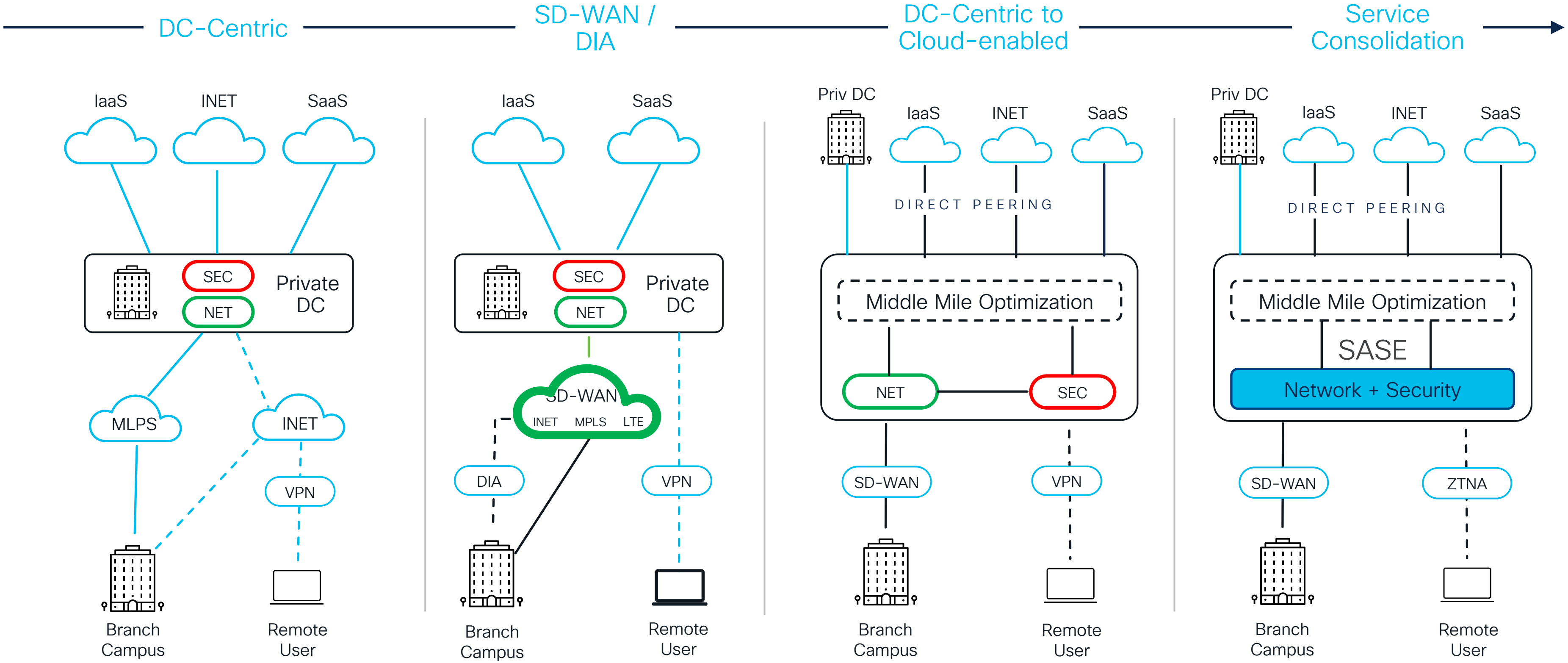
Cisco Secure Connect (SASE)

Unmanaged endpoint detail



1. Browser connection to specific URL, DNS resolved, and redirected to nearest DC (Anycast DNS)
2. Svc edge proxies traffic from browser, and rqst sent for auth'c & posture
3. Once completed sent to policy engine
4. Ultimately route to application

