The bridge to possible

Cisco Secure Access

Poslednja Cisco SSE inovacija

Dragan Novaković
Security Solutions Engineer

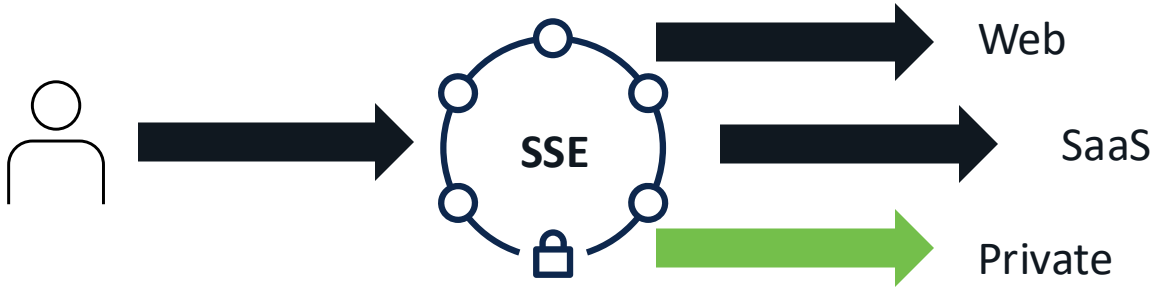
Agenda

- What is SSE?
- What problems can it solve?
- Cisco Secure Access
  - Architecture
  - Use Cases
  - Design & Admin Experience
- Q&A

What is SSE?

Security **S**ervice **E**dge

- Solution to secure access to Web, SaaS, and Private applications



- Protect users wherever they are, wherever they are going, all the time

What problems does SSE aim to solve?

Cisco Secure Access

- Consolidate Security & maintain consistent enforcement
- Provide flexible deployment options
- Enable a secure *hybrid* enterprise
- Offer Seamless admin & end user experience

Let’s get started!

Cisco Secure Access

Latest SSE from Cisco!

Core
Capabilities

- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB) & DLP
- Zero Trust Network Access (ZTNA)
- Firewall as a Service (FWaaS) & IPS

Beyond
Core Capabilities

- DNS Security
- Multimode DLP
- Remote Browser Isolation
- Advanced Malware Protection
- File Sandbox
- TALOS
- VPN as a Service

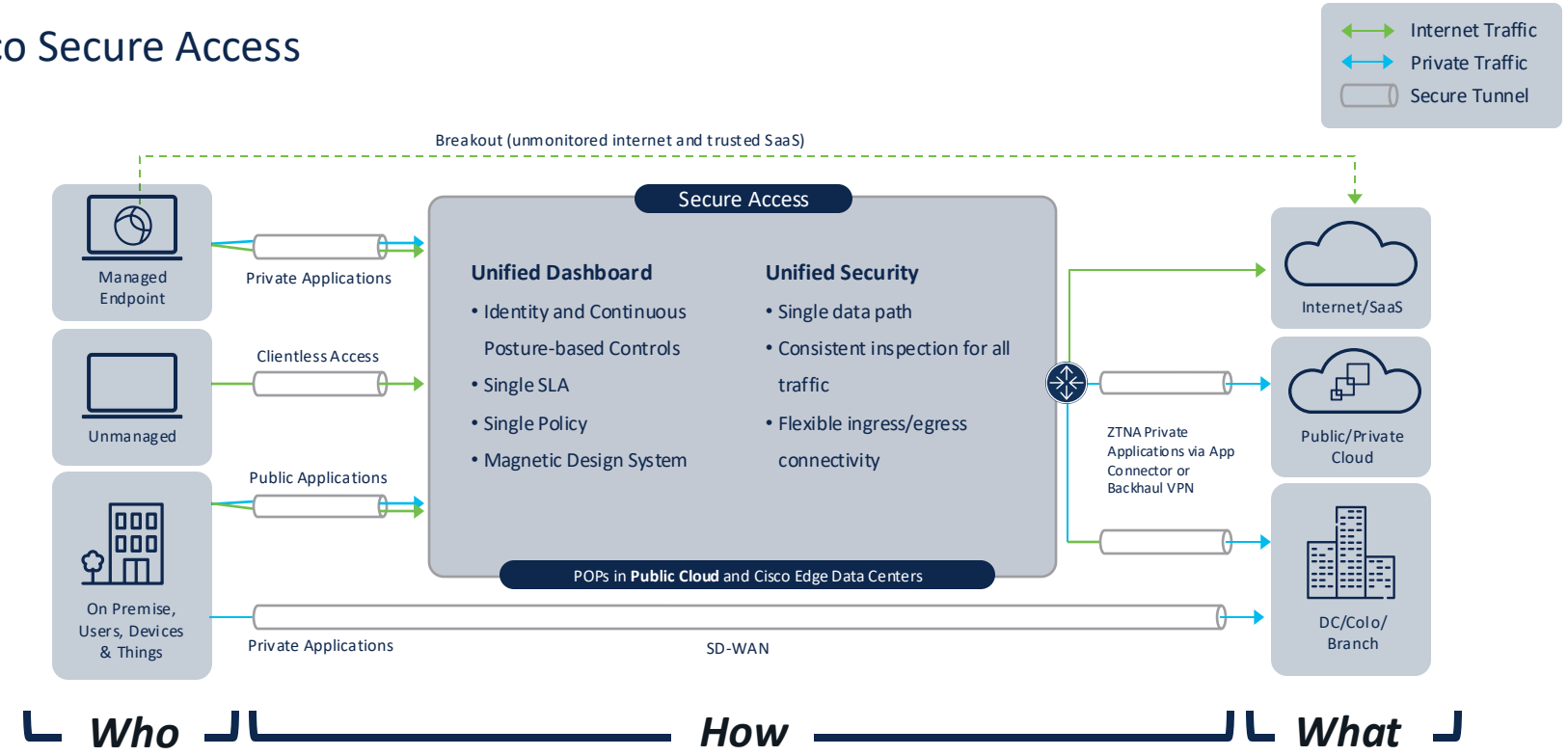
Even More…
Cisco value-add

- Cisco SD-WAN integration
- Synergistic Cisco solutions: DEM, XDR, DUO/SSO, CSPM, ISE and more
- 3rd party integrations (SD-WAN and other security tools)

Cisco Secure Access
Architecture

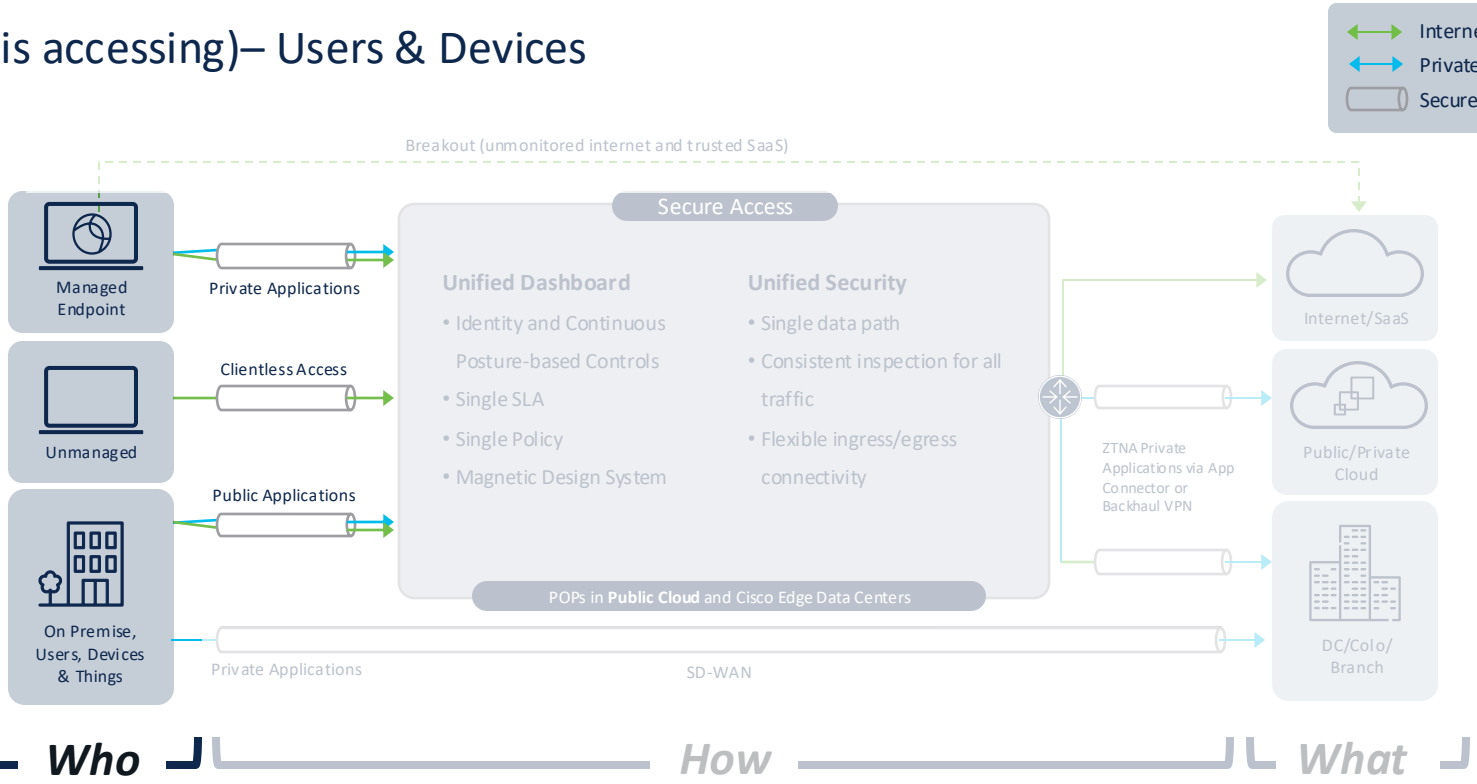
Architecture Overview

Cisco Secure Access



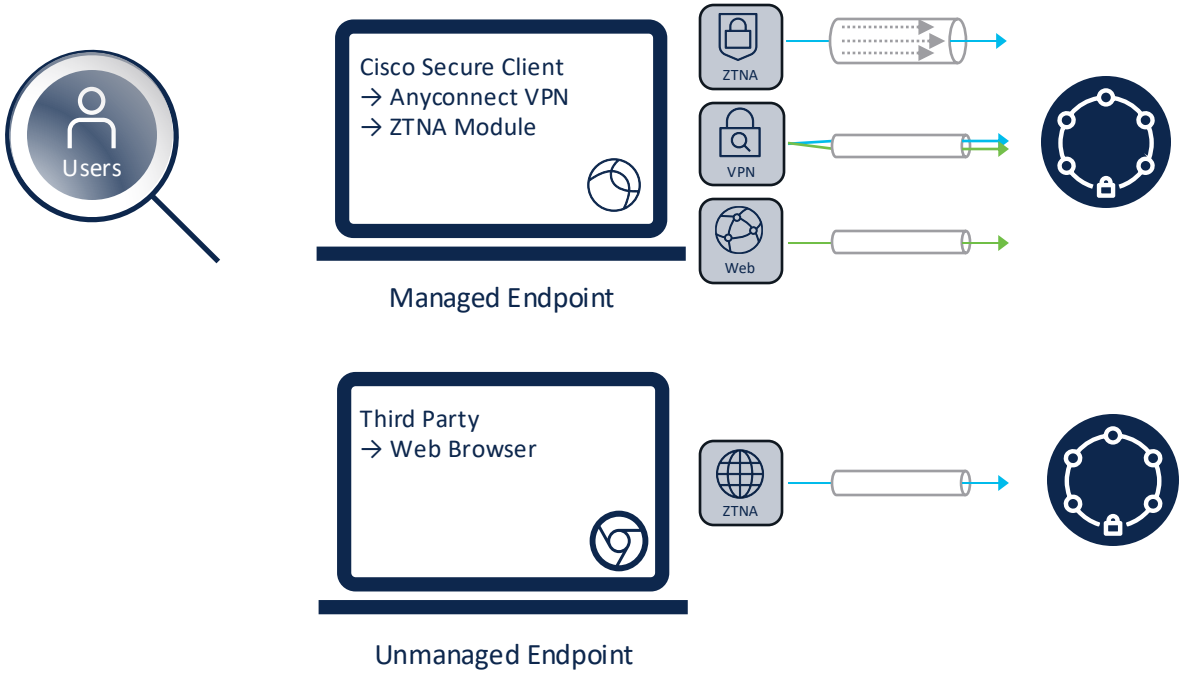
Architecture Detail

Who (is accessing)– Users & Devices



Architecture Detail

Who (is accessing)– Users & Devices



Anyconnect VPN
→ Authentication & Posture @ Connect time
→ TLS Tunnel
→ Carry Internet & Private Traffic (all ports)
→ SAML, (+) Cert, & (+) Multi-Cert Authentication

