Introduction to the Cisco Secure Networking Architecture

June 1, 2026

Executive summary

Enterprise networks are undergoing a fundamental transformation. Organizations must securely connect an expanding ecosystem of users, devices, applications, cloud services, AI-driven workloads, and autonomous agents while maintaining operational simplicity, resilience, and security. Hybrid workforces, distributed campuses and branches, cloud-native applications, operational technology, IoT devices, and emerging AI services have dramatically increased the scale and complexity of modern environments.

At the same time, the threat landscape continues to evolve. AI-powered attacks now operate at machine speed, data exfiltration remains a top business risk, and traditional perimeter-focused security models are no longer sufficient. Organizations must not only secure external access points but also continuously authenticate users, devices, and agents, enforce least-privilege access, contain lateral movement, and maintain visibility across increasingly dynamic environments.

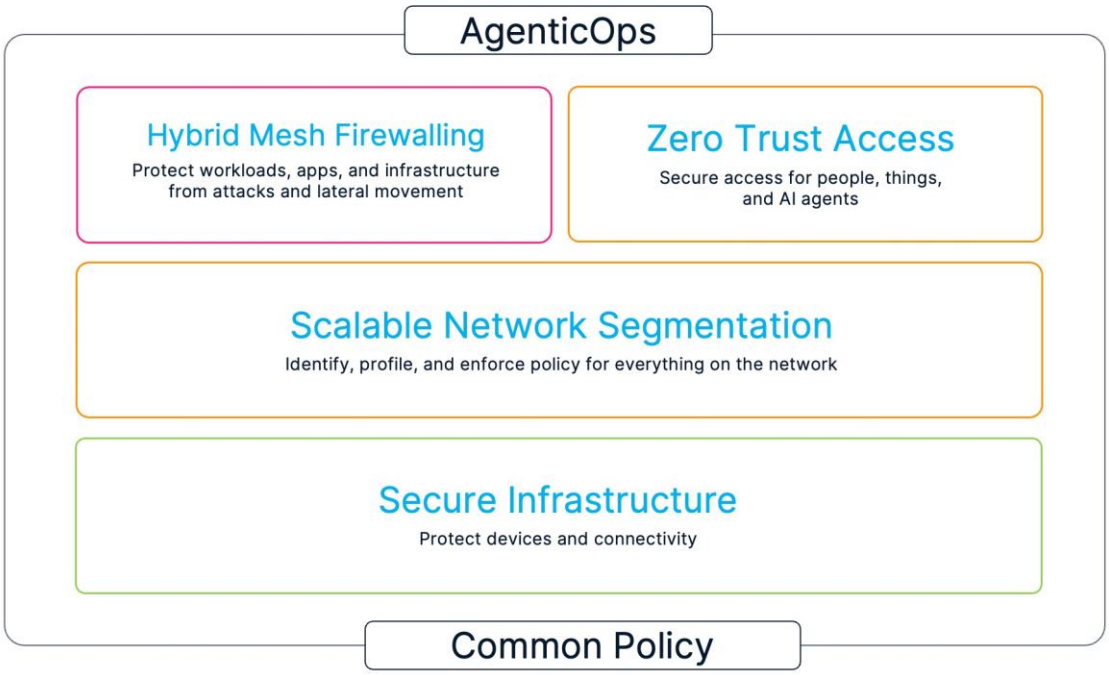
These challenges require a new approach where networking and security operate as a unified system rather than separate technology domains.

The **Cisco Secure Network Reference Architecture (SNRA)** provides that framework.

SNRA is Cisco's validated secure networking architecture for campus, branch, hybrid, and distributed enterprise environments. It combines secure connectivity, identity, segmentation, telemetry, policy enforcement, security operations, and ecosystem integration into a cohesive architecture where the network becomes an active participant in security enforcement and operational intelligence.

This document aligns to Cisco's Future-Proofed Workplaces and Cisco Secure Networking strategy by introducing the architectural foundation used to support secure, adaptable, and operationally efficient workplace environments..

Figure 1. Cisco Secure Networking Reference Design



Rather than treating security as a collection of isolated controls, SNRA distributes policy, visibility, and enforcement throughout the infrastructure. Cisco Identity Services Engine (ISE) serves as the primary source of identity context. Through authentication, authorization, device profiling, posture assessment, and policy evaluation, Cisco ISE establishes the identity attributes that drive policy decisions throughout the architecture. These identity attributes are represented through Security Group Tags (SGTs), authorization policies, and contextual metadata that can be consumed by networking and security platforms.