Example: From DC-centric Topology to SASE



Zero Trust

Zero Trust Principles

- Never assume trust
- Always verify
- Enforce least privilege

Cisco Zero Trust

Step 1

Establish Trust

Step 2

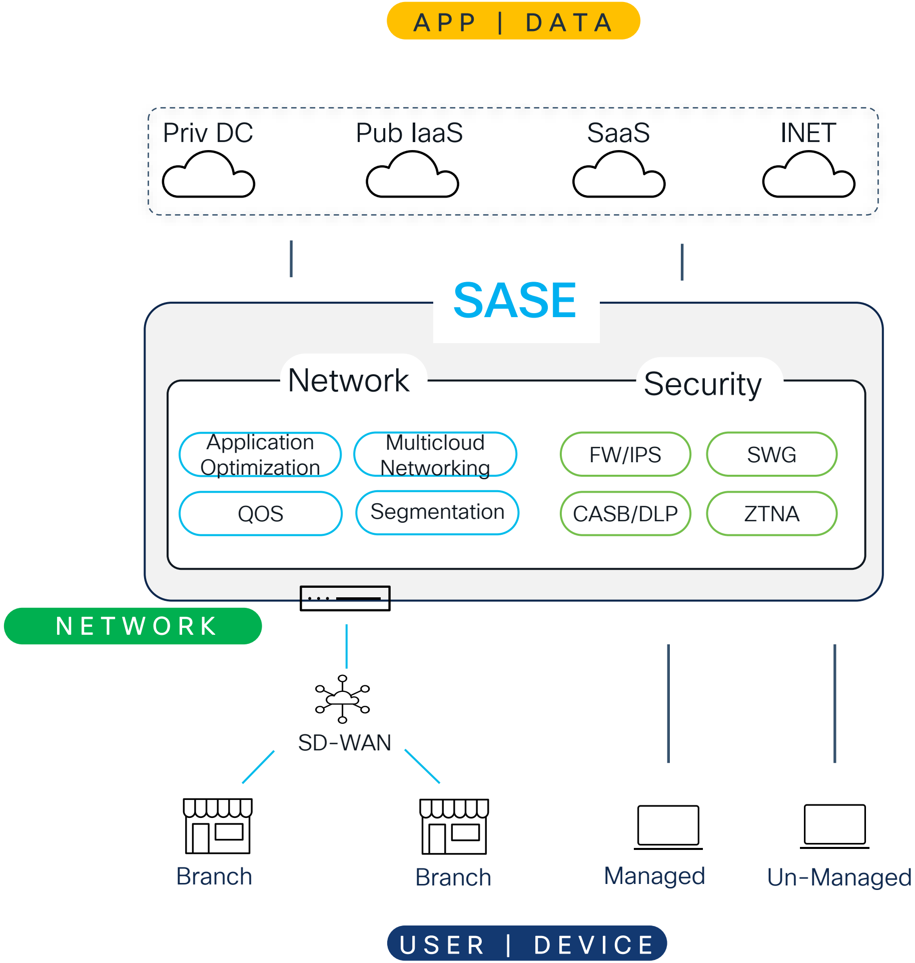
Enforce Trust

Step 3

Continually Verify Trust

For

User/Device, Network, App/Data



Zero Trust for **User/Device**

ESTABLISH TRUST

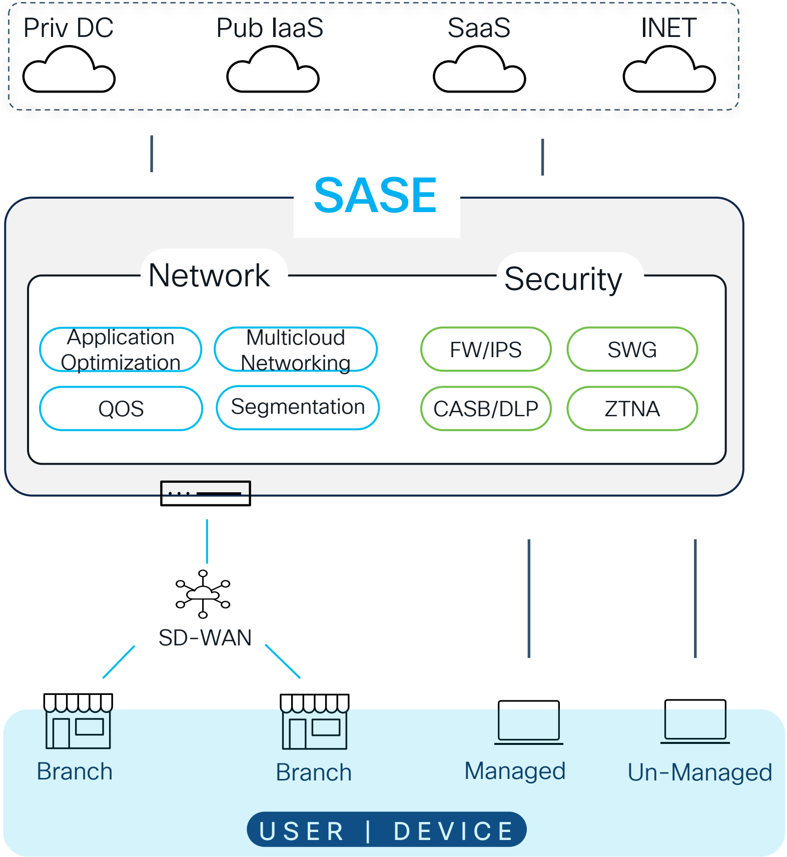
- Only authorized users are attempting to access - I.E. MFA.
- Endpoint managed or unmanaged, corporate owned or BYOD, and device posture
- Combine context to establish trust.