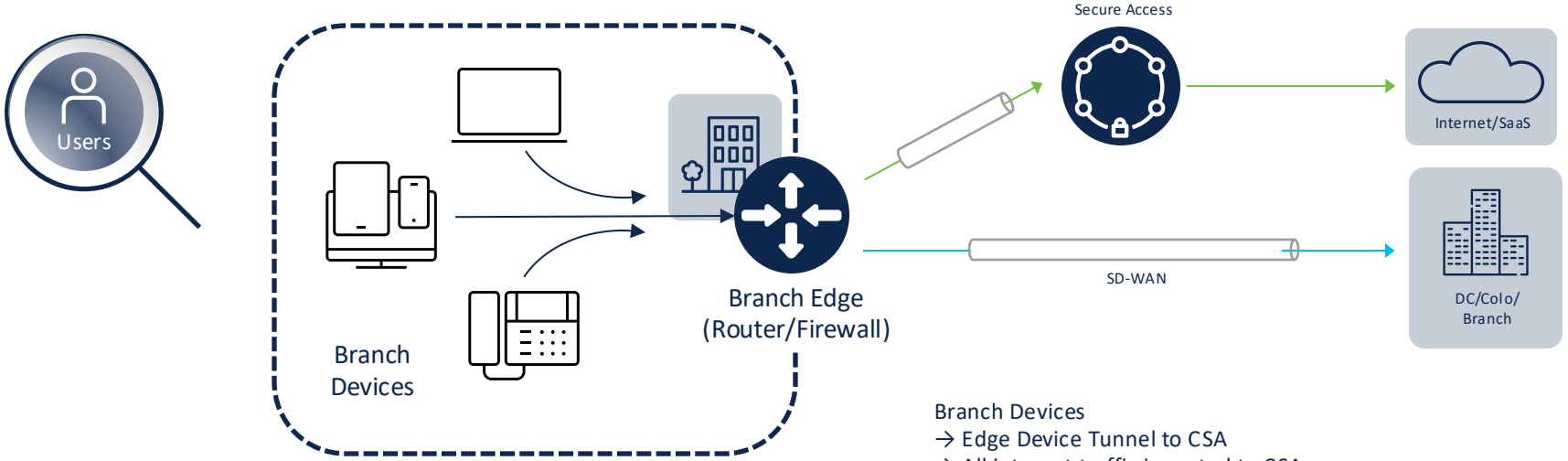
ZTNA Module
→ Authentication & Posture per connection
→ QUIC tunnel (MASQUE proxy)
→ Carry Private Traffic (All ports & protocols)
→ SAML Auth + Auto re-new

Web Roaming Module
→ Device Enrollment (profile)
→ Carry Internet Web Traffic (80/443)

Clientless ZTNA
→ Accessible from any browser that supports SAML/Cookies
→ Request based posture (geolocation, browser version, OS)
→ Web Apps Only

Architecture Detail

Who (is accessing)– Users & Devices

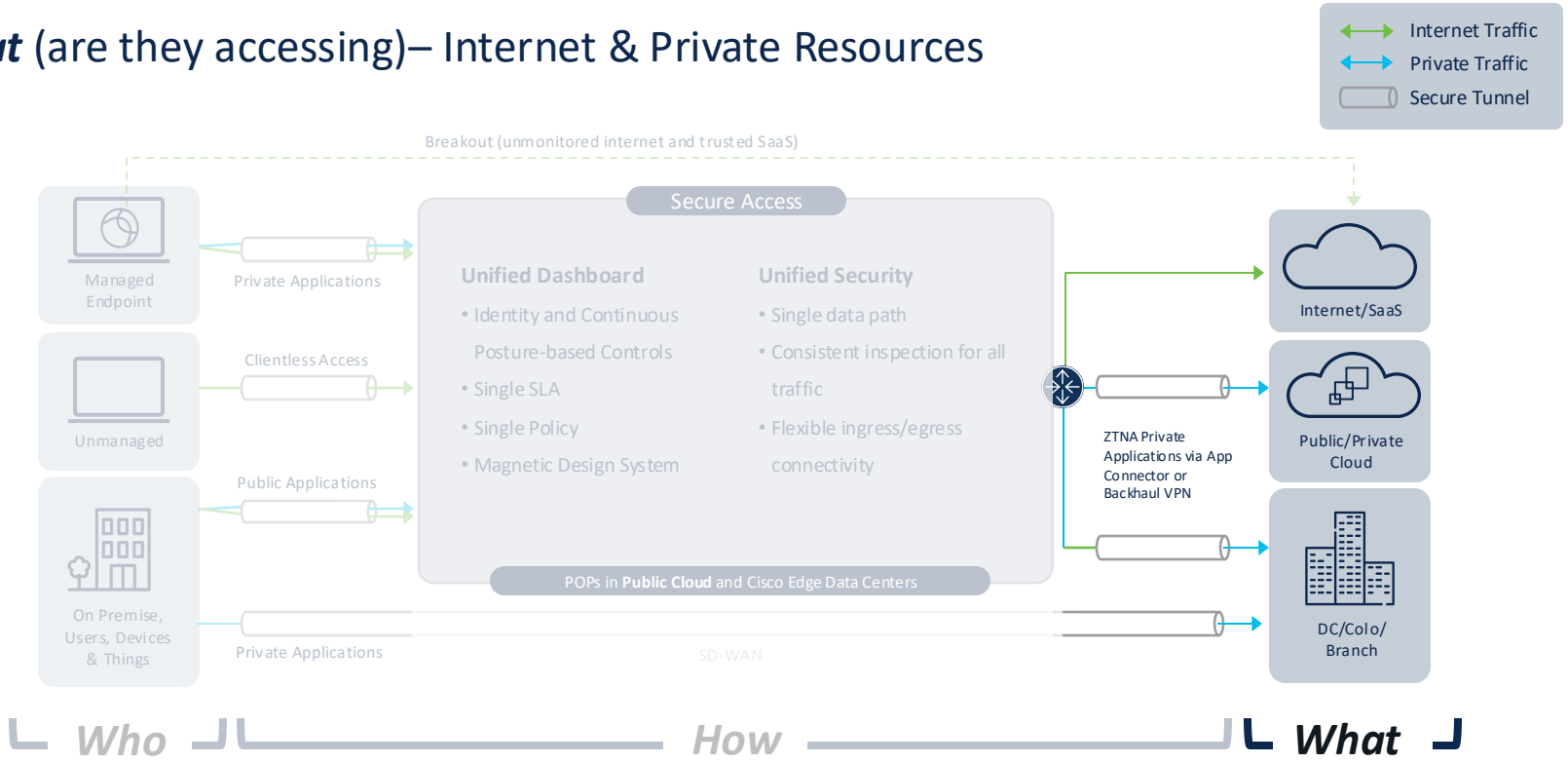


Branch Devices
→ Edge Device Tunnel to CSA
→ All internet traffic is routed to CSA
→ Auto Tunnels with Viptela SD-WAN DIA branches
→ Private traffic respects optimized SD-WAN*

* ZTNA use case changes behavior in certain scenarios (will be covered later)

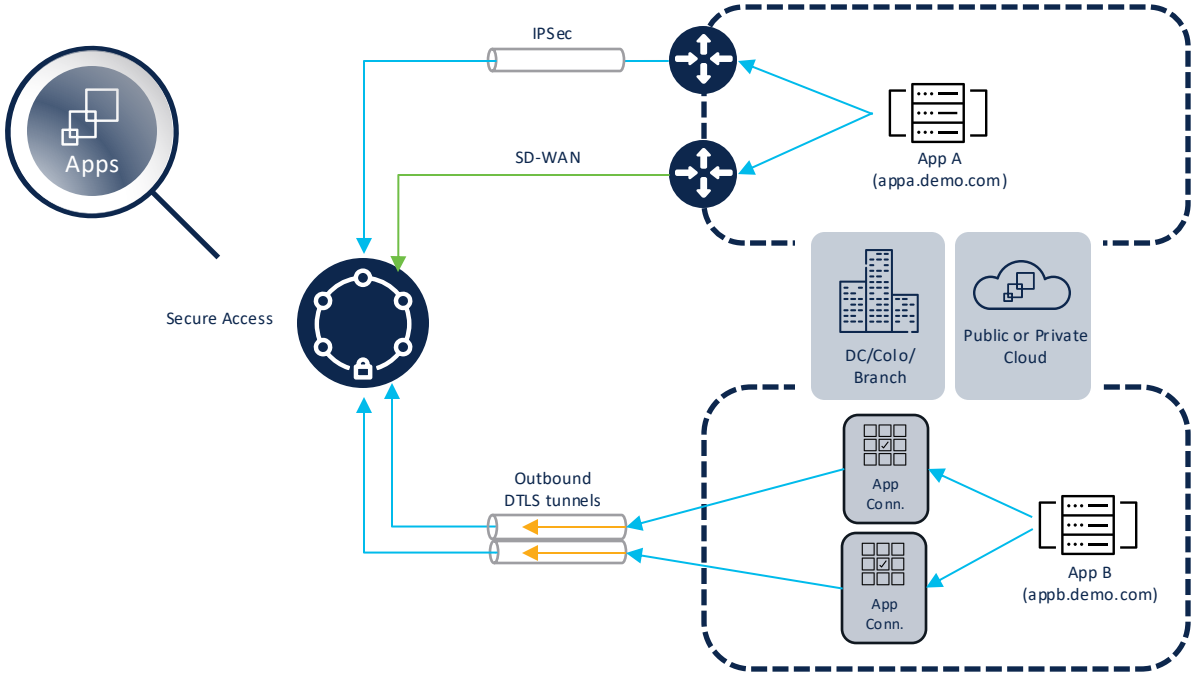
Architecture Detail

What (are they accessing)– Internet & Private Resources



Architecture Detail

What (are they accessing)–Private Resources

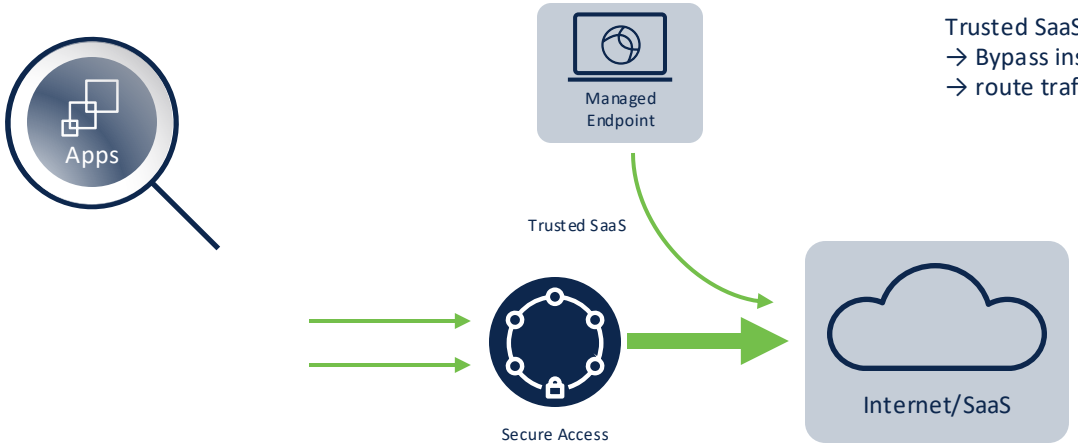


Network Tunnel
→ IPSec Backhaul
→ Automated SD-WAN Backhaul
→ Static or BGP based routing
→ Auto Failover/ Redundancy

