ROCTEL
www.roctel.net

Cisco Partner
Premier Provider

Universal ZTNA: The Practitioner's Handbook

Table of Contents

Executive Summary 2

Understanding the Key Concepts Behind Universal ZTNA..............3

Traditional ZTNA Leaves Gaps...9

How to Know if Traditional ZTNA Isn't Enough for Your Organization 11

Evolving to Universal ZTNA: A Ten Step Checklist 12

Cisco Universal ZTNA Accelerates Zero Trust.......13

Jumpstart your zero trust project today.......14

Executive Summary

Imagine it's Monday morning and you're about to log into Outlook to check your email. While that's happening in the comfort of your own home, another teammate is on site preparing for a meeting. They are logging into Dropbox to get a slide deck they've been collaborating on with a third party, while using Slack to coordinate with other presenters. These two examples of user-to-app connections are a fraction of the scenarios that need protecting. The now vast landscape of users and things connecting to applications isn't simply pushing the limits of traditional access and protection methods, it's mandating a change.

This shift away from a traditional perimeter, born out of necessity, has introduced security gaps, and complicated the user experience. Now more than ever, IT teams still need a way to connect users securely to a myriad of applications which are often dispersed across public and private clouds and data centers. The question becomes, not only how, but how to consistently connect and protect no matter the user, device, or location.

Organization's users and applications are increasingly distributed and need robust security that is flexible enough to fit different use cases. To do this, security practitioners have turned to the Universal Zero Trust Network Access (ZTNA) model that moves security closer to the edge.

Return-to-office mandates have added another layer of complexity. How do organizations ensure seamless security across both remote and on-site work scenarios?

To help practitioners accelerate their transition to a more powerful ZTNA, we have created a blueprint for adopting Cisco's approach to Universal ZTNA. In this field guide, you will find definitions, practical recommendations, and tools to help you transition to truly universal zero trust.

Understanding the Key Concepts Behind Universal ZTNA

Before we jump into the nuts and bolts of how to adopt Universal ZTNA, it's important to understand some key concepts around securing application access for users.

Let's begin with the precursor: VPNs.

What is VPN?

A Virtual Private Network (VPN) is a technology that establishes a secure and encrypted connection over a public network, typically the internet. By creating a virtual tunnel between a user's device and a remote server, VPNs facilitate the safe transmission of data, ensuring confidentiality and integrity. Traditionally, VPNs have been used to provide remote access to corporate networks, enabling users to access resources as if they were directly connected to the same local network. This encryption and tunneling mechanism helps protect sensitive information from interception by unauthorized entities, thereby maintaining privacy and security in communication.

Goals of a VPN:

- **Secure Data Transmission:** Establish encrypted tunnels over the internet to protect data integrity and confidentiality, ensuring that sensitive information is shielded from interception by unauthorized entities.
- **Remote Access:** Enable users to securely connect to corporate networks from remote locations, simulating the experience of being directly connected to the internal network and facilitating access to necessary resources.
- **Privacy Protection:** Mask user IP addresses and encrypt communications to enhance privacy, preventing unauthorized tracking and maintaining confidentiality of user activities.

Key takeaway: VPN solutions have traditionally served as a cornerstone for secure remote access, providing encrypted pathways for data transmission and protecting user privacy. However, in the face of evolving security challenges and the demand for more granular access controls, organizations are increasingly looking towards Zero Trust Network Access (ZTNA) to complement and enhance their security frameworks. Despite these advancements, VPNs and VPN-as-a-Service solutions continue to play a role for applications that can't be accessed through ZTNA technology.

What is ZTNA?

Cloud-delivered Zero Trust Network Access (ZTNA) is a key component of Security Service Edge (SSE) solutions. ZTNA solutions enable users to connect to applications—generally from remote locations, and usually to private applications—without using a VPN. ZTNA typically provides capabilities for deeper posture checking and more granular access controls than traditional, hardware-based VPNs to enforce the “least privilege” concept and reduce the attack surface.

Goals of a ZTNA solution:

- **Prevent private application discovery.** Ensures nefarious actors cannot discover internal organizational resources. Such obfuscation blinds bad actors and prevents attacks.
- **Enforce least privilege on a per-user, per-app basis.** Maintains ultra-granular control over which users can access various applications, under what conditions, and with specific user to application proxy connections that prevent cyberthieves from ‘piggybacking’ onto existing legitimate user connections.

Key takeaway: While initial ZTNA solutions provided some benefits, early adopters quickly recognized security and user experience limitations, and we'll tackle those in the upcoming section of this field guide.

What is Universal ZTNA?

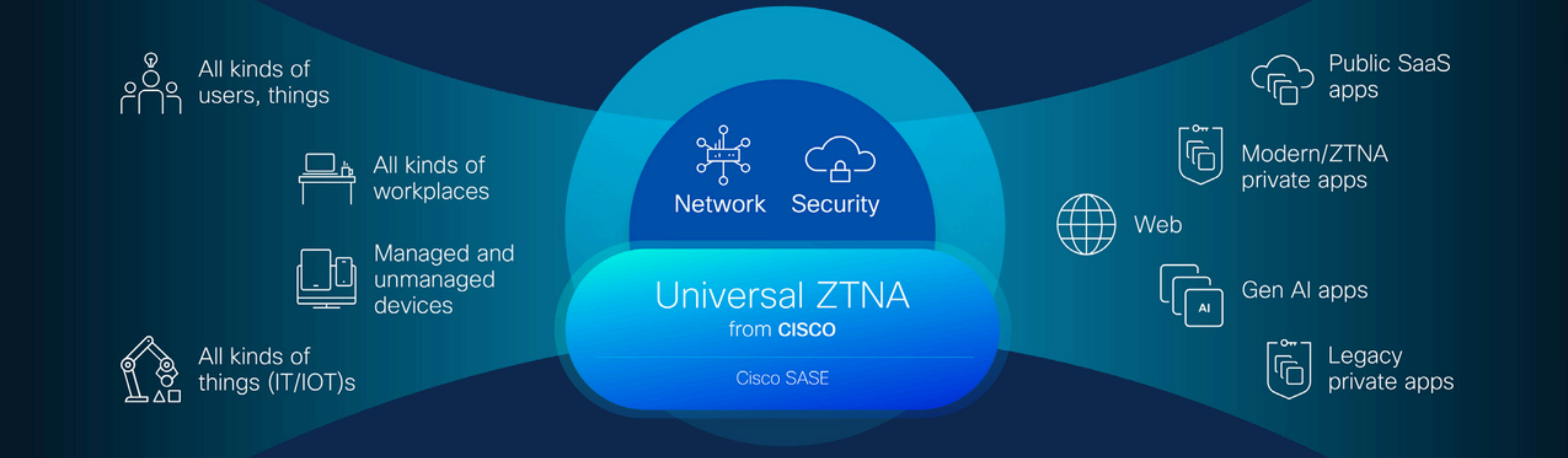
To truly modernize remote access, you need to go beyond classic ZTNA. A new approach is required, one that further reduces risk and simplifies IT management tasks, while improving the end-user experience and enhancing workforce productivity. Universal ZTNA refers to a security approach that applies the principles of ZTNA consistently across all user locations, whether they are working in the office, remotely, or on the go.