The architecture is designed to help organizations achieve several critical business outcomes:

- **Reduction and Simplification** through centralized management, automation, policy consistency, and reduced operational complexity.
- **Agility, Resilience, and Performance** through scalable architectures, resilient connectivity, and defense-in-depth design principles.
- **Secure and Consistent Access** through identity-driven controls and Zero Trust policy enforcement across users, devices, agents, applications, and locations.
- **Compliance, Risk Mitigation, and Enhanced Security Posture** through segmentation, least-privilege access models, and integrated policy enforcement.
- **Secure Agentic AI Readiness** through distributed security enforcement, authentication, visibility, telemetry, analytics, and extensible architecture that can adapt to emerging AI-driven traffic patterns and security requirements.

SNRA organizes these capabilities across five integrated architecture domains that provide a conceptual framework for understanding the architecture and how its major functions interact:

1. **Secure Network Infrastructure**
   Provides the resilient wired, wireless, routing, WAN, and cloud connectivity foundation required to securely transport users, devices, agents, applications, and services.
2. **Scalable Network Segmentation**
   Enables macro- and micro-segmentation strategies that build on network topology, business boundaries, and policy domains to contain risk, simplify policy application, and provide scalable separation of users, devices, agents, applications, and business functions. Segmentation is established through architectural constructs such as VRFs, overlays, security groups, and policy domains that create a scalable foundation for security enforcement.
3. **Zero Trust Access and Hybrid Mesh Firewall**
   Builds upon the segmentation foundation by applying identity-driven access control, contextual policy enforcement, and least-privilege principles across users, devices, agents, and applications. Identity, posture, location, device type, and other contextual attributes are used to dynamically enforce access decisions and security policy distributed security policy across campus, branch, cloud, remote-access, and application environments.
4. **Unified Management and Agentic Operations**
   Delivers centralized visibility, assurance, analytics, automation, lifecycle management, and AI-assisted operational workflows that simplify administration and improve operational efficiency.
5. **Extended Integration**
   Integrates networking, security, observability, IT operations, and third-party platforms into a coordinated operational model that improves visibility, incident response, and business alignment.

Together, these domains create a modular architecture that aligns infrastructure, segmentation, policy, operations, and ecosystem integration into a unified Secure Networking model. Below we focus on

introducing these domains and their relationships rather than providing detailed design, deployment, implementation, or validation guidance.

Deployment models

Recognizing that organizations operate under different business, operational, and regulatory requirements, SNRA supports multiple deployment approaches while maintaining a common architectural framework. Below are the deployment models supported by SNRA and the common architectural principles that span each approach:

- **Cloud-Managed**, emphasizing operational simplicity, centralized visibility, rapid onboarding, and SaaS-based lifecycle management.
- **On-Premises**, supporting organizations that require localized control, governance alignment, or customized operational workflows.
- **Programmable**, enabling infrastructure automation, API-driven operations, and integration with DevOps and NetOps practices.

Regardless of deployment model, the architectural principles, policy framework, and intended security and operational outcomes remain consistent.

This document provides an introduction to the Cisco Secure Network Reference Architecture (SNRA), presenting the architectural framework, core principles, major domains, and intended business outcomes that define the architecture. Intended for architects, engineers, technical leaders, partners, and customers, it establishes a foundational understanding of the structure, purpose, and value of the SNRA approach while serving as the basis for more detailed design, deployment, and validation guidance.

Business and technical drivers

Business drivers

Organizations continue to modernize infrastructure to support hybrid work, distributed operations, cloud adoption, and evolving security requirements. Modern enterprise architectures must improve agility, simplify operations, and maintain resiliency without increasing operational complexity.

Common business drivers include:

- **Lowering operational cost and increasing simplification** through simple centralized management, automation, policy consistency, lower network complexity, and less manual intervention.
- **Increasing agility, resilience, and performance** through a hardened, scalable architecture that supports resilient connectivity and defense-in-depth.
- **Providing secure and consistent access** through identity-driven access control and embedded Zero Trust principles that provide consistent policy enforcement across users, devices, and applications.
- **Providing for compliance, risk mitigation, and enhanced security posture** through segmentation, least-privilege access models, and integrated policy enforcement that help reduce exposure and strengthen security controls.
- **Agentic AI readiness** through distributed security enforcement, visibility, telemetry, analytics, and extensible architecture that support evolving application and traffic requirements.