Application Connector
→ Software deployment (VM or Cloud Instance)
→ Deploy closest to application
→ Outbound connectivity (no holes in firewall)
→ Auto failover / load balancing

Architecture Detail

What (are they accessing)–Internet

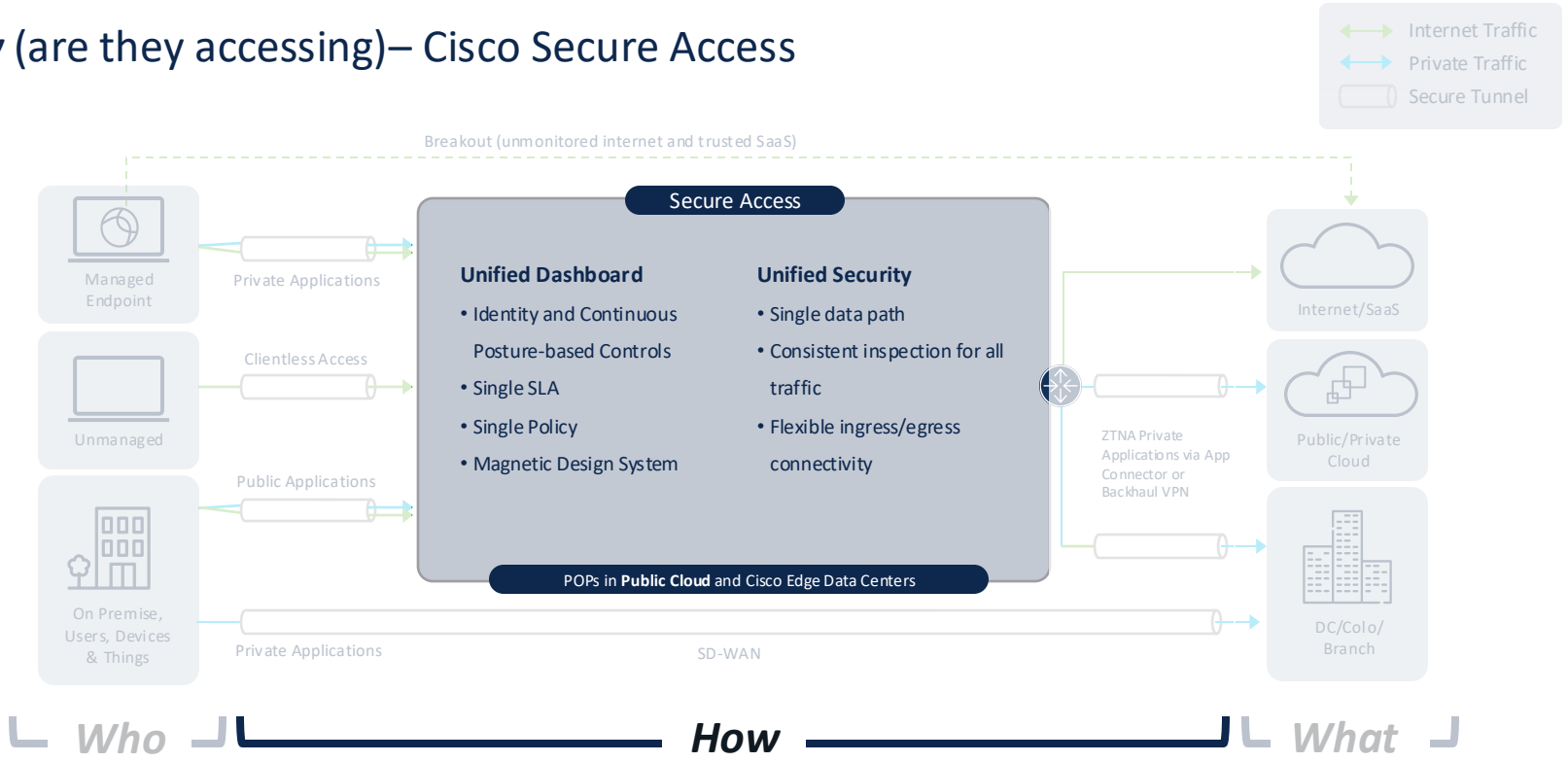


Trusted SaaS / Bypass
→ Bypass inspection for trusted web applications
→ route traffic directly to internet from host

Secure Internet Access
→ All internet traffic filtered through CSA
→ Branch traffic routed via network and IP sec Tunnel
→ Remote traffic acquired via Secure Client

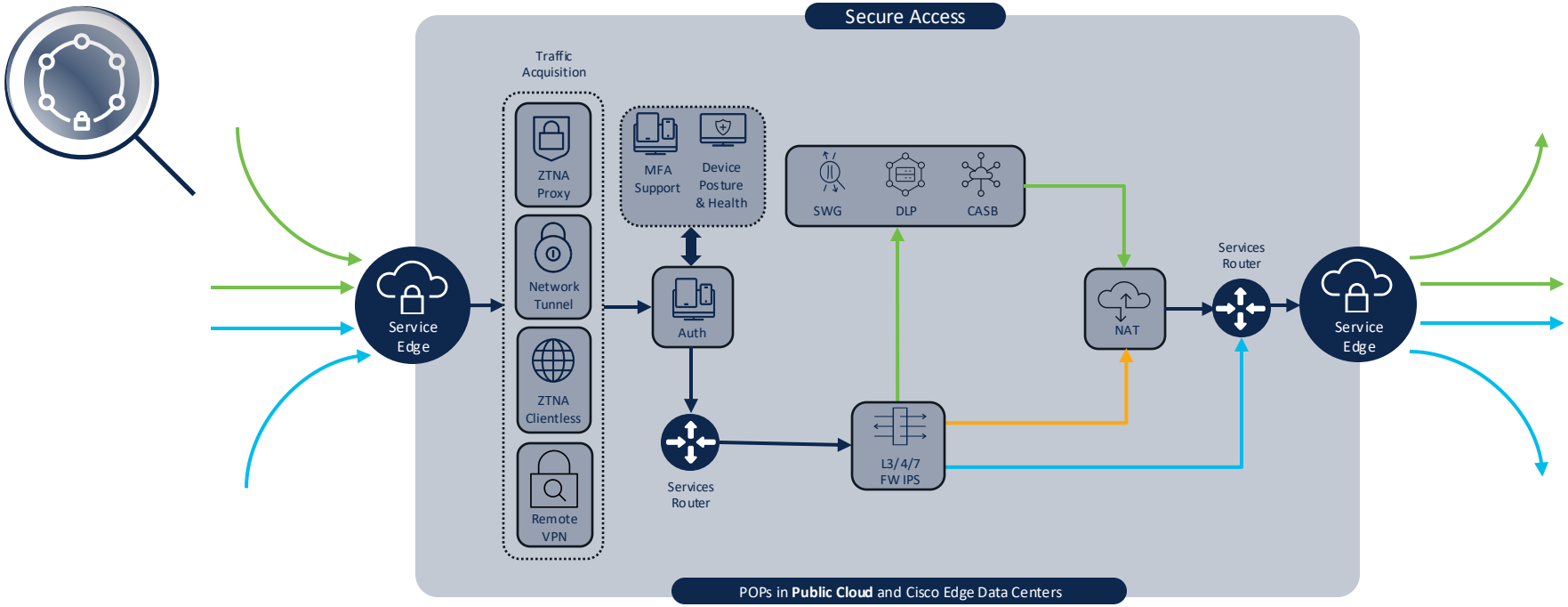
Architecture Detail

How (are they accessing)– Cisco Secure Access



Architecture Detail

How (are they accessing)– Cisco Secure Access

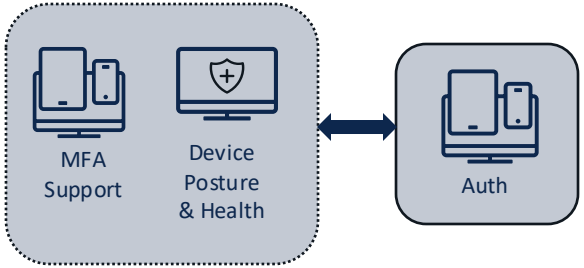


Architecture Detail

How (are they accessing)– Cisco Secure Access (Authentication)

MFA Support
→ Layer MFA via SAML Provider
→ Native browser based authentication (support WebAuth etc.)

Authentication
→ IdP/CSV/AD Sync User Provisioning
→ SAML Authentication



Device Posture & Health
→ Operating System
→ Geolocation Check (Policy)
→ Firewall
→ Disk Encryption
→ Browser Check
→ Anti-Malware
→ File Check
→ Registry Check (windows only)
→ Process Check
→ System Password
→ Certificate Check

Architecture Detail

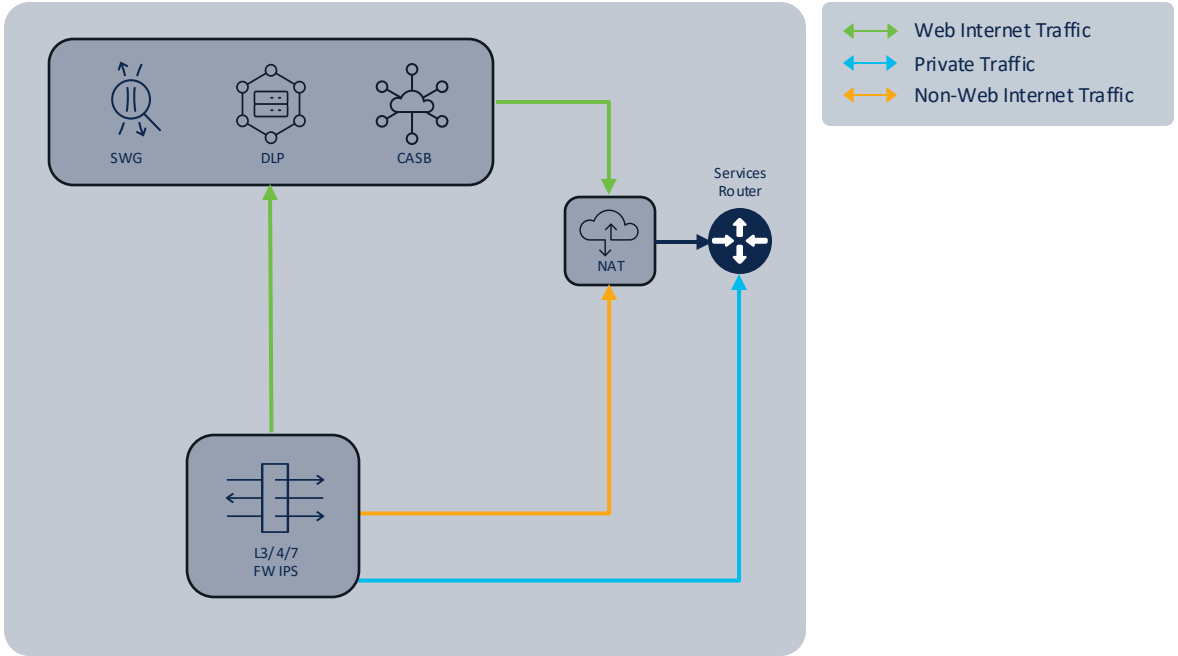
How (are they accessing)– Cisco Secure Access (Security Inspection)

SWG (Secure Web Gateway)
→ Full forward proxy
→ TLS Decryption (Internet)
→ Inline SAML authentication
→ Cloud Tennant Controls

DLP (Data Loss Prevention)
→ Exact Data Matching
→ Inline detection & prevention
→ Out of Band Detection and remediation

CASB (Cloud Access Security Broker)
→ Tunable Application Control
→ Inline detection & prevention
→ Out of Band Detection and remediation