Goals of a Universal ZTNA solution:

- **Secure access to all applications, for all users.** Expands upon ZTNA capabilities. Ensures access to applications regardless of their physical location, all under a single, unified policy.
- **Eliminate the need for separate solutions.** Provides consistent security for all environments while also creating a seamless user experience.

Key takeaway: Cisco expanded traditional ZTNA beyond its conventional use — extending trust across all user locations, all apps located anywhere, and not only users but also things as well. Our approach unifies identity-first zero trust access for modern and legacy apps, IoT/OT devices, and challenging network environments, combining industry-leading performance, policy validation, and visibility to eliminate complexity and protect critical assets.

Universal identity makes Universal ZTNA possible



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

What is Identity Intelligence?

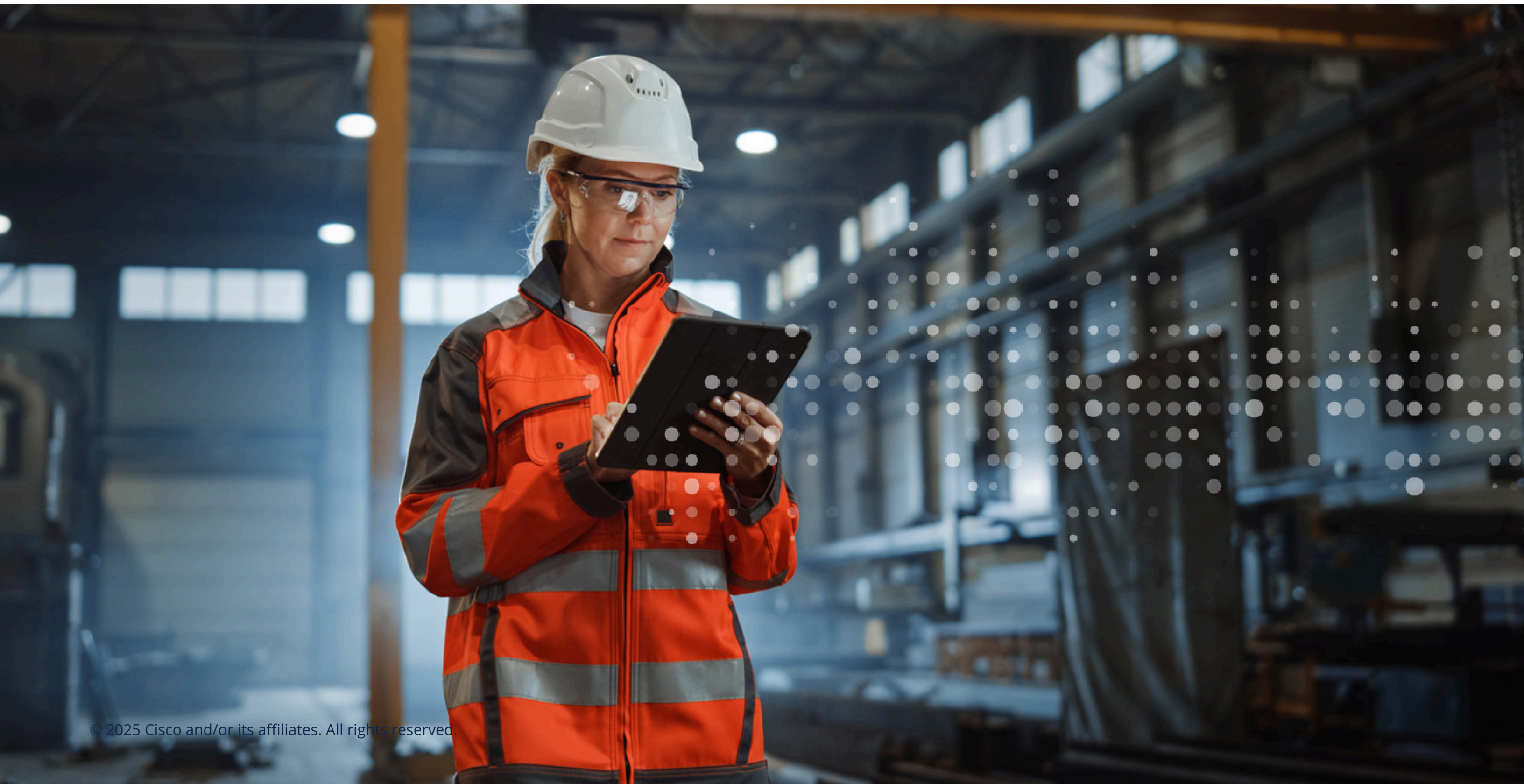
Identity Intelligence is an analytics layer that provides cross-platform visibility into how identities are used across an environment. It provides advanced capabilities for monitoring, analyzing, and managing user identities and their associated activities. By leveraging machine learning and behavioral analytics, Cisco Identity Intelligence helps identify and respond to potential security threats related to user identities.

