

# Ground the Cloud: Bring Zero Trust Back in your Control

Sarah Frisanco – SSE Solution Engineer



# Agenda

1. What is Zero Trust?
2. What is Universal ZTNA?
3. SSE & Hybrid Private Access
4. SDWAN & ISE
5. Identity
6. Cisco Live Teasers
7. Survey

# About Me:

- 4+ Years at Cisco
- 6+ Years covering SASE
  - Deployed Zscaler and Palo Alto Firewalls
- Manufacturing, Healthcare, Education
- Green Bay, Wisconsin
- Find me on LinkedIn:



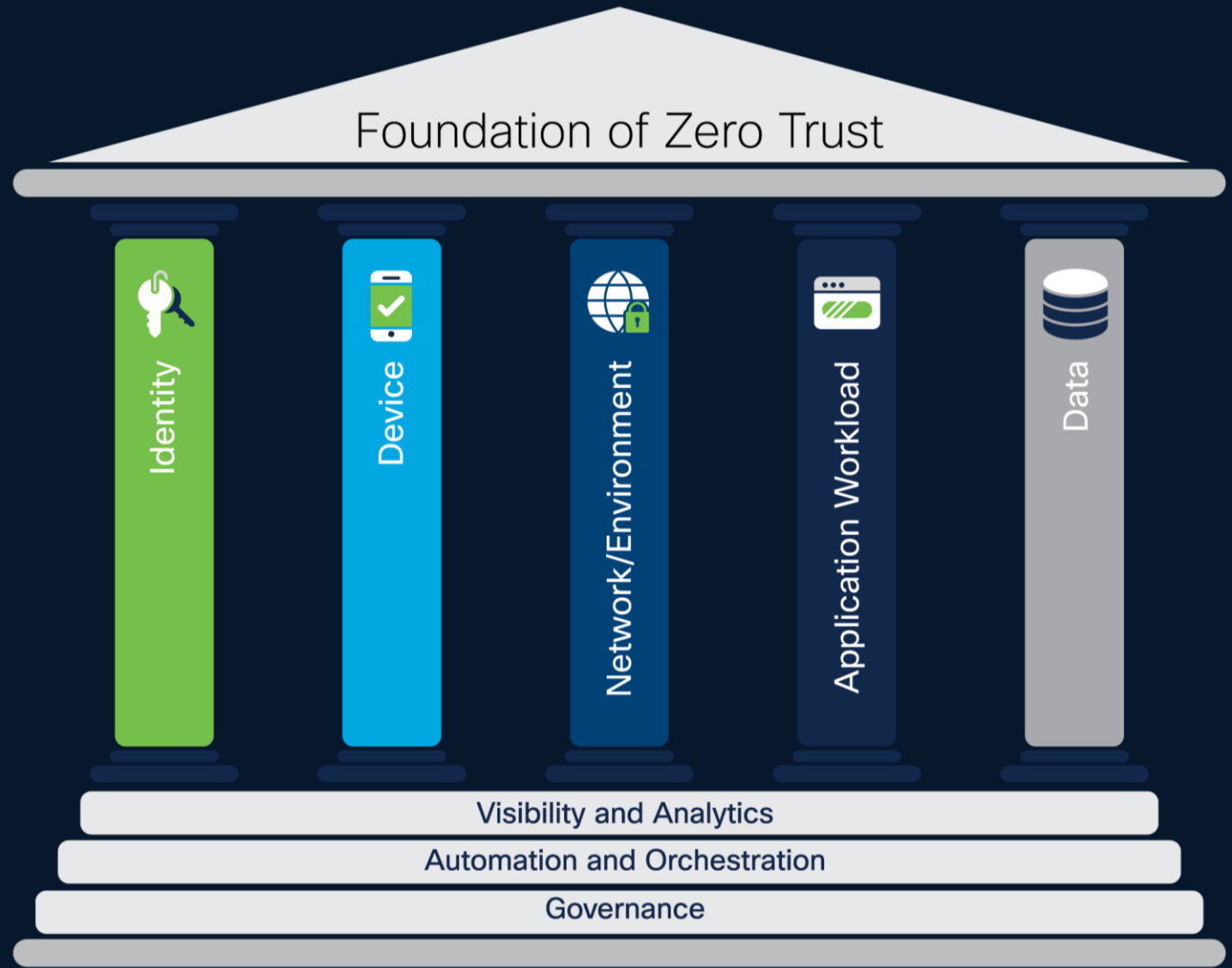
**What are some things  
you've heard about Zero  
Trust?**