L3-7 Firewall (Transparent)
→ Intent based policy
→ TLS Decryption
→ IPS signature detection and/or prevention



Cisco Secure Access

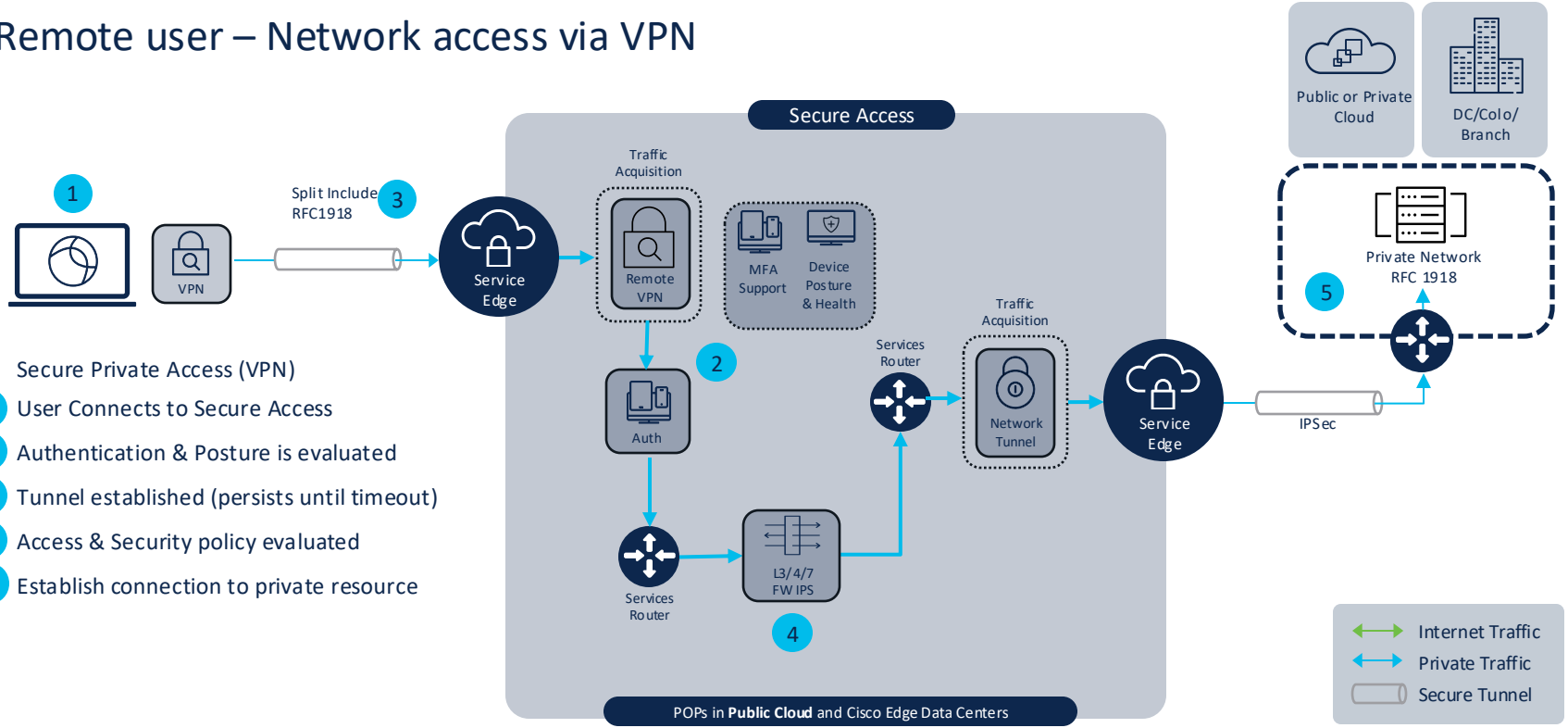
Use Cases

Use Case Summary

- Private Network Access
- Remote User needs access to Private Network
  - Remote Access VPN connection
  - Roaming User (Secure Client)
  - Onsite (SD-WAN)
  - Application in Private DC / Public Cloud

Private Network Access

Remote user – Network access via VPN



Secure Private Access (VPN)

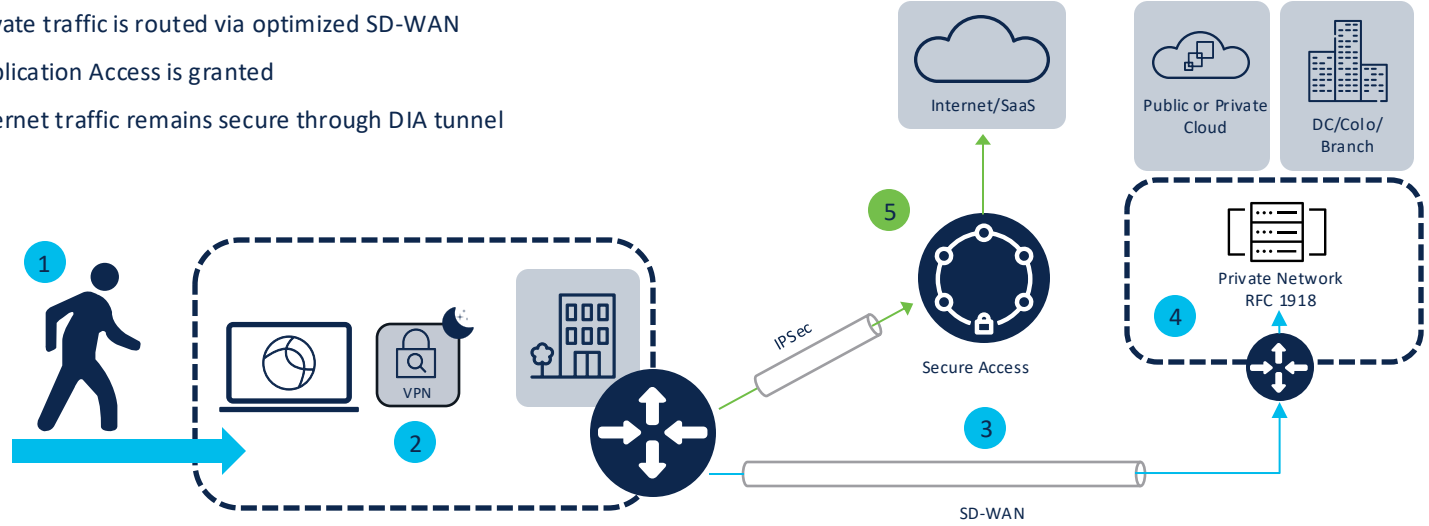
1. User Connects to Secure Access
2. Authentication & Posture is evaluated
3. Tunnel established (persists until timeout)
4. Access & Security policy evaluated
5. Establish connection to private resource

Private Network Access

Onsite user – Network access via SD-WAN

Secure Private Access (SD-WAN)

1. User Comes Onsite
2. Secure Client VPN goes to sleep (Trusted Network)
3. Private traffic is routed via optimized SD-WAN
4. Application Access is granted
5. Internet traffic remains secure through DIA tunnel

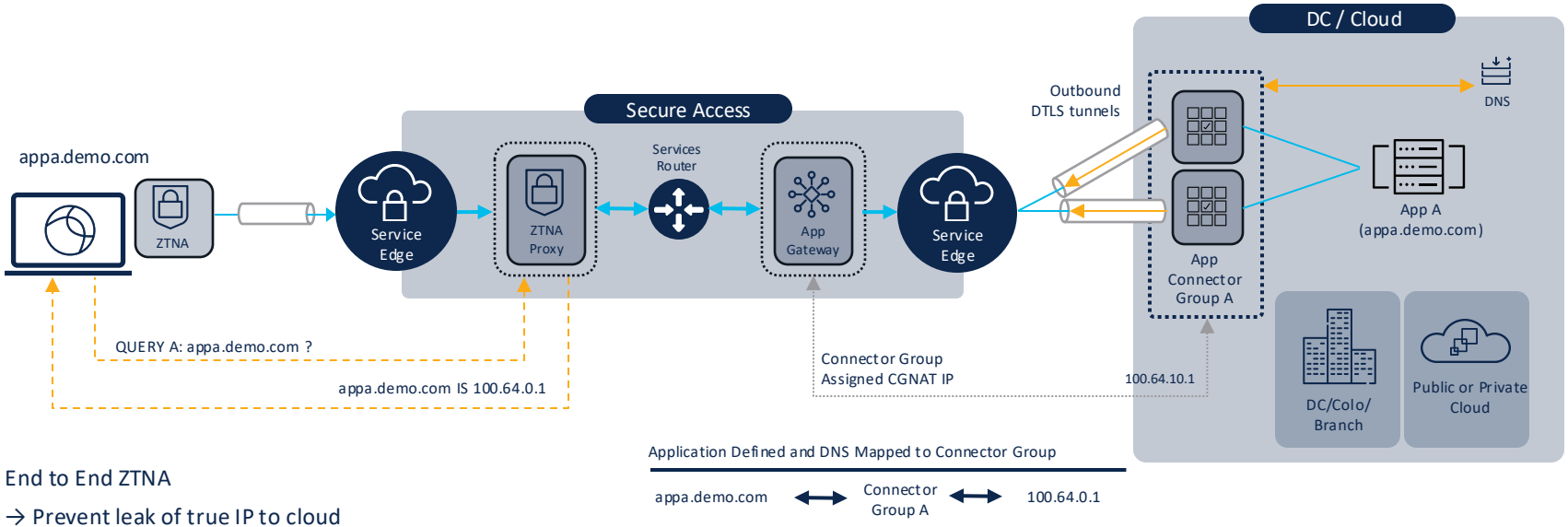


Use Case Summary

- Private Application Access
- Remote User needs access to ZTNA Application
  - Secure Client ZTNA Module
  - Consistent when Roaming & Onsite
  - Application in Private DC / Public Cloud
    - Private application accessed via IPsec
    - Private application accessed via Application Connector

ZTNA End-to-End Architecture

ZTNA Architecture



End to End ZTNA

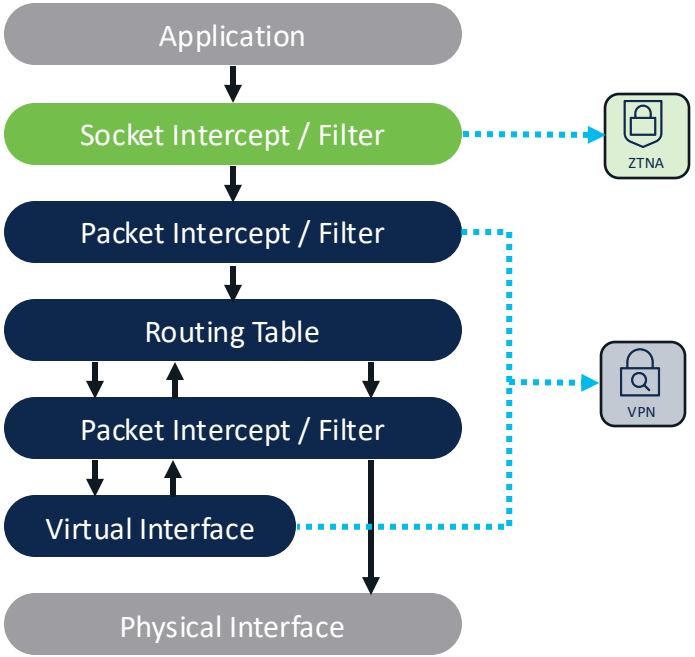
→ Prevent leak of true IP to cloud

→ Per connection security

→ Dynamic App Connector Group selection (Can have multiple)

ZTNA Architecture

Module Socket Interception



Socket Filter Advantages

→ Control of over DNS and application traffic *before* VPN

→ No route table manipulation

→ Capture Traffic based on FQDN, Wildcard, IP, or CIDR

→ Interoperate with existing Cisco & Non-Cisco VPN solutions

ZTNA Architecture

Why MASQUE?