Technical challenges

Many enterprise environments evolved through using separate tools, inconsistent policy models, and manually intensive processes. These conditions can limit visibility, increase operational overhead, and expand security exposure.

Common technical challenges include:

- Fragmented networking and security management platforms
- Limited visibility across users, devices, applications, and sites
- Inconsistent segmentation and policy enforcement
- Manual provisioning and change management workflows
- Difficulty scaling legacy designs for new locations or modern workloads
- Complex troubleshooting across wired, wireless, WAN, and security domains
- Increased risk from flat or loosely controlled networks

Design requirements

The Secure Network Reference Architecture (SNRA) was created to address these requirements through a modular, scalable, and deployment-flexible architectural framework that aligns networking, security, operations, and business outcomes..

The following functional requirements help illustrate the types of capabilities and outcomes the SNRA framework is intended to support and provide context for the architectural domains introduced throughout this document.

Functional requirements

The architecture should provide the following capabilities:

- Provide secure wired, wireless, WAN, and remote connectivity for users and devices

- Enable segmentation for business units, device classes, applications, and trust zones
- Support centralized identity-aware access control and policy enforcement
- Deliver integrated visibility for health, performance, telemetry, and security monitoring
- Support centralized and distributed operational workflows across deployment models
- Simplify onboarding and lifecycle management of sites, devices, and services
- Support resilient infrastructure and high-availability design practices
- Enable API-driven automation and integration with external platforms and operational tools
- Scale consistently across small, medium, and large enterprise environments

Non-functional requirements

The architecture should also support:

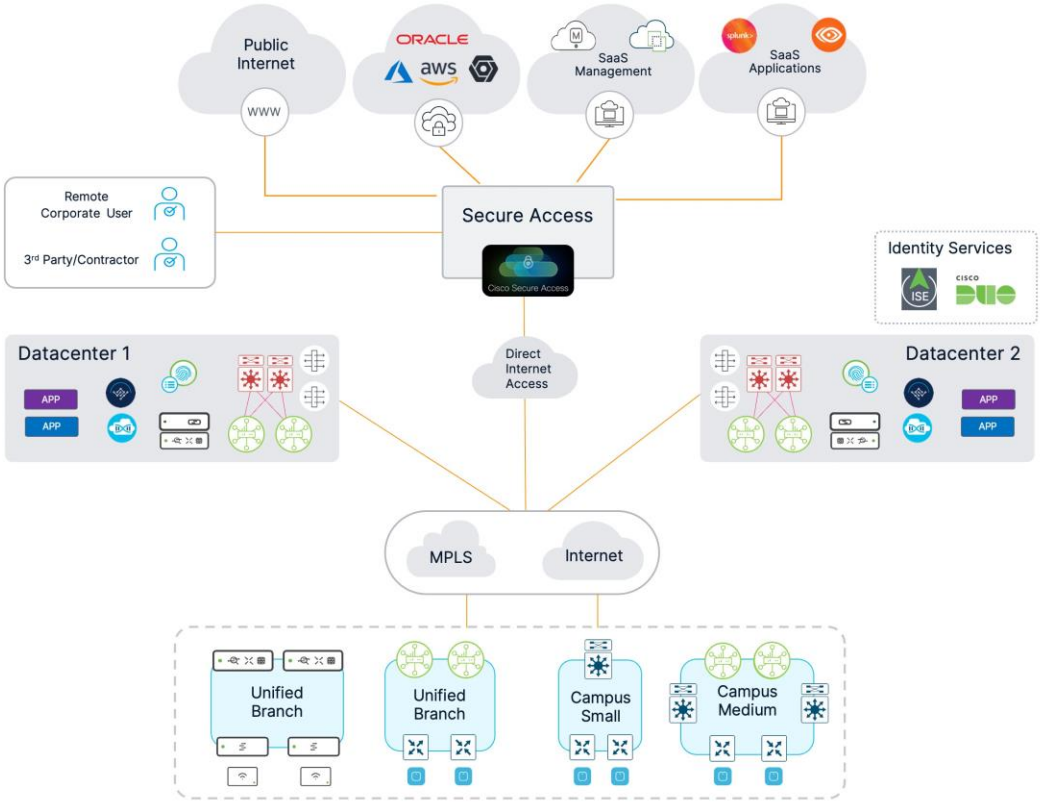
- High availability and resilient service delivery
- Scalable growth across additional users, devices, and locations
- Consistent operational model across multiple sites
- Simplified lifecycle management and software maintenance
- Zero Trust-aligned security architecture
- Reduced operational overhead
- Flexibility for future technology and business requirements