ENFORCE TRUST-BASED ACCESS

- Visibility of endpoint current security state of each access request
- Access policy based on use case risk level
- Report on device health via agent, agent-less, or MDM integration techniques.

CONTINUOUSLY VERIFY TRUST

- Continuous monitoring of endpoint health, management status, and anomalous behavior, so actionable responses can be tied to deviations (self-managing/healing)



Zero Trust for the Network

ESTABLISH TRUST

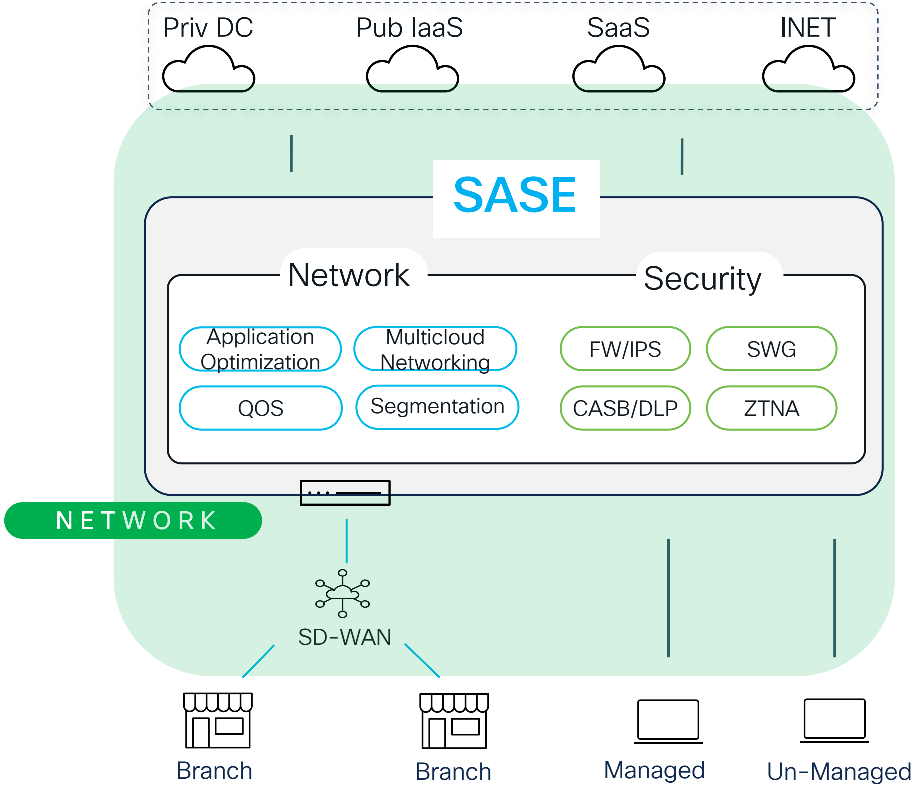
- Discover/classify users and devices (computer/mobile)
- Discover/Classify IoT devices
- Device Posture of managed and BYOD
- Combine attributes for role-based Authentication / Authorization

ENFORCE TRUST-BASED ACCESS

- Define policy using "least privilege" approach.
- Prevent "untrusted" entities from connecting to in-scope network
- Restrict network access and contain infected endpoints using segmentation

CONTINUOUSLY VERIFY TRUST

- Continuous monitoring w/vulnerability assessments and indicators of compromise.
- Tying actionable responses to behavior for self-managing/healing