No direct application access – Proxy Architecture

Broad application support; TCP, UDP, IP

Fallback to HTTP/2 (TCP) of QUIC is blocked (UDP)

Per-Connection, application, or device tunnels

Native device OS Support (no added client)

ZTNA Architecture

Why QUIC?

Fast Connection times (0-RTT)

UDP transport (safe from TCP Meltdown)

Change IPs without renegotiation (Connection migration)

No head-of-line blocking (Stream Multiplexing)

Individually encrypted packets

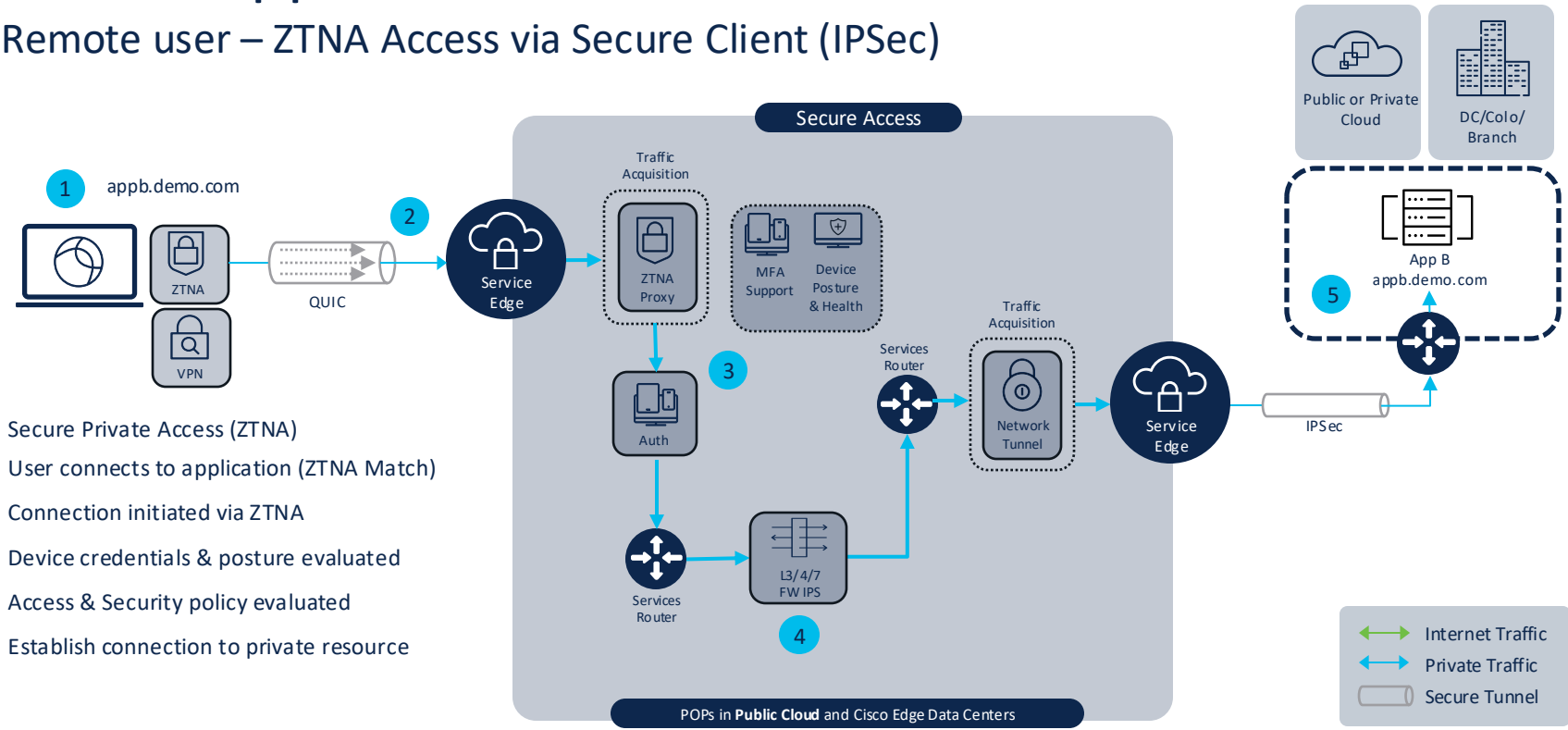
Can simultaneously use multiple interfaces (Multipath)

Cisco Secure Access

Use Cases (Cont.)

Private Application Access

Remote user – ZTNA Access via Secure Client (IPSec)

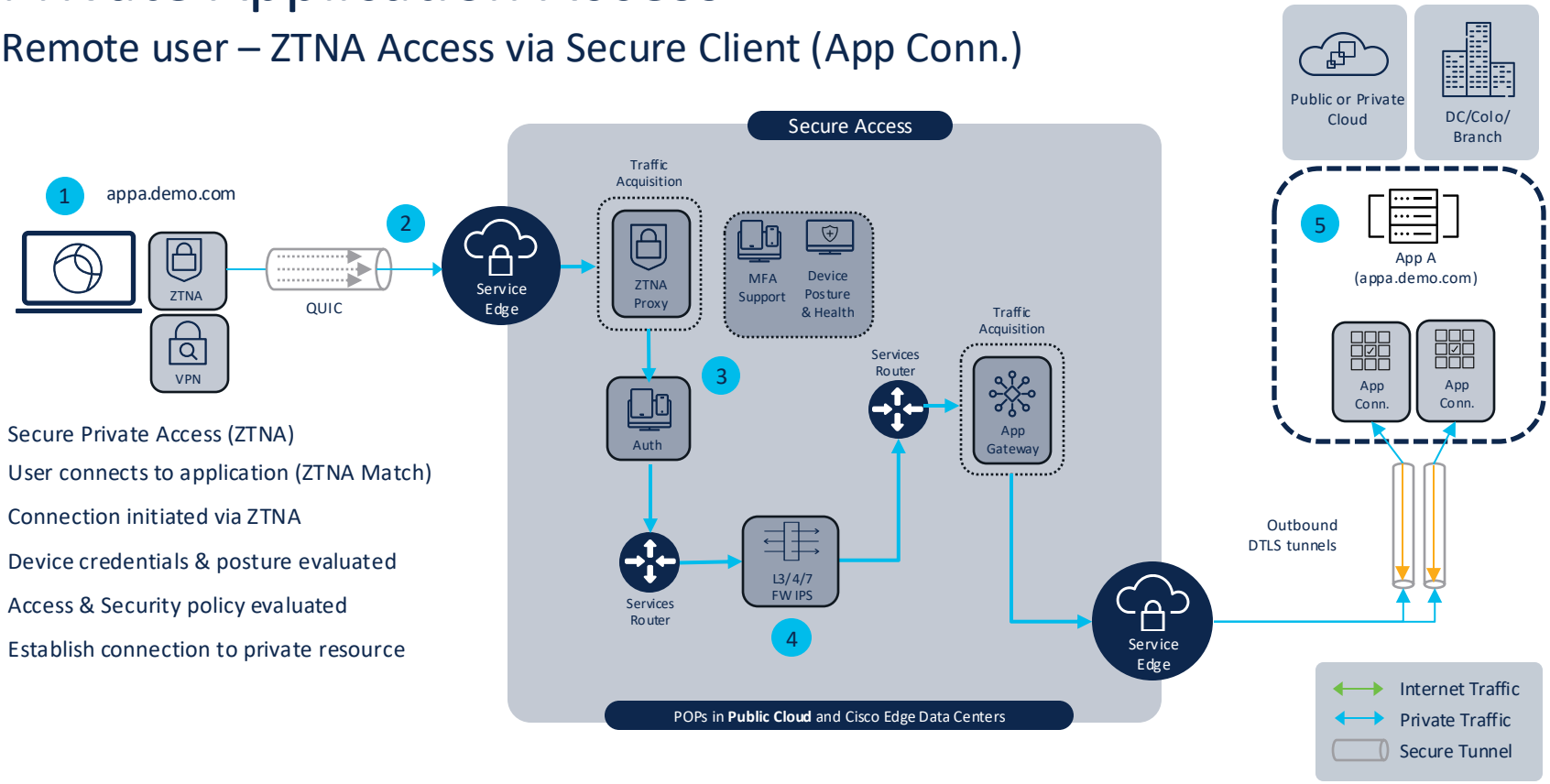


Secure Private Access (ZTNA)

1. User connects to application (ZTNA Match)
2. Connection initiated via ZTNA
3. Device credentials & posture evaluated
4. Access & Security policy evaluated
5. Establish connection to private resource

Private Application Access

Remote user – ZTNA Access via Secure Client (App Conn.)



Secure Private Access (ZTNA)

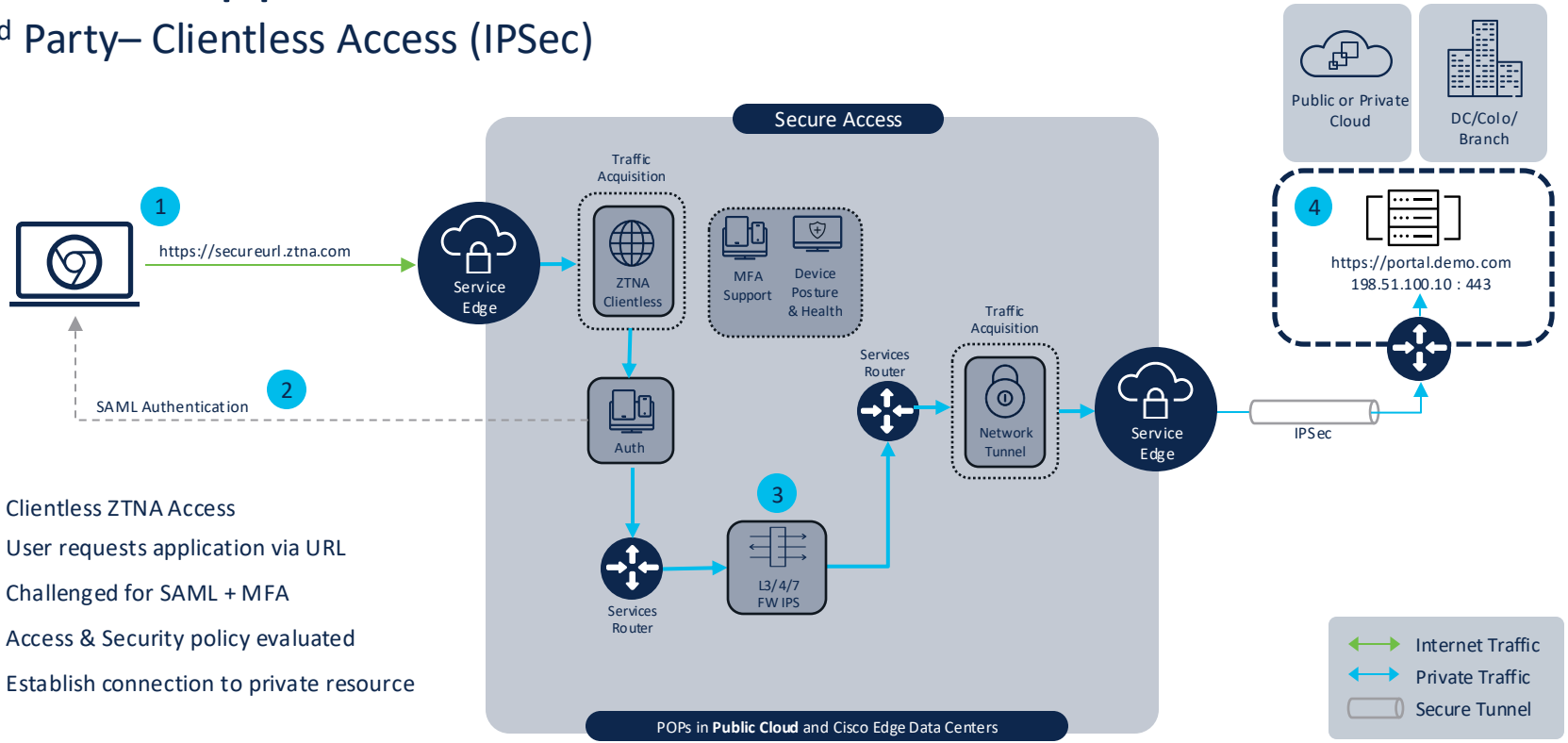
1. User connects to application (ZTNA Match)
2. Connection initiated via ZTNA
3. Device credentials & posture evaluated
4. Access & Security policy evaluated
5. Establish connection to private resource