# Common Examples

- Never Trust, Always Verify
- “We have MFA therefore we have Zero Trust”
- Our Zero Trust journey is one and done
- Microsegmentation vs. Macrosegmentation
- No more firewalls, our SSE solution is our firewall

# Zero Trust

Least Privilege  
Access is Key



US Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Pillars

# The Nebula

# The Nebula

The Network you  
Can Control

The Network you  
Can't Control

Identity

Universal ZTNA



**What is UZTNA?**

# Cisco Universal ZTNA

Takes ZTNA to users and **devices**

## Security Cloud Control

Secure  
SD-WAN

+

Secure  
Services Edge

+

**Continuous  
Trusted Identity  
for Everything**

Single vendor SASE

Digital Experience (ThousandEyes)  
“Threat Detection & Response (Talos, XDR, Splunk)”

**Security Services Edge**

# Cisco Secure Access

- Go beyond core Secure Service Edge (SSE) to better connect and protect your business

## Core SSE



Secure Web Gateway (SWG)



Cloud Access Security Broker (CASB) and DLP



Zero Trust Network Access (ZTA)



Firewall as a Service (FWaaS) and IPS

## Cisco delivers the core and more in a single subscription...



DNS Security



Multimode DLP



Advanced Malware protection



Sandbox



Talos Threat Intelligence



VPN as a Service



Digital Experience Monitoring\*



Remote Browser Isolation\*

\* Included in the unified experience / separate license (optional)