Zero Trust for App/Data

ESTABLISH TRUST

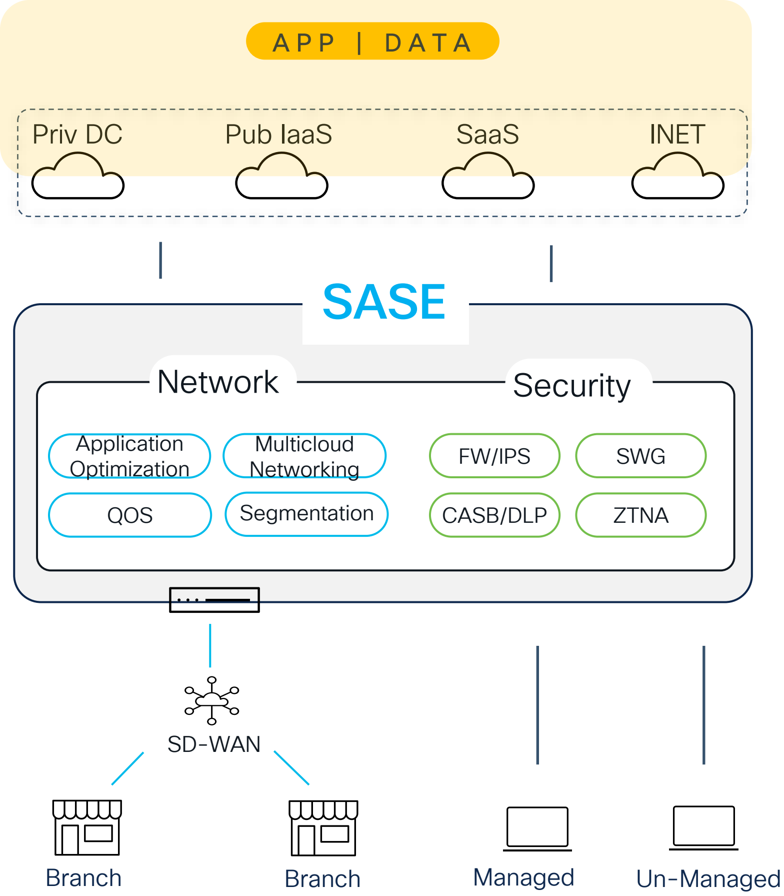
- Visibility into the devices, processes, packets, network flows within the application environments
- Analyze the network communications and data flows to model applications

ENFORCE TRUST-BASED ACCESS

- Implement policy to minimize trust within the entire application ecosystem, simulate, validate, deploy the policy consistently across all environments
- Contain breaches & minimize lateral movement with application micro-segmentation using a whitelist approach