Use Case Summary

- Private Application Access
- 3rd Party needs access to private resource
- ZTNA Controls
- Browser based access (Clientless)
  - Private application accessed via IPsec
  - Private application accessed via Application Connector

Private Application Access

3rd Party– Clientless Access (IPSec)

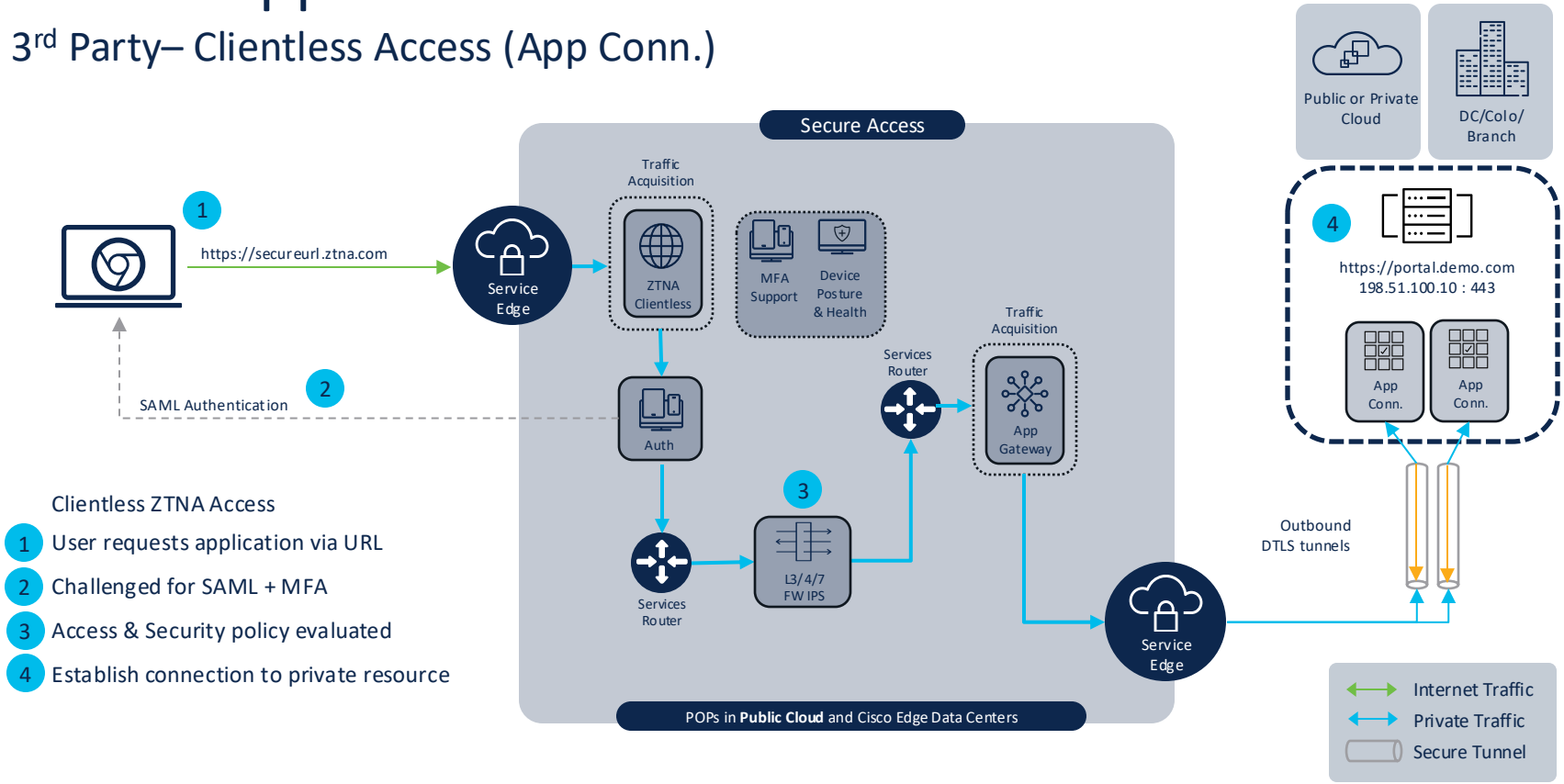


Clientless ZTNA Access

1. User requests application via URL
2. Challenged for SAML + MFA
3. Access & Security policy evaluated
4. Establish connection to private resource

Private Application Access

3rd Party– Clientless Access (App Conn.)



Clientless ZTNA Access

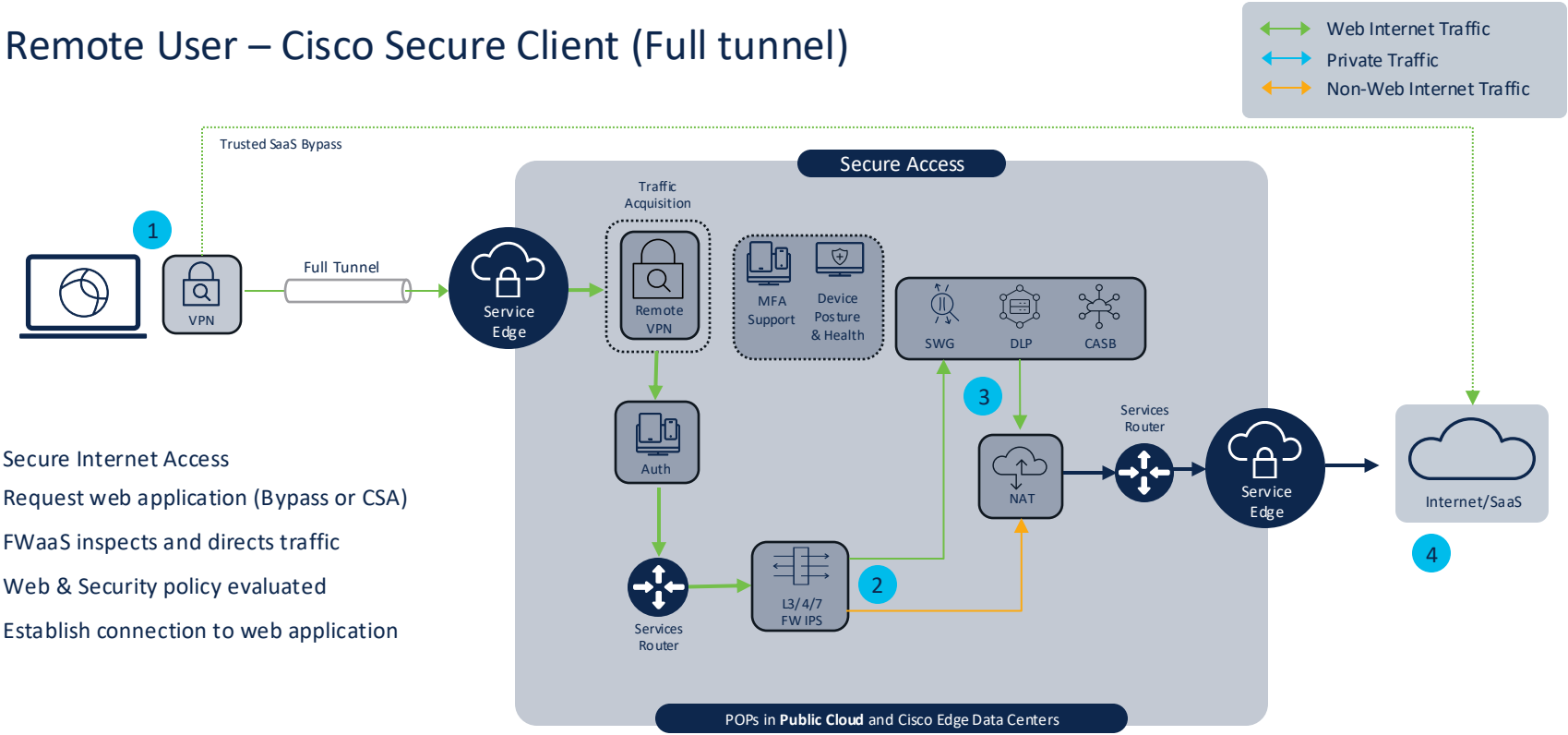
1. User requests application via URL
2. Challenged for SAML + MFA
3. Access & Security policy evaluated
4. Establish connection to private resource

Use Case Summary

- Secure Internet Access
- Managed endpoints
  - Secure Client
  - Remote users
  - Onsite Users
- Unmanaged endpoints
  - In branch – OT/IoT devices

Secure Internet Access

Remote User – Cisco Secure Client (Full tunnel)

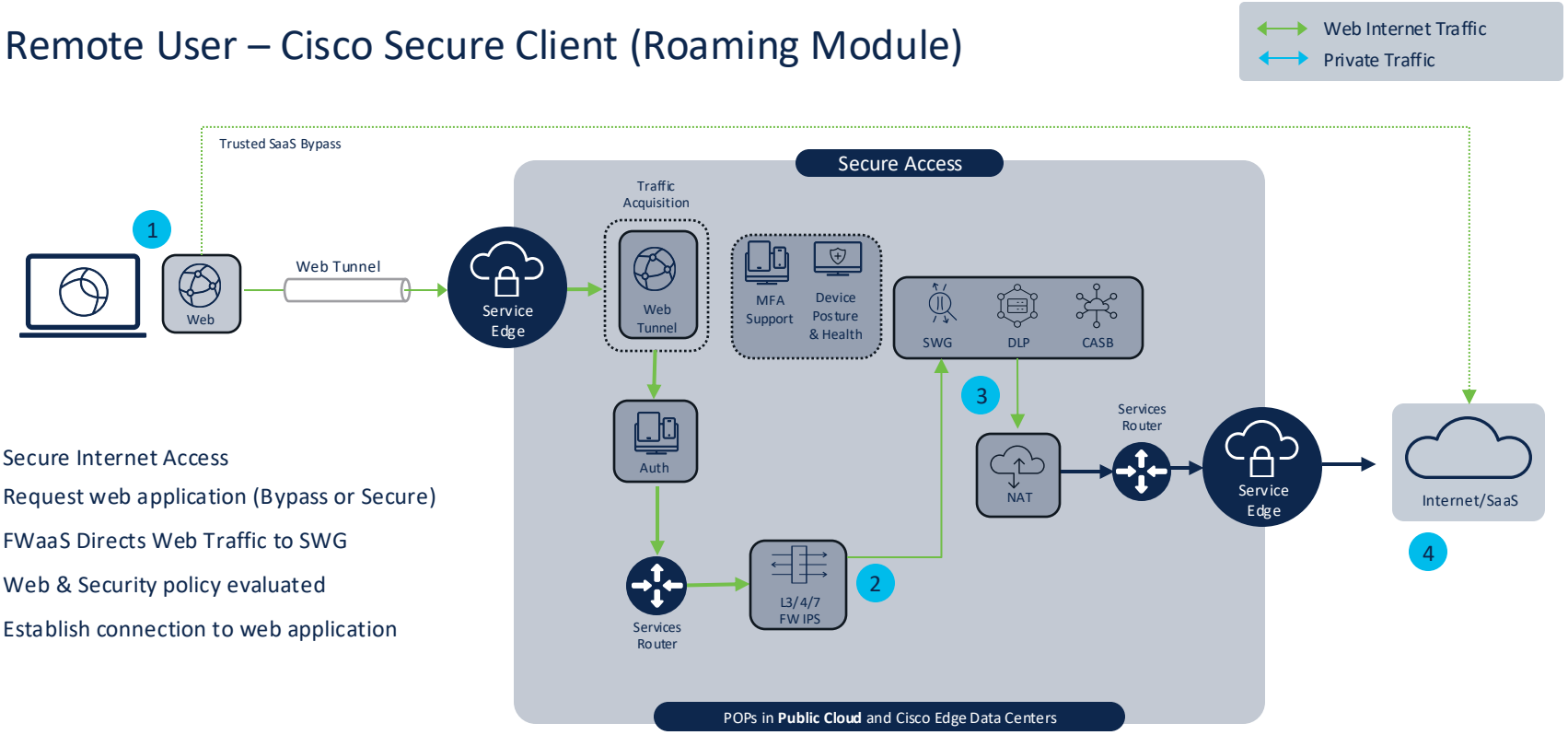


Secure Internet Access

1. Request web application (Bypass or CSA)
2. FWaaS inspects and directs traffic
3. Web & Security policy evaluated
4. Establish connection to web application