## Add-on solutions



SD-WAN



XDR



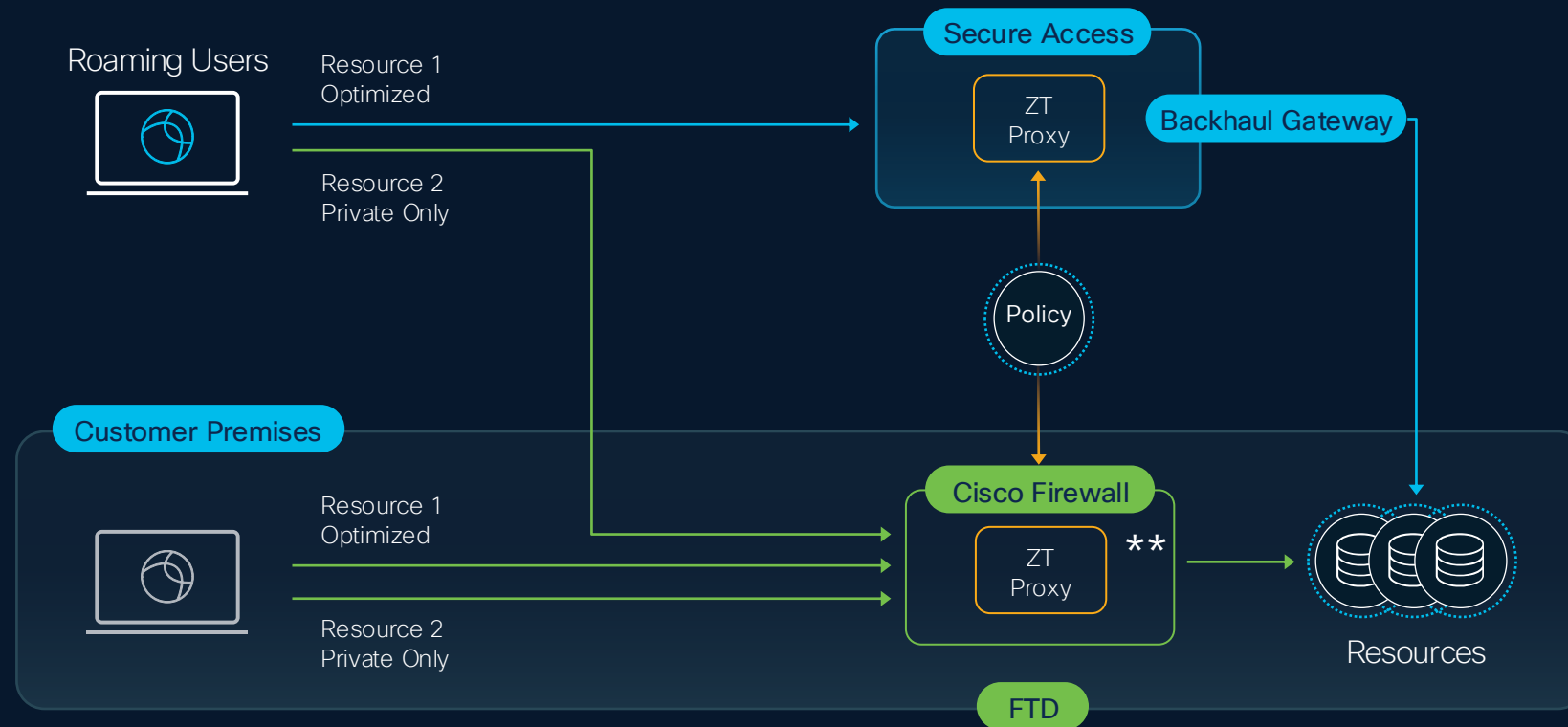
DUO MFA/SSO



CSPM

# Hybrid Private Access for flexible enforcement

- Single set of ZTNA policies used in cloud and on-premise



\*\* Roadmap: policy enforcement on 8k routers

# Decide Per Application

Client-based connection

Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture).

## Enforcement points

Cloud-only

Cloud or Local (Universal Zero Trust Access)

### Local enforcement points

FMC.s... X Search by FTD na... v

Traffic from users within a trusted network will get enforced at the selected Firewalls.

Local-only

### Enforcement point for Remote User

Remote user

Secure Access Cloud

Private Resource



via Internet



### Enforcement point for Local user

User in a trusted network

Local Firewall

Private Resource



via local network



# Hybrid Private Access Demo



# Home

[Set default homepage](#)

[All Insights](#)

## Top Insights & Alerts 12 Active Insights

**Access Control Policy Anomalies** ...

Data source: Test-abc Cloud-delivered FMC

AIOps has detected 32 anomalies in Access Control policy 'Test-abc'.

28d ago [Details](#)

**Best practices and recommendations** ...

Data source: ftdv-test6

AIOps has detected 6 needs review checks.

24d ago [Details](#)

**Best practices and recommendations** ...

Data source: ftdv-test5

AIOps has detected 6 needs review checks.

24d ago [Details](#)

- Products
- AI Defense
  - Firewall
  - Hypershield
  - Multicloud Defense
  - Secure Access
  - Secure Workload

- Platform services
- Favorites
  - Identity Intelligence
  - Security Devices
  - Shared Objects
  - Platform Management

### Multicloud Defense Multicloud Defense

**Account Resources**

<b>21</b> VPCS/ VNets	<b>35</b> Security Groups	<b>31</b> Route Tables	<b>69</b> Subnets
<b>8</b> Instances	<b>1</b> Load Balancers	<b>0</b> Tags	<b>1</b> Applications

**Security Considerations**

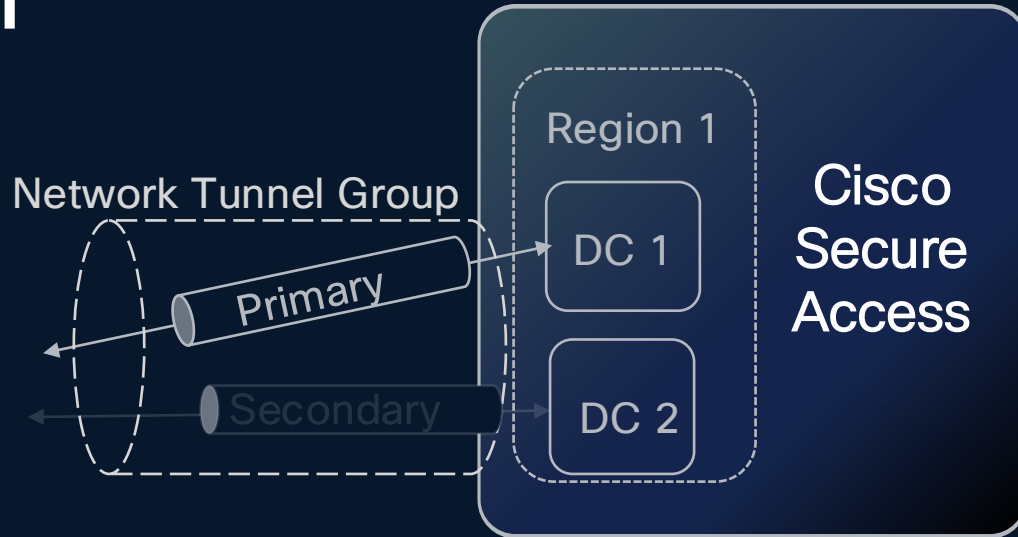
<b>1</b> Applications not protected	<b>20</b> VPCS/VNets not protected	<b>0</b> Service VPC/VNets without Gateways
-------------------------------------	------------------------------------	---

