

Cisco **Security**

Zero Trust Access



Ozan Küçük

Technical Presales Consultant

Cisco ZTA

CUSTOMER SECURITY OUTCOMES

Secure Connectivity (SASE)

Security First Identity

Zero Trust Network Access

Secure Internet & AI Access



Secure SD-WAN

Secure
Firewall

Catalyst

Meraki



Cisco Secure Access



Cisco ThousandEyes



Trusted Identity Edge

ISE

Duo

SINGLE VENDOR SASE

SECURITY CLOUD CONTROL

Protect users everywhere, on any device, with frictionless zero-trust secure access and layered security

Cisco ZTA

CUSTOMER SECURITY OUTCOMES

Secure Connectivity (SASE)

Security First Identity

Zero Trust Network Access

Secure Internet & AI Access

Security Use Cases

Campus / Branch SASE

Delivers unified security and SD-WAN networking across campus and branch locations, ensuring consistent policies, greater visibility, and a seamless user experience through a single, cloud-managed platform.

Defending Identity

Safeguards organizations from advanced identity-based attacks with unified visibility, adaptive authentication, and phishing-resistant security, all through a single, security-first platform.

Hybrid Private Access

Delivers secure, seamless access to private resources anywhere, applying consistent Zero Trust policies and device checks through a single Cisco platform, simplifying management and protecting productivity.

Remote Access VPN

Enables secure, reliable connectivity to private and legacy resources from anywhere. With Cisco's cloud-native solution, organizations unify access, simplify management, and ensure users stay protected and productive.

Secure Internet Access

Protects users and devices everywhere by blocking threats, safeguarding sensitive data, and ensuring safe, productive access to web and SaaS applications without degrading performance and productivity