Secure Internet Access

Remote User – Cisco Secure Client (Roaming Module)

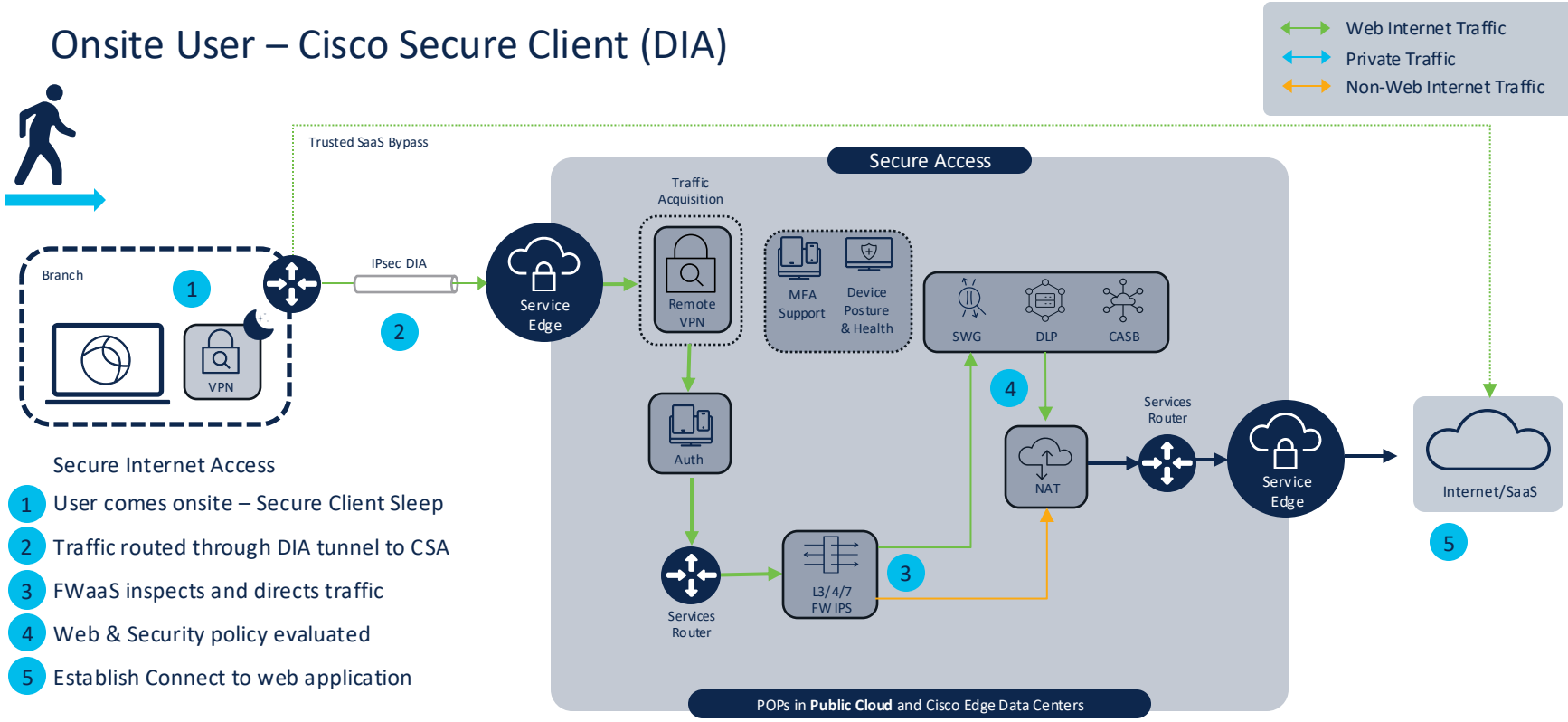


Secure Internet Access

1. Request web application (Bypass or Secure)
2. FWaaS Directs Web Traffic to SWG
3. Web & Security policy evaluated
4. Establish connection to web application

Secure Internet Access

Onsite User – Cisco Secure Client (DIA)

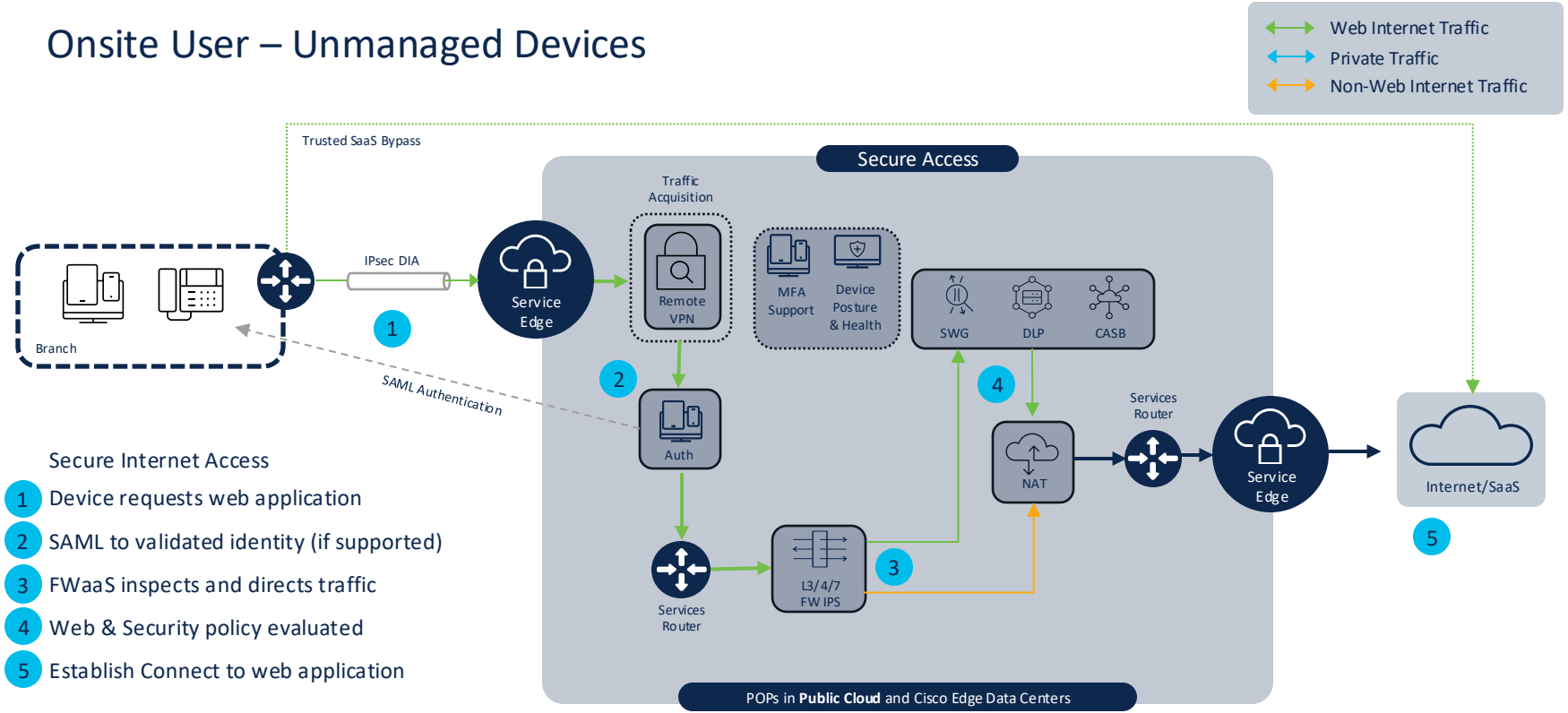


Secure Internet Access

1. User comes onsite – Secure Client Sleep
2. Traffic routed through DIA tunnel to CSA
3. FWaaS inspects and directs traffic
4. Web & Security policy evaluated
5. Establish Connect to web application

Secure Internet Access

Onsite User – Unmanaged Devices



Secure Internet Access

1. Device requests web application
2. SAML to validated identity (if supported)
3. FWaaS inspects and directs traffic
4. Web & Security policy evaluated
5. Establish Connect to web application

Cisco Secure Access
Design & Admin Experience

Design and Experience Challenges

Does more flexibility mean more complex?

- Flexible deployment options
- Numerous ways for end users to connect
- Different policy / inspection for different traffic
- Enterprise scale

All New UI Designed with Admin Experience as #1 Priority

Magnetic Design System

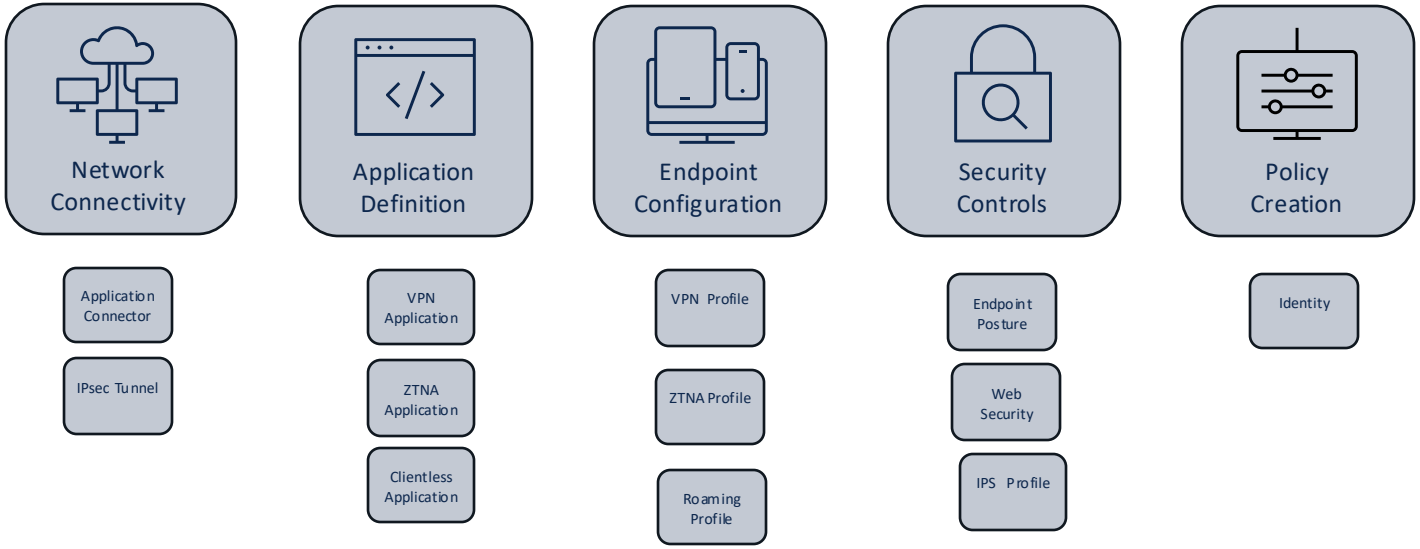
Modular, simple, effective

What does Magnetic mean for Cisco Secure Access?