### Overall Inventory 32 Total Devices

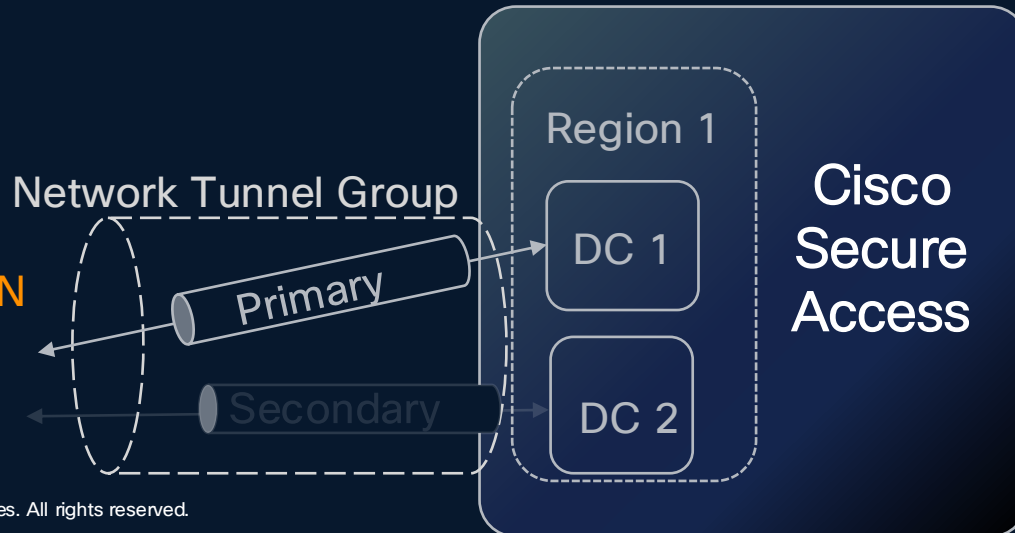
### RA VPN Sessions

**SDWAN**

# Branch



## Catalyst SD-WAN



## Site-to-site Tunnels with IPsec

- Standards-based IPsec connection
- Single tunnel for Internet and private application access
- Static or BGP routing support
- Auto failover for redundancy + ECMP for scale
- Regional redundancy
- Outbound NAT support for internet only tunnels