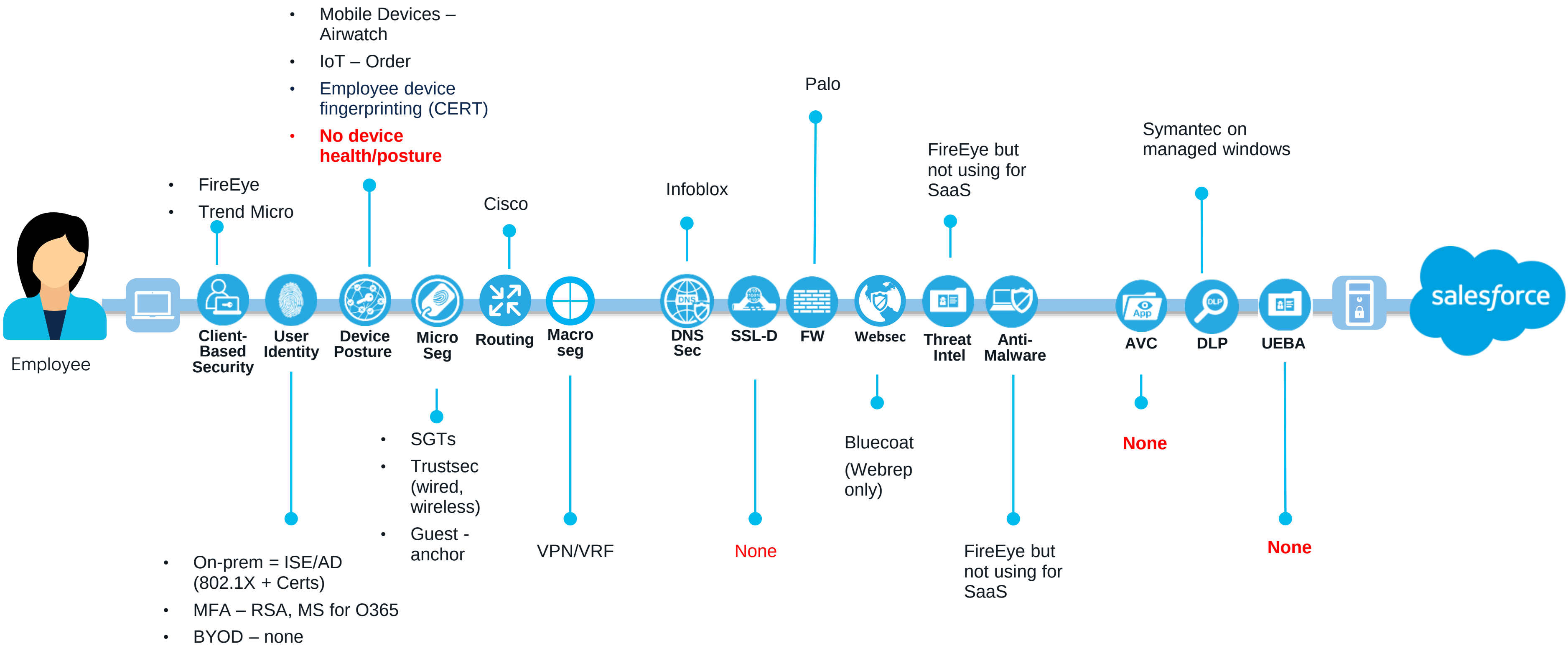
CONTINUOUSLY VERIFY TRUST

- Alert or block communications by continuously monitoring & responding to indicators of compromise



Customer Example - Document Capabilities per Use Case

Branch Employee to SaaS



Client-Based Security
- FireEye
- Trend Micro

User Identity
- On-prem = ISE/AD (802.1X + Certs)
- MFA – RSA, MS for O365
- BYOD – none

Device Posture
- Mobile Devices – Airwatch
- IoT – Order
- Employee device fingerprinting (CERT)
- **No device health/posture**

Micro Seg
- SGTs
- Trustsec (wired, wireless)
- Guest - anchor

Routing: Cisco

Macro seg: VPN/VRF

DNS Sec: Infoblox

SSL-D: None

FW: Palo

Websec: Bluecoat (Webrep only)