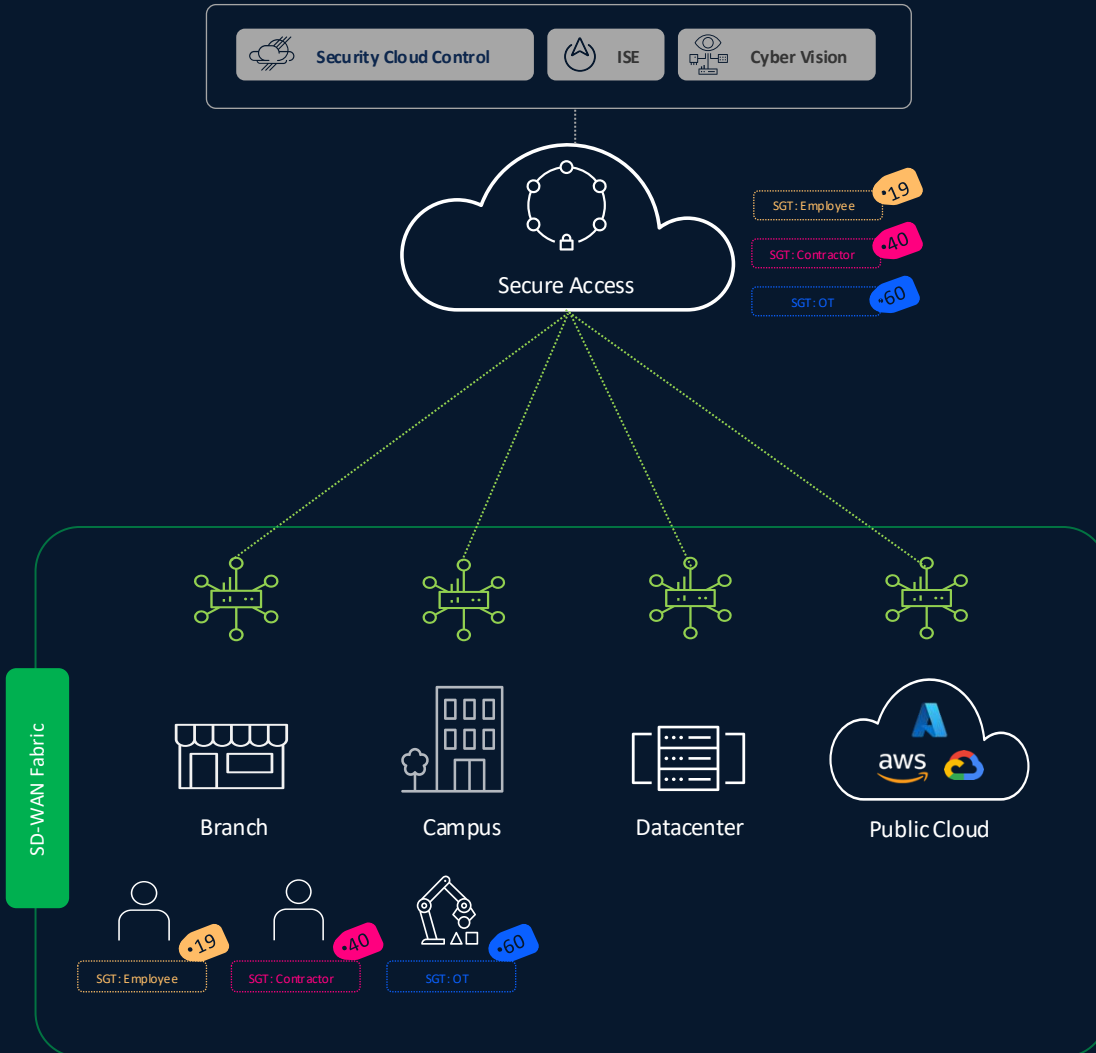
Shadow AI Access

Gives organizations visibility and control over unsanctioned AI tool usage, reducing risks of data loss and compliance breaches. With Cisco's integrated platform, enterprises can safely adopt AI and boost productivity without added complexity.

Zero Trust Access

Campus / Branch SASE

Campus / Branch SASE



Objective

This architecture simulates a real-world enterprise fabric designed to showcase how Cisco SGT based policy delivers consistent, identity-driven access across SD-WAN fabric. It demonstrates how user and workload traffic can originate anywhere and reach authorized destinations while preserving micro-segmentation through Cisco Secure Access.

Devices and flows are uniquely identified using SGT assigned by Cisco ISE. Policy is then enforced based on SGT identity rather than IP or location, therefore controls remain consistent end-to-end, from campus, branch and data center to multi-cloud, even as users, apps, and network paths change.

Architecture Layout

- **Security Cloud Control** – Unified management platform for Cisco SASE fabric
- **User / OT** – represent different roles with different access permissions / rights
- **Secure Access** – zero trust enforcement on accessing public and private resources
- **SD-WAN Fabric** – offering improved application aware policies and enhanced security
- **ISE** – The network access control and Security Group Tag (SGT) policy implementation
- **Cyber Vision** – provide IoT/OT visibility and context sharing with ISE