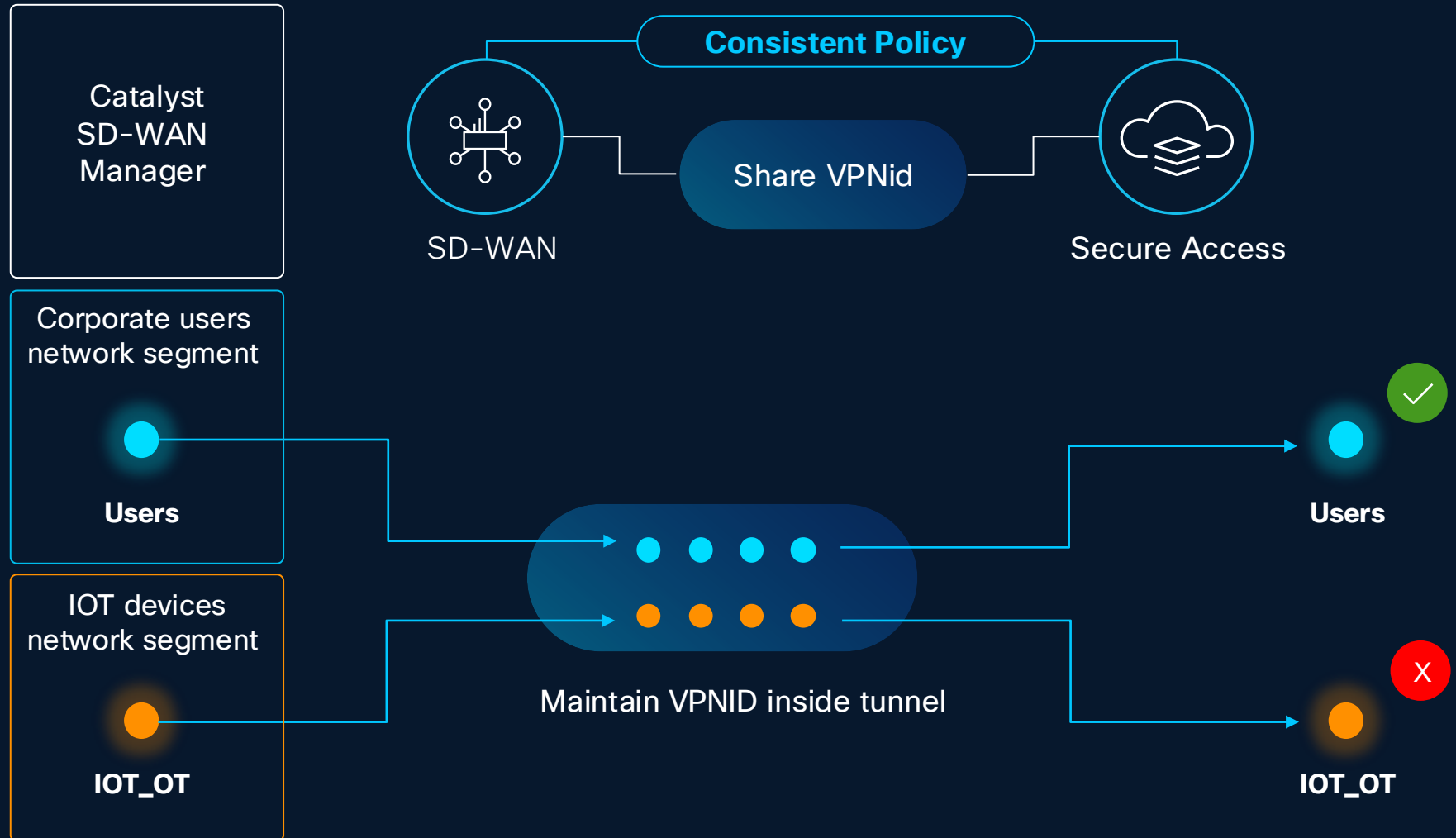
## Catalyst SD-WAN

- Auto-tunnel from Catalyst SD-WAN for Internet apps now
- Auto-tunnel from Catalyst SD-WAN for Private apps in 20.18
- 1GB per tunnel
- Up to 8 active, 8 backup per tunnel group
- SD-WAN tracker support for regional redundancy

# Catalyst SD-WAN

## VPNid support for consistent segmentation

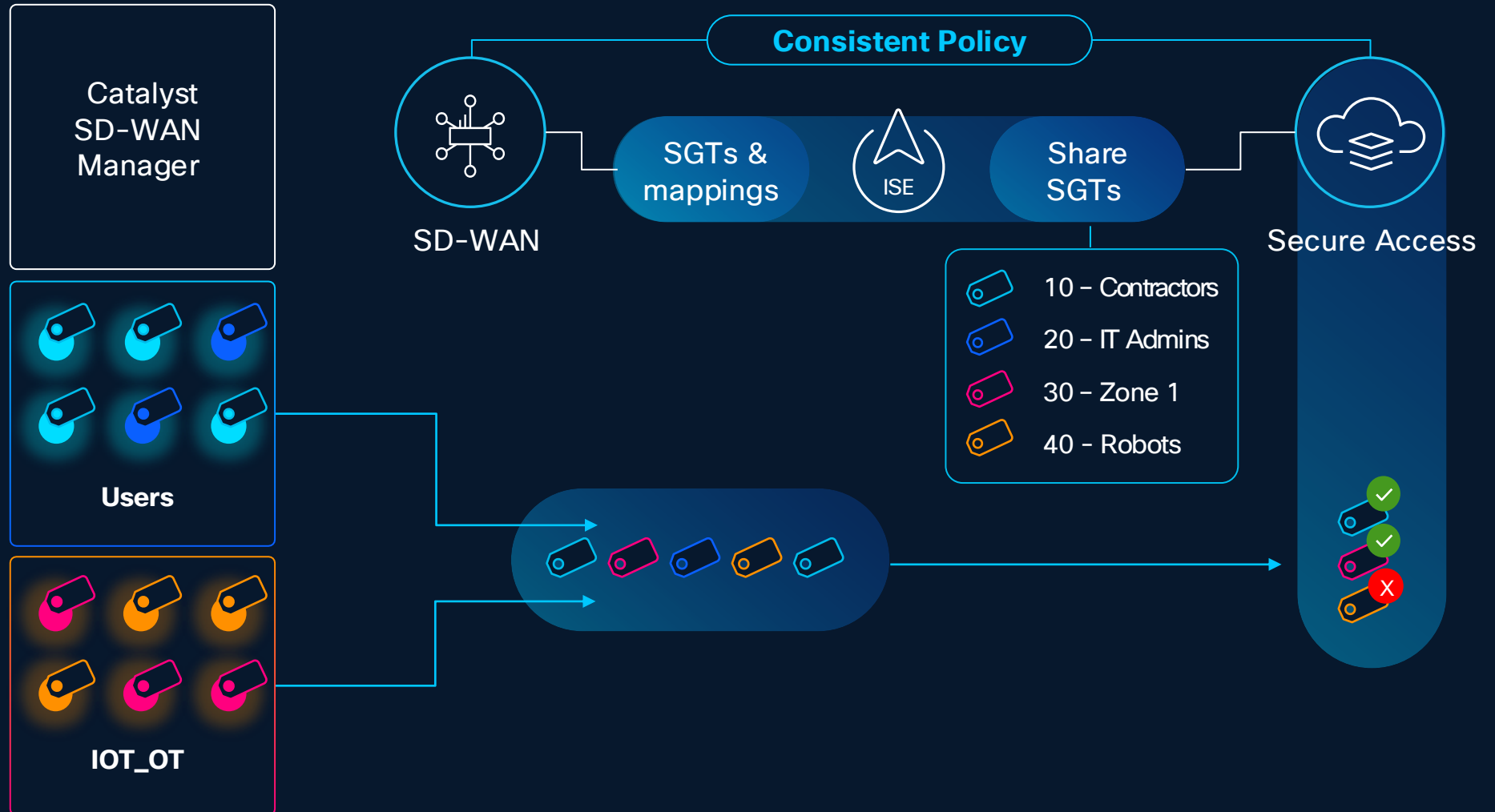
- VPNid Based policy across both SDWAN & Secure Access
- Maintain segmentation in branch & in the cloud