Threat Intel: FireEye but not using for SaaS

Anti-Malware: FireEye but not using for SaaS

AVC: **None**

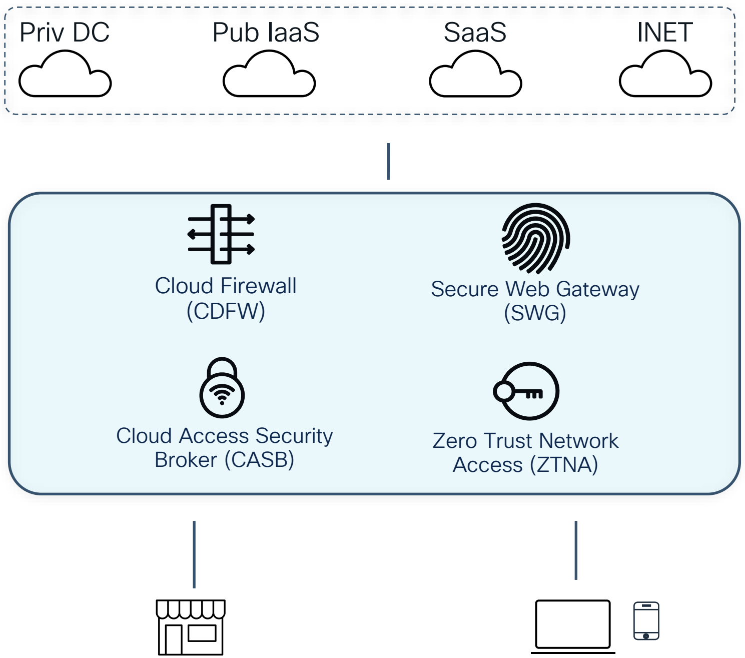
DLP: Symantec on managed windows

UEBA: **None**

Summary

SSE vs SASE

SSE



Priv DC

Pub IaaS

SaaS

INET

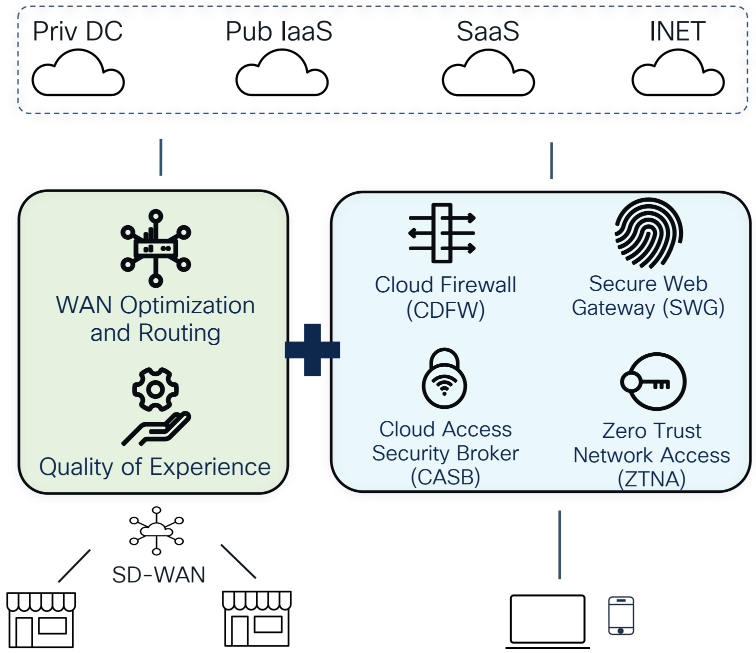
Cloud Firewall (CDFW)

Secure Web Gateway (SWG)

Cloud Access Security Broker (CASB)

Zero Trust Network Access (ZTNA)

SASE



Priv DC

Pub IaaS

SaaS

INET

WAN Optimization and Routing

Quality of Experience

Cloud Firewall (CDFW)

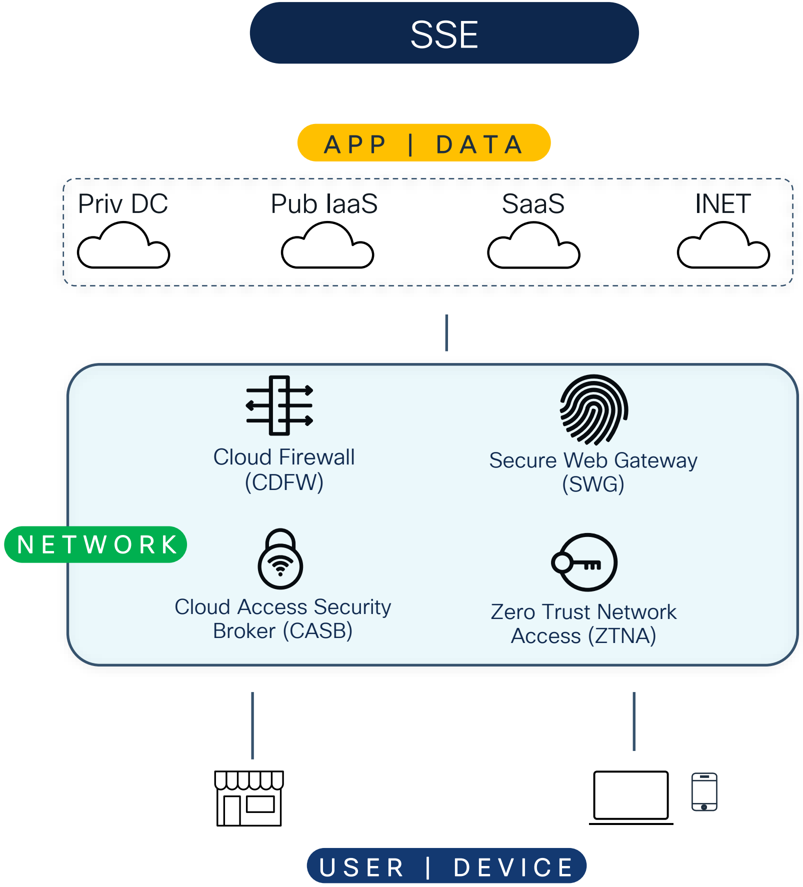
Secure Web Gateway (SWG)