Benefits of Cisco Identity Intelligence:

1. **Behavioral Analytics:** Utilizes machine learning algorithms to establish a baseline of normal user behavior, enabling the detection of anomalies or suspicious activities that may indicate compromised credentials or insider threats.
2. **Access Control:** Enhances access management by ensuring that users have the appropriate permissions based on their identity and role within the organization, supporting zero trust principles.
3. **Integration with Existing Security Frameworks:** Works seamlessly with other Cisco security solutions and third-party systems to provide a comprehensive security posture that covers identity management, network security, and data protection.
4. **Reporting and Compliance:** Offers detailed reporting and analytics to support compliance requirements and audits, ensuring that identity-related activities are logged and traceable.

Key takeaways

By implementing Cisco Identity Intelligence, organizations can strengthen their security infrastructure, improve the accuracy of threat detection, and reduce the risk of identity-related breaches.



What is SSE?

SSE solutions help organizations provide secure connectivity for hybrid workforces, while protecting corporate resources from cyberattacks and data loss. Cisco's SSE solution, Cisco Secure Access, unifies multiple security functions into a cloud service to protect users and infrastructure from threats.

Goals of Cisco Secure Access:

- **Improve the user experience and productivity.** Delivers a universal experience that seamlessly and securely connects any user to any app or resource over and port or protocol.
- **Ease IT efforts.** Simplifies deployment and operations with a single console and centralized policy management that expands visibility into cloud applications, shadow IT, and shadow AI.
- **Achieve a higher level of consistent security.** Mitigates risk with granular, app-specific access to private applications.

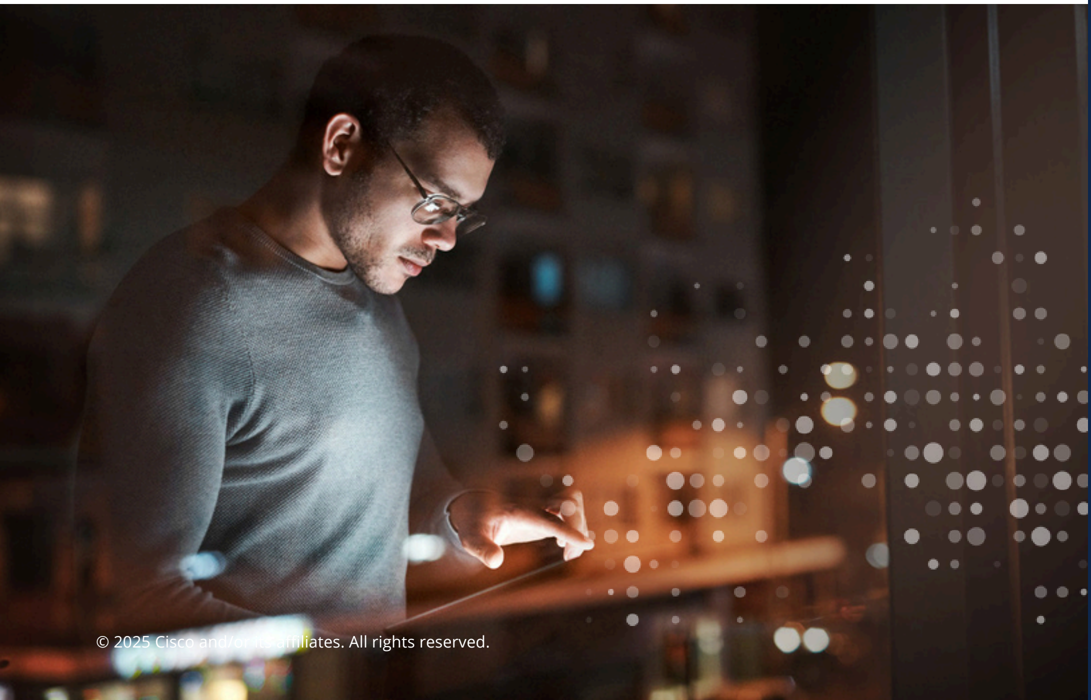
Key takeaway: The right SSE solution is one that can meet you where you are on your zero trust journey, and take you where you need to go. For example, you can roll out SSE capabilities like ZTNA, SWG, CASB, or DLP on your own timetable with flexible enforcement to meet geo-specific privacy mandates and optimize traffic flows.

SSE Core Capabilities

- Secure Web Gateway
- Zero Trust Network Access
- Firewall as-a-Service
- Cloud Access Security Broker
- DNS Security
- VPN as-a-Service
- Data Loss Prevention
- Sandbox
- Remote Browser Isolation

So much more

- GenAI App Usage Guardrails
- Digital Experience Monitoring
- Advanced Malware Protection
- Talos Threat Intelligence
- AI-powered Platform



What is Secure Access Service Edge?

Secure Access Services Edge (SASE) extends the notion of multiple security capabilities, unified and delivered in the cloud, by adding SD-WAN capability. A SASE solution can secure users from any location or device as they access the internet, SaaS apps, and private apps, while delivering a secure SD-WAN fabric across disparate connections and simplified, centralized management.