Solution overview

The Secure Network Reference Architecture (SNRA) provides a validated framework for designing secure campus, branch, and distributed enterprise networks through a unified Secure Networking architecture. Rather than treating networking and security as separate domains, this section introduces the major architectural domains and explains how connectivity, segmentation, identity, policy, security enforcement, observability, automation, and integrations operate together within a unified architectural model..

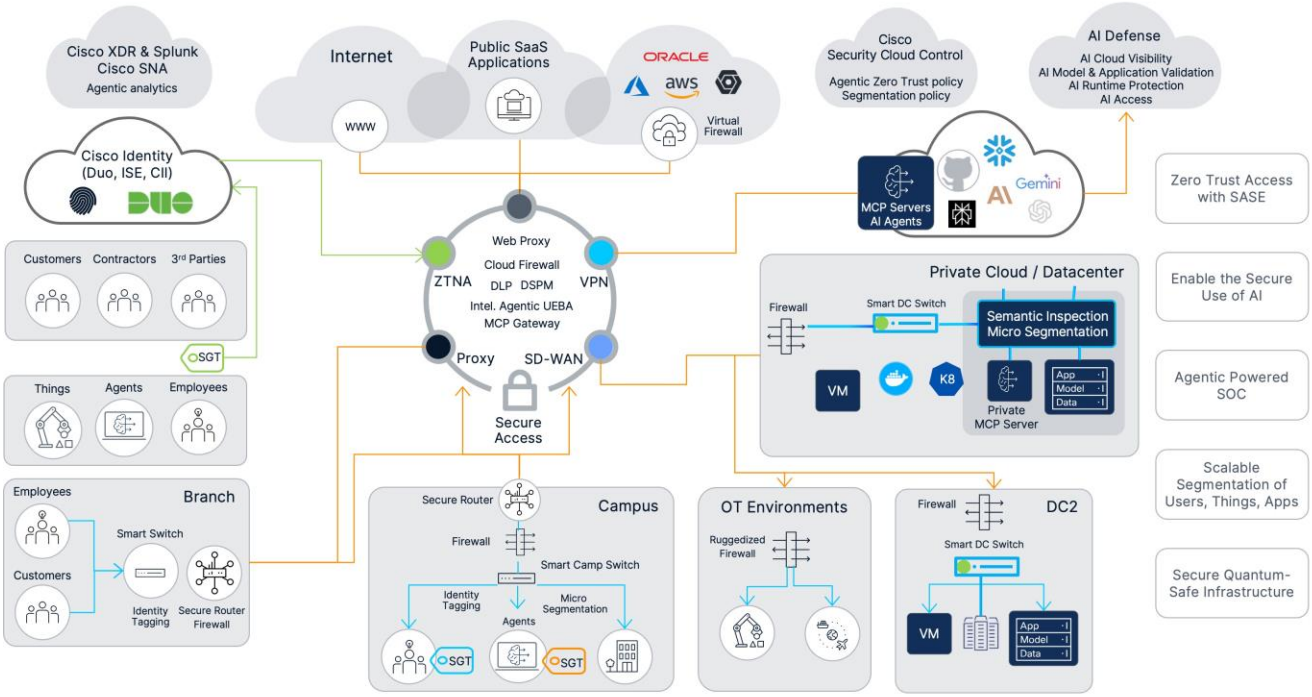
For Network Operations teams, SNRA provides a familiar networking foundation built on resilient switching, wireless, routing, WAN, and cloud connectivity services. The architecture preserves established networking design principles while extending the network into a distributed enforcement and observability platform. Identity, segmentation, telemetry, and policy information flow through the infrastructure, allowing the network to participate directly in security enforcement, visibility, and operational intelligence. This approach supports operational cost reduction and simplification while improving agility, resilience and performance across campus, branch, and cloud-connected environments.