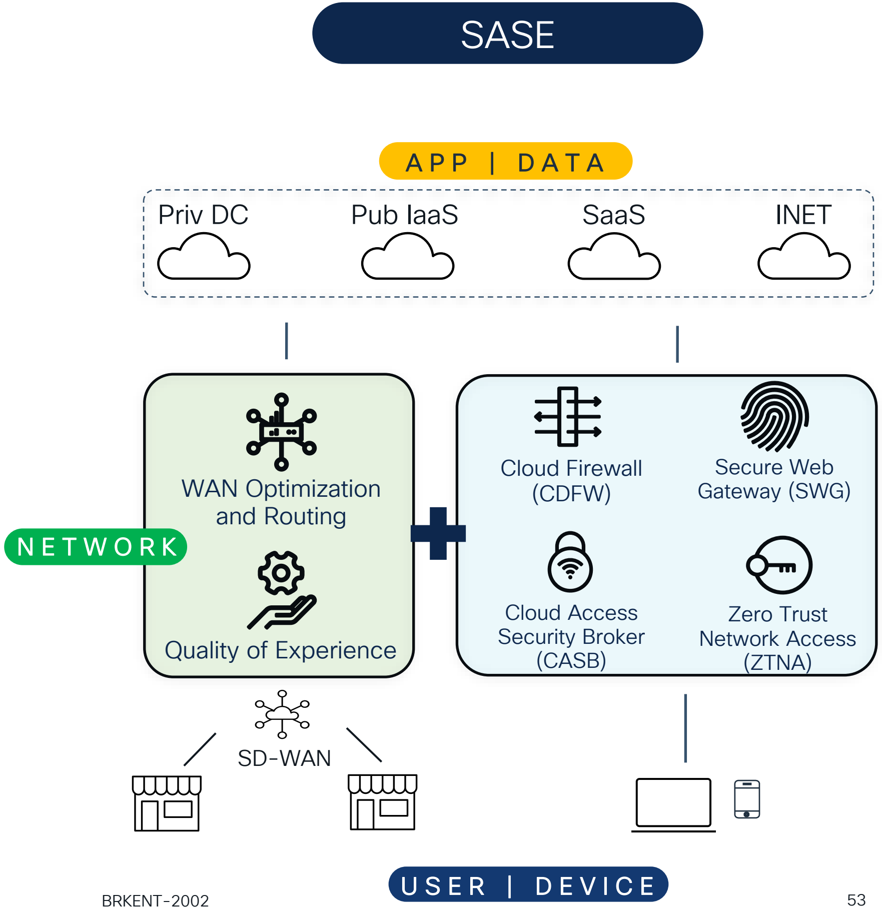
Cloud Access Security Broker (CASB)

Zero Trust Network Access (ZTNA)

SD-WAN

SSE / SASE adhering to Zero Trust Framework





SSE or SASE – which one?

I want a remote workforce solution that secures managed and unmanaged access to public and private applications, and consume it aaS → Secure Access (SSE)

I want to consolidate my security capabilities (FW, SWG, CASB, DLP, etc), and unify the UI/operations/support, and consume it aaS. → Secure Access (SSE)