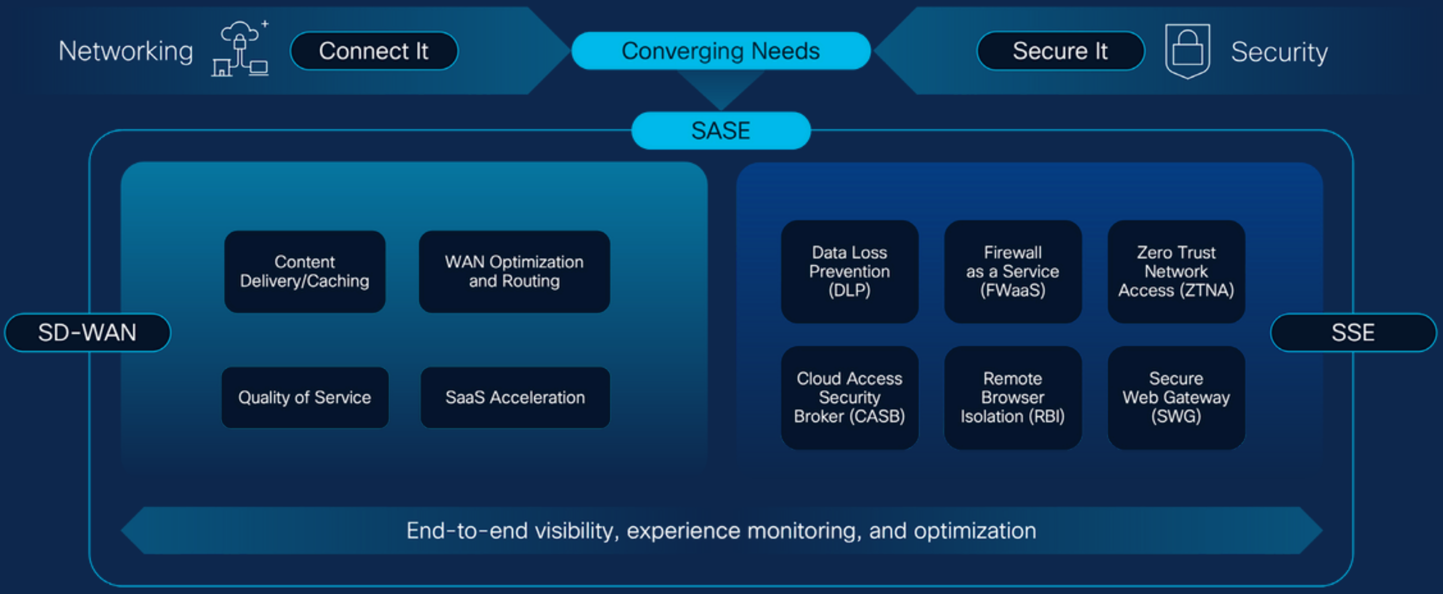
Goals of a SASE solution:

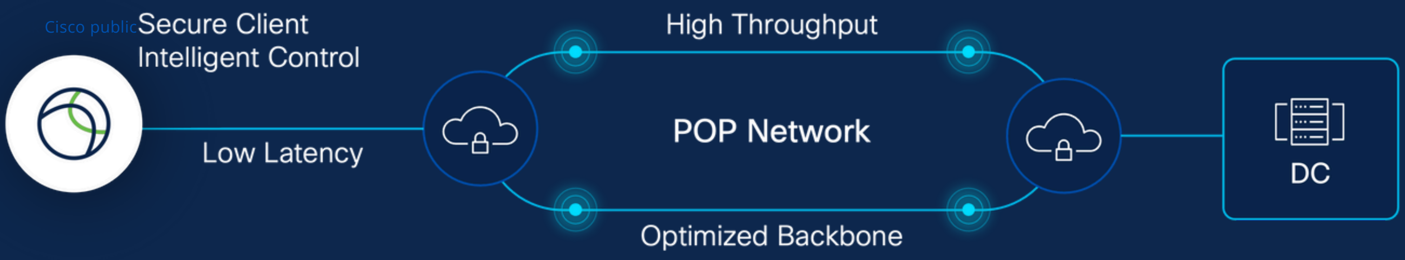
- **Connect everywhere work happens.** Enables secure remote and mobile access for distributed workforces to private and SaaS apps, plus other internet services.
- **Improve security with consistent policy.** Implements zero trust security, allowing you to control access with identity-first security and policy enforcement.
- **Reduce cost and complexity.** Streamlines operations with a single-vendor SASE and closes gaps, strengthening security posture and building greater resilience.

Key takeaway: SASE is a broad concept, which means you have flexibility in choosing options that are right for your needs. No matter the environment, a solution that is flexible and can be iterative at a pace that you choose is always a wise option. The two major SASE concepts are consolidation and simplification, so choosing a vendor that offers networking and security elements will position you for the most advantages. Additionally, if you are in a regulated industry or conduct business across different countries, data protection and sovereignty are important factors.

Secure Access Service Edge (SASE)

Thearchitectureforasecurelyconnectedexperience in today’s hyper-distributed environment


Networking
Connect It
Converging Needs
Secure It
Security
SASE
SD-WAN
Content Delivery/Caching
WAN Optimization and Routing
Quality of Service
SaaS Acceleration
Data Loss Prevention (DLP)
Firewall as a Service (FWaaS)
Zero Trust Network Access (ZTNA)
Cloud Access Security Broker (CASB)
Remote Browser Isolation (RBI)
Secure Web Gateway (SWG)
SSE
End-to-end visibility, experience monitoring, and optimization



Cisco's modern PoP architecture

LeveragesMASQUE/QUIC,VectorPacketProcessing (VPP), and a global peering

What are QUIC and MASQUE?

QUIC, originally developed by Google and subsequently standardized by the Internet Engineering Task Force (IETF), represents a transformative advancement in transport protocol technology. Operating atop the User Datagram Protocol (UDP), QUIC offers significant performance enhancements over the traditional Transmission Control Protocol (TCP).

Key Performance Advantages of QUIC:

1. **Connection Establishment:** QUIC significantly reduces latency by consolidating the handshake and encryption setup into a single step, as opposed to the multiple round trips required by TCP. This streamlined connection process facilitates quicker data transmission and improved network responsiveness.

2. **Built-in Security:** By integrating Transport Layer Security (TLS), QUIC provides encrypted connections by default, thereby enhancing both privacy and security within network communications.

