Secure Access Service Edge (SASE)

Cisco Partner
https://cs.co/1page

Secure Access Service Edge (SASE) is a network architecture that combines VPN and SD-WAN capabilities with cloud-native security functions such as secure web gateways, cloud access security brokers, firewalls, and zero-trust network access. These functions are cloud delivered and provided as a service by the SASE vendor.

Functions of SASE Architecture (Core):

Secure Web Gateway (SWG): A gateway that inspects web traffic to provide full visibility, URL and application controls, and protection against malware. Some can also inspect web-hosted files and decrypt (HTTPS) traffic for advanced threat protection.

Firewall as a Service (FWaaS): Also referred to as a *Cloud Delivered Firewall* (CDFW). Offers visibility and control of internet traffic across all ports and protocols. You can log all activity and block unwanted traffic using IP, port, and protocol rules. You can also block or allow activity by application and by user.

Cloud Access Security Broker (CASB): Software that detects and reports on cloud applications in use across your network, exposing shadow IT and enabling the ability to block risky SaaS apps and specific actions and with multi-mode DLP capability.

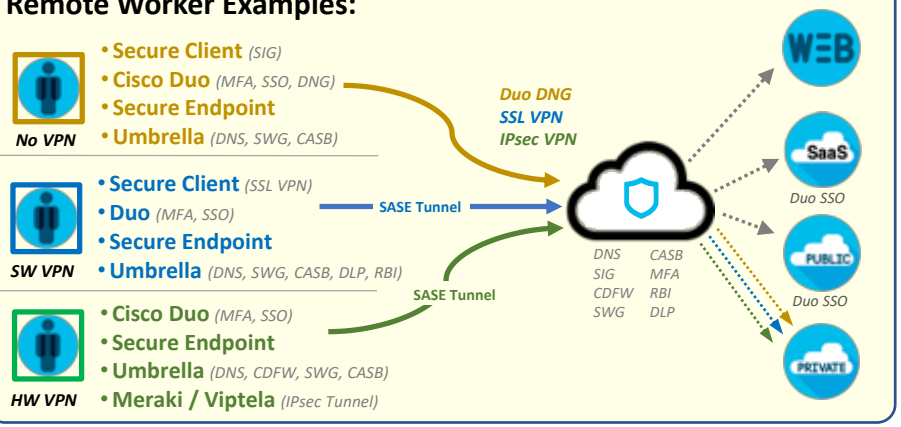
Zero Trust Network Access (ZTNA): A framework that helps prevent unauthorized access, contain breaches, and reduce risk of lateral movement across the network.

SD-WAN: A virtual WAN that allows companies to use any combination of transport services (MPLS, LTE, and broadband) to securely connect users to apps and locations.

Discovery Questions:

- What are you currently doing for security and visibility across your SD-WAN?
- What is your risk tolerance?
- What is your cloud strategy?
- What applications or data is critical to your organization?
- Where are you in your security journey?

Remote Worker Examples:



Cisco Solutions:

Cisco Secure Connect: Connect remote users to company applications with secure access to the internet, trusted SaaS and private applications.

Duo MFA: MFA is the foundation for zero trust. Duo verifies that your users are who they say they are, before they access your data — and with multiple second-factor options, including one-touch Duo Push, users can easily authenticate in seconds.

Duo Network Gateway (DNG): A reverse proxy that allows users to securely access on-prem websites, web applications, and SSH servers using a browser without VPN.

Meraki MX: Cloud managed security & SD-WAN appliance designed for distributed deployments that can direct traffic and prioritized across multiple uplinks.

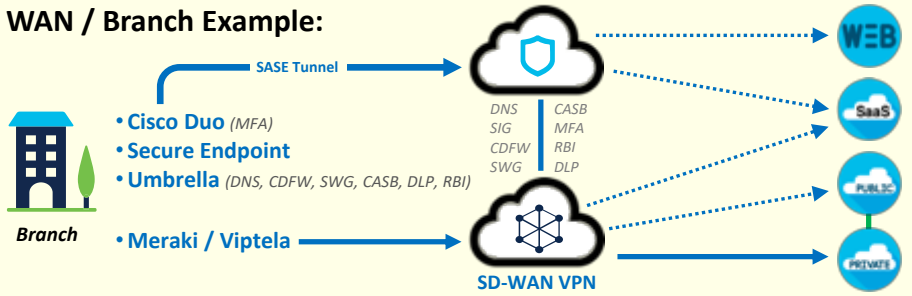
ThousandEyes: Visibility into the Internet, cloud, SaaS and the networks your organization runs on by combining Internet and WAN visibility.

Umbrella: A DNS cloud security platform that secures Internet access and cloud applications across your network, branch offices, and roaming users.

Umbrella Secure Internet Gateway (SIG): A set of security functions in a single, cloud-native service including firewall, secure web gateway, cloud access security broker, data loss prevention, Remote Browser Isolation (RBI) and more.

Viptela (SD-WAN): Software-defined approach to managing the wide-area network, or WAN. Extend intent-based networking across the branch, WAN, and cloud.

WAN / Branch Example:



Resources:

Products & Platform	SASE NFR Lab Guide	What is SASE?
Cisco Secure Connect	SASE vs SSE Positioning	Cisco SD-WAN
SASE Architecture Guide	Deployment case study	Public page