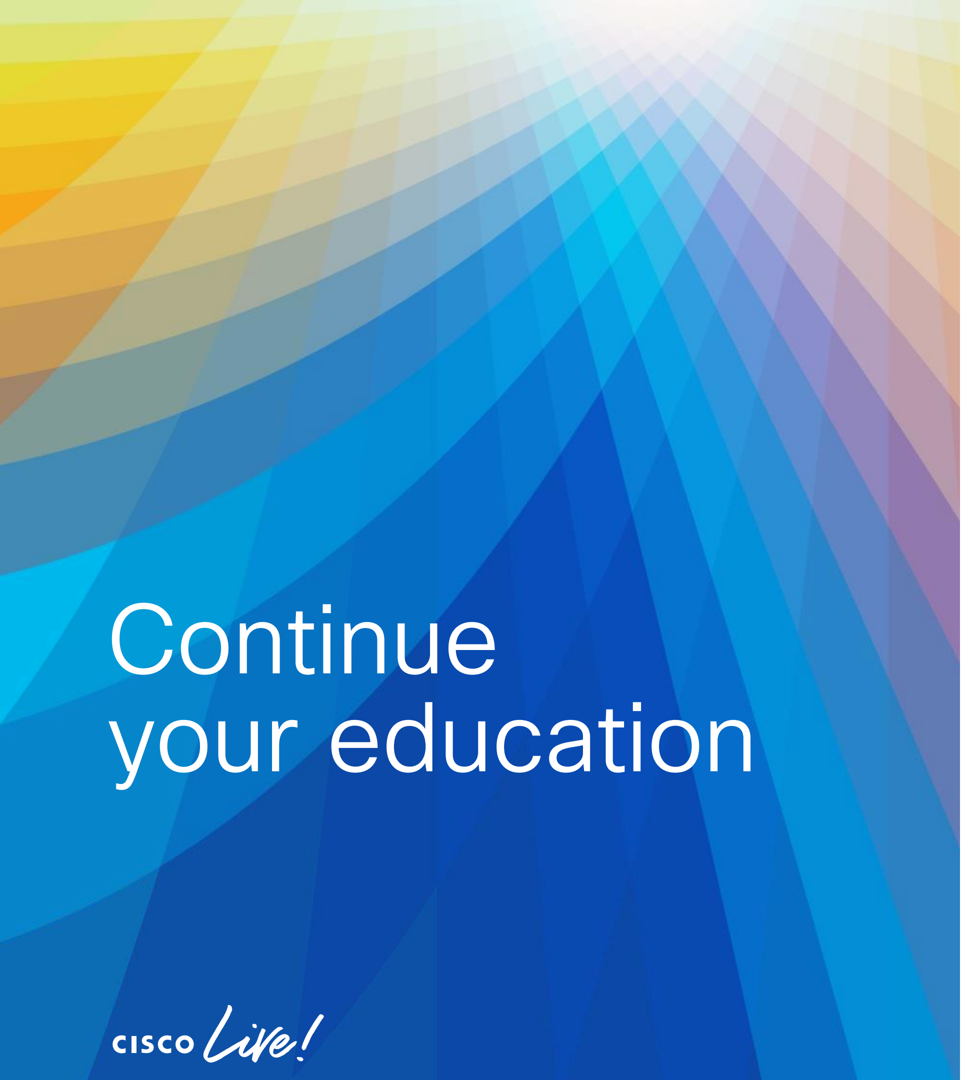
I want to consolidate my SD-WAN, security, and remote access capabilities, and unify the UI/operations/support, and consume it aaS. → Secure Connect (SASE)

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

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



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

The bridge to possible

Thank you

#CiscoLive

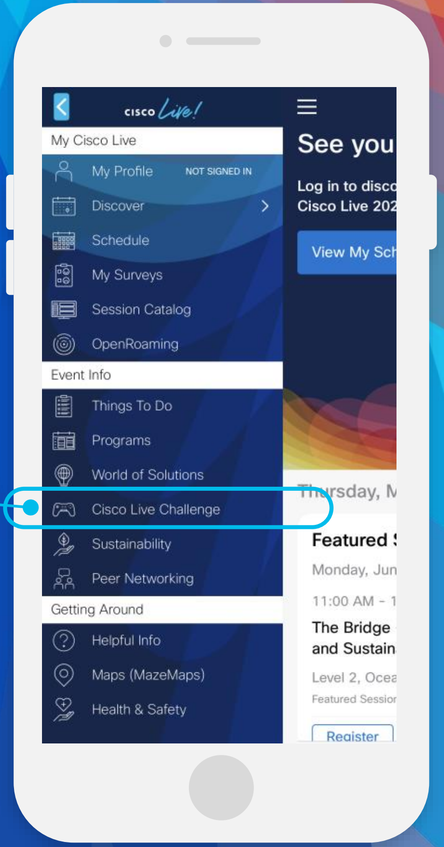
Cisco Live **Challenge**

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!

cisco Live!

Let's go

#CiscoLive