3. **Multiplexing Streams:** QUIC supports multiple independent data streams within a single connection, effectively eliminating head-of-line blocking-a prevalent issue in TCP. This capability enhances user experiences by ensuring faster and more reliable data delivery, particularly beneficial for streaming, gaming, and web browsing applications.

4. **Connection Migration:** QUIC permits seamless connection migration without necessitating IP renegotiation, thus offering robust performance in environments characterized by low connectivity or for users who are frequently mobile.

By leveraging UDP, QUIC circumvents various inefficiencies associated with congestion control, retransmissions, and connection management, establishing itself as an ideal complement to MASQUE for modern network traffic optimization. In scenarios where QUIC might be restricted within an organization, a fallback to HTTP/2 is available to maintain continuity.

MASQUE (Multiplexed Application Substrate over QUIC Encryption), akin to specialized high-speed trains designed for QUIC's efficient rail system, is a standard developed to adeptly tunnel network traffic over QUIC. Its objectives include enhancing privacy, minimizing overhead, and providing seamless support across diverse protocols.

Benefits of MASQUE:

1. **Encryption:** MASQUE operates atop QUIC, inheriting its robust encryption capabilities to ensure secure data transmissions.

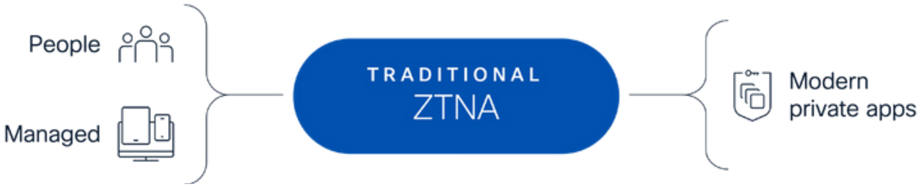
2. **Multiplexing:** MASQUE facilitates the conveyance of varied traffic types (such as HTTP/3 and VPN traffic) over a single connection, obviating the need for multiple protocol layers.

3. **Performance:** By reducing latency and overhead, MASQUE is particularly advantageous in mobile and constrained environments, eliminating the requirement for multiple TCP connections.

Key takeaway: The integration of MASQUE and QUIC into applications such as web browsers and mobile devices enhances end-user experiences by streamlining network operations and reducing the complexity associated with traffic routing and encryption. A practical illustration of MASQUE and QUIC's capabilities is evident in iCloud Private Relay, which bolsters privacy and performance by securely routing internet traffic through multiple relay servers. These technologies are seamlessly embedded within iOS and Samsung devices, delivering secure, resilient connectivity across platforms.

Traditional ZTNA Leaves Gaps

Moving from a legacy, hardware-based VPN to a cloud-based ZTNA model can work for most applications, but not all. Applications and their architectures are diverse, and trying to fit all apps into ZTNA will not work, meaning VPNs are still necessary.



ZTNA primarily uses HTTPS connections for modern applications. However, legacy applications might need a VPN/VPNaaS connection, which requires different handling and infrastructure.

SD-WAN customers pursuing a SASE architecture may struggle to protect their application performance gains. In these scenarios, complications can crop up when trying to integrate SSE solutions into the network infrastructure.

By using a disparate toolset, it can add complexity and introduce silos that prevent a unified, end-to-end picture of network performance.

Key challenges

- **Protecting identities for users and things.** Identity is central to zero trust, and that is precisely why it's under attack. As teams roll out controls like MFA, they must ensure they can deploy it in ways that frustrate attackers and not users. Plus, enforce least privilege for devices (e.g., printers, cameras, etc.), which is often overlooked by legacy VPN approaches.
- **Enforcing least privileged access.** Broad and inconsistent access privileges introduce security gaps and increase the risk of lateral movement.
- **Building resilience.** IT struggles with complexity, issue detection, and visibility. This increases the risk of configuration issues.

Common legacy applications that need a VPN/VPNaaS connection

If your organization uses any of the following key business applications, make sure the ZTNA solution you use can support them.

- SAP ERP
- Microsoft Exchange Server
- Oracle database

Traditional ZTNA does not adequately support today's hyper-distributed environments

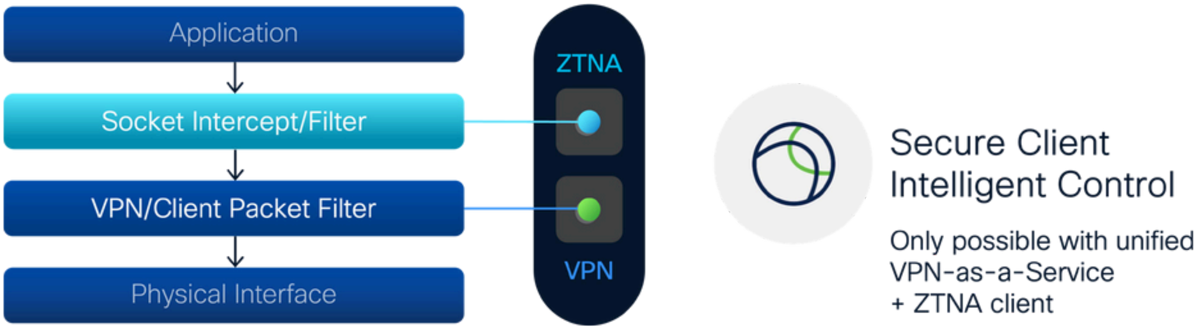
- All kinds of users
- All kinds of workplaces
- All kinds of things (IoT/IT)
- Managed and unmanaged devices
- Traditional/legacy apps
- Gen AI apps

Deep dive: The magic of Cisco's Secure Client

As networking paradigms evolve, moving from traditional models to Zero Trust Network Access (ZTNA) becomes crucial for organizations seeking enhanced security and seamless connectivity. Cisco's innovative approach employs advanced filtering technologies within Windows and macOS, such as the Windows Filter Driver and Network Extension framework, to support sophisticated traffic interception via our multi-purpose Secure Client (formerly known as AnyConnect). Unlike conventional VPNs that function at the packet level, Cisco's Socket Intercept technology operates at the socket and application stream level, capturing application streams and DNS requests before they reach the packet filter for more refined control and security.