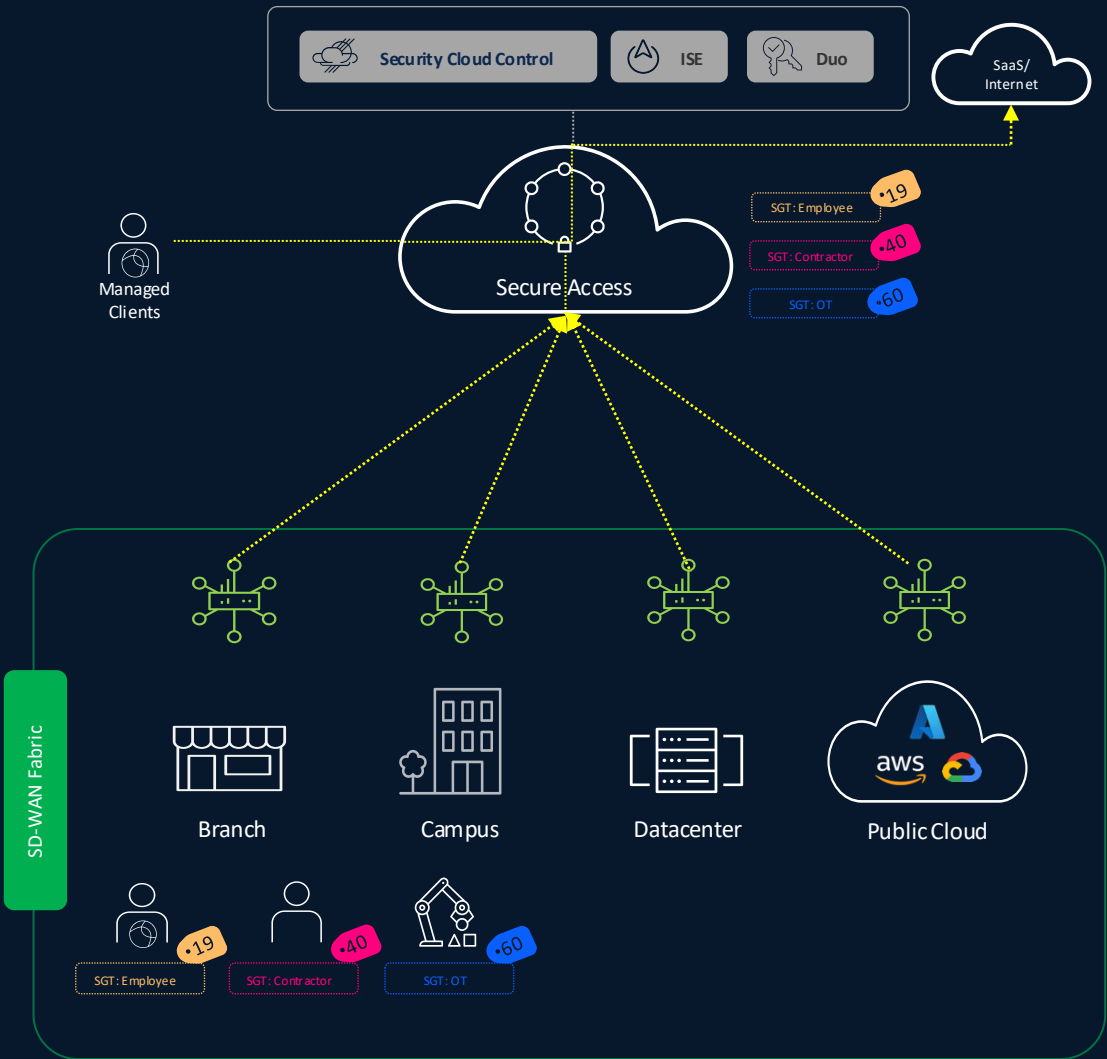
Scenarios

- **Catalyst SD-WAN** - This demo shows how Catalyst SD-WAN provides secure and optimized connectivity between branch sites and private resources. By integrating Secure Access, Cisco ISE, and Secure Cloud Control (SCC), branch traffic is authenticated, authorized, and segmented using SGT based identity. Cyber Vision delivers visibility into IoT and OT devices through integration with ISE, while ThousandEyes offers Digital Experience Monitoring (DEM) for real-time insights into network and application performance.
- **Firewall** - This demo highlights how Secure Access in combination with SCC and ISE, provides intelligent threat defense and consistent policy enforcement across hybrid environments. By leveraging SGT based identity, Secure Access's policies are applied dynamically to users and devices, ensuring secure, context-aware access regardless of location.
- **Meraki** - This demo focuses on the simplicity and scalability of Meraki combined with Secure Access. As Secure Connect is transitioning into Secure Access, additional integrations are being built out between Meraki and Secure Access. Meraki MR and MX integrate with Cisco Secure Access DNS security for proactive threat protection. IPsec connectivity can be used to connect Meraki MXs to Secure Access for additional security capabilities as well as private app connectivity.

