Cisco Secure Connect

Securely Interconnect Applications and Resources Hosted Anywhere

September 2024

Contents

Product overview

The new era of hybrid work requires a new approach, and SASE (Secure Access Service Edge) is a key enabler of any organization's hybrid-work strategy. SASE combines networking and security functions in the cloud with campus, branch, remote worker, and contractor (B2B) connectivity to deliver a secure, seamless user experience, anywhere users work – office, home, or coffee shop. But deploying SASE can be complicated. Connecting existing branch SD-WAN appliances and the myriad of user endpoints to a cloud-based fabric requires planning, integration, and configuration.

Cisco Secure Connect is a unified, turnkey solution with a blueprint for SASE made easy that converges Software-Defined Wide Area Network (SD-WAN) and Security Service Edge (SSE) to enable operational consistency across premises to the cloud in one powerful Cisco Meraki® dashboard, streamlining management across networking and security. Designed to be simple, complete, and unified, Secure Connect powers hybrid work across branch and remote, delivering greater network resiliency and seamless user experiences, everywhere.

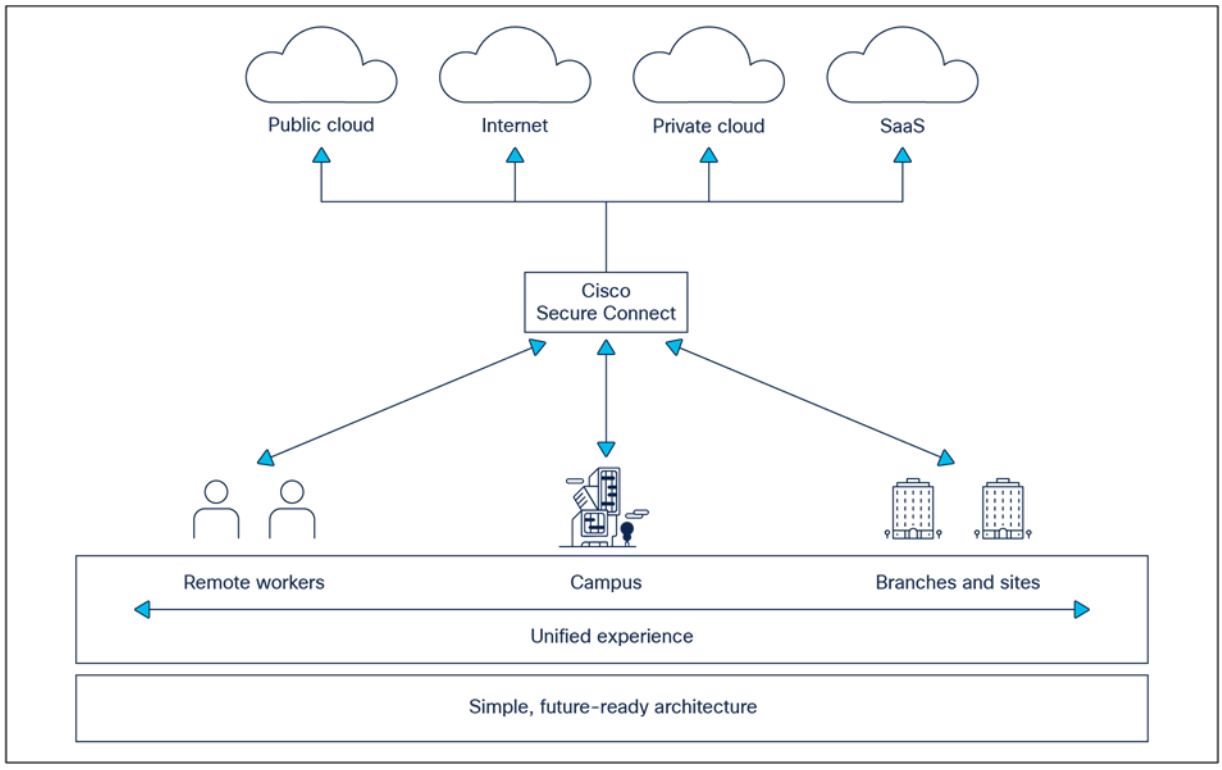

Figure 1.
Cisco Secure Connect use cases

Cisco Secure Connect securely connects users anywhere (in the branch or remote) to any application (in the private data center, public cloud, or SaaS) with a single subscription. The solution integrates client-based and clientless browser-based remote worker access, native Cisco Meraki SD-WAN connectivity, comprehensive cloud-based security capabilities with Zero-Trust Network Access (ZTNA), enhanced traffic acquisition, and Cisco Meraki SD-WAN policy import, with unified policy on the near horizon for enhanced posture.

Cisco Secure Connect is offered in two packages that make it easy for customers to choose the right level of protection and coverage for their organizational needs, so they can SASE their way.