Figure 2. Example Connection Types for the Cisco Secure Networking Reference Architecture



For Security Operations teams, SNRA provides a consistent framework for applying Zero Trust principles across users, devices, workloads, applications, and AI-enabled systems. Identity information established during onboarding and access control processes becomes a shared architectural context consumed by segmentation, policy enforcement, Hybrid Mesh Firewall services, observability platforms, and operational workflows. This integration enables secure and consistent access, improves compliance, risk mitigation and enhanced security posture, and supports emerging secure agentic AI requirements through coordinated policy enforcement and visibility across hybrid environments.

Figure 3. Example Connection Types for the Security Operations Reference Architecture



SNRA establishes a common architectural foundation that aligns networking and security operations under a unified operating model. Identity context flows from access and onboarding services into segmentation policies, security enforcement platforms, telemetry systems, operational analytics, and ecosystem integrations. This architectural progression enables organizations to reduce complexity, improve policy consistency, accelerate operations, and maintain security controls as users, devices, applications, cloud services, and AI-driven workloads continue to expand.

Key capabilities

SNRA enables organizations to modernize networking and security operations through a common architecture that integrates connectivity, identity, segmentation, security enforcement, observability, and automation. Each architectural layer contributes to a continuous operational workflow where identity context informs segmentation policy, segmentation guides enforcement decisions, enforcement generates telemetry, and telemetry drives operational intelligence and ecosystem integration.

The architecture delivers secure wired, wireless, branch, remote, and cloud connectivity while maintaining consistent policy enforcement and user experience. Macro-segmentation and micro-segmentation establish scalable trust boundaries, identity-aware controls apply least-privilege access decisions, and centralized operations platforms provide assurance, automation, and lifecycle management.

Key capabilities include:

- Secure connectivity across users, devices, workloads, applications, and sites
- Scalable macro-segmentation and micro-segmentation with identity-aware policy enforcement
- Distributed security enforcement through Zero Trust Access and Hybrid Mesh Firewall architectures
- Centralized visibility, assurance, telemetry correlation, and lifecycle operations
- Consistent identity context propagation across networking and security domains
- Flexible cloud-managed, on-premises, or programmable deployment models

- Open Ecosystem Integration and automation readiness
- End-to-end observability supporting user experience, operational assurance, and security operations

Cisco solution components

SNRA can be implemented using Cisco technologies selected according to operational requirements, deployment scale, management preferences, and business objectives. These platforms work together to create an integrated Secure Networking architecture in which identity, segmentation, policy, telemetry, and operational workflows are shared across networking and security domains rather than operating as isolated systems.

Possible solution components include:

- **Cisco Security Cloud Control (SCC)** for centralized security policy coordination, visibility, and multi-platform security operations
- **Cisco Meraki Dashboard** for cloud-managed operations, monitoring, assurance, and lifecycle management
- **Cisco Catalyst Center** for centralized automation, assurance, telemetry analysis, and operational management in on-premises LAN environments
- **Cisco SD-WAN Manager** for centralized WAN assurance, automation, policy orchestration, and operational management
- **Secure Access** and related Cisco security services for secure user connectivity, cloud-delivered enforcement, and Zero Trust access
- **Cisco Unified Branch** for full-stack cloud-managed branch operations
- **Cisco Identity Services Engine (ISE)** for identity services, authentication, authorization, device profiling, posture assessment, and policy-based access control
- **Cisco Hybrid Mesh Firewall** for distributed security enforcement across campus, branch, remote access, cloud, and application environments
- **Cisco Secure Firewall Threat Defense (FTD)** for advanced threat protection, segmentation enforcement, application visibility, and secure edge connectivity
- **Cisco Switches** for campus and branch wired access, policy-enabled connectivity, segmentation, and enforcement
- **Cisco Wireless** for secure mobility, wireless access, and identity-aware connectivity
- **Cisco Secure Routers** for branch connectivity, SD-WAN, segmentation transport, and integrated security services
- **ThousandEyes** for digital experience monitoring, path visibility, and end-to-end assurance

Together, these platforms enable identity information established by Cisco ISE to be consumed by segmentation services, Hybrid Mesh Firewall enforcement points, Secure Access, Secure Firewall platforms, Security Cloud Control, operational analytics systems, and ecosystem integrations. This shared context creates consistent policy enforcement and operational visibility across the architecture.

This overview establishes the architectural foundation, core concepts, and intended outcomes of SNRA, providing context for more detailed design, deployment, and operational guidance.