# Identity Services Engine (ISE)

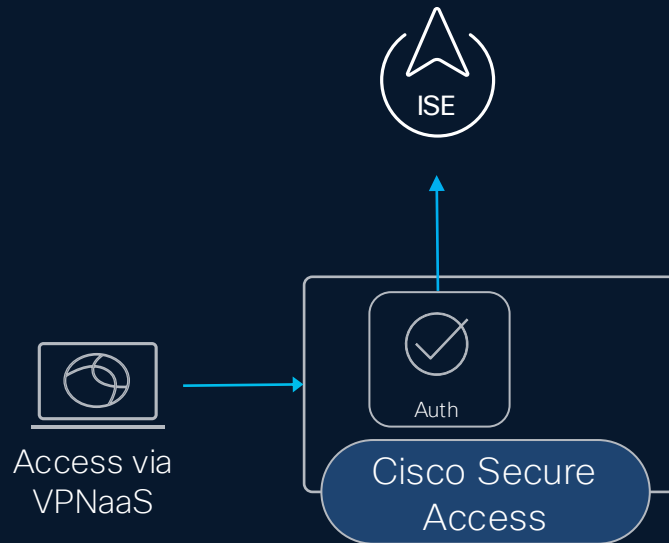
Leverage SGTs for granular access control

- SGT Based Policy across network & Cloud
- Maintain micro segmentation through Secure Access
- Uniquely identify devices and traffic based on context from ISE
- Apply policy to SGT Based identity



# ISE integration with Secure Access VPNaaS

RADIUS authentication, in addition to SAML authentication



- Cisco Identity Services Engine (ISE) or 3<sup>rd</sup> Party RADIUS supported
- AAA or authorize only
- Up to 8 servers within a single server group
- ISE posture supported (optional)
- SGT assignment via authorization

# SGT Demo

- Home
- Connect
- Resources
- Secure
- Monitor
- Admin
- Workflows

# Access Policy

[Rule Defaults and Global Settings](#)

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. [Help](#)

Search by rule name  Intent  Objects  Settings

[Add Rule](#)