> “Throughout using the product, the admin’s intent is kept at the forefront, while the complexity of the underlying engines is hidden to ensure a simplified, user-friendly experience.”
>
> Magnetic

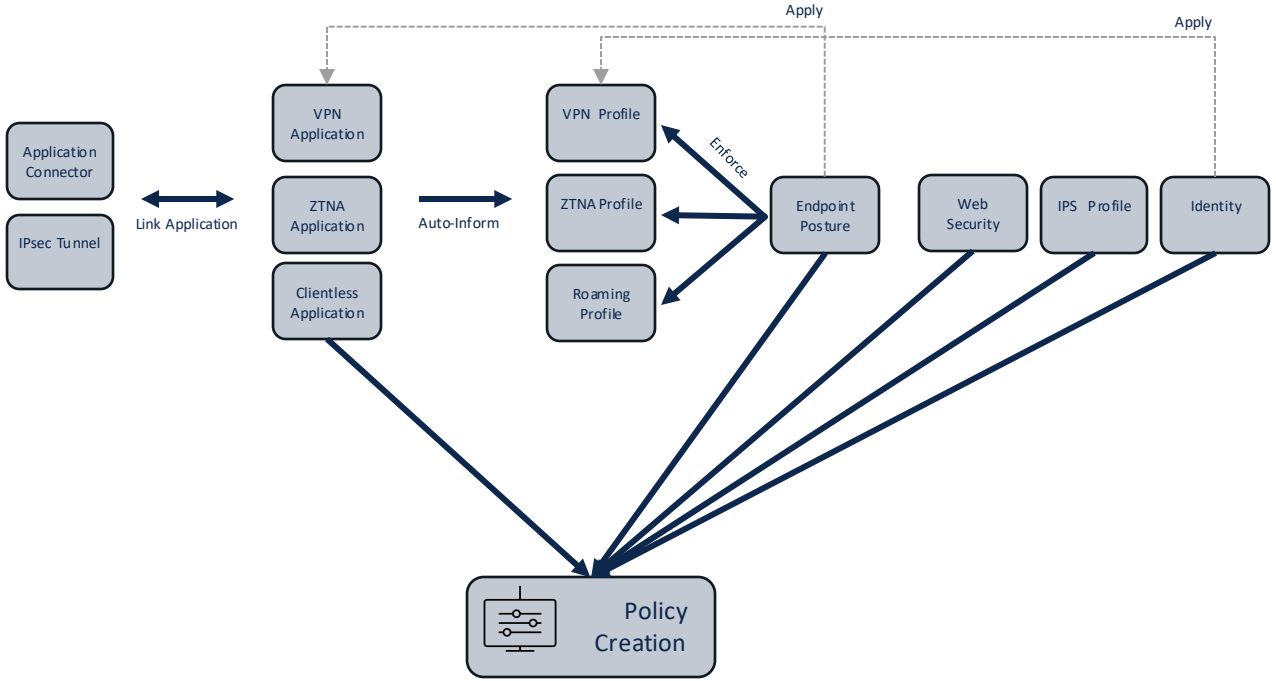
Building Blocks

The Modular pieces of Configuration



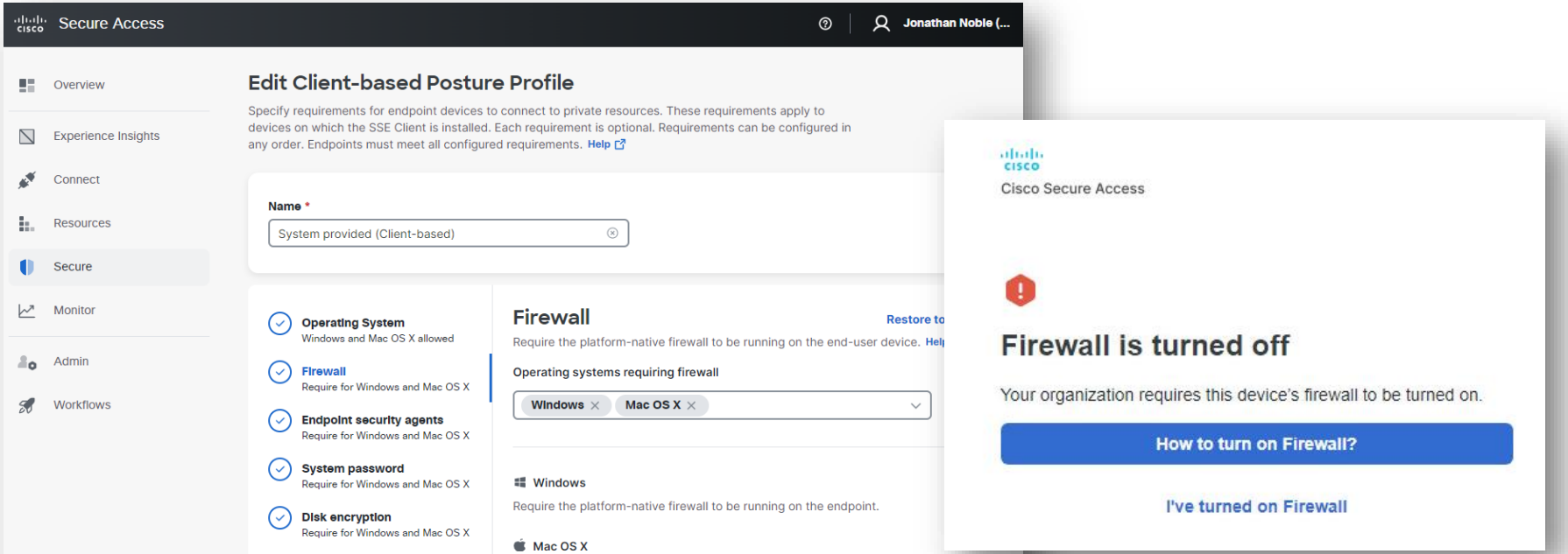
Configure Once - Use Everywhere

Example Use Case – Private Access



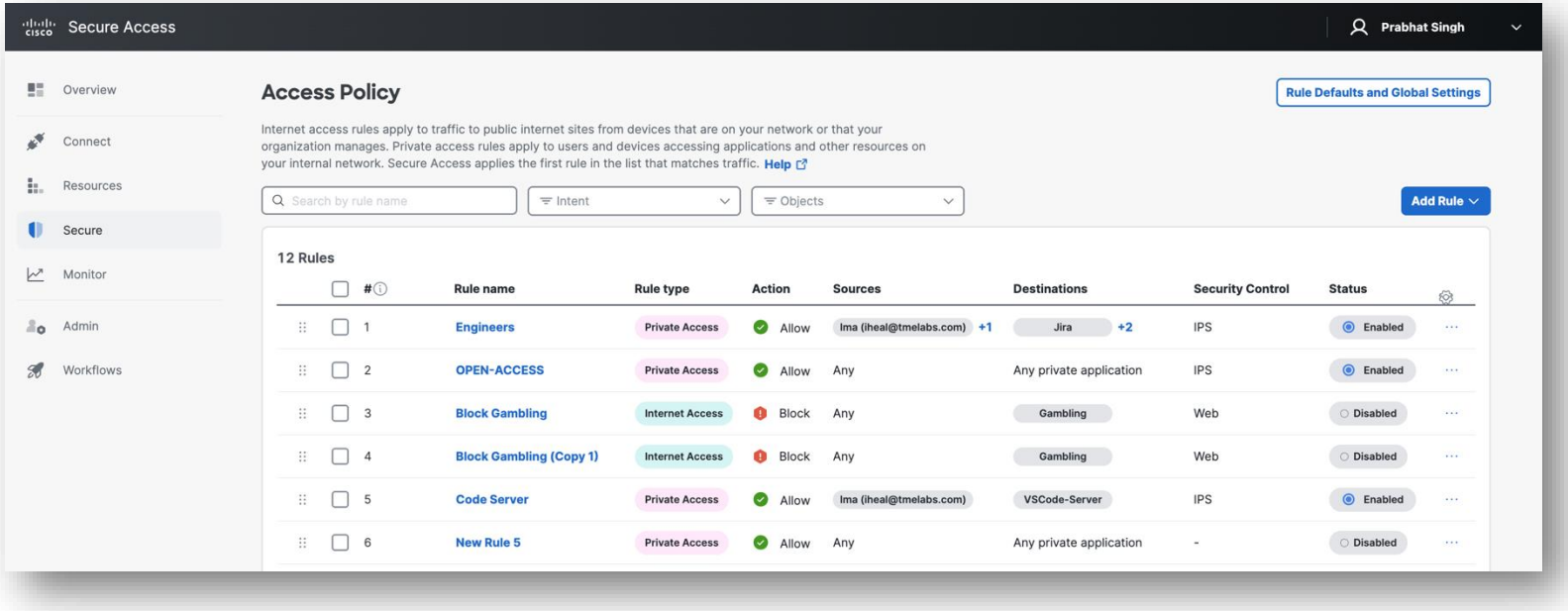
Transformation

…of our customers' admin and end-user experience



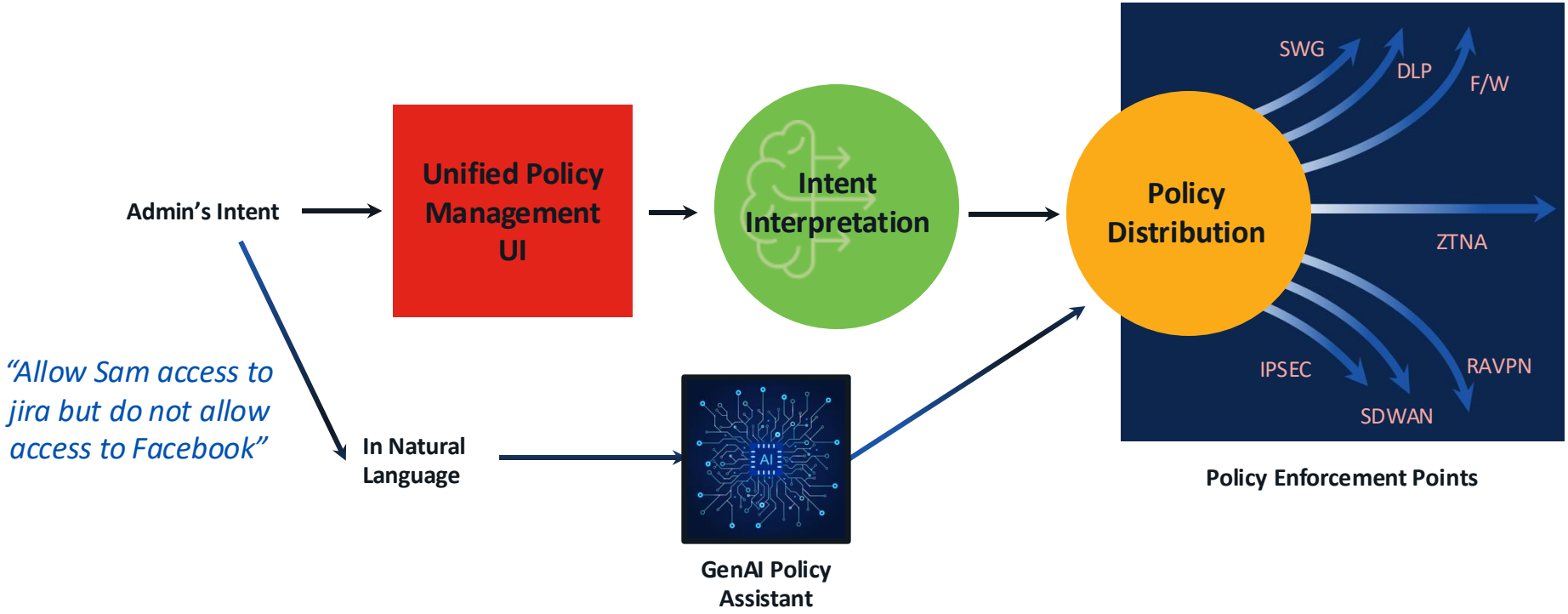
Unified, single, intent-based policy

- Based on the “what”, not the “how”
  - Allow user Sam access to Jira, but not to Facebook
  - No mention of Firewall or SWG, only what to allow and deny



Intelligent unified, intent-based policy

(first-to-market innovation)



The bridge to possible

Thank you