Zero Trust Access

Secure Internet Access

Secure Internet Access



Objective

This architecture simulates a real-world enterprise environment designed to demonstrate the capabilities of Secure Access in delivering secure, identity-driven connectivity to the internet and SaaS applications.

It showcases how users and devices, both on and off the corporate network are protected through DNS layered security, Duo authentication, and Zero Trust access enforcement.

Architecture Layout

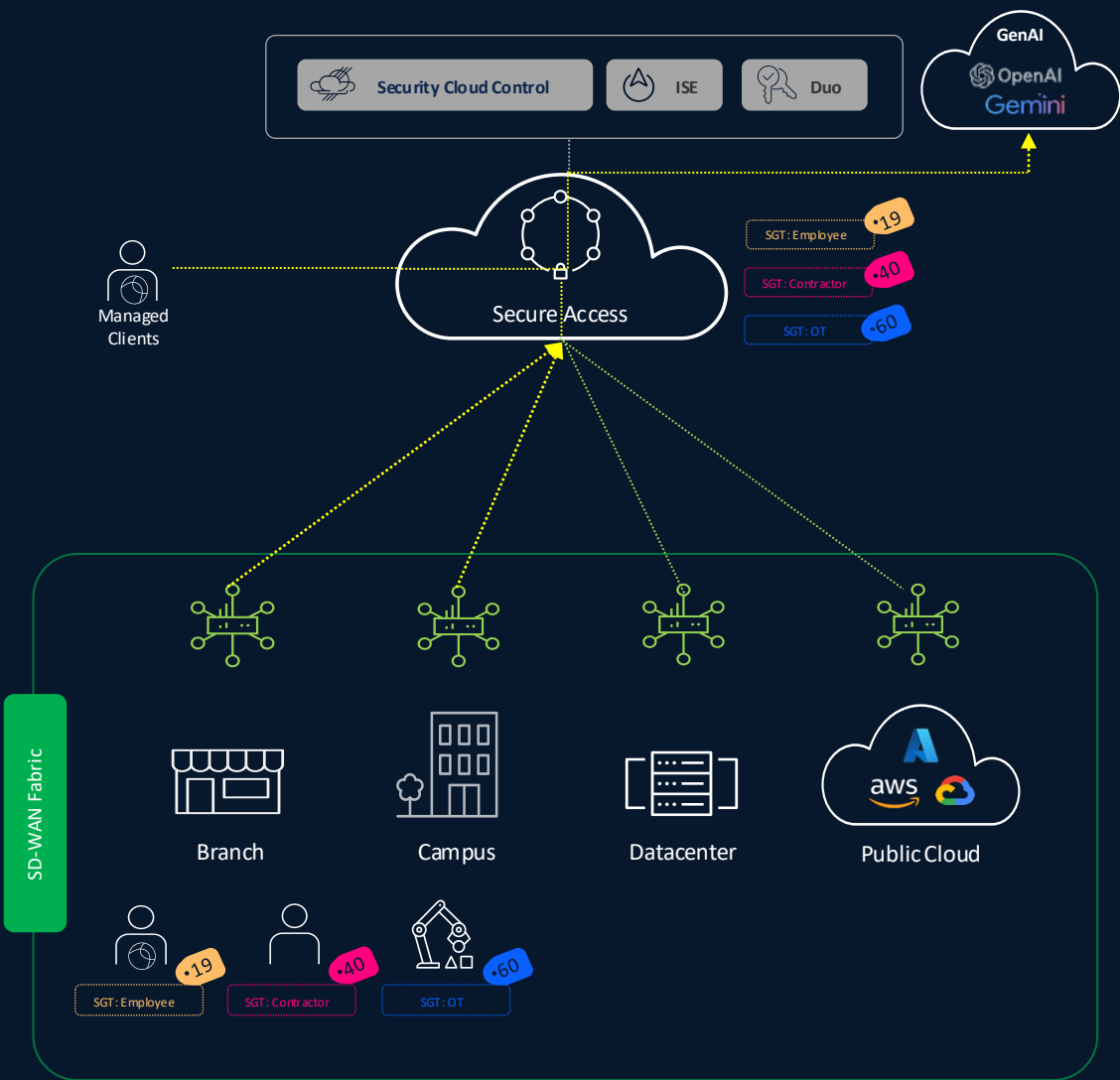
- **Security Cloud Control** – Unified management platform for Cisco SASE fabric
- **User / OT** – represent different roles with different access permissions / rights
- **Secure Access** – zero trust enforcement on accessing public and private resources
- **ISE** – The network access control and Security Group Tag policy implementation
- **Duo** – Provides strong user authentication, SSO, and continuous trust verification
- **Managed Client** – Verified + compliant device allowed to access SaaS / internet applications
- **SaaS / Internet** – Cloud-based and public web applications accessed via Secure Access