ZTNA and VPN-as-a-Service coexistence and fallback

DNSinterceptionandsocketintercept


Application
Socket Intercept/Filter
VPN/Client Packet Filter
Physical Interface
ZTNA
VPN
Secure Client Intelligent Control
Only possible with unified VPN-as-a-Service + ZTNA client

Cisco stands out with its ability to integrate ZTNA and VPN within a unified client framework. Typically, ZTNA models require applications to be predefined for either ZTNA or VPN, not both. Cisco's Secure Access overcomes this limitation by allowing dual definitions, facilitating a seamless fallback to VPN if ZTNA is temporarily unavailable. This dual-layered approach prioritizes private application traffic through ZTNA for optimal security while maintaining the flexibility of VPN as a backup. By prioritizing ZTNA in network traffic interception, Cisco offers a robust and adaptable solution, streamlining the transition from traditional networking to a universal ZTNA architecture.

How to Know if Traditional ZTNA Isn't Enough for Your Organization

Use this quiz to assess where you are on your Universal ZTNA journey:

☐ We don't know how to start with ZTNA. My team is worried about the risks of using traditional VPN for access, but also are afraid of disruptions from implementing cloud-based ZTNA.

☐ We struggle to maintain consistent security for our users working from remote, on-campus, and branch office locations.

☐ Our IT and security teams must manage separate access policies (across multiple platforms) for legacy VPN-dependent applications and modern ZTNA-aware apps, leading to inefficiencies and gaps in coverage.

☐ Contractors, partners, and BYOD users complicate security enforcement. Many of our solutions require agent-based models that are impractical for unmanaged devices.

☐ Misconfigured access policies have led to security gaps, outages, and compliance violations, placing a heavy burden on our IT team.

☐ Our IoT/OT devices are tough to manage and monitor since an agent-based approach won't work.

☐ When remote and mobile workers are in environments like airplanes, factories, and rural areas, they often face poor performance because traditional TCP/IP-based solutions falter.

☐ We can't keep sensitive app data from flowing through a cloud PoP while enforcing zero trust policies and providing a common, streamlined user experience.

☐ It's a struggle to get strong identity protection in place because of coverage gaps and user pushback about authentication friction.

If you checked one or more of the boxes, continue on to our 10-step checklist for evolving to Universal ZTNA.

Evolving to Universal ZTNA: A Ten Step Checklist

Ready to unleash the strength of convergence between network and security to deliver zero trust everywhere? Follow this 10-step checklist to get started.

1. Identify connectivity challenges. Recognize common issues such as reliance on VPNs, inconsistent security across locations, and latency due to POP-only architectures.

2. Address security complexities. Tackle siloed policies for legacy and modern apps, manage BYOD and unmanaged devices, and mitigate risks from misconfigured policies. Enhance IoT/OT support and strengthen identity security.

3. Enable secure, reliable access. Ensure every user, device, and application can connect securely from any location over any network. Focus on delivering low-latency access to enhance productivity.

4. Assess identity posture. Discover and evaluate your entire identity population including accounts that may be at risk or may pose a risk to your organization.

5. Unify application support. Support legacy VPN-dependent, modern ZTNA-aware, and SaaS applications with a single, multi-purpose client and policy engine.

6. Enable agentless access. Benefit from Cisco's partnerships with Google Chrome Enterprise, Apple, and Samsung to support unmanaged devices and optimize the mobile experience.

7. Leverage intelligent access decisions. Use Cisco Identity Intelligence and Identity Services Engine for granular identity management and IoT/OT device security.

8. Apply unified policy and flexible enforcement. Implement unified policy with proactive policy assurance and flexible enforcement.

9. Accelerate zero trust maturity. Deliver consistent security across all users, devices, and locations with flexible adoption. Optimize security and performance, enforce least privilege controls, and manage third-party AI applications.

10. Reap the benefits. Increase user productivity with high-performance, consistent experiences. Control GenAI app usage and enforce data protection, accelerating zero trust maturity with a single-vendor solution.

Cisco Universal ZTNA Accelerates Zero Trust

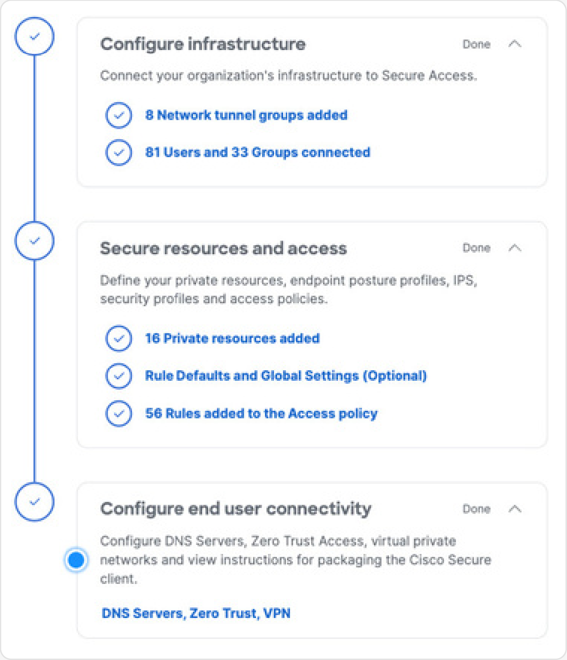
Simplifying zero trust access and policy management with a single vendor approach accelerates the journey to zero trust maturity. Cisco redefines what it means to achieve Universal ZTNA by using identity context to drive dynamic access policies for not only users, but the growing volume of things as well. With Cisco, security teams have the tools they need to deploy and manage zero trust for the modern, hybrid workforce using three pillars: access, identity, and resilience.