13 Rules

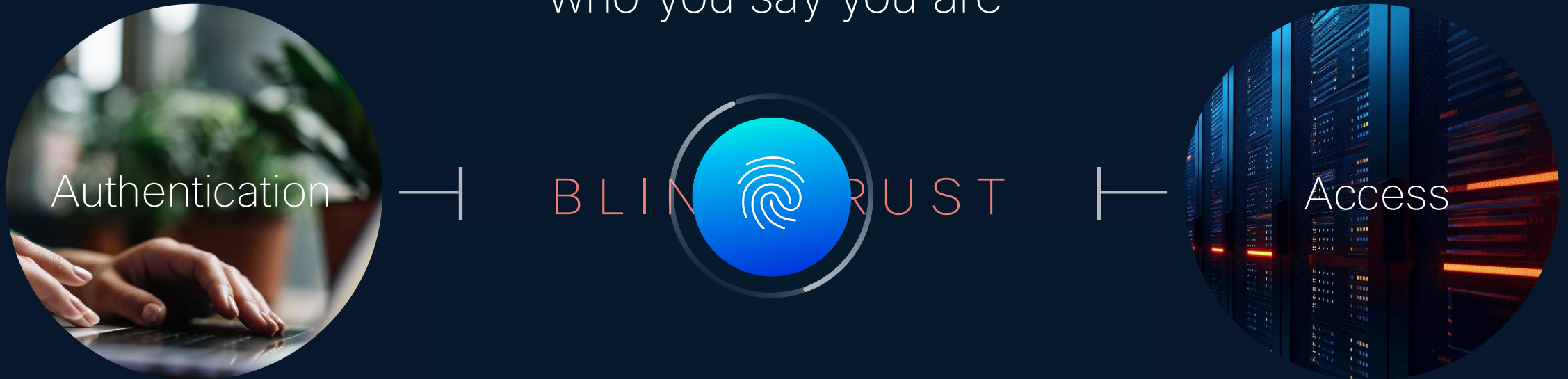
[Customize view](#)

<input type="checkbox"/>	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status	
<input type="checkbox"/>	1	<a href="#">AllowTunnelToInternet</a>	Internet	Allow	testLogicalA... +1	Any		-	⊖	⋮
<input type="checkbox"/>	2	<a href="#">AllowSGTtoAnyInternet</a>	Internet	Allow	Any Security...	Any		-	✓	⋮
<input type="checkbox"/>	3	<a href="#">AllowAnySGTtoAnyprivate</a>	Private	Allow	Any Security...	Any		-	✓	⋮
<input type="checkbox"/>	4	<a href="#">AllowSGT8ToSGT9</a>	Private	Allow	SGT-8	SGT-9	-	-	✓	⋮
<input type="checkbox"/>	5	<a href="#">AllowSGT9ToSGT8</a>	Private	Allow	SGT-9	SGT-8	-	-	✓	⋮
<input type="checkbox"/>	6	<a href="#">allowTun1ToTun2</a>	Private	Allow	testLogicalA... +1	1 IP Address/CIDR AND 1 Services +3	-	-	⊖	⋮
<input type="checkbox"/>	7	<a href="#">TunnelAllow8888</a>	Internet	Allow	testLogicalA... +1	1 IP Address/CIDR AND 1 Services		-	✓	⋮
<input type="checkbox"/>	8	<a href="#">TunnelBlock8844</a>	Internet	Block	testLogicalA... +1	1 IP Address/CIDR AND 1 Services		-	✓	⋮
<input type="checkbox"/>	9	<a href="#">AllowSGT2ToSGT1</a>	Private	Allow	SGT-2	SGT-1	-	-	✓	⋮
<input type="checkbox"/>	10	<a href="#">AllowSGT2SGT</a>	Private	Allow	SGT-1	SGT-2	-	-	✓	⋮
<input type="checkbox"/>	11	<a href="#">DenyPing8844</a>	Internet	Allow	SGT-5	Any		-	✓	⋮
<input type="checkbox"/>	12	<a href="#">AllowSGT6toAny</a>	Private	Allow	SGT-6	Any		-	✓	⋮

**Identity**

# Identity Intelligence

Continuously assess you are  
who you say you are



Works with existing IDPs

SailPoint

Dragos

Crowdstrike

Salesforce

Okta

PingIdentity

Cisco ISE

Auth0

Cyberark

Microsoft

Google

Amazon

# Cisco Identity Intelligence



USERS



MACHINES



SERVICES



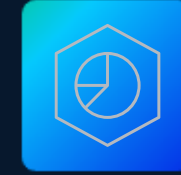
HRIS



DATA



APPS



PLATFORMS



SailPoint

Dragos

CrowdStrike

Salesforce

Cisco ISE

Okta

PingIdentity

Auth0

Microsoft

Google

Cyberark

Amazon

# User trust timeline

The screenshot shows the Cisco Identity Intelligence interface for user **Brian Hayes** (brian.hayes@simubiz.com). The user is located in the US and is active. The interface includes a navigation menu on the left, a top search bar, and a user profile header with tabs for Overview, Activity, Networks, Devices, Applications, Groups, and Checks (8). A yellow notification banner at the top states: "We identified other users with a similar username or the same employee ID as brian.hayes@simubiz.com. Do you want to link them?" with "Dismiss" and "Review" buttons.