Scenarios

- **Protection** – This demo highlights how Secure Access provides simple, consistent protection for users and devices residing inside and outside of the trusted network. It leverages DNS security as the first line of defense to block malware, phishing, and C2 threats before connections are established. Integration with ISE's Security Group Tags (SGTs) enables unified policy enforcement, extending protection seamlessly across users, devices, and locations.
- **Data Security & Compliance** – This demo showcase how organizations can protect sensitive data and maintain compliance with standards such as HIPAA, PCI DSS, and GDPR. Inline DLP secures data in motion for managed clients while SaaS API DLP safeguards data at rest within cloud applications. Features such as Exact Data Matching (EDM) and Index Data Matching (IDM) provide advanced detection and control of confidential information across all data flows.
- **Trusted Endpoint** – This demo exhibit how Secure Access ensures that only trusted, compliant endpoints can access critical SaaS applications securely. By combining device posture assessment, identity verification, and policy-based controls, it enforces Zero Trust principles and prevents unverified devices from reaching sensitive cloud resources.

Zero Trust Access
Shadow AI Access

Shadow AI Access



Objective

This architecture simulates a real-world enterprise environment designed to demonstrate the capabilities of Secure Access in delivering secure, identity-driven connectivity to the publicly available AI applications.

It showcases how Secure Access leverage CASB, DLP and AI Access features to deliver advanced protection against data leaks, prompt injection and AI supply chain risk while enabling secure and compliant adoption of AI technologies

Architecture Layout

- **Security Cloud Control** – Unified management platform for Cisco SASE fabric
- **User / OT** – represent different roles with different access permissions / rights
- **Secure Access** –zero trust enforcement on accessing public and private resources
- **ISE** – The network access control and Security Group Tag policy implementation
- **Duo** – Provides strong user authentication, SSO, and continuous trust verification
- **Managed Client** – Verified + compliant device allowed to access SaaS / internet applications
- **GenAI** – Cloud-based & public Generative AI applications accessed via Secure Access

Scenarios

- **AI App Discovery + Shadow IT** – This demo showcase how Secure Access use CASB to uncover shadow AI and SaaS applications use across the organization. Admin can take actions on those applications along with DLP to minimize the risk of shadow IT and data leakage
- **AI Guardrail** – This demo present how AI Guardrails use multi-model machine learning to analyze the intent behind AI prompts and response across 15 GenAI apps. This feature block malicious / harmful content, prompt injection and data exfiltration attempt thru bi-directional DLP
- **AI Supply Chain Risk Management** – This demo highlights how AI Access integrates with Cisco Foundation AI to assess and score AI/ML models for security, compliance, and integrity risks. It identifies vulnerabilities, malware infected LLMs, data poisoning and licensing issues (Hugging Face models)