Modern Application Access	Extend Identity Context	Build Operational Resilience
Least privilege enforcement everywhere. Delivering seamless, unified access through the convergence of VPN and ZTNA in a single client and policy framework — reducing complexity and avoiding performance issues from legacy or cloud-only architectures.	Zero trust for IT and IoT, users and devices. Identity Services Engine (ISE) customers can easily leverage their security group tags (SGTs) within Cisco Secure Access policies to provide highly granular protection for internet/SaaS traffic and soon private traffic. No longer do you have to base access control on IP addresses or network hierarchy.	Policy and experience assistance, zero downtime. Ensuring resilient, reliable access everywhere—from office to remote and lossy environments—through built-in failover, AI-driven policy validation, and deep visibility into network paths.

Jumpstart your zero trust project today.

Cisco makes it easy to start where your need is greatest and evolve at your own pace. From a single management console, you can accelerate zero trust adoption to protect all users, all locations, all apps, and all devices.

With three simple steps, users can begin to access digital private resources using Cisco Secure Access.



Configure infrastructure Done

Connect your organization's infrastructure to Secure Access.

✓ 8 Network tunnel groups added

✓ 81 Users and 33 Groups connected

Secure resources and access Done

Define your private resources, endpoint posture profiles, IPS, security profiles and access policies.

✓ 16 Private resources added

✓ Rule Defaults and Global Settings (Optional)

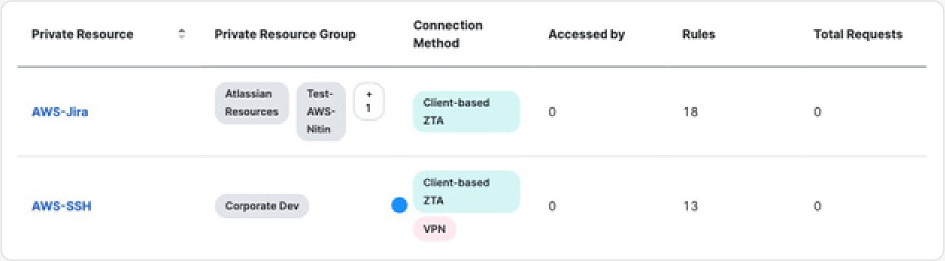
✓ 56 Rules added to the Access policy

Configure end user connectivity Done

Configure DNS Servers, Zero Trust Access, virtual private networks and view instructions for packaging the Cisco Secure client.

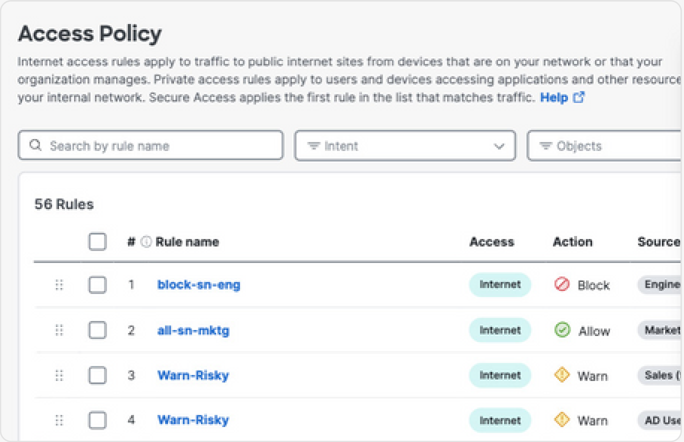
DNS Servers, Zero Trust, VPN

Step One: Decide how end users connect. You can allow secure access from managed and unmanaged devices to private and public resources leveraging ZTNA.



Private Resource	Private Resource Group	Connection Method	Accessed by	Rules	Total Requests
AWS-Jira	Atlassian Resources Test-AWS-Nitin + 1	Client-based ZTA	0	18	0
AWS-SSH	Corporate Dev	Client-based ZTA VPN	0	13	0

Step Two: Simplify policy management with application access that transitions seamlessly for users as they move between remote and local environments.



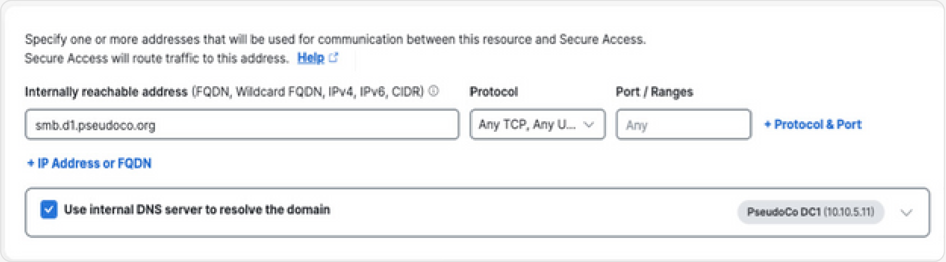
Access Policy

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 resource your internal network. Secure Access applies the first rule in the list that matches traffic. Help

56 Rules

☐	#	Rule name	Access	Action	Source
☐	1	block-sn-eng	Internet	Block	Engine
☐	2	all-sn-mktg	Internet	Allow	Market
☐	3	Warn-Risky	Internet	Warn	Sales (
☐	4	Warn-Risky	Internet	Warn	AD Use

Step Three: Set up client-based connections for your managed users and devices. This creates the definition of how users would access the private resource. You have the ability to define a variety of ports, protocols and port ranges.