Cisco Secure Connect Foundation

The Cisco Secure Foundation package includes Cisco Umbrella® SIG capabilities that provide secure internet access connectivity for branch and roaming users; Cisco Secure Connect fabric interconnect, providing private application access for branch users; a unified dashboard, offering streamlined operations management visibility and control for security and network policies; and unified, seamless support for your SASE needs. The Secure Connect Foundation package also includes 10 free-trial (non-production) licenses for hosted remote access as a service, which gives private application access for remote users.

Cisco Secure Connect Complete

The Cisco Secure Complete package includes production-level support, client-based remote access as-a-service capabilities, and both client-based and clientless browser-based ZTNA capabilities that provide a zero-trust security model for users.

Table 1. Core offer packages.

Package	Description	Features
Cisco Secure Connect Foundation Essentials	Secure internet-access connectivity for branch and roaming users	**Remote access:** free trial of 10 users with client-based access. **Security:** secure web gateway (proxy and inspection of web traffic URL filtering, secure malware analytics – up to 500 samples per day), cloud-access security broker (cloud application discovery, risk scoring, blocking, and cloud malware detection for two applications), Layer-3 and Layer-4 cloud firewall, and DNS-layer security. **Connectivity:** private access, network access control, direct SaaS and IaaS peering, Cisco Meraki Secure SD-WAN integration, and interconnection of sites, users, and applications. **Management dashboard:** simplified management and unified visibility of connectivity and security powered by Cisco Meraki. **Support:** 24x7 unified SASE support access through email and phone and access to documentation portal for self-help. **Global data center availability:** Foundation is now available globally in all SIG data centers. The enhanced headend capability is available in all of Europe, US, and part of Asia (Tokyo and Singapore).
Cisco Secure Connect Foundation Advantage	Data protection, advanced policy	**All features included in Cisco Secure Connect Foundation Essentials, plus:** **Security:** Layer-7 cloud-delivered firewall + IPS, inline data-loss prevention, cloud malware detection (for all supported applications), and secure malware analytics (unlimited sandbox submissions). **Global data center availability:** Foundation is now available globally in all SIG data centers. The enhanced headend capability is available in all of Europe, US, and part of Asia (Tokyo and Singapore).

Package	Description	Features
Cisco Secure Connect Complete Essentials	Secure internet, remote access as-a-service, and ZTNA for hybrid users	**Remote access/ZTNA:** client-based access, clientless browser-based access (up to 10 applications), granular user and application-based access policy, SAML authentication, posture and contextual access control, and reporting. **Security:** secure web gateway (proxy and inspection of web traffic URL filtering, secure malware analytics – up to 500 samples per day), cloud-access security broker (cloud application discovery, risk scoring, blocking, and cloud malware detection for two applications), Layer-3 and Layer-4 cloud firewall, and DNS-layer security. **Connectivity:** private access, network access control, direct SaaS and IaaS peering, Cisco Meraki Secure SD-WAN integration, and interconnection of sites, users, and applications. **Management dashboard:** simplified management and unified visibility of connectivity and security powered by Cisco Meraki. **Support:** 24x7 unified SASE support access through email and phone and access to documentation portal for self-help. **Global data center availability:** Cisco Secure Complete is now available globally, offering the full suite of unified SASE capabilities, including remote access and client as well as clientless ZTNA.
Cisco Secure Connect Complete Advantage	Data protection, advanced policy	**All features included in Cisco Secure Connect Essentials, plus:** **Remote access/ZTNA:** Client-based access and clientless browser-based access (up to 1000 applications/resources). **Security:** Layer-7 cloud-delivered firewall + IPS, inline data-loss prevention, cloud malware detection (for all supported applications), and secure malware analytics (unlimited sandbox submissions). **Global data center availability:** Cisco Secure Complete is now available globally, offering the full suite of unified SASE capabilities, including remote access and client as well as clientless ZTNA.

Features and benefits

Table 2. New features and benefits

Feature	Benefit
Native Meraki SD-WAN integration	Easily connect your branch and DC/HQ/private cloud Meraki sites (configured as hubs or spokes) to Cisco Secure Connect with built-in native Meraki SD-WAN integration for securing connections to the internet, SaaS, and private applications and resources. Leveraging the AutoVPN capability of your Meraki SD-WAN appliance at your branch sites for connectivity to the SASE fabric provides increased resiliency and intelligent path selection. This also enables the organization to implement consistent access and security controls across all connected sites.
Enhanced Meraki SD-WAN cloud head-end	Cisco Secure Connect introduces a dynamically scalable high-bandwidth headend solution for the Meraki SD-WAN integration. Leveraging Meraki's AutoVPN solution, this enhanced cloud traffic acquisition solution dynamically scales bandwidth per connecting Meraki SD-WAN site. The current bandwidth scale per site is approximately 500 Mbps, both unidirectional and bidirectional. This solution also offers an even more simplified user experience for integration of Meraki SD-WAN with Cisco Secure Connect.