**Summary**

- Inconsistent, Non Employee
- N/A
- N/A
- Oort
- US
- MFA Configured
- Sep 18, 2024 03:59:00 UTC (20 hours ago)
- N/A

Created Jul 18, 2010

**Trust Score** Last Updated: Sep 18, 2024 04:50:14 UTC  
**Untrusted**

Special account engaged in MFA flood attack  
New country for tenant and special account.  
New country for tenant, special account, resurrected account, and unmanaged device.

**Additional details**

- Special Account
- Resurrected Account  
Failing Checks: [Access From Dormant Account](#)
- MFA Flood  
Failing Checks: [Telecom MFA Limit Reached](#)
- New Country for Tenant  
Failing Checks: [New Country for Tenant](#)
- Unmanaged Device  
Failing Checks: [Unmanaged Devices Access](#)

5 events matching score [View in Activity Tab](#) [View all activities with a score](#)

**Last Login Attempt** [View more data](#)

# User Trust Score

The screenshot shows the Cisco Identity Intelligence interface for user Brian Hayes (brian.hayes@simubiz.com). The user's status is 'Active' and 'US'. A notification at the top indicates that other users with similar usernames or employee IDs were identified. The 'Trust Score' section shows the user is 'Untrusted', with a last update on Sep 18, 2024 at 04:50:14 UTC. The 'Additional details' section lists several security events: Special Account, Resurrected Account, MFA Flood, New Country for Tenant, and Unmanaged Device, each with associated failing checks and links for more information. A summary section on the left lists attributes like 'Inconsistent, Non Employee', 'N/A', 'Oort', 'US', and 'MFA Configured'. The bottom of the page shows the last login attempt and a link to view more data.



## User Trust Score

Identity Intelligence will be providing a user trust score for integrating solutions to leverage. Will be a single score, determined by a user's behaviors, actions and posture



## Easy Workflows

After assessment, seamlessly take response action from the console.

## Key Scores

- Trusted
- Favorable
- Neutral
- Questionable
- Untrusted
- Unknown

**Bringing It All Together**



There is no **universal zero trust** without **ubiquitous, shared identity** across the enterprise

# Cisco Universal ZTNA

Every device, person, thing, everywhere



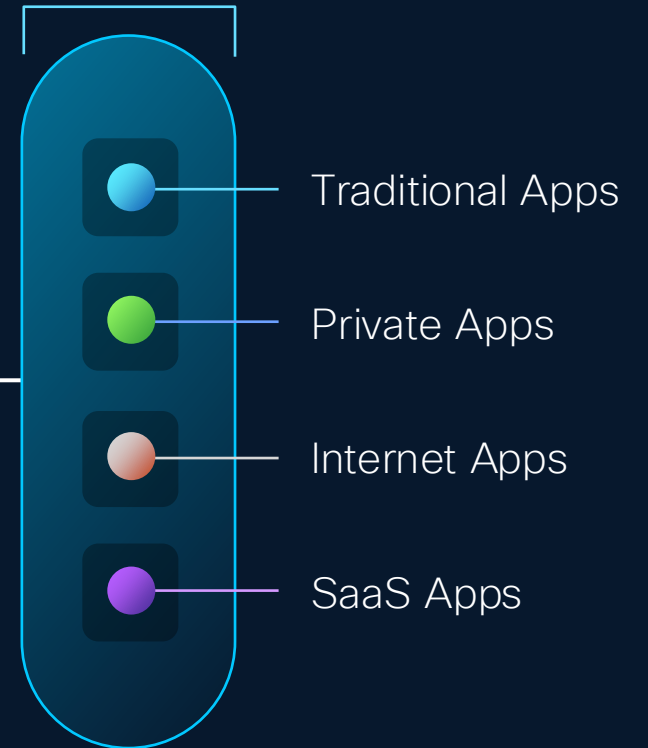
Zero impostors:  
Identity Trust



Zero downtime:  
Experience and Policy Assurance



Zero friction:  
We do the plumbing.



Consistent Security:  
Security Service Edge