Specify one or more addresses that will be used for communication between this resource and Secure Access. Secure Access will route traffic to this address. Help

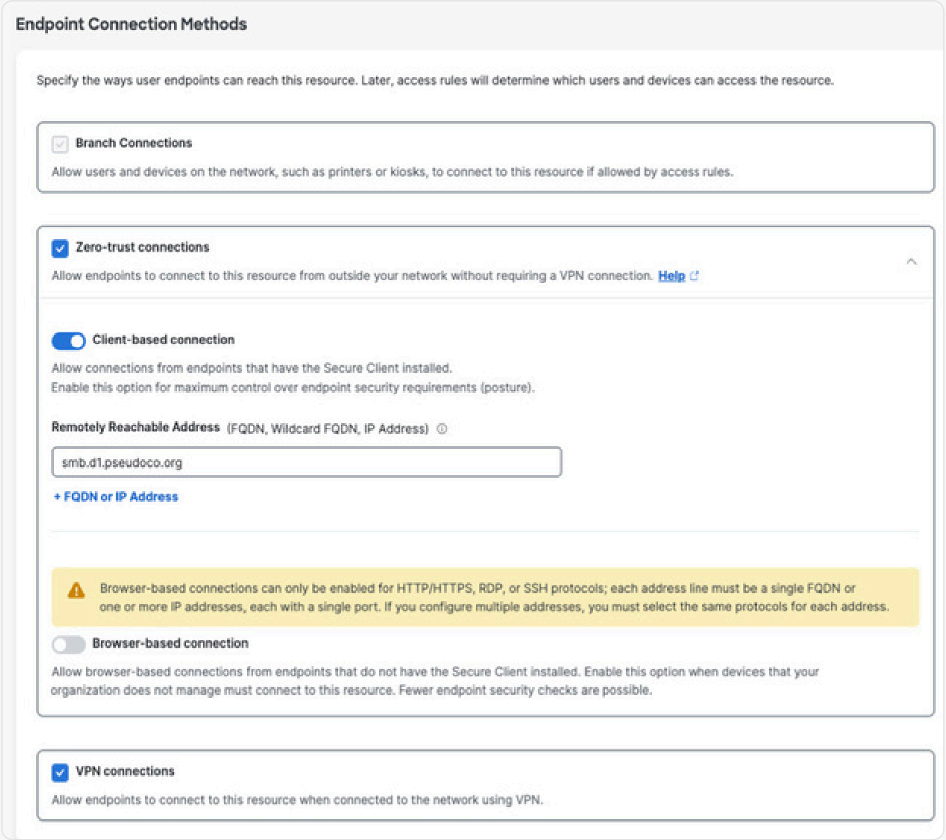
Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR): smb.d1.pseudoco.org

Protocol: Any TCP, Any U...

Port / Ranges: Any

☑ **Use internal DNS server to resolve the domain** — PseudoCo DC1 (10.10.5.11)

Next, create a definition for how the users would access the resource and define the connection method. This is one of the key differentiators that allows us to create a single resource but provide multiple connection methods that allows a private resource to have access over both VPN and ZTNA as an example.



Endpoint Connection Methods

Specify the ways user endpoints can reach this resource. Later, access rules will determine which users and devices can access the resource.

☑ **Branch Connections**

Allow users and devices on the network, such as printers or kiosks, to connect to this resource if allowed by access rules.

☑ **Zero-trust connections**

Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. Help

● **Client-based connection**

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

Remotely Reachable Address (FQDN, Wildcard FQDN, IP Address): smb.d1.pseudoco.org

⚠ Browser-based connections can only be enabled for HTTP/HTTPS, RDP, or SSH protocols; each address line must be a single FQDN or one or more IP addresses, each with a single port. If you configure multiple addresses, you must select the same protocols for each address.

○ **Browser-based connection**

Allow browser-based connections from endpoints that do not have the Secure Client installed. Enable this option when devices that your organization does not manage must connect to this resource. Fewer endpoint security checks are possible.

☑ **VPN connections**

Allow endpoints to connect to this resource when connected to the network using VPN.

App-to-app zero trust: Meet the Hybrid Mesh Firewall

Universal ZTNA secures user-to-application connections, while Hybrid Mesh Firewalls protect complex backend interactions happening in between applications. Modern applications rely on microservices that need robust security, but traditional firewalls can't cover all necessary points. The importance of firewall protection and segmentation has grown, vital for minimizing attack surfaces and reducing compromise impacts.

Cisco's Hybrid Mesh Firewall offers a distributed security fabric optimized for zero trust segmentation, covering cloud-native, legacy applications, and IoT. By integrating security into the network with DPU Switches and Security Cloud Control, Cisco brings security closer to applications, avoiding complex routing. AI-driven management simplifies operations, with Cisco 9300 Series Smart Switches and Hypershield, establishing efficient policy configuration and optimization.

Automatic configuration and deployment of cloud firewalls across environments leverage user and device context for segmentation. AI addresses patching gaps and detects threats in encrypted traffic without performance loss, supported by intelligence from Cisco's Talos. This ensures backend security matches initial user access protection.

Other vendors take a bolted-on approach to Universal ZTNA. Cisco leads the way by combining Universal ZTNA and Hybrid Mesh Firewall to provide a powerful defense strategy. By securing both the user access points and the intricate backend operations of applications, organizations can protect their digital assets with confidence.

Zero friction. Zero imposters. Zero downtime.

We know that if security is a barrier to productivity, users will go around it. Making security easy to get right for workers reduces risk and boosts productivity. Cisco delivers secure access with zero friction, protecting against identity-based attacks, so teams can enjoy resilient, zero downtime zero trust.

> “We wanted to approach security as one integrated ecosystem to ensure defense-in-depth. And the vendor with the most cohesive security platform was Cisco.”
>
> NetworkSecurityArchitect,Banking

Take the guesswork out of modernizing your security.

Ready to get started with Universal ZTNA? Work directly with a Cisco security specialist and see firsthand how Cisco’s Universal ZTNA is better for users, easier for IT, and safer for everyone.

- Gain deep understanding of how identity and trust make the user experience more seamless and achieve more granular control, a seamless user experience, and simplified IT operations.
- See how easy it is to implement our leading-edge SSE capabilities, including private access (ZTNA), data loss prevention (DLP), and remote browser isolation (RBI).
- Learn how to tailor Cisco Secure Access to address the unique pain points of your organization.
- Identify and isolate bottlenecks and issues with the network and end user experiences.

Register for a workshop today. Or, if you’d like to meet with one of our experts, feel free to request a call at your convenience.