Feature	Benefit
Browser-based Zero-Trust Network Access (ZTNA)	Cisco Secure Connect enables least privileged access control of private applications and resources without requiring any agent or client installed on the endpoint device. Administrators can easily assign access privileges for contractors and employees only to resources they need access to, without any lateral move capability. Administrators can configure posture profiles for endpoint OS and browser type to be used in the access decision.
Client-based Zero-Trust Network Access (ZTNA)	Client ZTNA offers a feature-rich solution powered by Cisco Secure Access, providing a seamless end-user experience that connects users to private applications and resources using any port and any protocol. User access to applications and resources is instant requiring fewer steps, delivering better remote worker experiences and stronger security. Administrators can reduce the attack surface, enforce least-privilege controls, enable posture validation, and eliminate security gaps in a distributed environment.
Client-based secure remote work (VPN)	Cisco Secure Connect enables remote users to access private applications from anywhere through the Cisco Secure Connect fabric using a Cisco Secure Client. Identity-based access control is possible using SAML authentication through the customer's IdP. Endpoint posture is also evaluated; this enables granular access control to private resources.
Secure internet access	Secure internet access provides safe access to the internet anywhere users go, even when they are off the VPN. Before the user is connected to any destination, Cisco Secure Connect acts as your secure onramp to the internet and provides the first line of defense and inspection, with hybrid protection on the edge and in the cloud. Regardless of where users are located or what they're trying to connect to, traffic can go through the fabric first. Once the traffic gets to the cloud platform, there are different types of inspection and policy enforcement that can happen, based on the security needs of the traffic. Cisco Secure Connect includes a secure web gateway, a cloud-delivered firewall, DNS-layer security, a cloud-access security broker, and data-loss prevention. This robust security solution receives real-time proactive threat updates from Cisco® Talos® intelligence, keeping your users secure while freeing your IT team from this tedious process.
User authentication	Cisco Secure Connect enables customers to bring their own identity provider (IdP) for end-user authentication to the service. Integration establishes a trust relationship with the IdP, which allows users to authenticate with their existing credentials via SAML 2.0 and synchronize any changes made in your IdP with Secure Connect via SCIM 2.0.
Meraki policy import	Cisco Secure Connect natively introduced a policy import feature that is specifically designed for those who currently have their remote workforce access company resources via remote access connections to the Meraki MX headend. If those customers are transitioning to Secure Connect remote access services, this feature will allow them to import their MX firewall policies affecting client VPN traffic to the Secure Connect cloud firewall through a guided wizard. This will help reduce the time administrators need to create and streamline their policies. Furthermore, it detects duplicates before the migration.

Feature	Benefit
Unified management	Cisco Secure Connect management is handled through a single dashboard to configure, monitor, and troubleshoot the service. Configuration is simplified with guided flows and dynamic checklists. Monitoring of users and sites occurs in a single pane of glass that unifies security and connectivity indicators. As part of consolidating network and security controls to unify and provide a single pane of glass experience, the following are some of the key updates: Unified Cloud-Delivered Firewall (CDFW): CDFW policy control and management of all branch-internet, remote users-internet, and interconnects is now available on the Secure Connect dashboard. Unified posture: Client-based and browser-based access posture control and management are now available on the Secure Connect dashboard. Remote access: Remote access service can now be configured and managed directly from the Secure Connect dashboard. Remote access logs can now be exported from the Secure Connect dashboard for all analysis and monitoring.
Network interconnect	Network interconnect provides intelligent routing between sources and destinations connected to Cisco Secure Connect. Any node connected to the interconnect seamlessly gains access to any already-connected node, with access policy -enforced in a unified way across the edge and cloud from Cisco Secure Connect. This drastically reduces network complexity, providing a highly available network fabric with minimal setup and maintenance.

Customer support

Cisco Secure Connect now offers 24/7 customer support by calling +1.617.206.4332 or by opening a support case from the product dashboard.

Document history

New or Revised Topic	Described In	Date
Updated Features to exclude geo location and versions for browser-based access, Generative AI and Meraki Authentication, updated Unified Management to address changes in remote access UI and number of supported app and resources	Page 5, 6, 7	August 16, 2024
Updated Features to include client ZTNA and Generative AI, updated core package to reflect global availability of Secure Connect Complete	Page 4, 5, 6	April 17, 2024
Made tweaks to Feature and Benefits	Page 5, 6	December 14, 2023
Updated package section to include Foundation and Complete details	Page 4, 5	June 21, 2023
Made tweaks to Product Overview, including use case graphic	Page 3	March 29, 2023
Added additional Features and Benefits	Page 5, 6	March 29, 2023
Changed services to reflect new customer support hours/availability	Page 6	October 20, 2022

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-3040871-07 09/24